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1四半期）

2018年7月26日

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

エグゼクティブサマリー

5/25にEU一般データ保護規則(GDPR)の適用が開始されました。EU居住者にサービスを提供している企業は、個人情報の取り扱いにますます注意を求められます。仮想通貨を標的にした金銭目的のサイバー攻撃が活発に行なわれています。ランサムウェア被害の件数は減少傾向ですが、身代金獲得を目的として、医療機関や重要システムが狙われています。ソフトウェアの脆弱性対策や、ウイルス対策ソフトの導入と最新化、データのバックアップなどの基本的なマルウェア対策が継続して重要です。

(1)個人情報保護に関する国内外の動向

- 3/17にイギリスの選挙コンサルティング会社 Cambridge Analytica社が、Facebookで得た個人情報を無許諾で自社ビジネスに利用していたことが、新聞紙にリークされました。Facebook社は、 被害にあったユーザ数を最大8,700万人と発表しました。SNSの利用者は、SNSへ掲載した情報やSNSアプリへ提供した情報が漏えいしたり、不正利用されたりするリスクを考慮して、SNSを利用しましょう。
- 6/14にホテル予約事業者 Fastbooking社で不正アクセスによる情報漏えいがありました。委託元の日本国内のホテル業者も被害を受け、GDPR対応事例として注目されました。

(2)サイバー攻撃の動向

- 仮想通貨Verge, Bitcoin Gold, Monacoinへ51%攻撃が行われ、同仮想通貨の取引所が二重支払いによる被害を受けました。従来、51%攻撃の現実的な脅威は低いと言われてきましたが、この被害により取引所での51%攻撃対策の必要性が顕在化しました。
- ルーターの脆弱性や設定不備を悪用して、大規模ボットネットを形成した事案が複数発生しました。ベンダ各社はファームウェアの最新化、デフォルトのパスワードの変更、管理画面をインターネットに公開しない、といった対策を呼びかけました。

エグゼクティブサマリー ～関連イベントのタイムライン～

▲：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。

4Q　4月　5月　6月

(1)個人情報保護に関する国内外の動向

個人情報の取り扱いに関するできごと

- ▲ 3/17 Facebookで得た個人情報をCambridge Analyticaの自社ビジネスに流用していたことがリークされた。
- ▲ 4/4 Facebookの情報流出ユーザ数最大8,700万件に上ると判明した。
- ▲ 5/25 GDPR適用
- ▲ 6/14 ホテル予約サービスのFastBookingで情報漏えい、100ヶ国、4,000以上のホテル事業者に影響した。
- ▲ 6/14 プリンスホテル等、複数の国内ホテル事業者が情報漏えいを公開した。

(2)サイバー攻撃の動向

脆弱性とそれを悪用した攻撃

- ▲ 3/28 CVE-2018-7600 Drupalに遠隔コード実行の脆弱性
- ▲ 4/18 警察庁が当該脆弱性を標的としたアクセスを観測した。
- ▲ 4/25 CVE-2018-7602 Drupalに遠隔コード実行の脆弱性
- ▲ 4/25 脆弱性公開から5時間後にDrupal開発者チームが攻撃を観測した。

仮想通貨を標的にした攻撃

- ▲ 5/17 仮想通貨Monacoinに51%攻撃が行われた。
- ▲ 5/18 Bitcoin Goldに51%攻撃、二重支払いにより攻撃者は18百万ドルを不正入手した。
- ▲ 5/23 仮想通貨Vergeに51%攻撃が行われた。

ランサムウェア

- ▲ 4/6 アトランタ市内のコンピュータがランサムウェアに感染し、水道局のウェブサイトを閉鎖した。
- ▲ 5/1 米マサチューセッツ州のレオミンスター学区のコンピュータが暗号化型ランサムウェアに感染し攻撃者に1万ドル相当のビットコインを支払った。
- ▲ 5/22 アトランタ市の行政機関がランサムウェアSamSamに感染し、システムの一部が停止した。

ルーターを標的にした攻撃

- ▲ 4/4 ロジテックが家庭用ルーターの設定を書き換える攻撃増加を公表した。
- ▲ 5/8 ボットネットMirai亜種による、GPONルーターを対象にした攻撃があった。
- ▲ 5/23 ボットネットVPNFilterがウクライナを中心に50万台以上のルーターに感染した。

(1) 個人情報の取り扱いに関するできごと

(1-1) GDPRの適用と影響

5/25 GDPR(EU一般データ規則)が適用されました。 GDPRとは欧州議会、欧州理事会が策定した個人情報保護の枠組みです。 EU内に拠点を置くデータ管理者や処理者のみでなく、EU居住者に商品やサービスを提供する場合にも適応されるため、大きな影響が予想されます。特に、インターネット上でドメインの所有者やIPアドレスの情報を取得可能なサービス「WHOIS」への影響は、大きな話題になりました。現在は"段階的アクセス"と呼ばれる方法が取られており、警察やブランド権利者、セキュリティ関係者に対してアクセス権限の付与を許可する制度導入の動きがあります。

(1-2) GDPRに便乗したフィッシングメール攻撃

5/22 Avira社がGDPRに便乗したフィッシングメールの注意を呼びかけました(*1-1)。同メールは、GDPR対応にともなう個人情報ポリシーの変更や個人情報の取り扱いの同意を求める通知メールを装っており、Webページ上で個人情報を入力させたり、マルウェアに感染させたりします。AppleやPayPal、Airbnbといった有名企業を装った同様のフィッシングメールが複数報告されているため、ユーザは注意が必要です。安易にリンクをクリックしない、不自然な点がないか確認するなど、GDPRに関係する内容のメールは慎重に取り扱う必要があります。

(1-3)GDPR違反の疑いのある事例

GDPR適用を受け、特にEU居住者にサービスを提供するグローバル企業は、自社内や委託先を含め、情報の取り扱いにますます注意が必要です。

- 5/25 非営利団体noybがGoogleやFacebookなど4社を提訴しました。新しいプライバシーポリシーをユーザに強制しており、GDPRを侵害しているという主旨でした(*1-2)。
- 6/26 プリンスホテルが12万4963件の個人情報漏えいを発表しました。プリンスホテルの委託先であるFastbookingにおいて、英語、韓国語、中国語の予約システム稼働サーバが不正アクセスを受けたことが原因でした(*1-3)。

(1-4)SNSでの個人情報の取り扱い

Facebookの個人情報保護関連のニュースが、世間で大きな話題になりました。

- 3/17 Cambridge Analyticaへ5,000万人分のデータを不正共有したとして話題になりました(*1-4)。
- 4/4 Cambridge Analyticaへの不正データ共有が8,700万人分であったことが明らかになりました(*1-5)。
- 4/10, 4/11 Cambridge Analyticaのデータ不正利用を含むいくつかの件について、Facebookのマーク・ザッカーバーグCEOは米議会に召喚されました。いくつかの問題についてザッカーバーグ氏は「悪用について十分な手を打てていなかった」「私の過ちだ。申し訳ない」と謝罪しました(*1-6)。

SNSやクラウドサービスへ個人情報を預ける際には、利用規約をよく読む、必要以上の情報を預けない、情報共有範囲を正しく設定するなど注意が必要です。さらにSNSの利用者は、SNSへ掲載した情報やSNSアプリへ提供した情報が漏えいしたり、不正利用されたりするリスクを考慮して、SNSを利用しましょう。

(2)ルーターを狙った攻撃

(2-1)企業向けルーターを狙った攻撃

- 4/5 Cisco TalosがCisco Smart Install Clientの脆弱性CVE-2018-0171を悪用する攻撃について、警戒を呼びかけました(*2-1)。全世界で168,000台、日本国内で10,000台以上の機器が脆弱な状態でした(*2-2)。2017年11月からCisco Smart Install Clientを探索する通信(図1参照)が増加し、3月に脆弱性 CVE-2018-0171が公表された直後は、さらに同通信が増加しました。攻撃者は、Shodanなどの検索ツールを使って容易に脆弱性のある機器を発見できたため、攻撃が急増しました。

