情報セキュリティに関する脅威の最新動向と対策状況

セキュリティ・ソリューション・フォーラム

平成19年10月26日

JPCERTコーディネーションセンター

常務理事 早貸 淳子

JPCERT CC®

1. JPCERT/CCとは

1．JPCERT/CC　概要

【名称】 有限責任中間法人　JPCERTコーディネーションセンター
（Japan Computer Emergency Response Team Coordination Center）

【ミッション】

国境を越えて広がるセキュリティインシデントに対応するため、国内全域をサービス対象とする CSIRT (**Computer Security Incident Response Team**) ※として、わが国における情報セキュリティ対策活動の向上を図る。

※CSIRT（シーサート）とは

- Computer Security Incident Response Team
- 起源と概要：
  - 1988年11月に不正プログラム(the Morris worm)の蔓延によりインターネットの利用が困難となる重大なインシデントが発生したことをきっかけに、インシデント発生から20日後、DARPAによって、Carnegie Mellon University の Software Engineering Institute(CMU/SEI)に“CERT/CC”設立。
  - サービス対象、サービス内容には様々なバリエーションがある。

- CSIRTの代表的な機能
  - インシデントハンドリング
  - 注意喚起、勧告、などのセキュリティ関連情報の提供
  - 適切な情報流通コミュニケーションチャネルの構築
  - 脆弱性ハンドリング

活動の概要

インシデント予防

脆弱性情報ハンドリング

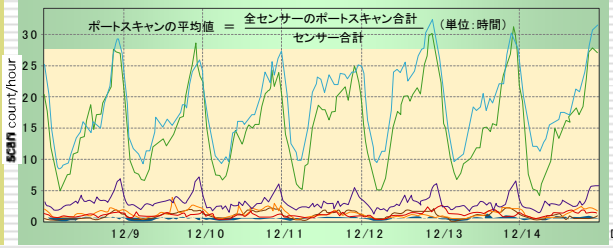
未公開の脆弱性関連情報を
製品開発者へ提供し対応依頼
国際的に情報公開日を調整

JVN Japan Vulnerability Notes

インシデントの予測と捕捉

定点観測（ISDAS）

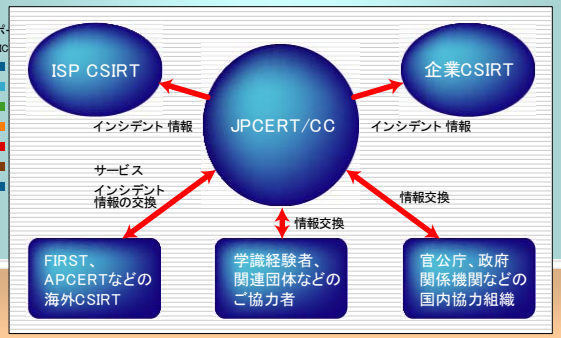
ネットワークトラフィック情報
の収集分析
定期的なセキュリティ予防情
報の提供



発生したインシデントへの対応

インシデントハンドリング

インシデントレスポンスの時間短
縮による被害最小化
再発防止に向けた関係各関の
情報交換および情報共有



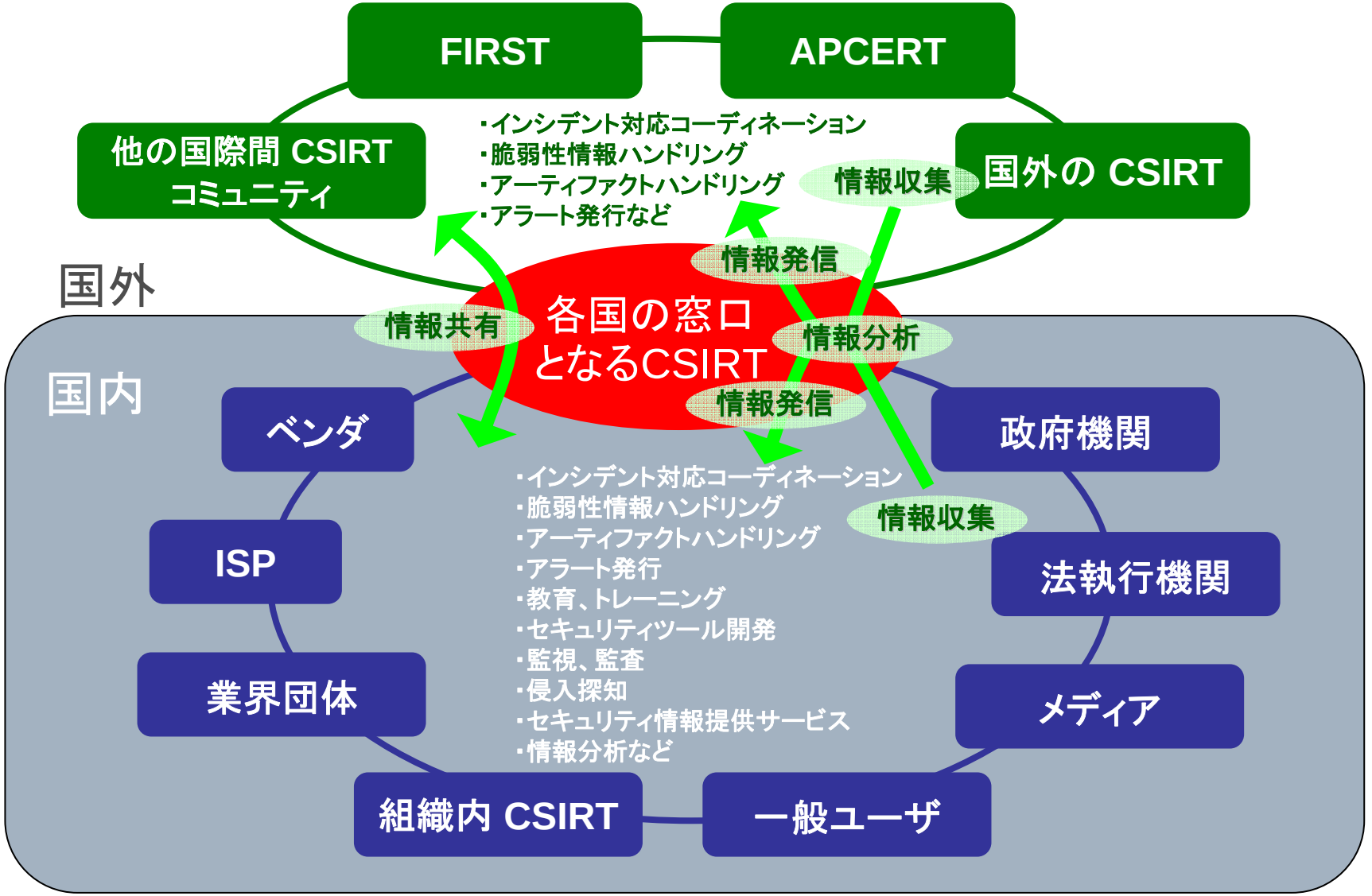
早期警戒情報

重要インフラ事業者等の特定組織向け情報発信

CSIRT構築支援

企業内のセキュリティ対応組織の構築支援

各国の窓口となる CSIRT の主な業務内容



JPCERT CC®

2. 情報セキュリティに関する脅威の現状

最近、耳にする脅威の例――

- ゼロデー攻撃
- 増え続ける脆弱性
  – 2006'の報告数8,046
  (CMU－CERT/CC統計情報)
- クライアントアプリケーションを
  対象とした攻撃
- 標的型攻撃
- マルウエアが埋め込まれた
  ウェブサイトへの誘導・ダウンロード
- ソーシャルエンジニアリング手法
  の高度化
- ボットネットの問題は
  よりいっそう深刻に
- 制御、コントロールシステム
  (SCADA) への注目
- DNSサーバーのようなインターネット
  インフラ自体への攻撃
- 国内ブランドのフィッシングサイト
- 初歩的な攻撃手法も引き続き発生
  ―辞書攻撃、パスワード攻撃
- P2Pファイル共有ソフトネットワークにおける
  情報漏えいは引き続き深刻

ちょっと異なる問題を感じさせるものですが、“Julie Amero” 事件から

- 2007年1月5日、米国コネチカット州の中学の代用教員（Julie Amero）が、未成年者に対する4つの傷害罪に問われ、最長40年の禁固刑を言い渡す有罪判決を受けた。
  →現在、再審請求が認められ、審理継続中。

- 容疑事実：授業中に、PCにわいせつな画像を掲出させ、意図的に生徒に見せたとされたもの

- 専門家たちは、ログの分析により、当該授業に使われていたPCがマルウエア対策やFWの導入等の対策がとられていなかったために、マルウエアに感染し、ハイジャックされて強制的にわいせつ画像のついたポップアップ広告が次々と表示されたものであると主張

最近のセキュリティインシデントの動向（1）

- 経済的な利益を目的とする攻撃が**組織化・高度化**
  - 価値のある情報資産（情報そのもの、機器等のリソース）を狙い撃ちにする標的型攻撃（ターゲテッド・アタック）
  - 特定の地域、特定の組織で多く使われているアプリケーションの脆弱性をターゲットとした攻撃
  - 多目的に利用できるように構築されたボットネットワークの利用
  - インターネットにつながってサービスを提供するものは全て、踏み台化され、サイバー犯罪や攻撃のインフラとして使われる可能性がある
  - 経済的な利益を得ようとする者に対して攻撃ツールを提供すること自体がビジネスに（分業化・専門化・組織化）

最近のセキュリティインシデントの動向(2)

- 脅威の潜在化
  - 攻撃・被害が認識されにくい方法を用いて行われている傾向
    - 例:ソーシャルエンジニアリングを使ったメール添付型
    - Root-kit,プロセスを表示させない不正プログラム
- 本格的な実用段階に入った巧妙なマルウエア
  - 堅牢な分散システム
    - 暗号化・難読化による安全(?)性
      - APIを直接呼ばずに専用の関数を実装、URL等のハードコードされる文字列
    - 冗長化による高可用性
    - ダウンローダー
  - パッキング
    - 自己解凍実行形式、ほとんどのマルウェアが何らかの形でパッキング、複数のパッキングを使っているマルウェアも

最近のセキュリティインシデントの動向（3）

- “Anti-”技術
  - デバッガ・仮想化環境
    ～デバッガや仮想化環境を検知して挙動を変える～
    - IsDebuggerPresent(), 割り込み, …
    - デバイス名, ホスト・ゲスト間の通信インターフェイス, …
  - アンチウイルス
    - アンチウイルスソフトのプロセスを停止
    - アンチウイルスベンダのサーバへのアクセスを妨害
- OSS的な開発手法
  - 無数の亜種が発生
  - 標的型攻撃(Targeted Attack)の温床
- ビジネス化
  - 成果だけでなく機能として売買される
  - 「潜む」ことで安定的に継続稼動

