特集

サイバー攻撃防衛のための取り組み

組織へのサイバー攻撃はますます巧妙化してきており、情報資産の流出や盗用、不正アクセスは組織に大きな損失をもたらしている。さらには、インターネット・バンキングにおける不正送金などの社会問題も起きており、今後、大学もその大きなリスクに晒される可能性もある。

そこで本特集では、サイバー攻撃の最新の攻撃パターン、攻撃への対処法として組織間の情報共有と分析、組織内での防御訓練などを紹介し、大学の喫緊の課題として、情報セキュリティの危機管理能力の向上、強化に向けて理解を深めたい。

サイバー攻撃の情報共有活動とその成果

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 主幹　松坂　志

1．はじめに

官民連携による標的型サイバー攻撃への対策の一つとして、IPAが「情報ハブ」（情報の集約・中継点）となり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）[1]が発足してから、３年が経ちました。

本稿執筆時点で、J-CSIPには五つの業界から53の企業・組織が参加し、特に標的型攻撃メールの情報を多く取り扱っています。IPAがJ-CSIPの参加組織から提供を受けた標的型攻撃メールの件数は累計で785件（2014年12月末時点）にのぼっており、これは、筆者が想定していた量を大きく超えています。これまで見えていた情報は氷山の一角であって、情報共有の体制を整え運用してきたことで、はじめて認知できたことが数多くあります。

本稿では、簡単ではありますが、このJ-CSIPの活動の中で明らかになった「やり取り型」標的型サイバー攻撃の手口の説明とともに、情報共有活動の有効性についてご紹介します。

2．「やり取り型」攻撃

「やり取り型」攻撃とは、一般の問い合わせ等を装った無害な「偵察」メールの後、ウイルス付きのメールが送られてくるという、標的型サイバー攻撃の手口の一つです。攻撃者からのメールは、当該組織への問い合わせがあるといった内容で始まり、窓口担当者がそれを受け付ける旨を返信すると、ウイルスが添付されたメールが送られてきます。組織の窓口部門としては、多少不審であっても添付ファイルを開いて内容を確認せざるを得ず、攻撃者もそのことを熟知した上で攻撃を行っていると思われます。実際の「やり取り型」攻撃の事例で、組織の窓口と攻撃者との間で送受信されたメールの流れを表１に示します。

表１　「やり取り型」攻撃の事例

No	種別	メールの内容
1	偵察	製品に関する問い合わせとして、最初のメール（無害）が着信した。
2	返信	窓口から回答を行った。
3	攻撃	「本研究室の資料」の送付と称し、Word文書ファイル（ウイルス）が添付されたメールが届いた。
4	返信	送付された文書ファイルの内容が確認できなかった旨を返信した。
5	攻撃	「本研究室の資料」の再送付と称し、今度はRAR形式圧縮ファイル（内容はウイルス）が届いた。
6	返信	送付されたファイルの内容が確認できなかった（解凍できなかった）旨を返信した。
7	偵察	解凍ソフトは何を使用しているか、攻撃者から質問のメール（無害）が届いた。
8	返信	「Lhaplus」という解凍ソフトを使用した旨を返信した。
9	攻撃	再度、「本研究室の資料」の再送付と称し、RAR形式圧縮ファイル（内容はウイルス）が届いた。このファイルは「Lhaplus」で解凍できるようになっていた。

この事例では、３回に亘り形式の異なるウイルスファイルが送りつけられており、標的とした組織の内部ネットワークへ何としてでも侵入しようという、攻撃者の明確な意思が感じられます。また、「圧縮ファイルが解凍できなかった」という組織からの返信に対し、使用している解凍ソフトを聞き出して、その解凍ソフトに対応するよう添付ファイルの圧縮方式を改善、すなわち、攻撃者が「学習」した形跡もありました。

このような悪質な標的型サイバー攻撃が、国内の組織に対して行われているのが現実です。そして、標的となっているのは、大企業や政府機関には限りません。

３．情報共有の有効性

IPAでは、J-CSIPや「標的型サイバー攻撃の特別相談窓口」等の活動を通し、この「やり取り型」攻撃について、関係組織間での情報共有と分析を行いました。その成果として、様々なことが明らかになっています。

