

## コンピュータセキュリティ インシデント対応チーム (CSIRT) のための ハンドブック

本翻訳文書は、有限責任中間法人 JPCERT コーディネーションセンターが、原書の著作権を保有する Carnegie Mellon University/Software Engineering Institute (CMU/SEI) から許諾を得て翻訳したものです。

CMU/SEI: <http://www.sei.cmu.edu/>

日本語版の内容について、原書に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。

また、翻訳監修主体は本文書に記載されている情報より生じる損失または損害に対し、いかなる人物あるいは団体にも責任を負うものではありません。

# コンピュータセキュリティ インシデント対応チーム (CSIRT) のための ハンドブック

Moira J. West-Brown  
Don Stikvoort  
Klaus-Peter Kossakowski  
Georgia Killcrece  
Robin Ruefle  
Mark Zajicek

初版 : 1998 年 12 月  
第 2 版 : 2003 年 4 月





**Carnegie Mellon  
Software Engineering Institute**

---

Pittsburgh, PA 15213-3890

コンピュータセキュリティ  
インシデント対応チーム  
(CSIRT) のための  
ハンドブック

CMU/SEI-2003-HB-002

Moira J. West-Brown  
Don Stikvoort  
Klaus-Peter Kossakowski  
Georgia Killcrece  
Robin Ruefle  
Mark Zajicek

初版 : 1998 年 12 月  
第 2 版 : 2003 年 4 月

**Networked Systems Survivability Program**

Unlimited distribution subject to the copyright.

本書の初版は、以下の団体・機関からの資金提供により発行されました：

U.S. National Science Foundation (NSF);  
SURFnet bv;  
SURFnet ExpertiseCentrum bv;  
M&I/STELVIO bv;  
German Federal Ministry of Education, Science, Research and Technology (Bundesministerium fuer Bildung, Wissenschaft, Forschung und Technologie);  
Verein zur Foerderung eines Deutschen Forschungsnetzes e.V. (DFN-Verein).

本書の改訂版は、Software Engineering Institute からの資金提供により発行されました。

発行元

SEI Joint Program Office  
HQ ESC/DIB  
5 Eglin Street  
Hanscom AFB, MA 01731-2116

本書で述べている意見と見解は、DoD（米国国防総省）の公式見解ではありません。本書は科学的、技術的情報交換の目的で発行されたものです。

FOR THE COMMANDER



Christos Scodras  
Chief of Programs, XPK

本書の制作は米国国防総省が後援しています。Software Engineering Institute は、米国国防総省が後援し、連邦政府資金によって運営されている研究開発センターです。

Copyright 2003 by Carnegie Mellon University.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use. Requests for permission to reproduce this document or prepare derivative works of this document for external and commercial use should be addressed to the SEI Licensing Agent.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (<http://www.sei.cmu.edu/publications/pubweb.html>).



---

# 目次

第2版の発行にあたって .....	ix
初版の発行にあたって .....	xi
謝辞 .....	xiii
要約 .....	xv
翻訳にあたって .....	xvi
<b>1 序文</b> .....	<b>1</b>
1.1 本書の目的.....	4
1.2 対象読者 .....	5
1.3 本書の活用.....	6
1.4 本書の構成.....	7
<b>2 基本事項</b> .....	<b>9</b>
2.1 CSIRTの枠組み.....	9
2.1.1 ミッションステートメント.....	10
2.1.2 Constituency（サービス対象者） .....	11
2.1.3 組織内の位置付け .....	17
2.1.4 他のチームとの関係 .....	19
2.2 サービスと品質の枠組み .....	21
2.3 CSIRTのサービス .....	23
2.3.1 サービスの分類.....	24
2.3.2 サービスの詳細.....	25
2.3.3 サービスの選択.....	34
2.4 情報流通 .....	34
2.5 ポリシー .....	38
2.5.1 属性 .....	39
2.5.2 内容 .....	40
2.5.3 検証 .....	40
2.5.4 施行、保守、強制.....	41
2.6 品質保証 .....	41
2.6.1 品質システムの定義 .....	42
2.6.2 チェック：品質パラメータの測定基準.....	44
2.6.3 バランス：品質保証のための手順.....	46
2.6.4 Constituencyの視点から見た品質.....	47
2.7 個別ニーズへの適応 .....	48
2.7.1 柔軟性の必要性.....	49
2.7.2 法律の問題.....	51



2.7.3	組織の規制	58
<b>3</b>	<b>インシデントハンドリングサービス</b>	<b>61</b>
3.1	サービスの詳細	61
3.1.1	目的	62
3.1.2	定義	63
3.1.3	機能の詳細	64
3.1.4	可用性	65
3.1.5	品質保証	65
3.1.6	やり取りと情報開示	65
3.1.7	他のサービスとのインタフェース	66
3.1.8	優先順位	66
3.2	サービス機能の概要	66
3.3	トリアージ機能	68
3.3.1	トラッキング番号の使用	70
3.3.2	報告用の標準フォームの使用	73
3.3.3	連絡先の事前登録	74
3.4	ハンドリング機能	75
3.4.1	インシデントのライフサイクル	76
3.4.2	インシデント分析	79
3.4.3	インシデント情報の追跡	91
3.5	アナウンス機能	93
3.5.1	アナウンスのタイプ	93
3.5.2	事前の検討事項	95
3.5.3	アナウンスのライフサイクル	97
3.6	フィードバック機能	100
3.7	やり取り	102
3.7.1	連絡窓口	103
3.7.2	認証	106
3.7.3	安全な通信	110
3.7.4	特別な考慮事項	110
3.8	情報のハンドリング	119
3.8.1	情報の収集	120
3.8.2	情報の検証	121
3.8.3	情報のカテゴリ化	121
3.8.4	情報の保管	123
3.8.5	情報のサニタイズと処分	124
3.8.6	優先順位付けの基準	125
3.8.7	エスカレーションの基準	129
3.8.8	情報開示	133
<b>4</b>	<b>チームの運営</b>	<b>137</b>
4.1	運営要素	137
4.1.1	作業スケジュール	137
4.1.2	通信	138
4.1.3	電子メール	138
4.1.4	ワークフロー管理ツール	139
4.1.5	World Wide Web情報システム	139
4.1.6	IPアドレスとドメイン名	140

	4.1.7 ネットワークとホストのセキュリティ .....	140
4.2	基本ポリシー .....	141
	4.2.1 行動規範 .....	142
	4.2.2 情報のカテゴリ化ポリシー .....	143
	4.2.3 情報開示ポリシー .....	145
	4.2.4 メディアポリシー .....	148
	4.2.5 セキュリティポリシー .....	149
	4.2.6 人的エラーポリシー .....	150
4.3	継続性の保証 .....	152
	4.3.1 継続性に対する脅威 .....	152
	4.3.2 ワークフロー管理ツール .....	155
	4.3.3 時間外の対応範囲 .....	157
	4.3.4 オフサイトの対応範囲 .....	159
4.4	セキュリティ管理 .....	160
4.5	スタッフの問題 .....	167
	4.5.1 CSIRTスタッフ .....	167
	4.5.2 スタッフの採用 .....	170
	4.5.3 着任および離任手続き .....	172
	4.5.4 スタッフのトレーニング .....	173
	4.5.5 スタッフの維持 .....	175
	4.5.6 スタッフの補充 .....	175
<b>5</b>	<b>あとがき .....</b>	<b>177</b>
5.1	初版を書き終えて .....	177
5.2	第2版を書き終えて .....	178
	<b>付録A：執筆者紹介 .....</b>	<b>181</b>
	<b>付録B：用語集 .....</b>	<b>187</b>
	<b>参考文献 .....</b>	<b>193</b>



---

# 図の目次

図 1 : 組織内のCSIRT .....	18
図 2 : CSIRT間の関係 .....	21
図 3 : ミッションステートメントから派生するサービスと品質の枠組み .....	22
図 4 : インシデントハンドリングサービスの機能 .....	67
図 5 : CERT/CCインシデントハンドリングのライフサイクル .....	77
図 6 : CERT/CC行動規範 .....	143



---

# 表の目次

表 1 : CSIRTの種類とそのミッションおよびConstituencyの例 .....	11
表 2 : CSIRTとConstituencyの間の考えられる権限関係 .....	14
表 3 : サービス明細の属性 .....	23
表 4 : 一般的なCSIRTサービスのリスト .....	25
表 5 : インシデントハンドリングサービスとの間に考えられる情報流通の例....	36
表 6 : 基本的なポリシーの属性 .....	39
表 7 : ポリシーの内容の特徴 .....	40
表 8 : 動的環境の要因の例とCSIRTへの影響 .....	50
表 9 : 不作為に起因する法的責任問題の例 .....	56
表 10 : 署名済み契約の内容に起因する法的責任問題の例 .....	56
表 11 : 情報開示に起因する法的責任問題の例 .....	57
表 12 : チームのタイプ別に考えられる インシデントハンドリングサービスの目的の範囲 .....	62
表 13 : ハンドリング機能属性の例 .....	76
表 14 : 分析の深さの要因 .....	82
表 15 : ログファイルの注目すべき特性 .....	84
表 16 : インシデント情報の追跡 .....	92
表 17 : 考えられるチーム内の支援タイプ .....	113
表 18 : 情報共有のための検討事項 .....	114



---

## 第2版の発行にあたって

『CSIRT ハンドブック』（CSIRT Handbook）の更新版が公開されているのかどうか、尋ねられることがよくあります。執筆者である私たちはハンドブックを定期的に見直しており、記載されている資料やガイダンスがまだ通用し、有効であり、新しいチームにも既存のチームにも役立つと考えています。取り上げている例と組織体の中には古くなったものもありますが、概念と推奨事項は現在の業務にも有効です。

2002年の夏、CERT<sup>®</sup> CSIRT Development Teamは、CSIRT機関のサービスの詳細についての標準セットを作るために、Trusted Introducer for European Computer Security Incident Response Teams（CSIRT）サービスとの連携を始めました。そしてその文書<sup>1</sup>が完成したときに、この新しいサービスリストを盛り込むように、CSIRTハンドブックを確かに更新すべきだと気付いたのです。ドキュメントの改訂を始めるにつれ、古い例や現在は使われていない用語を更新する時期だとも感じました。さらに必要に応じて、ハンドブックに説明されている情報に関連すると考えられる新しい話題、リソース、CSIRTの運営活動などの参考情報も追加しました。

ただし最終的には、初版への変更をできるだけ少なくすることにしました。主な変更点は以下のとおりです。

1. ハンドブックに掲載されていた例の多くは更新しました。旧版の例も概念的に正しく、ガイダンスは現在もなお有効であると分かっているため、いくつか残してあります。今日の読者により適していると思われる最近の例を新たに追加しました。
2. 新しいCSIRTサービスの定義がハンドブック全体に盛り込まれています。
3. 本書は、執筆者たちが制作した、あるいは制作中の他の新しいドキュメント、特に新しい『Organizational Models for CSIRTs』というハンドブックと関連しています。同書は本書の姉妹編であり、CSIRT機能を果たすために実装できる組織構成と対応サービスの種類に関する詳細情報が記載されています。この最新版のCSIRTハンドブックの公開は、『Organizational Models for CSIRTs』ハンドブックの出版と時期を合わせました。

CSIRTハンドブックの「初版の発行にあたって」に書かれているように、執筆者たちは他者の経験から学ぶことができ、毎日学んでいます。そのため、この第2版に関してご意見のある方、ご意見を共有したい方、あるいは追加のご提案などがある方はご連絡ください。FIRST Conferencesや他のCSIRTイベントにも定期的に参加しているので、直接お話する機会もありますし、

---

<sup>1</sup> サービスのリストは<http://www.cert.org/csirts/services.html>から入手できます。



csirt-handbook@cert.org 宛てに電子メールをお送りいただくことで、グループとしてご連絡をいただくことも可能です。

---

# 初版の発行にあたって

コンピュータセキュリティインシデントへの対応と防止のための体制を整える必要性に組織が対応するにつれ、コンピュータセキュリティインシデント対応チーム（CSIRT）の数も増え続けています。コンピュータサイエンスが、それ自体で科学の一分野として認められるように取り組みがなされてきたのと同様、コンピュータセキュリティも、コンピュータサイエンスの不可欠な要素として認められるように取り組みがなされてきました。同様に、セキュリティ分野においてCSIRTの必要性が認められるべきです。これまで新しいチームを作ろうとするたびに、その存在の必要性を正当化する必要があり、対応しようとしている問題に関する支持と理解を得るといった困難に直面してきました。このような困難を何とか克服しても、CSIRTを効果的に構築、運用し、その認知度を高める方法を示した文書情報がないというさらなる難問に直面してきました。そのため、本書のようなハンドブックの必要性が長年の懸案でした。

本書を執筆するアイデアは、1996年の夏に初版の執筆者たち（West-Brown、Stikvoort、および Kossakowski）が電子メールで議論したことから生まれました。当時、執筆者たちはそれぞれの組織で同じようなプロジェクトに関わっていました。他のCSIRTがそのポリシーや手順を作成・開発するのを支援していました。執筆者たちは、新たに構築されるチームから構築や運用に関する支援要請が増えるのを目の当たりにして、増え続ける要請に応えられる専門家が不足していることに気付きました。CSIRTの構築と運用の仕事は、チームの破たんにつながりかねない落とし穴がたくさんあるため、優秀で尊敬されるCSIRTの基盤を固めるためには、サポート情報とガイダンスが不可欠になることは明らかでした。

この種の多くのプロジェクトと同様に、ハンドブックの作成には当初の予想より時間がかかりました。空いた時間に取り組もうとしていたためです。この分野は変化が著しいうえに要求が厳しく、専門家が不足しているので、空き時間はたいてい深夜や週末でした。1996年の10月には1週間のほとんどを使える余裕ができ、集まってハンドブックの調査に専念し、問題の概要を22ページに構成しました。その基礎を準備して、各自の組織に戻り、さまざまなセクションの内容をゆっくり書き始め、その後のドキュメント作成を続けました。

その結果である初版がCSIRTの構築、管理、および運用に役立つ参考文書となることを期待しています。本書で紹介する資料は、各執筆者の組織におけるCSIRTの構築や運用、および他のCSIRTの構築や運用を支援する中で経験したことをベースにしています。



---

# 謝辞

初版のハンドブックの作成に貢献してくださった多くの人々に感謝いたします。まず、CERT<sup>®</sup> Coordination Center (CERT/CC)、Verein zur Foerderung eines Deutschen Forschungsnetzes e.V. (DFN-Verein)、M&I/STELVIO, U.S. National Science Foundation (NSF)、SURFnet ExpertiseCentrum bv、およびSURFnet bvに感謝いたします。これらの組織が資金提供を通じてこの取り組みを支援してくださったおかげで、このプロジェクトに時間とリソースをかけることができ、経験を積み、この分野で活躍する機会を得ることができました。このプロジェクトの締め切りに追われているときに、インシデントやコンピュータセキュリティの緊急事態への対応に協力してくれたCERT/CC、CERT-NL、およびDFN-CERTの同僚たちに特に感謝いたします。

また、CSIRTの構築や運用において支援を求めてくださった組織にも感謝いたします。厳密な調査を要する質問に答え、さまざまなニーズや状況を共有することで、その分野に関する洗練された考えを得ることができ、経験の範囲を広げることができました。

本書の初稿の技術レビューは、さまざまな方にご協力いただきました。CSIRTの構築に関心はあってもコンピュータセキュリティの分野をよく知らない人たちから、技術的または管理的視点からかなりの運用経験のある人たちまで、横断的な査読者を選びました。このような人たちが忙しいかもしれないので、草稿を読み短期間でフィードバックをくださるのはおそらく8名程度の方だろうと期待して15名の査読者を選びました。感動的にも、14名の方が何らかのフィードバックをくださいました。もう1名の方からは、病気のために査読できなかったとのご説明をいただきました。時間を割いて、本書の初稿にコメントを寄せてくださった査読者の方々全員に感謝いたします。

David Finch (MOREnet)  
Eduardo Garcia (Price-Waterhouse)  
John Horton (DANTE)  
Erik Huizer (SURFnet ExpertiseCentrum bv)  
Larry J. Hughes, Jr. (NorthWestNet)  
Georgia Killcrece (CERT/CC)  
Kathleen Kimball (Pennsylvania State University)  
Wolfgang Ley (DFN-CERT)  
Hannes P. Lubich (SWITCH-CERT)  
Jorgen Bo Madsen (NORDUnet CERT)  
Ken McNulty (SEI)  
Maj. Byron Thatcher (AFIWC/AFCERT)

---

<sup>®</sup> CERTは米国特許商標局に登録されています。

Wietse Venema (IBM)  
Mark Zajicek (CERT/CC)

特に、期待していた以上に非常に多くの詳細なコメントをくださった Larry J. Hughes, Jr.、Georgia Killcrece、Wolfgang Ley、Hannes P. Lubich、および Jorgen Bo Madsen には感謝したいと思います。

本書の初稿は、母国語が異なる 3 名の執筆者が書いた興味深い著作物でした。その原稿を受け取り、技術レビュー用の文書を作る作業は、Bill McSteen (SEI のテクニカルライター／エディタ) が担ってくれました。Bill が文章のばらつきを平準化する素晴らしい仕事をしてくれたおかげで、レビュー担当者は技術と構造に関するコメントに集中することができました。Bill の継続的な努力は、本書の最終版を提供するのに不可欠でした。

第 2 版では、同じく SEI のテクニカルライター／編集者である Pamela Curtis に感謝しています。彼女の専門的な支援がなければ、この仕事を成し遂げるのははるかに難しかったでしょう。その技術と編集での支援には大いに助けられ、執筆者たちは資料の内容に集中することができました。

また、技術部長の Barbara Laswell 博士にも心から感謝したいと思います。同氏は本書の改訂を後押しし、改訂に専念するリソースと時間を惜しみなく提供してくださいました。

最後に、家族にも感謝したいと思います。家族の支え、理解、励ましがなければ、本書を完成させることはできなかったでしょうし、これが楽しい経験であることにも気付かなかったでしょう。

---

## 要約

本書では、コンピュータセキュリティインシデント対応チーム（CSIRT）の構築と運用に関するガイダンスを提供します。本書は特に、組織において CSIRT のコアサービスであるコンピュータセキュリティインシデントハンドリングサービスの種類と範囲を定義し、文書化する際に役立ちます。本書では、サービスを構成する機能、それらの機能の相互関係、サービスの実装に必要なツール、手順、および役割について説明します。また、CSIRT と他の組織との相互関係や機密情報の取扱方法についても説明します。さらに、設備、セキュリティ、スタッフ配置の考慮事項など、運用上の問題や技術的な問題も取り上げます。

本書は、サービス、ポリシー、および手順が明確に定義または文書化されていない新たに構築されるチームや既存のチームに有益なリソースを提供することを目的としています。本書の主な対象読者は、CSIRT またはインシデントハンドリングサービスの構築や運用に対して責任のある管理者です。また、CSIRT のスタッフ全員、上級管理職、その他 CSIRT とやり取りする方などが参考資料として使うこともできます。

---

# 翻訳にあたって

本書は米国CERT<sup>®</sup> Coordination Centerより発行された『Handbook for Computer Security Incident Response Teams (CSIRTs)』を翻訳したものです。

本翻訳では、原著者の許可の下、原著に存在したいくつかの誤りを修正しています。また原著公開後に内容に変更が発生している点については訳注にて追記しています。

有限責任中間法人 JPCERT コーディネーションセンター (JPCERT/CC)

---

# 1 序文

インターネットの進化については広範囲に渡って記録されています。インターネットは、ある研究プロジェクトで地理的に分散したほんの少数のシステム間で通信を確立したことから生じ、現在では無数のシステムで構成されるネットワークの膨大な集合として世界中を網羅しています。

インターネットは地球上で最も強力に広範に利用できる通信媒体の1つとなり、インターネットへの依存も日々増えています。政府、企業、金融機関、および学校はインターネット上で日常業務を行っています。このような普及に伴い、ネットワーク上に存在して流れるデータも、銀行取引や証券取引から医療記録、著作権データ、個人の通信などさまざまです。

インターネットは安価で簡単に利用できますが、インターネットに接続するシステムは、管理が容易であるとは言えません。結果として、安全に構成されていないインターネットシステムが数多く存在します。さらに、インターネット通信を支える基盤のネットワークプロトコルはセキュアでなく、現在利用可能な数少ないセキュリティ保護機能を利用しているアプリケーションもわずかしかなかったりありません。

ネットワーク上で入手できるデータと、データを安全に保護することの難しさから、インターネットシステムは脆弱な攻撃対象になっています。メディアでインターネット上の侵入行為の記事を見かけることも珍しくありません。

しかし、インターネットにおけるセキュリティ侵害の問題は新しい現象ではありません。1988年には「インターネットワーム」インシデントが発生し、当時、ネットワーク上のシステムの大部分に障害が発生し、一時的に利用できなくなりました。このインシデントの直後に、インターネットにおけるコンピュータセキュリティインシデントへの対応を改善する方法を明らかにするための会議が開かれました。この会議の結果出された勧告には、セキュリティ情報を対象とする信頼できる広報機関として機能し、インターネットセキュリティ問題を扱う単一の窓口を設立する必要性が盛り込まれていました。この勧告を受けて、インターネット上のコンピュータセキュリティインシデントに対応するために、CERT<sup>®</sup> Coordination Center が結成されました（CERT/CCとも呼ばれており、もともとは Computer Emergency Response Team という名称でした） [CERT/CC 1997b]。

---

<sup>®</sup> CERTは米国特許商標局に登録されています。



CERT/CCは、この種の組織のうち最初に設立された組織、すなわちコンピュータセキュリティインシデント対応チーム (CSIRT<sup>2</sup>) の1つです。

CSIRTは消防署に例えると非常に簡単に説明できます。消防署には緊急電話番号があり、火災が発生したり、その疑いがあるときにかけられるのと同様に、CSIRTにも電話番号と電子メールアドレスがあり、コンピュータセキュリティインシデントが発生したり、その疑いがあるときに支援を求めて連絡を取ることができます。CSIRTサービスは、必ずしも目の前に現れて対応するものではありません(もっとも、そのようなサービスを提供するものもあります)。通常は、電話または電子メールによって対話を行います。

消防署とCSIRTのもう1つの類似点は、緊急事態への対応はサービスの一面に過ぎないということです。同様に重要なのは、第一に緊急事態が起こらないようにすることです。そのため、消防署が火災安全教育を実施して認識を高め、最善策を奨励しているように、CSIRTでは技術文書を発行して、同じ目的で教育およびトレーニングプログラムを実施しています。改善のための活動では、消防署は安全規定と耐火製品の改善を保証する法律に影響を与えます。同様にCSIRTは、基本のセキュリティ基準を改善するフォーラムに参加しています。

「インターネットワーム」インシデントが発生したときに、ネットワークの規模は60,000ホストと推定されました。10年後、インターネット上のホストは3,600万を超え、それに伴って侵入行為も増加しています。2003年1月のInternet Domain Survey [ISC 2003]によると、1億7,160万のホストがドメインネームサービスによって案内されています。1つのCSIRTでこのように膨大なConstituency(サービス対象)に効果的にサービスを提供できないことは明らかです。特に、単一のCSIRTでは、時間帯、言語、文化、および組織的な問題のため、インターネットを構成するさまざまなコミュニティの個別のニーズに対応できません。これに対し、いくつかの組織は、そのコミュニティに影響を与える侵入行為に対応する体制を整える必要性を予測していました。結果として、CSIRT構築への関心が急速に高まりました。

1988年以降、世界中で無数のCSIRTが結成されましたが、現在それらは、運用し始めるにつれて、CSIRTの構築のときと同様に多くの難問に直面しています。新たに構築されたチームは一般に、サービスの適用範囲の決定や、運用ポリシーおよび手順の作成のときに指導や支援を求めてきます[Pethia 1990a, Pethia 1990b]。この『CSIRTハンドブック』を1998年に最初に出版したときには、新

---

<sup>2</sup> 本書の初版を出版したときは、CSIRTのコアサービスを説明する際に「インシデント対応 (incident response)」という用語を使用しました(そのため、CSIRTという頭字語の「IR」文字が慣例になっています)。チームに対する理解が成熟するにつれ、インシデント対応は、何らかのイベントへの単なる対応以上のことを含む、より広い「インシデントハンドリング (incident handling)」サービスの1つの構成要素になりました。そのため、本書(および他の出版物)では「インシデントハンドリング」という表現を使用しています。しかし、「CSIRT」という頭字語はチームの総称であり、コミュニティで広く採用されている用語であるため、これから先も使用することにします。

しいチームによる適切で信頼できるサービスの構築の支援となるようなリソースは、それほど多くありませんでした。現在は、雑誌記事、書籍、チュートリアル<sup>3</sup>、その他各種の資料のほか、Web上のリソースを多数利用できます<sup>4</sup>。また、FIRST (Forum of Incident Response and Security Teams) やTERENAの後援を受けているTF-CSIRT (ヨーロッパにおけるCSIRT間の協力を推進する対策委員会) など、さまざまな組織がチーム間の協力を促進し、新生および既存のチームを支援するためにリソースを提供しています [TERENA 1995]。幸いなことに今日、新たに構築されるCSIRTは、独力で取り組む必要がありません (つまり、自らの経験だけから教訓を学んだり、コストのかかる間違いを犯したりする必要はありません)。他の多くのチームが苦労した経験を活用して、効率的なチームを構築・導入することができます<sup>5,6,7</sup>。

最近、組織による CSIRT 機能の構築に役立つ情報は増えてきましたが、残念ながら、運用上のポリシーや手順 (新たに構築されるチームが適合・修正して利用できる一般的な CSIRT ポリシー、手順、およびテンプレート) の面では利用できる情報はまだほとんどありません。既存のチームは文書化して共有するものが何もないか、機密性が高いために資料を共有できません。この分野の専門家がまだ不足しているため、専門家の助言を求めることも困難です。従来から活躍している専門家は引っぱりだこで、空き時間がほとんどなく、依頼すると費用が高くなる可能性があります。

運用段階に入った後も、明確に定義されたサービス、ポリシー、および手順の必要性が低下することはありません。既存の CSIRT の中で、明確に定義されたサービスが欠落しているところは共通して、運用上の問題が繰り返し発生しています。例えば、そのような CSIRT では、既存のスタッフが新しいスタッフにその運用経験を伝えるというやり方をしています。このような CSIRT が示すサービスの一貫性、信頼性、およびレベルは、各チームメンバーのさまざまな認識によって大幅に変化することがよくあります。結果として、これらの CSIRT の Constituency (コンスティテュエーション: サービス対象者) は、提供されるサービスに関して間違った印象を持つ可能性があるため、チームの成功に不可欠な CSIRT とその Constituency の信頼関係を危うくするおそれがあります。明確に定義され文書化されたサービスはチームに役立ち、さらに重要なことに、チームの Constituency にとってのガイダンスになり、結果として、CSIRT が提供するサービスやそれらをどのように利用すべきかについて理解を高めることができます。

---

<sup>3</sup> CERT/CCでは、例えば、CSIRTの管理責任者とインシデント対応者向けに、各種の講座を提供しています。 [http://www.cert.org/nav/index\\_gold.html](http://www.cert.org/nav/index_gold.html)を参照してください。

<sup>4</sup> 詳細については、CERTのCSIRT Development Teamのリソースリスト (<http://www.cert.org/csirts/resources.html>) を参照してください。

<sup>5</sup> 『Workshops on Computer Security Incident Handling』、Forum of Incident Response and Security Teams、(1989~2002年)も参照してください。

<sup>6</sup> Sandy Sparks, Katherine Fithen, Marianne Swanson, およびPat Zechman, 『Establishing an Incident Response Team』チュートリアル、9th Workshop on Computer Security Incident Handling、FIRST (Forum of Incident Response and Security Teams)、英国ブリストル、1997年6月。

<sup>7</sup> Don StikvoortおよびKlaus-Peter Kossakowski, 『Incident Response Teams: the European Perspective』、8th Workshop on Computer Security Incident Handling、FIRST (Forum of Incident Response and Security Teams) カリフォルニア州サンノゼ、1996年7月。

## 1.1 本書の目的

本書では、CSIRTを構築して運用するときに考慮すべき一般事項に関するガイダンスを提示します。消防署の例に戻りますが、効果的なサービスを提供するのは複雑な業務です。適切なポリシーと手順に基づき、一連の事後対応型

(reactive)と事前対応型(proactive)の両方の問題に対処していなければ、CSIRTは成功しません。消防署は有志や直接的な資金援助によって運営が成り立っています。提供するサービスは利用可能なリソースと資金に基づきます。CSIRTも他の組織と同様にコスト削減を要求されています。そのため、提供したいサービスの範囲および水準と、現実に提供できる内容との間で常にトレードオフする必要があります。これには、与えられた状況に適したCSIRTサービス、ポリシー、および手順の確認が含まれます。また、効率良いインシデントハンドリング機能を実装するために、取り組むべき運用上の問題を特定することも重要です。

特に、本書は、組織がコンピュータセキュリティインシデントハンドリングサービスの特徴と範囲を定義して文書化する際に役立ちます。この目的のために、サービスを構成する機能、それらの機能の相互関係、サービスの実装に必要なツール、手順、および役割について述べます。また、インシデント分析にも重点を置いています。消防署が火事の原因(天災、放火、電气的設計の過失)を理解するための調査を行うのと同様に、CSIRTもインシデントの原因を理解しようと取り組みます。消防署の分析には灰の鑑別などが含まれますが、CSIRTの分析にはシステムログや侵入者が残したファイルの調査などが含まれます。

消防署は、出動要請がピークのとことや難局に対応するときに応援を求める(または要求される)ことがあるため、他の消防署と協力する必要があります。また、他の救急隊と協力して適切に対応し、法的に必要とされる情報を警察に提供する場合もあります。本書では、CSIRTがセキュリティ問題を報告してくるサイト、他のCSIRT、警察、メディアなど、他の組織とどのように協力するかについて述べます。消防署も情報を処理する必要がありますが、その一部は犯罪者に関連することもあるので慎重に扱う必要があります。同様に、CSIRTも情報を適切に処理する必要があります。ほとんどのCSIRTは緊急用電話と同じように依頼者の機密を保持し、報告者と被害者に関する情報が公開されないように保護します。この原則はCSIRTの存続にとって不可欠です。情報を適切に処理してくれる組織として信頼できなければ、誰も報告しなくなり、CSIRTがほとんど役に立たないものになるためです。このため、情報の取り扱いが本書において最も重要な話題です。

専任スタッフを抱えているCSIRTもありますが、パートタイム、有志、および信頼できるセキュリティの専門家を集めてセキュリティ危機に対応しているCSIRTもあります<sup>8</sup>。CSIRTのスタッフは世間の人々との橋渡し役であり、個々のスタ

---

<sup>8</sup> さまざまなスタッフ配属モデルに関する詳細は、2003年にWebサイト(<http://www.cert.org/csirts/>)に公開されている手引書『Organizational Models for CSIRT』を参照してください。

スタッフがその行動を通じて与えるイメージ、提供するサービスの質はCSIRTの成功にとって最も重要です。適切な資格のあるスタッフは引く手あまたなので、見つけるのが難しいこともあります。しかし、CSIRTスタッフの採用責任者が無意識のうちに、人材候補に求めるスキルと資質を誤解していることがよくあります。そのため、スタッフ配置と採用の問題、および一貫性があり友好的でプロフェッショナルな対応を、チームに対してとれるCSIRTスタッフの確保について、取るべき手順について述べます。

CSIRTは、インシデントハンドリングサービスに加えて、脆弱性への対処や侵入検知サービスなど、さまざまなサービスを提供します。これらのサービスに関する高度な説明も盛り込みましたが、個別の手順やポリシーについては、本書では触れていません。

本書の内容は、有料サービス型のチーム、特定組織の社内チーム、または国際的なコーディネーションセンターなど、あらゆる種類のCSIRT環境に適用できるように、適度に汎用性を持たせて記述しています。

## 1.2 対象読者

多くの新しいCSIRTが構築され運用段階に入っていますが、これらのチーム数の増加はインターネットの成長と侵入者の活動に追いついていません。より多くの組織が、そのニーズに応えてくれるCSIRTの必要性を認識しています。このような必要性を予想して、本書は、CSIRTの設立に最も深く関与する方々を対象としています。

本書の主な対象読者は、以下の少なくとも1つについて責任がある管理者です。

- CSIRTの構築
- CSIRTの運用
- インシデントハンドリングサービスの創設
- インシデントハンドリングサービスの運用

上級管理者とすべてのCSIRTスタッフにとって有益な参考資料であるだけでなく、本書はCSIRTとやり取りする、もしくはCSIRTに影響を及ぼす問題を認識することで恩恵を受ける以下の方も利用できます。

- CSIRTのConstituencyのメンバ
- 法的執行機関
- メディアへの広報窓口

CSIRTサービス<sup>9</sup>を他のマネージドサービスプロバイダに「委託」している組織もあるとは思いますが、本書ではそのような読者には特に重点を置いていません。しかし本書の内容は、そうしたプロバイダも利用でき、組織や企業に有料サービスを提供するためのアプローチに合うように適用できると思います。そのため、サービスプロバイダにとっては、他のCSIRTがConstituencyにサービスを提供するときに直面するような問題を特定する場合に、本書が有益な資料になるでしょう。

## 1.3 本書の活用

本書は、サービス、ポリシー、および手順が明確に定義または文書化されていない新たに構築されるチームや、既存のチームに有益な資料を提供することを目的としています。理想的には、組織がCSIRTを構築するための経営管理者による支持と財政的支援を獲得したあと、チームが運用段階に入る前の早い段階で利用すべきです。しかし、運用段階にあるチームにも非常に有用な参考文献になると思われます。

本書は、新たに構築されるチームにとっては、CSIRT構築に伴うさまざまな問題を理解するための目安となります。その後は、ドメインまたは組織に固有の詳細なサービス定義、ポリシー、手順の策定、運用問題への取り組みの参考に利用できます。本書に提供されている資料を適用することにより、組織は文書化されて信頼性もあり、効果的で確実なインシデントハンドリングサービスの体制がほぼ整うはずです。

さらに、既存のチームは本書を利用して、インシデントハンドリングサービスを策定するときに組織に適した主要な問題と選択肢を網羅しているかを確認できます。

執筆者たちは成功したアプローチだけでなく、回避すべき落とし穴についても、適宜指摘しています。さらに、特定の状況に適している可能性のあるさまざまな選択肢、または国際対応チーム、国内対応チーム、顧客にサービスを提供するインターネットサービスプロバイダ (ISP) チーム、または大学や企業などの単一の組織に向けたチームなど、特定の種類のチームに適用できる選択肢についても説明します。ただし注意していただきたいのは、この資料は参考情報とガイダンスのために提供されているということです。個々のチームが実装すべきサービス、ポリシー、および手順の範囲や内容を指示することが目的ではありません。それらは、CSIRTとそのConstituencyの個別のニーズに基づいて決める必要があります。そのため、本書で示されている資料は、チーム固有の環境に該当する問題を理解したり、チームの目標、ニーズ、および要件を満たすアプローチを選択したりするために利用することをお勧めします。

---

<sup>9</sup> Software Engineering InstituteのNetworked Systems Survivability Programは、GSA FedCIRC (General Services Administration Federal Computer Incident Response Center) からの資金助成を受けて、『Outsourcing Managed Security Services』レポートを作成しました。CERT Webサイト (<http://www.cert.org/security-improvement/modules/omss/>) から入手できます。

## 1.4 本書の構成

本書の残りの部分は次のように構成されています。第2章では、CSIRTモデルの基本的な枠組みを示し、すべてのCSIRTで考慮して対処する必要がある基本的な問題について述べます。CSIRTの一般的な用語と概念も紹介します。具体的には、Constituencyを明確に定義することの重要性、ポリシーの作成と実装、CSIRTの組織上の問題や法律上の問題の影響などを取り上げます。さらにCSIRTが提供すると考えられるさまざまなサービスを紹介し、それらのサービスとインシデントハンドリングサービスがどのような関係にあるかについて述べます。ここで、本書の中心テーマ、すなわち第3章で詳しく述べるインシデントハンドリングサービスの対象範囲を設定します。第3章では、インシデントハンドリングサービスの構成とその機能要素について説明します。さらに、インシデントハンドリングサービスに関連するやり取りの範囲と特徴、および（大部分は機密性の高い）情報の取扱方法についても述べます。完全を期すために、第4章「チームの運用」では、すべてのCSIRTが考慮する必要がある実際の運用上および技術的な問題を取り上げます。設備、セキュリティ、スタッフ配置などの問題は、インシデントハンドリングサービスに限った問題ではありませんが、その成功には欠かせない事柄です。最後はいくつかの結びの言葉で締めくくり、その後に執筆者たちについての情報、CSIRT関連資料の目録、および略語と用語の解説が続きます。



---

## 2 基本事項

CSIRT はさまざまなサービスを提供することが考えられます。ただし少なくとも、本章で後述し、第3章で詳細に説明するインシデントハンドリングサービスの何らかの実装を提供する必要があります。インシデントハンドリングサービスの構成要素を少なくとも1つは提供しなければ、そのチームをCSIRTと呼ぶことはできません。消防署の例で考えてみましょう。消防署はさまざまなサービス（防火、周知、トレーニング）を提供し、火災安全検査を行います。しかし中心となるのは緊急対応という要素です。緊急消防隊を備えることで、時代に遅れず、現実的に即し、地域社会の信用、尊敬、および信頼を得ています。同様に、早期の検知と報告によるインシデントの影響の軽減や、インシデントの防止を目指す中で、周知やトレーニングなどのサービスを通じてチームは事前対応を行うことができます。しかし、インシデントハンドリングサービスがなければ、そのチームはCSIRTではありません。

本章では、CSIRTモデルの基本的な枠組みと、すべてのCSIRTに影響を与える問題について説明します。これらの問題は、規模、特徴、範囲にかかわらず、すべてのCSIRTで考慮し、取り組む必要があります。まず、CSIRTが何をするのか（ミッション）、誰に対して提供するのか（Constituency）、どのような位置付けにあるのか（組織における位置付け）、および誰と協力するのか（他者との関係）の観点から、CSIRTの枠組みを説明します。次に、ミッションステートメントから直接派生する枠組み、すなわちサービスと品質の枠組み、主要なCSIRTサービス、品質保証、主要コンポーネントとしてのポリシー、および基本的な境界条件として情報の流れについて検討します。最後の節では、CSIRTを環境ごとのニーズに適合させるときに直面する問題（特に重要なのは法律の問題です）について概説します。

### 2.1 CSIRTの枠組み

新しいチームを運営していく上でのガイドラインを確立するにあたり、手早い方法を模索する中で、多くの人々が自分たちの環境にそのまま適用できるのではないかと期待して、既存のCSIRTガイドラインを探します。しかし、既存のサービス定義、ポリシー、および手順を、他のCSIRTに適合させるのは不可能だとすぐに気がきます。さらに、厳格なガイドラインを定めたチームもいつの間にか、コンピュータセキュリティインシデントや攻撃というダイナミックな現実に対応させることに苦戦しているのです。

重要なことは、CSIRTが活動する環境固有の構造と要件、およびCSIRTがその環境でリスク管理に関して取るべき姿勢を理解することです。そのような理解によって、読者は本書をその構造と要件に合わせて適用できるようになります。最



終的には、当然ながら、各チームはその環境や Constituency を支援する独自の基準や運用ガイドラインを定義する必要があります。

構造化された方法でそうした目標を達成するには、まず CSIRT の基本的な枠組みを認識することが重要です。この枠組みは、「何をするのか」、「誰に対して提供するのか」、「どのような位置付けにあるのか」、および「誰と協力してするのか」という質問で構成されています。枠組みに関するこのような一連の質問をして、以下のことを確認します。

- ミッションステートメント：大局的な目標、目的、および優先順位
- Constituency：Constituency の種類および Constituency との関係
- 組織内における位置付け：組織構成、特にリスク管理における位置付け
- 他者との関係：国内（国外）CSIRT との協力や連携などの相互関係の設定

### 2.1.1 ミッションステートメント

既存の多くの CSIRT は、目標や目的への明確な理解が欠けており、またやり取りする相手にその情報を効果的に伝えることができていません。結果として、以下の対応のために労力とリソースを必要以上に浪費しています（多くの場合は危機的状況にあります）。

- 最も重要な活動に対応できるように、正しい優先順位を用いているかを把握する
- やり取りしている相手の不適切な期待を修正する
- 特定の状況にどのように対応するか、対応することが適切であるか把握する
- 状況のニーズに対応するために、ポリシーと手順を修正する
- 提供するサービスの範囲と性質を変更すべきか判断する

CSIRT において、簡潔で明確なミッションステートメントを定義し、文書化し、順守し、そして広く周知するまで、この状況はおそらく改善されません。ステートメントの重要性から、曖昧さを排除して、CSIRT が担うミッションを明記した 3、4 の文にまとめる必要があります。ステートメントは、チームが実現しようとしていることに関する基本的な理解を与えるのに役立ちます。さらに重要なことは、CSIRT の全体的な目標や目的の焦点を与えることができるのです。

さらに、CSIRT のミッションステートメントは、所属組織の上級管理職（企業のセキュリティ責任者、IT 部門のリーダー、取締役会、または同等の管理職）の支援と支持を得る必要があります。このような支援がなければ、CSIRT は承認とリソースを得るのに苦戦することになります。

CSIRT が提供するサービスの性質や範囲、ポリシーや手順の定義、サービスの質など、サービスおよび品質の枠組みを確立するには、ミッションステートメントが不可欠です。Constituency の定義に加えて、このサービスおよび品質の枠組み（2.2 節を参照）によって、あらゆる CSIRT 活動が推進・抑制されます。したが

って明らかに、チームが大きな組織に所属している、または外部団体から資金を提供されている場合、CSIRTのミッションステートメントはそれらの組織のミッションを補完する必要があります。

さらに、多くのCSIRTは、ミッションを補完し、チームが設立された理由を説明する「目的ステートメント (purpose statement)」も準備します。この情報を用意することで、CSIRTはそのミッションをサポートする目標と適切なサービスを定義できるのに十分な立場に位置づけられます。これらのステートメントは公的に入手できるため、その運用の過程においてCSIRTと必然的に関係を持つ他の団体はそのCSIRT (の役割、目的、および運用の枠組み) をよりよく理解できるようになります。

## 2.1.2 Constituency (サービス対象者)

運用の過程では、どのCSIRTもさまざまな組織と協力して行動することになります。その中で最も重要なのは、サービスを提供するために設立したCSIRTが対象とする特定のコミュニティ、つまりConstituencyです。CSIRTのConstituencyは無制限とすることも (依頼があれば誰にでもCSIRTがサービスを提供する)、いくつかの制約事項によって制限することもできます。ほとんどのCSIRTはConstituencyを制限しており、そこにはCSIRTの資金源が反映される傾向があります<sup>10</sup>。Constituencyを制限する最も一般的な制約には、国、地理、政治 (政府機関など)、技術 (特定オペレーティングシステムの使用など)、組織 (特定の組織や会社など)、ネットワークサービスプロバイダ (特定ネットワークへの接続など)、契約 (有料サービス型のチームの顧客など) があります。

表1に、各種のCSIRTごとのミッションの違いや、サービスを提供するConstituencyの違いを示します。

表1：CSIRTの種類とそのミッションおよびConstituencyの例

CSIRTのタイプ	ミッションの特徴	Constituencyのタイプ
国際的なコーディネーションセンター (連携)	他国のCSIRTと連携することにより、コンピュータセキュリティの脅威に関するグローバルな観点でのナレッジベースを獲得する。 CSIRT間で「信頼の輪 (web of trust)」を構築する。	世界各国のCSIRT
企業	組織の情報基盤のセキュリティを向上させ、侵入による被害の脅威を最小限にする。	システム管理者、ネットワーク管理者、および組織内のシステムユーザ
技術	特定のIT製品のセキュリティを向上させる。	製品ユーザ

<sup>10</sup> Kossakowski, Klaus-Peter. 『The Funding Process: A Challenging Task』、6th Workshop on Computer Security Incident Handling、FIRST (Forum of Incident Response and Security Teams)、マサチューセッツ州ボストン、1994年7月。

CSIRTにとって不可欠な作業は、Constituency とその関係を定義することと、CSIRT を Constituency に周知し、「仕事を適切にこなす (doing the job right) 」ことで信頼を得ることです。これらのテーマは、その境界線を越えて Constituency や協力関係のさまざまな側面にかかわっているため、以降の節でいくつか重点的に取り上げます。

### 2.1.2.1 Constituency の定義

Constituency は、ステートメントの形で定義される場合や、ドメイン名のリストによってサポートされる場合があります。

例：ペンシルベニア州立大学の対応チームの Constituency は、「ペンシルベニア州立大学」および「\*.psu.edu」と簡単に定義できます。

一方、チームのタイプによっては、Constituency をドメイン名で定義するのは難しい（あるいはできない）こともあります。Constituency が大規模でダイナミックである（顧客の出入りに応じて変化する）場合などです。

例：AusCERT の Constituency は、「AusCERT サービスの加入者」と簡単に定義できますが、「\*.au」ドメインにいるすべての人が AusCERT サービスの加入者になるわけではありません。しかし、AusCERT のサービスは契約顧客に合わせていますが、現実には他の外部 CSIRT が、コンピュータセキュリティインシデントに関与しているオーストラリアのサイトと他のサイトの間のやり取りを円滑に行えるように、連絡窓口として AusCERT を利用したことがあります。

Constituency を単一のドメインの形で簡単に定義できるように見える場合であっても、複雑な問題もありえます。学術環境（大学など）では、学生自治会や教授会、分離独立した営利団体、または研究機関が所有するシステムが大学のネットワーク上に共存している可能性があります。このようなシステムは大学のドメイン名を使用しているかどうかや、大学の CSIRT の配下にあるかどうか分かりません。

例：CERT/CC はカーネギメロン大学の一部であり、Software Engineering Institute に場所を与えられています。しかし CERT/CC のコンピュータ施設は、大学（および Software Engineering Institute）から切り離して管理されています。さらに、CERT/CC はカーネギメロン大学の CSIRT ではありません。

CSIRT が提供するサービスの範囲とサービスの特徴によって、CSIRT は複数の Constituency を定義する必要が生じることがあります。このような複数の Constituency は、その CSIRT がサービスを提供する他の Constituency と交錯していたり、部分集合または上位集合であったり、完全に分離していることなどが考えられます。例えば技術系の CSIRT は、特定の製品に関する一般的なセキュリティ情報を無制限の Constituency（インターネットなど）に、一般公開されている Web サイトを通じて提供します。また、製品の登録ユーザなど、Constituency の一部だけに対してはより高度なサービスを提供することが考えられます。

Constituency を非常に限定した CSIRT の場合でも、その Constituency に属していない組織に関連する（または由来する）情報も扱わなければならないことがよくあります。例えば、Constituency に直接影響を及ぼすインシデントレポートを Constituency 以外の組織から受け取り、その情報を適切に処理すると、情報が適切な連絡窓口に届いて Constituency 内で調整されるようにしたいと、限定された Constituency にインシデントハンドリングサービスを提供する CSIRT であってもほとんどの場合考えるはずでず。多くの CSIRT は、Constituency と他の外部組織（他の CSIRT、システム管理者、ベンダ、警察、弁護士、メディアなど）との調整ポイントとして機能します。これらのやり取りは、単純な要求の伝達から、データの完全共有や全面的な協力まで様々な可能性があります [Pethia 1990c]。重要なことは、CSIRT がこのようなやり取りの処理方法を決定し、文書化した上で、提示するということです（詳細は、3.7 節「やり取り」を参照）。

場合によっては、CSIRT はその Constituency を明確に示さないこともあります。例えば、CSIRT がネットワークサービスプロバイダである場合、顧客リストを専有情報と見なし、その情報を開示しないことが考えられます。同様に、有料サービス型の CSIRT は、顧客と Constituency を開示しない契約を結ぶこともあります。そのような場合に、CSIRT は Constituency を「当組織の顧客」のように非常に一般的な用語で記述することになります。このことにより、他の外部サイトおよびチームは、どの Constituency が CSIRT の Constituency に含まれているか分からず、活動を適切なチームに直接報告できません。そのため、このような CSIRT は Constituency にインシデント対応調整サービスを提供するのが困難な場合や不可能な場合があります。このような状況ではよくあることですが、顧客はインシデントに巻き込まれた他のサイトや CSIRT から直接連絡を受け、必要に応じて自分たちの CSIRT に支援を求めることができます（求めなくても構いません）。これは「Web 的な」信頼関係（信頼関係が 1 対 1 ではなく Web (=蜘蛛の巣) のように網状に複雑に築き上げられていること）が発展する可能性を示唆するものといえます。

### 2.1.2.2 Constituency の重複

すべての CSIRT に固有の Constituency があるとは限りません。複数の CSIRT が一定のサービスを提供する Constituency が重なっていることも珍しくありません。しかし、経験が示すように、すべての関係者がその責任を明確に理解していないかぎり、このように Constituency が重なっている状況は、CSIRT と Constituency の間に混乱を引き起こします。Constituency が重なっている CSIRT 同士が相互に適切に調整しなかったために、取り組みの重複と関係者の間で対立が生じたケースもあります。同様に、Constituency がどの CSIRT に支援や援助を求めるべきか分からず、結果として報告が重複したり、適切でなかったりする状況もあります。

例：ある営利企業が有料サービス型の CSIRT と契約を結び、結果として有料サービス型の CSIRT の Constituency になるとします。さらにその企業は、特定の国にあるために、その国内対応チームの Constituency にもなります。

例：ドイツ連邦政府機関は通信とインターネットアクセスを提供するために、German DFN ネットワークに接続しています。このような組織の多くは、次の 2 つのチームの Constituency になります。

- DFN-CERT。組織が DFN ネットワークに接続する結果として。
- CERT-BUND。ドイツ連邦政府のサイトに固有のニーズに対応するために German Information Security Agency (BSI [Bundesamt für Sicherheit in der Informationstechnik]) 内部に設立されたチーム。

ドイツ連邦政府のサイトに影響を及ぼすインシデントが報告されると、両チームが必要に応じて活動を調整します。CERT-BUND は連邦政府のサイトに対してインシデント対応の支援を行ないませんが、DFN-CERT は CERT-BUND とともに脆弱性の分析に関する技術サポートを提供することがあります。2つのチームは、双方に影響を及ぼす対応があるか検討・調整します。

例：CERT/CC は、別の CSIRT の Constituency に属する個人からの電話も受けています（継続して受ける場合もあります）。あるケースでは、英国の大学のシステム管理者がインシデントに関する支援を求めて米国の CERT/CC に電話をかけてきました。英国の時刻は午前 9 時でしたが、米国の現地時間は午前 3 時でした。CERT/CC のスタッフが呼び出されて、そのサイトをすぐに支援しました。英国のシステム管理者は（その職務に就いたばかりで）JANET-CERT が提供しているサービスを認識していませんでした。JANET-CERT の存在と、それがローカルの需要とタイムゾーンの点からより適切なサービスを提供してくれることを知らされると、今度は JANET-CERT に直接連絡しました。JANET-CERT は必要な支援とアドバイスを提供してフォローし、実際に米国の CERT/CC では提供できなかった法的状況に関する詳細を提供することができました。

### 2.1.2.3 Constituency との関係

CSIRT とその Constituency との関係の特徴は、CSIRT が提供するサービスの特徴に直接影響します。表 2 に示すように、CSIRT が Constituency に対して持っている権限の点から考えると、それらの関係は 3 つの一般的なカテゴリに分類されます。

表 2：CSIRT と Constituency の間の考えられる権限関係

権限のレベル	CSIRT と Constituency の関係
強制	CSIRT のメンバは、Constituency に代わり必要な活動や決定を行う権限がある。
非強制	CSIRT のメンバは、Constituency を直接支援し、意思決定プロセスを共有する（Constituency の決定に影響力を持つが、指示することはできない）。
なし	CSIRT のメンバは、Constituency に対する権限がなく、支援者またはアドバイザーとしてのみ活動できる。

4 番目の権限関係として、間接的な権限が考えられますが、一般的ではありません。このような関係では、CSIRT は Constituency に圧力をかけ、必要に応じて制裁措置をとります。主要なネットワークサービスプロバイダ (NSP) の CSIRT がそのサービスを受けるインターネットサービスプロバイダ (ISP) に与える影響、または ISP がその顧客に与える影響は間接的な権限の好例です。

権限関係に関わらず、CSIRTはある種のインシデントハンドリング、脆弱性分析および対応、またはトレーニングを提供できます。しかし、CSIRTがConstituencyに対する権限を持っていない場合、インシデント追跡や侵入検知などのサービス（表4「CSIRTサービスのリスト」に掲載）は提供できない可能性があります。そのような場合、これらのサービスの中のある種のものについては契約上の合意を適切に交わすことでサポートすることができます。ただしそうした合意によって権限関係が若干変わります。

例：広く利用されているネットワークデーモンに、悪用されるとシステムが危険にさらされるようなセキュリティ上の脆弱性があり、そのためのパッチをアナウンスするCERT勧告がリリースされたとします。Constituencyに対する権限が異なるCSIRTがそのようなアナウンスにどのように対処するのかを考えます。

#### 強制権限

CSIRTは、Constituencyがパッチをインストールするまで、すべてのConstituencyにネットワークから切断するよう「要求」できます。さらに、CSIRTは手動で介入して、従わないConstituencyを切り離すことができます。

#### 非強制権限

CSIRTは、Constituencyがパッチをインストールするまで、Constituencyにネットワークから切断するよう「アドバイス」と「催促」を行うことができます。さらに、調整とアドバイスへの対応を手伝うことで、Constituencyを「支援」することもできます。

#### 権限なし

CSIRTはConstituencyに「アドバイス」と「情報の伝達」を行うことができます。さらに、CSIRTはConstituencyがパッチをインストールするように「促す」こともできます。しかし、パッチのインストールをConstituencyに強制することはできません。

### 2.1.2.4 Constituency への CSIRT の周知

Constituencyを定義したら、（CSIRTサービスの範囲と特徴に関係なく）Constituencyや他の関係者がCSIRTとの間で期待できる相互関係を理解できるように、Constituencyの定義とCSIRTのサービスを周知することが重要です。特にCSIRTがコンピュータセキュリティインシデントを報告するためのConstituencyとの単一連絡窓口として機能することを目的としている場合は、インシデントを報告するときには特定のConstituencyではなくCSIRTに直接報告することを関係者全員が知っているように、Constituencyに周知する必要があります。同様に、ConstituencyはどのCSIRTがサービスを提供しているのか、またどのようにして適切なCSIRTに報告すべきかを知っておく必要があります。

チームのConstituencyは次のようにいくつかの捉え方ができます。

- 公表（declared）Constituency：チームが代表することを表明している、または希望しているConstituencyです。

- 契約 (contractual) Constituency : 公表 Constituency の一部で、チームへの報告について (実際に報告するかどうかに関係なく) 契約上合意しています。
- 報告 (reporting) Constituency : 公表 Constituency の一部で、チームをその代表と認識し、結果としてチームに報告します。
- その他 : 公表 Constituency に含まれていないが、チームのサービスを必要としている、あるいは何らかの形でチームに報告してくる関係者です。中には、報告先のチームがあることを知らない場合もあります。

CSIRT の目標は、公表 Constituency にチームの存在を認識してもらい、他のチームにも CSIRT とその Constituency のことを知ってもらい、一般にチームの認知度を高めるように、CSIRT 自身とそのサービスをできるだけ広く普及することです。チームがその役割とサービスを効果的に伝達しなければ、報告 Constituency の規模や広範な CSIRT コミュニティにおける認知度を高めることを期待するのは難しくなります。

CSIRT は次のようにできるだけ多くのコミュニケーションチャンネルを通じて自身を知ってもらう必要があります。

- Constituency のメーリングリストやニュースグループ
- CSIRT または組織の情報 / Web サーバ
- プレゼンテーション、ワークショップ、およびチュートリアル資料
- 一般の宣伝資料とニューズレター (定期と「速報」)
- メディア (電子メールや Web などのオンライン通信手段を使用する傾向がない Constituency や管理職にとどくことができるメディア)

### 2.1.2.5 Constituency の信頼獲得

CSIRT は Constituency との (権限) 関係に関係なく、Constituency を単に定義して公表する以上のことをする必要があります。Constituency の信頼と尊敬を獲得・維持しなければ、CSIRT を効率的に運用することはできません。CSIRT が Constituency に強制権限を持っていても、そのような関係で Constituency の信頼と尊敬を想定できるわけではありません。信頼は、獲得して醸成するものです。公表 Constituency の信頼と尊敬を獲得すると、一層多くの公表 Constituency がチームを認めて支援し始め、その結果、報告 Constituency も増えていきます。経験が示すように、チームが運用を開始し、公表 Constituency を公表してから、安定した報告 Constituency が確立されるまでに約 1 年かかります。

CSIRT が定義した Constituency に関係なく、どのようなチームでも Constituency による 100% の認知度が達成されることはまれです。公表 Constituency に与える可能性のある影響を予測するときには、このことを覚えておくことが役立ちます。チームがいかに熱心に Constituency に働きかけて、支援や影響を与えようとしても、Constituency 全員が反応を示すことはほとんどありません。

### 2.1.3 組織内の位置付け

CSIRTの基本的な枠組みでは、チームが目指していること（ミッションステートメント）と、誰に対してか（constituency）を定めるだけでなく、CSIRTの「ルーツ」、つまり親組織における位置付けを適切に定義する必要もあります。これは単なる管理上の定義の問題ではありません。それだけだとしたら、この節は不要だったでしょう。

CSIRTの親組織における位置は、CSIRTに定められたミッションと密接に結び付いており、Constituencyとも多少は結び付いています。このことは、フォーチュン500企業に選ばれたあるConstituencyに対する非常に目立った支援任務を持つCSIRTの極端な例を考えるとよく分かります。もし親組織のシステム管理部門の下に置かれる（明らかな責任の不一致）ようならば、CSIRTは失敗する運命にあります。このような落とし穴を避けられるように、この節では、親組織におけるCSIRTの位置付けに関する側面を取り上げます。

CSIRTは組織のセキュリティチーム全体を構成している場合か、組織のセキュリティチームと完全に区別されている場合があります<sup>11</sup>。あるいは、組織に明確なCSIRTがなくても、組織のセキュリティチームが事実上、暗黙的にその役割を果たす場合があります。どのような実装であるにしろ、インシデントハンドリングサービスを提供することが重要な問題です。本書では、図1に示すように、最も一般的で単純化した形のCSIRTを、親組織に属する大きなセキュリティチームの一部（重複部分の小さなものから完全に重複するものまで）と考えます。

---

<sup>11</sup> セキュリティチームは、たいていIT部門に置かれたシステム、ネットワーク、およびセキュリティ管理者として定義され、その職務権限は内部および対外セキュリティ保護に関するものです。例えば、セキュリティ問題やファイアウォール、アンチウイルスフィルタ、セキュアリモートアクセス、侵入検知などの技術を扱います。「セキュリティチーム」という用語は、これらの職務を遂行する個人を指す場合や、チームとして活動するグループを指す場合があります。これらの個人は1か所に配置されていることもありますが、たいていは企業全体に分散配置されています。



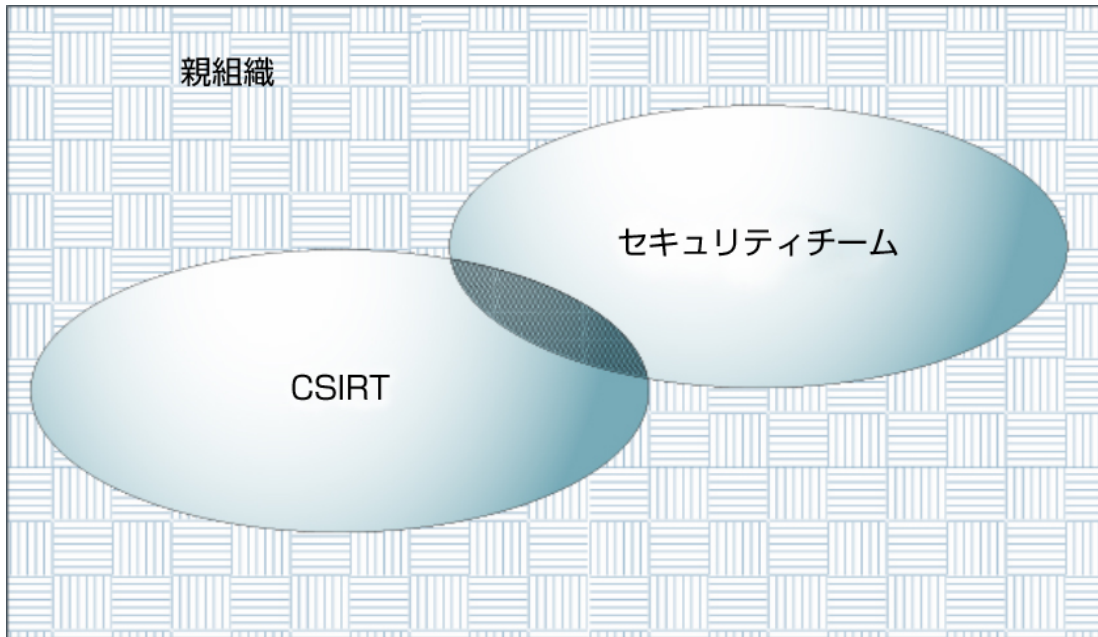


図1：組織内の CSIRT

企業環境では、CSIRT は組織の事業構造に適切に組み込まれる必要があり、一般には、組織の IT セキュリティ部門に属するか、部分的に重なります。

また、単一の親組織に複数のインシデントハンドリング機能が存在することも考えられます。このような状況はベンダ組織やネットワークサービスプロバイダで生じ、2つのチームが存在することがあります。1つはその会社自体のネットワークに関連するインシデントを処理するチームであり、もう1つは顧客にサービスを提供するチームです。ベンダ組織は、自社製品のセキュリティ上の欠陥に対応するサービスなど、付加的なサービスを提供することもあります。外部にサービスを提供しない単一の組織でも、複数の機能が生まれることがあります。例えば、悪意のソフトウェアが関連したり引き起こしたりするインシデントをある1つのチームで処理し、ネットワーク攻撃や侵入には別のチームで対処する企業などが考えられます。

CSIRT が運用ガイドラインを構築し始める前に、組織環境と **Constituency** との範囲で、CSIRT がリスク管理全体において果たす役割を決めることが重要です。この役割は、親組織の特徴およびチームがサービスを提供する **Constituency** の特徴によって異なります。結果として生じたどのような役割も、経営陣による支持と関係者全員の理解が必要となります。

(データが存在する) コンピュータ、ネットワーク、および通信装置をホスティングする組織の部署は、明らかに技術的なリスクを抱えています。事業リスクも考慮する必要があり、組織のさまざまな部署がそのリスクを抱えている可能性があります。しかし、リスクを管理する責任がどこにあるか、その分野に関与する組織の各部署がどのように対話をして責任を調整するのかを理解することが重要です。

営利組織の環境では、同じ組織のさまざまな部門がリスク管理のさまざまな側面に対して責任を持つことがあります。

例：ネットワーク運用チームはネットワークのセキュリティ問題に、システム管理者はホストのセキュリティ問題に、物理セキュリティチームは建物や施設へのアクセスに、CSIRTはコンピュータセキュリティインシデント報告の対応調整に、コーポレートセキュリティは他のセキュリティ関連のチームや人員もすべて含めて、会社全体のポリシーや手順の設定に対して責任があります。

リスク管理における個別の役割に関係なく、各グループはその責任が組織の他の部署とどのような相互関係にあるか、そして孤立して運用しないように他のグループとどのように協調すべきかを理解する必要があります。例えば、各グループの義務、対話／エスカレーションポイント、および共同責任などを明確に規定します。

同様に、組織が外部CSIRTにサービスを求めることもあります。その場合、外部CSIRTの責任と運用も組織のリスク管理の枠組みに含めて、同様に十分定義する必要があります。

## 2.1.4 他のチームとの関係

CSIRTの活動範囲はインターネットであり、ひいては世界です。CSIRTがサービスを提供している Constituency は世界中に多数あり、その数は増え続けています。この点に関し、CSIRTはある程度ですが職務を遂行するために相互運用する必要があります。この協力と調整の取り組みがCSIRTの枠組みのまさに核心です。単にミッションを提示し、Constituencyを定義し、組織内のCSIRTの位置付けを決めるだけでは十分とは言えず、調整の問題も対象とする必要があります。

