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

2021年度 第2四半期

目次　グローバルセキュリティ動向　四半期レポート2021年度　第2四半期

1 エグゼクティブサマリー

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。

1.1 東京2020オリンピック・パラリンピック競技大会から見たサイバー攻撃の動向

2021年7～9月に東京で開催された東京2020オリンピック・パラリンピック競技大会（以後、東京オリンピック・パラリンピック）では、大会運営に影響があるようなサイバー攻撃は起こりませんでしたが、多くのサイバー攻撃が発生しました。東京オリンピック・パラリンピック競技大会組織委員会等の主催組織本体を狙った攻撃があった一方で、サプライチェーンや東京オリンピック・パラリンピック観戦者といった周辺のステークホルダへのサイバー攻撃も発生しており、個人情報の漏えいなどのインシデントも報告されました。本稿では、新型コロナウイルスの流行や世の中のサイバー攻撃の流行が、主催組織本体から周辺のステークホルダへのサイバー攻撃が発生した一因ではないかという考えを説明します。

1.2 FortiGateの脆弱性の放置による代償

Fortinet社が2019年5月に公開したSSL-VPN装置FortiGateの脆弱性 CVE-2018-13379が、多数の組織で依然として対策が進んでおらず、この脆弱性を悪用した被害報告が続いています。脆弱性CVE-2018-13379は、組織の外部から内部へのアクセスを提供するSSL-VPN機能に存在し、認証情報が漏えいしてしまうため危険度が高く、Fortinet社や国内外のセキュリティ機関が注意喚起を繰り返しています。それにも関わらず、何故対策が進まない組織が多数あるのか、その原因を考察し、脆弱性の対策と脆弱性の対策を進めるための対応について説明します。

1.3 iPhoneの「BlastDoor」も回避するゼロクリック攻撃

2021年8月に、スパイウェア「Pegasus」を使ったiPhoneへのゼロクリック攻撃が報告されました。攻撃者は、iPhoneに含まれる脆弱性を悪用して、処理領域外へのメモリアクセスを可能にすることでPegasusをインストールし、端末内の情報を盗聴していました。iOS 14にて実装されたセキュリティ機能である「BlastDoor」や既存のiOSの脆弱性悪用防止の仕組みを回避していることが判明しています。すでにセキュリティアップデートが公開されており、iPhoneをiOS 14.8以降にアップデートすることで当該脆弱性を修正できます。攻撃者のもともとの目的は、Pegasusを使って特定の活動家を密かに継続的に監視することです。広範な標的を攻撃すると、誰かが攻撃に気づいて、攻撃方法を解析して検知できるようになってしまうため、その目的にそぐわなくなります。したがって、この攻撃は一般利用者を攻撃することはなく、すでに発見されて対策も提供済みのため、アップデートを実施すれば、被害は一般の利用者へ拡大しません。

1.4 予測

2021年7月～9月においても、EC-CUBEを利用したECサイトでWebスキミングの被害が継続して発生している状況です。このような状況から、脆弱性を放置したままで改ざんに気づかないサイトが現状でも存在すると想定され、しばらくEC-CUBEに関連するECサイトのインシデントの公表が継続すると予想します。

北京オリンピック・パラリンピックでは、オミクロン株再流行のおそれやサイバー攻撃の流行の変化も少ないと考えられることから、東京オリンピック・パラリンピックと同様に、周辺のステークホルダを狙ったフィッシング攻撃やサプライチェーン攻撃が行われると推測します。

また、AIの技術の進歩やそれを活用したサービスが注目されていますが、今後はAIを活用した「ディープフェイク」が攻撃者の攻撃手口として悪用されることが懸念されます。

“ECサイトのWebスキミングやディープフェイクによる被害が今後流行すると予想される”

2 注目トピック
東京2020オリンピック・パラリンピック競技大会と攻撃トレンド

2.1 東京2020オリンピック・パラリンピック競技大会から見たサイバー攻撃の動向

2.1.1. 東京2020オリンピック・パラリンピック競技大会でのサイバー攻撃の事例

2021年7月～9月に、東京2020オリンピック・パラリンピック競技大会（以後、東京オリンピック・パラリンピック）が東京で開催されました。新型コロナウイルスの影響により、1年の延期や無観客などの措置が取られた異例の大会でした。

このような大規模イベントは、世界中の注目が集まることもあり、サイバー攻撃の標的になります。東京オリンピック・パラリンピックの期間中も大会運営関連システムやネットワークに対して合わせて4億回を超えるサイバー攻撃がありました。ただし、対策によりすべてブロックし、大会運営への影響はなかったことが報告されています [1]。

東京オリンピック・パラリンピックに関連し報道されたサイバー攻撃の事例を表 1に示します。東京オリンピック・パラリンピック競技大会組織委員会（以後、大会組織委員会）や日本オリンピック委員会等の主催組織本体を狙った攻撃があった一方で、システムの委託先等のサプライチェーンや東京オリンピック・パラリンピック観戦希望者といった周辺のステークホルダへのサイバー攻撃も発生しており、個人情報の漏えいなどのインシデントも報告されました。

なぜ主催組織本体だけでなく、周辺のステークホルダを狙ったサイバー攻撃が発生したのでしょうか。次項では、周囲のステークホルダを狙ったサイバー攻撃が発生した要因やそれらのサイバー攻撃の特徴の見解を説明します。

表 1： 東京オリンピック・パラリンピック関連のサイバー攻撃の事例

項番	攻撃概要	発生時期	攻撃対象	攻撃内容
1	1年間の開催延期を受け国民に支援を呼びかける偽メール	2020年 4月下旬	オリンピック・パラリンピック観戦希望者	開催延期に伴う損害賠償費用の支援を求める偽のメールが確認されました。さらに、寄付の対価としてチケットを格安で購入できると騙って、入金後にメールで個人情報を送信させました [2]。
2	日本オリンピック委員会事務局のサーバにランサムウェア感染	2020年 4月下旬	日本オリンピック委員会	日本オリンピック委員会がサイバー攻撃を受け、事務局内のサーバやPCにランサムウェアが感染して、内部のデータにアクセスできなくなりました。内部情報流出の被害も、金銭要求もありませんでした。事務局の端末を全て入れ替え、業務を再開しました [3]。
3	東京オリンピック・パラリンピックの偽中継サイト	2021年 3月以降	オリンピック・パラリンピック観戦希望者	山口県内の聖火リレーのライブ配信を騙ったサイトが確認され、山口県警が注意を呼びかけました。動画を再生しようとすると、IDやパスワード、氏名、クレジットカード番号といった個人情報の入力が求められました [4]。 他にも、偽のスポーツ中継サイトへアクセスするとブラウザ通知スパムを引き起こす攻撃など、偽中継サイトによる複数の攻撃事例がありました [5]。
4	富士通のProjectWeb不正アクセスによる大会組織委員会関係者の個人情報漏えい	2021年 5月	システムの委託先企業	富士通社のプロジェクト管理サービスであるProjectWebへ不正アクセスがあり、内閣サイバーセキュリティセンターに関係するプロジェクトの情報が流出しました。流出した情報の中には、大会組織委員会の個人情報も含まれていました [6]。
5	購入済みチケットの払い戻しを行う偽サイト	不明	オリンピック・パラリンピック観戦希望者	購入済みチケットの払い戻しのフィッシングサイトが確認されました [7]。

2.1.2. 東京2020オリンピック・パラリンピックでのサイバー攻撃の考察

東京オリンピック・パラリンピックでは、大会運営への影響はなかったものの、大会組織委員会等の主催組織本体だけでなく、システムの委託先等のサプライチェーンや東京オリンピック・パラリンピック観戦希望者等の、周辺のステークホルダへのサイバー攻撃が発生していました。東京オリンピック・パラリンピックの開催時に世界中で新型コロナウイルスが流行していたことに一因があると推測します。またそれらのサイバー攻撃の特徴として、サイバー攻撃の流行に沿っていた可能性があります。上記2つの見解を詳しく説明します。

（1） 見解 ①：新型コロナウイルスの流行

2020年初頭に発見され、またたく間に世界中に流行した新型コロナウイルスは、東京オリンピック・パラリンピックの1年間の開催延期と無観客開催という大きな影響を及ぼしました。開催延期と無観客開催が、東京オリンピック・パラリンピックを狙ったサイバー攻撃へどう影響したのでしょうか。

当初は2020年の開催を予定していたため、大会組織委員会は大会会場や関連施設、航空券等を確保していました。しかし、1年間の開催延期によってキャンセルや変更を行う必要があり、それに伴って追加費用が発生したり、損害賠償が生じたりするおそれがありました。攻撃者は、これらの報道やうわさに便乗して、不特定多数を狙って「1年間の開催延期を受け国民に支援を呼びかける偽メール」（表 1の項番1）というタイトルのフィッシングメール攻撃を行いました。

昨今では、インターネット中継でスポーツを観戦したり情報を収集したりする人々が増えています。無観客開催によりインターネット中継や試合結果などの情報発信が強化されました。きっと攻撃者も、東京オリンピック・パラリンピック関連のWebサイトを検索したり閲覧したりする人々が増加すると推測したでしょう。実際に、東京オリンピック・パラリンピックの偽中継サイト（表 1の項番3）を使ったフィッシング攻撃がありました。また、無観客開催へ変更になったことにより、チケットの払い戻しが発生しました。それにより、購入済みチケットの払い戻しを行う偽サイト（表 1の項番5）を使ったフィッシング攻撃がありました。

このように、新型コロナウイルスの流行により、東京オリンピック・パラリンピックの開催期間と観戦者の行動が変化したため、それにあわせて、主催組織本体へのサイバー攻撃からフィッシング攻撃へと攻撃が移ったと推測します。

“新型コロナウィルスの流行により、手口の中心は
サイバー攻撃から
フィッシング攻撃へ”

（2） 見解 ②：サイバー攻撃の流行

IPAが公開している「情報セキュリティ10大脅威 [8]」（以後、10大脅威）と、東京オリンピック・パラリンピックを狙ったサイバー攻撃の関係を分析します。10大脅威とは、情報セキュリティ分野の専門家が審議および投票を行い、その1年間で社会的に大きな影響が見られたセキュリティインシデント、サイバー攻撃、脆弱性などのイベントを選出したものです。2020年に発生したイベントを元にして作成された2021年版の10大脅威を表2に示します。

東京オリンピック・パラリンピックを狙ったサイバー攻撃には、「1年間の開催延期を受け支援を呼びかける偽メール」（表 1の項番1）や「東京オリンピック・パラリンピックの偽中継サイト」（表 1の項番3）などといったフィッシング攻撃がありました。フィッシング攻撃は、10大脅威の個人分野の2位です。「富士通のProjectWeb不正アクセスによる大会組織委員会関係者の個人情報漏えい」（表 1の項番4）といったサプライチェーン攻撃は、10大脅威の組織分野の4位です。2020年版の10大脅威にも、フィッシング攻撃とサプライチェーン攻撃も上位に入っており、この2つの攻撃は前々から流行していることが分かります。

このように、東京オリンピック・パラリンピックを狙ったサイバー攻撃と昨今の10大脅威の上位のサイバー攻撃が合致しているため、東京オリンピック・パラリンピックを狙ったサイバー攻撃は、サイバー攻撃の流行に沿っていたと考えることができるでしょう。

表 2：情報セキュリティ10大脅威 2021 [8]

順位	昨年順位	昨年比較	個人
1	1	→	スマホ決済の不正利用
2	2	→	**フィッシングによる個人情報等の搾取**
3	7	↑	ネット上の誹謗・中傷・デマ
4	5	↑	メールやSMS等を使った 脅迫・詐欺の手口による金銭要求
5	3	↓	クレジットカード情報の不正利用
6	4	↓	インターネットバンキングの不正利用
7	10	↑	インターネット上のサービスからの 個人情報の窃取
8	9	↑	偽警告によるインターネット詐欺
9	6	↓	不正アプリによるスマートフォン利用者への被害
10	8	↓	インターネット上のサービスへの不正ログイン

