IPA Information-technology Promotion Agency, Japan

サイバー攻撃対策の情報共有組織「J-CSIP」の取り組み

2013年8月27日

独立行政法人 情報処理推進機構
技術本部 セキュリティセンター
松坂 志

J-CSIP
Initiative for Cyber Security
Information sharing Partnership of Japan

- Initiative for Cyber Security Information sharing Partnership of Japan
- サイバー情報共有イニシアティブ
  - 官民連携による、サイバー攻撃に関する情報共有の取り組み
  - IPAを情報ハブ（集約点）として、参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく

http://www.ipa.go.jp/security/J-CSIP/

業界を狙う攻撃の事業者相互の把握

- （競合関係にもある）事業者相互でのサイバー攻撃の状況の把握や、共同での検知・防御に繋がった。

質の高い情報の共有

- NDA（秘密保持契約）下での情報管理を前提としているため、迅速で密度の高い情報共有となっている。

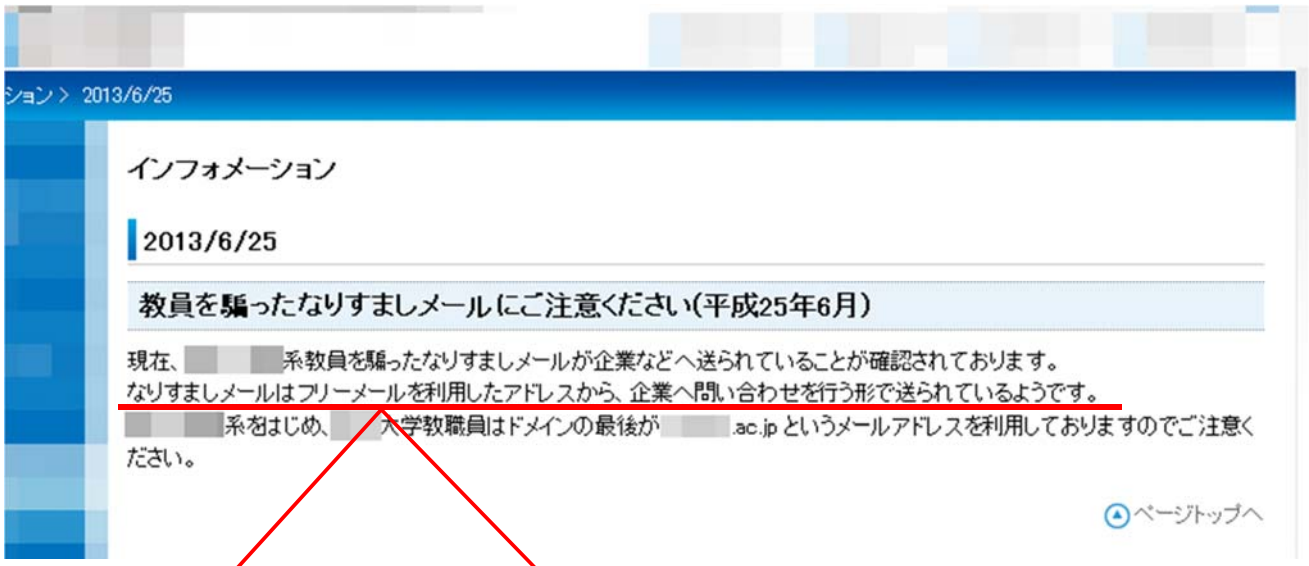
複数の攻撃情報の相関

- IPAが情報の集約点となることで、複数の攻撃情報の相関が把握でき、その情報も共有。各参加組織にて、今後想定される攻撃への対策検討等に活用。

（参考）大学にかかわる標的型攻撃の事例

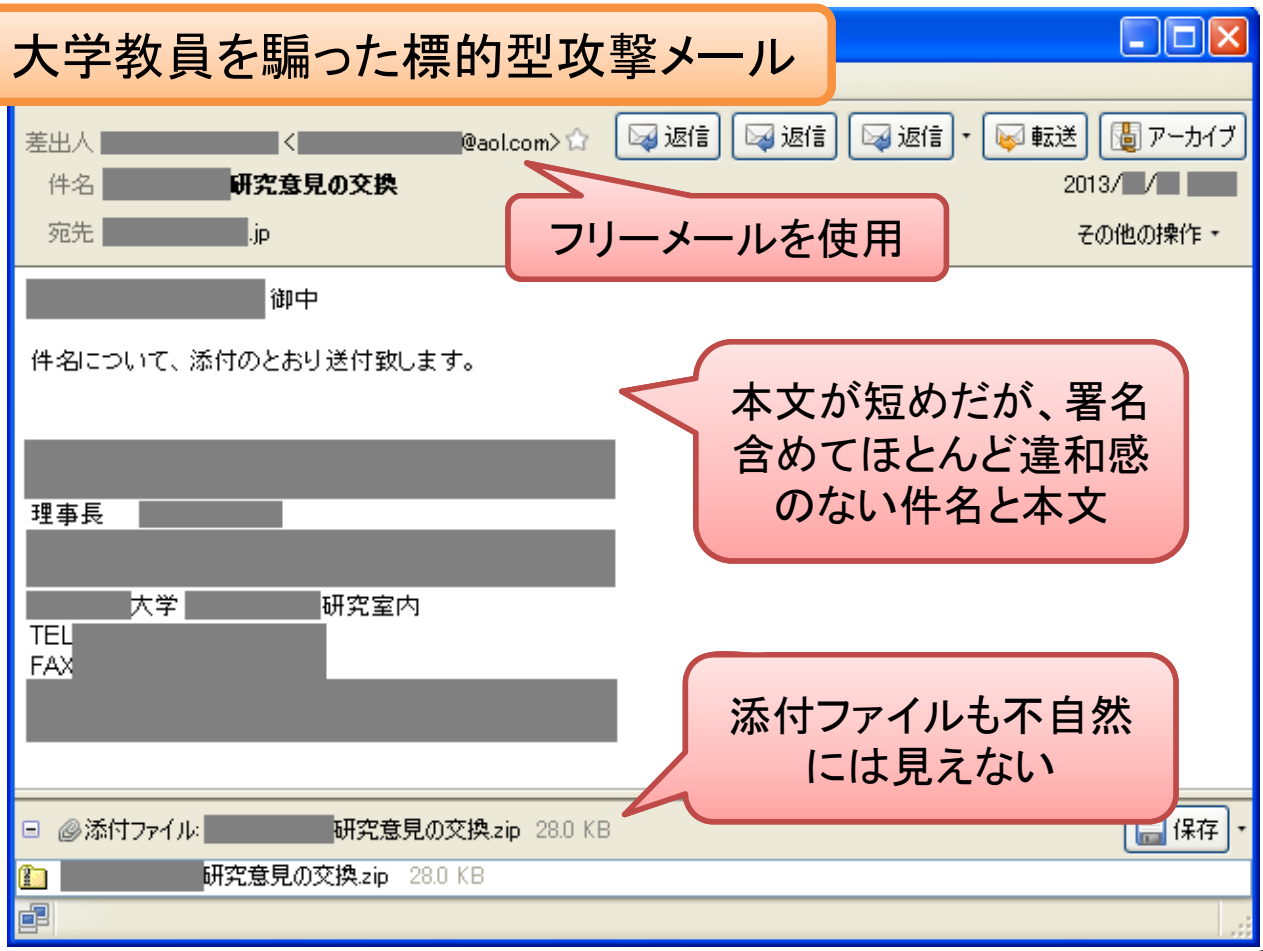
- 大学の教職員や学生を詐称し、企業・団体へ標的型攻撃メールが送信された事例
  - 「問い合わせ」等… 突然メールが来てもそれほど不自然ではない？
- 大学職員のアカウントから標的型攻撃メールが送信された事例
  - 当該大学職員も何らかの標的型攻撃を受けアカウントが乗っ取られた？

