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

2020 年度 第 1 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。

Zoomの情報セキュリティ上の問題

コロナウイルスの感染拡大に伴う働き方の変革で、オンライン会議ツール（Web会議ツール）の利用が拡大しています。なかでもZoomは、利用者が短期間で急激に増加し注目を集めました。しかし同時に、複数の脆弱性や利用者のプライバシー保護に関わる重大な問題、仕様や設計のミスなどがつぎつぎと明らかになり、セキュリティに関する懸念が広まっています。これらの中には、すでにZoom側でリスク対策がなされた脆弱性や仕様などの問題もありますが、"Zoom爆弾"など、利用者が注意しなければ回避できないリスクも残っています。本レポートでは、Zoomにどのような問題が指摘されたのか、それと併せてZoomを使用する際にどのような点に気を付ける必要があるのか、IPAが発行しているガイドラインをもとにチェックリストとしてまとめました。

ニューノーマルにおけるテレワークのセキュリティリスク

コロナウイルスは、2020年度第1四半期においても世界中で猛威を振るい、そのような状況に対応するために、世界中がニューノーマルな環境に移行していきました。そのなかでも、自宅PCからのリモートアクセス、コラボレーションツールの利用拡大、クラウドサービスの利用拡大、コミュニケーション方法の変化といった労働様式へのテレワークの本格的な導入は、特に大きな変化です。

これらの変化に伴い、自宅PCからの機密情報の漏えいや社内システム等への侵入拡大、コラボレーションツールを介した機密情報の漏えい、個人が利用するクラウドサービス上の機密情報の漏えい、個人の判断のミスによるインシデント被害の拡大といったリスクが増加しています。

このようなニューノーマルな環境では、各組織は、従来のセキュリティ対策がそのまま適用できないこと、組織のガバナンスが及ばないこと、個人がリスクを判断する必要があること等を考慮しなければなりません。組織は、これらの新たな事実に気づいた上で、ニューノーマルな環境のリスク分析を実施して、セキュリティ対策を見直す必要があると考えます。

Pulse Secure製品の脆弱性

脆弱性 CVE-2019-11510は、2019年4月に公表されたPulse Secure製品の脆弱性ですが、1年後の2020年4月になってもUS-CERTがこの脆弱性を狙ったサイバー攻撃を注意喚起しています。脆弱性の影響が長引いている原因は、この脆弱性がパッチ適用前に悪用されて認証情報を窃取された場合、パッチを適用しても被害が拡大するおそれがあるためです。このような認証情報を窃取されるおそれがある脆弱性が確認された場合、パッチ適用だけでなく、侵害の有無を確認して、侵害のおそれがある場合はパスワードを変更しなければなりません。また、SSL-VPN製品に多要素認証を導入して、認証を強化することも必要です。

予測

今後も、テレワークを中心とした労働様式のニューノーマルは継続すると想定されます。そのため、対面で実施していたビジネスコミュニケーションが、Zoomをはじめとしたオンラインツールを使った方法へ置き換わっていくと考えます。オンラインによるビジネスコミュニケーションは、なりすましや詐欺のリスクが伴うことを理解して、本人確認や情報の信頼性を確認する方法を備えなければなりません。

また、2020年上半期は約9,000件の脆弱性が報告されており、2020年は過去最高の2万件に達するおそれがあることから、テレワークにて利用されるVPN製品の脆弱性を突いた攻撃が増加すると想定されます。VPN製品は脆弱性が公開されてからサイバー攻撃を受けて侵害が発生するまでの期間が短くなっている傾向があるため、これまで以上に脆弱性に対して迅速かつ的確に対応しなければなりません。

さらに、テレワークによるクラウドサービスの利用増加により、Dockerの利用も増加していくと想定されます。セキュリティ対策が不十分なDockerを狙った攻撃も増えていくおそれがあることから、Dockerの対策を不十分な状態のままにしないために、コンテナのベストプラクティスを活用して、Dockerに対する設定のスキャンを行い、設定ルールの違反や設定ミスを明確にして対応することをお薦めします。

2. 注目トピック

2.1. Zoomの情報セキュリティ上の問題

コロナウイルスの感染拡大に伴って、世界中の多くのビジネスパーソンの働き方が大きく変化しました。職場以外の場所で仕事をするテレワーク（リモートワーク）を推進する動きが一気に加速し、そのためのさまざまなSaaSサービスも普及しました。今回はその中でも、オンライン会議ツール（Web会議ツール）として脚光を浴びたZoomに着目して、そのセキュリティ対策と、使用の際の注意点について考えてみます。

2.1.1. 利用者の急増と発覚したさまざまな問題

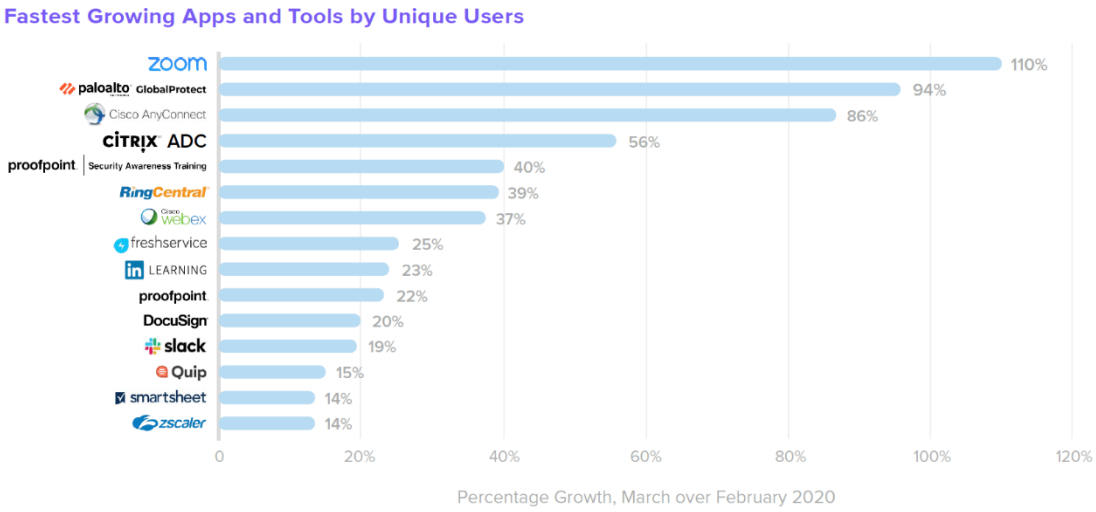


図 1：Oktaに統合されたSaaSツールの利用者の増加率
（Okta社のHP [1]より引用）

図 1は、2020年2月から3月にかけての、IDaaSツールのOktaに統合されたSaaSツールへのログイン状況ののび率を示しています。Paloalto社の"GlobalProtect"やCisco社の"AnyConnect"といった、テレワークをセキュアに実現するためのサービスを抑えて、Zoomの利用者が急激に増えていることが分かります。こうした動きは株価にも反映されており、時価総額で比較すると、Zoomを提供するZoomビデオコミュニケーションズ（以下、Zoom社）の企業価値は7大航空会社の合計を超えるとも言われています [2]。

その使いやすさや安定性から利用者の多いZoomですが、複数の脆弱性や、利用者の同意なくFacebookにデバイス分析データを送信していたこと [3]、会議の暗号化が不適切であったこと [4]などの問題が次々と明らかになり、セキュリティに関する懸念が広まることとなりました。Zoomの使用を制限する国や企業も出てきています。

2.1.2. 情報セキュリティ上の問題

情報セキュリティ対策を考えるうえで、まず押さえるべき3つの要素があります。

- 「機密性」：許可されたユーザだけが情報にアクセスできること
- 「完全性」：情報資産が正確で改ざんされていないこと
- 「可用性」：アクセス権を持つユーザが必要な時にアクセスできること

このなかでも特に、Web会議ツールを使う際に重視したい要素が「機密性」です。Web会議は、オフィスの会議室で実際に顔を突き合わせて行う会議とは違い、参加者がそれぞれの環境からアクセスするため、気付かずになりすましや盗聴、情報漏えいが発生するおそれが高いからです。Zoomに発覚したさまざまなセキュリティ上の問題のうち、「機密性」を脅かす問題について、Zoom社からの発表を含めて、以下にまとめます。

①　脆弱性

2020年に入ってから、Zoomに存在する8つの脆弱性が公表されて脆弱性情報データベースに登録されました。表 1に、脆弱性の概要と、それぞれの脆弱性が機密性・完全性・可用性に与える影響の大きさを示します。8つのうち6つの脆弱性で、機密性への影響度が「高」となっていることが分かります。

表 1：ZoomのCVE登録済み脆弱性 [5]

共通脆弱性識別子	CVSS v3 基本値※	脆弱性の概要	影響		
			機密性	完全性	可用性
CVE-2020-6109	9.8 緊急	パストラバーサルの脆弱性。アニメーションGIFを含むチャットメッセージにより、任意のファイルへの書き込み、任意のコードが実行される可能性がある [6]	高	高	高
CVE-2020-6110	8.8 重要	パストラバーサルの脆弱性	高	高	高
CVE-2020-11443	8.1 重要	パーミッション割り当てに関する脆弱性	—	高	高

CVE-2020-11469	7.8 重要	権限管理に関する脆弱性	高	高	高
CVE-2020-11500	7.5 重要	暗号アルゴリズムの使用に関する脆弱性	高	—	—
CVE-2020-11876	7.5 重要	ハードコードされた認証情報の使用に関する脆弱性	高	—	—
CVE-2020-11877	7.5 重要	暗号強度に関する脆弱性	高	—	—
CVE-2020-11470	3.3 注意	認証の欠如に関する脆弱性	低	—	—

※　共通脆弱性評価システム（CVSS）による脆弱性固有の深刻度

このほかに、脆弱性情報データベースに登録されていない脆弱性も報告されています。

- UNCパスインジェクションの脆弱性 [7] [8]

概要	会議のチャットウィンドウ上に送信したUNCパス（Windowsネットワーク上のフォルダやファイルにアクセスするためのパス）が、ほかのURLと同様にハイパーリンクに変換されてしまう
問題点	攻撃者が送信したUNCパスをクリックしたユーザのクレデンシャル情報が漏えいする危険性がある

①脆弱性 で挙げた脆弱性は、すでに修正済みです。Zoomを使用する際は必ず最新バージョンにアップデートして使いましょう。

②　会議の機密性保持やユーザのプライバシーにかかわる重大な問題

ユーザの誤解を招く暗号化仕様や、プライバシー侵害の危険性を高める設計のミスなど、①脆弱性 に挙げた脆弱性以外にも重大な問題が散見されます。

- 会議のエンドツーエンド（E2E）の暗号化が定義通りに行われていないことが判明 [4]

概要	Zoomの会議の暗号化は、「TCP接続はTLSを使用し、UDP接続はTLS接続でネゴシエートされたキーを使用してAESで暗号化する」という暗号化形態であり、「復号鍵はユーザのみが持つ」というE2Eの定義に沿わないことが判明
問題点	公式サイトには「会議はエンドツーエンドで暗号化されている」と説明されており、ユーザの誤解を招く
Zoom社の対応	Zoom社はこの件について謝罪し [9]、E2Eの暗号化機能を実装したが、株価が大幅に下落し株主から提訴されている [10]

- 会議が本来接続しないはずの中国のデータセンタを経由していることが判明 [11]

概要	ZoomのE2Eの暗号化について調査するため、カナダのトロント大学の研究チーム（Citizen Lab）が実際にZoomを使用して会議を実施してみたところ、会議の暗号化鍵が北京にあるサーバを経由していることが判明
問題点	中華人民共和国サイバーセキュリティ法に基づき、Zoomの中国拠点は、中国政府からの情報開示要求に応じる義務があるため、ユーザの機密情報が中国政府に渡るおそれが高い
Zoom社の対応	需要の急増に伴う急速な開発の過程で、ジオフェンシング（特定の地域への通信を遮断する仕組み）が誤って未実装になってしまったと弁明したうえで、すでに修正済みであると説明した [12]

- ユーザの同意を得ずに端末情報がFacebookに送信されていた [3]

概要	iOS版のZoomアプリへFacebookアカウントでログインするためにFacebook SDK（ソフトウェア開発キット）が使用されていたことで、ユーザのFacebookアカウントの有無に関わらず、IPアドレスやOSのバージョンを含む端末データがFacebookに転送されていた
問題点	プライバシーポリシには、Zoomを起動するたびにFacebookへデータを送信する旨の記載がなかった
Zoom社の対応	Zoom社はこの件について弁明・謝罪したうえでFacebook SDKを削除 [13]、プライバシーポリシを更新したが [14]、個人情報を無断で第三者に転送していたことは、カリフォルニア州消費者プライバシー法に違反するとして集団提訴された [15]

- 待機室のユーザが会議の内容を盗聴できる脆弱性 [16]

概要	Zoomサーバから待機室にいる全ユーザへ、ミーティングの復号化キーが自動的に送信される
問題点	待機室のユーザは、参加を承認されなくても、会議の内容を盗聴できるおそれがある。③運用上のリスク に記載のZoom爆弾への対策として導入されたが、脆弱性が見つかった
Zoom社の対応	Zoomサーバのプログラムを修正して対策済み

③　運用上のリスク

Zoom自体の問題ではなく、ユーザの使い方により機密性が脅かされる問題もあります。

- Zoom Bombing（Zoom爆弾） [17]

