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

2019 年度 第 3 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、セキュリティ技術部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。

狙われるOffice365のOAuth

Microsoft社のOffice365は、他のサービスやアプリケーションと連携するため、アクセス権限を認可するための標準フレームワーク「OAuth」を採用しています。ところがOffice365のOAuthの実装に脆弱性が存在したため、2019年度第3四半期においてOffice365のアカウント乗っ取りを狙うフィッシングキャンペーンが展開されました。OAuthやSAMLなどの連携プロトコルによるサービス連携は利便性が高い一方で、悪用された場合の被害は大きくなると考えられます。クラウドを利用する企業のクラウドサービスの管理者は、適切なセキュリティ設定を実施しましょう。また同管理者は、クラウドサービスが連携しているアプリケーションのリストを定期的に確認したり、通常ユーザへの注意喚起やアプリケーション連携の強制管理を行ったりすることを推奨します。

内部不正

2019年12月、神奈川県庁の行政文書が含まれるHDDが、ネットオークションを通じて転売されるといった事例が発生しました。ハードディスク廃棄を請け負ったブロードリンク社の従業員の内部不正によるものでした。また一方で、トレンドマイクロ社の従業員が、個人顧客の情報を不正に持ち出してブラックマーケットへ売り、攻撃に悪用された事例も報道されました。いずれもセキュリティ専門企業における内部不正の事例であり、セキュリティ対策も実施されていました。しかしながら、内部不正への対策としては不十分であった上、その運用に不適切な部分がありました。内部不正を防止するためには、内部不正を想定してリスク分析したセキュリティ対策を立案して導入し、適切な運用を行うことが必要となります。

米国で増加するPOSシステムへの攻撃

米国においてPOSシステムへの攻撃による、クレジットカード情報漏えいの事例が数多く報告されています。米国政府やクレジットカードの国際ブランドは、スキミングなどの攻撃に対して脆弱な磁気ストライプ決済から、EMVと呼ばれるICチップによる決済規格への移行を推進しています。この移行が進んでいない業界が特に狙われました。クレジットカード情報は金銭に直接つながることから、サイバー犯罪者に常に狙われていることを認識し、セキュリティ対策に尽力してください。

今後の予測

サイバー攻撃の手口が、より巧妙化・多様化する傾向にあります。ランサムウェアは窃取した情報の流出を盾に脅迫する事例が目立ち始め、今後より効果的な地域・組織に矛先が向く可能性があります。また、2019年はEmotetが猛威を振るいました。今後も被害は継続すると考えられますが、より大規模なボットネットを形成しDDoSやクリプトジャッキングなどの攻撃に転じる可能性があります。

クラウドサービスを用いたID統合やサービス連携などは非常に利便性が高いです。しかし、攻撃者にとっても効率のよい環境となる可能性もあり、クラウドサービスのアカウントの乗っ取りを狙う攻撃が増加する可能性があります。事故を想定した事後策が、今後より一層求められることになるでしょう。

2. 注目トピック

2.1. 狙われるOffice 365のOAuth

OAuthとは、3rdパーティのアプリケーションに対してAPIやデータへのアクセス権限を認可するための標準フレームワークです。2020年2月時点での最新はOAuth2.0であり、RFC6749 [1]およびRFC6750 [2]として発行されています。この標準に従い、TwitterやFacebookなど様々なWebアプリケーションがAPI連携の仕組みを実装しています。ユーザはこの機構を利用することで複数のアプリケーションやサービスを連携させることができます。
便利な機構である反面、攻撃者はこれを悪用しようと攻撃を仕掛けています。2012年には、IPAが意図しないOAuthを利用したサービス連携によりアカウントが乗っ取られる事例を注意喚起していました [3]。この2019年度第3四半期は、OAuthの仕組みを悪用してOffice 365のアカウントを乗っ取る特徴的な攻撃が発見されました。Office 365は、Microsoft社が手掛けるSaaSサービスであり、オフィスアプリケーションやメールサービスが利用できる他に、法人向けにはID連携サービスや社内チャットサービス「Teams」などを提供しています [4]。法人の利用者のOffice 365アカウントが乗っ取られると、企業内の機密情報を窃取されたり、スパムメールや標的型攻撃メールの送信元として悪用されたりすることが想定されます。表 1に2019年度第3四半期に発生したOAuth関連のイベント一覧を示します。

表 1：OAuth関連のイベント一覧

No.	日付	概要
1	12/2	CYBER ARK社は、OAuthの仕組みを悪用してOffice365やAzureのアカウントを乗っ取ることができる脆弱性「BlackDirect」を公表した [5] [6]。
2	12/9	PhishLabs社は、攻撃者がOffice 365のユーザのIDとパスワードの替わりに悪意のあるOffice 365アプリで悪用するためのOAuthトークンの窃取を試みるフィッシングキャンペーンを公表した [7]。

2.1.1. 脆弱性「BlackDirect」

攻撃者は、Office365にログインした状態の被害者に攻撃者が用意したリンクへアクセスさせて、表 1のNo.1の脆弱性を悪用してOAuthトークンを取得します。CYBER ARK社の解説によると、以下が脆弱性の要因です。

1. Office365アプリケーションが実装しているOAuthの仕組みは、各アプリケーションが要求したOAuthトークンを" ReplyUrls"パラメータに指定されたリダイレクトURLに転送する仕組みだった。
2. Microsoft社は、一部のアプリケーションにて、リダイレクト先のURLをホワイトリストへ登録していた。そのホワイトリストへ登録したURLへは、トークン転送が自動的に行われること。
3. ホワイトリストへ登録されていたあるドメインのサブドメインが、Microsoft社のサービスを通じて誰でも取得できた。

攻撃者は、そのサブドメインを取得後、自分が作成したアプリケーションのOAuthトークンを要求する時に、取得したサブドメインのURLを指定すれば、Microsoft社製アプリと同様に自動的にトークンを取得できました。トークンを取得した攻撃者は、トークンを発行したユーザと同等の権限でOffice365の操作が全て可能です。
CYBER ARK社はこの攻撃のデモ動画を公開しました [8]。この動画内で、被害者がOffice365にログインした状態で不審なリンクへアクセスし、その結果、Office365のアカウントに攻撃者のアプリケーションが紐付けられ、発行されたOAuthトークンを窃取、攻撃者用のユーザアカウントが作成されてしまいました。
この脆弱性は10月20日にMicrosoft社に報告され、11月19日に修正されました。

2.1.2. OAuthフィッシングキャンペーン

表 1のNo.2のフィッシングキャンペーンは、既存のフィッシングメールのようにOffice365ユーザを偽サイトに誘導してIDとパスワードを窃取する代わりに、No.1と同様にOffice 365アプリケーションをアカウントと連携させてOAuthトークン発行を求める正規のURLへ誘導してOAuthトークンを窃取する手口でした。

既存のフィッシングメールは、図 1に示す手口で行われます。

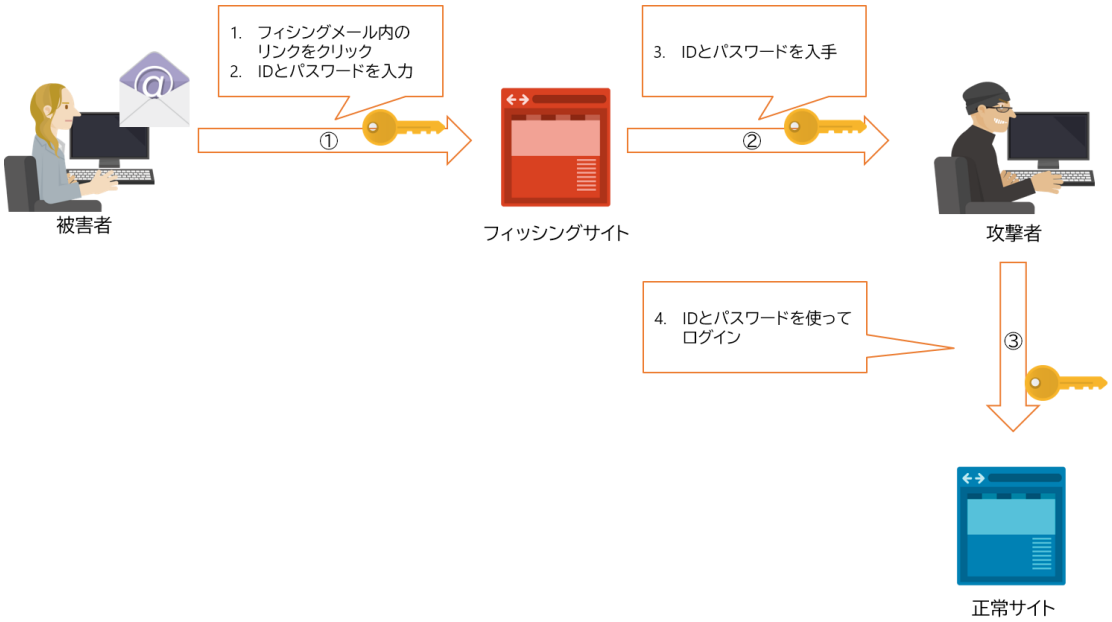


図 1:通常のフィッシングメールの手口

1. 正規サイトのユーザは、攻撃者の送付したメール内のリンクをクリックし、正規サイトを模倣したフィッシングサイトへ誘導される
2. ユーザは、フィッシングサイトへ自身の正規サイトのIDとパスワードを入力してしまう
3. 攻撃者は、フィッシングサイトからユーザの正規サイトのIDとパスワードを入手する
4. 攻撃者は、入手したIDとパスワードを使って、正規サイトへログオンする

この既存のフィッシングメールの手口は、ユーザがリンク先のドメインが正規サイトか模倣サイトか確認できれば、IDとパスワードの詐取を防ぐことができます。また、もしIDとパスワードを盗られたとしても、正規サイトがログイン認証方式に二要素認証を使っていれば、攻撃者の不正ログインを防ぐことができます。
今回発見された新しい手法は、ユーザを正規のMicrosoft社のサイトへ誘導するため、フィッシングメールのようにドメインの正規/非正規から判断できません。またOAuthトークンを取

得されてしまうため、Office365の二要素認証を有効化していても、不正アクセスを防げません。パスワードを変更しても、防止できません。

新しいフィッシングメールは、次に示す手口で行われます。

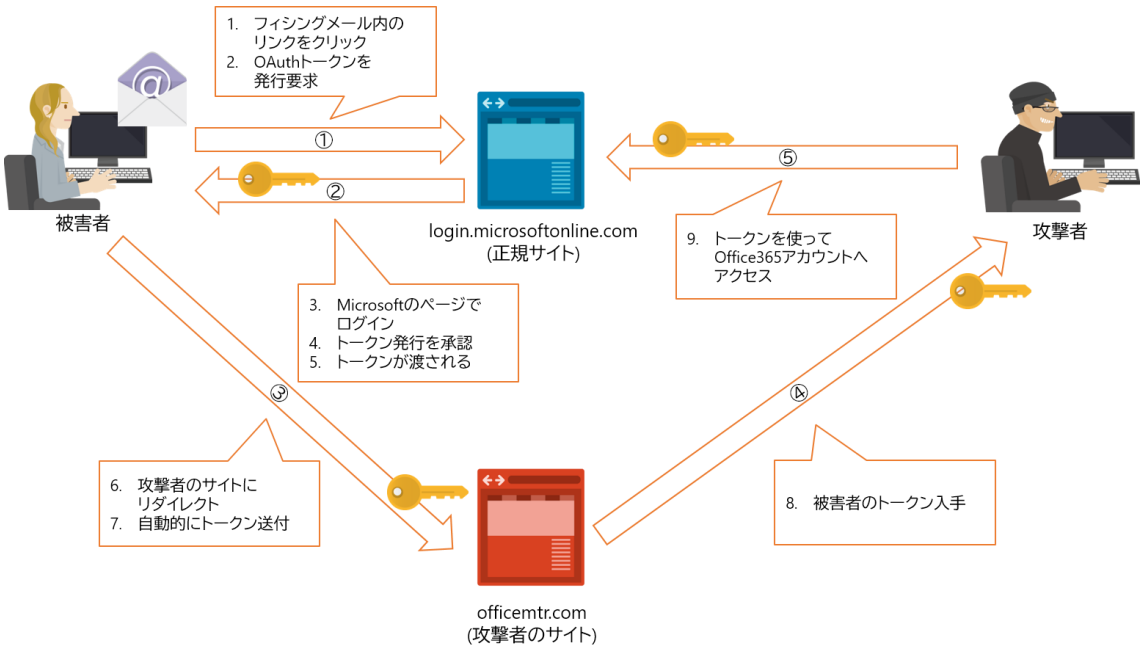


図 2:新しいフィッシングメールの手口

1. Office365ユーザが、攻撃者の送付したメール内のURLリンクをクリックして"login.microsoftonline.com"へ誘導される
2. 1と同時にURLリンクに指定されたパラメータによって、攻撃者の用意したOffice365アプリケーションに付与するOAuthトークンの発行を要求する
3. ユーザが"login.microsoftonline.com"にログインする
4. ユーザがOAuthトークンの発行を承認する
5. OAuthトークンが発行されてユーザへ送信される
6. 攻撃者がリダイレクトを設定しているため、OAuthトークンはユーザへ送信されたあと、攻撃者のサイト"officemtr.com"へ転送される
7. 攻撃者のサイト"officemtr.com"へ自動的にOAuthトークンを送付する
8. 攻撃者は、サイト"officemtr.com"からOAuthトークンを入手する
9. 攻撃者は、入手したOAuthトークンを使って、Office365のユーザアカウントへアクセスする