ある大学の注意喚起ページより



なりすましメールはフリーメールを利用したアドレスから、企業へ問い合わせを行う形で送られているようです。

大学教員を騙った標的型攻撃メール



フリーメールを使用

本文が短めだが、署名含めてほとんど違和感のない件名と本文

添付ファイルも不自然には見えない

標的型攻撃と情報共有

サイバー攻撃対策と情報共有の必要性

サイバー攻撃は、攻撃側が常に有利

全方位に対する完全な防御は非現実的

攻撃手口、対策ノウハウなどの情報が重要

相反

様々な事情、制約により情報が流通しにくい

基本的に、攻撃を受けた人や組織しか、その情報を持っていない

情報共有が有効

特に

限られた対象のみに行われる「標的型サイバー攻撃」

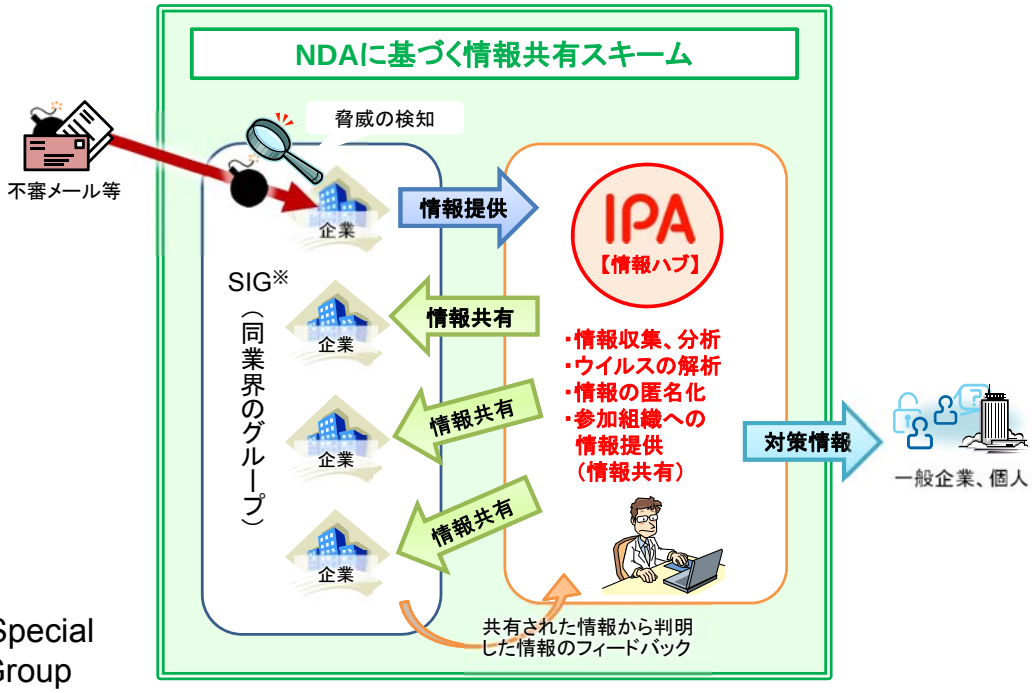
水面下で行われ、認知も難しい

J-CSIP 発足の背景

2010年 12月～	• 経済産業省「サイバーセキュリティと経済 研究会」開催
2011年 8月	• 「研究会」中間とりまとめ
2011年 9～10月	• 国内のサイバー攻撃に関する複数事案の報道
2011年 10月25日	• 官民連携による情報共有体制 J-CSIP 発足

