

応: ~インシデントに対応する(発見と調整)~

インシデントレスポンス概論

JPCERT コーディネーションセンター

山賀正人

office@jpcert.or.jp

インシデントレスポンスとは

Computer Security Incident

(以降、インシデントと略)

- コンピュータセキュリティに関係する人為的事象で、意図的および偶発的なもの
- 弱点探索、リソースの不正使用、サービス運用妨害行為など
- 『不正アクセス (行為)』は狭義に規定された

インシデントの分類

米国Sandia National Laboratoriesの報告書

“A Common Language for Computer Security Incidents”

http://www.cert.org/research/taxonomy_988667.pdf



JPCERT/CC によるインシデントの分類

報告者の視点で分類

- サービス運用妨害 (DoS: Denial of Service)
 - 分散型サービス運用妨害 (DDoS: Distributed Denial of Service)
- 詐称 (電子メール)
- サービスの悪用、不正中継
- 侵入、無権限アクセス
- 弱点探索 (スキャン、プローブ)
 - 「未遂」に終わったものを含む
- その他 (JPCERT/CC で扱えないものなど)

守るだけがセキュリティではない。

- 人為的ミス (パッチの適用忘れなど)
- 未知 (公知になっていない) の脆弱性の悪用
- パッチの提供が間に合わない

「100% 安全」はありえない。

いかに素早くインシデントに気づき、
対応できるか、が重要

インシデントレスポンスとは

- 「インシデントは起こる」という前提に基づいた「**事後の対応**」
- 未然に防ぐための「事前の対応」も含まれる



インシデントを発見する手順の明確化

- ログの取得内容の事前の整理、ログの確認
- 不審なプロセス、通信の検知
- 改ざんの検知 (完全性の確認)
- 異常事態発生時の報告の仕組みなど

外部からの通知連絡で気が付くケースもある

それは本当にインシデント？

- 操作ミス、設定ミス？
- 連絡ミス？
- ident (113/tcp) のように、こちらからのアクセスに伴う外部からの「正規の」アクセス？

まずは**落ち着いて**冷静に確認、判断

万が一の事態(インシデント)が 起こった後の対応手順

技術メモ - コンピュータセキュリティインシデントへの対応

<http://www.jpccert.or.jp/ed/2002/ed020002.txt>

手順1

- 手順の確認
 - セキュリティポリシー、作業マニュアル
- 作業記録の作成
- 責任者、担当者への連絡
 - 連絡体制の整備
 - インシデント対応の担当者への連絡



手順2

- 事実の確認
 - 本当にインシデントなのか?
- スナップショットの保存
 - 後の調査、分析
- ネットワーク接続やシステムの遮断もしくは停止
 - 意思決定プロセスや判断基準の事前の整理
 - 具体的な作業手順の明確化



手順3

- 影響範囲の特定
 - － 漏洩した情報の機密性の度合い
 - － 踏み台として、いつ、どこを攻撃してしまったか？
- 渉外、関係サイトへの連絡
 - － サイト内外への謝罪、情報提供
 - － アクセス元などへの通知連絡
 - 技術メモ - 関係サイトとの情報交換
 - <http://www.jpccert.or.jp/ed/2002/ed020001.txt>

手順4

- 要因の特定
 - どの脆弱性が悪用されたのか？
- システムの復旧
 - バックアップメディアからの復旧
- 再発防止策の検討、実施



手順5

- 監視体制の強化
- 作業結果の報告
- 作業の評価、ポリシー・運用体制・運用手順の見直し
- JPCERT/CC などへ報告



ポリシーの策定

- あなたの組織にとって、何が一番大切なのですか？
- 何を守りたいのですか？
- 何を優先すべきなのですか？
- 想定されるダメージは？
- あなたの組織にとっての「インシデント」とは？

OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation

<http://www.cert.org/octave/>

参考文献

- 管理者のためのセキュリティ推進室

インシデントレスポンス入門

<http://www.jpccert.or.jp/magazine/atmarkit/>



インシデントレスポンスに必要なもの

- 専門のチーム (CSIRT)
 - 普段から予行演習などを行なっておく
 - 想定されるインシデントのそれぞれについて対応手順を整備
 - 想定外のインシデントへの柔軟な対応
- 冷静さ
 - 落ち着いて行動

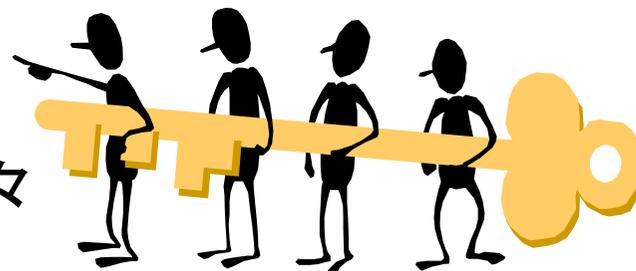


CSIRTとは

(Computer Security Incident Response Team)

CSIRTの歴史

- 1988年11年「Morris worm 事件」
- 米国カーネギーメロン大学の CERT/CC (Computer Emergency Response Team Coordination Center)
 - CERT という単語は CERT/CC の登録商標
- 現在では世界中に多数の組織
 - CERTCC-KR (韓国)
 - AusCERT (オーストラリア)
 - CERT-Renater (フランス)
-
- 組織によって形態・対応内容は様々
- RFC 2350 参照



