JPCERT CC®

セキュリティインシデント最新動向とその対策～JPCERT/CCの活動～

JPCERコーディネーションセンター
早期警戒グループ
マネージャ
鎌田敬介
Keisuke KAMATA
2007 / 10 / 17

本日のTOPIC

- JPCERT/CC の組織概要
- インシデントと脆弱性
- JPCERT/CC　の活動内容
- 組織内CSIRTとは？
- まとめ

JPCERT/CCの概要

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

- JPCERT/CC
  - Japan Computer Emergency Response Team Coordination Center
    - ジェーピーサート・コーディネーションセンター
  - コンピュータセキュリティインシデントに関する調整、連携などの活動をおこなっている
  - 国内組織や海外組織との連携活動
  - 情報収集・分析・発信活動
  - 「コーディネーションセンター」としての役割
  - 米国のCERT/CCを起源とする組織

JPCERT/CCの沿革

1992年	ボランティアベースの活動開始 コンピュータセキュリティインシデント報告対応業務開始
1996年10月	任意団体として発足
1998年8月	CSIRT として日本で最初に FIRST に加盟 －日本の National CSIRT として国際的に認知
2003年2月	APCERT(アジア太平洋コンピュータ緊急対応チーム)発足
2003年3月	中間法人として設立登記
2003年12月	インターネット定点観測システム（ISDAS）公開
2004年7月	経済産業省告示にて「脆弱性情報流通調整機関」として指定
2005年6月	JPCERT/CC のメンバが FIRST 理事に就任
2006年10月	任意団体発足後、10周年
2006年12月	サイバークリーンセンターにおいて、ボットプログラム解析業務開始
2007年6月	JPCERT/CC のメンバがFIRST理事に再任

JPCERT/CCの活動

インシデント予防

脆弱性情報ハンドリング

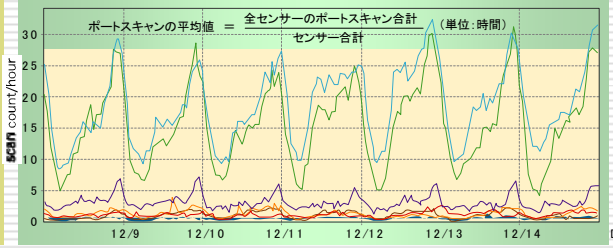
未公開の脆弱性関連情報を
製品開発者へ提供し対応依頼
国際的に情報公開日を調整

JVN Japan Vulnerability Notes

インシデントの予測と捕捉

定点観測（ISDAS）

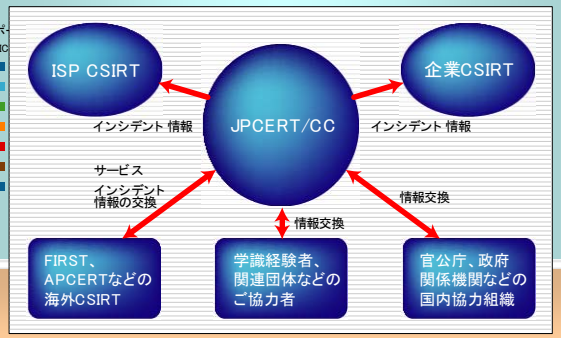
ネットワークトラフィック情報
の収集分析
定期的なセキュリティ予防情
報の提供



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

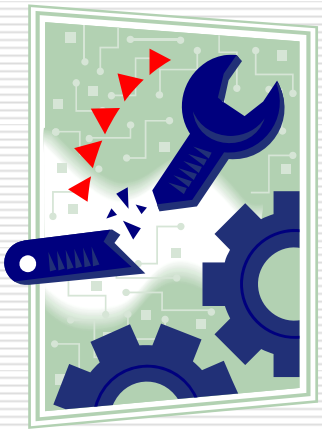
インシデントと脆弱性

- コンピュータセキュリティインシデント
  - インシデントの例
  - インシデントへの対応
- 脆弱性(Vulnerability)
  - 脆弱性の例
  - 脆弱性への対応

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) を含みます

JPCERT/CC Web より
http://www.jpcert.or.jp/faq.html#1a03

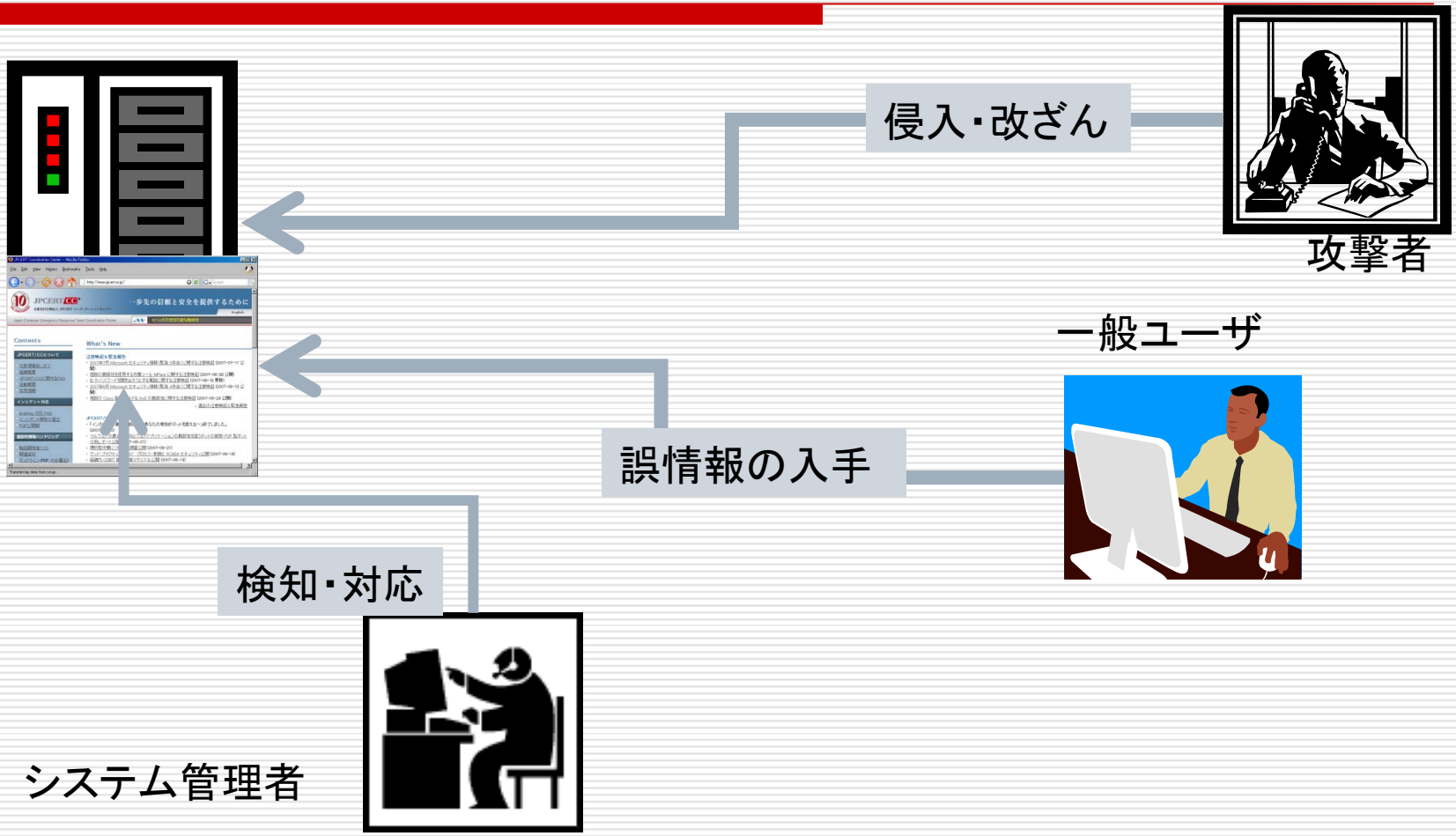


コンピュータセキュリティインシデント分類例

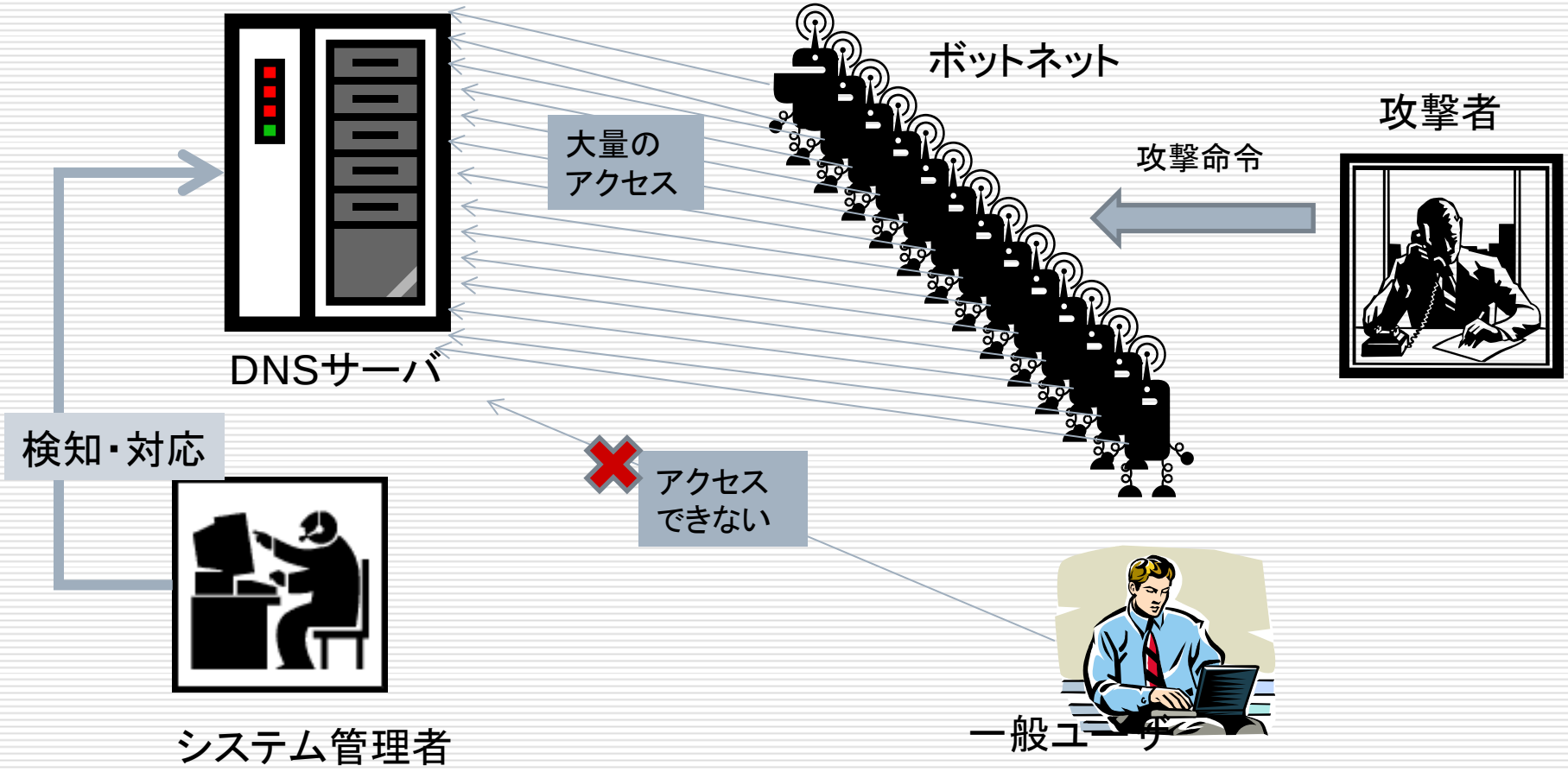
JPCERT/CCにおけるインシデントの分類

- [Scan]: プローブ、スキャン、そのほかの不審なアクセス
  - o 弱点探索(サーバプログラムのバージョンのチェックなど)
  - o 侵入行為の試み(未遂に終わったもの)
  - o ワームの感染の試み(未遂に終わったもの)
- [Abuse]: サーバプログラムの機能を使用した不正中継など
  - o 管理者が意図しないような、メールサーバやプロキシサーバなどの第三者による使用
- [Forged]: 送信ヘッダを詐称した電子メールの配送
  - o From: 欄などの詐称
- [Intrusion]: システムへの侵入
  - o システムへの侵入や改ざん
  - o DDoS 用プログラムの設置(踏み台)
  - o ワームの感染
- [DoS (Denial of Service)]: サービス運用妨害につながる攻撃
  - o ネットワークの輻輳(混雑)による妨害
  - o サーバプログラムの停止
  - o OS の停止や再起動
- [Other]: その他 o SPAM メールの受信
  - o コンピュータウィルスの感染

インシデントの例
1. ウェブサーバへの侵入被害



インシデントの例
2. DNSサーバへの大量アクセス



インシデントの例
3. フィッシングサイト

攻撃者

侵入・改ざん

JPCERT銀行
フィッシングサイト

ID/PWの入力

一般ユーザ

検知・対応

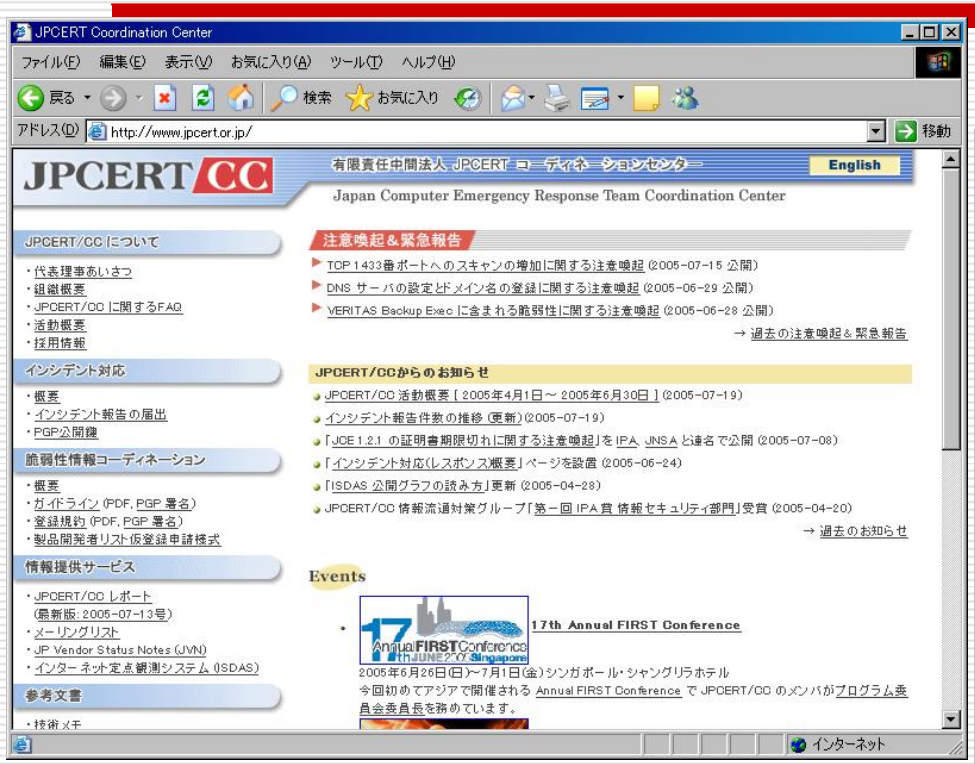
被害サーバの
システム管理者

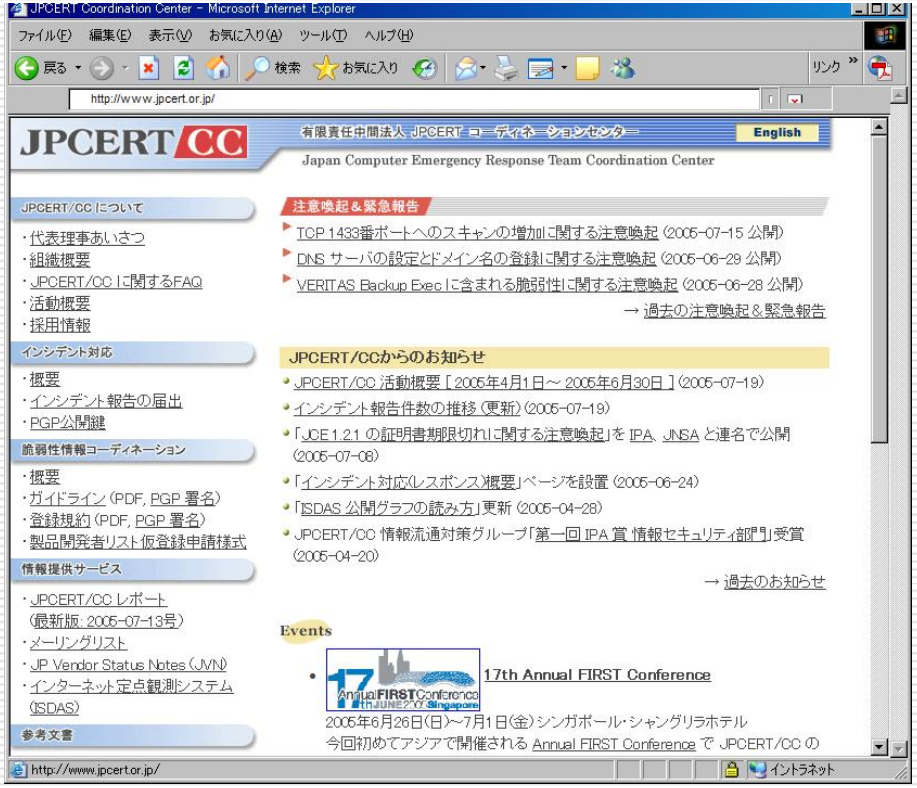
偽サイトへ誘導されてしまう

JPCERT銀行の
本物サイト

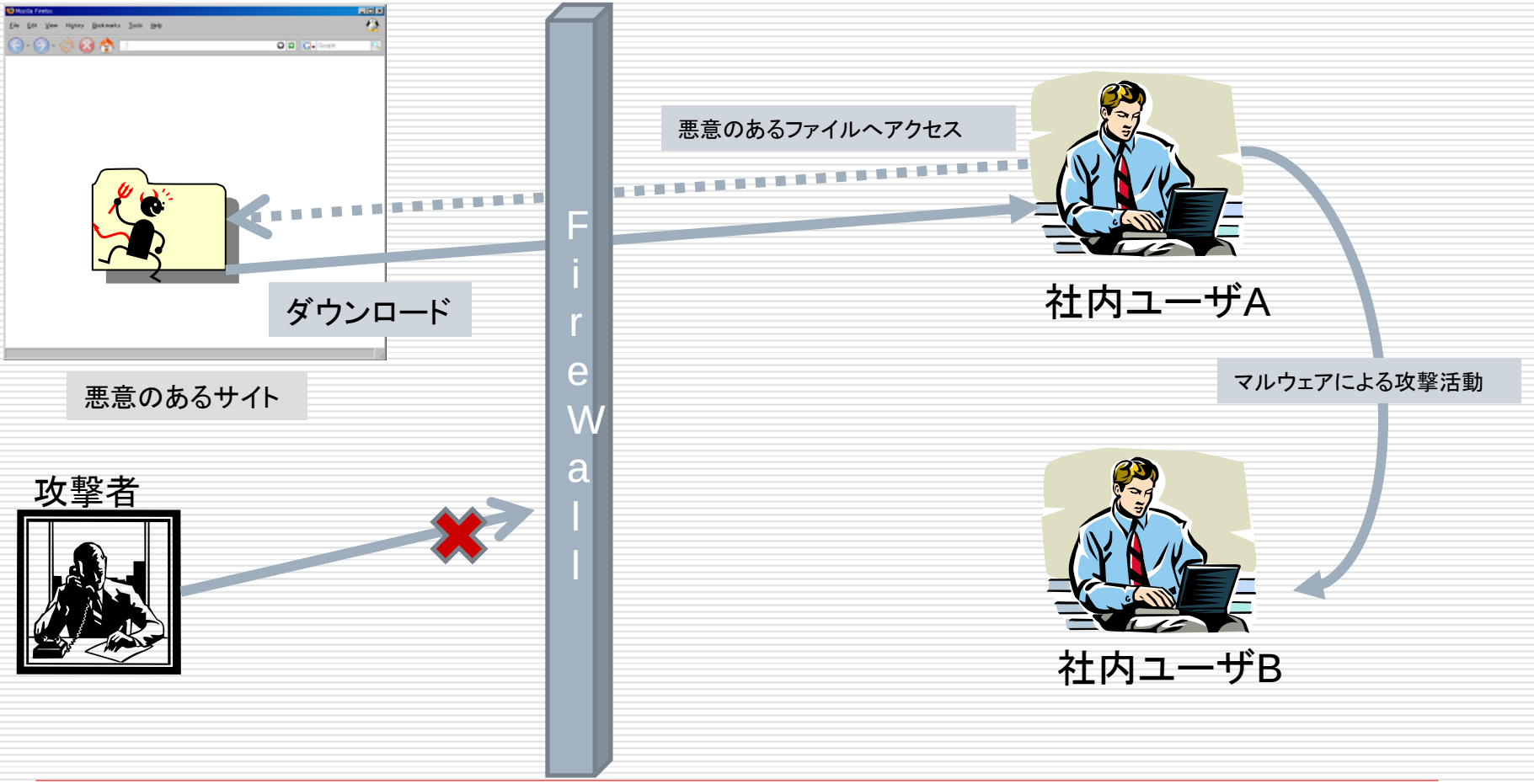
顧客の損失

フィッシングサイト:どっちが本物？





インシデントの例
4. マルウェアやウィルスの被害



インシデントへの対応

- インシデント発生時にどのように動くか？
- 組織内での取り決めや担当者は明確か？
- 同じ失敗を繰り返していないか？
- 効果的な「インシデント対応」とは？

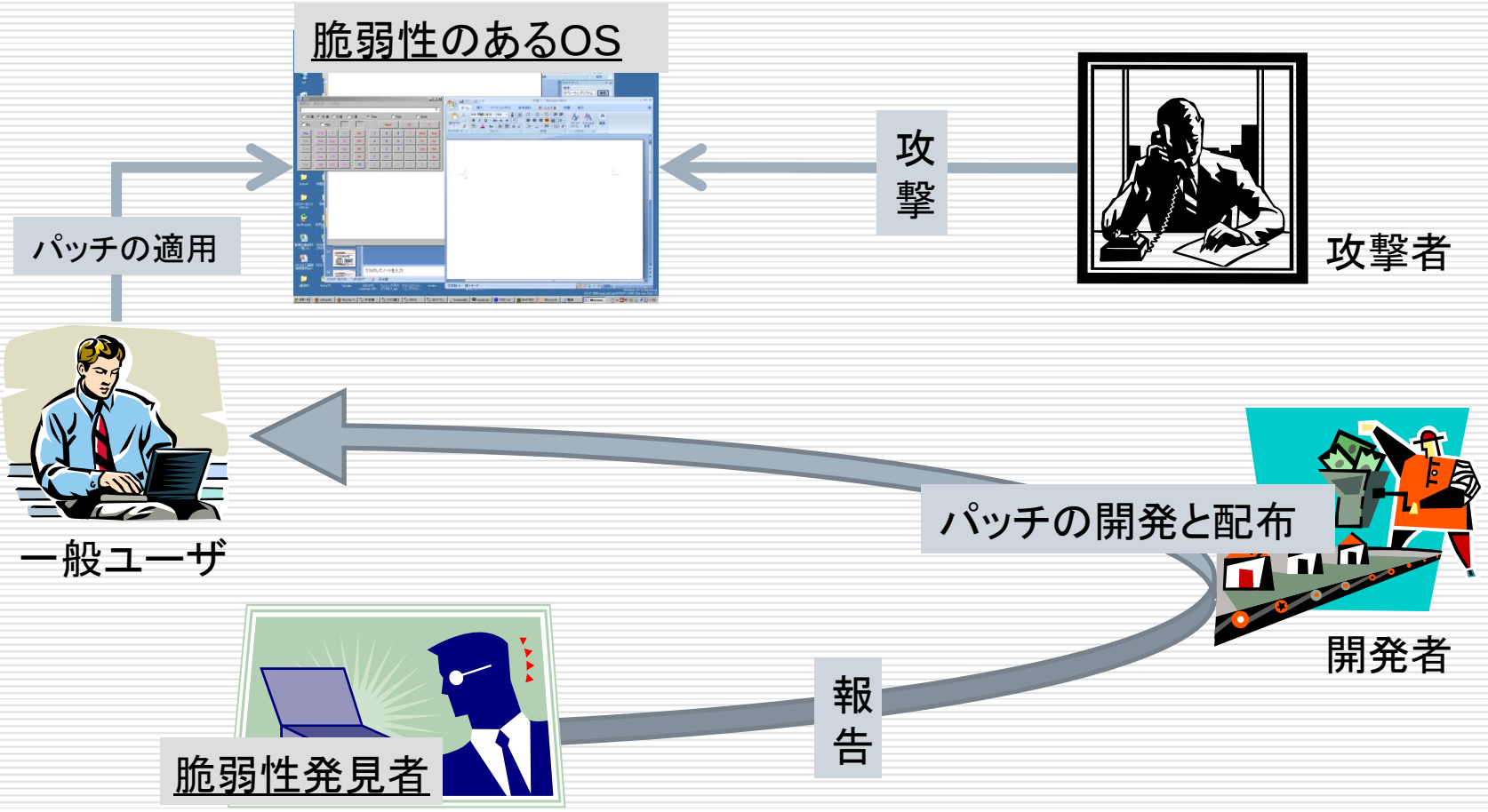
脆弱性とは？

- 経済産業省告示では以下のように定義
  - ソフトウエア等において、コンピュータウイルス、コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所。ウェブアプリケーションにあっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む。
- わかりやすくいえば「セキュリティホール」
- 英語では　Vulnerability（バルネラビリティ）
- 「システムの脆弱性」もありますがここではソフトウェアやハードウェアの脆弱性のことを指します

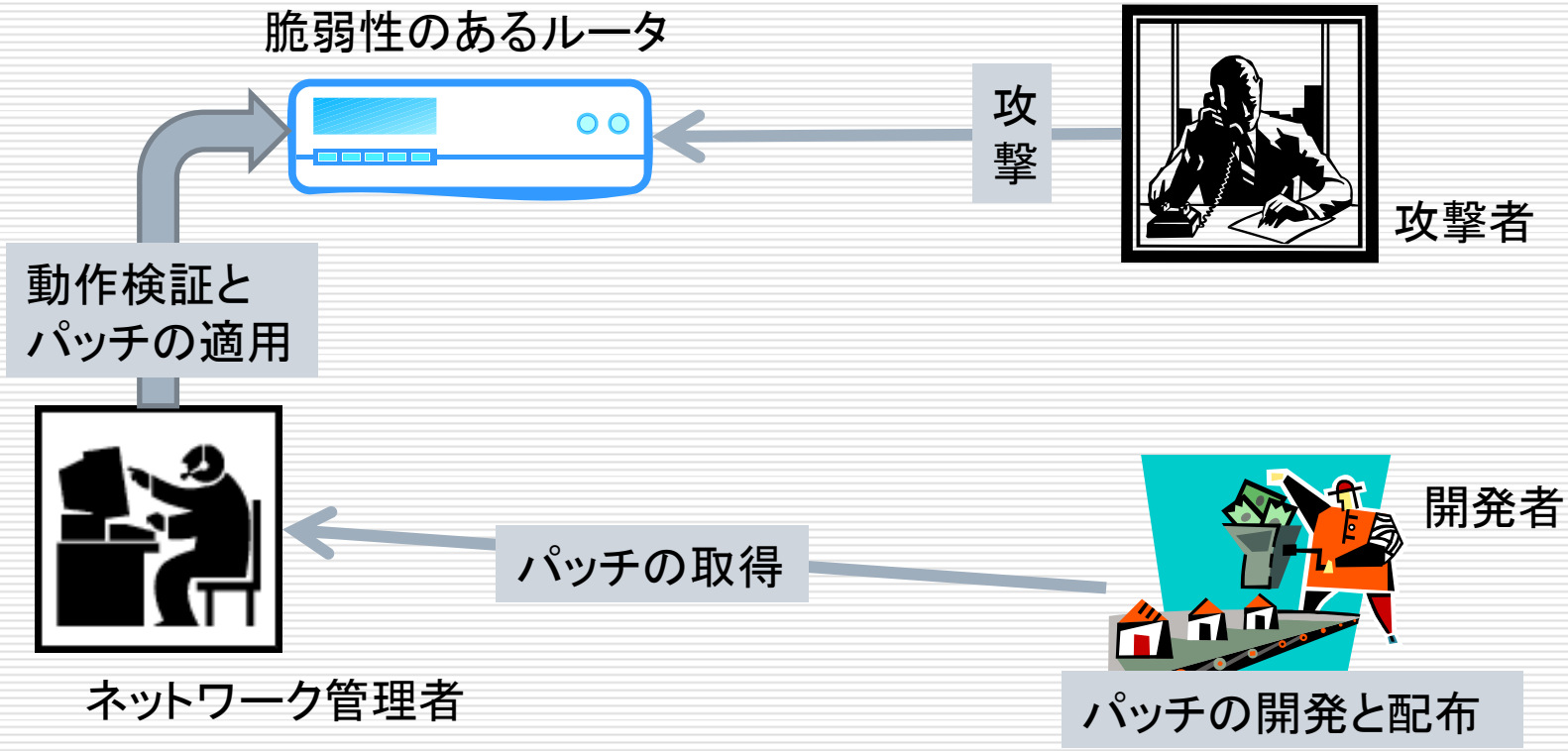
脆弱性案件の種類

- 特定の製品開発者における特定の製品に関わる脆弱性
  - 例えば、マイクロソフトの Windows　の脆弱性
- 複数の製品開発者にまたがる、汎用技術の根本的な問題による脆弱性
  - 通信プロトコル（TCPなど）の脆弱性
  - ライブラリ（zlibなど）の脆弱性
  - etc...

