資料　４
科学技術・学術審議会　研究計画・評価分科会
安全・安心科学技術委員会（第９回）H19．６．12

JPCERT CC®

情報セキュリティインシデントの現状と対応上の課題

JPCERTコーディネーションセンター

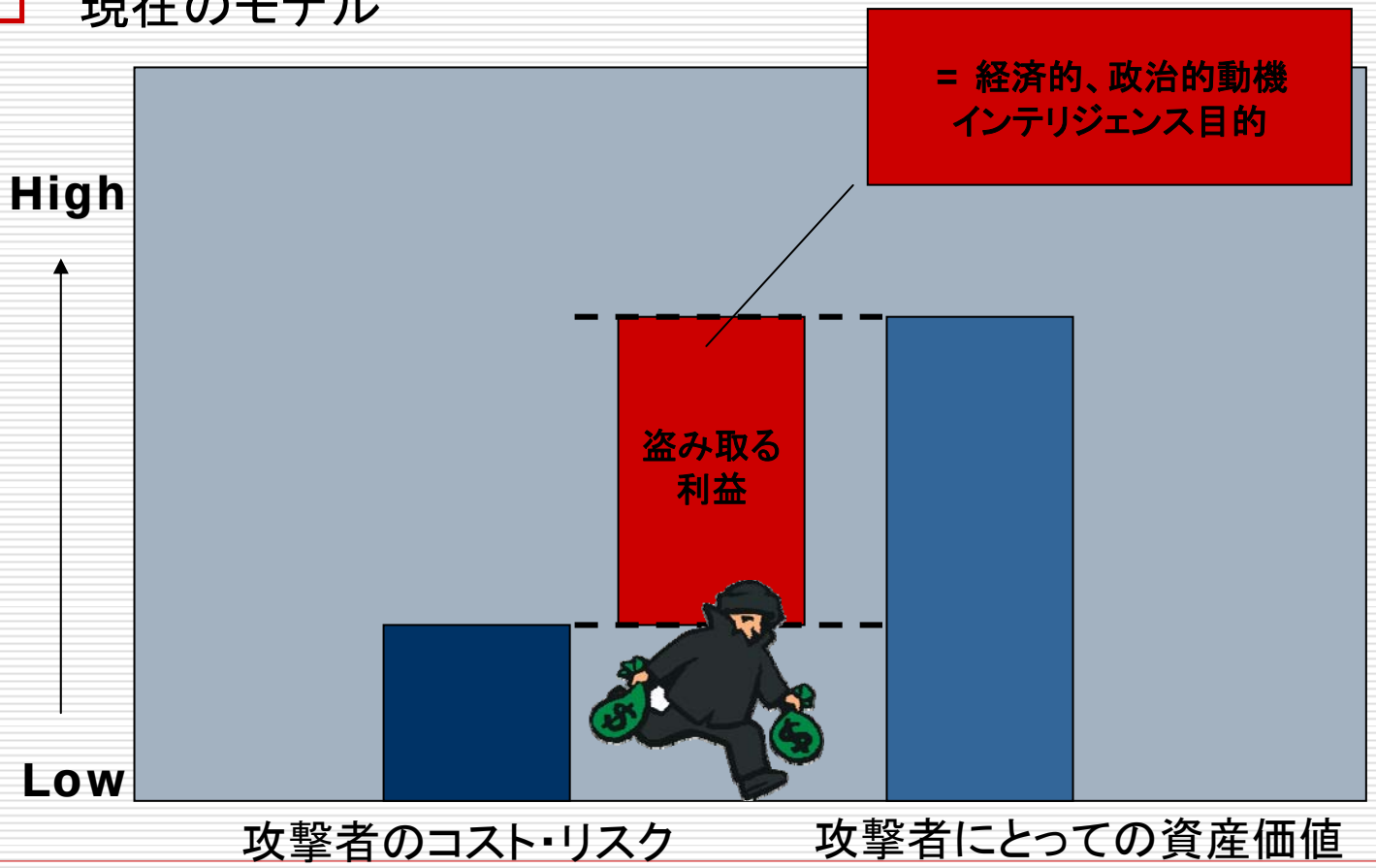
早貸淳子

2007年6月12日

Ⅰ　JPCERTコーディネーションセンターの活動

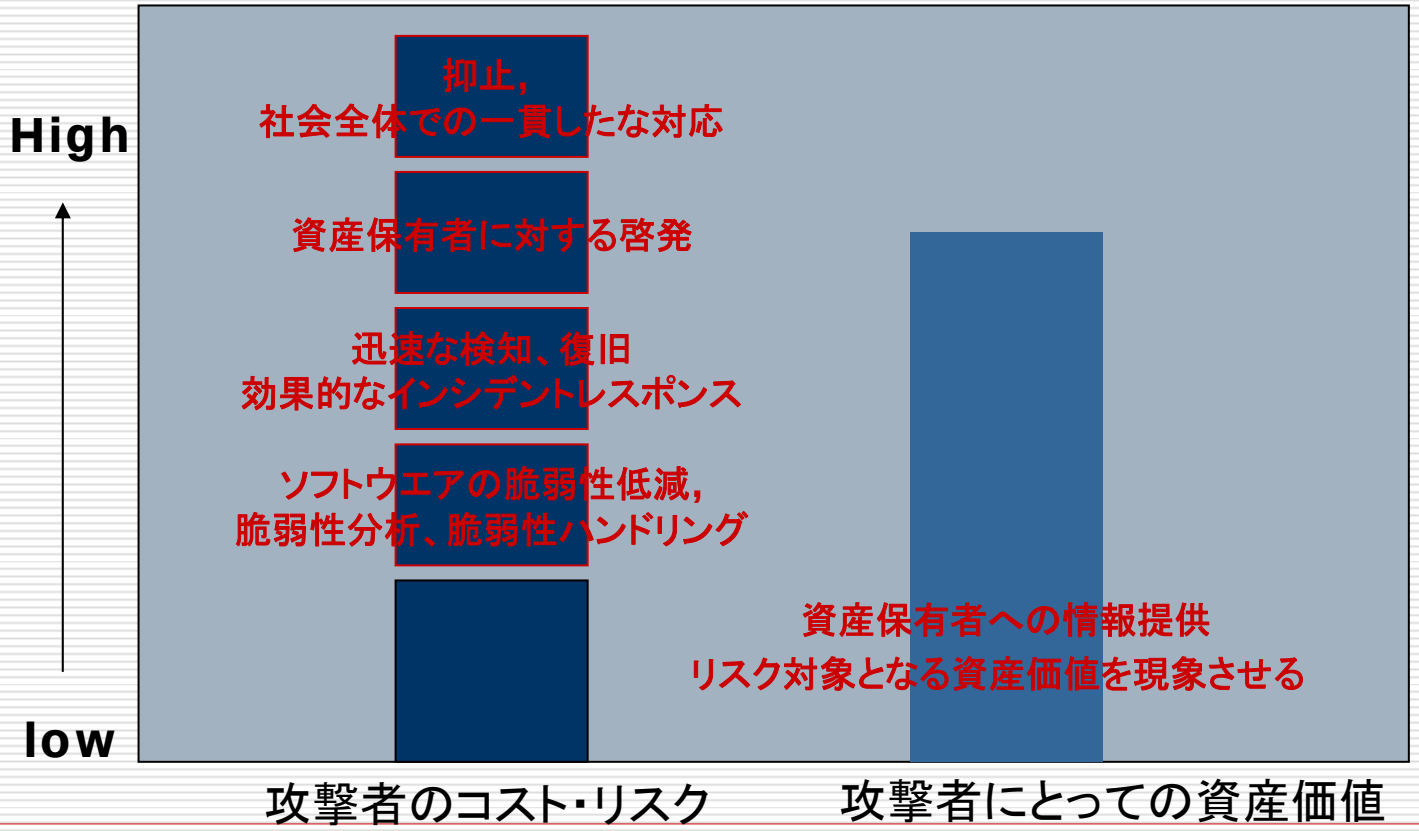
攻撃のコストと情報資産の価値

- 現在のモデル

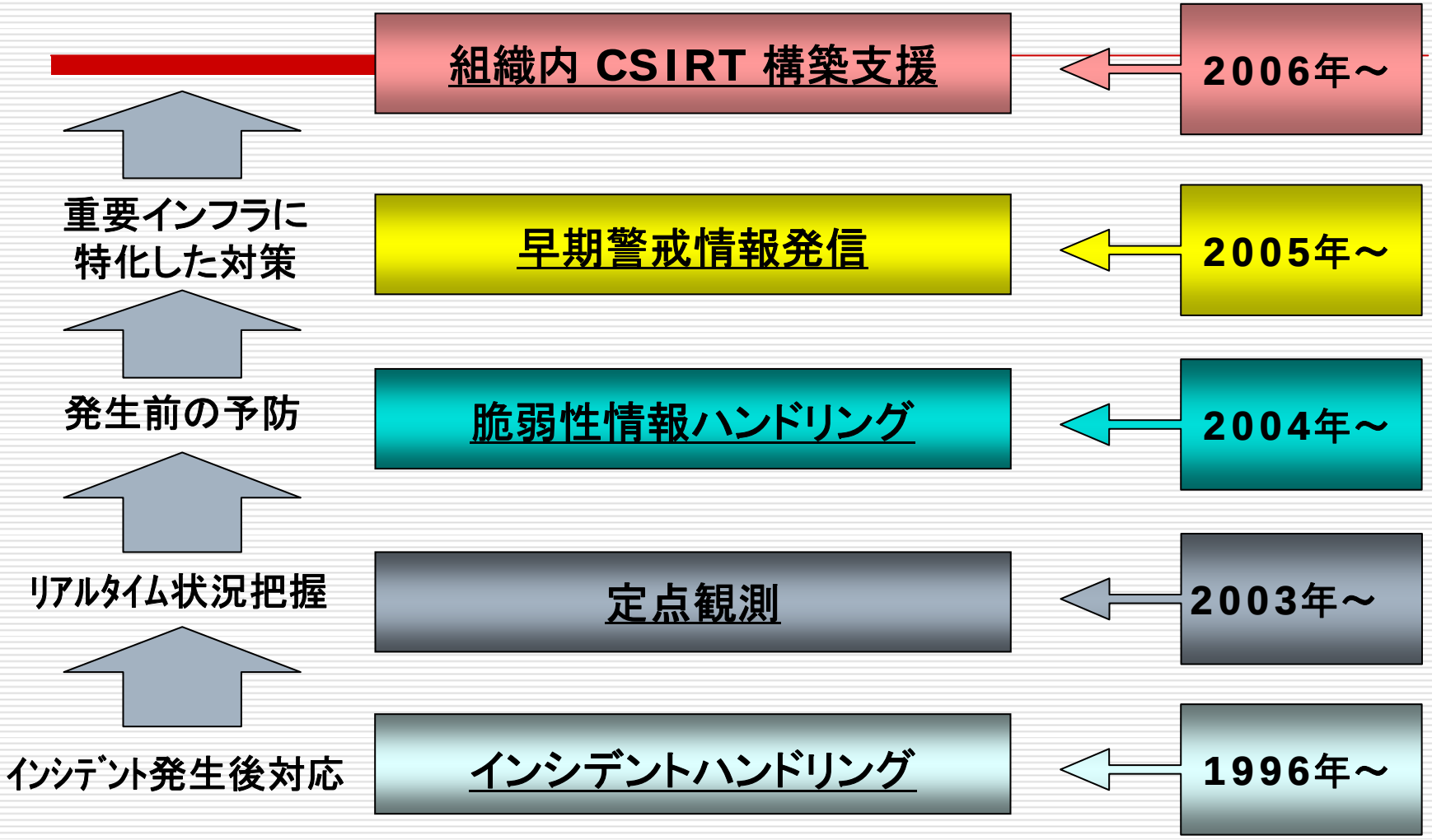


JPCERT/CC の活動目的

