サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2017 年 1 月～3 月]

2017 年 4 月 27 日
IPA（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

サイバー情報共有イニシアティブ（J-CSIP）[1]について、2017 年 4 月 27 日時点の運用体制、2017 年 1 月～3 月の運用状況、2016 年度（2016 年 4 月～2017 年 3 月）を含む年度毎の運用状況を示す。

1 運用体制

2017 年 4 月 26 日、J-CSIP で新たに「クレジット業界 SIG」が発足した。クレジット業界は「重要インフラの情報セキュリティ対策に係る第 3 次行動計画」[2]において、国内の重要インフラの 1 分野として追加された業界である。クレジット業界におけるサイバーセキュリティに関する活動の一環として、J-CSIP への参加を検討いただいていたところ、日本クレジット協会およびクレジット関係企業 28 社に「クレジット業界 SIG」として参加いただけることとなった。

なお、2017 年 1 月～3 月期に石油業界 SIG 内での組織改編に伴い、当該 SIG の参加組織数が 8 組織から 7 組織となっている。

2017 年 4 月 27 日時点において、J-CSIP の全体の運用体制は、図 1 に示すとおり、8 業界 115 組織の体制となった。

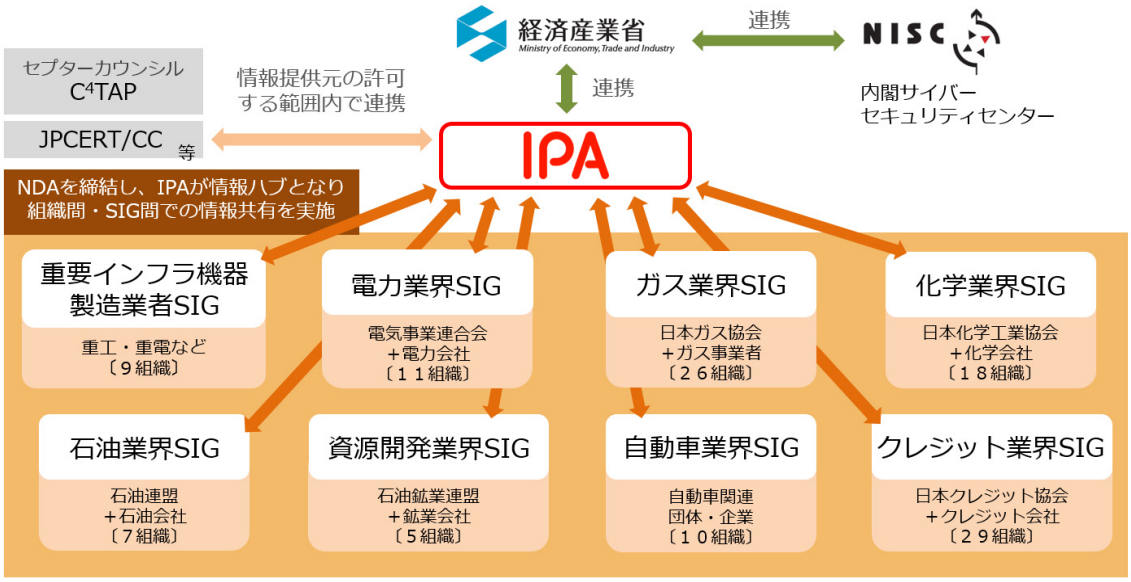

図 1 J-CSIP の体制図

---

[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/

[2] 「重要インフラの情報セキュリティ対策に関する主な資料」（内閣サイバーセキュリティセンター）
https://www.nisc.go.jp/active/infra/siryou.html

2　実施件数（2017 年 1 月～3 月）

2017 年 1 月～3 月に、J-CSIP 参加組織から IPA に対し、標的型攻撃メールと思われる不審なメール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（3 月末時点、7 つの SIG、全 86 参加組織での合算）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	2016 年			**2017 年**
		4 月～6 月	7 月～9 月	10 月～12 月	**1 月～3 月**
1	IPA への情報提供件数	1,818 件	218 件	396 件	**73 件**
2	参加組織への情報共有実施件数	33 件	32 件	22 件	**9 件**※1

※1 同等の攻撃情報が複数提供された場合等、1 件に集約して情報共有を実施する場合があり、情報提供件数と情報共有実施件数には差が生じる。また、IPA が独自に入手し J-CSIP 参加組織へ共有を行った情報 **5 件**を含む。

