JPCERT CC®

平成 27 年 11 月 26 日

一般社団法人 JPCERT コーディネーションセンター

組織内 CSIRT 構築支援マテリアルの改訂版の公開にあたって

1　組織内 CSIRT 構築支援マテリアル（改訂版）について

組織内 CSIRT 構築支援マテリアル（改訂版）（以下「本マテリアル」といいます。）は、一般社団法人 JPCERT コーディネーションセンターが平成 18 年度に実施した、企業等の組織内における CSIRT（Computer Security Incident Response Team）機能の構築を支援する一連の活動の成果物として公開されていたものを踏まえて、CSIRT 構築にあたる普遍的な部分を大切にしながら、次々に変わりゆく IT セキュリティ脅威にも対応できるように、加筆・修正をしたものです。

本マテリアルは、これから組織内 CSIRT を構築しようとする組織だけではなく、既に組織内 CSIRT やそれに準ずる組織を擁する組織に対しても、新しい IT セキュリティ脅威に対応するための情報およびノウハウを提供することを目的としています。

2　旧版：組織内 CSIRT 構築支援マテリアルの位置づけ

組織内 CSIRT 構築支援マテリアル（以下「本マテリアル」といいます。）は、一般社団法人 JPCERT コーディネーションセンターが平成 18 年度に実施した、企業等の組織内における CSIRT（Computer Security Incident Response Team）機能の構築を支援する一連の活動の成果物として公開するものです。

組織の事業内容や規模、部門構成、業務遂行形態、それぞれの組織や事業に対応する脅威やリスクの定義により、それぞれの組織内 CSIRT の活動内容や形態などが大きく異なるため、組織の状況にあわせて機能を構築していただくことが組織内 CSIRT を有効に機能させるうえで重要な意味を持ちます。

本マテリアルは、これから組織内 CSIRT を構築しようとする組織に対して、その構築過程に必要な情報およびノウハウを提供することを目的として公開するものです。

3　背景

最近の情報セキュリティ上の脅威の動向として、従来の不特定多数を狙った愉快犯と見られる攻撃が目立たなくなる一方で、特定の企業や組織を狙った攻撃が高度化していることが指摘されています。特に、経済的利得の不正取得などの明確な目的に基づいた標的型攻撃が増加するとともに、その攻撃手法が巧妙化・不可視化するなど、情報資産への脅威は増大しているといえます。また、脅威やリスクのとらえ方が企業・組織ごとに異なることもあり、想定される事前対策の内容もさまざまです。

そのため、個々の企業・組織に最適な情報セキュリティ管理体制や情報セキュリティ施策を組織全体に運用して、リスク管理の枠組みのなかで個々の事象に適切に対応するのは容易ではありません。

また、事業活動がかつてないほどに IT（情報技術）の利活用を前提とし、システムやネットワークの相互依存関係が無視できなくなってきている現況にかんがみると、システムやネットワーク上で発生したコンピュータセキュリティインシデント[1]（以下「インシデント」という。）の潜在的影響と被害は、従来の予測を超える規模に達することが予想されます。

さらに、広範な企業・組織に対して功を奏する攻撃手法によるインシデント（ボットネット、フィッシング、高度サイバー攻撃(APT)等）の問題も広がりを見せており[2]、組織を超えたインシデント対応の連携が求められる状況が発生しています。

このような状況から、情報資産保護策の一環として、考えられるあらゆる攻撃に対応する部門または部門を横断した対応チームを設け、組織内にインシデント対応機能を持つ必要性が高まってきています。組織内 CSIRT とは、このようなチーム・機能のことをいいます。

組織内 CSIRT を設けて、従来組織内に点在していたインシデントに関するさまざま情報を集約することにより、インシデントが発生した際に迅速かつ的確な「組織としての意思決定と対応」を行うことが可能となり、被害の最小化および同様の問題に対する事前策の検討などの効果を期待することができるようになります[3]。

また、組織内 CSIRT が外部のインシデント対応組織等との情報共有や信頼関係の構築の役割を担うことにより、組織外に起因するインシデントが発生した際に、そのインシデントに直接対応できる組織への対応依頼等を円滑に進めることができ、早期の解決を図ることができるようになります。

このように、組織内に CSIRT 機能を実現するための体制を構築し、組織としてのインシデント対応能力を向上させることの意義は大きく、情報セキュリティ管理体制の強化のみならず組織基盤の強化にも寄与する取り組みであるといえます。

4　本マテリアルの目的

各組織において組織内 CSIRT を構築する必要性が認識された後は、経営層の理解と意

---

[1] コンピュータセキュリティインシデントの定義は組織ごとに異なるが、一例として JPCERT コーディネーションセンターの定義を示す。「インシデント報告の届出」（http://www.jpcert.or.jp/form/）では「コンピュータセキュリティインシデントとはインターネットに接続されたシステムを運用する際に発生したセキュリティ上の問題として捉えられる事象のことです」としている。

