CYBER SECURITY REPORT

サイバーセキュリティレポート

2022

年間

安全なネット活用のための

セキュリティ情報

はじめに

本レポートでは、2022年1月から12月(以降2022年)に検出されたマルウェア、および発生したサイバー攻撃事例について紹介します。

「第1章 2022年マルウェア検出統計」では、2022年にESET製品で検出されたマルウェアについて、日本国内と世界全体の検出を比較して傾向を分析します。また、マルウェア検出数TOP10とマルウェア以外の脅威TOP10について詳しく分析します。

「第2章 マルウェアファミリーに着目したESET統計情報と上位マルウェアの紹介」では、セキュリティ製品におけるマルウェア検出名の仕組みについて解説します。また、マルウェアファミリー別で検出数1位のAgentTeslaの概要や解析結果を紹介します。

「第3章 2022年に確認された不正アクセスによるセキュリティインシデント」では、2022年に公表された不正アクセスによるセキュリティインシデントを収集し、組織別・業種別・被害別などの分類を解説します。また、多数確認した不正アクセスの原因と対策について紹介します。

「第4章 病院を狙うサイバー攻撃の増加とその背景」では、2021年10月末に発生した徳島県の公立病院へのランサムウェア攻撃を皮切りに報告が急増している医療機関へのサイバー攻撃について解説します。身近な医療機関である病院と診療所を主に取り上げ、サイバー攻撃による医療機関の被害事例と攻撃増加の背景を考察し、対策を紹介します。

「第5章 なぜ、脆弱性対応が放置されるのか」では、既知の脆弱性が対応されず放置されてしまう原因について考察します。最近のサイバー攻撃、特にランサムウェアの感染原因は人間の過失より脆弱性を悪用されるケースが多いことや、悪用される脆弱性はその対策方法が公開されていないゼロデイ(0-day)と言われる脆弱性ではなく、脆弱性に関する情報や対策方法が既に公開されている脆弱性を悪用するケースが多いことを解説します。

「第6章 Web証明書／PKIの最新動向と展望」では、Webの信頼を支えるインフラであるWeb証明書とPKIについて解説します。前半ではPKIの仕組みを解説し、過去に信頼性を揺るがした事件や信頼性を回復するために行われたさまざまな取り組みについて紹介します。後半では最近のPKIの動向とその変化を踏まえ、PKIが今後どのように変貌するのかを考察します。

contents

1

2022年
マルウェア検出統計

第 1 章　　2022年マルウェア検出統計

1.1.　マルウェアの検出数の比較

直近4年間の国内マルウェア検出数を、半期ごとにまとめた推移を紹介します。また2022年を通した検出数を、国内と全世界の月別推移とその比較を紹介します。

※検出数にはPUA（Potentially Unwanted/Unsafe Application; 必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーション）を含めています。

2018年下半期から2022年下半期までに国内で検出されたマルウェアの推移は、図 1-1のとおりです。2022年下半期の検出数は2022年上半期と比較して減少しています。直近4年間で最も検出されていた2020年下半期をピークに減少傾向が続いています。2020年と2022年を比較すると、アドウェアやPUAの検出数が減少していました。2022年におけるアドウェアの検出数減少の原因については、図 1-2 マルウェア検出数の月別推移（2022年・国内）のグラフで説明します。

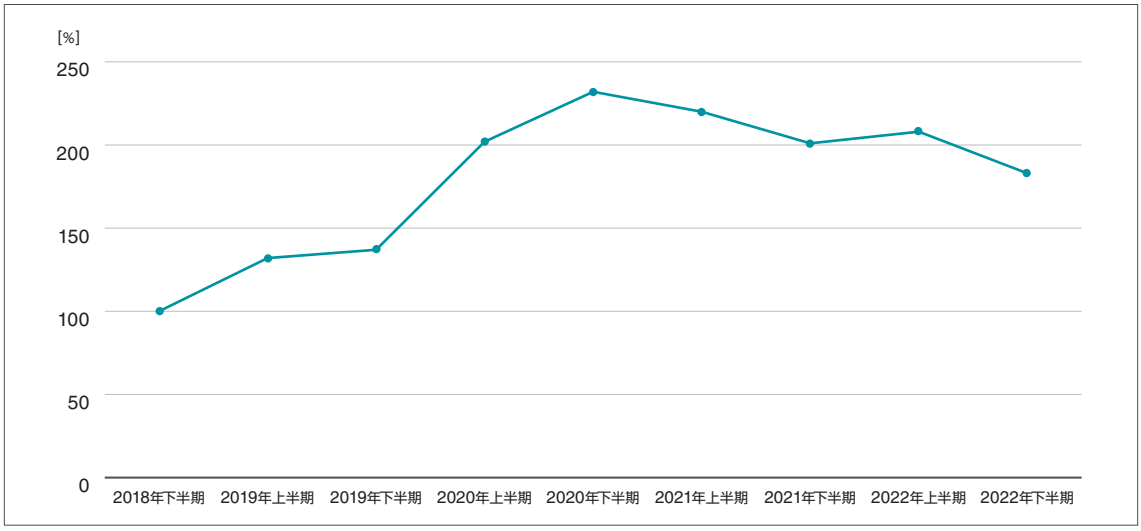

図 1-1　半期ごとの検出数の比較（2018年下半期～2022年下半期・国内）
※2018年下半期の検出数を100％として比較しています。

2022年に国内と全世界で検出されたマルウェアの検出数の推移は、図 1-2と図 1-3のとおりです。国内と全世界に共通して最もマルウェアが多く検出された月は 3月でした。3月の検出数増加は、2022年上半期サイバーセキュリティレポート[1]で紹介したEmotetのばらまきメールを多数検出したことが原因となります。
一方、10月から 11月にかけて、検出数が大きく減少しています。大きく減少した原因としては、10月の検出数上位を占めていた複数のマルウェアの検出数の減少が重なったことが挙げられます。検出数が減少したマルウェアとして、アドウェアやHTML形式のマルウェアといった Webブラウジング中に遭遇する脅威を確認しています。この期間における脅威アクターの活動低下や広告ネットワークを悪用したマルバダイジングの減少といったさまざまな理由が考えられます。要因を 1つに絞ることは難しいですが、脅威アクターの関心や対象が変わった可能性や次の攻撃の準備を実施している可能性が挙げられます。
今後のアドウェアをはじめとしたWebブラウジング中に遭遇する脅威の検出状況に注視していきます。

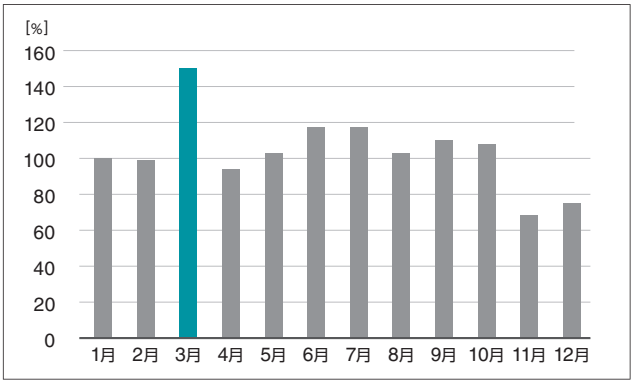

図 1-2　マルウェア検出数の月別推移(2022年・国内)
※2022年1月の検出数を100%としています。

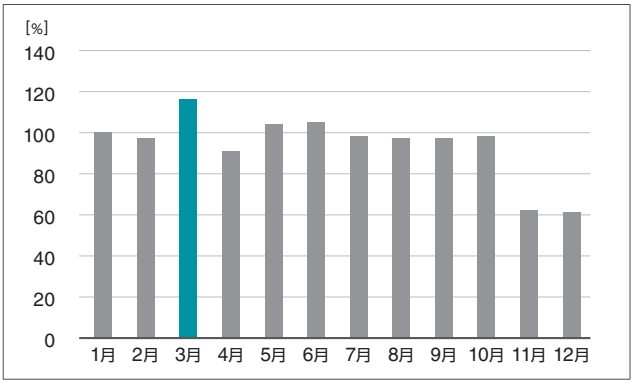

図 1-3　マルウェア検出数の月別推移(2022年・全世界)
※2022年1月の検出数を100%としています。

1.2.　2022年のマルウェア検出数TOP10

2022年における、マルウェア検出数のTOP10(国内と全世界)およびマルウェア以外の脅威検出数のTOP10(国内)を紹介します。

1.2.1.　　2022年のマルウェア検出数TOP10

図 1-4　マルウェア検出数のTOP10(2022年・国内(左)全世界(右))

2022年に国内で最も多く検出されたマルウェアは、JS/Adware.Agentです。JS/Adware.TerraClicksとDOC/TrojanDownloader.Agentがこれに続きます。JS/Adware.Agentは、不正な広告を表示させるアドウェアの汎用検出名です。
第2位のJS/Adware.TerraClicksもアドウェアの検出名であり、感染するとアドウェアサイトへのリダイレクト、アドウェアコンテンツの配布やブラウザー拡張機能としてアドウェアをインストールするなどの被害を生じさせる可能性があります。
第3位のDOC/TrojanDownloader.Agentは、Wordファイル形式のダウンローダーの検出名であり、さまざまなマルウェアをダウンロードします。
全世界で最も多く検出されたマルウェアは、JS/Packed.Agentです。JS/Adware.AgentとJS/Adware.TerraClicksがこれに続きます。JS/Packed.Agentは、パッカーと呼ばれる圧縮ツールによって、自己解凍形式で圧縮されたJavaScriptのマルウェアです。国内検出数第3位のDOC/TrojanDownloader.Agentは、上半期にEmotetのダウンローダーとして多く利用されたこともあり、2021年のTOP10圏外から2022年TOP10に大幅に順位を上げています。また、詐欺を目的とした脅威も国内検出数TOP10に入りました。2022年上半期サイバーセキュリティレポートでも紹介したHTML/Pharmacy以外に、検出数が増加しているマルウェアとして、HTML/FakeAlertがあります。
HTML/FakeAlertは、偽の警告文を表示させるHTMLファイルです。検出されるものとして、Windowsのサポートを騙ったWebサイトが確認されています。

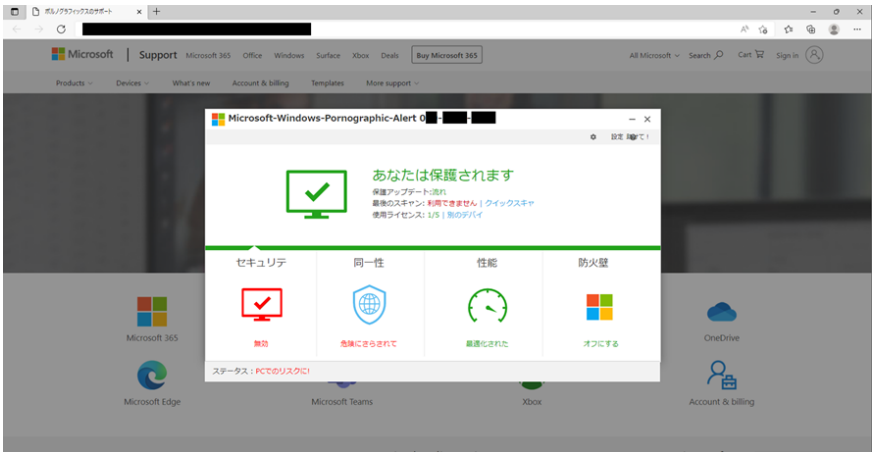

図 1-5　サポート詐欺を狙ったWebサイトの1つ（2022年）

このようなWebサイトにアクセスすると、偽の警告文が表示され、画面に書かれた電話番号へ連絡するように促されます。連絡すると、プリペイドカードや電子マネーによるサポート料の要求や指定したツールのインストールを指示されるケースがあります。指示されるツールは、攻撃者が端末に外部からアクセスするためのものです。こうした手口はサポート詐欺と呼ばれ、警視庁[2]や消費者庁[3]、国民生活センター[4]からも注意喚起が行われています。また、サポート詐欺の平均被害金額が増加しています[4]。2020年度は81,103円でしたが、2021年度には2倍近い値の141,665円となりました[4]。パソコンだけでなくスマートフォンなどのモバイル端末でもサポート詐欺サイトにアクセス可能ということもあり、被害が増加するおそれがあります。もしも、身に覚えのない警告/不審なサポートサイトにアクセスした場合は、画面に表示された電話番号へ連絡しないことが重要です。不安な場合やトラブルが生じた場合は、消費者生活センターやIPAの情報セキュリティ安心相談窓口へ相談してください。

1.2.2.　2022年のマルウェア以外の脅威の検出数TOP10

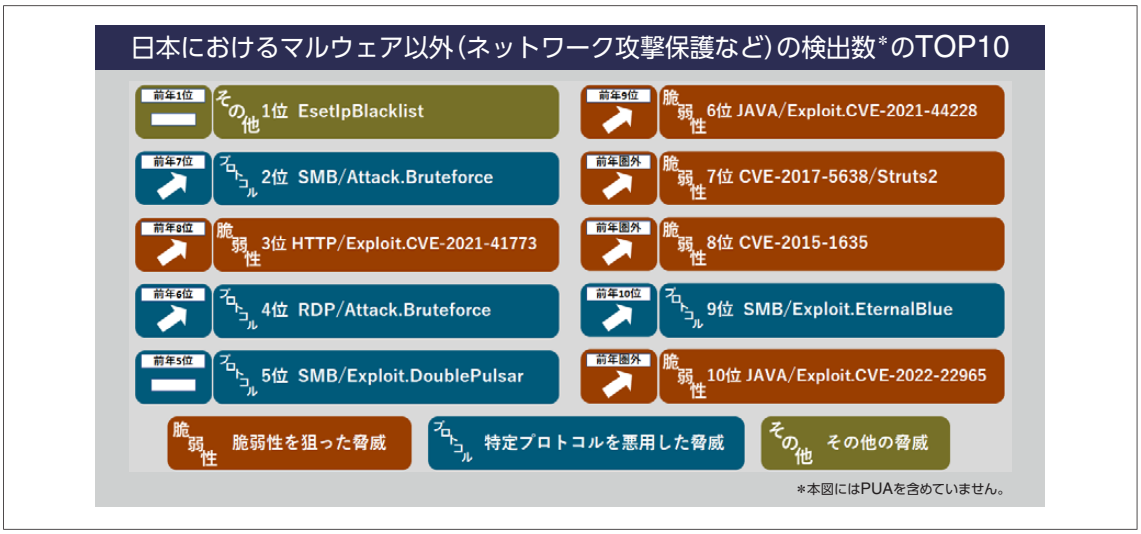

図 1-6　マルウェア以外の脅威の検出数TOP10（2022年・国内）

ESETクライアントでは、マルウェア以外にも通信プロトコルである RDPやSMB経由の攻撃、ソフトウェアの脆弱性を狙った攻撃などを検出することができます。
2022年に国内で最も検出数が多かったものは EsetIpBlacklistでした。SMB/Attack.BruteforceとHTTP/Exploit.CVE-2021-41773がこれに続きます。EsetIpBlacklistは HTTP（S）のデフォルトポート番号「80」「443」に対する悪意のあるIPアドレスやドメインへの通信、SMB/Attack.Bruteforceは SMBのデフォルトポート番号「445」に対するブルートフォース攻撃、HTTP/Exploit.CVE-2021-41773は Apache HTTP Serverのパストラバーサルの脆弱性を狙った攻撃です。
2021年と比較すると脆弱性を狙った脅威が多数観測されました。3位の HTTP/Exploit.CVE-2021-41773（Apache HTTP Serverのパストラバーサルの脆弱性を悪用した攻撃）と6位の JAVA/Exploit.CVE-2021-44228（Apache Log4jの任意のコード実行の脆弱性を悪用した攻撃）は、どちらも2021年10月以降に公表された脆弱性と関連する脅威です。
これらの脅威は 2022年に入ってからも継続して観測されたため順位を上げています。これらを含め、過去に発見された脆弱性を悪用する攻撃が年間を通して多く観測されているため、組織で利用しているソフトウェアのバージョン管理が重要です。利用ソフトウェアに関する脆弱性情報を常に把握し、脆弱性が発見された場合は速やかにパッチを適用するようにしてください。

脆弱性を狙った脅威以外では、SMBプロトコルを悪用した攻撃が 2位、5位、9位と多く見られました。特に 2位の SMB/Attack.Bruteforceは 2021年の 7位から順位を上げており、2022年における特徴的な傾向の1つであったことがわかります。Windowsを使用する組織の Active Directory環境において、SMBプロトコルはグループポリシーを各端末に配布する際に利用されるため、組織によっては運用上無効化することが困難です。こうした状況の中、最新の Windows 11ではSMBを悪用したブルートフォース攻撃を防ぎやすくなっているといった情報[5]もあり、ベンダーによるセキュリティ強化が継続して行われています。よって SMBプロトコルを安全に利用するために、可能な限り最新の Windows 11を利用するようにしてください。

1.3.　マルウェア検出数のファイル形式別割合

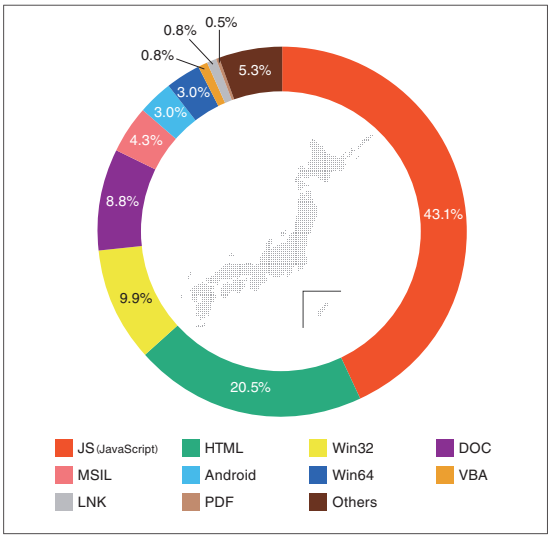

図 1-7　形式別マルウェア検出数の割合（2022年・国内）

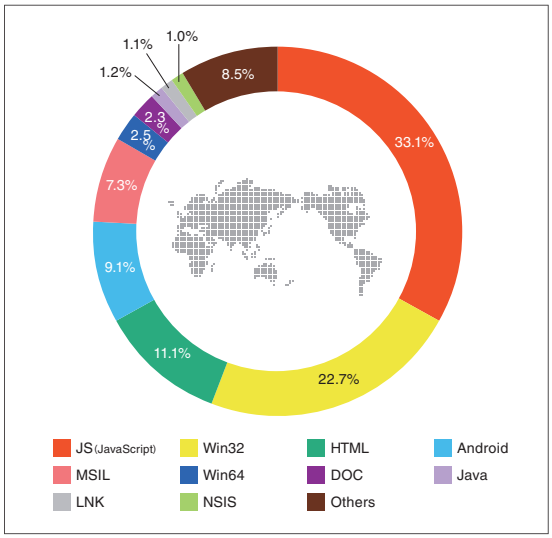

図 1-8　形式別マルウェア検出数の割合（2022年・全世界）

ESET製品で検出されるマルウェアはファイル形式（プラットフォーム）で大別することができます。国内と全世界におけるファイル形式別検出数の割合を図 1-7と図 1-8に示します。

国内と全世界ともに上位 3種をJS（JavaScript）形式、HTML形式、Win32形式で占めています。JS（JavaScript）形式とHTML形式については端末を問わずWebブラウジング中に遭遇する脅威が多いこと、Win32形式についてはWindowsがデスクトップOSとして世界で最もシェアの高いOSであり攻撃者に標的とされやすいことが、検出割合の高い理由であると推測されます。またDOC形式の割合を前年と比較してみると、国内（2021年:3.5%）と全世界（2021年:1.2%）どちらも2倍以上に増加していました。これは1.1節でも言及したように、3月を中心にEmotetの感染を狙ったばらまきメールが急増したことでマルウェアのダウンローダーであるDOC/TrojanDownloader.Agentの検出数が多かったことが影響していると考えられます。

国内ではDOC形式やVBA形式といったMicrosoft社の製品に関連したファイル形式の割合が高い傾向にあります。2021年のデータでは、国内のオフィスツールとしてMicrosoft 365やMicrosoft Office（パッケージ版）の利用率が高いという調査結果[6]があるため、攻撃者がそれらに関連する悪意のあるファイルを多く配布している可能性が考えられます。

