NTT DATA
Trusted Global Innovator

グローバルセキュリティ動向四半期レポート

2019 年度 第 1 四半期

NTT DATA
Trusted Global Innovator

目次

1. エグゼグティブサマリー

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

ドメイン名ハイジャック

攻撃者によりドメインを乗っ取られる攻撃「ドメイン名ハイジャック」によって、著名なアニメの公式サイトから不審なサイトへ誘導される事例が大きな話題となりました。既存の手法と異なり、JPドメイン特有のドメイン移管手続きを悪用していたことが特徴的でした。

継続して確認されるWebスキミング

2018年度第4四半期から継続して、脆弱なECサイトを改ざんし決済情報を窃取する「Webスキミング」による被害が多く確認されました。標的となるECプラットフォームの種類も以前より増加しているため、ECストアは攻撃を受けるリスクが高まっている状態です。

BlueKeep | Windowsリモートデスクトップサービスの脆弱性

脆弱性関連で大きく話題になったのは、Microsoft社が「WannaCry」と同様のリスクがあるとして公開したWindowsリモートデスクトップサービスの脆弱性でした。この脆弱性は「BlueKeep」とも呼ばれ、多くの組織から注意喚起がされました。特別措置として、サポート外のバージョンに対してもパッチ提供が行われました。

今後の予測

2019年度第2四半期は、2019年度第1四半期と同様に金銭と直接つながるサイバー攻撃の増加が予測されます。2018年度第4四半期、2019年度第1四半期と続いているWebスキミングはこのまま継続し続けると考えます。
米国の複数都市で発生したランサムウェア攻撃は、セキュリティ対策が十分ではない地方自治体を狙ったと考えられます。今後は米国のみではなく、各国の地方自治体でのランサムウェアによる攻撃が増加することが懸念されます。

2. 注目トピック

2.1. ドメイン名ハイジャック

ドメイン名ハイジャックとは、不正な手法により本来は管理権限を持たない攻撃者が既存のドメイン名を乗っ取る攻撃です。攻撃者は乗っ取ったドメイン名をC&Cサーバやマルウェア配布サーバ、フィッシングサイトなどの悪質なサーバへ割り当てます。攻撃者は乗っ取ったドメインへアクセスした利用者にマルウェアをダウンロードさせたり、フィッシングサイトでログイン情報を入力させたりするサイバー攻撃を仕掛けることができます。
これまでよく知られているドメイン名ハイジャックの手法は、下記の3つがあります [1]。

1. 攻撃者はドメイン名登録者や管理担当者になりすまし、レジストリ(ドメイン名管理機関)[1]に登録されているドメイン情報を不正に書き換える
2. 攻撃者は権威DNSサーバの脆弱性を悪用して、権威DNSサーバへ不正にログインしたり、不正なドメイン情報を送信して登録したりしてドメイン情報を書き換える
3. 攻撃者はDNSプロトコルの脆弱性を悪用することで、キャッシュDNSサーバへ不正なドメインデータを送信して、偽のドメイン情報をキャッシュさせる(DNSキャッシュポイズニング)

しかしながら、この2019年度第1四半期に話題となったドメイン名ハイジャックはこれらのよく知られている手法と異なり、レジストラ[2]間のドメイン名移管手続きを悪用して不正にレジストリのドメイン情報を書き換える手法でした。表 1にこの手法を用いたドメイン名ハイジャック事例一覧を示します。

[1] トップレベルドメイン毎に登録された全てのドメイン情報をデータベースで維持管理する機関 [106]。1つのトップレベルに1つのレジストリが存在します。例えば「.com/.net」はVeriSign、「.jp」はJPRSが管理しています。
[2] 登録者からドメイン情報の申請に基づいて、レジストリのデータベースへ登録する指定業者です [107]。レジストラはインターネットのIPアドレスやドメイン名などの資源管理を行っている非営利団体「ICANN：The Internet Corporation for Assigned Names and Numbers」に認定を受けなければなりません。

表 1:移管手続きを悪用したドメイン名ハイジャック事例一覧

No	日付	影響を受けたドメイン名	概要
1	2018年9月	amusecraft.jp	ゲーム制作会社ソフパルが運営するゲームソフト開発事業部のドメイン名が乗っ取られ、ドメインが第3者に譲渡された旨が当該サイトに表示される [2] [3]。
2	2019年2月	syrup-soft.jp	ゲーム制作会社クラインのブランドのドメイン名が乗っ取られ、解散のお知らせが当該サイトに表示される [4] [5]。
3	2019年2月	sukumizu.jp	同人サークル駿河電力のサイトのドメイン名が乗っ取られる [6]。
4	2019年4月	lovelive-anime.jp	アニメ"ラブライブ!"シリーズ公式サイトのドメイン名が乗っ取られ、"ラブライブは我々が頂いた!"というメッセージ記載のサイトが表示される [7] [8]。

表 1のいずれの事例も"○○○.jp"という形式の汎用JPドメイン名が不正に書き換えられて被害を受けています。No.1やNo.4の事例において、ドメイン名の乗っ取り後にそのドメイン名のトップページにて移管されたことを示すメッセージが表示された(図 1参照)ことから、汎用JPドメイン名を移管する手続きに特有の事象を悪用して乗っ取ったと考えられます。

ドメイン名が乗っ取られる前
公式Webサーバによる表示

ドメイン名が乗っ取られた後
別サーバへ誘導された時の表示

図 1:ドメイン名ハイジャックによるラブライブ!公式サイトの変化

下記および図 2にてその手法について説明します。

1. 攻撃者は自らが利用するレジストラ(A)において、乗っ取りたいJPドメイン名の移管申請を行う
2. 申請を受け付けたレジストラ(A)は、JPドメインのレジストリである株式会社日本レジストリサービス(JPRS[3])へドメイン名の指定事業者変更申請を行う
3. JPRSは申請が行われたドメイン名の登録者が利用するレジストラ(B)に対して、移管承認の意思確認を依頼する
4. レジストラ(B)もしくはそのレジストラ(B)から移管承認の意思確認の依頼を受けたドメイン名登録者が、返答しないで10日以上放置する、もしくは誤って移管を承認してしまう
5. JPRSは移管を承認し、ドメイン名は攻撃者に移管される。攻撃者は乗っ取りに成功する。

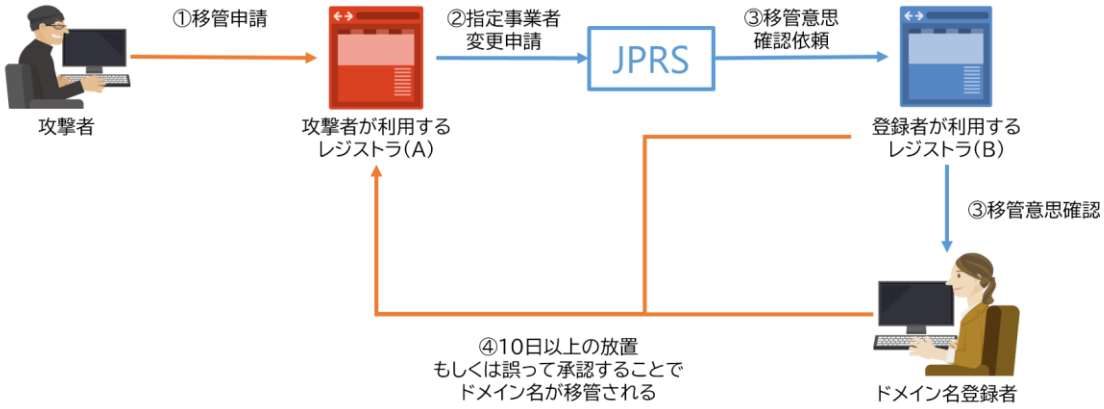


図 2:移管手続き悪用によるドメイン名ハイジャックの流れ
(NTTDATA-CERTにて作成)

[3] 株式会社日本レジストリサービス。JPドメイン名の登録管理とJP DNSの運用を行っている。

このJPドメインの移管手続きにおいて、移管意思確認の回答を10日以上放置すると自動的に承認されることは大きな問題です。この自動承認の規則はJPRSの「汎用JPドメイン名登録申請等の取次に関する規則」の第11条第2項に下記の通りに定められています [9]。

> *当社が、指定事業者に対して登録者の意思確認等を依頼した場合、指定事業者がその依頼のときから10日以内に登録者がその意思を有しない旨の回答をしない場合には、指定事業者において登録者の意思確認等を行い、登録者がその意思を有する旨の回答を得たものとみなす。*

上記の通り本規則は、レジストリ(JPRS)とレジストラ(指定事業者)の間の取り決めであり、レジストラとドメイン名登録者間の取り決めはレジストラによって異なります。あるレジストラは、事前にドメイン名登録者からレジストラへ転出する申し出がない場合は、JPRSからの移管意思確認へ不承認を返答するとしています。
しかしながら、表 1に示したとおり、不正移管の手法を使ってドメイン名が乗っ取られる事例が発生しています。ドメイン名登録者は自らが管理するドメインを乗っ取り攻撃から守るために、下記に示す管理体制の強化や各レジストラが提供するサービスの利用等を推奨します。これらの施策によりミスによる誤承認のリスクを低減することが可能です。

- ドメイン名の管理者は、常に連絡を行える状態を保つ。ドメイン名の管理者を複数人で担当し、異動や連絡先の変更による連絡ミス、誤承認のリスクを低減する。
- 利用しているレジストラのドメイン移管手続きを事前に確認する。手続きに問題があれば、対策を検討する。
- 定期的に自組織で保有しているドメイン名の登録状況を点検する
- 「ドメインロック」と呼ばれる登録情報を不用意に変更できないレジストラのサービスを利用する

ドメイン名は、ITサービス提供の根幹となる重要なパーツであるとともに、企業のブランドイメージとしての側面もあります。企業は、自社が保有するドメインを一括して把握できているほうがよいでしょう。この機会をきっかけにドメイン管理について一考することを推奨します。

2.2. 侵入口となるIoT機器

IoTとは"Internet of Things"(日本語訳：モノのインターネット)の略称です。従来のインターネットはコンピュータ同士が接続するためのものでしたが、IoTはテレビやカメラなどの家電や温度計、電力計などのセンサーに代表されるあらゆるモノがインターネット経由で通信することを意味します。昨今ではIoT機器の性能向上はめざましく、音声操作に対応したAIアシスタント機能を有するスマートスピーカーやRaspberry Piに代表されるDIYでIoT機器を作成可能な小型Linuxキットなどが登場しています。
IoT機器の普及によって、世の中がより便利になっていく反面、常にネットワークに接続されているIoT機器は、セキュリティをより一層注意していかねばなりません。スマートスピーカーの内部で使われているチップセットは数年前のスマートフォンと同等以上の性能があり [10]、Raspberry Piに至ってはコンピュータそのものであるため、IoT機器をさまざまに悪用することが可能です。攻撃者にとって、IoT機器は攻撃する価値のある対象となっています。2016年に登場し、脆弱な設定のIoT機器に感染し大規模なDDoS攻撃を行ったマルウェア「Mirai」は [11]、2019年度第1四半期においても新たな亜種が発見されるほどの脅威であり続けています [12]。
従来のIoT機器のインシデント事例は、IoT機器自体が持つ情報が漏洩したり [13]、DDoS攻撃を行うボットネットに組み込まれたりとIoT機器自体が攻撃のターゲットでした。しかし、2019年度第1四半期にはIoT機器を侵入口として組織の内部ネットワークへ侵入して機密ファイルを盗んだ事例が報告されました。

2019年6月18日にアメリカ航空宇宙局(NASA)は、2018年4月に攻撃者が内部ネットワークへ侵入して火星科学研究探査機のデータを含むジェット推進研究所(JPL)の研究データのファイル(23ファイル、合計500MB以上)が窃取されたことを報告書にて公開しました [14]。同報告書によると、攻撃者はJPLの内部ネットワークに無許可で接続されたRaspberry Piを踏み台にして、内部ネットワークに侵入しました(図 3参照)。その後、約10ヶ月の間潜伏し、ネットワーク内の脆弱性を悪用してデータを盗み出しました。

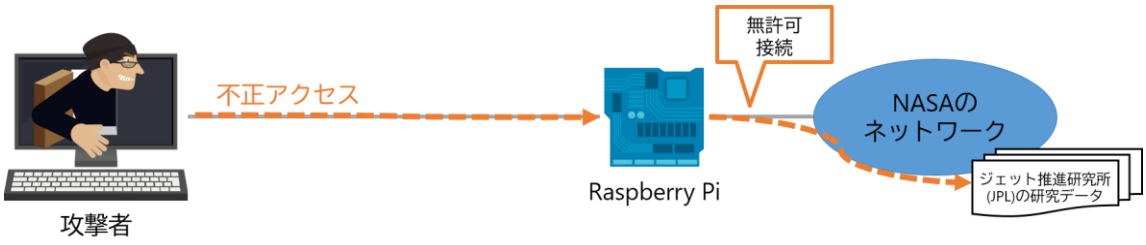


図 3:内部ネットワークへの侵入イメージ図(NTTDATA-CERTにて作成)

侵入口として使われたRaspberry Piは、本来ならば事前にセキュリティデータベース(ITSDB)に登録され、最高情報責任者室(OCIO)によるセキュリティレビューと許可を受けなければ、内部ネットワークへ接続してはいけないものでした。しかしながら、このセキュリティデータベースは不具合により更新できないことがしばしば発生し、登録を後回しにしたために、そのまま機器の登録を忘れてしまうことがあると報告されています(図 4参照)。そのため、ネットワークに接続されている機器を把握・管理することができていませんでした。報告書内では、他にもシステムの脆弱性が半年も放置されていたことや内部ネットワークが適切にセグメントで区切られていなかったことなどの問題点も指摘されています。