概要	SNSなどで共有されていた会議参加用URLを入手した攻撃者が会議に乱入し、暴力的な画像を画面上に表示したり、ヘイトスピーチを伴う暴言を吐くなどの嫌がらせが多数報告され、FBIが警告を発表。 単なる迷惑行為と捉えられがちだが、本来会議に関係ない第三者が会議に入り込むことによる機密性への影響が懸念される
Zoom社の対応	被害に遭わないための対策を公開 [9]

立て続けに問題が発覚したことでZoom社は2020年4月1日、90日間新規機能の開発をストップし、セキュリティやプライバシーを強化するためにリソースを投入すると発表しました[9]。また、Facebook社でCISOを務めたAlex Stamos氏を外部のアドバイザに指名するなど、組織の透明性の向上に努めるとしています。

2.1.3. Zoomの使用を制限・禁止した機関や企業

一連のさまざまな問題の発覚を受けて、Web会議ツールとしてZoomを使うことを禁止、または制限する機関や企業が増えています。その理由の多くは「セキュリティ上の懸念」であり、法律や企業のポリシに準拠していないことや、実際にZoom爆弾の被害を受けたことなどもきっかけとなっているようです。

【台湾】政府機関はZoomを使用すべきでないと勧告 [18]

- 台湾には、データセキュリティの懸念を引き起こすツールの使用を禁止するサイバーセキュリティ管理法があります。前項でまとめた一連のセキュリティ上の問題は「データセキュリティの懸念を引き起こす」として、政府機関と特定の民間組織に対してZoomを使用しないように勧告しました

【インド】政府職員はZoomを使用すべきでないと勧告 [19]

- 4月の携帯端末向けのZoomアプリの国別ダウンロード数世界1位のインドですが [20]、内務省は「Zoomは安全なプラットフォームではい」という理由で、政府職員に対してZoomを使用しないように勧告しています。これと同時に、個人的にZoomを使用する場合のガイドラインも示されました。5月に入り、Zoomに対抗する国産Web会議ツールの開発に国をあげて乗り出したという発表がありました [21]

【Google社】従業員用PCで、Zoomが機能しないように設定すると発表 [22]

- Google社は、前項で挙げたさまざまな脆弱性が自社の定めるセキュリティ基準を満たしていないとして、従業員のPCでのZoomの使用を禁止し、デスクトップ版が機能しないように設定すると発表しました

これ以外にも、ニューヨーク教育局やシンガポール教育省は、子どものプライバシー保護などを理由にZoomの使用を禁止するほか、NASAやオーストラリア軍など機密情報を扱う機関でも同様の措置が取られています。これらの動きは、Zoom社からの謝罪や脆弱性修正の報告後のことですが、高い機密性が求められる情報を扱う組織にとってはZoomを使用するリスクが非常に大きいと判断された結果と言えるでしょう。一度失ってしまった信用を取り戻すのは容易ではないことが分かります。

2.1.4. Zoomを使用する際の注意点

脆弱性が修正され、適切な暗号化方式が実装された最新バージョンのZoomを使用しても、Zoom爆弾のようにユーザが注意しなければ回避できないリスクは残ります。Zoomを使用する際はどのような点に注意すれば良いのか、IPAが発行している「Web会議サービスを使用する際のセキュリティ上の注意事項」 [23]を参考にチェックリスト形式でまとめます。

表 2：IPAによる注意事項とZoomにおける対処方法

IPAによる注意事項		Zoomにおける対処方法
会議参加者の制限を明確にし、会議の設定を適切に行っているか	非公開会議の場合は、会議を非公開に設定する	□ 会議にはパスコードを設定できる □ 待機室機能を有効にすることで、ホストが認めた参加者だけが会議に参加することができる □ 参加者が揃った時点でそれ以上のユーザが参加できないようにロックすることができる
	意図しない参加者を避けるため、会議パスワードを設定し、待機室機能を有効にする	
	参加者の入室時に許可する機能を確認する	□ 参加者のカメラやマイクのON/OFF※1、画面共有や共有画面の遠隔操作の可否※2、プライベートチャットの可否などをあらかじめ設定することができる ※1 Zoom爆弾による被害防止には、カメラやマイクのOFFがある程度有効 ※2 意図しない情報の映り込み等を防ぐ意味でも、画面のコントロールをほかのユーザに渡す必要がない場合はOFFにしておくことが望ましい
	会議の機密性、会議参加者の人数に応じ、会議案内メールと別経路での会議パスワードの送付、参加者の二要素認証、参加	□ 参加用URLにパスコードを埋め込めこまない形式に出来る ※パスコードを埋め込んだURLはワンクリックで参加できる点で利便性が高いが、

者の事前登録機能等を適切に使用する	URLを入手した不正な参加者の参加を防ぐには適さない
万が一意図しない参加者が登場した場合に備え、参加者の強制退室機能が使えることを確認したか	□ ホストは参加者を退出させることができる □ 退出させられた参加者の再参加の可否を設定することができる
組織外参加者がいる会議では特に、意図しない第三者が会議に参加しないよう、参加者確認業務の担当者を明確にしているか	□ ホスト前の参加を許可しない設定にすることで意図しない参加者の入室を防ぐことができる □ 参加者が自分の名前を変更することを許可しておくことで、本人確認可能な名前での参加が可能になる
会議録音・録画データ、共有資料、チャット等の会議データがクラウド上に存在する場合には、クライアント端末への移動・暗号化、クラウド上からの削除を実施したか	（無料会員の場合は録音/録画データはローカルに、有料会員の場合はこれに加えてZoomクラウド上に保存できる） □ ホストがクラウド上の記録を削除できる設定にできる □ 指定した日数後にクラウドの記録を自動的に削除する設定がある □ 録音/録画が意図せず第三者によって行われないように、開始/終了時に音声で通知する機能がある □ チャット上にファイルを送信する機能のON/OFFをあらかじめ設定することができる ※チャット上でのファイル共有は、意図しない参加者からマルウェアを拡散する不審なファイルが送付されるリスクがある

このほか、使用するアプリは最新版かどうか、端末のウイルス定義ファイルなどが最新かどうかは、Zoomに限らずあらゆるツールの使用に際してチェックする必要がある事項です。また、参加用URLとパスワードをSNSなどで共有することは業務で使用するケースでは推奨されません。特に機密性の高い会議の場合は、案内メールの漏えいに備え、メールの題名は機密性を悟られない文面にする、パスワードは別経路で送付するなど工夫しましょう。

社内の会議にZoomを使用して良いかどうかの基準は、会議の種別や機密性の度合い、業界の特性などを考慮する必要があるため世の中一律に定めることは出来ません。組織ごとに方針やルールを明確に定めた上で、それに沿った使い方をすることが重要です。本記事も参考にしながら、自分たちの環境でZoomをどのように考え、扱うのかをいまいちど見直してみてはいかがでしょうか。

2.2. ニューノーマルにおけるテレワークのセキュリティリスク

コロナウイルスは、2020年度第1四半期においても世界中で猛威を振るっていました。サイバー空間においても、コロナウイルスに関連したサイバー攻撃が継続して発生していました。

図 2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サイバー攻撃の件数の2020年1月～6月の推移を示したグラフです。4月下旬頃に3月末時点の約4倍のコロナウイルス関連の攻撃が発生しています。その後、攻撃件数は減少傾向にあるものの、6月時点で3月末時点の約2.5倍と、この2020年度第1四半期は、コロナウイルスに関連するサイバー攻撃が始まった2019年度第4四半期よりも非常に多くのコロナウイルス関連のサイバー攻撃が発生しています。また、日本においてもコロナウイルス関連の攻撃が同様に発生しています。

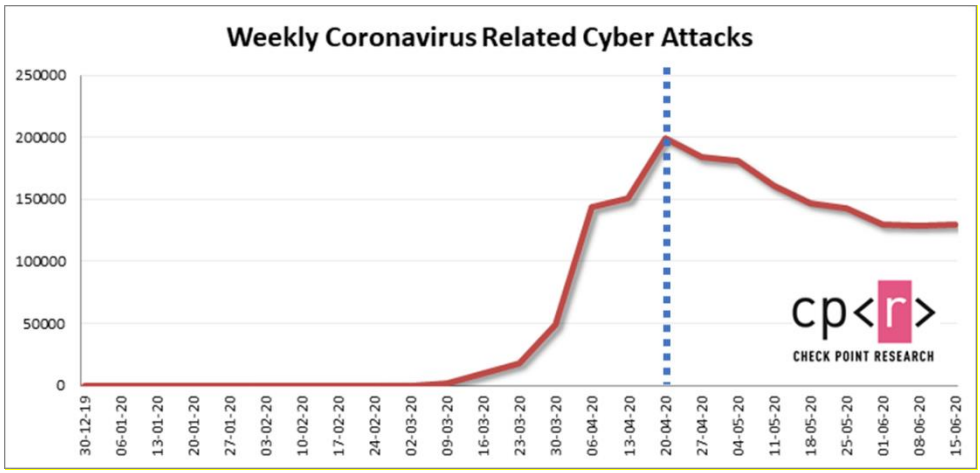


図 2：コロナウイルス関連のサイバー攻撃数の推移
(Check Point Blog [24]より引用)

コロナウイルス流行に対抗して、2020年5月ごろから日本では、これまでと違った新しい生活様式が使われはじめました。このように、コロナウイルスと共生していくために、世界中がニューノーマルな生活様式へ移行していきました。そのような変化のなかでも、労働が生活の中で多くの割合を占めること、労働を行う人だけでなくその関係者にも影響があることから影響を受ける人が多いこと、場所、業務、システム等多くのことが変化すること等から、労働様式がテレワークに変化したことは最も大きな変化と言えます。労働環境、技術、運用が大きく変化すれば、既存のセキュリティ対策ではカバーできていない部分が多く発生します。攻撃者は、このような労働様式がテレワークへ変化した部分を狙って、新たなサイバー攻撃を行っています。

2.2.1. テレワークを狙った攻撃

日本では、2020年4月～6月の間に緊急事態宣言等によりテレワーク、時差勤務、感染対策を行った上でのオフィスの利用が始まり、労働環境が大きく変化しました。アメリカにおいても、テレワークを実施している労働者の割合が、3月中旬の31%から4月上旬の62%へ増加しています [25]。このように、さまざまな国で、同様に労働環境の大きな変化がありました。この労働環境の変化に対応して増加した3つの攻撃を紹介します。

1つ目の攻撃は、リモートデスクトッププロトコル（RDP）で接続できる機器へのブルートフォースアタックです。RDPは、テレワークに必要なサービスです。しかしながら、インターネットからRDPポートへ直接アクセスできるセキュリティが不十分な状態で利用している場合があります。コロナウイルスの流行により、テレワークへの移行が始まりだした2020年1月～4月の間で、インターネットからアクセス可能なRDPポート数は約300万個から約450万個へと1.5倍ほど増加しています [26] [27] [28]。そして3月以降は、このようなRDPに対するブルートフォースアタックも増加傾向にあります [29] [30]。

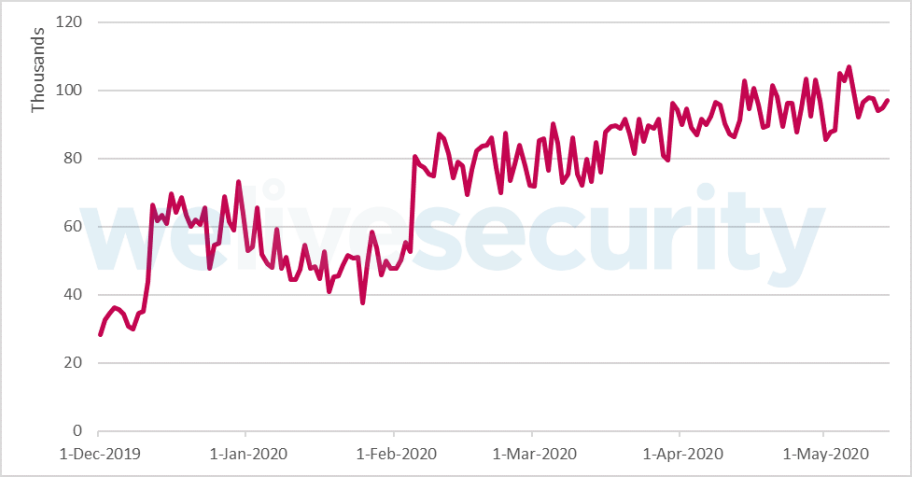


図 3: 単一クライアントに対するRDPへの攻撃試行の傾向
（ESET社のblog [30]より引用）

2つ目の攻撃はテレワークを狙ったフィッシング攻撃です。テレワークの拡大により、VPN接続やオンライン会議ツール、クラウドサービスの利用が増加しました。それらを狙ってフィッシング攻撃が増加しました。フィッシングメールを送付してフィッシングサイトへ誘導、資格情報などを窃取するフィッシング攻撃の手法は、従来の手法と大きく変わりません。コロナウイルス流行下で発生したテレワークを狙ったフィッシング攻撃の事例を以下に示します。

表 3：テレワークを狙ったフィッシング攻撃の事例 [31] [32] [33] [34]

フィッシングメールの内容	フィッシングサイト	窃取する資格情報
VPNの設定変更の通知	Office365のログインページ	Office365
Zoomの会議に関する通知	Zoomのログインページ	社用のメールアドレス
Microsoft Teams上の会話に関する通知	Office365のログインページ	Office365
Webexの証明書に関するエラー通知	Webexのログインページ	Webex

