PwC's Cyber Security Insights 2021

Cyber Intelligence

pwc

www.pwc.com/jp

はじめに

2021年に予定されるデジタル庁新設に見られるように、デジタルトランスフォーメーションの波は官民を問わず押し寄せており、ビジネスとITがさらに密接に結びついていくことは明らかです。これに伴い、サイバーセキュリティの重要性もますます高まっていくと考えられます。単に自組織の情報資産を守りビジネスを継続するためというだけでなく、社会や顧客から信頼されることで企業価値を高めていくためにサイバーセキュリティは必要不可欠なものとなっていくでしょう。

一方で、攻撃者は次々と新しい手口や脆弱性を利用した攻撃を仕掛け私たちを悩ませています。限られたリソースの中であふれる情報に振り回されることなく新たな攻撃に対処し続けていくには、「自組織の目的と活用方法に沿った意思決定のための情報」＝「脅威インテリジェンス」の活用が鍵となります。

脅威インテリジェンスの中でも、リソースの割り当てや組織戦略といった長期的な意思決定に関わる情報を「ストラテジック型脅威インテリジェンス」と呼んでいます。これには、政治・経済・社会・技術などのマクロ要因と、サイバー攻撃の背景・傾向・動機、および新しい戦術といった関連動向とを分析した情報が含まれます。このようなインテリジェンスを活用することで自組織が標的となり得る脅威を特定し、攻撃の目的や戦術に応じた対策を講じることが可能になります。

本レポートでは、国家の経済政策やセキュリティ戦略を背景とするストラテジック型脅威インテリジェンスとして、自動車産業をターゲットとする攻撃とICS（Industrial Control System）のセキュリティを取り上げました。また、新しい技術の普及に伴う脅威動向として、次世代メッセージサービスRCS（Rich Communication Services）とキャッシュレス決済のセキュリティリスクを解説しています。また、攻撃者の戦術については、人間の「脆弱性」を突くソーシャル・エンジニアリングの手法を紹介しました。二重恐喝型ランサムウェアは、新型コロナウイルス感染拡大以前から存在していましたが、リモートワークの普及という社会の変化に乗じて攻撃を活発化させた事例だと言えるでしょう。

これらの事例から得られる示唆が、脅威インテリジェンスを活用した効果的なセキュリティ対策を講じるための一助となれば幸いです。

Agenda

1 自動車産業をターゲットにするサイバー攻撃
——中国の一帯一路構想に呼応する脅威アクター 4

2 狙われるRCS
——次世代メッセージサービスが運び込んだ、
新しくも古い脆弱性 7

3 危機に瀕する日本のICSセキュリティ
狙われるPLC 12

4 キャッシュレス社会
システム会社のエンジニアが狙われている 17

5 日本企業のビジネス環境を織り込んだサイバー攻撃
——古典的テクニックでありながらも
すり抜けてしまうのはなぜか 21

6 リモートワーク導入により高まる
二重恐喝型ランサムウェアの脅威 26

1 自動車産業をターゲットにするサイバー攻撃 ——中国の一帯一路構想に呼応する脅威アクター

サイバー攻撃の動機は社会経済活動と連動

近年、国家の経済政策と関連し、長期にわたり計画的に行われるサイバー攻撃が世界で増加している。いわゆる高度で継続的に脅威を与えるAPT（Advanced Persistent Threat）を他国に仕掛けることで技術情報などを盗み出し、経済的な便益につなげようとする試みである。これらは必ずしも当該国自身あるいは関係機関の犯行とは言えない。当該国に情報を売りつけるために他国の情報を盗むハッカー集団も存在するからである。

ここ数年、日本の自動車メーカーおよびその関連企業はサイバー攻撃の標的となっている可能性が高い。国内組織が標的となるだけでなく、海外の現地法人や工場も攻撃を受けている。一見すると無差別かつ広範に攻撃が行われているようであるが、果たして本当にそうなのであるか。

現代は軍事や政治、経済や文化などの情報が国家間の競争に密接かつ統合的に活用されている。APTが観測された場合、社会経済的な動きと連動している可能性が高いのである。そのため、まず攻撃の背景にある社会経済的な変化を整理する。

技術革新を強く推進する一帯一路の進展

世界の経済を牽引している中国は、アジアと欧州をつなぐ陸路および海路での物流ルートを作り、貿易を活性化させる取り組みである一帯一路を通じて、新興国の市場を活性化している。中国は一帯一路を提唱して以来、既に125の国と29の国際機関との間で計173の契約を締結しており[1]、日本企業が海外で活動する場合、一帯一路と無関係でいることはもはや難しい状況である。

さらに中国は一帯一路に含まれる「デジタル・シルクロード構想」に基づき、アジアとアフリカを結ぶ海底ケーブルを敷設したり、測位衛星を打ち上げたりと、デジタル化推進の旗振り役としても存在感を示している。現在、世界で最も多くの測位衛星を保有しているのは中国である。北斗衛星導航系統（北斗衛星測位システム）と呼ばれ、多くのスマートフォンやカーナビゲーションなどで利用されている。次世代通信規格である5Gは中国企業が市場を占める割合が高い状況にあり、また中国企業が主導するeWTP（Electronic World Trade Platform）と呼ばれる国際電子商取引のプラットフォームや中国人民銀行による中央銀行デジタル通貨（CBDC：Central Bank Digital Currency）の整備も着々と進んでいる。日本企業が世界市場を相手にすることは、中国と接点を持つことと言っても過言ではないであろう。

自動車産業がサイバー攻撃に注意しなければならない理由

自動車産業においても中国の台頭は目覚ましく、2025年に販売台数において世界のトップ10に数社を食い込ませることを計画している。自動車は情報インフラの一部として機能することが想定されており、中国のデジタル・シルクロード構想にとっても重要な要素である。加えて中国では高速道路を代替滑走路として使うことも多く、一帯一路関係国の道路と自動車を押さえることは、軍事的にも意味を持つ。

自動車産業は今、2つの大きな変化に直面している。1つはガソリン車から電気自動車（EV）への移行、もう1つは発展途上国の道路整備に伴う市場の拡大である。この2つの変化は、新興企業のシェア拡大など業界再編を引き起こすと考えられている。こうした時期に技術開発やマーケティング活動で市場をリードすることは重要であり、競合企業の情報を手に入れたいニーズが極めて高いと言えるであろう。さまざまな産業の中でも自動車産業が特にサイバー攻撃への注意が必要な理由は、ここにある。

近年の自動車産業においては、一帯一路に呼応すると思われるサイバー攻撃も観測されるようになった。

モンゴルを例に挙げてみよう。同国では一帯一路の一環である「中国・モンゴル・ロシア経済回廊」によって、高速道路などのインフラ整備が急速に進み、自動車市場が拡大しているのである。モンゴルの自動車市場では、これまでは韓国車と日本車が大きなマーケットシェアを有していた。これらを背景に、モンゴルや、韓国、日本をターゲットにしたサイバー攻撃が増加したと考えられる。

サイバー攻撃の特徴から見る脅威アクター像

サイバー攻撃を背景および他事象との関係性に着目して分析することで攻撃者（脅威アクター）の特徴を知り、その由来を把握することができる。

一帯一路の中でも、モンゴル・ロシア・中国経済回廊に関連する脅威アクターは、PKPLUG、TONTO、TA428などである。

PKPLUGは過去6年以上活動を続けている脅威アクターで、そのターゲットは一帯一路に関係ある地域やASEAN、中国内の自治区などである。TONTOのターゲットは韓国と日本、TA428のターゲットはモンゴルである。

TONTOとTA428はいずれも、中国由来の脅威アクターが、東アジア圏への攻撃でよく利用するRoyal Road RTF Weaponizer（8.t）と呼ばれるツールを利用している。（図表1）

このツールを利用する他のアクターはベトナム、米国、フィリピン、ロシア、カンボジア、カザフスタンなどをターゲットにしている。これらのことから、上述のモンゴルに関連したサイバー攻撃も、中国の経済活動＝一帯一路と密接にリンクしていると考えられる。

とはいえ、全ての攻撃が国家やそれに呼応する脅威アクターによるものとは限らない。例えばベトナム由来のサイバー攻撃には民間企業の関与が疑われている。また、カナダの大学の研究機関に民間諜報企業が工作を仕掛けた事件では、その研究機関から批判を受けていた国の民間企業の関与が強く疑われている。国が関与せずとも、民間企業が民間諜報企業に依頼して情報収集や工作を行うことできる時代になっているのである。

図表1：Royal Road RTF Weaponizer（8.t）の動作の一例

社会経済活動とリンクしたサイバー攻撃を予知するには

経済活動とリンクしたサイバー攻撃では、中国だけでなくベトナムなどを拠点とした脅威アクターによるものも報告されている。現代においては経済活動の一部にサイバー攻撃が組み込まれていると言っても過言ではなく、特に新興国市場に参入する際には、企業は市場での競争だけでなく、サイバー攻撃にもさらされると考えた方がよいであろう。市場調査あるいはプロモーションを行うように、新興国の状況に合わせたサイバー攻撃への対策をあらかじめ講じることが、もはや必須となっているのである。

ではサイバー攻撃に対して、社会経済的要因を踏まえて総合的に対処するために、企業はどのようなアクションを取ればよいのであろうか。

重要なことは、技術や攻撃トレンドだけでなく、自社に関係する社会経済動向に注意し、呼応して発生し得るサイバー攻撃の可能性と脅威アクター、そしてそれに対する効果的な対処方法（サイバープレイブック）を事前に用意しておくことである。

自動車産業の場合は前述の通り、EV化や自動化、新興国での市場拡大という変化と、これとリンクしたサイバー攻撃に備える必要がある。注意しなければならないのは、攻撃を受ける可能性があるのは本社だけではない点である。自社製品がよく売れている国や、工場のある国で攻撃を受ける可能性もあるのである。

