JPCERT CC®

TCG JRF

第6回公開ワークショップ

サイバーセキュリティの脅威動向と取り組み

2014年12月3日（13:30-14:00）

JPCERTコーディネーションセンター
理事・分析センター長　真鍋　敬士

JPCERT/CCとは

一般社団法人　JPCERTコーディネーションセンター

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

- 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）がサービス対象
- 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（窓口CSIRT）

CSIRT: Computer Security Incident Response Team

※各国に同様の窓口となるCSIRTが存在する(米国のUS-CERT、CERT/CC、中国のCNCERT, 韓国のKrCERT/CC、等)

- 経済産業省からの委託事業として、サイバー攻撃等国際連携対応調整事業を実施

JPCERT/CCの活動

インシデント予防 → インシデントの予測と捕捉 → 発生したインシデントへの対応

脆弱性情報ハンドリング

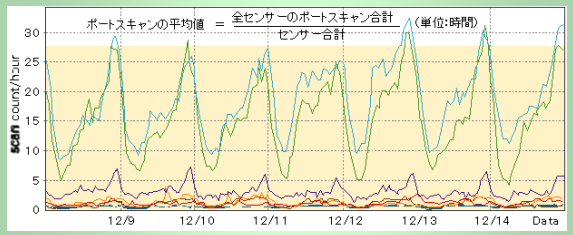
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

定点観測（TSUBAME）

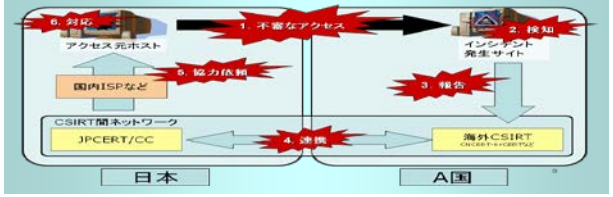
- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



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

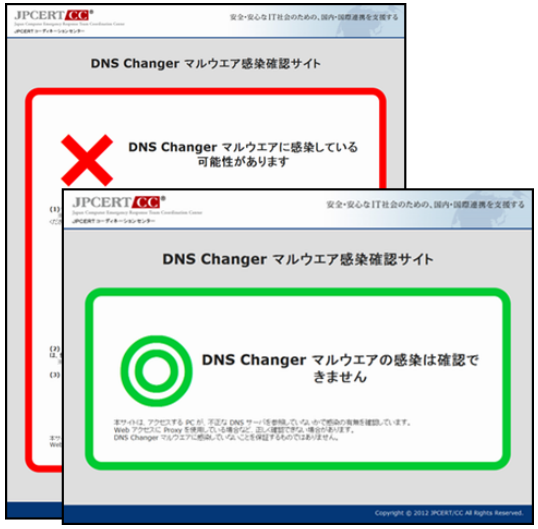


早期警戒情報	重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信
CSIRT構築支援	海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援
制御システムセキュリティ	制御システムに関するインシデントハンドリング、情報収集・分析発信
アーティファクト分析	マルウエア（不正プログラム）等の攻撃手法の分析、解析
国内外関係者との連携	日本シーサート協議会、フィッシング対策協議会の事務局運営等
国際連携	各種業務を円滑に行うための海外関係機関との連携

近年の特徴的な取り組み

DNS Changer 感染確認サイト

- DCWG（DNS Changer Working Group）
  暫定DNSサーバの運用を2012年7月9日に終了
- 感染確認サイト（終了）
  http://www.dns-ok.jpcert.or.jp/

