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4四半期

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。

攻撃グループ「Magecart」によるWebスキミングやソフトウェアサプライチェーンを利用した攻撃など従前から存在していたものの、回数や頻度が少なかった攻撃がその数を増やし存在感を表し始めました。情報漏えい関連においても過去に流出したアカウント情報が集約されたファイル「Collection #1」が公開される事例が発生しました。

攻撃グループMagecartによるWebスキミング

脆弱なオンラインストアが改ざんされ、決済情報が窃取される「Webスキミング」の事例が多く話題となりました。特に注目したのは、攻撃グループ「Magecart」が直接オンラインストアに不正なコードを挿入する手法の他に、JavaScriptライブラリを改ざんし、間接的に不正なコードを挿入する手法を取り入れたことです。この攻撃により広範囲のオンラインストアが間接的に改ざんされました。オンラインストア提供者にとって、脆弱性対応など従前のセキュリティ対策に加え、少しでも改ざんに気づけるようにすることが重要となっています。

ソフトウェアサプライチェーン攻撃

ソフトウェアサプラチェーン攻撃は過去何度か発生していましたが、この四半期はASUSによる事例が大きな話題となりました。「Operation ShadowHammer」と名付けられたこの攻撃は、ASUS社製PCにあらかじめインストールされたユーティリティソフトウェアのソフトウェアサプライチェーンを経由してマルウェアが配布されました。そのため、多くのASUS社製PCが被害を受けました。また、正規の証明書にて署名されていたため、大半のセキュリティ製品では検知できませんでした。

億を超えるアカウント情報の流通

情報漏えい関連で大きく話題になったのは、Collection #1に代表されるアカウント情報を膨大に含んだ7つのファイル群が次々と公開された事例です。全てを合計すると35億件を超えるアカウント情報が含まれた巨大なファイル群であり、内容は過去にインターネットに流出したことのあるアカウント情報を集約したものでした。このようなアカウント情報のリストが公開されるケースは稀であり、基本的には攻撃者がダークウェブ上で秘密裏にやり取りしています。アカウント情報の窃取や流出、それらを集約したリストの流通は定期的に発生していると考えるべきです。ユーザは自分自身のアカウント情報が漏えいしていないか考慮し、2要素認証の利用やパスワード使い回しを行わないなどの対策をする必要がある状況と言えます。

今後の予測

2019年度第1四半期以降、Webスキミングの増加や大量に流出したアカウント情報の悪用したリスト型攻撃の増加、そして市場価格の上昇に伴う暗号通貨関連への攻撃の増加が予測されます。
活発化したWebスキミングはこのまま継続し、被害を受けるオンラインストアが増加していくと考えられます。また、2018年度第4四半期に流出したアカウント情報を悪用した標的型攻撃やリスト型攻撃が発生することは容易に想像できます。暗号通貨の市場価格下落を受けて数が減少していた暗号通貨関連への攻撃は、価格の上昇に伴って増加することが懸念されます。

2. 注目トピック

2.1. Webスキミング

Webスキミングとは、従来のATMやクレジット決済装置に細工をして決済情報を窃取する替わりに、オンラインストア上に不正なコードを挿入して、オンラインストア上で入力された決済情報を窃取する攻撃です。2018年度にこの攻撃を用いて話題になった攻撃グループがありました。世界中で利用されているメジャーなECサイト構築用プラットフォーム「Magento」へ攻撃を行っていたことから、その攻撃グループは「Magecart」と名付けられました [1]。この攻撃グループは以前から存在しており、過去2回、その事例をグローバルセキュリティ動向レポートで取り上げていました [2] [3]。この2018年度第4四半期は、Magecartによる活動や関連する事例が多数見られ、表 1にその一覧をまとめました。

表 2：Webスキミング関連イベントの一覧

No.	日付	概要
1	1/7	キッチン用品企業OXO International社は、同社のオンラインストアが2年以上もの間、改ざんされ、決済情報が漏えいしていたおそれがあることを公表した [4]。ニュースメディアBleepingComputerは、独自に調査して、同社のオンラインストアにはスキミングコードが挿入されていたと報道した [5]。
2	1/16	トレンドマイクロ社は、広告配信用ライブラリを改ざんしてオンラインストアに不正なコードを間接的に仕込みWebスキミングを行う新たな攻撃手法を発見した [6]。フランスのオンライン広告企業Adverline社が提供する正規のJavaScriptライブラリに不正なコードが挿入されており、277ものオンラインサイトでWebスキミングが行われていた。
3	1/17	オランダのセキュリティ研究者 Willem de Grootは、Magecartが悪用している脆弱性を公表した [7] [8]。MySQLの脆弱性で、クライアントアプリが悪意あるMySQLサーバに接続した際に、クライアント側にある任意のローカルファイルを送信してしまうという脆弱性であった。攻撃者は、管理用MySQLクライアントを自らが設置した悪意あるMySQLサーバへ接続させて、同クライアント上に保存されている管理対象サイトの管理者パスワードが記載されたファイルを抜き取った。
4	2/22	スポーツトレーディングカード企業のTopps社は、MagecartのWebスキミングにより顧客の決済情報が漏えいしていたことを公表した [9]。漏えいしたのは、2018/11/19 - 2019/1/9の間にTopps社のオンラインストアで商品を購入した顧客の情報であった。
5	3/14	ニュースメディアSecurity Affairs社は、セキュリティ企業Group-IB社の調査により、新しいWebスキミング用のツールJS Sniffer 「GMO」が見つかったと報道した [10]。スポーツ用品メーカーFILA UK社のサイトを含む7つのオンラインストアで同ツールによりWebスキミングが行われていることが分かった。

No.	日付	概要
6	3/20	セキュリティ企業 RiskIQ社は、寝具販売企業のMyPillow社とAmerisleep社のオンラインストアがMagecartにWebスキミングされていたことを公表した [11]。MyPillow社は2018年10月-2018年11月の間、Webスキミングされていた。Amerisleep社は2018年12月からWebスキミングが開始され、公表時点ではまだスキミングコードがアクティブな状態であった。

セキュリティ企業 RiskIQ社が公開したレポートにて解説されているMagecartが用いているWebスキミングの従来手法を説明します [12]。

1. 管理画面等へ総当たり攻撃を行って ID/PW を推測したり、脆弱性スキャンを行って改ざん可能な脆弱性を把握したりする
2. 1.の情報を用いて、不正ログインしたり、Web コンテンツを改ざんしたりして、決済画面などに Web スキミング用の不正なコードを挿入する
3. ユーザがオンラインストアで決済情報を入力すると、攻撃者のサーバへ決裁情報を送信する

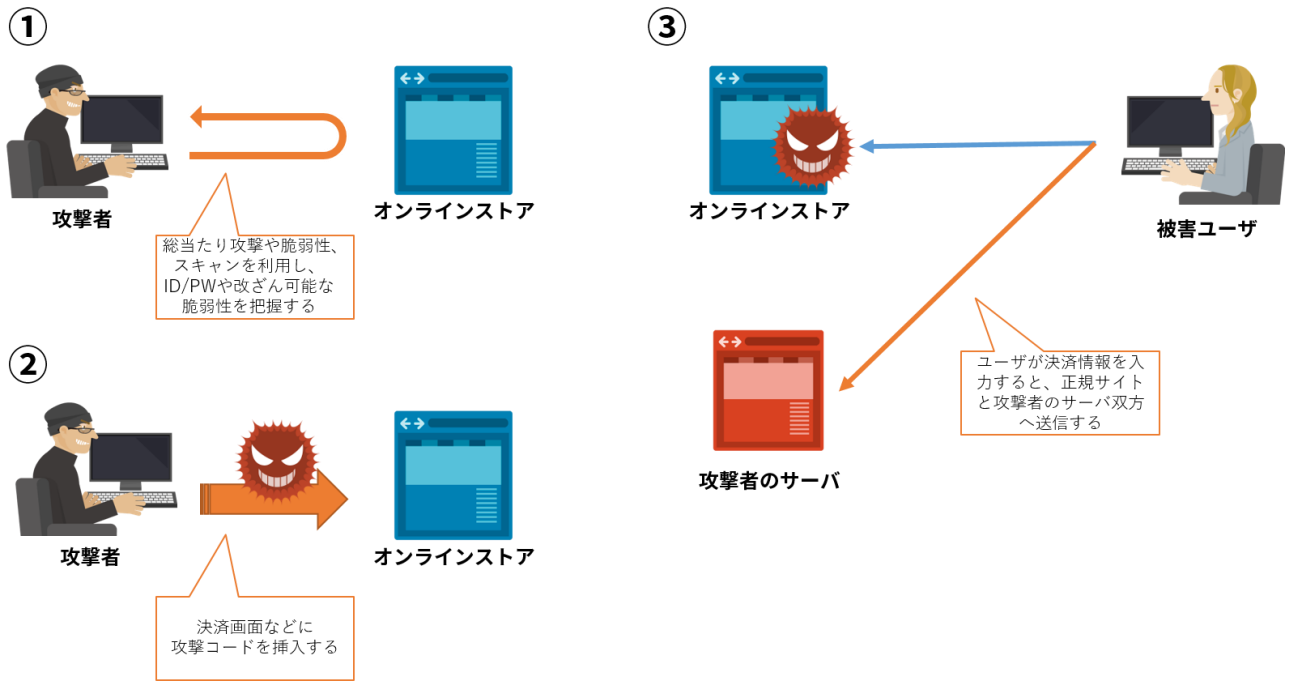


図 1:既存のWebスキミングの流れ(RiskIQの情報 [12]を基にNTTDATA-CERTが作成)

2018年度第4四半期にトレンドマイクロ社が確認した攻撃(No.2の事例)は、従来手法のように直接オンラインストアを改ざんしてWebスキミング用の不正なコードを挿入する手法ではなく、ソフトウェアサプライチェーンを悪用して改ざんしたJavaScriptライブラリを配布することで、多数のオンラインストアへ間接的にWebスキミング用の不正なコードを挿入する手法でした [13]。以下の図 2を使って、この手法を説明します。

1. 攻撃者は、広告配信サービスの提供者の環境へ侵入する
2. 攻撃者は、広告配信で使用する JavaScript ライブラリを改ざんし、Web スキミング用の不正なコードを挿入する。改ざんされた JavaScript ライブラリがオンラインストア(e コマースサイト)へ配信される。同ライブラリを利用しているオンラインストア(e コマースサイト)へ不正なコードが読み込まれる
3. ユーザがオンラインストアで決済した時に、不正なコードにより決済情報が Web スキミングされる
4. 摂取された決済情報が攻撃者のサーバへ送信される

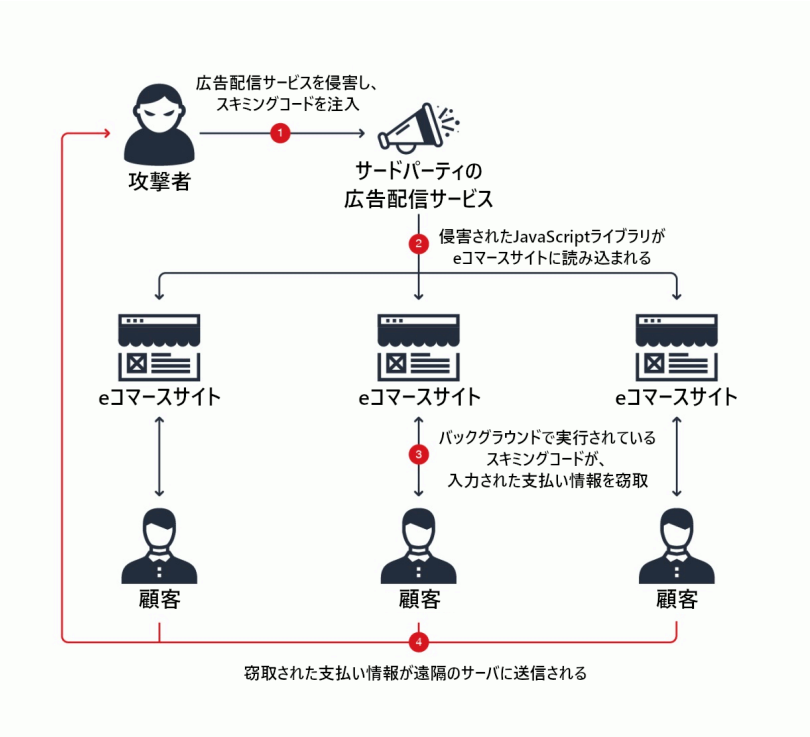


図 2:新しいWebスキミングの流れ(トレンドマイクロセキュリティブログより転載 [13])

