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

2020 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。

改正個人情報保護法の施行

2022年（令和4年）に改正個人情報保護法が施行されます。企業活動のグローバル化やデジタル化に伴い、個人データの海外への移転が増加していることを背景に、改正個人情報保護法では海外移転する個人データの取り扱い方法が変更されます。今年3月に、LINE社の保有する個人データが海外に保管されていたことがニュースになりました。個人情報保護法の現行法を論拠に、個人情報保護委員会よりLINE社の海外委託先の監督不足が指摘されています。また、現行法では問題がないが、改正法ではLINE社の対応が必要な箇所もあります。本稿では、LINE社の事例を元に個人データの海外移転に関する新旧個人情報保護法の違いと、必要な企業の対応を解説します。企業が個人情報を適切に扱うには、個人情報を管理可能な体制と適切な管理方法の実践が必要です。これらの対応には、個人情報保護の規格であるJIS Q 15001（個人情報保護マネジメントシステム-要求事項）を用いた活動が効果的です。自社がJIS Q 15001へ準拠して個人情報保護を推進していることを社外へアピールするには、プライバシーマーク認定を取得することもできます。

証券システム開発者による顧客預金の横領

松井証券株式会社は、証券取引システムの開発・運用業務委託先の元従業員により、顧客の証券口座から約2億円が不正に出金されたことを公表しました。本事件は犯行開始から発覚まで2年半かかっており、長期間関係者の目をすり抜けた要因が複数存在することが判明しています。本事件の詳細を解説し、金融システムに携わる運用部門と開発部門が実施すべきセキュリティ対策を解説します。また、顧客目線で被害を防ぐ方法、早期発見する方法を提案します。

Microsoft Exchange Serverに発生した脆弱性

2021年3月にMicrosoft社は定例外のセキュリティ更新プログラムを公開しました。攻撃者は、これらの脆弱性を悪用して、別サーバ経由で本来アクセスできないExchange Serverへ443ポートを介してアクセスして認証を突破し、管理者に成りすますことが可能です。この更新プログラムが修正する７つの脆弱性のうち、４つの脆弱性はゼロディ脆弱性で、すでに更新プログラムの提供前から攻撃グループによる活発な攻撃やランサムウェアの被害が確認されています。インターネット上に未対応のExchange Serverが大量に見つかっていますが、それらはすでに攻撃を受けたあとかもしれません。迅速に対応すべきです。

予測

婚活サイトのOmiaiにおいてユーザの運転免許証を含む本人確認書類の画像データが流出しました。攻撃者は、流出したデータをもとに運転免許証の画像を偽造して、その画像を悪用したなりすましが増加すると予測します。

新型コロナウイルスのワクチン接種に関する詐欺が横行しています。接種対象が広がる6月からはより幅広い年代を狙った攻撃が広まるおそれがあります。

また、ランサムウェアの被害にあった場合の身代金の支払いは、米国財務省の外国資産管理局（OFAC）の勧告のように禁止する動きが増えています。しかし、情報公開により大きなダメージを受けるおそれがある限り、攻撃された組織が身代金を支払ってしまうというケースは、今後も残り続けるでしょう。

2. 注目トピック

2.1. 個人情報保護法改正について

2.1.1. はじめに 個人情報保護法改正の要旨

個人情報保護法は3年ごとに定期的な見直しが図られており、2022年（令和4年）に改正法が施行されます。今回は、表 1に挙げる6つのポイントが改正されます [1]。

表 1：個人情報保護法改正内容概要

改正ポイント	内容
1. 個人の権利の在り方	• 利用停止、消去などの個人の請求権の拡充 • 保有個人データのインターネットを含めた開示方法を、本人が指示できるようにする • 個人データ授受に関する第三者提供記録について、本人が開示請求できるようにする • 6 か月以内に消去する短期保存データについて、保有個人データに含める事とし、開示、利用停止等の対象とする • オプトアウト規定により第三者に提供できる個人データの範囲が限定される
2. 事業者の守るべき責務の在り方	• 要配慮個人情報、不正アクセス等の漏えいなどにより個人の権利を害する恐れが生じた場合に、個人情報保護委員会への報告、本人への通知が義務化する • 違法または不当な行為を助長する等の不適正な方法により個人情報を利用してはならない旨を明確化する
3. 事業者による自主的な取組を促す仕組みの在り方	• 認定団体精度について、現行制度に加え、企業の特定分野（部門）を対象とする団体を認定できるようにする
4. データ利活用の在り方	• 氏名等を削除した「仮名加工情報」を創設し、内部分析に限定する等を条件に、開示・利用停止請求への対応等の義務を緩和する • 提供元では個人データに該当しないものの、提供先において個人データとなることが想定される情報の第三者提供について、本人同意が得られている事等の確認を義務付ける

5. ペナルティの在り方	• 委員会による命令違反、委員会に対する虚偽報告等の法定刑を引き上げる • 命令違反等の罰金について、法人への罰金刑の最高額を引き上げる
6. 法の域外適用・越境移転の在り方	• 日本国内にある者に係る個人情報等を取り扱う外国事業者を、罰則によって担保された報告徴収・命令の対象とする • 外国にある第三者への個人データの提供時に、移転先事業者における個人情報の取扱いに関する本人への情報提供等の充実を求める

出典：個人情報保護委員会 [1]

2021年3月に、LINE社の利用者情報が国外から閲覧可能、また一部情報が国外で保管、という問題がメディアで取り上げられ、個人データの越境移転のあるべき姿に注目が集まりました。本稿では、LINE社の事例を「6.法の域外適用・越境移転の在り方」（個人情報保護に関する法律 第24条）の改正前・改正後に照らし合わせ、越境移転時の個人データの第3者提供方法について解説します。改正法については、未だガイドラインなど詳細が固まっていない点もあるため、現時点で公開されている議論の方向性を踏まえた記述となります。

2.1.2. 個人データを海外移転している事業者への改正の影響

改正個人情報保護法では、「法の域外適用・越境移転の在り方」について、次の表 2の2点が改正されます。

表 2：法の域外適用･越境移転の在り方の改正内容

項番	改正内容
①	日本国内にある者に係る個人情報等を取り扱う外国事業者を、罰則によって担保された報告徴収・命令の対象とする。
②	外国にある第三者への個人データの提供時に、移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等を求める

表 2の改正内容の①は、海外企業が日本国内の個人データを扱う際に同法の罰則適用範囲内となることを明記しています。現行法の権限では、同法に抵触した場合は指示・勧告といった強制力のない罰則でしたが、改正後は、罰則に担保された報告徴収・命令の権限が追加され、また命令に従わない場合は同法に抵触した事実を公表できるようになります。

改正内容の②は、個人データを海外へ移転している国内企業に影響を及ぼします。例えば、日本国内で収集した社員データを海外BPO会社へ移転している場合や、日本国内で収集した顧客データを国外の親会社へ移転した場合などが挙げられます。LINE社が採用していた個人情報取扱方法は、この改正内容②の影響を受けます。

現行法、改正法ともに、外国にある第三者に個人データを提供できる条件は、下記図 1で示す通り、(a)本人の同意、(b)基準に適合する体制を整備した事業者、(c)我が国と同等の水準を持つ国の3つがあります。外国にある第三者へ個人データを提供するためには、3つの条件のうちのいずれか1つを満たさなければなりません。

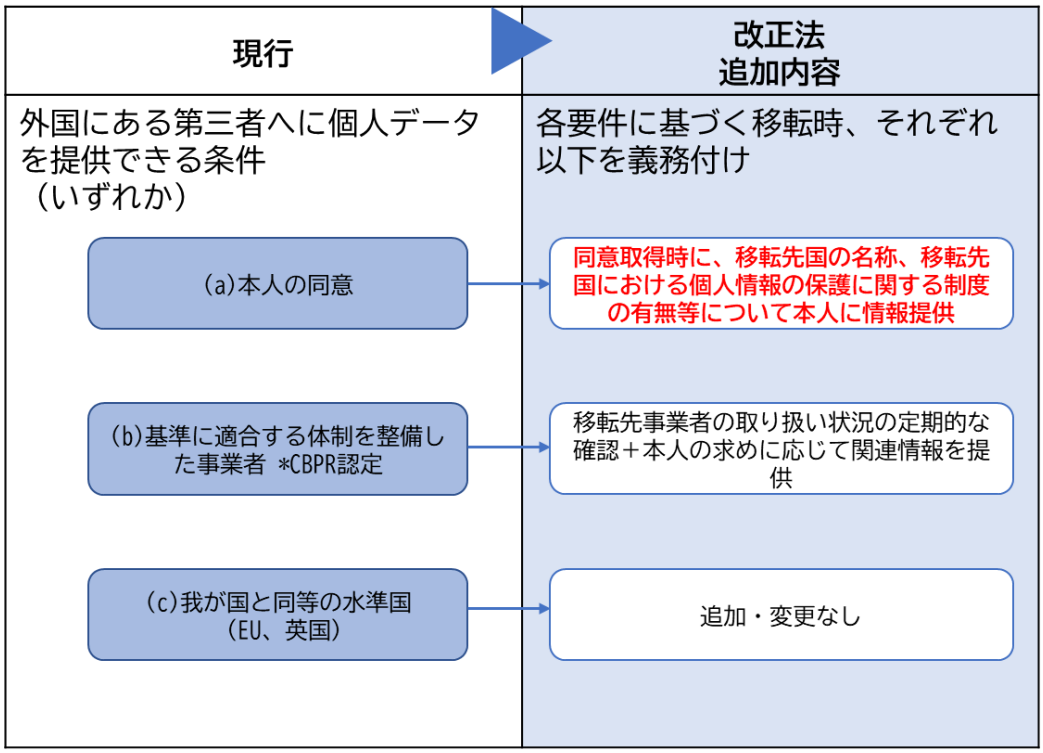


図 1：外国にある第三者へ個人データを提供できる条件の改正内容 [2]（出典より筆者改変）

図 1 の(b)の基準に適合する体制を整備した事業者には、CBPR（Cross Border Privacy Rules ： APEC越境プライバシールールシステム）認証を取得した事業者が該当します。2021年5月時点では2社がCBPR認証を取得 [3]しています。(c)の我が国と同等の水準国は、EUと英国が該当します。2019年1月にEUと英国は、GDPR（General Data Protection Regulation：一般データ保護規則）第45条に基づいて、日本へ十分性認定を付与しています [4] [5]。つまり、日・英EUは相互に十分性を認定しており、個人データの十分な保護水準を確保しています。この点については、今回の改正前後で差分はありません。

今回の改正で大きく影響を受ける条件は、(a)本人の同意です。現行法では、『個人情報取扱事業者が外国にある第三者に個人データを提供する場合には、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない』となっています。それに対して改正法では、『現行法に加え、本人の同意取得時にあらかじめ外国における個人情報の保護に関する制度、移転事業者が講ずる個人情報保護のための措置、その他当該本人に参考となるべき情報を当該本人に提供しなければならない』 [6]との記述が追加されました。それぞ

れの具体的な内容は現時点では検討段階ですが、2020年11月に個人情報保護委員会より発表された「改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）」 [7]に、同意取得時に本人に提供すべき情報の内容（表 3）が記載されています。

表 3：改正法で追加される、本人へ提供すべき情報の内容（要約）

改正ポイント	本人へ提供すべき情報の内容（方向性）
(ア)当該外国における個人情報の保護に関する制度	• 我が国の個人情報保護法との間の本質的な差異を認識できる程度の内容、粒度 • 個人情報保護委員会が、外国の制度について事業者の参考になる情報を取りまとめて公表予定
(イ)当該第三者が講ずる個人情報の保護のための措置	• 個人データの取扱いについて、我が国の個人情報取扱事業者に求められる措置との間の本質的な差異を認識可能な内容 • 同意取得時に第三者が講ずる個人情報の保護のための措置の情報提供が困難な場合は、その旨及び理由について情報提供を求める
(ウ)その他当該本人に参考となるべき情報	• 移転先の第三者が所在する外国の名称 • 移転先の外国が特定できない場合は、移転先の外国の範囲の情報また事後的に移転先の外国が特定できた場合は、本人の求めに応じて情報提供を行うことが望ましい

(ア)、(イ)、(ウ)に共通して、本人が自己の個人データの越境移転に伴うリスクを適切に認識できることが重要視されます。個人データをどの国へ移転し、その国ではどのような個人情報保護関連の法令が定められており、また移転先の事業者ではどのような個人情報取扱いの取り組みを実施しているかを、事業者は本人に説明しなければなりません。

2.1.3. LINE社の個人情報海外移転問題

ここでは、2021年3月に報道されたLINE社の個人情報取扱いにまつわる問題を例に取りあげ、個人情報保護法の改正前と改正後の個人データの海外移転に関する差分を比較します。国民的インフラでもあるLINE社の問題は、メディアでも数多く取り上げられて大きな社会問題になりました。安全保障や電気通信事業法の観点からも着目されましたが、本稿では個人情報保護法の観点でどのような問題が発生したか、また改正後の個人情報保護法のどのような点を遵守すべきか、取り上げて解説します。

2021年3月に、LINE社の中国の関連会社が、サービスの開発や一部コンテンツを監視するために、日本国内利用者の個人データへアクセスできるようになっていました。また、韓国IT大手NAVER社のサーバで、日本のトークに投稿されたすべての画像と動画が保管されている、と報じられました。これらの報道内容をまとめると、表 4の3つの問題が発生していたおそれがあります。

表 4：LINE社の個人情報海外移転の3つの問題

項番	問題の内容
問題1.	利用者に十分な説明をせず、外国の委託先に個人データを提供していたおそれ
問題2.	外国の委託先に対する監督が不十分だったおそれ
問題3.	外国のクラウドサービスに個人データ（画像や映像）を保存する際に必要な対応が不十分だったおそれ

表 4の問題1、2、3のそれぞれについて、現行法と改正法を用いて解説していきます。また、現行法上では問題がない部分のうち、改正法では問題が生じるケースを比較して解説します。

2.1.3.1 問題1：LINE利用者への個人情報海外移転の説明不足

LINE社は、LINE利用者へ示している個人情報に関する指針には「利用者の同意を得た場合や法律で認められる場合に個人情報を第三国に移転することがある」と記載していました。ただし、どのような場面でどの国へ情報を移転するのか、具体的な言及がありませんでした[8]。