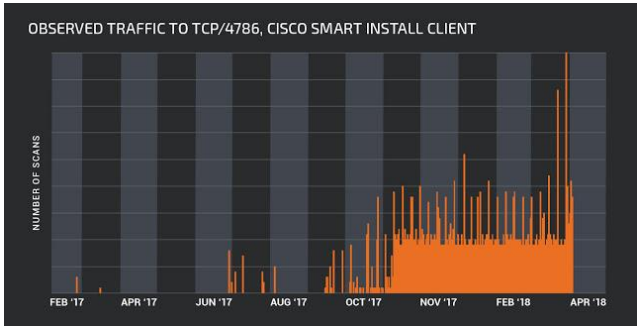


図1: Cisco Smart Install Clientのポート宛の通信
(Cisco「Critical Infrastructure at Risk: Advanced Actors Target Smart Install Client (*2-1)」より引用)

- 4/16 米国の国土安全保障省(DHS)、連保捜査局(FBI)、英国の国家サイバーセキュリティセンター(NCSC)が共同でロシア政府のサイバー活動に関する警告を発表しました(*2-3)。政府及び民間部門のネットワーク機器を標的に、Cisco Smart Install Clientの脆弱性を悪用するサイバー攻撃が行なわれていたとする内容でした。

I. 2018年度 第1四半期のトピック(4/11)
(2)ルーターを狙った攻撃

(2-2)消費者向けルーターを狙った攻撃

- マルウェアVPNFilterが世界で50万台以上の消費者向けルーターへ感染しました(*2-4)。VPNFilterは、消費者向けルーターに3段階の攻撃を仕掛けます。国内では、ロジテックやバッファローといったパソコン周辺機器メーカーの消費者向けルーターが被害を受けました(*2-5)。
- マルウェアRoaming Mantisがアジア地域を中心に感染が拡大しました。Roaming Mantisは、ルーターのDNS設定を改ざんして、Android端末がルーター経由でインターネットへアクセスすると、マルウェアをインストールさせたり、フィッシングサイトを表示したりして個人情報やクレジットカード情報を詐取します(*2-6)。

(2-3)同攻撃の対策

- 各メーカーは、ルーターが侵害されたおそれのある場合、すぐに窓口に問い合わせるよう、呼びかけました。ルーターを狙った攻撃への一般的な対策には、機器のファームウェアを最新版に更新すること、管理画面のパスワードをデフォルトから変更して複雑なパスワードを設定すること、管理画面をインターネットに公開しないことなどがあります。
- VPNFilterに感染してしまった場合、ルーターを再起動すれば第2、第3段階の攻撃で感染したマルウェアを削除できます。第1段階で感染したマルウェアは、ルーター内の不揮発性メモリ上にインストールされるため、マルウェアを削除するには工場出荷状態へのリセットが必要です。
- 3/6 総務省は国会にNICT法の改正案を提出しました(*2-7)。総務省配下のNICTが国内の脆弱なIoT機器を調査して特定し、利用者に注意喚起できるようにするための措置です。

消費者個人で行える対策には限界があります。セキュリティベンダやネットワーク機器メーカーによる自動アップデートや、政府が策定した基準に則ったメーカーの対策強化が期待されます。

(3)仮想通貨を狙った攻撃

攻撃手法の分類

表1は、仮想通貨を狙った攻撃手法を仮想通貨の取引や標的で分類したものです。過去のレポートでは、通貨を狙った攻撃と対比して整理するために、この分類を使用しました。本レポートでは、標的別に攻撃を整理しました。

表1：仮想通貨を狙った攻撃手法の分類

仮想通貨の取引	標的	攻撃の説明、例
仮想通貨取引の当事者	仮想通貨サービス提供者・・・(3-1)	仮想通貨取引所のウォレットを狙った攻撃など。
	仮想通貨サービス利用者	仮想通貨取引所へログインする認証情報を窃取する攻撃など。
仮想通貨取引の有無によらない	パソコン保有者・・・(3-2)	仮想通貨マイナーへ感染させる。ドライブバイマイニング。など

(3-1)仮想通貨サービス提供者を狙った攻撃

- 5/22 取引アプリTaylorがハッキング被害に遭い、150万ドル相当の仮想通貨が盗難されました(*3-1)。
- 5/23 仮想通貨Vergeが51%攻撃を受け、100万ドル相当の被害を受けました(*3-2)。
- 6/10 韓国の仮想通貨取引所Coinrailが、4,000万ドル相当のICOトークンを盗難されました(*3-3)。
- 6/20 韓国の仮想通貨取引所Bithumbが、3,100万ドル相当の仮想通貨を盗難されました(*3-4)。

51%攻撃とは、仮想通貨取引に必要な計算力の過半数を独占して不正行為を行う攻撃です。仮想通貨取引所の51%攻撃への対策は、取引承認で確認する承認数を増やすことです。特定の攻撃者が必要な計算力の過半数を占めた場合にも、ブロックチェーン不正操作の影響を受けにくくします。上記のすべての攻撃に対する利用者の対策は、取引所のウォレットから、自己の管理するウォレットに、都度、資金を移動させることです。

(3-2)パソコン保有者を狙った攻撃

- 6/16 中国のセキュリティ企業 Qihoo 360がマルウェアWinstarNssmMinerの流行を報告しました。このマルウェアは、クリプトジャッキング(*)という方法で3日間で約50万台のコンピュータに感染し、仮想通貨Monero 28,000ドル相当を不正に採掘しました(*3-5)。対策は、クリプトジャッキングに対応したWebブラウザ、または同様の機能を持つブラウザの拡張機能を用いることです。
(*)クリプトジャッキング: 悪意ある第三者がWebサイトに悪意のあるコードを埋めこみ、無断でサイト訪問者のパソコン上でそのコードを実行させて、仮想通貨を不正に採掘すること。
- Androidデバイスに感染して仮想通貨Moneroを採掘するマルウェアADB.Minerが、Amazon Fire TV、Fire TV Stickにも感染を拡大しました(*3-6)。Fire TV等のデバイスがマルウェアに感染した場合、映像の再生がすぐに停止する・映像を再生できない、といった症状が現われる場合があります。マルウェアに感染した場合、工場集荷時の状態にリセットしてマルウェアを削除します。

これらの仮想通貨に関する攻撃はランサムウェアよりも確実に収益を得られるため、攻撃者は、パソコン保有者を狙った、仮想通貨を不正に獲得する攻撃に注力しています。仮想通貨取引所や仮想通貨利用者でない一般利用者も、パソコンのCPUリソースを悪用して仮想通貨を採掘するマルウェアへの感染に留意する必要があります。

(4)ランサムウェアSatanが感染拡大機能を持つようになった

2018年4月中旬に、攻撃ツールEternalBlueによる攻撃が多数観測されました。この攻撃は、ランサムウェアSatan(別名DBGer)がEternalBlueを用いて攻撃したと推測されます(*4-1)。Satanは、ランサムウェアの作成、身代金の集金、身代金を支払った被害者への復号ツールの提供等をクラウドサービスとして提供しています。このようなサービスは、RaaS(Ransomware as a Service)と呼ばれています。

Satanには、以下の感染拡大機能が追加されています。

- 2017/1　Satanが発見されました(*4-2)。
- 2017/11　感染拡大にEternalBlueを使うようになりました(*4-3)。
- 2018/5　感染拡大にJBoSSやWeblogicの脆弱性を使うようになりました(*4-4)。
- 2018/6　DBGerと名称を変更し、感染拡大にMimikatzを使うようになりました(*4-5)。

良く知られたRaaSの1つであるCerberとSatanを比較すると、以下のような点が異なります。

- 支払われた身代金のうち、クラウドサービス提供者の取り分は、Satanが3割(*4-2)、Cerberが4割です(*4-6)。
- Satanには、感染拡大機能が追加されています。
  Cerberには、検知回避や仮想通貨の窃取機能が追加されています(*4-7)。

(5)サプライチェーンを侵害する攻撃

(5-1)ソフトウェア開発元を狙った攻撃

- サーバ用のJavaScript環境 Node.jsを管理している「Node Packaged Modules (npm)」に登録されているgetcookiesパッケージにバックドアが仕込まれていることがわかりました(*5-1)。
- Pythonモジュール「SSH Decorator」にSSHの認証情報を窃取するバックドアが仕込まれていることがわかりました。開発者はバックドアを仕込まれたモジュールが配布サイトへ不正にアップロードされたと報告しています(*5-2)。
- Gentoo LinuxのGitHubアカウントが侵害され、ファイルを削除するマルウェアが設置されました(*5-3)。