- 攻撃者のコストを引き上げるための活動を引き続き実施

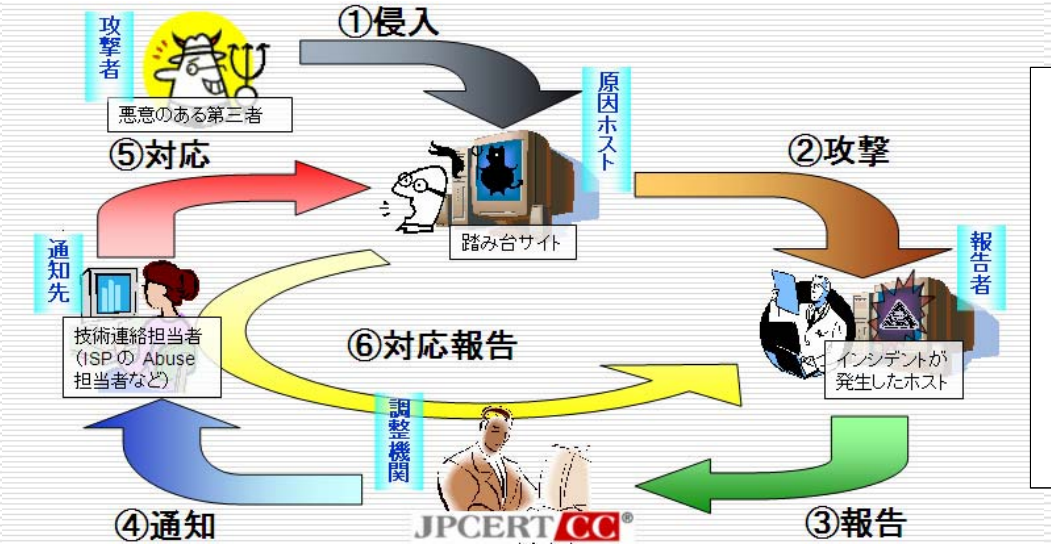


JPCERT/CCの活動

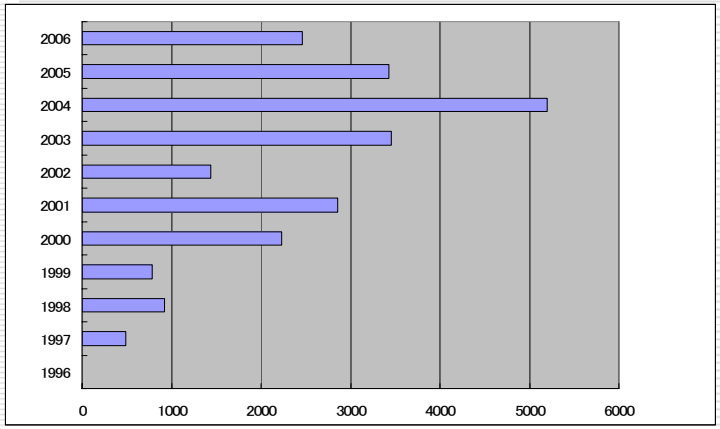


1. インシデントハンドリング

インシデント対応の流れ

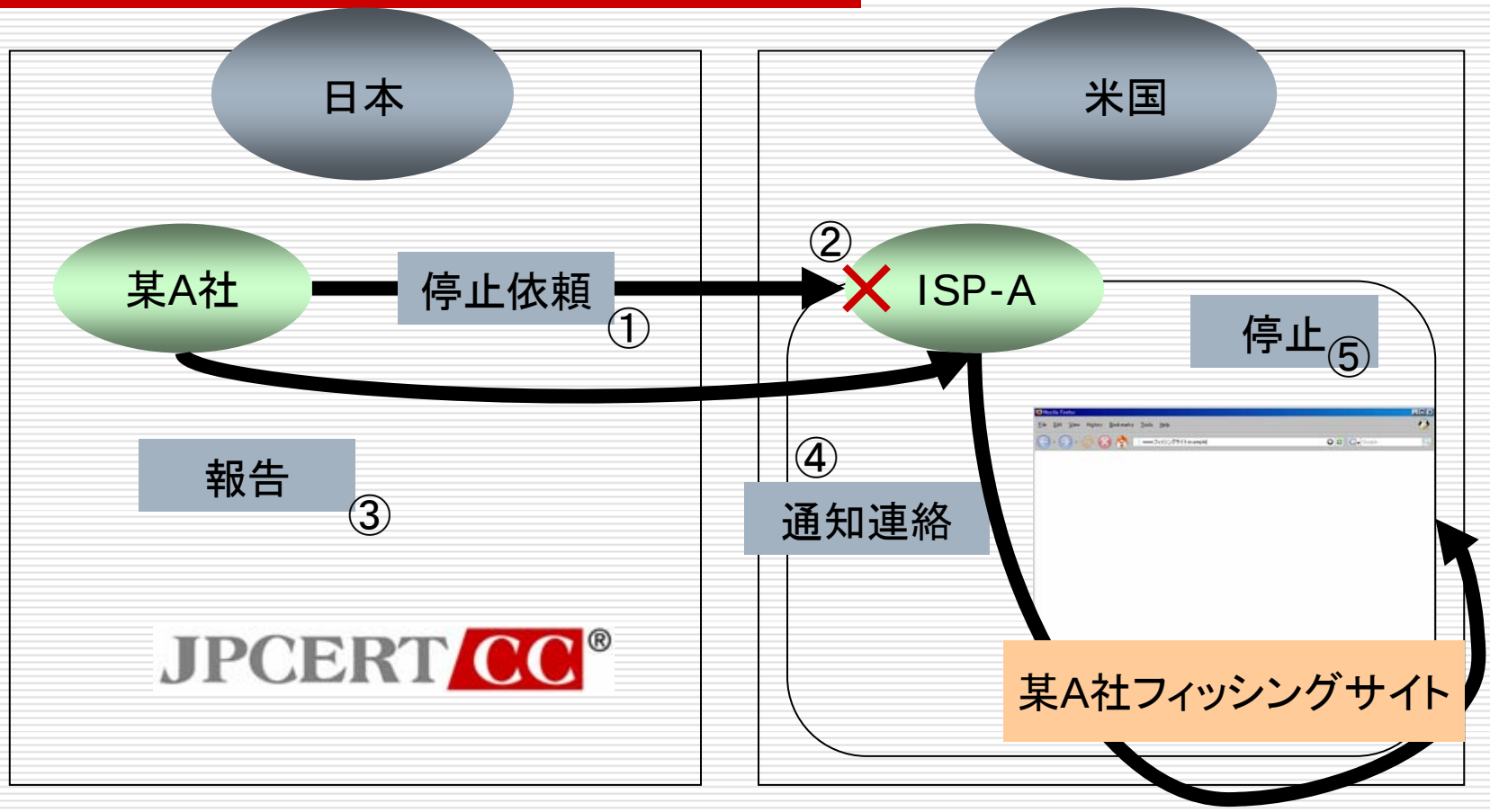


インシデント報告件数の推移



※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。
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) などがあります。

