JPCERT CC®

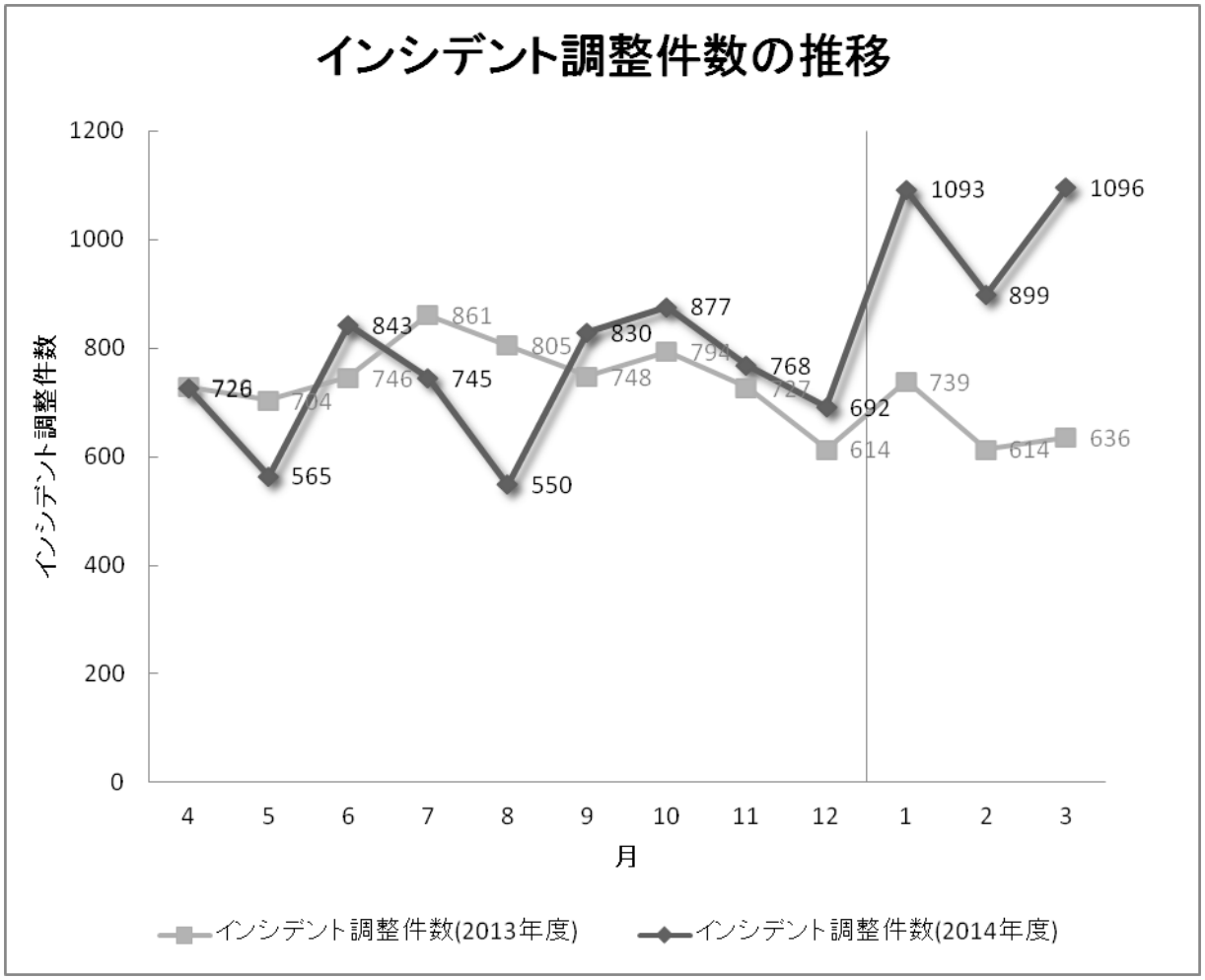
標的型攻撃への対応
- JPCERT/CC -

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

●Page3：6月23日現在の数字を6月30日現在の数字に更新しました。●

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/re