攻撃者はこの攻撃方法を成功させるために、複数のテクニックを駆使しています。

テクニック１ “フィッシングメール文”（図 2のステップ1）

攻撃者は、Office365ユーザをOffice365のサイトへログインさせる違和感の無い内容のフィッシングメールを作成して送付します。

- フィッシングメールの内容例
  - OneDriveのExcelファイル共有の通知 (図 3参照)
  - Office365アカウントのパスワードの有効期限切れ通知 (図 4参照)

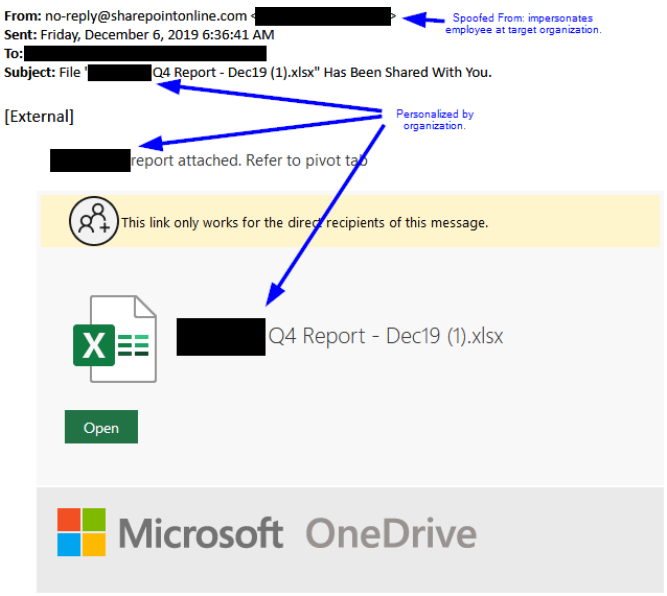


図 3：OneDriveのExcelファイル共有通知のフィッシングメール
(The PhishLabs Blog [7]より転載)

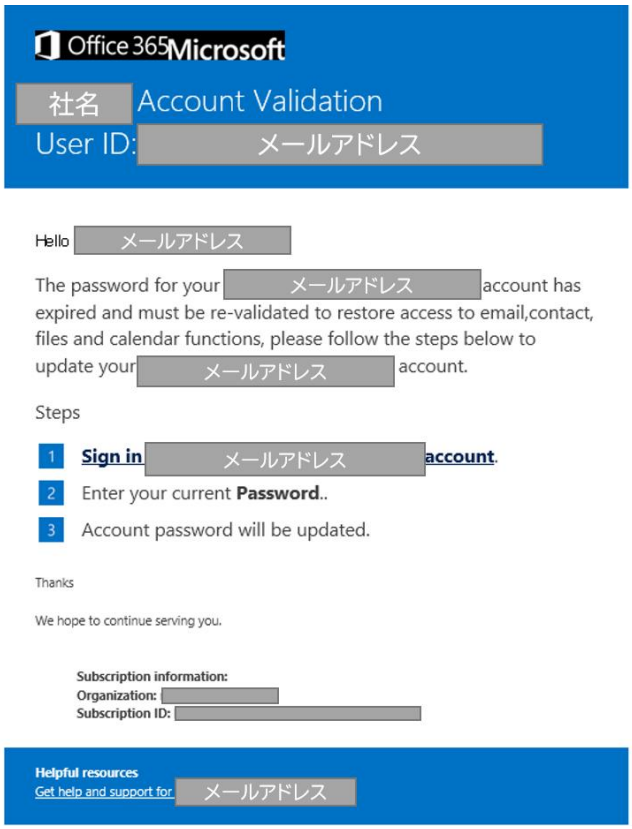


図 4：Office365アカウントのパスワードの有効期限切れ通知

テクニック２ “URLリンク”（図 2のステップ2）

フィッシングメール内のURLリンクには、表 2のURLが記載されていました。このURLには、攻撃者のアプリケーションに対してOAuthトークンを発行し、それを攻撃者のサイトへ転送するURLパラメータが設定されています。ドメイン及びURLパラメータは、Microsoft社のOffice365サイトの規約に則った正規の形式であり、URLリンクから不審な点に気づくことは困難です。

表 2：フィッシングメール内のURLパターン

URLパターン
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?%20client_id={client_id} &response_type=id_token+code&redirect_uri={Redirect_uri} &scope={要求権限} &state={state}&response_mode=%20form_post&nonce={nonce}

テクニック３ “正規の承諾ページ”（図 2のステップ4）

ステップ4.では、図 5のような画面が表示され、ユーザへあるアプリケーション用のOAuthトークンを発行の承諾が依頼されます。OAuthトークン発行には、攻撃者が事前に欲しい権限が指定してあります。ユーザがOAuthトークン発行を承諾すると、そのアプリケーションは上記の攻撃者が指定した権限を獲得できてしまいます。図 5の例では、永続的アクセスとプロファイルへの読み取り権限がアプリケーションへ許可されます。攻撃者は、権限を付与されてアプリケーションを使って様々な不正行為を行います。

図 5:権限要求の例

NTTDATA-CERTでは、攻撃検証用のSample Appおよび図 2の攻撃者のサイトに相当する模擬サイトを構築して検証実験を行いました。その結果、社内ネットワークからのみアクセスを可能なOneDriveやTeamsが攻撃検証用のSample Appを使うとインターネット上のどこからでもアクセス可能でした。

2.1.3. 攻撃検知、暫定対応および未然防止策

表 1のNo.1, No.2ともにOffice 365アプリケーション連携に伴うOAuthトークン発行プロセスを悪用した攻撃です。これらの攻撃はアプリケーション連携状況を調査により検知が可能です。

攻撃検知方法

図 6に示すように、Office 365およびAzureの管理者がAzureポータルを使い、現在テナントが連携しているエンタープライズアプリケーションの一覧を取得して、不審なアプリケーションの有無をチェックします。見覚えのない名称のアプリケーションがあった場合は、攻撃が成功しているおそれがあります。

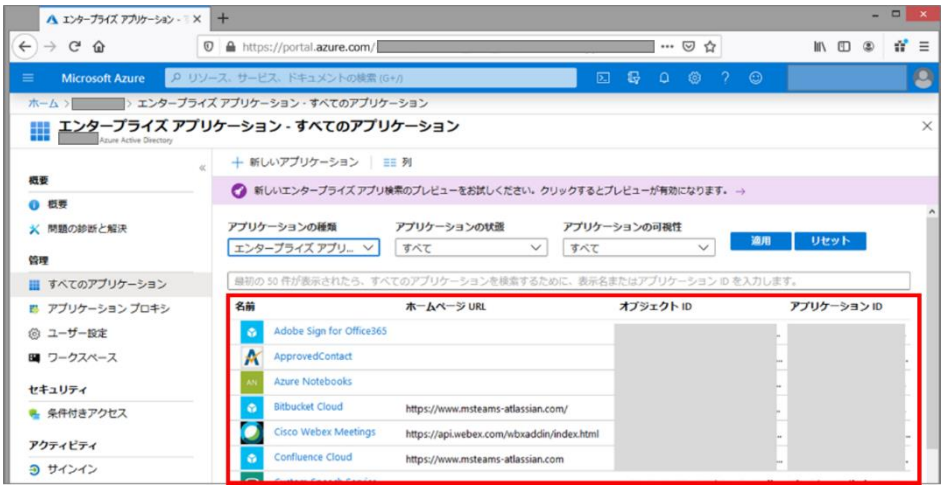


図 6:Azureポータルにおけるアプリケーション登録状況確認

暫定対応

不審なアプリケーションがあった場合は、図 7に示した不審なアプリケーションのプロパティから箇所を「いいえ」にすれば、不審なアプリケーションのサインインを無効化できます。

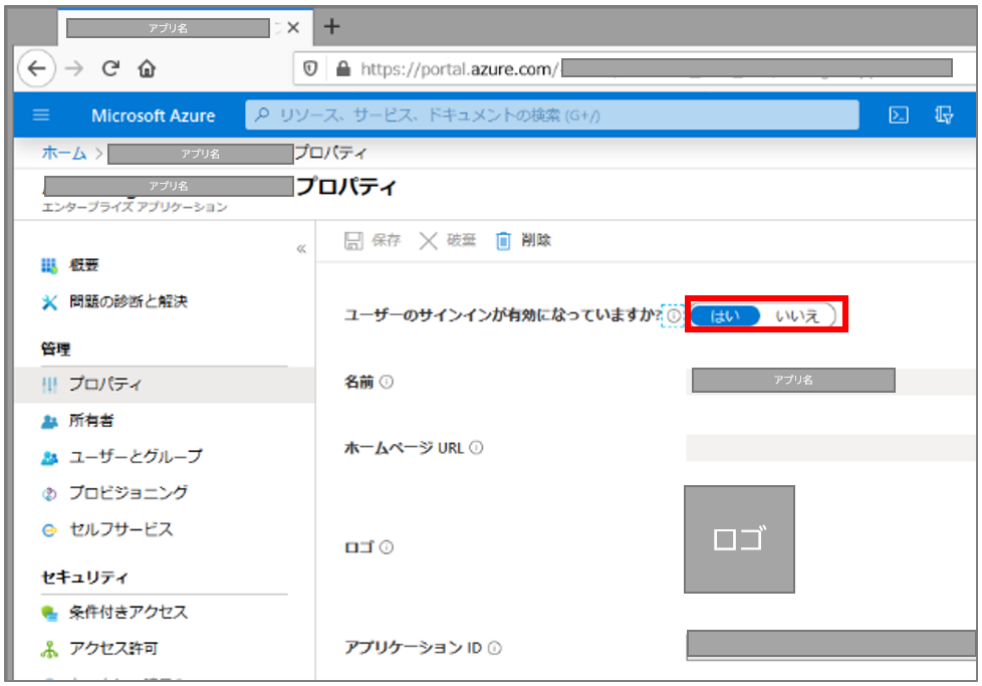


図 7:Azureポータルにおけるアプリケーションの無効化

未然防止策

Office365およびAzureの管理者がAzureポータル上で一般ユーザのアプリケーション用OAuthトークン発行を制限する設定を行えば、不審なアプリケーション用のOAuthトークン発行を防止できます。図 8に示したように、AzureポータルでAzure Active Directoryの設定の当該項目を「いいえ」に設定すると、一般ユーザはアプリケーション用のOAuthトークン発行を承認できなくなります。

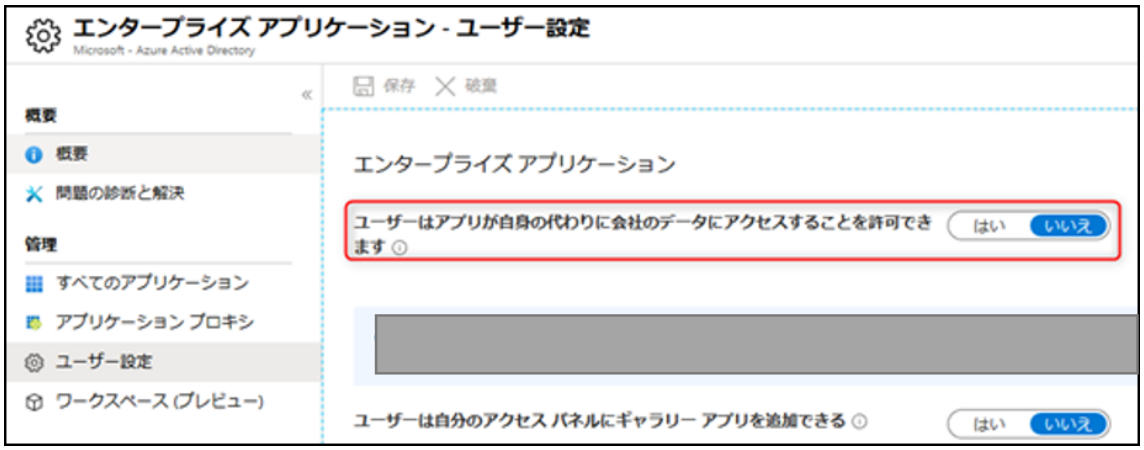


図 8:一般ユーザのアプリケーション連携許可の禁止

2.1.4. まとめ

OAuthやSAMLなどのアプリケーション連携プロトコルに対応したクラウドサービスが増えるに従い、ユーザの利便性が上がる一方、連携用トークンを窃取する攻撃の増加が予測されます。これらのトークンの悪用の検知は難しく、クラウドサービスの利用拡大に伴って、トークンを窃取されてしまった場合の被害はより大きくなると考えられます。クラウドサービスを利用する企業のクラウドサービス管理者は、適切なセキュリティ設定を実施しましょう。また、管理者がクラウドサービスと連携しているアプリケーションを定期的に確認したり、通常ユーザへの注意喚起やアプリケーション連携の強制管理を行ったりすることを推奨します。