本四半期は情報提供件数が **73 件**であり、うち標的型攻撃メールとみなした情報[3]は **0 件**であった。標的型攻撃メールの観測数の多寡には波があるとはいえ、3 ヶ月連続で 0 件となったのは、2012 年度の J-CSIP 運用開始以来、初めてのことである。四半期ごとの件数で見ても、これまで最も観測数が少なかったのは 2015 年度第 3 四半期（10～12 月）と 2016 年度第 3 四半期（10～12 月）の 19 件である。

なお、この四半期、J-CSIP での提供は無かったが、IPA 全体としては国内での標的型攻撃の発生を観測している。J-CSIP に限らず IPA の他の窓口等を含め情報提供を受けた範囲では、国内の組織へ少なくとも 10 件を超える標的型攻撃メールが着信しており、また、分析の結果、それらは 2016 年以前から行われている一連の攻撃の一部であろうことも確認している。IPA としては、標的型攻撃の脅威が衰えたという認識はなく、今も変わらず注意が必要であると考えている。

本四半期に限らず、2015 年頃から標的型攻撃メールの観測数は減少傾向にある。この理由は明らかでないが、例えば次の 2 点の可能性が考えられる。

1 点目は、標的型攻撃メールがこれまで以上に巧妙化し、現状の対策では検知しにくく、「攻撃が見えなくなっている」可能性である。2014 年頃までの傾向と比較すると、攻撃者はより慎重に行動しているように思われる。例えば、複数の組織・従業員に対し何通も攻撃メールが着信する事例よりも、ほんの数件（場合により 1 件のみ）が着信するという事例が多くなっているように見受けられる。

2 点目は、防御できているがために、攻撃を認知・確保できなくなっている（よって情報提供に繋がらない）可能性である。メールフィルタやウイルス対策機能の性能の向上や、危険な拡張子の添付ファイルを拒否するといった対策が有効に機能すると、多くの攻撃メールについて、着信する前にブロックできる。これ自体は好ましい状況であるが、一方で、着信まで至っていないメールの中には、広くばらまかれたウイルスメールに混じり、「自組織を標的とした攻撃が失敗したもので、調査を行い今後の対策に活かすべき事案」も含まれる可能性がある。このような、ブロックに成功した不審メールまでを調査する組織は少ないものと思われるが、それにより攻撃の兆候が捉えにくくなるとすれば、今後の課題となってくると思われる。

---

[3] J-CSIP では、広く無差別にばらまかれたと思われるウイルスメールは除外した上で、添付ファイルにより感染させられるウイルスの種類、過去の攻撃との関連性、メールの内容の巧妙さといった観点により、標的型攻撃メールと見なし対応するか否かを判断している（判断が難しいケースもあり、その場合は情報共有を実施しながら、分析を継続する）

本四半期に提供を受けた情報の中では、日本語のばらまき型メールが前四半期に引き続き観測されている。ばらまき型メールとは、国内の一般利用者を攻撃対象に、広く大量に送信されているウイルスメールであり、添付ファイルを開いた場合、オンラインバンキングの情報を窃取するウイルス等に感染させられることを確認している。日本サイバー犯罪対策センター[4]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おり、多くの人の目にウイルスメールの情報が留まりやすくなっているが、日本語のばらまき型メールについては一見して不自然だと判断しにくいものが増えているため、こちらも引き続き注意を要する状況にある。

3 実施件数の年度毎推移

J-CSIP が運用開始した 2012 年度から、2016 年度までの J-CSIP の活動における情報提供件数等の推移を次の表 2 と図 2 に示す。

表 2 5 年間の情報提供件数・標的型攻撃メールの件数・情報共有件数

項目	2012 年度	2013 年度	2014 年度	2015 年度	2016 年度
IPA への情報提供件数	246 件	385 件	626 件	1092 件	2505 件
標的型攻撃メールと見なした件数	201 件	233 件	505 件	97 件	177 件
情報共有実施件数	160 件	180 件	195 件	133 件	96 件