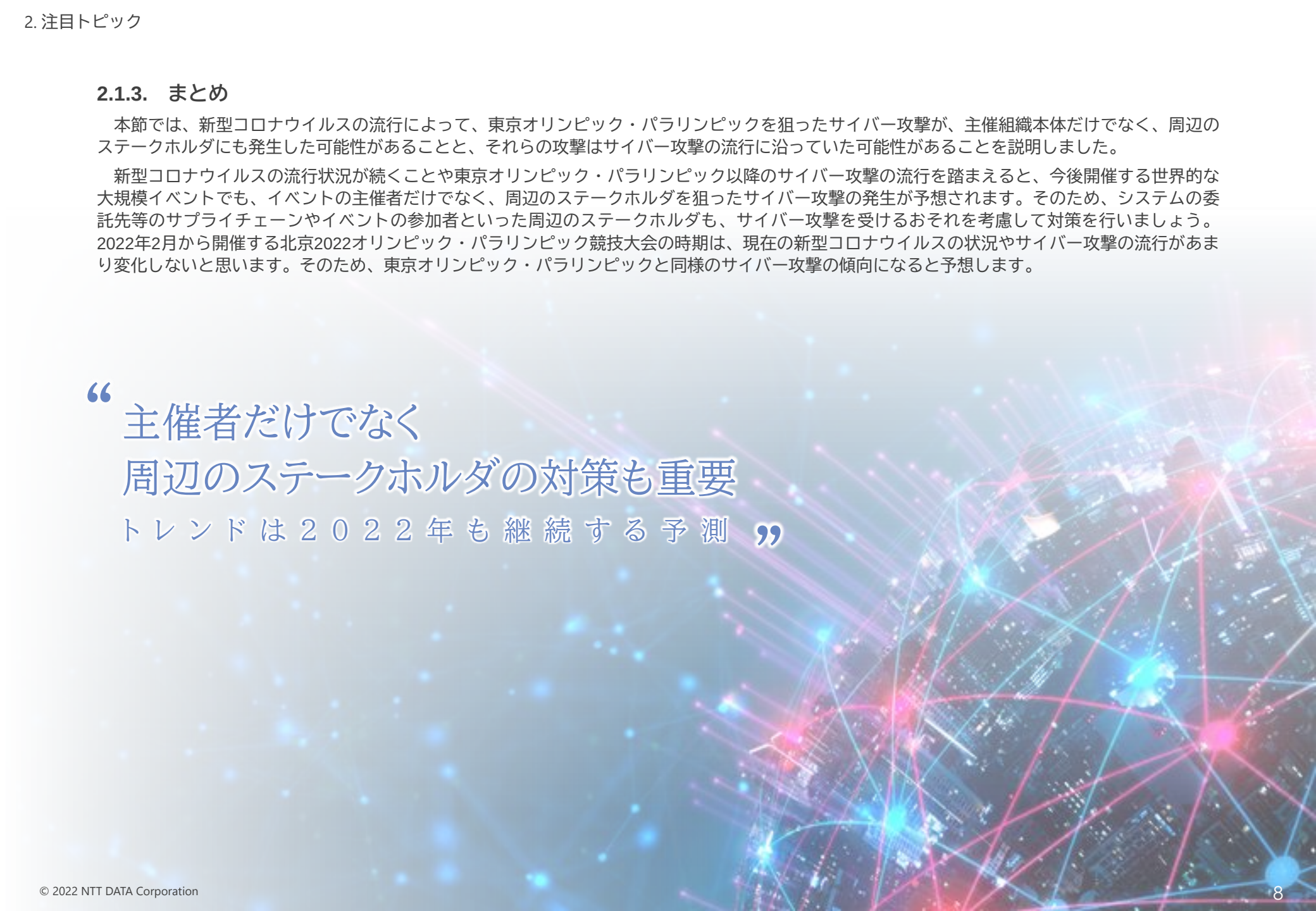
順位	昨年順位	昨年比較	組織
1	5	↑	ランサムウェアによる被害
2	1	↓	標的型攻撃による機密情報の搾取
3	-	NEW	テレワーク等の ニューノーマルな働き方を狙った攻撃
4	4	→	**サプライチェーンの弱点を悪用した攻撃**
5	3	↓	ビジネスメール詐欺による金銭被害
6	2	↓	内部不正による情報漏えい
7	6	↓	予期せぬIT基盤の障害に伴う業務停止
8	16	↑	インターネット上のサービスへの不正ログイン
9	7	↓	不注意による情報漏えい等の被害
10	14	↑	脆弱性対策情報の公開に伴う悪用増加

2.1.3. まとめ

本節では、新型コロナウイルスの流行によって、東京オリンピック・パラリンピックを狙ったサイバー攻撃が、主催組織本体だけでなく、周辺のステークホルダにも発生した可能性があることと、それらの攻撃はサイバー攻撃の流行に沿っていた可能性があることを説明しました。

新型コロナウイルスの流行状況が続くことや東京オリンピック・パラリンピック以降のサイバー攻撃の流行を踏まえると、今後開催する世界的な大規模イベントでも、イベントの主催者だけでなく、周辺のステークホルダを狙ったサイバー攻撃の発生が予想されます。そのため、システムの委託先等のサプライチェーンやイベントの参加者といった周辺のステークホルダも、サイバー攻撃を受けるおそれを考慮して対策を行いましょう。2022年2月から開催する北京2022オリンピック・パラリンピック競技大会の時期は、現在の新型コロナウイルスの状況やサイバー攻撃の流行があまり変化しないと思います。そのため、東京オリンピック・パラリンピックと同様のサイバー攻撃の傾向になると予想します。

“主催者だけでなく
周辺のステークホルダの対策も重要
トレンドは２０２２年も継続する予測”



3 情報漏えい
FortiGateの深刻な脆弱性

3.1 FortiGateの脆弱性の放置による代償

Fortinet社は、2019年5月に脆弱性 CVE-2018-13379 を公開しました [9]。CVE-2018-13379 は、Fortinet社のSSL-VPN装置FortiGateに存在する脆弱性で、2019年度版 第2四半期のグローバルセキュリティ動向四半期レポートでも深刻な脆弱性として取り上げています。この脆弱性は影響が大きいため、同時期にFortinet社のPSIRT（Product Security Incident Response Team）や国内外のセキュリティ機関も、複数回にわたり注意喚起しています [10]。しかし、さまざまな組織からの注意喚起後も当脆弱性に対して対策しない組織が多数存在しており、この脆弱性を悪用した攻撃によってFortinet社のFortiGateの認証情報の漏えいや不正侵入の被害が繰り返し発生しています。

2020年11月に何者かが当脆弱性を悪用して収集した約5万台分のFortiGateの認証情報をインターネット上で公開して、大きな注目を集めました [11]。日本国内で利用しているFortiGateの認証情報は、そのうちの約1割にあたる5千台分でした。日本の組織の中には、大学などの教育機関や航空関連、独立行政法人などが含まれていました。また2021年9月にも、Fortinet社がFortiGate 8万7千台分の認証情報が流出していることを公表しました [12]。本稿では、脆弱性の対策が依然として進まない原因を考察し、脆弱性の対策と脆弱性の対策を進めるための対応について説明します。

2019年5月から2021年9月の時系列を表 3に示します。

表 3：Fortinet社PSIRT及びセキュリティ機関による注意喚起

日付	組織	タイトル
2019年5月24日	Fortinet PSIRT	特別に細工されたHTTPリソースリクエストによるSSL-VPNを介したFortiOSシステムファイルの漏えい [13]
2019年9月2日	JPCERT/CC	複数の SSL VPN 製品の脆弱性に関する注意喚起 [14]
2020年7月16日	Fortinet PSIRT	SSL VPNの欠陥を標的としたATP 29 [15]
2020年11月27日	JPCERT/CC	Fortinet 社製 FortiOS の SSL-VPN 機能の脆弱性 CVE-2018-13379 の影響を受けるホストに関する情報の公開について [16]
2020年11月30日	Fortinet PSIRT	CVE-2018-13379 に関するアップデート [17]
2020年12月3日	内閣サイバーセキュリティセンター	Fortinet製VPNの脆弱性 CVE-2018-13379 に関する重要インフラ事業者等についての注意喚起の発出について [18]
2020年12月11日	Fortinet PSIRT	FireEye レッドチームツールの侵害 [19]
2021年4月2日	CISA/FBI	Fortinetの脆弱性悪用に関するCISA-FBI共同勧告 [20]
2021年4月3日	Fortinet PSIRT	パッチと脆弱性の管理 [21]
2021年5月27日	FBI	MI-000148-MW [22]
2021年6月1日	Fortinet PSIRT	ネットワークの整合性を確保するには、パッチ適用を優先することが不可 [23]
2021年9月8日	Fortinet PSIRT	悪意のあるアクターがFortiGate SSL-VPNの認証情報を公開 [12]

3.1.1. 脆弱性 CVE-2018-13379の解説

CVE-2018-13379は、Fortinet社製品のSSL-VPN装置FortiGateに存在する脆弱性です。FortiGateは、出張や在宅ワークなどでインターネットから会社の内部ネットワークへのアクセスに適したSSL-VPNを提供します [24]。SSL-VPNでのアクセスには、Fortinet社が提供するVPNクライアントソフトを利用するトンネルモードとWebブラウザを利用するWebモードがあり、このモードを設定するポータル画面にパストラバーサルの脆弱性が存在します [25]。攻撃者は、この脆弱性を悪用して、認証なしでFortiGate上の任意のファイルを指定してダウンロードできるおそれがあります。特に攻撃者は、FortiGate上に保存されているsslvpn_websessionファイルのパスを指定してダウンロードを試みます。このファイルには、SSL-VPN接続用のユーザIDと平文パスワードが含まれているため、もし攻撃者がこのファイルのダウンロードに成功すれば、攻撃者は、認証情報を使って正規ユーザになりすまして、FortiGateへSSL-VPN接続できてしまいます [26]。

攻撃者がSSL-VPN接続すると正規ユーザと同様の組織内部のシステムへアクセスできるため、FortiGate上に保存されている機密情報が漏えいする被害に留まりません。脆弱性 CVE-2018-13379を悪用した他のシステムの情報漏えいや改ざんなど、二次被害が大きくなります。

当該脆弱性に該当するFortiGateのファームウェアバージョンを以下の表 4に示します。

表 4：脆弱性該当ファームウェアバージョン

パッチ系統	該当バージョン
5.4系	5.4.6 ～ 5.4.12
5.6系	5.6.3 ～ 5.6.7
6.0系	6.0.0 ～ 6.0.4

3.1.2. CVE-2018-13379を悪用したランサムウェア攻撃

（1）ランサムウェア「Cring」による攻撃事例

トレンドマイクロ社によると、2021年1月から4月に同社がインシデント対応を支援したランサムウェア攻撃のうち、約7割がランサムウェア「Cring」による攻撃でした [27]。Cringは、ファイルの暗号化や脅迫文（ランサムノート）の作成、バックアップファイルの削除、システム回復機能の無効化など標準的なランサムウェアの活動を行います。攻撃者は、標的のネットワークへ侵入して、ネットワーク内部でツールを用いてアカウント認証情報の窃取やC＆Cサーバとの継続的な通信のやり取りするためのバッチファイルを配信した後にランサムウェアを実行して感染させます。同社が日本国内で確認した事例では、攻撃者はFortiGateの脆弱性を悪用して侵入しており、特に脆弱性CVE-2018-13379を悪用した事例が多数ありました。また、もう一つ注目したい点は、攻撃を受けた組織の中には、セキュリティパッチを適用したにも関わらず、FortiGate上のSSL-VPNユーザのパスワード変更が未実施だったことが原因で、Cringによる被害を受けた組織があったことです。

（2）サイバー攻撃集団APT29による悪用

英国の国家サイバーセキュリティセンター (NCSC)とカナダ通信保安局（CSE）、米国のCISA、NSAは、「Dukes」または「Cozy Bear」とも呼ばれているサイバー攻撃集団「APT29」の攻撃の起点の一つにFortinet社の脆弱性が使われている点を挙げて、次のように報告しています [28]。

「ATP29」は、さまざまなツールと手法で、主に政府、外交、シンクタンク、医療機関およびエネルギー関連施設などを標的に情報取得しており、 2020年を通じて、カナダ、米国、英国において、COVID-19ワクチン開発に関与する様々な組織を対象に、COVID-19ワクチンの開発に関する情報や知的財産を盗むおそれがあります。COVID-19ワクチンの研究開発を標的とした最近の攻撃では、攻撃の初期ベクターで、組織が所有する特定の外部IPアドレスの脆弱性スキャンにより脆弱性を特定し、攻撃に悪用しています。悪用する脆弱性にFortiGateの脆弱性 CVE-2018-13379 の他、2019年度版 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で取り上げたCitrixの脆弱性、2020年度版 第1四半期のグローバルセキュリティ動向四半期レポートで取り上げたPulse Secureの脆弱性も挙げています [29] [30]。

3.1.3. 脆弱性 CVE-2018-13379の対策

脆弱性 CVE-2018-13379への対策としては、セキュリティパッチの適用が必要です。2019年5月に脆弱性が公開されて以来、2021年10月時点ですでに2年6ヶ月も経過しているため、まだセキュリティパッチを適用していない場合は既に攻撃を受けて認証情報が漏えいしている確率が高いです。そのため、これからセキュリティパッチを適用する場合は、既に認証情報が漏えいして二次被害が起きている前提で、脆弱性の対策だけでなく、同時に二次被害の対応も進めてください。直ちに行うべき暫定対策と本格的に対処すべき恒久対策、二次被害を防ぐための対策を以下に示します。

（1）脆弱性 CVE-2018-13379の暫定対策

① SSL-VPN接続の停止

SSL-VPN接続を使用していない場合は、SSL-VPN接続を停止してください。SSL-VPN接続を停止すれば、だれもSSL-VPN接続を使用できなくなります。攻撃者も窃取した認証情報を悪用してSSL-VPN接続経由で不正アクセスできません。ただし、正規の利用者もSSL-VPN接続を使用できないため、利便性を失います。

（2）脆弱性 CVE-2018-13379の恒久対策

① セキュリティパッチの適用

脆弱性 CVE-2018-13379を修正するセキュリティパッチを適用してください。以下の表 5に、パッチ適用後の脆弱性が修正済みのバージョンを示します [13]。

本レポート執筆時点では5.4系と5.6系は既にメーカサポートが終了しており、原則Fortinet社はセキュリティパッチを提供しません。6.0系もクリティカルな脆弱性のみセキュリティパッチを提供する限定的なサポートになっているため、セキュリティパッチを提供しない場合があります。Fortinet社から継続してセキュリティパッチ提供のサポートを受けるためには、バージョン6.2系を維持してください。その際、古いバージョンからいきなり最新のセキュリティパッチを適用してバージョンアップしてしまうと、設定内容が正常に引継がれないことがあるため注意が必要です。設定を正常に引継ぐためには、メーカの推奨する順序で段階的にパッチを適用し、最新バージョンにアップグレードしてください [31] [32]。