インシデント対応事例
（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事例

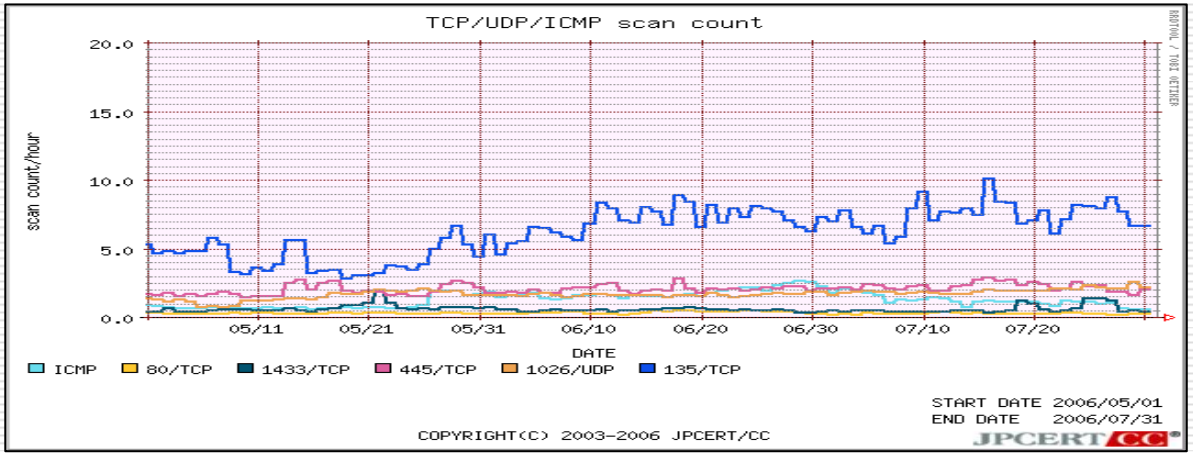
2. インターネット定点観測事業

- インターネット定点観測システム

  ISDAS: Internet Scan Data Acquisition System

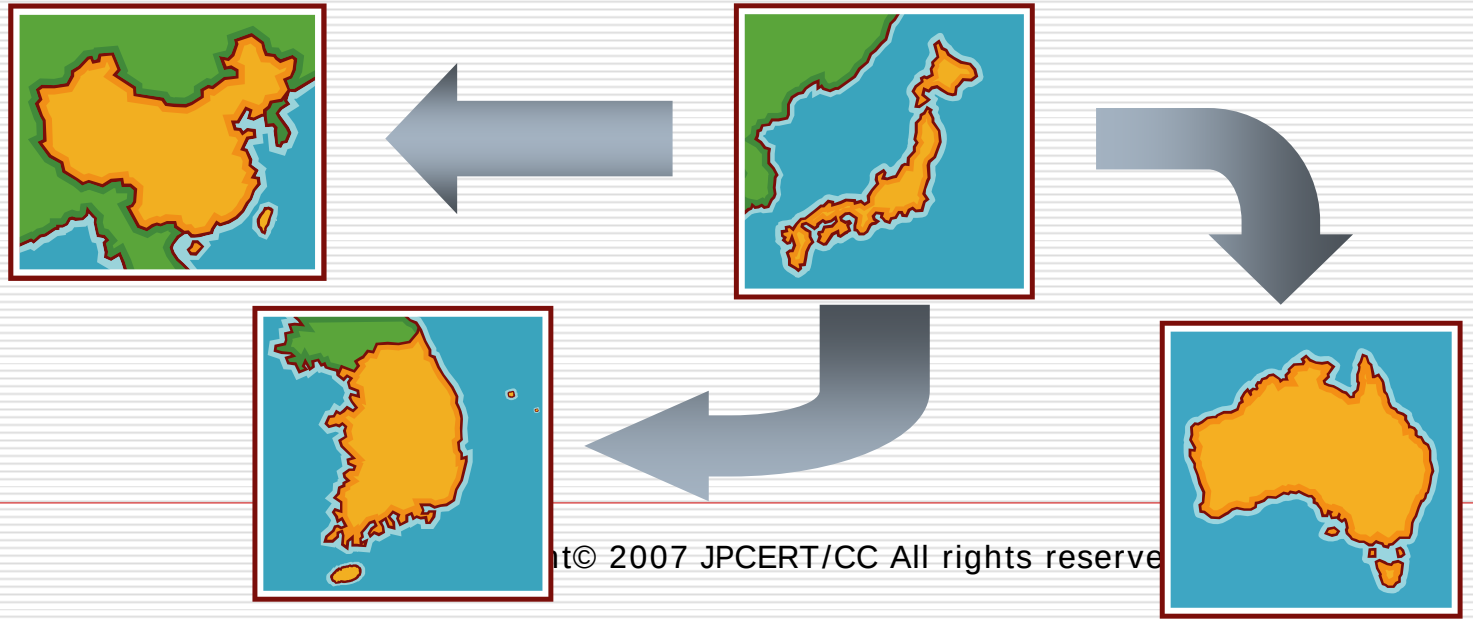
  http://www.jpcert.or.jp/isdas/

