

標的型攻撃への対応

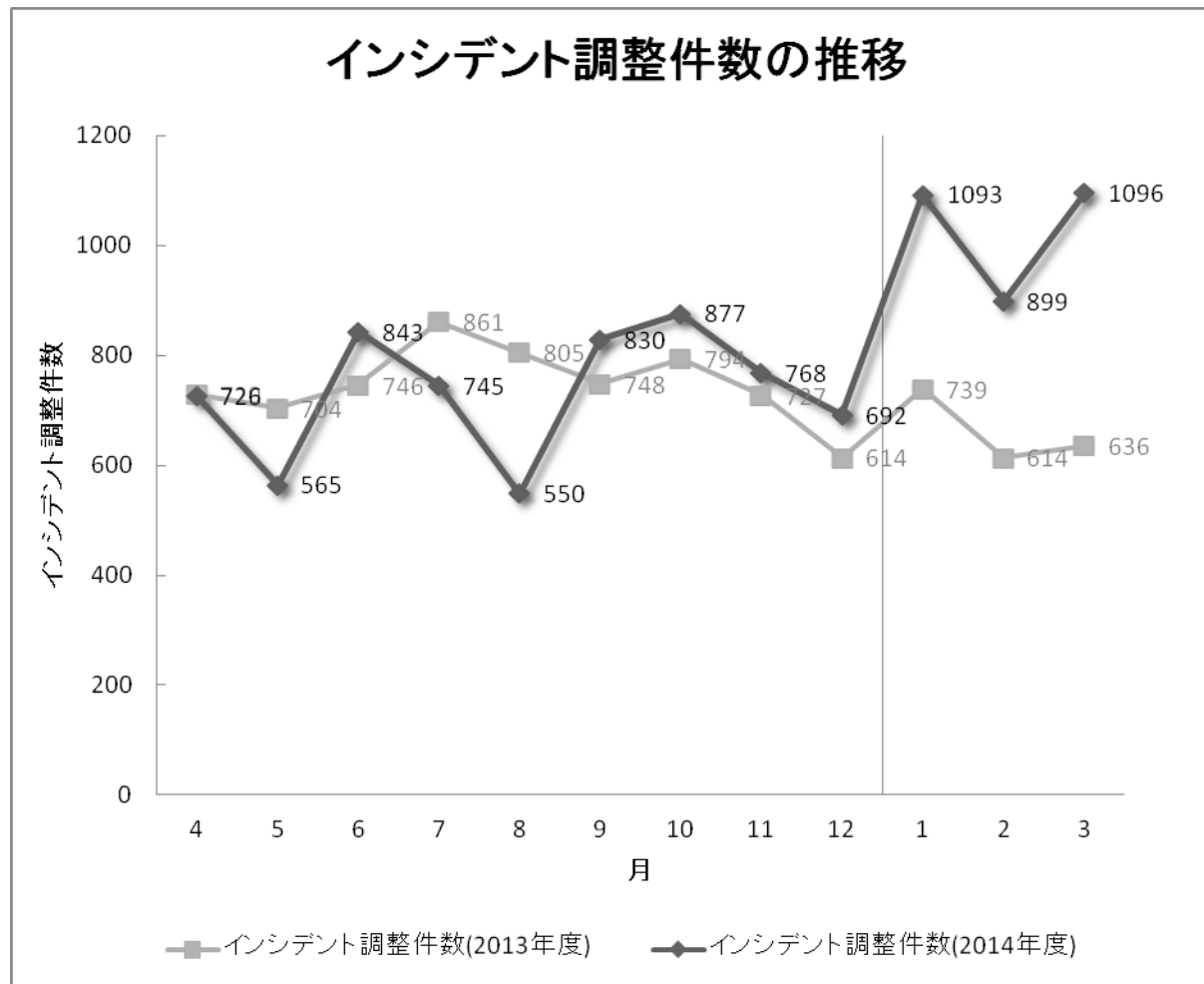
- JPCERT/CC -

一般社団法人JPCERTコーディネーションセンター
インシデントレスポンスグループ
久保 啓司

JPCERT/CCと標的型攻撃

- EMDIVIを事例として -

インシデント調整件数の推移



2015年4-6月期
調整件数
2,479件
(6/23現在)