2021年3月時点では、現行法では、「外国の第三者（注：委託先を含む）に個人データを提供する際は、その旨を事前に本人に説明し同意を取得するなどの要件が必要」と定めていますが、情報移転先の国名の開示までは求められていません。厳密に言えば、保護法ガイドラインQ&Aの9-2項で、「外国の第三者へ提供する際、提供先の国名を示す必要があるかどうかは、本人が同意するか否かを判断するために必要と考えられる情報を提供する必要がある。具体的には国名を具体的に示す、外国の第三者に提供する場面を具体的に特定するなどの方法が考え得る」 [9]と記載されています。しかし、個人情報保護委員会事務局審議官の佐脇

氏の著作『一問一答 令和2年改正個人情報保護法』では、「必ずしも当該外国の国名や当該外国における個人情報保護に関する制度についての情報提供までは求められませんでした」と現行法では、要求事項に限界があったことを言及しています [10]。これらを踏まえると、現行法では、やはり国名を本人へ伝える義務は生じていないことが分かります。

つまり、現行法における外国にある第三者への個人情報提供という論点では、LINE社が法律に抵触するおそれは低いと考えられます。実際、個人情報保護委員会も2021年4月23日の発表では、「個人情報の保護に関する法律に基づく行政上の対応について」において、『「本人の同意」については、プライバシーポリシーにおいて、利用者の個人情報の利用目的（サービスの提供・改善、コンテンツの開発・改善、不正利用防止等）及び業務委託先の外国の第三者へ提供することが明記されており、利用者にとって外国にある第三者に提供する場面を特定できなかったとは言い難い。』 [11]と述べています。個人情報保護委員会は、表 4の問題1に関して不問としています。

個人情報保護委員会は、LINE社に対して「LINE サービスの提供に関してメッセージ等の個人情報を取得する場合には、取得する個人情報の範囲を分かりやすく通知するとともに、通知内容が適切に表示されているか確認する体制を整備すること」という指導を実施しています。LINE社の問題は法令違反ではないが、LINE社が取り扱う情報は秘匿性が高く、個人データの数量も多いことから、このような対応を取ったとみられます。

仮に今回のLINE社の問題に、改正法を適用した場合を考えてみます。改正法では、表 3の改正のポイント(ア)、(イ)、(ウ)のそれぞれについて、以下の表 5へ記載した具体的な情報を本人へ提供しなければなりません。中国と日本は、欧州のGDPRと日本の個人情報保護法のように国家間で十分性認定を取り交わしておらず、(ア)「当該外国における個人情報の保護に関する精度」について、具体的な日中間の差分を書く必要があります。自社で差分を確認できない場合は、個人情報保護委員会が外国の制度について事業者の参考になる情報を取りまとめて公表したあとに対応すれば良いでしょう。

表 5：改正法を適用した場合にLINE社が提供すべき情報

改正のポイント	仮に今回のLINE社のケースで改正法が適用された場合において、新たに個人情報の海外第三者移転について本人へ提供すべき情報
(ア)当該外国における個人情報の保護に関する制度	委託先企業の設置場所である中国の個人情報保護に関する法律内容と、日本の個人情報保護法の差分について記述する。中国政府の個人データへの関与の可能性も含めて記述が必要な可能性もある
(イ)当該第三者が講ずる個人情報の保護のための措置	委託先企業における個人情報取扱の方針について、自社基準と同等な内容、委託先ならではの対応、など実態に即した情報を記載する
(ウ)その他当該本人に参考となるべき情報	移転先の第三者が所在する外国の名称として、中国と記載する

2.1.3.2 問題2：海外委託先の監督不足

「問題2. 外国の委託先に対する監督が不十分だったおそれ」とは、中国にあるLINE社の開発関連企業従業員が日本のサーバへ接続し、利用者の氏名や電話番号、メールアドレス、メッセージの内容などが閲覧可能になっていた問題です。LINE社によると、不適切なアクセスは確認されず、また2021年2月下旬に中国からサーバへの接続ができないように設定を変更したとのことです [12]。この問題を受け、個人情報保護委員会は委託先の管理監督を強化することを指導しました。その中には、アクセス権限の詳細な設定や、定期的な委託先の監査、委託内容の見直しの検討などを含んでいます。指導の根拠は、個人情報保護法第22条「委託先の監督」に依るものです。これは海外事業者への個人データを移転にするときに限らず、日本国内で情報を委託するときも対策が必要です。今回は中国への委託という点が注目されましたが、国外でも国内でも、委託先で個人データが安全に取り扱われるよう、委託元は委託先に対して必要かつ適切な管理を要求しなければなりません。

セキュリティ対策の観点から見ると、最小権限の原則に基づいた権限付与ができているかを確認し、余分な権限があれば削除するべきです。LINE社が意図して中国での開発時に個人データの閲覧の権限を付けたかは定かではありません。しかし、国外での開発時に本当に日本利用者そのものの情報が必要であったかは疑問が残ります。

2.1.3.3 問題3：外国クラウドサービス上での個人情報保護対策の不足

「問題3. 外国のクラウドサービスに個人データ（画像や映像）を保存する際に必要な対応が不十分だったおそれ」とは、日本の利用者の個人データが韓国NAVER社のサーバへ保管され、保管サーバへのアクセス権をNAVER社の従業員が持ち合わせていた問題です。保管されていたデータは、複数サーバに分散して保管するなど特殊なセキュリティ対策が施されており、サーバ管理者は保管された動画や画像を閲覧できなかったと報じられています [13]。

クラウドサービスを利用する際に、個人データを取り扱う企業は、当該クラウドサービスを提供している企業へ個人データを提供しているか否かを確認しなければなりません。個人情報保護法ガイドラインでは、個人データをクラウド事業者へ提供している例として「個人データをキーワードとして情報を抽出する場合」 [9]を記載しています。情報を直接クラウドサービス内で利用する場合は、個人データをクラウドサービスへ提供しているとみなされます。コンピュータやスマホ上のアプリケーションであっても、SaaSのようなクラウドサービスと連携していて、個人データをクラウド上へ送信して処理しているソフトウェアは注意が必要でしょう。

個人データをクラウドサービスへ提供している場合、クラウド事業者へ個人データを委託しているとして扱われます。外国の第三者への個人データの委託には、原則として本人の同意など、図 1で示した内容の対応が必要です。改正法において本人の同意を元にして委託する際、本人へ委託先の国名、移転先国の精度有無などを伝える必要がある点は、表 3で示した内容と同様です。

一方、個人データの移転先の事業者の業務がハードウェア・ソフトウェア保守にとどまる場合や、個人データをクラウドサービス提供事業者へ預けない運用、かつ契約条項によって

クラウドサービス提供事業者がサーバに保存された個人データを取り扱わない事が定められていれば、第三者への個人データの提供には当たりません [14]。個人情報保護法ガイドラインでは、個人データの提供に当たらない例として「システム修正パッチやマルウェア対策のためのデータを配布し、適用する場合」を挙げています [9]。

今回のLINE社の事例では、個人データの保管先のクラウドサービス提供事業者であるNAVER社からLINE社が保有する個人データへのアクセスは制限されており、NAVER社からは個人データを扱えない状態であったと説明されています。アクセス制限に加えて、もしLINE社とNAVER社の間にNAVER社がサーバ上の個人データへアクセスしない事を明記した契約があれば、日本の利用者の個人データが韓国NAVER社のサーバ上へ保管されていた件は、個人データの第三者への提供には当たりません。この場合、LINE社は利用者への同意などの対応なしにクラウド上へ個人データの保管が可能です。

2.1.3.4 LINE社問題の影響と企業に求められる対応

中央省庁などの多くの政府機関が正式にLINEを業務で利用していましたが、この事件の後、LINEメッセンジャーの使用を停止しました。23政府機関のうち18機関がLINEの業務利用をしており、それらの業務のうち、およそ2割の業務で個人データを含めた機密情報を扱っていました [15]。LINE社の出澤社長は会見内で、「法的にどうこうではなく、ユーザのわかりやすさ、感覚として『気持ち悪い』という点への配慮が欠けていた。(後略)」 [16] と述べていることからも分かる通り、利用者目線で自分のデータがどのように利活用されるのかを読み取ることのできる情報提供は、企業にとって不可欠です。近年では、利用者に対しより分かりやすく個人データ取扱い方法を示す企業も出現しています。米国大手IT企業のApple社では、プライバシーの説明に加え、「あなたのデータの一日 公園で。父と娘のストーリー」をWeb上で公開し、ストーリー仕立てで個人データの取扱いについて解説しています。利用者が実際の目線に立ってApple社にまつわるデータ共有や広告、トラッキングといった個人データの流れを知ることができ、ユーザに対する手厚い配慮を感じられます。

2.1.4. 企業で扱う個人情報の取扱いと、利用者への情報提供

LINE社の事例で示したように、改正法の外国を含めた第三者への個人情報移転の項目に対応するには、自社で個人データがどのように扱われているかを把握し、適切に取り扱うことができるようにしなければなりません。また、これらの個人データ保護を持続的にできる体制を構築する必要があります。企業の中には、個人データ保護の監査や是正が機能不全に陥っているケースも見受けられます。今回の改正をきっかけに、まずは経営陣が自社の明確な課題と認識し、社長直下のような強い権限を持った個人情報保護管理者を任命するべきです。個人情報保護管理者に強力な権限があれば、情報セキュリティ管理組織は実効力を持ち、従業員教育や内部監査の実効力強化のような、健全な個人データ保護への取り組みが実施できます。個人データの適切な保護方法や、組織の体制作りについてどこから手を付ければよいかわからない、また自社がどの程度適用できているかを知りたいといった場合、一般的な規

格に沿った対応を始めてみる事を推奨します。

個人情報の保護には、JIS Q 15001（個人情報保護マネジメントシステム-要求事項）という規格が存在します。企業で取り扱う個人データは多岐にわたり、Web上の会員サイト、就職希望者の情報、過去の販売データ、従業員の情報など様々なものがあります。これらを洗い出した上でリスクの評価や対策を実施することが、JIS Q 15001 では求められます。プライバシーマークは、JIS Q 15001に沿っていることをベースとして適用される第3者による認証制度です。社内の情報の洗い出しや、個人情報取扱方針の制定に苦慮している場合は、プライバシーマークを取得支援している企業に改正個人情報保護法への対応を頼ってみるのも一案でしょう。プライバシーマークは第3者認証のため、社会的な信用にも繋がります。

自社の個人情報保護の取り組み内容を利用者へ開示する方法は、プライバシーポリシーの公開が一般的です。外国にある第三者への個人データ移転の情報などは、まさにこのプライバシーポリシー内へ記述して開示します。企業のウェブサイトではテンプレートをそのまま用いたような記述も多々見受けられますが、今回の改正を機に社内の個人データへの取り組みと体制を整備し、社外へ適切な内容を分かりやすく発信することで利用者の信頼を向上し、ひいては企業価値を高める取り組みとしていただきたいです。

2.1.5. 罰則強化による企業の対応への影響

改正法は、法人向けの罰則が大幅に強化されています。個人情報保護委員会からの命令への違反や個人情報データベース等の不正提供時には、表 6に示すように最大1億円以下の罰金が科されます。これは、改正前の最大50万円以下からみて大幅な増額となりました。海外に目を向けると、GDPRの制裁金は、最大2,000万ユーロ(約26億円)または年間売上高の4%を上限としています。また、中国で法案が公表された中国版個人情報保護法についても、最高5,000万元(約8億円）を科すことになりそうです [17]。全世界で個人情報保護関連法への厳しい違反罰則が制定されている背景には、利用者の個人データ保護意識の高まりによる訴訟リスクや、他国と足並みをそろえないことにより発生する経済的な損失回避の狙いなどがあります。

表 6：改正法における罰則の改定内容

		懲役刑		罰金刑	
		改正前	改正後	改正前	改正後
個人情報保護委員会からの命令への違反	行為者	６月以下	１年以下	３０万円以下	１００万円以下
	法人等	-	-	３０万円以下	１億円以下
個人情報データベース等の不正提供等	行為者	１年以下	１年以下	５０万円以下	５０万円以下
	法人等	-	-	５０万円以下	１億円以下
個人情報保護委員会への虚偽報告等	行為者	-	-	３０万円以下	５０万円以下
	法人等	-	-	３０万円以下	５０万円以下

出典：個人情報保護委員会 [18]

また今回の法改正により、個人データ流出の疑惑が上がった時点で個人情報保護委員会への報告が必要になります。個人情報保護委員会への報告命令違反や虚偽報告に罰則が科されることを踏まえると、有事の際に備えた報告手段も準備しておくべきです。どのような個人データがどういう経緯で漏えいしたのかを確認できる方法も準備しておくことが望ましいです。企業によって個人データの取扱い方法や内容は異なりますが、一般的には個人データ持ち出し管理簿の整備や日常的な機器やソフトウェアのログ収集、メールやアップロード等の利用者行動履歴保管のような対策を講ずるべきでしょう。

2.1.6. まとめ

「個人情報の保護に関する事業者の取り組み実態調査（平成29年度）報告書」によると、個人データの越境データ移転を実施している事業者は全体の12.3%に及びます [19]。今後、IT部門の海外移転や、開発拠点のオフショア化、クラウドソーシングの促進、M&Aでの海外子会社追加など、様々な要因で増えていくことになるでしょう。

令和2年改正個人情報保護法への対応は、個人情報保護法を取り扱う全事業者にとって必要となります。第三者への個人データの移転先に海外が含まれるか否かは企業ごとに異なりますが、思わぬところで個人データを移転しているおそれもあります。社内情報の整理は日常的に実施し、必要に応じて利用者に適切な情報を開示できる体制を確保することが重要です。

2.2. 証券システム開発者による顧客預金の横領

松井証券株式会社は、証券取引システムの開発・運用業務委託先であるSCSK株式会社の元従業員により、顧客の証券口座から約2億円が不正に出金されたこと、および元従業員が逮捕されたことを公表 [20]しました。

本事件は犯行開始から発覚まで２年半かかっており、逮捕されるまでは更に１年ほど期間がかかっていることが特徴です。2020年1月に松井証券が顧客から「身に覚えのない取引があった」との問い合わせを受けて調査したところ、業務委託先のSCSK社の元従業員が複数の顧客の情報を不正に取得し、顧客に成りすまして現金を不正に出金していたことが判明しました（図 2）。松井証券は不正出金の被害を受けた顧客に対して被害額を全額返金し、SCSK社は松井証券へその被害相当額を支払いました。

