要求中心的なOSINT手法と平昌オリンピックを狙った攻撃の解析例

セコム株式会社 IS 研究所
稲垣　俊

1. はじめに

サイバー空間における攻撃者の優位性は、しばしば議論の対象となる。攻撃側は自由に攻撃対象を選べるだけでなく、防御側の出方を見つつ攻撃を進化させることができる。その一方で防御側はどのような攻撃を受けうるのかを想定し、限られたリソースで対策を決定しなくてはならない。この意思決定を支援するために公開情報を用いるという試みこそがOSINT（Open Source INTelligence）である。

本稿ではサイバーセキュリティにおける要求中心的なOSINT手法を紹介したのち、その一例として平昌オリンピックを狙った攻撃解析の結果の一部を示す。なお、今回は情報整理手法を示すことが主目的である。本来であれば含むべき、情報源および提供された情報の信憑性に関する議論にはあえて踏み込んでいないことに注意されたい。

2. サイバーセキュリティとインテリジェンス

「インテリジェンス」それ自体の普遍的な定義は確認されていない。ここでは、本稿で議論するインテリジェンスを定義するために、次のふたつのインテリジェンスに関する定義を参考にした。それらはインテリジェンスに関する小林の定義「政策決定者が国家安全保障上の問題に関して判断を行うために政策決定者に提供される、情報から分析・加工された知識のプロダクト、あるいはそうしたプロダクトを生産するプロセス」（小林良樹「インテリジェンスの基礎理論」）[1]、および脅威インテリジェンスに関するガートナーのMcMillanの定義「資産に対する既存あるいは今後現れうる脅威や危害に関する経験に基づく知見である」（Rob McMillan「Definition: Threat Intelligence」）[2]である。

> 本稿では「資産に向けられた脅威に対抗する意思決定者の要求に基づき、収集、処理、解析された情報であり、意思決定を支援する生産物および生産プロセス」を脅威インテリジェンスと呼ぶ。また、「オープンソースすなわち公開情報から法的かつ倫理的に入手できる情報を用いたインテリジェンス生産プロセス」を本稿ではOSINTとして扱う。

本定義では意思決定者がインテリジェンスの要求者であり、消費者であることを示している。サイバー攻撃に対する脅威インテリジェンスについても、意思決定者が誰であるか何を要求しているのかを明確にした要求中心的な脅威インテリジェンス生産を行わなければならない。

MWR InfoSecurityらが作成したフレームワークでは、インテリジェンス消費者という観点から脅威インテリジェンスを4種類に分類した[3]。それらは戦略（Strategic）脅威インテリジェンス、作戦（Operational）脅威インテリジェンス、戦術（Tactical）脅威インテリジェンス、技術（Technical）脅威インテリジェンスである。表1はそれぞれのインテリジェンスの概要を示している。インテリジェンスの消費者が異なるということは、彼らから要求されるインテリジェンスも異なる。したがって、インテリジェンス生産者は消費者に合わせてインテリジェンスを提供しなければならない。

この4種類の脅威インテリジェンスは先に本稿で定義した要求中心的な脅威インテリジェンスと相性が良いため、次節以降ではこれらに沿った形でインテリジ

表1　脅威インテリジェンスの分類

種類	消費者 / 要求者	概要
戦略脅威インテリジェンス	役員などの主要な意思決定者	組織の重要な意思決定に影響を与えうる情報
作戦脅威インテリジェンス	セキュリティ担当のマネージャなど	組織に対する攻撃情報（攻撃者像など）
戦術脅威インテリジェンス	セキュリティ担当者	攻撃者の手口
技術脅威インテリジェンス	アプライアンスなど	IP アドレスなどのデータ

ェンス例を紹介する。

3. インテリジェンスの準備

インテリジェンスは何らかの意思決定を支援する情報である。したがって、それを生産するためには要求が必要となる。本稿ではオリンピック関係組織の経営者が次のような状況に遭遇したことを仮定することにした。