情報共有のスキーム

- IPAが情報の集約点となり、参加組織とのNDA（秘密保持契約）に基づき、情報共有を実施



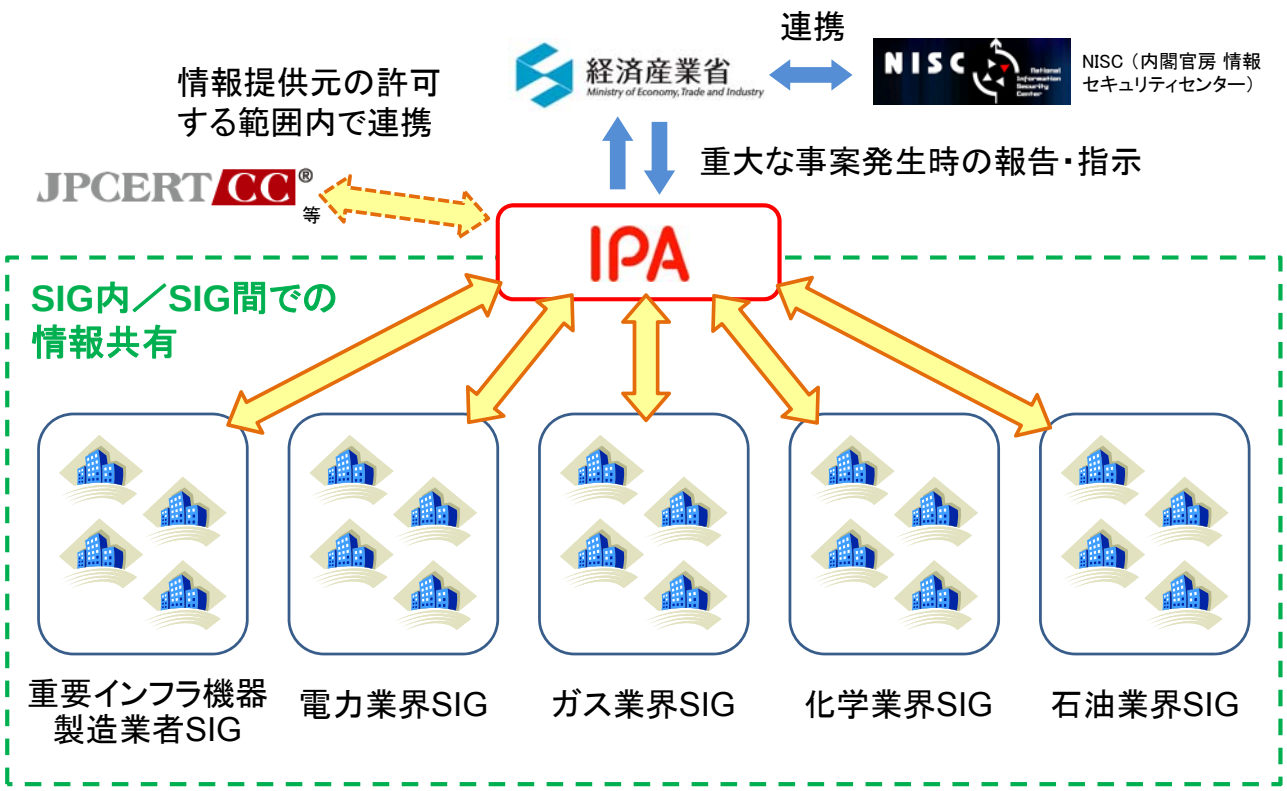
※ SIG: Special Interest Group

情報共有体制の確立

2011年10月25日 J-CSIP発足 の後…

～2012年3月末	• 参加組織等の実務者にて協議を重ね、NDA策定、情報共有ルール整備
2012年4月	• 重要インフラ機器製造業者SIG においてNDA締結、運用開始 ※ SIG：Special Interest Group
2012年7～10月	• 電力、ガス、化学、石油業界へ拡大 • 業界間（SIG間）での情報共有開始
2013年8月現在	• 5業界、45参加組織にて運用中 （4月時点：39参加組織）

J-CSIPの全体イメージ



（参考）情報共有関連の取り組み

- どのような取り組み（スコープ）とするか
  - 官民連携（PPP：Public-Private Partnership） or 民間
  - 何を目的とし、何の情報を共有するのか？
    - 取り組み構築のガイド：『Good Practice Guide on Cooperatve Models for Effective PPPs』（ENISA Oct 01, 2011）
    - ノウハウの共有、脅威指標（Threat Indicator）の共有、etc
    - メンバに求めるものは何か、求めないものは何か
- どのように情報を流通させるか
  - 安全な伝達経路の設定
  - メカニズム（ルール）、情報の表現形式
    - サイバーセキュリティ情報交換フレームワーク CYBEX、サイバー攻撃観測記述形式 CybOX …
- 国内、国外、様々な情報共有体（体制）が存在
  - それぞれスコープが異なっている
  - J-CSIPは、（半）官民連携 ＋ 業界ごとのSIG ＋ NDAによる連携 ＋ 参加組織のベストエフォート … といった特徴