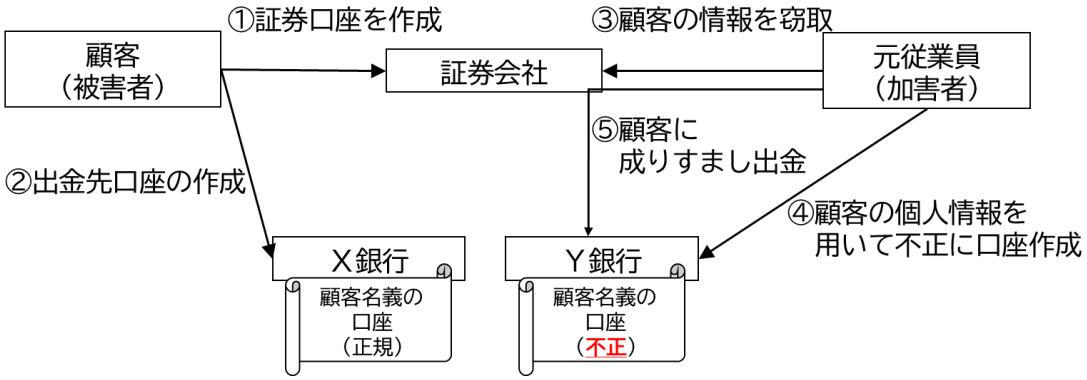


図 2：事件の概要

2.2.1. 事件詳細

松井証券とSCSK社から公表された内容 [21]をもとに、不正出金の準備の流れ（図 3）と出金実行の流れ（図 4）を説明します。

◆ **不正出金の準備（図 3）**

不正出金を行った元従業員は、松井証券がシステム開発・運用業務を委託先したSCSK社の社員であり、業務遂行のために本番環境と開発環境にアクセスする権限を付与されていました [22]。元従業員は、本権限を用いて、本番環境から顧客のIDやパスワード等の情報を含んだバックアップデータを作成し、開発環境に複製しました。開発環境でバックアップデータから顧客情報を抽出し、私用のメールアドレス宛に送信しました。そして、手に入れた顧客情報を用いて被害者に成りすまして、被害者名義の偽の銀行口座を開設しました。

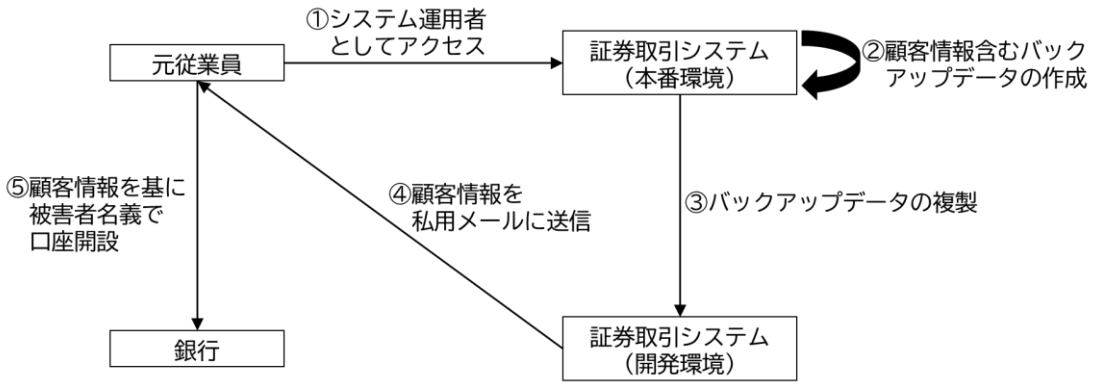


図 3：不正出金の準備の流れ(①～⑤)

◆ **不正出金の実行**（図 4）

元従業員は、取得した顧客情報に含まれていたIDとパスワードを用いて証券取引システムにアクセスして、顧客の有価証券を売買して現金化を行いました。元従業員は、売却した有価証券の現金と証券口座へ預け入れられていた現金を被害者名義の偽の銀行口座へ出金して、その銀行口座から現金を引き出しました。後日、被害者が証券取引システムにアクセスして、身に覚えのない出金を見つけるまでは、本事件は発覚しませんでした。

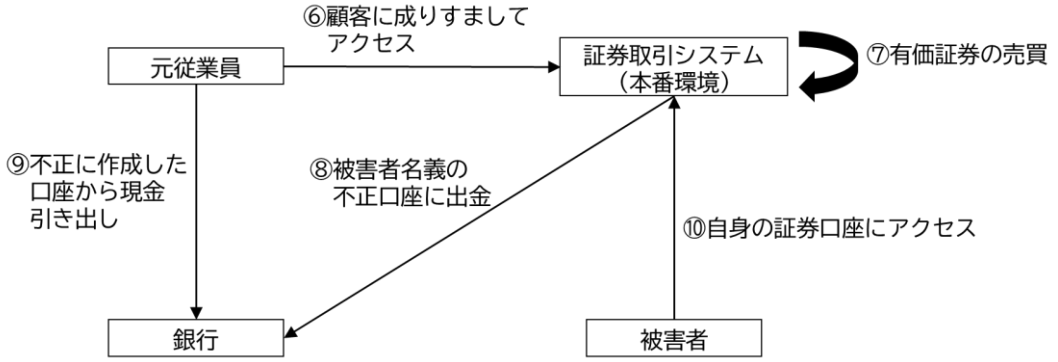


図 4：不正出金の実行の流れ(⑥～⑩)

この不正出金に依る被害額は15顧客、約２億円にのぼっていますが、松井証券によってすべての顧客に全額返金済みと公表されています。

2.2.2. 事件の特徴

◆ **犯行から発覚までの期間**

元従業員は松井証券のシステム運用を入社以来18年間担当しており、プロジェクトリーダーとして業務フローやシステム構造に精通していました [22]。元従業員の入社から逮捕まで

の時系列を表 7にまとめます。

表 7：元従業員の入社から逮捕までの時系列

日時	出来事
2002年4月	元従業員が入社
2017年6月29日 ～2019年11月12日	不正出金の実行
2020年1月	顧客からの問い合わせ
	松井証券による調査開始
	松井証券から監督官庁への報告および警察への相談開始
2020年9月	SCSK社から警察へ告発状を提出
2021年3月24日	元従業員逮捕および懲戒解雇処分

元従業員の犯行が始まったのは2017年6月からですが、顧客が気づいて問い合わせを行ったのは2020年1月であり、最大で２年半もの期間が空いています。長期間、犯行が発覚しなかった理由は、元従業員が取引履歴等から資金移動の少ない口座や証券取引システムへのアクセスが少ない顧客を不正出金の対象へ選んでいたからと推測されます。元従業員は、何度も顧客情報を取得して顧客の取引履歴やアクセス履歴を調査して、不正出金が発覚しにくい顧客を綿密に選んでいた可能性が考えられます。

◆　本番環境から開発環境への顧客情報持ち出し

金融情報システムセンター（以下、「FISC」とする）が刊行している『金融機関等コンピュータシステムの安全対策基準・解説書（第９版改訂） [23]』（以下、「安全対策基準」とする）の統制基準には、不正防止のために以下の基準が定められています。

> コンピュータシステムに係わる業務を円滑かつ適正に運営するとともに、不正を防止するため、業務範囲並びに責任及び権限を明確にし、相互牽制体制を整備すること。（中略）業務組織の分離が困難な場合には、少なくとも担当者を定期的にローテーションすることなどで相互牽制が働く仕組みとすることが必要である [24]。

松井証券は、金融庁からFISCの安全対策基準への準拠状況を監査されるため、上記の安全対策基準の統制基準に沿って内部犯行リスクが対策されていたと思われます。しかし本事件では、厳重に守られているはずの顧客情報が外部に持ち出されています。開発環境へのアクセス権限を持つ元従業員に対して、システムの維持運用のために本番環境へのアクセス権限が払い出されたことにより、両環境へのアクセス権限を同時に持つタイミングが発生してしまいました。これにより、他の運用担当者に気づかれずに本番環境で取得した顧客情報を開発環境に送付することが可能となったと推測されます。

◆ **顧客のIDやパスワードの取得**

本番環境から顧客情報の持ち出しに成功したとしても、顧客情報が暗号化されている場合は不正利用することは出来ません。FISCの安全対策基準の実務基準の項目には、データ保護として以下の基準が定められています。

> ファイルの不正コピー、盗難等による漏洩を防止するため、重要なデータについてはデータ保護の対策を講ずること。（中略）特に個人データを蓄積する場合には、暗号化・パスワード設定等ファイルの不正コピーや盗難の際にもデータの内容がわからないようにするための対策を講ずることが必要である。また、電子的取引において蓄積されるデータについても暗号化・パスワード設定等の対策を講ずることが必要である。 [25]

松井証券の広報は、事件当時のセキュリティ対策について「セキュリティに関わるため回答できない [26]」と発言していますが、データベースの暗号化やアクセス権限の制限等の多数のデータ保護対策が行われていたものと推測されます。そうであれば、元従業員が本番環境から開発環境へ顧客のIDやパスワードを持ち出せたとしても、暗号化されていて不正利用ができなかったはずです。元従業員が長年のシステム開発の中で蓄積した知見をもとにセキュリティ上の穴を見つけ、顧客情報の取得・復号を行ったと推測されます。あくまで推測ですが、復号化するためのキーが本番環境と開発環境で同一になっており、情報を持ち出せさえすれば復号可能な状態になっていたおそれが考えられます。

◆ **第三者が出金できた理由**

法令では本人名義以外の取引を取り扱えないよう定められており、第三者の銀行口座に出金することは禁止されています。そのため、本来は顧客本人でなければ証券口座から出金することはできません。しかしながら本事件では、松井証券に提出されていた顧客情報を盗み出すことにより、第三者である元従業員が顧客本人に成りすまして顧客本人名義の銀行口座を開設して、そこへ出金しています。多要素認証が設定されていない顧客のIDとパスワードを使用して証券取引システムにアクセスして操作しているため、システム上は顧客本人が顧客名義の銀行口座へ出金していることになり、第三者による犯行であると検知することが困難になっていました。

2.2.3. 対策

セキュリティは予防策に加え、インシデントが発生することを前提とした早期の発見や対処方法を事前に検討しておくことが重要です。本事件に関連するそれぞれの立場における対策案を以下にまとめます。

A) 運用部門

◆ 予防

松井証券の和里田社長は記者会見で「不正の抑止や監視体制が十分でなかった」と謝罪しており、本番環境から開発環境への顧客情報持ち出しの予防策として、承認手続きの見直しをすると述べています [27]。気をつけるべき点として、一律で承認行為を厳格化して手続きを煩雑にしすぎると、かえって承認手続きが形骸化して正しく機能しなくなるおそれがあります。そのため、個人情報を含むファイルへのアクセスの申請であれば厳格な承認手続きを行い、アプリケーションログの取得の申請であれば簡易な手続きを行う等、取り扱う情報や作業の重要性に着目したリスクベースのセキュリティ運用設計を行うべきです。運用上の負担にならないバランスのとれた予防策を目指すとよいでしょう。

たとえば、顧客向けには、口座開設後の初回の出金先口座の指定はオンラインで指定可能にしても、その後の口座変更は登録済み住所へ手続書類を郵送して行う等、手続き内容の重要度に応じて適切なレベルの身元確認と当人認証を行わなければなりません。なお、2020年度第2四半期のグローバルセキュリティ動向四半期レポートで、オンライン決済システムの不正アクセス事件を取り上げて、eKYCを使ったオンライン決済サービスにおける利便性の高い本人確認方法を解説 [28]しています。

◆ 早期発見

本番環境の全ての作業ログを目視で精緻に監視することは運用負荷が大きく、現実的ではありません。内部不正を伴う不審な行動を自動で検知する方法は、ユーザやデバイスの行動を分析するUEBA（User Behavior Analytics）を用いた検知システムが効果的です。UEBAを使った検知システムは、作業ログを分析して通常とは異なるユーザやデバイスの行動を自動的に検知できます。またそのためには、システムを深く理解して、機微情報にアクセスする処理や重要な操作を作業ログへ残すようシステムを設計、構築することが必須条件です。

FISCの安全対策基準では、「5. 金融機関等が外部委託を行う場合には、委託する業務の遂行状況及び、外部委託先の要員によるルールの遵守状況等について、評価・検証することが必要である [29]」と定義しています。委託先の開発部門が、システムトラブルやソフトウェアのバージョンアップ等の通常とは異なる作業で本番環境へアクセスする際も、作業に乗じてルールを逸脱した操作を行なっていないか、作業ログを目視で監視して牽制し続けなければなりません。

B) 開発部門

◆ 予防策

システムのセキュリティ設計を理解している者でも不正を行えないように、機微情報を外部に持ち出せない仕組みや不正を容易に発見できる仕組みを作らなければなりません。本番環境で顧客情報を取得したり、顧客情報を開発環境に送付したりする高い権限が必要なコマンドやファイルアクセスは、複数人の作業者がいないと実行できない仕組みにすることや、実行時に操作者とは別の運用部門へ通知する仕組みを設けることで、内部不正を予防できま

す。他には、本番環境から持ち出せるデータに制限をかけて、個人情報を含むデータを解析できる環境を他の環境から隔離することでも予防できます。すべての作業を二人一組にしたり、検知のレベルを低く設定して通知が過剰になったりすると、運用負荷が高くなりすぎます。また、通知が過剰になると目視確認がおざなりになり、不正を見逃してしまうおそれもあります。リスクベースの設計を行い、複数階層の権限設計を導入すべきです。しかし本番環境のトラブル対応時に、想定外の追加作業に備えて、予定していた作業に必要な権限よりも高い権限を申請する場合があります。原則、必要最低限の権限の払い出しを申請しましょう。さらに、それらの作業内容を詳細化してコマンドレベルまで落とし込んだ手順を作成すること、それをもとに作業ログを機械的にチェックする仕組みを作るとよいでしょう。

元従業員は、同システムの開発からその後の維持運用業務まで、同じシステムに長年関わっていました。一人に権限が集中しない仕組みや、ジョブローテーションを行うことで潜在的なリスクを低減させることができます。

◆　早期発見

システムトラブル等、どうしても本番環境からデータを持ち出さなければならないときや、特殊な権限を払い出さなければならないときなど、事前に予測が困難な逸脱対応が発生する可能性があります。その場合は、データのトレーサビリティを確保し、運用部門だけではなく開発部門の有識者を複数人交えて作業ログの監査をすれば、不正行為を特定することができます。

C)　顧客

◆　予防策

本事件の準備段階では、顧客が把握できない方法で個人情報の窃取と出金用の銀行口座の作成が行われました。しかしながら、証券システムへの不正ログインは、システムが提供しているセキュリティ機能の設定を有効化すれば、予防や検知が可能だったと考えられます。多要素認証が設定されていれば、元従業員はその顧客になりすましたログインができませんでした。金融機関が提供しているサービスにより利用できる機能は異なりますが、口座にアクセスする際の多要素認証や接続元のデバイスやIPアドレスを制限する設定を有効化すれば、第三者によるアクセスを防げます。

