NTT DATA
Trusted Global Innovator

グローバルセキュリティ動向四半期レポート

2019 年度　第 4 四半期

NTT DATA
Trusted Global Innovator

目次

1. エグゼグティブサマリー

本レポートは、NTTDATA-CERTが期間中に収集したサイバーセキュリティ関連情報に基づき、その四半期におけるグローバル動向を独自の観点で調査・分析したものです。

コロナウイルス感染拡大とフィッシング攻撃

コロナウイルスの感染拡大に伴い、フィッシング攻撃が増加しています。コロナウイルスの感染状況を確認できるマップを騙ってマルウェアを配布する不正なアプリケーションや、「マスクの無料配布」を知らせるSMS を配信してフィッシング攻撃を行うRoaming Mantisと呼ばれる攻撃グループの活動が多く見られています。攻撃者たちは人々の不安心理を利用する巧妙な手口を用いるため、ユーザが気づかないうちに被害に遭ってしまいやすいのがコロナウイルス関連のフィッシング攻撃の特徴です。しかし、その手口の特徴を知って、情報発信者が確実かつ正しく情報を発信する工夫をすることで、被害を防止することができます。併せて、フィッシングの被害に遭わないために情報受信者が気を付けるポイントをまとめました。

ラテラルムーブメント

2020年1月に、日本の防衛関連企業4社へのサイバー攻撃が発覚しました。その中の1社である三菱電機株式会社の事例は、攻撃者がよく使用する手法への対策は施されていたと想定される環境においても、それでも広範囲にラテラルムーブメントして侵害を広げていることから、高度なサイバー攻撃だったと考えられます。このような攻撃には、侵入されることを前提に、攻撃者の標的である機密情報が保存されているエンドポイントに焦点を当てた対策が有効です。政府組織や防衛関連企業はこのような高度なサイバー攻撃の標的とされやすく、それらの関連組織や取引先企業も同様の高度なサイバー攻撃を受けるおそれがあります。標的組織や企業への直接的な攻撃だけではなく、サプライチェーンを構成する関連組織や取引先企業への攻撃にも気をつける必要があります。

情報暴露型のランサムウェア攻撃

米国においてMazeやSodinokibiなどのランサムウェアの被害が大きな話題となりました。これまでのランサムウェア被害は、暗号化されたファイルの復旧を盾に身代金を要求されるものが中心でしたが、組織から盗み出した情報の暴露を盾に身代金を要求する、情報暴露型のランサムウェアの被害が多く確認されるようになりました。

情報暴露型のランサムウェアによって窃取された情報を取り戻すことは困難であるため、窃取された情報は既に漏えいされたと考えて事後対応策に臨まれる事を推奨します。

今後の予測

2019年度第4四半期は、企業を標的とした「情報暴露型ランサムウェア」による被害が目立ちました。今後も、情報暴露型のランサムウェアが被害の中心となるおそれがあり、その標的が個人へと拡大すると予測します。特に、コロナウイルスは引き続き全世界規模で高い関心を引く話題であり、話題に便乗した攻撃には引き続き警戒が必要です。少しでも不審だと思ったら自身の思い込みで判断せず、第三者の客観的な意見を求めることで、サイバー攻撃から身を守る事を心掛けてください。

また、景気悪化に伴う予算削減により、検討していたセキュリティ対策の中止や延期、現行のセキュリティ運用の縮小などが起こり、セキュリティレベルが低下するおそれがあります。サイバー攻撃は増加している状況ですので、必要なセキュリティレベルを確保するための予算を組み、対策を行うことをお薦めします。

2. 注目トピック

2.1. コロナウイルス感染拡大とフィッシング攻撃

2019年12月以降、コロナウイルスによる感染症が世界中で爆発的な感染拡大を見せています。日々、感染者数の報告やひっ迫する医療現場を支える医療従事者の方々の声、経済対策や、停滞する経済状況への抗議活動の様子などが報道されている中、サイバー空間でも「非常時」特有の動きが確認されています。

地震・台風・ハリケーンなどの大規模な自然災害やテロ、今回のような感染症によるパンデミックが発生して世の中が混乱状態に陥ると、それに便乗したマルウェアの拡散や標的型攻撃、フィッシング攻撃などが増加します。これは、人々の不安感情や支援者の善意につけ入り、認証情報や金銭を窃取することを目的としています。

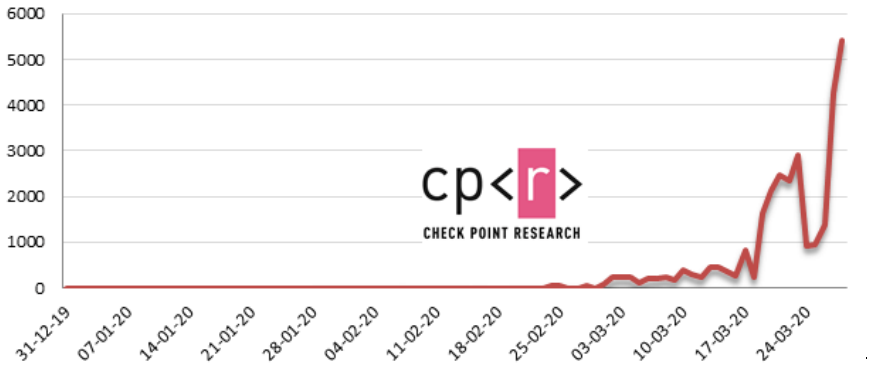


図 1：コロナウイルス関連のサイバー攻撃数の推移 [1]

図 1は、Check Point 社が発表した、自社のソリューションで検知されたコロナウイルスに関連するさまざまな攻撃の件数の増加を示したグラフです。検知した攻撃の約84%が、フィッシングによる攻撃であることが分かっています。Knowbe4 社によると、2020年1～3月にかけて実施したフィッシングメール訓練の結果、コロナウイルス関連の訓練メールに引っかかってしまった人が2番目に多かったことが分かりました。これは、パスワードを即刻確認するように通知する訓練メールに次ぐ件数だったと報告されています [2]。2020年に入り、コロナウイルスに関連するフィッシングメールによる攻撃が6倍に増えていることもあり、同社は、今後も多くの情報を求める人々の心理につけ入る、コロナウイルス関連のフィッシング攻撃が増加するので注意が必要だとコメントしています。

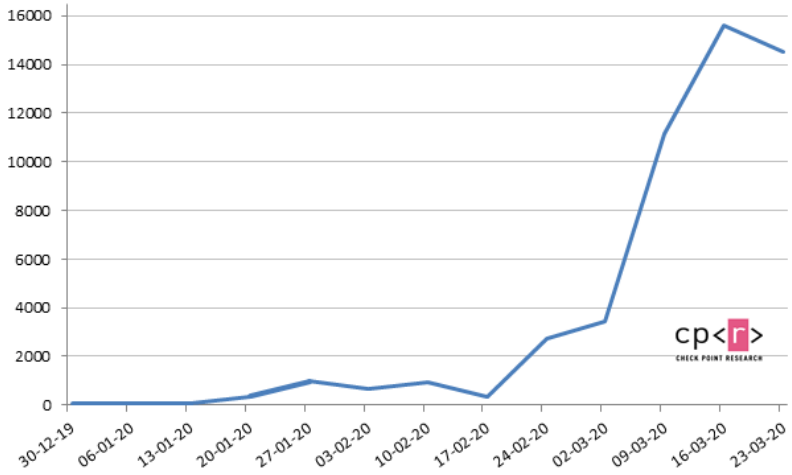


図 2:コロナウイルス関連の新規ドメイン登録数の推移(1週間あたり) [1]

図 2は、Check Point 社がまとめた、コロナウイルス関連のドメインの新規登録数の増加の様子を示したグラフです。縦軸の数値は、新しく登録されたドメインの数を示しています。2020年1月以降、このようなドメインは合計で51,000個以上登録されていることが分かります。図 2のうち、直近の2週間に登録された当該ドメインの中には、悪意のあるドメイン(0.4%)や疑わしいドメイン(9%)が含まれています。コロナウイルス関連のWeb サイトを検索した場合、そのうち10%程度はリスクがあるサイトが表示されるかもしれません。

本レポートでは、手口が巧妙であるために、気が付かないうちに被害に遭ってしまいやすいコロナウイルス関連のフィッシング攻撃について考えてみます。

2.1.1. 不正なアプリケーションの拡散

攻撃者がマルウェアを配布する方法はいくつかありますが、正規のアプリケーションを騙る不正なアプリケーションを、フィッシングサイト上で不正なものとは気が付かずにダウンロードしてしまうことでマルウェア感染が広まってしまうケースが増えています。

「コロナ禍での不正なアプリケーション」

コロナウイルス感染拡大に伴い、ウイルスの流行状況を確認できる「新型コロナウイルス感染マップ」に関連するさまざまなアプリケーションが配布されています。しかしこれらの中には、感染マップを騙った不正なアプリケーションも紛れ込んでいます。不正なアプリケーションを起動してしまうと、スマートフォンがロックされて、解除のために仮想通貨を要求されたり、PC やスマートフォンにAZORult と呼ばれるマルウェアやその亜種がインストールされて個人情報を窃取されたりします [3] [4]。AZORult は、ロシアの地下フォーラムで一般的に販売されている、情報窃取を目的とした商用のトロイの木馬です [5]。エクスプ

ロイトキットやフィッシングメールを介して感染を広げて、ID やパスワード、メールの認証情報、Cookie、ブラウザの履歴、暗号通貨を窃取したり、バックドアとしても機能したりすることが分かっています [6]。AZORult は、2018年7月の北米でのスピアフィッシングキャンペーンに使用されたことが確認されているほか、国内でも、同年11月、東北地方の人々へ送られた気象庁の津波警報を騙るフィッシングメールを介して感染を広げたことが確認されました [7]。表 1に、コロナウイルス感染マップに関連した不正なアプリケーションの例を示します。

表 1:コロナウイルス感染マップに関連した不正なアプリケーションの例

アプリケーション名	標的	概要
Corona-Virus-Map[.]com **[3]**	Windows	・ Johns Hopkins 大学が設置しているコロナウイルス感染情報提供Web サイトを騙るフィッシングサイト“Corona-Virus-Map[.]com”へアクセスすると“Corona-Virus-Map[.]com.exe”という実行ファイルのダウンロードを要求される [8] ・ 実行ファイルをダウンロードしてインストールすると、AZORult を含んだマルウェアがインストールされてAZORult が起動する。この時タスクスケジューラへAZORult の起動タスクが登録される ・ マルウェアはコロナウイルス感染マップを表示して、その裏でOS やブラウザから情報を窃取してC&C サーバへ送信する
Corona live 1.1 **[9]**	Android	・ Johns Hopkins 大学が公開しているコロナウイルスの感染状況を示すマップを騙った偽のアプリケーション ・ Google Play ストアではなく、Web サイト上で配布されている ・ アプリケーションの初回起動時には、特別なアクセス権限は不要である旨が通知される。その後「コロナウイルスの拡散を追跡可能」にするために、位置情報やスマートフォンのカメラへのアクセス権限が要求される ・ 攻撃者は、獲得したアクセス権限でユーザの位置情報や写真、動画を勝手に記録したり、デバイス上の個人情報を窃取したりする