[2] ボットネットの現況については、JPCERT コーディネーションセンターが 2006 年 7 月に公開した調査報告書「ボットネットの概要」を参照されたい（https://www.jpcert.or.jp/research/2006/Botnet_summary_0720.pdf）。APT とは先進的で（Advanced）執拗な（Persistent）脅威（Threat）。

[3] 組織内 CSIRT の位置づけや主要な役割期待の定義例については、本活動成果物の各マテリアルを参照されたい。

思決定を端緒として組織内 CSIRT の構築に着手するのが一般的です。その際には、提案者と IT リスク管理に関係する各部門や IT ユーザーとの連携が不可欠となります。

組織内に CSIRT を構築する必要性が理解された後に問題となるのは、構築に必要となる情報が十分に得られないという問題です。組織内 CSIRT の構築に向けた取り組みは海外で先行して開始されたため、過去においては、関連する情報を積極的に入手するためには海外文献に頼らざるを得ませんでした[4]。この状況は、前回 CSIRT 構築マテリアルをリリースしてから 5 年近くが経過した今も大きな違いはなく、枠組みとしての CSIRT 組織を構築するには充分な情報であっても、その後の運用や、昨今発生する先進的な攻撃に対して、どのように対処すべきかといった情報は、依然として海外文献に頼らざるを得ない状況です。

また、組織内に CSIRT を構築することを決定した後に、具体的にどのようなプロセスで構築していくのかを決定するのは容易とはいえません。

本マテリアルは、このような現状にかんがみ、組織内 CSIRT を構築しようとする企画発案や構築にたずさわる方々に、必要な情報の提供と具体的な構築プロセスの立案の支援を行うことを目的としています。

作成にあたっては、組織内 CSIRT 構築を目指す方々が、本マテリアルを活用して、関係部署や経営層などに対して組織内 CSIRT に関する説明と意識の共通化を進めることができるよう、できるだけ多くの図表を挿入して視覚的に理解いただけるものとなるよう配慮しました。

5　本マテリアルの構成

本マテリアルは、大きく分けて、組織内 CSIRT の「認知」、「理解」、「実践」の３つに分類されます。

「組織内 CSIRT の認知」は、さまざまな角度から組織内 CSIRT の必要性に関する論点を提供しています。また、インシデント対応体制の設置の意義やメリットおよび事前のインシデント対応計画の立案の重要性を述べることによって、本マテリアルの利用者がそれぞれのポイントにおいて自組織内の状況と照らし合わせながら組織内 CSIRT の必要性に対する理解を深めることを意図しています。

「組織内 CSIRT の理解」においては、組織内 CSIRT の役割モデルを客観的な視点からまとめ、組織の視点から見いだされる組織内 CSIRT の活動の定義と範囲に関する考察ポイントなどを提供しています。さらに、組織内 CSIRT の形態分類とそれらの特徴に関する情報を提供することにより、本マテリアルの利用者に、自組織に組織内 CSIRT を構築

[4] CERT/CC が公開している CSIRT 構築のための手引き *Handbook for CSIRTs* の日本語訳を JPCERT/CC が「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」として提供している（http://www.jpcert.or.jp/research/）。また、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）などが公開した情報セキュリティに関する文書の日本語訳を情報処理推進機構 セキュリティセンター（IPA/ISEC）が提供しているので合わせて参照されたい（http://www.ipa.go.jp/security/publications/nist/index.html）。

する際の計画立案に役立つポイントを把握していただくことを意図しています。

最後の「組織内 CSIRT の実践」は、組織内 CSIRT 構築の全体的なプロセスに関する情報と実作業に有益な情報を提供しています。また、組織内 CSIRT 構築の実作業をすすめる上で参考にし、ひな型として活用できるフォームとその作成例を提供しています。さらに、平成 18 年度に実施したフィールドリサーチの過程でいただいた要望などを参考に、インシデント対応マニュアルの作成や組織内 CSIRT における情報管理等に役立つ参考資料も提供しています。これらのマテリアルを活用することにより、組織内 CSIRT 構築に必要な人員の割り当てや工数の見積もり等の計画に役立てていただくとともに、実際の構築の作業を円滑に進める一助としていただくことを意図しています。

6　本マテリアルの活用方法

本マテリアルは、下記のように利用することができます。

(1) 「認知」および「理解」の分類のマテリアルについて

- 利用者自身が、組織内 CSIRT を理解および習得するために通読する。
- 関係部署や経営層に対して組織内 CSIRT に関する理解をしてもらうために、本マテリアルの全部あるいは一部を説明資料として活用する。

(2) 「実践」の分類のマテリアルについて

- 利用者自身が、組織内 CSIRT の構築に必要な作業の見積もりを算出するために通読する。
- 組織内 CSIRT の構築の実作業の各工程の成果物について、それぞれ提供されている作成例を参考にしながらフォームの各項目を記述することにより、実作業の進捗を進める。また、各成果物の完成をマイルストーンとして、実作業の確実な作業進捗を図る。

