NTT DATA
Trusted Global Innovator

# グローバルセキュリティ動向四半期レポート

## 2020 年度 第 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。

## 活発化するサプライチェーン攻撃

第3四半期は複数の組織がサプライチェーン攻撃の被害を受けました。なかでもSolarWinds社に対するソフトウェアサプライチェーン攻撃が大きな話題となりました。このように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いるため、日本国内では、2020年10月30日に経済産業省が「サプライチェーン・サイバーセキュリティ・コンソーシアム（Supply Chain Cybersecurity Consortium: SC3）」を設立しました。このようにサプライチェーン攻撃に対する関心が高まりつつあります。

攻撃者は、サプライチェーン全体の中のセキュリティ対策が不十分な部分から侵入します。よってサプライチェーン攻撃の対策は、サプライチェーン全体の中から攻撃が成功するようなセキュリティ上の弱点をなくすことです。しかし委託元が委託先へセキュリティ対策を強制できなかったり、広範囲で複雑なサプライチェーン全体からすべてのセキュリティ上の弱点を見つけて対策できなかったりするため、全ての弱点をなくすことは容易ではありません。まだ、サプライチェーン攻撃の対策を効率的に構築できる決定的な方法は完成していません。そのため、過去の複数のサプライチェーン攻撃事例を分析し、サプライチェーン攻撃のパターンとサプライチェーン全体をカバーできる対策方式を模索していく努力が必要です。

## 二重脅迫ランサムウェア攻撃の増加

ランサムウェア攻撃はデータの暗号化に留まらず、データを窃取して身代金の支払いを迫る「二重脅迫型」へと攻撃手法が進化し、攻撃事例が増加傾向にあります。ランサムウェア攻撃が増加している背景として、テレワークの拡大に伴う攻撃者の侵入経路の増加など昨今の環境変化が影響していると考えられます。CrowdStrike社による意識調査では、調査に回答した日本の組織の半数以上がランサムウェア攻撃の被害に遭い、そのうちの約3割が身代金を支払ったという結果があります。

二重脅迫ランサムウェア攻撃への対策は、被害を未然に防ぐための防御策を講じることが最も効果的ですが、攻撃者の攻撃手法も進化を続けているため、全ての攻撃を防ぐことは困難です。2020年10月に米国財務省の外国資産管理局（OFAC）から出された勧告のように、身代金の支払いは犯罪を助長する行為のため、禁止する動きが増えています。もし、二重脅迫ランサムウェア攻撃の被害に遭った場合、犯罪者の脅迫に決して屈しない強い決意をもって対応することが重要です。

## Salesforceの設定不備に起因した情報漏えい

2020年度第3四半期以降、Salesforceプラットフォームの設定不備に起因する情報漏えいが相次いで発生しました。Salesforceプラットフォームを利用している場合は、セールスフォースドットコム社の案内に従って、ゲストユーザのアクセス制御の権限設定を確認してください。

本件のような設定不備による情報漏えいは、責任共有モデルを踏まえると、クラウドサービスを利用しているクラウドサービスカスタマに責任があります。しかし本件は、クラウドサービスプロバイダであるセールスフォースドットコム社の対応が不足していたことが原因のひとつと考えられます。クラウドサービスを安全に利用するために、クラウドサービスプロバイダは、クラウドサービスカスタマが設定不備を起こさないようにサポートし、クラウドサービスカスタマは、クラウドサービスの仕様をよく理解して利用すべきです。

## 予測

Salseforceのインシデントのようなクラウドサービスプロバイダ側も対応が必要な事象アは、対策が不十分なクラウドサービスプロバイダが存在すると想定されることから、今後も発生すると考えられます。また、多数発生したサプライチェーン攻撃については、別の攻撃を行うために、複数の組織を経由するサプライチェーン攻撃を仕掛けなければならなくなります。そのため、検知を回避するための隠蔽技術が更に発達していき、企業が攻撃を検知することがより困難になると推測されます。

2020年度第3四半期には、ビットコインの市場価格が過去最高値を記録して、上昇傾向にあります。今後、上昇傾向だった2019年前半と同様に、暗号通貨を狙った攻撃が発生するかもしれません。

# 2. 注目トピック

## 2.1. 活発化するサプライチェーン攻撃

2020年度第2四半期に引き続き、サプライチェーン攻撃による被害事例が、多数報告されています。過去の四半期レポートでも、何度かサプライチェーン攻撃に関してご紹介してきましたが、ますますその攻撃が高度化、巧妙化している傾向にあります。

表 1 ： 2020年度第3四半期に発生･報告されたサプライチェーン攻撃

| 日付 | 対象(委託元) | 対象(委託先) | 概要 |
|---|---|---|---|
| 11/17 ※ | サービス利用組織 | 日本 /イベント管理/ Peatix Japan株式会社 | Peatix Japan株式会社にて、10月16日から10月17日にかけて不正アクセスが発生した。この影響により、Peatix Japan株式会社の管理するユーザの個人情報が最大677万件引き出された [1] |
| 11/26 ※ | 日本/音楽/株式会社エブリシングジャパン | 日本/アプリ運営/株式会社Dear U | 株式会社Dear Uにて、第三者からの不正アクセスが発生した。この影響により、株式会社エブリシングジャパンが運営を委託していたカラオケアプリ「エブリシング」に対し、11月5日から11月10日の期間に会員が登録した個人情報707件が流出した [2] |
| 12/11 ※ | 日本/発電システム/三菱パワー株式会社 | 日本/情報通信/株式会社日立システムズ | 三菱パワー社が利用するマネージドサービスプロバイダー経由の不正アクセスが発生した。この影響により、同社のサーバ1台が侵入され、IT関連の情報が流出した [3] |
| 12/13 ※ | ソフトウェア(OrionPlatform)利用組織 | アメリカ/ソフトウェア開発/SolarWinds, Inc | SolarWinds社のネットワーク管理ソフト「Orion Platform」を悪用したサイバー攻撃が発生した。この影響により、最大で1.8万社に被害が出たおそれがあるとみられている [4] |

※公表日

この4件の中で特に大きく話題となったのは、SolarWinds社の事例です。現在のところ、被害組織の約8割は米国であると報告されていますが、日本でも多くの企業がSolarWinds社の製品を導入しており、すでにこの攻撃によるマルウェアの感染が検知されています。このサプライチェーンを悪用した攻撃の被害は、今後もさらに拡大するおそれがあるため注意が

必要です。

サプライチェーン攻撃に対して、日本では2020年10月30日に経済産業省が「サプライチェーン・サイバーセキュリティ・コンソーシアム（Supply Chain Cybersecurity Consortium: SC3）」の設立を公表 [5]しました。SC3は、多様な産業分野の組織が集まって、サプライチェーン攻撃に対するサイバーセキュリティ対策の推進をめざす団体です。また、情報処理推進機構（IPA）が2019年と2020年に公表した「情報セキュリティ 10大脅威」では、サプライチェーンの弱点を突いた攻撃が4位にランクインしています。ますますサプライチェーン攻撃に対する注目が高まっています [6]。

## 2.1.1. サプライチェーン攻撃とは

デジタルトランスフォーメーションが進む中、IT業務のアウトソース、ITシステムの構築や運用・保守の外部委託、ソフトウェアの調達など、IT業務に関わるサプライチェーンが拡大しています。そのようなIT業務のサプライチェーンは、業界にとらわれず多くの企業が攻撃のターゲットになるおそれがあります。

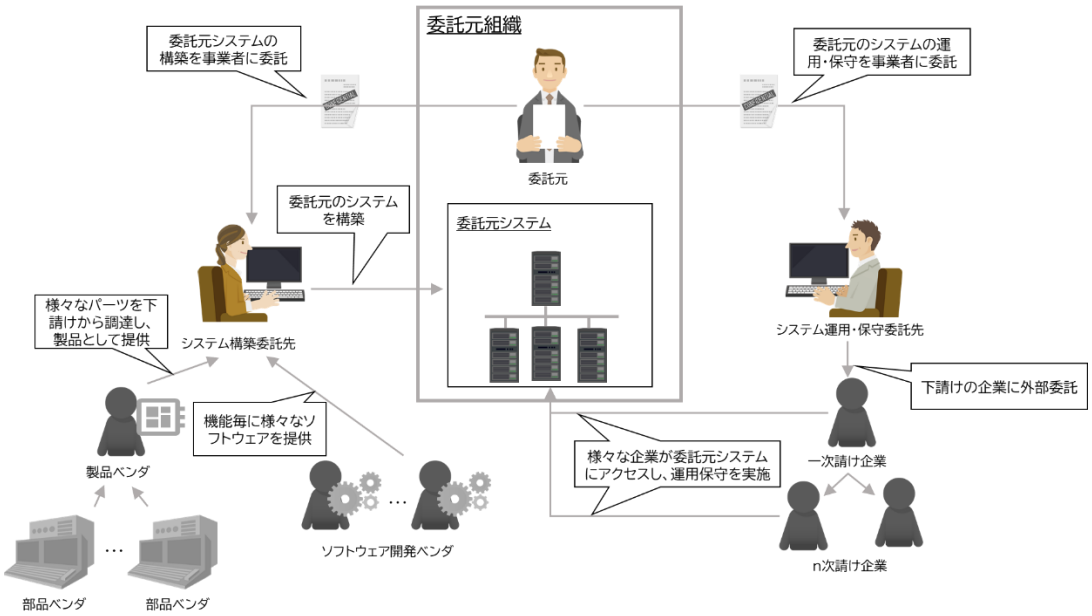



図 1 ： ITにおけるサプライチェーンの例

企業は、攻撃者が用いるサプライチェーン攻撃の手法を把握して、サプライチェーン攻撃の対策を進めなければなりません。以降で、サプライチェーン攻撃の3つの手法を具体的に紹介します。

### 2.1.1.1. サプライチェーン攻撃の手法

過去の四半期レポートで取り上げたサプライチェーン攻撃の事例より、サプライチェーン攻撃の手法は、大きく「①委託先を踏み台にした攻撃」、「②ソフトウェアサプライチェーン攻撃」、「③委託先からの情報窃取」の3つに分類されます。表 2に3つのサプライチェーン攻撃の事例を示します。

表 2 ： 3つのサプライチェーン攻撃手法の攻撃事例（過去の四半期レポートより）[7] [8] [9]

| 分類 | 日付 | 対象(委託元) | 対象(委託先) | 概要 |
|---|---|---|---|---|
| ①委託先を踏み台にした攻撃 | 2019/7/13※ | アメリカ/情報通信/Sprint Corporation | 韓国/電気機器/Samsung Electronics Co., Ltd. | サムスングループの公式サイトsamsung.com経由で不正アクセスを受け、Sprint社が管理する個人情報の漏えいが発生した [10] |
| | 2019/9/18※ | サービス利用組織 | ITサービス事業者(サウジアラビア) | サウジアラビアのITサービス事業者が攻撃された。この影響により、サービスを利用する11組織が攻撃を受け、少なくとも2つの組織のサーバに情報収集ツールが仕込まれた [11] |
| ②ソフトウェアサプライチェーン攻撃 | 2019/1/19※ | ソフトウェア利用組織 | PHP PEAR | パッケージ管理ツールPEARの公式サイトに攻撃が行われた形跡が見つかり、改ざんされたインストーラが置かれていたことが判明した [12] |
| | 2019/3/13※ | ソフトウェア利用組織 | Android SDK | RXDriodeという広告関連のSDKにアドウェアが仕込まれており、当該SDKを使って開発された200以上のアプリにアドウェアが埋め込まれていた [13] |
| | 2019/3/25※ | ソフトウェア利用組織 | ASUS Live Update | ASUS社製PC用の自動アップデートソフトASUS Live Updateを悪用してマルウェアが配布された [14] |
| ③委託先からの情報窃取 | 2019/7/13※ | ロシア連邦保安庁 | SyTech社 | SyTech社にて第三者からの不正アクセスが発生した。この影響により、ロシアの情報機関である連邦保安庁の情報が盗み出された [15] |
| | 2020/7/11※ | アメリカ/オークション/LiveAuctioneers | 外部(詳細未公表) | 同社が外部委託していた入札者データベースが不正アクセスを受けた。この影響により、顧客情報が漏えいした [16] [17] |
| | 2020/7/16※ | サクソバンク証券 | 外部(詳細未公表) | 外部委託していたサーバが不正アクセスを受けた。この影響により、顧客情報が漏えいした [18] [19] |
| | 2020/7/21※ | イスラエル/ビデオメーカ/Promo.com | 外部(詳細未公表) | サードパーティ・サービスの脆弱性を突かれ、ユーザレコードが漏えいした [20] [21] |

※公表日

2020年度第3四半期では、この3つの手法に該当するサプライチェーン攻撃の事例が発生しました。各事例を基に、「①委託先を踏み台にした攻撃」、「②ソフトウェアサプライチェーン攻撃」、「③委託先からの情報窃取」を紹介します。

### 委託先を踏み台にした攻撃

この攻撃は、取引先などのサプライチェーンの中のセキュリティ対策が甘い組織を攻撃の足がかりにして、大企業や政府組織など標的の組織を攻撃して不正アクセスする手法です。三菱パワー社の攻撃事例は、「委託先を踏み台にした攻撃」に該当します。同社は、2020年12月11日にマネージド・サービス・プロバイダ（以下「MSP」という）を経由で第三者から不正アクセスを受けたことを公表しました [3]。翌日の12月12日に日立システムズ社の運用監視サービスを経由した攻撃であることが報道されました [22]。以下にその侵入経路を示します。

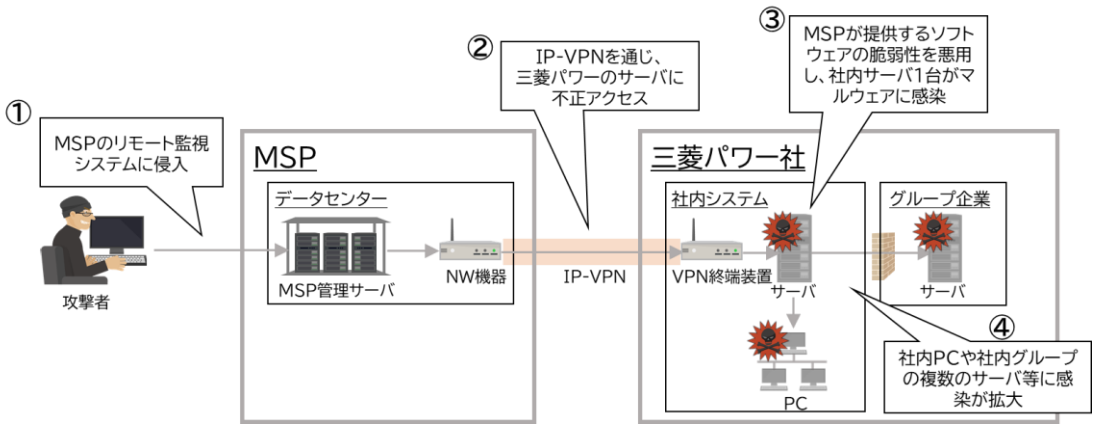



図 2 ： 三菱パワー社が受けた一連の攻撃の流れ

攻撃者は、日立システムズ社が顧客のシステムを監視するための運用監視システムに侵入し（1）、そこを経由して、三菱パワー社のサーバへ不正アクセスしました（2）。その後、日立システムズ社が提供するソフトウェアの脆弱性を悪用し、社内サーバ1台へマルウェアを感染させました（3）。更に社内ネットワークのファイアウォールが適切に設定されていなかったため、マルウェアが社内のPCやグループ企業の複数のサーバへ感染拡大しました（4）。

この攻撃による機密性の高い技術情報、取引先に係る重要なビジネス情報、個人情報の流出はありませんでしたが、サーバの設定情報、アカウント情報、認証処理プロセスのメモリダンプ等のIT関連情報が流出しました。

### ソフトウェアサプライチェーン攻撃

この攻撃は、ソフトウェアの開発元や配布元などソフトウェアのサプライチェーンを通じて、マルウェアや攻撃コードを挿入したソフトウェアを配布して攻撃の足がかりにする手法

です。2020年12月13日に公表されたSolarWinds社の攻撃事例 [4]は、「ソフトウェアサプライチェーン攻撃」に該当します。攻撃者は、同社が手掛けるネットワーク管理およびリモート監視ソフトウェア「Orion Platform」へトロイの木馬型マルウェア「SUNBURST」を仕込んで、正規アップデートを悪用して利用者へ配布しました。SUNBURSTが含まれたこのソフトウェアは、Symantecにより発行されたSolarWinds社のコード署名が行われていたため、利用者は、ウイルス対策ソフト等でもこのソフトウェアが感染していることを検知できず、感染が拡大してしまいました。以下にその流れを示します。