2.2. 内部不正

内部不正による情報セキュリティインシデントは、外部からの攻撃よりも1件当たりの被害が大きい場合が多々あり、ひとたび発生してしまうと事業に大きな影響が生じることもあります。
2019年度第4四半期には、大量の個人情報や秘密情報が残存した神奈川県庁の使用済みのハードディスク（HDD）が、ネットオークションを通じて転売され、流出する事例が発生しました。この事例では、セキュリティ専門企業であるブロードリンク社の社員が、データ消去と物理破壊までを依頼されたHDDを破壊処理せず、ネットオークションを通じて転売しました [9]。この社員がネットオークションで転売したHDDなどの記録媒体は3,500個以上あり、そのうちの何個がブロードリンク社から盗まれたものなのかは分かっていません。また、ブロードリンク社は神奈川県以外にも様々な官公庁や企業からHDD廃棄を請け負っており、影響範囲の拡大が懸念されます [10]。そして当該企業は、従業員の1割が解雇、複数の事業所も閉鎖、社長も退任の意向を示すという、大きな代償を払うこととなりました [11]。
同様にセキュリティ専門企業であるトレンドマイクロ社でも、内部不正による個人情報の流出がありました。こちらは海外のユーザサポートに関するものでしたが、元従業員の不正行為によって個人ユーザの情報が外部に持ち出され、持ち出された情報の提供を受けた第三者により犯罪に悪用されてしまいました。持ち出された情報は、海外で提供している個人向けセキュリティ製品ユーザのうち、英語を話すユーザのサポートに関するものでした [12]。
なぜ、セキュリティを生業とする企業である両社で内部不正が発生してしまったのか、情報が多いブロードリンク社を事例として内部不正の対策について考えてみます。

2.2.1. 対応実現の難しさ

「動機」「機会」「正当化」という3つの要素がそろったときに内部不正が発生するという米国の組織犯罪研究者 ドナルド・R・クレッシーが提唱した不正のトライアングルという理論があります [13]。内部不正を実行できる機会を減らしたり、内部不正して得られる利益を減らして動機を抑えたりするなど、3つの要素がそろわないようにすれば、内部不正を軽減できるという考えです。
同社は、表1の対策を実施していました [14]。しかし不審者の侵入と盗難、ケアレスミスの対策が中心で、HDDの物理的な盗難という内部不正に対抗できる対策は2つしかありません。

表 3:ブロードリンク社の既存の内部不正対策

No.	対策	概要	内部不正への対策効果[1]	
1	カードキーと指紋認証による入退出	入荷エリア：カードキーによる入退出 データ消去室：カードキーと指紋認証による入退出 梱包と出荷エリア：カードキーによる入退出	－	不審者対策、無許可者対策であり、入退出の権限を持つ内部不正には効果が期待できません
2	入退出ログ管理	誰がいつ入退出したか社員固有IDキーと扉番号、入室時間、退出時間を記録	△	入退出ログを監査して不審な時刻を検知すれば、抑止効果が期待できますが、不正は実行できてしまいます
3	24時間監視カメラ	監視カメラにより24時間録画	△	不正行為をカメラへ記録できれば抑止効果は期待できますが、不正行為を止めることは出来ません
4	1台1台の個体管理	個体に管理番号と管理バーコードラベルを貼り付けし、1台1台の入荷からデータ消去、出庫まで荷物の個体を管理	○	常に全数管理すれば内部不正を早期検知できるため抑止効果が高い
5	私物管理（持ち込み防止）	設備内に私物を持ち込まないように専用ロッカーを設置	－	PCや携帯電話の持ち込み対策であり、HDD持ち出しには効果が期待できません
6	私物管理（持ち出し防止）	持ち出し防止に手荷物検査を実施	○	HDDの持ち出しを発見、阻止できるため、「機会」を絶やすことができます
7	開閉アラーム警報	1分間開いていたら警報	－	不審者対策、無許可者対策であり、入退出の権限を持つ、内部不正には効果が期待できません
8	ポケット縫い付け専用ユニフォーム	ポケットが縫い付けられている専用ユニフォームを着用	－	うっかりポケットへUSBメモリをいれたまま持ち出してしまうミスを防ぐ対策

凡例：○: 物理的なHDD盗難に対して、有効な対策
△: 抑止効果は期待できるが、限定的な対策
－: 物理的なHDD盗難に関係しない対策

[1] 本表における「内部不正」は、物理的なHDD盗難に対する効果にフォーカスして評価したものです。物理的なHDD盗難に関係しない内部不正は「－」としています。

表 3のNo.3の「24時間監視カメラ」のように内部不正への対策効果が△の対策は、抑止効果しかなく、権限があり、悪意を持っている内部者の不正実行を止められません。表 3のNo.4とNo.6の2つは、内部不正に効果が期待できる対策です。しかし、これらの対策は、表 4のように適切に運用されていませんでした。

表 4：表 3の内部不正に効果が期待できる対策の運用状況

No.	対策	概要	内部不正へ対策効果がない理由
4	1台1台の個体管理	個体に管理番号と管理バーコードラベルを貼り付けし、1台1台の入荷からデータ消去、出庫まで荷物の個体を管理	出庫までの個体管理が適切に実施されていれば、HDDの不正持出しがすぐに見つかったはずです。外部から指摘されるまで気づかなかったことから、正しく運用できていなかったと推測します
6	私物管理（持ち出し防止）	持ち出し防止に手荷物検査を実施	手荷物検査は「不定期の実施で、（頻度が）十分ではなかった」と公表しています

その後の報道で、内部不正を行った社員が「始業前に行けば簡単だった」と説明していることから、内部不正への対策が不十分であることを見抜いて、HDDを持ち出していたことが分かります [15]。表 3の対策は、内部不正を想定してリスク分析して作成したセキュリティ対策ではなく、情報漏えい対策のベストプラクティスを集めて作成したセキュリティ対策ではないか、と推測しています。そのため、内部不正を阻止できる十分な対策効果が無かったのではないかと思います。また、もし内部不正への対策を立案して導入できていたとしても、適切な運用が伴っていなければ、内部不正を防ぐことはできません。

2.2.2. 内部不正対策の考え方

ブロードリンク社は、以下の追加対策を実施すると発表しました [14]。しかし表 5の追加対策を見ると、表 3のブロードリンク社の既存の内部不正対策と同様に、悪意を持った内部不正者には効果が期待できない対策が含まれています。

表 5:ブロードリンク社の追加の内部不正対策

No.	対策	内部不正へ対策効果がない理由[2]	
1	全てのHDDの物理破壊前と破壊後の写真撮影を必須化	△	HDDの固有番号がわかるように破壊前と破壊後の写真を撮影すれば、HDDの同一性を証明できる。全てのHDDの写真有無の確認も必要
2	操業時間帯の入退出時は、有人によるハンディ金属探知機での身体チェックと手荷物検査を実施	○	HDDの消去と物理破壊作業の専用ルームを設置して、操業時間帯以外の出入りの禁止と左記の対策を行えば効果あり、時間外に持ち出されるおそれあり
3	入退出セキュリティゲート設置と警備員によるハンディ金属探知機での身体確認及び手荷物検査の実施	△	お客様から受け取ったHDDを専用ルームへ持ち込む前に不正に持ち出されることを阻止する対策。24時間体制でチェックしない場合、持ち出しできるおそれがある
4	セキュリティカメラの増設	△	抑止効果は向上しますが、不正行為を完全に止めることは出来ません。映像のチェック作業も必要
5	外部講師によるセキュリティ研修の定期的な実施	ー	強い悪意や犯罪目的の内部不正者には効果がない

凡例：○: 物理的なHDD盗難に対して、有効な対策
△: 抑止効果は期待できるが、限定的な対策
ー: 物理的なHDD盗難に関係しない対策

表 5の追加対策は、表 3のブロードリンク社の既存の内部不正対策を部分的に強化したものと推測されます。ブロードリンク社のHDDのデータ消去と物理破壊の業務について、内部不正を中心にリスク分析して作成したセキュリティ対策ではないのでしょう。

上記で不正のトライアングルを用いた内部不正対策を述べましたが、以下のロナルド・クラークの状況的犯罪予防論と合理的選択理論のほうが内部不正対策を導出しやすいため、情報セキュリティ分野の内部不正を防止する対策のみを用いて導出した対策を提案します [16]。

[2] 本表における「内部不正」は、物理的なHDD盗難に対する効果にフォーカスして評価したものです。物理的なHDD盗難に関係しない内部不正は「ー」としています。

- 状況的犯罪予防
  犯罪の時空間的側面（犯罪発生機会・状況）に着目し、その機会を減らすことにより犯罪を予防する
- 合理的選択理論
  人間は、損得の合理的計算のもとで行動を選択する
  ① 犯行の難易度を高める（例：侵入しにくくする）
  特定の内部不正行為の実施を防止、または直接的に阻害する対策を導入
  ② 犯行の発見のリスクを高める（例：監視性の確保）
  管理や監視を強化して内部不正を検知する、内部不正者を特定できる対策を導入
  ③ 獲得する報酬を減らす（例：被害対象物の除去）
  高価な資産を取り扱わない、資産価値を下げる

つまり、内部不正によって得られる利益よりも、内部不正の検知や内部不正者の特定のデメリットを増やせば、内部不正を行う動機を減らして、内部不正を防止できます。

表 6：合理的選択理論に基づく対策案

	原則	概要
①	犯行の難易度を高める	HDDを不正に持ち出せないようにする。お客様から預かったHDDを施錠運搬して、作業専用ルーム内でのみ取り出す方法を導入。出入口の施錠と操業時間帯以外の出入りの禁止。破壊されたHDDのみ持ち出し可。破壊済みHDDの個数を2人以上で確認して報告
②	犯行の発見のリスクを高める	監視カメラによる録画と映像のチェック。作業専用ルームへの物品の持ち込み/持ち出しを原則禁止し、入退出時にボディチェック
③	獲得する報酬を減らす	再販できないようにHDDは全て物理破壊する。

2.2.3. まとめ

今回の事例では、入退室管理や監視といったセキュリティ対策を実施していましたが、内部不正への対策としては不十分でした。更に、手荷物検査の実施が不定期であるといった不適切な運用も相まって、大量の個人情報や秘密情報が流出する事態へと発展してしまいました。
内部不正を防止するためには、情報漏洩対策のベストプラクティスを集めて実施するのではなく、内部不正を想定してリスク分析したセキュリティ対策を立案して導入し、適切な運用を行うことが必要となります。
企業側として内部不正を防止するため、内部不正によって得られる利益よりも、内部不正の検知や内部不正者の特定といったデメリットを増やし、内部不正を行う動機を減らすことが望まれます。
セキュリティ専門企業やセキュリティを重要視しなければならない組織であれば、内部不正を行う動機を減らすとともに、内部不正自体の発生を前提として、漏洩時の被害を少しでも減らすよう、情報の暗号化などの対策を検討することも必要でしょう。

3. 情報漏えい

3.1.1. 米国で増加するPOSシステムへの攻撃

2019年度第1四半期、第2四半期ではWebスキミングによりECサイトからクレジットカード情報を窃取する攻撃の増加を掲載しました。2019年度第3四半期は、Webスキミングが継続して確認されている一方で、米国において実店舗のPOSシステムへの攻撃によるクレジットカード情報の漏えい事例が数多く報告されています。

表 7に挙げた事例は、いずれもPOSマルウェアと呼ばれるPOSシステムへの攻撃に特化したマルウェアに感染しており、決済処理で磁気ストライプからクレジットカード情報を読み取った時に、POSマルウェアによってクレジットカード情報が窃取されています。POSマルウェアは、POSシステムからカード番号、氏名、有効期限といったクレジットカード情報を自動で収集し、外部の攻撃者に送信します。犯罪者は、攻撃者からクレジットカード情報を入手して、本人になりすまして不正使用します。