		・スパイウェア"SpyMax" [1]を偽装するために作成されて配布されているアプリケーションの1つ
Coronavirus Tracker **[10]**	Android	・Google Play ストアではなく、Coronavirusapp[.]site というドメインのWeb サイト上で配布されている ・Coronavirusapp[.]site へアクセスすると、"Coronavirus Tracker"というコロナウイルスの発生状況マップを表示するアプリケーションのインストールを促される ・インストールを承諾すると、CovidLock と呼ばれるランサムウェアがユーザのスマートフォンにインストールされて、全操作がロックされる。ロック解除のためには、ビットコインを要求される ・インストールサイトは現在閉鎖済み

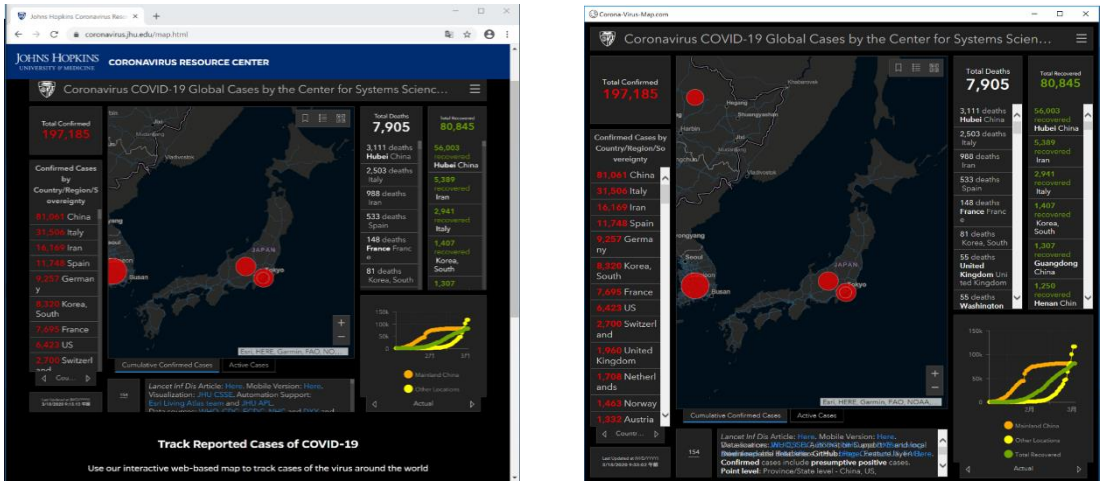


図 3： 正規の感染マップ(左)と偽の感染マップ(右) [11]

図 3は、Johns Hopkins 大学の正規のWeb サイトの表示と、マルウェア "Corona-Virus-Map[.]com.exe" の画面表示の比較です。図 3右の感染マップを表示させるには、フィッシングサイト "Corona-Virus-Map[.]com"へアクセスして、実行ファイルをダウンロードしてインストールする必要があります。この点が、正規のサイトとの大きな違いです。しかし、攻撃者が "Corona-Virus-Map[.]com"といういかにも本物らしいドメイン名のフィッシングサイトを立ち上げて、Johns Hopkins 大学がGitHub で公開している [12]集計データを使用して正規のサイトそっくりの画面を表示するアプリケーションを作成して配布しているため、ユーザは不審なアプリケーションと疑わず、感染マップ表示アプリケーションに扮したマルウェアをダウンロードしてインストールしてしまいます。マルウェアをインストールしてしまったあとも、マルウェアがJohns Hopkins 大学が公開しているデータを使って最新の感染マ

ップを表示するため、ユーザはマルウェアが動作してユーザの情報を盗み出していることに気が付きません。

2.1.2. Roaming Mantis の活動の広がり

"Roaming Mantis" は、PC やスマートフォンを標的としたフィッシング攻撃を行う攻撃グループです。コロナウイルスの感染拡大に便乗して再び活動が確認されるようになっています。

「コロナ禍でのRoaming Mantis」

コロナウイルスの感染拡大に伴って増えているのが、Roaming Mantis による「マスクの無料配布」を騙るSMS の配信です。SMS を用いたフィッシング攻撃は、「スミッシング」と呼ばれています。2018年に本レポートでも取り上げた、宅配業者を騙る送信者からの不在通知のスミッシングと同様の手口で、マスク無料配布の文言を含んだスミッシングの例が報告されています [13] [14]。

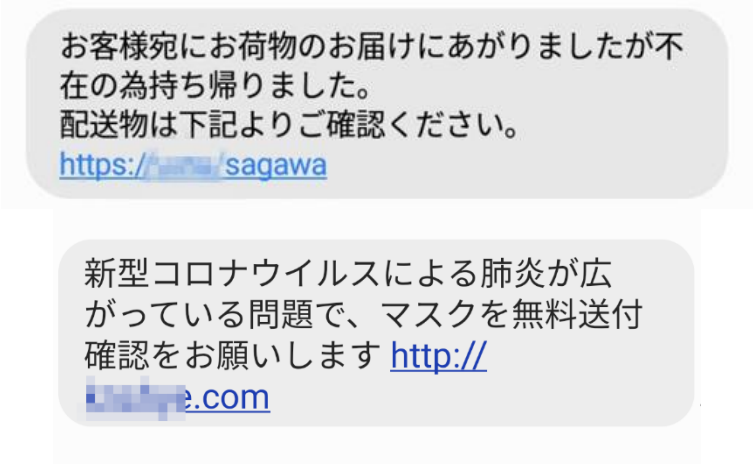


図 4： 宅配業者からの不在通知を騙るSMS の一例（上） [15]と マスク無料送付を騙るSMS の一例（下） [16]

スミッシングで誘導されたリンク先のページをランディングページと呼びます。上記のURLのランディングページは、Apple ID などの認証情報を窃取しようとする不正サイトや、不正なアプリケーションのインストールを促すサイトになっています。このようなコロナウイルス関連のスミッシングが始まったのは、国内でも感染者が出始めて、さまざまなイベントの中止が決まり始めた2月初旬でした。Roaming Mantis は、メッセージの文言を時事的な話題に変えることで、素早く既存の攻撃を変化させています。人々の不安心理や興味をそそる内容が巧妙に使用されるため、引き続き注意が必要です。

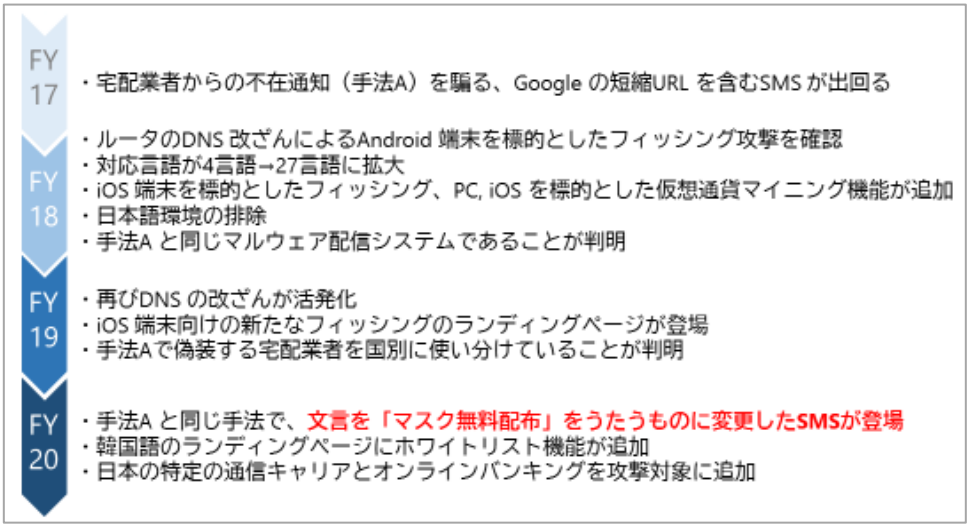


図 5： Roaming Mantis に関連した動き [17] [18] [19] [20] [21]

図 5に、攻撃グループRoaming Mantis に関連した動きをまとめました。Roaming Mantis は、対象言語や標的とする対象デバイスを素早く変化させて、攻撃対象を拡大させています。一連の流れからRoaming Mantis は、まず限定的な地域、おそらく韓国を対象に攻撃の効果を確認して、その後、攻撃範囲を広げて確実に攻撃対象のユーザを騙していると考えられます。

2020年になって、Roaming Mantis は2つの新しい機能を追加しました。1つは、フィッシングサイトへのホワイトリスト機能です [21]。これにより、ユーザがランディングページにアクセスすると、携帯電話番号の入力を要求されるようになりました。その番号が、攻撃者が保持しているリストに存在する場合だけ不正なアプリケーションが配信されます。これにより、調査チームがサンプルを入手することが難しくなります。現時点では韓国だけが対象ですが、今後は調査の目を回避しながら攻撃対象の拡大と攻撃の高度化を図ると考えられます。

また、もう1つ、スマートフォン用マルウェアに追加されたのが、デバイス情報を収集する機能です。マルウェアは、感染したスマートフォンの中に特定の銀行のアプリケーションを検出した場合や、特定のキャリアを使用していることが判明した場合に、ユーザをそれらに合わせたフィッシングサイトへ誘導するという機能を追加しました [22]。Roaming Mantis が、金銭の獲得を攻撃の大きなモチベーションにしていることは明らかです。

今後、政府から国民への一律10万円給付や、自治体によるマスク購入券の配布など、コロナウイルスに関連した金銭に絡む動きが増えると予想されます。例えば、「10万円給付に際して口座の確認が必要」などの文言と、確認用と見せかけた不正なURL を記載したSMS を送信して、接続先のサイトで口座情報を窃取する、スミッシングとフィッシング攻撃の手法が考えられます。ドイツでは、給付金申請サイトのフィッシングサイト経由で市民の個人情

報を窃取して、その情報で申請者になりすました攻撃者が、正規の申請サイトから偽の口座へ給付金を振り込ませるという偽申請が相次ぎました [23]。日本の正規の給付金申請サイトでは、振込先の口座情報の入力が求められますが、攻撃者は、給付金申請サイトのフィッシングサイトを用意し、口座情報だけでなく、オンラインバンキング経由で不正送金するために必要な暗証番号の入力を求めてくる可能性があります。オンラインバンキングで多く利用されるワンタイムパスワードなどの二要素認証を狙う手口も巧妙化している [24]ため、注意が必要です。

2.1.3. まとめ（対策）

フィッシング攻撃は、対策を周知徹底することで被害を防止することができます。今回取り上げた「新型コロナウイルス感染マップ」を騙る不正なアプリケーションや、Roaming Mantisによるスミッシングの被害に遭わないようにするために、情報の発信者と受信者の視点から、それぞれが気を付けるポイントをまとめます。

情報発信者が気を付けるポイント

コロナウイルス関連のフィッシング攻撃が増えていることを考慮して、紛らわしい情報を発信しないようにすることや、自分たちの情報発信媒体がスミッシングやフィッシング攻撃に悪用されないようにする工夫が必要です。特に、政府機関や自治体の担当者は、国民や市民に、確実かつ正しく情報を伝達するために、そのメッセージが「本物」であることを証明できる必要があります。まず情報の発信媒体としてSMS を使用するのは避けた方が良いでしょう。SMS は不正な送信元を制限する機能がなく、誰でもスミッシングのメッセージを送付できてしまうので、悪用されやすい傾向にあります。また、フィッシングサイトへの対策として、SSLサーバ証明書の取得があります。SSL サーバ証明書にはその認証レベルによって、「ドメイン認証型」「企業認証型」「拡張認証型」の3種類があります。フィッシング攻撃対策には、3つの中でも最も厳格な審査が必要な「拡張認証型」のSSL サーバ証明書が有効です。Web サイトの運営者が実在するかどうかを保証できるため、そのWeb サイトの信頼度が高まります [25]。

