NTT DATA
Trusted Global Innovator

グローバルセキュリティ動向四半期レポート

2021 年度 第 3 四半期

NTT DATA
Trusted Global Innovator

目次

1.エグゼグティブサマリー

本レポートは、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。

Apache Log4jの深刻な脆弱性「Log4Shell」

2021年12月にApache Log4jの脆弱性、Log4Shell(CVE-2021-44228)の情報が公開されました。Log4jがJava系のシステムにおいて広く採用されているライブラリであること、また脆弱性の深刻度を示す指標であるCVSSスコアが最も深刻な10.0であったことから、非常に大きな話題となりました。Log4jの脆弱性の影響を受けるシステムを一つも漏れなく対策することは困難であり、今後も被害報告が後を絶たないと予想されます。

Log4Shellのように影響の大きなソフトウェアやライブラリの脆弱性に備え、システムの運用者はソフトウェアサプライチェーンを意識した構成の管理を行う必要があります。その手法の一つとして、ソフトウェア部品管理表(SBOM)の作成・運用について紹介します。

最低限のセキュリティベースライン「Minimum Viable Security Product （MVSP）」策定

GoogleやSalesforceを中心に、ベンダ中立的な最低限のセキュリティベースライン「Minimum Viable Security Product （以下、「MVSP」とする）」が策定されました。MVSPは、BtoBのソフトウェアやビジネス・プロセスのアウトソーシングサービスを提供する企業が実装すべき必要最低限のセキュリティ要件です。サプライチェーン攻撃が活発化し、サプライチェーン全体のリスク評価の重要性が高まる一方で、リスク評価プロセスは複雑で時間がかかり、評価する側／される側の双方にとって負担が大きいという課題があります。MVSPはこの課題を解決するために開発され、許容できる最低限のセキュリティ要件に絞った簡素なチェックリストとなっています。解釈の曖昧性を排除するために、セキュリティ対策の実装方法や基準、対策の重要性が明確に示されています。MVSPを契約時や定期的な委託先のリスク評価やRFPのセキュリティ要件として活用することで、審査プロセスを簡素化できるでしょう。MVSPはあくまで最低限のセキュリティ要件のため、場合によっては要件を追加するなどカスタマイズが必要な点には注意が必要です。今後採用する企業が増えれば、MVSPはデファクトスタンダードとなる可能性もあります。

ZohoのUEM製品に発生した脆弱性

Zoho社のManageEngine関連製品は、マシンへエージェントをインストールして、システム管理者が遠隔から、社員の端末やサーバを遠隔から管理できる統合エンドポイント管理（UEM）製品です。このManageEngine関連製品のエージェントへ接続して遠隔管理するときに、認証をバイパスできてしまう脆弱性がありました。APT攻撃グループが、この脆弱性を悪用してゼロデイ攻撃を行いました。攻撃者がUEM製品を乗っ取ってしまうと、自社の情報や資産を守るための製品が、攻撃者を手助けする製品へと様変わりします。UEM製品のような大量のマシンを統合して集中管理するソフトウェアは、より強固にセキュリティ対策を行って、攻撃者が悪用しないように守らなければなりません。

EMOTET攻撃活動を再開

2021年1月にテイクダウンしたはずのEMOTETが、2021年11月14日頃から攻撃活動を再開しました。テイクダウン前にEMOTETを使っていたランサムウェアContiの攻撃グループが、ランサムウェア攻撃活動を再開するために、TrickBot / Qbotの攻撃グループを使ってEMOTETのボットネットを再構築しました。その結果、Contiの攻撃グループとTrickBot / Qbotの攻撃グループが、再構築したEMOTETのボットネットを使って、ランサムウェア攻撃活動を再開しています。

攻撃活動再開後のEMOTETは、感染手法が変化しており、人的対策だけでは感染防止が難しくなっています。そのため、個人のセキュリティ意識に頼らず、EMOTETに関するIoC（Indicator of Compromise）情報を迅速に入手して、FirewallやSIEMなどのセキュリティ機器へ適用して、システムでEMOTET感染を未然に防止したり、早期検知したりするべきです。

予測

米国財務省外国資産管理局（OFAC）や警察が身代金の支払いを規制する命令を告示して、ランサムウェア攻撃グループへ身代金を支払わない組織が増えてきました。そのため、ランサムウェア攻撃グループは、身代金要求以外で収益を確保する手段へシフトしていくと予測します。今後、ランサムウェア攻撃グループが、詐取した情報の販売など身代金要求以外のサブプランを用意することや、あるいはセキュリティ対策の裏をかいた新たな収益モデルの攻撃手段を開発する可能性も十分に考えられます。今は、その過渡期にあるといえるでしょう。

一方で、身代金を支払わない組織が無くなっているわけではありません。その一因として、身代金に対応したサイバー保険に加入している組織が、早く、かつ安く解決できるため、身代金の支払いを選択することです。しかしながら、サイバー攻撃が増加している米国のサイバー保険会社のTOP10のうち4社が赤字であり、このまま赤字が拡大すれば、保険会社は、ランサムウェアに関わる身代金の保険金支払いの特約をやめてしまうかもしれません。その場合、身代金の支払いが減ると予測し、減る場合にはランサムウェア攻撃も減少する可能性

があります。

　また、コロナ禍でのリモートワークの増加により、社外からインターネット経由で社内システムへVPN接続したりクラウドサービスを利用したりする機会が増加し、社内システムに侵入することを目的としたフィッシング攻撃が一般化しています。フィッシング攻撃に必要な作業をas-a-Serviceで提供するビジネスであるPhishing as a Service（PHaaS）が存在しており、PHaaSビジネスが活性化すればするほど、フィッシング被害も拡大していくと推測します。

2.注目トピック

2.1. Apache Log4jの深刻な脆弱性「Log4Shell」

2.1.1. Log4Shellとは

The Apache Software Foundationは、2021年12月に脆弱性CVE-2021-44228を公開しました [1]。CVE-2021-44228は、Javaのライブラリであるlog4jに存在する脆弱性で、「Log4Shell」という通称で呼ばれます。Log4jが動作するシステム上で、リモートから任意のコードが実行可能であり、実行難易度が低く、悪用が非常に容易な脆弱性です。脆弱性の深刻度を示す指標であるCVSSスコアも、最も深刻な10.0でした。

また、Log4jがJava系のシステムにおいて広く採用されていることも、事態の深刻さに拍車をかけています。Googleが調査した結果 [2]、Maven Central Repository1に存在する35,000個以上のライブラリが脆弱性を含むLog4jに依存していることが明らかになりました。The Apache Software Foundationは、2022年1月に脆弱性を対策したバージョン Log4j 2.15を既にリリースしていますが、Log4jに依存するライブラリもLog4j 2.15を取り込んだバージョンへ修正が必要です。また、ライブラリ同士も複雑に依存しあっており、Log4jを含んだ他のライブラリの修正後でないと、自身のライブラリの修正に着手できない、といった状況も発生しています。図 2-1のように、Log4jを含んだ脆弱な下位のライブラリの修正待ちが発生しています。

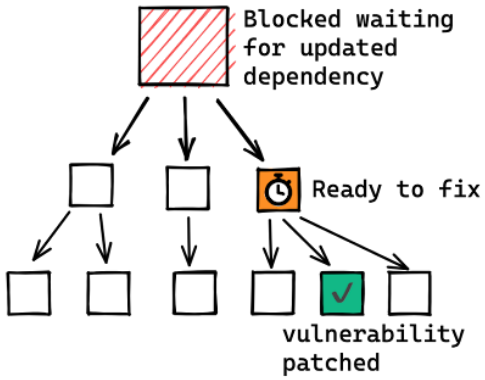


図 2-1 ： ライブラリの依存関係の概念図(Google Security Blogより引用

[1] Javaのライブラリが公開されているサイトの一つ。多数のライブラリが公開されており、Javaの開発者はここから必要なライブラリをダウンロードして利用する。運営はThe Apache Software Foundation。

[2])

Maven Central Repository上に存在するLog4jに依存した全てのライブラリを修正するだけでも、短期間での対応は困難だと言われています。また、前述のLog4jに依存したライブラリを利用しているJavaのシステム群にまで影響調査の範囲を広げると、もっと大量のシステムが影響を受けています。Log4jの脆弱性の影響を受けるシステムを一つも漏れなく対策することは、非常に困難です。今後、どこかのライブラリやシステムに脆弱性 Log4Shellが残っていて、世界のどこかで被害が発生すると予想します。

2.1.2. 脆弱性のメカニズム、回避策

（１） 脆弱性のメカニズム

Log4jはシステムのログを出力するためのライブラリです。Log4jには、システム外部のオブジェクトやリソースを参照するためのJNDI Lookupという機能を実装しています。このJNDI Lookup機能は、特定の書式を使って外部のオブジェクト参照先を指定して、そのオブジェクトを読み込むことができます。Log4jは、ログにこの特定の書式と同じ文字列が含まれている場合に、JNDI Lookup機能がその文字列の指示にしたがって、外部のオブジェクトやリソースを参照する脆弱な実装になっていました。

攻撃者は、このJNDI Lookup機能の脆弱な実装を悪用して、標的のシステムを攻撃者が用意したサーバへアクセスさせて、標的のシステムが外部のオブジェクトを参照するように仕向け、その結果システム上で任意のJavaオブジェクトを実行させることが可能でした。また、このJNDI Lookupが初期状態で有効な設定になっていたため、Log4jを利用するシステムの多くが対策を迫られる事態となりました。

攻撃の前提として、攻撃者がシステムのログの出力内容に干渉する必要がありますが、多くの場合これはあまり難しいことではありません。例えばWebサーバの場合では、アクセスしてきたユーザの"User-Agent"というパラメータをログに出力する事が一般的ですが、この"User-Agent"は攻撃者が自由に指定することが可能です。

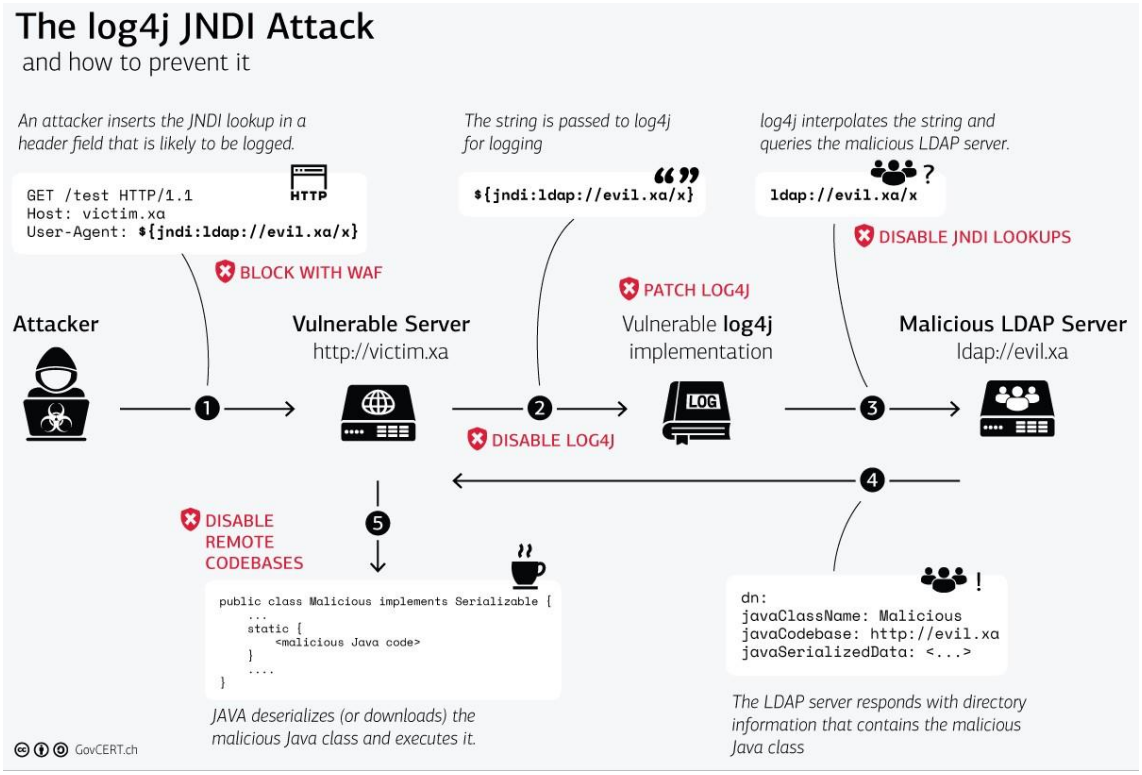


図 2-2 ： LDAPを介した攻撃例(GovCERT.chの解説ページより引用 [3])

図 2-2ではLDAPを介して、攻撃者がリモートから任意のJavaのコードを実行する流れを示します。

1. 攻撃者は、HTTP通信のクライアント環境の"User-Agent"へ、攻撃者が用意したLDAPサーバのアドレス情報を設定します。
2. 攻撃者が、攻撃対象のWebサーバにアクセスすると、Webサーバがこのアクセスに関連するログを記録します。このとき、アクセス元のクライアント環境の"User-Agent"情報をログへ出力する仕様になっていた場合、上記の攻撃者が設定したLDAPサーバのアドレス情報をそのままログへ出力します。
3. JNDI書式のLDAPサーバのアドレス情報をログへ出力する時、Log4jのJNDI Lookup機能がデフォルトで有効になっているため、同機能がログ上のJNDI書式を解釈してLDAPサーバのアドレス情報を抽出します。
4. Log4jは、取得したアドレスのLDAPサーバへ問い合わせを行います。
5. LDAPサーバから、別のサーバのアドレス情報が返ってきます。
6. 上記の返ってきたアドレス情報のサーバへアクセスして、悪意のあるコードをダウンロードして実行します。

