進化するインシデントレスポンス
ー攻撃の変質への対応、新たな領域への対応

平成24年5月24日
サイバー犯罪に関する白浜シンポジウム　講演
一般社団法人JPCERTコーディネーションセンター　早貸淳子

JPCERT/CCとは

一般社団法人JPCERTコーディネーションセンター

（JPCERT/CC（ジェーピーサート・コーディネーションセンター））

Japan Computer Emergency Response Team Coordination Center

- https://www.jpcert.or.jp/
- サービス対象: 日本国内のインターネット利用者やセキュリティ管理担当者、ソフトウエア製品開発者等（主に、情報セキュリティ担当者）
- コンピュータセキュリティインシデントへの対応、国内外にセンサをおいたのインターネット定点観測、ソフトウエアや情報システム・制御システム機器等の脆弱性への対応などを通じ、セキュリティ向上を推進
- インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、**我が国の窓口となる CSIRT**

※各国に同様の窓口となる CSIRTが存在する

（例えば、米国のUS-CERT,CERT/CC、中国のCNCERT, 韓国のKrCERT/CC、など）

- 経済産業省からの委託事業として、コンピュータセキュリティ早期警戒体制構築運用事業を実施

JPCERT/CCの活動

JPCERT CC®

インシデント予防

脆弱性情報ハンドリング

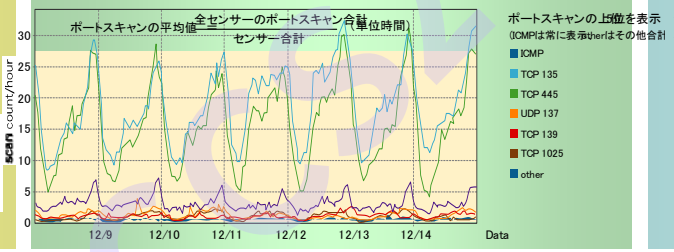
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

インシデントの予測と捕捉

情報収集・分析・発信
定点観測（ISDAS/TSUBAME）

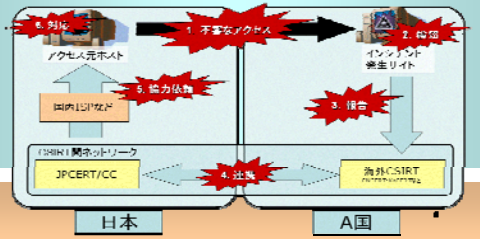
- ネットワークトラフィック情報の収集分析
- 定期的なセキュリティ予防情報の提供