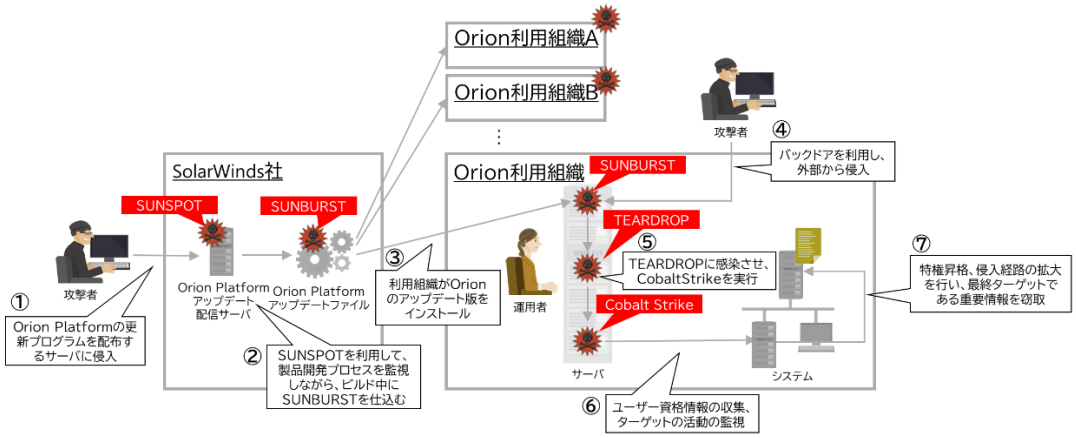



図 3 ： SolarWinds社から発生した一連の攻撃の流れ

攻撃者は、まず初めにSolarWinds社のOrion Platformソフトウェアの更新プログラムを配布するサーバに侵入しました（1）。次に「SUNSPOT」と呼ばれるマルウェアでOrion Platformのビルドに関係するプロセスをモニタリングして、ビルドの隙きを突いて製品のソースコードファイルをトロイの木馬型マルウェア「SUNBURST」のコードを混入させたファイルへ置き換えました（2）。その後、1万8000社を超える組織が、マルウェアが混入したOrion Platformソフトウェアのアップデート版をインストールしました（3）。SUNBURSTには、バックドア機能が含まれており、攻撃者はこれを利用して、インターネット上からマルウェアが混入したOrion Platformソフトウェアを使用しているシステムへ侵入しました（4）。SUNBURSTは、自身が動作中のマシン内へ攻撃者のサーバからプログラムをダウンロードしたり、任意のプログラムを実行したりできる機能を持っています。攻撃者は、これらの機能を使用して当該マシンへもう一つのマルウェア「TEARDROP」を感染させます。TEARDROPは、ペネトレーションテストツール「Cobalt Strike」をメモリ上へダウンロードして実行します。攻撃者は、Cobalt Strikeを使ってユーザ資格情報の収集や当該マシンの活動を監視できるようになります（5）。その結果、攻撃者は、当該マシンでの特権昇格と他のマシンへの侵入を繰り返し行っていき（6）、最終的に重要情報の窃取を行った（7）ことが確認されています。

SolarWinds社が米証券取引委員会（SEC）に提出した資料によると [23]、SUNBURSTが仕込まれたのは2020年3月から6月までの更新プログラムであり、当該更新プログラムをインストールした組織は1万8000以上にまで及ぶとされています。そのなかには、サイバーセキュリティ企業として世界的にも有名なFireEye社も含まれます。FireEye社は、この攻撃によって自社製のペネトレーションテストツールや政府機関を含む顧客に関する情報が盗まれました [24]。

**委託先からの情報窃取**

この攻撃は、セキュリティ対策が不十分な委託先を狙って、委託先が委託元から預かっている個人情報や重要情報を窃取する手法です。2020年11月17日に公表されたPeatix Inc.の攻撃事例 [1]や、2020年11月17日に公表されたDear U社の攻撃事例 [2]が「委託先からの情報窃取」に該当します。例えば、委託元がシステムの構築を社外組織へ委託している場合、システムの仕様などの機密情報が委託元から委託先へ提供されます。また、委託元が、委託先が提供するクラウドサービスを利用している場合、同サービス上に個人情報や重要なビジネス上の機密情報が保存されるケースがあります。厳重に対策されている委託元のシステムよりもセキュリティ対策が不十分な委託先やクラウドサービスは、攻撃者にとって侵入しやすい環境です。

## 2.1.1.2. サプライチェーン攻撃の危険性

サプライチェーン攻撃の恐ろしいところは、サービスを受ける側がそのリスクを完全にコントロールすることが困難な点にあります。

例えば、委託元は、委託先のセキュリティ対策を細かくアセスメントしたり、指示したり、強制したりできません。契約条件に含める方法もありますが、様々な面で限界があり自社と同等のセキュリティをコントロールすることが困難です。それに増して、委託先がクラウドサービスの場合は、複数の顧客向けに同一の仕様のサービスを提供しているため、委託元個社の要求に対応できません。そのような背景から、委託先におけるセキュリティリスクが見過ごされ、「①委託先を踏み台にした攻撃」、「③委託先からの情報窃取」を受ける結果に繋がります。

更に「①委託先を踏み台にした攻撃」では、攻撃者が委託先を経由して委託元へ不正アクセスしても、委託元は委託先を信頼しているため、高度な振る舞い検知をおこなっていなければ、委託元は不正アクセスを検知することが困難です。また、特に注意しなければならないケースは、三菱パワー社の攻撃事例のように、攻撃者がマネージドサービスプロバイダ（MSP）を経由する攻撃です。最近の傾向として、攻撃者は運用監視システムを狙っています。運用監視システムは、セグメント分割の少ない運用管理ネットワークを使って、裏側からシステムへ接続します。そのため、攻撃者は、運用監視システムを乗っ取ることができれば、そのシステムの様々な機器へ容易に侵入して、活動の範囲を広げることが可能です。攻撃者がMSPの不正アクセスに成功すれば、多くの組織の情報資産が攻撃を受けて被害が発生

します。

「②ソフトウェアサプライチェーン攻撃」には、次に述べる危険性があります。ユーザは普段から広く普及しているソフトウェア製品の開発元を信用しているため、その開発元からダウンロードした製品のアップデートプログラムを躊躇せずにインストールします。もし開発元の提供するアップデートプログラムを信頼しないユーザがいたとしても、アップデートプログラムを解析して不正な処理を発見することは非常に困難です。SolarWinds社のように、多くのユーザが利用している有名なソフトウェアであればあるほど、攻撃者が侵入に成功したときの被害が大きくなります。つまり「②ソフトウェアサプライチェーン攻撃」は、有名な信頼されているソフトウェア製品が侵害された場合は、ユーザがほぼリスクをコントロールすることができません。

## 2.1.2. サプライチェーン攻撃への対策

サプライチェーン攻撃においては、あらゆる対象を攻撃の手段として利用されるおそれがあります。そのため、グループ会社やビジネスパートナー、あるいは自組織でさえ、疑いの目をもってリスクを考えることが重要です。

例えば、サプライチェーンとの通信において、その通信は安全なのか、詐称する第三者ではないか、または、自組織で取り扱っているアプリケーション、データ、ハードウェアは実はマルウェアに感染していて、既に攻撃者がシステムに攻撃しているのではないかといった疑問を持ち、自組織の資産や外部/内部の通信をすべて検証する意識を持つことも重要となります。このように、自組織が管理している通信、資産の信頼性が十分であると過信せずに、自組織におけるサプライチェーン攻撃のリスクを整理し、その上で対策の検討を行う考え方は非常に重要です。また、「②ソフトウェアサプライチェーン攻撃」や、注意が必要なMSPを踏み台にした「①委託先を踏み台にした攻撃」の特徴から、サプライチェーン攻撃においては委託先、すなわちソフトウェア開発元、あるいはサービス委託先が最初に狙われる傾向があります。

以降では、ソフトウェア開発、サービス委託、それぞれの視点からのセキュリティ対策の例を紹介しますが、数あるサプライチェーン攻撃のリスクを低減するための一部であることに留意してください。

### 2.1.2.1.ソフトウェア開発におけるセキュリティ対策

ここでは、ソフトウェア開発元において検討すべき対策について紹介します。過去に発生したソフトウェアサプライチェーン攻撃の事例でも、本件のSolarWinds社の攻撃事例でも、2つの原因が共通します。攻撃者がビルド環境へ侵入できたこと、攻撃者がアップデートプログラムへマルウェアを混入させて配布できたことです。この2つの共通する原因の対策を強化することが、委託先がソフトウェアサプライチェーン攻撃を防止するための対策であると考えます。SolarWinds社の攻撃事例にて、これらの原因に対する要因と、考えられる対策を紹介します。

① ビルド環境へ侵入

まだ調査中で明確な原因は不明ですが、攻撃者が多要素認証をバイパスして侵入した、またはGitHubの脆弱なFTPパスワードを突破して侵入したと推測されています。SolarWinds社が米国証券取引委員会へ報告した資料やVolexity社の情報 [25]によると、攻撃者が多要素認証システムDuo Securityの統合秘密鍵を入手して、認証を迂回してあるユーザになりすまして侵入したおそれがあります。その結果、攻撃者はSolarWinds社の正規ユーザになりすますことに成功したと思われます。

まずはソフトウェア製品の開発元は、一般的に知られている脆弱性や攻撃方法では侵入できないように、ビルド環境へのリモートアクセス方式のセキュリティを十分に確保すべきです。また多要素認証を導入していても、攻撃者がそれを迂回して侵入するケースが増えてきました。多要素認証を迂回されたり突破されたりするリスクの検討も始めましょう。

② アップデートプログラムへのマルウェアの混入と配布

攻撃者がマルウェアの混入と配布ができた原因は、アップデートプログラムを改ざんできる権限を奪取できたことと、改ざんしたアップデートプログラムへコード署名ができたことだと考えられます。

- アップデートプログラムを改ざんできる権限の奪取

  攻撃者がSolarWinds社のネットワークへ侵入する時に正規ユーザになりすますことに成功したのであれば、その時点で同時にアップデートプログラムを修正できる権限を取得できていたおそれがあります。その場合は、EDRを導入して、Orion Platformのビルドプロセスをモニタリングするマルウェアの振る舞いや、プログラム開発者とは異なる攻撃者の不審な振る舞いを検知して対処すべきです。もし攻撃者がアップデートプログラムを修正できる権限を取得できていなかった場合は、権限昇格などの不審な動きをEDRで検知すれば対処可能です。

  正規ユーザになりすまされてネットワークへ侵入されても、開発環境を使用するためのアカウントを別アカウント/別の認証パスワードにして開発環境をもう一段階セキュリティレベルが高い区画に設定する方法も有効です。ただし、まだ明確な原因が不明なため、原因の判明後に再検討が必要かもしれません。

- 改ざんしたアップデートプログラムへコード署名

  改ざんされたアップデートプログラムは、Symantecから発行されたSolarWinds社のコードサイニング証明書でコード署名が行われていました。攻撃者は、SolarWinds社のコードサイニング証明書を盗み出したか、または乗っ取ったユーザ権限を使ってコード署名できたと推測されます。

  コードサイニング証明書の管理が不十分で、攻撃者に盗まれて悪用されたのであれば、HSMで管理すべきです。場合によっては、コード署名できるユーザを少人数に限定したり、ユーザ2名揃わないと署名できない仕組みにしたりしなければならない

かもしれません。

これら2つの共通する原因の対策を強化することが、委託先がソフトウェアサプライチェーン攻撃を防止するための対策ではないでしょうか。

## 2.1.2.2.サービス委託におけるセキュリティ対策

委託先を踏み台にした攻撃のうち、三菱パワー社の攻撃事例では、攻撃者が委託先である日立システムズ社の運用監視システムへ侵入できてしまったことが1つ目の原因です。2つ目の原因は、攻撃者が権限のあるアカウントを使えたと思われる点です。これら2つの原因には、外部からのアクセス制御、アカウント等の重要資産に対する保護、不正な特権昇格の防止等、様々な対策が考えられます。

サプライチェーンで連携した個々の組織がそれぞれリスク分析や対策を行って十分な水準のセキュリティを確保できたとしても、どこか一つでも対策が不十分な組織があれば、サプライチェーン攻撃が成功してしまいます。そのため、繋がっている全ての組織やネットワーク、システムを抜け漏れなく対策しなければなりません。この場合、①委託元のガバナンスを委託先まで強制できるケースと②強制できないケースが存在します。以下にそれぞれの具体的な対策を挙げます。

① 委託元のガバナンスを委託先まで強制できるケース

委託元と同じ社内やグループ会社へ委託する場合は、サプライチェーン全体を把握して、委託元のセキュリティ対策を委託先へ適用して一括管理できる場合があります。例えば、すべての取引先から業務手順やセキュリティ対策内容を開示させて妥当性をチェックしたり、委託元のセキュリティ対策を委託先へ導入させたりします。委託先は自組織の従来のセキュリティ対策に加えて追加対策を受け入れなければならないため、一般的には非常に大きな負担が伴います。委託元と委託先が同じ社内やグループ会社の場合は、セキュリティポリシや対策方針が統一されているため、この方法に対応できる場合があります。

近年では、複雑なサプライチェーン全体のセキュリティ対策状況を一元管理し、弱点や攻撃を受けやすいポイントを可視化するサービスがあります。そのようなサービスを利用することも有効です。

② 委託元のガバナンスを委託先まで強制できないケース

委託元が社外組織へ委託する場合は、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べきです。委託先のサプライチェーン攻撃に対する安全性を確認、判断する方法を以下に挙げます。

- サプライチェーン攻撃の「①委託先を踏み台にした攻撃」「②ソフトウェアサプライチェーン攻撃」「③委託先からの情報窃取」について、具体的なセキュリティ対策の状況を確認する。

セキュリティ対策状況の確認後、サプライチェーン全体のセキュリティ対策に不足があると判断した場合、対策の抜け漏れを防ぐために、以下の手順の流れにしたがってセキュリティ対策を検討します。

I. サプライチェーン全体からリスクを洗い出す。
II. リスクを防ぐ/軽減するセキュリティ対策を挙げる。
III. 委託元と委託先でセキュリティ対策の実施主体や責任範囲、それに応じたセキュリティ対策の分担を明確に定める。
IV. 委託元と委託先は、それぞれセキュリティ対策を実施する。

上記と併せて、委託先のISMS、プライバシーマーク等の第三者認証の取得状況を確認する方法もあります。ただし、セキュリティ認証だけでは委託先の安全性が確保できない場合もありますので、補足的な手段としてご検討ください。

ここまでで挙げた対策を実施しても、サプライチェーン全体のセキュリティ対策の抜け漏れ/リスクの残存を解消できない場合は、委託元が対策を追加することも検討します。たとえば、以下のような方法があります。

- 攻撃者が委託先を経由して攻撃するおそれを考慮して、自システムにおける攻撃に対する検知力を高める
- 委託先へ提供した情報が漏えいするおそれを考慮して、予め連携先に提供する情報を必要最低限に留める

## 2.1.3. まとめ

グローバルセキュリティ動向四半期レポート 2020年度版 第2四半期 [9]にて、サプライチェーン攻撃が今後も引き続き継続すると予測しました。その予測通り、第3四半期も複数の組織がサプライチェーン攻撃の被害を受けました。特にSolarWinds社のサプライチェーン攻撃事例は、SolarWinds社の新CEOが、「攻撃の種類、規模と潜在的なダメージを考えると、歴史上最も複雑で洗練されたサイバー攻撃の一つである」と述べています [26]。また、攻撃者は、三菱パワー社のサプライチェーン攻撃の事例 [3]のようにMSPへ侵入してから、運用管理システムを踏み台にして、ターゲット組織のシステムへ侵入するという、効率の良い方法を見つけました。

本記事で紹介した対策や様々な組織から提供されているサプライチェーンマネジメントに関するガイドラインや対策フレームワークを参考にサプライチェーン攻撃の対策を進めなければはなりません。サプライチェーン攻撃は、あらゆる所に発生リスクが潜んでいるため、組織は従来の自組織内の対策だけでなく、委託先を含んだより広い範囲の対策を考える必要があります。このような広範囲で複雑なサプライチェーン全体を効率的に対策できる決定的な方法は、まだ完成していません。これまでの複数のサプライチェーン攻撃事例を分析して、サプライチェーン攻撃のパターンとサプライチェーン全体をカバーできる対策方式を少しずつ作り上げていくのでしょう。

