# サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2018 年 7 月～9 月]

2018 年 10 月 26 日
IPA（独立行政法人情報処理推進機構）
セキュリティセンター

サイバー情報共有イニシアティブ（J-CSIP）[1]について、2018 年 9 月末時点の運用体制、2018 年 7 月～9 月の運用状況を報告する。1 章、2 章は全体状況を、3 章以降は本四半期で把握、分析した特徴的な攻撃事例や動向等を併せて解説する。

## 目次



[1] IPA が情報ハブ（集約点）となり、サイバー攻撃等に関する情報を参加組織間で共有する取り組み。
https://www.ipa.go.jp/security/J-CSIP/

## 1　運用体制

2018 年 7 月～9 月期（以下、本四半期）は、次の通り参加組織の増加があり、全体では 2018 年 6 月末の 11 業界 229 組織＋1 情報連携体制の体制から、11 業界 238 組織[2]＋1 情報連携体制（医療業界 4 団体およびその会員約 5,500 組織）の体制となった（図 1）。

- 2018 年 8 月、ガス業界 SIG に新たな参加組織があり、54 組織から 63 組織となった。

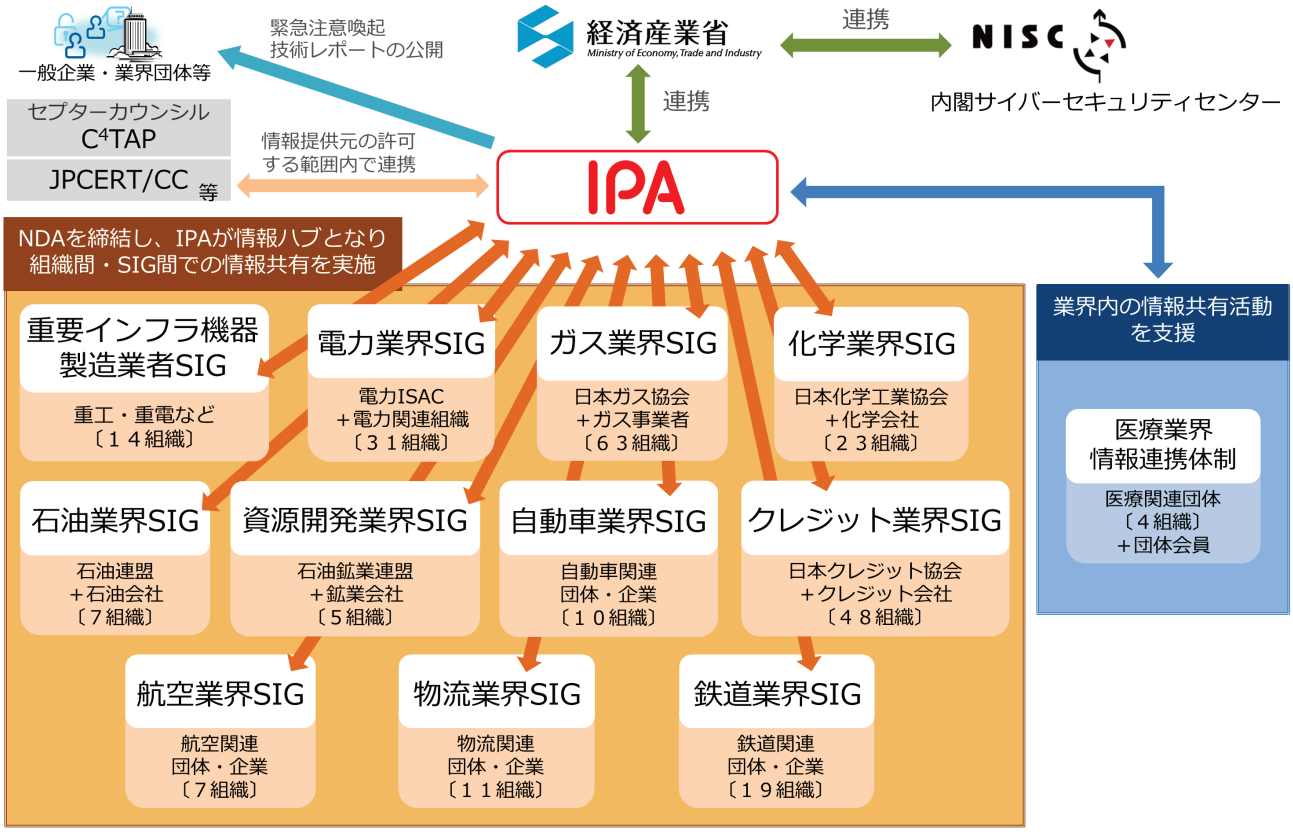


**図 1 J-CSIP の体制図**

[2] 複数業界に関係する組織が、複数の SIG に所属するケースも現れている。ここでは延べ数としている。

## 2　実施件数（2018 年 7 月～9 月）

2018 年 7 月～9 月に、J-CSIP 参加組織から IPA に対し、サイバー攻撃に関する情報（不審メール、不正通信、インシデント等）の情報提供が行われた件数と、それらの情報をもとに IPA から J-CSIP 参加組織へ情報共有を実施した件数（9 月末時点、11 の SIG、全 238 参加組織と、1 つの情報連携体制での合算）を、表 1 に示す。

**表 1 情報提供および情報共有の状況**

| 項番 | 項目 | 2017 年 | 2018 年 | | |
|---|---|---|---|---|---|
| | | 10 月～12 月 | 1 月～3 月 | 4 月～6 月 | **7 月～9 月** |
| 1 | IPA への情報提供件数 | 1,930 件 | 256 件 | 191 件 | **519 件** |
| 2 | 参加組織への情報共有実施件数※1 | 123 件 | 76 件 | 49 件 | **39 件※2** |

※1 同等の攻撃情報（不審メール等）が複数情報提供された際に情報共有を 1 件に集約して配付することや、広く無差別にばらまかれたウイルスメール等、情報共有対象としない場合があるため、情報提供件数と情報共有実施件数には差が生じる。

※2 IPA が独自に入手した情報で、J-CSIP 参加組織へ情報共有を行ったもの **15 件**を含む。

本四半期は情報提供件数が **519 件**であり、うち標的型攻撃メールとみなした情報は **30 件**であった。