ソフトウェアの配布サイトの開発者のアカウントが侵害される事例が複数報告されています。ソフトウェアの配布サイトへの多要素認証の導入等の対策が必要です。

(5-2)画像ファイルへの悪意のあるコードの挿入

サンドボックスゲームMinecraftで、アバターの見た目を変更するスキン(PNGファイル)へ悪意のあるパワーシェルスクリプトが仕込まれました。
Minecraft: Java版のユーザであれば、 Minecraftのサイトにカスタマイズしたスキンをアップロード可能であることを悪用されました(*5-4)。
今回の案件に関しては、スキンをダウンロードしただけではコードは実行されないと報告されています(*5-5)。

図2: 悪意あるスクリプトを仕込まれたスキン
(Avast「Minecraft players exposed to malicious code in modified “skins” (*5-4)」より引用)

I. 2018年度 第1四半期のトピック(9/11)
(6)パスワードの定期変更を不要とする方針

(6-1)パスワードの定期変更の不要論

パスワードの定期変更を強制すると、単純なパスワードを使用したり、パスワードを使い回したりして、かえってリスクが高まることが、国内外の研究で明らかになりました。今後、パスワードの定期変更に代わって多要素認証やリスクベース認証の導入がより加速すると見られています。

- 2017/12 NIST SP800-63B(電子的認証に関するガイドライン)で、サービス提供者側がパスワードの定期変更を要求すべきでないと表明しました。(*6-1)
- 2017/12 NISC 情報セキュリティハンドブックで、パスワードの定期変更は不要としました。(*6-2)
- 2018/3 総務省が国民のための情報セキュリティサイトへ「パスワードの定期変更は不要」と記載しました。
- 2018/4 プライバシーマーク発行機関の日本情報経済社会推進協会は、認定時の審査基準を改定し、インターネット利用時のパスワードの定期変更を不要としました。(*6-3)
- 2018/4 Yahooがパスワードの定期変更を促す文言を削除する方針と発表しました。(*6-4)

利用するサービスによっては、パスワードを定期的に変更することを求められることもありますが、実際にパスワードを破られアカウントが乗っ取られたり、サービス側から流出した事実がなければ、パスワードを変更する必要はありません。

総務省「安心してインターネットを使うために 国民のための情報セキュリティサイト」より抜粋
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/01.html

(7)国際的なイベントと連動したサイバー攻撃

(7-1) 2018 FIFAワールドカップ ロシア

- 6/4 ブラジルのユーザを標的に、公式ジャージの当選を装ったメッセージがWhatsAppで出回りました(*7-1)。
- 6/6 ワールドカップ関連くじの当選を装う詐欺メールが見つかりました(*7-2)。
- 6/14 アメリカの情報機関関係者が、「ロシア旅行者のモバイル機器が、ロシア政府により不正アクセスを受けるおそれがある」と述べました(*7-3)。
- 7/6 イスラエルの国防軍が、同国兵士を標的にしたAndroidスパイウェアをインストールさせる攻撃があったと発表しました。スパイウェアはワールドカップの結果速報アプリを装っていました(*7-4)。

図3: ワールドカップ関連くじの当選を装う詐欺メール
(ESET「You have NOT won! A look at fake FIFA World Cup-themed lotteries and giveaways (*7-2)」より引用)

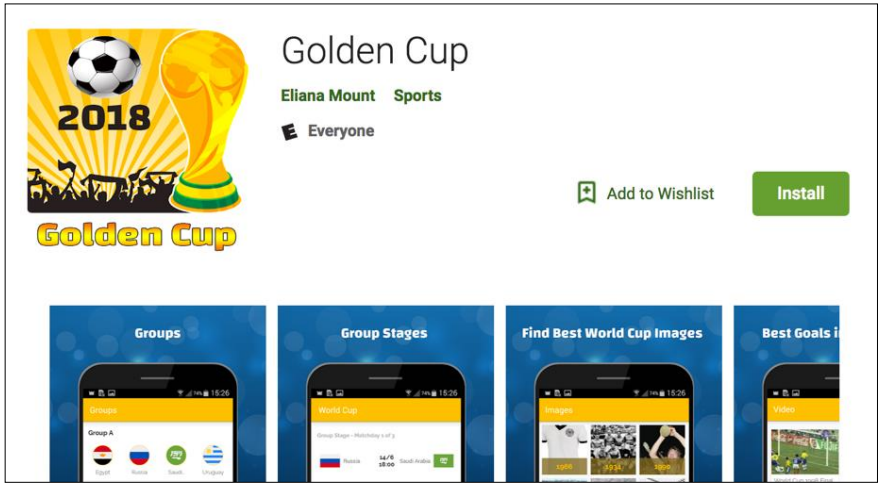


図4: 結果速報アプリを装うマルウェア
(Symantec「GoldenCup: New Cyber Threat Targeting World Cup Fans (*7-4)」より引用)

(7-2)シンガポール米朝首脳会談

- 5/31 Cisco Talosが、6/12に開催されるシンガポール米朝首脳会談の関連文書を装う文書をおとりとしたマルウェアを発見しました。この文書は、韓国でシェアトップのワープロソフト「アレアハングル」の形式で作成されており、遠隔操作ツールNavRATをインストールさせるものでした。マルウェアは、韓国最大手のインターネット検索ポータルサイト NAVERのメールプラットフォームを介して、C&Cサーバと通信していました(*7-5)。

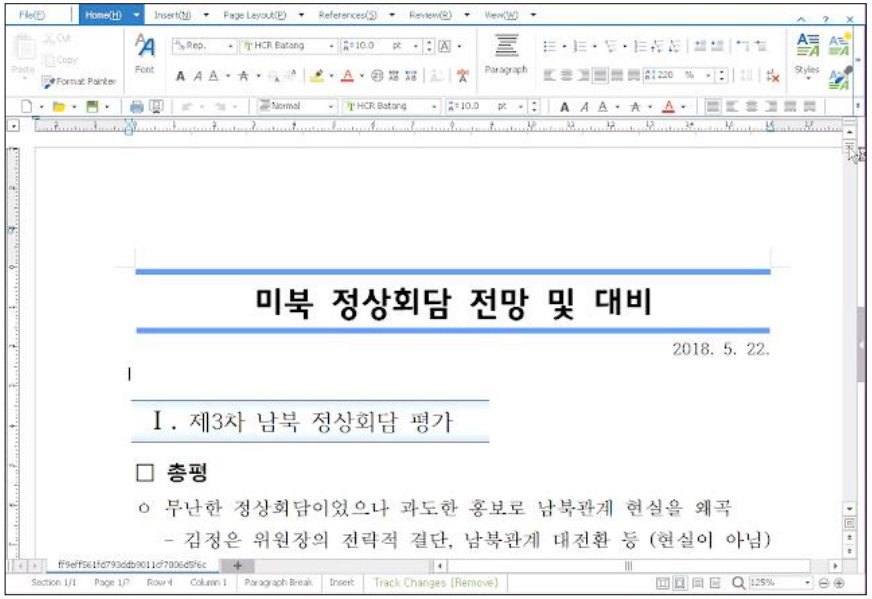


図5: 会談関連文書を装ったハングル語の文書
(Cisco「NavRAT Uses US-North Korea Summit As Decoy For Attacks In South Korea (*7-5)」より引用)

- 6/4 FireEyeが、北朝鮮のサイバー攻撃集団APT37と中国の集団が攻撃情報を交換しているとの分析結果を発表しました。APT37は韓国へのスパイ活動を継続しており、韓国政府の外交情報の不正入手を狙っています。(*7-6)。

II. 2018年度 第2四半期以降の予測(1/2)

(1)GDPRに関連したサイバー攻撃の流行

- GDPRに違反した企業は、最大で年間売上の4%、または2,000万ユーロの制裁金を課されます。
  そこでサイバー犯罪者が、この規則を悪用して企業を脅迫するおそれがあります。たとえば、以下のようなシナリオが想定されます。
  1. サイバー犯罪者が、EU居住者の個人情報を扱う企業から個人情報を盗み取ります。
  2. 犯罪者は盗みとった情報の一部を企業へ提示し、金銭を支払わなければ情報を流出させると企業を脅迫します。
  3. 企業から監督機関への通知が遅れた場合には、制裁金をたてに、さらに高額の金銭を要求します。

- GPDPRへの対応を求めて不安をあおるフィッシング詐欺や、GDPRを題材にしたビジネスメール詐欺が流行するおそれがあります。情報漏えいの事実を72時間以内に監督機関へ通知するという規則を巧みに使って、金銭の支払いを急がせるおそれがあります。

