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 2 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。

決済サービスに必要なセキュリティ

情報処理推進機構が発表した「情報セキュリティ10大脅威 2020」で、個人向けの脅威1位に「スマホ決済の不正利用」が今回初めてランクインしました。2020年度第2四半期にはSBI証券やNTTドコモで大規模なサービスの不正利用が発生しています。各社はそれぞれ、複数の対策を実施すると発表していますが、共通するのが「本人確認」の強化です。本記事では、経済産業省による「本人確認」の定義に基づき、一般的な決済サービスが持つ「アカウント登録」や「銀行口座登録」「支払い」といった各機能について、本人確認という観点でどのようなセキュリティ対策を実装すべきかを解説します。

Zerologon（CVE-2020-1472）

Zerologonは、Active Directoryで利用される認証プロトコルをWindows上に実装した際の脆弱性です。攻撃者は、脆弱性を悪用して不正に認証を突破することで、ドメインコントローラの管理者権限を奪取し、ドメインに参加しているすべてのデバイスを乗っ取り、機密情報を窃取したり、マルウェアを感染させたりすることが可能になります。Microsoft社は、この脆弱性に対して2段階の対策を計画しています。本記事では、脆弱性の概要、段階ごとに実施すべき設定変更や監視すべきログについて解説します。

Emotetの再流行とランサムウェア被害の深刻化

Emotetが再び大流行しており、2020年9月には前回ピーク時の5.7倍以上の感染が発生しました。感染拡大の一因は、Emotetがマルウェアを含んだ不審なWordファイルをパスワード付きzipファイルにして、メールへ添付して送付する新しい攻撃手法を使ったためです。セキュリティ製品は、パスワード付きzipファイルの中身をウイルス検査できません。マルウェアを含んだzipファイルを添付されたメールは、駆除されずにユーザへ配信されます。パスワード付きzipファイルの使用は、Emotetに悪用されるだけでなく、情報漏えい対策として不十分なため、利用をやめることが有効です。

また、ランサムウェアによる被害も深刻化しています。ランサムウェアにより、病院の医療システムが麻痺して、初めて人命が失われるという悲劇や、GPSサービスに障害が発生して、世界規模での混乱が起こりました。ランサムウェアは感染した段階でシステムの停止に

つながるおそれが高いため、EDR等を活用して、可能な限り未然に感染を防止できる対策を実施することが重要です。

予測

身元を隠したままSMS認証を不正に突破してSNSやクラウドサービスのアカウントが作成できるSMS認証代行というサービスがあります。これをつかうとSMS認証を不正に突破することが簡単なため、格安SIMとSMS認証代行サービスを組み合わせて、不正行為をおこなうケースがもっと増加すると考えられます。オンライン上の手続きだけでアカウントの新規登録が可能なサービスを提供する事業者は、スマートフォンのSMS認証などのオンライン上の「認証」だけでは本人確認と当人認証を分離して、身元をごまかせることを再認識しましょう。身元をごまかしたユーザの利用が問題になるサービスの場合は、eKYCなどの本人確認を行える方式を採用していくことが必要です。また、サプライチェーン攻撃に対して多くの組織で対策を実施できていないことや、サプライチェーンでつながった各組織がテレワークに移行して、攻撃者が狙いやすい箇所が増加したことがわかりました。よって、引き続きサプライチェーンを狙った攻撃が発生すると想定されます。サプライチェーンマネジメントに関するガイドラインやフレームワークの活用、サプライチェーンリスクを評価するサービスを利用した対策をお薦めします。

最後に、コロナウイルスワクチンの接種が始まるタイミングで、ワクチンをテーマにしたフィッシング等の攻撃が発生すると想定されます。それ以外にも、労働様式がテレワークに移行したことで、通常のビジネス活動においても、オンライン上で初めてやりとりする人の本人確認と当人認証を行わなければならなくなってきましたこのオンライン上でのコミュニケーションによる本人確認行為の隙を狙った詐欺やサイバー攻撃が増えると予測します。

2. 注目トピック

2.1. 決済サービスに必要なセキュリティ

2020年8月25日、情報処理推進機構が「情報セキュリティ10大脅威 2020」を公開しました [1]。この「10大脅威」は、前年に発生した情報セキュリティを脅かすさまざまな出来事をもとに、100名を超える研究者や企業の実務担当者によって審議、決定されます。社会全体としての重要度が高いと考えられる順に、対個人と対組織についてそれぞれ10の脅威がランキング形式で示され、トレンドの理解だけではなく対策の優先度付け等の参考にすることができます。2020年版の個人に対する脅威は以下のようになっています。

表 1:「情報セキュリティ10大脅威 2020」で発表された個人に対する脅威

順位	昨年順位	昨年順位との比較	脅威
1	—	NEW	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の詐取
3	1	↓	クレジットカード情報の不正利用
4	7	↑	インターネットバンキングの不正利用
5	4	↓	メールやSMS等を使った脅迫・詐欺の手口による金銭要求
6	3	↑	不正アプリによるスマートフォン利用者への被害
7	5	↓	ネット上の誹謗・中傷・デマ
8	8	→	インターネット上のサービスへの不正ログイン
9	6	↓	偽警告によるインターネット詐欺
10	12	↑	インターネット上のサービスからの個人情報の窃取

「スマホ決済の不正利用」は今回初めて10大脅威に選ばれ、かつ最も社会的重要度の高い脅威と判断されました。ランキング上位の「スマホ決済の不正利用（1位）」「クレジットカード情報の不正利用（3位）」「インターネットバンキングの不正利用（4位）」はいずれも直接金銭を狙った脅威です。2位の「フィッシングによる個人情報の詐取」は、本人になりすましてスマホ決済やクレジットカード、インターネットバンキングを不正に利用するための事前準備であり、こちらも金銭を狙った脅威であると言えます。昨今、国内外問わずこれらの脅威に起因するさまざまなインシデントが発生していることから、本レポートでは「決済・金融関連サービス」に必要なセキュリティについて考えます。

2.1.1. 決済・金融関連サービスの不正利用

決済・金融関連サービスに必要なセキュリティを考えるために、まず2020年第2四半期に発生した決済・金融関連サービスの不正利用の例を2つ紹介します。

① 証券口座への不正アクセスで顧客の資産9,000万円以上が流出（株式会社SBI証券）

この事案は、SBI証券に口座を持つ顧客から「身に覚えのない取引があった」と問い合わせがあったことを発端に、複数件の不正アクセス・不正出金が行われていたことが判明したものです。SBI証券からの発表 [2]をもとに、攻撃の流れを示します。

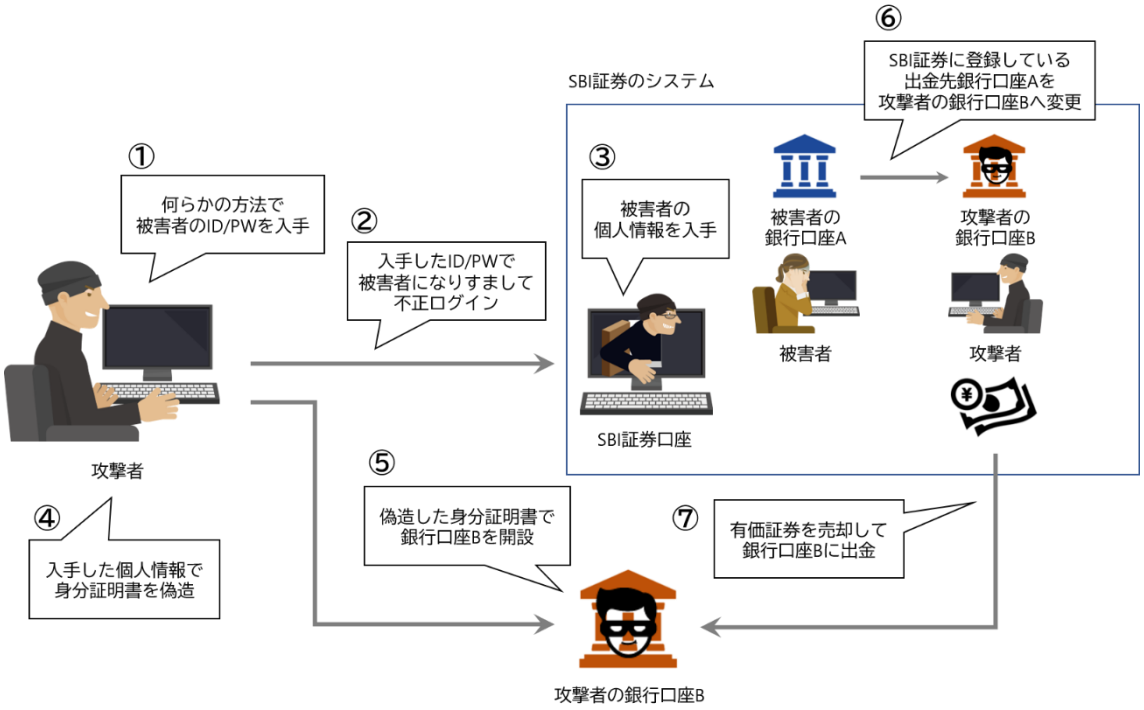


図 1：SBI証券での不正アクセスの流れ

攻撃者は、何らかの方法で入手（①）したSBI証券の顧客のユーザネーム（図では"ID"と表記）とログインパスワード（図では"PW"と表記）でお客様サイトへ不正ログインし（②）、その顧客（被害者）の個人情報を取得します（③）。攻撃者は、この個人情報を用いて被害者の身分証明書を偽造し（④）、被害者名義の別の銀行口座（B）を開設します（⑤）。その後、SBI証券のマイページ上で出金先の銀行口座AをBに変更します（⑥）。そして攻撃者は被害者の有価証券を売却し、売却金を銀行口座Bへ出金していました（⑦）。この不正利用による被害額は6口座で9,864万円にのぼっていますが、SBI証券によって全額補償すると発表されています。

SBI証券では、出金先に本人名義の銀行口座しか指定できないようにしていましたが、出金先の銀行口座を変更する際の本人確認手続きが不十分で、攻撃者が出金先を被害者のものではない銀行口座へ変更できたために、今回の不正利用が発生してしまいました。このインシデントを受けてSBI証券は、出金先の銀行口座の変更手続を、本人への郵送による手続きへ変更しました。この対策とともに、不正アクセスに対する監視体制やログイン認証、本人確認、銀行との連携を強化すると発表しています。

② 電子決済サービス経由で預貯金2,000万円以上が不正引き出し（株式会社NTTドコモ）

2020年9月以降、「ドコモコウザ」という名義で預貯金が引き出されているというSNS上の複数の書き込みから、不正利用の実態が明るみに出ました。ドコモ口座は、メールアドレスだけで登録が可能な「dアカウント」を持っていれば、誰でも開設できるバーチャルウォレットで、チャージしたお金をインターネット上での支払いに利用したり、ユーザ同士で送金したりできるシステムです [3]。ドコモ口座の不正利用は、2019年5月にも今回と同様の手口で起きていたことが分かっています [4]。図 2で、不正利用の流れを説明します。

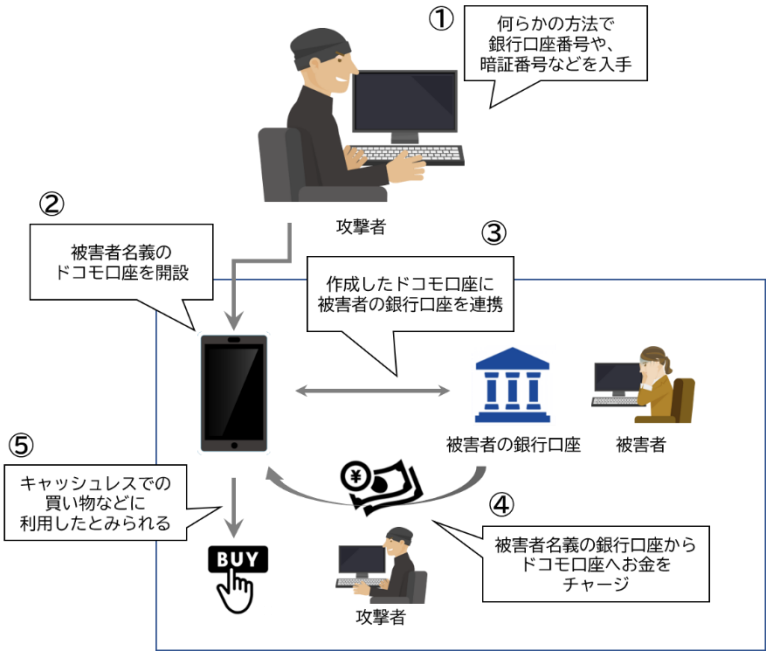


図 2：ドコモ口座の不正利用の流れ

攻撃者は、何らかの方法で銀行口座の名義と口座番号、キャッシュカードの暗証番号を入手し（①）、同じ名義でドコモ口座を開設します（②）。ドコモ口座と銀行口座を連携し（③）、入手したキャッシュカードの暗証番号を使って銀行口座からドコモ口座へ不正に現金をチャージする（④）ことで、被害者の預貯金を不正に取得する仕組みです。

最終的に攻撃者は、ドコモ口座で使用できるキャッシュレス決済である「d払い」を被害者名義で使用していたと見られており、10月28日時点でこの不正利用による被害額は128件、2,885万円にのぼっています。これらは、すべて補償済みであると発表されています [5]。一連の事態を受けてNTTドコモは、ドコモ口座における銀行口座の新規登録を当面停止しています。ドコモ口座はドコモ回線契約者以外のユーザの獲得を狙う目的もあり、メールアドレスだけあれば開設できる状態であったことで、悪意のある攻撃者による不正利用ができてしまう作りになっていました。今後は、SMS認証やユーザが撮影した自分の写真と身分証明書の画像をアップロードさせて本人確認を行う等の対策を講じると発表しています [6]。

