ウクライナ情勢から学ぶ
サイバー攻撃への対策強化のポイント

2022 年 3 月 28 日
名和 利男

はじめに

2022 年 3 月 21 日、米国バイデン大統領は、ビジネスラウンドテーブルの CEO 四半期会議で演説し[1]、サイバーセキュリティについて、次の趣旨の発言をした。

- 「進展するインテリジェンス（evolving intelligence）に基づいて、ロシアが我々に対するサイバー攻撃を計画している可能性があるという新たな警告を行政が発した。」
- 「ロシアのサイバー能力の大きさはかなり重大であり、それは近づいている。」
- 「連邦政府は、ロシアによるサイバー攻撃に備えて、その役割を果たしている民間企業の CEO においても、同じようにすることが、国益にかなうものである。」
- 「民間企業の CEO は、ロシアによるサイバー攻撃に備えてシステムを強化するという愛国的な義務がある。」
- 「民間企業は、連邦政府の支援は必要だが、決断するのは CEO 自身である。」

このサイバーセキュリティにかかる情勢判断において、バイデン大統領は、「懸念」（気にかかって不安に思うこと）という感覚的な言葉は使わず、「進展するインテリジェンス」という表現で、信頼性と確度のある情報に基づいた判断であることを示唆している。

同日、米国ホワイトハウスは、ウェブサイト上で「我が国のサイバーセキュリティに関するバイデン大統領の声明[2]」および「ファクトシート：潜在的なサイバー攻撃から保護するために今すぐ行動する[3]」を公開し、米国の全ての組織に対して、認識および実施すべき事項を提示した。この中で、ロシアによるサイバー攻撃の発生可能性および実施すべき対策として、次のように示されている。

（ロシアによるサイバー攻撃の発生可能性について）

---

[1].President Biden Joins the Business Roundtable's CEO Quarterly Meeting（2022 年 3 月 21 日、The White House）
https://www.youtube.com/watch?v=dFn8_ESsffI

[2].Statement by President Biden on our Nation's Cybersecurity（2022 年 3 月 21 日、The White House）
https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/

[3].FACT SHEET: Act Now to Protect Against Potential Cyberattacks（2022 年 3 月 21 日、The White House）
https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/

- 「私は以前、ロシアが米国に対して悪意のあるサイバー活動を行う可能性について警告した。これには、同盟国やパートナーとともにロシアに課した前例のない「経済的コストへの対応」（経済制裁）も含まれる。これはロシアのプレイブックの一部である。今日、私の政権は、ロシア政府が潜在的なサイバー攻撃の選択肢を模索しているという『進展するインテリジェンス』に基づいて、これらの警告を繰り返している。」

（ロシアによるサイバー攻撃に備えて民間企業が実施すべき対策）

- 攻撃者がシステムに侵入するのを困難にするために、システム上で多要素認証の利用を義務付ける。
- コンピュータやデバイスに最新のセキュリティツールを導入し、継続的に脅威を探索し、軽減させる。
- サイバーセキュリティの専門家に相談し、既知の脆弱性に対してパッチが適用され、システムが保護されていることを確認し、ネットワーク全体のパスワードを変更し、以前に盗まれた認証情報が悪意のある行為者にとって無用になるようにする。
- データをバックアップし、悪意のある行為者の手の届かないところにオフラインでバックアップしておく。
- 攻撃の影響を最小限に抑えるため、緊急時における対応策の訓練や演習を行い、迅速に対応できるようにする。
- データを暗号化し、盗まれても使用できないようにする。
- 攻撃者が電子メールやウェブサイトで使用する一般的な手口について従業員を教育し、コンピュータや携帯電話が異常にクラッシュしたり、動作が非常に遅くなったりするなどの異常な動作を示した場合は、報告するよう奨励する。
- 地元の FBI 支局や CISA 地域事務局と積極的に関わり、サイバーインシデントに備えて関係を構築しておく。IT およびセキュリティ部門のリーダーに対し、CISA および FBI の Web サイトにアクセスし、技術情報やその他の有用なリソースを入手するよう推奨する。

このように米国では、ロシアが「前例のない経済制裁」への対抗策の一つとして、米国およびその同盟国やパートナーの民間企業にサイバー攻撃を仕掛ける可能性があるとしているため、日本の企業がその攻撃対象の中心の近くにあると見るのが自然である。