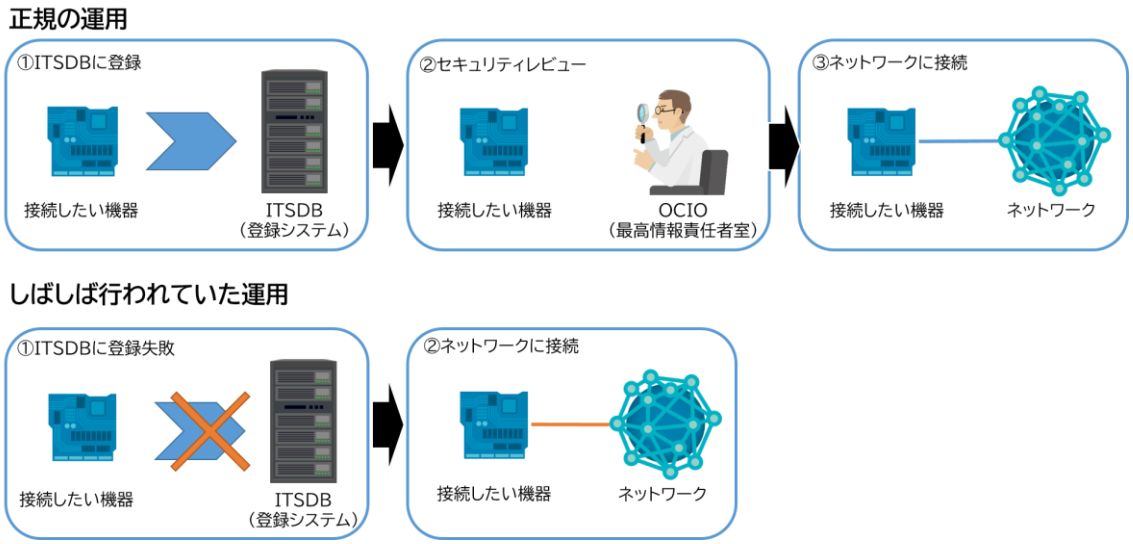


図 4：NASAで行われていた機器管理運用(NTTDATA-CERTにて作成)

NASAは、今回の事件の主な原因は標的型攻撃と報告していますが、報告書内で指摘されていた問題点は、他の組織においても発生しているおそれが十分にある問題点です。
1つ目の問題点は、内部ネットワークに接続されている機器を把握していなかったことです。今回の事例のように不正侵入の原因となったネットワーク接続機器が管理されていない場合は、不正侵入の発見や原因特定が遅れる要因になります。前述のとおり、IoT機器も攻撃対象となることから、今後は既存のPCやサーバと同様にIoT機器も管理すべきです。
2つ目の問題点は、セキュリティ維持のための運用手順が決まっていたにも関わらずそれが守られていなかったことです。今回の事例においても運用手順が守られていれば、1つ目の問題点は発生しませんでした。実際には、セキュリティデータベースの不具合により運用手順が煩雑になり、勝手に省略された運用がされていたことが原因でした。この問題は2016年のセキュリティカンファレンス「CODE BLUE」の基調講演においても"行動を制限しようとする防御は容易に迂回されてしまう"と指摘されています [15]。加えて、それが大きなインシデントの要因となることが多いとも言及されています。そのため、セキュリティ対策を導入する際は、よりユーザに不便を強いない、ユーザの手動操作に頼らないで安全性を確保で

きる対策を選択すべきだと思います。例えば今回の事例では、Raspberry Piがネットワークに接続された段階で自動的に一時的に隔離ネットワークに接続されて、セキュリティデータベースへ情報が登録されるなど、ユーザの手動操作を介さない仕組みが望ましいです。

3. 情報漏えい

2019年度第1四半期も情報漏えい関連の事例が数多く報告されました。日本国内でも、複数の企業が不正アクセスを受けて情報が流出した旨を報告しています。なかには、パスワードリスト型攻撃を受けたとされる事例もあり、2018年度第4四半期のレポートで予測したようにリスト「Collection #1」をはじめとする大規模情報漏えいにより流出した情報が悪用されているおそれがあります [16]。2018年度第4四半期にダークウェブ上で大量の個人情報販売を計4回行った「Gnosticplayers」と呼ばれる攻撃者は、4月にも6,550万件の情報を販売目的で公開しました [17]。
2018年度第4四半期のレポートで予測した通り、Webスキミング関連の事例が増加しています。また、データベースシステムの設定不備による情報漏えいが目立ちました。これらの事例について以下にまとめます。

3.1. 継続して確認されるWebスキミング

Webスキミングと思われる攻撃による被害が、複数確認されています。Webスキミングは2018年から攻撃が増加し、攻撃手法も巧妙化しています。2019年度第1四半期には、新たな攻撃グループや、「Magento」以外の新たなECサイト構築用プラットフォームが標的にされていることが確認されました。以前から話題となっている「Magento」への攻撃手法も改良されています [18]。いま攻撃者は、ECサイト構築用プラットフォームを狙って攻撃を行っています。ECサイトを運営する企業は、今後もより一層の注意が必要です。
セキュリティ企業 TrendMicro社はWebスキミングを行う新たな攻撃グループについて報告しています [19]。対象の攻撃グループは「Mirrorthief」と呼ばれています。Mirrorthiefは、大学が運営しているオンラインストアを攻撃し、米国とカナダの201の大学が被害に遭いました。これらの大学は、PrismRBS社が開発した大学向けのECサイト構築用プラットフォーム「PrismWeb」を使用していました。Mirrorthiefは、PrismWeb上で使用されるJavaScriptライブラリにスクリプトを注入してWebスキミングを行いました。この事例のように、攻撃者がECサイト構築用プラットフォームやライブラリを攻撃した場合、一度に複数のオンラインストアへ影響が及び、大きな被害につながります。

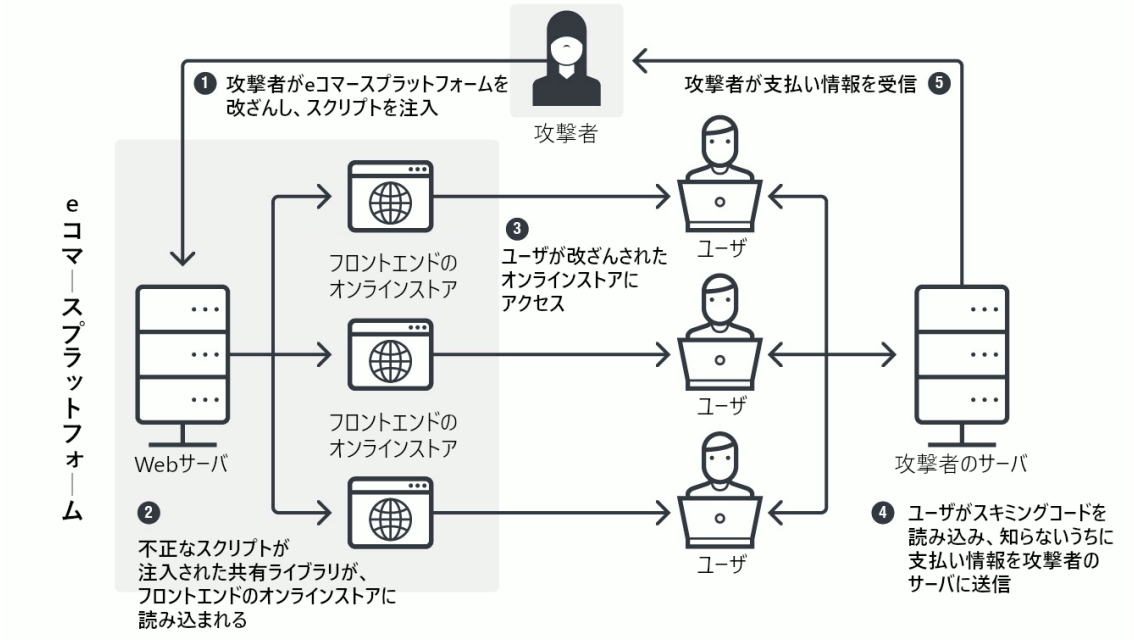


図 5:新しいWebスキミングの流れ
(トレンドマイクロセキュリティブログより引用 [20])

標的となるECサイト構築用プラットフォームの増加も確認されています。セキュリティ会社のRiskIQ社は、5月1日に同社Webサイトにて「Magent」以外にも「OpenCart」や「OSCommers」といったプラットフォームが狙われていると報告しました [21]。我々は、2018年度第4四半期のレポートにて、日本国内のシェアが高いECサイト構築用プラットフォームが狙われた場合は、国内でも被害が増加すると予測しました。5月9日に株式会社イーシーキューブは、自社公式Webサイトにて注意喚起「【重要】サイト改ざんによるクレジットカード流出被害が増加しています」を掲載しました [22]。イーシーキューブ社が提供するECサイト構築用プラットフォーム「EC-CUBE」は、日本国内で最も多く使用されているECサイト構築用プラットフォームです。注意喚起によると、特に「EC-CUBE」のVersion 2の系列について攻撃を受けるおそれがあり、実際に複数の被害が発生しています。「EC-CUBE」を使ってECサイトを運用している組織は、使用しているバージョンやセキュリティ対策の確認が必要です。
イーシーキューブ社の注意喚起 [22]は、セキュリティ対策が不十分な場合に攻撃を受けて被害が発生するおそれがあると述べており、チェック事項と対策方法を示しています。以下にイーシーキューブ社が出した注意喚起の文書中の具体的なチェック事項と対策方法を転載します。

表 2：EC-CUBE 具体的なチェック項目と対策方法
(EC-CUBE公式サイトより引用 [22])

1. 既に「改ざん」が行われていないか

下記のような「改ざん」の疑いが見つかった場合は、直ちにサイトを停止し、詳しい方にご相談ください。

- 購入確認画面等に覚えのない JavaScript が設置されていないか
- 購入フローのクレジットカード入力画面が不正な URL になっていないか

2. 管理画面のURLが/admin/など推測されやすいURLになっていないか

管理画面の URL を変更せず /admin/ のままで運用していた場合、攻撃者が管理画面にアクセスしやすい状況になっておりますので、早急に変更をお願いします。EC-CUBE2.11 以降のバージョンでは、管理画面のURL がインストール時やインストール後の管理画面から変更が可能です。

管理画面の URL を変更する方法は、設定変更方法資料「2. 管理画面の URL を変更する方法」をご確認ください。

3. 管理画面へのアクセス制限が行われているか

管理画面のログイン画面に外部から容易にアクセスできる状態ですと、パスワードの総当たり攻撃等で、管理画面にログインされる可能性がございます。

特に、管理画面 URL が/admin/で外部からのアクセスもできる状態ですと、攻撃されやすい状態でございますので、早急に管理画面に部外者がアクセスできないよう対策をお願いします。

- IP 制限をかける（外部からは全くアクセスできない状態にする）
- Basic 認証をかける（管理画面にパスワードをかける）

管理画面へのアクセス制限については、設定変更方法資料「3. 管理画面へのアクセス制限」をご確認ください。

4. EC-CUBEの公開されるべきでないディレクトリが公開されてしまっていないか

EC-CUBE の /data ディレクトリや /install といったディレクトリが運用環境で公開されている場合、そこから管理画面へのアクセス情報やバックアップファイル、アップロードした CSV ファイルなどが流出する恐れがあります。

インストール完了後の/install の削除、/data ディレクトリへのアクセス制限を行なってください。

参考） https://nob-log.info/2013/05/25/wrong-installation-eccube-is-dangerous/

/data ディレクトリのアクセス拒否設定については、設定変更方法資料「4. Data ディレクトリへのアクセスを拒否する方法」をご確認ください。

5. 御利用のサーバーや利用しているCMS等のセキュリティが担保されているか

御利用のサーバーの OS やミドルウェアの脆弱性が対応されているかサーバー管理者にご確認ください。

WordPress や Drupal などの CMS やその他のファイル操作やデータベースへの接続を行うアプリケーションをインストールしている場合は、各アプリケーションやプラグインの脆弱性が対応されていることもあわせてご確認ください。

表 2の1に記載があるように、未然防止のセキュリティ対策だけでなく、既に不明なJavaScriptが設置されている等の改ざんの有無を定期的に確認してください。また、被害に遭わないためにはECサイト構築用プラットフォームを含む周辺環境で基本的なセキュリティ対策を徹底することが重要です。表 2の5は、OSやデータベース、CMSなどの脆弱性が悪用され、結果としてECサイト改ざんにつながるケースを示しており、攻撃者がECサイトの改ざんに至るまでの侵入経路は複数存在します。ECサイト構築用プラットフォームのみでなく、利用している環境すべてにおいてセキュリティ対策が必要です。

3.2. データベースの設定不備による情報漏えい

2019年度第1四半期はデータベースの設定不備による情報漏えいが多く報告されました。設定不備によりデータベース内の機密情報が不用意に公開されただけでなく、攻撃者がそのデータベースへ侵入して機密情報を詐取したあとにデータを削除し、復元のための金銭を要求するといった攻撃事例も発生しています。

5月17日にコンピュータヘルプサイト Bleeping Computerが公開した記事によると、たった3週間で12,000ものインターネット上のMongoDBからデータが削除されました [23]。データベース内には、データ復元の脅迫メッセージと攻撃者の連絡先のみが残されていました。

また、4月から5月にかけてGitHubやGitLabにおいても、不正アクセスにより情報が削除されて、金銭を要求された事例が複数発生しました [24]。GitHubやGitLabは、ソフトウェア開発や保守においてソースコード等の情報を一元管理するクラウド上のリポジトリシステムです。