port.html

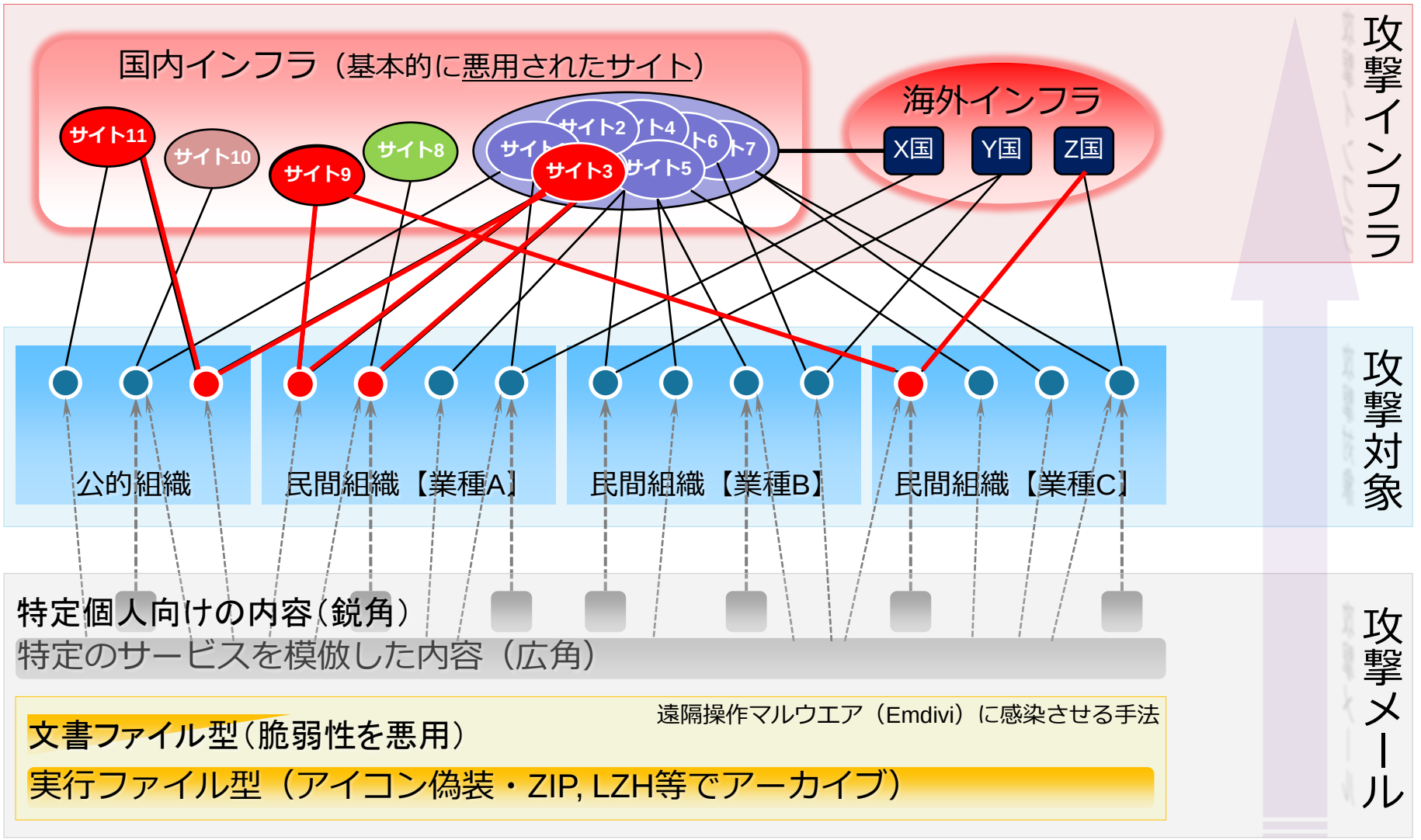
標的型攻撃に関する通知連絡

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

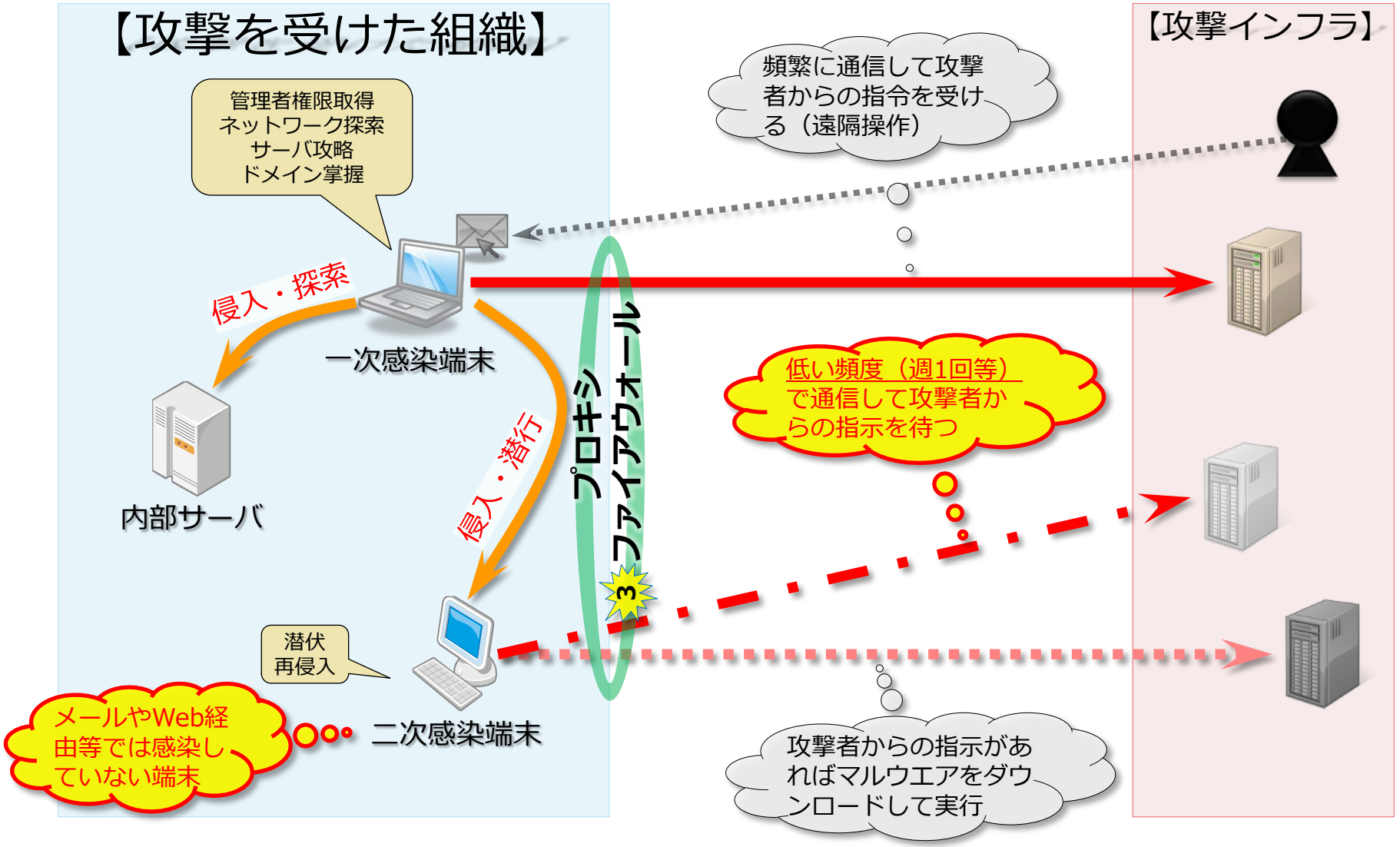
66組織

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

- マルウエ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
  - マルウエア感染状況
  - 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
    - ソフトウエア導入状況
      - —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