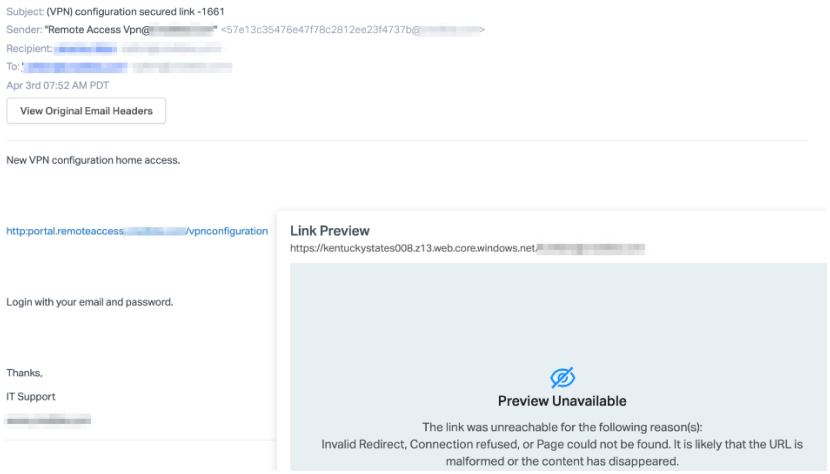


図 4：VPNの設定変更の通知を装ったフィッシングメール
（Abnormal Security社のHP [31]より引用）

3つ目の攻撃は、テレワークを狙った偽インストーラや偽スマートフォンアプリの配布です。オンライン会議ツールとして利用者数が急激に伸びたZoomやVPNクライアントソフトを騙って配布された偽インストーラや偽スマートフォンアプリの事例を以下に示します。

表 4:テレワークを狙った偽インストーラ/スマートフォンアプリの事例 [35] [36]

偽アプリ	対象OS	偽アプリのインストール時の動作
Zoomの偽インストーラ①	Windows	● 偽インストーラが、実行中のすべてのRemote Utilitiesに関連するプロセスを強制終了させる ● WindowsファイアウォールへTCP 5650ポートの受信を許可する設定を追加する ● レジストリに、以下の偽アプリの動作状況等と、それらをC&Cサーバに通知するための設定を追加する ✓ メール送信先情報 ✓ 認証情報を窃取済みであること ✓ 本感染PCがアクセス可能な状態であることを遠隔操作サーバ（C&Cサーバ）へ通知するための設定 ● 偽インストーラが正規のZoomをダウンロードしてインストール
Zoomの偽インストーラ②	Windows	● 偽インストーラが、インターネット上から、以下の機能を持つマルウェアと正規のZoomをダウンロードしてインストールする ✓ ユーザのデスクトップとアクティブなウィンドウのスクリーンショットを取得する ✓ システムをスキャンして、接続されているWebカメラを探す ✓ 上記の情報をC&Cサーバへ送信する ● 偽インストーラが正規のZoomをダウンロードしてインストール ● PCの起動後、マルウェアも自動起動して収集したすべての情報を30秒ごとにC&Cサーバへ送信する
VPNクライアントソフトの偽スマートフォンアプリ	iOS	● App store上から有料アプリとしてダウンロードしてインストールする（デバイスから個人情報を盗む等、悪意のある動作をしないため審査を通過している） ● App storeからダウンロードするときにサブスクリプション料金の支払いが発生する ● 偽スマートフォンアプリを起動しても、VPN接続機能が実装されていないため、VPN接続できない

今回紹介したどの事例も攻撃手法は従来と大きく変わりません。ただし、以下のようなニューノーマルな状況下を上手く悪用して、攻撃を成功させやすくしています。

- 業務継続を重視して、急いでテレワーク環境を構築したため、設定のレビューや設計が不十分
- フィッシング攻撃は、VPN接続やオンライン会議ツール、クラウドサービスの使用に慣れていない状況、かつ以前よりも受信するメールが増えている状況で、フィッシングメールの判断が難しい
- 偽インストーラや偽スマートフォンアプリは、新しくこれらのソフトウェアの利用を開始する人が多いために、引っ掛かりやすい状況である
- フィッシング攻撃や偽インストーラや偽スマートフォンアプリは、テレワークのため、新しいソフトウェアの正しい情報を周りから入手できないこと、上司や同僚へ相談することが難しい

2.2.2. ニューノーマルにおけるテレワークのリスク

前述で挙げたテレワークを狙った攻撃は一部にすぎません。これら以外にどのようなセキュリティ上のリスクがあるのか、以下のテレワークによって変化した項目のリスクを分析しました。

① 自宅のPCからのリモートアクセス
② コラボレーションツールの利用拡大
③ クラウドサービスの利用拡大
④ コミュニケーション方法の変化

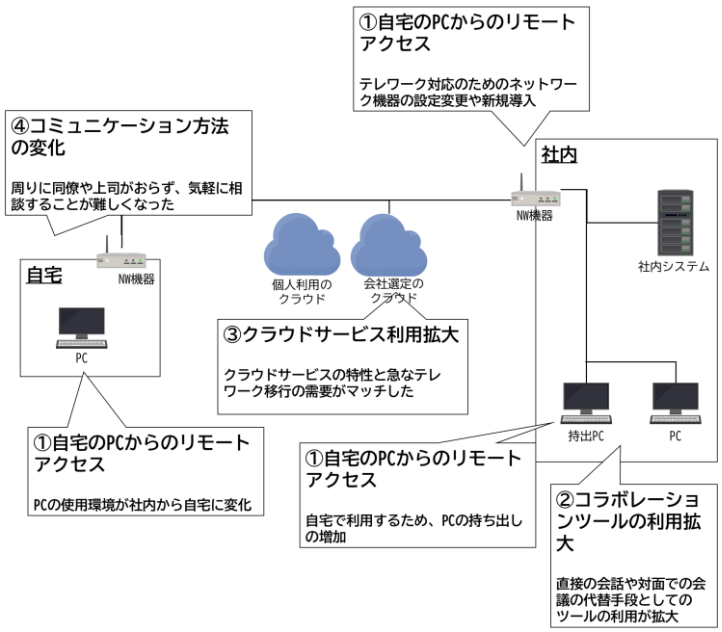


図 5：テレワークによる変化

① 自宅のPCからのリモートアクセス

1つ目は、テレワーク対応のため、PCを自宅へ持ち出したり、PCの使用環境が社内ネットワークから自宅の家庭ネットワークへ変化したりすることで、PC自体がサイバー攻撃を受けて被害が発生するリスクが増加しています。PCは、社内ネットワークに接続している状態よりも、ウイルス感染やランサムウェア被害、情報漏えい、クリプトマイニングなど、さまざまな情報セキュリティインシデントが起きやすい状況です。特にテレワークで使用しているPCは、社内ネットワークで使用していた時よりも機密情報の漏えいのリスクが高いため、情報漏えいインシデントの発生件数が増加すると推測できます。PCからの情報漏えいは、機密情報の漏えいだけでなく、認証情報の漏えいによるリスクに注意しなければなりません。PC上からさまざまな認証情報が漏えいすると、BECメールのリスク、社内ネットワークや使用しているクラウド環境への侵入など、大きな被害へ発展するおそれがあります。原因は、PCへのセキュリティパッチの適用やウイルス対策等のセキュリティ対策が個人任せになったためです。PCを社内ネットワークへ接続していた時のように自動的にセキュリティパッチを適用するなどのコントロールが困難になり、セキュリティ対策が弱体化しました。

2つ目は、攻撃者が社内ネットワークやクラウドへ侵入したり、マルウェアが社内ネットワークやマシンへ持ち込まれたりするリスクです。テレワークが拡大する前から、社外へ持ち出したPCを経由してマルウェアが持ち込まれたり、PC上のバックドアを経由して社内ネットワークへ侵入されたりするインシデントは発生していました。しかし、テレワーク拡大により、持ち出しPCの台数が大幅に増加して、上記のリスクが爆発的に増加しています。原因は、これまでの境界防御の考え方に基づくセキュリティ対策では、テレワーク主体の労働環境のリスクへ十分に対策できないためです。ゼロトラストの考え方に基づいたセキュリティ対策を検討して実施しなければなりません。

3つ目は、テレワーク対応で急遽、ネットワーク機器の設定を変更したり、新たにネットワーク機器を導入したりしたために発生したリスクです。上記のリスクの原因は、事業継続するために可用性重視で急いでネットワーク機器を導入したためです。ネットワーク機器の設定変更のレビューや安全な設計が不十分だったからでしょう。加えて、攻撃者が、急増したテレワーク用のネットワーク機器の脆弱性を集中的に狙っていることも原因です。

② コラボレーションツールの利用拡大

テレワークにより、直接会話する機会や対面の会議開催が難しくなりました。それらを補完するために、

Microsoft TeamsやSlack等のコミュニケーションをサポートするツールや、ZoomやWebex等のオンライン会議ツールの利用が拡大しました。これらのコミュニケーションツールの使用に伴い、新たなリスクが発生しました。これらのツールには、ファイル共有機能やチャット、インターネット上でさまざまな人が会議へ参加できる機能があります。攻撃者がこれら

のツールを悪用したり、利用者が操作を誤ったりした場合に、業務に関する機密情報が漏えいするおそれがあります。例えば、攻撃者が関係者を装ってチャットへの参加を要求して、ユーザがそれを誤って承認した場合、チャットの内容やチャット中に共有されたファイルが漏えいします。

③ クラウドサービスの利用拡大

デジタルトランスフォーメーションの流行によりクラウドサービスの利用が拡大していました。これに加えて、テレワーク対応により、さらにクラウドサービスの利用が拡大しました。テレワーク時のクラウドサービス利用における主なリスクを2つ取り上げます。

１つ目は、組織で使用するクラウドサービスに関わるリスクです。クラウドサービスは、オンプレミス環境と比べて、セキュリティ対策を考慮せずに誰でも容易に構築できてしまうこと、セキュリティの設定方法が大きく異なるため設定不備が発生しやすいことから、ニューノーマルの前から情報の漏えい等のインシデントが発生していました。上記に加えて急速なテレワーク移行に対応するために、業務継続を優先して短期間でクラウドサービスの利用を開始したため、クラウドのセキュリティ設計が不十分なおそれがあります。短期間で利用を開始したクラウドサービスについては、直ぐに、設定を見直すことをお薦めします。また、仮に、スキルが不足する等見直しが難しい場合には、設定不備等を自動で検知するクラウドセキュリティポスチャ管理（CSPM）製品、設定の診断サービス等が有用です。

2つ目は、個人で利用しているクラウドサービスに関わるリスクです。テレワーク環境の場合、個人が利用しているクラウドサービスを制限することが難しく、危険な設定のクラウドサービスも利用できてしまいます。業務でそのようなクラウドサービスを使用すると、第三者から攻撃を受けてクラウドサービス上の機密情報が漏えいするおそれがあります。

④ コミュニケーション方法の変化

職場で働いていた時と異なり、テレワーク環境では周りに上司や同僚はいません。そのような状況では、ウイルスに感染した時やフィッシングメールを受信した時など、セキュリティに関して迷った時に気軽に相談することができません。自分で判断して行動する必要があります。そのために、判断が遅れたり誤ったりしてインシデント対応が遅れて、被害が拡大するおそれがあります。このリスクは、ニューノーマル下のセキュリティ対策に広く影響します。労働環境やコミュニケーションスタイルが大きく変化したため、これまで蓄積していたセキュリティ管理策のノウハウが通用しません。これまでの常識や経験に固執せず、セキュリティ対策の考え方を大きく変えていかなければならないでしょう。

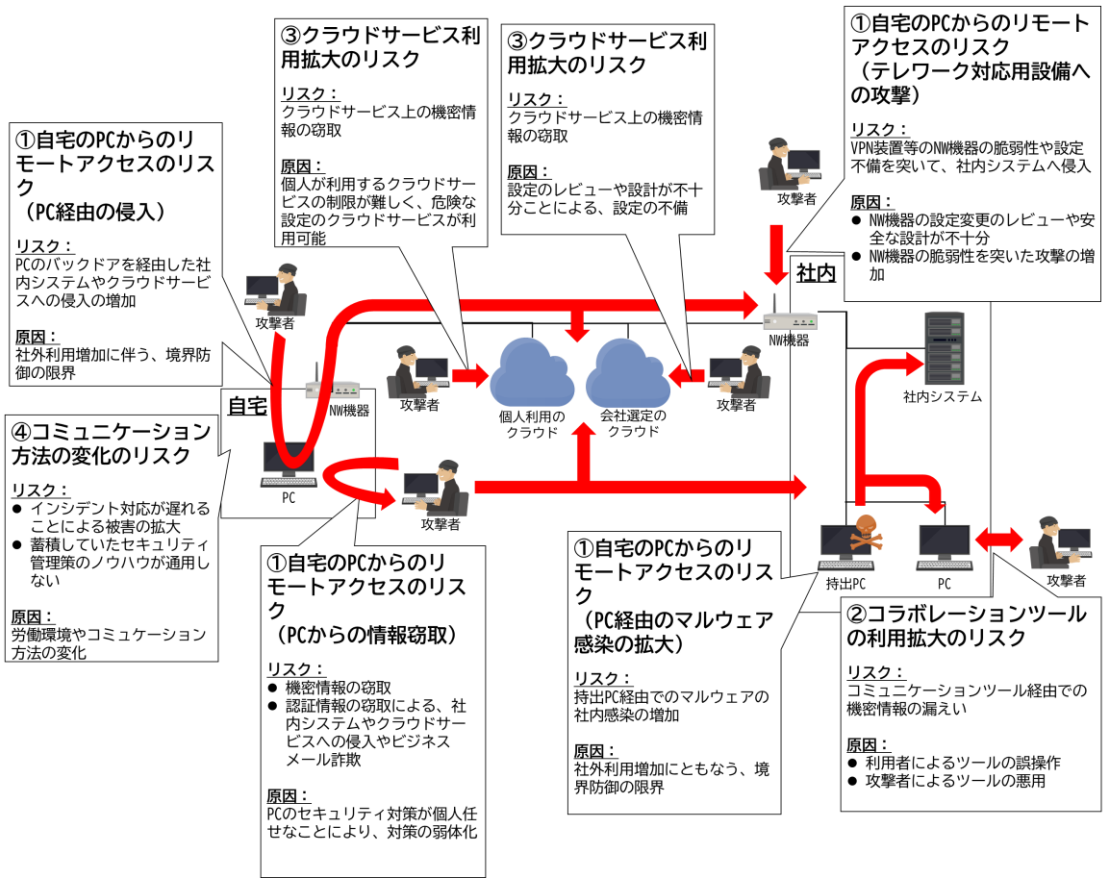


図 6：テレワークの変化に伴うリスク

2.2.3. まとめ

多くの企業は、テレワークの導入をはじめニューノーマルな働き方への変革により、大きな環境の変化がありました。セキュリティリスクも大きく変化しており、前項で挙げたような新しいリスクが発生しています。これまでのセキュリティ対策では、大きく変化したセキュリティリスクへ対応できません。よって、ニューノーマルな環境のリスク分析を実施して、セキュリティ対策を見直す必要があると考えます。リスク分析やセキュリティ対策の実施にあたっては、以下のようなことに気を付けると良いでしょう。