図 1-9は国内と全世界におけるOSのシェアを比較したグラフです。Android OSに着目してみると、国内と全世界ではシェアの傾向に大きな違いが見られ、全世界は Android OSのシェアが最も高いことがわかります。このシェアの高さが影響し、全世界ではAndroidで動作するマルウェアの検出数が国内よりも高くなっていると推測されます。

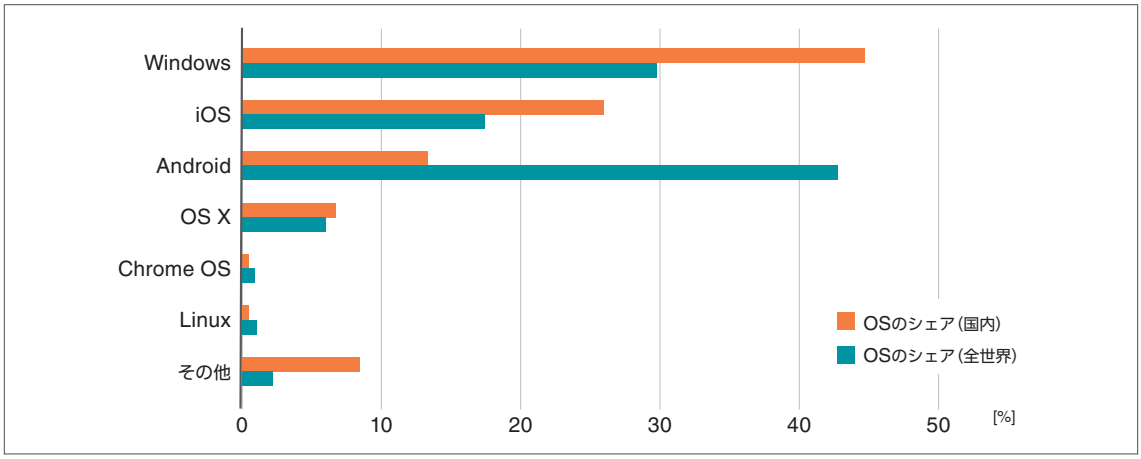

図 1-9　国内と全世界におけるOSの利用率（2022年）
※StatCounterのデータをもとに作成しています。

1.4. まとめ

本章では2022年のESET検出統計について紹介しました。
国内のマルウェア検出数は2020年下半期をピークに減少傾向に転じています。また国内と全世界ともに2023年は10月から11月にかけて検出数が大きく減少しました。これは主にWebブラウジング中に遭遇する脅威の減少が反映された結果です。検出数が減少している一方で、国内ではEmotetの感染を狙ったばらまきメールに関連するDOC/TrojanDownloader.Agent、詐欺被害につながるHTML/PharmacyやHTML/FakeAlertなど、2021年と比べて順位を上げているマルウェアが存在します。
マルウェア以外の脅威では、過去に発見された脆弱性を狙う攻撃が年間を通して多く観測されました。ファイル形式別検出数では、国内におけるMicrosoft製品の利用率やAndroid OSのシェア率から国内と全世界の傾向に違いが現れています。攻撃者による脅威は継続して存在するため、セキュリティ製品を導入して防御を怠らないようにすることや組織内の教育で従業員のITリテラシーを高めることなどを引き続き実施してください。また組織において資産管理を徹底し、脆弱性情報を確認した場合は速やかにパッチを適用してください。

---

1 2022年上半期サイバーセキュリティレポート ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/files/user/malware_info/images/ranking/pdf/CybersecurityReport_2022FirstHalf.pdf

2 ウイルス感染の警告とサポートへの電話番号が表示された ｜ 警視庁
https://www.keishicho.metro.tokyo.lg.jp/sodan/nettrouble/jirei/warning_screen.html

3 「Microsoft」のロゴを用いて信用させ、パソコンのセキュリティ対策のサポート料などと称して多額の金銭を支払わせる事業者に関する注意喚起 ｜ 消費者庁
https://www.caa.go.jp/notice/entry/023149/

4 そのセキュリティ警告画面・警告音は偽物です!「サポート詐欺」にご注意!!ー電話をかけない!電子マネーやクレジットカードで料金を支払わない!ー ｜ 独立行政法人 国民生活センター
https://www.kokusen.go.jp/news/data/n-20220224_2.html

5 Windows 11 gets better protection against SMB brute-force attacks ｜ Bleeping Computer
https://www.bleepingcomputer.com/news/microsoft/windows-11-gets-better-protection-against-smb-brute-force-attacks/

6 「Microsoft 365」と「Google Workspace」の利用状況（2021年）／前編 ｜ キーマンズネット
https://kn.itmedia.co.jp/kn/articles/2104/15/news019.html

2

マルウェアファミリーに着目したESET統計情報と上位マルウェアの紹介

第 2 章　マルウェアファミリーに着目したESET統計情報と上位マルウェアの紹介

2.1.　はじめに

ITが日々進歩する中で、悪意のあるプログラムであるマルウェアもその環境に合わせてテクニックを変化させています。マルウェアが悪用する手法はさまざまあり、その一例を表 2-1に示します。

表 2-1　マルウェアが悪用する手法の一例

手法	主な目的
プロセスを偽装する	マルウェアの存在を隠ぺいさせ、ユーザーやスレットハンティングから発見されにくくする
メモリー上に悪意あるペイロードを展開する	セキュリティ製品からの検知を回避する
パッカーや暗号化・符号化を用いて難読化する	耐解析機能を持たせ、解析やフォレンジックの難易度を上昇させる
ダウンローダーを利用する	攻撃者がマルウェアの更新や変更を容易に行えるようにする

表 2-1の手法が悪用された場合、バイナリのダウンロード/展開/実行を繰り返しながら複数の段階を経て目的のマルウェアに感染します。

さて、このように複数の段階を経てマルウェアに感染する検体の場合、それぞれの段階で展開される悪意あるバイナリに対してセキュリティ製品の検出名[i]が異なることをご存じでしょうか?

図 2-1はメール経由でマルウェア感染する場合を例に、各段階とESET検出名の関係を表したものです。この図はあくまで一例に過ぎませんが、感染のきっかけとなる最初の検体(図の一次検体)から最終的に端末上で悪意のある動作を行う検体(図の最終検体)に至るまで、それぞれ異なるESET検出名が付けられていることがわかります。

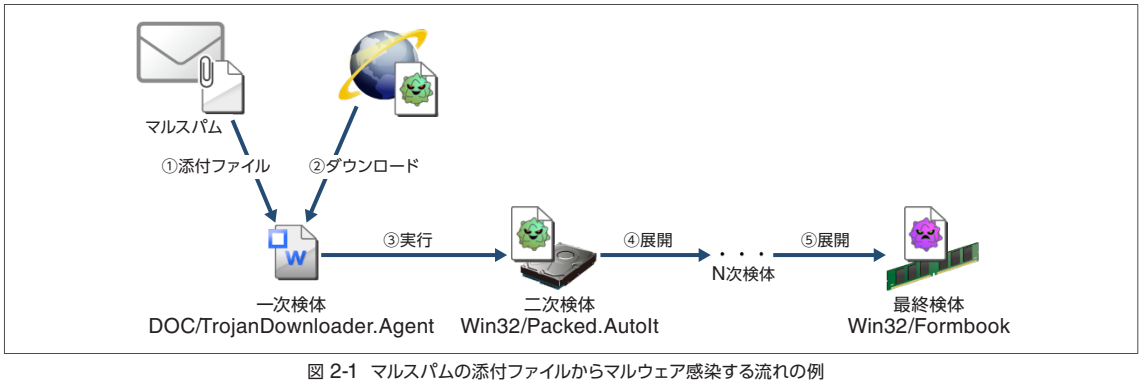

図 2-1　マルスパムの添付ファイルからマルウェア感染する流れの例

i　セキュリティ製品によっては、不正なバイナリに対する検出名だけでなく不正な通信に対する検出名(ESETの場合はSMB/Attack.Bruteforceなどが該当)が存在します。マルウェアによる不審な挙動を不正な通信に対する検出名で検出する場合があります。

最近のセキュリティ製品はメモリー上にファイルレスで展開される検体も含めて、各検体をリアルタイムあるいは定期的にスキャンしてマルウェアを検知します。しかし、定義ファイルの更新が行われていない場合や未知のファイル形式あるいは暗号化・符号化が使用されている場合などは、それぞれの段階で検知できず最終検体に感染してしまう可能性があります。また、そもそもセキュリティ製品をインストールしていなかった端末では、ユーザーが気づかないうちに最終検体に感染しているリスクがあります。

上記のように最終検体に至るまでの途中の段階で検知できなかった場合や既に感染が疑われる端末に対して、セキュリティ製品をインストールして最新の定義ファイルを適用した状態でスキャンすると、最終検体を含む各段階の検体を検出する可能性があります。このうち、特に最終検体として検出されるマルウェアは、難読化の解除やプロセスの偽装などが完了して実際に悪意ある動作を開始するバイナリであるため、マルウェアファミリー名を含む検出名である可能性が高くなると推測されます。

以上のことから、マルウェアファミリー名に着目してセキュリティ製品の検知ログを読み解くことで、組織にどのようなマルウェアの脅威が迫ったのか、そのマルウェアに感染することでどのような影響を受けるのかということを推測することができます。

2.2.　マルウェアファミリー名が含まれる2022年のESET検出統計

2022年の国内における、マルウェアファミリーに着目したESET検出統計は表 2-2のとおりです。なお本稿では、MITRE ATT&CKが定義するソフトウェア[1]以外のグレイウェアおよび汎用検出名に該当する検出名を除外しています。

表 2-2　マルウェアファミリー名を含むマルウェア検出数上位（2022年・国内）
※1位のMSIL/Spy.AgentTeslaの検出数を100とした相対値で算出しています。

順位	マルウェア	相対値	マルウェアファミリー名
1	MSIL/Spy.AgentTesla	100.0	AgentTesla
2	Win32/Formbook	61.7	Formbook
3	INF/Conficker	26.3	Conficker
4	Win32/TrojanDownloader.Delf	23.7	Delf
5	Win32/PSW.Fareit	18.9	Fareit（別名：Pony、Siplog）
6	Win32/Conficker	13.0	Conficker
7	JS/TrojanDownloader.Nemucod	10.5	Nemucod
8	MSIL/TrojanDownloader.Tiny	5.5	Tiny（別名：Tinba）
9	Win32/Rescoms	5.4	Rescoms（別名：Remcos）
10	Win32/Netsky	4.2	Netsky

検出数1位のAgentTesla[2]、検出数2位のFormbook[3]、検出数5位のFareit（別名:Pony、Siplog）[4]はいずれも情報窃取型のマルウェアです。メールまたはFTPのクライアントソフトに関連する認証情報、端末のスクリーンショット、キーボードの入力情報などを取得してC&Cサーバーに送信する機能を有しています。

検出数3位と6位のConficker[5]、検出数10位のNetsky[6]はどちらもワームの一種で、別の端末に感染を広げます。これに加えてConfickerは感染端末をボットネットに組み込んでスパムメールを配信する機能があり、Netskyは特定のサービスに対してDDoS攻撃を行う機能も確認しています。

検出数4位のDelfはトロイの木馬の一種で、オンラインゲームのパスワードを窃取したり、リムーバブルメディアを介して感染を広げたりする亜種が確認されているマルウェア[7]です。

検出数7位のNemucodはランサムウェアや情報窃取型のマルウェアなど、ほかのマルウェアを感染させるダウンローダーまたはドロッパーの機能を有したマルウェア[8,9]です。
検出数8位のTiny（別名:Tinba）はバンキングマルウェアであり、感染端末が銀行のWebサイトにアクセスすると、キー入力情報や送受信されるデータを窃取します。
検出数9位のRescoms（別名:Remcos）は、パソコンをリモートで操作および管理するソフトウェアとして販売されている製品です。しかし攻撃者によって感染端末を遠隔操作する目的で悪用されていることから、マルウェアファミリーに分類[10]されています。
以上の上位10種のマルウェアのうち最も検出数の多かったMSIL/Spy.AgentTeslaについて、日別検出数の推移から2022年の国内傾向を解説します。

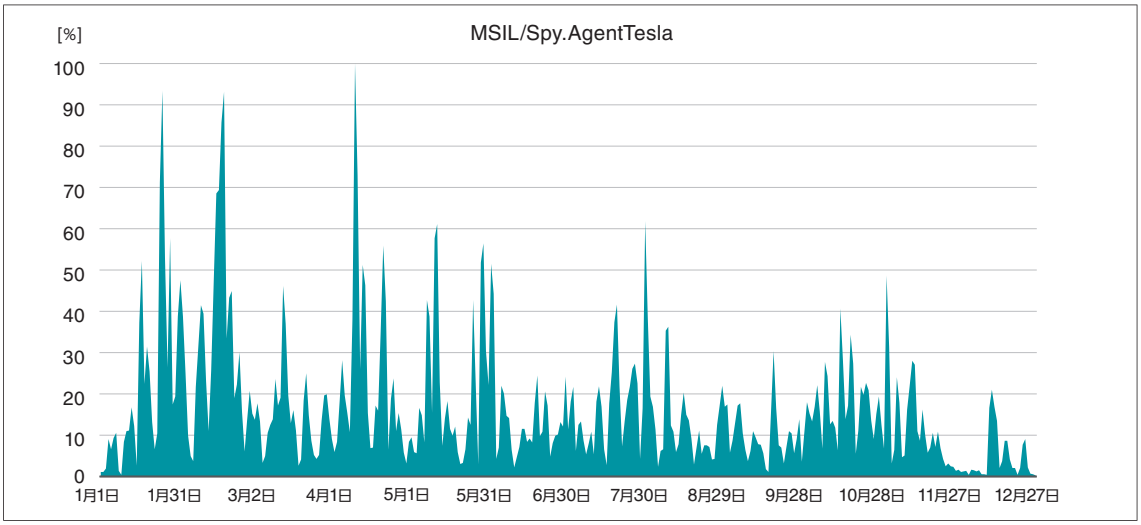

図 2-2　MSIL/Spy.AgentTeslaの日別検出数推移（2022年・国内）
※最も検出数の多かった4月10日を100%として算出しています。

2022年は上半期に検出数が多い傾向となりました。特に1月と2月、4月に検出数のピークが確認できます。さらに下半期は、7月から8月中旬および10月後半から11月にかけて高い検出数を観測しました。AgentTeslaを含む情報窃取型のマルウェアはアンダーグラウンドフォーラムで比較的安価に購入できることから、2021年後半以降に検出数が拡大傾向にあります[11]。よって2023年も依然として猛威を奮うことが考えられるため、引き続き警戒する必要があります。
次項では、マルウェアファミリーとして検出数の最も多かったAgentTeslaについてさらに深堀りします。

2.3. AgentTeslaとは

AgentTeslaは2014年に初めて確認された.NETベースのマルウェアであり、主に情報窃取を目的としています。一般的にAgentTeslaに感染すると、以下の情報を取得して攻撃者が用意したC&Cサーバーへ送信することが知られています。

●ソフトウェア(Webブラウザー、FTPクライアント、メールクライアント、VPNクライアント、遠隔操作ソフトウェア、インスタントメッセンジャーなど)に保存された認証情報
●暗号通貨ウォレットの情報
●キーボードの入力情報
●スクリーンショット
●クリップボードの情報
●OSやCPUなどのハードウェア情報

多くの検体はC&Cサーバーに対してSMTPで通信を行いますが、その他にもHTTPやFTPを利用して通信する検体や、TelegramやTorプロキシを悪用する検体もあります。
当初は公式のWebサイトから購入することができました[12]が、公式サイトが閉鎖した現在もアンダーグラウンドフォーラムでMaaS(Malware as a Service)として提供されています。現在出回っているAgentTeslaは難読化手法や機能の違いといった観点から、バージョン2およびバージョン3の2種類が確認されています[13]。
AgentTeslaは主にメールの添付ファイルを介して感染します。これまでにAgentTeslaの感染を狙った攻撃キャンペーンがいくつか確認されています。例えば2020年には新型コロナウイルスの感染拡大に乗じて悪意のある添付ファイルをクリックさせるマルスパムが日本国内で出回りました[14]。また、2022年には南米やヨーロッパの企業を標的にした攻撃キャンペーンが観測[15]されています。このように不定期でAgentTeslaの感染を狙った攻撃が世界中で観測されているため注意が必要です。

2.4. AgentTeslaの解析

2.4.1. 一次検体

ここからは2022年に確認されたAgentTeslaを紹介します。AgentTeslaの感染を狙ったマルスパムは、不審なURLが埋め込まれたメールでした。米国の運送会社であるFedEx社を騙っており、荷物の運送のために追加の手続きが必要である旨を本文に記載して本文の画像に埋め込まれたURLのクリックを誘導しています。このURLはチャット・通話サービスであるDiscordのファイル共有機能を悪用しており、Discordの正規ドメイン(cdn.discordapp.com)で構成されているためセキュリティ製品による検知を困難にしています。

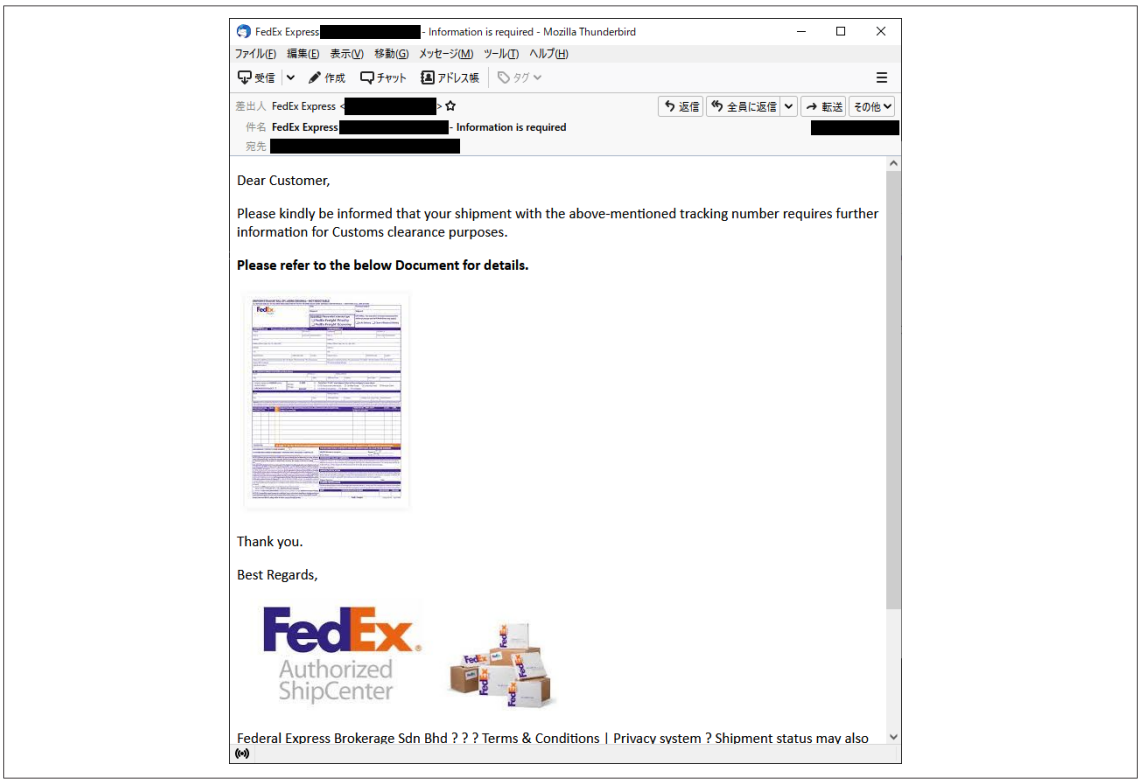

図 2-3　AgentTeslaの感染を狙ったマルスパム

URLにアクセスすると、不審なISOファイルがダウンロードされます。さらにこのISOファイルからはEXEファイル（以降一次検体とする）が展開されます。この一次検体は内部的に「BHhHUiu.exe」というファイル名が設定されています。また「Crypto Obfuscator For .Net」というツールによって難読化されており、ESET製品でスキャンすると「MSIL/Kryptik.AHQJ」で検出されました。