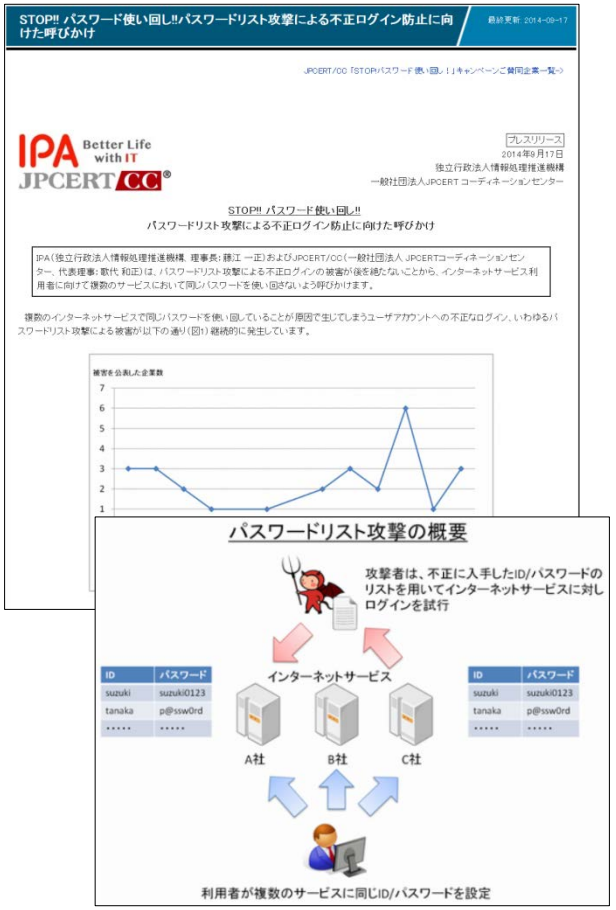


オープンリゾルバ確認サイト

- オープンリゾルバ問題
  2006年ころから実際のインシデントとして認知されるように
- 確認サイト（2013年10月31日～）
  http://www.openresolver.jp/

STOP!! パスワード使い回し!

- 賛同企業 24社と協力して普及啓発



本日お話ししたいこと

近年報告されるサイバー攻撃の中には、インターネットやイントラネットの仕組みを巧妙に悪用したものが見受けられます。そのような攻撃に対しては、組織全体で他組織とも協力しながら取り組む必要があります。
このセッションでは、サイバーセキュリティの脅威動向について紹介し、特に執拗に行なわれる種類の攻撃に対する取り組みについて説明します。

サイバーセキュリティの脅威動向

- サイバー攻撃の傾向

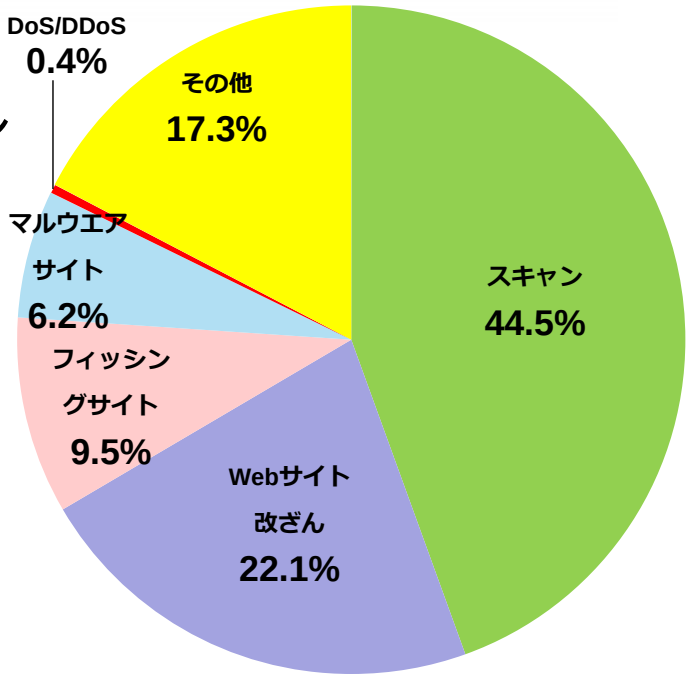
  不正送金、標的型攻撃、水飲み場型攻撃

対応・対策

- サイバー脅威への対応
- 国内外での取り組み

サイバー攻撃の傾向

- Webサイト改ざん
  - HTMLファイル・スクリプトファイル
  - JavaScriptによる誘導
- フィッシングサイト
  - 金融機関を装ったサイト（69.2%）
  - オンラインゲームサービスを装ったサイト（6.7%）
- その他のインシデント
  - 海外HTTP プロキシサイトに関する対応
  - ボットネットのC&C サーバから発見された日本国内のボットの情報