- リスク分析の対象は、社内環境だけでなく、クラウドサービスや自宅環境を考慮すること
- 従来のセキュリティ対策がそのまま適用できないこと
- セキュリティ対策の管理策を検討する際には、クラウドサービスや自宅、個人所有PCなど、会社のガバナンスが及ばないことを考慮すること。
- 個人がセキュリティリスクを判断しなければならないこと。個人の判断に依存しないためには、技術的なセキュリティ対策を増やすこと。

- 個人が会社からのセキュリティ関連の情報を受け取りやすくすること。気軽に相談でできる窓口や手段を用意すること
- インシデントの発見や対応が遅延する場合を考慮した対応方法を検討すること

3. 情報漏えい

2020年度第1四半期は、2019年度から引き続きWebスキミングや設定不備による情報漏えいが確認されています。2019年度第4四半期は、ソフト・オン・デマンド社の事例が大きな話題を呼びました。2020年度第1四半期は、同様な海外のアダルトサイトからの情報公開が確認されました。

3.1. 「CAM4」の情報公開

米国のアダルトライブチャットプラットフォーム「CAM4」において、ユーザの氏名、性的指向、支払い記録といった個人情報や不正、スパム検出ログ等の内部情報を含む100億8800万件、7TB分のデータが公開状態にあったことが明らかになりました。セキュリティ調査を行っている団体 Safety Detectivesがインターネット接続機器の検索エンジン「SHODAN」を使って公開サービスの調査をして、この事実を発見しました。Safety DetectivesがCAM4を所有するアイルランドの企業「Granity Entertainment」へ情報が公開されている事実を連絡したところ、30分以内に情報公開は停止されました [37]。

3.2. 情報公開の原因

情報公開の原因は、検索エンジン「ElasticSearch」の設定ミスでした。本来、機密情報として扱うべき情報が設定ミスにより外部から閲覧可能な状態となっていました。ElasticSearchは、アプリ検索、ログ分析、コンテナ監視等へ利用できるオープンソースの全文検索エンジンです。オンプレ環境からクラウドまで幅広く利用されています。今回の情報公開の原因が具体的にどのような設定ミスであったかは現時点で不明です。過去のElasticSearchの設定ミスによる情報漏えい2件は、いずれもログイン認証の不備が原因でした。CAM4の情報公開の原因も、ログイン認証の設定ミスのおそれがあります。

3.2.1. 類似事例. エクアドル

2019年9月16日、イスラエルのVPN監査サービス企業「vpnMentor」から、エクアドルのほぼ全国民の情報がインターネット上から閲覧可能になっていたことを発表しました。閲覧可能になっていた情報の中には、氏名、生年月日、電話番号、国民ID番号、家系図等の情報、計2000万人以上の個人情報が含まれていました。原因は、ElasticSearchサーバが認証なしでアクセス可能となっていたことでした [38]。

3.2.2. 類似事例. 本田技研工業

2019年7月31日、クラウドフレア社のJustin Paine氏は、本田技研工業の従業員のメールアドレス、内部ネットワークのセキュリティ関連情報が閲覧可能状態になっていることを発見しました。特にセキュリティに関する情報には、セキュリティ対策の弱点、適用パッチ、エンドポイントセキュリティソフトウェアのステータスの情報が含まれていました。

原因は、ElasticSearchサーバへ認証なしでアクセス可能となっていたことでした。本田技研工業がアクセスログを確認したところ、第三者がデータをダウンロードした形跡はありませんでした [39]。

3.3. 「CAM4」の対応と情報漏えい防止策

Safety Detectivesの調査によると、CAM4のElasticSearchは悪意のある第三者からアクセスされた形跡がなく、情報の漏えいは確認されなかったと公表しています。Safety Detectivesからの連絡後、30分で公開を停止した素早い対応も、被害発生を防ぎました [37]。ただし、もしCAM4のログの記録期間が情報公開期間よりも短い場合は、アクセスの形跡が消えているおそれがあります。その場合は、CAM4のユーザの氏名、性的指向、支払い記録といった個人情報が漏えいしているおそれがあります。

この情報漏えいを防ぐためには、設定手順を文書化するなどして設定ミスを防ぐ方法と、インターネット側から対象サービスのネットワークスキャンを定期的に実施してアクセス可能な通信ポートを調査する方法が有効です。これはElasticSearchの管理者用のログインページは外部公開しないように設定することが望ましいためです。加えて、サイバー攻撃や脆弱性による情報漏えいを早期発見するために、ElasticSearchへの外部からのアクセスを監視するツールを導入したりログを定期的に調査したりする方法が有効です。

3.4. まとめ

CAM4の情報公開は、100億件以上のレコードが閲覧可能となっていながら、データの流出は認められなかったため、深刻な事態にはなりませんでした。しかし、一歩間違えれば大規模な情報漏えい事故となっていました。クラウドの発展により、サービスを構築してインターネット上へ公開することが容易になりました。その反面、ログイン認証やアクセス制御などのセキュリティ対策の重要性を理解せずにクラウド上へサービスを構築したり、設定を変更したりして、インシデントが発生するケースが増えています。クラウドを使ってインターネットへ公開するサービスを構築する際には、基本的なセキュリティ対策の考え方を踏まえて実施することを強く推奨します。

3.5. 2020年度第1四半期情報漏えい事例

表 5：2020年度第1四半期で発覚した情報漏えい

日付	組織	原因	概要
4/10	フエルモール	システム脆弱性	SQLインジェクションによりクレジットカード情報94件を含む最大12万件の顧客情報が流出 [40]
5/7	NTTコム	サイバー攻撃	シンガポール拠点のサーバが攻撃を受け、顧客621社の情報が流出したおそれがある [41]
5/8	日本経済新聞社	フィッシング攻撃	メールの添付ファイルからマルウェアに感染。約1万2千件の従業員情報が流出 [42]
5/19	メルセデスベンツ	設定ミス	GitLab上でスマートカー用コンポーネントが公開状態となっていた [43]
5/19	イージージェット	サイバー攻撃	サイバー攻撃により約900万件の顧客情報が流出 [44]
6/9	任天堂	パスワードリスト攻撃	ゲームソフト購入に利用された個人アカウント約30万件が流出 [45]

4. 脆弱性

本章では、Pulse Secure製品に生じた脆弱性（CVE-2019-11510）について解説します。この脆弱性がパッチ適用前に悪用された場合、パッチを適用しても、被害が拡大するおそれがあるため、侵害有無の確認や認証強化が必要です。

4.1. Pulse Secure製品に発生した脆弱性

CVE-2019-11510は、Pulse Secure社のSSL-VPN製品の脆弱性です。攻撃者はこの脆弱性を悪用することで、認証を回避して、任意のファイルを閲覧することができます。

グローバルセキュリティ動向四半期レポート（2019年度版 第2四半期） [46]にも記載したとおり、この脆弱性は2019年4月に公表された脆弱性であり、パッチ[1]は既に公開されています。しかし、2020年以降もこの脆弱性を悪用した攻撃が報告[1]されています。このような状況を受けて、2020年4月16日、US-CERT（CISA）は悪用事例や対策をまとめた注意喚起（AA20-107A） [47]を発行しました。

表 6：CVE-2019-11510に関わるニュース

日付	概要
2019/04	CVE-2019-11510公表 [48] Pulse Secureがパッチをリリース
2019/08	Bad Packets社が悪用を試みるスキャンを観測 [49]
2019/09	JPCERT/CCが注意喚起 「複数のSSL VPN製品の脆弱性に関する注意喚起 [50]
2020/01	US-CERTが注意喚起（AA20-010A） [51]
2020/04	US-CERTが注意喚起（AA20-107A） [47]

4.2. 脆弱性を狙った攻撃事例と対策

攻撃者は、URIにディレクトリトラバーサルを狙う文字列を組み込んだリクエストを送信して認証を回避して、任意のファイルを閲覧することができます。攻撃者が、このCVE-2019-11510の脆弱性を悪用して平文の認証情報を窃取できた場合、攻撃者は正規のユーザになりすまして、SSL-VPN接続が可能になります。一度、認証情報を窃取されてしまうと、パッチを適用して脆弱性を修正した後も、攻撃者は不正にSSL-VPN接続ができます。実際に、パッチ適用後も攻撃者が認証情報を悪用してSSL-VPN接続して、内部ネットワーク上のマシンへ不正ログインして、エンドポイントセキュリティの無効化、およびランサムウェアをインストールした事例 [52] が報道されています。

CVE-2019-11510を対処していないPulse Secure社のSSL-VPN製品を利用している場合、まずはパッチ適用が必要です。また、パッチ適用と同時に、攻撃者によるパッチ適用前の脆弱性の悪用有無を調査する必要があります。しかし、攻撃者が脆弱性を悪用して認証情報を閲覧した痕跡はログから確認できません。そのため、認証ログから、窃取された認証情報を悪用した不正アクセスの有無を確認する必要があります。

認証情報の窃取を確認する場合、ログから正規ユーザになりすました不審なログインの痕跡を探します。例えば、当該ユーザの普段とは異なるホスト名、IPアドレス、時間帯の認証成功や短期間で送信元IPアドレスのレンジが大きく異なっている認証成功がないか確認します。

脆弱性が悪用されたおそれがある場合、窃取された情報を悪用した不正アクセスを防ぐために、必ずPulse Secure製品へログインする運用管理者のアカウント、Pulse Secure製品へSSL-VPN接続するための全ユーザのアカウントのパスワードを変更してください。

4.3. まとめ

今回は、Pulse Secure製品の脆弱性を取り上げました。通常、脆弱性対応は迅速なパッチ適用が重要とされていますが、CVE-2019-11510はパッチ適用後も被害が拡大するおそれがあるため、パッチ適用前の侵害有無を確認する必要があります。また、侵害されたおそれがある場合は、認証情報の変更等の対策が必要になります。

JPCERT/CCの調査 [53]によれば、2020年3月24日時点で、日本国内に298件の脆弱なPulse Secure製品が見つかっており、引き続き対応が必要な状態です。コロナウイルス感染拡大の影響により、テレワークが広がり、SSL-VPN製品は今後も普及していくと考えられます。SSL-VPN製品を利用する際には、定期的な脆弱性情報の収集や迅速なパッチ適用だけでなく、認証情報を窃取されるおそれがある脆弱性が公表された場合は、侵害確認する必要があります。また、多要素認証を導入して認証を強化することで、認証情報が窃取された場合でも不正アクセスのリスクを低減することができます。

5. マルウェア・ランサムウェア

5.1. 2020年度第1四半期の概況

2019年度第4四半期に引き続き、SodinokibiやSnake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。

2019年度第4四半期のグローバルセキュリティ動向四半期レポート [42]では、SodinokibiやMazeなど情報を盗み出すタイプのランサムウェアが、個人、特に政治家や芸能人といった著名人を狙うおそれがあると予測しました。予測の通り、2020年度第1四半期に著名人がランサムウェアの被害を受けました。

2020年5月、メディアやエンターテイメント分野に携わる多くの著名人を顧客として持つ米大手法律事務所Grubman Shire Meiselas & Sacks社がREvilランサムウェア（Sodinokibiの別名）の攻撃を受けて、歌手のレディ・ガガやマドンナなどの顧客データが窃取されました[54]。攻撃者は、犯行の証拠として、窃取した契約書や個人情報等が含まれたデータ756GBをダークウェブのフォーラムに投稿しました。攻撃者は、身代金として4,200万ドルを要求しており、支払われない場合は、徐々に情報を公開すると脅しました。これまでは窃取した情報を単に公開するだけでしたが、身代金が払われない場合にも金銭を得る手段として、情報公開を使った脅迫を始めたと推測します。また、攻撃者が金銭を得る手段はこれだけにとどまりません。REvilランサムウェアの攻撃者は、オークションサイトを開設して企業から窃取した情報を販売しています [55]。オークションサイトの告知では、法律事務所から窃取した歌手のマドンナなどの情報も公開すると示唆しています。窃取した機密情報のオークションは、身代金の支払いを拒否されたときに金銭を得るための代替手段というだけでなく、オークションの結果、個人情報が犯罪者の手に渡ってより大きな被害が発生することを想起させて、身代金を支払うように仕向けることができる狡猾な戦略だと思います。このように情報の価値が高い著名人の個人情報を標的としたランサムウェアは、一層増加するおそれがあります。