J-CSIPの活動状況

活動状況

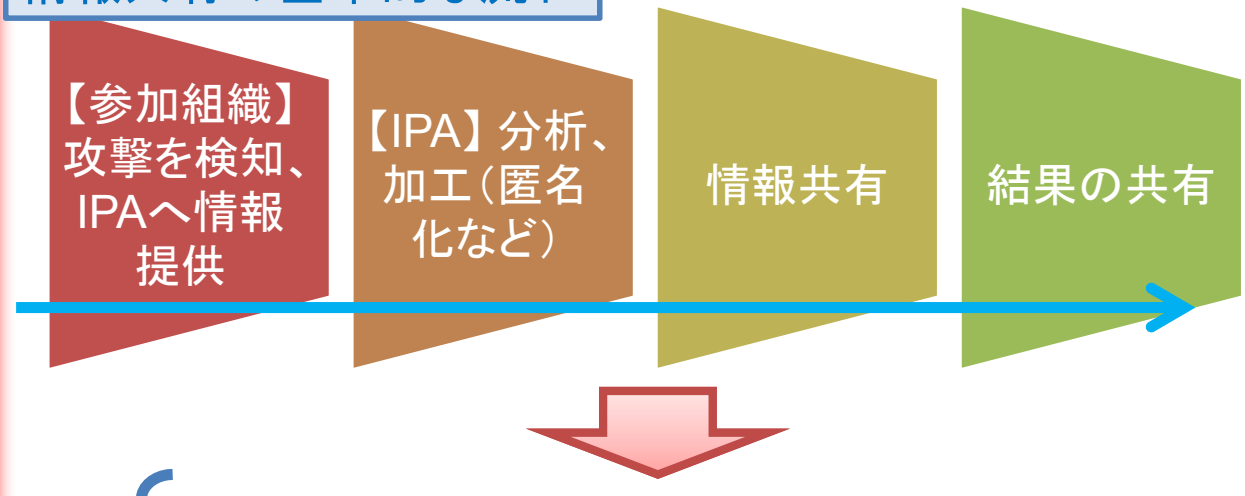
① 5つの業界、45組織での情報共有体制

② 標的型攻撃メールについて、参加組織からの情報提供をもとに情報共有を実施

- FY2012 攻撃メール 201件
- FY2013[1Q] 攻撃メール 64件

情報共有の流れと目的

情報共有の基本的な流れ



目的

① 類似攻撃の早期検知と被害の回避
② 攻撃に対する防御の実施
③ 今後想定される攻撃への対策検討

※ 標的型攻撃メールを当面の主対象として運用中

情報共有の事例　（概略）

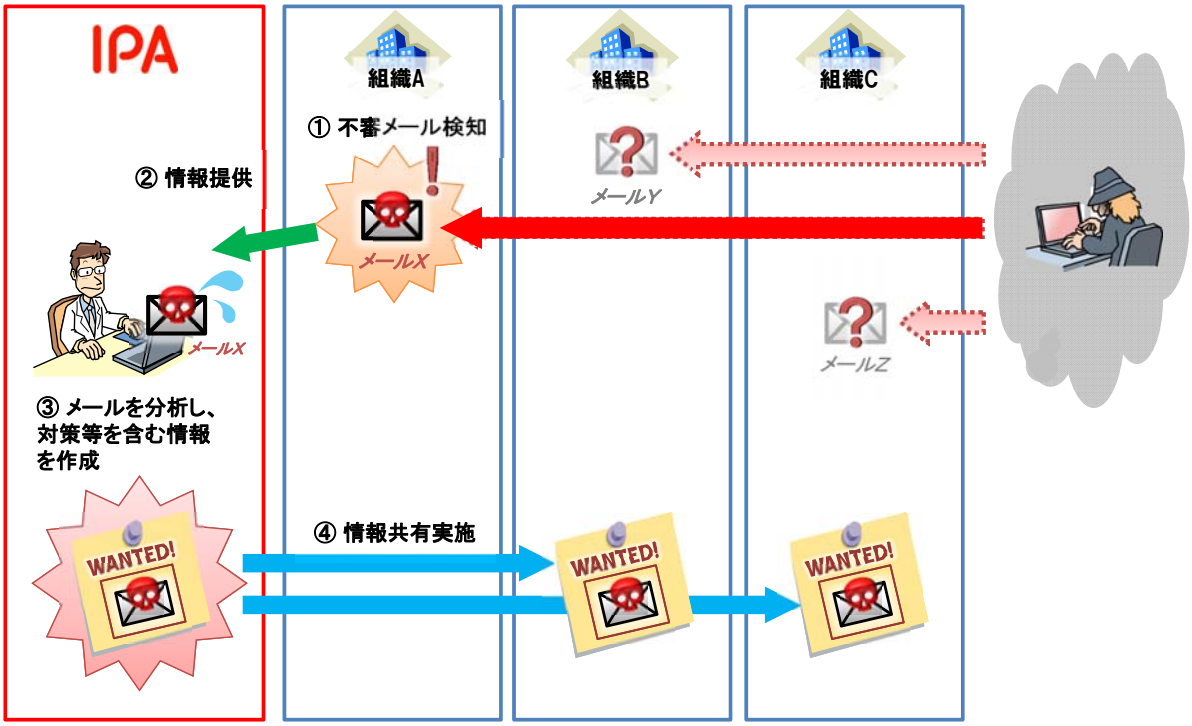
- 情報共有により、同種の不審メールが複数組織に着信していたことが判明。
- それらの情報を集約し、更なる情報共有へ繋げた。