この間接的にWebスキミング用の不正コードを設置する手法は、一度の改ざんで広範囲のオンラインストアへWebスキミングの仕組みを設置して、より多くの情報が窃取可能になることが大きなメリットです。図 3は、2018年末から1月の初週にかけてトレンドマイクロが検出したWebスキミング活動による不正なドメインへのアクセス検出数の推移 [13]です。2019年1月1日から2日にかけて、このソフトウェアサプライチェーンを悪用してWebスキミングを設置したことによって、検出数が急増しました。

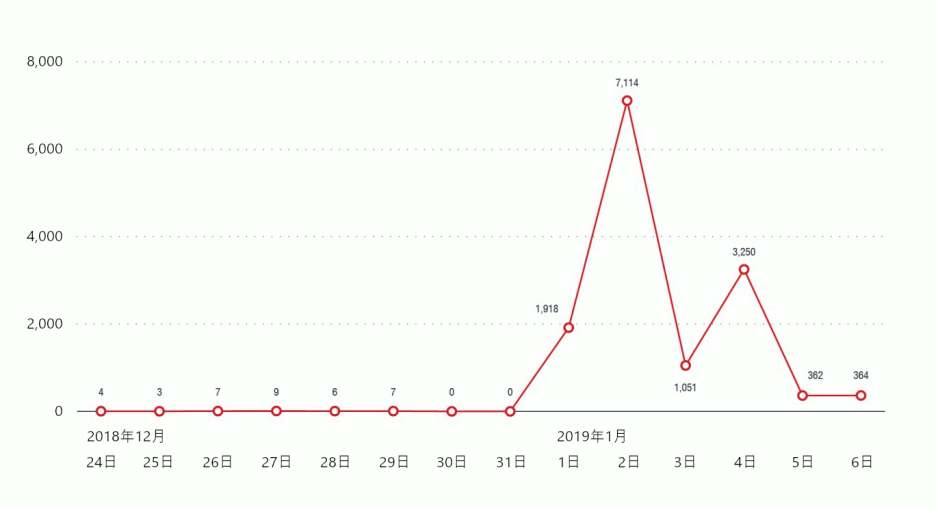


図 3：Webスキミング活動による不正なドメインへのアクセス検出数(トレンドマイクロセキュリティブログより転載 [13])

間接的にWebスキミング用の不正コードを設置する手法は、堅牢なJavaScriptライブラリ提供者や広告配信サービスの提供者の環境へ侵入しなければならないため、2018年度第4四半期に発生した件数は、この1件の事例のみでした。しかし、攻撃が活発になってきていることから、従来の直接オンラインストアを改ざんしてWebスキミング用の不正なコードを挿入する手法と、この間接的な手法の両方方法で多くのオンラインストアへWebスキミングが設置されて決済情報が窃取されると予測します。Webスキミングの被害に遭わないために、オンラインストア提供者は、ミドルウェアやプラットフォームを適宜アップデートして脆弱性を解消するとともに、認証の仕組みやセキュリティ設定などの見直しにより、オンラインストアを堅牢化することを推奨します。また、間接的な手法による被害を防ぐためには、信頼できるライブラリやプラグインのみを利用すること、効果的な対策ではありませんが、少しでも早く改ざんされたライブラリに気づくために、セキュリティ診断やWeb改ざん検知ソリューションの導入なども一考してください。

2.2. 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 [14]。
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、取引先などの商流(サプライチェーン)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。この攻撃は、IPAが発表した「情報セキュリティ10大脅威2019」にて、組織向け脅威第4位に新たにノミネートされています [15]。
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、マルエ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。2016年にはMac用P2Pファイル共有ソフト「Transmission」のアップデータに、2017年にはWindows用システムクリーナーソフト「CCleaner」のインストーラにマルウェアを挿入したサプライチェーン攻撃が行われました [16] [17]。この2018年度第4四半期には、表 3に示す2つ目のいわゆるソフトウェアサプライチェーン攻撃に関する事例が4件発生しました。

表 3:ソフトウェアサプライチェーン攻撃関連イベントの一覧

No.	日付	分類	概要
1	1/19	PHP PEAR	PHP向けのパッケージ管理ツールPEARの公式サイトに攻撃が行われた形跡が見つかり、改ざんされたインストーラ(go-pear.phar)が置かれていたことが判明した [18]。
2	1/22	Debian APT	Debian系Linuxディストーションのパッケージ管理ツールAPTに脆弱性があることが判明。当該脆弱性を悪用して悪意あるアプリをインストールしたり、任意のコードを実行したりすることが可能であった [19]。
3	3/13	Android SDK	チェックポイント社は、Google Play Store上でアドウェアキャンペーン「SimBad」を発見した。RXDrioderという広告関連のSDKにアドウェアが仕込まれており、当該SDKを使って開発された200以上のアプリにアドウェアが埋め込まれ、当該アプリのダウンロードは通算1億5,000万回も行われた [20]。
4	3/25	ASUS Live Update	カスペルスキーラボは、ASUS社提供のソフトウェア「ASUS Live Update」を悪用してマルウェアを配布する攻撃「Operation ShadowHammer」の調査結果の一部を発表した [21]。

この4件の中で大きく話題になったのは、ASUS社の事例です。カスペルスキーラボによって「Operation ShadowHammer」と名付けられたこの攻撃は、ASUS社製PC用の自動アップデートユーティリティソフト「ASUS Live Update」を悪用してマルウェアを配布していました [22]。このユーティリティソフトは、最新のASUS社製PCの大部分にプリインストールされています。攻撃者は、このユーティリティソフトへマルウェア機能を追加するコードを挿入したあと、ASUS社から盗んだ正規

の証明書を使って、ソフトウェアへコード署名を施しました。その後、攻撃者は公式のアップデートサーバへ侵入して改ざんしたユーティリティソフトを配信しました。ウイルス対策ソフトは、コード署名を使って、そのソフトウェアが改ざんされていないことを検証します。そのため、ウイルス対策ソフトは正規の証明書でコード署名されたこのユーティリティソフトの改ざんを検知できず、5万7,000台以上のコンピュータが感染しました [23]。

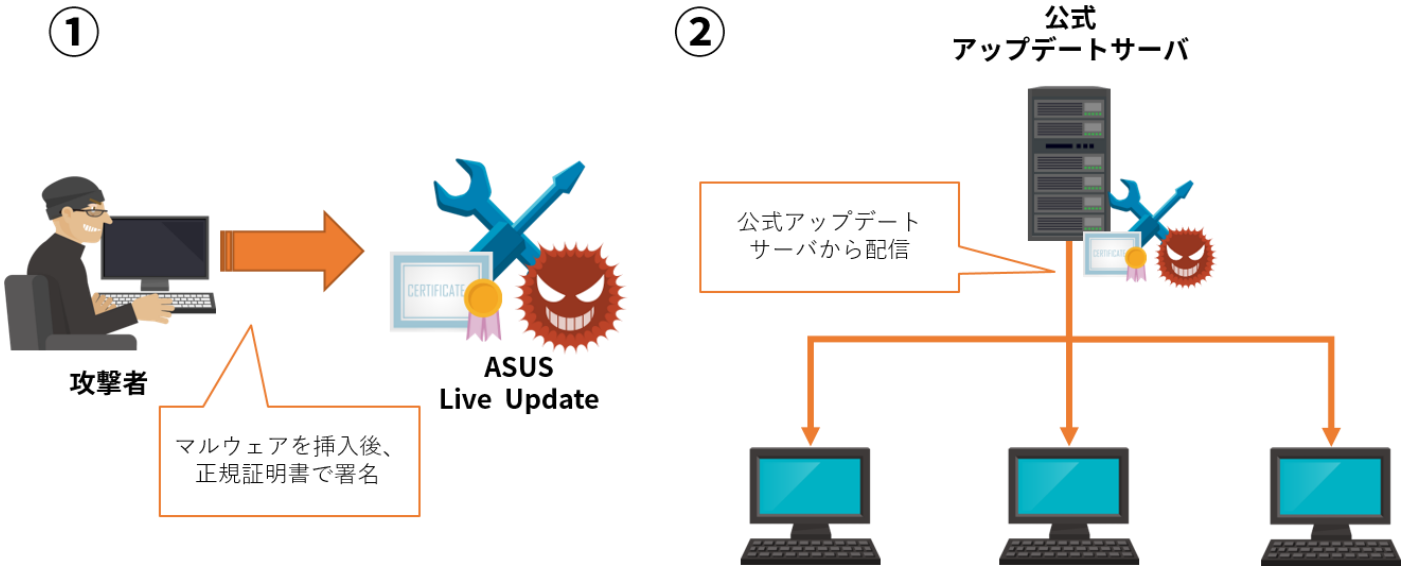


図 4：Operation ShadowHammer攻撃の流れ(カスペルスキーラボの情報 [22]を元にNTTDATA-CERTにて作成)

ユーザ側が、今回のようなソフトウェアサプライチェーン攻撃を早期に検知して対処することは難しいです。メーカー側は、アップデートサーバなどの顧客へ広範囲に影響を与えうるサーバは優先的に堅牢化するとともに、攻撃者に利用されないように証明書などの重要ファイルの管理を厳重にすることを推奨します。

2.3. 2要素認証

2要素認証とは、『ユーザだけが知っている何か』『ユーザだけが所有している何か』『ユーザ自身の特性（指紋など）』のうち、２つの要素を組み合わせてユーザの身元を確認する仕組みです[24]。例えば、ユーザだけが知っているIDとパスワードの組み合わせとユーザだけが所有している携帯電話へ届いたSMSメッセージに書かれているワンタイムパスワード、またはユーザだけが所有している端末上のスマートフォンアプリが生成したワンタイムパスワードを組み合わせています。

従来のIDとパスワードを組み合わせた方式と比べて、総当たり攻撃や情報漏えいなどでIDとパスワードの組み合わせが攻撃者に特定されてしまった場合でも、攻撃者は直ちに不正ログインできないため、より安全です。しかしながら、表 4に示すように、この2要素認証の安全性を揺るがすような事例がこの2018年度第4四半期にありました。

表 4：2要素認証関連のイベント一覧

No.	日付	概要
1	1/2	ポーランドのセキュリティ研究者Piotr Duszyńskiは、2要素認証を突破するツール「Modlishka」を公開した [25]。当ツールはフィッシングサイトと正規サイトの間で動作するリバースプロキシとして動作し、ユーザの入力データおよび認証データを窃取する。
2	2/1	ニュースメディアMotherboardが、英国の銀行MetroBankのオンラインサービスの2要素認証が突破されて、銀行口座から預金が盗まれたことを報道した [26]。当該銀行は、送金確認時の２要素認証の2要素目のワンタイムパスワードの配布にSMSメッセージを利用していた。攻撃者は公衆電話交換網で使用されている信号方式SS7の脆弱性を悪用してSMSメッセージを傍受し、ワンタイムパスワードを取得していた。