今日存在するCSIRTという枠の中には、さまざまなタイプのチーム間に見られる、ある種の階層構造があります。明確な Constituency にサービスを提供しているチームもあれば、CSIRTの（通常は国内または国際的な）グループ間で調整役を果たしているチームもあります。ただし、この構造は実際の階層ではなく、たいていの場合は非公式で自発的なものです。この非公式な構造は、信頼しているCSIRTとは迅速で効果的に情報を共有できる一方で、信頼性を判断する機会があまりなかった他のチームに対しては慎重に対応できるという柔軟性があるため、メリットがあると見られています。

米国軍隊などには、公式の階層も存在します。例えば、米国陸軍、空軍、および海軍（それぞれACERT/CC<sup>12</sup>、AFCERT、NAVCIRT）はそれぞれのConstituencyにサービスを提供していますが、米国国防総省のDOD-CERTはすべての米国軍隊チームの調整を行っています。

---

<sup>12</sup> 例えば、Army CERTは、地理的に分散された地域の陸軍チーム（それぞれ「RCERT」と呼ばれる）の調整役を果たしています。

ここで注意すべきは、ある種の活動について、多くのチームが他の同階層チームと直接対話を取るのに対して、調整役の CSIRT とはまったく対話をしないということです。これは、関係するチームが特定の問題に対応するのに調整役の CSIRT を参加させる必要がないと考える場合によくあります。しかし、調整役の CSIRT は通常、対象ドメインにおける活動水準の全体像を把握し、付加的な活動や関連する活動に目を光らすよう他のチームに対して注意を喚起するために、すべての活動を知らせるように要求します。

図 2 に示すように、CSIRT 間にはさまざまなタイプの同格関係が考えられます。あるチームが他の CSIRT 間の調整役を果たしている場合、そのチームを調整役の CSIRT と見なすことができます。図 2 の例では、CSIRT A と CSIRT B を調整役 CSIRT として描いています。CSIRT B には、CSIRT C と CSIRT D の調整に加えて、C または D が対象としていない、B が直接サービスを提供している別の Constituency があります。他方で、CSIRT A には、他の CSIRT (B、E、F、G) のみで構成された Constituency があります。しかし、A の Constituency である CSIRT は厳密な階層には分かれていません。CSIRT E と CSIRT F の連絡調整は、CSIRT A とそれらの連絡調整とは無関係に行われるためです。

この節で説明した関係は、環境や目的に関わらず、任意の CSIRT を表現する場合に使用できます。例えば、International Coordination Center (CERT/CC など)、National Response Team (DK-CERT、JPCERT/CC など)、有料サービス型の対応チーム (dCERT、IBM/MSS など)、営利団体によるチーム (Motorola 社の MCERT、Boeing 社の BCERT など)、ネットワークサービスプロバイダチーム (UNI-CERT、BT-CERT/CC など)、および大学 (ペンシルベニア州立大学の PSU-CERT、スタンフォード大学の SUNSeT など) はすべて、この方法で表現できます。

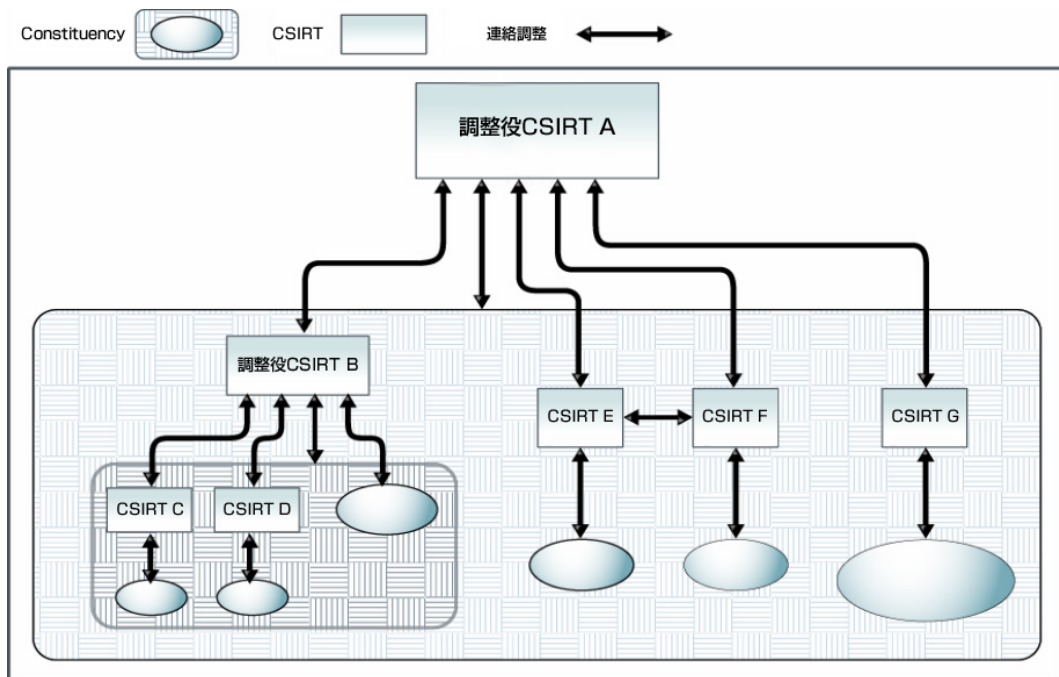


図2 : CSIRT 間の関係

## 2.2 サービスと品質の枠組み

CSIRT のミッションステートメントからは原則的に、サービス、ポリシー、および品質の3つが派生し、それぞれがミッションステートメントの範囲と目的を具体化している必要があります。チームが提供するサービスは、チームのミッションを遂行するための手段です。サービスは通常、チームの **Constituency** に提供されます。ポリシーは、チームを運用する上での主要な原則です。品質は、すべての活動が実施される際に求められる基準です。CSIRT 内を流れる情報は、ミッションステートメントの派生事項のすべてに浸透します。サービス、ポリシー、および品質によって規定される手順は、活動をどのように行うかを指定します。このフレームワークを図3に示します。

この枠組みに続いて、ミッションステートメントの3つの派生事項（サービス、ポリシー、および品質）についてさらに詳しく説明します。情報の流れももちろん、4番目に取り上げるべき話題ですが、この項では取り上げません。本書の目的のために、主として外部関係者に関連する情報のフローに重点を置くことにします。とはいえ、内部の情報の流れ（チームメンバー間、提供される各種のサービス間など）を定義・改善することはチームにとって重要です。

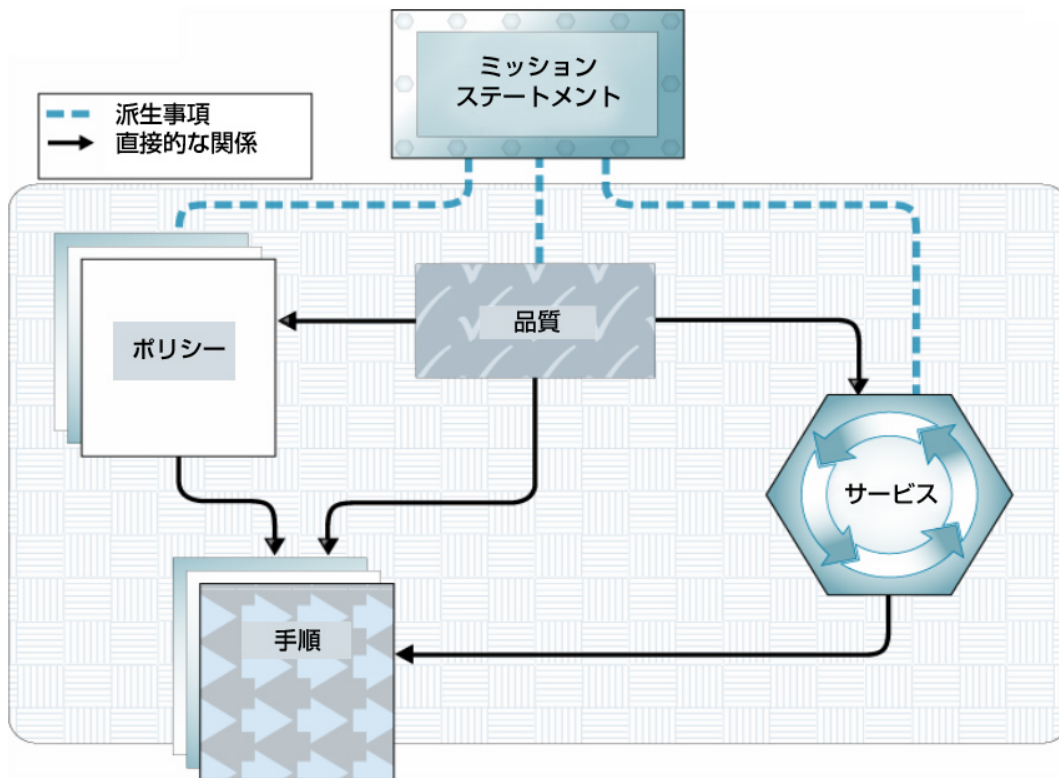


図3：ミッションステートメントから派生するサービスと品質の枠組み

本書では外部とのコミュニケーションに関係がある場合にのみ、情報流通を基本的な関心事項と考えているため、情報流通フロー自体（チーム内部の情報流通など）は、明らかに CSIRT の基本的課題ではないと見なしています。内部の情報流通に関する話題は、2.4節「情報流通」においてサービスに関連して説明します。また第3章と第4章において、CSIRT の問題のその後の取り扱いについて関連する場合に述べることにします。

CSIRT は、ミッションステートメントでの確約を直接反映したさまざまなサービスを Constituency に提供します。本書の中心であるインシデントハンドリングサービスについては、第3章で詳しく説明します。ただし、サービスの議論に必要な枠組みを示すために、この節ではすべての CSIRT サービスにとって一般的な問題と、いくつかの CSIRT が提供している他の一般的なサービスについて簡単に述べます。

提供するサービスごとに、CSIRT は Constituency に対して、できるだけ詳しいサービス明細（または正式なサービスレベル契約）を提供する必要があります。特に、CSIRT が提供するサービスには、表3のような属性と説明を含める必要があります。

表3：サービス明細の属性

属性	説明
目的	サービスの目的と特徴。
定義	サービスの範囲と深さの説明。
機能説明	サービスの各機能の説明。
可用性	サービスを誰が、いつ、どのように利用できるかの条件。
品質保証	サービスに適用可能な品質保証パラメータ。Constituencyの期待値の設定と制限の両方が含まれる。
やり取りと情報開示	CSIRTとConstituencyの関係者（Constituency、他のチーム、メディアなど）の間のやり取り。関係者がサービスを利用するための情報要件の設定、および（制限付きと公開）情報の開示に関する方針の定義が含まれる。
他のサービスとのインタフェース	このサービスと、CSIRT内でやり取りする他のサービスとの情報流通の交換窓口を定義、指定する。
優先順位	このサービス内の個々の機能の相対的な優先順位、および、CSIRTの他のサービス内でのこのサービスの優先順位。

これらの説明は、チームがサービスを定義、実装、および運用するときに役立ちます。同様に、サービスに対する正しい期待を公示・設定するために、Constituencyが（何らかの形で）利用できる情報も提供する必要があります。この分野は絶えず変化し、優先順位が変わり、技術が進歩するものであるため、CSIRTは環境の変化と利用可能なリソースに対応するために、提供するサービスの特徴とレベルを頻繁に見直す必要があります。さらに、Constituencyには、顕著な変更を知らせる必要もあります。

## 2.3 CSIRTのサービス

CSIRTと見なされるためには、そのチームは1つ以上のインシデントハンドリングサービス（インシデント分析、オンサイトでのインシデント対応、インシデント対応支援、またはインシデント対応の連絡調整）を提供する必要があります。前述のとおり、インシデントハンドリングサービスには、インシデント分析と、他のインシデントハンドリングサービス（インシデント対応解決、インシデント対応支援、またはインシデント対応調整）が少なくとも1つ含まれます（その違いの詳細については後述します）。実際に、CSIRTは一般に、基本的なインシデントハンドリングサービスに加え、Constituencyのニーズに応じて他のサービスを提供しています<sup>13</sup>。これらの付加的なサービスは、CSIRTが単独で、あるいは他の組織体（ITまたはセキュリティ部門）と協力して提供することがあります。

必須のインシデントハンドリングサービスに加えて、CSIRTが提供する最も一般的なサービスと、それらのサービスが実施される形態を表4に示します。この付加的サービスのうち、いくつか（アナウンスや脆弱性分析および対応など）はイ

<sup>13</sup> 例えば、勧告、アラート、警告、脆弱性ハンドリング、他の事前対応告知、Constituencyのトレーニングや意識向上などがあります。

ンシデントハンドリングサービスと密接に関連しているため、提供される可能性はさらに高くなります。

ここでの説明は CSIRT が提供するサービスに重点を置いています。これらと同じサービスの多くは、通常の管理業務の一環として臨時のインシデントハンドリングを行うシステム管理者、ネットワーク管理者、およびセキュリティ管理者でも提供することができます。このような臨時のチームを、「セキュリティチームまたは他のセキュリティ関連グループ」と呼ぶことがあります。

### 2.3.1 サービスの分類

CSIRT が提供できるサービスは数多くあります。各 CSIRT が提供するサービスは、チームのミッション、目的、および Constituency に基づいている必要があります。




CSIRT サービスは 3 つの種類に分類できます。

- 事後対応型サービス：セキュリティ侵害のあったホストの報告、悪意のコードの蔓延、ソフトウェアの脆弱性、侵入検知またはログ記録システムで確認されたものなど、何らかのイベントまたは要請を受けて実施されます。事後対応型サービスは CSIRT の中心的な活動です。
- 事前対応型サービス：攻撃、問題、またはイベントに備えて、Constituency システムの対策、防御、および安全確保に役立つ支援と情報を提供します。これらのサービスを実施することで、将来のインシデントの数が減少します。
- セキュリティ品質管理サービス：インシデントハンドリングとは無関係に、従来から組織の他の領域（IT、監査、またはトレーニング部門など）で実施されており、定着している既存のサービスを補強します。CSIRT がこれらのサービスを実施または支援する場合は、CSIRT の視点と専門知識が組織のセキュリティ全体を向上させ、リスク、脅威、およびシステムの脆弱性を特定する手掛かりとなります。これらのサービスは一般に事前対応型ですが、インシデントの数を軽減するのに間接的に役立ちます。

各カテゴリに相当するサービスを表 4 に示し、以下に詳しく説明します。

いくつかのサービスには、事後対応型と事前対応型の両面があります。例えば、脆弱性ハンドリングは、能動的に悪用されるソフトウェア脆弱性が発見されると、それを受けて実施できます。しかし、コードの見直しやテストによって脆弱性の有無を判断することで事前対応として実施すれば、脆弱性の問題が広く知られたり悪用されたりする前に修正することができます。

表4：一般的な CSIRT サービスのリスト

事後対応型サービス 	事前対応型サービス 	セキュリティ品質管理サービス 
<ul style="list-style-type: none"> <li>+アラートと警告</li> <li>+インシデントハンドリング                             <ul style="list-style-type: none"> <li>-インシデント分析</li> <li>-オンサイトでのインシデント対応</li> <li>-インシデント対応支援</li> <li>-インシデント対応調整</li> </ul> </li> <li>+脆弱性ハンドリング                             <ul style="list-style-type: none"> <li>-脆弱性分析</li> <li>-脆弱性対応</li> <li>-脆弱性対応調整</li> </ul> </li> <li>+アーティファクトハンドリング                             <ul style="list-style-type: none"> <li>-アーティファクト分析</li> <li>-アーティファクト対応</li> <li>-アーティファクト対応調整</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>○ アナウンス</li> <li>○ 技術動向監視</li> <li>○ セキュリティ監査または審査</li> <li>○ セキュリティツール、アプリケーション、インフラ、およびサービスの設定と保守</li> <li>○ セキュリティツールの開発</li> <li>○ 侵入検知サービス</li> <li>○ セキュリティ関連情報の提供</li> </ul>	<ul style="list-style-type: none"> <li>✓ リスク分析</li> <li>✓ ビジネス継続性と障害回復計画</li> <li>✓ セキュリティコンサルティング</li> <li>✓ 意識向上</li> <li>✓ 教育/トレーニング</li> <li>✓ 製品の評価または認定</li> </ul>

## 2.3.2 サービスの詳細

### 2.3.2.1 事後対応型サービス

事後対応型サービスは、支援依頼、CSIRT の Constituency からのインシデントに関する報告、および CSIRT システムに対する脅威や攻撃に対応することを目的としています。第三者による通知や、監視システムまたは侵入検知システム (IDS) のログとアラートを確認することによって開始されるサービスもあります。

#### アラートと警告

このサービスでは、侵入者による攻撃、セキュリティ上の脆弱性、侵入検知のアラート、コンピュータウィルス、または偽の情報 (hoax) について通知するとともに、結果として生じた問題に対処するために推奨される短期的な措置を提供します。アラート、警告、勧告は、現在の問題に反応して送信され、Constituency に活動を知らせることと、システムを保護したり影響を受けたシステムを回復したりするためのガイダンスを提供することを目的としています。情報は CSIRT によって作成されることも、ベンダ、他の CSIRT やセキュリティの専門家、その他の Constituency から再配布されることもあります。



## インシデントハンドリング

インシデントハンドリングには、要請や報告の受け取り、トリアージ<sup>14</sup>、および対応、そしてインシデントやイベントの分析を伴います。個々の対応活動には以下のものが含まれます。

- 侵入行為によって影響を受けたり、脅威にさらされたりするシステムやネットワークを保護するための対応措置を講じる
- 関連する勧告やアラートをもとに解決策と軽減方法を提供する
- 他のネットワーク上での侵入行為を探す
- ネットワークトラフィックをフィルタリングする
- システムを再構築する
- システムへのパッチの適用やシステムの修復を行う
- 他の対応または回避策を立てる

インシデントハンドリング活動は、さまざまな CSIRT によって異なる方法で実施されるため、このサービスは、実施する活動と提供する支援の種類に基づいて以下のように分類されます。

**インシデント分析：**さまざまなレベルのインシデント分析とサブサービスがあります。インシデント分析は基本的に、インシデントやイベントに関して入手できるあらゆる情報と補助的な証拠、あるいはアーティファクト (artifact) を調査することです。分析の目的は、インシデントの範囲、インシデントが引き起こす被害の程度、インシデントの特徴、および利用可能な対応方法や回避方法を確認することです。CSIRT は脆弱性およびアーティファクト分析 (後述) の結果を利用して、特定のシステムで起こったことに関する最も完全で最新の分析を理解して提供することができます。CSIRT は活動をインシデントと関連付け、相互関係、傾向、パターン、または侵入者の痕跡を判断します。CSIRT のミッション、目標、および処理に応じて、以下の2つのサブサービスをインシデント分析の一環として実行できます。

- **フォレンジックによる証拠収集 (Forensic evidence collection)：**システムに加えられた変更を明らかにし、セキュリティの侵害に至った事象の流れを再構築できるように、セキュリティが侵害されたコンピュータシステムから証拠を収集、保全、文書化、および分析すること。このような情報や証拠の収集は、証拠法則に基づいて裁判所で採用される立証可能な分析過程の管理を文書化する方法で行う必要があります。法廷証拠収集に関する職務には、影響を受けたハードディスクのビットイメージコピーの作成、システムに対する変更 (新しいプログラム、ファイル、サービス、ユーザなど) のチェック、実行中のプロセスとオープンポートの確認、トロイの木馬プログラムとツールキットのチェックなどがあります (これだけにとどまりません)。この機

---

<sup>14</sup> トリアージとは、インシデント報告や他のCSIRTの依頼を選別、分類し、優先順位を付けることです。病院が、すぐに診る必要がある患者と援助を待てる患者を分けるトリアージにたとえることができます。

能を遂行する CSIRT スタッフは、公判において鑑定人を務めるための準備をする必要もあります。

- **追跡 (Tracking or tracing)** : 侵入者の起点までの追跡、または侵入者がアクセスしたシステムの特定。この活動には、影響を受けたシステムや関連ネットワークに侵入者がどのようにして入ったか、アクセスするためにどのシステムを利用したか、どこから攻撃が始まったか、攻撃の一環として他のどのシステムやネットワークを使用したかなどを追跡する作業が伴うことがあります。侵入者の身元の特定を試みることもあります。この作業は単独で行うこともありますが、通常は警察職員、インターネットサービスプロバイダ、その他の関連する組織との協力を伴います。

**オンサイトのインシデント対応<sup>15</sup>** : CSIRTはConstituencyがインシデントから回復できるように、直接オンサイトで援助します。電話や電子メールによるインシデント対応支援（下記参照）を提供するだけではなく、CSIRT自体が物理的に、影響を受けたシステムを分析し、システムの修復と回復を行います。このサービスには、インシデントの疑いがあるかまたはインシデントが発生した場合に必要な、現場でのすべての措置が含まれます。影響を受けたサイトにCSIRTがない場合に、チームメンバがサイトに出張して対応します。現場チームが既にサイトにおいて、通常業務の一環としてインシデント対応を提供するケースもあります。設置されたCSIRTの代わりに、システム、ネットワーク、またはセキュリティ管理者の通常職務権限の一環としてインシデントハンドリングを提供する場合は、特にこのような傾向があります。

**インシデント対応支援** : CSIRT は攻撃の被害者をインシデントから回復させるときに、電話、電子メール、ファックス、または文書によって支援・指導します。これには、収集したデータの解釈に関する技術援助、連絡先の提供、または軽減および回復方法に関するガイダンスの伝達などが含まれることがあります。前述の直接のオンサイトインシデント対応活動は伴いません。代わりに、現場の担当者が回復作業を行うことができるように、CSIRT がリモートから指導します。

**インシデント対応調整** : CSIRT は、インシデントに関与する関係者間で対応活動を調整します。この関係者には通常、攻撃の被害者、攻撃に巻き込まれた他のサイト、攻撃の分析に関する援助を要求しているサイトなども含まれます。また、インターネットサービスプロバイダ、他の CSIRT、当該サイトのシステムおよびネットワーク管理者など、被害者に IT サポートを提供している関係者も含まれます。調整作業には、連絡先の収集、（攻撃の被害者または起点として）巻き込まれている可能性があるサイトへの通知、関係サイト数に関する統計情報の収集、情報交換および分析の促進などを伴うこともあります。調整作業の一環として、組織の弁護士、人事部、または広報部への通知や協力が必要になることもあります。警察との調整も行う場合があります。このサービスには、直接のオンサイトインシデント対応は含まれません。

---

<sup>15</sup> ここでは、CSIRTサービスの一種を示すために「インシデント対応」を使用しています。「インシデント対応チーム」などのチーム名で使用している場合、この表現は通常、広義のインシデントハンドリングを意味します。

## 脆弱性ハンドリング

脆弱性ハンドリングには、ハードウェアとソフトウェアの脆弱性に関する情報や報告の受け取り<sup>16</sup>、脆弱性の性質、構造、および影響の分析、脆弱性の検知と修復に関する対応方法の開発が含まれます。脆弱性ハンドリングの活動はさまざまなタイプのCSIRTによってさまざまな方法で実施されるため、このサービスは提供する活動と援助の種類に基づいて以下のように分類されます。

**脆弱性分析：**CSIRTはハードウェアまたはソフトウェアの脆弱性に関する技術的分析と検査を行います。これには、疑いのある脆弱性を確認したり、脆弱性がどこにあり、どのように使用されるおそれがあるかを判断するために、ハードウェアまたはソフトウェアを技術的に検査したりするといった内容が含まれます。分析では、ソースコードを見直したり、デバッガを使って脆弱性がどこにあるか割り出したり、テストシステムで問題を再現することもあります。

**脆弱性対応：**このサービスには、脆弱性を軽減または修復するために、適切な対応を判断する行為が含まれます。パッチ、修正版、および回避方法の開発や調査が含まれることもあります。場合によっては勧告やアラートを作成・配布して、軽減方法を他者に通知することもあります<sup>17</sup>。パッチ、修正版、または回避策となる機能をインストールすることで対応する場合があります。

**脆弱性対応調整：**CSIRTは企業や Constituency のさまざまな部署に脆弱性について通知し、その脆弱性を修正または軽減する方法に関する情報を共有します。脆弱性対応方法がうまく実施されたかの確認も行います。このサービスには、ベンダ、他のCSIRT、技術者、Constituencyのメンバ、脆弱性を最初に発見または報告した個人やグループとのやり取りが含まれることがあります。活動としては、脆弱性の分析や脆弱性の報告の促進、対応する文書、パッチ、または回避方法のリリーススケジュールの調整、さまざまな関係者が実行する技術的分析のまとめなどがあります。さらに、脆弱性情報と対応方法に関する公開／非公開アーカイブまたはナレッジベースの保守が含まれることもあります。

## アーティファクトハンドリング

アーティファクトとは、システムとネットワークの探査や攻撃に関与した、もしくはセキュリティ対策を無効化する目的で使用された可能性のある、システム内で発見されたファイルまたはオブジェクトのことをいいます。アーティファクトには、コンピュータウイルス、トロイの木馬プログラム、ワーム、攻撃スクリプト、ツールキットなどがあります（これだけではありません）。

アーティファクトハンドリングには、侵入攻撃、偵察、その他の無許可の活動または破壊的活動に使用されたアーティファクトに関する情報やそのコピーの受け

---

<sup>16</sup> 脆弱性とは、ハードウェアまたはソフトウェアに存在する欠陥や弱点を指し、それが悪用された結果、暗黙または明示的なセキュリティポリシーが侵害されるものをいいます。

<sup>17</sup> 他のCSIRTがそのサービスの一環として、元の勧告やアラートをさらに再配布することもあります。

取りが含まれます。アーティファクトを受け取ったら、すぐに検査します。これにはアーティファクトの特徴、構造、バージョン、および利用方法の分析、さらにアーティファクトを検知、除去、防御するための対応方法の開発（または提案）などが含まれます。アーティファクトハンドリング活動はさまざまなタイプの CSIRT によってさまざまな方法で実施されるため、このサービスは提供する活動と援助の種類に基づいて以下のように分類されます。

**アーティファクト分析：**CSIRT は、システム内で見つけられたアーティファクトの技術的検査および分析を実行します。この分析では、アーティファクトのファイルタイプや構造を特定したり、新しいアーティファクトを既存のアーティファクトや同じアーティファクトの他のバージョンと比較して類似点や相違点を確認したり、アーティファクトの目的や機能を究明するためにコードのリバースエンジニアリングや逆アセンブルを行うことがあります。

**アーティファクト対応：**このサービスでは、システムからアーティファクトを検知して除去するための適切な処置、さらにアーティファクトのインストールを防ぐための対策を究明します。アンチウィルスソフトウェアや IDS（侵入検知システム）に追加できるシグネチャを作成することもあります。

**アーティファクト対応調整：**このサービスでは、他の研究者、CSIRT、ベンダ、その他のセキュリティ対策専門家とアーティファクトに関連する分析結果や対応方法の共有や取りまとめを行います。活動には、さまざまな関係者からの技術的分析の取りまとめと、他の関係者への通知が含まれます。既知のアーティファクトとその影響度をまとめた公開されたアーカイブまたは Constituency のアーカイブを保守したり、対応方法を連絡することもあります。

### 2.3.2.2 事前対応型サービス

事前対応型サービスは、インシデントやイベントが発生したり検知されたりする前に、サービス対象のインフラやセキュリティ処理過程を改善することを目的としています。主な目的はインシデントを回避し、発生したときにはその影響や範囲を軽減することです。

#### アナウンス (Announcements)

これには侵入アラート、脆弱性警告、およびセキュリティ勧告が含まれます（これだけではありません）。このようなアナウンスでは、新たに発見された脆弱性や侵入ツールなど、中長期的に影響する新しい開発情報について Constituency に通知します。アナウンスによって、Constituency は新たに発見された問題が悪用される前に、システムやネットワークを保護することができます。

#### 技術動向監視

CSIRT では、将来生じる脅威の発見に役立てるために、新しい技術開発、侵入活動、および関連する動向を監視・観察しています。確認する対象を広げて、法的な決定や立法上の決定、社会的脅威や政治的脅威、新技術などを盛り込むことも

あります。このサービスでは、セキュリティに関するメーリングリスト、セキュリティ関連の Web サイト、さらに科学、技術、政治、および政府の分野における最新ニュースや雑誌の記事を読み、Constituency のシステムやネットワークのセキュリティに関連する情報を抜き出したりします。最も正確で優れた情報や解釈が得られるように、これらの分野の権威である他の関係者とやり取りすることも含まれます。このサービスの成果物は、中長期的なセキュリティ問題に重点を置いた、何らかの形のアナウンス、ガイドライン、または勧告などが考えられます。

## セキュリティ監査または審査

このサービスでは、組織または該当する他の業界標準によって定義された要件に基づいて、組織のセキュリティインフラの詳細なレビューと分析を行います<sup>18</sup>。また、組織のセキュリティ対策の調査を行うこともあります。提供できる監査または審査には、次のようにさまざまなタイプがあります。

- インフラのレビュー—ハードウェアやソフトウェアの構成、ルータ、ファイアウォール、サーバ、およびデスクトップ機器を手作業でレビューし、組織または業界で最善と見なされているセキュリティポリシーと標準構成に適合していることを確認します。
- 最善策のレビュー—従業員、システム管理者、およびネットワーク管理者にインタビューして、彼らが実践したセキュリティ対策が、定義された組織のセキュリティポリシーや一定の業界標準に適合しているか判断します。
- スキャニング—脆弱性スキャナまたはウィルススキャナを使用して、どのシステムやネットワークが脆弱であるかを調べます。
- 侵入テスト—システムとネットワークを意図的に攻撃して、サイトのセキュリティをテストします。

こうした監査や審査を実施するには、上級管理職の承認を得る必要があります。このようなアプローチの中には、組織のポリシーによって禁止されているものもあります。このサービスでは、テストや審査を実施する基準となる共通の実施要領を作成したり、テスト、審査、監査、レビューなどを実施するスタッフに求められるスキルセットや認定要件を策定したりすることもあります。このサービスは、監査と審査の実施に必要な専門的技術のある第三者の請負業者やマネージドセキュリティサービスプロバイダに委託することもできます。

## セキュリティツール、アプリケーション、インフラ、およびサービスの設定と保守

このサービスでは、CSIRT の Constituency や CSIRT 自身が使用するツール、アプリケーション、および一般的なコンピュータ設備を安全に設定・保守する方法に

---

<sup>18</sup> 業界標準および方法論としては、Operationally Critical Threat, Asset, and Vulnerability Evaluation<sup>SM</sup> (OCTAVE<sup>SM</sup>)、CCTA Risk Analysis and Management Method (CRAMM)、Information Security ForumのFundamental Information Risk Management (FIRM)、Commonly Accepted Security Practices and Regulations (CASPR)、Control Objectives for Information and (Related) Technology (COBIT)、Methode d' Evaluation de la Vulnerabilite Residuelle des Systemes d'Informa (MELISA)、ISO 13335、ISO 17799、ISO 15408 などがあります。

関する適切なガイダンスの定義や提示を行います。ガイダンスの提示に加えて、CSIRT は、IDS、ネットワークスキャンシステム、ネットワーク監視システム、フィルタ、ラッパー、ファイアウォール、仮想プライベートネットワーク (VPN)、認証メカニズムなど、セキュリティツールやサービスの設定の更新や保守を行うこともあります。さらに CSIRT は、これらのサービスを主要な職務の一部として提供することもあります。また、セキュリティガイドラインに従って、サーバ、デスクトップ、ラップトップ (ノートパソコン)、携帯端末 (PDA)、その他のワイヤレス機器を設定・保守することもあります。また、脆弱な可能性があるとして CSIRT が判断したツールやアプリケーションの利用方法や設定に関しての不具合や問題点を、管理職にエスカレーションすることも、このサービスの一環です。

## セキュリティツールの開発

Constituency や CSIRT に必要な、Constituency 固有の新しいツールを開発するサービスです。例えば、Constituency が使用しているカスタマイズされたソフトウェアのセキュリティパッチや、障害が起きたホストを再構築するためのセキュアなソフトウェア配布物の開発などです。また、脆弱性やネットワークのスキナーの新しいプラグイン、暗号化技術の利用を容易にするスクリプト、または自動化パッチ配布メカニズムなど、既存のセキュリティツールの機能を拡張するツールやスクリプトの開発も含まれることがあります。

## 侵入検知サービス

このサービスを実施する CSIRT は、既存の IDS ログのレビュー、定義した限界値に達しているイベントへの対応の分析と開始、あらかじめ定義されているサービスレベル契約またはエスカレーション方法に従ったアラートの送付を行います。侵入検知とセキュリティログの分析作業は、環境内でセンサーを配置する場所を決める場合だけでなく、記録された大量のデータを収集して分析する場合にも困難な作業になることが考えられます。多くの場合、間違った警告や攻撃、ネットワークイベントを識別するために情報を組み合わせて解釈し、そうしたイベントを排除するか最小限に抑える手段を講じるためには、特殊なツールや専門的知識が必要です。組織によっては、このような活動をマネージドセキュリティサービスプロバイダなど、専門的知識のある第三者に委託する場合があります。

## セキュリティ関連情報の提供

このサービスでは、セキュリティ向上に役立つ包括的で見つけやすい一連の情報を Constituency に提供します[Kossakowski 2000]。これには次の情報が含まれます。

- CSIRT への報告のためのガイドラインと連絡先
- アラート、警告、および他のアナウンスのアーカイブ
- 最新の最善策に関する文書
- 一般的なコンピュータセキュリティガイダンス
- ポリシー、手順、およびチェックリスト

- パッチ開発と配布情報
- ベンダへのリンク
- インシデント報告に関する現在の統計情報と動向
- セキュリティ対策全体を改善できるその他の情報

この情報は、CSIRTまたは組織の別の部署（IT、人事部、または広報部）において作成・発行されます。その情報には他のCSIRT、ベンダ、セキュリティ専門家など、外部リソースからの情報が含まれることがあります。

### 2.3.2.3 セキュリティ品質管理サービス

このカテゴリに分類されるサービスは、特にインシデントハンドリングやCSIRTに固有のものではありません。これらは周知の確立したサービスであり、組織のセキュリティ全体を向上することを目的としています。前述の事後対応型サービスと事前対応型サービスを提供する中で得られた経験を利用することで、CSIRTはこの品質管理サービスに別の方法では得られない独自の観点を持ち込むことができます。これらのサービスは、インシデント、脆弱性、および攻撃への対応によって得られた知識からのフィードバックや教訓を組み込むことを目的としています。このような経験を、セキュリティ品質管理プロセスの一環として、確立した従来のサービス（後述）に活かすことで、組織の長期的なセキュリティ活動を向上させることができます。

組織の構成と責任に応じて、CSIRTはこれらのサービスを提供したり、より大きな組織的なチーム活動の一部として参加したりすることが考えられます。

以下に、CSIRTの専門的知識がこれらのセキュリティ品質管理サービスにどのようにメリットをもたらすのかについて説明します。

#### リスク分析

CSIRTはリスク分析と評価に価値を付加することができます。これにより組織は、現実の脅威の評価、情報資産に対するリスクの現実的な質的・量的評価、および保護策や対応計画の評価を行う能力を高めることができます。このサービスでは、CSIRTは、新しいシステムと事業プロセスに向けた情報セキュリティリスク分析活動を実施または支援したり、Constituencyの資産とシステムに対する脅威と攻撃を評価したりすることが考えられます。

#### 事業継続と障害復旧計画

インシデントやセキュリティ動向の過去の事例と今後の予測から、事業運営に深刻な影響をもたらすインシデントはますます増える可能性があります。そのため、計画の取り組みにおいて、事業運営の継続を保証するためのインシデントへの最適な対応方法を決めるときに、CSIRTの経験と提言を検討する必要があります。このサービスでは、CSIRTは、コンピュータセキュリティの脅威と攻撃に関連するイベントを対象とした事業継続と障害復旧の計画に関与します。

## セキュリティコンサルティング

CSIRT は、Constituency の事業運営のために実装すべき最適なセキュリティ対策に関するアドバイスやガイダンスを提供することができます。このサービスを行う CSIRT は、新しいシステム、ネットワーク機器、ソフトウェアアプリケーション、エンタープライズ規模の事業プロセスを、購入、導入、保護するための推奨事項の準備や要件の特定を行うこととなります。このサービスには、組織または Constituency のセキュリティポリシーを策定する場合のガイダンスと支援の提供が含まれます。また立法機関や他の政府機関に証言やアドバイスを提供することもあります。

## 意識向上

CSIRT は、承認されたセキュリティ対策と組織のセキュリティポリシーに従うために、Constituency にどのような情報やガイダンスが必要かを明らかにすることができます。Constituency の全般的なセキュリティ意識の向上により、セキュリティ問題の理解を高めるだけでなく、日常業務をより安全な方法で遂行することにも役立ちます。これによって、攻撃の成功率を抑え、Constituency が攻撃を検知・報告する可能性を高めることができます。その結果、回復時間が短縮され、損失はなくなるか最小限に抑えられます。

このサービスを行う CSIRT は、セキュリティの最善策について説明し、予防手段に関するアドバイスを提供する記事、ポスター、ニューズレター、Web サイトなどの情報リソースを作成することによって、セキュリティ意識を高める機会を追求します。活動には、Constituency に現行のセキュリティ手順と組織のシステムに対する潜在的な脅威の最新情報を伝える会合やセミナーのスケジュール調整も含まれます。

## 教育／トレーニング

このサービスでは、セミナー、ワークショップ、コース、チュートリアルを通じて、コンピュータセキュリティ問題に関する情報を Constituency に提供します。テーマとしては、インシデント報告のためのガイドライン [CERT/CC 1998a]、適切な対応策、インシデント対応ツール、インシデント予防策など、コンピュータセキュリティインシデントの防止、検知、報告、対応に必要な情報などが挙げられます。

## 製品の評価または認定

このサービスでは、CSIRT は、製品のセキュリティと、それらが CSIRT または組織の許容可能なセキュリティ対策に適合していることを保証するために、ツール、アプリケーション、その他のサービスを対象に製品評価を行います。対象のツールとアプリケーションはオープンソースでも市販製品でも構いません。このサービスは組織または CSIRT が適用する基準に応じて、評価結果として提供したり、認定プログラムを通じて提供したりすることができます。



上記の節で説明した一連のサービスについてまとめると、執筆者たちの経験と他者との議論で分かったことは、CSIRTがどのようなサービスを提供することになったとしても、親組織または管理側は、チームがConstituencyに価値の高いサービスを提供するために必要なリソース（人材、技術的専門知識、設備、およびインフラ）を確実に確保する必要があるということです。さもないと、CSIRTは成功せず、Constituencyもインシデントの報告を行わないでしょう<sup>19</sup>。

### 2.3.3 サービスの選択

CSIRTは、提供するサービスを選ぶ際に最大限の注意を払う必要があります。提供する一連のサービスによって、チームが適切に機能するために必要なリソース、スキルセット、およびパートナーシップが定まります。選択するサービスは、何よりもまずCSIRTのConstituencyまたは親組織の事業目標を支援し、実現するものでなければなりません。提供するサービスは、チームの規模と専門的知識およびスキルの範囲に基づいてチームが現実的に本当に提供できるものにして下さい。

概して、CSIRTの成功はConstituencyに提供するサービスの全体的な品質によって決まります。広範なサービスを不十分に提供するより、少数のサービスを十分に提供するべきです。CSIRTがConstituencyから信頼と尊敬を受けるにつれ、スタッフと財源が許す限りサービスの拡張を図ることができます。

提供するサービスの範囲と性質を決めるときには、サービス選択によってCSIRTのミッション全体を支援・補完できるように気を付けてください。実際に、多くのチームが限られたサービスを提供していますが、そのConstituencyは自分たちの必要に適合するように改変したサービスや追加サービスを要求しています。こうした追加の要請が影響力のあるConstituencyメンバからなされ、CSIRTの上層部の管理支援が十分でない場合、チームの正式な設立綱領から外れていても、そうしたサービスに相当する何らかの支援を提供する傾向があります。

表3の属性と定義を利用すると、第3章に示すインシデントハンドリングサービスと同じ方法でその他の追加サービスを説明できます。

## 2.4 情報流通

CSIRTによって提供されるサービスが何であれ、そうしたサービスのうち相互に関連し合っているものや、どのような相互依存性があるかを理解することが重要です。特に、サービス間のやり取りと、それに付随するサービス間の情報流通方法を明確にする必要があります。次のことが明らかになっていることが重要です。

---

<sup>19</sup> CSIRTがサービスを提供せず、マネージドセキュリティサービスプロバイダなどの別の組織に活動を委託する場合も、CSIRT、組織のデータ、およびサービスを保護するためにスタッフ配置、設備、およびインフラに関して同じ基準を維持することが重要であり、基準を順守する必要があります。

- どのサービスがどのサービスからの情報に依存し、どのサービスに情報を提供するか。
- どのサービスがどのサービスに情報を提供し、どのサービスから情報を要請する責任があるか。
- どのサービスがどの機能や情報に対して共通のニーズを持っているか。
- どのサービスがどのサービスあるいは外部（他の CSIRT や Constituency）に対して、情報固有の責任（機密保持、適正使用）を移管するか。

この情報を使用することで、リソースの使用の最適化、重複作業の回避、既存の情報の有効利用が可能になります。例えば、すべての依頼を集中ヘルプデスクで処理し、依頼を適切なサービスに振り分ける（もしくは「トリアージ方式で対処する」という方法があります。それ以外に、受けた依頼に直接対応するサービスの場合は、作業の無駄な重複を避けるために、他の（関連する）CSIRT サービスとの情報の流れがどのようにつながっているかを適切に識別し、共有できるように注意する必要があります。

例：ウイルス以外のインシデント報告に対応する CSIRT と、ウイルスの活動に対応する別の部門という場合について例を挙げます。例えば Constituency が CSIRT に、システムに対する変更（ユーザアカウントの追加、システム変更、Web ページの改ざんなど）と、ウイルスの活動の兆候（セキュリティが侵害されたマシンに対する既知のウイルスまたはワームプログラムのインストール）の両方が含まれる障害を報告したとします。同時に、Constituency は当該システムの責任者が最近交代したことも通知したとします。Constituency は新しい担当者の最新の連絡先を通知しています。この場合 CSIRT は、ウイルスハンドリング部門が知っているべき情報を持っていることとなります。この CSIRT は、手順に従って情報を確認し、情報を他の部門に渡す許可を得てから、関連情報をウイルスハンドリング部門に渡します。これにより、Constituency がウイルスハンドリング部門に連絡してウイルスの活動を別個に知らせる必要がなくなります。また、どちらのグループも、自分たちのグループの監督下に入る活動が発生していることを認識できます。2つのグループは協力することも、どちらか一方の主導でインシデントを解決することに同意することもできます。

情報共有が一貫性をもって適切に行われるように注意しなければなりません。サービスごとに情報の扱いの要件は異なります。状況に応じて、情報の流れは何らかのポリシー（情報開示ポリシーなど）によって制限されることがあります。さらに、何らかのデータクレンジング（data cleansing：データ洗浄）の実施や、適切な契約上の合意のない限り、これらの多様な要件によって情報流通自体が妨げられてしまうこともあります。この問題は、サービス間での情報共有を決める前に検討し、ポリシーや手順が変更されたときには常に見直す必要があります。

依頼元に応じて、同じ類の依頼に対して異なる優先順位を付ける必要が生じることもあります。例えばインシデントハンドリングサービスが、脆弱性ハンドリングサービスと教育／トレーニングサービスの両方から、インシデントの統計情報の依頼を同時に受けることなどが考えられます。脆弱性ハンドリングサービスは、

確認された脆弱性が悪用される頻度を評価し、その後の活動に優先順位を付けるためにこの情報が必要であり、教育／トレーニングサービスは、公表資料を更新する手続きなどのためにこの情報が必要です。このような場合、脆弱性ハンドリングサービスからの依頼の方が優先順位が高くなるはずですが。というのは、インシデントの統計情報全体、そしてそれが脆弱性の検査と分析に与える影響の大きさに（そして、脆弱性ハンドリングサービスが **Constituency** にガイダンスを提供している場合は **Constituency** にも）すぐに影響する可能性があるためです。これに対し、トレーニング、教育、および啓発といった要素の更新の場合は、事前対応型のニーズよりも事後対応型のニーズであることが考えられます。この例では、情報共有の問題も再び浮上します。脆弱性ハンドリングサービスに提供される情報は、報告されたインシデントの頻度に関する詳細情報であることが多く、その中に具体的な悪用方法も含まれています。一方、教育／トレーニングサービスに提供される情報は、一般向けのトレーニング教材用に、悪用情報の具体的な詳細がおそらく削除されています（少なくとも未解決の悪用方法やサイトなどに関する詳細情報は削除されます）。

表 5に、通常提供される CSIRT サービスとインシデントハンドリングサービスとの間で考えられる情報流通の關係の基本的な例の概要をいくつか示します。これらの例は網羅的なものではなく、必須のやり取りを明示するものでもありません。どのようなタイプのやり取りが想定されるか、その一端を示すものです。もちろん、独自の CSIRT サービスを検討するときは、インシデントハンドリングサービスとのやり取りだけでなく、考えられるすべてのサービスとのやり取りのマトリクスを作成することが重要になります。

多くのチームでは利用可能なリソースが限られており、一般的なサービスのいくつかは密接なつながりがあるため、サービスの違いは曖昧になることがあります。区別に不自然さが生じる場合は、密接な關係のあるサービスを1つのサービスにまとめたほうがおそらく賢明です。その場合、サービス内の個々の要素は本書の用語に従って「機能」と呼ぶことができます。

表5：インシデントハンドリングサービスとの間に考えられる情報流通の例

サービス名	インシデントハンドリングへの情報流通	インシデントハンドリングからの情報流通
アナウンス	現在の攻撃シナリオに関する警告	統計またはステータスの報告 考慮または調査すべき新しい攻撃のプロファイル
脆弱性ハンドリング	特定の脆弱性の悪用から保護する方法	新しい脆弱性の存在の可能性

アーティファクトハンドリング	特定のアーティファクトの使用を認識する方法に関する情報 アーティファクトの影響/脅威に関する情報	インシデントにおけるアーティファクトの識別に関する統計情報 新しいアーティファクトのサンプル
教育/トレーニング	なし <sup>20</sup>	事例と動機付け 知識
侵入検知サービス	新しいインシデント報告	チェックすべき新しい攻撃プロファイル
セキュリティ監査またはアセスメント	侵入テストの開始/終了スケジュールの通知	一般的な攻撃シナリオ
セキュリティコンサルティング	一般的な落とし穴と脅威の大きさに関する情報	事例/経験
リスク分析	一般的な落とし穴と脅威の大きさに関する情報	統計情報、シナリオ、または損失
技術動向監視	将来の攻撃シナリオに関する警告 新しいツール配布に関するアラート	統計またはステータスの報告 考慮または調査すべき新しい攻撃のプロファイル
セキュリティツールの開発	Constituency が使用できる新しいツールの入手方法	製品の必要性 現在の対策に関する見解の提示

以下の例では、サービス間の関係と、サービス間の情報フローを評価する必要性を強調します。

例：CSIRT が（インシデントハンドリングサービス以外にも）指定されたシステムを攻撃してテストするチームメンバを割り当て、詳細なセキュリティアセスメントサービスを提供するというシナリオを考えます。テストの間、担当しているシステム管理者やネットワーク管理者が、セキュリティアセスメントが行われることをほとんど知らされなかったとします。そのため、テスト中にセキュアでないホストへの攻撃が成功した場合、セキュリティが侵害されたマシンのシステム管理者はその行為に気づき、侵入と考え、侵入として CSIRT に報告すると考えられます。セキュリティアセスメントサービスプロバイダがインシデントハンドリングサービスにテストの事前通知を行えば、CSIRT チームはまず、報告された行為がテストによるものかどうかをセキュリティアセスメントチームのメンバに確認することができます。事前にアラートが出されていないと、インシデントハンドリングサービスは正式なインシデント報告と考えられるものに対応するために、弁護士に通報したり、他の部署に支援を要請した

<sup>20</sup> 表 5 にまとめた情報の流れとやり取りのコンテキストでは、インシデントハンドラが必要とする可能性のある、あるいは他のソースから入手する可能性のあるトレーニングや指導については取り上げていません（もっとも、それが必要であり、チームの知識とスキルにとって重要な要素であることは認識しています）。CSIRT の教育/トレーニングサービスは通常、他のサービスからのアウトプットの「受取人」であり（例えば、インシデントハンドリング担当者が提供するインシデント、脆弱性、またはアーティファクトのハンドリングサービスなどから知識を習得する）、情報をトレーニング製品にまとめます。これらの製品はパッケージ化され、トレーニング、クラス、セミナー、ミーティング、または他の場を通じて適切な形で Constituency に提供されます。

りするなど、不要な労力を費やし始める可能性があります。結果として、CSIRT の貴重なリソースを浪費することになります。さらに重要なことは、チームの外部（サイト経営者、システム管理者、法律顧問など）には、そのCSIRT 内でチームの別の担当部門の取り組みを相互に把握していないように映るため、CSIRT の評判が損なわれる可能性もあるということです。

## 2.5 ポリシー

ポリシーは組織やチームが採用する運営原則です。この節では、ポリシーとはどのようなものであり、どのようなものであるべきか、またどのような性質を持つべきかを概括的に述べます。ただし、ポリシーを文書化して終わりというわけではありません。ポリシーの施行と強制が可能かどうか、また、期待どおりに機能するかどうかを把握することが重要です。この節は、これらの問題に関する議論で終わっています。どのCSIRT にとっても欠かせない要件であるグローバルポリシー（情報開示ポリシーやメディアポリシーなど）の詳細については、4.2節「基本ポリシー」で取り上げます。

まず組織のポリシーを明確に示し、組織の全員に理解させる必要があります。ポリシーを十分に理解していないと、スタッフはその職責を正しく実践し、成果を挙げることはできません。

サービスが原則として「顧客向け」に定義される場合（インシデント対応支援サービスや教育／トレーニングサービスなど）、サービス提供の根本的なポリシーは、主に特定の活動にとってふさわしい行動を規定するための、内部のガイドラインです。この場合のポリシーには、情報の分類、セキュリティ、メディア、および行動規範が含まれます。後者の2つに関しては、単に内部のコミュニケーションだけでなく、外部のコミュニケーションに大きく関係するのではないかという意見もあるかも知れません。確かにそのとおりですが、この外部の側面は顧客に「提供される」ものではありません。それ自体はサービスではなく、サービスが提供される方法と品質に影響を及ぼすに過ぎません。

ポリシーはサービスに固有である可能性があります。例えば、インシデント対応支援サービスでは依頼元の認証に（インシデント情報を交換する前に、依頼元の確認のための手順の定義）に関して具体的なポリシーを必要とすることがあります。教育／トレーニングまたは技術動向監視など、別のサービスでは、依頼元の認証を必要としないこともあります。この節では、CSIRT のサービスを網羅する全体ポリシーに重点を置きます。しかし、ここで述べることのほとんどは、サービス固有のポリシーにもそのまま当てはまります。

ポリシーと手順はよく混同されるため、その関係を理解することが重要です。手順とは、ポリシーの範囲内でチームがどのように活動を行うかを詳細にしたものです。手順はポリシーを成功裏に運用するのに非常に役立ちますが、対応する手順のないポリシーが存在しうることはごくまれです。きわめてシンプルなメディア向けポリシーは、「メディアには丁寧に接し、決して嘘をついてはいけませんが、

一般的な匿名情報についてのみ話す」ことです。しかし、対応する手順があれば、特に緊張した状況では、多くのスタッフがポリシーガイドラインから逸脱しないようにするのに役立ちます。以降のポリシーの説明においては、問題の理解を深める場合にのみ手順に触れることにします。

## 2.5.1 属性

ささいなことかも知れませんが、ポリシーを詳細な手順として定義するべきではないことを強調しておきます。ポリシーは、特定のテーマ領域に不可欠な特徴を概説するものでなければならず（この場合も、前述したメディアポリシーの例を考えてください）、ポリシーの施行を助ける詳細手順のベースとなる、必要な情報をすべて提供するものでなければなりません。ポリシーはすべて同じレベルの抽象性をもって書かれている必要があります、法律面のレビューと該当する適合性のレビューを受けなければなりません。表 6 に、ポリシーに盛り込む必要のある一連の属性を示します。

表6：基本的なポリシーの属性

属性	説明
管理職による承認	ミッションステートメントと同様に、上級管理職に承認されない限り、ポリシーは実施できません。
明確さ	技術職、管理職、経営職を問わず、あらゆるチームメンバが、ポリシーが何に関するものかを容易に理解できなければなりません。不要な専門用語を避け、曖昧にならないようにし、ごく短い文を使用します。可能であれば（開示制限に従って）、セキュリティまたは IT 部門以外の誰かにポリシーを読んでもらってください。その人が理解できない場合は、ポリシーを書き直します。
簡潔さ	簡潔なものがよいポリシーであると言えます。長いポリシーは悪いポリシーであるか（すなわち、余計な言葉を使用している）、実は手順が含まれているようなポリシーです。  残念ながら、セキュリティポリシーは実際に簡潔でない場合が多く、紛らわしいことに管理面（ポリシー）と運用面（手順）を混同しているため、現実的に誰の関心も引かなくなることが考えられます。このような状況は避けなければなりません。
必要かつ十分	ポリシーには、特定のテーマ領域（セキュリティポリシーなど）における適切な行動を規定するもののすべてを含める必要がありますが、それ以上に詳細であったり弾力的であったりする必要はありません。そうした属性は対応する手順と品質管理に盛り込むことができます。
有効性	「最先端のセキュリティを提供する」のように魅力的に聞こえるが、役に立たないステートメントは、解釈が自由なので避けてください。「お客様に丁寧に対応すること」といった常識的なステートメントは、人々が同じ認識を共有するため、ポリシー内でも適切であり有効です。
施行可能性	ポリシーは施行可能なものでなければなりません。「お客様に丁寧に対応する」という例では、スタッフがお客様への対応の仕方を理解できるように、定期的なトレーニングを提供する必要があることを基本的に述べるようなステートメントを追加することになるかも知れません。
強制可能性	ポリシーは強制可能なものでなければなりません。そうでなければ、ほとんど価値はありません。たいてい、ポリシーが実行可能であれば、矛盾したことを述べていない限り、通常は強制可能でもあります。ポリシーの使用を評価するには、具体的な測定基準が必要です。  例：矛盾するポリシーの例としては、例えば、内部の情報セキュリティを優先順位 1 位に設定しながら、同時にスタッフのプライバシー保護を徹底するようなセ

属性	説明
	セキュリティポリシーです。プライバシー保護の徹底によって、内部の者による脅威に際してセキュリティを強制するのが困難であるか、不可能となる場合さえあります。

## 2.5.2 内容

ポリシーの内容は主に、特定のテーマ領域における行動の定義です。例えば、メディアへの対処法、入ってくる情報の分類方法、人為ミスの結果の対処方法などです。これらの特徴はポリシー定義の境界条件です。ポリシーの内容に現れる、一般的な特徴をいくつか明示することもできます。これらの特徴を表7に示し、必要に応じて例を盛り込みます（一貫性のため、以下の例ではメディアポリシーの領域に重点を置きます）。

表7：ポリシーの内容の特徴

特徴	説明
ミッションとのつながり	ポリシーがどのようにミッションステートメントから派生しているかを記述します。
役割の識別	ポリシーの（さまざまな局面の）対象となる関係者を明確に識別する必要があります。例：メディア、メディア連絡窓口、その他のスタッフ。
責任	該当する場合は、識別した関係者の義務と責任を定義する必要があります。（注：ただし、メディアの義務を定義することはできません）
やり取り	ポリシー内で識別される関係者間の適切なやり取りを記述します。例えば、メディアに直接または電話で話をする、インタビューの前に質問のリストを要求する、書かれたテキストは発行の前にレビューを要求するなどです。
手順	基本的手順を指示することもできますが、ポリシー内で詳しく説明するべきではありません。例えば、メディア関係者のIDを確認する手順を準備する必要がある、あるいは権限を与えられたスタッフだけが（適切なトレーニングの後でのみ）メディアと話をできると記載します。
関係	このポリシー、サービス、その他のポリシーの関係を確認します。メディアポリシーの例では、セキュリティポリシーとの関係や、ほかにインシデントハンドリングサービスの情報取得のプロセスとの関係などです。
保守	文書の保守と更新に関する責任とガイドライン（例えば、依頼はトリアージ機能を通じて受け取ることができるなど）を記述します。
用語解説	CSIRTの用語定義を提供し、組織のローカルな用語や略語をすべて定義する必要があります。これによって、すべての人、特に新しいチームメンバーがポリシーを理解できるようになります。

## 2.5.3 検証

ポリシーを定義したら、実際に施行する（場合により強制する）前に、現実面での妥当性を検証することをお勧めします。妥当性のチェックとは、ポリシーにおける考え方をすべて現実の行動に置き換えられるかどうかを検証することです。

例：頑固で攻撃的な人々に対応するときに、「常に優しく接すること」というだけではほとんど役に立ちません。

ポリシーの検証に関しては、以下の点を考慮する必要があります。

- 可能であれば、ポリシー検証の責任者は、ポリシー作成者と別の人物にします。これによって利害の対立を防ぐことができ、ポリシーの客観的な評価が保証されます。
- ポリシーが曖昧にならないように、表 6 および 7 に詳述したポリシー属性と内容の特徴の検証には特に注意してください。
- 他のポリシー、サービス、および手順との間で、またポリシー内での一貫性チェック（矛盾がないことの確認）を行ってください。  
例：ネットワークセキュリティを採用しているにもかかわらず、パスワードを平文で送信する習慣がある。
- 施行可能性と強制可能性を検証します。ポリシーを試験的に施行し、最悪の場合のシナリオを選択して、強制可能性も含めて現実の行動をチェックするのは、ポリシーを検証する上で非常に良い方法です。

## 2.5.4 施行、保守、強制

ポリシーの検証を終えたら、改訂を加えられるよう、ポリシー作成者にフィードバックする必要があります。改訂が終了したら、ポリシーを再度テストする必要があります。検証が終わり、それ以上変更を加える必要がなければ、ポリシーを施行できます。

一度すべてが完了したら、ポリシーを保守する必要があります。つまり、現実の行動を定期的にチェックする必要があります。これらのチェックの多くは検証と同じであり、新しいチェック項目がいくつか追加されることもあります。後者の例としては、メディアポリシーを利用して、情報の依頼を受けてから事前に設定した時間内にメディアに情報を提供しているかをチェックすることなどが挙げられます。この現実の行動が検証段階で測定されていないのは明らかです。

検証プロセスで生じたチェック項目とポリシーの継続的な検証とは、実際のところ、「品質パラメータ」の動きをチェックすることです。保守と強制（チェックで「何かがおかしい」となった場合に実行すべきこと）は、2.6節「品質保証」で述べる通常の品質保証システムに含まれます。どのポリシーにも、そのポリシーに則って実施されたサービスの品質を追跡し、必要に応じてポリシー変更を提案する保守管理者が必要です。時間の経過とともに状況が変化しても、一度しか施行されず、永久に「現状のまま」使われるポリシーがあってはなりません。「今までこのようにしてきたのでこのまま」という言い訳は、今使われている技術の変化の速さ、CSIRT の役割、Constituency に提供するサービスを考えれば、通用しません。

## 2.6 品質保証

Constituency に「十分な」サービスを提供するには、サービス、サービス間の情報の流れ、およびサービスを機能させる手順を定義するだけでは明らかに不十分です。関連する形態の品質保証も必要です。この保証は、「試みる」という形態



のステートメントから、関連する強制やエスカレーションの手順、法的責任および違約条項に支えられた完全指定の品質パラメータまでさまざまです。

CSIRT の分野では、類似点はあるものの、すべてのチームに渡って標準的なアプローチが使われることはめったにありません。いくつかのチームは少なくともインシデントに優先順位を付けて、優先順位の高いインシデントと見なしたものに先に取り組もうとします。あるチームの報告によれば、最もよく使われる品質の測定基準は「上級管理職に連絡する苦情がないこと」でした。しかし、公式または非公式に品質保証（QA）に取り組んでいるチームはほとんどないため、これらは例外です。QA が欠けていると、提供するサービスにおける一貫性の欠如、目的を果たさないサービス、人的リソースの不適切な起用につながります。この節では、CSIRT 環境に適した QA アプローチを提案します。時間と経験によって、他のどのようなアプローチがこの分野に（より）適しているかが分かるでしょう。

基本的な品質保証の要素と CSIRT 環境におけるそれらの利用について説明します。QA システムは 3 つの部分、すなわち品質システムの定義、チェック、およびバランスで構成されます。

定義では、QA システムの品質を説明するパラメータを指定します。チェックは、これらの品質パラメータを実際に測定するために設けられています。最後に、バランスでは、これらの測定結果を品質保証に活用できるようにします。

## 2.6.1 品質システムの定義

第一段階では、ミッションステートメントによって要求される QA レベルを記述するための最小限の品質パラメータセットを見つけます。複数のサービスを提供する場合は、複数の品質パラメータセットを各サービスに 1 セットずつ割り当てることができます。さらに、より細かいレベルで、サービス内の機能ごとにパラメータのサブセットを割り当てることができます。

品質システムは、ミッションステートメントからポリシーとサービス、それらのサービスを構成する機能、および関連するすべてのやり取りと手順に至るまで、トップダウンで定義する必要があります。ミッションステートメントは、CSIRT の品質について受け取られる全般的な感触を導き出せるものにします。例えば、ミッションステートメントには、「タイムリー」、「ベストエフォート」、または「フレキシブル」のような品質の受けとめ方を含めることもできるでしょう。言うまでもなく、それに続く品質定義はすべて、ミッションステートメントに沿っている必要があります。

品質パラメータセットには、すべてのポリシー、サービス、サービス機能、および手順に対する品質パラメータが含まれます。これらの要素ごとに、独自の品質パラメータのサブセットが含まれますが、サービス間やサービス機能間でパラメータがいくつか共通する場合があります。しかし、留意すべき重要なことは、ポリシー、サービス、およびサービス機能の中だけでなく、情報の流れのように、

それらの間でも品質は動的で定義可能であるということです。そのため、品質パラメータを定義するときには、サービスのやり取りも考慮する必要があります。

例：チームのミッションステートメントでインシデントおよび脆弱性ハンドリングサービスに言及しているとします。当然、この場合は2つの品質パラメータセットを定義するのが現実的です。1つはインシデントハンドリングサービスに関するもので、もう1つは脆弱性ハンドリングサービスに関するものです。インシデントハンドリングのセットの典型的なパラメータとして、Constituencyからの最初のインシデント報告への対応にかかる時間の上限があります。一方、脆弱性ハンドリングのパラメータとしては、解決策がある場合に脆弱性に関する勧告を公表するというだけでなくかも知れません。

品質パラメータを拡張して、インシデントハンドリングサービスと脆弱性ハンドリングサービス間のやり取りも品質パラメータの格好の対象になると考えられます。例えばこのようなパラメータとして、インシデントハンドリングサービスがインシデントの分析中に脆弱性の悪用と考えられる証拠を発見した場合に、脆弱性サービスが脆弱性の評価をインシデントハンドリングスタッフ（または他の人）に提供するのにかかる時間の上限などがあります。

品質システムの多様性と幅をさらに明らかにするために、他の品質パラメータの例を以下に示します。

- サービスイベント（インシデント報告や脆弱性報告など）および／または優先スキームに対する応答時間
- サービスイベント（短期）に提供する情報のレベル
- サービスイベントの有効期間
- 長期中で提供する情報のレベル（報告、要約、アナウンス）
- 秘密保持
- 検証

品質パラメータの適切なセットが明らかになったら、パラメータのすべての「数量」に値を割り当てることで品質システムの定義が完了します。

例：

パラメータ	値
脆弱性報告に対するフォローアップ時間	急を要さない脆弱性に関して、CSIRTは最初の報告から2営業日以内にConstituencyをフォローアップします。
優先度の高いインシデントのフォローアップ	優先度の高いインシデントは2時間以内に受領確認します。このような報告を受けてから1時間以内に分析が開始されます。
優先度の低いインシデント報告のフォローアップ	インシデント報告は4時間以内に受領確認します。このような報告を受けてから48時間以内に分析が開始されます。