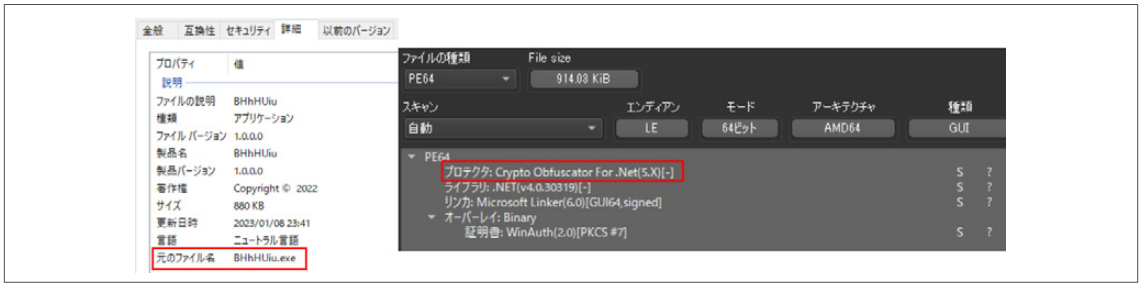

図 2-4　一次検体のファイル名と使用されている難読化ツール

一次検体はBase64エンコードされたデータを保持しています。一次検体を実行すると動的にこのデータがデコードされ、DLLファイルとEXEファイルがそれぞれ1つずつ展開されます。

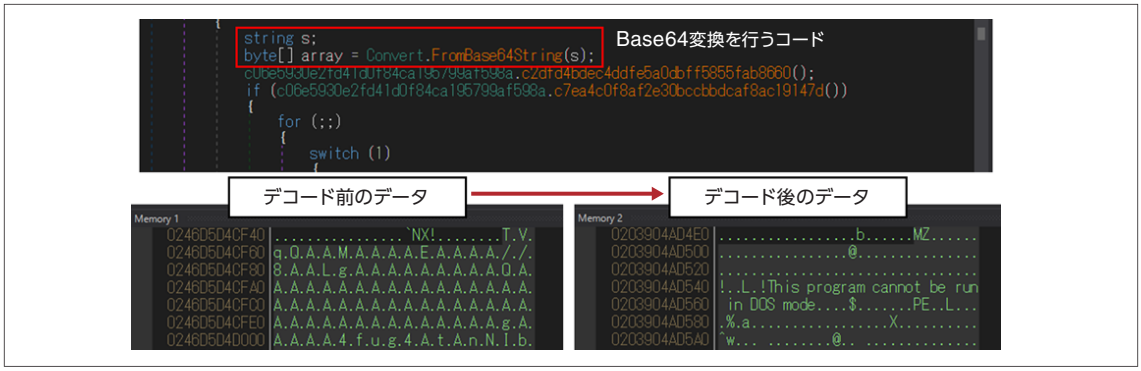

図 2-5　Base64デコードによりWindows実行形式ファイルが展開される様子

どちらのファイルも32bitアプリケーションであり、DLLファイルは「Hawk.dll」（以降二次検体とする）、EXEファイルは「sertGXVusAqHcGOkUCKb.exe」（以降三次検体とする）というファイル名が設定されています。また二次検体は一次検体と同様に「Crypto Obfuscator For .Net」で、三次検体は「Obfuscar」というツールで難読化されていました。ESET製品でそれぞれの検体をスキャンすると、二次検体は「MSIL/Injector.FCD」、三次検体は「MSIL/Spy.AgentTesla.C」で検出しました。

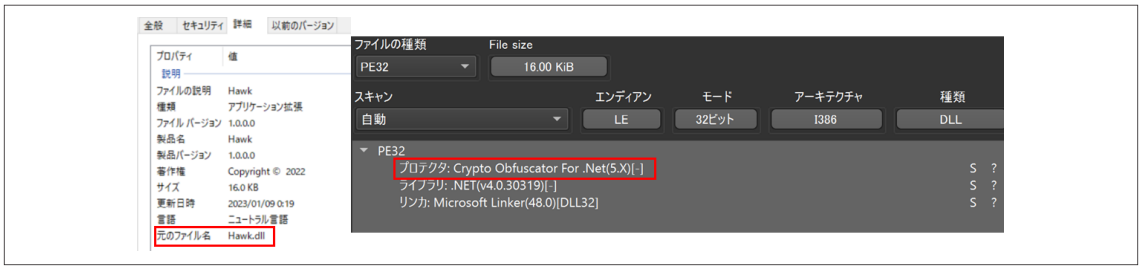

図 2-6　二次検体のファイル名と使用されている難読化ツール

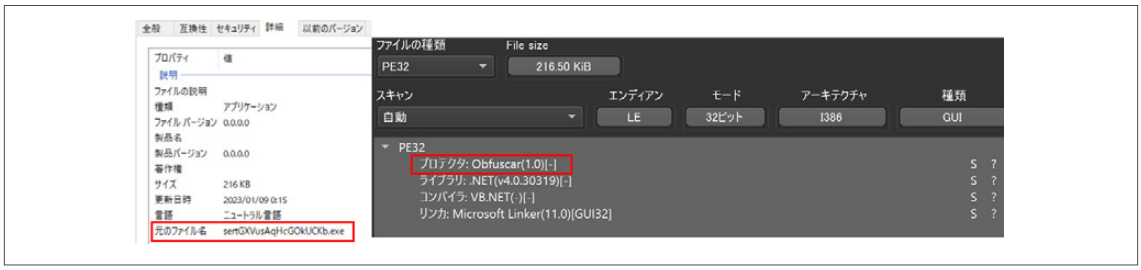

図 2-7　三次検体のファイル名と使用されている難読化ツール

二次検体と三次検体を展開後、Assembly.Loadメソッドで DLLファイルである二次検体のデータを読み込みます。そしてGetType.InvokeMemberメソッドにより、二次検体の「Hawk」ネームスペースに定義されている「Hawk」クラスの「Haw」メソッドを実行します。

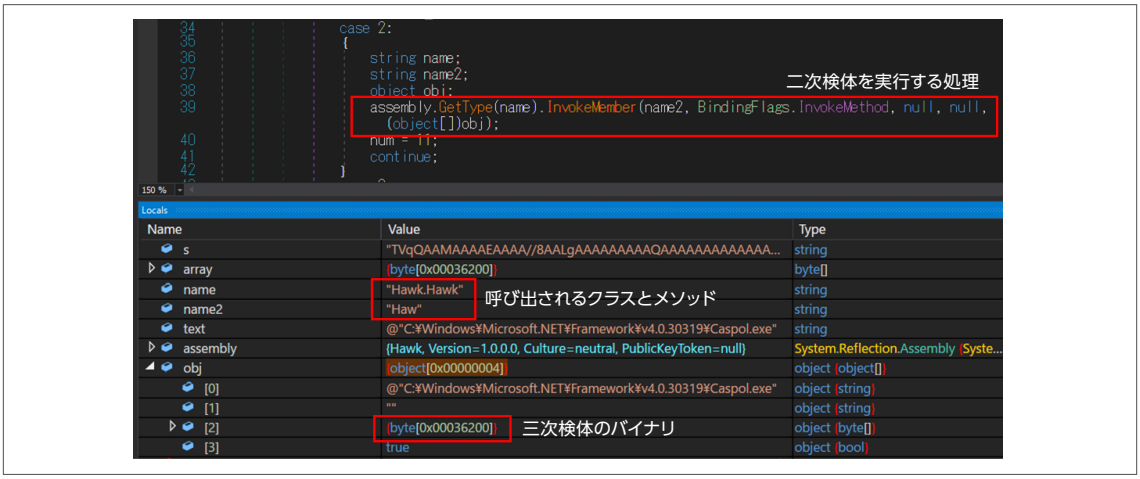

図 2-8　二次検体を実行する様子

2.4.2.　二次検体

二次検体は一次検体の処理の中で呼び出されます。この際、三次検体のバイナリを引数に与えられます。そして Process Hollowingと呼ばれる手法[16] を用いて三次検体を実行します。Process Hollowingによる三次検体が実行されるまでの流れは以下のとおりです。

①CreateProcessを実行して正規の.NET Frameworkツールの1つであるCaspol.exe[17]のプロセスを
　サスペンド状態で生成します。

②UnmapViewOfSectionを実行してCaspol.exeの一部の領域を削除します。

③WriteProcessMemoryを実行して削除した領域に三次検体のバイナリを書き込みます。

④SetThreadContextを実行してCaspol.exeのエントリーポイント[ii]を三次検体が実行されるように書き換えます。

⑤ResumeThreadを実行してCaspol.exeを起動します。

ii　プログラムの開始アドレスのことです。

図 2-9　Process Hollowingの処理の流れ

2.4.3.　三次検体

ESET検出名(MSIL/Spy.AgentTesla.C)から推測されるとおり、三次検体がAgentTesla本体であり、今回の一連のマルウェア感染における最終検体です。2.3節で述べたように、AgentTeslaはさまざまなソフトウェアに保存されている認証情報を窃取します。Google Chromeに保存された認証情報の窃取に着目してみると、認証情報が格納されているファイルを読み取り、対象のサービスがわかる情報[iii]と、そのサービスにログインするためのユーザー名およびパスワードを取得します。これらに加えてソフトウェアを識別する情報[iv]の合計4つのパラメーターを配列に格納します。

iii　Google ChromeではサービスのURLを確認しています。

iv　Google Chromeでは「Chrome」という文字列を確認しています。

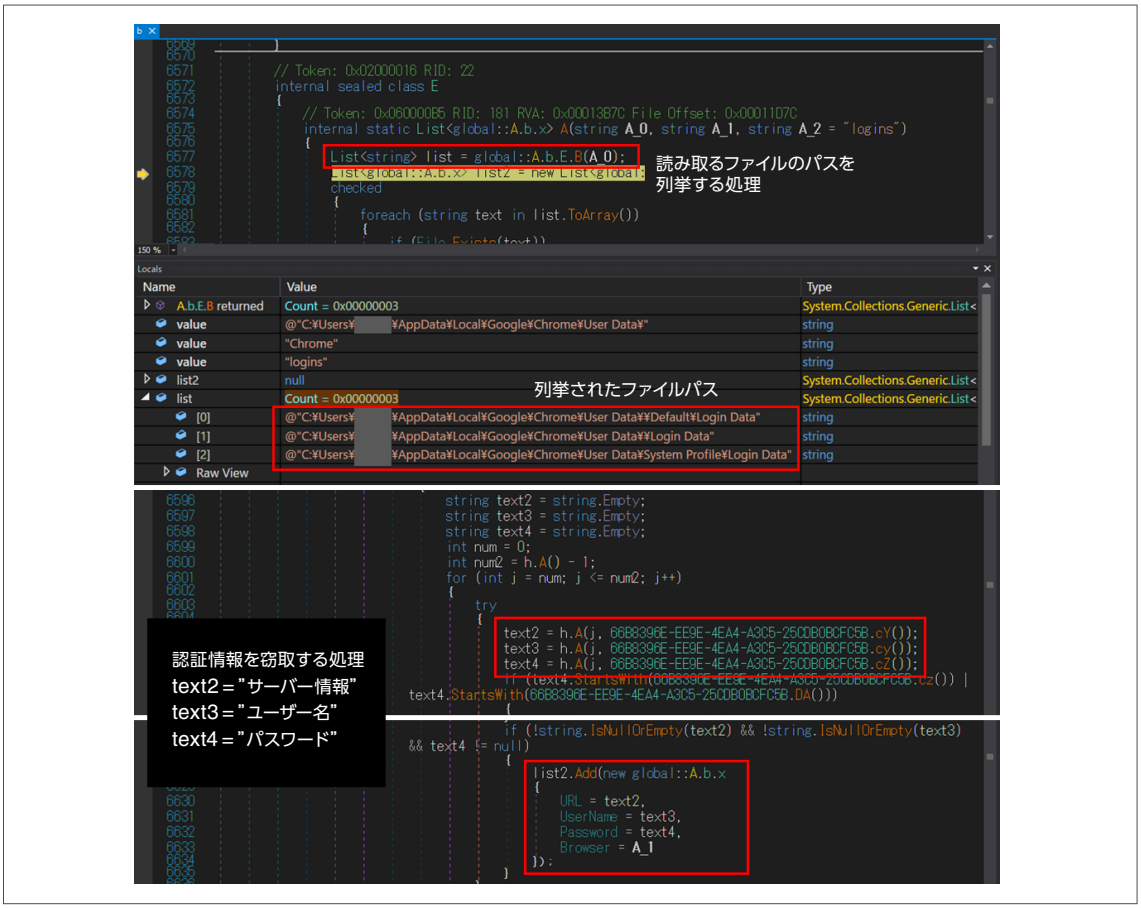

図 2-10　Google Chromeに保存された認証情報を窃取する様子

このような要領で Google Chromeを含むさまざまなソフトウェアの情報やキーボードの入力情報などを窃取します。三次検体から確認することができた窃取対象は表 2-3を参照してください。

表 2-3　三次検体の情報窃取対象

Webブラウザー	・Amigo　・BlackHawk Web Browser　・Brave　・CentBrowser　・Chedot ・Chromium　・Citrio　・Coccoc　・Comodo Dragon　・Comodo IceDragon ・CoolNovo　・Coowon　・Cyberfox　・Elements Browser　・Epic Privacy ・Falkon　・Firefox　・Flock　・GNU IceCat　・Google Chrome　・IceCat ・Iridium Browser　・Kometa　・K-Meleon　・Liebao Browser　・Microsoft Edge ・Opera Browser　・Orbitum　・Pale Moon　・QIP Surf　・QQ Browser ・Safari　・SeaMonkey　・Sleipnir 6　・Sputnik　・Torch Browser　・UC Browser ・Uran　・Vivaldi　・Waterfox　・Yandex Browser　・360 Browser　・7Star
FTPクライアント	・Core FTP　・FileZilla　・FlashFXP　・FTP Commander Pro　・FTPGetter ・FTP Navigator　・SmartFTP　・WinSCP　・WS_FTP
メールクライアント	・Becky! Internet Mail　・Claws Mail　・eM Client　・Eudora　・Foxmail ・IncrediMail　・Mailbird　・Microsoft Outlook　・Opera Mail　・Pocomail ・Postbox　・The Bat!　・Thunderbird
VPNクライアント	・NordVPN　・OpenVPN　・Private Internet Access
遠隔操作ソフトウェア	・RealVNC　・TigerVNC　・TightVNC　・UltraVNC　・WinVNC
インスタントメッセンジャー	・Internet Download Manager　・jDownloader　・Psi　・Trillian
データベースソフトウェア	・MySQL Workbench
端末の情報	・CPU情報　・IPアドレス　・OS情報　・Windows資格情報マネージャーの情報 ・キーボードの入力情報　・クリップボードの情報　・コンピューター名　・スクリーンショット ・メモリーサイズ　・ユーザー名

窃取した情報は外部サーバーに送信されますが、今回の三次検体はインスタントメッセンジャーの1つであるTelegramに対して送信されることを確認しました。このようにTelegramを悪用した通信はAgentTeslaのバージョン3に見られる特徴です。図 2-10はGoogle Chromeの情報を窃取した後にTelegramへ通信を行う様子を示しています。図中の番号の対応関係は以下のとおりです。

①TelegramのチャットID
②端末のユーザー名
③端末のコンピューター名
④端末のOS情報
⑤端末のCPU情報
⑥端末のメモリーサイズ
⑦感染日時
⑧端末のIPアドレス（接続元のIPアドレスを返す公開WebAPIサービス（api[.]ipify[.]org）から正しく取得できた場合に格納されます）
⑨Google Chromeに保存された認証情報（サーバー情報）
⑩Google Chromeに保存された認証情報（ユーザー名）
⑪Google Chromeに保存された認証情報（パスワード）

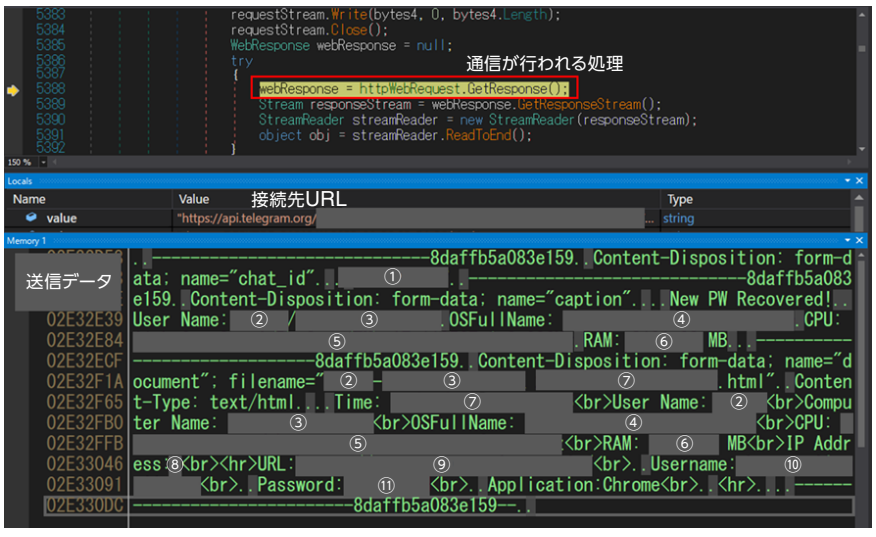

図 2-11　Telegramに対して窃取情報を送信する処理

2.4.4.　AgentTeslaのまとめ

今回紹介したAgentTeslaはメールの本文に記載されたURLへのアクセスから端末に侵入します。そのURLにアクセスするとISOファイルがダウンロードされ、ISOファイルから一次検体が展開されます。一次検体を実行すると二次検体を経てAgentTesla本体である三次検体に感染します。この三次検体はProcessHollowingの手法を用いて正規プログラムに自身の存在を隠ぺいします。最後に三次検体の処理によって、端末の情報や保存された認証情報が窃取され外部に送信されます。

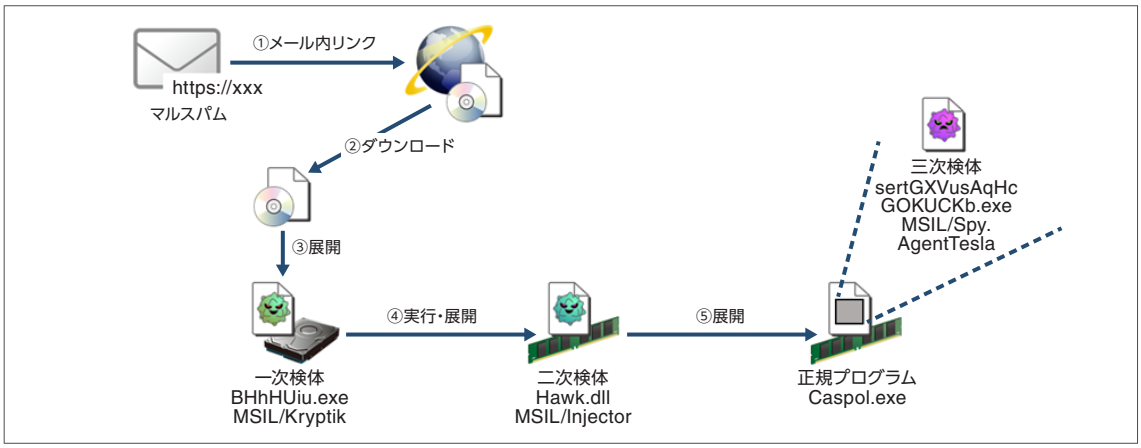

図 2-12　今回紹介したAgentTeslaの感染フローとESET検出名の関係

2.5.　まとめ

マルウェアの高度化に伴い、近年は複数の段階を経て目的のマルウェアに感染させる挙動が多く見られるようになりました。この段階ごとにさまざまなバイナリが展開されますが、今回紹介したようにセキュリティ製品によってそれぞれのバイナリの検知名は異なります。組織がどういったマルウェアに狙われているのか、マルウェア感染によってどのような影響を受けたのかといったことを把握するために、検知名の違いを把握したうえでセキュリティ製品のログを分析することが重要です。
またマルウェアを確実に検知および駆除するために、セキュリティ製品のバージョンや定義ファイルを定期的に更新する、定期的に端末をスキャンするなど、セキュリティ製品の正しい運用を心がけてください。