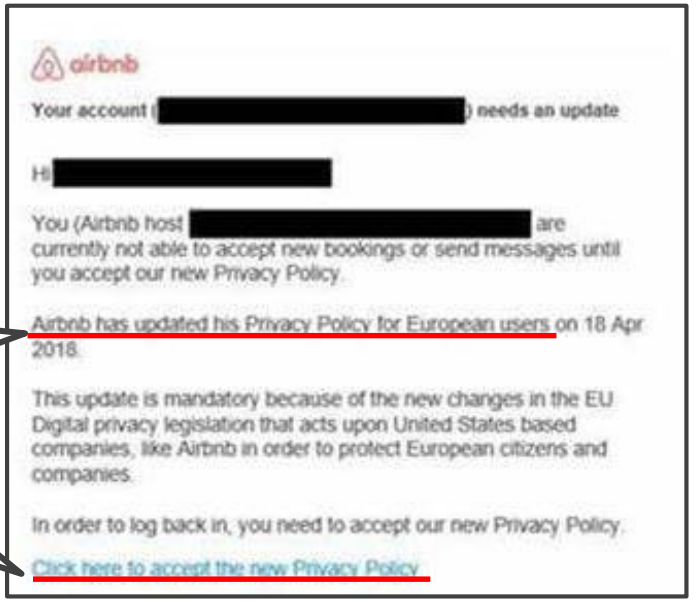


図6: Airbnbになりすまし、プライバシーポリシーへの同意を求めるフィッシングメール
(Redscan「REDSCAN IN THE NEWS: RAISING AWARENESS OF GDPR PHISHING SCAMS (*8-1)」より引用)

II. 2018年度 第2四半期以降の予測(2/2)

(2)仮想通貨の発掘ソフトウェアの新たな不正実行先

ランサムウェアよりも確実に収益を得られる手段として、サイバー犯罪者は、より一層、仮想通貨の不正獲得を狙います。しかしその一方で、仮想通貨を不正に発掘するためのソフトウェア「マイナー」は、ウイルス対策ソフトによる検知や公式アプリストアからの締め出しが進んでいます。個人のパソコンやスマートフォンでマイニングをさせることは難しくなりつつあります。

一方で、企業のクラウド利用が加速している反面、セキュリティ対策は後手になりがちです。攻撃者は、Kubernetes等の構築と運用の自動化が進んだクラウド環境の脆弱性や設定不備などを悪用して不正にログインし、仮想通貨の発掘ソフトウェアがインストールして、大規模な不正採掘が行われる事件が増加すると予想しています。

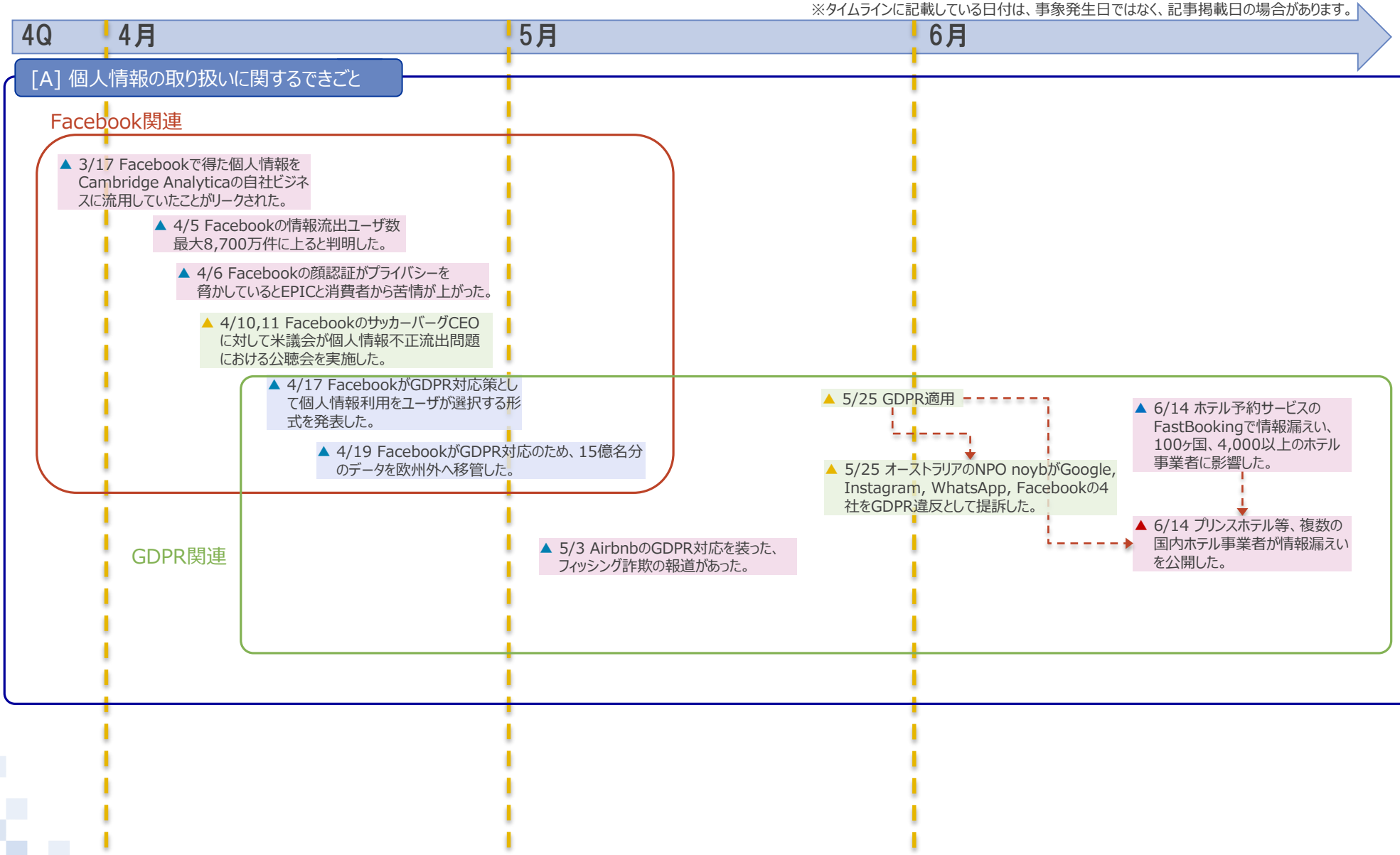
(3)FY2018 第2～3四半期の政治イベントに関連したサイバー攻撃

- アメリカ-中国間の貿易摩擦に関連し、両国間でサイバー攻撃が過熱するおそれがあります。
- 11/6 アメリカ中間選挙に関連し、選挙システムへのサイバー攻撃の脅威が高まります。また、2016年の大統領選挙と同様に選挙操作を狙ったフェイクニュースが出回るおそれがあります。

