Carnegie Mellon
Software Engineering Institute

JPCERT CC Japan Computer Emergency Response Team Coordination Center

CERT Coordination Center 15 Years of Service 1988 - 2003

CERT/CC、JPCERT/CC
脆弱性情報ハンドリング

伊藤友里恵
JPCERT/CC

ショーン・ハナン
CERT/CC

CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

CERT Coordination Center 15 Years of Service 1988 - 2003

脆弱性情報ハンドリングプロセス

脆弱性情報ハンドリングとは、ソフトウェアシステムのセキュリティ上の欠陥に関する情報を必要に応じて公開することにより、悪用のおそれ、または障害を引き起こす危険性を最小限に食い止めるプロセスである。

JPCERT CC

脆弱性とは?

脆弱性の定義は、人によってまちまち
CERT/CCとJPCERT/CCは、下記の認識を共有
- 明白、または暗示的なセキュリティポリシーの違反
- 通常ソフトウェアの欠陥によって引き起こされる
- 同種の欠陥は同じ脆弱性情報とする(例:SNMPは2つの脆弱性と理解)
- 頻繁に予期しない挙動を引き起こす

明確に脆弱性から除外するもの
- トロイの木馬 (悪意のある添付つきメール)
- ウィルス、ワーム (自己増殖型コード)
- 侵入ツール (スキャナ、rootkit等)

- 脆弱性とは、技術的欠陥で、上記の事象を存在させるもの

JPCERT CC

脆弱性の定義はなぜ必要か?

ポリシーの問題
- 情報公開
- 修正
- 責任、義務
- 意思決定者が、エキスパートの主観的意見に左右される

分析的問題
- 定義のないものを原因として分析することが困難
- 特性を明確に説明することが困難

- 自動化した情報交換がほとんど機能しない。

JPCERT CC

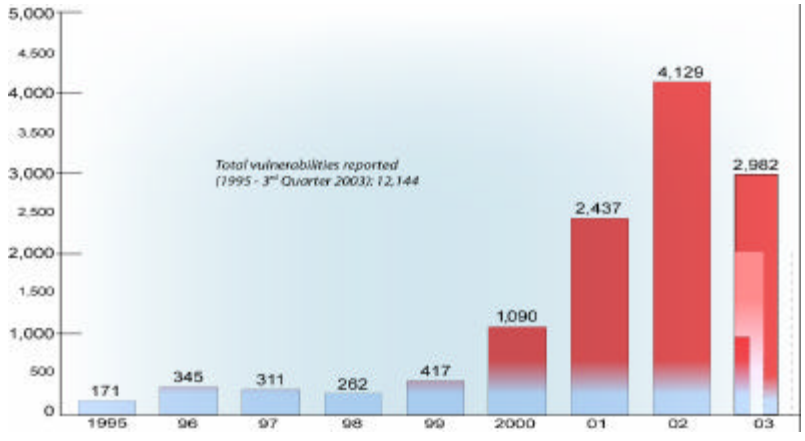
プロセス指向

脆弱性情報は、再現可能な方法でハンドリングされる

- 事前評価
- 通知
- リサーチ
- コーディネーション
- 公開
- フォローアップ

JPCERT CC

CERT/CCに報告された脆弱性情報数推移



潜在的な危険を減らす

ベンダは、パッチを開発するために、事前に問題を認知するべき

- CERT/CCは、ベンダデータベースに600以上のコンタクトを所有
- 情報漏洩の危険なく、受信者個別のセキュアな情報交換方法に対応するツールを使用
- 情報公開のコーディネート:誰も単独ベンダーシステムだけを使用しているわけでない。