現地と日本本社とが連携し、攻撃を検知できない可能性がある箇所のリスクシナリオを想定し、モニタリングの強化をはじめとする対策を迅速に講じる必要があろう。

今回のポイント

1
一帯一路参加国に進出している企業はサイバー攻撃へリスクが高まるとの認識のもと、攻撃シナリオの想定やモニタリング強化、サイバープレイブックの用意などが必要。

2
本社だけではなく、工場や現地法人なども攻撃対象となる。現地と日本本社との連携の強化が必要。

3
民間企業が主導するサイバー攻撃の動きにも注意が必要であり、幅広い脅威情報の確認が不可欠。

2 狙われるRCS —次世代メッセージサービスが運び込んだ、新しくも古い脆弱性

次世代のメッセージサービス、台頭の予感

企業と一般消費者の取引であるB2C（Business to Customer）のコミュニケーションにおいては現在、ショートメッセージサービス（SMS）が最も普及しているツールとされている[2]。

一方で、近年このSMSの代替を目的とした高機能なサービスとして、新しいコミュニケーションツールであるRCS（Rich Communication Services）が世界的に活用され始めているのである。

従来のテキストメッセージのみならず、ビデオ通話やファイルの共有なども可能にするRCSの利用には電気通信事業者（通信キャリア）のサポートが必要であるが、2019年12月、米国では通信キャリアが未対応の場合でも国内でRCSを利用可能とした[3]。既に英国やフランス、メキシコでは同様の仕組みで、RCSの提供が開始されている。

日本国内でも大手通信キャリア3社が『+メッセージ』としてRCSサービスを導入し、2018年の3社同時ローンチの時点から、3社間の完全な相互運用性を実現しているのである。

同3社は、2019年7月にユーザーが1,000万人を突破したことを発表しており[4]、またある調査では、2020年の終わりまでに1,750万人に上り、2023年までには4,200万人を超えると予測されている[2]。また、消費者は受信したRCSメッセージの85%以上を開封し、RCSメッセージからのクリックスルー率はSMSや電子メールの場合に比べて40%以上高くなっているとも言われている[2]。

2019年5月以降に発売されたAndroidスマートフォンには+メッセージアプリがあらかじめインストールされており、それ以前のAndroidやiOS向けにダウンロード可能なアプリも既に展開・利用されている[5]。+メッセージはレストランや携帯電話販売店の予約といった企業と消費者のコミュニケーションに活用されており、今後は金銭の授受、例えばオンラインショップの決済、電気料金など生活インフラの決済、交通系ICカードのチャージなどに利用が拡大すると考えられる。

企業はRCS公式アカウントを開設することで、アプリの追加開発なしにパーソナライズされたメッセージを消費者に送信でき、インタラクティブに対応をすることができる。ユーザー数の増加と高い開封率により、今後、RCS利用企業による消費者とのコミュニケーションを主軸としたビジネス展開が加速すると予想されるのである。

RCSの出現・台頭によって、企業と消費者とのコミュニケーションの在り方が、大きく変わり始めている。しかし同時に考慮しなければならないことがある。B2CにおいてRCS利用企業と不特定多数の消費者との金銭の授受をも担うであろうRCSは、サイバー攻撃の標的とされる可能性が高いとも考えられているのである。

RCSとSMSで異なる通信方式

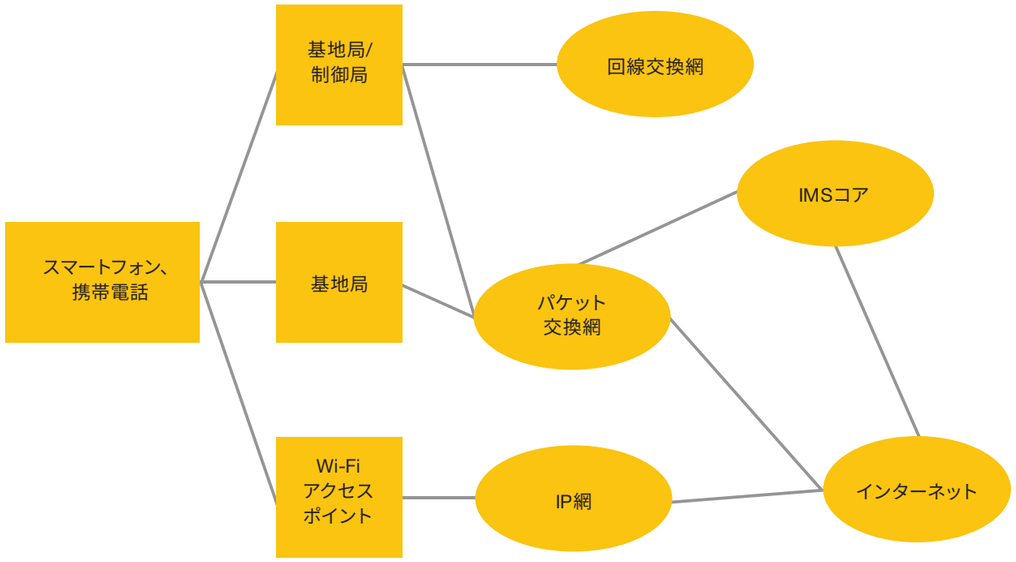
RCSがいかにしてサイバー攻撃の標的になり得るのか、その仕組みを見ていこう。RCSは、通信端末を電話番号で識別する。SMSと同様に送信者／受信者は通信キャリアによって事前に審査・認証されるため、安全に使用できると考えられている。

RCSとSMSで異なる部分は、通信方式である。

SMSは、通信キャリアの回線交換ネットワーク（電話に使われる方式）を通信に使用する。一方でRCSは、IMS（IP Multimedia Subsystem）を用いてIP上でHTTPとSIP（Session Initiation Protocol）により実装され、通信キャリアのパケット交換ネットワークを通信に使用する（受信者がRCSをサポートしていない場合は、SMS／MMSでの配信となるのである）。通信キャリアが提供する回線交換・パケット交換ネットワークで通信をしている限りは、悪意ある第三者が一般的なPC単体で通信を傍受、改ざんすることは困難で、特別な機器や専門知識・技術が必要となるのである。

しかし、パケット交換によるデータ通信は、自宅や外部のWi-Fiアクセスポイントに接続して行われる可能性があるのである。消費者の中には、通信キャリアによって制限されている月々のデータ通信量を超えないように、自宅や公共施設など、可能な場所ではWi-Fiアクセスポイントからインターネットへの接続を試みる人もいるであろう。この場合、RCSプロトコル、アプリケーションの設計・実装次第では一般的なWi-Fiセキュリティと同様、通信の傍受、改ざんなどのリスクが生じる可能性があるのである。

図表2：回線の全体像



セキュリティリスクが存在するWi-Fiインフラを消費者が知らずに利用する可能性

Wi-Fiインフラのサイバーリスクを消費者の観点で見た場合、大きく2種類の古典的な脅威源が存在する。

1つ目は、脆弱なWi-Fiアクセスポイントの利用である。これはオープンシステム認証、WEP（Wi-Fi Protected Access）のような脆弱な暗号化・認証方式や、事前共有鍵が事実上公知な状態で運用されているアクセスポイント（カフェなどで散見される）の利用、アクセスポイント自体がアクセス制限不備やセキュリティパッチ未適用などの脆弱な状態で運用されており、それを利用してしまうといったケースが挙げられる。

2つ目は、悪意あるWi-Fiアクセスポイントの利用である。悪意ある第三者が正規アクセスポイントを装った偽のアクセスポイントを設置し、ユーザーがだまされて当該アクセスポイントに接続してしまうケースが挙げられるのである。

こうしたケースでは、攻撃者によるWi-Fi通信の盗聴、改ざん、なりすましの攻撃を受ける可能性がある。対策としては、HTTPS、VPN（Virtual Private Network）の利用などが挙げられる。

しかし上述のような脅威と対策は、あくまでWi-Fiインフラを利用する消費者観点のものである。RCS利用企業は、消費者がRCSの通信にどのような通信やインフラを利用するかを選択・制限することはできない。そのため企業は、RCSを利用したサービスをプランニングする段階から、こうした脅威の全体像を踏まえてサービスを設計することが求められるのである。

RCS特有のセキュリティ上の懸念事項

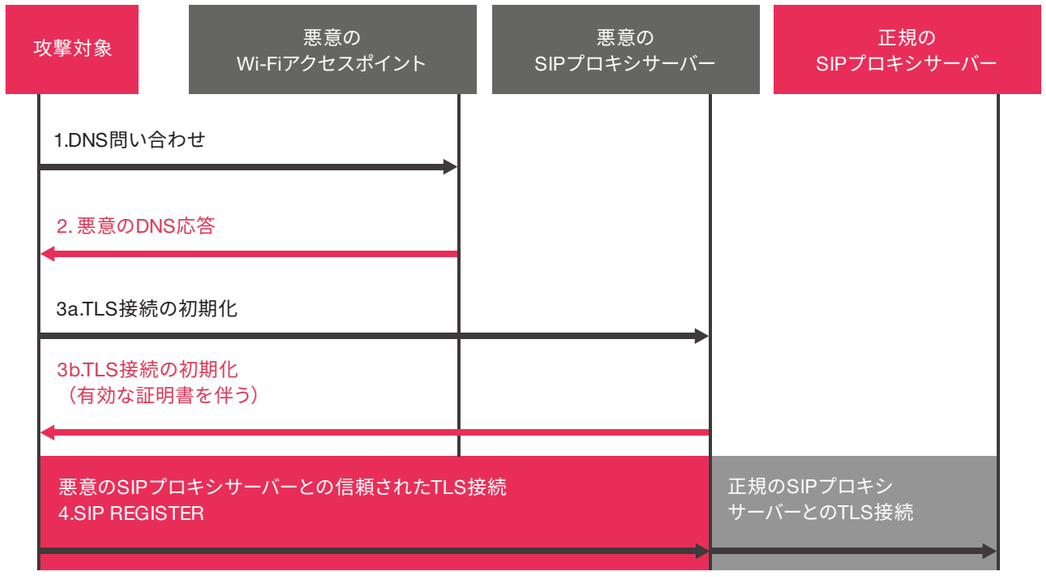
Wi-Fiインフラにセキュリティリスクが存在する場合でも、End-to-Endの強力な暗号化が施されていれば、一般的に通信を傍受されることはない。しかしRCSでは、RCSクライアントとサーバー間でのTLSによる通信の暗号化はサポートされているものの、クライアント間でのEnd-to-Endの暗号化は提供されない。そのため、原理的にはRCSサーバーおよび経路上で中継・保存される通信データを盗聴される可能性がある。SMSでは、SMSクライアントからのデータを受信するSMSC（SMSセンター）サーバーを標的とした攻撃が報告されており[6]、RCSでも今後、同様の攻撃が発生することが想定されるのである。