2020年第1四半期においても、コロナウイルスの世界的流行に便乗したサイバー攻撃が数多く報告されています。一部のランサムウェアの攻撃者は「医療機関を標的とした攻撃を行わない」と声明を出しましたが、国際刑事警察機構（INTERPOL）によると、実際には世界中の病院でランサムウェアを使ったサイバー攻撃が急増しました [56]。コロナウイルスの感染が再拡大するなか、これに便乗したサイバー攻撃は、医療提供者のみならず、研究所、医療機器メーカー、物流会社等のサプライチェーンまで範囲が拡大するおそれがあります。引き続き警戒が必要です。

日系企業を標的としたランサムウェアの被害も発生しました [57]。自動車メーカーのホンダは6月8日にサイバー攻撃を受けて、世界的な大規模システム障害が発生しました。本社などのオフィスのパソコンが使えなくなるだけでなく、ネットワークシステムにも影響が広が

り、国内外の工場で生産や出荷が一時止まりました。詳細は公表されていませんが、Snake(EKANS)ランサムウェアが全社に広がったと推測されています。

5.2. コンテナ環境を狙った攻撃の具体事例

ランサムウェアの攻撃対象はテクノロジーの進化と共に変化しています。近年、多くの組織がデジタルトランスフォーメーション（DX）を推進しており、その取り組みを加速させる手段としてクラウドを採用する組織が増えています。なかでも、開発を効率的に行うことができるコンテナ技術に注目が集まっています。コンテナ技術を用いてアプリケーションの開発を行うソフトウェアの一つであるDockerにおいて、Docker Daemon APIの設定不備を狙ったKinsingマルウェアが報告されました [58]。Kinsingマルウェアの目的は、コンテナ環境のCPUやメモリといった計算リソースを不正使用した暗号資産の発掘（クリプトマイニング）です。Kinsingマルウェアは以下の表 7の手順で攻撃を行います。

表 7：Kinsingマルウェアの攻撃手順 [59, 60]

#	分類	概要
1	侵入	オープン状態のDocker Daemon APIポートに接続する
2	コンテナ起動	Ubuntuコンテナを起動する
3	自己防衛	シェルスクリプトをダウンロードし、以下を実行する ● 再起動後もコンテナが自動的に実行されるよう設定する ● セキュリティ対策を無効にして、ログをクリアする ● 他のマルウェアやクリプトマイナーを停止する。他のマルウェアやクリプトマイナーに関するファイルを削除する ● 競合するDockerコンテナを強制終了して、それらのイメージを削除する ● Kinsingマルウェアをダウンロードする
4	マルウェアの実行	Kinsingマルウェアを実行して以下を行う ● 暗号資産の発掘(クリプトマイニング)を行う ● 様々な情報を収集して、C&Cサーバへ送信する ● 収集した情報を使用して、ネットワーク内の他ホストやコンテナ環境へマルウェアを感染拡大する

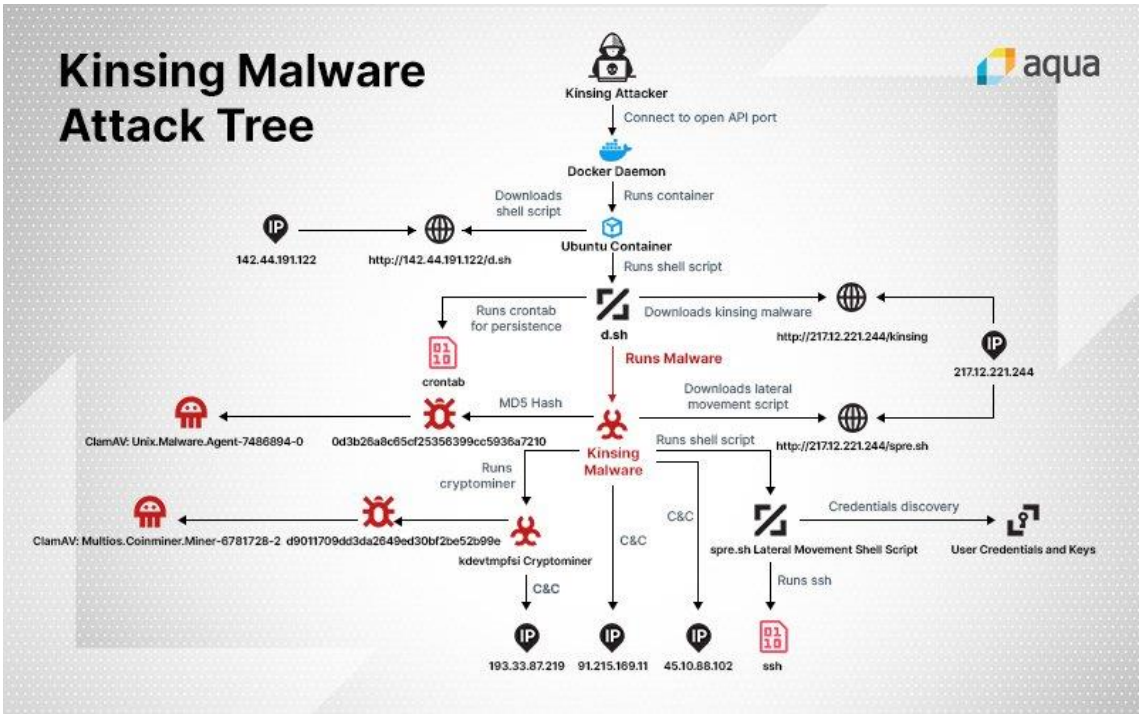


図 7：Kinsingマルウェアの攻撃フロー
（Aqua Security社の技術ブログ [58]より引用）

Kinsingマルウェアが非常に危険な点は、Docker Daemon APIポートを侵害して、root権限を奪うことです。root権限を使用できるため、コンテナを新規に立ち上げる、ファイアウォール等の設定を変更しセキュリティ対策を無効にする、攻撃に必要なツールをインストールする、競合するマルウェアを削除するなどして、クリプトマイニングをより効果的に実行できます。また、マルウェアを感染拡散するスクリプトを実行して、コンテナネットワーク全体に被害が拡大します。root権限を持ったKinsingマルウェアは、コンテナを新規に立ち上げることができるため、従量課金制のコンテナサービスを利用している場合、利用料金が高額になるおそれもあります。

対策は、Docker Daemon APIを正しく設定すること、コンテナ環境のAPIが信頼できるソースにしかアクセスできないように設定することなどがあります。コンテナに特有のセキュリティリスクと対策観点をまとめた文書“Application Container Security Guide”（NIST SP 800-190）が、アメリカ国立標準技術研究所（NIST）から公開されています [61]。本文書の記載によると、Kinsingマルウェアには、コンテナからの通信先制限やCenter for Internet Security Docker Benchmark(CIS Benchmarks) [62]などを活用したコンテナの設定やバージョンのスキャンが有効です。スキャンは自前でコンテナを構築した場合に限らず、他者が構築済みのコンテナを利用する場合も実施するべきです。また、新しく公開された脆弱性がコンテナに含まれる場合もあるため、スキャンを継続的に実施しましょう。コンテナ技術を活用したアプリケーションの開発においては、この文書がセキュリティ確保のスタンダードになります。

最近ではコンテナ向けセキュリティ対策製品も登場しており、こういった製品を活用することも有用です。 [63]

5.3. その他の被害事例

2020年度第1四半期もさまざまな組織がマルウェアやランサムウェアの攻撃に遭っています。特に最近は、医療関係企業や電力等のインフラ企業からランサムウェアの被害が多く報告されています。2019年度第1四半期に報告されたマルウェアやランサムウェアの被害事例を表 8に示します。

表 8: マルウェア・ランサムウェアの被害事例

日付	標的	概要
4/6	アルジェリア/国営石油企業/Sonatrach	ランサムウェアに感染して機密文書を含むデータベース全体が漏えいした [64]
4/7 ※	イギリス/治験専門機関/Hammersmith Medicines Research	Mazeランサムウェアに感染して一部の治験協力者の個人情報が2020年03月21-23日に公開された。現在は対処済み [65]
4/8 ※	イギリス/Fintech企業/Finastra	3月20日にランサムウェアに感染して顧客への影響が発生した。情報漏えいは確認されていない [66]
4/9 ※	イギリス/外貨両替専門店/Travelex	2019年12月31日にSodinokibiランサムウェアに感染した。攻撃者はファイルを暗号化して300万ドルの身代金を要求した。支払わない場合はファイルを公開すると脅迫した。Travelex は230万ドルの身代金を支払ったことを公表した [67]
4/9	アメリカ/ITサービス企業/Cognizant	Mazeランサムウェアに感染してファイルの窃取と暗号化が行われた。身代金の要求とファイル公開を脅迫された [68]
4/10 ※	アメリカ/精密部品メーカー/Visser Precision	2020年3月にDoppelPaymerランサムウェアに感染した。2020年3月末の期限までに身代金を支払わなかったところ情報が流出した。流出した文書は、Tesla社、Lockheed Martin社、Boeing社、SpaceX社などに関連したものであった [69]
4/14 ※	ポルトガル/エネルギー企業/EDP	Ragnar Lockerランサムウェアに感染した。攻撃者は10 TBを超える機密情報を盗んだと主張し、身代金1,580BTCを支払わない場合、盗まれたすべてのデータを漏らすと脅迫した [70]

4/18	アメリカ/ITサービス企業/Cognizant	内部システムがMazeランサムウェアに感染して、一部の顧客向けサービスが停止した [71]
4/21 ※	アメリカ/トーランス市	DoppelPaymerランサムに感染した。攻撃者は、市の予算情報を含む200GB以上の機密情報を盗んだと主張して身代金100BTCを要求した [72]
4/22	神奈川県/川崎市立高校	校内ネットワークサーバがランサムウェアに感染して、サーバ内のファイルが暗号化された。同校は2019年10月にもランサムウェアの感染被害が発生して被害に遭っている。セキュリティ対策は強化していた。今回感染したランサムウェアは、前回と異なるものだった [73]
4/24 ※	アメリカ/ビデオ配信ソフトウェア企業/SeaChange International	Sodinokibiランサムウェアに感染した。攻撃者は、システムを暗号化する前に機密情報を盗んだと主張した [74]
4/26 ※	アメリカ/製薬会社/ExecuPharm	3月13日にCLOPランサムウェアに感染した。攻撃者は盗んだ情報をダークウェブのウェブサイトに公開した [75]
4/28 ※	イギリス/建築設計会社/Zaha Hadid Architects	ランサムウェアに感染した。攻撃者はファイルを盗み、ファイルを暗号化した。身代金を要求し、支払わない場合はファイルを公開すると脅迫した [76]
4/28 ※	アメリカ/バイオ医薬品企業/ExecuPharm	3月13日にCLOPランサムウェアに感染した。身代金を要求されて、窃取された一部の企業および個人情報を公開された [77]
5/5	オーストラリア/物流企業/Toll Group	Nefilimランサムウェアの亜種に感染した。一部のシステムが停止したが、バックアップを使用してファイルを復元した。同社は2月3日にもMailToランサムウェアに感染している [78]
5/6	ドイツ/病院運営会社/Fresenius Group	Snakeランサムウェアに感染した。感染の翌日に、48時間以内に連絡や支払いがない場合、窃取したデータベースや文書を公開する旨の脅迫文が届いた [79]
5/7	アメリカ/テキサス州/裁判所管理局	ランサムウェアに感染した。身代金の支払いには応じないとの意向を示した [80]

5/11	アメリカ/ATMメーカー/Diebold Nixdorf	ProLockランサムウェアに感染した。身代金の支払いには応じないとの意向を示した [81]
5/13 ※	アメリカ/ヘルスケアマネジメント会社/Magellan Health	ランサムウェアに感染した。情報を窃取されたが、悪用された形跡はないと公表した [82]
5/19	オーストラリア/鉄鋼メーカー/BlueScope Steel	ランサムウェアに感染して、一部の製造および販売業務に影響が発生した [83]
5/24	アメリカ/半導体メーカー/MaxLinear	Mazeランサムウェアに感染した。同社の業務に大きな影響は発生しなかった。一部の機密情報がオンライン上に公開された [84]
5/26	アメリカ/アラバマ州/フローレンス市	ランサムウェアに感染して、内部のITネットワークが停止した。同市は、攻撃者に30万ビットコインを支払うことを議会で決めた [85]
5/28	アメリカ/ミシガン州立大学	Netwalkerランサムウェアに感染した。身代金の支払いに応じなかったため、攻撃者は盗んだファイルをリークサイトに公開した [86]
6/2 ※	イギリス/電力会社/Elexon	Sodinokibiランサムウェアに感染して、内部のITネットワークに影響が発生した。攻撃者は盗んだファイルをリークサイトに公開した [87]
6/3	アメリカ/カリフォルニア大学サンフランシスコ校	Netwalkerランサムウェアに感染した。114万ドル相当のビットコインを攻撃者へ支払った [88]
6/3	アメリカ/大陸間弾道ミサイル保守業者/Westech International	Mazeランサムウェアに感染して、一部のファイルが暗号化された。軍の機密情報が窃取されたかどうかは不明 [89]

