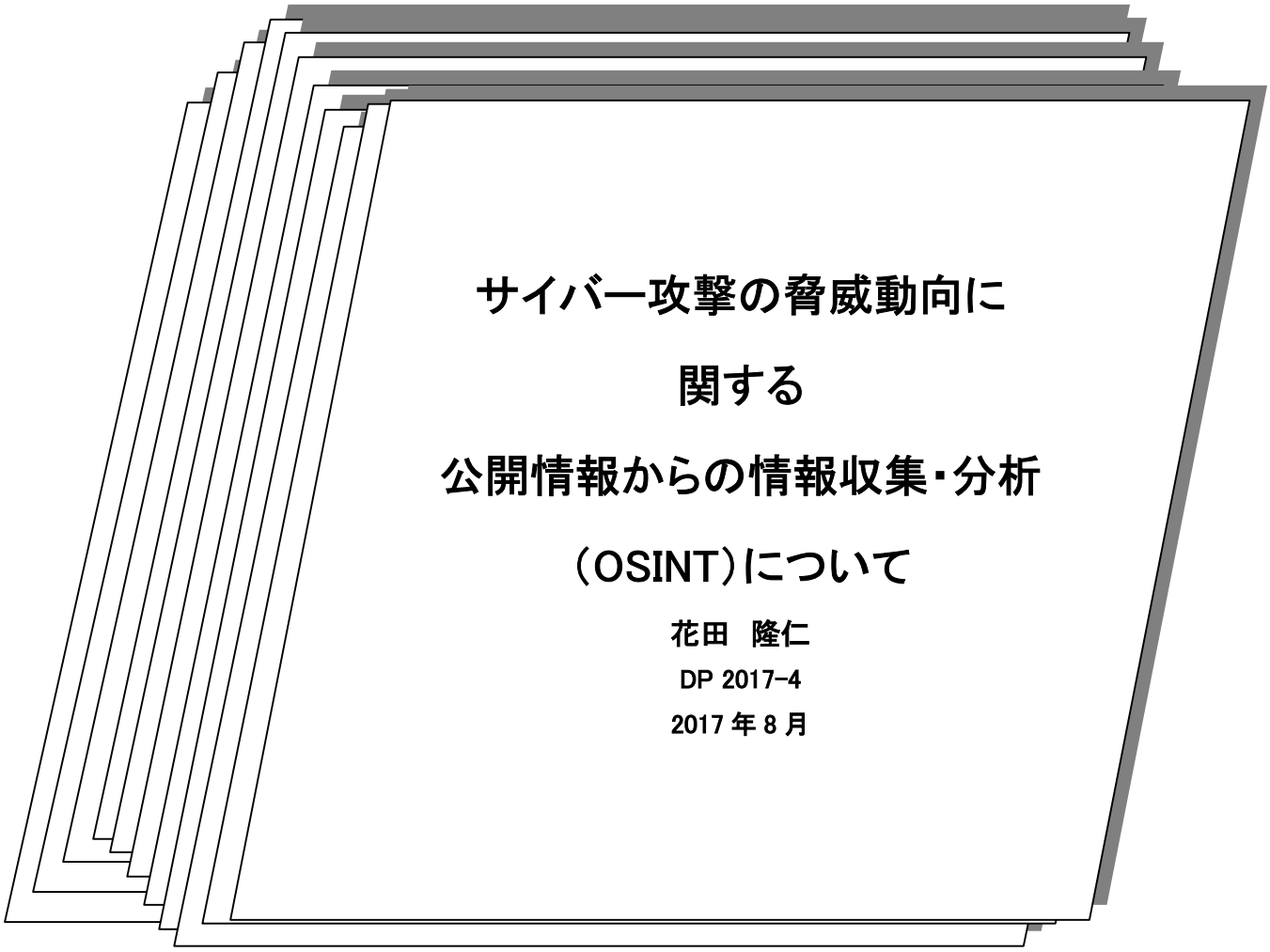
FSA Institute
Discussion Paper Series



サイバー攻撃の脅威動向に関する公開情報からの情報収集・分析（OSINT）について

花田　隆仁

DP 2017-4

2017 年 8 月

金融庁金融研究センター
Financial Research Center (FSA Institute)
Financial Services Agency
Government of Japan

＜金融庁金融研究センター　ディスカッションペーパー DP2017-4（2017 年 8 月）＞

サイバー攻撃の脅威動向に関する公開情報からの情報収集・分析（OSINT）について

花田　隆仁*

概要

金融機関や官公庁をはじめとして、組織を狙ったサイバー攻撃の脅威が増加しており、また攻撃手法も多様化している。こうした中、日々変化し続けるサイバー攻撃の脅威動向に対応すべく、金融機関や官公庁においても自らサイバー攻撃に関する情報収集・分析を行い、自組織のサイバーセキュリティ態勢の見直し（自助）、及び他組織との情報共有（共助・公助）に繋げていくことが重要である。

筆者は 2015 年より、当庁の研究官として、公開情報を用いて情報の収集、分析などを行う OSINT を活用し、主に金融業界におけるサイバー攻撃の脅威動向の把握、及び庁内職員への情報展開を業務として行ってきた。今回、この業務を通じて得られた、サイバー攻撃の脅威動向に関する情報収集・分析の具体的かつ効果的な手法、及び組織内への情報展開方法等について説明する。 特に、収集すべき情報ソースの種類、有用な情報ソースの見極め方、収集した情報の分析時に留意すべきポイントなどについて、実例も交えて詳説する。最後に日本の金融機関がどのような対応をすればよいかについて、私見を述べる。

キーワード：サイバーセキュリティ、サイバー攻撃、OSINT

* 金融庁金融研究センター研究官。本稿の執筆に当たっては、金融庁鎌田参与、総務企画局政策課サイバーセキュリティ対策企画調整室鈴木室長、及び監督局総務課稲田監督管理官に有益なご意見を賜った。なお、本稿は筆者の個人的見解であり、金融庁および金融研究センターの公式見解ではない。また、ありうべき誤りは、全て筆者個人の責に帰すべきものである。

1　はじめに

1.1 日本国内に対する最近のサイバー攻撃の脅威動向

金融機関や官公庁をはじめとして、日本国内に対するサイバー攻撃の件数は年々増加の一途をたどっている。例えば、国立研究開発法人・情報通信研究機構（NICT）が 2017 年に公表したデータ[†)]によると、2016 年の 1 年間に検知した国内ネットワークに向けられたサイバー攻撃関連の通信が、前年比 2.4 倍の約 1,281 億件にのぼっている。加えて、警察庁が公表しているデータ[‡)]では、2016 年に把握した標的型攻撃を意図したメールの検知件数が、前年比 218 件増加の 4,046 件となっている。

また、サイバー攻撃は件数が増加しているだけでなく、その手口も日々進化している。例えば、DDoS 攻撃[§)]の手口について、従来のような攻撃先のサーバに対して複数台のコンピュータを用いて大量の通信を発生させる攻撃手法だけでなく、最近では「Mirai（ミライ）」などに代表される、IoT 機器[**)]を外部から不正操作するマルウェアを用いて、無数の IoT 機器から同時に通信を発生させ、攻撃先のサーバに対して従来の手法よりも大きい負荷を与える手法なども確認されている。他にも、システムやソフトウェアの脆弱性について、最近では脆弱性が公表された翌日には攻撃手法がインターネット上に公開されてしまい、攻撃者がそれを用いて攻撃することにより、被害が発生するといった事例も発生している。

1.2 本論文の目的

このように、日々脅威を増すサイバー攻撃に対処するには、具体的な対策を講じる前に、まずは現在発生しているサイバー攻撃の手口や攻撃者の動向、攻撃に晒され得るシステムやソフトウェアの脆弱性の状況などについて日常的に情報収集を行い、どのような脅威が存在しているかについて把握することが必要である。その上で、収集した情報から攻撃手法の特徴などの分析を行い、自組織に対する脅威を洗い出し[††)]、サイバーセキュリティの態勢を必要に応じて見直す（自助）等の対応が必要となる。また、収集した情報は、他の組織にも共有し、業界全体などで広く対応態勢を強化する（共助）等の行動が必要となるほか、筆者が所属する金融庁においては特に注意が必要な脅威動向に関し、監督下の金融機関に対して注意喚起を実施（公助）【参考１】している。

[†)] http://www.nict.go.jp/cyber/report.html

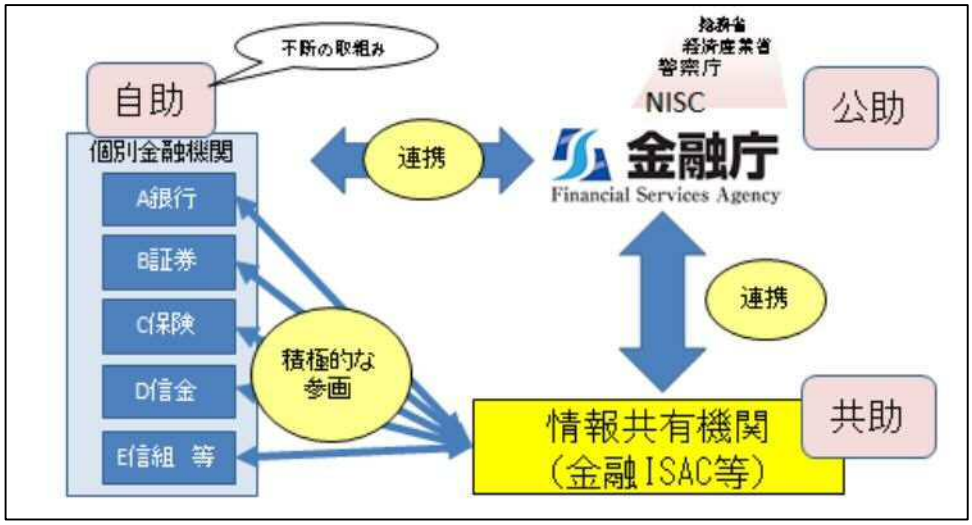
[‡)] http://www.npa.go.jp/news/release/2017/20170323cyber_jousei.html

