プロジェクト名 : 〇〇〇 CSIRT 構築プロジェクト

組織内 CSIRT 構築

CSIRT 記述書

（バージョン 1．0 2015 年 X 月 X 日）

担当部署	作成者
〇〇〇部 〇〇課	〇〇 〇〇

	〇〇課	〇〇課	〇〇課	
審議欄				

承認者

CSIRT 記述書（Description）

目　次

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。*

(例)
- ✧ バージョン 1.01（更新日 2007.11.01）

(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。*

(例)
- ✧ CSIRT 記述書が変更になった場合は、メーリングリスト（[*メーリングリストのアドレス*]）を受信しているところに配布されています。
- ✧ このメーリングリストを受信希望する場合は、[*メーリングリストのアドレス*] 宛てに、件名を “subscribe” にして送信し、その後受信されるメールの指示に従って登録してください。

(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。*

(例)
- ✧ 現在のバージョンの記述書は、以下の URL で公開されています。
  http://www. ○○○○.co.jp/csirt/CSIRT-descr.txt

(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。*

(例)
- ✧ 現在のバージョンの記述書は、○○○○-CSIRT の PGP キーで署名されています。その署名については、以下の URL で公開されています。
  http://www.○○○○.co.jp/csirt/CSIRT-descr.asc

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*

(例)

- 略称：〇〇〇〇-CSIRT
- 正式名称：〇〇〇〇 Computer Security Incident Response Team

(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*

(例)

- 〒〇〇〇-〇〇〇〇 東京都〇〇〇区〇〇〇１－２３－４　〇〇ビル５階
  〇〇〇〇株式会社　情報セキュリティ室内

(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*

(例)

- 東京／日本（GMT+0900）

(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*

(例)

- +81 03 1234 5678（"〇〇〇〇-CSIRT" と尋ねてください）

(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*

(例)

- +81 03 1234 5678

(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*

(例)

- 上記の電話及び FAX 以外の音声通信回線は用意されていません。

(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*

(例)

- *[CSIRT の代表メールアドレスを表示]*

(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*

(例)
- ✧ ○○○○-CSIRT の公開鍵に関する情報は以下の通りです。
  ・KeyID： 12345678
  ・Fingerprint： 11 22 33 44 55 66 77 88　88 77 66 55 44 33 22 11
- ✧ ○○○○-CSIRT の公開鍵は、一般の公開鍵サーバーにあるか、以下の URL にあります。
  http://www.○○○○.co.jp /csirt/CSIRT-pub.asc

(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*

(例)
- ✧ ○○○○-CSIRT の代表は、山田太郎です。
- ✧ 業務責任者は、鈴木花子です。
- ✧ その他のメンバについては、以下の URL で公開されています。
  http://www.○○○○.co.jp/csirt/teamlist.html

(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*

(例)
- ✧ 09:00 – 18:00（GMT +09:00）（土日祝日を除く、平日のみ）

(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*

(例)
- ✧ ○○○○-CSIRT に関する一般的な情報については、以下の URL にあります。
  http://www.○○○○.co.jp/csirt/index.html

(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*

(例)
- ✧ ○○○○-CSIRT に対する連絡は Email で、[*CSIRT の代表メールアドレス*] 宛てにお願いいたします。
- ✧ もし、Email を使用することができない場合は、電話で連絡をお願いいたします。ただし、業務時間内しかすぐに対応できません。また、業務時間外は、留守番機能による対応となりますが、その留守電の確認は、次の業務開始直前となっています。
- ✧ インシデント報告をされる場合は、この記述書内に定められている「インシデント報告フォーム」を使用してください。

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*

(例)

- 会社内及び子会社の従業員に対し、コンピュータセキュリティインシデントによる被害が軽減されるための環境及び仕組みの構築への支援をする。
- 会社内及び子会社の従業員に対し、インシデントが発生した場合の対応の支援をする。
- インターネットサービスを契約している顧客が、弊社インターネットサービスを起因とするインシデントに巻き込まれた場合、その被害の軽減と、迅速な復旧をする。

(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*

(例)

- 会社内及び子会社の従業員及び弊社インターネットサービスを契約している顧客

(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*

(例)

- ○○○○-CSIRT は ○○○○社の予算で活動しています。

(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

(例)

- ○○○○-CSIRT は、○○○○社の情報セキュリティ室の統制の中で活動します。
- ○○○○-CSIRT のメンバは、インシデント対応のためにシステム管理者及びネットワーク管理者と協力して活動を行います。
- ○○○○-CSIRT のメンバは、○○○○社のセキュリィポリシー委員会に所属し、社内セキュリティポリシーの策定に深く関わっています。

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*

(例)
- ✧ ○○○○-CSIRT で対応可能なインシデントの種類とその対応レベルは、以下の通りです。
  （省略）
- ✧ ユーザから直接報告を受け、直接サポートすることはありません。○○○○-CSIRT は、システム管理者、ネットワーク管理者、或いは、インシデントを直接対応する各部署に対してサポートをします。
- ✧ ○○○○-CSIRT は、○○○○社内でさまざまなインシデントの発生の未然防止の努力として、さまざまな技術情報や最新のセキュリティ動向に関する情報を提供していきます。

(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*

(例)
- ✧ 他社のインシデント対応チームとの連携に関するポリシーは、以下のとおり。
  （省略）
- ✧ JPCERT/CC との連携及び情報共有に関するポリシーは、以下のとおり。
  （省略）
- ✧ 警察機関への情報提供に関するポリシーは、以下のとおり。
  （省略）
- ✧ 報道機関に対するポリシーは、○○○○社の法務部門のポリシーを活用する。
- ✧ ○○○○-CSIRT で取り扱うすべての情報については、統計情報として定期的に開示する。

(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*

(例)
- ✧ 機微な情報を取り扱う場合は、PGP を使用すること。
- ✧ 外部に対してメールを送信する場合は、メールの本文の中に PGP キーのクリアテキスト署名をつけること。

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*

(例)
✧ ○○○○-CSIRT は、インシデント対応に必要な技術情報のハンドリングをすることにより、システム管理者のインシデント対応を支援します。

(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*

(例)
✧ 報告されたインシデントが本当に発生しているかどうかを調査します。
✧ インシデントの影響範囲を見積もります。

(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*

(例)
✧ インシデントの原因に基づき、関係するところに連絡をします。
✧ 必要により、法務部門を通じて警察に通知をします。
✧ 他の CSIRT に報告をします。
✧ 必要により、全ユーザに対する告知文を作成します。

(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*

(例)
✧ パッチの適用等により、脆弱性を取り除きます。
✧ 証拠の収集をします。

(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*

(例)
✧ 社内情報共有の仕組みを活用して、最新のセキュリティ動向及び関連する技術情報の提供をします。

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*

(例)

- ○○○○-CSIRT に対するインシデントの報告は、以下の URL にあるフォームを使用して報告してください。
  http://www.○○○○.co.jp/csirt/incident_reporting_form/

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*

(例)

- 本文書、または、本文書に含まれる情報を利用することで、直接・間接的に生じた損失に関し、○○○○-CSIRT は一切責任を負わないものとします。