理解すべき重要なことは、品質システムが必ずしも静的なもの、すなわち、すべてのパラメータを定義して、特定の値を割り当てただけのものではないということです。あるパラメータの状態が他のパラメータに割り当てられた値に影響したり、柔軟なパラメータのセットが使用されたりする場合があります。

例：すべてが正常な状態とは異なって見える、危機的状況を考えてください。このような事態には異なる2つのアプローチで対応できます。

- a. 「危機」というパラメータがあり、考えられる値は「有」と「無」であり、他にもいくつかの品質パラメータが定義されているとします。「危機」が「無」であれば、残りのパラメータがすべて使用され、値が割り当てられます。しかし、「危機」が「有」になると、品質パラメータの多くは無視され、(応答時間など)残りのパラメータには厳しい値が割り当てられます。
- b. CSIRTは単に、「優先順位の低いインシデントの95%は5日以内に処理する」など、柔軟なパラメータを使用します。これらのパラメータについてConstituencyは知らされていますが、CSIRTが緊急事態のときには明確に意識する必要はありません。

いずれにしてもCSIRTは、Constituencyがサービスレベルに関する品質パラメータの変更について知らされない、暗闇に取り残されたように感じるかもしれないということを考慮しなければなりません。

## 2.6.2 チェック：品質パラメータの測定基準

品質システムを定義するだけでは十分ではないので、その品質システムがチームの期待に応えるものかどうかをチェックする必要があります。そのため、品質パラメータのチェック(現実の行動の測定)は、どのようなQAシステムでも不可欠な部分になるのです。

品質パラメータを定義したら、それらのパラメータをチェックする方法とそれらを測定する方法を定義する必要もあります。これは決して軽視してよい作業ではなく、報告体制の確立など、いくつかの重要な施策を事前に準備することが求められます。さらにチェックシステムの定期的な監査も行い、現実の世界で適切に機能しているか、また最終的な要求である品質についての十分なチェックになっているかを見る必要があります。

この（チェックの）要求は、品質パラメータが明確であること、および定量化できることが望ましい理由を示しています。「良好」または「不良」のような適性を評価するのは困難ですが、最初のインシデント報告に対応するのにかかる平均時間などのパラメータを測定するのは簡単です。

パラメータをチェックする頻度も実際には、それ自体が品質パラメータであることに留意してください。その値も慎重に最適化する必要があります。チェックが少なすぎると、明らかに QA を危うくしますが、あまりに頻繁にチェックすると、実際に仕事をするよりも、優先順位の再検討など期待に応えるために費やす時間が長くなってしまいます。

### 2.6.2.1 報告と監査

品質を追跡するには、パラメータ（応答時間、問題のカテゴリ、優先順位など）を測定するワークフロー管理システム（4.3.2節「ワークフロー管理」を参照）と（標準およびエスカレーション手順の使用を評価する）報告体制が必要です。報告にはさまざまなレベルがありますが、明白なカテゴリとしては、運営管理、総括管理、Constituency、世間一般への報告があります。ワークフロー管理ソフトウェアが導入されていると、報告を自動化する傾向（もしくは要望）があります。しかし注意しなければならないのは、このような報告が可能だというだけで報告を生成するものではないということです。報告というものは受取側にとって必要且つ役立つ情報を提供するものでなければならないのです。

品質を確保するには、QA チェックシステム自体の定期的な監査（あるいは追跡）も必要です。そこでシステムに甘さや不備がないかをチェックしなければなりません。具体的には以下のことを行う必要があります。

- 必要な手順の数を最小限に抑え、明確なものにする
- CSIRT スタッフになぜその手順を導入しているのかを理解してもらう（スタッフのモチベーションを高めるため）
- 細かい記述は避ける：自分で考えられるほうが、スタッフのモチベーションが高まる（また、すべてについてルールを作るのは不可能に近い）
- 監査を実施し、結果を見直しのサイクルに申し送る

犯しやすい間違いの1つに、システムを評価するために長く複雑なルールを作ってしまうということがあります。これではたいてい、ルールが守られているかを確認するために非常に厳しい監査を実行しなければならなくなります。多くの場合、このような監査はあまりにも厳格であるために事前にアナウンスする必要が

生じ、その結果として、品質保証を支援するという大きな目標に監査を役立てるのではなく、監査要求を満たすこと自体が目標になりがちです。

品質チェックシステムは、もともとは効果的なものとして設計されていても、いざれ不十分なものになるおそれがあります。そうなるのは、品質パラメータが変化する可能性があるためです。

例：顧客からのインシデント報告に対する最初の応答時間をパラメータとして定義したとします。「報告を受け取りました...ありがとうございます」という短いメッセージで報告の「受信確認」だけをする自動電子メール応答サービスを導入するまでは、十分妥当なパラメータであるかも知れません。このプロセスは非常に迅速であるかも知れませんが、おそらく最初に測定するつもりだった品質パラメータではなくなります。そのため、状況に応じてパラメータを改良する必要があります。例えば、「顧客からの報告を受信したら、最初の自動応答を電子メールで送信します。CSIRTスタッフによる人的な応答は、初期レビュー後 24 時間以内<sup>21</sup>に電子メールで送信します」などが考えられます。

### 2.6.3 バランス：品質保証のための手順

品質を保証するには、品質パラメータについての現実の行動をチェックするだけでは不十分です。品質が危険な状態にあるときには、品質を強制する手順が必要です。その際、標準の強制手順ではうまくいかない場合や、品質システム自体が不十分であることが明らかになった場合の、エスカレーション手順を定義できます。最終的には、罰則および賠償条項が品質を強制するのに役立ち、同時にサービスプロバイダがむやみに潜在的な訴訟の対象にならないようにします。これらの手順と条項は、品質保証のための「バランス」と見なすとよいでしょう。

スタッフのストレスレベルが高く、リソースが全般的に脆弱で無理を強いられるような、要求の厳しい CSIRT の環境では、スタッフが不要な障害に押しつぶされずに職務を高い水準の品質で遂行できることが重要です。そのため、手順、チェック、職務遂行能力の間で適切なバランスを追求する必要があります。正しく書かれた手順は人的ミスの緩衝装置の役割を果たします。（人的）ミスを考慮に入れていない手順は設計に不備があります（4.2.6節「人的ミスに関するポリシー」を参照）。

また、品質を強制する何らかの手段を顧客（Constituency）に提供することもお勧めしますが、これは通常、間接的なプロセスになります。これは「受けがよい」だけでなく、最良の品質判定は、このサービスを実際に利用している（またはサービスに苦しんでいる）顧客から聞こえてくる場合がよくあります。

Constituency に影響力を持たせる便利な手段の 1 つに、ユーザグループや諮問機関（あるいはその両方）などを設けることが挙げられます。ただしこのような手段も有効ですが、最も効果的な方法はおそらく罰則条項を導入することです。つ

---

<sup>21</sup> あるいは、規定した他の何らかの時間枠（またはパラメータ）。

まり、期待されたレベルのサービスを実施しないと、チームは顧客にお金を支払ったり払い戻したりしなければならないということです。

顧客が契約の一部を果たさないこともあります。その状況が続き、深刻である場合（守秘義務違反など）は、そのような顧客の支援を中断または縮小する手順も用意する必要があります。

CSIRT スタッフの観点からは、エスカレーション手順は通常は規定されており、CSIRT プロセス全体の不可欠な部分です。しかし、品質が本当に危険にさらされ、月次報告または四半期報告がまとまるまで待っていると間に合わない場合、運営管理者は上位の管理者に迅速かつ効果的に通知することができます。日常業務には、問題とその修正にかかる時間の見積もりを顧客に通知するかどうかの決定が含まれます。この決定は、合意しているサービスレベルと、その問題によって生じる直接的な障害によって決まります。また、品質システム自体がうまくいかず、修正する必要がある場合は、エスカレーションが行われることもあります。

品質を定義して公示する（ただし保証はしない）と、サービスパラメータが満たされず、Constituency が損害をその不履行の結果だと主張した場合に、ほとんどの国で CSIRT が責任を問われることとなります。ただし、チェックとバランスも含めた QA システムを配備した一般的なケースであっても、一部の国（特に米国）では賠償請求が予想されます。場合によっては、特に罰則条項も用意されている場合は、QA に賠償条項を追加すると役に立ちます。このような条項は法律の専門家が対応するのが一番です。ほとんどの国では、金銭上の損害に対する責任を拒否するだけでは不十分です。

要点：品質を定義する場合は、必ずその品質を保証してください。保証手段に優先順位を付けます。教育と意識向上は、特に長い目で見れば、圧力を高めるより効果的な手段です。ワークフロー管理ソフトウェアシステムを配備している場合は、そのシステムに通常の強制とエスカレーションの手順を統合することが可能であり、お勧めします。これは時間の経過とともに手間が減り、手順の利用に関する報告書を作ることもできます。

最後に 1 つ大事なことは、手順とポリシーは永遠のものではないため、所有者および/または保守管理者を設定し、ライフサイクルを明確にする必要があります。たいてい、手順は計画段階で作成されます。そして、計画段階が終わると変更管理は行われなくなりますが、誰かが実際にその手順につまづくまで管理されないままその手順は存在し続けるのです。

## 2.6.4 Constituency の視点から見た品質

ミッションステートメントに対応する適切な品質レベルが確実に保たれるように、内部用の品質パラメータセットがすべて揃っている必要があります。しかし、Constituency に伝えられる品質パラメータセットは一般に、内部用の品質パラメータのサブセットです。

商業上の観点からは、（すべてではないにしても）十分なパラメータセットを Constituency に伝えることをお勧めします。そうすることで、Constituency にまじめに対応しており、隠すことが何もない、というメッセージを伝えることとなります。一方、同じ商業上の観点から、また時には法的責任の観点から、CSIRT が簡単に保証できるパラメータのみを伝えるのが賢明かも知れません。

2つの間で歩み寄ったところが最良の選択肢です。いずれにしても、定義が明確でない品質パラメータを伝えたり、定量化できないパラメータを設定したりするのは、それらが全体的な品質保証に役立つものであっても避けてください。Constituency は理解できないものを嫌う傾向があります。

## 2.7 個別ニーズへの適応

多くの場合、CSIRT を構築する理由は、組織が直面した何らかのニーズや問題から生まれます。したがって論理的には、CSIRT としてどんなに一般的な形態を選択しても、少なくとも個別のニーズに合うように適応することになります。

例：多様なユーザで構成されるあるコミュニティの、ネットワークベースの攻撃を何回か経験したことによる、コミュニティ内の支援と調整を円滑にする調整 CSIRT の設立。このチームは必ずしもコンピュータウィルスに専念するとは限りません。

例：上の例の調整 CSIRT はやがて、ユーザからの報告や世界中にある他の同格のチームからの情報で、コンピュータウィルスとワームに対する懸念が増大していることに気が付きます。この CSIRT は、悪意のソフトウェアによる攻撃を専門に扱う新しいスタッフを雇用します。

例：重大なコンピュータウィルス問題を抱えており、既にウィルス対策チームが確立している組織では、コンピュータウィルスや悪意のソフトウェアなどによるインシデントには対応せず、ネットワーク攻撃に専念する CSIRT を設立します。この CSIRT とウィルス対策チームの間の合意したやり取りの方法と窓口によって、有益で必要であればいつでも連携をとることが保証されています。

どのチームにも適応すべき環境がそれぞれ存在します。そのため、基本構造だけは同じであっても、細部に渡って同じ CSIRT は2つとありません。

例：強制権限（Constituency のシステムへのアクセス権など）があり、極秘データ（軍事、商用、医療）を扱う環境で活動する CSIRT は、特別に厳しいセキュリティ対策に適応し、担当者を頻繁に審査する必要があります。審査のレベルは CSIRT によって異なり、提供するサービスは似ている場合や、まったく異なる場合もあります。

CSIRT ごとに、ミッションステートメントとサービスを定義するときに、CSIRT の要件を整備し、適応させることは言うまでもありません。当然、品質保証シス

テムにも、それらの変更を必要に応じて反映する必要があります。しかし、適応が最もはつきりしてくるのは、CSIRT のポリシーと手順、つまりチーム運営のかなり現実的な処理においてです（第 4 章に記載）。

それでも基本的なポリシーは、以下の例に示すように暗黙的に現れます。

例：軍隊や企業の CSIRT は、あらゆる問題とテーマを対象とする比較的抑制的なメディアポリシーを採用します。

例：国立の研究ネットワークのユーザコミュニティにサービスを提供する調整 CSIRT は、技術的詳細をすべて説明することは認めますが、関係する個人や組織の身元を明かすことは認めないというメディアポリシーを採用します。

例：ウィルス対策 CSIRT は、切り離されたテスト環境やその環境を再インストールしてクリーンな初期状態に戻す完全なバックアップイメージも含め、入ってくるバイナリ（ウィルスサンプルなど）の取扱方法に関する厳しい手順を採用します。

例：分析サービスを提供しない調整 CSIRT にも、同じように厳しい手順はありますが、ウィルスサンプル（バイナリ）を受け取っても、必須のコンピュータウィルス検査を行った後でアーティファクトを単に切り離すだけです。そのような CSIRT は組織内に分析能力がないため、受け取ったバイナリをさらに分析することはできません。

この段階で注目に値するトピックが 2 つ残っています。1 つめのトピックは、すべての CSIRT が適切な作業を実行するために直面せざるを得ない環境変化にすぐ適応できる CSIRT の「一般的な」能力です。2 つめのトピックは法律、法的責任、および規制に関するものです。これらについては後述します。

### 2.7.1 柔軟性の必要性

CSIRT はコンピュータセキュリティインシデントや攻撃による動的環境変化に備える必要があります。また、既存のガイドラインや専門知識では明示的にカバーできない可能性のあるどのような状況にも対処できるようにする必要があります。柔軟性の必要性を示す例として、CSIRT 環境を動的に変化させる要因のいくつかと、CSIRT への影響を表 8 に示します。



表8：動的環境の要因の例と CSIRT への影響

要因	CSIRT への影響
CSIRT が受け取るインシデント報告の回数は、簡単には予測できません。	CSIRT は、予期しない長期に渡る作業負荷のピークや、優先順位の衝突を経験します。
侵入者（または攻撃者）は新しい攻撃手法を企てたり、既存の攻撃手法を変えたりしながら、絶えず攻撃の新しい手法を考え、策を講じています。	CSIRT に報告されるインシデントの種類や複雑さが、時間の経過とともに変化します。
技術の進歩によって、Java や ActiveX に起因するものなど、新しい攻撃の可能性がもたらされます。	CSIRT に要求される技術的な専門知識が変わります。CSIRT のスタッフは、技術の進歩に遅れないようにする必要があります。
国によっては、新しい問題と考えられるものに対応するための法律の整備が始まったばかりです。世界中の多くの国で、技術の変化や侵入者の活動によって引き起こされる脅威に遅れを取らないように、コンピュータ犯罪に関する法律が検討され、積極的に改正されています。	CSIRT は、運営されている環境において絶えず変化する法的枠組みを認識し、それらに合わせて適応する必要があります。
CSIRT がやり取りする各関係者のニーズ、技術的専門知識、経験、理解のレベルに基づいて、CSIRT に対してさまざまな要求がなされます。	CSIRT への相反する要求を満たすために効果的に対応するには、体制が十分でない CSIRT 内のリソースでは足りない状況が生じます。

表 8 のような要因によって、CSIRT に報告されるインシデントの種類、優先順位の付け方、対応の性質、および適切な報告要件は、時間の経過とともに変化することが十分に予想されます。変化の原因が作業負荷、技術的なフォーカス、法律問題、または Constituency のニーズの変動のいずれであっても、CSIRT はそうした変化に容易に適応できるように、柔軟なポリシーと手順を持つ必要があります。

これらの要因は通常、CSIRT が直接コントロールできる範囲の外にありますが、ある程度の事前の計画によって備えることができます。

- 外部リソースを確保し、協力してもらうことで危機的な状況（極端な作業負荷や優先順位の衝突など）に対応するか、そうした状況が続いている間はサービスのレベルを低くしたり変更したりする。
- 現在の技術と新しい技術に関してスタッフ教育または専門的能力の開発を継続的に行う。
- スタッフ研修プログラムを導入する。
- 適切な情報リソースへタイムリーにアクセスできるようにする。
- 適切な技術カンファレンスへのスタッフの参加を奨励する。
- 管理職、法律顧問、および法執行機関（または必要に応じて他の関係者）との継続的な協力体制を確保する。
- サービス定義、ポリシー、および手順は、変化や予期しない状況が生じることを見込むことも、許容することもできないほど厳格にならないようにする。

これらの課題の大部分については、4.2 節「基本的なポリシー」で詳しく説明します。

CSIRT は予期しない出来事が生じた場合でも、動的な環境変化に適応できる柔軟性を持つ必要がありますが、そのような出来事に対してチーム全体の目的や運営スタイルと矛盾しない方法で対応する必要があります。柔軟性がなければ、CSIRT のガイドラインは一般的過ぎて助けにもガイダンスにもなりませんし、また限定的過ぎて予期しない出来事に適応することもできないでしょう。

CSIRT のミッションと運営方法に、Constituency との接し方にも影響を及ぼすような変更が生じた場合は、そのような変更を Constituency に伝える必要があります。

例：CSIRT がその運営方法を変更して、以前は他の資金調達モデルに基づいて Constituency に提供していたサービスを有料化するとします。このような場合、CSIRT はその旨を Constituency に通知するために適切な手段を取る必要があります。

## 2.7.2 法律の問題

本書の執筆者はいずれも法律の専門家ではないため、この分野では自分たちの経験や自分たちが目にした他者の経験について意見を述べることはできません。ここでは、検討するに値すると考えられる問題に注目することにします。読者は法律顧問と相談して、それぞれの状況に当てはまる問題を明らかにする必要があります。

CSIRT にとっては、法的助言が得られることが重要です。そうでなければ、チームはそうとは知らずにチームの廃止につながりかねない不適切な活動や違法行為を行ってしまう可能性があります。法的助言が簡単には得られない小規模なチームは非常に不利な立場にあります。少なくともサービスの開始前や、ポリシーまたは運営手順を大きく変更するときには、可能な限り法的助言を求める必要があります。

法律問題は品質保証に少し似ています。ミッションステートメントから運営手順まで、ほとんどすべてのテーマに広がっているからです。品質保証との比較では、興味深い違いもあります。品質保証は「これをしろ、あれをしろ」というものであるのに対し、法律問題は多くの場合、スタッフ、チーム、または組織が責任を問われる可能性のある不適切な言動を「回避すること」を中心に検討します。もちろん、安定した法的な立場を保証することは、単に何かをしないということだけのものではありません。証拠となりうるもの（ログファイルや他のアーティファクトなど）に適切な日付があり、その真正性が証明されたものであることを確認するなど、積極的な行動も要求されます。

全体的な枠組みを定義して測定基準を設定することが有効である品質保証と異なり、法律問題で同じことは現実には困難です。実際のところ、法律問題は、テーマや分野が当てはまるたびに取り組むのが普通です。これは、主要な活動がインシデントハンドリングであり、司法ではない CSIRT にとって、悪いアプローチではありません。法律問題は境界条件であり、徹底的な、ただし現実的な方法でしかるべく対処する必要があります。しかし、計画性のないアプローチでよいと

ということではありません。何人かの決まった法律顧問に協力してもらうなどして、全体を見渡せるようにしておくべきです。この観点から見れば、よく使われる「法的助言」という表現よりも、「法律問題管理」という表現の方が好ましいと思われる。

組織の問題は法律問題と似ています。ただしこの場合、国内法または国際法は、CSIRT が所属する組織を支配している「法律」すなわち規則と置き換えられます。これらの規則を順守する必要があることは言うまでもありません。最大の違いは法的責任で、組織の規則に違反することが組織に法的責任を負わせることにならない限り、組織の場合には法的責任は問われません。

この節の残りでは、CSIRT の観点から法律問題の管理について述べ、法的責任に関する重要事項であり、且つ法的責任を問われる主な原因である情報の開示に重点を置きます。

### 2.7.2.1 法律問題の管理

CSIRT チームがかかわる法律問題の管理とは、チームが直面する法律問題に関して一貫した見解を示すということです。法的助言は、その分野での経験があり、CSIRT の日常業務の基礎となる専門用語や問題を理解している何人かの決まった人々（大部分は法律専門家）から得るようにする必要があります。このような人々（通常は数名で、1名の場合もある）は、協力して一貫した共通の見解を持つ必要があります。助言者に必要な特定分野にかかわる知識の量を軽視することはできないため、長期に渡って（数か月ではなく数年）法律顧問の協力を得ることが重要です。顧問が1名しかいない場合は特にそうです。代替りの顧問が現状に追い付くには、早くても数か月はかかります。非常に現実的な解決策は親組織の法律顧問に協力してもらうことですが、特有の問題について指導できる十分な経験がある場合に限りです。この場合も継続性を保証する必要があります。法務スタッフがそのニーズに適していない場合は、実現可能ならば、固有の要件に適した弁護士に依頼するか弁護士を抱えておくほうが賢明かも知れません。

法律顧問が必要とする経験の種類は、以下のテーマ領域から導き出すことができます。以下は、法律顧問が検討し、助言する必要がある事柄の例です。

#### 契約書の分析

すべての契約書、特に顧客との契約の法的妥当性をチェックする必要があります。これには、法的に意味のない、拘束力のない、あるいは明らかに間違っただけでなく、CSIRT にとって法的に悪影響を及ぼす可能性のある漏れを見つけることも含まれます。

#### サービス定義と品質保証

Constituency に対して「売る」（保証する、約束するなど）のはサービスです。当然ながら、サービスとその品質保証をどのように定義したかについて、Constituency によって責任を問われます（特に物事がうまく行かなかった場合）。そのため、サービスとして何をうたうにしても、法的に妥当でなければなりません。

## ポリシーと手順

ポリシーと手順には制裁などのかなり積極的な措置を伴う記述も含まれているため、法律上の落とし穴がないかどうかチェックする必要があります。このような措置は、他の法律に違反する危険性を必ず内在します。以下の例は、CSIRTのポリシーと手順に関する事前の法的助言が効果を発揮する状況を明確にするのに役立ちます。

例：ポリシーに、開示ポリシーに違反した場合は解雇すると書かれていたとします。これは地域または組織の法律に抵触する可能性が高いです。従業員の解雇がそれほど問題にならない国もあれば、非常に困難な国もあるためです。

例：Constituency との極秘データのやり取りは暗号化された方法でのみ行うということを手順の中に記述したとします。Constituency が問題を抱えており、データを FAX で送信してほしいと言われたらどうでしょう。拒否した場合、それがどのような正当な理由だったとしても、自分たちの手順を順守することはできますが、Constituency に対するサービス目標を達成できるのかわくは疑問です。暗号化が法的要件なのか、それとも単に望ましい実施方法なのか、事前に分かっているのが理想です。

例：上記の例の別の事例として、暗号化通信に対応するつもりがまったくなく、必要なツールも保有していないにもかかわらず、Constituency が極秘情報を交換したいという場合もあります。

## 権利放棄と免責条項

免責条項は、サービスの詳細説明、ポリシー、Web サイト、発信する電子メールなど、多くの場所に見られます。すべての免責条項について法的妥当性をチェックするか、あるいは、少なくとも法的な目的を持たせるべきです。これがない場合は、免責条項を削除するべきです。一方、判例法で妥当性が証明されている免責条項は追加することもできます。判例法によって追加された免責条項の逸話があります。それは、ずぶぬれで家に帰ってきた小犬を電子レンジで暖めてしまったという、驚くような話です。その犬が死に、電子レンジメーカーは法廷で責任があるという判決を下されました。この判例のために、メーカーは電子レンジの取扱説明書にいくつかの適切な文言を追加しました。少なくとも、その逸話ではそういう話になっています。

例：手荷物預かり所や他の場所の張り紙で、かくかくしかじかには何か問題が起こっても（コートを盗まれるなど）一切責任はないと書かれているのをよく目にします。これは簡単な逃げ道のように思われますが、たいてい、弁護士はそのような文言を笑い飛ばし、決めるのは裁判官だと言います。しかし一方で、これらの免責条項がまったく役に立たないわけでもありません。免責条項がそこになかったら、配慮が足りなかったとして立場がさらに悪くなるからです。

CSIRT では、CSIRT の法的責任を何らかの方法（例えば「ベストエフォート」、  
「適切な配慮」または「業界標準」）で限定するための権利放棄書に署名するよ  
う顧客に要求することがあります。法律顧問は、CSIRT がそのような権利放棄を  
最も適切に利用できる範囲の提案を行うことができると思われま。権利放棄書  
の作成にあたっては免責と同様の見直しを行い、注意を払う必要があります。

### 秘密保持契約

CSIRT のスタッフは、CSIRT に入るときと辞めるときに、秘密保持契約  
（NDA : Non-Disclosure Agreement）への署名が義務付けられていることがあり  
ます。その場合、CSIRT 業務の詳細を共有する非常勤スタッフや訪問者にも同じ  
NDA が必ず適用されます。清掃員や警備員などにも適用されることがあります。  
しかし秘密保持契約を作成し、署名させるだけでは、法的に無効な場合もありま  
す。まず署名者が NDA の対象範囲を理解していなければなりません。そして  
NDA を実装する前に、法律顧問に見直してもらい、文言が適切か、組織のポリ  
シーに適合しているか確認してもらう必要があります。法律家による見直しと承  
認がなければ、NDA は単なる心理的な保護手段に過ぎなくなり、裁判所におい  
て効力を有しない可能性があります。

### 事前対策

法執行機関が CSIRT に対して情報を法的に要求してきたと仮定します。CSIRT  
は、そのような事態やその後に起こるかもしれないことに備えていますか？ ま  
た CSIRT が賠償訴訟に召喚されたとしたらどうでしょう。訴訟に対応できるよ  
うに準備していますか？ そのような場合に備えるには、2つのことが前提とな  
ります。

- （サービス仕様に）明言した方法で職務を遂行し、「しかるべき注意」を払  
います。「しかるべき注意」の意味は地域の法律によって異なるため、法律  
顧問に相談してください。
- 妥当な範囲で、ワークフローにおける重要なイベントの全てと、インシデン  
ト発生時のワークフローを文書化し、タイムスタンプを付加します。

例：CSIRT がログを特定の期間だけ保存し、その旨を公表しており、これを  
不可とする法律がない場合、その期間が過ぎた後にログを入手できないとし  
ても、誰も文句を言うことはできません。一方、逆の場合を考えます。特定  
の期間後に監査によって、データがかなり早い時期に削除されたことが分か  
ったとします。これは賠償訴訟の理由になる可能性があります。

2番目のポイント（文書化とタイムスタンプ）は事前対策が有効に働くところ  
です。法律顧問は CSIRT のニーズを支えるアプローチに対して見解を示したり助  
言を提供したりする必要があります。基本的にその作業は、CSIRT のイベント  
（特にインシデント）を文書化する最低水準を明らかにすることであり、またこ  
れを実行する正しい方法を明らかにすることです。「最低」とは、法律で規定さ  
れている水準、および明らかに訴訟で要求される（または有用な）可能性がある  
水準を意味します。「それを実行する正しい方法」とは、訴訟で資料を法的に要  
求されたり調査されたりしたときに、（設定されている目的の範囲における）完  
全性、ロジック、および信頼性に対して高い評価を得られる方法で証拠（文書、

ログ、保存記録など)を収集する必要があるということです。これは簡単に聞こえますがそれほど簡単ではありません。分かりやすい例をひとつ示しましょう。

例：Dutch 事件（州対 Ronald O.、1993～5）では、侵入事件の容疑者が裁判にかけられ、検察官が提出した証拠には一連のログが含まれていました。ログには元のページ番号が付けられていましたが、いくつかのページが欠けていました。それらのページは、関係するデータが含まれていなかったために、ログを提供した関係者がずっと以前に廃棄していました。ページが欠けていたために、被告側は証拠の提示が差し控えられていると主張しました。判事は被告側の抗弁を却下しました。しかし、有力な証拠（ログファイル）の扱い方がもっとよければ、この問題は起こらなかったはずでした。

記録を保存しておくことは弁護士を雇うよりも安く済むので、すべてのデータを保存するよう助言する人もいます。また、機密情報は、たとえ要求されても提出できないように、できるだけ早く処分するように忠告する人もいます。チームに適した解決策は、チームのミッションのほか、チームが置かれている司法管轄によっても決まります。法的利用の可能性があると理由でデータを保管する場合は、情報の保管に適した記録媒体を使うことを検討してください。CD-ROM やマイクロフィッシュ／フィルムのような記録媒体は、一度作成すると簡単には偽造されず、比較的 low コストで作成できます。CSIRT がどのようなアプローチを取ったとしても、この分野では適切にスタッフを指導する必要があります（法執行機関が CSIRT の設備を押収する場合の対応方法など）。

### 2.7.2.2 法的責任

法的責任問題とは、発言、行動、記述をすること、またはしないことに対して、人がある程度裁判で勝てる見込みを持った上で訴訟を起こそうとする可能性のあるものすべてです。米国のように、賠償訴訟の件数が多く、またその結果としてしばしば課せられる膨大な罰金のために、会社全体が容易に破滅しかねないことを考えると、訴訟は重大な懸念の理由になります。他の多くの国々では、運営で大きく失敗し、Constituency などの他の関係者に損害を与えない限り、法的責任はあまり問題になりません。

法的責任の問題はこのように地域の法律に大きく依存しており、本質的に法的な問題であるため、この問題に関しては法律顧問に相談する必要があります。法的責任を回避するには、先を見越した取り組みが必要です。必要とされる取り組みの種類は、状況に応じて異なることがあります。CSIRT が Constituency と交わした署名済みの契約書の内容に起因する法的責任（例えば、サービスの可用性が欠如しているために、サービス定義に即したサービスを提供できないなど）から、情報開示や不作為に関する法的責任まで多岐に渡る可能性があります。表 9～11 の例で、これらの多様な状況に起因するさまざまな問題について説明します。

表9：不作為に起因する法的責任問題の例

法的責任の範囲：不作為	
問題	例
情報開示の不足	侵入者の活動を示すログファイルを受け取ったにもかかわらず、その手掛かりを徹底的に追求しなかった。その事実が明らかにされた場合、情報に従って行動しなかったことについて責任を問われる可能性がある。
副次的な影響を忘れている	特定のインシデントで「新しい」脆弱性に対応したが、その脆弱性をベンダおよび／または他のチームに報告するのを怠った。それから1か月後、同じ脆弱性が攻撃されたためにインターネットが停止した。
法によって求められる報告またはファイル保管義務を認識していない	多くの国では、（故意の）殺人などの重大犯罪が伴う場合がある事件に関して、法執行機関に報告したり、保存記録を作成したりする義務がある。これは機密扱いの政府システムへの侵入などの犯罪にも適用される。

表10：署名済み契約の内容に起因する法的責任問題の例

法的責任の範囲：署名済み契約の内容	
問題	例
不適切なサービス定義	休日の間または限定的な理由により、サービスが利用できない。そして、そのことが契約の中に適切に記載されていない、あるいは「休日」の意味を定義していない。その期間中に Constituency が侵入行為に遭い支援を求めたが、サービスを利用できなかった場合、Constituency が訴訟を起こす可能性がある。
定義されたサービスレベルパラメータが達成されていない	Constituency にオンラインサポートを約束したが、（何らかの理由で）Constituency が緊急事態のときに利用できなかった。
定義された品質パラメータが達成されていない	営業時間外に Constituency が緊急支援を要請したときに、約束した応答時間に対応しなかった。このような状況で Constituency に金銭的損失があった場合、その一部の弁償を求めるのはもつともであり、職務に関係のない口実は受け入れられない。

表11：情報開示に起因する法的責任問題の例

法的責任の範囲：情報の開示	
問題	例
個人または組織への言及	ある団体が進行中の攻撃に関与しているという印象を与える。これはその団体の評判や事業に損害を与えるおそれがある。
身元の口外	この場合、法的責任を問われるかどうかは情報を要請した人によって異なる。（事前の同意なしに）被害サイトの身元を他の被害者、法執行機関、またはメディアに口外すると、責任を問われる可能性がある。しかし、同じ情報を内部監査に報告するように義務付けられている場合は、責任を問われないこともある。
誤った情報の配布	オペレーティングシステム XYZ の重大なバグに関する情報を配布したが、これが誤った情報であると判明した。XYZ のベンダは快く思わないかもしれない。
	ある問題について誠実に通知したが、うまくいかない解決方法をアドバイスした。うまくいかないことが自明ではなく、そのために損害が生じた場合は、責任を問われる可能性がある。
不適切なアドバイス（不完全、古い、または単なる間違い）	いくつかの問題を解決するためにファイアウォールを修正するよう Constituency にアドバイスしたが、その解決方法によって LAN に他のセキュリティ問題が生じた。
	CSIRT に公開された情報源から、より優れた情報が既に入手できるのに、ひどく古い情報を Constituency に提示した。チームメンバーは単に把握していなかったただだったが、Constituency はこれにより損害を被る可能性がある。

この場合もやはり法的責任を極力抑える方法には、明白な答えがあります。職務を正しく遂行し、文書化することです。何をすべきかについては、既に数多く述べました。しかし、法的責任とその結果に対抗する構造化されたアプローチを以下に提示します。

- 法的に「安全な」表現を用いた標準契約を使用します。
- サービス定義、サービス品質のレベル、およびポリシーから、不正確、達成が困難（または不可能）、または法的に不明確な記述をすべて取り除きます。
- 法的に妥当な免責条項を作成します。
- ワークフロー、ポリシー、および手順を定義します。また、運営中にしかるべき注意を払っていることをいつでも証明できるように、適切な文書化プロセス、施行プロセス、および管理プロセスを導入します。
- リスクがコストを超える場合は、サービスに保険をかけます。
- CSIRT が特定の義務または顧客や他の CSIRT に与えた損害に対する責任を問われるのを制限・回避するために、権利放棄の利用を検討します。

### 2.7.2.3 情報開示

情報開示は、CSIRT に法的責任が生じる可能性が最も高い分野です。情報開示は、報告や勧告を作成することだけではありません。電話でアドバイスするのも情報開示です。こうした「予測できる」開示だけでなく、予測できない開示もあります。

- 裁判所の命令



- CSIRT（信頼できる専門家、現従業員、または元従業員）からの情報漏えい
- （物理的な、またはネットワーク経由の）侵入によって取得した情報

法的責任につながるいくつかの情報開示の例については、前の節で既に説明しました。しかし法的責任に関するこれらの事例がきわめて深刻であり、膨大な損害賠償請求を伴う可能性があることはいくら強調しても強調し過ぎということはありません。予測可能かどうかを問わず、情報開示によって起こりうる影響に関して興味深い例を以下に示しますので、これで理解が深まると思います。

例：ある Constituency に関する機密情報が漏れたり、配慮なく公表されたりすると、Constituency のサイトのセキュリティ、評判、または事業が深刻な危険にさらされるおそれがあります。

例：あるサイトが捜査の対象となっているときに、別のサイトから関連するアラートがその疑わしいサイトに与えられたり漏れたりした場合、それが容疑者を警告することになり、捜査が妨げられる場合や台無しになる場合さえあります。多くの場合、CSIRT は進行中の捜査について知ることができませんし、当然予期したり、制御したりできるような状況ではありません。CSIRT は適切な権利放棄によって、そのような状況にさらされることを制限できます。

情報開示によって法的責任が生じないようにするには、主として（前述したように）しかるべき注意をしていることをいつでも証明できるようにワークフローと手順を管理することです。明らかに、情報開示ポリシーは制限的なタイプでなければなりません。言い換えれば、このポリシーでは、情報を知る必要がある場合にのみ開示するという原則で配布すると述べる必要があります。

ほとんどの場合、CSIRT では情報を開示する条件を定義しています。しかし、CSIRT は組織、地域、または国際的な（法執行機関や Forum of Incident Response and Security Teams [FIRST] のような団体などとの）関係によって強制的な報告要件が課される場合もあります。要件とその結果は CSIRT による情報開示に影響を与え、CSIRT が法的責任を問われる可能性があるため、明確に理解する必要があります。最も一般的な例としては、CSIRT は内部監査人からの報告要求には従う必要がありますが、外部監査人からの要求に応じることは、CSIRT が運営されている司法管轄によって義務であるかどうかが決まります。

### 2.7.3 組織の規制

地域の（および国際的な）法律のほかに、CSIRT は親組織固有の規制に従って活動する必要もあります。これらの規制を法律として見なすと、前述の推奨事項のほとんどはこの場合にも当てはまります。チーム自身の法的責任は、最小限であるかまたは問われないこともあります（組織固有の規制に違反した場合のリスクは比較的小さいものです）。ただし、これらの規制に違反すると、親組織が責任を問われる場合があります。そのため、この場合も上記と同じであり、親組織に対応しなければならないという複雑さが加わるだけです。リスクが大きい場合は、CSIRT を別法人などにして法的に分離してもよいでしょう。この分離によって、

リスクをコントロールしやすくなります。ただし、親組織内にある他の部署とやり取りしようと試みると、CSIRTに他の問題が生じる可能性もあります。

組織の規制には、次のようなものがあります。

- 米国エネルギー省 (DoE) の規定 (例えば、DoE の CSIRT である CIAC はこれらの規定に従います)
- 社内の規定 (金融機関や大企業の規定など)
- 軍の服務規定
- 国際的な監査基準
- その他の連邦規制または国内規制



---

## 3 インシデントハンドリングサービス

前の章では、各 CSIRT に関わる基本的な問題について概説しました。次に、インシデントハンドリングサービスに関連する必須の問題を詳しく述べます。この章では、インシデントハンドリングサービスの基本要素と、それらを支えるための適切な手順について説明します。

また、この章の構成でもうひとつ注目すべき点は、サービスに関するどのような説明にも少なくとも 2 つの側面が必要だという点です。

- **仕様——論理的側面**  
サービスとその機能の目的および構成に関する説明 (3.1～3.2 節)
- **施行——技術的側面**  
指定された機能を指定された方法で施行するための実際のツール、手順、および役割の組み合わせ (3.3～3.8 節)

最後に、インシデントハンドリングサービス（さらに言うとあらゆる CSIRT サービス）の 2 つの一般的な特徴、すなわちやり取り (3.7 節「やり取り」と情報のハンドリング (3.8 節「情報のハンドリング」) について説明します。

### 3.1 サービスの詳細

CSIRT が提供するサービスは明確に定義する必要があります。どの定義も、CSIRT および CSIRT とやり取りする関係者に周知され理解されなければなりません。これらの定義は、さまざまなレベルで抽象化できます。2.2 節「サービスと品質の枠組み」で述べたように、CSIRT が提供するサービスごとに、そのサービスの詳細を詳述することが重要です。この節では、インシデントハンドリングサービスの詳細を作成するときに考慮すべき事柄について述べます。

以下の項目は、CSIRT のサービスの詳細を記入するテンプレートとして使用できるように論理的な順番に並べています。ただし、CSIRT 以外 (Constituency など) に提供する説明を考える際には、IETF ワーキンググループによる

「Guidelines and Recommendations for Incident Processing」 (GRIP) [RFC 2350] を参照することをお勧めします。また、TERENA Task Force の最終報告「CERTs in Europe」 [TERENA 1995] にも、技術的な観点から見た (資金問題は除く) いくつかのサービスレベルの説明例があります。

### 3.1.1 目的

ポリシーと手順の策定を容易にするために、CSIRTはその目的を明確に定義する必要があります。例えば、トップダウン式を進めると、インシデントハンドリングサービスの目的はCSIRTのミッションステートメントから導き出され、そのミッションステートメントはセキュリティチーム、親組織、または他の後援組織のミッションから導き出されます。CSIRTの目的に従って、それらを実現するための適切な機能の範囲と程度を定義することができます。表12に、ミッションの異なるさまざまなチームの、考えられるサービスの目的をいくつか示します（サービス目的を網羅したリストではありません）。

表12：チームのタイプ別に考えられるインシデントハンドリングサービスの目的の範囲

CSIRTのタイプ	ミッションの特徴	考えられるサービスの目的
国際的なコーディネーションセンター	他国のCSIRTと連携することにより、コンピュータセキュリティの脅威に関するグローバルな観点でのナレッジベースを獲得する。	世界中の他のCSIRTと連携して、コンピュータセキュリティインシデントに対する技術的支援を提供する。 インシデントハンドリング活動を通じて、現在または潜在的な侵入脅威に関する技術的詳細を追求して文書化する。 侵入脅威の検知、防止、復旧に関する情報を作成して開示する。
国のチーム	コンピュータセキュリティの脅威に関する国の対外連絡窓口を維持し、国内のシステムから行われたセキュリティインシデントおよび、国内のシステムを標的としたセキュリティインシデントの数を低減する。	コンピュータセキュリティインシデントに対する技術支援をその国の言語とタイムゾーンで提供する。 脆弱性を検知、防止、および復旧するための技術情報を提供する。 国内の法執行機関に対する連絡窓口としての役割を果たす。
ネットワークサービスプロバイダチーム	顧客のネットワーク接続のためのセキュアな環境を提供する。コンピュータセキュリティインシデントに関して効果的な対応を顧客に提供する。	コンピュータセキュリティインシデントに対する技術的支援を提供する。 ネットワークインフラのセキュリティを確保する。 国のチームなどへの連絡窓口としての役割を果たす。
ITベンダ	製品のセキュリティを向上させる。	脆弱性に対する技術支援を提供する。CSIRTと協力して、インシデントの原因を分析する。 新しいパッチや現在のベストプラクティスに関する注意喚起を作成し、一般に公表する。
企業のチーム	社内の情報インフラのセキュリティを向上させ、攻撃や侵入による損害の脅威を最小限に抑える。	インシデントハンドリング支援のための総合的拠点を社内のシステム管理者、ネットワーク管理者、およびシステムユーザに提供する。 社内のシステムに影響を及ぼすインシデントに対してオンサイトの技術支援を提供し、侵入脅威や攻撃を隔離して復旧する。

### 3.1.2 定義

インシデントハンドリングサービスをどのように実施して目的を達成するかを記述するには、利用可能なリソースに基づいて、提供すべきサービスの範囲と深さを理解することが重要です。まず、提供できるサービスレベルの制約となる事柄を明らかにすると良いでしょう。提供するサービスは、サービスに規定された目的だけでなく、チームが利用できるリソース（物理的リソース、資金、専門知識）と **Constituency** に対するチームの権限範囲によっても制約されます。現在では多種多様なインシデントハンドリングサービスが存在しています。そこで以下に例として、さまざまなサービスがさまざまな制限要因によって制約を受けている中で、どのようにすれば重要な役割を果たし、目的を達成できるかを示します。

例：最も一般的な制限要因の1つが資金であり、サービスを実施するスタッフの配置と物理的リソースに影響を及ぼします。しかし、最近のセキュリティチームの多くは、トリアージ機能、ハンドリング機能、およびフィードバック機能（3.2節「サービス機能の概要」を参照）の単純な仕組みをすべて組み合わせた最小限のインシデントハンドリングサービスを1つの「サービス」として提供しています。

例：国、組織、およびサービスプロバイダレベルで、資金が制限されているCSIRTは、詳細な支援やオンサイトの支援は行わずに、すべての **Constituency** との間で活動の連絡調整を行うことに専念します。このようなチームは **Constituency** との一元的な連絡窓口になり、インシデントの影響を受ける関係者にインシデント情報を直接伝達することで、信頼できる仲介者としての役割を果たします。

例：逆に、何人ものスタッフを雇う資金はあっても、必要な深い専門知識のあるスタッフの勧誘、確保、あるいは訓練ができないCSIRTもあります。そのような状況では、チームはすべての機能を備えた包括的なインシデントハンドリングサービスを自力では提供できない可能性があります。深い専門知識が不足していると、綿密なハンドリング機能を提供できません。つまり、インシデントが技術的にどのようなものなのかを十分に把握できないからです。この場合、**Constituency** 内で利用・開示するための情報を得るために、チームは技術に精通した他のチームがまとめた情報に頼らざるを得ません。このようにチームの活動範囲が制限されている、例えば他のチームのサービス結果に依存しているなどの場合、サービス機能を単なる情報の中継に下げることになります。

利用可能なリソース、制限要因、既存の組織構成で利用できる仕組み、および達成しようとする目的を理解することで、インシデントハンドリングサービスを定義することができます。そのために、提供できるサービスレベルの境界を定め、サービスの提供に必要な一連の機能に対してそのサービスレベルを課します。

同じ基準と定義を基に、サービスの説明書を2つ作成するのがよい場合もあります。1つは外部向けのもので、サービスを利用できる **Constituency**、サービスを依頼する方法、または顧客が期待できるCSIRTサポートなどの情報を提供します。もう1つは内部向けのもので、外部向けの説明書（誰が、どのような方法で、

何を)に加えて、サービスを実施するための内部の実施方法と、CSIRT内でのサービスの管理方法に関する具体的で詳細なガイダンスが含まれます。後者は、例えば、情報を追跡・記録する方法、対象機能の責任者、依頼に対する優先順位の付け方、およびサービスの範囲内で実際に顧客に何を提供するか決定方法などが含まれます(例えば、インシデントの現状、経営陣の指示、顧客の資金に応じて、提供するサポートを増やしたり減らしたりすることが考えられます)。この観点から考えると、外部向けの説明書は、実際には内部向けの説明書の副産物として、あるいは一部として作成するべきです。Constituencyの種類に応じて、文章全体を外部用書き換えて、CSIRT分野の専門家でない人にも理解できるようにしたり、サービスレベルサポートが期待されるやり方から変化したときのために背景情報を補足したりすることもあります。

### 3.1.3 機能の詳細

インシデントハンドリングサービスには一般に、報告、分析、および支援が含まれます(表4のサービスリストを参照)。さらに詳細に記述して、4つの主要な機能、すなわちトリアージ、ハンドリング、アナウンス、およびフィードバックを含めることができます。これらの機能については、3.3節「トリアージ機能」から3.6節「フィードバック機能」で詳しく説明します。トリアージ機能はベテランの秘書のようなもので、受け取った情報を見て判断し、適切な担当受付(つまり機能)に渡します。他の機能は一目瞭然なので、この段階では詳しく紹介する必要はないでしょう。

これらの(または追加の)機能のそれぞれについて、CSIRTの内部向けに、明確な説明を文書化するべきです。これらの説明は、関連する手順を作成するときに役立ちます。個々の説明は、サービスを利用する関係者に公開されるサービス全体の説明のうち、機能以外の要素を構成するために使われます。しかし、他のさまざまな実装の詳細は、チームにとっては重要であっても、外部関係者を単に混乱させる可能性もあるため、通常はチーム外部へ公開しても意味がありません。

機能の定義には、少なくとも以下の情報を含める必要があります。

- 機能の目的
- 実装の詳細と、対応する手順へのポイント

例：その機能は、内部のアクション(つまりCSIRT内の別の機能やサービス)によって発動するものなのか、あるいは外部(つまりConstituencyや他の関係者)によって発動するものなのか？ その機能はどのようにして発動され、利用されるのか？ どのような形態(電子メール、電話、報告など)を取るのか？ その機能は、利用者からどのようなデータを要求するのか？ または利用者にどのようなデータを提供することが求められているのか？ イベントのライフサイクルはどのくらいか？

- 機能内で使われる優先順位の基準
- 提供するサービスのレベル
- 期待値の設定および使用する品質保証基準

### 3.1.4 可用性

サービスの可用性を定義するには、「誰が誰にいつ連絡できるのか」だけでなく、「どのような条件で」という質問への回答も必要です。

- **誰がサービスを利用できるか**

そのサービスには、公表 Constituency に限定されている側面（インシデントに関するアナウンスや技術支援など）と、より幅広い層の人々が利用できる側面（公表 Constituency に影響を及ぼすインシデント報告は誰からでも受け付けるなど）があるか？

- **サービスを利用できる時間**

時間帯によって利用できるサービスのレベルが異なるか？ 例えば、フィードバック機能は営業時間中の規定された時間帯でのみ利用できるのに対し、ハンドリング機能は営業時間中いつでも利用できる、あるいは、インシデントの全部または一部の種類については 24 時間 365 日利用できる、または Constituency の一部だけが利用できるなどが考えられます。

- **サービスを提供する条件**

例えば、チーム指定の報告用フォームを使い、必須項目が記入されているもののみインシデント報告として受け付けるのか、などです。

### 3.1.5 品質保証

サービスの利用者に対しては、サービスを利用するにあたって期待できる品質レベルがどこまでであるかが分かるような情報を提供しなくてはなりません。また対象に応じて、期待できるレベルを変えることができます。例えば、資金提供者と公表 Constituency に対しては、他に対するよりも高いレベルの品質を提供できます。その場合、サービスによって何が提供され、サービスから何が除外されるかを明確にしなくてはなりません。またサービス利用者が、通常どれくらいの時間枠で対応してもらえると期待してよいのかを示すことも有効です。さらに CSIRT は、提供する各種の情報のハンドリングに関して、サービス利用者が CSIRT に何を期待できるのかも示さなくてはなりません。なお、期待値の設定は、そのサービスの優先順位付けの基準と整合していません。

### 3.1.6 やり取りと情報開示

サービス利用者は、CSIRT とサービスの対象となっている関係者との間でどのようなやり取りが発生するか、また情報（開示）がどのように取り扱われるかを把握しておく必要があります。例えば、サービス利用者は、インシデントの間にチームに提供したアーティファクトやログファイルに対して何が行われると期待してよいのでしょうか？ アーティファクトやログファイルは、他のチーム、ベンダ、または専門家と共有されるのでしょうか？ また、その場合、どのような条件下で情報の転送が行われ、情報はどのようにしてサニタイズされ、保護されるのでしょうか？ これらの問題については、3.7節「やり取り」と3.8節「情報のハンドリング」、特に3.8.8節「情報開示」で詳しく述べます。



### 3.1.7 他のサービスとのインタフェース

インシデントハンドリングサービスと、やり取りする他のサービスとの間の CSIRT 内における窓口と情報流通の基準は、チームが他にどのようなサービスを提供しているかによって異なります。例えば、トリアージは多くのサービスに共通しており、たいていは複数のサービスに対して1つのトリアージ機能が提供されます。

### 3.1.8 優先順位

サービスの各機能内のイベントに優先順位を付けるだけでなく、サービスを構成する機能間の相対的な優先順位や、インシデントハンドリングサービスと CSIRT が提供するそれ以外のサービスとの間の相対的な優先順位を付けることも重要です。相対的な優先順位は、チームとそのチームが提供するサービスの全体的な目標と目的を反映したものになります。リソースが限られている場合は、通常ハンドリング機能がフィードバック機能やアナウンス機能よりも優先します。これは、チームがインシデントの劇的な増加に直面しているときに、それに応じたスタッフの増員ができない場合も同様です。どのような状況が起こっているかによらず、ハンドリング機能に専念すると、他の活動に利用できるリソースがほとんど残らないことは *Constituency* にも明らかです。

ただし、トリアージはハンドリング機能が効果的に機能するための前提条件です。そこで、すべてのフィードバックとアナウンスについて *Constituency* に随時情報提供できるように、水準を下げて限定的なトリアージを行うことも考えられます。チームが通常の運用状態に戻ることができるまで、詳細なトリアージはハンドリング機能に重点を置きます。そうすることで、他の依頼者には現在の運用状況を説明して、情報を随時提供できるようになります。

優先順位付けに関する問題は、3.8.6節「優先順位付けの基準」で詳しく説明します。

## 3.2 サービス機能の概要

前述したように、インシデントハンドリングサービスには通常、サービスの提供を支える他の活動も含まれており、トリアージ、ハンドリング、アナウンス、およびフィードバックの4つの機能で構成されています（図4を参照）。これらの機能とその関係については以下で説明し、次の4つの節でさらに詳しく取り上げます。

図4に示す機能仕様に対応した CSIRT は現在数多く存在していますが、その実装方法には大きな違いがあることを理解することが重要です。その違いは、資金、利用できる専門知識、または組織構造などの要因によって生じます。このような違いの一部については、3.1.2節「定義」で論じました。

例：小さなチームでは、サービス機能を1つ1つ区別できないこともあります。（必要なスキルセットを持つ）ある一人の担当者が、一定期間サービス

機能を提供し、その後で別のチームメンバーに対応を引き継ぐことがあります。大きなチームでは、トリアージ機能とフィードバック機能の処理には技術スキルの高くないスタッフで構成されるヘルプデスクを設置し、ハンドリング機能は技術スキルの高いスタッフに任せることがあります。

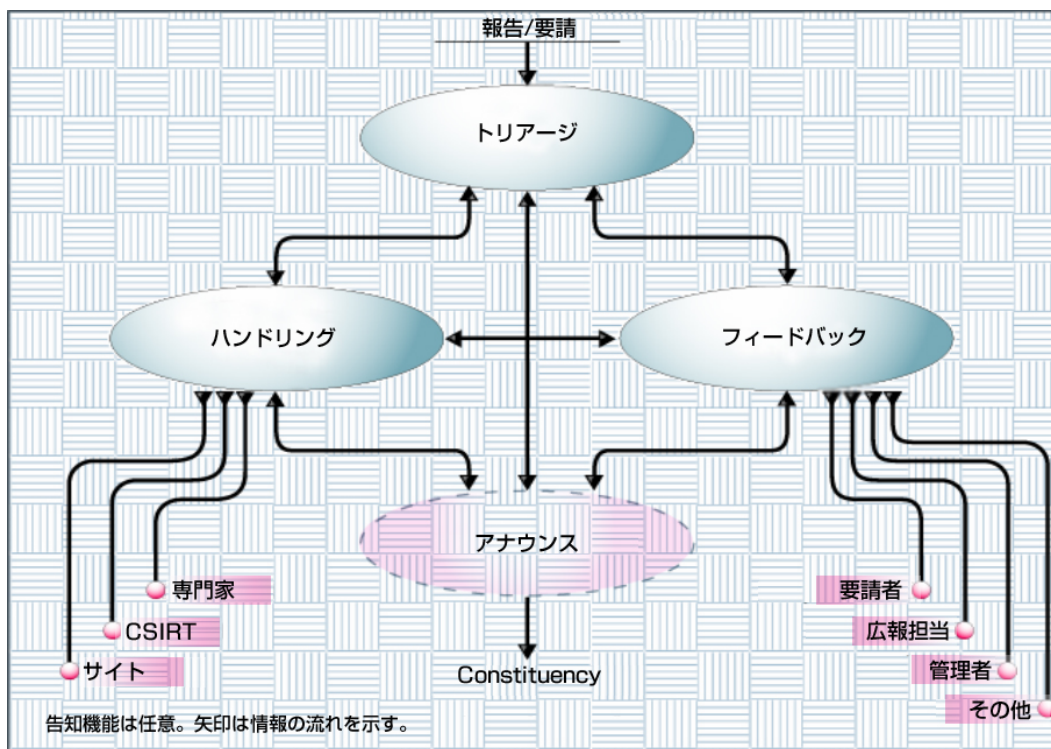


図4：インシデントハンドリングサービスの機能

#### トリアージ機能

トリアージ機能は、サービスが受け取る情報の単一の共通連絡窓口であり、情報の受け付け、収集、分類、順序付け、および受け渡しの拠点でもあります（3.3節「トリアージ機能」を参照）。さらにこのトリアージ機能は、外部向けのすべての（発信）情報が渡されるチャンネルになることもあります。この機能は、チームと Constituency のニーズに適したさまざまな入力チャンネルをサポートします。新規イベントと思われるイベントには、初期の優先順位と、場合によってはイベントに関連付けるトラッキング番号（トラッキング番号）が割り当てられます。トリアージ機能の一部として、その後のインシデントハンドリング活動を容易にするために付加的な活動（記録保存、翻訳、またはメディア変換など）を行うこともあります。

#### ハンドリング機能

ハンドリング機能は、疑わしいまたは確認済みのセキュリティインシデント、脅威、および攻撃に関する支援とガイダンスを提供します。この機能にはいくつかの異なる活動を含むことがあります。報告（インシデント報告など）の精査は、何が起きたのか、またはどのような活動がかかわっているのか、あるいはその両方を判断するために行われます。報告の分析には、誰が関与しているのか（誰に連絡をとる必要があるか）や、どのような支援が要請/提供されているのかを明

らかにするために、補足の証拠や資料（ログファイルなど）の精査が含まれることがあります。チームは（CSIRTのミッション／目標／サービスに合った）適切な対応を明らかにし、報告者や Constituency に対する実際の通知やフォローをする必要があります。このハンドリングについては、3.4節「ハンドリング機能」で詳しく説明します。

### アナウンス機能

アナウンス機能は進行中の脅威に関する詳細、それらの脅威から身を守るために取りうる手順、またはチームに報告された最近の攻撃の範囲と特徴に関する動向情報を、好ましくない部分を削除して、Constituency に合わせてさまざまな形式で情報を開示するために作成します（3.5節「アナウンス機能」を参照）。本書においては、この機能の範囲はインシデントハンドリングサービスに直接適用できる場合に限定します。しかし、広範なサービスを提供するような CSIRT では、アナウンスを公開することはそれ自体でサービスと見なすことができ、脆弱性またはアーティファクト分析などの他のサービスからもたらされる広範な情報を提供すると考えられます。

### フィードバック機能

フィードバック機能は、特定のインシデントに直接結びつかないような問題に関するフィードバックの提供をサポートします（3.6節「フィードバック機能」を参照）。フィードバックは（メディアなどによる）明示的な依頼に応じて提供したり、依頼がなくても定期的に（年次報告などで）提供したり、または必要に応じて提供（メディアへの事前情報提供など）したりすることがあります。この機能は少なくとも最低限の FAQ（よくある質問への回答）をサポートし、メディアからの依頼の橋渡し役、またはチーム全体への入力への橋渡し役と見なされます。

## 3.3 トリアージ機能

この機能の目的は、情報が届けられた方法（電子メール、FAX、電話、または郵便など）に関係なく、インシデントハンドリングサービスの対象となるすべての情報を、適切に区分されサービスとしてのハンドリングを実施するために、単一の拠点を経由して振り分けることです。この目的は通常、トリアージ機能をインシデントハンドリングサービス全体の単一連絡窓口として広く知らしめることで達成されます。Constituency などがトリアージ機能を迂回できないように制限する場合は、個々のチームのメンバへの直通の連絡先（電話番号や電子メールアドレスなど）を表に出してはいけません。

これは多くの CSIRT サービスで一般的な要件であるため、チームは通常、CSIRT 全体の単一連絡窓口のみを案内しています。また、求められるサービスに関係なく、CSIRT が提供するすべてのサービスに対して単独のトリアージ機能が提供されます。

例：DFN-CERT では、トリアージ機能の担当者のことを「CERT ホットライン担当」と呼んでいます。この担当者はインシデント対応チームのエイリアスに届く電子メールをすべて読み、すべての郵便物を開封し、受信したファ

ックスに目を通し、すべての電話に対応しています。インシデント関連の電話をすべて集中処理するために、DFN-CERT ホットラインおよびチームメンバーの電話回線はすべて、この担当者の電話に転送されます。

報告と関連情報の収集が積極的に行われるように、使いやすく効率の良い報告のしくみを Constituency に提供する必要があります。

- 明確に定められた連絡窓口
- 定められた連絡窓口の利用に関する詳細情報
- 単純かつ明確な手順
- 報告すべきイベントの種類に関する分かりやすいガイドライン
- 報告者用の関係書類（報告用フォームや利用可能な他の書類への参照など）

トリアージによって情報が受け取られると、受領確認が送られたのち、情報の分類、優先順位付け、追跡、サービス内の他の機能への受け渡しが行われます。また、トリアージ機能では暗号化されたメッセージを復号し、デジタル署名をチェックして、その情報を後で使用するために保存し、内容を実際に読めるようにする必要があります。この作業を行うために、トリアージ機能は、インシデントハンドリングサービスの他の機能が使用しているデータリポジトリにアクセスできなければなりません。

受け取った情報およびリポジトリ内の既存のサービスイベントに関するデータを基に、まずその情報をどのインシデントハンドリングサービスの機能が処理すべきかを判定するために最初の分類を行います。次のステップでは、情報が現在または過去のイベントに直接関連するものかどうかを判断します。情報が既存のイベントまたは以前に追跡したイベントに直接関連している場合は、そのイベントの一部としてタグ付けされます。関連していない場合は、特定のタイプの新しいイベントとして追跡され、適切なタグが付けられます。分類とタグ付けに加えて、トリアージ機能は通常、サービス内の機能で使用されている優先順位付けのスキームに従って、情報に最初の優先順位を割り当てます。情報がハードコピー資料の形で入ってきた場合、トリアージ機能は通例、その情報をオンラインに入力するか、資料の物理的な保管場所をオンライン照会できるようにします。

情報やイベントの入力、利用、追跡を行うツールによって、データの操作性と検索性が大幅に向上し、半自動化されます。このようなツールは、以下の鑑定方法を確立するのに役立ち、トリアージの担当スタッフを支援できます。

- 新しいイベント（インシデント、要求、脆弱性報告、その他の情報通知）
- 現在追跡しているイベントに直接関連する情報
- 以前に終了したイベントに直接関連する情報
- 別に追跡しているが、直接関連している可能性があるイベント
- インシデントハンドリングサービスの範囲外と考えられる情報

情報に詳細な内容が含まれていない場合や、情報が不完全な場合、トリアージ機能は遅くなったり、不正確になったり、役割を果たせなくなったりします。このような場合には、情報提供者に詳細な情報を求めないと、情報を適切にトリアージできないため、処理が遅れます。トリアージ機能を直接的に支援するツールに加えて、トラッキング番号、標準報告用フォーム、および連絡先の事前登録など、情報の品質を向上させる他の措置を取ることができます。次の3つの節では、これらのトピックを取り上げます。

### 3.3.1 トラッキング番号の使用

トラッキング番号方式を使い、その後の連絡業務において、他のチームにもその割り当てられた番号を使うように推奨または要求できれば、トリアージを円滑に進めることができます。自動化による支援を積極的に進めるには、番号方式で人間とツールが認識できる単純な識別子を提供する必要があります。ある堅牢な追跡システムでは、トラッキング番号は「タグ」であり、システムはこれを使うことにより、この初期段階では人間の手を介さずに、受信した情報を自動的に分類し、他の関連する活動と一緒に保存します（関連させます）。これによってプロセスが簡素化し、トリアージ機能はタグのない情報を正しく関連させることに専念することができます。トラッキング番号は、電子メールでは件名の中で使用し、FAXでは表紙に記入し、音声メッセージでは口頭で指定するといったことが簡単にできます。

トラッキング番号は、インシデントハンドリングサービスの各機能の下で生じるイベントの追跡に使用します。そこでさまざまなサービスごとに、異なるプレフィックスを使用することがあります。そのためには外部とのやり取りを考慮して、その番号を「所有する」チームを識別できるような番号（文字列）を含めなければなりません。つまりフィードバック、インシデント、およびアナウンスに、それぞれ独自のトラッキング番号を付ける必要があります。

例：CERT/CCでは、インシデントの追跡にはCERT#というプレフィックス識別子を使用しています。脆弱性の追跡にはVU#を使用しています。優先順位の低い、その他の情報の識別にはINFO#を使用しています。また、各種の内部文書と外部文書には、他のプレフィックスを使用しています。

#### 3.3.1.1 CSIRT 内における一意のトラッキング番号

トラッキング番号の基本要件は一意であることです。番号方式の基準として、あらかじめ定めた範囲の整数から番号を割り当てる方法が一般的です。チームのインシデントハンドリングサービス内において、またできればすべてのCSIRTサービスに渡って（トラッキング番号は、脆弱性ハンドリングやアーティファクト分析などのサービスにも使用できます）、機能ごとに一意のプレフィックスを使用し、プレフィックスに続くトラッキング番号も必ず一意にするのが最も望ましい方法です。複数の機能に同じ番号を付けると、関係者がプレフィックスを付け忘れて番号だけで照会した場合に、混乱や他の問題が生じる可能性があるからです。理想的には、インシデント番号60とフィードバック番号60のような付け方はしないでください。タグ番号自体が一意のイベントを指していなくてはなりません。