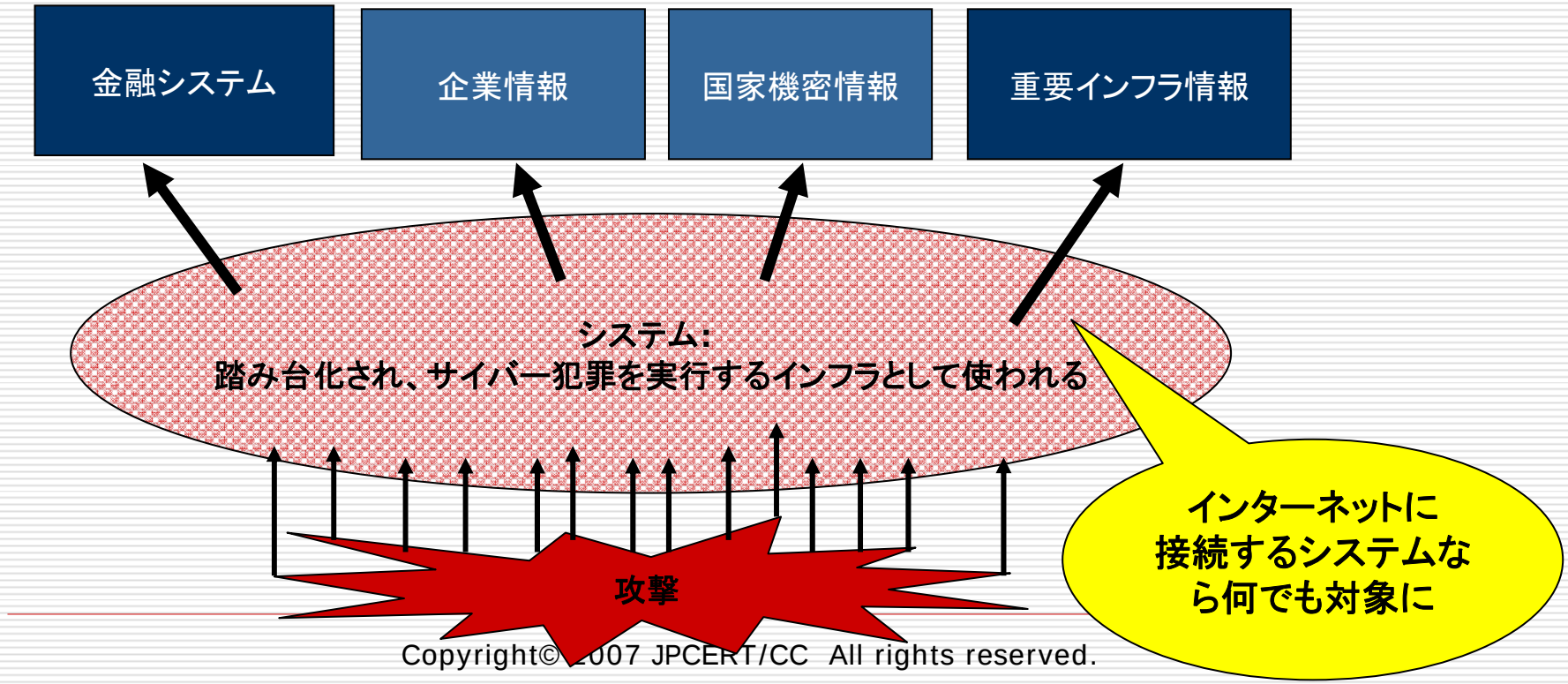
脅威の背景

- 攻撃コストも処罰(逮捕)されるリスクも高くない一方で、ネットワーク上には、お金になるデータ、リソースが溢れている。
  - 攻撃技術の高度化、専門化
  - 攻撃者のシンジケート化
  - 管理の甘い多数のコンピュータの存在

- 対策のインセンティブとして働かない市場、社会制度

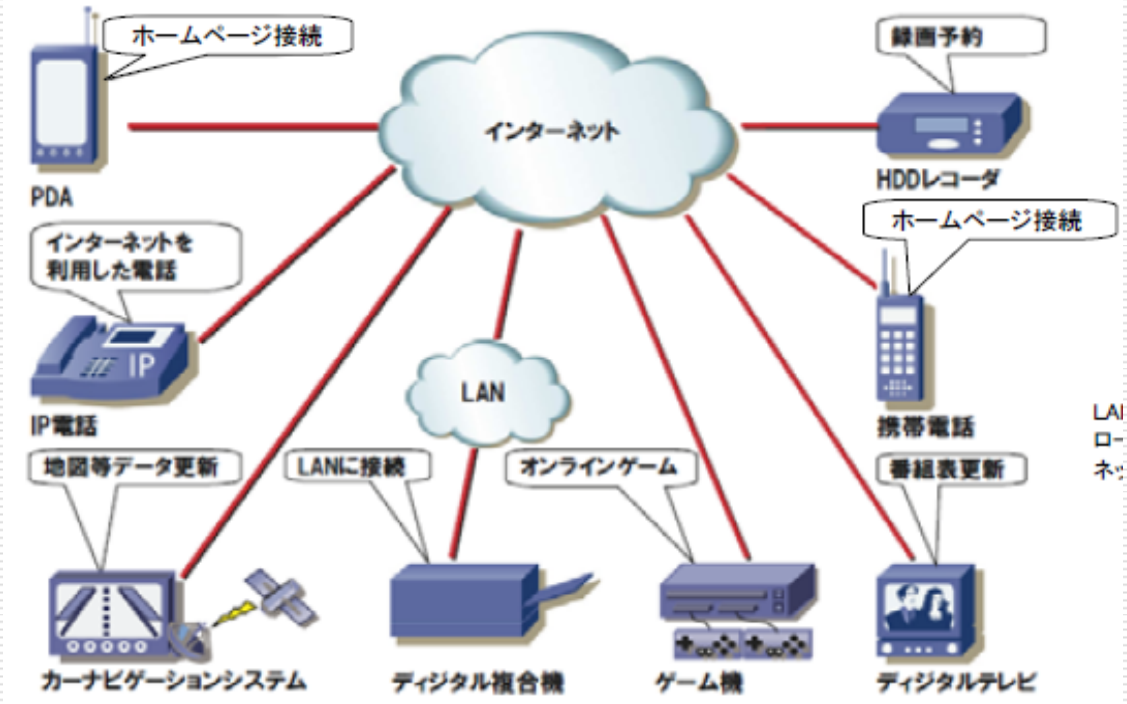
A. 手段を選ばない攻撃の手段：踏み台

セキュアに守られている標的システムに対して直接攻撃をかけるよりも、そのシステムにアクセスできるユーザーシステムに侵入し、踏み台にして標的にしているシステムへの攻撃をかける。



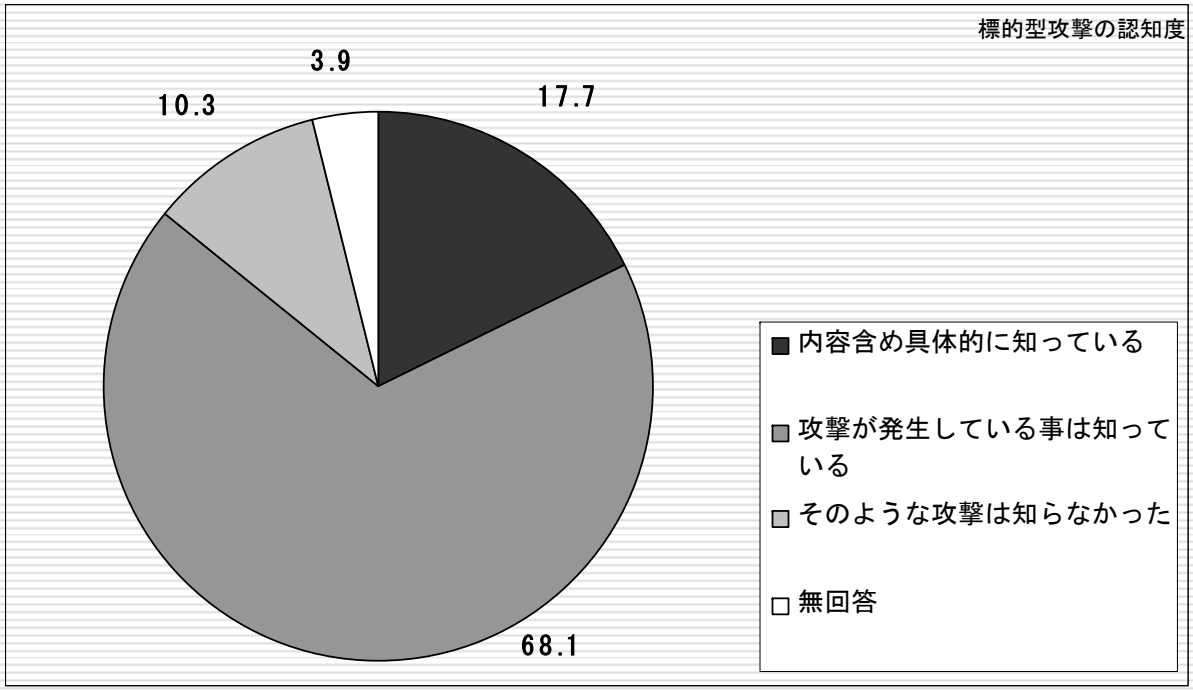
インターネットにつながるものは すべて踏み台にすべく、攻撃対象になる

- 情報家電は24時間ネットワークに接続される時代。



独立行政法人　情報処理推進機構 「組込みソフトウェアを用いた機器におけるセキュリティ」より

B. 標的型攻撃
JPCERT/CCが実施したアンケート調査

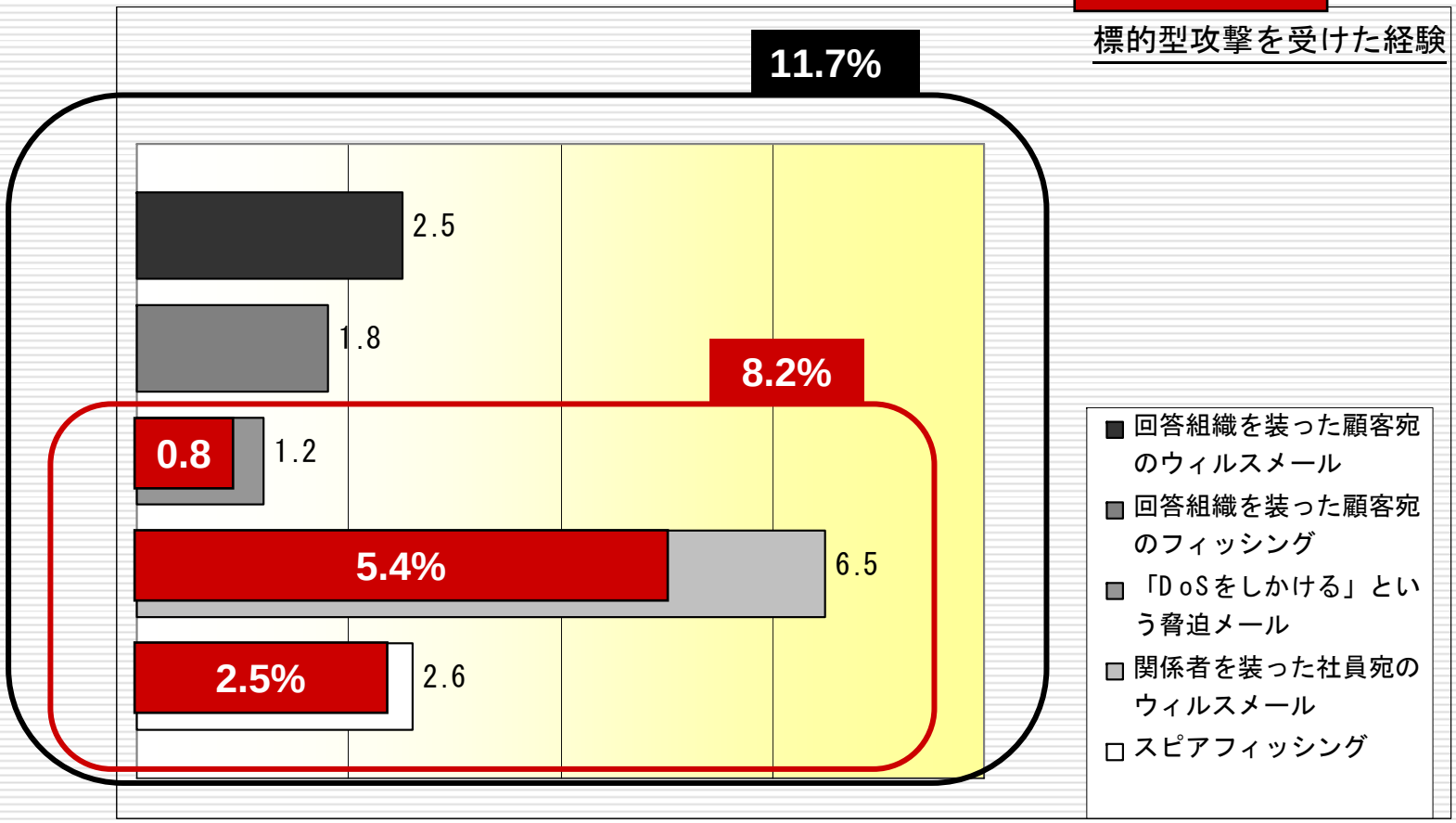


- 調査時期: 2007年3月2日から23日
- 送付先: 企業(東証一部・二部上場企業、店頭公開企業)、電気通信事業者、医療関連、教育関連、行政サービス(市町村役所)。
- 宛名は「情報セキュリティ担当者様」として合計2000社に送付。
- 回答数: 282 (回答率14.1%)