事例No.1のポーランドのセキュリティ研究者Piotr Duszyńskiが公開したツール「Modlishka」[27]は、Webブラウザと正規サイトの間で動作するリバースプロキシです。ユーザがModlishkaに入力した認証情報をリアルタイムで正規サイトに送信し、正規サイトからの応答はModlishkaを経由してユーザへ表示します(図 5参照)。ユーザから見ると、Modlishkaには正規サイトへアカウント情報や各種データを入力している時と同じ処理結果が表示されます。ところが実際には、ユーザが入力した情報がModlishkaを経由して正規サイトへ転送されているだけで、ユーザが入力した情報は全て攻撃者へ知られてしまいます。

公開されたデモ動画 [28]では、Googleのフィッシングサイトを作成し、攻撃者がGoogleのSMSメッセージを利用した2要素認証を突破して不正アクセスが成功している様子を見ることができます。

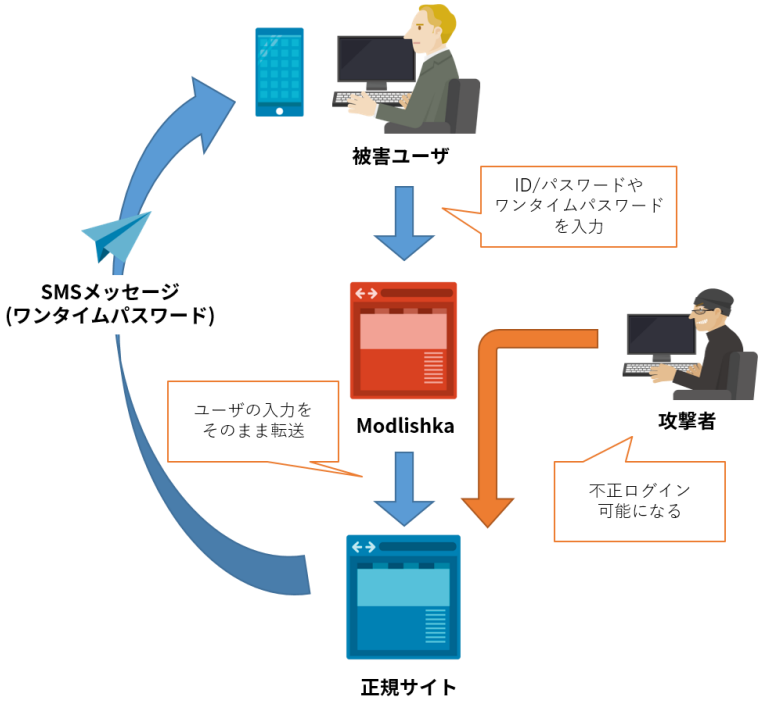


図 6：Modlishkaの通信の流れ(Piotr Duszyńskiのブログ [25]を基にNTTDATA-CERTにて作成)

英国の銀行MetroBankの事例(No.2)では、攻撃者は公衆電話交換網を制御するための信号プロトコルであるSS7(Common Channel Signaling System No.7)の脆弱性を悪用し、被害ユーザのSMSメッセージを窃取することで2要素認証を突破しました。SS7は国際標準規格であり、日本を含む世界各国で利用されています。しかし、SS7は通信事業者間のみでの利用を前提としており、コマンド送信者認証プロセスがなく、全てのコマンドが処理されてしまうため、攻撃者が受信者になりすましてSMSメッセージを受信することが可能です。2015年には、この脆弱性を悪用して通信を傍受できると報じられていました [29]。2017年にはドイツの銀行において、今回の件と同様にSMSメッセージを窃取されて2要素認証が突破され、不正に送金された事例が報道されていました [30]。

どちらの事例も2要素認証を採用していたとしても実装方式によっては、セキュリティ的に万全でないことを示しています。Piotr Duszyńskiは、ブログ内で2要素認証をより安全にする方法として、FIDO U2Fプロトコルに基づくハードウェアトークンを2要素認証の2番目の要素として採用することを挙げています。FIDOでは、サービス毎に鍵を生成しており、FIDOに対応したトークンとクライアントがユーザに替わりサービスと認証通信を行います。そのため、SMSに2要素目の情報が流れたり、ユーザが不正なサイトに2要素目の情報を入力してしまったりすることがなくなり、今回紹介した事例を防ぐことができます。サービス提供者は、FIDOのようなよりセキュアな認証方法をユーザに提供し、ユーザはよりセキュアな認証方法を選択することで、セキュリティ事故の発生は減少すると考えられます。

3. 情報漏えい

2019年1月17日、オーストラリアのセキュリティ研究者Troy Hunt氏は、ファイル群「Collection #1」の解析結果を公開しました [31]。「Collection #1」には7億7,300万件ものアカウント情報が含まれており、大きな話題となりました。また、セキュリティジャーナリストのBrian Krebs氏の報告によると、「Collection #1」は、より大きなファイル群"Collection"の一部であることが判明しました。すべてを合計すると35億件を超えるアカウント情報が含まれていました [32]。

Brian Krebs氏は、インスタントメッセージシステムのTelegramを使って「Collection #1」を公開したユーザ「Sanixer」に連絡し、調査を行ったと述べています。Sanixerは、「Collection #1」は2，3年前の情報であること、より大きなファイル群"Collection"以外にもアカウント情報を保持していること、1年以内に収集した新しいアカウント情報を合計で4テラバイト以上保有していること等をBrian Krebs氏へ伝えています。

また、Recorded Future社が「Collection #1」に関係する攻撃者の調査を実施しました [33]。Recorded Future社は、オンライン上で「C0rpz」と呼ばれる人物が過去3年間に渡り、何十億件ものアカウント情報を収集したと報告しています。「C0rpz」から、KrebsOnSecurityのBrian Krebs氏が接触した「Sanixer」や、「Clorox」と呼ばれる人物へアカウント情報が売られたと報告しています。

「Collection #1」関連のアカウント情報の売買、情報公開の時系列は、以下の通りです。

表 5：「Collection #1」関連のアカウント情報の売買、情報公開の時系列

日付	概要
2018年4月	インターネット上で「ANTIPUBLIC #1」が共有される
2018年10月	アンダーグラウンドフォーラムへ初めてCollection #1の関連データが投稿される
2018年末頃	ダークWeb上に「Collection #1」が出現する
2019年1月7日頃	ハッカーフォーラムに「Collection #1」の存在が投稿される
2019年1月6日-12日頃	Troy Hunt氏が「Collection #1」について複数の報告を受ける
2019年1月17日	Troy Hunt氏が解析結果を公開
	Brian Kreb氏が「Collection #1」を含む合計7つのパッケージを報告する

表 6:”Collection”の情報

名称	サイズ
ANTIPUBLIC #1	102.04 GB
AP MYR & ZABUGOR #2	19.49 GB
Collection #1	87.18 GB
Collection #2	528.50 GB
Collection #3	37.18 GB
Collection #4	178.58 GB
Collection #5	40.56 GB

ソリトンシステムズ社は、「Collection #1」を分析して、末尾が「.jp」のメールアドレスやファイル名を抽出して日本人や日本の組織に関係するアカウント情報の件数を算出しました [34]。日本人と推測されるメールアドレスとパスワードが対になったアカウント情報は総数2,002万件、そのうち比較的新しいと推測されたアカウント情報は803万件ありました。アカウント情報が流出している日本のWebサービスのサイトは、総数402サイト、比較的新しいアカウント情報が流出していると思われるWebサービスが6サイトありました。

アカウント情報の窃取や流出、それらのアカウント情報を集約したリストの流通は、常に発生していると考えるべきです。それらのリストは、基本的にダークウェブ上でやり取りされるため、「Collection #1」のようにインターネット上に公開されるケースは多くありません。通常はダークウェブ上で秘密裏にやり取りされていたアカウント情報が、誰でも容易に取得できてしまったため、能力が低い攻撃者でも簡単にリスト型攻撃が行えます。公開されていないアカウント情報も存在するため、両方のケースを考慮して対策する必要があります。アカウント情報を悪用したリスト型攻撃への対策は、2要素認証の利用を強く推奨します。2要素認証の利用により、アカウント情報が漏えいしても不正ログインを防ぐことが可能です。あるサービスからの漏えいしたアカウント情報により他サービスへ不正ログインされるリスクを無くすためには、パスワードの使い回しは、避けるべき必須ルールです。

「Collection #1」関連の情報漏えい以外にも2018年度第4四半期は、複数の大規模な情報漏えいが発生、または発覚しました。発生した、または確認された情報漏えいの一部を下記にまとめました。2018年度第3四半期以前と比較して、1億件以上の大規模なアカウント情報の漏えいや公開の事件が複数件発生したことが特徴です。

表 7:情報漏えい関連の出来事

日付	概要	被害件数
12/28	HackenProofのBob Diachenko氏が、中国の求職者の履歴書等の2億件を超える情報がMongoDBにおいて認証なしでアクセス可能な状態であることを発見した [35]。公開された日付は不明であるが、発見から一週間後にデータベースは保護されたという。	2億件
1/21	オンラインカジノグループが、1億800万件以上の情報を漏えいしたことが明らかになった。顧客の個人情報、預金、引き出し等の情報が含まれます。大金を持っている顧客が詐欺や強盗などの標的にされることが懸念される [36]。	1億800万件
1/25	オージス総研は、大容量ファイル転送サービス「宅ふぁいる便」の一部サーバが不正アクセスを受けて、全登録ユーザ数に相当する480万件の顧客情報が流出したと発表した。調査より、国外から不正アクセスされたおそれが高いという [37]。	480万件
2/11	「Gnosticplayers」と呼ばれる攻撃者がダークウェブの「Dream Market」で個人情報の販売を2 月から3月の間に4回実施した。1回目に6億2,000万件、2回目に1億2,700万件、3回目に9,300万件、第4回に2,650万件の個人情報を販売したという [38]。	8億6,650万件 （4回合計）
2/25	セキュリティ研究者のBob Diachenko氏およびVinny Troja氏がパスワードで保護されていないMongoDBを発見した。データベースはVerifcations.io というEメールマーケティング会社のもので、約8億900万件の個人情報が格納されていた。Bob Diachenko氏はこのDBから漏えいしたおそれのある個人情報と、「Collection #1」で確認された個人情報は別であると言っている [39]。	8億900万件
3/8	3/8にCitrix社が社内ネットワークへの不正アクセスがあったことを発表した。Resecurity社やFBIからの情報提供で不正アクセスが判明した。パスワードスプレーと呼ばれる手法を用いて、6テラバイト以上のデータを盗み出されたとみられている [40]。	6テラバイト （詳細件数不明）

4. 脆弱性

2019年2月20日、Check Point Software Technologies社がWindows向けファイル圧縮・解凍ユーティリティ「WinRAR」のディレクトリトラバーサルの脆弱性（CVE-2018-20250）を公開しました [41]。本脆弱性は、過去19年間にリリースされたすべてのバージョンに影響するとされています。脆弱性は「.ace」形式のアーカイブを解凍する「UnAceV2.dll」ライブラリに存在しています。Check Point社は、攻撃者が脆弱性を悪用してWindowsスタートアップフォルダにマルウェアを植え付けることができると指摘しています。