6/9	オーストラリア/飲料メーカー/Lion	ランサムウェアに感染した。同社は感染拡大を防ぐためにITシステムを停止したため、製品の出荷遅延等の影響が発生した。同社のドキュメントリストが公開されたり、一部の機密情報が公開されたりした [90]
6/11	イタリア/電力会社/Enel Group	Snakeランサムウェアに感染し、内部のITネットワークに影響が発生した [91]
6/11	アメリカ/コンサルティング会社/Threadstone Advisors	Mazeランサムウェアに感染した。攻撃者はファイルを盗んだあとで暗号化した。同社は元Spice GirlsのVictoria Beckham氏らを顧客に持つ米コンサルティング会社である [92]
6/25 ※	韓国/総合家電メーカー/LG Electronics	Mazeランサムウェアに感染した。攻撃者は40 GBのソースコードを盗んだ [93]

※公表日

6. 予測

オンライン会議ツールによるコミュニケーションの新しいリスク

本稿では、Zoomを使用する際にユーザが気を付ける点について紹介しました。これまで同じ場所に集まって行って、対面で行っていたさまざまなビジネスコミュニケーションは、今後、Zoomをはじめとしたオンラインツールを使った方法へどんどん置き換わっていくでしょう。しかし、誰でもどこからでも接続できるオンラインでのコミュニケーションの普及は、これまであまり意識することのなかった新しいリスクを生むことも忘れてはいけません。例えば、従来企業の営業担当者は対面で名刺交換をして、顔を見せて信頼を得て商材やサービスを売り込んでいましたが、この活動がオンラインになることで、なりすましや詐欺などが簡単に行えるようになります。オンラインが当たり前になればなるほど、顔を知らない相手からの歩み寄りに対する警戒心も薄れるため、攻撃者にとっても攻撃を仕掛けやすくなると考えられます。コミュニケーションのオンライン化を進める際は、なりすましや詐欺のリスクが伴うことを理解して、本人確認や情報の信頼性を確認する方法を備えなければなりません。

VPN製品の脆弱性を狙った攻撃の増加

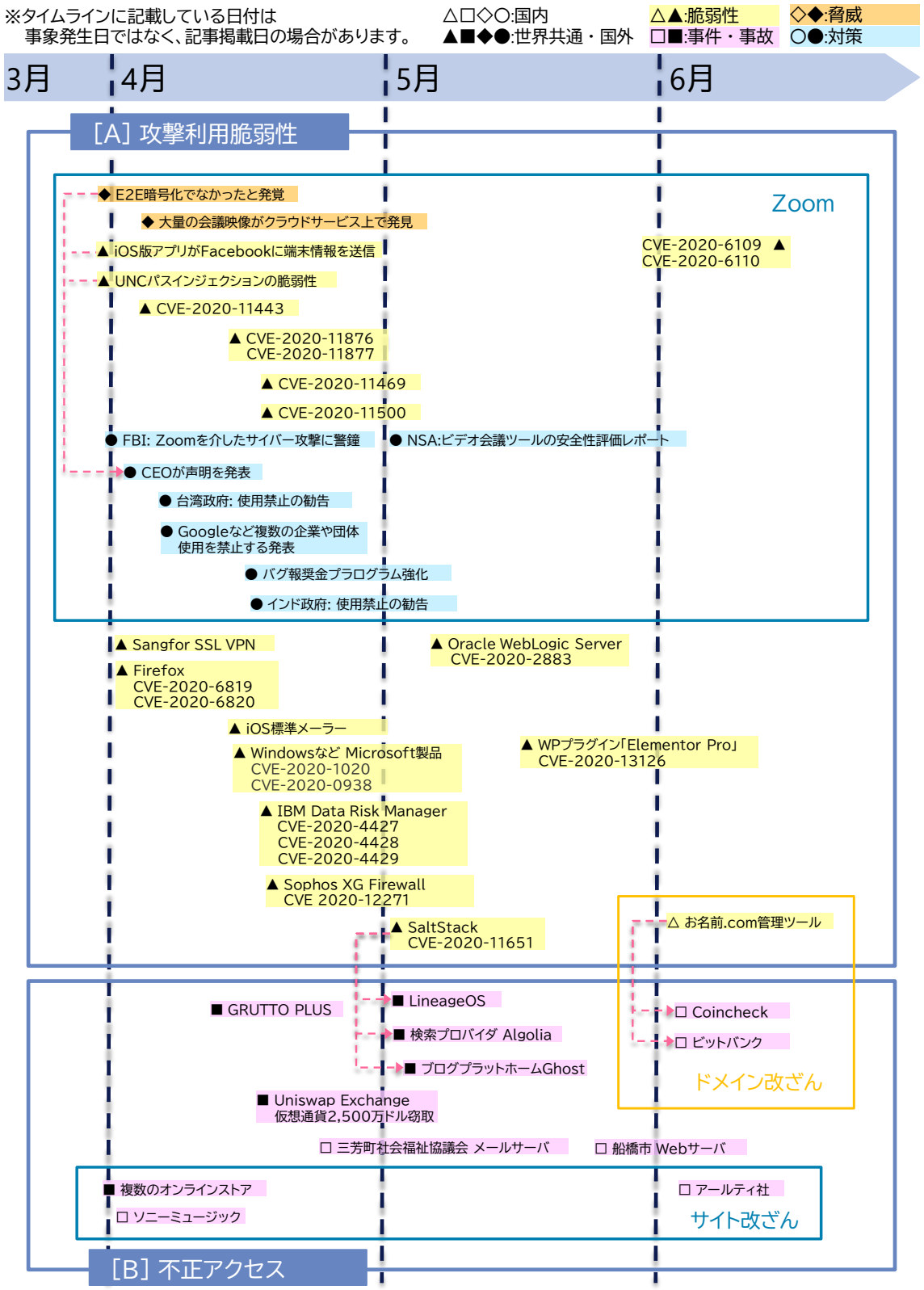
Skybox Securityの調査 [94]によれば、2020年上半期は約9,000件の脆弱性が報告されており、2020年は過去最高の2万件の脆弱性が報告されるおそれがあります。コロナウイルスの感染拡大の影響でテレワークが拡大し、急速にVPN製品が普及していくことを踏まえると、VPN製品の脆弱性を狙った攻撃が増加することが予測されます。また、リモートでのコード実行や認証情報の窃取が可能になるVPN製品の脆弱性は、脆弱性が公開されてからサイバー攻撃を受けて侵害が発生するまでの期間が短くなっている傾向があります。VPN製品を利用している場合は、該当する製品の脆弱性情報を収集して、その内容をすぐに確認してください。その脆弱性がインターネット上の第三者からアクセス可能な脆弱性の場合は、2～3日以内のパッチを適用するか、VPN製品の一時停止を判断してください。

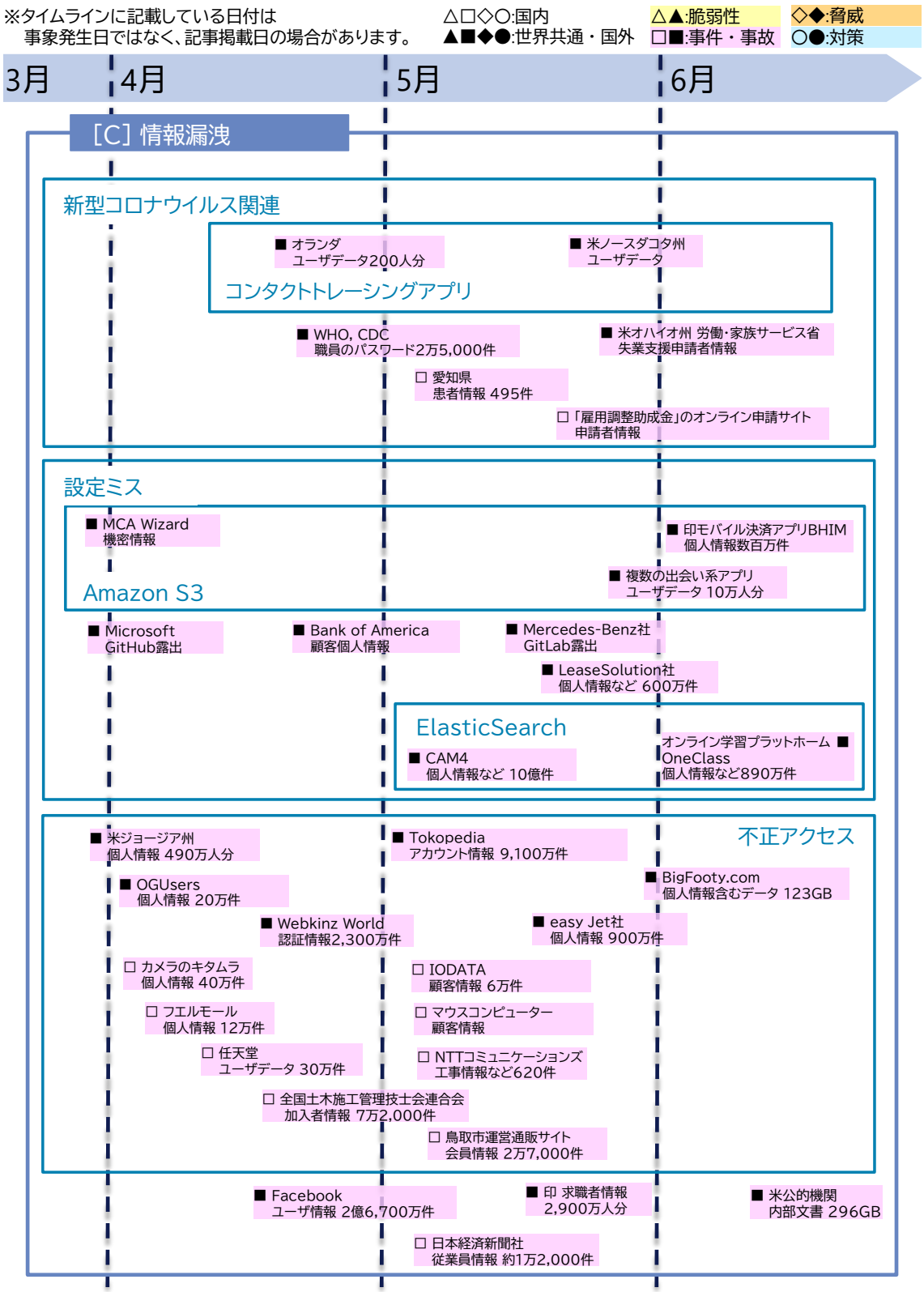
Dockerを狙った攻撃の増加

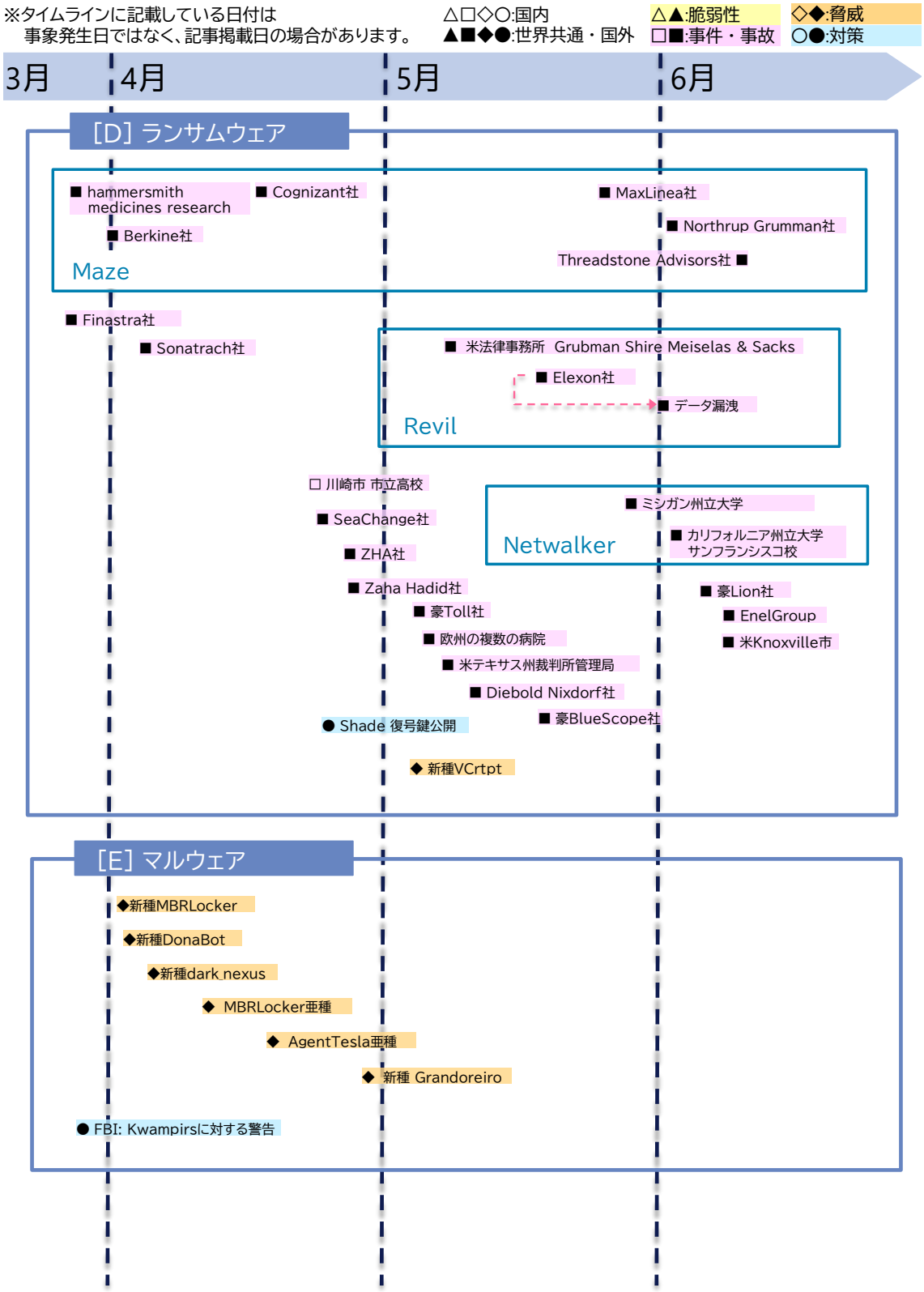
デジタルトランスフォーメーションやテレワークの拡大により、クラウドサービスの需要が増加すれば、Dockerの利用が増加していくと想定されます [95]。利用の増加とともに、セキュリティ対策が不十分なDockerも増えて、そのようなDockerを狙った攻撃も増えていくおそれがあります。