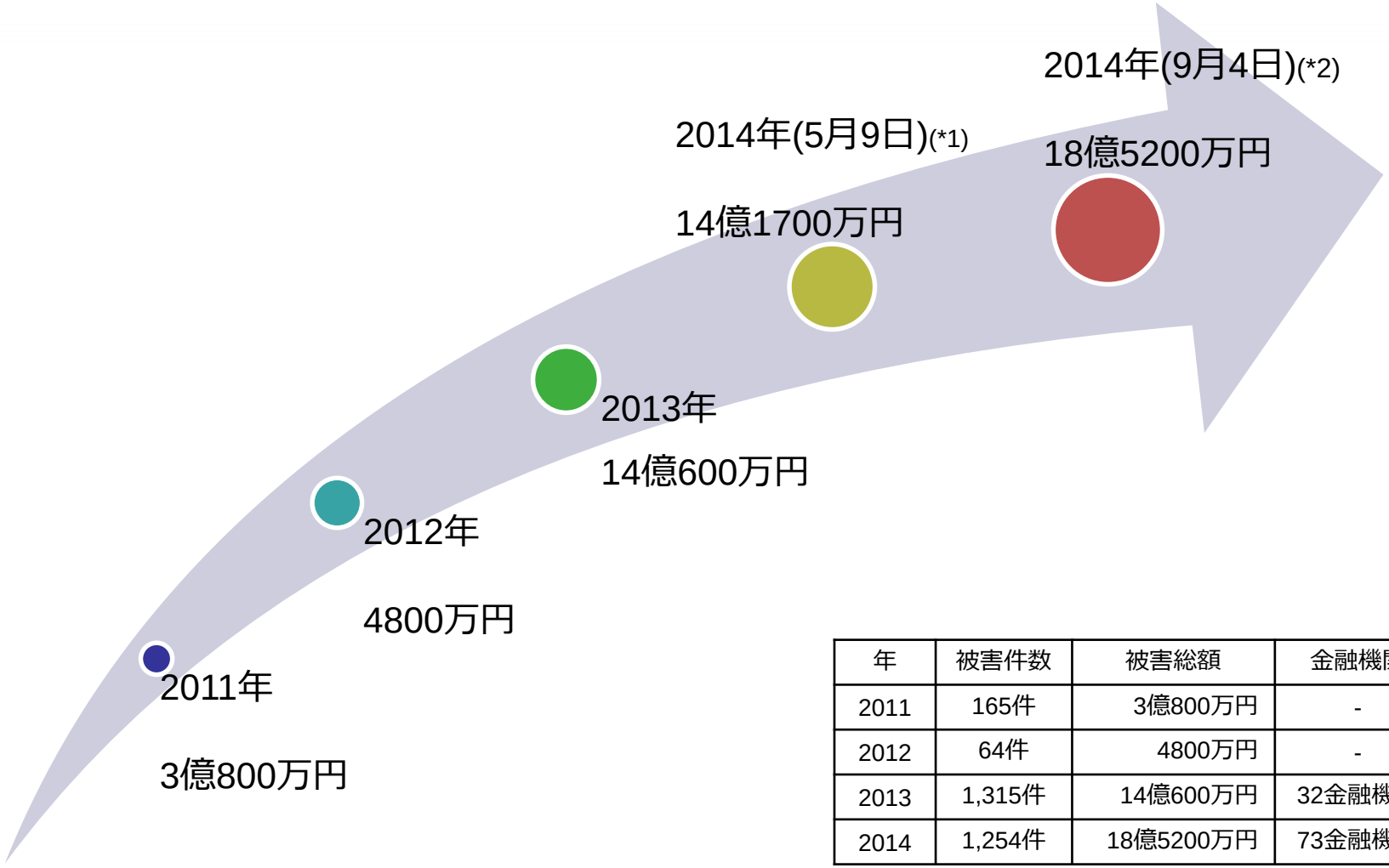


JPCERT/CCに報告されたインシデントの傾向
（2014年7月～9月）

【参照】 https://www.jpcert.or.jp/pr/2014/PR20141009.pdf
https://www.jpcert.or.jp/pr/2014/IR_Report20141009.pdf