[§)] Web サイトなどに対して大量の通信を発生させ、サーバに大きな負荷をかけたり、サーバに至るまでのネットワークを圧迫する攻撃。攻撃が成功すると、対象の Web サイトが閲覧不可となる等により、Web サイトでの顧客へのサービス提供が不可能になる等の被害が発生する。

[**)] インターネットに接続されたルータや家電製品、OA 機器などを指す。

[††)] なお、前提として、自組織が保有する情報資産の状況、サイバー攻撃への対策状況、外部委託先の状況等、自組織における IT システムに関するリスクの状況を確認しておく必要もある。

【参考１】自助・共助・公助のイメージ



（金融庁公表資料より引用）

では、金融機関や官公庁をはじめとした組織において、サイバー攻撃の脅威動向に関する情報収集・分析を行い、自組織に対する脅威を特定するためにはどうすれば良いか。例えば、情報収集についてグループ内や業界内の他組織、及び業界団体等からの情報連携に頼る、という方法もある。しかし、自組織に必要な情報が十分に得られない可能性や、情報連携が遅れ、その前に自組織への攻撃が発生する可能性がある。従って、外部の組織に依存しすぎず、自組織内でも情報収集を行い、脅威動向の分析を行なう必要がある。その方法の１つとして、本や雑誌、新聞、インターネット等で一般に公開されている情報（公開情報）活用するという方法が考えられる。このような公開情報からの情報収集・分析は、OSINT（オシント：Open Source Intelligence）とも呼ばれており、多くの国々の情報機関においても採用されている手法である。情報機関によっては、活動全体の 80%以上を占めるとも言われている。

筆者は金融庁において、金融業界におけるサイバー攻撃に関する脅威動向について、公開情報、特にインターネット上に公開されている情報の収集・分析を行い、得られた知見を組織内に提供する業務に当たってきた。そこで本論文では、筆者が業務を通して得た、情報収集・分析、及び組織内での情報共有における具体的な手法について説明し、その有効性や注意点などについて私見を述べたい。なお、本論文では、金融業界のサイバー攻撃の脅威動向を把握することを目的に、筆者が業務にて実際に行なった内容を説明するため、金融機関などが業務の参考にされる際には、「金融業界」と記載している箇所を適宜「自組織」と読み替えていただきたい。また、本論文の内容や意見については、筆者個人に帰属するもので、金融庁ならびに金融研究センターの公式見解ではない。

2　情報収集・分析のプロセスについて

まず、情報収集・分析を行うにあたり、どのようなプロセスが存在するかについて整理する。ここでは世界各国の情報機関が同様の活動を行う際のプロセスである「インテリジェンスサイクル（情報活動サイクル）」という概念を紹介したい。

「インテリジェンスサイクル」の定義は、「情報を収集、分析し、最終的に意思決定を行なうために必要な情報を提供する一連のプロセスについて整理したもの」である。「インテリジェンスサイクル」の構成要素については諸説ある模様だが、例えば米国の国家情報長官室が発行している「2009 年国家インテリジェンス使用者の手引き（2009National Intelligence Consumer’s Guide）」では、「計画と指示（Planning and Direction）」、「収集(Collection)」、「整理‡‡)(Processing)」、「分析と生産(Analysis and Production)」、「情報提供§§)(Dissemination)」の５つのプロセスを挙げている。各プロセスの概要は表１の通りである。

【表１】「インテリジェンスサイクル」の各フェーズの概要

#	フェーズ	概要
①	計画と指示	自組織に、どのような情報が必要かについて明らかにした上で、収集すべき情報と、その収集方法について検討を行なう。
②	収集	「計画と指示」フェーズで決めた内容を基に、情報の収集を行なう。
③	整理	収集した情報について分析が出来るように、収集した情報の信頼性等を評価した上で、外国語の情報の翻訳や収集した複数の情報の一覧化などを行なう。
④	分析・生産	整理された情報を基に、インテリジェンスを生産する。
⑤	情報提供	生産したインテリジェンスを、インテリジェンスを必要とする関係者に提供する。

（米国国家情報長官室「2009National Intelligence Consumer’s Guide」p.17-19 を参考に筆者が作成）

‡‡) 「Processing」の本来の日本語訳は「加工」であるが、このフェーズで実施する内容に照らして、「整理」の方が趣旨に沿うとの筆者の判断の上、本論文では「整理」として説明する。
§§) 「Dissemination」の本来の日本語訳は「配布」であるが、上記と同じ理由で、本論文では「情報提供」として説明する。

ここで、上記概要の「インテリジェンス」という言葉について解説したい。引用元には「インテリジェンス」という言葉の具体的な定義が存在しないため、筆者の見解となるが、「インテリジェンス」とは前述した「インテリジェンスサイクル」を経て生産されるもの、すなわち収集した情報そのものではなく、収集した情報を基に分析を行い、そこから得た知見を指すものと考えられる。例えば本論文でテーマとしているような、サイバー攻撃に関する動向を調査し、金融業界に対する脅威を特定するという目的で、情報収集・分析を行っているという場合の「インテリジェンス」は、収集した情報を分析した結果として導き出された、金融業界に対する脅威に関する知見のことを指す。

また、これも筆者の見解であるが、インテリジェンスサイクルは「計画と指示」から「情報提供」まで一方向に進むだけではない。例えば「分析・生産」フェーズにて情報を分析した結果、更に必要となる情報が判明する場合や、「情報提供」フェーズにて組織内に情報を提供した後に、追加で情報収集の依頼を受ける場合がある。この際には、再度「収集」のフェーズに戻ることになる。むしろ、一回の情報収集だけで情報の分析や提供が完了するといったことは稀であり、前後のフェーズを何回も繰り返し、より多くの情報を収集して分析結果を更に深めていく、ということが一般的であると考えられる。

以降、本論文では本項で示したインテリジェンスサイクルのプロセスごとに、具体的な手法等について説明する。

3　計画と指示

本項では、収集すべき情報と収集の手段について説明する。

3.1 収集すべき情報について

本論文における収集すべき情報とは、金融業界に対するサイバー攻撃の脅威動向を把握するための情報である。これに関して、筆者は具体的に以下のような情報収集を行なっていた。

- 実際に発生したサイバー攻撃事案に関する詳細情報
- 流行しているサイバー攻撃の手口に関する情報
- システムやソフトウェアの脆弱性に関する情報
- サイバー攻撃を行っている者・組織の動向に関する情報

これらの具体的な内容については、次のとおりである。

3.1.1 実際に発生したサイバー攻撃事案に関する詳細情報

実際に発生したサイバー攻撃事案に関して情報を収集する目的は、同様の事案が自組織に対して発生する可能性の確認や、攻撃の発生に備えた自組織のサイバーセキュリティ態勢の見直しを行うためである。そのため、筆者は国内外問わず、発生したサイバー攻撃について、以下の観点を中心に情報を収集した。

【表２】実際に発生したサイバー攻撃事案に関する詳細情報の収集の観点

＃	情報収集の観点	概要
①	事案のタイムライン	攻撃発生から対応まで一連の事象とそれらの発生日時
②	攻撃によって生じた被害	攻撃を受けた組織や組織の利用者が被った被害（金銭的被害、情報漏えい、サービス停止、顧客からの信頼損失等）
③	攻撃者	攻撃を実施した、あるいは実施したことを疑われている者（軍事的組織、金銭目的の犯罪集団、アノニマス、個人等）
④	攻撃の手口	攻撃に利用されたマルウェア、脆弱性、攻撃ツール、ソーシャルエンジニアリング等
⑤	攻撃が成功した要因	攻撃の成功に関する、被害者側に起因する要素、反省点。（脆弱性の修正パッチ未適用、ゼロデイ脆弱性の利用、セキュリティ機器の未実装、インシデント対応の遅れ等）

まず、「①事案のタイムライン」は、当該攻撃事案を時系列的に整理することで、当該事案における攻撃の特徴や、対応における反省点等を把握することを目的とした情報である。攻撃を受けた組織内のシステムがマルウェアに感染してから、システム内に保存されている機密情報が窃取されるまでに、どのような段階や期間を要して攻撃が行なわれたのか、被害を受けた組織はどのように対応を行なったかなど、当該事案の一連の流れを把握する。

次に、「②攻撃によって生じた被害」は、当該事案にて、攻撃を受けた組織にどのような被害が発生したかを確認するための情報である。これにより、同様の攻撃が成功した場合に、例えば金融機関ではどの程度の被害が発生し得るかを予想する上で必要な情報となる。

「③攻撃者」は、当該攻撃は誰が行なったかに関する情報である。国家機密情報の窃取などを目的とした軍事的組織や、金銭の取得が目的の犯罪集団、自らの主張の公表が目的のアノニマス、サイバー攻撃について学んだ知識を試してみた個人等、様々な可能性がある。この情報を収集する理由は、攻撃者によって攻撃の目的や攻撃手法のレベルが異なるためである。例えば、軍事的組織による攻撃は過去に確認されていないマルウェアや、ゼロデイ脆弱性[***)]を使うなどの高度な攻撃を行なうケースが多い一方、個人による攻撃は、インターネット上にて収集できる知識や攻撃ツールを用いて攻撃するケースが多い。そのため、想定される攻撃者の違い

[***)] パッチが未完成であるなど、対応策が存在していない状況にある脆弱性のこと。

によって、ゼロデイ脆弱性を利用する等の高度な攻撃への対策をすべきなのか、又は既存の攻撃ツールへの対策をしておけばよいのか等、防御する組織側に求められる対策のレベルも異なる。

「④攻撃の手口」は、攻撃に利用された脆弱性や攻撃ツール等の情報である。この情報を基に、例えば金融機関において、攻撃に使われたものと同じ脆弱性が存在しないか、同じ攻撃ツールが利用された場合に、攻撃が成功する可能性がどの程度あるのか、などの観点から分析することが可能となる。

「⑤攻撃が成功した要因」は、当該事案で攻撃が成功した要因に関する情報である。これはいわば、被害を受けた組織における、反省点ともいえる。具体的には、システムやソフトウェアに存在した脆弱性を利用されて攻撃を受けた事例の場合は、パッチが公表されていたにもかかわらず適用が漏れていたのか、ゼロデイ脆弱性を突かれたため、脆弱性そのものに対する対策が困難であったのか等の情報である。