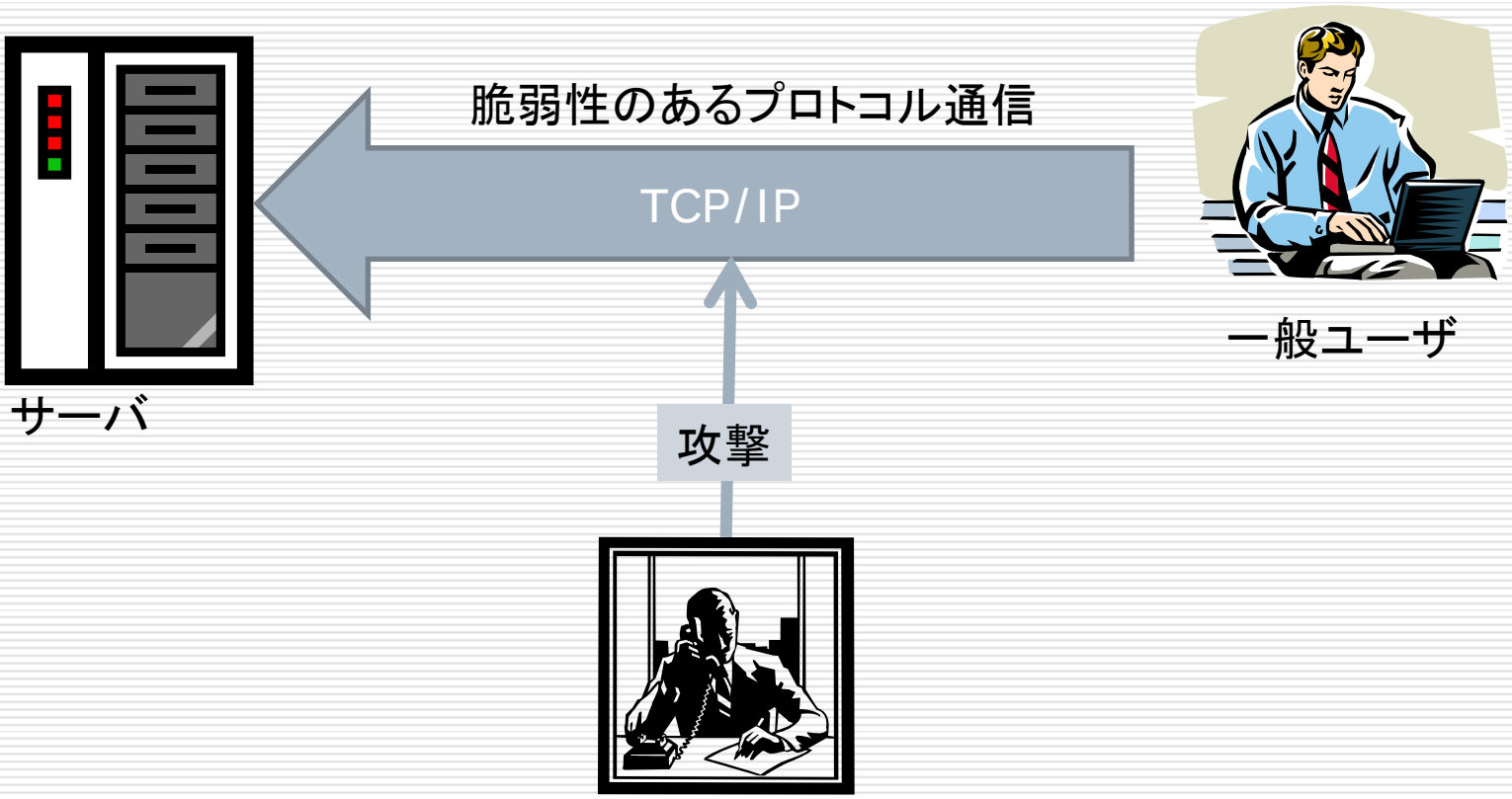
脆弱性の例
1. OS の脆弱性



脆弱性の例
2. ハードウェアの脆弱性

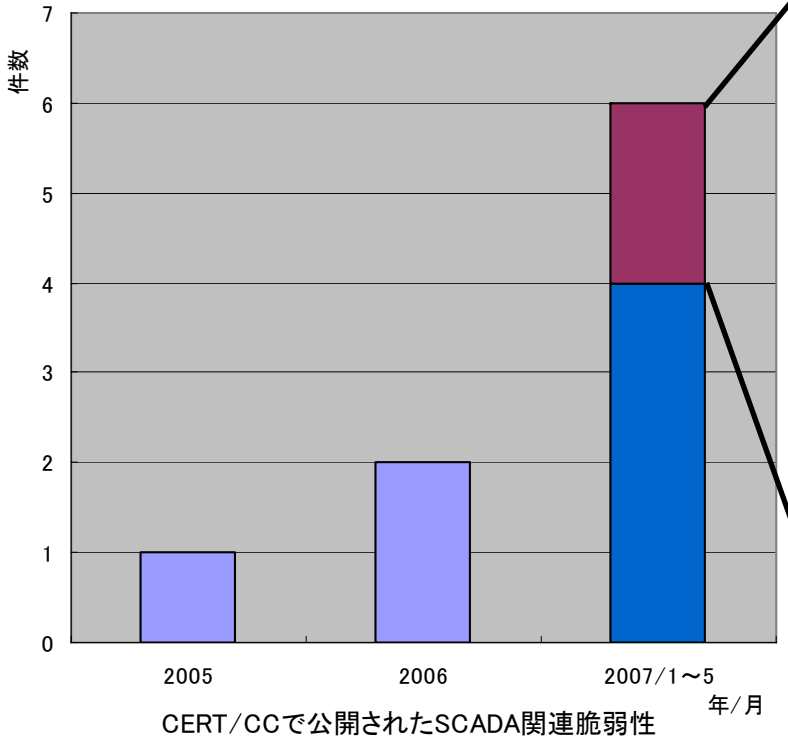


脆弱性の例
3. プロトコルの脆弱性



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

脆弱性への対応（システム運用）

- 組織内で使われているシステムに関する脆弱性の情報を収集しているか？
- 個々の脆弱性情報への対応の判断はどのように行っているか？
- パッチやワークアラウンドの適用における問題点とは？

脆弱性への対応（製品開発）

- 開発している製品への脆弱性対応はどのように行われているか？
- 報告窓口は設置・公開されているか？
- 脆弱性を作り込まない開発を行っているか？

インシデント・脆弱性のここ数年の傾向

- 攻撃の規模：大規模→局所化
  - 特定の組織・個人を狙った攻撃
  - targeted attack (標的型攻撃)
- 愉快犯→金銭目的
  - 国際的には法的な面での整備も進み「犯罪」として法執行機関が動く体制

JPCERT/CC の活動内容

- インシデントレスポンス
- 定点観測事業
- 脆弱性ハンドリング
- 早期警戒
- ボットネット対策

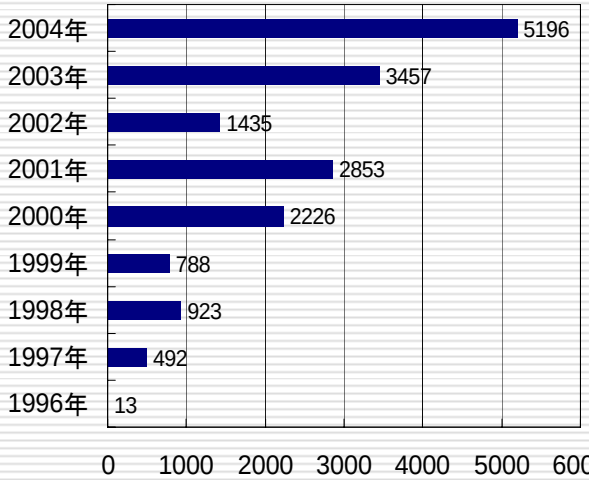
インシデントレスポンス

「CSIRT of CSIRTs」

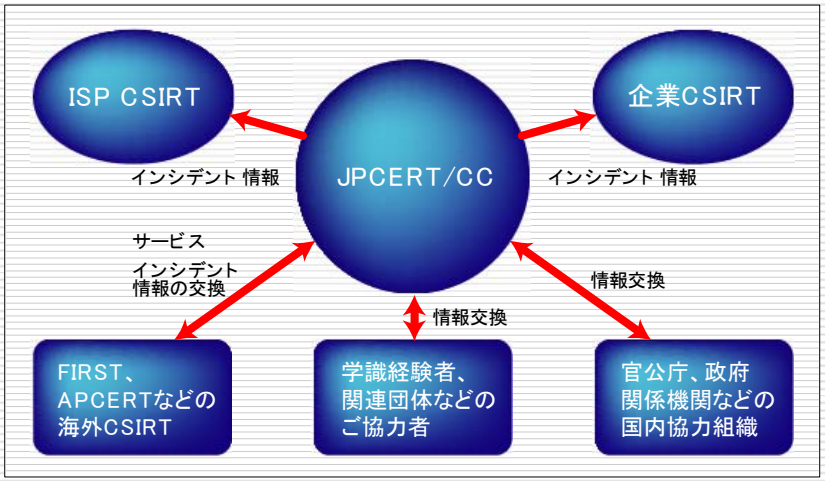
CSIRT (Computer Security Incident Response Team)間の連携をコーディネート

- 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機関の情報交換および情報共有

インシデント報告件数の推移



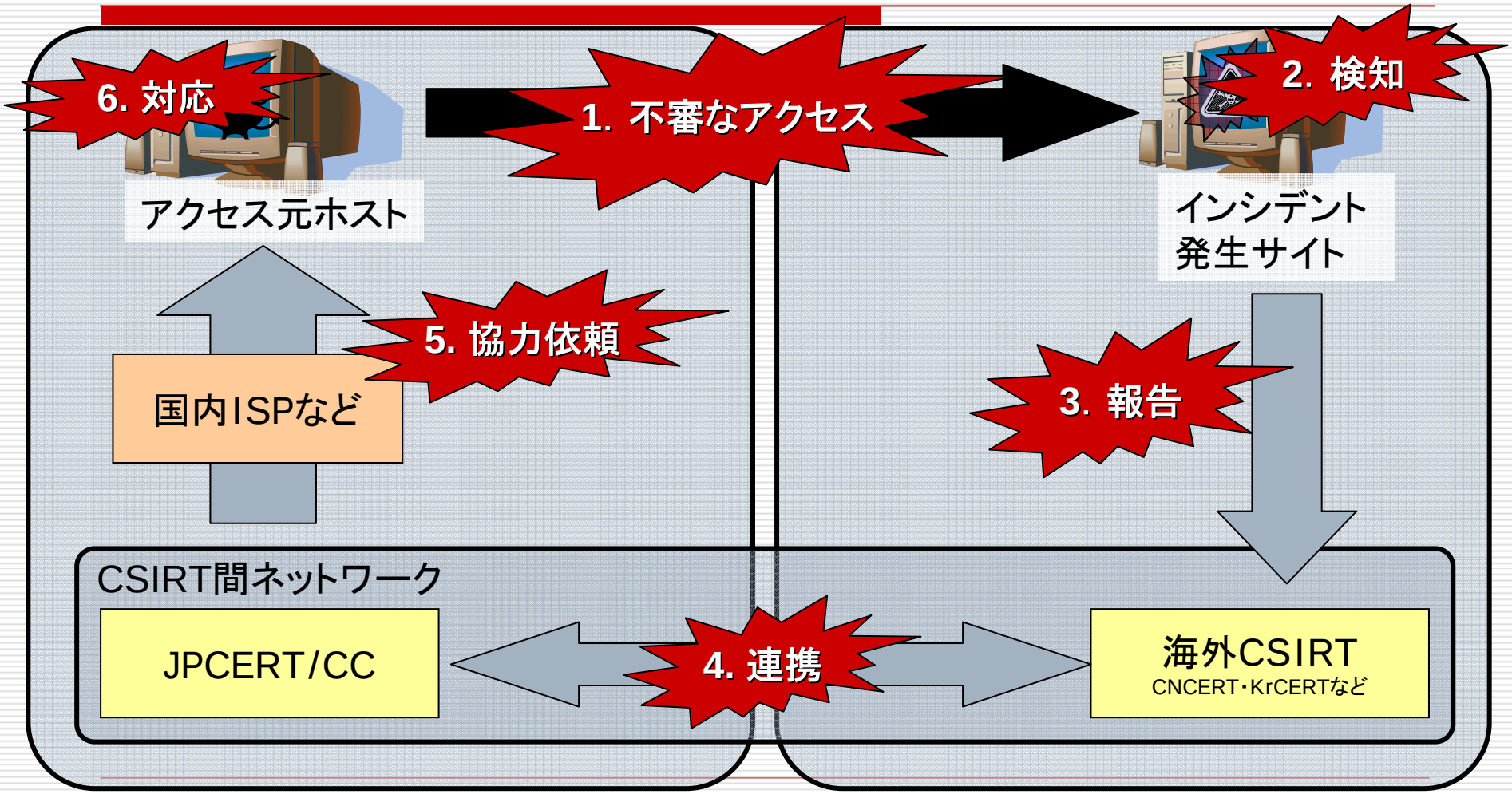
※JPCERT/CC が1996年から2004年に受領したインシデント報告



インシデント報告の受付

- JPCERT/CCでは国内外からのインシデント報告を受け付けています
  - インシデント報告の届出
    http://www.jpcert.or.jp/form/
  - 報告の目的を記載
    - インシデントの情報提供
    - 質問（インシデント対応に関するもの）
    - 関係サイトへの連絡
    - その他

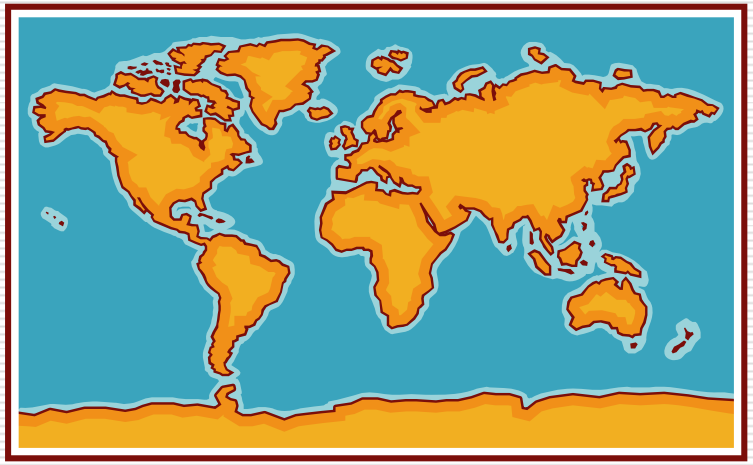
インシデントハンドリングの国際連携



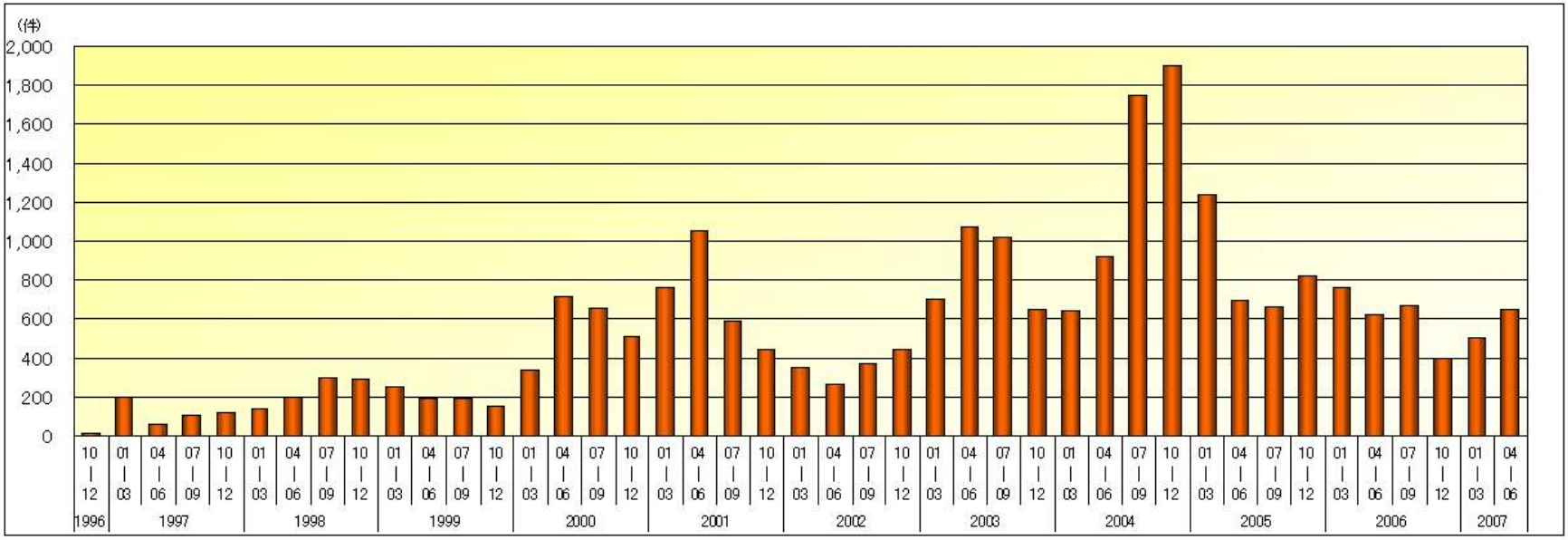
インシデントハンドリングの国際連携

- 国際連携によって越えられる壁
  - 言語の違い
  - 文化の違い
  - 法律・制度の違い

- 各国CSIRT間の
  連携・協調活動として
  最も進んでいる分野

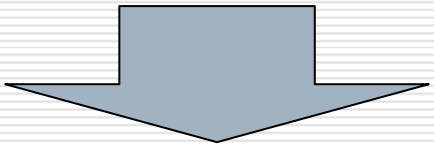


JPCERT/CCへの
インシデント報告件数の推移



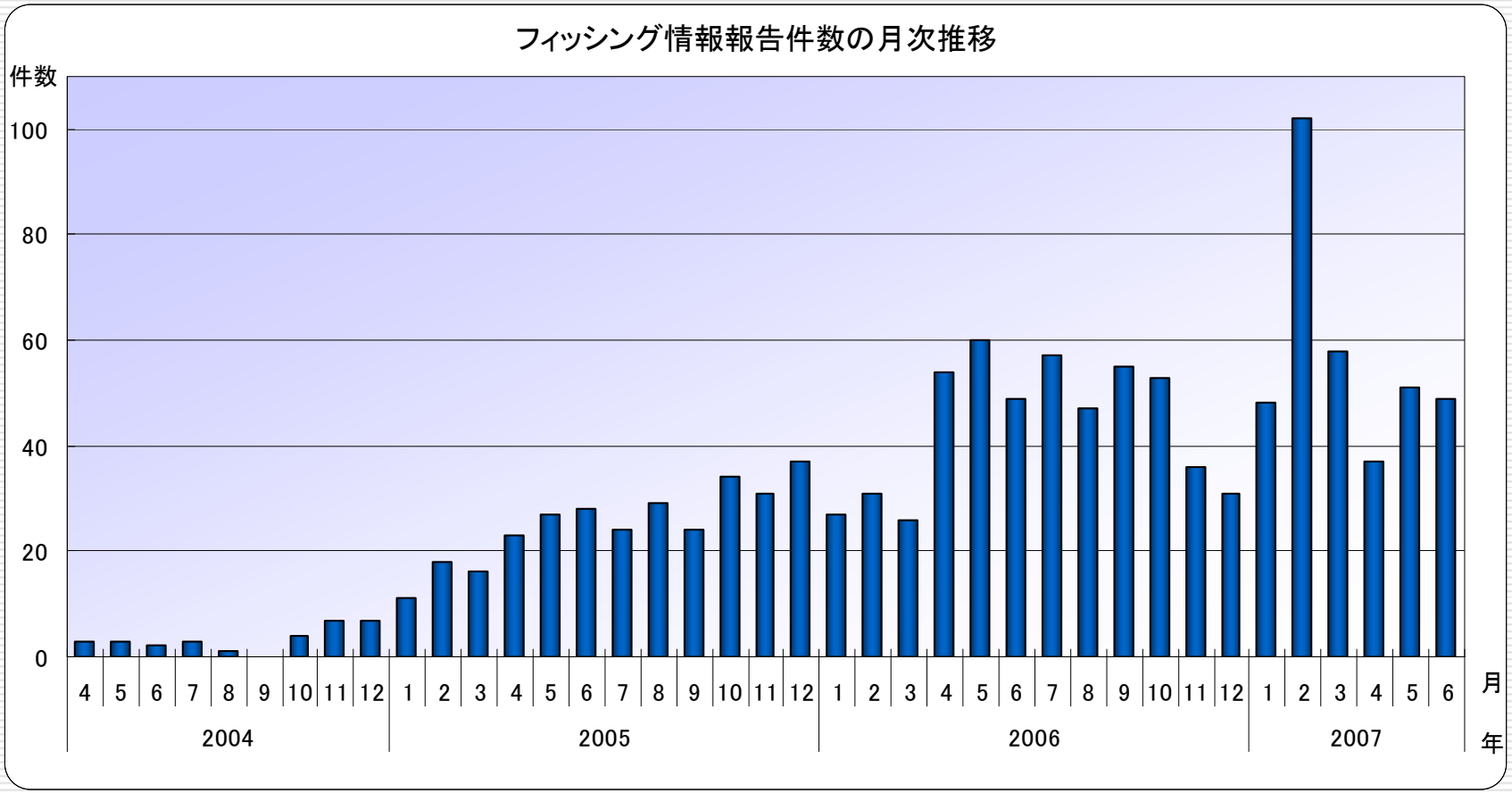
「フィッシングサイト」のコーディネーション

- 2004年4月からコーディネーションを開始
  - 国内、海外からの報告
- インシデントの一形態（不正侵入）として取り扱う
- 該当サイトの連絡先を探して通知
  (whois データベースを使用)



管理者の意図しないページ公開の停止依頼

フィッシングサイト報告件数（月別）



フィッシングサイト閉鎖事例1

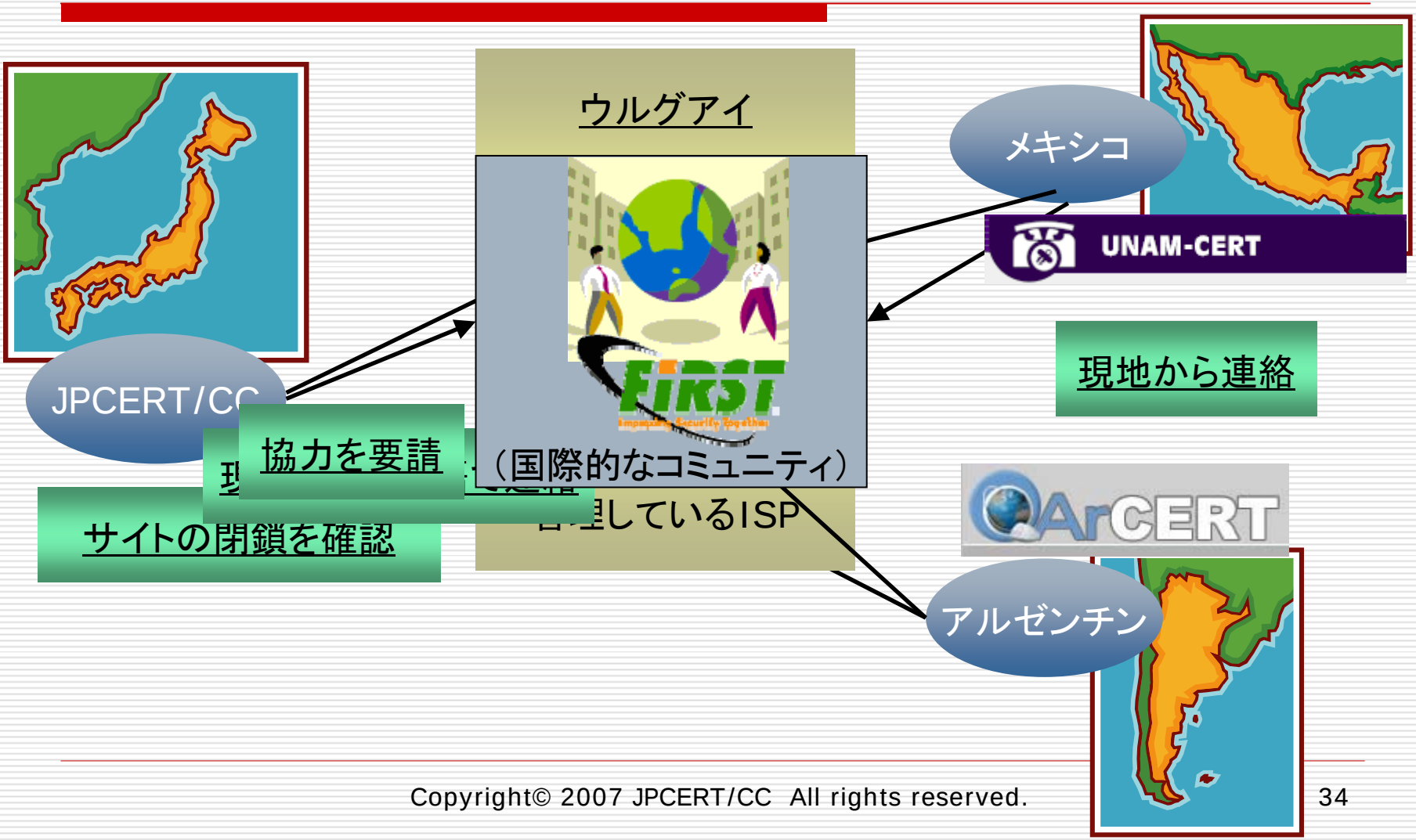
- 2005年3月に韓国、ポーランド、ウルグアイに開設されていたUFJ銀行のフィッシングサイトを閉鎖した事例を紹介します

  - 2005年3月19日付
    - 日経新聞 朝刊
    - NIKKEI NET

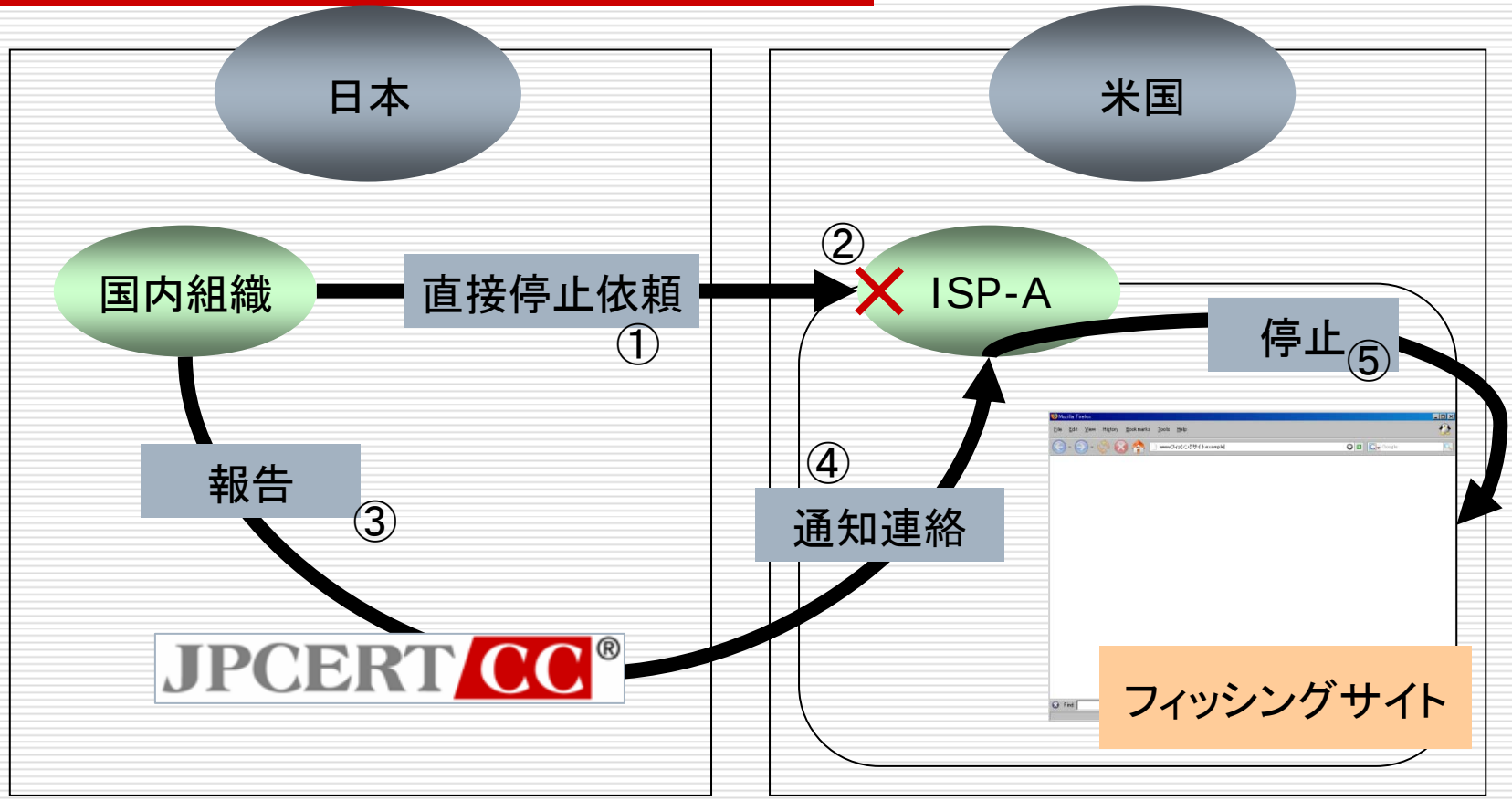
フィッシングコーディネーション事例

- 2005年3月：UFJ銀行のフィッシングサイトのURLが日本国内からJPCERT/CCに報告される
  - 3ヵ国：韓国、ポーランド、ウルグアイ（Whois を使用）
- CSIRTの国際連携ネットワークを活用しJPCERT/CCから韓国、ポーランドへ連絡
  - 韓国KrCERT/CC
    - 4時間後に停止を確認
  - ポーランドCERT Polska
    - 20時間後に停止を確認
  - ウルグアイは…？

フィッシングコーディネーション（続き）



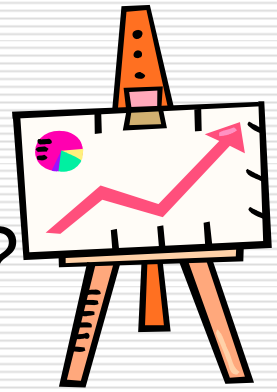
インシデント対応事例2
（フィッシングサイト閉鎖コーディネーション）



某A社が直接連絡したが、フィッシングサイトが停止せず
JPCERT/CCへ報告しコーディネーションした結果フィッシングサイトが停止した

国内のフィッシング動向

- 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
- 国内のサーバに侵入されフィッシングサイトにされてしまう
  - サーバ管理者への働きかけが必要
- 自社のフィッシングサイトの可能性は?



