情報セキュリティ関連情報

「サイバー情報共有イニシアティブ（J-CSIP）」の紹介

独立行政法人情報処理推進機構（IPA）
技術本部セキュリティセンター
情報セキュリティ技術ラボラトリー 主任 松坂　志

1．はじめに

各国の政府機関や企業・組織に対するサイバー攻撃に関するニュースが後を絶ちません。攻撃者の正体も明らかになっておらず、高度化・巧妙化を続けるサイバー攻撃に対し、防御側（攻撃を受ける側）においては、組織を越えた「情報共有」が有効であると、国内外で様々な活動が行われています。

本稿では、IPAが「情報ハブ」（情報の集約・中継点）として民間組織と共に運用している「サイバー情報共有イニシアティブ」（J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan、ジェイシップ）について紹介します。

2．サイバー攻撃と情報共有

最初に、サイバー攻撃の特性と情報共有の必要性、そして課題について整理します（図1）。

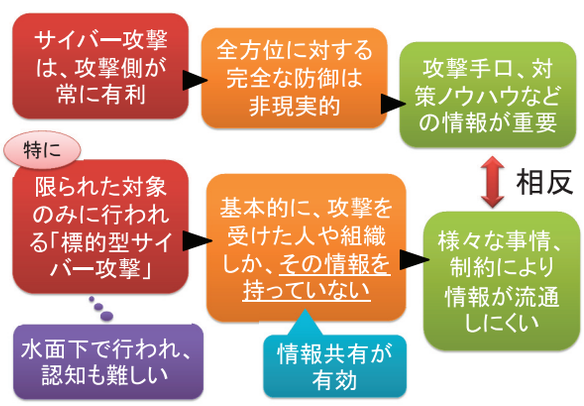


図１　サイバー攻撃の特性と情報共有の課題

（1）情報共有の必要性

サイバー攻撃においては、攻撃側が一方的に有利な状況となっています。サイバー攻撃を行う者は、攻撃するタイミングや攻撃手段を自由に選びつつ、攻撃対象の最も弱い所を突けばよい一方で、防御側の組織や企業は、全方面に完全な対策を施すことが非現実的であるためです。

このため、防御側にとっては、具体的な対策実施手段や、効果的な防御力向上のための施策の優先順位・コスト配分を検討する上で、実際の「攻撃の手口」の情報が重要です。

一方で、限られた対象のみに行われる「標的型サイバー攻撃」については、基本的に、攻撃を受けた当事者（被害者）しか、その攻撃手口の情報を知りえません。

多くのセキュリティインシデントが報じられていますが、攻撃手口の情報は明らかとなっていないか、非公開となっており、情報は常に不足しています。

このような背景から、これらの情報を共有していくことが非常に有用である、ということになります。

（2）情報共有の難しさと課題

ところが、実際の情報共有においては、「サイバー攻撃を受けた」というだけで組織の風評被害に繋がるリスクがあったり、公開しにくい内部情報が含まれていたりと、様々な障害があります。また、根本的な点として、組織にとって、情報を受け取るメリットはあっても、情報を提供するメリットが特に無いという問題もあります。

このため、攻撃に関する詳細かつ具体的な情報を組織間で共有することは簡単ではなく、洗練された組織的な攻撃者たちに対し、防御側は互いに孤立し、被害が多発している状態にあるといっても、過言ではないでしょう。

攻撃手口に関する情報が防御側に行き渡り、対策が十分に取られたことが攻撃者に伝わってしまうと、攻撃者は手口を変えて攻撃してくるようになります。情報が詳細で具体的になるほど、その情報の取り扱いには注意が求められます。