日本政府の対応と企業間の情報格差

これを受けて、日本の複数の政府機関（経済産業省、総務省、警察庁、内閣官房内閣サイバーセキュリティセンター）が連名で、2022 年 3 月 25 日に「現下の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）」を公表した。しかし、その内容は、ロシアによるサイバー攻撃を十分に理解したものとは言い難く、メディアや業界団体等を通じた日本企業への周知努力が見られない。同年 2 月 1 日から 3 月 18 日までの間、内閣サイバーセキュリティセンターがかなりの予算をかけて、日本の国民や企業に周知努力をしていた「2022 年サイバーセキュリティ月間」と比べると、日本の行政機関におけるサイバーセキュリティ対策に「ちぐはぐな対応」が目立つ。

他の主要国と比較すると、日本の政府機関は、サイバー情勢の変化に追随できる仕組みや能力の成熟度が低く、必然的に、民間企業に対するサイバー脅威への情報支援が非常に少ない。そのため、資金に余裕があり、かつリーダーシップのある経営層がいる企業のみがサイバー脅威の高まりと比例した危機意識を持つことができ、政府機関からの要請に応えるような対策推進が見られる。しかし、資金に余裕のない企業は、経営層のリーダーシップの有無に関わらず、変化するサイバー情勢を適切に認識できる情報が得られないため、または雑多な情報が氾濫しているため、サイバー脅威の高まりを直感的に理解することが困難な状況となっている。日本における数多くの格差問題の中に、「企業間の情報格差」も存在していると言える。

したがって、昨年（2021 年）9 月 28 日に閣議決定された「サイバーセキュリティ戦略[4]」において示されている、「経営層の意識改革」を確実に実現するためには、このような情報格差を減らすための取り組みが必要であると考える。

そこで、本コラムの読者向けに、一部ではあるが、ウクライナ情勢に関連したサイバー攻撃に関する状況認識を共有させていただく。

ウクライナ情勢から学ぶサイバー攻撃への対策強化のポイント

まず、ウクライナ情勢に連動したサイバー活動の多くは、外交や軍事にかかる問題と連動した、ロシア特有の「影響工作を伴った情報戦をベースとしたサイバー攻撃」である。その観点で、筆者がモニタリングしている状況認識からピックアップすると、次のリストを作成することができる。

- **2021 年 4 月～　ロシアが世界各国にサイバー偵察を活性化**
- 2021 年 10 月～　ロシアがウクライナにサイバー偵察を強化
- 2022 年 1 月 13 日　ウクライナにデータ破壊マルウェア攻撃
- **2022 年 1 月 13 日　ウクライナ政府サイトの同時多発的な改ざん**
- 2022 年 2 月 15 日　ウクライナの軍や銀行等に DDoS 攻撃
- 2022 年 2 月 23 日　ウクライナ兵士に脅迫的なテキストメッセージ
- 2022 年 2 月 23 日　ウクライナに再度のデータ破壊マルウェア攻撃
- 2022 年 2 月 23 日　ウクライナの軍や銀行等に再度の DDoS 攻撃
- 2022 年 2 月 24 日　欧州の通信衛星システムにサイバー攻撃
- 2022 年 2 月 25 日　ウクライナ軍へのスピアフィッシング攻撃
- 2022 年 2 月 25 日～　Anonymous によるロシアへのサイバー攻撃

[4].サイバーセキュリティ戦略（2021 年 9 月 28 日、閣議決定）
https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf

上記の中から、近い将来に発生が懸念されている台湾有事[5] において、日本の企業が深刻な影響を受ける可能性のあるものとして、2 つのサイバー攻撃について概説し、それぞれを想定脅威と捉えた場合における対策強化ポイントを紹介する。

2021 年 4 月～ ロシアが世界各国にサイバー偵察を活性化

（サイバー攻撃の状況）

2021 年 4 月ごろから、ロシアの国家の支援を受けていると見られる攻撃グループが、世界中の企業や政府機関を標的にしたサイバー侵入を行った[6]。この攻撃グループは、2020 年 12 月、米国 SolarWinds Orion Platform のソフトウェアのビルドシステムを介して、最大で 18,000 社にのぼる SolarWinds 顧客が、気づかぬうちに侵害される事態を引き起こしたロシアの攻撃グループと関係すると分析されている。