※最新情報はJPCERT/CC
インシデント報告対応レポート
をご覧ください。
<https://www.jpcert.or.jp/ir/report.html>

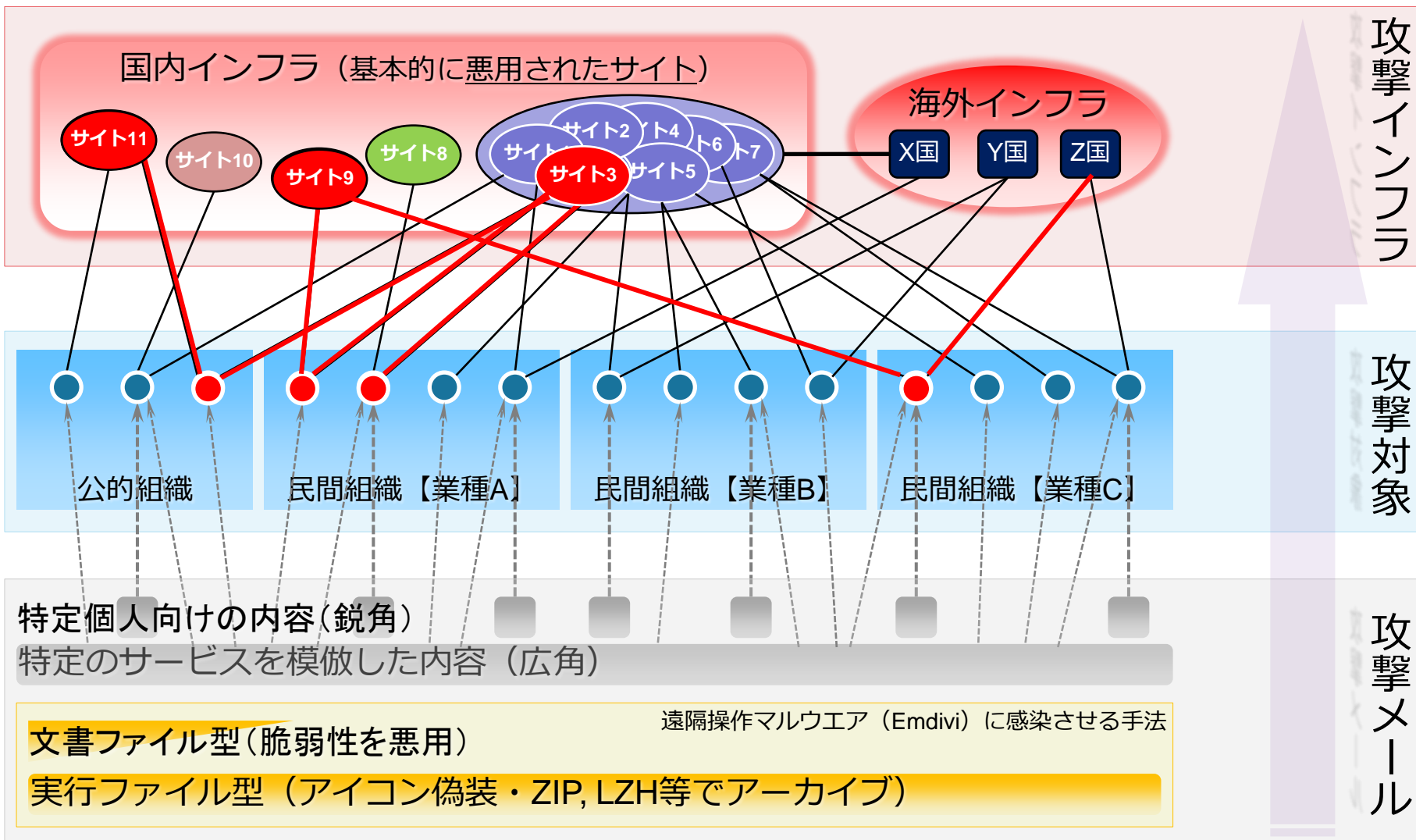
標的型攻撃に関する通知連絡

- 2015年4-6月期（6/30現在）
 - マルウェア感染とは限らない
 - 調査目的の通信なども確認

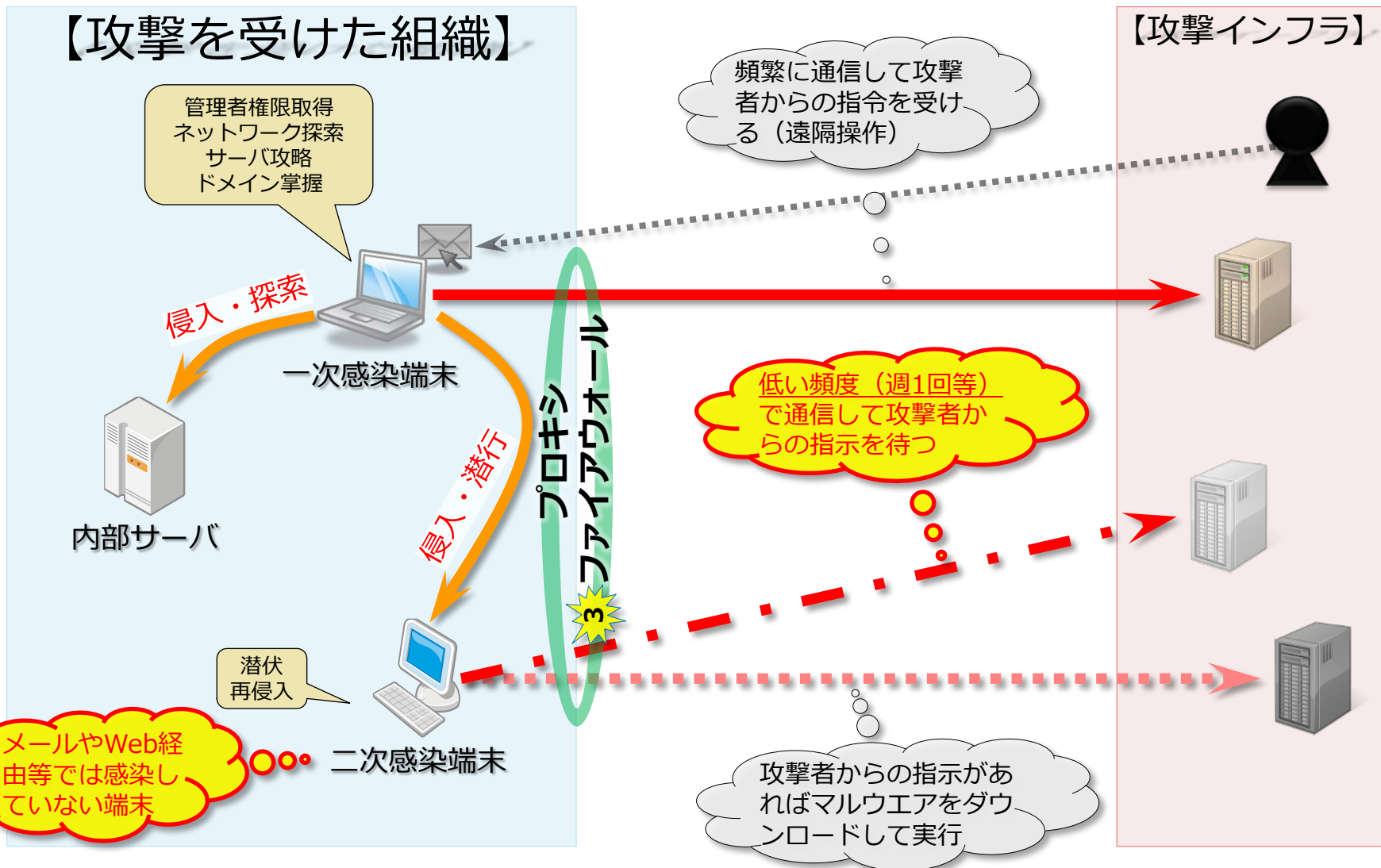
66 組織

うちEmdivi関連: 44 組織

攻撃イメージ (Emdivi)