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
（インシデント対応*調整*支援）

- マルウエアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有



早期警戒情報提供

重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信

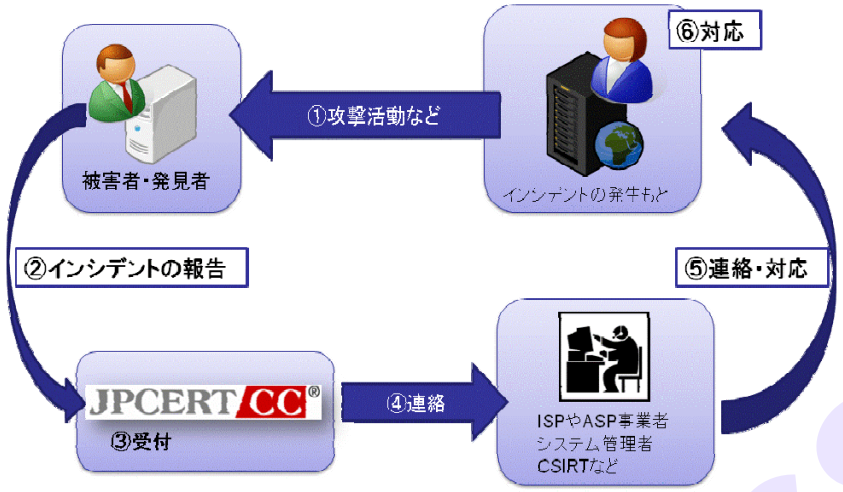
CSIRT構築運用支援

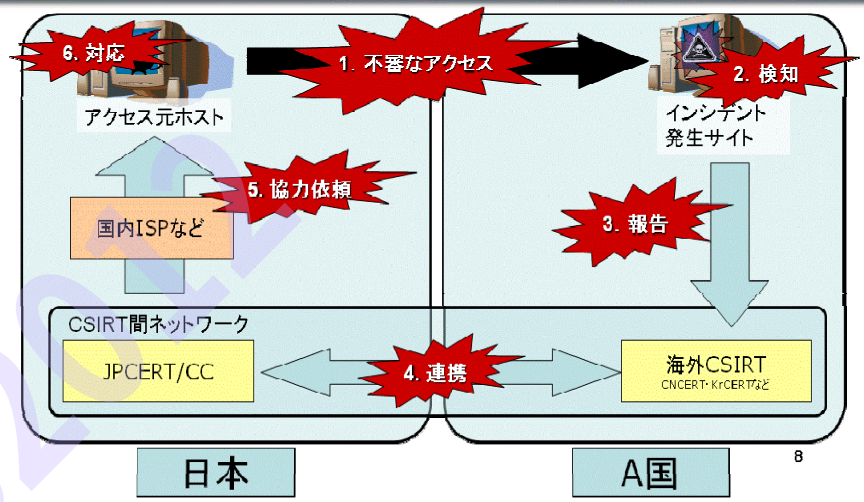
海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援

