グローバルセキュリティ動向四半期レポート

2022 年度　第 2 四半期

目次

1. エグゼクティブサマリー

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。

注目トピック 『Covid-19後のテレワークにおけるリスクと対策』

Covid-19の流行により、多くの企業は社員が人混みを避けることができるよう、テレワーク等のリモートワーク中心の働き方へ切り替えて、社員の出社を抑制しました。その際、事業継続性を優先するために社内セキュリティルールへ特例/例外ルールを追加したものが、セキュリティインシデントの原因を引き起こすタイミングの増加につながっています。

アフターコロナを見据え、特例/例外ルールをもとに戻す検討が必要になります。もしくは、特例/例外ルールのリスクを分析し、セキュリティ上の問題点を解決するセキュリティ対策を追加した上で、ルール自体を更新すべきです。

注目トピック 『個人情報保護法の改正について改めて考える』

2022年4月に施行された改正個人情報保護法では、事業者の守るべき責務の注目度が増しており、「個人情報保護委員会への報告や本人への通知の義務化」や「法の域外適用・越境移転の在り方」が注意すべきポイントとなっています。

事業者の対応としては、３年ごとに見直される個人情報保護法の改正に合わせて、定期的に自社のルールや手順を見直すことが重要です。また、技術の進歩や社会の情勢により、事業者が個人情報の扱い方をその時代に合った最適なものに見直すことも必要です。

脆弱性 『多要素認証の脆弱性を突いたMFA疲労攻撃』

多要素認証（MFA）のプッシュ通知を悪用した、MFA疲労攻撃による被害が発生しています。

まず、プッシュ通知の方式改善や他方式への変更などの技術的対策の検討が必要です。また、MFA疲労攻撃の認知度を上げ、身に覚えのないプッシュ通知は絶対にログイン許可しない、不審なプッシュ通知を発見したらシステム管理者へ報告しパスワードを変更する、といった組織的・人的対策を行うことも重要になります。

マルウェア・ランサムウェア 『Linuxを標的としたマルウェアの感染手法と検知回避技術の高度化』

2022年度 第2四半期は、クラウド上のサーバやIoT機器などのうち、Linuxを狙った金銭目的のマルウェアの攻撃が増加しています。さらにLinuxを標的とした検知が難しい高度なマルウェアが見つかっています。この高度なマルウェアのうち、検知が難しいOrbitとShikitegaを紹介します。Orbitは、感染後のマルウェア活動の検知を回避する手法に特徴があり、例えばOrbitは、ユーザが感染マシン上で通信ログを調査しても、Orbitのバックドアの通信記録を見ることができません。Shikitegaは、感染が成功するまでの間、複数の技術を使って検知を回避する手法に特徴があります。例えば、悪意のあるコードを3段階に分けてインストールする感染チェーンと呼ばれる手法を用いたり、「Shikata Ga Nai(仕方がない)」というエンコーダでシェルコードを難読化する手法を用いたりして、パターンマッチングによる検知を回避しています。

2. 注目トピック 『Covid-19後のテレワークにおけるリスクと対策』

2.1. Covid-19後のテレワークにおけるリスクと対策

2.1.1. 一般的になったニューノーマル

2020年、新たな感染症、Covid-19が流行し、各企業はそれぞれの事業を継続すべく、様々な対応策を実施してきました。

2020年：Covid-19が流行。突貫工事で「テレワーク」を導入
2021年：テレワークに関するルールの見直しを実施
2022年:アフターコロナの働き方としてテレワークが定着しつつある(現在)

IPAは、2020年と2021年に「企業・組織におけるテレワークのセキュリティ実態調査」をおこない、各社のセキュリティ対策や業務委託契約にどのような影響があったのか、アンケート調査を行いました。「2021年度企業・組織におけるテレワークのセキュリティ実態調査」のアンケートでは、委託元企業239社と委託先269社の合計508社が回答しました。本記事では、この「2021年度企業・組織におけるテレワークのセキュリティ実態調査」のアンケート回答をもとに、テレワーク導入当時に一時的に採用した特例/例外ルールを考察していきます

2.1.2. 特例/例外として扱われたルールたち

多くの企業は、Covid-19が感染流行したため、社員が人混みを避けることができるよう、テレワーク中心の働き方へ切り替えて、社員の出社を抑制しました。働き方を大きく変更して、かつ事業継続性を優先したため、社内セキュリティルールへ特例/例外ルールを追加しました。一例として以下のようなルールがあります。

- 機密情報を保存できる会社支給PCの持ち出し
- 個人所有PCの業務利用（BYOD）
- 機密情報の社外（自宅・サテライトオフィス等）での印刷

上記のルールは、前記の2021年の調査結果でも取り上げられており、アフターコロナの今まで特例/例外ルールとして残っていることがわかります。では、これらの特例/例外ルールが引き起こすおそれのあるセキュリティリスクを考察していきます。

2.1.3. 特例/例外化ルールとのインシデントの関係

2020年4月以降に実際に発生したセキュリティインシデントはどうだったのでしょうか。アンケート結果より、委託元と委託先では、以下の3つのセキュリティインシデントが多く発生しました。

- テレワークで利用するPCのマルウェア感染（委託元/委託先 共通）
- テレワークで利用するPCの紛失・盗難（委託元）
- 紙資料や書類・USBメモリ等の電子記録媒体の紛失・盗難（委託先）

まずテレワークで利用するPCのマルウェア感染は、「個人所有PCの業務利用（BYOD）」と関連性が深く、セキュリティ対策が不十分な個人所有PCを利用しているため発生している可能性が高いです。会社貸与PCはURLフィルタやEDR、SWG(Secure Web Gateway)などの最先端のセキュリティ対策製品を多層的に導入していますが、個人所有PCは一般的にウイルス対策ソフトをインストールだけの対策です。さらに個人所有PCは、業務でWebアクセスする場合と異なり、制限なくさまざまなWebサイトを閲覧します。そのため、インシデントの主な原因となる不審/発信元不明なサイトへのアクセス、ソフトウェアインストール、メール開封などを行いやすく、対策も不十分なためインシデントにつながると予想します。

テレワークで利用するPCの紛失・盗難は、「機密情報を保存できる会社支給PCの持ち出し」が関連してきます。紛失・盗難の原因は、Covid-19の流行前と変わらず、電車の棚に置く、どこかに放置するなどの外出先でPCを肌身離さず持ち歩かない場合や安全な場所で管理していない場合に発生します。ただしCovid-19の流行前と比較して、現在はテレワークする社員が増加しております。つまりPCを職場と自宅の間を持ち歩く機会が増えており、それだけインシデントの原因を引き起こすタイミングの増加につながっています。

紙資料や書類・USBメモリ等の電子記録媒体の紛失・盗難も「機密情報の社外（自宅・サテライトオフィス等）での印刷」が同じ理由であげられます。紛失・盗難の主な原因は変わらず、社外において印刷ができることで置き忘れする可能性を増やしています。

2.1.4. 対策

前述の特例/例外ルールとセキュリティインシデントの関係の仮説をもとに、セキュリティインシデントのセキュリティ対策を提案します。セキュリティ対策には、関連している特例/例外ルールのあるべき姿もまとめます。

テレワークで利用するPCのマルウェア感染は、「個人所有PCの業務利用（BYOD）」と関係が深く、主な原因は会社貸与PCと比較して、セキュリティ対策が不十分であることです。会社が用意するセキュリティ対策製品を個人所有PCへ導入する場合は、ライセンス上の問題があります。そのため個人所有PCのセキュリティ対策の強化は難しく、個人所有PCの業務利用（BYOD）は、やはりリスクが大きく、会社貸与PCを使用する方が良いです。特例/例外ルールのあるべき姿は、「特例/例外ルールとして認めず、いかなる状況でも会社貸与PCを使用すること」です。

テレワークで利用するPCの紛失・盗難は、「機密情報を保存できる会社支給PCの持ち出し」が関連しています。ただ主要な原因はCovid-19流行前から変わらないこと、そして注目すべきは紛失・盗難後の情報流出にあることから、特例/例外ルールのあるべき姿は、「紛失・盗難から情報流出までのリスクを考慮したセキュリティ対策を施した会社支給PCの使用を許可すること」になります。またこのルールにおいては特例/例外ルールではなく、規定や手順を整理し、認可した状態を作るべきです。具体的には紛失・盗難後の情報流出まで注目し「紛失・盗難後はリモートアクセスによる端末初期化」が実施できる環境構築と紛失・盗難後の手順にするなどあげられます。

急いでテレワーク中心の働き方へ切り替えていた当時は、特例/例外ルールが必要だったと思います。しかし一時的な特例/例外ルールの追加は、セキュリティ対策として設けた制限や規制を緩和し、その結果、セキュリティ対策自体を弱めてしまいます。一時的な対応である以上、特例/例外ルールには有効期限をさだめるべきです。また、社内のセキュリティルールの見直しや遵守状況の再確認のタイミングでは、特例/例外ルールをもとに戻す、もしくは特例/例外ルールのリスクを分析し、セキュリティ上の問題点を解決するセキュリティ対策を追加した上で特例/例外ルールのまま運用せず、ルール自体を更新すべきです。

2.1.5. NTTデータのテレワーク

テレワーク時のPCの紛失・盗難のリスクは、シンクライアント端末を利用すれば対策可能です。しかし、常に通信回線を維持してリモートアクセスして作業しなければならず、通信回線を維持できない環境では使用できません。ユーザ目線に立つと、シンクライアント端末はいつでもどこでも使える、可用性の高い環境とはいえません。やはり可用性は、ファットクライアント端末が優位でしょう。

NTTデータではCovid-19の流行前からテレワークの強化を進めており、セキュアFATと呼ばれるよりセキュアなファットクライアント端末を利用しています。一例として、ゼロトラストの考え方に基づいた弊社のテレワーク環境を紹介します。（図 2-1）

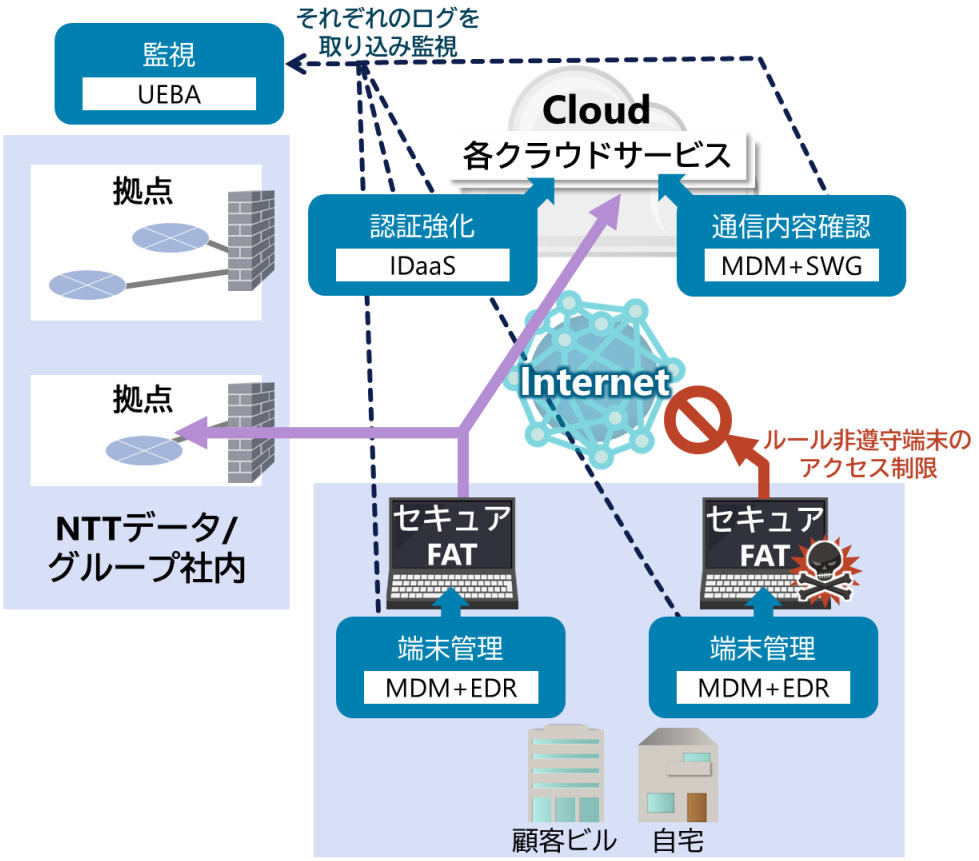


図 2-1 ： NTTデータにおけるテレワーク構成図

主要な要素技術は以下の通りとなります。

- セキュアFATは、集中管理により自動的にパッチを適用したり、マルウェアやサイバー攻撃を検知・遮断したりして、健全な状態を維持します。2.1.3で挙げたインシデントの1つ「テレワークで利用するPCのマルウェア感染（委託元/委託先 共通）」の対策です。以下の要素技術を使用します。
    - MDM（Mobile Device Management）：
      セキュアFATのOSやアプリのバージョンチェックやパッチ適用を自動で行います。管理者が管理コンソール(SaaS)から集中管理します。
    - EDR（Endpoint Detection and Response）：
      セキュアFATの操作や動作をリアルタイムに監視して、マルウェア感染やサイバー攻撃を検知して、自動対処や管理者による遠隔対処を実現します。APT攻撃や高度なマルウェア感染も検知できます。フォレンジック担当者が管理コンソール(SaaS)から詳細調査したり、マルウェアを駆除したりできます。
- セキュアFATからインターネット上のクラウドサービスやNTTデータ社内リソースへ通信する場合、ユーザとセキュアFATを識別・認証して、すべての通信をこまかく許可/制御して守ります。識別・認証は、「テレワークで利用するPCの紛失・盗難（委託元）」後に、第三者がそのPCを悪用して社内リソースへ不正アクセスするリスクを防ぎます。通信の許可/制御は、「テレワークで利用するPCのマルウェア感染（委託元/委託先 共通）」の対策です。以下の要素技術を使用します。
    - IDaaS（Identity as a Service）：
      IDを一元管理して、セキュアFATからクラウドサービスやNTTデータ社内リソースへアクセスするときにID 連携を行い、統一した認証を提供します。シングルサインオンや多要素認証の機能も提供します。
    - MDM＋SWG（Secure Web Gateway）：
      セキュアFATからクラウドサービスやNTTデータ社内リソースへ送信する通信を暗号化したり、ポリシにしたがって通信内容をチェックしたりして、通信を制御するクラウド型プロキシです。サイバー攻撃やマルウェア関連の危険な通信やポリシに違反する通信を遮断します。MDMと連携してOSの最新パッチが未適用なPCを特定して、状態が改善するまで、クラウドサービスやNTTデータ社内リソースへの通信を遮断します。SSL通信を復号して，通信内容を監視できます。
    - MDM：
      セキュアFATの紛失や盗難、もしくは長期間使用していない場合は、管理者が管理コンソール(SaaS)からセキュアFATを強制初期化（リモートワイプ）します。
    - UEBA（User and Entity Behavior Analytics）：
      IDaaSやSWG、クラウドサービス、EDR、セキュアFATのログを集約して監視して、ユーザやデバイスの異常な振る舞いからサイバー攻撃を検知します。振る舞いの教師モデルの作成には機械学習を使用します。ユーザやデバイスの異常な振る舞いが積み重なるとリスクスコアが高くなり、サイバー攻撃などのリスクとして検知します。

