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

2021 年度 第 1 四半期

NTT DATA
Trusted Global Innovator

目次

1.エグゼグティブサマリー

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

EC-CUBEのクロスサイトスクリプティング脆弱性

2021年5月に、株式会社イーシーキューブは複数のクロスサイトスクリプティング脆弱性を公開しました。複数の脆弱性のうち、すでに2つの脆弱性を悪用したStored XSS攻撃が確認されています。攻撃者は、ECサイトの入力フォームへ不正スクリプトを入力してデータベース内へ格納し、管理者が管理画面を操作したときに、これらの脆弱性を悪用して当該不正スクリプトを実行することができます。その結果、攻撃者は認証情報を窃取したり、遠隔操作できるWebShellを設置してクレジットカード情報を窃取したりするおそれがあります。EC-CUBEを利用したECサイトの管理者や開発者に対して、迅速な更新プログラムの適用や、攻撃と被害の確認を提案します。

メルカリ社へのソフトウェア・サプライチェーン攻撃

フリマアプリ「メルカリ」を運営する株式会社メルカリは、2021年5月、第三者からの不正アクセスにより、同社の顧客情報等が外部に流出したことを公表しました。本事件の特徴は、攻撃者がソフトウェア・サプライチェーン攻撃を仕掛けて、段階的に複数のシステムへ侵入している点です。本稿では、攻撃者がどのようにしてシステムへ侵入できたのか、また開発環境への侵入を防ぐためには、どのような対策を講じるべきか解説します。

情報漏えい

ネットマーケティング株式会社は、恋愛や婚活を支援するマッチングアプリ「Omiai」を管理するサーバへ不正アクセスがあり、最大で171万1756人分の運転免許証や健康保険証、パスポート、マイナンバーカードの画像データが流出したと発表しました。本稿では、eKYCを使った本人確認方法の信頼性の観点にもとづいて、大量の身分証明書の画像の流出による社会的な影響を解説します。

予測

サイバー攻撃を行った攻撃グループやその犯罪に関与した国家に対して、被害国が名指しで批判を行う動きがあります。この動きにより、国家に支援されている攻撃グループは、関係する国家の特定を防ぐため、身元が特定される情報をより隠すようになると考えられます。

また、新型コロナウイルスの流行状況に合わせたサイバー攻撃が発生するおそれがあります。新型コロナウイルスが再流行し、ワクチン接種が再度必要になる場合には、ワクチン接種に関する情報を悪用したフィッシング攻撃が再び発生するでしょう。一方で、現状のままアフターコロナに移行した場合には、製薬会社やヘルスケア産業を狙った攻撃、レジャーに関連したフィッシング攻撃、新しいビジネスや投資を狙った攻撃等、アフターコロナにおいてお金がある箇所を狙う攻撃が発生すると想定されます。

2.注目トピック

2.1. EC-CUBEのクロスサイトスクリプティング脆弱性

トレンドマイクロは、2021年4月28日（米国時間）に「不正注文」でオンラインショップを侵害する攻撃キャンペーン「Water Pamola」のブログを発表しました [1]。同社は、2019年以降、「Water Pamola」と名付けた攻撃キャンペーンを追跡していました。Water Pamolaは、当初、不正な添付ファイルを含むスパムメールを介して、日本、オーストラリア、ヨーロッパ諸国のオンラインショップを侵害しました。しかし、2020年初頭からWater Pamolaの攻撃活動が変わり、スパムメールの代わりに、図 1のように不正なスクリプトを利用してクロスサイトスクリプティング攻撃を行っています。不正なスクリプトによる被害者は、主に日本国内です。そのため、Water Pamolaは、日本国内のオンラインショップを狙っていると推測できます。

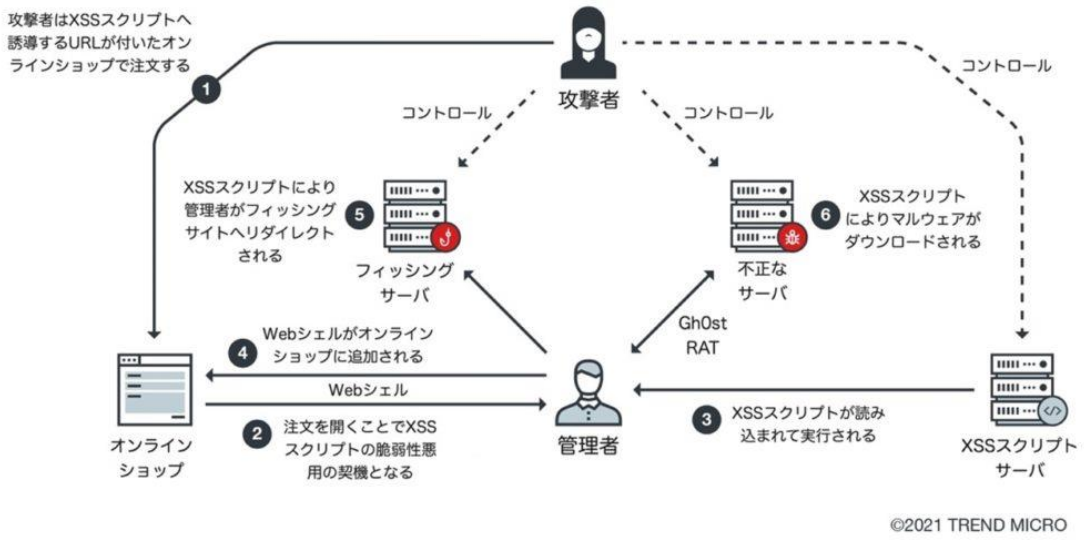


図 1 ： Water Pamolaの攻撃フロー [1]

2021年に侵害されたECサイトを調査した結果 [2]、不正アクセスによるクレジットカード情報漏洩事件が35件ありました。その35件のECプラットフォームを図 2に示します。多くのECサイト構築に利用されるEC-CUBEは攻撃者に狙われているおそれがあると推測しています。

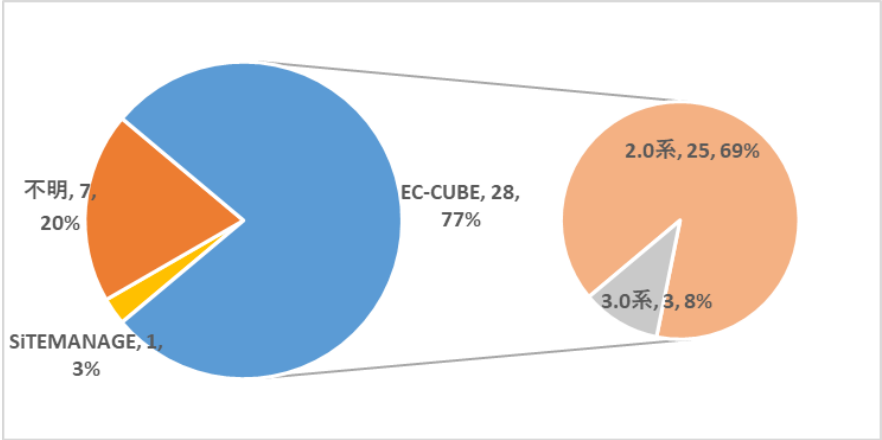


図 2 ： 侵害されたECサイトのプラットフォーム名とバージョン

本稿では、2021年5月以降、新たに公開されたEC-CUBEの脆弱性を取り上げて、EC-CUBEの脆弱性や脆弱性を悪用した攻撃方法の詳細を説明します。さらに、EC-CUBEを利用しているECサイト管理者のセキュリティ対策も提案します。

2.1.1. EC-CUBEの脆弱性

（1） EC-CUBE 本体の脆弱性

2021年5月7日、株式会社イーシーキューブから、EC-CUBEのクロスサイトスクリプティングの脆弱性（CVE-2021-20717） [3]に関する注意喚起が公開されました [4]。同月10日、JPCERT/CCからも同一脆弱性に関する注意喚起が公開されました [5]。脆弱性情報は、表 1にまとめました。

攻撃者は、当該脆弱性を悪用して、特定の入力欄に不正なスクリプトを入力します。ECサイトの管理者が特定の管理画面操作をする際に、攻撃者が入力した不正なスクリプトが実行されます。不正なスクリプトが実行された場合、攻撃が成功して、攻撃者がECサイトへ不正アクセスしたり、クレジットカード情報を窃取したりするおそれがあります。株式イーシーキューブによると、すでに当該脆弱性を悪用した攻撃が複数確認されています。

表 1 ： 脆弱性(CVE-2021-20717)情報 [6]

公開日	2021年5月7日
CVE番号	CVE-2021-20717
CVSSスコア	6.1
CVSSメトリクス	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
影響を受ける製品	EC-CUBE 4.0.0 から 4.0.5 まで
脆弱性の種類	クロスサイトスクリプティング（Stored XSS）

さらに、2021年6月10日に、株式会社イーシーキューブから、EC-CUBEのクロスサイトスクリプティングの脆弱性（CVE-2021-20750、CVE-2021-20751） [7] [8]が公開されました。脆弱性情報は、表 2、表 3にまとめました。

脆弱性CVE-2021-20750とCVE-2021-20751は、どちらもReflected XSSの脆弱性です。攻撃者は、ECサイトの管理者またはユーザを偽サイトへ誘導して特定の操作を実施させます。脆弱性があるEC-CUBEが使われるサイトにおいて、管理者またはユーザが特定の操作を実施すると、管理者またはユーザのウェブブラウザ上で不正なスクリプトが実行されます。攻撃が成功すると、攻撃者はユーザのウェブブラウザからCookieを窃取したり、HTMLタグを使った入力フォームでクレジットカード情報または認証情報を収集したりするおそれがあります。

表 2 ： 脆弱性(CVE-2021-20750)情報 [9]

公開日	2021年6月10日
CVE番号	CVE-2021-20750
CVSSスコア	6.1
CVSSメトリクス	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
影響を受ける製品	・EC-CUBE 3.0.0 から 3.0.18-p2 まで ・EC-CUBE 4.0.0 から 4.0.5-p1 まで
脆弱性の種類	クロスサイトスクリプティング（Reflected XSS）

表 3 ： 脆弱性(CVE-2021-20751)情報 [9]

公開日	2021年6月10日
CVE番号	CVE-2021-20751
CVSSスコア	6.1
CVSSメトリクス	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
影響を受ける製品	EC-CUBE 4.0.0 から 4.0.5-p1 まで
脆弱性の種類	クロスサイトスクリプティング（Reflected XSS）

（2） EC-CUBE プラグインの脆弱性

2021年6月15日に、JPCERT/CCから、EC-CUBE3.0系用の複数のプラグインにおけるクロスサイトスクリプティングの脆弱性に関する注意喚起が公開されました [10]。脆弱性情報を表 4、表 5、表 6、表 7にまとめました。

脆弱性CVE-2021-20735とCVE-2021-20742は、どちらもStored XSSの脆弱性です。この脆弱性を悪用した場合、攻撃者が、EC-CUBEの受注画面上の入力欄へ受注情報の代わりに不正なスクリプトを入力して、EC-CUBEの注文データベースへ保存しておきます。EC-CUBEの管理者が、配送伝票番号プラグインなどのEC-CUBEの特定のプラグインの管理画面を操作すると、注文データベースから受注情報と同様に不正なスクリプトも読み出されて、管理者のウェブブラウザで処理されます。不正なスクリプトが実行します。また、JPCERT/CCによると、すでに脆弱性CVE-2021-20735を悪用した攻撃が確認されています。

表 4 ： 脆弱性(CVE-2021-20735)情報 [11]

公開日	2021年6月15日
CVE番号	CVE-2021-20735
CVSSスコア	6.1
CVSSメトリクス	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
影響を受ける製品	・配送伝票番号プラグイン(3.0系) 1.0.10 およびそれ以前のバージョン ・配送伝票番号csv一括登録プラグイン(3.0系) 1.0.8 およびそれ以前のバージョン ・配送伝票番号メールプラグイン(3.0系) 1.0.8 およびそれ以前のバージョン
脆弱性種類	クロスサイトスクリプティング（Stored XSS）

表 5 ： 脆弱性(CVE-2021-20742)情報 [12]

公開日	2021年6月15日
CVE番号	CVE-2021-20742
CVSSスコア	6.1
CVSSメトリクス	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
影響を受ける製品	・EC-CUBE 3.0 用プラグイン「帳票出力プラグイン」 バージョン1.0.1 より前のバージョン （EC-CUBE 3.0.0 から 3.0.8 の環境でのみ）
脆弱性種類	クロスサイトスクリプティング（Stored XSS）

それに対して、脆弱性CVE-2021-20743とCVE-2021-20744は、Reflected XSSの脆弱性です。攻撃者は、事前に細工したページを用意し、ユーザまたは管理者を当該ページに誘導し、特定の操作を実行させます。すると、脆弱性があるEC-CUBEの特定のプラグインを利用したユーザまたは管理者のウェブブラウザ上で、不正なスクリプトが実行されます。攻

撃が成功した場合、フィッシングサイトへアクセスしたり、偽サイトから不正プログラムをダウンロードし自社環境を感染したりする恐れがあります。

表 6 ： 脆弱性(CVE-2021-20743)情報 [12]

公開日	2021年6月15日
CVE番号	CVE-2021-20743
CVSSスコア	6.1
CVSSメトリクス	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
影響を受ける製品	・EC-CUBE 3.0 用プラグイン「メルマガ管理プラグイン」バージョン1.0.4 より前のバージョン （EC-CUBE 3.0.0 から 3.0.8 の環境でのみ）
脆弱性種類	クロスサイトスクリプティング（Reflected XSS）

表 7 ： 脆弱性(CVE-2021-20744)情報 [12]

公開日	2021年6月15日
CVE番号	CVE-2021-20744
CVSSスコア	6.1
CVSSメトリクス	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
影響を受ける製品	・EC-CUBE 3.0 用プラグイン「カテゴリコンテンツプラグイン」バージョン1.0.1 より前のバージョン （EC-CUBE 3.0.0 から 3.0.8 の環境でのみ）
脆弱性の種類	クロスサイトスクリプティング（Reflected XSS）

2.1.2. Reflected XSSとStored XSS

2.1.1で述べたEC-CUBEに関する複数の脆弱性は、Reflected XSS（反射型）とStored XSS（蓄積型）の2種類のクロスサイトスクリプティングの脆弱性でした。それぞれ、攻撃手口が異なります。以下で、Reflected XSSとStored XSSを説明します。

クロスサイトスクリプティング（XSS）の脆弱性は、図 3のようにReflected XSS（反射型）、Stored XSS（蓄積型）とDOM Based XSS（DOM型）の3種類に分類できます。

図 3 ： XSSの種類 [13]

典型的なReflected XSSは、攻撃者が偽サイトを用意します。まず攻撃者は、不正なスクリプトを含んだ偽サイトを設置します。つぎに、ターゲットのユーザへ、偽サイトのURLを含んだメールを送って、そのユーザを偽サイトへ誘導します。ユーザは、偽サイトへアクセスすると、不正なスクリプトがレスポンスとしてユーザへ送信され、ユーザのウェブブラウザ上で実行されます。実行された不正スクリプトが、ブラウザからCookie情報や認証情報を窃取します。

それに対して、Stored XSSは、図 4のように攻撃者が、不正なスクリプトを含んだ文字列をWebサーバへ送信します。すると、その文字列がWebサーバ内やデータベースへ格納されます。そして、ユーザが当該Webサイトへアクセスした時に、Webサーバやデータベースに格納された文字列が出力されます。その時、文字列の出力処理や表示処理に脆弱性が存在するため、文字列が不正なスクリプトとしてブラウザ上で実行されます。この不正なスクリプトが、マルウェアなどをダウンロードしてユーザのマシンで実行します。

Reflected XSSは、攻撃者から届いたフィッシングメールなどに気づき、その誘導に引っかからなければ、不審なURLへアクセスしてReflected XSSの被害を受ける心配がありません。しかし、Stored XSSの場合は、フィッシングメールなどの不審なイベントがありません。ユーザは、通常通りにWebサイトの情報を表示するだけで、ユーザのブラウザ上で不正なスクリプトが自動実行されます。Stored XSSは、ウェブブラウザ上の画面遷移などがない、より隠ぺいされた攻撃手法のため、不正なスクリプトの実行を発見しにくく、被害が拡大しやすいと考えられます。

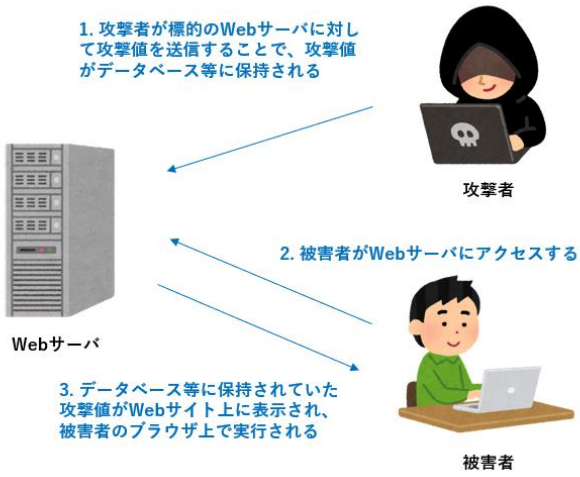


図 4 ： Stored XSSの攻撃フロー [14]