- 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

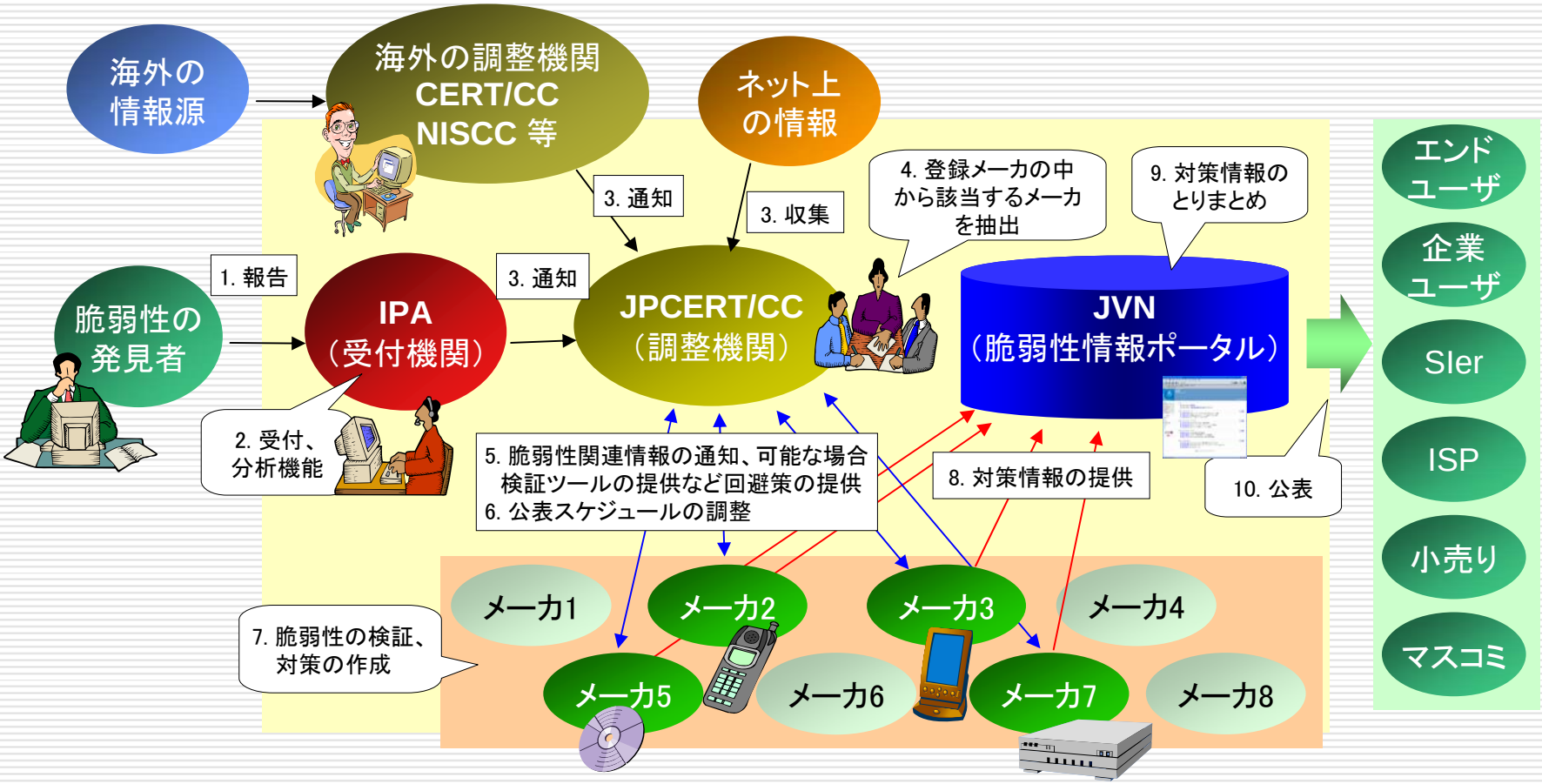


ISDASデータ:
中国・韓国・オーストラリアへの情報連携

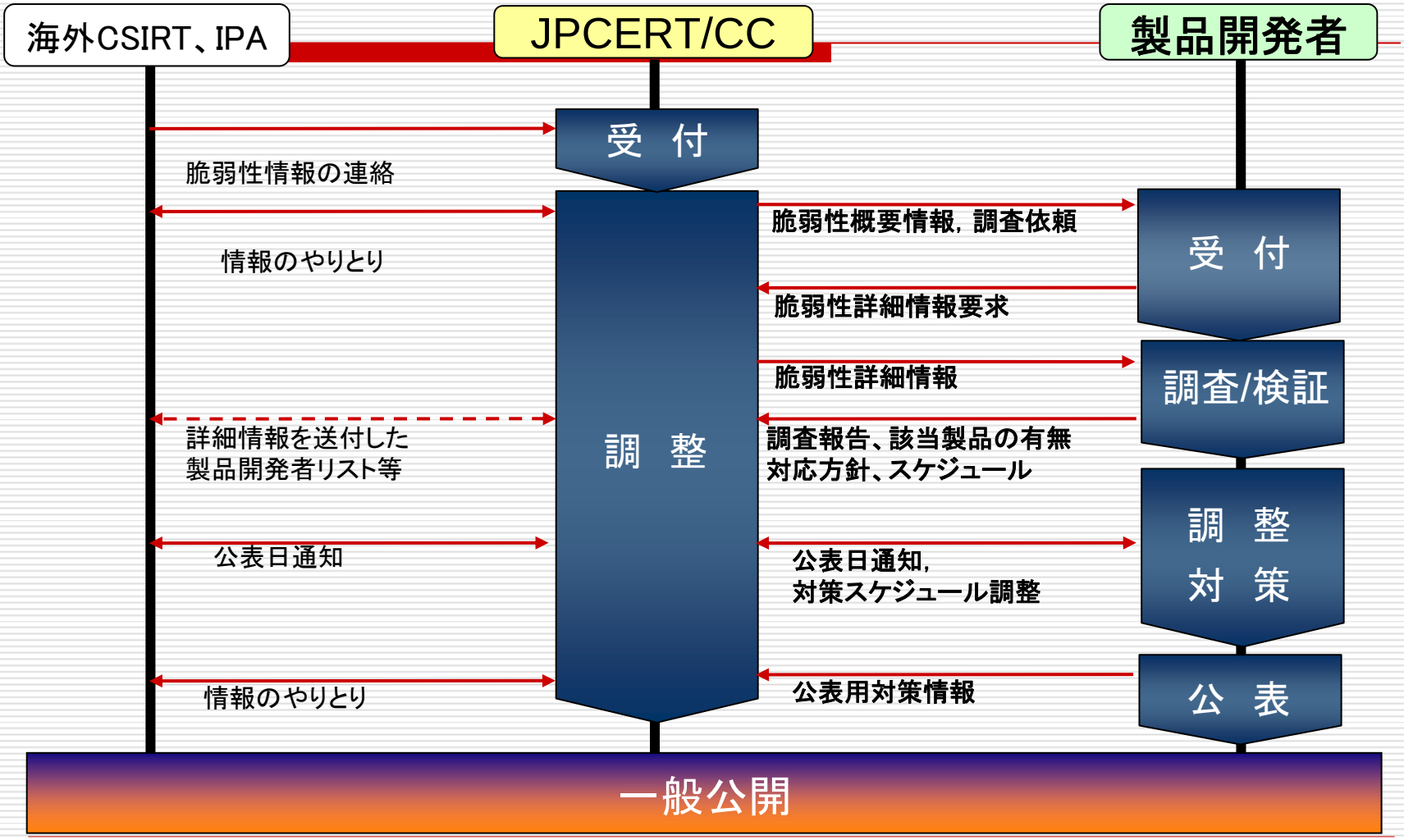
- ISDASにて収集した各国発のスキャンデータを IODEF形式で送信
  - 1日分を毎日送信
  - src_ip, src_port, dest_port, protocol timestamp を送信
  - 各国にて情報分析・インシデントの対応に利用