「サイバー攻撃の傾向」

不正送金の被害金額（警察庁の発表より抜粋）

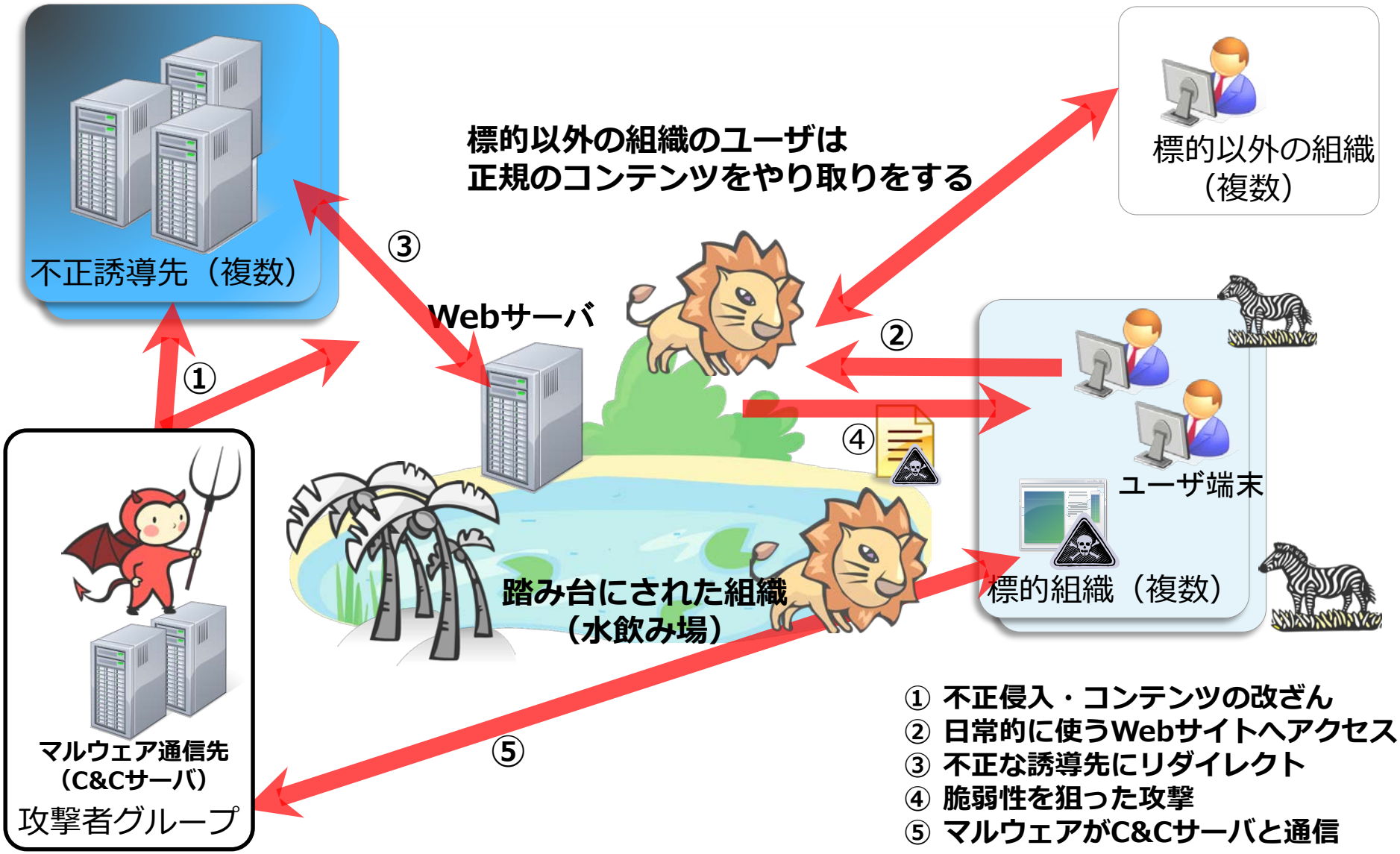


年	被害件数	被害総額	金融機関
2011	165件	3億800万円	-
2012	64件	4800万円	-
2013	1,315件	14億600万円	32金融機関
2014	1,254件	18億5200万円	73金融機関

(*1) 2014年5月9日: 4月30日までの集計情報
(*2) 2014年9月4日: 6月30日までの集計情報

「サイバー攻撃の傾向」

水飲み場型攻撃



① 不正侵入・コンテンツの改ざん
② 日常的に使うWebサイトへアクセス
③ 不正な誘導先にリダイレクト
④ 脆弱性を狙った攻撃
⑤ マルウェアがC&Cサーバと通信