2.1.6. まとめ

今回問題視した特例/例外ルールは、急いでテレワーク中心の働き方へ切り替えるために、社内のセキュリティルールに穴を開けてしまうことをわかった上で、やむを得ず取った方法だと思います。しかし、2.1.3で紹介した、Covid-19の感染流行下で多く発生した3つのセキュリティインシデントは、決して防げないセキュリティインシデントではありません。インシデントの発生を防いだり被害を軽減できたりするさまざまなセキュリティ対策があります。特にゼロトラストの考え方に基づいたセキュリティ対策は、Covid-19の感染流行で安全なテレワーク環境の構築ニーズにあわせて、多くの組織が既存の境界防御方式のセキュリティ対策から乗り換えたと思います。最新の対策や技術を用いてセキュアな業務環境を構築することが大切です。

このように、NTTデータも既存の境界防御方式からゼロトラスト方式のセキュリティ対策へブレークスルーを経験して、構築や運用のノウハウを蓄積できました。「ゼロトラストがわからない」「何を準備すればいいのだ」「どういった基準を設ければいい」など、ゼロトラストの考え方に基づいたテレワーク環境の構築で悩み事には、ヒントを提供できると思います。そして共に素晴らしいテレワーク環境を構築しましょう。

3. 注目トピック『個人情報保護法の改正について改めて考える』

3.1. 2022年全面施行した改正個人情保護法

個人情報保護法は3年ごとに見直されており、2020年に改正された個人情報保護法は2022年4月に施行されました。今回の改正では、下記の点を反映することを目的としています [1]。

- 個人の権利の保護と活用の強化
- 越境データの流通増大に伴う新たなリスクへの対応
- AI・ビッグデータ時代への対応

2022年に施行された改正個人情報の概要は、表 3-1の通りです [2]。

表 3-1 ： 改正部分の概要

カテゴリ	改正点
①個人の権利の在り方	1．短期保有データの保有個人データ化 2．個人情報の利用停止・消去、第三者提供禁止の個人請求権の緩和 3．個人データの電磁的記憶の開示を含め開示方法の指定（デジタル化） 4．第三者提供記録の本人開示請求 5．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を限定
②事業者の守るべき責務の在り方	1．個人情報保護委員会への報告や本人への通知の義務化 2．不適正な方法での個人情報利用が禁止
③事業者による自主的な取り組みを促す仕組みの在り方	1．認証個人情報保護団体制度で、企業の特定分野（部門）を対象とする団体の認定制度を新設
④データ利活用の在り方	1．「仮名加工情報」を創設 2．提供先で個人データとなることが想定される場合の確認義務
⑤ペナルティの在り方	1．命令違反・虚偽報告等の行為者への罰金が引き上げ（法人は行為者より罰金刑最高額が引き上げ）
⑥法の域外適用・越境移転の在り方	1．日本国内の個人情報等を取り扱う外国事業者を、罰則付きの報告徴収・命令の対象とて追加 2．外国の第三者への個人データ提供時、移転先での個人情報の取り扱いに関する本人への情報提供の充実

3.2. 事業者が注意すべきポイント

3.2.1. 個人情報漏えい時の報告通知義務

表 3-1に記載した改正の概要の中のうち、「②事業者の守るべき責務」は年々注目度が増しています。今回の改正では、「⑤ペナルティの在り方」の「1．命令違反・虚偽報告等の行為者への罰金が引き上げ」が行われており、この条項に抵触しないためには、「②事業者の守るべき責務の在り方」の「1．個人情報保護委員会への報告や本人への通知の義務化」が大きなポイントです。

（1） 漏えい時の報告通知義務の詳細 [3]

個人情報漏えいが発生した場合の個人情報保護委員会への報告および本人への通知は、以前は努力義務でしたが、改正により下記の4点に該当する場合は報告と周知が義務になりました。

(a) 要配慮個人情報が含まれる個人データの漏えい等
(b) 不正利用により財産的被害が生じるおそれがある個人データの漏えい等
(c) 不正の目的をもって行われたおそれがある個人データの漏えい等
(d) 個人データに係る本人の数が千人を超える漏えい等

改正前と改正後の報告の違いをまとめたものが図 3-1となります [4]。

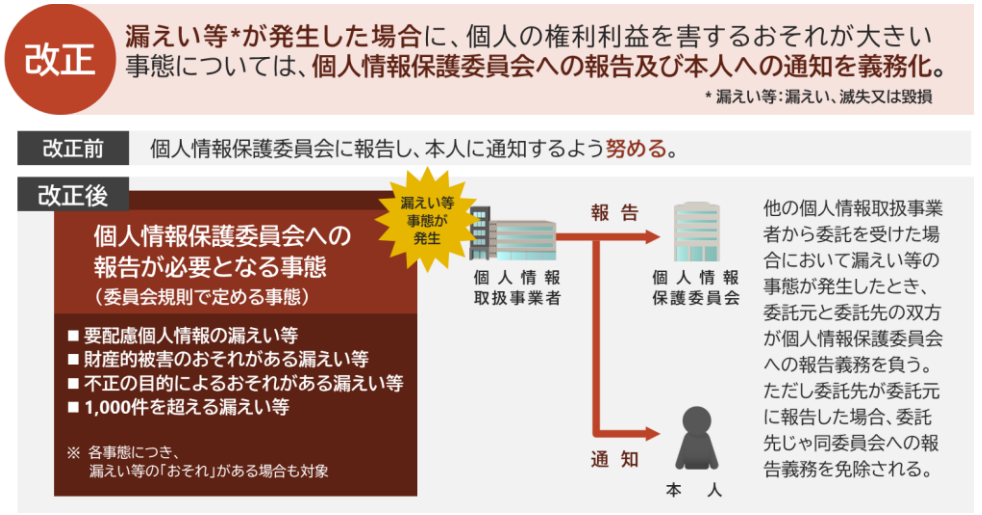


図 3-1 ： 報告通知義務に関する改正

また、個人情報保護法施行規則では、個人情報保護委員会への報告は「速報」と「確報」という２つの形を定めています。表 3-2に示すように、速報と確報は、報告期限が異なります。速報は、表 3-2の①から⑨のうち、報告時に把握している内容を報告します。

表 3-2 ： 報告と通知

対応事項		期限	報告（通知）内容
個人情報保護委員会への報告	速報	報告の対象となる事態を知ったときは、速やかに（おおよそ3～5日以内）	①概要、②漏えい等が発生し、又は発生したおそれがある個人データの項目、③漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数、④原因、⑤二次被害又はそのおそれの有無及びその内容、⑥本人への対応の実施状況、⑦公表の実施状況、⑧再発防止のための措置、⑨その他参考となる事項 （速報では上記のうち報告時に把握している内容）
	確報	30日以内 （不正目的の個人データの漏えいの可能性がある場合は、60日以内）	
本人への通知		当該事態の状況に応じて速やかに （把握状況、本人の権利利益が保護される蓋然性、通知により生じる弊害等を勘案して判断）	報告事項のうち下記の項目： ①概要、②漏えい等が発生し、又は発生したおそれがある個人データの項目、④原因、⑤二次被害又はそのおそれの有無及びその内容、⑨その他参考となる事項

（2） 個人情報漏えいの公表と報告

東京商工リサーチの個人情報漏えい・紛失事故調査によると、上場企業とその子会社が公表した個人情報の漏えい・紛失事故の件数は、2021年の137社から2022年の165件、公表した上場企業とその子会社の数は、2021年の120社から2022年の150社へと、どちらも2年連続で過去最多を更新しています [5]。また、個人情報漏えいの原因をみると「ウイルス感染・不正アクセス」が55.1%で、こちらも2021年の49.6%を上回っています。個人情報漏えいの原因が、この「ウイルス感染・不正アクセス」の場合は、報告を義務づけている「(c)不正の目的をもって行われたおそれがある個人データの漏えい等」に該当し、個人情報保護委員会への報告対象です。

実際に個人情報保護委員会が、2022年度上半期活動実績で報告している個人情報保護委員会へ届け出があった個人データの漏えい事案、つまり2022年度上半期の個人情報漏洩事故の届け出件数は1,587件となっており、前年同期比で約3倍の報告が上がっています [6]。個人情報の漏えい・紛失事故の公表数の1.2倍の増加と比べて、2022年度上半期の届け出件数の3倍の増加のほうが、一段と増えています。同報告書は、単に個人情報の漏えい・紛失事故が増えたというだけでなく、個人情報保護法の改正により、2022年度から個人情報保護委員会への報告義務が課せられたことから、今まで見過ごされてきた個人情報の漏えい・紛失事故も報告するようになったと、述べています。また、最近の個人情報の保護に関する注目度や「⑤ペナルティの在り方」の「1．命令違反・虚偽報告等の行為者への罰金が引き上げ」なども影響を与えていると考えます。

（3） 中小企業の実態

個人情報漏えい・紛失事故の報告数の増加に加えて懸念されるのが、報告対象となる個人情報漏えい・紛失事故の全てが、適切に個人情報保護委員会に報告されているとは限らない点です。個人情報保護委員会が実施した調査によると、既に改正個人情報保護法が施行された後である2022年6月時点でも、4割弱の中小企業が改正個情法の内容を「知らない」と答え、4社に3社は個人情報漏えい事故の報告義務を把握していませんでした [7]。要配慮個人情報を扱うことが多い病院や薬局などは中小企業であることも多く、実際に報告されるべき個人情報漏えい・紛失事故は、個人情報保護委員会にあった1,587件よりもさら

に多いと予想します。

なお、東京商工リサーチの個人情報漏えい・紛失事故調査 [5]によると、個人情報漏えいを公表した上場企業の7割以上が東証プライムに上場していました。また同調査では、大手企業は事業範囲や従業員数、顧客数も多く、サイバー犯罪に巻き込まれる可能性が高いが、一方でガバナンス体制が充実し、情報開示のフローなどを徹底していることも公表数が多い要因と考察しています。これは企業数・従業員数の合計ともに、大企業より中小企業の方が多いため [8]、単純な紛失事故は中小企業の方が多いと予想します。しかし個人情報漏えいの公表数は極端に大手企業に偏っていることからも、大企業はガバナンス体制が充実し、情報開示のフローが徹底していると考えられます。

表 3-3に上記の個人情報漏えいに関する公表数と報告数をまとめました。表3-3のように個人情報漏えいに関する公表数と報告数の増加の違いや、中小企業の4社に3社は漏えい報告義務を把握していない実態、さらには大企業と比べて中小企業の方がガバナンスや情報開示のフローが未整理であるという推測から、中小企業では、報告数よりさらに多くの個人情報の漏えいが起こっていると考えます。

改正個人情報法保護法は、新たに個人情報保護委員会への報告と本人通知のプロセスが加わりました。中小企業も個人情報保護委員会のWebページなどから改正内容を把握し、必要に応じて個人情報漏えい時のフローやプロセスを整理することが求められます。また、自社では個人情報保護法の改正にあわせて既に個人情報の管理や運用フローの整備を適切に実施している場合も、委託先や関係会社の中小企業も、改正にあわせて適切に対応が完了していることを確認しましょう。

表 3-3 ： 公表と報告の実態

対象組織	対象数	2021年	2022年	増加率
上場企業とその子会社	個人情報の漏えい･紛失事故の公表数	137件（120社）	167件（150社）	1.21倍（1.25倍）
民間事業者	個人情報保護委員会へ報告された上半期の個人データ漏えい事案数	報告数は上半期のみ 517件	1,587件	3.07倍

3.2.2. 越境移転の在り方

2020年の改正後にLINE社が海外拠点にて個人情報を扱っていたということが騒がれたこともあり、表 3-1の「⑥法の域外適用・越境移転の在り方」も、注目すべきポイントです。

今回の改正に関する越境移転の在り方の注意点は、2020年度の四半期レポートに詳細に説明しています [9]。まず個人情報を取り扱う事業者は、表 3-2の「⑥法の域外適用・越境移転の在り方」の「2. 外国の第三者への個人データ提供時の本人への情報提供の充実」に記載の改正内容を把握することが必要となります。つぎに事業者は、外国の第三者へ個人データを提供する際に、本人へ法令に沿った形で個人情報の取り扱いに関する情報をより分かりやすく提供するフローやプロセスを整備します。これらは事業者が利用者の信頼を獲得する上で不可欠です。

3.2.3. その他の対応

3.2.1および3.2.2章で述べた漏えい時の報告および通知と越境移転の在り方以外にも、改正に伴い、新たに対応が必要となる部分が存在します。対応が必要な部分は、図 3-2の作業1～3のように、扱っているデータの利用方法を根本的に確認しなおさなければならない大変な事項から、現在のフローやプロセスに項目を追加するだけの簡単な事項まであります。

例えば「①個人の権利の在り方」の「1. 短期保有データの保有個人データ化」は、新たに保有個人データの定義が見直されたため、図 3-2の作業1のように現在取り扱っているデータの中に新たに保有個人データに該当するデータはないか、確認する必要があります。もし新たに保有個人データに該当するデータがある場合は、以降の作業2、3の作業のように新しく保有個人データとなるデータに関する運用フローやプロセスを見直す必要がでてきます。