せん。番号の再利用を考える場合は、あるイベントが終了してからその番号を再利用するまでに確実に十分な時間をとるように、徹底した管理を行ってください。十分な時間差を取ることによって、その番号が、以前に追跡されていた活動やイベントに関するものであると誤解される可能性がより低くなります。

例：1994年、DFN-CERTは1～65,535の番号を使用しました。番号を再利用する計画はありませんでした。4年間の運用で使用されたのは、約600件の番号でした。一意のタグ番号を割り当てる回数は増えても、古い番号を再利用したり異なる番号範囲を採用したりする必要が生じるまでに、まだ何年もあります。

例：CERT/CCではインシデント報告と脆弱性報告を追跡するために、ランダムに生成される番号の組み合わせも使用しています。複数の報告が関連していたために相互参照されたり、後からより大きな活動にマージされたりしない限り、インシデントや脆弱性に同じ初期トラッキング番号が割り当てられることはありません。その場合にも、活動の性質によっては、複数の活動間での別の関係を示す他のトラッキング番号を参照することがあります。しかしCERT/CCでは大量の報告に対応していたため、インシデント報告以外の情報（例えばCERT Summary、案内、CERT Incident Notes、CERT Vulnerability Notesなど）を追跡して参照番号を割り当てるために、別の種類の追跡識別子を処理できるような補足的な体系が必要になりました。

一定の整数範囲をトラッキング番号に使用するのではなく、考えられる識別子を制限なく提供する方法も採用されてきました。このような方法が望ましいのは、大規模なConstituencyに対応する場合や、手続きを変更することなく数年間は使用できる拡張性のある方法を確保する必要がある場合などです。

例：1994年のはじめ、AusCERTは最初、YYMMDDHHMMという形式のインシデント番号方式を採用していました。この番号は、AusCERTがインシデントを「オープンした」（対応を開始した）日付と時刻から生成されました。これは利用可能な番号の大きさには対応していましたが、同時にこの番号は、報告に関する望ましくない他の情報、例えば、このインシデントがチームに報告され、CSIRTによって最初に識別された（または追跡対象となった）時間なども示してしまったのです。そのため、AusCERTでは別の方式を採用しました。

### 3.3.1.2 CSIRT間における一意のトラッキング番号

トラッキング番号はCSIRT内だけでなく、さまざまなCSIRTのConstituencyの間でも一意でなければなりません。複数のCSIRTがインシデント対応に関わるため、それぞれが独自の識別子を使用してそのインシデントを参照することになります。そうでないと、2つのチームが異なるインシデントに同じ識別子を使用する可能性があり、混乱が生じ、適切な対応やフィードバックの遅れにつながります。

例：現在、CERT/CCとDFN-CERTは、一定範囲の整数をインシデントに割り当てています。一意性を保証するために、どちらのチームも独自のトラッキ

ング番号を示すプレフィックスを付けています。例えば、CERT#12345 と DFN-CERT#12345 は別々のトラッキング番号で、まったく関係のない2つのインシデントを示しています<sup>22</sup>。最近のチームでは、他のチームとCSIRT活動についての連絡や情報交換をするときには、関わるすべてのチームの番号をすべて記録するのが最善策であるということが一般的に受け入れられています。これによって、そのようなイベントの識別、追跡、および相関が非常にやりやすくなっています。

さまざまなチームが使用している各種のトラッキング番号の形式を認識できるようなツールを使用すると、トリアージ機能をさらに促進できます。全てのチームが効率良く識別および処理ができるように、関連のあるイベントについてやり取りするときには、関わっている他のチームのトラッキング番号を各々参照することが推奨されます。

### 3.3.1.3 トラッキング番号は公開情報である

トラッキング番号は、チームの外部とのやり取りで使用されるため、公開される情報と見なす必要があり、関係しているホスト名やドメイン名などの機密情報を示すようなものであってはなりません。追跡手段において避けるべき機密情報としては他に、報告されたイベント（特にインシデントの場合）の数、性質、または範囲を示す情報などがあります。このような理由から、トラッキング番号に乱数生成方式を使用するのは妥当な策であると言えます。

### 3.3.1.4 トラッキング番号のライフサイクル

トラッキング番号のライフサイクルも考慮する必要があります。識別子を使ってイベントを追跡する場合は、イベントを識別した時点からイベントがチームの観点から処理され、クローズしたと見なされるまで、最初に割り当てたトラッキング番号がそのイベントとともに存続します。しかし、このような単純なモデルに適合せず、以下の考慮を必要とするような状況も起こります。

- **情報が正しくトリアージされていない：**  
イベントが実際には他のイベントと直接関連しているのに、トリアージによって間違っ​​て新しいイベントと識別されていることがあります。
- **情報が正しくタグ付けされていない：**  
間違っ​​たトラッキング番号による情報が届き、結果として不適切な追跡を行うことがあります。
- **イベントの再オープン：**  
イベントがクローズした（対応が終了した）後で、そのイベントに関する新しい情報が届くと、そのイベントは再度オープンされることとなります。

---

<sup>22</sup> 各チームで乱数発生器によって生成されたインシデント報告への番号が偶然にも一致してしまう可能性もあります。しかし実際にはその可能性は低く、たとえ起こったとしても、プレフィックスを使用することで、その活動がどのCSIRTに関係しているかを明確に識別できます。

- イベントのマージ：

以前は別々に追跡していた2つのイベントを直接結び付ける新しい情報が届くことがあります。これによって保存記録が難しくなります。すべてのインシデントには適切な相互参照を付ける必要があります。インシデントが関連しているように思える場合は、さらに詳しく分析して、2つのインシデントをマージする必要があるかどうかを判断してください<sup>23</sup>。

### 3.3.2 報告用の標準フォームの使用

報告用の標準フォームを使用することで、関係者からチームへ、完全且つ適切な情報を提供しやすくなります。また、新しい報告をタイミング良く見つけ、【関連する活動の正しい機能】に情報を振り分けることも容易になります。さらに、初期段階でのやり取りにおける完全性と理解度も上がるため、以降の対応が円滑に進みます。ほとんどのサービスに対して、Constituencyや一般向けに、使い勝手のよいフォームをデザインし、実装することができます（脆弱性ハンドリングサービス内では脆弱性報告フォームなど）。

インシデントハンドリングサービス内では、インシデント報告と情報提供依頼に利用できるフォームを作成することがあります。使いやすさのため、フォームはできるだけ明確かつ簡潔で、必要なときにすぐに利用できなければなりません。ハンドリング機能自体と、トリアージ機能（インシデント報告と、現在追跡している活動との関係性を判断する）の両方に対応するために、インシデント報告フォームでは一般に次のような情報を要求します<sup>24</sup>。

- インシデントに対応して連絡を取り合う報告元サイトやその他の関係者の連絡先
- インシデントに巻き込まれているホストの名前とネットワークアドレス
- 活動の性質
- 活動と関連情報の説明（ログ、タイムゾーン、アーティファクトなど）
- （現地のセキュリティチームまたは他のCSIRTによって）既に割り当てられているトラッキング番号

例：調整活動中に、攻撃を受けたマシンのログが、報告元サイトからCSIRTに提出されます。ログは以下の形式をとります。

---

<sup>23</sup> 注：イベントをマージする場合でも、その識別子に関する問題を考慮する必要があります。いろいろなサイトが関与している（そして、インシデントが以前は別々に追跡されていた）場合は、イベント全体を管理するのが複雑になる可能性があります。そのような場合には、元の問い合わせ識別子と新たに「マージした」識別番号を使用できます。代わりに、個々の報告をすべてマージして、まったく新しい番号を割り当てることもできます。いずれにしても、影響を受ける関係者（サイト、Constituencyなど）には適切な追跡番号識別子を使用するよう通知・要求する必要があります。CSIRTが関係者にそのような要求をしても、影響を受けるサイトやConstituencyのメンバが必ずしも要求に従う保証はないことを認識してください。

<sup>24</sup> これらはCERT/CCインシデント報告フォーム [CERT/CC 1997a] から抜粋したものです。<[http://www.cert.org/nav/index\\_red.html](http://www.cert.org/nav/index_red.html)>では、より新しいインシデント報告フォームも（オンライン報告フォームまたはテキストの形式で）入手できます。



Mar 2 02 10:34:12 myhost tcpd[52345]. connect REFUSED from cumber.some.where

上記のログのタイムゾーンが分からないと、チームはその時間の前後に記録されたユーザのローカルログを調べるための十分な情報を `cumber.some.where` の管理者に提供できません。国際的な環境や複数のタイムゾーンがある国では、活動が生じたと考えられる時間帯が広がるため、この問題はさらに悪化します。

時には、人々に報告の必要性を理解してもらうのに苦労することもあります。インシデントを報告しようとしても、そのフォームが面倒であり効果的ではないと感じてしまったら、進んで報告する気にはならないでしょう。初期段階での情報に多少不足があっても、報告がまったく得られないよりは良いと考え、Constituency に電話をかけてもらったり、「自由形式」（書式なし）で情報を送ってもらったりしているチームもあります。しかしその結果、CSIRT スタッフは、その報告から関連情報を引き出して、CSIRT 追跡システムに入力するためにより多くのリソース（時間）を必要とすることになります。フォームを提供する場合は、できるだけ明確かつ簡潔な形式にして、報告しやすくする必要があります。これは、1つのチームで使用するフォームの数にも当てはまります。CSIRT へのさまざまな問題、依頼、その他の情報の報告用に、単一の基本的なフォームまたはテンプレートを使用できないか検討してください。フォームを提供して、Constituency に使ってもらうことを期待するだけでなく、チームはフォームを使用するメリットを広く認識させ、フォームによる報告を奨励する必要があります。

### 3.3.3 連絡先の事前登録

報告用フォームの使用に加え、Constituencyの規模や性質に応じて、トリアージ機能（およびインシデントハンドリングサービスを構成する他の機能）に役立つ情報をあらかじめ集めるといった事前措置を取ることもできます。このプロセスを拡大して、他のCSIRTや法執行機関などの他の関係者からも事前に情報を集めることもできます。このような登録プロセスにより、新しい報告／依頼のたびに個別に標準的な問題に対応する必要がなくなります<sup>25</sup>。事前登録しておく役立つ項目には次のようなものがあります。

- 信頼できる連絡窓口と関連する連絡先（少なくとも年に一度は定期的に確認する必要がある）
- 情報開示の制限
- 暗号化および／または署名付き情報を交換するための（検証された）鍵

場合によっては、サイトのドメインやタイムゾーン情報など、他の情報を事前登録すると役立つことがあります。しかし、役立つかどうかは、登録されている連絡先と同じタイムゾーンに対象のホストがあるかどうかによります。

---

<sup>25</sup> Kossakowski, Klaus-Peter, 『The Role of Site Security Contacts』。7th Workshop on Computer Security Incident Handling, FIRST (Forum of Incident Response and Security Teams)、ドイツ・カルルスルーエ、1995年9月。

例：AusCERTは1994年、そのConstituencyが（数の上で）小規模ではっきりしていたことを考慮し、『Forming an Incident Response Team』[Smith 1994]で詳述されているように、最初はConstituency登録プロセスを定めました。このプロセスには、信頼できる連絡窓口の設置や情報開示の制限などが含まれていました。AusCERTはその後有料サービスチームになり、このプロセスを変更しましたが、加入者から可能であれば連絡先を入手するという基本的な考え方は踏襲しました。

例：CERT-NLは（インターネットサービスプロバイダである国の研究ネットワークと、その顧客サイトの間での）契約書で規定したConstituencyにサービスを提供しており、そのためサイトのセキュリティ窓口と暗号鍵の登録プロセスを支援し、機密性が高く信頼できる電子メール通信を可能にしています。さらに、そのConstituencyのタイプは学術系であるため、CERT-NLは標準の情報開示ポリシーを使うことができます。

例：CERT/CCは広範なConstituencyを抱えているため、潜在的なすべての報告者からこのような事前登録の連絡先を得ることはできません。しかし、定期的な報告者や、チームがやり取りしている報告者（信頼できる専門家、スポンサー、ベンダなど）については、詳細情報をチームは保持しています。

### 3.4 ハンドリング機能

この機能の目的は、Constituency（および、場合によっては他の関係者）から受ける報告に対応し、支援活動を実施することです。この機能は、少なくとも以下の属性を具体化したものでなければなりません。

- **報告窓口**：Constituencyに関するインシデント報告を受け取る窓口。
- **分析**：報告に対する一定の水準の検証と、報告された活動についての技術的把握。これには、通知した内容の下で提供される、適切な対応を特定する作業も含まれます。
- **通知**：適切な対応／復旧情報を（少なくとも）Constituencyに、可能であれば影響を受ける他のサイトやCSIRTにも伝えます。

「対応」という用語の定義は、チームごとのインシデントの定義と、インシデントハンドリングサービスの目的に応じて異なります。また、その他の要素も考慮する必要があります。中でも最も重要なのは、インシデント報告に割り当てる優先順位と、インシデントに巻き込まれたサイトとの関係（例えばインシデントが個々のチームのConstituencyのものか、影響を受けたサイトのものかなど）です。

表13に、ハンドリングサービスの実施に必要な機能の例を示します。

表13：ハンドリング機能属性の例

属性	例
報告窓口	<ul style="list-style-type: none"> <li>• Constituency に影響を与える報告に対応し、報告内容を（必要に応じて）Constituency 内の影響を受けるサイトに伝える</li> <li>• Constituency 以外のサイトと CSIRT に影響を与える、Constituency からの報告に対応し、必要に応じてそれらの関係者に伝える</li> <li>• 上記の両方</li> </ul>
分析	<ul style="list-style-type: none"> <li>• ログファイルの検査</li> <li>• 影響を受けるサイトの特定</li> <li>• 技術文書や勧告文書の参照先の提示</li> <li>• 技術支援の提供</li> <li>• 回避方法と修正に関する情報の提供</li> <li>• オンサイトでの支援</li> </ul>
通知	<ul style="list-style-type: none"> <li>• 適切な連絡窓口を提供する、またはその設置を支援するリソースの提示</li> <li>• 適切な連絡窓口のリストの提供</li> <li>• インシデントの影響を受ける他の関係者との連絡</li> <li>• 影響を受ける他の関係者および法執行機関との連絡</li> </ul>

分析について詳しく述べる前に、第一報から分析、通知、クローズまで、インシデントのライフサイクルの概要を説明しておきます。インシデント分析機能をうまく実施するには、ある特定の情報を追跡する必要があります。これについても、次の節で述べます。

### 3.4.1 インシデントのライフサイクル

チームのインシデントの定義に関係なく、そのライフサイクルはこの節で説明するライフサイクルに合致しているものと考えられます。3.3節「トリアージ機能」で述べたように、インシデントのライフサイクルは、トリアージ機能内で扱われる場合があります。これは、そのインシデントを最初に分類し、追跡すべき新しいイベントとして、もしくは既に追跡している既存のインシデントの一部として特定することが可能な場合です。まずインシデントに適切なトラッキング番号（新しいトラッキング番号、または既に追跡されており、そのインシデントが属する活動の番号）を割り当てます。しかし正しくトリアージされていない情報、間違ったトラッキング番号でチームに提供された情報、または詳細な技術分析の末に発見された新しい情報などの結果として、ハンドリング機能の実施中に新しいインシデントが特定されることもあります。図 5に、CERT/CC インシデントハンドリングのライフサイクルプロセスを図示します。これについては、以下の段落でさらに詳しく説明します。

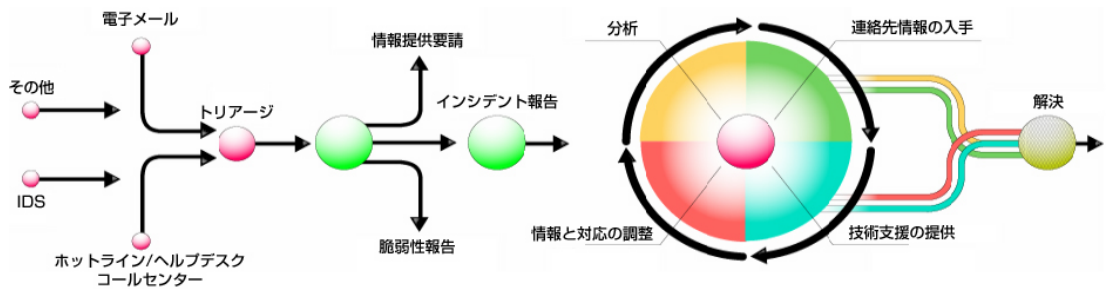


図5：CERT/CC インシデントハンドリングのライフサイクル

インシデントは、いったんオープンすると、そのインシデントに関連するあらゆる情報とともにさまざまな状態を遷移し（状態の変化と関連するアクション）、チームの観点から、それ以上のアクションが必要なくなれば（ライフサイクル図の「円」の部分）、インシデントは最終的にクローズします。インシデント（またはイベント）は、その活動のライフサイクルの間に、分析段階を何度も廻る可能性があることを認識しておくことも重要です<sup>26</sup>。

インシデントがクローズするのは通常、そのインシデントの関係者が誰も CSIRT に新しい情報の確認や報告をしなくなり、且つ CSIRT が影響を受けたすべての関係者への適切な対応を行うというアクションを取ったときです。新しい報告があることが予想されても、それ以上フォローアップする意味がなければ（チームにそれ以上できることがない場合など）、インシデントをクローズすることもあります。

例：ある CSIRT はウイルス報告に関する外部からの【更なる】情報を受信しています。しかし、そのウイルス報告は既に受信、分析、処理され、CSIRT の Constituency には適切な通知がなされました。さらに分析しても何も新しいものは得られません。したがってこのインシデントはクローズします。

例：ある会社の CSIRT は、インシデントに関する訴訟事件が起きた場合は、それが完了するまでインシデントをクローズしないことがあります。

例：ある大規模な Constituency にサービスを提供している調整役の CSIRT は、インシデントに巻き込まれたサイトがそれ以上の技術支援を必要としなくなった場合にインシデントをクローズすることがあります。

このように、インシデントをクローズする基準はチームによって異なるのです。

また、たとえチームがインシデントをクローズしても、インシデントに巻き込まれたサイトがインシデントの解決に引き続き関わっていたり、システムを復旧する準備をしていたり、また加害者に対する訴訟に関与したりしている場合は、まだインシデントがオープン状態であると見なされている可能性があることにも

<sup>26</sup> この「CERT/CC インシデントハンドリングのライフサイクル」の図はCSIRTのトレーニングコースから抜粋したものです（<<http://www.cert.org/training/>>参照）。

留意してください。後者の例で、CSIRTが幅広いConstituencyを持つ調整役のチーム（例えば国レベルのチーム）である場合は、影響を受けたサイトが起こしている訴訟手続に関与することはないでしょう。

インシデントは、そのライフサイクルの間に、次のように多様な状態を遷移する可能性があります。

- 要アクション：インシデントに対応したアクションがチームに必要とされている。
- 待機：チームは外部の関係者の対応を待っている。

CSIRTがインシデントをクローズするときには、影響を受けた関係者全員に、インシデントのクローズを事前または事後に知らせる必要があります。これにより、CSIRTに期待してよいことが適切に設定され、インシデントがまだオープンの状態だと考えられたり、CSIRTからその後の連絡がないことに疑問を抱かれたりといった混乱を避けることができます。その際、インシデントをクローズするときに関係者全員に個別に知らせる方法もあれば、進行中のインシデントの連絡時に関係者に知らせる方法もあります。前者は時間がかかる上に、瑣末な電子メールによる対応を立て続けに行うこととなります。また最終的にインシデントを「要アクション」の状態に戻すような対応になる可能性もあります。後者の方法では、連絡担当者にとってはタイミング良く情報を提供しやすくなり、限られたCSIRTリソースを効果的に活用することにもなります。

例：以前、直接的な1対1のインシデント対応がもっと多かった時期に、CERT/CCのインシデントハンドリング担当者は、連絡先のサイトに対して、指定日までに連絡担当者から更なるフィードバックがなければ、そのインシデントの一連の処理はCERT/CCによってクローズされたものと見なすと伝えることがありました<sup>27</sup>。

インシデントに巻き込まれたサイトの1つで再発した活動についての報告など、チームが新しい情報を入手した場合に、クローズしたインシデントを再びオープンにする必要が生じることがあります。インシデントを再びオープンする必要性が生じた場合は、できる限り元のトラッキング番号を再利用すべきです<sup>28</sup>。ただし、その活動が元のインシデント／報告の続きであるとは考えられない場合は、その活動に対して新しいインシデントと見なし、新しいトラッキング番号を発行するのが適切です。

---

<sup>27</sup> 最近では、CERT/CCは多くのConstituencyを支援する（1対多の）より戦略的な調整役に重点を置いているため、エンドユーザとの直接的なやり取りは少なくなっています。処理するインシデントのタイプに応じて、CERT/CCは報告を「オープン」の状態にして、連絡担当者からさらに情報を集めることもあります（CERT/CCからの一般的な自動応答メッセージは、インシデントの負荷が重いと、すべてのインシデント報告が個別のフォローアップを受けられるわけではないことを示しています）。

<sup>28</sup> 残念ながら、一部のトラブルチケットシステムでは、いったんクローズしたチケット番号を再びオープンにすることができません。

また、前述したように、以前は関係ないと思われていた複数のインシデントを直接結び付ける新しい情報を入手することもあります。そのような場合は、インシデントを1つにマージするか（この場合は、使用するトラッキング番号と情報を知らせる関係者を特定します）、あるいは別々のインシデントのままにして関連ありのマークを付けるか決める必要があります。どのようなスキームを採用する場合も、影響を受ける可能性のある手順、ツール、およびデータベースはすべて、そのイベントに対応できるものでなくてはなりません。このような技術的問題は解決できますが、人間に関する問題は簡単に解決できるものではないため、配慮する必要があります。あいにく、インシデントの番号を付け替えたりクローズしたりした後でも、新しい活動を報告する際に、期限切れのトラッキング番号が含まれた古いメッセージに返信してくる人が現れることがあるのです。

### 3.4.2 インシデント分析

インシデントのライフサイクルにおいては、分析によって、意思決定プロセスに重要な役割を果たす情報と、チームのポリシーおよび手順に従って次に取るべきステップが明らかになります。

インシデント分析の最初のインスタンスは、実際にはトリアーゼ機能の実施中に発生し、新しい情報が入ってくるたびに発生します。この種の分析については既に取り上げているので、ここでは触れません。ここでは、ログファイル、悪意のコード、およびインシデントの構成について、より詳細な技術的分析に重点を置くことにします。

例：病院の救急室との類似性を考えてください。トリアーゼ機能ではまず、どのような患者が運ばれてきたら、どこに送るかを決めます（第1の「初期」ハイレベル分析）。その後、血液検査、スキャン、心電図、X線検査など、総合的な分析を行います。これらの検査結果は、薬か治療か（または両方）など、次の処置の決定に役立ちます。

さまざまなタイプの分析が、インシデントハンドリングサービスとは別個の、独立したCSIRTサービスになり得ます。例えば、インシデントハンドリングサービスに加えて（あるいは完全に別個の）、アーティファクトハンドリングサービスを提供することなどが考えられます<sup>29</sup>。

アーティファクトは、侵入者による活動の痕跡の中で見つけることができます。アーティファクトの探索と分析、およびその後できる限りコスト効率良く無効化する作業は、個々の手法で行われます。このような個別のサービスの説明は、この節の目的ではありませんが、アーティファクトはたいていインシデントハンドリングサービスの間に発見され、アーティファクト分析はある程度インシデントハンドリングに含まれるため、必要に応じてアーティファクトの話題に触れます。ただし詳しくは述べません。

---

<sup>29</sup> CERT/CCではこのサービスを提供することになりました。CERT/CCのプレゼンテーション資料『Overview of Incident Trends』（<http://www.cert.org/present/cert-overview-trends/module-1.pdf>）を参照してください。

インシデント分析は一般に次の2つに分類できます。

- **インシデント内の分析**

特定のインシデントに関する問題の分析です。最も一般的なタイプは次のとおりです。

- 侵入者の活動によって残されたアーティファクトの分析（ログファイル、攻撃手法、ウィルス、トロイの木馬プログラム、ツールキットなど）
- インシデントが発生したソフトウェア環境の分析
- インシデント内における信頼のネットワークの分析

- **インシデント間の分析**

インシデント間、およびインシデントの横断的な関係に関する事柄の分析、すなわち、進行中のインシデントの構成の分析です。この分析は、侵入者の活動の大元が同じか、関連している可能性を示している別々のインシデントの間で、対称性を見つけることが目的です。

分析は非常に大きなテーマ領域です。優れたインシデントハンドリングサービスを提供するには十分な分析が不可欠であるため、この章で分析について詳しく取り上げることにしました。まず、全体的な分析調査（「全体像」）の重要性と、実際に行う分析の深さに影響を及ぼす事柄から取り上げます。

### 3.4.2.1 全体像

すべての分析結果の全体的な理解、すなわち「全体像」を持つことが重要です。全体像は主に、傾向（考えられる将来の攻撃の種類、セキュリティ向上）、統計データ（例えば、巻き込まれたホストの数、インシデント報告の頻度）、およびケーススタディ（例えば、侵入者コミュニティや、特定のシステムおよびアプリケーションへの影響度合いの把握）に関するものです。CSIRT ごとに、Constituency にとって最も適切な独自の全体像を構築します。

各種の分析に取り組むためにさまざまなスタッフが割り当てられていることがあるため、このような全体像を把握することが困難な場合があります。チーム内のいろいろな人々が、分析から得られるさまざまな情報を持ちます。チーム全体に提供された情報から全体像を得るためには、情報収集プロセスを設定することが重要です。そのためには、チームメンバが定例会議でやり取りしたり、インシデント管理者がチームのメンバから情報を得るようにします。

全体像を絞り込むと、学んだ教訓を確認するときに特に役立ち、将来のインシデントへの対応を向上させることができます。長期に渡るインシデントハンドリングの結果、身に付いた教訓と経験を学ぶことによって、得られた事例の履歴情報は、将来においても、またすぐにでも、スタッフが適切な決定を行う上で役立ちます。このプロセスを支援するナレッジベースを導入すると役立つことがあります。ナレッジベースは、人間のように雇用者を変えることも休暇を取ることもないため、特に継続性のためには有効です。ケーススタディも、新しい CSIRT メンバにとって優れた学習ツールです。

例：次の例は、適切な事例履歴にアクセスすることによって、どのように全体像を理解できるかを示しています。インシデント内およびインシデント間

分析の結果、インシデントが何度も確認された障害が起きたシステムには、ある特定の変ったディレクトリ名があり、ファイルシステムのどこかにトロイの木馬プログラムが置かれていることが分かりました。このチームは、次にこの変ったディレクトリ名が見つかったら、「直ちに」対応するトロイの木馬を探すことになりました。

全体像を（好ましくない部分を適切に除外して）、他のチームや場合によっては法執行機関に提供することが有効であり、賢明です<sup>30</sup>。全体像の提供は、無料のテキスト配信によるニュース速報や、公開用の共通フォーマットで行うことができます。CSIRTコミュニティでは、共通フォーマットはまだ採用されていません。さらに、Constituencyに最新情報を提供し、意識を向上させ、新たな傾向や展開を洞察してもらうために、アナウンス機能を通じてConstituencyに報告書を公開しているチームもあります（3.5節「アナウンス機能」を参照）。他の取り組みとして、データを表すための、より定型化された方法を求める取り組みが進行中です（例えば、「TERENA's Incident Object Description and Exchange Format Requirements」 [RFC 3067] を参照）。この取り組みの目的は、最終的に「アラート、調査中のインシデント、保存記録、統計データ、報告などを含めて、CSIRT間でインシデントに関する情報の説明、保存記録、および交換を行うための共通データフォーマット」を提供することです。

### 3.4.2.2 分析の深さ

インシデントの分析はどの程度まで詳細に行い、またどの程度のリソースを投入するべきでしょうか？ 分析の深さは要因の範囲によって異なります。表 14に例をいくつか示します。

---

<sup>30</sup> Carpenter, Jeffrey J., Dunphy, Brian P. 『Moving Towards the Exchange of Incident Statistical Data』。FIRST (Forum of Incident Response and Security Teams) のコンピュータセキュリティインシデントハンドリングおよびレスポンスに関する第 10 回年次カンファレンス、1998 年、メキシコ・モンテレー。



表14：分析の深さの要因

分析の深さに関する要因	説明
チームのミッションと技術力	Constituencyのセキュリティ保護をミッションとするチームは、進行中のインシデントを詳細に調査するためにあらゆることを行う必要があります。そのための技術力がチームに必要です。特定の領域での技術力が欠けていると、詳細な分析になりません。その場合には、その領域の分析を外部に委託することも考えられます <sup>31</sup> 。
インシデントの深刻度	資金と人材が十分にある場合は、優先順位の低いインシデントでも頻繁に、広範囲に渡り調査を行える可能性があります。一方、資金や人材が限られているチームでは、分析の深さに慎重になる必要があり、たいてい優先順位の高いインシデントに集中します。
繰り返しの可能性	侵入者が別の機会に別の場所を攻撃する可能性がある場合は、インシデントの分析に時間をかけることは無駄ではありません。インシデントを調査し、Constituency、他のチーム、および場合によっては法執行機関に関連情報を提供することで、インシデントの繰り返しに起因する影響が軽減されます。このようなインシデントの分析は内部でも利用することで、他のチームメンバが全体像を把握できます。
新しい活動を識別する可能性	侵入者が誇示する活動や使用されたツールと手法が一般に知られている場合、インシデントを詳細に分析することはあまり重要ではありません（チームがその分析から新たに学ぶことは何もありません）。しかし、侵入者が新しい攻撃手段、または既存の手段やツールの新しいバリエーションを使用している疑いがある場合は、活動を理解するために詳細な分析が必要です。
Constituencyからの支援	サイトからインシデントの報告が行われても、詳細な分析に必要な情報が提供されていないと、それ以上の分析は事実上できなくなります。

イベントを徹底的に分析して、結果を Constituency と他のチームに適切に開示するための時間がある場合は、CSIRT はあらゆるアクションを取ることができます。リソースがより必要になる順番に、考えられるアクションを以下に示します。

- ログファイルの検査
- 悪意のコードとソフトウェア環境の検査
- 回避方法または修正プログラムの提供
- 積極的な問題解決
- サイトのセキュリティと、そのサイトのネットワークの（「信頼」）関係の検査

例：内部（イントラネット）および外部（インターネット）の観点から見て、サイトのホストシステムに明らかな欠陥がない場合、チームは市販の脆弱性スキャナを使って積極的に調査することもあります。この方法でサイトのセキュリティ体制をチェックするのは非常に簡単です。しかしこうしたチームの活動が、サイトへの「侵入」だというような誤解を避けるために、管理者の承認を得る必要があり、チームとサイトのポリシーと手順を順守しなくてはなりません。見落としたセキュリティ上の弱点に対する法的責任を避ける

<sup>31</sup> CERT/CC Webサイトの『Outsourcing Managed Security Services』（<http://www.cert.org/security-improvement/modules/omss/>）を参照してください。

ために、結果を入念に分析する必要があるので、このようなチームの活動には非常に時間がかかります。

### 3.4.2.3 ログファイル分析

適切なハードウェアプラットフォームとオペレーティングシステム、および多くのプログラム（特にサーバ型ソフトウェア）には、アラームとログの機能が付いています。アラームは、パケットフラッドなど、あらかじめ定義された何らかの（通常は好ましくない）イベントが発生すると、注意を促すために発動します。ログは、イベント（有害と無害の両方）が記録されるファイルです。何らかのログエントリが、あらかじめ定義されたアラーム条件を満たしている場合にアラームが鳴ります。

アラームは主に対象となるオペレータのためのものであるのに対し、ログファイルは可搬性があり、詳細情報が豊富に記録されているため、幅広く使われます。ログファイルには次のような情報が記録されます。

- 誰がいつどこからログインしたか
- どのようなログイン（SSH、telnet、rlogin、X など）が行われたか
- どこ宛の電子メールが送信されたか
- どのようなエラーが発生したか

ログファイルに、必要なレベルの詳細情報が記録されるようにするのは、関連するシステムのオペレータの仕事です。もちろんインシデントハンドリングサービスでは、インシデントの過程で、しかし同時に予防策として **Constituency** に適切なログファイルの活用方法を伝えるといったアドバイスができます。関連ログを受け取り、処理し、その結果に対応するのは **CSIRT** の責任です。

DNS システム内で変更が行われ、ホスト名や IP アドレスがもう有効でない、あるいは別のホストを指しているといったことが生じる場合があります。そのため、ログファイルを単に付随的に利用するだけでない場合は、ログファイルは一定の特性（表 15 を参照）を示さなければならず、可能な限り迅速に分析する必要があります。また、ログを生成したツールの設定ファイル（`/etc/syslog.conf` など）と併せて精査することで、ログの価値が最大限に得られます。

ログファイルの受け付け、受け取り、および処理には、**CSIRT** が考慮すべき一般的な問題が含まれています。これらの問題について以下で検討します。さらに、**CSIRT** の施設内にあるすべての資料を保護する必要もあります（3.8.4 節「情報の保管」を参照）。同様に、必要とされなくなり使用されなくなったすべての資料を慎重に破棄することも重要です（3.8.5 節「情報のサニタイズと処分」を参照）。

表15：ログファイルの注目すべき特性

特性	説明
タイムスタンプ	ログには、記録するほとんどすべての内部イベントについて、タイムスタンプがなくてはなりません。いろいろなサイト（または同じサイトの異なるマシン）のログを比較するときに混乱を避けるために、NTP（Network Time Protocol）のような時間同期ソフトウェアの使用を強く推奨します。同じ理由から、タイムスタンプには、タイムゾーン情報も含めてください。
ログの出所	ログを生成したマシンに関するあらゆる詳細（インターネット名、ネットワークアドレス、マシンタイプ）を収集する必要があります。また、ログの生成に使用したソフトウェア（バージョン番号を含む）と関連する設定ファイルを知っておくことも重要です。
ログの認証	認証がなければ、ログファイルが本物であり、問題になっているイベントの後で作成されたり、活動が発見される前に改ざんされたりしたものでないと言ふことはできません（結局、ログはまだ大部分がテキストファイルであるため、コンピュータ上でテキストエディタを使って作成できます）。法律によっては、重要なログファイル（印刷したログファイル）には、できればログが生成された同じ日に、2人の人間が日付と署名を付けることを推奨しています。このような処置は主として、訴訟が考えられる場合に重要です。あるいは、アクセスが厳しく制限されている別のホストマシンにログを書き込むことです。

## 分類

ログファイルはどのような分類（機密または公開）に属するのでしょうか。トリアージ機能によって適用される情報の分類に関するポリシーがなくてはならず、結果として、その分類に沿って情報を処理しなくてはなりません。

ログファイルの場合はたいがい、1つのログに複数の分類を関連付ける必要があります。一般的な情報は通常、マシン名、ネットワークアドレス、社員名が明らかになるような特定の情報に比べて、機密性は高くありません。

例：IP スニファールログには通常、機密性がまったくないものから、明確なユーザ名／パスワードの組み合わせ、さらに電子メールや添付書類などの情報が含まれている可能性があります。

通常は、ログファイルを実際に入手する「前」に、ログファイルの大まかな分類を行う必要があります。（ログ内の明白な情報に基づいた）分類によって、ログの受け取り方法と、ログの扱い方に境界条件が課せられる場合があるためです。

## 受け取り

ログがチームに提供されるときには、ログ情報の分類に応じた、相応の注意を払う必要があります。機密情報は安全な方法（暗号化チャネルの使用など）で送信する必要がありますが、重要でない情報は電子メールを使ってプレーンテキストで送信できます。ネットワーク上で大量のログを暗号化して送信することができない場合は、ディスクやテープでの送付が適切な場合もあります。

## 検証

そのログファイルは本物でしょうか。認証方法について報告する側と合意している必要があります。解決策の1つとしてはデジタル署名があります。また MD5 と RSA は、これを実装している定番のアルゴリズム/プロトコルです。MD5 (チェックサムアルゴリズム) は受信データと送信データが等しいことを確認するだけですが、RSA (公開鍵アルゴリズム) は送信者の同一性と受信データの真正性を証明するのに役立ちます。しかし、侵入者や他の関係者によってログが改ざんされていないことを 100%証明できる方法はありません。

## クレンジング

機密性が高くても、無関係な情報は多くの場合、公開される可能性を完全に排除するために、直ちに破棄するかサニタイズすることが最善策です。

例：パスワードはたいてい、受領したログからすぐに取り除くことができます。パスワード情報を CSIRT が利用することはほとんどなく、パスワード情報が漏れることは望ましくありません。関係者にすべてのパスワードを変更するように要請することもできますが、それでは時間がかかり、また全ての Constituency が必ずしも要請に応じるとは限りません。そのため、不要なリスクを回避することが重要です。オリジナルのログは法的な調査の際に使用される可能性があるため、無変更のまま残しておく必要があります<sup>32</sup>。

## ログの一部の開示

インシデントのフォローアップが行われ、他の Constituency やチームへ、活動についての情報や、インシデントのうちその Constituency やチームと関連する情報を通知する場合に、ログファイルからの情報を送信しなければならないことがよくあります。原則として、ログファイルを完全且つ無削除のまま送信することはありません。関係する部分だけを抜粋して関係者に送信します。この抜粋には、関係者に特に関連する情報だけが含まれています。

### 3.4.2.4 アーティファクト分析

侵入者はたいてい、様々なファイルを侵入するシステム上に残します。それらは Ethernet スニファーログファイル、パスワードファイル、攻撃スクリプト、ソースコード、さらには各種のプログラムやツールなど、多岐に渡ります。一般的に、これらは「残留ファイル (remnant file)」と呼ばれます。悪意が存在する可能性のあるスクリプトやソースコード (悪意のコード) などのプログラムは、「アーティファクト」として扱います。これらのファイルにはまったく悪意がないものもあるかも知れませんが、分析しなければ分かりません。悪意がないと証明されるまで、アーティファクトスクリプトまたはプログラムは悪意のあるものと見なすことが初期段階での想定としては適切です。

---

<sup>32</sup> これは実際には非常に古い例ですが、FTPやPOP3、さらにHTTPベーシック認証のようなクリアテキストパスワードプロトコルがいまだに広く使用されていることを考えると、これはまだ十分に有効でしょう。

侵入者によって通常のファイルが置き換えられ、ファイル名はそのまま中身はオリジナルとは異なるものになっている場合があります。このようなトロイの木馬プログラムは、侵入者の間でよく知られています。トロイの木馬は、元のプログラムで意図していたことをすべて実行しているように見えるのに、間違っただけで実行するプログラムです。つまり（さらに悪いことに）、元のプログラムで想定されていたことをその通りに実行するとともに、他のこと（何が起きているのか最新情報を侵入者に伝えたり、機密情報を隠された記録先に送信したり、情報を外部宛てに送信したりするなど）も実行します。

例えば「トロイの木馬」バージョンのtelnetデーモンは、ユーザが入力したユーザ名/パスワードの組み合わせをログに記録し、そのログを侵入者に電子メールで送信したり、侵入者が取り込めるようにディスク上のどこかに保存したりするといったことが考えられます。トロイの木馬などの偽プログラムは、日付やサイズなどのファイル属性では明確に特定することはできません。侵入者は、ファイルの内容以外のあらゆるファイルシステム属性に関して、トロイの木馬をオリジナルのプログラムと同じものにするために手を尽くしています。つまり、ファイルの違いを検知するには、適切な暗号チェックサムの実行を行う以外に方法がないということです。そのため、（些細な侵入の後でもシステムを完全に再インストールするのではない限り）システムファイルや重要なプログラムについては、オフラインで読み取り専用のチェックサムのリストを保存しておくことが良い対策です。Tripwire<sup>33</sup>などのプログラムやThunderByteなどのウィルス対策プログラムは、この種のリスト作成を日常処理の一部としており、ファイルのチェックサムが変わっているとユーザに知らせるようになっています。

CSIRT がインシデントハンドリングサービス（または別個のサービス）の一環として悪意のコードを分析すべきか否かという問いに答えることは重要です。これについてはCSIRTによって見解が異なります。以下はその違いが顕著に現れている例です。

例：チームによっては、悪意のコードを分析する専門家が常駐していないため、そうした分析を行うには他のCSIRTや専門家に頼らなくてはなりません。

例：サイトのネットワークのセキュリティ保護を業務にしている営利チームは、通常は必要に応じて、悪意のコードの分析など、問題の原因を詳細に調査します。

誰が業務を遂行するかに関係なく、悪意のコードの適切な分析に、ある程度は取り組まなくてはなりません。それ以外の方法で、他のインシデントを分析するのに役立つ可能性のある侵入者の痕跡を引き出すことができるでしょうか？ そのコードが何をしようとしているかを実際に観察せずにその後の調査の方向性を知るすべは他にあるのでしょうか？ すべてのアーティファクトを取り除き、システムを一から構築するのは、侵入の解決策としてはあまりにもコストがかかります。また、そのような解決策はたいてい非常に認識の甘いもので、特に初めの段階で

---

<sup>33</sup> Tripwire<sup>®</sup>は、<http://www.tripwire.com/>で市販されています。一般公開版は<ftp://ftp.cerias.purdue.edu/pub/tools/unix/ids/tripwire/>から入手できます。

侵入を許した欠陥が取り除かれていない場合はなおさらです。「アーティファクトの中に侵入者は潜んでいる」ため、アーティファクト分析とはアーティファクトが何をやるものであるかを理解することで役に立つ可能性があるのです。

インシデントハンドリングサービスの一環として悪意のコードを分析する責任を CSIRT が負うと仮定すると、以下の点を考慮する必要があります。

### アーティファクトを分析する場所

通常、悪意のコードを被害を受けたシステム上で分析してはいけません。Constituency はできるだけ早く通常業務に戻ることを望みますが、さらに Constituency の環境を危険にさらすことはできません。侵入者の観点からすると、コードが間違った形で呼び出された場合にハードディスク上の情報を破壊しようとするように悪意のコードを書くことはとても簡単なことです。

可能な限りオリジナルの環境を正確に反映したアーティファクトと周辺環境を再現する場合は注意してください。これはファイルを送信する Constituency だけに該当するものではなく、CSIRT のメンバもしくは知識のある他の権限保持者にも該当します。つまり、Constituency はチームメンバに関連システムへの一時的なアクセスを許可するか、CSIRT スタッフが提供する指示やガイダンスに従って Constituency 自らが作業を行うこともあるということです。

理想的には、アーティファクトは隔離された、すなわちネットワークから切り離されたラボで分析します。アーティファクト分析には、テスト用コンピュータ設備とテスト用ネットワーク環境を使用してください。また、テスト環境のデータが全部なくなっても、全く問題がないようにしてください。実用上の理由から、外部からテスト環境へのアクセスを可能にする必要がある場合は、非常に厳しく制限されたファイアウォールを通じてのみアクセスできるようにする必要があります。

例：いくつかの対応チームで、実稼動環境（つまり隔離されていない環境）で、INND（ネットニュースデーモン）の欠陥をテストしていました。その結果、Newsの「制御メッセージ」がテストシステムから抜け出し、NNTP<sup>34</sup>で行うことをそのまま実行してしまいました。つまり世界中に広がってしまったのです。不運にもこれらの制御メッセージは、INNDの欠陥を使って特定の電子メールアドレス（この場合はテストを行っていたCSIRTチーム）に/etc/passwdファイルが送信されるようになっていたのです。そのため、このようなメッセージを何千通も受信することになってしまいました。チームが適切に隔離された試験環境を利用していたら、このような事態は起こらなかったでしょう。

### 専門家グループを必要とする場合

平均的な CSIRT の規模を考えると、各チームがあらゆるオペレーティングシステムのバージョンやネットワークプロトコルについてすべて把握することはおそ

---

<sup>34</sup> Newsプロトコル。

らく不可能です。そのため、多くの場合は、他の専門家グループと分析プロセスを共有することが推奨され、その方が望ましいこともあります。作業の機密性のために、情報を共有したり分析を実施したりする前に、CSIRTとConstituencyの性質に応じて、専門家をあらかじめ特定し、適切な事前措置（適正審査や秘密保持契約など）を講じてください。

例：CERT-NLは、ある専門家グループと連携しています。これはCERT-NLのConstituencyからの専門家による自主的な活動です。専門家にとっては、新しい情報を直接受け取れるというメリットがあります。CERT-NLにとっては専門家のフィードバックが得られるというメリットがあります。

例：分析（たいていは脆弱性分析やアーティファクト分析）を実行するときにはより熟練したチームが共同で対応し、1つのチームが指揮し、残りのチームが「専門家」の役割を果たす場合もあります。

### 中止する場合

分析を中止したり、別の組織（別のアーティファクト分析サービスなど）に受け渡したりすることを判断するまでの、分析の深さと幅の限度を決める基準を事前に定めるべきです。中止するための判断基準としては、費やされるスタッフの労力の限界のような自明なものもあれば、問題の複雑さのように評価が変わっていくものに基づくものもあります。

### 3.4.2.5 ソフトウェア環境の分析

トロイの木馬プログラム、Ethernet スニファーログ、および攻撃スクリプトを分析する（すなわち、アーティファクト分析）だけは不十分です。パズルを解決して、全体像を理解するには、これらの残留物が見つかった環境の調査も重要です。例えば、攻撃スクリプトを取り上げてみましょう。そのようなスクリプトが想定どおりに動作するかどうかは、シェル環境、存在するソフトウェア、利用可能な権限などによって決まります。

運用状態のシステムは、何十もの実行中のプログラムやドライバ、そして何百もの実行可能状態にあるプログラムで構成されています。ファイルシステムはたいてい複雑で、各種の権限が多数のユーザとグループに半ばランダムな方法で分配されています。攻撃スクリプト自体は、それが何を行うかが分かるため分析は比較的簡単ですが、コードの中にランダムな一連のイベントが発生するような条件が含まれていたり、挙動を理解しづらくするように書かれていたりする場合があります。

実行可能形式の攻撃ファイルはまったく異なり、活動の分析結果を完全に理解するには、実行してみなくてはなりません。また競合条件（race condition）を使う攻撃手法（コードの実行が予期できない上に結果は不明）の場合は、試験環境の状況がオリジナルのソフトウェア環境に酷似していなければ再現できないため、より難しくなります。

ソフトウェア環境の分析はアーティファクト分析と緊密に関係しているため、その一方を他方から切り離すことはできません。その結果、アーティファクト分析に関する先述の内容の大部分はここにも当てはまります。本質的に

- アーティファクト分析を実行する人（Constituency、インシデントハンドリングサービス、または別のアーティファクト分析サービス）は、ソフトウェア環境の分析も行う必要があります。
- アーティファクトを取得して分析することは、オリジナルの環境をできるだけそのまま取得して反映することにもなります。できれば、同じバージョンのオペレーティングシステム、パッチレベル、ドライバ、および設定ファイルなどを使用してください。この要件は、アーティファクト分析がいかに入り組んでいて、複雑であるかを示しています。本当に求められるのはオリジナルの環境で分析を行うことですが、前述したように、当然ながら Constituency は実験台になるのをたいてい拒否するため、めったに実現しません。そのためのリスクが大き過ぎるのです。しかし、Constituency によっては、分析に参加する準備ができていたり、参加できる場合もあります（例えば、スキルのある技術スタッフがいて、すぐに投入でき、隔離したテスト設備も利用でき、時間もおり作業への関心も高い学術環境など）

アーティファクトとそのソフトウェア環境を分析することによって、（特定の環境の）特定のソフトウェアにおける既知の脆弱性が明らかになる場合があります。その場合は適切なアドバイスで被害者を支援し [Garfinkel 1996]、広範囲に及ぶ攻撃の場合は、「注意喚起」を Constituency や他の CSIRT に送ることができます。一方、分析によって未知の（少なくともパッチ未適用の）脆弱性が明らかになることもあります。その場合は、この問題を脆弱性ハンドリングサービスに転送しなくてはなりません。脆弱性ハンドリングサービスは、CSIRT 内またはチームの外部（信頼できる専門家、同業者、またはベンダチーム）に存在していることがあります。理想は、脆弱性に対してすぐにパッチを当てられ、影響を受ける全員に適切な情報が提供されることです。

### 3.4.2.6 「インシデント発生現場内」での関連性（Web-of-Relations）分析

高度な侵入者は通常、インターネット全体に接続網を張り巡らし、気に入った脆弱性を使ってシステムへのアクセス権を得て、そうして侵入したシステムを「踏み台」にして他のシステムを攻撃します。侵入者はこの接続網を複雑にして、発見されたり手がかりがつかまされたりしないようにしています。この接続網の中心を特定できれば（一連の侵入行為の中で最初に障害が起きたシステムなど）、犯人の発見や特定につながる場合があります。

例：侵入者が電話システムを利用し、公共のオンラインサービスの1つを経由してインターネットにアクセスしている場合、電話会社は侵入者が接続に使用した電話番号の追跡に協力してことがあります（この場合は通常、法執行機関が関与します）。

例：侵入者が公共の端末室（大学やインターネットカフェなどにある）から接続網を操作している場合は、侵入者を現行犯で捕える必要があります。犯



罪者が次に活動を再開する際、通常は、組織内の IP 番号を通してマシンの位置を追跡できます。しかしインターネットカフェ自身が攻撃を検知しようとしなければ、そうしたインフラの不正利用を特定することができません。

侵入者を見つけようとするときには、多大な注意を払う必要があります。その過程で、侵入者と調査員はともに同じシステムを利用するかも知れません。多くの場合、侵入者はシステムに対する最高の特権付きアクセス権（UNIX の root 権限など）を持っているため、アラートを受け取ったり、調査を妨害したりすることもできます [Stoll 1989, Shimomura 1995]。

「インシデント内」における関連性(Web-of-Relations)を分析することは非常に重要で、インシデントを封じ込めるのに役立ちます。侵入者の操作と関係を理解すればするほど、その活動に対抗したり、次の犠牲者が出ないようにしたりすることが容易になり、最終的には犯罪者を逮捕できる可能性もあるのです。

このような分析を行うときには、ログファイルに示された関係をたどり、侵入者のシグニチャを追跡してください。

#### ログファイルの関係の追跡

侵入に関連するログファイルまたはその一部（侵入者の活動の telnet ログ、スニファールログなど）を入念に調べ、他のシステムとの関連性をすべて調査してください。通常これは、知っておくべきという理由で、Constituency や他の CSIRT を巻き込み、ログの関係のある部分だけを提供することを意味します。ただし、仲間の CSIRT（または少なくとも正常な関係にあるチーム）にはアラートを出し、侵入者が用いたと思われる攻撃方法に関する情報を提供することをお勧めします。これは、他のチームが事前に対応したり、発生時に同様の活動であると認識したりするのに役立ちます。理想的には、逆の立場になったときに、他のチームが恩返しに情報を提供してくれることが期待されます。

調査の結果、関係のある新しいログファイルが見つかったら、これらも同様に分析する必要があります。これはかなり時間のかかる作業になることがあります。Ethernet スニファールログが関係するインシデントでは特にそうです。このようなインシデントによって、いくつかの CSIRT では、侵入されたおそれのあるシステムの影響を受けるサイトをすべて追跡し、通知するという膨大な作業が発生します。

#### 侵入者のシグニチャの追跡

インシデント全体に渡って、侵入者のシグニチャを抽出し、既知のシグニチャと比較する必要があります。シグニチャとは、侵入者が作業に取り掛かった方法、使用したスクリプト、試みたパスワード、破壊しようとしたプログラム、悪用した脆弱性、ツールを保存するために作成または使用したファイル名またはサブディレクトリ名です。

このシグニチャを追跡すると、侵入者に対する理解が高まります。また、シグニチャがまったく異なっているように見えるインスタンスも見つけることができます。侵入者が非常に独創的であったのかも知れませんが、偶然に見つかった別の侵入者のシグニチャかも知れません。あるいは、そのシグニチャは、複数の侵入者の共同作業と情報共有の結果かも知れません。1人の侵入者の痕跡を追うことで、その仲間の痕跡が見つかることもあります。こうした痕跡には、非常によく似ている点と、まったく異なる点の両方が表れていることがあります。

### 3.4.2.7 進行中のインシデントの構成の分析

個々の「インシデント内」のあらゆる関係を調査するだけではなく、別のインシデントを相互に比較する必要もあります（これにより、この節で前述した「全体像」の理解が高まります）。あらゆる分析活動において評価すべき主な項目として、ここでも同じ2つの点が代表的なものになります。すなわち、侵入者のシグニチャと、さまざまな関係の網です。

見た目上一貫性のあるインシデントを分析した結果、別の侵入者の痕跡が手続きを混乱させていることが分かることがあるため、複数のインシデントの構成分析によって、別々に扱われているインシデントがグループを成していることが分かることがあります。同じシグニチャを使った同じ侵入者から、もしくは類似またはほぼ同一のシグニチャと、関係の網を使って協力し合っている侵入者のグループから、類似点が見つかることがあります。あるいは、まったく異なる関係のない攻撃が同じ標的を対象としていることもあります。分析プロセスを通じてのみ、このような知識が得られるのです。

### 3.4.3 インシデント情報の追跡

どのようなインシデントも、そのライフサイクルの間に、インシデントに関連する情報をさまざまな詳細度で追跡することが非常に重要です。これにより、情報の整理と、効果的なインシデント対応が容易になります。論理的かつ組織化された方法で情報を記録することで、報告された活動と、取られたアクションの履歴にもなり、インシデントの作業負荷の分散と割り当てに役立てることができます。この記録は、統計情報と動向情報にもなり、ハンドリング機能内で、または他の機能やサービス（例えば経営陣やスポンサーへの報告書、顧客品質保証、スタッフの業績指標など）によって使用することができます。

記録する詳細のレベルは、具体的な要件、提供するインシデントハンドリングサービスのレベル、実施する分析の深さに基づいてチームごとに異なることが考えられます。あらゆるインシデントに対応するには、最低でも表 16に詳述した情報を取り込み、追跡するとよいでしょう。

個々のポリシーに応じて、チームはインシデント情報を必要になるかもしれない短期間だけ（インシデントをクローズした後の数週間や定期的に統計情報を作成する場合など）ネットワーク上に保管します。通常、情報はインシデントを再オープンする可能性を考慮して、少なくとも少し長めに保管します。ツールがインシデントの再オープンに対応している場合は、これは不可欠です。場合によって

は、最初の報告から1年（またはそれ以上）経ってインシデントの再オープンを経験することもあります。これは主に、そのサイトがインシデントの活動のログを定期的に見直していないことが原因ですが、何らかの事件が公判期日を迎えた結果であることも考えられます。チームや提供するサービスの性質に応じて、収集したインシデント情報全体を保管する必要はありませんが、履歴目的では役に立つこともあります。このトピックの詳細については、3.8節「情報のハンドリング」で説明します。

表16：インシデント情報の追跡

追跡する情報	説明
ローカル CSIRT 固有のインシデントトラッキング番号	チームが提供する一意のトラッキング番号。この番号は、インシデントに関するすべての情報とアクションの追跡に使用されます。
他の CSIRT のインシデントトラッキング番号	関係している他のチームが割り当てるトラッキング番号。この番号は、インシデントに関する他のチームとの適切な連絡調整を容易にします。
キーワードまたは分類	インシデントを分類し、異なるインシデント間の関係を設定するのに役立つ情報。この情報は、インシデントのライフサイクルで新しい情報を入手するたびに変わることが考えられます。
連絡先	インシデントに巻き込まれているすべての関係者の名前、電話番号、電子メールアドレス、その他の連絡先。これには、申請された暗号化方式と鍵の詳細も含まれています。
ポリシー	インシデントの処理方法に影響を及ぼす法的パラメータまたはポリシー。
優先順位	CSIRT の優先順位のスキームに従った、インシデントの優先順位。インシデントの優先順位は、ライフサイクルにおいて変更されることがよくあります。
その他の資料	ログファイルやハードコピー資料など、インシデントと関係がある他の資料の保管場所。
インシデント履歴	インシデントと関係があるすべての電子メールと他の通信（電話会話の詳細、ファックスなど）に関する記録。
ステータス	インシデントの現在のステータス
処置	インシデントに関する過去、現在、および将来のアクションのリスト。それぞれのアクションには特定のチーム番号を割り当てる必要があります。これらのアクションには、必要に応じて完了した日付や他の期日を記録することもあります。
インシデントコーディネータ	チーム内でこのインシデントへの対応を調整するスタッフを割り当てることがあります。このスタッフは常に空いているとは限らないこともあり、そのことが特有の問題を引き起こしますが、1人の人間が当該インシデントに関する全情報を確認するほうが全体像を把握できます。
品質保証パラメータ	サービス品質の評価に役立つ情報。このインシデントの処理に影響を与える可能性のあるサービスレベル契約（合意書）への参照。
文章による説明	他の追跡フィールドでカバーされていないその他の情報に対応する自由書式の説明

## 3.5 アナウンス機能

3.2節「サービス機能の概要」で前述したように、アナウンス機能は、Constituency に応じて情報をさまざまなフォーマットで生成します。アナウンスの目的はさまざまで、進行中の脅威の詳細情報、その脅威から守るために取ることができる措置、チームに報告された最近の攻撃の範囲と特徴に関して、不要な情報を取り除いた動向情報の開示などがあります。本書の目的に即して、この機能の範囲は、インシデントハンドリングサービスに直接適用できることに制限されます。しかし、広範なサービスを提供する CSIRT の場合、アナウンスを発行すること自体をサービスと見なすことができ、脆弱性分析やアーティファクト分析などの他のサービスから得た広範な情報を提供することが考えられます。

例：CERT Advisories [CERT/CC 1988] のようなアナウンスでは、インシデント報告、脆弱性報告、およびパッチに基づいたテストの結果として一般に発見される脅威の防止に関する情報と、ベンダコミュニティから得られたセキュリティの更新に関する情報を提供しています。

最初の CSIRT の設立以来、チームの Constituency へのアナウンスは、明示的なサービスであれ、インシデントハンドリングサービスの一部であれ、一般に何らかの形で CSIRT の日常業務の中に含まれています。しかし、前述のように、アナウンス機能は基本的なインシデントハンドリングサービスの提供にとって不可欠なものではないため、提供するかどうかは任意です。アナウンスの主な目的は、Constituency に情報を開示すること、システムの保護を支援すること、もしくは潜在的な脅威または現在や最近の脅威に関する情報を提供して、考えられる攻撃の徴候を探すこと、さらに脅威の検知、脅威からの復旧、または脅威の防止に関する方法をアドバイスすることです。特定の攻撃タイプに関する情報を開示するときには、受信者が脅威を理解し、チェックするには十分であるが、その情報を使って攻撃できるほど詳細ではないという開示レベルを保つように注意してください。これがアナウンス機能の最も難しい課題です。

アナウンスのタイプの一覧と、アナウンスのライフサイクルを3.5.1節～3.5.3節で説明します。Constituency へのアナウンスを作成する際に考慮すべき他の項目については、3.8.8節「情報開示」で概要を取り上げます。

### 3.5.1 アナウンスのタイプ

アナウンスは、進行中の特定タイプの活動に関する短期的な情報を提供するものから、意識の向上やシステムセキュリティの向上のための長期的な全般情報を提供するものまで、多岐に渡ります。それぞれに短所と長所があります。

#### 注意喚起 (Heads-up)

注意喚起は通常、短いメッセージの形式を取り、詳細情報が入手できないときに発行されます。その目的は、近い将来に重要になりそうなことを Constituency や他の関係者に知らせることです。注意喚起にはさまざまな利点があります。まず、CSIRT は Constituency に、考えられる問題や脅威について事前に警告したり、情報を提供したりできます。第2に、注意喚起で取り上げた問題について、受信者

の方が CSIRT よりも多少知っている（あるいは、それに関する追加情報を持っている）こともあります。このような場合は、Constituency がチームにフィードバックするチャンスになります。第 3 に、受信者が注意喚起の内容に関する情報に後日遭遇するかも知れません。この場合、受信者はその情報と潜在的な重要性を容易に認識できます。しかし、そのような形の情報は変わりやすいという抗議の声もあります（多くの場合、変わることが想定されます）。そのため、「注意喚起」の文章には免責条項を目立つように記載して、その情報が未確認で推測によるものである場合はその旨を明記します。

### アラート (Alert)

アラートは重大な進展に関する短期的な通知で、最近の攻撃、成功した侵入、または新たな脆弱性について、一刻を争う情報が含まれています。アラートの対象に関する完全な情報が既にあるかも知れませんが、新しい情報を発行する必要がある変更がなされている可能性があります。例として、「named」問題に関する CERT Summary [CERT/CC 1998b]、各種の CERT Incident Notes と Vulnerability Notes [CERT/CC 1998c、CERT/CC 1998d]、その他にも CERT Current Activity（現在の活動）のページ ([http://www.cert.org/current/current\\_activity.html](http://www.cert.org/current/current_activity.html)) にある最近の同様のアラートなどの文書があります。

### 勧告 (Advisory)

勧告は、CSIRT が発行する最も一般的な文書の 1 つです<sup>35</sup>。勧告は問題や解決策に関する中長期的な情報を提供するもので、意識を向上させたり、インシデントを回避したりするのに役立ちます。通常は、新しい脆弱性に関する情報が含まれていますが、侵入者の活動に関する情報も含まれています。勧告は多くの場合、十分に調査されており、パッチと回避策に関するかなりの技術的詳細が含まれています [Cormack 2002]<sup>36</sup>。勧告は通常、システム管理者やネットワーク管理者などの専門的な読者をターゲットにしていますが、専門的でない読者のために付加的な背景情報が含まれることもあります。例としては、CERT Advisories [CERT/CC 1988] などがあります。

### 参考情報 (For Your Information)

中長期的な情報が含まれた文書で、勧告に似ていますが、内容が短く、専門的でない広範な読者を対象にしています。これらは、概要 (brief)、速報 (bulletin)、またはニューズレターと呼ばれることもあります。このような文書には通常、セキュリティに関心のある非技術系の人が使用できるチュートリアルまたは教育的性質の情報が含まれます。この読者としては、経営陣や法務スタッフ、報道関係者も含まれます。例として、CIAC C-Notes（元々は CIAC ノートと呼ばれていました） [CIAC 1994]。

---

<sup>35</sup> 例えば CERT Advisory はおそらく CERT/CC の仕事を人々が認識する最も一般的な方法です。

<sup>36</sup> McMillan, Robert D. 『Vulnerability/Advisory Processes』、8<sup>th</sup> Workshop on Computer Security Incident Handling、FIRST (Forum of Incident Response and Security Teams)、カリフォルニア州サンノゼ、1996 年 7 月。

### ガイドライン (Guideline)

ガイドラインは、技術の基礎を理解している人の知識を広げ、また（システムまたはネットワークセキュリティの）直接的な向上にも役立つことを意図したプロセスを通じて、学習できる一連の手順です。ガイドラインには、非常に長い文書で、技術スタッフのセキュリティおよび日常業務に関する基本的な知識の向上を目的としたものもあります [CERT/CC 2000]。その他の例としては、Site Security Handbook [RFC 2196]、CERT Security Improvement Modules [CERT/CC 1997c] などがあります。

### 技術手順 (Technical Procedure)

技術手順はガイドラインよりもかなり長く、専門的な読者向けにより技術的な詳細が含まれており、たいていは特定の問題領域を対象にしています。この例としては、「Problems with The FTP PORT Command」 [CERT/CC 1998e] などの CERT Tech Tips や、Security Improvement モジュール「Security Public Web Servers」 [Kossakowski 2000] などがあります。

## 3.5.2 事前の検討事項

一連のアナウンスタイプを定義することが、包括的なアナウンスプロセスへの第一歩です。そのようなアナウンスを発行する前に、検討・対処しなければならない要素がいくつかあります。これらの要素は、アナウンスを発行する基準から配布方法まで多岐に渡ります。これらについては、以下で詳しく述べます。

### 3.5.2.1 アナウンスの引き金

何が引き金となり、各種のアナウンスが作成、配布されるのかを定めた基準を整備する必要があります。これらの基準は、単に別のチームの情報から得たことや、チームに報告されている現在の攻撃の急増を示す何かであることが考えられます。明らかに、基準を満たすために必要な情報は、定期的に追跡し、監視する必要があります。通常、情報源は、CSIRT 自体、報告された活動、チームで行った調査、または他のチームのアナウンスのいずれかになります。

