プロジェクト名：

\_Label\_Keyword\_公開情報\_Keyword\_\_Label\_Keyword\_社外向け文書\_Keyword\_\_Label\_Keyword\_個人情報を含まない\_Keyword\_

組織内 CSIRT 構築

CSIRT 記述書

（バージョン　 年 月　　日）

|  |  |
| --- | --- |
| 担当部署 | 作成者 |
|  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 審議欄 |  |  |  |  |  | 承認者 |
|  |  |  |  |  |

CSIRT 記述書（Description）

目　次

**１　文書情報 (Cocument Information) 　３ページ**

　(1)　最終更新日 (Date of Last Update)

　(2)　通知の他の配布リスト (Distribution List for Notifications)

　(3)　本文書の場所 (Locations where this Document May Be Found)

　(4)　本書の検証 (Authenticating this Document)

**２　連絡先情報 (Contact Information) 　４ページ**

　(1)　チーム名 (Name of the Team)

　(2)　所在地 (Address)

　(3)　時間帯 (Time Zone)

　(5)　ファクシミリ番号 (Facsimile Number)

　(6)　他の音声通信手段 (Other Telecommunication)

　(7)　電子メールアドレス (Electonic Mail Address)

　(8)　公開鍵と他の暗号化情報 (Public Keys and Encryption Information)

　(9)　チームメンバー (Team Members)

　(10)　業務時間 (Operating Hours)

(11)　他の情報 (Other Information)

(12)　顧客連絡先 (Points of Customer Contact)

**３　憲章 (Charter) 　６ページ**

　(1)　ミッションステートメント (Mission Statement)

　(2)　サービス対象者 (Constituency)

1. スポンサーシップと提携 (Sponsorship and/or Affiliation)
2. 権限 (Authority)

**４　ポリシー (Policies) 　７ページ**

　(1)　インシデントの種類とサポートレベル (Type of Incident and Level of Support)

　(2)　協力、相互活動及び情報の開示 (Co-operation, Interaction and Disclosure of Information)

　(3)　コミュニケーションと本人認証 (Communication and Authoentication)

**５　サービス (Serveices) 　８ページ**

　(1) インシデント対応 (Incident Response)

　　ア　インシデントトリアージ (Incident Triage)

　　イ　インシデントコーディネーション (Incident Coordination)

ウ　インシデント解決 (Incident Resolution)

　(2)　予防的活動 (Proactive Activities)

**６　インシデント報告フォーム (Incident Reporting Forms) 　９ページ**

**７　免責事項 (Disclaimers) 　９ページ**

|  |
| --- |
| **１　文書情報 (Document Information)** |
| **(1) 最終更新日 (Date of Last Update)** |
| * + *ポイント*
		- *この記述書が最新版であるかどうかを確認するために記述する。*
 |
|  |
| **(2) 通知の他の配布リスト (Distribution List for Notifications)** |
| * *ポイント*
	+ - *CSIRTの記述書の配布先のリストを記述する。*
		- *通常はCSIRTメーリングリスト等による配布が一般的であるが、その際はデジタル署名等をつける。*
 |
|  |
| **(3) 本文書の場所 (Locations where this Document May Be Found)** |
| * *ポイント*
	+ - *CSIRT記述書の入手先を明示するために記述する。*
 |
|  |
| **(4) 本書の検証 (Authenticating this Document)** |
| * *ポイント*
	+ - *CSIRT記述書をオンラインで公開する場合は、デジタル署名をつける。*
 |
|  |

|  |
| --- |
| **２　連絡先情報 (Contact Information)** |
| **(1)　チーム名 (Name of the Team)** |
| * *ポイント*
	+ - *略称と正式名称を記述する*
 |
|  |
| **(2)　所在地 (Address)** |
| * *ポイント*
	+ - *郵便物の送付、および、訪問する際に必要な情報を記述する*
 |
|  |
| **(3) 時間帯 (Time Zone)** |
| * *ポイント*
	+ - *CSIRTが主に活動するタイムゾーンを記述する*
		- *海外からの問い合わせが想定される場合は必須となる*
 |
|  |
| **(4) 電話番号 (Telephone Number)** |
| * *ポイント*
	+ - *CSIRT専用の電話番号ではない場合は、”XYZ-CSIRTと尋ねてください” のような記述を追加する*
 |
|  |
| **(5)　ファクシミリ番号 (Facsimile Number)** |
| * *ポイント*
	+ - *FAX による問い合わせが想定される場合に記述する*
		- *受信した情報がCSIRT以外の人の目に触れる可能性がある場合は、それができないような手段を講じるか、FAX 番号を公開しない*
 |
|  |
| **(6)　他の音声通信手段 (Other Telecommunication)** |
| * *ポイント*
	+ - *電話やFAX以外の連絡手段がある場合に記述する*
		- *特に、サービス対象者との特別な専用線等による電話番号等がある場合には記述する*
 |
|  |
| **(7)　電子メールアドレス (Electonic Mail Address)** |
| * *ポイント*
	+ - *CSIRTのメンバに直接届く代表アドレスを記述する*
 |
|  |
| **(8) 公開鍵と他の暗号化情報 (Public Keys and Encryption Information)** |
| * *ポイント*
	+ - *PGPの公開鍵の検証用の情報を記述する*
 |
|  |
| **(9) チームメンバー (Team Members)** |
| * *ポイント*
	+ - *CSIRTメンバの役職と氏名を記述する*
 |
|  |
| **(10) 業務時間 (Operating Hours)** |
| * *ポイント*
	+ - *インシデント対応が可能な時間帯を明示的に示しておくことにより、インシデント報告者のストレスを軽減させる*
		- *業務時間外の対応については、メールの自動応答や留守番電話等の対応を検討する*
 |
|  |
| **(11) 他の情報 (Other Information)** |
| * *ポイント*
	+ - *CSIRTに関する他の情報があれば、その情報、またはそれが存在する場所を記述する*
 |
|  |
| **(12)　顧客連絡先 (Points of Customer Contact)** |
| * *ポイント*
	+ - *サービス対象者や他組織のCSIRTチームからの連絡を受ける窓口情報を記述する*
 |
|  |