表 7:POSマルウェアによる情報漏えいインシデントの事例

日付	対象		概要
10/3	Hy-Vee	小売業 (スーパー・ガソリンスタンド)	一部の支払い処理システムがPOSマルウェアに感染した事例の調査結果を報告 [17]。 窃取されたカード情報530万件がダークウェブで販売された [18]。 侵害期間：2018/12～2019/8
10/24	Krystal	外食業 (ファーストフード)	一部の支払い処理システムがPOSマルウェアに感染 [19]。 窃取されたカード情報400万件がダークウェブで販売された。(2019年8月に発生したFocus Brandsで窃取されたカード情報を含む [18]) 侵害期間：2019/7～2019/9
11/13	ガソリンスタンド	燃料小売業	VISAが北米のガソリンスタンドで発生したPOSマルウェアによる攻撃を2件報告 [20]。
12/11	ガソリンスタンド	燃料小売業	VISAが北米のガソリンスタンドで発生したPOSマルウェアによる攻撃を3件報告 [21]。
12/20	Wawa	小売業 (コンビニ・ガソリンスタンド)	支払い処理システムがPOSマルウェアに感染。850以上の拠点に影響あり [22]。 侵害期間：2019/03/03～2019/12/10

3.1.2. POSシステムへの攻撃の流れ

POSシステムへの攻撃は、以下の流れで実行されます。

1. 攻撃者は、攻撃対象の企業のネットワークに侵入します。侵入手段は、標的型攻撃、インターネットに公開されているサーバの脆弱性や設定不備の悪用です。
2. 攻撃者は、企業のネットワーク内を偵察してPOSシステムの認証情報を取得し、その企業が運営しているPOSシステムへ侵入します。POSシステムへ侵入すると、各店舗の決済端末へRAMスクレーパーと呼ばれるPOSマルウェアを感染させます。
3. 決済処理の際、磁気リーダで読み込まれたクレジットカード情報はメモリ上に平文で保存されます。RAMスクレーパーは、このメモリ上のカード情報を検索して抜き取り、不正に外部に送信します。

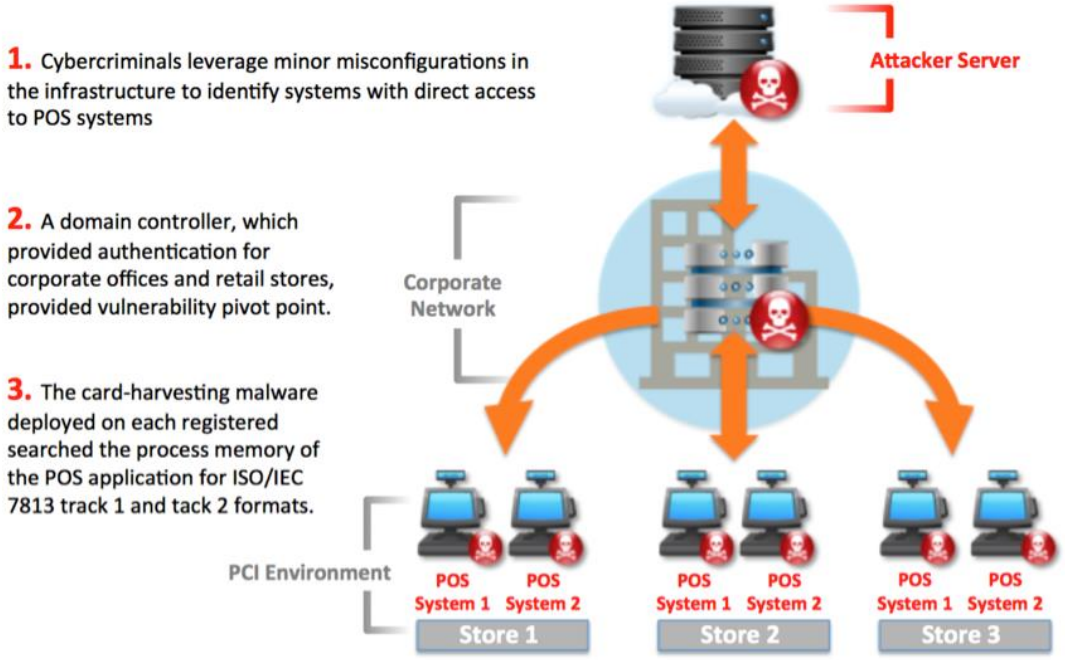


図 9:POSマルウェアによる攻撃モデル

(VMware Carbon Black セキュリティブログより引用 [23])

3.1.3. 米国におけるセキュリティ対策の動向

磁気ストライプはセキュリティ面で脆弱であることから、世界的にICチップへの移行が進んでいます。ICチップが搭載されたクレジットカードの国際的な統一規格をEMVと呼び、クレジットカード、決済端末の両方がEMVに準拠することでICチップによる決済処理が可能となります。前述のPOSマルウェアへの対策としては、クレジットカード、決済端末のEMV準拠と併せて、POSシステム内で平文のクレジットカード情報を扱わない対応が有効と言われています [24]。

米国では、2013年にHome Depot社、Hyatt社、Target社など、多数の企業がクレジットカード情報漏えいの被害に見舞われました。特にTarget社の事例においては、4,000万件ものクレジットカード情報が漏えいしたと伝えられています [25]。これを受け、連邦政府は2014年にクレジットカード決済のセキュリティに関する大統領令を出し、EMVに準拠したクレジットカードの発行を義務化しました。また、クレジットカードの国際ブランドは、EMVに準拠した決済端末の導入促進のため、2015年にライアビリティシフトの運用を開始しました。ライアビリティシフトとは、EMVに準拠していない端末で偽造クレジットカードが決済処理された場合に、債務責任がクレジットカード発行会社ではなく加盟店に課せられるルールです。新たな端末の導入には時間もコストもかかることから、ライアビリティシフトへの対応(EMV準拠の決済端末の導入とそれに伴うシステムの改修)は原則2017年10月を期限としています。また、ガソリンスタンドは給油向けの特別な技術や複雑なインフラを利用しているとの理由から、例外的にライアビリティシフトの対応期限を2020年10月としています。

カスペルスキー社の当時のブログ記事によると、ライアビリティシフトへの対応の移行期間であった2016年に小売店からのクレジットカード情報の漏えい被害が増加していました。2017年10月のライアビリティシフトへの対応期限前に、攻撃者がEMVに準拠していない端末を活発に攻撃していたと推測されます [26]。

2019年11月、12月に出されたVisaの注意喚起では、ガソリンスタンドを標的とした攻撃の増加とサイバー犯罪集団「FIN8」の関与の可能性を指摘しています [20] [21]。FIN8は、POSマルウェアを使用してクレジットカード情報を窃取する高度なサイバー犯罪集団です。2016年と2017年に活発に活動していたものの、2017年以降、その活動が衰退していました。しかし現在、ガソリンスタンドを標的として活発に活動しています。ガソリンスタンドのライアビリティシフトへの対応期限まで1年を切った現在、FIN8が活動を再開して、2016年の事象と同様に駆け込みで磁気ストライプ決済端末を標的とした攻撃が多発しているおそれがあります。まだまだPOSマルウェアへの警戒が必要です。

3.1.4. まとめ

Webスキミングによるカード情報の窃取が主流となっている一方で、長く存在するPOSシステムからのカード情報の窃取が増加している傾向を取り上げました。クレジットカードのセキュリティ対策で、米国と同様に後進国とされていた日本は、2018年6月に施行された割賦販売法により、2020年3月までに対面加盟店におけるカード・決済端末のIC対応化、カード情報の非保持化等が義務付けられており、クレジットカードの利用環境は改善されつつあります。しかし、日本クレジットカード協会が2019年7月に実施した調査によると、IC対応化されたクレジットカードの利用率は61.8%で、依然として磁気ストライプが利用されています [27]。磁気ストライプの利用が続く限り、POSマルウェアによる攻撃が日本に集中する可能性があります。また、米国の事例のように、政策や法令による対応期限の前後において犯罪件数が増加する傾向もあるため、クレジットカードを扱う組織は、前述のセキュリティ対策を迅速に行い、情報漏えいを未然に防ぐことが重要です。また、クレジットカードの利用

者は、不正利用の発生にいち早く気づくため、利用明細に身に覚えのない取引がないかを定期的に確認してください。クレジットカード情報は金銭に直接つながることから、サイバー犯罪者に常に狙われていることを認識し、セキュリティ対策に尽力してください。

4. 脆弱性

4.1. PHP-FPMの脆弱性

脆弱性がCapture The Flagで発見される

The PHP Groupは、PHP-FPMの脆弱性CVE-2019-11043の情報を公表しました。この脆弱性は、PHPのFastCGI 実装のひとつの PHP-FPM（FastCGI Process Manager）の脆弱性です。特定の構成、設定の場合にリモートから任意コード実行が可能となります。脆弱性を悪用するためには、PHPの特定のバージョン、構成、設定等の条件を満たさなければならず、影響を受けるシステムは限定されます。しかし、条件を満たすサーバは一般的に存在するものであるため、危険な脆弱性です。 [28]
この脆弱性は、CTF (Capture the Flag)と呼ばれるセキュリティコンテストで最初に発見されました [29]。脆弱性発見、情報公開、PoC公開、パッチリリースの流れは以下の通りです。またこの脆弱性は、情報公開当初は修正パッチ等の本格対処が出る前に公開されてしまったゼロデイ脆弱性でした。

- 9/14-9/16 ：「Real World CTF 2019 Quals」で研究者Andrew Danau氏がバグを発見
- 9/26 ：研究者Emil Lerner氏が「PHP Bug Tracking System」に脆弱性情報を投稿
- 10/22 ：Github上でPoCが公開
- 10/24 ：The PHP Groupが修正パッチをリリース

nginxとPHP-FPMを組み合わせたWebシステムへの攻撃

PHP-FPMの脆弱性は、特にnginxとPHP-FPMを組み合わせて構築したWebシステムで悪用できることがわかりました [30]。攻撃者は、nginx側の改行コードの処理における不備と、PHP-FPMの脆弱性を悪用することで、PHP実行環境の環境変数を変更可能です。環境変数を変更した結果、攻撃者がリモートから任意コードを実行できるようになります。NTTデータ先端技術社の検証レポートによると、nginxの設定が以下4つの条件を満たす場合に、環境変数を変更可能です [31]。

1. locationディレクティブでリクエストをPHP-FPMに転送するようになっていること
2. PATH_INFO変数を割り当てる際にfastcgi_paramディレクティブが使用されていること
3. fastcgi_split_path_infoディレクティブが存在し、
   「^」で始まり「$」で終わる正規表現が用いられていること
4. 「try_files $uri =404」のようなファイルの有無を判断するためのチェックがないこと

4つの条件がそろった設定のnginxは一般的に存在します。上記の4つの条件を満たすnginxの設定ファイル(.conf)の例を以下に示します。

```
        location ~ [^/]¥.php(/|$) {
             fastcgi_split_path_info ^(.+?¥.php)(/.*)$;
             fastcgi_param PATH_INFO $fastcgi_path_info;
             fastcgi_pass php:9000;
             ...
        }
```

ランサムウェア「NextCry」による脆弱性の悪用

オンラインストレージを構築できるオープンソースソフトウェア「NextCloud」を狙い、ファイルの暗号化を試みるランサムウェア「NextCry」が観測されています [32]。ランサムウェア「NextCry」は、PHP-FPMの脆弱性を悪用してWebシステムへ感染します。
Nextcloudは、別途Webサーバエンジンを用意して構築する必要があります。そのWebサーバエンジンのひとつにnginxが含まれます。Nextcloudは過去にnginxを用いた構成を推奨していたことがあり、攻撃が成功するおそれが高いことから標的になっています。Nextcloud社は、脆弱性公開後にnginxを使用するシステム管理者へ向けて注意喚起を実施しました [33]。
NextCryは、PHP-FPMの脆弱性を悪用して次のような行動を行います。まずNextCryは、NextCloudの設定ファイル「config.php」を参照して、データが保存されるディレクトリパスを取得します。つぎに、取得したディレクトリパスに保存されているデータを暗号化し、NextCloudの管理画面や操作画面に脅迫文を表示します。脆弱性公開前にPoCが公開されていたため、脆弱性公開後数日でNextCryが悪用できたと推測します。

まとめ

PHP-FPMの脆弱性はゼロデイ脆弱性でした。ゼロデイ脆弱性は、本格対処となる修正パッチの提供前に攻撃が発生するおそれがあります。特に修正パッチ提供前に攻撃コードが公開された場合は、すぐに攻撃が始まるおそれが高く非常に危険です。修正パッチが適用できるようになるまで、設定変更による攻撃の回避や脆弱性のある機能やモジュールの使用停止等、攻撃を受け付けない対策を実施してください。もし脆弱性の影響を完全になくすことが困難である場合は、攻撃発生を早期検知するための監視を強化や、攻撃を受けたときにすぐに被害を最小限にするための対応ができる準備をしてください。修正パッチを適用した後であっても、修正パッチを適用する前にすでに攻撃を受けたおそれがあるため、攻撃有無の調査が必要です。
PHPは、広く利用されるスクリプト言語であるため脆弱性の影響も大きくなります。PHP-FPMの脆弱性は、nginxやNextcloudに大きく影響しました。使用している製品の特性を把握して、