（１）認知されていなかった攻撃の発見

J-CSIPでは、情報提供元に関する情報を伏せた上で、不審なメールの送信元メールアドレスや件名等の情報を参加組織間で共有しています。

この情報共有によって、標的型攻撃として認知されていなかった、同様の「やり取り型」攻撃メールが複数の組織で発見されました。情報共有を行っていなければ、これらのメールは未発見のままであった可能性があります。

さらに、いくつかの組織で、最初の「偵察」メールを不審と感じ、返信していなかった案件も見つかりました。この場合、その後に控えているウイルス付きメールが送られてこないため、当該メールの正体が悪意のあるものか否か、その組織にとっては不明な状態でしたが、他の組織から共有された情報によって、それが「やり取り型」攻撃の一部であったということが分かりました。同じ攻撃者によって狙われていたことが確定したため、直接的に攻撃を受けなかった（ウイルスの受信までは至らなかった）組織においても、警戒態勢の強化に繋がっています。これも、単独の組織では分からなかったことです。

（２）国内複数組織を狙う攻撃の実態解明

こうした情報共有を通じて発見された情報をさらに集約していくことで、この「やり取り型」攻撃が、日本国内の複数の組織に対し、継続して巧妙に行われていた実態が明らかになりました。

例えば、この攻撃者（あるいは攻撃グループ）は、表１で示した約10日間に亘る一連の「やり取り」と同時並行して、合計３組織、六つの窓口に対して攻撃を行っていたことが分かりました（図１）。それぞれの攻撃では、騙る身分や問い合わせの内容を変化させており、攻撃が露見しないよう慎重に行動していたことが伺えます。

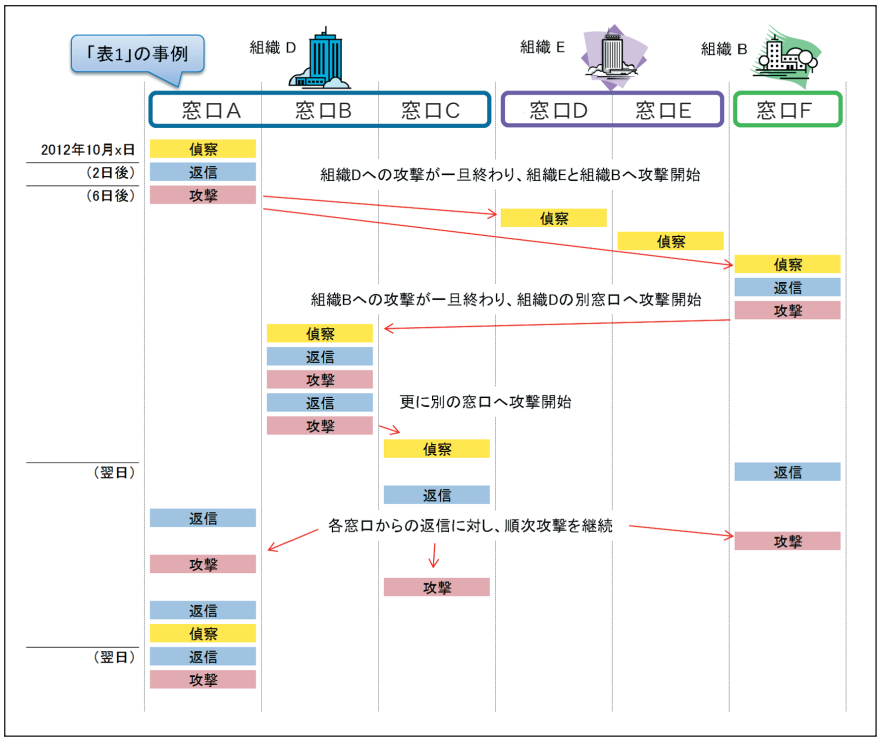

図１　複数組織への攻撃が並行している様子

また、表１の事例では、攻撃者が“添付ファイルの圧縮方式の改善”を行いました。確認したところ、この事例より過去の「やり取り型」事例で観測された圧縮ファイルは、同様にすべて「Lhaplus」では解凍できませんでした。しかし、この件より後の事例で観測された圧縮ファイルは、最初から「Lhaplus」で解凍可能となっており、攻撃者がこの事例の時点で「学習」し、以降の攻撃へもその技術が反映されているということが、より明確になりました。