フィッシングに関わる国際的な情勢
海外での事例

- 海外事例：フィッシングは ”金融犯罪”
  - 法体制の整備
    → 個人情報の窃盗としての扱い
    → 捜査官へのトレーニングの実施
  - 報告受付体制の整備
    → 米国においてはFBIとUSSSがそれぞれで設置
  - 官民の連携体制の整備
    → リソースの共有、役割の分担など
  - 業界での取り組み

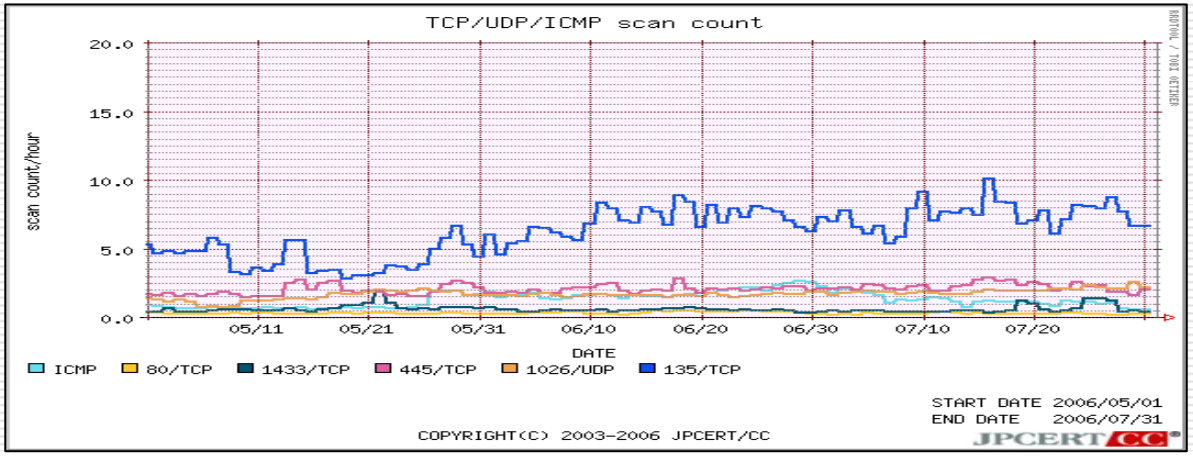
インターネット定点観測事業

- インターネット定点観測システム

  ISDAS：Internet Scan Data Acquisition System

  http://www.jpcert.or.jp/isdas/

- インシデントの早期把握のための観測および情報提供
  - 定期的なセキュリティ予防情報の提供
  - 異なる監視・観測アプローチをとる定点観測および広域モニタリング間での情報共有により精度の高い情報共有



ISDAS 概論

理念

- インターネット上に何が起きているのか、リアルタイムの状況や兆候を把握することができれば未然に対応することも可能になるのではないか？

概説

- ISDAS ではスキャンパケットの観測を目的
- 各センサーが記録したログ情報を元に、公開グラフを生成

ISDAS システム概要

SCAN

SCAN

SCAN

SCAN

Internet

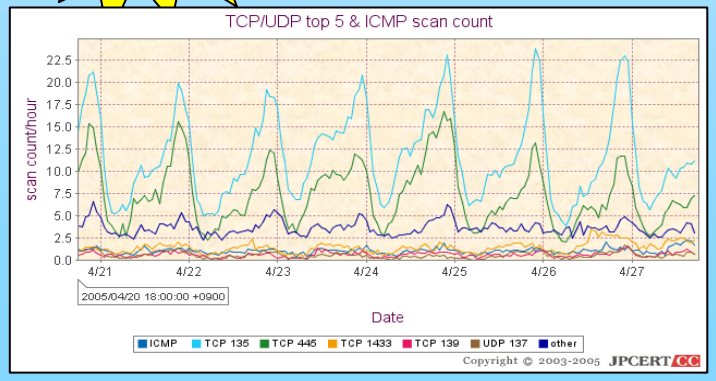
REPORT

REPORT

REPORT

REPORT

センサー群



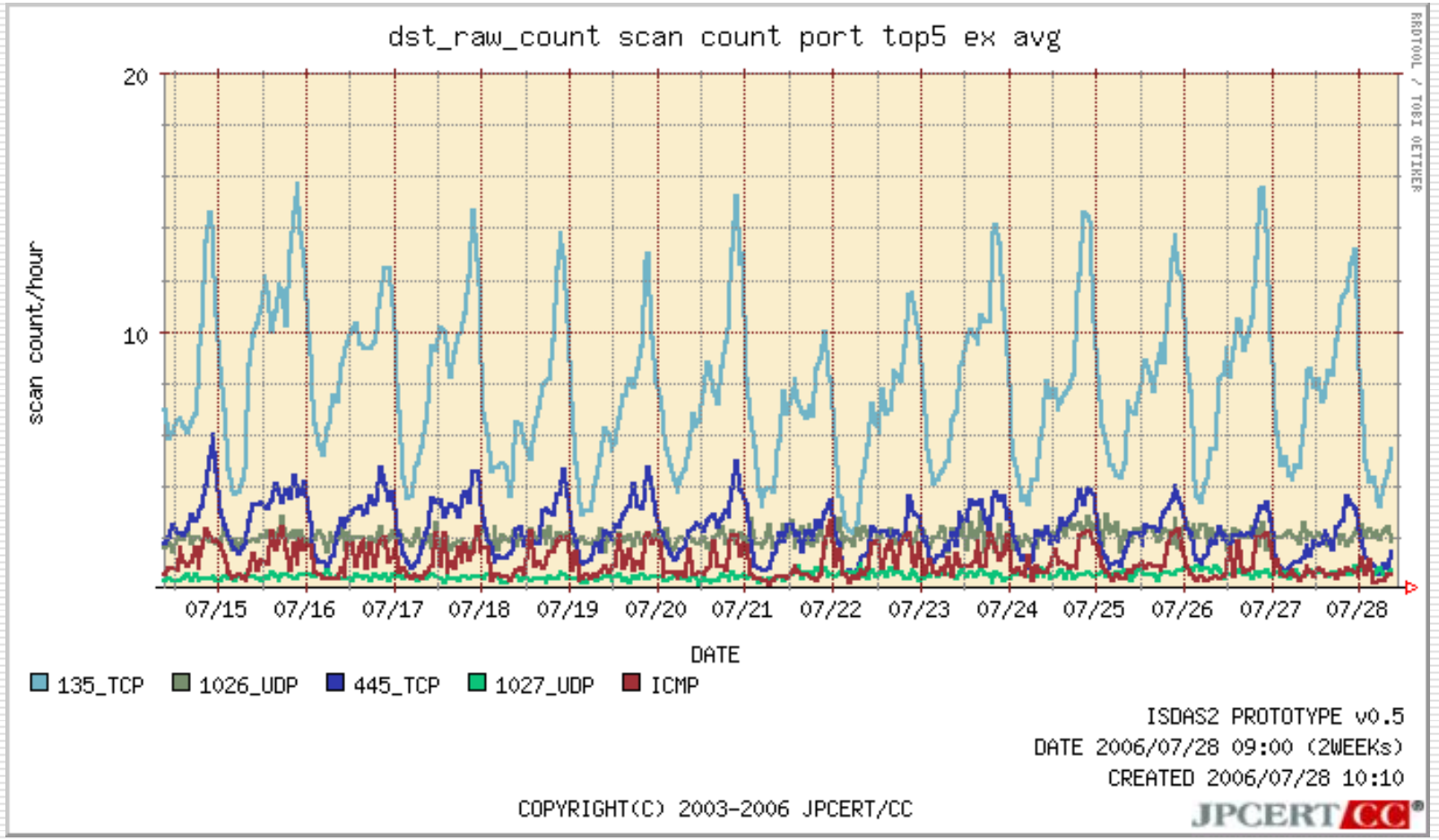
ISDAS
システム

センサーとは?

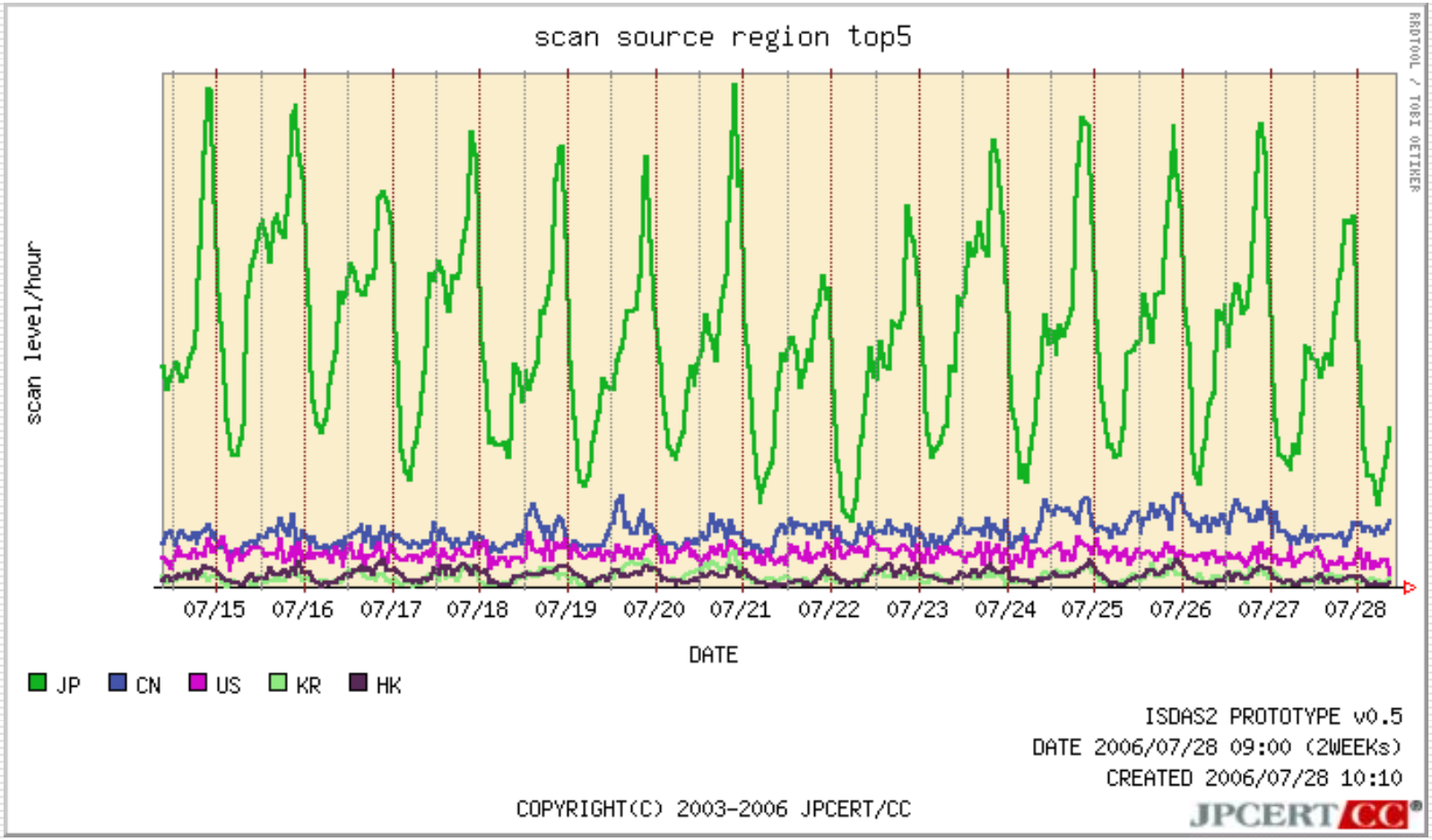
- インターネットから来るスキャンパケットを収集しISDASシステムへ送信しているbox
- センサーが収集している情報
  - 時刻
  - プロトコル(TCP/UDP/ICMP)
  - 送信元IPアドレス
  - 送信元ポート番号
  - 送信先IPアドレス
  - 送信先ポート番号

センサー (イメージ図)

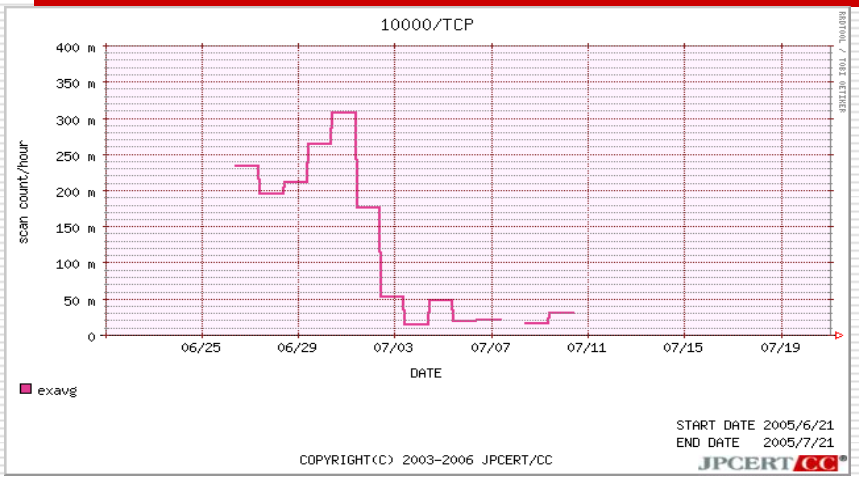
アクセス先ポートグラフ

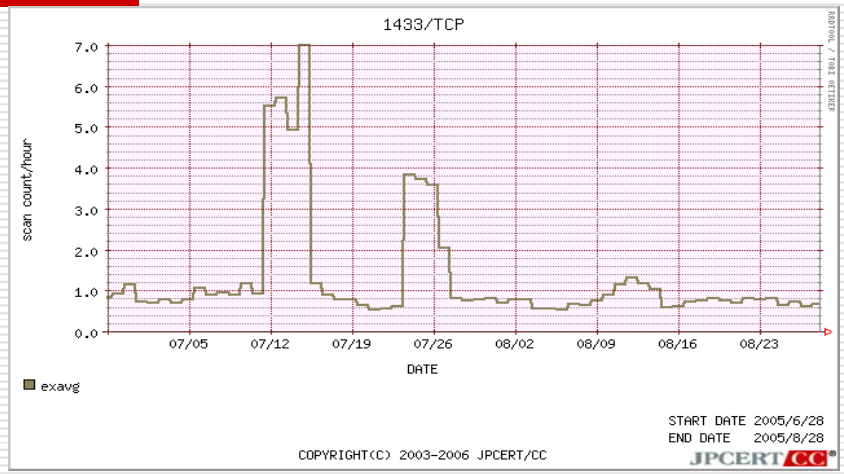


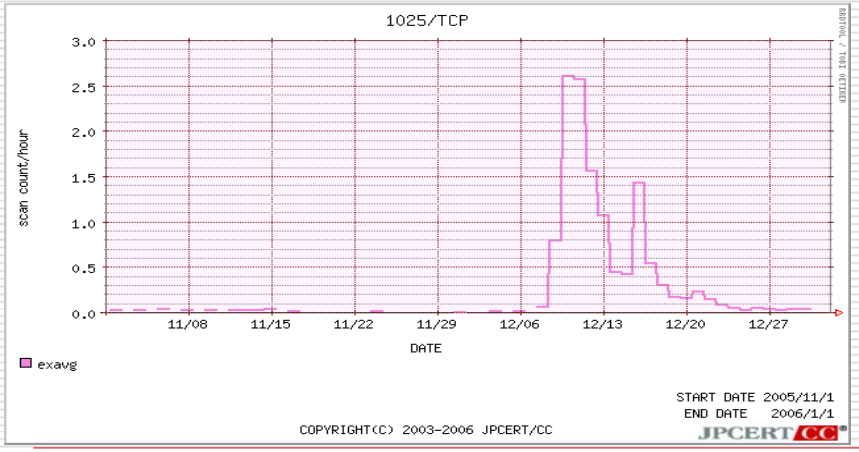
アクセス元地域別グラフ

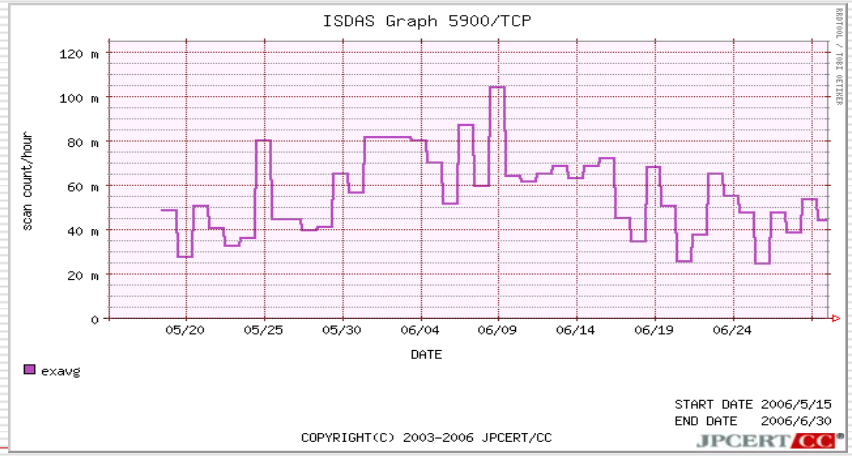


ポート別グラフ









収集データの利用方法

- Web を通じたグラフによる情報公開

  http://www.jpcert.or.jp/isdas/

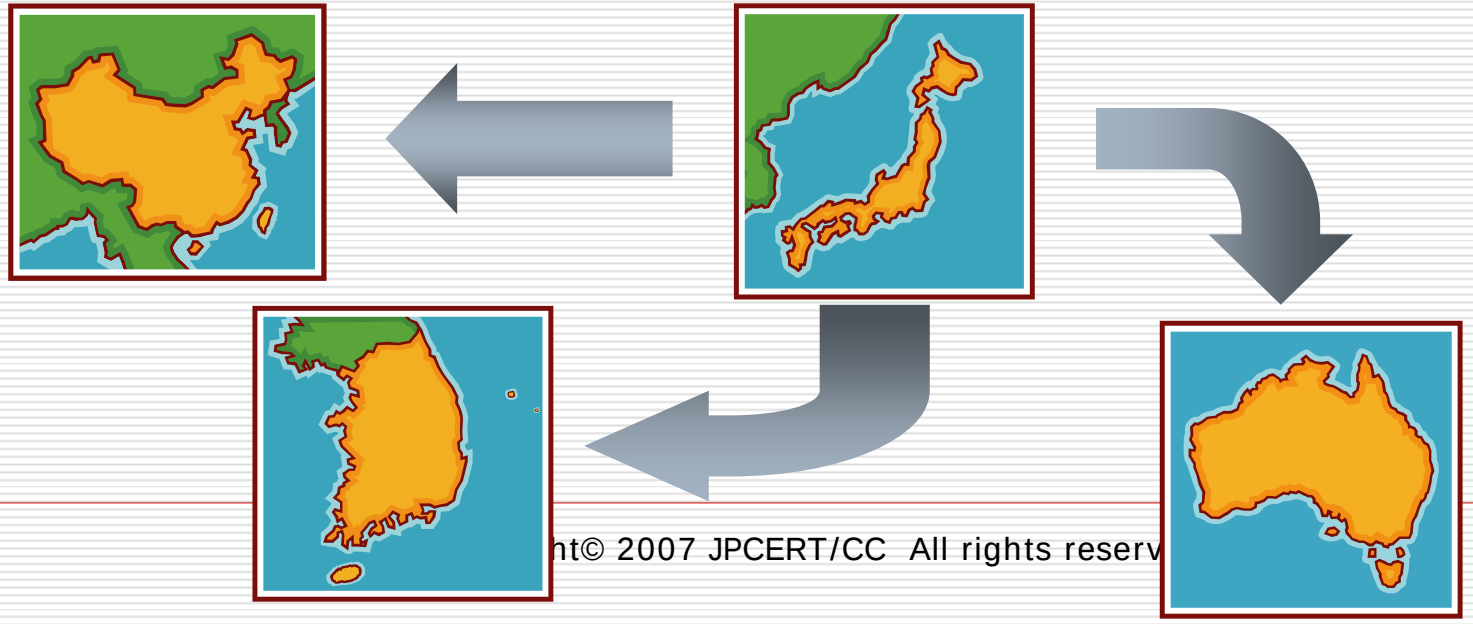
- 注意喚起等公開情報発行時の参考資料
- IODEF形式にて海外CSIRTへの情報連携

  ※IODEF：Incident Object Data Exchange Format の略でインシデント情報を交換する際に利用可能なXMLフォーマット

- 他の定点観測事業者との情報共有
  - 警察庁　サイバーフォースセンター
  - 情報処理推進機構（IPA）　セキュリティセンター
  - インターネット早期広域攻撃警戒システム「WCLSCAN」
  - Telecom-ISAC Japan　など

ISDASデータ:
中国・韓国・オーストラリアへの情報連携

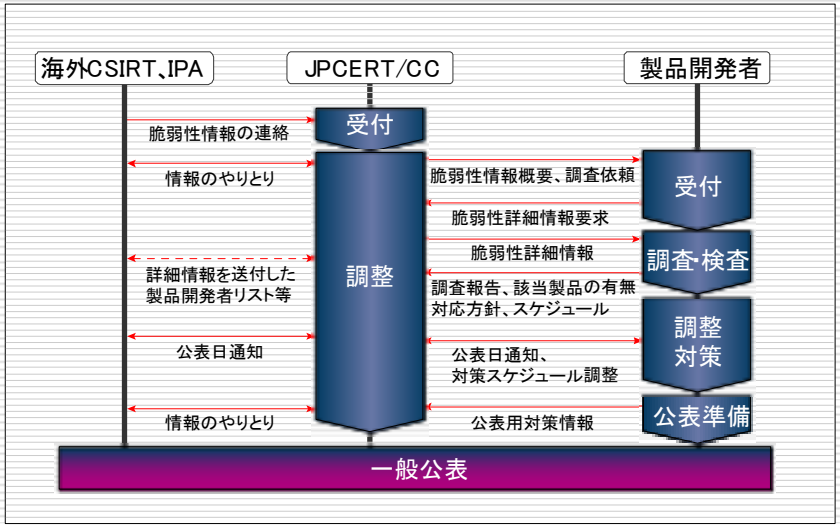
- ISDASにて収集した各国発のスキャンデータをIODEF形式で送信
  - 1日分を毎日送信
  - src_ip, src_port, dest_port, protocol timestamp を送信
  - 各国にて情報分析・インシデントの対応に利用



脆弱性情報ハンドリング事業

- 「ソフトウェア等脆弱性関連情報取扱基準」（2004年7月：経産省告示）認定調整機関
  - 登録開発ベンダ向けに、脆弱性関連情報を提供し対応依頼
  - 国際的に情報公開日を調整

JPCERT/CCとの製品開発者のハンドリング　（やり取り）フロー図

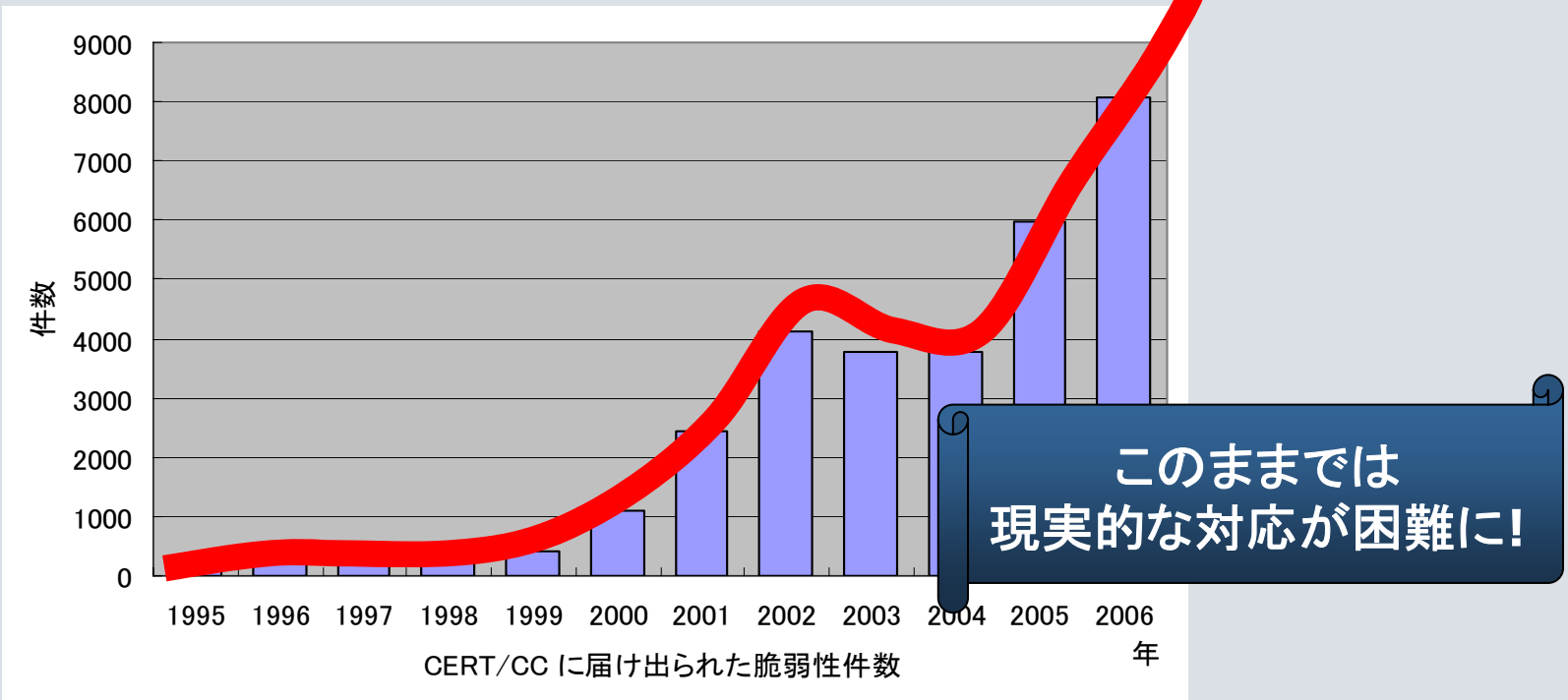


情報提供サイト
JVN（Japan Vulnerability Notes）

JVN Japan Vulnerability Notes

http://jvn.jp/

- 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

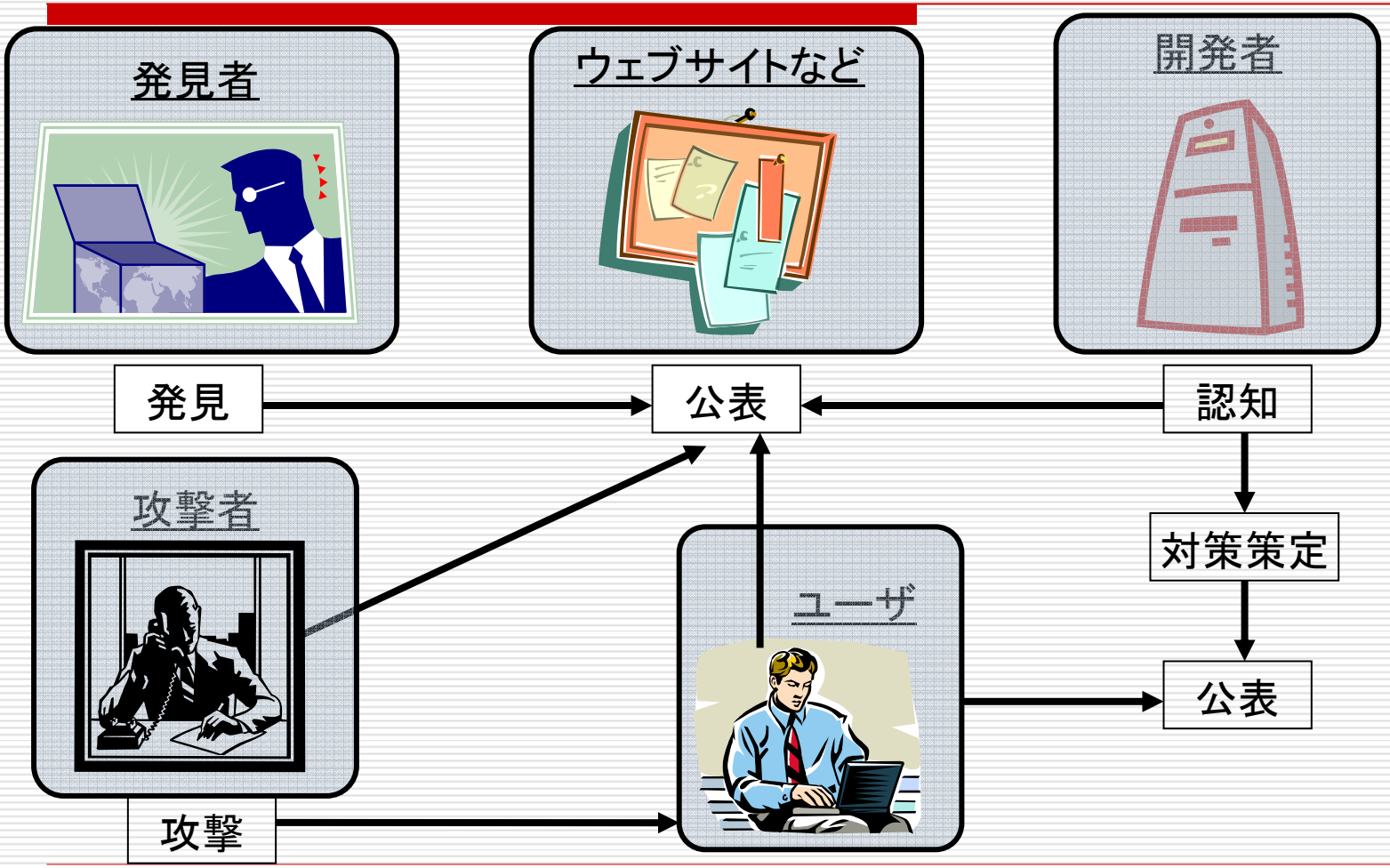
- 全ての攻撃に備えることは不可能
  - 日々新たな攻撃手法が出現
- 開発が大規模になればなるほど、既知の脆弱性対策の反映が困難
  - 脆弱性情報の収集と取り纏め
  - 外部委託先での管理
- 製品に脆弱性が発見された場合に、ユーザに不安を与えず、冷静に対処してもらうことが重要