### 3.5.2.2 分類基準

アナウンスの元になる情報を分類する際に役立つ基準、つまりその情報にふさわしいアナウンスタイプを選択するのに役立つ基準を作っておくと便利です。情報の出処に基づいた基準は定義しやすいですが、内容の種類に基づいた基準は定義が難しくなります。

例：Bugtraq などの公開メーリングリストから得た情報は、注意喚起につながるかも知れませんが、他の調査を通じて内容のダブルチェックや検証（またはこの両方）を行わない限り、勧告にはなりません（出処に基づく基準）。同様に、CSIRT で一般にウィルス問題に対応しない場合、ウィルスの新たな急増があっても勧告やガイドラインにはつながりませんが、アラートや注意喚起を発行することは考えられます（内容の種類に基づいた基準）。

元になる情報の内容を分類するときには、アナウンスの対象読者も考慮する必要があります。

例：Sendmail 攻撃に関する非常に専門性の高い情報は、一般の「ユーザ」ではなく、経験のあるシステム管理者を対象とした技術的に詳細な勧告を発行する十分な引き金になりえます。一方、広く使われている Web ブラウザにおける問題に関するそれほど詳細でない技術情報は幅広い読者を対象とした「参考情報」にするのがよいでしょう。

### 3.5.2.3 優先順位

いくつかの（多少は主観的な）要因が、個々のアナウンス自体の重要性に影響を与えます。特定のタイプのアナウンスだけでなく、その内容（例えば、サービス運用妨害攻撃やウィルスなど、さまざまなトピックのうちのいくつか）にも基づいて、アナウンスごとに客観的な優先順位を事前に割り当てる場合は注意してください。CSIRT は的確な伝達手段（アナウンスタイプなど）で的確な読者に適切な情報を発信する必要があります。

例：元々 CERT/CC には、Constituency に情報を公にアナウンスする手段は、1 つしかありませんでした。すなわち、CERT Advisory です。この種の文書は、システム管理者やネットワーク管理者が「注意を払う」べき重要な情報を CERT のスタッフが発信するための手段でした。これは非常に有効でしたが、話題によってその重要性は明らかに異なります。多種多様な情報を発信するために、1 つの発行手段だけでは、その発行手段の効果が薄れる可能性があります（例えば、すべてが最高の優先順位になることはできません。これはインシデントとアナウンスにも当てはまります）。

そのうち、CERT/CC は CERT Summary、CERT Incident Notes、CERT Vulnerability Notes、CERT Current Activity（現在の活動）など、他の通知方式を作り出しました。このようにして、CERT/CC は、Constituency（システム管理者やネットワーク管理者など）がすぐに精査し、その状況に応じて対処すべきだと CERT スタッフが考える最も重要な問題に対して「勧告（Advisory）」というアナウンスタイプを使用しています。CERT/CC の他の発行手段については、3.5.1 節を参照してください。

### 3.5.2.4 アナウンスにおける情報の許可

情報の開示を管理する CSIRT のポリシーと手順に応じて、アナウンスでの使用を目的とした情報には、適切なレベル（公開または制限付き配布）で開示の許可を与える必要があります。この手続きが実際にスムーズに進むように、一般的な許可ルールをあらかじめいくつか設定してください。

例：公開アナウンスの場合の明らかな許可ルールは、個人や個人のサイトに関する詳細を決して含めないというものです。もう 1 つのルールは、発信する情報が他のチームから得た情報に基づいたものか、単にその再配布である場合、そのチームから適切な許可を得る必要があり、適切な権利帰属を記載する必要があるということです。

### 3.5.2.5 配布チャネル

適切な配布チャネルを選択するときには、アナウンスのタイプに応じて、いろいろな問題を考慮する必要があります。

- 情報の機密性。配布チャネルは十分に安全か？
- 対象とする読者（Constituency）。読者に届けるのにチャネルは適切か？
- スピード。チャネルは十分に高速か？
- コスト。アナウンスを作成・配布することで期待される結果はコストに見合うか（時間、労力、素材、価値など）

配布チャネルに関するもう1つの問題には、情報を配布または発信する方法が含まれています。この問題については、3.5.3.5節「配布」で解説します。たとえメカニズムが適切だと考えられる場合であっても、事前に準備してテストしてから、Constituencyに周知してください。

## 3.5.3 アナウンスのライフサイクル

適切なアナウンススタイルと初期基準を決定したら、次のステップでは、アナウンスを実際に生成する際のプロセスと手順を定義します（タイプ、フォーム、スタイルなど）。一般に、この節で説明する5つの段階は、そのニーズに応じた最初のきっかけから最終的な配布まで、アナウンスのライフサイクルとして理解することができます。

### 3.5.3.1 開始

アナウンスの候補となる情報を発見したら（インシデント分析時、メーリングリストなどの考えられるソースの監視中など）、その情報が3.5.2節「事前の検討事項」に示した一般的な基準を満たしているか、すなわちアナウンスすべき重要な内容であるかを判断する必要があります。アナウンスすべきと判断された場合は、アナウンスのタイプ、内容の種類、および対象読者を明確にする必要があります。これは内部のトラッキング番号を割り当てる場合に役立ちます。これによりアナウンス作成の追跡／記録が容易になります。

トピック、アナウンスのタイプ、内容の種類、および読者の優先順位または重要性によって以下の重要なパラメータが決まります。

- アナウンスを記述するスタイルと詳細度
- 情報取扱許可手段
- 配布チャネル

その他、日程案、必要な内部リソース、業務の責任、他の関係者との協力（内容の提供、アナウンスの品質向上、他の協力者とのアナウンス発行の同期）などについても検討または決定する必要があります。



### 3.5.3.2 アナウンスに対する内部での優先順位付け

この段階では、現在作成中のすべてのアナウンスを定期的に見直します。アナウンスに関する複数の作業が（さまざまな作成段階で）同時進行することがあります。まだ発行されていないアナウンスは、事前に定義した基準と、内容の作成を始める時点で決められた他の関連する基準に基づいて優先順位が付けられています。特定のタイプのアナウンスが（その本来の性質からして）最も高い優先順位を付けられることがあります。例えば、一刻を争うアナウンスであれば、既に待ち行列にある他の重要なアナウンスよりも優先される可能性があります。一般的な統計情報を提供するだけのアナウンスは優先順位が最も低く、アナウンスの発行予定が後日に延期されることもあります。重要性が同じ2つのアナウンスの間でリソースが競合しているときには、相対的な優先順位がすぐには明らかにならない場合もあります。そのような場合は、対処する脅威または巻き込まれている Constituency の規模（または両方）など、問題の重大性に基づいて優先順位を付けることが最も適切なやり方です。

### 3.5.3.3 作成

この段階は、アナウンスの技術的説明、編集、および全体的な文章作成で構成されます。ほとんどのチームでは、アナウンスのタイプごとに、適したレイアウトと内容を示す標準テンプレートを作成しています。この「雛形」は、資料の作成を大いに円滑化し、アナウンスフォームの外見が統一されることで、Constituency はアナウンスの内容がどのようなものか予想しやすくなります。次に、アナウンスの草稿を内部と一部の外部へレビュー用に提出し、アナウンスの作成に直接的な責任のない専門家から詳細なコメントを集めます。この情報を他の関係者に提供するときには、何らかの使用制限を明らかにする必要があります。

例：レビューとコメントを依頼するために、アナウンスの草稿がすべての FIRST チームに送付されますが、草稿には「再配布禁止」と記載されています。攻撃や開示の可能性からさらに保護するためには、レビューとコメントのために配布するときに草稿とコメントを暗号化してデジタル署名を付ける必要があります。

### 3.5.3.4 最終準備

最終的に発信する前に、アナウンス自体または参照している項目の暗号チェックサムを生成するなど、いくつかの技術的問題に対処する必要があります。しかし、この段階で残っている問題の大部分は技術面ではなく、通常は、全体的な表示と内容（日付、ヘッダ、フッタ、謝辞、免責条項など）に関することです。アナウンスを発表する前に、含まれているすべての参照が有効（すなわち、URL とパッチファイルが正しく且つアクセス可能）であることを確認しなくてはなりません。

もう1つ、仲間の CSIRT やチームのメディア窓口など、一部の読者にアナウンスを事前に配布するべきかどうかを検討します。これにより関係者は、何らかの対応に備える機会が得られます。仲間の CSIRT の場合、これは独自のアナウンスの準備を意味することもあります。例えば、情報を別の言語に翻訳する必要が

ある場合や、アナウンスを独自の雛形を使って「仕上げる」場合などです。そうした場合、直前に変更が必要になることも考えて、最終的な開示のときまでアナウンスの開示制限を設けておくこと有効です。

例：いくつかの CSIRT では、勧告の最終草案を暗号化して、すべての FIRST チームに送信しています。ただし、その情報を利用して独自のアナウンスを準備することはできても、最終的な公開配布版が提供されるまでは、情報を自由に再配布することはできないという条件が付けられています。こうすることで、利害関係の問題が生じる可能性を最小限に抑えることができています。レビュー担当者の 1 人が最終的な公開配布日より前に情報を開示した場合、他の人がまだ機密事項だと信じている情報が漏れたことになり、プロセス全体が損害を受けることになります。

トリアージ、フィードバック、または他のインシデントハンドリング機能を提供するチームメンバは、アナウンスに対する Constituency、メディア、その他の関係者からの返信をコピーしたり対応の準備をしたりする必要があります。これらのチームメンバには、すべてのアナウンスについて事前の説明を行う必要があります。

最終的に、発信するすべてのアナウンスには、外部トラッキング番号を割り当てる必要があります。この番号は通常、アナウンスのタイプごとに順次割り当てます。次に、アナウンスには、改ざんされないようにデジタル署名を付ける必要もあります。

例：CERT/CC が配布するすべての CERT Summary には、CS-YYYY-XX という形式の番号を付けます（YYYY は Summary を発行した年で、XX という番号は、その年に発行した各 Summary に 01 から順次割り当てます）。真正性と完全性は、PGP（または GPG）で生成されるデジタル署名で確保します。これは他の CERT 文書（CERT Advisory、Incident Notes、Vulnerability Notes など）にも当てはまります。

### 3.5.3.5 配布

配布とは、アナウンスのタイプごとに定められた配布方法を通じて、最終的なアナウンスを配布または発信するための取り組みに関連する活動です。これには、チームの FTP サーバや Web サーバなどの適切な情報サーバへのアナウンスの配置、メーリングリストなどの他の方法による配布、FAX による自動配信、またはニュース配信メカニズムなどが含まれます。

例：CERT/CC は多くのアナウンス（CERT Advisory や CERT Summary など）を、cert-advisory メーリングリストとして知られているメーリングリストや USENET ニュースグループの comp.security.announce に発行しています。後者は CERT スタッフによってモデレート（内容確認）されており、CERT のアナウンス専用に使われることを目的としています。また、CERT/CC では、すべ

てのアナウンスを（メーリングリストやニュースグループを通じて直接開示しないものも含めて）Webサーバに保管しています<sup>37</sup>。

## 3.6 フィードバック機能

大部分の CSIRT の主な目的は、インシデントからの復旧とインシデント対応のための支援を提供することです。この役割において効果が上がると、インシデントハンドリング活動に必ずしも限定されない要請（もしくは、おそらく Constituency に提供される CSIRT のミッションやサービスの一部ですらない要請）や問題が、チームに向けられることがあります。残念ながら、CSIRT の役割と責任の範囲を超えている場合であっても、そのような要請や問題を無視すると、それだけでチームの評判やチームに対する Constituency の姿勢に影響を与ることがあります。したがって、そうした要請に対して、最低限のレベルで適切なフィードバックをある程度提供することはすべての CSIRT の利益に繋がるのです。

その一方で、ナレッジマネジメントの見地からすれば、この種の要請により、CSIRT は Constituency の現在のニーズを洞察でき、チームにさらなる利益がもたらされる可能性もあります。明らかな問題点や誤解を無視せずに、そのような要請に対してフィードバックを提供すれば、結果的により良いサービスを提供し、同時に Constituency の期待を明確にすることができます。CSIRT は、どのような要請であっても（たとえ、「サービス範囲外であるためこの要請には対応できません。」という回答や、他の情報源を紹介する返答になったとしても）、要請に応えられるように懸命に取り組まなくてはなりません。

例：質問への返答がないと、要請した側は、そのチームが役に立たないか、支援の能力がないと考えるかも知れません。または、そのチームが横柄である、あるいはそれ以上に悪い（管理が悪い、連絡体制がいい加減、など）と考える人もいるかも知れません。このように認識されないために、少なくともチームの目的と、これ以上のフィードバックを提供できない理由を伝える必要があります。こうした要請のいくつかは、公開されていない情報を引き出すとする「調査報道」目的の可能性もあり、さまざまな形でやってくる可能性がある点を念頭に置いてください。

受け取る要請は通常、次の4つのいずれかのカテゴリに分類されます。

### 1. コンピュータセキュリティ全般に関する要請

通常、このような要請では、予防的なセキュリティ対策を通じたインシデント回避に関する情報や、インシデントが発生した場合に CSIRT に連絡する方法に関する情報などが求められます。CSIRT は、何度もインシデントに対応しているため、この種の情報を提供するだけの知識があります。したがって、このような質問をチームに投げかけるのは当然だと人々は考えます。チームは、可能なときにはいつでも、このような機会を利用して積極的に Constituency の意識の向上を支援し、インシデントを回避（あるいは抑制）し、全体的なセキュリティを改善する必要があります。

---

<sup>37</sup> <http://www.cert.org/>

## 2. メディアからの要請

これは一般的なセキュリティ記事、アナウンス、または特定のインシデントに関する話を求めているメディアからの要請です。CSIRTは、チームの情報開示ポリシーに違反せず、可能なときにはいつでも、メディアからのこのような要請に適切に対応できるように準備しておく必要があります。

## 3. 他の要請と問題

上記以外に、Constituencyが提起する、またはチームがフィードバックしたいと考えるさまざまな要請と問題が存在します。これには、会議での講演依頼や、チームから入手した著作権のある資料の利用許可の申請なども含まれます。このような要請に対応すれば、チームの認知度を高める効果があります。要求が実現可能で適切なものである限り、無視してはなりません。CSIRTの年次報告書の送付は、要請に対する応答ではなく情報を積極的に広めることですが、この一般カテゴリに分類できます。

## 4. 範囲外の要請

この要請は、CSIRTが提供するサービスとは関係ありません。しかし、たとえそうであっても、前述のように、よくある質問（FAQ）への参照を添えた簡単な受領確認を送る、もしくは範囲外の要請の対処方法に関するポリシーを伝える方が、ただ無視するよりも有益です。

例：明らかに範囲外によくある実例を以下に示します。---インターネットに接続するにはどうすればいいですか？---ドイツのハンブルクに住む私の旧友の住所がわかりますか？---ペンパルが欲しいです---。これ以外にも、CSIRTが提供するサービスの範囲を超えているものがあります。例えば、---私のネットワークに侵入テストを行ってくれませんか？---オペレーティングシステムのバージョン/アプリケーション/ソフトウェアツールは、どれを使ったらいいでしょうか？---、などです。

### 3.6.1.1 ライフサイクル

さまざまなタイプの要請に、さまざまなタイプのトラッキング番号を付けて追跡することができます。あるいは、1つのタイプのトラッキング番号を持つすべての要請を追跡したり、異なるタイプの要請や、要請ごとに提供した応答の種類を記録に残したりすることができます。要請には、インシデントのライフサイクルと同じようなライフサイクルがあります。ただし、これらの要請がチームからの最初の回答の後、長期に渡ってオープンの状態のままになることはまれですが、要請によってはさらなる対話が必要になることがあります。

### 3.6.1.2 FAQ およびその他のデフォルトのフィードバック

要請への応答は個別に行うこともできますが、多くの場合、これでは時間がかかります。また、CSIRTもこの作業に専念するリソースを投入できないこともあります。そこで、大部分のチームでは、前述のようにFAQなどの文書を事前に作成して準備しています。このような文書では、チームについての一般的な質問への回答、チームが提供するインシデントハンドリングサービスの詳細情報、Constituencyに合わせてカスタマイズされた、特定のニーズに対応する文書へのアクセス方法などを提供します。このような文書があれば、該当する文書の提供場所を示したり、または該当する文書のコピーを提供したりすることによって、

大部分の要請に応えることができます。たとえ範囲外の要請であっても、FAQでチームのサービスを概説し、それ以外の要請はすべて不適切であることを示せば、FAQが適切な応答となり得るのです。その一方で、CSIRTには要請された情報がない（したがって提供できない）ことを要請者に丁寧に伝える簡単な標準応答文を作成しておくといよいでしょう。

例：新しく結成されたCSIRTでは、最初はよくある種類の要請を明らかにするためにConstituencyからの要請を追跡し、その要請に応答し、それから、そのような一般的な（あるいは似た）要請にすぐに対応するためのFAQを開発するという選択が可能です。やがて、そのようなFAQは、更新され拡張されて、チームのWebサイトに置かれて将来の要請に備えることとなります。CSIRT Development TeamのFAQは、このような方法で発展してきました[CERT/CC 2002b]。

メディアからの要請に対しては、チームはそのポリシーに応じて、組織の既存の広報室を使用する、またはメディアとやり取りした経験のあるチームメンバーや同僚を通してメディアとやり取りすることが考えられます。メディアからの接触要請をどこに向けるかについてポリシーを確立したら、メディアからの要請にはすべて、そのポリシーに従って対応する必要があります。また、付加的な支援をフィードバック機能によってメディアに提供する必要はありません。ポリシーに応じて、FAQなど、チームについて公に入手できる情報をメディアに提供することが適切な場合もあります。

### 3.6.1.3 フィードバック機能の編成

標準問答集があれば、詳細な技術知識のない技術スタッフや、直接的なWebインタフェースによっても、この機能内のよくある問い合わせに対してフィードバックを提供することができます。あるいは、別のチームによって提供されている技術ガイドラインのオンラインアーカイブのような他の情報源や、他の技術専門家を紹介することも考えられます。

チームメンバー向けに、各種の要請への対応手順を示した内部用FAQ（またはその他のガイドライン）を用意することも非常に有益であり、これによってどのような要請に対しても首尾一貫した対応が保証されるとともに実現可能になります。このような文書には、要請の優先順位の付け方も詳述されている必要があります。例えば、スポンサーからの要請の優先順位が最も高く、Constituencyからの要請がこれに続くかも知れません。あるいは、要請者ではなく要請のタイプに基づいて優先順位を付ける場合もあります。内部用FAQは、新しいCSIRTスタッフメンバーのための学習ツールとしても使用できます。

## 3.7 やり取り

インシデントライフサイクル全体を通して、CSIRTの大部分の活動は、他の関係者とのやり取りを伴います。このようなやり取りは重要であり、影響も生じるため、「適切な」関係者と連絡がとれるように十分な注意を払う必要があります。

(3.7.1節「連絡窓口」を参照)。大部分のやり取り(すなわち通信)では、真正性を保証すること(3.7.2節「認証」と機密性を保つこと(3.7.3節「安全な通信」)も同様に重要です。この節の最後では、Constituency、他のチーム、法執行機関とのやり取りなど、特に重要なやり取りについて考慮すべき項目の概要を取り上げます(3.7.4節「特別な考慮事項」)。次の例は、サイトとCSIRTに否定的な影響を与える可能性のある事象について示しています。

例：あるインシデントが進行中であるとします。誰かがCSIRTに電話をかけ、自分はサイトAの管理者だと名乗りました。そこでCSIRTは、インシデントの技術的詳細と適切な技術的解決策を提供しました。翌朝、インシデントに関する詳細な報告とともに、被害に遭ったサイトAを特定する暴露報道がありました。結局、あるジャーナリストがインシデントに関するうわさを聞きつけ、チームをだまして情報を提供させたことが判明したのです。

例：CSIRTとサイトAの間の暗号化されていない電子メールメッセージが、インターネットメールホストでの保管中に第三者によって傍受され、コピーされました。その後、この電子メールは、大勢の読者を抱えるインターネットニュースグループに配信されました。

その一方で、次の例のように、効果的な通信は非常に肯定的な影響をもたらす可能性があります。

例：CERT/CCは2002年2月、CERT Advisory CA-2002-03「Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)」を発行しました。この勧告の作成と準備にあたり、「適切な」連絡窓口を特定し、そこと確実に連絡が取れるように、多くのベンダ連絡窓口を新たに定める必要がありました。この勧告は、多数のベンダ(100社以上)や他の専門家との調整、安全な通信、やり取りが関わるもので、今日までに発行されたうち、最も複雑な勧告の1つです。ほぼ1年後に引き続き作成されたベンダ情報の最新版は、ベンダコミュニティから新情報として提供されました<sup>38</sup>。

### 3.7.1 連絡窓口

連絡窓口は、インシデントの過程で必要に応じて設定されます。しかし、「正しい」、つまり適切な連絡窓口を設定することは、それ自体が1つの技術です。情報を伝えることも重要ですが、より重要なのは、情報の処理および受け取りに最も適した人物やアクションを講じたり必要な決定を下したりする権限のある人物を見つけることです。したがって、インシデントハンドリングプロセスのニーズを満たすために信頼の輪(Web of Trust)を構築するという目的を持って、適切な連絡窓口の設定と保守をCSIRTの継続的な取り組みとして遂行しなくてはならないのです。

---

<sup>38</sup> この勧告の印刷版は、CERT Webサイトにあり、50ページ以上あります。

ここでの目的では、連絡窓口は、インシデント関連の連絡窓口と、非インシデント関連の連絡窓口という2つのカテゴリに大きく分類できます。詳細は次の節で説明します。

### 3.7.1.1 インシデント関連の連絡窓口 (Point of Contact : POC)

これは、CSIRTが特定のインシデントに対応する際に必要とする連絡窓口です。インシデントに遭遇している組織の内部および外部の連絡窓口を含めることができます。このような連絡窓口の例を次に示します。

- 上層経営陣（経営幹部、課長、部門長、局長）
- スポンサー
- 他の部門
- 技術（システムおよびネットワーク）管理者
- セキュリティ担当者
- 法律顧問または法令遵守部門
- 内部監査部門
- リスク管理グループ
- ネットワークオペレーションセンター
- ネットワーク情報センター

大規模な組織では、CSIRTがその特定のサイトで発生しているインシデント報告について通知する、最初の連絡窓口（POC）があらかじめ決まっていることがあります。しかしその後、活動に対応できる特定の部門や適切な担当者との連絡が取れるように取り計らってもらうことが必要になる場合があります。適切な技術または管理レベルのスタッフに直接連絡できなければ、CSIRTは貴重な時間とリソースを浪費してしまうことになりかねません。

### 3.7.1.2 非インシデント関連の連絡窓口

非インシデント関連の連絡窓口は、チームに（またはチームに関する）背景情報を提供し、そのサービスの実施を支援し、場合によってはチームの活動を支援するのに利用できます。あるいは、特定分野の専門家から情報を得るために利用することもできます。次のリストは、連絡窓口データベースの作成時に考慮に入れることのできる、非インシデント関連連絡窓口の一部を分類した例です。

- (Constituency) サイトのセキュリティ連絡窓口
- その他の Constituency サイトの連絡窓口（管理、物理的セキュリティ、人材など）
- Constituency 外部のサイト
- インターネットサービスプロバイダ
- 別の CSIRT
- 法執行機関、法律顧問

- ベンダ
- 専門家
- メディア

### Constituency サイトの連絡窓口

前述のように、1つの組織内でさまざまな種類の連絡窓口を保持するのには極めて正当な理由があります。それはエスカレーションが必要になることが考えられるためです。通常、1つの部門と協力してインシデントに対応することは妥当ですが、管理権限または監督を要する結果をインシデントが招いている、あるいは、インシデントが複数の部や課にまたがっていることが明らかな場合は、上層経営陣が関与する必要があります。

#### 3.7.1.3 連絡窓口の特定

組織の適切な連絡窓口を見つけることは、必ずしも簡単な作業とは限りません。さほど重要ではない連絡窓口の場合は、電話帳や、それと同様のサービス、例えば CD-ROM やインターネットでの検索を通じて提供されるサービスのような公に入手できるリソースを利用することが可能です。

連絡に基づいて重大な決定を下す必要がある場合に間違った連絡窓口を使用すると、不適切な関係者や（たいてい悪質な）部外者に重大な情報が漏れてしまうことがあります。このことは、CSIRT 内の管理の欠如、および細部への配慮の欠如を証明することにもなり、評判を落としかねません。

Constituency の信用を維持するために、正しい連絡窓口を特定（調査）し、利用するには十分な注意を払う必要があります。一般公開されている連絡窓口情報が偽造、改ざん、破壊されている可能性（印刷媒体や CD からネットワークディレクトリサーバまでさまざまなリスクを伴う非常に現実的な脅威の可能性）がある場合は、使用前に確認する必要があります。より望ましいのは、情報源から直接、あるいは連絡窓口自体またはその管理者（もしくは指名された代表者）から直接、連絡窓口情報を入手することです。

#### 3.7.1.4 連絡窓口の保守

これは一見すると簡単な作業のようですが、実際のところ連絡窓口情報の保守は、連絡窓口情報を見つけることより手間がかかり、難題である場合があります。人々が退職したり、昇進したり、他の職務に配置転換されたり、電話番号が違う別の机／オフィス／ビルに移ったりすれば、その連絡窓口情報は（部分的に）古いものになります。この種の変更にに関する情報を伝えてもらうように連絡窓口（例えば Constituency サイト）に依頼することもできますが、現実には連絡がもらえることはめったにありません。重要ではない連絡窓口の場合は、古い情報や間違った情報がデータベースに存在する可能性を受け入れ、正しい情報が分かったときに情報を修正するというのが最善の方法です。しかし、重要な連絡窓口の場合、この方法はあまり適切ではありません。変更や更新を伝えてもらうように連絡窓口に依頼することに加えて、定期的（3 か月ごと、半年ごと、年 1 回、契約の変更時など）に点検することがこの問題の解決に役立つでしょう。



例：CERT-NL は、管理者が「サイトのセキュリティ連絡窓口（SSC）」を指名し、連絡窓口情報（および関連する変更）を CERT-NL に伝えるように各 Constituency に求めています。実用的な理由から、Constituency がサイトのセキュリティ連絡窓口用に `ssc@somesite.nl` という形式の総合的な電子メールアドレスを作成することも勧めています。その場合、現場の管理者が電子メールアドレスの保守を担当します。これにより、CERT-NL が事前に関与することなく情報を伝達できるようになります。また、CERT-NL は、`sep@somesite.nl` という形式の電子メールアドレスで「セキュリティエントリポイント」を作成するように Constituency に勧めています。このセキュリティエントリポイントは、サイトのセキュリティ連絡窓口が休暇を取ったり病気になったりする可能性を考えて、それとは別に、インシデントや他のセキュリティ問題にリアルタイムで対応することを目的とした、ローカル CSIRT のようなものです。

例：別の CSIRT は、少なくとも RFC により規定されているドメインごとの「postmaster」および「security」用標準電子メールアドレスを提供するように勧めています。

### 3.7.2 認証

他者とやり取りする際に重要になるのは真正性です。この用語は通常、その人が本当に、名乗っているその人であることを保証するときに使用されます。専門的な通信設備を使用することにより、呼び出し元または呼び出し先の真正性を確認することが本質的にいっそう難しくなります。したがって、十分に注意を払う必要があります。保護しなければならない情報は、呼び出し元または呼び出し先のどちらかが認証されていて、且つもう一方によるその情報へのアクセスが許可された場合にのみ、明らかにされるようにする必要があります。後になってこの情報が重要になることもあるため、各連絡窓口とその発信元はログに記録しておく必要があります。

その人が、名乗っている本人であるかどうか確認することも重要ですが、それだけでは不十分です。妥当性と権限も重要です。真正性の確認に加えて、その組織の対話相手としてその人が「正しい」、つまり適切な人であるか判断することも不可欠です。ここで述べた「正しい」とは、その人が情報について受け取り、受け入れ、措置を許可されているという意味です。

例：インシデントの発生中に、XYZ という組織のセキュリティ管理者に電話がかかってきました。しかし、その管理者が電話に出られなかったため、代わりに秘書が対応しました。秘書の本人確認はできるかも知れません。しかし、管理者宛てを意図した詳細情報について秘書と話し合ったり秘書に明かしたりすることは適切ではない場合があります。できるだけ早く電話をかけ直すように管理者に伝言を残すことが適切な場合もあります。

あるいは、XYZ の上級管理者が CSIRT に電話をかけて、その同じインシデントに関して取るべきあらゆるアクションを尋ねることもあります。この人物が、そのような問題に対するチームの登録連絡窓口でなければ、CSIRT は

(該当する場合) 適切な「指揮系統」を介して要求が行われるように、その組織の登録連絡窓口に要求を差し戻す必要があります。

このような認証手順が整っていない場合、チームとその Constituency は、潜在的にソーシャルエンジニアリング攻撃（後述）を受けやすくなっていると言えます。

### 3.7.2.1 ソーシャルエンジニアリング

ソーシャルエンジニアリングとは、誰かが偽の識別情報を提示して他人をだまし、本当の識別情報を知っていれば通常行わない何かを行わせるという状況を表す、CSIRT コミュニティでよく使用される用語です[Gordon 1995、Greening 1996]。

(前述の例のような) ソーシャルエンジニアリングの典型的な例は、誰かが高級官僚を装って警備員に電話をかけ、門を開けるように命じるというものです。そして驚くことに、これに似た強引な心理的攻撃が今なお成功している形跡があるのです。このタイプの攻撃で比較的良好に知られている2つの例を次に示します。

- **メディアからの一方的な電話**

メディア関係者は、インシデントが発生していると考えた場合、内部情報を得ようとする場合があります。彼らが身元を隠す、あるいは明示的に「別の被害者」を装うことで、チームメンバは被害者の復旧を支援しようとして情報を明かしてしまう可能性があります。

- **侵入者からの電話**

ソーシャルエンジニアリングは、侵入者によく知られた手法です。侵入者は、CSIRT が自分の活動（侵入など）を監視している可能性があると考えた場合、その活動が既に検知されたかどうかを明らかにしようとしてチームに電話をかけてくる場合があります。また、前述のメディアの例のように、活動に関する情報を引き出すために、サイトの連絡窓口を装う場合もあります。

人々をそそのかして添付ファイルを取り込ませたり URL を訪問させたりするためのよく知られた策略に、別のソーシャルエンジニアリング手法を見ることができます。これには、悪意のある副作用が含まれることがあります。

例：電子メールに関して言えば、疑うことを知らない受信者に一方的な電子メールが送信されます。このような電子メールには、返信アドレス、興味をそそるエンベロープ、あるいは他にも受信者が電子メールを開きたくなるような何かが含まれる場合があります。悪意のある電子メールには、往々にして、我々が知っている誰かの返信アドレスが記載され、興味をそそる言葉が件名に並べられています。だまされやすい受信者は、そのようなメッセージの扱いに対してしかるべき注意を払っていない可能性があります<sup>39</sup>。

---

<sup>39</sup> 「Home Computer Security (家庭用コンピュータのセキュリティ)」について、Constituencyの助けとなる、ソーシャルエンジニアリング攻撃（およびそれ以外のコンピュータセキュリティ問題）に関するさらなる情報が記載された読みやすい記事がCERTのWebサイト (<http://www.cert.org/homeusers/HomeComputerSecurity/#3>) から入手できます。

### 3.7.2.2 技術的な可能性と制約

ISDN などの最近の通信設備には「発信者 ID」機能があります。この機能では、発信者の電話番号が呼び出し先に通知されます。電話機にディスプレイが付いていれば、電話を受け取る人に発信者の電話番号を示すことができます（ただし、発信者 ID をブロックする機能もあります）。

専門的な通信設備によっては、真正性の証明や検証の機能をサポートしている場合もあります。今日のネットワークに関して最もよく知られている認証方法の 1 つは、安全な電子メールシステムである PGP や S/MIME などで使用されているデジタル署名です。

例：送信されるすべての電子メールの発信元を認証するために、PGP で生成されたデジタル署名によって、各電子メールメッセージが DFN-CERT からのものであることが認証されます<sup>40</sup>。受信者はみな、PGP でこの署名を検査（検証および認証）できます。この検査は、DFN-CERT のメンバがデジタル署名に使用する公開鍵の真正性に依存しています。そのため、DFN-CERT チームメンバ全員の発行済み PGP 公開フィンガープリントを使用して署名を検査するのは受信者の責任となります。

S/MIME などのその他のツールでは、認証局 (CA) または信頼のおける第三者 (TTP) がユーザの真正性、およびユーザと公開鍵との関係を検査するという階層的な鍵認証プロセスを使用します。CA または TTP は、この情報を証明できた場合に、この鍵の真正性を保証します。

デジタル署名では、対応する暗号化機能を使用することによって、高い真正性を確保し、開示やその他の攻撃から保護できるという点を認識することが重要です（例えば、PGP と S/MIME はどちらもこの能力を備えています）。また、使用するメカニズムの制約を理解し、その制約の中で各メカニズムを使用することが重要です。固有の問題やトレードオフが存在する場合は、組織的なアプローチを取ることが、必要なセキュリティの確保に役立ちます。

例：CERT-NL では、毎年新しいチーム鍵を使用しています。チーム鍵は日常業務で使用されるため、多かれ少なかれ、インターネットに直接接続されているシステムに保存されています。しかし、常にオフラインで（インターネットに接続されているホストでは決して使用されず）、厳密な手続きによって使用が管理される CERT-NL マスタ認証鍵もあります。新しい CERT-NL チーム鍵は、生成されるたびに、このマスタ認証鍵によって署名されます。CERT-NL スタッフメンバのすべての鍵も、このマスタ認証鍵によって署名されます。このシステム全体が、現実的な要求とセキュリティをきちんと満たしているのです。Constituency は、スタッフ鍵がマスタ認証鍵によって適切に署名されていることを検証する必要があります。その後は、スタッフ鍵を検証するために各スタッフメンバの指紋を 1 つ 1 つチェックすることなく、

---

<sup>40</sup> 他の多くの CSIRT も、メールおよび CSIRT が作成または配布するその他の文書に PGP 署名しています。

スタッフ鍵を安全に使用できます。このプロセスを迅速に進めるために、すべての Constituency は公開マスタ認証鍵を取得して検証する必要があります。

### 3.7.2.3 データベース

ツールが関連するもう1つの領域は、情報データベース、特に連絡窓口情報が格納されるデータベースの使用についてです。内部データベースは、やり取りのプロセスと CSIRT 通信インフラの重要な部分を形成するため、十分に注意して保護する必要があります。攻撃者がデータベースを不正に操作できた場合、データが改ざんされてしまい、外見上は認証済みのデータが入力され、チームメンバがそのデータを信用してしまうことも起こりえるのです。

この同じ問題は、公開されている情報源を使用する場合にも存在します。現在、不正操作の可能性はますます大きくなっています。そのため、CSIRT が築く、そのような情報に対する信用は限られたものになります。

例：DNS システムと Whois データベース（どちらもインターネットで広範に渡って使用されるディレクトリサービス）は、より適切な連絡窓口情報が入手できない場合に、被害に遭ったサイトと連絡を取るのに使用されることが少なくありません。ただ、別のシステムの DNS サーバになりすますことが可能であるため、どの公開情報サーバも「信用できない」と考える必要があります。入手できる情報の真正性が疑問視されるだけでなく、データの完全性に疑いを持たれるのも当然のことです。例えば、Whois 情報は、古かったり、エラーが含まれていたりすることがよくあります。このような欠陥により、最悪の場合、不適切な人間に情報が渡されるということが起こりかねません。

例：ヨーロッパでは、European CSIRT のディレクトリが Trusted Introducer サービスによって管理されています<sup>41</sup>。このサービスは、European CSIRT の関連レコードを Whois データベース（IRT オブジェクト）に保持しています。これにより、IP アドレスに基づいて担当 CSIRT を検索することができます。

### 3.7.2.4 匿名情報

最後の領域は、チームが匿名の電話、またはまったく認証できない電話に対処する方法です。電話をかけてきた人が匿名なら、機密情報や重要情報を渡すべきではありません。しかし、新しい情報が提供された場合、チームは、その情報が役立つものであるか、また、その情報に対処すべきか（そしてどのように対処すべきか）、判断する必要があります。提供された情報は検証できないこともあります。したがって、情報にタグを付けてその旨を示す必要があります。また、その匿名の発信元にもタグを付ける必要があります。匿名情報の利用について検討する最も道理にかなった理由の1つは、例えば警告を知らせたのが匿名の発呼者であろうがなかろうが、警告そのものに違いはないということです。どちらにしても、安全のために、その警告が確かなものであるかどうかは確認します。

---

<sup>41</sup> Trusted Introducer サービスの詳細については、<http://www.ti.terena.nl/teams/index.html#DIR> を参照してください。

### 3.7.3 安全な通信

重要データの発信元を認証することは、安全なデータ処理のほんの一部に過ぎません。ネットワーク間での情報伝送時に情報を保護するのに適したセキュリティメカニズムを選ぶことも重要です。これは、コンピュータ、電話、およびこれ以外の通信ネットワーク（リモートシステムおよびリモートアクセスを含む）だけでなく、攻撃（または紛失）に対して脆弱でもある郵便や宅配業者などの伝統的な方法によって送られる情報にも当てはまります。

暗号化メカニズムは、真正性を保証するのと同じ方法で機密性を保証できます。効率良い暗号化メカニズムがいろいろありますが、さまざまな理由により、一般的に許可されていないものや、国外に輸出できないものがあります（政府による規制）。

暗号化メカニズムが使用される場合は常に、ポリシーと運用手順による鍵管理が、対処すべき重要な問題になります。

例：FIRSTでは、電子メール通信の保護にPGPを使用しています。多数の関係者で公開鍵暗号化を使用するのは大変難しいため（2003年1月、FIRSTには約130のメンバチームがありました）、従来の（対称）暗号化が使用されています。全FIRSTメンバは、定期的に変更される同じパスフレーズの知識を共有しています。さらに、真正性を証明するのにデジタル署名も使用できます。これにより、他のチームがメッセージの発信元を確認できます。鍵の使用および保守の手順は、FIRSTメンバに配布されています[FIRST 1998]。

通信ネットワークの場合、機密性が常に通信サービスのデフォルト機能というわけではないため、追加のブラックボックスを利用することもあります。このような暗号化装置は、一般向けに販売されているので簡単に入手できます。ただし、実現される保護機能は、実装や、全世界における製品の入手可能性を制限する輸出規制などのその他の要因によって決まる場合があります。

例：一部のチームでは、通信を保護できる Secure Telecommunication Unit (STU III) または SECURE TERMINAL EQUIPMENT (STE) といった装置を使用しています。このような装置は、特別なハンドリング／報告手順と利用要件を持つ被制御装置であり、特定の利用コミュニティ（例えばアメリカ、カナダなど）に限定されています。

例：他の国々でも GSM 携帯電話または ISDN 接続用の暗号化技術が開発されています。通常、そのような技術のアプリケーションは、その同じ技術を共有し、必要な暗号鍵を交換している通信相手にのみ効果があります。

### 3.7.4 特別な考慮事項

次に、ある特定の環境に固有のやり取りに関する考慮事項を示します。その目的は、既に述べたやり取りについて実践的な考慮事項を説明することです。やり取

りに関わる関係者については詳しく説明しませんが、重要な問題について例を通じて説明します。

対話を行う際に、チームがそのポリシーおよび手順で対処すべき最初の問題の1つは、別のグループに提供してもかまわない、もしくは提供することができるサービスのレベルです。この記述には、応答時間などの詳細が含まれることがあります。あるいは、情報交換のための特定の形式について述べられている場合もあります。これにより、使用可能なリソースが検討され、特定のタスクおよび優先順位に割り当てられます。

各チームの状況はさまざまであるため、以下の例では可能な限り、とるべき有益なアプローチと避けるべき落とし穴の両方を示します。ここに示す例では、予想される多様な関係者を取り上げていますが、これ以外の関係者が存在する可能性も確かにあります。とはいえ、考慮すべき最も重要なやり取りを取り上げたという確信もあります。特定された他の関係者は、たいていの場合、下記のカテゴリのいずれかと同様に扱うことができます。あるいは、メディアとのやり取りもほぼ同じです（すなわちオープン、公開、不明）。

#### 3.7.4.1 Constituency のサイト

CSIRT の主な目的は、その Constituency を支援することです。考慮すべき問題の大部分は、本書のこれまでの節で既に取り上げています。やり取りに関して1つ追加して述べる必要がある考慮事項としては、1つのサイト内においても各種の連絡窓口が必要であるということです。当然、サイトで同じ人が複数の役割を果たしている場合、サイトの連絡窓口は1つしかないこともあります。

インシデント対応におけるエスカレーションプロセスでは、意思決定（法執行機関に報告するための決定など）を必要とするため、エスカレーションの段階ごとに連絡窓口が必要となります。

例：インシデントの技術的な詳細は、ネットワーク接続の日常業務を担当する管理者に渡されますが、一部の情報は経営陣にも伝えなくてはなりません。例えば、新しいインシデントを報告するサイトが既に法執行機関に通知している場合、他のサイトは、この事実を考慮しながら独自の決定を下せるように、この情報を把握する必要があります。その一方で、この情報はその CSIRT が利用できるようにはならない場合があり、その場合は他に渡すことはできません。

CSIRT は、ポリシーおよび手順を定義する際、ある特定の活動が他のすべての活動に優先しなければならないほど重要なものがある場合を除き、単一サイトまたは Constituency がチームの使用可能なリソースをすべて消費してしまわないようにする必要があります。人員が限られる時期（例えば休暇や会議など）は、対応可能なスタッフに活動を分散するために優先順位付けがよりいっそう重要になります。

文書化され、一般に公開されたポリシーにより、サイトと Constituency は制約と規制を理解できますが、その場合でも、Constituency にこのような時期を通知する手段を講じる必要があります。例えば、優先順位の高い報告手続きに対して情報を提供するといった休暇メッセージを配布することができます。これにより、Constituency の期待は適切に満たされ、このような方法がないときよりも CSIRT に対して寛容になります。

Constituency の規模と提供されるサービスによっては、事前登録も可能です。明らかに、Constituency の規模が比較的小さく（百単位）、非常に安定している場合にのみ、Constituency の事前登録が可能です。また、Constituency と CSIRT との関係が、営利目的の有料サービスチームやネットワークサービスプロバイダとの関係のように契約ベースである場合にも可能なことがあります。既存の契約に補足として事前登録条件を追加するのは簡単です。事前登録時には、情報開示制限、信頼できる連絡窓口、好ましい安全な通信方法などの問題に対処する必要があります。

### 3.7.4.2 CSIRT

他の関係者との外部のやり取りを必要としないインシデントは、今日の「境界のない」のネットワーク環境ではまれです。これは、インシデントが外部との関係や副作用を持たず局所的である場合にのみ発生します。その場合でも、法執行機関が関係するときなどには外部とのやり取りが必要になることもあります。

Constituency のサイトの直接の連絡窓口に加えて、CSIRT の最も重要な協力パートナーは、仲間のチームです。インシデントに対応している間は、直接的な支援と情報交換が最も重要ですが、チーム同士で支援し合う可能性もあります。これは、チームが長い間 CSIRT 事業に携わっていたり、特殊な技術的専門知識を持っていたりする場合に特に当てはまります。これ以外の支援の例については、表 17 を参照してください。

情報の交換により、協力しているチームはたいがい利益を得ることができ、義務を果たしたりよりよいサービスを提供したりすることが簡単になります。しかし、そもそも情報共有は、考えているほど簡単ではありません。表 18 にまとめた問題を検討すると、どの程度チームが情報を交換し、部外秘の問題で協力してくれるかは、今までの互いの信頼関係にかかっているということがはっきりします。2 つのチームの間に正式な（書面の）契約があれば、前述のすべての問題が既にきちんと理解されているものとして、チームが情報を交換するのがいっそう容易になる場合もあります。

2 つのチームが協力関係を築く必要がある場合は、まず、信頼を築くことが必要です。信頼を築くことは容易ではなく、時間もかかります。信頼関係の構築にもっとも重要なステップの 1 つは、お互いを知ることです。それぞれのチームを訪問し合い、互いの目的、目標、手順、およびポリシーをできる限り理解しようと努める必要があります。これにより、チームはより深い関係が実現可能で利益になるかどうかを現実的に評価することができます。最初は、大きく複雑でリスク

の高い仕事から始めるのではなく、リスクの小さい小規模のプロジェクトから協力することが望ましい場合があります。

表17：考えられるチーム内の支援タイプ

支援のタイプ	説明
教育／トレーニング	「新規 CSIRT の設立」のような問題から、インシデントの性質を理解するための技術的なチュートリアルまで、さまざまな範囲に及ぶことが考えられます。
時間外の適用範囲	ある CSIRT は営業時間中のみサービスを提供し、またある仲間の CSIRT は、提携契約の一部として営業時間外の電話受け付けを行うことが考えられます。これは、チームがコーディネーションセンターの間接的な管理の下で運営している場合に特に関連します。
技術的専門知識	技術的な問題に対処し、その知識を他のチームと共有します。
共同作業	難しすぎて1つのチームのリソースでは解決できない問題に対処するため、2つ以上のチームが協力してその解決策を探るといったことがあるかも知れません。本書は、この種の協力の良い例です。
他者の意見	特定の問題の解決に取り組んでいる間、それに携わるチームのメンバーは、問題に近すぎて客観的に見られなくなることがあります。このような状況で生じる悪影響を避けるため、解決策を公に配布する前に、別のチームが、提案された解決策を再検討し、それに対する意見を述べるように求められる場合があります。既に存在している CSIRT は、長い間勧告の草案を交換してきており、たいていの場合、最終的な勧告が発表される前に多くの提案を取り入れています。
他のチームまたは専門家の連絡窓口	チームは、特定のサイトまたはネットワークの信頼できる連絡窓口が必要になることがあるため、他のチームが設定済みの連絡窓口を持っているか、または、他の問い合わせ先を知っているか、他のチームに尋ねることがあります。また、これは技術専門家とベンダの連絡窓口にも当てはまります。



表18：情報共有のための検討事項

問題	説明
機密性／秘密保持	情報は他のグループにとっても有益である可能性があるため、その機密性は保持されなければなりません。これは、転送、保存、および実際の使用について言えることです。チームメンバの反応を見るだけで、情報の少なくともある部分（例えば、新しいバグやセキュリティホールが存在、あるいはそれ以外のインシデントの存在）が明らかになる場合があります。
適正な利用	情報は1つのチームに属しますが、その情報を利用するために、他のチームは元のチームがその情報に設けた制約に従い、元のチームが「適正な利用」と考えるものに従う必要があるという点を、そのチームに対して明らかにしなければなりません。この情報が利用できるようになるには、ほとんどの場合、機密保持契約書の正式な署名が必要です。また機密保持契約書には、適正な利用が行われるための権利と義務が明示されている部分があります。
開示	情報は、将来のある時点で公に配布する可能性があるため、あらかじめ開示制限を提示しておく必要があります。チームの中には、情報に対する時間制約を設けているところもあります。期限前にはいかなる方法でも情報を開示することは禁止されますが、期限後に開示されたこの情報を勧告に取り入れるのは問題なく認められます。しかし、国際的な環境で予定表を設定するのは容易ではありません。時差があるということは、世界のある地域のシステム管理者が仕事を終えようとしているか既に帰宅しているかもしれないときに、別の地域では勤務時間が始まるようとしているということです。
適切な謝辞	情報の収集、分析、提供は他のチームによって行われているので、情報を使用するチームは、元の情報源に対して公平且つ適切な感謝の意を示すことを考える必要があります。

以前のやり取りから知っているチームもあれば、聞いたことはあってもよくは知らないチームもあります。そのチームが適切な能力を備えているか、あるいは本物であるかはわからないため、そのチームに情報を渡すかどうか判断が難しい場合もあります。最初にそのチームに関するある程度の知識があれば、判断は容易になることもあります。このような情報を得るための1つの方法は、良好な関係を築いている別のチームに、自分たちがよく知らないチームとどのような経験をしてきたか尋ねることです。信頼できるチームを識別する方法を利用すればもっと簡単ですが、今のところそのような方法は存在しません。

次に、チーム間の協力に関するその他の問題について取り上げます。これらの問題は、CSIRTの操作手順と密接に関係しています。

### 必須の情報

入ってくる情報の取り扱いに関する問題は既に取り上げました。チームが報告を処理する前に把握しておかなければならない重要な情報があります。この情報が最初の報告に記されていないと、チームがその情報を取得するまで遅れが生じます。場合によっては、例えば、その報告が週末の直前に送られた場合や、大きな時差がある場合などには、その遅延が深刻になることがあります。チーム間の報告フォームを使用して、別のチームから必須情報が報告されるように試みることはできますが、このようなプロセスは、この種の状況が発生する前に整備しておかなければなりません。

例えば、同格の CSIRT 同士で情報を共有または報告するという方法をとることがあります。また、組織構造により、上位のコーディネータチーム（例えば、政府または国レベルの CSIRT）に報告するという方法を取ることも考えられます。あるいは、（規制により）チームに報告を義務づけることもできます（例えば、アメリカの一部のチームは、指定時間内に「指揮系統の上流に」報告することが求められています）。チーム間のすべての関係が同格であるとは限りません。状況によって自発的な階層で参加するチームもあります。

例：悪意のコードまたは新しい脆弱性の分析において、2～3 の CSIRT が役割を共有し、1つのチームが各チームから分析を収集して、包括的な分析に統合するといったことが行われる場合があります。これは、自発的な階層構造を持った同格関係です。

ある活動に対して同格チームとしてやり取りしているからといって、それが、別の対応において異なる方法でやり取りすることを妨げることにはなりません。しかし、それほど多くはありませんが、強制的な階層構造の中にあるチームも存在します（例えば、軍の支部の中には「指揮系統の上流」に位置するコーディネータの CSIRT に報告するものもあります）。

例：前述の例を取り上げます。3つの CSIRT が、報告されている活動の分析の任務を分担することに同意しているとします。それぞれが作業の一部を担当します。あるチームは脆弱性を調べ、別のチームはログを調べます。そして、3番目のチームは影響を受けたサイトへの対応とフォローアップに関するあらゆることを調整するために発信する情報の準備に取りかかります。この最後のチームが、外部と接触する役割を担うチームです。すべての情報は、このチームから別のグループに渡されます。その後、他のチームが同様の活動に参加する可能性があります。おそらく役割は異なります。そのような役割であっても、各 CSIRT は、自身の階層内で別の役割を果たすことがあります（例えば、スポンサーや他のコーディネータチームへの報告など）。

ここで重要なことは、チームはさまざまな状況でさまざまな役割を担うことができ、同格のチームとして、またはコーディネータやリーダーとして、あるいは法執行機関やメディアとの窓口として、もしくはそれ以外の役割で任務を果たすことができるということです。

### 誰がリードするか

通常は、同格レベルでやり取りしている場合でも、たいていの場合、1つのインシデントの処理中に一時的な自発的階層が現れます。1つのインシデントに複数のチームが関与する場合は、調整が必要です。調整をしないと、同じ情報を持つ同じサイトに複数のチームが連絡するなど、手間の重複が生じます。このようにチームとサイトの時間を無駄にしないように、通常は特定のインシデントに対して1つのチームがリーダーシップをとります。インシデントへの対応の調整において誰がリーダーシップをとるかは、普通はケースバイケースで決められます。一般に、最初の報告を受け取った CSIRT か、インシデントの最も広い範囲を担当している CSIRT が調整を行います。また、調整については、あらかじめ決め

られた申し合わせ（例えば、強制的な従属を伴う調整サービスへの同意）によって前もって合意を取り付けておくこともできます。

### 3.7.4.3 Constituency 以外のサイト

チームが1つの企業または組織のローカルな側面以外にも対応している場合は特に、チームの知名度が上がるにつれて、ほぼあらゆるところから要請や情報が来るようになります。

例：CERT-NLは、（単に名前から判断されて）誤って Dutch CSIRT と見なされることがあります。人々がオランダに CSIRT があるということ以外は知らない場合、そして、オランダのホスト/サイトに関するインシデントがある場合、インシデントは CERT-NL に報告される可能性があります。これは、巻き込まれているサイトが CERT-NL の正式な Constituency、つまりインターネットサービスプロバイダである SURFnet の顧客でもない場合にも当てはまります。

CERT-NL は、そのような情報を受け取ったら、政府、大学、営利組織に存在する他のいずれかの CSIRT にその情報を渡します。インシデントの報告を受け取ったら、チームはその報告に適したチームであるかどうかを問わず、ある程度の対応を行う必要があります。Constituency またはサービスが非常に特殊なチームでは、おそらくこの種の報告にはまったく対応しないことを選ぶ場合もあります。報告者が期待できるのは、せいぜい、その報告を別のチームに送り直してくださいという内容の簡単なメッセージ程度でしょう。

例：医療との類似性を考えます。健康上の問題が生じ、助けを求めている人がいる場合、医者や看護師がそれを無視できるわけがありません（少なくとも世界の多くの地域においては）。

ただし、このような状況で提供する支援は、自身の正式な Constituency に提供するものとは異なる場合があります。サイトへの対応に影響を及ぼす可能性のあるもう1つの要因は、信用レベルです。報告元がわからないと、その報告の質と関連性を評価するのが難しくなります（提供されるデータが真正性、正確さ、関連性を検証できる場合を除く）。

例：CSIRT には多種多様な電話がかかります。そのような電話の中には匿名の電話で報告された脆弱性に関係しているものがあるかも知れません。1つの電話に与えられる信用レベルは制限される場合があります。しかし、チームが、コミュニティの信用できるメンバ（例えば、他の CSIRT や信用できるエキスパート）から脆弱性に関する同様の電話を受け取った場合、後者の電話には、その報告に妥当性（あるいは質と関連性の可能性）があるという高いレベルの信頼が与えられることになります。

チームを確立し、リソースと担当を割り当てる際には、おそらく公表 Constituency 以外からの要請が発生し、それに対応しなければならなくなるという点を理解しておくことが重要です。たいていの場合、本来報告すべき適切な

アドレスを記した簡単な返答だけでも、報告元のサイトに正しい関係者を知らせるのに役立ちます（そして、将来的な同様の要請が起こるのを抑えます）。そのような返答ができるように、チームは前もって必要な情報を準備し、どのような質問または報告にはどのような返答が適切か、ポリシーを確立しておく必要があります。

以前、いくつかのチームは、特に大規模な **Constituency** を担当していたとき、報告元サイトに適切なアドレスを知らせていました。そして、この情報の取り次ぎに加えて、報告元サイトにある種の「応急処置」も施していました。これにより、報告元サイトが **Constituency** メンバと同じサービスを受けるということが多々ありました。この方法はチームの評判を高めますが、さらなるリソースが必要となり、次のような問題を招きかねません。

- 他の CSIRT は、自分たちの **Constituency** が別のチームからの支援を受けることを好みません（その CSIRT が取得する必要がある、またはそのサイトに提供する必要がある情報が存在するかも知れません。しかし、そのサイトが別の CSIRT から事前情報を受け取り、それだけで十分だと考えれば、自分たちの CSIRT にまったく連絡しないということも起こりえます）。
- 上層経営陣（またはスポンサー）は一般に、チームのリソースが「外部の」（**Constituency** ではない）関係者に使われるのを好みません。
- 公表 **Constituency** に対するサービスが、リソースの制約により悪影響を受ける可能性があります。

報告元サイトがどの CSIRT の公表 **Constituency** にも該当しない場合、特別な問題が発生することがあります。

例：現在、全ヨーロッパの約 90% の国には、資金の提供を受けた（有志ではない）CSIRT があります。多くの国では、研究ネットワークのためにこのような CSIRT が設立されています。したがって、それぞれのポリシーに応じて、自国の商用サイトに関係するインシデントに対応します。その他の国には最大 15 のチームが存在しますが、有効範囲は依然として完全ではありません。たいていの場合、CSIRT は個人ユーザには対応しません。

したがって、各チームは、明確な予想を立て、外部からの要請に応えるための理解可能且つ強制可能なポリシーを確立する必要があります。報告元サイトを担当する CSIRT が別にあるときは常に、その CSIRT またはその報告について知らせる必要があるチームに報告するように報告者を誘導する必要があります。報告者が 100% の確かさを求めてくる場合は、担当の CSIRT に直接連絡するように勧め、そうすることの利点を説明する必要があります。例えば、適切な対応や支援が受けられるから報告者のチームに報告する方が適切であると伝えたり、報告者のチームに報告することを要求する強制的な規則が存在する可能性があるといったことを指摘したり、場合によっては大規模な活動（前述の「全体像」）の一端としてこの報告を見ることによって報告者のチームが得られる付加的な利益を説明したりします。

さらに、Constituency 以外のメンバからの報告に機密扱いの要求が伴っているということは、それ自体が担当 CSIRT にとって有益な情報であるため、最初に報告を受けたチームは要請元に関する詳細を明かさずに、報告について担当 CSIRT へ、不適切な部分を削除してから情報を提供することもできます。（担当 CSIRT は、この情報を生かして、元の報告者が機密性を求めた理由を突き止め、今後は同様の状況が発生しないようにサービスを改善したり手順の一部を変更したりできる場合があります）。

#### 3.7.4.4 親組織

チームの親組織としては、上層経営陣、資金提供団体、株主などが考えられます。Constituency の他のメンバ同様、親組織も、インシデント対応からコンサルティング、トレーニング、プレゼンテーションの配信に至るまで、サービスを依頼することがあります。

これは重要であり政策上の問題でもあります。ほとんどの場合、親組織は他の Constituency からの同一のサービス要求に対して通常割り当てられる優先順位よりも高い優先順位が与えられます。インシデントの場合は、攻撃対象である可能性もある複数の業務部門によって親組織が構成されている場合、チームはその報告に対応し、直ちにその部門に関係するインシデントを CSIRT の管理者に注目されるようエスカレーションすることも考えられます。

#### 3.7.4.5 法執行機関

インシデントが犯罪に関連するときは常に法執行機関との関係が重要な問題になります。法執行機関は次のことを行います。

- インシデントそのものについての詳細の把握
- 関係する技術的な問題についての詳細の把握
- 巻き込まれているサイトの特定、およびサイトへの連絡
- インシデントに関連する最近の活動および損害に関する情報の取得

チームは、Constituency に対する守秘義務と法執行機関への協力の必要性のはざままで微妙な立場に立たされます。チームのポリシーにより、チームが自主的に法執行機関に提供する情報の量と種類が決まります。法的な命令によって（召喚令状またはそれ以外の裁判所命令によって）求められた場合、CSIRT は法執行機関が要求する特定の情報を提供しなければなりません。ポリシーと手順では、法執行機関に提供するサービスを定義し、情報を明らかにする状況を明確に示す必要があります。

チームと法執行機関との間により協力関係を築くには、相互尊重につながる相互理解が不可欠です。このようなやり取りを始めるために、できるだけ早く法執行機関の適切な連絡窓口との関係を築くことが推奨されます。

チームのポリシーにおいて法執行機関と話をする担当者を定める必要があります。この担当者の役割としては、地元以外の、場合によっては国際的な法執行機関か

らの要求に対応することもあります。そのような要求は対応が難しいため、地元の法執行機関に回す必要があります。したがって、法執行機関の連絡窓口を知り、このような要求に前もって備えることは、各チームにとってプラスになります。

法執行機関との協力におけるもう1つのメリットは、統計データを交換できること、そして、CSIRTが認識している（またはCSIRTに報告された）活動に関して法執行機関のコミュニティ内の意識を高めるのに寄与できることです。CSIRTは、コンピュータ犯罪だけでなく、犯罪とは見なされないインシデントに関する生の情報を有しているため、法執行機関の全体像を描く能力を大幅に高めることができます。同時に、法執行機関は必要に応じて、CSIRTが報告を確認しているその他の関連するインシデント活動の中でCSIRTが興味を持つ可能性がある活動に関して、好ましくない部分を削除したフィードバックをCSIRTと共有できる場合があります。

### 3.7.4.6 メディア

メディアには世論に対する強い影響力があるため、各チームはメディアポリシーを持ち、関連手順を確立しておく必要があります。その目的は次のとおりです。

- 妥当なフィードバックと情報を提供すること
- サイトの利益を守ること
- 自分たちの考えを述べ、サイトにサイト自身の考えを述べてもらうこと

メディアにはインシデントに関する情報を得ることに對して独自の目的と理由があります。これらの目的はたいていの場合、CSIRTの目的と対立します<sup>42</sup>。その結果、メディアは往々にして、チームが快く提供する以上の情報を得ようとし、そこでまずメディアからの依頼に対するチームの連絡窓口をメディアに知らせておく必要があります。そして連絡窓口となる人は、メディアとの初めての接触に先立って、メディアがかかわる状況で予想すべきことやその状況に適切に対応する方法など、メディアとの対話について適切な訓練を積んでおく必要があります。

このトピックについては、3.8.8節「情報開示」でさらに詳しく取り上げます。

## 3.8 情報のハンドリング

インシデントのハンドリングは、常に情報のハンドリングと関連しています。特定の情報がサイト、製品、新しい脆弱性、進行中の攻撃、またはパスワードに関係するかどうかにかかわらず、常に情報が鍵となります。

---

<sup>42</sup> McGillen, Terry, 『CERT Incident Communications』、5th Workshop on Computer Security Incident Handling, Forum of Incident Response and Security Teams、ミズーリ州セントルイス、1993年8月。McGillen, Terry, Fithen, Katherine T, 『Public Communications in the World of Incident Response』、9th Workshop on Computer Security Incident Handling, Forum of Incident Response and Security Teams、英国ブリストル、1997年6月。

収集された情報は、CSIRT がどのようなタイプのシステムを使っているかによらず、インシデント報告とその他の関連データの記録および追跡に使用しているシステムに入力しなければなりません。どの情報も、CSIRT が保有している間は格納および保護する必要があります。種類と重要度に応じて情報にタグを付けておくと、その後の処理が円滑になります。情報の処理を進める前に、最も重要な情報が最初に処理されるように優先順位を付ける必要があります。情報が調査、分析されたら、関与している関係者（通常はチームの **Constituency**）にガイダンスと支援を提供するために、情報そのもの、またはいくつかの情報の一部を開示する場合があります。

### 3.8.1 情報の収集

CSIRT が処理する情報の大部分は直接受け取るものが対象になりますが、積極的に Web で情報を検索したり他のソース（技術報告書、分析、ニュース、信用できる専門家など）から情報を入手したりする必要もあります。

情報を収集する前に、次のことを決定するための専用のポリシーと適切な手順を設定することが推奨されます。

- どの種類の情報源が受け入れ可能か
- どの種類の品質管理を実施すべきか
- どのようにしてエラー、脱落、不正確なデータを認識すべきか

情報を能動的に収集する場合、情報は次の 2 つの情報源のどちらかから得られます。

1. 一般公開されている情報：一般公開されているあらゆる種類の情報が含まれます。ニュースやメーリングリストなどの従来のサービスから、検索エンジンや Web に及びます。
2. 他の関係者との情報交換：チームが必要としている情報を既に他の人たちが保有していることがあるため、他の人たちとの情報の交換により、チームに直ちに利益がもたらされる可能性があります。ここでの大きな問題は、その情報を誰が持っているかを明らかにすることと、その人またはチームが快く情報を共有してくれるように信頼関係を築くことです（これは、他者と良いパートナーシップを築くことの重要性を浮き彫りにします。3.7節「やり取り」を参照してください）。

利用できる情報は絶えず変化するため、情報収集とその他の関連ポリシー、および手順は、最新の情報源が調べられるように頻繁に評価および検証を行う必要があります。

他のグループから入ってくる情報は、チームのトリアージ機能を経由する必要があります（3.3節「トリアージ機能」を参照）。イベント、脆弱性、興味深いと考えられるディスカッションスレッドに関連する情報の報告を促進するために、報告してくるユーザに対して報告用フォームのような適切な支援を提供する必要があります。このような支援については、他の種類の情報の報告や CSIRT への

要請の送付に使用できるように、チームの電話番号や電子メールアドレスなどの連絡窓口情報も含めると良いでしょう。

ポリシーや手順の枠を超えて標準化すれば、チームは統一のとれた形式で情報を収集できるようになります。使用する形式を標準化することで、情報の保存、検証、カテゴリ化、優先順位付けといった情報に対する今後の処置が行いやすくなります。