その他、情報の共有を進めたからこそ分かった事実がいくつもあります。詳しくは、J-CSIPのウ

ェブページで公開している「2013年度 活動レポート」を参照いただければと思います。

なお、IPAでは、2014年８月から10月にかけ、再び「やり取り型」と同等の攻撃が、国内の五つの組織に対し計７件発生したことを観測しました。この状況を受け、特に各組織の窓口部門の方へ、注意を呼びかけています[2]。

４．大学間情報共有の重要性

本稿で挙げた「やり取り型」の事例では、「攻撃があったことに気付いていなかった」という組織が少なくありませんでした。

本格的に大学を標的としたと思われるサイバー攻撃について、筆者は少数の事例を確認しているのみですが、実際はどうなのでしょうか。大学は、まだあまり標的となっていないのでしょうか。それとも、表面化していないだけでしょうか。

標的型サイバー攻撃に限らず、ネットワーク上で発生している様々な問題は、認知しにくく、対応も難しいものです。これは、システム管理を担っている職員の方々が苦心していることと思います。

まだそのような取り組みがないのであれば、これからのことを考え、大学間での情報セキュリティに関する情報共有の仕組みを検討することが重要であると思います。具体的には、検知した攻撃（脅威）に関する情報や、インシデント対応に関する情報の共有です。大学という、やや特殊なIT環境において、どのような攻撃や事故が発生したか、それらをどのように対応したか、といった情報を相互に共有することは、役に立つと考えられ、今までまったく見えていなかった問題が見えるようになる可能性もあります。

情報共有が有効であろうことは、本稿での指摘がなくとも誰しも認識していることでしょう。ただ、実際には、機微な内容を含む情報の交換となりますし、各組織の信頼できる窓口を決め、情報の取り扱いのルールを定め、何よりも、各組織が一歩前に踏み出し情報を提供していくという、いくつかのハードルが存在します。

しかし、少しずつでも、そのような情報共有のネットワーク（これは、信頼のネットワークでもあります）を形成・維持していくことが重要です。いざというとき、例えば、複数の大学が関係し、機微な内容を含むようなセキュリティインシデントや標的型サイバー攻撃が発生した場合を想定します。誰に連絡すればよいのか、また、連絡した内容は適切に扱われるのか、そのときになってから調整するのではなく、既に確立した情報共有のネットワークがあれば、スムーズな連携と対応が可能になるのではないでしょうか。

５．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
https://www.ipa.go.jp/security/tokubetsu/

関連URL

[1] https://www.ipa.go.jp/security/J-CSIP/
[2] https://www.ipa.go.jp/security/topics/alert20141121.html

参考：大学等へのサイバー攻撃事例

実際に大学等が標的とされたサイバー攻撃の事例を以下に掲載します。

（私立大学情報教育協会）

事例1	研究プロジェクトの成果を紹介するWebサーバ内に、マルウェアと思われる不正なファイルが置かれ、ダウンロード可能な状態となっていた。調査により、ＣＭＳの脆弱性を突かれたことが判明した。
事例2	市町村と実施している観光スポット紹介のWebサーバ（市町村が管理）のセキュリティホールを利用して、ハッキング成功を誇示するHTMLファイルがサーバ内に置かれた。そのファイルは英語とイスラム語で書かれていた。
事例3	一部のサイトを管理するサーバに侵入され、英語で「侵入成功」と記された不正なファイルが置かれていた。サーバOSの脆弱性を突かれた可能性がある。