アーティファクト分析

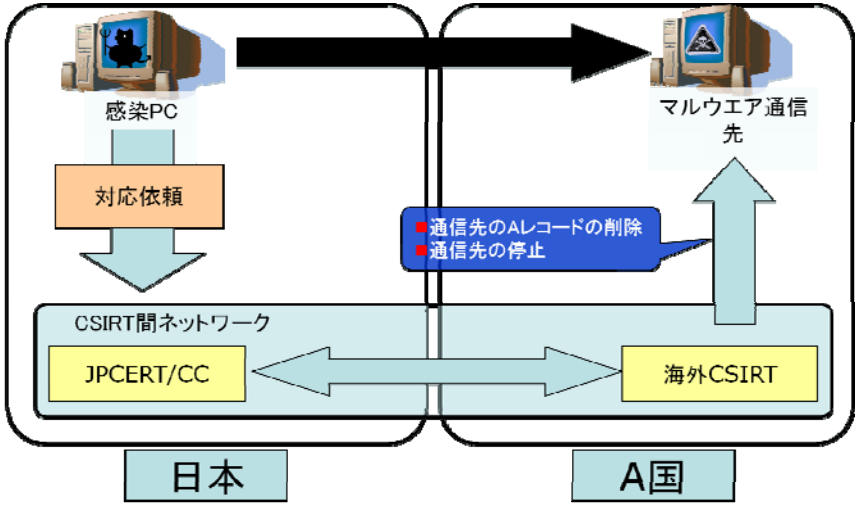
マルウエア（不正プログラム）等の攻撃手法の分析、解析

1. インシデントハンドリング
(1) 従来型の対応支援活動



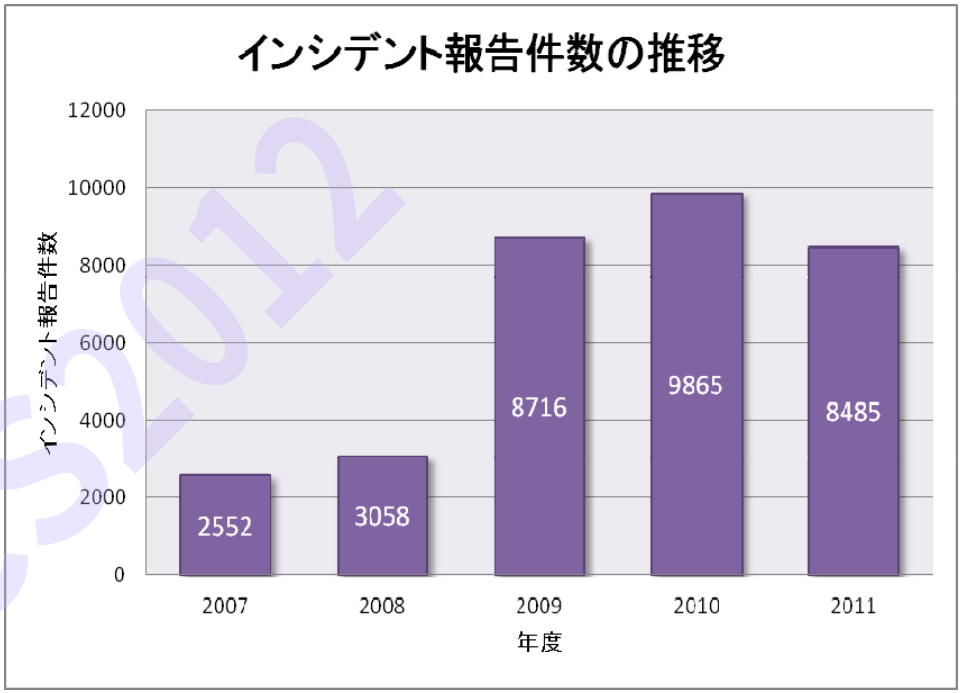


1. インシデント報告の受付
2. (必要に応じ)マルウエアの解析
   - ① 挙動、機能、脅威
   - ② 被害拡大抑止のための調整を実施するための接続先等の情報の抽出
3. 被害の拡大抑止のための関係先へのコーディネーション
4. 必要に応じ、早期警戒情報、注意喚起の発行



実際に取り扱っている案件（一部）
※複合的な場合が多い

- フィッシングサイト停止依頼
  - 国内事業者のサイトが海外に
  - 海外事業者のサイトが国内に
- キーロガー等による情報流出
  - 国内ユーザの個人情報
- マルウェア公開サイト停止依頼
- 攻撃予告
  - ○月×日に某ウェブサイトを攻撃する、などの内容
- SQLインジェクション攻撃
- 標的型攻撃
  - マルウェアに関する対応
- 侵入
  - サーバへの侵入被害
- ボット・ボットネット・C&C
  - 海外のボットネットと通信している国内のC&Cのリストなど
- DoS/DDoS
  - 海外からの大規模なアクセス
- 脆弱なホストのリスト
  - 海外組織によって収集された国内の脆弱なホストのリスト
- ID/PW公開サイト



(2)従来型の対応調整では解決が難しい問題

- いわゆるAPT型の攻撃と活動家による攻撃では、同じ標的型攻撃であっても対応の仕方が異なる。
  - APTの場合は、被害者は気付きづらく、攻撃者は攻撃については一切公開しない
    - インシデントの発生の事実自体が公表されない。
    - 攻撃に気づいたことを攻撃者に気づかれずに対処する等の工夫
  - 活動家による攻撃では、攻撃の成功についての声明が出たり、窃取した情報が公開されたりする
    - インシデント発生の事実や窃取された情報が公開される
    - インシデントへの対処ぶりについても注目があつまる
    - 社会的な反応が活動家による攻撃のエネルギーにもなる
- が、双方とも従来型の対応支援（サイト閉鎖や活動の停止依頼等）では解決が困難な場合が少なくない。

※Advanced Persistent Threat (APT):
(仮訳) 複合的な（たとえば、サイバー上の、物理的な、又は詐欺的な）攻撃手法を用いることにより、目的を達成する機会を作出することができる、高度な専門的知識と莫大なリソースを有する攻撃主体。ここでいう目的とは、一般的に、情報窃取や、任務・事業若しくは組織の重要な局面に関する弱体化又は妨害、あるいは将来においてこれらの目的を実現するための準備行為を目的として、標的とした組織のITインフラ中に、足場を構築し、利用し続けることが挙げられる。
advanced persistent threatは、(i) 長期にわたって、繰り返し繰り返し目的を達成しようとし、(ii) 対策を講じる側の対抗措置に応じて変化し、（iii）目的を達成するために必要となる双方向の通信レベルを維持する確固たる意志をもつ。
※NIST SP800-39「Managing Information Security Risk: Organization, Mission, and Information System View」【Appendix B GLOSSAR Y】http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