> オリンピック開催にあたり、スポンサー/パートナー企業として大会を支えることとなった。近日中にサイバー攻撃対策の指針を立てるので、その判断材料が欲しい。

そして、この状況における各要求者の要求を仮定し、インテリジェンスを生産する。

なお、今回用いた情報収集手法はOSINTのみである。短期間で情報収集を行うことを仮定したため、情報収集期間は2018年2月21、22、23日および26日の4日間のみとした。また、今回は情報整理手法の一例を示すことが主目的であるため、情報源や提供された情報の信憑性に関する議論をあえて行っていないことに注意して欲しい。次節以降では戦略脅威インテリジェンスと戦術脅威インテリジェンスの一部を示す。また、戦術脅威インテリジェンスの一例として図1に開会式を狙った攻撃のタイムラインを示す。

4. 戦略脅威インテリジェンスの例

まずは経営者のような上層部の意思決定者を想定としたインテリジェンスについて記述する。

> **要求**
> 2020年のオリンピック開催にあたり、スポンサー/パートナー企業として大会を支えることとなった。それに先立ち、サイバー攻撃対策の指針を立てるために、その判断材料が欲しい。その参考として2018年の平昌オリンピックを対象にしたサイバー攻撃の情報をまとめ、その特徴について報告せよ。

4.1. 状況の要約

遅くとも2017年12月頃からオリンピック関係組織に対する攻撃が複数行われている[4, 5, 6]。そのうちの

図 1　平昌オリンピックの開会式を狙った攻撃のタイムライン

2018-02-09T19:15	メインプレスセンターの IPTV が遮断 [16, 17]
2018-02-09T19:15	接続障害が発生、その後 1 日以上続く [8, 18, 19]
2018-02-09T19:**	メインプレスセンターの IPTV が復旧 [17]
2018-02-09T19:**	組織委員会はネットワークからサーバを遮断 [16]
2018-02-09T19:**	上記対応に伴い公式 Web サイトの一部がアクセス不能 [16, 17]
2018-02-10T08:**	公式 Web サイトが復旧 [16, 8]
2018-02-10	オリンピックの報道官が障害はサイバー攻撃が原因であると発表 [7]
2018-02-12	Cisco の Talos が攻撃に用いられたと思しきマルウェアの解析結果を公表 [15]
2018-02-12	各種メディアがサイバー攻撃について報道
2018-02-12	Microsoft が攻撃に EternalRomance （ ER ）が用いられた可能性を示唆 [20, 21]
2018-02-12	Intezer がマルウェア解析に基づくアトリビューションの結果を公表 [13]
2018-02-13	ENDGAME がマルウェア解析結果を公表 [23]
2018-02-15	Talos の研究者がマルウェアから ER の PoC に類似する断片を発見 [22]
2018-02-15	三井物産セキュアディレクションがマルウェア解析結果を公表 [24]
2018-02-20	トレンドマイクロがマルウェア解析結果を公表 [25]
2018-02-24	ワシントンポストがアメリカ諜報機関の話として、ロシアの攻撃関与を示唆 [12]

ひとつはオリンピック開会式が行われた時間に会場の通信や公式サイト、チケットの発券機能などのサービスを利用不能に追い込んだ[7]。なお、競技の進行自体には影響がなく、12時間後に障害はほぼ復旧した[8]。

4.2. 国家規模の関与が疑われる攻撃

一部のメディアは今回の攻撃に国家規模の攻撃者が関与している可能性を報じている。しかしながら、ここで重要であるのはどの国が攻撃をしたのかということではなく、高度な攻撃が大規模に行われたということである。そのような攻撃に対して、一組織であらかじめ防御策を展開することは困難である。攻撃を防ぐよりもむしろ普通ではない状態に迅速に気付き、対処可能なシステムや人員を確保すべきだろう。それを踏まえた上で、様々なメディアが報じる攻撃者について収集した情報を記載する。

攻撃に北朝鮮またはロシアが関与している可能性を一部メディアが論じている。今回オリンピックが開催された韓国は北朝鮮の核開発を巡り、緊張状態が続いている。しかしながら、北朝鮮要人の訪韓や、統一チームの大会参加などで融和ムードとなっていること[9]を挙げ、北朝鮮が攻撃に関与している可能性が低いと見積もる見解もある[10]。