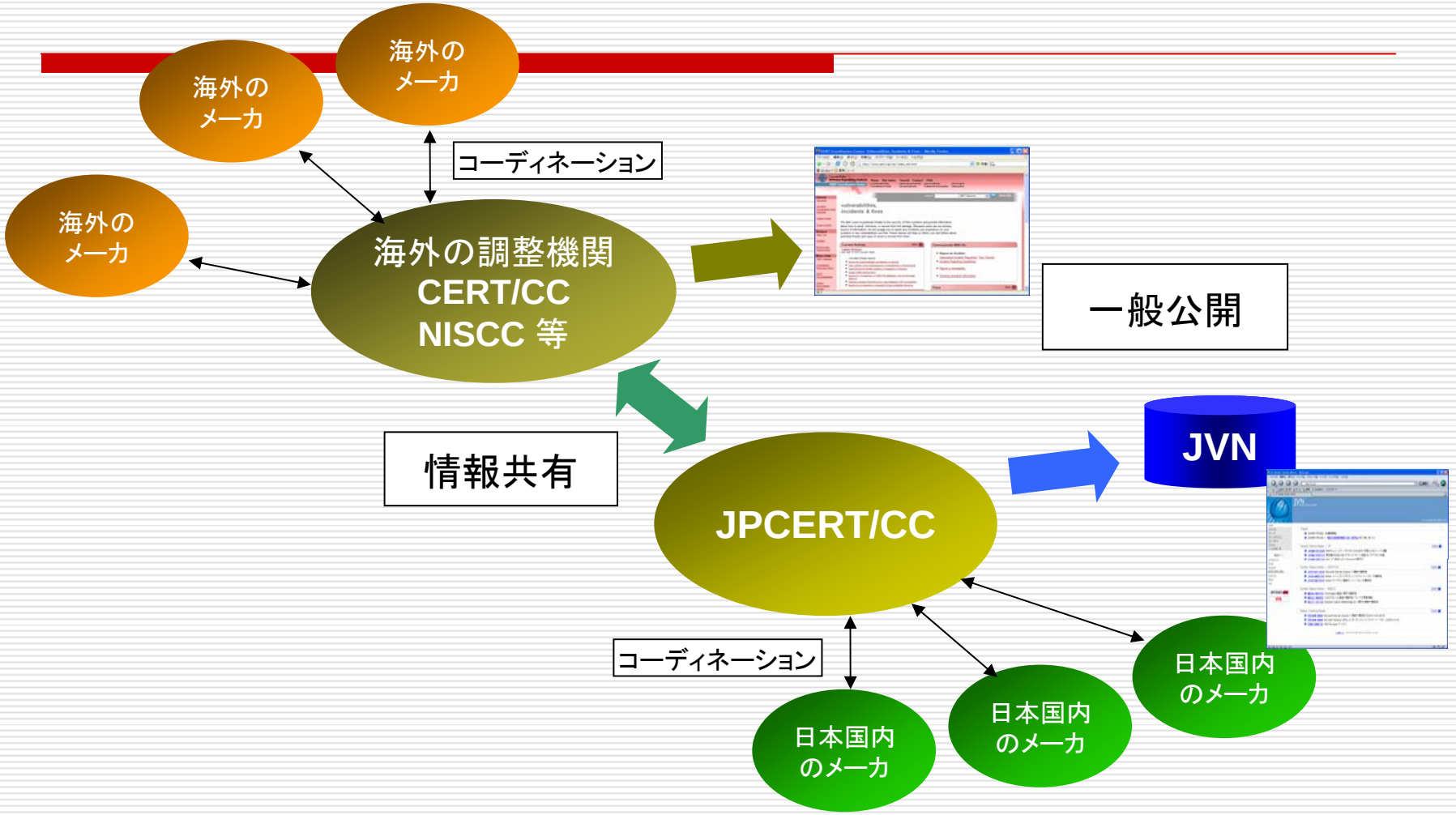
3. 脆弱性関連情報ハンドリング



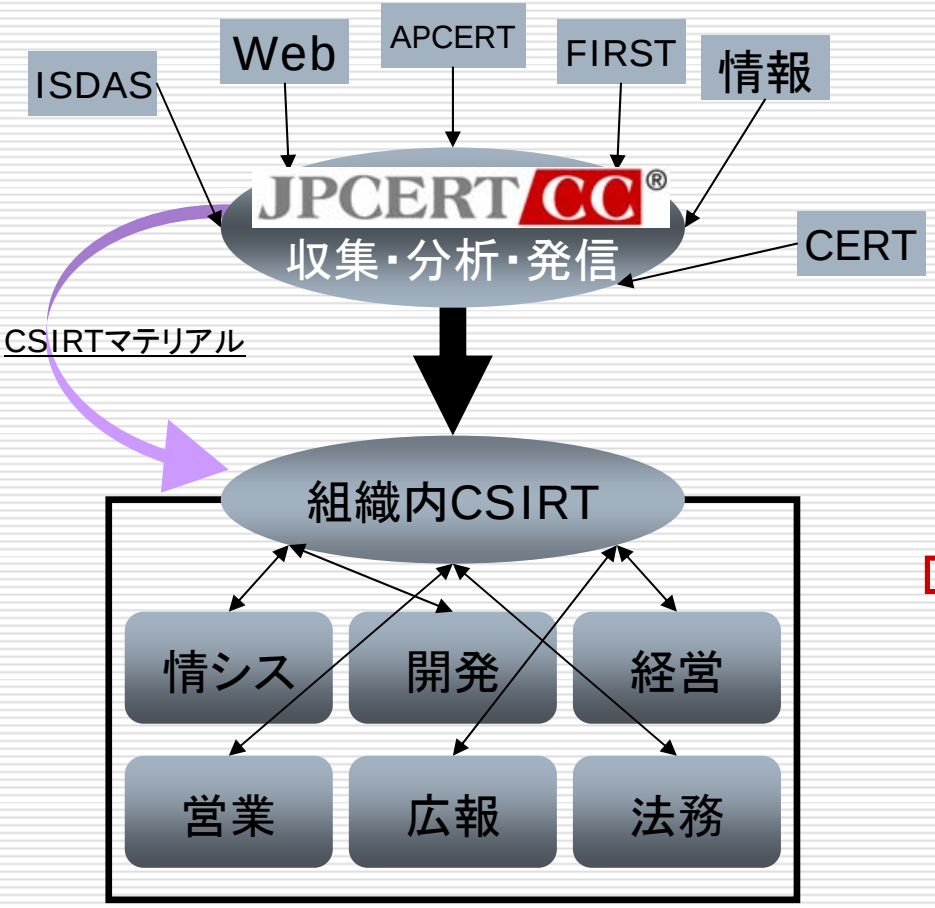
JPCERT/CCと製品開発者のハンドリング(やり取り)概要図



国際的な枠組みについて



4. 早期警戒事業



- 注意喚起（一般公開）の発行
- 早期警戒情報（非公開）の発信

- 組織内CSIRT 構築支援活動
  - CSIRT構築支援活動の知見の蓄積
  - CSIRT構築に必要なマテリアルの作成

組織内における円滑なインシデント対応

5. アジア太平洋地域における JPCERT/CCの主な国際連携活動

- 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

- National-CSIRT構築支援

  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
  - 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。