一方、「①個人の権利の在り方」の「3. 個人データの電磁気記録の開示を含め開示方法の指定（デジタル化）」は、個人データを電磁的方法で提供する方法を検討する必要はあるものの、現在の開示方法のフローに新たに確認事項を追加するだけの場合が多いと考えます。

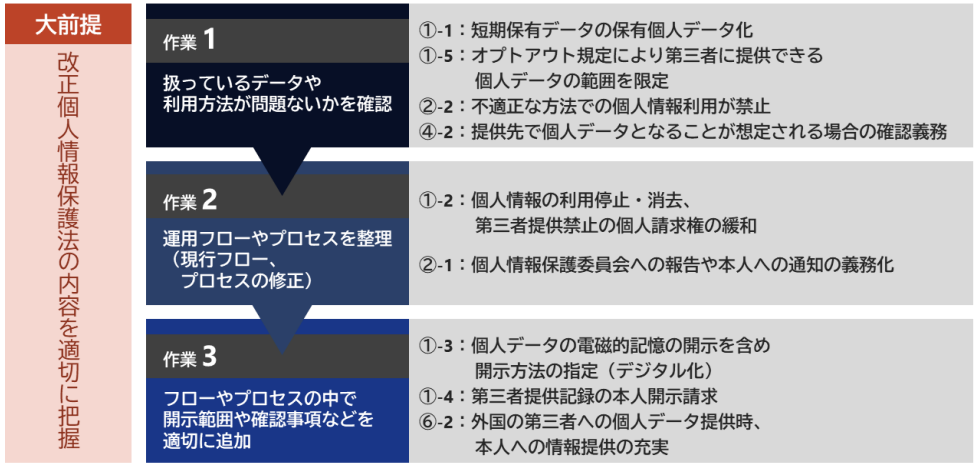


図 3-2 ： 改正部分の対応

現在は問題ない運用フローやプロセスでも、長年見直ししていない状態が続くと、法改正後は、現在の運用フローでは違法となるおそれがでてきます。当然、その内容を把握するには、個人情報保護法は定期的に変更があること念頭に置いて、個人情報保護法の改正を察知して、改正部分を把握すれば対応できます。法改正は頻繁に発生するものではないため、年1回、個人情報保護法の改正などの周知を確認する作業を設ければ、有効です。個人情報保護委員会のWebページには、個人情報保護法の改正点をまとめた中小企業向けのサポートページなどもあります [10]。これらを活用して、個人情報保護法の改正に関する情報を把握することが大切と考えます。また、既に定期的な個人情報保護法の改正の確認体制や個人情報の運用フローの定期的な見直しが実施できている場合は、その範囲をサプライチェーン全体へ広げて、委託先や関連会社の対応状況も確認して、個人情報を取り扱う範囲全てで対応できれば安心です。

3.3. 個人情報保護法の改正と運用の見直しについて

2020年の個人情報保護法の改正以降も、個人情報漏えいが多く発生し、ニュースなどで注目を集めていました。尼崎市によるUSB紛失といった世間を騒がせた事件 [11]や情報銀行などの新しい情報利活用の事例もありました [12]。個人情報保護法は、今後も事件による対応や技術開発の進歩にあわせて改正されていくと考えます。

個人情報をまったく取り扱わない事業者は、存在しません。個人情報に関する運用フローやプロセスなどは、一度作成すればよいというものではありません。なぜなら、今後も個人情報を取り巻く技術および社会が変化して、それに伴って個人情報保護法も対応するために3年ごとに見直すことが必要だからです。

個人情報保護法の改正に合わせて定期的に自社のルールや手順を見直すことはもちろん重要です。さらに個人情報保護法と同様に技術の進歩や社会の情勢により、事業者が個人情報の扱い方をその時代に合った最適なものに見直すことが大切です。

4. 脆弱性『多要素認証の脆弱性を突いたMFA疲労攻撃』

ライドシェアやフードデリバリなどのサービスで有名なUber Technologies Inc.は、2022年9月にセキュリティ侵害を受けたことを発表しました [13]。公式サイトの発表によれば、攻撃者は「多要素認証疲労攻撃」により多要素認証（Multi Factor Authentication。以下「MFA」とします）を突破して社内システムに侵入したと報告しています。

実は近年、複数の大企業が同様の攻撃の被害にあっており、MFAを使用しているから安全安心とは言えない状況になっています。本稿では、MFA疲労攻撃の概要と対策方法について解説します。

4.1. MFAの概要

はじめにMFAを簡単に説明します。MFAを理解されている方は、本節をスキップいただいて問題ありません。

4.1.1. MFAとは

あなたがPCやWebサイトにログインしようとしたとき、システムはログインしようとしている人が本当にあなた本人なのか、他人がなりすましていないかを確認します。これが「認証」であり、一般的に次の3つの要素を使用します。

① 知識。パスワードやPINなど
② 所有物。ICカードやワンタイムパスワード（OTP）発生器など
③ 生体。指紋や静脈、顔など

この中で、さまざまなシステムがもっとも広く使っている要素①のパスワードですが、脆弱なパスワードを使用したり、同じパスワードを使いまわしたりしているため、攻撃者が認証に成功してしまう問題点が指摘されています。とはいえ、要素②の所有物は盗難の恐れがあったり、要素③の生体は誤認識を完全になくせなかったりと、残念ながらリスクがない完璧な認証を実現できる要素はありません。

それなら複数の要素を組み合わせれば安全性が高まるのではないか、ということで生まれた方法がMFAです。つまり、先ほどの3つの要素の内、2つ以上を使用する認証をMFAと言います。要素が2つの場合、二要素認証とも呼びます。また、第1パスワードと第2パスワードのように、同じ要素で2回認証することは二段階認証と呼び、二要素認証とは区別します。

近年、オンラインバンキングではMFAを使った認証が一般的になっており、ポイントサービスのような換金性の高いデータを扱うサービスでも普及が進んでいます。エンタープライズ分野に目を移すと、2021年12月時点でMFAを含む強力な認証機能を有効化しているAzure ADの利用者は、全体の22%であったとの報告があり、普及の途上と言えます [14]。

4.1.2. MFAの方式例

MFAと一口に言っても、認証要素の組み合わせにより多くの方式があります。代表的なMFAを普及した時期が古いMFAから順に表 4-1に並べています。項番1を除けば、かつては項番2か項番3の方式を多く使用していましたが、本稿執筆時点では項番4以降の方式が増加しています。

表 4-1 ： 主なMFAの方式例

項番	要素1	要素2	組み合わせ	備考
1	PIN	ICカード	知識＋所有物	クレジットカードやATM
2	パスワード	OTP発生器	知識＋所有物	
3	パスワード	SMS	知識＋所有物	
4	パスワード	OTPアプリ	知識＋所有物	
5	パスワード	プッシュ通知	知識＋所有物	MFA疲労攻撃の対象
6	秘密鍵	指紋	所有物＋生体	FIDO2の一例

4.2. MFA疲労攻撃の仕組みと事例

認証の安全性を高めるためにMFAは非常に有効です。しかし、MFAも絶対的な安全を保証するわけではありません。本節ではプッシュ通知を利用するMFAを攻撃対象とするMFA疲労攻撃の仕組みを説明し、Uber社を中心に被害事例を紹介します。なお、MFA疲労攻撃は、英語圏ではMFA Fatigue AttackやMFA Bombing Attackと呼ばれることが多いようです。

4.2.1. 攻撃の仕組み

MFA疲労攻撃は、前節の表 4-1の項番5のプッシュ通知を本人に誤って認証させる方法です。MFA疲労攻撃の手順は、下記の通りです。

① 攻撃者は、何らかの方法で被害者のパスワードを入手する
② 攻撃者が、被害者のパスワードを使用してシステムへログインを試みる
③ システムが、被害者へプッシュ通知を送信する
④ 攻撃者は、被害者がログインを許可するまで②③を繰り返す
⑤ 被害者が、誤ってログインを許可する

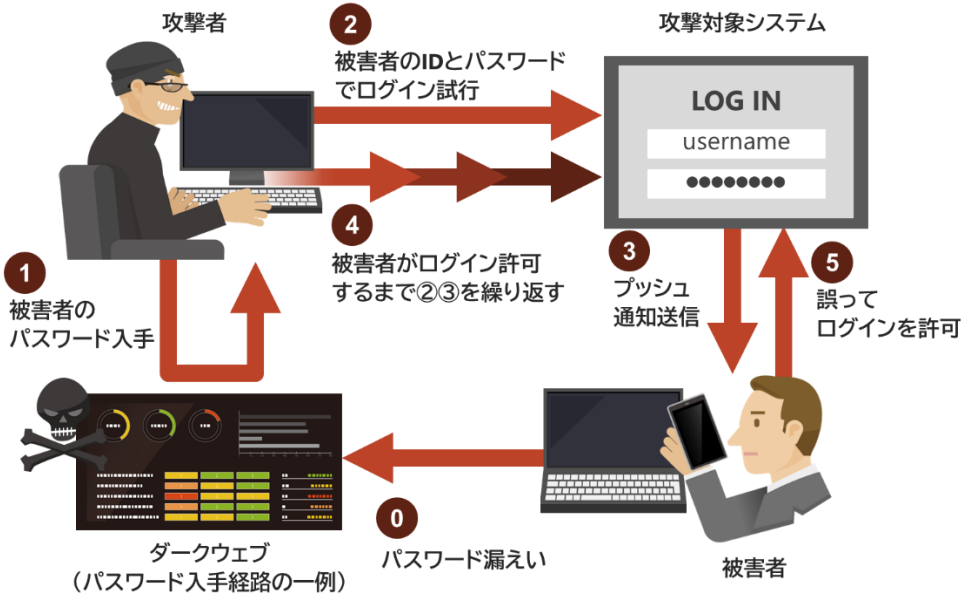


図 4-1 ： MFA疲労攻撃の模式図

MFA疲労攻撃は、執拗にプッシュ通知を送り続けることが名前の由来です。あらためてMFA疲労攻撃の手順を見ると、極めてシンプルな攻撃であることがわかります。被害者は、何度も何度も届くプッシュ通知に対して、いつも認証しているように反射的に許可したり、誤って許可したり、タップ位置がずれて許可したり、通知の嵐に根負けして許可したりすると攻撃者の勝利です。

4.2.2. 攻撃の事例

Uber社が2022年9月19日に発表したMFA疲労攻撃のセキュリティ侵害の内容から、発生した事象をまとめます [13]。

① 攻撃者がUber社の外注業者のアカウントのパスワードを入手した
② 攻撃者が請負業者のパスワードを使用してログインを試みた
③ 請負業者にプッシュ通知が届いたが、しばらくログインを許可しなかった
④ 攻撃者が繰り返しログインを試みた結果、請負業者が許可した
⑤ 攻撃者はUber社の複数の社内システムにアクセスした

①で攻撃者がパスワードを入手した方法は、外注業者のPCへのマルウェア感染によるパスワード流出と、ダークウェブでのパスワード売買であったと推測しています。また一部報道によると、攻撃者は1時間以上にわたってプッシュ通知を送り続けた後、IT部門の人物を装い「通知を止めたいならログインを許可しなければならない」と伝えたそうです [15]。

Uber社の発表によれば、幸い商用サービス用システムには影響がなく、社内システムにも大きな被害はなかったようですが、一歩間違えればサービス停止や個人情報漏えいが発生したおそれが十分にあったと思います。

Uber社以外にも、MicrosoftやCiscoもMFA疲労攻撃の被害を受けたことが報道されています [16] [17] [18]。これら3社の被害は、いずれもサイバー犯罪グループ「Lapsus$」の攻撃によると推測されており、Lapsus$による他のサイバー攻撃もMFA疲労攻撃を使用している確率があります。

4.3. MFA疲労攻撃への対策

本節では、MFA疲労攻撃の対策を技術的対策と組織的・人的対策に分けて解説します。

4.3.1. 技術的対策

前節で説明したように、MFA疲労攻撃はパスワード認証が既に破られていることが攻撃の前提となります。そのため、当然パスワードを守る対策が非常に重要なのですが、これはMFA疲労攻撃に限らないため本稿では割愛します。ただし、万が一MFA疲労攻撃を受けた場合は、パスワードが漏れているため即座にパスワードをリセットしなければなりません。被害者のパスワードはもちろんですが、漏えいの原因や範囲が特定できない状況だと全社員のパスワードリセットも検討してください。

さて、それではMFA疲労攻撃への技術的対策はどうすればよいでしょうか。この対策は2つあります。ひとつはプッシュ通知から他の方式に変更すること、もうひとつはプッシュ通知を改善することです。

まずは、プッシュ通知から他の方式に変更することです。これはMFA疲労攻撃への本質的な対策となります。しかし、ユーザへの操作方法の周知が必要であったり、場合によってはシステムの改修が必要になったりと、時間とコストがかかります。またプッシュ通知は抜群のユーザ体験を提供するため、他の方式に変更するとユーザから不満が生じるおそれがあります。例えば表 4-1の項番4のOTPアプリに変更すると、ユーザは適切なアプリの起動と、6桁の数字入力が求められ、手間が増えてしまいます。今後さらなる普及が見込まれるFIDO2 (WebAuthn)は、MFA疲労攻撃を受けないだけでなく、プッシュ通知やOTPアプリにないフィッシング耐性を持ち、ユーザ体験も良くなっています。利用可能な環境も拡大していますので、検討対象に加えることをおすすめします。

次にプッシュ通知の改善です。MFA疲労攻撃が成立する背景には、攻撃者が

一方的にプッシュ通知を発生させるだけで、ユーザ（被害者）が自身の認証時のプッシュ通知と勘違いしてログインを許可してしまうところに大きな要因があります。そこで、最も有効と思われる対策は、ナンバーマッチングと呼ばれる機能を利用することです [19]。これはログインを試行する側の画面に数字を表示し、プッシュ通知を受けた側の画面でログインを許可する際にその数字を入力させる機能です（図 4-2参照）。ユーザは、攻撃者が発生させたプッシュ通知を受け取っても、入力すべき数字がわからないため、ログインを許可できません。なお本稿執筆時点において、Microsoftは2023年5月8日よりAzure ADの全ユーザへこの機能を自動適用するとしています [20]。Microsoftだけでなく、Okta社のNumber ChallengeやCisco社のVerified Duo Pushなど、他社のサービスでも同様の機能を用意しています。ただし本稿執筆時点で、Number Challengeは表示される3つの数字から選択する形式のため、ユーザが適当に数字を押すと1/3の確率でログインを許可してしまうことをご留意ください。