情報公開の姿勢と仕組みが必要

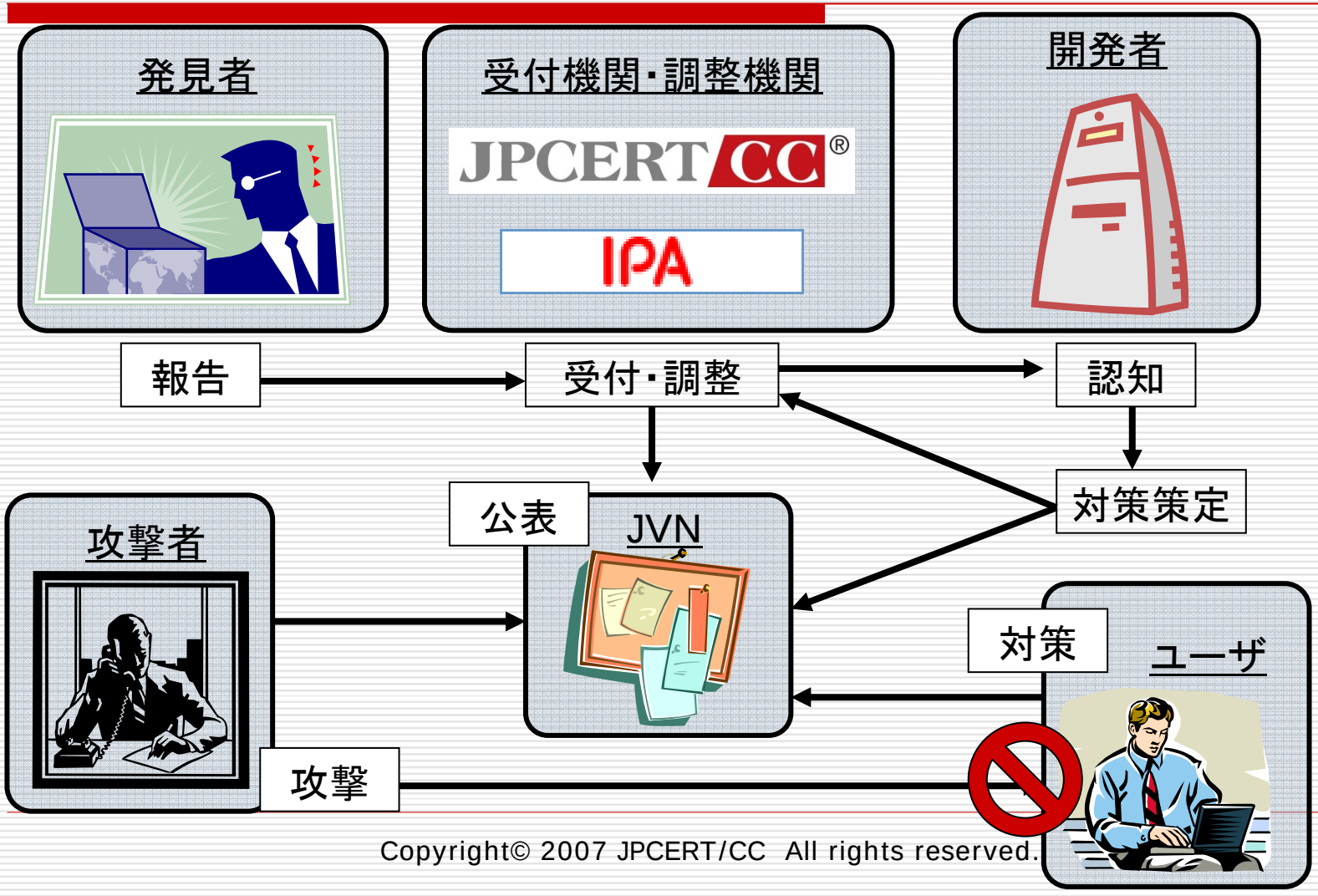
― JPCERT/CCの脆弱性情報ハンドリング ―
情報セキュリティ早期警戒パートナーシップ

- 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されている
  - 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

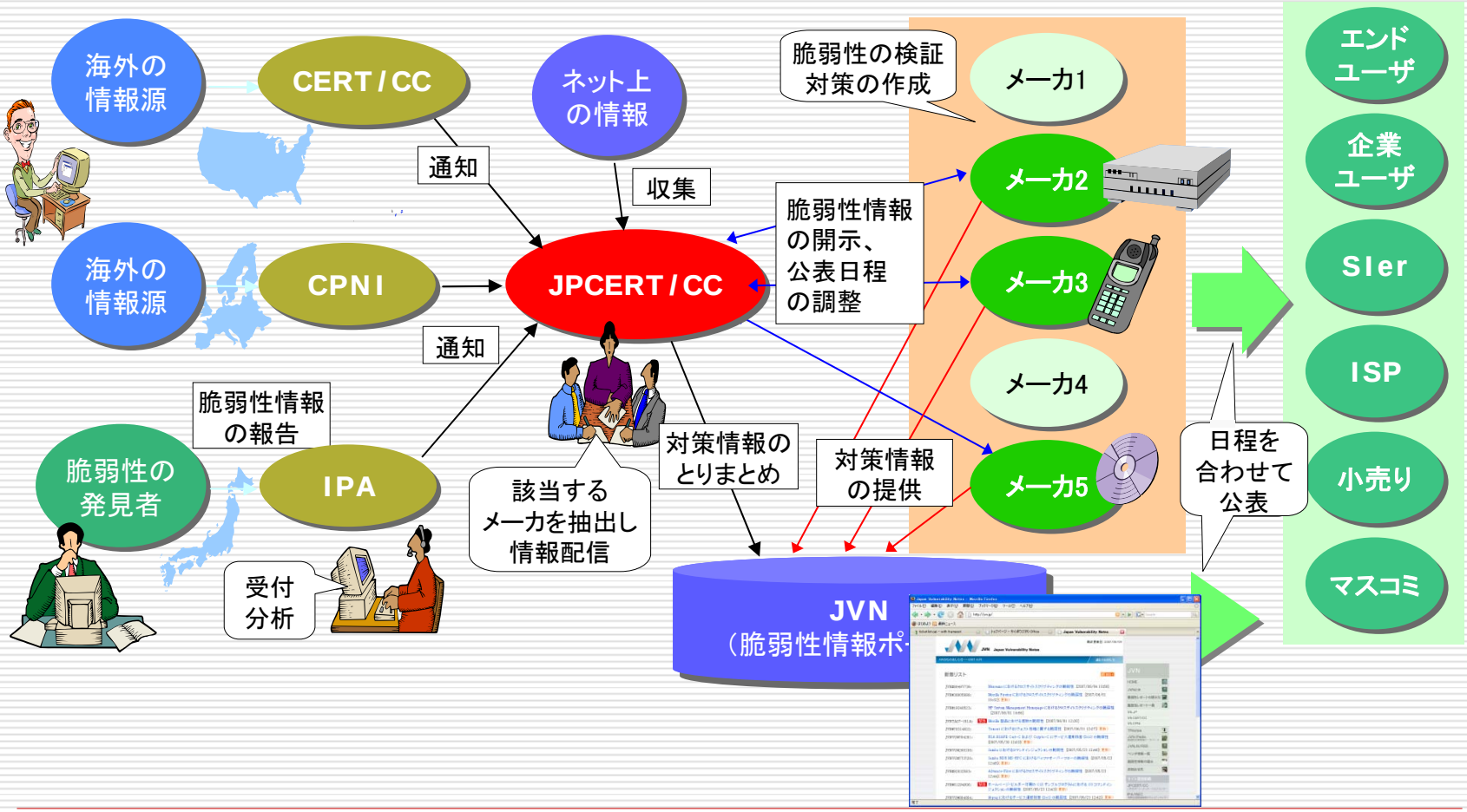
脆弱性情報ハンドリング開始前



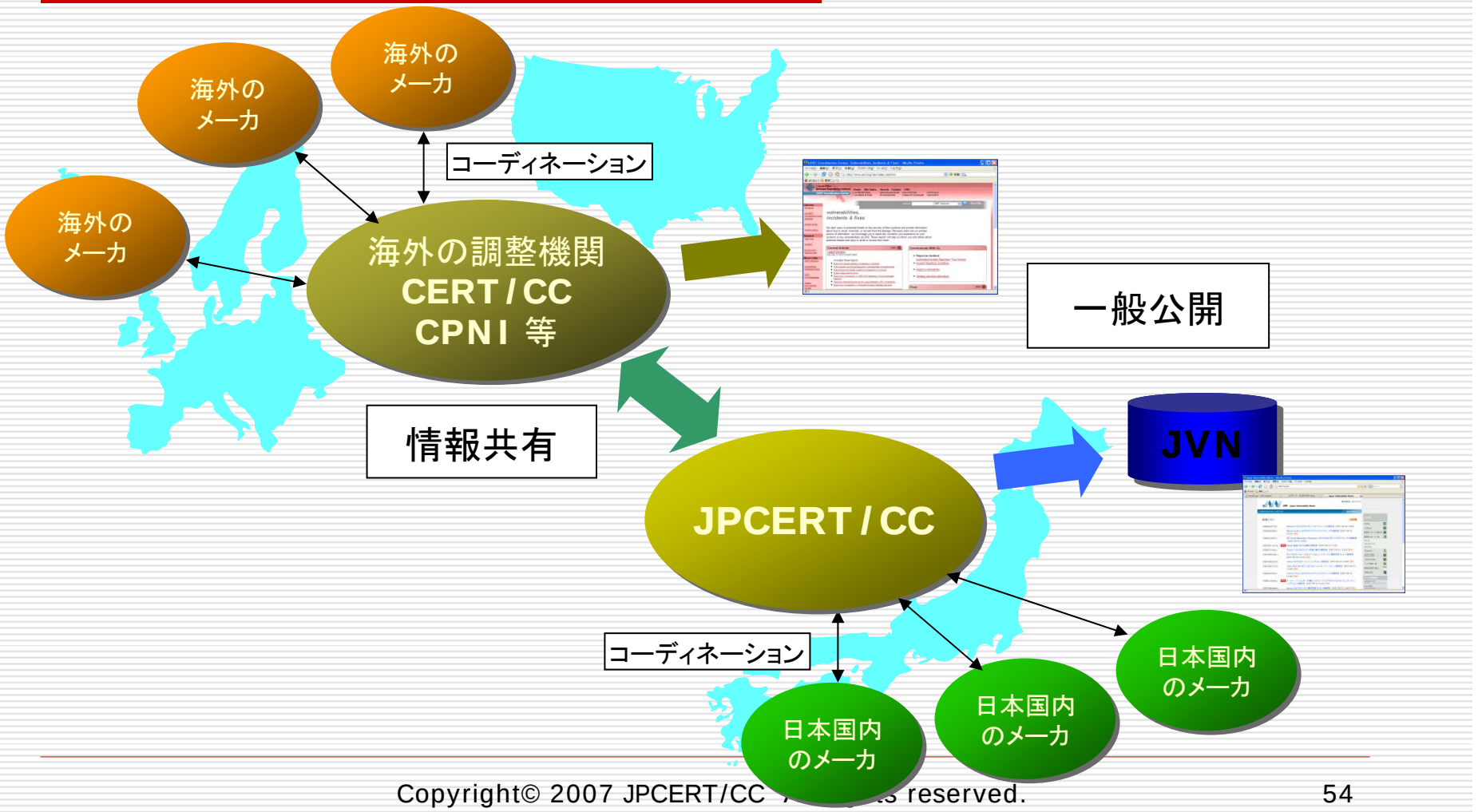
脆弱性情報ハンドリング開始後



― JPCERT/CCの脆弱性情報ハンドリング ―
脆弱性情報流通の枠組み



― JPCERT/CCの脆弱性情報ハンドリング ―
国際的な枠組みについて

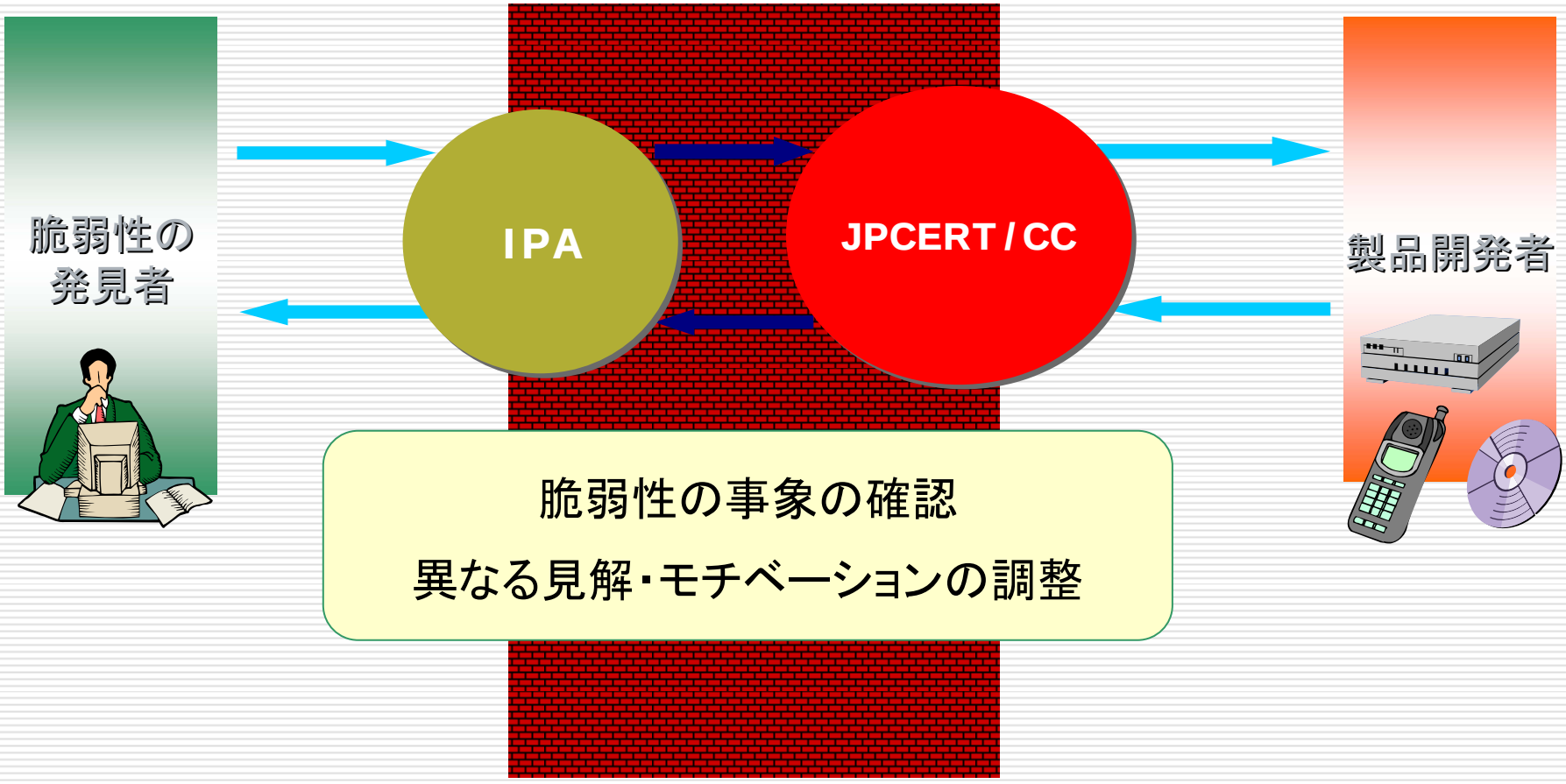


JPCERT CC®

― JPCERT/CCの脆弱性情報ハンドリング ―
脆弱性情報の一般公開の調整

- 隠しておくのは得策ではない
  - 情報公開により、脆弱性をユーザに周知し、対策の適用を促す
  - いずれ悪意の第三者が脆弱性を発見し、攻撃に利用される可能性
- 「公表日一致の原則」の遵守
  - 脆弱性情報と、対策情報を同時に公開する
  - 脆弱性の影響を受けるすべての製品開発者が同時に情報公開する
- すべての関係者が同時に情報公開するよう日程調整
  - 脆弱性の影響を受ける製品を開発するすべてのベンダ
  - 海外の調整機関や製品開発者を含む
  - 発見者の要望が影響する場合もある

― JPCERT/CCの脆弱性情報ハンドリング ―
発見者と製品開発者の間の調整

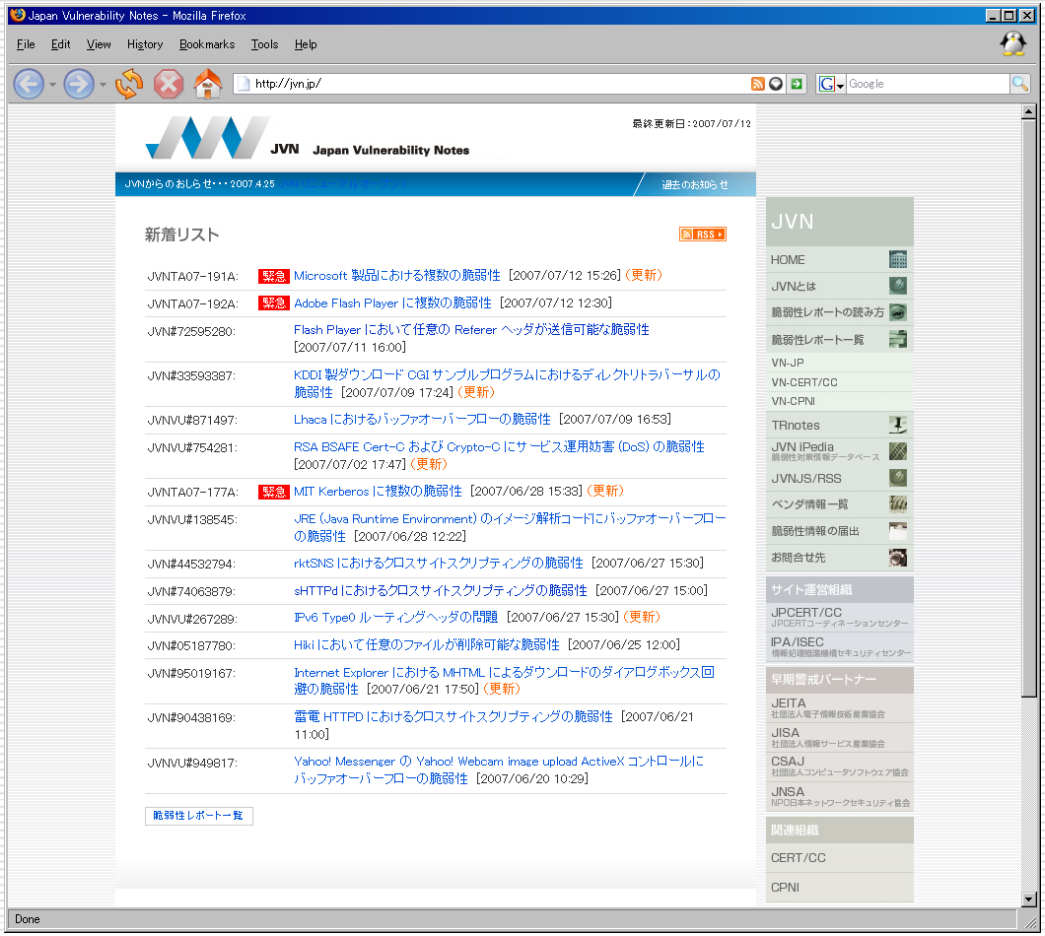


JPCERT CC®

ー JPCERT/CCの脆弱性情報ハンドリング ー
製品開発者にとってのメリット

- 製品に関係する脆弱性情報を早期に入手し、一般公開前から余裕をもって対応を始めることができる
- 脆弱性情報の公開と同時に対策情報を公開することで、ユーザへの影響を低減できる
- 製品開発者間の調整、発見者との調整を、中立な第三者機関（JPCERT/CCとIPA）がおこなう
- 脆弱性情報・対策情報の告知媒体として、JVNを利用できる
  - http://jvn.jp/

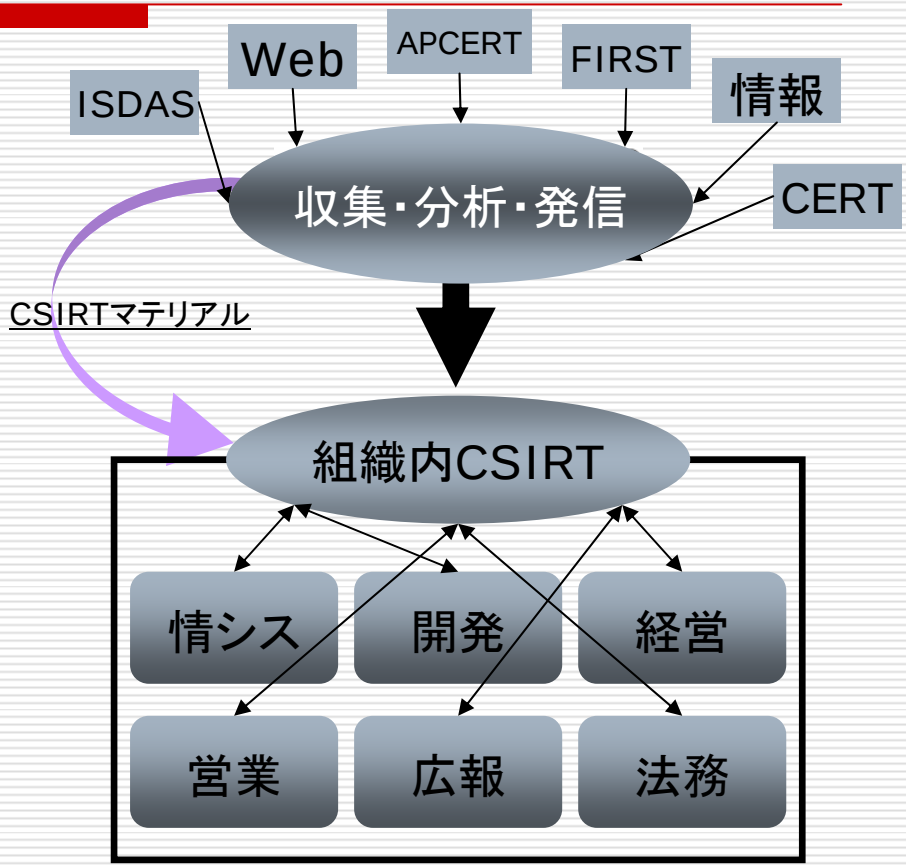
http://jvn.jp/



早期警戒

早期警戒活動

- 国内の重要なポイントへの分析情報の発信と組織内対応体制の構築・活動支援
  - 一般への告知
  - 国内のCSIRTs
  - 国内の重要インフラ事業者
- 情報の
  収集・分析・発信
- CSIRT 構築・活動支援
  - 組織内対応体制構築の支援
  - CSIRTマテリアルの提供
  - CSIRT協議会の運営



組織内における円滑なインシデント対応

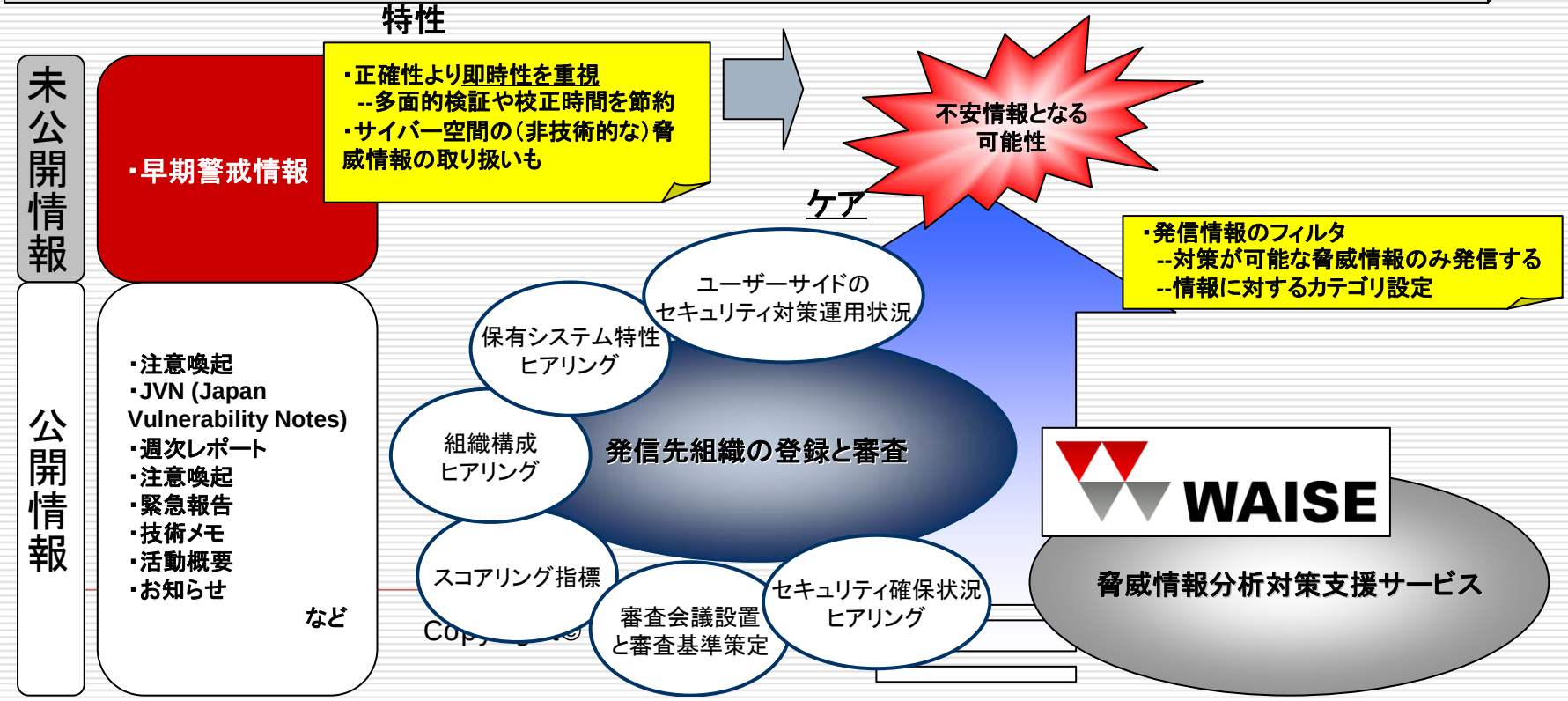
“Watch and Warning” 情報収集・分析・発信

- さまざまなポイントからの継続的かつ網羅的な情報収集
  - 国内外関係組織から得られる情報
  - Webで一般公開されている情報
- JPCERT/CC内部の分析機能を活用した情報分析
  - 脆弱性分析
  - マルウェアやフィッシングサイトなどの解析
  - リスク分析
- 一般情報公開のほか、特定の組織、組織内CSIRTへの情報発信
  - 一般への注意喚起情報の発信
  - 特定組織への早期警戒情報の発信
  - Weekly Report の週次発行
  - その他

早期警戒情報提供スキーム

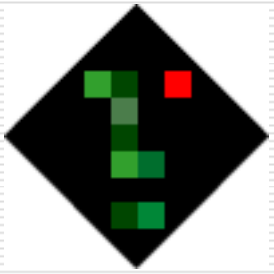
早期警戒情報の特性を踏まえた登録審査とWAISE(仮称)との関係

1. 不安情報とならないための方策
2. 発信効果を最大化するための方策
3. 利活用を促進させるための方策



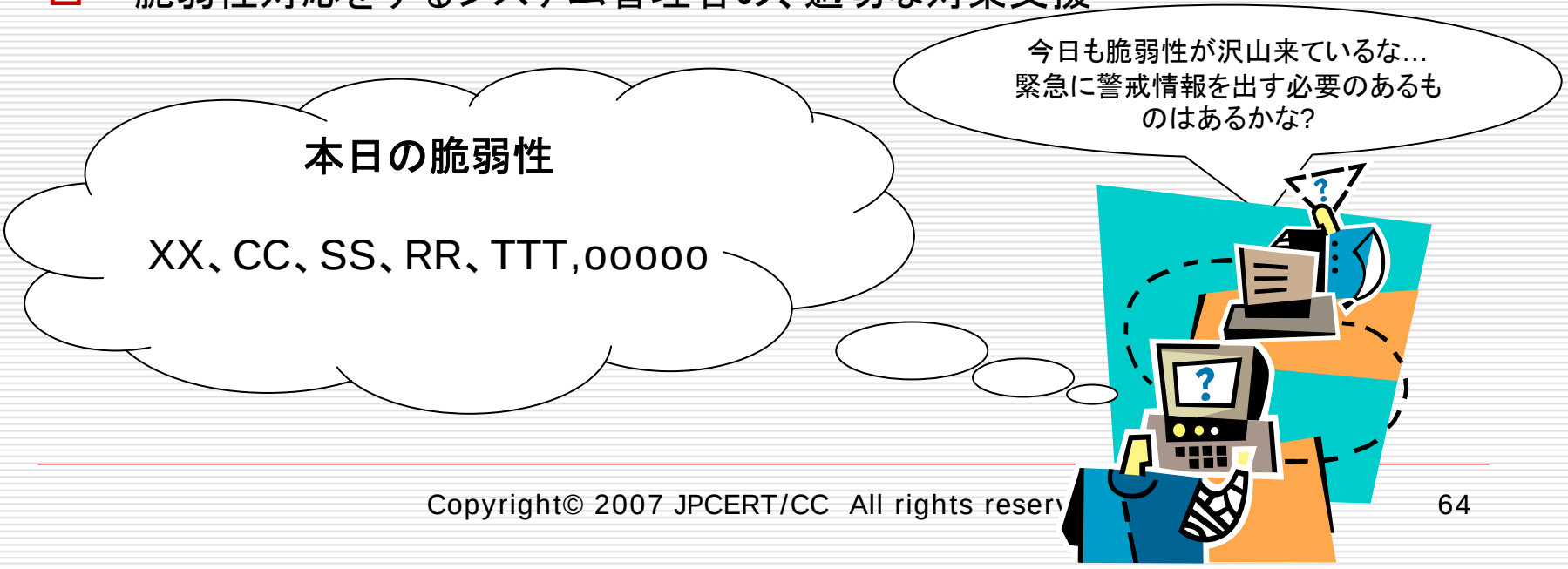
組織内における脆弱性対応のサポート

- **KENGINE**プロジェクト
  - 米国CERT/CCとJPCERT/CCによる、2005年度共同プロジェクト
  - ツールのコンセプトを共同企画し、システム仕様をCERT/CCが担当、実装(ツール開発)をJPCERT/CCが担当
  - 2006年度、拡張仕様の策定
  - 2007年度、実装と運用開始