これらの一連の情報を収集することで、当該サイバー攻撃事案の攻撃の特徴や対応における注意点などを把握することができる。特に、「④攻撃の手口」を分析したうえで、「⑤攻撃が成功した要因」の調査を重点的に行なうことで、どのような場合に攻撃が成功するのか、攻撃が発生した場合にどのような態勢であれば対応できるのか、同様の攻撃が金融業界で成功してしまう可能性はどの程度あるのか、等の分析に繋げることができる。なお、通常は「攻撃の手口」や「攻撃が成功した要因」に関する情報の全容について、詳細に把握できるケースは少ない。使用されたマルウェアや利用された脆弱性などの一部の情報しか得られず、例えば感染経路や内通者の有無などに関する詳細な情報については不明なケースもある。そのため、不明な点については、複数の情報を集め、各情報でどのような推察を行なっているかを確認し、また過去に発生した同様の事案の情報なども調査した上で、情報収集者自身で推測するといった行動も必要となる。

筆者が実施した情報収集の例として、2016 年２月にバングラデシュ中央銀行で発生した不正送金事案を用いて説明したい。本事案は、バングラデシュ中央銀行の海外金融機関に対する送金に関するシステム（SWIFT[†††]）の業務を行う端末などがマルウェアに感染し、攻撃者の遠隔操作によって約 8100 万ドルの不正送金が実施され、盗まれたという事案である。攻撃の手口としては、攻撃者があらかじめバングラデシュ中央銀行の PC にマルウェアを感染させ、これを足掛かりに海外金融機関への送金業務を行う PC にも感染を広げ、当該 PC で行われる海外送金業務の手順を把握した。その後、行員が不在の定休日に、攻撃者が自ら用意した口座に対して

[†††] 金融機関同士で国際的に送金を行なう場合に、その送金内容に関するメッセージを送受信するシステムのこと。

通常の手順通りに海外送金を実施し、その後送金を実施したことが発覚しないように、海外送金のシステムに存在した脆弱性を利用して、送金した旨のログを改ざんしたというものである。

本事案については、北朝鮮政府に関連する軍事組織の関与が疑われているところである。この軍事組織は、外貨の獲得目的でサイバー攻撃を行なっているという情報があるため、同様の攻撃はどの金融機関に対しても発生する可能性があったと考えられており、実際にベトナムやフィリピンなどで同様の攻撃が発生していたことも判明している。このように、攻撃者が軍事組織の場合は、既に検知されて分析されているマルウェアを再度使用する、ということは考え難いため、これまでに使われたことのない、新しいマルウェアにて攻撃を受けた場合の対応態勢について検討、見直しを行う必要がある。

攻撃が成功してしまった要因としては、

①海外送金を行うシステムも含めて銀行内のシステムが同じネットワーク内に接続されていたため、マルウェアの感染拡大を許してしまったこと

②海外送金を行うシステムが定休日でも利用できる状態になっていたこと

③攻撃者に正常な送金フローが把握されてしまい、その手順どおりに不正送金が実行されてしまったこと

等が挙げられている。そのため、例えば各金融機関がサイバーセキュリティ態勢の見直しを行う観点として、自組織内の海外送金のシステムと他のシステムとの接続状況や、定休日における海外送金のシステムの稼働状況（その必要性も含め）、利用された脆弱性に対するパッチの適用状況、などといった観点等を整理することができた。

3.1.2 流行しているサイバー攻撃の手口に関する情報

セキュリティベンダーや警察当局等が、増加傾向にある攻撃の手口に関する情報や、サイバー攻撃の発生件数の統計データなどを公表している。具体的には以下のような情報が挙げられる。

- 検知や発生件数が増えている攻撃の手口
- マルウェア感染を狙ったメールの特徴（タイトル、本文の内容等）
- 攻撃を意図した通信元 IP アドレスや通信先ポート等

これらの情報は、実際に攻撃を確認し、対応を行う際において有益な情報となる。例えば、2017 年６月に、不正送金マルウェア‡‡‡)に感染させることを目的に、「請求書」というタイトルのメールが国内の個人や組織を問わず、無差別に送信されるという事象が確認されている。

‡‡‡) 攻撃者が、インターネットバンキングを利用する個人や法人の口座から、不正な送金を行って資金を窃取することを目的に、利用者のインターネットバンキングの ID やパスワードを盗むマルウェア

これについて、独立行政法人情報処理推進機構（以下、「IPA」）等が注意喚起【参考２】を行っていたが、当該注意喚起を把握していたかどうかにより、「請求書」というタイトルの不審なメールを検知した際の対応が変わってくると思われる。もし把握していれば、最近流行している不審なメールであるということを踏まえて対応できるが、把握していない場合は何も事前情報がない中で対応をすることになり、メールの検知時点ではどのような攻撃なのか見当がつかず、対応に時間がかかるおそれがある。そのため、インシデント対応を迅速に行なうためにも、流行しているサイバー攻撃の手口に関する情報収集は必要であると考えられる。

【参考２】流行しているサイバー攻撃手口に関する情報の例

（IPA の Web サイトより引用
引用元：https://www.ipa.go.jp/security/topics/alert271009.html）

なお、注意点としては、同じ組織から様々な攻撃に関する情報が公表されており、情報収集時には個々の情報について、分析対象として取り上げるか否かを判断する必要があるということである。例えば、IPA のような公的機関が公表している不審なメールに関する注意喚起については、上記のような不正送金マルウェアへの感染目的のメール以外に、標的型攻撃やランサムウェアへの感染などを目的としたメールに関する情報も公表されている。これらの注意喚起は、全て同様なトーンで公表されるケースが多い。そのため、一見全ての情報について、金融

業界への脅威として分析や対応を行なう必要があると思いがちだが、これは情報収集の目的によって異なる。金融機関自身に対する攻撃の脅威動向を把握するという目的に照らすと、標的型攻撃やランサムウェアに関する情報について優先的に収集や分析を行なうべきと考えることもできる。このように、情報が示す脅威の特性に応じて、分析や情報提供の対象とするか、逐一判断することが必要である。

3.1.3 システムやソフトウェアの脆弱性に関する情報

システムやソフトウェア等における脆弱性は、様々な形で公表される。例えば、提供元のシステムベンダーや、JPCERT/CC をはじめとした公的機関等が公表している。このほか、サイバーセキュリティの研究者が自らのブログやイベントでの講演にて未公表の脆弱性を公表する場合や、ダークウェブ§§§)上で未公表の脆弱性の売買****)が発見されたことをきっかけに公表される場合もある。

脆弱性については、例えば攻撃者にシステムの管理者権限を奪われ、不正に操作されるなどの攻撃を受ける原因になる可能性があるため、特に金融業界にて利用されている可能性が高いソフトウェアやシステム等に関わる脆弱性について、注意して情報を収集している。具体的には以下のような情報である。

【表３】脆弱性に関する情報の収集の観点（例）

#	情報収集の観点	概要
①	当該脆弱性の内容	脆弱性がもたらす影響、対象となるシステム・ソフトウェアのバージョン、CVSSにおける評価等
②	当該脆弱性への対策の有無	修正パッチやアップデートファイルの公開状況 一時的な回避策（特定のポートを閉じる等）の有無　等
③	当該脆弱性を利用する攻撃ツールの公開の有無	インターネット上のフォーラムやダークウェブにおける、当該脆弱性を利用する攻撃ツールや攻撃手法の公開や取引の有無
④	当該脆弱性を利用した攻撃の発生状況	国内外における、当該脆弱性を利用した攻撃の発生有無、被害状況等

まずは、「①該脆弱性の内容」として、当該脆弱性はどのような悪影響をもたらす脆弱性なのか、また対象となるシステムやソフトウェアのバージョンは何か、といった内容について確認する。また、IPA などの公的機関においては、脆弱性の内容等とともに、CVSS（Common Vulnerability Scoring System）と呼ばれる脆弱性の深刻度を評価する指標値を公表している。CVSS では、以下の３つの評価基準【表４】によって、脆弱性の評価を行なっている。

§§§)利用者の発信元を隠すソフト「Ｔｏｒ（トーア）」などを使わないと接続できないインターネットサイトの総称。違法薬物やサイバー攻撃ツールなどが売買されているサイトも存在。
****) 未公開の脆弱性を攻撃で利用したいとのニーズが存在しており、売買がされているケースがある模様。

【表４】CVSS における脆弱性の評価基準

CVSSの評価基準	説明
基本評価基準	脆弱性そのものの特性について、「機密性」、「完全性」、「可用性」に対する影響及び、ネットワークから攻撃可能かという基準で評価。
現状評価基準	脆弱性の現在の深刻度について、攻撃コードの出現有無や対策情報が利用可能であるかといった基準で評価。
環境評価基準	最終的な脆弱性の深刻度について、攻撃を受けた場合の二次的な被害の大きさや、組織での対象製品の使用状況といった基準で評価

（IPA のサイトを参考に筆者が作成）

CVSS の評価結果として、「基本評価基準」による評価の結果（基本値）が公表される【参考３】ことが多い。「基本評価基準」における評価結果において、筆者は特に、脆弱性を悪用した攻撃はどこから実行することが可能かを示す「攻撃元区分」（ローカル環境内からのみ可能なのか、ネットワーク経由でリモートから可能なのか）という観点に着目した。特にリモートから攻撃可能な場合は、あらかじめ攻撃対象の組織のネットワーク内に侵入するといったことは不要となり、インターネット上の IP アドレスや URL を指定するだけで、システムを直接攻撃することが可能となる。この場合、攻撃を実行する難易度が下がるため、攻撃が発生する可能性が高く、注意が必要となる。

【参考３】IPA による脆弱性情報の公表ページの例

JVNDB-2016-004926

ISC BIND 9 にサービス運用妨害 (DoS) の脆弱性

概要

ISC BIND 9 には、サービス運用妨害 (DoS) の脆弱性が存在します。

ISC BIND 9 には、レスポンスパケットの生成処理に起因するサービス運用妨害 (DoS) の脆弱性が存在します。
特定の条件に一致するクエリに対するレスポンスパケットの生成処理に問題があり、buffer.c で例外が発生し、named が異常終了します。
この問題は、クエリの送信元アドレスが許可されていなくても発生します。

CVSS による深刻度 (CVSS とは?)