III. 2018年度第1四半期のタイムライン(1/10)

▲：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

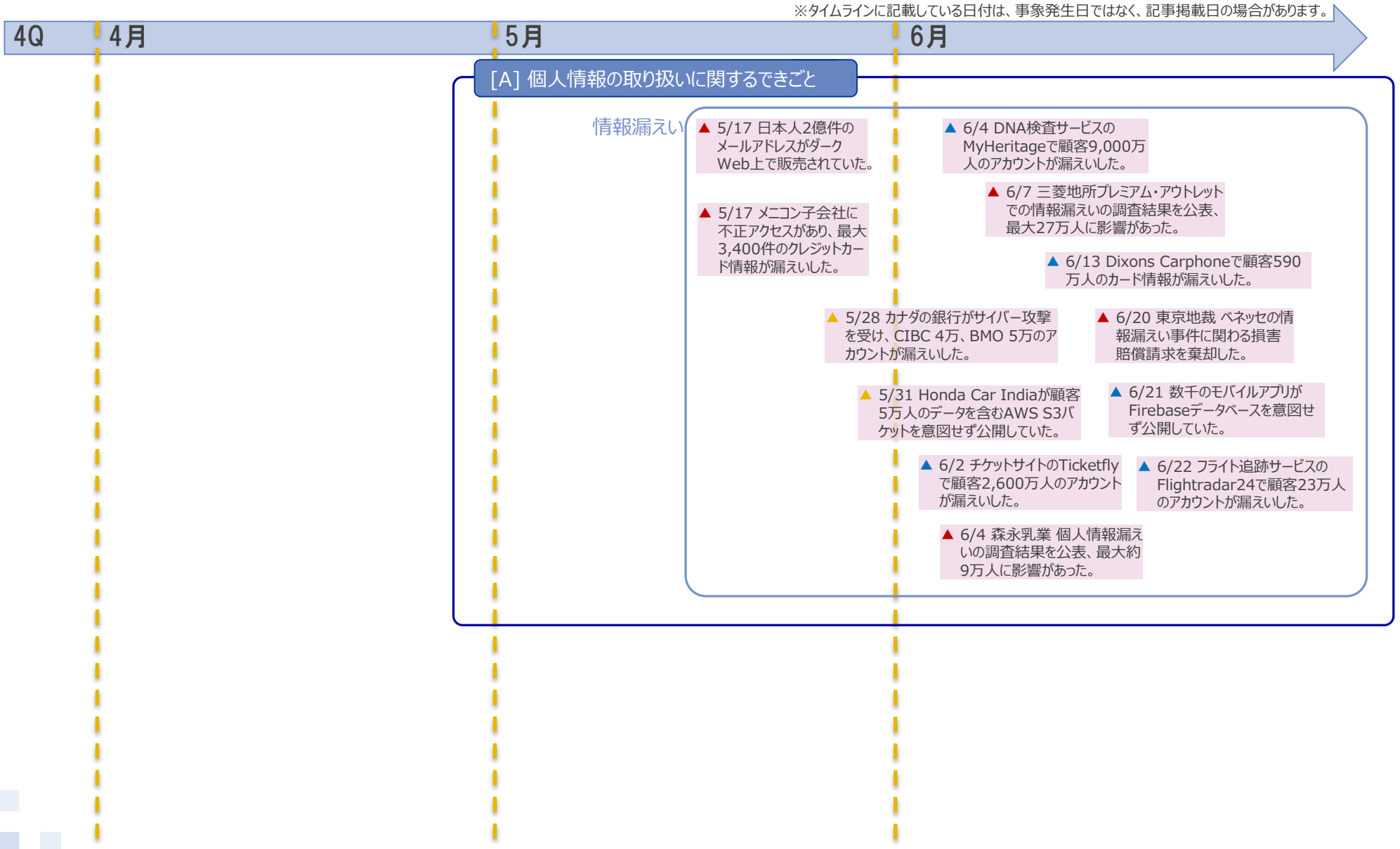
※タイムラインに記載している日付は、事象発生日ではなく、記事掲載日の場合があります。



III. 2018年度第1四半期のタイムライン(2/10)

▲：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。



III. 2018年度第1四半期のタイムライン(3/10)

▲：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。

4Q　4月　5月　6月

[B] ルーターを標的にした攻撃

- ▲ 4/4 ロジテックが家庭用ルーターの設定を書き換える攻撃増加を公表した。
- ▲ 4/7 イランが米国旗を表示するサイバー攻撃を受けたと発表した。
- ▲ 4/12 Akamaiがルーター65,000台以上に対する不正アクセスを発見した。
- ▲ 4/16 ブラジルでルーターおよびネットワークインフラを狙う攻撃が発生した。
- ▲ 4/16 米国DHSおよびFBI、英国NCSCが共同でルーターを狙う攻撃について警告を発表した。
- ▲ 3/28 CVE-2018-0171 Cisco Smart Install Clientの遠隔コード実行の脆弱性が公開された。
- ▲ 4/5 Cisco TalosがCisco Smart Install Clientを悪用する攻撃について注意喚起した。
- ▲ 4/6 JPCERTが脆弱性を標的にしたスキャン活動の急増を報告した。
- ▲ 5/10 Qihoo360 NetlabがIoTボットネットがDASAN Networks Solutions 社のGPONルーターに感染しようとしていると発表した。
- ▲ 5/15 UPnPの脆弱性を悪用するDDoS攻撃が報告された。
- ▲ 5/3 GPONルーターの脆弱性公開 CVE-2018-10561 認証バイパ CVE-2018-10562 コマンドインジェクション
- ▲ 5/8 ボットネットMirai亜種による、GPONルーターを対象にした攻撃があった。
- ▲ 5/21 ボットネットTheMoonによる、GPONルーターを対象にした攻撃があった。
- ▲ 5/23 ボットネットVPNFilterがウクライナを中心に50万台以上のルーターに感染した。
- ▲ 5/24 FBIがボットネットの通信先ドメインをテイクダウンした。
- ▲ 5/18 DreyTek製ルーターにDNS設定を書き換えるゼロデイ攻撃があった。

[C] 重要インフラを標的にした攻撃

- ▲ 4/2 Energy Transfer Partners社が利用するEDIプラットフォームがサイバー攻撃により機能を停止した。
- ▲ 4/4 米国の4つのパイプライン事業者が電子システムへの攻撃を受けていたと判明した。
- ▲ 4/10 カリブ海のシント・マールテン政府がサイバー攻撃を受けインフラストラクチャが一週間停止した。
- ▲ 5/11 サイバー犯罪者集団Allaniteがアメリカやイギリスの産業制御システムを標的に活動を活発化させている。
- ▲ 6/28 米下院が産業制御システムへの脅威にそなえ、「DHS産業制御システム能力強化法案」を可決した。