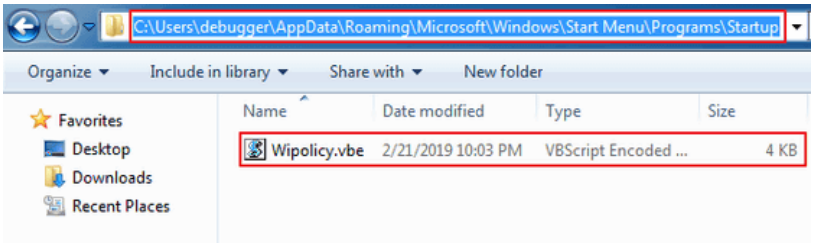


図 7:画像ファイルや文書ファイルとは別にスタートアップフォルダに展開されるファイルの例
(360威胁情报中心blogより転載 [42])

本脆弱性は、2018年に発見され、2019年1月28日に脆弱性を対策した「WinRAR 5.70 Beta 1」がリリースされました。WinRARの開発者らは、「.ace」アーカイブ形式のサポートを打ち切る形でこの脆弱性に対処しました。しかし、脆弱性が公表されて以来、様々な悪用が確認されています。展開されるファイルも、ばらまき型と思われる技術文書やアダルト画像から、標的型と思われるウクライナの法律に関する文書や国際連合（UN）と人権に関する文書まで存在しています。攻撃者は脆弱性を悪用して任意の場所に任意のファイルを作成可能であるため、ウイルス感染のリスクがあります。WinRARの利用者は、アップデート等の対策を実施するとともに、提供元不明ファイルの取り扱いには注意する必要があります。

2018年度第4四半期に公開された脆弱性のうち、特にゼロデイ脆弱性、悪用された脆弱性、話題となった脆弱性を中心に表 8へまとめました。

表 8:その他ゼロデイ脆弱性および話題となった脆弱性

公開日	製品	脆弱性番号	概要
1/9	IDenticard PremiSys アクセス制御システム	CVE-2019-3906 CVE-2019-3907 CVE-2019-3908 CVE-2019-3909	Tenable Researc社は、IDenticard社のPremiSysシステムに4つの脆弱性を発見し、1/14に公開した [43]。本脆弱性を悪用すれば、管理者権限で様々なアクションを実行可能である。IDenticard社は世界中の企業、教育機関、医療施設、政府機関など数万社以上の顧客を持っている。1/31にIDenticardより修正パッチが提供された。
1/16	ES File Explorer File Manager (Android)	CVE-2019-6447	2014年以来5億件以上ダウンロードされたAndroid用アプリケーション「ES File Explorer File Manager」に入力確認に関する脆弱性が発見された。アプリケーションを開くと同時にHTTPサーバを起動し、同一ネットワークから任意コード実行が可能になる。アプリケーションを削除してもポートは開いたままとなる [44]。
1/25	Cisco RV320, RV325デュアルギガビットWAN VPNルータ	CVE-2019-1652 CVE-2019-1653	Cisco RV320およびRV325デュアルギガビットWAN VPNルータに、情報流出の脆弱性とコマンドインジェクションの脆弱性が発見された。1/25にCisco社によりアップデートで修正されたが、Bad Packets Report社は、サイバー攻撃の標的にされていると1/26に報じ、攻撃コードも公開されていることから確認やパッチ適用を呼び掛けた [45]。
1/25	Ttal Donations (WordPress)	CVE-2019-6703	Calmar Webmedia社が提供するWordPress向けプラグイン「Ttal Donations」にサイトの管理者権限を奪われるおそれがある脆弱性が発覚した。脆弱性を悪用すれば、新規ユーザを作成して管理者権限を付与できるため、本来アクセスできないデータへアクセスが可能である。Defiant社によると、メンテナンスはすでに行われていない可能性が高い [46]。
2/7 ※関連情報初報は1/29	iOS, macOS	CVE-2019-6223 CVE-2019-7286 CVE-2019-7287	FaceTimeのビデオ通話機能において相手の操作なしで呼び出し先の音声を聞くことができる脆弱性が話題となった。本脆弱性が修正されたバージョンには、その他にも権限昇格や任意コード実行が可能となるゼロデイ脆弱性2件の修正が含まれていた [47]。また、GoogleのProject ZeroはmacOSカーネルの重大なゼロデイ脆弱性およびPOCコードを公開した [48]。

公開日	製品	脆弱性番号	概要
2/11	runc	CVE-2019-5736	DockerやKubernetesなどで使われているコンテナ･ランタイム「runc」に脆弱性が発見された。本脆弱性を悪用すれば、悪意あるコンテナがruncバイナリを上書きして、ホストするシステムのroot権限でコードを実行できてしまう。コンテナ全体に影響を及ぼし、同一ホスト上の数百から数千のコンテナに被害を及ぼすおそれがあるとして大きな話題となった[49]。
2/20	Drupal	CVE-2019-6340	Drupalに認証なしでリモートから任意のコード実行が可能な脆弱性が発見された。脆弱性はREST APIを利用するモジュールを有効にしている場合に影響を受ける。すぐに攻撃コードが公開された。LAC社によると脆弱性が公開された翌日にDrupalのバージョンを調査する試みを多数観測したという。[50]
3/1	Adobe ColdFusion	CVE-2019-7816	Adobe ColdFusionに攻撃者がファイルアップロードの制限を回避してWebから閲覧可能なディレクトリにファイルをアップロードすることができる脆弱性が発見された。攻撃者がColdFusionの実行ユーザの権限で任意のコードを実行できるおそれがある。Adobe社は脆弱性公開時点で、すでに悪用された旨の報告を受けていた [51]。
3/1	Google Chrome	CVE-2019-5786	3/1にGoogle社は、ChromeのFileReader APIの解放後使用（UAF：Use After Free）の脆弱性を公開した [52]。Google社のセキュリティ担当者によると3/1のパッチ公開前に脆弱性を悪用した攻撃を受けていたという。Windows win32k.sysのカーネルドライバのローカル権限昇格の脆弱性と組み合わせて悪用されており、リモートから任意コード実行が可能である [53]。
3/13 ※関連情報初報は3/1	Windows	CVE-2019-0797 CVE-2019-0808	Microsoftの月例パッチアップデートで修正された脆弱性のうち2件が「Win32k」のゼロデイ脆弱性であった。悪用されるとリモートよりコードを実行されるおそれがある。「CVE-2019-0808」は、Googleの研究者が指摘していた脆弱性であり、上記のGoogle Chromeの脆弱性と組み合わせた攻撃が確認されている [54] [55]。

5. マルウェア・ランサムウェア

2018年度第4四半期に、確認されたマルェアに関する攻撃キャンペーン、ランサムウェア、その他マルウェアを表 9から表 10に示します。

表 11：2018年度第4四半期に確認、報告されたマルウェアに関するキャンペーン

時期	名称	概要
1月	Emotet （マルウェア名）	Melon Security社の研究者より、さらに多くのシステムに感染するよう進化した「Emotet」のキャンペーンが報告された。Word文書に偽装されたXMLファイル内のマクロを悪用する。ヘルスケア業界を筆頭に様々な業界が標的となっていた [56]。
1月	SpeakUp （マルウェア名）	Check Point Software Technologies社がトロイの木馬「SpeakUp」を使った攻撃キャンペーンを確認。AWS等のクラウド上でホストされたLinuxを標的とする。中国、インド、東南アジア、南米のサーバが標的にされていた [57]。
1月	Ursnif （マルウェア名）	Cisco Talos社が情報搾取型マルウェア「Ursnif」を配布する新しいキャンペーンを報告した。悪意のあるVBAマクロを含んだWord文書からUrsnifへ感染する。感染後は、CABファイルを用いて搾取するデータを圧縮することで検出を回避するとされる [58]。
1月	Love you	Love Youスパムメールと呼ばれるキャンペーンが確認された。件名は「I Love You」や「My love letter for you」と書かれており、件名が英文になる以前は顔文字のみであった。ランサムウェア、コインマイナー、スパムボットに複合感染するおそれがある [59]。
2月	Astaroth Trojan （マルウェア名）	Windows OSの正規のプロセスやウイルス対策ソフトを悪用するトロイの木馬が2018年10月に発見された。標的はブラジルとヨーロッパ諸国とされている。2月に進行中のキャンペーンとして報告された [60]。
2月	Shlayer （マルウェア名）	macOSを対象とするマルウェア「Shlayer」の新種が発見された。Adobe Flashの更新プログラムとして配布された。侵害された合法的なドメインを用いるケースがあり、使用されたDMGファイルの多くは正規のApple開発者IDで署名されていた [61]。
2月	Operation Pistacchitto	2016年より活動が確認されているイタリアを起源とするマルウェアキャンペーン。Githubプラットフォームによる拡散が2月に報告された。スパムメール内の悪意のあるリンクにより感染する。Windowsのみでなく、Android、Linux、macOSを対象とする亜種も確認されている [62]。

表 12：1月から3月に確認、報告されたランサムウェア

時期	名称	概要
1月	Anatova	McAfeeの研究者によって発見された強力な暗号化機能やモジュール型の拡張機能を備えたランサムウェア [63]。ゲームやアプリケーションのアイコンに似せてユーザにクリックさせてランサムウェアをダウンロードさせる。ピアツーピアのネットワークを経由して拡散する。
2月	Jokeroo	「Jokeroo」は、Twitter経由で宣伝され、アンダーグラウンドハッキングフォーラム「Exploit.in」で配布されている新たなRaaSである。当初はGandCrabに関係するかのように装っていたが、何の関係もないことを開発者が明かした。ファイルを暗号化して金銭を要求する [64]。
3月	CryptoMix	ランサムウェア「CryptoMix」の亜種が発見された。個々のコンピュータではなくネットワーク全体を標的にしている。実行ファイルはコード署名されており、ウイルス対策ソフトは検知しない。本体起動後、ウイルス対策ソフトを無効にし、すべてのファイルを閉じて暗号化する。 [65]。
3月	JNEC.a	WinRARの脆弱性（CVE-2018-20250）を悪用して拡散するランサムウェア。ファイルを暗号化して拡張子を「.Jnec」へ変更する。金銭を支払った後に復号化キーを受け取るためのGmailアドレスを生成するという特徴がある [66]。
3月	Yatron	ランサムウェア「Yatron」は、PCに感染しているマルウェアEternalBlueとDoublePulsarを悪用してネットワーク上の他のコンピュータへの拡散を試みる。72時間以内に金銭が支払われなかった場合、ファイルを削除する [67]。
3月	LockerGoga	システム管理ツール「PsExec」を悪用してPCへランサムウェアを送り込んで実行する。身代金を支払うことでファイルを復号する機会さえ与えられないことから、業務停止を目的として拡散されたと思われる。1月にAltran Technologies社が攻撃されたと報告した。欧州のいくつかの企業が影響を受けている [68]。

表 13：1月から3月に確認、報告されたその他マルウェア

時期	名称	概要
1月	Vidar	マルウェア研究者によると、Fallout Exploit Kitを使って新たな情報収集型ハッキングツール「Vidar」が拡散した。Fallout Exploit Kit は、ランサムウェアGan d Crabの拡散にも用いられた。Vidarはプロセス情報を盗み取る目的で利用する [69]。
1月	CookieMiner	「CookieMiner」は、Apple社のMacで動作するChromeやSafari等のブラウザからCookieを盗み取り、ブラウザに保存されたユーザ名、パスワード、クレジットカード情報。SMS情報等を窃取する [70]。
1月	Rietspoof	FacebookのMessengerやSkypeなどのインスタントメッセージングアプリケーション経由で拡散する。セキュリティ企業 Avast社の報告によると、2018年8月に発見され、2019年1月に拡散活動が活発化した。感染したホスト常駐し、その他のマルウェアのダウンロードを試みる [71]。