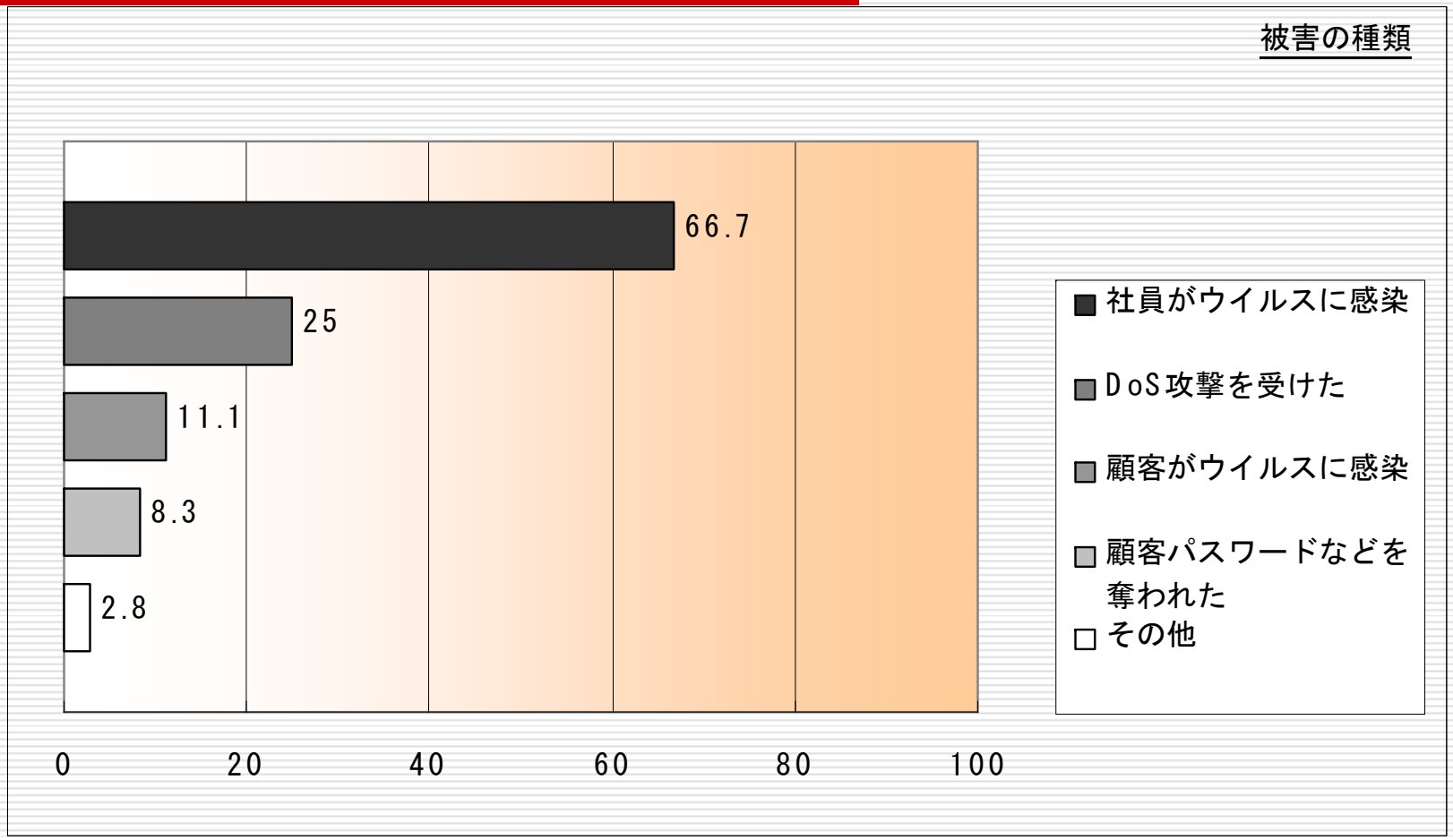
【攻撃の実態】

過去1年間に

標的型攻撃を受けた経験



【どんな被害が発生しているか】



【誰が攻撃を行っているのか】

特定できなかった	63.9%
その他、社外の人物	19.4%
特定しようとしなかった	5.6%
社員、あるいは契約社員	5.6%
取引先	2.8%
その他	2.8%
元社員、あるいは元契約社員	0%

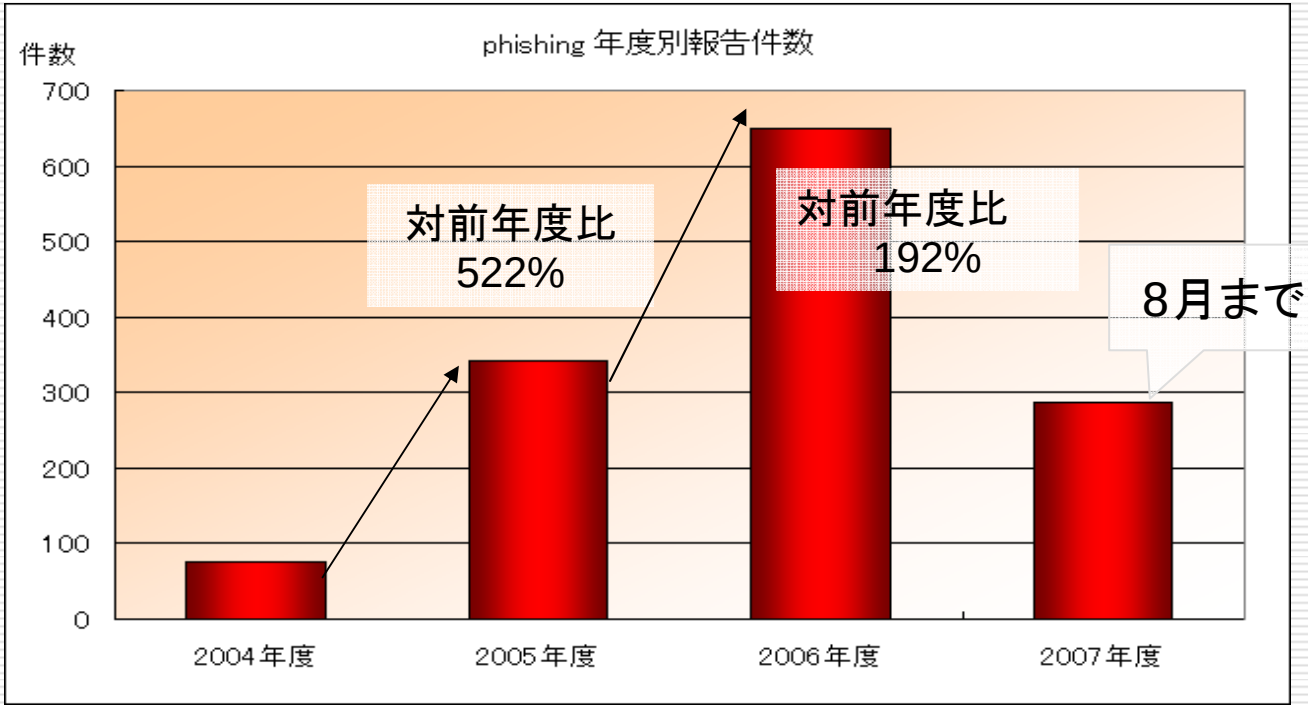
- 過半数のケースで攻撃者の特定に至っていない
- 社員という回答が5.6%ある

【インターネットだけが危ないのか】

- アンケート調査で標的型攻撃を受けたと回答した企業のうち約4割は、施設への物理的侵入、窃盗、廃棄物からの情報持ち出しなどの被害を経験している。

- **金融**
  - 回答事業者の14.3%が「関係者を装っての情報詐取」被害を経験しており、4.8%が「廃棄物からの情報持ち出し」被害を経験している。

C. フィッシングの動向
報告件数(年度別)



国内金融機関のフィッシングサイトの増加

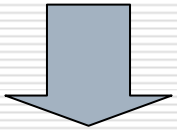
※国内金融機関を装ったフィッシングサイトに関する注意喚起(2007-04-03)
http://www.jpcert.or.jp/at/2007/at070009.txt

フィッシング被害サイト(種別件数)

被害サイト	2004年度	2005年度	2006年度
ISP・xSP	40	110	362
企業	25	158	231
学校	2	22	17
海外サイト	3	38	23
不明	5	11	17