提供された情報の主なものとして、8 月上旬に大量にばらまかれた IQY ファイル（拡張子が .iqy の Microsoft Excel に関連するファイル）が添付された日本語のばらまき型メールが約 75%を占めている。IQY ファイルを使った攻撃の手口については、2018 年 4 月～6 月の J-CSIP の運用状況 [3]でも注意を促していたところであった。また、本四半期においては、送信先は無差別と思われるが、これまでの日本語のばらまき型メールとは異なり、少数に宛てた日本語の攻撃メールも確認している。これについては、5 章で改めて述べる。

さらに、本四半期では日本語の文面によるビジネスメール詐欺が試みられたという事例を IPA として初めて確認した。これまで IPA では国内組織等に対する英文でのビジネスメール詐欺を確認しており、2017 年 4 月には注意喚起 [4]を公開していた。今回、更に日本語による攻撃を確認したことで、あらゆる国内企業・組織が攻撃対象となりうる状況になったと考え、2018 年 8 月、改めてビジネスメール詐欺の注意喚起 [5]を続報として公開した。なお、トレンドマイクロ社のブログ [6]によると、今回 IPA が確認した日本語のビジネスメール詐欺と同等の攻撃が複数の国内企業に着信していたとのことであり、今後、攻撃の継続・拡大が懸念される。

この他、本四半期には、J-CSIP の参加組織より、産業用機器へのウイルス感染事例の提供を受けた。この事例は、当該機器の導入時からウイルスに感染していたと思われるものであった。これについては、3

---

[3] サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2018 年 4 月～6 月]（IPA）
https://www.ipa.go.jp/files/000068064.pdf

[4] 【注意喚起】偽口座への送金を促す”ビジネスメール詐欺”の手口（IPA）
https://www.ipa.go.jp/security/announce/20170403-bec.html

[5] 【注意喚起】偽口座への送金を促す”ビジネスメール詐欺”の手口（続報）（IPA）
https://www.ipa.go.jp/security/announce/201808-bec.html

[6] 日本語の使用が確認された「ビジネスメール詐欺」、その背景に迫る（トレンドマイクロ）
https://blog.trendmicro.co.jp/archives/19654

章で述べる。また、組織内ネットワークでウイルスが複数のマシンに感染拡大したという事例の情報提供を受けた。ウイルスは、MS17-010[7]の脆弱性を悪用するものであり、組織内の一部のマシンに当該脆弱性の修正プログラムが適用されていなかったことで感染が拡大した。これについては、4 章で述べる。

その他、IPA へ次のような相談・報告事例があった（表 2）。

**表 2 相談・報告事例**

| 項番 | 相談・報告内容 | 件数 |
|---|---|---|
| 1 | パスワードリスト型攻撃を受けた。 | 1 件 |
| 2 | Office 365 のアカウント情報を狙うフィッシングメールの攻撃を確認した。 | 9 件 |
| 3 | 組織内から外部の不審サイトに不正通信を行っていることを検知した。 | 7 件 |