情報受信者が気を付けるポイント

コロナウイルス関連のWeb サイトやアプリケーション、メールなどが多く出回っています。正しい情報を伝えるものも多い一方で、攻撃者はこれに便乗して悪意のあるWeb サイトなどを用意しています。自宅で過ごすことが多くなり、インターネットを使用する時間も長くなる傾向にありますが、コロナウイルスに関連した情報を提供するWeb サイトには、10%程度の割合でリスクのあるサイトが紛れ込んでいることを認識しておく必要があります。外出の自粛や働き方の変化に伴い精神的にも不安になりがちですが、いつも以上にメールや

SMS に記載されているURL を不用意にクリックしないように意識し、特に、内容をすぐに確認するように要求する緊急性の高そうなメッセージは、文章につられてリンクをクリックしないように注意してください。表 2に、情報受信者がフィッシング攻撃の被害に遭わないために気を付けることをまとめました。

表 2：フィッシング攻撃の被害に遭わないために気を付けること

情報受信者が気を付けるべきこと	理由（攻撃者の意図）
• アプリケーションは公式ストアからインストールする。Web サイトから直接インストールしたり、サードパーティのアプリストアを使用したりしない • アプリケーション（ファイルなども含む）のダウンロードは必要最低限のものに限定して、アクセス権限などを確認してからインストールする	• Coronavirus Tracker やCorona live 1.1 のように、マルウェアを含む不正なアプリは、公式のアプリストアのセキュリティ審査を回避するために、フィッシングサイトやサードパーティのアプリストアで配布されます
• メールやSMS に記載されているURL を不用意にクリックしない。短縮URL の場合は注意が必要。特に、内容をすぐに確認するように要求する緊急性の高そうなメッセージは、文章につられてリンクをクリックしないように注意する • リンクをクリックする前にリンク先のURL を確認する方法も有効。PC の場合は、ブラウザ上でリンク文字上へマウスカーソルをあわせるとURL が表示される（ホバー機能）	• 攻撃者は、ユーザをフィッシングサイトへ接続させるために、巧みな文章と共にURL を記載したメッセージを使用します • SMS は、不正な送信元を制限する機能がなく、誰でもスミッシングのメッセージを送付できます • 短縮URL は、リンク先のドメイン名などを隠ぺいできるので、詐欺サイトであることを気が付かせずにアクセスを誘うことができます
• OS やアプリケーションは、脆弱性が修正された最新のバージョンを使用する	• 攻撃者は、アプリやOS の脆弱性を悪用して攻撃したり、マルウェアへ感染させたりします
• 安全性を確認できないフリーのWi-Fi アクセスポイントを使用しない	• 攻撃者は、フリーのWi-Fi アクセスポイントを用意して、接続したPC やスマートフォンのWeb アクセスをフィッシングサイトへ誘導します

2.2. ラテラルムーブメント

昨今、多くの企業がサイバー攻撃に狙われています。2020年1月には、日本の防衛関連企業4社へのサイバー攻撃が発覚しました。その中でも、三菱電機株式会社(以下、三菱電機)の事例では､情報システム環境における多層防御機能の実装やインシデント発生時の緊急対応体制の整備・運用等を実施していましたが、防衛省指定の注意情報(貸出時に誓約書の提示し、保全の徹底を要求されていた情報)や8122件の個人情報などが流出したおそれがありました [26] [27] [28]。

このような事態となったのは以下のような組織内における侵害を広げる行為(以下、ラテラルムーブメント)が一因と思われます。

- 中国国内の1拠点から複数拠点への侵害拡大
- 中国国内の拠点の端末から国内拠点のウイルス対策管理サーバへの侵害
- ウイルス対策管理サーバから国内複数拠点への侵害拡大

ラテラルムーブメントについて、どのような攻撃か、またどのよう対策が有効かを考えてみたいと思います。

2.2.1. ラテラルムーブメントについて

ラテラルムーブメントは、APT攻撃(Advanced Persistent Threat)において目的とする重要資産に近づくために、組織内で侵害範囲を広げる行為です。ラテラルムーブメントでは以下の表 3のような手法を使用します [29]。

表 3：ラテラルムーブメントの手法

	分類名	概要
1	脆弱性の悪用	・ OA環境や社内システムのマシンが使用しているRDP、SMB、印刷スプーラーサービス等の一般的なサービスや、MySQL等のサーバが利用しているサービスの脆弱性を悪用して、他のマシンへ不正アクセスする
2	OS標準機能の悪用/OSベンダ純正ツールの悪用	・ RDP、SSH、SMB/Windows Admin Share、WinRM、PsExec、WMI等を既存のアカウントを用いて利用し、他のマシンへ不正アクセスする ・ 侵入したマシンにおいて、schtasks、atを用いてマルウェアをタスク登録する

3	代替認証要素の悪用	・ パスワードハッシュやKerberos認証のチケット等の代替認証要素を悪用して通常の識別と認証をバイパスして、他のマシンへ不正アクセスする
4	管理ツールの悪用	・ 管理、モニタリングツールを悪用して他のマシンへ不正アクセスする

三菱電機の報道発表などから、三菱電機の事例におけるラテラルムーブメントがどのように行われたか推測してみます。報道発表の内容だけでは、読み取れない部分は過去のサイバー攻撃の事例をもとに推測しました。その結果、今回のサイバー攻撃は、以下の図 6のような流れだったと想定されます [26] [30]。

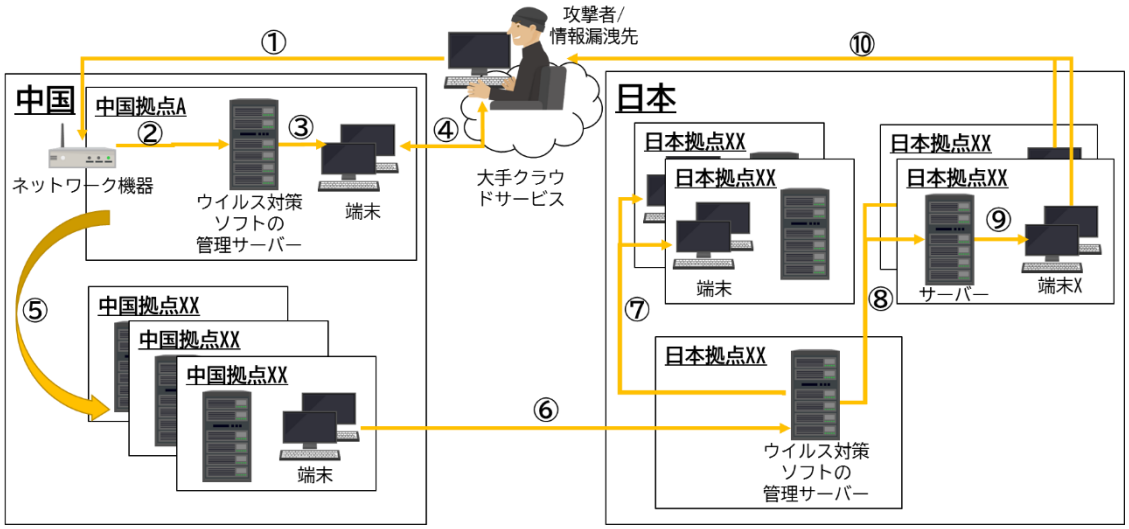


図 6: 三菱電機へのサイバー攻撃の流れ(イメージ)

① 中国国内の拠点Aの管理が十分でないネットワーク機器へ侵入
② 拠点Aのウイルス対策ソフトの管理サーバの未公開脆弱性を攻撃して同管理サーバへ侵入
③ 同管理サーバのパターンファイルアップデート機能を悪用して、同拠点Aの多数の端末へDropperマルウェアを配布
④ 当該端末のウイルス対策ソフトに脆弱性があり、ウイルス対策ソフトが正規ファイルと置き換えられたDropperマルウェアを起動する。Dropperマルウェアは、欺瞞したPowerShellとPowerShellスクリプトを実行して攻撃者のサーバから遠隔操作マルウェアをダウンロードして実行する。これにより外部から遠隔操作が可能になる
⑤ ③④を繰り返して、中国国内の複数拠点へ侵害を拡大
⑥ 攻撃者の遠隔操作により、中国拠点の端末から日本国内のウイルス対策ソフトの管理サーバへ②の手法を用いて侵入

⑦　中国国内の同様に、③④を繰り返して日本国内の複数拠点の端末へ侵入を拡大
⑧　同様に③④の手法で日本国内拠点のあるサーバへも侵入
⑨　⑧のサーバ上の機密情報を端末X経由で外部へ送信
⑩　攻撃者は、端末X経由で機密情報を受け取る

社内ネットワークへ侵入した攻撃者は、ウイルス対策ソフトの管理サーバの脆弱性を悪用してサーバへ侵入(②)後、その配布機能(③)とウイルス対策ソフトの脆弱性を悪用して他のマシンへ侵入(④)します。攻撃者は、③と④を繰り返して侵害範囲を拡大しています。

今回の事例において、攻撃者は、少なくとも表 3の1と4のラテラルムーブメントの手法を使用しています。以下の理由から、攻撃者はこの手法を選択したと考えられます。

- 三菱電機は、PsExec、WMI、PowerShell等のラテラルムーブメントへ悪用される機能を制限していたため、攻撃者は悪用できなかった
- 三菱電機が、PsExec、WMI、PowerShell等のラテラルムーブメントへ悪用される機能の挙動を監視しているおそれがあったため、検知されにくい手法を使用した

このように、今回の事例は、攻撃者がよく使用するラテラルムーブメントの手法への対策がされていたと想定される社内システム環境においても、広範囲にラテラルムーブメントして侵害を広げていることから、高度なサイバー攻撃だったと考えられます。

2.2.2. 対策

このような高度な攻撃に対して、どのようなセキュリティ対策を行ったら良いのでしょうか。さまざまな対策がありますが、侵入されることを前提に、攻撃者の標的である機密情報が保存されているエンドポイントに焦点を当てた対策を紹介します。

ラテラルムーブメント防止

エアギャップ化やマイクロセグメンテーション化により、攻撃者のネットワークの移動を制限し、ラテラルムーブメントによる機密情報への到達を防ぎます。

エアギャップとは、重要な機密情報が保存されたマシンをインターネットに接続されたネットワーク等から物理的に隔離された状態にすることです。侵入された場合でも、ネットワークが物理的に繋がっていないため、攻撃者が機密情報の保存されたマシンへ到達するリスクや機密情報を持ち出すリスクを低減できます。

マイクロセグメンテーションとは、従来のオクテット単位でネットワーク設計する場合のセグメントと比べて、より細かい単位でセグメントを分割して、セグメント間の通信を必要最低限に制限することです。侵入された場合でも、攻撃者が移動できる範囲を狭めることができるため、侵害拡大のリスクを低減することが可能です。なお、この2つの対策は、運用