2.1.3. EC-CUBE脆弱性を悪用した攻撃事例の解説

2.1で述べたように、トレンドマイクロは、ECサイトへクロスサイトスクリプティング攻撃を行っているWater Pamolaの攻撃活動を発見しました。JPCERT/CCも、類似した攻撃を複数確認しています。2021年7月6日に、JPCERT/CCは、EC-CUBEの脆弱性CVE-2021-20717、およびCVE-2021-20735 を悪用した攻撃の解説ブログを公開しました [15]。EC-CUBEの脆弱性（CVE-2021-20717、CVE-2021-20735）に対するXSS攻撃の流れを図 5に示します。

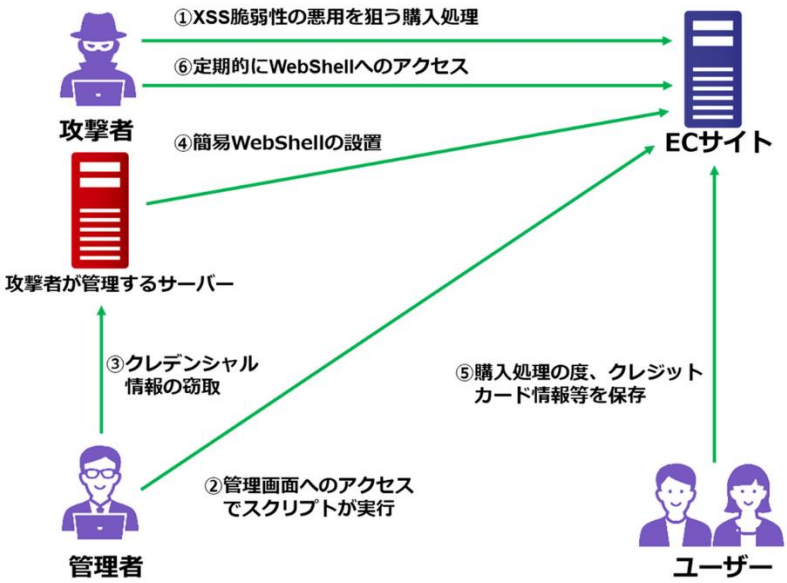


図 5 ： XSS攻撃の流れ [15]

攻撃者は、脆弱性があるEC-CUBEで作成されたECサイトの注文フォームに対して、図 6に示す不正なスクリプトを含んだ文字列を入力して、購入処理を実行します（図 5の①）。通常は、文字列に不正なスクリプトが含まれていても、そのスクリプトを誤って実行しないよう無害化処理を行いますが、脆弱性CVE-2021-20717が存在するEC-CUBE4.0系を利用したサイトは、無害化処理が無効化されているため、不正なスクリプトを含んだ文字列が、そのままにEC-CUBEのデータベースに保存されます。

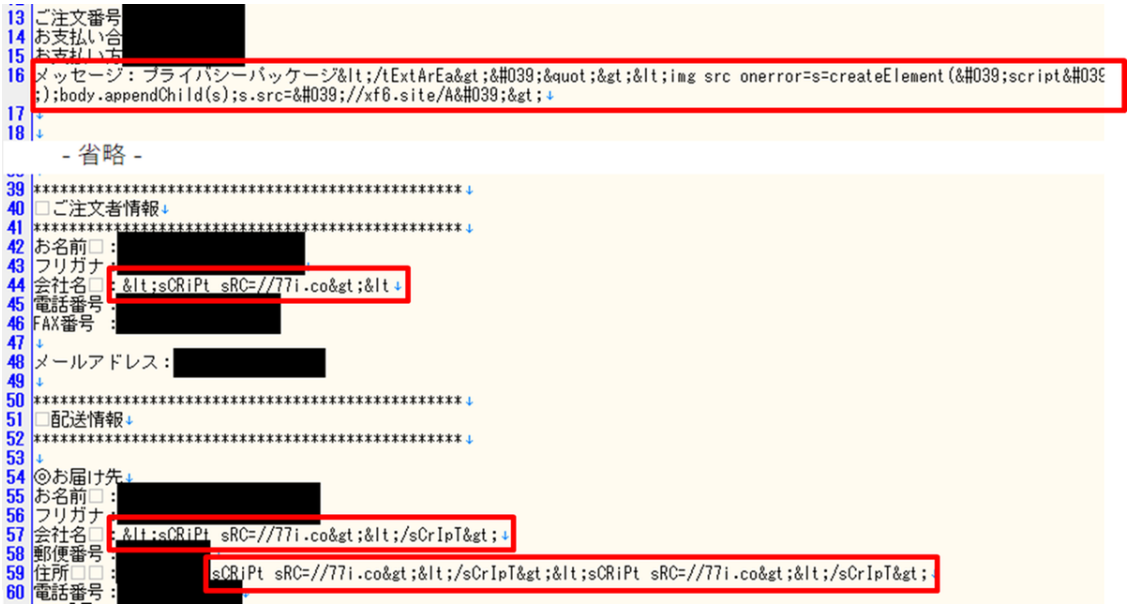


図 6 ： 複数の入力欄におけるXSSを狙った注文内容 [15]

つぎにECサイトの管理者が、EC-CUBEの管理画面へアクセスして、注文内容を表示します（図 5の②）。すると、EC-CUBEのデータベースから不正なスクリプトを含んだ文字列が読み出され、管理画面上にスクリプトとして表示されます。

無害化処理が実装されたEC-CUBE3.0系のプラグインを利用するサイトも、この脆弱性が存在する場合があります。EC-CUBE3.0系の特定のプラグインの処理にhtml_entity_decode関数が使われているため、無害化処理された文字列をスクリプトとして実行可能なもとの不正な文字列へ戻して、ウェブブラウザへ出力します。その結果、ECサイトの管理者が、該当するプラグインの機能で通常通りに管理画面で注文を閲覧すると、管理者のマシン上で不正なスクリプトが実行されます。攻撃者の不正なスクリプトが、管理者の認証情報を窃取して、攻撃者の管理サーバへ送信します。そして、攻撃者は、窃取した認証情報を使ってECサイトへ不正ログインして、WebShellを設置します（図 5の③、④）。設置されたWebShellが発見されて駆除されるまで、攻撃者はWebShellを通じてECサイトを遠隔操作して、図 7のようにクレジットカード情報を窃取します。（図 5の⑤、⑥）

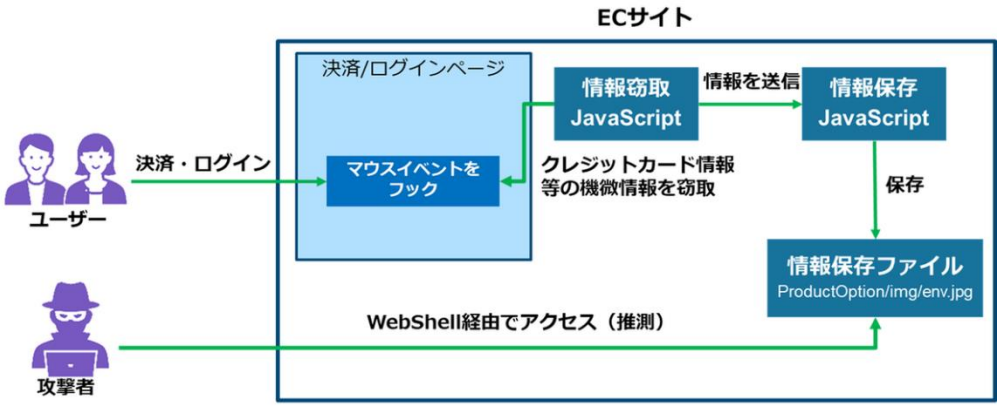


図 7 ： クレジットカード情報等を窃取する流れ [15]

2.1.4. EC-CUBEサイト管理者へセキュリティ対策の提案

EC-CUBE社が提供しているバージョンの確認手順 [16]にしたがって、利用中のEC-CUBEのバージョンを確認して、該当するバージョンごとに以下の（１）の脆弱性の修正を実施してください。もし脆弱なバージョンの製品を利用していた場合は、必ず（２）攻撃の確認と（３）被害の確認も実施して下さい。

（１） バージョン確認と脆弱性修正

① EC-CUBE4.0系を利用している方

EC-CUBE4.0系の最新版「EC-CUBE 4.0.6-p1」 [17]にアップデートしてください。EC-CUBE本体のソースコードをカスタマイズしている方には、コードの修正差分を反映してください。

最新版にバージョンアップすれば、脆弱性CVE-2021-20717を含め、CVE-2021-20750およびCVE-2021-20751が修正されます。詳細な修正方法は、株式会社イーシーキューブが公開した脆弱性ページ [8]をご確認ください。

② EC-CUBE3.0系を利用している方

（ア） EC-CUBE3.0本体の脆弱性修正

EC-CUBE3.0系用の修正パッチを適用してください。EC-CUBE本体のソースコードをカスタマイズしている方には、コードの修正差分を反映してください。

詳細な修正方法は、株式会社イーシーキューブが公開した脆弱性ページ [7]をご確認ください。

（イ） ETUNA製の配送伝票番号関連プラグインを利用している場合

すでに当該脆弱性を悪用した攻撃が発生しているため、表 8に記載された影響を受けるプラグインを使用している場合は、すぐに最新版へアップデートしてください。

表 8 ： ETUNA製プラグインのアップデート方法

影響を受けるプラグイン	アップデート方法
配信伝票番号プラグイン（3.0系）	1.0.11以降のバージョン [18]にアップデートしてください。
配信伝票番号csv一括登録プラグイン（3.0系）	1.0.9以降のバージョン [19]にアップデートしてください。
配送伝票番号メールプラグイン（3.0系）	1.0.9以降のバージョン [20]にアップデートしてください。

（ウ） イーシーキューブ製EC-CUBEプラグインを利用している場合

すでに当該脆弱性を悪用した攻撃が発生しているため、表 9に記載された影響を受けるプラグインを使用している場合は、すぐに最新版へアップデートしてください。

表 9 ： イーシーキューブ製プラグインのアップデート方法

影響を受けるプラグイン	アップデート方法
帳票出力プラグイン	1.0.1以降のバージョン [21]にアップデートしてください。
メルマガ管理プラグイン	1.0.4以降のバージョン [22]にアップデートしてください。
カテゴリコンテンツプラグイン	1.0.1以降のバージョン [23]にアップデートしてください。

（エ） EC-CUBE用のプラグインを開発している場合

株式会社イーシーキューブは、EC-CUBE3.0系のプラグインを開発する方へ、カテゴリコンテンツプラグインというサンプルプラグインを提供しています [24]。そのプラグインでhttp_entity_code関数が使われているため、2.1.3で述べたように無害化されたデータを逆に実行可能なスクリプトへ変換して出力し、クロスサイトスクリプティング攻撃が発生するおそれがあります。開発したプラグインがhtml_entity_decode関数を使用しているか否かを確認してください。使用している場合は、EC-CUBEの修正方法 [25]を参考にしてソースコードを修正してください。

2021年6月14日に、カテゴリコンテンツプラグインの最新版のバージョン1.0.1がリリースされましたが [26]、過去に古いバージョンを利用してプラグインを開発した、かつ現在はEC-CUBE 3.0.0～3.0.8を利用する場合、影響を受ける可能性があります。

（2） 攻撃の確認

これらの脆弱性は、EC-CUBE3.0系と4.0系の全バージョンに存在します。よく使用されている複数のプラグインにも脆弱性が含まれています。攻撃者は、これらの脆弱性がある日本国内のオンラインショップを積極的に攻撃していたため、すでに攻撃されているおそれが高いと思います。脆弱性修正を対応した後、必ず攻撃を受けたかどうかを確認してください。脆弱性CVE-2021-20717などを悪用したStored XSS攻撃を受けた場合、攻撃者は、顧客や受注、または配送に関するデータベースの名前や住所、会社名などへ、スクリプト化できる文字列”<script>”を入力して保存しています。その場合、「<」や「>」は、無害化されて「<」や「>」の文字列に置き換えられています。データベースで ”<script>” の文字列を検索して下さい。ただし、管理画面から調査すると攻撃が成立するおそれがあるため、データベースを直接検索したり、メールボックスに残っている受注メール本文を調査したりしてください。

（3） 被害の確認

攻撃の痕跡が見つかった場合、すぐにEC-CUBEのシステムをネットワークから切り離して、早急にセキュリティ担当者へ連絡してください。JPCERT/CCは、攻撃者のIP/ドメイン、または攻撃に使われた各ファイルのSHA256ハッシュ値を公開しています [5]。これらの情報を活用して、攻撃者の侵害内容を調査してください。ECサイトにWebShellが設置されていたり、ECサイトから不審なIPアドレス/ドメインへの通信の痕跡を発見したりした場合は、クレジットカード情報の窃取などの被害が発生しているおそれが高いです。すぐに顧客へクレジットカードの不正利用を連絡したり、セキュリティ関係機関または監督官庁へ報告したりするなど、インシデント対応を実施してください。

2.1.5. まとめ

本稿では、2021年に新たに公開されたEC-CUBEの脆弱性と、その脆弱性を悪用した攻撃方法を説明しました。公開された複数のEC-CUBEの脆弱性のうち、Stored XSSの脆弱性CVE-2021-20717およびCVE-2021-20717は、脆弱性を悪用した攻撃が発生しています。EC-CUBEを使ったECサイトの管理者は、すぐにバージョンを確認して下さい。

EC-CUBEは攻撃者に狙われやすく、攻撃キャンペーン「Water Pamola」も日本のEC-CUBEの脆弱性を狙っています。攻撃が発生している脆弱性のあるバージョンを使用している場合は、すでに攻撃を受けているおそれがあります。攻撃や被害の痕跡を発見した場合

は、被害を最小限に抑えるように、すぐにECサイトのネットワーク遮断や顧客への連絡を実施してください。

2.2. メルカリ社へのソフトウェア・サプライチェーン攻撃

2.2.1. 事件の概要

フリマアプリ「メルカリ」を運営する株式会社メルカリ(以下、「メルカリ社」)は、2021年5月、第三者からの不正アクセスにより、同社の顧客情報等が外部に流出したことを公表しました [27]。本事件の特徴は、サードパーティ製のコードカバレッジツール「Codecov」への不正アクセスをきっかけとしたソフトウェア・サプライチェーン攻撃である点です。本稿では、攻撃者がどのようにして複数のシステムへ侵入できたのか、また侵入を防ぐためにはどのような対策を講じるべきか解説します。

2.2.2. 三段階のソフトウェア・サプライチェーン攻撃

（1） メルカリのシステム開発環境

まず、本事件が発生したシステム環境について説明します。メルカリのシステム開発は、図 8で示すCI環境(継続的インテグレーション環境)にて行われていました。Codecov等のコードカバレッジツールは、開発中のソースコードに対するテストがどの程度完了したかを可視化するツールです。メルカリのシステム開発環境においては、CodecovによってCI環境上で開発しているアプリケーションのテストが行われ、テストが完了したソースコードがGitHubに格納されていたものと思われます。また、本番環境とCI環境はネットワーク的に隔離されていたと推察されます。

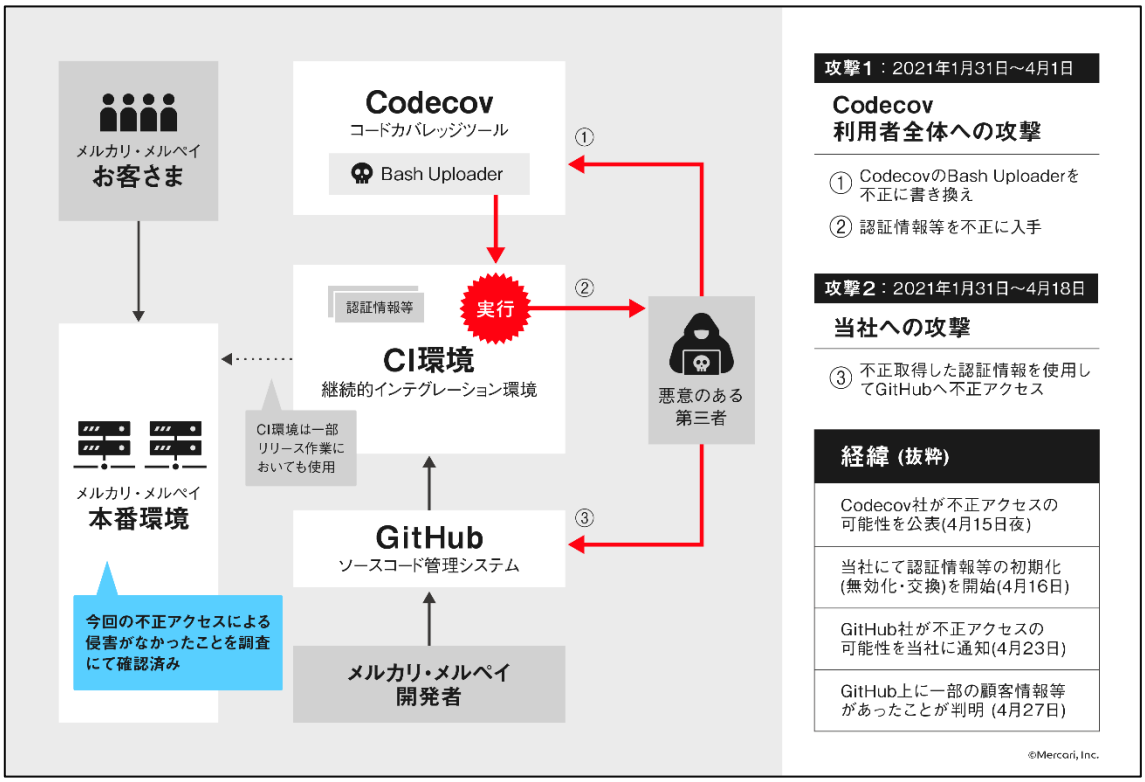


図 8 ： メルカリのシステム開発環境 [27]