技術エキスパートとの協力

- セキュリティエキスパートは、製品エキスパートと同一でない。

JPCERT CC

影響を最小限化する

全ての危険性が同じレベルではない。

重要インフラサイトには、事前に通知

- 厳重に
- 状況を鑑みて慎重に
- 適切な場合、秘密保持契約のもと

最終的な一般公開通知へのフィードバック

JPCERT CC

情報公開

汎用目的のソフトウェアの脆弱性は公開される必要がある。

- 悪意のある者が、未公開の脆弱性情報を発見して、その情報を危険性を高める方法で公開するケースを防ぐ
- 管理者に、パッチの適用を動機付けさせる。
- 全ての安全性の懸念を認識しきれない。
- ベンダ、研究者、関係者と調整し、対応可能なスケジューリングを行う。

JPCERT CC

脆弱性に関連する情報

一般にも、脆弱性に関する正確、かつ客観的な情報が必要

- 影響
- 前提条件
- 修正

バグ情報自体へのアクセスが有意義な関係者は、限られている。

JPCERT CC

ベンダとのやり取り (CERT/CC)

多数のハード、ソフトウェアベンダと強い信頼関係を築いている。

各ベンダ内のキーパーソンのコンタクト情報(自宅電話番号含む)を所有、各社内の脆弱性情報対応手続きの作成を支援。

多くの場合、脆弱性を修正するのに最適な方法と、それによって引き起こされる全ての派生的な影響についてまで、ベンダとの情報交換を行う。

往々にして、企業内の取締役クラスの担当者より、その企業内でどの部署がどんな問題を修正できるかについて、把握している場合もある。

ベンダとのやり取り-2 (CERT/CC)

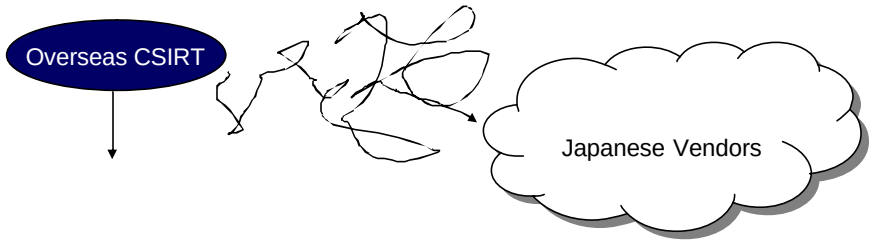
ソフトウェア、ハードウェアベンダのセキュリティ担当者のデータベースを管理

- アウトバンド認証を利用して本人認証
- サポートできる全ての担当者と安全なコミュニケーションチャネルを使用
- 各コンタクト別にカスタマイズした通知を送れるツールを使用(srmail)
  - 最も一般的な暗号化技術を使用、コンタクト先の鍵で暗号化
  - 各メッセージは宛先別にサイン
  - 他に誰が同じ連絡を受けているかコンタクト先情報が漏洩される恐れがない。
- このデータベースに、800以上のコンタクトを管理、内600以上がハードウェア、ソフトウェアベンダ

(CERT/CCは外部使用目的の暗号化メールの世界最大ユーザだろう。)

海外から日本国内への脆弱性情報流通の難点

JPCERT CC



-どのベンダが、影響のある製品を扱っているかどうやって選抜?
-組織内での正しいコンタクトポイントは?
-信頼できるコンタクトポイントをメンテナンスするには?
-安全に情報をハンドリングするためには?
-情報漏れを防止する方法?
-言葉や、文化の違いをカバーするリソースの確保?
-信頼関係の構築?

ベンダとのやり取り (JPCERT/CC)

JPCERT CC

- ハードウェア、ソフトウェア、ルータ、ファックスコピー、機器メーカが多数日本に存在
- これらの日本のベンダについて、脆弱性情報が一般公開される前に、影響のある製品への対応を行うことは重要。
- ベンダの脆弱性ハンドリングの方針やルールをサポートする必要あり。
- JPCERT/CCは、CSIRTのコミュニティ内で、日本への情報発信のコンタクトポイントとなるコーディネーションセンタとして活動。脆弱性情報のコーディネーションを行っている。
- 日本国内で、ベンダとの強い信頼関係を構築している。

ベンダとのやり取り2 (JPCERT/CC)