1 Software ｜ MITRE ATT&CK
https://attack.mitre.org/software/

2 2021年10月 マルウェアレポート ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2110.html

3 チェック・ポイント、2022年8月に最も活発だったマルウェアを発表　FormBookがEmotetに代わり首位、GuLoaderとJokerが急浮上 ｜ PR TIMES
https://prtimes.jp/main/html/rd/p/000000144.000021207.html

4 Pony or Fareit Malware Analysis, Overview by ANY.RUN
https://any.run/malware-trends/pony

5 「コンフィッカー」ワームの脅威を振り返る ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/trend/detail/170316.html

6 インターネットセキュリティの歴史 第20回「Netsky ウイルス」 ｜ JPCERT/CC
https://www.jpcert.or.jp/tips/2008/wr083301.html

7 Delf ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/term/detail/00027.html

8 ASCII.jp：専門家も混乱!?　新しいNemucodランサムウェアが登場!
https://ascii.jp/elem/000/001/205/1205310/

9 継続は力なり：ダウンローダー Nemucod、進化しつつ認証情報窃取を試みる ｜ Palo Alto Networks
https://unit42.paloaltonetworks.jp/unit42-practice-makes-perfect-nemucod-evolves-delivery-obfuscation-techniques-harvest-credentials/

10 Remcos, Software S0332 ｜ MITRE ATT&CK
https://attack.mitre.org/software/S0332/

11 ESET Threat Report T1 2022
https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf

12 AgentTesla ｜ Juniper Networks
https://blogs.juniper.net/en-us/threat-labs-knowledge-base/agenttesla

13 Threat Thursday : Agent Tesla Infostealer ｜ BlackBerry
https://blogs.blackberry.com/en/2021/06/threat-thursday-agent-tesla-infostealer-malware

14 新型コロナウイルス感染症関連組織を狙うフィッシング攻撃 日本も標的に ｜ Palo Alto Networks
https://unit42.paloaltonetworks.jp/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/

15 AgentTesla is threatening businesses around the world with a new campaign ｜ Avast Threat Lab
https://decoded.avast.io/pavelnovak/agenttesla-is-threatening-businesses-around-the-world-with-a-new-campaign/

16 Process Injection: Process Hollowing, Sub-technique T1055.012 – Enterprise ｜ MITRE ATT&CK
https://attack.mitre.org/techniques/T1055/012/

17 Caspol.exe (コード アクセス セキュリティ ポリシー ツール) ｜ Microsoft
https://learn.microsoft.com/ja-jp/dotnet/framework/tools/caspol-exe-code-access-security-policy-tool

3

2022年に確認された
不正アクセスによる
セキュリティインシデント

第３章　　2022年に確認された不正アクセスによるセキュリティインシデント

3.1.　2022年に起きたセキュリティインシデントについて

2022年も多くのセキュリティインシデントが公表されました。インシデントの種類もさまざまあり、情報漏えい・ランサムウェア感染・Webサイト改ざん・不正ログインなどが挙げられます。実際に、決済サービス提供企業への不正アクセスによる情報漏えいや自動車関連企業・医療機関といった組織におけるランサムウェア被害を報道で目にしたことがあると思います。これらのインシデントを引き起こす要因の1つとして、不正アクセスが挙げられます。不正アクセスとは、本来アクセス権限を持たない者が、サーバーや情報システムの内部へ侵入を行う行為です[1]。その手段もさまざまで、脆弱性を悪用するケースや不正に認証を突破するケースがあります。被害と手口がさまざまである不正アクセスによるセキュリティインシデントを振り返り、対策の気づきを得ることも重要です。
本章では、サイバーセキュリティラボで公開情報を元に調査し、2022年に確認された不正アクセスによるセキュリティインシデントの集計結果を組織別や規模別、被害別、業種別に紹介します。

3.2.　2022年に起きた不正アクセスによるセキュリティインシデントの集計結果

本節では、2022年に確認された不正アクセスによる国内のセキュリティインシデントの集計結果を紹介します。インシデント報告書のタイトルや本文中に不正アクセスへの言及があったものを今回の集計対象としています。また、集計したインシデント報告書は、2022年に第一報が公表された報告書のうち、レポート執筆時点（2023年1月26日）に確認できたものです。そのため、実際のインシデント発生日が 2021年の報告書も集計に含まれています。そして、インシデントによっては、サービスの提供先と提供元の双方で公表が行われているケースがあります。そのようなケースでは、提供元のインシデントを1件として集計しています。
以上の条件で集計を行い、2022年1月1日～2022年12月31日に214件の不正アクセスによるセキュリティインシデントを日本国内で確認しました。
セキュリティインシデントは発覚から公表までに時間を要すること、また公表義務がないインシデントもあることから、実際はより多くのセキュリティインシデントが発生していると考えられます。

●組織別集計と組織規模別集計

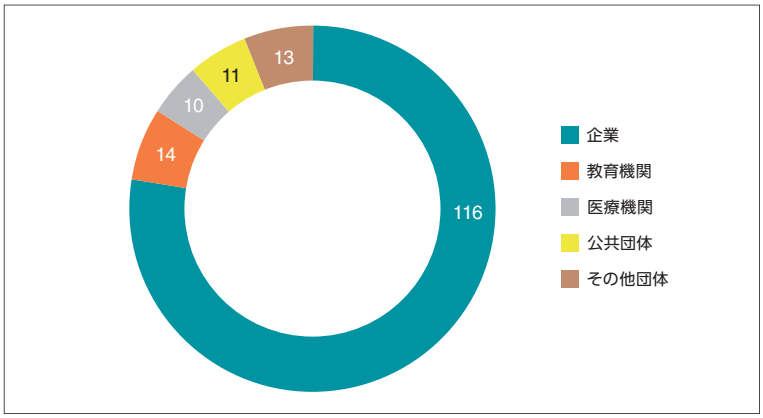

図 3-1　不正アクセスによるセキュリティインシデントの組織別集計（2022年・国内）

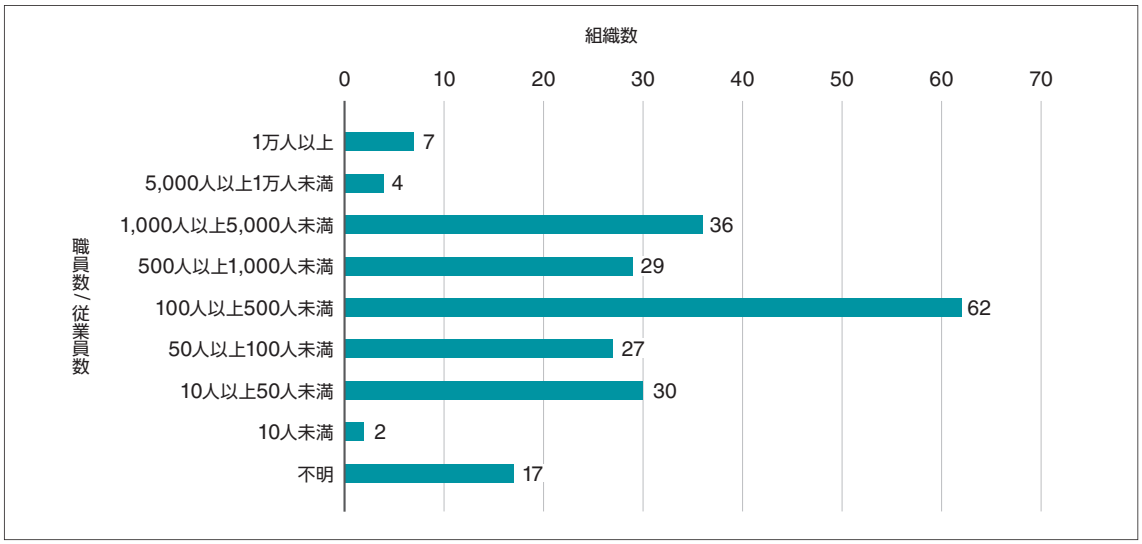

図 3-2　不正アクセスによるセキュリティインシデントの組織規模別集計（2022年・国内）

最も公表が多かった組織は、企業でした。そして、学校や医療機関が、その後に続きます。
そもそも他の組織と比較して企業数が多いため、組織別集計にも影響を与えています。また、2022年には学校や医療機関を狙ったサイバー攻撃が多く発生したこともあり、第2位と第3位になっていると考えられます。これらの組織を規模ごとに分類したものが、図 3-3です。
最も報告が多い規模は、100～500人の組織でした。国内における100～500人の組織数が多いためと考えられます。また、個人情報やクレジットカード認証情報といった攻撃者が欲しい情報は、組織の規模に関わらず保有しているケースがあります。そのため、攻撃者はあらゆる規模の組織を対象にし、その中でも攻撃しやすいセキュリティ対策が追い付いていない組織を狙います。結果として、100～500人の組織で多くの被害が生じていると考えられます。また、大きな組織への攻撃の足掛かりにするために、関連組織を狙うサプライチェーン攻撃などが起きていることも考えられます。
一方で、一般的にセキュリティ対策が取られていると考えられる規模の大きい組織においても、被害が確認されています。組織内で利用している製品やツールが多く、管理できていない脆弱性を狙われることや関連組織経由で攻撃されている可能性が考えられます。

●企業業種別集計

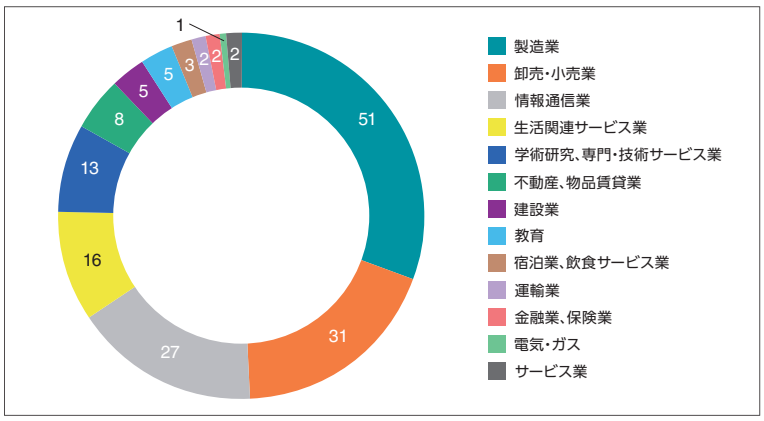

図 3-3　不正アクセスによるセキュリティインシデントの企業業種別集計（2022年・国内）

集計した業種を見ると、製造業が最も多く、卸売・小売業と情報通信業がその後に続いています。製造業は企業数が多いこと、卸売・小売業はECサイトで個人情報を扱うことが多いことが、要因として考えられます。
被害が多かった業種の上位3つを、被害別に分類したものが図 3-4です。

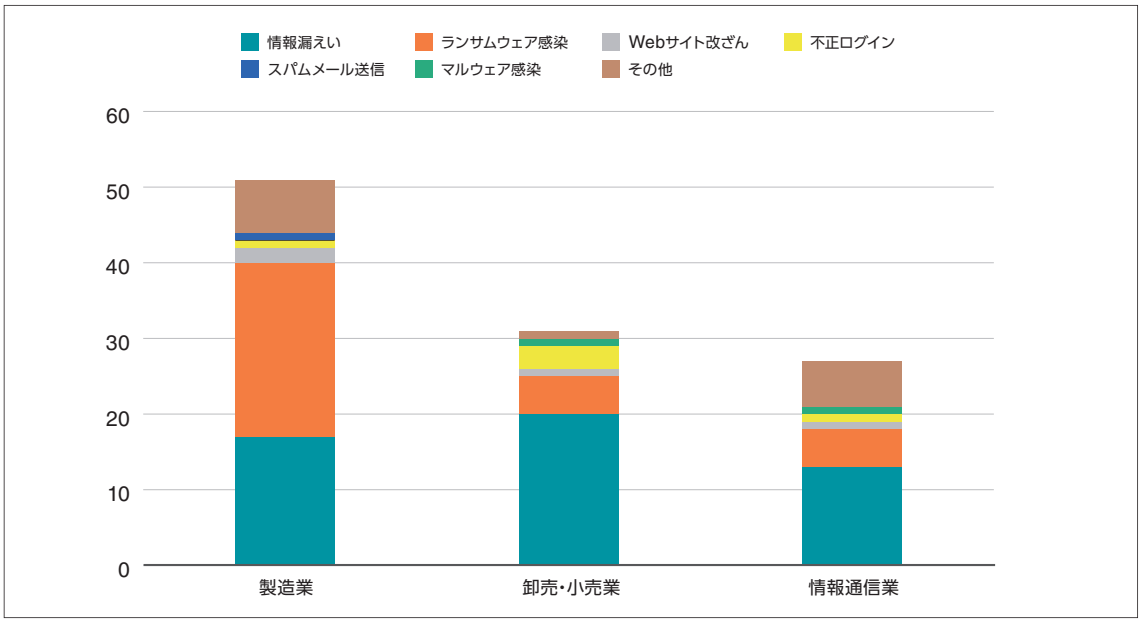

図 3-4　インシデント報告数上位3つの業種の被害別集計（2022年・国内）

製造業は企業数が多いため、それぞれの被害の件数も多くなっています。また、関連企業やグループ会社が多いため、サプライチェーン攻撃による情報漏えいやランサムウェア被害といった特定の企業を狙った被害が起きていることも考えられます。卸売・小売業 では、ECサイトなどでクレジットカード情報や顧客の情報を扱うことが多いため、標的になりやすく情報漏えいに繋がる不正アクセス被害に遭っていることが考えられます。また、情報通信業では、サイバー空間における資産が多いことから、被害に遭遇しやすくなっていると考えられます。

●被害別集計

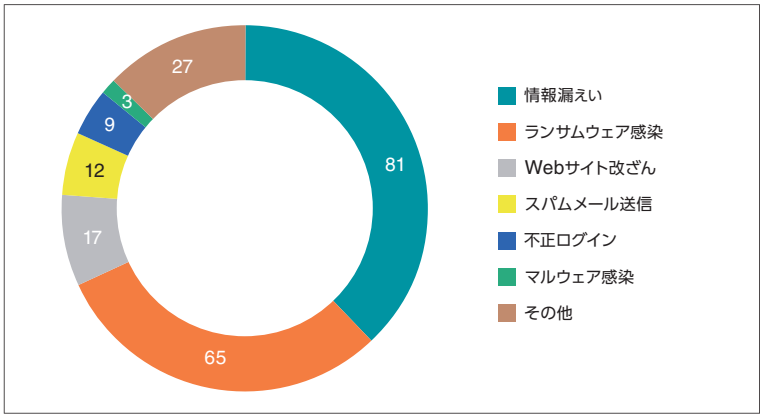

図 3-5　不正アクセスによるセキュリティインシデントの被害別集計（2022年・国内）

最も公表が多かったセキュリティインシデントは、情報漏えいでした。今回の集計では、情報漏えい以外の被害に振り分けたインシデントにおいても、情報漏えいの可能性があるものがありました。実際には、図 3-5の件数以上の情報漏えいインシデントが発生しています。
漏えいした可能性のある情報もさまざまありました。代表的な漏えい情報として、クレジットカード情報や氏名・住所、メールアドレスなどの個人情報を確認しています。
クレジットカード情報については、企業側では保持していないケースでも、Webアプリケーションが改ざんされたことで窃取されている事例がありました。
情報漏えいの次に多かったインシデントは、ランサムウェア感染です。2022年は、自動車関連企業や医療機関において、多くのランサムウェア被害が報道されました。図 3-5中のランサムウェア感染においても、自動車関連企業をはじめとした製造業（23件）と医療機関（7件）での公表を確認しています。製造業の23件は企業の業種では最も多く、医療機関の7件は企業を除く組織の中では最多となっています。
また、これらの組織におけるランサムウェア被害は、データ暗号化や情報流出だけでなく工場の操業停止や診療停止といったフィジカル空間での被害に繋がっています。
身代金を支払う可能性が高い組織や特定の業種を狙っている可能性もありますが、脆弱性を放置した状態の製品やツールを利用していることや、不用意に通信ポートを開けているといった攻撃者にとって攻撃しやすい環境かどうかも大きな要因だと考えられます。
次項では、被害に繋がった不正アクセスの原因について紹介します。

3.3. 不正アクセスによるセキュリティインシデントへの対策について

3.3.1. 不正アクセスの原因について

今回集計したインシデントの原因を「脆弱性を悪用した攻撃」「認証を狙った攻撃」「機器・システムを狙った攻撃」「機器・システムの設定不備」「クライアントでのマルウェア感染」「その他」に分類しました。公表されたインシデント報告書の中には、調査中であることやセキュリティの観点から不正アクセスの原因が公開されていないものもあります。今回は、原因について言及があった129件を集計しています。

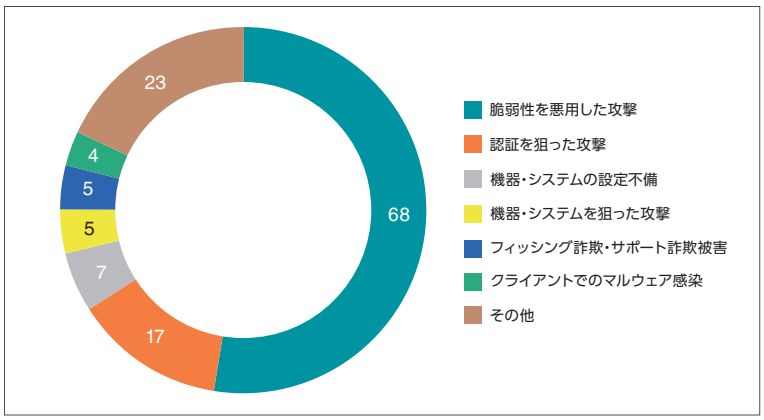

図 3-6 不正アクセスの原因別集計（2022年・国内）

多くのインシデントにおいて、不正アクセスの原因となったのは、「脆弱性を悪用した攻撃」でした。「脆弱性を悪用した攻撃」は、さまざまな脆弱性が悪用されています。図 3-6の「脆弱性を悪用した攻撃」をさらに分類したものが図 3-7です。詳細については後述します。
次に多く確認された原因は、「認証を狙った攻撃」です。認証を狙った攻撃では、過去に流出したIDとパスワードを用いたパスワードリスト攻撃やブルートフォース攻撃を確認しています。具体的には、VPN機器といったネットワーク機器や会員サイトやモバイルアプリを対象とした攻撃がありました。また、1章の「マルウェア以外の脅威の検出数TOP10」にも、ブルートフォース攻撃の検出が入っており、攻撃が多いことがわかります。
ほかにも、フィッシング詐欺によって認証情報を窃取されたケースやサポート詐欺によって攻撃者に不正アクセスされたケースを確認しています。また、今回の集計では、マルウェア感染の原因が言及されていないものを「クライアントでのマルウェア感染」に分類しています。多くの場合は原因の記載があるため、この分類の数は多くありません。

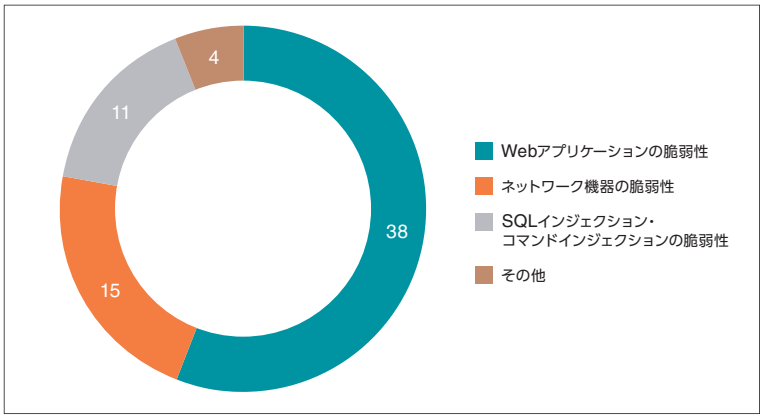

図 3-7　脆弱性を悪用した攻撃と認証を狙った攻撃の詳細（2022年・国内）

最も多く悪用されていたのは、Webアプリケーションの脆弱性でした。Webサーバー上のアプリケーションやCMS（Contents Management System）の脆弱性が悪用されていました。これらの脆弱性は、情報漏えいのインシデントの原因として主に確認しており、そのインシデント数に影響を受けています。直近では、CVE-2021-41773（Apache HTTP Serverの脆弱性）やCVE-2022-22965（Spring Frameworkの脆弱性）といった脆弱性が確認されており、1章の「マルウェア以外の脅威の検出数TOP10」の第3位と第10位に入っています。
次に多かったものは、ネットワーク機器の脆弱性です。
直近では、CVE-2018-13379やCVE-2019-11510といったVPN製品の脆弱性が多く確認されており、CISAをはじめとした各国の機関が共同で公開した2021年に悪用された脆弱性の上位15種[2]に入っています。
3つ目に多かったものは、SQLインジェクションやコマンドインジェクションといった脆弱性です。古くから悪用されている脆弱性ですが、今もなお悪用されています。