（2） 三段階のソフトウェア・サプライチェーン攻撃の解説

メルカリ社およびCodecov社から公表された内容をもとに、本事件で行われた攻撃について説明します。

① Codecovへの攻撃

攻撃者は、CodecovシステムのDockerイメージの作成プロセスのエラーを狙って攻撃して、CodecovのBash Uploaderスクリプトを書き換える権限の認証情報を窃取しました。その後、2021年1月31日(米国時間)以降に、攻撃者は窃取した認証情報を使ってCodecovのBash Uploaderスクリプトを改ざんしました [28]。Bash Uploaderスクリプトとは、Codecov社の顧客が、テスト結果のレポート（コードカバレッジレポート）をCodecovプラットフォームへ送信するために利用するスクリプトです。レポートをCodecovプラットフォームへ送信することで、テスト結果をマージや分析した結果を得ることができます。

② CI環境からの情報取得

改ざんされたBash Uploaderスクリプトには、Codecov利用者の認証情報等を取得して攻撃者へ送信するように変更が加えられていました。メルカリ社の開発者が、

コードカバレッジレポートを送付しようと、改ざんされたBash Uploaderスクリプトをメルカリ社のCI環境上へダウンロードして実行したときに、開発者がCI環境で使用していた認証情報等が攻撃者へ送信されました。そのようにして漏えいした情報の中に、メルカリ社がGitHubへログインするための認証情報が含まれていたため、攻撃者の侵害範囲がGitHub環境にまで及ぶことになります。

③ Githubへの攻撃

4月22日、GitHub社はCodecovに関する不審なアクティビティを発見しました。そして4月23日にはメルカリ社に対して、GitHub上に格納されていたソースコードの一部もBash Uploaderスクリプトの改ざんの影響を受けているおそれがあると通知しました。これを受けてメルカリ社がGitHub上の自社リポジトリのログ調査を行ったところ、GitHubが不正アクセスされたことが判明しました。リポジトリにはメルカリのアプリケーションを構成するソースコードが格納されており、ソースコード内には顧客情報等が含まれていました。攻撃者によりリポジトリ内のソースコードを窃取された結果、累計27,927件の顧客情報が流出しました。(2021年8月6日に公表された追加情報 [29]を含む)

（3） 本事件の影響

メルカリ社の調査結果より、GitHubから流出した情報の一覧を記載します。着目すべき点は、漏えいした情報の「古さ」です。

1. GitHub上に格納されていたメルカリ（US版メルカリおよび過去提供サービスを含む）とメルペイのソースコードの一部
2. 上記ソースコードに含まれていたメルカリの顧客の口座振込みデータや問合せデータ（個人情報含む）
   - 2013年8月5日～2014年1月20日に実行された売上金の顧客口座への振込みに関連した情報（銀行コード、支店コード、口座番号、口座名義人（カナ）、振込金額）：17,085件
   - 2015年11月～2018年1月の間におけるカスタマーサービス対応に関連した情報（氏名、住所、Eメールアドレス、電話番号、お問い合わせ内容） ：217件
   - 2013年5月に実施したイベントに関連した情報（氏名、年齢、性別、Eメールアドレス）：6件
   - 2015年12月～2019年2月の間におけるカスタマーサービス対応に関連した情報（氏名、住所、生年月日、取引メッセージ）：13件(2021年8月6日に公表された追加情報 [29])
3. 上記ソースコード内に含まれていたメルカリおよびメルペイの一部取引先等に関する情報：

- メルペイ加盟店情報（個人事業主名）：7,925件
- メルカリおよびメルペイの取引先等に関する情報（氏名、生年月日、所属、Eメールアドレス等）：41件
- メルカリ社(子会社を含む)の一部従業員の個人情報（2021年4月時点の一部従業員の氏名、会社Eメールアドレス、従業員ID、電話番号、生年月日等 ※過去の在籍者や一部外部委託先含む）：2,615件
- メルカリ社(子会社を含む)の一部従業員の個人情報（2021年4月時点の一部従業員の氏名、会社Eメールアドレス、従業員ID等 ※過去の在籍者や一部外部委託先含む）：25件(2021年8月6日に公表された追加情報 [29])

今回漏えいした情報には、「2013年8月5日～2014年1月20日に実行された売上金の顧客口座への振込みに関連した情報」など、非常に古い情報が含まれています。メルカリ社の方針ではGitHub上に顧客情報を保管しないこととしていましたが、過去の運用に漏れがあったということです [30]。 このように、運用上必要ない機密情報をシステムに保管することは、不正アクセスがあった際に漏えいするリスクを生みます。

2.2.3. 攻撃者のねらい

本事件では、利用していたサードパーティ製品が侵害を受けたことをきっかけに、GitHubの認証情報が奪われて、GitHub上に保存されていた顧客の個人情報や口座情報等が漏えいする事態となりました。

しかし元々の攻撃者のねらいは、GitHub上に保存されていた個人情報だったのでしょうか。あくまで推測ですが、一般的にGitHub上に大量の個人情報や口座情報を保存しないこと、メリカリ社もGitHub上に個人情報や認証情報を保存しないようルールを定めているため、攻撃者もGitHub上から大量の個人情報を窃取することが目的ではなかったのではないでしょうか。過去のグローバルセキュリティ動向四半期レポート(2019年度第1四半期 [31])で取り上げた「EC-CUBE」の攻撃事例のように、攻撃者の本来のねらいは、EC関連システムの本番環境に侵入し、フロントエンドのオンラインサイトを改ざんして不正なプログラムを仕込んで、クレジットカード情報を窃取しようとしていたと推測します。

幸いにも、メルカリの事件では、攻撃者が本番環境へ侵入したり、改ざんしたプログラムが稼働中のサービスへ影響を与えたりした被害は、発生していません [27] [32]。メルカリ社が攻撃をどのように防いでいたかは不明ですが、本事件のようなソフトウェア・サプライチェーン攻撃に対して、どのような対策を講じるべきか、以下の項目にて解説します。

2.2.4. 対策

2020年度第3四半期のグローバルセキュリティ動向四半期レポート [33]でも取り上げたSolarWinds社の事件では、広く普及している運用監視ソフトウェアのOrion Platformを使用している複数のユーザ企業が、開発元のSolarWinds社を信用して、攻撃者が改ざんしたアップデートプログラムをダウンロードしてインストールしてしまい、その攻撃者に侵入されて被害が発生しました。SolarWinds社やメルカリ社の事件のように、ユーザ企業が信頼している提供元のソフトウェアであっても、ソフトウェア・サプライチェーン攻撃は発生します。

サプライチェーン攻撃は、商流を伝播する組織連鎖のサプライチェーン攻撃とソフトウェア・サプライチェーン攻撃があり、どちらの対策も異なる複数の組織が関係するため、複雑です。アメリカ国立標準技術研究所（NIST：National Institute of Standards and Technology）は、サプライチェーンのリスク管理に関する文書 SP800-161をすでに公開しており、米国大統領令 13873を受けて、本文書の改定をすすめているようです。欧州ネットワーク情報セキュリティ機関（ENISA：The European Union Agency for Cybersecurity）も、24件のサプライチェーン攻撃の分析した結果と対策方法をまとめた「Threat Landscape for Supply Chain Attacks」を公開しました。この報告書は、サプライチェーン攻撃の対策方法をユーザ企業向けと提供元向けに分けて記載しています。以下にユーザ企業向けの対策の一部を抜粋します。

- 組織内外の情報源およびサプライヤーのパフォーマンスモニタリングとレビューから得られた知見に基づいて、サプライチェーンのリスクと脅威を監視する
- 生産やサポートが終了した製品またはコンポーネントを含む、製品またはサービスのライフサイクル全体にわたってサプライヤーを管理する
- サプライヤーと共有している、またはサプライヤーがアクセスできる資産と情報を分類し、そのアクセスと取り扱いに関する適切な手順を定義する
- これら全ての義務と要件を契約に盛り込み、下請けのルールと潜在的に連なる要件について合意する
- サプライヤーとサービスプロバイダーから隠し機能またはバックドアが故意に含まれていないことの保証を受ける
- ツールや技術の変更など、サプライヤーとの契約における変更を管理するプロセスを定義する

これらの対策をきちんと実施することが理想です。しかし、この一部抜粋した対策でさえ、その実施は容易ではありません。いきなり、この対策を網羅することは困難でしょう。そこで、まずはメルカリの事件のように、本番環境への侵害を防ぐことが必須の対策です。1つ目は、攻撃者が本番環境へ侵入できないように、本番環境への接続経路を限定すること、多要素認証を使ってなりすましを防ぐことです。2つ目は、改ざんされたソースコードのリリ

ース防止です。本番環境への攻撃者の侵入を防いでも、本事件のように攻撃者がGitHubへ侵入していれば、ソースコードが改ざんできます。もしリポジトリ内のソースコードへオンラインバンキングやクレジットカードの情報を抜き取る不正な処理を埋め込んでいたら、古い口座情報だけではなく最新の口座情報やクレジットカードのセキュリティコードが窃取されて、被害がより大きくなっていたおそれがあります。開発の自動化が進むと改ざんされたソースコードが自動的にリリースされてしまい、被害が発生するまで気づかないことが多くなるでしょう。リリース前のソースコードの改ざんや不正なコードの有無のチェックは、必須です。

2.2.5. まとめ

メルカリの事件は、Codecovという比較的新しい開発者用のクラウドサービスを攻撃して、そこから同サービスの利用者の開発環境内へと芋づる式に攻撃して侵入しようとしたソフトウェア・サプライチェーン攻撃です。攻撃者は、複数の開発用のクラウドサービスと開発環境と本番環境が接続した構成を想定して、攻撃を仕掛けていると思います。継続的インテグレーション(CI)や継続的デプロイメント(CD)を使った開発モデルでは、ビルド、テスト、リリースの自動化が進むため、もし攻撃者が不正なコードを仕込んで本番環境の悪用を狙っている場合は、それを未然に防止したり、気づいたりすることが難しくなります。

もし「2.2.4 対策」で説明したソースコードのセキュリティチェック機構が不正なコードを検知できなかった場合、攻撃を受けたこと/受けたおそれがあることに気づいたあとに、いかに迅速にインシデントに対応できるかが、被害の拡大防止のポイントです。メルカリの事件では、4月15日にCodecov社が第三者による不正アクセス事件を公表して、その翌16日に、メルカリ社は一次対応としてCI環境にある認証情報の初期化（無効化・交換）を行っています。もしこのときに、Codecovと連携しているGitHubやCI環境への侵害調査を開始していたら、4月23日にGitHub社から連絡されて対応を開始するよりも早期に侵害を発見し初動対応を開始できたでしょう。攻撃を受けたおそれがあると気づいたときに、該当するシステムの連携先や接続先まで調査して、そこから攻撃の痕跡を発見して正確に被害範囲を特定することが、インシデント対応の第一歩です。メルカリ社の初動対応は比較的早かったと思いますが、こういったきっかけを有効に使えずに、インシデントの発見や対応が遅れるケースが多いため、参考にしてほしいと思います。

3.情報漏えい

2021年5月21日に、ネットマーケティング社は、恋愛や婚活を支援するマッチングアプリ「Omiai」を管理するサーバへ外部からの不正アクセスがあり、年齢確認のために提出された運転免許証や健康保険証、パスポート、マイナンバーカードの画像データが流出したと発表しました [34] [35]。本稿では、悪意のある第三者が、流出した運転免許証などの身分証明書の画像データを悪用するリスクについて、2020年度第4四半期レポートの予測で紹介したeKYCとこれを規定する犯罪収益移転防止法の各条項を交えて説明します。

3.1. Omiaiの情報漏えい

ネットマーケティング社の運営するOmiaiから、最大で171万1756人分の年齢確認書類の画像データが流出しました。Omiaiは、「インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律（出会い系サイト規制法）」にしたがって、運転免許証などの身分証明書の画像を使って、申請者の年齢を確認していました。そのため、Omiaiに蓄積していた身分証明書の画像データは、以下の特徴があります。

- 18歳以上の顔写真
- 信頼性の高い公的な身分証明書
- スマートフォンのカメラで撮影した高解像度データ

過去に、このような信頼性の高い公的な身分証明書の高解像度の画像データが、100万人単位で漏えいした個人情報漏えいインシデントは、発生した記憶がありません。悪意のある攻撃者が、信頼性の高い公的な身分証明書を100万人単位で取得できたら、どのような犯罪行為へ悪用されるでしょうか。

たとえば、18歳以上であれば就労年齢の区分に該当するため、攻撃者は画像データからターゲットの連絡先を特定して、ターゲットの所持している資産を狙った詐欺行為を仕掛けることができます。また100万人単位の信頼性の高い公的な身分証明書の高解像度の画像データがあれば、身分証明書を偽造して、そのターゲットになりすますことができるかもしれません。発表された情報によると、流出した画像データのうち、約6割、約100万件が運転免許証でした。運転免許証は、本人確認するときの身分証明書として、よく利用されています。みなさんも、郵便物や宅配物を受け取るときや、小売店の会員証を発行するときなど、対面で本人確認するときに提示したことがあるでしょう。それだけでなく、このOmiaiのようなオンラインサービスの本人確認手段としても、身分証明書を使った本人確認方法が広く普及してきています。身分証明書の高解像度の画像データが悪用できるようになった場合に、世の中へどのような影響がおよぶのか、考察してみます。

3.2. 流出した身分証明書の画像データの不正利用

3.2.1. eKYCの規格

オンラインサービスの申込時に本人確認する手段として、既存の身分証明書を使った確認方法が広く普及してきています。クラウドサービスなどのオンラインサービスの普及にあわせるように、そのアカウントの本人確認方法も、多くのユーザはオンライン上で完結する方式を求めています。オンラインだけで本人確認を完結させる場合、本当に本人であることを確認できるのか、その信頼性が気になるのではないでしょうか。オンラインサービスを提供する企業は、確実に本人確認できなければ、アカウントを安心して発行できないでしょう。もし不審なユーザが身分を詐称してアカウントを作成できてしまえば、オンラインサービスの提供企業は、自社サービスのアカウントが犯罪に使われたり、利用料を徴収できなかったりと、深刻な問題が発生すると思います。

「本人確認」とは何でしょうか。経済産業省は、本人確認が、ユーザの実在性を確認する「身元確認」とそのユーザが実際に操作していることを確認する「当人認証」の2つで成り立つと定義付けています [10]。詳しくは、2020年度第2四半期レポートの「2.1.2.「本人確認」とは何か」の記事でわかりやすく解説しているので、読んでみて下さい。身分証明書を使ってオンラインなど非対面で本人確認を行う仕組みが、eKYC（electronic Know Your Customer）です。FinTechの拡大により、オンライン銀行やオンライン証券の口座開設時の本人確認の手続きに時間がかかることが、問題視されました。そこで、2018年11月30日に「犯罪による収益の移転防止に関する法律」が改定されて、オンラインによる非対面での本人確認が行えるようになりました。これにより、ブラウザやスマートフォンのアプリを使って、オンラインだけで迅速に本人確認できるようになった点が、eKYCの大きな特徴です。eKYCは、本人確認の所要時間の短縮や手続きの簡素化により、申請者の利便性が向上しました。サービス提供側は、本人確認業務が効率化されて、本人確認のコストも削減できました。しかし、オンラインで早く便利になった代わりに、高度な偽造身分証明書でなりすましされるリスクが一部分において許容されていると思います [36]。

「犯罪による収益の移転防止に関する法律」（以下、「犯収法」とする）が改定されて、6条1項1号にeKYCの規格が記載されました。このeKYCの記載をもとに、表 10へ特徴を整理しました。犯収法では、eKYCを4つに分類しています。

表 10 ： eKYCの規格 [37] [38] [39] [40]

条項	方式	本人確認方法	偽造身分証明書への耐性	使われているサービス
ホ	セルフィーアップロード型	身分証明書撮影＋容貌撮影	△ なりすまし成功のおそれあり	・銀行 ・証券 ・消費者金融 ・通信キャリア
ヘ		ICチップ読取＋容貌撮影	◎ なりすまし困難	一部の銀行
ト	フェデレーション型	① 身分証明書撮影＋銀行等に顧客情報を照会/クレジットカード照合	○ 条件付きでなりすまし成功の可能性あり（銀行口座がある場合）	クレジットカード
		② ICチップ読取＋銀行等に顧客情報を照会/クレジットカード照合	◎ なりすまし困難	
ワ		公的個人認証/マイナンバーカード利用（ICチップ読取）	◎ なりすまし困難	・e-Tax ・一部の証券 ・一部の決済アプリ

現状は「ホ」が最も普及しており、銀行口座のオンライン開設にも用いられています。しかし、「ホ」の方法を利用した本人確認は、偽造身分証明書を使ったなりすましに対して最も脆弱です。一部の銀行では、より信頼性の高いICチップ読取を用いた「ヘ」を利用した方法が採用されています。たとえば、ICカード免許証は、内蔵されたICチップに記録された情報とオンラインで入力された情報を照合することができます。そのため券面を偽造された場合でも、ICチップから取得した正しい情報を使って見破ることができて、より安全です。