ナンバーマッチングを利用すればMFA疲労攻撃の成功確率を低減することができますが、プッシュ通知を繰り返し受け取ることは止められません。ナンバーマッチングに加えて、認証失敗が一定回数連続した場合のアカウントロックや、例えばAzure AD Identity ProtectionのようなIDaaSや認証サービスが提供しているセキュリティ機能などのIDの基本的なセキュリティ対策が必要でしょう。

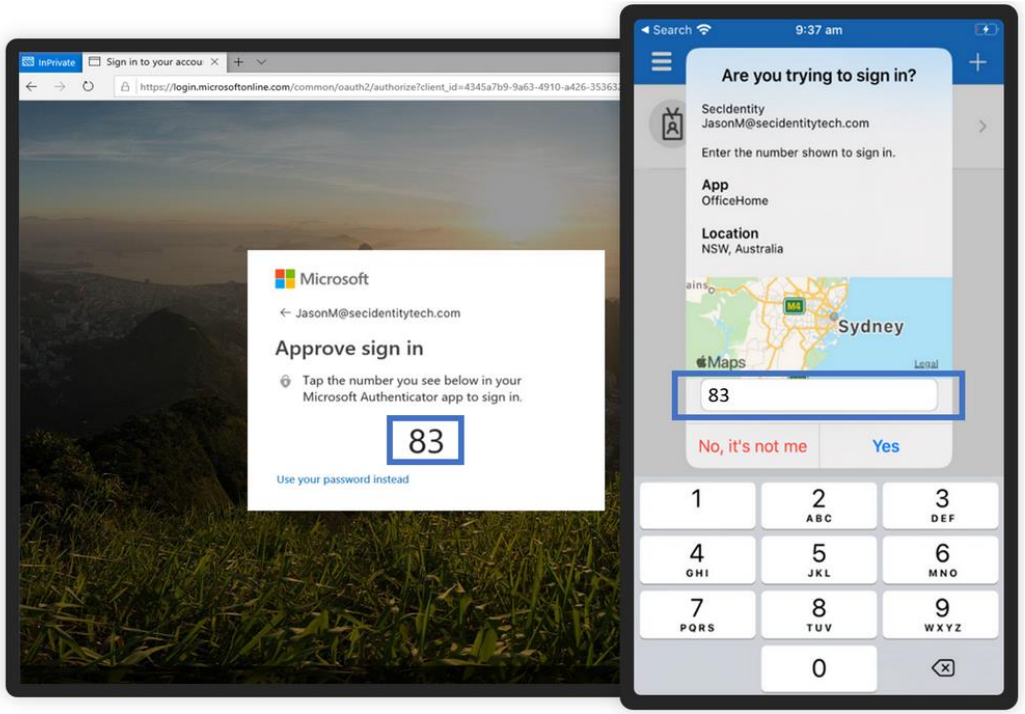


図 4-2 ： ナンバーマッチングの例
（Microsoft社ブログより引用 [21]）

4.3.2. 組織的・人的対策

MFA疲労攻撃が悪用する脆弱性は、人間の注意力や忍耐力、正常性バイアスであり、ソーシャルエンジニアリングに通じるものがあります。従って、ユーザに下記事項を周知徹底することが重要です。

① MFA疲労攻撃という攻撃手法の存在
② 身に覚えのないプッシュ通知は絶対にログイン許可しないこと
③ そのような通知が届いた場合は事前に定めた窓口に通報すること
④ たとえ「システム管理者」等を名乗る人物から許可するよう連絡を受けても鵜呑みにせず、窓口に確認すること

なお、ユーザからMFA疲労攻撃の通報を受けた場合は、ユーザの勘違いでない限り、攻撃者が正しいパスワードを使用して不正にログインを試みています。そのため、システム管理者は直ちに当該ユーザのパスワード変更と、他のユーザで同様の事象が発生していないか、確認してください。

4.4. まとめ

本稿では、MFA疲労攻撃の概要と対策を解説しました。絶対に安全なセキュリティは存在せず、MFAも例外ではありません。プッシュ通知を使用している組織は、MFA疲労攻撃に対する耐性がある方式かどうかを点検しましょう。

本稿の技術的対策の節でも触れた通り、MFA疲労攻撃を受けない認証方式の多くはフィッシング攻撃等に対する脆弱性があるため、現時点でセキュリティに優れた認証方式で、かつ現実的に採用しやすい認証方式はFIDO2 (WebAuthn) であると考えます [22]。MFA疲労攻撃の対策に限らず、今後認証方式を検討する際には、まずFIDO2を第一候補として検討することが多くなるのではないでしょうか。

5. マルウェア・ランサムウェア『Linuxを標的としたマルウェアの感染手法と検知回避技術の高度化』

5.1. Linuxへのマルウェア攻撃

5.1.1. 急増するLinuxへのマルウェア攻撃

2022年度 第2四半期はLinuxを標的としたマルウェア攻撃が増加しています。トレンドマイクロ社によると、2021年の上半期と比較して2022年の上半期は、Linuxシステムを標的とするマルウェアのうち、ランサムウェアの攻撃が約75%増加、暗号通貨をマイニングするマルウェアのマイナーの検知数が約145%増加しています [23]。このことから、Linuxシステムを狙った金銭目的のマルウェアの攻撃が増加していることが分かります。Linuxを標的とした新たなマルウェア自体の発見数も増えています。AV-ATLASのマルウェアの統計データによると、Linuxを標的とした新種のマルウェアの2022年の上半期の数は1,687,755個であり、2021年の上半期の226,324個と比較して、約650%増加しています [24]。一方、Windowsを標的とした新種のマルウェアの2022年の上半期の数は41,435,792個であり、2021年の上半期の72,538,050個と比較して、約43%減少しています [24]。依然として、新種のマルウェアの数自体は、LinuxよりもWindowsの方が多いです。しかし、Windowsの新種のマルウェアの数が減少している一方で、Linuxを標的とした新種のマルウェアの数が増加していることから、攻撃者がLinuxへの攻撃に注力していると予測します。

5.1.2. なぜLinuxが狙われるのか

攻撃者の主な目的は、金銭を得ることです。実際、6.1.1節で述べたように、金銭目的でのマルウェア攻撃が増加しています。攻撃者の視点で考えてみると、企業や組織のクライアントマシン内のデータを窃取、暗号化して脅迫するよりも、企業や組織のファイルサーバやWebサーバといったサーバ内のデータを窃取、暗号化して脅迫をした方が、多くの情報を窃取できたり、大きな社会的影響を及ぼしたりできます。企業や組織へより大きな被害を及ぼせば、身代金を支払う確率や身代金の額を高くできます。そのため、攻撃者はサーバを狙うことが多いと考えます。

サーバのOSは、Unix系/Linux系が多いです。実際、Webサーバで使用しているOSの割合は、Linuxが約38%、Windowsが約20%とLinuxの方が約2倍も多く、Unix系OSも含めると、Webサーバの約80%がUnix系/Linux系OSを利用しています [25] [26]。また、サーバを含む社内インフラをオンプレからクラウドへ移行する企業が増えており [27]、かつPaaSやIaaSにおいてLinuxを選択することが多いことから、今後もサーバのOSはLinuxが占める割合が高いと考えます [28]。

以上のことから、攻撃者はサーバを狙うことが多く、かつ、サーバのOSとしてLinuxを選ぶケースが多いことにより、Linuxを標的としたマルウェア攻撃が増加していると推測します。

5.1.3. Linuxを標的としたマルウェアの高度化

5.1節で述べた通り、Linuxを標的としたマルウェア攻撃が増加しています。そ

れだけではなく、Linuxを標的とするマルウェアが高度化しています。例として、2022年第2四半期に新たに発見したLinuxを標的としたマルウェア「Orbit」と「Shikitega」を紹介します。

5.2. 検知・削除が難しい新種「Orbit」

Orbitは、2022年7月6日にIntezerが発見して発表したLinuxを標的とするマルウェアです [29]。Orbitは、検知と削除を回避する高度な機能を持ち、感染すると痕跡を残さずに情報を窃取されるおそれがあります。特にマシンの再起動後もOrbitが自動的に起動するよう永続化する手法とOrbitの削除を困難にする手法は、従来のマルウェアと異なる高度な手法を用いています。Linuxを標的とするマルウェアの高度化を示すOrbitの動作について、Intezerの分析 [29]を元に見ていきます。

（1） 感染の仕組み

Orbitを永続化するためには、管理者権限が必要です。永続化とは、マシンの再起動後もマルウェアが自動的に起動されるよう設定することです。そのため、Orbitは、ブルートフォース攻撃やソーシャルエンジニアリング攻撃、フィッシング攻撃で管理者権限をもつアカウントで標的のLinuxマシンへ不正にログインします [30]。攻撃者は不正ログインしたあと、以下の流れでOrbitを永続化します（図 5-1）。

① ドロッパーの実行

執筆時点では、どのようにOrbitのドロッパーをマシンにダウンロードするかの情報はありませんが、攻撃者は、まず何らかの方法でドロッパーをLinuxマシン上へダウンロードして、管理者権限で実行します。このとき、攻撃者は、ドロッパーへ引数を設定して、以下のドロッパーの動作を切り替えます。

- マシン再起動後のOrbitの挙動の設定
  - マシン再起動後にOrbitを自動的に起動するよう永続化する
  - もしくは、マシン再起動後にOrbitを削除する
- Orbitのインストール先パスの設定
- Orbitのアンインストール

② 共有ライブラリに悪意のあるコードを追加

ドロッパーは起動すると、攻撃者のサーバから悪意のあるコードをダウンロードします。この悪意のあるコードのファイル形式は、Shared Object（.so）です。Shared Objectは共有ライブラリに用いられるファイル形式で、環境変数への追加や設定ファイルの編集などにより、Shared Objectを共有ライブラリに追加することで、プログラムの実行時に悪意のあるコードのShared Objectをロードすることが出来ます。

③ 永続化

Linuxでは、プログラムが起動するときに、そのプログラムの起動前にプリロードの機能を使って共有ライブラリをロードします。Orbitは、この共有ライブラリのプリロードの機能を使って永続化します。Orbitは、2つの別々のプリロードする方法を使っています。1つ目は、ローダが使用する設定ファイルにOrbitを含んだ共有ライブラリのパスを追加する方法です。2つ目はローダ自体を改ざんして、偽の設定ファイルを経由してOrbitを含んだ共有ライブラリをロードする方法です。つまり悪意のあるコードを共有ライブラリに追加すると、バックドアの設置や情報窃取などの悪意のある動作が可能になるため、Orbitに感染したといえます。

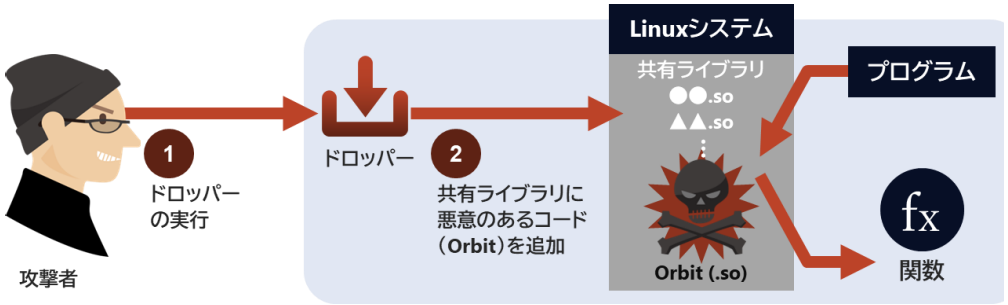


図 5-1 ： Orbitの感染の仕組み

（2） 攻撃機能

① 関数フック

Orbitは、起動したときに、libc、libcap、Pluggable Authentication Module (PAM)の3つのライブラリの特定の関数をフックし、関数の処理を書き換えます。既存のプロセスも新規のプロセスもlibc、libcap、PAMの特定の関数を使用する場合は、Orbitに書き換えられた関数を使用することになります。この関数フックにより、Orbitは、バックドアの設置や情報の窃取といった悪意のある動作を行います。後ほど説明します。

② バックドア

Orbit がPAMライブラリをフックした場合の動作を説明します。PAMライブラリは、ユーザ認証に用いるライブラリです。Orbitは、PAMライブラリの3つの関数pam_open_session、pam_authenticate、pam_acct_mgmtをフックします。pam_authenticateは、ユーザを認証するための関数です。SSHは、認証処理を行うときにpam_authenticateを呼び出します。Orbitは、自身のバイナリファイル内にハードコードしてある攻撃者を認証するためのユーザ名、パスワードと、pam_authenticateを呼び出した時に入力された認証情報が同じ値か否かをチェックします。同じ場合は、あとでログなどからこの通信の痕跡を消せるよう接続に使用するポート番号を記録して、攻撃者とのSSH接続を開始します。Orbitにハードコードしてあるユーザ名、パスワードは、攻撃者だけが知っています。つまり、Orbitは、Orbitが感染したLinuxマシンのSSHへ攻撃者が接続を要求した場合、攻撃者のアカウントが無くても、SSHの接続を許可できます。つまり、攻撃者はSSHをバックドアとして使って、Orbitに感染したLinuxマシンへ不正ログインできます。

③ SSH認証情報の窃取

pam_authenticateを呼び出した時に入力された認証情報が、ハードコードしてあるユーザ名、パスワードと同じでなかった場合、Orbitは、その認証情報を記録し、処理を継続します。Orbitは、感染した端末へSSHでリモートアクセスしたときの認証情報も窃取して、攻撃者へ提供します。