時期	名称	概要
1月	TrickBot （亜種）	リモートデスクトップアプリVNC、PuTTY、RDPの認証情報を窃取する「pwgrab」モジュールが追加された。不正マクロを含むExcelを添付したメールが感染経路として確認されている [72]。
1月	Mirai （亜種）	脆弱な設定、パスワードのIoTデバイスを攻撃することで知られる「Mirai」の亜種が報告された。デジタルサイネージ用機器、ワイヤレスプレゼンテーションシステムなど様々なIoTデバイスへ感染する [73]。その他にも、さまざまな「Mirai」の亜種が確認されている。
2月	Winpot	ATMを不正操作して金銭を得るジャックポットと呼ばれる攻撃に用いられるマルウェア。スロットのプレイ画面に模して作られている。物理的、またはネットワーク経由でATMにアクセスしてインストールされる [74]。

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2008年度第4四半期では、アメリカを中心に政府や公共機関主導のセキュリティ施策や法案提出が行われました。

表 14：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	1/16	アメリカ	アメリカ国防高等研究計画局(DARPA[1])は、システム間の情報と通信を安全かつ確認可能な状態で追跡する手段を有するソリューション作成を目的としたプロジェクト「GAPS」を発表 [75]。 このプロジェクトは、異なるセキュリティレベル間の情報移動やリスクの高いトランザクションに対して物理的に確認可能なハードウェアやソフトウェアアーキテクチャを開発することを最終目標としている。
2	1/16	アメリカ	超党派の議員グループは、ホワイトハウス内に「Office of Critical Technologies and Security」の設置を求める法案をアメリカ上院および下院へ提出した [76]。 これは、国家支援を受けた技術盗用への対抗を目的としている
3	1/30	アメリカ	司法省は、FBIとアメリカ空軍犯罪捜査司令部(AFOSI[2])が北朝鮮のハッカーが使用するボットネットを調査・テイクダウンする取り組みを発表した [77]。連邦刑事訴訟規則の規則41の改正に従い、裁判所命令および捜索令状を取得すれば、ボットネットの調査やテイクダウンの他にISPを通して感染端末ユーザに被害を連絡できる。
4	2/15	アメリカ	ニュースメディアdelmarva now.は、ランサムウェア攻撃を行った場合の刑罰を重くする新たな法案がアメリカのメリーランド州議会に提出されたと報道した [78]。1,000USD(約13万円)以上の損失を与えた場合を重罪とし、最大10万USD(約1,300万円)の罰金と10年の懲役刑を課す。
5	2/20	日本	情報通信研究機構(NICT)が、インターネット上のIoT機器にスキャンを行い、悪用のおそれのある機器情報をISPへ通知する取り組み「NOTICE」の実施が開始された [79]

[1] the Defense Advanced Research Projects Agency : アメリカ国防高等研究計画局

[2] U.S. Air Force Office of Special Investigations ： アメリカ空軍犯罪捜査司令部

No.	日付	国/地域	概要
6	2/20	ロシア	ニュースメディアBBCは、ロシア議会がロシア軍の兵士による勤務中のスマートフォン使用を禁ずる法案を可決したと報じた [80]。 この法案は、機密情報の漏えいなどの国家安全保障上の問題に対処するために、インターネットへの接続や写真撮影、SNSへの投稿などを禁止した。
7	2/24	インド	ニュースメディアE Hacking Newは、インド政府がマルウェアやフィッシングからユーザを保護する機能を持つDNSサーバを準備中であると報道した [81]。ユーザが不審なサイトにアクセスした際にポップアップを表示し、危険を知らせることができる。
8	3/18	EU	EU理事会は、国境を超える大規模サイバー攻撃に備えるために、EU法執行緊急対応プロトコルを採択した [82]。ユーロポールに、中心的な役割を与えている。
9	3/25	アメリカ	アメリカ国立標準技術研究所(NIST[3])は、マイクロサービスベースのアプリケーションシステムに対するセキュリティ戦略を記したSP 800-204のドラフトを公開した [83]。

[3] National Institute of Standards and Technology :アメリカ国立標準技術研究所

6.2. GDPR関連

EUデータ保護規則(GDPR)が2018年5月に施行されてから、欧州各国のデータ保護機関による違反指摘や罰金による制裁事例増えてきています。この2018年度第4四半期は、罰金による制裁の他に具体的な行動指示や技術に対する見解、日本との相互取り組み発効が行われました。

表 15：GDPR関連イベントの一覧

No	日付	国/地域	概要
1	1/3	ポルトガル	ニュースメディアiappは、ポルトガルのデータ保護機関(CNPD[4])がGDPRに従い、Barreiro Montijo総合病院に対して、40万ユーロの罰金を科したと報じた [84]。
2	1/21	フランス	フランス国家データ保護委員会（CNIL[5]）はGDPRに従い、Googleに対して5千万ユーロの罰金を科した [85]。これは、オーストリアの非営利プライバシー保護団体「noyb」が2018年5月25日に行った、苦情申し立てを受けて始まった調査によるもの。
3	1/23	日本	日本-EU間の相互の円滑な個人データ移転を図る枠組みが発効された [86]。 これは、個人情報保護委員会が個人情報保護法第24条に基づく指定をEUに対して行い、欧州委員会がGDPR第45条に基づく十分性認定を日本に対して行うことで成立している。
4	1/24	EU	GoogleはGDPR違反による罰金について、不服を申し立てることを公表した [87]。
5	1/28	EU	欧州委員会は、GDPR施行後8カ月間で各国のデータ保護機関に寄せられたGDPR違反の指摘件数が、計95,000件以上に上ることを明らかにした [88]。
6	3/7	オランダ	オランダのデータ保護当局(DPA[6])は、ウェブサイト訪問者に対して広告目的でトラッキングされること同意を求める機能、いわゆるCookieウォールはGDPRにそぐわないとの見解を示した [89]。 これは、同意を拒否したためにWebサイトへのアクセスを拒否された多数のユーザからの苦情を受けてのこと。
7	3/26	ポーランド	ポーランドの個人データ保護局(UODO[7])はGDPRに従い、同国に支社を持つデジタルマーケティング企業Bisnode社に対して、22万ユーロの罰金を科すとともに、第14条に規定された義務による通知を受けとっていない約570万人へ3ヶ月以内に連絡を取るよう求めた [90]。

[4] Comissão Nacional de Protecção de Dados

[5] Commission Nationale de l'Informatique et des Libertés

[6] The Dutch Data Protection Authority

[7] Urzędu Ochrony Danych Osobowych

オランダの事例(No.6)でオランダのデータ保護当局(DPA)は、最近のWebサイトでよく見られるCookieウォール(図 8参照)はGDPRの要件を満たさないとの見解を示しました。Cookieウォールとは、Webサイト閲覧時に広告目的でWebサイト閲覧者の情報がトラッキングされることに対して同意を求める機能です。同意を拒否したためにWebサイトへのアクセスを拒否された多数のユーザからの苦情がDPAへ寄せられたため、ガイダンスを公表する事となりました。このガイダンスではCookieウォールに対する見解の他に、トラッキングCookieやトラッキングピクセル等の様々なトラッキングソフトウェアを使用する際には、閲覧者の許可を得ることが求められています。

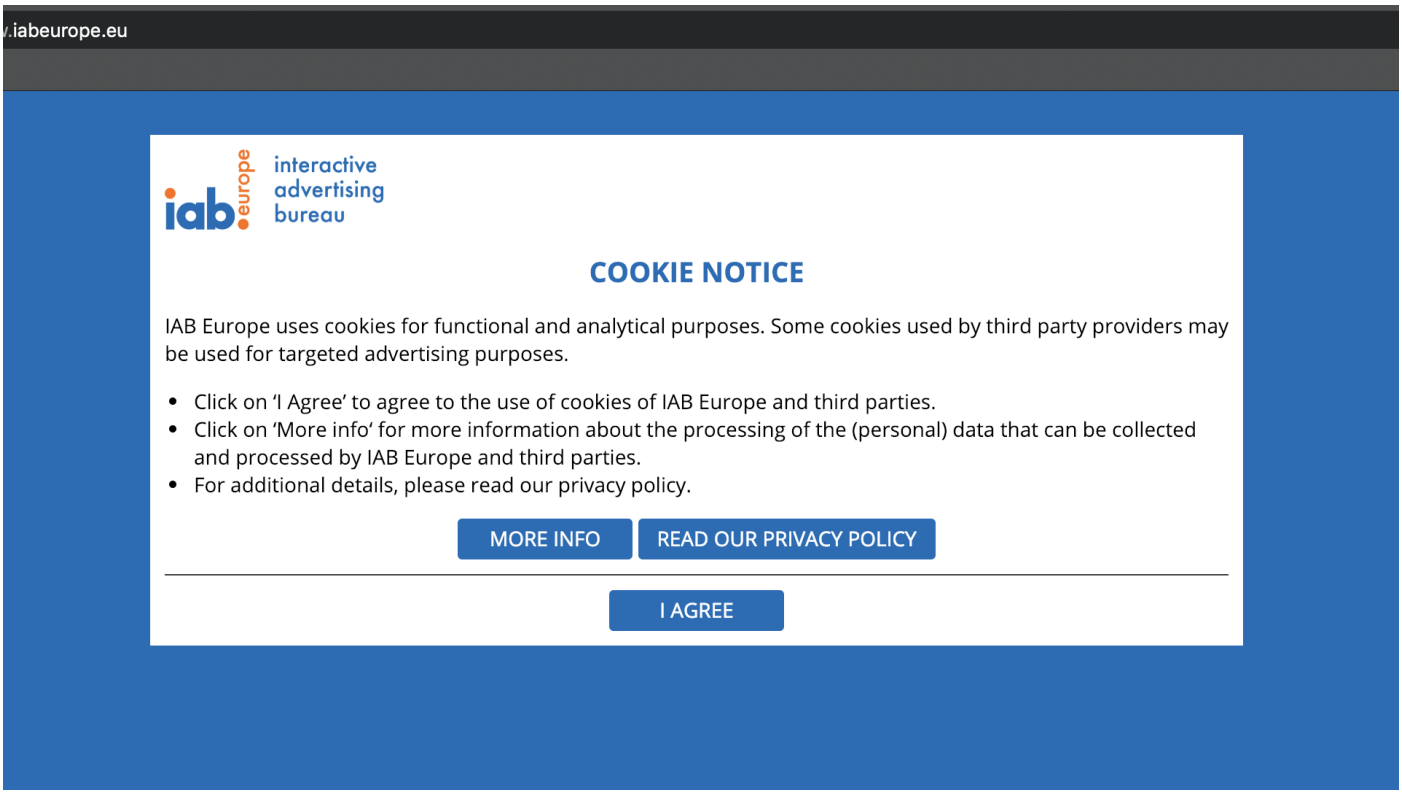


図 8:Cookieウォールの例(TechCrunch [91]より転載)

ポーランドの事例(No.7)では、スウェーデンに本社をポーランドに支社を設置しているデジタルマーケティング企業Bisnode社がGDPR第14条に規定されている通知義務を履行していないとして22万ユーロの罰金を課されています。GDPR第14条では、データ管理者が直接取得していない個人情報を使用する際は、当事者に通知することを義務付けています。本件の場合、Bisnode社は指摘後にメールアドレスが判明している約68万件にはメールにて通知しましたが、それ以外はWebサイトでの情報掲示にとどまりました [92]。これに対して、個人データ保護局(UODO)は、残りの570万件に対しても何かしらの方法で連絡を取るよう求めました。