また2019年、ドイツの研究機関SRLabs[7]によってRCSの実装の一例が検証され、世界的に普及するRCS対応のアプリでさえドメインと証明書の検証が十分とは言えず、DNSスプーフィングによる比較的単純な中間者攻撃によりRCSのテキスト／通話の傍受や改ざん、発信者IDのなりすましなど、RCSハイジャッキングが可能である、と指摘された[8]。

加えて、多くのネットワークではRCSの機能をアクティブにするためのプロビジョニング（SIM＜加入者を特定するためのID番号が記録されたICカード＞を利用した認証および初期設定）プロセスが十分に保護されていないため、攻撃者はSIPおよびHTTP資格情報を含むRCS構成ファイルを盗み、ユーザーアカウントを完全に乗っ取ることが可能とも指摘されている。これらは、RCSがSMSと同じ通信方式であれば問題視されなかったであろう。しかしRCSはIP上で実装され、消費者はWi-Fiインフラを介してRCSサーバーに接続する可能性がある。この例では、Wi-Fi環境下におけるRCS通信に対して従来の攻撃手法が転用されたと言えるのである。

このことから、Android端末にプリインストールされるRCSがWi-Fiセキュリティ上の懸念を拡大させ、スマートフォンを利用するほぼ全ての消費者を、SMSでは心配する必要がなかった脅威にさらすことになった、との声も聞かれる。こうした事態に、SRLabsは強い懸念を示しているのである。

図表3：攻撃のイメージ



RCS利用企業が実施を検討すべき、セキュリティ上の問題の軽減策

SRLabsが指摘した脆弱性はあくまで実装上の問題であり、RCSを展開している各国の通信キャリア全てが同じ脆弱性を持つとは言えない。しかし、実装の問題で同じ脆弱性が発生し得るのであれば、RCS利用企業は常にこの問題を念頭に置いて、サービスを開発・展開・運用する必要があるのである。

SRLabsは通信キャリア向けに、ベストプラクティスとして以下のリスク軽減策を提言している。

- SIMやセキュアエレメントを利用した認証、強力なパスワードの利用など、プロビジョニングプロセスの保護
- 送信元IPアドレス、Cookieなどに基づいたSIPセッションの検証、通信データからの機微情報の削除、アップロード制限などのRCSサービス上の対策
- 信頼できるドメイン／証明書のみ接続を許可し、信頼できる証明書の連鎖（Chain of Trust）を使用するなどの、RCS利用企業側の対策

RCSは今後も利用拡大が見込まれるため、サービスの普及と共に新たな脅威が明らかになる可能性がある。RCS利用企業は、こうした脅威動向、さらには国内の対応動向を認識した上で、RCSを利用したサービスを設計・運用していくことが重要となるのである。

今回のポイント

1
RCSはSMSと異なり、Wi-Fi接続を介したインターネット経由で通信される場合がある。通信環境やRCSプロトコル、アプリケーションの設計・実装次第では、盗聴・改ざん・なりすましといった攻撃を受ける可能性がある。

2
ドイツでは、RCS実装の不備を悪用した攻撃が既に実証されている。

3
RCS利用企業は、脅威動向および国内の対応動向を把握し、キャリアと連携してサービスを検討することが必要である。

3 危機に瀕する日本のICSセキュリティ 狙われるPLC

攻撃の標的となる日本のICSセキュリティ

産業用制御システム（ICS）セキュリティに対する脅威が近年、特に高まっている。直近の事案として、イランとイスラエルにおける制御システムにサイバー攻撃が発生し、国家安全保障に対する攻撃の一部であったと報道されている[9]。また、米国の産業制御システムサイバー緊急事態対応チーム（ICS-CERT）のアドバイザリー件数は、2010年に18件だったのが2019年には231件と約13倍に増加した。また2019年のICSへの攻撃は、2018年と比較すると2,000%増という異常な伸びを見せた[10]。これまでもICSセキュリティは重要な課題であったが、現在はより深刻さを増し、重要度が高まっていると言えるであろう。その脅威はサイバー攻撃によって社会や経済に深刻な被害をもたらすものとなっている。

2018年ごろからBlack Hatをはじめとするサイバーセキュリティカンファレンスでも、ICSセキュリティに関する発表が増加している。日本企業およびその製品もターゲットとなっているが、残念ながら国内の多くの企業は、依然ICSセキュリティへの危機意識は薄くICSを狙う攻撃グループの実態を理解しきれていないと言わざるを得ず、格好の標的になっている可能性がある。

深刻な被害をもたらすICSへのサイバー攻撃、その手口とは

近年、ひときわ注目を集めたのはTRITONと呼ばれる攻撃フレームワークである[11]。2017年、このサイバー攻撃によって石油化学プラントが停止した。ターゲットになったのは重電メーカーの安全計装システム（SIS：Safety Instrumented System）の脆弱性であった。同社のPLC（Programmable Logic Controller：工場などの機械を自動的に制御する装置）は数多くの日本の企業で使用され、SISについては世界中のプラントで採用されているシステムであることから、その脅威は深刻である。

あるセキュリティ企業の報告によると、2019年の段階でHEXANE、PARISITE、WASSONITEなど11の攻撃グループが活動しており、その脅威は米国とアジア・太平洋地域で増大し、日本もターゲットに含まれている[12]。

報告によればITシステムとOTシステムをブリッジして侵入するもの、リモートアクセスの際に利用するVPN（Virtual Private Network）の脆弱性を突くもの、サプライチェーンを狙うものなどさまざまな攻撃手法が確認されている。ITシステムとOTシステムがネットワークで結ばれているシステムが増えていることから、この2つをブリッジして攻撃を行う手法が特に広がっている。

各国のセキュリティ基準を満たさない製品は排除されるのか

こうした攻撃の激化に対して、米国や欧州を中心として対策が本格化してきている。これは同時に、米国が2019年に一部の外国製通信機器の締め出したように、安全保障上のセキュリティ問題のある製品の排除につながる。今後の購買や調達において一定の基準を満たさない製品やサービスは不利な立場になり、排除されることが予想される。

米国ではNIST（国立標準技術研究所）が2015年に「産業用制御システム（ICS）セキュリティガイド」SP800-82Rev2を、2017年にセキュリティ基準SP800-171を公開した。米国政府機関と取引するために、企業にはSP800-171への準拠が求められることになった。

この基準では米国政府が定める機密情報以外の重要情報（CUI：Controlled Unclassified Information）を扱う企業や研究機関が対象になる。CUIにはヘルスケア情報や通信基地局の通信データなど、広範なデータが含まれ、ヘルスケア情報を保有する医療施設や貴重な研究データのある研究施設もこの対象となる。また、重要インフラの設備情報も対象となっており（ICSに侵入された場合、その設備の物理構成やシステム構成が漏えいする可能性が高いため）、情報を保護するための物理セキュリティとしてビル管理システムや監視システムも含まれている。

自社製品に使われている他社製品なども対象となり、さらにその他社製品に使われている製品も対象となるため、対象になる企業は莫大なものとなる。日本の防衛省も防衛調達にこの基準を採用することになり、対象となる企業は9,000社に上ると言われている。米国政府あるいは日本の防衛省と直接取引をしていなくても、サプライチェーンの中に組み込まれている企業は全て対象となるため、知らない間に準拠を求められていたという日本企業も少なくないであろう。

EUで は2016年7月6日 にNIS指 令（「The Directive on Security of Network and Information Systems」＜ネットワークと情報システムのセキュリティに関する指令＞）が成立した。加盟各国に指令に準拠した法令を整備することを求めるもので、既にEU各国は法令の整備を行っている。NIS指令はエネルギー、運輸、医療、水道などの重要インフラ事業者を対象としており、ICS製品やサービス事業者にとって無視できないものとなっている。この法律が定めるセキュリティ基準を満たさない場合、2021年6月28日以降は処罰されることになる。最大2,000万ユーロまたは企業における全世界の売上高の4%を罰金として課される。

これらは世界各地で進んでいるICSセキュリティ強化の一例に過ぎない。今後、さらにICSセキュリティ向上のための法令や制度が整備されていき、製品やサービスはそれらへの準拠が求められることになることは明白である。

中国やロシアはICSに対する研究に力を注いでおり、世界中のPLC（Programmable Logic Controller）の脆弱性を調査していると言われている。現に、中国を拠点とする研究者によるICSセキュリティに関する論文は年々増加している。中国とロシアが今後、脆弱性のある製品を購買しなくなる可能性も十分に考えられる。ICSセキュリティへの対応の遅れはこうした国々でのビジネスを妨げる要因になりかねず、さらに言えば、今後の世界経済の中心になる可能性があるアフリカや中南米市場を失うことにもつながる危険があるのである。