◆　早期発見

第三者の不正ログインや不正取引の実行に気づく手段として、ログイン時や口座関連の設定の操作時、セキュリティ設定変更時に、設定したメールアドレスへ通知を行うシステムも多く存在しています。あらかじめ設定しておけば、心当たりの無い操作に早期に気づくことができます。また、家計簿アプリを活用し、お金の動きを一元管理し見えるようにすることで気づく可能性が高まります。

2.2.4. まとめ

松井証券における内部不正の事例をもとに、複数の観点で対策を考えました。金融サービスは、本人確認を厳密に行うことでセキュリティを向上させる一方で、顧客の利便性が低下したり、逆にオンラインのみの簡易な手続きですぐに利用できるようにするとセキュリティ対策が疎かになったりと、他のシステムより安全性と利便性のバランスが難しいシステムです。顧客が安心して利用でき、かつ利便性の高いサービスを提供するためには、リスクベースでアプローチし、機能や運用ごとに必要十分なリスクマネジメントを行う対策方法が効果的です。決済分野はオンラインサービスの利用率が年々高まっており、オンラインで支払いできる税金の種類を増やすなど、国としても金融のオンライン化やデジタル化を推進していくと思われます。金融システムに関わる企業は、本稿を参考に必要なセキュリティ対策をご一考いただければと思います。また、金融システムを利用する顧客としては、自身が利用しているオンラインの金融サービスのセキュリティ機能の設定を適切に設定し直して、サイバー攻撃や内部不正の被害に遭わないように予防していただければと思います。

3. 情報漏えい

2021年月3月に、国際航空情報通信機構(以下、「SITA社」という)のシステムに対する不正アクセスにより、委託元組織であるANAホールディングス傘下の全日本空輸が加盟する「スターアライアンス」と同様に委託元組織の日本航空が加盟する「ワンワールド」の会員情報の流出が発生しました。本稿では委託元の航空会社の視点で、委託先であるSITA社からの情報窃取の原因と対策や法制度の比較、SITA社とLINE社の報道影響の比較について取り上げます。また、引き続き発生しているSalesforceの設定不備による情報漏えいについても取り上げます。

3.1. SITA社の情報漏えい

3.1.1. 概要

SITA社の情報漏えいでワンワールドではブリティッシュエアウェイズ、スターアライアンスではユナイテッド航空、シンガポール航空が被害を受けました。日本の航空会社では全日本空輸は約100万件、日本航空は約92万件の会員情報が漏えいしました。漏えいしたのは以下の会員情報でした [30] [31]。

- アルファベット表記の氏名
- 会員番号
- 会員のティアステータス

被害を受けた航空会社は、図 5に示すように会員が提携航空会社の航空便へ搭乗する際のサービス提供のため、SITA社を経由して提携航空会社内で会員情報を相互に共有していました。このSITA社の米国にあるサーバが不正アクセスされたため、保存されていた会員情報が漏えいしました。

不正アクセスされた原因は公開されていませんが、SITA社はすでに被害を受けたシステムとインターネットの接続を遮断済みで、引き続き追加の漏えい有無を調査しています。今回の事例は、委託元組織の顧客情報が委託先組織で漏えいしたため、サプライチェーン攻撃にあたります [32]。

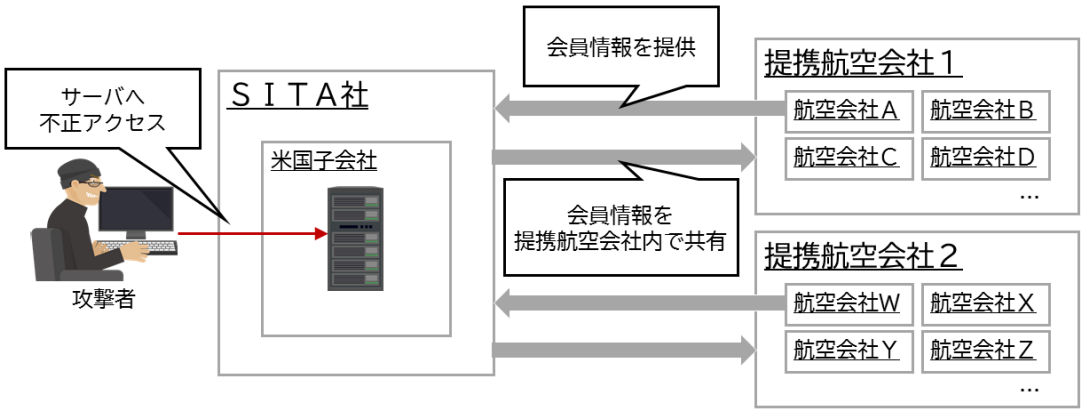


図 5：会員情報の提供と不正アクセス

3.1.2. 委託先からの情報窃取の原因と対策

2020年度第3四半期のレポートでサプライチェーン攻撃の手法は、大きく「①委託先を踏み台にした攻撃」、「②ソフトウェアサプライチェーン攻撃」、「③委託先からの情報窃取」の3つがあると紹介しました。今回の事例は「③委託先からの情報窃取」にあたります。

委託先組織で個人情報の漏えいが発生した場合、委託元組織は個人情報保護法に則った対応が必要になります。原則、個人情報保護委員会等へ報告を行います。また、個人に被害が及ぶおそれがある個人情報の漏えいは、二次被害を防ぐために個人への通知や注意喚起などを行います。

今回の事例では、複数の提携会社共通のシステムだったため、SITA社が個社のガバナンスに合わせてセキュリティ対策されたシステムを構築することが難しかったと考えられます。また、複数の提携航空会社のグループを跨いで同時に漏えいが発生しており、システムやデータベースの管理者権限がグループ毎に分離されていない、またはデータベースが暗号化されていなかったおそれが考えられます。このように委託先に重要な情報を預けるケースでは、委託元組織は、攻撃者がクラウドや委託先組織の基盤システムの管理者権限を不正取得した場合でもその中の機密データを保護する対策を行っていることなど、委託先組織が「③委託先からの情報窃取」のサプライチェーン攻撃に対して十分な対策をおこなっていることを確認すべきです。

3.1.3. 海外委託先の法制度

SITA社の本社所在地であるスイスでは、スイス連邦データ保護法(Federal Act on Data Protection：以下、「FADP」という)が施行されていますが、2020年9月25日に改正案が成立し、2022年半ばに発行する予定です [33]。改正案は、一般データ保護規則(General Data Protection Regulation：以下、「GDPR」という)を大きく意識した内容で全74条にわたっています。しかし、2022年の発行までは現行法が適用されており、現行法は1992年に成立した全

39条にすぎないため、現在のGDPR下では十分性認定を維持できない内容です [34]。そのため、SITA社のシステムが現行法に基づいて設計、構築、運用されていた場合、そのセキュリティ対策は十分でなかったおそれがあります。海外へ委託する際は、委託先組織に適用される法制度とGDPRや個人情報保護法を比較してセキュリティ対策の要求が低いことはないか確認すべきです。

3.1.4. SITA社とLINE社の報道影響の比較

2021年3月に、LINE社の個人情報取り扱いにまつわる問題が大きく報じられました。

中国の委託先が登録したメールアドレスや氏名、個人的なやり取り等のデータへアクセス可能であったという報道 [12]を受けて、LINEの個人利用者の中で自身の個人情報を覗き見されるプライバシー侵害の懸念が広がりました。自組織の業務やサービスでLINEを利用している省庁や自治体は、LINE上で取り扱う秘匿性の高いデータの保管場所や海外委託先へのデータ受け渡しが個人情報保護法に抵触しているおそれを懸念して、LINEの利用を停止しました。外部からの不正アクセスや情報漏えいが発生したわけではありませんが、総務省はLINEの利用を停止しました。

しかしSITA社の事例では情報漏えいが発生したにも関わらず、大きくは報じられていません。この差は「保管データの重要度の違い」と「SITA社の漏えい規模」が関係していると考えられます。LINE社で保管されているデータは画像（保険証等含む）や動画、決済サービスの取引情報などの多様で重要なデータを含んでいるのに対して、SITA社で保管されているデータはアルファベット表記の氏名、会員番号、会員のティアステータスに限定されます。また全日本空輸のANAマイレージクラブは約3702万人 [35]、日本航空のJALマイレージバンクは約3000万人 [36]の利用者がいます。今回、漏えいした個人情報は、そのうちの全日本空輸が約100万件、日本航空が約92万件です。漏えいした個人情報の数は、全日本空輸、日本航空の全体の利用者数からすると少なく、かつ個人情報の種類はLINE社の個人情報と比べて直接個人を特定しにくく悪用が難しいため、日本国内の両社利用者への影響が小さいと推測します。そのため、報道の取り上げ方が小さかったと考えられます。

3.2. Salesforce経由の情報漏えい（続報）

2020年第3四半期の報告書で取り上げたときと同様に、2020年第4四半期でもSalesforceの設定不備に起因する情報漏えいが複数報告されています。表 8に示したSalesforce経由の情報漏えいの多くは、第3四半期の報告書で取り上げた情報漏えいと同じ原因でした。それらの情報漏えい起こした組織は、セールスフォースドットコム社の周知への対応が遅れたり、インシデントの分析に時間が掛かったりして、情報公開が遅くなったのかもしれません。第3四半期の報告書では、ユーザの設定ミスが起きないように、クラウドサービスプロバイダが安全な初期値を設定しておく対策方法を提案しました。この提案通り、セールスフォースドットコム社は、ゲストユーザのアクセス制御の権限設定不備の対策として、「一般ユーザ

への最小限のアクセス権限の付与」と「ゲストユーザへ初期設定を可能な限り安全な状態に設定するセキュリティポリシーの強制適用」を開始しました。

また表 8のfreee社とイオン社の事例は、2020年第3四半期の報告書に取り上げたこれまでのSalesforceの情報漏えいの事例と原因が異なります。これまでのSalesforceの情報漏えいの原因は、ゲストユーザのアクセス制御の権限設定の不備でした。しかしfreee社は、同社の事例はそれら他社とは発生している経緯が異なると説明しています [37]。入力フォームの送信内容を保存する箇所のアクセス制御の権限設定の不備が原因だったと推測されます。その結果、フォームの送信内容が外部から閲覧可能になってしまいました。

表 8：2020年度第4四半期のSalesforce経由の情報漏えい事例

[38] [39] [40] [41] [42] [43]

公開日	組織	概要
1/27	イオン	同社の問い合わせフォームに設定不備があり、名前や性別、メールアドレス、電話番号、問い合わせ内容を含む859件の情報が外部から不正アクセスを受けた
2/10	freee	同社の複数の問い合わせフォームに設定不備があり、送信内容が外部から閲覧可能となっていた
2/10	両備システムズ	同社の提供する自治体向けシステムで、外部の第三者が一部顧客の情報へアクセスした。当該システムの設定を変更し、外部の第三者からのアクセスを遮断した。設定変更前のアクセス状況を調査している
3/1	コナミデジタルエンタテインメント コナミアミューズメント	クラウドサービス上の顧客管理システムに設定の不備があり、顧客の個人情報が外部からアクセスされた
3/8	SMBC信託銀行 SMBC日興証券	新規に口座開設手続きをした顧客の個人情報が、SMBC信託銀行から最大101人分、 SMBC日興証券から最大50人分が流出した
3/16	国際協力機構	国際協力機構が運営する国際キャリア総合情報サイト「PARTNER」に対して第三者によるアクセスがあり、個人情報が閲覧されていた

3.3. まとめ

サプライチェーン攻撃の対策では、委託元組織だけに留まらず委託先組織も含めた広範囲のセキュリティ対策が必要になります。しかしSITA社の事例では、サプライチェーンの問題以前に、システムやデータベースの管理者権限がグループ毎に分離されていない、またはデータベースが暗号化されていないといった、データベースシステムの基本的なセキュリティ対策が不足していたおそれがあります。幸いにも、情報漏えいの規模が全日本空輸、日本航空の全体の利用者数からすると少なく、かつ直接個人を特定しにくく、悪用も難しい種類の個人情報だったため、日本国内の両社利用者への影響が小さく済みました。もっと多くの情報が提供されていたら、被害は甚大になっていたでしょう。

2020年第4四半期に発生したSalesforce経由の情報漏えいのほとんどが、第3四半期の報告書で取り上げた情報漏えいと同じ原因でした。セールスフォースドットコム社は、ゲストユーザのアクセス制御の権限設定不備の対策として、セキュアな初期設定の強制を開始しました。ユーザへの周知や注意喚起、啓発だけでは、設定ミスを完全になくすことが困難であるため、サービス提供者はセキュアな標準設定やシステムによる対策を導入するべきでしょう。表 8のfreee社とイオン社の事例は、2020年第3四半期の報告書に取り上げたSalesforceの情報漏えいとは原因が異なりました。詳細な原因が公開されていないために断定できませんが、2020年第3四半期に記載した内容と同様に、クラウドサービスカスタマの理解不足とクラウドサービスプロバイダの説明不足の双方に原因があったと推測します。まだSalesforce上に類似の問題が残存しているおそれが懸念されます。クラウドサービスカスタマだけでは、類似の問題の発見が難しいため、セキュリティの専門家やセールスフォースドットコム社の調査に期待しましょう。

4. 脆弱性

本稿では、Microsoft社のExchange Serverに生じた脆弱性を解説します。この脆弱性は、複数の脆弱性が関係した複合的な脆弱性で、複数の脆弱性のうち、JVNへ掲載されたCVSS v3 Base値の最大値は9.1と深刻なレベルです。既に悪用が確認されている脆弱性もあるため、早急に修正プログラムの適用、緩和策の実施が必要です。

4.1.Windows Exchange Serverに発生した脆弱性

2021年3月3日、Microsoft社は定例外のセキュリティ更新プログラムを公開しました [44]。この更新プログラムが修正する７つの脆弱性のうち、既に以下の４つの脆弱性の悪用が確認されています。

表 9：悪用が確認されているExchange Serverの脆弱性

CVE番号	概要
CVE-2021-26855	SSRF（Server Side Request Forgery：直接アクセスできないサーバへの攻撃）脆弱性
CVE-2021-26857	Undefined Messagingサービスの安全でないデジリアライズ脆弱性
CVE-2021-26858	任意のファイルへの書き込み
CVE-2021-27065	任意のファイルへの書き込み

米国サイバーセキュリティインフラセキュリティ庁（CISA）は、上記の脆弱性について緊急指令 [45]を発令しました。CISAの緊急指令は、深刻なサイバーセキュリティの脅威が検出された際、米国の政府機関に緊急指令を出せるという法律に基づくものです。Exchange Serverは、米国政府調達基準に含まれている製品です。このような製品に深刻な脆弱性が発覚した場合、政府の機密情報が外部に漏えいすることが考えられるため、CISAは緊急対応を指示しました。