④ ファイル読み書き、プログラム実行のデータ窃取

また、OrbitはSSH認証情報以外の情報も窃取します。Orbitは、2つの関数read、writeをフックして、端末上でプロセスがハードディスクなどへデータを読み書きすると、フックした関数からデータを取得します。この際、ハードコードされたsniff_ssh_sessionフラグを参照し、フラグがfalseの場合は、sudoまたはsshセッションのプロセスで読み書きしたデータのみをログに記録します。フラグがtrueの場合は、呼び出し元のプロセスを検証せずに、書き込まれた全てのデータをログに記録します。さらにOrbitは、プログラムを実行する関数execveもフックして、実行ファイルのフルパスと実行時刻を取得します。フックされた関数execveが終了すると、execveの戻り値を返します。もしも、ユーザがプログラムを実行した時に、戻り値を返さなかったり、想定と異なる値が返ったり

すれば、ユーザが異常に気づく可能性があります。Orbitは、関数フックした関数の正常な戻り値を返すため、ユーザから見たプログラムの挙動は正常で、感染に気づくことが出来ません。つまり、Orbitは、ユーザが気づかないように、プロセスが読み書きしたデータとプログラムの実行結果の情報を窃取します。

⑤ 検知回避（Orbitの関連ファイルの隠蔽）

Orbitは検知されることを回避するために、様々な関数をフックして、処理結果を書き換えることで、ログファイルや実行中のプロセスからOrbitの存在が明らかにならないようにします。このようないくつかあるOrbitの検知回避の機能を見ていきます。

Orbitがreaddir関数をフックして検知を回避する例を説明します。readdir関数は、ディレクトリやファイルの読み取りを行う関数です。Orbitは、readdir関数をフックして、readdir関数の呼び出し元のプロセスのGID値をチェックします。GID値とはグループIDのことであり、ユーザやプロセス、ファイルに紐付いており、グループ毎のアクセス制限に用います。Orbitに関連したディレクトリやファイル、プロセスには、Orbitに関連していることがわかるようにある特定のGID値が設定されています。Orbitに関連するプロセスがreaddir関数を実行したときは、Orbitは、OrbitのGID値を持つプロセスがreaddir関数を実行したことを判定し、readdir関数の戻り値である全てのディレクトリ、ファイル名の一覧を出力します。Orbitに関連しないプロセスがreaddir関数を実行した場合は、OrbitのGID値とは異なるGID値を持つプロセスがreaddir関数を実行したと判定し、readdir関数の戻り値の全てのディレクトリ、ファイル名の一覧からOrbitのGID値を持つ全てのディレクトリ、ファイル名を削除した一覧を出力します。

この例のように、GID値を使ってOrbit以外のプロセスからはOrbitに関する情報が見えないよう関数の挙動を変更して、Orbitの存在が明らかになる情報を隠蔽しています。

⑥ 検知回避（Orbitのプロセスや通信などの動的情報の隠蔽）

readdir関数をフックしてOrbit関連のディレクトリやファイル名を隠すだけでは、システム内の標準的なログファイルなどに残っているOrbitの動作の痕跡から、ユーザがOrbitに気づく可能性があります。そこで、Orbitの動作の痕跡を記録している全てのファイルを隠してしまう方法がありますが、するとこんどは、ユーザから本来存在しているはずの標準的なログファイルなどが見えなくなり、不審に思ったユーザがOrbitに気づく可能性があります。そのためOrbitは、図 5-2のようにOrbitの動作の痕跡を含むファイル自体は隠さず、ファイルの中身からOrbitに関連する情報のみを削除して出力します。具体的には、Orbitはファイルを開く関数であるfopen、open、 open64、openatをフックし、各関数に入力されたファイルがprocファイルシステムの一部であるかどうかをチェックします。procファイルシステムは、システムの実行中のプロセスやメモリ、ハードウェア等に関する様々な情報を格納しており、procファイルシステムにあるファイルを参照すれば、システムのさまざまな情報を得ることが出来ます [31]。入力されたファイルがprocファイルシステムの一部であった場合、Orbitはファイルパスやファイル内容をチェックします。そして、ファイル内にOrbitに関わる情報があった場合は、その情報だけ削除して、残りの情報を出力します。

例えば、Orbitは、TCPのコネクション情報が入っている「/proc/net/tcp」をチェックします。この/proc/net/tcp配下のファイルには、Orbitの設置したバックドアの通信の情報が残る可能性があり、ユーザに見られた場合、ユーザがバックドアの存在に気づく可能性があります。そのため、ユーザが/proc/net/tcp配下のファイルを開いた場合、Orbitはバックドアの痕跡を隠すための処理を行います。具体的には、Orbitは、/proc/net/tcp配下の開いたファイルの内容を1行ずつ読み取り、攻撃者がSSHへ接続した時に記録したポート番号やアドレス情報と比較します。そして、その情報が含まれる行を削除した一時ファイルを作成します。最後にOrbitは、バックドアの痕跡が消えたその一時ファイルの内容

を戻り値としてユーザへ返します。つまり、ユーザがproc/net/tcp配下のファイルを開いたとしても、攻撃者がバックドアを使った痕跡は見つかりません。

ユーザが、procファイルシステム上のCPU使用率やプロセスの状態に関する情報を提供するファイルを開いた場合にも、Orbitは前述と同様の方法で、これらのファイルの出力からOrbitに関係する情報を削除して、Orbitの存在を隠します。

また、プログラムを実行するexecve関数の挙動もOrbitを隠すように変更しています。例えば、ネットワークに関する情報を表示するipやiptablesコマンドを実行した場合、コマンドの出力からOrbitに関する情報を削除して出力します。

以上の⑤⑥の説明のように、Orbitは様々な関数をフックし、ログファイルやコマンドの出力からOrbitに関する情報を削除して、Orbitの存在を隠蔽するため、検知が困難になっています。Intezerがウイルス対策ソフト 60製品でOrbitを検知できるかテストした結果、検知できたウイルス対策ソフトはなかったとのことです。このことからも、Orbitに実装された検知回避技術は非常に高度であると言えます。

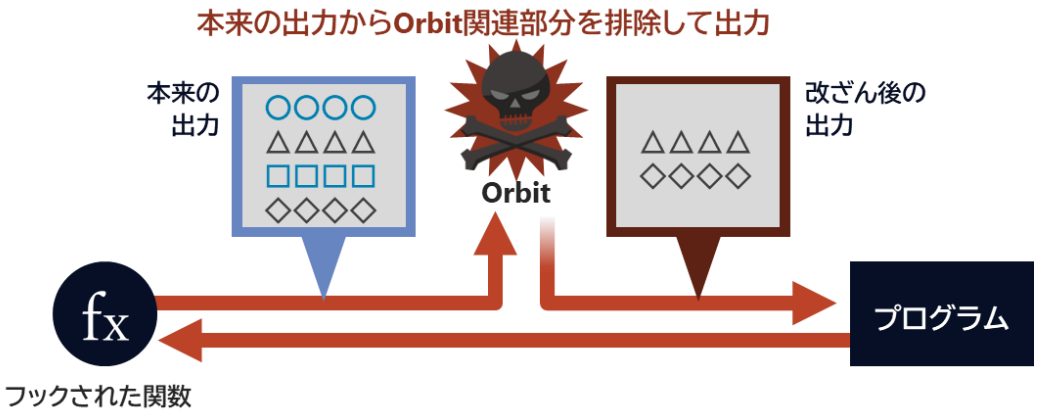


図 5-2 ： Orbitの検知回避手法

（3） 永続化の方法

Orbitは、独自の方法を用いて永続化を行い、削除を困難にしています。マルウェアが共有ライブラリを用いて永続化する通常の方法は、LD_PRELOADという環境変数を使用して他のライブラリに優先してOrbitをプリロードします。Orbitは上記の通常の方法とは異なり、環境変数ではなく、設定ファイルを使用してOrbitをプリロードして永続化を実現しています。Orbitは、（1）感染の仕組みの③永続化で説明したように、2つの独自の方法を用いてOrbitをプリロードしています。1つ目は、ローダが使用する設定ファイルにOrbitを含んだ共有ライブラリのパスを追加する方法です。2つ目はローダ自体を改ざんして、偽の設定ファイルを経由してOrbitを含んだ共有ライブラリをロードする方法です。ここでいうローダとは、Linuxにおいて、プログラムが必要とする共有ライブラリを見つけてロードし、プログラムの実行を準備するプログラムであるld.soおよびld-linux.soを指します [32]。

① 設定ファイルへのパス追加による永続化

図 5-3のように設定ファイル「/etc/ld.so.preload」にOrbitを含んだ共有ライブラリへのパスを追加する方法です。これにより、ローダはOrbitを最初にロードします。更に、すべての新しいプロセスも、Orbitを最初にロードするようになります。

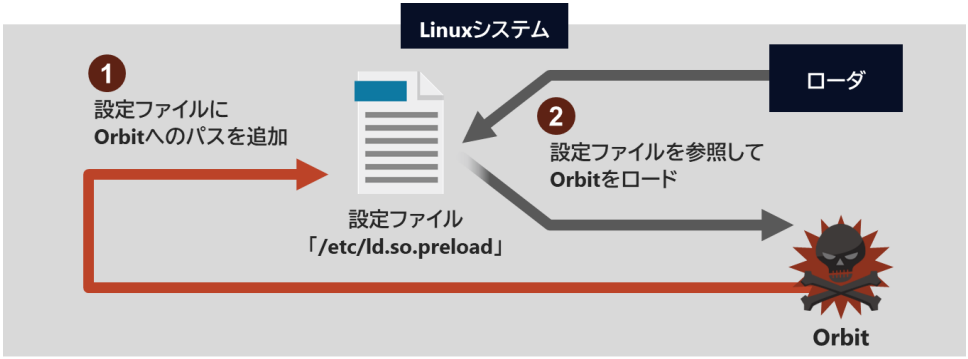


図 5-3 ： 設定ファイルへのパス追加による永続化

② ローダへのパッチ適用による永続化

Orbitはまず、ローダのバイナリファイルのコピーを作成し、パッチを適用できるようにします。そして、コピーしたバイナリファイル内の「/etc/ld.so.preload」という文字列を検索し、その文字列をOrbitが用意した偽の設定ファイルへのパスに置き換えます。この偽の設定ファイルは、Orbitへのパスを含みます。つまり、図 5-4のようにローダにパッチが適用されると、ローダは、本来参照する設定ファイルである「/etc/ld.so.preload」の代わりに、Orbitが用意した偽の設定ファイルを参照してOrbitをロードします。

Orbitの作者は、これらの2つの方法のどちらかが消えてしまった場合に備えて、相互に補い合うように設定しています。例えば、Orbitに感染したLinuxマシンの管理者が、設定ファイル「/etc/ld.so.preload」を削除してOrbitのロードを阻止しようとした場合は、パッチが適用されたローダがOrbitをロードしてしまいます。そして、ロードされたOrbitは、設定ファイル「/etc/ld.so.preload」へOrbitへのパスを再度追加します。一方、管理者が、改ざんされたローダを正規のローダで上書きして、正常なローダへ戻した場合、正常なローダは、Orbitへのパスを追加してある設定ファイル「/etc/ld.so.preload」を使うため、Orbitをロードしてしまいます。そして、ロードされたOrbitは、再度、ローダを改ざんします。

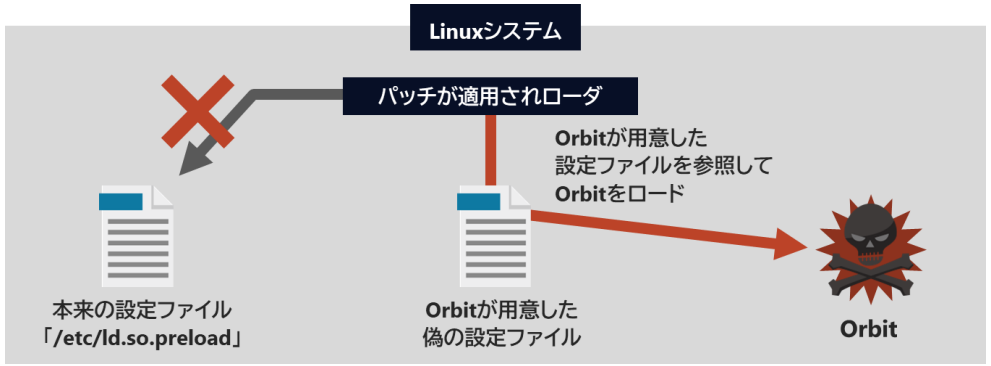


図 5-4 ： ローダへのパッチ適用による永続化

5.3. 検知が難しく、IoTも標的とする新種「Shikitega」

Shikitegaは、2022年9月6日にAT&T Alien Labsが報告したLinuxを標的とするマルウェアです [33]。Linuxを用いたIoTも標的となります。Shikitegaは検知を回避する複数の技術を実装し、感染すると管理者権限を奪取したり、感染したマシンのCPUリソースを暗号通貨のマイニングに使用したりします。Orbitは感染後のマルウェアの活動を検知回避する手法に特徴がありましたが、Shikitegaは感染が成功するまでの間の検知を回避する手法に特徴があります。AT&T Alien Labsの分析 [33]を元にShikitegaの感染の仕組みと検知回避手法を解説します。

（1） 感染の仕組み

Shikitegaは検知を回避するために、Shikitegaの悪意のあるコードの全体が明らかにならないよう徐々に悪意のあるコードをインストールします。図 5-5のように最終的なプログラムのインストールまでを3段階に分けて、3種類のドロッパーを用います。3種類のドロッパーは、それぞれ異なったタスクを担当しています。

① ドロッパー①：Metasploitのダウンロードと実行

Shikitegaの最初のドロッパー①は、370バイト程度の非常に小さなELFファイルです。このドロッパー①は、オープンソースのペネトレーションテストツールであるMetasploitのモジュール Mettleをダウンロードして実行します。Mettleを使用することにより、Webカメラの制御、スニッファ、シェルコードの実行など、幅広い攻撃が可能になります。さらにドロッパー①は、wgetを使用して２段階目のドロッパー②をC&Cサーバからダウンロードします。

② ドロッパー②：管理者権限の奪取

ドロッパー②は、検知を回避するためにMetasploitに含むエンコーダ「Shikata Ga Nai」で暗号化されており、暗号化状態で1キロバイト程度のELFファイルです。ドロッパー②のシェルコードを実行するために、Shikitegaは「Shikata Ga Nai」を用いて、実行可能なシェルコードが出てくるまで復号を繰り返します。このシェルコード