フィッシングサイト公開ホストの傾向

- パスワードを破られ侵入
  - sshのみで遠隔からのログインが可能、かつ脆弱なパスワード
- 脆弱性をつかれ侵入
  - 長期間放置されたテストサーバ



フィッシングサイト公開は、侵入被害の延長
（情報漏えい、不正行為への加担）

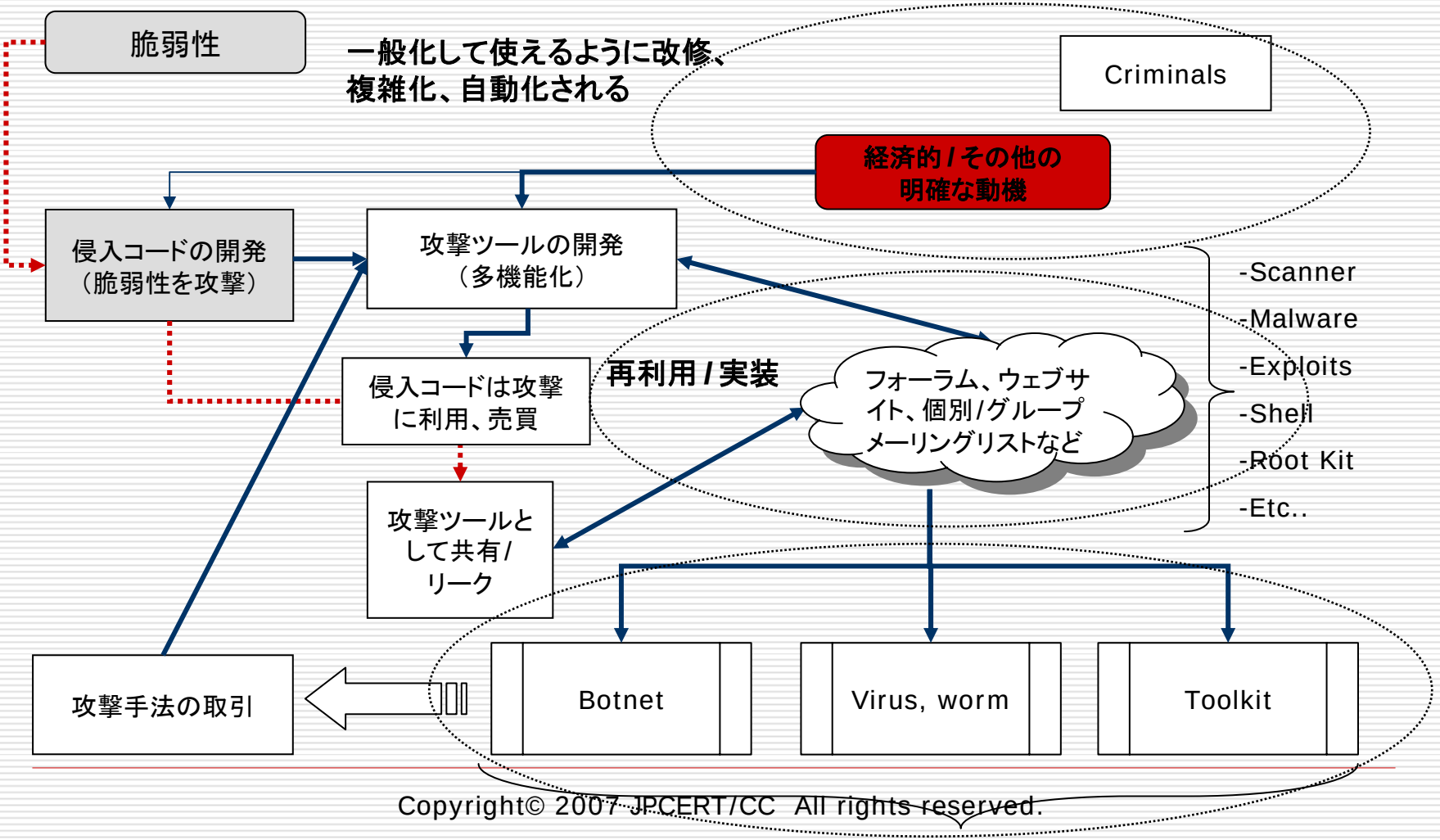
フィッシングサイト公開ホストでの改ざん例

- ユーザ認証機構の改ざん
- アカウント情報の追加、変更
- 侵入者に関する情報を出力から除外するコマンドへの置換
- バックドアや盗聴プログラムの設置

など

D. ソフトウエア等の脆弱性

攻撃者コミュニティにおける脆弱性、マルウェアの売買取引



脆弱性情報の売買取引市場の形成

脆弱性/攻撃コード	価格	情報ソース
“ある”攻撃コード	$200,000 - $250,000	米政府当局者
Internet Explore	$60,000 - $120,000	H.D. Moore
Vista exploit	$50,000	Raimund Genes, Trend Micro
Weaponized exploit	$20,000 - $30,000	David Maynor, SecureWorks
ZDI, iDefense purchases	$2,000-$10,000	David Maynor, SecureWorks
WMF exploit	$4000	Alexander Gostev, Kaspersky
Microsoft Excel	$1200	Ebay auction site
Mozilla	$500	Mozilla bug bounty program

The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales
Charlie Miller, PhD, CISSP

脆弱性情報取引サイト

WabiSabiLabi

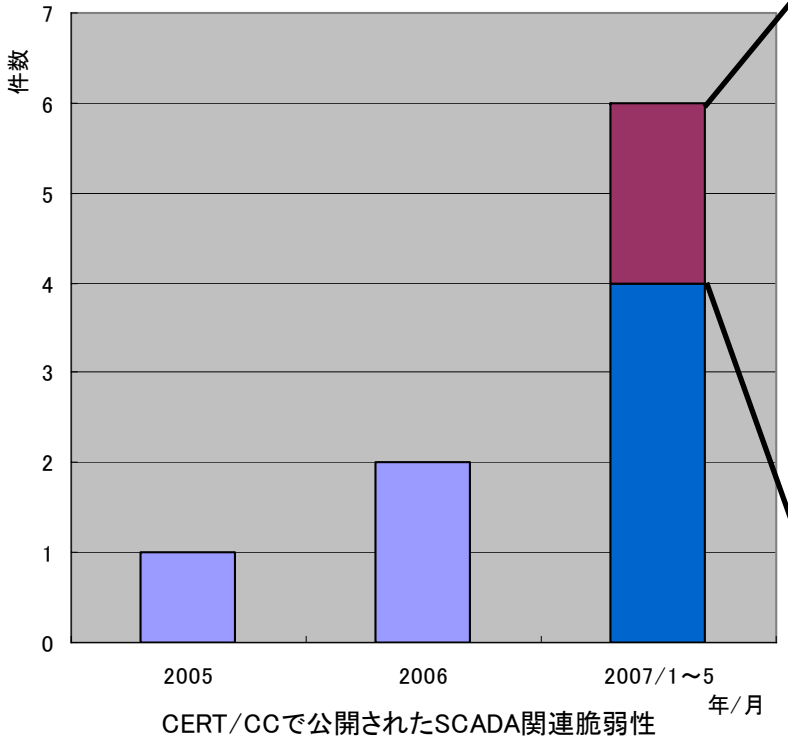
Open Office の脆弱性:

2000ユーロ (約30万円)

2007年 7月27日

SCADAシステムの脆弱性

- 増加するSCADAシステム関連脆弱性



CERT/CCで公開されたSCADA関連脆弱性

- 日本でも情報を公開

■ JVNVU#296593:
NETxAutomation 社製 NETxEIB OPCServerに OPC server handle を適切に処理できない脆弱性

■ JVNVU#202345:
デバイスエクスプローラMELSEC OPC サーバに バッファオーバーフローの脆弱性

■ JVNVU#346577:
デバイスエクスプローラ MODBUS OPC サーバに バッファオーバーフローの脆弱性

■ JVNVU#926551:
デバイスエクスプローラ TOYOPUC OPC サーバに バッファオーバーフローの脆弱性

■ JVNVU#581889:
デバイスエクスプローラ SYSMAC OPC サーバに バッファオーバーフローの脆弱性

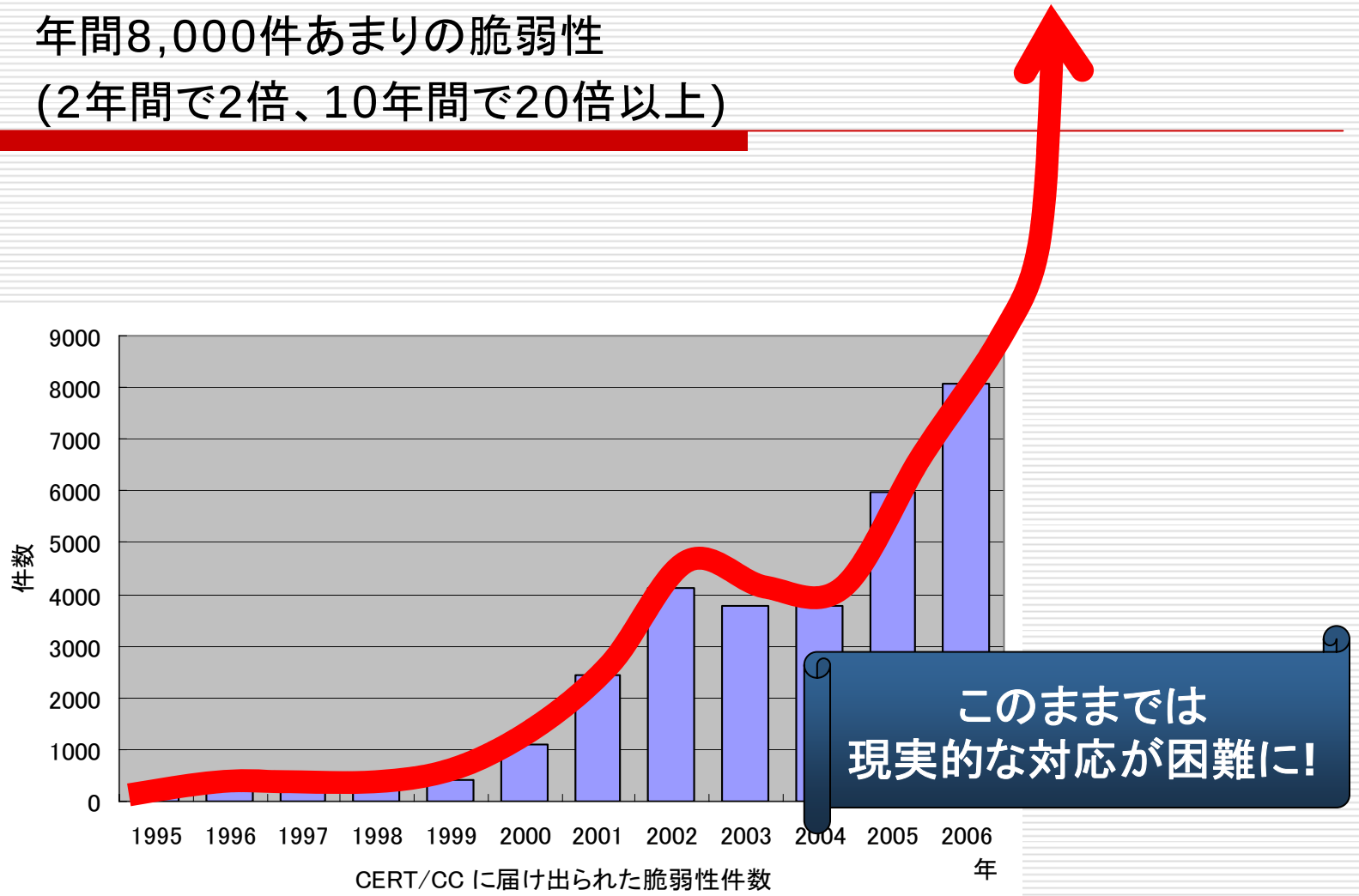
■ JVNVU#907049:
デバイスエクスプローラ FA-M3 OPC サーバに バッファオーバーフローの脆弱性

■ JVNVU#347105:
デバイスエクスプローラ HIDIC OPC サーバに バッファオーバーフローの脆弱性

JPCERT CC®

ソフトウェア脆弱性の発見は増加の一途

- 年間8,000件あまりの脆弱性
  (2年間で2倍、10年間で20倍以上)



ソフトウェア開発者にとって脆弱性の存在は不可避

- 全ての攻撃に備えることは不可能
  - 日々新たな攻撃手法が出現
- 開発が大規模になればなるほど、既知の脆弱性対策の反映が困難
  - 脆弱性情報の収集と取り纏め
  - 外部委託先での管理
- 製品に脆弱性が発見された場合に、ユーザに不安を与えず、冷静に対処してもらうことが重要

情報公開の姿勢と仕組みが必要

E. ユーザリテラシーリスク

※　ユーザは、サービスや製品のセキュリティレベルを理解して選択できる？

- サービスにアクセスするためのID,パスワードを忘れてしまったときに、教えてくれるサービスと、変更の手続きを求めるサービス、どちらを選ぶべき？
- 2.0時代のデータマイニングの活発化に鑑みると、本人を特定するためのデータを公開している人（組織）と、公開していない人（組織）どちらが脆弱？
- セキュリティ対策がどの程度とられているかを確認して製品・サービスを選択するにはどうすればよいかを誰が教えてくれる？