サイバー脅威への対応

フィッシング

標的型メール攻撃

やり取り型

バンキング
トロージャン

ウェブ改ざん

水飲み場型攻撃

エクスプロイト
キット

パスワード
リスト攻撃

対応方法から見る“2つの脅威”

排除する ⟷ 対応の違い ⟷ 観察する

- 概して直接的な被害をともなう
- 短期間で攻撃が行われる
- 変化しながらも単体の攻撃として繰り返される

- 被害がわかりにくい
- 必要に応じて長期間かけて攻撃が行われる
- 様々な手段で継続的に攻撃が行われる

広い対象を持つ脅威

特定の対象に向かう脅威

使われる技術や手段には共通性もある
成果がやりとりされている可能性もある

簡単に見分けられるとは限らない

対抗する側での温度差

- 攻撃を受けることを「非」とする
  - レピュテーションリスクへの懸念
  - 「情報共有」≒「公表」という理解
- 攻撃を過小評価する
  - 組織全体としての取り組みにならない
  - 社会全体として被害の最小化につながらない

【攻撃を受けた組織の視点】

- ✓ 目に見えたものが全て
- ✓ 攻撃は不幸な事故
- ✓ 早期の終結を望む

【セキュリティ対応機関の視点】

- ✓ 目に見えたものは氷山の一角
- ✓ 攻撃には意図がある
- ✓ 全容の解明を望む

分断・孤立は攻撃者を利する

「サイバー脅威への対応」

各組織に期待する取り組み

事後対応

- 緊急対応体制の起動
  - 組織内の統制
  - 対応スケジュールの検討
- サーバ・端末やログ等の調査
  - 侵入経路や影響範囲の特定
  - クリーンナップ
- 外部への情報発信
  - 二次被害の危険性のある対象への注意喚起
  - メディア等への対応
  - セキュリティベンダ等への情報提供