この攻撃グループは、「ロシアの利益に繋がるデータを窃取する傾向」が見られ、サイバー侵入した環境に対する適応力を持ち、サイバー活動を進展させる能力を持っていた。特に、次のような戦術を取っていたことが確認されている。

- クラウドサービス事業者、IT サービス提供者、再販業者（リセラー）を標的とする。
- 他のサイバー攻撃グループが、情報窃取キャンペーンにより取得した可能性のある資格情報を悪用して、組織へ最初にアクセスする。
- 機密性の高いメールデータを収集する「アプリケーション偽装権限」を持つアカウントを使用することがある。
- 侵害に成功した標的システムと通信するための、「住宅用 IP プロキシサービス[7]」と「新しくプロビジョニングされ地理的に配置されたインフラ」の両方を使用する。
- 新しい TTP（戦術、技術、手順）を使用して、内部ルーティング構成する仮想マシンを抽出するなどをして、侵害した標的システムのネットワーク環境内のセキュリティ制限を回避する。
- CEELOADERv と呼ばれる、新しい特別なダウンローダーを使用する。
- 有効な資格情報を取得し、標的のユーザーのスマートフォンに表示される「プッシュ通知」をタップさせることで、多要素認証を回避する。「住宅用 IP プロキシサービス」を併用することで、標的のユーザーの不信感を和らげている可能性がある。

---

[5].6 年以内に台湾有事、今も懸念（2021 年 12 月 17 日、共同通信）
https://nordot.app/845937739532713984

[6].Suspected Russian Activity Targeting Government and Business Entities Around the Globe（2021 年 12 月 6 日、Mandiant）
https://www.mandiant.com/resources/russian-targeting-gov-business

[7]「住宅用 IP プロキシ」とは、国や地域等の場所に依存させる目的で作成されたプライベートインターネットプロキシのこと。主な用途は、Web スクレイピング（調査対象のウェブサイトから特定のデータを抽出する技術）、ソーシャルメディアボット、特定の国からのアクセスを制限したウェブサイトへのアクセスなどがある。

（対策強化のポイント）

まず、企業のサイバーセキュリティ担当役員（CISO 等）が、最低限、信頼できるサイバーセキュリティ企業の公表するレポートで示されている攻撃の TTP（戦術、技術、手順）を理解して、その脅威に適応した対策強化のための指示や、予算承認に向けた調整をする必要がある。主なポイントは、次のとおり。

- サイバーセキュリティが一定水準以上確保されたクラウドサービス事業者を利用する。例えば、ISO/IEC27017 等の第三者認証の取得[8] や ISMAP（政府情報システムのためのセキュリティ評価制度）登録[9] を選定基準にすることが考えられる。
- ユーザーや運用管理者等の資格情報が持続的に漏洩しているとみなして、二要素認証や多要素認証の利用を義務付ける。レガシーシステムにおいて利用が困難な場合は、「Have I been Pwned[10]」等を利用して、認証プロセスの監視を徹底する。
- 稼働中のサーバーアプリケーションについて、極力低い権限のユーザーに偽装（impersonate）して実行されるように設計している場合、不自然な偽装ユーザーが作成されていないかを監視する努力を継続する。
- アクセス制限のための IP フィルタリング機能に限界があることを受け入れ、「住宅用 IP プロキシサービスやローテーションプロキシ[11]」により、悪意のある通信の探索努力として、重要な領域については、IP アドレスに加えてペイロード（IP パケットのデータ部分）に基づいたフィルタリングを行う必要がある。例えば、DPI（Deep Packet Inspection）の採用などが考えられる。
- 仮想ルーターで設定される内部ルーティングの文書化および変更管理を厳格に行い、定期的にセキュリティレビューを行う。
- モバイルデバイスのユーザーに対して、「悪意のある者が、別の手段で窃取したユーザーの資格情報で不正にログインした後に、ユーザーのモバイルデバイスに表示される「プッシュ通知」で「OK」をタップ（クリック）させて認証を成功させる手法」などの攻撃手口を知らしめる教育を行う。

2022 年 1 月 13 日　ウクライナにデータ破壊マルウェア攻撃

（サイバー攻撃の状況）

ウクライナ国内の組織に対して、2022 年 1 月 13 日に発生したデータ破壊マルウェア攻撃は、成熟したランサムウェアの戦術・技術・手順をそのまま流用しつつ、身代金を支払うメカニズムを割愛して、標的のデバイスを動作不能にするように設計されていた