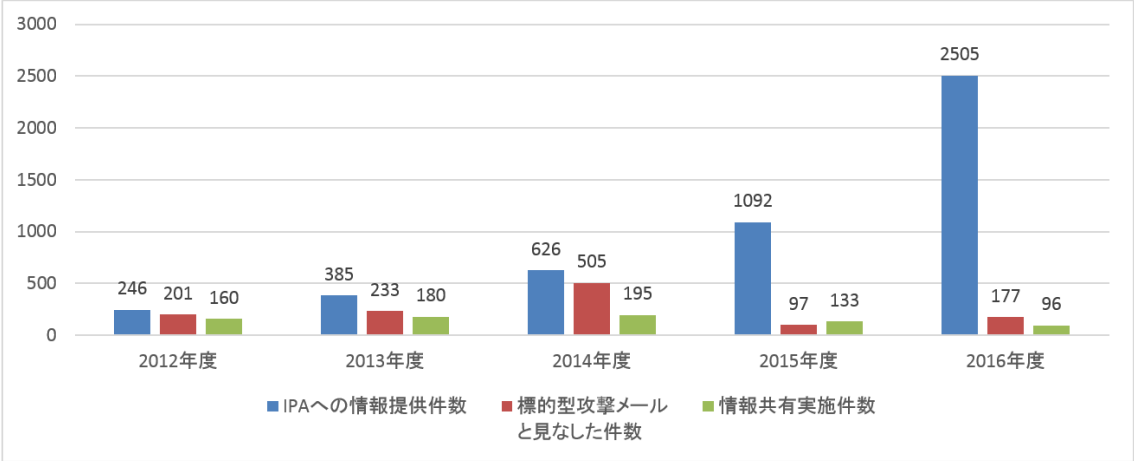

図 2 5 年間の情報提供件数・標的型攻撃メールの件数・情報共有件数 グラフ

標的型攻撃メールの件数は 2014 年度の 505 件が最も多く、年度単位で最も件数が少なかったのは 2015 年度の 97 件である。2015 年度は国内の多数の組織で標的型攻撃の被害が報告された時期でもあるため、この結果は意外かもしれないが、攻撃メールの観測数と、攻撃の危険性は必ずしも連動するものではないことを示している。

攻撃者は、広い対象に一斉に攻撃を行ったり、攻撃が露見しないよう慎重に（目立たないよう）攻撃を仕掛けたりと、手口を変えてくる。標的型攻撃との戦いは、ウイルスとの戦いではなく、ウイルスを送りつけてくる人間との戦いであり、簡単に数字で表すことが難しいものでもあると言えるだろう。

---

[4] 一般財団法人日本サイバー犯罪対策センター JC3
https://www.jc3.or.jp/topics/virusmail.html

IPA への情報提供件数に着目すると、2012 年度から毎年増加傾向にあり、特に 2015 年度からの増加が顕著で、2016 年度は 2012 年度の約 10 倍となった。J-CSIP の参加組織の増加も一部要因であるが、この提供件数の増加は、先にも述べたばらまき型メールの提供が主な要因である。

J-CSIP では、不審だと考えたならば、広くばらまかれたウイルスメールの可能性があっても、可能な範囲で情報提供をいただくよう呼びかけている。特に 2015 年度以降は、広くばらまかれるウイルスメールの件名・本文・添付ファイル名に日本語が使われるようになり、ますます注意が必要となっている。2017 年度に入ってからも、様々なパターンの日本語のばらまき型メールが出回っており、これらについても、必要に応じて情報共有を行っている。

サイバー攻撃に関する情報提供は、「ウイルスが添付されたメール」には限らず、その一つの例として、ビジネスメール詐欺（BEC[5]）に関する情報共有も実施している。ビジネスメール詐欺とは、巧妙に細工したメールのやりとりにより、企業の経理部門等の担当者を騙し、攻撃者の用意した口座へ送金させる詐欺の手口である。この攻撃手口について、J-CSIP 内で提供・共有された、複数の参加組織からの情報を整理し、2017 年 4 月 3 日、レポート「ビジネスメール詐欺 『BEC』に関する事例と注意喚起」[6]として公開した。

ビジネスメール詐欺は手口が巧妙かつ悪質であり、標的型攻撃とも通じるところがあるもので、被害を防ぐために何よりも重要と言えるのは、各組織の経理部門等がこのような手口の存在を認識しておくことである。レポートでは、なかなか表には出てこないと思われる、実際に国内企業やその関連企業が受けた攻撃について、攻撃者とのメールのやり取りの経緯や、メールに仕掛けられた様々な騙しの手口を紹介している。重要な点のみまとめた「要約版」も併せて公開しているため、広く企業や組織で参考としていただければと考える。

国内の企業・組織を狙うサイバー攻撃と戦っていくための一つの手段として、J-CSIP は 2017 年度以降も情報共有の活動を継続していく。

「標的型サイバー攻撃特別相談窓口」への情報提供のお願い

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る。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、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である。ぜひ、相談や情報提供をお寄せいただきたい。

「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

---

[5] Business E-mail Compromise （ビーイーシー）
[6] 【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
https://www.ipa.go.jp/security/announce/20170403-bec.html