# 2.2. 二重脅迫ランサムウェア攻撃の増加

## 2.2.1. 二重脅迫ランサムウェア攻撃の概況

ランサムウェア攻撃による被害事例は以前より報告されていましたが、2020年度第3四半期においても国内、国外を問わず多数の被害事例が報告されています。特に二重脅迫するランサムウェア攻撃による被害事例が、多く報告されていました。二重脅迫するランサムウェア攻撃は、データを暗号化して解除のための身代金を要求するだけでなく、身代金を支払わなければ窃取したデータを公開すると二重に脅します。本稿は、今後も被害が拡大するおそれがある二重脅迫ランサムウェア攻撃を取り上げます。2020年度第3四半期の二重脅迫ランサムウェア攻撃に関する被害事例を下記、表 3に示します。

表 3 ： 二重脅迫ランサムウェア攻撃の事例

| 公開日 | 組織 | 概要 |
|---|---|---|
| 10/22 | 塩野義製薬<br>（日本の製薬会社） | 塩野義製薬の台湾現地法人がランサムウェア攻撃を受けパソコンを使用不能とされた上、盗まれた情報の一部（医療機器の輸入許可証や社員の在留許可証）がインターネット上に公開され、金銭を支払わなければ、さらに情報を暴露すると脅された [27] [28] |
| 10/27 | エネルグループ<br>（イタリアのエネルギー会社） | 2020年6月に続き、2020年10月に2度目のランサムウェア攻撃に見舞われた。数TBのデータが暗号化され、さらに窃取された。身代金1400万ドルを支払わなければデータを公開すると脅迫を受けた [29] |
| 11/3 | カンパリ<br>（イタリアの飲料ベンダー） | ファイルを復号するための身代金1500万ドルを要求した。また、最初の侵入から1週間以内に身代金要求を支払わなかった場合、カンパリのネットワークから盗んだファイルを公開すると脅迫した。犯罪グループは、データが危険にさらされていることと、カンパリが支払いを拒否していることをFacebookの広告で掲載した [30]。 |
| 11/12 | カプコン<br>（日本のゲームメーカー） | サイバー犯罪グループから盗まれた機密情報と引き換えに、多額の金銭（11億円）を要求された。11/11朝以降、情報の一部とみられるファイルが公開された [31] |

## 2.2.2. 二重脅迫ランサムウェア攻撃とは

① 二重脅迫ランサムウェア攻撃の概要 [32]

データのバックアップを厳重に行うなどランサムウェア攻撃への対策が進む中、攻撃者はデータを暗号化したあとに、データを窃取して身代金を支払わない場合に公開すると被害者を二重に脅迫するランサムウェア攻撃の事例が増加しています。従来のランサムウェア攻撃と二重脅迫ランサムウェア攻撃の違いをそれぞれ下記、図 4及び図 5に示します。

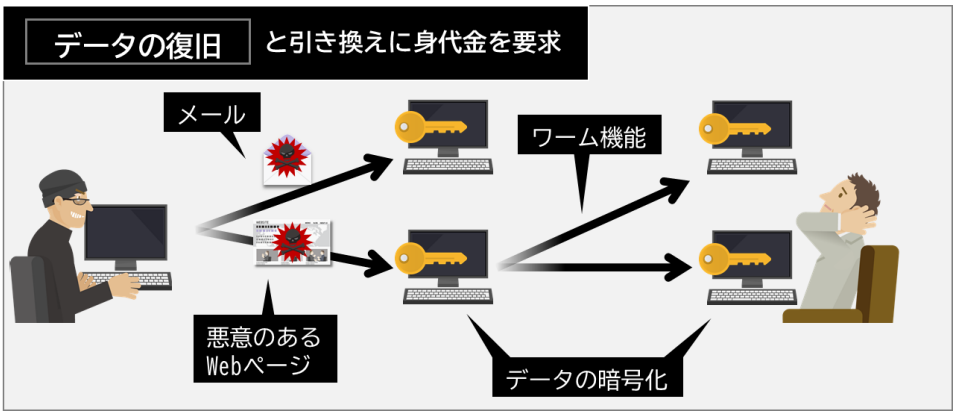



図 4 ： 従来のランサムウェア攻撃

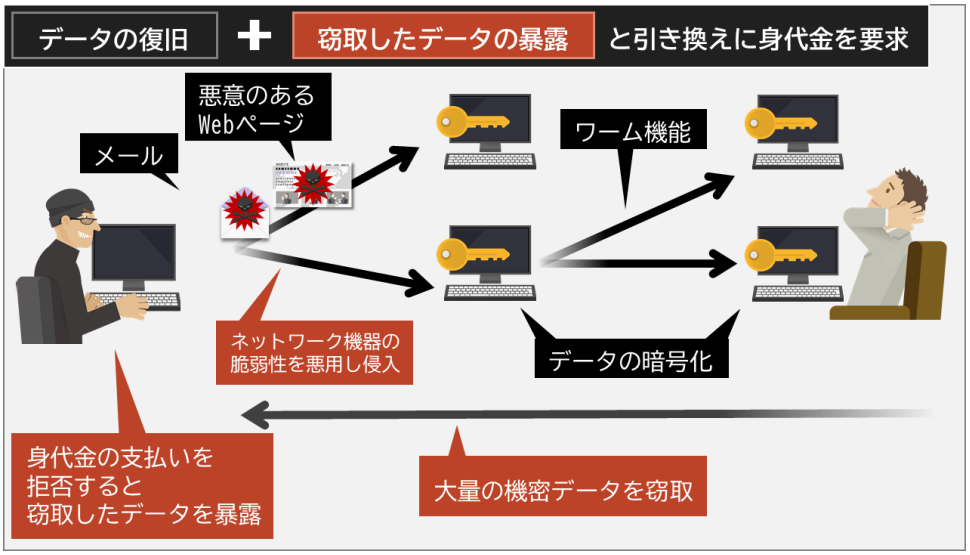



図 5 ： 二重脅迫ランサムウェア攻撃

② カプコン社の二重脅迫ランサムウェア攻撃の被害

2020年11月16日、日本の大手ゲームメーカーであるカプコン社が、標的型攻撃を受けてオーダーメイド型ランサムウェアに感染して、9人分の個人情報が流出したことを発表しま

した。2021年1月12日にも新たに16,406人分の個人情報の流出が確認されたことを発表しています。また、流出したおそれがある個人情報は最大約39万人であると公表しており、今後さらに被害が拡大するおそれがあります [33] [34]。

カプコン社は、同11月4日に第三者から不正アクセスを受けて2020年11月2日にシステム障害が発生したと発表しています。その後の調査で、システム障害の原因はランサムウェア攻撃であることが判明しました。カプコン社は、2020年11月16日にランサムウェア攻撃の被害状況を発表しました。サーバに保存された情報が暗号化されたり、アクセスログが削除されたりしたため、調査や解析に時間がかかったとカプコン社は説明しています [33] [35]。

犯行グループである「Ragnar Locker」は、カプコン社の日本、米国、カナダのネットワークへ侵入し、約2,000台のデバイス上のファイルを暗号化し、1TBを超えるデータを盗んだと主張しています。また攻撃者は、暗号化したデータの復号と窃取したデータの削除のために、ビットコインで1100万ドルの支払いを要求しました [36]。カプコン社は身代金の支払いを拒否し、大阪府警に通報しています。カプコン社が支払いを拒否したため、犯行グループは、表 4に示した情報をダークウェブ上に公開しました。 [37]

表 4 ： 流出を確認した情報

| 発表日 | 情報種別 | 情報詳細 |
|---|---|---|
| 11/16 | 個人情報 | ● 元従業員の個人情報（5件）<br>① 氏名、サイン：2件<br>② 氏名、サイン：2件<br>③ 氏名、住所：1件<br>④ パスポート情報：2件<br>● 従業員の個人情報（4件）<br>① 氏名、人事情報：3件<br>② 氏名、サイン：1件 |
| | その他 | ● 販売レポート<br>● 財務情報 |
| 1/12 | 個人情報 | ● 取引先等の個人情報：3,248人<br>氏名、住所、電話番号、メールアドレス等のうち1つ以上<br>● 退職者及び関係者の個人情報：9,164人<br>氏名、メールアドレス、人事情報等のうち1つ以上<br>● 社員及び関係者の個人情報：3,994人<br>氏名、メールアドレス、人事情報等のうち1つ以上 |
| | その他 | ● 売上情報、営業情報、開発資料、取引先情報等 |

表 5 ： カプコン社のランサムウェア攻撃の時系列状況

| 日付 | 状況 |
|---|---|
| 11/2 | 未明に社内システムへの接続障害を確認、システムを遮断し被害状況の把握に着手。カプコンを標的としたランサムウェアがサーバ上のファイルを暗号化したことを確認。「Ragnar Locker」と名乗る集団からの脅迫メッセージから身代金要求が判明。大阪府警に通報 |
| 11/4 | カプコン社が「不正アクセスによるシステム障害発生に関するお知らせ」を公表 |
| 11/9 | Ragnar Lockerがリークサイトでカプコンに対する脅迫メッセージを掲載 [38] |
| 11/11 | Ragnar Lockerがリークサイトでカプコンから窃取したデータを公開 [38] |
| 11/12 | カプコン社が9件の個人情報、及び一部の企業情報の流出を確認 |
| 11/16 | カプコン社が流出した情報9件以外に流出のおそれのある情報を公表 |
| 1/12 | カプコン社は新たに16,406人の情報流出を確認し、流出したおそれのある情報は最大約39万人であることを公表。Ragnar Lockerはリークサイトにおいて、12/11の時点で11回、あわせて200GB近くのデータを公開している [39] |

③ 二重脅迫ランサムウェア攻撃増加の背景 [40] [41]

ランサムウェア攻撃がデータを窃取して身代金の支払いを迫る「二重脅迫型」へと進化を遂げて、攻撃が増加している背景には、被害者、攻撃者双方におけるビジネス環境の変化があると考えられます。

- テレワークの拡大に伴う侵入経路の増加

従来のランサムウェア攻撃では、攻撃者はメールを使用して感染させる攻撃手法を用いていました。近年、攻撃者はネットワーク機器の脆弱性を悪用しネットワーク内部に侵入して感染させる攻撃手法を取り始めています。2019年は「VPN」に関連する脆弱性が多数明らかとなっています。2020年に入ると新型コロナウイルス感染拡大の影響もあり、テレワークが広がる中で突貫工事によるテレワーク環境の導入が進み、脆弱性を対処しないままのネットワーク機器が使用されました。そのような状況だったため、ネットワーク機器の脆弱性を狙ったランサムウェア攻撃が拡大したと考えられます。

- ランサムウェア攻撃のビジネス化

「Ransomware as a Service(以下、RaaSという)」は、ランサムウェアに感染させて身代金を得ようとする攻撃者に対して、ランサムウェア本体やダウンローダー、C&Cサーバなどの機能を持ったインフラを提供します。RaaSは、使用期間、使用できる機能などで差をつけ、数万円から数十万円でダークウェブ上に販売されています。攻撃者がランサムウェアのプログラミングなど特別な開発技術力が無くても、RaaSを購入すれば容易にランサムウェア攻撃

を行うことが可能です。また、頻繁に機能追加が行われているRaaSもあり、今後も攻撃者にとって魅力的な機能が追加されるおそれもあります。RaaSはビジネスとして成立してしまっており、攻撃増加の一因になっていると考えられます。

- 安価な大容量ストレージの普及

二重脅迫ランサムウェア攻撃では、攻撃者が一度に数十から数百GB、時には数TB単位の大量データを窃取します。暗号化したデータの復号と引き換えに脅迫する従来のランサムウェア攻撃の手法が長年の主流であり、大量データの窃取まで行うことは稀でした。近年、安価で大容量のクラウドストレージサービスが登場したため、攻撃者は盗み出した大容量データを容易に保管できるようになりました。この安価な大容量ストレージサービスの普及が、二重脅迫ランサムウェア攻撃の拡大を後押ししたと考えられます。

## 2.2.3. 二重脅迫ランサムウェア攻撃にどう対応するべきか

① 身代金を支払う企業の割合 [42] [43] [44]

CrowdStrike社は、世界12か国の企業のIT関連部門の意思決定者とITセキュリティ担当者2,200人（うち日本は200人）を対象にセキュリティ調査を実施しました。その2020年度版グローバルセキュリティ意識調査の結果より、以下のランサムウェア攻撃による被害の調査結果が公表されています。

- ✓ 質問に回答した日本の組織の半数以上（52%）が過去1年間にランサムウェア攻撃の被害に遭い、うち28%は2回以上の攻撃を受けた
- ✓ ランサムウェア攻撃の被害にあったと回答した日本の組織のうち、42%は攻撃者と交渉を試み、32%が身代金を支払った
- ✓ 被害にあったと回答した日本の組織が攻撃者に支払った身代金の平均額は117万ドル（約1億2,300万円）

調査に回答した日本の組織の半数以上がランサムウェア攻撃の被害があったと回答するなど、ランサムウェア攻撃による被害が顕著であることがわかります。同調査によると、ランサムウェア攻撃のリスクを懸念している世界中の組織の回答者の割合は、2019年「42%」から2020年「54%」へと急増しています。日本の組織の回答者の68%が新型コロナウイルス（COVID-19）に関連したランサムウェア攻撃のリスクへの懸念が高まっていると回答しています。また世界的にも、ランサムウェア攻撃のへ対策方法は、ランサムウェア攻撃の未然防止ではなく、感染後にデータを復旧するための犯人との交渉に論点がシフトしつつあります。

② 身代金支払い時の注意点 [45]

- 身代金を支払えばデータが戻るのか

ランサムウェア攻撃を受けるとシステムの動作に必要なファイルも暗号化されてしまい、

システムに障害が発生して業務が停止するおそれがあります。重要なシステム、停止時間に比例して被害額が大きくなるシステムであれば、身代金を支払ってでも復旧する方が被害額を小さくできる場合があります。そのような場合、多くの組織は身代金を支払うこと選択するでしょう。実際に上記のCrowdStrike社による意識調査の結果の通り、多数の組織が身代金を支払っています。

身代金を支払う相手は犯罪者です。たとえ身代金を支払ったとしてもデータが戻る保証はありません。トレンドマイクロ社の調査によると、身代金を支払った組織の5社に1社はデータを取り戻せていません。データが返却されたとしても、そのデータが改ざんされていない保証はありません。財務情報などデータによっては、改ざんされていないことを保証できなければ、返却されたとしてもデータの価値はありません。また、たとえデータが返却されて改ざんされていなかったとしても、データがコピーされていれば、復号のための身代金を支払った後に、再びそのデータの公開を脅迫されるおそれがあります。一度、身代金を支払った組織は、支払い実績のある組織として攻撃者同士のネットワークで共有され、別の攻撃者から標的にされるおそれもあります。また、ランサムウェアへの感染原因が判明していない場合、同じ手段により再度侵害を受けるおそれがあることも認識する必要があります。

- 身代金の支払いはテロリストの支援となりうる [46] [47] [48]

2020年10月1日、米国財務省の外国資産管理局（OFAC）は、金融機関、サイバー犯罪向けのセキュリティ保険会社などランサムウェア被害者の身代金支払いを支援する企業は、OFAC規則に違反するおそれがあり、以下の制裁の対象となると勧告しました。

- ✓ 犯罪者へ身代金支払いを助けることは、犯罪者に利益を与え、違法な目的を助長し、アメリカの安全保障と外交政策の目的に反する活動に資金を提供することになる。OFACの規則に違反するため、罰金や制裁の対象とする
- ✓ ランサムウェア攻撃の被害が出た際は、法執行機関に報告して全面的に協力すること

上記勧告は、支払った身代金がテロリストなどの危険な犯罪組織に渡った場合、そのような組織を助長したと見なし、身代金を支払った企業に制裁を科すおそれがあることを示しています。アメリカでは2019年7月の全米市長会議の第87回年次総会において、ランサムウェアによる攻撃を受けても身代金を支払わないという決議案に220人を超える市長が署名しました。これは身代金の支払いを拒否することで攻撃者の攻撃意欲をくじく目的がありました[49]。今回の勧告は、身代金を支払わないという流れをさらに押しすすめるものと考えられます。米国の法律が及ぶ範囲の組織において、ランサムウェア攻撃の被害を受けて、身代金を支払うかどうか組織として検討する場合は、上記OFACの勧告を考慮する必要があります。

③　二重脅迫ランサムウェア攻撃の被害を防ぐためにどうするべきか [50] [51] [52]

ランサムウェア攻撃による被害が深刻化し、被害内容も複雑になっています。ランサムウェア攻撃による重大な被害を出さないために、企業・組織としてできる限りの対策を講じる

ことが重要となります。

カプコン社の二重脅迫ランサムウェア攻撃事例のように、攻撃者は標的型サイバー攻撃と同様の攻撃手法で企業・組織のネットワークへ侵入して二重脅迫ランサムウェア攻撃を行う事例が増えています。そのような二重脅迫ランサムウェア攻撃は、主に以下の4つのステップの戦術が使われます。

1. ネットワークへの侵入
2. ネットワーク内の侵害範囲拡大
3. データの窃取
4. データの暗号化

米国MITRE社が、攻撃者のサイバー攻撃手法をまとめた「ATT&CK」 [53]というナレッジを公開しています。「ATT&CK」は、Tactic（戦術：攻撃者の目的）、Tacticを実現するためのTechnique（攻撃手法）、そしてTechniqueへの対策となるMitigation（緩和策）/Detection（検知手法）から構成されています。上記の標的型サイバー攻撃に類似した二重脅迫ランサムウェア攻撃の4つのステップに該当する「ATT&CK」を使って、自組織向けの二重脅迫ランサムウェア攻撃対策を講じましょう。

## 2.2.4. まとめ

ランサムウェア攻撃は情報処理推進機構（IPA）により選出される情報セキュリティ10大脅威に過去数年10位以内にランクインし続けていますが、その攻撃手法は「ばらまき型」から特定の組織を狙った「標的型」、そしてデータを窃取して身代金の支払いを迫る「二重脅迫型」へと進化しています。CrowdStrike社の調査結果では、回答した日本の組織のうち、ランサムウェア攻撃の被害にあった組織の約3割が身代金を支払っています。しかしながら、2020年10月の米国財務省の外国資産管理局（OFAC）の勧告のように、身代金の支払いは犯罪を助長する行為のため、禁止する動きが増えています。二重脅迫ランサムウェア攻撃による被害を出さないためにも、企業・組織としてできる限りの防御対策を講じておくことが最も効果的ですが、攻撃手法も進化をしているため100%防ぐことは難しいと思われます。二重脅迫ランサムウェア攻撃による被害を受けたとしても、犯罪者の脅迫には絶対に屈しないという強い決意を持ち、インシデント対応に臨むことが重要と考えます。

# 3. 情報漏えい

2020年度第3四半期は、Salesforceの設定不備に起因する情報漏えいが相次いで発生しました。本件のようなクラウドサービス経由の情報漏えいは、責任の所在が問題になります。本章では、Salesforceの設定不備に起因する情報漏えいの概要とクラウドサービス利用時のセキュリティの考え方である責任共有モデルについて解説します。

## 3.1. Salesforce経由の情報漏えい

2020年12月、PayPay社および楽天社は、クラウド型営業管理システムの設定不備により、情報が漏えいしたおそれがあると公表 [54] [55]しました。PayPay社、楽天社ともに、既に海外の第三者から不正アクセスがあったことを公表しています。両社は、セールスフォースドットコム社のSalesforceプラットフォーム上のクラウド型営業管理サービスを利用していたと報道 [56]されており、設定不備の原因は、製品刷新時におけるセールスフォースドットコム社の情報発信が不足していたという報道 [57]もされています。また、第4四半期に入ってからも、Salesforceプラットフォームの設定不備による情報漏えいが相次ぎ報道 [58]されています。こうした状況を受けて、金融庁およびNISCは、セールスフォースドットコム社のクラウド型営業管理サービスの設定不備の注意喚起 [59] [60]を発出しています。

セールスフォースドットコム社は、以下の製品または機能において、第三者が一部の情報を閲覧できることを公表 [61]しました。

- コミュニティ
- Salesforceサイト（旧 Force.com サイト）
- Site.comのサイト上に構築する公開サイト機能

本件の事象が発生するおそれがあるSalesforceプラットフォームを利用している場合は、セールスフォースドットコム社の案内（https://www.salesforce.com/jp/company/news-press/stories/salesforce-update/）に従って、ベストプラクティスを参考にゲストユーザのアクセス制御の権限設定を確認してください。もし自社で確認できない場合は、セールスフォースドットコム社のSalesforceヘルプからケースを起票するか、導入に関わったSIパートナー等への問い合わせを実施してください。

セールスフォースドットコム社は、本件の事象について、以下のように公表しています。

- 本件の事象は、製品の脆弱性に起因するものではない
- ゲストユーザのアクセス制御の権限設定が不適切な場合に発生した事象である
- 利用者は、ゲストユーザのアクセス制御の権限設定が適切か確認する必要がある

- 本件の事象について、製品アップデート時に設定が変わった等の事実はない
- 製品アップデートに合わせて、標準のリリースノートを公開している

本件の事案では、Salesforceプラットフォームを利用した公開サイト等において、認証が不要なゲストユーザのアクセス制御の権限設定が不適切であったために、ゲストユーザがアクセス制限された情報を参照できてしまいました。よってSalesforceプラットフォームのアクセス制御の権限を適切に設定できていれば問題はありません。しかし、同様の事案が相次いで発生していることから、セールスフォースドットコム社の対応が不十分だったおそれも考えられます。本件の情報漏えいの責任の所在は、クラウドサービスにおける責任共有モデルや発生原因を踏まえて考える必要があります。

## 3.2. 責任共有モデル

クラウドサービスにおけるセキュリティは、責任共有モデル（図 6）という責任分担の考え方が基本となっています。責任共有モデルとは、クラウドサービスを提供するクラウドサービスプロバイダとクラウドサービスを利用するクラウドサービスカスタマで、クラウドサービス利用時に責任をもつ範囲を明確にするための考え方です。本件の事案であれば、クラウドサービスプロバイダがセールスフォースドットコム社で、クラウドサービスカスタマはPayPay社・楽天社となります。責任共有モデルは、クラウドサービスの種類によって、以下のように大きく分類されます。また、責任範囲の境界のことを責任分界点と呼びます。

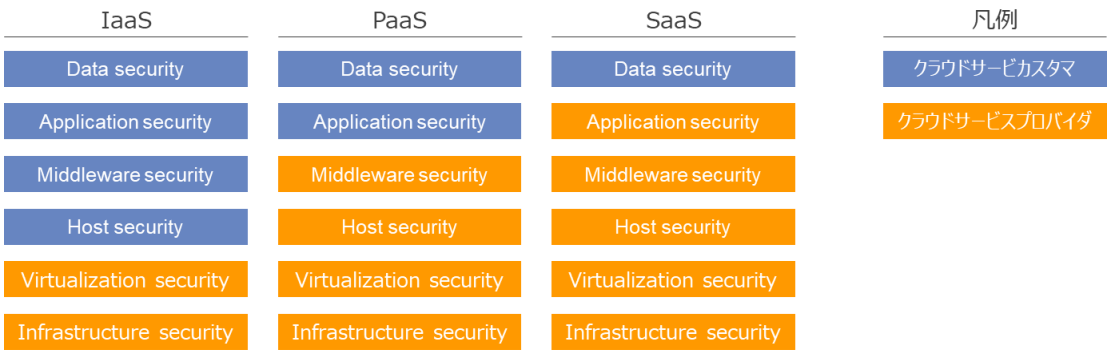



図 6 ： 責任共有モデル

出典：Cloud Security Alliance クラウドにおけるセキュリティサービスの効果的な管理のガイドライン [62]を基に作成

本件の事案は、クラウドサービスプロバイダが提供するPaaSにおける、ゲストユーザのアクセス制御の不適切な権限設定に起因した情報漏えいです。アクセス制御の権限設定は、図6のData securityに当てはまり、一義的にはクラウドサービスカスタマの責任範囲だったことがわかります。本件の情報漏えいは、クラウドサービスカスタマが、利用しているクラウドサービスをよく理解して適切に権限を設定していれば、発生しませんでした。

しかし、本件の事案は、PayPay社、楽天社だけでなく、同様の設定不備による情報漏えいのおそれが相次いで報道されており、単純な人為的ミスとは考えにくいです。セールスフォースドットコム社は、本件に関係するとされる機能追加についても、リリースノートへ記載していると主張しています。これは機能追加について、クラウドサービスカスタマに説明がされており、クラウドサービスカスタマは適切な対応が可能であるという主張と捉えることができます。しかし、多くの会社が同じ設定不備を起こしていることを踏まえると、セールスフォースドットコム社の機能追加に伴う追加設定の説明やアクセス制限の仕組みが不足していたと考えられます。情報漏えい等、重大な問題を引き起こしうる設定不備の発生を未然に防ぐことは、クラウドサービスプロバイダの注意義務と捉えることができます。特に、Salesforceプラットフォームのような広く普及しているクラウドサービスは、問題が起きた際の影響が大きいため、重大な問題を引き起こしうる設定変更の周知は重要です。注意義務を適切に果たせていない場合、設定不備による情報漏えいの責任は、不適切な設定をしたクラウドサービスカスタマだけでなく、クラウドサービスプロバイダにもあると考えます。

クラウドサービス利用時の責任は、責任共有モデルを前提に判断されるため、今回起きた情報漏えいの責任は、クラウドサービスカスタマが負うべきと考えます。しかし、本件の事象の原因は、利用しているクラウドサービスの仕様の理解が不足していたクラウドサービスカスタマおよびクラウドサービスカスタマへの説明が不足していたクラウドサービスプロバイダの双方にあります。

本件の事象のように、発生した問題の原因が双方にあっても、責任共有モデルを踏まえて、責任は一方にあると判断される場合もあります。しかし、責任範囲以外は、何も対策を講じなくてよいわけではなく、原因の一端を担うものとして、講じなければならない対策があると考えます。クラウドサービスの設定不備において、クラウドサービスプロバイダおよびクラウドサービスカスタマはどのような対策を講ずるべきか、考える必要があります。

## 3.3. 設定不備に起因した情報漏えい

Salesforceプラットフォームだけでなく、クラウドストレージ等、機密情報を格納するクラウドサービスは、設定不備によって不正アクセスや情報漏えいが発生するおそれがあります。

例えば、アクセスしたい通信ポートやファイルへアクセスできない場合に、クラウドサービスカスタマが必要以上のアクセス許可を与えて、本来であればアクセスできないユーザがその通信ポートやファイルへアクセスできてしまい、結果として不正アクセスや情報漏えいが発生します。

このような設定不備は、クラウドサービスカスタマの単純な設定ミスや仕様の理解不足によって発生するおそれがあります。クラウドサービスカスタマは、利用するクラウドサービスの仕様や設定方法を十分に理解すること、設定を変更したときは設定ミスがないようにチェックを行ってください。クラウドサービスプロバイダが提供するスキル認定資格を持った

クラウドサービスカスタマのみに操作を許可してミスを防ぐ方法もあります。設定不備を発見するためのアクセス範囲の検証テストも有効です。

クラウドサービスプロバイダは、クラウドサービスの仕様変更時にクラウドサービスカスタマの対応が限りなく少なくなるように配慮したり、初期設定を安全な値にしたり等、提供するクラウドサービスの仕組みによって、設定不備のリスクを低減することも可能です。クラウドサービスプロバイダは、クラウドサービスカスタマに対して適切な手段およびタイミングで十分な情報提供やサポートを行うことも必要です。特に、情報漏えい等の深刻な問題を引き起こしうる設定は、設定方法に関するサポート、ベストプラクティスの提示によって、クラウドサービスカスタマが不適切な設定を行わないように周知する必要があります。クラウドサービスカスタマ側で設定変更が必要な場合も、より入念なサポートや周知が必要です。

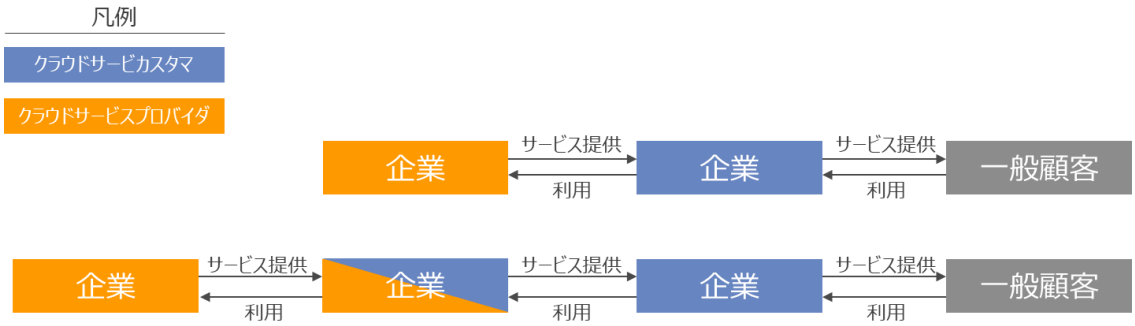



図 7 ： クラウドサービスプロバイダ/クラウドサービスカスタマ

クラウドサービスカスタマは、そのクラウドサービスを自身の顧客に提供する場合、自身がクラウドサービスプロバイダになる場合（図 7）があります。そのような場合、クラウドサービスカスタマかつサービスプロバイダであることになるため、それぞれの観点で上述のような対策を検討・実施する必要があります。

## 3.4. まとめ

Salesforceプラットフォームの設定不備は、同様の事例が相次いで確認されているため、Salesforceプラットフォームを利用している場合は、セールスフォースドットコム社の案内に従って、ゲストユーザのアクセス制御の権限設定が適切であるか確認してください。

クラウドサービスは、責任共有モデルによって責任が分担されていますが、クラウドサービスプロバイダおよびクラウドサービスカスタマの状況によっては、双方に原因がある場合もあります。クラウドサービスプロバイダは、クラウドサービスカスタマが設定不備を起こさないようにサポートする必要があります。クラウドサービスカスタマも、責任共有モデル（図 6）に基づいて自身の責任範囲とクラウドサービスの仕様をよく理解した上で、設定不備を起こさないように利用しましょう。

# 4. 脆弱性

## 4.1. 2020年度第3四半期の概況

CentOS 6のサポートが2020年11月30日に [63]、Adobe Flash Playerのサポートが2020年12月31日に終了しました [64]。今後この2つのソフトは、アップデートやセキュリティパッチの配布が行われないため、利用を停止することをお薦めします。

セキュリティ企業であるFireEye社からレッドチームが利用するツールが窃取されました。セキュリティ企業が攻撃者に侵入されたことに加えて、セキュリティ企業のツールが窃取されて攻撃に悪用されるおそれがあることが話題になりました。以降でツールの窃取による影響を述べます。

## 4.2. ツール窃取による影響

2020年12月8日に、FireEye社は標的型攻撃を受けて自社のレッドチームのツールが窃取されたことを発表しました [65]。攻撃の手口は、米国政府機関等の多くの組織が被害にあった、SolarWinds社のネットワーク管理製品であるOrion Platformのアップデートを悪用したサプライチェーン攻撃でした [66]。攻撃そのものについては「2.1活発化するサプライチェーン攻撃」に詳細を記載しているため、ここではツール窃取による影響を述べます。

窃取されたツールの利用主体であるレッドチームとは、疑似的な攻撃により企業のセキュリティ体制を評価する専門チームのことです。窃取されたツールは、このチームが疑似攻撃を行う際に利用するツールのため、既知の脆弱性を利用した攻撃コードも含まれていました [65]。攻撃者がこのツールに含まれる脆弱性を悪用すると、組織の内部へ侵入できるおそれが高く、脆弱性が未対応の組織は攻撃で大きな被害を発生するおそれがあります。表 6に、FireEye社が公開した、深刻度が高く優先的に対応が必要な脆弱性を示します。

表 6 ： FireEye社が公開した優先的に対応が必要な脆弱性の一覧 [67]

| No | CVE | 対象製品 | CVSS | 概要 |
|---|---|---|---|---|
| 1 | CVE-2019-11510 | Pulse Secure Pulse Connect Secure | 10.0 | パーミッションに関する脆弱性 |
| 2 | CVE-2020-1472 | Microsoft Windows Server | 10.0 | 権限昇格の脆弱性 |
| 3 | CVE-2018-13379 | Fortinet FortiOS | 9.8 | パストラバーサルの脆弱性 |
| 4 | CVE-2018-15961 | Adobe ColdFusion | 9.8 | 危険なタイプのファイルの無制限アップロードに関する脆弱性 |

| | | | | |
|---|---|---|---|---|
| 5 | CVE-2019-0604 | Microsoft SharePoint | 9.8 | リモートでコードを実行される脆弱性 |
| 6 | CVE-2019-0708 | Microsoft Windowsのリモートデスクトップ サービス | 9.8 | リモートでコードを実行される脆弱性 |
| 7 | CVE-2019-11580 | Atlassian Crowd および Crowd Data Center | 9.8 | 入力確認に関する脆弱性 |
| 8 | CVE-2019-19781 | Citrix Application Delivery Controller および Gateway | 9.8 | パストラバーサルの脆弱性 |
| 9 | CVE-2020-10189 | Zoho ManageEngine Desktop Central | 9.8 | 信頼性のないデータのデシリアライゼーションに関する脆弱性 |
| 10 | CVE-2014-1812 | Microsoft Windows | 9.0 | グループポリシーの実装における重要な認証情報を取得される脆弱性 |
| 11 | CVE-2019-3398 | Confluence Server および Data Center | 8.8 | パストラバーサルの脆弱性 |
| 12 | CVE-2020-0688 | Microsoft Exchange Server | 8.8 | リモートでコードを実行される脆弱性 |
| 13 | CVE-2016-0167 | Microsoft Windows | 7.8 | カーネルモードドライバにおける権限昇格の脆弱性 |
| 14 | CVE-2017-11774 | Microsoft Outlook | 7.8 | 任意のコマンドを実行される脆弱性 |
| 15 | CVE-2018-8581 | Microsoft Exchange Server | 7.4 | 権限を昇格される脆弱性 |
| 16 | CVE-2019-8394 | Zoho ManageEngine ServiceDesk Plus | 6.5 | 危険なタイプのファイルの無制限アップロードに関する脆弱性 |

2017年に大流行したWannaCryは、米国安全保障局から攻撃グループにより流出したとされるツールが悪用されました。今回の件においても、同様の事象が発生するおそれが考えられます [68] [69]。しかしWannaCry以降、その教訓に基づいて、表 6のような深刻な脆弱性で、かつ悪用が確認された脆弱性は、適切にセキュリティパッチの適用が行われるようになっています。表 6の脆弱性の多くがツール窃取前に悪用が確認されて対策がすすんでいること、ツールを悪用した攻撃が事件後に確認されていないことから、この事件により当該脆弱性による脅威が大幅に増加するおそれは、現状では少ないと考えられます。

もし表 6の脆弱性の中に未対策の脆弱性がある場合は、迅速にセキュリティパッチを適用してください。脆弱性の数が多い場合は、どの脆弱性から対応を行えば良いか迷うかもしれません。対応の優先度の考え方を次の節で示しますのでご参考ください。

## 4.3. 脆弱性対応の実施事項とポイント

表 6の脆弱性のうち、優先的に対応が必要な脆弱性はすべて既知の脆弱性です。日頃から、脆弱性対応を実施していなかった組織では急いで対応を行う必要があったと想定します。また、日々、多くの脆弱性が発見されており、放置した場合、脆弱性を悪用した攻撃を受けるおそれがあります [70]。脆弱性対応を急遽実施することになったり、脆弱性を悪用した攻撃を受けたりしないために、脆弱性対応を日頃から行うことは重要です。しかしながら、脆弱性対応は、資産管理から修正措置適用までの一連の作業を継続して実施する必要があるだけではなく、日々発見される多数の脆弱性に対応する必要もあることから、作業量が多く、十分に実施できていない組織も多く存在すると考えます [71]。日々、脆弱性対応を実施していくために、効率的に行うポイントを説明します。

まずは、NIST等のガイドラインを参考に作成した、脆弱性対応の実施事項を表 7に示します [72] [73] [74] [75]。

表 7 ： 脆弱性対応の実施事項

| No | 実施事項名 | 実施事項の具体的な内容 |
|---|---|---|
| 1 | 方針の決定 | 脆弱性対応のプロセス、体制を決定する。 |
| 2 | 対象ソフトウェアの把握 | 脆弱性対応を行う対象を明確化するために、情報システムのソフトウェア構成（ソフトウェアの種類、バージョン 等）や変更履歴（パッチの適用 等）を管理する。 |
| 3 | 脆弱性情報の収集 | 把握したソフトウェアに対する脆弱性、修正措置、脅威に関する情報を定期的に確認する。 |
| 4 | 優先度の決定 | 以下の観点を踏まえて、修正措置の優先度を決定する。<br>✓ 脆弱性の現状（悪用の状況等）<br>✓ システムの機密性、完全性、可用性の要求度<br>✓ システムの状態を加味した脆弱性の深刻度 |
| 5 | 修正措置の適用 | ● 修正措置を本番環境に適用する前に、以下の事項を行う。<br>✓ 対処方針（本格対処または暫定対処）の決定<br>✓ 本番環境以外でテストを行い、問題が発生しないことの確認<br>✓ 本番環境の完全バックアップの取得<br>● 修正措置を適用する。<br>● 修正措置適用後に、意図どおりに脆弱性が修正または軽減されたことを確認する。 |
| 6 | 脆弱性対応の改善 | 脆弱性対応の実施状況を確認して、プロセスや体制を見直す。 |

次に、この流れを効率的に行うためのいくつかのポイントを図 8に示します。

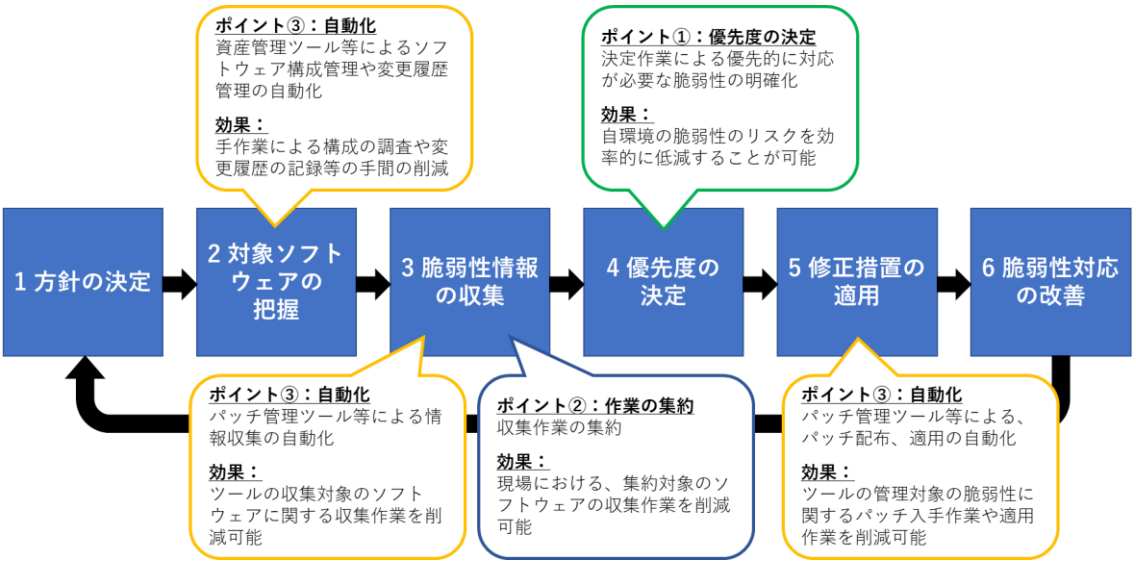



図 8 ： 脆弱性対応の流れとポイント

ポイントの1つ目は優先度の決定です。対応の優先度を決めることにより、真に対応が必要な脆弱性から対応を行うことができます。優先度を決める際には、表 7に記載した以下の３つの観点を踏まえて評価します。

- 脆弱性の現状（攻撃の有無、対策の程度、情報の正確度）
- システムの機密性、完全性、可用性の重要度
- システムの対策状況を加味した脆弱性の深刻度

脆弱性のリスクを評価する方法として、上記の３つ観点を加味したCVSS環境評価基準（Environmental Metrics）があります [76]。CVSS環境評価基準を使ってCVSS環境値（Environmental Score）を算出する場合は、脆弱性を悪用する手法を理解した上で、対象システムの構成、設定、対策状況等から、最大14個のCVSSの項目の値を検討します。CVSS環境値の算出が難しい場合は、CVSS基本評価基準（Base Metrics）に基づいて、ネットワーク越しの攻撃の可否、攻撃情報、PoCの有無など、観点を絞った独自の方法で評価する方法もあります。また、作業の集約や自動化等により、現場のシステム維持運用者の作業時間を確保することや、脆弱性対応の手順の明文化、現場のシステム維持運用者の教育等により、スムーズに評価できるように事前準備を行うことも重要です。

2つ目は作業の集約です。脆弱性情報の収集等の各現場で共通する作業を集約することにより、各現場のシステム維持運用者が行う脆弱性情報の収集等の作業負担を軽減できます。特に各現場で共通のソフトウェアを使用している場合は、容易に重複していた脆弱性情報の収集作業等を減らすことができます。併せて、各システムを構成するソフトウェアを共通化できれば、より集約効果が高まります。集約する際には、収集対象のソフトウェアや収集す

る情報の種類などを集約側と現場との作業の担当範囲を明確にして、作業の漏れがないようにすることが重要です。一方で、セキュリティ対応とシステムの運用を1人で兼任しているなどのリソースが不足している場合は、外部リソースの活用をお薦めします。脆弱性情報の配信サービスを利用する等、一部の作業を外部委託すれば、空いた稼働で優先度決めや適用前の動作検証などの委託できない作業に注力することができます。

最後のポイントは、自動化です。対象ソフトウェアの把握、脆弱性情報の収集、修正措置の適用等の手動作業は、多くの時間がかかります。IT資産管理ツールやパッチ管理ツール等の活用により作業を自動化すれば、作業負荷を大幅に削減できる可能性があります。

## 4.4. まとめ

FireEye社が公開した深刻度が高く優先的に対応が必要な脆弱性は、事件前から公開されて悪用されているものも多く存在しています。そのため、WannaCryの教訓に基づいて、適切にセキュリティパッチの適用を行っている組織にとって大きな脅威ではありません。FireEye社のツール窃取のような事件を受けて、急遽、脆弱性対応を行うことになったり、脆弱性を放置してそれを悪用した攻撃を受けたりしないように、日頃から、脆弱性対応を行うべきです。

日頃から脆弱性対応をスムーズに実施できるように、自組織に適した脆弱性のリスクの評価方法の検討やスムーズに実施するための準備を行うことをお薦めします。また、優先度決め等の各現場のシステム維持運用者の作業時間を確保するために、他の作業の集約や作業の自動化等により作業時間を削減することもお薦めします。

# 5. マルウェア・ランサムウェア

## 5.1. 2020年度第3四半期の概況

2020年度第2四半期に引き続き、マルウェアやランサムウェアによる被害が国内外で発生しています。日本国内では、2020年9月に過去最大規模の感染を確認したマルウェアEmotetによる被害や、ランサムウェアによる被害を確認しています。海外では、ヘルスケア・教育分野を標的にしたランサムウェアの被害や、日本国内と同様にEmotetによる被害を確認しました。

本章では、2020年度第2四半期に引き続き猛威を振るったEmotetの動向と、日本国内で感染が確認され始めたEmotetに類似するマルウェアIcedIDについて紹介します。海外では、SANS Instituteが2020年7月中旬以降にIcedIDの感染を確認したと公表 [77]しました。日本国内では2020年10月下旬以降にIcedIDの感染が複数確認され、JPCERT/CC 分析センターが2020年11月にTwitterで注意喚起しました [78]。今後被害が増えていく懸念が高く、Emotetとの共通点・相違点に留意することで対処できるマルウェアであるため、本章で解説します。

## 5.2. Emotetの動向

2020年11月は落ち着きを見せていたEmotetですが、セキュリティベンダのCheck Point Software Technologies社が公表した2020年12月の「Global Threat Index」では、再度、感染が多いマルウェアのランキング1位 [79]にランクインしました。第3四半期のEmotetのメールは、マイクロソフト社のWindows Updateを装ったメール [80]と、年末の時期に合わせて「クリスマス」や「賞与支給」のキーワードを使ったメール [81]が使用されています。Emotetのメールは、添付されたWord文書を開いて「コンテンツの有効化」をクリックするとEmotetへ感染するのですが、攻撃者はユーザがクリックしたくなるようにメールコンテンツへ工夫を凝らしてきています。このような手口の対策として、独立行政法人情報処理推進機構などが公開している攻撃メールの具体的なメール文章や添付ファイル名をいち早く把握して、正規メールとの区別に利用することが有効です。また、攻撃者はEmotetを定期的にアップデートしています。今回見つかったEmotetは、悪意あるペイロードの更新や検出回避機能の改善が行われていました [79]。JPCERT/CCが2020年2月に提供した検出ツールEmoCheckを利用している組織もあると思いますが、JPCERT/CCによると、2020年12月21日より活動が再開されたEmotetはEmoCheck v1.0で感染有無を確認できません [82]。2021年1月27日より上記のEmotetの感染有無を確認が可能なEmoCheck v2.0が提供されています。

LAC社が2020年11月に公表したレポートによると、2020年9月に同社のサイバー救急センターがEmotetに感染した端末を調査した事案のうち、約90%の事案がマルウェアZloaderにも感染していました [83]。オンラインバンキング情報の窃取を目的とした攻撃者がZloader

を配布するためにEmotetを使用しているためと思われます。過去の四半期レポートでも紹介している通り、Emotetの感染を確認した際は他マルウェアの感染を疑う必要があり、特にZloaderの感染とそれに伴うオンラインバンキング情報の漏えいに留意する必要があります。

## 5.3. Emotetに類似したIcedID

IcedIDはメールやブラウザなどの情報を窃取するトロイの木馬型の不正プログラムです。Emotetと同様に他のマルウェアを二次感染させる機能を持ちます。トレンドマイクロ社によると、2020年10月下旬より日本で検知され始め、同社の製品における日本国内での検知台数は2020年10月27日～2020年11月6日の10日間で70件強です [84]。IcedIDはEmotetと共通している点が多く、一部の相違点を考慮すれば既存のEmotet対策が有効です。われわれが、セキュリティベンダが公表したIcedIDの情報とEmotetの特徴を比較したところ、以下のような攻撃方法の共通点と相違点がありました。

- パスワード付きZIP形式の添付ファイル付きメールが配送される。パスワードは同一メール内に記載 [85]
- 件名が「Re:」と返信型になっている [85]
- ユーザがZIPファイルを解凍し、Word文書を開封、「コンテンツを有効化」するとIcedIDに感染する [85]
- メールの認証情報などを窃取しメールアカウントに不正ログイン、やり取りのある組織へ攻撃メールを拡散する [86]
- 別のマルウェアをダウンロードし被害拡大するおそれがある [86]

上記で紹介した攻撃方法の共通点は、有効な対策の共通点でもあります。IcedIDは、以下のようなEmotetと同じ対策が有効です。

- 不審なメールや添付ファイルを閲覧しない
- 「コンテンツの有効化」ボタンをクリックしない（マクロ自動実行はオフにする）
- メールやエンドポイントの検知可能なセキュリティ製品を導入する
- パスワード付きzipファイルを添付したメールの送受信の利用をやめる

一方で、EmotetとIcedIDの相違点は、以下のとおりです。

1点目は、現時点で確認しているIcedIDの攻撃メールの日本語はEmotetと比較すると稚拙なことです [85]。よって稚拙な日本語のメールを見極めることが効果的な対策です。ただし、Emotetが初期の流行からアップデートを重ねる中で日本語が洗練されてきたように、IcedIDも正規メールと区別が難しいようにアップデートすることが予想されます。

2点目は、正規の取引先などを経由してメールが送付されていることです。Emotetの場合、

Display Name/表示名を偽装しているケースがあるため、その偽装の有無から攻撃メールか否かを判別することができました。しかしIcedIDの場合はメールアカウントを乗っ取って攻撃メールを送信するため、Display Name/表示名を偽装していません。偽装の有無から攻撃メールの判別ができません [85]。

3点目は、IcedIDの攻撃が日本国内で検知され始めてから期間が短く、そのマルウェアの存在を把握できていない組織が存在することです。Emotetに関する攻撃手法や有効な対策の情報は広く広まっており、先に述べた検出ツールEmoCheckを導入している組織もあると思われます。無論、EmoCheckではIcedIDは検知できません [86]。IcedIDに有効なセキュリティ製品を導入する必要があります。継続的なマルウェアのアップデートが予想されるため、パターンマッチングのみに頼らず異常な振る舞いを検知可能な次世代アンチウィルス製品の導入を検討してください。

IcedIDの被害を防ぐために、セキュリティ関連の組織が発信する最新のIcedIDの情報を収集して異なるサンプルの存在や最新の攻撃手法を把握し、上記に整理した共通点・相違点と組み合わせて対策しましょう。

## 5.4. マルウェア・ランサムウェアによる被害事例

5.1 2020年度第3四半期の概況で述べた通り、マルウェア・ランサムウェアによる被害が国内外で多く発生しています。米国のCISA（Cybersecurity and Infrastructure Security Agency）は、連邦捜査局（FBI）と共同で、医療機関 [87]と教育機関 [88]を狙ったサイバー攻撃を警告しました。以下に紹介する事例には、医療機関や教育機関の被害事例が含まれています。

表 8 ： マルウェア・ランサムウェアの被害事例

| 日付 | 標的 | 概要 |
|---|---|---|
| 10/8 ※ | アメリカ（マサチューセッツ州)/スプリングフィールド公立学校 | ネットワークの潜在的な脅威を特定したため学校を閉鎖、リモート教育を一時停止した。ランサムウェア攻撃を受けたと見られている [89] |
| 10/10 | アメリカ/法律事務所/Seyfarth Shaw LLP | ランサムウェアに感染し、システムを停止した [90] |
| 10/10 | アメリカ/書店チェーン/Barnes&Noble | ランサムウェアに感染し、システム障害が発生した。ユーザが購入した電子書籍のライブラリにアクセスできないなどの影響が生じた [91] |
| 10/16 ※ | 日本/電子部品・電気機器メーカー/京セラ株式会社 | Emotetに感染し、不審メールが発信された。社内外関係者のメールアドレス、氏名、住所、電話番号などの個人情報およびメール本文が外部に流出したおそれがある [92] |

| | | |
|---|---|---|
| 10/30<br>※ | 日本/教育機関/学校法人関西医科大学 | Emotetに感染し、同学校とは異なるサーバから不正メールが送信された。同学校に附属する各病院の診療系ICTシステムは独立ネットワークで運用しているため影響は無かった [93] |
| 11/1 | イタリア/酒類会社/CampariGroup | RagnarLockerランサムウェアに感染し、ITサービスとネットワークが停止。攻撃者は2TBのデータを窃取した。身代金1500万ドルを要求された [94] |
| 11/2 | 日本/ゲームメーカー/CAPCOM | Ragnar Lockerランサムウェアに感染し、攻撃者は1TBのデータを窃取した。氏名、住所含む個人情報も漏洩した。身代金1,100万ドルを要求された [95] |
| 11/30<br>※ | 日本/システムインテグレータ/株式会社アイロベックス | オーダーメイド型ランサムウェアに感染し、PC及びファイルサーバ上のデータが暗号化された [96] |
| 11/25 | アメリカ（メリーランド州）/教育機関/ボルチモア郡公立学校 | ランサムウェアに感染し、バーチャルラーニングを一時停止、学校を閉鎖した [97] |
| 11/29 | メキシコ/電子機器製造会社/Foxconn | DoppelPaymerランサムウェアに感染し、Webサイトがダウンした。攻撃者は盗んだファイルをリークサイトに公開した [98] |
| 11/30<br>※ | アメリカ/営利教育会社/K12 Inc. | Ryukランサムウェアに感染した。システムをシャットダウンした。オンライン学習管理システムは影響がなかった。サイバー保険を利用して身代金を支払った [99] |
| 12/6<br>※ | アメリカ（メリーランド州）/病院/グレーター・ボルティモア・メディカル・センター | ランサムウェアに感染し、コンピュータシステムと病院の運用に影響が生じた [100] |
| 12/16<br>※ | 中国/医療系サービス/WellBe Holdings Limited 上海鼎安保険公估有限公司 | Emotetに感染し、成りすましメールが送付された。6,906件メール本文の内容が流出したおそれがある [101] |
| 12/30<br>※ | リトアニア /国立公衆衛生センター（NVSC） | Emotetに感染し、偽の電子メールが発信された。ウイルスの拡散を阻止するため、電子メールシステムを一時的に停止した [102] |

※公表日

## 5.5. まとめ

今回、Emotetと類似したマルウェアIcedIDを紹介しました。IcedIDは、Emotetと同様に日本語が洗練されたり、感染機能が高度化していく懸念があります。しかし、EmotetとIcedIDは攻撃方法や有効な対策に共通点があり、既に多くの組織が実施している対策が有効です。Emotetの対策に十分に取り組んでいた組織は、IcedIDが新たな脅威として警戒は必要ないと思われます。類似したマルウェア、もしくはアップデートされたマルウェアが今後も増えていくことが予想されますが、大幅な変更が行われない限り、それらのマルウェアの特徴を捉えてセキュリティ対策を積み重ねていくことにより、多くの攻撃を防ぐことができると考えます。

# 6. 予測

## 変化するサプライチェーン攻撃に引き続き警戒

三菱パワー社のインシデント事例は、運用管理システムを踏み台にして複数のシステムへ効率の良く侵入したサプライチェーン攻撃でした。また、SolarWinds社へのサプライチェーン攻撃では、「不正侵入のために多要素認証をバイパスする技術」、「製品開発プロセスを監視することで、組織に検知されずに悪意のあるソフトウェアバックドアを仕込む技術」など、従来のサプライチェーン攻撃に比べて、より狡猾な攻撃方法が使われました。この2つのサプライチェーン攻撃の事例により、三菱電機、NECなど防衛省と取引関係にある企業、FireEye社、Microsoft社、Cisco社などのIT企業、更には複数の政府機関などの世の中に対して影響力の大きな組織が被害を受けました。

このように、運用管理システムを経由したサプライチェーン攻撃やソフトウェアやOSなどの主要なソフトウェアのアップデート配布を悪用したソフトウェアサプライチェーン攻撃は、効率的に多くのシステムへ侵入できるため、積極的に攻撃者は狙います。そのため、運用監視サービス、あるいはソフトウェアを提供している組織は、特にサプライチェーン攻撃対策を強化することが必要となります。更に、攻撃者は、サプライチェーン攻撃を効率的に行える組織へ侵入するために、今後は別のサプライチェーン攻撃を仕掛けるようになります。それに伴い、攻撃者は複数の組織を経由するサプライチェーン攻撃を仕掛けなければならなくなるため、検知を回避するための隠蔽技術が更に発達していきます。その結果、企業が攻撃を検知することがより困難になると推測されます。

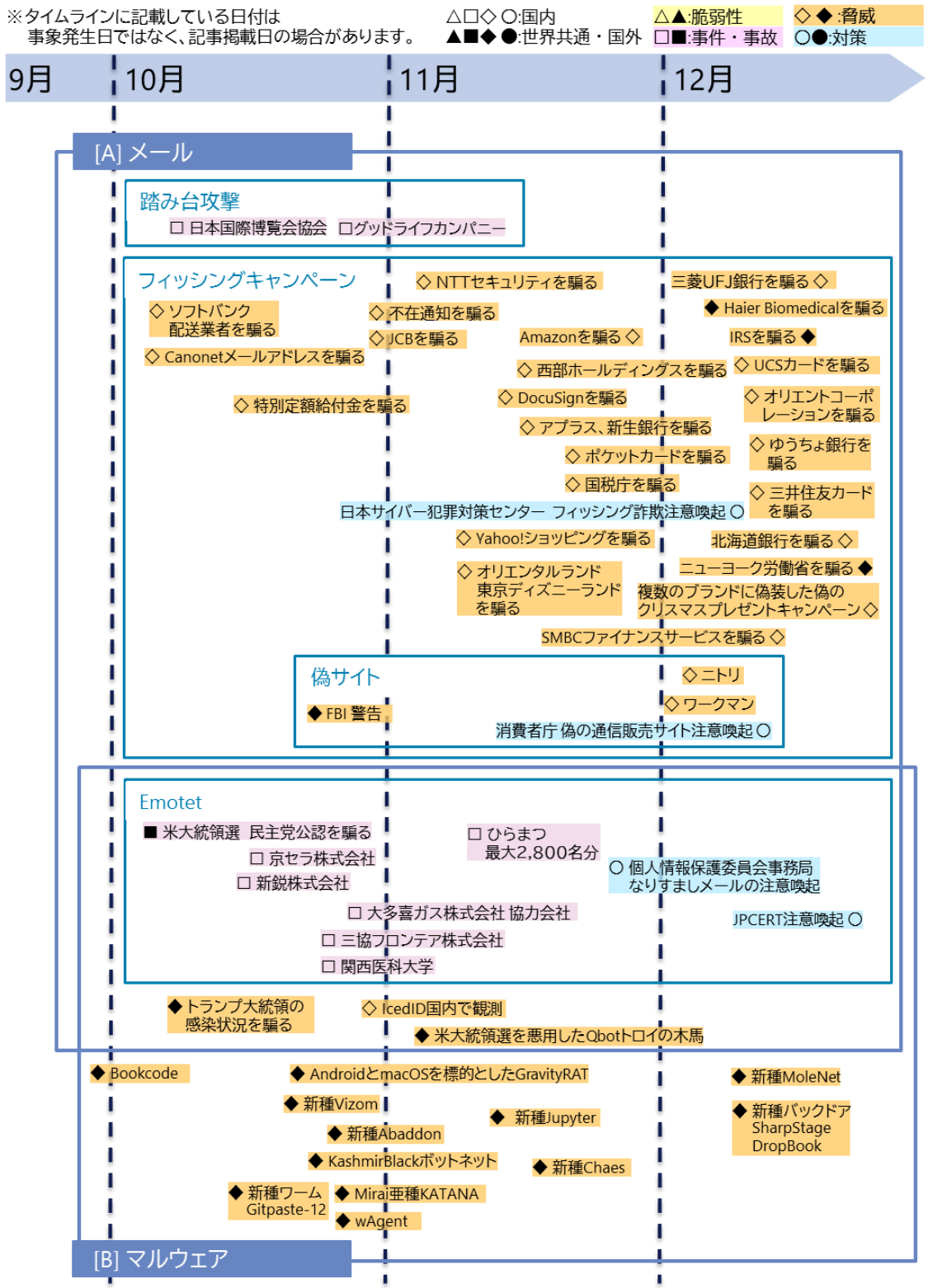
## クラウドサービス設定不備によるインシデント

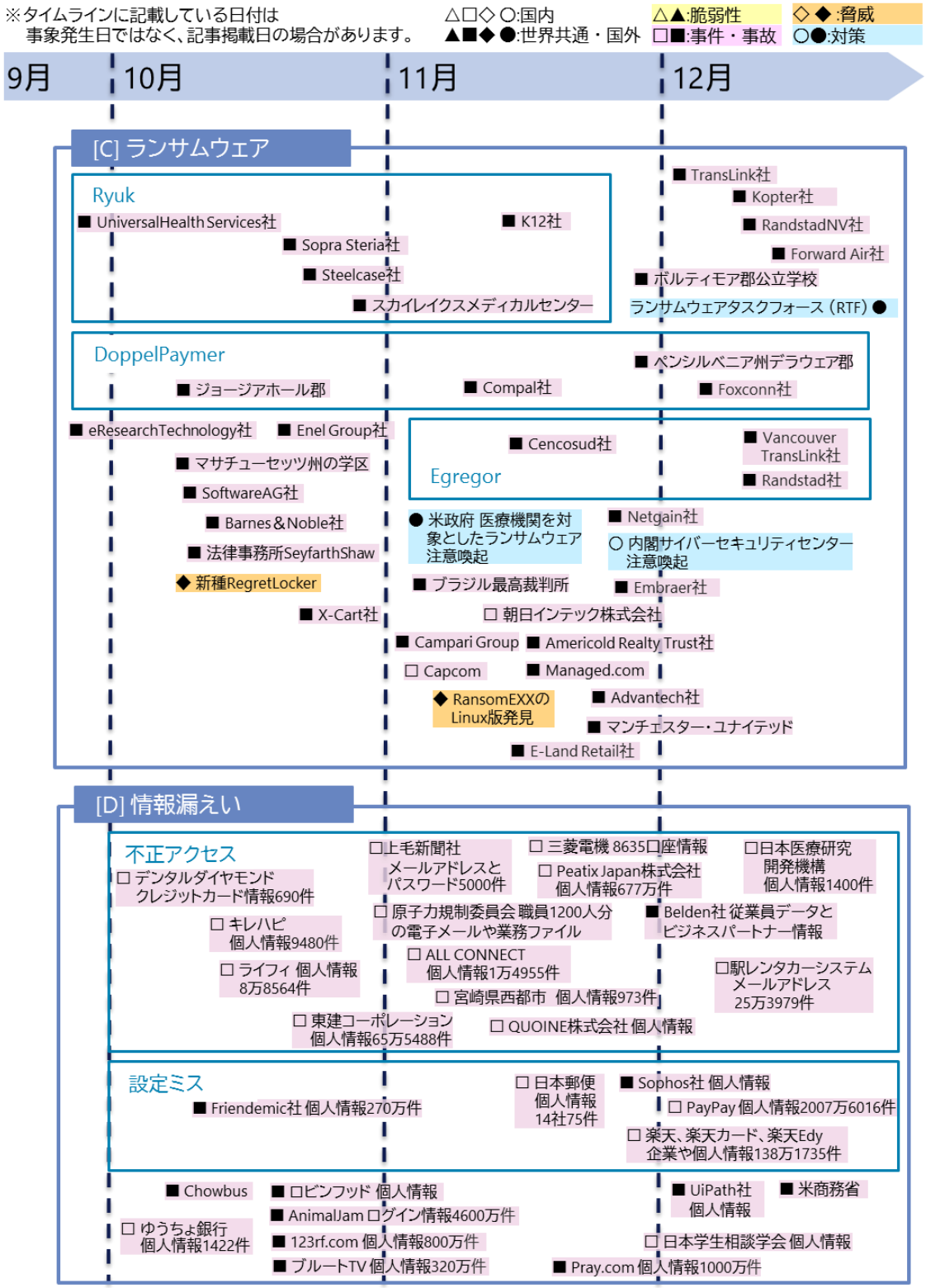
2020年度第3四半期は、Salesforceの設定不備に起因する情報漏えいが相次いで発生しました。このインシデントは、クラウドサービスカスタマが指示通りに対策すれば落ち着くと想定されます。単純な設定不備は、クラウドサービスカスタマが、クラウドサービスの仕様を十分に理解してから、クラウドサービスプロバイダの提供する情報と仕組みを活用して正しく設定すれば防ぐことができます。しかしながら、今回のように、クラウドサービスプロバイダにも原因があるインシデントは、クラウドサービスプロバイダ側もセキュリティリスクを考慮したサービスの提供が必要になります。まだまだ、対策が不十分なクラウドサービスプロバイダが存在すると想定されることから、今回のようなインシデントは今後も発生すると考えられます。さらに、デジタルトランスフォーメーションの推進や新型コロナウイルス流行による働き方改革等により、クラウドサービスの利用は引き続き増加していくと想定されることから、今後、同様のインシデントが発生した場合には、より多くの企業が被害にあうおそれがあります [103] [104] [105] [106] [107]。

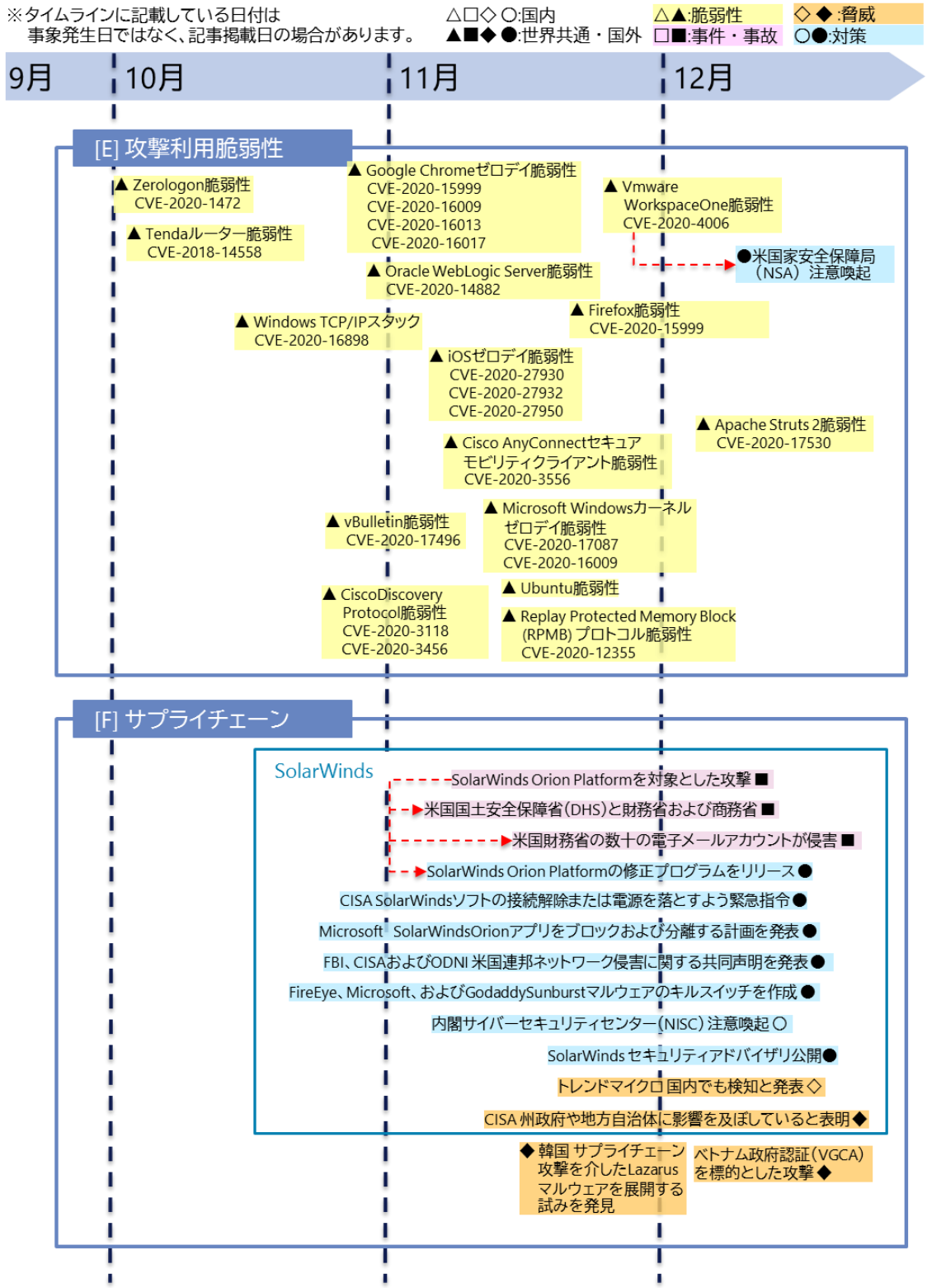
## 暗号通貨を狙った攻撃

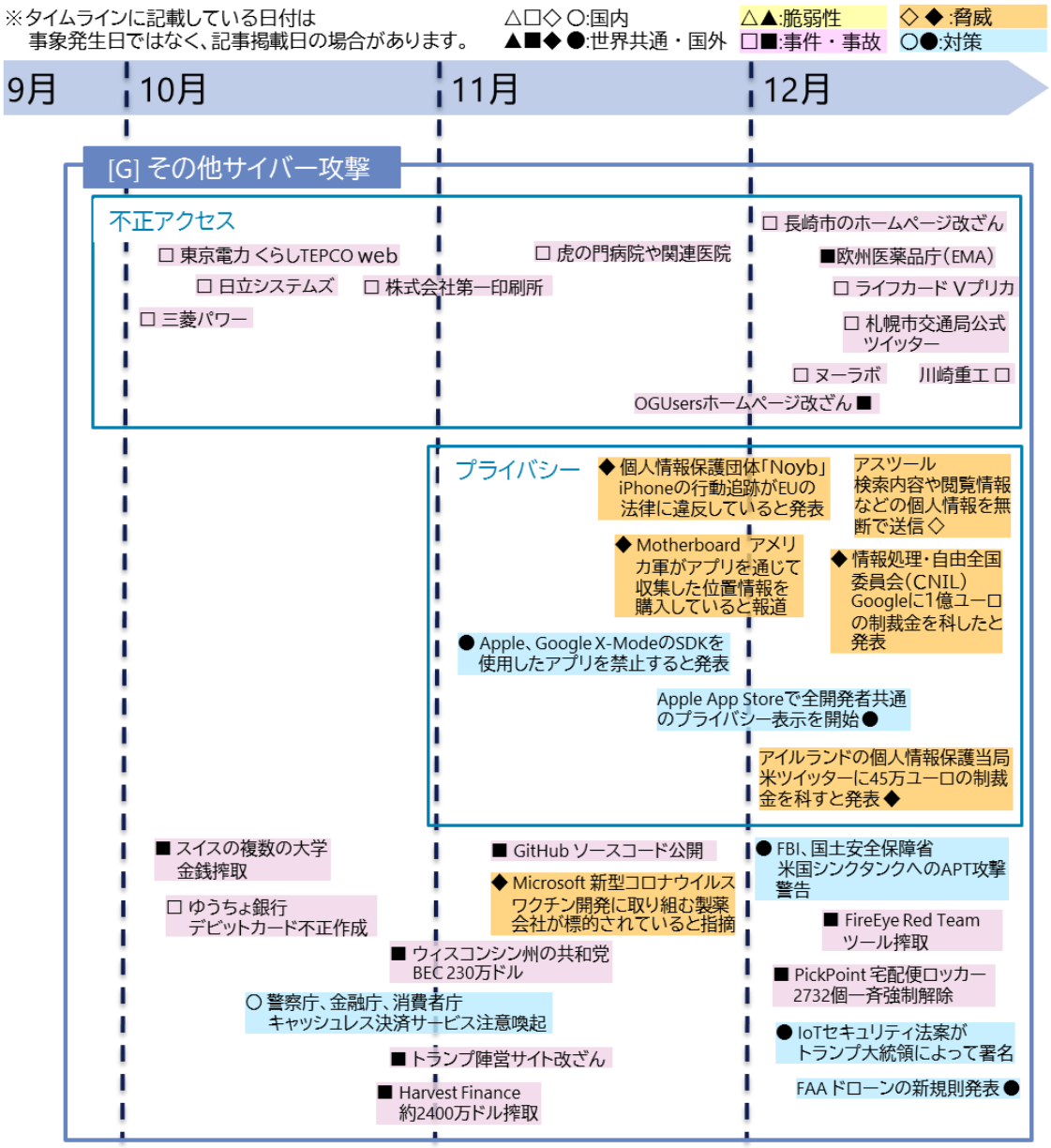
ビットコインの市場価格が、2020年12月17日に過去最高値を記録しました。その後も上昇傾向が続いています [108]。同じように上昇傾向だった2019年5月には、大手仮想通貨取引所「Binance」を標的としたサイバー攻撃が発生して、7,000ビットコイン（当時の市場価格で44億円相当）が流出しました [109]。市場価格が2019年の倍以上で、かつ上昇傾向であることから、現在の状態が継続する場合、暗号通貨を狙った攻撃が発生するおそれがあります。

# 7. タイムライン









# 参考文献


[1] Peatix Japan株式会社, “Peatixへの不正アクセス事象に関するお詫びとお知らせ,” 17 11 2020. [オンライン]. Available: https://peatix.com/event/1721625.

[2] 株式会社エブリシング, “弊社委託先への不正アクセスによる「エブリシング」個人情報流出に関するお詫びとお知らせ,” 26 11 2020. [オンライン]. Available: https://everysing.co.jp/2020/11/18/.

[3] 三菱パワー株式会社, “当社ネットワークに対するマネージド・サービス・プロバイダを経由した第三者からの不正アクセスに係る件,” 11 12 2020. [オンライン]. Available: https://power.mhi.com/jp/news/20201211.html.

[4] SolarWinds, Inc, “SolarWinds Security Advisory,” 13 12 2020. [オンライン]. Available: https://www.solarwinds.com/ja/securityadvisory.

[5] 経済産業省, “サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）が設立されます,” 30 10 2020. [オンライン]. Available: https://www.meti.go.jp/press/2020/10/20201030011/20201030011.html.

[6] 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 2020,” 28 8 2020. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/10threats2020.html.

[7] 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（2018年度版 第4四半期）,” 30 5 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2018_4q_securityreport.pdf.

[8] 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（2019年度版 第2四半期）,” 29 11 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_2q_securityreport.pdf.

[9] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート（2020年度版 第2四半期）,” 11 12 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2020/121100/121100-01.pdf.

[10] C. Cimpanu, “Sprint says hackers breached customer accounts via Samsung website,” CBS Interactive., 16 7 2019. [オンライン]. Available: https://www.zdnet.com/article/sprint-says-hackers-breached-customer-accounts-via-samsung-website/.

[11] S. S. R. A. I. Team, “Tortoiseshell Group Targets IT Providers in Saudi Arabia in Probable Supply Chain Attacks,,” Broadcom., 18 9 2019. [オンライン]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain.

[12] PEAR, “PEAR公式Twitterアカウント,” 19 1 2019. [オンライン]. Available: https://twitter.com/pear/status/1086634389465956352.

[13] Check Point Software Technologies LTD, “SimBad: A Rogue Adware Campaign On Google Play,” 13 3 2019. [オンライン]. Available: https://research.checkpoint.com/simbad-a-rogue-adwarecampaign-on-google-play/.

[14] AO Kaspersky Lab, “Operation ShadowHammer,” 25 3 2019. [オンライン]. Available: https://securelist.com/operation-shadowhammer/89992/.

[15] C. Cimpanu, “Hackers breach FSB contractor, expose Tor deanonymization project and more,” CBS Interactive, 20 7 2019. [オンライン]. Available: https://www.zdnet.com/article/hackers-breach-fsb-contractor-expose-tor-deanonymization-project/.

[16] LiveAuctioneers, “July 11, 2020 - LiveAuctioneers Account Security,” 7 11 2020. [オンライン]. Available: https://help.liveauctioneers.com/article/496-july-11-2020-liveauctioneers-account-security.

[17] G. Cluley, ““Millions of LiveAuctioneers passwords offered for sale followingdata breach,” 13 7 2020. [オンライン]. Available: https://grahamcluley.com/liveauctioneers-passwords-for-sale/.

[18] サクソバンク証券株式会社, “サイバー攻撃による個人情報流出に関するお詫びとお知らせ,” 17 9 2020. [オンライン]. Available: https://www.home.saxo/ja-jp/about-us/security-incident/personal-information-leakage.

[19] サクソバンク証券株式会社, “個人情報流出についてお客様からお寄せいただいたご質問ならびに回答,” 2020. [オンライン]. Available: https://www.home.saxo/ja-jp/about-us/security-incident/questions-and-answers.

[20] Promo, “Promo Data Breach July 21, 2020 FAQ,” 21 7 2020. [オンライン].

Available: https://support.promo.com/en/articles/4276475-promo-data-breach-july-21-2020-faq.

[21] Bleeping Computer, “Promo.com discloses data breach after 22M user records leaked online,” 27 7 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/promocom-discloses-data-breach-after-22m-user-records-leaked-online/.

[22] 日本経済新聞, “三菱パワーの不正アクセス、日立システムズ経由で侵入,” 12 12 2020. [オンライン]. Available: https://www.nikkei.com/article/DGXZQODZ121VP0S0A211C2000000.

[23] U.S. Securities and Exchange Commission, “Form 8-K Solarwinds Corp Current report, item 8.01,” [オンライン]. Available: https://sec.report/Document/0001628280-20-017451/. [アクセス日: 14 12 2020].

[24] FireEye, Inc., “Unauthorized Access of FireEye Red Team Tools,” 8 12 2020. [オンライン]. Available: https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html.

[25] Volexity, Inc., “Dark Halo Leverages SolarWinds Compromise to Breach Organizations,” 14 12 2020. [オンライン]. Available: https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/.

[26] CRN, “SolarWinds CEO: Attack Was ‘One Of The Most Complex And Sophisticated’ In History,” 7 1 2021. [オンライン]. Available: https://cloud.watch.impress.co.jp/docs/topic/special/1301088.html.

[27] 日本経済新聞, “塩野義製薬にサイバー攻撃　台湾現地法人、金銭要求も,” 22 10 2020. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO65325770S0A021C2CR8000.

[28] 読売新聞, “塩野義製薬の台湾現地法人にサイバー攻撃…盗まれた情報の一部がネットに公開,” 23 10 2020. [オンライン]. Available: https://www.yomiuri.co.jp/national/20201023-OYT1T50124/.

[29] BLEEPINGCOMPUTER, “Enel Group hit by ransomware again, Netwalker demands $14 million,” 27 10 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million/.

[30] DZNet, “Italian beverage vendor Campari knocked offline after ransomware

attack,” 5 11 2020. [オンライン]. Available: https://www.zdnet.com/article/italian-beverage-vendor-campari-knocked-offline-after-ransomware-attack/.

[31] 朝日新聞デジタル, “カプコンへのサイバー脅迫　記者はちらつく影を追った,” 12 11 2020. [オンライン]. Available: https://digital.asahi.com/articles/ASNCD3DNQNCCULZU00J.html.

[32] 独立行政法人情報処理推進機機構 セキュリティセンター, “事業継続を脅かす新たなランサムウェア攻撃について,” 20 8 2020. [オンライン]. Available: https://www.ipa.go.jp/files/000084974.pdf.

[33] 株式会社カプコン, “不正アクセスによる情報流出に関するお知らせとお詫び,” 16 11 2020. [オンライン]. Available: https://www.capcom.co.jp/ir/news/html/201116.html.

[34] 株式会社カプコン, “不正アクセスによる情報流出に関するお知らせとお詫び【第3報】,” 12 1 2021. [オンライン]. Available: https://www.capcom.co.jp/ir/news/html/210112.html.

[35] 株式会社カプコン, “不正アクセスによるシステム障害発生に関するお知らせ,” 4 11 2020. [オンライン]. Available: https://www.capcom.co.jp/ir/news/html/201104.html.

[36] BLEEPING COMPUTER, “Capcom hit by Ragnar Locker ransomware, 1TB allegedly stolen,” 5 11 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/capcom-hit-by-ragnar-locker-ransomware-1tb-allegedly-stolen/.

[37] アサ芸Biz, “個人情報の身代金を支払い拒否！「カプコン」の強硬姿勢が称賛されたワケ,” 19 11 2020. [オンライン]. Available: https://news.nifty.com/article/economy/business/12277-866199/.

[38] ITmedia, “カプコン情報流出、ロシア周辺国が関与の可能性,” 24 11 2020. [オンライン]. Available: https://www.itmedia.co.jp/news/articles/2011/24/news045.html.

[39] NHK, “ハローカプコン！暴露型サイバー攻撃の衝撃,” 23 12 2020. [オンライン]. Available: https://www3.nhk.or.jp/news/special/sci_cul/2020/12/special/20201223capcom/.

[40] Security NEXT, “凶暴性増すランサムウェアの裏側 - 今すぐ確認したい「意外な設定」,” 12 11 2020. [オンライン]. Available: https://www.security-

next.com/120578.

[41] キヤノンITソリューションズ, “手頃な値段でランサムウェアを販売する業者がいる,” 11 7 2018. [オンライン]. Available: https://ascii.jp/elem/000/001/705/1705420/.

[42] 日本経済新聞, “クラウドストライク、2020年度版グローバルセキュリティ意識調査結果を発表,” 26 11 2020. [オンライン]. Available: https://www.nikkei.com/article/DGXLRSP600746_W0A121C2000000/.

[43] DZNet Japan, “ランサムウェアの身代金支払い額、日本は平均で約1億2300万円,” 26 11 2020. [オンライン]. Available: https://japan.zdnet.com/article/35162969/.

[44] CROWDSTRIKE, “2020 CROWDSTRIKE GLOBAL SECURITY ATTITUDE SURVEY,” [オンライン]. Available: https://www.crowdstrike.com/resources/reports/global-attitude-survey-2020/.

[45] 大元隆志 | クラウドセキュリティアナリスト/国士舘大学経営学部非常勤講師, “ランサムウェアの被害にあったら、身代金を支払うべきか?,” 18 11 2020. [オンライン]. Available: https://news.yahoo.co.jp/byline/ohmototakashi/20201118-00208356/.

[46] BLEEPING COMPUTER, “US govt warns of sanction risks for facilitating ransomware payments,” 1 10 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/us-govt-warns-of-sanction-risks-for-facilitating-ransomware-payments/.

[47] Digital Keeper, “【2021年最新】進化したランサムウェアの被害を防ぐ対策とは～身代金は支払うべきか？,” 13 1 2021. [オンライン]. Available: https://keepmealive.jp/ransomware-protection/.

[48] DRS, “ランサムウェアの身代金支払いへの勧告と制裁に関する米国事情,” 20 1 2021. [オンライン]. Available: https://www.drs.co.jp/column/security/20210120_100000.html.

[49] DZNet, “全米市長会議、ランサムウェア攻撃で身代金支払い拒否へ--年次総会で決議採択,” 16 7 2019. [オンライン]. Available: https://japan.zdnet.com/article/35139937/.

[50] 経済産業省, “最近のサイバー攻撃の状況を踏まえた経営者への注意喚起,” 18 12 2020. [オンライン]. Available: https://www.meti.go.jp/press/2020/12/20201218008/20201218008-2.pdf.

[51] 内閣サイバーセキュリティセンター, “ランサムウエアによるサイバー攻撃について【注意喚起】,” 26 11 2020. [オンライン]. Available: https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf.

[52] 独立行政法人 情報処理推進機構, “事業継続を脅かす新たなランサムウェア攻撃について,” 20 8 2020. [オンライン]. Available: https://www.ipa.go.jp/files/000084974.pdf.

[53] MITRE, “MITRE ATT&CK,” [オンライン]. Available: https://attack.mitre.org/.

[54] PayPay株式会社, “当社管理サーバーのアクセス履歴について,” 7 12 2020. [オンライン]. Available: https://paypay.ne.jp/notice/20201207/02/.

[55] 楽天株式会社, “クラウド型営業管理システムへの社外の第三者によるアクセスについて,” 25 12 2020. [オンライン]. Available: https://corp.rakuten.co.jp/news/update/2020/1225_01.html.

[56] 日経クロステック, “楽天だけでなくPayPayでも、セールスフォース製品の設定不備を狙った不正アクセス,” 26 12 2020. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/news/18/09412/.

[57] 日経クロステック, “楽天とPayPayがつまずいたセールスフォース製品の「設定不備」、被害は氷山の一角か,” 22 1 2021. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/column/18/00989/012000044/.

[58] 日経クロステック, “セールスフォース製品「設定不備」による不具合続々、バンダイや日本政府観光局でも,” 1 2 2021. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/news/18/09570/.

[59] 日経クロステック, “金融庁の注意喚起で金融機関が対応急ぐ、セールスフォース製品への不正アクセスで,” 29 12 2020. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/news/18/09416/.

[60] 日経クロステック, “NISCが「セールスフォース製品の設定不備」に注意促す、楽天などで不正アクセス,” 30 1 2021. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/news/18/09560/.

[61] 株式会社セールスフォース・ドットコム, “Salesforceサイトおよびコミュニティにおけるゲストユーザのアクセス制御の権限設定について,” 21 2 2021. [オンライン]. Available: https://www.salesforce.com/jp/company/news-press/stories/salesforce-update/.

[62] 日本クラウドセキュリティアライアンス, “クラウドにおけるセキュリティサービスの効果的な管理のガイドライン,” 21 2 2021. [オンライン]. Available:

https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2019/09/Guideline-on-Effectively-Managing-Security-Service-in-the-Cloud-06_02_19_J_FINAL.pdf.

[63] The CentOS Project, “About/Product - CentOS Wiki,” The CentOS Project, 12 12 2020. [オンライン]. Available: https://wiki.centos.org/About/Product.

[64] アドビ株式会社, “Adobe Flash Player End of Life,” アドビ株式会社, 13 1 2021. [オンライン]. Available: https://www.adobe.com/jp/products/flashplayer/end-of-life.html.

[65] ファイア・アイ株式会社, “FireEye Red Team のツールに対する不正アクセスに関して | FireEye Inc,” ファイア・アイ株式会社, 9 12 2020. [オンライン]. Available: https://www.fireeye.com/blog/jp-threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html.

[66] WatchGuard Technologies, Inc., “FireEye の侵害は SolarWinds へのサプライチェーンハッキングが原因,” WatchGuard Technologies, Inc., 14 12 2020. [オンライン]. Available: https://www.watchguard.co.jp/security-news/solarwinds-supply-chain-hack-responsible-for-fireeye-breach.html.

[67] FireEye, Inc., “red_team_tool_countermeasures CVEs_red_team_tools.md,” FireEye, Inc., 9 12 2020. [オンライン]. Available: https://github.com/fireeye/red_team_tool_countermeasures/blob/master/CVEs_red_team_tools.md.

[68] 株式会社カスペルスキー, “WannaCry：情報まとめ,” 株式会社カスペルスキー, 18 5 2017. [オンライン]. Available: https://blog.kaspersky.co.jp/wannacry-faq-what-you-need-to-know-today/15594/.

[69] E. Moyer, “Stolen NSA hacking tool now victimizing US cities, report says,” CNET, A RED VENTURES COMPANY., 25 5 2019. [オンライン]. Available: https://www.cnet.com/news/stolen-nsa-hacking-tool-now-victimizing-us-cities-report-says/.

[70] 独立行政法人情報処理推進機構, “脆弱性対策情報データベースJVN iPediaの登録状況 [2020年第4四半期（10月～12月）]：IPA 独立行政法人 情報処理推進機構,” 独立行政法人情報処理推進機構, 20 1 2021. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/report/JVNiPedia2020q4.html.

[71] 株式会社ブロードバンドセキュリティ, 株式会社イード, “厳しい条件のもとでも高い意識で脆弱性管理に取り組む「一人情シス」たち ～ 日本企業の脆弱性管理実態探る５００名調査実施,” 23 10 2020. [オンライン]. Available:

https://www.bbsec.co.jp/news/pdf/20201023.pdf.

[72] National Institute of Standards and Technology, “Special Publication 800-40 Version 2.0 Creating a Patch and Vulnerability Management Program,” 11 2005. [オンライン]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-40ver2.pdf.

[73] 独立行政法人情報処理推進機構, “セキュリティ担当者のための脆弱性対応ガイド 第3版第2刷,” 3 2017. [オンライン]. Available: https://www.ipa.go.jp/files/000058493.pdf.

[74] 独立行政法人情報処理推進機構, “脆弱性対策の効果的な進め方（ツール活用編）～ 脆弱性検知ツール Vuls を利用した脆弱性対策 ～,” 21 2 2019. [オンライン]. Available: https://www.ipa.go.jp/files/000071584.pdf.

[75] 独立行政法人情報処理推進機構, “脆弱性対策の効果的な進め方（実践編）第2 版～脆弱性情報の早期把握、収集、活用のスヽメ～,” 21 2 2019. [オンライン]. Available: https://www.ipa.go.jp/files/000071660.pdf.

[76] 独立行政法人情報処理推進機構, “共通脆弱性評価システムCVSS v3概説,” 独立行政法人情報処理推進機構, 1 12 2015. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/CVSSv3.html.

[77] SANS Institute, “More TA551 (Shathak) Word docs push IcedID (Bokbot),” 14 10 2020. [オンライン]. Available: https://isc.sans.edu/forums/diary/More+TA551+Shathak+Word+docs+push+IcedID+Bokbot/26674/.

[78] JPCERT/CC 分析センター公式Twitterアカウント, 6 11 2020. [オンライン]. Available: https://twitter.com/jpcert_ac/status/1324561915738091522.

[79] Check Point Software Technologies Ltd., “December 2020’s Most Wanted Malware: Emotet Returns as Top Malware Threat,” 7 1 2021. [オンライン]. Available: https://blog.checkpoint.com/2021/01/07/december-2020s-most-wanted-malware-emotet-returns-as-top-malware-threat/.

[80] Bleeping Computer LLC, “Watch out for Emotet malware's new 'Windows Update' attachment,” 18 10 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/watch-out-for-emotet-malwares-new-windows-update-attachment/.

[81] 独立行政法人情報処理推進機構, “「Emotet」と呼ばれるウイルスへの感染を狙

うメールについて,” 22 12 2020. [オンライン]. Available: https://www.ipa.go.jp/security/announce/20191202.html.

[82] 一般社団法人JPCERTコーディネーションセンター, “マルウエアEmotetへの対応FAQ,” 23 12 2020. [オンライン]. Available: https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html.

[83] 株式会社ラック, “分析レポート：Emotetの裏で動くバンキングマルウェア「Zloader」に注意,” 25 11 2020. [オンライン]. Available: https://www.lac.co.jp/lacwatch/people/20201106_002321.html.

[84] トレンドマイクロ株式会社, “「EMOTET」に続き「IcedID」の攻撃が本格化の兆し、パスワード付き圧縮ファイルに注意,” 9 11 2020. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/26656.

[85] マクニカネットワークス株式会社, “IceID /IcedIDマルウェアへの対応について,” 12 11 2020. [オンライン]. Available: https://mnc.macnica.net/2020/11/iceid.html.

[86] トレンドマイクロ株式会社, “緊急セキュリティ速報：マルウェア「IcedID」に注意,” 10 11 2020. [オンライン]. Available: https://www.trendmicro.com/ja_jp/about/announce/announces-20201110-01.html.

[87] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, “Ransomware Activity Targeting the Healthcare and Public Health Sector,” 28 10 2020. [オンライン]. Available: https://us-cert.cisa.gov/ncas/current-activity/2020/10/28/ransomware-activity-targeting-healthcare-and-public-health-sector.

[88] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, “Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data,” 10 12 2020. [オンライン]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-345a.

[89] Bleeping Computer LLC, “Massachusetts school district shut down by ransomware attack,” 8 10 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/massachusetts-school-district-shut-down-by-ransomware-attack/.

[90] Security Affairs by Pierluigi Paganini, “Leading Law firm Seyfarth Shaw discloses ransomware attack,” 13 10 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/109435/malware/seyfarth-shaw-ransomware-attack.html.

[91] Security Affairs by Pierluigi Paganini, “U.S. Bookstore giant Barnes & Noble hit by cyberattack,” 15 10 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/109511/hacking/barnes-noble-cyber-attack.html.

[92] 京セラ株式会社, “弊社を装った不審メールと個人情報等の流出の可能性に関するお詫びとお知らせ,” 16 10 2020. [オンライン]. Available: https://www.kyocera.co.jp/information/2020/1001_alpf.html.

[93] 学校法人関西医科大学, “本学職員を装った不審メールについてのお知らせとお詫び,” 30 10 2020. [オンライン]. Available: http://www.kmu.ac.jp/news/20201030_Emotet.html.

[94] Bleeping Computer LLC, “Campari hit by Ragnar Locker Ransomware, $15 million demanded,” 5 11 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/campari-hit-by-ragnar-locker-ransomware-15-million-demanded/.

[95] Bleeping Computer LLC, “Capcom: 390,000 people may be affected by ransomware data breach,” 12 1 2021. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/capcom-390-000-people-may-be-affected-by-ransomware-data-breach/.

[96] 株式会社アイロベックス, “【重要なお知らせ】不正アクセスの影響によるご迷惑をおかけしたことのお詫び,” 25 12 2020. [オンライン]. Available: https://www.ilovex.co.jp/event/20201225/ilovex20201225_release.pdf.

[97] Bleeping Computer LLC, “Baltimore County Public Schools hit by ransomware attack,” 25 11 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/baltimore-county-public-schools-hit-by-ransomware-attack/.

[98] Bleeping Computer LLC, “Foxconn electronics giant hit by ransomware, $34 million ransom,” 7 12 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/foxconn-electronics-giant-hit-by-ransomware-34-million-ransom/.

[99] Security Affairs by Pierluigi Paganini, “K12 education giant paid the ransom to the Ryuk gang,” 2 12 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/111824/malware/k12-ryuk-ransomware.html.

[100] Security Affairs by Pierluigi Paganini, “A ransomware attack hit the Greater Baltimore Medical Center,” 7 12 2020. [オンライン]. Available:

https://securityaffairs.co/wordpress/112017/malware/greater-baltimore-medical-center-ransomware.html.

[101] WellBe Holdings Limited, “ウイルスメール感染に関するお詫びと注意喚起,” 16 12 2020. [オンライン]. Available: http://wellbemedic.com/topics/detail/post_86.html.

[102] Bleeping Computer LLC, “Emotet malware hits Lithuania's National Public Health Center,” 30 12 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/emotet-malware-hits-lithuanias-national-public-health-center/.

[103] IDC Japan 株式会社, “国内パブリッククラウドサービス市場予測を発表,” IDC Japan 株式会社, 14 9 2020. [オンライン]. Available: https://www.idc.com/getdoc.jsp?containerId=prJPJ46845820.

[104] Gartner, Inc., “Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020,” Gartner, Inc., 13 11 2019. [オンライン]. Available: https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020.

[105] 佐藤由紀子, “Microsoftの10～12月決算、コロナ禍で売上高・純利益ともに過去最高,” アイティメディア株式会社, 27 1 2021. [オンライン]. Available: https://www.itmedia.co.jp/news/articles/2101/27/news079.html#:~:text=Azure%E3%82%84%E3%82%B5%E3%83%BC%E3%83%90%E3%83%BC%E8%A3%BD%E5%93%81%E3%82%92,146%E5%84%84%E3%83%89%E3%83%AB%E3%81%A0%E3%81%A3%E3%81%9F%E3%80%82.

[106] 佐藤由紀子, “Amazon.com、巣ごもり需要による大幅増収増益で過去最高に,” アイティメディア株式会社, 3 2 2021. [オンライン]. Available: https://www.itmedia.co.jp/news/articles/2102/03/news061.html#:~:text=2021%E5%B9%B4%E7%AC%AC1%E5%9B%9B%E5%8D%8A%E6%9C%9F,%E3%81%AF%E5%89%B5%E6%84%8F%E3%81%AE%E4%BC%81%E6%A5%AD%E3%81%A0%E3%80%82.

[107] R. Nieva, “Google discloses more on cloud business as it looks beyond search,” CNET, A RED VENTURES COMPANY. , 2 2 2021. [オンライン]. Available: https://www.cnet.com/news/google-discloses-more-on-cloud-business-as-it-looks-beyond-search/.

[108] V. Hajric, “最高値更新続いたビットコイン、21年は規制当局の監視強まる可能性,” Bloomberg L.P., 28 12 2020. [オンライン]. Available:

https://www.bloomberg.co.jp/news/articles/2020-12-28/QM03DST1UM0X01.

[109] Binance.com., “Binance Security Breach Update,” Binance.com., 8 5 2019. [オンライン]. Available: https://www.binance.com/en/support/articles/360028031711.

[110] The Hacker News, “Software Supply-Chain Attack Hits Vietnam Government Certification Authority,” 17 12 2020. [オンライン]. Available: https://thehackernews.com/2020/12/software-supply-chain-attack-hits.html.

[111] 防衛相, “三菱電機㈱による機微な情報の漏えいの可能性について,” 10 2 2020. [オンライン]. Available: https://www.mod.go.jp/j/press/news/2020/02/10a.pdf.

[112] 日本電気株式会社, “当社の社内サーバへの不正アクセスについて,” 31 1 2020. [オンライン]. Available: https://jpn.nec.com/press/202001/20200131_01.html.

[113] Data Centre Dynamics Ltd (DCD), “Tech companies like Intel, Nvidia, Microsoft, and Cisco installed SolarWinds malware,” 23 12 2020. [オンライン]. Available: https://www.datacenterdynamics.com/en/news/tech-companies-intel-nvidia-microsoft-and-cisco-installed-solarwinds-malware/.

[114] 独立行政法人情報処理推進機構, “情報セキュリティ5か条,” 19 3 2019. [オンライン]. Available: https://www.ipa.go.jp/files/000055516.pdf.

[115] J. LEMON, “Alleged Russian SolarWinds Hack 'Probably an 11' On Scale of 1 to 10, Cybersecurity Expert Warns,” Newsweek, 24 12 2020. [オンライン]. Available: https://www.newsweek.com/alleged-russian-solarwinds-hack-probably-11-scale-1-10-cybersecurity-expert-warns-1554606.

NTT DATA
Trusted Global Innovator

2021年3月16日発行

株式会社NTTデータ
セキュリティ技術部
大谷 尚通 / 小林 義徳 / 大石 眞央 / 山下 大輔
星野 亮 / 伊藤 明宏 / 小澤 陽平 / 宮崎 大輔 / 木下 盾 / 中村 勉 / 福田 裕紀