---

[8].ISMS クラウドセキュリティ認証取得組織検索
https://isms.jp/isms-cls/lst/ind/

[9].ISMAP クラウドサービスリスト
https://www.ismap.go.jp/csm?id=cloud_service_list

[10].「Have I been Pwned」（HIBP）は、自分のパスワードなどが流出していないかを無料で確認できるサイトのこと。米連邦捜査局（FBI）の捜査過程で発見された流出パスワードの情報を加えられている。
https://haveibeenpwned.com/

[11].「ローテーションプロキシ」とは、大量のリクエストをする IP アドレスをブロックするセキュリティを実装しているウェブサイトに対して、セッションごとまたは定期的に IP アドレスを変更する住宅用 IP プロキシのこと。

[12]。被害を受けた組織は、ウクライナに拠点を置く複数の政府、非営利、および情報技術の企業等に集中していた。

また、ロシアの侵攻の前日（2022 年 2 月 23 日）と当日（2022 年 2 月 24 日）には、別の種類のデータ破壊マルウェア攻撃が発生し、ウクライナ国内の金融、防衛、航空、IT サービス企業が被害を受けた。このデータ破壊マルウェアは、1 月 13 日の攻撃で使用されたマルウェアと類似性があり、ランサムウェアに見られる回復のメカニズムを提供せず、コンピュータの起動に関する情報を記録したハードディスクの領域（マスターブートレコード）を上書きして OS 起動を不能にする戦術を取っていた。セキュリティリサーチャーの分析によると、被害者のサーバーの 1 つに攻撃者が事前にアクセスしていたことが示されており、このマルウェア破壊攻撃は、数か月前から計画されていた。

（対策強化のポイント）

このデータ破壊マルウェア攻撃に備えた対策は、一般的なランサムウェア対策に加えて、ロシアが 2015 年頃からジョージアやウクライナの重要組織を標的にしたワイパー（データ破壊）攻撃や、2018 年平昌オリンピックの開会式直後に発生した「Olympic Destroyer」への対策を付け加えたものとなる。特に重要な対策強化のポイントは、次のとおり。

- 国家サイバーセキュリティ機関（他の主要国）やサイバーセキュリティ専門組織と連携するなどして、IoC（Indicator of Compromise：侵害指標）を積極的かつ持続的に取得し、自組織の IT システムに侵害が存在するかどうかを調査する。
- 速やかに二要素認証や多要素認証の使用を義務付ける。やむを得ずパスワード認証を許す場合は、その認証プロセスを継続的に監視する。
- Windows システムにおいてマスターブートレコードへの上書きを防ぐ場合は、Microsoft 社が提供する「フォルダーアクセスの制御」を有効にする[13]。
- このようなデータ破壊型マルウェア攻撃が一斉に発生するタイミングは、外交や軍事における緊張の高まりと同期している。下記のような 2022 年 1 月 13 日前後のウクライナ情勢に関する外交の状況を理解し、近い将来の日本周辺での軍事的緊張に備える。
    - 2022 年 1 月 10 日、米国とロシア両政府は、スイス・ジュネーブで「戦略的安定性に関する対話」を開催し、ウクライナ情勢について協議した。ロシアは北大西洋条約機構（NATO）の東方不拡大の保証を要求した。米国はこれを拒否し、ウクライナ国境周辺に展開するロシア軍部隊の撤収を改めて求めた。これらの主張の隔たりは大きく、議論は平行線をたどった。
    - 2022 年 1 月 12 日、NATO とロシアは、ベルギー・ブリュッセルで

---

[12].Destructive malware targeting Ukrainian organizations（2022 年 1 月 15 日、Microsoft）
https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

[13].制御されたフォルダー アクセスを有効にする
https://docs.microsoft.com/ja-jp/microsoft-365/security/defender-endpoint/enable-controlled-folders?view=o365-worldwide

「NATO・ロシア理事会会合[14]」を開催した。ロシアは、ロシアの安全保障上、NATO が加盟国を増やして拡大することは受け入れられないと主張した。NATO はこれを拒否し、東方不拡大の保証はできないと改めて強調し、双方の隔たりは埋まらなかった。