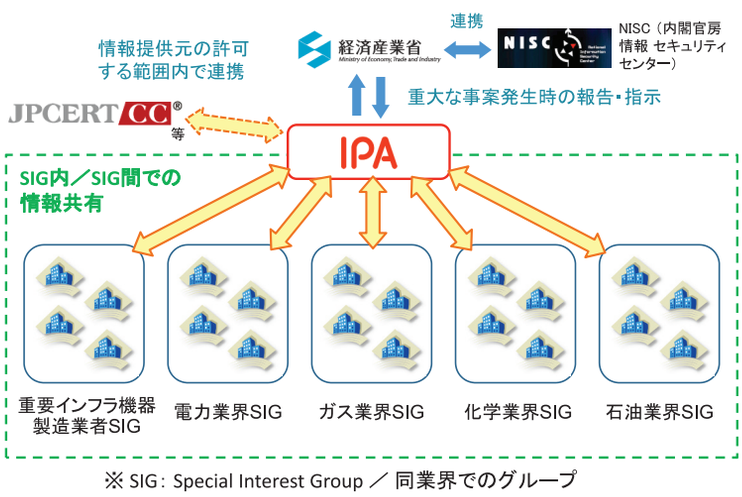
このような課題を克服し、情報共有を進めていく必要があります。

3． J-CSIPの設立

2010年末より経済産業省が開催した「サイバーセキュリティと経済 研究会」[1]における主要な提言の一つとして、「サイバー攻撃に対する官民での情報共有の必要性」が挙げられ、その実現のための準備が同省にて進められてきました。

しかし、それと時を同じくして、2011年９月には国内の重工業等複数社に対するサイバー攻撃事案が報道される事態となりました。これをうけ、同年10月25日、経済産業省の呼びかけによって、国内の重工・重電９社[1]が集まり、IPAを情報ハブとした情報共有体制、J-CSIPが発足しました。

2012年4月にはIPAと参加組織９社との間でNDA（Non-Disclosure Agreement、秘密保持契約）の締結と情報共有ルールの策定が完了し、正式運用を開始。同年７月から10月にかけ、同じ枠組みを電力・ガス・化学・石油業界へ拡張しました。本稿執筆段階では、５業界45組織がJ-CSIPへ参加しています（図２）。



※ SIG：Special Interest Group ／ 同業界でのグループ

図２ J-CSIPの体制全体イメージ

4．情報共有の枠組み

2011年10月のJ-CSIP発足から翌年４月に正式運用を開始するまでの約半年間、実務者による会合にて、どのような枠組み（体制・ルール）で情報共有を行うか、議論を重ねてきました。海外（特に米国や欧州）の先行事例もありますが、当事者である日本の各参加組織が納得できる形とすべく、情報共有のルール等は協議の上、白紙から作成しています。

J-CSIPの情報共有の枠組みは次の通りです（図３）。

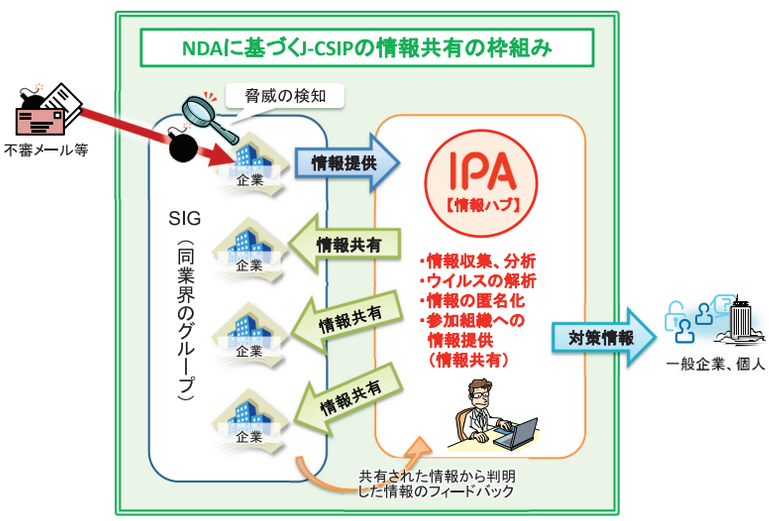


図３ J-CSIPの情報共有の枠組み

- IPAと各参加組織がNDAを締結し、情報の授受はIPAを中継して実施する。
- IPAは参加組織から情報提供を受け、必要な分析や加工を行った上で、全参加組織へ情報共有を行う。