上記の2つの事案について、各社が発表した対策を表 2にまとめます。

表 2：SBI証券とNTTドコモが発表した対策

	発表された主な対策 [2] [6]
SBI証券	1. 監視 ✓ 不正アクセスに対するモニタリング体制の強化、WAF[*1]の導入 ✓ IPレピュテーションサービス[*2]の一層の活用 2. 認証 ✓ OTP[*3]による2要素認証[*4]、リスクベース認証[*5]の導入 ✓ アクセス許可する端末を限定する機能の導入 3. 本人確認 ✓ 出金先銀行口座登録時の**本人確認**の強化 （出金先銀行口座変更は詳細な**本人確認**ができる郵送でのみ受付ける） 4. その他 ✓ 出金先銀行との連携強化 ✓ ダイナミックセキュリティ技術[*6]の導入
NTTドコモ	1. 認証 ✓ SMSによる2段階認証の導入 2. 本人確認 ✓ eKYC[*7]による**本人確認**の確実な実施

*1 WAF

Web Application Firewall。Webサーバの前段階に設置し、Webアプリケーションの脆弱性を悪用した攻撃からWebサイトを保護するセキュリティ対策 [7]

*2 IPレピュテーションサービス

不審なIPアドレスからの通信を遮断するサービス

*3 OTP

One Time Password。一定時間で自動更新される使い捨てのパスワード

*4 2要素認証
指紋や虹彩といった「生体情報」、パスワードや秘密の質問といった「知識情報」、マイナンバーカードやOTPトークンといった「所持情報」の認証の3要素のうち、2つを使って行う認証方式
*5 リスクベース認証
なりすましや不正ログインを防ぐために、通常時と異なる認証行為が発生した場合に追加の要素による認証を要求する方法 [8]
*6 ダイナミックセキュリティ技術
アプリケーション実行時に、制限時間付きのセキュリティモジュールのプログラム配置しておき、制限時間を過ぎるとそのプログラムが廃棄され、新しいモジュールが生成されるという、EverSpin社独自のアプリケーション監視技術 [9]
*7 eKYC
electronic Know Your Customer。本人確認の手続きをオンライン上で完結させる仕組み

2社の事例からも分かる通り、決済・金融関連サービスの不正利用対策として「本人確認」というキーワードがよく使われます。特に手続きをオンライン上で完結させる場合、あるユーザ名義で作られたアカウントが、実在するユーザ本人のものであるかを確認する必要があります。経済産業省によって、「本人確認」は次に説明する2つを組み合わせて行うことが必要とされています。

2.1.2.「本人確認」とは何か

経済産業省は、ユーザの実在性を確認する「身元確認」と、そのユーザが作業していることを確認する「当人認証」の2つで「本人確認」が成り立つと定義付けています [10]。表 2でNTTドコモによる対策として挙げたeKYCは、サービス登録時の「身元確認」の手段の1つであり、2要素認証や2段階認証は「当人認証」の手段です。身元確認と当人認証は、それぞれ表 3に示すような3段階でレベル分けされています。これは、アメリカ国立標準技術研究所（NIST）が制定している「電子的認証に関するガイドライン（NIST SP-800-63）」をもとに整備されており、行政サービスにおいてオンラインで本人確認を実施する際の基準にもなっています。身元確認や当人認証の強度（レベル）とコスト、利便性はトレードオフの関係にあります。オンラインサービスは、性質に応じてこれらのバランスを総合的に判断したうえで、本人確認の適切なレベルを選択することが必要です。

表 3：身元確認と当人認証のレベル区分 [10]

	身元確認	当人認証
レベル3	「対面」で「公的身分証」をもとに実施	3要素のうちの複数を使用 ただし、マイナンバーカードなど、情報の不正な読み出しが困難なハードウェアによる認証を必ず含める
レベル2	「郵送等の非対面」で「公的身分証」を活用して実施	3要素のうちの複数を使用
レベル1	「自己申告」をもとに実施	3要素のうちの1つを使用

2.1.3. 決済サービスに必要なセキュリティ

ここまで、オンライン上で使用する決済サービスを含む金融関連サービスの不正利用の事例と、対策としてよく挙げられる「本人確認」について説明してきました。実際に店員と客が対面してお金のやり取りをしたり、自分のキャッシュカードを使用してATMから現金を引き出したりするのとは違い、オンラインで金銭を扱う場合は、アクセスしてきたユーザの信用を確かめる方法が重要になります。それを実現する方法が上記の「身元確認」や「当人認証」といった概念です。ここからは、一般的な決済サービスにある機能を安全に実現するために必要な機能について述べていきます。想定するサービスの概要を図 3に示します。

- インストール
  - ① スマホアプリ上でアカウント登録
- チャージ
  - ・ コンビニATMから現金でチャージ
  - ② 銀行口座を登録し、口座残高からチャージ
  - ③ クレジットカードを登録
  - ※チャージという形ではなく、クレジットカードによって決済される
- 支払い
  - ④ 自分のQRコード（またはバーコード）を表示し、店員に読み取ってもらう
  - ・ 店に掲示されているQRコードを読み取り、自分で支払金額を入力して支払う
- 出金
  - ⑤ 登録済み（または登録する）銀行口座へ残高を出金
- 送金
  - ・ アカウントを持つユーザに送金

図 3：決済サービスの代表的な機能

ユーザはまず、スマートフォン（以下、スマホ）で動作しているアプリケーション（以下、アプリ）上で、アカウントを登録します（①）。アプリへの現金のチャージは現金をコンビニのATMから直接入金する、または登録した銀行口座から入金する（②）か、クレジットカードを登録する（③）ことで後払いすることも可能です。銀行口座やクレジットカードを登録するには、アカウント登録時に実施したものに加えて、追加の身元確認が必要となります。実際の支払いには、自分のQRコードを画面上に表示して店舗のPOSレジで読み取ってもらう（④）か、店舗のQRコードをスマホで読み取って支払い金額を入力する方法があります。アプリ上の現金は、銀行口座に出金したり（⑤）、同じアプリのアカウントを持つユーザに送金することが可能です。

それぞれの機能に必要な本人確認の要素を表 4に、各機能の要件と具体的な対策を表 5にまとめます。

表 4：各機能に必要な本人確認とそのレベル

機能	身元確認	当人認証
①アカウント登録	推奨 ②③で必須のため、①のタイミングで実施することが推奨される ただし、決済機能を使わずポイントサービスのみ利用するユーザも存在するようなケースでは、最低限当人認証のみ行えば良い （その場合は②③で必ず身元確認を実施する）	推奨 *①
②銀行口座の登録/変更	必須（①で実施していればOK） レベル2 *②-1	必須 レベル2 *②-2
③クレジットカードの登録/変更	必須（①で実施していればOK） レベル2 *②-1	必須 レベル2 *③
④ユーザがQRコードを表示して支払い	③までで完了している前提	— *④
⑤銀行口座へ出金	③までで完了している前提	推奨

*① 一般社団法人キャッシュレス推進協議会が定めている「コード決済における不正な銀行口座紐づけの防止対策に関するガイドライン [11]」では、アカウント作成時の当人認証について、決済を行おうとするユーザとアカウントの作成を行った者とが同一であることを確認できるようにするための情報収集として重要であると述べられています。

*②-1 一般社団法人全国銀行協会が定めている「資金移動業者等との口座連携に関するガイドライン [12]」では、連携される側の銀行は、決済サービス側がアカウント開設時に実施しているユーザの実在性や同一性の確認プロセスをチェックすることが重要であるとされています。レベル 1 の身元確認は信用度がほとんどないと言われている [13]ため、レベル 2 での実施が必要です。

*②-2 *①のガイドラインにおいて、アカウントに銀行口座を連携させる際は、複数の要素による認証手段を組み合わせることによる堅牢な認証手続きが必要であると定められています。

*③ *①と同じ協議会が定めている「コード決済における不正流出したクレジットカード番号等の不正利用防止対策に関するガイドライン [14]」では、クレジットカード登録時の不正利用対策として、カードに記載されている情報で行う認証と併せて、クレジットカードの名義人のみが知る情報を照合する方法を導入するなどの対策を行うことが必須とされています。

*④ *①と同じ協議会が定めている「コード決済に関する統一技術仕様ガイドライン【利用者提示型】 [15]」では、QR コードの不正複製等による不正利用を防止するために、QR コードに有効時間を設定することが必須とされています。

表 5：各機能の要件と対策

機能	要件	対策
①アカウント登録	➢NTTドコモの例のように、他人名義で勝手にアカウントを作成されないために、実在するユーザが、確かに自分のアカウントを作成していることを保証する必要がある ➢犯罪収益移転防止法によって、マネーロンダリングや犯罪組織への資金供与を防止するために、特定の金融機関は、特定の方法での本人確認を実施することが定められている [16]。	＜**身元確認**＞ ● eKYC NTTドコモも発表しているように、「写真付きの本人確認書類を撮影及び撮影画像のアップロードを行い、撮影画像の人物と本人確認書類上の人物の同一性を確認 [6]」します。これにより、アカウントのユーザが、本人確認書類と同じ容貌の本人であることを確認することが出来るため、なりすましを防止することができます。 ＜**当人認証**＞ ● SMS認証 ユーザが入力した電話番号に、ランダムな4~6桁の数字を記載したSMSを送信し、その数字を入力することで本人による操作であることを確認する方法です。QRコード決済サービスシェアNo.1のPayPayは2020年6月24日、”AB-1234”のように2文字の無作為の英字＋4桁のランダムな数字で構成される認証番号を新たに導入しました。2文字の英字は認証画面上にも表示されているため、フィッシングによる被害を防ぐことが出来ます [17]。 ※SMS認証は広く使われている手法ですが、これを傍受するSMSインターセプト [18]や、電話番号を乗っ取るSIMスワップ [19]と呼ばれる手口も存在することから、十分な認証方法とは言えません。 ● ソーシャルログイン（API連携） GoogleやTwitter、FacebookなどのSNSアカウントを利用してアカウントを作成する方法です。アカウント登録時のSNS側のセキュリティレベルを引き継ぐことが出来ます。ソーシャルログインの場合、SNS側に通知が届くなどなりすましをある程度防ぐことが出来ます。 ※SNSアカウントは1人複数持つことが出来るほか譲渡も可能であるため、十分な認証方法とは言えません。

②銀行口座の登録／変更	他人の銀行口座情報が勝手に登録されないようにするために、連携される銀行側でユーザ本人の口座であること、この作業をユーザ本人が実施していることを確認する必要がある	＜**身元確認**＞ ①で実施していない場合は、①に記載した方法で実施します ＜**当人認証**＞ ● 2要素認証 銀行口座開設時に登録したパスワードや秘密の質問（知識情報）と、USBトークンなど（所持情報）で認証する方法や、インターネットバンキングに対応している銀行の場合は、OTPを利用する方法があります。 [20] ※最近、SMSの傍受やアプリによって生成されたOTPを盗み取るといった機能を持つ、決済サービスに関連する認証情報を窃取するためのマルウェア（トロイの木馬）が報告されています [21]。多くはフィッシングサイト（偽装されたWebサイト）を間違ってロードしてしまうことなどによって感染すると見られているため、不審なURLをクリックしないなどフィッシングへの基本的な対策は必須です。

③クレジットカードの登録／変更	他人のクレジットカード情報が勝手に登録されないように、連携されるクレジットカード会社側でユーザ本人のクレジットカードであることを確認する必要がある	＜**身元確認**＞ ①で実施していない場合は、①に記載した方法で実施します ＜**当人認証**＞ クレジットカード番号や有効期限、セキュリティコードといったカードに記載されている情報は、クレジットカードを目にする機会があれば盗用出来てしまいます。これだけでクレジットカードをアカウントに登録出来てしまっては危険です。 ● 3Dセキュア クレジットカードに記載されている情報のほかに、カード会社のサイトに別途登録したパスワードによって認証する方法です [22]。所有情報（クレジットカードに記載の番号）と知識情報（パスワード）を組み合わせる2要素認証の1つです。クレジットカード会社側で、カード発行時に身元確認を実施しているため、3Dセキュアに対応しているクレジットカードのみ連携を許可する仕組みにしておきます。
④CPM方式で支払い	他人のコードで決済されないような工夫が必要	通信している2者の間に入り込んで情報を盗聴する攻撃を、中間者攻撃（MITM：Man-in-the-Middle）と言います。CPM方式における支払いの際は、他人のQRコードを表示して決済する、物理的MITMを防ぐ必要があります。 ● コードの有効期限 端末上に表示するQRコードやバーコードは、短い時間（5分程度が一般的）で更新し、古いものは破棄されていく仕組みにしておくことで、事前に撮影しておいた他のユーザの画面を使って決済するリスクを下げることが出来ます。 ※端末の画面キャプチャを取得するような機能を持つマルウェアを仕込んでおく方法などでもMITMが可能となってしまいます。ユーザは、支払い直前までコードは表示させない、アプリからの通知を必ず確認するなどの対策が必要です。

⑤銀行口座へ出金	②までで行っている身元確認により、なりすましのリスクは抑えられるが、より認証強度を高めることも可能	＜**当人認証**＞ ● リスクベース認証 銀行口座に残高を出金する際、普段使用している端末やネットワーク、いつもの利用パターンと異なるアクセスがあった際に追加の認証項目を要求することで、攻撃者によるなりすましを防ぐことが出来ます。 ※SBI証券の事例のように、出金先の銀行口座を攻撃者によって勝手に変更できないようにするために、郵送による変更のみを受け付けるといった対策もあります。