国家をあげたICSセキュリティ研究が進行中

前述のように、世界各国はICSセキュリティに注力するようになっている。その中でも特にロシアと中国の動きは目覚ましく、世界をリードしていると言っても過言ではない。ロシアや中国は、重要な課題となっているICSセキュリティの研究に国家をあげて取り組んでおり、ベストプラクティスと呼んでもよいであろう。

ロシアでは中央科学研究機構（CNIIHM＝the Central Scientific Research Institute of Chemistry and Mechanics）がICSセキュリティに関する研究を行っている。雑誌『MIT Technology Review』で「世界で最も殺人的なマルウェア」と評されたTRITONやAPTへの関与が疑われているほどである[10]。

中国でも大学や研究機関をもとに構成される国家重点実験室（State Key Laboratory：SKL）をはじめとし、ICSセキュリティの研究が活発化している。同実験室には「学科国家重点実験室」、「企業国家重点実験室」と「省部共建国家重点実験室」の3つの研究拠点がある。この中で、制御理論やシステム工学などを研究する産業制御技術国家重点実験室のテーマには「ICSセキュリティ」が加えられ、また産業情報技術省重点実験室の研究テーマに「ネットワークセキュリティ」が加えられるなど、セキュリティ研究にシフトしていることが分かる。この動きは、5月に開催された中国両会において、産業用インターネットが今後のキーワードの1つとして挙げられていることから、さらに強化されることが予想される。

また、SKLでは組織の枠を超えた連携が実現されており、中国のトップレベルの大学の頭脳が結集して研究に当たっている。海外から優秀な研究者を招聘する「千人計画」にも組み込まれていることからも、力の入れ方が伺える。研究結果の一部は脆弱性報告として当該メーカーへ報告されている。

各国の研究で興味深いのは、中国に関わらず、これらの国営研究機関には、安全保障に関連する組織も関与していることである。ICSが今後の各国の経済成長に影響を与えることは、米国や中国の経済摩擦の状況に鑑みても明らかである。つまり、ICSセキュリティは、自国の経済活動を停止させないためにも重要な要素といえ、これまで以上に対策が求められるようになると予想される。

ロシアと中国の詳細な研究内容は明らかではないが、こうした分野の研究を行う以上、レッドチームが必要になることから攻撃手法およびゼロデイ脆弱性の研究を行っている可能性が高いと言えるであろう。特にICSセキュリティの要の1つであるPLCについては世界中の製品を集めて、研究を行っていると言われている。当然、日本のPLCも対象であると考えられる。

同様の研究は米国をはじめとする各国でも行われており、国、民間、研究機関が連携している。

図表4：PLCをターゲットにした脆弱性、マルウェアの例

名称	ターゲット	
Rogue7	電子縄器メーカーのオートメーションシステム	2019，米国，Black Hat発表
URGENT ／ 11	組み込みシステム向けリアルタイムオペレーティングシステム	2019，米国セキュリティベンダーが公開
PLC Blaster	電子機器メーカーのオートメーションシステム	2016，米国，Black Hat発表

大幅に立ち遅れた日本企業

日本においては技術研究組合制御システムセキュリティセンター（CSSC）、経済産業省の産業サイバーセキュリティ研究会、情報処理推進機構（IPA）の産業サイバーセキュリティセンターおよび産業技術総合研究所サイバーフィジカルセキュリティセンター（CPSEC）などをはじめとする各機関が、ICSセキュリティの向上と啓発に努めている。また、経産省が提唱する「Connected Industries」においてもICSセキュリティが重要な課題として挙げられ、国土交通省、厚生労働省などをはじめとする各省庁も真剣に取り組んでいる。

ICSセキュリティは民間企業の課題である以上に安全保障上の問題であり、米国やロシア、中国のように国家が民間と連携して横断的、統合的に取り組む必要があるものである。残念ながら日本の体制はそこまでには達しておらず、省庁や官民学の枠を超えた連携は今後の課題である。

民間企業への啓発も遅れており、脆弱性報告があってもすぐに対応できない、あるいは一部しか対応できないといったことは珍しくない。インターネット上では、脆弱性のある日本企業の製品が他の日本企業に使われていたり、パスワードをハードコーディングしている製品が存在したりする事実が公にされている。こうした状況は、一刻も早く改善されなければならない。

中でも、各国で研究が進んでいるPLCを製造する企業は注意が必要である。研究が進んでいるということは、攻撃に悪用されかねない脆弱性が発見される頻度が増えるとともに、その脆弱性を持つ製品が購買や調達から外される可能性をはらんでいるからである。

ICSセキュリティの早急な体制確立のために

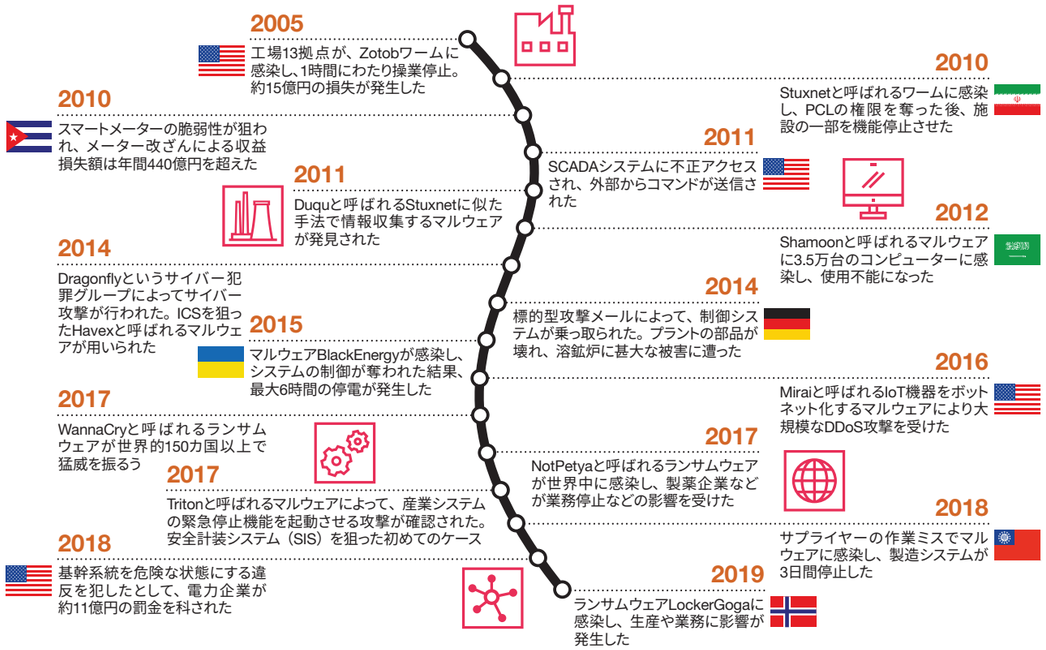
日本政府を中心とした取り組みは行われてはいるものの、目の前の脅威に対抗できる状態には至っていないのが現状と言わざるを得ない。日本全体での有効な枠組みが出来上がるまでは、企業自ら、身を守るための対処をしなければならない。特に重点的に研究が行われ、攻撃も増加しているPLCのメーカーや利用企業は、早急な体制の確立が必要である。そのためには脅威情報の収集とその適切な活用が重要と考えられる。

ICSセキュリティの脆弱性対応とパッチマネジメントにはITセキュリティとは違う、特有の大きな問題がある。脆弱性もパッチも、必要かつ検証されたものだけを適切なタイミングで迅速に対応しなければならないのである。2019年に行われたセキュリティ企業主催のあるセミナーでは、報告されているICSセキュリティ脆弱性の64％は実際にはリスクを引き起こさず、さらに34％は不正確と指摘されている[13]。

日本ではICSセキュリティ関係の脆弱性が積極的に報告もしくは公開されていないのが実情である。これにより、報告されている脆弱性だけでは十分な対処を行えない可能性がある。

脅威情報を活用することで、狙われている機器や脆弱性、攻撃方法を事前に察知し、備えることができる。また、攻撃グループの狙いを知ることも防御の上では役に立つ。ICSセキュリティは、緒に就いたばかりである。各国あるいは攻撃グループが研究している内容が実戦に投入されるこれからが本番と言えるであろう。

図表5：工場・発電所などへのサイバー攻撃



4 キャッシュレス社会 システム会社のエンジニアが狙われている

加速するキャッシュレス決済の普及

現在、世界的にキャッシュレス決済が推進され、既に私たちの日常生活にも浸透した。

経済産業省の『キャッシュレス・ビジョン』[14] によると、各国のキャッシュレス政策はさまざまな事情から実施されており、結果として経済状況を大きく好転させていることが分かる。

キャッシュレス決済は主にカード決済（クレジット、デビット、プリペイド）／電子マネー決済（ICカード、スマートフォン）／QRコード決済（スマートフォン）に分類され、特に後者2つは急速に市場を拡大している。

キャッシュレス化の進展によって、支払いデータの利活用による消費の活性化や、実店舗などの無人・省力化、不透明な現金の流通の抑止による税収向上などにつながることが期待されている[14]。今後も日本は政府主導のトップダウンによる強いキャッシュレス推進により、飛躍的にキャッシュレス決済の普及が進むと考えられる。

共有・悪用され続ける流出情報、パスワードリスト攻撃の危険性

このような中、経済産業省・金融庁・個人情報保護委員会による「キャッシュレス決済機能を提供する事業者の皆様への注意喚起」にも記載があるように、パスワードリスト攻撃の危険性が指摘されている[15]。パスワードリスト攻撃とは、サイバー攻撃により情報流出したIDとパスワードの組み合わせを用いて、他のウェブサイトや電子マネーアカウントなどへのログイン試行を繰り返すものである。