※　インシデントに巻き込まれたり、加害者としての容疑をかけられたときに、自らの責任の有無を立証できる？　証拠を正しく理解してもらえる？

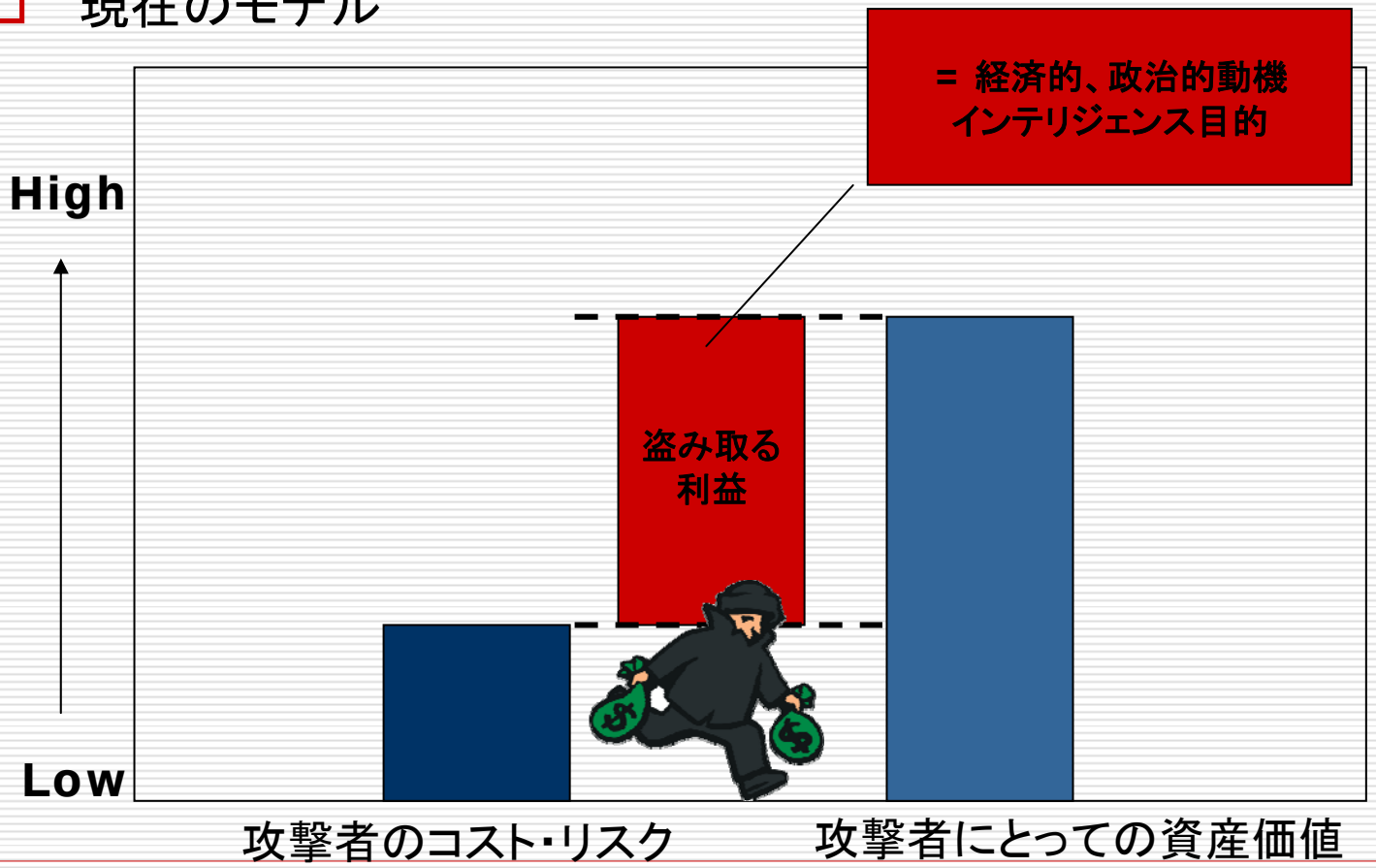
JPCERT CC®

3. 対策の状況

対策の視点：

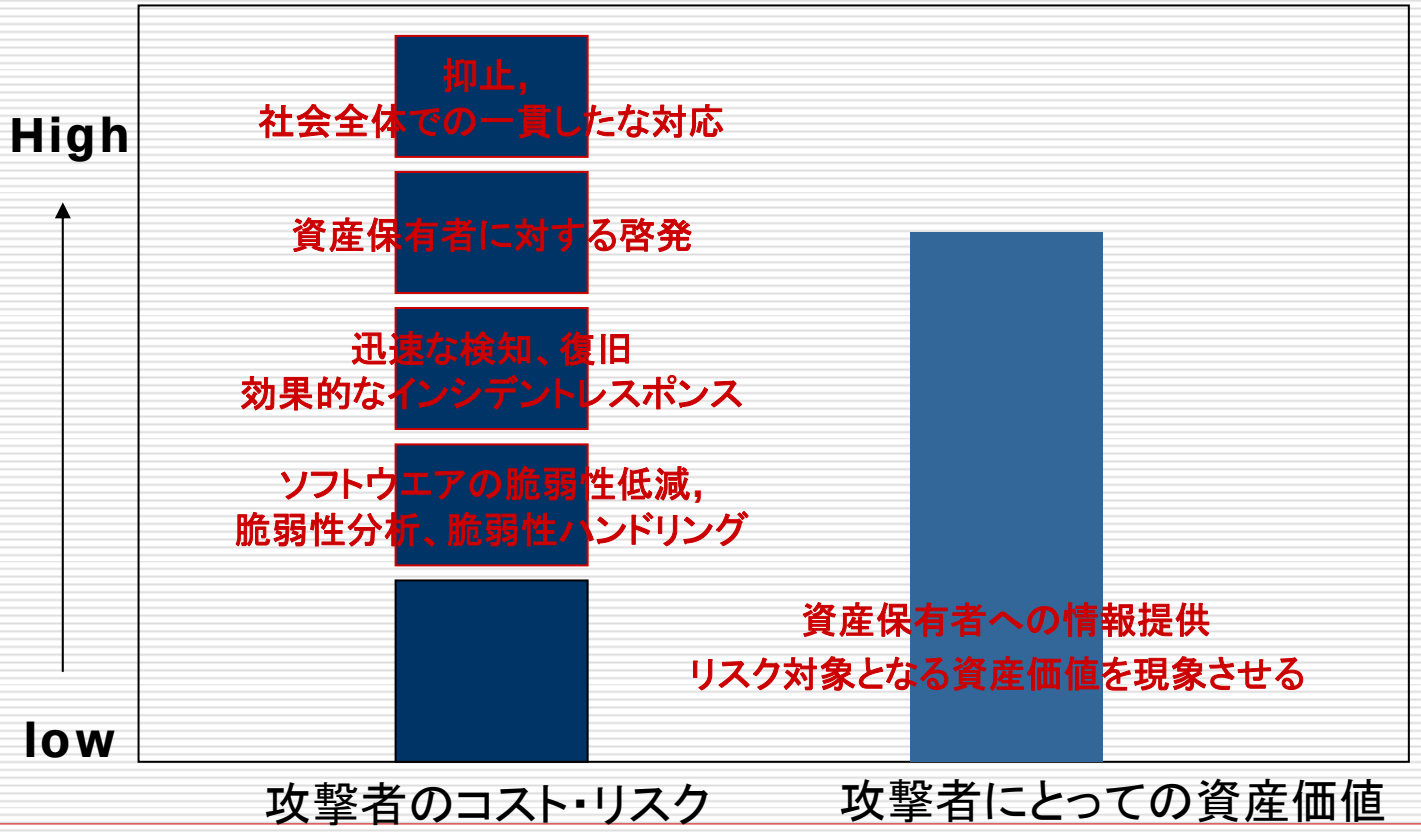
攻撃者のコスト･リスクを上げて、ビジネスとして成り立たなくさせる

- 現在のモデル



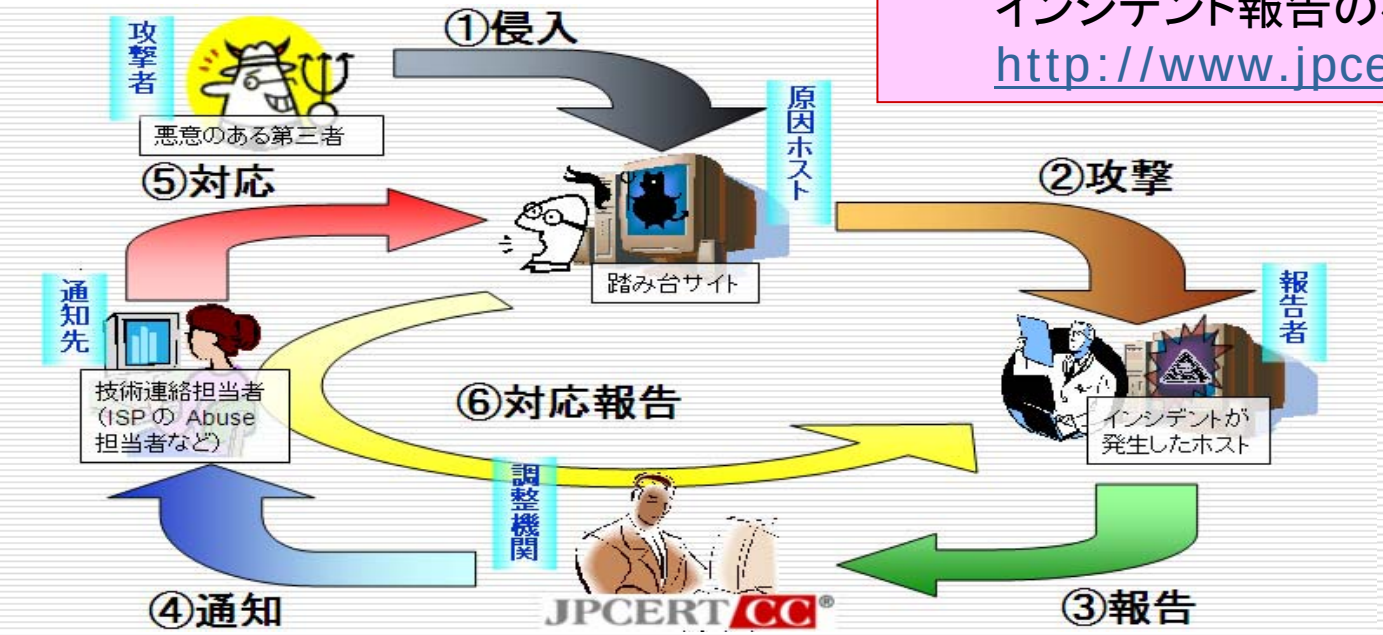
JPCERT CC®

□ 攻撃者のコストを引き上げ、攻撃を抑止する



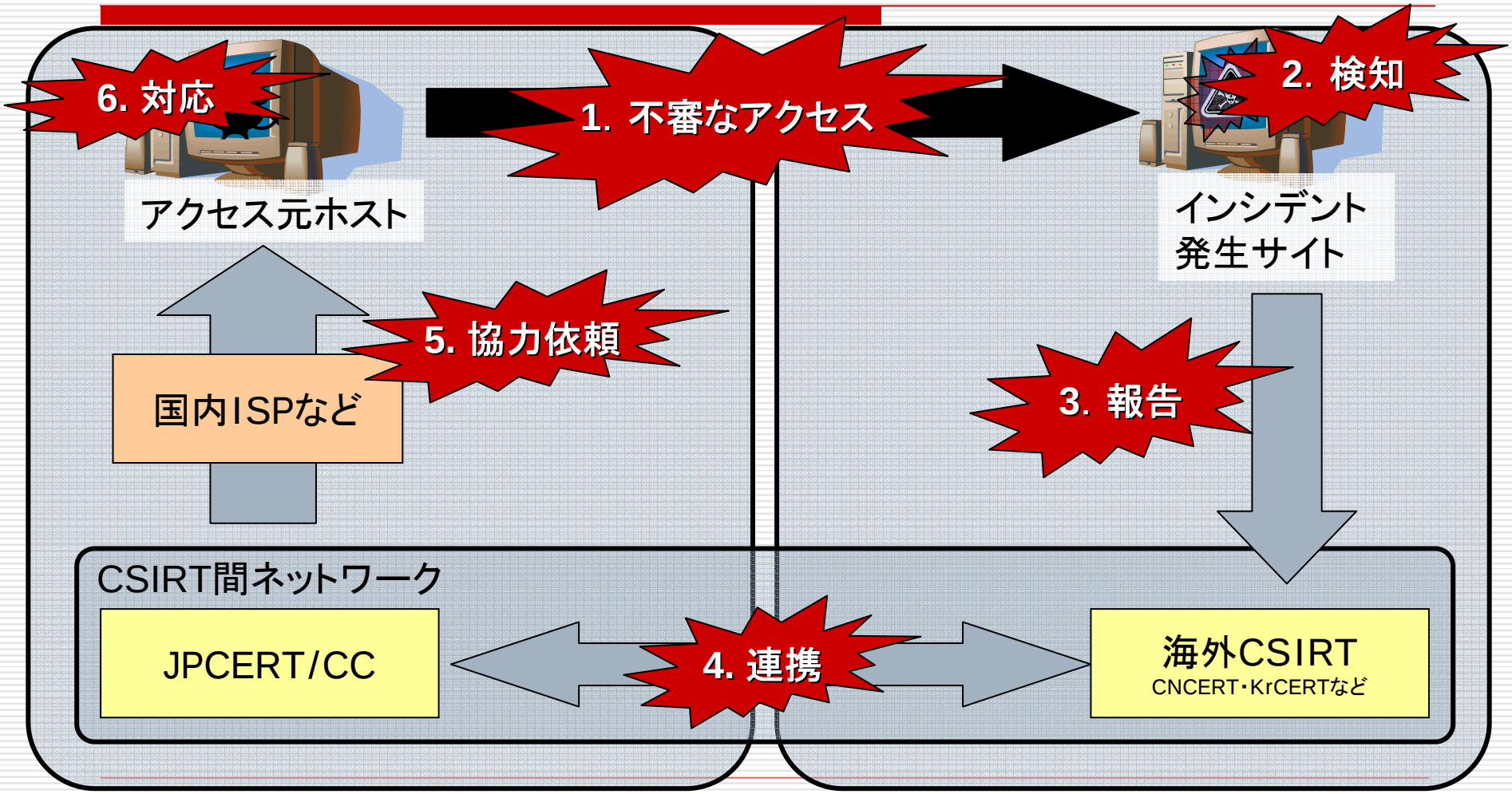
A. 攻撃を長く稼動させないための迅速なレスポンス
インシデントハンドリング：報告受付と対応支援