ロシアは組織的なドーピングを指摘され、今回のオリンピックに国家として参加することが認められなかった。そのロシアが国際反ドーピング協会に対して悪意を向ける可能性があるとして、攻撃者の候補に挙げている機関も存在する[10,11]。特に、ワシントンポストはアメリカ諜報機関が非公式に公表した内容として、ロシアが攻撃の背後にいると報道している[12]。また、技術的な分析からは中国が関与していると思しき攻撃に似た痕跡が確認されたとの報告もあった[13]。

4.3. 攻撃の起点となりうる関連企業

今回発生したインシデントのひとつは攻撃の起点がどこであるか未だ判明していないが、一部のメディアは攻撃を解析した結果からオリンピック運営関係企業が攻撃の起点になっている可能性があるとの見解を示している[14]。攻撃の痕跡に基づく推測のみから当該企業が攻撃の起点であると判断することは早計である。しかしながら、関連企業からイベントに対する攻撃が始まる可能性を承知し、それを踏まえて対策を検討することは防御者にとって有益であると考えたため、それを踏まえたインテリジェンスを以下に記載した。

当該企業に対する攻撃はオリンピック開催のひと月以上前から行われている可能性があり、その場合入念に準備が行われていたことが予想できる。国家規模の攻撃であれば、このようなことが起きた事例は珍しくない。なお、当該企業は現在大手セキュリティベンダと調査にあたっている最中であるため、詳細なコメントを避けている。

オリンピックのような大規模なイベントになれば関係者は爆発的に増加する。攻撃者が目的を達成させるためには、そのうちのセキュリティが最も弱い部分を狙うだけでよい。重要なことは自組織がそのような弱い部分になる可能性を考慮し、攻撃に素早く気づきそれを迅速に封じ込める耐性を作ることである。その封じ込めを適切に行うためには事前の準備が必要となるが、今回のオリンピックでは封じ込めに伴い、公式サイトが停止するという自体が発生した。そのようなことが起きないよう、あらかじめリスクを適切に評価した上で、問題を最小限に食い止める必要があるだろう。

4.4. 破壊が目的の攻撃

今回の攻撃のうちひとつは情報窃取よりも破壊を目的としている可能性が高い[15]。大規模なイベントや重要インフラなど稼働していること自体が大きな意味を持つシステムに対して、このような攻撃が行われることもある。そのことを認識せず、情報窃取の脅威を重視した対策のみを施した場合、本質的なリスクを低減させることは難しいだろう。

今回の場合、重要なことはインシデントから素早く立ち直り、業務を継続させることである。事前に分析やシステム構成の検討を行うのみならず、十分に訓練することも必要となる。机上訓練などを通して、どのような時に何をしなければならないのか、どこに何を伝えなければならないのかを把握しておくことで、円滑な問題解決を行うことができるようになるだろう。

5. 作戦脅威インテリジェンスの例

公開情報を対象に情報収集を行ったところ、主にふたつの攻撃に対する報告が寄せられていることがわかった。ひとつはフィッシングメールを用いた攻撃であり、もうひとつは開会式を狙った攻撃である。

複数のセキュリティベンダがそれぞれの攻撃について報告を行っている。したがって、それらは大規模に発生した攻撃または実害を引き起こした攻撃であることがわかる。以下では、各攻撃の攻撃者像についてまとめた内容を記述する。

> **要求**
> インテリジェンス要求者が守るべき組織（防御対象組織）を狙う攻撃者の目的、素性について判明する限りを報告せよ。これを基に、2020年のオリンピックにおいて防御対象組織が狙われる可能性があるか判断するために必要な情報を提供せよ。

5.1. フィッシングメールを用いた攻撃

2017年末から続く平昌オリンピックを狙ったフィッシング攻撃について、CrowdStrikeやMcAfeeが報告を行っている[4, 5, 6]。フィッシングメールを受信した者の多くはイベント関係者であり、その内容を分析すると韓国に狙いを定めたものであったことがわかった。フィッシングメールが韓国語で記載されていただけでなく、それを被害者に開かせるための「おとり」として鳥インフルエンザの話題が用いられていた。これは2017年末からオリンピック開催周辺地域で流行が懸念されていたものである。さらに、マルウェアが動作するためには韓国で広く用いられているワープロソフトが必要であった。また、攻撃が行われた時刻は韓国の国家テロ対策センターが訓練中であったことから、攻撃者は内部事情をよく把握している可能性があるようである。