適切な脆弱性マネジメントを実施することが重要です。今回のケースでは「PHP-FPMとnginx」「Nextcloudとnginx」といった連携関係を把握している必要がありました。脆弱性のなかにはシステム構成次第で影響が変わるものも多く存在します。製品やシステムを構成しているミドルウェアやプラットフォーム、ライブラリ、モジュールなどの環境を正しく把握することが、迅速な脆弱性対応を可能にしてシステムをサイバー攻撃から守ることにつながります。

4.2. 攻撃利用脆弱性

PHP-FPM の脆弱性以外に、2019 年度第 3 四半期に悪用された、または悪用の試みが確認された脆弱性の一部を表 8 に示します。

表 8:悪用が確認された脆弱性

CVE番号/別名	対象製品	概要
CVE-2018-0296	Cisco ASA	脆弱性を悪用した攻撃の急増が観測され、Cisco Systems 社が重要度のレーティングを変更。 [34]
CVE-2019-2215	Android	Android 8.x 以降に影響する権限昇格の脆弱性。Pixel、Samsung、Xiaomiなどに影響。 [35]
CVE-2018-7600 Drupalgeddon2	Drupal	Akamai社の研究者が脆弱性悪用によりマルウェアを配布する新たなキャンペーンを発見。 [36]
CVE-2019-11510 CVE-2019-11539 CVE-2018-13379	SSL VPN 製品	9月に悪用する攻撃が増加して話題となった脆弱性 [37]。NSA含む複数の機関が攻撃グループによる悪用について警告。 [38]
CVE-2019-18187	ウイルスバスター	ディレクトリトラバーサルの脆弱性。 TrendMicro社が悪用攻撃を確認。 [39]
CVE-2019-13720 CVE-2019-13721	Google Chrome	オーディオの解放後メモリ利用の脆弱性。ゼロデイであった期間があり攻撃も確認された。 [40]
CVE-2019-0708 BlueKeep	Windows RDP	5月に見つかった脆弱性。これまで何度も注意喚起されている。CERT NZ社が再度呼び掛け。 [41]
CVE-2015-2419 CVE-2018-4878 CVE-2018-15982 CVE-2018-8174	Internet Explorer Adobe Flash Player	TrendMicro社の研究者が新たに発見されたエクスプロイトキット「Capesand」が脆弱性を悪用していることを確認。10月段階で継続的に攻撃に利用されているとした。 [42]
CVE-2019-8144	Magento	Magento Commerce 2.3.x 利用者に脆弱性悪用攻撃の被害を防ぐために更新を呼びかけ。 [43]
CVE-2019-1429	Internet Explorer	スクリプトエンジンのメモリ破損の脆弱性。 ゼロデイ攻撃が確認された。 [44]
CVE-2019-1458	Windows	「Operation WizardOpiu」と呼ばれるキャンペーンで悪用された。ゼロデイ脆弱性であった。 [45]

5. マルウェア・ランサムウェア

5.1.1. 国内で多発したEmotet被害

2019年度第3四半期で最も話題となったマルウェアとして、Emotetが挙げられます。Emotetがどのようなマルウェアなのかは2019年度第1四半期レポートをご参照ください [46]。グローバルセキュリティ動向四半期レポートでは、2019年度第1四半期、第2四半期にEmotetについて取り上げていますが、いずれも海外での事例でした。しかし、第3四半期では国内での大規模な感染が確認されました。9月には検出台数が86台だったのに対し、10月には1700台、12月には8019台と急激に増加しています [47]。12月にJPCERT/CCとIPAは注意喚起を行い [48] [49]、内閣官房長官が記者会見を行うまでに発展しました [50]。なぜこれほどまで国内で感染が広まっているのでしょうか。

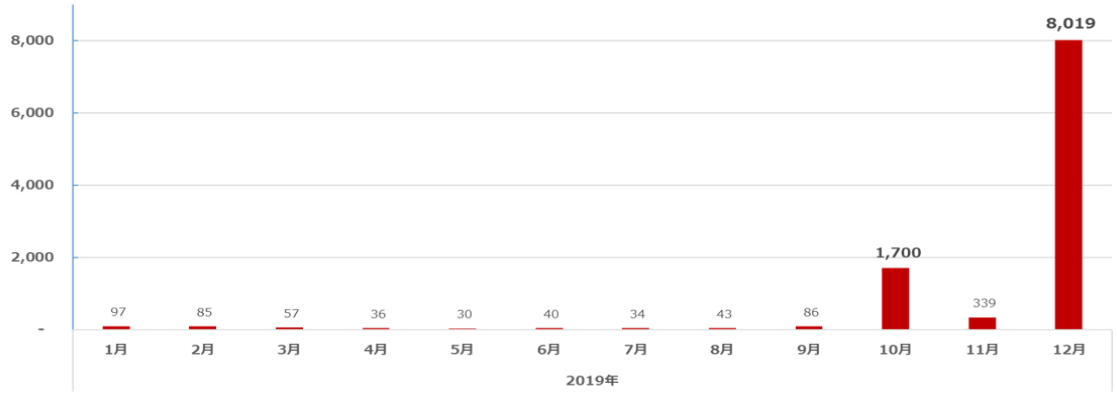


図1：国内でのEmotet検出台数の推移
（トレンドマイクロセキュリティブログより転載）

以下2つの理由が挙げられます。1つ目の理由は、攻撃者が送信するEmotetのメールは、正常なメールと不正なメールの区別がつきにくくなってきたためです。メール本文は、主語や述語がずれた言い回しがなくなりつつあります。本文が3行程度で抽象度の高い簡潔な日本語（「参考までに」、「ご確認お願いいたします。」等）であることから、添付された過去のやり取りとその簡潔な日本語が噛み合っているようにみえてしまいます [49]。日本人は行間を読むので、早とちりして、本人と思い込んでしまって開いているようです。2つ目の理由は、不正なメールが日本の企業文化、イベントに合わせた内容になってきたためです。10月にEmotetが流行した際には、請求書に関する文面が多く見られましたが、12月にはボーナス支給のタイミングに合わせて、賞与支払いに関する文面のメールが確認されています [49]。

IPAはEmotetのメールで実際に使用された件名、本文をまとめて公開しています [49]。短い文章のメールや、世間で流行している事柄に関するメールを受信した際には、IPAやJPCERT/CCの発信している情報 [48]を利用し、そのメールが適切なものか判断してください。もし判断に迷うことがありましたら、1人で解決しようとせず、上司や専門家に必ず相談してください。

5.1.2. 新たな広まりを見せるランサムウェア「BitPaymer」

BitPaymerはランサムウェアの一種で、2017年頃から活動が確認されています [51]。感染経方法は複数確認されていて、例としてはEmotetを利用したTriple Threat [52]やPowerShellを用いたファイルレスマルウェア攻撃 [53]が挙げられます。今回、イスラエル発のサイバーセキュリティ企業Morphisecは、8月にBitPaymerの被害を受けていた自動車業界の複数大手企業が、新たな攻撃方法により被害を受けていたことを報告しました [54]。Morphisec社の報告によると、攻撃者はBonjourの脆弱性を悪用し、BitPaymerをWindowsマシンへ感染させようとします。Apple社は、2019年10月にWindows版のiTunesとiCloudの複数の脆弱性を修正するパッチを公開しました [55]。修正された脆弱性のひとつが、アップデートコンポーネント「Bonjour」の脆弱性で、アップデート時に実行するプログラムの実行パスが引用符で囲まれていないために意図しないコードが実行される恐れがあるというものでした [54]。Bonjourの脆弱性を悪用したBitPaymerの感染の流れは以下の通りです。

1. 攻撃者は、標的のWindowsマシンのCドライブ直下のディレクトリへ「Program」というファイル名のBitPaymerを送り込みます。
2. Bonjourが自動アップデート機能を用いて「C:¥Program Files¥～～」フォルダ配下の正規ファイルを実行しようとします。
3. しかしBonjourには、上記のフォルダの実行パス「C:¥Program Files¥～～」が引用符で囲まれていないバグがあります。そのため、「C:¥Program」の次の空白文字で実行パスが終端されてしまいます。よってBonjourは「C:¥Program」を実行します。
4. 「C:¥Program」はBitPaymerのため、BitPaymerが実行されて感染します。

このように、攻撃者はCドライブ直下のディレクトリへ「Program」というファイル名のBitPaymerを保存できれば、標的のWindowsマシンのアカウントや実行権限無しで、BitPaymerへ感染させることができます [56]。この脆弱性はBonjourへパッチを適用すれば除去できます。しかし過去にWindows版のiTunesまたはiCloudを使っていて、現在アンインストールしている場合であっても、注意が必要です。BonjourはiTunesやiCloudをアンインストールしてもWindowsマシン内に残存して動作しているためです [54]。過去にiTunesやiCloudをアンインストールした人は、最新版のiTunesやiCloudをインストールしてBonjourを最新化してください。または手動でBonjourを削除して、脆弱性を取り除いてください [57]。

5.1.3. ヘルスケア業界を狙うランサムウェア攻撃

2019年度第3四半期は、第1四半期、第2四半期に続き、米国でのランサムウェア被害が多発しています。その中でも、ヘルスケア業界へのランサムウェア攻撃が急増しました。2019年度第3四半期における米国のヘルスケア業界を狙ったランサムウェア被害事例を表 9にまとめました。

表 9:米国におけるヘルスケア業界のランサムウェア被害一覧

日付	標的	概要
10月1日	アラバマ州 DCHヘルスシステム	ランサウェア攻撃を受けてシステムが一部停止したため、業務を停止した。身代金を支払い、復号キーを受け取ったとされている。支払額は不明 [58]
10月11日	オレゴン州 モントレーヘルスセンター	ランサムウェア攻撃により、医療記録が暗号化された。データは復元できたが、サーバからデータが削除された。患者情報の流出有無は不明 [59]
11月17日	バーチャルケアプロバイダ社	ランサムウェア「Ryuk」に感染。約80,000台のマシンへ影響を及ぼし、1,400万ドルの身代金を要求された [60]
11月20日	ミズーリ州 セントフランシスヘルスケア	ランサムウェア攻撃を受けて、医療記録にアクセスできなくなる。バックアップを取っていたため復旧したが、一部のデータは復元できなかった。身代金の支払いは拒否した [61]
11月25日	ネブラスカ州 グレートプレインズヘルス	ランサムウェア攻撃を受けて、メールや電子医療記録等へアクセスできなくなった [62]
12月2日	ニュージャージー州 ハッケンサックメリディアンヘルス	ランサムウェア攻撃により、関係する17の病院・診療所すべてに影響が出た。システム回復のために身代金を支払った。支払額は不明 [63]。
12月11日	ハワイ州 ハワイがんセンター	ランサムウェア攻撃を受けて、2つの治療センターの癌放射線治療サービスを一時的に停止した [64]。

第 3 四半期は、ランサムウェア攻撃で被害を受けた地方自治体が極めて少なくなっています。これは、2019 年 7 月の米国市長会議で採択されたランサムウェア攻撃の身代金支払いに反対する決議 [65]が、米国の地方自治体へのランサムウェア攻撃を牽制している可能性があります。ランサムウェアへ感染しても身代金を支払わないのであれば、攻撃者は攻撃しても身代金を得ることができないため、攻撃者のモチベーションが低下している可能性があります。そのため、第 2 四半期まで地方自治体を狙っていた攻撃者は、ヘルスケア業界にターゲットを変更したと推測します。ヘルスケア業界でのランサムウェア攻撃の被害は、単純に業務が止まる

だけでなく、早急に復旧できない場合、患者の命に影響を与えかねません。医療機関は、患者の命と身代金を天秤にかけたとき、身代金を支払ってシステムを復旧する方を選択する可能性が高いでしょう。そのため攻撃者の格好のターゲットになったと考えられます。

5.1.4. まとめ

2019年度第3四半期において、日本国内でEmotetの感染事例が数多く報告されました。違和感の少ない日本語が用いられていたこともあり、特にセキュリティ対策や訓練が十分でない中小企業においては、幅広く感染が起こったのだと推測されます。メールは依然として広く普及しているコミュニケーションツールであり、今後もEmotetのようなマルウェアのばらまきに利用される状況は継続するでしょう。地道な手段ですが、標的型攻撃メールの訓練は有効な対策です。不審なメールの開封率の低減や、マルウェア感染時の初動対応のスピードや質の向上などの効果が期待できます。