- 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：アジア太平洋地域におけるCSIRTの集まり。日本、中国、韓国、マレーシア、シンガポール、フィリピンなどが加盟している。
※AP* Retreat：アジア太平洋地域のインターネット団体の代表や、各国・地域で重要な役割を担っている組織から参加者が集まる会合。
年に1～2回開催されている。

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 に属してない国
  - ・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

最近のインシデントの傾向と課題

最近、目にする、耳にするトピックス

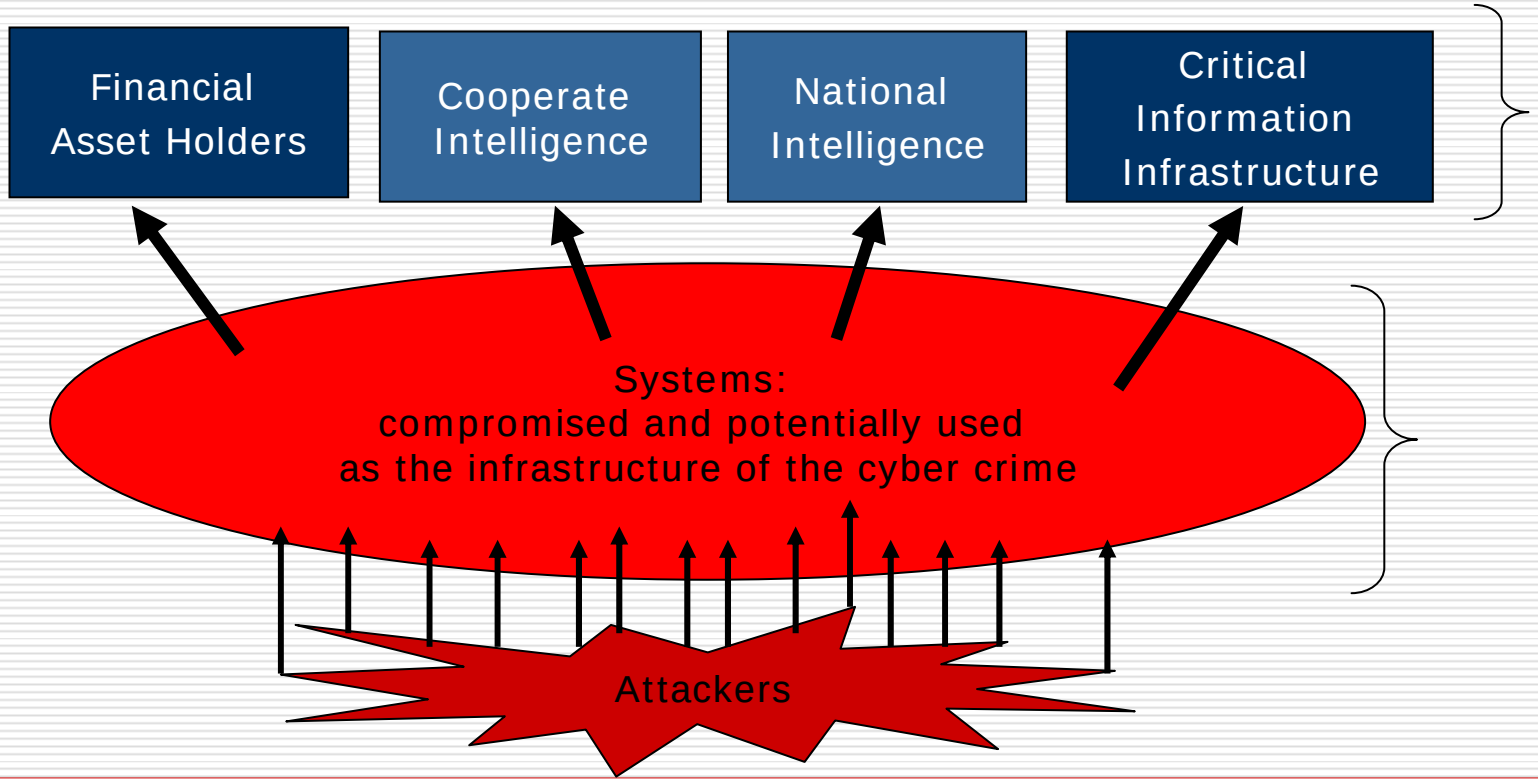
- ゼロデー攻撃
- 増え続ける脆弱性
  – 2006'の報告数8,046
  (CMU－CERT/CC統計情報)
- クライアントアプリケーションを対象とした攻撃
- ターゲット型攻撃
- 悪意のあるソフトウェアによって引き起こされるインシデントの増加
- ソーシャルエンジニアリング手法の高度化
- ボットネットの問題はよりいっそう深刻に
- 制御、コントロールシステム(SCADA) への注目
- DNSサーバーのようなインターネットインフラ自体への攻撃
- AP地域間の経済地域間における攻撃
- 初歩的な攻撃手法も引き続き発生
  —辞書攻撃、パスワード攻撃
- P2Pファイル共有ソフトネットワークにおける情報漏えいは引き続き深刻

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）
  - 攻撃対象数は限られているが被害は甚大
    - 日本独自のアプリケーション、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を利用
  - 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）

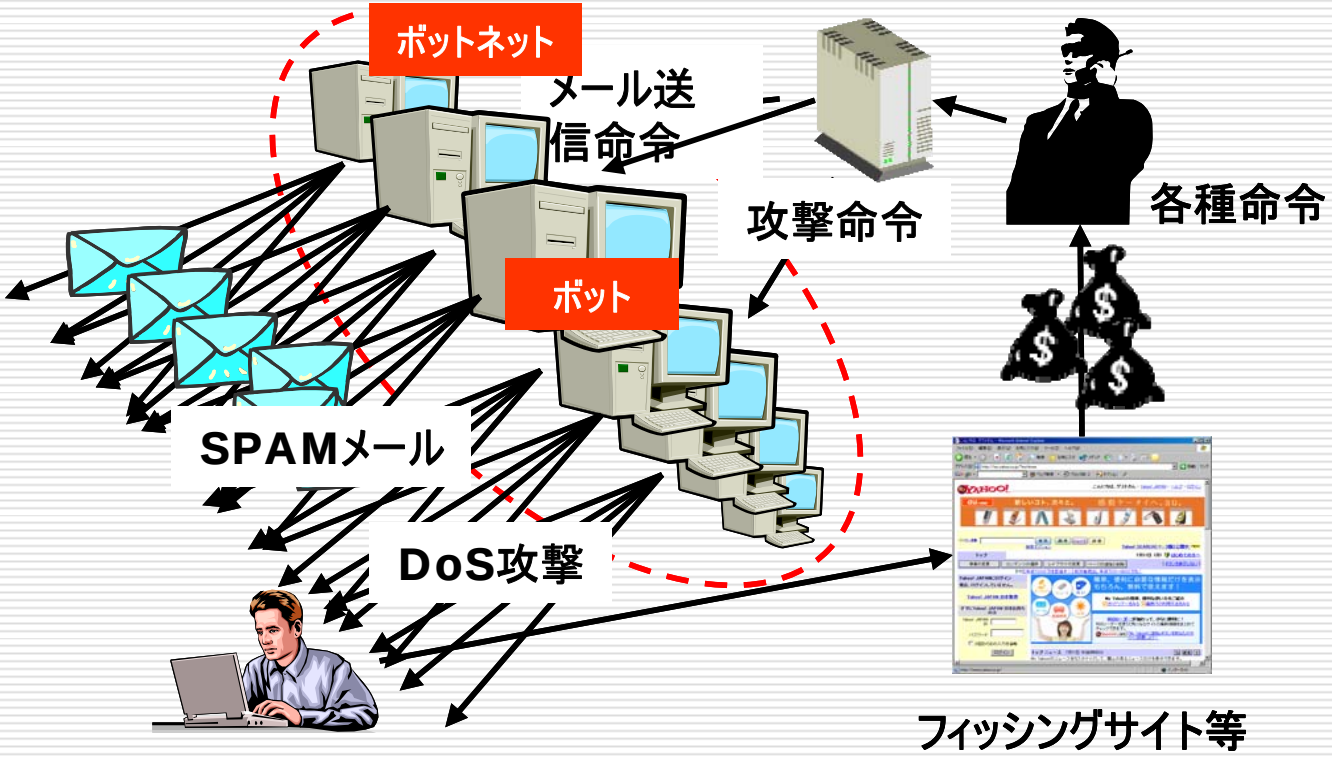
攻撃形態の一つ

パッチのあたった、セキュアなシステムに直接攻撃するよりも、そのシステムにアクセス権できる
ユーザー権限を持つPCに侵入し、それらを踏み台として、次の攻撃目標への攻撃をかける