4.2. タイムライン

表 10に脆弱性が発見されてから公開されるまでの出来事の時系列を示します。

表 10：Exchange Server脆弱性の公開までの時系列

日付	できごと
2020年12月10日	DEVCORE社が認証プロキシの脆弱性（CVE-2021-26855）を発見 [46]
2021年1月3日	Volexity社が上記脆弱性を悪用したサイバー攻撃を確認 [47]
2021年1月5日	DEVCORE社がMicrosoft社へ報告 [46]
2021年1月27日	Dubex社がデジリアライズの脆弱性（CVE-2021-26857）を悪用した攻撃をMicrosoft社に報告
2021年2月28日	複数の脅威グループによる本脆弱性の悪用を観測
2021年3月3日	Microsoft社が修正プログラムを配布

本脆弱性は、Microsoftから公表された2021年3月3日より前の2020年12月10日に、台湾のセキュリティ企業「DEVCORE」のOrange Tsai氏が発見しました。脆弱性公開前に攻撃が観測されたゼロディ脆弱性です。2021年3月3日の修正プログラムの配布後、3月9日にはGitHub上にPoCコードが公開されたり、本脆弱性を悪用する攻撃の急増が確認されたりしています。Microsoft社は、中国で活動している攻撃グループ「HAFNIUM」や、ランサムウェア「DearCry」が本脆弱性を悪用していると述べています [48]。他にも、複数の脅威グループによる悪用が報告されています。今回はゼロディ攻撃であったため、脆弱性への対応ができておらず攻撃が多発したと考えられます。その結果、KrebsOnSecurityの記事によると、本脆弱性によって米国全体で少なくとも30,000以上の組織が攻撃を受けたと述べています [49]。

4.3. 攻撃の流れと対策

攻撃者は、443ポートを介したCVE-2021-26855のSSRF脆弱性を悪用してExchange Serverの認証を回避したあと、CVE-2021-26857のデシリアライズの脆弱性を悪用して管理者に成りすますことができます。この攻撃方法はExchangeのプロキシアーキテクチャとログオンメカニズムを悪用することから、DEVCORE社によって「Proxylogon」と命名されました。攻撃者は管理者に成りすましたあと、任意のコードを実行できます。攻撃者は、他にもCVE-2021-26858やCVE-2021-27065の脆弱性を悪用して任意のファイルを書き込めます。

Microsoft社からは修正プログラムと緩和策、そしてCVE-2021-26855のSSRFの脆弱性チェックツールが公開されています [44]。本脆弱性はゼロディ脆弱性のため、インターネットへ公開しているシステムは、修正プログラムの提供前に侵入されているおそれがあります。攻撃者が侵入してバックドアを設置している場合は、修正プログラムを適用してもバックドア

経由で攻撃者が侵入できてしまいます。まずは攻撃者の侵入の有無を調査してください。攻撃者が侵入している場合は、ネットワークを物理遮断して侵入している攻撃者の排除とバックドアを削除したあとで修正プログラムを適用しなければなりません。

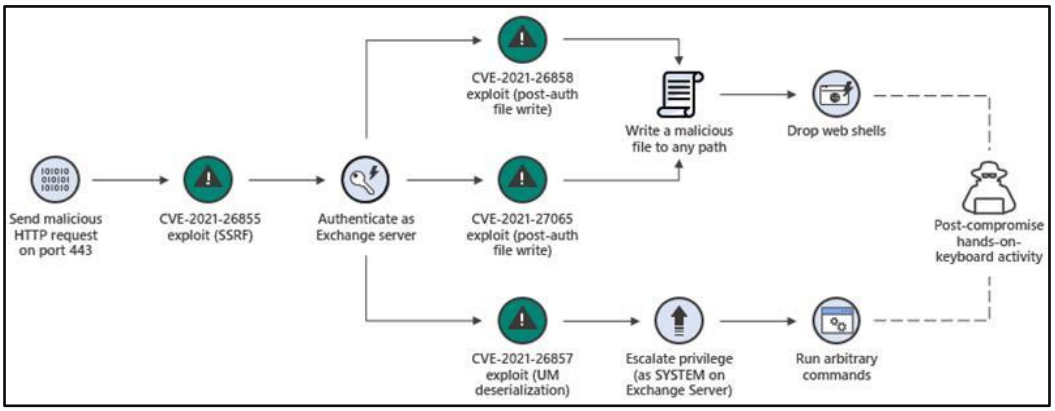


図 6： Exchange Serverのエクスプロイトチェーン [50]

4.4. まとめ

本稿では、Microsoft社のExchange Serverのゼロディ脆弱性を取り上げました。Palo Alto Networks社は、Expandsプラットフォームを使って調査した結果から、修正プログラム公開から5日経った3月8日時点でパッチ適用していないインターネット公開状態のExchange Serverが世界に12万5000台以上残っていたと推測しています [51]。すでに攻撃が行われて被害も発生している危険な脆弱性にもかかわらず、多くの組織は対応が遅れていました。

対策が遅れている理由として、それらの組織は、脆弱性が公表されてから次のアクションが起こせていないのかもしれません。2019年に日本損害保険協会が中小企業経営者向けに実施したサイバーリスク意識調査では、サイバー攻撃への対策の課題として「サイバー攻撃への対策方法がわからない」、「誰に相談すればよいのかわからない」と回答した企業が大企業に比べて多く見られました。また、24%の企業が「サイバー攻撃に対する対策をしていない」と回答していることから、脆弱性を対策せずにそのまま放置しているおそれもあります [52]。脆弱性を放置している企業は、まず自社内のシステムやソフトウェアのバージョンを確認しましょう。危険な脆弱性が残存しているシステムやソフトウェアを使っている場合は、なるべく早くパッチを適用してください。パッチ適用は、その一度だけでは終わりではありません。定期的に脆弱性情報を確認してパッチ適用を続けなければなりません。脆弱性対応の運用体制と運用サイクルを定めて、継続的に実施しましょう。そしてできるだけ迅速にシステムやソフトウェアの脆弱性情報を収集しましょう。脆弱性情報を頻繁に収集できない場合は、脆弱性情報の自動配信サービスやバージョン管理を支援するツールやサービスの活用を推奨します。

5. マルウェア・ランサムウェア

5.1. 2020年度第4四半期の概況

2020年度第3四半期から引き続き、マルウェアやランサムウェアによる被害報告がされています。マルウェアEmotetは、世界中で2014年から近年まで大規模な被害を与えていましたが、欧州刑事警察機構（EUROPOL）と欧州司法機構（EUROJUST）は、Emotetを遠隔操作するための運用基盤を停止することに成功したことを発表しました。

また、2019年度第4四半期に取り上げたスミッシングは、日本国内の対策が遅れており、被害が拡大していると報告されています [53] [54] [55]。

本稿では、2014年から被害を与えていたEmotetの運用基盤の停止の経緯や日本の対応と、変化したスミッシングの攻撃手法と日本国内で報告されている被害事例について記載します。

5.2. Emotet テイクダウン作戦「Operation LadyBird」

Emotetは、ユーザが正規のメールを装った攻撃メールの添付ファイルを実行してコンピュータに感染し、コンピュータ内の情報を窃取する、又はコンピュータへ別のマルウェアを感染させるマルウェアです [56]。攻撃者は、Emotetを使って狙ったユーザへ標的型攻撃を仕掛けます [57]。 2020年1月27日に、EUROPOLとEUROJUSTの調整の下で、オランダ、ドイツ、アメリカ、イギリス、フランス、リトアニア、カナダ、及びウクライナの8か国の警察が協力して実行した作戦「Operation LadyBird」によって、Emotetの運用基盤が停止しました [58]。Operation LadyBirdの実施結果 [58] は、以下のとおりです。

(1) Emotetを遠隔操作する上流C&Cサーバの押収
(2) Emotetを制御し無害化
(3) Emotetの運用・保守グループのメンバの逮捕

本稿では、Emotetのテイクダウン作戦の詳細とEmotetのテイクダウン後のEmotetの対応を説明します。

5.2.1. 国際協力によるEmotetのテイクダウン

オランダ、ドイツ、アメリカ、イギリス、フランス、リトアニア、カナダ、及びウクライナの8か国の警察は、協力して「Emotet」の運用基盤を捜査しました [59]。

2018年8月に、ドイツ警察はドイツ国内で感染が広がっていたEmotetの捜査を開始しまし

た。捜査を進めていくと、Emotetのボットネットを構成する複数のC&Cサーバを特定できました [60]。押収したドイツ国内のC&Cサーバに保管されていたデータを分析することにより、さらに欧州の複数の国で稼働するC&CサーバやEmotetの感染範囲を特定できました。しかし特定したC&Cサーバがドイツ国外に存在していたため、ドイツ警察は関係する他国の警察及び国際警察と協力して捜査をすすめました。その結果、オランダ、リトアニア、ウクライナにあるEmotetのボットネットを構成するC&Cサーバを押収しました [60]。押収されたC&Cサーバのデータを分析した結果、ついにボットネットを経由してEmotetを遠隔操作する上流のC&Cサーバ2台の場所を特定し、押収できました [61]。

オランダ警察は押収したC&Cサーバを用いて、Emotetに感染したコンピュータがオランダ警察の管理するC&CサーバとのみEmotetの設定を変更しました [62]。そのあと、そのC&Cサーバから無害化された検体を配布して、コンピュータに感染しているEmotetを無害化されたEmotetへアップデートしました [59] [61]。この取り組みにより、大量のEmotetを無害化してEmotetの被害を終息させました [62]。

Operation LadyBirdでは、Emotetの運用基盤の押収に加え、Emotetを運用・保守するグループのメンバの一部の逮捕にも成功しました。Operation LadyBirdに参加したウクライナ警察によって、Emotetの運用基盤を保守していたとされる2人の容疑者を逮捕しました [63]。この時に押収した情報から、Emotetがアメリカ及びヨーロッパの金融機関に対して25億ドルの被害を与えていたことが判明しました [63]。この2人の容疑者は、不正アクセスやマルウェアの作成、詐欺等の罪により最大12年の懲役刑となる可能性があります [63] [64]。ウクライナ警察は、今回の捜査でEmotetを使用してサイバー攻撃を行った他のグループも特定して、逮捕に向けて動いています [63]。

5.2.2. Emotetテイクダウン後のEmotet対応

Operation LadyBirdは、複数のC&Cサーバを押収して停止させましたが、すべてのC&Cサーバを停止させることはできませんでした。そのためドイツ警察は、Emotet用のシンクホールサーバを設置しました。シンクホールサーバとは、マルウェアがDNSへC&Cサーバの名前解決をリクエストしたときに、そのC&Cサーバとは異なる無害なIPアドレスを回答して、マルウェアからC&Cサーバへの通信を防止したり、マルウェアに感染したマシンのIPアドレスを特定したりする特殊なDNSサーバです。

EUROPOL及びEUROJUSTによる取り組みよって、Emotetは無害化されましたが、無害化の前に二次感染したマルウェア Ursnif、Trickbot、Qbot、Zloader、及びIcedIDは駆除されるわけではありません [65]。2021年1月27日にOperation LadyBirdによってEmotetの運用基盤が停止した後、ドイツ警察が管理するEmotet用のシンクホールサーバへ通信がとどいたIPアドレスや、押収されたC&Cサーバのデータから発見されたメールアドレスは、各国を代表するCSIRTへ提供されました。各国を代表するCSIRTは、このIPアドレスを使用して二次感染した

マルウェアの駆除を実施しました。

日本国内にあるEmotetに感染したコンピュータも、ドイツ警察が管理するC&Cサーバと通信を行った場合、その通信データがJPCERT/CCへ情報提供されるようになりました [58]。JPCERT/CCは、情報提供された通信記録データをもとに、日本国内で約900台のコンピュータがEmotetに感染していることを確認しました。2月以降になっても500台のコンピュータがEmotetに感染したまま残っていました [58]。

JPCERT/CCは、ドイツ警察から受け取った感染したコンピュータのIPアドレスをインターネットサービスプロバイダへ提供しました。インターネットサービスプロバイダは、IPアドレスから、Emotetに感染したコンピュータのユーザを特定して、二次感染したマルウェアの駆除方法を連絡しました。連絡を受け取ったユーザは、これに従って二次感染したマルウェアの駆除を行いました [66] [67]。

また盗まれてインターネット上へ拡散したおそれがある情報も、回収されたり削除されたりするわけではありません。オランダ警察は、これまでに押収したC&Cサーバに保存されていた窃取情報を集めて、感染コンピュータのユーザが自身の情報の窃取の有無を調査できるWebサイトを構築して公開しました [62]。ユーザは、このWebサイトへ自身のメールアドレスを入力すれば、自身のメールアドレス、アカウント名、パスワードといった認証情報やその他の情報が窃取されていないかどうかを確認できます。認証情報が窃取されていた場合は、認証情報を悪用されて各種サービスへ不正ログインされないように、すぐにパスワードを変更してください。

Emotetの運用基盤停止は、EUROPOLとEUROJUSTの調整の下で、オランダ、ドイツ、アメリカ、イギリス、フランス、リトアニア、カナダ、及びウクライナの8か国の警察が協力して実行したとても大きな成果です。Operation LadyBirdによってEmotetは終息しましたが、2020年度第3四半期で紹介した「IcedID」というEmotetに類似したマルウェアによる攻撃は絶えず発生しています [62]。攻撃者の手は休まることはないと考え、行動し、対処していく必要があります。

5.3. スミッシングの最新動向

スミッシングとはフィッシング詐欺の一つの形で、情報を窃取する攻撃手法の一つです。スマートフォンに対して、正規のショッピングサイトや宅配不在通知等のサービスを装ったSMSメッセージを送信し、受信者を不正なWebサイトに誘導し、個人情報や認証情報等の情報を窃取することを試みます [68]。

スミッシングによる被害が拡大しているため、本稿ではスミッシングの攻撃手法、被害状況、及び対策について解説します。

5.3.1. スミッシングの被害状況

フィッシング詐欺全般の被害件数が増加してきている中で、スミッシングによる被害件数も増加傾向にあります。2020年度第4四半期におけるフィッシング詐欺全般の被害件数は、2021年1月は前年のどの月よりも多い件数が報告され、2月は低水準となったものの、3月にはすぐ1月と同等の水準に戻りました [53] [54] [55]。スミッシングの具体的な件数は記載されていませんが、フィッシング対策協会は、スミッシングの被害件数が増加傾向にあると言っています [53] [54] [55]。スミッシングの被害は、日本国内だけでなく海外でも多く、FBIによるアメリカ国民を対象としたインターネット犯罪の調査報告書よると、2020年だけで241,342件、約5,400万ドルに及ぶ被害が発生しています [69] [70]。アメリカでも、スミッシングを含めたフィッシング詐欺が増加しています。