執拗に行われる巧妙な標的型攻撃の場合のインシデント対応

JPCERT CC®

- コーディネーションにともなうリスクの検討
  - 対応していることを気付かれる

    → 攻撃手法が切り替わってしまい、対策を講じたつもりでも、無意味になってしまう可能性も。
  - 情報やサイトの価値を気付かせる

CASE1) JPCERT/CC宛に届いたマルウエア添付メール(2009年3月)

- メールの送信元IPアドレスが他の標的型攻撃で使われたマルウエアの通信先と同じ
- 通信先は国外IPドメイン・国外IPアドレス
- コーディネーション後
  - Aレコードが削除される

コーディネーション以外の手段
＝たとえば、検知・対策情報の共有等も必要

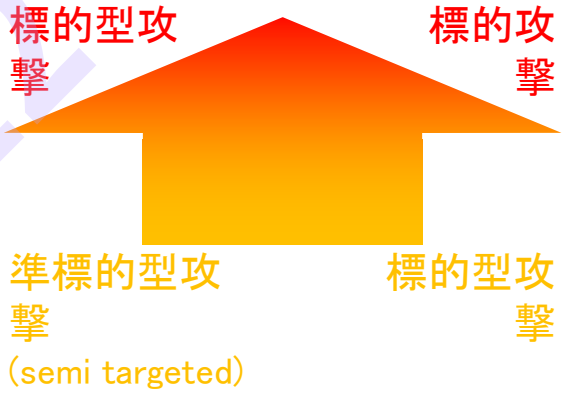
  - 同じIPアドレスが他のサイト名でも使われていることを確認

CASE2) インシデント情報として提供された複数のマルウエア(2009年5月)

- 同じ通信先の同種のマルウエアを複数受領
- 通信先は国外IPドメイン・国外IPアドレス
- コーディネーション後
  - Aレコードが削除される
  - 同じIPアドレスが他のサイト名でも使われていることを確認

標的型攻撃：手法的にもいろいろ

- ソーシャルエンジニアリング的手法
  - 特定の組織や個人を対象とした攻撃
    - かなり”鋭利”なソーシャルエンジニアリング
      - ✓ 対象にとって価値のある情報を添える
      - ✓ 鋭利さ故に攻撃を受けた事実を外部に提供し難い
  - 特定の事柄に関心を持つ人を対象とした攻撃
    - 比較的”広角”なソーシャルエンジニアリング
- マルウエアの特徴
  - 未修正の脆弱性が積極的に悪用される
    - 修正アップデートが提供されている脆弱性も悪用される
    - ソフトウエア等の脆弱性を悪用するとは限らない
      → アイコン偽装やファイル名(拡張子)偽装等で実行ファイルを開かせる
  - インストールされるマルウエアの傾向
    - 情報収集を基本機能として有する
      → MACアドレスやコンピュータ名等を識別ID代わりに使う
    - バックドア型のマルウエア(RAT)がインストールされる
    - 外形的には使い捨てだが、中は同種ツールの使いまわし



“ゼロデイ”も多いが全てではない!!

“特注品”とは限らない!!