今回の攻撃が何者によって、なぜ行われたかを特定することは困難であるが、攻撃対象に関する入念な調査が行われたうえで攻撃が行われていたことがわかる。必要に応じて攻撃者像を推定することは、防衛リソース振り分けの一助となるかもしれない。

5.2. 開会式を狙った攻撃

開会式を狙った攻撃はあるマルウェアによって引き起こされたものである可能性が高いとCiscoのTalos Intelligenceは報告している[15]。そして、そのマルウェア（Olympic Destroyer）は自己を複製しながら破壊を行う。マルウェアそれ自体には破壊機能が主に実装されていることから、今回の攻撃の目的は破壊であるとTalosは結論付けた。

Intezerは攻撃に用いられたマルウェアを解析した[13]。そして、その一部について、国家の関与が疑われている攻撃者が用いるコードとの類似性を報告している。なお、当該攻撃者は欧州、米国、日本の重要セクターを狙い、知財情報の窃取等を行っていたという報告が上がっている。

ソースコードの流出、バイナリの再利用、偽旗作戦など様々な可能性を考えられるものの、高度な攻撃の背景には国家規模の存在が絡んでいる可能性を否定できない。すなわち、単なる一般的なセキュリティ対策ではこのような攻撃を防ぎきれない可能性があることを心に留めなければならない。

6. おわりに

今回は紙面の都合上、戦術脅威インテリジェンスと技術脅威インテリジェンスを割愛するが、先に示した2種類のインテリジェンス同様にそれらも要求に応じて生産することが可能である。

特にイベントが発生したばかりの際には、様々なセキュリティベンダが各種インテリジェンスを発表し、それぞれの情報が更新され続ける。それらを効率よく表現するためには図1で示したようにイベントと記事の発行を時系列で表示するとよい。

なお、弊社では2017年に世界的に問題となったランサムウェアWannaCryに対しても公開情報とタイムラインを用いてインシデントの概要を把握する試みを実施した[26]。興味を持たれた読者はそちらも参照していただきたい。

参考文献

[1] 小林良樹（2014）「インテリジェンスの基礎理論」、立花書房
[2] Rob McMillan（2013）「Definition: Threat Intelligence」、<https://www.gartner.com/doc/2487216/definition-threat-intelligence>（参照2018-02-26）
[3] MWR InfoSecurity（2015）、「Threat Intelligence: Collecting, Analysing, Evaluatin」、<https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/MWR_Threat_Intelligence_whitepaper-2015.pdf>
[4] Falcon Intelligence Team（2018）「Malicious Spear-Phishing Campaign Targets Upcoming Winter Olympics in South Korea」、CrowdStrike, Inc.、<https://www.crowdstrike.com/blog/malicious-spear-phishing-campaign-targets-upcoming-winter-olympics-in-south-korea/>（参照2018-02-26）
[5] Ryan Sherstobitoff et al.（2018）、「Malicious Document Targets Pyeongchang Olympics」、McAfee, LLC、<https://securingtomorrow.mcafee.com/mcafee-labs/malicious-document-targets-pyeongchang-olympics/>（参照2018-02-26）
[6] Ryan Sherstobitoff et al.（2018）、「Gold Dragon Widens Olympics Malware Attacks, Gains Permanent Presence on Victims' Systems」、McAfee, LLC、<https://securingtomorrow.mcafee.com/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/>（参照2018-02-26）
[7] Sean Ingle(2018)「Winter Olympics was hit by cyber-attack, officials confirm」、The Guardian、<https://www.theguardian.com/sport/2018/feb/11/winter-olympics-was-hit-by-cyber-attack-officials-confirm>（参照2018-02-26）
[8] BBC（2018）「Winter Olympics hit by cyber-attack」<http://www.bbc.com/news/technology-43030673>（参照2018-02-26）
[9] Zeeshan Aleem（2018）「Hackers attacked the opening ceremony of the Winter Olympics. The question is who they were.」、VoxMedia、<https://www.vox.com/world/2018/2/12/17003444/winter-olympics-cyber-attacks-russia-north-korea>（参照2018-02-26）
[10] Doug Olenick（2018）「Russian actors mentioned as possibly launching cyberattack on 2018 Winter Olympic Games」、SC Media、<https://www.scmagazine.com/russian-actors-mentioned-as-possibly-launching-cyberattack-on-2018-winter-olympic-games/article/743835/>（参照2018-02-26）
[11] Feike Hacquebord、「Update on Pawn Storm: New Targets and Politically Motivated Campaigns」、Trend Micro Incorporated、<https://blog.trendmicro.com/trendlabs-security-intelligence/update-pawn-storm-new-targets-politically-motivated-campaigns/>（参照2018-02-26）
[12] Ellen Nakashima（2018）「Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say」、The Wasington Post、<https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html>（参照2018-02-26）
[13] Jay Rosenberg（2018）「2018 Winter Cyber Olympics: Code Similarities with Cyber Attacks in Pyeongchang」、Intezer、<http://www.intezer.com/2018-winter-cyber-olympics-code-similarities-cyber-attacks-pyeongchang/>（参照2018-02-26）
[14] Chris Bing（2018）「Atos, IT provider for Winter Olympics, hacked months before Opening Ceremony cyberattack」、CyberScoop、<https://www.cyberscoop.com/atos-olympics-hack-olympic-destroyer-