7. 2019年度 第1四半期の予測

2019年度第1四半期（4月から6月）は、Webスキミングの被害増加、流出したアカウント情報の悪用、暗号通貨の市場価格上昇による攻撃増加があると予測します。

Webスキミングの被害増加

Webスキミングの被害は、現在も継続して発生しています。攻撃グループ「Magecart」は、グローバルでのECサイト構築用プラットフォームの利用数上位の「Magento」へWebスキミングを仕掛けました。今後、攻撃者は、同様に別の利用数上位のECサイト構築用プラットフォームを狙って不正ログインして、Webスキミングを仕掛けるおそれがあります。Webスキミングの被害は、今後も継続的に発生すると予想されます。日本では「Magento」があまり使用されていないため、2018年度第4四半期の日本国内のWebスキミングの被害は多くありませんでした。日本で普及しているECサイト構築用プラットフォーム「Color Me Shop」や「MakeShop」「eStore」などは、日本固有のECサイト構築用プラットフォームです。そのため、グローバルでのWebスキミング被害と比べて、日本国内の被害はまだ少ないと予測します。しかし日本国内での利用数が多いECサイト構築用プラットフォームの中には、グローバルで広く普及しているコンテンツ・マネジメント・システム（CMS）を使ったプラットフォームも存在します。攻撃者がそのようなCMSの脆弱性を発見した場合、日本国内のECサイト構築用プラットフォームも攻撃されてWebスキミングの被害が発生するでしょう。オンラインストアの提供者や利用者は、ECサイトの設定ミスや総当たり攻撃による不正ログインだけでなく、プラットフォームを構成するソフトウェアの脆弱性や不正コードが含まれるCMSのプラグインを悪用してWebスキミングが仕掛けられるケースにも注意が必要です。

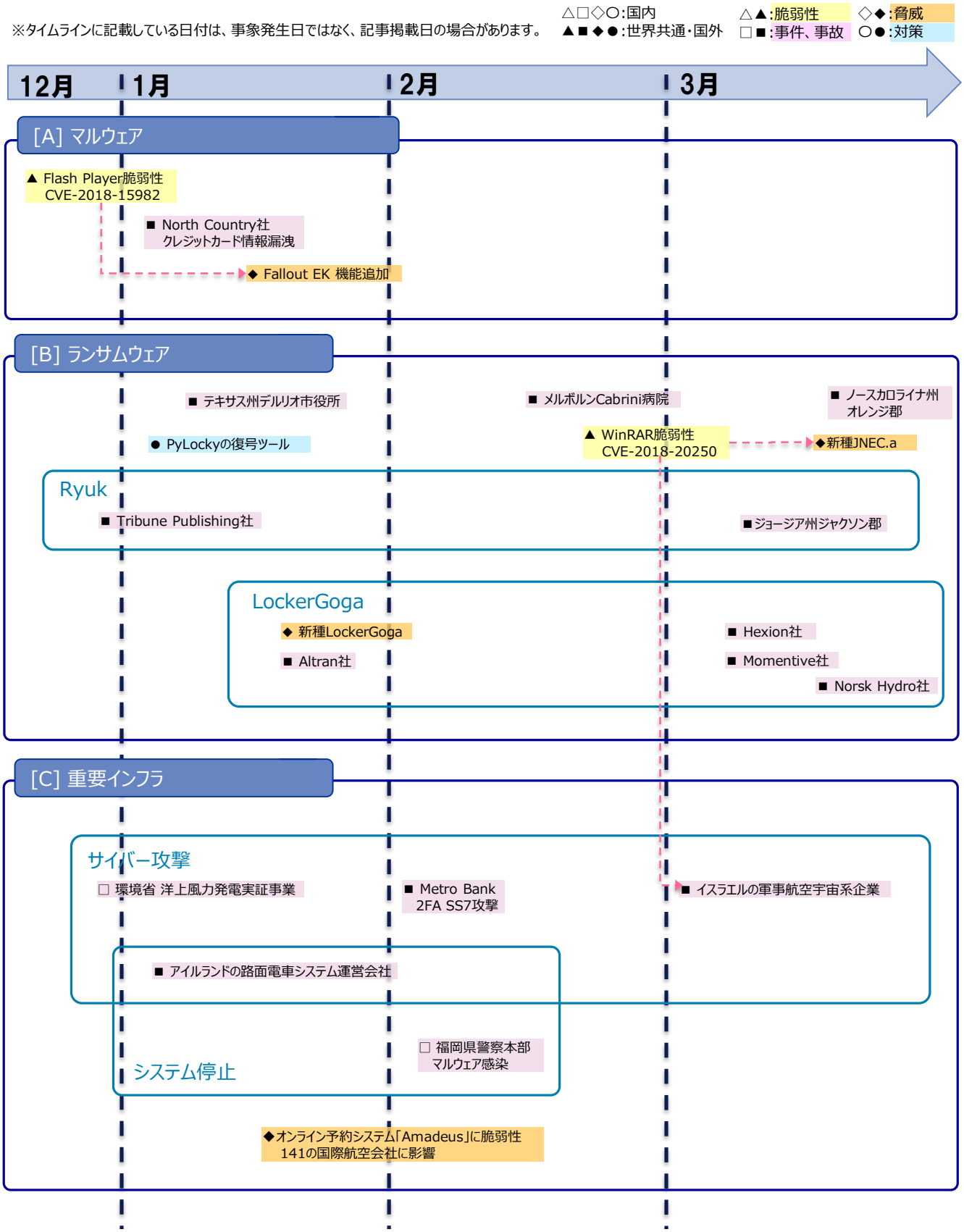
流出したアカウント情報の悪用

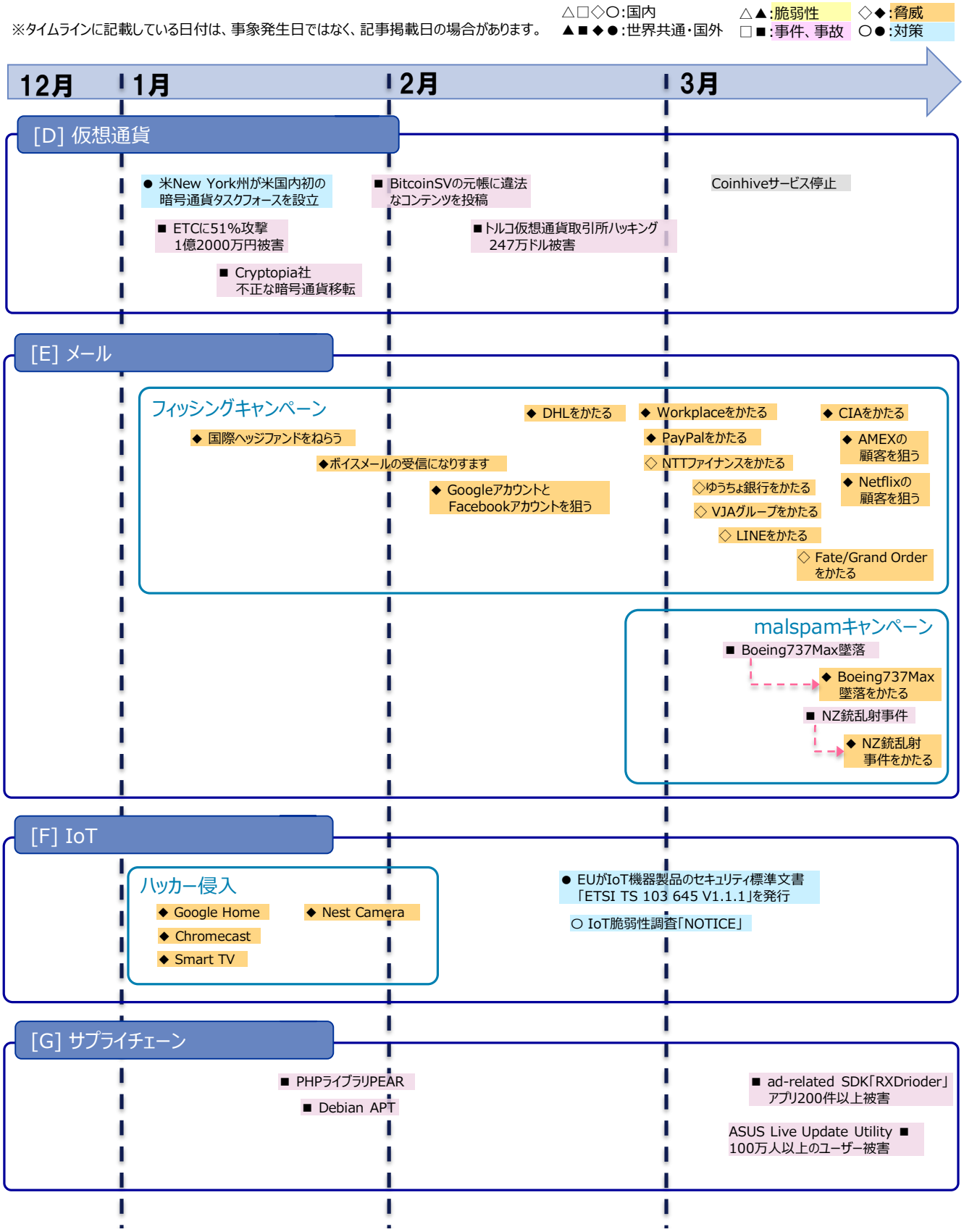
2018年度第4四半期は、膨大な件数のアカウント情報が集約された「Collection #1」などのリストが、相次いでインターネット上に公開されました。通常はダークウェブ上で秘密裏にやり取りされていたアカウント情報が、誰でも容易に取得できてしまったため、能力が低い攻撃者でも簡単にリスト型攻撃が行えます。そのため、これらの公開されたアカウント情報を悪用した攻撃が、今後多発すると予測されます。前記のWebスキミングを設置するケースにつながるおそれもあります。このようなアカウント情報が悪用されたとしても不正ログインを防ぐことができる2要素認証の利用を強く推奨します。同じパスワードを他のクラウドサービスで使い回さないことは、必須ルールです。

暗号通貨関連の攻撃増加

暗号通貨関連のインシデントの情報を収集、分析した結果、2018年度第4四半期は、暗号通貨を狙う攻撃が少なく、被害も小規模でした。これは、2018年度第3四半期のレポートで予測した通り、暗号通貨の市場価格下落により、攻撃者が暗号通貨を狙う攻撃からその他の攻撃に切り替えたためと考えます。しかし、現在暗号通貨の市場価格は再び上昇傾向にあります。したがって、2019年度第1四半期は、暗号通貨を狙う攻撃が再び増加するおそれが高いと予測します。2019年度第1四半期の攻撃は、マイニングなどのPCリソースを狙った攻撃よりも、直接、暗号通貨の窃取するために、暗号通貨の交換所などのサービス提供者やサービス利用者を狙った攻撃が増加すると予測します。暗号通貨を狙う攻撃は、これからも暗号通貨の市場価格に合わせて変化すると考えます。

8. 2018年度 第4四半期のタイムライン





※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。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件、事故