これらは、いずれも業務に少なからず影響が発生するものである。項番 1 では、情報提供元組織が運営する会員専用ウェブサイトに対して、パスワードリスト攻撃によるものと思われる不正アクセスが発生したものであり、本事例では実際に不正なログインが確認された。J-CSIP では、本件のインシデントに関する情報について同業界内で共有を実施している。

項番 2 は、Office 365 のアカウント情報を狙うフィッシングメールであり、継続して確認されている。改めて、Office 365 を導入している組織の利用者は、自身のアカウント情報の重要さや、そのアカウント情報を狙うフィッシング詐欺という攻撃が存在するということ、悪意のある者によってアカウント情報を騙し取られた場合、大きな被害に繋がる可能性があることを認識するべきであろう。

また、項番 3 については、前四半期から引き続き相談を受けている事例であり、組織内の PC から不審サイトへのアクセスをセキュリティ機器で検知したというものである。これらはいずれも、ウェブ閲覧中に、改ざんされたサイトや不正な広告等により、詐欺や偽警告を行う悪意のあるウェブサイトへ誘導されたと思われるものであった。通常業務の中でもこのようなことは発生しうるため、攻撃の被害に遭わないよう、不審サイト・詐欺サイト・偽警告 [8]等に騙されないように従業員への教育を行うことが重要である。また、PC のソフトウェアの脆弱性が悪用される可能性もあるため、脆弱性の解消も必須である。

[7] マイクロソフトセキュリティ情報 MS17-010 -緊急 （マイクロソフト）
https://docs.microsoft.com/ja-jp/security-updates/securitybulletins/2017/ms17-010

[8] 被害低減のための偽警告の手口と対策を紹介する映像コンテンツを公開 （IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20170411.html

## 3　産業用機器へのウイルス感染の事例

本四半期、工場に導入した機器（鋼板へ加工を施す機器）が、導入時点からウイルスに感染していたという情報提供があった。本事例においては、幸い特段の障害や問題等は発生していなかったが、状況によっては、工場等でのシステム障害に繋がりかねないものであった。本章では、ウイルス発見に至った経緯等について説明する。

**表 3 ウイルス発見に至る経緯**

| 時期 | 内容 |
|---|---|
| 2016 年上旬 | 本件機器（鋼板へ加工を施す機器）を工場に搬入・設置した。（※） |
| 2018 年 8 月 | 新たに導入した IDS で不審な DNS クエリを検知した。 |
| （約 2 週間後） | 不審な DNS クエリのリクエスト元を特定し、本件機器をネットワークから切断した。 |
| （約 1 週間後） | 本件機器のメーカーによるウイルス検査を実施したところ、機器内の制御用コンピュータ（OS: Windows Embedded）からウイルスを検出したため、駆除した。 |
| 2018 年 9 月 | 本件機器のメーカーから、開発期間中にウイルスに感染した可能性が高いとの報告があった。 |

（※）情報提供元組織にて DNS サーバのログを遡って調査したところ、工場へ設置した日付の近辺から不審な DNS クエリが発生していたことが確認できている。

感染していたウイルスは、特段、制御システムや工場を標的としたウイルスではなく、インターネットバンキングの情報を窃取する種のウイルスであったことを確認している（なお、詳細は確認できていないが、このウイルスは別のウイルスをダウンロードさせて感染させる機能等を備えているという情報もある）。

本件では、情報提供元組織において、インフラ設備側で次の対策（アクセス制御）を行っていたため、今回のウイルスが持ち込まれたことによる実質的な被害はなかった。

- 当該機器からは、社外のホストに対して IP アドレスを解決できないようにしていた。
- 当該機器からは、社外のサーバにはアクセスできないようにしていた。

しかしながら、外部への通信を必要としない、破壊的かつワーム型（感染拡大型）のウイルス[9]がこのような形で工場等に持ち込まれた場合、より大きな被害につながる可能性もある。

今回の事例から、工場用の機器であったとしても、制御用コンピュータを搭載しているような場合は、導入時に、ウイルスに感染していないか、不審な通信は無いか等について、念のため事前に確認する運用を検討する意義はあるものと考える。