ランサムウェアは米国を中心に被害が長期化しています。長年続いていた自治体への被害件数は減少しました。その一方で、ヘルスケア業界の被害が拡大しています。自治体が身代金の支払いを拒否するケースが増えており、身代金の獲得が困難になった攻撃者が、標的を変更したのだと推測しています。今後、もしヘルスケア業界からの身代金要求が難しくなった場合に、攻撃者は更に標的を変更すると予想されます。高い可用性が要求される電力会社や鉄道会社といったインフラ関連企業のシステムは、格好の攻撃対象となり得るでしょう。また、Emotetが日本国内で流行した例もあり、日本国内の企業がより一層ランサムウェアの被害に晒される可能性は十分にあります。企業内で大規模なランサムウェア感染が発生した場合、システムが停止し業務に多大なる影響が発生する恐れがあります。ランサムウェアの感染を前提とし、システムが停止した際の事業や業務の継続プランを策定し、プランに沿った定期的な訓練の実施を推奨します。

6. 予測

2019年度第3四半期の事例から、現在の傾向および今後の予測を記載します。攻撃の手口や、攻撃が成功した後の換金手段などが、より巧妙化・多様化する傾向にあります。事故を想定した事後策が今後より一層求められることになるでしょう。

変化を続けるランサムウェア攻撃

SodinokibiやMazeなど、ファイルの暗号化だけでなく、情報を盗み出すタイプのランサムウェアが確認されています。攻撃者は、盗み出した情報の流出を盾に脅迫を行うことが可能です。企業の個人情報などの重要情報が、ランサムウェアの標的とされる可能性があります。
また一方で、2020年にはタイで個人情報保護法が施行されるなど、アジア地域において個人情報保護関連の法律の整備が進んでいます。アジア地域の企業の個人情報流出リスクは、よりシビアな問題となりつつあります。
このような背景から、これまで米国中心であった情報を盗み出すタイプのランサムウェア被害が、アジア地域(特に日本・中国・ASEAN地域)にシフトすると予測します。より多くの個人情報を抱えるBtoCビジネスを手掛ける企業は、特に標的になるおそれがあります。

Emotetによる攻撃手口の巧妙化

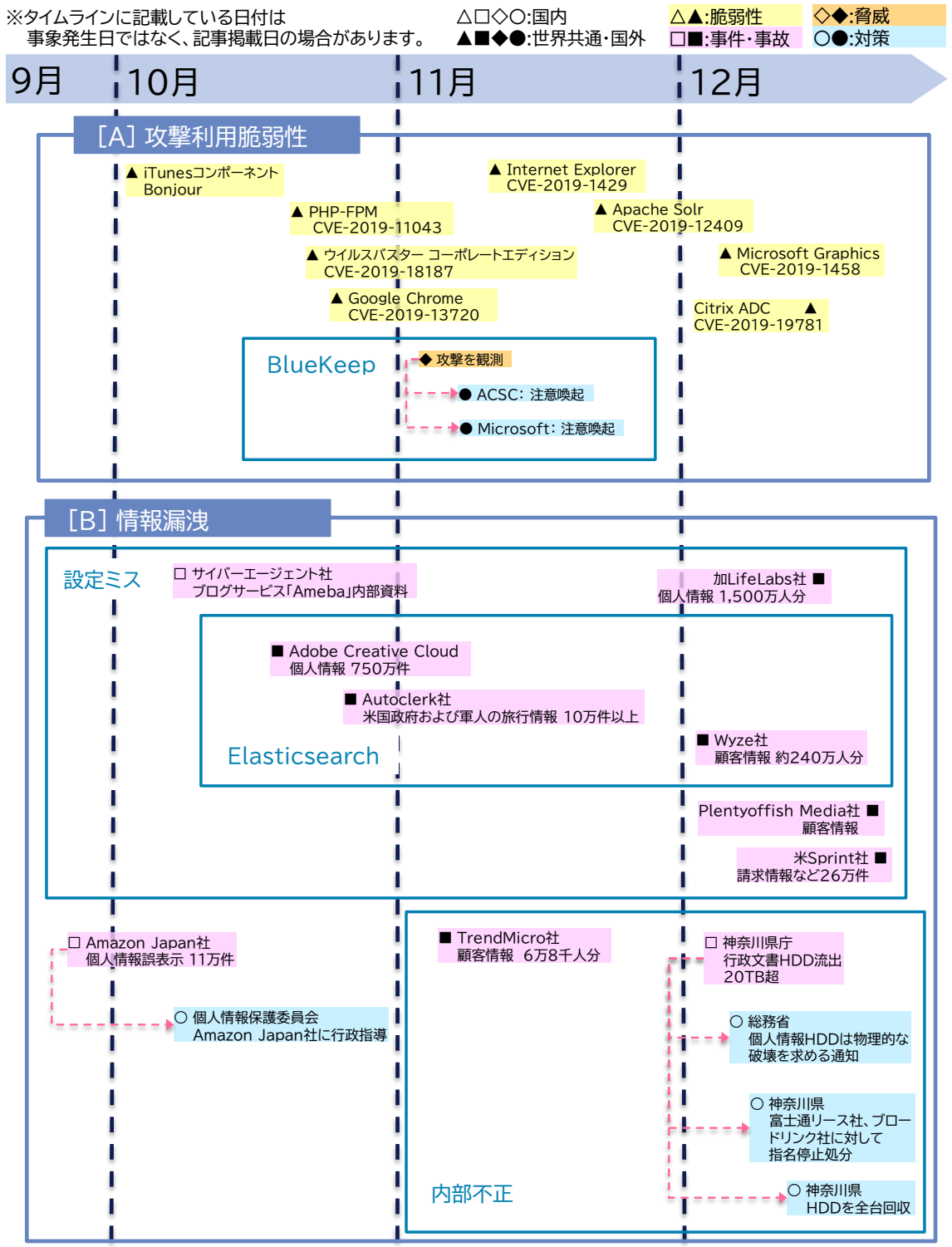
Emotetにも引き続き警戒が必要です。2019年はEmotetによる被害が多発しました。これによって各被害組織から大量のメールが流出したおそれが高く、攻撃者はこのメールの情報を悪用してより広範囲へEmotetを拡散できる準備が整ったと言えます。これまでEmotetの攻撃は、感染した組織やその関係組織へ被害を及ぼすことが中心でした。これからは、攻撃者が大規模なEmotetボットネットを悪用して、任意の組織へDDoSやクリプトジャッキングなどのサイバー攻撃を仕掛けるようになると予測します。

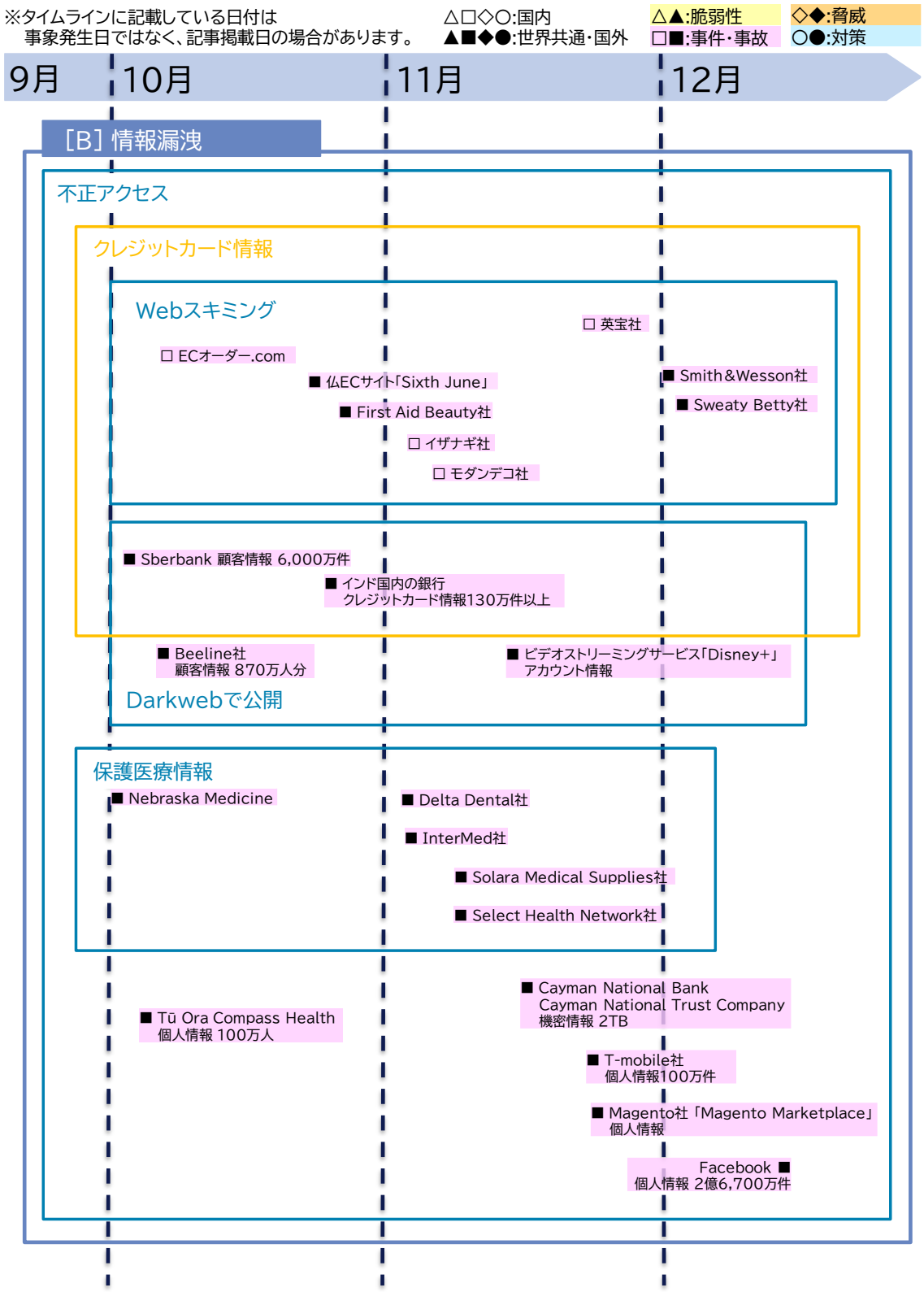
働き方改革、DXに付け入る攻撃に注意

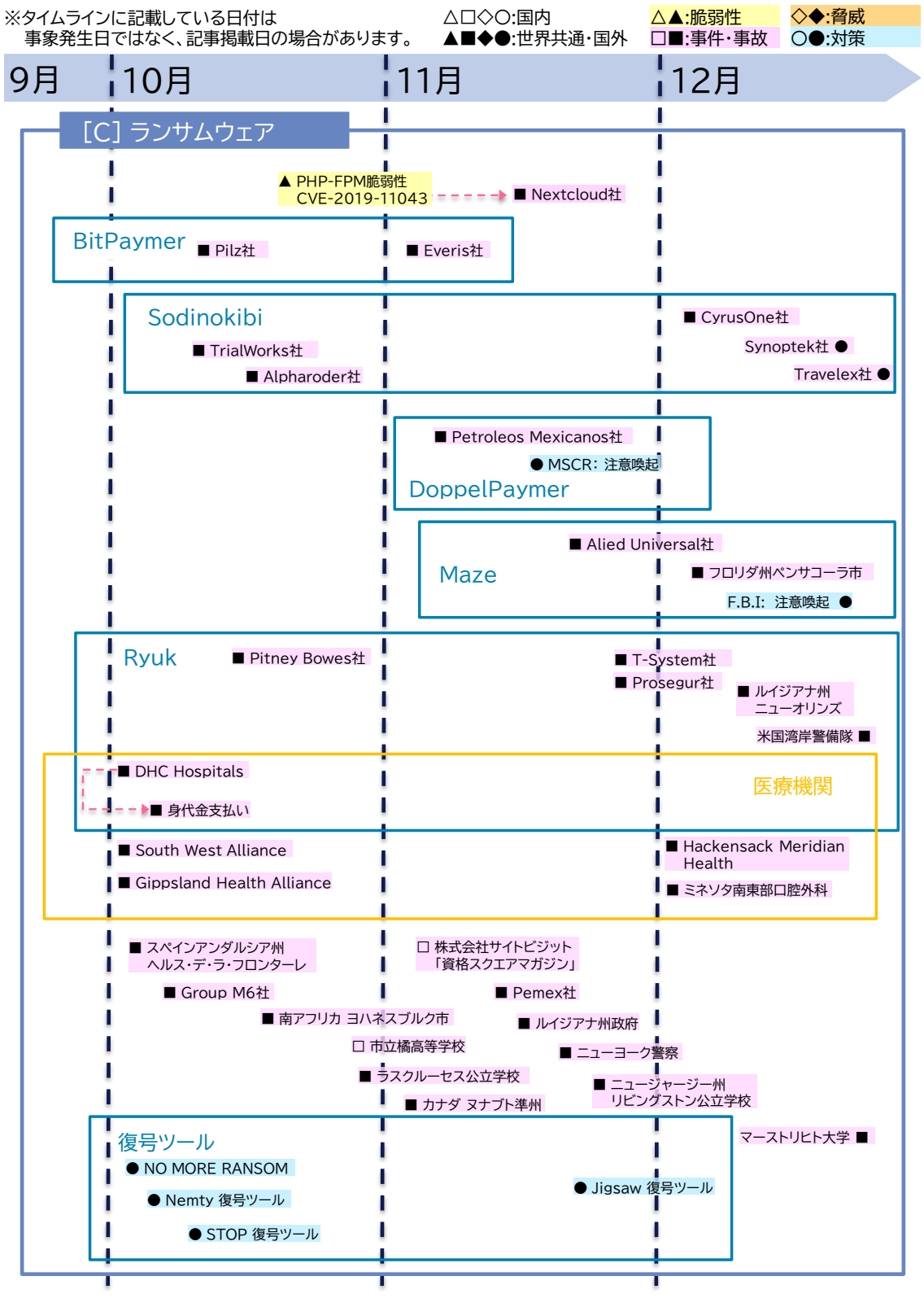
2019年度第三四半期においては、Office365のアカウント乗っ取りを狙う攻撃が発生しました。アカウントの乗っ取りが成功すると、OneDriveなどのOffice365連携アプリから認証なしでOffice365のサービスへアクセス可能でした。
複数のクラウドサービスを利用している場合、ID統合の機能は、複数のクラウドサービスを利用するときの識別認証を一箇所で統合して行えるようになるため、非常に利便性が高いです。しかしその反面、攻撃者は一つのサービスアカウントを侵害できれば複数のクラウドサービスへアクセス可能になります。攻撃者にとって、ID統合の機能で連携したクラウドサービスは、少ない攻撃コストで不正に多くの対価を獲得できる、効率の良い環境となるおそれがあります。攻撃者は今後より一層高いモチベーションで、クラウドサービスのアカウントの侵害を狙ってくると予想します。