JPCERT CC

- JVN (JPCERT/CC Vendor Status Notes)
- 2003年より、日本国内で利用されているソフトウェアや装置を対象とした、国内の各ベンダが提供する対策情報や更新情報を主体にまとめているサイトを運営支援。
- 慶應義塾大学土居・高田研究室を中心に JVN ワーキンググループを構成して活動
  - Vendors listed;

Apple Computer, Cisco Systems, Debian GNU/Linux,
The FreeBSD Project, Fujitsu, HP Japan, Hitachi, NEC, IIJ,
Internet Security Systems K.K., LAC, Microsoft KK,
Miracle Linux, Net BSD Project, Open BSD Project,
Oracle Japan, Red Hat, Japan SCO, Japan SGI,
Sun Micro Systems, Turbo Linux, Project Vine

CERT Coordination Center 15 Years of Service 1988 - 2003

CERT/CC & JPCERT/CC
脆弱性情報コーディネーション

JPCERT CC

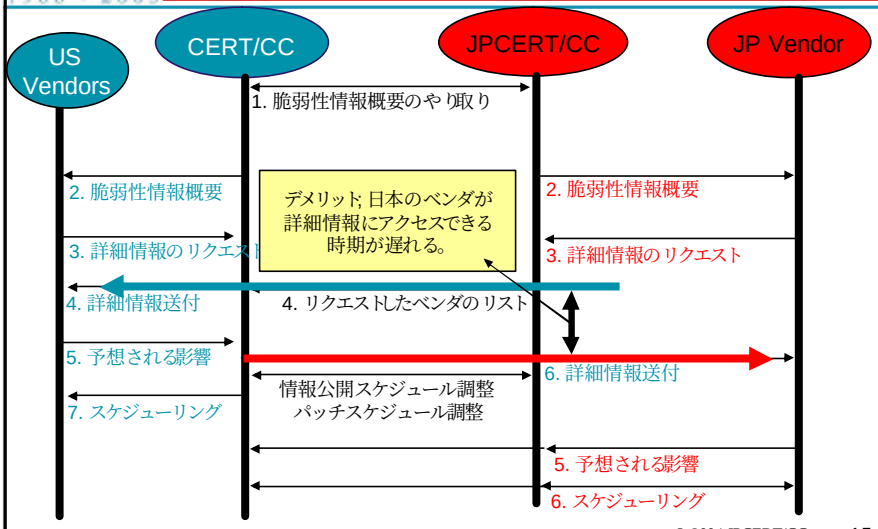
CERT/CC と JPCERT/CC の脆弱性情報ハンドリングは; アメリカ、インターナショナルベンダーと、日本のベンダーが、脆弱性情報へのアクセス、その修正を、同じタイミングで行える機会を持つためのコーディネーション。