クレジットカード会社は「ト」の方法を用いています。「ト」の方法は、身元確認の方法が、表 10のように①身分証明書撮影の場合と②ICチップ読取の場合の2パタンに分かれます。「① 身分証明書撮影＋銀行等に顧客情報を照会」の方法よりも、「ヘ」と同様に「② ICチップ読取＋銀行等に顧客情報を照会」の方がより安全です。例えばクレジットカードの申し込みで、この方法を使って審査する場合は、申し込み時に入力した内容と、銀行に既に登録している住所、生年月日などの情報を突合することで身元確認を行います。クレジットカード会社とeKYC処理を連携している信頼性の高い銀行の口座を持っていなければ、身元確認を行えません。

「ワ」の方法は、マイナンバーカードを使用した本人確認方法です。主にe-Taxや一部の証券会社と決済アプリで使われています。マイナンバーカードは、カードの「所持」とマ

イナンバーカードのICチップを読み取るためのパスワードの「知識」で身元確認をおこなっています。たとえば、証券会社の口座開設する時は、ICカードリーダへセットしたマイナンバーカードを使って、口座開設の申し込み情報を暗号化して、暗号化前の情報と暗号化情報、公開鍵、署名用電子証明書を一緒に証券会社へ送信します。証券会社は、受信した公開鍵で暗号化情報を復号して、暗号化前の情報と突合して改ざんを検知したり、署名用認証局へ署名用電子証明書の有効性を照会したりして、身元確認を確認します。このようにICチップが入ったマイナンバーカードの偽造は困難であり、かつ署名用電子証明書を使った有効なマイナンバーカードの確認も行えるため、表 10のeKYC方式の中では最も信頼性が高い身元確認の方法です。

3.2.2. eKYC「ホ」判定方式の能力

eKYCを用いた本人確認も、身元確認と当人認証の2つの処理で構成されています。例えば、表 10の「本人確認方法」列の「ホ」に記載している「身分証明書撮影」が身元確認で、その結果と「容貌撮影」を組み合わせて当人認証を行います。

もし偽造した身分証明書を悪用して、eKYCで本人確認しようとした場合は、どのように真贋を判別しているでしょうか。身分証明書を撮影して真贋を判定する方法を使っている場合は、複写機でコピーした身分証明書を使う程度の攻撃方法を想定していると思います。そのため身分証明書の真贋を識別する手段としても、身分証明書の写真や文字の鮮明さに加えて、身分証明書の厚みの有無で真贋を判断する方法を採用しています。日本国内では、他人の運転免許証などの公的な信頼性の高い身分証明書の画像データは、ほぼ手に入れることができません。警察庁の犯罪統計によると文書偽造の認知件数はここ数年で減少傾向にあることから、日本国内は身分証明書の偽造が難しいと思われます [41]。もし紛失した身分証明書が悪用された場合でも、信用情報機関の失効リストなどを使ってチェックすれば悪用や偽造を検知できる場合があるため、紛失や盗難された身分証明書の偽造も多く行われていないと想像できます。このように、これまでは信頼性の高い公的な身分証明書は偽造が難しく、身分証明書を撮影する程度の判別方法でも、偽造身分証明書を使った本人確認の成功を一定数以下に抑えることができていた、身分証明書の判定の信頼性が確保できていたと推測します。

Omiaiの情報漏えい事件から流出した信頼性の高い公的な身分証明書の高解像度の画像データが大量に出回った場合、犯罪組織がその画像を使って作成した精度の高い偽造身分証明書が、これまでよりも多く出回ることが懸念されます。そうなると、表 10の「ホ」の判定方式では、偽造身分証明書を見破れなくなるでしょう。今後は、eKYCの「ホ」の判定方式を採用しているオンラインサービスは、偽造身分証明書を使った口座開設の申請を承認してしまうかもしれません。その結果、以前よりも、他人になりすました新規のアカウントが増加すると予測します。特にオンライン銀行やオンライン証券の口座開設に使用している場合は、以前よりも特殊詐欺やマネーロンダリングなどの犯罪への悪用が増えるかもしれません。該

当する金融機関は、不正な入出金などの利用を監視や本人確認の方法の見直しを検討したほうが良いでしょう。それ以外のオンラインサービスも、より信頼性の高い方法への変更することで不正なりすましによって損害を負うリスクを減らすことができます。

3.2.3. eKYC「ヘ」および「ト」② 判定方式の能力

eKYCの「ヘ」および「ト」の②の判定方式は、身分証明書のICチップを読み取ります。たとえば、ICカード免許証の偽造は非常に困難なため、偽造ICカード免許証を使った身元確認は失敗します。したがって、この2つの判定方式は、Omiaiの情報漏えい事件の影響を受けません。同方式は、身元確認の信頼性が担保されます。また、ICカード免許証は、免許証の表面に記載されている生年月日、顔写真データと、表面に記載されていない本籍と国籍の情報などを内部のICチップへ記録しています。eKYCのICチップ読取と容貌撮影を組み合わせている「ヘ」の判定方式は、ICチップ内の顔写真データと撮影した本人の顔画像を照会するため、もしICカード免許証の表面の写真が差し替えられている場合は、当人認証で不正を検出できます。このため、ICカード免許証を使う「ヘ」および「ト」の②の判定方式は、券面を偽造した免許証の不正使用を防ぎ、攻撃者による新規のなりすましアカウントの開設を未然に防止できます。

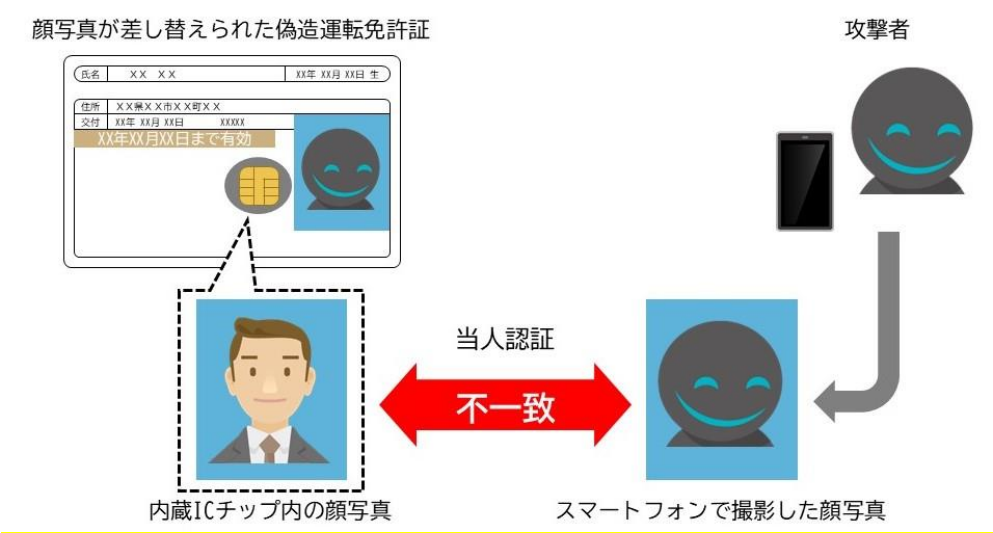


図 9 ： eKYCの「ヘ」および「ト」の②判定方式 [42]

3.2.4. eKYC「ト」① および「ワ」判定方式の能力

もし漏えいした身分証明書の画像データから偽造した身分証明書を作って本人確認した場合、上記で解説した3つ以外のeKYCの方式は、それを見破ることができるでしょうか。独自に評価した結果を3.2.1の表 10の「偽造身分証明書への耐性」へまとめました。

「ト」の①方法は、身分証明書撮影と銀行等やクレジットカード会社への照会を行う方

法です。この方法は、身分証明書撮影は券面の偽造を見破ることが難しく、ICチップ読取と比較して偽造身分証明書への耐性が劣っています。銀行やクレジットカード会社に顧客情報を照会する方法は、2つあります。1つ目は、銀行やクレジットカード会社の本人情報を利用する方法です。たとえば、eKYCの本人確認処理の途中でオンラインバンキングに接続して、事前に入力した内容とオンラインバンキングに登録されている氏名、住所、生年月日などの情報を照会して身元確認をおこないます [43]。2つ目は、通帳の記帳データを利用する方法です。証券会社などのサービス提供者が、申請者本人名義の既存の銀行口座へ一定金額を振り込んで、申請者がその振込金額を確認してサービス提供者へ回答して、当人認証を行います。どちらの方法も偽造身分証明書を使って事前に銀行口座を用意していた場合は、なりすましを見破ることが困難です。

「ワ」のマイナンバーカードを使った公的個人認証方式は、電子証明書を用いて本人確認を行います。電子証明書には、「署名用電子証明書」と「利用者証明用電子証明書」があります。

署名用電子証明書を使えば、インターネットで情報を送信する時に、本人が情報を送信したことと情報が改ざんされていないことを確認できます。

図 10を用いて、この仕組みを説明します。例えば、利用者は、口座開設などを申請する時に、マイナンバーカードをICカードリーダへセットして、パスワードを入力します。するとマイナンバーカード内のICチップの秘密鍵を使って、ICチップ内で申請情報を暗号化します（図 10の(1)）。暗号化した申請情報（暗号文）と暗号化前の申請情報、公開鍵、署名用電子証明書を一緒にサービス提供者へ送信します（図 10の(2)）。サービス提供者は、送られてきた公開鍵で暗号化した申請情報（暗号文）を復号して、暗号化前の申請情報と突合して改ざんを検知できます（図 10の(3)(4)）。またサービス提供者は、署名用認証局の地方公共団体情報システム機構（以下、「J-LIS」という）へ署名用電子証明書の有効性を照会します。J-LISは、失効情報と照会して結果を返します（図 10の(5)）。署名用電子証明書が有効であれば、身元確認が成功します（図 10の(5)）。

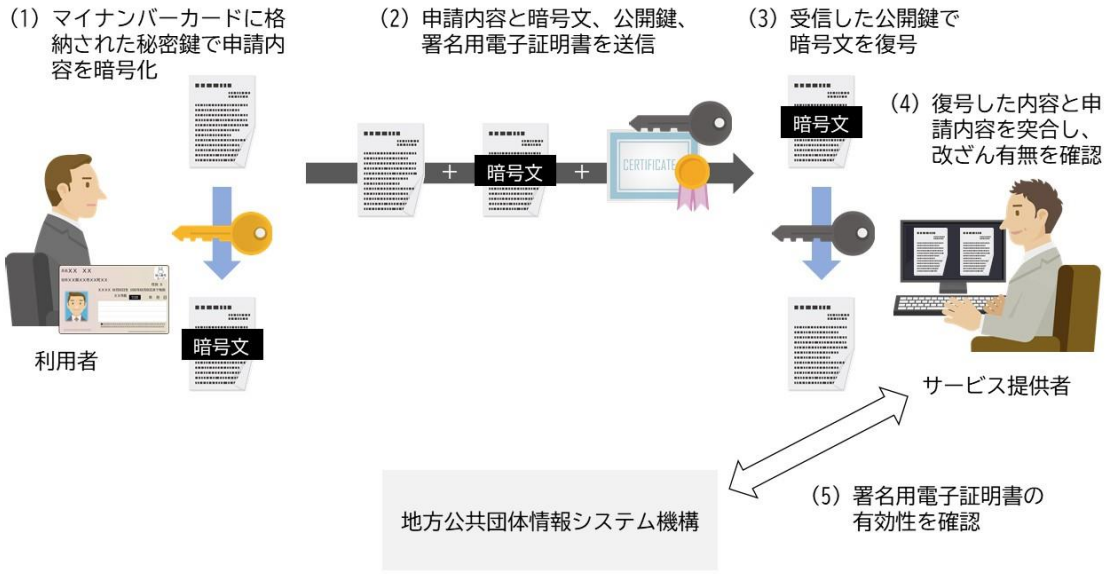


図 10 ： 署名用電子証明書を使った公的認証サービスの仕組み [44]

利用者証明用電子証明書を使うと、利用者本人であることを証明できます。例えば、口座開設時に本人確認が必要になった場合は、署名用電子証明書のときと同様に、ユーザはパスワードを入力して、サービス提供者から送信された乱数をマイナンバーカード内のICチップの秘密鍵を使って、ICチップ内で暗号化します（図 11の(2)）。利用者は、暗号化した乱数と暗号化前の乱数、利用者証明用電子証明書、公開鍵を返送します（図 11の(3)）。サービス提供者は、公開鍵で暗号化した乱数（暗号文）を復号して暗号化前の乱数と突合して改ざんを検知できます（図 11の(4)(5)）。また、署名用電子証明書のときと同様に利用者証明用電子証明書の有効性を照会して、結果を受領します（図 11の(6)）。利用者証明用電子証明書が有効であれば、本人確認が成功します（図 11の(6)）。

「ワ」のマイナンバーカードを使ったeKYC方式は、「署名用電子証明書」と「利用者証明用電子証明書」のどちらかを使って、身元確認をおこなっています。

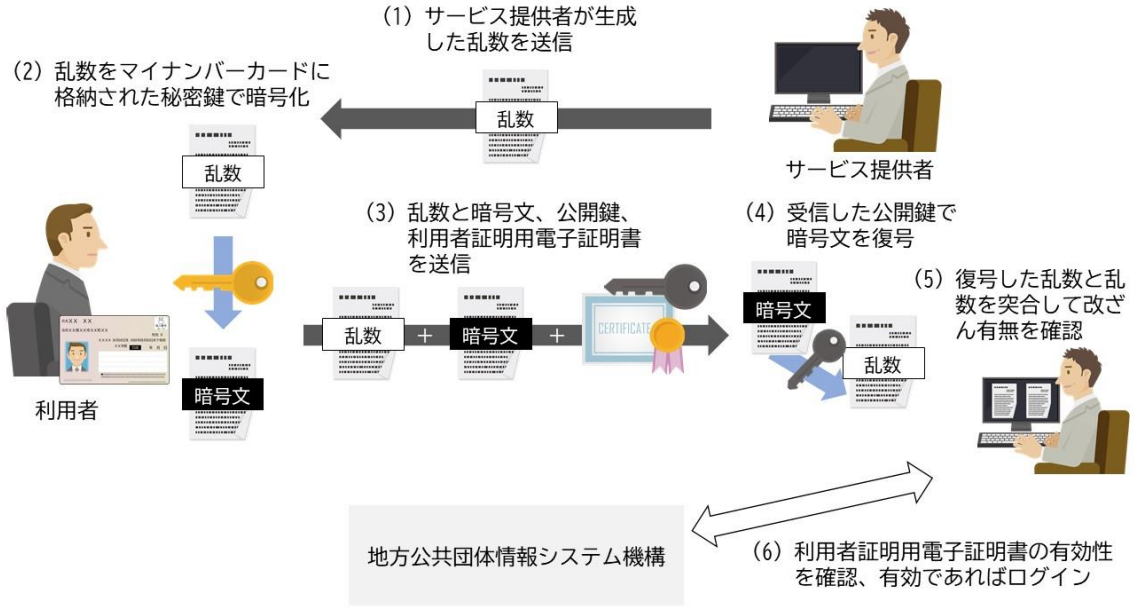


図 11 ： 利用者証明用電子証明書を使った公的認証サービスの仕組み

[44]

3.2.5. 旧来の本人確認への影響

Omiaiの情報漏えい事件の運転免許証の画像データの流出は、eKYCを使った本人確認だけでなく、旧来の本人確認にも影響が懸念されます。

運転免許証の画像データ流出は、その画像データから氏名や住所、生年月日、顔写真などの個人情報が取得できてしまいます。これら情報があれば旧来の本人確認手法で口座・アカウント開設の本人確認を行える金融サービスなどもあり、今後、ID・パスワードの流出よりも、大きな被害が出るおそれもあります。運転免許証のコピーだけを使って審査をする旧来の本人確認の場合も、本事件の影響でリスクが高まるおそれがあります。また、身分証明書を使って本人確認する本人限定受取郵便にも、影響が及ぶかもしれません。技術のある犯罪組織であれば、顔写真や住所を差し替えた運転免許証を偽造できてしまい、郵便局で券面を偽造した運転免許証を提示して、本人になりすまして郵便の受け取りに成功してしまうかもしれません。攻撃者が、他人になりすます場合は、最も脆弱な本人確認方法を狙います。企業は、旧来の本人確認方法も見直す必要があります。

3.3. まとめ

2020年度第4四半期レポートの予測「情報漏えい事件の二次被害に警戒」では、自社のサービスでなりすましが起きるリスクを算定して、リスクの回避や低減、受容といった対策をとならければならないと述べました。

これまでは警察庁の犯罪統計からも分かるように、身分証明書の偽造は難しく、身分証明書を撮影する方式の本人確認でも、券面を偽造した身分証明書を使ってなりすまされる懸念は、あまりありませんでした。しかし、犯罪組織は、Omiaiの情報漏えい事件によって流出した身分証明書の画像データを使って、精度の高い偽造身分証明書を作成することができてしまうかもしれません。企業は自社サービスでなりすましが行われていないか状況をモニタリングして、なりすましが多発するようであれば、本人確認の方法を見直した方が良いでしょう。