基本値: 7.8 (危険) [NVD値]

- 攻撃元区分: ネットワーク
- 攻撃条件の複雑さ: 低
- 攻撃前の認証要否: 不要
- 機密性への影響(C): なし
- 完全性への影響(I): なし
- 可用性への影響(A): 全面的

（脆弱性対策情報データベース（JVN IPedia）より引用

引用元：http://jvndb.jvn.jp/ja/contents/2016/JVNDB-2016-004926.html）

なお、「基本評価基準」による評価値の高低のみが、そのまま各組織に対するリスクの高低に直結するものではないことに注意する必要がある。例えば、金融業界への具体的なリスク等について判断する際には、当該脆弱性が発見されたシステムやソフトウェアの、金融業界における利用状況や、攻撃ツールの公表有無、攻撃が発生した場合に予想される被害等、「現状評価基準」や「環境評価基準」に関する観点も必要である。そのため、以下で説明するような情報も収集を行なう。

「②当該脆弱性への対応策の有無」であるが、例えば脆弱性を修正するパッチの有無を確認することが挙げられる。ただし、パッチが公表されている場合においても、例えば組織内の重要なシステムにかかわる脆弱性であり、業務に対する影響などを考慮した結果、即日のパッチの適用が難しい場合もある。その場合には、一時的な代替策なども公表されている場合があるため、このような情報も収集し、最終的には自組織の状況に鑑みて、適切な対策をどのような順序で対応するか検討する必要がある。

「③当該脆弱性を利用する攻撃ツールの公開の有無」については、サイバーセキュリティの研究者などが利用するインターネット上のフォーラムの中には、公開された脆弱性への攻撃方法や攻撃ツールに関する情報を交換するサイトがあり、このようなサイトで確認を行なう。サイト上で攻撃手法や攻撃ツールが公開された場合、誰でも攻撃を行うことが可能となるため、すぐにその脆弱性を利用した攻撃が発生する可能性が高い。例えば、2017 年２月に公開された WordPress（ワードプレス）の脆弱性が公表された際のケースについて紹介する。WordPress とは、Web サイトの作成や運用のためのソフトウェアであり、CMS（コンテンツマネジメントシステム）と呼ばれる。本ケースでは、当該ソフトウェアにおいて、Web サイトのコンテンツの改ざんが可能な脆弱性が発見された。この事案で特徴的なのは、脆弱性の公表翌日には、当該脆弱性を利用する攻撃ツール【参考４】が公開されたことである。この結果、脆弱性の公開翌日に当該脆弱性を利用した攻撃の発生が確認され、その後 1 週間ほどで、全世界で約 155 万サイトが改ざんされたと報道されている。日本国内においても、中小企業や地方公共団体、医療機関等の Web サイトに対して攻撃が発生した。このように、攻撃ツールが公開されたタイミングで攻撃が開始される場合もあるため、攻撃ツールの公開に関する情報収集、及び「④当該脆弱性を利用した攻撃の発生状況」の収集も必要である。

【参考４】攻撃ツールが公開されている Web ページの例

3.1.4 サイバー攻撃を行っている者や組織に関する動向

本節では継続的にサイバー攻撃を行っている者や組織に関する動向の情報収集について説明する。このような情報を収集する目的は、「3.1.1 実際に派生したサイバー攻撃事案に関する詳細情報」の節でも説明したとおり、想定される攻撃者によって、実施すべき対策の内容が変わるためである。具体的には以下のような情報が挙げられる。

【表５】サイバー攻撃を行なっている者や組織に関する動向の収集の観点

＃	情報収集の観点	概要
①	攻撃者のプロフィール	攻撃者の国籍や背景（軍事的組織、ハッカー集団、個人等）
②	攻撃の目的と標的	攻撃の目的：金銭、情報窃取、自らの主張の公表等 攻撃の標的：特定の国の組織、金融業界、特定の個人等
③	攻撃手法	DDoS攻撃、標的型攻撃などの攻撃の種類、及び使用するマルウェアや攻撃ツール等

まず、「①攻撃者や組織のプロフィール」については、どのような背景を持った攻撃者なのか、具体的には、攻撃者の国籍や、攻撃者は軍事的組織なのか、あるいは個人なのか、等の情報となる。

次に、「②攻撃の目的と標的」については、攻撃の目的と標的となる個人や組織についての情報を指す。例えば、「Anonumous（アノニマス：匿名の意）」と自らを呼称している攻撃者の中には、日本の捕鯨活動への抗議運動など、自らの主張を世の中に表明するためにサイバー攻撃を実施するといった目的を持った者がいる。実際に、日本の捕鯨活動に対する抗議活動を目的に行なわれているサイバー攻撃（通称「OpKillingBay（オペレーションキリングベイ）」）では、捕鯨活動を行っている地域の地方公共団体や鯨肉を販売する企業等を攻撃の標的としていた。なお、「OpKillingBay」については、攻撃者のパーソナリティについては不明であり、かつ攻撃を行なう人物は複数存在するものの、組織だって活動しているような様子は見られない。また、この活動自体は数年間にわたって継続的に実施されているが、攻撃者については同一の人物や組織が継続的に実施しているのではなく、前年とは異なる人物が実施している場合がある、という特徴がある。

「③攻撃手法」については、例えば標的型攻撃によって情報の窃取を行う、DDoS 攻撃により Web サイトをダウンさせる等、具体的な攻撃手法に関する情報を指す。特に金融機関を標的としていると思われる攻撃者に対しては、その攻撃手法に関する情報を集め、金融業界に対して攻撃が発生した場合を想定し、注意すべきポイントの洗い出しに役立てることができる。

3.2 情報収集の方法について

情報収集の方法についてであるが、本論文では主に、公開情報から情報収集・分析を行うオシント（OSINT）と呼ばれる手法[††††)]について紹介する。オシントは新聞や雑誌、インターネット等、一般に公開されている情報を収集・分析する手法であり、冒頭にも述べた通り世界各国の情報機関の活動の 80%以上を占めると言われるほど、有効な方法である。この手法のメリットとして、公開情報という誰もがアクセス出来る情報を収集するため、他の方法と比較して容易であり、かつコストも低い。一方デメリットとして、情報が膨大に存在するため収集した情報の取捨選択が難しいという点や、また公開されていない秘匿性の高い情報について収集することが困難であるという点が挙げられる。

本論文では、公開情報の中でもインターネット上で公開されている情報について取り上げたい。その理由としては、情報が公表されるスピードについて、テレビや新聞等の他の媒体と比べ、インターネットが一番早いためである。これは、テレビや新聞などから情報を収集することを否定しているわけではない。1 つの事案について網羅的かつ体系的に整理された情報を入手したい場合は、テレビや新聞などの方が相応しいことが多いと思われる。しかし、サイバー攻撃に対する脅威動向を調べるにあたり、攻撃の発生や脆弱性の公表等のイベントが生じた際に、どれだけ迅速に情報を収集し、対応できるかということは重視しておくべき要素である。この点について、2017 年５月に発生したランサムウェア「WannaCry（ワナクライ）」の事案を例に説明する。この事案は、日本時間 2017 年５月 13 日（土）未明より、イギリスをはじめとした複数の国々で、WindowsOS の PC やサーバがランサムウェア「WannaCry」に感染するという事案が発生した。この感染が初めに確認されたのが日本時間５月 13 日(金)の深夜であったが、被害状況や「WannaCry」の概要について、14 日（土）の午前中には海外の情報ソースや国内のセキュリティベンダー等がインターネット上で情報を公開していた。一方で、テレビや新聞での報道は、14 日（土）の夕方以降であった【表６】。このように、インターネット上での情報収集と、テレビや新聞などの媒体での情報収集では、情報が公開されるスピードが変わってくるのである。

†††††) なお、情報収集の手法としては、他にも人間と直接会話する中で情報収集を行うヒューミント(HUMINT)、衛星写真などの画像から情報収集を行うイマジント（IMAGINT）、通信や電子信号を傍受して情報収集を行うシギント（SIGINT）など複数の手法がある。

【表６】「WannaCry」事案における、各メディア媒体の報道タイミング

日時（日本時間）		各媒体での情報の公表状況
2017/5/12（金）	深夜	・欧州を中心に「WannaCry」の感染が確認。 ・海外メディアやベンダーが、インターネット等で情報を公開。
2017/5/13（土）	午前中	・インターネット上にて日本語の情報が公開。 ・以降、海外の動向やセキュリティベンダーの分析に関する情報が、随時更新される。
	夕方	・新聞社各社が夕刊で報道。
2017/5/14（日）	午前中	・新聞社各社が朝刊で報道。
	夕方	・各テレビ局がニュース等で報道。

（筆者が収集した情報を基に作成。インターネット上の情報は、公開のスピードが最も早く、かつ随時最新情報に更新された。）

「3.1.3 脆弱性に関する情報」の節でも説明した通り、脆弱性の公表の翌日に攻撃が発生する場合がある状況で、新聞やテレビだけに情報収集を頼っていては、攻撃の発生までに自組織の対応が間に合わないケースもあり得る。そのため、サイバー攻撃の動向については、速報性の高いインターネットからの情報収集を取り入れるべきである。

4　収集

本項では、筆者が実際に行っている、インターネット上の公表情報の収集において、情報の収集源ごとに手法を解説する。情報収集の手法として、筆者は「Web サイトからの情報収集」と「SNS からの情報収集」を実施しており、本項ではこの２点について説明を行なう。

なお、情報を収集する際には、日本語で書かれた情報だけに頼りすぎず、海外の情報も積極的に収集する必要がある。これは、例えば海外で発生したサイバー攻撃や、日本時間の深夜・早朝・休日に、日本を含んだ複数の国々で発生したサイバー攻撃の場合には、海外の情報源による情報の公表の方が早い。また、外国語で書かれた情報を日本語に翻訳して公表している情報の場合、特定の部分のみ切り出されて翻訳されている場合や、誤訳が存在する場合がある。このような場合、元の情報の内容を正確に読み取れない可能性が高い。これらの理由から、積極的に外国語の情報を収集することが必要である。