(3)情報共有+APTを意識したインシデントレスポンス方法の選択による対策

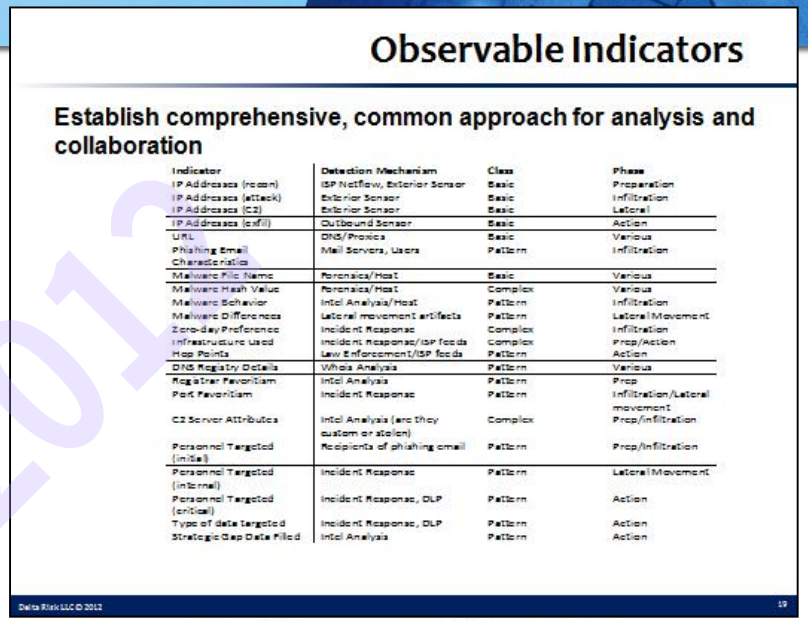
JPCERT CC®

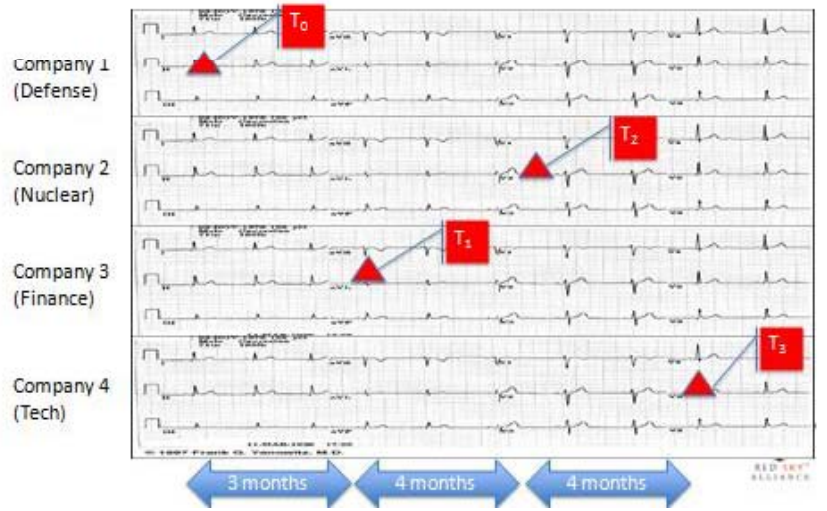
- 標的型攻撃を検出し、適切なレスポンス（対応）方法の選択を可能とするための**情報共有**の枠組み
  - 米国の先行事例
    - 検知情報等の共有
    - 情報窃取を目的とするステルス型の標的型攻撃への対応を可能とするセキュリティ対策製品やサービス
  - 日本モデル

※ 検知情報：

誰とでも共有できる情報ではないし、
誰でも使いこなせる情報でもない。

- 攻撃の検知のための情報等の共有を受けることが可能となる機能や体制が必要＝組織内CSIRT等





平成24年2月14日開催「サイバー情報共有のためのワークショップ～海外事例と情報共有の取組について～」配付資料から

(4)経営層のリスク認識を深めてもらうための活動も必要

Nortel の情報漏えい事案

- *Wall Street Journal* (2012年2月14日)によると, Nortel 社(2009年破産手続き開始) が10年以上にわたって、技術文書や、研究開発報告書、経営戦略、従業員のe-mail等の文書を窃取されていた。
- Nortel社のCEO等(詐欺罪等による刑事訴訟中)は、その事実を知っていたが、事業や知財権の売却の過程で、その事実を相手方に公開せず。

(記事からの抜粋)

"Mr. Shields and a handful of the firm's computer-security officers soon learned that hackers had apparently obtained the passwords of seven top officials, including a previous CEO. The hackers had been infiltrating Nortel's network, from China-based Internet addresses, at least as early as 2000, Mr. Shields and his colleagues determined.