表 5：脆弱性CVE-2018-13379修正済みのFortiGateのバージョン

バージョン	修正済みバージョン	サポート状況
5.4系	5.4.13	サポート終了
5.6系	5.6.8以降	サポート終了
6.0系	6.0.5以降	サポート終了
6.2系	6.2.0以降	サポート中

（3）二次被害（認証情報漏えい）の暫定対策

① FortiGateの侵害調査

脆弱性 CVE-2018-13379は、2019年5月に脆弱性が公開されてから2年半以上が経過しており、対策していなければ、既に攻撃を受けている確率が非常に高いです。よって、脆弱性CVE-2018-13379が公開されて時間が経ってから対策する場合は、すでに攻撃者がFortiGateの攻撃に成功してFortiGate上からSSL-VPN接続用の認証情報を窃取して、正規ユーザになりすまして不正ログインしていることを十分に想定した上で、必ずFortiGateへの攻撃者の侵害の有無を調査してください。

② SSL-VPNユーザのパスワード変更

攻撃者がFortiGateへの不正ログインに成功していた場合、3.1.2の事例のように、FortiGateへセキュリティパッチを適用した後でも攻撃者は認証情報を悪用して、パッチ適用済みのFortiGateへ侵入できてしまいます。よって、攻撃者が侵害している場合は、セキュリティパッチ適用後に必ずパスワード変更してください。

（4）二次被害（認証情報漏えい）の強化対策

脆弱性 CVE-2018-13379で認証情報が漏えいした場合に限らず、SSL-VPN接続の接続元IPアドレス制限と多要素認証の導入は、認証情報の漏えい時の強化対策です。

① SSL-VPN接続の送信元IPアドレス制限

SSL-VPN接続の送信元IPアドレスを固定できる場合は、SSL-VPN接続の送信元IPアドレスを制限することで、攻撃者のIPアドレスからの不正ログインを遮断できます。認証情報が漏えいしても、不正ログインを防止できます。

② 多要素認証の導入

ユーザIDとパスワードの知的認証に、生体認証や、ワンタイムパスワードなどの所有物認証を追加して、複数の認証方式を組み合せて認証する多要素認証を導入しましょう。認証方法の1つが突破されても不正ログインを防止できることから、多要素認証は認証情報が盗まれた場合だけでなく、脆弱なパスワードを使っている場合や、フィッシングサイトへ誤ってパスワードを入力して漏えいした場合も有効な対策です。だれでもアクセス可能なポートで、ログイン認証付きサービスをインターネットへ公開している場合は、多要素認証方式の採用を強く推奨します。

“FortiGateの脆弱性に対しては
パッチ適用後の侵害調査と
パスワード変更に加え、IPアドレス制限や
多要素認証導入など強化対策が重要”

3.2 脆弱性CVE-2018-13379を放置した理由の考察

本章では、脆弱性CVE-2018-13379が対策されずに長期間放置されていた理由を考察します。

2年半の間、脆弱性CVE-2018-13379の対策を放置した組織は、セキュリティパッチを適用できない理由があったのでしょうか。例えば、「セキュリティ対策に予算をかけられない業種や規模の組織がセキュリティパッチを適用できなかった」と推測すると思います。この推測が正しいかどうか、脆弱性を悪用されてFortiGateの認証情報が漏えいした組織の情報を集めて分析しました。報道された該当組織の情報を整理した結果を表 6に示します。表 6から、官公庁や民間企業、教育機関など、さまざまな業種の組織で被害が発生しており、特定の業種に偏っていませんでした。組織の規模も様々で、偏りや共通点はありませんでした。よって、脆弱性対策を長期間放置した原因は、業種や組織の規模に起因していないと考えます。

では、表 6の各組織は、適切な脆弱性対策プロセスを取っていたのでしょうか。

表 6：認証情報漏えい組織一覧

分類	組織名称	規模（職員数/従業員数など）
官公庁	警察庁 [33]	職員数：7,995名 [34]
	岐阜県庁 [35]	職員数：約5,000名（公安委員会・教員委員会を除く） [36]
	佐賀県伊万里市役所 [11]	職員数：431名（再任用職員を除く） [37]
	愛知県東郷町役場[38]	職員数：308名 [39]
	日本政府観光局 [40]	職員数：207名 [41]
民間企業	株式会社リクルート[35]	従業員数：15,807名（アルバイト・パート含む) [42]
	日新製糖株式会社 [43]	従業員数：259名 [44]
	株式会社ディーカレット [45]	従業員数：52名 [46]
教育機関	慶應義塾大学 [33]	教員数：2,791名（常勤者 有期契約を含む） [47]
	札幌大学 [48]	教員数：76名 [49]
	福井工業大学 [50]	教員数：99名 [51]
医療機関	一宮市立市民病院 [33]	医師数：180名、看護師数：664名 [52]

われわれが考えた脆弱性対策サイクルを図 1に示し、以下で脆弱性対策サイクルを構成する各プロセスを説明します。

まず、脆弱性対策サイクルの1つ目のプロセスは、「構成管理」です。構成管理は、利用している機器情報やバージョン情報を正確に把握することから始めます。機器情報やバージョン情報を管理していないと、2つ目のプロセスの「脆弱性収集」が行われません。これにより、脆弱性の公表や注意喚起があったとしても、自組織の機器やソフトウェアが脆弱性に該当するかどうかがわかりません。よって、対策を検討することもなく、脆弱性を放置してしまうおそれがあります。

2つ目のプロセスは、「脆弱性収集」です。脆弱性収集では、構成管理している対象機器やソフトウェアについて、メーカやセキュリティ情報サイトからの脆弱性情報を収集して調査したり、セキュリティ診断したりして、脆弱性の有無を確認して管理します。機器やソフトウェアの脆弱性に気づくためには、脆弱性情報の収集は欠かせません。この脆弱性情報の収集と調査のプロセスが欠けてしまうと、脆弱性を放置して被害が発生するおそれがあります。

3つ目のプロセスは、「リスク評価」です。リスク評価では、脆弱性の危険度を評価します。具体的には、該当する機器やソフトウェアが脆弱性を悪用した攻撃を受けてそれが成功する確率、攻撃が成功した場合の影響度などを評価して、脆弱性対策の必要性と緊急度を決定します。リスク評価で脆弱性の緊急度の評価を誤ると、4つ目のプロセスの「対策実施」が遅れて、攻撃を受けてしまうかもしれません。

4つ目のプロセスの「対策実施」では、脆弱性を対策します。このプロセスでは、対策ミスしないことが重要です。セキュリティパッチを適用する作業では、ほとんど問題が発生しませんが、暫定対策や強化対策では、やり方を間違えると効果が得られません。特定のシステム構成や設定内容など、特定条件に一致する場合のみ、有効な対策もあります。勘違いして、条件に一致しないシステムへ暫定対策や強化対策を実施してしまう場合もあります。

図 1:脆弱性対策サイクル

以上の4つのプロセスのうち、どこかに脆弱性が放置され続けた原因があると推測します。まず構成管理ができていない場合は、自組織で使用している機器やソフトウェアのバージョンを特定できません。そのため、脆弱性情報を公表してもリスク評価や対策実施せず、脆弱性の注意喚起が繰り返し行われたとしても自分の機器やソフトウェアが該当することに気づかず、脆弱性を長期間放置してしまうでしょう。

つぎに脆弱性収集ができていない場合です。どんなにしっかり構成管理をしていても、脆弱性情報の収集を行わなければ、メーカやセキュリティベンダが報告する脆弱性の存在に気づくことはありません。またセキュリティ関連のニュースを受信しているだけでは、脆弱性のニュースに漏れなく気づくとは限りません。脆弱性収集ができていない場合やきちんと構成情報と脆弱性情報を照会していない場合は、脆弱性を長期間放置すると思います。

リスク評価ができていな場合、誤ってリスクを低く評価してしまい、対策実施を遅らせることがあります。しかし、重大な脆弱性は、メーカやセキュリティ機関が繰り返し注意喚起するため、構成管理と脆弱性収集を適切に行っていれば、それらの情報からリスク評価を誤り続けて、脆弱性を長期間放置することは考えにくいです。

対策実施ができていない場合は、セキュリティパッチを適用するまえの検証に長時間を要する場合が考えられます。しかし、どんなに検証に時間がかかる場合でも、約2年6カ月は掛からないはずです。

よって、情報システム部門や情報セキュリティ部門などのシステム管理者が構成管理と脆弱性収集を怠り、脆弱性を認識できなかったから、脆弱性を長期間放置したと推測します。報道でも、外部からの指摘で初めて事態を認識したとコメントした組織もありました [33] [35]。また、構成管理や脆弱性収集を怠った組織は、その後のリスク評価や対策実施のプロセスが機能していません。脆弱性による被害をなくすためには、脆弱性対策サイクルは確実に実施しなければなりません。しかし、これまで脆弱性を放置してきた組織に脆弱性対策サイクルを浸透させるのは簡単ではありません。構成管理の方法と脆弱性収集の方法を決めて、管理対象の情報を集めることから始めなければなりません。リスク評価の基準も決める必要があります。コストもかかりますし、セキュリティのスキルも必要です。現場のシステム管理者だけでは、とても対応しきれないでしょう。組織によって、FortiGateなどのネットワーク機器の運用保守を外部ベンダに委託している場合もあるかもしれません。外部ベンダは、ハードウェア保守のみが作業範囲で、パッチ適用や脆弱性対策などのセキュリティ対策が作業範囲に含まないことがよくあります。その場合は、委託内容に脆弱性対策サイクルを明確に含めるべきです。

ここまで述べてきたように、脆弱性対策サイクルは、組織内は勿論、外部の委託先ベンダも含めて徹底させる必要があります。これらを解決するには、要員不足やコスト、社内ルール化の課題があるので、経営層がトップダウンで組織全体に脆弱性対策サイクルの取り組みを指示するべきです。脆弱性を長期間放置することはサイバー攻撃による業務停止などの被害につながるため、経営リスクです。経済産業省のサイバーセキュリティ経営ガイドラインVer2.0によると、「経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要」と書かれています [53]。経営層は、このガイドラインに沿って、組織内のセキュリティ対策の責任者とその役割を明確化して、その責任者へ脆弱性対策サイクルの取り組みを指示するべきです。

また、経営層への脆弱性対策サイクルの導入状況の定期的な報告を義務付けたり、脆弱性対策サイクルの運用状況の監査も取り入れたりすると、脆弱性を長期間放置することは無くなると考えます。

3.3 まとめ

SSL-VPN装置のFortiGateは、組織外部から内部システムにアクセスする環境を提供します。FortiGateの脆弱性を長期間放置してしまうと、攻撃者からFortiGate本体、およびSSL-VPN経由でアクセス可能な内部システムまで、幅広く侵害を許して、二次被害、三次被害と被害が拡大するおそれがあります。被害の規模によっては、事業の停止は避けらず、ランサムウェア攻撃を受けて、多額の身代金を支払ったり、システムの復旧に長期間を要したりすると経営が悪化して、最悪の場合は組織の存続を脅かします。

そのため、経営層は脆弱性を長期間放置することが経営リスクにつながることを認識し、組織内のセキュリティ対策の責任者を任命しその役割を明確化して、トップダウンで脆弱性対策サイクルの取り組みを指示する必要があります。指示を受けた責任者や情報システム部門は脆弱性対策サイクルの運用を確立し、順守しなければなりません。さらに、その脆弱性対策サイクルの運用が適切に実行されていることを確認する監査の仕組みまで経営層が主体となって確立させることで、脆弱性に対して確実に対応することができるはずです。

4 脆弱性
iPhoneで発見された脆弱性

本稿では、iPhoneに生じた脆弱性CVE-2021-30860とそれを悪用した攻撃事例について解説します。

4.1 iPhoneの「BlastDoor」も破るゼロクリック攻撃

2021年8月24日に、カナダのトロント大学のセキュリティ研究所Citizen Labは、バーレーン政府がイスラエルのNSO Groupのスパイウェア「Pegasus」を使って複数人の人権活動家のiPhoneにゼロクリック攻撃を仕掛けていた、と報告しました [54]。バーレーン政府によるPegasusを使った盗聴は、彼らの活動の監視が目的だったようです。

4.1.1. ゼロクリック攻撃とは

ゼロクリック攻撃とは、2016年頃に見つかった被害者の操作を必要とせずにマルウェア感染等を行う攻撃手法です。被害者自身が端末を操作しなくてもマルウェアに感染するため、被害者は攻撃を受けていることに気付きません。

2020年12月20日、Citizen Labが、iPhoneのデフォルトアプリiMessageに含まれる脆弱性を悪用したエクスプロイト「Kismet」によるゼロクリック攻撃を公表しました [55]。このゼロクリック攻撃に悪用された脆弱性は特定できていませんが、Citizen Labは被害者のiPhoneを解析して攻撃手法の解明を試みました。被害者のiPhoneは、Pegasusインストールサーバにアクセスする直前に、図 2の“Highly unusual connections to Apple servers”に示すように多数のiCloudパーティションへ異常な接続を行っています。その後、”*.regularhours.net”へ接続して、Pegasus Installation Server からPegasusをインストールします。この２つの処理間のログを分析したところ、上記の処理は、iMessageやFaceTimeを処理するための組み込みアプリであるimagentプロセスをつかってroot権限で実行されていました。したがって、Citizen Labは、imagentプロセスに含まれる未知の脆弱性が悪用されたと推測しています。