4.1Web サイトからの情報収集

まず、Web サイトからの情報収集について説明する。一次情報と二次情報に分けると、筆者はそれぞれ、以下のような情報ソースから情報収集を行なった。

【一次情報】

- セキュリティベンダーの公表情報
- ソフトウェアやシステムを製造するベンダーの公表情報
- サイバー攻撃を受けた当事者が公表する情報
- サイバーセキュリティに関するフォーラム等で共有される情報
- 政府機関や公的機関が公表する情報　等

【二次情報】

- ニュースメディア等の Web サイト
- サイバーセキュリティの専門家や研究者が情報を収集し、まとめている Web サイト

ここで、一次情報と二次情報に区別した理由は、二次情報だけでは一次情報の内容を正確に把握することが難しいケースもあり、二次情報から情報を得た場合にはその情報源である一次情報の確認が必要となるためである。例えば、二次情報では一次情報の特定の部分のみを切り出してまとめられている場合や、先ほど説明したとおり、一次情報と二次情報で言語が異なる場合（例えば英語が一次情報である内容を、日本語に翻訳して二次情報として公表する場合など）に、誤訳等が発生する場合がある。そのため、収集した情報が一次情報か二次情報かを区別し、二次情報の場合は、必ずその一次情報を確認する必要がある。

また、公的機関等が攻撃手口や脆弱性に関する注意喚起等を公表する際に、その組織が参照した情報（攻撃手口を分析した結果や脆弱性の詳細に関する情報等が掲載されている Web サイト）が、併せて公表される【参考５】場合がある。このような場合は、情報の参照元として記載されている情報も確認する必要がある。

【参考５】公表された情報の参照元が示されるケース

更新：Apache Struts2 の脆弱性対策について(CVE-2017-5638)(S2-045)(S2-046)

最終更新日：2017年3月31日

※追記すべき情報がある場合には、その都度このページを更新する予定です。

概要

Apache Software Foundation が提供する Apache Struts は、Java のウェブアプリケーションを作成するためのソフトウェアフレームワークです。

参考情報

公式情報

- S2-045
  https://struts.apache.org/docs/s2-045.html
- S2-046
  https://struts.apache.org/docs/s2-046.html
- Security Bulletins S2-045
  https://cwiki.apache.org/confluence/display/WW/S2-045

検証報告

- Apache Struts 2 の脆弱性 (S2-045) に関する注意喚起
  https://www.jpcert.or.jp/at/2017/at170009.html
- CVE-2017-5638 - 脆弱性調査レポート
  https://www.softbanktech.jp/information/2017/20170308-01/
- TrendLabs Security Intelligence BlogCVE-2017-5638: Apache Struts 2 Vulnerability Leads to Remote Code Execution - TrendLabs Security Intelligence Blog
  http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-5638-apache-struts-vulnerability-remote-code-execution/

（IPA ホームページより引用

引用元：https://www.ipa.go.jp/security/ciadr/vul/20170308-struts.html）

4.1.1 セキュリティベンダーが公表する情報

セキュリティベンダーは、主に自社のブログ等で、実際に発生したサイバー攻撃事例の解説や注意喚起を行っている。個々の攻撃において用いられた脆弱性や攻撃手法（マルウェアに感染させることを目的としたメールや、脆弱性を利用した攻撃の最初に○番ポートへの通信が行われるといった具体例）等が示されており、同時に具体的な対策が説明されていることが多い。このため、攻撃事例を理解するための情報とともに、攻撃への対策を行うにあたって参考になる情報が多い。一方、注意点としては、セキュリティベンダーによって公表する情報の内容が異なっている場合がある。そのため、１つの事象に対して、可能であれば複数のセキュリティベンダーの情報を収集し、比較すべきである。例として、2017 年６月に世界各国で感染が確認されたランサムウェア「Petya（ペトヤ）」の事案を説明する。本事案は、ウクライナやロシアを発端に、世界各国の PC やサーバがランサムウェア「Petya」に感染したというものある。本

事案について、セキュリティベンダー各社は、感染が最初に観測された翌日には 攻撃手口に関する記事を、各社のブログに掲載していた。ところが、感染のルートについて、セキュリティベンダーA 社のブログ記事では「不審なメールの添付ファイルを開封したことによる感染」旨を記載していた一方、セキュリティベンダーB 社のブログ記事では「ある会計ソフトのアップデートファイルに「Petya」が不正に組み込まれている」としていた‡‡‡‡)。このように、同じ事案においても、セキュリティベンダーによって公表する情報の内容が異なる場合がある。「Petya」の事案のように、世界中で同じランサムウェアへの感染が大量に確認されるといった、影響範囲が大きな事案等においては、一刻も早く情報を公表することが重視されるため、公表される情報について十分な検証がされていない可能性がある。従って、世界中で流行しているサイバー攻撃事案については、複数のセキュリティベンダーが分析記事【参考６】を公表することが多いため、可能な限り複数の情報源から情報を入手すべきである。また、セキュリティベンダーが十分な検証後に、公表している情報を更新する可能性がある。そのため、同じ情報ソースについて、時間を置いて複数回確認することも必要となる。

‡‡‡‡) 本事案では、結果的にはメールの添付ファイルによる感染は確認されず、B 社の情報が正しかった模様。しかし、当該事案の発覚当初、公的機関でも、感染原因の可能性の１つとして、「メールからの感染」について注意喚起を実施していた組織も存在し、混乱を広げてしまったという事象も発生した。そのため、公的機関の情報も一次情報の１つである、という認識を持ち、複数の情報源から情報を収集する、ということに留意する必要がある。

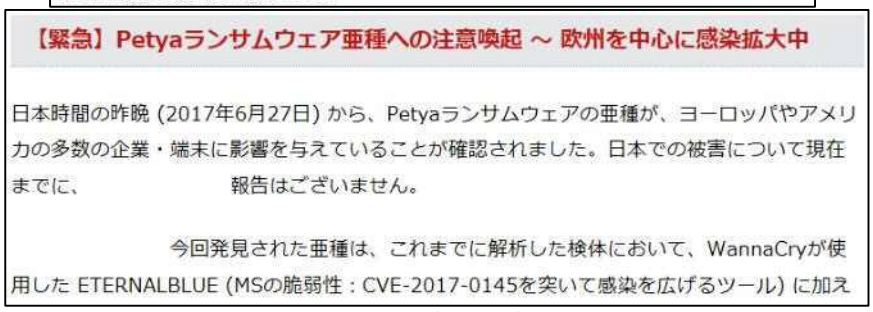
【参考６】セキュリティベンダーが公表する情報の例

（どちらも「Petya」による攻撃に関する分析記事を公表。なお、本文中に事例として出したセキュリティベンダーではない。）

大規模な暗号化型ランサムウェア攻撃が欧州で進行中、被害甚大

投稿日: 2017年6月28日
脅威カテゴリ: 不正プログラム, サイバー犯罪

暗号化型ランサムウェア「PETYA（ペトヤまたはペチャ）」の亜種による大規模な攻撃が、欧州を中心に確認されています。　この亜種が、攻撃経路において脆弱性攻撃ツール「EternalBlue」と「PsExec」の両方を利用することを確認するとともに、「RANSOM_PETYA.TH627」、「RANSOM_PETYA.SMA」などとして既に検出対応しています。法人および個人の皆さんは、下記の対策を取り、感染拡大を防ぐようお願いします。



【緊急】Petyaランサムウェア亜種への注意喚起 ～ 欧州を中心に感染拡大中

日本時間の昨晩 (2017年6月27日) から、Petyaランサムウェアの亜種が、ヨーロッパやアメリカの多数の企業・端末に影響を与えていることが確認されました。日本での被害について現在までに、　報告はございません。

今回発見された亜種は、これまでに解析した検体において、WannaCryが使用した ETERNALBLUE (MSの脆弱性：CVE-2017-0145を突いて感染を広げるツール) に加え

（セキュリティベンダーのブログ記事より引用）

4.1.2 システムやソフトウェアを製造するベンダーの公表情報

システムやソフトウェアを製造するベンダーは、主にそれぞれのベンダーが販売や配布している製品のアップデート情報や脆弱性情報について公表を行っている。特にアップデート情報については、未公表の脆弱性を修正する内容である可能性もあるため、自組織で利用している製品のベンダーが公表する情報については、注意して情報を収集する必要がある。

例えば、ランサムウェア「WannaCry」の事案では、Windows の機能である SMB[§§§§)]の脆弱性を利用して感染を広げる機能を持っていた。しかし、「WannaCry」にて利用されている脆弱性については、同年３月にマイクロソフト社が公表し、提供しているアップデートファイル【参考７】を適用すれば、解消できるものであった。しかしながら、アップデートファイルを適用していなかった PC やサーバが相当数存在していたことも一因となり、世界 150 か国、20 万台以上の PC やサーバに感染が広がってしまったといわれている。

§§§§) 複数の端末でプリンタやファイルサーバを共有するための機能。

【参考７】2017 年３月にマイクロソフト株式会社が公表したアップデート情報

（日本マイクロソフト株式会社ホームページより引用

引用元：https://technet.microsoft.com/ja-jp/library/security/ms17-010.aspx）

注）2017 年３月に公表された更新プログラムで「MS17-010」の脆弱性を解消していれば、ランサムウェア「WannaCry」には感染しない模様。

4.1.3 被害が発生した組織が公表している情報

サイバー攻撃事案について情報収集を行う際には、実際にサイバー攻撃を受け、被害が発生している組織が公表している情報を確認することも有用である。これにより、発生した攻撃の攻撃手口や被害状況等について、正確な情報を把握することができる。また、組織によっては自組織が受けたサイバー攻撃について、「3.1.1 実際に発生したサイバー攻撃事案に関する詳細情報」で説明した、自組織の対応も含めた攻撃全体のタイムラインや、攻撃手法、攻撃が成功してしまった要因等の情報を具体的に公表している場合がある。これらの情報を教訓に、自組織の態勢の見直しに活用することができる。