面や可用性などに大きな影響を与えるおそれがあります。機密性が高い情報のみ適用するなど、全ての情報に適用するのではなく、機密性や可用性、運用面などを考慮し、メリハリをつけて対策を行うことをお薦めします。

高度なサイバー攻撃による機密性の高い情報への不正アクセスには、以下のような考えに基づいて、対策を行うと良いのではないでしょうか。

- 運用面や可用性等を考慮して、可能な場合に、エアギャップ環境にて情報を扱う
- 上記が難しい場合には、以下のマイクロセグメンテーション化を行う
  - 情報を扱う部署単位で、セグメントを分割する
  - ActiveDirectoryやウイルス対策ソフト管理等の当該部署を運用/管理するサーバや端末は、分割したセグメント内に設置する

機密情報の漏洩防止

機密情報を暗号化することにより、攻撃者がその情報にアクセスできたとしても、暗号化鍵が無ければ、その情報を読み取り、使用することができない状態にします。

高度なサイバー攻撃による機密情報な持ち出しには、以下のような考えに基づいて、対策を行うと良いのではないでしょうか。

- 機密情報を電子政府推奨暗号リストに記載のアルゴリズムを用いて暗号化を行う
- 暗号化に利用した鍵は、OSの識別認証情報だけではアクセスできないようにするなど適切に管理する

エンドポイントでの攻撃検知と対応

EDR(Endpoint Detection and Response)を導入したり、SIEM(Security Information and Event Management) でマシンの情報を分析したりすれば、クライアントPCやサーバ上で攻撃者の挙動の早期に検知して、検知後の対応をスムーズに行うことができます。

- プロセス、レジストリ操作などのマシンの情報を収集して、EDR自身やSIEMで分析することにより、複数のWindowsマシンでネットワークレベル認証(NLA)の無効化などのレジストリ不審に変更されていること、複数のWindowsマシンで普段よりPowerShellプロセスが多く起動されていることなど、攻撃者が行った行為を早い段階で検知できる
- 侵害されたマシンが遠隔地にあっても、EDRを利用してプロセスのタイムラインを表示して解析したり、怪しいファイルを入手したりして、侵害の状況を素早く調査できる
- 侵害が広範囲かつ多くのマシンに及んだ場合であっても、EDRを利用して、複数マシンの情報を一気に収集したり、攻撃の痕跡(IOC)を使って複数の侵害されたマシンのプロセス、ファイル、レジストリなどを検索したりして、侵害の状況を素早く調査できる
- 侵害されたマシンのネットワーク隔離やマシン上の怪しいファイルの削除等の対応も、現地に出向くことなくリモートで対応できる

2.2.3. まとめ

三菱電機の事例は、防衛関連企業が直接攻撃された事例でしたが、高度なサイバー攻撃の標的となりやすい政府組織や防衛関連企業の関連組織、取引先企業が狙われるケースもあります。このような関連組織/企業は、三菱電機と同様の高度なサイバー攻撃を受けるおそれがあります。このようなサプライチェーン攻撃 [31]にも気をつけなければなりません。

3. 情報漏えい

2019年度第1～第3四半期は、Webスキミングによる情報漏洩が継続して確認されていることが確認されました。2019年度第4四半期も傾向は変わりませんが、加えて、クラウドサービスの設定ミスにより、本来であれば第三者に公開してはならない情報がインターネット上から誰でも参照できる漏えい事例が数多く報告されました。

一方、国内でもクラウドサービスの設定不備による情報漏えい事例が2件発生し、そのうちソフト・オン・デマンド(以下、SOD)社の事例は漏えいした内容から大きな話題となりました。

3.1. 成人向け動画サービス「SODプライム」の情報流出

SOD社は、同社サービス「SODプライム」に会員登録したユーザ情報の一部が、他のユーザから閲覧可能となる事象が発生していたことを、3月19日に公表しました。原因は、アクセス集中対策のために導入したCDNサービス導入時の設定誤りでした。この事件により、最大で68,898人の個人情報が第三者へ閲覧可能となり、情報の中には、氏名や動画の視聴履歴などが含まれている場合もありました。SOD社はお詫びとして、氏名等の情報が閲覧された可能性がある利用者については、1人当たり5,000円を支払い、その他の情報が閲覧された可能性がある利用者には同社サイトの500ポイントを付与するとしています [32]。

3.2. 流出の原因

SOD社はコロナウイルスの感染拡大を受け、同社の動画配信サービス「SODプライム」の有料作品の一部を無料配信するキャンペーンを3月13日から開始しました。このキャンペーンによりアクセスが殺到したため、SOD社はCDNを活用しアクセス集中への対策を行いました。しかし、CDN導入時の設定に不備があり、同サービスに利用者がアクセスした際、他の利用者の個人情報の一部が表示される不具合が発生し、このため個人情報が流出しました [32]。

CDNとは「Content Delivery Network」の略で、Webサイトや動画配信サービスにおいて同一のコンテンツを多くのユーザに効率的に届けるための仕組みです。通常のWebサイトでは、コンテンツを配信するサーバを自前で用意するため、大量のアクセスが発生した場合、サーバの負荷が上昇し、レスポンス低下やサービス停止となる事象が発生します。CDNはこの問題を解決するため、コンテンツを一時的に保存するキャッシュサーバを大量に用意し、

利用者はこの大量に用意されたキャッシュサーバからコンテンツを入手することで、安定した配信を可能とします。

本来であれば、CDNのキャッシュサーバに保存する設定は動画コンテンツに関するもののみを行うべきでしたが、急な対応ということもあり、本案件では利用者情報も含めた情報が誤ってキャッシュサーバに保存されてしまいました。更にこの状態において、CDNに対する設定の不備が重なり、利用者が自身の情報を参照しようとした際に、キャッシュサーバに保存された他の利用者の情報を表示してしまう事象が発生しました。

こうした事例は今回が初めてではありません。メルカリ社 [33]やシンガーソングライターaikoのファンクラブサイト [34]でも同様の事例が発生しており、同様に他の利用者の個人情報の一部が表示された事例が発生しています。そのため、SOD社も過去の事例を参考にしていれば防ぐことができたと言えます。

3.3. 事件の影響

過去の個人情報漏えい事例を見ると、ソフトバンクBB社やベネッセ社で発生した過去の個人情報漏えい事件では、いずれもお詫びとして500円の金券が被害者に送られています [35] [36]。また、2002年にTBC社が体のサイズや身体的な悩み等といった機微な情報を含む個人情報を漏えいした事件では、2次被害をうけた被害者による民事訴訟が行われ、最大3万5000円の慰謝料を支払われました [37]。

今回の事故では、成人動画の視聴履歴など他者に知られたくない情報が流出し精神的な苦痛も大きいことが考慮されてか、他の個人情報漏えい事件と比べても高額な1人当たり5,000円のお詫びの金額を支払うこととしています [32]。漏洩した場合に精神的な苦痛を伴う情報を扱う組織は、より慎重にセキュリティ対策する必要があることが改めて浮き彫りになったのではないでしょうか。

また、利用する側もこうした事故は起こりうると想定し、しっかりとしたセキュリティ対策を行っているかを見極めた上でサービスを利用する必要があると言えます。

影響はこれだけには留まりません。事故原因の調査や再発防止に向けた対策にかかる費用、サービス停止に伴う売上の減少、ブランドイメージの低下など大きな代償を払わなければならなくなります。今回は該当しませんが、こうした事故の発生により、プライバシーマーク等のセキュリティ認証の取消しに繋がることもあります [38]。取消された場合、セキュリティ認証が要件となる案件への入札ができなくなるなど、事業へ大きな影響を与える場合もあります。

3.4. まとめ

クラウドサービスの設定不備に関係する情報漏えい事例を取り上げました。現在は、CDNをはじめとした様々なクラウドサービスが提供されており、サービスの拡充や規模の拡大が容易に行えるようになりました。一方で、設定不備に伴う被害も短期間で拡大してしまう傾向があります。特にクラウドサービスで機微な情報を扱う場合は、該当するクラウドサービスのベストプラクティスを参考にするなどして設定不備を効率的に確認し、迅速かつ安全にサービスを提供していただきたいと思います。

4. 脆弱性

本章では、Citrix社の製品に生じた脆弱性（CVE-2019-19781）について解説します。JVNへ掲載された当該脆弱性のCVSSのBase値は9.8であり、極めて深刻な脆弱性です。当該製品を導入している組織は、早急にパッチを適用する必要があります。

4.1. 複数のCitrix製品に発生した脆弱性

2020年1月17日、Citrix Systems社は2019年12月に公開されたCitrix社の製品 Citric ADCとCitrix Gatewayに存在する脆弱性（CVE-2019-19781）を悪用した攻撃を確認したと公表しました [39]。この脆弱性が発見された段階ではパッチ等はなく、ゼロデイ脆弱性となっていました。

通常、Citrix ADCとCitrix Gatewayはユーザからのリクエストを複数のサーバに振り分けるネットワーク機器です。セキュリティ面ではユーザ認証やシングルサインオンの機能を有しています [40]。当該機器は、ユーザからファイルへのアクセスを要求されたときに、要求を送信したユーザが認証されたユーザなのか、ファイルへのアクセス権を認可されているのかを判断してから処理します。今回、このパスの処理にディレクトリトラバーサルの脆弱性が確認されました。攻撃者は、インターネット上から当該機器へ本脆弱性を悪用した要求を送信して、ユーザ認証なしでシステム構成ファイルから機密情報を読み取ったり、任意のコードを実行したりできます。

2020年1月11日にインドのセキュリティ研究者グループのProject Zero Indiaが、本脆弱性を悪用して攻撃を成功させることができる検証コード(PoC)をGitHub上に公開しました [41]。

セキュリティ教育のSANS Instituteは、**図 7**の破線で示した2020年1月11日のPoC公開後よりハニーポットに対して本脆弱性を狙ったスキャン(**図 7**の緑線)が増加したこと、おなじくPoC公開後から本脆弱性を悪用したバックドア設置を狙った攻撃通信が増加したこと(**図 7**の赤線)を報告しています。1月11日時点ではセキュリティパッチや修正されたバージョンの製品は提供されていません。PoCを公開したことが、ゼロデイ攻撃の発生に繋がりました。修正されたバージョンは、最初の攻撃発生から13日後の1月24日に公開されました。

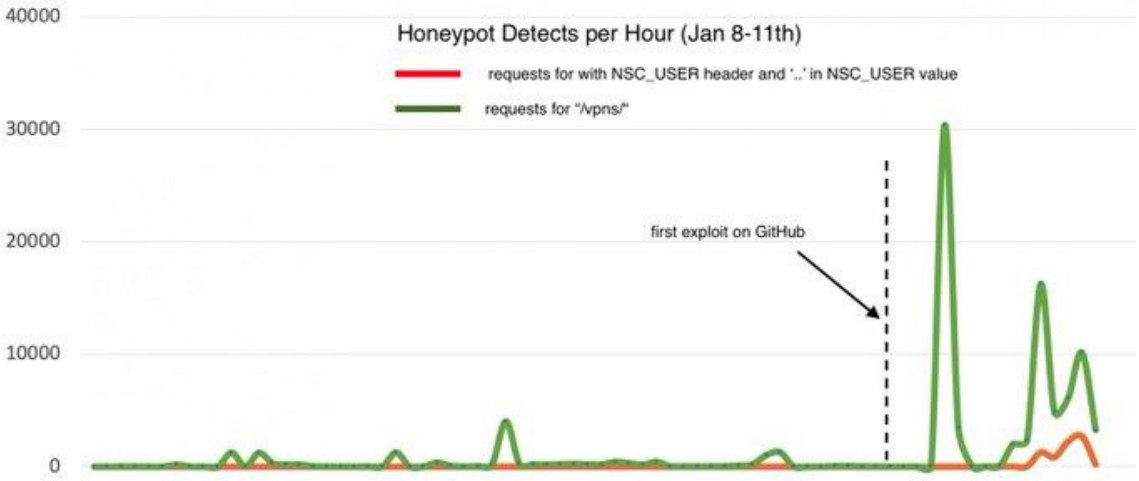


図 7：1時間当たりのハニーポットの検知件数（1/8~1/11）[42]