インシデント報告の様式等
http://www.jpcert.or.jp/form/

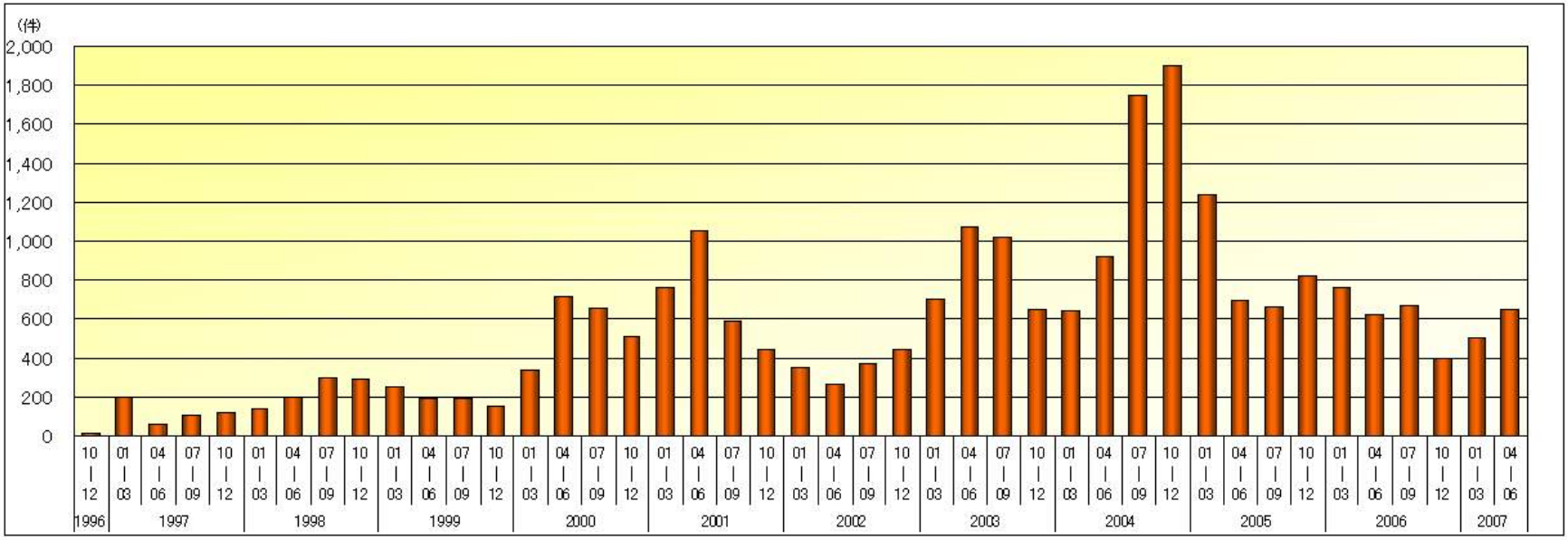


※インシデントとは：
コンピュータセキュリティに関係する人為的事象で、意図的および偶発的なもの
(その疑いがある場合 を含む。)
例えば、リソースの不正使用、サービス妨害行為、データの破壊、意図しない情報の開示や、さらにそれらに至るための行為 (事象) など

インシデントハンドリングの国際連携

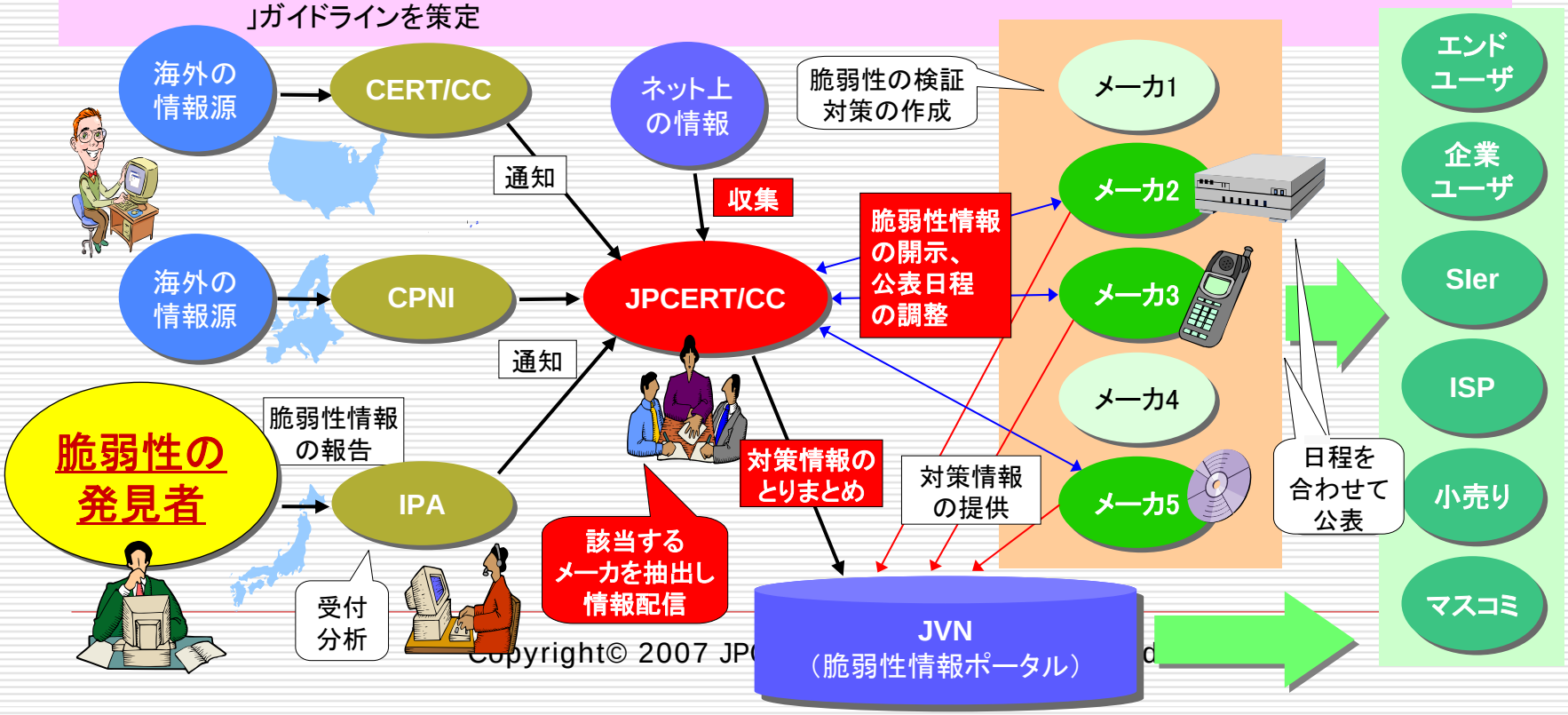


JPCERT/CCへのインシデント報告件数の推移



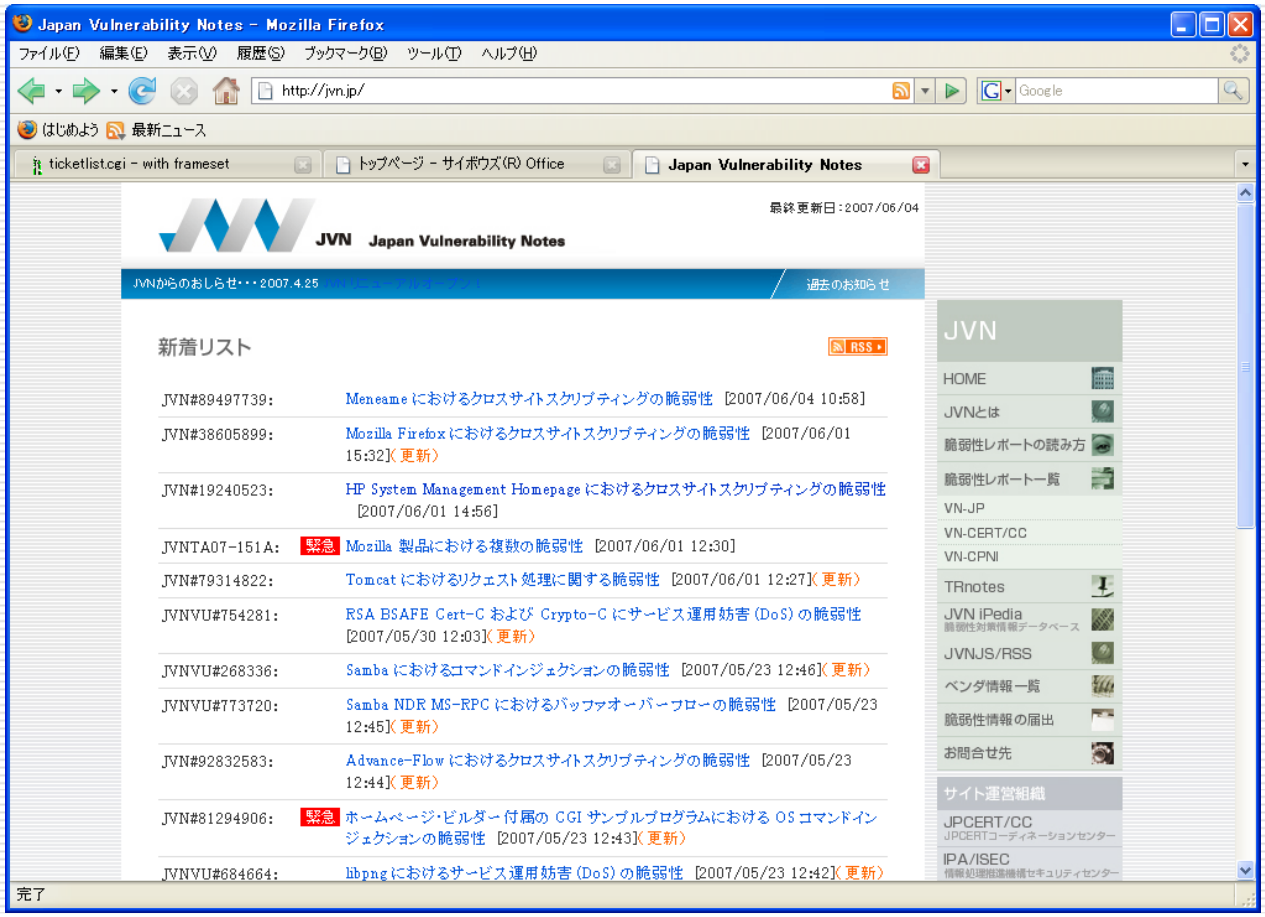
B. ソフトウエア等の脆弱性対応「情報セキュリティ早期警戒パートナーシップ」

- 脆弱性関連情報を、適切な関係者へ事前に開示し、被害を最小限に食い止めるためのプロセス
  - 未公開脆弱性情報の受付 ⇒ 検証 ⇒ 製品開発者に開示
  - 国外の関係機関（CERT/CC、CPNI等）と連携し、国内外の製品開発者へ情報展開
  - 関係するすべての製品開発者が同時に情報公開するよう調整
  - 脆弱性情報ポータルサイト（JVN）を運営し、脆弱性情報と各社の対応を公開
- 経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」に基づく活動
  - JPCERT/CCが調整機関として指定
  - JEITA、JNSA、JISA、CSAJ、IPA、JPCERT/CC が協同で「情報セキュリティ早期警戒パートナーシップ」ガイドラインを策定