4.1.2. BlastDoorとは

AppleはiMessageの脆弱性を悪用したゼロクリック攻撃への対策として「BlastDoor」と呼ばれる機能をiOS 14から実装しています。BlastDoorは、メッセージをimagentプロセスから隔離した独自のサービスプロセス内で処理する仕組みです（図 3）。identityservicesdプロセスで解凍されたメッセージはMessagesBlastDoorServiceプロセスに格納され、XMLファイルの整形処理やデータのシリアライズ処理等を受けます。この際にネットワーク操作も発生しないため、MessagesBlastDoorServiceプロセスはサンドボックス化された環境としてデータを処理します。imagentプロセスはMessagesBlastDoorServiceプロセスの処理が完了してからデータを受け取るため、もしメッセージ内に悪意のあるコードが含まれていても、iOS上で直接コードが実行されることはありません。本機能の実装により、Kismetによるゼロクリック攻撃は機能しなくなりました。

図 2：Kismetエクスプロイトによる攻撃のタイムライン [55]

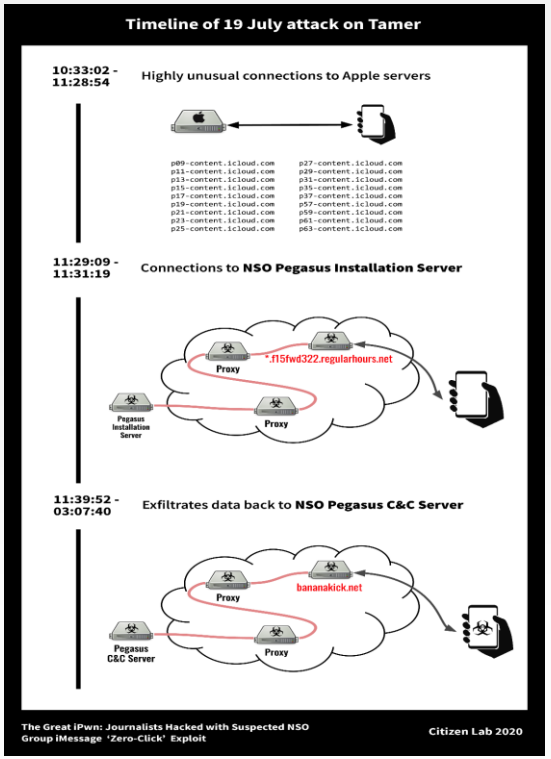
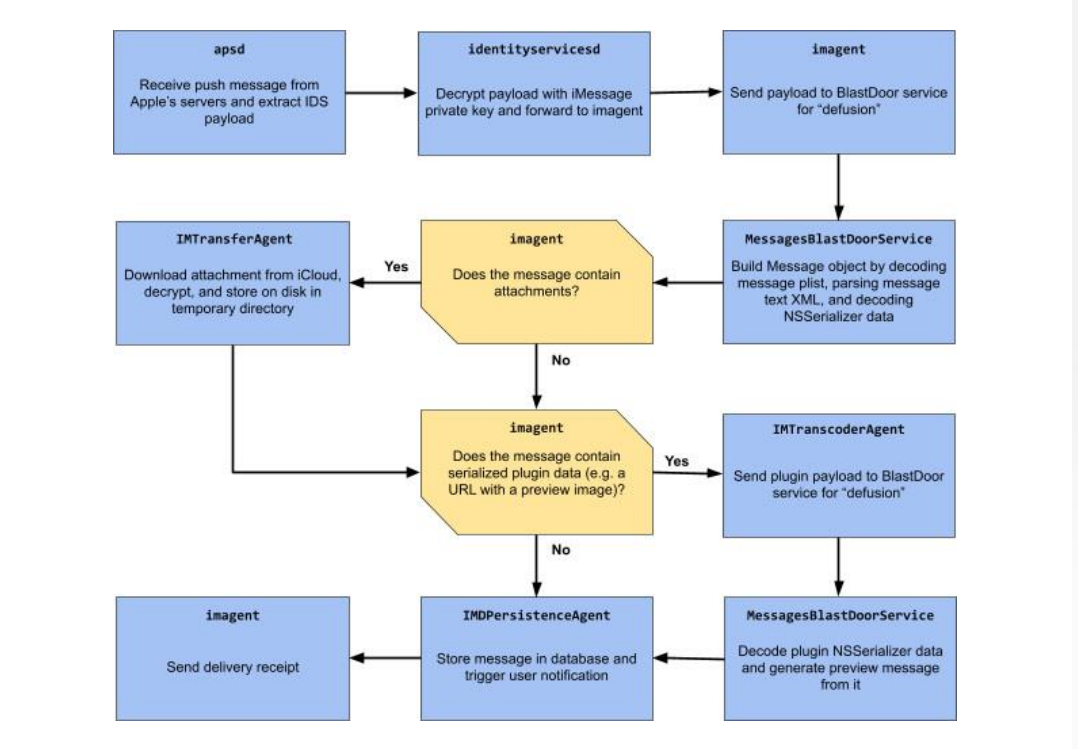


図 3：BlastDoorを導入したiMessageの処理パイプライン [56]



4.1.3. 「BlastDoor」を回避するゼロクリック攻撃

iPhoneの「Blast Door＝防爆扉（爆発から守る分厚い扉）」を「Forced Entry=こじ開けて侵入」できるのが今回取り上げる攻撃です。この攻撃は、iMessageに含まれる脆弱性CVE-2021-30860を悪用するエクスプロイト「ForcedEntry」を使います [57]。当該脆弱性は、iMessage の中のAppleのベクトル描写フレームワークであるCoreGraphicsに存在し、悪意のあるファイルを処理すると整数オーバーフローが発生して、処理領域外へのメモリアクセスを可能にしてしまいます。具体的には、GIFに偽装したAdobe PhotoshopのPSDファイルを処理する際に上記の問題があり、PSDファイルに偽装した悪意のあるファイルを送り付けて処理させると、上記のBlastDoorを回避してiPhoneをハッキングできます。さらに、トレンドマイクロ社による解析では、ForcedEntryは、BlastDoorだけでなく、以下の2つのiOSの脆弱性悪用防止の仕組みも回避していることがわかりました [58]。

（1）アドレス空間配置のランダム化（ASLR）の無効化

ASLR（Address space layout randomization)とは、メモリ破壊型の脆弱性の悪用を抑止する仕組みです。OSがプログラムを実行する際に、データ領域やスタック領域、ヒープ領域などのデータを格納するCPUメモリ領域のアドレスをランダムに配置します。この仕組みにより、攻撃者は、特定のメモリアドレスに不正な命令を送り付けることが困難になります。

iOSにもASLR機能を実装しているのですが、トレンドマイクロ社の解析によれば、ForcedEntryの悪用前にASLR機能が無効化されていました。なぜ、ASLR機能を無効化できたのか、解明できていません。

（2）ポインタ認証コード（PAC）のバイパス

ポインタ認証コード（Pointer Authentication Code）とは、メモリ破壊型の脆弱性の悪用を抑止する仕組みです。OSが命令を実行する際、CPUメモリ内の別のアドレスに保存された処理を呼び出すために使用するポインタに対して、署名（ポインタ認証コードの生成）を行います。OSは呼び出し先の処理の実行前にポインタ認証コードの検証を行い、検証に失敗すると処理を中止します。この仕組みにより、攻撃者は、ポインタを改ざんした不正なコード実行を行うことが困難になります。しかし、トレンドマイクロ社の解析によれば、攻撃者がポインタ認証コードのセキュリティ機能をバイパスして処理の呼び出しに成功しています [58]。

このように、ForcedEntryの攻撃者は、iOSが処理を実行する際に必ず動作している2つの防御機構を回避しています。現在、ASLR無効化とポインタ認証コード機能をバイパスする手法は解明できておらず、ForcedEntryの攻撃者は高度な攻撃手法を用いていたといえます。

“iOSの脆弱性悪用防止の仕組みも回避
攻撃手法は
未だ解明されていない”

4.2. まとめ

本稿では、iMessageに含まれる脆弱性CVE-2021-30860とそれを悪用した「ForcedEntry」エクスプロイトを使用した攻撃事例を取り上げました。今回の攻撃は、iPhoneの複数の防御機構を回避する高度で複雑な攻撃手法であり、安全と言われるiPhoneにおいても被害が発生しました。当該脆弱性は、iPhoneをiOS 14.8以降のバージョンにアップデートすることで修正できます。攻撃者のもともとの目的はPegasusを使って特定の活動家を密かに、継続的に監視することにあります。仮にこうした攻撃を広範な標的に実行してしまうと、活動自体が露見されやすくなり、その目的にそぐわなくなります。したがって、アップデートを実施すれば一般の利用者への被害は拡大しないと考えます。

5 マルウェア・ランサムウェア
脆弱性Proxy Shellを利用した攻撃

5.1. Microsoft Exchange serverの脆弱性 ProxyShellを利用したマルウェア攻撃

「ProxyShell」とは、Microsoft Exchange Serverにおいて2021年4月に発見された3つの脆弱性の総称です [59]。未だに多くのサーバが脆弱性を修正しておらず [60]、攻撃されるおそれがあります。

Microsoft社は、2021年4月および5月にProxyShellを修正するための更新プログラムを公開しました [61] [62] [63]。しかし、ProxyShellが発見されてから7か月経った2021年11月初頭でも、約2万7千台のサーバがまだProxyShellを修正していません [60]。そのため、ProxyShellを修正していないMicrosoft Exchange Serverを標的としたサイバー攻撃が、多く発生しています [64]。具体的には、上記のMicrosoft Exchange Serverを標的にしたサイバー攻撃で、ランサムウェア「LockFile」による被害が発生しています。様々な業界で猛威を振るっているランサムウェアです [65]。LockFileはProxyShellの発見を機に、新しく発生して、2021年7月に初めてアメリカで確認されたランサムウェアです。アメリカおよびアジアを中心として世界各地の様々な業界で猛威を振るって、被害が拡大しているランサムウェアです [65]。被害を受けた具体的な組織名や被害総額は2021年10月末時点では不明ですが、製造系やファイナンシャルサービス、エンジニアリング、法律関係、旅行関係等、幅広い業界に被害を与えています [65]。

本稿ではProxyShellを悪用する攻撃の一連の流れ、ProxyShellの特徴、および推奨する対策について解説します。

5.1.1. 攻撃のステップ

本セクションでは攻撃の流れを、図 4に基づいて解説します。攻撃者は合計で10個のステップを経て標的組織の内部に侵入して、マルウェアを実行します。ステップ④までがProxyShellにかかわる部分なので、詳細に解説します。

【攻撃のステップ】

① ProxyShellの脆弱性有無を探索：

攻撃者は、インターネット上の複数のMicrosoft Exchange Serverをスキャンして、ProxyShellの脆弱性があるMicrosoft Exchange Serverを特定します。

② バックエンドサーバへSYSTEMユーザとして侵入：

攻撃者はステップ①で特定した脆弱性があるMicrosoft Exchange Serverに対して、CVE-2021-34473を悪用して攻撃します。攻撃者は、細工したURLをクライアントアクセスサービス（次のセクションにて解説）へリクエストすると、クライアントアクセスサービスがそのURLをバックエンドサービス宛てに書き換えます [66]。その結果、攻撃者はバックエンドサービスにSYSTEMユーザとしてアクセスできます [66]。

③　WebShellを設置する：

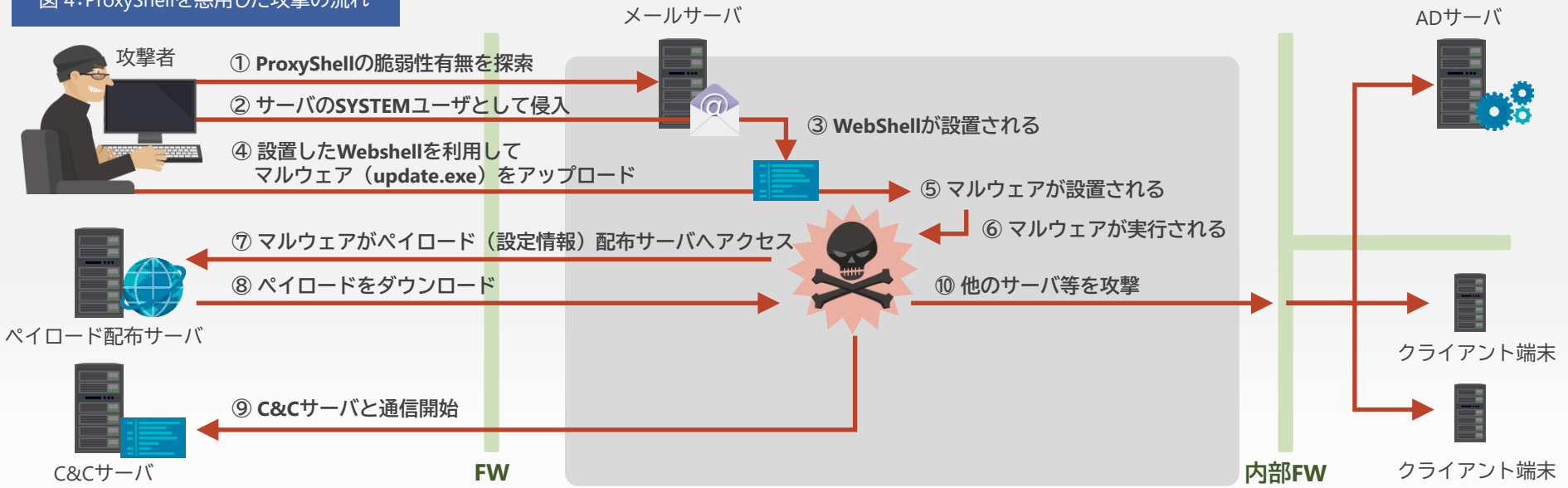
バックエンドサービスに侵入済みの攻撃者は、攻撃者の用意したサーバから標的のMicrosoft Exchange Serverのメールボックスへ WebShellのファイルをメールへ添付して送付します。WebShellとは、ユーザがサーバ上で任意のコマンドを実行するために、インストールして使うバックドアプログラムやその仕組みを言います [67]。SYSTEMユーザはメールボックスを持っていないため、CVE-2021-34523を悪用してSYSTEMユーザからMicrosoft Exchange Server の管理者に権限昇格します。これにより、攻撃者は管理者権限でPowerShellを使って、管理者のメールボックスからWebShellのファイルを取り出して保存できます [66]。しかしこのままでは、WebShellのファイルは、プログラム実行を禁止したフォルダにしか保存できません。そこで攻撃者は、ファイルを任意のパスに書き出すことができる脆弱性 CVE-2021-31207を持っているExchange Sever管理用PowerShellのメールのエクスポート専用コマンドを使って、WebShellファイルを含むメールボックスをpstファイルとしてWebrootフォルダへエクスポートします [68]。pstファイルからWebShellファイルを抽出して、Webrootフォルダで実行します [68]。