malware-peyongchang/>（参照2018-02-26）
[15] Warren Mercer et al.（2018）、「Olympic Destroyer Takes Aim At Winter Olympics」、Cisco Systems, Inc.、<http://blog.talosintelligence.com/2018/02/olympic-destroyer.html>（参照2018-02-26）
[16] 김형열（2018）、「개회식 때 평창조직위 홈피 사이버 공격…10일 오전 복구『邦訳：開会式の時、平昌組織委員会ホームページサイバー攻撃…10日午前、復旧』」、SBS、<https://news.sbs.co.kr/news/endPage.do?news_id=N1004617403>（参照2018-02-26）
[17] 聯合ニュース（2018）、「[올림픽] IOC·평창조직위、사이버 공격 확인…안전 위해 세부내용 비공개『邦訳：[五輪]IOC・平昌組織委員会、サイバー攻撃確認…安全のために細部内容非公開』」、<http://www.yonhapnews.co.kr/bulletin/2018/02/11/\\0200000000AKR20180211032900007.HTML>（参照2018-02-26）
[18] NICOLE PERLROTH（2018）、「Cyberattack Caused Olympic Opening Ceremony Disruption」、The NewYork Times、<https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html>（参照2018-02-26）
[19] Waqas Amir（2018）、「Cyber Attack Disrupts Winter Olympics Website During Opening Ceremony」、HACKREAD、<https://www.hackread.com/cyber-attack-disrupts-winter-olympics-website-opening-ceremony/>（参照2018-02-26）
[20] Windows Defender Security Intelligence(2018)、<https://twitter.com/WDSecurity/status/963308636276584448>（参照2018-02-26）
[21] Windows Defender Security Intelligence（2018）、<https://twitter.com/WDSecurity/status/963887214835859457>（参照2018-02-26）
[22] Paul Rascagnères（2018）、<https://twitter.com/r00tbsd/status/964055076590403584>（参照2018-02-26）
[23] Amanda Rousseau et al.（2018）、「Stopping Olympic Destroyer: New Process Injection Insights」、Endgame、<https://www.endgame.com/blog/technical-blog/stopping-olympic-destroyer-new-process-injection-insights>（参照2018-02-26）
[24] 吉川 孝志、菅原 圭（2018）、「Olympic Destroyerの内部構造を紐解く」、三井物産セキュアディレクション株式会社、<https://www.mbsd.jp/blog/20180215.html>（参照2018-02-26）
[25] 岡本 勝之（2018）、「平昌五輪開会式に影響を及ぼしたとされる不正プログラムを解析」、トレンドマイクロ株式会社、<http://blog.trendmicro.co.jp/archives/17023>（参照2018-02-26）
[26] 葛野 弘樹ら（2017）、「WannaCryを事例としたセキュリティレポートの分析」、情報処理学会、コンピュータセキュリティシンポジウム 2017