III. 2018年度第1四半期のタイムライン(4/10)

▲：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。

4Q　4月　5月　6月

[D] 仮想通貨

▲ 2017/3/26 CVE-2017-7269 IIS 6.0にバッファオーバーフローによる遠隔コード実行の脆弱性が公開された。

▲ 4/12 仮想通貨Electroneumを採掘させる攻撃があった。

▲ 4/2 マルウェアnjRATがランサムウェアと仮想通貨窃取機能を追加実装した。

▲ 4/9 仮想通貨 Verge でソフトウェアの不具合を悪用した不正マイニングが発生した。

▲ 4/13 インドの大手仮想通貨取引所Coinsecureが約3Mドル相当の盗難被害を受けた。

▲ 4/17 ランサムウェアXIAOBAが仮想通貨採掘の機能も備えた。

▲ 4/23 トレンドマイクロが仮想通貨Moneroを採掘するワームRETADUPの新種を発見した。

▲ 5/11ボットネットSatoriによるEthereumマイニングソフトを標的にした大規模なスキャン活動があった。

▲ 5/17 マルウェアWinstarNssmMinerが3日間で50万台以上に感染、仮想通貨を採掘した。

▲ 5/17 仮想通貨Monacoinに51%攻撃が行われた。

▲ 5/18 Bitcoin Goldに51%攻撃、二重支払いにより攻撃者は18百万ドルを不正入手した。

▲ 5/23 仮想通貨Vergeに再度51%攻撃が行われた。

▲ 5/28 ブロックチェーンEOSに遠隔コード実行の脆弱性が発見された。

▲ 5/28 仮想通貨取引アプリTaylorが仮想通貨150万ドル窃取の被害を受けた。

▲ 6/10 韓国の取引所Coinrailが侵害され、4,000万ドル相当のICOトークン盗難の被害を受けた。

▲ 6/11 Ethereum採掘ノードを標的とした攻撃で、サイバー犯罪者に2,000万ドル以上の収益があった。

▲ 6/12 仮想通貨Moneroの流通量のうち5%がマルウェアによる採掘だった。

▲ 6/15 クリップボードを不正に操作し仮想通貨を盗みとるマルウェアが300万台以上のマシンに感染した。

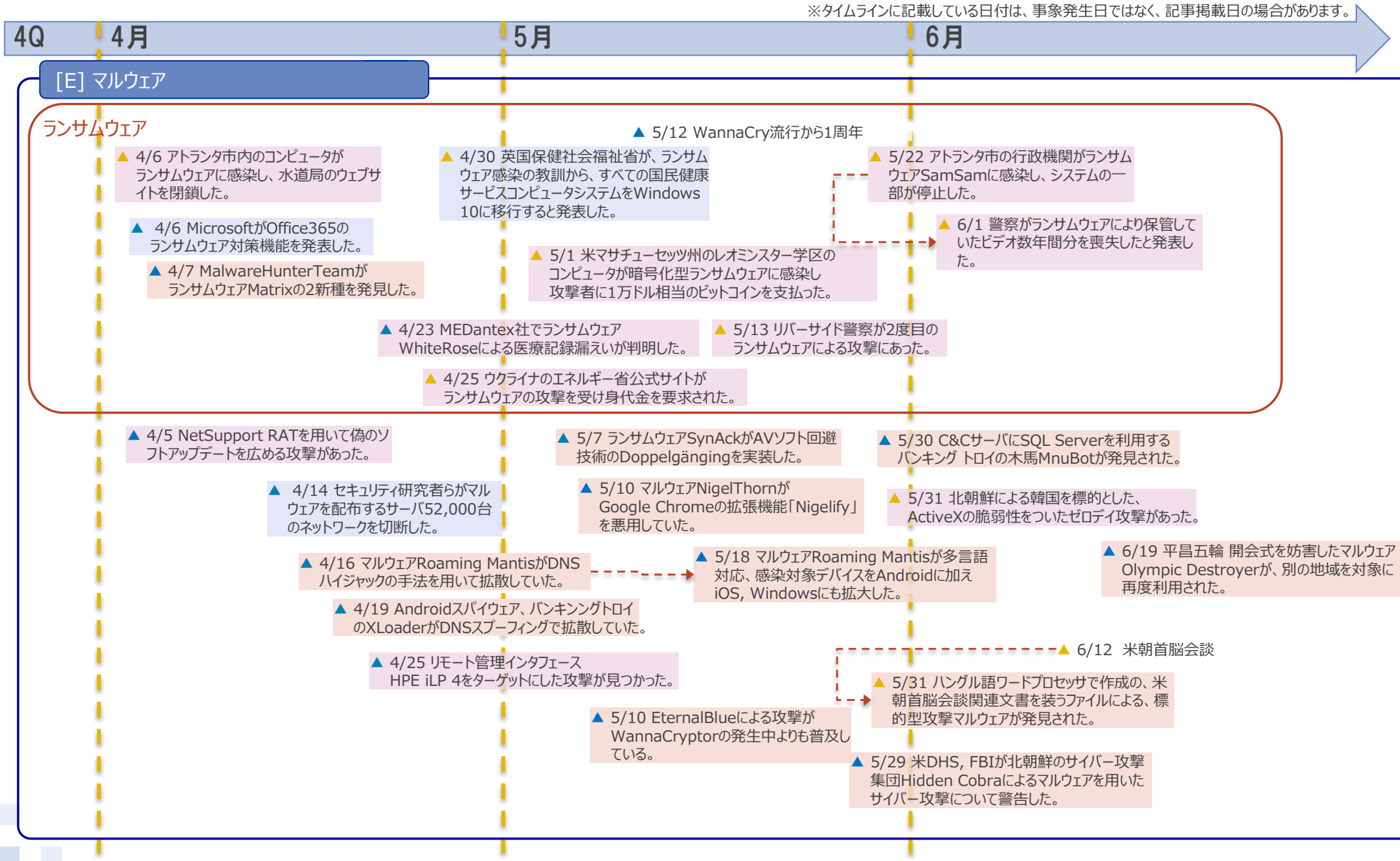
▲ 6/18 Amazon Fire TV, Fire TV Stickを標的にした、仮想通貨をマイニングするマルウェアが発見された。

▲ 6/24 韓国の取引所Bithumbが侵害され、31Mドル相当の仮想通貨盗難の被害を受けた。

III. 2018年度第1四半期のタイムライン(5/10)

▲：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

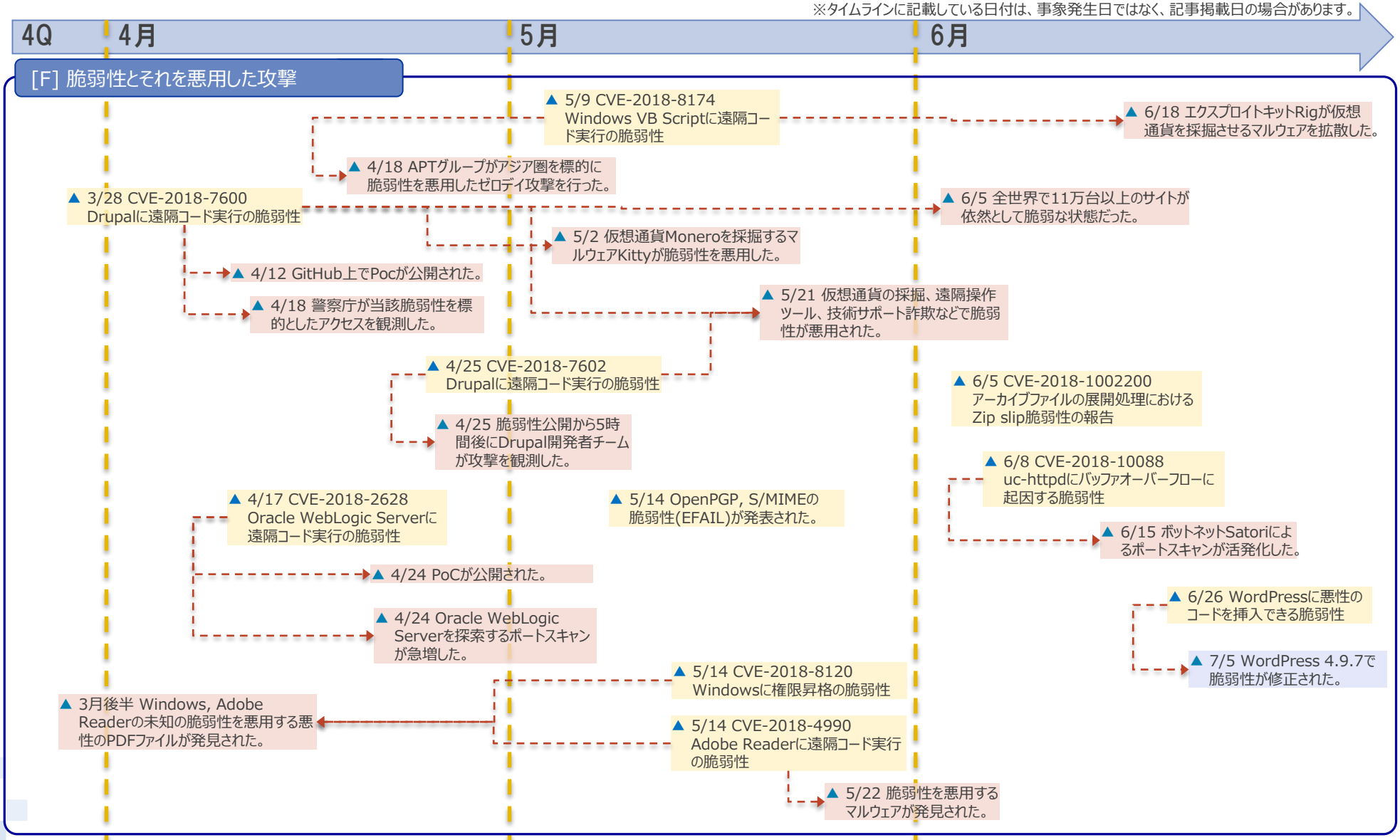
※タイムラインに記載している日付は、事象発生日ではなく、記事掲載日の場合があります。