④　設置したWebShellを利用してマルウェアをダウンロード：

攻撃者は、Microsoft Exchange Serverが動作しているマシン上でランサムウェアなどのマルウェアを実行するためには、攻撃者のマシンからマルウェアをダウンロードします。WebShellで任意のコマンドを使用して、マルウェア（update.exe）をアップロードします。

ステップ⑤以降は、マルウェアを起動して、C＆Cサーバと通信を開始することで、攻撃者がリモートで他のサーバにマルウェアを複製したりランサムウェアをしかけたりします。

図 4：ProxyShellを悪用した攻撃の流れ



5.1.2. 脆弱性ProxyShellの危険性

本セクションでは、ProxyShellの影響度の高さおよび攻撃の容易さを踏まえて、ProxyShellが危険な脆弱性であることを解説します。

（1） 影響度：3つの脆弱性を悪用した攻撃による情報資産の窃盗やランサムウェア被害

攻撃のステップでも解説したように、ProxyShellは3つの異なる脆弱性を指していて、3つを順番に実行すると攻撃者が認証なしで遠隔から簡単にコマンド実行できてしまいます [69]。3つの脆弱性が連携して作動することで攻撃が成立することから、エクスプロイトチェーンとも言われています [70]。エクスプロイトチェーンは2019年あたりから使用されている新しい用語で、一続きのエクスプロイト（ソフトウェアやシステムが内包しているセキュリティの脆弱性を攻撃するプログラム [71]）を指しています。ProxyShellのエクスプロイトチェーンを構成している3つの脆弱性を表 7に示します [61] [62] [63] [68]。

表 7：Microsoft社が発表したProxyShellの3つの脆弱性

No.	CVE番号	脆弱性の特徴
1	CVE-2021-34473	認証を回避してリモートからコードを実行できる脆弱性
2	CVE-2021-34523	特権の昇格の脆弱性
3	CVE-2021-31207	セキュリティ機能をバイパスして 任意のファイルを上書きできる脆弱性

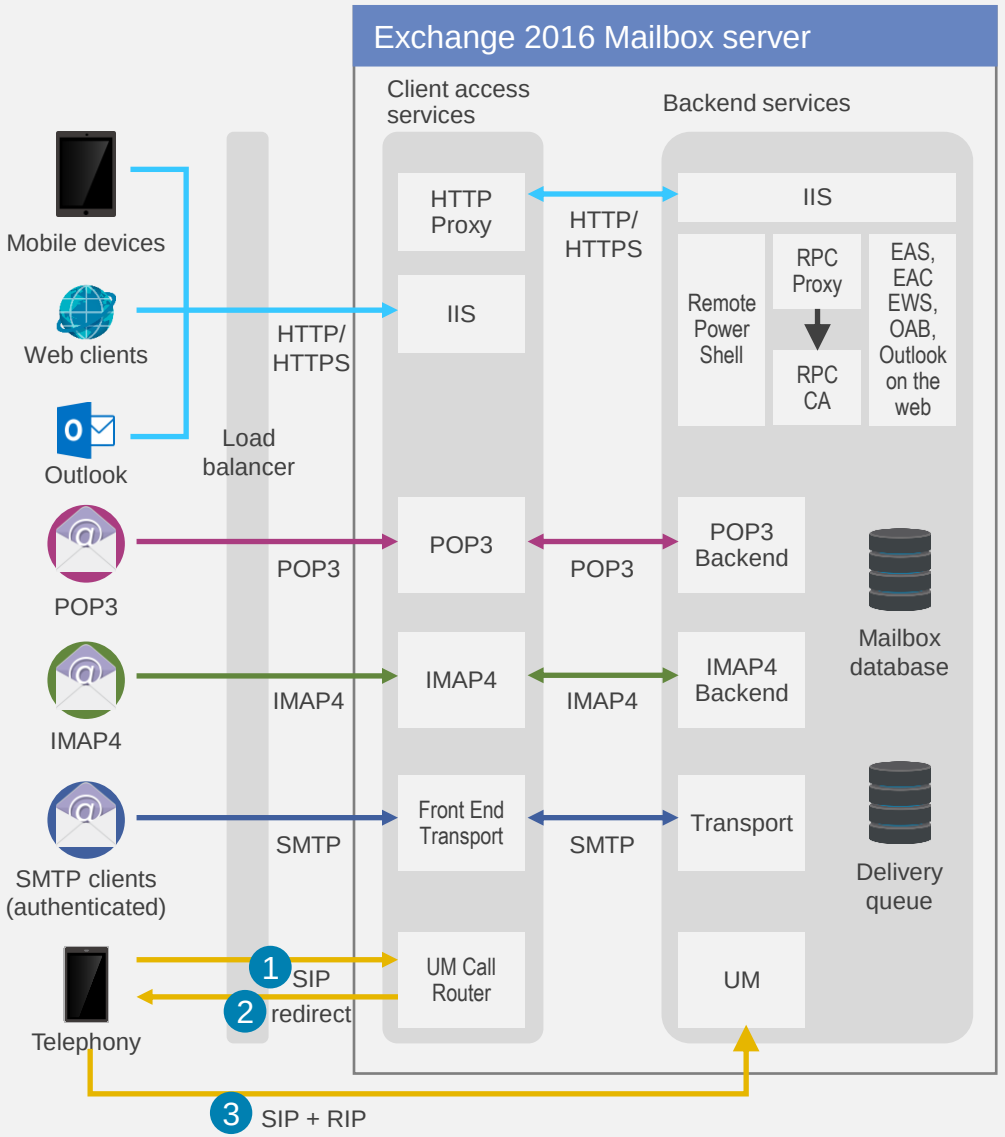
“ ProxyShellには
3つの
脆弱性があり、
組み合わせることで
攻撃が成立してしまう ”

図5で「Client access services」と囲まれている部分が、Microsoft Exchange Serverのクライアントアクセスサービス（以下、「CAS」という）のフロントエンドサービスで、「Backend services」と囲まれている部分がバックエンドサービスです。CASは、クライアント接続に対して認証サービスとプロキシサービスを提供します [72]。Microsoft社によると、CVE-2021-34473は、CASのフロントエンドサービスに脆弱性CVE-2021-34473が存在します。攻撃者は、インターネット経由でフロントエンドサービスへ直接通信できるため、脆弱性CVE-2021-34473を容易に攻撃できます。バックエンドサービスは、CASから転送されたPOP3/IMAP4/SMTP クライアントや Web クライアント (HTTP/HTTPS) などの様々なリクエストを受け取っています [72]。通常、OutlookやWebブラウザなどのクライアントソフトは、CASを経由して、バックエンドサービスにあるメールボックスなどへアクセスするため、バックエンドサービスに直接アクセスできません。しかし、CASに脆弱性 CVE-2021-34473があると、攻撃者はこの脆弱性を悪用して、バックエンドサービスにアクセスできてしまいます [59]。

脆弱性CVE-2021-34523およびCVE-2021-31207は、バックエンドサービスに侵入しないと悪用できないため [66]、Microsoft社は攻撃者が悪用できる確率が低いと説明しています [61] [63]。しかし、CVE-2021-34473がバックエンドサービスへの侵入を許す脆弱性であるため、侵入に成功した攻撃者は、悪用の確率が低いCVE-2021-34523およびCVE-2021-31207も悪用できてしまい、最終的にこの3つの脆弱性を連ねると任意のコマンドが実行できるようになってしまいます [64]。

攻撃者が任意のコマンドを実行できると、バックエンドサービスにあるメールのデータベースからメール情報を盗んだり、ランサムウェアをダウンロードして実行したりします。これらの攻撃により、情報漏洩やシステム停止に発展するおそれがあるため、組織への影響度は高いと考えられます。

図 5：Microsoft社が提示しているMicrosoft Exchange Server 2016のネットワーク構成図



（2） 攻撃の容易性：40万台以上のExchange Serverがインターネットに露出

Microsoft Exchange Serverは、スマートフォンやパソコン等を使ってどこからでもアクセスできるよう、ユーザの利便性を考慮してインターネットに露出しています [73]。インターネットに露出しているMicrosoft Exchange Serverの数の合計は、約40万台以上です [59]。また、攻撃者は、攻撃可能な脆弱性があるMicrosoft Exchange Serverを活発的にスキャンしています [64]。この状況により、脆弱性が発見された4か月後の2021年8月でも、ProxyShellに関連するインシデントレポートが2日間で100件以上報告されていました [74]。よって、脆弱性情報と更新プログラムの公開後、時間が経過しても、ProxyShellを悪用した攻撃が多く発生していることが分かります。

5.1.3. まとめ

本稿の冒頭でも述べた通り、ProxyShellの発見から7か月経った2021年11月初頭でも、約2万7千台のサーバがまだProxyShellを修正していません [60]。その原因の多くは、2021年度第2四半期のグローバルセキュリティ動向四半期レポートの情報漏えいの記事で考察したように、情報システム部門や情報セキュリティ部門などのシステム管理者が構成管理と脆弱性の情報収集を怠り、脆弱性を認知していないからだと思います。ただし、ProxyShellは脆弱性管理ができていたとしても、対応の優先度の判断が難しい脆弱性です。3つの脆弱性のうち、1つめの脆弱性 CVE-2021-34473だけではWebShellを設置できません。2つ目以降の2つの脆弱性は悪用できる確率が低いと説明しています [61] [63]。そのため、対応不要と判断してしまうかもしれません。システム管理者は、ひとつひとつの脆弱性のリスクを評価するだけでなく、実際のサイバー攻撃の情報から3つの脆弱性を組み合わせて攻撃が成功すること、及び攻撃者がWebShellを使った場合のリスクの両方をあわせて評価すべきです。

このように複数の脆弱性を組み合わせてサイバー攻撃が成功する場合もあるため、セキュリティ関連企業やセキュリティ専門家の解説記事からも情報収集を行って、脆弱性のリスク評価を行ってください。そして、すぐに更新プログラムを適用してください。

5.2. ランサムウェアの被害事例

2021年度第2四半期に起きたランサムウェアのインシデントをいくつかピックアップして、表 8に示します。

表 8：2021年度第2四半期におけるランサムウェアの被害事例

No.	発生の日付	被害者	インシデントの概要
1	2021年7月2日※	Arthur J. Gallagher (AJG)	米国に本拠を置く世界的な保険仲介およびリスク管理会社である Arthur J.Gallagher（AJG）は、ランサムウェア攻撃を受けて、影響を受けるおそれのある個人に違反通知書を郵送した [75]
2	2021年7月7日	株式会社ニップン	同社子会社のニップンビジネスシステムが運用するネットワークで、サーバや端末が暗号化されたことによって、約9割のシステムで被害が発生した。システムの起動そのものが不可能となった。 [76]
3	2021年7月9日※	Kaseya	米IT企業 Kaseyaのソフトウェアがランサムウェア（身代金ウィルス）攻撃を受け、被害が世界規模で広がっている。同社は、影響は最大で1500社に及ぶと発表 [77]
4	2021年8月1日	イタリア・ラツィオ州	イタリアのラツィオ州の保健医療用ITシステムがサイバー攻撃を受けて、新型コロナウイルスワクチンの予防接種の新規予約ができない事態となった [78]
5	2021年8月11日※	アクセンチュア	アクセンチュア社のマーケティング情報がランサムウェア「LockBit」のリークサイトへ掲載された。 [79]
6	2021年8月13日	ビーウィズ株式会社	株式会社パソナグループの子会社であるビーウィズ株式会社は、不正アクセスで過去のアルバイト応募者の情報15,421名分および同社従業員9,375名分の情報が暗号化されたと発表した [80]
7	2021年8月19日	オリエンタルコンサルタンツ	業務関連データが暗号化され、情報が外部に流出したおそれがある。約7億5000万円の特別損失が計上された [81]
8	2021年8月30日	株式会社阿部長商店	株式会社阿部長商店は、社内ネットワークへの不正アクセスにより、サーバや端末等に保管していた業務関連データが外部へ流出したおそれがあると発表した [82]
9	2021年9月10日※	八神製作所	医療機器や福祉用具の販売を手がける八神製作所は、社内ネットワークがランサムウェア攻撃を受けた。社内ネットワークの接続に影響が出ていると発表した [83]
10	2021年9月19日	Crystal Valley	Crystal Valleyは、コンピューターシステムがランサムウェアに感染して会社の日常業務が大幅に中断された [84]