Hackers had almost complete access to the company's systems, Mr. Shields said, because the internal structure of Nortel's network posed few barriers. "Once you were on the inside of the network, it was soft and gooey," he said.

About six months later, Mr. Shields said, he saw signs that hackers were still in the system. Every month or so, a few computers on the network were sending small bursts of data to one of the same Internet addresses in Shanghai involved in the password-hacking episodes. Unexpected transmissions like these—where one computer sends a quick "ping" to another—often suggests the presence of spyware, security experts say.

"That's the really deep covert presence," said one person familiar with Nortel's investigation. "There is something on those computers that's doing that, and finding it is very difficult."

(5)別の視点：法改正への対応

不正指令電磁的記録の作成、提供等（刑法）やフィッシング、IR・パスワードの不正流通の犯罪化（不正アクセス禁止法）に伴う対応の検討

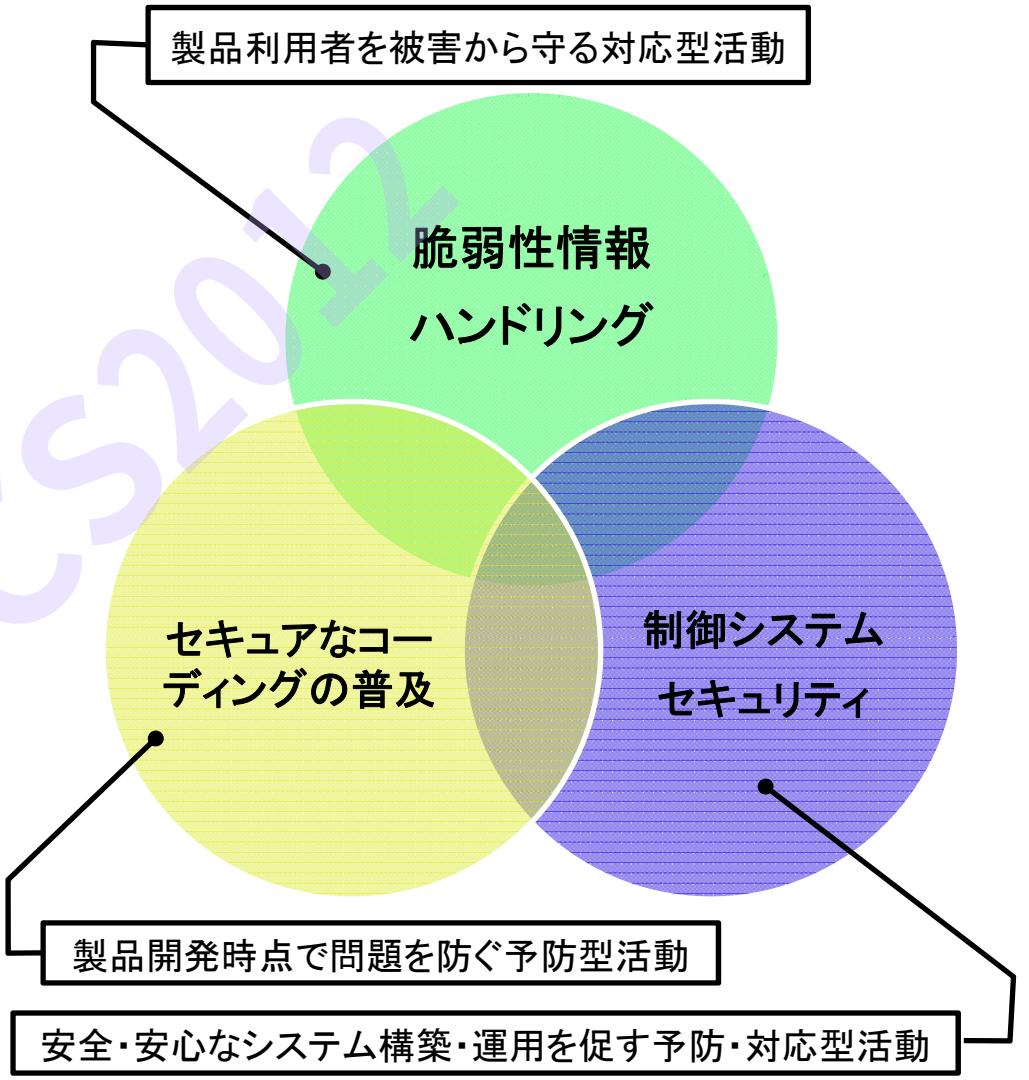
- 関係機関との連携のための具体的な方法について、官民ボード等において検討を進めている。
  - 攻撃に関与している者を捕まえることが、最善の抑止策
  - とはいえ、具体的な対応の局面では、事象の解決や被害拡散抑止のための対策を優先させる必要も
  - たとえば、