- 2022 年 1 月 13 日、欧州安全保障協力機構（OSCE）は、オーストリア・ウィーンで「常任理事会（欧州、北米、旧ソ連他全 57 加盟国）」を開き、ウクライナ国境に集まるロシア軍によって緊張が高まるウクライナ情勢について協議した。ロシアは、NATO の東方不拡大の保証要求に加え、ウクライナやジョージアの NATO 加盟を認めないこと、東欧に配備した NATO の部隊や兵器を撤去すること、NATO のミサイル配備の規制や軍事演習を制限することを要求した。米国と NATO はこれらをすべて拒否し、「NATO の門戸開放政策[15]」の原則に基づいて東方不拡大は問題外とした。

おわりに

ロシア軍によるウクライナの主要都市への物理破壊が本格化するまでに、ウクライナが経験したサイバー攻撃は、多種多様でありながら、その観測と分析から推定できる攻撃者の意図や狙いは、「攻撃準備のための偵察」、「恐怖心や不安感の植え付け」、「システム機能の破壊」となっていた。

本コラムでは触れなかったが、ウクライナに対するウェブサイト改ざんや DDoS 攻撃の発生と同時に、不自然な SNS による意図的な拡散や、SMS（ショートメッセージサービス）による巧妙なメッセージ配信により、ウクライナ人を特定の行動に仕向けるような情報工作も行われた。

日本は、9 年ほど前の 2013 年に初めてサイバーセキュリティ戦略[16] を策定し、さまざまな政府機関が努力を積み重ねてきた。しかしながら、最近の日本の企業におけるランサムウェア攻撃や Emotet マルウェアの被害増加を眺める限り、これまでおよび現在の戦略に基づく施策は、結果として、国民や企業を守ることができないことが露呈した。この背景や理由はさまざまであると考えられるが、筆者は、日本は国家としてサイバー脅威を直視し、徹底的に理解しようと努力する姿勢が乏しく、施策を客観的に評価して新たな施策に反映させる仕組みが弱いため、迫りくるサイバー脅威から、国家を守るという強い意志を具現化した態勢を作りづらくしていると見ている。

---

[14].NATO・ロシア理事会とは、NATO とロシアが、国際テロ対策などで協調するために 2002 年に設立された共同意思決定機関。

[15].NATO の「門戸開放政策」は、同盟の創設文書である北大西洋条約（1949 年）の第 10 条に基づいている。同条約は、「この条約の原則を推進し、北大西洋地域の安全保障に貢献する立場にある欧州の国」であれば、NATO への加盟が可能であると定めている。また、拡大に関するいかなる決定も「全会一致で」行わなければならない。
https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-enlargement-eng.pdf

[16].サイバーセキュリティ戦略（2013 年 6 月 10 日、情報セキュリティ政策会議）
https://www.nisc.go.jp/pdf/policy/kihon-s/cyber-security-senryaku-set.pdf

このような日本における弱いサイバー脅威への態勢は、「多数の日本企業がサイバー攻撃による甚大な被害を受けている」という、日本国民の誰もが理解できるような事象が立て続けに発生するまで続くと考えている。その理由は、日本における自然災害に対する素晴らしい態勢が整備および維持されている背景に、数多くの命・身体・財産に対する大きな犠牲があり、ほとんどの国民がそれらを理解および強い問題意識をもったことで、国家としての態勢整備（特に責任の所在の明確化、指揮命令系統の整備、継続的な訓練の実施等）や予算確保がされているためである。そして、痛ましい経験を忘れないようにする、関係機関（特に報道機関）の献身的な努力もある。

そのため、日本の企業は、セキュリティ担当部門ではなく、経営層自らが、組織と従業員の利益を守るために、実際に発生しているサイバー脅威の有り様を理解する努力を継続的に行う必要がある。多くのセキュリティ担当部門は、すでに十分に脅威の現状を理解していながら、社内調整や経営層の理解獲得に強い困難を感じ、一部では諦めの雰囲気さえ出している。

経営層による「サイバーリスクのためのリーダーシップの発揮」や「セキュリティの投資」という判断や行動は、（部下などの）他者から説得されて実現するものでも、業界や競合他社からの同調圧力で行うものでもないはずである。もしそうだとしたら、恥を知らなければならない。サイバー脅威から組織や従業員を守りたいという強い思いが前提となる。そして、私たちは一瞬で全てを失うという大きなリスクのある「デジタル」に、ビジネスを委ね始めていることを改めて認識し、今後の日本におけるサイバー脅威への強い態勢の実現につなげていただきたい。

本コラムが、そのような「サイバー脅威」の本質的理解の一助になればと願っている。

以上