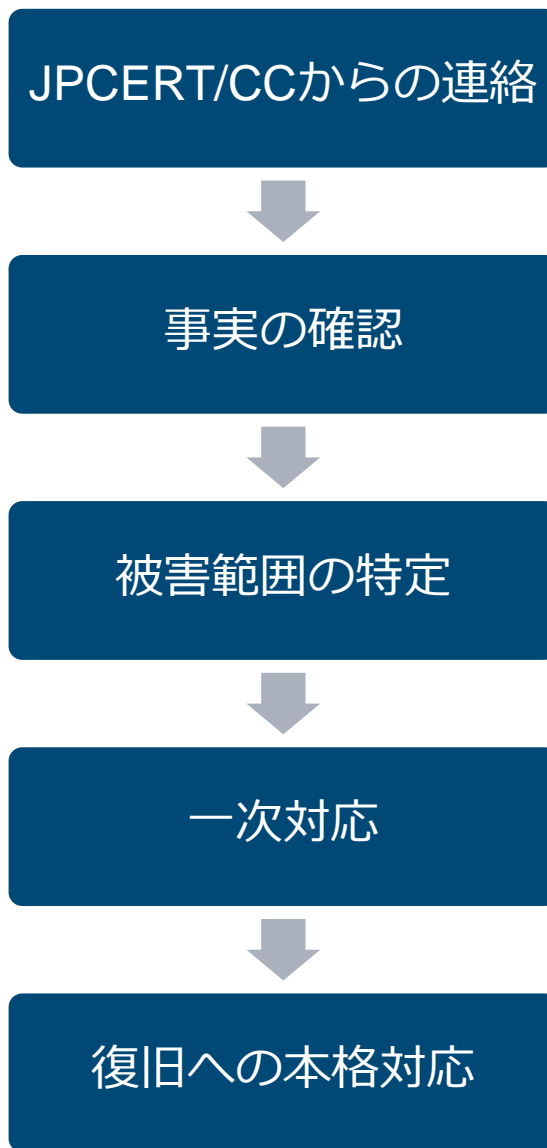


被害組織で発生していること



JPCERT/CCからの連絡への対応

JPCERT/CCが期待する対応（概要）



JPCERT/CCからの連絡

■ 客観的事実に基づいた連絡

■ 連絡窓口の確認

— IPアドレスの情報から連絡

■ Whois 登録情報の確認

■ IPアドレス割当申請時のままになっていないか

■ まずは事実確認を

— 通知に足る確度の高い情報を連絡しています

— 不明な点があれば問合せください

事実の確認と被害範囲の特定

- マルウェア通信の有無の確認
 - ファイアウォール、プロキシのログの確認
- 通信していたPCの特定
 - 証拠保全を第一に
 - 該当PCをネットワークから切断し保全
 - JPCERT/CCで把握できているのは感染の一部だけ
- 他のPCやサーバなどの被害状況の確認
 - 類似の通信の調査
 - 通信確認した段階でPCの切断と保全
 - 侵入経路の調査
 - 攻撃メールの受信の確認
 - Active Directory、ファイルサーバなどへの侵害の確認
 - ATコマンドによるタスク登録確認
 - 不審なサービス、待ち受けポートの確認など