を実行すると、C&Cサーバへ通信を行い、管理者権限を奪取するのに必要な追加のシェルコードとファイルをダウンロードします。追加のシェルコードとファイルは、検知を回避するため、ハードディスク上には保存されずメモリ上へ展開してから実行します。これにより、CVE-2021-4034とCVE-2021-3493の2つのLinuxの脆弱性を悪用して、管理者権限でのコマンドの実行を可能にします。また、ドロッパー②のシェルコードは、ドロッパー③をダウンロードします。

③ ドロッパー③：マイナーの実行と永続化

ドロッパー③も検知を回避するために「Shikata Ga Nai」で暗号化されています。ドロッパー③も実行可能なシェルコードが出てくるまで復号を繰り返します。このドロッパー③のシェルコードを実行すると、C&Cサーバへ通信を行い、暗号通貨のモネロ(Monero)のマイナーであるXMRig minerとその設定ファイルと、その永続化に必要な5つのシェルスクリプト（表 5-1）をダウンロードします。これらのシェルスクリプトとファイルも、同様にメモリ上で実行します。ダウンロードしたXMRig minerを実行して、モネロをマイニングすることで、攻撃者はモネロを得ることが出来ます。XMRig minerは、マシン再起動後も実行されるよう永続化します。永続化は、ダウンロードした5つのシェルスクリプトを実行することで実現します。具体的には、定期的にプログラムを自動実行するcronを設定するコマンドcrontabを実行して、cronの設定ファイルへ以下の4つのプログラムを登録します。

- 感染時にログインしていたユーザの権限で、C&CサーバからXMRig minerと設定ファイルをダウンロードするプログラム
- 感染時にログインしていたユーザの権限で、XMRig minerを実行するプログラム
- 管理者権限でXMRig minerと設定ファイルをダウンロードするプログラム
- 管理者権限でXMRig minerを実行するプログラム

これにより、C&CサーバからXMRig minerと設定ファイルを継続的にダウンロードして実行できます。Linuxマシン上にcrontabコマンドが存在しない場合、Shikitegaはcrontabをインストールします。永続化に成功すると、cronの設定のみで、継続的にモネロのマイニングが出来るため、他のファイルは必要ありません。そのため永続化に成功すると、Shikitegaは痕跡を隠すため、マシンからShikitegaがダウンロードしたすべてのファイルを削除します。

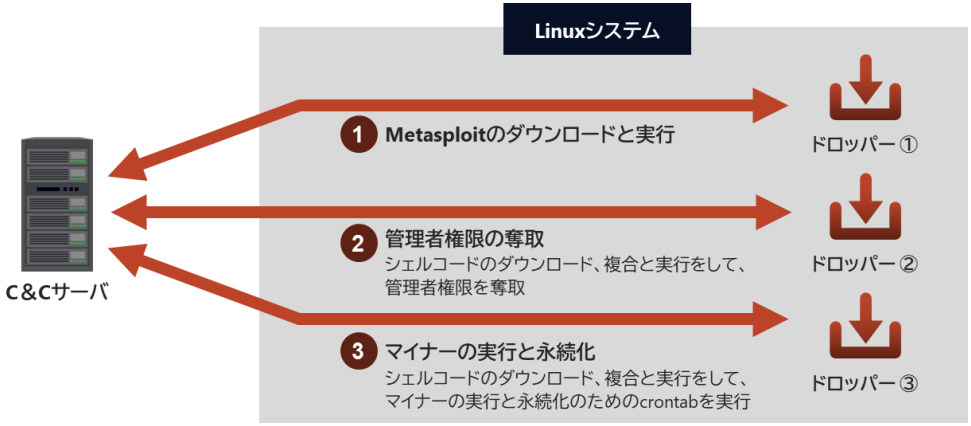


図 5-5 ： Shikitegaの感染の仕組み

表 5-1： 永続化のためのシェルスクリプト

スクリプト名	動作
unix.sh	Linuxマシン上にcrontabコマンドの有無を調査し、存在しない場合はcrontabをインストールします
truct.sh	感染時にログインしていたユーザの権限で、C&CサーバからXMRig minerと設定ファイルをダウンロードするプログラムをcrontabに登録します
brict.sh	感染時にログインしていたユーザの権限で、XMRig minerを実行するプログラムをcrontabに登録します
restrict.sh	管理者権限でXMRig minerと設定ファイルをダウンロードするプログラムをcrontabに登録します
politrict.sh	管理者権限でXMRig minerを実行するプログラムをcrontabに登録します

（2） 検知回避の方法

Shikitegaは、主に以下3つの方法を用いて検知を困難にしています。

① 感染チェーンによるShikitegaのインストール

Shikitegaは、感染のためのプログラムを一度にインストールせず、3回に分けてインストールします。感染チェーンとは、このように感染のためのプログラムを多段階に分けてインストールして実行するする手法のことです [34]。感染チェーンを用いることで、ウイルス対策ソフトのパターンマッチングによる検知を難しくすることが出来ます。例えば、1つのプログラムとして実行した場合は、既知マルウェアのプログラムと特徴が一致してしまいパターンマッチングにより検知されてしまうが、感染チェーンにより複数のプログラムに分けて実

行した場合は、パターンマッチングによる検知を回避できます。さらに、ドロッパーがC&Cサーバからダウンロードしたシェルコードとシェルスクリプトとファイルは、ハードディスクには保存せず、メモリ上へ展開してから実行します。多くのウイルス対策ソフトは、ハードディスク上のファイルを監視しているため、メモリ上で直接実行することで、ウイルス対策ソフトでの検知が難しくなっています。

② ポリモーフィックエンコードによる難読化

Shikitegaは、Metasploitが使用している一般的なエンコーダの1つである「Shikata Ga Nai（仕方がない）」を利用して、シェルコードを難読化することで、ウイルス対策ソフトのパターンマッチングによる検知を困難にしています。具体的には「Shikata Ga Nai」は、ポリモーフィックXOR加法フィードバックエンコーダを使用しています。ポリモーフィックXOR加法フィードバックエンコーダは、一つのシェルコードを複数回に分けて暗号化しており、かつ毎回暗号鍵が異なるため、暗号化後の出力が異なるといった特徴があります [35]。それにより、ウイルス対策ソフトのパターンマッチングによる検知を難しくすることが出来ます。また、シェルコードを難読化することで、静的解析も困難にしています。具体的には、もしShikitegaがドロッパーを削除する前に取得できたとしても、中身は「Shikata Ga Nai」により暗号化されており、復号することが困難なため、スクリプトを静的解析できません。

③ 正規のクラウドサービス上のC&Cサーバ

Shikitegaは、正規のクラウドサービスを用いてC&Cサーバをホスティングしています。また、ShikitegaからC&Cサーバへの通信は、ドメイン名ではなく、直接IPアドレスを使って接続する場合があり、かつ長期間同じIPアドレスを用いないため、有効なIoCの作成が困難になります。以上により、ShikitegaからC&Cサーバへの通信の検知やブロックは、あまり有効に機能しません。

5.4. OrbitとShikitegaへの対策

5.1節で述べた通りLinuxを標的としたマルウェアが増加しており、Linuxもきちんとマルウェア対策しなければなりません。また、5.2節と5.3節で例示したOrbitとShikitegaのように、Linuxを標的としたマルウェア攻撃が高度化しています。そのため、ウイルス対策ソフトの導入やパッチ適用といった一般的な対策だけでは、マルウェア感染を防げないおそれがあります。OrbitとShikitegaの分析結果を踏まえて、以下の３つの対策を提案します。

（１） SELinux の利用

OrbitもShikitegaも、悪意のあるコードの実行には管理者権限が必要だったことから、管理者権限を制限できるSELinuxの利用が効果的な対策と考えます。

（２） 振る舞い検知のできるエンドポイントセキュリティ製品の導入

Shikitegaはポリモーフィックエンコードでシェルコードを難読化してパターンマッチングによる検知を困難にしているため、ウイルス対策ソフトだけでは検知が困難だと考えます。そういったマルウェアの対策として、端末内の情報を監視し、不審な振る舞いをプロセスレベルで検知できるエンドポイントセキュリティ製品の導入を組み合わせることが有効であると考えます。具体的には、NGAV(Next Generation Anti-Virus)やEDR(Endpoint Detection and Response)の中には振る舞い検知ができる製品が存在しています。例えば、振る舞い検知のできるエンドポイントセキュリティ製品を用いれば、共有ライブラリの書き換えやペネトレーションテストツールのMetasploitのダウンロードや実行を異常な挙動として検知して、プロセスをブロックできる可能性があります。

（3） UEBA の導入

Orbitは活動の痕跡が見つからないように出力を改ざんするため、マシン上の情報だけでは検知が困難です。そういったマルウェアへの対策として、感染したマシン以外のログも用いて振る舞い検知するUEBA(User and Entity Behavior Analytics)の導入を組み合わせることが有効と考えます。例えば、上記のEDRの異常検知のアラートとFirewallのログからOribtに感染したマシンから普段はアクセスしないインターネット上の攻撃者のサーバへの通信の検知、ブルートフォース攻撃による認証失敗ログを組み合わせて、Orbitの感染を検知できる可能性があります。

5.5. まとめ

クラウド上サーバやIoT機器などLinuxを狙った金銭目的のマルウェアの攻撃が増加しています。さらにLinuxを標的としたOrbitとShikitegaのような検知が難しい高度なマルウェアが増えています。そのため、Linuxへのマルウェア攻撃にも備えるべきであり、ウイルス対策ソフトの導入やパッチ適用といった、これまでの一般的な対策だけではなく、検知が難しい高度なマルウェアに対抗できる振る舞い検知のできるエンドポイントセキュリティ製品やUEBAの導入とそれらを組み合わせた多層防御が必要になってきました。読者の皆様の組織においても、Linuxを用いたシステムの対策の状況を確認し、このようなマルウェアの攻撃にも備えるべきではないでしょうか。

6. 予測

チャットボットのサイバー犯罪への悪用

2022年の暮れにOpenAIが公開したChatGPTは、瞬く間に世界的な話題となりました。人間とAIのどちらが書いたのか判別困難なほどの性能を誇るこのチャットボットに、サイバー犯罪者も興味を惹かれています。

ダークウェブでは、攻撃者たちがChatGPTを悪用したフィッシングコンテンツの生成や、マルウェアの自動生成に関する意見交換を行っているようです [36]。ChatGPTをはじめとしたチャットボットを使用すれば、比較的スキルが低くてもサイバー攻撃に参加しやすくなり、元々スキルをもっていた攻撃者はより効率的に武器を仕込むことが可能になるでしょう。今後、チャットボットの悪用はサイバー攻撃のバリエーションを増加させると予測します。

一方でサイバー犯罪者だけでなく、防御する側でもAIの活用が拡大すると予測します。これまでもマルウェアや通常と異なるふるまいの検知など、いくつかの分野でAIを活用してきました。しかし、インシデントレスポンスの完全自動化に成功している事例は少なく、たいていのインシデント対応フローには人間の判断ポイントが含まれています。人間が判断を下す際、情報や経験の不足がボトルネックになります。大量の情報を学習し、経験を蓄積し続けるのはAIが得意な領域です。近い将来、人間の判断を支援するための相談相手となるAIが出現するでしょう。さらにその先には、AIがOSINTと組織内のあらゆる情報を分析し続けて、発見したインシデントを一瞬で解決してしまう未来がやってくるかもしれません。24時間365日休みなく、ぶれない判断を下し続けるAIに、人間はどこまで判断を委ねることができるのか、試されることになるでしょう。

医療情報を含んだ要配慮個人情報の漏えい

3章でも取り上げた個人情報保護委員会の2022年度上半期活動実績報告によると報告された漏えいの主な発生原因は、「病院や薬局における要配慮個人情報を含む書類の誤交付及び紛失」と述べています [6]。個人の医療情報は要配慮個人情報となります。つまり医療情報が漏えいした場合は、その情報の重要性から漏えいの理由やデータ数に関係なく個人情報保護委員会へ報告が必要となります。

2023年1月にこうのす共生病院の医師が私用のスマートフォンの動画配信アプリで誤って診察時の音声を配信するという情報漏えい事故が発生しました [37]。個人情報に関する教育やルールの徹底といった対策も重要ですが、人的なミスは無くなることはありません。そのため、根本的に漏えいを防止する対策をとる必要があります。

大企業では会社が業務専用のスマートフォンを提供して、機密情報を扱うエリアでは個人スマートフォンの持ち込みを禁止する対策をとっています。当然、業務専用のスマートフォンには、業務関連の機能やアプリのみをインストールしてあります。MDMなどのデバイス管理技術を用いて、アプリのインストールを制御する対策が一番ですが、ルールによる運用で私用スマートフォンと業務用スマートフォンへインストールするアプリを分けるだけでも、人的なミスは防ぐことが可能です。

しかし、医療現場では、即時性や可用性の観点よりスマートフォンの使用やエリアを限定することが出来ないと予想します。さらに病院や薬局は、中小企業で個人情報に対するシステム的な対応は、コスト面から難しいと考えます。これらの理由より、中小企業や医療機関は、短期間で根本的なスマートフォンの情報漏えい対策を行うことは、難しいと考えます。そのため病院や薬局からの個人情報漏えいは、今後も続いていくと予想します。