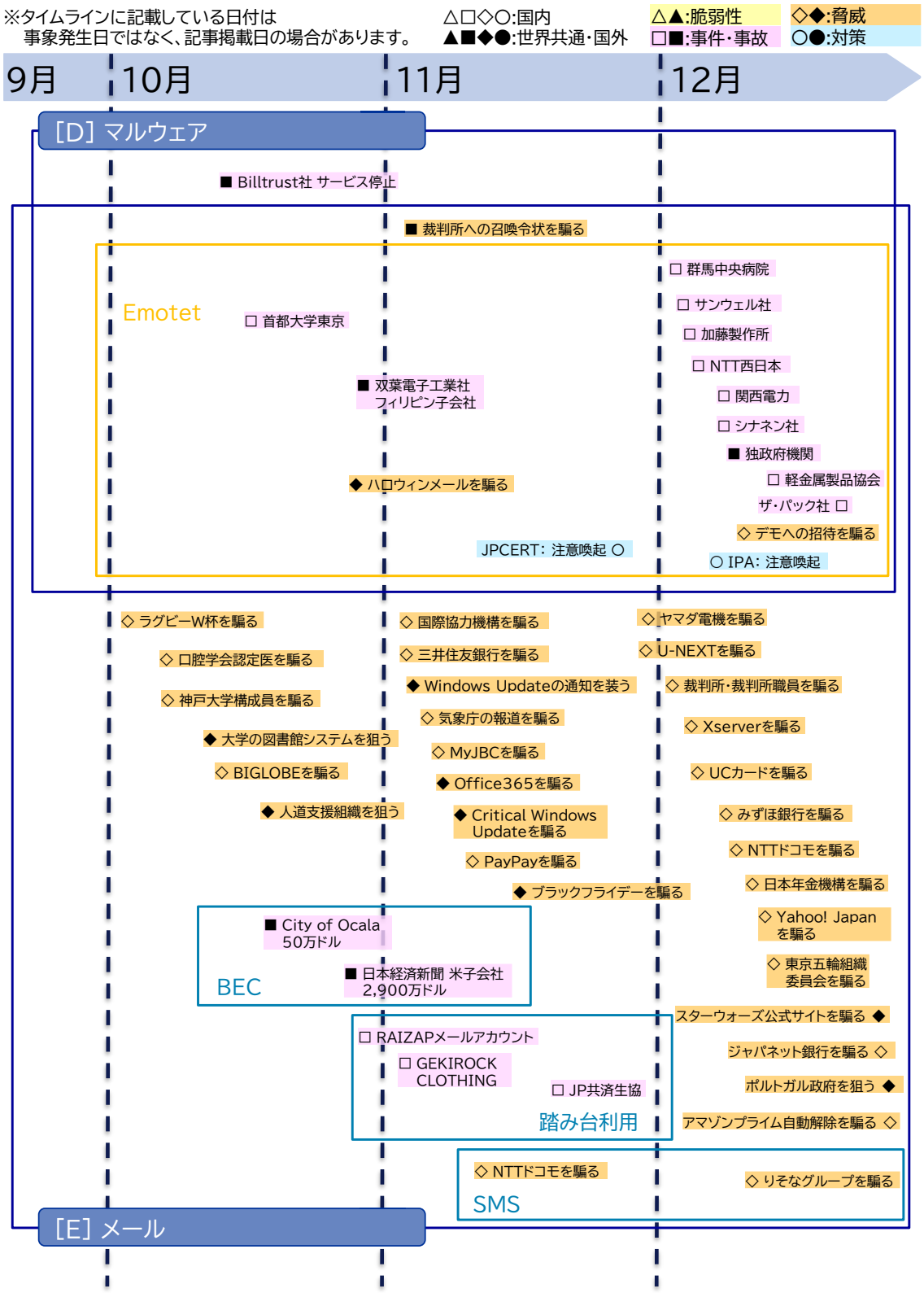
東京五輪、新型肺炎騒動によるテレワークの活用や、企業のデジタルトランスフォーメーション(DX)の推進などで、企業におけるクラウドサービスの利活用が拡大しています。企業のクラウドサービスの管理者は、クラウドサービスの認証、及び認可の設計・運用を厳密に実施してください。また、クラウドサービス上の情報に対しても、適切な資産管理も必須となります。リスクを正しく恐れ、利便性と安全性の両方を高める姿勢が、今後より一層求められると考えます。

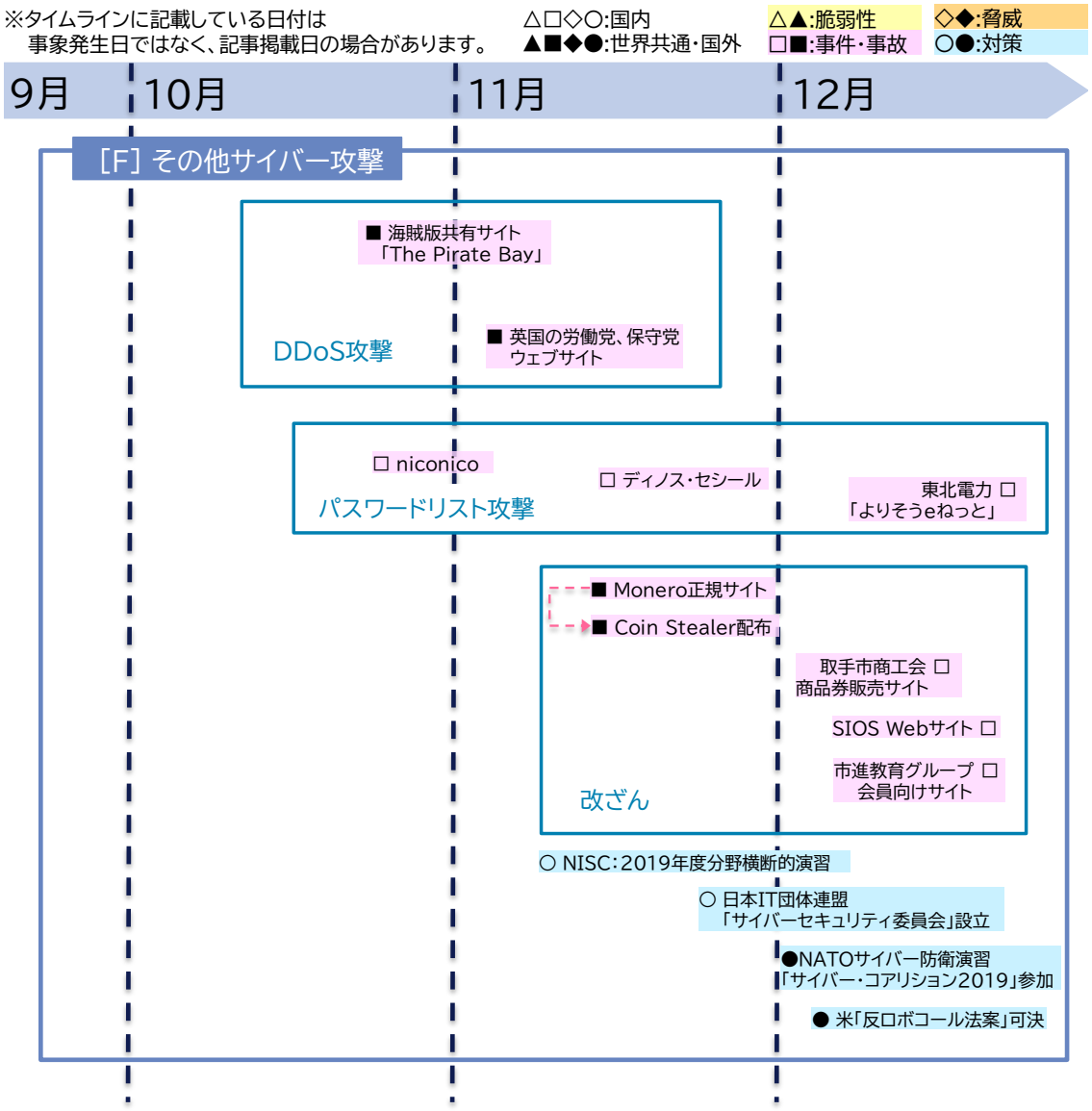
7. タイムライン











参考文献

[1] D. Hardt, "The OAuth 2.0 Authorization Framework," Internet Engineering Task Force, 10 2012. [Online]. Available: https://tools.ietf.org/html/rfc6749.

[2] D. Hardt and M. Jones, "The OAuth 2.0 Authorization Framework: Bearer Token Usage," Internet Engineering Task Force, 10 2012. [Online]. Available: https://tools.ietf.org/html/rfc6750.

[3] 独立行政法人情報処理推進機構, "「 SNS におけるサービス連携に注意！ 」," 独立行政法人情報処理推進機構, 1 10 2012. [Online]. Available: https://www.ipa.go.jp/security/txt/2012/10outline.html.

[4] Microsoft, "Microsoft 公式 - 家庭向けおよび一般法人向け Office 製品の比較," Microsoft, 2020. [Online]. Available: https://products.office.com/ja-jp/compare-all-microsoft-office-products?&activetab=tab:primaryr2.

[5] O. Tsarfati, "BlackDirect: Microsoft Azure Account Takeover," CyberArk Software Ltd., 2 12 2019. [Online]. Available: https://www.cyberark.com/threat-research-blog/blackdirect-microsoft-azure-account-takeover/.

[6] CyberArk Software Ltd., "Microsoft and Azure Account Takeover," CyberArk Software Ltd., 2019. [Online]. Available: https://black.direct/.

[7] M. Tyler, "Phishing Campaign Uses Malicious Office 365 App," PhishLabs, 9 12 2019. [Online]. Available: https://info.phishlabs.com/blog/office-365-phishing-uses-malicious-app-persist-password-reset.

[8] CyberArk Software Ltd., CyberArk Software Ltd., 2019. [Online]. Available: https://black.direct/videos/blackdirect_poc.mp4.

[9] 朝日新聞デジタル, “【独自】行政文書が大量流出　納税記録などのＨＤＤ転売,” 6 12 2019. [オンライン]. Available: https://www.asahi.com/articles/ASMD57WSXMD5UTIL065.html?iref=pc_extlink.

[10] 日経ビジネス, “神奈川HDD転売、元社員は3904個を販売　企業・官公庁に飛び火も,” 10 12 2019. [オンライン]. Available: https://business.nikkei.com/atcl/gen/19/00002/121000948/?P=2&mds.

[11] ITmedia, “HDD転売問題のブロードリンク、従業員30人に解雇通知　社長も退任の意向,” 8 1 2020. [オンライン]. Available: https://www.itmedia.co.jp/news/articles/2001/08/news137.html.

[12] ZDNet, “トレンドマイクロ、内部不正による個人ユーザーの情報流出を発表,” 6 11 2019. [オンライン]. Available: https://japan.zdnet.com/article/35144967/.

[13] IPA, “組織における内部不正対策,” 14 7 2015. [オンライン]. Available: https://www.ipa.go.jp/files/000047237.pdf.