2.1.4. まとめ

決済・金融関連サービスにまつわる不正利用の事例や、一般的な決済サービスが備えるべきセキュリティについて考えてきました。セキュリティレベルは、利便性や手続きのスピードとトレードオフの関係にあると言われますが、どちらも犠牲に出来るものではありません。オンラインですべての処理を完結させるサービスの場合は「すぐ利用開始できるかどうか」が重要であり、競合との差別化要因になります。一方で、特に金銭を扱うサービスでは「安心して利用できるかどうか」が重要であり、セキュリティレベルが競合との差別化要因になるべきであるとも言え、各事業者が、サービスごとに装備するセキュリティレベルを正しく判断する必要があります。今後ますますキャッシュレス化を推進する風潮が強まると考えられますので、本記事を参考に、QRコード決済サービスをどう安全に提供するか、そしてユーザは、利用中、または利用しようと思うサービスがどのようなセキュリティ対策を講じているのかを再度見直していただければと思います。

2.2. Zerologon（CVE-2020-1472）

Zerologonは、ドメイン内のデバイスとドメインコントローラ間で利用される認証プロトコルであるNetlogon Remote Protocolの脆弱性（CVE-2020-1472）です。攻撃者は、ドメインコントローラと通信可能なPC/デバイスから、特別に細工されたMS-NRPCリクエストをドメインコントローラへ送信し、脆弱性を悪用して不正に認証を突破することで、ドメイン管理者のアクセス権を取得します。Microsoft社は、この脆弱性に対して2段階の対策を計画しており、管理者はパッチ適用だけではなく、設定の変更が必要です。

2.2.1. Zerologonの概要

Zerologon（CVE-2020-1472） [23]は、Microsoft社が2020年8月に公開した脆弱性です。2020年9月11日に、オランダのセキュリティ企業SecuraがZerologonに関する技術レポート[24]を公開しました。2020年9月19日、米国のCISA（Cybersecurity and Infrastructure Security Agency）は、9月21日までにパッチを適用するよう、米国の行政機関へ緊急警告 [25]を発出しました。2020年9月24日にMicrosoft社は、この脆弱性を悪用した攻撃が発生していることを観測 [26]し、注意喚起 [27]を促しました。

2.2.2. Zerologonの脆弱性の解説

Zerologonは、Active Directoryにおいて、ドメイン内の各デバイスとWindows Server ドメインコントローラ（以下、ドメインコントローラ）間で、各々を認証するために利用する認証プロトコルNetlogon Remote Protocol（別称MS-NRPC、以下Netlogon）の脆弱性です。Netlogonは、認証に関わる通信を暗号化するために、AES-CFB8という暗号利用モードを利用していますが、暗号化処理に用いる初期化ベクトルの値の生成方法に問題がありました。初期化ベクトルとは、平文を暗号化する際に平文に追加するランダムなデータのことです。初期化ベクトルを予測できないランダムな値にすれば、同じ平文を暗号化しても異なる暗号文が出力され、暗号文から平文を推測することが困難になります。しかし、Netlogonへ実装されたプログラムでは、初期化ベクトルがランダムな値ではなく、常に0を使っていました。その結果、すべてが0で構成された64ビットの平文を用意して暗号化すると、1/256の確率で同じくすべてが0で構成された64ビットの暗号文が生成されてしまいます。

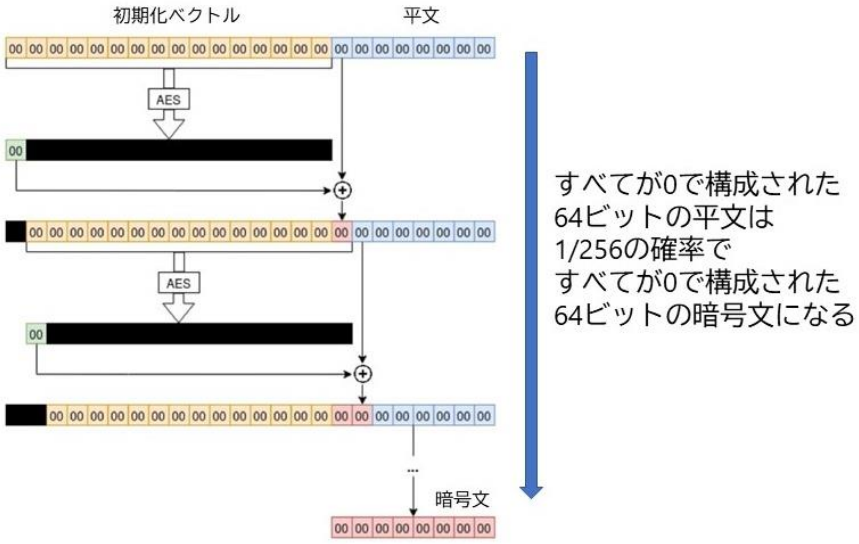


図 4: 初期化ベクトルが0に固定される影響

Secura社WHITEPAPER Zerologonの図を基に作成

Netlogonによる認証では、ドメインコントローラが、クライアントPCから受信したClient challengeコードと、同じくクライアントPCから受信したClient credentialコードをドメインコントローラ上のセッション鍵で復号して得た値が一致した場合に、クライアントPCを認証します。

- Client challenge：クライアントPCからドメインコントローラへ送信する任意の値
- Client credential：クライアントPCがClient challengeをセッション鍵（クライアントPCのパスワードのハッシュ）で暗号化した値

クライアントPCとドメインコントローラの共通の秘密鍵であるセッション鍵を持っていない攻撃者は、すべてが0で構成された64ビットのClient challengeコードと同じClient credentialコードをドメインコントローラへ送付することで、認証を試みます。Netlogonは認証が何度失敗しても制限がかからないため、攻撃者は、1/256の確率ですべてが0で構成された64ビットの復号文が生成されるまで、0で構成されたClient challengeコードとClient credentialコードの送付を繰り返します。1/256の確率ですべてが0の復号文が生成されると、攻撃者は、ドメインコントローラへ自身のクライアントPCを認証させることができてしまいます。この攻撃手法から、CVE-2020-1472は、Zero(0)logonと呼ばれています。

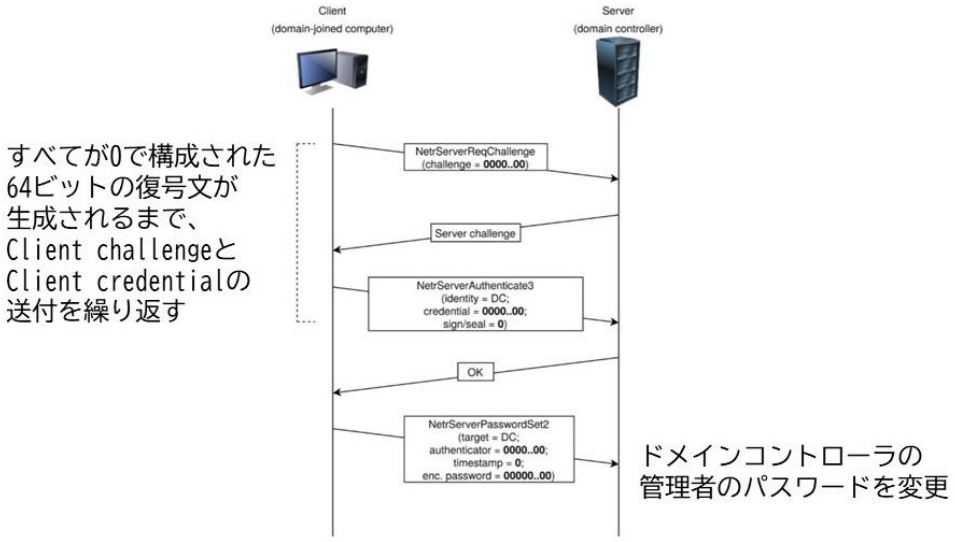


図 5：Netlgonの認証フロー

Secura社WHITEPAPER Zerologonの図を基に作成

攻撃者は、認証されたクライアントPC上から、同様にZerologonを狙った攻撃を繰り返して、ドメインコントローラの管理者のパスワード変更を成功することができます。攻撃者は、変更したパスワードを使って、ドメインコントローラへ管理者でログインできます。攻撃者は、ドメインコントローラの管理者権限を奪取できるため、ドメインに参加しているすべてのデバイスを乗っ取って、機密情報を窃取したり、マルウェアに感染させたりすることが可能になります。社内ネットワークに侵入する等、ドメインコントローラに直接アクセスできることが前提条件ではありますが、悪用された場合の影響が非常に大きいため、迅速な対処が必要です。

2.2.3. 段階的な対応

2020年8月11日に公開されたパッチは、一部のデバイスからのNetlogonを利用した接続を制限するものであり、適用するだけでは、Zerologonを狙った攻撃を完全に防ぐことはできません。すべてのデバイスにおいて、Netlogonに代わる安全な認証プロトコルであるSecure RPCの利用を強制することで、Zerologonを狙った攻撃を防ぐことができます。現在、製品サポートされているWindows OSは、Netlogonではなく、Secure RPCを利用可能です。ドメインコントローラがNetlogonの利用を禁止し、Secure RPCの利用を強制すれば、Zerologonを狙った攻撃の影響を受けません。

しかし、Secure RPCの利用を強制してしまうと、Secure RPCに対応していないデバイスが、ドメインに参加できなくなる問題が発生します。そのため、Microsoftは、初期展開フェーズと強制フェーズの2段階で、今回の脆弱性の対処 [28]を進めています。2020年8月11日に公

開されたパッチを適用することで、初期展開フェーズとなります。初期展開フェーズは、製品サポート中のWindows OSを搭載したデバイスのみにSecure RPCの利用を強制する暫定的な対策です。2021年2月に予定されているパッチを適用することで、強制フェーズとなります。強制フェーズでは、いかなるデバイスへもSecure RPCによる接続を強制する恒久的な対策です。

① 初期展開フェーズ

2020年8月に公開されたパッチを適用しただけでは、Windows OS以外のOSを搭載したデバイスは、Netlogonを使った接続ができてしまいます。そのため、初期展開フェーズでは、Netlogonを使った不審な接続を検知して対応したり、Secure RPCを利用可能なOSに変更したりする追加対策が必要です。初期展開フェーズでも、ドメイン内のすべてのデバイスがSecureRPCを利用できる場合は、ドメインコントローラのレジストリキーを以下のように設定することで、ドメイン内のすべてのデバイスにおいて、Netlogonの利用禁止とSecure RPCの利用強制をすることができます。

- FullSecureChannelProtection レジストリキーを 1 に設定

これによって、2021年2月のパッチを適用する前でも、Zerologonを悪用した攻撃をされるリスクを低減することができます。

Secure RPCの利用を利用できないデバイスがあり、Netlogonから接続する必要がある場合、グループポリシーを以下のように設定することで、指定したグループやアカウントに対してNetlogonの利用を許可することができます。

- ポリシー パス:**[コンピューターの構成]、[Windows の設定]、[セキュリティの設定]、[ローカル ポリシー]、[セキュリティ オプション]**
- 設定名:**ドメイン コントローラー:脆弱な Netlogon セキュア チャネル接続を許可する**

ただし、Netlogonによる接続を許可すると、Zerologonを悪用されるリスクが上がるため、注意が必要です。

2020年8月に公開されたパッチを適用すると、ドメインコントローラのイベントログに、以下のイベントIDが出力 [29]されるようになります。

表 6: イベントログへ記録されるNetlogon関連の情報

イベントID	分類	内容
5827	エラー （マシンアカウント）	Netlogonによる接続が拒否された際、ログに記録されるイベント
5828	エラー （信頼アカウント）	
5829	警告 （マシンアカウント）	Windows OS以外のOSを搭載したデバイスからのNetlogonによる接続が許可された際、ログに記録されるイベント（初期展開フェーズのみ）
5830	警告 （マシンアカウント）	Netlogonによる接続が許可された際、ログに記録されるイベント
5831	警告 （信頼アカウント）	

パッチ適用済みのドメインコントローラがNetlogonによる接続を拒否した場合、イベントログへイベントID 5827、または5828が記録されます。その場合は、以下の3つの場合が想定されます。

1. 製品サポート切れのWindows XPやWindows 7を搭載したデバイスから接続している場合です。OSをWindows 8.1や10へアップグレードしてください
2. Windows 8.1や10を搭載したデバイスがNetlogonを使用している場合です。Netlogonではなく、Secure RPCを利用するように設定を変更してください
3. Windows以外のOSを搭載したデバイスは、Secure RPCを利用するように設定を更新してください

パッチ適用済みのドメインコントローラが、Windows以外のOSを搭載したデバイスからのNetlogonによる接続を許可した場合に、イベントログへイベントID 5829が記録されます。その場合は、該当するデバイスは、Secure RPCを利用するように設定を変更してください。該当するデバイスがSecure RPCを利用できない場合は、強制フェーズ以降、ドメインに参加できなくなります。デバイスの更改を検討してください。

グループポリシーを設定してNetlogonによる接続を許可している状態で、パッチ適用済みのドメインコントローラが、Window OSを搭載したデバイスからのNetlogonによる接続を許可した場合に、イベントログへイベントID 5830、または5831が記録されます。該当するデバイスが、Secure RPCを利用できるOSにアップデートできる場合は、OSをアップデートしてください。すべてのデバイスがSecure RPCを利用できるようになったら、ドメインコントローラのレジストリキーを設定し、グループポリシーを初期設定へ変更してSecure RPCの利用を強制してください。

② 強制フェーズ

2021年2月に予定されているパッチを適用したドメインコントローラは、接続するすべてのデバイスに対して、Secure RPCを強制します。ただし、初期展開フェーズと同様、グループポリシーを設定することで、指定したグループやアカウントに対してNetlogonの利用を許可することもできます。Netlogonによる接続を許可する場合は、Zerologonを悪用されるリスクが上がるため、イベントログを監視してNetlogonによる接続を検知してください。