現在、J-CSIPでは標的型攻撃メールを最初の主な情報共有の対象としています。標的型攻撃メールは、標的型サイバー攻撃での組織内ネットワークへの侵入の足掛かりとして非常に多く使用される手口であり、大きな脅威となっています。このことから、参加組織の関心も高く、実際に多くの情報が共有されています。

5．情報共有の流れ

J-CSIPにおける情報共有の流れについ

て、概要を説明します（図４）。

まず、参加組織で検知された攻撃メール等のデータが、安全な方法でIPAへ情報提供されます。攻撃を検知する手段については各組織に任せられており、IPAへの情報提供を行うか否かについても、各組織のベストエフォートとしています。

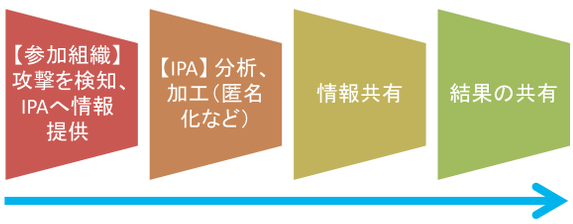


図４　情報共有の流れ

続いてIPAは、提供されたデータを分析し、必要に応じてメールに添付されたウイルスの解析情報等を付加します。また、情報提供元に関する情報や機微情報のマスク（匿名化）を行います。情報の匿名化はJ-CSIPに限らず情報共有活動における原則ですが、過剰にマスクすると情報の有効性が損なわれてしまう可能性もあり、どのような基準でマスクするか、ある程度事前に定め、合意しています。

その後、情報提供元の最終確認を経て、他の参加組織への情報提供（情報共有）を行います。こうして共有された情報を基に、各組織で調査や対策を講じます。

J-CSIPでは「結果の共有」も重視しており、共有された情報を基に分かったこと（特に無ければその旨）を、IPAへ可能な限り報告するルールとしています。同様の攻撃が発見された場合等、IPAは必要に応じてそれらの情報を再共有しています。

６．活動成果

2012年度の1年間では、全参加組織から合計246件の情報提供を受け、うち201件を「標的型攻撃メール」として取り扱いました（広くばら撒かれたウイルスメール等を除外しています）。そして、重複等を除き、有用と思われる情報の共有を160件実施しました。

IPAでは2008年から標的型攻撃メールに関する一般利用者からの情報提供の窓口を設置し、こちらは2012年度末時点の約５年間で、累計145件の情報が提供されています。J-CSIPでは１年間でこの量を超える情報提供がなされており、潜在化していた標的型サイバー攻撃の実態の一部を把握できつつあると考えています。

情報共有の直接的な成果としては、ある参加組織からの情報を基に、他の参加組織へ着信していたが未発見であった攻撃メールを発見できた、あるいは事前の対策（メールのブロック等）に繋がったという事例が複数あり、参加組織より情報共有が有効であると評価されています（図５）。

また、J-CSIPの体制の中で、ビジネス上は競合関係にもある同業他社間で情報共有を行うことができ、これまでは明確に認知できていなかった「業界を標的とした攻撃」の実情も参加組織間で共有できるようになりました。さらに、情報をIPAへ集約することで、複数の攻撃情報の相関関係が把握できるようになってきており、これらは情報共有活動による大きな進歩となっています。