|  |
| --- |
| **３　憲章 (Charter)** |
| **(1)　ミッションステートメント (Mission Statement)** |
| * *ポイント*
	+ - *サービス対象者に対して、「大局的に何をする」のかを記述する*
		- *親組織のミッションに基づかなければならない、あるいは、その範囲内に解釈されるものでなければならないことがある*
		- *CSIRT設立目的を併記することが多い*
 |
|  |
| **(2)　サービス対象者 (Constituency)** |
| * *ポイント*
	+ - *CSIRTは「誰のために」あるいは「どの範囲に対して」活動をするのか*
		- *サービス対象者の定義とその関係を明示する*
		- *サービス対象者を定義しない場合、その理由を明確にする。例えば、顧客がサービス対象の場合は、顧客情報やサービス提供の内容を秘密にする場合がある*
		- *サービス対象者が、他組織によるサービス対象者と重複する場合があるが、その際は、サービス対象者に対する権限の違いを明確にする*
 |
|  |
| **(3) スポンサーシップと提携 (Sponsorship and/or Affiliation)** |
| * *ポイント*
	+ - *CSIRT活動に必要な資金を提供するスポンサーを明示する*
		- *このスポンサーシップの情報により、他のCSIRTとの提携の際に、他のチームから信頼を得るのに役立つ*
 |
|  |
| **(4) 権限 (Authority)** |
| * *ポイント*
	+ - *サービス対象者に対する権限を記述する*
		- *他のCSIRTによるサービス対象者と重複する場合は、それぞれのサービス対象者に対する権限を明確にするための記述をする*
 |
|  |

|  |
| --- |
| **４　ポリシー (Policies)** |
| **(1)　インシデントの種類とサポートレベル (Type of Incident and Level of Support)** |
| * *ポイント*
	+ - *CSIRTの対応可能なインシデントの種類と、各インシデントで対応できるレベルの一覧を記述する*
		- *CSIRTの対応レベルに違いがある理由や背景を記述する*
		- *将来、予想外のインシデントに対応するためのポリシーを記述する*
 |
|  |
| **(2)　協力、連携、情報開示 (Co-operation, Interaction and Disclosure of Information)** |
| * *ポイント*
	+ - *他の組織やコミュニティとの連携に関するポリシーを記述する*
		- *その組織から入手した情報の取り扱いに関するポリシーを記述する*
		- *統計情報に利用するなどの情報開示に関するポリシーを記述する*
 |
|  |
| **(3)　コミュニケーションと本人認証 (Communication and Authentication)** |
| * *ポイント*
	+ - *コミュニケーションをする際の情報の扱い方に関するポリシーを記述する*
		- *本人認証をするための手段を記述する*
 |
|  |
| **５　サービス (Serveices)** |
| **(1) インシデント対応 (Incident Response)** |
| * *ポイント*
	+ - *インシデント対応をどのようにするのかを記述する*
 |
|  |
| **(1)-a　インシデントトリアージ (Incident Triage)** |
| * *ポイント*
	+ - *インシデントの分類と対応の優先度、対応中の他のインシデントとの関連について記述する*
 |
|  |
| **(1)-b　インシデントコーディネーション (Incident Coordination)** |
| * *ポイント*
	+ - *協力組織への情報共有のポリシーを記述する*
 |
|  |
| **(1)-c　インシデント解決 (Incident Resolution)** |
| * *ポイント*
	+ - *技術的な支援、抑制措置、復旧等について記述する*
 |
|  |
| **(2)　予防的活動 (Proactive Activities)** |
| * *ポイント*
	+ - *サービス対象者に対する情報提供、セキュリティツールの使用、教育訓練、製品評価等について記述する*
 |
|  |

|  |
| --- |
| **６　インシデント報告フォーム (Incident Reporting Forms)** |
| * *ポイント*
	+ - *インシデント報告用のフォームについて記述する*
 |
|  |

|  |
| --- |
| **７　免責事項 (Disclaimers)** |
| * *ポイント*
	+ - *本記述書の利用にかかる免責事項を明示的に記述する*
 |
|  |