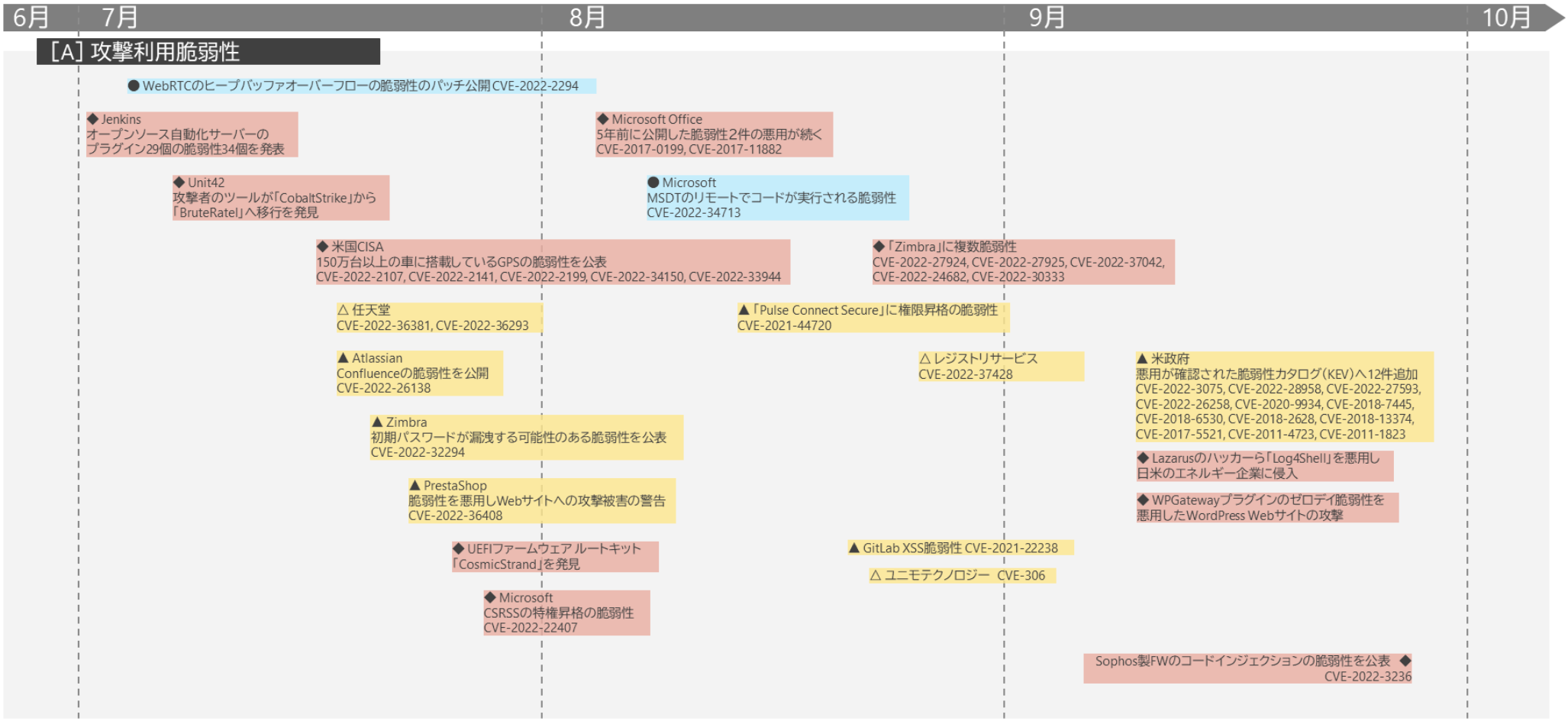
7. タイムライン

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

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策

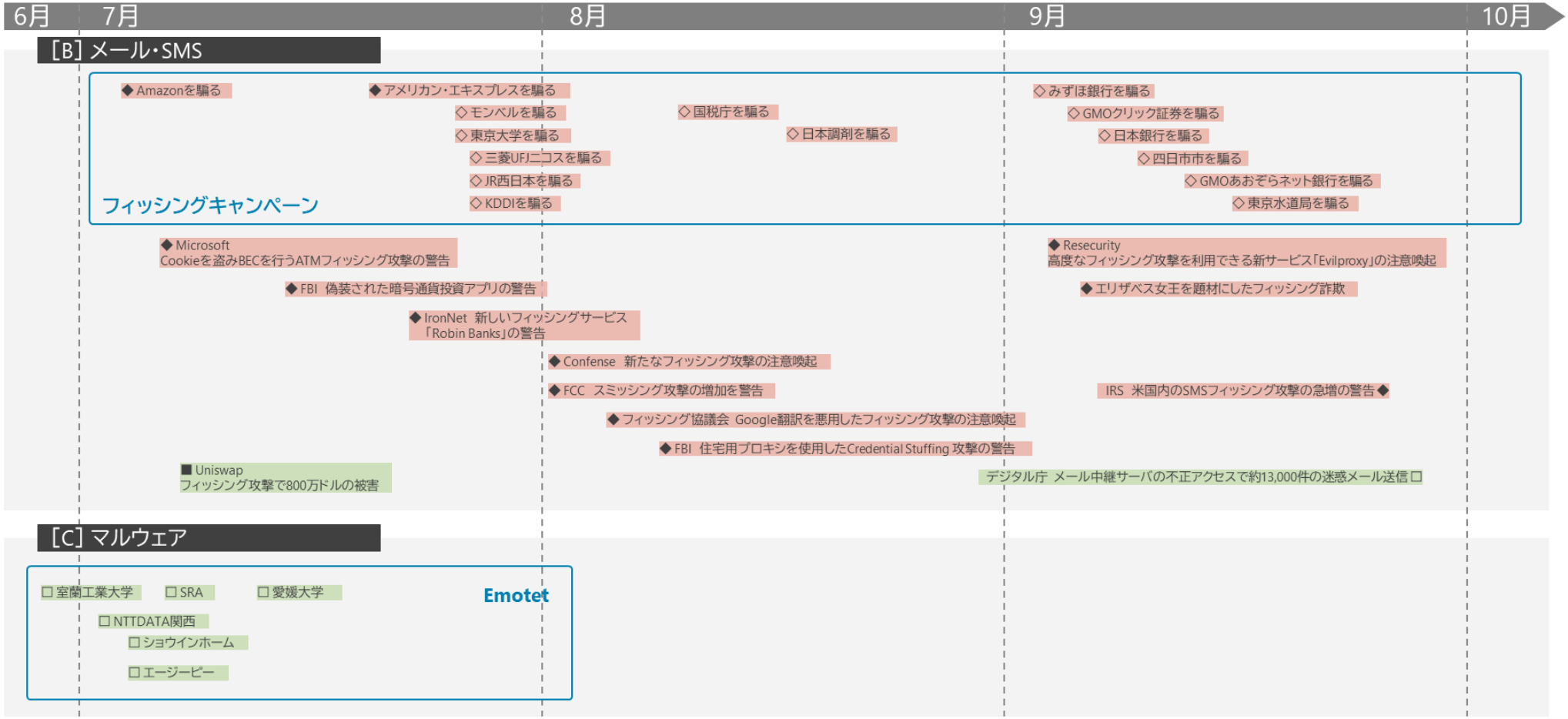


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策

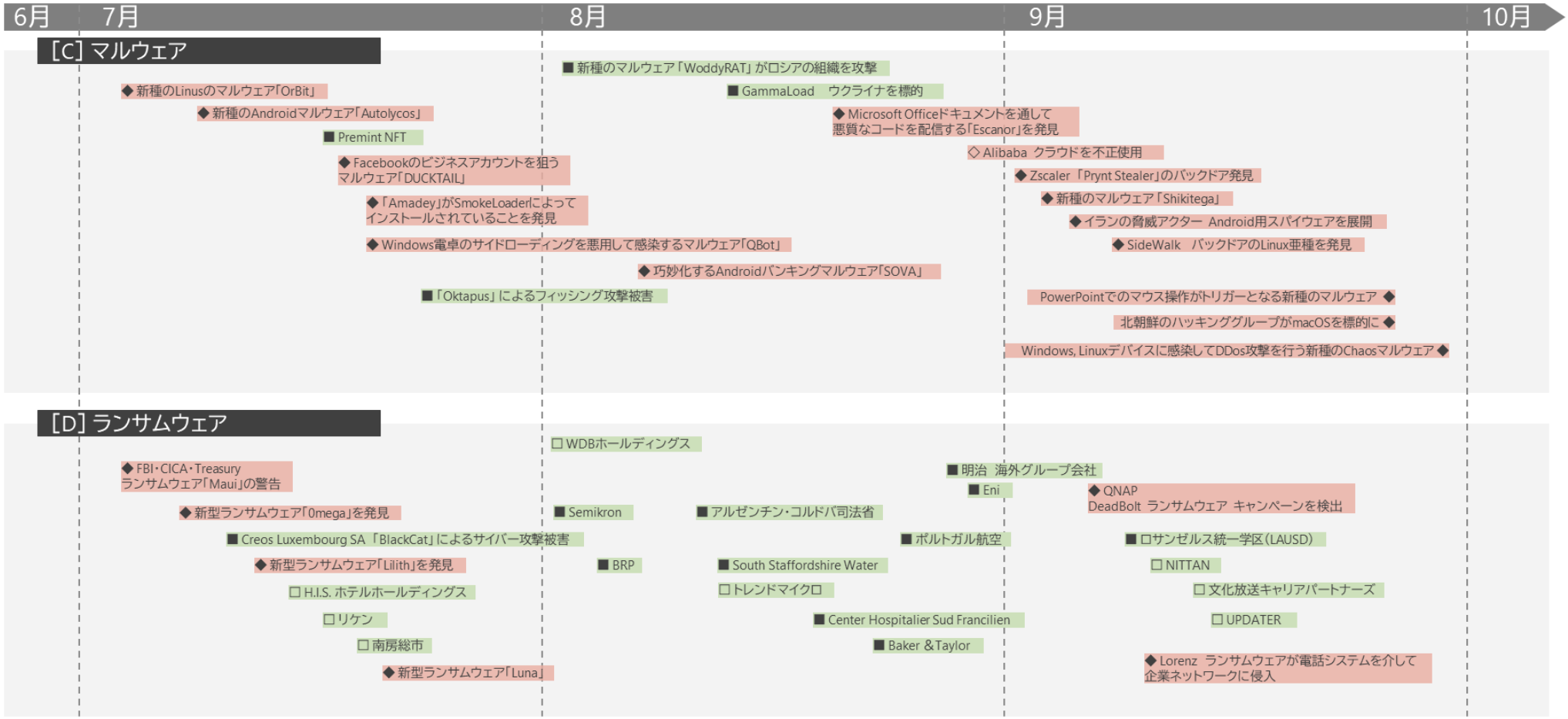


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

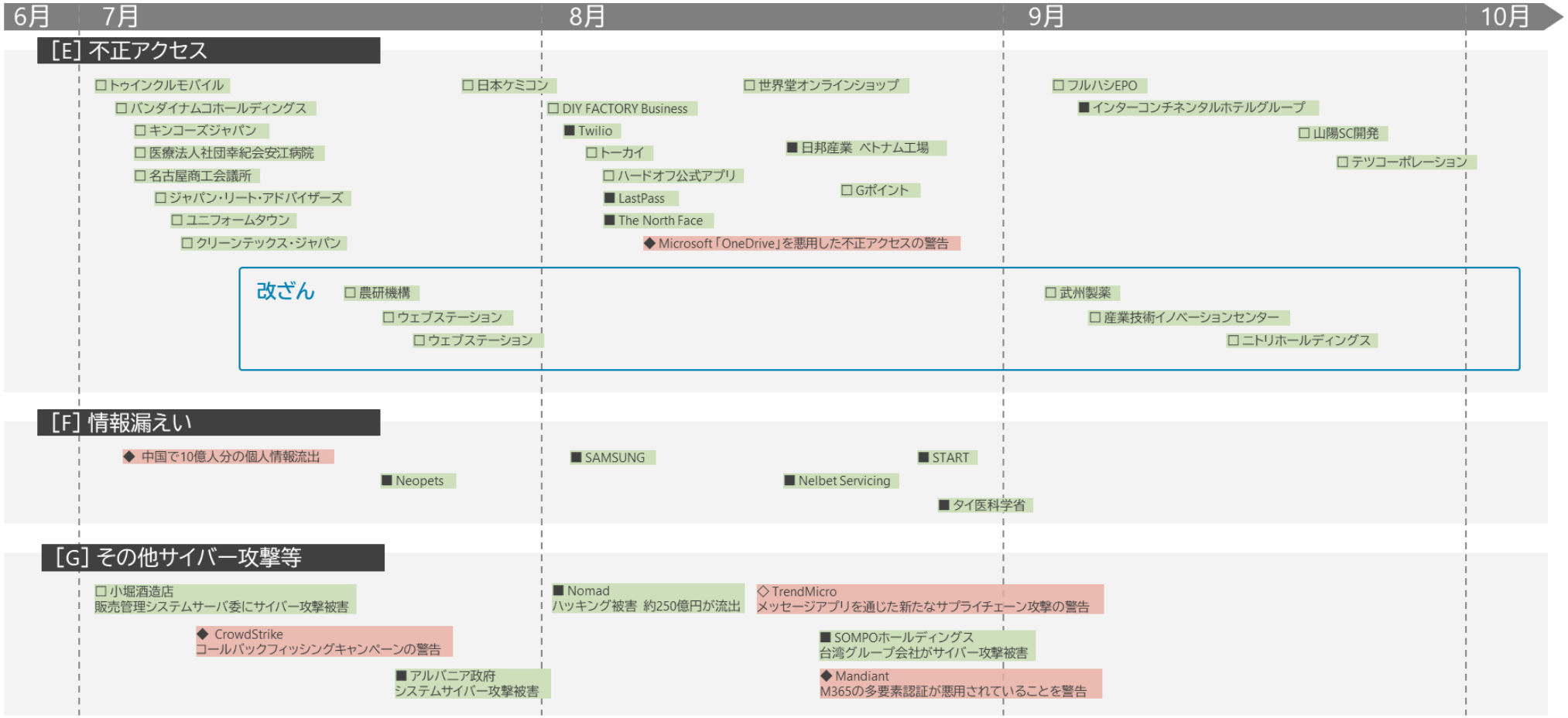
◇◆:脅威
○●:対策



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

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故
◇◆:脅威
○●:対策

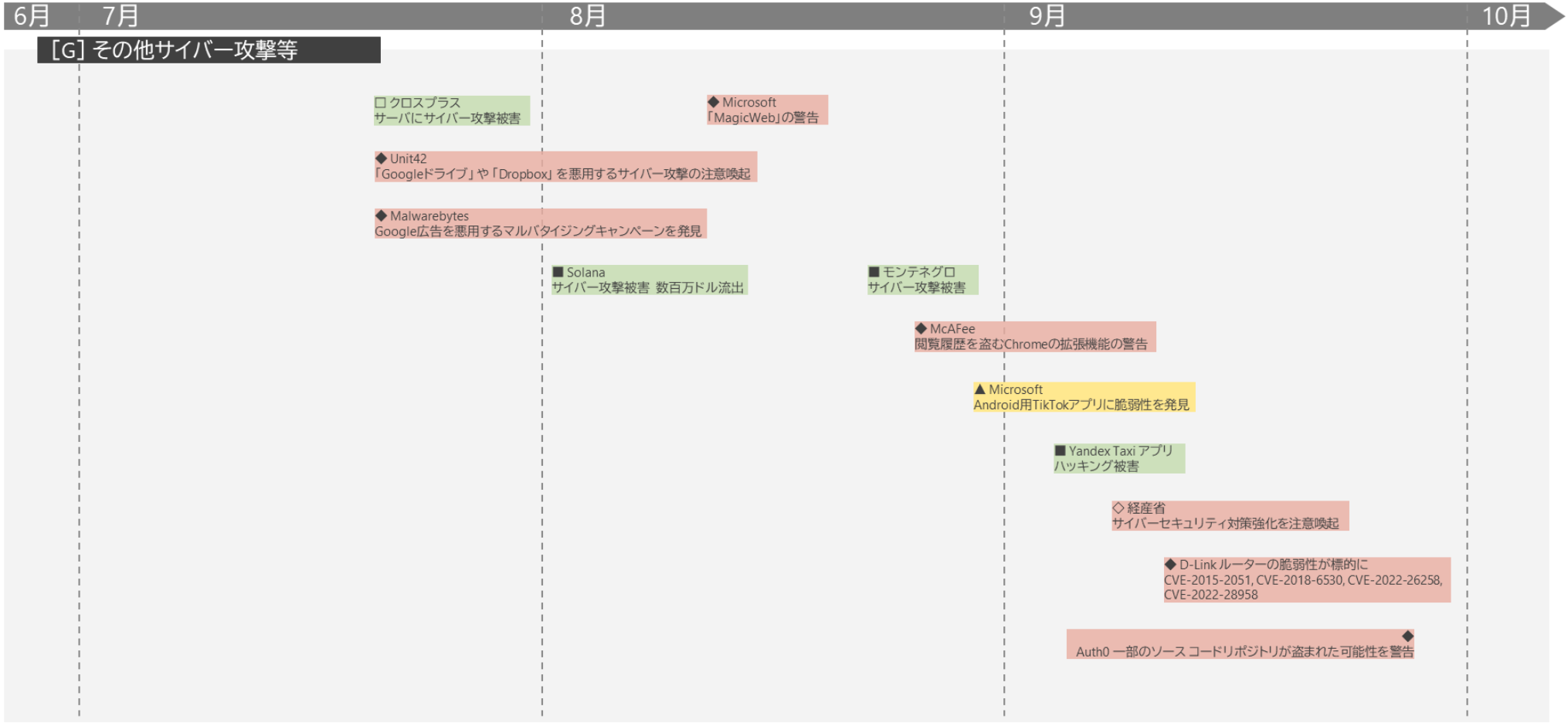


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策



参考文献

[1] 独立行政法人情報処理推進機構, “情報セキュリティ白書2022,” 1 9 2022. [オンライン]. Available: https://www.ipa.go.jp/files/000100474.pdf.

[2] 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）,” [オンライン]. Available: https://www.ppc.go.jp/files/pdf/200612_gaiyou.pdf.

[3] 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（通則編）,” 8 9 2022. [オンライン]. Available: https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a3-5-3.

[4] 個人情報保護委員会, “令和２年改正個人情報保護法概要リーフレット(令和4年2月）,” 4 2022. [オンライン]. Available: https://www.ppc.go.jp/files/pdf/revised_APPI_leaflet2022.pdf.

[5] 株式会社東京商工リサーチ, “個人情報漏えい・紛失事故 2年連続最多を更新 件数は165件、流出・紛失情報は592万人分 ～ 2022年「上場企業の個人情報漏えい・紛失事故」調査 ～,” 19 1 2023. [オンライン]. Available: https://www.tsr-net.co.jp/news/analysis/20230119_01.html.

[6] 個人情報保護委員会, “令和４年度上半期における個人情報保護委員会の活動実績について,” 9 11 2022. [オンライン]. Available: https://www.ppc.go.jp/files/pdf/R4_kamihanki.pdf.

[7] 個人情報保護委員会, “中小規模事業者の安全管理措置に関する実態調査,” 27 6 2022. [オンライン]. Available: https://www.ppc.go.jp/files/pdf/R3_chuushou_anzenkanri_analysisreport.pdf.

[8] 中小企業庁, “2021年版 中小企業白書（HTML版） 第1部 令和2年度（2020年度）の中小企業の動向 第2章 中小企業・小規模事業者の実態 第1節 多様な中小企業・小規模事業者,” [オンライン]. Available: https://www.chusho.meti.go.jp/pamflet/hakusyo/2021/chusho/b1_2_1.html.

[9] 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年度第4四半期,” 18 6 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2020_4q_securityreport.pdf.

[10] 個人情報保護委員会, “中小企業の皆様（中小企業サポートページ）,” [オンライン]. Available: https://www.ppc.go.jp/purpose/SMEs/.

[11] 尼崎市, “個人情報を含むUSBメモリーの紛失事案について,” 28 12 2022. [オンライン]. Available: https://www.city.amagasaki.hyogo.jp/kurashi/seikatusien/1027475/1030947.html.

[12] 斎藤健二（ITmedia），“三菱UFJ信託が情報銀行事業開始　Dprimeで「お金の代わりに個人情報を預かる」,” 1 7 2021. [オンライン]. Available: https://www.itmedia.co.jp/business/articles/2107/01/news126.html.

[13] Uber Technologies Inc., “Security update | Uber Newsroom,” 16 9 2022. [オンライン]. Available: https://www.uber.com/newsroom/security-update/.

[14] Microsoft Corporation, “Cyber Signals: Defending against cyber threats with the latest research, insights, and trends - Microsoft Security Blog,” 3 2 2022. [オンライン]. Available: https://www.microsoft.com/en-us/security/blog/2022/02/03/cyber-signals-defending-against-cyber-threats-with-the-latest-research-insights-and-trends/.

[15] IDG Communications, Inc., “Multi-factor authentication fatigue attacks are on the rise: How to defend against them | CSO Online,” 22 9 2022. [オンライン]. Available: https://www.csoonline.com/article/3674156/multi-factor-authentication-fatigue-attacks-are-on-the-rise-how-to-defend-against-them.html.

[16] Built In Inc., “MFA Fatigue: What It Is and How to Avoid It | Built In,” 3 11 2022. [オンライン]. Available: https://builtin.com/cybersecurity/mfa-fatigue.

[17] Microsoft Corporation, “DEV-0537 criminal actor targeting organizations for data exfiltration and destruction - Microsoft Security Blog,” 22 3 2022. [オンライン]. Available: https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/.

[18] Cisco Systems, Inc., “Cisco Talos shares insights related to recent cyber attack on Cisco,” 10 10 2022. [オンライン]. Available: https://blog.talosintelligence.com/recent-cyber-attack/.