5.3.2. スミッシングの種類

ユーザを不正なWebサイトへ誘導するスミッシングのメッセージは、表 11に示すように「サービスを装うメッセージ」と「サービスのセキュリティ機能を装うメッセージ」に分類できます。

表 11：ユーザを不正なWebサイトへ誘導するメッセージ

種類	説明
サービスを装う	サービスからの通知のSMSメッセージを装った偽のSMSメッセージを送る。 【例】 ● クロネコヤマトや佐川急便などの宅配業者の不在通知メッセージを装う [71] ● 楽天市場などのショッピングサイトの商品発送通知メッセージを装う [72]
サービスのセキュリティ機能を装う	サービス使用時の多要素認証やアクセス確認のメッセージなど、セキュリティ機能のメッセージを装う。 【例】 ● 三井住友銀行からの「第三者からの不正アクセスを検知したため確認をして下さい。」という警告メッセージを装う [73] ● 三井住友銀行からの支払い承認のメッセージを装う ● SNSへのアクセス確認のメッセージを装う

攻撃者は、上記のようなメッセージでユーザを不正なWebサイトへ誘導したり、不正なアプリケーションを実行させたりして、ユーザの情報を盗みます。ユーザの情報盗む方法を表12に記載します。

表 12：情報窃取の手口

種類	説明
不正なWebサイト	SMSメッセージに不正なWebサイトのURLを記載し、Webサイトにアクセスしたユーザに個人情報や認証情報といった情報を入力させ、情報を窃取する [71]
不正なアプリケーション	SMSメッセージに記載したURLから、ユーザに不正なアプリケーションをダウンロードさせる。そのあと、ユーザが不正なアプリケーションをインストールして、かつ不正なアプリケーションの権限付与の要求を許可する。その結果、不正なアプリケーションが、スマートフォン上の連絡帳等から情報を窃取して、インターネット上の攻撃者へ送信する [72]

攻撃者は、上記の手口により窃取した情報を悪用し、ネットバンキングを介した不正送金等のサービスの悪用や更なるスミッシングの拡散など被害を拡大させます。

5.3.3. スミッシングに対する対策

Proofpoint社の報告書によると、未だに多くのユーザがスミッシングの攻撃手口を認識すらしていないと報告されています。また、同報告書において、調査対象の半数以上の企業が、スミッシングのセキュリティトレーニングを実施していないという結果も報告されています[74]。上記を踏まえると、スミッシングの被害が続いている理由は、ユーザへのスミッシングのリスクの周知が不足していると考えられます。

スミッシングを知らないユーザには、まずスミッシングというサイバー攻撃の存在とその危険性を知ってもらうことです。一般ユーザは、情報セキュリティの情報を発信している情報処理推進機構（IPA）のWebサイトを見る機会が少ないでしょう。そのため、スミッシングに悪用されている金融機関や運送業者等のサービス提供者が、サービスのユーザに対して積極的に注意喚起を行っていくことが必要です。サービス提供者は、ユーザが利用するWebサイトやアプリケーションを介して、積極的にスミッシングの注意喚起を行えば、多くのユーザへスミッシングを知ってもらうことができます。また、ユーザに対する注意喚起の中でスミッシングのSMSメッセージの実例を公表すれば、サービスを利用するユーザがスミッシングのSMSメッセージに騙される確率が低減し、被害件数が減少するでしょう。さらに、サービス利用に対するユーザの安心感や信頼の向上にも繋がります。

企業などの組織は、セキュリティ教育やフィッシングシミュレーションといった演習を定期的に開催して、スミッシングに対する社員の意識啓発や理解、及びスキルの向上を図るこ

とができます。

最近は、攻撃者によって、スミッシングやフィッシング詐欺のメッセージや不正なWebサイト、不正なアプリケーションが巧妙に作り込まれています。上記のようなスミッシングのSMSメッセージの注意喚起だけでは、被害を防ぐことが困難になってきています。そこでユーザには、以下のような機能を備えた技術的対策の導入を推奨します。

- スミッシングのSMSメッセージを受信拒否する機能を有効化にする。通信プロバイダから提供される怪しいSMSメッセージの条件に合致したSMSメッセージをブロックする [75]。
- スマートフォンのURLフィルタリング機能を有効にする。ユーザがSMSメッセージに記載された不審なURLをタップしても、既知のフィッシングサイトへの通信を自動的に遮断する [76]。
- 必ず公式ストアからアプリケーションをインストールする。公式ストアのAppStoreやGoogle Playに公開されている審査済みのアプリケーションをインストールする。また、iOS及びAndroid端末は、アプリケーションのインストールが公式ストアからだけに制限されている。この設定を無効化しない。
- 社用のスマートフォンの場合、EMMやMDMを導入して、許可されたアプリケーションだけを端末へインストールさせたり、危険なアプリケーションのインストールを禁止したりして、スマートフォン上のアプリケーションを管理する [77]。

5.4. まとめ

今回、本稿ではEmotetのテイクダウンとスミッシングの動向について紹介しました。Emotetの運用基盤は、欧米8か国の法執行機関が協力したテイクダウン作戦「Operation LadyBird」によって無害化されました。この事例は、Emotetのような世界的に被害を及ぼすマルウェアの根本的解決には、国境を越えた協力が必要であることを示しました。Emotetは終息しましたが、Emotetによって盗まれた情報は返ってこず、また二次感染したマルウェアも自動的に駆除されるわけではありません。第三者が盗まれたパスワードを悪用して不正アクセスしないようにパスワードを変更して、二次感染したマルウェアの被害を止めるために駆除を実施しましょう。

まだまだ多くのユーザが、スミッシングというサイバー攻撃を知りません。一人でも多くのユーザがスミッシングという脅威を認識して対応するように、サービスを提供する企業が中心となって注意喚起等の啓発活動を実施していく必要があります。

Emotetとスミッシングのいずれにも該当しますが、ユーザ及び企業はそれぞれ継続的にマルウェアを含むセキュリティに関する最新の情報を収集し、脅威を正しく認識したうえで、適切な対応を取っていく必要があると考えます。

6. 予測

情報漏えい事件の二次被害に警戒

社会情勢や法制度からも個人情報保護の機運は高まっていますが、依然として漏えい事件は後を絶ちません。2021年5月には、婚活サイトのOmiai（ネットマーケティング社）について、ユーザの運転免許証を含む本人確認書類の画像データが流出しました。Omiaiの本人確認書類の画像データ流出は約171万件と発表されており [78]、攻撃者は、この流出した画像データを使って運転免許証の画像を偽造できてしまいます。そのため、今後、このような本人確認書類の画像データを悪用したなりすましが増加すると予測します。例えば、上記の本人確認書類1枚だけを用いて本人確認していたオンライン銀行は、運転免許証の偽造画像を使った攻撃者の口座開設の申請を承認してしまうかもしれません。オンラインで本人確認する手段として、eKYCが広く使われています [79]。eKYCは、犯罪収益移転防止法に基づいて4段階の確認方法が定められています。本人確認の信頼性が最も低い「身分証撮影＋容貌撮影」の方法では、今回の流出データを用いて偽装した運転免許証により、なりすましが成立してしまう恐れがあります。eKYCで用意されている他の本人確認方法には、ICチップの読み取りや、クレジットカードの照合といった、別の媒体を併用する多要素認証があります。なりすましが多発するようであれば、より信頼性の高い本人確認方法に切り替えることを検討する必要があります。

本人確認の重要性は企業やサービスによってまちまちです。自社のサービスにおいて本人確認書類の偽装はどれくらいのリスクがあるのかを算定し、リスクの回避や低減、受容といった対策を講じることが必要です。

ワクチン接種を装ったスミッシング詐欺

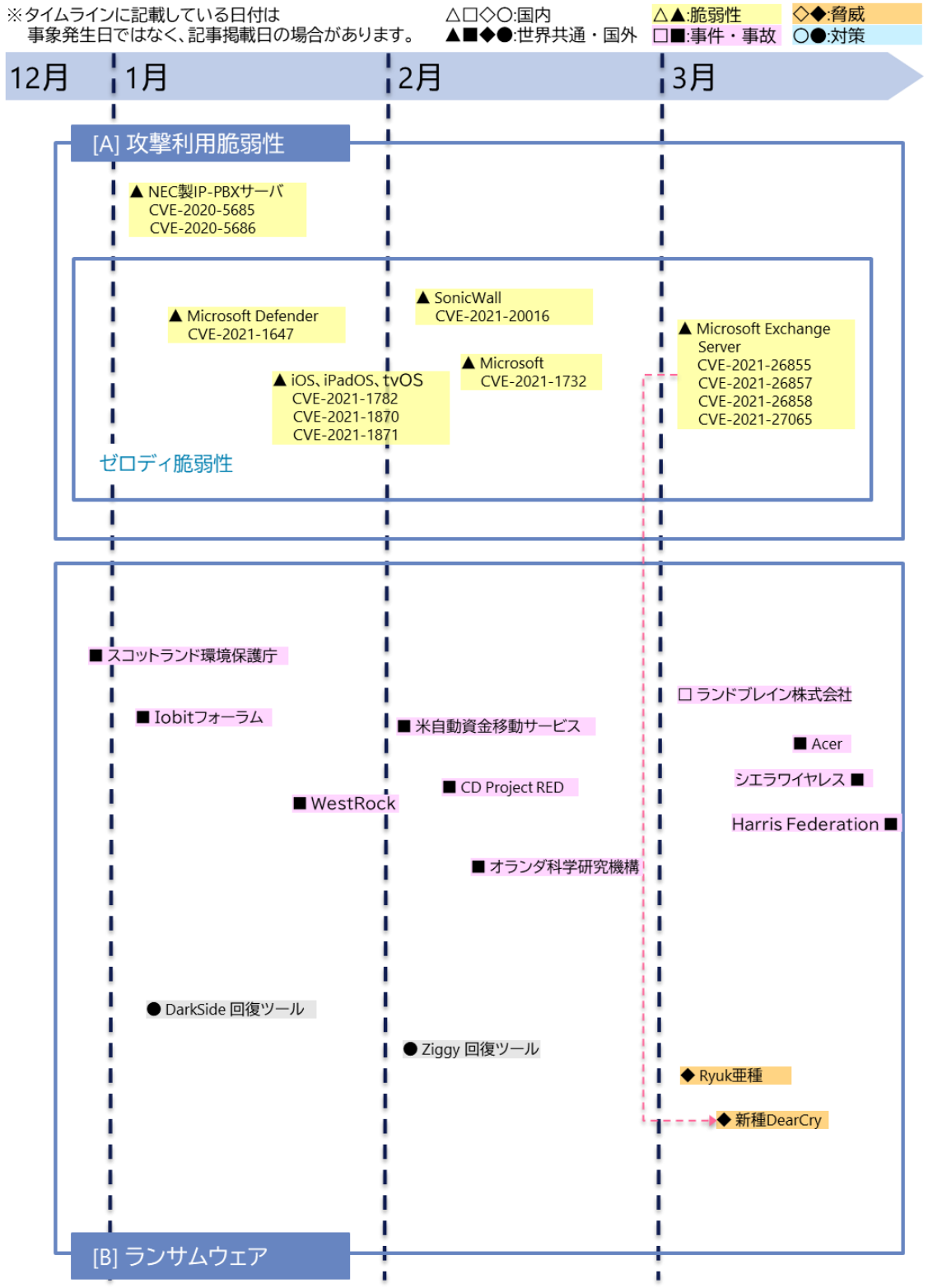
新型コロナウイルスのワクチン接種に関する詐欺が横行しています。現在は、高齢者のワクチン接種を優先しているため、高齢者をターゲットにした電話や訪問による詐欺が多く、被害が相次いでいます。6月からはより幅広い年代が接種対象になるため、電話や訪問ではなく、インターネットを使った詐欺が増えると予測します。その方法の一つとして、攻撃者がスミッシングを多用すると予測します。例えば、政府関連機関を装って「医療者向けのワクチンが余ったので、有料で接種可能」 [80]、「特別に副反応の少ないワクチンの接種ができるが、金銭が必要」のようなメッセージをスマホへ送り、攻撃者の口座へ現金を振り込ませる、あるいは偽のフィッシングサイトにクレジットカードなどの情報を入力させる、といった攻撃が予想できます。ワクチン接種に関して金銭を要求するメッセージは詐欺です。新型コロナウイルス関連のメッセージを受信して、すこしでも怪しいと思った場合は、国民生活センターの「新型コロナワクチン詐欺 消費者ホットライン: フリーダイヤル：0120-797-188」 [81]へ相談してください。