4.1.4 サイバーセキュリティに関するフォーラム等で共有される情報

「3.1.3 脆弱性に関する情報」の節でも説明したとおり、脆弱性の攻撃手法や攻撃ツールなどについて情報を公開しているサイトが存在する。そのため、特に影響範囲が広いと思われる脆弱性が公表された場合には、即座に攻撃が発生する可能性を分析するため、このようなサイトで攻撃手法や攻撃ツールが公開されているかについても確認を行うことも有効である。攻撃手法や攻撃ツールが公開されている場合には、実際に攻撃が発生する可能性が高い。

4.1.5 政府機関等の公的機関が公表する情報

政府機関等の公的機関では、流行しているサイバー攻撃手口や、多くの組織に影響が及ぶ可能性のある脆弱性などについて注意喚起を公表している。国内では、「3.計画と指示」の項で例としてあげた IPA のサイトの他にも、JPCERT/CC や警察庁などの機関が注意喚起情報などを公表している。海外においても、US-CERT や CERT-EU など、各国の CERT 等の組織が、同様の情報を公表している。

【参考８】韓国インターネット振興院（KISA）と KrCERT による、DDoS 攻撃への注意喚起情報

（KeCERT の Web サイトより引用　引用元：
https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=25964）

※上記の情報は、「Armada Collective（アルマダ・コレクティブ）」という攻撃グループによる DDoS 攻撃が増加していることに対する注意喚起情報。同じタイミングで日本の企業にも同様の事案が発生しており、JPCERT/CC が注意喚起を公表*****）している。

4.1.6 ニュースメディア等の Web サイト

ニュースメディア等の Web サイトは、新聞社等の Web サイトやサイバーセキュリティを専門している Web サイトまで、多種多様なサイトが存在する。これらの Web サイトでは、サイバー攻撃事案や重大な脆弱性等、上記の「一次情報」 で紹介した情報について、複数の情報を整理し、要点をまとめた形で公表している場合が多い。また、サイバー攻撃の手口や脆弱性に関する情報について、関連する技術的な要素を噛み砕いて、理解しやすい解説を行なっているサイトも見受けられる。そのため、情報を収集したい事案等について、速やかに概要を把握したい場合や、関連する技術的な要素に関する情報も併せて収集したい場合などに有益である。

*****） https://www.jpcert.or.jp/newsflash/2017062901.html

4.1.7 サイバーセキュリティの専門家や研究者が情報収集し、まとめている Web サイト

サイバー攻撃事案などについて、ニュースメディアだけではなく、専門家や研究者が、公表されている情報を個人的に収集し、整理した上で公表している Web サイトが存在する。このようなサイトも、短時間で事案の概要の把握ができ、かつ情報収集活動において収集できていなかった情報を補完できるといった点で有益であるといえる。ただし、このようなサイトについては、あくまで個人が運営しているものであり、途中で情報の更新されなくなる場合もある。そのため、特に事案の発生から時間が経っている場合などにおいては、特に、最新の情報を他の情報源などとあわせて調べることも必要である。

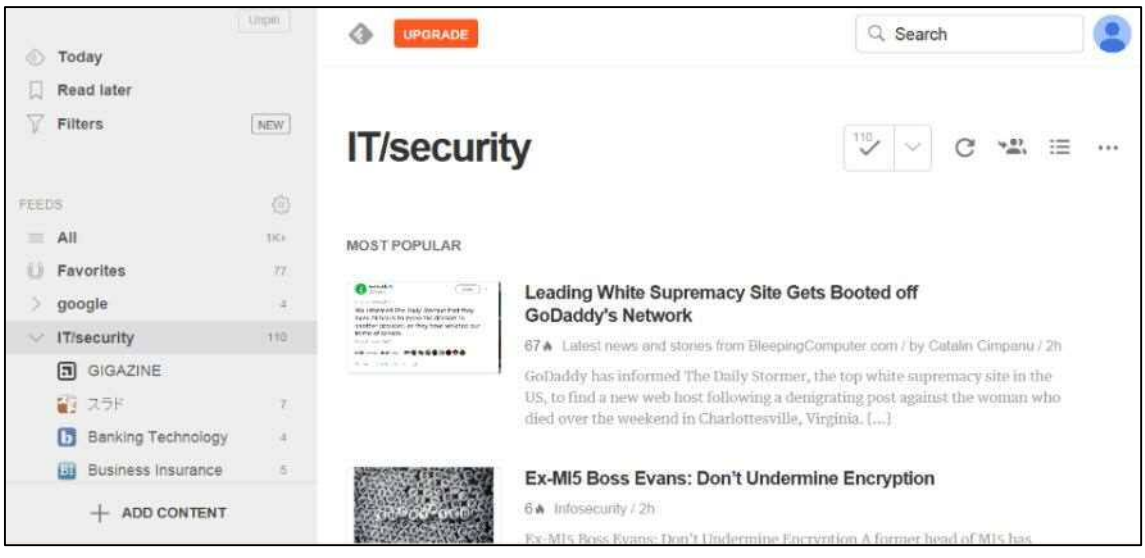
4.1.8 インターネット上の公表情報を効率的に収集するツール

ここで、Web サイト上で公表される情報を収集する際に、筆者が特に有用であると考えているツールを紹介する。

・Feedly

情報収集のために、個々の Web サイトを巡回し、更新情報を確認するのは非効率的である。筆者は様々な Web サイトの更新情報を効率的に確認するために、Feedly という RSS 情報収集ツールを使っている。RSS 情報収集ツールとは事前に登録しておいた Web サイトの更新情報を収集するツールのことである。本ツールを使うことで、画面上に情報収集の対象となる Web サイトの更新情報【参考９】がまとめて表示されるため、短時間で効率よく情報収集を行なうことが可能である。

【参考９】Feedly の画面イメージ（画像は筆者が利用している画面）



・Google アラート

例えば、「DDoS 攻撃」等の攻撃手法や「アノニマス」といった攻撃者の名称など、特定のキーワードに関する情報を幅広く収集したい場合がある。この際、筆者は「Google アラート」というサービスを利用している。これは、特定のキーワードを登録すると、インターネット上に公開されている情報を Google の検索機能を用いて日次で自動的に検索し、キーワードに関する情報が収集されるサービスである。普段は、「サイバー攻撃」、「cyber attack」等のキーワードで情報収集をしているほか、特定のマルウェアや攻撃手法（例えばマルウェア「Mirai」）が流行している場合には、それらをキーワードに登録し、情報を幅広く収集している。

4.2 SNS からの情報収集

次に、SNS からの情報収集について説明する。筆者は、主にツイッターやフェイスブックを用いて、以下のような情報を収集した。

- サイバー攻撃を行なう者、組織が投稿する情報
- サイバーセキュリティの専門家や研究者が投稿する情報　等

4.2.1 サイバー攻撃を行う者、組織が投稿する情報

サイバー攻撃者や組織によっては、SNS 等でサイバー攻撃の予告や犯行声明を投稿する場合がある。例えば、サイバー攻撃によって自身の主張を世の中に公表しようとする、アノニマスを称する者たちである。

アノニマスは、ツイッター上で自身の主張を表明する投稿や、自身がサイバー攻撃を行なった旨を投稿している。このほか、フェイスブックを使って、抗議活動の告知やサイバー攻撃への参加者を募集する†††††)ケースがある。一例として、OpIcarus（オペレーションイカロス）と名づけられた活動においては、フェイスブック上で攻撃対象の組織のリストとして世界各国の中央銀行等を記したリストを投稿した上で、サイバー攻撃に参加する者を募集していた。筆者は、ツイッターを使った情報収集の中で、フェイスブック上でこのようなページが作成されているとの情報を確認した。そして、実際にフェイスブック上の該当ページにアクセスすることで、攻撃の動向を把握している。

†††††) フェイスブック利用者に対する、イベントの告知と参加者を募集する機能を使い、「○月×日から抗議活動を実施する」旨やサイバー攻撃への参加者の募集、標的のリストや攻撃ツールの共有等が行なわれるケースがある。

【参考 10】アノニマスによるサイバー攻撃予告の投稿の例

（フェイスブックより引用）

4.2.2 サイバーセキュリティの専門家や研究者が投稿する情報

筆者は主にツイッターを活用し、サイバーセキュリティの専門家や研究者が投稿する情報を収集している。このような情報としては、例えば専門家や研究者が収集した公表情報等について、意見や分析を付与した投稿等が挙げられる。これらの情報を収集することで、自身の分析の参考になるほか、自身が収集できていなかった情報を補完することができる。特に、Web サイトの更新情報を日々確認することが難しいという場合には、著名な研究者や専門家の方が SNS 上で投稿している情報を確認するだけでも、有益な情報収集活動の一助になると思われる。

5　整理

本項では、収集した情報の真偽や信頼性に関する評価の方法、及び収集した複数の情報をまとめ、情報が示す内容を整理、把握する方法について説明する。この作業を通して、得られた情報が示す脅威動向を理解した上で、次フェーズの分析作業を行なう。

5.1 その情報の真偽、信頼性に関する評価

まず、収集した情報の内容の真偽や信頼性に関して評価を行う。重要な点としては、明らかに誤った情報は分析の対象から除外するとともに、個々の情報の信頼性を評価することにある。例えば、「4.1.1 セキュリティベンダーが公表する情報」で例に挙げた「Petya」の事案の際は、事案が発生した直後はセキュリティベンダー側での分析も進行中であり、セキュリティベンダーによっては見解が分かれていた内容も存在した。そのため、各ベンダーが公表している情報を比較するなどして、個々の情報の信頼性について検討、判断を行った。

具体的に筆者は、以下の観点から評価を行った。

① 一次情報や複数の情報ソースとの比較

「収集」でも述べた通り、二次情報については、その内容の真偽を必ず一次情報に照らして確認を行うことが必要である。誤訳や一部の内容だけが切り取られ、正確な情報が把握しにくい可能性があるためである。また、一次情報を収集した場合においても、同様の情報について複数の情報源が公表しているのであれば、可能な限り複数の情報を収集して比較し、情報の信頼性を検証することが必要となる。