今後は、身分証明書を撮影する方式ではなく、偽造身分証明書を見破ることができるICチップ読み取り方式のeKYC 「ヘ」、「ト」の②、「ワ」が普及すると思います。

4.脆弱性

本稿の読者も普段から使用している、ある身近なものに脆弱性が隠れていることをご存じでしょうか。2021年5月、ニューヨーク大学アブダビ校のマシー・ヴァンホーフ（Mathy Vanhoef）氏（以下、ヴァンホーフ氏と記す）は、無線LANの国際的な標準規格の１つとして最も広く普及している、標準規格IEEE 802.11に複数の脆弱性が存在することを公表ました [45] [46]。これらの脆弱性はIEEE 802.11に属するすべての無線LAN機器に存在し、無線LAN機器を利用しているユーザは誰でも被害を受けるおそれがあります。本稿では、ヴァンホーフ氏によって発見された脆弱性がどのようなものか、またどのような対処をすればよいのか、解説します。

4.1. FragAttacksの概況

ヴァンホーフ氏によって発見された複数の脆弱性は、「FragAttacks （**fr**agmentation and **ag**gregation **attacks**）」 [47] と総称します。これらの脆弱性の一部は、米国電気電子学会によって初めて無線LAN規格が発表された1997年から、20年以上の期間に渡り発見されずに存在していました [45]。

ほとんどの無線LAN機器は、IEEE 802.11にもとづいて技術仕様を決定し、Wi-Fi Allianceという業界団体[5]によって他社メーカ機器間の相互接続性がテストされています[5]。わかりやすく言えば、Wi-Fi Allianceに認められたWi-Fi認証 [48]を取得している無線LAN機器には、FragAttacksが存在します。つまり、Wi-FIで通信する全ての無線LAN機器、及びWi-Fiを利用している全てのユーザが攻撃対象となりえます [45] [48]。さらに、無線LANのセキュリティを強化するプロトコルWEPやWPA3等もIEEE 802.11にもとづいているため、FragAttacksが存在します。私たちにとって身近な存在であるWi-Fiには、長い間ずっと脆弱性が潜んでいたのです。

ただし、FragAttacksは、攻撃者が標的となる無線の通信と同じ範囲内にいなければならないこと、また、攻撃の手法が複雑であることなどから、FragAttacksの発表以降、この脆弱性に関する被害はまだ報告されていません [45]。しかし、攻撃者がFragAttacksの情報を使用して、この脆弱性を攻撃するツールを開発すれば、今後、被害が起きるおそれは否めません。

4.2. FragAttacksの起因と攻撃の仕組み

4.1で説明した通り、FragAttacksはFrame aggregation及びFrame fragmentationを合わせて名づけられています。FragAttacksは、これらの無線LAN機器の規格の設計上及び実装上の欠陥が起因の脆弱性です [49]。Frame aggregationに関連する設計上の脆弱性が1つ、

Frame fragmentationに関連する設計上の脆弱性が2つ [45]、そしてこれらの設計上の脆弱性に紐づいた実装上の脆弱性が幾つか存在します。

攻撃者はこれらの脆弱性に対してどのように攻撃することができるのでしょうか。

4.2.1. Aggregation攻撃

まず、Frame aggregationの設計上の不備（CVE- 2020-24588）を悪用したAggregation攻撃を紹介します [45] [50]。Frame aggregationとは、1つ以上の802.2/802.3形式のフレームを、IEEE 802.11形式のフレーム1つにまとめ、Wi-Fiで効率的に送信する方法です[1]。IEEE802.11形式のフレームヘッダには、1つ以上のA-MSDU（Aggregate MAC Service Data Unit）フレームを集約した集約フレームであることを示すA-MSDUフラグがあります。集約フレームの場合は、A-MSDUフラグを1に設定します。IEEE 802.11では、A-MSDUフラグ（図 12の“is aggregated”）が保護されていないため、第三者がこのA-MSDUフラグを不正に書き換えることが可能です [45] [50]。このようにすることで、攻撃者は、単体のIEEE 802.11形式のフレームへA-MSDUフラグをセットして、この単体フレームを1つ以上のA-MSDUフレームを集約した集約フレームへ見せかけて、受信者に送り出します。次に攻撃者は、集約フレームに見せかけたA-MSDUフレームのヘッダに含まれるフレーム長の値を改変します。攻撃者は、改変したフレーム長にあうように、フレームを追加できます。攻撃者は、この追加フレームに攻撃を仕込むことができます。

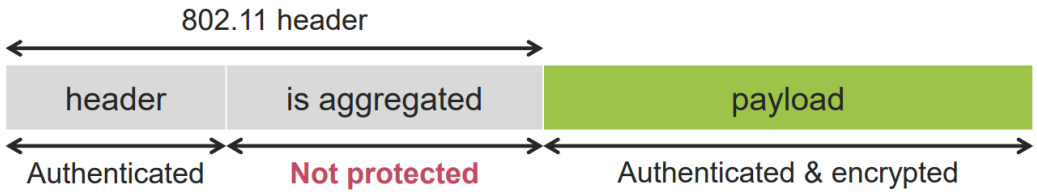


図 12 ： IEEE 802.11規格のデータ送信時のフレーム [47]

この方法を使えば、攻撃者は、例えばICMPv6 RA（Router Advertisement/ルータ広告）を悪用した攻撃パケットをフレームの中へ入れて、攻撃対象のマシンへ届けることができます。攻撃対象のマシンがIPv4/IPv6デュアルスタックの場合は、このICMPv6 RAの攻撃パケットを受信すると、攻撃者が準備した悪意のあるDNSサーバを使用するようにOSの設定が変更されます。ユーザが、インターネット上のあるWebサイトへアクセスしようとすると、攻撃対象のマシンは攻撃者が準備した悪意のあるDNSサーバへWebサイトの名前解決を依頼します。すると、攻撃者のDNSサーバから偽のIPアドレスが提供されて、ユーザは攻撃者が用意したフィッシングサイトへ誘導されてしまいます。例えば、ユーザがAmazonで買い物をしようとして、ブラウザへ”www.amazon.com”を入力すると、マシンは

悪意のあるDNSサーバへ名前解決を依頼します。すると攻撃者のDNSサーバは、正規のAmazonのIPアドレスではなく、攻撃者が用意したフィッシングサイトのIPアドレスをマシンへ返答します。ユーザは、攻撃者が用意したAmazonそっくりのフィッシングサイトへ誘導されて、IDとパスワードを入力してしまいます。攻撃者は、このようにWi-Fiに接続したIPv4/IPv6デュアルスタックのマシンを使用しているユーザへ、容易にフィッシング攻撃を行えます。

4.2.2. Mixed key攻撃

次に、Frame fragmentationの設計上の不備である2つの脆弱性を悪用した攻撃を紹介します[1]。Frame fragmentationとは、IEEE 802.11を使用してWi-Fiでデータを送信する時に、サイズの大きいパケットを複数の断片パケットへ分割して、それをフレームへ載せて送る方法です [45]。

Frame fragmentationの1つ目の脆弱性 CVE2020-24587を悪用したMixed key攻撃を解説します。Frame fragmentationでは、送信側が１つのパケットを複数の断片パケットへ分割してから、分割したそれぞれの断片パケットを暗号鍵 "k"で暗号化してフレームに載せて、無線LANアクセスポイント（以下、「AP」とする）へ送信します。この時に問題となるのが、IEEE 802.11では、暗号鍵 "k"で暗号化した断片パケットが載ったフレームと、暗号鍵 "m" で暗号化した断片パケットが載ったフレームが混在しても、APは、それぞれのフレームを受信して、それぞれの暗号鍵で断片パケットを正しく復号できる点です [50] 。APは、復号した断片パケットをつなげてパケットを再構築して、そのパケットのヘッダで指定した宛先へ、パケットを送信します。もし攻撃者がWi-Fiを中継できる場合、攻撃者は、上記の方法で盗聴対象のマシンが送信したフレームと別のフレームを混在させて、盗聴対象マシンの情報を含んだパケットを再構築します。そして、そのパケットを受信して、情報を盗聴します。

以下で、Mixed key 攻撃の方法を説明します。まず攻撃者は、盗聴対象のマシンを攻撃者の用意したインターネット上のWebサイトへアクセスさせます。この時、攻撃者は、盗聴対象のマシンと無線LANアクセスポイント（以下、「AP」とする）の間に割り込んで、通信を中継します。つまり、攻撃者は中間者攻撃（MITM：Man-In-The-Middle）を行える状態にしておきます。さらに盗聴対象のマシンが、攻撃者のWebサイトへアクセスしたときに、パケットの分割（fragmentation）が発生するように、文字数の長いドメインやFQDN、URLを宛先へ指定します。すると、盗聴対象のマシンは、パケットを複数の断片パケットへ分割して暗号鍵”k”で暗号化したあと、複数のフレームへ載せて送信します。

次に攻撃者は、上記の複数のフレームを受信します。1つ目のフレーム（図 13 の ”$Enc_k\{Frag_0(s)\}$”）のフラグメント番号やシーケンス番号”s”を取得して、そのままAPへ転送します。2つ目以降のフレームは、APへ転送せずに破棄します。APは、1つ目のフレームをメモリ上に保存して、2つ目以降のフレームの到着を待ちます。

盗聴対象のマシンとAPは、一定時間間隔で暗号鍵を変更します。このように暗号鍵を"m"へ変更したタイミングで、攻撃者は、盗聴対象のマシンから送信された断片パケットが載った複数のフレームを受信します。今度は、1つ目のフレーム（図 13 の "$Enc_m\{Frag_0(s')\}$"）を破棄します。2つ目以降のフレーム（図 13 の "$Enc_m\{Frag_1(s')\}$", "$Enc_m\{Frag_2(s')\}$"…）は、最初に中継したフレーム"$Enc_k\{Frag_0(s)\}$" に合わせて、ヘッダのシーケンス番号"s'"を"s"へ改変します。その後、この2つ目以降の不正なフレームをAPへ転送します。

最後に、APはメモリ上に保存している1つ目のフレーム "$Enc_k\{Frag_0(s)\}$"と、それとは別の通信の2つ目以降のフレーム "$Enc_m\{Frag_1(s)\}$、$Enc_m\{Frag_2(s)\}$・・・$Enc_m\{Frag_x(s)\}$" をそれぞれの暗号鍵kとmで復号して、分割されていたパケットを再構成します。つまり、攻撃者は、1つ目のフレームに攻撃者のWebサイト宛のパケットヘッダ部分を入れて、2つ目以降のフレームに盗聴対象のマシンが送信した断片パケットを入れて順番にAPへ送付すると、APは暗号を復号して、異なるパケットのヘッダとペイロードを合成してパケットを生成します。このパケットは、攻撃者のWebサイトへ送付され、攻撃者はペイロード部分から、盗聴対象のマシンの情報を入手できます。これを繰り返せば、攻撃者は、盗聴対象のマシンから有益な情報を盗み出せます [45] [47]。分割した複数のフレーム（フラグメント）を処理するために、APのメモリ上へフレームを一時的に保存するのですが、このフレームの削除タイミングや管理方法が決まっていないことが、この脆弱性の原因です。

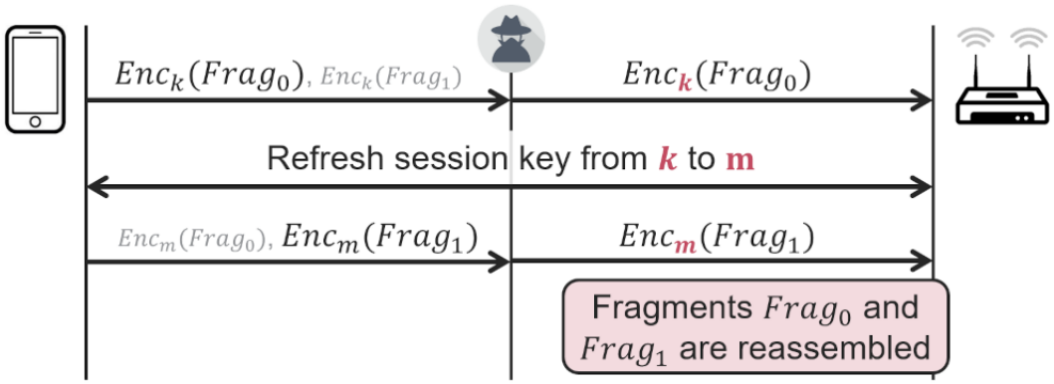


図 13 ： Mixed keyの攻撃のフロー図 [47]

4.2.3. Fragment cache攻撃

Frame fragmentationの2つ目の脆弱性 CVE2020-24586を悪用した攻撃は、Fragment cache攻撃と呼ばれています。IEEE 802.11では、断片パケットが入っている複数のフレームの再構成中に何かしらの理由で通信が遮断された場合、再構成途中のフレームがAPのメモリに残ってしまいます。攻撃者は、APへ不正なフレームを送って残存したフレームとあわせて中身の断片パケットを再構築して取り出します。Fragment Cacheを汚染

（Poisoning）する攻撃です。

以下でFragment cache攻撃の方法を説明します。

最初に攻撃者は、盗聴対象のマシンのMACアドレスを偽装してAPへ接続して、中間者攻撃を行える状態にしておきます。盗聴対象のマシンが、宛先を攻撃者へ指定したAP接続用の認証用フレームを送信します。攻撃者は、この認証用フレームの先頭部分だけを抜き出して暗号化したフレーム（図 14の"Enc_k {$Frag_0(s)$}"）を作成してAPへ送信します。すると、APはこのフレームを復号して取り出した断片パケット "$Frag_0(s)$" をメモリへ保存します。攻撃者は、APへ切断通知を送信してWi-Fiを切断します。

次に攻撃者は、もう一度、APへ接続して、最初のときと同様に中間者攻撃を行える状態にしておきます。このとき、IEEE 802.11の仕様には、Clientが切断または再接続したときに保存した断片パケットを削除する規定がないため、APのメモリには 断片パケット "$Frag_0(s)$"がそのまま残ります。この断片パケット ”$Frag_0(s)$”が、1つ目の断片パケットとなります。攻撃者は、盗聴対象のマシンから分割した複数のフレームが送信されたら、それを受信して、1つ目のフレーム（図 14の "Enc_ℓ ($Frag_0(s')$)"）を破棄します。2つ目以降のフレーム（図 14の "Enc_m ($Frag_1(s')$)", "Enc_m ($Frag_2(s')$)"…）は、APのメモリ上に残っている”$Frag_0(s)$”に合わせて、ヘッダのシーケンス番号 "s'" を"s"へ改変します。その後、この2つ目以降の不正なフレームをAPへ転送します。

最後に、4.2.2 Mixed key攻撃と同様に、APはメモリ上に保存している1つ目の断片パケット”$Frag_0(s)$”と、そのあとに受信した2つ目以降のフレーム "Enc_m{$Frag_1(s)$}、Enc_m{$Frag_2(s)$}・・・Enc_m{$Frag_x(s)$}" を暗号鍵mで復号して取り出した断片パケットをつなげてパケットを再構成します。1つ目のパケットは、宛先を攻撃者に指定しているため、APは再構成したパケットを攻撃者へ送信します。攻撃者は、このパケットを受信して、ペイロード部分から、盗聴対象のマシンの情報を入手できます。攻撃者は、4.2.2 Mixed key攻撃と同様に、これを繰り返して、盗聴対象のマシンから有益な情報を盗み出します。

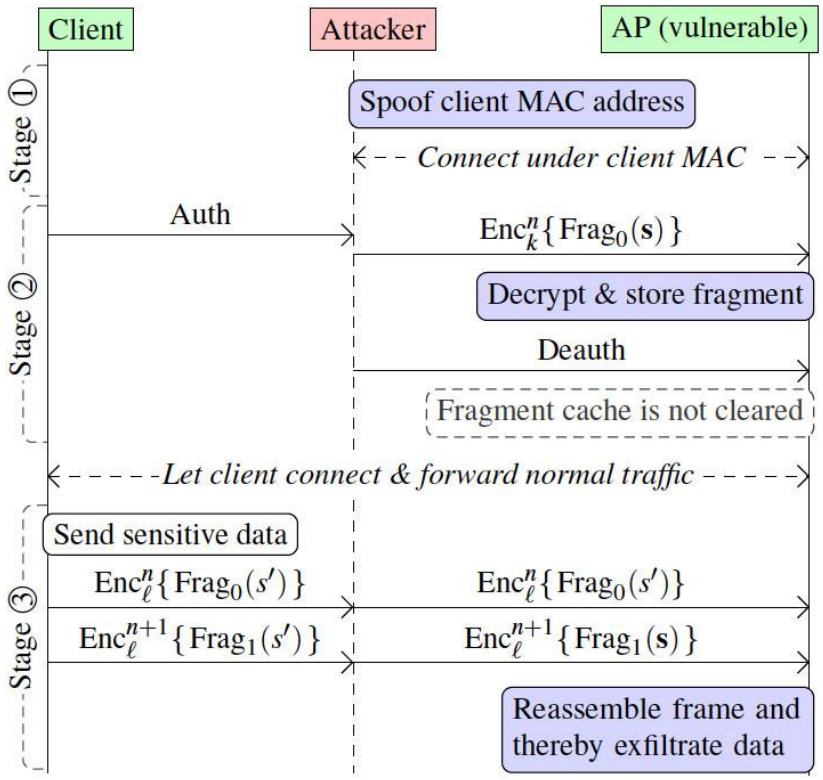


図 14 ： fragment cache攻撃のフロー図 [45]