III. 2018年度第1四半期のタイムライン(6/10)

▲：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。

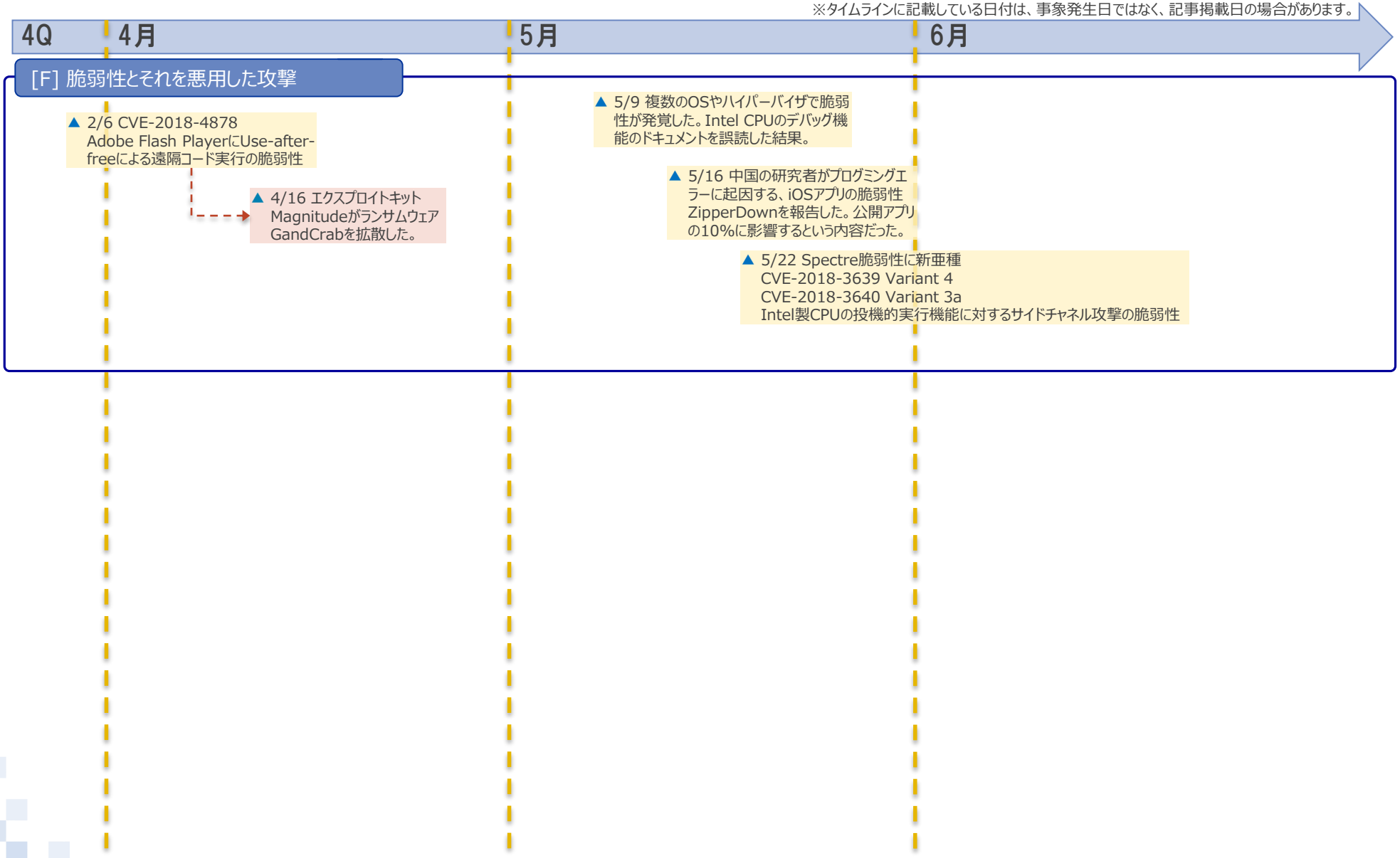


NTT DATA

III. 2018年度第1四半期のタイムライン(7/10)

▲：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。



III. 2018年度第1四半期のタイムライン(8/10)

▲：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。

4Q | 4月 | 5月 | 6月

[G] サプライチェーン攻撃

- ▲ 5/3 JavaScriptライブラリ"getcookies"にバックドアが発見された。
- ▲ 5/4 中国のサイバースパイ集団がソフトウェア会社を侵害し、コード署名証明書を収集していた。
- ▲ 5/9 Pythonモジュール"ssh-decorate"にバックドアが発見された。
- ▲ 5/25 格安スマホ 141機種のファームウェアにマルウェアが発見された。
- ▲ 6/28 Gentoo LinuxのGitHubレポジトリが侵害され、OSイメージにファイルを削除するコードが仕込まれた。

[H] DDoS攻撃

- ▲ 4/20 警察庁がmemcachedに対するスキャン活動の増加を報告した。
- ▲ 4/24 米国、英国、およびオランダの警察当局がWebstresserをシャットダウンした。またIT管理者らが逮捕された。
- ▲ 5/2「Webstresser.org」の閉鎖以降、欧州でのDDoS攻撃が約60%減少した。
- ▲ 5/14 UPnPを悪用するDDoS攻撃が観測された。

[I] 機械学習の応用

- ▲ 6/4 TrendMicroが機械学習によりWebのトップページを改ざんする攻撃を検出する手法を発表した。
- ▲ 6/11 TrendMicroが機械学習により署名付きマルウェアを検知する手法を発表した。
- ▲ 6/17 機械学習によりパスワード推測の効率を18-24%向上する手法が発表された。

III. 2018年度第1四半期のタイムライン(9/10)

▲：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。

4Q　4月　5月　6月

[J] 政府や公共機関による取り組み

- ▲ 4/2 NISTが「連邦政府の情報システムにおけるIoTのセキュリティおよびプライバシーのリスクを管理するための留意事項」の原案を公開した。
- ▲ 4/2 経団連が東京五輪でのサイバー攻撃を懸念して対策の強化を発表した。
- ▲ 4/2 警視庁はサイバー攻撃やネット犯罪対応部署を1か所に集約した。
- ▲ 4/4 政府が「サイバーセキュリティ戦略」の骨子を取りまとめた。
- ▲ 4/19 国土交通省は国内の約60の関連企業・団体でつくる「交通ISAC」（仮称）設立の支援を決定した。
- ▲ 4/25 IPAは「非機能要求グレード改訂ワーキング・グループ」における成果をまとめ「非機能要求グレード2018」を公開した。
- ▲ 4/27 ASEANがサイバー防衛分野で協力を強化することに合意した。
- ▲ 5/4 NISTが「Platform Firmware Resiliency Guidelines」を発行した。
- ▲ 5/6 政府はエストニアへ防衛省職員を派遣しサイバー分野での協力関係強化を行うと決定した。
- ▲ 5/29 EUユーロポールが法執行機関をからメンバを集めダークWeb調査のチームを設立した。
- ▲ 5/30 IPAが「ウェブサイト開設等における運営形態の選定方法に関する手引き」を公開した。
- ▲ 6/7 政府が2021年までのサイバーセキュリティ戦略案をまとめ。量子コンピュータやAI、サイバー攻撃に強い暗号技術の開発支援を決定した。
- ▲ 6/15 経済産業省とIPAがサイバーセキュリティ対策の情報交換に「コラボレーション・プラットフォーム」を設置した。
- ▲ 6/15 IPAが「ウェブサイト開設等における運営形態の選定方法に関する手引き」を公開した。

[K] 金融機関への攻撃

- ▲ 4/30 メキシコの銀行がサイバー攻撃を受け、3億ペソ以上の盗難被害を受けた。
- ▲ 5/24 チリの銀行がワイパーKillDiskによる攻撃を受け、システムが停止した。

III. 2018年度第1四半期のタイムライン(10/10)

▲：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。

4Q　4月　5月　6月

[L] パスワードの定期変更を不要とする動き

- ▲ 2017年 12月 NIST SP800-63B
- ▲ 2017年 12月 NISC 情報セキュリティハンドブック
- ▲ 3月 総務省
- ▲ 4月 Pマーク発行機関の日本情報経済社会推進協会
- ▲ 5/3 Twitterが3億3,000万人のユーザにパスワードを変更するよう促した。パスワードがログに平文で記録されていたため。
- ▲ 5/4 Googleが新たなトップレベルドメイン .appを公開した。HTTPS通信のみ許可する。
- ▲ 6/11 アメリカでネット中立性規則が失効した。

[M] Office 365の認証情報の詐取を狙ったフィッシング攻撃

- ▲ 4/27 人事部門からの連絡を装い、O365の認証情報の詐取を狙ったメールが流通した。
- ▲ 6/11 フィンランド 政府組織がフィッシングの注意喚起をした。
- ▲ 6/27 文部科学省が国内6大学にフィッシングへの注意喚起をした。
- ▲ 6/27 弘前大学がフィッシングの被害を受けたことを公表した。

[N] 国際的なイベントと連動したサイバー攻撃

- ▲ 4/23 NTTグループが「海賊版サイト」に対して、ブロッキングを実施すると発表した。
- ▲ 4/26 NTTが量子コンピューターでも解けない 新暗号技術を開発した。
- ▲ 4/27 北朝鮮のハッキンググループが事業を拡大し17カ国で広い事業分野をターゲットに活動していると判明した。
- ▲ 6/14 ロシアでサッカー ワールドカップが開幕した。
- ▲ 6/4 WhatsApp上で偽メッセージ、ワールドカップ公式シャツの当選をうたうものだった。
- ▲ 6/6 ワールドカップ関連くじを装う詐欺メールが発見された。
- ▲ 7/6 ワールドカップの結果速報アプリを装うスパイウェアが発見された。
- ▲ 6/12 米朝首脳会談
- ▲ 5/31 ハングル語ワードプロセッサで作成の、米朝首脳会談関連文書を装うファイルによる、標的型攻撃マルウェアが発見された。