脆弱性情報対応状況ポータルサイト

JVN (Japan Vulnerability Notes)
http://jvn.jp/

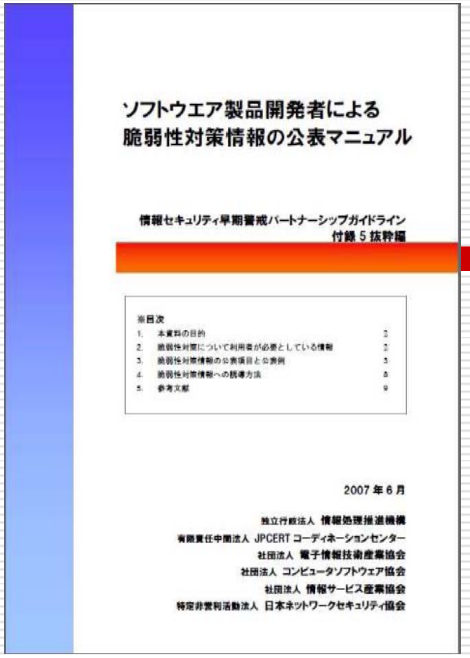


問題点

- 脆弱性を作りこまない体制
  - 脆弱性が発見されてから対応するのでは追いつかない。
    ⇒　脆弱性を作りこまない開発、製品出荷の体制
  - セキュアなコーディング、出荷前テストにはコストがかかるが、コストをかけていることが見えない。
    ⇒競争力につながらない。
    ⇒セキュアなコーディングへの取組みが進まない。
  - セキュアなコーディング、出荷前テストが円滑に導入できるようにするために
    - 脆弱性リスクの定量評価、コーディング技術の普及活動、検証ツールの評価

- 情報家電の脆弱性
  - 出荷後に発見された脆弱性の修正の困難さ
  - 修正プログラムをインストールしないユーザに対する責任の考え方

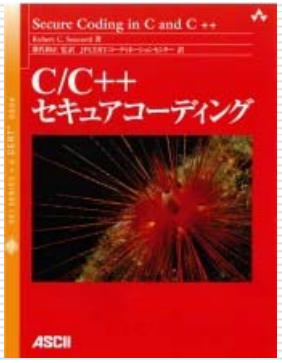
JPCERT CC®



「ソフトウエア製品開発者による脆弱性対策情報の公開マニュアル」
http://www.ipa.go.jp/security/ciadr/partnership_guide.html

http://www.ipa.go.jp/security/vuln/vuln_contents/

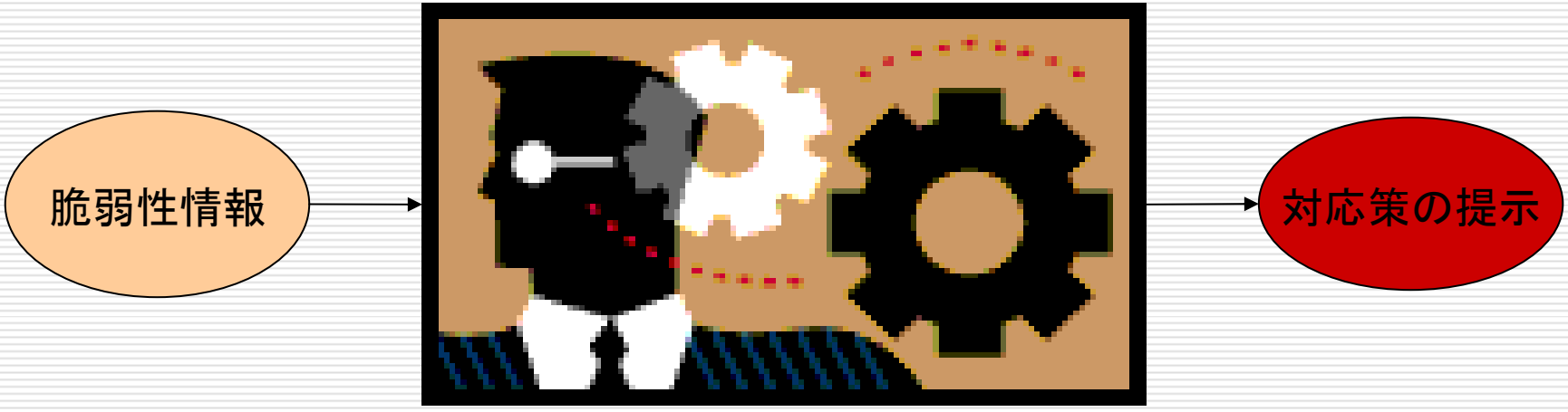
http://www.ipa.go.jp/security/vuln/websecurity.html



C/C++ セキュアコーディング
Robert C. Seacord 著
JPCERT/CC 翻訳
攻撃リスクを除去・緩和するための
効果的かつ実用的な回避策を提示

ソフトウエア等の脆弱性対応：ユーザ支援
脆弱性対応意思決定支援ツールの提供

- 分析者の判断ロジック(組織の判断基準に基づく)をシステム化できるツール。⇒**KENGINE**
- そのため**KENGINE**は、個別組織の判断基準に基づいた、とるべき対策を、脆弱性毎に具体的に提案できる。



C. 組織内インシデント対応チームへの支援 —対応ナレッジの提供

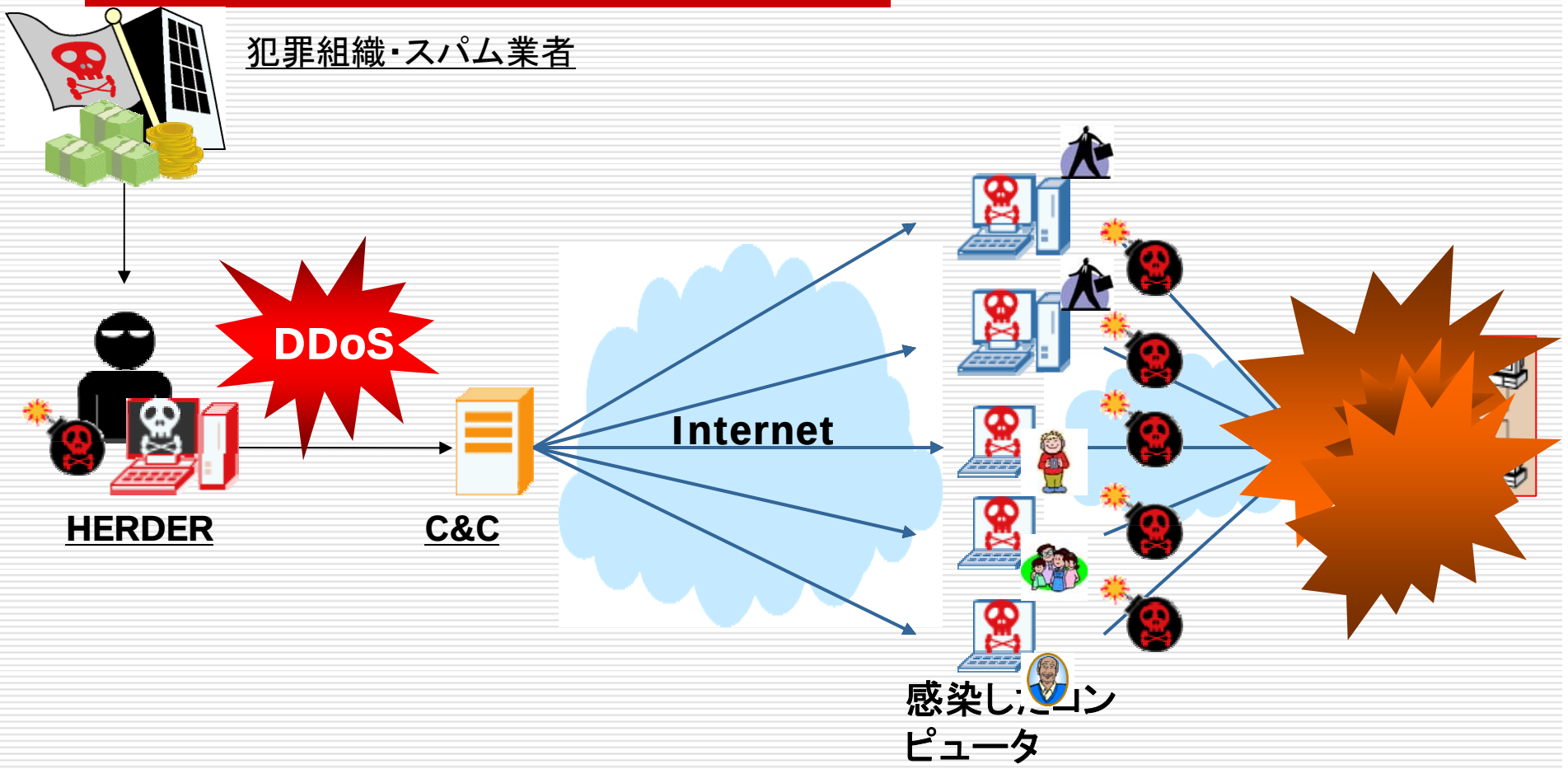
- 組織毎に異なる組織内 CSIRTの形態、活動内容
  - 組織の事業内容、規模、部門構成、業務遂行形態、リスクの定義などにより、それぞれの組織内 CSIRT の活動内容や形態が大きく異なる
  - 組織の状況にあわせた機能を持つ組織内 CSIRT の構築が必要
  - JPCERT/CC から組織内 CSIRT 構築過程に必要な情報及びノウハウを提供
    - 組織内 CSIRT 構築支援マテリアル
      http://www.jpcert.or.jp/csirt_material/
- 日本シーサート協議会も発足

組織内 CSIRT 構築支援マテリアル

- http://www.jpcert.or.jp/csirt_material/

認知	組織内 CSIRT の必要性	インシデント対応活動の必要性やその対応体制の設置の意義を説明し、組織内 CSIRT 構築を推奨しています。
理解	組織内 CSIRT の役割	組織内 CSIRT の基本かつ重要なポイントから、その役割について説明し、具体的な例をあげながら、組織内 CSIRT の役割について説明をしています。
	組織内 CSIRT の活動	組織内 CSIRT の活動に必要なフレームワークと活動内容を定めるにあたっての考察ポイントを説明しています。
	組織内 CSIRT の要員	組織内 CSIRT の要員に必要なヒューマンスキルとテクニカルスキルを説明しています。
	組織内 CSIRT の形態	組織内 CSIRT の形態の種類と組織の実情に合わせた選択の説明をしています。
実践	組織内 CSIRT の構築プロセス	組織内 CSIRT の全体的な構築プロセスを説明しています。
	組織内 CSIRT の実作業	組織内 CSIRT を構築の実作業のマイルストーンとそれぞれの成果物を説明しています。
参考	インシデント対応マニュアルの作成について	組織内 CSIRT 構築活動におけるインシデント対応マニュアルの作成のポイントについて説明しています。
	組織内 CSIRTの情報管理と設備について	組織内 CSIRT の情報管理のポイントとその設備の例を説明しています。
	組織内 CSIRTにおける電話応対について	組織内 CSIRT における電話対応のポイントについて説明しています。
	PGP の説明に役立つデータ	CISRT 間で必要になることが多い PGP について、その説明に役立つデータを提供していすます。