ボットネットによる攻撃

■ウイルスのように感染し、攻撃者の命令に基づき、あらかじめ埋め込んだボットプログラム等を実行
■多数のボットが連携（ボットネット）することで、攻撃元を偽装し、対策を取りにくくすることが可能
■攻撃方法の複合化・高度化と、攻撃者の組織化・分業化の相乗効果により、被害の拡大が進む

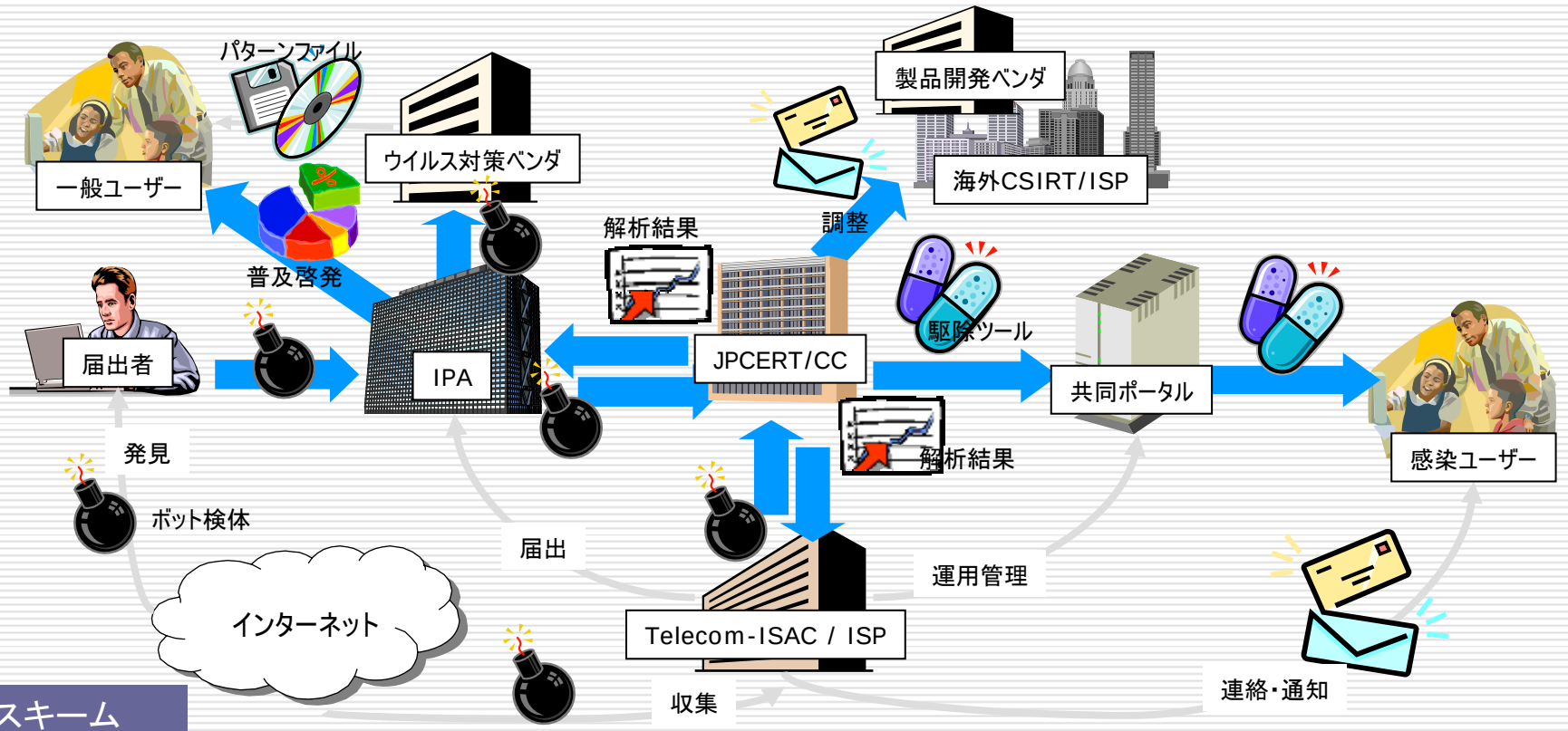


ボット対策推進事業（総務省・経済産業省共同事業）

目的

管理の不十分なコンピュータにユーザの知らない間にボットが設置されることで、DDoS攻撃、迷惑メールの送信、金銭詐取などが大規模かつ組織的に行われる事例が発生しており、ボットの感染防止、駆除及び被害の局限化等が急務

※ボット：「ロボット」から取られた造語で、ある種のプログラム（ボットプログラム）を埋め込まれたコンピュータを指す。ボット化したコンピュータは、攻撃者の命令に基づき、情報詐取、迷惑メール送信等の様々な活動を行う。多数のボットが連携（ボットネット）することで、攻撃元を偽装し、対策を取りにくくすることが可能