Wi-Fi Allianceの発表によると、IEEE802.11の設計上及び実装上の脆弱性は全部で12種類あります [51]。設計上の脆弱性は上記で説明した3つで、IEEE802.11の実装上の脆弱性は9つあります。これらの12種類の脆弱性をNational Vulnerability Database(NVD)の CVSS v3のBase値が高い順番に表 11へ一覧化しました [52]。Base値は、脆弱性の基本特性をもとにして、その脆弱性の深刻度を算出した値です。

表 11 ： 脆弱性FragAttacksの一覧 [53]

CVE番号	CVSS v3 Base値	脆弱性の内容	問題の種類
CVE-2020-26139	7.8	送信者が認証されていない場合でも、EAPOLを悪用してフレームを転送する	実装上の不備
CVE-2020-26142	7.5	フラグメント化されたフレームをフルフレームとして処理する	実装上の不備
CVE-2020-26140	6.5	保護されたネットワークにおいて、平文のデータフレームを受け入れる	実装上の不備
CVE-2020-26141	6.5	フラグメント化されたフレームのTKIP MICが検証されない	実装上の不備
CVE-2020-26143	6.5	保護されたネットワークにおいて、フラグメント化された平文のデータフレームを受け入れる	実装上の不備
CVE-2020-26144	6.5	暗号化されたネットワークにおいて、EtherTypeにEAPOLが指定されたRFC1042ヘッダを持つ平文のA-MSDUフレームを受け入れる	実装上の不備
CVE-2020-26145	6.5	暗号化されたネットワークにおいて、平文のブロードキャストフラグメントをフルフレームとして受け入れる	実装上の不備
CVE-2020-26147	5.4	暗号化されたフラグメントと平文のフラグメントを混合してリアセンブルする	実装上の不備
CVE-2020-26146	5.3	連続しないパケット番号を持つ暗号化されたフラグメントをリアセンブルする	実装上の不備
CVE-2020-24586	3.5	ネットワークの再接続時にメモリからフラグメントのキャッシュがクリアされないことにより、特定の状況下において攻撃者がパケットの内容を窃取する	設計上の不備
CVE-2020-24587	3.5	異なる鍵で暗号化されたフラグメントをリアセンブルしてしまうことにより、特定の状況下において攻撃者がパケットの内容を窃取できる	設計上の不備
CVE-2020-24588	2.6	ヘッダ中のフレームアグリゲーションフラグが保護されていないため、攻撃者によりヘッダ情報を書き換えられ、不正なパケットが挿入される	設計上の不備

4.3. まとめ

FragAttacksを悪用した攻撃は、まだ報告されていません。これは、FragAttacksを実行する前提条件を満たすことが難しかったり、コストが高かったりするからです。攻撃者は、攻撃対象のマシンやWi-Fi APが使う電波が受信可能な距離に近づいたり、攻撃用の装置を設置したりしなければなりません。敷地や建物へ物理的な侵入が制限されていれば、攻撃者は攻撃対象の電波が受信できる距離へ近づけません。さらに攻撃対象との距離が300m離れると、Wi-Fiフレームの到着時間は1μs遅れます。中間者攻撃ではフレームを不正加工する時間も必要になり、フレームの受信から送信までの時間がさらに遅れるため、中間者攻撃が失敗しやすくなります。攻撃を成功するためには、高性能な攻撃用装置が必要になるでしょう。また多くの攻撃対象を攻撃したい場合は、攻撃が可能な場所へ移動するコストがかかります。

上記を踏まえると、世界各地でFragAttacksによる大量の被害が発生するとは考えにくいでしょう。しかし、世界中には脆弱な無線LAN機器が大量に存在しているため、それを放置する事はできません。できるだけ多くの無線LAN機器の管理者やWi-Fiの利用者への注意喚起が必要でしょう。インターネットセキュリティの業界団体のICASIやWi-Fi Allianceは、各ベンダ企業が公開しているアドバイザリを紹介したり、対策の必要性を説明した記事を発信したり、FragAttacksに関するさまざまな情報発信をしています [51] [54]。しかし、ユーザに指示して、世界中のすべての無線LAN機器へパッチを当てることは不可能でしょう。世界中には、パッチを当てる方法がわからないユーザがたくさんいるでしょう。管理者が不在のまま、動きつづけている無線LAN機器もたくさんあるでしょう。全ての無線LAN機器に自動的にパッチを当てるしくみが備わっていなければ、この問題はすぐに完全解決できないと思います。まだまだ先が長い対応になりそうです。

5.マルウェア・ランサムウェア

5.1. 2021年度第1四半期の概況

2020年度に引き続き、マルウェアやランサムウェアによる被害が報告されています。攻撃による被害が国民生活に大きく影響する、インフラ企業への攻撃も増えています。5月7日、米国石油パイプライン最大手のコロニアル・パイプライン社（以下、コロニアル社）がランサムウェア攻撃を受け、全パイプラインの操業を停止しました [55]。また同月31日には、ブラジル食肉最大手のJBS社がランサムウェア攻撃を受けたことを発表しました [56]。これにより、JBS社は北米と豪州の食肉処理場のシステムの停止を余儀なくされました。

本稿では、コロニアル社の事件を取り上げ、事件の経緯やコロニアル社の対応について記載します。さらに、ランサムウェア攻撃への米国の対応や日本の対応について述べます。

5.2. コロニアル社へのランサムウェア攻撃

5.2.1. 概要

2021年5月7日、米国の石油パイプライン企業であるコロニアル社が、ランサムウェア攻撃を受け、全パイプラインの操業を停止しました [55]。コロニアル社は米国東海岸の燃料消費の半分近くのシェアを占める、米国内最大手のインフラ企業です。本事案は、二重脅迫ランサムウェア攻撃 [57]を行う攻撃グループ「Darkside」による犯行でした。Darksideは、暗号化したデータを復号するための身代金として、440万ドル相当の暗号通貨の支払いをコロニアル社に要求しました。さらに、身代金を支払わなければ窃取したデータを公開すると、二重に脅迫を行いました。

当初は「コロニアル社に身代金を支払う意思はない」と報道されていましたが、後日、コロニアル社のブラウントCEOは、Darksideの要求通り身代金を支払ったことを発表しました [58]。ブラウントCEOは、「身代金の支払いが物議を醸す行動であることを承知の上で、パイプラインの停止が国民生活や経済活動に多大な影響を及ぼすリスクを考慮して、苦渋の決断を下した」と述べています [58] [59]。実際に、パイプライン停止後、米国内でガソリンの価格が急騰し、人々がガソリンを買い占める混乱が見られました。身代金の支払い後、コロニアル社はDarksideから提供された復号ツールと自社バックアップによりデータを復元し、5月15日からはパイプラインの通常操業を再開しました。

コロニアル社の事件では、被害者が身代金を攻撃グループに支払ってシステムを復旧しましたが、この事件のインシデント対応はこれで終わりではありませんでした。6月7日、

米国連邦捜査局（FBI）は、コロニアル社が支払った身代金約440万ドルのうち、約230万ドルに相当する63.7ビットコインをDarksideから奪還することに成功しました [60]。ランサムウェア攻撃のインシデント対応の結果、一度支払った身代金を回収できたことは珍しいケースです。コロニアル社の事件の時系列を以下に示します。

表 12 ： コロニアル社へのランサムウェア攻撃の時系列

日付	状況
5/6	攻撃グループ「Darkside」が2時間のうちに100Gバイト近いデータをコロニアル社ネットワークから窃取 [55] [61]
5/7	コロニアル社がランサムウェア攻撃を受けたことに気づき、全パイプラインの操業を停止。米政府やFBIへ連絡。Darksideに約440万ドルの身代金を支払い
5/10	FBIが、攻撃にDarksideランサムウェアが使われたことを発表
5/15	コロニアル社がパイプラインの通常操業を再開
6/7	米司法省は、コロニアル社が支払った身代金のうち約230万ドル相当のビットコインをFBIが奪還したと発表 [60]

5.2.2. FBIによる身代金の奪還

では、FBIは、身代金として支払われたビットコインの一部をどのような方法で差し押さえることに成功したのでしょうか。犯罪者は、身代金として得た暗号通貨を、支払われた暗号通貨アカウントからすぐにマネーロンダリング（資金洗浄）します。マネーロンダリングとは、犯罪や不正取引で得た違法な金銭を、架空口座や他人名義の口座を転々と移動させることで出所を分からなくして、警察などの捜査機関による発見や検挙を逃れようとする行為です [62]。ランサムウェアの攻撃グループは、身代金を小口に分けて複数の暗号通貨アカウントに送金したり、別の暗号通貨に変えたりすることで、マネーロンダリングを行います。

マネーロンダリングされた身代金を回収するには、以下の3つのアクションが必要です。なお、コロニアル社の事件では、FBIが以下の（１）～（３）を実現できたため、身代金を回収することができました。

（１）暗号通貨の追跡とアカウントの特定

FBIは、ブロックチェーンを検索して取引の金額や宛先を特定できるソフトウェア「ブロックチェーンエクスプローラ」を用いて、Darksideのマネーロンダリングを監視しました [63] [64]。その結果、ある1つのビットコインアカウントに63.7ビットコインが集められていることを突き止めました。

（2）ビットコインアカウントの秘密鍵の入手

FBIが、身代金が集められていたビットコインアカウントのロックを解除するための秘密鍵を入手することに成功しました。ただし、その入手方法は公表されていません。FBIがDarksideにスパイを送り込んで入手したという説や、Darkside側に裏切り者がいて秘密鍵をFBI側に漏らしたといった説がありますが、攻撃グループが秘密鍵を管理しているストレージサーバのセキュリティがずさんだったという説が濃厚だと言われています [65]。

（3）アカウント内の暗号通貨の差し押さえ

FBIは、カリフォルニア州北部地区連邦地方裁判所に、身代金の差し押さえ令状を請求しました。これを受けてすぐに裁判所が差し押さえ令状を発付して、カリフォルニア州北部地区連邦検事局の特別検察部門および資産没収部門が、ある1つのビットコインアカウントに集められたビットコインを差し押さえました [66] [67]。

コロニアル社の事件において、上記の段取りを進めることができたのは、被害者であるコロニアル社と米政府やFBIなどの法執行機関が迅速に連携したことがポイントであったと考えられます。暗号通貨の追跡自体は珍しい捜査方法ではありませんが、コロニアル社が攻撃を受けた後、早急に米政府や法執行機関と連携したことで、FBIは、身代金を支払った時点から暗号通貨の流れを徹底的に追跡することができました。FBIは、日頃から攻撃グループに関する情報収集や暗号通貨の流れの追跡を行っており、コロニアル社の事件では、その培った捜査技術を存分に活用することができたと考えられます。さらに、FBIは、カリフォルニア州の裁判所とも連携して迅速に差し押さえ令状を発付できたことで、連邦検事局が資金の差し押さえをスムーズに行うことができました。このように、コロニアル社と法執行機関が連携してランサムウェア攻撃へ対応できた背景には、OFACによる勧告やランサムウェア攻撃対策組織の設立など、米国におけるランサムウェア攻撃への取り組み強化があります。

5.2.3. 米国におけるランサムウェア攻撃への対応

米国では、ランサムウェア攻撃への危機感が高まっており、国を挙げて対応の強化が進められています。ここでは、その具体的な動きとして、身代金の支払いに関する勧告の発令とランサムウェア攻撃対策組織の発足について述べます。

2020年10月、米国財務省の外国資産管理局（OFAC）より、身代金の支払いに関する勧告が発表されました。これは2020年度第3四半期レポートでも取り上げました [57]。勧告の内容は、攻撃グループに身代金を支払った組織は罰金と制裁の対象となる場合があり、攻撃を受けた場合は速やかに法執行機関に報告して協力しなければならない、というものです。

さらに米国では、2021年1月、Ransomware Task Force (RTF)というランサムウェア攻撃対策組織が発足しました [68]。ランサムウェア攻撃は日々増えており、規模も拡大しています。ところが、対策が不十分な組織は少なくなく、ランサムウェア攻撃による被害は増加し、またそれぞれの被害が深刻化しているのが現状です。そこで、ランサムウェア攻撃への対応のフレームワークを標準化して、組織横断的に攻撃に立ち向かうことを目的として、本組織が結成されました。RTFは、AmazonやCisco、Microsoftといった大手IT企業や政府機関、法律事務所、学術機関など、60以上のメンバで構成されています。RTFからは、ランサムウェア攻撃に対して政府や企業が取るべき行動をまとめたレポート（RTF Report）が発表されています [69]。RTF Reportでは、以下に示す４つの目標が掲げられています（ [69]より引用)。

表 13 ： RTF Reportが掲げる目標

目標	実施内容
①国内外で連携してランサムウェア攻撃を抑止する	ランサムウェア攻撃を抑止するためには、各国が国力を駆使して取り組むこと、そして国際的に協力することが必要です。各国に捜査の優先度を上げるよう呼びかけ、攻撃グループをかくまう国家へ圧力をかけます。さらに、ランサムウェアのテイクダウンにも国際的に協力して取り組みます。
②攻撃グループの活動を妨害する	ランサムウェア攻撃の被害を減らすためには、攻撃グループのビジネスモデルを崩すことも必要です。攻撃による収益性を下げたり、攻撃者側のリスクを増加させたりします。また、刑事訴追等で攻撃グループのメンバを追い詰めます。
③組織のランサムウェア攻撃対策を支援する	多くの組織は、ランサムウェア攻撃への対策がまだ不十分です。各組織に注意喚起を行い、各組織が適切に情報を得られるように、またそれぞれの現状に応じた対策を施せるようサポートします。
④ランサムウェア攻撃へ効果的にインシデント対応する	データが永久に戻らないことや自組織の信頼失墜を恐れて、被害者が焦って身代金を支払ってしまうケースも少なくありません。身代金を支払う前に政府に報告するよう周知することや、被害者を適切にサポートする環境を整えます。

RTF Reportには、表 13の目標を達成するための48の推奨事項が記載されており、多くの項目に官民の垣根を超えて組織横断的に対応するための具体的な方法が記載されています。例えば、目標②を達成する推奨項目として、「暗号通貨取引所、仮想キオスク、店頭取引デスクに現行法の遵守を求める」という記載があります。コロニアル社のケースと同様に、攻撃者は、ランサムウェア攻撃の身代金を暗号通貨で支払うことを求めます。攻撃グループが身代金として得た暗号通貨をマネーロンダリング後に現金化する場合は、暗号通貨取引所等を経由します。そのため、RTF Reportは、暗号通貨取引所等に対して、KYC

（Know Your Customer：顧客の身元確認）やAML（Anti-Money Laundering：マネーロンダリングの防止）、CFT（Combatting Financing of Terrorism：テロ資金供与防止）に関する法律を守るよう求めています。暗号通貨取引所がこれら推奨項目を強化すれば、攻撃グループが、暗号通貨取引所に口座を開設できなかったり、マネーロンダリングできなかったりするため、身代金を現金化できません。

5.3. 日本におけるランサムウェア攻撃への対応

5.2.では、米国におけるランサムウェア攻撃への取り組みについて述べました。5.3では、日本政府や国内の法執行機関の、ランサムウェア攻撃への現在の対応方法を取り上げてみます。

日本の組織がランサムウェア攻撃を受けて被害届を提出した場合は、都道府県警に設置されているサイバー犯罪捜査課などのサイバー犯罪を扱う部署が中心となって、捜査を行います。しかし、地方ではサイバー犯罪に精通した人員が少なく、都道府県警間で捜査レベルに差があったり、企業や法執行機関との連携や海外の捜査機関との連携が難しかったりするのが現状です。各都道府県警のサイバー犯罪対応部署だけでは、最新のサイバー犯罪への対応力に限界があります。

その問題を解決するための一歩目として、2022年度、警察庁に「サイバー局」が設置されることが発表されました [70] [71]。現在、警察庁の生活安全局や警備局等にまたがって扱われているサイバー事案が、サイバー局で一元的に管理されます。また、国直轄の専門捜査部隊（「サイバー直轄隊（仮称）」）が新たに設けられ、全国から集められた専門知識を持つ捜査員約200人が重大なサイバー攻撃の捜査に当たります。国の直轄部隊として警察庁がサイバー事案を直接捜査することで、サイバー事案に関する情報収集・分析の強化や捜査技術の向上が見込まれます。また、民間企業との連携や世界各国との連携が行われやすくなることも期待されています。

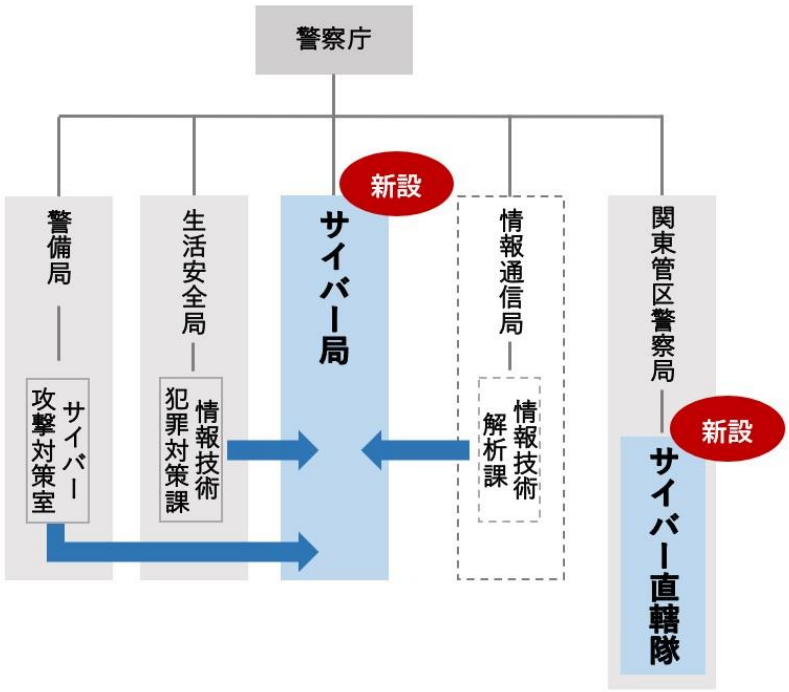


図 15 ： 警察庁組織改編案のイメージ [72]