表 7: 実施すべき対応とNetlogonによる接続可否

フェーズ	対応	Netlogonによる接続
初期展開フェーズ	パッチ適用	Windows OS以外のOSを搭載した SecureRPC非対応デバイス以外は禁止
	パッチ適用 レジストリキー変更	禁止（例外なし）
	パッチ適用 レジストリキー変更 グループポリシー変更	指定したデバイス以外は禁止
強制フェーズ	パッチ適用（2021年2月）	禁止（例外なし）
	パッチ適用（2021年2月） グループポリシー変更	指定したデバイス以外は禁止

2.2.4. まとめ

Zerologonは、ドメインコントローラの管理者権限を奪取されてしまう重大な脆弱性です。社内ネットワークへ侵入されなければ問題ないと思うかもしれませんが、社内ネットワークに侵入されてしまうケースは依然として発生しており、この脆弱性を放置することは非常に危険です。もし、2020年8月のパッチが未適用の場合は、直ちにパッチを適用してください。ただし、このパッチをドメインコントローラへ適用しても、ドメインコントローラは、Windows OS以外のOSを搭載したデバイスから攻撃を受けます。Zerologonを悪用された攻撃のリスクを少しでも早く低減するためには、2021年2月公開予定のパッチを待たずに、ドメインコントローラの設定を変更して、Netlogonによる接続を禁止することを推奨します。また、Secure RPCに対応していないデバイスが存在する場合は、可能な限り迅速にデバイスのOSをSecure RPCに対応したOSへ変更をすることを推奨します。

脆弱性が公表された場合、速やかにパッチを適用することが重要とされています。一方で、Zerologonのように、パッチを適用しただけでは対策が不十分な場合や、やむを得ずパッチを適用できない場合も想定されます。業務への影響を抑えつつ、脆弱性が悪用されるリスクを低減するためには、脆弱性及びパッチの内容を理解し、パッチによる業務への影響を検証した上で、パッチを適用することが重要です。また、速やかにパッチが適用できない場合も、暫定的な対策を実施し、少しでも脆弱性が悪用されるリスクを低減することが必要です。

3. 情報漏えい

2020年度第2四半期は、サプライチェーンの弱点を突いた攻撃による情報漏えいが相次いで発生し、マイナンバーや社会保障番号などの重要な個人情報が流出している事例も起きています。近年、グローバル化やビジネスモデルの多様化等の影響でサプライチェーンが複雑化したことにより、このような事例が多く見られるようになりました。情報処理推進機構（IPA）が毎年公表している「情報セキュリティ 10大脅威」では、2019年、2020年とサプライチェーンの弱点を突いた攻撃が上位（4位）にランクインしており、サプライチェーンリスクマネジメントの重要性が高まってきています [30]。

3.1. サプライチェーンの弱点を突いた事例

表 8: サプライチェーンの弱点を突いた事例

組織	事例
サクソバンク証券（※サクソバンクA/Sの日本法人）	ネット証券会社サクソバンク証券において、氏名や住所、メールアドレス等を含む約3万8千件の顧客の個人情報の漏えいが発生し、このうちの378人は、マイナンバーカードの情報が漏えいした。取引に必要なログインパスワード等は親会社であるサクソバンクA/Sが管理しているサーバに保管されていたため、漏洩していない。原因は、海外の攻撃者集団が、同社が外部委託していた入出金ツールを格納していたサーバへ不正アクセスしたためである [31] [32]。
LiveAuctioneers	オークションサイトLiveAuctioneersにおいて、氏名、メールアドレス、電話番号、暗号化されたパスワード等を含む340万件の顧客の個人情報が漏えいし、攻撃者が300万件のパスワードを復号した。原因は、サプライヤ1社がサイバー攻撃を受けて、入札者データベースが不正アクセスされたためである [33] [34]。
Promo.com	ビデオ作成サイトPromo.comにおいて、氏名、メールアドレス、ハッシュ化されたパスワード等を含む2,200万件のユーザレコードが漏えいして、ハッカーフォーラムで公開された。攻撃者がパスワードを復号したおそれがある。漏えいの原因は、サードパーティ・サービスの脆弱性である [35] [36]。

Dave	デジタルバンキングサービスDaveにおいて、氏名、メールアドレス、電話番号、暗号化された社会保障番号等を含む顧客データを窃取され、顧客情報約750万件がハッカーフォーラムRAIDで無料提供された。攻撃者は、元サードパーティ・サービスプロバイダーであるGit分析会社Waydevのデータベースにブラインド SQLインジェクションの脆弱性を利用して侵入、DaveのGitHubまたはGitLabへのアクセス権を取得した。そして、攻撃者は取得したアクセス権を利用し、Daveアプリの顧客データへ不正アクセスしたことが漏えいの原因である [37] [38] [39]。

3.2. サプライチェーンリスクの対策

サクソバンク証券の事例では、システムリスク管理や外部委託先管理に関して十分な再発防止策が講じられていないとし、金融庁は業務改善命令を出しました。同社は2要素認証の導入等の対策を公表していましたが、金融庁は外部委託していた入出金ツールの脆弱性が存在したまま運用されていた問題に対して、組織的な見直しが必要と判断したと思われます。

セキュリティ対策が不十分であるサードパーティからの情報漏えい、もしくは、サードパーティを経由した攻撃（サプライチェーン攻撃）からの情報漏えいを防ぐためには、サプライチェーン全体のセキュリティ対策状況を把握し、抜け漏れなくリスクを低減することが求められます。過去の四半期レポートの注目トピックとしても取り上げている、２つの方法について紹介します [40]。

1つ目は、サプライチェーン全体を把握して、それらの責任の境界を一括して適切に管理する方法です。すべての取引先へ業務手順やセキュリティ対策内容を開示させたり、セキュリティ対策を依頼して実装させたりします。自組織外の業務手順やシステムを完全に把握したり、セキュリティ対策を管理したりできないため、実現には非常に高い難易度を伴います。この方法は、自組織がそのサプライチェーンにおいて最上流であり、末端組織まで統制を完全に取れる場合のみ可能です。

2つ目は、予め連携する組織同士でセキュリティ対策の実施主体や責任範囲を定めて各自でセキュリティ対策を実施する方法です。事前に発生しうるリスクを洗い出し、すり合わせることでサプライチェーン全体での対策の抜け漏れを防ぎます。しかし、自組織外のセキュリティ対策は連携先を信頼するしかないため、万が一、攻撃者が連携先を経由して攻撃したり、連携先へ提供した情報が漏えいしたりすることも踏まえ、攻撃の検知や提供する情報を必要最低限に留める対策も実施する必要があります。

3.3. 情報漏えいに伴う組織に与える影響

情報漏えいに伴う組織に与える影響を認識することは、セキュリティ対策を推進する上でとても重要です。情報漏えいを起こしてしまった場合、組織に与える影響は以下のような例が考えられます。

表 9: 情報漏えいに伴う組織に生じる影響例

影響	内容
損害賠償	情報漏えいによって損害が生じた人、組織への損害賠償費用
対応費用	原因調査・再発防止策にかかる費用、謝罪広告などによる広報費用
機会損失	サービス中断、社会的信用失墜による売上低下、取引中止
法的制裁	各国の法令（個人情報保護法、GDPR等）による刑事罰（罰金、入札停止）

情報漏えいした個人情報やパスワード等のアカウント情報は、標的型フィッシング攻撃やパスワードリスト型攻撃にも悪用されるおそれがあり、それによる二次被害の損害賠償が組織に対して求められるおそれも考えられます。また、欧州連合（EU）におけるGDPRをはじめに、世界各国で罰則規定を伴う個人情報保護に関する法整備が進められています。日本においても2020年6月に「個人情報の保護に関する法律等の一部を改正する法律」が公布され、一部の罰金刑の最高額の引き上げが行われました。今後も法的制裁による組織への影響は大きくなっていくことが予想されます。

また、2020年7月にIBM Securityが公表した「情報漏えい時に発生するコストに関する調査2020」によると、情報漏えい時に発生するコストはインシデント1件あたり平均386万ドル（約4億円）にものぼることが明らかになっています。そのうち、顧客の個人情報が漏えいした事例では、発生するコストが最も高い調査結果となっています [41]。

セキュリティ対策を推進し意思決定を行う際には、組織に与える影響を踏まえた上で判断していくことが重要です。

3.4. 2020年度第2四半期情報漏えい事例

表 10： 2020年度第2四半期情報漏えい事例

公表日	組織	原因	概要
7/10	Dunzo	サイバー攻撃	サードパーティのサーバが不正アクセスを受け、電話番号、メールアドレス等のユーザ情報が流出 [42]
7/16	MyCastingFile	設定ミス	氏名、住所、電話番号、メールアドレス等を含む約26万人の登録ユーザ情報が公開状態 [43]
8/7	三菱重工業株式会社	ソーシャルエンジニアリング	社有PCで社内ネットワークを経由せずに外部ネットワークに接続、SNSを利用した際にウイルスに感染し従業員情報が流出 [44]
8/11	SANS Institute	フィッシング	職員がフィッシングメールを受信し、個人情報を含む約2.8万件のデータが侵害 [45]
9/10	野村證券株式会社	内部不正	元社員が法人顧客275社の顧客情報を不正に他社へ流出 [46]
9/12	LINE株式会社	パスワードリスト攻撃	コミュニケーションアプリLINEのユーザアカウント約7.4万件に対し、不正ログイン [47]
9/24	HJホールディングス株式会社	パスワードリスト攻撃	動画配信サービスHuluのユーザアカウント約800件に対し、不正ログイン [48]

3.5. まとめ

今回、サプライチェーンの弱点を突いた攻撃の事例と対策、情報漏えいが発生してしまった場合に組織へ与える影響について紹介しました。

サプライチェーンリスクに対する方法を2つ紹介していますが、攻撃を完全に防ぐことは現実として困難な状況です。サプライチェーンマネジメントに関するガイドラインやフレームワークがさまざまな組織から提供されています。例として、2019年に経済産業省より発行された「サイバー・フィジカル・セキュリティ対策フレームワーク」があげられます。サプライチェーンリスク管理として組織がとるべき対策だけでなく、国内外の関連標準（NISTが発行するCybersecurity Framework等）との対応付けも示されています [49]。

また、近年、サプライチェーンリスクを評価するサービスも増加しており、複雑化するサプライチェーン全体のセキュリティ対策状況を一元管理し、弱点や攻撃を受けやすいポイントを可視化することができるサービスもあるため有効です。

日本においては、人的な要因等によりセキュリティ対策が不十分で攻撃の標的となりやすい中小企業のインシデント対応を支援する事業なども行われています [50]。これらの方法を活用し、リスクを低減していくために継続的な取組みが求められています。

4. 脆弱性

本章では、複数のBIG-IP製品に生じた脆弱性（CVE-2020-5902）について解説します。JVNへ掲載された当該脆弱性のCVSS Base値は10であり、極めて深刻な脆弱性です。当該製品を導入している組織は、早急にパッチを適用する必要があります。

4.1. 複数のBIG-IP製品に発生した脆弱性

4.1.1. 脆弱性概要

2020年7月6日、JPCERT/CCが「複数のBIG-IP製品の脆弱性（CVE-2020-5902）に関する注意喚起」を公開しました [51]。当該脆弱性は、F5 Networks社 BIG-IP製品の管理画面であるTraffic Management User Interface（TMUI）に発見されました。攻撃者は、この脆弱性を悪用することで、認証の有無に関わらず遠隔から任意のコードを実行可能です。当該製品において、TMUIがインターネットからアクセス可能となるよう設定している場合、当該脆弱性の影響を受けるおそれがあります [52]。

当該脆弱性の恒久対策として、F5 Networks社より脆弱性を修正するアップデートが提供されています [52]。また、暫定対策として、脆弱性の影響を緩和するアクセス制限などの実施方法も併せて提供されています [52]。

4.1.2. タイムライン

表 11に、複数のBIG-IP製品の脆弱性（CVE-2020-5902)が発見されてから、当該脆弱性を悪用する方法が一般公開されるまでの出来事を時系列に示します。

表 11：CVE-2020-5902の悪用方法公開までのタイムライン

日付	できごと
2020年4月1日	Positive Technologies社のMikhail KlyuchnikovがF5 Networks社のBIG-IP製品に存在する脆弱性を報告しました [53]。
2020年4月3日	F5 Networks社が上記脆弱性を再現しました [53]。
2020年7月1日	F5 Networks社はBIG-IP製品に存在する脆弱性（CVE-2020-5902）を確認したと公表し、修正パッチおよびアドバイザリを公開しました [54]。
2020年7月2日	Positive Technologies社は、独自のアドバイザリを公開しました [55]。

2020年7月5日	本脆弱性を悪用して攻撃を成功させることができる検証コード(PoC)がTwitter上に公開されました [56]。
2020年7月6日	Metasploit用のexploitモジュールがGitHub上に公開されました [57]。

当該脆弱性は7月1日に公表されました。その後、表 11に示すように4日後の7月5日にはSNS上に検証コードが公開され、その翌日の7月6日にはGitHub上にMetasploit用のexploitモジュールが公開されました。脆弱性情報の公表後、1週間以内に悪用方法が広く一般に公開されたことになります。

昨今、脆弱性情報の公表翌日に攻撃が開始されるケース [58]や、脆弱性が公表された時点ではパッチ等の対策が存在しないケース（ゼロデイ脆弱性）など、脆弱性情報の公表からの悪用方法の公開までが短時間でなされ、脆弱性対応に充てられる猶予期間が非常に短くなるケースがあります。

そのため、組織の情報セキュリティ担当者は、定常的に脆弱性情報の収集を行う必要があります。もし、使用している製品の脆弱性情報を確認した場合は、緩和策の実施やパッチの適用などの対応を迅速に行うことが重要です。