[9] Wanna Cryptor（別名 WannaCry、WCry）等。

## 4　組織内で感染拡大するウイルスの事例

2018 年 7 月、組織内ネットワークでウイルスが複数のマシンに感染拡大したという相談とともに情報提供があった。本事例で感染したウイルスは、暗号通貨のマイニングを不正に行い、かつ、ネットワーク上の他のマシンへも感染を拡大する機能を持つものであった。本章では、この経緯について説明するとともに、組織がどのように対策を行ったかについて説明する。

今後も、ネットワーク上で感染拡大を行うウイルスが現れる可能性があり、また、これらのウイルスの感染が拡大することを防ぐため、組織として注意が必要である。

### 本件のウイルスの感染拡大の手口

本件のウイルスは、Microsoft 製品に関する脆弱性（MS17-010）を悪用してネットワーク上の他のマシンへ感染を拡大させ、同時に暗号通貨の不正マイニングを行う。この際、それぞれの感染マシンから社外の不正接続先への通信も発生する。この脆弱性は、2017 年 5 月に世界中で大規模な感染拡大を確認した、ランサムウェアである「Wanna Cryptor」（別名 WannaCry、WCry 等）[10]の感染拡大に悪用された脆弱性である。なお、本件のウイルスには、ランサムウェアの機能（感染マシン内のファイルの暗号化）はない。

### 発覚から対策までの流れ

発覚：

情報提供元組織において、セキュリティソフトがウイルスを検知したことにより、ウイルスの感染を確認した。セキュリティソフトが検知したファイルの削除を試みたが、マシンを再起動すると再びセキュリティソフトによってウイルスが検知され（すなわち、再生成され）、ウイルスの駆除ができない状態[11]であった。

また、一部のサーバ類に対しても、MS17-010 の修正プログラムを適用していなかったため、クライアントマシンのみならず、サーバへも感染が拡大した。

初動対応：

J-CSIP 事務局は、情報提供元組織から、セキュリティソフトが検知したウイルスファイルと現在の状況について連絡を受けた。これに対し、ウイルスの挙動や特徴、悪用する脆弱性等について、把握できた範囲で回答した。

それとともに、情報提供元組織において、ウイルスを駆除する手順を特定し、各マシンに対し次の対応を行うことで、対策を進めた。

1. 機器の再起動時に、ウイルス本体を起動する設定がされたレジストリを削除する。
2. マシンの再起動後(ウイルスが稼働していない状態で)に、ウイルス本体のファイルを削除する。
3. MS17-010 の修正プログラムを適用する。

その後：

情報提供元の組織にて、次の対策を継続し、本インシデントに対して対応を行った。

---

[10] 更新：世界中で感染が拡大中のランサムウェアに悪用されている Microsoft 製品の脆弱性対策について（IPA）https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html

[11] セキュリティソフトによって検知、および削除するファイルとは別に、ウイルスを生成する親ファイル（ウイルス本体）が存在し、そのファイルが駆除されていない状況であったものと推測している。

1. 機器の再起動時に、ウイルス本体を起動する設定がされたレジストリを削除するスクリプトを作成（他の担当者でも対応ができるように）し、そのスクリプトファイルを配付して、各マシン・サーバ等へ対応を行った。
2. MS17-010 の修正プログラムの適用を徹底した。
3. ウイルスが発生させる不正通信の状況を監視し、当該不正通信が発生していない（感染マシンが残っていない）ことを確認した。

本事例のように、MS17-010 の脆弱性は、ランサムウェア以外にも、暗号通貨の不正マイニングを行うウイルス等へも転用されている。この脆弱性を悪用するウイルスは今後も発生する可能性があり、改めて修正プログラムの適用を徹底していただきたい。また、今後、同様の脆弱性が発見された場合に備えて、クライアントマシンのみならず、サーバ類を含め、修正プログラムの適用計画や体制の整備等が必要である。

本件のウイルスは、ネットワーク上の他のマシンへ感染を拡大する機能があった。これに対し、内部ネットワークにおいて、システム上不要なマシン間の通信は遮断するといった対策も有効である。本事例に限らず、典型的な標的型攻撃における、攻撃者による内部ネットワークの側方移動（Lateral Movement）を防止・緩和することにも繋がると考えられる。

## 5　日本語ばらまき型メール等の動向

2015 年 10 月頃から国内で多く観測されるようになった日本語のばらまき型メールは、着信した組織等への偏りは見られず、個人・法人によらず広く無差別に、かつ継続的・大量に送信されている。日本サイバー犯罪対策センター[12]等からもばらまき型メールの注意喚起情報が定期的に発信されている。また、2017 年の日本語のばらまき型メールの動向について、2017 年 10 月～12 月の J-CSIP の運用状況[13]にて公開している。