（出典より筆者改変）

一方で、強化しなければならないのは、警察の捜査体制だけではありません。日本は、ランサムウェア攻撃への対応を、国を挙げてより強化する必要があります。まずは、もしランサムウェア攻撃を受けて被害が発生してしまった場合に、被害組織が身代金の支払いやシステムの復旧に関して適切な意思決定をできるように情報を提供すべきと考えます。米国のように身代金を取り返せる体制を整えることは難しいと思いますが、日本は、次にランサムウェア攻撃を受けるおそれがある組織へ、ランサムウェア対策をもっと普及させるべきです。そのためには、官民が連携する体制を整えて、多方面からランサムウェア対策の普及施策を展開するべきです。米国がOFACによる勧告やRTFによる提言を普及展開したように、日本政府には、各業界と法執行機関、司法機関、行政機関をまとめた横断組織を作ることや、国内のランサムウェア対策施策の具体的な指示を出すことが求められています。

5.4. まとめ

本稿では、コロニアル社の事件を取り上げ、この事件が一度支払った身代金の一部を回収することができた珍しいケースであったことを説明しました。そして、米国では国を挙げた組織横断的なランサムウェア攻撃への取り組みがあることを紹介し、米国と日本のランサムウェア攻撃への取り組み状況を比較しました。

コロニアル社の事件における身代金の回収は、あくまで身代金を支払った後の特殊な対応方法です。ランサムウェア対策は、まずはランサムウェア攻撃を未然に防ぐこと、そして攻撃を受けたとしても被害を最小限に抑えるように対応することです。ランサムウェア対策が不十分な組織は、この２つの対策を整えるべきです。しかし、各組織のランサムウェア対策は、あまり進んでいません。特に日本は、政府を中心にランサムウェア攻撃への対応をより強化する必要があります。政府として取り組むべきことは、被害組織と公的機関が迅速に連携できる、組織横断的な対応ができる体制を整えることです。その一歩目として、政府は、攻撃を受けた被害組織が、真っ先に頼ることができるような組織や仕組みをつくることからはじめるべきではないでしょうか。被害組織がシステムの復旧や身代金の支払いに関して適切な意思決定を行えるように情報提供を行ったり、被害組織が取るべき具体的な行動を指示したりして、被害を最小限に抑えるための支援ができる官民横断の組織が求められています。

6.予測

攻撃グループに関係する国家の名指し批判

サイバー攻撃を行った攻撃グループやその犯罪に関与した国家に対して、被害国が名指しで批判を行う動きがあります。2021年4月、警察庁は、2016年から2017年にかけて宇宙航空研究開発機構（JAXA）をはじめとする日本国内の研究機関や企業へ行われたサイバー攻撃は、中国人民解放軍が攻撃を指示した疑いが強いことを発表しました [73]。このような名指し批判は、日本だけでなく、米国のバイデン大統領がロシアのプーチン大統領にサイバー攻撃を阻止するよう求めるなど、世界的に行われています [74] [75]。

５章では、ランサムウェア攻撃対策組織であるRTFが、攻撃グループをかくまう国家へ圧力をかけることを推奨していることを述べました。これと関連して、他のあらゆるサイバー攻撃においても、被害国の政府は、サイバー攻撃に対抗する姿勢を示していく必要があります。自国の組織がサイバー攻撃された場合、その組織が被害を受けるだけでなく、国民の生活基盤や経済基盤にも大きな影響がおよび、国全体が被害を受ける場合があります。そのため、被害国は、攻撃グループに関係する国家へ政治的に対応を要求する必要があり、その手段として名指し批判は今後も増加すると考えられます。

この動きにより、国家に支援されている攻撃グループは、関係する国家の特定を防ぐため、攻撃グループが特定されないように、より身元が特定される情報を隠すようになると考えられます。具体的には、攻撃の痕跡が解析されないようにしたり、残った痕跡から身元がばれないようにしたり、わざと他の攻撃グループによる犯行に見せかけたりするなど、身元がばれないよう工夫することが推測されます。

新型コロナウイルス再流行の場合のサイバー攻撃

新型コロナウイルスのワクチン接種も進み、死者数も減少傾向であることから、このまま新型コロナウイルスが収束に向かう可能性もあります。一方で、ワクチンの効果が弱くなるおそれもあることや、寒くなりウイルスの感染力が高くなることから、新型コロナウイルスが再流行し、ワクチン接種が再度必要になるおそれもあります。

現状進行中のワクチン接種の際には、ワクチン接種の関心が高まったことにより、ワクチン予約サイト装い個人情報やクレジットカード情報を窃取する等のワクチンに関する情報を悪用したフィッシング攻撃が、各国で発生しました [76] [77] [78]。ワクチン接種が再度必要になった場合には、同様の攻撃が再び発生するでしょう。

アフターコロナ移行の場合のサイバー攻撃

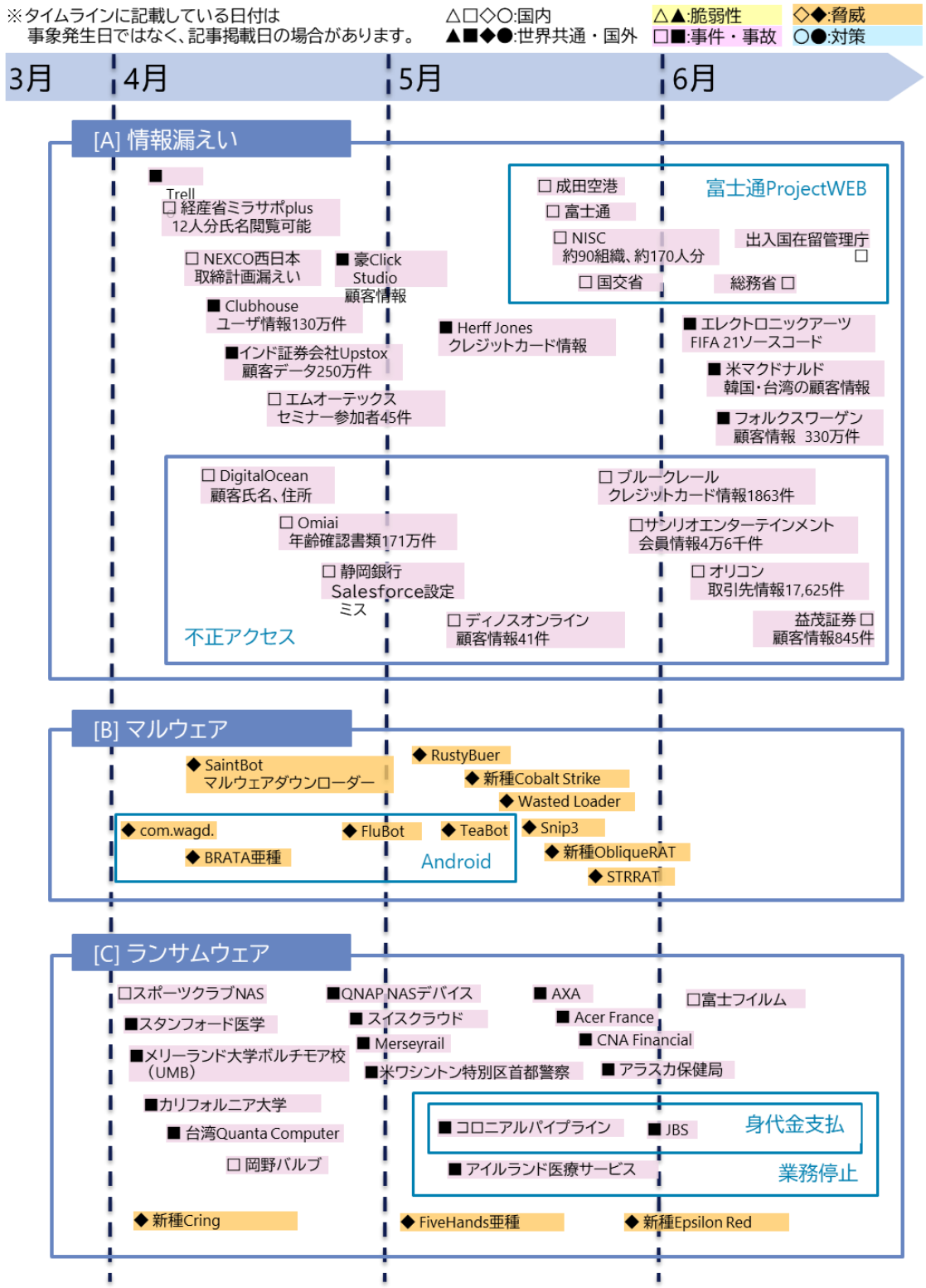
新型コロナウイルスのワクチン接種も進み、死者数も減少傾向であることから、世の中の経済活動やレジャーは回復し始めています。この状況が続く場合、今まで新型コロナウイルスに関連した事象を狙っていたサイバー攻撃も、アフターコロナにおいてお金がある箇所を狙うように変化するのではないでしょうか。次のようなサイバー攻撃が発生すると想定します。

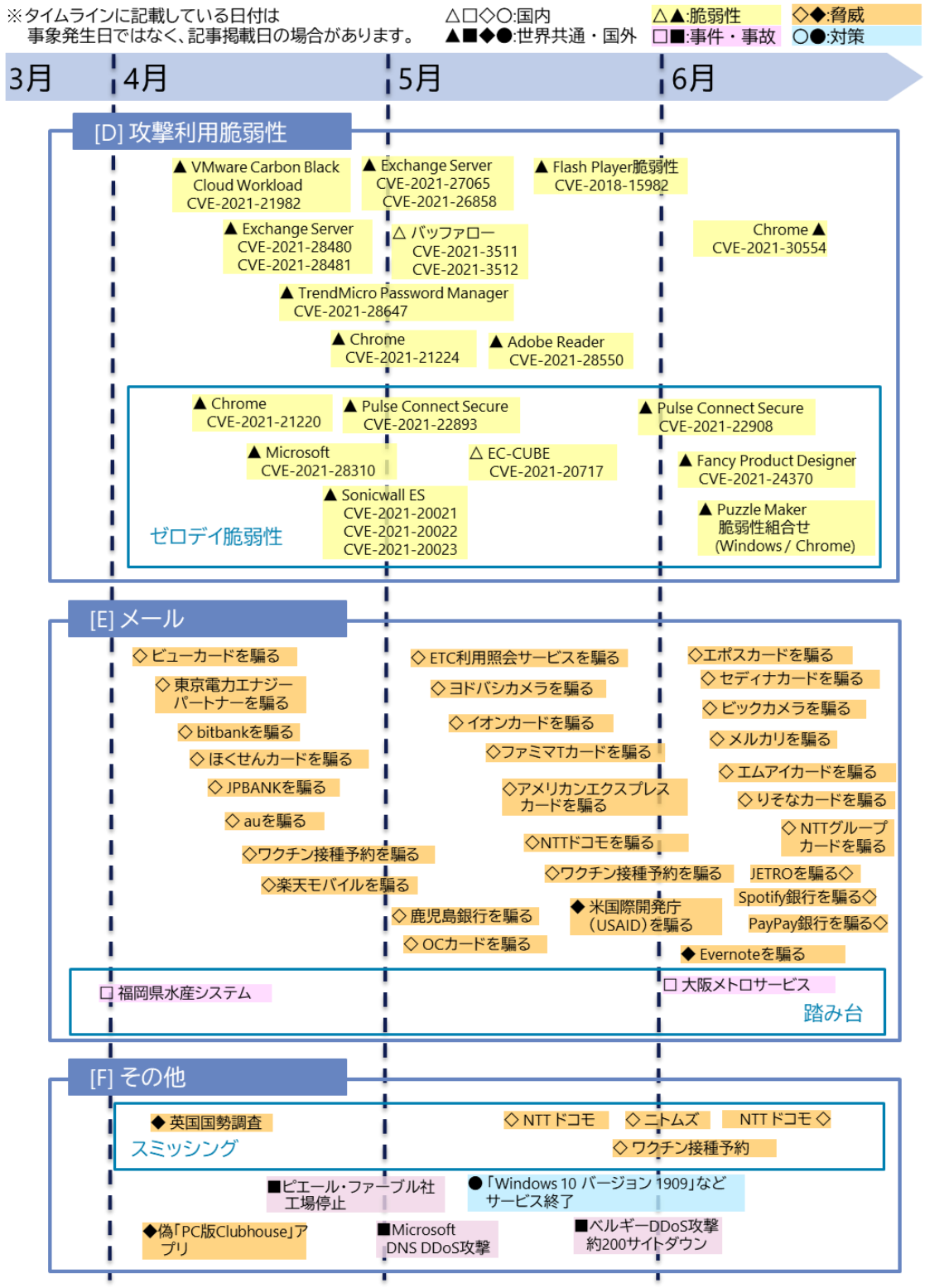
１つ目は、製薬会社やヘルスケア産業を狙った攻撃です。新型コロナウイルスのワクチンを開発した製薬会社は、売り上げ増により業績が好調です。ワクチンの供給量も安定して新型コロナウイルスの危険性がコントロールできるようになってきていることから、攻撃者は、製薬会社を狙うおそれが高いと予測します。

２つ目は、レジャーに関連したフィッシング攻撃です。コロナ禍で遊びや旅行を諦めていた人々は、レジャーに飢えています。アフターコロナ後は、人々はコロナ禍の制限から解放されて、これまでのストレスを発散するために、インターネット上でさまざまなレジャーの情報を調べたり、申し込んだりするでしょう。攻撃者は、そこに目をつけるでしょう。レジャーを求めているユーザを騙そうと、レジャーに関連した内容のフィッシングメールやフィッシングサイトが増加するでしょう。

３つ目は、新型コロナウイルス後の経済回復にあわせて盛り上がってくる新しいビジネスや投資を狙った攻撃です。新しいビジネスやビジネスが回復してきた企業に対して多くの投資が行われると想定されます。攻撃者は、大企業だけでなく、ベンチャー企業のような中小企業も積極的に攻撃するでしょう。

7.タイムライン





参考文献

[1] トレンドマイクロ株式会社, “Water Pamola Attacked Online Shops Via Malicious Orders,” 28 4 2021. [オンライン]. Available: https://www.trendmicro.com/en_us/research/21/d/water-pamola-attacked-online-shops-via-malicious-orders.html.

[2] “クレジットカード情報漏洩事件のまとめ（2021年上半期）,” 14 7 2021. [オンライン]. Available: https://foxestar.hatenablog.com/entry/2021/02/09/110000.

[3] 株式会社イーシーキューブ, “EC-CUBE 4.0系: クロスサイトスクリプティング脆弱性（JVN#97554111）について,” 7 5 2021. [オンライン]. Available: https://www.ec-cube.net/info/weakness/20210507/.

[4] 株式会社イーシーキューブ, “【重要】EC-CUBE 4.0系における緊急度「高」の脆弱性(JVN#97554111)発覚と対応のお願い,” 7 5 2021. [オンライン]. Available: https://www.ec-cube.net/news/detail.php?news_id=383.

[5] JPCERT/CC, “EC-CUBEのクロスサイトスクリプティングの脆弱性（CVE-2021-20717）に関する注意喚起,” 10 5 2021. [オンライン]. Available: https://www.jpcert.or.jp/at/2021/at210022.html.

[6] JVN, “JVN#97554111　EC-CUBE におけるクロスサイトスクリプティングの脆弱性,” 10 5 2021. [オンライン]. Available: https://jvn.jp/jp/JVN97554111/.

[7] 株式会社イーシーキューブ, “EC-CUBE3.0におけるクロスサイトスクリプティングの脆弱性(JVN#95292458),” 10 6 2021. [オンライン]. Available: https://www.ec-cube.net/info/weakness/20210610/index30.php.

[8] 株式会社イーシーキューブ, “EC-CUBE4.0におけるクロスサイトスクリプティングの脆弱性(JVN#95292458),” 10 6 2021. [オンライン]. Available: https://www.ec-cube.net/info/weakness/20210610/index40.php.

[9] JVN, “JVN#95292458　EC-CUBE における複数のクロスサイトスクリプティングの脆弱性,” 23 6 2021. [オンライン]. Available: https://jvn.jp/jp/JVN95292458/.

[10] JPCERT/CC, “複数のEC-CUBE 3.0系用プラグインにおけるクロスサイトスクリプティングの脆弱性に関する注意喚起,” 15 6 2021. [オンライン]. Available: https://www.jpcert.or.jp/at/2021/at210028.html.