ここ数年、オンラインショップをはじめとする多数のウェブサービスからログインID／パスワードなどのアカウント情報が流出し続けている[16]。攻撃者は無差別に脆弱なウェブサイトを探索し、手当たり次第に攻撃していると思われ、一見サイバー攻撃被害とは縁の薄そうな、地方の観光情報サイトや行政サイトなどの一般ウェブサービスからの流出情報も多く見受けられる。こうして流出する情報の中には、流出の公式アナウンスやユーザーへの通知がなく、そもそも運営企業が攻撃を受けた事実に気付いていないと思われるものも含まれる。流出に至る経緯はさまざまであるが、一度流出した情報はダークウェブなどで共有・販売され、ネット上から消えることはない。

しかし、運営企業がサービスを安全に設計すれば攻撃の緩和は可能と思われ、また利用者がパスワードの使い回しを行わなければ他サービスへの2次被害を緩和できるとも考えられる。

以下に利用者／事業会社（ウェブサービスなどの運営企業）／システム開発会社それぞれが置かれている状況を整理し、どのように対応していくべきか、示唆を述べる。

【利用者】
2段階認証サービスの利用で安全なキャッシュレス利用を

私たちが日常的に利用している各種ウェブサービスや電子マネーアカウントなどは、常に悪意のある犯罪者による攻撃の脅威にさらされている。利用者は、インターネット上に登録された自分の情報が流出して公開されてしまうことを前提として、自分の身を守るための最低限の努力をする必要がある。

強力なパスワードを設定することは、効果的な手段の1つである。情報流出は、誰の身にも起こり得ることである。パスワードを複数のサービスで使い回さず、また簡単に推測可能な一般的な単語などを避け、長い文字列を選択することで漏えいのリスクを軽減する必要がある。

また、IDおよびパスワードのみでログイン認証を行うウェブサービスの利用は控えること、IDとパスワードは上述の通り、推測可能文字列を使わずに、二段階認証などの安全なログイン方法を活用することが望ましいと考えられる。

【事業会社】
セキュアな認証機構の導入を

経済産業省や総務省によるパスワードリスト攻撃への注意喚起もあり[15・17]、中小企業にもパスワードリスト攻撃の存在と手法が徐々に認識され始めた。同攻撃の代表的な事例として、キャッシュレス決済サービスへの不正アクセスが挙げられる。これは、他社サービスから流出したID・パスワードを使用してログイン試行が繰り返されたことによる被害と判明している。脆弱な認証システムにより、攻撃に対する防御力が弱体化しているところを狙われた。また、大手企業のウェブサービスにおいて、外部からのパスワードリスト攻撃により、数千件を超えるアカウントが不正にログインされるという事象が発生した。どちらも二段階認証などのセキュアな認証システムを導入していれば、未然に防げた可能性のある事例である。IDとパスワードのみでログイン可能な認証は避け、二段階認証やワンタイムパスワード、CAPTCHA認証など、よりセキュアなシステムを構築・運用する必要があると考えられる。

【システム開発会社】
バージョン管理システムの利用に細心の注意を

ITシステムの開発会社は、バージョン管理システムの利用に注意する必要がある。

2019年、あるオンラインショップのアプリケーションのソースコードがバージョン管理システム上で外部公開されているのが見つかり、話題となった[18]。

セキュアなオンラインバージョン管理システムを利用していたとしても、公開リポジトリにソースコードやパスワードなどの機密情報をプッシュしている例は多く見られる。バージョン管理システムは、情報漏えいに気付いた利用者が削除したつもりでも実際には削除されずに復旧可能な場合が多く、攻撃者は日常的にこれらの情報を探索している。

外部公開される可能性のあるオンラインシステムを、機密データを含むバージョン管理システムとして利用することは避ける必要がある。

狙われるエンジニアをいかに守るか

同時にシステム開発会社は、自社のエンジニアの保護にも力を入れる必要がある。2019年10月以降、北朝鮮が関与していると言われる悪意のあるハッカー集団・Lazarus Groupによるサイバー攻撃が、仮想通貨事業者を中心に、複数の国で観測・報告されている。北朝鮮の外貨獲得活動の一環と言われるこの活動は、金融分野の技術者を標的として行われており、近年増加傾向にあるものである。

観測された攻撃キャンペーンでは、リクルーティング会社の社員を装った攻撃者が金融分野の開発者に対して、ビジネス特化型のSNSのメッセージ機能を通じてヘッドハンティングをかたって攻撃を行ったことが確認されている。同SNS上の当該アカウントが、同名のアカウントを乗っ取ったものなのか、実際の攻撃への協力者であるかは不明であるが、プロフィールに記載された所属組織への在籍は確認されていない。なお、同名のアカウントは、他の複数のSNSにも存在していた（図表6）。

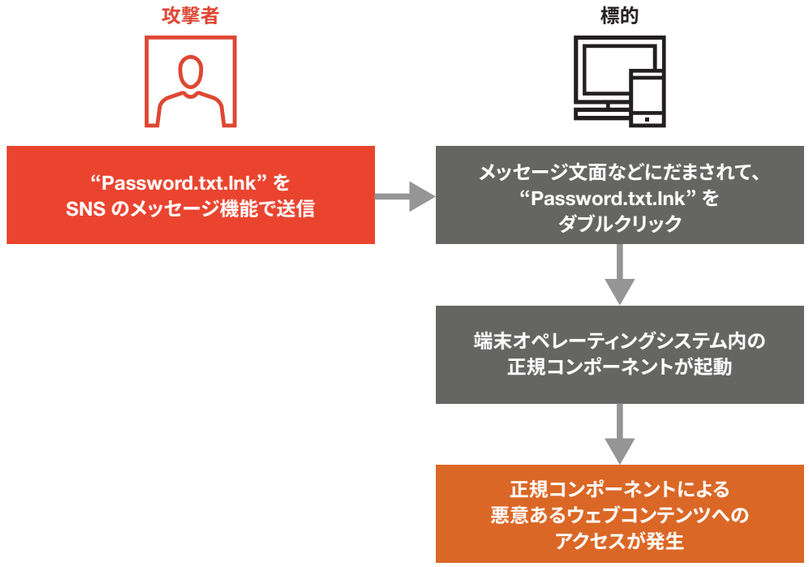
こうしたビジネス特化型SNSのメッセージ機能を利用した攻撃は、2019年1月に報告されたチリの金融サービス事業者へのサイバー攻撃でも使われており、Lazarus Groupが金融分野の技術者を標的とする際に好んで利用する手口である。

攻撃には、「Password.txt.lnk」というファイル名のショートカットファイルが悪用されている。標的に当該ショートカットファイルをクリックさせることで、オペレーティングシステム（OS）内に標準で存在する正規システムコンポーネントを起動させ、当該コンポーネントを介して、インターネット上の悪意あるウェブコンテンツへのアクセスを発生させるという手法である（図表7）。同様のショートカットファイルを悪用した攻撃は2019年にも、メールの添付ファイルを使用したものが観測されている。両者のサンプルを比較すると同一の構造であることが分かる。

このようにLazarus Groupの攻撃の標的は、明らかにシステム開発者および運用者へと向き始めている。SNSとメールの併用が主な攻撃手法であると考えられており、開発会社は従業員に対して、SNS上で開示できる情報とできない情報をセキュリティ方針として定義し、SNS経由の情報流出やこうした攻撃に注意していく必要がある。

図表6：攻撃者のアカウント情報イメージ

図表7：SNSのメッセージ機能を利用した攻撃の流れ



今回のポイント

1
キャッシュレス社会の到来と並行して、パスワードリスト攻撃の脅威が増加している。

2
現状、各種ウェブサービスなどからは恒常的に情報が流出し続け、それがダークウェブ上で拡散している。これを止める手段は事実上存在しない。

3
システム開発会社は従業員に対して、SNS上で開示できる情報とできない情報をセキュリティ方針として定義し、SNS経由の情報流出やサイバー攻撃に注意していく必要がある。

5 日本企業のビジネス環境を織り込んだサイバー攻撃 ―古典的テクニックでありながらもすり抜けてしまうのはなぜか

サイバー攻撃では情報量や対象範囲の広さの差から攻撃者が有利な状況であり、CISO（Chief Information Security Officer）などのセキュリティ担当責任者は、より積極的なサイバー攻撃への防御戦略を策定しなければならない。PwC's Cyber Intelligenceでは、今後のリスク要因の特定を支援するため、スレットインテリジェンスとその背景にある攻撃者の動向を解説する。

狙われ続ける人間の「脆弱性」

この10年ほど、マルウェアを用いた情報漏えいやランサムウェアによる被害の多くは、メール添付ファイルの閲覧や不審なWebサイトへのアクセスなど、ユーザーによる受動的なアクションが攻撃の起点となっている。

特にマルウェア感染の9割が、一般企業が業務で利用するメールに起因するという統計が複数確認されている[19]。日々、セキュリティ技術が進歩し、その導入も進んでいる中であっても、このトレンドは継続していくことが予想される。個々のセキュリティ対策製品の性能が向上しても、それらを組み合わせて有効なセキュリティ対策にすること、また、その対策を有効に活用できることは別の問題だからである。

信頼と関心で「ユーザー自身を操作」する攻撃者

2020年6月、北朝鮮が関与していると言われる攻撃者グループであるLazarus Groupが、新型コロナウイルス感染症（COVID-19）に便乗した大規模なフィッシングメール攻撃を、日本を含む6カ国に対して計画していたことが報告された[20]。こうした時勢に応じた攻撃は、過去に東日本大震災などでも確認されている。

昨今では、こうした出所が不確かなメールはスパムフィルタにはじかれてしまうことが多く、高度なセキュリティ対策を実施している企業や組織では、メールによる添付ファイルの受信さえ制限している。しかし、そのような環境でも、比較的容易に攻撃を成功させることができる余地は残る。ちなみに、送信ドメイン認証の仕組みであるSPF／DKIM／DMARCといった技術の導入は、DNS（Domain Name System）設定による不具合への不安などから、JPドメイン名における送信ドメイン認証技術の設定率は低いものとなっている[21]。