⇒ 時系列に沿って、3つの段階に分けて紹介

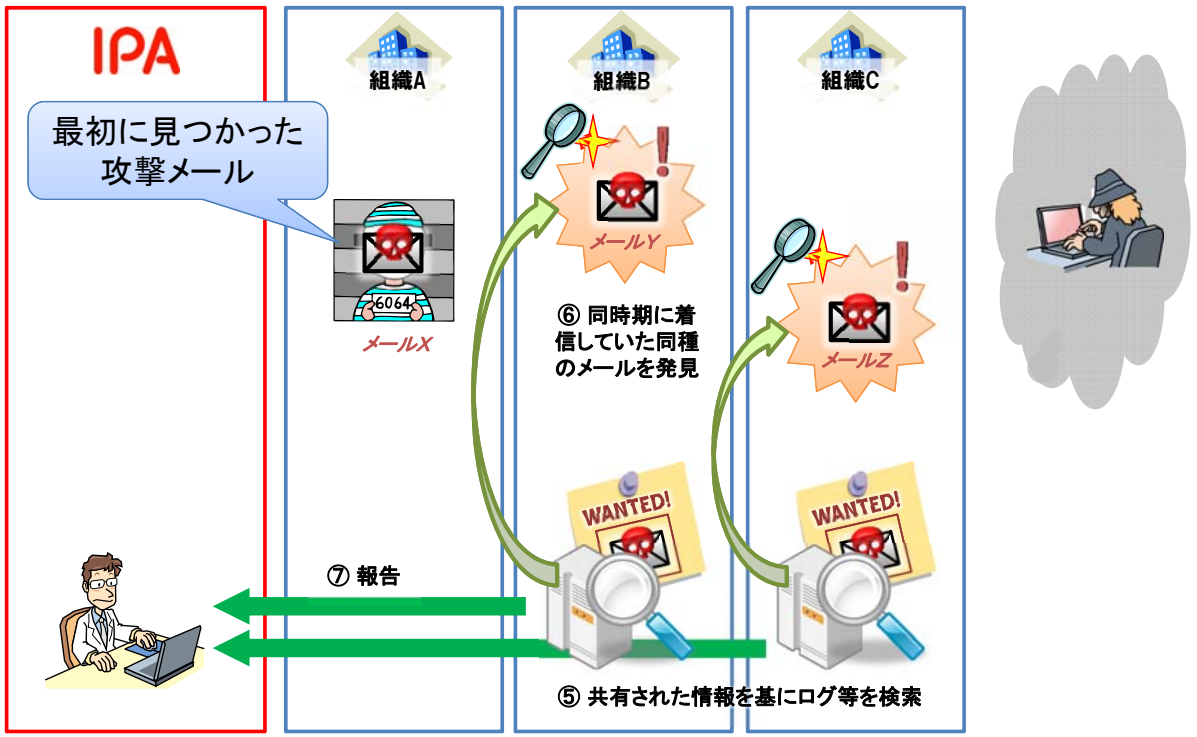
第一段階	第二段階	第三段階
• 攻撃メールの発見 ～ 情報共有	• 各組織での同種のメール発見	• 情報の集約分析と更なる情報共有