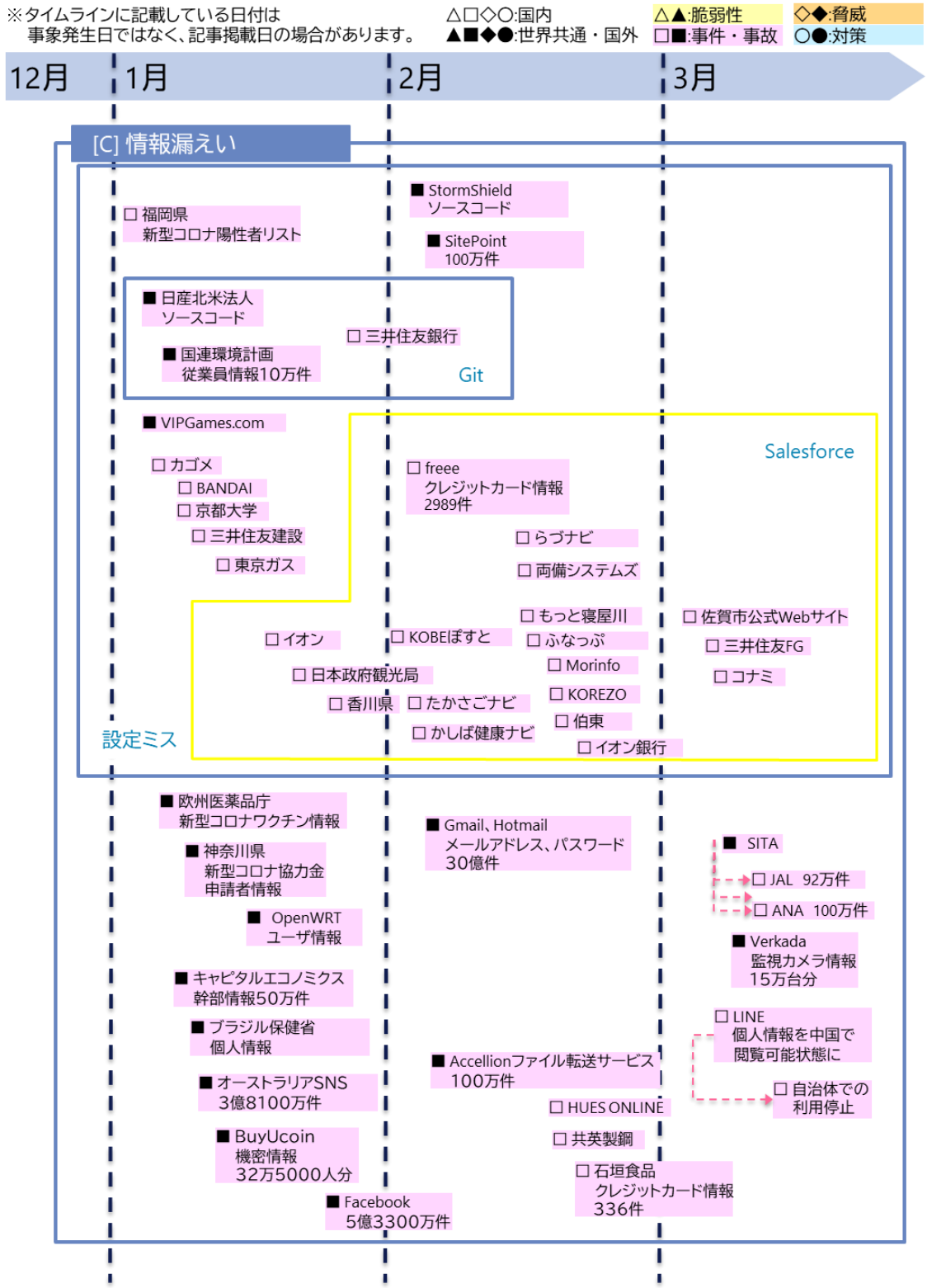
二重脅迫ランサムウェア攻撃の継続

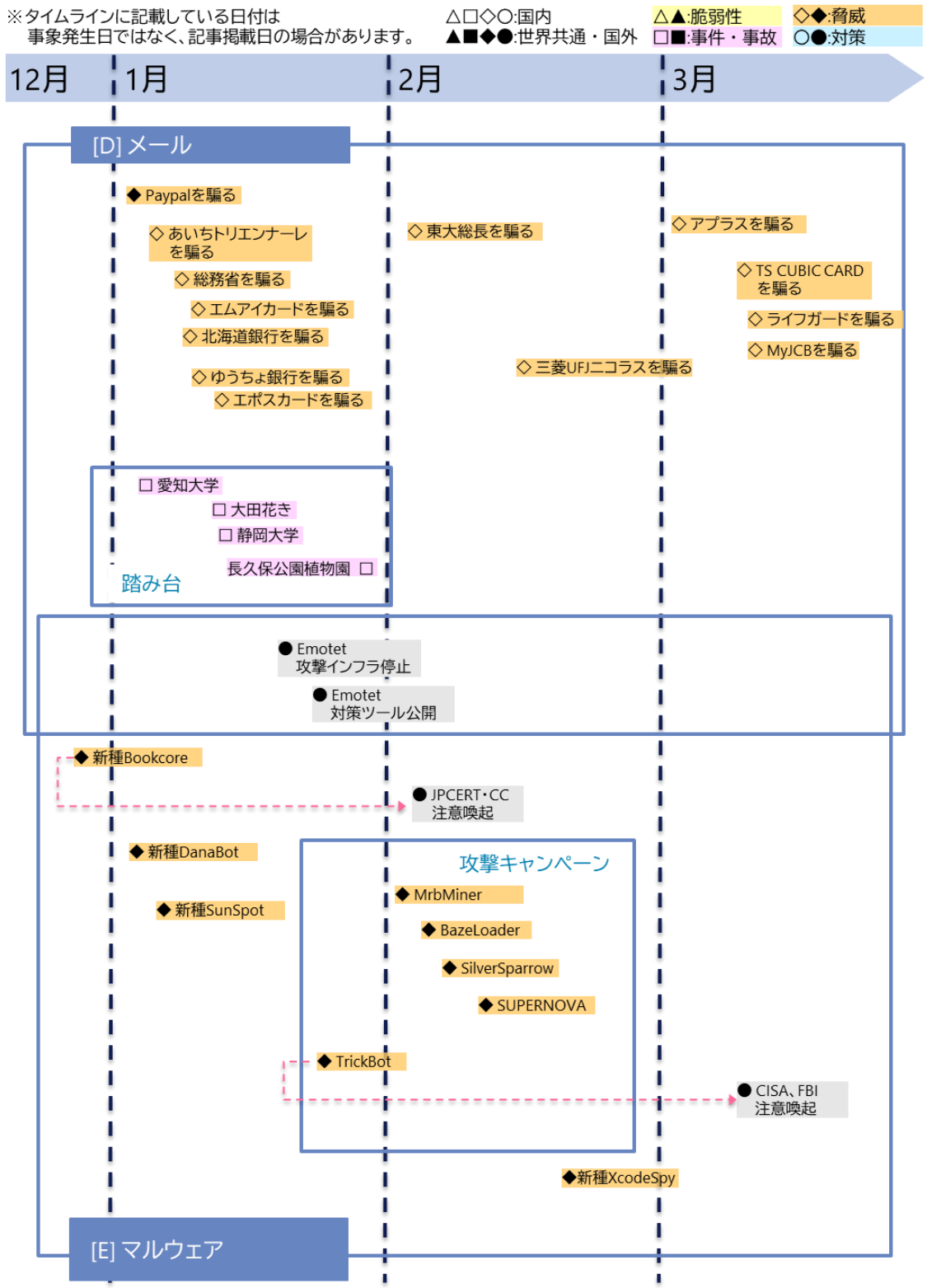
2020年度第3四半期のレポートでは、二重脅迫ランサムウェア攻撃を取り上げました。第4四半期も、ゲーム開発企業のCD Projekt S.A.や公共事業を広く受託しているランドブレイン社等が、ランサムウェア攻撃を受けました [82] [83]。米保険会社のCNA Financialは、2020年の最高額の4000万ドルの身代金の支払いに同意したことが報じられました [84]。

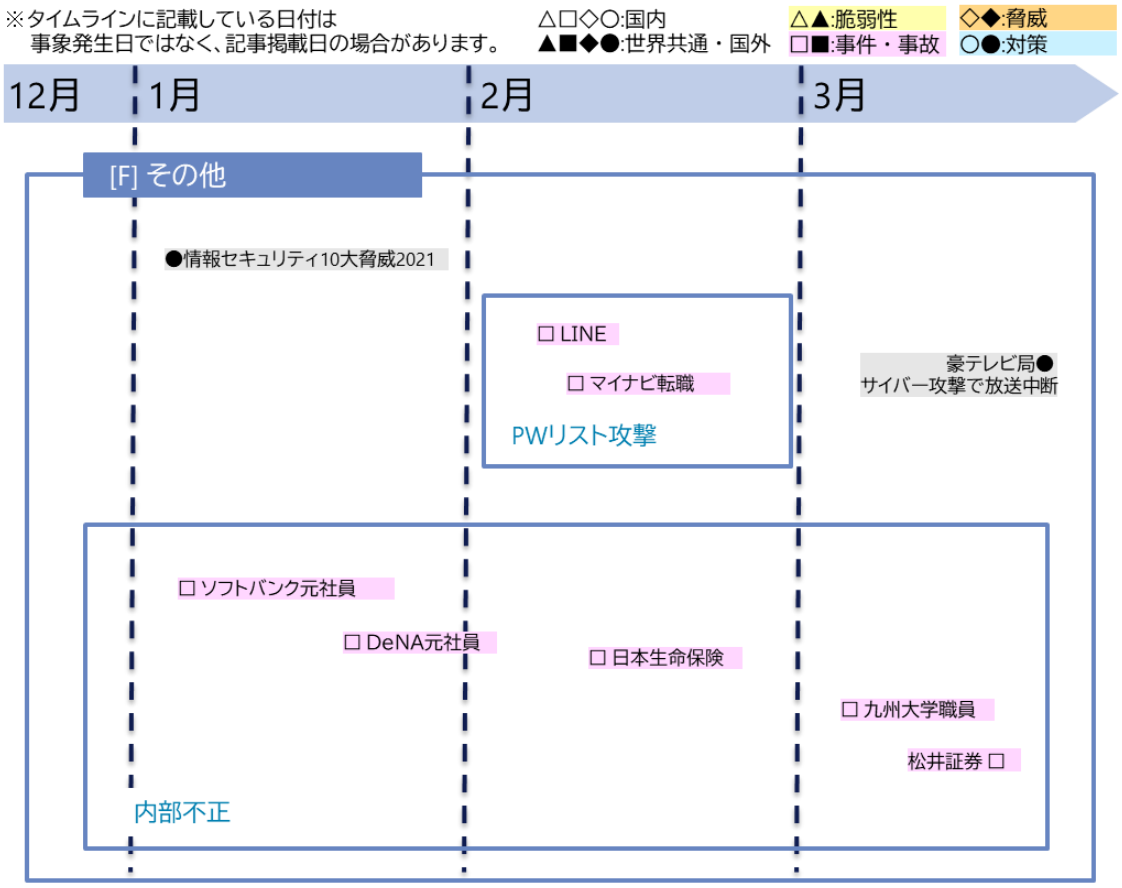
2020年10月の米国財務省の外国資産管理局（OFAC）の勧告のように、身代金の支払いは犯罪を助長する行為のため、禁止する動きが増えています。そのため、身代金を支払うケースは、今後減少していくと考えられます [85]。しかし、攻撃された組織は二重脅迫ランサムウェアにより情報を公開されて、大きなダメージを受けるかもしれません。そのような場合がある限り、身代金を支払ってしまうというケースは、今後も残り続けるでしょう。

7. タイムライン









参考文献

[1] 個人情報保護委員会, “「個人情報の保護に関する法律等の一部を改正する法律（概要）」より抜粋編集,” [オンライン].

[2] 佐脇紀代志, “一問一答 令和2年改正個人情報保護法,” 商事法務, 2020, pp. 53-4.

[3] 一般社団法人日本情報経済社会推進協会, “CBPR認証,” 17 5 2021. [オンライン]. Available: https://www.jipdec.or.jp/protection_org/cbpr/.

[4] 一般社団法人日本情報経済社会推進協会, “十分性認定後の日本企業のGDPR対応　越境データ移転を中心に,” 18 4 2019. [オンライン]. Available: https://www.jipdec.or.jp/library/report/20190418.html.

[5] 個人情報保護委員会, “個人情報の保護に関する法律に係るEU及び英国域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール,” [オンライン]. Available: https://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf.

[6] 佐脇紀代志, “一問一答 令和2年改正個人情報保護法,” 著: *一問一答 令和2年改正個人情報保護法*, 商事法務, 2020, p. 96.

[7] 個人情報保護委員会, “改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）,” 4 11 2020. [オンライン]. Available: https://www.ppc.go.jp/files/pdf/201104_ekkyouiten.pdf.

[8] NHK, “LINE社長 中国からの個人情報へのアクセス遮断を明らかに,” 23 3 2021. [オンライン]. Available: https://www3.nhk.or.jp/news/html/20210323/k10012931491000.html.

[9] 個人情報保護委員会, “「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するQ＆A,” 個人情報保護委員会, 12 11 2019. [オンライン]. Available: https://www.ppc.go.jp/files/pdf/1911_APPI_QA.pdf.

[10] 佐脇紀代志, 一問一答 令和2年改正個人情報保護法, 商事法務, 2020.

[11] 個人情報保護委員会, “個人情報の保護に関する法律に基づく行政上の対応について,” 23 4 2021. [オンライン]. Available: https://www.ppc.go.jp/files/pdf/210423_houdou.pdf.

[12] 読売新聞オンライン, “「ＬＩＮＥ」個人情報が丸見え、管理委託の中国企業から…運用見直しを検討,” 17 3 2021. [オンライン]. Available: https://www.yomiuri.co.jp/national/20210317-OYT1T50123/.

[13] 朝日新聞DIGITAL, “日本のLINE利用者の画像・動画全データ、韓国で保管,” 17 3 2021. [オンライン]. Available: https://www.asahi.com/articles/ASP3K64ZCP3KUHBI01W.html.

[14] 西村あさひ法律事務所 濱野 敏彦, “BUSINESS LAWYERS,” 4 1 2021. [オンライン]. Available: https://www.businesslawyers.jp/practices/1314.

[15] NHK, “LINE利用でガイドライン “機密情報 残さない仕組みを” 政府,” 1 5 2021. [オンライン]. Available: https://www3.nhk.or.jp/news/html/20210501/k10013007361000.html.

[16] 朝日新聞DIGITAL, “「漏洩は確認してない」 LINE社長の会見、一問一答,” 23 3 2021. [オンライン]. Available: https://www.asahi.com/articles/ASP3R7R94P3QUTIL06F.html.

[17] 東洋経済オンライン, “中国が「個人情報保護法」制定に踏み出す事情,” 23 10 2020. [オンライン]. Available: https://toyokeizai.net/articles/-/382436.

[18] 個人情報保護委員会, [オンライン]. Available: https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/.

[19] 株式会社 野村総合研究所, “個人情報の保護に関する事業者の取組実態調査（平成２９年度）報告書,” 3 2018. [オンライン]. Available: https://www.ppc.go.jp/files/pdf/personal_report_3003_jigyosya.pdf.

[20] 松井証券株式会社, “業務委託先元従業員の逮捕について,” 24 3 2021. [オンライン]. Available: https://www.matsui.co.jp/parts/pdf-view/web/viewer.html?file=/company/ir/press/pdf/pr210324.pdf.

[21] SCSK株式会社, “https://www.scsk.jp/news/2021/pdf/20210324.pdf,” 24 3 2021. [オンライン]. Available: https://www.scsk.jp/news/2021/pdf/20210324.pdf.

[22] 日経クロステック／日経コンピュータ, “SCSK元社員の2億円不正出金事件はなぜ起こった？IT大手8社の内部不正対策を調査,” 16 4 2021. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/column/18/00989/041400051/.

[23] 金融情報システムセンター, “金融機関等コンピュータシステムの安全対策基準・解説書（第9版改訂）,” 3 2019. [オンライン]. Available: https://www.fisc.or.jp/publication/book/003930.php.