4.1.3. 攻撃関連の事例

2020年7月上旬のBIG-IP製品の脆弱性（CVE-2020-5902）の公表後、BAD PACKETS社は当該脆弱性に関する大量のスキャンを観測しました [59]。日本国内においても、当該脆弱性に対するスキャンや脆弱性の悪用を試みたと推察される通信が複数組織により観測されています [51] [60]。脆弱性のスキャンは、脆弱性があるシステムの存在確認や、システムに不正に侵入できるおそれのある弱点を発見するために行われます [61]。スキャン自体はシステムへ悪影響を及ぼしません。しかし、攻撃者がスキャンによって悪用が可能な脆弱性の残ったシステムを発見した場合、そのシステムを攻撃するおそれがあります。

BAD PACKETS社が、インターネットに公開されているBIG-IP製品を調査した結果を表 12に示します [59]。同調査によると、7月5日時点でTMUIがインターネットに公開されている同製品が計8,204台（内3,012台が当該脆弱性未修整）発見されています。この場合、インターネット経由で当該製品に対して誰でも容易にスキャンやアクセスを試行することが可能となり、攻撃を受けるリスクが高まります。

TMUIはBIG-IP製品の管理者用インターフェースであり、本来インターネットに公開することは推奨されません。TMUIへのアクセス経路として、Management PortとSelf IPsの二通りがあります。前者の経路においては、接続元IPアドレスによるアクセス制限を実施することが推奨されていますが [62]、デフォルト設定ではすべてのIPアドレスからのアクセスが許可されています [63]。また、後者の経路においては、デフォルト設定ではアクセス可能なプロトコルとサービスが必要最低限に制限されていますが [64]、TMUIへのアクセスに必要なHTTP

やSSHは許可されています。上記のようなデフォルト設定を適切な設定に変更せずに同製品を使用している場合や、設定を誤って意図せずTMUIをインターネット上へ公開しているケースも考えられます。脆弱性対応と併せて、当該製品の設定や当該製品を含むネットワーク設計を再度確認することを推奨いたします。

表 12：脆弱性が未修正のBIG-IP製品の台数 [59]

国名	未修正台数
アメリカ	1,237
中国	496
台湾	144
タイ	114
韓国	91
マレーシア	80
フィリピン	79
インドネシア	72
ブラジル	65
日本	60

また、トレンドマイクロ社は、当該脆弱性を悪用するIoTマルウェアのダウンローダを確認しています [65]。当該ダウンローダはインターネットからアクセス可能なBIG-IP製品を探索し、当該脆弱性を悪用して内部に侵入します。その後、不正サイトに接続し、IoTマルウェア「Mirai」の亜種である「SORA」 [66]をダウンロードして実行します。「SORA」は脆弱なBIG-IP製品経由でIoT機器に侵入し、IoTボットネットを構築します。また、当該ダウンローダは表 13に示すような同時期に公表された様々な脆弱性を悪用した攻撃を行うこともわかっています。

表 13：ダウンローダが悪用する脆弱性 [65]

機器	脆弱性	CVE識別子
Apache Kylin 3.0.1	コマンドインジェクション	CVE-2020-1956
Aruba ClearPass Policy Manager 6.7.0	未認証の遠隔からのコード実行	CVE-2020-7115
Big-IP 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, 11.6.1-11.6.5.1	TMUIでの遠隔からのコード実行	CVE-2020-5902

Comtrend VR-3033	コマンドインジェクション	CVE-2020-10173
HP LinuxKI 6.01	遠隔からのコマンドインジェクション	CVE-2020-7209
Tenda AC15 AC1900	遠隔からのコード実行	CVE-2020-10987
Nexus Repository Manger 3	遠隔からのコード実行	CVE-2020–10204
Netlink GPON Router 1.0.11	遠隔からのコード実行	なし
Netgear R7000 Router	遠隔からのコード実行	なし
Sickbeard 0.1	遠隔からのコード実行	なし

4.2. まとめ

今回は、BIG-IP製品の脆弱性を取り上げました。マクニカネットワークスセキュリティ研究センターの調査 [67]によれば、2020年7月8日時点で、日本国内に当該脆弱性が修正されずにTMUIがインターネットに公開されているBIG-IP製品が67台あり、引き続き対応が必要な状態です。組織の情報セキュリティ担当者は、組織のソフトウエア構成や変更の状況の管理、脆弱性情報の収集を行い、危険な脆弱性が見つかった場合は迅速にパッチ適用する必要があります。パッチを適用した時点で、既に侵害が発生している場合もあります。パッチ適用だけで安心せずに、IoC検出ツール [68]等を利用して侵害の有無を調査することも重要です。

新型コロナウイルス感染に伴うテレワーク化により、システム管理も自宅から遠隔で作業を行うようになりました。すべての管理者が職場からアクセスしていたときと異なり、複数の管理者が自宅からプロバイダ経由で管理対象のシステムの管理画面へ接続しなければなりません。接続元IPアドレスによるアクセス制限が困難な場合もあるでしょう。そのような事情から、アクセス制限されていないTMUIが大量に存在していたのかもしれません。管理画面へのアクセス制限ができない場合は、クライアント証明書を使ったSSL-VPN接続や二要素認証を使用したログイン方式を使うなど、攻撃者による不正接続を防止する対策を導入してから、安全に利用しましょう。

5. マルウェア・ランサムウェア

5.1. 2020年度第2四半期の概況

2019年度第3四半期に国内で感染が多発したマルウェアEmotetの活動が再び確認されています。2020年度第1四半期に引き続き、MazeやNetWalker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。国内では、マルウェア感染による不正アクセスや情報漏えいの被害が報告されています。海外では、ランサムウェア感染によるサービス障害の被害が報告されています。本稿では、今後の被害拡大による影響が大きいという理由で、Emotetの再流行、ランサムウェア攻撃による被害の深刻化について取り上げます。

5.1.1. Emotetの再流行

Emotetは2019年10月から2020年2月まで国内で多数の感染事例が報告されていましたが、2020年3月から7月までは感染活動が沈静化していました。しかし、2020年7月末から再び活発な感染活動が確認され、9月には過去最大規模の感染が確認されました [69]。

図 6: 国内でのEmotet検出台数の推移 [69]

Emotet感染拡大の原因として、拡散の手口が巧妙化している点が挙げられます。2020年7月以降のEmotetメールは、国内のビジネスメールでよく見られる内容をまねして書かれています。メール本文が「協力会社各位」という書き出しで始まっていたり、件名・添付ファイル名が「消防検査」「ご入金額の通知・御請求書発行のお願い」「次の会議の議題」となって

いたりと、一見しただけでは正規のメールとの判別が難しくなっています。

2020年9月以降、パスワード付きzipファイルを利用した新たなEmotet拡散の手口が報告されています [70]。パスワード付きzipファイルは暗号化されているため、メール配信経路でセキュリティ製品によるウイルス検知をすり抜け、ファイルを駆除できないおそれがあります。したがって、受信者のもとまで悪意のあるファイルが届いてしまう確率が高くなります。パスワード付きzipファイルを添付したメールの送信は、1通目に暗号化した添付ファイルを、2通目に解凍パスワードを分けて送ることでメール誤送信による情報漏えい対策として国内で広く使われてきました。しかしながら、メールを盗聴できる攻撃者は添付ファイルとパスワード両方を取得できる可能性が高いため、情報漏えい対策として不十分だと言われています。中央省庁でもパスワード付きzipファイルの使用を廃止する方針が発表されています [71]。

今回の新たなEmotet拡散の手口の対策は、思い切ってパスワード付きzipファイルを添付したメールの送受信の利用をやめることが有効です。上記のような不十分な情報漏えい対策の廃止に加えて、悪意のあるファイルが駆除されずに開封されてしまうリスクを回避できます。

2019年度第3期四半期レポートでは、大企業に比べてセキュリティ対策や訓練が不十分な中小企業において幅広く感染が起こったと推測しました [72]が、2020年度第2四半期の流行においても同様の傾向が見られます。Emotetをはじめとするメールを入口とした標的型攻撃に対しては、メールシステム上で攻撃を検知し食い止めるソリューションを構築することが効果の高い対策ですが、導入にはコストと時間がかかるため、中小企業にとってハードルが高いといえます。中小企業に向いている対策として、Gmailのような悪意のあるメールの検知や振り分け機能を備えたメールサービスを利用することが挙げられます。既存のメールサーバに検知や振り分けのソリューションを導入して運用することに比べて安価で、導入に時間がかかりません。

今後さらなる手口の巧妙化により、Emotetの被害は拡大が懸念されます。IPAはEmotetのメールで実際に使用された件名、本文をまとめて公開しています [70]。IPAやJPCERT/CCの発信している情報 [73]など最新の情報を収集して引き続き警戒を行ってください。

5.1.2. ランサムウェア攻撃による被害の深刻化

2020年9月、独デュッセルドルフの大学病院がランサムウェア攻撃に見舞われ、病院の医療システムが麻痺したために搬送中の患者が死亡するという悲劇が発生してしまいました [74]。医療機関を標的としたランサムウェア攻撃は過去にも発生していましたが、人命が失われたケースは今回が初めてです。ランサムウェアが直接患者の命を狙っておらず、病院を運営する大学が主な標的だったことから、このケースでは攻撃者に人命を狙った意図はないと推測されます。しかしながら、2019年度第4四半期から新型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ること [75] [76]からも、医療機関を標的にしたランサムウェア攻撃によって人命が奪われる事態が発生するおそれが高まっています。

2020年7月に発生した米GPSサービス企業Garmin社への攻撃では、ランサムウェア感染に

よるサービス障害が発生しました [77]。ユーザのアクティビティやデータをクラウドや他のデバイスに同期するGarmin Connect、航空航行やルート計画を行うflyGarminといったサービスが停止し、これらを利用する全世界数百万人のユーザが1週間にわたり影響を受けました。同様の障害が航空管制システムやプラント制御システムといった重要インフラで発生した場合、サービス停止によって社会活動の混乱を招き、世界中に悪影響をもたらすおそれがあります。

上記の事例のように、ランサムウェア攻撃による被害は単なる金銭的被害に留まらず、人命に関わる被害や世界規模の混乱を招くおそれがあります。特にランサムウェアは感染した段階でシステムの停止につながるおそれが高いため、可能な限り未然に感染を防止することが重要です。ランサムウェアの発症の発端となるエンドポイントにおける対策が有効です。具体的には、EDR製品の振る舞い検知によって不審なシェルスクリプト動作に関わるアクティビティを検知して、これを停止することが挙げられます。マルウェア対策ソフトによる検知を回避するファイルレス攻撃に対しても検知が可能です。

5.1.3. その他のマルウェアの被害事例

2020年度第2四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。最近は、海外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。国内では、マルウェア感染による不正アクセスや情報漏えいの被害が報告されています。海外では、ランサムウェア感染によるサービス障害の被害が報告されています。2020年度第2四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 14に示します。

表 14： マルウェア・ランサムウェアの被害事例

日付	標的	概要
7/7	アメリカ/アラバマ州 Chilton郡	ランサムウェア攻撃の疑いにより、コンピュータネットワークを一時的に閉鎖した [78]
7/18	アルゼンチン/通信企業 /Telecom Argentina	ランサムウェアに感染した。社内VPNとデータベースアクセスに障害が発生した [79]
7/23	スペイン/国営鉄道インフラ管理企業/ADIF	REVilランサムウェアに感染した。攻撃による大きな影響は出なかった [80]
8/6	アメリカ/電気機器企業 /キヤノンUSA	Mazeランサムウェアに感染した。運営するクラウドプラットフォーム上の一部データが消失した [81]
8/7	三菱重工	社用ノートパソコンがマルウェアに感染した。社内ネットワークに感染が拡大し、不正アクセス被害が発生した [82]
8/16	アメリカ/酒造企業 /Brown-Forman	Sodinokibiランサムウェアに感染した。システムデータの暗号化は防ぐことができた [83]

8/21	経済同友会	事務局システムの一部がランサムウェアに感染し、障害が発生した [84]
8/28	福岡県/不動産販売/ダックス	マルウェアに感染し、過去のメール送受信履歴が流出した。同社従業員や同社メールアドレスに装ったメールの送信も確認された [85]
9/5	アメリカ/サイバーセキュリティ企業/Cygilant	NetWalkerランサムウェアに感染した [86]
9/7	パキスタン/電力企業/K-Electric	NetWalkerランサムウェアに感染した。オンライン請求サービスに障害が発生した [87]
9/14	アメリカ/ファイバーレーザー企業/IPG Photonics	RansomExxランサムウェアに感染した。社内ITシステムがシャットダウンされ、電子メール、電話、ネットワーク接続等に障害が発生した [88]

5.2. まとめ

日本国内ではマルウェアEmotetの活動再開が確認されました。今回新たに確認されたパスワード付きzipファイルを悪用したEmotetへの対策としては、思い切ってパスワード付きzipファイルを添付したメールの送受信の利用をやめることが有効です。また、2020年度第2四半期は、ランサムウェア攻撃によって人命が失われるケースが発生しました。ランサムウェアは感染した段階でシステムの停止につながるおそれが高いため、可能な限り未然に感染を防止できる対策を実施することが重要です。