* このコーディネーションは、日本のベンダが、CERT/CCに直接コンタクトすることを妨げるものではありません。

プロセスモデル 1

JPCERT/CCがベンダのコンタクト情報だけをコーディネートして、ベンダがリクエストしたときにハンドリングをサポートするモデル

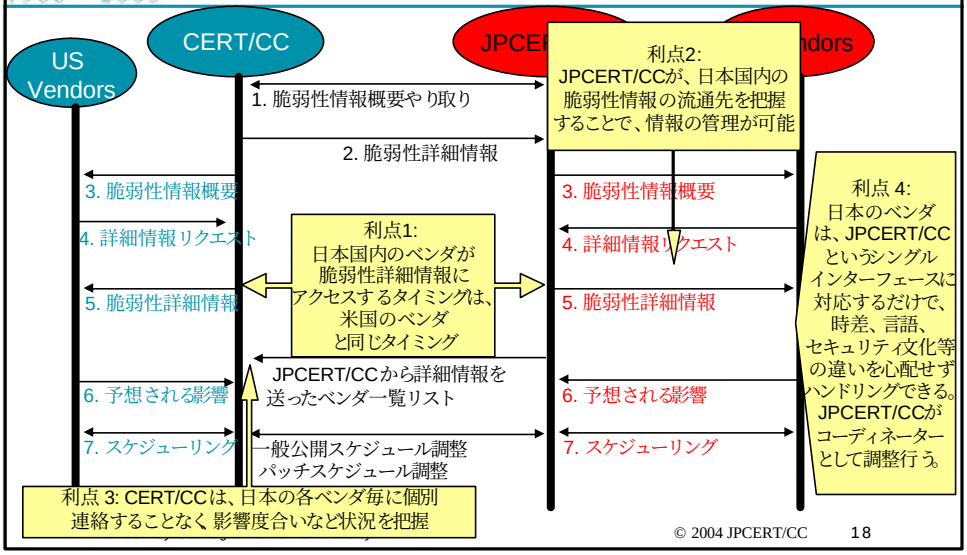
JPCERT CC



プロセスモデル 2

JPCERT/CCが詳細情報をベンダにコーディネーション する

JPCERT CC



組織内脆弱性対応チーム

JPCERT CC

- ベンダ組織内脆弱性ハンドリングチームは、下記分野別スペシャリストのグループで構成が理想的

- 品質管理部門
  - 組織内のコンタクトポイントとして、脆弱性情報を受付、組織内の適切な担当者へ対応をコーディネートする
  - CSIRTと密に連絡を取りながら、関連するドキュメント、パッチ、ワークアラウンドの発表時期のコーディネーション を行う
- 製品開発者
  - 製品の脆弱性の影響を調査、確認する
  - パッチ、修正プログラム、ワークアラウンドを作成
- 法務、広報担当者
  - アドバイザリ、アラートなどの作成
- 製品デリバラー
  - パッチや、修正プログラム、ワークアラウンドの適応によって派生する問題に対応

問題を元から絶つ

- 多くの脆弱性は、繰り返し発生する少数の不注意なエラーが原因。

- システム管理者は、パッチやアップデートが多すぎて対応しきれていない。

- パッチは、取り扱いに注意が必要なので、大規模サイトでは、パッチの適用までに数週間ものテストが要求される。ー 処置策は、大抵実際の病気より悪。

- ソフトウェアが広く実装される以前に、ソフトウェア製造段階における問題を元から修正することが不可欠。

JPCERT CC

人工に換算すると

2003年に5500件の脆弱性が報告されたこととは?
- 誰かが脆弱性の内容を読む必要あり
  - 5500×読解20分=229日(脆弱性情報を読むだけに費やす)
- その内10%の脆弱性に影響を受けているとすると
  - 550脆弱性×パッチのインストールに1時間=一台のマシンにパッチをあてるだけで69日
- セキュリティニュースを読んで、マシン一台にパッチをあてるだけで229+69=298日間

- セキュリティ速報を5分だけ読んで、ヒット確率を1%とすると、ほとんど65日間のコスト、または、非常に有能な管理者の25%のコストをかけることになる。

JPCERT CC

原因の理解

•全体の約75%の脆弱性は、最もよく起こる原因トップ10に起因している。

•問題が非常にディテールなレベルで発生することがよく知られている。

•SEIのソフトウェアプロセスグループと協力して、このような問題を回避するためのソフトウェアエンジニアリング技術の開発にも注力している。

JPCERT CC

まとめ

ソフトウェアやハードウェアには、多くのセキュリティ問題が存在していると認識すべきである。

問題がない完全なソフトウェアだとユーザーに思わせるより、ユーザーには、脆弱性情報を正しいプロセスで公開し、対策情報を的確に配布するほうが有益。

CERT/CCとJPCERT/CCは、脆弱性情報のコーディネーションを通し、問題の解決と、ベンダの最適な脆弱性情報の公開をサポートします。

CERT/CCとJPCERT/CCは、新たなパートナーシップを構築し、日本のベンダが、脆弱性情報に事前にアクセスし、安全にそれに対応し、対策情報をワールドワイドに公開するのをサポートします。

Questions and Answers

JPCERT CC