（2） 脆弱性の対応策

下記の①の本格対策の実施してください。①の実施が難しい場合は、②の暫定対策を実施

してください。

① 本格対策 - Log4jのバージョンアップ

脆弱性CVE-2021-44228を修正済みのLog4jへバージョンアップしてください。修正済みバージョンは表 2-1に示す通りです。Java 6系と7系は、ベンダのサポートが終了しているため、可能な限りJava 8系以降へ切り替えてください。

表 2-1 ： 修正済みLog4jのバージョン (2022.1時点)

Javaバージョン	修正済みLog4jバージョン
6系	2.3.2以降
7系	2.12.4以降
8系	2.16.0以降

② 暫定対策 - JNDI Lookup機能の無効化

バージョンアップが難しい場合、JNDI Lookup機能の無効化を検討してください。具体的には、JNDI Lookupクラスをクラスパスから除外します [4]。上記に挙げた対策の他に、システムから外部へのアクセスを制限することも有効な対策です [4]。ただしDNSを使用するシステムの場合は、DNSのアクセスを制限することはできません。

2.1.3. 脆弱性対応におけるソフトウェアサプライチェーンの問題

Log4jはThe Apache Software Foundation(Apacheソフトウェア財団)に属する、いわゆるオープンソースのソフトウェアです。オープンソースのソフトウェアは、そのライセンスで定められた条件下において無料でソフトウェアを利用することが認められています。Log4jの場合は、Apache License 2.0が適用されます [5]。Apache License 2.0 では、ソフトウェアの複製、派生ソフトウェアの作成・実行・公開が無料になっており、その手軽さから多くのシステムの開発現場が採用しています。

システム開発者が、システムを開発するときに、開発者自身がLog4jを組み込んでいるケースもあれば、採用したソフトウェアやライブラリへすでにLog4jが組み込まれているケースもあります。後者のように、システムを構成するソフトウェアやライブラリへあらかじめLog4jが組み込まれている場合は、開発したシステムにLog4jが組み込まれていることの把握が難しくなります。Log4jは、ログ出力という汎用的な機能を実現するソフトウェアであり、オープンソースのソフトウェアの中でも特に広く利用されています。このため、一体どのシステムにLog4jが組み込まれているのか、そのバージョンはいくつか、Log4Shellの影響を受け得るのか、実態の把握に非常に多くの時間と手間がかかります。Log4Shellはとても危険で、さらにこのような利用実態や影響の把握が難しい、対応に苦労した脆弱性でした。

もしLog4j以外にも、このようなソフトウェアがシステムへ組み込まれていて、深刻な脆

弱性が見つかった場合、それはシステムにとって重大なリスクです。システムにどのようなソフトウェアが組み込まれているのか、あらかじめ把握しておき、深刻な脆弱性が見つかったときに、脆弱性を含んでいるソフトウェアをすばやく洗い出して、影響を評価できる方法があれば安心です。それを実現する手段の一つが、ソフトウェア部品管理表(SBOM : Software Bill of Materials)です。SBOMは、ソフトウェアの部品や部品同士の関連を記述する方法です。

（2）ソフトウェア部品管理表(SBOM)

Solarwinds社の脆弱性を悪用して複数社が侵害されたインシデントなど、ソフトウェアサプライチェーン攻撃の問題が深刻化しており、SBOMの有用性が議論されています。ソフトウェアサプライチェーン攻撃に関しては、2020年度第3四半期のレポートにも掲載しました[6]。SBOMとは、例えば自動車や家電などの工業製品における部品表のようなもので、システムに組み込まれているソフトウェアを表した資料です。米国NTIAの定義 [7]によると、SBOMは表 2-2に示す要素群で構成されます。

表 2-2 ： ソフトウェア部品管理表(SBOM)の構成要素

要素	概要
作成者名	ソフトウェア部品管理表(SBOM)の作成者の名称。
タイムスタンプ	ソフトウェア部品管理表(SBOM)の最終更新日。
サプライヤ名	ソフトウェアのサプライヤの名称。
コンポーネント名 (ソフトウェア名)	ソフトウェアの名称。
バージョン	ソフトウェアのバージョン情報。
ハッシュ値	ソフトウェアのハッシュ値。 利用されているソフトウェア・バージョンなどを一意に特定する識別子です。ハッシュ値に加えて、ハッシュを再現するためにその生成方法も定義する必要があります。
ID	ユニークなID。
リレーション	各ソフトウェアの関係性。 別のソフトウェアを包含、または依存関係にある場合その関係性を示します。

SBOMの概念を図 2-3へ示します。SBOMは、システムやソフトウェア、ライブラリのリレーションを入れ子構造で表現します。図 2-3を例に説明すると、コンポーネント「Foo Application」は、2つのコンポーネント「foo-framework-logger」と「bar-framework-http」を含みます。そのうちの一つのコンポーネントである「foo-framework-logger」は「log4j-

api」を含んでいます。もしlog4j-apiのバージョン2.14.0に深刻な脆弱性があることが発表された場合、Foo ApplicationのSBOMがあれば、Foo Applicationとlog4j-apiに依存関係があることが判ります。さらに依存関係があるlog4j-apiのバージョンが2.14.0であることも、すぐに判ります。

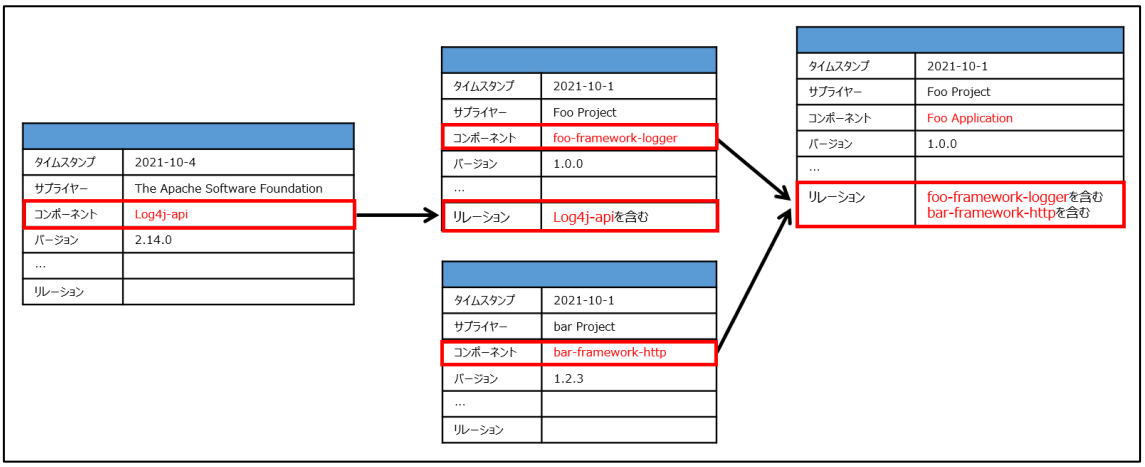


図 2-3 ： ソフトウェア部品管理表(SBOM)の概念図

このようなSBOMを作成・運用することで、脆弱性が公表されたソフトウェアが、運用中のシステムに組み込まれているのか、また組み込まれている場合、どのソフトウェアと依関係にあるのか、瞬時に把握できます。SBOMは、図 2-4に示すように、脆弱性の影響があるシステムの特定時間の短縮や、脆弱性の影響があるシステムの把握漏れを防止できると期待されています [8]。

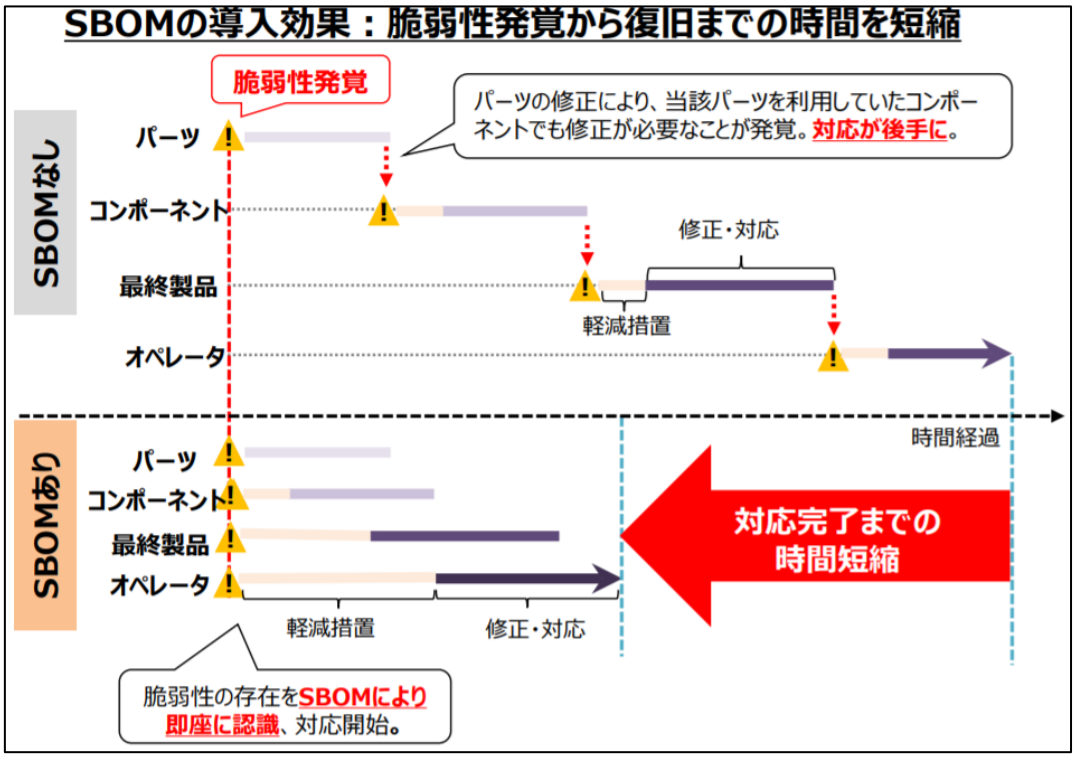


図 2-4 ： ソフトウェア部品管理表(SBOM)の効果 [8]

2.1.4. まとめ

Log4jの脆弱性Log4Shell (CVE-2021-44228)は、非常に深刻な脆弱性です。容易にリモートから任意のコードが実行可能であり、脆弱なLog4jが組み込まれたJavaのシステムであれば、サーバ・クライアントを問わず攻撃可能です。Log4jは広く利用されているため、脆弱なLog4jが含まれているにも関わらず、まだ脆弱性を解決していないソフトウェアがまだ残っているおそれがあります。今後、このような残存した脆弱なLog4jが原因で、様々な被害の報告が予想されます。このように、システムに内包するソフトウェアやライブラリに脆弱性が存在する場合、システムの製造元でなければ、その脆弱性のリスクを調査できず、脆弱性が残存し続けてしまう、という問題が判明しました。

脆弱性を放置することは、即、重大なセキュリティ侵害につながるおそれがあります。特に大規模システムを複数運用している組織は、広く利用しているライブラリの脆弱性の調査が大変な重荷になります。そこで、ソフトウェアサプライチェーンの構成管理が行えるソフトウェア部品管理表(SBOM)が注目されています。SBOMの作成と運用は、脆弱性対応をより正確に、より短時間で実行することができるため、非常に効果があると言えます。

2.2. 最低限のセキュリティベースライン「Minimum Viable Security Product（MVSP）」策定

2021年10月、GoogleやSalesforce等を中心に、ベンダ中立的な最低限のセキュリティベースライン「Minimum Viable Security Product （以下、「MVSP」とする）」が策定されました。MVSPは、BtoBのソフトウェアやビジネス・プロセスのアウトソーシングサービスを提供する企業が実装すべき必要最低限のセキュリティ要件として開発されました。MVSPは、上記のソフトウェアやサービスを提供する企業をセキュリティ評価するときのプロセスの複雑さやそれによって生じるオーバーヘッドを排除できるように、許容できる最低限のセキュリティ要件に絞った簡素なチェックリストになっています [9]。本稿では、MVSPが策定された背景やMVSPの概要、活用方法についてご紹介します。

2.2.1. MVSP策定の背景

（3）サプライチェーン全体のリスク評価の重要性

コスト削減やコア業務への集中などを目的に、クラウドサービスを活用したり、IT業務やシステムの開発・運用・保守などを外部委託したりする企業が増え、ITに関わるサプライチェーンが拡大しています。その結果、自社のセキュリティ対策をしっかり実施していても、セキュリティ対策が不十分な委託先など、サプライチェーンの弱点を突かれてサイバー攻撃を受ける事例が増えています。商流を伝播する組織連鎖のサプライチェーン攻撃の被害を完全に防ぐことは困難ですが、万が一攻撃を受けた場合の被害を最小限に抑えるためには、サプライチェーン全体を把握して、適切なリスク低減策をとるべきです。このリスク低減策は、委託元のセキュリティ対策をすべての委託先へ適用して一括管理する方法や、委託先がサプライチェーン攻撃に対して十分な対策を行って安全であることを確認してから契約する方法などがあります [10]。いずれの方法も、まずは委託先などのサプライチェーン全体のセキュリティ対策状況を把握し、適切にリスク評価しなければなりません。

（4）サプライチェーンのリスク評価における課題

委託元が委託先のリスク評価を行う場合、一般的には、①委託元が独自に策定したセキュリティベースラインを用いてセキュリティ対策状況を評価する方法、または②セキュリティ企業が提供しているリスク評価サービスを利用する方法のどちらかを使います。

①の場合、委託元は自前でセキュリティベースラインを策定するだけでなく、委託先の回答内容の確認や取りまとめに時間を要するため、委託先の安全性の判断が遅くなる問題があります。技術や社会のトレンドが急速に変化する現代において、意思決定が遅れて契約に時