6. 予測

身元確認の実施がますます重要に

「決済サービスに必要なセキュリティ」の中で、SMSを使った2要素認証はSMSインターセプトやSIMスワップと呼ばれる行為で破られる可能性が高いため十分な認証方法とは言えないと述べました。しかし、SMS認証が当人認証手段として不十分である理由は他にもあります。それは「SMS認証代行」の存在です。もともとは、SMS非対応のSIMカードで使用しているデバイスでアカウントを作成したいケースや、複数アカウントを作成したいものの電話番号は1つしか持っていないといったケースを想定したサービスです。しかし最近は、アプリユーザが身元を隠す目的でサービスを使用する事例が増えており、犯罪を助長するとして埼玉県警などが警鐘を鳴らしています [89]。背景にあるのは、身元確認手続きなく取得できるSIMカードの存在です。SIMカードの所有者が電話番号とその番号に届いた認証コードを代行依頼者に伝えれば、依頼者は身元を隠したまま認証を突破できてしまいます。大手キャリアを介さない格安SIMの利用者が増加している中、今後、SMS認証を不正に突破することはより簡単になると考えられます。利用者からの信用を獲得する意味でも、オンライン上で完結するサービスを提供する事業者は、本人確認処理は「認証」だけでは成り立たないことを再認識し、eKYCを含めた身元確認の実施を行っていくことが必要です。

サプライチェーンに対する攻撃の継続

2020年6月～9月の間にサプライチェーンを狙った攻撃が多く発生しました。また、米国や英国等の5カ国において、8割の組織がサプライチェーン攻撃を過去1年間に受けているという調査結果も存在します。この攻撃へ対策するには、まずサプライチェーン全体のセキュリティ対策状況を把握することが必要ですが、米国や英国等の5カ国の77%の組織で対策状況の把握が実施できていないという調査結果があります [90]。このことから、多くの国の多くの組織が対策を実施できていないこと想定されるため、多くの組織でサプライチェーン攻撃の対策が必要です。

さらに、2020年のセキュリティ市場の成長は鈍化するという予測から、対策もあまり進んでいないと想定されます [91]。その上、新型コロナウイルスの流行を受け、サプライチェーンでつながった各組織の労働様式がテレワークに移行しました。自宅PCからのリモートアクセスの増加により、攻撃者が狙いやすい箇所がさらに増えています [92]。このような状況のため、攻撃者は引き続きサプライチェーン攻撃を行うと想定されます。そのため、「3. 情報漏えい」で示したようにサプライチェーンマネジメントに関するガイドラインやフレームワークの活用、サプライチェーンリスクを評価するサービスの利用等をお薦めします。また、日本において、大企業と中小企業がともにサイバーセキュリティ対策を推進するための団体として、サプライチェーン・サイバーセキュリティ・コンソーシアム

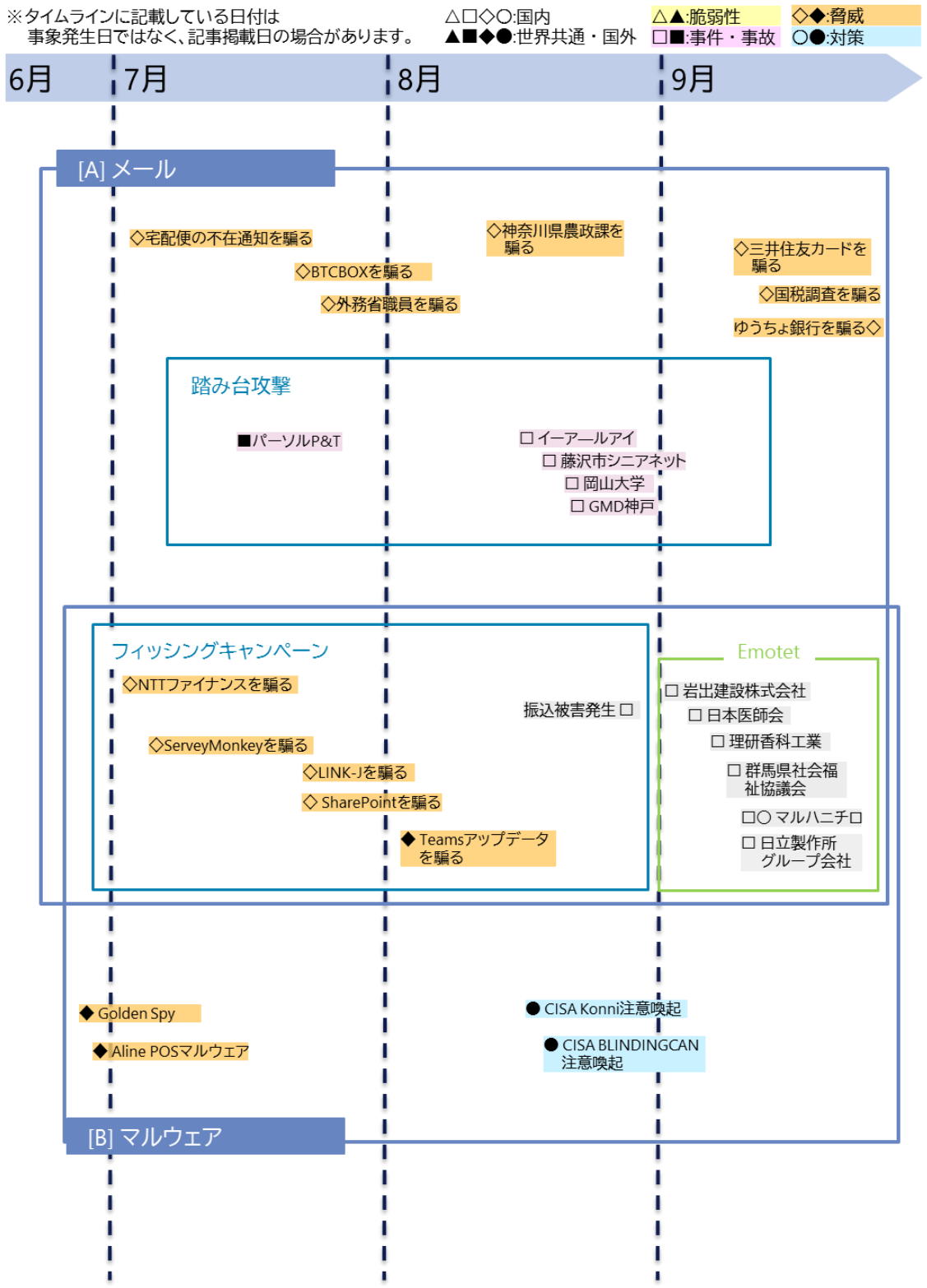
が設立されました。このような団体が発信する情報を活用していくことも有効です [93]。

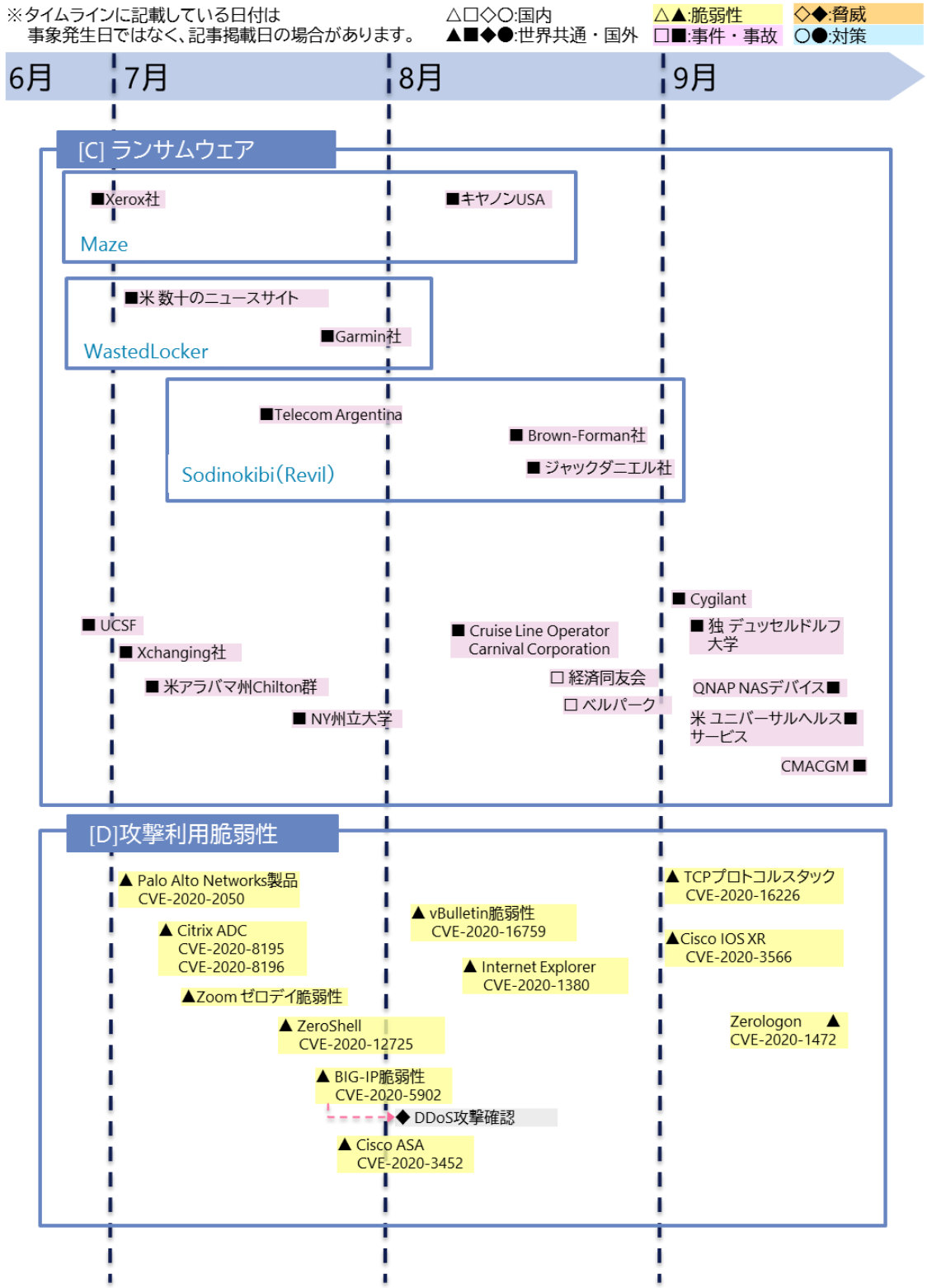
新型コロナウイルスに関連したサイバー攻撃に引き続き警戒

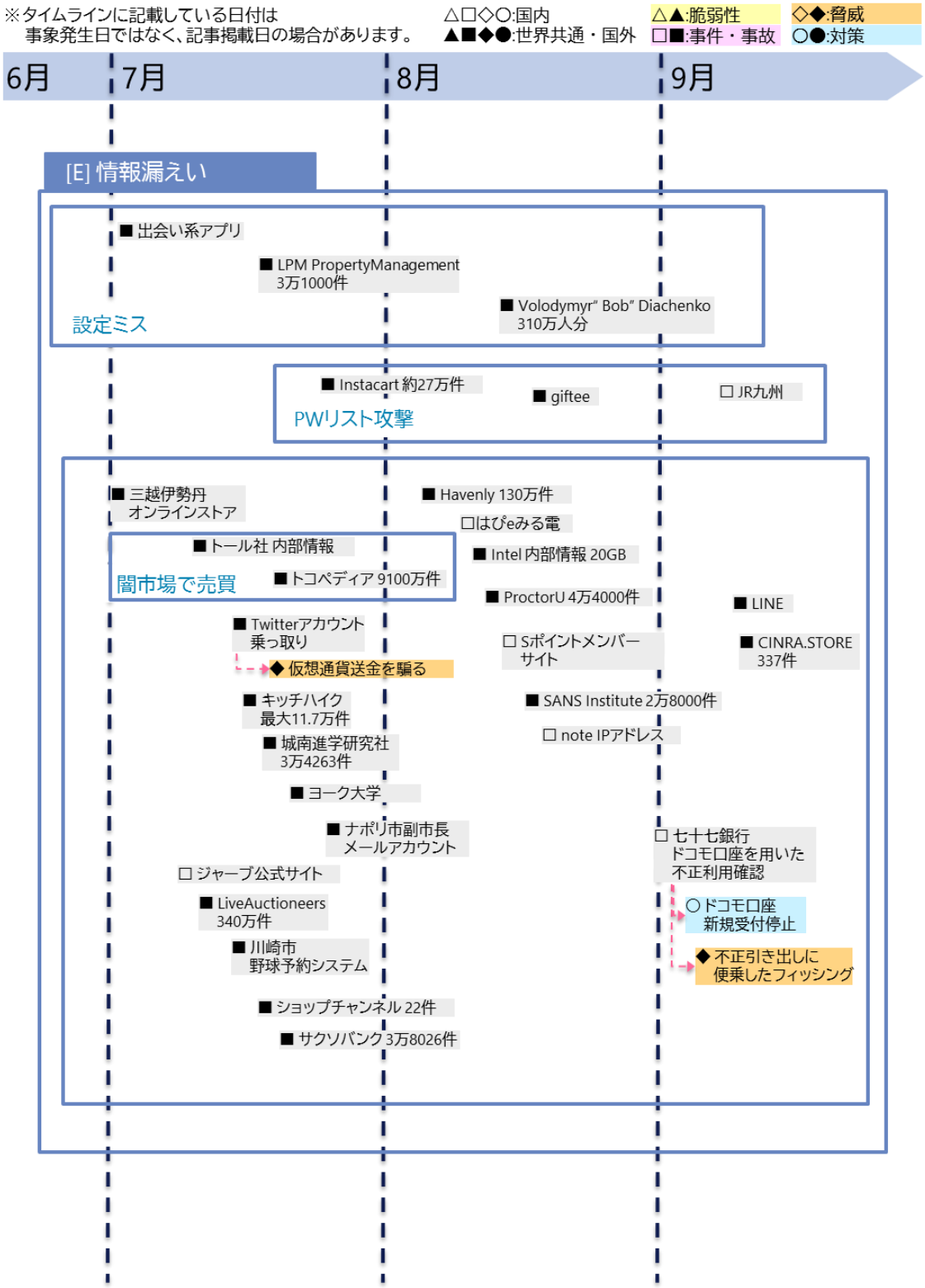
新型コロナウイルスの感染情報提供を装ったフィッシングメール等の攻撃メールは、9月時点でも発生していますが、4月のピーク時と比較すると減少しています [94] [95]。これは、新型コロナウイルスの感染数や死者数が増加する一方で、世界中の各組織から、新型コロナウイルス情報関連の攻撃メールに対する注意喚起が出されたことにより、人々が騙されにくくなったこと、またテレワークやステイホーム等のより騙しやすいテーマがあったためと考えます [96]。この種の攻撃メールは、新型コロナウイルス関連の情報の大きな変化が無ければ、減少していくと考えられます。しかしながら、今後、各国で新型コロナウイルスワクチンの接種が始まっていけば、人々はワクチン情報を強く求めるため、初期の新型コロナウイルス流行時と同様にワクチンの情報を使ったフィッシング、スミッシング、偽アプリ等の攻撃が増加していくと予想されます。攻撃メールの被害に会わないためには、2019 年度 第 4 四半期のレポートに記載した情報受信者が気を付けるポイントを普段から心がけておくことをお薦めします [97]。