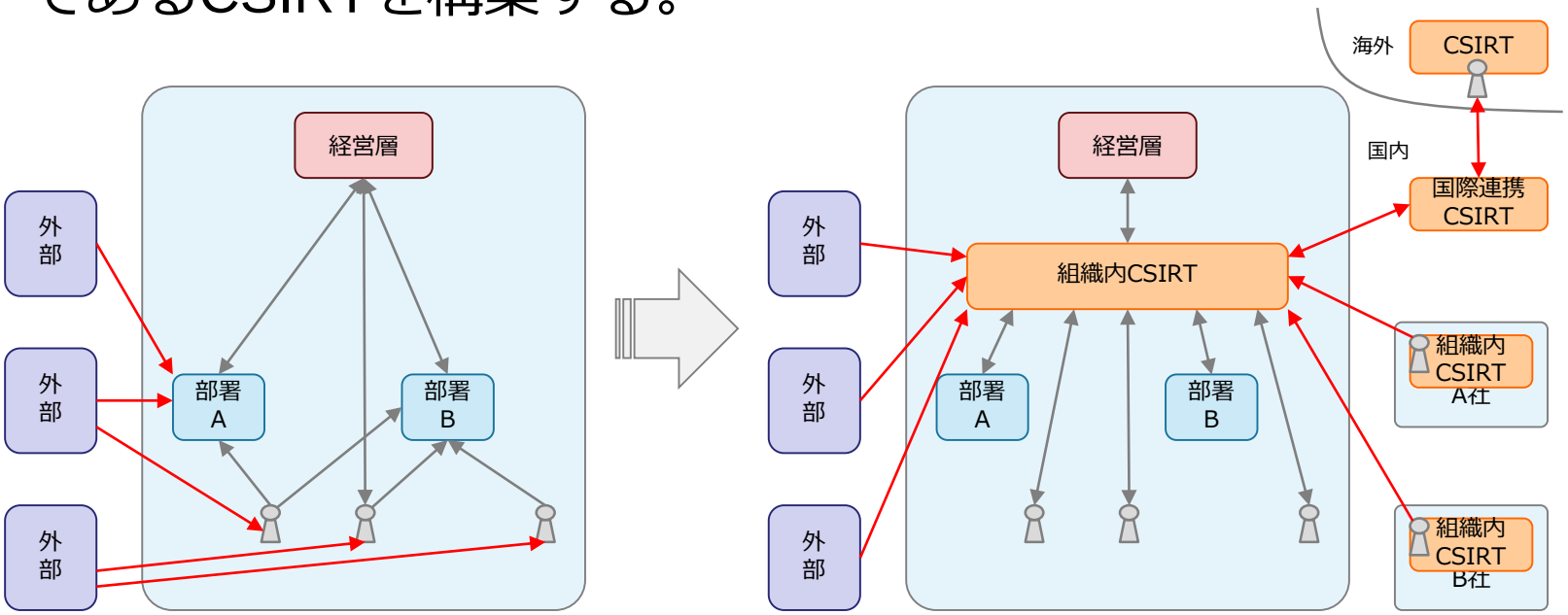
ゼロからの対応は困難

事前対策

- 情報集約と情報連携の推進
  - CSIRT機能の構築
  - 情報連携の取組みへの参加
- 脅威との共存を意識した環境作り
  - セキュリティ教育・トレーニング
  - ログ設定のチューニング
  - メールのアーカイブ・検索
  - 次世代ファイアウォール等の導入検討
- 情報資産の把握・保護
  - ネットワークやシステムの構成把握
  - 保護すべき情報の洗い出し

組織内CSIRTに期待される役割

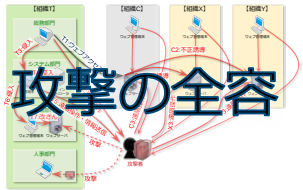
- 組織の内外に対し、インシデントに関する一元的な対応窓口であるCSIRTを構築する。



メリットの例：
①社内セキュリティ情報の共有、集中管理の実現
②セキュリティ対応にかかる指示系統の迅速化（ダイレクトリーチ）
③外部に対して信頼性のある窓口先の提供
④外部からの情報の一元管理の実現
⑤インシデントレスポンスに必要な情報量の向上
⑥想定外（予想外）のインシデントへの柔軟な対応

国内外での取り組み

個々の攻撃・事象



脅威の観察

共有化・共通化の検討・促進

技術改善・協力者の動機付け

総合的な情報収集力の向上

セキュリティ関連機関間での連携

「国内外での取り組み」

ボットネットテイクダウン作戦

- 国際的な活動
  アメリカ合衆国国土安全保障省やFBIなど、複数の企業や組織が協力しGameOver ZeuS botnetの対策を実施。
- 国内での活動
  警察庁、総務省、一般社団法人日本データ通信協会テレコム・アイザック推進会議およびJPCERT/CCが協力。

  - インターネットバンキングに係る不正送金事犯に関連する不正プログラム等の感染端末の特定及びその駆除について
    http://www.npa.go.jp/cyber/goz/
  - インターネットバンキングに係るマルウェアへの感染者に対する注意喚起の実施
    http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000080.html
  - JPCERT/CC、「インターネットバンキングに係わる不正送金事犯に関連する不正プログラム等の感染端末の特定及びその駆除について～国際的なボットネットのテイクダウン作戦～」に協力
    https://www.jpcert.or.jp/pr/2014/pr140002.html

今後の脅威を考えるうえで・・・

Windowsサポート期限

2014年4月8日	Windows XP
2015年7月14日	Windows Server 2003
2017年4月11日	Windows Vista
2020年1月14日	Windows 7
	Windows Server 2008
2023年1月10日	Windows 8
	Windows Server 2012

接続されるデバイス数

2003年	5億デバイス	（Cisco IBSG, 2010）
2010年	125億デバイス	（Cisco IBSG, 2010）
2015年	250億デバイス	（Cisco IBSG, 2010）
2020年	500億デバイス	（Cisco IBSG, 2010）
	295億デバイス	（ARM, 2013）

インフラ

【長いライフサイクル】
- 様々な分野でネット活用
- 既存の技術が浸透

サービス

【短いライフサイクル】
- リソースのサービス化
- デバイスの多様化

利用者

対策を打ち込むチャンス

対策・対応の構図が大きく変わる可能性も

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：https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- Web：https://www.jpcert.or.jp/form/

ご清聴ありがとうございました。