間がかかれば、事業の立ち上げが遅れてビジネス機会の損失につながります。

また、①、②どちらの場合も、委託元が複数あれば、委託先はリスク評価を何度も実施しなければなりません。評価項目は委託元またはリスク評価サービス毎に異なる場合が多いため、結果的に膨大な量のセキュリティ要件に対応しなければならず、委託先にとっても負担が大きいという課題があります。

2.2.2. MVSPとは

（1） MVSP の概要

MVSPは、上述の委託先をはじめとしたサプライチェーンのリスク評価の負担を軽減するために、Google、Salesforce、Okta、Slackなど、業種を超えた複数の企業によって開発されました [9]。MVSPは、最低限実装すべきコントロール24項目から成るチェックリストです。Googleなどの複数企業が、企業のセキュリティ評価に用いている評価項目を分析し、これらの要件のほとんどが組み込まれています [11]。24項目のコントロールは、ビジネスコントロール、アプリケーション設計コントロール、アプリケーション実装コントロール、運用コントロールの4つに分類できます。チェックリストには、各コントロールとして実施すべき具体的な内容が書いてあります。また、チェックリストとは別にFAQが用意されており、各コントロールの詳細な説明と各コントロールがセキュリティ対策に重要な理由が書いてあります [12]。以下にMVSPチェックリストの一部抜粋を示します。

表 2-3 ： MVSPチェックリスト（一部抜粋）[13]

コントロールの分類名	コントロールの具体名	コントロールの説明
1 ビジネスコントロール	1.4 外部テスト	セキュリティベンダと契約し、年1回、自社システムの包括的なペネトレーションテストを実施する。
	1.7 インシデントハンドリング	侵害を発見してから72時間以内に、過度に遅れることなく顧客に通知する。通知には、以下の情報を含める。 ・ 関連する連絡先 ・ 侵害の技術的な予備分析 ・ 合理的なスケジュールを伴う改善計画
2 アプリケーション設計コントロール	2.1 シングルサインオン	最新の業界標準プロトコルを使用したシングルサインオンを実装する。
	2.4 パスワードポリシー	シングルサインオンに加えてパスワード認証を使用する場合： ・使用可能な文字を制限しない。 ・パスワードの長さを64文字以下に制限しない。

		・パスワードリセットの要件として、秘密の質問を単独で使用しない。 ・パスワード変更要求のメール認証を必須とする。 ・パスワード変更時に、新しいパスワードに加えて、現在のパスワードも要求する。 ・新しく作成したパスワードは、一般的なパスワードリストや流出したパスワードのデータベースと照合する。 ・既存のユーザーパスワードが漏洩していないか定期的にチェックする。 ・メモリハードまたはCPUハードの一方向ハッシュ関数を使用して、パスワードをハッシュ化およびソルト化して保存する。 ・適切なアカウントロックアウトとアカウントアクセス時のブルートフォース対策を実施する。
	2.6 依存関係のパッチ	重大度スコアが「中」以上のセキュリティパッチを適用するか、パッチリリース後1カ月以内に、アプリケーションスタックのすべてのコンポーネントで同等の緩和策を利用できるようにする。
3 アプリケーション実装コントロール	3.3 脆弱性の防止	少なくとも以下の脆弱性を防ぐために、開発者の教育や開発ガイドラインを実施する。 ・ 認証のバイパス（例：通常のアカウントから他の顧客データや管理者機能にアクセスする） ・ 安全でないセッションID（例：推測可能なトークン、安全でない場所に保存されたトークン。(secureおよびhttpOnly属性が設定されていないCookieなど)） ・ インジェクション（例：SQLインジェクション、NoSQLインジェクション、XXE、OSコマンドインジェクション） ・ クロスサイトスクリプティング（例：安全でないJavaScript関数の呼び出し、安全でないDOM操作の実行、エスケープせずにHTMLにユーザ入力をエコーバックする） ・ クロスサイトリクエストフォージェリ（例：異なるドメインからのOriginヘッダを持つリクエストの受け入れ） ・ ・脆弱性のあるライブラリの使用（例：脆弱性が判明しているサーバサイドフレームワークやJavaScriptライブラリの使用）

	3.4 脆弱性の修正時間	セキュリティに重大な影響を与えるアプリケーションの脆弱性に対し、発見から90日以内にパッチを作成し、適用する。
4 運用コントロール	4.1 物理的アクセス	以下の管理が行われていることを確認し、関連施設の物理的セキュリティを検証する。 ・ 階層的な境界管理及び内部バリア ・ 鍵管理 ・ 入退室ログ ・ 侵入者警報に対する適切な対応計画

（2）既存のセキュリティベースラインとの比較

代表的なセキュリティベースラインとしては、米国の非営利団体であるCIS (Center for Internet Security) が管理する「CIS Controls」や、情報処理推進機構（IPA）が公開する「非機能要求グレード」などがあります。

CIS Controlsは、グローバルでの知名度が高く、多くの企業が参考にして自社のルール策定やセキュリティ対策を実装しています。CIS Controlsは、サイバー攻撃への技術的対策のベストプラクティスを18項目のコントロールに分類して記載した対策リストです。CIS Controlsは、コントロールごとに実装グループ(IG)が示されており、組織の規模や成熟度に応じて実装の優先順位を決めることができます。さらに、コントロールを実装するために組織がとるべき153項目の具体的な手段がリスト化されているほか、用語集や各コントロールの重要性、実装手順とツールなどの情報も整理されています [14]。個々の対策が実現可能であることを重視して設計されており、コントロールを実装するための手順やツールなどが具体的に示されています。また、解釈が人によって異なるのを避けるために曖昧な言葉を使わず、一部の対策については閾値を定めることで対策の実装レベルなどを測定できるようにしています。

非機能要求グレードは、システム基盤に対する非機能要求項目を網羅的にリストアップしたものです。システム開発の要件定義などの場面で非機能要求を提示、提案する際に発注者・受注者が共通認識を持つことを目的に策定されています。要求項目は可用性、性能・拡張性、運用・保守性、移行性、セキュリティ、システム環境・エコロジーの6項目に分類され、セキュリティに関する要求は37項目あります。システムの重要度ごとに要求レベルが段階的に示されています。要求項目一覧のほかに、用語集や利用方法などが書かれた利用者ガイドが用意されています [15]。

以下に、MVSPおよび既存のセキュリティベースラインの特徴およびメリット・デメリットをまとめます。

表 2-4 ： セキュリティベースラインの特徴およびメリット・デメリット

セキュリティベースライン	特徴	メリット	デメリット
MVSP	・ 対象企業をセキュリティ評価するためのセキュリティ要件に限定しており、チェックリストの項目数が少ない ・ コントロールの実現方法を具体的に示しており、判断基準や重要性を明示している	・ リスク評価プロセスを簡素化できる ・ 認識齟齬が起きにくい	・ セキュリティ要件の網羅性に欠ける ・ 適用できる組織が限定される
CIS Controls	・ サイバー攻撃のトレンドを踏まえた実践的な技術的対策を網羅している ・ コントロールの実現方法を具体的に示しており、判断基準や重要性を明示している ・ 他のセキュリティフレームワークとの整合性がある ・ 組織の規模や成熟度に応じて実装の優先順位をつけられる ・ グローバルで普及している	・ 規模や成熟度の異なるあらゆる組織に適用できる ・ 認識齟齬が起きにくい ・ グローバル企業との親和性が高い	・ セキュリティ要件の数が多く、すべての対応にコストがかかる
非機能要求グレード	・ システム基盤に対するセキュリティ要件に限定されている ・ 重要項目と非重要項目を区別している ・ 各要求項目の定量的な要求レベルを示している ・ 利用者向けのガイドが充実している	・ 対策の優先度をつけやすい ・ 定量的な評価ができる	・ システム基盤以外で実現するセキュリティ要件が含まれていない ・ 日本でしか使われていない

3つのベースラインの中で、最もセキュリティ要件の網羅性が高いのはCIS Controlsです。自社のルール策定や重要度の高い情報を扱うシステムや企業のリスク評価を行う場合など、金銭的・時間的コストよりもセキュリティ要件の網羅性を重視する場合にはCIS Controlsを活用するのがよいでしょう。一方で、委託元が多くの委託先に対してリスク評価を行う場合は、1件に掛けるコストが限られたり、スピードを重視したりします。その場合には、最低限のセキュリティ要件に絞ったMVSPを活用するのもよいでしょう。また、システム開発の要件定義などの場面では、システム基盤で実現すべきセキュリティ要件に特化して、システムの重要度に応じた要求レベルを示している非機能要求グレードが向いているといえます。

このように、セキュリティベースラインによって特徴やメリット・デメリットが異なるため、目的に応じて使い分けるのがよいでしょう。

2.2.3. MVSP活用時のメリットおよび注意点

サプライチェーン全体のリスクを低減するには、委託先のリスク評価は非常に重要ですが、サプライチェーンが複雑化するほど、委託元と委託先の双方の負担が大きくなります。サプライチェーンにおける委託先のリスク評価にMVSPを活用すれば、委託元と委託先が以下の表 2-5のメリットを享受できます。

表 2-5 ： MVSPを活用した場合の委託元と委託先のメリット

委託元	委託先
独自のセキュリティベースラインを策定する手間を省くことができる	委託元ごとに異なる独自の要件に都度対応せずとも、MVSPの要件に対応するだけで済む
委託先のリスク評価（回答の確認、分析など）にかかる時間を削減できる	チェックリストの回答にかかる時間を削減できる
MVSPに対応している委託先を選定することで、契約時の審査プロセスを短縮できる	MVSPに対応していることが顧客へのアピール材料となる

MVSPは、契約時や定期的な委託先のリスク評価に活用することができます。セキュリティ対策の実施内容や基準、実施すべき理由が明確に示されているため、契約時に委託元と委託先の間で対策内容の認識齟齬が起きにくくなります。また、チェックリストの項目数が24項目と少ないため、回答する委託先と回答を評価分析する委託元の双方ともに、負荷が少なくて済みます。またMVSPは、提案依頼書（RFP）の策定に活用することもできます。MVSPをRFPのセキュリティ要件とすれば、委託元は簡素な審査プロセスで最低限のセキュリティを確保できます。

しかし、上記いずれの場合も、MVSPでは最低限のセキュリティしか確保できない点に注意してください。大量のクレジットカード情報や遺伝子情報のような機微な情報を扱う高いセキュリティ対策レベルを求める企業は、MVSPに加えて、業界が定めるスタンダードなセキュリティ対策や追加対策を実施することを推奨します。

2.2.4. まとめ

グローバル化やビジネスモデルの多様化に伴い、サプライチェーンはますます複雑化すると予想します。サプライチェーン全体のリスクを正確に把握することが難しくなり、対策に抜け漏れが生じやすくなるでしょう。その結果、サプライチェーン上にセキュリティ対策の不十分な企業が増え、サプライチェーン攻撃の被害に遭う企業が今後も増えると予想できます。サプライチェーン攻撃に対する決定的な対策は存在しないため、サプライチェーン全体

で脆弱な部分を作らないことが重要です。そのためには、サプライチェーン全体のリスクを適切に評価し、リスクの高いところから対策する必要があります。しかし、従来のリスク評価プロセスは複雑で時間がかかり、評価する側／される側双方にとって負担が大きいため、サプライチェーン上のすべての組織のリスク評価は困難です。MVSPは、このリスク評価プロセスを簡素化し、最低限のセキュリティを確保することに役立つため、サプライチェーン全体のリスク評価に採用する企業が増えると予想します。今後、MVSPを採用する企業が増えれば、MVSPはデファクトスタンダードとなる可能性があります。委託元や委託先となりうる企業はMVSPに対応できるよう備えておくと良いかもしれません。

3.情報漏えい『EC-CUBEの脆弱性のインシデント継続』

2021年5月7日に株式会社イーシーキューブが、EC-CUBEのクロスサイトスクリプティング（XSS）の脆弱性に関する注意喚起を公開しました [16]。2021年度版 第1、第2四半期の本レポートでも、これらの脆弱性で発生したインシデント事例や対策を取り上げましたが [17] [18]、第3四半期においても、依然としてEC-CUBEの当該脆弱性を悪用した攻撃によって、ECサイトからクレジットカード情報等の漏えい被害が発生しています。

本稿では、これまでのインシデント事例から、脆弱性への対策が遅れる理由、および適切に対策を進める方法を考察します。

3.1. 2021年5月に公開されたEC-CUBEの脆弱性

（3）本体とプラグインの脆弱性の解説

EC-CUBEには、2021年5月に公開されたXSS攻撃が成立する2つの脆弱性があります。通常、ユーザが文字列を入力するWEBページは、想定していた文字列の代わりにスクリプトを入力しても、スクリプトを実行しないように対策します。しかしEC-CUBE 4.0系は、入力したスクリプトを無害化する処理を無効化していました。これが、1つ目の脆弱性 CVE-2021-20727です。またEC-CUBE 3.0系は無害化の処理を行っていたが、特定のプラグインがその無害化したスクリプトを実行可能な状態に戻す処理を実装していました。これが、2つ目の脆弱性CVE-2021-20735です。

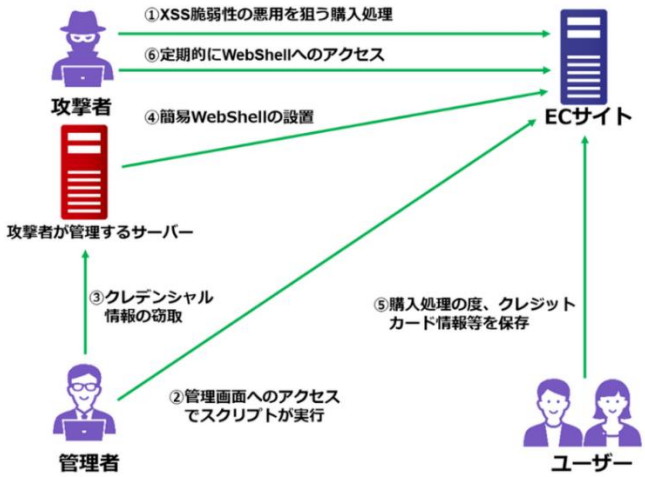


図 3-1 ： EC-CUBE脆弱性のXSS攻撃の流れ [19]