◇◆:脅威
○●:対策

12月 1月 2月 3月

[H] 情報漏洩

GDPR
○ 日EU間で十分性認定
Google5000万ユーロの罰金

● AndroidがFIDO2認定
● 「WebAuthn」ウェブ標準

◆ Dailymotion社
パスワードリスト攻撃

Facebook,何億人もののアカウントパスワードが◆
プレーンテキストで保存

□ 東京理科大学
メール3,727通

オレゴン州ヒューマンサービス部 ■
医療情報200万件

フィッシング

設定不備

mongoDB
■ 中国人履歴書
個人情報2億200万件

■ インドのデリー市民
個人情報約50万人分

■ 電子メール検証サービス
「Verifications.io」
個人情報8億900万件

■ 発信者IDアプリ「Dalil」
個人情報500万件

データベース
■ VOIPO社
VoIP電話ログ670万件
SMS/MMSメッセージログ600万件

■ UW Medicine社
個人情報974000件

■ Health Sciences Authority
個人情報80万件

■ Dow Jones社
政府高官や犯罪者情報242万件

■ Gearbest社
個人情報150万件

Elasticsearch
■ AIESEC社
個人情報400万件

■ Eskom社
個人情報

■ Mountberg Limited社
個人情報1億800万件

■ 北京机到网络科技有限公司
求職者の個人情報3300万

■ オクラホマ証券局
密情報3Tバイト

■ MedHelp社
通話録音データ

■ インドSBI銀行
口座情報100万件

※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。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件、事故

◇◆:脅威
○●:対策

12月 1月 2月 3月

[H] 情報漏洩

不正アクセス

- ■ Vision Direct社
- ■ BevMo社 個人情報1万4,500人分
- ■ Adverline「広告配信サービス」 277のeコマースサイト被害
- ■ Topps社 顧客の決済情報

Magecart

- ■ BlankMediaGames社 個人情報760万人
- ■ citrix社 機密データ6Tバイト
- ■ パキスタン政府のWebサイト サイト訪問者の入力情報
- ■ ビクトリア州政府 個人情報3万件
- □ ユニクロ 社外協力者の個人情報804件
- ■ Kathmandu社 個人情報
- □ オージス総研「宅ふぁいる便」 顧客情報480万件

Darkwebで販売

- ■ 出会い系アプリ「Coffee Meets Bagel」 個人情報600万件
- ■ Meezan Bank Joker's Stashでカード情報7万件
- ■ Collection #1を含む7つのパッケージ 個人情報4Tバイト

Gnosticplayers

- ■ 個人情報6億2,000万人分
- ■ 個人情報1億2,700万人分
- ■ 個人情報9,300万人分
- ■ 個人情報 2,650万人分

[I] 攻撃利用脆弱性

- ▲ Flash Player脆弱性 CVE-2018-15982
- ▲ systemdの複数の脆弱性 CVE-2018-16866
- ▲ Linux管理ツールapt脆弱性 CVE-2019-3462
- ▲ Cisco製ルータ脆弱性 CVE-2019-1652,CVE-2019-1653
- ▲ WordPress Plugin脆弱性 CVE-2019-6703
- ▲ Apple facetime脆弱性 CVE-2019-6223
- ▲ Apple IOKitの脆弱性 CVE-2019-7287
- ▲ Apple Foundationの脆弱性 CVE-2019-7286
- ▲ Docker runc脆弱性 CVE-2019-5736
- ▲ Drupal RCE脆弱性 CVE-2019-6340
- ▲ WinRAR脆弱性 CVE-2018-20250
- ▲ Cisco RCE脆弱性 CVE-2019-1663
- ▲ Adobe ColdFusion脆弱性 CVE-2019-7816
- ▲ Google Chrome脆弱性 CVE-2019-5786
- ▲ Windows win32k.sysドライバ脆弱性 CVE-2019-0808,CVE-2019-0797
- ▲ WordPress EasyWPSMTP脆弱性

参考文献

[1] Barracuda Networks, Inc, “2019年以降のアプリケーションセキュリティトレンド,” 14 3 2019. [オンライン]. Available: https://www.barracuda.co.jp/column/detail/964.

[2] NTT DATA Corporation, “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),” 31 10 2018. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2018/2018103101/nttdata_fy2018_2q_securityreport.pdf.

[3] NTT DATA Corporation, “グローバルセキュリティ動向四半期レポート(2018年度第3四半期),” 13 2 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2018_3q_securityreport.pdf.

[4] OXO International, Ltd., “Submitted Breach Notification,” 3 1 2019. [オンライン]. Available: https://oag.ca.gov/system/files/OXO%20International%202%20Ad%20r2fin_0.pdf.

[5] L. Abrams, “OXO Breach Involved MageCart Attack That Targeted Customer Data,” 7 1 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/oxo-breach-involved-magecart-attack-that-targeted-customer-data/.

[6] Trend Micro Incorporated, “New Magecart Attack Delivered Through Compromised Advertising Supply Chain,” 16 1 2019. [オンライン]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/.

[7] Sanguine Security, “Adminer leaks passwords; Magecart hackers rejoice,” 17 1 2019. [オンライン]. Available: https://gwillem.gitlab.io/2019/01/17/adminer-4.6.2-file-disclosure-vulnerability/.

[8] Sanguine Security, “MySQL client allows MySQL server to request any local file,” 20 1 2019. [オンライン]. Available: https://gwillem.gitlab.io/2019/01/20/sites-hacked-via-mysql-protocal-flaw/.

[9] The Topps Company, Inc., “NOTICE OF DATA BREACH,” 22 2 2019. [オンライン]. Available: https://oag.ca.gov/system/files/CustomerNotice%28US%29%282.2019%29_0.pdf.

[10] P. Paganini, “Payment data of thousands of customers of UK and US online stores could have been compromised,” 14 3 2019. [オンライン]. Available: https://securityaffairs.co/wordpress/82403/cyber-crime/payment-data-security-breach.html.

[11] Y. Klijnsma, “Consumers May Lose Sleep Over These Two New Magecart Breaches,” 20 3 2019. [オンライン]. Available: https://www.riskiq.com/blog/labs/magecart-mypillow-amerisleep/.

[12] RiskIQ, Inc, “Inside Magecart,” 13 11 2018. [オンライン]. Available: https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf.

[13] Trend Micro Incorporated., “サイバー犯罪集団「Magecart」の新しい攻撃を確認、広告配信サービスを侵害しスキミングコードを注入,” 18 1 2019. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/20150.

[14] 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/.

[15] 独立行政法人情報処理推進機構, “情報セキュリティ10大脅威2019,” 17 4 2019. [オンライン]. Available: https://www.ipa.go.jp/files/000072667.pdf.

[16] キヤノンマーケティングジャパン株式会社, “「Mac OS X」が生まれて16年――迫りつつあるマルウェアの脅威,” 13 10 2017. [オンライン]. Available: https://eset-info.canon-its.jp/malware_info/trend/detail/171013.html.

[17] キヤノンマーケティングジャパン株式会社, “2017年9月 マルウェアレポート,” 20 10 2017. [オンライン]. Available: https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1709.html#anc_02.

[18] PEAR, “PEAR公式Twitterアカウント,” 19 1 2019. [オンライン]. Available: https://twitter.com/pear/status/1086634389465956352.

[19] M. Justicz, “Remote Code Execution in apt/apt-get,” 22 1 2019. [オンライン]. Available: https://justi.cz/security/2019/01/22/apt-rce.html.

[20] Check Point Software Technologies LTD, “SimBad: A Rogue Adware Campaign On Google Play,” 13 3 2019. [オンライン]. Available: https://research.checkpoint.com/simbad-a-rogue-adware-campaign-on-google-play/.

[21] AO Kaspersky Lab, “Operation ShadowHammer,” 25 3 2019. [オンライン]. Available: https://securelist.com/operation-shadowhammer/89992/.

[22] AO Kaspersky Lab, “Kaspersky Lab、サプライチェーン攻撃手法を利用したAPT「ShadowHammer」を発見,” 29 3 2019. [オンライン]. Available: https://www.kaspersky.co.jp/about/press-releases/2019_vir29032019.

[23] AO Kaspersky Lab, “Operation ShadowHammer: a high-profile supply chain attack,” 23 4 2019. [オンライン]. Available: https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/.

[24] GMO GlobalSign K.K., “二要素認証とは,” [オンライン]. Available: https://jp.globalsign.com/service/clientcert/tfa.html.

[25] P. Duszyński, “Phishing NG. Bypassing 2FA with Modlishka.,” 2 1 2019. [オンライン]. Available: https://blog.duszynski.eu/phishing-ng-bypassing-2fa-with-modlishka/.

[26] J. Cox, “Criminals Are Tapping into the Phone Network Backbone to Empty Bank Accounts,” 1 2 2019. [オンライン]. Available: https://www.vice.com/en_us/article/mbzvxv/criminals-hackers-ss7-uk-banks-metro-bank.

[27] P. Duszyński, “GitHub - drk1wi/Modlishka: Modlishka. Reverse Proxy.,” 31 1 2019. [オンライン]. Available: https://github.com/drk1wi/Modlishka/.

[28] P. Duszyński, “Phishing with Modlishka (bypass 2FA) on Vimeo,” 29 12 2018. [オンライン].

Available: https://vimeo.com/308709275.

[29] Security Affairs, “SS7 flaw allows hackers to spy on every conversation,” 15 8 2015. [オンライン]. Available: http://securityaffairs.co/wordpress/39409/cyber-crime/ss7-flaw-surveillance.html.

[30] Süddeutsche Zeitung Digitale Medien GmbH / Süddeutsche Zeitung GmbH, “Schwachstelle im Mobilfunknetz: Kriminelle Hacker räumen Konten leer,” 3 5 2017. [オンライン]. Available: https://www.sueddeutsche.de/digital/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504.

[31] T. Hunt, “The 773 Million Record "Collection #1" Data Breach,” 17 1 2019. [オンライン]. Available: https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/.

[32] K. o. Security, “773M Password ‘Megabreach’ is Years Old,” 17 1 2019. [オンライン]. Available: https://krebsonsecurity.com/2019/01/773m-password-megabreach-is-years-old/.

[33] RECORDED FUTURE, “Threat Actor Behind Collection #1 Data Breach Identified,” 1 2 2019. [オンライン]. Available: https://www.recordedfuture.com/collection-1-data-breach/.

[34] Soliton Systems, “約27億件の巨大漏洩ファイル「Collection#1」における日本の被害を特定,” 21 2 2019. [オンライン]. Available: https://www.soliton.co.jp/news/2019/003509.html.

[35] HackenProof, “No more privacy: 202 Million private resumes exposed,” 10 1 2019. [オンライン]. Available: https://blog.hackenproof.com/industry-news/202-million-private-resumes-exposed.

[36] ZDNet, “Online casino group leaks information on 108 million bets, including user details,” 21 1 2019. [オンライン]. Available: https://www.zdnet.com/article/online-casino-group-leaks-information-on-108-million-bets-including-user-details/.

[37] オージス総研, “宅ふぁいる便」サービスにおける不正アクセスについて　～お客さま情報の漏洩について（お詫びとご報告）～,” 14 3 2019. [オンライン]. Available: 宅ふぁいる便」サービスにおける不正アクセスについて　～お客さま情報の漏洩について（お詫びとご報告）～.

[38] ZDNet, “ハッカーが約2カ月で10億件に迫るユーザー情報をダークウェブで公開の恐れ,” 16 4 2019. [オンライン]. Available: https://japan.zdnet.com/article/35135809/.

[39] B. DIACHENKO, “800+ Million Emails Leaked Online by Email Verification Service,” 7 3 2019. [オンライン]. Available: https://securitydiscovery.com/800-million-emails-leaked-online-by-email-verification-service/.

[40] Citrix, “Citrix provides update on unauthorized internal network access,” 4 4 2019. [オンライン]. Available: https://www.citrix.com/blogs/2019/04/04/citrix-provides-update-on-unauthorized-internal-network-access/.

[41] C. P. Research, “Extracting a 19 Year Old Code Execution from WinRAR,” 20 2 2019. [オンライン]. Available: https://research.checkpoint.com/extracting-code-execution-from-winrar/.

[42] 360威胁情报中心, “Warning! Upgrades in WinRAR Exploit with Social Engineering and Encryption,” 27 2 2019. [オンライン]. Available: https://ti.360.net/blog/articles/upgrades-in-winrar-

exploit-with-social-engineering-and-encryption/.