・　・　・　・　・

2. 制御システム　セキュリティ
(1)従来の活動

- 高度な情報処理を実現するICT環境に潜む脆弱性によって脅かされる、全ての利用者の安全を守る為に3つの観点から活動

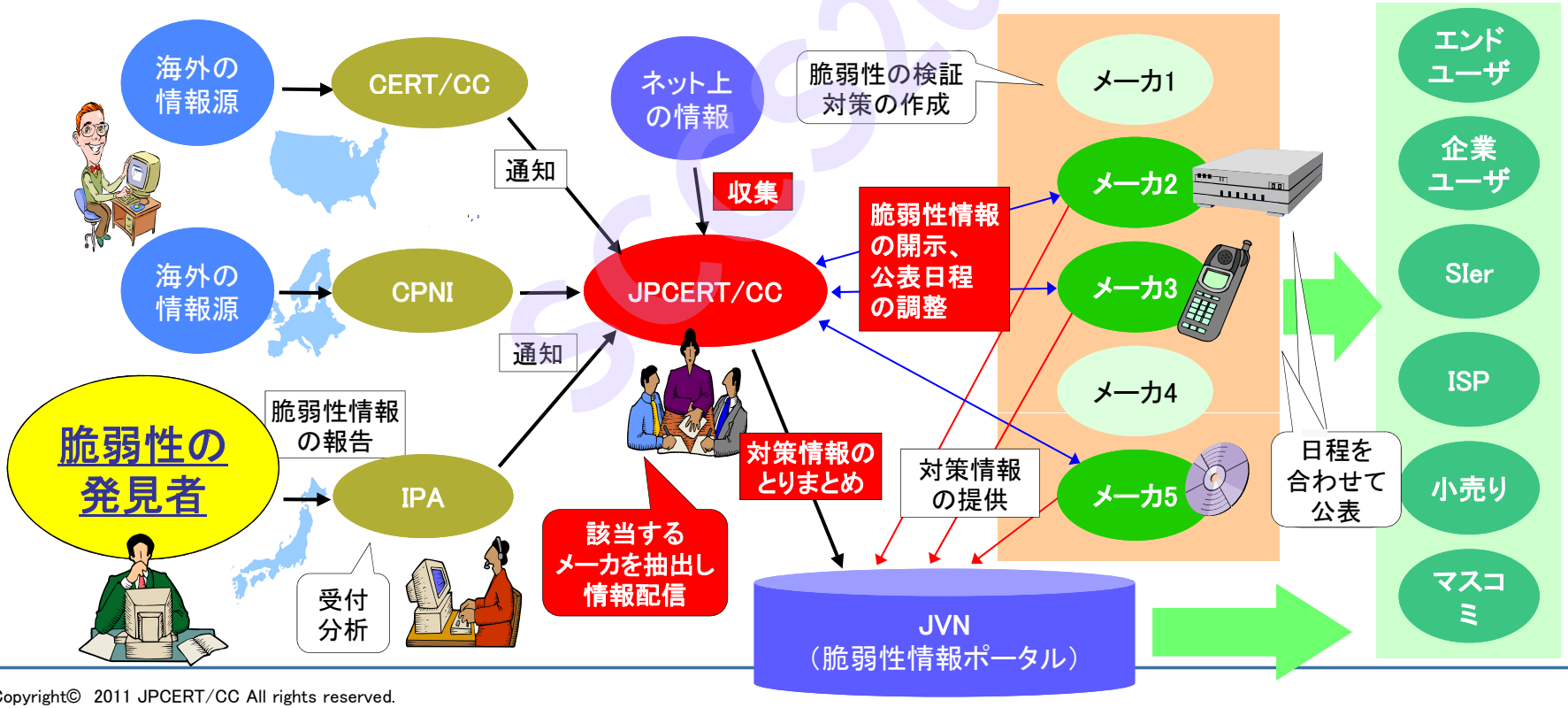
  - ゼロデイの脅威から製品利用者を守る
    ⇒脆弱性情報ハンドリング
    発見された製品や規格の脆弱性が、対策も取られないまま公になる前に、拡大する被害を未然に防ぐための活動
  - 正しいコーディング方法を広め、安全な製品開発を促す
    ⇒C/C++セキュアコーディング
    不十分な理解によりコーディングされた脆弱なソフトウエア製品がもたらす脅威を未然に防ぐための活動
  - 安全・安心なシステムの開発・運用を促す
    ⇒制御系システムセキュリティ
    汎用IT製品が導入された事によって、その脅威にさらされ始めた制御系システムにおいて、安全・安心な環境を維持する為の開発・運用を促す活動