これらの脆弱性を悪用した攻撃は、図 3-1に示す流れで行われます。攻撃者は、ECサイトの注文フォームへ不正なスクリプトを含んだ文字列を入力します。攻撃者が入力した不正なスクリプトは、ECサイトのデータベースへ保存されます（図 3-1の①）。この状態で、ECサイトの管理者がEC-CUBEの管理画面をブラウザで開いて上記の注文情報を閲覧すると、ブラウザが不正なスクリプトを読み込んで実行します（図 3-1の②）。攻撃者の不正なスクリプトは、管理者のマシン上から認証情報を窃取して、攻撃者の管理サーバへ送信します（図 3-1の③）。攻撃者は、窃取した認証情報を使ってECサイトへ不正にログインして、Webshellを設置します（図 3-1の④）。攻撃者は、設置したWebshellを用いて、ユーザがECサイト上へクレジットカード番号等の情報を入力するたびに、その情報を窃取できます（図 3-1の⑤, ⑥） [19]。

（４） EC-CUBE の XSS 脆弱性攻撃の被害事例

2021年度版 第2四半期のレポートでは、当時発生したEC-CUBEを攻撃した被害の事例 [18]を紹介しましたが、下記の表 3-1に示すとおり、第3四半期も継続して同じ脆弱性の被害事例が公表されています。

表 3-1 ： EC-CUBEを利用したECサイトの被害事例（2021年度第2, 3四半期）

#	公表日	ECサイト名	ECサイトの運営会社
1	2021/7/6	Hoick [20]	株式会社ソングブックカフェ
2	2021/7/12	コスモスオンラインストア [21]	株式会社コスモス薬品
3	2021/7/13	TRANSIC [22]	TRANSIC株式会社
4	2021/7/14	よみファねっと [23]	株式会社読売情報開発大阪
5	2021/7/20	ＥＣサイトプロショップ匠 [24]	株式会社キャンディルデザイン
6	2021/7/21	毎日元気公式ショッピングサイト [25]	有限会社毎日元気
7	2021/7/26	KQLFT TOOLS [26]	株式会社SONS-MARKET
8	2021/8/16	FUKUYAONLINE [27]	株式会社フクヤ
9	2021/8/18	THE HAIR BAR TOKYO オンラインストア [28]	ギャップインターナショナル株式会社
10	2021/8/23	コマキ楽器WEBサイト [29]	株式会社コマキ楽器
11	2021/9/7	たち吉オンラインショップ [30]	株式会社たち吉
12	2021/9/14	伊勢せきやオンラインショップ [31]	株式会社関谷食品
13	2021/9/16	オムニECシステム [32]	株式会社ジーアール
14	2021/10/21	ALPHAICON [33]	株式会社アイコンズ

15	2021/10/26	www.tapiocaworld.jp [34]	株式会社ネットタワー
16	2021/10/28	TANAXオンラインショップ [35]	タナックス株式会社
17	2021/11/2	ベイシアネットショッピング [36]	株式会社ベイシア
18	2021/11/2	パーツクラブオンライン [37]	株式会社エンドレス
19	2021/11/2	ROOMDECOオンラインショップ [38]	株式会社かねたや家具店
20	2021/11/9	LINK IT MALL [39]	株式会社リンクイット
21	2021/11/16	杏林堂オンラインショップ [40]	株式会社杏林堂薬局
22	2021/11/18	グラントマトオンラインショップ [41]	グラントマト株式会社
23	2021/11/18	トコちゃんドットコムECサイト [42]	有限会社トコちゃんドットコム
24	2021/12/2	芝寿しオンラインショップ [43]	株式会社芝寿し
25	2021/12/2	EVANGELION STORE [44]	株式会社グラウンドワークス

3.2. インシデント被害を公表した企業の傾向

表 3-1のインシデント被害が発生した企業の情報や報告書を分析した結果、以下の傾向があることが分かりました。

（1）業種と規模

表 3-1より、業種を問わず、多岐にわたる業種の企業が、本脆弱性を狙った攻撃の被害にあったことが分かります。また、被害を公表した企業は、比較的に中小企業が多いです。セキュリティ対策の重要性を感じつつも、十分な予算や人員を割り当てられずに、脆弱性の調査や対策が不十分なままになってしまい、当該脆弱性の被害が発生したおそれがあります。

（2）インシデント発見のタイミング

表 3-1の被害の報告書を分析すると、大部分の運営会社が、カード会社やお客様からクレジットカードの不正利用の連絡を受けてから、インシデントに気づいていることが分かりました。以下に、外部から連絡を受けるまで、運営会社がインシデントに気づかなかった理由を推測します。

- セキュリティ製品を利用した対応ができない
  - セキュリティ製品を導入していない
  - セキュリティ製品が検知しない（検知できない不完全な状態）
  - セキュリティ製品が検知したが、判断を誤る
- 侵害の監視やログの定期的な調査をしていない
  - ECサイトのWebアクセスのログを監視していない

- 管理者のログインや操作のログを定期的に監査していない
- 脆弱性対策サイクルの運用に問題があった
  - 構成管理と脆弱性情報収集をしていない
  - 脆弱性のリスク評価をしていない
  - 侵害調査をしていない、できない

3.3. 被害企業がとるべき脆弱性対策

2021年度第2四半期のレポートでは、FortiGateの脆弱性が原因で発生したインシデント事例を取り上げ、適切に脆弱性対策サイクルを運用することの重要性を説明しました [18]。3.2で分析した結果から、EC-CUBEの脆弱性起因で被害にあったECサイトの多くは、脆弱性対策サイクルの「①構成管理」、「②脆弱性収集」が充分でなかったと推測します。そのために、カード会社やお客様からの被害の連絡があるまで、脆弱性を放置していたと推測します。脆弱性対策は、まずは①構成管理と②脆弱性収集を確実に実施することです。

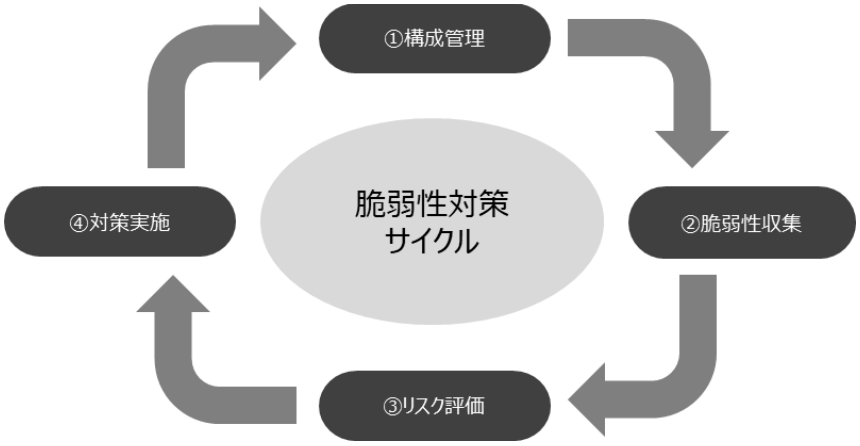


図 3-2 ： 脆弱性対策サイクル [18]

またEC-CUBE社は、2021年5月の脆弱性に比べると影響の深刻度は低いものの、2021年11月にもアクセス制御の不備の脆弱性 CVE-2021-20841とクロスサイトリクエストフォージェリの脆弱性 CVE-2021-20842を公開しています [45] [46]。このように、一つの製品から複数の脆弱性が次々に見つかる場合があります。FortiGateのインシデント事例の記事では、脆弱性対策サイクルを確実に運用するために、自組織のセキュリティ体制を整備することを提言しました。しかし、3.2で述べたとおり、表 3-1の被害企業には、自組織のみでセキュリティ体制を構築、運用することが難しいと思われる中小企業を多く含んでいます。こうした中小企業は、外部ベンダへECサイトの構築と運用をすべて委託するケースが一般的です。そのため、以下の条件を満たす委託先へ、ECサイトの維持運用業務を委託するべきです。

- 脆弱性対策サイクルを運用できること
  - 構成管理ができる
  - 脆弱性情報収集ができる、脆弱性のリスク評価と影響分析ができる
  - パッチ適用や暫定対処ができる
  - 侵害調査ができる
- ISMSやPマークなどの第三者認証を取得している

上記の条件を満たす委託先へECサイトの維持運用業務を委託することが困難であれば、SaaS型のクラウドサービスの利用も検討してみましょう。その場合は、脆弱性が見つかった時に積極的に情報公開していたり、迅速に脆弱性対応していたりするクラウドサービスが安心です。クラウドサービスの脆弱性の対応状況がわからない場合は、ISO/IEC 27017やISMSクラウドセキュリティ認証などの第三者認証を取得しているサービスを選択してください。

3.4. まとめ

EC-CUBEのXSS脆弱性を悪用した攻撃被害の報告は、公表から半年以上経過した2021年12月でも続いています。3.2で述べたように被害にあった企業の多くは、公表された脆弱性に気づかず、有効な対策をとらないまま攻撃を受けたと思われます。このように公表済みの脆弱性を放置すると、高い確率で攻撃を受けて大きな被害が発生します。脆弱性情報の収集など、脆弱性対策サイクルを導入して継続的に回すことが、有効な対策です。しかし、十分な情報セキュリティ体制を持てない中小企業は、自組織のみで脆弱性対策サイクルを回すことは困難です。システム開発や運用を委託するときは、脆弱性対策サイクルを安心して任せることができる委託先へ依頼するか、SaaS型のクラウドサービスを積極的に活用するべきです。

4.脆弱性『ZohoのUEM製品に発生した脆弱性』

本章では、Zoho社の ManageEngine Desktop Centralの複数の脆弱性を解説します。アメリカ国立標準研究所（NIST）が公開している脆弱性データベース（NVD）に掲載された当該脆弱性のCVSS値は9.8であり、深刻な脆弱性です。当該製品を導入している企業、組織は早急にパッチを適用しなければなりません。

4.1. ZohoのUEM製品に発生した脆弱性

4.1.1. 脆弱性の概要

Zoho社は、2021年12月3日にManageEngine Desktop Centralに生じた脆弱性 CVE-2021-44515とManageEngine ServiceDesk Plusに生じた脆弱性CVE-2021-44526へのセキュリティアドバイザリーとパッチを公開しました [47]。CVE-2021-44515は、リモートからManageEngine Desktop Centralのエージェントへ接続するときの認証をバイパスできてしまう脆弱性です。攻撃者は、細工したリクエストをエージェントへ送信して認証をバイパスして、リモートから任意のコードを実行できるおそれがあります。CVE-2021-44526も認証をバイパスできてしまう脆弱性です。攻撃者は、アプリケーションフィルタの脆弱性を狙って細工したリクエストを送信すると、認証をバイパスして、認証済みユーザのみが利用できる機能にアクセスできます。これらの脆弱性は、パッチ公開前に攻撃が発生したゼロデイ脆弱性です。国家が支援している攻撃グループが、この脆弱性を攻撃に悪用しています。

FBIのレポートによると、あるAPT（Advanced Persistent Threat）攻撃グループが、すでに2021年10月下旬から、この脆弱性を悪用したゼロデイ攻撃を行っています [48]。このAPT攻撃グループは、8月から3つの攻撃キャンペーンを展開し、少なくとも13組織を侵害しました。まず、2021年9月16日、米Cybersecurity and Infrastructure Security Agency(CISA)は、APT攻撃グループがセルフサービス型のパスワード管理およびシングルサインオンソリューションのManageEngine社のADSelfService Plusの脆弱性を悪用して、図 4-1のキャンペーン1の攻撃をおこなっていると警告しました。11月7日、PaloAlto社は、キャンペーン2で少なくとも9つの組織が侵害されたと発表しました。そしてAPT攻撃グループは、キャンペーン3で攻撃対象をManageEngine社の別製品 ServiceDesk Plusへ変更して、10月25日から11月8日にかけて脆弱性を攻撃して複数の組織を侵害しました。

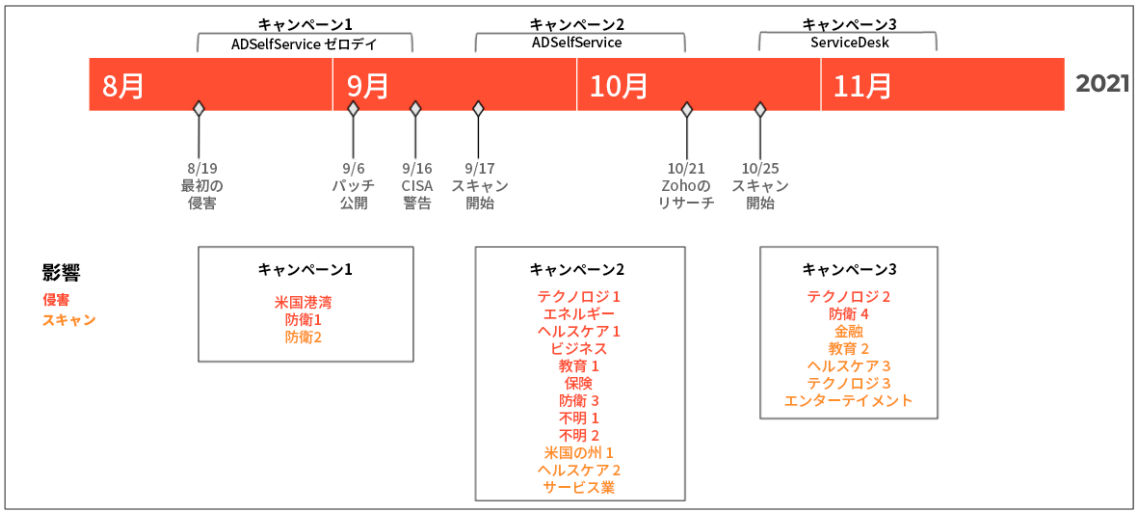


図 4-1: キャンペーンのタイムラインと影響 [49]

4.1.2. ManageEngine製品の概要

ManageEngine Desktop Centralは、システム管理者が、社員の端末のパッチ管理、ソフトウェアインストールやライセンス管理、各種外部デバイスの接続制御、モバイルデバイス管理を統合コンソール上で集中管理できる統合エンドポイント管理（UEM）と呼ばれるソフトウェア製品です [50]。管理対象のデバイスにエージェントをインストールすれば、ネットワーク経由で、どこからでもアクセスして、Windows/Mac/Linux端末の各種管理とリモートコントロールができます。ネットワークが繋がっていれば、別のビルの端末や海外の端末も遠隔から効率的に管理できます。

ManageEngine ServiceDesk Plusは、インシデント管理、問題管理、変更管理、CMDB、資産管理、顧客満足度調査など、豊富な機能を持つWebベースのITサービスマネージメントツールです。

4.1.3. 脆弱性CVE-2021-44515とCVE-2021-44526の解説

4.1.1へ記載した通り、CVE-2021-44515は認証をバイパスする脆弱性です。攻撃者は、特別に細工したリクエストを脆弱なエージェントへ送信すると、CVE-2021-44515を悪用してManageEngine Desktop Centralの認証をバイパスできて、リモートから任意のコードを実行できます。当該脆弱性を悪用すると、遠隔からエージェントが動作しているマシン上へソフトウェアをインストールしたり、コマンドプロンプトを直接操作したりする機能が悪用できると推測します。APT攻撃グループは、脆弱性CVE-2021-44515を悪用してManageEngine Desktop Central のAPIの経由で、認証なしでWebshellをアップロードします。このWebshellで、正規のManageEngine Desktop CentralのAPI機能を上書きしてしまいます。Webshellは、ManageEngine Desktop Centralへ届いたリクエスト通信を取得して、その中から攻撃者の命

令を抽出して、SYSTEMユーザ権限でコマンドを実行します。APT攻撃グループは、上記のWebshellを使って侵害したマシンを踏み台にして、つぎの攻撃を行います。APT攻撃グループは、ドメインコントローラを攻撃して侵入して、Mimikatzを使用して認証情報を取得したり、pwdumpやProcDumpを使ってLSASSプロセスメモリからパスワード取得したりします。

CVE-2021-44526は、細工したURLを送付して、アプリケーションフィルタを正しく設定していない問題を悪用して認証なしでサーブレットプログラムへアクセスできる脆弱性です。PaloAlto社によると、ManageEngine ServiceDesk Plusを遠隔管理するためのREST APIに脆弱性があります。APT攻撃グループは、まず細工したURLを使って、ManageEngine ServiceDesk Plus のサーバのREST APIへ"msiexec.exe" というファイル名のマルウェア(ドロッパー)のアップロードを要求します。このとき、認証は不要です。つぎに、APT攻撃グループは、同様の手順でREST APIへ、このmsiexec.exeの起動を要求します。このときAPT攻撃グループは、ManageEngine ServiceDesk Plusが正規のmsiexec.exeの代わりに、マルウェアを実行するように設定します。マルウェアの実行が成功すると、同一マシン上でマルウェが複数起動しないように排他制御する仕組みであるミューテックスを作成します。このミューテックスが、攻撃キャンペーン1や2で見つかったマルウェアのミューテックスと同じだったため、同じAPT攻撃グループの攻撃だと推測しています。このマルウェアは、APT攻撃グループのサーバからWebshellをダウンロードして、メモリ上へロードして実行します。このWebshellは、Apache TomcatのJava Servlet Filter機能を利用して動作します。そのため、APT攻撃グループからWebshellへの命令の通信は、特定の送信先URLを指定しなくても、フィルタリング処理時にWebshell向けの通信だけを抽出してWebshellへ渡します。そのため、セキュリティフィルタも回避してしまいます。APT攻撃グループは、この脆弱性を悪用してインストールしたWebshellを使って、ManageEngine ServiceDesk Plus のサーバを遠隔操作できます [51]。

4.1.4. 当該脆弱性の危険性

このUEM製品の脆弱性は、リモート接続可能な製品の脆弱性とは、異なる危険性があります。攻撃者がUEM製品を攻撃して乗っ取った場合、どのような影響が発生するでしょうか。

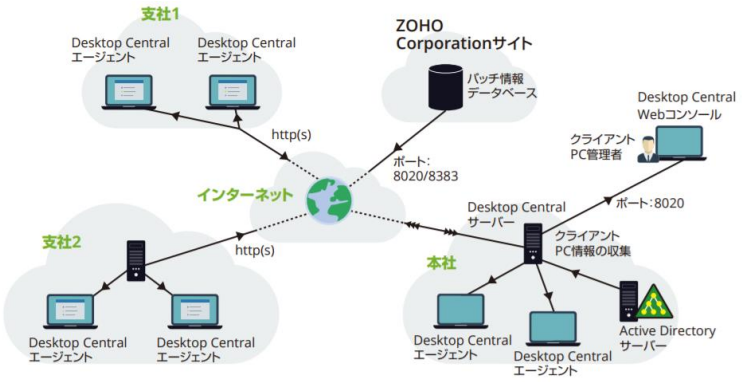


図 4-2 ： ManageEngine Desktop Centralのアーキテクチャ [50]

APT攻撃グループが、図 4-2の本社に設置してあるManageEngine Desktop CentralやServiceDesk Plusのサーバを攻撃して遠隔操作できるようになった場合、ManageEngineアプリケーションのサーバの管理機能を使うことができます。4.1.2 で説明したように、ManageEngine Desktop Centralは、エージェントをインストールしてある全端末へ遠隔からソフトウェアをインストールしたり、コマンドを実行したりできます。APT攻撃グループは、全端末へマルウェアをインストールすることも、端末上の情報を詐取することも可能です。

ManageEngine ServiceDesk Plusは、WebベースのITサービスマネージメントツールのため、端末を遠隔操作する機能はありません。しかしAPT攻撃グループは、ManageEngine ServiceDesk Plusのサーバを踏み台にして、隣接するActive Directoryサーバを攻撃することができます。APT攻撃グループがActive Directoryサーバへの侵入に成功して、Windowsドメインの管理者権限を取得できた場合、Windowsドメインへ参加している端末をしたり、信頼関係のあるドメインへ侵害範囲を拡大（ラテラルムーブメント）したりするおそれがあります。

4.2. まとめ

攻撃者が組織やシステム内の端末を侵害して、そこを踏み台に侵害範囲を拡大する場合と比べて、UEM製品を侵害して管理者権限を取得した場合は、容易にマルウェアを大量感染させたり、機密情報を盗んだり、侵害範囲を拡大したりできます。本来は、自社の情報や資産を守るためのUEM製品が、攻撃者を手助けする製品へと様変わりします。UEM製品のような大量のマシンを統合して集中管理するソフトウェアはより強固にセキュリティ対策を行って、攻撃者が悪用しないように守らなければなりません。もし侵害された場合は、短期間で広範囲へ影響が拡大するため、暫定対処や復旧が容易ではありません。事前に影響範囲を特定する方法やネットワーク遮断やシステム停止による被害拡大を阻止する方法、復旧方法を検討して、いざと言うときのために備えておきましょう。

5.マルウェア・ランサムウェア『EMOTET攻撃活動を再開』

2021年1月にテイクダウンしたEMOTETが、2021年11月14日頃から攻撃活動を再開しているとThe Record by Recorded Futureが発表しました [52]。その後、IPAが、2021年11月16日に"Emotetの攻撃活動再開について"と題して､攻撃メールや注意喚起を発表しました [53]。

本稿では、EMOTETが攻撃活動の再開に至った背景や目的を考察し、再開後のEMOTETの特徴や注意喚起を説明します。

5.1. EMOTETのこれまで

EMOTETは、ユーザが正規メールを装った攻撃メールの添付ファイルやリンクをクリックすると感染して､機密情報の窃取や別マルウェアの二次感染を引き起こします｡EMOTETは、攻撃者が用意したインターネット上の指令・制御サーバ（Command and controlサーバ。以下､「C2サーバ」という）と通信します。EMOTETのマルウェア本体は、柔軟性が高いモジュール型で､簡単に機能追加し､C2サーバと大規模なボットネットを構成する特徴があります。2014年頃に登場して以降、EMOTETは世界中で大規模な被害を引き起こしました。しかし、2021年1月27日にEUROPOLとEUROJUSTの調整の下､オランダ､ドイツをはじめとする8か国の警察が協力して「Operation LadyBird」作戦を実行し、EMOTETの運用基盤は停止（テイクダウン）しました。テイクダウンの開始から終了までの詳細な流れは、弊社発行の「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」にて解説していますので、ご参照ください [54]。

IPAによると､テイクダウン後はEMOTETに関する情報の提供や観測が徐々に少なくなり、EMOTETによる攻撃や被害が停止あるいは大幅に減少しました [53]。また、JPCERT/CCのレポートによると､感染端末の時刻が 2021年4月25日 12:00になるとEMOTETのプログラムは、自分自身を無害化したプログラムへ自動的に更新して動作が停止します｡その結果､2021年4月26日以降、国内におけるEMOTETの感染は、ほぼ観測されなくなりました [55]。

ところが、2021年11月14日頃、The Record by Recorded FutureがEMOTETの攻撃活動の再開を確認したと発表しました [52]｡また､IPAが実際に受信したEMOTETの攻撃メールの情報を提供しています [53]｡攻撃再開後の感染規模は､テイクダウン前と引けを取らない状況です。2021年12月に、悪質サイトの追放プロジェクト"URLhaus"へ報告されたEMOTETに関係する悪性URLの件数は、2020年12月の悪性URLの報告件数の約2倍でした [56]。

では、なぜEMOTETは攻撃活動再開に至ったのでしょうか。次章で考えられる背景や目的を紹介します。

5.2. EMOTET攻撃活動再開を解説

5.2.1. 攻撃活動再開の背景

テイクダウン前のEMOTETの攻撃グループは、EMOTETを介して、TrickBot / Qbotを含むさまざまなマルウェアをコンピュータへ感染させていました（二次感染）。TrickBot / Qbotの攻撃グループは、TrickBotなどを介して、コンピュータへConti (旧 Ryuk) / DoppelPaymer / Darkside / Revil などのランサムウェアを感染させて実行していました（三次感染）。

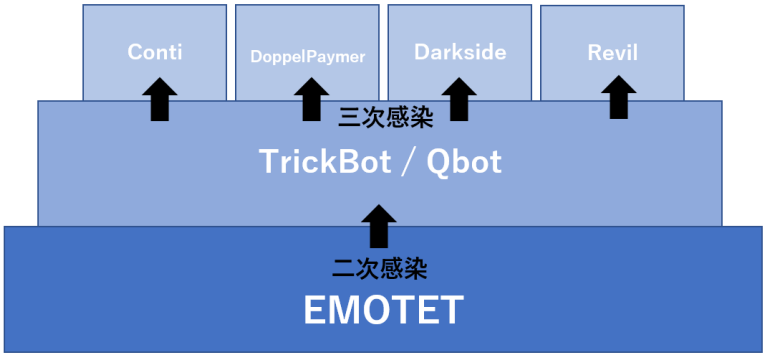


図 5-1 ： EMOTETプラットフォーム利用した他マルウェア感染イメージ

2021年1月に警察がEMOTETのボットネットをテイクダウンすると、これらのランサムウェア攻撃グループはEMOTETのボットネットを使った攻撃ができなくなりました。その結果、EMOTETのボットネットを利用していた複数の攻撃グループは、ランサムウェア攻撃活動を停止してしまいました。

しかし、それらの攻撃グループの中のランサムウェアContiの攻撃グループだけは、活動を休止したランサムウェア攻撃グループから人材を寄せ集め、EMOTETのボットネットの再構築へ向けて動き始めました。ランサムウェアContiの攻撃グループは、EMOTETボットネットのプラットフォームを利用して、自身の感染拡大を行っており、従来から提携関係にあったTrickBotの攻撃グループに話を持ち掛け、EMOTETの再構築を開始したと考えられています[57]。Bleeping ComputerやBlackBerryの報道によると、TrickBot / Qbotの攻撃グループが、TrickBotマルウェアが感染したデバイスへ、TrickBotマルウェアを使用してEMOTETローダー（EMOTETをダウンロードして当該マシンへ感染させる役割を持つプログラム）を送り込んで実行し、EMOTETのボットネットを再構築しました [57] [58]。このような経緯で、ランサムウェアContiの攻撃グループとTrickBot / Qbotの攻撃グループが、ランサムウェア攻撃活動を再開するために、EMOTETのボットネットを再構築しました。

上記はBleeping Computerらが考えた仮説ですが、もし仮説通りであれば、EMOTETの攻撃メールの送付再開はEMOTETの感染拡大が目的ではなく、ランサムウェアContiの攻撃グルー

プの攻撃活動の再開が目的です。

今後、再び警察がEMOTETのボットネットのテイクダウンに成功して、EMOTETのボットネットを運営していた攻撃グループのメンバを逮捕したとしても、またEMOTETのボットネットを使っていた別の攻撃グループがEMOTETのボットネットを再構築してランサムウェア攻撃を再開するでしょう。そう考えると、根本解決のためにはEMOTETの攻撃グループメンバだけでなく、提携関係にあるランサムウェアの攻撃グループメンバを含む広範囲の逮捕や活動休止に追い込む必要があります。

5.2.2. 攻撃再開後の特徴

では次に、テイクダウン前のEMOTETと攻撃活動再開後のEMOTETの特徴の違いを説明します。以下の2つの観点に着目しました。

（1）感染手法の違い

感染手法の違いは、以下の2点です。

まず、新たなOfficeファイルの利用です。攻撃活動再開後のEMOTETの感染手法は、テイクダウン前と同様に正規メールへの返信を装った攻撃メールや、業務上開封しそうな巧妙な文面の攻撃メールを使った手法です。攻撃メールには、ファイルを添付します。テイクダウン前には、Microsoft Wordのマクロ有効文書ファイル（拡張子「.docm」）を多用していましたが、再開後は新たにMicrosoft Excelのマクロ有効文書「.xlsm」を用いるようになりました [59]。マクロを含むOfficeファイルは、テイクダウン前と同様、直接メールに添付されるほか、zipファイルとして添付されるケースがあります。また、テイクダウン前と同様、添付ファイルのないケースも見受けられました。その場合、メールにURLが記載されています。URLへアクセスすると、マクロを含むOfficeファイルや後述のAPPINSTALLERファイルをダウンロードするリンク設計となっています。このURLはクッションページと呼ばれています [60]。このOfficeファイルのマクロは、コマンドプロンプトからPowerShellを呼び出して、EMOTETへの感染に必要なファイルを取得・実行します。

次に、PowerShellが添付してあるケースやアプリインストーラーを利用したケースが、新たに見つかっています。APPINSTALLERファイルは前述のクッションページで配布されていました。アプリインストーラーは、拡張子「.appinstaller」のAPPINSTALLERファイルを読み込んで、インストールプログラムが起動します。クッションページで配布していたAPPINSTALLERファイルの場合は、Adobe PDFに見せかけたEMOTETのドロッパーがインストールされて、ユーザがWindowsにログオンした際などに起動して、EMOTETをダウンロードして感染させます [60]。

（2） EMOTET 本体の機能の違い

EMOTET本体の機能の違いは、以下の4点です。

まず、大きな違いとして攻撃再開後のEMOTET本体は、HTTPSなどの暗号化通信を利用してC2サーバと通信し始めました [59]。その結果、通信の特徴からC2通信を検知する方法では、通信内容を復号できないプロキシなどの通信経路上で、EMOTETのC2通信を検知できなくなりました。また、HTTPリクエストがPOSTメソッドからGETメソッドに変化しました [59]。テイクダウン前のEMOTET通信の特徴であるPOSTメソッドで通信先URLとReferrerが同じURLという点を使って検知している場合は、その見直しが必要となるでしょう。

その他には、攻撃活動再開後のEMOTETは、Cookieヘッダにランダムに生成されたキー名とbase64でエンコードされたキー値が含まれています [59] [61]。また、C2サーバの通信先情報は、テイクダウン前と同様にEMOTET本体にハードコーディングされていますが、攻撃活動再開後のEMOTETは、XORベースのアルゴリズムを使用して暗号化しています [61]。

5.3. EMOTETとContiランサムウェアへの対策

テイクダウン前も攻撃活動再開後も、EMOTETはメール経由で感染を拡大します。そのため、これまでと同様に、攻撃メールやその添付ファイルに注意し、不審な添付ファイルやリンクは開かないといった基本的な対策が重要です。しかし、前章で述べた通り、攻撃活動再開後のEMOTETは、感染手法が多岐にわたり、また返信型の攻撃メールや業務に関係する巧妙な文章を用いた攻撃メールを利用するため、人が正規メールかどうかを判断して防ぐことは、より困難になっています。そのため、上記のような各個人のセキュリティ意識に依存した対応とは別に、組織がシステムでEMOTET感染を未然に防止したり、早期検知したりする対応が重要です。EMOTETに関するIoC（Indicator of Compromise）情報を迅速に入手して、FirewallやSIEMなどのセキュリティ機器へ反映できれば、実現できます。これを実現する具体的な手段の１つに、MISP（Malware Information Sharing Platform）の導入があるでしょう [62]。MISP は、Feed機能でIoC情報を自動収集できたり、Synchronisation機能を利用して他組織のMISPとIoCを容易に共有できたりします。

また「6.2.1. 攻撃活動再開の背景」にて言及した通り、Conti攻撃グループはTrickbotのインフラを使ってEMOTETのボットネットを再構築しました。Contiランサムウェアは、暗号化だけでなく、情報を盗み出して公開する「二重脅迫ランサムウェア」です。2020年5月に初めて発見されたランサムウェアですが、近年、その攻撃活動が活発化しています。ダークネットをリアルタイム監視するシステム darkfeed.ioによると、EMOTET活動再開直後の2021年12月において、Contiは全ランサムウェア被害全体の約24%を占めていました [63]。Contiランサムウェアは、感染端末のファイルを暗号化するだけでなく、アクセスできる共有フォルダを探索して他端末のファイルの暗号化を試みます [64]。Contiランサムウェアは、開発サイクルが短く、短期間でバージョンアップしています。新しいバージョンのContiランサム

ウェアは、最初にローダーが感染して、そのローダーがDLLをダウンロードしてメモリ上へ展開して実行するファイルレスタイプです。これにより、ウイルス対策ソフトベンダやセキュリティ専門家によるContiランサムウェアの分析を回避します [64]。よって、Contiランサムウェアのダウンロード先のIoC情報を入手してセキュリティ機器へ反映できれば、被害を軽減できます。

5.4. まとめ

攻撃活動再開したEMOTETに焦点をあて、再開に至った背景やその特徴を解説しました。その背景には、テイクダウン前にEMOTETを使っていたランサムウェアContiの攻撃グループが、ランサムウェア攻撃活動を再開するために、TrickBot / Qbotの攻撃グループを使ってEMOTETのボットネットを再構築したと考えられています。攻撃再開後のEMOTETは、テイクダウン前と比較し、感染手法が変化しており、これまでの検知方法や見分け方法が適用できないケースも見受けられます。また、感染手法の巧妙化も増しており、人的対策だけでは感染防止が難しくなっています。そのため、個人のセキュリティ意識に頼らず、EMOTETに関するIoC情報を迅速に入手して、FirewallやSIEMなどのセキュリティ機器へ適用して、システムでEMOTET感染を未然に防止したり、早期検知したりするべきです。

6.予測

ランサムウェア攻撃グループの収益モデルの変化

ランサムウェアの攻撃グループの攻撃方法に、新たな変化が見えています。2017年に大流行したWannaCryに代表されるように、従来のランサムウェア攻撃グループの手口は、組織や個人のデータを暗号化して、その復号の対価として身代金をせしめる収益モデルが中心でした。2021年度第3四半期では、ランサムウェア攻撃グループがデータの暗号化を行わない攻撃事例が見つかっています。

スウェーデンの自動車メーカーであるVolvo社は、ランサムウェア攻撃グループ"Snatch"の攻撃被害に遭いました。Snatchは、Volvo社より盗み出したデータの一部を、自身が運営するリークサイトで公開しました。BleepingComputer [65]の記事によると、Snatchは「データの暗号化を行わない」と表明しているため、Volvo社の事件でもデータの暗号化は行われなかったと推測しています。Snatchは、被害者が身代金を支払われなかった場合は、盗み出したデータを第三者へ販売するおそれがあります。

2020年に米国の財務省外国資産管理局（OFAC）が身代金の支払いを規制する勧告 [66]が発表したこともあり、ランサムウェア攻撃グループへ身代金を支払わない組織が増えてきました。また、日本国内においても、身代金の支払いを拒否する事例がありました。徳島県つるぎ町立半田病院は2021年10月にランサムウェア被害に遭い、電子カルテを暗号化されてしまいましたが、身代金支払いを拒否した上で自力での復旧の道を選択しました [67]。暗号化した情報を脅迫する手法の場合は、身代金支払いを拒否されるとランサムウェア攻撃グループは利益を上げることができません。その結果、身代金を要求する従来型のランサムウェア攻撃の収益化が難しくなってきています。

ランサムウェア攻撃グループは、身代金が支払われなくても利益を確保するために、身代金要求以外で収益を確保する手段へシフトしていくと予測します。たとえば、Snatch攻撃グループのように、企業から大量の情報を詐取していれば、その情報を換金できる可能性があります。仮に詐取した情報がクレジットカード番号などの決済情報や、ID/パスワードリストなど換金性の高い情報であれば、ランサムウェア攻撃グループは身代金に依存せずとも収益をあげることが可能になるかもしれません。今後、ランサムウェア攻撃グループが、詐取した情報の販売など身代金要求以外のサブプランを用意することや、あるいはセキュリティ対策の裏をかいた新たな収益モデルの攻撃手段を開発する可能性も十分に考えられます。今は、その過渡期にあるといえるでしょう。

ランサムウェア感染時の身代金支払いの動向

ランサムウェア攻撃では、攻撃者は企業の資産である情報が入ったファイルを暗号化して、復号のための支払いを身代金として要求します。米国財務省外国資産管理局（OFAC）や警察など様々な組織から身代金を支払わないようにという規制や指示が出ているものの、身代金を支払う企業は後を絶ちません [68]。身代金を支払うケースがなくならない理由の一つとして身代金の支払いに対応したサイバー保険があるからです。この保険に加入している組織は自社で費用を掛けてシステムを復旧するより早く、かつ安く解決できるため、身代金の支払いを選択します。
しかし、このサイバー保険で身代金を支払う方法は、使えなくなるかもしれません。2020年の米国TOP10のサイバー保険会社のうち、4社は収益が赤字でした [69]。特に米国はランサムウェアをはじめとするサイバー攻撃が多く発生していることから、ランサムウェア関連の保険金の支払いが増えていると推測できます。さらに、ランサムウェアの攻撃者は、保険会社からサイバー保険の顧客リストを窃盗し、身代金を保険金で支払える企業へターゲットを定めてランサムウェア攻撃を行っていると話しています [70]。もしこのまま保険会社の赤字が拡大すれば、保険会社はランサムウェアの身代金を保険金支払いの特約をやめてしまうかもしれません。もしそうなれば、ランサムウェア被害にあった企業の多くは、身代金を支払わなくなると予測します。身代金の支払いが大幅に減れば、ランサムウェア攻撃も大幅に減る可能性があります。

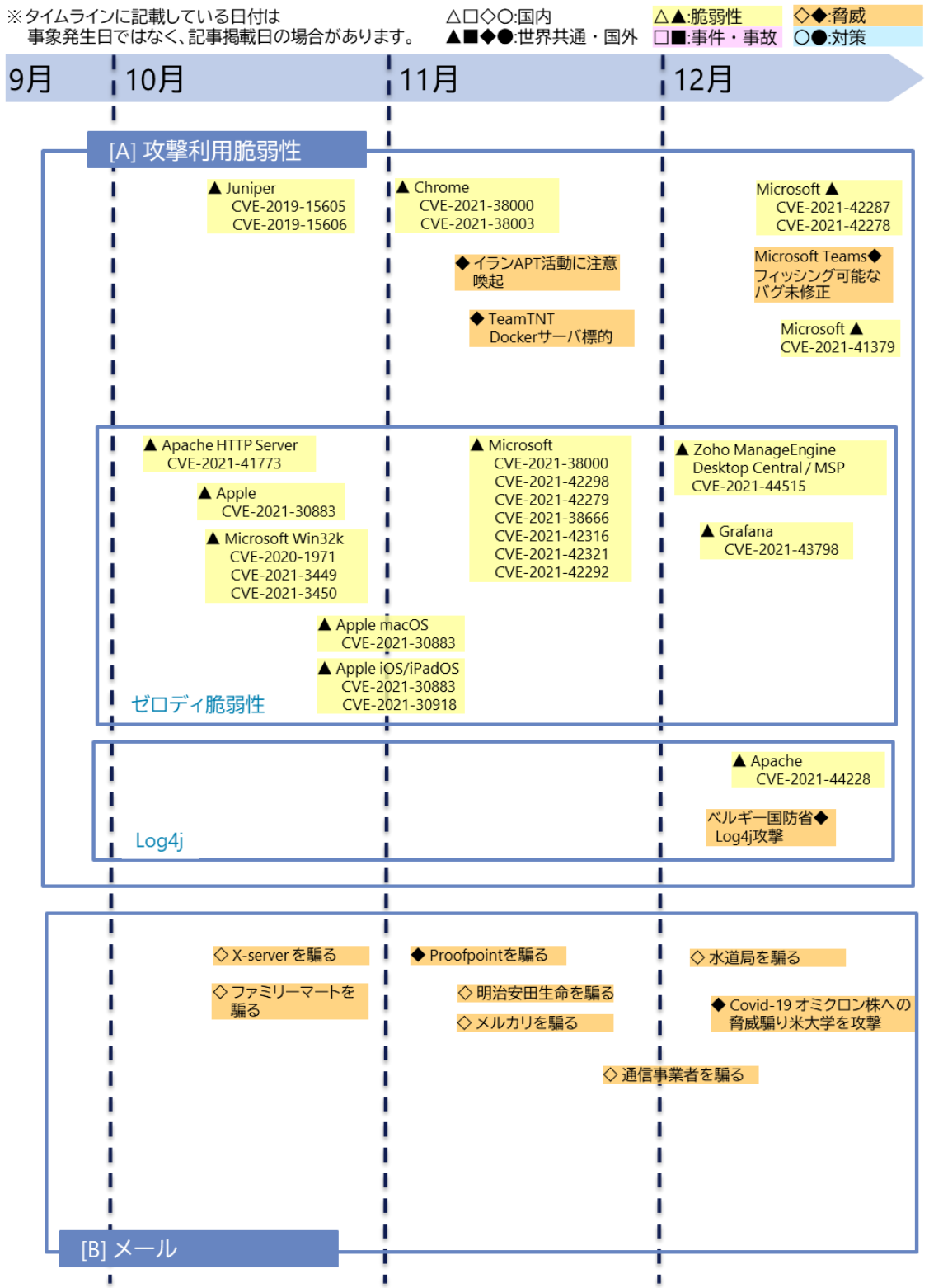
Phishing as a Service(PHaaS)の活性化

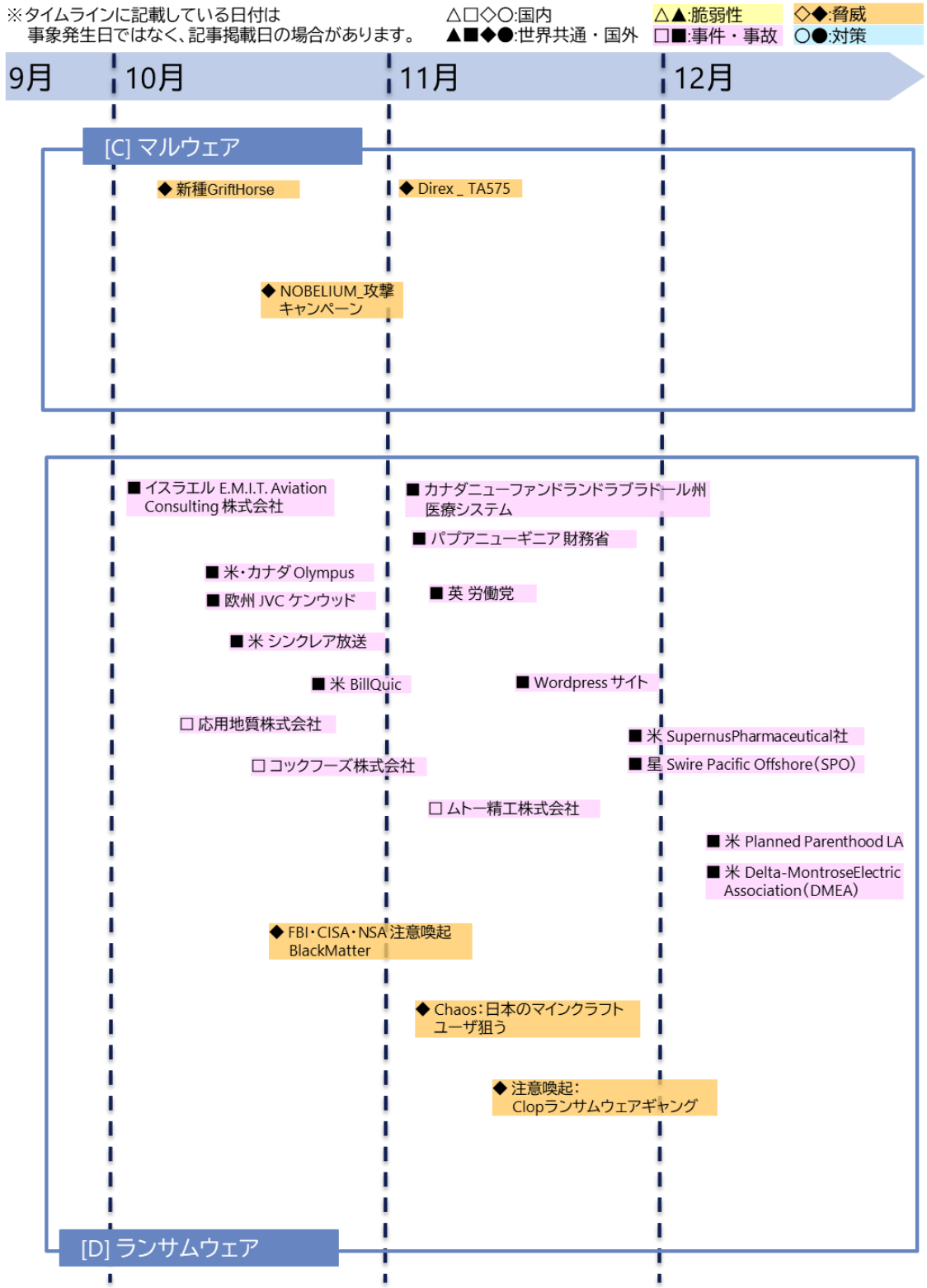
コロナ禍でのリモートワークの増加により、自宅や社外の出先からインターネット経由で社内システムへVPN接続したりMicrosoft365などのクラウドサービスを利用したりする機会が増えました。このような状況に応じて、社内システムに侵入することを目的としたフィッシング攻撃が一般化しています。フィッシング攻撃により企業関連のアカウントのIDとパスワードを詐取されてしまった場合、たとえば、攻撃者が重要なシステムへ不正ログインしてランサムウェア攻撃を行なえば、個人のフィッシング詐欺被害の場合とは比較にならない被害が発生します。

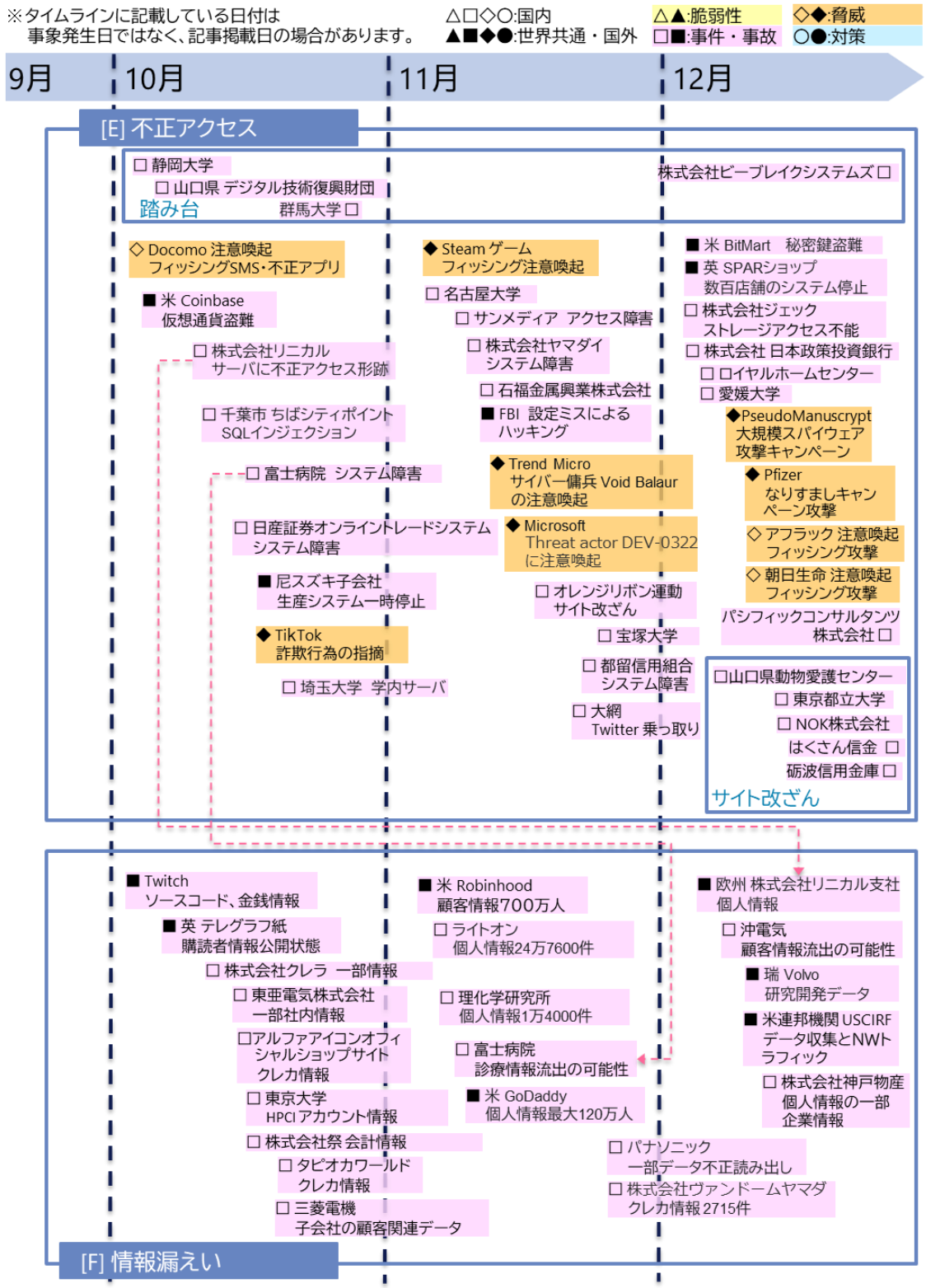
攻撃者がフィッシング攻撃を実行するためには、ID/パスワードを詐取するフィッシングサイトの構築や、そのサイトへ誘導するためのフィッシングメールの作成と送信先のアドレス収集、大量のメール送信など、準備に手間と時間が掛かります。このようなフィッシング攻撃に必要な作業をas-a-Serviceで提供するビジネスがPhishing as a Service（PHaaS）です。アンダーグラウンドの世界では、PHaaS専門の業者も生まれています。中には、as-a-Serviceの名のとおり、攻撃者のニーズに応じて、フィッシングに必要なそれぞれのプロセスを、機能単位にこまかく分割してサブスクリプション形式で提供する業者も存在します。すでに攻撃者が、精巧なフィッシング攻撃を効率的に行えるエコシステムが形成されています。こう

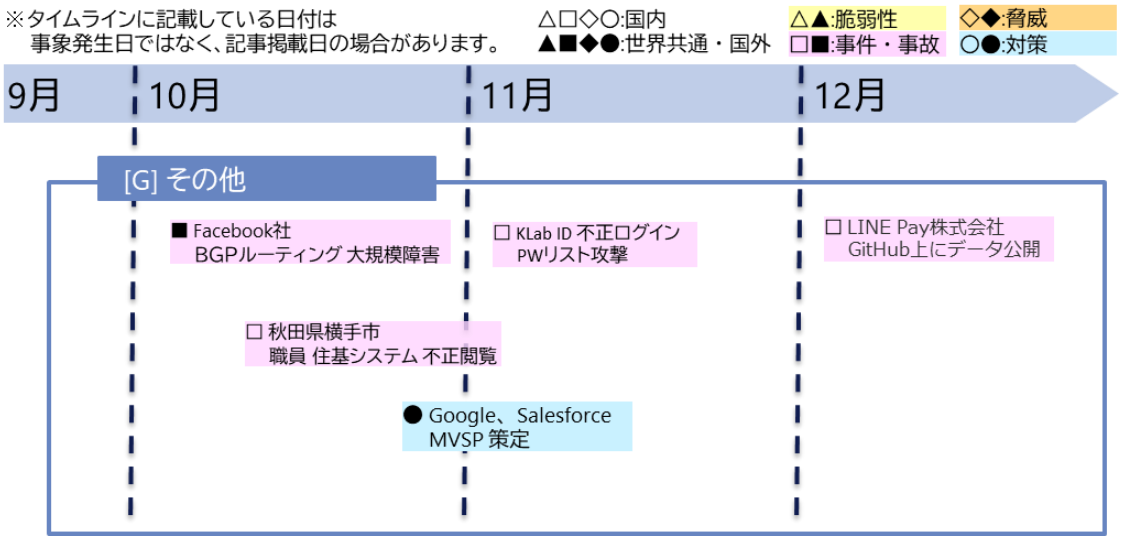
いったPHaaSビジネスが活性化すればするほど、フィッシング被害も拡大していくと推測します。

7.タイムライン









参考文献

[1] The Apache Software Foundation, “Apache Log4j Security Vulnerabilities,” [オンライン]. Available: https://logging.apache.org/log4j/2.x/security.html#CVE-2021-44832.

[2] Google, “Google Online Security Blog: Understanding the Impact of Apache Log4j Vulnerability,” 17 12 2021. [オンライン]. Available: https://security.googleblog.com/2021/12/understanding-impact-of-apache-log4j.html.

[3] Swiss Government Computer Emergency Response Team, “Zero-Day Exploit Targeting Popular Java Library Log4j,” 12 12 2021. [オンライン]. Available: https://www.govcert.admin.ch/blog/zero-day-exploit-targeting-popular-java-library-log4j/.

[4] Japan Vulnerability Notes(JVN), “Apache Log4jにおける任意のコードが実行可能な脆弱性,” 13 12 2021. [オンライン]. Available: https://jvn.jp/vu/JVNVU96768815/.

[5] The Apache Software Foundation, “APACHE LICENSE, VERSION 2.0,” 1 2004. [オンライン]. Available: https://www.apache.org/licenses/LICENSE-2.0.

[6] NTTデータ, “サイバーセキュリティに関するグローバル動向四半期レポート（2020年10月～12月）,” 16 3 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/news/information/2021/031600/.

[7] National Telecommunications and Information Administration(United States Department of Commerce), “SOFTWARE BILL OF MATERIALS,” [オンライン]. Available: https://www.ntia.gov/SBOM.

[8] 経済産業省, “『第３層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性,” 13 12 2021. [オンライン]. Available: https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/daisanso/pdf/005_03_00.pdf.

[9] R. Hansen, “Google Security Blog,” Google, 27 10 2021. [オンライン]. Available: https://security.googleblog.com/2021/10/launching-collaborative-minimum.html.

[10] 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3四半期）,” 16 3 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2020_3q_securityreport.pdf.

[11] MVSP, “Minimum Viable Secure Product,” 27 10 2021. [オンライン]. Available: https://mvsp.dev/.

[12] MVSP, “MVSP FAQ,” MVSP, 27 10 2021. [オンライン]. Available: https://mvsp.dev/faq.en/index.html.

[13] MVSP, “MVSP Checklist,” MVSP, 27 10 2021. [オンライン]. Available: https://mvsp.dev/mvsp.en/index.html.

[14] Center for Internet Security, “CIS Critical Security Controls Version 8,” Center for Internet Security, 18 5 2021. [オンライン]. Available: https://www.cisecurity.org/controls/v8.

[15] 独立行政法人情報処理推進機構, “システム構築の上流工程強化（非機能要求グレード）,” 独立行政法人情報処理推進機構, 18 9 2019. [オンライン]. Available: https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html.

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

[17] 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 2021 年度第 1 四半期,” 2 11 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2021_1q_securityreport.pdf.

[18] 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 2021 年度第 2 四半期,” 18 1 2022. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2021_2q_securityreport.pdf.

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

[20] ニュースガイア株式会社, “保育関係者向けサイトに不正アクセス - クレカやアカウント情報が流出,” 6 7 2021. [オンライン]. Available: https://www.security-next.com/127865.

[21] 株式会社コスモス薬品, “弊社が運営する「コスモスオンラインストア」への不正アクセスによるお客様情報流出に関するお詫びとお知らせ,” 12 7 2021. [オンライン]. Available: https://www.cosmospc.co.jp/notice/upload/ed661581b067c469eb29047679fa8a86e6446fe7.pdf.

[22] ニュースガイア株式会社, “革製品通販サイトに不正アクセス - クレカ情報流出の可能性,” 13 7 2021. [オンライン]. Available: https://www.security-next.com/128099.

[23] ニュースガイア株式会社, “読売関連会社のネットショップに不正アクセス - クレカ情報が被害,” ニュースガイア株式会社, 14 7 2021. [オンライン]. Available: https://www.security-next.com/128114.

[24] 株式会社キ ャ ン デ ィ ル, “当社子会社が運営するオンラインショップへの不正アクセスによる個人情報漏洩に関するお詫びとお知らせ,” 20 7 2021. [オンライン]. Available: http://fs.magicalir.net/tdnet/2021/1446/20210719469018.pdf.

[25] 有限会社毎日元気 , “弊社が運営する「毎日元気公式ショッピングサイト」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 21 7 2021. [オンライン]. Available: https://www.mainichigenki.co.jp/210721.pdf.

[26] 株式会社 SONS-MARKET, “弊社が運営する「KQLFT TOOLS」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 26 7 2021. [オンライン]. Available: https://kqlft.com/card.pdf.

[27] 株式会社フクヤ, “弊社が運営するオンラインショップへの不正アクセスによる個人情報流出に関するお詫びとご報告,” 株式会社フクヤ, 16 8 2021. [オンライン]. Available: https://www.fancy-fukuya.co.jp/topics/news20210816/.

[28] ギャップインターナショナル株式会社, “クレジットカード情報流出に関するお詫びとお知らせ,” ギャップインターナショナル株式会社, 18 8 2021. [オンライン]. Available: https://thehairbar.jp/blogs/news/information001.

[29] 株式会社コマキ楽器, “弊社が運営する「コマキ楽器WEBサイト」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 株式会社コマキ楽器, 23 8 2021. [オンライン]. Available: https://komakimusic.co.jp/pages/important-notices.

[30] 株式会社たち吉, “お詫びとお知らせ　「たち吉オンラインショップ」への不正アクセスによる個人情報漏えいについて,” 株式会社たち吉, 7 9 2021. [オンライン]. Available: https://www.tachikichi.co.jp/2021/09/07/%e3%81%8a%e8%a9%ab%e3%81%b3%e3%81%a8%e3%81%8a%e7%9f%a5%e3%82%89%e3%81%9b/.

[31] 株式会社関谷食品, “弊社が運営する「伊勢せきやオンラインショップ」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 株式会社関谷食品, 14 9 2021. [オンライン]. Available: https://www.sekiya.com/notice/.

[32] 東芝テック株式会社, “株式会社ジーアールが運営する「オムニＥＣ」への不正アクセスについて,” 東芝テック株式会社, 16 9 2021. [オンライン]. Available: https://www.toshibatec.co.jp/information/20210916_01.html.

[33] 株式会社アイコンズ, “弊社が運営する「アルファアイコンオフィシャルショップサイト」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 20 10 2021. [オンライン]. Available: https://alphaicon.com/uploads/news/file/00000/131/691ecdadfd5530d9f1e034aed6e4532a.pdf.

[34] 株式会社ネットタワー, “弊社が運営する「www.tapiocaworld.jp」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 25 10 2021. [オンライン]. Available: https://www.tapiocaworld.jp/topics_detail.html?info_id=29.

[35] タナックス株式会社, “弊社が運営する「TANAXオンラインショップ」への不正アクセスによる 個人情報漏えいに関するお詫びとお知らせ,” 27 10 2021. [オンライン]. Available: https://www.tanax.co.jp/motorcycle/topics/900.html.

[36] 株式会社ベイシア, “弊社「ベイシアネットショッピング」委託先への不正アクセスによるお客様情報流出に関するお詫びとお知らせ,” 1 11 2021. [オンライン]. Available: https://www.beisia.co.jp/wp-content/uploads/2021/11/c9f3e8b196c27d7f25d6e823c664f247-1.pdf.

[37] 株式会社エンドレス, “弊社が運営する「パーツクラブ オンライン」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 1 11 2021. [オンライン]. Available: https://cdn.shopify.com/s/files/1/0554/1009/8341/files/211101.pdf?v=1637726561.

[38] 株式会社かねたや家具店, “弊社が運営する「オンラインショップ」への不正アクセスによる個人情報漏洩に関するお詫びとお知らせ,” 28 10 2021. [オンライ

ン]. Available: https://www.kanetaya.com/infomation2021.pdf.

[39] 株式会社リンクイット, “弊社が運営する「LINK IT MALL」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 4 11 2021. [オンライン]. Available: https://www.boujeloud.com/c/information/card.

[40] 株式会社杏林堂薬局, “「杏林堂（公式）オンラインショップおよび「店頭予約者情報」への不正アクセスによるお客様情報漏えいに関するお詫びとお知らせ,” 10 11 2021. [オンライン]. Available: https://www.kyorindo.co.jp/news/pdf/kyorindo_online_news.pdf.

[41] グラントマト株式会社, “不正アクセスによる個人情報流出の可能性に関する調査結果のご報告,” 15 11 2021. [オンライン]. Available: https://www.grantomato.jp/topics/topics.php?id=687.

[42] 有限会社トコちゃんドットコム, “弊社が運営する「トコちゃんドットコムＥＣサイト」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 15 11 2021. [オンライン]. Available: https://tocochan.com/info/information.pdf.

[43] 株式会社芝寿し, “弊社「芝寿しオンラインショップ」委託先への不正アクセスによる お客様情報流出に関するお詫びとお知らせ,” 30 11 2021. [オンライン]. Available: https://www.online-shibazushi.com/user_data/20211130_oshirase.pdf.

[44] 株式会社グラウンドワークス, “弊社株式会社グラウンドワークスが運営す「EVANGELION STORE(オンライン)」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ,” 30 11 2021. [オンライン]. Available: https://www.evastore.jp/.

[45] 株式会社イーシーキューブ, “EC-CUBE 2系における複数の脆弱性(JVN#75444925),” 11 11 2021. [オンライン]. Available: https://www.ec-cube.net/info/weakness/20211111/.

[46] JVN, “EC-CUBE 2系における複数の脆弱性,” 11 11 2021. [オンライン]. Available: https://jvn.jp/jp/JVN75444925/.

[47] E. V. Kumar, “[Security advisory for CVE-2021-44526 and CVE-2021-44515] Authentication bypass vulnerabilities in ServiceDesk Plus and Desktop Central,” Zoho ManageEngine, 6 12 2021. [オンライン]. Available: https://pitstop.manageengine.com/portal/en/community/topic/security-advisory-for-cve-2021-44526-and-cve-2021-44515-authentication-bypass-vulnerabilities-in-servicedesk-plus-and-desktop-central.

[48] “FBI、Zoho ManageEngine Desktop Centralのゼロデイ脆弱性狙う攻撃を警告,”

TECH+, 22 12 2021. [オンライン]. Available: https://news.mynavi.jp/techplus/article/20211222-2234822/.

[49] Robert Falcone, Peter Renals, PaloAlto, “APT攻撃グループ ManageEngine への攻撃をさらに拡大 ServiceDesk Plus も攻撃の対象に,” 2 12 2021. [オンライン]. Available: https://unit42.paloaltonetworks.jp/tiltedtemple-manageengine-servicedesk-plus/.

[50] “統合エンドポイント管理（UEM）ソフト | Desktop Central (manageengine.jp),” Zoho ManageEngine, [オンライン]. Available: https://www.manageengine.jp/products/Desktop_Central/features.html?utm_source=DC-index-page-cta.

[51] FBI, “APT Actors Exploiting Newly-Identified Zero Day in ManageEngine Desktop Central,” FBI, 17 12 2021. [オンライン]. Available: https://www.ic3.gov/Media/News/2021/211220.pdf.

[52] The Record by Recorded Future, “Emotet botnet returns after law enforcement mass-uninstall operation,” 15 11 2021. [オンライン]. Available: https://therecord.media/emotet-botnet-returns-after-law-enforcement-mass-uninstall-operation/.

[53] 独立行政法人情報処理推進機構, “「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて,” 12 9 2021. [オンライン]. Available: https://www.ipa.go.jp/security/announce/20191202.html.

[54] 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.

[55] 一般社団法人JPCERTコーディネーションセンター, “マルウェアEmotetのテイクダウンと感染端末に対する通知,” 22 2 2021. [オンライン]. Available: https://blogs.jpcert.or.jp/ja/2021/02/emotet-notice.html.

[56] abuse.ch, “URLhaus,” 12 2021. [オンライン]. Available: https://urlhaus.abuse.ch/.

[57] Bleeping Computer LLC, “Emotet botnet comeback orchestrated by Conti ransomware gang,” 19 11 2021. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/emotet-botnet-comeback-orchestrated-by-conti-ransomware-gang/.

[58] BLACKBERRY.COM, “Threat Thursday: Emotet Update,” 6 1 2022. [オンライン]. Available: https://blogs.blackberry.com/en/2022/01/threat-thursday-emotet-update.

[59] 株式会社ラック, “【注意喚起】マルウェアEmotetが10カ月ぶりに活動再開、日本も攻撃対象に,” 19 11 2021. [オンライン]. Available: https://www.lac.co.jp/lacwatch/alert/20211119_002801.html.

[60] デジタルアーツ株式会社, “復活したEmotetの1か月,” 2 2 2022. [オンライン]. Available: https://www.daj.jp/security_reports/220202_1/.

[61] Zscaler, Inc., “Return of Emotet: Malware Analysis,” 13 12 2021. [オンライン]. Available: https://www.zscaler.com/blogs/security-research/return-emotet-malware-analysis.

[62] MISP Project, [オンライン]. Available: https://www.misp-project.org/.

[63] darkfeed.io, “DarkFeed DeepWeb Intelligence Feed,” [オンライン]. Available: https://darkfeed.io/.

[64] Cybereason Inc., “サイバーリーズン vs. Contiランサムウェア,” 16 02 2021. [オンライン]. Available: https://www.cybereason.co.jp/blog/ransomware/5760/.

[65] “BleepingComputer,” 10 12 2021. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/volvo-cars-discloses-security-breach-leading-to-randd-data-theft/.

[66] 米国財務省外国資産管理局(OFAC), “Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,” 1 10 2020. [オンライン]. Available: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

[67] 時事通信社, “サイバー攻撃で診療停止　電子カルテ、２カ月使えず―病院に「身代金ウイルス」・徳島,” 24 1 2022. [オンライン]. Available: https://www.jiji.com/jc/article?k=2022012400094.

[68] “サイバー攻撃、半数が要求応じる,” 共同通信社, 18 6 2021. [オンライン]. Available: https://nordot.app/778459067998420992.

[69] “7 Major Cyber Insurers Form Company to Coordinate Cyber Analysis, Risk Mitigation,” INSURANCE JOURNAL, 21 6 2021. [オンライン]. Available: https://www.insurancejournal.com/news/national/2021/06/21/619446.htm.

[70] “‘I scrounged through the trash heaps… now I’m a millionaire:’ An interview with REvil’s Unknown,” The Record, [オンライン]. Available:

https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/.

[71] C. Tills, “CVE-2021-44515: ZoHo Patches ManageEngine Zero-Day Exploited in the Wild,” tenable, 6 12 2021. [オンライン]. Available: https://www.tenable.com/blog/cve-2021-44515-zoho-patches-manageengine-zero-day-exploited-in-the-wild.

[72] “APT Expands Attack on ManageEngine With Active Campaign Against ServiceDesk Plus,” palo alto networks, 2 12 2021. [オンライン]. Available: https://unit42.paloaltonetworks.jp/tiltedtemple-manageengine-servicedesk-plus/.

[73] Robert Falcone, Peter Renals(paloaltonetworks), “APT攻撃グループ ManageEngine への攻撃をさらに拡大 ServiceDesk Plus も攻撃の対象に (paloaltonetworks.jp),” 2 12 2021. [オンライン]. Available: https://unit42.paloaltonetworks.jp/tiltedtemple-manageengine-servicedesk-plus/.

NTT DATA
Trusted Global Innovator

2022年3月15日発行

株式会社NTTデータ
セキュリティ技術部
大谷 尚通 / 小林 義徳 / 大石 眞央 / 山下 大輔
大山 千尋 / 伊藤 友洋 / 佐藤 可奈子 / 内藤 航 / 西塚 大貴 / 清水 一貴 / 宮崎 大輔
nttdata-cert@kits.nttdata.co.jp