3.3.2.　不正アクセスの原因への対策

前項で紹介した原因の中で最も多く確認された「脆弱性を悪用した攻撃」とそれに次いで多かった「認証に対する攻撃」への対策について紹介します。

①脆弱性を悪用した攻撃への対策
- ・組織内で使用しているハードウェアとソフトウェアを把握・管理
- ・脆弱性に関する情報の収集
- ・脆弱性に対するセキュリティパッチの早急な適用

特に組織内でシステムやアプリケーションを構築している場合は、構築に使用しているツールなどを見落としてしまう可能性があるため、注意が必要です。
アメリカでは、SBOM(Software Bill of Materials)の整備・普及が進められています。
SBOMとは、製品に含むソフトウェアを構成するコンポーネントや互いの依存関係、ライセンスデータなどをリスト化した一覧表です[3]。リストでコンポーネントやソフトウェアの脆弱性を管理することで、脆弱性の情報収集を容易にし、脆弱性の把握漏れを防止する効果が期待されます。日本でも経済産業省を中心に整備が進められており、SBOM利用の推奨やソフトウェア提供企業へのSBOMの義務化といった施策なども考えられます。
SBOMは、脆弱性管理だけでなくオープンソースソフトウェアのライセンス管理でも有用です。組織内のセキュリティ担当者やソフトウェアを管理している方は、今後の動向に是非注目してください。

②認証に対する攻撃への対策
<サービス提供者の場合>
- ・多要素認証の導入
- ・ログイン試行回数の制限
- ・アクセス可能なIPアドレスの制限
- ・管理者用ID、パスワードの流出の有無を確認
- ・パスワードは使い回さず、強固なものを使う

<ユーザーの場合>
- ・利用しているID、パスワードの流出の有無を確認
- ・パスワードは使い回さず、強固なものを使う

過去に流出したパスワードを利用し続けていたことが、不正アクセスに繋がった事例を確認しています。また、パスワードを使い回していると、別のアカウントやシステムで被害に遭う可能性があります。流出の有無を確認する場合、「Have I Been Pwned[4]」といったWebサイトの利用が効果的です。

3.4.　まとめ

本章では、2022年に確認された不正なアクセスによるセキュリティインシデント集計結果を紹介しました。多くの情報漏えいやランサムウェア感染といった被害を確認しました。
また、2022年のセキュリティインシデントを振り返る目的で集計を行いました。さまざまな要因によって公開時期や内容の粒度は組織によって異なりましたが、被害防止に繋げるためにも、インシデント公表のタイミングや内容について検討が必要だと思われます。JPCERT/CCからも「サイバー攻撃被害情報の共有と公表のあり方について[5]」という報告書が公表されています。
そして、インシデント発覚時の初期対応の1つとして、所管の警察署やIPA、JPCERT/CCといった機関への報告・相談を行ってください。

1　不正アクセスとは？ | 総務省 安心してインターネットを使うために国民のためのサイバーセキュリティサイト
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_risk_06.html

2　2021 Top Routinely Exploited Vulnerabilities | CISA
https://www.cisa.gov/uscert/ncas/alerts/aa22-117a

3　SBOM(Software Bill of Materials) | NRI SECURE キーワード解説
https://www.nri-secure.co.jp/glossary/sbom

4　Have I been pwned
https://haveibeenpwned.com/

5　サイバー攻撃被害情報の共有と公表のあり方について(公開版) | JPCERT/CC
https://www.soumu.go.jp/main_content/000762951.pdf

4

病院を狙うサイバー攻撃の増加とその背景

第 4 章　　病院を狙うサイバー攻撃の増加とその背景

4.1.　はじめに

2021年10月31日、徳島県の公立病院がランサムウェアを用いたサイバー攻撃の被害を受け通常診療の停止を余儀なくされました。このサイバー攻撃により引き起こされた通常診療の停止期間は 2ヶ月に及び、再開は年をまたいだ 2022年となりました[1]。現在、医療機関の業務は電子カルテシステムなど、多くの ITシステムに支えられています。電子カルテシステムは、受診者の名前や生年月日、住所といった個人情報、病状や既往歴、処方されている薬など過去の診療記録を保存しているほか、検査機器、会計システムとも連携しています。このため、この公立病院の事例のように ITシステムで発生した障害の影響が医療機関の業務全体に及ぶことも珍しくありません。

米ミネソタ大学の研究によると、米国の医療機関に対するランサムウェアによる攻撃数は、2016年から 2021年にかけて 2倍以上に増加したとされています[2]。日本国内においても医療機関へのサイバー攻撃の被害報告が相次ぐ中、厚生労働省は2022年3月、「医療情報システムの安全管理ガイドライン[3]」を改訂し、医療機関等[i]に対してランサムウェアによる攻撃への備えを求めるなど、医療機関のサイバー攻撃対策強化を計っています（表 4-1）。

日本における医療機関とは、医療法で定められた医療提供施設のことを指します。中でも医療サービス（医業・歯科医業）を行う医療機関としては、病院と診療所が規定されています。本章では私たちにとって最も身近な医療機関である病院と診療所を主に取り上げ、サイバー攻撃による医療機関の被害事例と医療機関が被害を受けるとどのような事態が発生するのかを解説します。

表 4-1　日本における医療機関のサイバー攻撃対策強化施策（2022年）

2022年3月	医療情報システムの安全管理ガイドライン第5.2版	医療情報システムに関する全体構成図および、システム責任者一覧整備（6章2節）や、ランサムウェアによる攻撃を含む非常時に備えたバックアップの実施と管理やセキュリティ体制の整備（6章10節）などを規定
2022年4月（施行）	改正個人情報保護法	医療機関を含む事業者に対し、サイバー攻撃などにより個人データの漏えいなどが発生し、個人の権利利益を害するおそれがあるときは、個人情報保護委員会への報告および本人への通知が義務化（第26条）
2022年度（令和4年度）	診療報酬改定[4]	病床数が400床以上の保険医療機関について、診療情報管理体制加算の施設基準として以下の2点を追加 ①専任の医療情報システム安全管理者を配置 ②定期的に必要な情報セキュリティ研修（少なくとも年1回程度）の実施 また、医療情報システムのバックアップ体制の確保が望ましいことを要件に加え、定例報告において、当該体制の確保状況について報告を求める

i　病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等

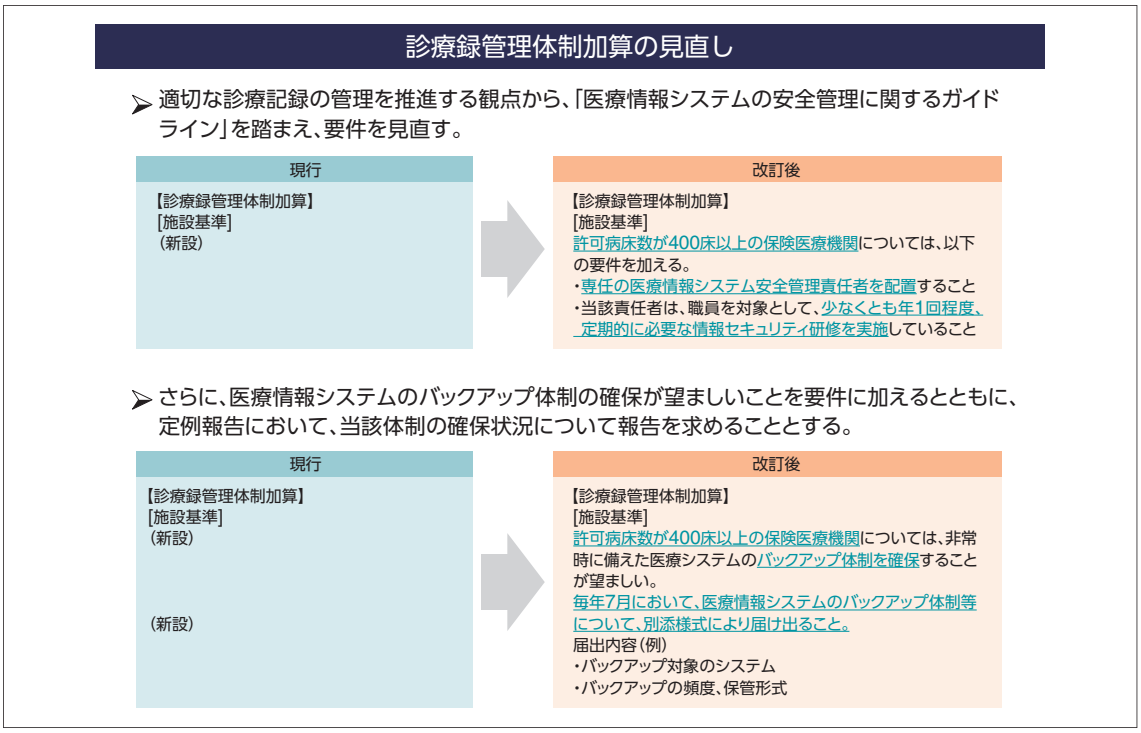

図 4-1　診療録管理体制加算の見直し
※出典：「令和4年度診療報酬改定の概要」(厚生労働省)を加工して作成しています。[4]

4.2.　サイバー攻撃による医療機関の被害

本節では、サイバー攻撃による国内の医療機関の被害事例を紹介します。医療機関がサイバー攻撃の被害を受けた際に発生する影響を実際の事例から解説します。

4.2.1.　　サイバー攻撃による国内の医療機関の被害事例

日本国内においても複数の医療機関からサイバー攻撃による被害事例が報告されています。
執筆時点(2023年1月10日)で一般公表されているサイバー攻撃による国内医療機関の被害事例から、被害の発覚時期が2021年以降のものを紹介します。
日本国内の病院・診療所からは2021年には5件、2022年には11件の被害が報告されています(表 4-2)。今回集計した被害報告件数は16件でしたが、サイバー攻撃の被害に遭ったとしてもそれを一般には公表しないケースを考慮すると、これよりも多くの被害が発生していると考えられます。
被害を受けたサイバー攻撃の種別をみると、ランサムウェアを用いた攻撃が16件の被害報告のうち8件と半数を占めています(図 4-2)。その他不正アクセスに集計した事例の中にも、公表情報の中にランサムウェアと明示されてはいないものの、電子カルテシステムや患者情報データベースにアクセスできなくなるなど、ランサムウェアによる攻撃が疑われるものが含まれています。また、2022年3月には「2022年上半期サイバーセキュリティレポート[5]」でも取り上げたマルウェアEmotetによる被害が2件報告されています。ランサムウェアを用いた攻撃などのサイバー攻撃によりシステム障害が発生した結果、次のような影響が発生したことが報告されています。

●診療業務の停止、または縮小
●診療会計業務の停止
●受診者の住所、氏名、年齢、既往歴などの個人情報の漏えい

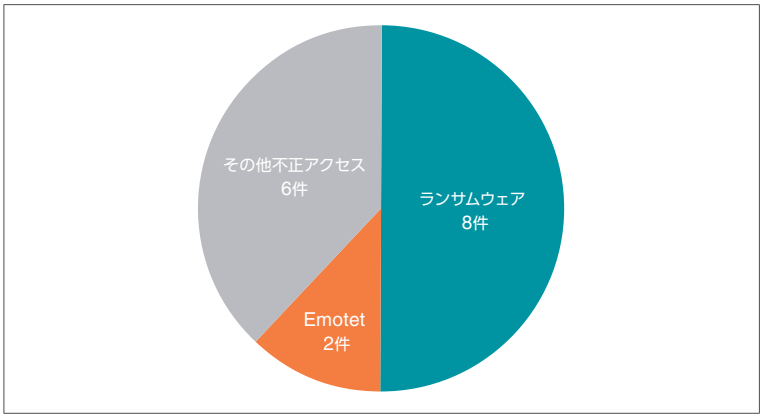

図 4-2　病院・診療所へのサイバー攻撃の種別内訳（国内）

表 4-2　サイバー攻撃による病院・診療所の被害事例（国内・2021年以降）
※サイバーセキュリティラボ調べ

時期		医療機関	被害内容
2021年	1月	公立病院（静岡県）	メールアカウント1件が不正アクセスを受け、大量の迷惑メールが送信された
	5月	公立病院（大阪府）	医用画像参照システムサーバーに対する不正アクセスがあり、一部データベースが破壊される[6]。ランサムウェア（REvil）を用いた攻撃と報道[7]
	7月	民間病院（神奈川県）	メールアカウント2件が不正アクセスを受け、これらのアカウントより大量の迷惑メールが送信される
	10月	民間病院（静岡県）	外部からの不正アクセスを受け、システムの一部に障害が発生。調査の結果、サーバー内で保管・管理されていた情報の一部が海外のサーバーへ流出した可能性があることが判明[8]。ランサムウェアを用いた攻撃と報道[9]
	10月	公立病院（徳島県）	ランサムウェア（LockBit2.0）により電子カルテシステムに障害が発生。新規患者の受け入れを2ヶ月間停止
2022年	1月	大学付属病院（東京都）	サーバーがマルウェアに感染し、電子カルテが使用できなくなる。一部の診療などを停止し、4日後に再開
	1月	民間病院（愛知県）	外部から不正アクセス（疑い）。これにより電子カルテシステム、医事会計システムのプログラムに不具合が生じる[10]。ランサムウェアを用いた攻撃と報道[11]
	2月	大学付属病院（愛知県）	教職員のメールアカウントが第三者により不正にアクセスされ、個人情報が含まれる電子メールが閲覧された可能性[12]
	3月	公立病院（沖縄県）	職員のパソコンがマルウェア（Emotet）に感染。職員を名乗る不審なメール（なりすましメール）が、複数の関係者へ発信される[13]
	3月	公立病院（栃木県）	院内ネットワークに接続している事務処理用のパソコン1台がマルウェア（Emotet）に感染。同端末上のメールソフトで過去にやり取りした関係者の名前を名乗る不審メールが送信されていることを確認[14]
	4月	民間病院（大阪府）	ランサムウェア（LockBit2.0）により電子カルテシステムに障害
	5月	民間病院（岐阜県）	不正アクセスにより患者情報データベースへのアクセスができなくなる。最大で約11万3千人の個人情報流出の可能性[15]
	6月	民間病院（徳島県）	ランサムウェア（LockBit2.0）によるシステムへの侵入被害を受け、電子カルテ、院内LANシステムが使用できなくなる[16]
	10月	民間病院（静岡県）	ランサムウェア（種別不明）を用いた攻撃により電子カルテシステムが使用できなくなる[17]
	10月	公立病院（大阪府）	ランサムウェア（Phobos亜種）による攻撃により、電子カルテシステムに障害が発生し、緊急以外の手術や外来診療の一時停止など2ヶ月に及び通常診療ができなくなる[18,19]
	12月	民間病院（石川県）	不正アクセスにより電子カルテの一部が閲覧できなくなる[20]

4.3.　医療機関を狙うサイバー攻撃が増加する要因

4.3.1.　ランサムウェア攻撃者グループの動向

2020年3月に新型コロナウイルス感染症の世界的流行の中で、一部のランサムウェア攻撃者グループから「新型コロナウイルス感染症がまん延している間は医療機関を標的としない」といった声明がリリースされていました[21]。また、ランサムウェア攻撃者グループの中には独自のアフィリエイトルールの中で医療機関に対する攻撃可否ポリシーを定めているグループもあります。LockBitもそうしたグループのひとつであり、医療関係組織への攻撃に関して次のようなポリシーが示されています。

It is allowed to very carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries, especially those that change sex and force to be very careful in Thailand, as well as any other organizations provided that they are private and have rhubarb.
It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals and the like, that is, those institutions where surgical procedures on high-tech equipment using computers may be performed.
It is allowed to steal data from any medical facilities without encryption, as it may be a medical secret and must be strictly protected in accordance with the law. If you can't pinpoint whether or not a particular medical organization can be attacked, contact the helpdesk.

(製薬会社、歯科医院、美容整形外科のような医療関連機関は慎重かつ選択的に攻撃することを許可します。心臓病センター、脳神経外科、産婦人科医院など、ファイルの破損が死につながる可能性のある施設、つまりコンピューターを使ったハイテク機器の手術が行われる可能性のある施設の暗号化は禁止します。医療機関のデータを暗号化せずに盗み出すことは許可します。医療機関のデータは医療機密である可能性があり、法律に基づき厳重に保護する必要があるためです。特定の医療機関が攻撃可能かどうかを特定できない場合は、ヘルプデスクにお問い合わせください。)

しかし、こうした声明やポリシーの主張とは裏腹に、現実として医療機関へのランサムウェアを用いたサイバー攻撃は確認されています。表 4-2で示した被害事例の中にも、紹介したアフィリエイトプログラムを掲げるLockBitによるものとされるランサムウェア攻撃が複数含まれています。こうした攻撃者の主張と被害実態の不一致がランサムウェア攻撃者グループの総意なのか一部のアフィリエイトパートナー[ii]によるものなのかは判断できませんが、攻撃者の主張に関わらず、適切な対策を講じることが必要と考えられます。

ii　ランサムウェア攻撃者グループが運用するサービス(RaaS(Ransomware as a Service))の利用者。攻撃の実行者

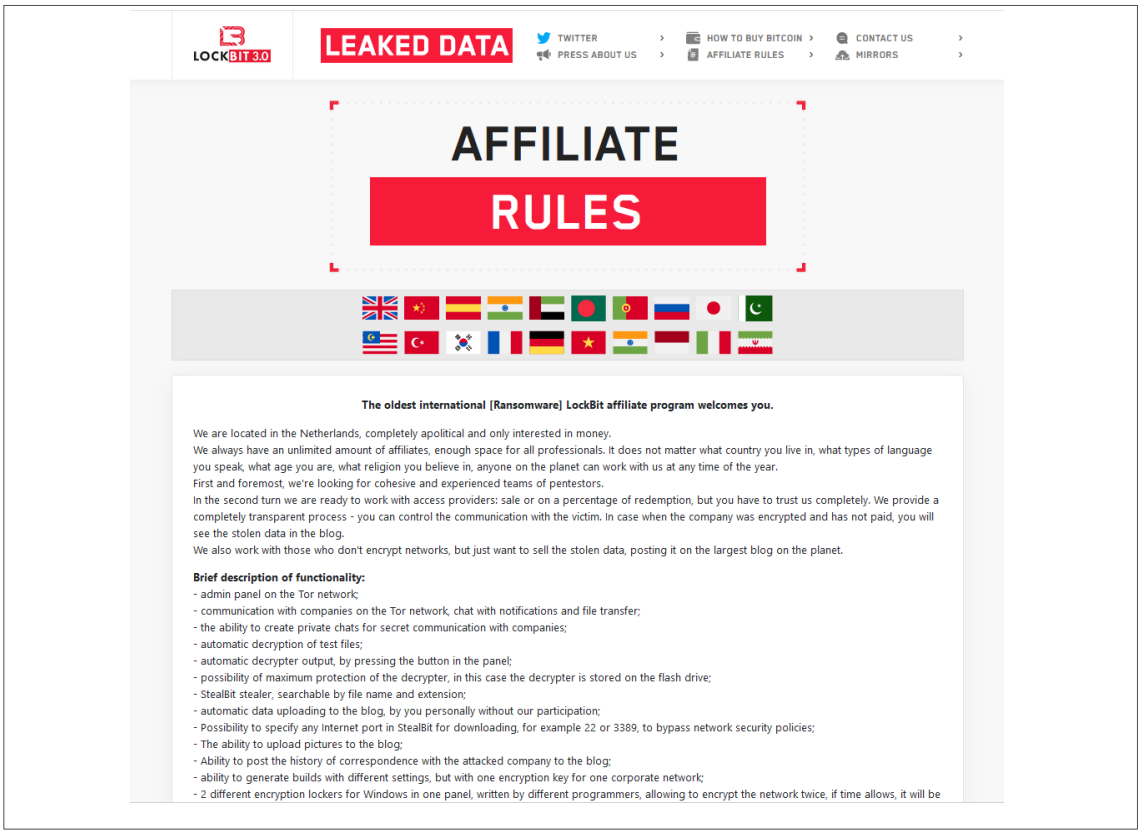

図 4-3　LockBit 3.0 Affiliate Rules

4.3.2.　医療機関を狙ったサイバー攻撃の影響拡大の背景

IT活用により医療機関を取り巻く環境も変化しています。こうした変化や医療機関特有の事情の中にも、医療機関を狙ったサイバー攻撃の増加とその影響拡大につながる要因があります。