※ 詳細は「J-CSIP 2012年度 活動レポート」を参照願います。

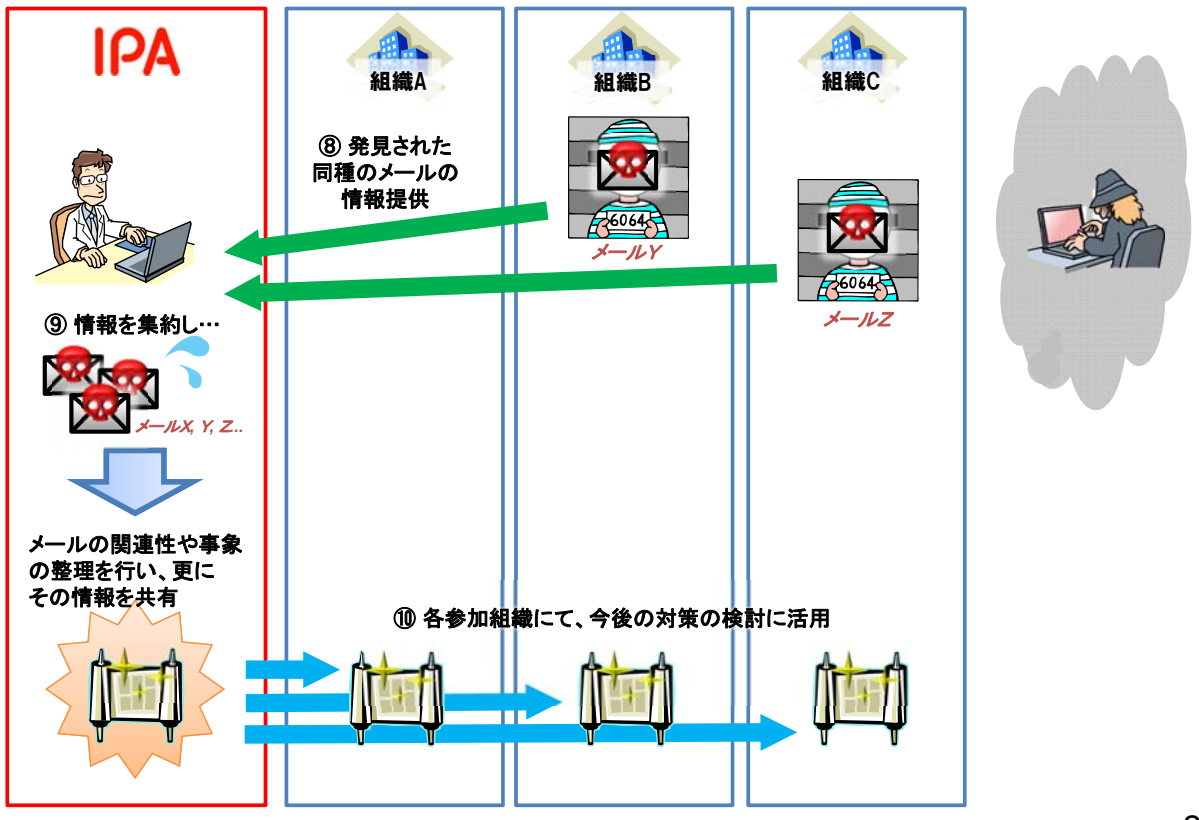
第一段階：不審メール情報の情報共有



第二段階：各組織での同種のメールの発見

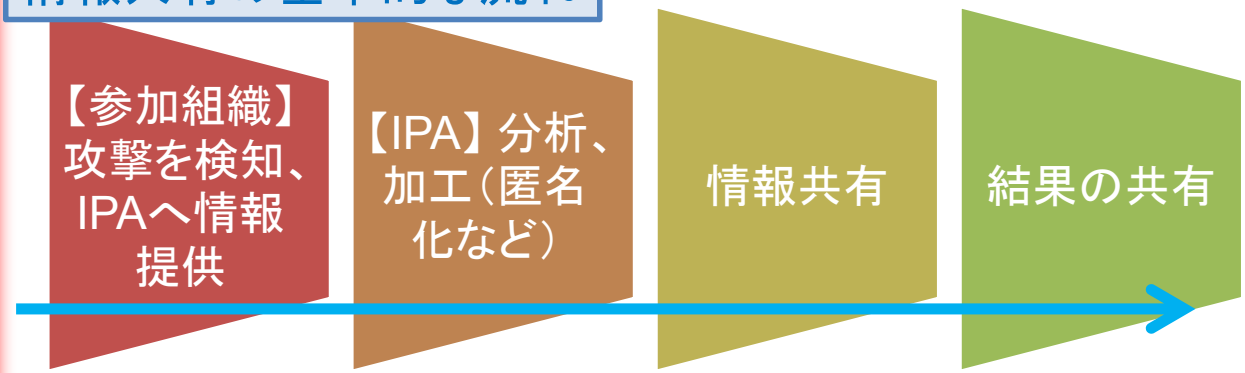


第三段階：情報の集約分析と更なる情報共有



情報共有の流れと目的（再掲）

情報共有の基本的な流れ



目的

① 類似攻撃の早期検知と被害の回避
② 攻撃に対する防御の実施
③ 今後想定される攻撃への対策検討

※ 標的型攻撃メールを当面の主対象として運用中

総括 ／ 考察（1）

① 類似攻撃の早期検知と被害の回避

→ 組織Aからの情報を基に、他の組織でも発見

⇒ 同様の事例は他にも複数あり、情報共有が有効であると参加組織から評価

・（競合関係にもある）事業者相互での把握
・NDA下での迅速な／詳細な情報共有

② 攻撃に対する防御の実施

→ ウイルスが試みる不正な通信の通信先の情報も共有　⇒ 各組織にて通信遮断策へ反映

③ 今後想定される攻撃への対策検討