### 3.8.2 情報の検証

情報を使用する前に、何らかの検証を行う必要があります。通常、これに関するプロセスでは、少なくとも次の3つの点を考慮します。

1. 発信元：情報源、および報告者の知識、経験、役割、職務といった関連要素。すべてのコミュニケーションと同様、発信元は、提供された情報のその後の処理に大きな影響を及ぼすことがあります。

例：DFN-CERTがあるオランダの大学のネットワークから送られた広範なIPアドレスのIPポートスキャンをCERT-NLに報告した場合、CERT-NLは、見知らぬ個人から提出されてきた報告よりもこの報告の方に高い優先順位を割り当てます。とはいえ、この報告もダブルチェックされます。

報告が信用できるソースから提出されたものである場合は、フォローアップがいくぶん容易になることがあります。しかし、発信者の身元が状況を困難あるいは複雑にするときもあります。

例：資金提供団体からの電話の場合は、実際の優先順位に関係なく、他の発信者よりもフォローアップに多くの時間が費やされます。

2. 内容：その情報は真実であると考えられますか？ それとも、明らかに間違っていたり誤解を招いたりするような情報ですか？ 内容が技術的に正しいかどうか、情報のその後の処理に影響を与えることがあります。

例：他の関係者から偽のウィルス報告を受け取ったConstituencyはたいいてい、検証のためにその報告をCSIRTに送ります。一般に、偽の報告には技術的に正しくない、あるいは不可能な情報が含まれています。CSIRTは、場合によっては、偽の報告が広まっているという事実に対してConstituencyの注意を喚起する必要があるかも知れませんが、この報告に対しては、技術的に正しく見え、且つさらなる分析と調査に値するウィルス報告より低い優先順位が割り当てられるでしょう。

3. 配布：これは、報告に使用されたチャンネルと、受け取った報告の真正性に対して起こりうる影響度に関係します。デジタル署名された証明可能な報告から、匿名電話や郵便で受け取る報告までが対象範囲になり得ます。

### 3.8.3 情報のカテゴリ化

組織に入ってくる情報は、何らかの方法でカテゴリ化する必要があります。情報はすべて、トリアージ機能を介してCSIRTに入ります。これにより、最初のカテゴリ化が円滑化されます。よく知られているカテゴリの例としては、プライベート/仕事、緊急/緊急ではない/不要などがあります。通常、このような簡単な



カテゴリははっきりと示されることはありません<sup>43</sup>。カテゴリ化は優先順位付け（3.8.6節「優先順位付けの基準」で取り上げます）の意味を含みますが、別個の独立した活動と考えた方が適切です。

情報のカテゴリは、その後の情報の処理（例えば、保管、普及、配布、処分）に影響します。どの情報も区別なく、最高レベルで保護し、同じように処分する必要があります。

明確なカテゴリ化が行われていない場合は、受信した情報を見て、各情報のタイプと重要性について自分の認識を当てはめます。このような認識は個人個人で異なる可能性があるため、このプロセスを標準化し、手引きとなる簡単明瞭な手順（4.2.2節「情報のカテゴリ化ポリシー」を参照）を提供する必要があります。

多くの CSIRT は、インシデント報告と情報提供依頼に使用されるプロセスとは別に、連絡先情報を処理するプロセスや手順を用意しています。連絡先（人、組織）は通常、信用できる仲間のチームに対してさえ漏れないように保護されています。したがって、この種の情報をサニタイズ（sanitize = 不適切な部分の削除）する方法に関する説明が手順に含まれる場合があります。また連絡先情報を独自のカテゴリとして保持する場合があります。

カテゴリ化は、たいいていの場合、情報そのものに基づいて行われます。時として、カテゴリ化は情報提供者との双方向の対話の後で行われます。またある時には、情報提供者が情報のカテゴリを指定することもあります（例えば、Constituency が脆弱性やインシデントを報告する場合）。

また、情報は（論理的に）分割する必要が生じることもあります。例えば、インシデントログでは、特定の名前または IP アドレスは開示されないように保護する必要がありますが、残りの情報は他の関係者に自由に転送できます。

例：CERT/CC は、データに対して次の 3 つのカテゴリで情報開示制限をどこまでと設定するか示すようにインシデント報告者に依頼することで、連絡先情報のカテゴリ化に対応しています。

- そのインシデントにかかわっている他のサイト
- 他の対応チーム
- 法執行機関

報告元のサイトが（CERT/CC のインシデント報告フォーム[CERT/CC 1997a]で要求される）この情報を提供しない場合、CERT/CC はデフォルトの「開示しない」を使用します。これは、報告元のサイトを特定する情報を隠して他のサイトや対応チームと連絡をとるように CERT/CC に求めているということになります。

---

<sup>43</sup> ガイドラインの中には、情報分類ポリシーに言及しているものもあります。このガイドラインでは、代わりにカテゴリ化を使用することにしました。「分類」という語は、この節全体と 4.2.2 節「情報のカテゴリ化ポリシー」で一般的な文脈で使用しています。限られた軍事的または政治的な文脈では使用しません。

### 3.8.4 情報の保管

情報が保管される時は常に（手書きであるかコンピュータシステムに格納されるかに関係なく）、セキュリティが非常に重要です。現実問題として、セキュリティなしで Constituency の利益、および関係するサイトの機密を保護することは考えられません。

これは、大規模データベースなど、情報が集合的に保管される場合に特に当てはまります。このような場合、集められた情報の価値は、情報の断片を寄せ集めた場合よりも増します。集められた情報は、（チームが全体像を把握するのに役立つ）大きな恩恵をCSIRTにもたらす一方で、弱点でもあります。不適切な保管と保護が原因でわずかな情報（例えば、1~2件の電子メール）が漏れてしまったくらいであれば、CSIRTはその状況を切り抜けられるかも知れません<sup>44</sup>。しかし、集められた情報が大量に漏れた場合には（例えば、サニタイズされていない単一のインシデントのサマリ）、CSIRTの評判に対する影響は深刻です。

CSIRT は、侵入者にとって魅力的なサイトです。悪評によって CSIRT を廃止に追い込むことは明らかに、侵入者が CSIRT のデータへの不正アクセスを試みる動機の一つであると考えられます。しかし、考慮すべきもう一つの動機は、侵入者がデータへのアクセスから入手できる情報です。侵入者は、自分の活動がどこまで特定されて CSIRT に報告されているかを明らかにし、脆弱なサイトに関する情報を突き止め、新しい脆弱性に関する情報を取得するなどといったことが簡単にできるかも知れないのです。

複数の論理データベースを使用することは、情報の保管のための一つの有効な方法です。これにより、情報にアクセスしやすく、情報や変更が簡単になり、情報がさまざまなサービスを支援するのに十分な柔軟性を持つようになります。

データをどのように保存する場合でも、次の情報にはアクセスできるようになっていなければなりません。

- 連絡先
- 取られる（または取るべき）アクション
- インシデント（活動、ステータス、変更が発生したときの進行中のサマリに関する現在の情報）
- 脆弱性およびパッチ
- アーティファクト（スクリプト、ツール、ファイルの残留物など）
- ログ、または保存されている情報に関連するその他のデータ

---

<sup>44</sup> とはいえ、極めて重要なメッセージが1つ漏れただけでも、CSIRTの信用と評判に対して壊滅的な影響を与える可能性がある点に注意する必要があります。

### 3.8.5 情報のサニタイズと処分

情報のサニタイズ（sanitize = 不適切な部分の削除、無害化）と処分は、情報の処理に不可欠な要素です。これは、人々の（ことによると大規模な）集団や組織を参照する機密情報を持つことが多い CSIRT に特に当てはまります。3.8.3節「情報のカテゴリ化」で説明したように、特定のカテゴリの情報は、情報に付加された機密性に適した一貫した方法でサニタイズし、処分する必要があります。

多くの場合、情報は、受取人に提供される情報の有用性に悪影響を及ぼすことなく、機密情報が不適切に開示されないようにサニタイズできます。

例：サイト A は、侵害されたことのあるシステムの 1 つで見つかった、侵入者のさまざまなアーティファクトの中に、パスワードファイルのコピーを見つけました。サイト A の CSIRT には、パスワードファイルの出所がわかりません。しかし、パスワードファイルの出所に関する完全な情報が存在しない場合であっても、可能性のある出所を示すのに十分な情報がファイルに含まれていることもあります。その場合、サイト A の CSIRT は、出所と思われるサイト（サイト B）に連絡を取り、サイト B も侵害されていたか確認することができます。CSIRT は、確認のため、暗号化されたパスワードがすべて取り除かれたファイルのコピーをサイト B に送ります。これで、パスワードの平文送信によるさらなる潜在リスクの発生を防ぐことができます。ユーザ名やホームディレクトリなどの特定の情報は元の状態のままにします。結果、他者によって取得された場合に不正使用されそうな情報をさらに配布することなく、確実性を高めることができます。また、もしもサイト B がパスワードファイルの出所ではなかったとしてもパスワードは保護されます。つまり CSIRT は、無関係の第三者に機密情報を渡してはいないのです。

ユーザおよびサイト関連情報の保存、および、インシデントと特定組織との関係には、関連するプライバシーの問題があります。情報の完全なログを保持することが CSIRT にとって何よりの利益になることがあります。これはともすれば、情報が保管されているすべての関係者に影響を及ぼすことにもなります。

例：侵入者に関する特定情報を提供するという法規定がある場合、法執行機関は、侵入者に関するデータが保管されているすべての媒体を求めてくる場合があります。結果として、チームは、同じ媒体に保管されている、侵入者の攻撃とは無関係の他の情報の機密性を保証できなくなります。このようなことを Constituency が知ってしまうと、今後の問題を CSIRT に報告することに抵抗を感じる可能性があります。このような印象とそれが現実になることを避けるために、さまざまなインシデントに関するデータがすべて別々に保管され、別々にアクセスできるような技術的手段を適用する必要があります。法執行機関から 1 つのインシデントに関する情報を提供するように求められたら、そのインシデントに関する部分だけを渡すようにします。

漏えいの可能性を抑えるために、チームは一定期間後にサニタイズされた情報のみを保管したり、統計的および技術的な点だけが含まれるサマリを残したりする場合があります。この選択により、不要になった情報をすべて処分するために相

当な労力を費やさなければなりません（第一に、この統計的および技術的な点のサマリを用意するための労力が必要です）。これはバックアップの場合に特に困難です。バックアップのそもそもの目的は、長期に渡り情報の可用性を確保することだからです。必要なくなった情報の処分のために古いバックアップテープを簡単に書き換えることはまず不可能です。

例：この問題に対処する1つの方法は、2つの異なるバックアップ方式を使用することです。1つはオペレーティングシステムおよびユーザデータ用で、もう1つはインシデント関連情報用です。これは、ユーザのデータ領域にインシデント関連データは保管されないということを暗に示しています。通常のバックアップテープは必要ときに再使用されますが、インシデント関連テープは、以前保存された情報が後で回復されないように、再使用前に数回上書きされます。テープが使用されなくなった場合、そのテープは、単に捨てるのではなく物理的に破壊する必要があります。

### 3.8.6 優先順位付けの基準

多くのインシデントのタイプは「重大」または「深刻」ですが、このような個々のカテゴリ内においても、CSIRTはどれから先に対応すべきかを定めるために優先順位を割り当てる必要があります。インシデントの重要度は、さまざまな要因に左右される場合があります。また、優先順位も、新しい情報が発見されたり報告されたりすると、変わることがあります。そのため、進行中のインシデントの優先順位リストを作成し、維持することは簡単ではなく、実際のところ、動的な活動となる可能性があります。

最も重要なインシデントを選択するための方法、または、複数のインシデントをランク付けするための方法には、さまざまなものがあります。

- インシデントに対応するのに必要なリソース
- Constituency に対する影響度
- インシデントのタイプ
- 損害のタイプまたは程度
- 攻撃対象または攻撃元

いつものことですが、選択した方法ではすぐに対応できない例外も発生します。そのため、このような例外を見越して柔軟性を持たせる必要があります。例えば、インシデントに適切な優先順位を付けるのに十分な情報が集まるまで、最初のうちは、優先順位の間中または最上位に位置する順位をデフォルトでインシデントに割り当てることなどが考えられます。優先順位付けプロセスに影響するポリシーは、かつては例外と見なされたが現在では普通になった項目に対応し、また傾向および必要性におけるその他の変化が反映されるように、時とともに定期的に見直して改良する必要があります。

例：数年前、CERT/CCは優先順位が最も高いインシデントとしてシステムのルート侵害をリストアップしました。しかし、時がたつにつれて（インター

ネットが成長し、チームのミッションが変わったため)、他のタイプのイベントに高い優先順位が与えられるようになりました。「Incident Reporting Guidelines」の「CERT/CC Tech Tip<sup>45</sup>」には、次の優先順位が示されています。

- 生命にかかわる可能性のある活動
- 次のようなインターネットインフラに対する攻撃
  - ルートネームサーバ
  - ドメインネームサーバ
  - 主要なアーカイブサイト
  - ネットワークアクセスポイント (NAP)
- インターネットサイトに対する広範囲に及ぶ自動化された攻撃
- 新しいタイプの攻撃または新しい脆弱性

例：新しく送られてきたインシデント報告は、経験豊富なスタッフが調べます。このスタッフには洞察力があり、どのようなインシデントも適切なスタッフに割り当てることができます。例えば、よく知られたインシデント活動（ポートスキャン、UBC/UCE 報告、よく知られたセキュリティ上の脆弱性を使用した攻撃など）の報告は、新人の CSIRT スタッフに割り当てます。その一方で、対応に深い専門技術と知識を必要とする複雑なインシデントは、CSIRT スタッフのうちの上級メンバに割り当てます。

インシデントの優先順位の付け直しも継続的に行う必要があります。特定のインシデントに関する新しい情報が入ってきたときは常に、全体の優先順位が変わる可能性があります。優先順位の変更は、報告者と関連サイトにも影響するため、適宜知らせる必要があります。これは、インシデントの優先順位が下がった場合に非常に重要です。一方、一見低い優先順位のインシデントも、新しい情報の発見により優先順位が突然上がった場合には、同様の理由で報告者と関連サイトに知らせる必要があります。

ほとんどのチームは、限られたリソースで運営しているため、報告されたすべてのインシデントには対応できないときがあります。まれに、そのようなインシデントが他のチームに回されることもあります。インシデントに対応できない場合は、報告者に知らせる必要があります。そうしたコミュニケーションがないと、ユーザは蚊帳の外に置かれることになり、チームの明らかな無反応についてうわさが流れます。これは、チームの評判に傷を付け、運営全体に悪影響を及ぼすことがあります。

ほとんどのチームは、いくつかの優先順位付け方法を組み合わせて、全体的な優先順位付け基準を定めています。一般に、1つの方法に基づいて優先順位を付け、それから別の方法を1つ以上適用してその優先順位を微調整します。選択した方法によっては、トレードオフを考慮に入れなければならない場合があります。自分たちのインシデントは考えられる最も高い優先順位に値するはずだと主張する人が必ずいるため、トレードオフは防御可能なものでなくてはなりませんし、また相手に伝えなくてはなりません。以降の節で、考えられる優先順位付け方法を取り上げながら、いくつかのトレードオフを明らかにしていきます。

---

<sup>45</sup> [http://www.cert.org/tech\\_tips/incident\\_reporting.html](http://www.cert.org/tech_tips/incident_reporting.html)

### 3.8.6.1 攻撃対象または攻撃元

攻撃対象に基づいて優先順位を付ける場合、順位は、役割、任務、攻撃対象サイトまたは攻撃対象システムの重要性に基づいて割り当てられます。Constituency内の攻撃対象は、Constituency外の攻撃対象より重要であると考えられます。なぜなら、CSIRTの役割は、その内側のConstituencyのために働くことだからです。Constituency内に複数の攻撃対象がある場合、チームは、想定されるさまざまな攻撃対象を見分け、相当する優先順位を付けることができなくてはなりません。攻撃対象の順位は、攻撃対象に格納されているデータのタイプ、ネットワークインフラ内で攻撃対象が果たす役割、あるいはその他の要因によって決まることがあります。

例：Constituencyが製造会社であるCSIRTについて考えてみましょう。「攻撃対象」優先順位方式を使用すると、それほど重要ではないデータが格納されているシステムに対するインシデントより、企業秘密（例えば、研究や生産システム）や従業員データが格納されているシステムをターゲットにしているインシデントの方に高い優先順位が割り当てられることとなります。

侵入者は活動の起点を隠すことができるため、本当の攻撃元を必ずしも特定できるとは限りません。多くの場合、侵入者は攻撃の開始前に多くのシステムを縫うように（たいてい国境を横断して）進んできます。結果として、最初のインシデント報告における攻撃元に関する唯一明らかな情報は、攻撃の開始に使用されているサイトです。この攻撃を行っているサイトは、必ずしも本当の攻撃元であるとは限りません。

この方法は、攻撃対象に対してとられた方法とほぼ同じです。優先順位は、認識された脅威に基づいて、想定される攻撃元のタイプに割り当てられます。

例：Constituencyが軍隊であるCSIRTについて考えてみましょう。「攻撃元」優先順位方式を使用すると、「敵対的な攻撃元」、戦闘組織、または外国（特に敵国と見なされている国）のサイトからの攻撃にかかわるインシデントに高い優先順位が割り当てられることとなります。

### 3.8.6.2 損害のタイプまたは程度

インシデントの結果として生じた実際の損失または損害の程度は、評価が難しいこともあります。このようなデータは、事後に収集するのが難しいだけでなく、それ以上に、正確に予測することも困難です。この評価は、評価者の個人的な経験、受け取る報告の正確さ、チームが入手できる情報の種類に影響されます。Constituencyに対して直接的な権限のあるCSIRTは、Constituencyを巻き込むようなインシデントに関する詳細情報にアクセスできる可能性があります。しかし、権限が少ないチームは、正当な評価を下すために必要な詳細レベルの情報にアクセスできる可能性はほとんどありません。このため、この種の方法は、Constituencyへの権限のあるチームでよく見られます。

損害が分かっている、説明することが可能であっても、異なるインシデント間で比較できるように同じ測定基準を使用する必要があります。

例：病院と救急チームは、ほぼ同じ優先順位付け方法を使用します。

1. 生命の損失
2. 人間のけが
3. 金銭上の損失／権利の侵害

優先順位の決定に「金銭上の損失」を使用する場合は、金銭上の損害を算出するためのモデルが必要になります。しかし、一部のインシデントでは、金銭上の損害の算出は非常に困難です。例えば、侵入による知識や情報の漏えいによって組織が失った可能性のある金額を見積もることは簡単ではありません。そのためこの基準は、インシデントの優先順位付けでは用途が限られる可能性があります。

### 3.8.6.3 インシデントタイプ

この基準を使用した場合は、既知のインシデントタイプが、総合的な（潜在的な）技術的影響度に応じてランク付けされます。例えば、サービス運用妨害か特権侵害か、などです。インシデントタイプによる優先順位付けの結果として、「最高の優先順位」に振り分けられる項目が多くなり過ぎることがよくあります。その上、新しい、または珍しい、あるいは完全には分かっていないタイプの攻撃が発見された場合を除けば、技術的影響度だけでは通常は興味の対象となりません。このため、この方法は一般に他のタイプの優先順位方法と組み合わせて使用されます。

例：ルート侵害に関する5つの新しいインシデントが報告されました。これらは「最高の優先順位」と見なされるため、できるだけ早くすべて対処される必要があります。2つのインシデントは主要な大学からのもので、そのサイトには5つ未満のホストがかかっています。これらの大学には、インシデント対応を経験している職員がいます。1つのインシデントは、病院に対するサービス運用妨害攻撃で、医療記録データベースや研究室のテスト結果のデータが格納されている2つのホストが影響を受けています。残りの2つのインシデントは、攻撃者が、侵害されているホストを起点に他のサイトで攻撃スクリプトを実行しているため、定義された Constituency 内の何百ものホストがかかっています。

問題は、どのインシデントに最初に対応すべきかを決定することです。例えばすべてのものを外して、最も数が多いホストに対応しますか？ 2つの主要な大学は経験のある職員がいるため、外しますか？ 現在の報告に対処するために短期的に利用できる、チーム内の他のリソースは使用可能ですか？ 他のチームに助けをくれるように頼むことができますか？ 病院に「応急処置」を施し、技術的な影響が大きいインシデントに対応した後で細かくフォローアップすることが可能ですか？ などです。

ここで、このシナリオを少し変えてみましょう。実は病院がスポンサーのサイトであり、Constituency 内の何百ものホストにかかわるインシデントも依然として存在するとしたらどうでしょうか。この場合、優先順位付けはどう変わるのでしょうか？

### 3.8.6.4 フィードバック要求の優先順位付け

一般に、フィードバックの要求は、インシデント報告とは異なる方法で対応できます。「先着順」の原則が適用されますが、作業負荷またはその他の要因（使用できる人員や専門知識など）のため、この場合にも優先順位付けが必要なことがあります。フィードバック要求の優先順位付けの1つの方法は、要求している人が誰であるかによって、最初に応答を返す相手を決めるというものです。通常、Constituency またはチームの資金提供団体の地位が高い職員からの要求は、優先順位リストの最上位に移動するのに十分な理由になります。

### 3.8.7 エスカレーションの基準

エスカレーションは、優先順位付けと混同されることが少なくありません。活動は似ていますが、エスカレーションは、優先順位に関係なく活動の重要性を高めることに関係しています。エスカレーションでは、意志決定のため、少なくとも管理層の1つが関与する必要が常にあります。1つまたは複数の活動のエスカレーションが発生した場合は通常、チームが、普段とは異なる、もしくは高い作業負荷を経験していて、普段よりかなり切迫した状況にあるというサインです。

エスカレーションの基準および関連するプロセス、手順、ガイドラインは、使用に備えて前もって定義しておく必要があります。ここでも、定期的に基準を見直し、必要性の変化と新しい展開（新しい攻撃方法、インシデントタイプ、スポンサー組織など）に適合させ続ける必要があります。

エスカレーション基準は、CSIRT サービス全体またはインシデントハンドリングサービスにも適用できます。

例：CERT/CC は 1993 年後半、ネットワーク傍受攻撃、そしてユーザ名およびパスワード情報の取り込みに関連するインシデント報告の受け付けを開始しました。これらの報告はそれぞれ個別のイベントであり、分析も対応も難しくありませんでした。しかし、時がたち、何千ものユーザアカウントとパスワードの組み合わせが取り込まれたログが添付された報告が数多く送られるようになるにつれて、インシデントハンドリングスタッフは、その活動範囲に圧倒されるようになりました。ルートが侵害された多くのシステムと、盗み取られた何万ものユーザアカウント/パスワードの組み合わせに関する報告に対応するため、チームのリソースは、その限界まで使い尽くされ、プログラムの責任者にまでエスカレーションされました。そこで、対応活動を手助けするためにプログラム内から追加スタッフを調達する計画の概要が説明され、管理者によって承認されました。

例：1999 年のメリッサウィルスの流行は、CERT/CC 内でエスカレーションされたインシデントでした。CERT/CC は、その活動の前まで、ウィルス報告をその対応活動の対象にしていませんでした。その時点までウィルスは一般に、広範囲に及ぶものではありませんでした（例えば、汚染されたファイルの共用によって広がったり、限られた数のユーザや単一の団体にのみ影響したりしていました）。この種の脅威がエスカレーションに値するようになった



たのは、ウィルスが伝搬方法としてインターネットを使用するようになってからです。これは、Constituency に対する CERT/CC のサービス提供方法を変えたイベントの一例です。

### 3.8.7.1 複数のインシデントエスカレーション

優先順位に関係なく、個々のインシデントをエスカレーションさせる必要が生じる場合があります。インシデントのエスカレーションは一般に、インシデントハンドリング担当者がインシデントの1つ以上の側面に適切に対処できない場合の結果として生じます。インシデントハンドリング担当者は、エスカレーションしたインシデントに適切に対応するために、最後には追加の支援や管理職による監督が必要になったり、他の作業を肩代わりしてもらう必要が出てきたりします。インシデントが展開し、新しい情報が見つかり、そのインシデントが割り当てられた人間には、インシデントに適切に対応するための技術的専門知識がないことが明らかになる場合があります。その場合にエスカレーションの必要が生じます。当然のことながら、インシデントのエスカレーションは、インシデントの優先順位付けに関連する問題と同様の問題によって左右されます。

例：新人スタッフが電子メール爆弾インシデントに対応しています。関係のあるサイトとの通信中に、新しい情報が見つかり、攻撃の開始に使用されているアカウントそれ自体が侵害されていることが分かりました。このアカウントには、1,000 を超えるさまざまなシステムのパスワードファイルが含まれています。このインシデントには多数のホストがかかわっており、スタッフにも経験が不足しているということから考えて、このインシデントにはエスカレーションが必要です。

個々のエスカレーションでよく使用される基準には次のようなものがあります。

- 攻撃を受けているサイトおよびシステムの数
- 危険にさらされているデータのタイプ
- 攻撃の深刻度
- 攻撃の状態
- 攻撃元または攻撃対象
- インフラの完全性への影響度または復旧のコスト
- 見たところ「安全な」システムに対する攻撃
- インシデントに対する世間一般の認識
- 使用されている新しい攻撃方法
- コミュニケーションの断絶
- 個々の CSIRT スタッフの専門的な技量、知識、経験

また、チームでは、通常とは異なる、または重要になる可能性がある状況を管理者にただ通知するだけのエスカレーション基準が決められているのが一般的です。

例：あなたの **Constituency** 外のローカルネットワークサービスプロバイダが、公開されているニュースグループに詳細なインシデント報告を送信しました。この報告では、サイト内の侵害されたシステムから 1,000 個のリモートシステムへ接続したことを特定しています。接続のいくつかは、無許可の活動によるものであると考えられます。リソースが限られており、侵害されたシステムの登録ユーザに連絡をとることもできないため、報告元のサイトは、正当な接続と無許可の接続を区別することができません。記載されたリモートシステムのうち 50 を超えるシステムが、あなたの **Constituency** に含まれています。この活動に対してマスコミの注目が集まる可能性があるため、このインシデントは直ちに管理職にエスカレーションする必要があります。

コミュニケーションの断絶は一般に、チームに対する **Constituency** または他の関係者の不満（妥当かどうかは無関係）に起因します。**Constituency** は、インシデントの技術的または手続き上の対処方法に満足していないのかも知れません。あるいは、スタッフに対する特別な不満があるのかも知れません。チームの評判が危うくなるこのような状況では、管理職へのエスカレーションを行うのが賢明です。

インシデント情報が欠如していると、チームは先に進むことができない場合があります。しかし、たいていの場合、これは問題にならず、チームは入手できる部分的な情報を利用してインシデントをフォローアップします。とはいえ、重要なインシデント情報の欠如は懸念の原因になります。重要な情報が存在するのにそれがチームに渡されていないと考えた場合、情報取得のためのさらなる手段（または影響力）が得られるように、インシデントをエスカレーションすることがあります。

例：チームの **Constituency** 内のあるサイトが、継続して侵入者の活動の起点となっています。チームは、このサイトに対して電子メールと電話で何度も情報の提供を求めてきましたが、いまだに何も提供されていません。チームは、エスカレーションにより、このサイトにチームメンバを送ることで通常のサービスレベルを超えることができるかも知れません。またこのインシデントをエスカレーションするもう 1 つの方法としては、制裁措置（例えば、利用規定で概説されている正当な方法で対応しなければ、ネットワーク接続を遮断する、など）をサイトの管理者に伝えるといった方法もあります。

### 3.8.7.2 複数のインシデントエスカレーション

エスカレーション基準は、インシデントハンドリングサービスの観点から、その他の要素も考慮に入れる必要があります。例えば、チームが現在受けている全体的な作業負荷、ミッションを果たすための要件、インシデント活動の全体像にそのインシデントを適合させる方法を獲得して維持する必要性、チームが利用できる追加リソースなどです。

チームは、対応できる限度以上のインシデントを抱えていたり、発表された対応期限内に間に合わせることができなかつたりする場合があります。インシデント報告の回数が速いペースで増えるにつれ、このような状況が次第に発生するようになってきます。またあるときには、インシデント報告に突然、急激なピークが

やってきました。どちらの場合も、チームが状況に適切に対処できるように、エスカレーションを適用できます。

エスカレーションの結果としてもたらされる（大抵は同時に適用される）アクションは、チームごとに決めます。実行可能なものとしては、追加リソースの適用（例えば、スタッフの勤務時間の延長や他のスタッフに対する CSIRT の支援要請など）、または提供するサービスのレベルの低減などがあります。

例：2000 年問題のとき、CERT/CC の管理者は、技術面および管理面での追加支援を親組織のメンバに要請しました。追加の技術スタッフは、情報の一覧表作成、サイトとの電話連絡、Web および電子メール文書用コンテンツの作成支援に投入されました。追加の管理スタッフは、CERT/CC ホットラインの応答を手助けしました。追加スタッフのおかげで、チームのインシデントハンドリング担当者は、必要とされるインシデント分析や対応作業に専念し続けることができました。

CSIRT は、追加リソースを求めてインシデントをエスカレーションする場合は、そのようなリソースを得るための、確立済みで、且つ合意に達しているガイドラインに従う必要があります。計画と手順については、追加スタッフを提供してくれる部門と前もって話し合っておく必要があります。スタッフは、要請があったらいつでも手助けできるように、あらかじめ選定し、訓練しておきます。支援を要請するための連絡窓口と方法を事前に確立しておけば、エスカレーションプロセスが円滑化されます。またこれにより CSIRT スタッフは、連絡窓口や訓練方法を考えることなく、進行中のインシデント活動に集中し続けることができますようになります。予想されるリソースには次のようなものがあります。

- CSIRT 内で IR 部門以外の他の従業員
- 親組織内で CSIRT 以外の他の従業員
- 他のチーム、外部のコンサルタントまたは専門家
- Constituency または有志

支援の獲得は、スキルと専門知識、選ばれるグループへの要求によって、手配や交渉が簡単であったり困難であったりします。

エスカレーションの結果、インシデント対応において提供されるサービスのレベルが下がる可能性が生じることがよくあります。このような場合は、そのエスカレーションをすべてのインシデントに適用する必要があるかどうか、あるいは、特定のタイプのインシデントを除外できるかどうか、判断することが重要です。時には、サービスのレベルは、チームが被害者に速やかな直接支援を提供するだけというレベルにまで下げられることがあります。これは、チームを安定した状態に戻すために必要なステップですが、影響もあります。特に、ある特定のインシデントの犯人を明らかにするための通常の一連の取り組みに悪影響を及ぼします。また、侵入者が使用した手法とメカニズムの分析結果が制限されることもあります。

インシデント対応を調整する 1 つの大きな利点は、CSIRT が全体像を作成、確認、解釈できるということです (3.4.2.1 節を参照)。この全体像はそれだけで、Constituency への重要なサービスです。しかし、これはまた、即時および将来のリソース管理を決定する上での根拠となる指標の役割も果たします。したがって、通常のサービスが減って全体像が把握できなくなると、エスカレーション時、つまり全体像がチームとその Constituency の両方にとって重要なときに、特に深刻な損失になります。可能な限り、全体像の維持に不可欠な、インシデントに対する必要な分析レベルが保たれるように、注意を払う必要があります。

チームが危機的状況にあり、作業負荷または他の予期しないイベントによってリソースがすべて消費されている場合は、できるだけ早く通常の運用に戻ることが重要です。そして、危機が去ったことを判断するための一定の基準を確立する必要があります。これにより、チームメンバのストレスレベルが緩和され、危機が生じていたときに中断されていた通常業務を再編成し、優先順位を付け直し、正常に戻すことができます。

### 3.8.8 情報開示

チームを運営するためには、情報を開示する必要があります。しかし、開示が不適切に行われると、この日常的な活動がチームの廃止につながる可能性もあります。不適切な (間違った、許可されない) 開示を防ぐために、開示されるすべての情報は、チームの開示ポリシーに準拠してはなりません。このポリシーは、チーム運営の認知度と成果を上げるために重要であるため、4.2.3 節「情報開示ポリシー」で詳しく取り上げます。ここでは、一般的かつ現実的な問題について説明します。

情報の開示が必要な理由はさまざまであり、その情報を受け取る団体や組織もさまざまです。情報開示のプロセスは、その情報を受け取るグループ、および情報に対するそのグループの計画によって異なります。次に、情報を受け取るさまざまなグループと、情報を受け取る理由の例を示します。

情報の開示先として以下が考えられます。

- 発見された新しい脆弱性にかかわっている他のチーム。
- インシデント分析または対応作業で協力している他のチーム。
- 攻撃対象または攻撃元であるサイト。
- 管理職。予算のため。
- 管理職。統計報告のため。
- リスク管理グループ。インフラおよびセキュリティの改善計画を支援するため。
- 資金提供団体または株主。CSIRT 活動の正当性を証明するため。
- 法執行機関。捜査または起訴のため。
- 政府機関。届け出またはさらなる報告のため。

- 既得権益を持つすべての人。進行中の活動、および推奨される軽減または予防方法を認識させるため。

開示の必要性は、要求または報告によって生じることがあります。また、開示は、警告や勧告の発表など、特定のアクションを要求するイベントによって生じることがあります。CSIRTの開示ポリシーは、開示のタイプおよび理由の両方に関連する状況を考慮に入れる必要があります。

例：Constituencyの中に大規模な攻撃の対象になっているサイトがあるときは常に、CSIRTは既知の被害者だけではなく Constituency 全体にその旨を知らせます。通常、そのような攻撃の攻撃元は明らかにされません（攻撃対象となったサイトも明らかにされないことがあります）。しかし、時には、攻撃の起点を開示する正当な理由が存在します。例えば、攻撃を阻止するために起点の情報が不可欠である場合、起点が是正措置をとろうとしない場合、（本当の緊急事態の際に）チームのリソースが使い尽くされ、被害を最小限にするまたはくい止める唯一の方法が、攻撃に関するできるだけ多くの情報（予防策や事後対応策など）を Constituency に提供してそのサイト自身に対応させることである場合、などです。Constituency 全体に知らせる重要な理由は、システム管理者、ネットワーク管理者、およびセキュリティ管理者の注意を喚起するためです。そして、一般ユーザとともに、気付いていない可能性のある疑わしい活動を監視し報告するためでもあります。

ポリシーを定義する際には、最小主義的な方法を使用する必要があります。大部分の対話および開示では、情報全体を明らかにする必要はありません。本当に必要なのは一部分の情報だけだからです。したがって、ポリシーの記述によって、デフォルトである「知っておくべき事柄」と、正当であることが証明され且つ厳密に定義された例外における全面開示のどちらにするか決める必要があります。

例：DFN-CERTによって CERT/CC に新しいアーティファクトが提供された場合でも、そのアーティファクトが収集されたサイトに関する情報は開示されません。その一方で、入手元を隠す必要がない場合や、入手元が USENET ニュースグループなどの公開されているものである場合には、入手元が開示されることがあります。CERT/CC は、アーティファクトを分析するために入手元からのさらなる情報が必要になったら（入手元がサイトの場合）、その情報がなぜ必要か理由を添えて情報を要求します。その理由が有効であれば、DFN-CERT はサイトの識別情報を明かす前に、サイトと連絡を取り、状況を説明して、要求された情報を開示する許可を求めます。たいていは許可されますが、それでもなお、最初に尋ねることが重要です。間違いなく、このような情報はできるだけ早く得られる方が有益です。

情報の開示はさまざまな形をとり、それぞれにトレードオフや利点があることが考えられます。3.5.1節「アナウンスのタイプ」では、発表のタイプ（注意喚起、アラート、勧告、参考情報、ガイドライン、技術手順）について説明しました。一般に、これらは公開されるアナウンスです。情報の開示は、これらの例が示唆するものより明らかに範囲が広がります。インシデント報告（特定のインシデントにかかわる Constituency や仲間のチーム向け）や内部報告（例えば管理者向け）など、リストには多くの項目を追加できます。

ポリシーは他にも影響するため、誤解や問題を防ぐ最善の方法は、すべての状況に適した情報開示の初期設定を規定することです。選択の幅がある場合、選択に必要なデータは、実際の状況で必要になる前に要求しておく必要があります。これにより、余計な遅れを回避できます。

例：AusCERT は最初、サイトがインシデントに巻き込まれたときに AusCERT がサイトの連絡窓口情報を別の CSIRT に渡してもよいかサイトに尋ねる登録プロセスを実装しました。サイトは特定のインシデントに関して連絡してほしいときは、AusCERT にその旨知らせれば、連絡窓口情報が他の CSIRT に渡されないようになります。後日、理由を問わず連絡窓口情報が必要になった場合、AusCERT はそのサイトに戻り、許可を求めることができます。

サイトの連絡窓口情報および被害に遭ったサイトの情報に関するプライバシーの問題は言うまでもないことです。適切なポリシーを定め、地域の法律に注意を払うことで、多くの問題を回避できます。

CSIRT によっては、情報提供用のフォームを用意しているところもあります。トレードオフもいくつかありますが、大抵はフォームにより報告者とチームの両者にとって関連情報の入手が容易になります。インシデントまたは新しい脆弱性の報告者は、多くの質問に答えることを求められますが、これにより、標準化されたフォームを使用せずに回答する場合よりもはるかに情報量が増えます。

例：CERT/CC は、インシデントおよび脆弱性の報告フォームを Web サーバから入手できるようにしました<sup>46</sup>[CERT/CC 1997a, CERT/CC 1996]。

チームによっては **Constituency** に対してフォームへの記入や決められた一連の情報の報告といった特定の要件を課すこともあります。またポリシーによっては、チームまたは組織は、不完全な情報または非公式な情報を受け取ることもあります。

統計と傾向の生成は、単なるインシデント対応を越えた、CSIRT が提供する最も魅力的なサービスの 1 つです。CSIRT は特別な役割を持つため、次のことが可能です。

- **Constituency** のためにインシデント活動の全体像を作り上げる。
- 資金提供団体に追加の背景情報を提供する。
- **Constituency** により良いサービスを提供する。
- 実際的な見通しに対する意識を高める。

CSIRT のミッションには、収集した情報を最大限に活用して **Constituency** に利益をもたらすことも含まれています。CSIRT にとって重要なことは、収集する情報についてよく考え、その情報をどのように使用するか、誰に配布し開示するか、他者とのさまざまな対話または協力関係においてどのような情報開示ポリシーお

---

<sup>46</sup> [http://www.cert.org/nav/index\\_red.html](http://www.cert.org/nav/index_red.html)

よび手順を適用するか、戦略的に計画することです。例えば、FIRST への CSIRT 統計情報の開示については担当予定の各メンバと可能な用件について検討します。担当予定のメンバは、どのような情報をどのような形式で開示できるか、よく考える必要があります。

情報の開示に関係する最後の問題は標準化です。開示プロセスは各 CSIRT の最も目立つ業務である可能性があるため、人目を引くような統一されたインタフェースが「世界」、特に **Constituency** および他の CSIRT に提供されるように細心の注意を払う必要があります。情報の配布方法は、例えば以前の統計と比較できるように、時がたっても一貫していなければなりません。さらに、標準化により CSIRT の一貫した「コーポレートアイデンティティ」が守られます (CSIRT が別の組織内部に置かれる場合は、この親組織の要件を考慮に入れる必要があります)。この一貫したインタフェースの一部として検討すべき項目は次のとおりです。

- 提供されるテキストの形式 (ヘッダ、アウトライン、フッタ、ロゴ)。テキストの配布がメーリングリストによるかオンライン情報サーバによるかは無関係。
- 正式な署名による真正性。
- 内容およびスタイルのガイドライン。

---

## 4 チームの運営

第2章では、インシデントハンドリングサービスの基盤となる主な機能、それらの機能間のやり取り、情報のハンドリングについて説明しました。本書では、インシデントハンドリングサービスの構築に必要なものについて説明してきました。これを家の建築に例えてみます。家の設計図は提示しました。部屋とその用途も説明しました。階段、廊下、電気、電話、暖房、水道の各システムについても検討しました。まだ取り上げていないのは、家をどのように機能させ、守っていくかについてです。すなわち、暖房およびその他のシステムの保守、毎年の煙突掃除、保険手続き、火災報知および防犯警報の手続きです。これらは家の「運営」要素です。この章ではこうした CSIRT の運営について詳細に説明します。

この節では、まず主な運営要素について概説し、次に運営上の4つの不可欠な問題、すなわち基本ポリシー、継続性の保証、セキュリティ管理、スタッフの問題について説明します。

これらのトピックの多くは、インシデントハンドリングサービスだけにとどまりません。このため、これらのうち一部の側面については、既に第3章で取り上げています。その都度同じ説明を繰り返す代わりに、該当する参照先の節を示します。ただし、この節では、第3章の「ポリシー」のレベルで可能だった方法よりも実際的な方法を紹介します。この章では、実用的で一般的な「手順」について説明します（手順とはポリシーステートメントの実装であることを思い出してください）。

### 4.1 運営要素

運営要素とは、電子メールシステムから作業スケジュールまでのさまざまな運営の根幹をなす基礎です。ここでは運営要素を、インシデントハンドリングサービスと直接関連する要素に限定し、給与制度やコーヒーマーカーなど、間接的な要素はすべて除外します。この節で取り上げる要素は、すべてを網羅したものではありません。最も重要で現実に即した運営の要素の中から選択したものについてのみ説明します。必要に応じて、実際の例を挙げ、特に重要な事柄については詳細に説明します。

#### 4.1.1 作業スケジュール

作業スケジュールでは、通常の営業時間と営業時間外を区別する必要があります。これには、交替制勤務（関係するスタッフを含む）、営業時間外スタッフの手配



(警備員や、取り次ぎサービスを提供するオペレータなど)、交替要員、スタッフ総がかり時の手配などが含まれます。

交替制勤務について検討する際には、ルーチンワークを約 2 時間行ったら明らかに休憩が必要であり、ストレスの多い集中した作業にかかわっているときには (大きなインシデントの最中など) 1 時間でも疲労することを念頭に入れておくことが、経験から言って大切です。作業スケジュールを設定する際には、継続性の保証 (詳細については 4.3 節「継続性の保証」を参照) が、提供するサービスの質に関する最も重要な目標となります。

### 4.1.2 通信

これには、電話、ファックス、携帯電話、ポケットベル、自動応答機能などの「昔ながらの」通信方法が含まれます。この種の技術 (およびそれ以外の通信) は、要件に従って組織およびそのメンバと連絡をとり、「且つ」必要に応じて Constituency やその他の関係者とのコミュニケーションを開始するための技術を備えておくために必要です。ただし実装はチームのミッションとサービスの仕様によって異なります。

しかし、保証された通信などは存在しないことを思い出してください。電話システムでさえ、ときどき故障することがあります。電話のベルが聞こえなければ、最高にぜいたくで豪華な技術も役に立ちません。同様に、グランドキャニオン (あるいは暗くて長いトンネル) では、携帯電話はおそらく機能しないでしょう。Constituency は、電話でサービスを利用しようとしたときに誰かが電話に出るまで呼び出し音を 5 回以上聞かなければならないとしたら、たいてい不快な気分になります。また、緊急事態だと考えているときに音声メッセージシステムにつながったとしたら、もっと不愉快な気持ちになるでしょう。そしてメッセージを残したにもかかわらず、迅速な応答 (例えば 15 分以内) がなければ、Constituency はさらに不快になると思われます。一方、ボイスボックスは、最初の受領確認や、期待するものに関する追加情報を提供するのに役立つ場合があります。最近の装置は、新しい電話を受けた後、あらかじめ決められた番号に連絡します。これを使えば、発信者は、CSIRT チームメンバに連絡をとるのにそのメンバの電話番号を知る必要がありません。

### 4.1.3 電子メール

今日のネットワーク環境における優れた電子メールシステムの必要性は言うまでもありません。マルチメディア (MIME) およびセキュリティ (PGP、S/MIME) の最新の規格に準拠した使いやすくて堅牢な電子メール環境を構築することは可能です。しかし、インシデントハンドリングサービスでは、優れたフィルタリング機能、高度な検索機能、自動応答ツールなどほかにも必要な要件があるため、CSIRT にとっては決して簡単な作業ではありません。

CSIRT 固有のニーズに合う製品がないため、通常は、いくつかの標準ツールを組み合わせ、スクリプトを使ってそれらに機能を加えた独自の電子メール環境を構

築します。さらに、ユーザの中には PC オフィスパッケージを使用して明らかに ASCII 互換ではない「美しい」電子メールを書くユーザがいる可能性があるため、CSIRT はさまざまなコンバータ (MIME、binhex、uudecode、zip、gzip など) およびワードプロセッサを使用します。技術が進化するにつれて、このような互換性の問題は、シームレスな使用のために一層透過的になると思われます。とはいえ、ワークフローが扱えるように、電子メール環境とその他の環境との間のインタフェースの必要性について検討することは重要です。そのようなインタフェースがなければ、入ってくる情報の大部分は自律的、自動的には統合されません。電子メールは、情報を非同期に交換するための使いやすい技術です。受信した電子メールに優先順位を付けることによって、CSIRT スタッフの作業効率を向上させることができます。実際、多くの場合、電子メールは電話ほど時間がかかりません。しかし、電子的な手段が直接的なコミュニケーションに取って代わることができない場合もあります。いずれにせよ、Constituency は使用される通信方法によらず、時宜を得たフィードバックを期待していることを認識しなくてはなりません。

#### 4.1.4 ワークフロー管理ツール

作業負荷が高く、交替勤務体制を敷いている運営環境では、ワークフローや進行中の作業の引き継ぎを管理するのに役立つツールが不可欠です。手書きの業務日報は古典的な一例です。最近では、問題が複雑で、関係する情報が膨大であるため、この種の業務日報は廃止してしかるべきです (しかし残念ながらそうはなっていません)。CSIRT には、イベント (インシデント、要請、進行中の分析など) の流れをたどったり、イベントを追加したりできるワークフロー管理ソフトウェアツール (実質的にはプログラムをかぶせたデータベース) が必要です。現在は、一般的なデータベースとの組み合わせで動作する優れたワークフロー管理ツールが販売されています。しかし、たいいていの場合、このようなシステムのセキュリティは不十分です。したがって、一般的には、安全な (ただし、外で対応する場合や分散型の CSIRT にとって厄介な場合がある) イントラネット内でのみ使用できます。電子メールツール、Web、電話システム (およびポケットベル) の統合は、受信するすべての情報を収集し、イベントを相互に連結するために必要です。

#### 4.1.5 World Wide Web 情報システム

World Wide Web (WWW) は、情報の取得に使用され、至る所に普及している現在最もホットな媒体です。言うまでもなく、これがなくては、チームは何もできません。既存の匿名 FTP ディレクトリもまだ、プログラムや文書の大規模なアーカイブにアクセスする手段として使われています。しかし、このアーカイブに Web を介して一応アクセス可能になったという点と、Web ベースの情報がこのアーカイブとリンクできるという点で進歩しています。ところで CSIRT の Web サーバと公開情報サーバ (公開情報を提供する) の情報が許可のないグループによって操作されないように安全な方法で実装する必要があるのは明らかです。とはいえ、後者の要件は一般にとっての利便性と対立します。この矛盾を回避するために考えられる 1 つの方法は、ファイアウォールで保護された DMZ (非武装地帯) 内に Web サーバを配置し、優れた保守および制御手段によってその安全性を維持することです。維持する情報の真正性と完全性を確保するには、内部に置

かれたマスタサーバに情報を保持し、その情報を定期的に（例えば毎晩）Webサーバにダウンロードすることが有効な場合があります[Kossakowski 2000]。また、暗号チェックサム（TripwireやMD5など）に基づいた追加の検査も役に立ちます。チームメンバが内部情報を使用できるようになっている場合、これらの各ページと、この情報を指し示しているすべてのリンクは、公に配布する前に取り除いておく必要があります。

#### 4.1.6 IP アドレスとドメイン名

セキュリティ上の理由で他のすべてのネットワークから内部ネットワークを切り離すには、チーム専用のIPアドレススペースの所有権が必要になります。インターネットIPアドレススペースのCIDR（Classless Inter-Domain Routing）ブロックでは、あなたのチームだけがそれらのアドレス番号を使用し、上位組織の他の部署が使用しないのであれば、問題はまったくありません<sup>47</sup>。あるいは、チームは、専用アドレススペース（例えば10.0.0.0）を使用し、外部接続についてはネットワークアドレス変換（NAT）またはファイアウォールを利用することもできます。

ドメインネームサービス（DNS）は、特定のホストで動作しているオペレーティングシステムのタイプなどの機密情報を列挙したり、すべての内部ホストの完全な一覧表を配布したりするべきではありません。これは、技術的な攻撃やソーシャルエンジニアリング攻撃に役立つ情報が明らかになる可能性があるためです。ほとんどの場合は、チームの存在をアピールし、電子メールまたはWebのための覚えやすいインタフェースを提供できるようにチーム専用のインターネットドメインを要求することは妥当であり有益です。一般に、ドメインスペースはcompany-csirt.some-org.tldまたはcompany-csirt.tldという形になります<sup>48</sup>。

#### 4.1.7 ネットワークとホストのセキュリティ

インシデントハンドリングサービスの内部コンピュータやネットワーク、他のネットワークへの接続は、安全に設定され、攻撃から守られている必要があります。これは、内部ネットワークをそれぞれ異なる機能を持つ区画に分割し、十分にしっかりしたファイアウォールを通じて外部とのインタフェースを持つことを意味します。少なくとも2つの区画があるべきです。1つは運用ネットワークで、ここですべてのサービスタスクが処理され、使用されるデータが格納されます。もう1つはテストベッドです（テストをまったく行わない場合を除く）。区画間は分離されていて、データ転送が必要な場合に限りファイアウォールを介して相互に接続されるようにするべきです。テストベッドに対して一時的な接続を確立する場合は、それはあくまで一時的であるようにすることを注意してください。ほとんどの場合、テストベッドを他のネットワークに接続する必要はまったくありません。テストネットワークを他のマシンやネットワークに接続することが危険

---

<sup>47</sup> すなわち、CSIRTのIPアドレススペースは、親組織が使用するIPアドレスとは異なるということです。当然のことながら、CSIRTのドメイン名とIPアドレスを取得し登録するための労力と料金が必要になります。

<sup>48</sup> 「tld」は.com、.edu、.org、.nl、.de、.ukなどのトップレベルドメイン(top-level domain)を意味します。

過ぎる場合は、取り外し可能なメディアを使用してデータを転送する方法があります。

選択するファイアウォールは、予算に応じたものになってしまうでしょう。一般に、二重スクリーンファイアウォールは高水準のセキュリティを提供します。この種のファイアウォールは、外向けの1つのルータ、内部区画向けに1つのルータ、1つ以上の要塞ホスト (bastion host) から構成されます。この要塞ホストは、内部のクライアントまたはサーバが外部の通信相手と「直接」やりとりしないように、アプリケーションレベルのゲートウェイ (プロキシ) によって内部クライアントと外部サーバを相互接続します。さらに、DMZ は、内部に対しても外部に対してもファイアウォールで保護されており、利用可能なサービスを一般の人々に提供するサーバ (WWW サーバ、ftp サーバ) 、あるいは、ゲートウェイまたは転送システムとして機能するサーバ (プロキシサーバ、電子メールゲートウェイ) を配置します。

言うまでもなく、すべての組織の中で CSIRT こそは、セキュリティパッチおよび更新に関してシステムを最新以上の状態にしておかなくてはなりません。侵入の試みを突き止めて防ぐために、ログイン機能、ラッパー、それ以外のさまざまな防御ツールが役立つはずですが、しかし、機密情報を扱う作業にホームシステムやノートパソコンを使用する場合は、ホームシステムのセキュリティ、およびホームシステムやノートパソコンからのアクセスも考慮する必要があります。

サービス運用妨害攻撃は、チームの業務遂行能力に影響するため、慎重に検討する必要のある特別な攻撃に分類されます。複数のサービスプロバイダのネットワーク接続を利用できるようにしておくことは、この問題を解決する一助となるでしょう。少なくともそうすれば、正面玄関がブロックされた場合、非常口を使用して、電子メールなどの最低限の通信手段を確保することができます。CSIRT のセキュリティ管理の詳細については、4.4 節「セキュリティ管理」で取り上げます。

## 4.2 基本ポリシー

多くのポリシーは「基本」(つまりチームが選択するサービスやサービスレベルに依存しないもの) であり、規定されている必要があります。基本的な事柄については第2章で取り上げました。また、第3章では、サービス固有のポリシーの例をいくつか挙げました。この節では、チームの運営のための基本ポリシーについて詳しく説明します。しかし、基本ポリシーの内容にはサービスおよび品質の詳細が影響を及ぼすことが考えられるため、以下の説明は一般的なものであり、分かりやすいようにいくつかの例以外は取り上げていない点を念頭に置いてください。

## 4.2.1 行動規範

組織の行動規範とは、組織のミッションステートメントの趣旨に則し、組織の品格を保つためにどのように行動すべきかを示した一連の一般規則のことです。行動規範は、組織のあらゆるレベルのスタッフに適用されます。行動規範は取り組み姿勢であり、職位による違いがあってははいけません。また、行動規範は、ある状況下でどのように振舞うべきかについての基本的な指針であり、チームの内外両方におけるやり取りの基礎を築くものです。

行動規範は、他のポリシー、ルール、手順がすべて適用できないように思われる場合や、考える時間もなく取り残された場合に頼みにできるポリシーです。そしてそれは、経験豊富なインシデントハンドリング担当者のプロとして当然の行動パターンとなるべきものです。新人の CSIRT スタッフには、承認されたチームの行動規範を自分のものにするように教育する必要があります。

行動規範は何ページもの文章にする必要はありませんが、長くても、例を示して説明しても構いません。行動規範が長過ぎる場合は、おそらく、明らかに含めるべきではないような手順が含まれていると思われるかもしれません。短くするメリットは、内部に対しても外部に対しても伝えやすいという点です。誰も自分の行動規範を恥ずかしく思うはずはありませんから、Constituency と仲間のチームのために公開したらどうでしょうか。これは、チーム間の協力に必要な基本的認識を形成するのにも役立ちます。

(CSIRT ポリシーおよび手順を補完する) 非常に簡単な行動規範の例を次に示します。

しかるべき好奇心を明示します。しかし、同時に...  
適度な自制心も示します。

知る必要がある人には十分な情報を提供します。しかし...  
うわさ話はしません。

しかるべき注意を払います。しかし...  
優先順位を忘れません。

常に礼儀正しく前向きに振舞います。しかし...  
適切に検証しないうちは誰も信用しません。

手順を理解し、それに従います。しかし...  
ミッションが優先されることを決して忘れません。

この例は、ほとんど詩といってもいいものです。形式、および言葉の選択は、すべて組織のタイプに応じて異なります。行動規範は、組織のミッションと性質によって決まることを忘れないでください。もう 1 つの興味深い例はある CSIRT 行動規範です。この行動規範 (図 6 を参照) は、CERT Coordination Center の主席マ

ネージャである Rich Pethia によって 1991 年 1 月に作成された行動様式の一覧を書き換えたものです<sup>49</sup>。

## 4.2.2 情報のカテゴリ化ポリシー

CSIRT には情報の分類に関するポリシーが必要です。このポリシーがないと、CSIRT スタッフは、自分で考えた分類を各情報に適用したり、各情報をまったく区別しようとしなかったりします。個人個人の認識は異なる可能性があり、結果として矛盾し、場合によっては不適切なサービスにつながることもあるため、分類が正しく行われるように導くためのポリシーを用意する必要があります。

このポリシーの複雑さと長さは、チームのミッションと **Constituency** によって異なります。例えば、最も簡単なケースでは、「機密」情報と「残りすべて」の情報という区分しかありません。機密情報はすべて格別に注意して扱わなければなりません。一方、残りすべての情報は公開されていると考えられます。



**CERT® Coordination Center**  
行動規範項目

**CERT® Coordination Center**  
行動規範

11. 事実を述べること。
12. 誠実であること。
13. コントロールすること。
14. 過激な行動を取らないこと。
15. 信頼を維持すること。
16. 保証はしないこと。
17. 指導すること。
18. 肯定的な表現を使用すること。
19. 品質管理をすること。
20. 建設的な意見を述べること。

1. CSIRTの強みに意識を向けること。
2. 対象者に合わせて対応すること。
3. 自分の考えを表明すること。
4. 他人の話をしないこと。
5. 完全な文章を作成すること。
6. 簡潔な文章を作成すること。
7. 仲間内の言葉を使わないこと。
8. 繊細であり社会的であること。
9. 横柄な態度をとらないこと。
10. 馴れ馴れしい態度をとらないこと。

<http://www.cert.org/>  
© 2000 by Carnegie Mellon University

図6 : CERT/CC 行動規範

<sup>49</sup> CERT Coordination Center、「CSIRT Code of Conduct」、Managing Computer Security Incident Response Teams (CSIRT) コースの資料。

もう少し細かい分類方法を使用すると、チーム内でのみ使う「内部機密」という分類を定義できます。「内部非機密」は、知る必要がある場合のみ開示するという原則で仲間のチームと交換するためのものです。「外部パートナー」は、Constituency や仲間のチームとやり取りするためのものです。最後の「外部公開」は公開情報のためのものです。これは、CERT-NL によって採用され、その運用の枠組みの中で詳細化されています[CERT-NL 1992]。

CERT-NL のこの分類の短所は、現実には「内部機密」と「内部非機密」の違いが常に明確であるとは限らない点です。これらの表現を「完全機密」、「部分機密」、「非機密」に変えると良いかも知れません。主な違いは、最も厳格な分類ではチーム内に限って伝達が認められるのに対し、「部分機密」の分類では、知る必要がある場合のみ開示するという原則と、多かれ少なかれ信頼のあるやり取りの相手（他の CSIRT など）の信頼度順の一覧表とを組み合わせている点です。しかし名前が問題だということではありません。本当に唯一重要なことは、全員が同じ分類方法に従うことです。最初に分類方法を整備する際の実際的な方法としては、チームメンバに対して、いくつかの文書を分類するように別々に依頼し、（各チームメンバによる分類の根拠を理解するために）各自がその文書をどのように分類またはランク付けしたかを調べて評価することで、全員が支持して使用できる分類を作る上でのコンセンサスを得るという方法が考えられます。

例えば、軍関係のチームの場合、すべての分類について情報の取り扱い方法の手順を網羅した、軍事情報のすべての機密レベル（「最高機密」または「国家機密」まで）が整備されていることが期待されます。

また、選択された分類は情報の取り扱いの方法（例えば、保存、開示、処分）に影響を及ぼす点に注意してください。そのため、分類ごとにポリシーと手順を作成する必要があります。そうすれば、この首尾一貫したポリシーと手順の組み合わせが、情報の内容に関係なく、その分類のすべての事例に適用されます。運営上の作業に関わるすべてのポリシーと手順に、各分類の取り扱いの方法に関する記述を含めるべきです。これには、デフォルトの分類値の指定が含まれます。デフォルト値が「公開」であるか「内部」であるかによって大きな違いが生じます。デフォルト値は情報のタイプによって異なる場合があります。また、各分類においてどのように取り扱うのかも必然的に異なります。

例：連絡窓口情報のデフォルトの分類は「内部」であり、他の CSIRT によって発行され公に発表された勧告に対するデフォルトの「公開」とは異なる場合があります。

情報が複数の分類に属する可能性があると考えられる場合、その情報をどの分類に入れるべきかはっきりしないときがあります。ここで「Better safe than sorry（後悔するよりは安全策を採る）」という古いことわざが当てはまります。CSIRT 環境において選択される分類は通常、情報が最大限に確実に保護されることを保証するものです。こうすれば後になって、情報が不適切な分類に入れられたことを示す詳細が新たに明らかになっても、簡単に分類し直すことができます。

### 4.2.3 情報開示ポリシー

CSIRT が注意を払わなければならない最も重要な問題の 1 つは、どのようにして Constituency や他のチームに尊敬され、信頼してもらうかということです。信頼と尊敬がなければ、人々はチームに情報を報告するのを渋り、その結果、チームは効果的に機能できなくなります。インシデント対応の範囲内および範囲外の情報開示ポリシーを定義することが重要です。このようなポリシーがなければ、CSIRT スタッフは、電話や電子メールに対応するときいつ誰に何を言えるか、分からなくなってしまう。

大部分のチームでは、報告されたすべての情報を極秘に取り扱い、直接のチームメンバの範囲を超えて情報を共有することはありません。例外は、傾向調査と統計の目的のために一般情報を使用する場合、あるいは関係しているサイトおよび関係者が、自分たち自身やサイトについての情報を他者（インシデントに巻き込まれている他のサイト、法執行機関、インシデント対応を調整する他の対応チームなど）に開示することを承諾した場合です。

このポリシーは、独自の要件（場合によっては、外部監査の法律上の義務）を持っている可能性のある、他の組織や親組織から、CSIRT に提供された情報に設定されている情報開示制限を考慮に入れておく必要があります。例えば、他の CSIRT がインシデントを報告した場合、その Constituency は、報告された情報の開示に関して何を期待することができるのでしょうか？ この情報は、法執行機関や CSIRT 管理者に報告されるのでしょうか？ ポリシーには制約を明記すべきです。そしてポリシーを（Constituency や他の利害関係者に）公開すべきです。ではどのような場合に、チームは機密情報（連絡窓口情報までも）を法執行機関や裁判所に渡さなければならないのでしょうか？ 現在のところ、クライアントの機密保持に関して（医師や弁護士との義務と）同様の法的地位を持たせるような、CSIRT への義務付けはないようです。

例：CERT-NL がインシデントについての情報を CERT/CC に提供するというシナリオを考えます。インシデントはオランダの教育機関のサイトで発生し、そこから侵入者はアメリカのシステムへの攻撃を成功させたとします。CERT-NL は、ログとタイムスタンプを CERT/CC に渡し、適切な詳細情報をアメリカの当該サイトに送るよう依頼します。また、CERT-NL は、インシデントに巻き込まれた他のサイトに情報を渡してもよいかどうかを知らせます。さらに CERT-NL は、名前と連絡窓口情報は CERT/CC でのみ使用し、他には配布しないという了解の下で、オランダの教育機関のサイトの名前と、そのサイトのシステム管理者の連絡窓口情報を CERT/CC に提供するといったことが考えられます。

この追加情報は、CERT/CC が全体像や関連する活動を理解する上で役立ちます。CERT/CC は、この情報を利用することで、（おそらく、いくつかはまだ CERT-NL が知らない）オランダのホストが関係する、類似あるいは関連する他のイベントと当該インシデントを関連付けることができます。CERT-NL は、この追加情報を受け取ると、今度は、Constituency の他の 3 つのサイトが、以前検出されなかった（そしてその後、CERT/CC から受け取った情報に基づいて特定された）ルート侵害からの復旧を支援することができます。



チームに提供される情報の開示制限に加えて、情報開示ポリシーは、情報を受け取りたいという他からの要請も考慮に入れる必要があります。このような要請は一般に、詳細な技術情報または機密情報を求める要請です。

情報を開示するかどうか、そしてどこまで、またどのように情報を開示するかを決定する要素としては、基本的に3つあります。すなわち、情報の「目的」「対象」「分類」です。

1. なんらかの情報の開示には、根本となる目的が必要です。言い換えれば、誰かがその情報を「知る必要がある」ということです。この「知る必要がある場合に開示する」の原則は、あらゆる情報に適用できます。

例：サイト管理者に、使用している HTTP デーモンのソフトウェアバージョンが脆弱であるため、サイトのマシンが侵害されている可能性があることを警告するには、最低限の情報だけで十分です。侵入そのものに関する情報はなくても、必要なのは、脆弱性そのもの、利用可能な対策、またはパッチに関する情報だけです。

例：ただし、インシデントが脆弱なソフトウェアによって組み込まれたバックドアを介した侵入行為を伴う場合は、関連ログ、タイムスタンプ、および起点 IP アドレスの各情報を提供する必要があります。そしてその結果として、連絡窓口情報も一部明らかにする必要が生じることもあります。

この2つのケースでは、開示する情報の目的と範囲が異なります。

2. 情報の対象とは情報が関係する人のことです。例えば、CSIRTのConstituencyのメンバ、他のCSIRT、内部の管理職、法執行機関、メディア、訪問者、専門家、一般の人々などです。