このような不特定多数に配信されるスパムとは異なり、攻撃者が特定のユーザー（担当者）に添付ファイルを開かせるために必要なことは、まず、本文を読んでもらうことである。一般的な企業・組織の採用・顧客対応といった部門では、送信元が不特定であっても業務上、メールを読むことは避けられない。そのため、攻撃者がこうした窓口の担当者にマルウェアを送り込もうとすることは、必定と言える。

当然、担当者も攻撃を疑う可能性がある。攻撃者はそうした場合に備えて、事前にSNSなどの交流サイトを通じて、実在する人物になりすまして担当者の信頼を得ようとする。また、メールの送受信でも、ソーシャル・エンジニアリングの手法が発揮される。1通目のメールでは、編集ができない形式のファイルを意図的に文字化けした状態で送り、「文字化けして見えない」という返信を担当者から引き出した後、「文字化けしない方法が分からないため元のドキュメントファイルを送ります。パスワードは別送します」といった日本の組織特有の暗号化ZIP添付メールの慣習（後述）のように、マルウェアを添付したメールを送信し、添付ファイルを開くように誘導する。こうした攻撃は、主にAPT（Advanced Persistent Threat）の初期フェーズで行われており、目にする機会は限られている。

別の事例として、メールに添付されたドキュメントに、図8のようなメッセージが1行だけ記載されているといったものも紹介する。

ドキュメントの本文には“This Document was created using older version, please click options in the security warning above and Enable Content to view”という記載がされており、閲覧ソフトウエアの設定を変更してドキュメントのマクロ機能の有効化を誘うものとなっている。このようなマクロを有効にしないと閲覧できないドキュメントを作成して送ることは、通常だと考え難い行為であろう。しかし、「見ることができない」と思うと、つい見たくなる心理が働かないとは言い切れない。

また、こうした添付メールの暗号化対策として、企業や組織がドキュメントを自己解凍アーカイブに埋め込み、送信するといった対策製品を導入しているケースもある。こうした環境では、標的となる担当者の関心とは無関係に、添付ファイルを閲覧するために操作が必要と認知され、上記のような設定変更の誘導に対して心理的抵抗が低くなる可能性がある。

さらに、攻撃者は攻撃対象となる国の商習慣にも敏感である。日本では特に、添付ファイルをメールで送る際はパスワード付き圧縮ファイルとして送り、その後パスワードを別送する、という商習慣がある。これは、プライバシーマーク制度の導入に伴い、認証取得の審査項目として、個人情報を含む添付ファイルをメール送信する際の対策が求められるようになったことが要因として考えられる。

このパスワード付き圧縮ファイルを作成するためには、パスワード付き圧縮ファイルを生成できるソフトウエアが必要である。しかし、このパスワードを用いた暗号化機能がオペレーティングシステムの標準機能でサポートされていない場合、日本語に対応したフリーソフトウエアのサードパーティ製ファイルアーカイバを利用するケースが多く見受けられる。攻撃者は、このファイルアーカイバの脆弱性や、サポートするアーカイブ形式が増えることを利用する、といったことも行う。

図表8：ドキュメントに記載されたメッセージ

This document was created using cyber version, please click options in the security warning above and Enable Content to view.

他にも、APT攻撃と言われている、標的を定めた無差別でない攻撃で利用されている、RTF（Rich Text Format）フォーマットに多数のオブジェクトを埋め込むことができる仕様を用いた攻撃手法がある[22]。これらの攻撃では、主にオフィススイートのコンポーネントを狙う。オペレーティングシステムが最新であっても、既存業務やシステムとの相互運用性を考慮し、業務端末に1世代または2世代古いオフィススイートがインストールされている・利用されている場合に、こうした攻撃の影響を受ける可能性がある。この脆弱性を悪用して起こる数式エディタへの攻撃は、90%以上が日本に集中しているとの報告もある。例えば、COM（Common Object Model）コンポーネントとして独立したプロセスで実行されるため、アンチウイルスソフトウェアなどのエンドポイント対策製品による監視から漏れることがあり、攻撃者に好んで利用されている。

図表9：オフィススイートの脆弱性の例

オフィススイートで利用するソフトウェアコンポーネントの処理に存在する脆弱性
ワードプロセッシングソフトウェアに対するリモートからコード実行の脆弱性
外部URLから取得したリソースの処理に起因する脆弱性
数式エディタに関する脆弱性
数式エディタの脆弱性に対する修正漏れ

他にも昨今、ドキュメントのテンプレートをネットワーク上から取得し、テンプレート内に同梱されているマクロを悪用した攻撃が確認されている[23]。攻撃者は、まずネットワーク上に攻撃用のマクロを含んだ文書テンプレートを事前に設置する。次に、当該ドキュメントテンプレートへの参照を含んだ、特別に細工した攻撃用ドキュメントを作成し、標的に添付ファイルとしてメールで送信する。本文などによりだまされた特定のユーザー（担当者）が当該ドキュメントファイルを開くと、オフィススイートの仕様により、自動的に参照先であるドキュメントテンプレートが取得され、同梱されたマクロが実行される。この攻撃では、標的がメールで受信した攻撃用ドキュメントファイル自体にはマクロが含まれておらず、従来のアンチウイルスソフトウェアなどで当該ドキュメントファイルを検査するだけではマルウェアとして検知できない恐れがある。

セキュリティ製品にとって苦手なファイル形式

ここまで攻撃側の巧妙な手口を解説してきたが、防御側の技術も日々、進化している。最新のオペレーティングシステムでは、サードパーティのアンチウイルスソフトウェアを支援するための機能が提供されており、ドキュメントに同梱されたマクロを実行する直前に検査するといった機能も提供されている。アンチウイルスソフトウェアも、従来のようなウイルス定義ファイルに依存したパターンマッチングに留まらず、機械学習やディープラーニング（深層学習）といった技術の実用化が進んでいる。また、メールの添付ファイルをメールサーバー上あるいはネットワーク上に設置したサンドボックス製品で検査するといった対策ソリューションも隆盛を極めている。

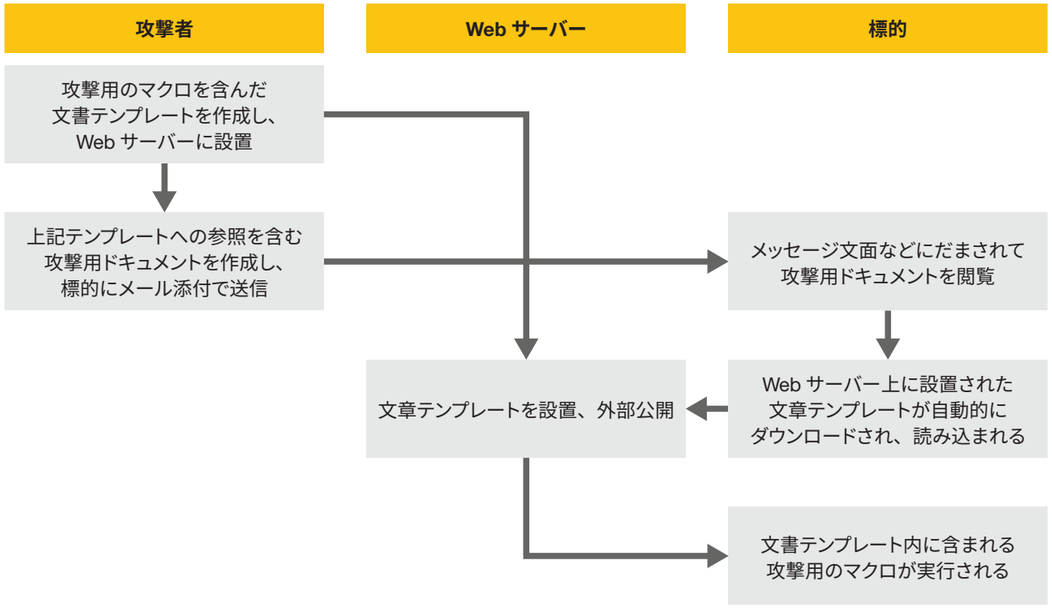
しかし、古今東西、攻撃側が優位であるという原則を覆すには至っていない。例えば、2016年ごろから、ショートカットリンク（.lnk）を用いて、ユーザーにマルウェア起動を促す攻撃が盛んに行われている[24]。

ショートカットリンクの利用は、攻撃者にとって以下の利点がある。

- 標的の業務端末にインストールされているアプリケーションのアイコンを使って、アイコンを偽装することができる。
- コマンドラインインターフェイス経由ではなく、オペレーティングシステム標準シェル経由での実行となる。そのため、例えばWebアクセス用の正規コンポーネントへのショートカットにインターネットURLを引数に指定し実行することで、エンドポイント対策製品による検知を回避することが期待される。
- ファイル自体の情報量が少なく、またアンチウイルスソフトウェアなどで検知される可能性が低い。

こうした攻撃は、サンドボックス製品などによる検査が最善策となるが、パスワード付き圧縮ファイルで暗号化されていた場合、チェックをすり抜ける可能性がある。

図表10：文章テンプレートを使った攻撃の流れ



セキュリティ投資を無駄なく有効に割り当てるためには

特筆すべきは、攻撃者が、日本で広く利用されているパスワード付き圧縮ファイルでの添付ファイルの送受信などの商習慣を把握し、人間心理を巧みに突いて攻撃してきていることである。セキュリティ対策を導入していても、商習慣やビジネスルールによってその機能が十分に活用されていない場合、攻撃者はそうした事情を織り込んで攻撃を行ってくる。そのため企業や組織は、セキュリティ対策製品を導入するだけでなく、その効果を最大化するためのビジネスルールの見直しも併せて実施することが求められる。特に、昨今の急速な在宅勤務（リモートワーク）の導入・普及により、リモートでの業務環境と既存のビジネスルールに不整合が生じている可能性が考えられる。