(3) 「参考資料」の分類のマテリアルについて

- 利用者自身が、組織内 CSIRT に関して標準的な目安となる情報を把握するために通読する。
- 関係者や経営層に対して、組織内 CSIRT に関して必要な情報を提供するために、本マテリアルの全部あるいは一部を説明資料として活用する。

7　各文書の名称と概要

(1)　組織内 CSIRT に関する共通認識の形成

分類	マテリアル名	概　要
認知	組織内 CSIRT の必要性	インシデント対応活動の必要性をさまざまな観点から説明することによって、組織内 CSIRT の意義やメリットを視覚的に説明している。また、事前の対応計画の立案にも触れている。
理解	組織内 CSIRT の役割とその範囲	組織内 CSIRT を客観的な視点からみた在りようを、役割という観点から説明している。特に、「インシデント」との関係から組織内 CSIRT を 3 つに類型化し、それぞれの組織内 CSIRT の責務と使命の一般的な例を示している。また、組織内 CSIRT の理解を助けるために、消防署の役割との類似比較や CSIRT という概念の起源に関する情報を提供している。
	組織内 CSIRT の活動	組織内 CSIRT の内側の視点から、活動のために重要な「インシデントの定義」に関する説明と、そのほかに必要となる定義対象の考察ポイントを提供している。また、参考情報として、IT 部門の活動範囲との関係図の例を提供している。
	組織内 CSIRT の要員	組織内 CSIRT 要員に重要なスキルの説明と、ヒューマンスキルとテクニカルスキルの両面で求められる要求事項に関する情報、トレーニングに関する情報を提供している。また、参考情報として、求められるスキルにおける IT 部門の要員との違いの例を提供している。
	組織内 CSIRT の形態	組織内 CSIRT の設立形態を分類し、それぞれの特徴を解説している。また、どの形態を参考として自らの組織の CSIRT を構築するかを判断するための目安として、各形態に共通して見られる前提条件をまとめている。

(2) 組織内 CSIRT の構築

分類	マテリアル名	概　要
構築	組織内 CSIRT の構築プロセス	組織内 CSIRT の構築を実現するために必要な 8 つのプロセスとそれぞれのポイントを説明している。また、組織内 CSIRT 構築に関して検討しなければならない事項をまとめた一覧も提供している。
	組織内 CSIRT 構築の実作業	組織内 CSIRT 構築に必要な実作業の工程について説明している。特に、人的リソースや作業見積もりの算定に役立つ情報を提供している。
	組織内 CSIRT 構築：構築活動のためのプロジェクト憲章	「組織内 CSIRT 構築の実作業」中の「キックオフ、スケジューリング」における成果物のフォームと作成例を提供している。
	組織内 CSIRT 構築：構築活動のためのスコープ記述書	「組織内 CSIRT 構築の実作業」中の「ゴールの設定とタスクの細分化」における成果物のフォームと作成例を提供している。
	組織内 CSIRT 構築：構築に必要な現状把握	「組織内 CSIRT 構築の実作業」中の「組織内の現状把握」における成果物のフォームと作成例を提供している。
	組織内 CSIRT 構築：CSIRT の基本的な枠組み	「組織内 CSIRT 構築の実作業」中の「組織内 CSIRT の設定」における成果物のフォームと作成例を提供している。特に、大きな指針をまとめるときに活用することができる。
	組織内 CSIRT 構築：CSIRT 記述書	「組織内 CSIRT 構築の実作業」中の「組織内 CSIRT の設定」における成果物のフォームと作成例を提供している。特に、RFC 2350「コンピュータセキュリティインシデント対応への期待」に準拠するために活用することができる。

(3) 参考用資料

分類	マテリアル名	概　要
参考資料	インシデント対応マニュアルの作成について	インシデント対応マニュアルの作成に必要なノウハウと考察すべきポイントを説明している。また、幾つかのインシデントの対応事例により、そのインシデントフローの捉え方の例を提供している。
	組織内 CSIRT の情報管理と設備について	組織内 CSIRT における情報管理とそれを実装する設備等を整備するために必要な考察および留意ポイントを提供している。
	組織内 CSIRT における電話対応について	組織内 CSIRT における電話対応について、配慮すべき事項と、電話応対の記録や要領手順の例を提供している。

8　本文書を含む活動成果物の引用・転用について

9　免責事項

10　謝辞

本マテリアルの作成にあたっては、日本国内の企業・組織の実情に即したマテリアルの整備を目的として、フィールドリサーチを行いました。ご協力いただいた企業・組織の方々にこの場をお借りして感謝申し上げます。また、組織内 CSIRT 構築支援マテリアルの公開に当たり、日本シーサート協議会設立発起人各位をはじめとする多くの方々にご協力をいただきました。ここに心より感謝の意を表します。

11 変更履歴

初　版：2007 年 6 月 14 日

第 2 版：2015 年 11 月 19 日

12 連絡先

一般社団法人 JPCERT コーディネーションセンター

Email: pr@jpcert.or.jp