→ 一連の攻撃の相関や流れといった、攻撃手口の情報も共有　⇒ 各組織にて今後の対策検討に活用

総括 ／ 考察（2）

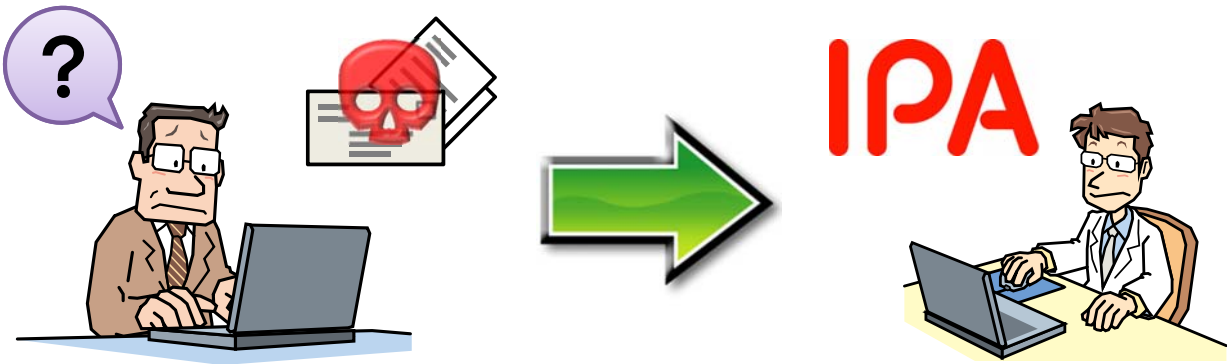
「不審なメールは捨てる」のままでよい？

不審なメールなど、「気づき」があった時に、組織内で相談を受け付けられるように

スムーズな連絡、情報共有のための下準備を

標的型サイバー攻撃の特別相談窓口

標的型攻撃メールかな？ と思ったら・・・



IPAへご相談ください！

http://www.ipa.go.jp/security/tokubetsu/

（参考）「設計・運用ガイド」第3版について

2011年11月30日 公開
『新しいタイプの攻撃』の対策に向けた設計・運用ガイド
改訂第2版

「第3版」近日
公開予定です。

http://www.ipa.go.jp/security/vuln/newattack.html

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

J-CSIP
Initiative for Cyber Security
Information sharing Partnership of Japan