●医療分野の情報化

旧来、カルテをはじめとする紙媒体で記録・保管されていた医療情報のデータ化が急速に進んでいます。一例として電子カルテシステムの普及率は、厚生労働省による調査結果によると2008年時点の一般病院[iii]全体で14.2%でしたが、2020年時点では一般病院全体で57.2%、病床数400以上の一般病院に限定すると91.2%に及ぶことが示されています(表 4-3)[22]。これまで紙でやりとりしていた院内業務や医療機関間における情報連携を効率的に行えることが期待される一方で、医療分野が情報化されたことにより医療機関がサイバー攻撃の対象となり、サイバー攻撃によるシステム障害の影響が大きくなったと考えられます。

●医療機関ネットワークと外部ネットワークの接続増加

ほかの組織と同様に医療機関の業務も組織単独で実施することはできません。外部サービスの利用や、導入システムのリモートメンテナンスのため、インターネットを含む外部のネットワークと接続されています。こうした外部ネットワークとの接続を通じてサイバー攻撃が行われた事例も確認されています。

iii　病院のうち、精神科病床のみを有する病院および結核病床のみを有する病院を除いたもの

●セキュリティ予算の不足

四病院団体協議会が、2022年1月31日から2月28日に四病院団体協議会の加盟病院5,596件を対象に実施したセキュリティアンケートに関する調査結果では、年間のセキュリティ予算が500 万円未満と回答した病院の割合が51%を占め、回答した病院全体の45%が現在のセキュリティ予算が十分ではないと回答しています。診療報酬という公定価格に基づく病院の収支構造上、十分なセキュリティ予算を計画的に捻出することが困難であり、予算の制約上、本来病院として実施すべきと考えるセキュリティ対応も結果的に行えなくなっていると推測されています[23]。

表 4-3　電子カルテシステムの普及状況（厚生労働省の公表情報より作成）

	一般病院全体	病床規模別		
		400床以上	200～399床	200床未満
2008年	14.2%	38.8%	22.7%	8.9%
2011年	21.9%	57.3%	33.4%	14.4%
2014年	34.2%	77.5%	50.9%	24.4%
2017年	46.7%	85.4%	64.9%	37.0%
2020年	57.2%	91.2%	74.8%	48.8%

2021年 10月に徳島県の公立病院がランサムウェアを用いたサイバー攻撃の被害を受けた事例では詳細な報告書が公開されています。報告書ではランサムウェアの初期侵入として以下のように述べられています[1]。

電子カルテを始めとした医療機器のメンテンナンス等を行う際に接続する VPNのみが侵入経路と考えられ、当該ネットワークにおいて VPN装置の脆弱性が放置されていた事実、また脆弱性を使い取得された VPN装置の管理者の資格情報がダークウェブで公開されていた事実[24]を鑑みると、VPN装置の脆弱性を悪用した侵入が考えられ、当該ネットワークを悪用して侵入した可能性が極めて高い。

さらに、サポート期限切れ OSの使用や短いパスワードの使用、ログオンに失敗した際に一定時間ログオンを制限するロックアウトの設定が無効になっていた点に加えて、電子カルテシステム、医事会計システムの動作が不安定になるという理由から脆弱性管理を実施せず、かつ、ウイルス対策ソフトの動作を停止し、OSやアプリケーションのアップデートを停止していたことなども、被害を拡大した情報システムの問題点として挙げられています。

VPN装置の脆弱性に関しては、その他の被害事例でも初期侵入経路として指摘されており、前述の四病院団体協議会が実施したセキュリティアンケートに関する調査結果では、内閣サイバーセキュリティセンターや厚生労働省が脆弱性を指摘したVPN製品・ソリューション[25]を使用する病院の割合は 40%であり、そのうちの66%は脆弱性への対応を行っているものの、状況不明も含めれば未対応が34%を占めていることが示されています[23]。

また、サイバー攻撃の初期侵入経路は医療機関自身のみではありません。2022年10月の大阪府の公立病院の事例では、ランサムウェアの侵入口は取引業者のシステムである可能性が高いとされています。病院と取引業者は VPNにより接続されていました。この VPNで使用する VPN装置のファームウェアが古く初期侵入経路として悪用された可能性が指摘されています[26]。「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）（厚生労働省）[25]」で述べられているとおり、自組織のみならずサプライチェーン全体を俯瞰し、発生が予見されるリスクを医療機関等自身でコントロールできるようにする必要があることから、関係事業者のセキュリティ管理体制を確認した上で、関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき、脆弱性対策を実施することが重要です。

4.4.　対策

セキュリティ対策で実施すべきことは医療機関であってもほかの組織と大きく変わりません。システム運用に際し注意すべき点をご紹介します。

●ガイドラインやチェックリストの活用

さまざまな機関が、調達時のセキュリティ要件の参考となるガイドラインやチェックリストを公開しています（例:医療情報システムの安全管理ガイドライン（厚生労働省）[3]）。こうしたガイドラインやチェックリストに従うことにより、想定される脅威に対抗することができます。

●構成管理の徹底

利用しているハードウェア、ソフトウェア、クラウドサービスなどの製品・サービスのベンダー、ライセンスなどの契約内容、設定などの構成要素を把握し、常に最新に保ち続けるようにしてください。障害が発生した際など構成情報が必要となったとき、すぐに確認できるようにしておくことも重要です。

●非常時に備えたバックアップの実施と管理

自然災害やシステム障害だけではなく、ランサムウェア攻撃のようにデータ自体が利用不能となるような事態も考慮し、バックアップデータまで被害が拡大することのないよう、バックアップを保存する記録媒体などの種類、バックアップの周期、世代管理の方法を検討することが重要です。バックアップデータを保存した媒体をネットワークから切り離して保管することも有効です。

●教育と訓練の実施

サイバー攻撃の初期侵入経路は公開サーバーやVPN機器だけではありません。一般職員に届いたメールの添付ファイルや表示したWebページからマルウェアに感染する事例も多く報告されています。定期的にセキュリティ教育やトレーニングを行い、セキュリティ上の脅威への理解を深め、取るべき対策・行動を組織内で共有することが重要です。

●脆弱性への対応

サプライチェーン攻撃では、利用している製品の脆弱性が悪用されるケースが多く確認されています。セキュリティアップデートがリリースされている場合は速やかに適用を検討してください。また、必要に応じて、脆弱性診断サービスを定期的に利用し、脆弱性の対応漏れが発生していないか確認することも有効です。

●ロギングとモニタリング

クライアントやサーバー、ネットワーク機器やセキュリティ製品のログを保存し、万が一の事態が発生した際に、取引先や社会全体に対し説明責任を果たすことも重要となります。また、保存したログをモニタリングすることで攻撃の兆候にいち早く気づくことができます。

●インシデント対応の明確化

インシデント発生時の対応を明確化しておくことも、有効な対策です。何から対処すればいいのか、何を優先して守るのか、インシデント発生時の対応を明確にすることで、万が一の事態が発生したときにも、慌てずに対処することができます。

●情報収集と情報共有

最新の脅威に対抗するためには、日々の情報収集が欠かせません。当社をはじめ、各企業・団体から発信されるセキュリティに関する情報に目を向けましょう。 また、同じ業種・業界の企業は、同じ攻撃者グループに狙われ、同じマルウェアや戦略が使われる可能性が高いと考えられます。業界ごとのISAC(Information Sharing and Analysis Center)[iv]における情報共有は特に効果的です。

4.5.　さいごに

本章では医療機関、特に病院・診療所を狙うサイバー攻撃に着目し、日本国内で報告された被害事例、攻撃者の動向、サイバー攻撃増加の要因について解説しました。医療業界の情報化は今後もより加速し、私たちの生活を支え、便利にしていくでしょう。その一方で、情報がデータ化されたことにより、サイバー攻撃が与える影響はより大きくなると考えられます。
守るべき法規制や参照するガイドラインは業界ごとに異なるとしても、対策すべき項目の根幹は医療機関とほかの組織で大きく変わりません。情報化と並行してセキュリティ対策もアップデートしながら安全な運用を心がけ、このような攻撃に備えることが重要です。

---

1 コンピュータウイルス感染事案有識者会議調査報告書について ｜ 徳島県つるぎ町立半田病院
https://www.handa-hospital.jp/topics/2022/0616/index.html

2 Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021 ｜ JAMA Health Forum
https://jamanetwork.com/journals/jama-health-forum/fullarticle/2799961

3 医療情報システムの安全管理に関するガイドライン　第5.2版(令和4年3月) ｜ 厚生労働省
https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html

4 令和4年度診療報酬改定説明資料等について ｜ 厚生労働省
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000196352_00008.html

5 2022年上半期サイバーセキュリティレポートを公開 ～Emotetの再流行、脆弱性Log4shellを悪用した攻撃などを解説～ ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/220927.html

6 医用画像参照システムサーバへの不正アクセスに対する対応状況の経過報告について ｜ 市立東大阪医療センター
https://www.higashiosaka-mc.jp/news/notice/20210924_notice.html

7 事前に警鐘が鳴らされていたのに身代金脅迫ウイルスに襲われた東大阪の病院 ｜ 毎日新聞
https://weekly-economist.mainichi.jp/articles/20210803/se1/00m/020/025000c

8 システム障害に関するお詫びとお知らせ(2021/11/04) ｜ 富士病院
http://www.yuurinkouseikai.or.jp/info/20211104.asp

---

iv　業界内での情報共有・分析・連携の取り組み推進を図る組織。米国大統領令によって設立された米国の非営利団体が発祥

9 「記者さん、わかりますか?」身代金ウイルスに侵された病院の苦悩 | 朝日新聞
https://www.asahi.com/articles/ASQ2D6TRTQ28ULZU013.html

10 不正アクセス(疑い)によるシステム障害発生のお知らせ | 春日井リハビリテーション病院・附属クリニック
http://www.kreh.or.jp/2022/01/19/3837/

11 [サイバーテロ　病院の危機]<5>対策の不備　責任重く…「経営層が賠償」可能性 | 読売新聞
https://www.yomiuri.co.jp/national/20220222-OYT1T50041/

12 名古屋大学への不正アクセスによる個人情報流出について | 名古屋大学医学部附属病院
https://www.med.nagoya-u.ac.jp/hospital/news/news/2022/02/24135730.html

13 沖縄県病院事業局の職員を騙った不審メールに関するお詫びと注意喚起について | 沖縄県立中部病院
https://chubuweb.hosp.pref.okinawa.jp/news/2022/03/post-26110/

14 那須南病院におけるコンピューターウイルス感染と関係者への不審メール発生に関するお詫びとお知らせ | 南那須地区広域行政事務組合
http://www.minaminasukouiki.jp/wp-content/uploads/2022/03/20220303kokuchi.pdf

15 不正アクセスによる個人情報等流出の可能性に関するお知らせとお詫び | 幸紀会医療福祉グループ
http://www.koukikai.gr.jp/wp-content/uploads/2022/07/42995092c93cf84701e532ad245bbd0e.pdf

16 令和4年6月20日　サイバー攻撃による被害について(第1報) | 医療法人久仁会　鳴門山上病院
https://kyujinkai-mc.or.jp/info/20220620/

17 電子カルテの不具合について | 医療法人社団 真養会 田沢医院
http://shinyoukai.or.jp/tazawa-clinic/news/20221101.html

18 「電子カルテシステム」の障害発生について | 大阪府急性期・総合医療センター
https://www.gh.opho.jp/pdf/info20221031.pdf

19 診療体制の復旧について(第9報) | 大阪府急性期・総合医療センター
https://www.gh.opho.jp/pdf/info20230110.pdf

20 コンピューターの不正アクセスによる障害発生について | 医療法人社団博友会　金沢西病院
https://www.knh.or.jp/news/2022/12/08/%e3%82%b3%e3%83%b3%e3%83%94%e3%83%a5%e3%83%bc%e3%82%bf%e3%83%bc%e3%81%ae%e4%b8%8d%e6%ad%a3%e3%82%a2%e3%82%af%e3%82%bb%e3%82%b9%e3%81%ab%e3%82%88%e3%82%8b%e9%9a%9c%e5%ae%b3%e7%99%ba%e7%94%9f%e3%81%ab/

21 Ransomware Gangs to Stop Attacking Health Orgs During Pandemic | BLEEPING COMPUTER
https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/

22 医療分野の情報化の推進について | 厚生労働省
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/index.html

23 四病院団体協議会セキュリティアンケート調査結果(最終報告)
https://www.hospital.or.jp/pdf/06_20220323_01.pdf

24 VPN機器8.7万台分の認証情報が公開 - Fortinetが注意喚起 | Security NEXT
https://www.security-next.com/129771

25 医療機関等におけるサイバーセキュリティ対策の強化について(注意喚起) | 厚生労働省
https://www.mhlw.go.jp/content/10808000/001011666.pdf

26 大阪の病院は取引業者からランサムウエアがなぜ広がった?「攻撃の横展開」に注意 | 日経XTECH
https://xtech.nikkei.com/atcl/nxt/column/18/00001/07441/

5

なぜ、脆弱性対応が放置されるのか

第 5章　なぜ、脆弱性対応が放置されるのか

最近のサイバー攻撃、特にランサムウェアの感染原因は、うっかりミスなどの人間の過失より、脆弱性を悪用されるケースが多くなっているようです[1]。そして、悪用される脆弱性は、その対策方法が公開されていないゼロデイ(0-day) と言われる脆弱性ではなく、脆弱性に関する情報や対策方法が既に公開されている脆弱性を悪用するケースが多いようです。本章では、なぜ対策方法が公開されている脆弱性が、対応されず放置されてしまうのかについて考察します。

5.1.　最近のインシデント

IPAが2022年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から決定した「情報セキュリティ10大脅威2023」の組織編[2]の1位は「ランサムウェア被害」でした。そして、この「ランサムウェア被害」は2020年から3年連続で1位にランキングされています。JNSAも同様に「セキュリティ十大ニュース」を毎年公表しています。昨年末に公表された「JNSA 2022セキュリティ十大ニュース」[3]では、5位に「大阪急性期・総合医療センターでランサム被害」とランサムウェアによる事案が取り上げられています。また1位「ロシアがウクライナへ軍事侵攻」に次いで2位の「取引先企業へのサイバー攻撃でトヨタ自動車の国内全工場が稼働停止」は、実は国内の仕入れ先のランサムウェアによるシステム障害が原因でした。

表 5-1　IPA情報セキュリティ2023より

■情報セキュリティ10大脅威 2023　　圏外：昨年はランクインしなかった脅威

前年順位	個人	順位	組織	前年順位
1位	フィッシングによる個人情報等の詐欺	1位	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3位	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	5位	テレワーク等のニューノーマルな働き方を狙った攻撃	4位
7位	不正アプリによるスマートフォン利用者への被害	6位	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	7位
6位	偽警告によるインターネット詐欺	7位	ビジネスメール詐欺による金銭被害	8位
8位	インターネット上のサービスからの個人情報の搾取	8位	脆弱性対策情報の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの不正ログイン	9位	不注意による情報漏えい等の被害	10位
圏外	ワンクリック請求等の不当請求による金銭被害	10位	犯罪のビジネス化(アンダーグラウンドサービス)	圏外

表 5-2　JNSA 2022セキュリティ十大ニュース

第1位	2月24日	ロシアがウクライナへ軍事侵攻 ～国家間の戦争においてサイバー攻撃はどう位置付けられるのか?～
第2位	3月1日	取引先企業へのサイバー攻撃でトヨタ自動車の国内全工場が稼働停止 ～改めて浮き彫りになったサプライチェーン全体でのセキュリティ対策の重要性～
第3位	6月23日	全市民46万人余の個人情報が入ったUSBを紛失　尼崎市が発表 ～情報に　対する思いの　サイイタク（差異痛く／再委託）～
第4位	7月2日	KDDI大規模通信障害　丸2日間 ～119番通報を含むインフラに過去最大級の障害～
第5位	10月31日	大阪急性期・総合医療センターでランサム被害 ～人質は電子カルテ、外来診療や手術の停止など深刻な影響～
第6位	5月18日	経済安全保障推進法公布 ～国民生活や国家の安全確保の一端をサイバーセキュリティが担う時代が到来～
第7位	11月4日	休眠から再び戻ってきたEmotetが活動再開、猛威は続く ～活動開始から8年、進化を続けるEmotetに終焉は来るのか～
第8位	4月1日	改正個人情報保護法施行 ～迅速な法整備とそれに足並みを揃えた社会への展開が課題～
第9位	9月1日	デジタル庁発足1周年、期待と実績、改革は道半ば ～全員参加で大胆な改革を!～
第10位	7月11日	米国政府はLog4jの脆弱性に前例のない警鐘を鳴らした ～既に侵入されている?動き出した攻撃者に対策は間に合うのか～
番外	11月1日	ISMAP-LIU運用開始 ～Low-ImpactはHigh-Impactになるか、その影響力に期待～

このように近年、ランサムウェアによるインシデントが非常に多く発生し、特に医療機関での被害が目立ちメディアでも多く取り上げられることとなりました。

表 5-3　2021年4月以降に発生した主なランサムウェアのインシデント（国内中心）

時期		企業名	概要	原因・感染経路
2021年	5月	公立医療センター（大阪府）	医用画像参照システムサーバーがランサムウェア「REvil（レビル）」に感染し停止[4]	VPN機器の脆弱性
	6月	フィルムメーカー（東京都）	2021年6月1日夜にランサムウェアによるサーバーに対する不正アクセスを確認[5]	―
	7月	食品メーカー（東京都）	財務管理、販売管理といった主要な基幹システムサーバーやデータが暗号化。これにより、2022年3月期第3四半期報告書の提出が遅延[6]	―
	8月	建設コンサル（東京都）	サーバーがランサムウェア被害[7]。業務を委託していた東京都、群馬県、滋賀県、埼玉県、千葉県市川市などの業務に影響	―
	10月	民間病院（静岡県）	外部から不正アクセスを受け、システムの一部に障害が発生[8]	―
		民間病院（徳島県）	ランサムウェアにより電子カルテシステムに障害、新規患者の受け入れ停止、診療報酬の業務が停止[9] 「LockBit」が犯行声明（LockBit2.0）	VPN機器の脆弱性
		情報システム（東京都）	サーバーおよびPCに格納されたファイルが暗号化。拡張子が nightsky に変更	Webサービスの脆弱性を悪用しADサーバーに侵入
2022年	1月	民間病院（愛知県）	ランサムウェアにより電子カルテシステム、会計システムが停止[10]	VPN機器
	2月	愛知県	愛知県PCR検査システムがサイバー攻撃を受けランサムウェアに感染	―
		自動車部品メーカー（愛知県）	ランサムウェアにより、サーバーやパソコン端末の一部でデータが暗号化され、トヨタ自動車、トヨタ車体などの生産が一時停止[11]	リモート接続機器（子会社が特定の取引先との専用通信に利用）