4.2. Citrix製品の脆弱性を悪用された攻撃事例

2020年1月20日、フランスの通信会社Bretagne Télécom社は、このCitrixの脆弱性を悪用されてランサムウェアDoppelPaymerに感染したことを報告しました。脆弱性が修正されたCitrix製品は1月24日に公開されたので、Bretagne Télécom社への攻撃はゼロデイ攻撃でした。

Bretagne Télécom社は、この攻撃で顧客企業 約30社分のデータを含む30テラバイト分のデータが暗号化され、約35ビットコイン（当時の価格で35万ドル）を要求されたと公表しました。Bretagne Télécom社はバックアップを取っていたため、3日間ですべてのデータを回復することに成功し、身代金も支払わなくて済みました [43]。Bretagne Télécom社は幸いにもデータを回復できましたが、ランサムウェア感染を未然に防ぐことはできなかったのでしょうか。Bretagne Télécom社のインシデントに関係する報道からは、Citrix製品の脆弱性が悪用された原因はわかりません。一般的には、以下の3つの原因のうち、いずれか1つの可能性があります。

Citrix製品の脆弱性情報に気づかなかった

Citrix製品の脆弱性情報やCitrix社の注意喚起に気づいていなかった場合、攻撃を全く防ぐことができません。対策は、製品の製造元や保守契約した販売代理店、セキュリティ機関から提供されるCitrix製品の脆弱性情報を常に確認することです。脆弱性情報を調査可能な無料のデータベースは、日本国内のJVNやアメリカのNVD、中国のCNNVDが挙げられます。

Citrix製品の使用を停止できなかった

Citrix Systems社は、2019年12月に脆弱性を公表した時に、製品の利用中止、または緩和策を実施するように注意喚起しました [39]。Citrix社の注意喚起に従って、すぐにCitrix製品の使用を停止していたら、ランサムウェアの被害には遭わなかったでしょう。しかしCitrix製品の使用を停止したら、業務に大きな影響が発生するおそれがあります。そのためにCitrix製品の使用停止に踏み切れず、その判断ミスでランサムウェアへ感染したおそれがあります。

緩和策の実施遅れ

Citrix製品の利用停止できない場合は、設定変更による攻撃の暫定的な緩和策を実施することも可能でした。自社の業務に大きな影響がある製品は、設定変更するまえに動作検証が必要です。動作検証に時間がかかっていたため、攻撃の発生のほうが早く、緩和策が間に合わない場合があります。もし緩和策の実施に時間がかかる場合や緩和策では完全な未然防止ができない場合は、暫定的に監視を強化して遠隔コード実行やランサムウェア感染を早期検知するという選択肢もありました。

4.3. まとめ

今回、Citrix製品の脆弱性について触れました。2017年に脆弱性を悪用して世界的にランサムウェアWannaCryの感染が流行したケースがありました。WannaCryの感染のケースは、3月にWindowsのServer Message Block(SMB)の脆弱性(CVE-2017-0144)の公開と修正とパッチの提供から、大規模な攻撃が発生するまでに時間がありました。Citrix製品の脆弱性はゼロデイ攻撃が発生したため、WannaCryのケースよりも対応が難しかったと考えられます。

もしBretagne Télécom社がシステム停止の判断や設定変更の実施判断を誤ったことがランサムウェア感染の原因であれば、収集した脆弱性情報から自社に起こり得る被害を予測して、適切な対応を判断できなかったことが、その要因と言えます。Citrix製品の脆弱性は、攻撃者が遠隔から任意のコードを実行できたこと、修正パッチが提供される前に攻撃が始まっていたことから、セキュリティ担当者は、脆弱性が公開された時点で、すぐに攻撃者が自社社内ネットワークへ侵入して、情報漏えいやランサムウェアによるデータの暗号化といった大きな被害が発生するおそれを予測できなければなりませんでした。これを予測できていれば、Citrix製品の使用停止や緊急メンテナンスで設定変更する決断ができたでしょう。

組織のセキュリティ担当者は、普段から上記に記載した脆弱性情報データベースを用いて、自組織の業務へ大きな影響がある製品の脆弱性情報を確認すべきです。確認対象製品の種類が多い場合は、脆弱性情報が膨大な量になります。対象製品の脆弱性情報の収集を支援するツールや配信するサービスを活用しましょう。そして、脆弱性による業務影響を評価する方法を作成して運用しましょう。

5. マルウェア・ランサムウェア

5.1. 2019年度第4四半期の概況

2019年度第3四半期に引き続き、マルウェアEmotetや、SodinokibiやMazeのようなランサムウェアの被害事例が多数報告されています。

Emotetは従来のメールを介した拡散が確認される一方で、感染した端末からWi-Fiを経由して拡散する新たな手口も確認されています [44]。トレンドマイクロの報告によると少なくとも2018年から存在する亜種のようですが、日本国内においては国の政策としてWi-Fi環境の整備が進められていた背景 [45]もあり、今後ますます悪用の懸念があります。

ランサムウェアに関しては、SodinokibiやMazeなどに情報を盗み出すタイプが確認されていることを、情報第3四半期のレポート [46]にて紹介しました。第4四半期は、身代金支払い拒否した被害者の情報が暴露される被害の報告が目立ちました。ランサムウェアは感染した端末上のファイルを暗号化することで、システムや組織の可用性を盾に身代金を要求する手口がこれまでは一般的でした。しかし、バックアップの取得といったランサムウェアの対策が浸透しつつあることや、No More Ransomプロジェクト [47]をはじめとする啓発活動の影響により、もはや情報の暗号化のみでは身代金の獲得が困難になりつつある状況とも考えられます。そのため、今後は、情報暴露型のランサムウェア被害がより一層増加する可能性があります。

2020年2月中旬に差しかかかると、コロナウイルスの世界的流行に便乗し、フィッシングなどの手口でマルウェア拡散を目論む事例が数多く報告されるようになりました。攻撃者が世間の関心事に便乗した攻撃キャンペーンを展開することは珍しくはありません。しかし、コンピュータヘルプサイトBleeping Computerの取材によると、一部のランサムウェア攻撃者は「医療機関を標的とした攻撃を行わない」といった旨の声明を出しています [48]。表面上は人道的見地からといった建前ですが、コロナウイルス被害が長期化することによる世界経済への打撃は、ランサムウェア攻撃者にとっても看過する事のできない事態であると推測します。

5.2. 情報暴露型ランサムウェアの被害

2019年12月、米Southwire社はMazeランサムウェアの被害に見舞われました。878台のデバイスから120GB程度のファイルをランサムウェアによって盗み出さたと報告されています [49]。その後、およそ600万ドルとも言われる身代金の支払いを拒否すると、攻撃者によっておよそ12GB分のファイルが攻撃者の運営するWebサイト上で暴露されてしまいました。

窮地に立たされたSouthwire社は訴訟に踏み切りました。相手は、どこの誰とも不明なMaze

ランサムウェアの攻撃者です。裁判所は攻撃者のWebサイトをホスティングしていた業者に対して差止命令を行い、業者は命令に従う形で攻撃者のWebサイトを停止させました。一旦は情報流出に歯止めをかけることに成功したかに見えました。しかしながら、攻撃者は強硬な態度を崩しませんでした。追加で14GBのファイルを公開した上で、「身代金支払いに応じないなら、更に追加でファイルを公開する」と繰り返しの脅迫を行っています。

Southwire社の対応は、いたちごっこに過ぎず、問題の解決には至りませんでした。それどころか、ランサムウェア攻撃者を刺激してしまったおそれがあります。もちろん、これらは結果論であり、安易にSouthwire社の対応を批判する事はできません。情報暴露型のランサムウェアに関しては、一度感染してしまうと根本的な解決が難しいでしょう。仮に身代金を支払ったとしても、情報が暴露されない保証もありません。情報暴露型のランサムウェアに感染してしまった場合は、既に情報が漏えいしている状況と考えるべきかもしれません。被害の規模の確認や関係各所、被害者への迅速な連絡など、事後の対応に臨まれることを推奨します。もちろん、感染を防止することが最善ですが、会社の情報資産の棚卸と評価を定期的に実施し、万が一の事態に迅速な判断が下せるよう準備することが重要です。

表 4：ランサムウェア攻撃者によって情報が暴露された事例

日付	被害組織	概要
2019/12	Southwire社	ランサムウェアMazeに感染。身代金の支払いを拒否した後、窃取された情報の一部が公開される。その後、ランサムウェア攻撃者に対する訴訟に発展
2019/12	米ペンサコーラ市	ランサムウェアMazeに感染。実際はわずかな情報のみしか窃取できていないといった報道があった。それに反論する目的で窃取した情報の一部が公開された
2020/1	Artech Information Systems社	ランサムウェアSodinokibiに感染。窃取された内部情報のうち、337MBがロシアのハッカーフォーラム上で公開された
2020/1	MDLab社	ランサムウェアMazeに感染。身代金の支払いを拒否したため、窃取された情報のうち9.5GBが公開された
2020/2	BretagneTélécom社	ランサムウェアDoppelPaymerに感染。バックアップから復旧を行ったため、身代金の支払いを拒否。その後、従業員の情報やデジタル証明書等が公開された

2020/3	Visser Precision社	ランサムウェアDoppelPaymerに感染。身代金の支払いを拒否したため、防衛や宇宙開発関連の機密情報の一部が公開された

5.3. まとめ

日本国内ではマルウェアEmtoetが猛威を振るいましたが、米国においてはMazeやSodinokibiなどのランサムウェアの被害が大きな話題となっていました。これまでのランサムウェア被害は、自治体や医療機関が標的とされ、暗号化されたファイルの復旧を盾に身代金を要求されるものが中心でした。しかし2019年度第4四半期になると、民間企業が標的になるケースが多く確認されるようになり、組織から盗み出した情報の暴露を盾に身代金を要求する、情報暴露型のランサムウェアの被害が多く確認されるようになりました。情報暴露型のランサムウェアによって窃取された情報を取り戻すことは困難であるため、窃取された情報は既に漏えいされたと考えて事後対応策に臨まれる事を推奨します。また、コロナウイルス流行を受けて、世界各国で緊急の経済対策や国民への支援制度が急ピッチで進められている状況です。この混乱に乗じた新たな手法でマルウェア拡散を狙う攻撃者も少なくないと思われます。日本国内においても、JPCERT/CCや日本サイバー犯罪対策センター(JC3)などが適宜注意喚起を行っております。そういった機関から最新のサイバー犯罪やマルウェアについての情報を収集し、引き続き警戒にあたってください。