※ 記事の公開日

6 予測
従来のトレンドが継続 & ディープフェイクを警戒

EC-CUBEに関連するECサイトのインシデント公表の継続

2021年度第1四半期のレポートにて、EC-CUBEのクロスサイトスクリプティングの脆弱性を取り上げました [85]。EC-CUBEの脆弱性は、攻撃者に狙われやすいため、上記の記事で注意を促しました。2021年度第2四半期（2021年7月～9月）においても、表9のとおり、EC-CUBEを利用したECサイトでWebスキミングの被害が継続して発生している状況です。これは、第1四半期のレポートの推測と合致します。このことから、脆弱性を放置したままで改ざんに気づかないサイトが現状でも存在すると思います。そのため、しばらくEC-CUBEに関連するECサイトのインシデントの公表が継続すると予想します。

またEC-CUBEの脆弱性は、2021年5月と6月に7つ発見されたように、今後も、まだ新しい脆弱性が発見されるおそれがあります [85]。イーシーキューブ社の脆弱性の発表に注意してください。

表 8：2021年度第2四半期におけるEC-CUBEを利用したECサイトのインシデント事例 [86] [87] [88] [89] [90] [91] [92] [93] [94] [95] [96] [97] [98]

No.	公表日	ECサイト名	ECサイトの運営会社
1	2021/7/6	Hoick	株式会社ソングブックカフェ
2	2021/7/12	コスモスオンラインストア	株式会社コスモス薬品
3	2021/7/13	TRANSIC	TRANSIC株式会社
4	2021/7/14	よみファねっと	株式会社読売情報開発大阪
5	2021/7/20	ＥＣサイトプロショップ匠	株式会社キャンディルデザイン
6	2021/7/21	毎日元気公式ショッピングサイト	有限会社毎日元気
7	2021/7/26	KQLFT TOOLS	株式会社SONS-MARKET
8	2021/8/16	FUKUYAONLINE	株式会社フクヤ
9	2021/8/18	THE HAIR BAR TOKYO オンラインストア	ギャップインターナショナル株式会社
10	2021/8/23	コマキ楽器WEBサイト	株式会社コマキ楽器
11	2021/9/7	たち吉オンラインショップ	株式会社たち吉
12	2021/9/14	伊勢せきやオンラインショップ	株式会社関谷食品
13	2021/9/16	オムニECシステム	株式会社ジーアール

北京2022オリンピック・パラリンピック競技大会を狙ったサイバー攻撃

東京2020オリンピック・パラリンピック競技大会（以後、東京オリンピック・パラリンピック）を狙ったサイバー攻撃は、東京オリンピック・パラリンピック競技大会組織委員会等の主催組織本体だけでなく、システムの委託先等のサプライチェーンや東京オリンピック・パラリンピック観戦希望者等の周辺のステークホルダにも発生していました。2.1節では、周囲のステークホルダにもサイバー攻撃が発生した一因が新型コロナウイルスの流行と関連があること、世の中のサイバー攻撃の流行と関連があることを説明しました。

2022年の2月から、北京2022オリンピック・パラリンピック競技大会（以後、北京オリンピック・パラリンピック）を開催します。2.1節の内容を踏まえると、世界的な大規模イベントである北京オリンピック・パラリンピックでは、東京オリンピック・パラリンピックと同様に、周辺のステークホルダを狙ったフィッシング攻撃やサプライチェーン攻撃が行われると推測できます。まず、中国国内での新型コロナウイルスの感染状況は落ち着いてきており [99]、北京オリンピック・パラリンピックは有観客（中国本土在住者のみ）での開催になるようです [100]。しかし、世界各地でオミクロン株という変異種が流行し始めているため、今後中国国内で感染者が急増し、無観客開催に変更になるおそれがあります。よって北京オリンピック・パラリンピックでも偽中継サイトを用いたフィッシング攻撃が行われると予想します。続いて、東京オリンピック・パラリンピックから北京オリンピック・パラリンピックの開催時期まで期間が短いことから、サイバー攻撃の流行もほとんど変化がないでしょう。そのため、フィッシング攻撃やサプライチェーン攻撃といった、今の流行に沿ったサイバー攻撃が行われると推測できます。

ディープフェイクを悪用した攻撃

AIの技術の進歩やそれを活用したサービスが注目されていますが、今後はAIを活用した「ディープフェイク」が攻撃者の攻撃手口として悪用されることが懸念されます [101]。ディープフェイクとは、AIの深層学習（ディープラーニング）を使用して作成された偽の動画や音声で、2020年以降のサイバーセキュリティ業界において脅威として注目されています [102]。実際、英国を拠点とするエネルギー企業が、ディープフェイクを悪用した攻撃によって約2600万円を攻撃者に送金した事例が2019年に起きています。エネルギー会社のCEOが、上司にあたるドイツの親会社のCEOから電話で送金を頼まれたため実行したが、実はその電話はディープフェイクによって作成された音声であったことが判明しました [103]。

このような状況を踏まえ、セキュリティ対策のツールを既に開発して発表している企業があります。Microsoft社は動画や写真を分析し、人工的に作成されたものかを確立や信頼度のスコアで表してくれる「Microsoft Video Authenticator」を発表しました [104]。

今後、ディープフェイクの技術は更に向上するとされているため [104]、ツールを導入するだけではなく、偽りの情報であること見極めるための情報リテラシーもより必要とされると考えます。