表 5-3　2021年4月以降に発生した主なランサムウェアのインシデント（国内中心）

時期		企業名	概要	原因・感染経路
2022年	2月	自動車部品メーカー（奈良県）	複数のサーバーやPCが暗号化され一部の受発注業務や生産・出荷に遅れが発生[12]	ネットワークシステムの脆弱性が悪用
		シリコンウェハーメーカー（新潟県）	社内サーバーに不正アクセスされ製造、出荷が停止[13]。「Pandora（パンドラ）」から犯行声明がダークウェブ上に出され一部のデータが暴露	—
		食品製造メーカー（東京都）	ランサムウェアによる不正アクセスが発生[14]	従業員のリモートアクセス用機器の脆弱性が悪用
	3月	アニメーション制作会社（東京都）	社内サーバーやパソコン端末の一部のデータがランサムウェアに感染し暗号化[15]	ソフトウェアを外部サイトよりダウンロード
		菓子食品メーカー（東京都）	複数のサーバーへ不正アクセスされ内部の一部データがロック。当該企業が運営するECサイトで商品を購入したことのある164万人以上の個人情報が流出した可能性[16]	ネットワーク機器の脆弱性を悪用された可能性が高い
		アンテナメーカー（東京都）	ランサムウェアによりサーバーデータが暗号化されシステム障害発生[17]	—
	4月	ダイレクトマーケティング会社（東京都）	ランサムウェアにより勤怠・人事給与システムのユーザデータが暗号化され身代金を要求[18]	メンテナンス用のリモートデスクトップ接続環境から侵入と推測
		清酒メーカー（京都府）	ランサムウェアによるサイバー攻撃を受けサーバーデータが暗号化。お客様などの個人情報が流出した可能性が判明[19]	ネットワーク機器の脆弱性を悪用された可能性が高い
		建設会社（千葉県）	ランサムウェアの攻撃により、サーバーに保管されていたデータなどの一部が暗号化[20]	—
		民間病院（大阪府）	電子カルテシステムにランサムウェアの攻撃。院内のプリンターに英語のメッセージが大量に印刷、パソコンに英語で「金を支払え」と表示[21]	—
		電気設備部品メーカー（愛知県）	ランサムウェアによる不正アクセス攻撃を受け、サーバー内の一部のデータが暗号化（ランサムウェアの「CryptXXX」による攻撃）[22]	SSL-VPNの脆弱性が悪用
	5月	衣料品販売会社（埼玉県）	サイバー攻撃を受け、社内のシステムの一部に障害[23]。「LockBit2.0」と名乗るハッカー集団が、インターネット上の闇サイトで当該企業のデータを盗み取ったと主張	—
	6月	民間病院（徳島県）	ランサムウェアLockbit 2.0 によるシステムへの侵入被害を受け、電子カルテ、院内LANシステムが使用不能[24]	—
		教育サポート会社（東京都）	管理を委託している外部サーバーが、ランサムウェアによるとみられる攻撃を受け、サーバー内のデータが暗号化[25]	—
	7月	商工会議所（名古屋）	不正アクセスを受けサーバーの一部にランサムウェアが感染[26]	—
		マット製造メーカー（兵庫県）	複数のサーバーでデータが不正に暗号化[27]	過去にVPN機器の脆弱性により流出した認証情報を悪用
		ホテル運営会社（東京都）	ホテルの無人チェックインシステム管理パソコンにランサムウェアが感染しデータが消去[28]	—
		自動車部品メーカー（東京都）	サーバーにランサムウェアとみられる不正なアクセスを確認[29]	VPN機器の脆弱性により流出した認証情報を悪用
		市教育委員会（千葉県）	ランサムウェア攻撃によりサーバーが使用不可。サーバーの被害状況からLockBit 3.0の攻撃によるものと判明[30]	攻撃者はSSL-VPN装置の管理者アカウントのID／パスワードを使用
		衣料品メーカー（愛知県）	ランサムウェアにより、サーバーのデータが暗号化[31]	—
		倉庫会社（神奈川県）	ランサムウェアにより、複数のサーバー上のファイルが暗号化もしくは破壊[32]	VPN機器から侵入
		派遣サービス（兵庫県）	ランサムウェアによりサーバーやパソコンの一部でデータが暗号化[33]	—

表 5-3　2021年4月以降に発生した主なランサムウェアのインシデント（国内中心）

時期		企業名	概要	原因・感染経路
2022年	9月	パチンコチェーン（東京都）	ランサムウェアによりサーバーが不正アクセスを受け、データの一部が暗号化され社内システムに障害が発生[34]	ー
		採用コンサルティング会社（東京都）	ランサムウェアによりサーバー、パソコンのデータが暗号化	VPN機器の脆弱性を悪用されて認証情報が窃取
		再生可能エネルギー（東京都）	ファイルサーバーがランサムウェア感染[35]	—
		清酒メーカー（兵庫県）	サーバーがランサムウェアに感染[36]	SSL-VPN機器の脆弱性
	10月	航空専門学校（大阪府）	サーバーにランサムウェアとみられる不正アクセス[37]	ー
		市民生活協同組合（奈良県）	ランサムウェアによりシステムで重大な障害発生し商品配達に影響。奈良県内の複数の店舗や支所のプリンターから大量の「犯行声明」が印刷。印刷内容は、システムを復元するソフトと引き換えに、ビットコインで金銭を支払うよう要求[38]	ー
		国立大学（愛知県）	情報システムのアカウントを管理するサーバーが、身代金要求型マルウェア（ランサムウェア）に感染し、データの一部が改変[39]	外部からネットワークアクセス制限が要求される個所の設定に不備があった
		民間病院（静岡県）	ランサムウェアの攻撃により、電子カルテシステムが使用不可[40]	ー
		公立病院（大阪府）	ランサムウェアと思われる攻撃により、電子カルテシステムに障害。院外調理による給食サービスを展開する業務委託先のデータセンター経由で侵入されランサムウェアに感染[41]	委託業者が利用していたリモートメンテナンス用VPN機器の脆弱性をつき侵入され、その後、水平展開が行われほかのコンピューターに被害が拡大
	11月	産業振興機構（宮城県）	サーバーがランサムウェアにより攻撃され、ネットワーク内部のファイルが暗号化[42]	ー
		民間病院（石川県）	不正アクセスにより、電子カルテの一部が閲覧不可[43]	ー
		市立図書館（東京都）	図書館の一部の業務用ファイルサーバーなどがコンピューターウイルスのランサムウェアに感染[44]	ネットワーク機器を介して業務用サーバーへ感染

5.2.　インシデント発生原因の特徴

上記のインシデント一覧からわかる特徴的な事柄として、ランサムウェアに感染した原因・感染経路が挙げられます。感染経路がネットワーク機器と明らかにされているのが、44件のインシデントの内18件で全体の約41%です。ランサムウェアの感染の原因としては、内部不正や人間の過失より、外部からの攻撃によるものが目につきます。IPAではランサムウェアに感染させる攻撃方法が、従来と異なる攻撃方法に変化しているとしています。これまでのランサムウェアの攻撃では、攻撃者はマルウェアを添付したメールのばらまきや悪意あるWebサイトの閲覧者への攻撃など、明確な標的を決めず個人や企業・組織への感染を試みていました。しかし、近年攻撃者は明確に企業・組織を標的とした攻撃で、事業継続のための金銭を支払わざるを得ない状況を作り身代金を得ようとしている、としています[45]。

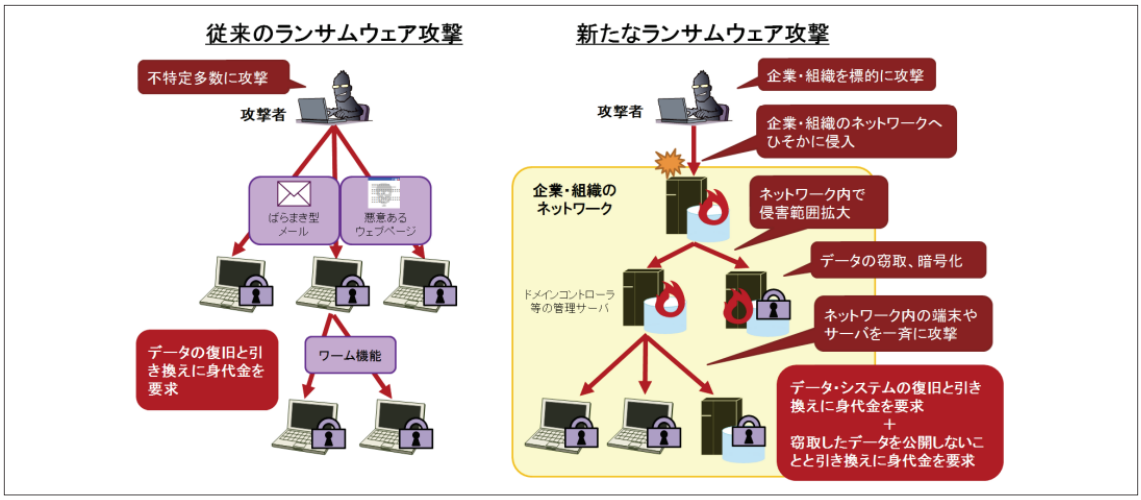

図 5-1　IPA「事業継続を脅かす新たなランサムウェア攻撃について」より

このことを裏付ける警察庁発表のデータがあります。警察庁が2022年4月に発表した「令和3年におけるサイバー空間をめぐる脅威の情勢等について」に記載されているランサムウェア被害に関するアンケート調査では、ランサムウェアの感染経路について76件の有効な回答があり、このうち、VPN機器からの侵入が41件で54%、リモートデスクトップからの侵入が15件で20%を占めており、不審メールやその添付ファイルからの侵入が5件(7%)でした。[46]

そして、「令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について」(2022年9月15日 警察庁)では、同様にランサムウェアの感染経路について質問したところ、47件の有効な回答があり、このうち、VPN機器からの侵入が32件で68%、リモートデスクトップからの侵入が7件で15%を占めており、不審メールやその添付ファイルからの侵入が4件(9%)[47]でした。

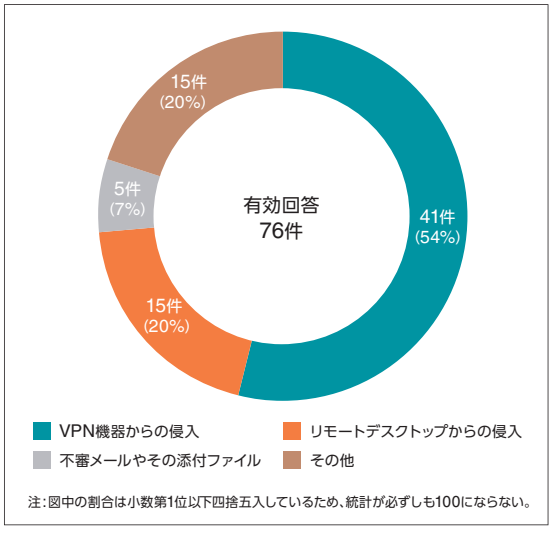

図 5-2「令和3年におけるサイバー空間をめぐる脅威の情勢等について」より

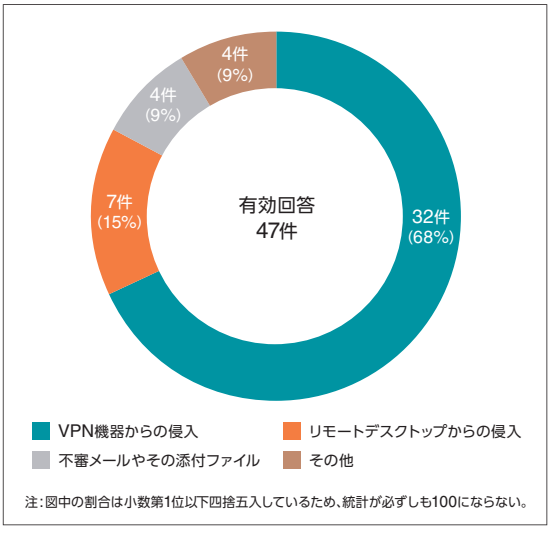

図 5-3「令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について」より

令和 3年（2021年）の 1年間と令和 4年（2022年）上半期の半年を比べても、不審メールやその添付ファイルからの侵入が7%（5件）から9%（4件）と2ポイントの増加に対して、VPN機器からの侵入は54%（41件）から68%（32件）と14ポイント増加し、2022年上半期ではテレワークにも利用される機器などの脆弱性や強度の弱い認証情報などを利用して侵入したと考えられるものが 83%と大半を占める結果になっています。このように近年 VPN機器などから組織内部に侵入されランサムウェアに感染するケースが増加し、先のインシデント一覧などにもあるように未対応な脆弱性を悪用されているケースが多く見受けられます。

5.3.　脆弱性対応が放置される理由

脆弱性の対応がされず未対応な状態が放置される原因はさまざま考えられますが、主に次のことが考えられます。

●脆弱性情報の収集不足
　脆弱性情報を収集又は入手できていない。

●不十分なリスク評価
　脆弱性が自組織におよぼす影響を正しく判断できていない。

●リソース不足
　脆弱性対応に必要なリソース（人員や時間など）が不足している。

●優先順位の問題
　ほかの課題が優先される。脆弱性対応の調整（システム停止など）に時間を要する。

●保守サポート期間切れ
　ソフトウェア、ハードウェアの保守サポートが切れている。

5.3.1.　サプライチェーンの影響

脆弱性情報が把握できない原因の 1つとして、日本の商習慣が深く関係していることが考えられます。SSL-VPN製品などアプライアンス製品の多くは海外製品で、その販売方法は日本法人や日本総代理店が直接ユーザーに販売・サポートするのではなく、いわゆるリセラー業者や SIer経由で販売・導入されます。[48] そのため、メーカーと使用するユーザーが直接契約関係にない場合があり、製品の脆弱性などの重要な情報を直接ユーザーに伝える連絡ルートがない場合があります。また、SIerはシステム導入のみの契約で、運用・保守の契約がされていない場合や、保守契約の内容がハードウェア障害の対応のみで、脆弱性対応などファームウェアの更新作業は契約内容に含まれていないことが多くあります。

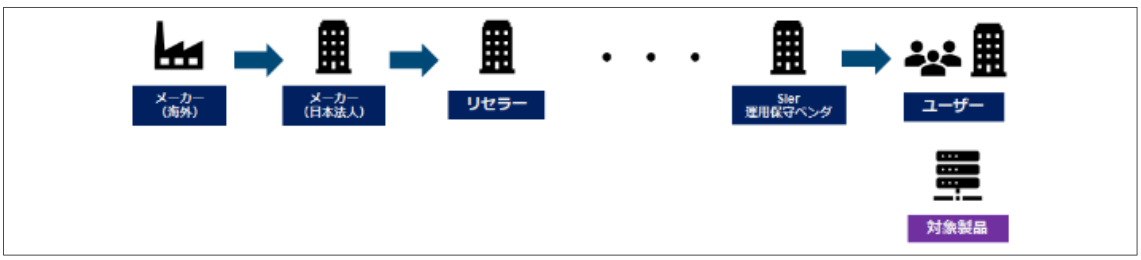

図 5-4　JPCERT/CC「なぜ、SSL-VPN製品の脆弱性は放置されるのか」より

5.3.2.　予算と体制の影響

日本の全企業の 99.7%が中小企業と言われています。[49] 大企業であれば豊富な人材と資金で情報セキュリティの体制を確立し、CSIRT（Computer Security Incident Response Team）や PSIRT（Product Security Incident Response Team）などの組織を設け、サイバーセキュリティ対策を実施することも不可能ではありません。しかし、日本の全企業の大半を占める中小企業、および病院や公共施設などそれに準ずるような組織・団体では IT投資への予算は多くはなく、情報セキュリティに関しては必要性すら感じていない企業も少なくありません。[50] このような状況で、情報セキュリティとりわけサイバーセキュリティの高いリテラシーを持った人材の不足に起因して陥りやすいのが、システム構築やその運用・保守などの外注業者へのいわゆる丸投げです。
依頼することが丸投げ状態となり発生しやすいのが、依頼元と依頼先の間での認識の齟齬（そご）です。依頼元の発注者としては、主たる特定の業務システムだけでなく、それらに付随した機器などのセキュリティ対策も含んで依頼しているつもりが、依頼先の発注を受ける業者は、特定の業務システム以外の付随した機器などのセキュリティ対策については明確に依頼されている認識がないような場合です。このような状況では、手離れを良くするために不具合なく安定稼働しているシステムに対して、変更を加えるような保守作業も避けることがあるかもしれません。

5.4.　運用と保守

システムを開発しサービスのリリース後は、滞りなく稼働させるために、それらの運用業務と保守業務が必要となります。この「運用」と「保守」は「運用保守」と一括りにされることが多いですが、本来「運用」と「保守」は別のものです。運用はシステムに対して変更を加えることはありませんが、保守はシステムに変更を加える場合があることが、この2つの大きな違いです。

運用とは、システムを計画通りに安定稼働させる業務で、電源 ON,OFFや I/Oオペレーションおよび稼働監視、性能監視で、障害発生時に対応手順書に従った対処を行い、サービスの提供を維持することをその範疇としているケースも多いです。
保守とは、システムで障害が発生した場合の復旧や、運用に支障が出ないように予防処置を行う業務で、故障したハードウェアの入れ替え、システム上のバグ改修、システムのアップデート、セキュリティパッチの適用、および古くなった機器のリプレースなどが含まれます。
従って、システムが安定に稼働していれば、運用業務のほとんどは定型作業となりますが、保守業務は定型作業とはなりません。

5.4.1.　ランニングコスト削減とアウトソース

先に述べた、「脆弱性が放置される理由」の原因の 1つである「リソース不足」は、運用・保守の業務に対する考え方が影響する場合があります。上述のように運用と保守には明確な違いがありますが、ランニングコストとして同じ業務として扱われてしまう場合があります。
システムが安定に稼働していれば運用の業務は定型作業となり、自動化によって効率化できコストダウンが可能な場合があります。ただし、保守の業務には必ず役務が発生し、それは定型作業にすることはできないため、自動化による効率化は困難で容易にコストダウンはできません。しかし、同じランニングコストとしてコスト削減の対象とされ、保守業務も併せて予算が削減されてしまうことがあります。このコスト削減によって、突発的に発生する脆弱性対応の保守業務で対応要員のリソース不足を招き、すぐに対応できないことが生じてしまいます。

対応要員のリソース不足の解決策として、運用・保守をアウトソースすることが考えられます。アウトソースするメリットは、先の「リソース不足（人員）の解消」や「運用の属人化の防止」そして「進化する ICT環境への対応」に適応できることです。

この運用・保守のアウトソースは非常に魅力的に見えますが、アウトソースする側と受ける側との間で、運用・保守業務内容や責任範囲（責任分界点）などの認識の食い違いが生じ、しばし障害発生時の対応に問題になることが少なくありません。従って、アウトソースで運用・保守を外部に委託する場合は、SLA（Service Level Agreement）を取り交わすなど、委託する内容と責任について明確にすることが重要です。

5.4.2.　運用・保守業務の範疇と責任範囲

さらに、既存のシステムと外部のサービスを連携する場合や運用・保守業務をアウトソースする場合などで、VPN機器などハードウェアを使った仕組みを使用する場合にも注意が必要です。ハードウェアを含んだサービスを利用する場合、そのハードウェアの運用や保守の業務はどのような内容で誰が行うのか、またその管理業務はサービスを使用する側か提供する側か、誰の責務で行う必要があるのか、という点です。このような場合にも両者の認識のずれ、お互いの思い込みで問題が発生しないように、あらかじめ内容と責任範囲（責任分界点）についてお互いに明確にしておくことが非常に重要となります。

5.5.　まとめ

●保守契約の締結と内容の把握

製品の最新バージョンや脆弱性情報、脆弱性対策を入手するのは、その製品の提供元であるメーカーからが基本です。従って、ソフトウェア、ハードウェアの製品の保守契約は必ず締結する必要があります。そして、その製品の保守契約の内容について理解することが重要で、ハードウェア故障時の交換方法はもとより、製品に関する脆弱性情報やその対策の提供方法は、メーカーから提供されるのか、販売店から提供されるのか、構築したSIerから提供されるのか、その提供方法はユーザー側から能動的に取得しなければいけないのかなど、契約段階で保守契約の内容を確認し、その内容を運用および保守の要員と情報共有しておくことが重要です。

●シフトレフトの考え方

ここ最近、セキュリティに関する工程を前倒しにして、システムのリリース・スケジュールに影響を与えないようにする考え方として「シフトレフト」という言葉が使われています。運用・保守についてもソフトウェア、ハードウェアのリプレースや脆性対応などをシステムのリリース段階やリリース後に考えるのではなく、企画段階から想定して予算化しておくことが望ましいと考えます。発生するかしないか定かではない、いつ発生するかわからない脆弱性の対応について、予算化することはその組織や業界の習慣によって困難なことも考えられます。しかし、新機能の追加や機能改善がなくてもそのシステムを使用している限り、OSやミドルウェア、アプリケーションの安定稼働を維持するためにメンテナンスは必要です。