[24] 金融情報システムセンター, “金融機関等コンピュータシステムの安全対策基

準・解説書（第9版改訂）,” 2019, p. 統制基準（第９版）統９.

[25] 金融情報システムセンター, “金融機関等コンピュータシステムの安全対策基準・解説書（第9版改訂）,” 2019, p. 実務基準（第９版）実３.

[26] Security NEXT, “松井証券で顧客資産約2億円が不正引出 - 長年業務に携わる委託先SEが権限悪用,” 25 3 2021. [オンライン]. Available: https://www.security-next.com/124542.

[27] 日本経済新聞, “松井証券顧客の株式を無断売却か　SCSKエンジニア逮捕,” 24 3 2021. [オンライン]. Available: https://www.nikkei.com/article/DGXZQODG246R70U1A320C2000000/.

[28] 株式会社ＮＴＴデータ　セキュリティ技術部, “サイバーセキュリティに関するグローバル動向四半期レポート（2020年7月～9月）を公開,” 11 12 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/news/information/2020/121100/.

[29] 金融情報システムセンター, “金融機関等コンピュータシステムの安全対策基準・解説書（第9版改訂）,” 2019, p. 監査基準（第９版）監１.

[30] 日本経済新聞, “JAL、92万人分の情報流出　マイレージ会員対象,” [オンライン]. Available: https://www.nikkei.com/article/DGXZQODZ05ABI0V00C21A3000000/.

[31] 日本経済新聞, “ANAも100万人分流出　マイレージ情報、不正被害は未確認,” [オンライン]. Available: https://www.nikkei.com/article/DGXZQODZ060KO006032021000000/.

[32] SITA, “SITA statement about security incident,” [オンライン]. Available: https://www.sita.aero/pressroom/news-releases/sita-statement-about-security-incident/.

[33] Pestalozzi Attorneys at Law, “The revised Federal Act on Data Protection,” [オンライン]. Available: https://pestalozzilaw.com/en/news/legal-insights/revised-federal-act-data-protection/.

[34] 日本貿易振興機構, “スイス連邦データ保護法改正案の内容およびEU「一般データ保護規則」との比較,” [オンライン]. Available: https://www.jetro.go.jp/ext_images/_Reports/01/74c0fb55f759d238/20170108.pdf.

[35] 全日空商事, “ANA MEDIAKIT ANAメディアキットのご案内,” [オンライン]. Available: https://www.anahd.co.jp/ana-

info/ana/mediadata/pdf/mediakit/ANA_MEDIA_KIT_outline.pdf.

[36] JALブランドコミュニケーション, “JAPAN AIRLINES MEDIA INFORMATION JAL 広告メディアのご案内,” [オンライン]. Available: https://www.jalbrand.co.jp/common/pdf/adv_all.pdf.

[37] Security NEXT, “「Salesforce」利用の複数フォームに設定不備 - 他社事例と異なる部分,” [オンライン]. Available: https://www.security-next.com/123273.

[38] 日本経済新聞, “イオンでも不正アクセス、セールスフォース製品で,” [オンライン]. Available: https://www.nikkei.com/article/DGXZQOFK280XJ0Y1A120C2000000/.

[39] freee, “クラウド型お問い合わせ管理システムに対しての第三者によるアクセスの可能性について,” [オンライン]. Available: https://corp.freee.co.jp/news/system-research.html.

[40] 両備システムズ, “クラウド型システムへの第三者からのアクセスについて,” [オンライン]. Available: https://www.ryobi.co.jp/news/notification20210210.

[41] 株式会社コナミデジタルエンタテインメント, “第三者のアクセスによる情報流出につい,” [オンライン]. Available: https://www.konami.com/games/corporate/ja/news/topics/20210301a/.

[42] 日本経済新聞, “三井住友FG傘下2社が顧客情報流出、システム設定不備で,” [オンライン]. Available: https://www.nikkei.com/article/DGXZQODF086CX0Y1A300C2000000/.

[43] 国際協力機構, “「PARTNER」への第三者による不正アクセスについて,” [オンライン]. Available: https://www.jica.go.jp/information/info/2020/20210316_10.html.

[44] Microsoft, “Microsoft Exchange Server 2019、2016、2013 用のセキュリティ更新プログラムについて: 2021 年 3 月 2 日 (KB5000871),” Microsoft, 2 3 2021. [オンライン]. Available: https://support.microsoft.com/ja-jp/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-march-2-2021-kb5000871-9800a6bb-0a21-4ee7-b9da-fa85b3e1d23b.

[45] Infrastructure Security Agency, “Emergency Directive 21-02,” Infrastructure Security Agency, 3 3 2021. [オンライン]. Available: https://cyber.dhs.gov/ed/21-02/.

[46] DEVCORE, “ProxyLogon,” DEVCORE, 3 2021. [オンライン]. Available:

https://proxylogon.com/.

[47] M. M. S. K. S. A. T. L. Josh Grunzweig, “Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities,” volexity, 2 3 2021. [オンライン]. Available: https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/.

[48] Microsoft, “HAFNIUM targeting Exchange Servers with 0-day exploits,” Microsoft, 2 3 2021. [オンライン]. Available: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/.

[49] KrebsOnSecurity, “At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft’s Email Software,” KrebsOnSecurity, 5 3 2021. [オンライン]. Available: https://krebsonsecurity.com/tag/microsoft-exchange-server-flaws/.

[50] Microsoft, “Analyzing attacks taking advantage of the Exchange Server vulnerabilities,” Microsoft, 25 3 2021. [オンライン]. Available: https://www.microsoft.com/security/blog/2021/03/25/analyzing-attacks-taking-advantage-of-the-exchange-server-vulnerabilities/.

[51] palo Alto Network, “Microsoft Exchange Server Attack Timeline,” palo Alto Network, 11 3 2021. [オンライン]. Available: https://unit42.paloaltonetworks.com/microsoft-exchange-server-attack-timeline/.

[52] 日本損害保険協会, “数字で見るサイバーリスクと保険,” 日本損害保険協会, 2020. [オンライン]. Available: https://www.sonpo.or.jp/cyber-hoken/data/2019-01/pdf/cyber_report2019.pdf.

[53] フィッシング対策協議会, “2021/01 フィッシング報告状況,” [オンライン]. Available: https://www.antiphishing.jp/report/monthly/202101.html.

[54] フィッシング対策協議会, “2021/02 フィッシング報告状況,” [オンライン]. Available: https://www.antiphishing.jp/report/monthly/202102.html.

[55] フィッシング対策協議会, “2021/03 フィッシング報告状況,” [オンライン]. Available: https://www.antiphishing.jp/report/monthly/202103.html.

[56] 独立行政法人情報処理推進機構, “「Emotet」と呼ばれるウイルスへの感染を狙うメールについて,” [オンライン]. Available: https://www.ipa.go.jp/security/announce/20191202.html.

[57] サービス &セキュリティ株式会社, “Emotetテイクダウン成功後の現状と今後の対策,” [オンライン]. Available: https://www.ssk-kan.co.jp/topics/?p=11545.

[58] 一般社団法人JPCERTコーディネーションセンター, “マルウェアEmotetのテイクダウンと感染端末に対する通知,” [オンライン]. Available: https://blogs.jpcert.or.jp/ja/2021/02/emotet-notice.html.

[59] Security Next, “「Emotet」を追い詰めた「Ladybird作戦」 - 攻撃者がバックアップ保有の可能性も,” [オンライン]. Available: https://www.security-next.com/122910.

[60] Bundeskriminalamt, “Infrastruktur der Emotet-Schadsoftware zerschlagen,” [オンライン]. Available: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html.

[61] POLITIE, “Internationale politieoperatie LadyBird: wereldwijd botnet Emotet ontmanteld,” [オンライン]. Available: https://www.politie.nl/nieuws/2021/januari/27/11-internationale-politieoperatie-ladybird-botnet-emotet-wereldwijd-ontmanteld.html.

[62] トレンドマイクロ株式会社, “サイバー犯罪の根本解決：EUROPOLによるEMOTETテイクダウン,” [オンライン]. Available: https://blog.trendmicro.co.jp/archives/27132.

[63] Національної поліції, “Кіберполіція викрила транснаціональне угруповання хакерів у розповсюдженні найнебезпечнішого в світі комп’ютерного вірусу «EMOTET»,” [オンライン]. Available: https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-transnaczionalne-ugrupovannya-xakeriv-u-rozpovsyudzhenni-najnebezpechnishogo-v-sviti-komp-yuternogo-virusu-EMOTET/.

[64] 日経XTECH, “最も危険なマルウエア「Emotet」が壊滅,” [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/mag/nnw/18/041800012/042100139/.

[65] ZDNet Japan, “マルウェア「Emotet」の国内感染は推定約500台--駆除活動が本格化,” [オンライン]. Available: https://japan.zdnet.com/article/35166831/.

[66] Malwarebytes Inc, “Cleaning up after Emotet: the law enforcement file,” [オンライン]. Available: https://blog.malwarebytes.com/threat-analysis/2021/01/cleaning-up-after-emotet-the-law-enforcement-file/.

[67] BLEEPINGCOMPUTER Inc, “Europol: Emotet malware will uninstall itself on April 25th,” [オンライン]. Available: https://www.bleepingcomputer.com/news/security/europol-emotet-malware-will-uninstall-itself-on-april-25th/.

[68] キヤノンマーケティングジャパン株式会社, “SMSを利用したスミッシングによるサイバー詐欺の危険性,” [オンライン]. Available: https://eset-info.canon-its.jp/malware_info/special/detail/201210.html.

[69] Proofpoint, Inc., “FBIインターネット犯罪報告書：2020年に最大の金銭的損失をもたらしたのはメール詐欺,” [オンライン]. Available: https://www.proofpoint.com/jp/blog/email-and-cloud-threats/fbi-internet-crime-report-shows-email-fraud-represents-largest.

[70] Federal Bureau of Investigation, “INTERNET CRIME REPORT 2020,” [オンライン]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[71] Whoscall株式会社, “スミッシンク□ってなに?被害事例やその手口・対策方法をこ□紹介,” [オンライン]. Available: https://whoscall.com/ja/blog/articles/196-%E3%82%B9%E3%83%9F%E3%83%83%E3%82%B7%E3%83%B3%E3%82%AF%E3%82%99%E3%81%A3%E3%81%A6%E3%81%AA%E3%81%AB%EF%BC%9F%E8%A2%AB%E5%AE%B3%E4%BA%8B%E4%BE%8B%E3%82%84%E3%81%9D%E3%81%AE%E6%89%8B%E5%8F%A3%E3%83%BB%E5%AF%BE%E7%AD.

[72] トレンドマイクロ株式会社, “偽装SMSから誘導される不正アプリをインストールしてしまったらどうなる？,” [オンライン]. Available: https://is702.jp/news/3803/partner/101_g/.

[73] ニフティ株式会社, “三井住友カードのなりすまし迷惑メールに注意|詐欺手口と見分け方について解説,” [オンライン]. Available: https://koneta.nifty.com/koneta_detail/1141008010565_1.htm.

[74] Proofpoint, Inc., “State of the Phish 2021,” [オンライン]. Available: 220252.37-pfpt-jp-a4-r-state-of-the-phish-2021.pdf.

[75] 株式会社NTTドコモ, “SMS拒否設定,” [オンライン]. Available: https://www.nttdocomo.co.jp/info/spam_mail/sms/.

[76] 株式会社Innovation & Co, “おすすめフィルタリングソフト８製品を徹底比較！選び方も解説！,” [オンライン]. Available: https://it-trend.jp/filtering/article/98-0002.

[77] 株式会社Innovation & Co, “EMMとは？MDMやMAMとの違いもわかりやすく解説！,” [オンライン]. Available: https://it-trend.jp/mdm/article/160-0005.

[78] 朝日新聞　DIGITAL, “婚活アプリの個人情報が流出か　免許証など171万件,” 朝日新聞社, 21 5 2021. [オンライン]. Available: https://www.asahi.com/articles/ASP5P5Q3PP5PULFA02S.html.

[79] 金融庁, “「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令」の公表について,” 30 11 2018. [オンライン]. Available: https://www.fsa.go.jp/news/30/sonota/20181130/20181130.html.

[80] 消費者庁, “便乗悪徳商法の注意喚起,” 消費者庁, [オンライン]. Available: https://www.caa.go.jp/policies/policy/consumer_policy/information/notice/efforts_002.html.

[81] 独立行政法人　国民生活センター, “「新型コロナワクチン詐欺　消費者ホットライン」をご利用ください,” 14 5 2021. [オンライン]. Available: http://www.kokusen.go.jp/info/data/coronavirus_vshotline.html.

[82] L. Abrams, “CD Projekt's stolen source code allegedly sold by ransomware gang,” BleepingComputer, 13 2 2021. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/cd-projekts-stolen-source-code-allegedly-sold-by-ransomware-gang/.

[83] Security NEXT, “不正アクセス被害のランドブレイン、調査結果を公表 - ランサムウェアは「Cring」,” Security NEXT, 19 5 2021. [オンライン]. Available: https://www.security-next.com/126310.

[84] K. M. a. W. Turton, “CNA Financial Paid $40 Million in Ransom After March Cyberattack,” Bloomberg, 21 5 2021. [オンライン]. Available: https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack.

[85] U.S. DEPARTMENT OF THE TREASURY, “Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,” 1 10 2020. [オンライン]. Available: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

[86] aaa. [オンライン].

[87] 日本貿易振興機構（ジェトロ）, “GDPR適用開始から2年、域外適用の範囲を明示,” 4 6 2020. [オンライン]. Available: https://www.jetro.go.jp/biznews/2020/06/c81164d22cfa1274.html.

[88] MOTHERBOARD TECH BY VICE, “Bot Lets Hackers Easily Look Up Facebook Users' Phone Numbers,” 26 1 2021. [オンライン]. Available: https://www.vice.com/en/article/xgz7bd/facebook-phone-numbers-bot-telegram.

[89] I. NEWS, “5.33億人のFacebookユーザーの電話番号を含む個人情報、犯罪フォーラムで公開,” 4 4 2021. [オンライン]. Available: https://www.itmedia.co.jp/news/articles/2104/04/news016.html.

[90] LINE Corporation, “LINEプライバシーポリシー,” 31 3 2021. [オンライン].

NTT DATA
Trusted Global Innovator

2021年6月18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 /星野 亮 / 川合 絢也 / 野呂 優介 / 宮崎 大輔 / 清水 一貴 /
遠藤 千晶 / 神谷 優治
nttdata-cert@kits.nttdata.co.jp