本四半期では、IQY ファイルを添付した日本語のばらまき型メールに加え、遠隔操作ウイルスへの感染を企図する日本語のウイルスメールを少数確認した。これらについて、本章で説明する。

### 5.1 IQY ファイルを悪用する攻撃

本四半期、8 月の上旬に IQY ファイルを添付した日本語のばらまき型メールが国内に大量に送信された。J-CSIP の参加組織からも情報提供が多数あり、把握した範囲では 25,932 件の着信があったことを確認している。

この事象については、各ベンダからの注意喚起の記事や、報道等によって広く周知された。IPA では、2018 年の 5 月に海外で本手口による攻撃が観測されていることを確認しており、2018 年 4 月～6 月の運用状況にて、参考資料[14]として注意を促していた。なお、8 月に攻撃を観測したタイミングで、資料を改版し、日本語のメール事例を追記し、再公開している。8 月の上旬以降、IQY ファイルを添付した日本語のばらまき型メールについては確認していないが、今後も注意が必要であろう。

日本語のばらまき型メールについては、これまでも様々な手口の工夫による攻撃を観測してきた。今後も今までにない新たな手口で攻撃が行われる可能性がある。このような攻撃をひとつの対策で防ぐことは難しく、メールフィルタリング、セキュリティソフト、メール受信者の自己防衛まで含めた総合的な対策（多層防御）を行うことが重要である。

### 5.2 遠隔操作ウイルスが添付された日本語のウイルスメール

本四半期、送信先は無差別と思われるが、遠隔操作ウイルス（RAT）が添付されている日本語のウイルスメールを確認した。これは、これまで多く観測されているインターネットバンキングを狙う攻撃とは異なる意図によるものと思われる。J-CSIP の参加組織内で情報共有したところ、同等の攻撃に関する情報提供があり、ごく少数の組織かつ少人数に対して送付されたであろうことを確認している。

特定の業種や組織を狙った攻撃と判断できるだけの情報はなく、現時点では標的型攻撃とは見なしていないが、同等の攻撃が継続する可能性があるため、引き続き注視していく。

---

[12] 日本サイバー犯罪対策センター（JC3）
https://www.jc3.or.jp/

[13] サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2017 年 10 月～12 月]（IPA）
https://www.ipa.go.jp/files/000063812.pdf

[14] 【参考資料】IQY ファイルを悪用する攻撃手口に関する注意点（第 2 版）（IPA）
https://www.ipa.go.jp/files/000068065.pdf

## 6　WIZ ファイルを悪用した攻撃の手口

2018 年 9 月、マクロ機能を悪用する、Microsoft Word の WIZ（Wizard）ファイルを用いた攻撃手口の情報を入手した。

メールに添付される Office 文書ファイルによる攻撃の多くは、Microsoft Office の「保護ビュー」の機能で防御することが可能であり、本攻撃手口も「保護ビュー」を有効にしている状態ではウイルスに感染しないことを確認している。

マクロ機能の悪用に対してはマクロ機能を有効にしないように徹底することで危険を避けることが可能だが、今回確認した手口では、通常ではあまり見かけない拡張子の Word 文書ファイルであり、利用者ひとりひとりに注意点を周知するべく、参加組織へ情報共有を実施した。

この手口について、今後、国内での攻撃に使われるようになる可能性があるため、攻撃手口と注意点をまとめた一般利用者向けの参考資料を、本紙と併せて公開した[15]。

IPA で確認できている範囲では、海外で無差別にばらまかれたウイルスメールの添付ファイルで悪用された手口であり、2018 年 9 月時点では、日本語のメールで攻撃が行われた可能性を示す情報は確認していない。攻撃の特徴、ウイルス感染を防ぐため利用者が選択するべき操作について広く周知することが重要だと考える。必要に応じ、参考資料を活用していただきたい。

### 関連情報のご提供のお願い

本書で紹介した事例について、J-CSIP では関連情報を求めています。
同様の事例を確認した場合など、下記窓口へ情報提供をいただけますと幸いです。

**J-CSIP 事務局　ご連絡窓口（IPA）**
jcsip-info@ipa.go.jp

### 標的型サイバー攻撃特別相談窓口

IPA の「標的型サイバー攻撃特別相談窓口」では、標的型サイバー攻撃を受けた際の相談を受け付けています。お気づきの点があれば、ご相談ください。

**標的型サイバー攻撃特別相談窓口（IPA）**
https://www.ipa.go.jp/security/tokubetsu/

以上

[15] 【参考情報】WIZ ファイルを悪用する攻撃手口に関する注意点