引用一覧(1/3)

(*1-1) Help! GDPR or Phishing Mail? | Avira https://blog.avira.com/help-gdpr-or-phishing-mail/
(*1-2) GoogleとFacebook、GDPR施行初日にさっそく提訴される | ITmedia http://www.itmedia.co.jp/news/articles/1805/27/news011.html
(*1-3) プリンスホテルの委託先サイトに不正アクセス、12.5万件の情報漏えい | ZDNet https://japan.zdnet.com/article/35121487/
(*1-4) Trump campaign-linked data firm Cambridge Analytica reportedly collected info on 50M Facebook profiles | TechCrunch https://techcrunch.com/2018/03/17/trump-campaign-linked-data-firm-cambridge-analytica-reportedly-collected-info-on-50m-facebook-profiles/
(*1-5) An Update on Our Plans to Restrict Data Access on Facebook | Facebook https://newsroom.fb.com/news/2018/04/restricting-data-access/
(*1-6) フェイスブックＣＥＯ「私の過ち」 米議会で謝罪 | 日経 https://www.nikkei.com/article/DGXMZO29242870R10C18A4000000/

(*2-1) Critical Infrastructure at Risk: Advanced Actors Target Smart Install Client | Cisco https://blog.talosintelligence.com/2018/04/critical-infrastructure-at-risk.html
(*2-2) Cisco Smart Install プロトコルを狙った攻撃の急増 | NICTER http://blog.nicter.jp/reports/2018-03/cisco-switch-hack/
(*2-3) Advisory: Russian state-sponsored cyber actors targeting network infrastructure devices | NCSC https://www.ncsc.gov.uk/alerts/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices
(*2-4) ネットワーク機器を狙う IoT ボット「VPNFilter」、世界で 50 万台以上に感染 | TrendMicro https://blog.trendmicro.co.jp/archives/17484
(*2-5) ルーターへのサイバー攻撃相次ぐ 個人情報盗む目的か | 日経 https://www.nikkei.com/article/DGXMZO29079420W8A400C1CR0000/
(*2-6) DNS設定を乗っ取りAndroidデバイスに感染するRoaming Mantis | Kaspersky https://blog.kaspersky.co.jp/roaming-mantis/20105/
(*2-7) IoTサイバー攻撃情報を事業者間で共有、総務省が国会に改正法案を提出 | TrendMicro https://www.trendmicro.com/jp/iot-security/news/20157

引用一覧(2/3)

(*3-1) Cryptocurrency trading app Taylor says all funds have been stolen in cyberattack | ZDNet https://www.zdnet.com/article/all-of-cryptocurrency-trading-app-taylors-funds-have-been-stolen/

(*3-2) Hacker mines up to $1 million in Verge after exploiting major bug | Sophos https://nakedsecurity.sophos.com/2018/04/09/hacker-mines-up-to-1-million-in-verge-after-exploiting-major-bug/

(*3-3) South Korean Cryptocurrency Exchange Coinrail hacked, hackers stole over $40M worth of ICO tokens | Security Affairs https://securityaffairs.co/wordpress/73426/cyber-crime/cryptocurrency-exchange-coinrail-hacked.html

(*3-4) Bithumb $31 Million Crypto Exchange Hack: What We Know (And Don't) | CoinDesk https://www.coindesk.com/bithumb-exchanges-31-million-hack-know-dont-know/

(*3-5) WinstarNssmMiner Coinminer Campaign Makes 500,000 Victims in Three Days | Bleeping Computer https://www.bleepingcomputer.com/news/security/winstarnssmminer-coinminer-campaign-makes-500-000-victims-in-three-days/

(*3-6) Amazon Fire TV and the ADB.Miner malware ? what you need to know | CordCutters https://www.cordcutters.com/amazon-fire-tv-and-adbminer-malware-what-you-need-know

(*4-1) One year later: EternalBlue exploit more popular now than during WannaCryptor outbreak | ESET https://www.welivesecurity.com/2018/05/10/one-year-later-eternalblue-exploit-wannacryptor/

(*4-2) New Satan Ransomware available through a Ransomware as a Service. | Bleeping Computer https://www.bleepingcomputer.com/news/security/new-satan-ransomware-available-through-a-ransomware-as-a-service-/

(*4-3) Satan ransomware adds EternalBlue exploit |Blaze's Security Blog https://bartblaze.blogspot.com/2018/04/satan-ransomware-adds-eternalblue.html

(*4-4) Satan Ransomware Spawns New Methods to Spread | AlienVault https://www.alienvault.com/blogs/labs-research/satan-ransomware-spawns-new-methods-to-spread

(*4-5) DBGer Ransomware Uses EternalBlue and Mimikatz to Spread Across Networks | Bleeping Computer https://www.bleepingcomputer.com/news/security/dbger-ransomware-uses-eternalblue-and-mimikatz-to-spread-across-networks/

(*4-6) 「CERBER」バージョン6：ランサムウェアの変遷と今後の展開 | TrendMicro https://blog.trendmicro.co.jp/archives/15054

(*4-7) ランサムウェア「CERBER」に新たな機能追加。ビットコインを窃取 | TrendMicro https://blog.trendmicro.co.jp/archives/15664

引用一覧(3/3)

(*5-1) Reported malicious module: getcookies | The npm Blog https://blog.npmjs.org/post/173526807575/reported-malicious-module-getcookies
(*5-2) Backdoored Python Library Caught Stealing SSH Credentials | Bleeping Computer https://www.bleepingcomputer.com/news/security/backdoored-python-library-caught-stealing-ssh-credentials/
(*5-3) File-Wiping Malware Placed Inside Gentoo Linux Code After GitHub Account Hack | Bleeping Computer https://www.bleepingcomputer.com/news/linux/file-wiping-malware-placed-inside-gentoo-linux-code-after-github-account-hack/
(*5-4) Minecraft players exposed to malicious code in modified “skins” | Avast https://blog.avast.com/minecraft-players-exposed-to-malicious-code-in-modified-skins
(*5-5) MINECRAFT: JAVA EDITION SKINS ISSUE UPDATE | Minecraft https://minecraft.net/en-us/article/minecraft-java-edition-skins-issue-update

(*6-1) SP800-63B | NIST https://openid-foundation-japan.github.io/800-63-3/sp800-63b.ja.html
(*6-2) 情報セキュリティハンドブック | NISC https://www.nisc.go.jp/security-site/handbook/index.html
(*6-3) 「JIS Q 15001:2006をベースにした個人情報保護マネジメントシステム実施のためのガイドライン-第2版-」の一部改訂について | JIPDECプライバシーマーク推進センター https://privacymark.jp/news/system/2018/0410.html
(*6-4) ヤフーがパスワードの定期変更求める記載削除へ　総務省も「安全なもの」前提呼びかけ | ITmedia http://www.itmedia.co.jp/news/articles/1804/24/news058.html

(*7-1) False contest to win jersey of the Brazilian team found on WhatsApp | ESET https://www.welivesecurity.com/2018/06/04/false-contest-win-brazilian-jersey-whatsapp/
(*7-2) You have NOT won! A look at fake FIFA World Cup-themed lotteries and giveaways | ESET https://www.welivesecurity.com/2018/06/06/fake-fifa-world-cup-themed-lotteries-giveaways/
(*7-3) 2018 Russia World Cup : Russian cyber spy may hack travelers’ mobile devices | Security Affairs https://securityaffairs.co/wordpress/73527/security/world-cup-survaillance.html
(*7-4) GoldenCup: New Cyber Threat Targeting World Cup Fans | Symantec https://www.symantec.com/blogs/expert-perspectives/goldencup-new-cyber-threat-targeting-world-cup-fans
(*7-5) NavRAT Uses US-North Korea Summit As Decoy For Attacks In South Korea | Cisco https://blog.talosintelligence.com/2018/05/navrat.html
(*7-6) 北朝鮮ハッカー集団「ＡＰＴ３７」、中国と連携　攻撃技術の情報交換　米朝会談見据えスパイ継続 | 産経ニュース https://www.sankei.com/world/news/180604/wor1806040019-n1.html

(*8-1) REDSCAN IN THE NEWS: RAISING AWARENESS OF GDPR PHISHING SCAMS | Redscan https://www.redscan.com/news/redscan-news-raising-awareness-gdpr-phishing-scams/

NTT DATA

Trusted Global Innovator