このプロジェクトの発端となった問題

- 組織の限られたリソースの中で、年間8000件以上収集される脆弱性にどのように対応すべきか？
  - 以下のような問題設定として考える:
    [d1] そもそも対応すべきなのか？
    [d2] 対応するとすればどのような対応をすればよいのか？
- 優先順位をつける際、一貫した判断基準に結びつく分析、理由付けが必要
- 脆弱性対応をするシステム管理者の、適切な対策支援

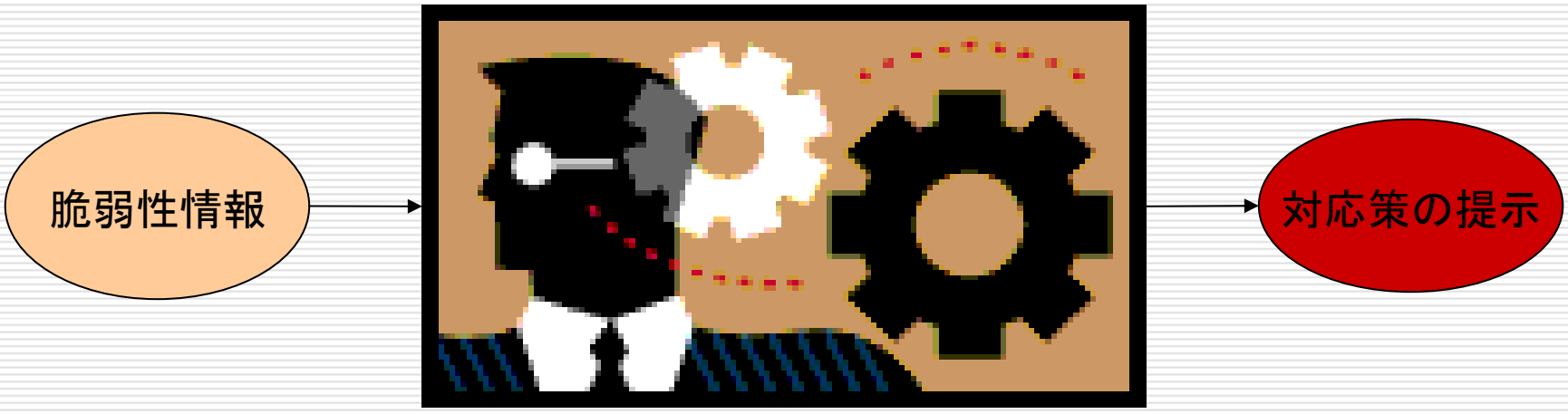


脆弱性脅威度スコアシステムは巷に多数あるが

- 全てのユーザーに、脅威度をスコアする計算式(アルゴリズム)がひとつはおかしい。
  - 例えば脆弱性の事実情報に関しても、その重みはユーザー別に異なるはず
    - 侵入よりもサービス妨害が最も脅威である組織
    - バッファーオーバーフローについては、別途回避対策導入している組織
    - 内部の信頼できる組織のスタッフがローカルアカウントのみでシステムにアクセスしている組織
- 数字で点数を出すこと、色分けなどの意味
  - 自分の組織に置ける脅威度を測らずに、平均値数で対応が取れるのか。
    - スコア7.0 = 具体的な対策は? 7.0とはどういう意味か?
    - 脅威度中 = どういう意味? どんな対策を取ったら良いの?

KENGINEとは

- 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。
- 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。

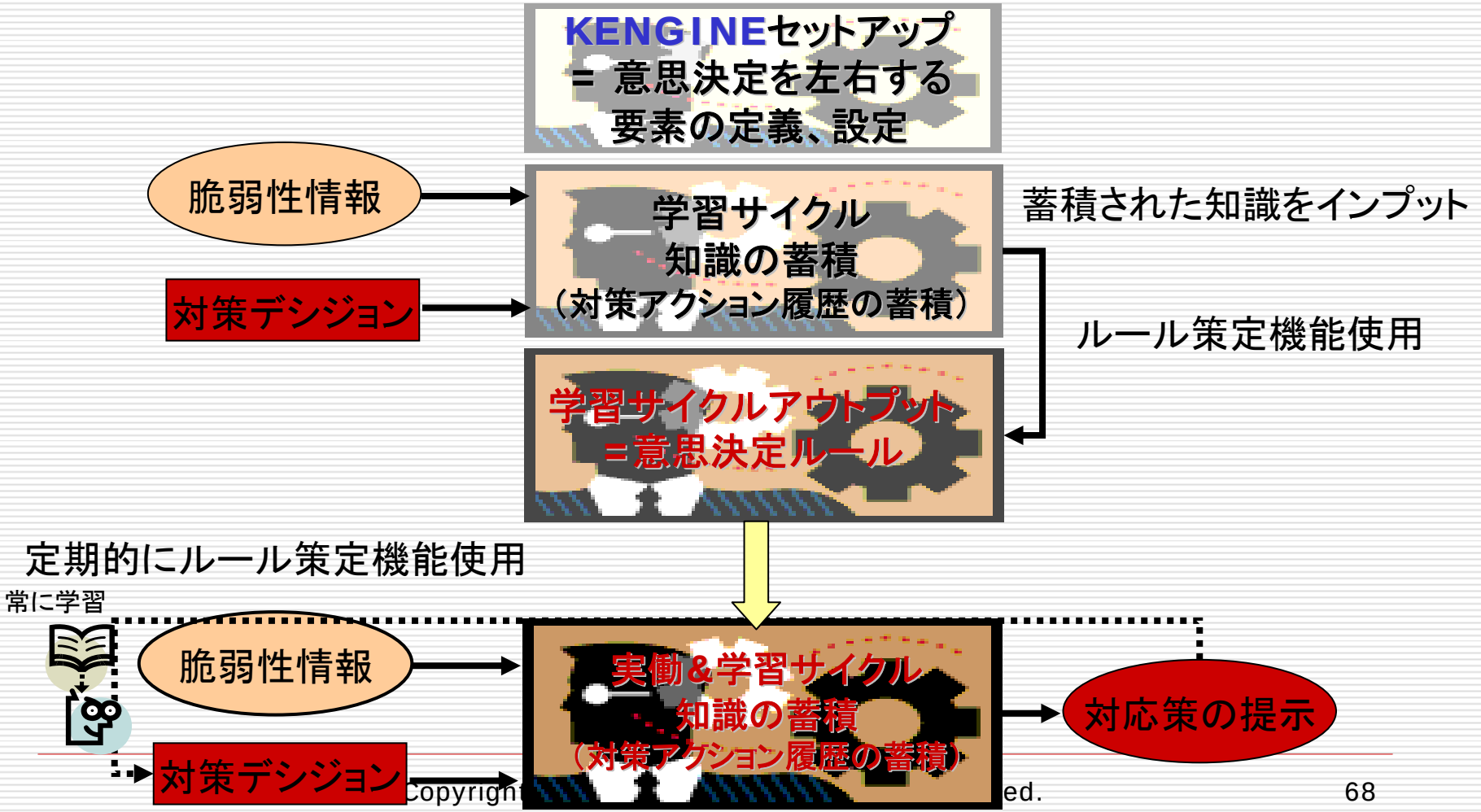


KENGINEツールの効果

- KENGINEは、組織として一貫性のある脆弱性情報の分析と適切な対策アクションを提示する

- その結果
  - 判断の一貫性の確保する
  - 意思決定の質を向上させる
  - 対応の判断を容易に下せるようにすることで、最小限の努力で多数の脆弱性を扱えるようになる

KENGINEの使い方：全体像
セットアップステージと、ラーニングサイクル



分析者の頭のロジックをシステム化:
KENGINEセットアップ

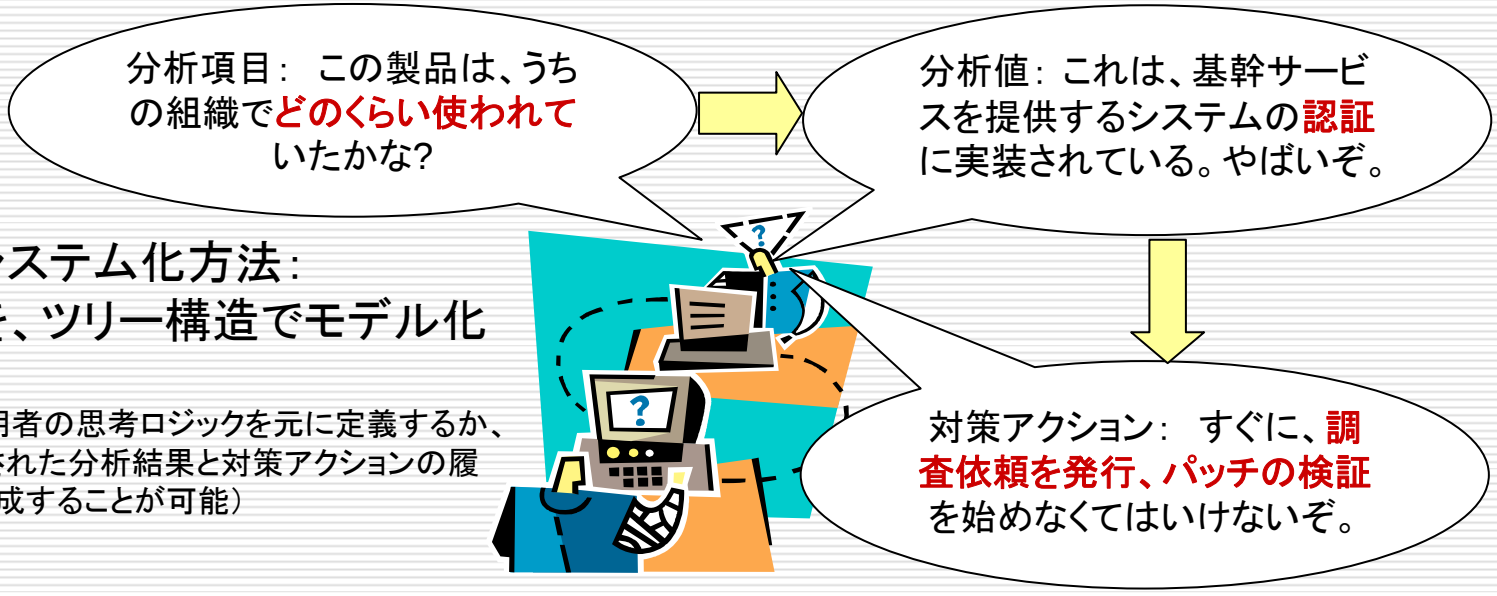
脆弱性情報が入ってきた際、分析対策担当者が考慮している意思決定を左右する要素をダンプしてシステム化する。

具体的なシステム化方法:
KENGINEカスタマイズ設定者が、脆弱性を通常取り扱う分析者(システム管理者など)から、ヒアリングを行い、意思決定を左右する要素を導出する。

意思決定ルールの策定:
学習サイクル

□ 意思決定ルールとは

- ■ 分析項目(Q&A)、分析値(重み付け)、対策アクションの依存関係のこと



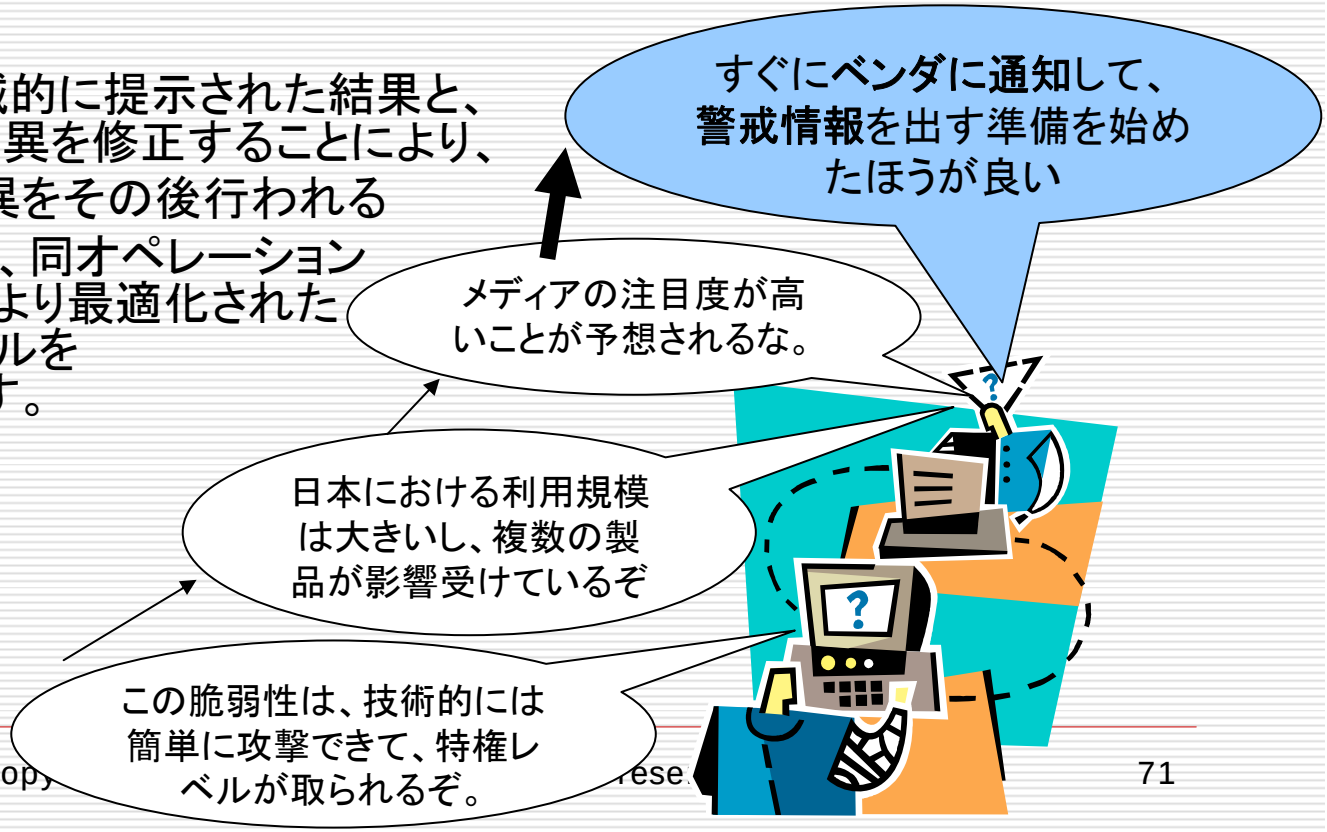
具体的なシステム化方法:
依存関係を、ツリー構造でモデル化する。
(モデル化は利用者の思考ロジックを元に定義するか、あるいは、蓄積された分析結果と対策アクションの履歴を元に自動生成することが可能)

脆弱性分析値から、対策アクションを提示:
実稼動サイクル ＆ 意思決定ルールの最適化

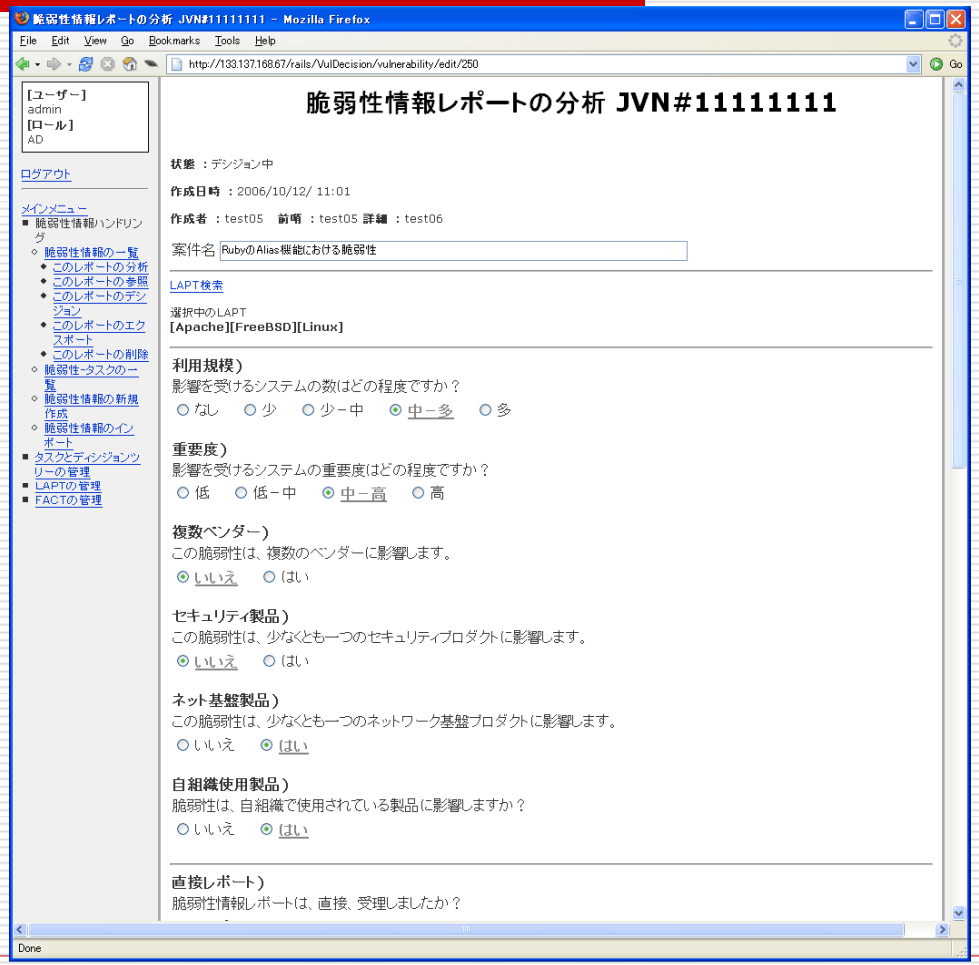
- 導出された分析値は、対策アクションの依存関係を表現したディシジョンツリーによって評価され、その結果として実施することが望ましい対策アクションが提示されます。

例:JPCERT/CCでは

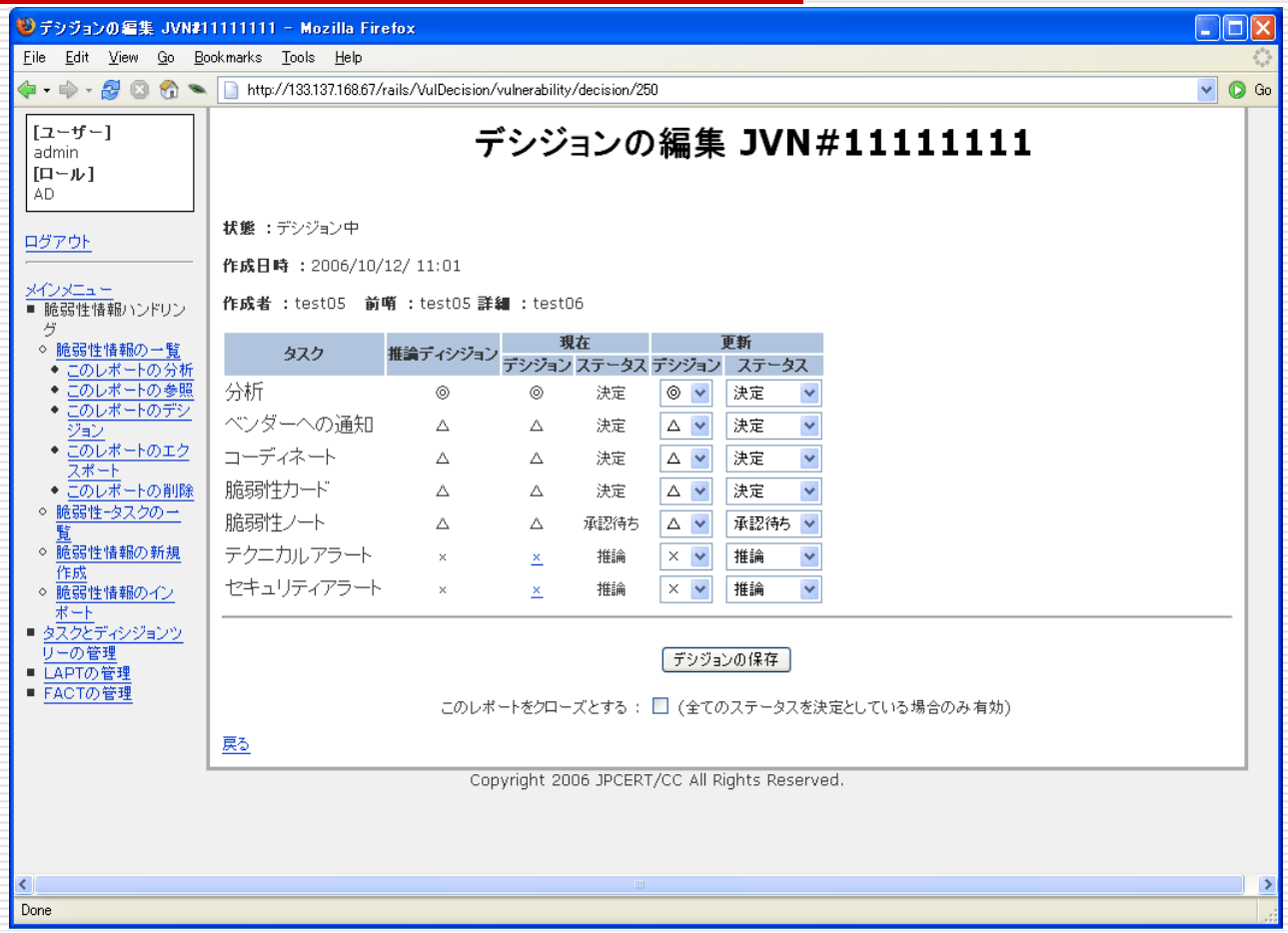
- KENGINEにより機械的に提示された結果と、本来望ましい結果の差異を修正することにより、KENGINEはこの差異をその後行われる推論に反映しますので、同オペレーションを繰り返すことにより、より最適化された推論結果を得るサイクルを実現することができます。



KENGINE画面イメージ
脆弱性情報レポートの分析

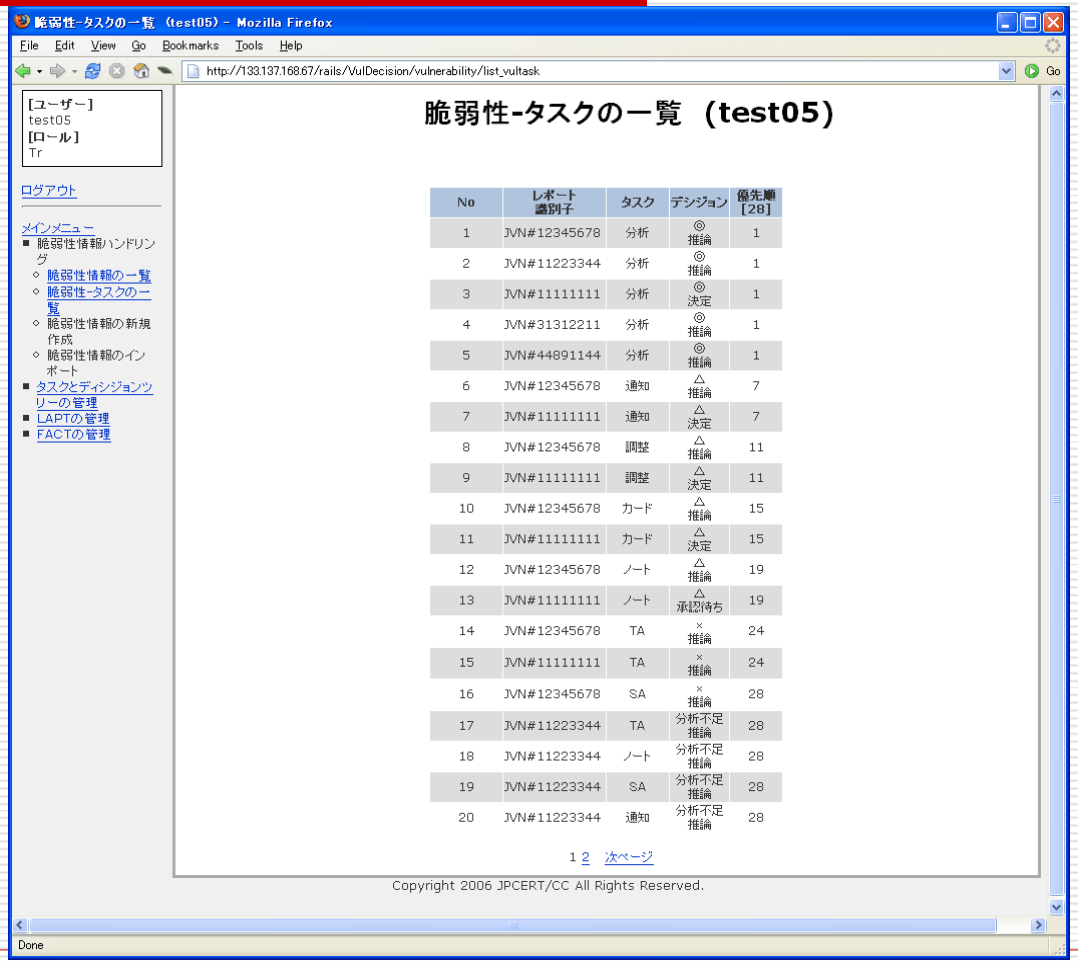


KENGINE画面イメージ ディシジョン



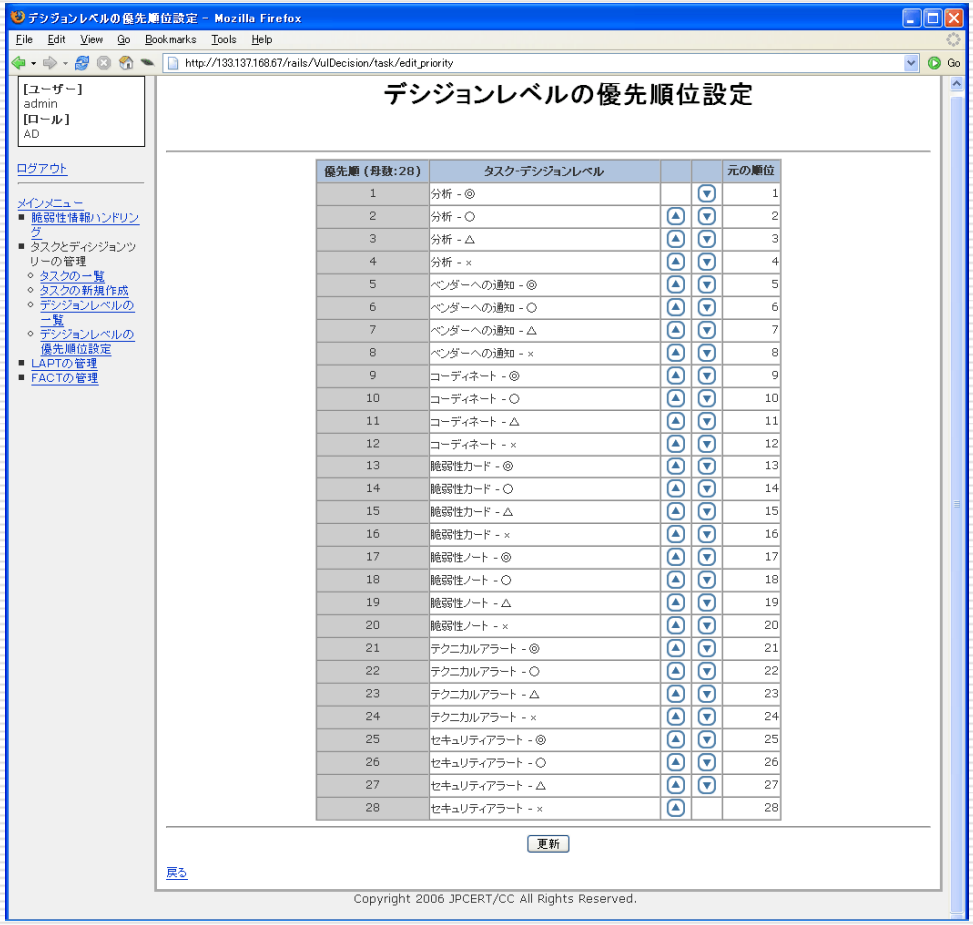
KENGINE画面イメージ
脆弱性情報レポート一覧

KENGINE画面イメージ
優先度でソートされたタスク一覧



KENGINE画面イメージ
タスクの一覧

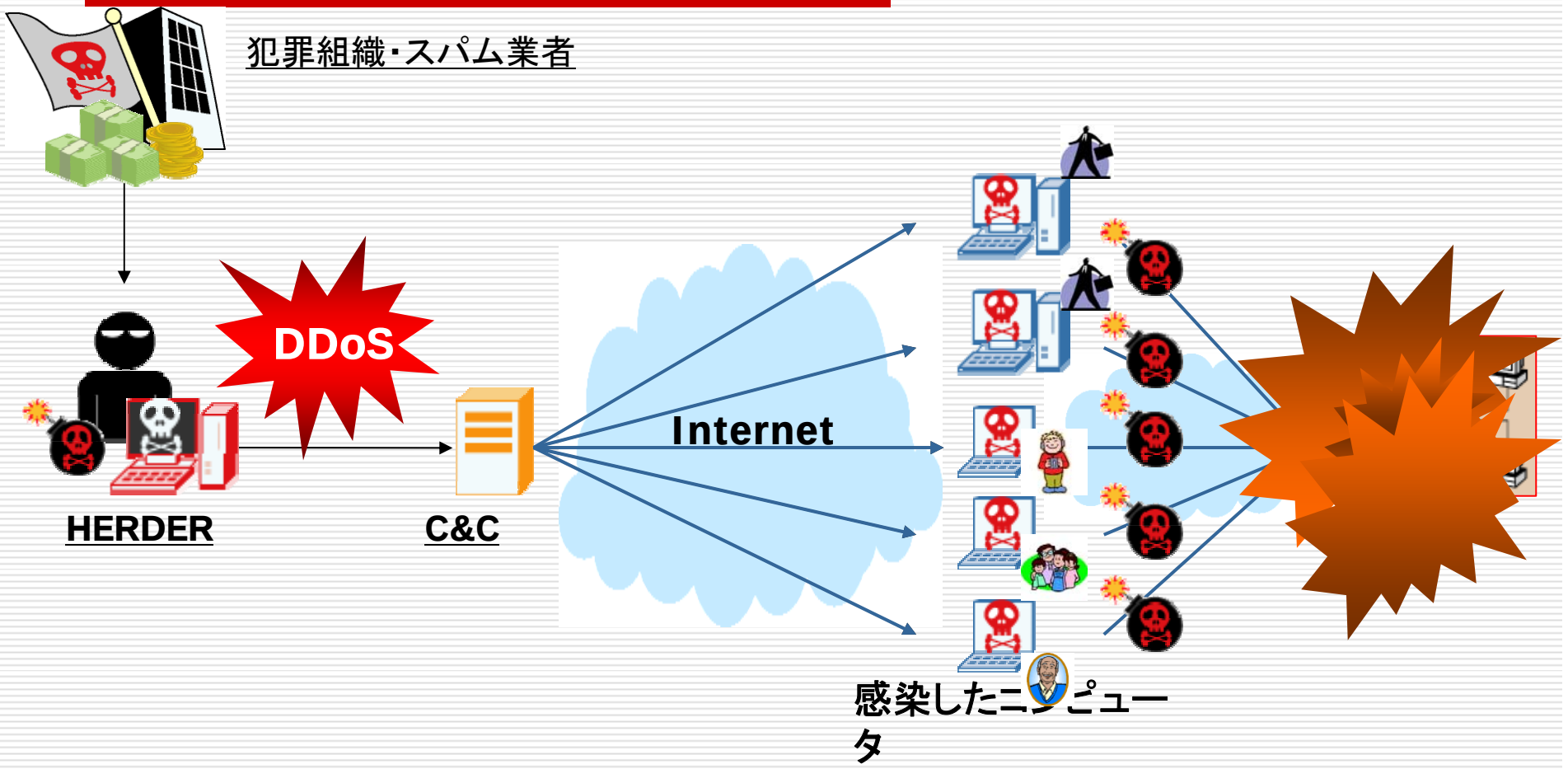
KENGINE画面イメージ
タスクの優先順位設定



ボットネット対策

- ボットネットのおさらい
- 脅威の変化
- JPCERT/CCの取り組み
  - サイバークリーンセンター
- ユーザの対策

ボットネットのおさらい



– ボットネットのおさらい –

ボットとは…

- マルウェア(広義のウィルス)の一形態
  - Malicious Software
  - Robot
- 複数の機能をあわせもつ
  - 感染(脆弱性, 便乗, ソーシャルエンジニアリング, …)
  - 情報収集(アカウント情報, 脆弱なシステムの情報, …)
  - 攻撃(DDoS, スパム, …)
  - 自己防衛(暗号化, 難読化, ”Anti-”技術, …)
  - 遠隔制御・管理(IRC/P2P, バージョンアップ, …)