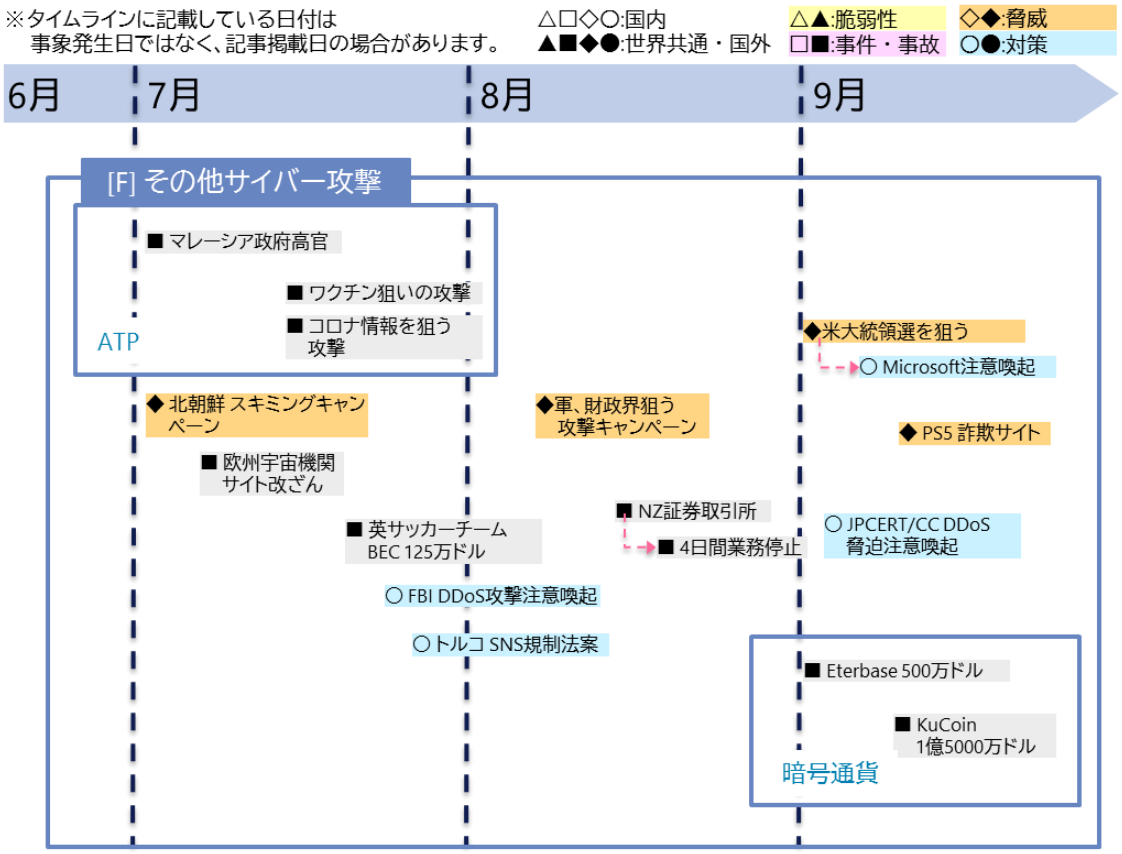
また、新型コロナウイルス関連の攻撃として、ニューノーマルに対する攻撃も忘れてはいけません。労働様式がテレワークに移行したことで、様々なリスクが新たに発生しました [92]。テレワークに移行してから十分な時間が無かったことや、新型コロナウイルスの影響で十分なセキュリティ予算を確保できていないこと等から、多くの組織は、テレワークの変化に伴うリスクに対して十分に対応できていないと想定されます。このような状況のため、自宅PC、クラウドサービス、コミュニケーションツールを狙った攻撃や、コミュニケーションが取りにくくなったことによるインシデント被害の拡大は、今後も発生していくと想定されます。2020 年度 第 1 四半期のレポートにテレワークの増加に伴うリスクと気をつけるべきポイントを記載していますので、ご一読いただき、対応を検討することをお薦めします [92]。

7. タイムライン









参考文献

[1] 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 2020,” 独立行政法人情報処理推進機構, 28 8 2020. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/10threats2020.html#download.

[2] 株式会社SBI証券, “悪意のある第三者による不正アクセスに関するお知らせ,” 株式会社SBI証券, 16 9 2020. [オンライン]. Available: https://www.sbisec.co.jp/ETGate/WPLETmgR001Control?OutSide=on&getFlg=on&burl=search_home&cat1=home&cat2=corporate&dir=corporate&file=irpress/prestory200916_02.html.

[3] 株式会社NTTドコモ, “ドコモ口座とは？,” 株式会社NTTドコモ, [オンライン]. Available: https://docomokouza.jp/detail/about.html.

[4] 株式会社日本経済新聞社, “ドコモ口座不正引き出し、りそな銀行で19年5月にも,” 株式会社日本経済新聞社, 9 9 2020. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO63655670Z00C20A9EE8000/.

[5] 株式会社日本経済新聞社, “ドコモ口座、判明被害の補償完了　128件で2885万円,” 株式会社日本経済新聞社, 28 10 2020. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO65570570Y0A021C2000000/.

[6] 株式会社NTTドコモ, “ドコモ口座への銀行口座の新規登録における対策強化について,” 株式会社NTTドコモ, 9 9 2020. [オンライン]. Available: https://www.nttdocomo.co.jp/info/news_release/detail/20200909_00_m.html.

[7] “Webアプリケーションファイアーウォール（WAF）,” キヤノン, [オンライン]. Available: https://cweb.canon.jp/it-sec/solution/siteguard/waf/.

[8] NECソリューションイノベータ株式会社, “リスクベース認証,” NECソリューションイノベータ株式会社, [オンライン]. Available: https://www.nec-solutioninnovators.co.jp/ss/insider/security-words/24.html.

[9] “アシアナIDT　フィンテック分野のセキュリティベンダーと協業　新たにセキュリティ事業を切り開く,” 11 2 2016. [オンライン]. Available: https://www.weeklybcn.com/journal/news/detail/20160211_14606.html.

[10] “オンラインサービスにおける身元確認手法の整理に関する検討報告書を取りまとめました,” 経済産業省, 17 4 2020. [オンライン]. Available: https://www.meti.go.jp/press/2020/04/20200417002/20200417002.html.

[11] 一般社団法人キャッシュレス推進協議会, “コード決済における不正な銀行口座紐づけの防止対策に関するガイドライン,” 一般社団法人キャッシュレス推進協議会, 18 9 2020. [オンライン]. Available: https://www.paymentsjapan.or.jp/wordpress/wp-content/uploads/2020/09/Fraud_Prevention_Guidelines_bkac_linked.pdf.

[12] 一般社団法人全国銀行協会, “資金移動業者等との口座連携に関するガイドライン,” 一般社団法人全国銀行協会, 30 11 2020. [オンライン]. Available: https://www.zenginkyo.or.jp/fileadmin/res/news/news321130.pdf.

[13] 各府省情報化統括責任者（ＣＩＯ）連絡会議, “行政手続におけるオンラインによる本人確認の手法に関するガイドライン,” 各府省情報化統括責任者（ＣＩＯ）連絡会議, 15 2 2019. [オンライン]. Available: https://www.kantei.go.jp/jp/singi/it2/cio/kettei/20190225kettei1-1.pdf.

[14] 一般社団法人キャッシュレス推進協議会, “コード決済における不正流出したクレジットカード番号等の不正利用防止対策に関するガイドライン,” 一般社団法人キャッシュレス推進協議会, 16 4 2019. [オンライン]. Available: https://www.paymentsjapan.or.jp/wordpress/wp-content/uploads/2019/04/Fraud_Prevention_Guideline.pdf.

[15] 一般社団法人キャッシュレス推進協議会, “コード決済に関する統一技術仕様ガイドライン【利用者提示型】,” 一般社団法人キャッシュレス推進協議会, 31 10 2019. [オンライン]. Available: https://www.paymentsjapan.or.jp/wordpress/wp-content/uploads/2019/10/CPM_Guideline_1.2.pdf.

[16] 金融庁, “「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令」の公表について,” 金融庁, 30 11 2018. [オンライン]. Available: https://www.fsa.go.jp/news/30/sonota/20181130/20181130.html.

[17] PayPay株式会社, “「PayPay」のSMS認証機能のセキュリティー強化について,” PayPay株式会社, 24 6 2020. [オンライン]. Available: https://about.paypay.ne.jp/pr/20200624/01/.

[18] “NISTが警告、SMSでの二段階認証が危険な理由,” ZDNetJapan, 27 1 2017. [オンライン]. Available: https://japan.zdnet.com/article/35095393/.

[19] “欧米でも「決済アプリの不正出金・詐欺」多発、スクエアのCashAppやZelleでも――ドコモ、PayPayだけではない,” coindesk Japan, 19 10 2020. [オンライン]. Available: https://www.coindeskjapan.com/84820/.

[20] 公益財団法人金融情報システムセンター, “口座振替による不正出金に対する金融情報システムへの安全対策のあり方,” 公益財団法人　金融情報システムセン

ター, 2020.

[21] “New 'Alien' malware can steal passwords from 226 Android apps,” ZDNet, 24 9 2020. [オンライン]. Available: https://www.zdnet.com/article/new-alien-malware-can-steal-passwords-from-226-android-apps/.

[22] 株式会社ゼウス, “3Dセキュア（クレジットカード本人認証サービス）,” 株式会社ゼウス, [オンライン]. Available: https://www.cardservice.co.jp/service/creditcard/3d.html.

[23] Microsoft Security Response Center, “Netlogon の特権の昇格の脆弱性,” 11 8 2020. [オンライン]. Available: https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2020-1472.

[24] Secura, “Zerologon: Instantly Become Domain Admin by Subverting Netlogon Cryptography (CVE-2020-1472),” 14 9 2020. [オンライン]. Available: https://www.secura.com/blog/zero-logon.

[25] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, “WINDOWS SERVER VULNERABILITY REQUIRES IMMEDIATE ATTENTION,” 18 9 2020. [オンライン]. Available: https://www.cisa.gov/blog/2020/09/18/windows-server-vulnerability-requires-immediate-attention.

[26] Microsoft Corporation, “ZeroLogon is now detected by Microsoft Defender for Identity (CVE-2020-1472 exploitation),” 1 10 2020. [オンライン]. Available: https://techcommunity.microsoft.com/t5/microsoft-365-defender/zerologon-is-now-detected-by-microsoft-defender-for-identity-cve/ba-p/1734034.

[27] Microsoft Security Intelligence@MsftSecIntel, “Microsoft is actively tracking threat actor activity using exploits for the CVE-2020-1472 Netlogon EoP vulnerability, dubbed Zerologon.,” 24 9 2020. [オンライン]. Available: https://twitter.com/MsftSecIntel/status/1308941504707063808.

[28] Microsoft Security Response Center, “[AD 管理者向け] CVE-2020-1472 Netlogon の対応ガイダンスの概要,” 14 9 2020. [オンライン]. Available: https://msrc-blog.microsoft.com/2020/09/14/20200915_netlogon/.

[29] 日本マイクロソフト株式会社, “CVE-2020-1472 に関連する Netlogon のセキュリティで保護されたチャネルの接続の変更を管理する方法,” 20 11 2020. [オンライン]. Available: https://support.microsoft.com/ja-jp/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc.

[30] 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 2020,” 独立行

政法人情報処理推進機構, 28 8 2020. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/10threats2020.html.

[31] サクソバンク証券株式会社, “サイバー攻撃による個人情報流出に関するお詫びとお知らせ,” 17 9 2020. [オンライン]. Available: https://www.home.saxo/ja-jp/about-us/security-incident/personal-information-leakage.

[32] サクソバンク証券株式会社, “個人情報流出についてお客様からお寄せいただいたご質問ならびに回答,” 2020. [オンライン]. Available: https://www.home.saxo/ja-jp/about-us/security-incident/questions-and-answers.

[33] LiveAuctioneers, “July 11, 2020 - LiveAuctioneers Account Security,” 11 7 2020. [オンライン]. Available: https://help.liveauctioneers.com/article/496-july-11-2020-liveauctioneers-account-security.

[34] G. Cluley, “Millions of LiveAuctioneers passwords offered for sale following data breach,” 13 7 2020. [オンライン]. Available: https://grahamcluley.com/liveauctioneers-passwords-for-sale/.

[35] Promo, “Promo Data Breach July 21, 2020 FAQ,” 21 7 2020. [オンライン]. Available: https://support.promo.com/en/articles/4276475-promo-data-breach-july-21-2020-faq.

[36] Bleeping Computer, “Promo.com discloses data breach after 22M user records leaked online,” 27 7 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/promocom-discloses-data-breach-after-22m-user-records-leaked-online/.