D．ボットネット対策

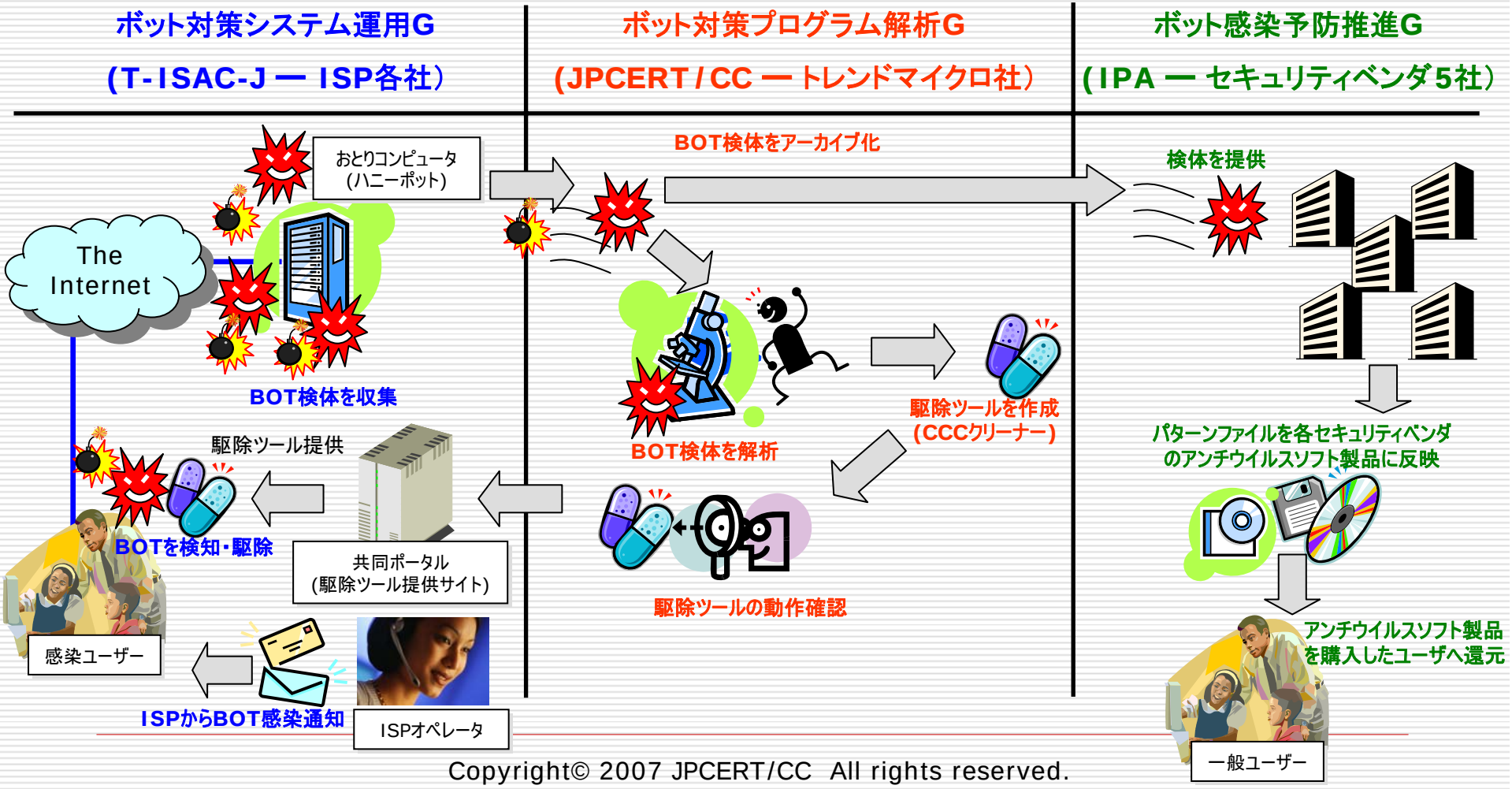


総務省･経済産業省共同によるボット対策プロジェクト

CCC(サイバークリーンセンター)

サイバークリーンセンター
(https://www.ccc.go.jp/)

サイバークリーンセンタープロジェクトの概要



活動実績（平成16年12月から17年7月）

RTCC®

① 収集検体総数：3,198,796

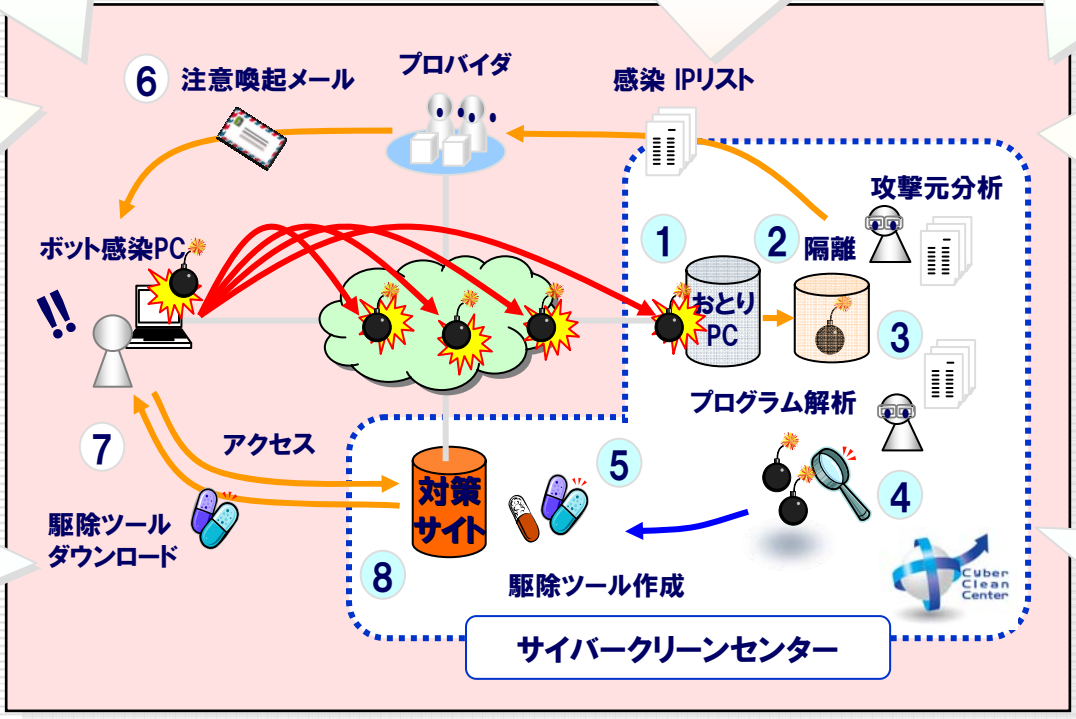
「おとりPC」に対する無数の攻撃の中から、ボットウィルス等の検体（バイナリファイル）を収集します

② 同定検体数：83,240

同じ検体が多数収集されるため、検体のサイズや外形的特徴の重複を除いた一意な検体（バイナリファイル）を選別・隔離します

③ 未知検体数：4,854

隔離した検体を市販のウィルス対策ソフトで検査し、検知できなかったものを選別します



⑥ 注意喚起数：93,026回

協力ISPから感染者に出した注意喚起メール数

注意喚起対象者は 28,009件

④ 駆除ツール作成検体数 4,046

未知検体を分析し、危険度が高く、感染者の多い検体について駆除ツールを作成します

⑦ 被注意喚起者駆除ツールダウンロード率 30%

⑤ 駆除ツール更新回数：26回

駆除ツールは毎週更新します

※一部を除きデータ収集期間は平成18年12月12日～平成19年7月31日

駆除ツールダウンロード総数：164,561 回

E. アジア太平洋地域における国際連携活動

- APCERT事務局の運営
  - ウェブサイトの管理
  - AP* Retreat への参加
  - 年次報告書のとりまとめ
  - APCERTドリルの実施
  - APCERTにおける連絡体制の維持
- 国際間インシデント情報の連携体制を円滑に行うため、多くの国にCSIRTを設立し、コンタクト可能な状況を確立することが重要
  - 2006度は、東南アジア諸国連合（ASEAN）に着目し、現在のASEAN加盟国を含め、状況調査を行うために、右記7ヶ国を訪問
  - 2007年3月にはカンボジアにて、CSIRTトレーニングをマレーシアと共同で実施。ミャンマー、ラオス、カンボジアから計12名が参加した
- マレーシア
  - CSIRT 構築支援セミナを共催 (2007/03)
  - MyCERT 主催イベント INFOSEC.MY にて講演 (2006/12)
- 台湾
  - 技術講演の実施、TWNCERT との MOU 締結(2007/01)
- ベトナム
  - APCERTメンバーへの推薦・スポンサー(2007/02)
- ミャンマー、ラオス、カンボジア
  - CSIRTトレーニングの実施 (2007/01)
- インドネシア
  - 国内における CSIRT 発展状況の把握 (2007/02)

APCERT ドリルの実施

「 APCERT国際インシデントハンドリングドリル」を実施

- 国際間インシデントハンドリングの円滑な情報連携及び協力体制の強化が目的
- 実施:2006年12月19日
- アジア太平洋地域の 15 CSIRT組織が参加

日本(JPCERT/CC)、韓国(KrCERT/CC)
中国(CNCERT/CC)、香港(HKCERT/CC)
台湾(TWNCERT)、マレーシア(MyCERT)
シンガポール(SingCERT、NUSCERT)
オーストラリア(AusCERT)、ブルネイ(BruCERT)
インド(CERT-In)、タイ(ThaiCERT)、
ベトナム(BKIS)

及び APCERT に属してない
ニュージーランド(CCIP)
ベトナム(VNCERT)

F. 技術的対策：マルウエア解析・脅威分析

- 捕獲
  - インシデント報告
  - ハニーポット・ダウンロード
- 解析
  - 動的解析
  - 静的解析
- 成果
  - 捕獲・解析手法の改善と共有
  - 傾向・統計

分析・解析におけるリスク

- 捕獲・分析手法
  - リーガルリスク
  - 手法の進歩がマルウェアの進化を促す
    - “Anti-”技術はダマシ合い
    - 暗号化・難読化には無数の選択肢

ジレンマ:

分析手法の進歩、分析結果に基づく対策方法への実装に対抗して、マルウエアが進化するとすれば、

⇒　分析によりマルウエア対策が進めば進むほど、新しい対策の実装に追随できない層をリスクにさらすことになりはしないか？

JPCERT CC®

最後に:

- 見えにくくなってきている脅威情報の集約・分析⇒適切な相手に、適切な対策情報の発信
- 不正プログラム解析・分析能力の向上
  - 攻撃者側は組織化しており、攻撃手法の高度化のスピードも加速　⇒　守る側の解析・分析チームの連携、リソースの共有等　⇒　結果の利用のあり方
- ソフトウエア等の脆弱性関連情報の実際の対策への反映
  - より対策につながりやすい脆弱性関連情報の提供・対策方法意思決定支援ツールの提供等
- ネットワーク家電や制御系のシステム等の脆弱性対策
- 脆弱性を作りこまないセキュアなコーディング手法等の対策を「実装」してもらうための施策
- ユーザが製品・サービスのレベルを理解した上で選択できる環境
- 2.0時代のリテラシー

お問い合わせ、インシデント対応のご依頼は

- JPCERTコーディネーションセンター
  - Email:office@jpcert.or.jp
  - Tel:03-3518-4600
  - Web: http://www.jpcert.or.jp/
- インシデント報告
  - Email:info@jpcert.or.jp
  - Web: http://www.jpcert.or.jp/form/