– ボットネットのおさらい –

ボットネットとは…

- ボットで構成されたネットワーク
  - 指令者によって運用される
    - ハーダー(HERDER)/マスター(MASTER)
    - C&C(Command and Control)
  - 堅牢な分散システム
    - 暗号化・難読化による安全(?)性
    - 冗長化による高可用性
- カスタマイズや管理・運用が容易

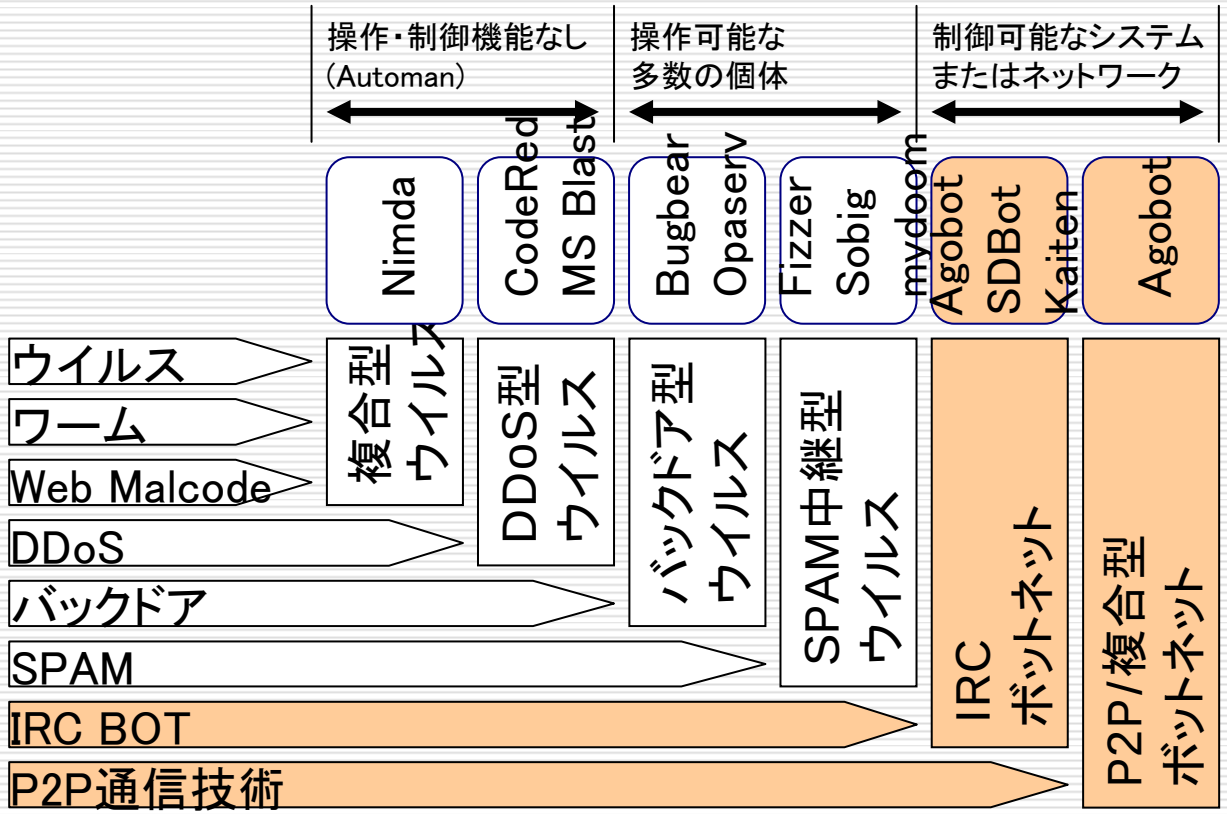
– ボットネットのおさらい –

注目すべき点は?

- 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

マルウェアは本格的な実用段階に

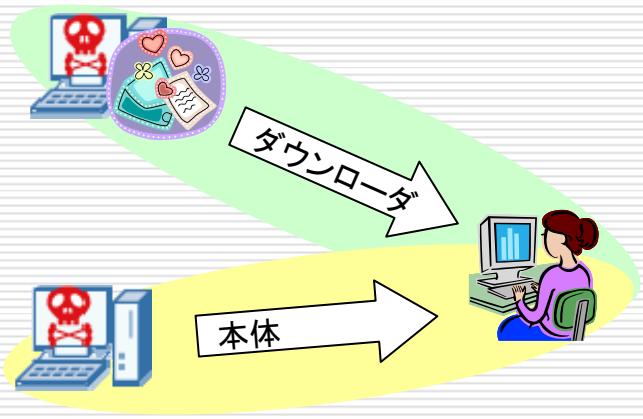
脅威の変化:マルウェアの進化



－脅威の変化－

侵入・感染に使われる技術

- ソフトウェアの脆弱性
- アカウントへの辞書攻撃
- 他のマルウェアに便乗
- ソーシャルエンジニアリング的手法
  - 個人情報や組織内情報の漏洩が温床に



– 脅威の変化 –

自己防衛に使われる技術(1)

- 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
- 暗号化・難読化
  - API呼び出しの変造
    APIを直接呼ばずに専用の関数を実装
  - 文字列のエンコード
    URL等のハードコードされる文字列

– 脅威の変化 –

自己防衛に使われる技術(2)

- “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

－脅威の変化－

最近の傾向

- 技術の複合化
  - 「より大きな脆弱性」=「人」への流れ
    - 一般利用者に近い場面での脆弱性
    - 標的型攻撃(Targeted Attack)
  - 攻撃技術は「短時間化」と「多様化」
- ビジネスとしての確立
  - 自己顕示から金銭目的へ
  - 現実社会における犯罪との関連
  - 流行を避けて潜む

JPCERT/CCの取り組み

- インシデントレスポンス
  - CSIRTの構築
  - 業種・地域・管轄・分野を越えた連携
- 脆弱性情報取り扱い
  - 情報の適切なコントロール
  - 設計開発・品質管理へのフィードバック
- 脅威分析・研究
  - ボットを始めとするマルウェアの分析
  - 短期と中長期の両方の視点から対策を検討

– JPCERT/CCの取り組み –

マルウェア分析

- 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

－ JPCERT/CCの取り組み －

解析手法

	Blackbox	Whitebox
静的	Surface分析	(狭義の)静的解析 ～リバースコードエンジニアリング～
動的	(狭義の)動的解析	デバッギング

分析におけるリスク

- 捕獲・分析手法
  - 法律への抵触
  - 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
- 検体や分析結果の取り扱い
  - インシデント情報の混入
  - 漏出による二次被害

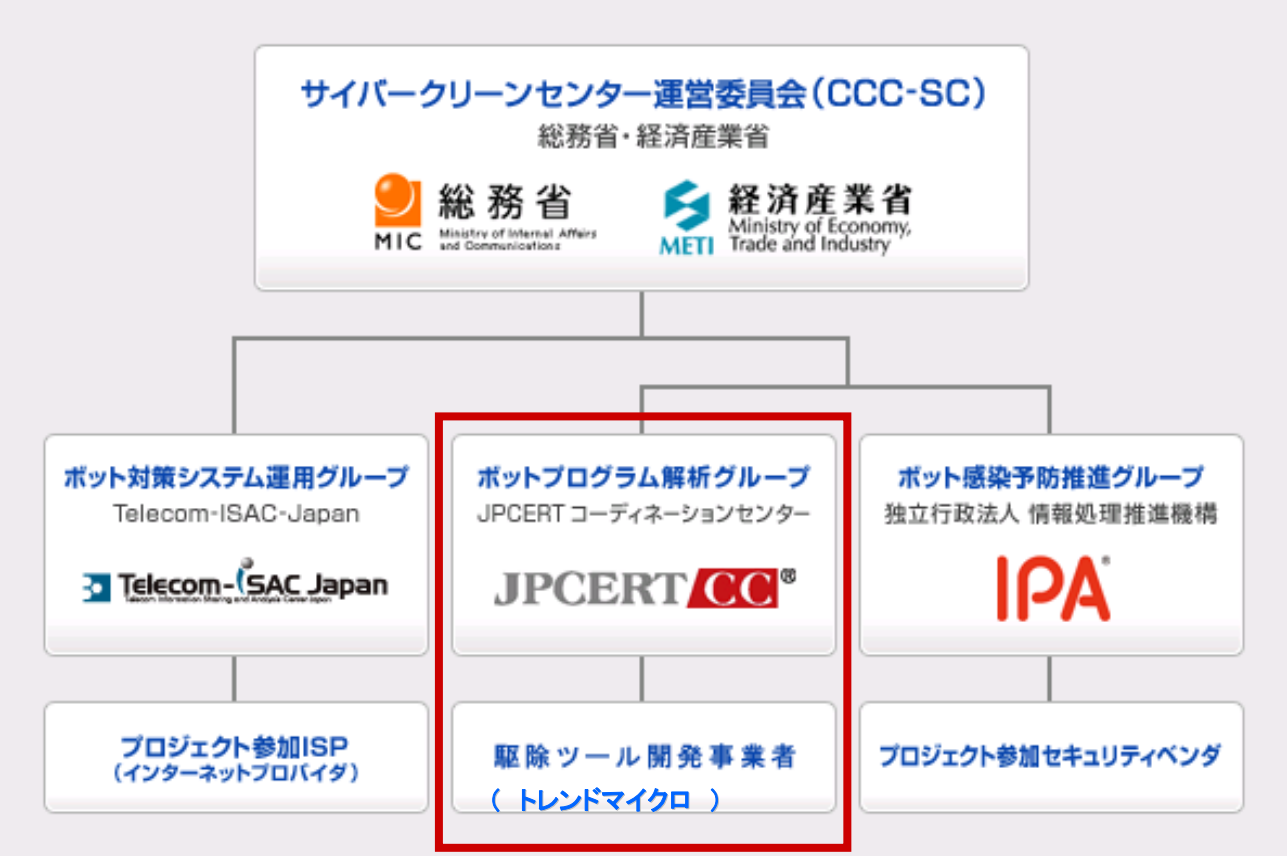
– JPCERT/CCの取り組み –

調査/研究資料

- http://www.jpcert.or.jp/
  Home>公開情報>調査/研究
- 2006年7月20日公開
  - ボットネット概要
- 2007年6月21日公開
  - マルウェアの最近の傾向とウェブアプリケーションの脆弱性を狙うボットの実態
  - P2P型ボット分析レポート

– JPCERT/CCの取り組み –

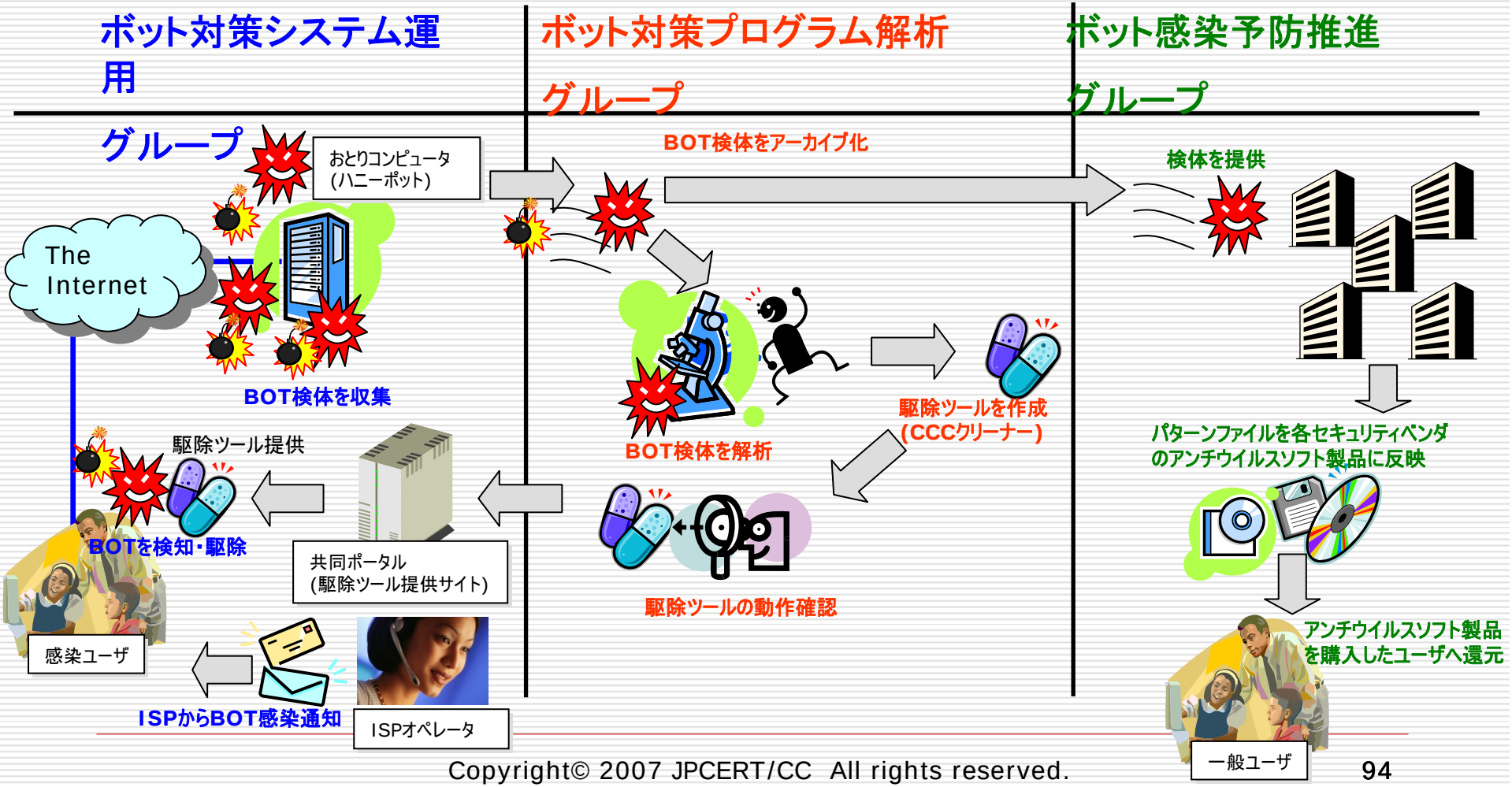
CCC(サイバークリーンセンター)



サイバークリーンセンター
(https://www.ccc.go.
j

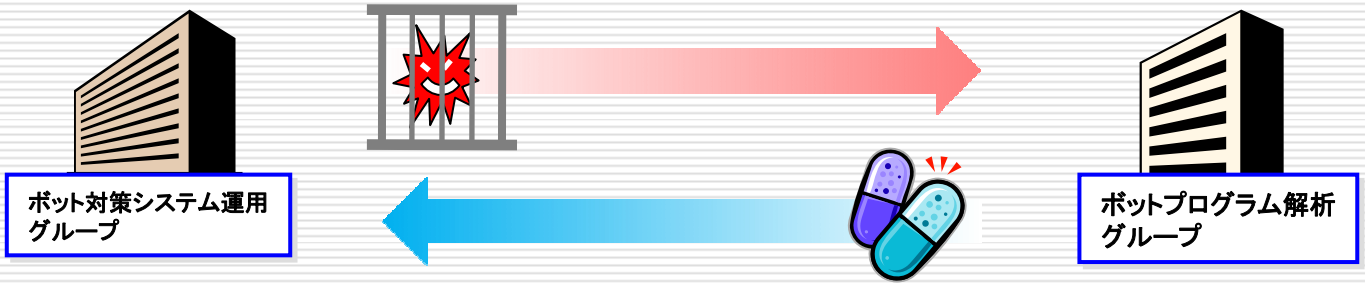
－ JPCERT/CCの取り組み －

各グループの役割



－ JPCERT/CCの取り組み －

活動状況(2007年6月末時点)

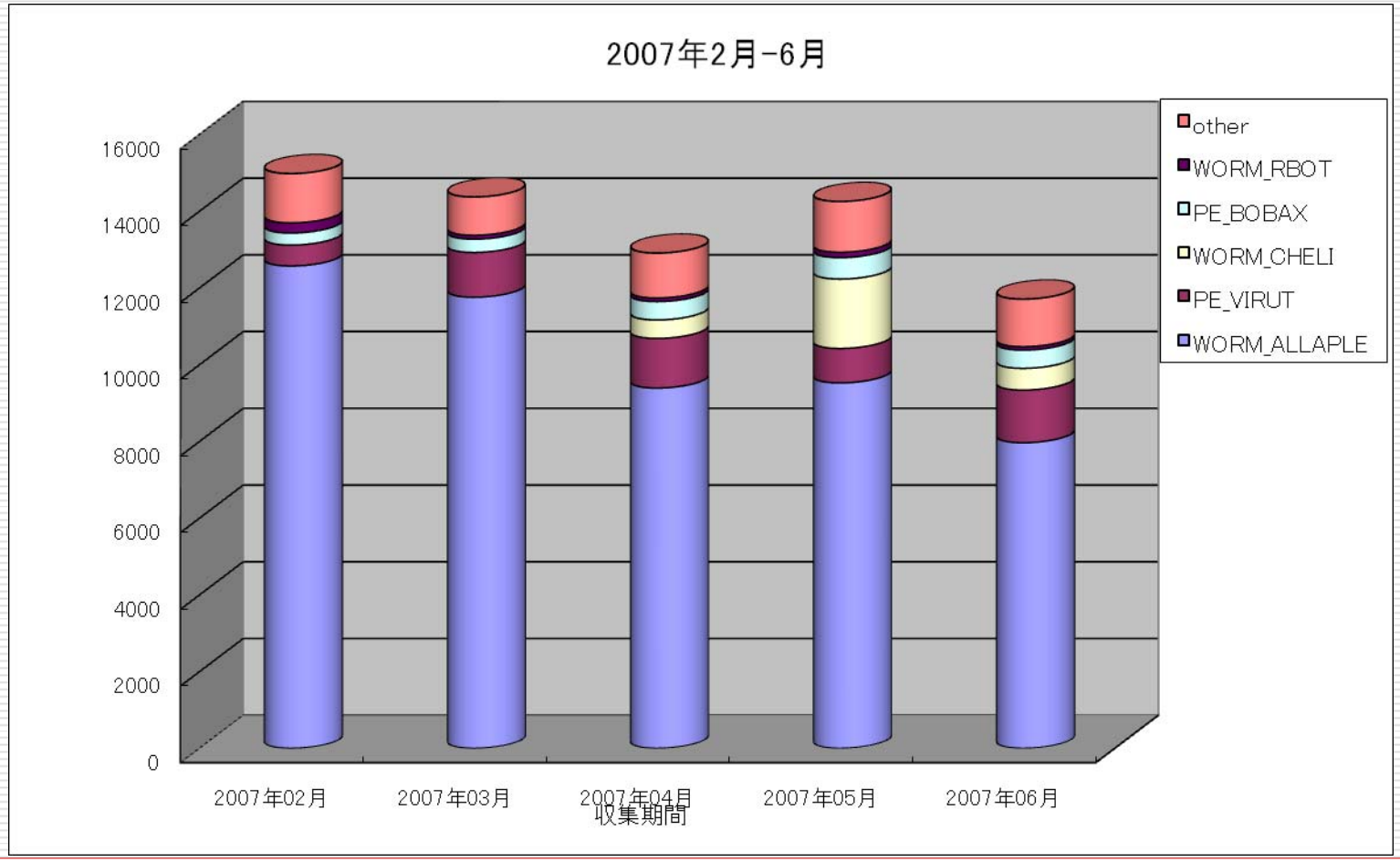


収集検体総数	1,374,606
同定検体数	69,803
未知検体数	4,446

更新回数	22
確認検体数	65,546
作成検体数	3,567

－ JPCERT/CCの取り組み －

収集検体トップ5(2007年2～6月)



ユーザの対策

- ウイルスの一種として
  - ウイルスと同じ対策から始める
- ボットとして
  - ボットに弱点はないか?
  - ボットの特徴を活かせないか?

特効薬はあるのか？

－対策－

体調管理

- セキュリティのための習慣
  - Webサイトへのアクセス
  - メールの添付ファイル・HTMLメール
- セキュリティアップデート
  - 脆弱性を利用するものは少なくない
    - ボット詳細解析(20検体)
      - 脆弱性を利用する可能性があるものが8検体
      - それぞれが複数(3～12種類)の脆弱性を利用
        MS02-039, MS02-061, MS03-007, MS03-026, MS03-049,
        MS04-007, MS04-011, MS04-012, MS05-039, …

    → 未知の脆弱性は防げない

－対策－

免疫力の維持

- ファイアウォール
  - ワーム型ウイルスに有効
  - ブロードバンドルータのNAT/NAPT機能でも有効
    → UPnPや簡易DMZのような機能に注意
- セキュリティ対策ソフトウェア
  - アンチウイルス
    → 必ずしもすべてのボットに対応できるわけではない
  - スパム・フィッシング対策

－対策－

ボット対策の問題点

- 潜行化
  - ボット化したら見た目では発見不可能
  - 通信プロトコルとしてHTTPを使うものも
- 組織化

ひとりひとりの意識を高めて総合的な対策力を向上させる

JPCERT/CCと海外組織との連携

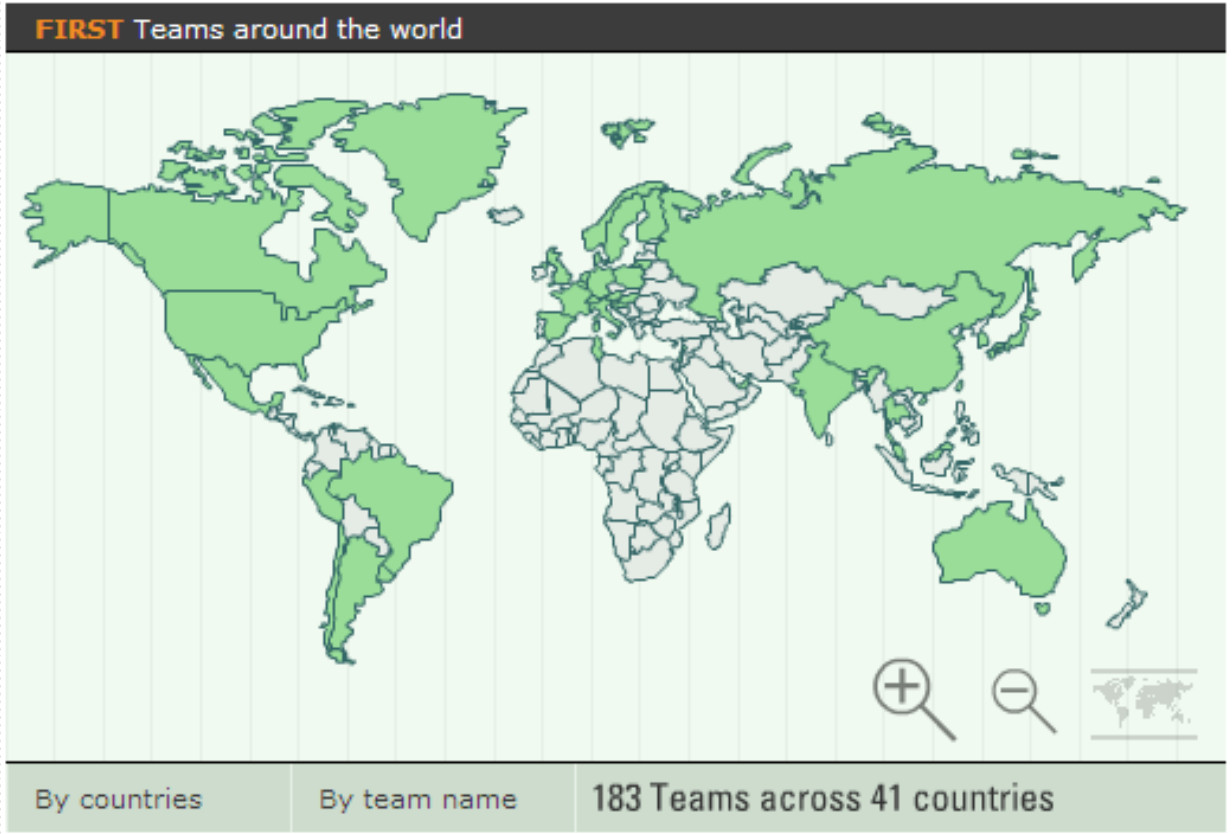
国際フレームワーク：FIRST

http://www.first.org/

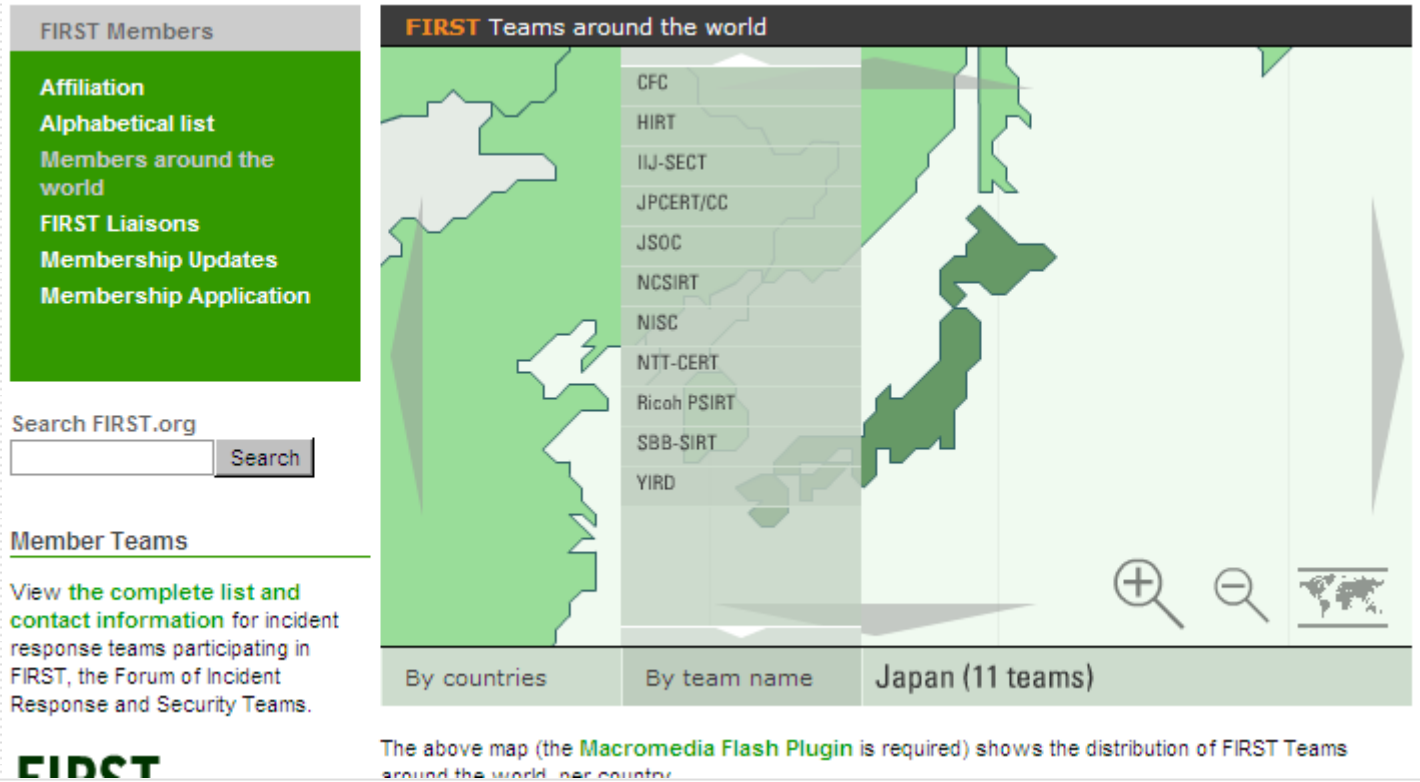
- Forum of Incident Response and Security Teams
- 1990年に CERT/CC などが中心となって設立
- 世界中の CSIRT 同士の交流を目的にした組織

  http://www.first.org/team-info/
  - 年に一度の国際会議の開催（2007年はスペイン）
  - インシデント対応 (Incident Response) の国際協力
  - 世界から180以上のチーム40ヵ国以上が参加