[37] Dave, “Notice of Data Breach,” 21 8 2020. [オンライン]. Available: https://www.dave.com/blog/notice-of-data-breach/.

[38] ZDnet, “Tech unicorn Dave admits to security breach impacting 7.5 million users,” 26 7 2020. [オンライン]. Available: https://www.zdnet.com/article/tech-unicorn-dave-admits-to-security-breach-impacting-7-5-million-users/.

[39] ZDnet, “Hackers stole GitHub and GitLab OAuth tokens from Git analytics firm Waydev,” 27 7 2020. [オンライン]. Available: https://www.zdnet.com/article/hackers-stole-github-and-gitlab-oauth-tokens-from-git-analytics-firm-waydev/.

[40] 株式会社NTTデータ, “サイバーセキュリティに関するグローバル動向四半期レポート（2019年7月～9月）,” 株式会社NTTデータ, 29 11 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/-

/media/nttdatajapan/files/services/security/nttdata_fy2019_2q_securityreport.pdf
.

[41] IBM, “IBM、セキュリティーに関する調査レポートを公開,” 25 8 2020. [オンライン]. Available: https://jp.newsroom.ibm.com/2020-08-25-ibm-security-concern-investigation-report-release.

[42] Dunzo, “Your Security is our Top Priority!,” 10 7 2020. [オンライン]. Available: https://medium.com/dunzo/your-security-is-our-top-priority-def5ebe5db12.

[43] SafetyDetectives.com, “US casting site leaks personal data belonging to 260,000+ actors,” 16 7 2020. [オンライン]. Available: https://www.safetydetectives.com/blog/mycastingfile-leak-report/.

[44] 三菱重工業株式会社, “当社グループ名古屋地区のネットワークに対する第三者からの不正アクセスに係る件,” 7 8 2020. [オンライン]. Available: https://www.mhi.com/jp/notice/notice_200807.html.

[45] 朝日インタラクティブ株式会社, “セキュリティ教育機関で2.8万件のデータ侵害、フィッシングが原因に,” 朝日インタラクティブ株式会社, 13 8 2020. [オンライン]. Available: https://japan.zdnet.com/article/35158096/.

[46] 野村證券株式会社, “法人のお客様の情報流出について,” 10 9 2020. [オンライン]. Available: https://www.nomuraholdings.com/jp/news/nr/nsc/20200910/20200910.pdf.

[47] LINE株式会社, “LINEアカウントへの不正アクセスに対する注意喚起,” LINE株式会社, 12 9 2020. [オンライン]. Available: https://linecorp.com/ja/security/article/330.

[48] ＨＪホールディングス株式会社, “Hulu「リスト型アカウントハッキング（リスト型攻撃）」による弊社サービスへの不正ログインの発生について,” 24 9 2020. [オンライン]. Available: https://www.hjholdings.jp/release/20200924.html.

[49] 経済産業省, “サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を策定しました,” 18 4 2019. [オンライン]. Available: https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html.

[50] 情報処理推進機構（IPA）, “サイバーセキュリティお助け隊（令和2年度中小企業向けサイバーセキュリティ対策支援体制構築事業）,” 27 10 2020. [オンライン]. Available: https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html.

[51] 一般社団法人JPCERTコーディネーションセンター, “複数の BIG-IP 製品の脆弱

性 (CVE-2020-5902) に関する注意喚起,” 一般社団法人JPCERTコーディネーションセンター, 14 7 2020. [オンライン]. Available: https://www.jpcert.or.jp/at/2020/at200028.html.

[52] F5, Inc., “K52145254: TMUI RCE vulnerability CVE-2020-5902,” 23 7 2020. [オンライン]. Available: https://support.f5.com/csp/article/K52145254.

[53] M. Klyuchnikov, “Remote Code Execution in F5 Big-IP,” 15 7 2020. [オンライン]. Available: https://swarm.ptsecurity.com/rce-in-f5-big-ip/.

[54] F5, Inc., “Protect Against the BIG-IP TMUI Vulnerability CVE-2020-5902,” 2020. [オンライン]. Available: https://www.f5.com/services/support/big-ip-vulnerability-cve-2020-5902.

[55] Positive Technologies, “F5 fixes critical vulnerability discovered by Positive Technologies in BIG-IP application delivery controller,” 2 7 2020. [オンライン]. Available: https://www.ptsecurity.com/ww-en/about/news/f5-fixes-critical-vulnerability-discovered-by-positive-technologies-in-big-ip-application-delivery-controller/.

[56] Twitter, Inc., “@x4ce Twitterアカウント,” 5 7 2020. [オンライン]. Available: https://twitter.com/x4ce/status/1279790599793545216.

[57] GitHub, Inc., “Add F5 BIG-IP TMUI Directory Traversal and File Upload RCE (CVE-2020-5902),” 6 7 2020. [オンライン]. Available: https://github.com/rapid7/metasploit-framework/pull/13807.

[58] 株式会社ラック, “Apache Struts2 の脆弱性(S2-016)を悪用した攻撃の急増について,” 18 7 2013. [オンライン]. Available: https://www.lac.co.jp/lacwatch/alert/20130718_000168.html.

[59] Bad Packets LLC, “OVER 3,000 F5 BIG-IP ENDPOINTS VULNERABLE TO CVE-2020-590,” 5 7 2020. [オンライン]. Available: https://badpackets.net/over-3000-f5-big-ip-endpoints-vulnerable-to-cve-2020-5902/.

[60] 株式会社ラック, “【注意喚起】F5 BIG-IP製品の任意コード実行可能な脆弱性（CVE-2020-5902）を狙う攻撃活動を観測,” 8 7 2020. [オンライン]. Available: https://www.lac.co.jp/lacwatch/alert/20200708_002231.html.

[61] 一般社団法人JPCERTコーディネーションセンター, “攻撃を目的としたスキャンに備えて 2019年7月,” 一般社団法人JPCERTコーディネーションセンター, 22 7 2019. [オンライン]. Available: https://www.jpcert.or.jp/newsflash/2019072201.html.

[62] F5, Inc., “K13092: Overview of securing access to the BIG-IP system,” 27 3 2019. [オンライン]. Available: https://support.f5.com/csp/article/K13092.

[63] F5, Inc., “K13309: Restricting access to the Configuration utility by source IP address (11.x - 16.x),” 28 10 2020. [オンライン]. Available: https://support.f5.com/csp/article/K13309.

[64] F5, Inc., “K17333: Overview of port lockdown behavior (12.x - 16.x),” 14 8 2020. [オンライン]. Available: https://support.f5.com/csp/article/K17333.

[65] トレンドマイクロ株式会社 , “「BIG-IP」の脆弱性「CVE-2020-5902」を利用するIoTマルウェアを確認,” 18 9 2020. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/26197.

[66] トレンドマイクロ株式会社, “ホームルータや監視カメラ用ストレージシステムを狙うIoTマルウェア：「SORA」と「UNSTABLE」,” 17 2 2020. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/23916.

[67] マクニカネットワークスセキュリティ研究センター, “BIG-IP等のNW機器の脆弱性まとめとSHODANでの観測状況,” 10 7 2020. [オンライン]. Available: https://blog.macnica.net/blog/2020/07/big-ip-nw-shodan.html.

[68] GitHub, Inc., “CVE-2020-5902 IoC Detection Tool,” 22 7 2020. [オンライン]. Available: https://github.com/f5devcentral/cve-2020-5902-ioc-bigip-checker/.

[69] 安藤正芳, “Emotet検出数が前月比8倍の過去最大規模に、フィルタリングを巧妙に回避,” 日経クロステック, 22 10 2020. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/column/18/00001/04747/. [アクセス日: 2020].

[70] 独立行政法人情報処理推進機構, “「Emotet」と呼ばれるウイルスへの感染を狙うメールについて,” 2 9 2020. [オンライン]. Available: https://www.ipa.go.jp/security/announce/20191202.html.

[71] 樋口隆充, “霞が関でパスワード付きzipファイルを廃止へ　平井デジタル相,” ITmedia, 17 11 2020. [オンライン]. Available: https://www.itmedia.co.jp/news/articles/2011/17/news150.html.

[72] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート　2019年度第3四半期,” 株式会社NTTデータ, 28 2 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_3q_securityreport.pdf.

[73] 一般社団法人JPCERTコーディネーションセンター, “マルウェア Emotet の感

染拡大および新たな攻撃手法について,” 一般社団法人JPCERTコーディネーションセンター, 4 9 2020. [オンライン]. Available: https://www.jpcert.or.jp/newsflash/2020090401.html.

[74] L. Mathews, “史上初の身代金ウイルス攻撃による死者、ドイツの病院で発生,” Forbes Japan, 19 9 2020. [オンライン]. Available: https://forbesjapan.com/articles/detail/37142.

[75] 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 6 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2020/062600/062600-01.pdf.

[76] 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,” 11 9 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2020/091101/091101-01.pdf.

[77] Z. Whittaker, “ランサムウェア攻撃によってGarminのサービスが世界的に停止,” Cech Crunch Japan, 26 7 2020. [オンライン]. Available: https://jp.techcrunch.com/2020/07/26/2020-07-25-garmin-outage-ransomware-sources/.

[78] S. Coble, “Cyber-Attack Downs Alabama County's Network,” infosecurity, 9 7 2020. [オンライン]. Available: https://www.infosecurity-magazine.com/news/cyberattack-downs-alabama-countys/.

[79] P. Muncaster, “Telecom Argentina Has Tuesday Deadline to Pay $7.5m Ransom,” infosecurity, 21 7 2020. [オンライン]. Available: https://www.infosecurity-magazine.com/news/telecom-argentina-tuesday-75/.

[80] Security Affairs by Pierluigi Paganini, “Spanish state-owned railway infrastructure manager ADIF infected with ransomware,” 24 7 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/106304/cyber-crime/adif-revil-ransomware-attack.html.

[81] Bleeping Computer LLC, “Canon confirms ransomware attack in internal memo,” 6 8 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/canon-confirms-ransomware-attack-in-internal-memo/.

[82] ニュースガイア株式会社, “テレワーク環境でマルウェア感染、社内に拡大 - 三菱重工,” ニュースガイア株式会社, 11 8 2020. [オンライン]. Available: http://www.security-next.com/117404.

[83] Security Affairs by Pierluigi Paganini, “Sodinokibi ransomware gang stole 1TB of data from Brown-Forman,” 16 8 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/107190/data-breach/sodinokibi-ransomware-brown-forman.html.

[84] ニュースガイア株式会社, “ランサムウェアに感染、障害が発生 - 経済同友会,” ニュースガイア株式会社, 26 8 2020. [オンライン]. Available: https://www.security-next.com/117841.

[85] ニュースガイア株式会社, “マルウェアに感染でなりすましメール - 浄水器販売会社,” ニュースガイア株式会社, 3 9 2020. [オンライン]. Available: https://www.security-next.com/118027.

[86] Z. Whittaker, “サイバー脅威スタートアップのCygilantがランサムウェア「NetWalker」に襲われる、身代金は支払い済みか,” TechCrunch Japan, 5 9 2020. [オンライン]. Available: https://jp.techcrunch.com/2020/09/05/2020-09-03-cygilant-ransomware/.

[87] Bleeping Computer LLC, “Netwalker ransomware hits Pakistan's largest private power utility,” 8 9 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-pakistans-largest-private-power-utility/.

[88] Bleeping Computer LLC, “Leading U.S. laser developer IPG Photonics hit with ransomware,” 18 9 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/leading-us-laser-developer-ipg-photonics-hit-with-ransomware/.

[89] 株式会社中日新聞社, “危険です、ＳＭＳ認証代行　アプリ利用時など不正横行　ツイッターで県警警告,” 株式会社中日新聞社, 6 10 2020. [オンライン]. Available: https://www.tokyo-np.co.jp/article/59964.

[90] BlueVoyant, “Global Insights: Supply Chain Cyber Risk,” 2020.

[91] 株式会社グローバルインフォメーション, “サイバーセキュリティの市場規模、COVID-19の影響で2020年の年間成長率CAGR1.83%に鈍化 2023年にはV字回復しCAGR11.02%で成長予測,” 株式会社グローバルインフォメーション, 3 8 2020. [オンライン]. Available: https://www.value-press.com/pressrelease/249866.

[92] 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,” 11 9 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2020/091101/091101-01.pdf.

[93] 経済産業省, “サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）が設立されます （METI/経済産業省）,” 経済産業省, 30 10 2020. [オンライン]. Available: https://www.meti.go.jp/press/2020/10/20201030011/20201030011.html.

[94] Trend Micro Inc., “1H 2020 Cyber Security Defined by Covid-19 Pandemic,” Trend Micro Inc., 15 9 2020. [オンライン]. Available: https://www.trendmicro.com/en_us/research/20/i/1h-2020-cyber-security-defined-by-covid-19-pandemic.html.

[95] Trend Micro Inc., “Developing Story: COVID-19 Used in Malicious Campaigns,” Trend Micro Inc., 11 11 2020. [オンライン]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains.

[96] 株式会社日本経済新聞社, “チャートで見る世界の感染状況,” 株式会社日本経済新聞社, 2020. [オンライン]. Available: https://vdata.nikkei.com/newsgraphics/coronavirus-chart-list/.

[97] 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,” 株式会社NTTデータ, 26 6 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2020/062600/062600-01.pdf.

NTT DATA
Trusted Global Innovator

2020年12月11日発行

株式会社NTTデータ
セキュリティ技術部
大谷 尚通 / 小林 義徳 / 大石 眞央 / 山下 大輔
星野 亮 / 宮崎 大輔 / 伊藤 明宏 / 木下 盾 / 片井 拓弥 / 宍戸 りさ / 清水 一貴 / 工藤 完太郎
nttdata-cert@kits.nttdata.co.jp