[14] ブロードリンク, “今後の再発防止策,” 9 12 2019. [オンライン]. Available: https://www.broadlink.co.jp/info/pdf/20191209-03-press-release.pdf.

[15] 朝日新聞デジタル, “ブロードリンク元社員を再逮捕　会社からHDD窃盗容疑,” 22 1 2020. [オンライン]. Available: https://www.asahi.com/articles/ASN1Q3H0MN1QUTIL005.html.

[16] IPA, “組織における内部不正防止ガイドライン,” 1 2017. [オンライン]. Available: https://www.ipa.go.jp/files/000057060.pdf.

[17] Hy-Vee, “Notice of Data Breach,” 3 10 2019. [オンライン]. Available: https://www.hy-vee.com/corporate/news-events/announcements/notice-of-payment-card-data-incident-3/.

[18] Krebs on Security, “Sale of 4 Million Stolen Cards Tied to Breaches at 4 Restaurant Chains,” 26 11 2019. [オンライン]. Available: https://krebsonsecurity.com/2019/11/sale-of-4-million-stolen-cards-tied-to-breaches-at-4-restaurant-chains/.

[19] BleepingComputer, “U.S. Food Chain Alerts Customers of Payment Card Incident,” 28 10 2019. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/us-food-chain-alerts-customers-of-payment-card-incident/.

[20] VISA, “ATTACKS TARGETING POINT-OF-SALE AT FUEL DISPENSER MERCHANTS,” 11 2019. [オンライン]. Available: https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-security-alert-attacks-targeting-fuel-dispenser-merchant-pos.pdf.

[21] VISA, “CYBERCRIME GROUPS TARGETING FUEL DISPENSERMERCHANTS,” 12 2019. [オンライン]. Available: http://click.broadcasts.visa.com/xfm/?30761/0/0624013ddc6f39785bf56d504f3b812e/lonew.

[22] security affairs, “Payment card breach potentially impacts all locations of Wawa convenience store,” 20 12 2019. [オンライン]. Available:

https://securityaffairs.co/wordpress/95412/data-breach/wawa-payment-card-breach.html.

[23] VMware Carbon Black, “4 Point-of-Sale Security Flaws that Jeopardize Customer Data,” 2 10 2014. [オンライン]. Available: https://www.carbonblack.com/2014/10/02/4-point-of-sale-security-flaws-that-jeopardize-customer-data/.

[24] 株式会社　リンク, “PCI P2PE(PCI Point-to-Point Encryption)とは?,” 27 4 2016. [オンライン]. Available: https://pcireadycloud.com/blog/2016/04/27/862/.

[25] ScanNetSecurity, “Target のレジがマルウェアに感染、4,000 万のバンクカードを吸い上げる,” 23 1 2014. [オンライン]. Available: https://scan.netsecurity.ne.jp/article/2014/01/23/33411.html.

[26] カスペルスキー, “米国、EMV仕様クレジットカードへの移行で詐欺が増加,” 17 5 2016. [オンライン]. Available: https://blog.kaspersky.co.jp/us-emv-transition-increases-fraud/11188/.

[27] 日本クレジットカード協会, “ＩＣクレジットカードに関する消費者意識調査,” 27 11 2019. [オンライン]. Available: http://www.jcca-office.gr.jp/topics/topics_77.html.

[28] The PHP Group, "Sec Bug #78599 env_path_info underflow in fpm_main.c can lead to RCE," 26 9 2019. [Online]. Available: https://bugs.php.net/bug.php?id=78599.

[29] Help Net Security, "PHP RCE flaw actively exploited to pop NGINX servers," 28 10 2019. [Online]. Available: https://www.helpnetsecurity.com/2019/10/28/cve-2019-11043/.

[30] NGINX, "Addressing the PHP-FPM Vulnerability (CVE-2019-11043) with NGINX," 29 10 2019. [Online]. Available: https://www.nginx.com/blog/php-fpm-cve-2019-11043-vulnerability-nginx/.

[31] NTTデータ先端技術株式会社, "PHP-FPMに含まれるリモートコード実行に関する脆弱性（CVE-2019-11043）についての検証レポート," 6 11 2019. [Online]. Available: http://www.intellilink.co.jp/article/vulner/191106.html.

[32] BLEEPING COMPUTER, "New NextCry Ransomware Encrypts Data on NextCloud Linux Servers," 15 11 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-nextcry-ransomware-encrypts-data-on-nextcloud-linux-servers/.

[33] Nextcloud, "Urgent security issue in NGINX/php-fpm," 24 10 2019. [Online]. Available: https://nextcloud.com/blog/urgent-security-issue-in-nginx-php-fpm/.

[34] Cisco, "Cisco Adaptive Security Appliance Web Services Denial of Service Vulnerability," 24 9 2019. [Online]. Available: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-asaftd.

[35] Help Net Security, "Unpatched Android flaw exploited by attackers, impacts Pixel, Samsung, Xiaomi devices," 4 10 2019. [Online]. Available: https://www.helpnetsecurity.com/2019/10/04/cve-2019-2215/.

[36] Security Affairs, "Hackers continue to exploit the Drupalgeddon2 flaw in attacks in the wild," 8 10 2019. [Online]. Available: https://securityaffairs.co/wordpress/92239/malware/drupalgeddon2-campaign.html.

[37] NTT DATA, "グローバルセキュリティ動向四半期レポート 2019年度第2四半期," 29 11 2019. [Online]. Available: https://www.nttdata.com/jp/ja/news/information/2019/112900/.

[38] NATIONAL SECURITY AGENCY, "MITIGATING RECENT VPN VULNERABILITIES," 7 10 2019. [Online]. Available: https://media.defense.gov/2019/Oct/07/2002191601/-1/-1/1/CSA-MITIGATING-RECENT-VPN-VULNERABILITIES.pdf.

[39] Trend Micro, "【注意喚起】ウイルスバスター コーポレートエディションの脆弱性(CVE-2019-18187)を悪用した攻撃を確認したことによる最新修正プログラム適用のお願い," 28 10 2019. [Online]. Available: https://appweb.trendmicro.com/SupportNews/NewsDetail.aspx?id=3592.

[40] Google, "Stable Channel Update for Desktop," 21 10 2019. [Online]. Available: https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_31.html.

[41] CERT NZ, "Critical vulnerability in Microsoft remote desktop services," 5 11 2019. [Online]. Available: https://www.cert.govt.nz/it-specialists/advisories/vulnerability-microsoft-rdp-services/.

[42] Security Affairs, "Capesand is a new Exploit Kit that appeared in the threat landscape," 8 11 2019. [Online]. Available: https://securityaffairs.co/wordpress/93577/malware/capesand-exploit-kit.html.

[43] BLEEPING COMPUTER, "Magento Urges Users to Apply Security Update for RCE

Bug," 11 11 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/magento-urges-users-to-apply-security-update-for-rce-bug/.

[44] Security Affairs, "Microsoft Patch Tuesday updates fix CVE-2019-1429 flaw exploited in the wild," 13 11 2019. [Online]. Available: https://securityaffairs.co/wordpress/93787/hacking/cve-2019-1429-flaw-fixed.html.

[45] Security Affairs, "Microsoft fixes CVE-2019-1458 Windows Zero-Day exploited in NK-Linked attacks," 11 12 2019. [Online]. Available: https://securityaffairs.co/wordpress/94936/hacking/microsoft-fixes-cve-2019-1458.html.

[46] 尚. 大谷, 義. 小林, 眞. 大石 , 大. 山下, “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,” 株式会社NTTデータ, 29 8 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_1q_securityreport.pdf.

[47] 岡本勝之, “引き続き国内で拡大する「EMOTET」の脅威,” TREND　MICRO, 27 1 2020. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/23648.

[48] JPCERT/CC　コーディネーションセンター, “マルウエア Emotet の感染に関する注意喚起,” JPCERT/CC　コーディネーションセンター, 10 12 2019. [オンライン]. Available: https://www.jpcert.or.jp/at/2019/at190044.html.

[49] 独立行政法人情報処理推進機構 セキュリティセンター, “「Emotet」と呼ばれるウイルスへの感染を狙うメールについて,” 独立行政法人情報処理推進機構 セキュリティセンター, 31 1 2020. [オンライン]. Available: https://www.ipa.go.jp/security/announce/20191202.html.

[50] 時事通信社, “菅官房長官、ＰＣウイルスで注意喚起　「エモテット」,” 時事通信社, 28 11 2019. [オンライン]. Available: https://www.jiji.com/jc/article?k=2019112800997&g=pol.

[51] BBC, “Ransomware behind NHS Lanarkshire cyber-attack,” BBC, 28 8 2017. [オンライン]. Available: https://www.bbc.com/news/uk-scotland-glasgow-west-41076591.

[52] ウェブルート株式会社, “ウェブルート「最も危険なマルウェア2019」を公表,” ウェブルート株式会社, 17 12 2019. [オンライン]. Available: https://www.webroot.com/jp/ja/about/press-room/releases/2019.

[53] M. R. Lopez, “Spanish MSSP Targeted by BitPaymer Ransomware,” McAfee, 8 11 2019. [オンライン]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/spanish-mssp-targeted-by-bitpaymer-ransomware/.

[54] M. Gorelik, “APPLE ZERO-DAY EXPLOITED IN NEW BITPAYMER CAMPAIGN,” Morphisec, 10 10 2019. [オンライン]. Available: https://blog.morphisec.com/apple-zero-day-exploited-in-bitpaymer-campaign.

[55] Apple, “iTunes for Windows 12.10.1 のセキュリティコンテンツについて,” Apple, 2 12 2019. [オンライン]. Available: https://support.apple.com/ja-jp/HT210635.

[56] D. GOODIN, “Attackers exploit an iTunes zeroday to install ransomware,” Ars Technica, 11 10 2019. [オンライン]. Available: https://arstechnica.com/information-technology/2019/10/attackers-exploit-an-itunes-zeroday-to-install-ransomware/.

[57] C. Cimpanu, “Ransomware gang uses iTunes zero-day,” ZDNet, 10 10 2019. [オンライン]. Available: https://www.zdnet.com/article/ransomware-gang-uses-itunes-zero-day/.

[58] M. Garrity, “3 Alabama hospitals halt admissions after ransomware attack,” Becker's healthcare, 2 10 2019. [オンライン]. Available: https://www.beckershospitalreview.com/cybersecurity/3-alabama-hospitals-halt-admissions-after-ransomware-attack.html.

[59] M. Garrity, “Oregon medical center EHR encrypted in ransomware attack,” Becker's Healthcare, 17 10 2019. [オンライン]. Available: https://www.beckershospitalreview.com/cybersecurity/oregon-medical-center-ehr-encrypted-in-ransomware-attack.html.

[60] M. Garrity, “Virtual Care Provider target in $14M ransomware attack, leaving patient records inaccessible,” Becker's Healthcare, 25 11 2019. [オンライン]. Available: https://www.beckershospitalreview.com/cybersecurity/virtual-care-provider-target-in-14m-ransomware-attack-leaving-patient-records-inaccessible.html.

[61] M. Garrity, “Missouri health system alerts patients of ransomware attack,” Becker's Healthcare, 21 11 2019. [オンライン]. Available: https://www.beckershospitalreview.com/cybersecurity/missouri-health-system-alerts-patients-of-ransomware-attack.html.

[62] M. Garrity, “Great Plains Health cancels nonemergency procedures after

ransomware attack,” Becker's Healthcare, 27 11 2019. [オンライン]. Available: https://www.beckershospitalreview.com/cybersecurity/great-plains-health-cancels-nonemergency-procedures-after-ransomware-attack.html.

[63] J. Drees, “Hackensack Meridian paid ransom for cyberattack that shut down computer network,” Becker's Healthcare, 13 12 2019. [オンライン]. Available: https://www.beckershospitalreview.com/cybersecurity/hackensack-meridian-paid-ransom-for-cyberattack-that-shut-down-computer-network.html.

[64] M. Garrity, “Cancer radiation treatment halted after ransomware attack at Hawaii center,” Becker's Healthcare, 12 12 2019. [オンライン]. Available: https://www.beckershospitalreview.com/cybersecurity/cancer-radiation-treatment-halted-after-ransomware-attack-at-hawaii-center.html.

[65] The United States Conference of Mayors, “87th Annual Meeting Opposing Payment To Ransomware Attack Perpetrators,” The United States Conference of Mayors, 9 7 2019. [オンライン]. Available: http://legacy.usmayors.org/resolutions/87th_Conference/proposedcommittee-preview.asp?committee=Criminal%20and%20Social%20Justice.

NTT DATA
Trusted Global Innovator

2020年2月28日発行

株式会社NTTデータ
セキュリティ技術部
大谷 尚通 / 小林 義徳 / 大石 眞央 / 山下 大輔
星野 亮 / 鈴木 悦生 / 板山 健司郎 / 伊藤 友洋 / 加藤 崇之 / 清水 一貴
nttdata-cert@kits.nttdata.co.jp