【参考】(従来からの)情報システムに関する脆弱性関連情報ハンドリング
情報セキュリティ早期警戒パートナーシップ(国内)

JPCERT CC®

- 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
  - IPAが受付機関、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



(2)制御システムセキュリティに特化したチームを新設
＝日本版ICS-CERTの設置

これまで行ってきた制御システム機器に関する脆弱性関連情報ハンドリングや制御システムセキュリティに関する情報発信等の活動を進化させて、以下の活動を行う。

1. インシデントハンドリング支援業務
   - 事案対処支援：現地での対応支援を含む
   - 検証（再現性・攻撃ツール etc）：新設された制御システムセキュリティセンター（技術研究組合）テストベッド等とも連携
   - 執拗な特定の目的による巧妙な攻撃への対応については、情報システムに対するものと同様の問題が。

2. 脆弱性関連情報調整業務
   - 制御システム関連製品における脆弱性対応のスキーム検討
     - JVN等での公開が最適解ではない。
   - 制御システム関連製品開発者の脆弱性対応に係る支援　等

3. 制御システムに関するインシデントハンドリング、脆弱性関連情報調整のためのコミュニティ運営
   - カンファレンス開催
   - Idaho Advanced Training 日本向け開催　等

ご質問、お問合わせは

- インシデントの報告、対応依頼
  - http://www.jpcert.or.jp/research/#webdefacement
  - 電子メール：info@jpcert.or.jp (PGP 公開鍵)
    (*) JPCERT/CC PGP 鍵が更新されました。詳細はリンク先をご覧下さい。
  - FAX: 03-3518-2177 （インシデント報告以外のものは 03-3518-4602）
  - 電話: 03-3518-4600
- 早期警戒情報の配信、マルウエア解析レポート
  - http://www.jpcert.or.jp/wwinfo/
  - JPCERT/CC 早期警戒グループ 早期警戒情報登録受付窓口
    E-mail :ww-info@jpcert.or.jp
- 注意喚起、ウィークリーレポート等を受信いただくJPCERT/CCメーリングリストへの登録
  - http://www.jpcert.or.jp/announce.html