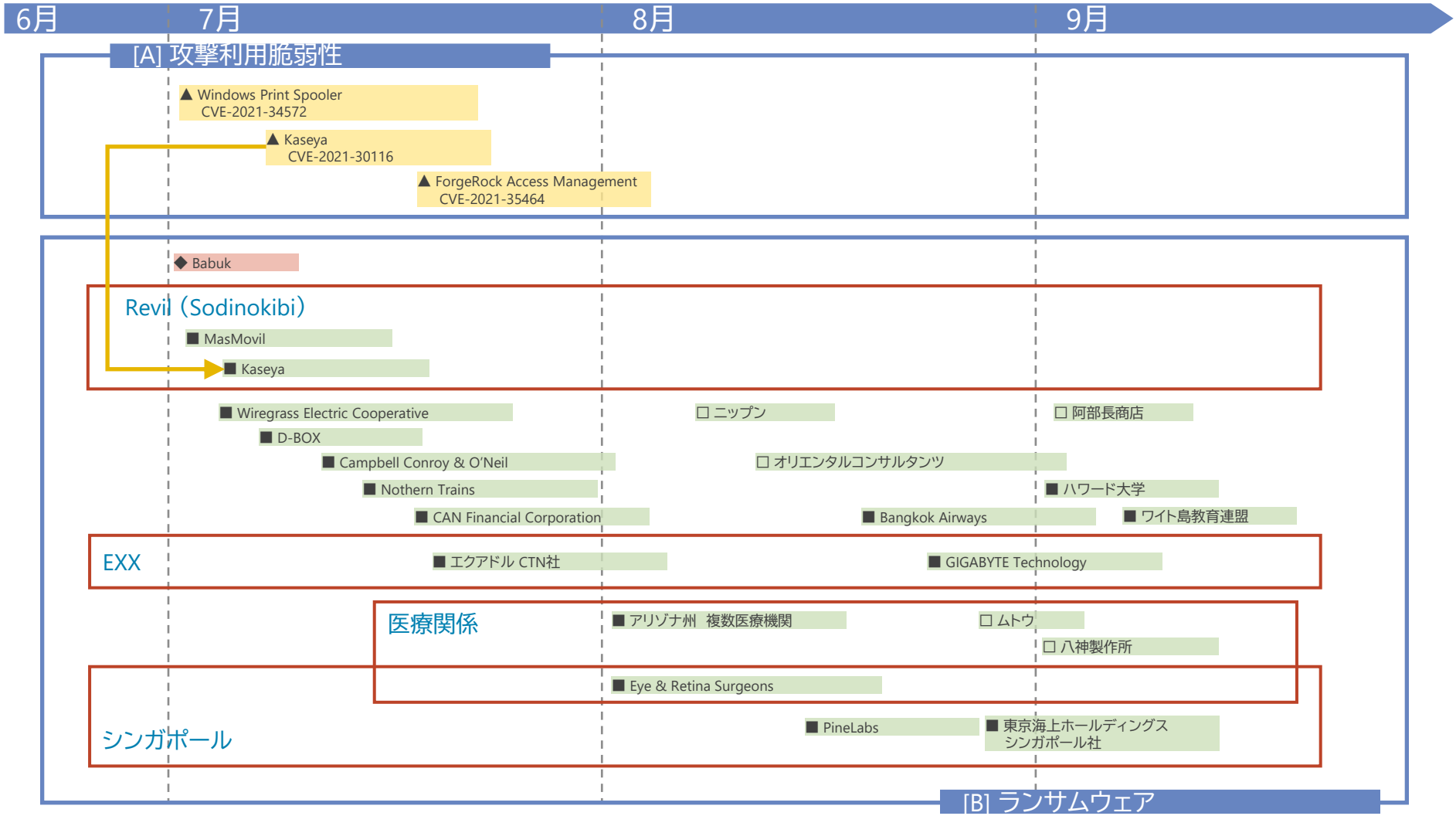
7 タイムライン
事象発生の時系列表

※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策

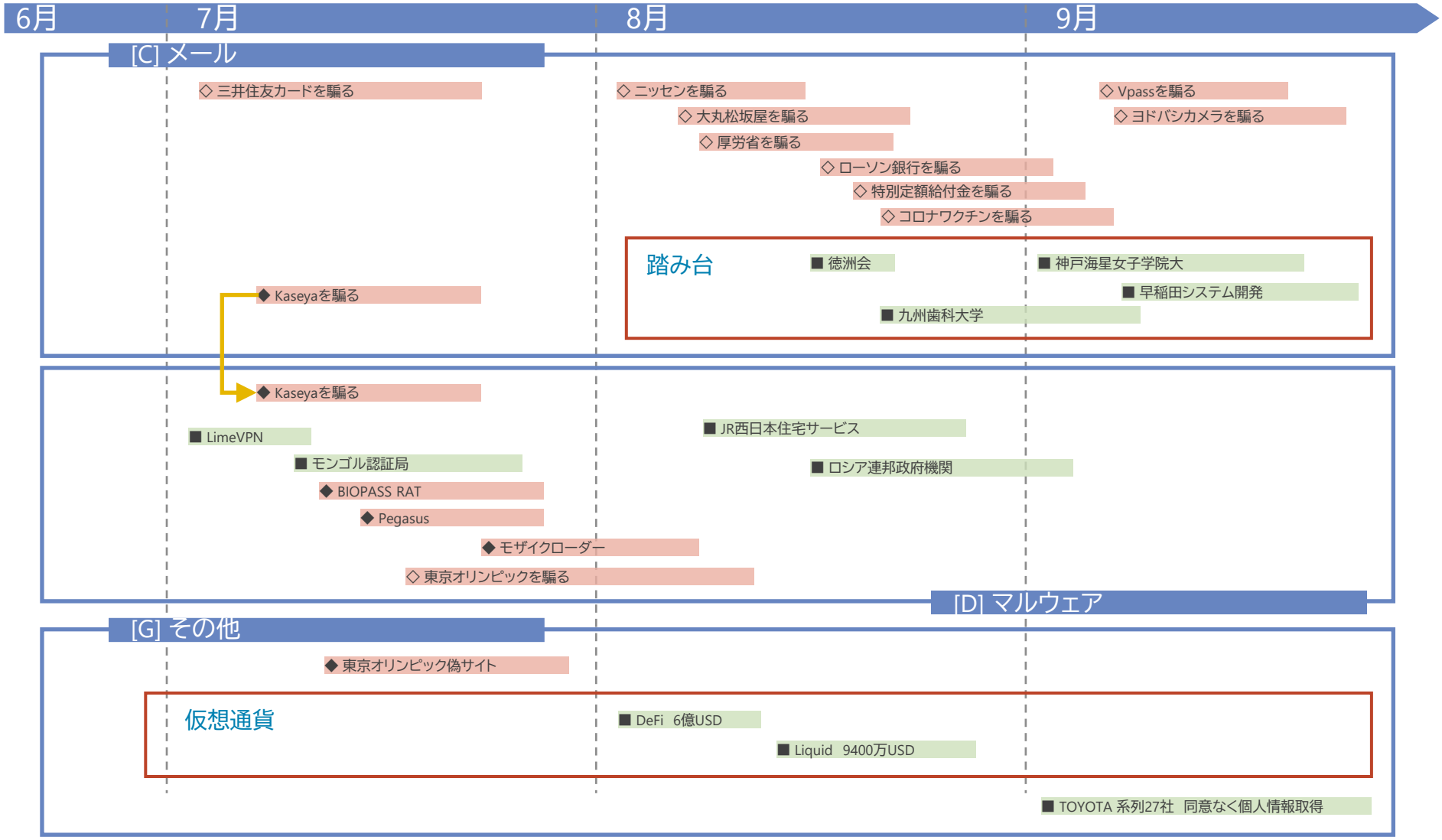


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策

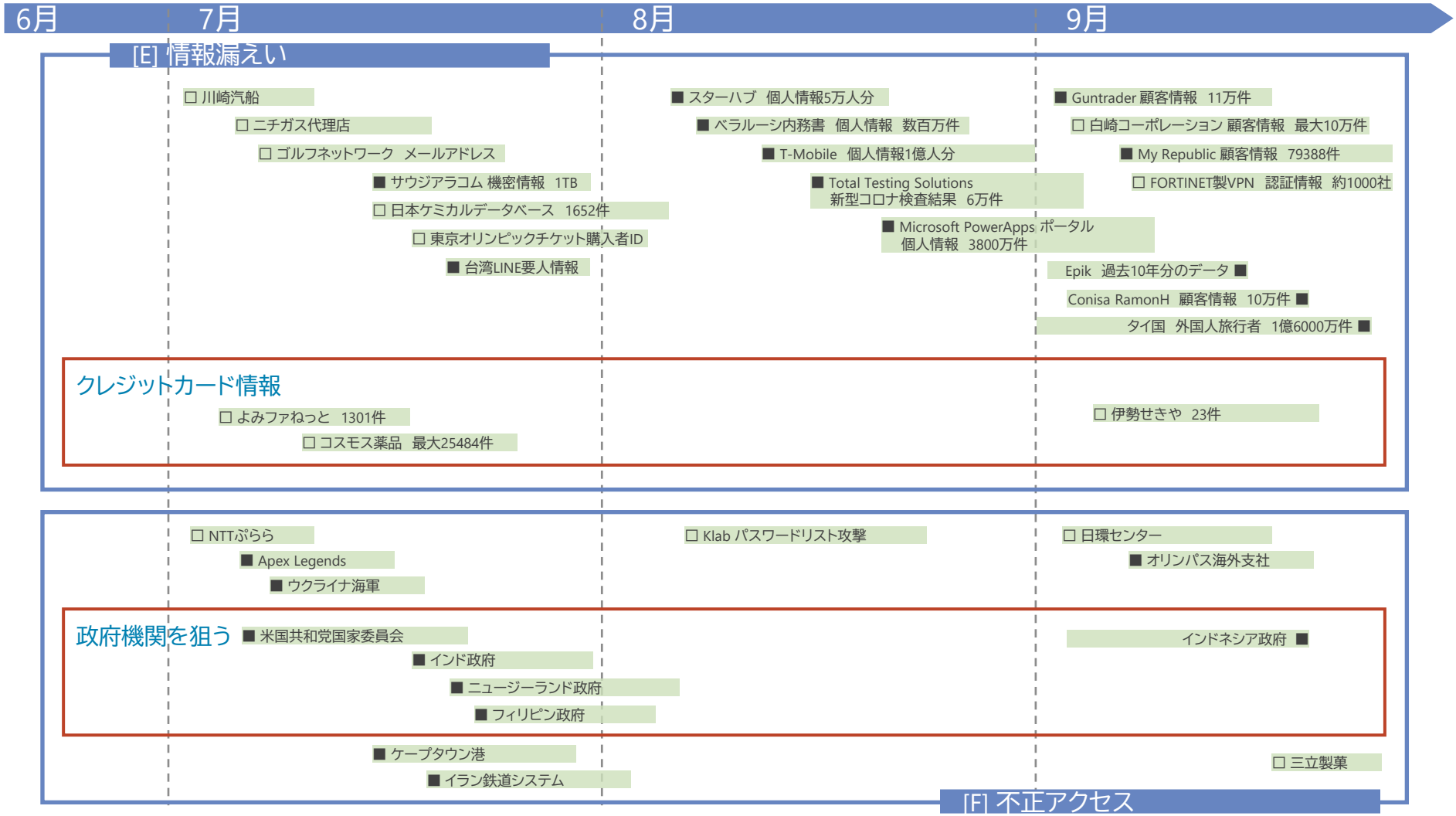


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策



参考文献

[1] 日本放送協会, “東京オリ・パラ期間 サイバー攻撃 4億5000万回 運営に影響なし,” 21 10 2021. [オンライン]. Available: https://www3.nhk.or.jp/news/html/20211021/k10013316541000.html.

[2] トレンドマイクロ株式会社, “【注意喚起】東京オリンピックへの支援を呼びかける偽の寄付メールに注意,” 30 4 2020. [オンライン]. Available: https://www.is702.jp/news/3675/.

[3] 株式会社朝日新聞社, “JOCにサイバー攻撃、全PC交換　金銭要求「ない」,” 25 6 2021. [オンライン]. Available: https://www.asahi.com/articles/ASP6S6V5TP6NULZU00B.html.

[4] 株式会社日本経済新聞社, “聖火リレーで偽サイト、警察が捜査　生中継うたう,” 15 5 2021. [オンライン]. Available: https://www.nikkei.com/article/DGXZQOUE149WN0U1A510C2000000/.

[5] トレンドマイクロ株式会社, “東京オリンピック開会直前、偽のTV放送予定ページからブラウザ通知スパムへ誘導する攻撃を確認,” 19 7 2021. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/28308.

[6] 株式会社日本経済新聞社, “五輪組織委の個人情報も流出　富士通の不正アクセス問題,” 4 6 2021. [オンライン]. Available: https://www.nikkei.com/article/DGXZQOUE04A290U1A600C2000000/.

[7] 株式会社カスペルスキー, “オリンピックに乗じたオンライン詐欺：5つのパターン,” 28 7 2021. [オンライン]. Available: https://blog.kaspersky.co.jp/olympic-scams-top-5-schemes/31272/.

[8] 独立行政法人 情報処理推進機構, “情報セキュリティ10大脅威 2021,” 27 1 2021. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/10threats2021.html.

[9] 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,” [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_2q_securityreport.pdf.

[10] Fortinet, Inc., “PSIRTと責任ある開示,” 20 8 2021. [オンライン]. Available: https://www.fortinet.com/jp/blog/psirt-blogs/psirt-and-the-responsible-disclosure.

[11] piyolog, “警察庁内端末不正アクセスと5万件の脆弱なVPNホストの公開についてまとめてみた,” 30 11 2020. [オンライン]. Available: https://piyolog.hatenadiary.jp/entry/2020/11/30/063636#f-6d9a455d.

[12] Fortinet, Inc., “悪意のあるアクターがFortiGate SSL-VPNの認証情報を公開,” 8 9 2021. [オンライン]. Available: https://www.fortinet.com/jp/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials.

[13] Fortinet, Inc., “特別に細工されたHTTPリソースリクエストによるSSL-VPNを介したFortiOSシステムファイルの漏えい,” 24 5 2019. [オンライン]. Available: https://www.fortiguard.com/psirt/FG-IR-18-384.

[14] JPCERT/CC, “複数の SSL VPN 製品の脆弱性に関する注意喚起,” 2 9 2019. [オンライン]. Available: https://www.jpcert.or.jp/at/2019/at190033.html.

[15] Fortinet, Inc., “SSL VPNの欠陥を標的としたATP 29,” 16 7 2020. [オンライン]. Available: https://www.fortinet.com/jp/blog/psirt-blogs/atp-29-targets-ssl-vpn-flaws.

[16] JPCERT/CC, “Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について,” 27 11 2020. [オンライン]. Available: https://www.jpcert.or.jp/newsflash/2020112701.html.

[17] Fortinet, Inc., “CVE-2018-13379 に関するアップデート,” 30 11 2020. [オンライン]. Available: https://www.fortinet.com/jp/blog/psirt-blogs/update-regarding-cve-2018-13379.

[18] 内閣サイバーセキュリティセンター, “Fortinet製VPNの脆弱性(CVE-2018-13379)に関する重要インフラ事業者等についての注意喚起の発出について,” 3 12 2020. [オンライン]. Available: https://www.nisc.go.jp/active/infra/pdf/fortinet20201203.pdf.

[19] Fortinet, Inc., “FireEye レッドチームツールの侵害,” 11 12 2020. [オンライン]. Available: https://www.fortinet.com/jp/blog/psirt-blogs/fireeye-red-team-tool-breach.

参考文献

[20] CISA/FBI, “FBI-CISA Joint Advisory on Exploitation of Fortinet FortiOS Vulnerabilities,” 2 4 2021. [オンライン]. Available: https://us-cert.cisa.gov/ncas/current-activity/2021/04/02/fbi-cisa-joint-advisory-exploitation-fortinet-fortios.

[21] Fortinet, Inc., “パッチと脆弱性の管理,” 3 4 2021. [オンライン]. Available: https://www.fortinet.com/jp/blog/psirt-blogs/patch-vulnerability-management.

[22] FBI, “MI-000148-MW,” 27 5 2021. [オンライン]. Available: https://www.ic3.gov/Media/News/2021/210527.pdf.

[23] Fortinet, Inc., “ネットワークの整合性を確保するには、パッチ適用を優先することが不可,” 1 6 2021. [オンライン]. Available: https://www.fortinet.com/jp/blog/psirt-blogs/prioritizing-patching-is-essential-for-network-integrity.

[24] SB C&S株式会社, “FortiGateでリモートアクセス設定　SSL-VPN編（初級者向け）,” 13 8 2020. [オンライン]. Available: https://licensecounter.jp/engineer-voice/blog/articles/20200813_fortigatesslvpn.html.

[25] ラクラウド株式会社, “SSL-VPNポータルを設定する,” [オンライン]. Available: https://www.teracloud.co.jp/manual_remotevpn_operationaldesign_portal.html.

[26] Tenable, Inc., “CVE-2018-13379、CVE-2019-11510： FortiGateおよびPulse Connect Secureの脆弱性を突いた攻撃が確認される,” 2019. [オンライン]. Available: https://jp.tenable.com/blog/cve-2018-13379-cve-2019-11510-fortigate-and-pulse-connect-secure-vulnerabilities-exploited-in.

[27] トレンドマイクロ株式会社, “ランサムウェア「Cring」の被害が国内で拡大、VPN脆弱性を狙い侵入,” 20 5 2021. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/27830.

[28] ncsc, “Advisory:APT29 targets COVID-19 vaccine development,” 2020. [オンライン]. Available: https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf.

[29] 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,” [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_4q_securityreport.pdf.

[30] 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 2020年度第1四半期,” [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2020/091101/091101-01.pdf.

[31] レムシステム株式会社, “Fortigateのファームウェアをv4.0からv5.0へアップグレードする手順,” [オンライン]. Available: https://www.rem-system.com/fortigate-firm-versionup/.

[32] Fortinet, Inc., “Upgrade Path Tool Table,” [オンライン]. Available: https://docs.fortinet.com/upgrade-tool.

[33] 日本経済新聞, “サイバー攻撃、「関門」が入り口に放置される欠陥,” 10 12 2020. [オンライン]. Available: https://www.nikkei.com/article/DGXZQODG080Z40Y0A201C2000000/.

[34] 警察庁, “図表7-1　警察職員の定員（令和2年（2020年）度）,” [オンライン]. Available: https://www.npa.go.jp/hakusyo/r02/honbun/html/w7711000.html.

[35] 株式会社日経BP, “VPNのパスワードが外部流出　脆弱性の注意喚起に気づかず,” 5 1 2021. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/mag/nc/18/020600011/122400071/.

[36] 株式会社マイナビ, “岐阜県庁,” [オンライン]. Available: https://job.mynavi.jp/23/pc/search/corp93217/outline.html.

[37] 佐賀県伊万里市役所, “等級及び職制上の段階ごとの職員数（令和3年4月1日現在）について,” [オンライン]. Available: https://www.city.imari.saga.jp/18291.htm.

[38] 愛知県東郷町役場, “12月1日の中日新聞報道について（続報）,” [オンライン]. Available: https://www.town.aichi-togo.lg.jp/kikaku/joho/chousei/jouhouseisaku/20201201cyber.html.

参考文献

[39] 愛知県東郷町役場, “等級及び職制上の段階ごとの職員数（令和３年４月１日現在）（その１）,” 1 4 2021. [オンライン]. Available: https://www.town.aichi-togo.lg.jp/jinji/jinji/chousei/jinji/jinjigyousei/documents/r3syokuinsuusono1.pdf.

[40] 一般社団法人共同通信社, “600超の組織にサイバー攻撃,” 1 12 2020. [オンライン]. Available: https://nordot.app/706248789438039137?c=39546741839462401.

[41] 日本政府観光局, “常勤職員は令和 2 年度末,” [オンライン]. Available: https://www.jnto.go.jp/jpn/about_us/reports/f_jigyou_r2.pdf.

[42] 株式会社リクルート, “会社概要,” [オンライン]. Available: https://www.recruit.co.jp/company/profile/.

[43] 日新製糖株式会社, “当社の社内システムに対しての不正アクセスについて（続報）,” 25 12 2020. [オンライン]. Available: https://www.nissin-sugar.co.jp/cms/wp-content/uploads/2020/12/201225.pdf.

[44] 日新製糖株式会社, “会社概要,” [オンライン]. Available: https://www.nissin-sugar.co.jp/company/outline/.

[45] 株式会社ディーカレット, 1 12 2020. [オンライン]. Available: https://news.decurret.com/hc/ja/articles/360060170213.

[46] パーソルキャリア株式会社, “株式会社ディーカレットの求人・中途採用・転職情報,” [オンライン]. Available: https://doda.jp/DodaFront/View/Company/j_id__10185053863/.

[47] 慶應義塾大学, “情報公開,” [オンライン]. Available: https://www.keio.ac.jp/ja/about/learn-more/data/.