データベースシステムも、クラウド上のリポジトリシステムも、アクセス制限を正しく設定する、認証情報を正しく管理するといったセキュリティ対策を徹底しましょう。

2019年度第1四半期に設定不備から攻撃を受けた事例を表 3にまとめます。

表 3：DB設定不備の事例

日付	概要	件数
4/16	インド大手検索サービス提供会社JustDialのデータベースが公開状態にあり、2015年から個人情報にアクセス可能であったと報道された [25]。	1億件
4/18	「doroshke-invoice-production」というMongoDBが公開状態で発見された [26]。イランのタクシーアプリ「Tap30」の運転手の情報が含まれていた。	670万件
4/18	LinkedInのユーザ情報を格納する8個のデータベースが公開状態で発見された [27]。データサイズの合計は229GBであった。	6,000万件
4/29	米国の世帯の最大65%に影響するとされる公開状態のデータベースが発見された [28]。大規模かつ個人に直接つながる情報漏えいであるため危険である。	8,000万件
5/9	SMSでスパムメッセージを送る攻撃者がMongoDBを公開状態にしていた [29]。標的候補と思われるユーザの情報が取得可能な状態となっていた。	8,000万件
5/13	TZ Insurance Solutions が運営するWebサイト「MedicareSupplement.com」に属する公開状態のMongoDBが発見された [30]。個人情報および詳細な健康状態が含まれていた。	500万件
5/14	公開状態にあるElasticSearchデータベースが発見され、パナマ国民の約90%を特定できる情報が保存されていた [31]。	340万件
5/16	公開状態にあるElastiSearchデータベースが発見され、米国の無料商品サンプルや懸賞、その調査に参加した個人の情報が取得可能な状態にあった [32]。	800万件
5/20	Instagramのアカウント情報を格納するデータベースが公開状態で発見された [33]。著名人やブランドの公式アカウント等も含まれていた。	4.900万件
5/24	権原保険サービスなどを提供するFirst American FinancialのWebサイトで口座情報、社会保障番号、免許証画像、納税記録等が閲覧可能であった。 [34]	8億8,500万件

4. 脆弱性

2019年度第1四半期は、数多くの脆弱性が報告されました。2018年度第4四半期とくらべて437件増の5,207件が報告されています [35]。なかでも危険度の高いOracle WebLogic ServerとWindowsリモートデスクトップサービスの脆弱性が話題となりました。

4.1. Oracle WebLogic Server の脆弱性

2019年度第1四半期は、Oracle WebLogic Serverの脆弱性について多くの話題がありました。Oracle社は、4月16日に四半期に1度のCritical Patch Updateを公開しました [36]。4月17日、4月のCritical Patch Updateに含まれていないOracle WebLogic Serverの脆弱性（CNVD-C-2019-48814）が中国の脆弱性情報データベースCNVD（China National Vulnerability Database）に登録され [37]、ゼロデイ脆弱性として話題になりました。4月25日には、この脆弱性（CNVD-C-2019-48814）の攻撃コードが公開されました。4月26日、Oracle社は、定例外のタイミングで、この脆弱性（CVE-2019-2725）を正式に発表し、修正パッチを提供しました [38]。6月15日に中国のセキュリティ企業 KnownSec 404 Teamによって、また新たなOracle WebLogic Serverの脆弱性が報告されました [39]。6月18日、Oracle社からこの脆弱性（CVE-2019-2729）が定例外で公開されました [40]。この脆弱性（CVE-2019-2729）は、当初、CVE-2019-2725の修正漏れと発表されていましたが、Oracle社は6月18日のブログ記事でCVE-2019-2725とは別の脆弱性であると訂正しました。

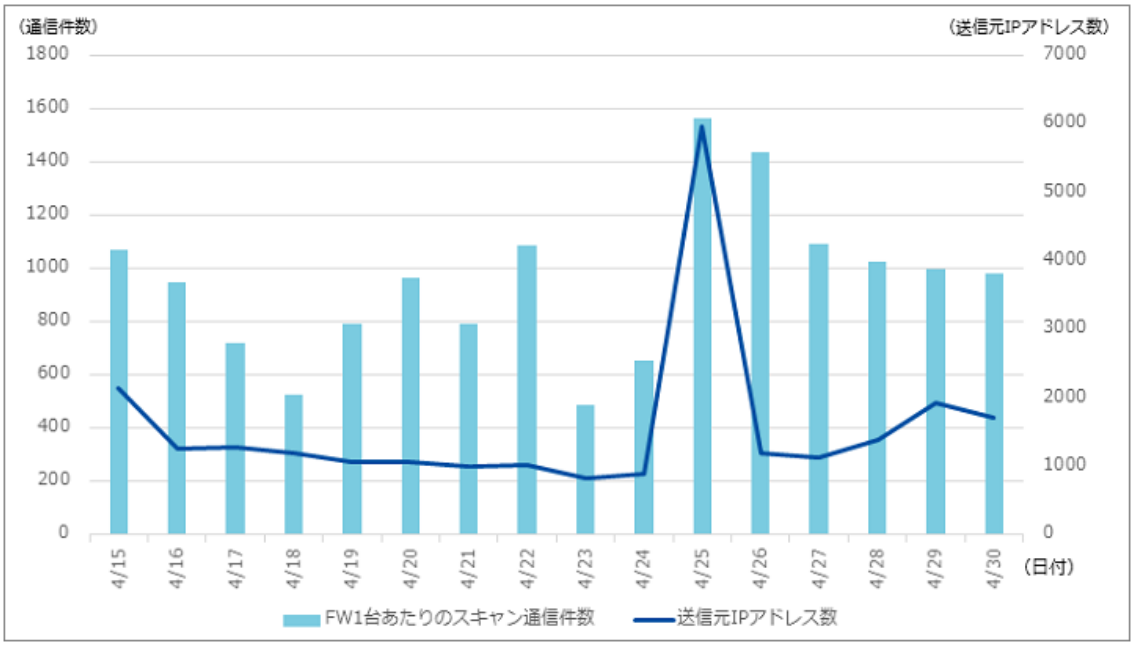


図 6:7001/tcpを宛先とするスキャン通信件数と送信元IPアドレス数
（wizSafe Security Signalより引用 [41]）

インターネットイニシアティブ（IIJ）社の調査結果 [41]よると、4月25日のOracle WebLogic Serverの脆弱性（CVE-2019-2725）を狙った攻撃コードの公開に起因して、攻撃者の活動が活発化しました。図 6より、通常時の7001/tcpを狙ったポートスキャン数と比較して、4月25日はポートスキャン数が増加し、ポートスキャンの送信元IPアドレス数が約9倍に増加しています。また、翌26日には、脆弱性悪用によりOracle WebLogic Server上にコインマイナープログラムをアップロードし、攻撃者がユーザをこのURLへ誘導してダウンロードさせる攻撃が発生しました。

図 7:概念実証コードのリクエストとそのレスポンス
（NTTデータ先端技術株式会社公式サイトより引用 [42]）

攻撃手法の詳細はNTTデータ先端技術株式会社より解説記事が公開されています [42]。脆弱性（CVE-2019-2725）への攻撃では、Oracle WebLogic Serverの管理コンソール用に使用するポート（TCP 7001番）に対して不正なHTTP POST リクエストを送信し、任意のOSコマンドの実行を試みます。図 7は、攻撃対象サーバに対して送信された不正なリクエストと攻撃対象サーバからのレスポンスを示したものです。青線部分は、攻撃者が「cat /etc/passwd」を実行して、その結果をOracle WebLogic の「wls9_asyncコンポーネント」が使用しているディレクトリ配下へ、ファイル名「favicon.ico」として保存させるOSコマンドです。このOSコマンドは、Oracle WebLogic Serverのプロセスと同等の権限で実行されます。

4.2. リモートデスクトップサービスの脆弱性

5月14日、Microsoft社はリモートデスクトップサービスにおける脆弱性（CVE-2019-0708）のセキュリティ更新プログラムを公開しました [43]。「BlueKeep」とも呼ばれるこの脆弱性を悪用すれば、攻撃者は、細工したリクエストをリモートデスクトップ接続用の通信経由で送信することで、遠隔から認証なしで任意のコードを実行できるおそれがあります。また、Microsoft社はブログ記事にて、「この脆弱性を悪用するワームは、2017年のWannaCryが世界中に広がった事案と同様に、脆弱なコンピュータから脆弱なコンピュータへ増殖するおそれがある」と述べました [44]。Windows XPやWindows 2003 Serverといったサポート切れのOSについても緊急でセキュリティ更新プログラムが提供されたことからも、脆弱性の危険度が高いことが伺えます [45]。様々なセキュリティ組織が注意喚起を行ったため、大きな話題となりました。当該脆弱性に関連する出来事を表 4に示します。

表 4：脆弱性「BlueKeep」関連の出来事

日付	組織	概要
5/14	Microsoft	リモートデスクトップサービスの脆弱性「BlueKeep」(CVE-2019-0708)を公開 [44]。WannaCry同様のワーム型マルウェアに悪用が可能であると記載。Windows 7、Windows Server 2008 R2、Windows Server 2008のみでなく、特別措置としてサポート対象外のWindows XP、Windows Server 2003についてもセキュリティ更新プログラムが提供され話題となった。
5/24	Microsoft	サポート対象外のWindows Vistaについてもセキュリティ更新プログラムを提供 [45]。
5/28	Errata Security	100万台のコンピュータに脆弱性が残存しているというスキャン結果を報告 [46]。
5/30	Microsoft	セキュリティ更新プログラムの適用を再度呼び掛けた [47]。Errata Security社のスキャン結果報告を受けて注意喚起を公式ブログ上で実施。WannaCryで悪用された攻撃ツールEternalBlueを例に出し、当該脆弱性の危険性を訴えた。
6/4	NSA	米国安全保障局（NSA）が脆弱性「BlueKeep」について注意喚起を実施した [48]。NSAが一般市民向けの注意喚起を公表することは極めて異例であり、話題となった。
6/7	Morphus Labs	「GoldBrute」と呼ばれるボットネットによる150万台のRDPサーバを標的としたブルートフォース攻撃が発見された [49]。脆弱性「BlueKeep」について多くの組織が警告を行っていることもあり、注目された。
6/17	CISA	米国土安全保障省のサイバーセキュリティ部門(CISA)は、脆弱性「BlueKeep」がWindows VistaやWindows 2000にも存在すると公表 [50]。Windows 2000について実際に悪用可能であることを確認したと報告。

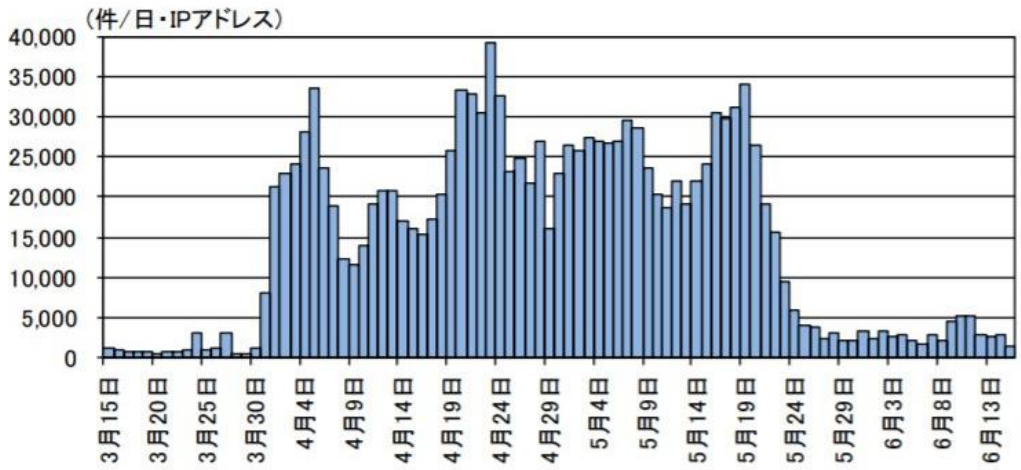


図 8:リモートデスクトップサービスを標的としたアクセス件数の推移
（H31.3.15~R1.6.15）
(警察庁@policeより引用 [51])

図 8は、リモートデスクトップサービスにおける脆弱性「BlueKeep」（CVE-2019-0708）を標的としたアクセス数の増加を表したグラフです [51]。図 3の3月下旬から5月下旬にかけて、アクセス数が増加していることがわかります。
脆弱性「BlueKeep」は、WannaCryと同様のワームに悪用可能とされて大きな話題となりました。WannaCryが悪用した脆弱性については、脆弱性情報公開からセキュリティ更新プログラム公開までに期間があり、注意喚起はさらに後に実施されました。対して脆弱性「BlueKeep」については、脆弱性とセキュリティ更新プログラムを同時に公開し、公開したタイミングから数多くの注意喚起が実施されました。現時点で当該脆弱性に関係した大きな被害やマルウェアの報告はなく、セキュリティ組織による注意喚起と各組織の対応が成功しているといえます。

4.3. その他の脆弱性

以下に2019年度第1四半期のゼロデイ脆弱性と悪用された脆弱性の一覧を示します。

表 5:2019年度第1四半期に報告されたゼロデイ脆弱性

日付	製品名	脆弱性番号	概要
4/9	Windows	CVE-2019-0803 CVE-2019-0859	Microsoft社が4月の月例パッチで2件のゼロデイ脆弱性に対処 [52] [53]。どちらも「Win32k」に影響する特権昇格の脆弱性。
5/10	Whats App	CVE-2019-3568	Facebook社がWhatsAppの脆弱性に対処するためのセキュリティ勧告をリリース [54]。脆弱性が悪用されるとデバイスを制御されるおそれがある。
5/24	Windows Internet Explorer	-	Zscaler社のセキュリティ研究者がWindowsのローカル特権昇格の脆弱性2件、IEのSandboxバイパスの脆弱性1件を報告 [55]。攻撃コードも同時に公開された。
5/24	macOS	-	Intego社がソフトウェアの起動を許可する「Gatekeeper」のバイパスが可能なmacOSのゼロデイ脆弱性を公表 [56]。マルウェアも確認された。
6/11	SymCrypt	CVE-2019-0865	Google「Project Zero」の研究者が暗号ライブラリSymCryptにWindows ServerでDoS状態を発生させられるゼロデイ脆弱性を公開 [57]。
6/24	Firefox	CVE-2019-11707 CVE-2019-11708	Mozilla社がJavaScriptの処理でクラッシュを引き起こすゼロデイ脆弱性に対処したバージョンをリリース [58]。

表 6:2019年度第1四半期に悪用が確認された脆弱性

日付	製品名	脆弱性番号	概要
4/10	WinRAR	CVE-2018-20250	Office 365チームが脆弱性を悪用するフィッシングメールキャンペーンを発見した [59]。
4/11	Jenkins	CVE-2019-1003000 CVE-2019-1003001 CVE-2019-1003002	Jenkinsの既知の脆弱性が悪用され、標準管理非営利団体「Matrix.org」のサーバに不正アクセスが発生した。資格情報を窃取され、本番環境にアクセス可能であった [60]。
4/17	ThinkPHP	CVE-2018-20062	Sucuri社がThinkPHPのバージョン5.1.X, 5.2.Xへ、マイニングマルウェアを仕込む攻撃が増加していると報告した [61]。
4/23 5/10	SharePoint	CVE-2019-0604	カナダ政府、サウジアラビア政府がSharePointサーバを標的とした攻撃キャンペーンを報告 [62] [63]。マルウェア「China Chopper」に感染させる攻撃という点で共通しているが、関連するという証拠はない。
5/7	Confluence Server	CVE-2019-3396	3月に報告されたAtlassian製のソフトウェア「Confluence」の脆弱性を悪用する攻撃をTrendMicro社が確認した [64]。
6/7	Office	CVE-2017-11882	既知の脆弱性CVE-2017-11882を悪用する不正なメールが出回っているとしてMicrosoftがTwitterで注意喚起を行った [65]。

脆弱性の報告件数は、年々増加傾向にあります。脆弱性情報の公開後、攻撃コードの流出や攻撃発生までにかかる時間が短くなっています。攻撃の種類も多岐に渡るため、誰もが脆弱性を悪用した攻撃の被害に遭うおそれがあります。
企業は、自組織の重要なシステムを狙った攻撃を受けて被害が発生しないよう対応が必要です。適切に対応するためには、まず必要な脆弱性情報を迅速に取得した後に、脆弱性の影響を正しく評価して対応要否の判断を行う必要があります。また、結果として脆弱性による影響が大きいと判断した場合は、その脆弱性への対応をすぐに実行へ移す必要があります。普段から、そのための仕組みや体制を整えておくことが重要です。しかし脆弱性の報告件数は多く、その件数が増加傾向にあることを考えれば、すべての脆弱性に対応することは困難です。2018年度は、公表された脆弱性のうち、CVSS基本値(Base Score)が「緊急レベル」とされる脆弱性だけでも年間2,000件でした。CVSS基本値は、共通脆弱性評価システム(CVSS) V3の基本評価基準(Base Metrics)を使って計算されます。CVSS基本値は、脆弱性の影響評価や対応要否判断の際に利用可能ですが、それだけでは膨大な件数の脆弱性を迅速かつ正確に評価、判断するための情報として不十分です。システムごとに設定やネットワーク構成、追加のセキュリティ対策が異なります。例えば、CVSS基本値から深刻度が緊急レベルと判断された脆弱性であっても、組織やシステムによっては、攻撃者が脆弱性を攻撃しようとしても影響しない場合もあります。
全ての脆弱性情報を処理するのではなく、組織ごとに自組織のシステムへ大きな影響がある脆弱性のみを選択できる効率的な方法を設けたり、重要なシステムにリソースを集中させて迅速に対応したりと、自組織に合った仕組みや体制を構築しましょう。

5. マルウェア・ランサムウェア

5.1. 進化を続けるマルウェア「Emotet」

2014年から確認されているマルウェア「Emotet」は、現在も進化を続けており、確認から5年を経過した今でも大きな脅威となっています。発見された当初は、オンラインバンキングのIDとパスワードを盗み出すバンキング型トロイの木馬でした。2015年ごろ、モジュール性の高いマルウェアとして進化して多様な機能を持てる多目的マルウェアになりました。2017年ごろに自己拡散機能が追加されたり、2018年に感染した被害者のメールを大量に収集する亜種が出現したりしました。現在は、ばらまき型攻撃メールを介して利用者のマシンへ感染し、情報窃取型マルウェアやランサムウェアとして猛威を振るっています。

セキュリティ企業 Proofpoint社の調査結果 [66]によると、2019年1月から3月の間にメール経由で悪質なダウンロードが発生した通信のうち、61%がボットネットであり、そのほとんどがEmotetとして検出されました。Proofpoint社のChris Dawson氏は、Emotetはモジュール型で柔軟性が高いこと、大規模なボットネットを構成していること、様々な地域、言語に対応して世界的に影響領域を広げていることなどを指摘しています。

4月11日に、ニュースメディアの米ZDNet社は、古いビジネスメールを利用してEmotet感染を狙う攻撃手法を報じました [67]。この攻撃手法の特徴は、実在する人物や組織からの正規のメールに返信したように見せかけて、悪意のあるURLリンクやファイルが添付されたメールがターゲットの人物へ届くことです。メールを受信した人は、実在する人物や組織と自分がやり取りしたメールが使われているため、本物の返信メールと思い込みURLリンクや添付ファイルを開封しやすくなります。これは、ばらまき型攻撃メールではなく、標的型攻撃メールを使った攻撃手法に近く、巧妙な手法です。現在は、2018年11月より前に感染したマシンから収集したメールを悪用しています。現在も感染したマシンからメールを収集している場合、攻撃者は新しく収集したメールを悪用して、攻撃を継続すると予想されます。

4月25日には、セキュリティ企業のTrendMicro社が、2019年3月後半に確認されたEmotetの新しい亜種に関する記事を公開しました [68]。新たに発見されたEmotetの亜種は、感染後のC&Cサーバとの通信トラフィックが変化しています。Emotetはこれまで多くの変化を繰り返してきましたが、トラフィックの変化は初めて確認されました。まず、これまでのEmotetはURIが空の状態で通信を行っていました。しかし、URIが空になっている通信は不正な通信のおそれがあると判断するセキュリティ対策製品が増えたことから、新しいEmotetの亜種はURIにランダムな単語を挿入し、検知を回避するようになりました。次に、これまでのEmotetはHTTP GETリクエスト通信のCookieヘッダにデータを含めて送信していました。新しいEmotetの亜種は、HTTP POST通信に変更して、HTTP通信のボディにデータを含めて送信するようになりました。このような変更により通信方法のバリエーションが増えたことによって、検出の回避や調査遅延につながります。

Emotetは、自己拡散機能や検出回避手法を必要に応じて取り入れることで、登場してから5年以上、大きな脅威であり続けています。Emotetの例から、サイバー攻撃手法は日々進化して巧妙化が進んでいることがわかります。したがって、セキュリティ対策についても攻撃手法に応じて進化する必要があり、一度対策を講じたからといって安心できるものではありません。特にEmotetのように柔軟に変化する攻撃に対応するためには、不審メール対策、不審通信の検知など、複数の対策を多層的に実施する必要があります。TrendMicro社の解説記事でも、Emotetのような脅威に対抗するためには、ゲートウェイ、エンドポイント、ネットワークおよびサーバにいたる多層的で積極的なセキュリティ対策が必要であるとしています[68]。

5.2. その他の被害事例

2019年度第1四半期も様々な企業、組織がマルウェア・ランサムウェアによる被害に遭っています。特に最近は、ランサムウェアによる被害が、米国各都市の自治体から多く報告されています。2019年度第1四半期に報告されたマルウェア・ランサムウェアによる攻撃・被害事例を表 7に示します。

表 7:その他マルウェア・ランサムウェアによる攻撃・被害事例

日付	組織名	概要
3/30	ニューヨーク州 アルバニー市	ランサムウェアによる攻撃を受けた [69]。一部データを失ったが復元可能であった。
4/2	ミシガン州 ジェネシー郡	ランサムウェアによる攻撃を受けた [70]。当初、4/8までに回復する目標を設定したが、4/17にまだ影響を受けていると報じられた。
4/4※	Bayer社	ドイツの製薬会社Bayer社が昨年「WINNTI」と呼ばれるマルウェアに感染した旨を発表 [71]。データ漏えいの証拠はないとしている。
4/9	神奈川大学	メール管理システムでランサムウェアに感染する被害が発生 [72]。サーバ内には氏名、メールアドレス、初期パスワード等を格納。
4/13	フロリダ州 スチュアート市	フィッシングメールからランサムウェア「Ryuk」に感染 [73]。サーバの強制シャットダウンを行った。
4/22	テキサス州 アマリロ	ランサムウェアによる攻撃を受け、ネットワーク全体を遮断した [74]。550人を超える従業員が業務に影響を受けた。
4/25	Aebi Schmidt社	ランサムウェアによる攻撃を受けメールシステム等が一部停止した [75]。一時的にシステムの電源を切ったことで感染拡大を防いだ。
5/7	メリーランド州 ボルチモア市庁舎	ランサムウェア「RobbinHood」の攻撃を受けた。多数のコンピュータが暗号化され、サービスの一部が完全に停止した [76]。
5/28	佐世保共済病院	放射線検査の危機と接続したパソコンからコンピュータウイルスを検知したと発表 [77]。被害防止のためネットワークを遮断した。
5/29※	Checkers Drive-In Restaurants社	米国内900店舗のうち102店舗のPOSシステムでマルウェアが発見された [78]。クレジットカード情報を含むデータ漏えいが確認された。
5/29	フロリダ州 リビエラビーチシティ	ランサムウェアにより、ファイルが暗号化されて市内のすべてのサービスが停止した [79]。データ回復のため60万ドル支払った。
6/7	ASCO社	航空機用部品メーカのASCO社にランサムウェアによる攻撃 [80]。情報の漏えいはないが業務停止により従業員1,000人が影響を受けた。
6/10	フロリダ州 レイクシティ	影響を受けたシステムを切り離したにも関わらず、ほぼすべてのシステムがランサムウェアに感染 [81]。42ビットコイン（50万ドル相当）を支払った。

※攻撃を受けた日付ではなく公表日

6. 分野別動向

6.1. 政府・公共機関のセキュリティ施策動向

この2019年度第1四半期は、IoT機器へのセキュリティ対策や取り組みが各国において行われました。

表 8:政府・公共機関のセキュリティ施策関連イベント一覧

No.	日付	国/地域	概要
1	4月1日	日本	内閣サイバーセキュリティセンター(NISC)は、"サイバーセキュリティ基本法の一部を改正する法律"に基づき、「サイバーセキュリティ協議会」が組織されたことを発表した。同協議会は、官民の多様な主体が連携し、脅威情報等の共有・分析や対策の作出・共有などを主に行う[82]。
2	4月22日	日本	総務省は、「電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第1版)」を公表した[83]。同ガイドラインには、IoT機器のセキュリティ基準に係る技術基準適合認定や電波を使用する端末機器に係る技術基準適合認定が整理されている。
3	4月23日	オランダ	National Cyber Security Centrum (NCSC)は、TLSに関するセキュリティガイドラインを更新したことを公表した[84]。同ガイドラインは、TLSの安全な設定を記載している。今回の更新では、TLS1.3に関する推奨設定が追加された。
4	4月29日	アメリカ	国土安全保障省(DHS)のCybersecurity and Infrastructure Security Agency(CISA)は、連邦政府関連機関に対して、インターネットからアクセス可能な保有システムに対する脆弱性スキャンを受け入れ、検知された脆弱性を一定の期間内で修正することを要求する運用指令「Binding Operational Directive 19-02」を発令した[85]。
5	4月29日	日本	ニュースメディアの共同通信社は、安全保障を脅かすサイバー攻撃へ反撃するためのマルウェアを防衛省にて作成・保有する方針を日本政府が固めたと報じた[86]。
6	5月1日	イギリス	ニュースメディアのBBCは、IoT製品がどのくらいセキュリティ的に安全かを消費者に示すラベルを導入する法案が提案されたことを報じた[87]。このラベルを得て製品販売するためには、共通ではないデフォルトパスワードやセキュリティアップデート対応期間の明示、脆弱性情報展開窓口の提供が要求される。
7	5月2日	アメリカ	トランプ大統領は、サイバーセキュリティ要員に対する大統領令を発令した[88]。同大統領令では政府内でのセキュリティ専門家の活動推進やセキュリティ教育のための採用活動などの内容が盛り込まれている。

No.	日付	国/地域	概要
8	5月14日	日本	ニュースメディアの時事通信社は、自民党がサイバー攻撃への対応に関する提案書を安倍首相に提出したことを報じた [89]。同報告書には、重要インフラ事業者に対する対策の義務付けやサイバーセキュリティ庁の新設が盛り込まれている。
9	5月20日	日本	独立行政法人情報処理推進機構(IPA)は、「入退管理システムにおける情報セキュリティ対策要件チェックリスト」を公開した [90]。本チェックリストは、入退管理システムにおいて想定される脅威に対するセキュリティ要件が盛り込まれている。
10	5月29日	日本	フィッシング対策協議会の技術・制度検討ワーキンググループは、事業者向けと利用者向けのフィッシング対策ガイドラインをそれぞれ改訂し、2019 年度版として公開した [91]。今回の更新では、2018年度の動向や新しい対策技術を踏まえた内容が盛り込まれている。
11	6月11日	アメリカ	アメリカ国立標準技術研究所(NIST)は、Secure Software Development Framework (SSDF)に関するホワイトペーパーのドラフトを公開した [92]。このフレームワークを採用することで、脆弱性のリスクが軽減できるとしている。
12	6月14日	日本	総務省は、マルウェアに感染しているIoT機器の利用者に対する注意喚起の実施について公表した [93]。既存の「NOTICE」の取り組みに加えて、国立研究開発法人情報通信研究機構(NICT)のNICTERプロジェクトにより、検知された機器の利用者に対して注意喚起を行う。
13	6月25日	アメリカ	NISTは、IoTを管理する際のセキュリティとプライバシーのリスクに関するガイドラインを公開した [94]。このガイドラインでは、考慮すべき３つの事項とそれらに対するリスク軽減について盛り込まれている。

6.2. プライバシー関連動向

この2019年度第1四半期は、日本で個人情報の活用について議論がされ、アメリカの各州にて個人情報保護を強化する法案が多く出てきました。

表 9:プライバシー関連イベントの一覧

No.	日付	国/地域	概要
1	4月9日	アメリカ	Mark Warner上院議員らは、ユーザを騙して個人情報を取得するUIを規制する法案「Deceptive Experiences To Online Users Reduction (DETOUR) Act」を上院に提出した [95]。本法案では、月間アクティユーザが1億人以上の大規模なオンラインプラットフォームが規制対象となる。
2	4月25日	アメリカ ワシントン州	ワシントン州議会は、データ漏えい時の通知要件に関する法案を可決した [96]。新しい法案"HB1071"では、ユーザの氏名が他の公共IDと組み合わせて漏洩した場合に、その漏えい元組織はユーザに通知する必要がある。
3	4月25日	イギリス	ニュースメディアのZDNetは、National Cyber Security Center(NCSC)とInformation Commissioner Office(ICO)が英組織におけるデータ侵害の際の役割分担について明確化したことを報じた [97]。NCSCは被害減少のために被害組織を支援し、ICOはGDPRの準拠状況を確認する。両組織は集められた情報を匿名で共有する。
4	5月3日	イギリス	歳入税関庁(HMRC)は、ICOからGDPRに抵触すると指摘されていた同意なく収集していた顧客500万人分の音声データについて、6/5までに削除するとICOに通知したことを報告した [98]。この問題は、英国プライバシー保護団体「Big Brother Watch」により発覚した [99]。
5	5月22日	日本	ニュースメディアの日経xTECHは、政府の有識者会合が個人データの利活用や官民のデータ連携を促すための政府提言をまとめたことを報じた [100]。情報銀行やデータ取引市場の普及のために実証実験をすることで、サービス構成やデータ形式を標準化するべきと提言している。
6	5月22日	アイルランド	アイルランドのデータ保護委員会(DPG)は、Google Ireland社に対する調査を開始した [101]。この調査は、同社の広告取引の各段階において個人情報の処理がGDPR関連規定に準拠しているかどうかを確認する。
7	5月30日	アメリカ メイン州	メイン州議会は、オンライン個人情報保護法を可決した [102]。本法案は、ISPがユーザの許可なく第三者に個人情報を開示または販売することを禁じている。

No.	日付	国/地域	概要
8	6月17日	アメリカ ニューヨーク州	ニューヨーク州議会は、情報漏えい通知法を可決した[103]。本法案は、情報漏えいを起こした企業に対して、影響を受ける個人への通常30日以内の通知を義務付けている。また、同州内企業だけではなく、同州住人の個人情報を持つ企業も対象としている。

7. 予測

2019年度第2四半期は、2019年度第1四半期と同様に金銭に直接つながるサイバー攻撃が増加するでしょう。インターネットを経由して金銭のやり取りを行う機会が増え、数多くのクレジットカード情報や暗号通貨に関する情報が、インターネットと接続されたサーバやクラウドなどのサイバー空間上に保存されています。攻撃者は、世界中の直接的に金銭に結びつく情報や金銭を取り扱うサービスを攻撃することで効率的に金銭を取得します。ランサムウェア攻撃を用いた脅迫による金銭要求も継続して発生するおそれがあります。

クレジットカード情報を狙う攻撃

2018年度第4四半期、2019年度第1四半期ともにWebスキミングに関するトピックを取り上げました。Webスキミングは金銭に直接つながるクレジットカード情報を窃取する手法として、増加傾向が続いています。ユーザは、使用しているサービスで情報流出が起きていないか、また身に覚えのない請求がないか確認してください。ECサイトを運営する組織は、ユーザのクレジットカード情報を取り扱うリスクを再認識し、改ざんが行われていないことの確認や、周辺環境を含めたセキュリティ対策の実施を徹底してください。ECサイトに限らず、これから普及する電子マネーをはじめとするサービスも、クレジットカード情報を登録するサービスはサイバー攻撃の標的になるおそれがあります。

暗号通貨を狙う攻撃

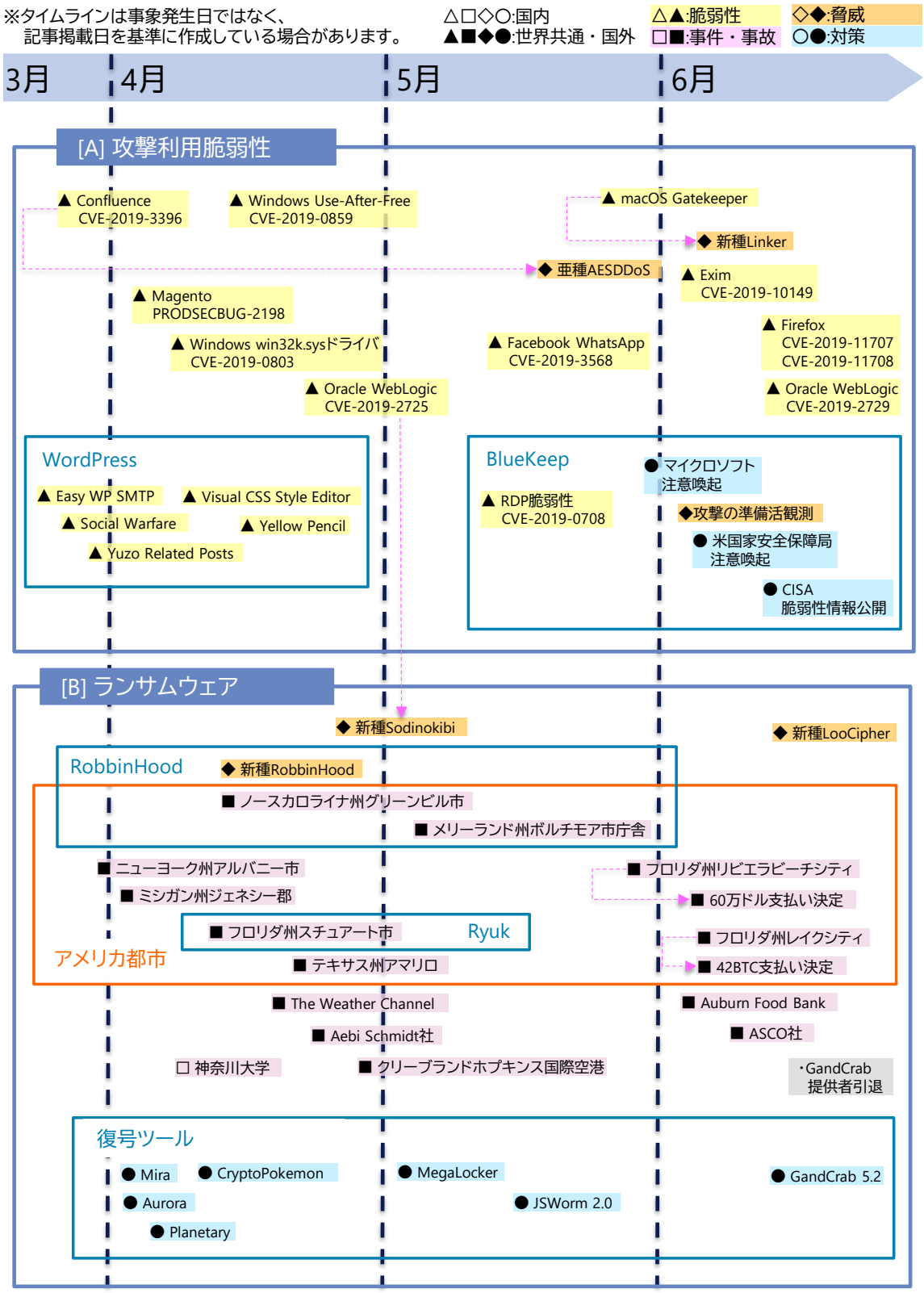
暗号通貨も、攻撃者がサイバー攻撃で直接金銭を得るための標的として適しています。我々は2018年度第4四半期のレポートで、暗号通貨の市場価格の上昇に合わせて2019年度第1四半期に攻撃が発生すると予測しました。実際に5月8日、大手仮想通貨取引所「Binance」がサイバー攻撃を受けて7,000ビットコイン（44億円相当）が流出したと発表しました [104]。市場価格の上昇傾向が続いている間は、同様の事例が引き続き発生するおそれがあります。

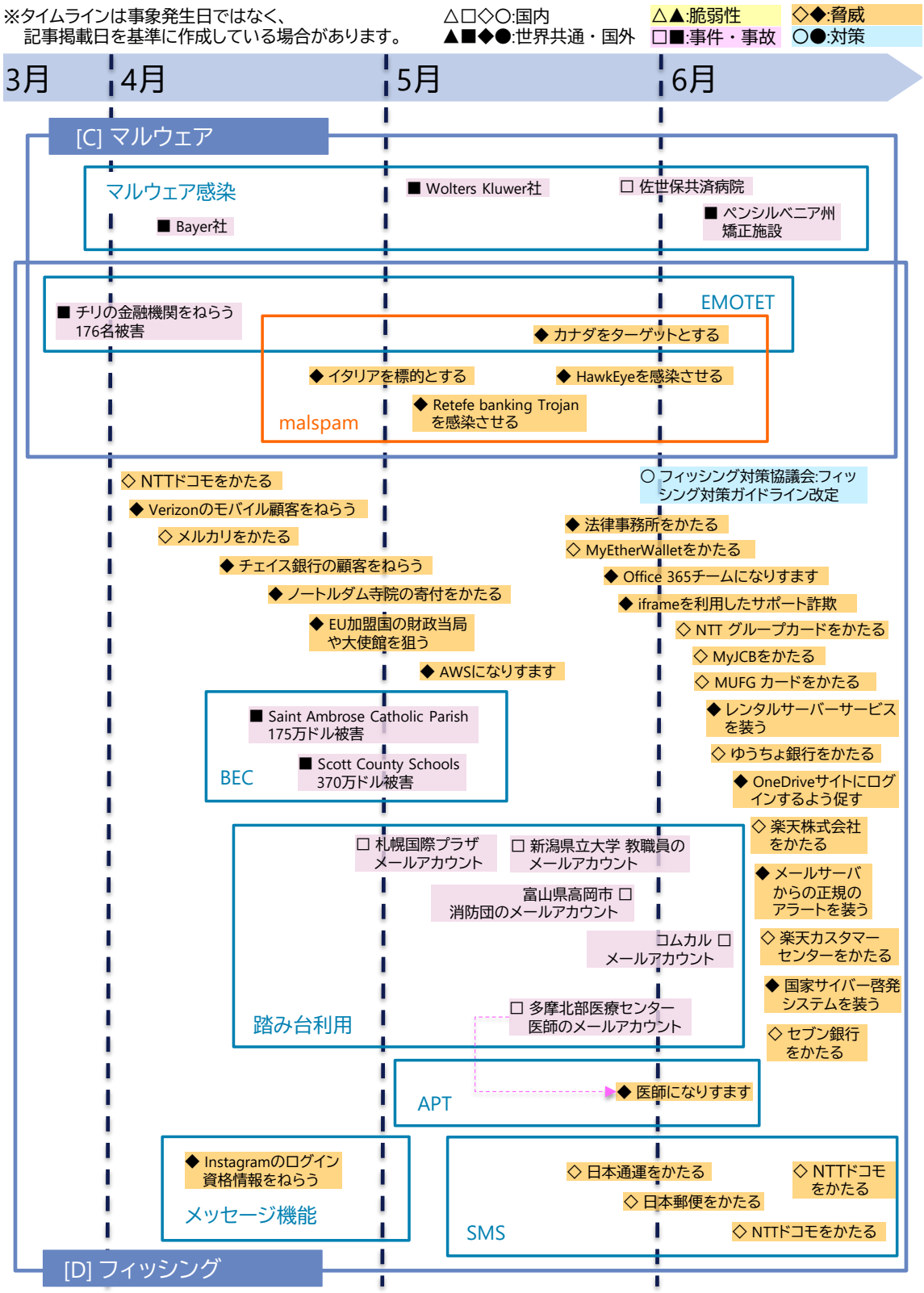
地方自治体を標的としたランサムウェア攻撃

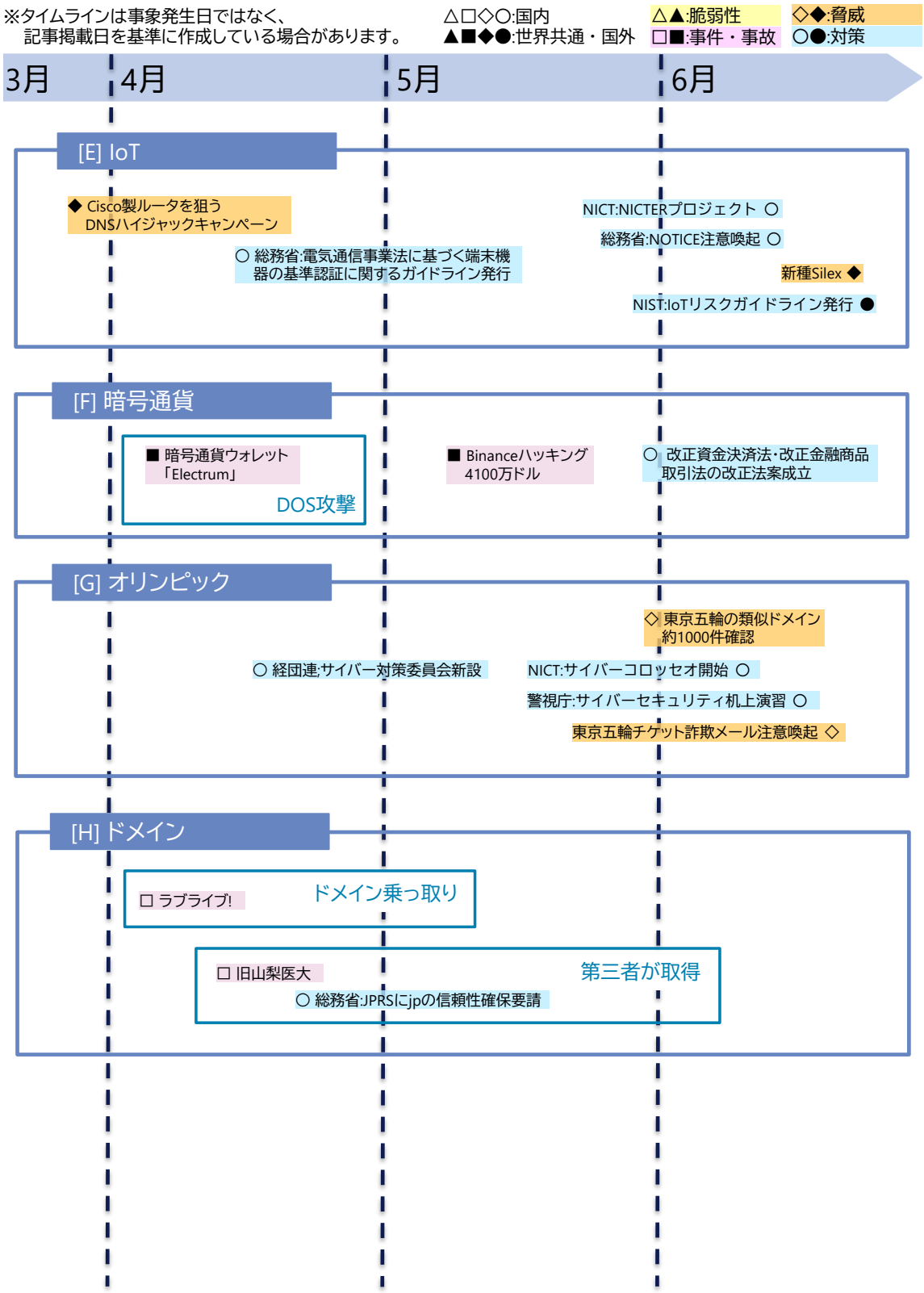
2019年度第1四半期は、米国の複数の都市でランサムウェア攻撃による被害がでました。個人や大企業ではなく、地方自治体のような組織を標的としたランサムウェア攻撃が増加傾向にあります。攻撃者は、予算不足によりセキュリティ対策が十分に実施できていない小・中規模な組織、停止すると生活に支障があるシステムを持っている組織といった特徴に合致することから、地方自治体を狙っているおそれがあります。今後もこのような特徴を持つ組織を標的としたランサムウェア攻撃の増加が懸念されます。米国は、全市長会議でセキュリティ侵害における身代金の支払いを拒否する旨を決定しました [105]。この決定によってランサムウェアの攻撃者が米国の地方自治体を狙わなくなるかどうかは不明です。しかし、身代金を支払わない方針に決めたことで、事前のセキュリティ対策やインシデント対応時の判断

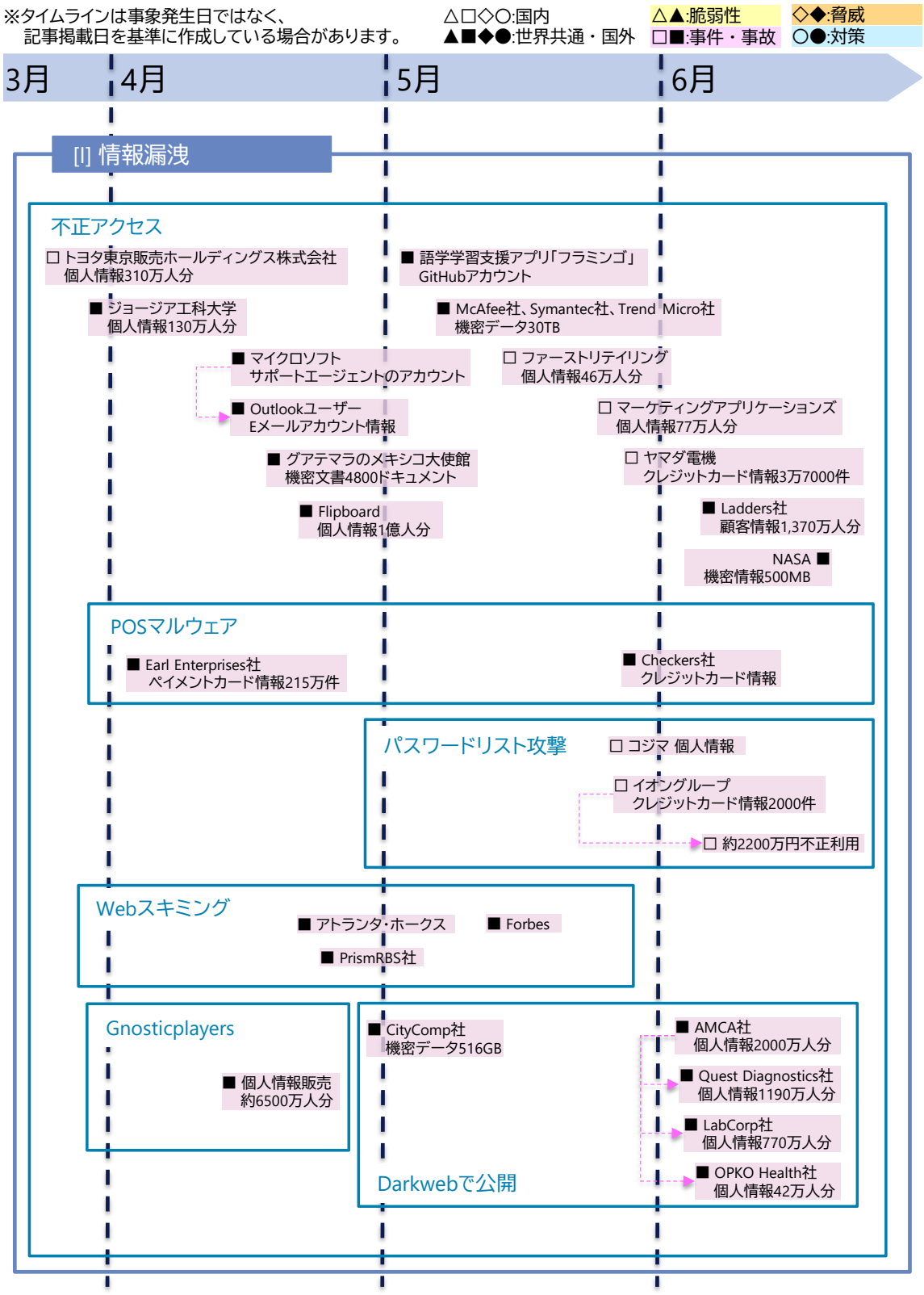
がシンプルになりました。今後は、米国以外の地方自治体が標的にされるおそれもあり、ランサムウェア攻撃への対応を検討する必要があります。その対応には、攻撃を受けないための事前対策から攻撃を受けた際の身代金支払いに関する対応方針の決定などが含まれます。

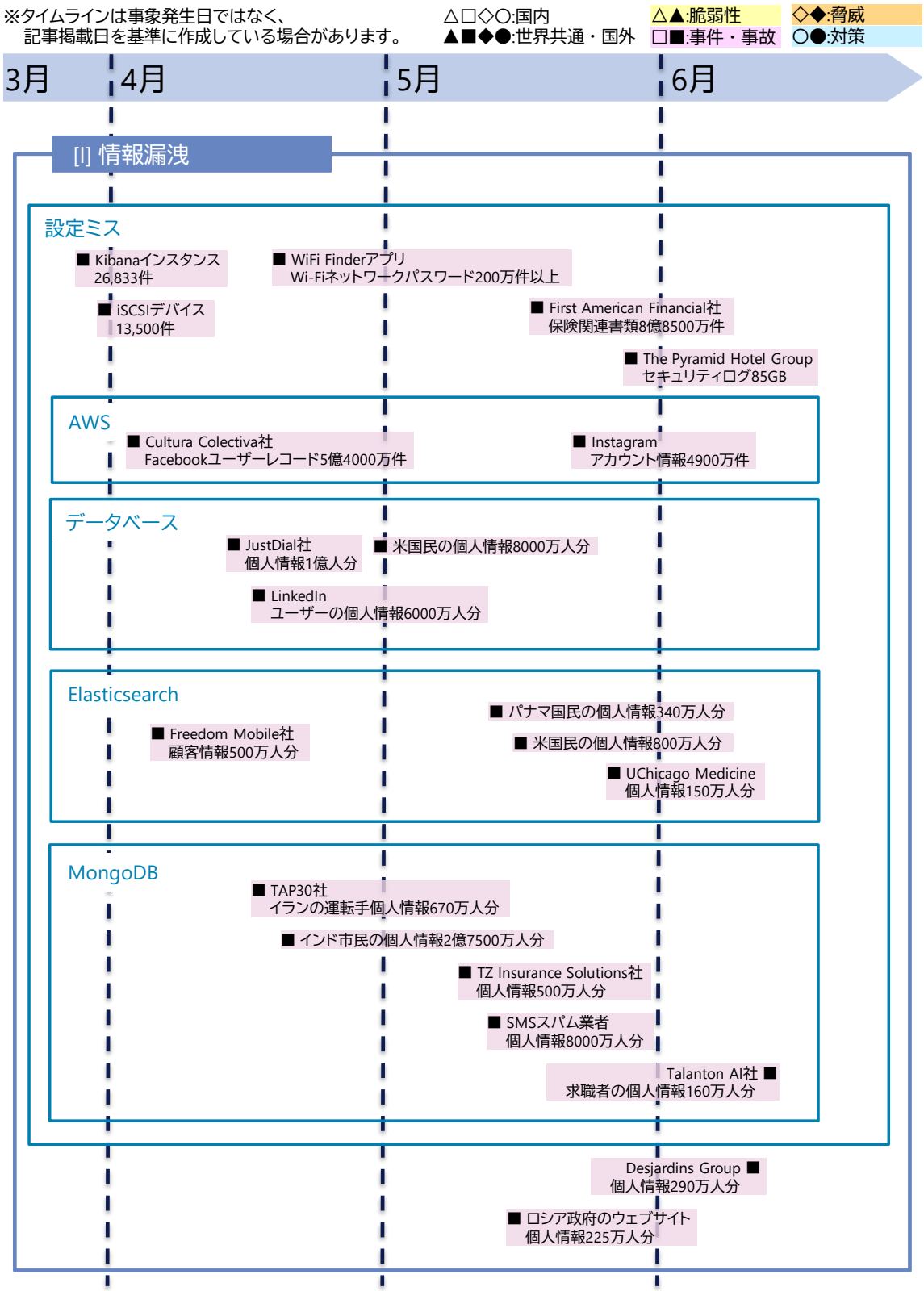
8. タイムライン

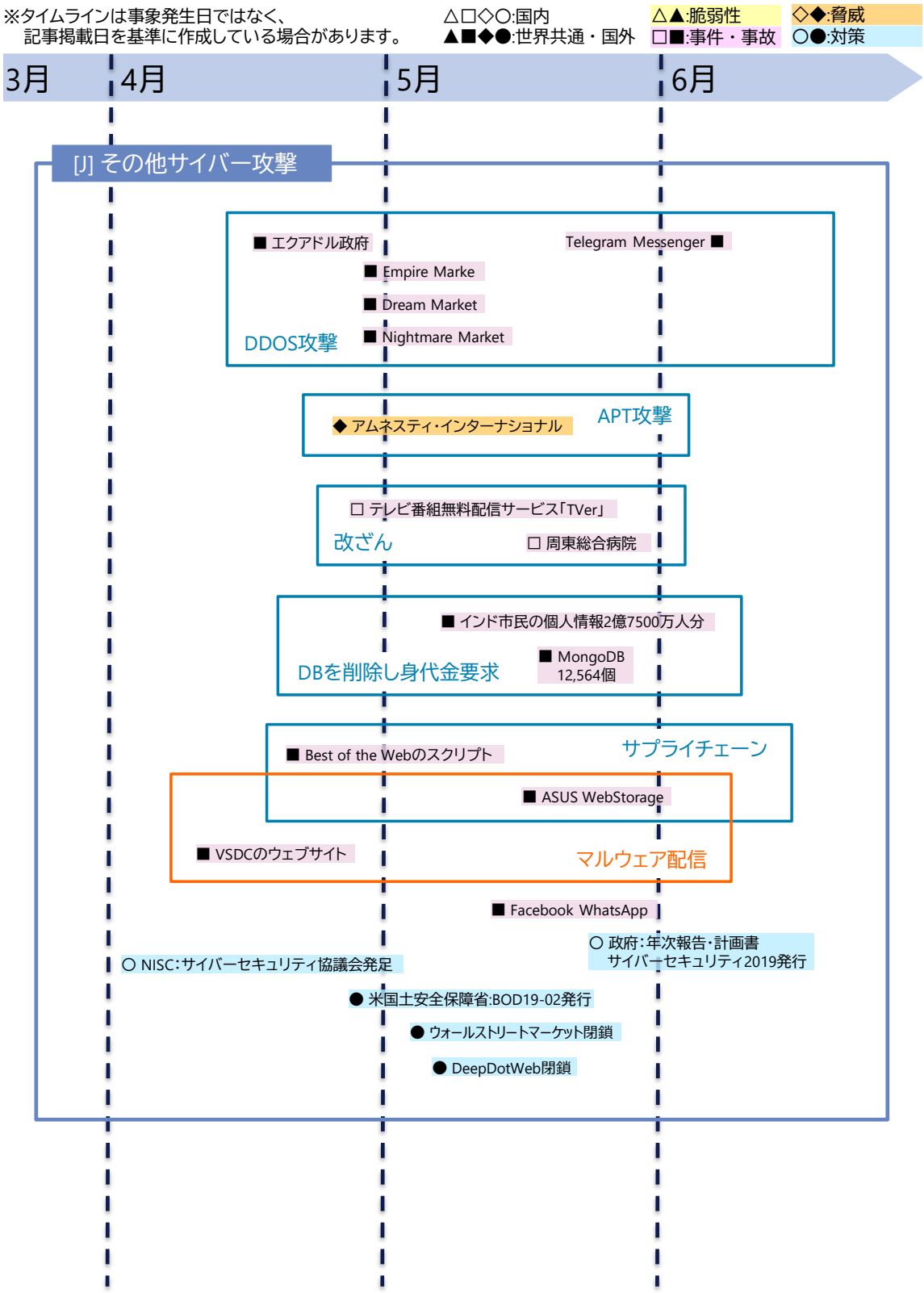












参考文献

[1] サイバーセキュリティ.com編集事務局, “ドメイン名ハイジャックとは？被害事例と対策方法を徹底解説,” CyberSecurity.com, 24 4 2019. [オンライン]. Available: https://cybersecurity-jp.com/cyber-terrorism/31073.

[2] “アミューズクラフトエロチカ公式Twitterアカウント,” 25 9 2018. [オンライン]. Available: https://twitter.com/AMUSECRAFT_ero/status/1044539803021135872.

[3] “Internet Archive,” 25 9 2018. [オンライン]. Available: https://web.archive.org/web/20180925133456/http://amusecraft.jp/. [アクセス日: 5 8 2019].

[4] “シロップ広報担当公式Twitterアカウント,” 15 2 2019. [オンライン]. Available: https://twitter.com/SYRUP_KOUHOU/status/1096225680004509696.

[5] “Internet Archive,” 29 2 2019. [オンライン]. Available: https://web.archive.org/web/20190214165224/http://www.syrup-soft.jp:80/mm/index.html.

[6] “タニシ@スク水.jpのTwitterアカウント,” 5 4 2019. [オンライン]. Available: https://twitter.com/tanishi009/status/1113985953264062464.

[7] “ラブライブ!シリーズ公式Twitterアカウント,” 5 4 2019. [オンライン]. Available: https://twitter.com/LoveLive_staff/status/1113871689128005634.

[8] “Internet Archive,” 4 4 2019. [オンライン]. Available: https://web.archive.org/web/20190404173940/http://www.lovelive-anime.jp/.

[9] Japan Registry Services Co., Ltd., “汎用JPドメイン名登録申請等の取次に関する規則,” Japan Registry Services Co., Ltd., 15 6 2016. [オンライン]. Available: https://jprs.jp/doc/rule/toritsugi-rule-wideusejp.html.

[10] iFixit, “Amazon Echo Dot 2nd Generation Teardown,” iFixit, 26 6 2018. [オンライン]. Available: https://jp.ifixit.com/Teardown/Amazon+Echo+Dot+2nd+Generation+Teardown/110989.

[11] State of New Jersey, “Mirai,” State of New Jersey, 28 12 2016. [オンライン]. Available: https://www.cyber.nj.gov/threat-profiles/botnet-variants/mirai-botnet.

[12] N. Ruchna, “New Mirai Variant Adds 8 New Exploits, Targets Additional IoT Devices,” Palo Alto Networks, Inc, 6 6 2019. [オンライン]. Available: https://unit42.paloaltonetworks.com/new-mirai-variant-adds-8-new-exploits-targets-additional-iot-devices/.

[13] K. VLADIMIR, “覗き見される映像：無防備なIP監視カメラを悪用するサイバー犯罪者のアンダーグラウンド動向,” Trend Micro Incorporated, 28 6 2018. [オンライン]. Available: https://www.trendmicro.com/jp/iot-security/special/50202.

[14] Office of Inspector General, “CYBERSECURITY MANAGEMENT AND OVERSIGHT AT THE JET PROPULSION LABORATORY,” NationalAeronautics and Space Administration, 18 6 2019. [オンライン]. Available: https://oig.nasa.gov/docs/IG-19-022.pdf.

[15] K. Nohl , “[CB16] 基調講演： セキュリティはどれくらいが適量? – How much security is too much? – by Karsten Nohl,” 9 11 2016. [オンライン]. Available: https://www.slideshare.net/codeblue_jp/cb16-nohl-ja.

[16] NTTDATA-CERT, “グローバルセキュリティ動向四半期レポート(2018年度第4四半期),” 30 5 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/news/information/2019/053000/.

[17] Security Affairs, “Gnosticplayers round 5 – 65 Million+ fresh accounts from 6 security breaches available for sale,” 15 4 2019. [オンライン]. Available: https://securityaffairs.co/wordpress/83904/data-breach/gnosticplayers-fifth-round.html.

[18] BleepingComputer, “Hackers Steal Payment Card Data Using Rogue Iframe Phishing,” 21 5 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/hackers-steal-payment-card-data-using-rogue-iframe-phishing/.

[19] TrendMicro, “Mirrorthief Group Uses Magecart Skimming Attack to Hit Hundreds of Campus Online Stores in US and Canada,” 3 5 2019. [オンライン]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/mirrorthief-group-uses-magecart-skimming-attack-to-hit-hundreds-of-campus-online-stores-in-us-and-canada/.

[20] TrendMicro, “新しく確認されたサイバー犯罪集団「Mirrorthief」、米国とカナダの201の大学オンラインストアにスキミング攻撃,” 31 5 2019. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/21422.

[21] RiskIQ, “Magento Attack: All Payment Platforms are Targets for Magecart Attacks,” 1 5 2019. [オンライン]. Available: https://www.riskiq.com/blog/labs/magecart-beyond-magento/.

[22] EC-CUBE, “【重要】サイト改ざんによるクレジットカード流出被害が増加しています（2019/05/09）,” 9 5 2019. [オンライン]. Available: https://www.ec-cube.net/news/detail.php?news_id=330.

[23] Bleeping Computer, “Over 12,000 MongoDB Databases Deleted by Unistellar Attackers,” 17 5 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/over-12-000-mongodb-databases-deleted-by-unistellar-attackers/.

[24] Bleeping Computer, “Attackers Wiping GitHub and GitLab Repos, Leave Ransom Notes,” ３ 5 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/attackers-wiping-github-and-gitlab-repos-leave-ransom-notes/.

[25] The Hacker News, “Over 100 Million JustDial Users' Personal Data Found Exposed On the Internet,” 17 4 2019. [オンライン]. Available: https://thehackernews.com/2019/04/justdial-hacked-data-breach.html.

[26] SECURITY DISCOVERY, “Iranian Ride-Hailing App Database Exposure,” 19 4 2019. [オンライン]. Available: https://securitydiscovery.com/iranian-ride-hailing-app-database-exposure/.

[27] “Unsecured Databases Leak 60 Million Records of Scraped LinkedIn Data,” 18 4 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/unsecured-databases-leak-60-million-records-of-scraped-linkedin-data/.

[28] Security Affairs, “Report: Unknown Data Breach Exposes 80 Million US Households,” 29 4 2019. [オンライン]. Available: https://securityaffairs.co/wordpress/84666/data-breach/80-million-us-households-leak.html.

[29] SECURITY DISCOVERY, “Massive SMS Bombing Operation Uncovered In Passwordless Database,” 9 5 2019. [オンライン]. Available: https://securitydiscovery.com/massive-sms-bombing-operation/.

[30] Bleeping Computer, “Open Marketing Database Exposes 5 Million Personal Records,” 28 6 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/open-marketing-database-exposes-5-million-personal-records/.

[31] Security Affairs, “Unprotected DB exposed PII belonging to nearly 90% of Panama citizens,” 2019. [オンライン]. Available: https://securityaffairs.co/wordpress/85462/data-breach/panama-citizens-massive-data-leak.html.

[32] Bleeping Computer, “Unsecured Survey Database Exposes Info of 8 Million People,” 16 5 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/unsecured-survey-database-exposes-info-of-8-million-people/.

[33] Security Affairs, “Data belonging to Instagram influencers and celebrities exposed online,” 20 5 2019. [オンライン]. Available: https://securityaffairs.co/wordpress/85905/data-breach/instagram-data-leak.html.

[34] Krebs on Security, “First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records,” 24 5 2019. [オンライン]. Available: https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/.

[35] IPA, “脆弱性対策情報データベースJVN iPediaの登録状況 [2019年第2四半期（4月～6月）],” 24 7 2019. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/report/JVNiPedia2019q2.html.

[36] Oracle, “Oracle Critical Patch Update Advisory - April 2019,” 16 4 2019. [オンライン]. Available: https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html.

[37] CHINA NATIONAL VULNERABILITY DATABASE, “关于Oracle WebLogic wls9-async组件存在反序列化远程命令执行漏洞的安全公告,” 17 4 2019. [オンライン]. Available: https://www.cnvd.org.cn/webinfo/show/4989.

[38] Oracle, “Oracle Security Alert Advisory - CVE-2019-2725,” 26 4 2019. [オンライン]. Available: https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html.

[39] KnownSec 404, “[KnownSec 404 Team] Oracle WebLogic Deserialization RCE Vulnerability (0day) Alert Again (CVE-2019-2725 patch bypassed!!!),” 16 6 2019. [オンライン]. Available: https://medium.com/@knownsec404team/knownsec-404-team-alert-again-cve-2019-2725-patch-bypassed-32a6a7b7ca15.

[40] Oracle, “Oracle Security Alert Advisory - CVE-2019-2729,” 18 6 2019. [オンライン]. Available: https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2729-5570780.html.

[41] “Oracle WebLogic Serverの脆弱性（CVE-2019-2725）を狙う攻撃の観測,” 10 5 2019. [オンライン]. Available: https://wizsafe.iij.ad.jp/2019/05/658/.

[42] NTTデータ先端技術株式会社, “Oracle WebLogic Serverに含まれるリモートコード実行に関する脆弱性（CVE-2019-2725）についての検証レポート,” 9 5 2019. [オンライン]. Available: http://www.intellilink.co.jp/article/vulner/190509.html.

[43] Microsoft, “CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability,” 14 5 2019. [オンライン]. Available: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0708.

[44] Microsoft, “Prevent a worm by updating Remote Desktop Services (CVE-2019-0708),” 14 5 2019. [オンライン]. Available: https://msrc-blog.microsoft.com/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/.

[45] Microsoft, “Customer guidance for CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability: May 14, 2019,” 14 5 2019. [オンライン]. Available: https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708.

[46] Errata Security, “Almost One Million Vulnerable to BlueKeep Vuln (CVE-2019-0708),” 28 5 2019. [オンライン]. Available: https://blog.erratasec.com/2019/05/almost-one-million-vulnerable-to.html#.XTBJy-j7RhE.

[47] Microsoft, “A Reminder to Update Your Systems to Prevent a Worm,” 30 5 2019. [オンライン]. Available: https://msrc-blog.microsoft.com/2019/05/30/a-reminder-to-update-your-systems-to-prevent-a-worm/.

[48] NSA, “NSA Cybersecurity Advisory: Patch Remote Desktop Services on Legacy Versions of Windows,” 4 6 2019. [オンライン]. Available: https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1865726/nsa-cybersecurity-advisory-patch-remote-desktop-services-on-legacy-versions-of/.

[49] Morphus Labs, “GoldBrute Botnet Brute Forcing 1.5 Million RDP Servers,” 7 6 2019. [オンライン]. Available: https://morphuslabs.com/goldbrute-botnet-brute-forcing-1-5-million-rdp-servers-371f219ec37d.

[50] CISA, “Alert (AA19-168A) Microsoft Operating Systems BlueKeep Vulnerability,” 17 6 2019. [オンライン]. Available: https://www.us-cert.gov/ncas/alerts/AA19-168A.