どのような対策を導入しても、人間による運用は切り離すことができない。操作ログの取得と保存といった、事前にインシデント発生時のトレーサビリティを確保することも重要となる。

6 リモートワーク導入により高まる二重恐喝型ランサムウェアの脅威

サイバー攻撃では情報量や対象範囲の広さの差から攻撃者が有利な状況であり、CISO（Chief Information Security Officer）などのセキュリティ担当責任者は、より積極的なサイバー攻撃への防御戦略を策定しなければならない。PwC's Cyber Intelligenceでは、今後のリスク要因の特定を支援するため、スレットインテリジェンスとその背景にある攻撃者の動向を解説する。

リモートワークの普及が招く新たなセキュリティリスク

新型コロナウイルス感染症（COVID-19）の影響で、在宅勤務をはじめとするリモートワークを導入する企業が増加した。しかし、普及が急に進んだため、セキュリティ面に多くの課題を残したままの企業は少なくない。今回は、リモートワークにまつわるセキュリティ上の脅威を概観すると共に、特に注目すべき動向として二重恐喝型ランサムウェアの脅威を取り上げる。

リモートワークは、十分なセキュリティ上の備えがないと思わぬ危険を招くきっかけになる。単純に攻撃者の侵入ポイントを考えただけでも、図表11のように、オフィスワークと比べると格段に多くなることが分かる。気を付けなければならないのは、家庭内ネットワーク（同一セグメント）に端末を接続している同居人の端末からも侵入を許す可能性があるということである。同じネットワーク内で共有を許可している場合、そこから攻撃される危険があるのである（シェアハウスなども、同様に他の住人の端末などが同一セグメントに接続している可能性がある）。悪意はなくとも相手の端末がマルウェアに感染し、意図せず被害を広げてしまうというケースは多々存在している。

オフィスで仕事をしていた際はシステム管理者の責任範囲だった侵入ポイントが、リモートワークになった途端、個人の責任となる。オフィス内で業務を行う場合と自宅で業務を行う場合では、自宅の場合の方が、個人で保全しなければならないポイントがはるかに増加する。

実際、COVID-19によるパンデミックをテーマとした詐欺、フィッシング、マルウェア攻撃の報告が、2020年3月の最初の2週間だけで5倍に増加したことが分かっている[25]。企業はリモートワークの普及に伴い、これまでに対峙してこなかったリスクに直面している。今こそ、こうした一連の新たなリスクに対するリスクシナリオを想定しておくことが求められる。

拡大する二重恐喝ランサムウェアの脅威

リモートワークのリスクの中でも最近、特に注目されているのがランサムウェアである。リモートワークの普及に伴い、ランサムウェアはおよそ7倍以上に増加したと言われており、深刻な脅威となっている[25]。以下に、その背景と手口を紹介する。

二重恐喝型ランサムウェアを支えるビジネスモデルRaaS（ランサムウェア・アズ・ア・サービス）

脅威拡大の背景にはランサムウェアのビジネスとしての拡大がある。2016年から2018年にかけて活動の目立ったSamSamと呼ばれるランサムウェアは1件当たり約100万円から500万円を得ており、合計で約6億5,000万円を手にしたと推計されている[26]。ランサムウェアがビジネスとして確立したのは、技術の高くない攻撃者でも容易に参入できるツールが揃ったためと報じられている[27]。その中核となっているのが、二重恐喝型のランサムウェアと、それを支えるRaaS（ランサムウェア・アズ・ア・サービス）である。

二重恐喝型のランサムウェアは、感染した相手に「復号してほしければ身代金を払え」という恐喝と、「払わなければデータをインターネット上に公開する」という2つの恐喝を行う。身代金を受け取った後に情報公開の脅迫を重ねて行うものや、身代金を支払わなかった場合にオークションにかけるといったバリエーションがある。

ランサムウェアの広範な拡散を実現するRaaS採用モデル

あるコンピューターヘルプサイトでは、およそ20のランサムウェアが紹介されている[28]。しかし、20のランサムウェアが20の攻撃アクターを意味するわけではないのが、新しいランサムウェアの怖いところである。

最近活発な二重恐喝型のランサムウェアであるSodinokibi（別名REvil）やNetWalkerなどはRaaSを採用している。この2例においては、RaaSを運営する組織（RaaSオペレー

図表11：オフィスワークとリモートワークの侵入のポイントの比較

侵入ポイント		オフィスワーク	リモートワーク	攻撃の例
本人	メール	○	○	フィッシング
	インスタントメッセンジャー	○	○	フィッシング
	SNS	○	○	フィッシング
	Web	○	○	ドライブバイダウンロードなど
	VPN		○	漏えいした認証情報によるなりすまし
	ホームルーター		○	DNSハイジャック
	ホームネットワーク		○	同一セグメント（同居人）の端末からの攻撃
	スマートフォン（BYOD）		○	フィッシング
	タブレット（BYOD）		○	フィッシング
	公衆Wi-Fi		○	脆弱性を突いた攻撃
	AI音声アシスタント		○	非可聴音によるコマンドインジェクションなど
同居人	メール		○	フィッシング
	メッセンジャー		○	フィッシング
	SNS		○	フィッシング
	Web		○	ドライブバイダウンロードなど
	スマホ		○	フィッシング
	タブレット		○	フィッシング
	ゲーム機		○	フィッシング
	AI音声アシスタント		○	非可聴音によるコマンドインジェクションなど

ター）と、それを利用してランサムウェアを拡散するグループが分離している。拡散するグループは複数存在し、それぞれ異なる方法で拡散し、アフィリエイトで稼ぐ。つまり20のランサムウェアがあった場合、攻撃に加担するグループは20よりはるかに多くなる。アフィリエイターも多い分、収益が拡大する可能性も高くなり、さらにビジネスの規模が拡大するということになる。

積極的にビジネスネットワークを拡大するRaaS収益モデル

RaaSを採用していたランサムウェアGandCrabは2019年5月、200億円以上の収益を上げたことを公開し、そのサービスを終了した[29]。十分な利益を得たことが理由と考えられている。GandCrabは代表的なランサムウェアの中でも1件当たりの要求金額は低い方で、約10万円から80万円であった[26]。仮に平均40万円とすると、5万回以上、身代金の受け取りに成功したことになる。

RaaSオペレーターはアフィリエイター募集広告をアンダーグラウンドのフォーラムに出すなど、積極的にビジネスネットワークを拡大している。あるセキュリティベンダーの調査によると、アフィリエイターの取り分はNetWalkerの場合、20%～80%と言われる[30]。NetWalkerは2020年3月からの四半期でおよそ25億円相当の仮想通貨を受け取っており、少なくとも5億円以上がアフィリエイターたちの手に渡ったことになる。

世界で広がるRaaSを活用した多様な攻撃

攻撃者が増えれば、攻撃方法も多様になる。例えば2015年に英国や米国で数十億円に及ぶ被害を出したマルウェアDridexは金融機関をターゲットにしており、現在はRaaSオペレーターと連携するようになっている。同じくマルウェアのEmotetはランサムウェアRyukのRaaSオペレーターと連携することがある。手動で侵入してランサムウェアを仕込むこともある（2020年、アルゼンチンのインターネットサービスプロバイダーがランサムウェアRyukに感染させられた際の攻撃は手動で行われたことが報告されている[31]）。

また近年、内部犯行による情報漏えい事件が増加している。2020年における情報セキュリティ脅威の第2位が内部不正である[32]。内部関係者がRaaSの仕組みを利用して、自社もしくは取引先の企業のデータをランサムウェアの餌食にする可能性があるのである。盗み出したデータを自分自身で現金化することは通常の従業員にはハードルが高く感じられるであろうが、RaaSを利用すれば脅迫と現金化を代行してくれる。社内のサーバーのアクセスログが取られていなかったり、詳細でなかったりする場合、共有資料にRaaSと連携するマルウェアを仕込んでおくだけで済むため、この手軽さが犯行の増加に拍車をかけていると考えられる。

ダークウェブで告知を行う二重恐喝型ランサムウェア

こうした二重恐喝型ランサムウェアを用いた脅迫や情報流出は、ダークウェブで告知される。いくつかの事例を紹介しよう。

あるサイトでは、ランサムウェアで暗号化したデータと同じものを盗み出した証拠に、そこに含まれている個人情報（氏名、パスポートの写真、IDカードなど）と盗み出したファイルの一覧を公開し、72時間以内に身代金を支払うよう要求していた。このサイトは誰でもアクセスできる状態だったため、企業は被害を受けたことが広く知られることになってしまう。

別のサイトでは身代金の要求先である企業（彼らは「クライアント」と呼んでいる）の一覧があり、非協力的（身代金の支払いに応じていない）なクライアントのデータの一部を公開している。データを持っている証拠として掲載している場合もあれば、徐々に公開するデータを増やしていくという恐喝の場合もある。

また、盗み出したデータをオークションにかけるサイトもある。米国の法律事務所がクライアントになった事例では、20億円以上の身代金が要求された。同事務所の顧客には著名人が含まれていたため、データの最高入札金額は40億円を超えた。

ダークウェブのランサムウェアのサイトには日本企業のクライアントもあり、データも公開されている。二重恐喝型ランサムウェアの脅威は決してひとごとではない。リモートワークの普及によって侵入ポイントが増えた分、攻撃方法の種類も増えていくのは間違いない。盗まれた自社データがオークションにかけられたり、被害を隠ぺいしていてもダークウェブでクライアントとして掲示されたりすることは、これまではあまり考えられなかったことである。防御側は、変化し多様化するリスクを反映したリスクシナリオを用意し、万全なセキュリティ対策を講じる必要がある。

リスクシナリオの見直しをはじめとする対処が急務

これまで紹介したように、リモートワークの拡大は、リスクの拡大につながる可能性をはらんでいる。攻撃者は既にリモートワークをターゲットにした攻撃を展開していることが判明している。以下に、企業が行うべき内容をまとめる。