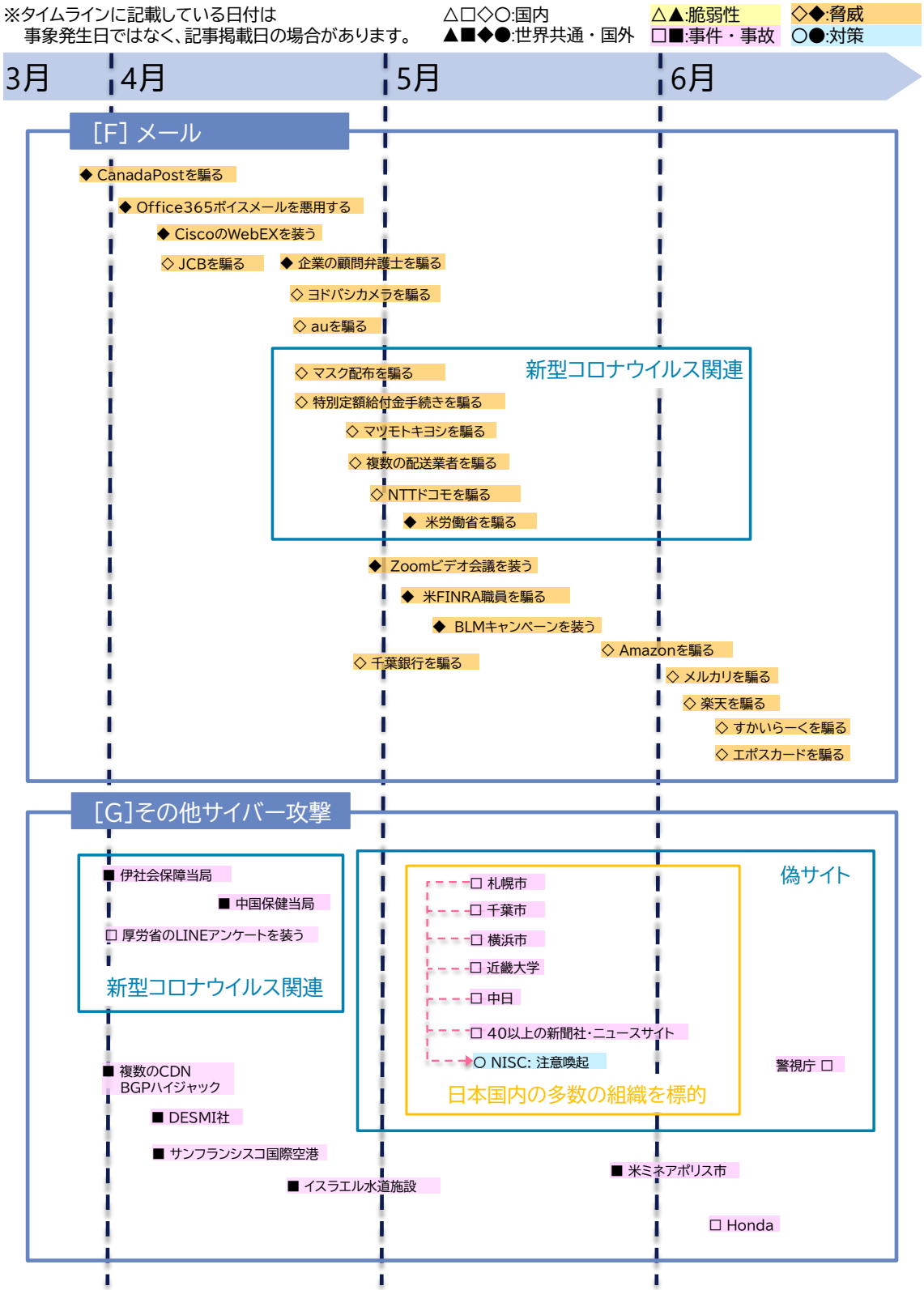
Dockerへ侵入する攻撃は、「5. マルウェア・ランサムウェア」で紹介した以外にも、Kubernetes等のコンテナオーケストラツールの設定不備や脆弱性を狙った攻撃、マルウェアを含むDockerイメージを配信する攻撃、コンテナを用いた開発時に、利用するツールの脆弱性や設定不備を悪用してコンテナにマルウェアを潜り込ませる攻撃等があります [96] [97]。このようなさまざまな攻撃に対応するためにも、“Application Container Security Guide”（NIST SP 800-190） [61]やCenter for Internet Security Docker Benchmark(CIS Benchmarks) [62]を活用して、現在利用中、または利用する予定のDocker対して、設定のスキャンを行い、設定ルールの違反や設定ミスを明確にして、対応することをお薦めします。

7. タイムライン









参考文献

[1] “Businesses @ Work (From Home) 2020,” Okta, 29 5 2020. [オンライン]. Available: https://www.okta.com/businesses-at-work/2020/work-from-home/.

[2] “Zoom is Now Worth More Than the World’s 7 Biggest Airlines,” Visual Capitalist, 15 5 2020. [オンライン]. Available: https://www.visualcapitalist.com/zoom-boom-biggest-airlines/.

[3] “Zoom iOS App Sends Data to Facebook Even if You Don’t Have a Facebook Account,” Motherboard, 26 3 2020. [オンライン]. Available: https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account.

[4] “Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing.,” The Intercept, 31 3 2020. [オンライン]. Available: https://theintercept.com/2020/03/31/zoom-meeting-encryption/.

[5] “ JVN iPedia 脆弱性対策情報対策データベース,” IPA, [オンライン]. Available: https://jvndb.jvn.jp/.

[6] “Talos Vulnerability Report,” Cisco, 3 6 2020. [オンライン]. Available: https://talosintelligence.com/vulnerability_reports/TALOS-2020-1055.

[7] “Attackers can use Zoom to steal users’ Windows credentials with no warning,” WIRED Media Group, 2 4 2020. [オンライン]. Available: https://arstechnica.com/information-technology/2020/04/unpatched-zoom-bug-lets-attackers-steal-windows-credentials-with-no-warning/.

[8] “Zoom Lets Attackers Steal Windows Credentials, Run Programs via UNC Links,” Bleeping Computer, 31 3 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/.

[9] “Zoom利用者へのメッセージ,” Zoom, 1 4 2020. [オンライン]. Available: https://blog.zoom.us/ja/a-message-to-our-users/.

[10] “Zoom sued by shareholder for ‘overstating’ security claims,” Techcrunch, 9 4 2020. [オンライン]. Available: https://techcrunch.com/2020/04/08/zoom-sued-shareholder-security/.

[11] “Move Fast and Roll Your Own Crypto,” Citizen Lab, 3 4 2020. [オンライン]. Available: https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/.

[12] “トロント大学 Citizen Lab研究へのレスポンス,” Zoom, 3 4 2020. [オンライン]. Available: https://blog.zoom.us/ja/response-to-research-from-university-of-torontos-citizen-lab/.

[13] “Zoomの iOS クライアントでのFacebook SDK 利用について (翻訳版),” Zoom, 27 3 2020. [オンライン]. Available: https://sites.google.com/zoom.us/zoomjapanfaq/zoomblog/zoom-use-of-facebook-sdk-in-ios-client.

[14] “Zoom’s Privacy Policy,” Zoom, 29 3 2020. [オンライン]. Available: https://blog.zoom.us/zoom-privacy-policy/.

[15] “Zoom Privacy Lawsuit,” Wexler Wallace, [オンライン]. Available: https://www.wexlerwallace.com/zoom-privacy-lawsuit/.

[16] “Zoom’s Waiting Room Vulnerability,” Citizen Lab, 8 4 2020. [オンライン]. Available: https://citizenlab.ca/2020/04/zooms-waiting-room-vulnerability/.

[17] “FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic,” FBI, 30 3 2020. [オンライン]. Available: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

[18] “Executive Yuan orders agencies to step up video conferencing security,” Executive Yuan, 7 4 2020. [オンライン]. Available: https://english.ey.gov.tw/Page/61BF20C3E89B856/849887da-0aa7-4b84-8fba-1b6b1183843f.

[19] “MHA issues Advisory on Secure use of ZOOM Meeting Platform,” Ministry of Home Affairs, 16 4 2020. [オンライン]. Available: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1615008.

[20] “India records highest Zoom installs in Q1 2020: Sensor Tower,” TechCircle, 17 4 2020. [オンライン]. Available: https://www.techcircle.in/2020/04/17/india-records-highest-zoom-installs-in-q1-2020-sensor-tower.

[21] “Government selects 10 Indian companies to develop Desi Zoom rival,” GADGETS NOW, 25 5 2020. [オンライン]. Available: https://www.gadgetsnow.com/tech-news/government-selects-10-indian-companies-to-develop-desi-zoom-rival/articleshow/75965854.cms.

[22] “Google Told Its Workers That They Can’t Use Zoom On Their Laptops Anymore,” BuzzFeed, 8 4 2020. [オンライン]. Available: https://www.buzzfeednews.com/article/pranavdixit/google-bans-zoom.

[23] “Web会議サービスを使用する際のセキュリティ上の注意事項,” IPA, 14 7 2020. [オ

ンライン]. Available: https://www.ipa.go.jp/security/announce/webmeeting.html.

[24] C. Point, “As organizations get back to business, cyber criminals look for new angles to exploit,” Check Point, 6 2020. [オンライン]. Available: https://blog.checkpoint.com/2020/06/25/as-organizations-get-back-to-business-cyber-criminals-look-for-new-angles-to-exploit/.

[25] M. BRENAN, “U.S. Workers Discovering Affinity for Remote Work,” Gallup, 3 4 2020. [オンライン]. Available: https://news.gallup.com/poll/306695/workers-discovering-affinity-remote-work.aspx.

[26] Shodan, “Trends in Internet Exposure,” Shodan, 29 3 2020. [オンライン]. Available: https://blog.shodan.io/trends-in-internet-exposure/.

[27] T. Roccia, “Cybercriminals Actively Exploiting RDP to Target Remote Organizations,” McAfee, 6 5 2020. [オンライン]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/cybercriminals-actively-exploiting-rdp-to-target-remote-organizations/.

[28] S. Gatlan, “RDP brute-force attacks are skyrocketing due to remote working,” BleepingComputer, 29 4 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/rdp-brute-force-attacks-are-skyrocketing-due-to-remote-working/.

[29] D. Galov, “Remote spring: the rise of RDP bruteforce attacks,” Kaspersky, 29 4 2020. [オンライン]. Available: https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/.

[30] O. Kubovič, “Remote access at risk: Pandemic pulls more cyber-crooks into the brute-forcing game,” ESET, 29 6 2020. [オンライン]. Available: https://www.welivesecurity.com/2020/06/29/remote-access-risk-pandemic-cybercrooks-bruteforcing-game/.

[31] Abnormal Security, “Abnormal Attack Stories: VPN Impersonation Phishing,” Abnormal Security, 3 6 2020. [オンライン]. Available: https://abnormalsecurity.com/blog/abnormal-attack-stories-vpn-impersonation-phishing/.

[32] Abnormal Security, “Abnormal Attack Stories: Zoom Phishing,” Abnormal Security, 21 4 2020. [オンライン]. Available: https://abnormalsecurity.com/blog/abnormal-attack-stories-zoom-phishing/.

[33] Abnormal Security, “Abnormal Attack Stories: Microsoft Teams Impersonation,” Abnormal Security, 1 5 2020. [オンライン]. Available: https://abnormalsecurity.com/blog/abnormal-attack-stories-microsoft-teams-

impersonation/.

[34] Abnormal Security, “Abnormal Attack Stories: Cisco Webex Phishing,” Abnormal Security, 5 5 2020. [オンライン]. Available: https://abnormalsecurity.com/blog/abnormal-attack-stories-cisco-webex-phishing/.

[35] Trend Micro, “Backdoor, Devil Shadow Botnet Hidden in Fake Zoom Installers,” Trend Micro, 21 5 2020. [オンライン]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-devil-shadow-botnet-hidden-in-fake-zoom-installers/.

[36] avast, “アバスト、「フリースウェア」と見られるiOS VPNアプリをApp Storeで発見,” avast, 17 6 2020. [オンライン]. Available: https://press.avast.com/ja-jp/avast-warns-of-fleeceware-apps.

[37] B. BARRETT, “Hack Brief: An Adult Cam Site Exposed 10.88 Billion Records,” WIRED, 5 5 2020. [オンライン]. Available: https://www.wired.com/story/cam4-adult-cam-data-leak-7tb/.