[43] tenable, “Multiple Zero-Day Vulnerabilities Discovered by Tenable Research in Building Access Technology,” 14 1 2019. [オンライン]. Available: https://www.tenable.com/press-releases/multiple-zero-day-vulnerabilities-discovered-by-tenable-research-in-building-access.

[44] TechCrunch, “Researcher shows how popular app ES File Explorer exposes Android device data,” 16 1 2019. [オンライン]. Available: https://techcrunch.com/2019/01/16/android-app-es-file-explorer-expose-data/.

[45] BAD PACKETS REPORT, “Over 9,000 Cisco RV320/RV325 routers are vulnerable to CVE-2019-1653,” 26 1 2019. [オンライン]. Available: https://badpackets.net/over-9000-cisco-rv320-rv325-routers-vulnerable-to-cve-2019-1653/.

[46] Defiant, “WordPress Sites Compromised via Zero-Day Vulnerabilities in Total Donations Plugin,” 25 1 2019. [オンライン]. Available: https://www.wordfence.com/blog/2019/01/wordpress-sites-compromised-via-zero-day-vulnerabilities-in-total-donations-plugin/.

[47] Apple, “About the security content of iOS 12.1.4 - Apple Support,” 7 2 2019. [オンライン]. Available: https://support.apple.com/en-us/HT209520.

[48] Google Project Zero, “1726 - XNU_ copy-on-write behavior bypass via mount of user-owned filesystem image - project-zero - Monorail,” 1 12 2018. [オンライン]. Available: https://bugs.chromium.org/p/project-zero/issues/detail?id=1726&q=.

[49] ZDNet, “Doomsday Docker security hole uncovered,” 11 2 2019. [オンライン]. Available: https://www.zdnet.com/article/doomsday-docker-security-hole-uncovered/.

[50] LAC, “【注意喚起】CMSのDrupal 、RCEで危険度の高い脆弱性(CVE-2019-6340)。至急、最新版への更新を,” 25 2 2019. [オンライン]. Available: https://www.lac.co.jp/lacwatch/alert/20190225_001779.html.

[51] Adobe, “Security updates available for ColdFusion | APSB19-14,” 1 3 2019. [オンライン]. Available: https://helpx.adobe.com/security/products/coldfusion/apsb19-14.html.

[52] Google, “Stable Channel Update for Desktop,” 1 3 2019. [オンライン]. Available: https://chromereleases.googleblog.com/2019/03/stable-channel-update-for-desktop.html.

[53] tenable, “Use-After-Free Vulnerability in Google Chrome Exploited In The Wild (CVE-2019-5786),” 6 3 2019. [オンライン]. Available: https://www.tenable.com/blog/use-after-free-vulnerability-in-google-chrome-exploited-in-the-wild-cve-2019-5786.

[54] Microsoft, “CVE-2019-0797 | Win32k Elevation of Privilege Vulnerability,” 12 3 2019. [オンライン]. Available: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0797.

[55] Microsoft, “CVE-2019-0808 | Win32k Elevation of Privilege Vulnerability,” 12 3 2019. [オンライン]. Available: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0808.

[56] Melon Security, “Emotet: A Small Change in Tactics Leads to a Spike in Attacks,” 12 2 2019. [オン

ライン]. Available: https://www.menlosecurity.com/blog/emotet-a-small-change-in-tactics-leads-to-a-spike-in-attacks.

[57] Check Point Research, “SpeakUp: A New Undetected Backdoor Linux Trojan,” 4 2 2019. [オンライン]. Available: https://research.checkpoint.com/speakup-a-new-undetected-backdoor-linux-trojan/.

[58] Cisco Talos, “Cisco AMP tracks new campaign that delivers Ursnif,” 24 1 2019. [オンライン]. Available: https://blog.talosintelligence.com/2019/01/amp-tracks-ursnif.html.

[59] TREND MICRO, “「顔文字」、「LoveYou」スパムの背後に凶悪スパムボット、ランサムウェア遠隔攻撃も実行,” 22 2 2019. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/20392.

[60] BLEEPING COMPUTER, “New Astaroth Trojan Variant Exploits Anti-Malware Software to Steal Info,” 13 2 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/new-astaroth-trojan-variant-exploits-anti-malware-software-to-steal-info/.

[61] Carbon Black, “TAU Threat Intelligence Notification: New macOS Malware Variant of Shlayer (OSX) Discovered,” 12 2 2019. [オンライン]. Available: https://www.carbonblack.com/2019/02/12/tau-threat-intelligence-notification-new-macos-malware-variant-of-shlayer-osx-discovered/.

[62] TG Soft, “21/02/2019 14:48:47 - Operazione Pistacchietto: Spyware italiano attivo dal 2016 si diffonde attraverso la piattaforma di GitHub,” 21 2 2019. [オンライン]. Available: https://www.tgsoft.it/italy/news_archivio.asp?id=987.

[63] McAfee, “Happy New Year 2019! Anatova is here!,” 22 1 2019. [オンライン]. Available: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/happy-new-year-2019-anatova-is-here/.

[64] BLEEPING COMPUTER, “Jokeroo Ransomware-as-a-Service Offers Multiple Membership Packages,” 5 3 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/jokeroo-ransomware-as-a-service-offers-multiple-membership-packages/.

[65] BLEEPING COMPUTER, “CryptoMix Clop Ransomware Says It's Targeting Networks, Not Computers,” 5 3 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/cryptomix-clop-ransomware-says-its-targeting-networks-not-computers/.

[66] BLEEPING COMPUTER, “JNEC.a Ransomware Spread by WinRAR Ace Exploit,” 18 3 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/jneca-ransomware-spread-by-winrar-ace-exploit/.

[67] BLEEPING COMPUTER, “Yatron Ransomware Plans to Spread Using EternalBlue NSA Exploits,” 12 3 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/yatron-ransomware-plans-to-spread-using-eternalblue-nsa-exploits/.

[68] Trend Micro, “暗号化型ランサムウェア「LockerGoga」について解説,” 8 4 2019. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/20840.

[69] BLEEPING COMPUTER, “GandCrab Operators Use Vidar Infostealer as a Forerunner,” 7 1 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/gandcrab-operators-use-vidar-infostealer-as-a-forerunner/.

[70] Unit 42, “Mac Malware Steals Cryptocurrency Exchanges’ Cookies,” 31 1 2019. [オンライン]. Available: https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/?fbclid=IwAR1q6bzf0Mz_9vyzRUMH6irpNGaKXN3n2A00F1nP11AL6YTFrh57zUg9Z-I.

[71] avast, “Spoofing in the reeds with Rietspoof,” 19 2 2019. [オンライン]. Available: https://blog.avast.com/rietspoof-malware-increases-activity.

[72] Trend Micro, “「Trickbot」がリモートデスクトップアプリの認証情報を窃取する機能を追加,” 18 2 2019. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/20375.

[73] Trend Micro, “サイネージTVとプレゼンテーションシステムを狙う「Mirai」の新しい亜種を確認,” 26 3 2019. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/20709.

[74] Kaspersky Lab, “ATM robber WinPot: a slot machine instead of cutlets,” 19 2 2019. [オンライン]. Available: https://securelist.com/atm-robber-winpot/89611/?utm_source=kdaily&utm_medium=blog&utm_campaign=jp_kd_Ex0124_organic&utm_content=link&utm_term=jp_kdaily_organic_Ex0124_link_blog_kd.

[75] U.S. Department of Defense, “DARPA Explores New Computing Architectures to Deliver Verifiable Data Assurances,” 16 1 2019. [オンライン]. Available: https://www.darpa.mil/news-events/2019-01-16.

[76] American Institute of Physics, “Office of Critical Technologies and Security Act - H.R.618 / S.29,” 16 1 2019. [オンライン]. Available: https://www.aip.org/fyi/federal-science-bill-tracker/116th/office-critical-technologies-and-security-act.

[77] U.S. Department of Justice, “Justice Department Announces Court-Authorized Efforts to Map and Disrupt Botnet Used by North Korean Hackers,” 30 1 2019. [オンライン]. Available: https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-efforts-map-and-disrupt-botnet-used-north.

[78] delmarva now., “Ransomware attacks would become felony with Maryland bill,” 15 2 2019. [オンライン]. Available: https://www.delmarvanow.com/story/news/local/maryland/2019/02/15/ransomware-attacks-would-become-felony-maryland-bill/2869037002/.

[79] National Institute of Information and Communications Technology, “IoT機器調査及び利用者への注意喚起の取組「NOTICE」の実施,” 1 2 2019. [オンライン]. Available: https://www.nict.go.jp/press/2019/02/01-1.html.

[80] BBC., “Russia bans smartphones for soldiers over social media fears,” 20 2 2019. [オンライン]. Available: https://www.bbc.com/news/world-europe-47302938.

[81] E Hacking News., “Soon DNS to protect users from malware,” 24 2 2019. [オンライン]. Available: https://www.ehackingnews.com/2019/02/soon-dns-to-protect-users-from-malware.html.

[82] European Union Agency for Law, “Law enforcement agencies across the EU prepare for major cross-border cyber-attacks,” 18 3 2019. [オンライン]. Available: https://www.europol.europa.eu/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks.

[83] National Institute of Standards and Technology, “Security Strategies for Microservices-based Application Systems: Draft NIST SP 800-204 Available for Comment,” 25 3 2019. [オンライン]. Available: https://csrc.nist.gov/news/2019/nist-releases-draft-sp-800-204-for-public-comment.

[84] International Association of Privacy Professionals., “First GDPR fine in Portugal issued against hospital for three violations,” 3 1 2019. [オンライン]. Available: https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/.

[85] Commission Nationale de l'Informatique et des Libertés, “The CNIL’s restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC,” 21 1 2019. [オンライン]. Available: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

[86] Personal Information Protection Commission, Government of Japan., “日EU間の相互の円滑な個人データ移転を図る枠組み発効,” 23 1 2019. [オンライン]. Available: https://www.ppc.go.jp/enforcement/cooperation/cooperation/310123/.

[87] CBS Interactive Inc., “Google appeals $57M GDPR fine, defends privacy practices,” 24 1 2019. [オンライン]. Available: https://www.cnet.com/news/google-appeals-57m-gdpr-fine-defends-privacy-practices/.

[88] European Commission, “Joint Statement by First Vice-President Timmermans, Vice-President Ansip, Commissioners Jourová and Gabriel ahead of Data Protection Day,” 25 1 2019. [オンライン]. Available: http://europa.eu/rapid/press-release_STATEMENT-19-662_en.htm.

[89] Dutch Data Protection Authority, “Websites moeten toegankelijk blijven bij weigeren tracking cookies,” 7 3 2019. [オンライン]. Available: https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies.

[90] The President of the Personal Data Protection Office, “The first fine imposed by the President of the Personal Data Protection Office,” 26 3 2019. [オンライン]. Available: https://uodo.gov.pl/en/553/1009.

[91] Verizon Media, “Cookie walls don't comply with GDPR, says Dutch DPA,” 8 3 2019. [オンライ

ン]. Available: https://techcrunch.com/2019/03/08/cookie-walls-dont-comply-with-gdpr-says-dutch-dpa/.

[92] Bisnode Polska sp. z. o.o., “Decision of UODO (Polish DPA) - Bisnode statement,” [オンライン]. Available: https://www.bisnode.pl/wiedza/newsy-artykuly/decyzja-urzedu-ochrony-danych-osobowych-w-sprawie-bisnode/.

NTT DATA
Trusted Global Innovator

2019年5月30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