リスクシナリオの見直し

攻撃対象領域（アタックサーフェイス）を最小化するのは防御の基本であるが、リモートワーク導入は攻撃対象領域を拡大してしまう。エンドユーザーの端末経由で侵入される可能性が増大するため、侵入ポイントごとに想定されるリスクと影響範囲を整理しておく必要がある。特に、シナリオごとに被害を受ける情報の範囲を把握することが重要である。

ISO31000（リスク管理の国際規格）に基づくリスク管理の一環として、リモートワークにおける最悪のシナリオを見出し、理解しておくことが、企業内部において利用可能なリソースと仕組みを最大限活用できる態勢を整えることにつながる。これにより、万が一のインシデント発生に伴う被害を最小限にすることが期待できる。

新しいリスクシナリオに対応した対策の作成

新しいリスクシナリオに対応したエンドユーザー権限やアクセス範囲の見直し、ガイドラインの策定や教育が必要となる。特に、リモートワークはオフィスワークに比べて、エンドユーザーが留意しなければならない範囲が拡大したという事実と、適切な管理方法を従業員に伝えることが重要である。

侵入された際にいち早く検知し、被害を最小に抑えるために、新しいリスクシナリオに対応したログ管理、ネットワーク監視、エンドポイント監視などの仕組みを整えておく必要もある。2020年9月に公開されたデータ保護・保全のガイドラインNIST SP 1800-11では、ランサムウェアなどによるデータ完全性侵害に対して組織が具備すべきケイパビリティ、リファレンスモデル、テストケースなどが記載されている。リスクシナリオの見直し結果に基づき現状のセキュリティ対策の妥当性を確認する上で、参考にすることが可能である。

また、データの完全性侵害に留まらず二重恐喝ランサムウェアによって暗号化・窃取された情報の漏えい被害を抑えるためには、IRM（Information Rights Management）などの対策が有効である。

事後対応体制と事業継続計画の見直し

特に二重恐喝型ランサムウェアを想定した身代金の支払いの可否を含めた事後対応体制と事業継続計画、データバックアップ体制の見直しが必要になる。システム関係部門だけではなく、経営者および法務、広報など複数の部門が一体となって事態に対処する体制を、事前に構築する。

身代金について触れておくと、一般的に考えれば、身代金は支払うべきではない。その理由は大きく2つある。身代金が攻撃者の収入源となりさらなる犯罪を誘発することと、身代金を払ってもデータが公開されない保証はないことである。しかし前者に関しては、オークションにかけて身代金以外で資金を得ることが可能になっており、犯罪抑止効果は薄れている。身代金を支払う会社が少なくないことは、ランサムウェアの増加の相関関係により推定できる。支払うか支払わないかの選択を迫られることのないよう、あらかじめの防御態勢の構築が不可欠である。

COVID-19がもたらした働き方の変化や通信技術の発達により、オフィス以外で働くのが当たり前の時代が来ることが予想される。オンラインでの商談や会議も一般的になることであろう。オンライン会議についてのリスクと対処方法に関しては米国国土安全保障省サイバーセキュリティ・インフラストラクチャ セキュリティ庁がビデオ会議やIoTなどについてのTipsやガイドを公開している[33]。その他「事業継続を脅かす新たなランサムウェア攻撃について」[31]に対策をはじめとする記載があるため、参考にしていただきたい。リモートワークは勤務形態の変化であると同時に、企業が抱えるリスクの変化のきっかけでもある。新しいリスクに対応するために、上記で述べたような施策を早急に実施することを推奨する。

おわりに

「はじめに」でも述べましたように、脅威インテリジェンスを「意思決定のための知見」として活用するには、目的と活用方法を明確にすることが重要です。本レポートで解説した脅威インテリジェンスの事例でも、「自組織の産業に対する脅威は何か?」あるいは「自組織に攻撃を仕掛ける脅威アクターは誰か?またその手法は?」といった質問に答えるという要件から出発してリスクを特定し、具体的な対処方法に落とし込んでいます。

脅威インテリジェンスを活用する際は、次のようなサイクルを繰り返すことが重要です。個々の情報はいずれ古くなるため、このサイクルを繰り返して継続的に情報を収集しながらインテリジェンスをアップデートすることが求められます。

1. 計画と指示（Planning & Direction）
2. 収集（Collection）
3. 処理（Processing）
4. 分析・作成（Analysis & Production）
5. 配布・フィードバック（Dissemination & Feedback）

「計画と指示」フェーズでは、意思決定者の要件に基づいてインテリジェンス生成計画を立案し、情報収集の指示を出します。「収集」フェーズでは内部および外部の情報源を特定し情報を収集します。「処理」フェーズでは生データを分析可能なフォーマットに加工します。加工したデータは「分析・作成」フェーズでインテリジェンスとなり、利用者に配布されます。最後に、インテリジェンスが要件を満たしているかを検証し次のサイクルにフィードバックします。

外部の脅威インテリジェンスサービスを利用する際もこの考え方は変わりません。明確な目的に基づいてサービスを選定しなければ、意思決定と行動に結びつかない単なる「情報」に投資してしまうことになりかねません。

世の中の変化が加速していると言われる中、将来のリスクに備えた効果的なサイバーセキュリティ対策を取るために脅威インテリジェンスの活用が推奨されます。

参考資料

1 China’ s Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism（2019年8月1日、Pacific Forum）
China’ s Digital Silk Road: A Game Changer for Asian Economies（2019年4月30日、THE DIPLOMAT）
2 日本におけるRCSビジネス・メッセージング（2019年12月、GSMA）
3 Sanaz Ahari Lemelson（Senior Director of Product Management at Google）の発表より
4 「+メッセージ（プラスメッセージ）」利用者数が1,000万を突破（2019年8月9日、KDDI株式会社、株式会社NTTドコモ、ソフトバンク株式会社）
5 「+メッセージ」の機能を拡充-携帯電話番号だけで、企業と安心・安全にメッセージのやりとりが可能に-（2019年4月23日、株式会社NTTドコモ、KDDI株式会社、ソフトバンク株式会社）
6 FireEye
7 Security Research Labs
8 The Future of Texting Is Far Too Easy to Hack（2019年12月4日、WIRED）
9 National Cyber Directorate head: Cyber winter is coming
10 X-Force Threat Intelligence Index2020（IBM Security）
11 Triton is the world’ s most murderous malware, and it’ s spreading（2019年3月5日、MIT Technology Review）
12 2019 YEAR IN REVIEW: The ICS Threat Landscape and Activity Groups(Dragos)
13 BRIDGING THE IT AND OT CYBERSECURITY DIVIDE（Dragos）
14 経済産業省商務・サービスグループ消費・流通政策課, キャッシュレス・ビジョン（2020年7月15日閲覧）
15 個人情報保護委員会、金融庁、経済産業省, キャッシュレス決済機能を提供する事業者の皆様への注意喚起（2020年7月15日閲覧）
16 ITmediaエンタープライズ,「 7億7300万件の流出情報、闇フォーラムで流通　平文パスワードも出回る」（2020年7月15日閲覧）
17 総務省, リスト型攻撃対策集について（2020年7月15日閲覧）
18 日 経XTECH,「 オムニ7」アプリのソースコードが流出、7payに続き新たな問題発覚（2020年7月15日閲覧）
19 F-Secure BLOG, 2018年11月12日, ‘Failed delivery spam and other naughty things to watch out for this holiday season’（2020年8月20日閲覧）
20 COINPOST,「 北朝鮮ハッカー集団ラザルス、コロナ給付金を装ったフィッシング詐欺を計画」（2020年7月28日閲覧）
21 I IJ Engineers Blog,「 世界と日本のメール送信ドメイン認証」（2020年7月28日閲覧）
22 Virus Bulletin, ’ Attribution is in the object: using RTF object dimensions to track APT phishing weaponizers’ [Michael, VB2019]（2020年7月28日閲覧）
23 Cisco Japan Blog,「 テンプレート インジェクションを利用した重要インフラへの攻撃」（2020年7月28日閲覧）
24 LAC,「 攻撃者グループmenuPassとマルウェア『Poison Ivy、PlugX、ChChes』の関連性」[JPCERT/CC, 2017] (2020年7月28日閲覧）
25 BitDefender, 2020年.’ Mid-Year Threat Landscape Report 2020’
26 Sophos, 2019年.’ SOPHOSLABS 2019 THREAT REPORT’
27 Forbes, 2019年9月12日. ‘The Big Business Of Cybercrime: The Dark Web’
28 Bleeping Computer, 2020年5月26日. ‘List of ransomware that leaks victims’ stolen files if not paid’
29 eset, 2019年.「 マルウェアレポート2019上半期」
30 McAfee Blog, 2020年8月12日.「 RaaSの進化 ― NetWalkerランサムウェアを調査」
31 独 立行政法人情報処理推進機構 セキュリティセンター , 2020年8月20日.「 事業継続を脅かす新たなランサムウェア攻撃について」
ZD-net, 2020年7月20日. ‘Ransomware gang demands $7.5 million from Argentinian ISP’
32 独 立行政法人情報処理推進機構 セキュリティセンター , 2020年4月.「 情報セキュリティ 10大脅威2020 各脅威の解説資料」
33 Cybersecurity and Infrastructure Security Agency, ‘CYBERSECURITY’

お問い合わせ先

PwC Japanグループ
https://www.pwc.com/jp/ja/contact.html

名和 利男
PwC Japanグループサイバーセキュリティ最高技術顧問

岩井 博樹
PwC Japanグループスレットインテリジェンスアドバイザー

林 和洋
PwCコンサルティング合同会社 パートナー

村上 純一
PwCコンサルティング合同会社 ディレクター

www.pwc.com/jp

発刊年月：2021年1月　　管理番号：I202010-06