一次対応

- インターネット遮断の判断
 - 事業継続（必要な通信はなにか）
 - C2サーバ通信の把握状況（限定して遮断できないか）
 - 侵害の範囲（ex. AD管理者権限は奪取されていないか）
- 関連組織への連絡、エスカレーション
 - 関連会社
 - 監督官庁
 - 警察
 - アナウンス、プレスリリース等の検討
- セキュリティ専門業者への協力依頼の判断
- 保全した証拠の調査分析
 - マルウェア感染状況
 - 流出した可能性のある情報の確認特定
- 通信状況の継続監視による感染端末のあぶり出し
- パスワード変更などの対応

復旧に向けた本格対応

- 侵害の範囲を特定するのは非常に困難
 - システム再構築も含めた検討も必要

- 業務継続のための現実解
 - 侵害が確認されたリソースの排除
 - 十分な監視体制のもと順次復旧へ
 - 通信の監視
 - ファイアウォール、プロキシ、組織内ネットワーク
 - 認証の監視
 - Active Directory、社内システム、データベースなど
 - ソフトウェア導入状況
 - 資産管理システムの活用

監視体制を保ったまま、平常状態に
(長期間かけて)

お問合せ、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 : ww-info@jpcert.or.jp

— Tel : 03-3518-4600

— <https://www.jpcert.or.jp/>

インシデント報告

— Email : info@jpcert.or.jp

— <https://www.jpcert.or.jp/form/>

制御システムインシデントの報告

— Email : icsr-ir@jpcert.or.jp

— <https://www.jpcert.or.jp/ics/ics-form>

Home

サイト内検索

検索

トップページ

情報提供

- 注意喚起
- 早期警戒
- 脆弱性対策情報
- Weekly Report

各種届出・申込

- 制御システムセキュリティ
- ラーニング
- 公開資料

- 四半期レポート
- 研究・調査レポート
- CSIRT マテリアル

イベント

- プレスリリース
- JPCERT/CC

関連組織

FIRST

JPCERT/CCはFIRSTのチームメンバーです。またJPCERT/CCスタッフがSteering CommitteeメンバーとしてFIRSTの運営に協力しています。

APCERT

JPCERT/CCはAPCERTの事務局長を務めています。

注意喚起

深刻度

- 2009-06-10 [公開] 2009年6月 Microsoft セキュリティ情報 (緊急5件) に関する注意喚起
- 2009-05-14 [公開] JavaScript が埋め込まれる Web サイトの改ざんに関する注意喚起
- 2009-06-13 [公開] Adobe Reader に関する注意喚起
- 2009-05-13 [公開] 2009年5月 Microsoft セキュリティ情報 (緊急1件) に関する注意喚起
- 2009-04-15 [公開] 2009年4月 Microsoft セキュリティ情報 (緊急5件) に関する注意喚起

脆弱性関連情報

ソフトウェア

- 2009-06-19 15:00 XOOOPS マニア製 PHP/MySQL におけるクロスサイトスクリプティングの脆弱性
- 2009-06-19 14:32 AS1 D.O.O 製 activeCollab におけるクロスサイトスクリプティングの脆弱性
- 2009-06-19 14:32 Movable Type 5.0.2 におけるクロスサイトスクリプティングの脆弱性
- 2009-06-19 14:32 Serene Bach におけるセッション ID が推測可能な脆弱性

Weekly Report

セキュリティインシデント...
フィッシングサイト...
Webサイトの改ざん...
マルウェア...
不正アクセス...

発生元への「調査」を依頼したい
インシデントを「報告」したい

ISDAS

[インターネット定点観測]

インターネット上に配置したセンサーにより、セキュリティ上の脅威となるトラフィックを観測しています。

おすすめページ

セキュリティ対策講座

教育担当者が使える、新入社員などが身につけておくべきセキュリティ知識などを紹介しています。

イベント

- 第21回 FIRST Annual Conference 京都 参加申し込み受付中
- O/O+ セキュアコーディング ハーフデイキャンプ参加申し込み