6. 予測

個人をターゲットとするランサムウェア

2019年度第4四半期は、民間企業を標的とした「情報暴露型ランサムウェア」の被害が目立ちました。従来型のファイルの暗号化のみを行うランサムウェアでは、身代金の支払いが拒否されるケースが増加していることから、今後は、情報暴露型のランサムウェアが被害の中心となるおそれがあります。また、その標的が個人へと拡大すると予測します。個人が自分専用のPCやスマートフォンを所有する事が当たり前である世の中となっていますが、個人所有のデバイスはパーソナルデータの宝庫です。暴露されることで、社会的なダメージを負うような情報が格納されているケースも珍しくはないでしょう。個人、特に政治家や芸能人といった著名人を標的とする「情報暴露型ランサムウェア」攻撃が、攻撃者にとって格好のビジネスとなり得るおそれがあります。

コロナウイルスに便乗した攻撃に引き続き警戒

本稿ではコロナウイルス関連のフィッシング攻撃について紹介しました。Proofpoint社のレポートによるとサイバー攻撃の99%以上が人間の関与を必要としており、攻撃者は人間の不安につけ込んで攻撃を仕掛けるため、このような状況はサイバー攻撃が成功するリスクが高いと言えます [50]。コロナウイルスのニュースは、全世界規模で最も注目されており、騒動に便乗したフィッシング攻撃には継続的な警戒が必要です。日本国内においては、厚生労働省が「新しい生活様式」「徹底した行動変容」を提唱しており [51]、今まさに社会が大きく変わろうとしています。コロナ禍の中でコミュニケーションがこれまで以上にメールやSNSへ依存するため、これまでよりもフィッシング攻撃を受ける機会が増えるおそれがあります。少しでも不審だと思ったら自身の思い込みで判断せず、第三者の客観的な意見を求めることで、フィッシング攻撃から身を守ることを心掛けてください。

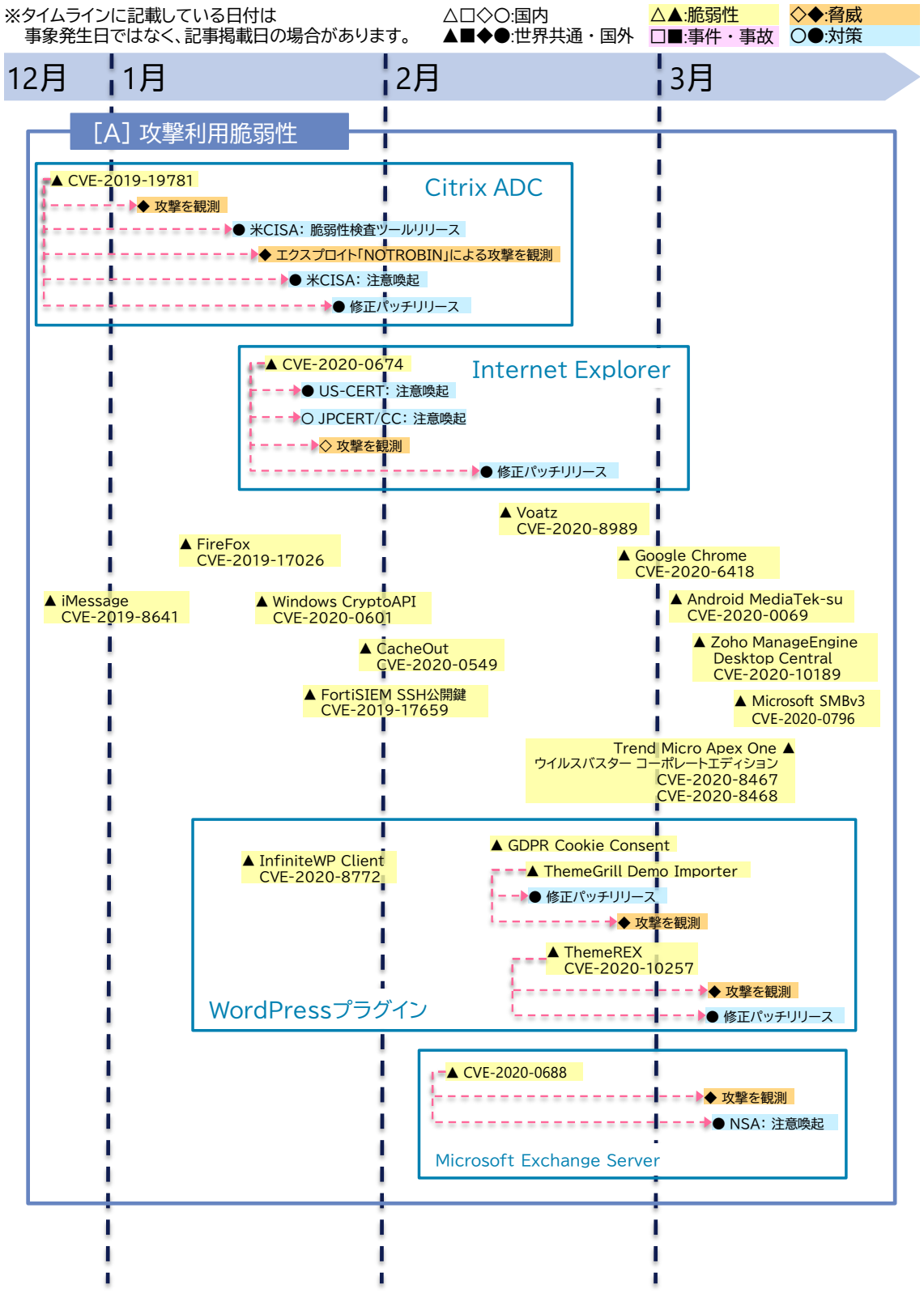
コロナウイルスによるサプライチェーン攻撃の増加

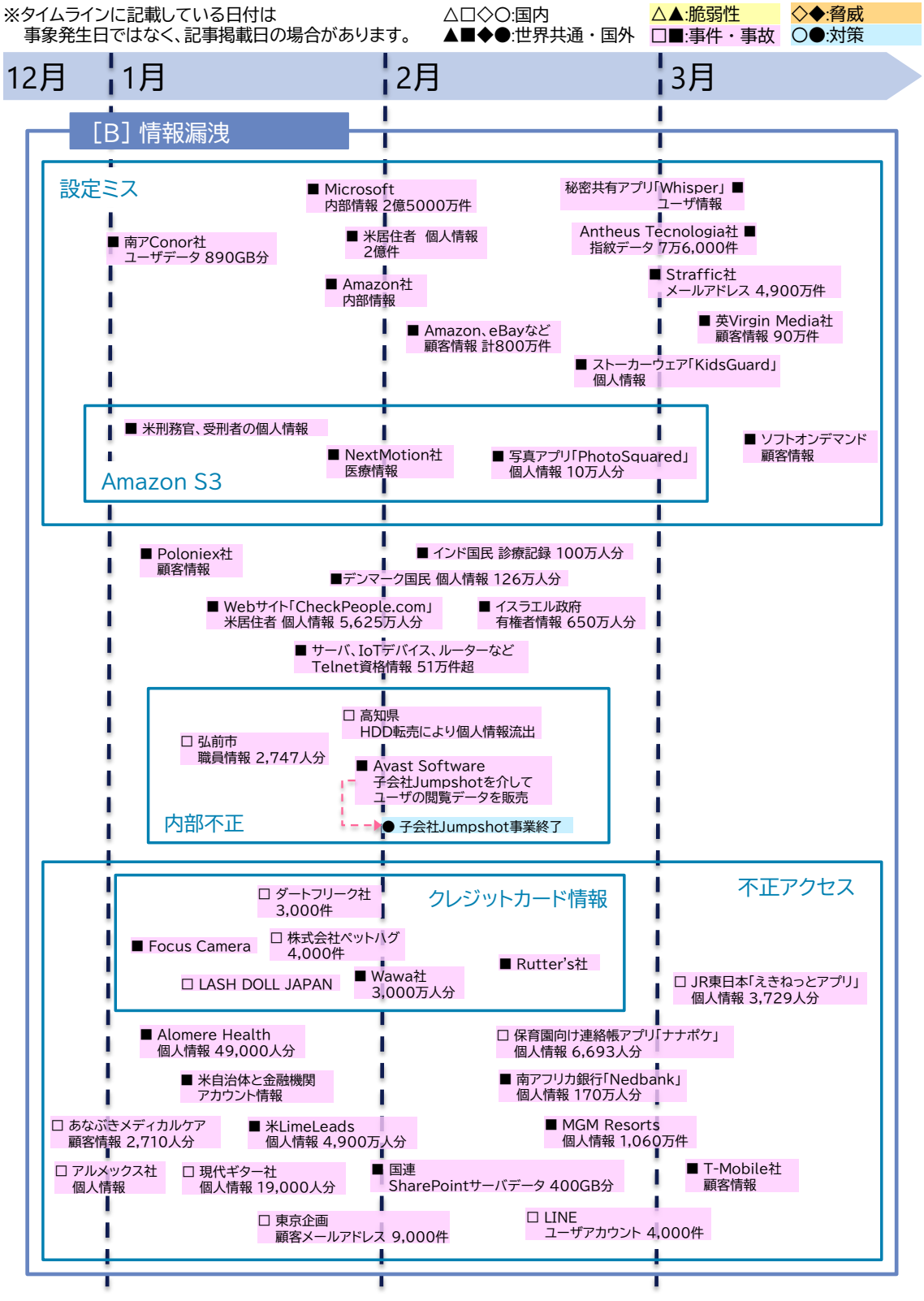
コロナウイルスによる影響で多くの企業で業績の悪化が懸念されています。業績が悪化した場合、さまざまな予算の削減に併せてセキュリティ予算も削減されると考えます。予算削減により、検討していたセキュリティ対策の中止や延期、現行のセキュリティ運用の縮小によって、組織に必要なセキュリティレベルが低下するおそれがあります。一方で、攻撃者は本稿でも紹介したコロナウイルスに関連する攻撃の増加など、このような状況を好機にと攻撃を強めています [52] [53]。