明らかに、信頼している仲間の CSIRT と対話するときよりも、一般の人々に情報を渡すときの方が制約があります。

3. 情報の分類は（前述のとおり）情報のカテゴリ化ポリシーによって決まります。

情報を開示するかどうかの判断について言えば、明らかに、情報が「内部」（例えば、Constituency の連絡窓口のアドレス）であるか「公開」（例えば勧告）であるかによって違いが生じます。この分類は、情報を保護する方法に影響します。例えば、公開情報は、デジタル署名による真正性証明によってのみ保護される、標準的な電子メールで受け渡すことができます。これに対し、内部情報は、暗号化やセキュアチャネルの使用が求められます。

仮に、特定の情報を開示する明確な目的があるとします。開示の決定が下されたら、情報、分類、対象の各要素により、どのように開示するか、そして情報のどの部分を誰に開示するかが決まります。

例：世界中の何千ものホストを巻き込む侵入行為による、大規模なインシデントについて考えてみましょう。このインシデントの結果、巻き込まれたサイトによってさまざまな詳細なログファイルがチームに提供されました。

- 信頼関係のある CSIRT およびサイトの場合、このログファイルで特に CSIRT またはその Constituency に関係する部分を渡すことができます。
- その他の被害者には、将来この種の攻撃から保護する方法を示したガイドラインとともに、自分たちのログを検査できるように彼らのサイトに関連するログの項目を渡します。
- インシデントの規模と広がり、および攻撃の一般的な詳細について法執行機関に報告し、注意を促すことができます。
- インシデントの規模と広がりについて、注意を促し励ます言葉でメディアに伝えることができます。
- 信頼できる専門家に対しては、攻撃、傾向、痕跡について詳しく学べるように、（サイト固有の情報に限定するようにサニタイズした後の）いっさいの詳細を提供することができます。

#### 4.2.3.1 2次レベルの開示

他者に情報を開示すると、その他者が、受け取った情報をさらに広める可能性があります。これは、そうなることが明らかな場合もあれば（例えばメディア）、そうでない場合もあります（例えば内部の管理職）。開示の対象者がその情報をどのように取り扱えるかについて、その対象者と合意を得ておくことが重要です。情報は、いったん渡したらコントロールできません。対象者が情報をどのように取り扱えるのかを示した拘束力のある契約が存在していたとしても、情報は漏れる可能性があります（例えば、セキュリティ侵害によって）、情報開示の起点となった関係者が影響を受ける可能性があります（評判に対するダメージだけでなく訴訟の可能性もあります）。

例：メディアに対しては、チームがコメントまたは承認を行えるように、発表前に草稿を送ってもらうように要請または要求することがあります。

仲間のチームには、多くの場合、情報がチームの Constituency のためにのみ使用され、それ以上広がらないという（たいていは暗黙の）想定の下に詳細情報を提供します。

その他の相手に対する有用な方法の1つは、配布する情報にしかるべき使用方法を明確に示したラベルを貼ることです（例えば、「CSIRT 内での使用に限定」など）。この方法は、他者と機密情報を交換する場合に特に役立ちます。

#### 4.2.3.2 開示のタイミング

情報は「いつ」または「どれだけ早期に」開示すべきでしょうか？ 一方では、何かを開示する前に事実関係を確実に把握しておくことが望ましいですが、多くの場合、それには多くの時間がかかります。他方では、情報が多少不完全または不正確であっても、おそらく被害者にはできるだけ早く警告するべきです。興味深いことに、特にチームがその Constituency と非常に明確な契約を結んでいる場合に、この2つについて極端な場合には訴訟を招くことがあります。

例：営利CSIRTが、迅速な対応や注意喚起をしていれば防止できた可能性のある問題に遭遇した場合、そのConstituencyは非常に強い不満を抱くかもしれ

ません。システムの停止につながる不適切な情報が提供された場合や、CSIRTの警告にもかかわらず脆弱のままだった場合も、Constituencyが苦情を申し立てたり訴訟を起こしたりする原因となり得ます。Constituencyのこの種の行動が、Constituencyに対して権限を持たないチームや契約を結んでいないチーム、あるいは主に他者に対してアドバイスを提供しているチームに向けられることはあまりありません（例えば、国のチーム、CERT/CC、あるいは分散している大規模な企業チームなど）<sup>50</sup>。

#### 4.2.4 メディアポリシー

メディアは、重要なCSIRT情報を発表したり広めたりするのに強力で有効な手段なので、親密な関係を築くとよいでしょう。メディアポリシーを持つことは良いことだということは誰にでも分かります。しかし、非常に詳細な情報伝達のポリシーがあったとしても、メディアへの対応は特に難しいものです。

考慮すべき主な問題は、メディアとの主要な接点をどこに置くかということです。CSIRTの内部でしょうか？ それとも外部でしょうか？ CSIRTおよび関連チームのように、非常に技術的且つ機密性の高いデータを扱うチームの場合は、チームの外部にスポークスパークソンを置くことをお勧めします。この方法なら、スポークスパークソンが機密データにアクセスする機会はほとんど、あるいはまったくありません。なぜなら、情報伝達のポリシーとメディアポリシーに従ってメディアに伝達するという役割を果たすために必要な情報のみを知らされるからです。この情報は通常、大幅にサニタイズされます。このような方法により、メディアに話し過ぎるといった危険性や起こりうる訴訟が回避されます。メディアスポークスパークソンがチームの外部に置かれる場合は、現在の情勢に関する最新情報をスポークスパークソンが継続的に受け取れるように、チーム内の誰かが責任を持つ必要があります<sup>51</sup>。

##### メディア連絡窓口リストの作成

発表記事が、信頼できない、またはレベルが低いジャーナリストによって書かれないようにする、あるいは「不適切な紙面」に掲載されないようにするには、メディア連絡窓口と新聞または雑誌をいくつか選別して、協力していきたいメディアの連絡窓口のリストを作成すると役に立ちます。協力していきたい優れた専門的なジャーナリストおよび出版物を積極的に探すべきです。多くの出版物では優れた人材がこの分野の仕事を担当していますが、多くの場合、セキュリティは依然として弱いところではあります。メディアの連絡窓口を収集する作業の一環として、強固な認証手段を確立し、且つジャーナリストの（技術的な）経歴と隠れた意図を理解する必要があります。

##### 対応規則の設定

この規則により、メディアがチームに何を期待できるか、そしてチームがメディ

<sup>50</sup> ただし、チームが、ある国または地域で特に訴訟好きな場所にある場合は、権限がなくても訴訟を起こされる可能性があるということを認識しておく必要があります。

<sup>51</sup> Terry McGillen、『CERT Incident Communications』、5th FIRST Workshop on Computer Security Incident Handling、ミズーリ州セントルイス、1993年8月。

アとどのように付き合うつもりでいるかをメディア連絡窓口を示します。遠慮なくメディアに期待していることを明示しましょう。次に例を示します。

- CSIRT が指名したスポークスパーソンとのみ連絡をとるようにしてください。
- 引用を曲げて伝えないでください。
- 掲載前に、記事についてコメント、編集、または承認する機会をスポークスパーソンに与えてください。
- この規則に違反があった場合は、そのメディア連絡窓口をメディア連絡窓口リストから削除します。

#### メディアへの事前説明

メディアが来るのを待つのではなく主導権を握ることによって、現状を何度も繰り返して説明する必要がなくなり、時間を大幅に節約できます。また、事前説明をすることで、狼狽させられたかもしれない質問に備えることもできます。さらに1歩進めて、メディアにチームのミッションを確実に理解してもらい、この役割がどのように果たされるかについての包括的な認識を持ってもらうようにします。そして、こうした機会を利用して、事前対策となるメッセージを広めてください。

#### 外での振る舞いの規定

チームメンバとメディアスポークスパーソンは、公の場に出る可能性があります。メディアの注目を集めているときには、突然相手にされなくなるということはありません。したがって、常にメディアと向き合う準備をしておくべきです。思いがけなくメディアと向き合うことになった場合、最も簡単な解決策は「ノーコメント」です。この解決策はチームメンバには許されますが、指名されているスポークスパーソンには許されません。より洗練された（そして難しい）方法は、メディアとのやり取りについてチームメンバを訓練し、公の場で「言えない」ことではなく「言える」ことを理解してもらうことです。この方が前向きであり、特定の状況について事前説明がなかったとしても、結果としてメディアに前向きな印象を与えます。

#### アナウンスによる広範囲への伝達

必要に応じて、あらかじめ決められた連絡窓口リストを使用して最新の報告資料を配布し、公に情報を流す前に、メディア連絡窓口に進行中の情勢に関する背景情報を提供します。さらに、このリストを使用して、予告（例えば、新サービスの提供のため）を送ったり、CSIRT が主催する予定のイベントや会議の詳細説明会にメディアを招待したりすることができます。

### 4.2.5 セキュリティポリシー

最近では、まともな組織であればどこも、ドアの鍵からバックアップ、パスワード、ファイアウォール、暗号化に至るあらゆるセキュリティ面に及ぶセキュリティポリシーを持っているか、持っていると主張しています。また、セキュリティポリシーの書き方に関するハンドブックも出ています[Wood 1998、RFC 2196]。

こうした取り組みを真似し損なう愚は避けて、ここでは、本書の読者に特に関係するセキュリティポリシーの側面のみを強調します。

第一に、CSIRTはネットワーク環境で運営するほかなく、そのため本質的に攻撃を受けやすい点を念頭に置く必要があります。これに、CSIRTが侵入者にとって非常に人気のある攻撃対象でもあるという事実を加えると、主要なリスク要素が見えてきます。すなわち、侵入の被害を受けているチームは、その事態を迅速且つプロフェッショナルな対応でコントロールしないと、活動する（対応する）ための機能を失うだけでなく、信用も失います。

CSIRTのシステムへの攻撃は、CSIRTが目立つ存在であり、多種多様な侵入者にとって人気の攻撃対象であるという事実が動機となっている可能性があります。未熟な侵入者はCSIRTを魅力的な攻撃対象と見なします。また、熟練した侵入者も、サービス運用妨害攻撃から基幹業務への侵入に至るまで、そしてこれ以外のさまざまな被害を経験した企業に関する情報を見つけられる可能性があるため、CSIRTに大いに興味を持っています。

セキュリティポリシーは他のポリシーに大きく影響されます。それは、ポリシーの目標とするものがセキュリティによって守られる必要があるためです。

例：情報のカテゴリ化ポリシーでは、セキュリティポリシーにも現れ、ファイルおよび文書の保護レベルを設定する変数が定義されます。これは、適切なテクノロジーと確立されたセキュリティ手順を使用して実装する必要があります。

セキュリティポリシーは、チームのコンピュータおよびネットワークに関するすべての面を扱い、他のネットワークへの接続も考慮に入れるべきです。

- 物理的なセキュリティ
- 復旧計画（バックアップなど）
- ローカルネットワークセキュリティ
- ローカル情報セキュリティ
- 外部通信セキュリティ
- ローカルセキュリティインシデントの対応
- 災害対応、事業継続性

#### 4.2.6 人的エラーポリシー

私たちは皆人間であり、誰でも間違いを犯します。CSIRTスタッフはこの特質から免れていると考えることができればすばらしいことです。しかし、CSIRTスタッフは、置かれているストレスに満ちた状況と、扱う情報の性質に伴う責任のために特に間違いが生じやすい立場にあります。

残念ながら、このような間違いが発生したときに、参照および使用できる人的エラーに関するポリシーは、無視されたり考慮されなかったりすることが少なくありません。人的エラーポリシーは、人的エラーが招いた損害を最小限に抑えたり防止したりするのに役立ちます。同時に、間違いを犯したスタッフとその上司である管理職の両方に、通常よく見られる非生産的な口論や不安ではなく、プロフェッショナルで建設的な方法で問題を解決する機会を提供します。人的エラーポリシーには、「好きなだけ愚かてください。私たちはいつでも優しくしてあげますよ。」と記すべきでは「ありません」。人的エラーポリシーは、良くない結果を引き起こす可能性のある間違いをスタッフが犯した場合に、そのスタッフが考慮すべき想定事態を明確に示す必要があります。また、管理職が示すべき適切な対応についても明確に記載し、帰結を概観する必要があります。

次のシナリオは、このような出来事に対処するための一般的なガイドラインと考えることができます。良くない結果を引き起こす可能性のある何かを行ったスタッフは、できるだけ早くしかるべき管理職に報告する必要があります。信頼できる「第三者」への緊急避難口を持つことが有益な場合もあります。間違いが認識できたら、管理職とスタッフはどちらも、当面の間は感情を脇において、状況の進展を食い止めるために「力を合わせて」取り組むべきです。明らかに、間違いを犯した人を参加させておくことが重要です（その行為がどう見ても悪意のあるものではない限り）。当面の問題に対処したら、スタッフと管理職（および信頼できる第三者）の間で、「次の」営業日のアポイントをとる必要があります。その話し合いの中で、同様の間違いが将来起こるのを防ぐために、間違いの原因を一緒に分析する必要があります。そのスタッフの悪習や間違った認識が原因の場合は、その習慣や認識を改めることに合意してもらわなければなりません。またその合意がきちんと守られているかを近い将来に確かめるためのチェックポイントを一緒に定義してもよいでしょう。原因によっては、スタッフをその立場に対応できるようにトレーニングしたり、または教育対策を施したりすることが最も有効な場合もあります。

次に、より具体的な例を示します。

例：暑い1週間の終わりの日のことです。プレッシャーも作業負荷も高い状態でした。あるスタッフが、誤って、サイトAに関する情報をサイトB宛ての電子メールメッセージに貼り付けてしまいました。このため、情報が不適切に開示されてしまいました。この過失は、直ちに上司およびサイトAとサイトBに伝えられました。どの当事者も理解ある人々です。その後、このような出来事が二度と起こらないようにするための方法が探られました（交替制の勤務時間の短縮、より使いやすいツール、補習研修、コーヒーの量を増やすなど）。

スタッフの間違いが日常的になりはじめたら、人的エラーポリシー以外の方法が必要です<sup>52</sup>。

---

<sup>52</sup> リスク管理には、このような状況に対処するための有名な原則があります。これには、「職務分離の原則」および知る必要がある人だけが特定情報にアクセスできるという

## 4.3 継続性の保証

信頼性のある一貫したサービスの継続は、CSIRTの活動が成功する上で不可欠です。これは、Constituencyが感じるチームの力量および信用レベルに直ちに影響します。継続性の保証は、活動の多くの重要な面に及ぶ運営全体の問題です。そのうちの3つ（ワークフロー管理、営業時間外の対応範囲、オフサイトの対応範囲）については、以降の節で取り上げます。これに着手する前に知っておくと役立つのは、継続性を保証する対象となる期間に応じて、遭遇する問題のタイプ、提供可能なサービス、（それらに応じて）講じる対策が大きく異なることを認識しておくとうりです。ここでは、3つの大まかな分類を使用します。そこで、実際のトピックを取り上げる前に、チームの活動の継続性を脅かす脅威について説明します。

### 4.3.1 継続性に対する脅威

継続性に関して各チームが直面する脅威を区別するために、実際の観点から3つの主要な分類に分けました。すなわち、数日から数週間に及ぶ短期の問題、数か月に及ぶ中期の問題、数年に及ぶ長期の問題の3つです。

#### 4.3.1.1 短期の問題

ここでは主に、数日から数週間以内の継続性に対する脅威を扱います。4つのトピック（時間不足、重要なスタッフの不在、勤務の交替、インフラ要素の利用不能）に分け、それぞれの課題を示します。これらは短期の問題における原因の大部分を占めています。

##### 時間不足

時間不足には偶発的なものと構造的なものがあります。構造的なもの（たいてい資金不足が原因）の場合は、本書の対象外であり、一般に短期の問題ではありません。偶発的な時間不足（例えば、広範な攻撃を伴う新しいインシデントによる予想外の作業負荷が原因で起こるもの）には、まず優先順位を付けて取り組みます。優先順位付けについては3.8.6節「優先順位付けの基準」で説明しました。これはインシデントハンドリングサービスにとっては、深刻な侵入問題に全神経を集中しているときは、2週間前のスニファーログは後回しにするということです。あらかじめ決められた優先順位付けの枠組みがなくても、優先順位付けは行うでしょう。しかし、枠組みがある場合よりも考えるために時間がかかり、一貫性も低くなると考えられます。極度の時間不足は、チームのサービスに悪影響を及ぼすため、危機管理の必要性につながることがあります。大量の仕事を抱えている場合は、起こっていることをメモしておくに役立ちます。次の交替勤務の同僚、あるいは夜間に仕事の一部を担う警備員やオペレータなどのチーム外部のスタッフに仕事を引き継ぐ時間になったとき、このメモが非常に重要な価値を持ちます。紙切れにメモをとるとするのはワークフロー管理の最も古い形態ですが、依然として役立つ方法です。ワークフロー管理については、以降の節で詳しく説明します。

---

「極秘の原則」が含まれます。詳細については、R. A. BothaおよびJ. H. P. Eloff、「Separation of duties for access control enforcement in workflow environments」、IBM Systems Journal Vol. 40, No. 3, 2001年、666～682ページなどを参照してください。

学校関係の CSIRT は、偶発的な時間不足に対して特に無防備です。この時間不足は、あまり厳密ではない略式のリソース計画が原因で起こります。さらに、作業負荷の対処に必要な時間は少なく見積もられており、チームが休憩したり未解決の仕事完了したりするのに十分な予備の時間帯も事前に割り当てられた仕事もありません。

### スタッフの不在

病気、事故、予想外の出来事は避けられないため、重要なスタッフの不在は、どのような時にも起こる可能性があります。そこで、単一障害点を作らないように、事前に代替要員の手配を行っておくべきです。チームメンバは互いに助け合うようにします（例えば、相互支援のために 2 人 1 組で仕事をするバディシステム）。重要なチームの全メンバに対しては、同じ日に休みをとることを認めるべきではありません。知識とそれに連動するリスクが分散されるように、通常業務のローテーションを考えることもできます。周りの要望に合わせるように教育することで、スタッフも全体像が把握でき、このような状況を回避するのに役立ちます。重要なスタッフの不在は、営業時間の直前および直後に起こることがあります。この時間、重要なチームメンバの大部分は、出社途中または帰宅途中の可能性があり、連絡をとることはできるかも知れませんが、具体的な行動を起こしてもらうのは難しい状況にあります。これは、チームメンバの勤務時間を「ずらす」ことで回避できます（例えば、あるスタッフは午前 7 時から午後 3 時まで働き、別のスタッフは午前 9 時から午後 5 時まで働くようにします）。スタッフは出張中であっても、ある作業にそのスタッフの特別な専門知識が必要なときは手伝えることがあります（手伝えないこともあります）。リモートサイトから会議などの重要な仕事を行わなければならないということは、部外者には「わくわくすること」のように見えるかも知れませんが、あまり楽しいものではありません。これは多くの問題を提起します。セキュリティへの影響はその 1 つに過ぎません。オフサイトの対応範囲は、別の一連の問題を提起するため、以降の節で取り上げます。スタッフの不在のもう 1 つの理由は、当然のことながら就業時間外のためです。このトピックについても以降の節で説明します。

### 勤務の交替

勤務の交替は、優れたワークフロー管理システムが利用できる場合であっても、特殊な問題をもたらします。状況に応じて、2 つの場合について考えなくてはなりません。1 つは営業時間中の普通の勤務交替であり、もう 1 つは営業時間中の勤務者と営業時間外の勤務者との交替です。前者の場合は、交替勤務者間で口頭で引き継ぎを行う時間を確保する必要があります。多くの場合、「直感」は不可欠ですが、データベースでそれを捕捉することは困難です。問題が解決せず、未解決の問題を引き継がなければならないこともあります。そのようなときには、さらなる説明が必要です。

例：一部のチームは、現在の作業を明確にするために勤務の交替時に毎日打ち合わせを行い（新規および継続しているインシデントの報告）、状況の最新情報（完了した作業、残されている作業など）を提供しています。

後者（営業時間外の勤務者との交替）の場合は、2 者間で対応範囲に違いがあるため、同じ問題についてより多くの側面がクローズアップされます。この違いに



はスタッフが含まれます（例えば、正規スタッフと、オペレータや警備員などの営業時間外取り次ぎサービススタッフ）。例えば、警備員はワークフロー管理システムにアクセスできないため、警備員による報告フォームを次の営業日に転送し、分析しなければならない場合もあります。さらに、このような警備員に CSIRT のスタッフと同じように電話に対応する技術スキルがあるとは考えられません。

#### インフラ要素の利用不能

重要な通信経路、および電子メールサーバや情報サーバ（WWW、匿名 FTP など）といった運用上の要素が利用できなければ、特定のサービスをタイミング良く提供できなくなります。その結果、CSIRT に対して苦情が寄せられたり、契約上の要件またはサービスが満たされないことに対する訴訟につながったりする可能性があります。場合によっては、CSIRT および Constituency の存続に深刻な影響が生じることもあります。

#### 4.3.1.2 中期の問題

中期的には、継続性の維持に役立つのは、人を集めて、起きていること、間違っていたこと、正しかったことを分析し、またこれらの情報に基づいてサービスをより良いものにする方法を分析することです。活動を見直すために、さまざまなインシデントの後で事後分析を行い、ポリシーと手順の両方を検討し、改善が必要な箇所（あるいは改善が必要かどうか）を明らかにする必要があります。これ以外にも定期的なブレインストーミングセッションや会議を計画すると良いでしょう。これにより、ポリシーや手順の不備が明らかになります。もう 1 つの中期の問題は、資金不足と、それがチームの活動、および Constituency に提供するサービスのレベルに与える影響です。また、特に多大な努力を必要とするインシデントハンドリングの現場では（そして、資金不足のときはいつも）、スタッフの燃え尽きも考慮すべき深刻なリスクです。労働条件が良ければ、各スタッフの負担が軽減します。CSIRT スタッフの健康と幸福のためには、「充電」や元気づけの効果がある休日や休暇をとるように勧めることがきわめて重要です。また、配置転換も有効です。これは燃え尽きにもつながる可能性のあるスタッフのマンネリ感の解消にも役立ちます。仕事がないためではなくインシデント対応業務の反復性のため、マンネリ感はインシデント対応において珍しいことではありません。職務を充実させたり継続的に教育を行ったりすることも、各スタッフのやる気を引き出すよい方法です。スタッフが新しい能力を開発し、チームのサービスの質を一層向上させるようになるため、これらはチームにとってメリットがあります。

#### 4.3.1.3 長期の問題

変化（例えば、技術またはサービス契約において）に適応する能力は、チームが長期にわたって存続するための能力に影響します。そのため、スタッフのトレーニングは、継続性に対する長期的な投資になります。同じ役割のためのトレーニングをより多くのチームメンバに実施すれば、単一障害点、動向の変化、チームメンバの退職または病気といった問題による影響が小さくなります。このトピックについては、4.5 節「スタッフの問題」で詳しく説明します。特にチームに長い間変化がない場合、時間と共に重要になってくる要素の 1 つは作業上の習慣です。ある種の習慣的手順になれば状況は安定しますが、これは継続性を保証する

ものではありません。安定は、チームが変化に適応する能力を制限してしまうおそれがあります。チームは、確立された手順をそのまま受け入れているがために無視してきたよくある間違いに対して脆弱である可能性があります。動的なインシデント対応環境に適応する能力を伸ばすために、チームもスタッフも継続的に学習をしていく必要があります。変化は日々の生活に組み込まれなければならないので、柔軟性が必要です。したがって、ポリシーと手順は業務に不可欠であり、一貫した行動がとれるようにきちんと整えておく必要がありますが、ポリシーと手順が継続して実行可能であり、チームが継続してそれらに従っていることを確認するために、また変更が必要ないかを判断するために、定期的に見直して検証しておく必要があります。

### 4.3.2 ワークフロー管理ツール

ワークフロー管理は文字どおりの意味です。仕事（ワーク。スタッフ自身の仕事、チームの仕事、会社の仕事）の一部である作業の流れ（フロー）を管理することです。ワークフロー管理は、洗練されたさまざまな方法によってあらゆるレベルで適用されます。家事であれば、通常は本人の意向と知恵だけを使ってワークフローを管理します。自動車会社の場合にはもう少し複雑なワークフロー管理が必要です。当然のことながら、今日のワークフロー管理手法の大部分は、ワークフロー管理が長年の課題となっている物流管理の分野から来ています。

インシデントハンドリングの継続性の問題は、CSIRT が長期にわたって多くの問題に対処しなければならないときに発生します。これは、状況が絶えず変わるため、そして（勤務者の交替、休日、配置転換、退職により）問題に取り組むチームメンバーも変わるためです。すべての問題、インシデント、関連課題について、全チームメンバーが、アーティファクトや脆弱性に関する情報といった関連情報を勤務時間中いつでも必要に応じて入手できるようになっているべきです。問題そのものに関する情報に加えて、チームが行ったその後の措置の追跡記録も入手できるようにするとともに、これからやるべきことも把握できるようにする必要があります。これにより、進行中のインシデントをチームメンバーに引き継ぐのが容易になります。

CSIRT に入ってくる情報の主な伝達手段（電子メール、ファイル、ファックス、電話のメモ、手紙）について考えてみましょう。この情報をすべてのスタッフがいつでも入手できるようにするのは容易ではありません。最初に行うことは、インシデントに番号を割り振り、そのインシデントに関するすべての情報に何らかのトラッキング番号または ID を付けることです。これについては、前の節で幅広く説明しました。それが済んだら、古典的な方法を選択することもできます。つまり、すべての書類（ファックスおよび手紙、可能なら電話のメモも）を見出しを付けて保管します。また、すべての電子ファイルは番号を付けて保存します（通常、電子メールとファイルは別々の場所に保存します）。さらに、参考のできる Web ページも存在するかも知れません。これにより、（1つのインシデントにつき）参考資料の保管先の数が4つにもなります。チームの中には、インシデントの追跡記録用に5つ目の保管先（ある種のデータベース）を使用するところもあります。

前述の古典的な方法により継続性は保証されますが、まったく効率的な方法ではありません。さらに、一刻を争う深刻な事態のときには裏目に出ることもあります。そのため、理想を言えば、究極の目標は保管先を「1つ」にすることです。少なくとも、目に見える保管先を1つにします。これをサポートするあらゆる仕組みは保管先を利用するチームメンバから隠されるべきです。

書類の排除はそれほど難しくありません。今日では、スキャニング技術はかなり高度化し、比較的費用もかかりません。これらのツールおよび技術を日々のインシデントハンドリング業務に組み込むのは賢い方法と言えます。ただし、大部分の情報は最初から電子的であるため、スキャニングは優先順位が高い作業ではないという点を認識しておいてください。文書を電子的な形式でのみ保持する場合、「元の」文書、または手紙を送った人の署名などにはたいてい法的な要件や権利があることを考慮に入れることが重要です。したがって、電子アーカイブに移されたハードコピーの資料はすべて、必要に応じて一定の期間、保持しなければなりません。

今日、電子メール、ファイル、Web へのアクセスを統合するための最も優れた方法は、おそらく Web ブラウザを使用した方法です。電子メールアーカイブは、たいていの場合 Web に変換できます (UNIX 環境では間違いなく可能です)。ブラウザからファイルにアクセスするのは簡単です。検索機能と索引付けも簡単に実装できます。この Web による解決策は、今のところ十中八九、チーム自らが開発し、カスタマイズする必要があります (【訳注: 現在ではこのような機能を実装した製品 (カスタマイズを含む) を導入して使用するケースも増えていきます】)。

ここで、さらに複雑なもの、すなわち適切にインシデントの履歴を保持する機能を追加する必要があります。前述の例では、インシデントが発生したときに単純に誰かがファイルやデータベースにメモを書き込み、Web やグループウェアシステムによってそのメモを利用可能にすることができます。しかし、これは、相変わらず作業そのものの「流れ」に対する実際の管理作業の大部分を勤務時間中のスタッフが行わなければならないことを意味します。このスタッフは、未解決のインシデントの定期的な確認 (社内で開発したツールやスクリプトの助けを借りた手作業である可能性が極めて高い)、情報の更新、記録への新しい情報やサイトなどの注釈付けといったあらゆるルーチンワークを行う必要があります。ルーチンワークは可能な限り機械に行わせるべきです。ワークフロー管理のための優れたソフトウェアはたくさん存在しているのです。

グループウェア (Lotus Notes など) のベンダは、この種の解決策を1つのソフトウェアパッケージとして提供しようと懸命に努力しています。このような開発は、CSIRT にとって大いに興味をそそられるものです。しかし、主として内部ネットワーク向けに開発されたワークフロー管理ソフトウェアの共通の問題点はセキュリティの不足です。このセキュリティの不足のため、ワークフロー管理ソフトウェアは一般に分散環境で使用するのは不適當です。そこで、チームは、分散作業が行えるようにインターネットを経由するセキュアトンネルを採用することがあります。Web ブラウザを使用し、セキュアトンネルを介してワークフロー管理ソ

ソフトウェア（および電子メールクライアントなどの他のツール）にアクセスすれば、簡潔な方法でセキュリティの問題を解決できます。

基本的に、ワークフロー管理ソフトウェアは、インテリジェントな方法で基盤データベースを使用し、そのデータベースで発生した変更を追跡します（あるいは、変更が「発生していない」ことを把握します）。

例：新しいインシデントが確認されました。このインシデントは、何らかの追跡 ID が割り当てられ、データベースに格納されます。以降、関連するすべての出来事がログ記録されます。どのインシデントにも「新規」から「完了」までのステータスフィールドがあります。ステータスが変わらなければ、アラームが発動する場合があります（これは単に中核となる機能です。インシデントのライフサイクル全体を通して、多くの可能性とその他の関連する活動が追跡され、記録されます）。

しかし、ほとんどの場合、このようなツールと Web またはグループウェアアーカイブとの統合が依然として欠如しています。これは深刻な問題です。全文検索エンジンは利用できますが、他の製品に追加して使用する必要があります。とはいえ、前途に光明も見えています。このようなツール用の Web ゲートウェイが登場しはじめており、いずれは Web ブラウザからワークフロー管理システムを利用できるようになるでしょう。また、グループウェアスイートには、ワークフロー管理機能が組み込まれはじめています。ただし、こちらは、CSIRT の見地からすればまだ成熟していません。

結論として、ワークフロー管理は、CSIRT の作業継続性の保証に対する支援を検討する上で重要であると言えます。問題の一部に対する実際的な解決策は数多く存在します。しかし、現在に至るまで、包括的な単一の解決策は存在しません。ツールの中にはすばらしいものもありますが、データベースとワークフローをローカルのニーズに適合させるためにカスタマイズやプログラミングが必要です。

### 4.3.3 時間外の対応範囲

サービスの仕様に営業時間外の対応範囲を含める場合は、営業時間外に想定されることと想定されないことについて概要をかなり明確に示す必要があります。それが明確になれば、営業時間外に利用できる必要がある機能と期待されるサービスレベルを明らかにできます。品質パラメータ（応答時間など）は、おそらく営業時間内と営業時間外とで異なるでしょう。（適切なポリシーおよび手順に加えて）明確な説明書や手引書がないと、Constituency はちょっとした問題でも助けを求めてくる可能性があります。そして、各機能は、継続性の観点から分析する必要があります。昼間、オフィスでささいな影響しかなかったものが、夜、自宅で大きな問題になるかも知れません。発生する問題はどれも取り除く必要があります。

以下に、営業時間外の代表的な問題の例を示します。オフサイトの対応範囲については次の節で取り上げます。

#### 4.3.3.1 ホットラインの対応範囲

ホットラインの対応範囲についてはさまざまな選択肢があります<sup>53</sup>。最も重要な点は、営業時間外に誰がホットラインの電話に対応するか定義することです。すなわち、勤務時間中のチームのスタッフか、別のスタッフか、あるいはボイスメール、警備員、通信プロバイダのコールセンタなどの取り次ぎサービスかということ。

それが決まったら、実際に電話対応する人に電話を取り次ぐ際の方法を決めます。考えられる方法はいくつかあります。直接チームメンバが電話に対応する場合は、電話中継メカニズムを使用して実装します。また、営業時間外電話用のホットライン番号（別の連絡窓口番号）を **Constituency** に伝えることもできます。もう1つ大事なものは、交替勤務のスタッフが勤務時間中に物理的にオフィスにいるようにすることです。

他のスタッフや外部の関係者を介してホットラインの電話を取り次ぐ場合は、各チームメンバの自宅の電話番号のリストを用意することができます。あるいは、スタッフを呼び出すためのホットライン番号（電話またはポケベル）を提供することもできます。

選択によって異なりますが、考慮すべき品質パラメータ（応答時間など）の制約があります。また、自宅に設備を用意することと、電話に対処するためにオフィスに行く時間との比較などの問題も考慮する必要があります。

#### 4.3.3.2 エスカレーション

日中に問題が発生した場合、エスカレーションはたいてい、他のチームメンバに助けを求めるという簡単な方法で行えます。しかし、営業時間外ではどうでしょうか？ この点を考える必要があります。知らせを受けてからすぐに応援要員として対応できるように別のチームメンバを少なくとも1人待機させておくのもよい方法でしょう。また、危機的状況下で誰が対応可能か探してその人に応援を要請することもできます。危機的状況はチームの活動に影響するため、混乱を解決する「当直管理職」というポジションが適切かも知れません。

#### 4.3.3.3 他のチームまたは顧客との連絡方法

営業時間外の対応を請け負っているのは自分のチームだけではありません。営業時間外の対応の可否に基づいて他のチーム、顧客、それ以外の人たちとの既存の実務上の関係性を評価し、これらの関係性を足がかりにします。この場合、通常は明らかにしない緊急連絡番号を快く教えてくれる可能性があります。また、時差の問題に注意してください。その場所では営業時間外でも別の場所では営業時間内の場合があり、その逆の場合もあります。祝祭日は世界中で異なります。また公休日は1つの国の中でも異なる場合があります。

---

<sup>53</sup> ヘルプデスク、カスタマサービス、コールデスクなどと呼ばれることもあります。

例：時差の問題は利点にもなります。アメリカ、ヨーロッパ、オーストラリアのチームが、多くの時間帯が含まれる地理的な隔たりを利用して問題に対する継続的な作業（インシデントや脆弱性の分析および解決など）を可能にしたという事例が報告されています。あるチームの営業日が終わると、その問題は営業日が始まったばかりの別のチームに引き継がれます。

例：独立記念日（アメリカがイギリスから独立したことを祝う日）は、アメリカで伝統的に毎年7月4日に祝われます。この祝日が週末（土曜日または日曜日）の場合、アメリカの一部の企業は、前日の金曜日から翌日の月曜日を休日にする場合があります。明らかに、この休日は世界の他の国では休みではありません。

例：アメリカの復員軍人の日は、伝統的にアメリカ政府（地方、州、連邦）と軍事機関のみが祝います。アメリカの銀行、それ以外の企業、組織は、この日を祝うところもあればそうでないところもあります。

#### 4.3.4 オフサイトの対応範囲

オフサイトの対応範囲は、通常サービスを遠隔地から提供する必要があるという点で、営業時間外の対応範囲とは異なります。一般に、勤務時間中のスタッフがオフサイト（会議場、Constituencyの所在地、場合によっては予備施設の場合も）にいる状態で営業時間のサービスを続けるには、正当な理由（災害やそれ以外の危機的状況など）が必要です。これは、営業時間外の対応範囲とほとんど同じかそれ以上の問題を招きます。なぜなら、期待されるサービスレベルは、営業時間に通常の活動場所から提供するサービスのレベルと同じだからです。

Constituencyは、スタッフの特殊な状況を認識できる必要はありません（できれば、認識されるべきではありません）。重要なのは問題に対処することであって、サービスを提供するために必要な措置を講じる手段についてConstituencyに不安を抱かせることではありません。言うまでもなく、簡単なことではないため、オフサイトの対応範囲は最小限に抑えるべきです。

勤務時間中のスタッフが作業する場所（例えば、営業時間外は自宅、会議の開催地ではホテルの部屋）は、必ずしも前もって分かっているわけではありません。これにより、一般にきわめて短時間で評価しなければならないセキュリティ上の余計な問題が生じます。状況に応じて、特定のサービスの提供に必要なセキュリティのレベルを下げるか、あるいは、セキュリティのレベルは高いままにし、必要なセキュリティ対策がないという理由で内部CSIRTネットワークへのアクセスを防止するか、どちらかに決めなくてはなりません。このような場合、様々な検討項目の中でチームのセキュリティを最も重要なポイントとして考慮しなければなりません。

関係するチームメンバにはオフサイトにいることに、本来であれば正当な理由があるのは明らかです。彼らには、オフサイトで行うように求められているインシデントハンドリング作業に加えて他の仕事もあります（例えば、会議や顧客との打ち合わせでのプレゼンテーション）。仕事の優先順位は、前もって決めておく必要があります。この優先順位により、優先する仕事、仕事を放置できる時間

(翌日まで、オフィスに戻るまで、または他のスタッフが対応できるようになるまで)が決まります。

## 4.4 セキュリティ管理

CSIRT が自らのセキュリティ保護に特に重きを置く必要があるのは明らかです。しかし、本書では、関連するすべての側面は取り上げません。

とはいえ、この節で説明する CSIRT の個々の問題には補足説明が必要です。CSIRT セキュリティ管理の目標を検討する際は、(大部分の組織では一般的な)次の要素を考慮に入れる必要があります。

- 機密性：許可されたものだけを取得できること
- 可用性：必要なときに必要なものを取得できること
- 完全性：情報が意図された状態のままであるようにすること
- 真正性：情報の発信元が確実に分かること
- 排他性：意図された受信者だけが情報を利用できるようにすること
- プライバシー：人および組織の利益が守られることを保証すること
- 義務：善管注意義務の要件が満たされることを保証すること

### 4.4.1.1 暗号化およびデジタル署名アプリケーションの使用

どのCSIRTにとっても、暗号化およびデジタル署名アプリケーションの使用は避けられません。このアプリケーションにより、チームのコンピュータシステムのデータ保護、そして安全ではないネットワークを介したデータ転送におけるデータ保護に対して優れた可能性をもたらします。また、暗号化によって真正性が保証され、(特に外部から)チームの内部ネットワークへの接続を保護できます(考慮すべき事項については下記を参照)。チームと協力者との間は、S/MIME およびPGPまたはGPG<sup>54</sup>などの一般的な暗号化ツールによって、機密データ(インシデントの分析、新しいアーティファクト、最近の傾向に関する定期的なサマリなど)の安全な受け渡しを実現できます。侵入に関するログファイルは、被害者および関係するシステムにかかわる機密情報を非公開に保つために、暗号化して、電子メールでConstituencyとの間で送受信できます。内部の暗号化に関しては、独自の規格を選択できます。優れた可能性がいくつか存在しますが、本書ではこれ以上取り上げません。外の世界に対応する場合は、PGPやGPGなどの(事実上の)標準を選択する必要があります。S/MIMEは、ますます普及しており、Microsoft、Netscape、その他のユーザコミュニティによる対応状況から判断して

---

<sup>54</sup> GPG (GnuPG) は、IETFで整備されたOpenPGP規格に対応したPGPのオープンソース実装です。GPGは新しいPGPリリースと互換性がありますが、PGP 2.6.xバージョンには対応していません。【訳注：PGP 2.6.xバージョンについては追加モジュールで対応可能です。】

事実上の標準となる可能性があります。機密性に加えて真正性も保てますが、結果として他の問題が生じます（下記の鍵管理と認証の問題を参照）。

S/MIME や PGP/GPG などの便利なプログラムが既に何年も前から利用できます。このようなプログラムを使用することで、ユーザはプログラムや技術の難題に直面することも多々ありますが（電子メールクライアントへの統合など）、強力な手段を手に入れることができます。S/MIME は現在、一般的な商用電子メールクライアント（Netscape、Microsoft）、およびオープンソースソフトウェア（Mozilla）に統合されています。PGP バージョン 6.x/7.x、および GPG など OpenPGP のその他の実装では、一層の使いやすさ、グラフィカルユーザインタフェース、電子メールクライアントとのより優れた統合が実現されています。

#### 4.4.1.2 鍵管理と認証

暗号の使用にあたっては、鍵管理と認証の問題が生じます。S/MIME および PGP/GPG では、強力な認証を実現するために非対称暗号方式（公開鍵暗号方式とも呼ばれます）が使用されます。これにより、対称鍵（単一鍵または秘密鍵とも呼ばれます）暗号方式の弱点が回避されます。秘密鍵の場合は、すべての通信相手はその鍵を知っている必要があります。このため発信元と宛先の真正性を実現することは不可能でした（鍵が「共有」されるため）。しかし、非対称暗号方式では、人／役割ごとに、相互に関係する 2 つの鍵が使用されます。公開鍵は、真正性を損なうことなく誰にでも配布できますが、秘密鍵は、パスワードと同じように保護する必要があります。

例：非対称暗号方式では、Moira が Don に暗号化された電子メールを送りたい場合、Moira は Don の「公開鍵」を使用してテキストを保護し、そのテキストを Don に送信します。その時、Don だけが唯一自分の「秘密鍵」を使用してそのテキストを復号できます。さらに、Moira は、自分の「秘密鍵」を使用して、送信するテキストに署名します。Don は、Moira の「公開鍵」を使用して発信元を確認できます。

鍵管理の問題は、公開鍵と秘密鍵の両方に関係します。秘密鍵は安全に保存する必要があります。秘密鍵が誰かに制御されると、あなたが復号できるすべてのものがその誰かによって復号されてしまうことになります。秘密鍵のロック解除は、パスフレーズと呼ばれる一種のパスワードを使用して行います。このパスフレーズは、セキュリティを確保するためにしっかりと保護する必要があります。フロッピーや USB トークンのようなリムーバブルメディアで秘密鍵を持ち歩く人もいますが、そのような方法ではセキュリティについて疑問を持たれると思われまます。特にフロッピー自体が通常秘密鍵の管理方法と同様にきちんと保護されていなければ、なおのことです。

適切な知識を持ち合わせていないまま強力な暗号を使用しても、まったく暗号にはならないことに注意してください。秘密鍵のロック解除に 3 文字のパスフレーズを使用したり、完全に切り離されたシステムでロック解除を行わなかったりすると、セキュリティの連鎖が断ち切られてしまいます。したがって、「強力な」プログラムを利用できることだけが重要なわけではありません。「正しい」方法で



使用する必要もあるのです。同様の問題は、コンピュータのディスク上またはプログラム／スクリプト内に秘密鍵のロックを解除するパスワードまたはパスワードを保持する場合にも関係します。

公開鍵の1つの問題は、取得した公開鍵が本物で、その鍵が帰属している人に本当に属しているかどうかチェックする必要があるという点です。現在、S/MIME またはPGP/GPGのための認証局が非常に一般的になり、必要になっているのは、このような理由からです。Verisignなどの信頼における第三者機関（TTP）では、ユーザに鍵ペア（公開鍵と秘密鍵）を販売しています（ユーザは、TTPがこのような鍵を発行する前に身元を確認するための適切なチェックを行っていると感じる必要があります）。ユーザの見地からすれば、自分がその秘密鍵を利用できる唯一の人間であるということが絶対に必要です。TTPから鍵を購入すると、TTPはその鍵に署名します。その結果、その鍵が一層信頼できるものになります。しかし、TTPに頼るときには注意が必要です。なぜなら、TTPは、自分たちのユーザおよび顧客にのみ関連する独自のポリシーを適用しているからです。現在、これらのシステムはいずれも、世界中のネットワークユーザが個人用IDシステムを（例えばパスポートの目視検査など<sup>55</sup>と）確実に比較できるようなデジタル識別情報を提供することはしていません。

ユーザが互いの鍵に署名する、または互いの鍵を承認することができる場合、同じ問題が生じます。すなわち、鍵の真正性のチェック方法です。フィンガープリントを検証するため利用できる、本人とフィンガープリントとの間の直接の関係が存在しない場合、ユーザは「信頼の輪（Web of Trust）」に頼る必要があります。これは、別のユーザが、鍵とその利用者との結び付きを確認したことを証明することを意味します。

例：MoiraはDonの公開鍵に署名しています。Moiraの同僚のAnnは、Donを知りませんが、Donに暗号化された電子メールを送りたいと思っています。AnnはDonの公開鍵を取得し、その公開鍵にあるMoiraの署名を見ました。Annは、（以前のとある機会に）Moiraの公開鍵が本当に「Moiraの鍵」であることを確認したことがあるため（AnnとMoiraが個人的に会って鍵のフィンガープリントを交換した後で）、Donの鍵にあるMoiraのフィンガープリント／署名を比較できます。そして、Annは、Donに直接会って確認することなくDonの鍵も信用します。これが、小さなユーザコミュニティ内での信頼関係を築き、広げていくという、PGPのユーザ認証の信頼の輪の考え方です。別の言い方をすると、自分が知っていて信頼している誰かが、直接は知らない誰かへとつながる鍵を検証するために正しいことをしている、ということです。

CSIRTは（チーム鍵、またはそれぞれのチームメンバの鍵を使用して）どのような場合に鍵に署名すべきか、またいつ署名すべきかという問題を解決する必要があります。言うまでもなく、後で信頼できないと分かった相手の鍵にCSIRTが署名をしてしまった場合、CSIRT自体が悪影響を受けます。厳密にはこれは正し

---

<sup>55</sup> とはいえ、狡猾な犯罪者たちは過去において確かにパスポートを偽造しており、言うまでもなく、このような比較も100%確実なものではありません。

くありませんが、CSIRTは可能な限り問題を避けるために、チーム鍵ではどの鍵にも署名しないことも選択できます。

例：CERT/CCでは、CERT/CCチームのPGP鍵では、外部のどの鍵にも署名しないことを選択しています。

例：CERT-NLでは、「非常に信頼できる」人たちに署名する場合にのみマスター認証鍵を使用しています。CERT-NLメンバが個人用の鍵を使用して署名できる対象についてのポリシーはあまり制限的ではありません。

#### 4.4.1.3 ファイアウォールとネットワークセキュリティ

チームのネットワークは、優れた設計のファイアウォールによって外界から切り離されているのが理想です。外の世界には、「チームの上位組織も含まれます」[Chapman 1995]。ファイアウォールは究極の解決策ではなく、ネットワーク全体に渡って適切な認証と承認によって補強する必要があります。攻撃、およびセキュリティ侵害の可能性を認識できるように、十分な管理と制御を徹底させなくてはなりません。ファイアウォールは、例えば、疑わしい活動がないかログファイルを定期的に（少なくとも毎日）検査しない限り、役に立ちません。Swatch<sup>56</sup>やlogsurfer<sup>57</sup>などのツールを使用すれば、疑わしいログファイルエントリをオンラインで認識することができ、分析とデータの削減に役立ちます。

ローカルネットワーク構築の際には冗長性の問題を考慮します。ファイアウォールおよび関連ホストだけでなく、サーバ（シャドーファイルサーバ、シャドーディスク、余ったワークステーション、ホットスペア）も重要な構成要素です。電源断に備えて、予備電源を用意しておく必要もあります<sup>58</sup>。

火事などの災害のことを考えて、忘れずに予備のバックアップテープを別の場所に保管しておきます。ただし、その別の場所の安全性は手元よりも低いことがあります。その場合は、バックアップを暗号化することをお勧めします。暗号化は、ファイルサーバなどの特定のサービスを提供する場合の選択肢としても考えられます。ローカルネットワークでは、Kerberosなどの暗号方式や、Kerberosに基づいた何か（AFSなど）の使用を検討してください。あるいは、少なくとも機密データにはファイルの暗号化を使用してください。これにより、ファイアウォールが個々の攻撃をブロックできない場合の、予備の保護手段となります。

#### 4.4.1.4 テスト用の切り離されたネットワーク

どのテストベッドも（例えば、ウィルス、アーティファクト、不明な動作をするプログラムに対するもの）、CSIRTの運用または実稼働ネットワークから切り離されている必要があります。切り離すことで、あらゆるテスト、悪意のコードの分析、汚染、サービス運用妨害など、チームの機能を遂行する能力に影響し、且つチームに対する世間の評価を落としかねないイベントによって、ミッションク

---

<sup>56</sup> <http://swatch.sourceforge.net/>

<sup>57</sup> <ftp://ftp.cert.dfn.de/pub/tools/audit/logsurfer>

<sup>58</sup> 無停電電源装置（UPS）

リティカルなコンピュータ、通信、ネットワークシステムの可用性と完全性が影響を受けることがないことを保証できます。これは、例えば、ウィルスの流出または攻撃がインターネットの他のシステムを巻き込む場合に特に言えることです。

例：1998年、INNDニュースデーモンソフトウェアの欠陥が原因で、CSIRTがテスト目的で作成したUSENETニュースの「制御メッセージ」が意図せず流され、世界中の脆弱なニュースサーバから何千もの/etc/passwdファイルが送信されました。これはCSIRTにとって非常に恥ずかしい出来事であり、テストを実施したチームの担当者が、切り離されたテストベッドを使用するか、テストベッドが適切に保護されていたら防げたでしょう<sup>59</sup>。

#### 4.4.1.5 ローカル設備へのサイト外からのアクセス

モバイルコンピュータを使用して自宅や出張先で作業する場合は、電子メールやワークフロー管理ツールがあるローカルシステムに安全にアクセスする上で特別な注意を払う必要があります。ファイアウォールは、この種のアクセスが可能になるように穴を開けるべきではありません。セキュリティと外部からのアクセスという、この矛盾について考えると、本質的に2つの実行可能な解決策にすぐに到達します。1つは、ネットワークへのダイヤルアップ接続です。これ自体は、特にアクセス手順で強力な認証（ワンタイムパスワードカードやチャレンジレスポンスカードなど）が使用されている場合には比較的安全です。もう1つは、あらかじめ決められた番号へのダイヤルバックを使用することです。その場合も、強力な認証機能は不可欠です。しかし、盗聴は依然として可能です。これも、暗号化装置や盗聴防止機能付き電話／機器を使用することで保護できます（例えばアメリカでは、aSTU IIIやSTEなどの装置を使用します）。モバイル（ノート型）コンピュータと、そのコンピュータまたは付随メディアに格納されているデータの紛失や盗難に対する物理的防護も、考えるべきセキュリティ問題です。

2つ目の解決策は、公衆網（たいていはインターネット）を使用する方法です。これを行う唯一の正しい方法は、エンドツーエンドの暗号化を行うために、強力な認証および暗号化機能に基づいてトンネル、すなわちVPN（virtual private network：仮想私設網）を構築することです。最も簡潔な解決策はアプリケーションレベルの暗号化ですが、たいていの場合、実現不可能か不十分です。

---

<sup>59</sup> このテストによるその後の問題のもう1点は、この対処すべきパスワードファイルがすべてCSIRTにあるということです。CSIRTがすべきことは何でしょうか？サイトに連絡して、テストスクリプトに問題が発生したことと、サイトのINNDソフトウェアが脆弱だったことを伝えればよいでしょうか？パスワードファイルをサイトに返すべきでしょうか？返す必要がある場合、恐らくCSIRTは、最初にそのファイルを（パスワードフィールドの中身を削除するために）サニタイズして送るということになるでしょう。したがって、次は、すべてのファイルに対するこの大量のサニタイズを行う方法、およびこのファイルを適切な連絡窓口を送る方法が問題になります。このこと自体も問題を招きます。チームには（正しい）連絡窓口情報があるのでしょうか？連絡窓口情報を調べるのにどのような労力が必要でしょうか？そもそもチームはこの作業も引き受けるべきなのではないでしょうか？サイトはConstituency内部でしょうか、それとも外部でしょうか？外部サイトに対するフォローアップは、チームのミッションおよび目的に含まれているのでしょうか？以上のように、この状況では対処しなければならない問題がたくさんあるのです。

別の方法として、ネットワークレベルでノートPC（またはその他の機器）からチームのネットワークへトンネルを構築することもできます。SSH（Secure Shell）のような製品はこのために作られました。しかし、これらのツールはどれもきわめて慎重且つ周到に導入する必要があります。さもなければ、角を矯めて牛を殺すことになりかねないことが経験から分かっています。多くのツールは比較的新しいため、十分なテストおよび保護が確実に行われる必要があります。また新しいツールの中には、ソフトウェア脆弱性が含まれている可能性もあります<sup>60</sup>。

しかし、自宅のシステム／ノートブックとチームのネットワークとの通信リンクを守るだけでは十分ではありません。なぜなら、関係するシステムのセキュリティによって、ネットワークに直接（チームのネットワークへのコンピュータウィルスの「漏えい」）、または間接的に（自宅のシステムからの機密データの無断コピー）影響を及ぼす可能性もあるからです。したがって、そのようなシステムにも多くのセキュリティ上考慮すべき事項を適用する必要があります。リモートアクセスの必要性を最小限に抑えたり、特に機密性の高い分類の対応はリモートアクセスに対して許可しないようにしたりする方が簡単かも知れません。

#### 4.4.1.6 物理的セキュリティ

CSIRTは、物理的セキュリティそのもののすべての側面を実践するのに必要な権限を完全に有しているとは限らない場合があります。物理的セキュリティは、多くの場合、上位組織によって提供されます。これを、できればCSIRTの要件に合うように強化する必要があります。物理的な侵入は、ネットワークを介した侵入と少なくとも同じくらい有害なことがあります。鍵の管理、机の整理整頓ポリシー、スタッフの承認、来訪者に関わる手配を考慮に入れる必要があります。さらに、文書の取り扱い（ロッカー、金庫、ごみの廃棄、シュレグダでの裁断）についても検討します。FAXとプリンタの物理的な位置、および「安全な」環境内部のホットラインの場所も忘れずに考慮してください。電話の会話は、他人（来訪者など）に聞かれる可能性がないようにしておく必要があります。

盗聴の可能性を考え、建物内の配線方法やハブの場所などに注意を払う必要があります。他のすべての公衆通信装置、特に、盗聴されやすいモバイル通信装置を疑ってください（これは物理的セキュリティ特有の問題ではありませんが）。疑わしい接続には暗号化の使用を検討します。暗号化は、物理的セキュリティが100パーセント保証されない場合にファイルシステムとバックアップメディアを保護するためにも利用でき、これによって一層高いセキュリティが実現します。技術的な方法によるものの他に、情報の「漏えい」が起こる可能性もあります。来訪者は、例えば、世間話の成り行きで、あるいは、インシデント関連の情報が語られているときにその部屋にいることによって、（こっそりとまたは公然と）情報を得ようとする場合があります。

---

<sup>60</sup> 例えば、次のCERT Advisoryを参照してください：「Trojan Horse OpenSSH Distribution」 (<http://www.cert.org/advisories/CA-2002-24.html>)、「Multiple Vulnerabilities in SSH Implementations」 (<http://www.cert.org/advisories/CA-2002-36.html>)。

建物の管理職員や清掃員、電力会社の従業員、他に設備に近づく可能性のある人を考慮に入れてください。このような人たちは、態度が控えめで、たいてい表に現れないため、見落とされることが少なくありません。しかし、セキュリティ設計を完全に台無しにすることも可能なのです。物理的セキュリティ計画では、そうした人たちのことも考慮するようにしてください。

例：CSIRT スタッフがいない場合、あるいは、清掃スタッフに警備員が付き添っていない場合、清掃スタッフは CERT/CC のオフィスに入れません。

#### 4.4.1.7 災害対応

極めて破壊的なネットワーク侵入、破壊行為、火事、天災といった災害に備えて、優先順位付け方法とエスカレーション手順、例えば最初にすべきこと（および無視すべきこと）や警告すべき相手などをきちんと整理しておく必要があります<sup>61</sup>。「災害モード」に入るタイミング（そして、通常業務に戻るタイミング）の定義も必要です。災害モードになると、普段は関係のない人たちがオフィスに出入りする傾向があります。その場合も、やはりセキュリティは重要です。このような災害から生じるリスクも適切に考慮する必要があります。

火事が激しいと、消防士は、厳重に保護されたコントロールルームやコンピュータルームの内部も含め、至る所に行くことになるでしょう。コンソールはロックされているでしょうか？ どのような機密文書が置かれているでしょうか？ プリンタは何を印刷しているでしょうか？ このような状況で最も厳しいセキュリティを課するのは事実上不可能です。しかし、災害対応の一環として、災害が起こったときにこのようなセキュリティ問題に当たる人を決めておいてください（言うまでもなく、危険にさらされない範囲での対応です）。これには、印刷書類や電子媒体などの機密情報および重要情報の収集を含める必要があります。また、CSIRT のプロセスと手順の見直しおよび評価のために事後分析を行い、うまくいったところと改善が必要なところを明らかにすることも有用です。

Constituency が CSIRT の活動に依存している場合は、危機や災害のときにバックアップが提供されるように予防措置を講じます。危機的状況が過ぎたら、迅速な復旧が可能なように対策を施す必要があります。

#### 4.4.1.8 内部セキュリティインシデントの対応

組織というものは、内部インシデントについては口をつぐみたがるものです。セキュリティポリシーに何も明示されて（書かれて）いなければ、その問題について語られることはないでしょう。「何も言わないこと」は自然な反応だからです。しかし多くの場合、これは間違った反応です。内部攻撃の可能性を除けば、インシデントは CSIRT のネットワーク外部のシステムと何らかのかかわりがあります。このため、外部の人間がインシデントに気付き、その情報を公表する可能性があります。間違いなく、犯人は攻撃を知ると、（自分の主張を裏付ける証拠を

---

<sup>61</sup> 本書では、（親組織の意味での）災害復旧作業および事業継続作業については取り上げませんが、CSIRTは、これらの役割（例えば、災害復旧計画や業務継続計画）を担当する組織内グループとの関係を前もって確立しておく必要があります。

示して) 侵入者として自分の行為を自慢し、公にするでしょう。内部で誰も報告しなくても、インシデントは世間に知れ渡ります。これは、人的エラーポリシー(4.2.6節を参照)とそれを支える手順をきちんと整えておくことの背景にある論理的根拠を示す良い例です。このような状況なら、各スタッフはインシデントを報告できます(報告する気になります)。CSIRTは、「人に説くことを自分でも実践する」必要があります。CSIRTに対する内部攻撃を無視することはできません。CSIRTの内部でインシデントが発生した場合、そのインシデントは、他(組織)の内部インシデントと同じように報告しなければなりません。CSIRTは、このようなインシデントに備え、対処する必要があります。これは、封じ込めという明白な理由のためだけではありません。CSIRTがインシデントを隠そうとし、その後、誰かがそのインシデントを公表した場合、チームの評判が取り返しのつかないほど傷付く可能性もあるからです。

このことは、セキュリティインシデント対応を事業として行っている組織にも当てはまります。問題を認めた場合、「あなた方のセキュリティはどうして不十分なのか」と問いただされることでしょう。そして、何が起こったのか説明しなければなりません。問題を隠し、その問題が漏れた場合、事業から撤退せざるを得ないこともあります。(何も言わなかったこととセキュリティのなさのために)もはや誰からも信用されません。また、自分たちのシステムすら守れなかったのですから、専門知識ももう信用されることはないでしょう。

優先順位が高い他の問題を無視するほどではないにせよ、明らかに、内部インシデントには高い優先順位を割り当てなければなりません。ここでは、注意深くバランスをとる必要があります。

## 4.5 スタッフの問題

文書化された適切なポリシーと手順の規定に関係なく、CSIRTの仕事は原則としてサービスを基本としています。結果として、チームのポリシーと手順を効果的に実行できるように、また、Constituencyに対応するときに外交能力を発揮できるように、有能且つ信頼できるスタッフに依存せざるをえません。このためCSIRTのスタッフは、運営のミッションとサービスの保証において極めて重要な役割を果たします。この節では、CSIRTに相応しいスタッフの選考、採用、トレーニング、維持に関する問題について説明します。また、着任と離任の手続き、スタッフの補充についても説明します。さらに、中心的な役割を果たすCSIRTスタッフが起り得る状況に対処する上で人数または技術スキルの点で十分でない場合に検討する代案についても取り上げます。

### 4.5.1 CSIRT スタッフ

多くの人は、CSIRTスタッフの最も重要な特質は技術的な経験であると誤解しています。技術的な経験は望ましい特質ですが、より重要な条件は、手順に従い、Constituency、顧客、その他CSIRTとやり取りする関係者とプロフェッショナルなインタフェースをとることができる意欲と能力です。技術的な経験が乏しくても優れた対人スキルとコミュニケーションスキルのある人を採用し、その人に

CSIRT 特有の技術スキルを身に付けさせる方が、その逆の場合より望ましい方法だと言えます。間違いなく、本書自体が、他のチームとやり取りし、適切なサービスを提供するために、すべてのスタッフに必要な認識を教育し強化する良い出発点となります。

チームメンバは、互いに、またはConstituencyや他の関係者（他の対応チームなど）と絶えず対話しているため、広範な対人スキルを持つことが重要です。チームの評判は、チームメンバが行うプロフェッショナルな対応にかかっています。技術的な専門家であってもコミュニケーションスキルが欠けているチームメンバの対応は、コミュニティにおけるチームの評判と立場を著しく傷付ける可能性があります。これに対して、プロフェッショナルで有能な印象を与える対応は、価値のあるサービスプロバイダとしてのCSIRTの評判を高めるのに役立ちます。したがって、個人の対人スキルに注意を払うことがきわめて重要になります<sup>62</sup>。

インシデントハンドリングスタッフにとって重要な対人スキルは次のとおりです（順不同）。

- 明確な指示や決まりがなくても、また、ストレスや厳しい時間的制約の下でも、受け入れ可能且つ効果的な判断が下せる常識。
- Constituency や他のチームと対話するために必要な、口頭および文書による効果的なコミュニケーションスキル（母国語および英語）
- 他のグループ（特にメディアや Constituency）に対応する際の外交能力
- ポリシーと手順に従う能力
- 勉強を続ける意欲
- ストレスに対処し、プレッシャーのある状況で仕事を遂行する能力
- チームプレーヤ
- チームの評判と立場を守る誠実さと信頼性
- あるトピックに関する自分自身の間違いや知識の限界を認めることをいとわない気持ち
- 新しい状況に対応し、効率的にインシデントに対処するための問題解決
- 優先する作業に集中するための時間管理

技術的な見地からすれば、各インシデントハンドリング担当者には、個人の専門知識のよりどころとなる基礎技術と問題点に関する基本的な理解が必要です。これらのスキルの性質は、チームや Constituency が使用している基本的なソフトウェアおよびハードウェア技術に関係なくほぼ同じです。

---

<sup>62</sup> Katherine T. Fithen、『Hiring IRT Staff Interview Process』、Forum of Incident Response and Security Teams、8<sup>th</sup> Workshop on Computer Security Incident Handling、カリフォルニア州サンノゼ、1996年6月。

インシデントハンドリングスタッフにとって重要な基礎技術は次のとおりです（括弧内に一般的な例を示します）。

- 公衆データ網（電話、ISDN、X.25、PBX、ATM、フレームリレー）
- インターネット（アーキテクチャおよび歴史から、将来像および理念に渡る側面）
- ネットワークプロトコル（IP、ICMP、TCP、UDP）
- ネットワークインフラ要素（ルータ、DNS、メールサーバ）
- ネットワークアプリケーション、サービス、および関連プロトコル（SMTP、HTTP、HTTPS、FTP、TELNET、SSH、IMAP、POP3）
- セキュリティの基本原則
- コンピュータおよびネットワークに対するリスクと脅威
- セキュリティの脆弱性／弱点および関連する攻撃（IP スプーフィング、インターネットスニファ、サービス運用妨害攻撃、コンピュータウイルス）
- ネットワークセキュリティ問題（ファイアウォール、仮想プライベートネットワーク）
- 暗号化技術（TripleDES、AES、IDEA）、デジタル署名（RSA、DSA、DH）、暗号化ハッシュアルゴリズム（MD5、SHA-1）
- ユーザとシステム管理両方の観点から見たホストシステムのセキュリティ問題（バックアップ、パッチ）

チームおよび Constituency が使用している技術と問題点をすべて深く理解しているスタッフがチームの中にいなくてはなりません。この一段高いレベルの専門知識は、チームの技術的な資源と能力を拡大し、且つ深め、トレーニングおよび文書を通して他のチームメンバを教育するのに使用される資源となります。また、これによりチームは Constituency の技術基盤の一部をカバーしたり、幅広いサービスを提供したりできるようになります。前述の各技術スキルを深く理解しているだけでなく、さらに考慮すべき専門スキルを次に示します。

- プログラミング、ネットワークコンポーネント（ルータ、スイッチなど）およびコンピュータシステム（UNIX、Linux、Windows など）の管理といった技術スキル
- 人とのコミュニケーション、会議でのプレゼンテーションの経験、グループの管理といった対人スキル
- 作業編成スキル