[11] JVN, “JVN#79254445　複数の ETUNA 製 EC-CUBE 用プラグインにおけるク

ロスサイトスクリプティングの脆弱性,” 15 6 2021. [オンライン]. Available: https://jvn.jp/jp/JVN79254445/.

[12] JVN, “JVN#57524494　複数のイーシーキューブ製 EC-CUBE 用プラグインにおける複数のクロスサイトスクリプティングの脆弱性,” 15 6 2021. [オンライン]. Available: https://jvn.jp/jp/JVN57524494/.

[13] IPA, “「クロスサイト・スクリプティング（XSS）の脆弱性の種類」,” [オンライン]. Available: https://www.ipa.go.jp/files/000024726.pdf.

[14] SSTバックヤード, “Stored(蓄積型)-XSSの危険性,” 15 4 2020. [オンライン]. Available: https://techblog.securesky-tech.com/entry/2020/04/15/.

[15] JPCERT/CC, “ECサイトのクロスサイトスクリプティング脆弱性を悪用した攻撃,” 6 7 2021. [オンライン]. Available: https://blogs.jpcert.or.jp/ja/2021/07/water_pamola.html.

[16] 株式会社イーシーキューブ, “セキュリティ対策について｜ご利用のEC-CUBEのバージョンを確認する,” [オンライン]. Available: https://www.ec-cube.net/info/security/#securit_flow01.

[17] 株式会社イーシーキューブ, “EC-CUBE2・3・4系ダウンロード,” 29 6 2021. [オンライン]. Available: https://www.ec-cube.net/download/other.php.

[18] “3.0系|配送伝票番号プラグイン(3.0系)|ETUNA,” 19 6 2021. [オンライン]. Available: https://www.ec-cube.net/products/detail.php?product_id=1001.

[19] “3.0系|配送伝票番号csv一括登録プラグイン(3.0系)|ETUNA,” 19 6 2021. [オンライン]. Available: https://www.ec-cube.net/products/detail.php?product_id=1007.

[20] “3.0系|配送伝票番号メールプラグイン(3.0系)|ETUNA,” 19 6 2021. [オンライン]. Available: https://www.ec-cube.net/products/detail.php?product_id=1089.

[21] 株式会社イーシーキューブ, “3.0系|帳票出力プラグイン|株式会社イーシーキューブ,” 14 6 2021. [オンライン]. Available: https://www.ec-cube.net/products/detail.php?product_id=959.

[22] 株式会社イーシーキューブ, “3.0系|メルマガ管理プラグイン|株式会社イーシーキューブ,” 14 6 2021. [オンライン]. Available: https://www.ec-cube.net/products/detail.php?product_id=960.

[23] 株式会社イーシーキューブ, “3.0系|カテゴリコンテンツプラグイン|株式会社イーシーキューブ,” 14 6 2021. [オンライン]. Available: https://www.ec-cube.net/products/detail.php?product_id=1070.

[24] 株式会社イーシーキューブ, “EC-CUBEプラグインをつくろう！ | ECサイト構

築・リニューアルは「ECオープンプラットフォームEC-CUBE」,” [オンライン]. Available: https://www.ec-cube.net/plugin/.

[25] EC-CUBE開発チーム, “html_entity_decodeを使っている箇所を修正,” 15 6 2021. [オンライン]. Available: https://github.com/EC-CUBE/ProductReview-plugin/pull/71/files.

[26] 株式会社イーシーキューブ, “カテゴリコンテンツプラグイン バージョン1.0.1をリリースしました。,” 14 6 2021. [オンライン]. Available: https://www.ec-cube.net/release/detail.php?release_id=5092.

[27] “「Codecov」への第三者からの不正アクセスによる当社への影響および一部顧客情報等の流出について,” [オンライン]. Available: https://about.mercari.com/press/news/articles/20210521_incident_report/.

[28] “Bash Uploader Security Update,” [オンライン]. Available: https://about.codecov.io/security-update/.

[29] “【調査結果のご報告】「Codecov」への第三者からの不正アクセスによる 当社への影響および一部顧客情報等の流出について,” [オンライン]. Available: https://about.mercari.com/press/news/articles/20210806_incident_report/.

[30] “メルカリ、顧客情報など2万7千件流出　不正アクセスで,” [オンライン]. Available: https://www.asahi.com/articles/ASP5P6DCLP5PULFA02M.html.

[31] “グローバルセキュリティ動向四半期レポート2019 年度 第 1 四半期,” [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_1q_securityreport.pdf.

[32] “メルカリを攻撃したcodecovのサプライチェーン攻撃の全貌：攻撃者のIPアドレスと攻撃者はどこの国？,” [オンライン]. Available: https://www.prsol.cc/?p=862.

[33] “グローバルセキュリティ動向四半期レポート2020 年度 第 3 四半期,” [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2020_3q_securityreport.pdf.

[34] 株式会社日経新聞社, “婚活アプリ「Omiai」会員情報流出　最大171万,” [オンライン]. Available: https://www.nikkei.com/article/DGXZQOUC21AEV0R20C21A5000000/.

[35] 株式会社朝日新聞社, “婚活アプリの個人情報が流出か　免許証など171万件,”

[オンライン]. Available:
https://digital.asahi.com/articles/ASP5P5Q3PP5PULFA02S.htm.

[36] SBクリエイティブ株式会社, “eKYCとは何か？ 本人確認や銀行口座連携の手法、関連サービスを解説,” [オンライン]. Available:
https://www.sbbit.jp/article/fj/46184.

[37] 経済産業省, “オンラインサービスにおける身元確認手法の整理に関する検討報告書,” [オンライン]. Available:
https://www.meti.go.jp/press/2020/04/20200417002/20200417002-3.pdf.

[38] 金融庁, “オンラインで完結する自然人の本人特定事項の確認方法の追加,” [オンライン]. Available: https://www.fsa.go.jp/news/30/sonota/20181130/01.pdf.

[39] 金融庁, “犯罪収益移転防止法におけるオンラインで完結可能な本人確認方法の概,” [オンライン]. Available:
https://www.fsa.go.jp/common/law/guide/kakunin-qa/2.pdf.

[40] 鈴. 淳也, “マイナンバーカードとJPKIで本人確認の仕組みは普及するか,” [オンライン]. Available:
https://www.watch.impress.co.jp/docs/series/suzukij/1313080.html.

[41] 警察庁, “犯罪統計,” [オンライン]. Available:
https://www.npa.go.jp/publications/statistics/sousa/statistics.html.

[42] 株式会社TIプランニング, “顔写真の自動照合機能を搭載したIC免許証の本人確認パッケージ（NEC）,” [オンライン]. Available:
https://paymentnavi.com/cardnavi/19152.html.

[43] TRUSTDOCK, “eKYC身分証アプリ「TRUSTDOCK」にて、三菱UFJ銀行の「本人確認サポート（個人） APIサービス」との連携による、犯収法eKYC[ト1]の提供を今夏より開始。顔写真が不要なeKYCが可能に。,” [オンライン]. Available:
https://prtimes.jp/main/html/rd/p/000000066.000033766.html.

[44] 総務省, “公的個人認証サービスの利活用について,” [オンライン]. Available:
https://www.soumu.go.jp/main_content/000324414.pdf.

[45] M. Vanhoef, “Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation,” [オンライン]. Available:
https://papers.mathyvanhoef.com/usenix2021.pdf.

[46] ASCII.jp, “無線LAN規格「IEEE802.11」について知ろう,” [オンライン]. Available: https://ascii.jp/elem/000/000/455/455925/.

[47] M. Vanhoef, “FragAttacks,” [オンライン]. Available:

https://www.fragattacks.com/.

[48] 永. 健. 康. 健. 泰司, “IEEE802.11とWi-Fi Allianceにおける 無線LANの標準化動向,” [オンライン]. Available: https://www.ntt.co.jp/journal/1002/files/jn201002077.pdf.

[49] TechTarget, “Wi-Fiデバイスのほぼ全てに影響　無線LANの脆弱性「FragAttacks」とは？,” [オンライン]. Available: https://techtarget.itmedia.co.jp/tt/news/2106/19/news01.html.

[50] M. Vanhoef, “FragAttacks: Presentation at USENIX security’21,” [オンライン]. Available: https://www.youtube.com/watch?v=OJ9nFeuitIU.

[51] ICASI, “Statement from the Industry Consortium for Advancement of Security on the Internet (ICASI) on Aggregation and Fragmentation Attacks against Wi-Fi,” [オンライン]. Available: https://www.icasi.org/aggregation-fragmentation-attacks-against-wifi/.

[52] NIST, “NVD - Search and Statistics - National Vulnerability Database,” [オンライン]. Available: https://nvd.nist.gov/vuln/search.

[53] Japan Vulnerability Notes, “JVNVU#93485736　IEEE802.11 規格のフレームアグリゲーションやフラグメンテーションに関する複数の問題（FragAttack）,” [オンライン]. Available: https://jvn.jp/vu/JVNVU93485736/.

[54] Wi-Fi Alliance, “Wi-Fi Alliance® security update – May 11, 2021 | Wi-Fi Alliance,” [オンライン]. Available: https://www.wi-fi.org/security-update-fragmentation.

[55] Bloomberg, “Colonial Hackers Stole Data Thursday Ahead of Shutdown,” 9 5 2021. [オンライン]. Available: https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown.

[56] BBC NEWS JAPAN, “世界最大の食肉加工会社にサイバー攻撃、米豪の工場が停止　ロシアの犯罪集団関与か,” 2 6 2021. [オンライン]. Available: https://www.bbc.com/japanese/57325741.

[57] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート（2020年度版　第3四半期）,” 16 3 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2020_3q_securityreport.pdf.

[58] THE WALL STREET JOURNAL, “Colonial Pipeline CEO Tells Why He Paid Hackers

a $4.4 Million Ransom,” 19 5 2021. [オンライン]. Available: https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636.

[59] CNN, “Colonial Pipeline CEO defends his handling of ransomware attack that crippled East Coast fuel supply,” [オンライン]. Available: https://edition.cnn.com/2021/06/08/politics/colonial-pipeline-ceo-on-capitol-hill-ransomware/index.html. [アクセス日: 8 6 2021].

[60] BBC NEWS JAPAN, “サイバー被害の米パイプライン、身代金の大半を回収　米司法省が発表,” 8 6 2021. [オンライン]. Available: https://www.bbc.com/japanese/57394900.

[61] REUTERS, “米コロニアル・パイプラインのハッカー、大量のデータを窃盗＝ＢＢＧ,” 9 5 2021. [オンライン]. Available: https://jp.reuters.com/article/usa-products-colonial-pipeline-idJPKBN2CQ03O.

[62] JAFIC, “マネーロンダリング対策の沿革,” [オンライン]. Available: https://www.npa.go.jp/sosikihanzai/jafic/maneron/manetop.htm. [アクセス日: 21 7 2021].

[63] Yahoo! ニュース, “FBIはどうやってハッカーから身代金を取り戻したのか,” 11 6 2021. [オンライン]. Available: https://news.yahoo.co.jp/articles/3d24553a6e171339e9e88388746d1271982bc19e.

[64] npr, “How A New Team Of Feds Hacked The Hackers And Got Colonial Pipeline's Ransom Back,” 8 6 2021. [オンライン]. Available: https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac.

[65] CNBC, “The FBI likely exploited sloppy password storage to seize Colonial Pipeline bitcoin ransom,” 9 6 2021. [オンライン]. Available: https://www.cnbc.com/2021/06/08/fbi-likely-exploited-sloppy-password-storage-to-seize-colonial-ransom.html.

[66] “Seizure Warrant,” [オンライン]. Available: https://www.scribd.com/document/510927692/Seizure-Warrant#download&from_embed.

[67] THE UNITED STATES DEPARTMENT of JUSTICE, “Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside,” 7 6 2021. [オンライン]. Available: https://www.justice.gov/opa/pr/department-

justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[68] Institute for SECURITY+TECHNOLOGY, “RANSOMWARE TASK FORCE,” [オンライン]. Available: https://securityandtechnology.org/ransomwaretaskforce/. [アクセス日: 20 7 2021].

[69] Institute for SECURITY+TECHNOLOGY, “RTF Report: Combatting Ransomware,” [オンライン]. Available: https://securityandtechnology.org/ransomwaretaskforce/report/. [アクセス日: 20 7 2021].

[70] 朝日新聞, “警察庁がサイバー局を新設へ　自ら捜査する「直轄隊」も,” 24 6 2021. [オンライン]. Available: https://www.asahi.com/articles/ASP6S3DBNP6RUTIL06J.html.

[71] NHK, “警察庁「サイバー局」新設へ 重大なサイバー犯罪の独自捜査も,” 24 6 2021. [オンライン]. Available: https://www3.nhk.or.jp/news/html/20210624/k10013101201000.html.

[72] 朝日新聞, “警察庁、対サイバー体制強化　局新設方針／自ら捜査へ直轄隊,” 25 6 2021. [オンライン]. Available: https://www.asahi.com/articles/DA3S14950563.html?pn=3.

[73] NHK, “JAXAなどに大規模なサイバー攻撃 中国人民解放軍の指示か,” [オンライン]. Available: https://www3.nhk.or.jp/news/html/20210420/k10012984761000.html. [アクセス日: 20 4 2021].

[74] 産経新聞, “米露首脳が電話会談　バイデン氏サイバー攻撃阻止要求,” 10 7 2021. [オンライン]. Available: https://www.sankei.com/article/20210710-BYXSB5KZ2ZMGHMGE67UURCDMCA/.

[75] REUTERS, “ノルウェー議会へのサイバー攻撃、中国が発信源＝外相,” 19 7 2021. [オンライン]. Available: https://jp.reuters.com/article/norway-cyber-idJPKBN2EP1GO.

[76] FEDERAL BUREAU OF INVESTIGATION, “Federal Agencies Warn of Emerging Fraud Schemes Related to COVID-19 Vaccines,” FEDERAL BUREAU OF INVESTIGATION, 20 12 2020. [オンライン]. Available: https://www.fbi.gov/news/pressrel/press-releases/federal-agencies-warn-of-emerging-fraud-schemes-related-to-covid-19-vaccines.

[77] BBC., “Beware fake Covid vaccination invites, NHS warns,” BBC., 26 1 2021. [オンライン]. Available: https://www.bbc.com/news/technology-55811161.

[78] 宇. 充, “新型コロナワクチン関連のフィッシング詐欺に要注意。防衛省や厚労省が呼びかけ,” 株式会社インプレス Impress Corporation, 31 8 2021. [オンライン]. Available: https://pc.watch.impress.co.jp/docs/news/1347158.html.

[79] 経済産業省, “株式会社イーシーキューブが提供するサイト構築パッケージ「EC-CUBE」の脆弱性等について（注意喚起）,” 20 12 2019. [オンライン]. Available: https://www.meti.go.jp/press/2019/12/20191220013/20191220013.html.

[80] IPA, “ECサイト構築で多く利用されている「EC-CUBE」を用いたウェブサイトでの情報漏えい被害の増加について,” 25 12 2019. [オンライン]. Available: https://www.ipa.go.jp/security/announce/alert20191225.html.

[81] 情報処理推進機構, “情報セキュリティ　10大脅威 2021,” 2 2021. [オンライン]. Available: https://www.ipa.go.jp/files/000088835.pdf.

[82] 国土交通省, “令和２年度　テレワーク人口実態調査　－調査結果の抜粋－,” 3 2021. [オンライン]. Available: https://www.mlit.go.jp/report/press/content/001391381.pdf.

[83] 総務省, “サイバー攻撃の最近の動向等について,” 3 12 2020. [オンライン]. Available: https://www.soumu.go.jp/main_content/000722477.pdf.

[84] 朝日新聞DIGITAL, “三菱電機へのサイバー攻撃、VPN装置にハッキングか,” 2 5 2020. [オンライン]. Available: https://www.asahi.com/articles/ASN517HP7N4XULZU012.html.

[85] 朝日新聞DIGITAL, “狙われた、社内への「接続口」　三菱電機へのサイバー攻撃、ＶＰＮ経由か,” 8 5 2020. [オンライン]. Available: https://www.asahi.com/articles/DA3S14468115.html.

[86] cnet Japan, “世界中で医療機関へのサイバー攻撃が頻発、2020年11月に45％増--ランサムウェア多用,” 8 1 2021. [オンライン]. Available: https://japan.cnet.com/article/35164749/#:~:text=%E5%8C%BB%E7%99%82%E9%96%A2%E4%BF%82%E6%A9%9F%E9%96%A2%E3%81%AB%E5%AF%BE%E3%81%99%E3%82%8B%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E6%94%BB%E6%92%83%E3%81%AE%E5%A2%97%E5%8A%A0%E7%8E%87%E3%82%92%E5%9C%B0%E5%9F%9.

[87] FBI, “FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19)

Pandemic,” 21 3 2021. [オンライン]. Available: https://www.ic3.gov/Media/Y2020/PSA200320.

[88] FBI, “FBI Urges Vigilance During COVID-19 Pandemic,” [オンライン]. Available: https://www.fbi.gov/coronavirus.

NTT DATA
Trusted Global Innovator

2021年11月2日発行

株式会社NTTデータ
セキュリティ技術部
大谷 尚通 / 大山 千尋 / 宮本 久仁男 / 大石 眞央 / 板山 健司郎 / 王 一帆 /
宮崎 大輔 / 中道 美澄 / 大山 正純 / 神谷 優治 / 佐々木 俊彦 / 瀧田 美香
nttdata-cert@kits.nttdata.co.jp