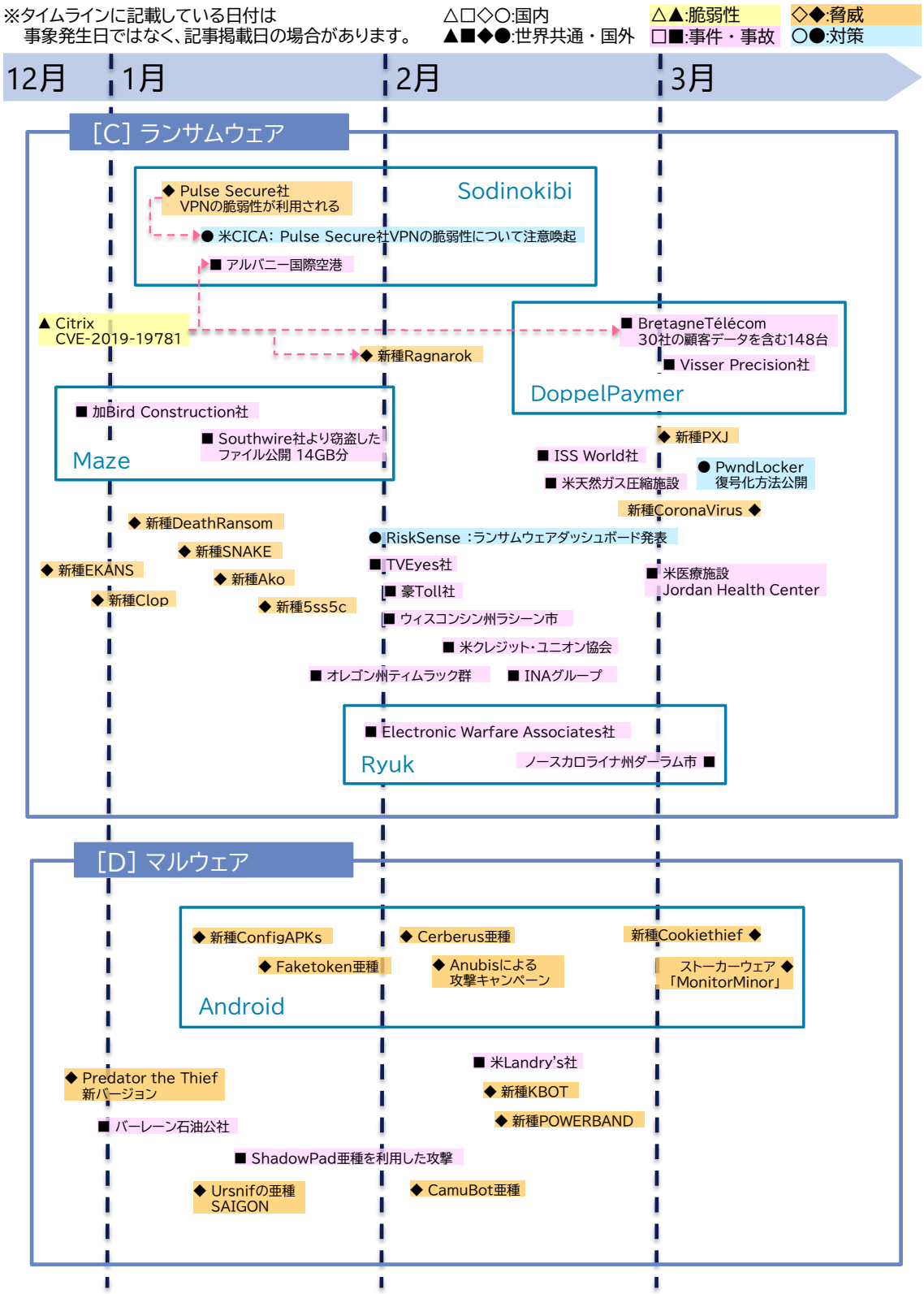
以上のような状況を踏まえると、サイバー攻撃を受けやすくなり、その被害が増えると想定されます。その中でも、特に、サイバー攻撃の高度化に対策が追いついていない箇所を狙ったサプライチェーン攻撃の被害が増加するおそれがあります。このような厳しい状況ですが、攻撃者は待ってはくれません。必要なセキュリティレベルを確保するための予算を組み、

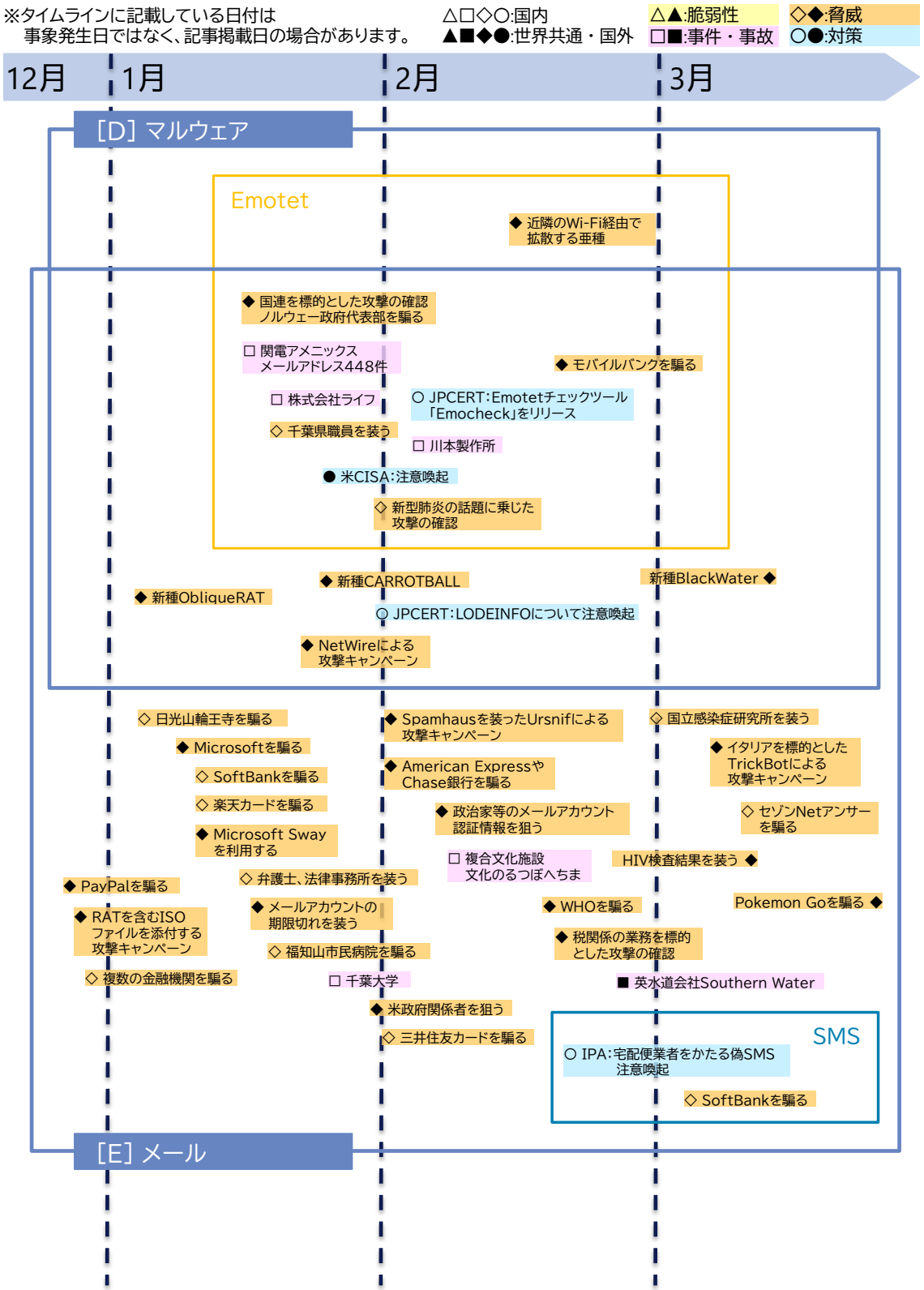
対策を行うことをお薦めします。

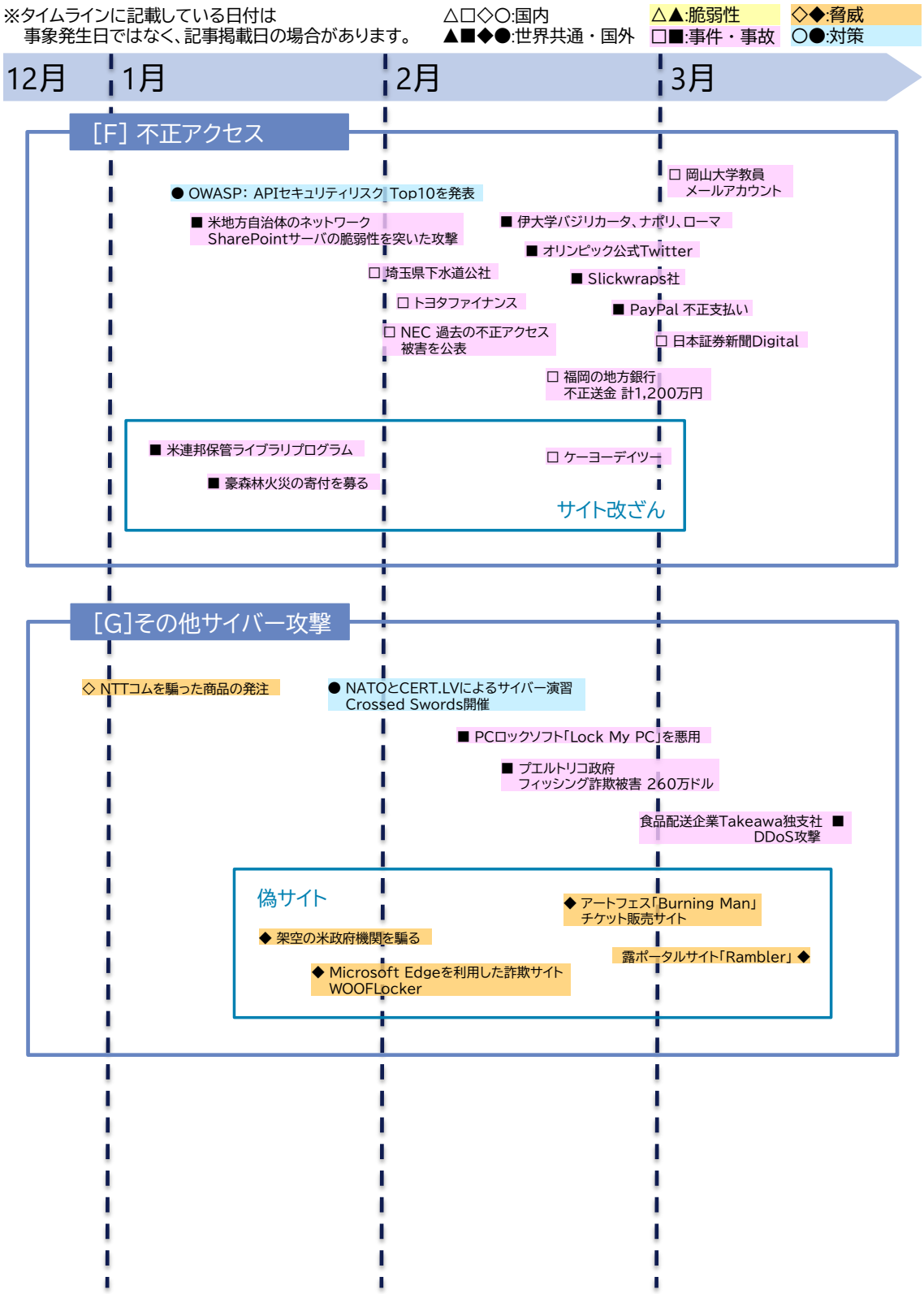
7. タイムライン











参考文献

[1] Check Point, “Coronavirus update: In the cyber world, the graph has yet to flatten - Check Point Software,” 2 4 2020. [オンライン]. Available: https://blog.checkpoint.com/2020/04/02/coronavirus-update-in-the-cyber-world-the-graph-has-yet-to-flatten/.