② 情報源（情報の出し手、収集元）

例えば、大手セキュリティベンダーのブログや、新聞社等のマスメディアのサイトであれば、情報源として、信頼できると考えられる。しかし、SNS 上にてサイバー攻撃を行っている旨の投稿をしている人物が発信する情報の場合は、直ちに信頼性を持って分析することは困難であると思われる。例えば、筆者はツイッター上で、ある組織のサイトに DDoS 攻撃を実施し、サイトをダウンさせたという投稿を見つけたため、そのサイトに実際にアクセスしてみたが、支障なくサイトを閲覧することができたことがあった。「4.収集」の項でも説明したように、インターネット上においては多種多様な情報源が存在する。すべての情報源を信頼するのではなく、中には不確かな情報源があることを認識しておくべきである。

5.2 情報が示す脅威動向の整理、理解

情報の信頼性を評価した後、筆者は以下の観点で情報を整理した。

① 攻撃を行う目的は何か

② どのような組織が狙われているのか

③ どのような攻撃が想定されるか

④ どのような組織が攻撃を行っているのか/行うことが予想されるか

⑤ 攻撃が発生した場合に、どのような影響が起こりうるか

これらの観点から情報を整理したうえで、予想されるサイバー攻撃の全体像を把握する。特に、「①攻撃を行う目的」は重要な観点である。攻撃の目的がいたずらなのか、金銭なのか、機密情報の収集なのかを明らかにすることで、金融業界が狙われる可能性がどの程度あるのか、攻撃を受けた場合にとるべき対応は何かを検討する際に、有益な情報となる。

収集した複数の情報を、上記に示した観点で整理すると、情報源によっては、他の情報源とは異なる情報を公表している場合もある。その場合には、即座に片方を切り捨てようとせず、双方の情報について信頼性を評価しつつ、可能性がある情報として残しておく方が良い。

なお、情報を整理した結果については、発生した事象を時系列に並べたタイムラインの作成や、攻撃の全容などについて１枚の絵を作成するなど、１つの表や絵でまとめておくことが望ましい。これは、自身が分析を行なう際だけでなく、収集・分析した情報を関係者に提供する際に、事案の全体像の説明において有用な資料となるためである。

また、情報を理解するにあたり、その情報で使われている単語や、対象となるシステムの概要等については、事前に把握しておく必要がある。例えば、DNS サーバに関する脆弱性について分析するのであれば、 DNS サーバについての知見がないと、その脆弱性が及ぼしうるリスクや影響が理解できない。そのため、可能であれば自身で実際に手を動かし、サーバを構築するなどの経験を通じて、そのシステムやソフトウェアについて学習することが有益である‡‡‡‡‡) と思われる。実際に自身で手を動かし、システムを操作してみることで、より具体的なイメージを自分の中に作ることができる。これにより、例えば公表された脆弱性について、どの程度脅威になり得るか、攻撃された場合の被害はどの程度か、などについて、正確かつ即座に把握することができる。情報の正確な理解のためにも、自身で手を動かす経験も重要である。

6　分析・生産

本項では、収集し、整理された情報を分析し、サイバー攻撃の脅威動向を評価する方法について説明する。筆者は、収集した情報がどの程度日本の金融業界への脅威になり得るのか、具体的に以下の観点から分析している。

- 標的として日本の金融機関が狙われる可能性があるか
- 日本の金融業界に対して、攻撃が成功する可能性があるか
- 対応策はどうすべきか

‡‡‡‡‡) 手を動かしてシステムやソフトウェアについて学習することの有効性については、補足情報②も参照。

6.1 標的として日本の金融機関が狙われる可能性があるか

「標的として日本の金融機関が狙われる可能性があるか」については、攻撃の目的や、過去及び現在における日本の金融機関に対する同様の攻撃の発生状況等の情報をもとに分析している。例えば、アノニマスによる「OpIcarus（オペレーションイカロス）」では、世界各国の中央銀行を中心に DDoS 攻撃を行う旨の予告があり、事前に公開されたターゲットリストに掲載された組織名も同様であった。更に、この事例では、日本国内の民間金融機関がターゲットリストに掲載されておらず、かつ過去の同様な事案で実際に攻撃の対象となっていた組織はターゲットリストに忠実であった。そのため、この活動によって日本国内の民間金融機関に攻撃が発生する可能性は少ないと判断した。また、2016 年に米国において「NoDAPL（ノーダコタアクセスパイプライン）」と称される、石油パイプラインの敷設に対する抗議運動では、当該パイプライン建設への融資を行なっているとして、日本のメガバンクや証券会社がターゲットリストに記載されていた。本事案の場合、アノニマスが提示している資料の中で、日本の金融機関の融資額が特に多い旨が記載されており、攻撃を受ける可能性が高いと分析した。

この他、アノニマスを称する別の者が行っている「OpKillingBay（オペレーションキリングベイ）」では、捕鯨活動を行う自治体や鯨肉を販売する企業など、捕鯨活動に直接関わる組織を中心にターゲットリストに掲載されていた。しかし、実際はリストに掲載されていない組織に対しても攻撃が発生していたため、日本の金融機関に対して攻撃が発生する可能性もあると分析した。また、「OpKillingBay」については、2016 年２月に金融機関に被害が生じた事象が発生している。これは、ある小売業界の企業の Web サイトに対して、アノニマスが DDoS 攻撃を行なったところ、当該企業が利用していた Web ホスティングサービスを提供する企業のデータセンター全体に影響が発生し、同じサービスを利用していた金融機関の Web サイトも閲覧できなくなる、という事象が発生している。このように、金融機関の外部委託先（同じサービスを共有する他の組織）に対する攻撃により、金融機関にも被害が発生する可能性もあることを、脅威動向の分析の際には念頭に置いておく必要がある。

6.2 日本の金融業界において、攻撃が成功する可能性があるか

次に、「日本の金融業界において、攻撃が成功する可能性があるか」についてである。このポイントではまず、「発生が予測される攻撃が成功する条件に、該当する可能性があるか」という観点について分析する。例えば脆弱性を利用した攻撃の場合には、その脆弱性が日本の金融機関のシステムにも存在する可能性があるか、という点を確認する。これと併せて、「攻撃に対して防御策がとられている可能性があるか」という観点でも分析する。これは例えば、DDoS 攻撃であれば、それに対応した防御策がどの程度とられているのか、という点を確認する。こ

れらの分析を元に、「日本の金融業界において攻撃が成功する可能性」について評価を行っている。

6.3 対応策はどうすべきか

最後に「対応策はどうすべきか」という点についてである。これは、金融機関等の各組織においては、分析結果から判明した脅威と、各組織における現状のサイバーセキュリティ対応態勢を比較した上で、必要な対応策や対応の要否を検討することになると思われる。攻撃者が通信先として狙っているポートを閉じる、脆弱性を修正するパッチを至急適用する、などの短期的な対応から、セキュリティ機器の追加導入や組織態勢の見直しなどといった、中長期的な対応まで幅広く存在すると考えられる。これは収集した情報の内容や、各組織におけるサイバーセキュリティ対応態勢等によって異なる。例えば、システムやソフトウェアの脆弱性への対応については、当該脆弱性の影響を受けるシステムの自組織における重要度や、その他の対策状況等によるものと考えられる。そのため、脆弱性の公表後、パッチの適用を行うことは大前提ではあるものの、即座に適用すべきとは一概には言えず、当該脆弱性のリスクや対応コスト等を評価しながら、例えば一時的には代替策にて対応するなどの判断もあり得ることに注意する必要がある。

なお、本項で示した「分析」フェーズの観点のうち、作業に慣れると、①と②で示した内容について、「収集」フェーズの情報収集と同時に、例えば記事のタイトルや冒頭の数行から判断ができる場合がある。これにより、整理、分析をすべき情報の選別が円滑に行えるようになり、作業全体の時間短縮にも繋げることができる。

７．情報提供

最後に収集した情報や分析の結果を、一般的には政策決定者、組織において、例えばサイバーセキュリティへの投資を判断する者に対して情報提供する。なお、筆者の意見としては、組織内でサイバーセキュリティに関わる者（例えば、組織内の CSIRT やシステムの監視部門などサイバーセキュリティに関わる業務を行っている者）にも情報や分析結果を提供し、組織内全体でサイバー攻撃の脅威動向に関する認識を高めていくことが有益であると考えている。

筆者の場合は、庁内にてサイバーセキュリティに関係する者に対して、対面、及び非対面での情報・分析結果の提供をそれぞれ実施した。

7.1 対面での情報提供

まず対面での情報提供であるが、筆者は週次にて庁内の関係者向けに、収集した情報や分析結果を共有することを目的とした、勉強会を実施した。勉強会の概要としては、所要時間 30 分ほどで、前の週に収集した公開情報から特に関係者で共有すべき事項と、金融業界における脅威動向に関する筆者の分析内容について、それぞれ説明した。また、単に分析内容を説明するだけでなく、攻撃ツールを使ったデモンストレーションや、攻撃が発生した際の画面を実際に見せるなど、脅威に関する知識のみを増やすだけでなく、具体的なイメージを伝えるべく工夫した。

対面での情報提供については、自身が発信した情報について、質疑応答やディスカッションが行なわれるため、筆者も気づきが得られるなどして、関係者の理解が深まりやすい点がメリットとして挙げられる。また、筆者が誤って理解していた情報についても、指摘を受けることで正しく理解することができ、参加者に対しても正しい情報を伝えることができた。そして、情報を伝えたい関係者に対し、直接かつ確実に伝えることができる。

7.2 非対面での情報提供

次に、非対面での情報提供であるが、主にメールや書面で配布する、という方式で行い、主に筆者が日々収集したサイバーセキュリティに関連する情報や、週次の勉強会を待っていては遅い、緊急性のある情報等の配布に利用した。

例えば筆者は、金融業界に影響があると想定されるサイバー攻撃関連のニュースなどを、「日刊サイバーインシデント情報（通称:日刊花田）」という形で、組織内の関係者に対して日次で情報提供している。内容としては、インターネット上に公表されている情報（海外の情報も含む）について、筆者が収集・分析を行ない、その結果を要約した形で提供している。これにより、日々変化するサイバー攻撃の動向について、関係者に対して速やかに情報共有を図ることができている。また、「日刊サイバーインシデント情報」とは別に、関係者に対して即座に注意を促すべきサイバー攻撃事案が発生した場合には、その情報の概要、被害の発生状況、対応策などをＡ４サイズで１、２枚程度の短時間で確認できるレポートを作成し、配布を行なっている。