[48] 札幌大学, “VPN(仮想私設網)へサイバー攻撃に関する報道について(第2報),” 4 12 2020. [オンライン]. Available: https://www.sapporo-u.ac.jp/news/su-news/2020/12043139.html.

[49] 札幌大学, “◆教員数/教員一人当たり学生数/年齢別教員数,” [オンライン]. Available: https://www.sapporo-u.ac.jp/img/2021_kyoinsuu.pdf.

[50] 福井工業大学, “VPN(仮想私設網)へのサイバー攻撃について,” 4 12 2020. [オンライン]. Available: http://www.fukui-ut.ac.jp/news/topics/entry-6566.html.

[51] 福井工業大学, “教職員情報,” [オンライン]. Available: http://www.fukui-ut.ac.jp/ut/introduction/public/teacher/.

[52] 株式会社ケアレビュー, “一宮市立市民病院,” [オンライン]. Available: https://hospia.jp/hosinfo/1232200369.

[53] 経済産業省, “サイバーセキュリティ経営ガイドライン Ver 2.0,” [オンライン]. Available: https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf.

[54] The Citizen Lab - University of Toronto, “From Pearl to Pegasus Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits,” 24 8 2021. [オンライン]. Available: https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/.

[55] The Citizen Lab - University of Toronto, “The Great iPwn Journalists Hacked with Suspected NSO Group iMessage ‘Zero-Click’ Exploit,” 20 12 2020. [オンライン]. Available: https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/.

[56] Project Zero, “A Look at iMessage in iOS 14,” 28 1 2021. [オンライン]. Available: https://googleprojectzero.blogspot.com/2021/01/a-look-at-imessage-in-ios-14.html.

[57] The Citizen Lab - University of Toronto, “FORCEDENTRY NSO Group iMessage Zero-Click Exploit Captured in the Wild,” 13 9 2021. [オンライン]. Available: https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/.

[58] トレンドマイクロ社, “スパイウェア「Pegasus」の攻撃で悪用されたiPhoneのゼロクリックエクスプロイト「ForcedEntry」を解説,” 27 9 2021. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/28782.

参考文献

[59] O. Tsai, “ProxyLogon is Just the Tip of the Iceberg. A New Attack Surface on Microsoft Exchange Server!,” 2021. [オンライン]. Available: https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-ProxyLogon-Is-Just-The-Tip-Of-The-Iceberg-A-New-Attack-Surface-On-Microsoft-Exchange-Server.pdf.

[60] SHODAN, “Shodan report,” 7 11 2021. [オンライン]. Available: https://www.shodan.io/search/report?query=http.title%3Aoutlook+exchange.

[61] Microsoft, “Microsoft Exchange Server のセキュリティ機能のバイパスの脆弱性,” 13 7 2021. [オンライン]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31207.

[62] Microsoft, “Microsoft Exchange Server のリモートでコードが実行される脆弱性,” 13 7 2021. [オンライン]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473.

[63] Microsoft, “Microsoft Exchange Server の特権の昇格の脆弱性,” 13 7 2021. [オンライン]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523.

[64] Tenable, “ProxyShell: Attackers Actively Scanning for Vulnerable Microsoft Exchange Servers (CVE-2021-34473),” 9 8 2021. [オンライン]. Available: https://www.tenable.com/blog/proxyshell-attackers-actively-scanning-for-vulnerable-microsoft-exchange-servers-cve-2021-34473.

[65] BROADCOM SOFTWARE (Symatec Enterprise Blogs), “LockFile: Ransomware Uses PetitPotam Exploit to Compromise Windows Domain Controllers,” 21 8 2021. [オンライン]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lockfile-ransomware-new-petitpotam-windows.

[66] ZERO DAY INITIATIVE, “FROM PWN2OWN 2021: A NEW ATTACK SURFACE ON MICROSOFT EXCHANGE - PROXYSHELL!,” 18 8 2021. [オンライン]. Available: https://www.zerodayinitiative.com/blog/2021/8/17/from-pwn2own-2021-a-new-attack-surface-on-microsoft-exchange-proxyshell.

[67] IT Media エンタープライズ, “Webシェル攻撃とはどんなものか　Microsoft 365 Defenderが月間14万件も検出する脅威,” 15 2 2021. [オンライン]. Available: https://www.itmedia.co.jp/enterprise/articles/2102/15/news130.html.

[68] 株式会社ソフテック, “Microsoft Exchange Server の脆弱性「ProxyShell」とは,” 6 9 2021. [オンライン]. Available: https://www.softek.co.jp/SID/blog/archive/entry/20210902.html.

[69] CertNZ, “Active scanning for Microsoft Exchange Proxyshell vulnerability,” 8 8 2021. [オンライン]. Available: https://www.cert.govt.nz/it-specialists/advisories/active-scanning-for-microsoft-exchange-proxyshell-vulnerability/.

[70] SecurityNext, “「Exchange」の脆弱性「ProxyShell」に要警戒 - 悪用発生で米政府が注意喚起,” 24 8 2021. [オンライン]. Available: https://www.security-next.com/129248/2.

[71] Canon, “エクスプロイトって何ですか？普通のマルウェア攻撃と何が違うのでしょうか？,” 10 9 2015. [オンライン]. Available: https://eset-info.canon-its.jp/malware_info/qa/detail/150910_1.html.

[72] Microsoft, “クライアント アクセス サービス,” 16 9 2021. [オンライン]. Available: https://docs.microsoft.com/ja-jp/exchange/architecture/client-access/client-access?view=exchserver-2019.

[73] 株式会社ソフィス, “ProxyShell vulnerabilities in Microsoft Exchange: What to do,” 23 8 2021. [オンライン]. Available: https://news.sophos.com/en-us/2021/08/23/proxyshell-vulnerabilities-in-microsoft-exchange-what-to-do/.

[74] Huntress, “Microsoft Exchange Server Still Vulnerable to ProxyShell Exploit,” 19 8 2021. [オンライン]. Available: https://www.huntress.com/blog/rapid-response-microsoft-exchange-servers-still-vulnerable-to-proxyshell-exploit.

[75] BLEEPING COMPUTER, “US insurance giant AJG reports data breach after ransomware attack,” 2 7 2021. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/us-insurance-giant-ajg-reports-data-breach-after-ransomware-attack/.

参考文献

[76] ScanNetSecurity, “ニップンへのサイバー攻撃、グループ会社を含む基幹システムやデータサーバも暗号化被害に,” 19 8 2021. [オンライン]. Available: https://scan.netsecurity.ne.jp/article/2021/08/19/46145.html.

[77] 朝日新聞 Digital, “米IT企業にサイバー攻撃　世界1500社に影響拡大か,” 9 7 2021. [オンライン]. Available: https://www.asahi.com/articles/ASP785DG0P78UHBI00F.html.

[78] GIGAZINE, “ワクチン予約システムがランサムウェア攻撃でダウン、被害を受けたイタリアの州知事は「テロリスト」とハッカーを非難,” 1 8 2021. [オンライン]. Available: https://gigazine.net/news/20210803-italys-lazio-hacker-vaccine-booking-website/.

[79] ZD Net, “Accenture says Lockbit ransomware attack caused 'no impact',” 11 8 2021. [オンライン]. Available: https://www.zdnet.com/article/accenture-says-lockbit-ransomware-attack-caused-no-impact-on-operations-or-clients/#ftag=RSSbaffb68.

[80] Scan Net Security, “パソナグループの子会社にランサムウェア攻撃、求人情報や従業員情報が被害に,” 13 8 2021. [オンライン]. Available: https://scan.netsecurity.ne.jp/article/2021/08/19/46146.html.

[81] IT Media NEWS, “ランサムウェア攻撃で7億円超の特別損失、建設コンサル大手のオリエンタルコンサルタンツが発表,” 17 9 2021. [オンライン]. Available: https://www.itmedia.co.jp/news/articles/2109/17/news149.html.

[82] Scan Net Security, “阿部長商店へランサムウェア攻撃、業務関連データや個人情報が暗号化,” 30 8 2021. [オンライン]. Available: https://scan.netsecurity.ne.jp/article/2021/09/08/46258.html.

[83] Security NEXT, “医療機器販売の八神製作所、サーバがランサム被害,” 10 9 2021. [オンライン]. Available: https://www.security-next.com/129574.

[84] DataBreaches.net, “Crystal Valley Computer Systems Infected By Ransomware Attack,” 19 9 2021. [オンライン]. Available: https://www.databreaches.net/mn-crystal-valley-computer-systems-infected-by-ransomware-attack/.

[85] 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 2021 年度第 1 四半期,” 2 11 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2021_1q_securityreport.pdf.

[86] ニュースガイア株式会社, “保育関係者向けサイトに不正アクセス - クレカやアカウント情報が流出,” 6 7 2021. [オンライン]. Available: https://www.security-next.com/127865.

[87] 株式会社コスモス薬品, “弊社が運営する「コスモスオンラインストア」への不正アクセスによるお客様情報流出に関するお詫びとお知らせ,” 12 7 2021. [オンライン]. Available: https://www.cosmospc.co.jp/notice/upload/ed661581b067c469eb29047679fa8a86e6446fe7.pdf.

[88] ニュースガイア株式会社, “革製品通販サイトに不正アクセス - クレカ情報流出の可能性,” 13 7 2021. [オンライン]. Available: https://www.security-next.com/128099.

[89] ニュースガイア株式会社, “読売関連会社のネットショップに不正アクセス - クレカ情報が被害,” ニュースガイア株式会社, 14 7 2021. [オンライン]. Available: https://www.security-next.com/128114.

[90] 株式会社キャンディル, “当社子会社が運営するオンラインショップへの不正アクセスによる個人情報漏洩に関するお詫びとお知らせ,” 20 7 2021. [オンライン]. Available: http://fs.magicalir.net/tdnet/2021/1446/20210719469018.pdf.

[91] 有限会社毎日元気 , “弊社が運営する「毎日元気公式ショッピングサイト」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,” 21 7 2021. [オンライン]. Available: https://www.mainichigenki.co.jp/210721.pdf.

[92] 株式会社 SONS-MARKET, “弊社が運営する「KQLFT TOOLS」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,” 26 7 2021. [オンライン]. Available: https://kqlft.com/card.pdf.

参考文献

[93] 株式会社フクヤ, “弊社が運営するオンラインショップへの不正アクセスによる 個人情報流出に関するお詫びとご報告,” 株式会社フクヤ, 16 8 2021. [オンライン]. Available: https://www.fancy-fukuya.co.jp/topics/news20210816/.

[94] ギャップインターナショナル株式会社, “クレジットカード情報流出に関するお詫びとお知らせ,” ギャップインターナショナル株式会社, 18 8 2021. [オンライン]. Available: https://thehairbar.jp/blogs/news/information001.

[95] 株式会社コマキ楽器, “弊社が運営する「コマキ楽器WEBサイト」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,” 株式会社コマキ楽器, 23 8 2021. [オンライン]. Available: https://komakimusic.co.jp/pages/important-notices.

[96] 株式会社たち吉, “お詫びとお知らせ　「たち吉オンラインショップ」への不正アクセスによる個人情報漏えいについて,” 株式会社たち吉, 7 9 2021. [オンライン]. Available: https://www.tachikichi.co.jp/2021/09/07/%e3%81%8a%e8%a9%ab%e3%81%b3%e3%81%a8%e3%81%8a%e7%9f%a5%e3%82%89%e3%81%9b/.

[97] 株式会社関谷食品, “弊社が運営する「伊勢せきやオンラインショップ」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,” 株式会社関谷食品, 14 9 2021. [オンライン]. Available: https://www.sekiya.com/notice/.

[98] 東芝テック株式会社, “株式会社ジーアールが運営する「オムニＥＣ」への不正アクセスについて,” 東芝テック株式会社, 16 9 2021. [オンライン]. Available: https://www.toshibatec.co.jp/information/20210916_01.html.

[99] ヤフー株式会社, “中国国内、新型コロナ新規感染者「2人のみ」…感染状況落ち着きを見せる＝中国報道,” 25 11 2021. [オンライン]. Available: https://news.yahoo.co.jp/articles/980d2096cc9d2da53b075b994c26982605c7592c.

[100] 株式会社日刊スポーツ新聞社, “北京五輪、観客上限は未定　新型コロナの影響で,” 10 11 2021. [オンライン]. Available: https://www.nikkansports.com/sports/news/202111100000113.html.

[101] TREND MICRO, “「ディープフェイク」による詐欺やサプライチェーン攻撃に警戒：2020年の脅威動向を予測,” 10 12 2019. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/23044.

[102] NECソリューションイノベータ, “ディープフェイク　「機械学習の活用により今後懸念される攻撃手法の一つ」,” 不明. [オンライン]. Available: https://www.nec-solutioninnovators.co.jp/ss/insider/security-words/33.html.

[103] ZDNet Japan, “CEOになりすましたディープフェイクの音声で約2600万円の詐欺被害か,” 5 9 2019. [オンライン]. Available: https://japan.zdnet.com/article/35142255/.

[104] Microsoft, “虚偽情報対策に向けた新たな取り組みについて,” 7 9 2020. [オンライン]. Available: https://news.microsoft.com/ja-jp/2020/09/07/200907-disinformation-deepfakes-newsguard-video-authenticator/.

グローバルセキュリティ動向四半期レポート

2021年度 第2四半期

2022年1月18日発行

株式会社NTTデータ
セキュリティ技術部
大谷 尚通 / 大山 千尋 / 宮崎 大輔 / 工藤 完太郎
太田 悠介 / 江崎 柚希 / 長田 健司
nttdata-cert@kits.nttdata.co.jp