FIRST 参加チームマップ



日本からのFIRST加盟チーム



JPCERT/CCのFIRSTへの関わり

- FIRST理事として運営に参画
  - Law Enforcement との国際的な連携の強化
  - 国際的なISP連携の体制の構築
- 日本における調査結果の発表
  - 標的型攻撃に関する調査結果
  - 国際パネルディスカッションへの参加
- 国内外組織のFIRST加盟の支援
  - 国内の組織内CSIRT
  - 海外CSIRTなど

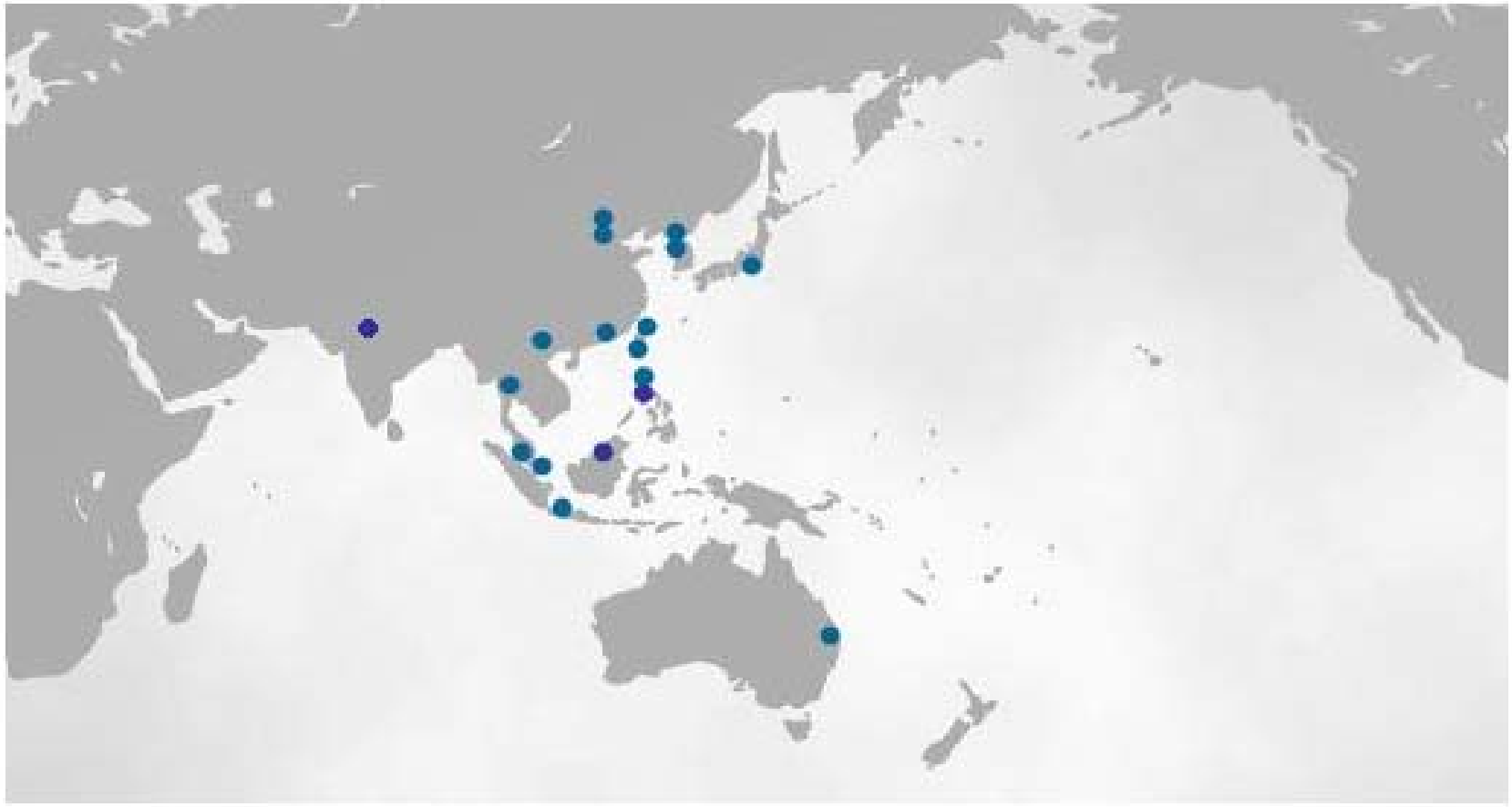
JPCERT CC®

アジア太平洋地域の枠組み

http://www.apcert.org/

- Asia Pacific Computer Emergency Response Team
  - アジア太平洋地域におけるCSIRTの集まり

    http://www.apcert.org/
  - 2003年2月設立
  - アジア太平洋地域の CSIRT のフォーラム
  - Steering Committee Member として参加
  - 年次定例会議としての APCERT
    - 2007年3月マレーシアにて開催
    - 各国の状況の報告や国際連携のディスカッション等



AusCERT(オーストラリア)、BKIS(ベトナムのベンダ)、CCERT(中国学術系)
CNCERT/CC(中国)、HKCERT(香港)、ID-CERT(インドネシア)
JPCERT/CC(日本)、KrCERT/CC(韓国)、MyCERT(マレーシア)
PH-CERT(フィリピン)、SingCERT(シンガポール)、ThaiCERT(タイ)
TWCERT/CC(台湾学術系)、TWNCERT(台湾政府系)
BP DSIRT(シンガポールベンダ)、BruCERT(ブルネイ)、CERT-In(インド)
GCSIRT(フィリピン)、NUSCERT(シンガポール学術系)、VNCERT(ベトナム)

アジア太平洋地域における JPCERT/CCの国際連携活動

- 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・フィリピン・モンゴル
  - 国内における CSIRT 発展状況の把握 (2007/09,10)

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)

アジア太平洋地域における National CSIRT 構築支援活動の様子

ミャンマー mmCERT

ベトナム VNCERT

ラオス

CSIRT トレーニング

カンボジア

CSIRT トレーニング

アジア太平洋地域における National CSIRT 連携活動の様子

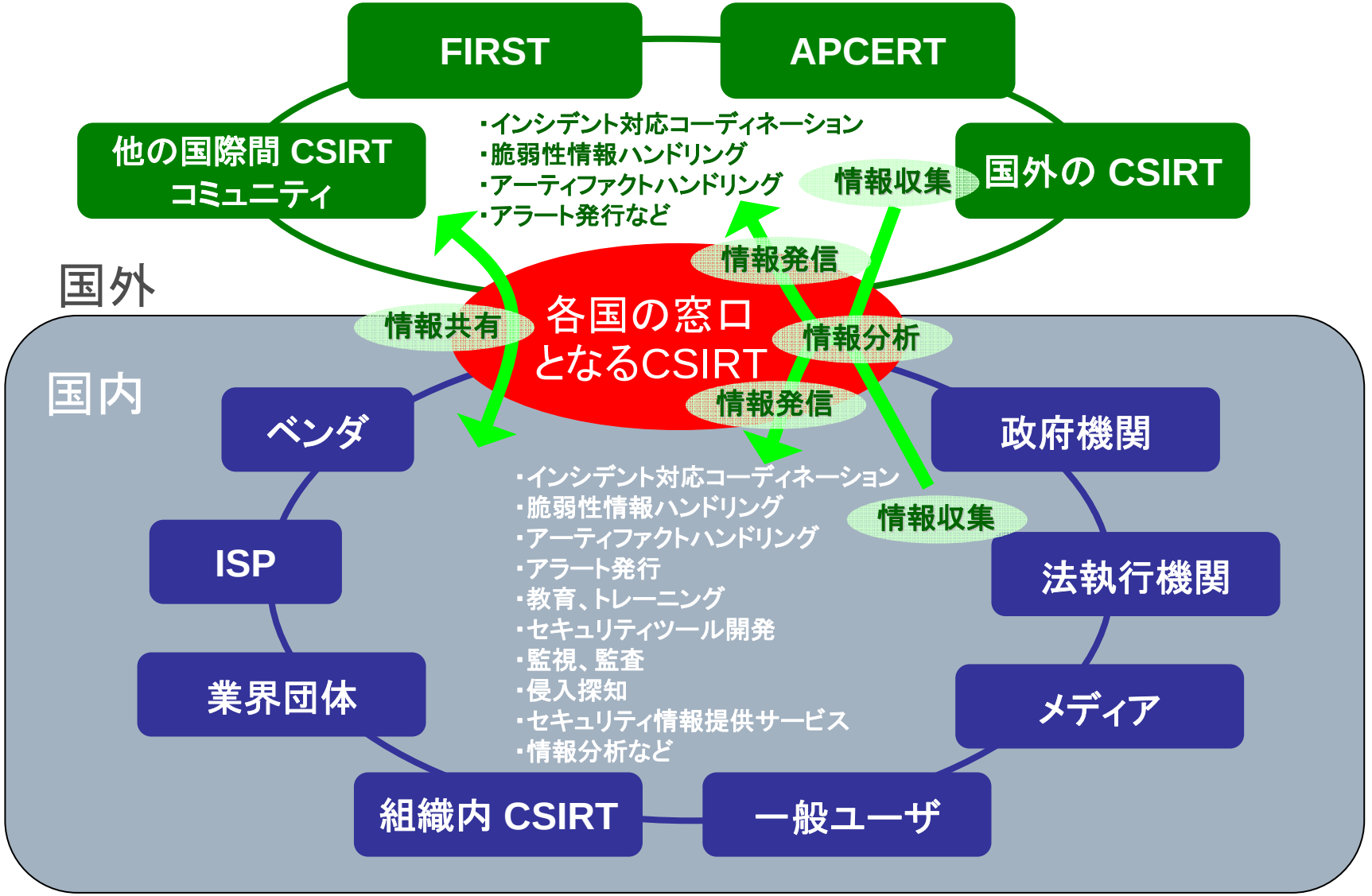
Incident Response Teams Around the World

International cooperation speeds response to Internet security breaches.

http://www.cert.org/csirts/csirt-map.html

(C) 2003 Carnegie Mellon University; Revised July 2005

各国の窓口となる CSIRT の主な業務内容

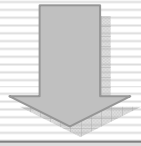


組織内CSIRTとは

CSIRT に関してよく聞かれること

CSIRT とは何か？

- CSIRTの正式名称
  - Computer Security Incident Response Team
- CSIRT は、サービス組織の概念である



「コンピュータセキュリティインシデント」の
報告や発生状況の受け付け、調査及び対応

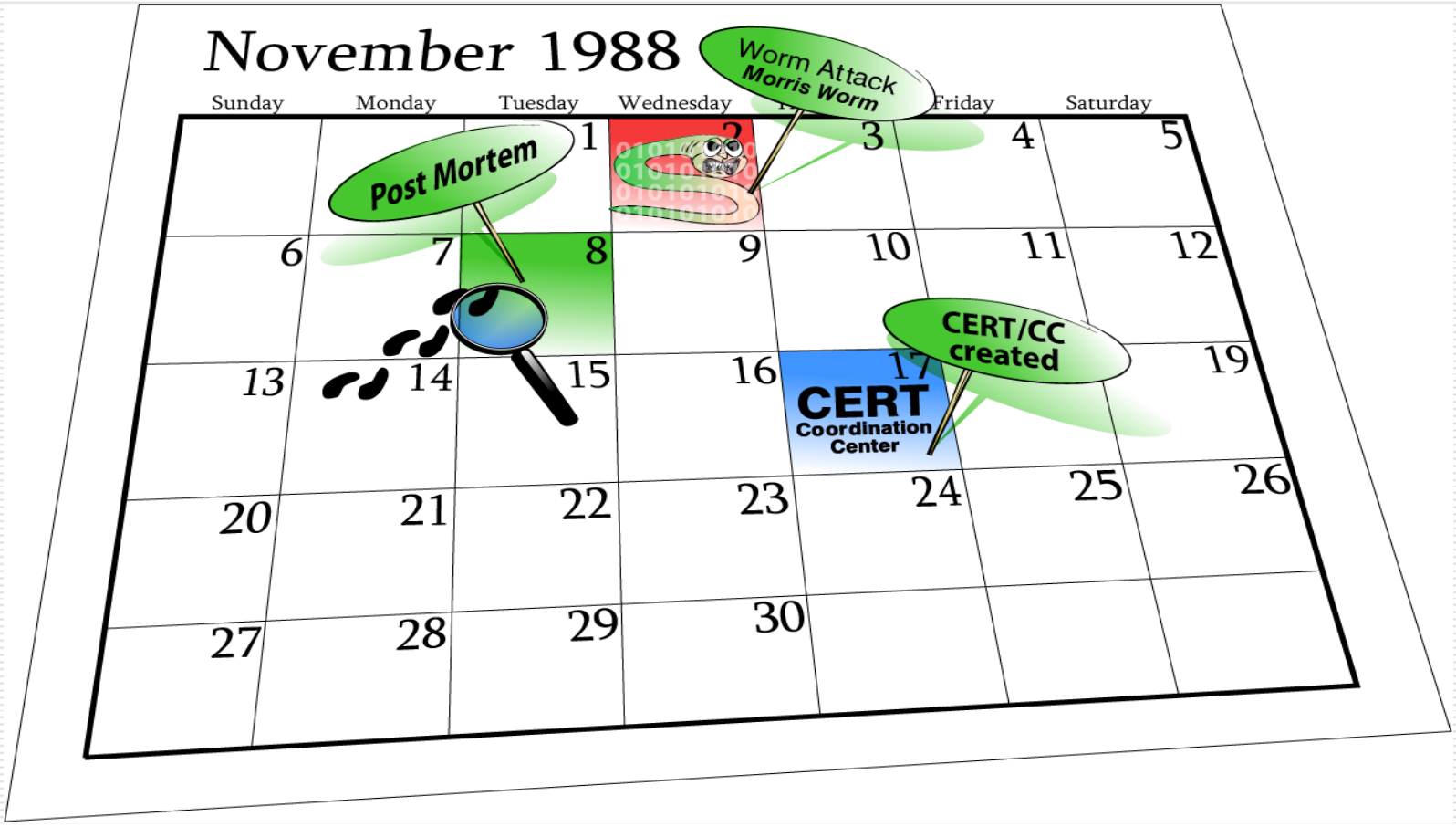
CSIRT に関してよく聞かれること

CSIRT が取り扱うものは何か？

- コンピュータセキュリティインシデント
  - 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) を含みます。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) などがある。
  - セキュリテイポリシーに違反する活動のことも指す場合がある。

CSIRT に関してよく聞かれること

CSIRT はどのようにして発足したのか?



JPCERT CC®

CSIRT に関してよく聞かれること

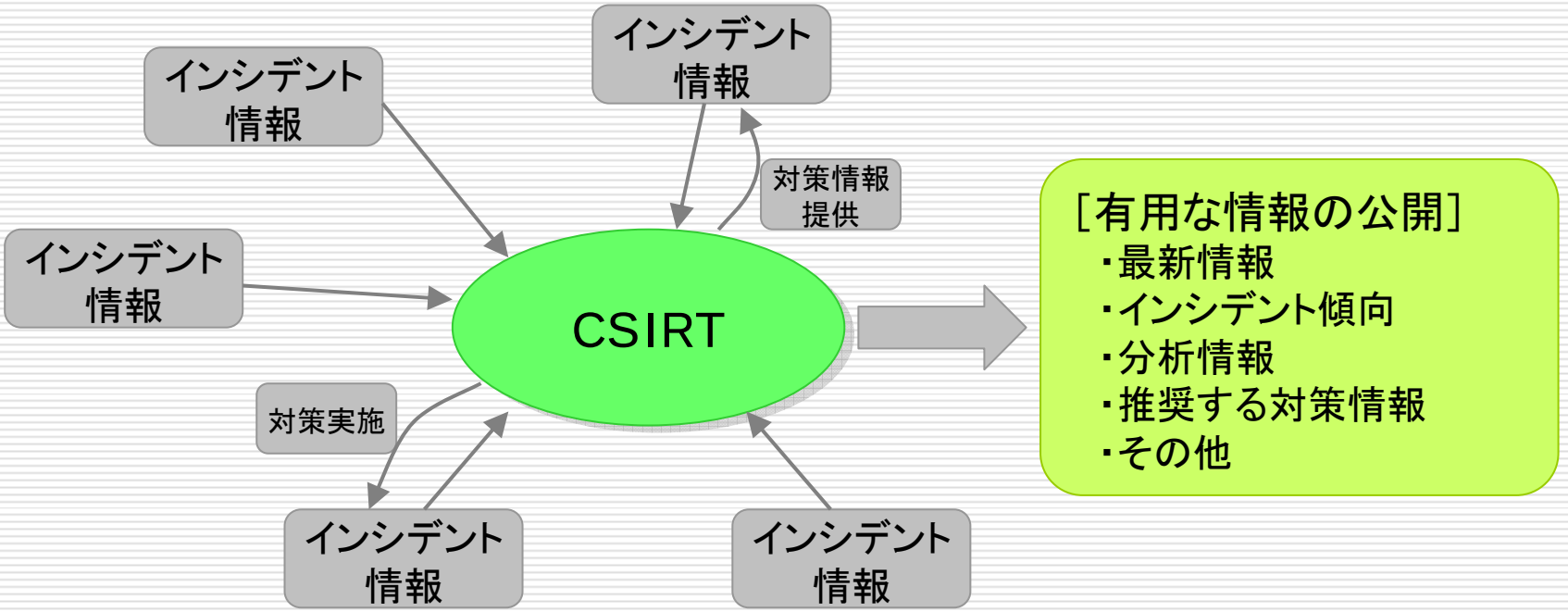
CSIRT に相当する既存の組織名は?

CSIRT	Computer Security Incident Response Team
CERT	Computer Emergency Response Team
CSIRC	Computer Security Incident Response Capability
CIRC	Computer Incident Response Capability
CIRT	Computer Incident Response Team
IHT	Incident Handling Team
IRC	Incident Response Center or Incident Response Capability
IRT	Incident Response Team
SERT	Security Emergency Response Team
SIRT	Security Incident Response Team

CSIRT に関してよく聞かれること

インシデントレスポンスとは何か?

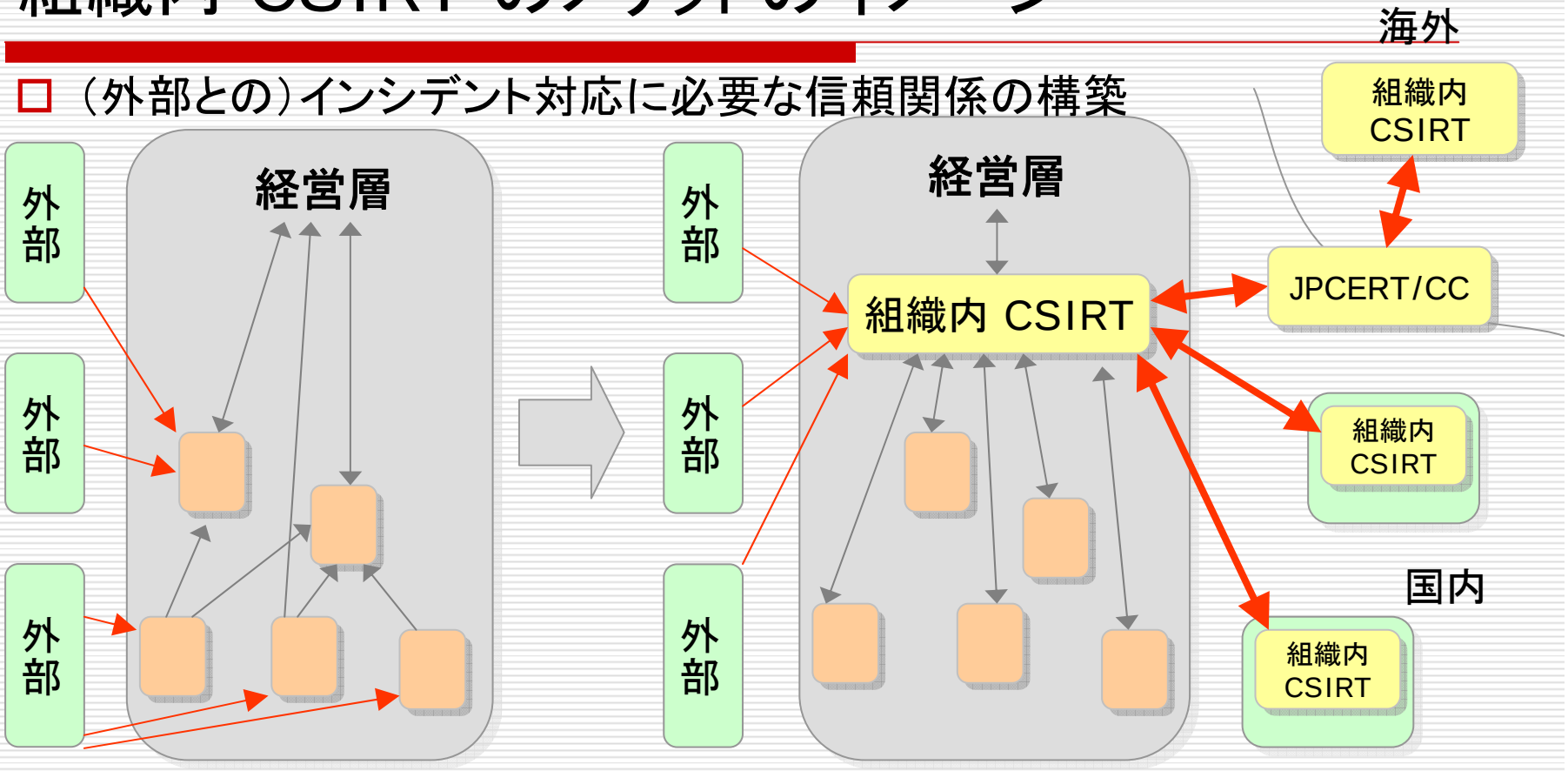
- 3つの役割
  - インシデントのレポート、分析、レスポンス



組織内 CSIRT の必要性

組織内 CSIRT のメリットのイメージ

- （外部との）インシデント対応に必要な信頼関係の構築



メリットの例：①インシデントレスポンスに必要な情報量の向上
②想定外（予想外）のインシデントへの柔軟な対応

CSIRT のフレームワーク

CSIRT のフレームワーク

ミッションステートメント

- ミッションは、所属している組織及びサービス対象者が期待するものに強く影響される

- 一般的な CSIRT のミッションの例
  - 構成システムのセキュリティの保守と維持管理
  - インシデントレスポンス活動の統制及び調整
  - セキュリティインシデントによる被害の最小化
  - サービス対象者に対するセキュリティ関連の教育及び啓蒙と最善策（”best practice”）の提供

JPCERT CC®

CSIRT のフレームワーク

サービス対象

- サービス対象（Constituency）及びその関係の定義
- CSIRT をサービス対象者に周知
- “doing the job right（仕事を適切にこなす）” により、サービス対象から信頼獲得

インシデント発生時における、CSIRT の有効な機能発揮

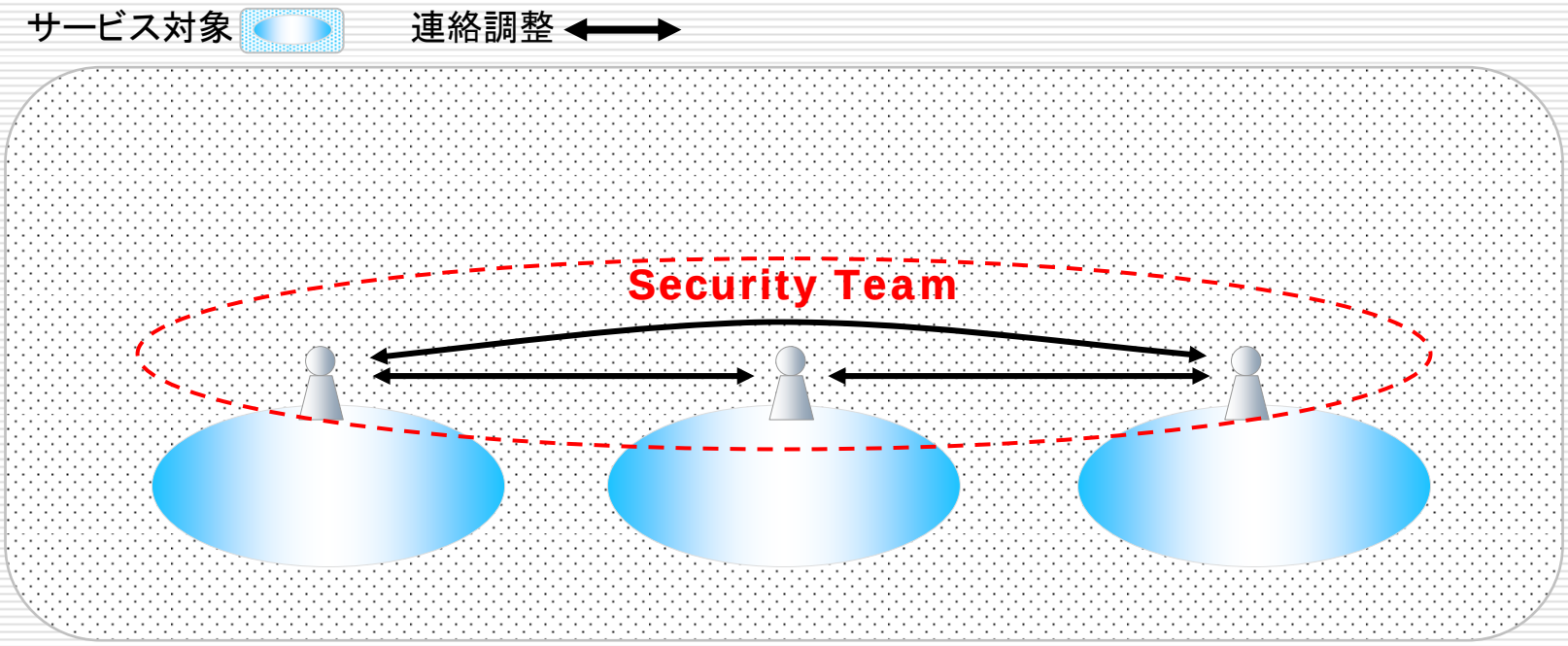
JPCERT CC®

CSIRT のフレームワーク
組織形態

- Security Team
  - セキュリティーチーム
- Internal Distributed CSIRT
  - 内部における分配型CSIRT
- Internal Centralized CSIRT
  - 内部における集中型CSIRT
- Internal Combined Distributed and Centralized CSIRT
  - 内部における統合(分配/集中)型CSIRT
- Coordinating CSIRT
  - 連絡調整としてのCSIRT