非対面方式での情報提供のメリットとしては、対面方式よりも広範囲の者に対して情報を伝えることが可能な点にある。特に、組織における上位者だけでなく、業務上はサイバーセキュリティとの関わりが薄いが、知見を高めてほしい人物に対しても、情報の提供を行なうことができる点がメリットといえる。

一方、この方式のデメリットとしては、一方的な情報伝達になってしまう可能性が高く、質問やディスカッションなどが生まれにくい、という点がある。このデメリットを克服するために、マイクロソフト社の「SharePoint」という、情報共有のための Web サイトを作成できるツールが有効である。作成されたサイトは、インターネット上の掲示板サイトのように情報をスレッド形式で投稿することができ、それに対して他者がコメントを書くことが可能となっている。金融機関によっては、海外拠点などの遠隔にある拠点との情報共有やディスカッションを行うために、このツールを利用しているケースがある模様である。例えば、先ほど紹介した「日刊サイバーインシデント情報」について、メールでの提供からこのツールを活用しての提供に移行した結果、提供した情報に関するディスカッションがサイトの利用者同士で生まれた。また、全ての利用者に対して情報の投稿を可能にしたため、サイバー攻撃について特に関心が高い者が、自主的に収集した情報を投稿するなど、利用者の間にも情報収集活動に取り組む姿勢が生まれた。ただし、投稿された情報を確認するためには、「SharePoint」で作成したサイトにアクセスする、という能動的な行為が要求されるため、日次で提供される情報を閲覧しているのは一部の利用者のみになる可能性がある。そのため、「SharePoint」で作成したサイトにて投稿された情報について、前日分の情報を翌日の朝に、全ての利用者に対して自動的にメールで通知するようにした。これにより、情報自体は全ての利用者に対して提供することができ、かつ更にディスカッションを行ないたい場合にはサイトを利用してもらう、という形式とした。

８．まとめと金融機関の対応策

ここまで、筆者の経験に基づき、サイバー攻撃の脅威動向に関する、公開情報からの情報収集・分析、及び関係者への情報提供について、有効性や留意点と共に説明した。最後に、本論文で述べたようなサイバー攻撃の脅威動向に関する情報収集や分析の実施にあたって、国内金融機関がどのように対応すべきか、という点について私見を述べた後、本論文のまとめを行う。

8.1 国内金融機関の対応策についての私見

本論文で説明したサイバー攻撃の脅威動向に関する情報の収集や分析については、国内金融機関においても規模の大小や業種にかかわらず、各組織で実施する必要があると考えられる。ただし、金融機関によっては、本論文で紹介した全ての情報を日常的に収集することは難しい場合もあると思われる。そのような場合においても、自組織に存在するシステムやソフトウェアに関する脆弱性の状況について確認しておくべきである。これは、サイバー攻撃が発生する際には、システムやソフトウェアに存在する脆弱性が利用されるケースが多いことが理由である。そのため、まず自社内のシステムをすべて洗い出し、利用しているソフトウェアやそのバ

ージョン等の情報を把握したうえで、該当のシステムやソフトウェアに関する脆弱性の情報などを確認しておく必要があると思われる。

また、金融業界に対するサイバー攻撃事案に関する情報についても、把握しておくべき情報といえる。これは、同様の攻撃が自組織に対して発生することに備えて、必要に応じて自組織の対応策を整備するために必要となるためである。

加えて、金融 ISAC の活用も有用である。金融 ISAC では、各金融機関のサイバーセキュリティ担当者が情報の共有や意見交換、スキルアップを図っている。このような場を活用することで、自組織内の情報収集・分析をさらに有効にできるほか、組織内でサイバーセキュリティに携わる人材の育成などにも効果的であると考えられる。

8.2 まとめ

ここまで説明したとおり、サイバー攻撃の脅威動向について OSINT を活用し、様々な公開情報から情報収集・分析等を行うことにより、現在発生している、または将来発生が予想されるサイバー攻撃に対して有効な対応策を整備することが可能である。特に、インターネット上で公表される情報は、事象が発生してから公表されるまでのスピードが速いことから、現在のサイバー攻撃のスピード感に対応するためには不可欠な情報である。そして、このような取り組みを日常的に行うことで、各組織におけるサイバーセキュリティ態勢の継続的な見直しや、サイバー攻撃事案に対して円滑に対応できる態勢の整備を行うことが、何よりも重要と考えられる。本論文で紹介した手法等が、このような取組みの一助になれば幸いである。

最後に、本論文の内容をもとに情報収集・分析を行う際に留意すべき点を述べる。まず、本論文で述べた内容は、ほぼ全て筆者が自身の業務を通して得た知見であるため、組織によっては収集すべき情報や分析の観点などが異なる場合がある。実際に本論文の手法を活用される場合には、自組織が求める情報やその時々の状況に合わせて、収集や分析の手法を絶えず見直していただきたいと思う。また、本論文に書かれていることをそのまま実行しようとしても、最初は必要な情報が十分に収集できないことや、分析結果が外れてしまうこともある。これにおいても、一朝一夕で上達するものではないため、トライアンドエラーを繰り返しながら活動を継続し、ノウハウを蓄積する必要があると思われる。

また、公開情報からの情報収集だけでなく、可能であれば、専門家や他組織のサイバーセキュリティ担当者などとも直接意見交換を行うことをお勧めする。例えば、筆者は専門家や他組織の方との意見交換の中で、自身の活動の中で収集できていなかった情報や、自身の分析内容についての議論を行い、分析の妥当性を確認した。

最後に、２年間、このような貴重な経験の機会を与えてくださった、金融庁の職員の方々に深く御礼を申し上げさせていただきます。

以上

○補足

補足として、以下２点について、私見を述べる。

①本論文で紹介した、情報収集・分析活動を担う人材に必要な素養

②自ら手を動かして、IT システムについて学ぶ有効性

補足①　本論文で紹介した、情報収集・分析活動を担う人材に必要な素養

本論文で述べたような情報収集・分析活動を行う人材について、どのようなスキルセットやパーソナリティを持ち合わせた人材が良いか、について述べる。

1) IT スキルについて

まず、IT システムに関する知識や業務経験についてである。知識面に関しては、情報収集の中で登場するような IT システムやサイバーセキュリティに関する用語について、知識を持っておく必要がある。目安としては、IPA の情報処理技術者試験のレベルにおける、「応用情報処理技術者」程度の知識は持っておく必要があると思われる。

しかし、知識だけではなく、実際の IT システムの開発や運用に関する業務やシステムリスクの管理に関する業務の経験も必要である。理由としては、組織が実際に利用する IT システムの構成に関する知識や、IT システムが攻撃されて稼動が止まった際に想定される被害に関する知識等が必要になるからである。具体的には、Web サーバの脆弱性についての情報を収集した際に、Web サーバがどのような役割を担っているサーバか、という知識だけでなく、Web サーバは組織内のシステム構成上、どのように配置されており、この脆弱性を攻撃されて Web サーバの稼動が止まってしまった際に、どのような被害が発生するのか、複数の観点から洗い出すことができるか、ということである。このような観点が無い場合は、脆弱性の内容が分かっても、どれほどの脅威なのか分からないため、対応すべきか否か、対応しなかった場合のリスクは何か、といった事が分析できない可能性があると思われる。

2) 言語スキルについて

本文でも説明を行なったが、日本語以外の言語からも情報収集を行なう必要がある。筆者の経験から、特に英語ソースの情報を収集する場面が多かったため、英語を読むこと、及び聞きとることについて、苦手意識がない方が望ましい。英語を聞きとる、という点については、論文では触れなかったものの、例えば海外の動向を収集するために、英語で放送されているラジオやテレビから情報収集を行なっている。

3)パーソナリティについて

能力に加えて、求められる資質として、コミュニケーション能力を挙げたい。コミュニケーション能力については、情報収集・分析については、他者からの依頼を受けて実施する場合も多い。その際に、依頼主が本当に要求している情報、提供された情報をどのように使うのか、といった点についても確認し、それに即して作業を行なう必要がある。他にも、自分が行なった情報収集や分析について、他者と意見交換を行なうことも必要となるため、コミュニケーション能力は必要となる。

補足②　自ら手を動かして、IT システムについて学ぶ有効性

論文内において「自らサーバを立ててみるなど、手を動かして学習」することの重要性について説明を行なった。これについて、筆者の経験について説明しておく。

筆者はこれまでの業務経験では、システム開発の企画や進捗管理の業務のみで、サーバを立てる、プログラミングを行なう、といった経験は無かった。そのため、例えば、Web サーバや DB サーバの役割は把握していても、どのような仕組みで稼動しているのか、具体的な設定の内容などは把握できていなかった。

DNS サーバ§§§§§)や Web サーバ、プロキシサーバ等を実際に構築することにより、これらの具体的な設定内容や仕様などについても学習することができた。例えば、DNS サーバを構築するためのソフトウェアの一種である「BIND（バインド）」の機能が止まる脆弱性が公表された際の、筆者の体験を説明したい。筆者は、元々DNS サーバの存在や機能は知っていたものの、「BIND」というソフトウェアを用いて構築する、ということは知らなかった。そのため、「BIND」が止まるという脆弱性の情報に気づいたときに、「BIND」が何か分からなかった。よって、脆弱性を攻撃されて機能が止まった際に、どのようなリスクが想定されるかについてもイメージすることができなかったのである。

実際に自ら手を動かしてサーバ等を構築することにより、実際にはどのような機能が稼動しており、どのような設定がされているのか、などといった知識を得ることができ、それを基に、サイバーセキュリティに関わる様々なリスクに対する正しい分析を行うことが可能となるのである。

§§§§§) URL などのドメイン名とサーバの住所代わりである IP アドレスとの対応関係を管理するサーバ。URL を用いて Web サイトにアクセスする際に、DNS サーバを用いて IP アドレスを確認する。そのため、DNS サーバが止まった場合、Web サイトの閲覧ができなくなる等の被害が想定される。

金融庁金融研究センター

〒100-8967　東京都千代田区霞ヶ関 3-2-1
中央合同庁舎 7 号館　金融庁 15 階

TEL：03-3506-6000（内線 3293）
FAX：03-3506-6716
URL：http://www.fsa.go.jp/frtc/index.html