

標的型攻撃の防御に向けた産業界との情報共有の枠組み、^{ジェイ シップ}J-CSIPの活動レポートを公開

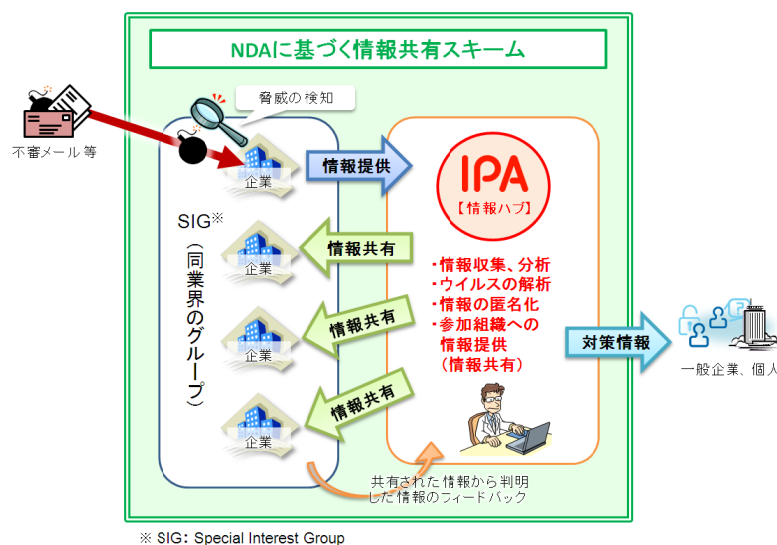
～活動の成果として参加企業から246件の情報提供を受け、うち160件を情報共有～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）では、2011年10月に発足、2012年4月から活動を開始した「サイバー情報共有イニシアティブ」（以後、J-CSIP^(*)という）において、これまで5業界、39組織での運用体制を確立しています。2012年度の活動では、参加組織から246件の情報提供を受け、IPAによる分析を経て、参加組織へ160件^(**)の情報共有の運用を行いました。これらJ-CSIPの活動内容を「サイバー情報共有イニシアティブ 2012年度 活動レポート」としてまとめ、公開しました。同レポートでは、運用や情報共有の体制、および情報共有による効果を紹介しています。

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

ここ数年、海外では組織の機密情報窃取や、ライフライン等の重要インフラの障害につながる攻撃が報道されています。この背景のもと、2010年12月に経済産業省主導で「サイバーセキュリティと経済研究会」が開催され、2011年8月に公表された中間とりまとめ^(***)における結論として、「標的型サイバー攻撃への対応」の必要性と、有効な対策の一つとして組織間での情報共有が挙げられました。またこの時期には、日本国内でも標的型サイバー攻撃と考えられる事案が複数件発生しました。

こうした状況を受け、IPAは経済産業省の協力のもと2011年10月25日、標的型サイバー攻撃への対抗施策として、重要インフラ機器製造業者9社とともに「J-CSIP」を発足させました。J-CSIPは秘密保持契約（NDA）に基づく情報共有を通じ、参加組織における、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、による防御力の向上を目的としています。



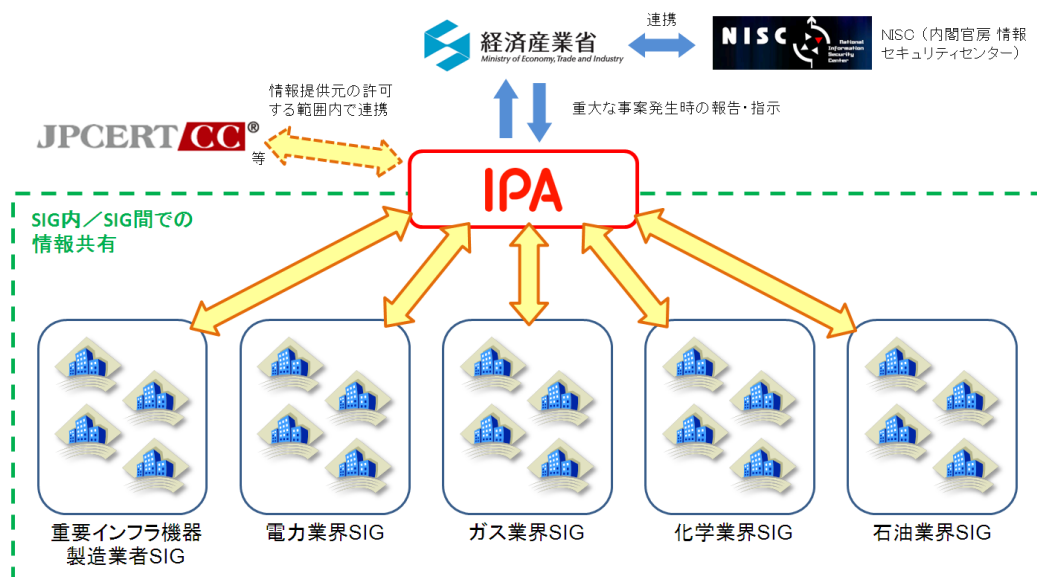
(*) ジェイシップ : Initiative for Cyber Security Information Sharing Partnership of Japan

(**) 情報提供を受け、類似の攻撃メールの情報の集約や、無差別にばらまかれたと考えられるメールの除外等の上、情報共有している。

(***) <http://www.meti.go.jp/press/2011/08/20110805006/20110805006.html>

そして、2012年4月からはIPAが情報ハブ（集約点）となり、参加企業との情報共有を主軸としたJ-CSIPの運用を開始、2012年7月以降、電力、ガス、石油、化学の各業界にも運用対象を拡張し、2013年4月現在、5業界、39組織での運用を行っています。

また、複数業界がJ-CSIPに参画したことを受け、2012年10月からは、業界内の情報共有だけでなく、業界間での情報共有を開始しています。



これまでのJ-CSIPの運用により、参加組織において以下の様な成果がありました。

- (1) 業界を狙った同一もしくは類似の攻撃が行われていることを組織間で相互に共有し、対策に寄与した。
- (2) NDA下での情報管理を前提とし、また、情報の匿名化などの情報共有ルールを適用することで、情報の共有可否に対する迅速な判断と、詳細な内容の情報共有を可能とした。
- (3) 複数組織に行われた攻撃間の相関についての分析結果を共有することにより、今後想定される攻撃に対する各組織での対策立案に繋がった。

これにより、例えば、共有情報をヒントに、発見できていなかったウイルス付き攻撃メールを見つけ出し、被害発生前の駆除に成功したり、ウイルスによって発生する不正通信の接続先情報を活用して、各組織における通信遮断策へ反映されたりした、などの効果がありました。

IPAは、今後もJ-CSIPの取組みを継続し、サイバー攻撃や脅威の発見、被害の予防、被害の拡大・再発防止を推進するとともに、適用業界の拡張、参加組織の増加を目指します。

■ 本件に関するお問い合わせ先
 IPA 技術本部 セキュリティセンター 金野／松坂
 Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: isec-info@ipa.go.jp

■ 報道関係からのお問い合わせ先
 IPA 戦略企画部 広報グループ 横山／白石
 Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp