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 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。

サプライチェーン攻撃

2019年度第2四半期において、サプライチェーン攻撃が再び話題となりました。特にSprint社の事例は特徴的であり、各組織間のセキュリティの責任の境界があいまいなケースに目をつけてWebサイトのシステム間連携を悪用し、「samsung.com」経由で顧客情報を窃取する手法が用いられていました。このような攻撃に対するベストプラクティスを模索することはセキュリティに携わる人たち共通の課題です。

Webスキミングの自動化

データベースシステムをはじめとして、設定不備に関係する情報漏えいは依然として数多く発生しています。また、以前から確認されているWebスキミングの手法が変化しています。攻撃者は、設定不備のあるクラウドサービス上のECサイトを自動的に探索して効率的に攻撃し、ECサイトへWebスキミングを仕込んでクレジットカード情報を盗んでいます。

米国ランサムウェア被害

2019年4月以降、米国でランサムウェア被害が発生し続けています。2019年度第2四半期も数多くのランサムウェア被害が報告されています。地方自治体に加えて、学校や病院も攻撃されて、広く公共機関で被害が発生しています。ランサムウェア感染の一例として「Emotet」「Trickbot」「Ryuk」の3種のマルウェアを組み合わせる「Triple Threat」と呼ばれる攻撃方法が見つかっています。

今後の予測

設定不備や脆弱性を狙う攻撃、マルウェア配布を目的とするメール攻撃、ランサムウェア攻撃など、これまでにも確認された攻撃がより巧妙な手口で継続します。攻撃者は、クラウドサービスの設定不備や脆弱性の自動探索、正規メールと区別できない攻撃メールの送付により、サイバー攻撃を成功させようとしています。これまでと同様の対策では被害が増加するおそれがあります。

2. 注目トピック

2.1. サプライチェーン攻撃

サプライチェーン攻撃とは、今日において2種類の攻撃手法を示す言葉です [1]。
1つ目は、大企業や政府組織など標的の組織を攻撃するために、取引先などの サプライチェーン(商流)において、セキュリティ対策が甘い組織を攻撃の足がかりにする手法です。
2つ目は、ソフトウェアの開発元や配布元などソフトウェアのサプライチェーンを通じて、マルウェアや攻撃コードを挿入したソフトウェアを配布して攻撃の足がかりにする手法です。
この攻撃手法は、「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」の注目トピックとして取り上げています [2]。
2019年度第2四半期では、1つ目のサプライチェーン攻撃のインシデントが再び話題となりました。

表 1:2019年度第2四半期に発生・報告されたサプライチェーン攻撃

No	日付	経由元	概要
1	7/13	請負業者 SyTech社	ニュースメディアZDNetは、攻撃者によりロシアの情報機関である連邦保安庁の情報が業務を請け負っていたSyTech社から盗み出されたと報じた [3]。攻撃者はハッキンググループ「0v1ru$」で、SyTech社のプロジェクト管理ツールJIRAやActive Directoryのサーバにアクセスし、7.5GBもの機密情報を盗み出した。機密情報は「別のハッキンググループDigital Revolution」へ共有された
2	7/22	Samsung.com	ニュースメディアZDnetは、米国の通信事業者であるSprint社がサムスングループの公式サイトsamsung.com経由で不正アクセスを受け、個人情報漏えいが発生したことを報じた [4]。Sprint社が影響を受けたユーザに対して送付したメールによると、新規回線契約のページ"add a line"にて、ユーザのSprintアカウントを用いて不正アクセスが行われていた [5]
3	9/18	ITサービス事業者	シマンテック社は公式ブログにて、2018年7月から攻撃グループ「Tortoiseshell」がサプライチェーン攻撃の第一歩として、サウジアラビアのITサービス事業者を攻撃していると発表した [6]。ITサービス事業者を利用していた11組織が攻撃を受けて、少なくとも2つの組織のドメインコントローラーサーバに情報収集ツールが仕込まれた

表 1のインシデントの中で特徴的だった事例は、No.2の米国大手通信事業者Sprint社の事例です。この事例は、直接Sprint社のWebサイトを攻撃して内部へ侵入してSprint社の顧客情報を盗み出す手法ではなく、一旦サムスングループのグループ会社のWebサイトへ侵入して、

迂回してSprint社の顧客情報を盗み出す手法でした。
ニュースメディアZDNetが報じた記事や、影響を受けた顧客へSprint社が報告した内容によると、不正アクセスはsamsung.com内の「add a line」という新規回線契約用Webページ経由で行われました。
通常利用の場合は、図 1の様な連携がsamsung.comのサイトとSprintの間で行われていたと考えられます。

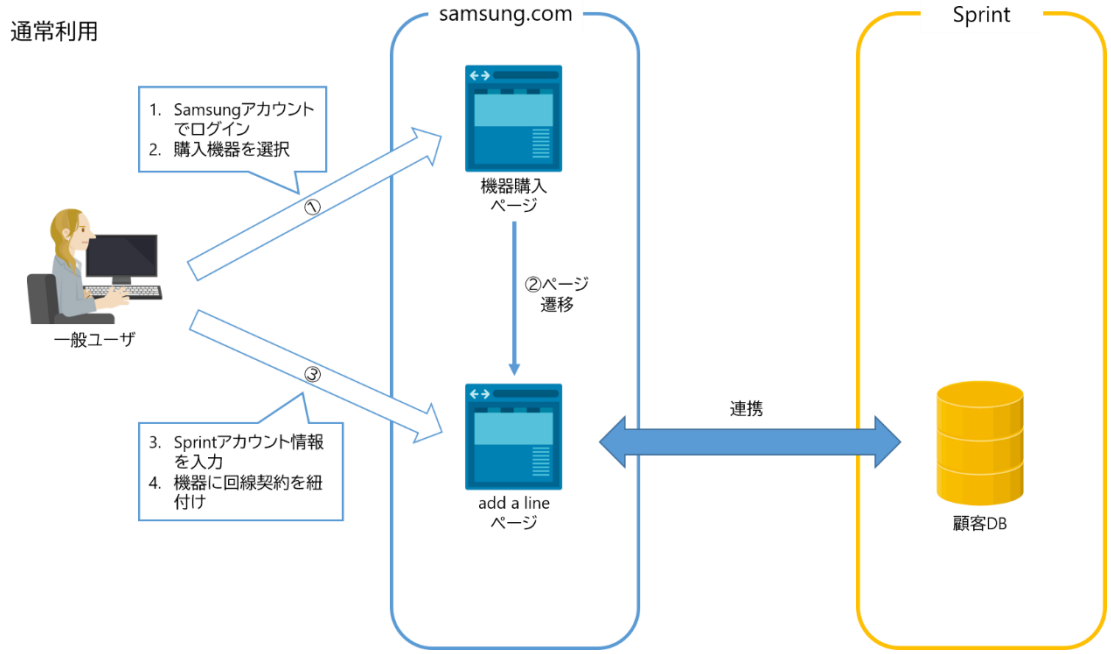


図 1:通常利用のアクセスの流れ(イメージ)

通常利用のアクセスの流れ

① 機器購入ページへアクセス
1. 一般ユーザは自らのSamsungアカウントでsamsung.comにログインする
2. samsung.comの機器購入ページで機器を選択

② 機器購入ページからadd a lineページへ遷移

③ Samsung.comのログイン状態を引き継いでadd a lineページへアクセス
3. 一般ユーザのSprintアカウント情報(IDとパスワード)を入力

④ 認証が成功し、サイト間で連携処理を行う。購入機器と回線契約が紐付けられる
4. 一般ユーザは回線契約情報を閲覧できる

一方、今回のインシデントの場合は図 2の流れで行われたと考えられます。

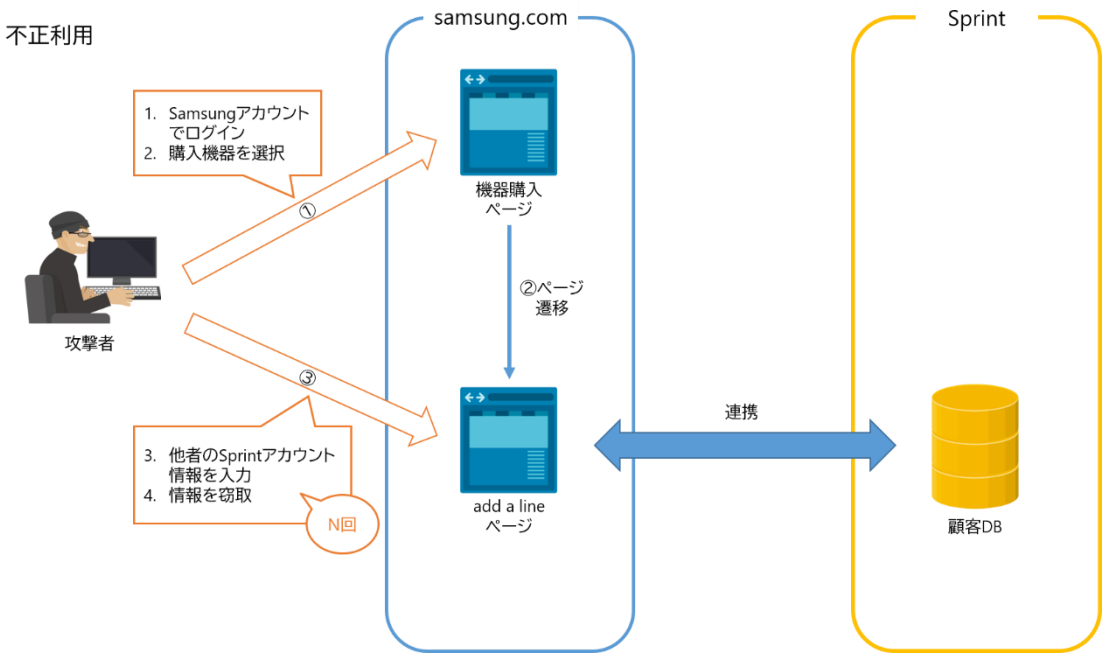


図 2:不正利用のアクセスの流れ(イメージ)

不正利用のアクセスの流れ

① 機器購入ページへアクセス
1. 攻撃者は、予め用意しておいたSamsungアカウントでsamsung.comにログインする
2. Samsung.comの機器購入ページで機器を選択

② 機器購入ページからadd a lineページへ遷移

③ Samsung.comのログイン状態を引き継いでadd a lineページへアクセス
3. 他者のSprintアカウントの認証情報を総当り攻撃で入力

④ 認証が成功した場合、サイト間の連携処理を行う。購入機器と回線契約が紐付けられる
4. 攻撃者は回線契約情報を閲覧できる
5. 3.と4.を繰り返して、Sprintアカウント情報(IDとパスワード)を窃取

通常、攻撃者はセキュリティ対策された組織を攻撃するために、 サプライチェーン(商流)でつながっているセキュリティ対策が甘い組織を攻撃して、その組織を足がかりして標的の組織への攻撃を成功させます。
しかし、前述の事例ではどちらの組織もセキュリティ対策が甘い組織ではないと思われます。一般的にインターネットに公開されているWebシステムのログインページには、総当たり攻撃などの不正アクセスに対するセキュリティ対策を実装しなければならないことが知られています。Samsung.comとSprint社はどちらも自社のWebシステムのログインページへ不正ア

クセス試行の監視や連続ログイン失敗時のロックアウトなどの不正アクセス対策を実装していると考えられます。
セキュリティ対策が充実している組織同士であっても、異なる組織間でシステムが接続する部分や業務が連携する部分は、セキュリティの責任の境界や範囲があいまいなケースが多く見受けられます [7]。本事例では、この責任の境界部分がセキュリティ対策の盲点になり、インシデントが発生しました。サムスングループのグループ会社とSprint社のWebシステムが自動的に連携している部分の不正アクセス対策は、どちらの組織も想定していなかったと考えられます。この境界部分のリスク分析が不十分で、どちらの組織もサムスングループのグループ会社のWebシステムからSprint社のWebシステムへSprintアカウントの総当り攻撃を行えることに気が付かなかったと思われます。

サプライチェーン攻撃は、サプライチェーンで連携した組織がそれぞれ独立してリスク分析やセキュリティ対策を行っても、どこかに抜け漏れが発生するおそれがあります。これを防止するための第一の方法は、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ことです。例えば、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。しかし、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。通常は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。
第二の方法は、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、万が一連携先から攻撃されたり、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べきです。

サプライチェーン攻撃を完全に防ぐことは現実として困難であり、費用対効果が高い施策を以てサプライチェーン全体のリスクを低減することが求められています。今現在、これを解決する決定的な手法や対策は存在していないため、サプライチェーン攻撃に対するベストプラクティスを模索することはセキュリティに携わる人たち共通の課題です。

3. 情報漏えい

2019 年度第 2 四半期に確認された情報漏えい事例についてまとめました。2018 年度第 4 四半期と 2019 年度第 1 四半期から傾向は変わらず、Web スキミングや設定不備による情報漏えいが目立ちます。Web スキミングは攻撃手法が改善されており、より効率的に多数のサイトを侵害する方法が確立されています。設定不備による情報漏えいの事例としては、多数の医療用システムが大量の情報を公開状態にしていることが判明しました。

攻撃の自動化が進むWebスキミング

RISKIQ社の報告によると、攻撃者はECサイトへWebスキミング用の不正コードを挿入する手順をプログラムで自動化しています。攻撃者は、まずAmazon Simple Storage Server（以下、Amazon S3と記載）を使用しているECサイトをスキャンすることで、不適切な設定のAmazon S3を探索します。権限設定が不適切なAmazon S3バケット内にECサイトのJavaScriptファイルが見つかったら、Webスキミング用の不正コードを挿入します。この手順をプログラムで自動的に繰り返せば、攻撃者は短期間で大量のECサイトへWebスキミング用の不正コードを挿入することが可能です。 [8]

Sanguine Security社の調査によると、7月5日にECサイトを侵害する大規模なWebスキミングキャンペーンが発生しました。このキャンペーンでは、24時間以内という短期間で960サイト以上に不正コードが仕込まれました。攻撃者は、自動化されたプログラムを使ってWebスキミングを仕掛けたと分析されています。 [9]

設定不備による情報漏えい

2019年度第2四半期も設定不備による情報漏えいが数多く報告されています。データベースの設定不備が原因で第三者にデータベース内の機密情報が公開されているケースが多いですが、データベース以外の設定不備が原因のケースもあります。7月に米金融大手のCapital One社から1億600万人分の個人情報が漏えいしたインシデントは、ファイアウォールの設定不備が原因と言われています。また、9月に行われたGreenbone Networks社の調査により、サーバの設定不備が原因でインターネット上に医療画像を公開している約2,300の医療用画像管理システムが発見されました。約4億枚の画像が公開状態でした。

情報漏えい事例

表 2に2019年度第2四半期に発生した情報漏えい事例の一部をまとめました。

表 2：情報漏えい事例(2019年度第2四半期)

日付	対象組織	原因	概要
7/1	ORVIBO	設定不備	20億件以上の機密情報を含むデータベースが2週間公開状態だった [10]
7/1	中国公安当局	設定不備	9,000万以上の個人情報を含むデータベースが公開状態だった [11]
7/5	Eコマースストア 多数	Webスキミング	攻撃グループ「Magecart」が不正スクリプト挿入の自動化により962のEコマースストアを侵害した [9]
7/8	Fieldwork	設定不備	個人情報、クレジットカード情報、自動ログインリンク等の情報を含む30日分(26GB)のログデータが公開状態だった [12]
7/30	Capital One	設定不備 不正アクセス	不正アクセスを受けて1億600万人分の個人情報が漏えい。ファイアウォールの設定不備を悪用された [13]
8/19	Option Way	設定不備	vpnMentor社の研究者により、航空券予約サイトのデータベースの情報にアクセス可能であることが判明。100GBの個人情報にアクセス可能だった [14]
8/19	DealerLeads	設定不備	自動車購入者の顧客情報等1億9,800万件を格納するデータベースが公開状態だった [15]
9/4	Facebook	設定不備	Facebookアカウントにリンクした電話番号4億1,900万件がパスワードで保護されていないサーバ上で発見された [16]
9/11	Lion Air グループ	不正アクセス	請負業者スタッフの不正アクセスにより最大3,500万人の個人情報が漏えいした [17] [18]
9/16	医療用システム 多数	設定不備	Greenbone Networks社の調査より、約2,300の医療用画像管理システムが約4億枚の医療画像を公開していると判明した [19]

まとめ

自動化されたWebスキミングを含め、設定不備に関係する情報漏えいを取り上げました。情報漏えいを未然に防ぐには、システムを正しく設定することが重要です。また、使用するハードウェア、ソフトウェアの脆弱性を確認することも重要です。攻撃者がシステムを侵害するためにセキュリティの欠陥を悪用する点は変化していません。攻撃者は攻撃プログラムの自動化により、インターネット上にある設定不備や脆弱性が残存しているシステムを24時間探索しています。そのため、脆弱性情報公開や設定不備発生の瞬間から、それらを発見して攻撃を開始するまでの時間が非常に短くなっています。設定不備の発生から10分程度で攻撃が行われたという実験結果もあります。管理が不十分なシステムは、想像している以上に、短い時間で侵害されるおそれがあります。設定不備の防止、迅速なセキュリティパッチの適用を実施して、不正アクセスや情報漏えいを未然に防ぐことが重要です。

4. 脆弱性

4.1. 複数のSSL VPN製品の脆弱性

2019年9月6日、JPCERT/CCが「複数の SSL VPN 製品の脆弱性に関する注意喚起」を公開しました [20]。該当の製品および脆弱性は以下の通りです。

- CVE-2019-1579 ：PAN-OS（Palo Alto Networks）
- CVE-2019-11510：Pulse Connect Secure, Pulse Policy Secure（Pulse Secure）
- CVE-2018-13379：FortiOS（Fortinet）

上記のなかには、他の脆弱性と組み合わせることで任意コード実行まで可能になる脆弱性もあり、いずれも深刻です。これらの脆弱性は、8月に発表されたことにより、セキュリティ専門家や攻撃者に広く認識されました。8月下旬より、攻撃者による脆弱性のスキャン活動やSSL VPN 製品への攻撃が活発化しました。

DEVCORE社は、8月に開催された「black hat USA 2019」で上記の複数のSSL VPN 製品の脆弱性とその攻撃方法を発表しました [21]。SSL VPN製品は、物理的な専用線等の設備なしで、インターネット経由でユーザが安全に内部ネットワークへ接続できるようにする製品です。SSL VPN 製品に問題があれば、攻撃者がインターネットから内部ネットワークへ接続可能になります。そのため、SSL VPN 製品には、高い安全性が求められます。DEVCORE社の発表によれば、SSL VPN製品は多くの企業が採用していますが、そのシェアは少数ベンダの製品に集中しています。そのため1つの製品の脆弱性でも、SSL VPNを使っているシステムへ影響する割合は高くなります。

BAD PACKETS社は、8月下旬にPulse Secure製品の脆弱性（CVE-2019-11510）に対する大量のスキャン活動を検知しました [22]。調査結果では、8月24日時点でこの脆弱性が修正されていない状態のPulse Secure製品がインターネット上で合計14,528台発見されました。

Fortinet社とPulse Secure社のSSL VPN製品は、これまでに報告された脆弱性が少なかったため、多くのユーザは頻繁にセキュリティパッチの確認を行っていなかったと思われます [21]。そのため同ユーザは、上記の脆弱性とそのセキュリティパッチに気づくことが遅れて、攻撃を受けてしまったおそれがあります。情報セキュリティ担当者は、SSL VPN 製品のようなインターネット接続境界を守るネットワーク機器の脆弱性やセキュリティパッチの情報に注意が必要です。脆弱性やセキュリティパッチの情報が提供される頻度が低くても、それらの情報の確認作業は、手を抜かずに実施しなければなりません。

4.2. その他の攻撃に利用された脆弱性

2019 年度第 2 四半期に攻撃された複数の脆弱性を以下の表 3 に示します。ただし、「複数の SSL VPN 製品の脆弱性」に関係する脆弱性は除きます。

表 3：攻撃に利用された脆弱性（2019年度第2四半期）

CVE番号・別名	対象製品	概要
CVE-2019-9082 CVE-2019-3396 CVE-2018-7600 他	ThinkPHP Atlassian Confluence Drupal	F5社が、マルウェア「Golang」がLinuxサーバの複数の脆弱性を悪用して、マイニングマルウェアを拡散していると7月2日にブログで報告した [23]
CVE-2017-11774	Outlook	米サイバー軍が2017年10月に公開された脆弱性を悪用した政府ネットワークへのサイバー攻撃について7月3日に警告した [24]
CVE-2019-1132	Windows	2019年6月に攻撃グループ「Buhtrap」が政府機関に脆弱性を悪用したゼロデイ攻撃を実施 [25] [26]。7月9日に脆弱性情報が公開された
CVE-2019-8978	Ellucian Banner System	米教育省が大学向けERPを標的とした攻撃を7月17日に警告。62の大学に影響した [27]
CVE-2019-0708 BlueKeep	Windows	7月23日にツール「CANVAS」にエクスプロイトが追加 [28]。7月24日にマルウェア「WatchBog」に脆弱性スキャン機能が追加 [29]。9月6日にツール「Metasploit」にエクスプロイトが追加 [30]
複数の脆弱性	WordPress （プラグイン）	Wordfence社が複数のWordPressプラグインの脆弱性を悪用する攻撃を報告 [31] [32]
CVE未採番	Apple iOS	Google社が未公開の脆弱性を悪用してハッキングを試みるWebサイトを発見。Apple社は、攻撃は限定的であると発表 [33] [34]
CVE未採番	LINE	LINE社が、8月31日に脆弱性の報告を受け、同日中に修正したと報告。8月30日から8月31日にかけて攻撃を確認 [35]
CVE未採番 Simjacker	SIMカード	Adaptive Mobile Security社がSIMカードの脆弱性を悪用する攻撃「Simjacker」について9月12日に発表。2年前から悪用されていた [36]
CVE-2019-1367	Internet Explorer	Microsoft社が9月23日に定例外のセキュリティ更新プログラムで2件の脆弱性を修正。うち1件のIEの脆弱性は脆弱性公開前の悪用を確認 [37]

5. マルウェア・ランサムウェア

米国で急増するランサムウェア被害

2019年度第2四半期は、第1四半期から引き続き米国でのランサムウェア被害が急増しています。地方自治体は引き続き標的にされており、地方自治体以外にも学校や医療機関が標的にされています。2019年度第2四半期における米国のランサムウェア被害事例を表 4にまとめました。

表 4：米国ランサムウェア被害事例

日付	標的	概要
7/1	ジョージア州 裁判所	ランサムウェアによる攻撃を受け、裁判所のネットワークを停止した。ランサムウェア「Ryuk」が使用された [38]
7/5	マサチューセッツ州 ニューベッドフォード市	ランサムウェア「Ryuk」の亜種による被害を受け、158台のコンピュータが暗号化された。530万ドルの身代金を要求されたが、支払いを拒否した [39]
7/6	インディアナ州 ラポート郡	ランサムウェア「Ryuk」の攻撃を受けて13万ドルの身代金を支払った。早期発見により、感染端末をネットワーク全体の7%に抑えたが、ドメインコントローラが含まれていたため、システムを停止した [40]
7/10	ニューヨーク州 Monroe College	ランサムウェア攻撃を受けてシステムを停止した。200万ドル相当のビットコインを要求されたが、身代金の支払いは不明 [41]
7/16	インディアナ州 ビーゴ郡	Associated Press社が、使用されたランサムウェアを特定できていないことや身代金要求に応じない方針であることを報じた [42]
7/27	ジョージア州 公安局	ランサムウェア攻撃を受け、Georgia State Patrol、Georgia Capitol Police、Georgia Motor Carrier Compliance Divisionが影響を受けた。全ITシステムを停止したが、電話等を代用することで業務に影響はなかった [43]
7/30	アラバマ州 ヒューストン郡 学校	マルウェア攻撃を受けて、1週間のうちに2度も開校日を延期した。セキュリティ専門家は、ランサムウェア攻撃に遭い、システム回復に時間を要したと推測している [44]
8/16	テキサス州 政府機関	23の政府機関のシステムがランサムウェアによる同時攻撃を受けた。影響を受けたほとんどのシステムは、小規模な地方自治体のシステムであった。身代金は支払わない方針である [45]
8/27	歯科医院	Digital Dental Record社がPerCSoft社と共同で提供する米歯科診療向けクラウドサービス「DDS Safe」がランサムウェア攻撃を受けた。400の歯科医院が患者情報にアクセスできない等の影響を受けた [46]

日付	標的	概要
9/4	コネチカット州 ウォルコット公立学校	ランサムウェア攻撃を受け、学校関係者はインターネットやメールシステムを利用できない状況になった。ウォルコット公立学校は6月にもランサムウェア攻撃を受けており、2度目の被害となる [47]
9/20	ワイオミング州 キャンベル郡 記念病院	ランサムウェア攻撃の被害を受けて、病院の運営が影響を受けた。キャンセルした手術や検査もあり、必要に応じて患者を別の施設に移送する方針を発表した [48]

急増するランサムウェア被害を受けて、米国の複数の組織が声明や方針を発表しています。米国市長会議は、7月10日にランサムウェア攻撃を受けた際の身代金支払いに反対する決議を採択しました [49]。7月30日には、CISA[1]、MS-ISAC[2]、NGA[3]、NASCIO[4]が、対策として「システムのバックアップ」「職員のサイバー攻撃に対するトレーニング」「攻撃発生時のインシデント対応計画の見直し」を実施するよう呼び掛ける共同声明を発表しています [50]。CISAは、8月21日に「組織を保護するために実施すること」「感染した際に実施すること」「今後の環境を保護するために実施すること」等をまとめた手順書を公開しました [51]。また、Morning Consult社とIBM社が共同で行った調査によると、米国市民の63%は身代金支払いに税金を使用するよりも、復旧費用に当てることを望んでおり、90%近くがサイバー攻撃で麻痺する都市機能を守るための連邦予算を増やすことに賛成しています [52]。

ランサムウェア攻撃につながるEmotet拡散メール

ランサムウェア被害につながるサイバー攻撃の一例として、Emotet拡散メールがあります [53]。攻撃者はまず、標的とする組織内の人間に対してメールを悪用してマルウェア「Emotet」を拡散します。Emotetに感染した端末は、Emotetのマルウェアを配布する機能によって、マルウェア「TrickBot」に感染します。TrickBotの主な機能は情報窃取です。TrickBotは、標的組織の機密性の高い情報を窃取します。もし身代金を要求できるような重要な情報を取得できた場合は、ランサムウェア「Ryuk」をダウンロードして実行します。この攻撃手法は、マルウェア配布機能としてEmotetを、情報窃取機能としてTrickBotを、身代金要求のためのランサムウェアとしてRyukを用いており、3種類のマルウェアを組み合わせることから「Triple Threat」と呼ばれます。Triple Threatの攻撃の流れを図 3に示します。Triple Threatの実際の事例としては、米フロリダ州が6月に攻撃を受け、46万ドルを攻撃者に支払いました [54]。

[1] Cybersecurity and Infrastructure Security Agency

[2] Multi-State Information Sharing and Analysis Center

[3] National Geospatial-Intelligence Agency

[4] National Association of State Chief Information Officers

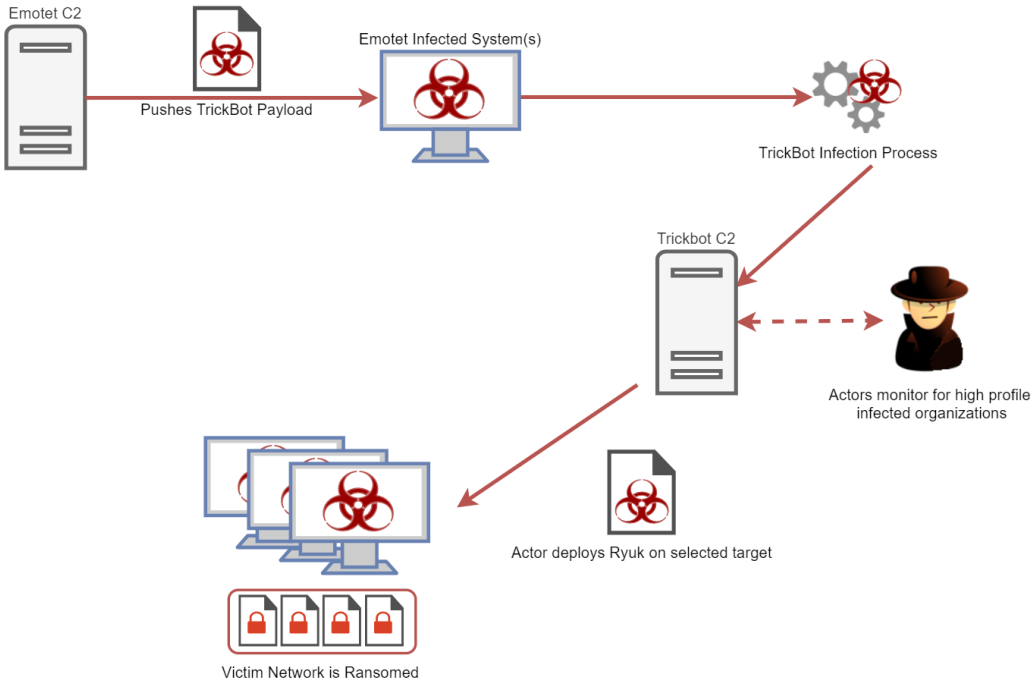


図 3：「Triple Threat」攻撃の流れ
（CYBEREASON公式ブログより転載 [53]）

Emotetの動向

2019年度第1四半期のレポートで述べたように、Emotetは5年以上も進化を続けているマルウェアです。Cofense社の調査によると、Emotetは5月の活発な活動の後、6月と7月の大半は活動を停止していました [55]。しかし、MalwareTech社の調査により8月21日にアクティブなC&Cサーバが新たに発見され、ブラジル、メキシコ、ドイツ、日本、米国を含む複数の拠点においてEmotetの活動が観測されました [56]。現在、Emotetは主にメールで拡散しており、手口の巧妙化が進んでいます。2019年第2四半期以降は、日本国内において件名や本文が日本語で記載されたEmotet拡散メールが数多く確認されました。

Emotetは、可能な限り多くの端末に感染するワーム機能や、感染端末から他組織に感染を広げるためのメール拡散機能、他のマルウェアを配布する機能を備えていることから非常に危険なマルウェアです。上記の理由から、CISAは7月に発表した警告文のなかで、Emotetをこれまでに見たなかで最も破壊的なボットネットの1つであると記載しています [57]。ソフォス社が過去に公開したレポートのなかでも、Emotetによる攻撃は2017年のWannaCryによる攻撃よりも危険であると記載されています [58]。

まとめ

2019年度第1四半期から継続して、2019年度第2四半期現在も、ランサムウェア攻撃が米国に集中し、多くの被害が発生しています。攻撃者が米国の地方自治体を標的にする主な理由は、米国が他国に比べてランサムウェア攻撃を受けて身代金を支払う傾向が強かったからであると考えられます。今後は、ランサムウェア攻撃を受けた際の身代金支払いに反対する決議などが影響して、ランサムウェアの標的が変化するかもしれません。

CISAが8月に公開した警告文 [51]に書かれた今すぐに実施すべきことには、データのバックアップやシステム更新に加えて、最新の事例を用いた訓練が記載されています。ランサムウェアによる被害を最小限に留めたり、早期に復旧したりするためには、訓練が重要な対策です。まずは、ランサムウェアに感染した時の状況やインシデント対応の詳細が書かれた報告書を参考に、自社で同様のインシデントが発生した場合を想定して、対応手順を作成しましょう。つぎにその手順を用いて、実際にシステムが正しく復旧できることを確認しましょう。最後に、いざというときに感染したマシンを隔離したりネットワークを遮断したりして、被害を最小限に留めたり、バックアップからシステムを復旧して、短時間で業務を正常な状態へ戻せるよう、訓練をおこないましょう。

6. 予測

2019年度第2四半期の事例から、現在の傾向および今後の予測を記載します。既存の攻撃手法に対して、自動化、巧妙化、機能追加、標的変更などが行われる傾向があります。これまでと同様の対策では防ぎきれないケースがあり、注意が必要です。

設定不備を自動探索するサイバー攻撃手法の発生

攻撃者は、設定不備のあるサービスやシステムを効率的に攻撃する手法を確立しています。「3. 情報漏えい」で記載した自動化されたWebスキミングは、Amazon S3の設定不備をスキャンすることにより24時間で960サイトを侵害しました。ポートスキャンに比べて、AWSのような特定のサービスに標的を絞ることで、同様の設定不備がある攻撃対象をまとめて検出可能です。パブリッククラウドやプラットフォームの利用機会が増加している現代において、非常に危険な攻撃手法です。2019年第3四半期以降は、人気の高いパブリッククラウドやプラットフォーム上の設定不備が、まとめて標的になるおそれがあります。これらのサービスやシステムを利用している場合は、アクセス制御をはじめとするセキュリティ関連の設定を正しく実施してください。

メールを使ったマルウェア配布

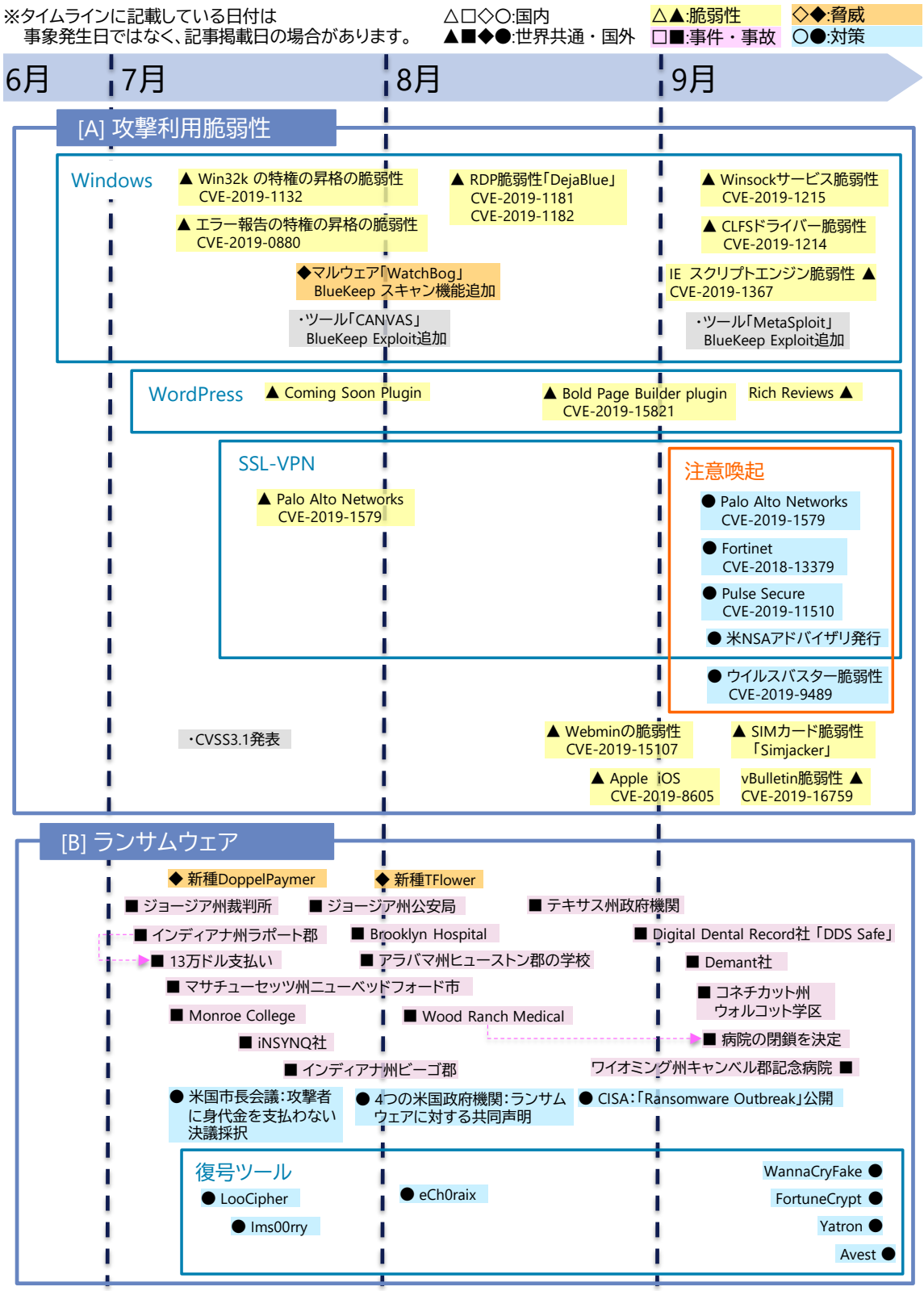
標的型のマルウェア配布には、依然としてメールが悪用されています。これは、異なる組織間の業務で最も利用されているコミュニケーションツールが、相変わらずメールであるためです。異なる組織間の業務連絡でもメール以外のコミュニケーションツールを利用する企業は増加傾向にありますが、メールを利用する組織に比べてまだ少数です。現状では、メールの利用を完全に廃止することは困難です。この特徴から、攻撃者にとってメールは外部組織の人間を装い標的を騙す手法に適しているといえます。これらの理由から、2019年第3四半期以降も、しばらくはメールを悪用するサイバー攻撃が継続すると予測します。特にマルウェアを配布するメールは、次々と新たな手法で巧妙に標的を騙そうとするため、被害が続くと考えます。

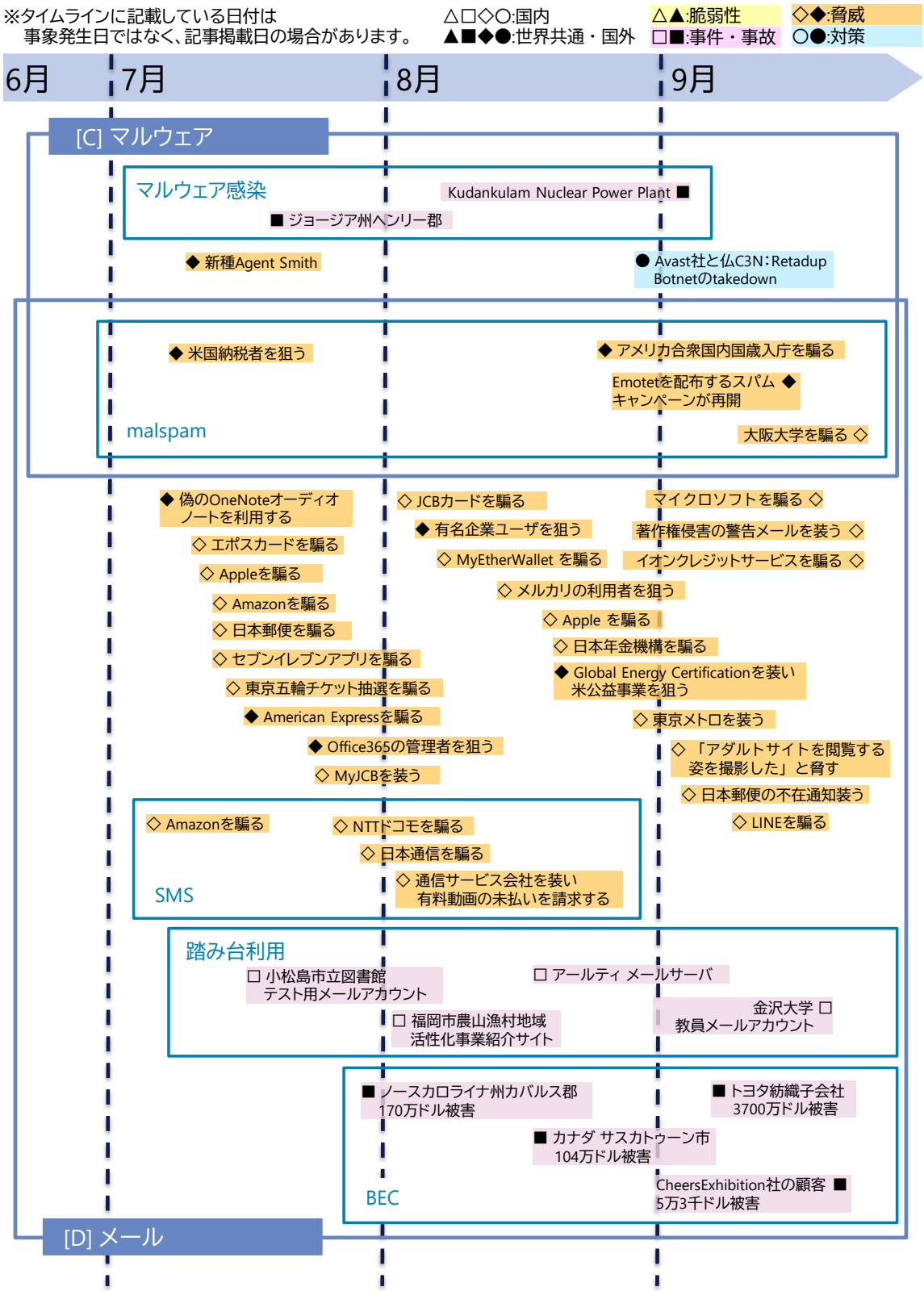
ランサムウェア攻撃の被害拡大

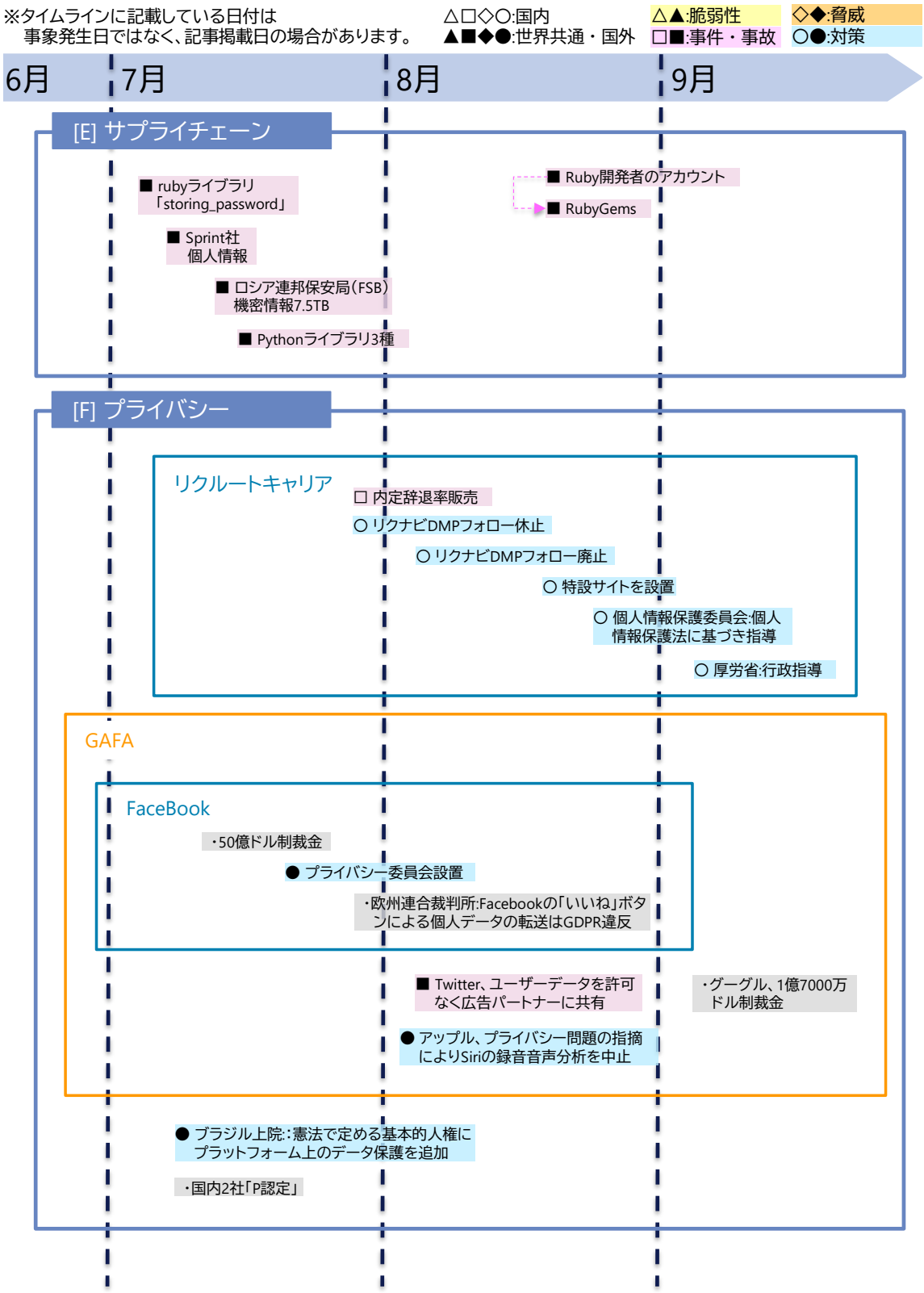
現在、ランサムウェア攻撃が米国の地方自治体等の組織に集中しています。これは、他国に比べてランサムウェア攻撃を受けて身代金を支払う傾向が強かった米国が標的にされたおそれがあります。しかし、米国も多くの被害を受けて身代金支払いに反対する意見が強くなっています。米国が他国と同様に身代金支払いに簡単に応じなくなれば、標的は変化すると考

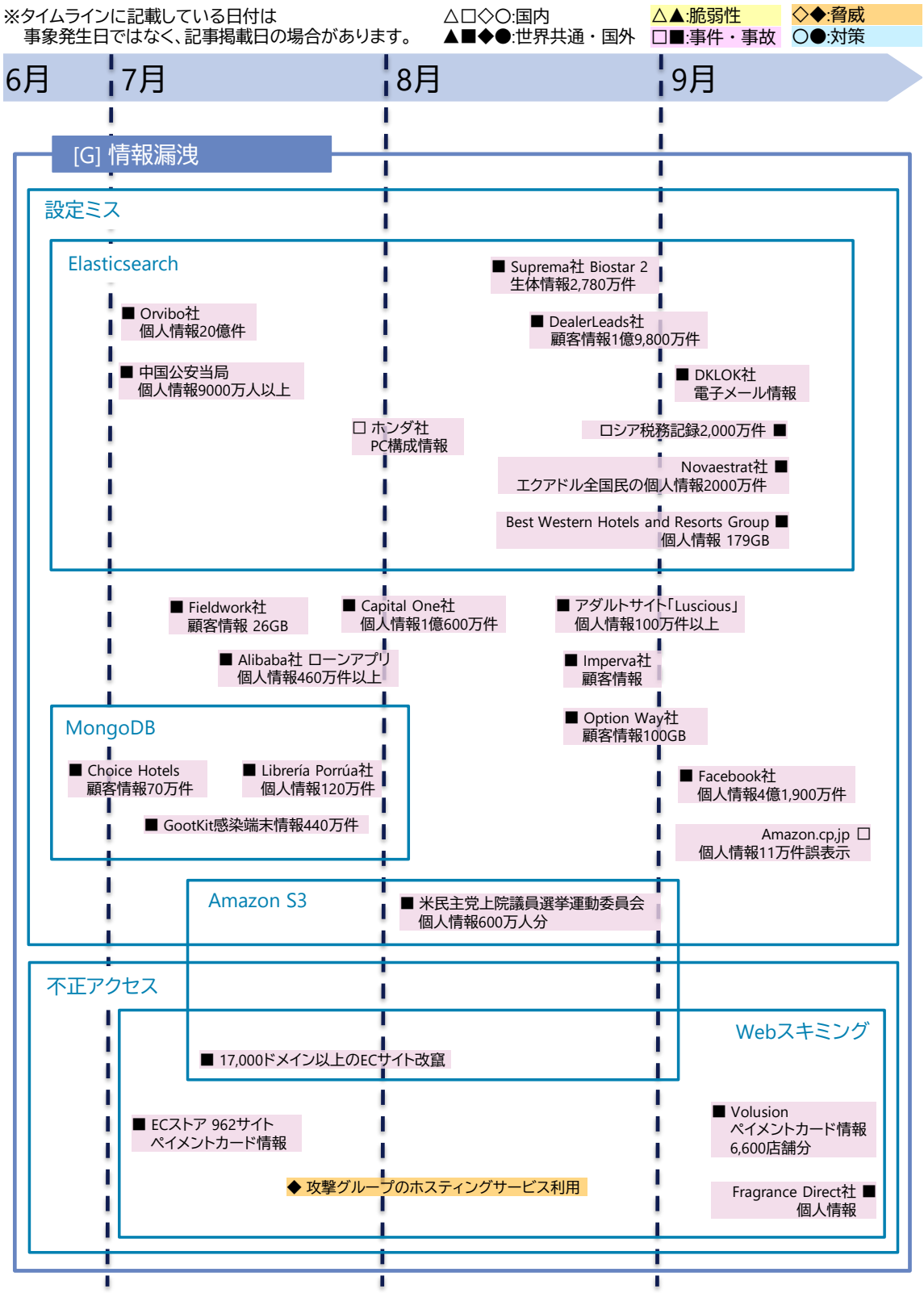
えられます。また、ランサムウェア攻撃は攻撃が成功して標的が身代金を支払った場合は大きな収入を得ますが、攻撃が成功しても標的が身代金を支払わない場合は全く収入が得られません。この特性から攻撃者は、攻撃の成功率を上げることよりも、同時に数多くの組織へ攻撃を仕掛けることに注力しています。このことから、2019年第3四半期以降はより多くの組織がランサムウェア攻撃を受けると予測します。ランサムウェア攻撃を受けて被害が発生する前に、自組織の対策状況、復旧や身代金支払いに関する方針を再度検討してください。

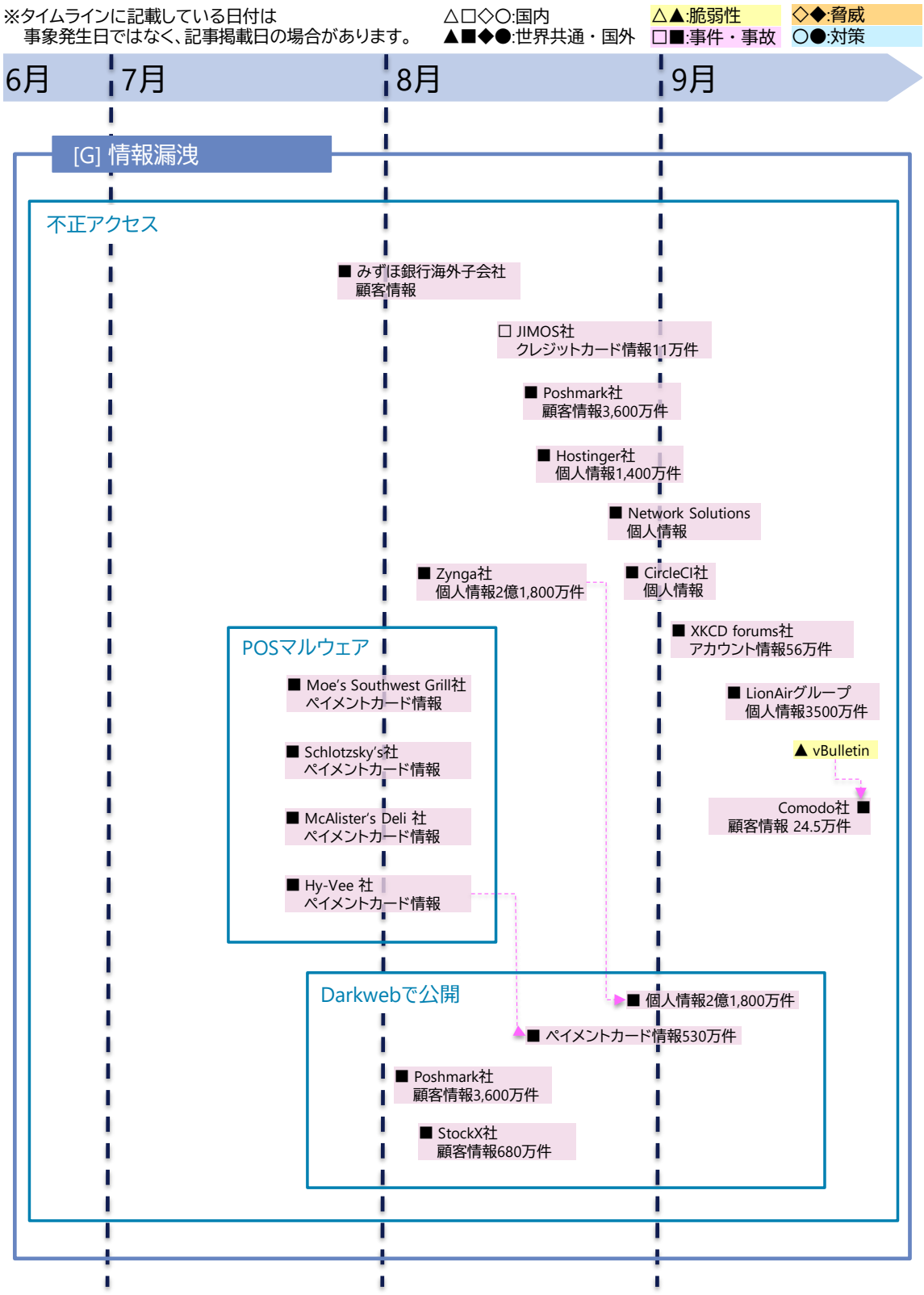
7. タイムライン

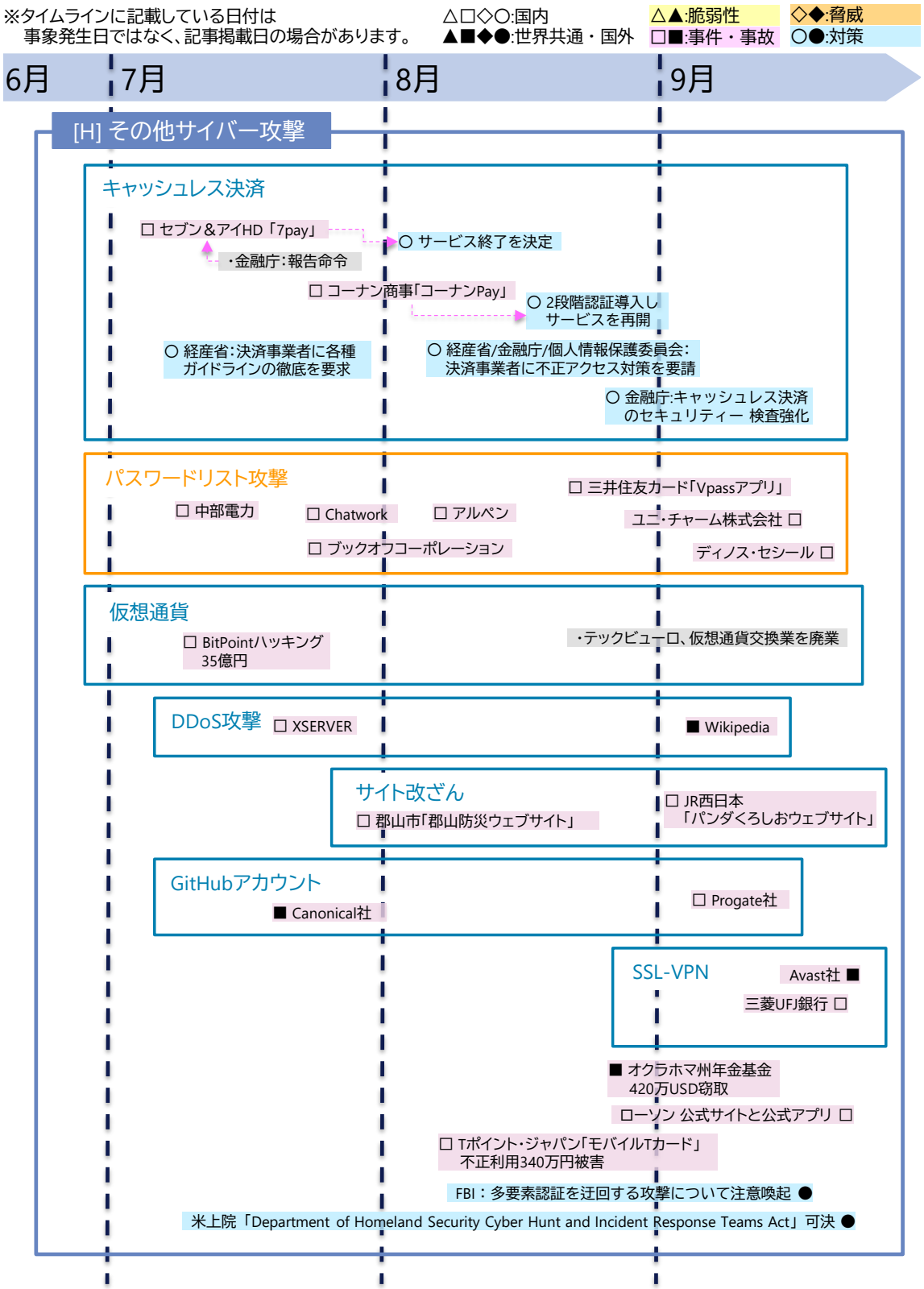












参考文献

[1] KADOKAWA ASCII Research Laboratories, Inc, “2018年はどんなセキュリティ脅威が？9社予測まとめ《前編》,” 5 1 2018. [オンライン]. Available: https://ascii.jp/elem/000/001/611/1611970/.

[2] 尚. 大谷, 義. 小林, 眞. 大石 , 大. 山下, “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,” 株式会社NTTデータ, 30 5 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2018_4q_securityreport.pdf.

[3] C. Cimpanu, “Hackers breach FSB contractor, expose Tor deanonymization project and more,” CBS Interactive., 20 7 2019. [オンライン]. Available: https://www.zdnet.com/article/hackers-breach-fsb-contractor-expose-tor-deanonymization-project/.

[4] C. Cimpanu, “Sprint says hackers breached customer accounts via Samsung website,” CBS Interactive., 16 7 2019. [オンライン]. Available: https://www.zdnet.com/article/sprint-says-hackers-breached-customer-accounts-via-samsung-website/.

[5] C. Cimpanu, “Sprint breach notification (Samsung.com),” Scribd Inc., [オンライン]. Available: https://www.scribd.com/document/417811440/Sprint-breach-notification-Samsung-com. [アクセス日: 12 11 2019].

[6] Symantec Security Response Attack Investigation Team, “Tortoiseshell Group Targets IT Providers in Saudi Arabia in Probable Supply Chain Attacks,” Broadcom., 18 9 2019. [オンライン]. Available: https://www.symantec.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain.

[7] “「ITサプライチェーンにおける情報セキュリティの責任範囲に関する調査」報告書について,” 独立行政法人 情報処理推進機構, 19 4 2019. [オンライン]. Available: https://www.ipa.go.jp/security/fy30/reports/scrm/index.html.

[8] RISKIQ, “Spray and Pray: Magecart Campaign Breaches Websites En Masse Via Misconfigured Amazon S3 Buckets,” 10 7 2019. [オンライン]. Available: https://www.riskiq.com/blog/labs/magecart-amazon-s3-buckets/.

[9] BleepingComputer, “Automated Magecart Campaign Hits Over 960 Breached Stores,” 5 7 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/automated-magecart-campaign-hits-over-960-breached-stores/.

[10] ZDNet, “Smart home maker leaks customer data, device passwords,” 1 7 2019. [オンライン]. Available: https://www.zdnet.com/article/smart-home-maker-leaks-customer-data-device-passwords/.

[11] Bleeping Computer, “Over 90 Million Records Leaked by Chinese Public Security Department,” 8 7 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/over-90-million-records-leaked-by-chinese-public-security-department/.

[12] vpnMentor, “Report: Fieldwork Software Leaks Sensitive Customer Data,” 8 7 2019. [オンライン]. Available: https://www.vpnmentor.com/blog/report-fieldwork-leak/.

[13] Capital One, “Information on the Capital One Cyber Incident,” 28 7 2019. [オンライン]. Available: https://www.capitalone.com/facts2019/.

[14] vpnMentor, “Report: Flight Booking Platform Exposes Customer Data,” 2 9 2019. [オンライン]. Available: https://www.vpnmentor.com/blog/report-option-way-leak/.

[15] Security Discovery, “Auto Dealer Leads Network Exposed 198 Million Records Online,” 11 9 2019. [オンライン]. Available: https://securitydiscovery.com/dealer-leads/.

[16] TechCrunch, “A huge database of Facebook users’ phone numbers found online,” 4 9 2019. [オンライン]. Available: https://www.businessinsider.jp/post-198159.

[17] ZDNet, “AWS servers 'secure' following Malindo Air data breach,” 20 9 2019. [オンライン]. Available: https://www.zdnet.com/article/aws-says-servers-secure-following-malindo-air-data-breach/.

[18] The Jakarta Post, “Lion Air data stolen, leaked by ex-GoQuo employees,” 24 9 2019. [オンライン]. Available: https://www.thejakartapost.com/news/2019/09/24/lion-air-data-stolen-leaked-by-ex-goquo-employees.html.

[19] Grreenbone Networks, “Information Security Report,” 16 9 2019. [オンライン]. Available: https://www.greenbone.net/wp-content/uploads/CyberResilienceReport_EN.pdf.

[20] JPCERT/CC, “複数の SSL VPN 製品の脆弱性に関する注意喚起,” 6 9 2019. [オンライン]. Available: https://www.jpcert.or.jp/at/2019/at190033.html.

[21] DEVCORE, “Infiltrating Corporate Intranet,” 7 8 2019. [オンライン]. Available: https://i.blackhat.com/USA-19/Wednesday/us-19-Tsai-Infiltrating-Corporate-Intranet-Like-NSA.pdf.

[22] BAD PACKETS, 24 8 2019. [オンライン]. Available: https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/.

[23] F5, “New Golang Malware is Spreading via Multiple Exploits to Mine Monero,” 2 7 2019. [オンライン]. Available: https://www.f5.com/labs/articles/threat-intelligence/new-golang-malware-is-spreading-via-multiple-exploits-to-mine-mo.

[24] Security Affairs, “US Cyber Command warns of Iran-linked hackers exploiting CVE-2017-11774 Outlook flaw,” 3 7 2019. [オンライン]. Available: https://securityaffairs.co/wordpress/87895/breaking-news/cve-2017-11774-apt33-attacks.html.

[25] Microsoft, “CVE-2019-1132 | Win32k Elevation of Privilege Vulnerability,” 9 7 2019. [オンライン]. Available: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1132.

[26] Bleeping Computer, “Windows Zero-Day Used by Buhtrap Group For Cyber-Espionage,” 11 7 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/windows-zero-day-used-by-buhtrap-group-for-cyber-espionage/.

[27] Federal Student Aid, “TECHNOLOGY SECURITY ALERT – Exploitation of Ellucian Banner System Vulnerability,” 17 7 2019. [オンライン]. Available: https://ifap.ed.gov/eannouncements/071719ITSecurAlertExploitationEllucianBannerSysVulnerability.html.

[28] Bleeping Computer, “BlueKeep RCE Exploit Module Added to Penetration Testing Tool,” 25 7 2019. [オンライン]. Available: bleepingcomputer.com/news/security/bluekeep-rce-exploit-module-added-to-penetration-testing-tool/.

[29] INTEZER, “Watching the WatchBog: New BlueKeep Scanner and Linux Exploits,” 19 7 2019. [オンライン]. Available: https://www.intezer.com/blog-watching-the-watchbog-new-bluekeep-scanner-and-linux-exploits/.

[30] ZDNet, “Metasploit team releases BlueKeep exploit,” 6 9 2019. [オンライン]. Available: https://www.zdnet.com/article/metasploit-team-releases-bluekeep-exploit/.

[31] Wordfence, “Recent WordPress Vulnerabilities Targeted by Malvertising Campaign,” 22 7 2019. [オンライン]. Available: https://www.wordfence.com/blog/2019/07/recent-wordpress-vulnerabilities-targeted-by-malvertising-campaign/.

[32] Wordfence, “Ongoing Malvertising Campaign Evolves, Adds Backdoors and Targets New Plugins,” 30 8 2019. [オンライン]. Available: https://www.wordfence.com/blog/2019/08/ongoing-malvertising-campaign-continues-exploiting-new-vulnerabilities/.

[33] Google Project Zero, “A very deep dive into iOS Exploit chains found in the wild,” 29 8 2019. [オンライン]. Available: https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html.

[34] Apple, “A message about iOS security,” 6 9 2019. [オンライン]. Available: https://www.apple.com/newsroom/2019/09/a-message-about-ios-security/.

[35] LINE, “LINEアカウントのプロフィール画像を変更可能な脆弱性の修正のお知らせ,” 2 9 2019. [オンライン]. Available: https://linecorp.com/ja/security/article/224.

[36] AdaptiveMobile Security, “Simjacker – Next Generation Spying Over Mobile,” 12 9 2019. [オンライン]. Available: https://www.adaptivemobile.com/blog/simjacker-next-generation-spying-over-mobile.

[37] Microsoft, “CVE-2019-1367 | Scripting Engine Memory Corruption Vulnerability,” 23 9 2019. [オンライン]. Available: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367.

[38] SOPHOS, “Georgia’s court system hit by ransomware,” 3 7 2019. [オンライン]. Available: https://nakedsecurity.sophos.com/2019/07/03/georgias-court-system-hit-by-ransomware/.

[39] New Bedford, “MAYOR DISCUSSES IMPACT OF RANSOMWARE ATTACK ON NEW BEDFORD’S COMPUTER SYSTEM,” 5 7 2019. [オンライン]. Available: https://www.newbedford-ma.gov/blog/news/mayor-discusses-impact-of-ransomware-attack-on-new-bedfords-computer-system/.

[40] NEWS-DISPATCH, “Malware attack on county computers,” 9 7 2019. [オンライン]. Available: https://www.thenewsdispatch.com/news/article_d9809e48-7e8d-52d5-9d08-5d6c1adab2a2.html.

[41] Inside Higher, “Hackers Demand $2 Million From Monroe,” 15 7 2019. [オンライン]. Available: https://www.insidehighered.com/news/2019/07/15/hackers-demand-2-million-monroe-college-ransomware-attack.

[42] Associated Press, “Indiana county targeted in malware assault on computers,” 24 7 2019. [オンライン]. Available: https://apnews.com/65b22b56e7384c7db4031a07c92c64f9.

[43] Fox 5 News, “Multiple Georgia state law enforcement agencies hit by ransomware attack,” 28 7 2019. [オンライン]. Available: https://www.fox5atlanta.com/news/multiple-georgia-state-law-enforcement-agencies-hit-by-ransomware-attack.

[44] WTVY, “Houston County Schools pushes school start back further,” 30 7 2019. [オンライン]. Available: https://www.wtvy.com/content/news/Houston-County-Schools-Announces-Additional-Delay-513399671.html.

[45] DIR, “Update on Texas Local Government Ransomware Attack,” 5 9 2019. [オンライン]. Available: https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=213.

[46] ZDNet, “Ransomware hits hundreds of dentist offices in the US,” 29 8 2019. [オンライン]. Available: https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/.

[47] Republican-American, “Wolcott school computers remain shut down a week after malware attack,” 9 9 2019. [オンライン]. Available: https://www.rep-am.com/local/news-local/2019/09/09/wolcott-school-computers-remain-shut-down-a-week-after-malware-attack/.

[48] Campbell Country Health, “SERVICE DISRUPTIONS AT CCH; NO ETA,” 20 9 2019. [オンライン]. Available: https://www.cchwyo.org/News/Press_Center/Health_News/2019/Service_Disruptions_at_CCH_no_ETA.aspx.

[49] The United States Conference of Mayors, “2019 Adopted Resolutions,” 9 7 2019. [オンライン]. Available: http://legacy.usmayors.org/resolutions/87th_Conference/proposedcommittee-preview.asp?committee=Criminal%20and%20Social%20Justice.

[50] The Cybersecurity and Infrastructure Security Agency, “Steps to Safeguard Against Ransomware Attacks,” 30 7 2019. [オンライン]. Available: https://www.us-cert.gov/ncas/current-activity/2019/07/30/steps-safeguard-against-ransomware-attacks.

[51] The Cybersecurity and Infrastructure Security Agency, “CISA Insights: Ransomware Outbreak,” 21 8 2019. [オンライン]. Available: https://www.us-cert.gov/ncas/current-activity/2019/08/21/cisa-insights-ransomware-outbreak.

[52] IBM, “LOCAL GOVERNMENT RANSOMWARE STUDY,” 5 9 2019. [オンライン]. Available: https://www.ibm.com/downloads/cas/MKPQVOL6.

[53] CYBEREASON, “TRIPLE THREAT: EMOTET DEPLOYS TRICKBOT TO STEAL DATA & SPREAD RYUK,” 25 4 2019. [オンライン]. Available: https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware.

[54] ZDNet, “Florida city fires IT employee after paying ransom demand last week,” 1 7 2019. [オンライン]. Available: https://www.zdnet.com/article/florida-city-fires-it-employee-after-paying-ransom-demand-last-week/.

[55] BANK INFO SECURITY, “Emotet Botnet Shows Signs of Revival,” 26 8 2019. [オンライン]. Available: https://www.bankinfosecurity.com/emotet-botnet-shows-signs-revival-a-12964.

[56] Bleeping Computer, “Emotet Botnet Is Back, Servers Active Across the World,” 23 8 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/emotet-botnet-is-back-servers-active-across-the-world/.

[57] Cybersecurity and Infrastructure Security Agency, “Alert (TA18-201A),” 20 7 2019. [オンライン]. Available: https://www.us-cert.gov/ncas/alerts/TA18-201A.

[58] SOPHOS, “Emotet:Nastier Than WannaCry and Harder to Stop,” 7 2 2019. [オンライン]. Available: https://dbac8a2e962120c65098-4d6abce208e5e17c2085b466b98c2083.ssl.cf1.rackcdn.com/emotet-nastier-than-wannacry-harder-to-stop-pdf-2-w-5139.pdf.

NTT DATA
Trusted Global Innovator

2019年11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