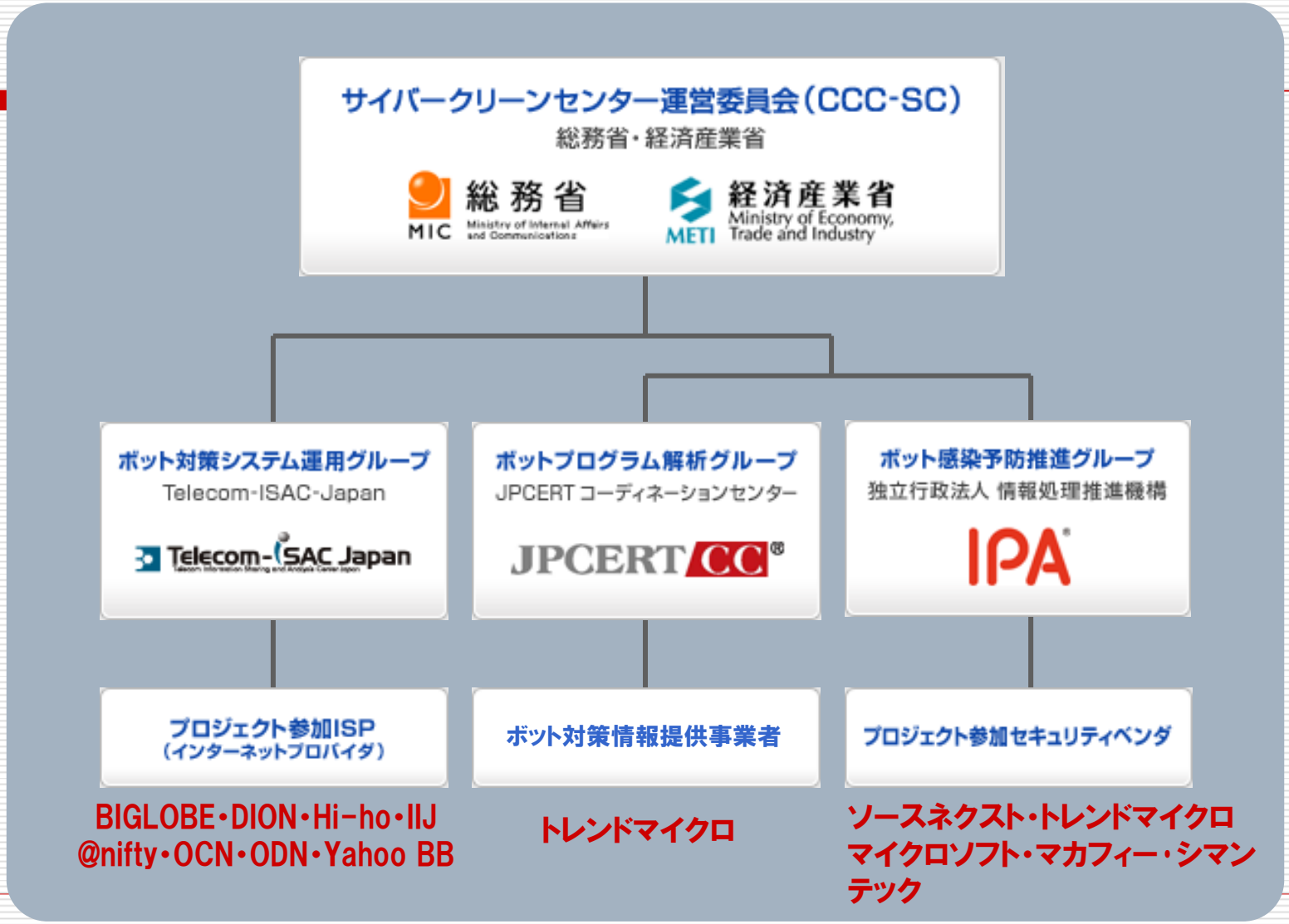


スキーム

■IPAに届け出窓口を設置すると共に、セキュリティベンダと連携してウイルスソフト等による対策も実施。（予防策）
■JPCERT/CCはTelecom-ISAC等と連携し、ボットの検体を入手、解析することで挙動を分析し、駆除ツールを作成する(感染後対策)。

出典：ボット対策事業開始式における説明資料

サイバークリーンセンター運営体制



専用ポータルサイト:
https://www.ccc.go.jp/

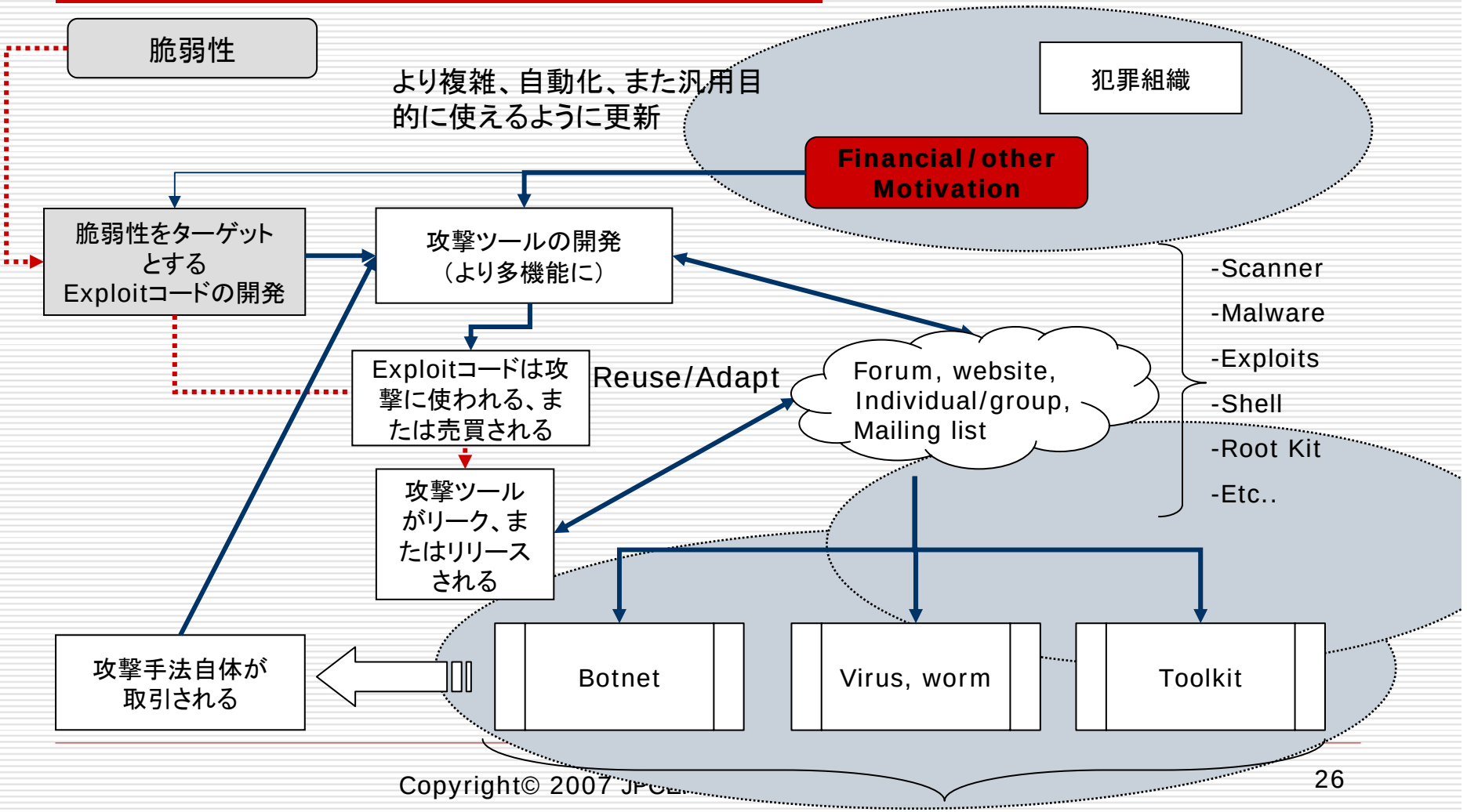
- 一般ユーザ向け啓発サイト
- ボット感染者向け対策サイト

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(潜行化、プロ化)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

- **攻撃手法の巧妙化と攻撃の迅速化**
  - 脆弱性の悪用
  - ゼロディアタック
  - ユーザーアプリケーションの脆弱性をターゲットとした攻撃
    - セキュリティ/認証製品や、通信機器の脆弱性をねらって、遠隔から攻撃、コントロールするという攻撃手法
      ⇒ ユーザーのマシーン上で使われているアプリケーション (ドキュメントファイルなど)の脆弱性をついて攻撃
      ※攻撃が一般ユーザーに近いところで

アンダーグラウンドコミュニティにおける マルウェアのライフサイクル



最近のセキュリティインシデントの動向（3）

- 原因追求の困難化
  - システムに特化した仕組みの理解
  - 人間の行動と密接に関連（技術だけの問題ではない）
  - 最新のセキュリティ関連情報の把握の必要性

- 企業情報窃取
  - 特許、市場戦略、プロセス、デザイン、開発啓発…

課題

- 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
  - 個々のインシデントに関する情報はあるが、脅威分析につかえるような統計データや分析手法が不足
  - マルウエア等の技術上の問題を解析する技術等はある程度備わってきているが、その背景や傾向を社会環境等と結びつけて分析する機能が不十分
- 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
- 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を「実装」してもらうための施策

お願い

- JPCERT / CCでは、
  - 情報セキュリティインシデントに関する情報提供を目的としたご報告（情報提供）
  - JPCERT / CCによる対応のご依頼（調整依頼）

  を受け付けております。

- 情報提供
  ⇒インシデントの状況の分析に役立てるとともに、統計情報として施策に反映
  （情報提供元に関する情報は非公開）

- 調整依頼
  ⇒ コーディネーションの実施、対策情報への反映

- ご報告、ご依頼は
  - Email：info@jpcert.or.jp
    PGP Fingerprint ：BA F4 D9 FA B8 FB F0 73 57 EE 3C 2B 13 F0 48 B8
  - インシデント報告様式： http://www.jpcert.or.jp/form/

連絡先

- 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/