[51] 警察庁, “リモートデスクトップサービスを標的としたアクセスの増加等について,” 21 6 2019. [オンライン]. Available: http://www.npa.go.jp/cyberpolice/important/2019/201906211.html.

[52] Microsoft, “CVE-2019-0859 | Win32k Elevation of Privilege Vulnerability,” 9 4 2019. [オンライン]. Available: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0859.

[53] Microsoft, “CVE-2019-0803 | Win32k Elevation of Privilege Vulnerability,” 9 4 2019. [オンライン]. Available: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0803.

[54] NCSC, “NCSC advice following WhatsApp vulnerability,” 14 5 2019. [オンライン]. Available: https://www.ncsc.gov.uk/guidance/whatsapp-vulnerability.

[55] Zscaler, “Microsoft vulnerability: Source code published for three zero-day vulnerabilities in Windows,” 24 5 2019. [オンライン]. Available: https://www.zscaler.com/blogs/research/three-zero-day-microsoft-windows-vulnerabilities.

[56] Filippo Cavallarin, “MacOS X GateKeeper Bypass,” 24 5 2019. [オンライン]. Available: https://www.fcvl.net/vulnerabilities/macosx-gatekeeper-bypass.

[57] Forbes, “Warning: Google Researcher Drops Windows 10 Zero-Day Security Bomb,” 12 6 2019. [オンライン]. Available: https://www.forbes.com/sites/daveywinder/2019/06/12/warning-windows-10-crypto-vulnerability-outed-by-google-researcher-before-microsoft-can-fix-it/#28019f052fd6.

[58] Mozilla, “Mozilla Foundation Security Advisory 2019-18,” 18 6 2019. [オンライン]. Available: https://www.mozilla.org/en-US/security/advisories/mfsa2019-18/.

[59] Microsoft, “Analysis of a targeted attack exploiting the WinRAR CVE-2018-20250 vulnerability,” 10 4 2019. [オンライン]. Available: https://www.microsoft.com/security/blog/2019/04/10/analysis-of-a-targeted-attack-exploiting-the-winrar-cve-2018-20250-vulnerability/.

[60] matrix, “We have discovered and addressed a security breach. (Updated 2019-04-12),” 12 4 2019. [オンライン]. Available: https://matrix.org/blog/2019/04/11/we-have-discovered-and-addressed-a-security-breach-updated-2019-04-12.

[61] Sucuri, “ThinkPHP 5.x Remote Code Execution,” 17 4 2019. [オンライン]. Available: https://blog.sucuri.net/2019/04/thinkphp-5-x-remote-code-execution.html.

[62] Canadian Centre for Cyber Security, “China Chopper Malware affecting SharePoint Servers,” 23 4 2019. [オンライン]. Available: https://cyber.gc.ca/en/alerts/china-chopper-malware-affecting-sharepoint-servers.

[63] ZDNet, “Microsoft SharePoint servers are under attack,” 10 5 2019. [オンライン]. Available: https://www.zdnet.com/article/microsoft-sharepoint-servers-are-under-attack/.

[64] TrendMicro, “CVE-2019-3396 Redux: Confluence Vulnerability Exploited to Deliver Cryptocurrency Miner With Rootkit,” 7 5 2019. [オンライン]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-3396-redux-confluence-vulnerability-exploited-to-deliver-cryptocurrency-miner-with-rootkit/.

[65] ITmedia, “Officeの既知の脆弱性を悪用した攻撃が活発化、不正なメールに注意呼び掛け――Microsoft,” 11 6 2019. [オンライン]. Available: https://www.itmedia.co.jp/enterprise/articles/1906/11/news065.html.

[66] Proofpoint, “Proofpoint Q1 2019 Threat Report: Emotet carries the quarter with consistent high-volume campaigns,” 28 5 2019. [オンライン]. Available: https://www.proofpoint.com/us/threat-insight/post/proofpoint-q1-2019-threat-report-emotet-carries-quarter-consistent-high-volume.

[67] ZDNet, “Emotet hijacks email conversation threads to insert links to malware,” 11 4 2019. [オンライン]. Available: https://www.zdnet.com/article/emotet-hijacks-email-conversation-threads-to-insert-links-to-malware/#ftag=RSSbaffb68.

[68] TrendMicro, “Emotet Adds New Evasion Techn,” 25 4 2019. [オンライン]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-adds-new-evasion-technique-and-uses-connected-devices-as-proxy-cc-servers/.

[69] StateScoop, “In Albany ransomware attack, officials say information was not compromised,” 11 4 2019. [オンライン]. Available: https://statescoop.com/in-albany-ransomware-attack-officials-say-information-was-not-compromised/.

[70] KnowBe4, “County Line Ransomware Fever,” 17 4 2019. [オンライン]. Available: https://blog.knowbe4.com/county-line-ransomware-fever.

[71] REUTERS, “Bayer contains cyber attack it says bore Chinese hallmarks,” 4 4 2019. [オンライン]. Available: https://www.reuters.com/article/us-bayer-cyber/bayer-contains-cyber-attack-it-says-bore-chinese-hallmarks-idUSKCN1RG0NN.

[72] Security Next, “メール管理システムがランサムウェア感染 - 神大,” 10 5 2019. [オンライン]. Available: http://www.security-next.com/104620.

[73] Security Affairs, “Stuart City is the new victim of the Ryuk Ransomware,” 24 4 2019. [オンライン]. Available: https://securityaffairs.co/wordpress/84439/malware/ryuk-ransomware-stuart-city.html.

[74] “Potter County officials’ computers remain dark after viruses hit,” 22 4 2019. [オンライン]. Available: https://www.newschannel10.com/2019/04/23/potter-county-officials-computers-remain-dark-after-viruses-hit/.

[75] Security Affairs, “The special-purpose vehicle maker Aebi Schmidt was hit by a malware attack that disrupted some of its operations.,” 26 4 2019. [オンライン]. Available: https://securityaffairs.co/wordpress/84501/malware/aebi-schmidt-ransomware.html.

[76] BBC, “Baltimore government held hostage by hackers' ransomware,” 23 5 2019. [オンライン]. Available: https://www.bbc.com/news/world-us-canada-48371476.

[77] 長崎新聞, “佐世保共済病院　患者受け入れ再開　新規と救急　システム障害復旧,” 4 6 2019. [オンライン]. Available: https://this.kiji.is/508439813399725153.

[78] SECURITY WEEK, “Malware Found on PoS Systems at Checkers and Rally's Restaurants,” 30 5 2019. [オンライン]. Available: https://www.securityweek.com/malware-found-pos-systems-checkers-and-rallys-restaurants.

[79] ZDNet, “Florida city pays $600,000 to ransomware gang to have its data back,” 19 6 2019. [オンライン]. Available: https://www.zdnet.com/article/florida-city-pays-600000-to-ransomware-gang-to-have-its-data-back/.

[80] SECURITY WEEK, “Aircraft Parts Maker ASCO Severely Hit by Ransomware,” 13 6 2019. [オンライン]. Available: https://www.securityweek.com/aircraft-parts-maker-asco-severely-hit-ransomware.

[81] ZDNet, “Second Florida city pays giant ransom to ransomware gang in a week,” 26 4 2019. [オンライン]. Available: https://www.zdnet.com/article/second-florida-city-pays-giant-ransom-to-ransomware-gang-in-a-week/.

[82] 内閣サイバーセキュリティセンター（NISC）, “サイバーセキュリティ基本法の一部を改正する法律の施行及び 同法に基づくサイバーセキュリティ協議会の組織について,” 内閣サイバーセキュリティセンター（NISC）, 1 4 2019. [オンライン]. Available: https://www.nisc.go.jp/press/pdf/kyogikai.pdf.

[83] “「電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第1版)」（案）についての意見募集の結果及びガイドラインの公表,” Ministry of Internal Affairs and Communications, 22 4 2019. [オンライン]. Available: http://www.soumu.go.jp/menu_news/s-news/01kiban05_02000179.html.

[84] National Cyber Security Centre, “Future-proof TLS configuration using the updated TLS guidelines from NCSC,” National Cyber Security Centre, 23 4 2019. [オンライン]. Available: https://english.ncsc.nl/latest/news/2019/juli/01/future-proof-tls-configuration.

[85] the Department of Homeland Security, “Binding Operational Directive 19-02,” the Department of Homeland Security, 29 4 2019. [オンライン]. Available: https://cyber.dhs.gov/bod/19-02/.

[86] 一般社団法人共同通信社, “政府、反撃用ウイルス初保有へ,” 一般社団法人共同通信社, 30 4 2019. [オンライン]. Available: https://this.kiji.is/495701484642698337.

[87] BBC, “Plan to secure internet of things with new law,” BBC, 1 5 2019. [オンライン]. Available: https://www.bbc.com/news/technology-48106582.

[88] The White House, “Executive Order on America’s Cybersecurity Workforce,” The White House, 2 5 2019. [オンライン]. Available: https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/.

[89] JIJI PRESS LTD., “インフラ事業者に対策義務付け＝サイバー攻撃、司令塔を新設－自民提言,” JIJI PRESS LTD., 14 5 2019. [オンライン]. Available: https://www.jiji.com/jc/article?k=20190514011711&g=pol.

[90] IPA, Japan, “入退管理システムにおける情報セキュリティ対策要件チェックリスト,” IPA, Japan, 20 5 2019. [オンライン]. Available: https://www.ipa.go.jp/security/jisec/choutatsu/ecs/index.html.

[91] Council of Anti-Phishing Japan, “資料公開: フィッシング対策ガイドラインの改訂のお知らせ,” Council of Anti-Phishing Japan, 29 5 2019. [オンライン]. Available: https://www.antiphishing.jp/news/info/guideline2019.html.

[92] National Institute of Standards and Technology, “Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF),” National Institute of Standards and Technology, 11 6 2019. [オンライン]. Available: https://csrc.nist.gov/publications/detail/white-paper/2019/06/11/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft.

[93] Ministry of Internal Affairs and Communications, “マルウェアに感染しているIoT機器の利用者に対する注意喚起の実施,” Ministry of Internal Affairs and Communications, 14 6 2019. [オンライン]. Available: http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00025.html.

[94] National Institute of Standards and Technology, “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks,” National Institute of Standards and Technology, 25 6 2019. [オンライン]. Available: https://www.nist.gov/publications/considerations-managing-internet-things-iot-cybersecurity-and-privacy-risks.

[95] “All Information (Except Text) for S.1084 - Deceptive Experiences To Online Users Reduction Act,” 9 4 2019. [オンライン]. Available: https://www.congress.gov/bill/116th-congress/senate-bill/1084/all-info.

[96] “HB 1071 - 2019-20,” 6 8 2019. [オンライン]. Available: https://app.leg.wa.gov/billsummary?BillNumber=1071&Initiative=false&Year=2019.

[97] D. Palmer, “You’ve been hacked, now what? How the UK’s cybersecurity and privacy watchdogs deal with incidents,” CBS Interactive, 25 4 2019. [オンライン]. Available: https://www.zdnet.com/article/youve-been-hacked-now-what-how-the-uks-cybersecurity-and-privacy-watchdogs-deal-with-incidents/.

[98] “Letter from Sir Jonathan Thompson to HMRC’s Data Protection Officer,” 3 5 2019. [オンライン]. Available: https://www.gov.uk/government/publications/letter-from-sir-jonathan-thompson-to-hmrcs-data-protection-officer.

[99] Big Brother Watch, “HMRC takes 5 million taxpayers’ Voice IDs without consent,” Big Brother Watch, 25 6 2018. [オンライン]. Available: https://bigbrotherwatch.org.uk/all-media/hmrc-takes-5-million-taxpayers-voice-ids-without-consent/.

[100] 忠. 玄, “政府会合が「情報銀行」の標準化など提言、GAFA対抗の「日本モデル」目指す,” Nikkei Business Publications, Inc, 21 5 2019. [オンライン]. Available: https://tech.nikkeibp.co.jp/atcl/nxt/news/18/05039/.

[101] The Data Protection Commission, “Data Protection Commission opens statutory inquiry into Google Ireland Limited,” The Data Protection Commission, 22 5 2019. [オンライン]. Available: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-google-ireland-limited.

[102] State of Maine, “An Act To Protect the Privacy of Online Customer Information,” State of Maine, 30 5 2019. [オンライン]. Available: http://legislature.maine.gov/LawMakerWeb/summary.asp?ID=280072014.

[103] The New York State Senate, “senate Bill S5575B,” The New York State Senate, 25 7 2918. [オンライン]. Available: https://www.nysenate.gov/legislation/bills/2019/s5575.

[104] BINANCE, “Binance Security Breach Update,” 9 8 2019. [オンライン]. Available: https://www.binance.com/en/support/articles/360028031711.

[105] Cnet, “US mayors resolve not to pay hackers over ransomware attacks,” 12 7 2019. [オンライン]. Available: https://www.cnet.com/news/us-mayors-adopt-resolution-to-not-pay-hackers-over-ransomware-attacks/.

[106] Japan Registry Services Co., Ltd., “JPRS用語辞典｜レジストリ,” Japan Registry Services Co., Ltd., [オンライン]. Available: https://jprs.jp/glossary/index.php?ID=0102.

[107] Japan Registry Services Co., Ltd., “JPRS用語辞典｜レジストラ,” Japan Registry Services Co., Ltd., [オンライン]. Available: https://jprs.jp/glossary/index.php?ID=0101.

NTT DATA
Trusted Global Innovator

2019年8月29日発行

株式会社NTTデータ
セキュリティ技術部 情報セキュリティ推進室 NTTDATA-CERT担当
大谷 尚通 / 小林 義徳 / 大石 眞央 / 山下 大輔
nttdata-cert@kits.nttdata.co.jp