チームは、何らかの理由で適切と思われる必要な専門スキルを持つスタッフに必要な資金を用意したり、そのようなスタッフを探し出したり採用したりすることができない場合があります。4.5.6節「スタッフの補充」では、このような状況に対処するための可能性について説明します。4.5.4節「スタッフのトレーニング」では、強力なスキルを構築して維持する方法と、Constituency、技術、サービス提供などの変化に合わせた継続的な改善に役立つ方法について説明します。



1つのスキルセットを、チームのすべてのポジションに適用できるわけではありません。チームの構成に適したスキルを判断するには、サービスの提供先である **Constituency**、および使用している技術の範囲を調べる必要があります。可能な限り、組織内の1人のチームメンバが絶対不可欠な存在にならないように、さまざまなスキルを持った人たちを採用する必要があります。これに対して、小さなチームでは、問題がプロフェッショナルな方法で対処されるように、技術に関して経験豊富な人を少なくとも1名任命する必要があります。ただし、この場合、そのような人がチームを去ったときに他の問題を招く可能性があります。一見矛盾しているように思われるかも知れませんが、実際にはスポンサーや資金提供組織および他のチームに対する窓口の役目を務める人よりも、最も経験豊富なチームメンバを替える方が簡単なのです。

## 4.5.2 スタッフの採用

スタッフの欠員募集を検討する場合は、最適な候補者を特定するための採用プロセスを事前に決めておく必要があります。経験から言えることは、表面上は適切なスキルセットがあるように見える候補者でも、**CSIRT**の作業環境に対応できないことがあるということです。また、危機的状況になったとき、自分の作業をこなすことができなくなる人もいます。関係者はみな、候補者の長所と短所を特定するように設計された採用プロセスに候補者を委ねる方が得策です。チームは、その情報を武器に、その候補者に必要な特定の技術を教えることができるかどうかを判断したり、その候補者を採用しないと決めたりすることができます。

どの **CSIRT** も、親組織、条例および国内法、文化による要件に基づいた特定要件に縛られています。しかし、可能且つ適切であれば、**CSIRT**の採用プロセスに次のステップを含めるべきです。

- 面接前の書類審査
- 面接前の電話による審査
- 技術的な能力から社会的スキル、チームへの適合性に至るまで各種の話題をカバーした面接
- 候補者の技術プレゼンテーション
- 必要に応じて、犯罪歴も含めた人物照会

親組織または **Constituency** の特殊な組織的要望によっては、機密情報の取扱許可や身元調査などのさらなるステップが必要な場合もあります。

全体的な採用プロセスは、候補者がポジションに適した対人スキルを備えているか、また、必要な技術スキルを持っているか（あるいは必要な専門技術を教え込むことができるか）が分かるように設計する必要があります。できるだけ多くのチームメンバが、候補者と話す機会を持つ必要があります（面接者として、ランチミーティングで、候補者の技術プレゼンテーションの参加者として）。また、

面接プロセスの間は、面接プロセスにかかるCSIRTスタッフの労力は最小限に抑えながら、最大限有効に活用することが重要です<sup>63</sup>。

候補者に関する面接前の書類審査と電話による審査は、その候補者に個人面接を行う価値があるかどうかを確認するのに役立ちます。このステップでは、コンピュータセキュリティに対する候補者の全般的な関心の度合いに合わせた広範囲な問題を取り上げ、履歴書に書かれている項目についてより具体的な詳細情報を得ることができます。しかし、最も重要なのは、これが候補者の口頭のコミュニケーションスキルについて良い印象を得られるかどうかを判断する機会になるということです。

候補者の面接を行う CSIRT スタッフを最大限に活かすために、面接プロセスを通して知りたい問題は何か（技術的および倫理的な問題から社会的スキルに至るまで）、候補者の問題に対処するのに今いるどのスタッフが最適かということを決めておくことが重要です。そうすれば、それぞれの面接者は特定の話題を取り上げ、労力の繰り返しを避けることができます。取り上げた問題に対する面接者のフィードバックについては、統合してチームメンバで議論することができます。場合によっては、別の方法をとることもできます。異なる観点から、特定の話題に関する候補者の知識の深さまたは広さを判断し、候補者の知識の弱点または誤りを指摘するために、面接プロセスに関係する他のチームメンバによって取って代わって同様の話題を取り上げることもあります。

候補者に技術プレゼンテーションを行ってもらえば、CSIRT は候補者の技術力や対人能力も評価することができます。チームは、候補者にどの程度の常識があるか、そして、いくぶん緊張に満ちた状況を候補者がどのように切り抜けるかを見極めることができます。また、一般的なプレゼンテーションスキル、細部への配慮、技術的な正確さ、その場で質問に答える能力などの特質も定量化できます。

言うまでもなく、ある候補者が採用されたら、CSIRT に組み入れるために多くの作業が必要になります。採用業務はこれからが本番です。新しいスタッフは、ある期間、トレーニングを受ける必要があります（4.5.4節「スタッフのトレーニング」を参照）一部の新しいスタッフは、適切な証明書または機密情報取り扱い許可（例えば、政府や軍の機密情報取り扱い許可）が得られるまで、限られた情報にしかアクセスできないことがあります。また、当然のことながら、すべての新しいスタッフは、CSIRT に順応できるように、また同様にチームや組織のその他の特定のポリシーおよび手順に順応できるように、何らかのトレーニング期間を経る必要があります。

---

<sup>63</sup> Michele Crabb、『How To Find and Hire Good Technical People』、Proceedings of SANS 1996 Conference、ワシントンDC、1996年5月12日－18日。Katherine T. Fithen、『Hiring IRT Staff Interview Process』、Forum of Incident Response and Security Teams、8th Workshop on Computer Security Incident Handling、カリフォルニア州サンノゼ、1996年7月。

### 4.5.3 着任および離任手続き

CSIRT が取り扱う情報は機密にかかわるものであるため、新しいスタッフの着任、およびチームからのスタッフの離任に関する特別な手続き方法をきちんと整えておくことが重要です。新しいスタッフは、親組織が要求する標準的な雇用契約（機密保持や知的所有権など）に加えて、CSIRT 独自の契約書に署名することを求められる場合があります。CSIRT 独自の契約書には、情報開示からネットワーク接続やメディアとの対話に至る様々な項目が含まれることがあります。

CSIRT のメンバが離任する前に（たとえ、チームから抜けるだけで同じ親組織に在籍する場合でも）、離任手続きを行う必要があります。離任手続きには、他の適切な CSIRT メンバ（チームのシステム管理者など）が行わなければならない作業が含まれます。離任手続きには次のことが含まれると考えられます。

- パスワードの変更（個人用パスワードとシステムパスワードの両方）
- 物理的なセキュリティ機器およびその他の媒体の返却（電話、ポケットベル、バックアップ）
- 鍵の破棄（物理的な鍵とデジタルの鍵の両方）
- 離任するスタッフの過去の実績を見直し、改善のためのアイデアを集める報告会
- 離任するスタッフに義務を思い出させるための離任面談（さらなる契約書への署名を伴う場合がある）
- CSIRT が日常的にやり取りしている Constituency および他の関係者への連絡
- 離任するスタッフ宛の今後の手紙（電子メール、郵送）に関してとるべき行動

スタッフが自分から進んでチームを去る場合は、そのような決断をした理由を知ることが重要です。これにより、チームは、注意を要する状況を理解し、他のチームメンバによる同様の離任を回避できる場合があります。

例：配置転換が長い間なかったため、あるスタッフは別の組織がマルチメディアセキュリティ分野における非常に魅力的な仕事を提示してきたのでチームを去りました。

チームメンバが解雇（契約解除）される場合、その決定には、その従業員に寄せた信頼をゆるがすような何らかの根本的な理由があるため、異なる離任手続きが適用されることがあります。この手続きには、解雇される従業員に付き添って私物を片付けさせること（CSIRT 管理者の監視下で）、組織の人事部と一緒に離任面談を受けさせること、解雇される従業員に付き添うこと／解雇される従業員を構内から離すこと（これは人事部長、サイトセキュリティ担当者、その他のセキュリティ担当者が対応することがある）が含まれる場合があります。このような場合でもパスワードの変更やその他の必要な措置を確実に実施します。特に、鍵やハードウェアトークンのような固有のものが回収できない場合は、不測事態対応計画を適切に立てる必要があります。

## 4.5.4 スタッフのトレーニング

次の3つの観点からスタッフのトレーニングが必要となります：業務の遂行に必要なレベルにまで新しいスタッフの技術レベルを引き上げる。個人の成長とチーム全体の利益のために、既存スタッフの能力を広げる。新技術と侵入者の傾向に応じて、CSIRT全体のスキルを最新状態に保つ。

チーム全体に必要なトレーニングを調べる際には、チームメンバ各自に必要な全般的スキルと、チーム全体として必要な一般的スキルの範囲を明らかにする必要があります。新しいスタッフには必須のスキルを直ちに教え、できるだけ早く戦力にする必要があります。より広い観点から、チームを全体として評価して、チームのスキルセットの対応範囲を広げるためのトレーニングや、また同時に特定の個人のスキルセットに焦点を当てたトレーニングを割り出す必要があります。少なくとも初期トレーニングを含み、且つポリシーと手順が変わっても現行のトレーニングが有効であることを保証するように、ポリシーと手順を整備しておく必要があります。確立されたポリシーと手順に従うことがなぜ重要なのか、しっかりした意識を持ち続けてもらうために、そして、ポリシーと手順に食い違いが認められる場合にスタッフが自分の常識を働かせなければならないという状況にも対応できるように訓練するために、研修が必要になることがあります。

この節の前の部分で説明した対人スキルと技術スキルに加えて、チームメンバ全員が、インシデントハンドリング機能や個々のチーム環境に固有の領域についてトレーニングを受ける必要があります。トレーニングには次の項目を含める必要があります。

- 新しい技術開発
- チーム固有のポリシーと手順
- 侵入手法の理解と特定
- サイトとの対話
- インシデント分析
- インシデント記録の保守
- チーム作り
- 作業負荷の分散と組織的手法

初期トレーニングは、OJT（オンザジョブトレーニング）に強く関係しており、詳しく説明するに値します。一般に、多くの専門職の初期トレーニングは、背景の解釈、観察、そして経験による学習という形をとります。このことは、インシデントハンドリングにも当てはまります。しかし、CSIRTスタッフのための正式な教育方針はなく、マニュアルも不十分です。大部分の資料は、講習会の報告書やプレゼンテーションのスライドの形をしています。インシデントハンドリングの学習に使用できる資料は限られているため、OJTが必要となります。

CSIRT Development Team は、CSIRT トレーニングのこの隙間を埋めるために努力しており、新しい（または既存の）インシデントハンドリングスタッフのトレ

ニングに役立つ一連のトレーニングコースと他の補助資料を開発し、拡充してきています。これらのトレーニング用資料は、CSIRTの作成および管理、セキュリティインシデントの対応および分析、ネットワークセキュリティの改善などを担当するマネージャと技術スタッフを対象にしています[CERT/CC 2002a]。

また、新しいCSIRTスタッフは、ポリシーと手順、事例研究、チームが保管している過去のインシデントの要約などの内部文書を調べ、そこから学ぶことが大切です。

最も経験豊富なスタッフでさえ、機密情報を扱う際にはある程度のストレスを感じるものです。このストレスの一部は、機密情報を不適切に扱った場合の結果の深刻さが分かっているために生じます。新しいスタッフは、CSIRTで直面する莫大な量の情報、ポリシー、手順に圧倒されることがあります。一般に、そのような新しいスタッフに最初のトレーニングをせずに、機密情報をうっかり開示しかねないような仕事を任せることは適切ではありません。訓練生が、損害の大きいミスを犯すことなく、専門職について学べるようにしてみましょう。よく使用される方法は、既存のCSIRTスタッフが、チームのポリシーと手順についてOJTを通して新しいスタッフに助言するという方法です。新しいスタッフは、小規模なインシデントの担当に移る前に、トリアージおよび要求対応の領域に精通しておくといよいでしょう。各領域では、新しいスタッフが、まず経験豊富なスタッフの行動を観察し、次に疑問点を解決するためにフォローアップの説明を受けるといった形をとることができます。その後、新しいスタッフは、環境についてよく理解できたら、経験豊富なチームメンバに見直しおよび編集をってもらうために電子メールの下書きを作成します。このようなことが、新しいスタッフがしかるべく熟達し、支援なしにそのような仕事を処理できると判断されるまで続けられます。

実際のインシデントに対応する前に、ロールプレイングゲームなどの別の方法を取り入れることが適切な場合があります。このような方法により、ポリシーと手順がハンドリングプロセスにどのように影響するかを新しいメンバに示すことができます[Smith 1994]<sup>64</sup>。

OJTは、知識の基礎を維持するためにトレーニングが必要な既存のチームメンバにも使用できます。技術の世界は急速に変わっているため、チームにトレーニングは不可欠です。また、会議への出席、技術交換、「ブラウンバッグランチ (brown-bag lunches、昼食を持ち寄るセミナー)」、適切な国際的タスクフォースおよびワーキンググループにおける活動により、直接関与したチームメンバの知識が増えるだけでなく、そのような知識がチーム内で共有されることでチーム全体の知識も増えることとなります。

---

<sup>64</sup> Thomas A. Longstaff、『Incident Role Playing: An Exercise to Develop New Insights Into the Process of Investigating a Computer Security Incident』、Forum of Incident Response and Security Teams、5<sup>th</sup> Workshop on Computer Security Incident Handling、ミズーリ州セントルイス、1993年8月。

### 4.5.5 スタッフの維持

本書の序論で述べたように、経験豊富な CSIRT スタッフは不足しており、スタッフを採用して CSIRT の環境に合うようにトレーニングするには費用がかかります。スタッフの選考、採用、トレーニングには時間と資金を投資しているため、スタッフの維持に努めることが最も重要です。CSIRT スタッフが辞職する 2 つの主な理由は、燃え尽きと給料の安さです。

多くの CSIRT スタッフが燃え尽き症候群に苦しんでいます（本書の執筆者も例外ではありません）。日々の（そして、24 時間サービスを提供している場合はしばしば夜の）インシデントハンドリング作業からの絶え間ないプレッシャーとストレスが重荷になり、私生活にも影響してきます。スタッフは、決まり切ったインシデントにうんざりし、肉体的に疲れ果て、細部への配慮を欠き、損害の大きいミスを犯す可能性があります。現在、大部分が有料サービスの CSIRT を介するインシデント対応の世界では、高い給料を望めるようになりつつあります。しかし、特に研究教育の世界では、競争力のある給料を払うだけの予算がすべてのチームにあるわけではありません。その一方で、このようなチームは、必ずしも 24 時間のサービスを提供するわけではありません。高い給料に引き寄せられる人は確かにいます。しかし、人によっては、仕事のやりがいや個人的な成長の可能性などが現職にとどまる動機となります。この両方の問題に対処するには、次の方法を検討する必要があります。

- ルーチンワークおよびインシデントハンドリングに関する職務のローテーション化
- インシデントハンドリングサービスに費やす各スタッフの労力を 80 パーセント以下に抑制
- 適切な技術会議／ワークショップ／チュートリアル（FIRST Conference など）<sup>65</sup>またはそれ以外のセキュリティプログラム（トレーニングコースなど）への出席
- 技術に関するワーキンググループへの参加（IETF など）
- 社内トレーニングコースの開発
- 社内トレーニングコースへの出席

優秀なスタッフの維持において大きな成功を収めているチームには、スタッフが職場だけでなくプライベートでも交流しているすばらしいチーム環境があります。また、すべてのチームメンバ（技術系および非技術系、新人およびベテラン）の貢献が尊重され、高く評価されている組織でもあります。

### 4.5.6 スタッフの補充

チームが必要とする専門スキルを持つ適切なスタッフへの資金提供や、そのようなスタッフの発見、トレーニング、採用が（何らかの理由で）できないことがあります。そのような場合、チームは、必要なスキルを持つその分野の専門家との

---

<sup>65</sup> <http://www.first.org/conference/>

関係（および了解事項の明確な合意）を確立することを検討することがあります。社内スタッフの専門知識が不十分という状況が発生したとき、欠けている部分を補ってもらおうようにこのような専門家に依頼することができます。CSIRT の環境の作業負荷は予測不能で、CSIRT が制御できない外部の出来事に左右されることが多いため、サービスの要求レベルに対応するのに今いる CSIRT スタッフでは不十分なときもあります。CSIRT は、中心的な CSIRT スタッフの代替要員または補充要員として事前に決められた人に助けを求める手順をきちんと整えておいた方がよい場合があります。これにより、チームは、インシデントの負荷が特定のしきい値を超えてピークに達した場合や、他にもチームのエスカレーションポリシーおよび手順に定義された状況に対処できるようになります。このような補助的な人材は、次のところから来てもらうことがあります。

- CSIRT の親組織内のセキュリティチームの他の部署
- CSIRT の親組織内の他のグループ
- CSIRT の Constituency 内のグループ
- 他の CSIRT 組織
- 外部の信頼できる専門家およびサービスプロバイダ

スタッフにこの役割を果たしてもらうことを検討する場合、CSIRT メンバとして同じ採用原則をそのスタッフに適用する必要があります。また、補充スタッフができるだけ早く活動できるように、事前に次のプロセスを確立しておく必要があります。

- 補充スタッフの参加を求める同意された基準
- 機密保持契約、サービス品質保証契約、覚書など
- 最新の連絡窓口情報
- 管理職による事前同意
- 安全な通信を確立するための手順
- 初期トレーニングおよび定期トレーニング

補充スタッフは、実際のインシデントハンドリングプロセスに参加する前に OJT を受ける必要があります。これにより、すべてのスタッフは、その日を通して互いに打ち解け、ポリシーと手順を実行する方法を理解できるようになります。

---

## 5 あとがき

### 5.1 初版を書き終えて

本書の執筆には、予想以上に時間がかかり、労力もかかりました。詳細情報を提供するかしないかを判断するのは、必ずしも簡単というわけではありませんでした。最初は短い報告書の形だったものが、やがて独り歩きを始めました。最終的に、本書にはハンドブックという表現が適切だろうということに決まりました。

執筆者たちが常に悪戦苦闘した問題の1つは、自分たちの環境にCSIRTを導入しようとしている方たちにとって、この情報がどの程度役に立つかということと、今後1年かそれ以上の時を経ても適用可能な情報をどのようにして提供するかということでした。概してセキュリティにも当てはまることですが、CSIRTのニーズはそれぞれ異なり、CSIRT環境は動的です。技術、Constituency、侵入者コミュニティは常に変わる可能性があるため、長期にわたる安定性を見込むことはできません。CSIRTの活動を確実に成功させるために、CSIRTには、環境ごとに変化するニーズに適応する能力と不測の事態に対応する柔軟性が必要です。さらにCSIRTは、ニーズに適応する能力、またはサービスを提供する能力に影響する可能性のある資金面の問題と組織の変化に同時に対応する必要もあります。

執筆者たちは、何年にもわたってCSIRTとインシデントハンドリングの分野で仕事をし、この分野に影響を与えてきましたが、これはやりがいのある仕事だということが分かりました（困難で、時にはいらだたく要求が厳しい仕事ではありますが）。そしてその見返りは、この仕事の価値を信じることで、世界中の熱心な他のチームメンバーと交流する機会を得ること、得られた教訓を進んで共有し、互いに支援し合うといったCSIRTコミュニティの姿勢を感じることで、そしてこの仕事とそれを支える基本技術に広く関心を持つことで得られるのです。

本書を執筆した主な目的の1つは、他の人たちを支援することです。執筆者たちは共同で、世界中の多くのチームが構成されるのを支援してきました。そして、そのプロセスで多くのことを学び、新しい友情が生まれ、楽しいときを過ごしました。しかし、他の人たちの利益になるように、私たちが学んで得たできるだけ多くの情報を文書化したいと考えました。情報を文書化できたというだけでなく、他の人たちにとって有意義且つ役立つ形で提供できていれば幸いです。CSIRTの構築、活動、プロセスの領域は、まだ初期段階にあり、コンピュータセキュリティの分野で居場所を見つけようと今なお奮闘しています。一方コンピュータセキュリティの分野はコンピュータの分野で適所を見出そうとしています。本書がCSIRTとその分野の継続的な発展と成熟に大きく貢献すると思っただけのことを願っています。そのように思っただけでないとしても、よりよい文書、ポリシー、そしておそらくは標準を作成するにあたって、本書がさらなる議論、改



良、改善、発議の出発点に少なくともなってくれば幸いです。他の人たちのこの種の取り組みには、喜んで関与または協力したいと考えています。

## 5.2 第2版を書き終えて

2002年後半頃、CERTのCSIRT Development Teamは、1998年の初版以来、更新された情報や得られた教訓を織り込んだ第2版を発行すべくCSIRTハンドブックの内容を見直すときが来たかと判断しました。

改訂はCSIRT Development Team (CDT)が行いました。CDTは、ペンシルベニア州ピッツバーグにあるソフトウェア工学研究所 (Software Engineering Institute) のNetworked Systems Survivability Program (CERT/CCも含まれる)の一環として設立されました。CERTスタッフは、1988年に対応した最初のホットライン電話以来、インシデント報告対応、習得、他への知識伝承を行っています。CERT/CCの歴史の初期において、スタッフは、アメリカ陸軍の陸上情報戦活動でインシデントハンドリング能力の構築を支援するトレーニング用教材を開発しました。以来、トレーニングはCERT/CCの活動の重要な要素となりました。1996年、CERT/CCのインシデントハンドリングチームの中からCSIRT Development Teamという概念が生まれ、このチームは独立した要素として承認されました。CDTのミッションは主に、CSIRTの世界的な発展にフォーカスしています。私たちは、コンピュータセキュリティインシデント対応の分野において、トレーニングコース、顧客との直接的な関係、そして啓発、教育、トレーニング、知識を提供する製品の開発を通してこのミッションを遂行しています。CDTは、何百人もの技術スタッフと管理スタッフをトレーニングし、独自のCSIRTの構築に必要な知識とスキルを彼らに提供してきました。

CERT/CCなどの国際的な組織の一員になると、新しいことが学べ、知力が伸び、視野が広がり、その結果、他の人たちに手を差し伸べることができるようになります。また、およそ15年にわたる活動で経験してきた教訓をコミュニティに提供し返すことができるようになります。各スタッフは、新しい友人と出会い、経験を共有し、CSIRTコミュニティの他のリーダーたちと仕事をし、世界中の熱心な他のCSIRTメンバと交流する機会が得られます。

今日の多くの組織は、攻撃やインシデントを検知し、適切な対応を開始する能力を備えたCSIRTを持つことになるだろうという共通認識がますます高まっています。実際、一部の分野では、組織はきちんと整えられたインシデント対応能力を備える必要があるという命令または規則が存在しています。この点において、企業の一部であるCSIRTは、リスクおよびセキュリティ管理のインフラと一体化したパートナーであると考えられます。独立した組織の多数のConstituencyを支援しているCSIRTは、インシデントハンドリングの支援（対応、通知、教育、トレーニング、啓発）を通じて、そして、脅威、攻撃、コンピュータセキュリティインシデントの影響を受けた組織の間をつなぐ頼れる連結役として、対応するコミュニティにさまざまな利益をもたらすサポートセンターであると考えられます。さらに、今日、重要インフラの保護は、以前にも増して重要になりつつあります。明確なインシデントハンドリングプロセス、および関連のある管理プロセ

スを備えた堅牢な CSIRT を持つ組織は、脅威や攻撃が発生したときに迅速且つ効果的に対応できます。

何年かするうちに他のことも変わりました。1998 年、初版の執筆者たちは「CSIRT の分野はまだ初期段階にある」と言っていました。2003 年、私たちは、インシデントハンドリングおよび管理活動の発展と推進において多くの点で CSIRT が依然として先駆者であると認識しています。

CSIRT は、今日の社会が依存している各種技術のリスクおよびセキュリティ管理の問題に対処するベストプラクティスを支援する上で、重要な役割を果たすことができます。CSIRT は、インシデント、脆弱性、攻撃への対応で得た知識からのフィードバックと教訓を採り入れることによって、組織全体に渡り長期的にセキュリティに取り組むためのセキュリティ品質管理プロセスの改善を支援できます。CSIRT はコンピュータセキュリティの分野で確立された役割と地位を獲得したと言っても過言ではないと私たちは考えています。このようなチームの活動における新たな関心事項は、攻撃やインシデントの間に実際に起こった事象の分析、脅威およびリスクの理解、効果的な対応の実装、および将来の攻撃の防御に対する必要性から生まれます。コンピュータフォレンジック（コンピュータ犯罪に対する科学調査）も、CSIRT 環境においてますます重要になりつつある分野であり、CSIRT が Constituency に提供する追加のサービスへと自然に発展するものと考えられます（実際、一部のチームによって既に提供されています）。

私たちは、ハンドブックの初版を読み、改訂版の作業に取り組んでみて、この仕事に対する情熱がまだ残っており、やりがいを感じ、他の人たちの役に立ちたいという気持ちがあることに気付きました。同時に、Moira、Don、Peter が最初のハンドブックを執筆したときに経験したのと同じ要求とフラストレーションが今日も依然として存在することが分かりました。CSIRT Development Team は、この4年間で、見返りはこの仕事の価値を信じることを、そして世界中で新しいチームができるのを目にすることから得られるということを確認しました。

締めくくりに、1998 年の初版の執筆者の言葉を言い換えてみたいと思います。本書が CSIRT の継続的な発展と成熟に大きく貢献すると思っただけのことを願っています。CSIRT ハンドブック初版は、新しいチームの出発点として、また、既存のチームが使用する評価およびベンチマークツールとして、さらに、この分野における活動のよりよいポリシー、プロセス、手順、標準を作成する際に、さらなる改良、改善、発議を提案する手段として、広範にわたって使用されてきています。

最後に、私たちはこの改訂版が、CSIRT Development Team が発行する他の文書<sup>66</sup>とともに、この重要な活動分野におけるさらなる一連の知識と支援を提供することになると強く確信しています。CSIRT 環境はそれぞれに少しずつ相違があり、私たちが求める全体的な知識に追加すべきものがあります。新規または既存の他

---

<sup>66</sup> <http://www.cert.org/csirts/>にある「State of the Practice of CSIRTs」、 「Organizational Models for CSIRTs」、その他のCSIRT関連発行物など。

のチームと教訓を共有すること、アイデアや経験、プロセスの交換の重要性は、CSIRT活動における「水準の引き上げ」に非常に大きな影響を及ぼします。私たちには、既存の多数のチームに関する知識があります（FIRSTやTERENAでの個人との独自の交流や話し合いを通して）。しかし、私たちがまだ知らない多くのチームが構築されているのではないかと思います。CSIRTを設立した場合はご連絡いただければ幸いです。

本書に関するご意見をお寄せください。賛成意見、あるいは本書への提案（またはそれ以外の意見）があれば、ご連絡ください。私たちは FIRST Conference に毎回出席しているので、直接お会いすることも可能ですし、[csirt-handbook@cert.org](mailto:csirt-handbook@cert.org) まで電子メールをお送りくださればグループに連絡することも可能です。

---

## 付録 A : 執筆者紹介

本書の執筆者たちは、チームのインシデントハンドリングサービスの形成、文書化、運用に関して幅広い経験があります。また、世界中のさまざまなコンピュータセキュリティインシデント対応チーム（CSIRT）の支援においても、発足から編成および運営まで豊かな経験があります。執筆者たちは CSIRT コミュニティの中心人物です。重要なインフラの問題から社会的影響に至るまで、さまざまなインターネットセキュリティに関する講演をたびたび依頼されています。

### **Moira J. West-Brown <moira@west-brown.com>**

Moira J. West-Brown は、1999 年までソフトウェア工学研究所（SEI : Software Engineering Institute）に本拠を置く CERT Coordination Center（CERT/CC）の上級技術スタッフでした。West-Brown は、SEI を去る前、世界中の新しい CSIRT の設立を支援するグループを率いていました。このグループは、国、政府、インターネットサービスプロバイダ、そして学術関係の CSIRT の設立において多種多様な組織を支援しました。

West-Brown は、1991 年にテクニカルコーディネータとして CERT/CC に加わり、コンピュータセキュリティインシデント報告と脆弱性報告に対応しました。数年間は CERT Operations チーム（コンピュータセキュリティ攻撃と脆弱性への対応を目的とした、事後対応に重点を置いたチーム）を取り仕切りました。West-Brown は、侵入者に関する報告の割合が劇的に増えた時期にチームを見事に導きました。また、今日他の CSIRT で採用されている運用上の多くの標準を確立し、発展させました。

West-Brown は、CERT/CC に加わる前は、学術機関や工業用ソフトウェアコンサルタント会社から、政府が出資する研究プログラムに至るさまざまな組織でシステム管理、ソフトウェア開発、ユーザサポート／窓口に関する幅広い経験を積みました。

国際的な CSIRT コミュニティでも活躍しました。CSIRT の運営上の問題や共同作業の問題に主な焦点を当てたさまざまなチュートリアルとワークショップ用の教材を開発しました。1995 年には FIRST Steering Committee（FIRST 運営委員会）の委員に選出され、1997 年から 1999 年には Steering Committee Chair（運営委員会委員長）を務めました。

また、イギリスのハル大学で計算科学の第 1 級（first class）学士号を取得しています。

## Klaus-Peter Kossakowski <kpk@presecure.de>

Klaus-Peter Kossakowski は、2000 年初めから、国際的な情報インフラ、IT セキュリティ、インシデント対応に関する上級コンサルティングを提供するドイツの独立系企業の常務取締役を務めています。現在は、リスクおよびセキュリティ管理、インシデント対応サービス、公開鍵インフラ、侵入検知、ネットワークセキュリティ、フォレンジック、セキュリティの改善などに取り組んでいます。

Kossakowski は、15 年以上セキュリティ分野で仕事をしてきました。1988 年、ハンブルクにある Virus Test Center の最初のメンバの一員です。ここでは、悪意のあるネットワークプログラムに重点的に取り組みました。DFN-CERT（オープンネットワークのためのドイツの最初の CSIRT）には発足からかかわりました。1993 年 1 月から DFN-CERT を去る 1997 年末まで、CERT/CC をモデルに作られたこの DFN-CERT チームを運営しました。研究活動から始まり、CSIRT コミュニティにおいて能力を認められ、広く尊敬を集める存在になるまで、このチームを見事に導きました。1998 年から 1999 年まで、ドイツの IT セキュリティプロバイダである secunet Security Networks AG の上級コンサルタント兼プロジェクトマネージャを務めました。ここでは、内部に secu-CERT チームを設立しました。1998 から 2003 年は CERT/CC の客員研究員も務めました。Kossakowski は、技術記事、文書、トレーニング用教材、それ以外の CSIRT 関連発行物を作成するために、CSIRT Development Team との共同作業を続けています。

CSIRT の領域で Kossakowski が特に関心を持っているのは、国際的な問題、連携、CSIRT インフラの構築です。1994 年以来、IETF ワーキンググループ「Guidelines and Recommendations for Incident Processing (GRIP)」の共同議長として、いくつかの RFC の整備に携わっています。Don Stikvoort とともに、ヨーロッパの CSIRT の間でより緊密な協力関係を作りだし、これらの CSIRT を支援するためにいくつかの定例会議を組織しました。そして、ヨーロッパの CSIRT コミュニティでの積極的な発言により、「ヨーロッパの CERT」と呼ばれる TERENA タスクフォースの議長に選出されました。このタスクフォースでは、ヨーロッパの CSIRT Coordination Center の概念とサービス定義の概略が紹介されました。この取り組みの結果、1996 年後半に、EuroCERT が設立されました。1997 年には FIRST (Forum of Incident Response and Security Teams) Steering Committee (運営委員会) のメンバに選出され、1999 年と 2001 年には再選されました。このとき、国際的な CSIRT の連携、および、新しい組織構成への FIRST の移行を積極的に支援しました。

Kossakowski は、ハンブルク大学で「Information Technology—Incident Response Capabilities」に関する博士論文の審査を受けました。ハンブルク大学では、情報科学の第 1 級 (first class) 学位を取得しました。Kossakowski は、ISOC (Internet Society)、ISSA (Information Systems Security Association)、ドイツの「Gesellschaft fuer Informatik e.V. (GI)」のメンバです。

## Don Stikvoort <don@elsinore.nl>

Don Stikvoort は、インターネットおよびイントラネットセキュリティの分野で上級コンサルティングサービスを提供するオランダの企業、STELVIO および S-CURE の常務取締役であり共同創立者です。

Don Stikvoort は、15 年以上、セキュリティ分野で仕事をしてきました。大学卒業後は、オランダ陸軍の歩兵小隊長の職に就きました。1989 年、オランダ国営の研究教育ネットワークである SURFnet に加わりました。SURFnet での 9 年間は、さまざまな責務を担いました。最初はコンサルタントでしたが、まもなく SURFnet バックボーン構築の責任者になりました。その後、SURFnet のヘルプデスクや他にもユーザ指向のサービスを担当する委託業者を管理し、いくつかの開発プロジェクトを指揮しました。1991 年に CERT-NL の設立に携わり、1992 年から 1998 年にはその議長を務めました。

Stikvoort は、特にセキュリティ問題に関して、国際的に、RIPE、TERENA、IETF、FIRST コミュニティに積極的に参加しています。Klaus-Peter Kossakowski とともに、1993 年にヨーロッパの CSIRT のより緊密な協力関係を作り出し、以来、より構造化されたヨーロッパのインシデントの連絡調整につながる活動に貢献しています。1996 年から 1998 年、FIRST が組織構成と資金調達モデルを発展させるのを積極的に支援しました。1998 年、Klaus-Peter Kossakowski および Moira J. West-Brown とともに、本書（『Handbook for Computer Security Incident Response Teams (CSIRTs)』）の初版を完成させました。Stikvoort は、オーストラリアのブリズベンで開催された 1999 年 FIRST Conference の Program Committee（プログラム委員会）の委員長を務めました。

Stikvoort は、オランダのライデン大学で実験低温物理学の学位を取得しました。ISOC のメンバであり、国によるいくつかのセキュリティフォーラムにも参加しています。また、国際的な FIRST 事務局および European Trusted Introducer サービス（ヨーロッパの CSIRT の独立認定プロセスを提供）の運営の最終責任者でもあります（これらはどちらも S-CURE に委託されています）。最近、kennisnet（オランダ国営の学校ネットワーク）およびオランダ政府の GOVCERT.NL 向けのコンサルティングに従事しています。現在は、いくつかの CSIRT コースの設立および運営に携わっています。そして、eCSIRT.net（CSIRT 間でインシデントデータおよび統計情報を交換するための IODEF 標準の構築を目指した EU 出資の研究プロジェクト）のコーディネータも務めています。

## Georgia Killcrece <georgia@cert.org>

Georgia Killcreceは、CERT® CSIRT Development Team（ペンシルベニア州ピッツバーグにあるカーネギーメロン大学のソフトウェア工学研究所（SEI：Software Engineering Institute）に本拠を置くNetworked Systems Survivability（NSS）Programの一環として設立）の技術スタッフです。Killcreceは、CERT Coordination Center（CERT/CC）が正式に設立されたわずか10か月後の1989年9月にCERT/CCに加わりました。

Killcreceは、CSIRTのさまざまな発展段階（教育／トレーニング、計画、実施、運用、協力）において、多様な組織（政府、産業、学術）と直接仕事をしてきました。また、公開トレーニングコースやオンサイトのトレーニングコースの開発と提供に携わっています。一連の5つのCSIRTコースを系統的に教える、Software Engineering Instituteの講師の1人でもあります。2002年末、Killcreceとそのチームは、CSIRTトレーニング用教材の使用を許諾するプログラムを完成させました。CSIRTコースを提供する認定を受けたTransition Partner（移行パートナー）を通して、世界のより広い範囲にCSIRTトレーニングを普及させることができます。同時に、このチームは、独自のCSIRTを設立する組織が情報を入手できるように、CERT Webサイト（<http://www.cert.org/csirts/>）上で文書を公開しています。

Killcreceは、CERT CSIRT Development Teamのリーダーになる前、1994年から1999年の間、CERT Coordination Centerのテクニカルコーディネータ兼インシデント対応コーディネータでした。これらの役割の中で、ペースの速いチーム環境における仕事の動的な変化も含め、インシデント対応チームの設立、運営、発展にかかわるプロセスの知識を現場でじかに得ました。主な担当は、コンピュータセキュリティ侵害および脆弱性報告の対応でした。またKillcreceは、Networked Systems Survivability ProgramのInformation Servicesチームの非常勤メンバーとして、CERT Webサイトで公開されるCERT/CC資料の作成および保守に貢献しました。

Killcreceは、Creating a Computer Security Incident Response Team: A Process for Getting Started、CSIRT Services、CSIRT Frequently Asked Questions、本書（『Handbook for Computer Security Incident Response Teams (CSIRTs)』）の改訂版など、コンピュータセキュリティインシデント対応チームに関する論文およびレポートの共同執筆者であり、また貢献者でもあります。他には、2003年にOrganizational Models for CSIRTsおよびState of the Practice of Computer Security Incident Response Teamsが公開される予定です<sup>67</sup>。

Killcreceに直接連絡するには、[georgia@cert.org](mailto:georgia@cert.org)宛に電子メールをお送りください。また、CSIRTトレーニングのエイリアスである[csirt-info@cert.org](mailto:csirt-info@cert.org)を通じて連絡可能です。

---

<sup>67</sup> 訳注：既に以下のURLでそれぞれ公開されています。

<http://www.sei.cmu.edu/publications/documents/03.reports/03hb001.html>

<http://www.cert.org/archive/pdf/03tr001.pdf>

## Robin Ruefle <rmr@cert.org>

Robin Ruefle は、CERT の CSIRT Development Team (SEI に本拠を置く Networked Systems Survivability Program の Practices, Development, and Training Group の一部) のテクニカルスタッフです。

Ruefle は、管理、手順、および技術のガイドラインの開発、ならびに、世界中の CSIRT の設立、発展、運営のための活動に重点的に取り組んでいます。Ruefle は、CSIRT マネージャとインシデントハンドリングスタッフに対する一連のコース (CSIRT の構築、CSIRT の管理、インシデントハンドリングの基礎、技術スタッフ向け上級インシデントハンドリングなど) を開発および提供しています。また、既存の CSIRT に対してこれらの製品の使用を許諾するトレーナ養成プログラムにも携わっています。Ruefle は、CERT の CSIRT Development Team のメンバとして、新規および既存の CSIRT に、実施方針、ポリシー、標準作業手順、対応計画、トレーニングプログラムの開発に関する手引きを提供しています。Ruefle は、Creating a Computer Security Incident Response Team: A Process for Getting Started、CSIRT Services、CSIRT Frequently Asked Questions など、コンピュータセキュリティインシデント対応チームに関する論文およびレポートの共同執筆者であり、貢献者でもあります。

Ruefle は、SEI に来る前は、ピッツバーグ大学の Academic Computing 部門でコンサルタント兼トレーナを務めていました。Academic Computing 在籍中に、学術コンピューティングの公開研究室、トレーニングプログラム、コンサルティングオフィスを管理しました。また、ワイヤレスラップトップ試験プログラムおよび Microsoft Windows NT 移行プロジェクトのリーダーも務めました。それ以前には、ペンシルベニア州予算局の中央サービス検査官用のデータベースプログラム、トレーニングコース、マニュアルを開発しました。

Ruefle は、ピッツバーグ大学で政治学の学士号と行政・国際関係学の修士号を取得しました。また、チャタム大学の MBA プログラム、およびピッツバーグ大学大学院行政・国際関係学研究科 (Graduate School of Public and International Affairs) の非常勤講師も務めています。そこでは、情報技術、経営情報システム、情報検索および情報分析の講座を担当しています。

Ruefle に直接連絡するには、rmr@cert.org 宛に電子メールをお送りください。また、CSIRT トレーニングのエイリアスである csirt-info@cert.org を通じて連絡可能です。



## Mark Zajicek <mtz@cert.org>

Mark Zajicek は、カーネギーメロン大学のソフトウェア工学研究所（SEI : Software Engineering Institute）の技術スタッフです。

現在、Zajicekは主に、他の組織が独自のコンピュータセキュリティインシデント対応チーム（CSIRT）を構築するのを支援しています。Zajicekは、SEIに本拠を置く Networked Systems Survivability Programの Practices, Development, and Training Groupの一部である CERT CSIRT Development Team (<http://www.cert.org/csirts/>) のメンバとして、全世界に及ぶ新規および既存のCSIRTにガイダンスを提供しています。また、さまざまな文書やトレーニング用教材を共同開発しました。CSIRTの管理者およびテクニカルスタッフのトレーニングのための一連のコースの講師でもあります。

Zajicek は、1992年に CERT Coordination Center (CERT/CC) のインシデントハンドリングスタッフに加わった後、CERT/CCの Daily Operations チームのリーダーになりました。CERT/CCに加わる前は、SEIの Computing Facilities グループのユーザコンサルタントでした。また、1988年の立ち上げ時に CERT/CC を支援しました。

Zajicek は、カーネギーメロン大学で電気工学および生物工学の学士号を取得しました。

---

## 付録 B : 用語集

ここでは、本書で使用される頭字語および略語を示すとともに、本書の目的に関連する最も重要な用語の定義を示します。

### 頭字語および略語

<b>24x7</b>	twenty-four hours a day, seven days a week (1日24時間、週7日)
<b>AFS</b>	Andrew file system (Andrew ファイルシステム)
<b>BCERT</b>	Boeing CERT (Boeing 社の CERT)
<b>CERT/CC</b>	CERT Coordination Center
<b>CERT-NL</b>	Computer Emergency Response Team Netherlands (オランダコンピュータ緊急事態対応チーム)
<b>CIDR</b>	Classless Inter-Domain Routing (クラスレスのドメイン間ルーティング)
<b>CIRC</b>	Computer Incident Response Capability (コンピュータインシデント対応能力)
<b>CIRT</b>	Computer Incident Response Team (コンピュータインシデント対応チーム)
<b>CSIRC</b>	Computer Security Incident Response Capability (コンピュータセキュリティインシデント対応能力)
<b>CSIRT</b>	Computer Security Incident Response Team (コンピュータセキュリティインシデント対応チーム)
<b>CSRC</b>	Computer Security Resource Center (コンピュータセキュリティリソースセンター)
<b>DFN-CERT</b>	Deutsches Forschungsnetz Computer Emergency Response Team (ドイツ研究ネットワークコンピュータ緊急事態対応チーム)
<b>DNS</b>	Domain Name System (ドメインネームシステム)
<b>FIRST</b>	Forum of Incident Response and Security Teams
<b>FTP</b>	file transfer protocol (ファイル転送プロトコル)
<b>GPG</b>	Gnu Privacy Guard
<b>GRIP</b>	“Guidelines and Recommendations for Incident Processing” (インシデント処理のガイドラインと勧告)

<b>HTTP</b>	Hypertext Transmission Protocol (ハイパーテキスト転送プロトコル)
<b>ICMP</b>	Internet Control Message Protocol
<b>IETF</b>	Internet Engineering Task Force
<b>IHT</b>	Incident Handling Team (インシデントハンドリングチーム)
<b>INND</b>	Internet news daemon
<b>IP</b>	Internet protocol (インターネットプロトコル)
<b>IRT</b>	incident response team (インシデント対応チーム)
<b>ISP</b>	Internet service provider (インターネットサービスプロバイダ)
<b>MCERT</b>	Motorola Computer Emergency Response Team (Motorola 社コンピュータ緊急事態対応チーム)
<b>MD5</b>	Message Digest 5
<b>MIME</b>	Multipurpose Internet Messaging Extension
<b>NTP</b>	Network Time Protocol
<b>PGP</b>	Pretty Good Privacy
<b>POC</b>	Point of contact (連絡窓口)
<b>RFC</b>	Request For Comments
<b>S/MIME</b>	Secure Multipurpose Internet Mail Exchange
<b>SERT</b>	Security Emergency Response Team (セキュリティ緊急事態対応チーム)
<b>SIRT</b>	Security Incident Response Team (セキュリティインシデント対応チーム)
<b>SMTP</b>	Simple Mail Transport Protocol
<b>SSC</b>	site security contact (サイトセキュリティ連絡窓口)
<b>SSH</b>	Secure Shell
<b>STE</b>	Secure Terminal Equipment
<b>STU III</b>	Secure Telecommunication Unit III
<b>SUNSeT</b>	Stanford University Network Security Team (スタンフォード大学ネットワークセキュリティチーム)
<b>TCP</b>	Transmission Control Protocol
<b>TERENA</b>	Trans-European Research and Education Networking Association
<b>TTP</b>	trusted third party (信頼できる第三者)
<b>UBC</b>	Unsolicited Bulk E-Mail

<b>UCE</b>	Unsolicited Commercial E-mail
<b>UDP</b>	User Datagram Protocol
<b>UNI-CERT</b>	Unisource Business Networks Computer Emergency Response Team (Unisource Business Networks 社コンピュータ緊急事態対応チーム)
<b>WWW</b>	World Wide Web

## 用語

### アーティファクト (Artifact)

侵入者の攻撃またはインシデント活動の残留物。侵入者が使用したソフトウェア、一連のツール、悪意のコード、ログ、ファイル、ツールからの出力、攻撃または侵入後のシステムのステータスが考えられます。アーティファクトは、トロイの木馬プログラムやコンピュータウイルスをはじめとして、侵害されたホストで見つかった脆弱性や未知のタイプ/目的のオブジェクトを悪用する（またはその存在を調べる）プログラムなど多岐にわたります。

### 真正性 (Authenticity)

何らかのサブジェクトまたはオブジェクトの識別情報を確認し、検証できたとき、サブジェクト/オブジェクトとその識別情報との関係は「真正である」と言うことができます。コンピュータセキュリティにおいては、通常、送信または受信した情報が伝送中に何らかの方法で変更されていないかを検証するときに使われます。

### Bugtraq

セキュリティ問題および脆弱性について議論するためのメーリングリスト。ときどき、このメーリングリストを介して、新しい脆弱性や攻撃ツールに関する情報を完全に開示したレポートが配布されることがあります。

### コンピュータセキュリティインシデント (Computer Security Incident)

コンピュータシステムまたはコンピュータネットワークのセキュリティに関する、有害事象または有害の疑いがある事象。このような事象の例を次に示します。

- ネットワークを介したコンピュータシステムへの侵入（多くの場合「ハッキング」と呼ばれる）
- コンピュータウイルスの発生
- ネットワークを介してさまざまなコンピュータシステムの脆弱性を探ること（多くの場合「スキャン」と呼ばれる）

コンピュータセキュリティの分野では、たいていの場合、このような出来事は単純にインシデントと呼ばれます。

### コンピュータセキュリティインシデントハンドリング (Computer Security Incident Handling)

基本的なサービスセット（トリアージ、ハンドリング、要求）を提供することによって、チームは定義された **Constituency** の支援を行い、コンピュータセキュリティインシデントに対応します。この基本セットに加えて、アナウンスサービスが提供される場合もあります。

## CSIRT

「コンピュータセキュリティインシデント対応チーム (computer security incident response team)」の頭字語。定義された Constituency にサービスを提供するチームのことです。同様のサービスを提供するチームを表す頭字語はいろいろあります (例えば CSIRC、CSRC、CIRC、CIRT、IHT、IRC、IRT、SERT、SIRT など)。本書では、コンピュータセキュリティコミュニティで広く採用されている「CSIRT」という総称を使用しています。

専門知識やリソースなどの要因によって、提供されるサービスのレベルおよび範囲がチームごとに異なる場合があります。

## Constituency

CSIRT が提供する特定のサービスを利用できる、ある決まったグループや組織。

## 侵入者 (Intruder)

コンピュータセキュリティインシデントの加害者である者。多くの場合、侵入者は「ハッカー」または「クラッカー」と呼ばれます。コンピュータが使われ始めた当時、「ハッカー」という用語は技術力が非常に高い専門家のことを指しましたが、その後、メディアによって、他のコンピュータシステムに侵入する人を指すときに使われるようになりました。一方「クラッカー」という用語は、「ハッカー」をもじって、侵入者がコンピュータシステムやセキュリティバリアを「crack する (破る)」という意味を込めて使われるようになりました。たいてい、「クラッカー」は、より悪名高い侵入者およびコンピュータ犯罪者を指すときに使われます。成功しなかった攻撃は侵入にはならないため、時として、「攻撃者」という用語の方が適切だと主張する人もいます。しかし本書では、攻撃に対して責任のある者ということ在意図して「侵入者」という用語を使用しています。

## 法的責任 (Liability)

損害または損失に対する責任のある人。

## ポリシー (Policy)

セキュリティやメディア対応などの特定のトピックについて組織またはコミュニティの活動を導く、書面による一連の記述。

## 手順 (Procedure)

ワークフロー、順序、メカニズムの形でのポリシーの実装。

## 残留ファイル (Remnant Files)

侵害されたシステムに侵入者が残したファイル。イーサネットスニファログファイルやパスワードファイル、攻撃スクリプト、ソースコードをはじめ、種々のプログラムなど多岐に渡ります (「アーティファクト」と呼ばれることもあります)。

## セキュリティポリシー (Security Policy)

セキュリティ関連の事柄を扱うポリシー。

## サイト (Site)

文脈に応じて、地理的位置、組織の管轄範囲、またはネットワークアドレスでグループ化されるコンピュータシステムを指します。

## サイトセキュリティ連絡窓口 (SSC, Site Security Contact)

サイトのコンピュータセキュリティ関連の責任者。

## ソーシャルエンジニアリング (Social Engineering)

ソーシャルエンジニアリングとは、自分が望む（他人が通常なら行わない）ことを他人に行わせる技術のことです。

侵入者は、技術的な方法で情報を収集するのではなく、電話で誰かの振りをしたり、それ以外の説得力のある方法（例えば、騙し、説得、誘導、そそのかし、挑発など）を使用したりするといったソーシャルエンジニアリングの方法を利用して、誰かに情報を開示させることもあります。これらは人々の社会的交流や習慣に基づくため、ソーシャルエンジニアリングと呼ばれます。

## トリアージ (Triage)

適切なハンドリングが容易にできるようにするための、情報の受け取り、初期選別、および優先順位付けのプロセス。

## トロイの木馬 (Trojan Horse)

関係するユーザ、システム、ネットワーク、アプリケーション、プロトコルのセキュリティを侵害する可能性がある（または侵害できる）不必要且つ未知の機能を備えるように変更された、【通常であれば】信頼できるプログラムまたはプロセス。

## 脆弱性 (Vulnerability)

システム、ネットワーク、アプリケーション、プロトコルのセキュリティを侵害する、好ましくない予期せぬ事態につながる可能性のある、設計上または実装上の誤りなどのソフトウェアの欠陥。

---

## 参考文献

- [Aslam 1995]** Aslam, Taimur, 『A Taxonomy of Security Faults in the UNIX Operating System』、Purdue 大学修士論文、1995年。
- [Brand 1990]** Brand, Russell L, 『Coping With the Threat of Computer Security Incidents:A Primer from Prevention Through Recovery』 バージョン CERT 0.6、ペンシルベニア州ピッツバーグ、1990年6月。
- [CERT/CC 1988]** CERT Coordination Center, 『CERT/CC Advisories』、ペンシルベニア州ピッツバーグ：カーネギーメロン大学ソフトウェア工学研究所、<<http://www.cert.org/advisories/>> (1988～2003年)。
- [CERT/CC 1996]** CERT Coordination Center, 『CERT/CC Product Vulnerability Reporting Form Version 1.0』、ペンシルベニア州ピッツバーグ：カーネギーメロン大学ソフトウェア工学研研究所、<[ftp://ftp.cert.org/pub/vul\\_reporting\\_form](ftp://ftp.cert.org/pub/vul_reporting_form)> (1996年10月)。
- [CERT/CC 1997a]** CERT Coordination Center, 『CERT/CC Incident Reporting Form, Version 5.2』、ペンシルベニア州ピッツバーグ：カーネギーメロン大学ソフトウェア工学研究所、<[ftp://ftp.cert.org/pub/incident\\_reporting\\_form](ftp://ftp.cert.org/pub/incident_reporting_form)> (1997年12月、2000年4月最終改訂)。
- [CERT/CC 1997b]** CERT Coordination Center, 『The CERT Coordination Center FAQ』、ペンシルベニア州ピッツバーグ：カーネギーメロン大学ソフトウェア工学研究所、<[http://www.cert.org/faq/cert\\_faq.html](http://www.cert.org/faq/cert_faq.html)> (2002年11月21日最終改訂)。
- [CERT/CC 1997c]** CERT Coordination Center, 『CERT Security Improvement Modules』、ペンシルベニア州ピッツバーグ：カーネギーメロン大学ソフトウェア工学研究所、<<http://www.cert.org/security-improvement/modules.html>> (2001年7月9日最終改訂)。



- [CERT/CC 1998a]** CERT Coordination Center, 『Incident Reporting Guidelines』、ペンシルベニア州ピッツバーグ：カーネギーメロン大学ソフトウェア工学研究所、  
<[http://www.cert.org/tech\\_tips/incident\\_reporting.html](http://www.cert.org/tech_tips/incident_reporting.html)>  
(1998年5月11日。2002年9月26日最終改訂)。
- [CERT/CC 1998b]** CERT Coordination Center, 『CERT Summary CS-98.05 - SPECIAL EDITION』、ペンシルベニア州ピッツバーグ：カーネギーメロン大学ソフトウェア工学研究所、  
<<http://www.cert.org/summaries/CS-98.05.html>>  
(1998年5月28日)。
- [CERT/CC 1998c]** CERT Coordination Center, 『CERT/CC Incident Notes』、1998～2002年。ペンシルベニア州ピッツバーグ：カーネギーメロン大学ソフトウェア工学研究所、  
<[http://www.cert.org/incident\\_notes/](http://www.cert.org/incident_notes/)> (2002年12月17日最終改訂)。
- [CERT/CC 1998d]** CERT Coordination Center, 『CERT/CC Vulnerability Notes』、ペンシルベニア州ピッツバーグ：カーネギーメロン大学ソフトウェア工学研究所、  
<<http://www.kb.cert.org/vuls/>>。
- [CERT/CC 1998e]** CERT Coordination Center, 『Problems With The FTP PORT Command or Why You Don't Want Just Any PORT in a Storm』、ペンシルベニア州ピッツバーグ：カーネギーメロン大学ソフトウェア工学研究所、  
<[http://www.cert.org/tech\\_tips/ftp\\_port\\_attacks.html](http://www.cert.org/tech_tips/ftp_port_attacks.html)>  
(1999年2月12日最終改訂)。
- [CERT/CC 2000]** CERT Coordination Center, 『Windows NT Configuration Guidelines』、ペンシルベニア州ピッツバーグ：カーネギーメロン大学ソフトウェア工学研究所、  
<[http://www.cert.org/tech\\_tips/win\\_configuration\\_guidelines.html](http://www.cert.org/tech_tips/win_configuration_guidelines.html)>。
- [CERT/CC 2002a]** CERT Coordination Center, 『CSIRT Development』、ペンシルベニア州ピッツバーグ：カーネギーメロン大学ソフトウェア工学研究所、<<http://www.cert.org/csirts/>>  
(2002年12月11日最終改訂)。

- [CERT/CC 2002b]** CERT Coordination Center、『Computer Security Incident Response Team Frequently Asked Questions』、ペンシルベニア州ピッツバーグ：カーネギーメロン大学ソフトウェア工学研究所、<[http://www.cert.org/csirts/csirt\\_faq.html](http://www.cert.org/csirts/csirt_faq.html)>（2002年7月2日最終改訂）。
- [CERT-NL 1992]** CERT-NL、『CERT-NL Operational Framework, Version 2.1』、オランダ・ユトレヒト、1992年6月23日。
- [Chapman 1995]** Chapman, D. Brent、Zwicky, Elizabeth、『Building Internet Firewalls』初版。カリフォルニア州セバストポール、O'Reilly & Associates、1995年。
- [CIAC 1994]** Lawrence Livermore National Laboratories、『CIAC Bulletin:Computer Incident Advisory Capability』、カリフォルニア州リバモア、<<http://ciac.llnl.gov/cgi-bin/index/notes>>（1994～1998年）。
- [Cormack, 2002]** Cormack, Andrew、『Writing Advisories』、JANET Guidance Notes GD/NOTE/007。ロンドン、2002年。  
<[http://www.ja.net/documents/gn\\_advisories.pdf](http://www.ja.net/documents/gn_advisories.pdf)>
- [Devargas 1995]** Devargas, Mario、『The Total Quality Management Approach to IT Security』。オックスフォード：NCC Blackwell、1995年。
- [FIRST 1997]** Forum of Incident Response and Security Teams、『Forum of Incident Response and Security Teams (FIRST) Operational Framework』、  
<[http://www.first.org/about/op\\_frame.html](http://www.first.org/about/op_frame.html)>（2002年7月30日最終改訂）。
- [FIRST 1998]** Nijssen, Teun、Ley, Wolfgang、Forum of Incident Response and Security Teams、『FIRST PGP FAQ Version 1.3』  
<<http://www.first.org/docs/pgpfaq/>>  
（1998年6月8日最終改訂）。
- [Garfinkel 1996]** Garfinkel, Simson、Spafford, Eugene、『Practical UNIX & Internet Security』第2版。カリフォルニア州セバストポール。O'Reilly & Associates、1996年。

- [Gordon 1995]** Gordon, Sarah、 『Social Engineering: Techniques and Prevention』 445-451. Proceedings of the 12<sup>th</sup> World Conference on Computer Security, Audit and Control. 英国ロンドン、ウエストミンスター、1995年10月25～27日：Elsevier、1995年。
- [Greening 1996]** Greening, Tony、 『Ask and Ye Shall Receive: A Study in ‘Social Engineering’』、ACM SIG Security, Audit & Control Review 14, 2 (1996): 8-14.
- [Icove 1995]** Icove, David、 Seger, Karl、 VonStorch, William、 『Computer Crime: A Crimefighter’s Handbook』、カリフォルニア州セバストポール、O’Reilly & Associates、1995年。
- [IETF 1997]** Internet Engineering Group Task Force、 『An Open Specification for Pretty Good Privacy (openpgp), Charter 1997-1998』、<<http://www.ietf.org/html.charters/openpgp-charter.html>> (2001年7月31日最終改訂)。
- [ISC 2003]** Internet Domain Survey、 Internet Software Consortium、<<http://www.isc.org/ds/WWW-200301/index.html>> (2003年1月)。
- [Kaufman 1995]** Kaufman, Charlie、 Perlman, Radia、 Spencer, Mike、 『Network Security: Private Communication in a Public World』 ニュージャージー州イングルウッドクリフス、Prentice Hall、1995年。
- [Kossakowski 1994]** Kossakowski, Klaus-Peter、 『The DFN-CERT Project』、6th Workshop on Computer Security Incident Handling、 Forum of Incident Response and Security Teams、 マサチューセッツ州ボストン、1994年7月。  
<<ftp://ftp.cert.dfn.de/pub/csir/dfncert/papers/6csihw.dfncert.ps.gz>> (1994年)。
- [Kossakowski 2000]** Kossakowski, Klaus-Peter、 Allen, Julia、 『Securing Public Webservers』、 (CERT Security Improvement Module CMU/SEI-SIM-011)。ペンシルベニア州ピッツバーグ：カーネギーメロン大学ソフトウェア工学研究所CERT Coordination Center。<<http://www.cert.org/security-improvement/modules/m11.html>> (2000年：2001年4月25日最終改訂)。

- [Kossakowski 2001]** Kossakowski, Klaus-Peter, 『Information Technology Incident Response Capabilities』、ドイツ・ハンブルグ大学博士論文、ハンブルグ : Books on Demand, 2001 (ISBN: 3-8311-0059-4)。
- [Longstaff 1993]** Longstaff, Thomas A, 『Results of a Workshop on Research in Incident Handling』 (CMU-SEI-93-SR-020)。ペンシルベニア州ピッツバーグ : カーネギーメロン大学ソフトウェア工学研究所CERT Coordination Center。<<http://www.sei.cmu.edu/publications/documents/93.reports/93.sr.020.html>> (1993年9月)。
- [NIST 800-12]** National Institute of Standards and Technology. 『An Introduction to Computer Security: The NIST Handbook』 (NIST Special Publication 800-12)。メリーランド州ゲイサーズバーグ : National Institute of Standards and Technology。
- [NRL 1995]** Naval Research Laboratory, IS Security Group, 『IS Security Incident Response Manual』 (Code 1220.2)、ワシントン D.C. : Naval Research Laboratory、1995年。
- [NRL 1997]** Naval Research Laboratory, IS Security Group, 『IS Security Incident Response Plan』、ワシントン D.C : Naval Research Laboratory、1997年1月。
- [Olnes 1994]** Olnes, Jon, 『Development of Security Policies』、Computers & Security 13, 8 (1994): 628-636。
- [Pethia 1990a]** Pethia, Richard D., 『Forming and Managing a Response Team』、Workshop on Computer Security Incident Handling、カリフォルニア州プレザントン、1990年6月。
- [Pethia 1990b]** Pethia, Richard D., 『Developing the Response Team Network』、Workshop on Computer Security Incident Handling、カリフォルニア州プレザントン、1990年6月。
- [Pethia 1990c]** Pethia, Richard D., van Wyk, K. R., 『Computer Emergency Response: An International Problem』、ペンシルベニア州ピッツバーグ : カーネギーメロン大学ソフトウェア工学研究所CERT Coordination Center、1990年。

- [RFC 1281]** Pethia, Richard D.、 Crocker, Steve、 Fraser, Barbara、  
『Guidelines for the Secure Operations of the Internet』 (IETF Request for Comments 1281)。  
<<http://www.faqs.org/rfcs/rfc1281.html>> (1991) 。
- [RFC 1422]** Kent, S. T.、 Linn, J.、 『Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-based Key Management』 (IETF Request for Comments 1422)。  
<<http://www.faqs.org/rfcs/rfc1422.html>> (1993 年) 。
- [RFC 1984]** IAB and IESG.、 『IAB and IESG Statement on Cryptographic Technology and the Internet』 (IETF Request for Comments 1984)。 <<http://www.faqs.org/rfcs/rfc1984.html>> (1996 年) 。
- [RFC 2196]** Barbara Fraser編集、 『Site Security Handbook』 (IETF Request for Comments 2196)。  
<<http://www.faqs.org/rfcs/rfc2196.html>> (1997 年) 。
- [RFC 2350]** Brownlee, N.、 Guttman, E.、 『Expectations for Computer Security Incident Response』 (IETF Request for Comments 2350, Best Current Practice)。  
<<http://www.faqs.org/rfcs/rfc2350.html>> (1998 年) 。
- [RFC 3067]** Arvidsson, J.、 Cormack, A.、 Demchenko, Y.、 Meijer, J.、  
『TERENA's Incident Object Description and Exchange Format Requirements』 (IETF Request for Comments 3067, Informational)。 <<http://www.faqs.org/rfcs/rfc3067.html>> (2001 年) 。
- [Schneier 1995]** Schneier, Bruce、 『Applied Cryptography: Protocols, Algorithms, and Source Code in C』、英国チチェスター：John Wiley & Sons、1995 年。
- [Shimomura 1995]** Shimomura, Tsumotu、 Markoff, John、 『Takedown』、ロンドン：Secker & Warburg、1995 年、ISBN 0-436-20287-5。
- [Smith 1994]** Smith, Danny、 『Forming an Incident Response Team』、クイーンズランド大学、オーストラリア・ブリズベン、1994 年 7 月。

- [Stoll 1989]** Stoll, Clifford、 『The Cuckoo's Egg』 、 Doubleday、 1989年、 326pp, ISBN 0-370-31433-6。
- [TERENA 1995]** Kossakowski, Klaus-Peter 編集、 『Final Report of the TERENA Task Force 'CERTs in Europe』 、 オランダ・アムステルダム : Trans-European Research and Education Networking Association、 1995年10月。
- [West-Brown 1995]** West-Brown, Moira J.、 『Incident Trends』 、 Proceedings of the UNIX Network Security Conference、 ワシントン D.C.、 1995年11月。
- [Wood 1998]** Wood, Charles Cresson、 『Information Security Policies Made Easy』 第6版、 カリフォルニア州ソーサリト : Baseline Software Inc.、 1998年。 ISBN# 1-881585-04-2。