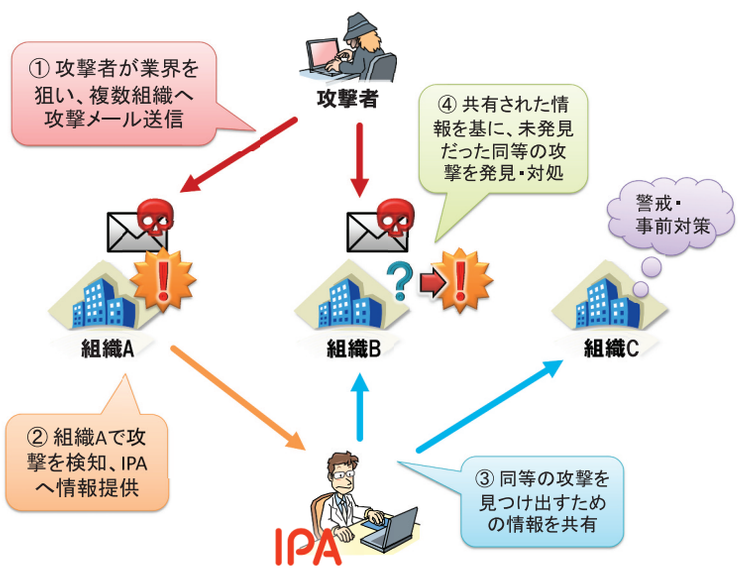


図５　情報共有による同等攻撃の発見（例）

最新のJ-CSIPの運用状況等について、詳しくはIPAのウェブサイト[2]に掲載しているレポートを参照して下さい。

７．情報共有活動のポイント

J-CSIPを立ち上げ、運用してきた中で得られた、情報共有活動のポイントを紹介します。

（1）体制・枠組み作り

情報共有を行うにあたり、まず体制を整えることになりますが、情報提供と共有が活発に行われる有意義な活動としていくためには、形だけの体制にならないよう注意が必要です。

まず、運用規程やルールの策定においては、参加者が正しく理解し、納得と合意を得られるものであることが重要です。例えば、最も重要なルールの一つである「情報の取り扱い」において、各参加組織は、情報を受領する側であり、同時に提供する側でもあることから、「共有された情報はこの範囲で使用してよい」＝「自らが提供した情報はこの範囲まで使用される」と明確に理解できる必要があります。J-CSIPでは、秘密保持の基礎的な部分はNDAで担保していますが、より細かいルールも別途定めています。

参加組織の同質性も一つの検討点です。直面している課題や問題意識、情報共有活動に対して割けるリソース（体制、工数、技術力等）がある程度同等な関係であると、後に述べる「スコープ」の輪郭がより定まりやすく、情報の授受や活用のしやすさにも繋がると思います。J-CSIPでは、この同質性を考慮して業界ごとにグループを分けています。実運用においても、グループにより活動の内容に差があるという印象です。

そして、センシティブな情報の共有には、やはり一歩踏み込んだ信頼関係が必要です。互いの顔の見える会合を持つ等、参加組織相互の、あるいは事務局（取りまとめ役）との信頼の熟成のための取り組みも、併せて検討すべきでしょう。

（2）活動のスコープ

いつでも何でも情報を共有すれば、とにかく役に立つのかというと、そうでもありません。何を目的とし（すなわち、どのような問題を解決するため）、何の情報を共有するのか、共有された情報をどう活かすのか、完全に明確でなくとも、参加組織に共通したスコープ（目的範囲）がなければ、ちぐはぐな活動となり、参加組織の満足が得られないかもしれません。

これには、「何を実施するのか」だけでなく「何を実施しないのか」の明確化も含まれます。例えば、サイバー攻撃は24時間いつでも行われる可能性があるのだから、情報共有も24時間体制にすべきという考え方もあれば、当面そこまでの必要はないという考え方もあるでしょう。また、活動のカバー対象として、大きく分けて「予防・検知」か、「インシデント対応・回復」か、あるいは両方なのかで、活動の方針は大きく変わってきます。

情報共有におけるスコープの明確さは、各参加組織からの情報提供のモチベーションにも影響するのではないかと考えます。まずは当面のスコープを必要十分な範囲に絞り、参加組織が同じ方向に向かって努力でき、同時に、活動の評価や見直しのための基点となれば好ましいでしょう。参加組織に必要以上の負荷がかかってしまったり、不要な情報の授受ばかり発生し、得られる効果よりもコストの方が高くなってしまったということでは、活動の意味がありません。