CSIRT の分類

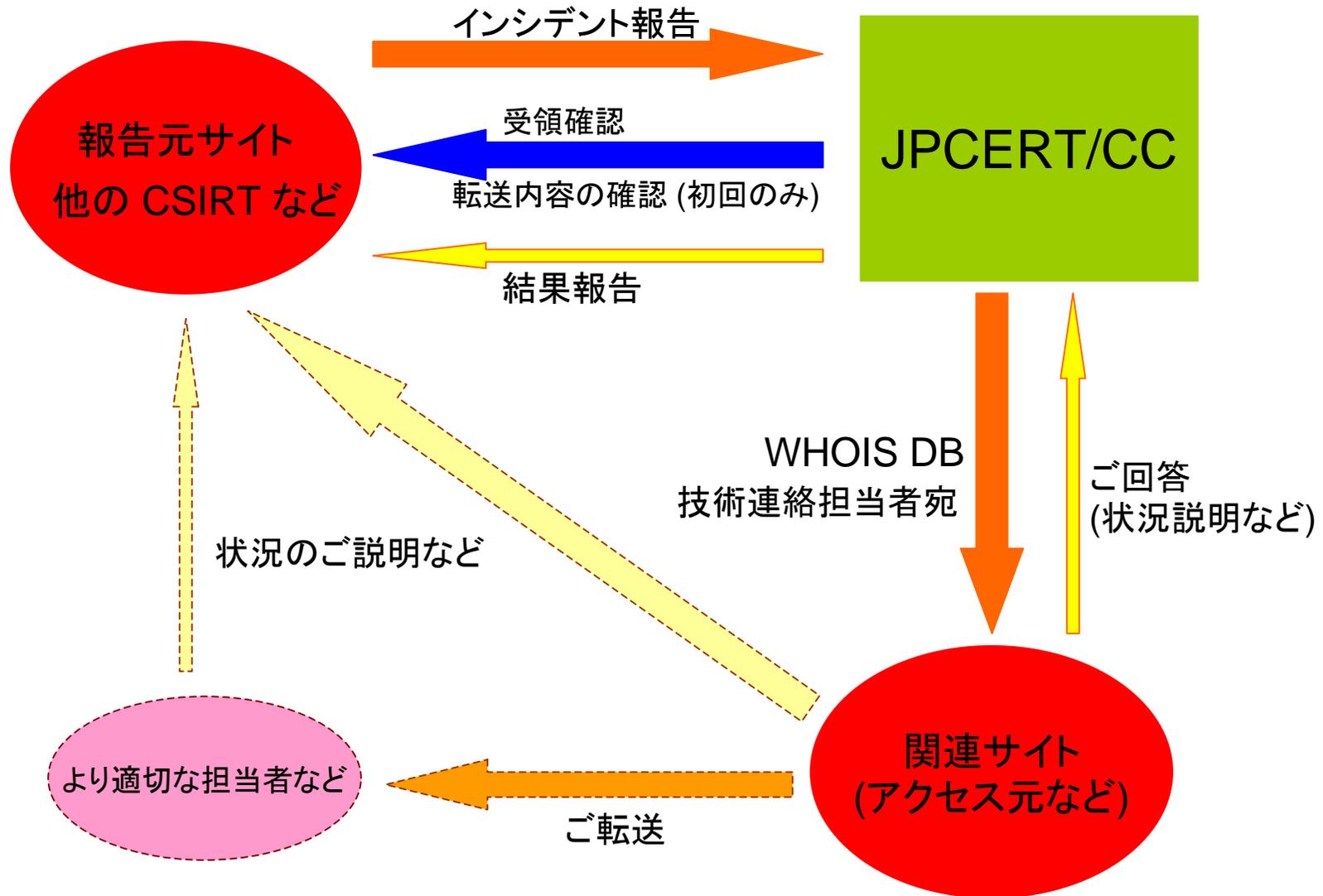
http://www.cert.org/csirts/csirt_faq.html

- constituencyと呼ばれるサービス対象によって分類
 - Internal CSIRTs
 - 自組織や顧客が関わるインシデントに対応
 - National CSIRTs
 - national = 地域のコンタクトポイント
 - Coordination Centers
 - Analysis Centers
 - Vendor Teams
 - 自社製品の脆弱性について対応
 - Incident Response Providers
 - いわゆる「セキュリティベンダ」

xSPとの連携

- xSP の顧客対応窓口は最も「ユーザ」に近いところにいる CSIRT の 1つである。
 - 「踏み台」にされている可能性のあるユーザへの速やかかつ効率的な通知連絡
 - (可能であれば) 必要に応じて対応のアドバイス
 - 技術的、非技術的
 - ポインタを示すだけでもかなりの効果





ベンダとの連携

- 脆弱性情報についての問合せ窓口の設置
 - 「発見者」とベンダとの間のコーディネーション
- 対応内容 (パッチ情報など) の確認
 - JVN (JP Vendor Status Notes)
<http://jvn.jp/>
 - 2004年7月より本運用開始



付録

JPCERT/CC 発行の技術メモ

<http://www.jpccert.or.jp/ed/>

コンピュータセキュリティインシデントに対する
一般的な対応方法についての説明

サイトごとのポリシー策定などの参考に

JPCERT/CC へのアクセス

-  E-mail: info@jpcert.or.jp
-  Web: <http://www.jpcert.or.jp/>
- 報告様式: <http://www.jpcert.or.jp/form/>
- メーリングリスト: <http://www.jpcert.or.jp/announce.html>
-  ファックス: 03-3518-2177

※ 電話によるインシデント報告は受け付けておりません。

PGP Fingerprint: BA F4 D9 FA B8 FB F0 73 57 EE 3C 2B 13 F0 48 B8