[38] J. Yeung, “Almost entire population of Ecuador has data leaked,” CNN, 17 9 2019. [オンライン]. Available: https://edition.cnn.com/2019/09/17/americas/ecuador-data-leak-intl-hnk-scli/index.html#:~:text=More%20than%2020%20million%20people,population%20could%20have%A20been%20affected..

[39] S. WHITE, “Honda struck by 40GB data breach,” PrivSec, 1 8 2019. [オンライン]. Available: https://gdpr.report/news/2019/08/01/honda-struck-by-40gb-data-breach/.

[40] ナカバヤシ株式会社, “弊社が運営する「フエルモール」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ【続報】,” ナカバヤシ株式会社, 3 6 2020. [オンライン]. Available: https://www.nakabayashi.co.jp/news/2020/info/715.

[41] NTTコミュニケーションズ, “当社への不正アクセスによる情報流出の可能性について,” NTTコミュニケーションズ, 28 5 2020. [オンライン]. Available: https://www.ntt.com/about-us/press-releases/news/article/2020/0528.html.

[42] 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4四半期,” 26 06 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_4q_securityreport.pdf.

[43] C. Cimpanu, “Mercedes-Benz onboard logic unit (OLU) source code leaks online,” ZDNet, 18 5 2020. [オンライン]. Available: https://www.zdnet.com/article/mercedes-benz-onboard-logic-unit-olu-source-code-leaks-online/.

[44] T. Brewster, “EasyJet Hacked For Four Months, Data On 9 Million Customers And

2,000 Credit Cards Stolen,” Forbs, 19 5 2020. [オンライン]. Available: https://www.forbes.com/sites/thomasbrewster/2020/05/19/easyjet-hacked-9-million-customers-and-2000-credit-cards-hit/#77d7441f1ae1.

[45] 任天堂株式会社, “「ニンテンドーネットワークID」に対する不正ログイン発生のご報告と「ニンテンドーアカウント」を安全にご利用いただくためのお願い,” 任天堂株式会社, 9 6 2020. [オンライン]. Available: https://www.nintendo.co.jp/support/information/2020/0424.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年度版第2四半期）,” 29 8 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_2q_securityreport.pdf.

[47] U. S. C. E. R. Team, “Alert (AA20-107A),” 22 4 2020. [オンライン]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-107a.

[48] P. Secure, “SA44101 - 2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX,” 24 4 2019. [オンライン]. Available: https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101.

[49] B. Packets, “Over 14,500 Pulse Secure VPN endpoints vulnerable to CVE-2019-11510,” 24 8 2019. [オンライン]. Available: https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/.

[50] 一. J. コーディネーションセンター, “複数の SSL VPN 製品の脆弱性に関する注意喚起,” 6 9 2019. [オンライン]. Available: https://www.jpcert.or.jp/at/2019/at190033.html.

[51] U. S. C. E. R. Team, “Alert (AA20-010A),” 10 1 2020. [オンライン]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-010a.

[52] tenable, “CVE-2019-11510: 「緊急」の Pulse Connect Secure の脆弱性、ランサムウェア「Sodinokibi 」の攻撃に悪用される,” 7 1 2020. [オンライン]. Available: https://jp.tenable.com/blog/cve-2019-11510-critical-pulse-connect-secure-vulnerability-used-in-sodinokibi-ransomware.

[53] 衛. 亮介, “Pulse Connect Secure の脆弱性を狙った攻撃事案,” 26 3 2020. [オンライン]. Available: https://blogs.jpcert.or.jp/ja/2020/03/pulse-connect-secure.html.

[54] CBS Interactive, “REvil ransomware gang launches auction site to sell stolen data,” 2 6 2020. [オンライン]. Available: https://www.zdnet.com/article/revil-ransomware-gang-launches-auction-site-to-sell-stolen-data/.

[55] Graham Cluley, “Malicious Coronavirus victim tracking app demands ransom payment from Android users,” 16 3 2020. [オンライン]. Available: https://www.grahamcluley.com/coronavirus-android-ransomware/.

[56] Data Breach TODAY, “No COVID-19 Respite: Ransomware Keeps Pummeling Healthcare,” 7 4 2020. [オンライン]. Available: https://www.databreachtoday.com/no-covid-19-respite-ransomware-keeps-pummeling-healthcare-a-14072.

[57] 朝日新聞, “ホンダ、サイバー攻撃被害認める　身代金ウイルス拡大か,” 9 6 2020. [オンライン]. Available: https://www.asahi.com/articles/ASN6966YFN69ULFA03G.html.

[58] Aqua Security, “Threat Alert: Kinsing Malware Attacks Targeting Container Environments,” 3 4 2020. [オンライン]. Available: https://blog.aquasec.com/threat-alert-kinsing-malware-container-vulnerability.

[59] CREATIONLINE, INC, “脅威：コンテナ環境を対象としたマルウェア「Kinsing」が増加中 #AquaSecurity #セキュリティ #コンテナ #マルウェア,” 8 4 2020. [オンライン]. Available: https://www.creationline.com/lab/34036.

[60] Trend Micro Incorporated, “Docker デーモンのオープンポートを狙うマルウェア、目的はボット感染とマイニング,” 16 7 2020. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/25580.

[61] National Institute of Standards and Technology, “Application Container Security Guide,” 9 2017. [オンライン]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf.

[62] Center for Internet Security, [オンライン]. Available: https://www.cisecurity.org/cis-benchmarks/.

[63] NTT DATA Corporation, “注目を集める仮想化技術「コンテナ」、そのセキュリティ対策とは？,” 31 1 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/data-insight/2019/0131/.

[64] HACKREAD, “Maze ransomware group hacks oil giant; leaks data online,” 6 4 2020. [オンライン]. Available: https://www.hackread.com/maze-ransomware-group-hacks-oil-giant-leaks-data/.

[65] Bleeping Computer LLC, “Drug testing firm sends data breach alerts after ransomware attack,” 7 4 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/drug-testing-firm-sends-data-breach-alerts-after-ransomware-attack/.

[66] Krebs on Security, “Security Breach Disrupts Fintech Firm Finastra,” 8 4 2020. [オンライン]. Available: https://krebsonsecurity.com/2020/03/security-breach-disrupts-fintech-firm-finastra/.

[67] Security Affairs by Pierluigi Paganini, “Travelex paid $2.3 Million ransom to restore

after a ransomware attack,” 9 4 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/101339/cyber-crime/travelex-paid-ransomware.html.

[68] Bleeping Computer LLC, “IT giant Cognizant confirms data breach after ransomware attack,” 17 6 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/it-giant-cognizant-confirms-data-breach-after-ransomware-attack/.

[69] Biting the hand that feeds IT, “Ransomware scumbags leak Boeing, Lockheed Martin, SpaceX documents after contractor refuses to pay,” 10 4 2020. [オンライン]. Available: https://www.theregister.co.uk/2020/04/10/lockheed_martin_spacex_ransomware_leak/.

[70] Bleeping Computer LLC, “RagnarLocker ransomware hits EDP energy giant, asks for €10M,” 14 4 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/.

[71] Sophos Ltd, “Maze ransomware hits US giant Cognizant,” 20 4 2020. [オンライン]. Available: https://nakedsecurity.sophos.com/2020/04/20/maze-ransomware-hits-us-giant-cognizant/.

[72] Bleeping Computer LLC, “DoppelPaymer Ransomware hits Los Angeles County city, leaks files,” 21 4 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-hits-los-angeles-county-city-leaks-files/.

[73] NEWSGAIA, “高校でランサム被害、セキュリティ強化するも再発 - 川崎市,” 8 5 2020. [オンライン]. Available: http://www.security-next.com/114691.

[74] Security Affairs by Pierluigi Paganini, “SeaChange video delivery software solutions provider hit by Sodinokibi ransomware,” 24 4 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/102177/cyber-crime/seachange-sodinokibi-ransomware.html.

[75] Verizon Media, “Hackers publish ExecuPharm internal data after ransomware attack,” 28 4 2020. [オンライン]. Available: https://techcrunch.com/2020/04/27/execupharm-clop-ransomware/.

[76] CBS Interactive, “Hackers threaten to leak data from high-end architecture firm Zaha Hadid,” 28 4 2020. [オンライン]. Available: https://www.zdnet.com/article/hackers-threaten-to-leak-data-from-high-end-

architecture-firm-zaha-hadid/?mid=1#cid=734236.

[77] MediaOps Inc, “Cybercriminals Leak ExecuPharm Internal Documents After Ransomware Attack,” 28 4 2020. [オンライン]. Available: https://securityboulevard.com/2020/04/cybercriminals-leak-execupharm-internal-documents-after-ransomware-attack/.

[78] rootdaemon, “Logistics giant Toll Group hit by ransomware for the second time in three months,” 6 5 2020. [オンライン]. Available: https://rootdaemon.com/2020/05/06/logistics-giant-toll-group-hit-by-ransomware-for-the-second-time-in-three-months/.

[79] Bleeping Computer LLC, “Large scale Snake Ransomware campaign targets healthcare, more,” 6 6 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/large-scale-snake-ransomware-campaign-targets-healthcare-more/.

[80] CBS Interactive, “Texas courts slammed by ransomware attack,” 12 5 2020. [オンライン]. Available: https://www.zdnet.com/article/texas-courts-slammed-by-ransomware-attack/.

[81] Krebs on Security, “Ransomware Hit ATM Giant Diebold Nixdorf,” 20 5 2020. [オンライン]. Available: https://krebsonsecurity.com/2020/05/ransomware-hit-atm-giant-diebold-nixdorf/.

[82] CyberRisk Alliance, LLC, “Magellan Health warns ransomware attack exposed PII,” 13 5 2020. [オンライン]. Available: https://www.scmagazine.com/home/security-news/magellan-health-warns-ransomware-attack-exposed-pii/.

[83] Security Affairs by Pierluigi Paganini, “Australian product steel producer BlueScope hit by cyberattack,” 19 5 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/103453/cyber-crime/bluescope-cyber-attack.html/.

[84] Reuters, “Chipmaker MaxLinear hit by 'Maze' ransomware attack,” 16 6 2020. [オンライン]. Available: https://www.reuters.com/article/us-maxlinear-cyber/chipmaker-maxlinear-hit-by-maze-ransomware-attack-idUSKBN23N243.

[85] Wells Media Group, Inc, “Alabama City to Pay $300K in Bitcoin Ransom in Computer System Hack,” 12 6 2020. [オンライン]. Available: https://www.insurancejournal.com/news/southeast/2020/06/12/572046.htm.

[86] Bleeping Computer LLC, “Netwalker ransomware continues assault on US colleges, hits UCSF,” 3 6 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/.

[87] Security Affairs by Pierluigi Paganini, “Sodinokibi ransomware operators leak files stolen from Elexon electrical middleman,” 2 6 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/104149/cyber-crime/sodinokibi-published-elexon-files.html.

[88] CyberRisk Alliance, “UCSF paid $1.4 million ransom in NetWalker attack,” 29 6 2020. [オンライン]. Available: https://www.scmagazine.com/home/security-news/ucsf-paid-1-4-million-ransom-in-netwalker-attack/.

[89] Sophos Ltd., “Nuclear missile contractor hacked in Maze ransomware attack,” 4 6 2020. [オンライン]. Available: https://nakedsecurity.sophos.com/2020/06/04/nuclear-missile-contractor-hacked-in-maze-ransomware-attack.

[90] CBS Interactive, “Lion warns of beer shortages following ransomware attack,” 12 6 2020. [オンライン]. Available: https://www.zdnet.com/article/lion-warns-of-beer-shortages-following-ransomware-attack/.

[91] Bleeping Computer LLC, “Power company Enel Group suffers Snake Ransomware attack,” 11 6 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/power-company-enel-group-suffers-snake-ransomware-attack/.

[92] Reed Exhibitions Ltd, “MAZE Attacks Victoria Beckham's Advisory Firm,” 11 6 2020. [オンライン]. Available: https://www.infosecurity-magazine.com/news/maze-attacks-victoria-beckhams/?&web_view=true.

[93] Bleeping Computer LLC, “LG Electronics allegedly hit by Maze ransomware attack,” 25 6 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/lg-electronics-allegedly-hit-by-maze-ransomware-attack/.

[94] P. Muncaster, “Experts Predict Record 20,000 CVEs for 2020,” 21 7 2020. [オンライン]. Available: https://www.infosecurity-magazine.com/profile/phil-muncaster/.

[95] Grand View Research, “アプリケーションコンテナーの市場規模| グローバル産業レポート、2019-2025,” Grand View Research, [オンライン]. Available: https://www.grandviewresearch.com/industry-analysis/application-container-market.

[96] 宮田健, “「コンテナセキュリティ」とは――コンテナを活用する人が知っておくべき6つのポイント,” @IT, 16 10 2019. [オンライン]. Available: https://www.atmarkit.co.jp/ait/articles/1910/16/news015_2.html.

[97] J. Chen, “セキュアでないDockerデーモンへの攻撃者の戦術とテクニックが明らかに 地理的分布で日本は全体の3.7%,” パロアルトネットワークス株式会社, 30 1

2020. [オンライン]. Available: https://unit42.paloaltonetworks.jp/attackers-tactics-and-techniques-in-unsecured-docker-daemons-revealed/.

NTT DATA
Trusted Global Innovator

2020年9月11日発行

株式会社NTTデータ
セキュリティ技術部 情報セキュリティ推進室 NTTDATA-CERT担当
大谷 尚通 / 小林 義徳 / 大石 眞央 / 山下 大輔
星野 亮 / 青木 隆行 / 伊藤 友洋 / 宮崎 大輔 / 木下 盾 / 宍戸 りさ / 清水 一貴
nttdata-cert@kits.nttdata.co.jp