[19] CISA (Cybersecurity & Infrastructure Security Agency), “Implementing Number Matching in MFA Applications,” 10 2022. [オンライン]. Available: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implement-number-matching-in-mfa-applications-508c.pdf.

[20] Microsoft Corporation, “Use number matching in multifactor authentication (MFA) notifications - Azure Active Directory - Microsoft Entra | Microsoft Learn,” 22 1 2023. [オンライン]. Available: https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match.

[21] Microsoft Corporation, “Defend your users from MFA fatigue attacks - Microsoft Community Hub,” 28 9 2022. [オンライン]. Available: https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/defend-your-users-from-mfa-fatigue-attacks/ba-p/2365677.

[22] CISA (Cybersecurity & Infrastructure Security Agency), “Implementing Phishing-Resistant MFA,” 10 2022. [オンライン]. Available: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

[23] Research, Trend Micro, “Defending the Expanding Attack Surface: Trend Micro 2022 Midyear Cybersecurity Report,” 31 8 2022. [オンライン]. Available: https://documents.trendmicro.com/assets/rpt/rpt-defending-the-expanding-attack-surface-trend-micro-2022-midyear-cybersecurity-report.pdf.

[24] AV-TEST, “AV-ATLAS - Malware & PUA,” 2022. [オンライン]. Available: https://portal.av-atlas.org/malware/statistics.

[25] Q-Success, “Usage Statistics and Market Share of Operating Systems for Websites, December 2022,” 16 12 2022. [オンライン]. Available: https://w3techs.com/technologies/overview/operating_system.

[26] Q-Success, “Usage Statistics and Market Share of Unix for Websites, December 2022,” 16 12 2022. [オンライン]. Available: https://w3techs.com/technologies/details/os-unix.

[27] ITmedia Inc., “日本企業の約4割がSaaS利用　ガートナー「クラウドは普及・拡大フェーズ」 - ITmedia NEWS,” 14 6 2021. [オンライン]. Available: https://www.itmedia.co.jp/news/articles/2106/14/news132.html.

[28] IBM, “IBM Security X-Force脅威インテリジェンス・インデックス | IBM,” 2 2022. [オンライン]. Available: https://www.ibm.com/reports/threat-intelligence/jp-ja/.

[29] Intezer, “OrBit: New Undetected Linux Threat Uses Unique Hijack of Execution Flow,” 6 7 2022. [オンライン]. Available: https://www.intezer.com/blog/incident-response/orbit-new-undetected-linux-threat/.

[30] Atlantic.Net, “OrBit Malware and Linux | What Is OrBit Malware? | Atlantic.Net,” 20 9 2022. [オンライン]. Available: https://www.atlantic.net/dedicated-server-hosting/orbit-malware-and-linux/.

[31] Red Hat, Inc., “2.3. /proc 仮想ファイルシステム Red Hat Enterprise Linux 7 | Red Hat Customer Portal,” 2022. [オンライン]. Available: https://access.redhat.com/documentation/ja-jp/red_hat_enterprise_linux/7/html/storage_administration_guide/proc-virt-fs.

[32] Linux man-pages project, “ld.so(8) - Linux manual page,” 18 12 2022. [オンライン]. Available: https://man7.org/linux/man-pages/man8/ld.so.8.html.

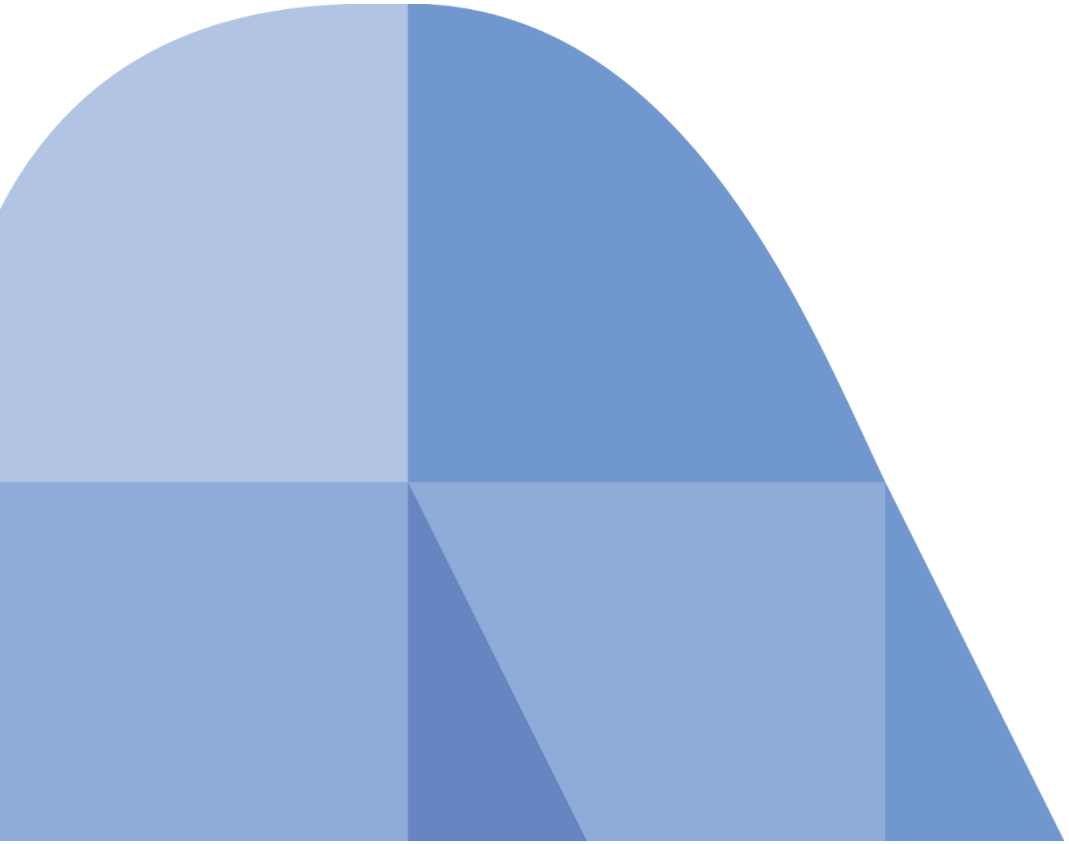
[33] AT&T Alien Labs, “Shikitega - New stealthy malware targeting Linux | AT&T Alien Labs,” 6 9 2022. [オンライン]. Available: https://cybersecurity.att.com/blogs/labs-research/shikitega-new-stealthy-malware-targeting-linux.

[34] Kaspersky, “What is an infection chain? | Kaspersky IT Encyclopedia,” [オンライン]. Available: https://encyclopedia.kaspersky.com/glossary/infection-chain/.

[35] Mandiant, “Shikata Ga Nai Encoder Still Going Strong | Mandiant,” 21 10 2019. [オンライン]. Available: https://www.mandiant.com/resources/blog/shikata-ga-nai-encoder-still-going-strong.

[36] Check Point Software Technologies LTD., “OPWNAI : Cybercriminals Starting to Use ChatGPT - Check Point Research,” 6 1 2023. [オンライン]. Available: https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/.

[37] 医療法人社団鴻愛会　こうのす共生病院, 16 1 2023. [オンライン]. Available: https://kouaikai.jp/category/notice/.



2023年3月30日発行

株式会社NTTデータ
サイバーセキュリティ技術部
大谷 尚通
松尾 俊彦 / 和光 裕希 / 瀧田 浩平 / 堰根 哲平 / 松原 諒之
nttdata-cert@kits.nttdata.co.jp