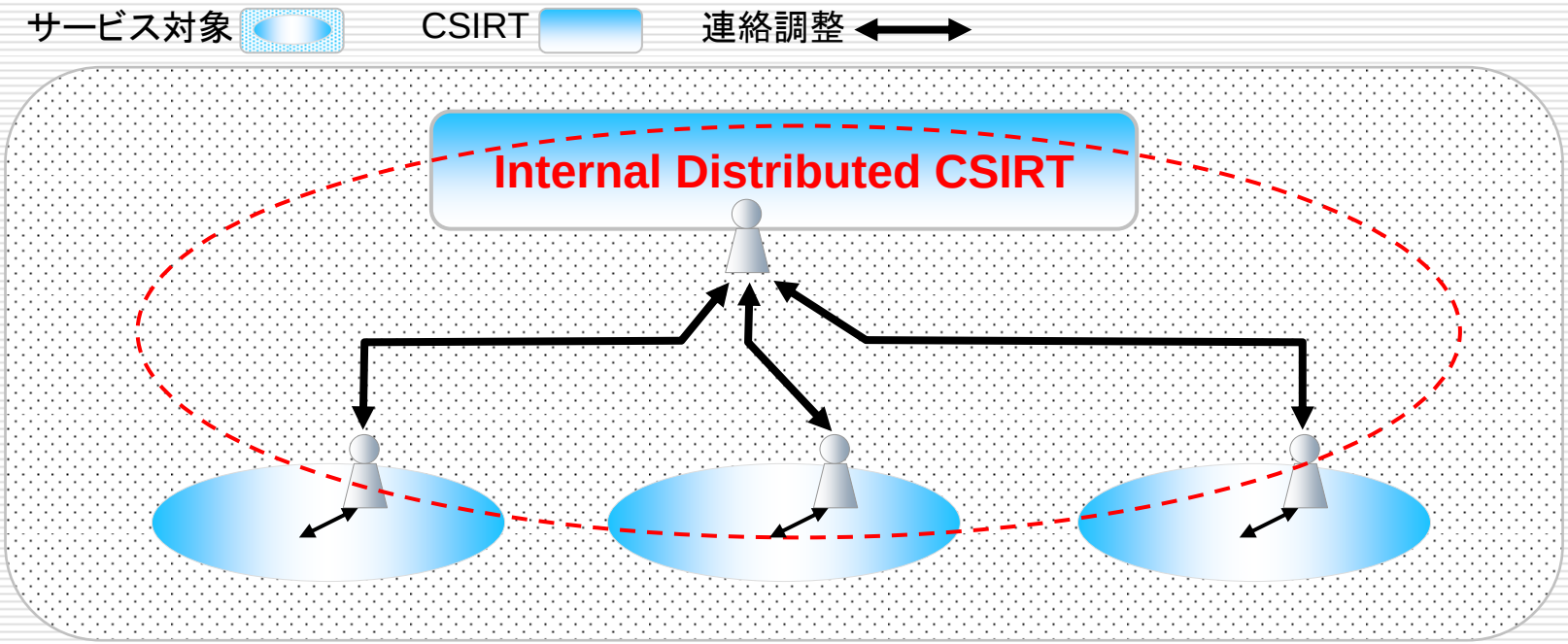
CSIRT のフレームワーク – 組織形態

Security Team



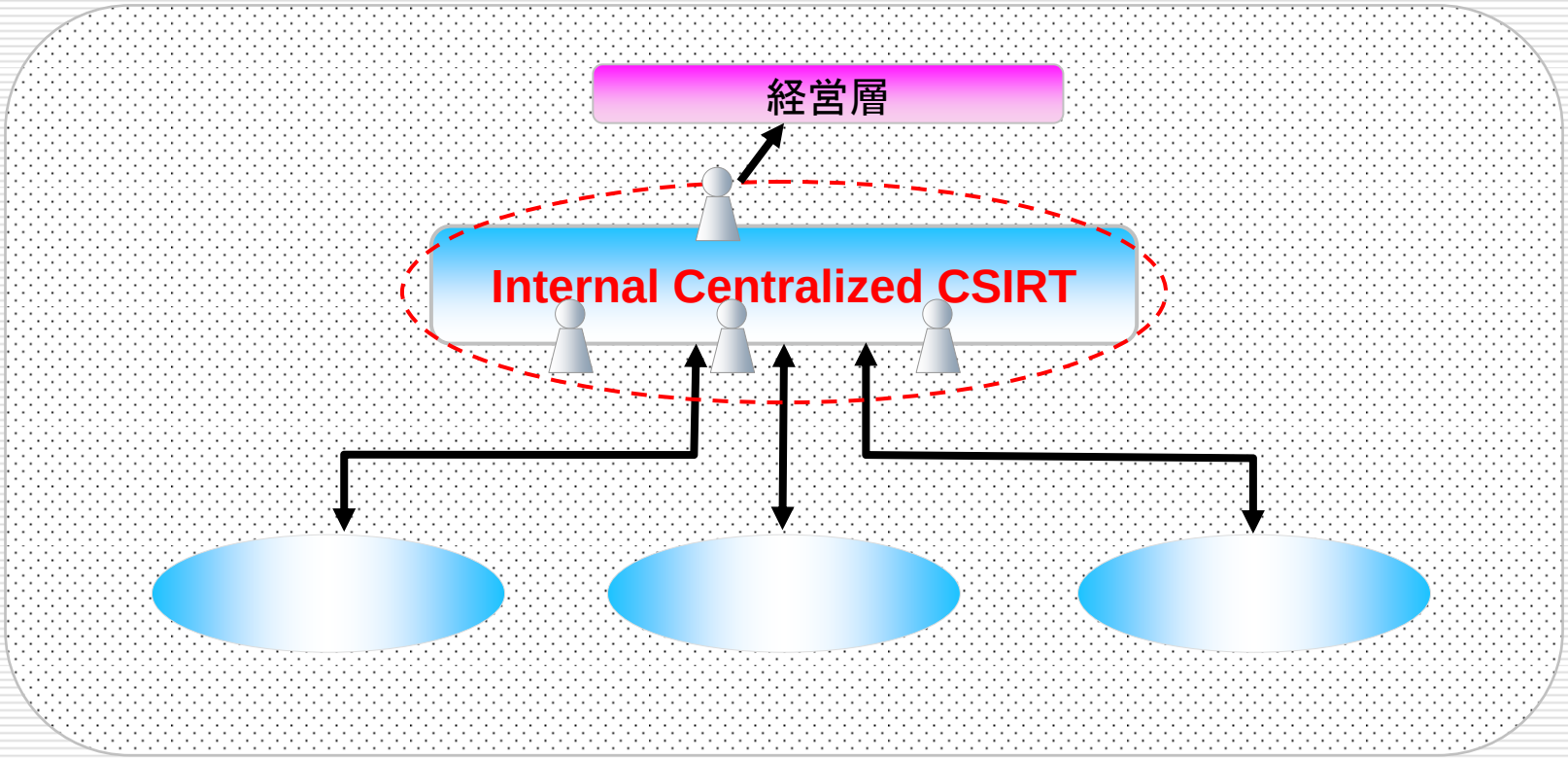
CSIRT のフレームワーク – 組織形態

Internal Distributed CSIRT

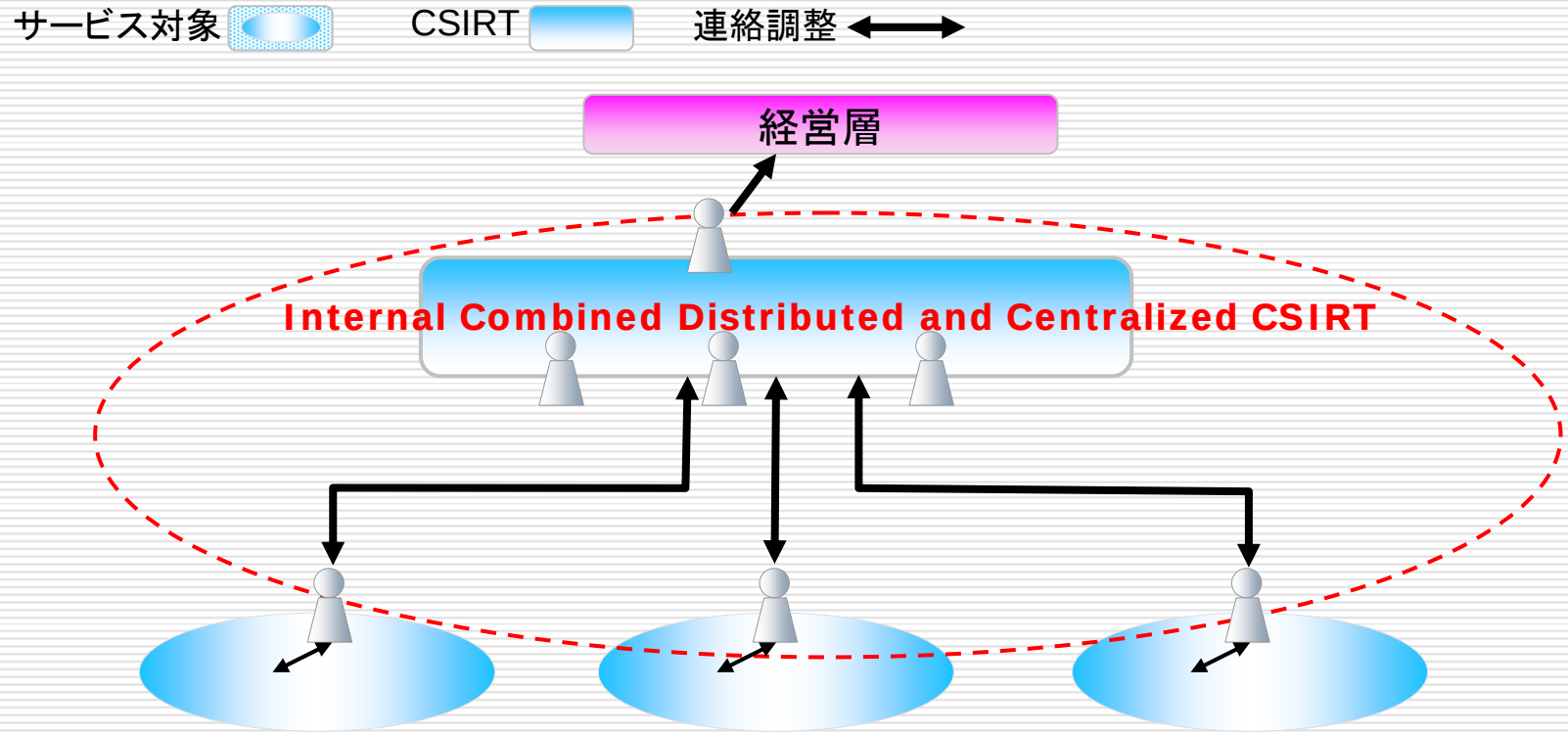


CSIRT のフレームワーク – 組織形態

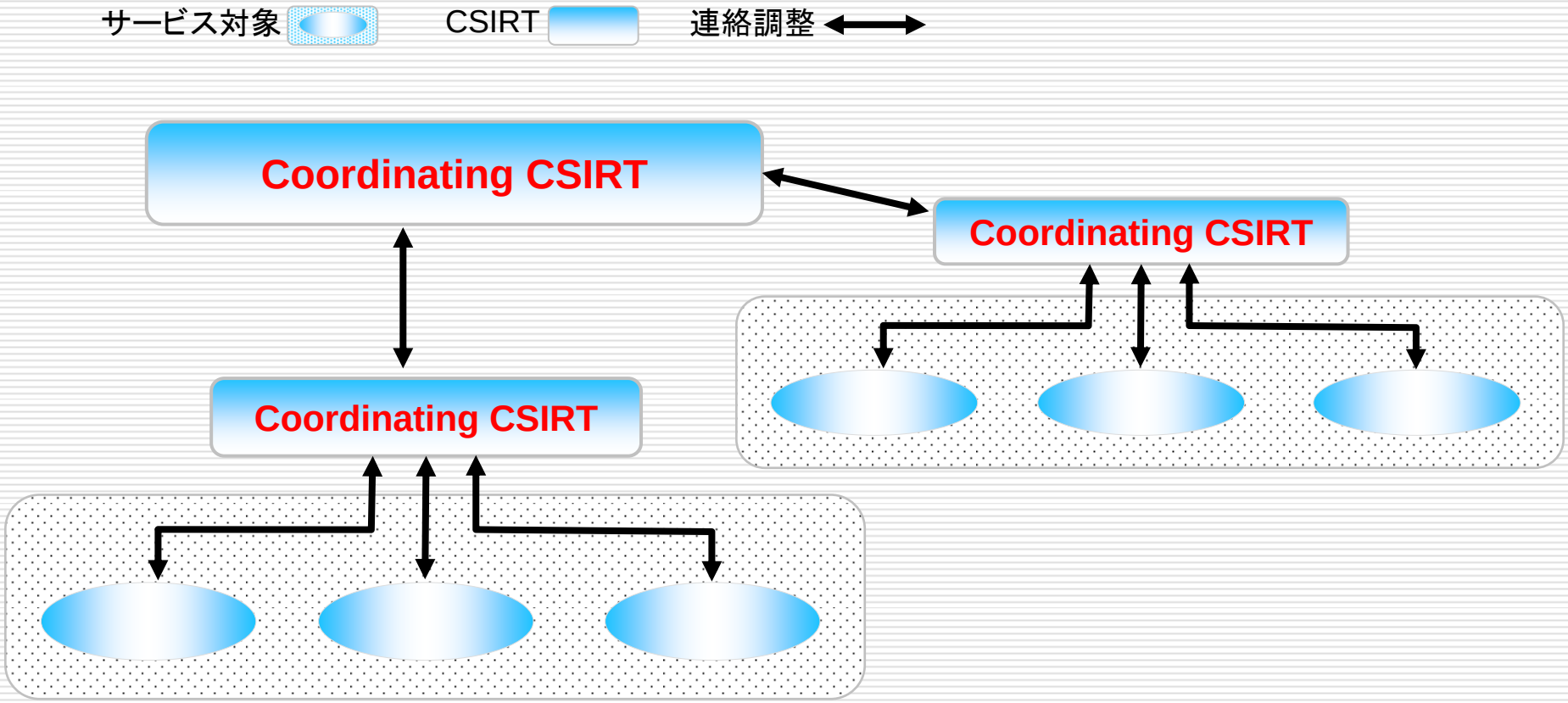
Internal Centralized CSIRT



CSIRT のフレームワーク – 組織形態
Internal Combined Distributed and Centralized CSIRT

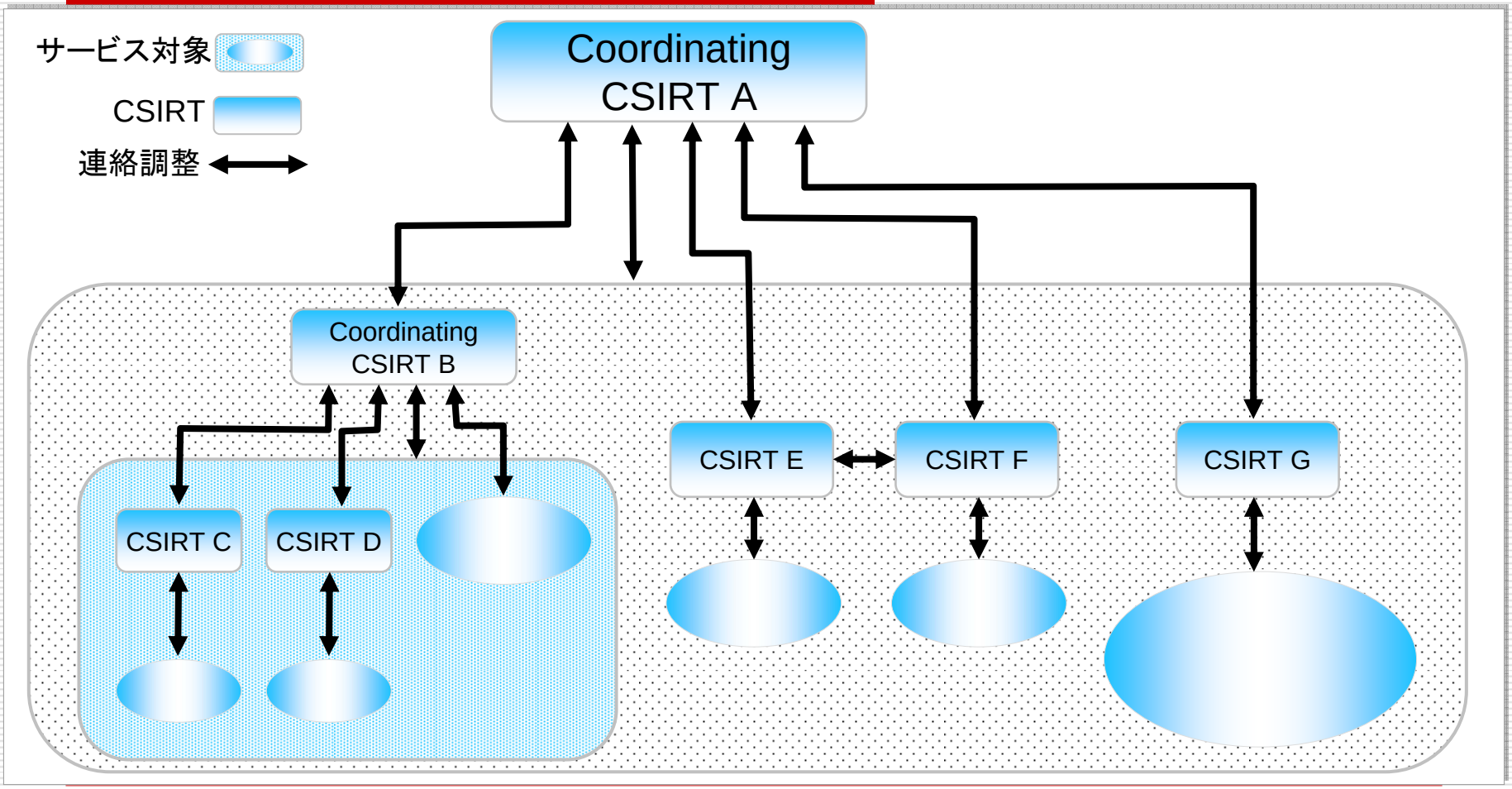


CSIRT のフレームワーク – 組織形態
Coordinating CSIRT



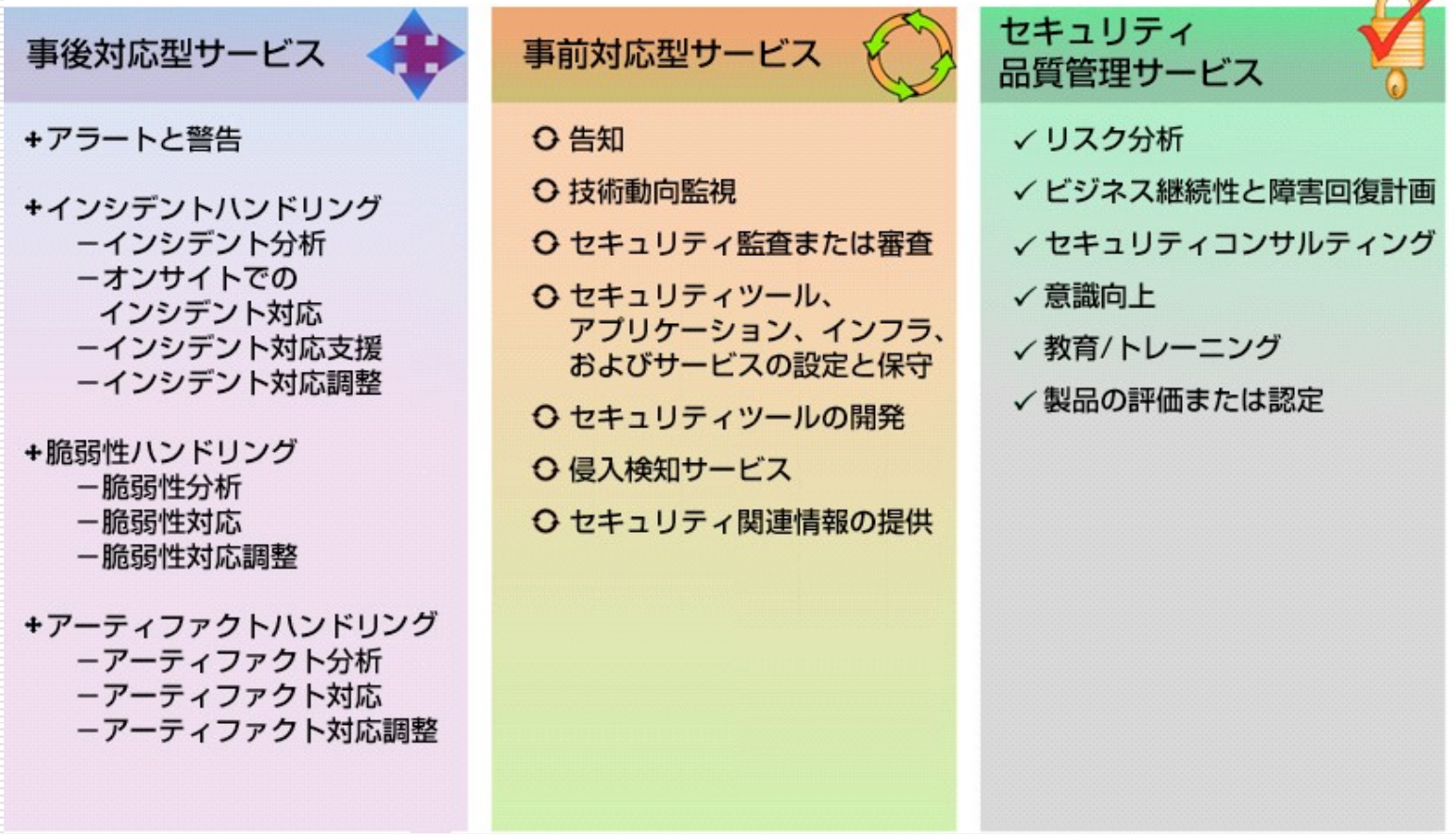
JPCERT CC®

CSIRT のフレームワーク
相互関係



CSIRT のサービス

CERT/CC におけるサービスの分類の例



JPCERT CC®

CSIRT のサービス

サービスの分類

- Reactive Service
  - Reactive: 反応
  - 各インシデント報告や不正検知システムなどからの情報による活動
  - CSIRTのもっともコアな活動
- Proactive Service
  - Proactive: 先を見越す
  - 事前にソフトウェアなどの脆弱性、脅威情報、攻撃予測情報などを提供する活動
  - 直接的にインシデント発生の抑制を図る
- Security Quality Management Service
  - セキュリティコンサルタント、教育など
  - 他のセキュリティー会社がすでに提供済みだが、CSIRT としての視点や専門知識での見識を提供できる。
  - 間接的にインシデント発生の抑制を図る

CSIRT のオペレーション

JPCERT CC®

CSIRT のオペレーション

3つの重要なプロシージャー

1. インシデント発生前
   - インシデントリスクを軽減
     - リスクがどこにあるかを知る必要がある。
   - CSIRT とユーザのためのインシデント対応準備
2. インシデント発生時のレスポンス
   - インシデントの対応手順の文書化
3. インシデント発生後
   - 何が起こったのかを検証
   - サービス対象と CSIRT にとって有益なことを学ぶ

JPCERT CC®

CSIRT のオペレーション

インシデント発生前

- セキュリティポリシーと実施計画
  - 組織はセキュリティ手段を理解し、定義しなければならない。また、全てが関連していなければならない。
- 予防活動の手段
  - 監査、リスクマネージメント、バックアップ、ログ、防御（Firewall など）、パッチ（アップデート）
- CSIRT の情報とツール
  - 連絡先の確保、IP アドレス表、診断／修正ツール
- CSIRT からの公表資料
  - 内部向けの email やニュースレター、Web page、トレーニング、ワークショップなど

JPCERT CC®

CSIRT のオペレーション

インシデント発生時の対応

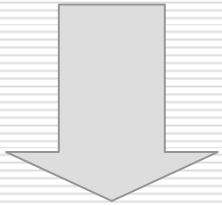
- 対応フロー確立のねらいは、一貫性の確保とストレスの軽減
  - 事前に、より多くの判断事項を作成しておく
  - インシデント対応中の判断は、ミスが多い
- インシデントの分類は、複数の可能性を想定
  - インシデント対応について常に複数の可能性を想定し、対応プランを検討する
- 可能であれば、演習として計画を立ててみる
  - 他の事例はどうしてうまく処理できたのか？
  - 経験から学んだことを手順に反映させる

インシデント対応

- インシデントに対応する人及び組織の明確化
- インシデント発生前の準備
- インシデント対応フロー
  1. インシデントの発見及び報告
  2. インシデントに対する初動対応
  3. インシデントに関する告知
  4. インシデントの抑制措置と復旧
  5. インシデントの事後対応

インシデントに対応する人及び組織の明確化

- 発生するインシデントのすべてを完全に予想することは不可能
- これまで各部署で経験したことがないインシデントに対して、対応すべき担当者や責任者が不明確なことがあり、対応に不備が出ることがある



- インシデント対応マニュアルには以下の記述が必要
  - 組織にとっての「インシデント」を定義する
  - 「想定外のインシデント」に対して責任を持つ部署／担当者を明確に定義する
  - 各部署で発生したインシデント対応について、全体の統括を行う部署またはチーム等を明確に定義する

インシデント発生前の準備

- インシデント対応に必要な連絡先の確保
  - これまでに経験したインシデント、あるいはこれから発生が予想されるインシデントの対応に必要な連絡先をリスト化する
  - 連絡先との連絡手段の疎通確認を実施する
  - 各連絡先と連絡先リストについての共通認識を持つ
- 各種規則の把握と整合性の確認
  - 親組織の規則（上位規則）にインシデント対応に関する記述がされている可能性があるため、関連する可能性のある規則を確認する
  - 上記を含め、インデント対応の活動に関係する規則等の相関関係を明確にしておく
- インシデント対応に有効なツールの利用
  - 社内での情報共有のためのインフラやツールがインシデント対応にリアルタイムに有効がどうか検討する
  - 有用なツール等がなければ、インシデント対応に活用できる別の手段を確保しておく
  - 可能であれば、事前に訓練等を実施しておく

JPCERT CC®

インシデントの対応フロー

1. インシデントの発見及び報告

- インシデントの発見者が迅速に報告する
  - 報告しやすい環境であることが必須
  - インシデントの報告窓口が設けられており、それが周知されていることが必要
- インシデントの報告を受けた者が、どのような判断で対応をするのか、あるいはより上位に報告するのか、の判断基準を明確にしておく
  - 最低限以下の判断が必要
    - 対応すべきインシデントとして認められるかどうか
    - 対応の優先度はどの程度か
    - 誰がインシデント対応を担当するのか
- すべてのインシデントの取り扱いに関する記録をとる
  - 責任の明確化のため
  - 事後の分析のため

インシデントの対応フロー

2. インシデントに対する初動対応

- 発生したインシデントに関して、どこまで情報を共有するのかを判断する
  - 外部のセキュリティサービス会社等を利用するのか
  - 同様なインシデントの発生が予想される場合、どの範囲まで、インシデント発生に関する告知をすべきか
- これまでに経験しているインシデントなのか、経験したことのないインシデントなのかを判断する
  - これまでに経験したインシデントであれば、過去の対応ノウハウを積極的に活用する
    - そのためには記録の所在を明確にしておく必要がある
  - 経験したことのないインシデントであれば、以下のリソースを活用することを検討する
    - 過去のインシデント対応経験者
    - 他組織における同様なインシデント対応に関する情報
    - 発生したインシデントに直接関係する資産の所有者

インシデントの対応フロー

3. インシデントに関する告知

- 外部組織等に対して、インシデント発生の事実と対応状況に関する報告をする必要があるかどうかを判断する
  - 社会通念上必要性があるため
  - 公的な規則で定められているため
  - ビジネス的なインパクトを軽減させるため
- 誰に、またはどの範囲に告知をすべきかを判断する
  - 社会全体に対してか？
  - 所轄官庁等の外部組織に対してか？
  - 顧客に対してのみか？
- 告知する手段の妥当性を検討する。
  - 自社 Web サイトのみか？
  - 新聞等のメディアを利用するのか？
  - 記者会見か？
  - そのほかか？

インシデントの対応フロー

4. インシデントの抑制措置と復旧

- 発生したインシデントの被害を抑制するための検討項目
  - 抑制措置の手段
  - 抑制措置によるビジネスにおけるダメージ
  - 抑制措置の実施期間
  - 最高意思決定者
  - 業務時間外における意思決定と実施方法
- 復旧に関する検討項目
  - 事業継続計画（BCP）との関係
  - データ等の資産の一部損失とのトレードオフ
  - 最終的な意思決定

インシデントの対応フロー

5. インシデントの事後対応

- インシデント復旧後のモニタリングを実施する
  - 一部のウィルスやワーム等については、再発する可能性があるため、必要に応じてモニタリングを行う
  - 表面的にはインシデントが解決したように見えても、本質的には問題が解決していない場合があるため
- 同様なインシデントの再発防止策を検討する
  - インシデント情報を告知することにより、同様なインシデントの発生を抑制することができる
  - ウィルスやワームには、同じ感染手法を用いた亜種などが発生する
- 他に影響がないかどうかの評価を実施する
  - インシデントを発生させ、他の資産をねらう攻撃手法が存在しているため
  - 影響が表面化しにくい攻撃手法が存在しているため
- 従業員やスタッフ等への教育を実施する
  - 情報セキュリティに関する教育による、再発防止

有効に機能するための CSIRT の要件

有効に機能するための CSIRT の要件

- 「サービス対象」が定義されていること
- 「インシデント」が定義されていること
- インシデントに対する、Response（対応）や Coordination(調整)ができること
- 信頼できる連絡先（PoC)が提供されていること

まとめ

- 脆弱性対応の必要性
  - 情報の収集と対応の判断、対応
- インシデントへの対応
  - インシデントを検知と分析、対応
- 組織内CSIRTの構築
  - 円滑な脆弱性・インシデント対応のために

参考資料

- JPCERT Coodrination Center : JPCERT/CC
  http://www.jpcert.or.jp/
  - インシデント対応とは？
    http://www.jpcert.or.jp/ir/
  - CSIRTマテリアル
    http://www.jpcert.or.jp/csirt_material/
  - コンピュータセキュリティインシデント対応チーム (CSIRT) のためのハンドブック
    http://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf
- サイバークリーンセンター:CCC
  http://www.ccc.go.jp/
- Japan Vulnerability Notes: JVN
  http://jvn.jp/
- FIRST
  http://www.first.org/
- APCERT
  http://www.apcert.org/
- CERT/CC
  http://www.cert.org/
- CPNI
  http://www.cpni.gov.uk/

お問い合わせ先

- 有限責任中間法人
  JPCERTコーディネーションセンター
  - Email:office@jpcert.or.jp
  - Tel:03-3518-4600
  - http://www.jpcert.or.jp
- インシデント報告の届出
  - 報告様式
    http://www.jpcert.or.jp/form/
  - Email:info@jpcert.or.jp
    PGP Fingerprint :470F F413 3DCC 5D38 7CAC 3500 80C4 944B 298F 386F