J-CSIPでも、順調に運用が進んでいる一方、全参加組織で共通の、より明確なスコープの設定という点については、今後の一層の改善を検討しています。

（3）不審メールに対する運用の見直し

IPAは一般利用者の方々に対し「不審なメールは開かず削除してください」と呼びかけており、それは今も変わっていません。

しかし、標的型サイバー攻撃の対象となっていることが明らかな組織については、その運用では不十分ではないかと考えています。具体的には、職員等が標的型攻撃メールと思われる不審なメールを受信した際に、システム管理部門等へ報告されるような仕組みが必要になってきています。

標的型攻撃メールは、一つの組織の中の複数人に着信することがあります。この時、不審であることに気付き、そのメールを削除した方は被害に遭わないのですが、他の着信者は添付ファイルを開き、ウイルスに感染した上、そのことに気付いてすらいないかもしれません。攻撃者はそのPCを遠隔操作し、組織内ネットワークへの侵入を試みます。

このようなケースを防ぐため、組織内での情報共有として、不審なメールに気付いた時はシステム管理部門へ報告してもらう運用とします。それ

が攻撃メールであると判断した場合は、当該メールと同様のメールが他の職員へ着信していないか、すみやかにメールサーバ等の検索を行い、着信者をフォローし、被害拡大を防ぐ必要があります。そして、可能であればウイルスの不正通信先（C&C[Command and Control]サーバ）を特定し、ファイアウォール等で通信を遮断することで、同等のウイルスに感染した未発見のPCによる被害も食い止められる可能性があります。

多くの組織において、不審なメールは削除し、特に報告もしないという運用を続けていることから、そもそも、攻撃が自組織に対して行われているのか否かも把握できていないのではないかと推察しています。不審なメールを探し出す試みは、被害拡大を防ぐだけでなく、攻撃の有無自体の把握や、もし攻撃が行われているとすれば、どれくらいの頻度で、どのような属性の職員が狙われているのか、あるいはどのような手口が使われているのかといった、量的・質的な状況把握に繋がります。

そして、こうして発見できた攻撃メールや不正通信先等の情報を、同時に組織間でも情報共有することで、他組織での未発見の攻撃メールやウイルスの検知、同種の攻撃による被害の防止・低減に資する可能性がある、ということになります。

ただ、ほとんどの場合において、システム管理部門の負荷の問題もあり、「不審なメールを受信したら報告してもらう」という運用に切り替えることはなかなか難しいのが実情です。しかしながら、少なくとも、組織内ネットワークで重要な権限を持っている方や、過去に不審メールが届いた経験のある方、重要な情報を取り扱っているグループ等、組織内の一部を対象とするところからでも、不審メールの報告という運用を検討していただければと思います。

他にも、PCやサーバが意図せず再起動したり、不自然な挙動を示した場合など、これまで特に報告の対象としていなかった些細な事柄も、可能であれば報告されるとよいかもしれません。こういった些細な異常から、組織内ネットワークへの攻撃者の侵入の検知に繋がった例もあり、システム的な対応だけでなく、人間の「気付き」というセンサーが有効であることを示しています。

8．情報提供のお願い

本稿の最後に、読者の皆様へお願いがあります。

IPAでは、一般利用者や企業・組織向けの「標的型サイバー攻撃の特別相談窓口」にて、標的型攻撃メールを含む標的型サイバー攻撃全般の相談や情報提供を受け付けています。限られた対象にのみ行われる標的型サイバー攻撃に対して、その手口や実態を把握するためには、攻撃を検知した方々からの情報提供が不可欠となっています。

お気付きの点がありましたら、ぜひ、相談や情報提供をお寄せください。

IPA 標的型サイバー攻撃の特別相談窓口
http://www.ipa.go.jp/security/tokubetsu/

注

(1)IHI、川崎重工業、東芝、日本電気、日立製作所、富士重工業、富士通、三菱重工業、三菱電機（50音順）の９社。

関連ＵＲＬ

[1] http://www.meti.go.jp/committee/kenkyukai/mono_info_service.html#cyber_security
[2] http://www.ipa.go.jp/security/J-CSIP/