[2] KnowBe4, “Q1 2020 KnowBe4 Finds Coronavirus-Related Phishing Email Attacks Up 600%,” 9 4 2020. [オンライン]. Available: https://www.knowbe4.com/press/q1-2020-knowbe4-finds-coronavirus-related-phishing-email-attacks-up-600.

[3] Reason, “COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report,” 9 3 2020. [オンライン]. Available: https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/.

[4] So-net, “新型コロナ感染状況マップを装うマルウェアが登場,” 27 3 2020. [オンライン]. Available: https://securitynews.so-net.ne.jp/news/sec_30155.html.

[5] MITRE, “Azorult,” 26 7 2019. [オンライン]. Available: https://attack.mitre.org/software/S0344/.

[6] cyberreason, “Bitbucketを使用したマルウェア攻撃：正規プラットフォームの悪用,” 20 2 2020. [オンライン]. Available: https://www.cybereason.co.jp/blog/cyberattack/4381/.

[7] FORTINET, “偽の津波警報が日本にマルウェアを送り込む,” 28 12 2018. [オンライン]. Available: https://www.fortinet.co.jp/blog/threat-research/fake-tsunami-brings-malware-to-japan.html.

[8] Malware Guide, “Corona-Virus-Map.comを削除する方法,” 3 2020. [オンライン]. Available: https://malware-guide.com/jp/corona-virus-map-comを削除する方法.

[9] Lookout, “New Threat Discovery Shows Commercial Surveillanceware Operators Latest to Exploit COVID-19,” 18 3 2020. [オンライン]. Available: https://blog.lookout.com/commercial-surveillanceware-operators-latest-to-take-advantage-of-covid-19.

[10] DoaminTools, “CovidLock: Mobile Coronavirus Tracking App Coughs Up Ransomware,” 13 3 2020. [オンライン]. Available: https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware#.

[11] ESET, “2020年1月・2月 マルウェアレポート,” 31 3 2020. [オンライン]. Available: https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2002.html.

[12] ESRIジャパン, “ジョンズ・ホプキンス大学の新型コロナウイルス感染状況ダッシュボード作成の裏側,” 17 4 2020. [オンライン]. Available: https://blog.esrij.com/2020/04/17/post-35916/.

[13] ikemen.tokyo, “[注意喚起] コロナウイルス対策としてマスク無料配布を語りAppleIDを要求するSMS,” 6 2 2020. [オンライン]. Available: https://ikemen.tokyo/2020/02/sms-musk/.

[14] 日本サイバー犯罪対策センター, “新型コロナウイルスに乗じた犯罪,” 4 2 2020. [オンライン]. Available: https://www.jc3.or.jp/topics/newmodel_coronavirus.html.

[15] 佐川急便, “佐川急便を装った迷惑メールにご注意ください,” 14 5 2020. [オンライン]. Available: https://www2.sagawa-exp.co.jp/whatsnew/detail/721/.

[16] トレンドマイクロ, “実例で見るネットの危険：「新型コロナウイルス」に便乗する攻撃メール,” 4 2 2020. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/23740.

[17] kaspersky, “DNS設定を乗っ取りAndroidデバイスに感染するRoaming Mantis,” 17 4 2018. [オンライン]. Available: https://blog.kaspersky.co.jp/roaming-mantis/20105/.

[18] kaspersky, “Roaming Mantis パート2：さらなる多言語化、フィッシング、そしてマイニング,” 18 5 2020. [オンライン]. Available: https://blog.kaspersky.co.jp/roaming-mantis-update/20383/.

[19] kaspersky, “Roaming Mantis パート3：iOSでの仮想通貨マイニングと、悪意あるコンテンツ配信システムを介した拡散,” 12 10 2018. [オンライン]. Available: https://blog.kaspersky.co.jp/roaming-mantis-new-methods/21749/.

[20] kaspersky, “Roaming Mantis パート4：Apple iOS向けの悪意ある構成プロファイル、アップデートされた悪意あるapkファイル（MoqHao/XLoader）の再拡散,” 4 4 2019. [オンライン]. Available: https://blog.kaspersky.co.jp/roaming-

mantis-part-iv/22949/.

[21] kaspersky, “Roaming Mantis パート5：スミッシングによる拡散とリサーチャー避けテクニックの強化,” 8 2 2020. [オンライン]. Available: https://blog.kaspersky.co.jp/roaming-mantis-part-v/26912/.

[22] Security NEXT, “スマホ狙う「Roaming Mantis」、新型コロナ便乗も,” 2 3 2020. [オンライン]. Available: http://www.security-next.com/112732.

[23] Forbes, “世界で勃発の「コロナ給付金」詐欺、ドイツでは100億円の被害,” 26 4 2020. [オンライン]. Available: https://forbesjapan.com/articles/detail/34051.

[24] サービス&セキュリティ, “急増するフィッシング被害　二要素認証突破の手口と対策,” 29 1 2020. [オンライン]. Available: https://www.ssk-kan.co.jp/topics/topics_cat05/?p=10604.

[25] GlobalSign, “SSLの種類と利用用途,” 3 7 2019. [オンライン]. Available: https://jp.globalsign.com/ssl-pki-info/ssl_beginner/types-of-ssl.html.

[26] 三菱電機株式会社, “不正アクセスによる個人情報と企業機密の流出可能性について（第 3 報）,” 三菱電機株式会社, 12 2 2020. [オンライン]. Available: https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf. [アクセス日: 18 5 2020].

[27] 防衛省, “三菱電機㈱による機微な情報の漏えいの可能性について,” 10 2 2020. [オンライン]. Available: https://www.mod.go.jp/j/press/news/2020/02/10a.pdf.

[28] 三菱電機株式会社, “不正アクセスによる個人情報と企業機密の流出可能性について,” 20 1 2020. [オンライン]. Available: https://www.mitsubishielectric.co.jp/news/2020/0120-b.pdf.

[29] MITRE, “Lateral Movement, Tactic TA0008 - Enterprise | MITRE ATT&CK®,” MITRE, 19 7 2019. [オンライン]. Available: https://attack.mitre.org/tactics/TA0008/.

[30] 株式会社　朝日新聞社, “三菱電機へのサイバー攻撃、VPN装置にハッキングか：朝日新聞デジタル,” 株式会社　朝日新聞社, 2 5 2020. [オンライン]. Available: https://www.asahi.com/articles/ASN517HP7N4XULZU012.html.

[31] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート 2019年度第2四半期,” 29 11 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_2q_securityreport.pdf.

[32] ソフト・オン・デマンド株式会社, “弊社運営の「ＳＯＤプライム」における個人情報等流出に関するお詫び及びお知らせ,” 27 3 2020. [オンライン]. Available: https://www.sod.co.jp/apology/index.html?date=20200332.

[33] 株式会社メルカリ, “Web版のメルカリにおける個人情報流出に関するお詫びとご報告 ※6/23追記あり,” 23 6 2017. [オンライン]. Available: https://about.mercari.com/press/news/article/20170622_incident_report/.

[34] Security NEXT, “ファンクラブサイトで不具合 - 会員情報を誤表示,” 10 1 2020. [オンライン]. Available: http://www.security-next.com/111366.

[35] ソフトバンク株式会社, “お客様情報流出問題に関する、現時点までの調査結果と今後の対策について,” 27 2 2004. [オンライン]. Available: https://www.softbank.jp/corp/group/sbb/news/press/2004/20040227_01/.

[36] 株式会社ベネッセコーポレーション, “事故の概要,” [オンライン]. Available: https://www.benesse.co.jp/customer/bcinfo/01.html.

[37] 日経XTECH, “〔78〕過去最高の賠償金となったTBCの情報流出,” 19 2 2007. [オンライン]. Available: https://xtech.nikkei.com/it/article/COLUMN/20070215/262166/.

[38] 日本経済新聞, “ベネッセの「プライバシーマーク」が取り消しに,” 26 11 2014. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO80153440W4A121C1000000/.

[39] C. Systems, “CVE-2019-19781：Citrix Application Delivery Controller、Citrix Gateway、Citrix SD-WAN WANOPアプライアンスで任意のコードが実行される脆弱性について,” Citrix Systems, 17 12 2019. [オンライン]. Available: https://support.citrix.com/article/CTX269194.

[40] C. Systems, “Citrix ADC (旧称NetScaler ADC),” Citrix Systems, [オンライン]. Available: https://www.citrix.com/ja-jp/products/citrix-adc/.

[41] P. Z. India, “Remote Code Execution Exploit for Citrix Application Delivery Controller and Citrix Gateway [CVE-2019-19781],” Project Zero India, 11 1 2020. [オンライン]. Available: https://github.com/projectzeroindia/CVE-2019-19781.

[42] J. Ullrich, “Citrix ADC Exploits are Public and Heavily Used. Attempts to Install Backdoor,” SANS Institute, 11 1 2020. [オンライン]. Available: https://isc.sans.edu/diary/25700.

[43] S. Gatlan, “DoppelPaymer Hacked Bretagne Télécom Using the Citrix ADC Flaw,” Bleeping Computer, 26 2 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/doppelpaymer-hacked-bretagne-t-l-com-using-the-citrix-adc-flaw/.

[44] トレンドマイクロ, “近隣Wi-Fiネットワークを侵害する「EMOTET」の活動を確

認,” 8 2 2020. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/24017.

[45] 総務省, “平成30年版 情報通信白書｜無料公衆無線LAN環境の整備促進,” 3 7 2018. [オンライン]. Available: https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd266220.html.

[46] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート 2019年度第3四半期,” 28 2 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/news/information/2020/022801/.

[47] “The No More Ransom Project,” [オンライン]. Available: https://www.nomoreransom.org/ja/index.html.

[48] Bleeping Computer, “Ransomware Gangs to Stop Attacking Health Orgs During Pandemic,” 18 3 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/.

[49] Bleeping Computer, “Maze Ransomware Publishes 14GB of Stolen Southwire Files,” 10 1 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/maze-ransomware-publishes-14gb-of-stolen-southwire-files/.

[50] Proofpoint, “The Human Factor 2019,” 9 9 2019. [オンライン]. Available: https://www.proofpoint.com/jp/newsroom/press-releases/proofpoints-annual-human-factor-report-details-top-cybercriminal-trends-more.

[51] 厚生労働省, “新型コロナウイルスを想定した「新しい生活様式」を公表しました（新型コロナウイルス感染症）,” 4 5 2020. [オンライン]. Available: https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000121431_newlifestyle.html.

[52] Check Point, “Increase in Remote Working and Coronavirus Related Threats Creating Perfect Storm of Security Challenges for Organizations, New Survey Finds,” 7 4 2020. [オンライン]. Available: https://www.checkpoint.com/press/2020/increase-in-remote-working-and-coronavirus-related-threats-creating-perfect-storm-of-security-challenges-for-organizations-new-survey-finds-2/#.

[53] VMware Carbon Black, “Modern Bank Heists 3.0 | VMware Carbon Black,” 5 2020. [オンライン]. Available: https://www.carbonblack.com/resource/modern-bank-heists-3-0/.

NTT DATA
Trusted Global Innovator

2020年6月26日発行

株式会社NTTデータ
セキュリティ技術部
大谷 尚通 / 小林 義徳 / 大石 眞央 / 山下 大輔
星野 亮 / 出沢 信雄 / 伊藤 友洋 / 宮崎 大輔 / 宍戸 りさ / 清水 一貴
nttdata-cert@kits.nttdata.co.jp