また、オンプレミス・サーバーやアプライアンス製品などハードウェアは基本的に約4年で更新することが発生します。これら対応には当然コストが発生するので、必要に迫られた時でなく企画段階から運用・保守計画として押さえておくことが重要です。システムやサービスのオーナーとなる事業部門は、役割と責務をアウトソース先に丸投げすることなく、その事業のオーナーとして企画段階から脆弱性対応を含む運用・保守までを、そのシステムやサービスのライフサイクルに含めて取り組む必要があります。

●そして今後

現在、SaaSサービスなど、さまざまな形態のクラウド・サービスがあり、それは今後も増えていくことが予想され、それらのサービスの中にはさまざまな種類のIoT機器を活用することが考えられます。一言でIoT機器といっても、その用途や目的はさまざまですが通常はその機能を実現するための、限られた処理能力とI/O機能しか保有していないことが多いです。特に非機能要件として扱われるセキュリティなどは、その限られたリソースのため十分な機能を有していない場合があり

ます（コスト重視でメンテナンス機能など持たないような場合も）。また、IoT機器に対する利用者のセキュリティ意識が不十分で、デフォルトの認証情報を使用したり、不用意にインターネットからアクセスできる環境に設置したり、時には開発用のデバッグポートが放置されたりする可能性もあります。そんなIoT機器に脆弱性が見つかった場合その対処はどうなるのでしょうか?IoT機器に対する責任の主体はIoT機器の提供者なのか利用者なのか?はたまたサービスの提供者なのか?サービス利用時の契約やサービス約款などにゆだねることになりますが、脆弱性の対応に悩まされることが終わることは当分なさそうです。

---

1 令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

2 情報セキュリティ10大脅威 2023
https://www.ipa.go.jp/security/vuln/10threats2023.html

3 JNSA 2022セキュリティ十大ニュース
https://www.jnsa.org/active/news10/

4 医用画像参照システムサーバへの不正アクセスに対する対応状況の経過報告について
https://www.higashiosaka-mc.jp/news/notice/20210924_notice.html

4 事前に警鐘が鳴らされていたのに身代金脅迫ウイルスに襲われた東大阪の病院
https://weekly-economist.mainichi.jp/articles/20210803/se1/00m/020/025000c

5 当社サーバーへの不正アクセスについて
https://www.fujifilm.com/jp/ja/news/list/6642

6 2022年3月期第3四半期報告書の提出期限延長に関する承認申請書提出のお知らせ
https://www.nippn.co.jp/topics/detail/__icsFiles/afieldfile/2022/02/14/20220214-1.pdf?_fsi=wz35yq4Z

7 ランサムウェア攻撃に関するご報告
https://www.oriconhd.jp/files/information/news20211008_01.pdf

7 ランサムウェア攻撃に関するご報告
https://www.cser.co.jp/topics/topics_2021-10-8.html

8 システム障害に関するお詫びとお知らせ
http://www.yuurinkouseikai.or.jp/info/20211104.asp

9 コンピュータウイルス感染事案有識者会議調査報告書について
https://www.handa-hospital.jp/topics/2022/0616/index.html

10 不正アクセス（疑い）によるシステム障害発生のお知らせ
http://www.kreh.or.jp/2022/01/19/3837/

10 あなたの病院の「感染」対策は大丈夫?〜問われる医療機関のセキュリティー〜
https://www3.nhk.or.jp/news/special/sci_cul/2022/05/special/2022-05-27-cyber/

10 [サイバーテロ　病院の危機]<5>対策の不備　責任重く…「経営層が賠償」可能性
https://www.yomiuri.co.jp/national/20220222-OYT1T50041/

11 小島プレス工業株式会社　システム停止事案調査報告書（第1報）
https://www.kojima-tns.co.jp/wp-content/uploads/2022/03/20220331_%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0%E9%9A%9C%E5%AE%B3%E8%AA%BF%E6%9F%BB%E5%A0%B1%E5%91%8A%E6%9B%B8%EF%BC%88%E7%AC%AC1%E5%A0%B1%EF%BC%89.pdf

12 不正アクセスおよび情報流出の可能性に関する調査結果のお知らせ
https://www.gmb.jp/upload/save_file/05201625_210066287426032afd.pdf

13 不正アクセスに伴うシステム停止について
https://www.sas-globalwafers.co.jp/jpn/whatsnew/%E4%B8%8D%E6%AD%A3%E3%82%A2%E3%82%AF%E3%82%BB%E3%82%B9%E3%81%AB%E4%BC%B4%E3%81%86%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0%E5%81%9C%E6%AD%A2%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6_20220302_3.pdf

13 グローバルウェーハズ・ジャパン、不正アクセスによりウェハ生産業務を停止
https://news.mynavi.jp/techplus/article/20220307-2287361/

14 不正アクセス事案に関する調査結果のお知らせ
http://www.higashiyadelica.jp/news/499.html

15 当社ネットワークへの不正アクセスに関する調査結果のお知らせ
https://corp.toei-anim.co.jp/ja/press/COPY-COPY-COPY-press3317734943536499846.html

16 不正アクセス発生による個人情報流出の可能性のお知らせとお詫び
https://www.morinaga.co.jp/public/newsrelease/web/fix/file6239a22a42a9c.pdf

16 森永製菓「ランサムウエア」で164万人以上の顧客情報流出か
https://www3.nhk.or.jp/news/html/20220322/k10013545891000.html

17 システム障害発生に関する調査結果についてのお知らせ
https://www.nippon-antenna.co.jp/ja/news/news/news-6120255908398465635.html

18 勤怠管理システムサーバに対する攻撃について
https://www.viax.co.jp/pdf/20220601.pdf

19 当社サーバへの不正アクセスに関するお知らせ（第二報）　お客様等の個人情報流出可能性のお知らせとお詫び
https://www.gekkeikan.co.jp/company/news/detail/326/

20 当社サーバーに対する不正アクセスに関するご報告（第2報）
http://keisei-const.jp/wp-content/uploads/2022/05/39ac64ecf8c86edd082dade7e9fdbfe6.pdf

21 大阪 藤井寺の病院に身代金要求型サイバー攻撃か カルテ使えず
https://www3.nhk.or.jp/news/html/20220428/k10013604371000.html

22 ランサムウェアによる不正アクセスに関するご報告(最終)
https://www.kawamura.co.jp/wp/wp-content/uploads/2022/07/%E3%83%A9%E3%83%B3%E3%82%B5%E3%83%A0%E3%82%A6%E3%82%A7%E3%82%A2%E3%81%AB%E3%82%88%E3%82%8B%E4%B8%8D%E6%AD%A3%E3%82%A2%E3%82%AF%E3%82%BB%E3%82%B9%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E3%81%94%E5%A0%B1%E5%91%8A%EF%BC%88%E6%9C%80%E7%B5%82%EF%BC%89.pdf

23 当社に関する報道について
https://www.shimamura.gr.jp/assets-c/uploads/426a71e424a28540adb3a1bf487f7b170d51a9c8.pdf

23 衣料品「しまむら」ランサムウエアによるサイバー攻撃受けたか
https://www3.nhk.or.jp/news/html/20220510/k10013620031000.html

24 令和4年6月20日 サイバー攻撃による被害について（第1報）
https://kyujinkai-mc.or.jp/info/20220620/

25 ランサム攻撃でサーバ内のデータが暗号化 - 帰国子女向け教育サービス
https://www.security-next.com/137398

26 本所システムサーバーへのウィルス感染と不正アクセスについて
https://www.nagoya-cci.or.jp/security-announce20220705/

27 2022年7月8日に発生した不正アクセスに関する調査結果及び確報について
https://www.kleen-tex.jp/20220906_1/

28 ウイルス感染による個人情報漏えいの可能性に関するお知らせ（続報）
https://www.hishotelgroup.com/news/1618/

29 当社サーバーへの不正アクセスに関するお知らせ（第四報）
https://www.riken.co.jp/upload/2AMMA3S-newsja_file.pdf

30 市内小中学校の校務ネットワークに対する不正アクセスについて（第2報）
https://www.city.minamiboso.chiba.jp/0000017428.html

31 不正アクセスによる情報漏えいの可能性に関するお知らせとお詫び
https://www.crossplus.co.jp/ir/2022/09/14/2915/

32 システム障害からの復旧と再発防止策に関するお知らせ（第5報）
https://www.sanwasoko.co.jp/news/detail.php?id=32

33 サイバー攻撃に関する調査結果の報告
https://www.wdbhd.co.jp/assets/pdf/ir/press/press221111_2.pdf

34 当社サーバーへの不正アクセスについて（第3報）
https://www.dyjh.co.jp/news/pdf/221101_dyjh.pdf

35 当社ファイルサーバーのランサムウェア感染についてお知らせとお詫び（第三報）※12/20更新
https://minden.co.jp/wp-content/uploads/2022/11/20221121_Notice-and-Apology-from-UPDATER_third-report_1220upd.docx.pdf

36 当社サーバーへの不正アクセスについてのご報告とお詫び
https://www.nihonsakari.co.jp/news/p/341

37 本学園サーバーへの不正アクセスについて
https://kouku.ac.jp/pdf/access.pdf

38 重大なシステムトラブルに伴う個人情報についてのお知らせ
https://www.naracoop.or.jp/naranews/cat1/4628.html?fbclid=IwAR2xMEfYcngzq9pRZa7fok9BBVzGElQ8iiqjlYmFo8BrNveuWGfuotWf7Rk

39 東海国立大学機構への不正アクセスによる個人情報流出について
https://www.thers.ac.jp/news/2022/11/20221118-jimu.html

40 電子カルテの不具合について
http://shinyoukai.or.jp/tazawa-clinic/news/20221101.html

40 沼津市内の医療機関にサイバー攻撃　電子カルテシステムに障害
https://www3.nhk.or.jp/lnews/shizuoka/20221108/3030018212.html

41 「電子カルテシステム」の障害発生について
https://www.gh.opho.jp/pdf/info20221031.pdf

41 サイバー攻撃被害によるシステム障害のお知らせ（第2報）
https://www.seichokai.or.jp/system/upload/bellkitchen/news/1672125435_020263400.pdf

42 不正アクセス被害について
https://www.joho-miyagi.or.jp/20221227-2

43 コンピューターの不正アクセスによる障害発生について
https://www.knh.or.jp/news/2022/12/08/%e3%82%b3%e3%83%b3%e3%83%94%e3%83%a5%e3%83%bc%e3%82%bf%e3%83%bc%e3%81%ae%e4%b8%8d%e6%ad%a3%e3%82%a2%e3%82%af%e3%82%bb%e3%82%b9%e3%81%ab%e3%82%88%e3%82%8b%e9%9a%9c%e5%ae%b3%e7%99%ba%e7%94%9f%e3%81%ab/

44 市立図書館におけるコンピュータウィルス感染について（第一報）
https://www.lib.city.hino.lg.jp/news/important/20221219-post_234.html

44 市立図書館におけるコンピュータウィルス感染について（最終報）
https://www.lib.city.hino.lg.jp/news/important/20221228-post_235.html

45 事業継続を脅かす新たなランサムウェア攻撃について
https://www.ipa.go.jp/files/000084974.pdf

46 令和3年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

47 令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

48 なぜ、SSL-VPN製品の脆弱性は放置されるのか
https://blogs.jpcert.or.jp/ja/2022/07/ssl-vpn.html

49 日本を支える中小企業
https://www.smrj.go.jp/recruit/environment.html

50 「2021年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について
https://www.ipa.go.jp/security/fy2021/reports/sme/index.html

6 Web証明書／PKIの最新動向と展望

第 6 章　Web証明書／PKIの最新動向と展望

6.1. はじめに

インターネットや Webサイトは私たちの日常に浸透し、今や生活や仕事に不可欠な存在となりました。同時に偽のサイトや悪質な意図を持つ有害な Webサイトも長年横行し続けており、その勢いが弱まる気配は全く感じられません。インターネットは自由でオープンな通信インフラで、参加するあらゆる端末と個別の通信を可能とする基本構造は昔から変わっていません。通信相手の選択は端末を使用する個人に委ねられており、利用者は Webサイトの信頼性を自ら判断しなければなりません。悪質なサイト所有者はそのようなインターネットの性質を逆手に取り、あらゆる手を使って被害者を自サイトへ誘い込もうとしています。

フィッシングはメールやショートメッセージ（SMS）などの手段で被害者を偽サイトや悪質サイトへ誘導し、認証情報やカード番号を窃取したり、端末にマルウェアをダウンロードするように仕向けたりする攻撃です。フィッシング対策協議会のレポートによれば、国内のフィッシングサイト URL件数は増え続けており、2021年下半期は過去最高で 4万件を上回りました。[1]攻撃者は金融機関やショッピングサイトなど大手の事業者、公共機関などになりすまし巧妙なメールやメッセージを送り付け、勘違いを誘い悪質なサイトへのリンクをクリックさせます。注意深く確認すればフィッシングであることを見破れる可能性もありますが、一見では見分けにくいドメインで攻撃をしてくることもあり容易ではありません。

インターネット上のドメインやアドレスの信頼性をどのように判断するのかは古くからある問題であり、今も継続しています。これに対し長年採用されてきたアプローチがデジタル証明書によるドメインと所有者の検証です。現在、Webブラウザー（以下ブラウザー）で一般的なサイトにアクセスすると、アドレスバーに鍵マークが表示されます。これはそのサイトとの通信が暗号化されていることを示していますが、同時にドメインやその所有者が信頼性の高い証明機関に認証されていることも意味しています。これを可能とする仕組みがデジタル証明書とそれを支えるPKI（Public Key Infrastructure｜公開鍵基盤）です。本章では伝統的なドメイン検証手法でありさまざまな用途に活用されている PKIの仕組みと動向を紹介し、今後の展望を考察します。

6.2. PKIの仕組み

PKIとは公開鍵暗号を使った認証基盤を指します。公開鍵暗号は素数や楕円曲線など数学理論に基づいた巨大な数値を含む秘密鍵と公開鍵のペアを使って、不特定多数の相手との秘密の共有や、デジタル署名（本人によるデータの真正性に対する証し）の作成・検証を実現する暗号技術です。秘密鍵は個人や組織など特定の主体のみが保有し、一切公開しません。秘密鍵では公開鍵で作成された暗号の復号や、あるデータに対するデジタル署名を作成することができます。それに対し公開鍵はあらゆる主体に公開することができます。公開鍵は情報を暗号化したり、データに付加されたデジタル署名を検証したりできます。[i]

例えば秘密鍵の所有者があるデータに対してデジタル署名を作成し、データと一緒に第三者に渡したとします。データを受け取った人は秘密鍵所有者のペアとなる公開鍵を入手し、それを使ってデータとデジタル署名を検証します。もし、データが何者かに改ざんされている場合、検証は失敗し不正なデータであると判断することができます。（図 6-1）

i　TLS等暗号化通信における公開鍵暗号技術の主要な用途はデジタル署名と鍵交換です。

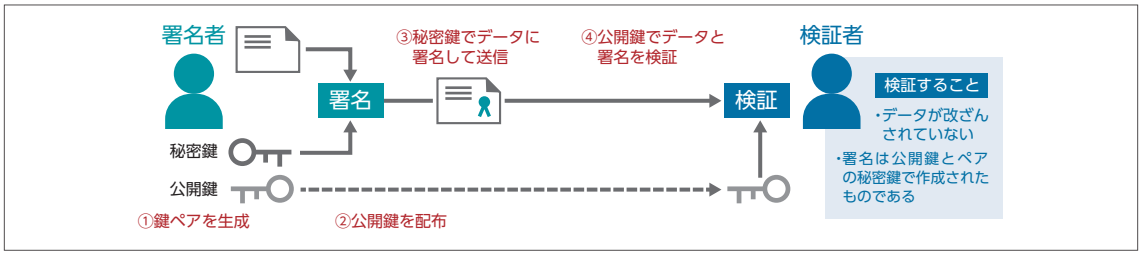

図 6-1　デジタル署名と公開鍵による検証

暗号化通信可能な Webサーバーは必ず公開鍵暗号の鍵ペアを所有しており、アクセスしてきたブラウザーに対して公開鍵を渡します。ブラウザーは Webサーバーが送ってきたデータとデジタル署名を Webサーバーの公開鍵を使って検証することで通信の信頼性を担保できます。ただし、これだけでは Webサーバーを信頼できるとは言えません。アクセスするサーバーのドメインが暗号化通信を開始しても問題のない信頼性のあるサイトであることを判断しなければなりません。そこで、公開鍵は「公開鍵証明書」という形式のファイルにして渡します。公開鍵証明書は公開鍵に加えて、そのサイトのドメインや所有者、証明書の発行元に関する情報が記載されたファイルで、ITU-Tの X.509勧告[2]と IETF[ii]により標準化[3]されており、サーバー証明書とも呼ばれています。Webサイトのサーバー証明書は図 6-2のようにブラウザーの鍵マークから表示させて中身を確認することができます。

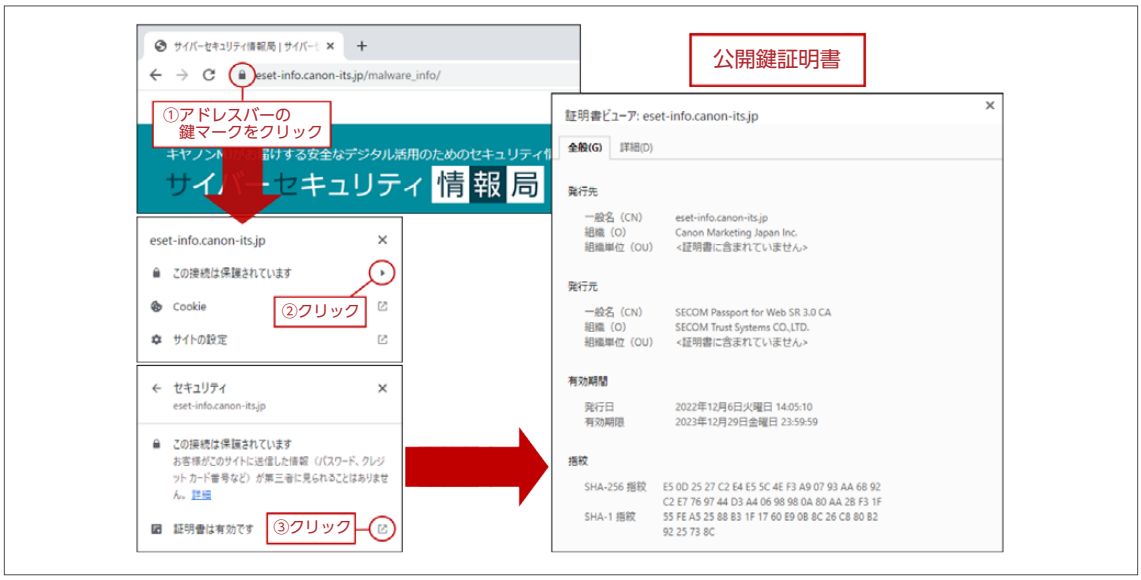

図 6-2　ブラウザーでサーバー証明書を表示する方法(Chrome ver109)

ii　Internet Engineering Task Force(インターネット技術の標準化を推進する任意団体)

証明書の中身を見ると、発行元は発行先（ドメイン所有者）と異なる組織であることがわかります。これはCA（Certification Authority｜認証局）という組織で、Webサイト管理者とドメインの関係を確認しサーバー証明書を発行している信頼性の高い第三者機関です。CAも公開鍵暗号のペアを所有しており、発行するサーバー証明書に対し自組織の秘密鍵で署名をしています。ブラウザーはCAの公開鍵を入手し、この署名を検証すれば、CAがサーバー証明書の公開鍵、ドメイン、所有者を認証していることが確認できます。PKIはこのように第三者の認証機関が公開鍵証明書を発行することによって信頼を提供します。

サーバー証明書は中間CAと呼ばれる認証局が発行しますが、世の中に無数に存在する中間CAを無条件に信頼することは不可能です。中間CAもWebサーバーと同様に信頼性の証しとなる証明書（中間CA証明書）が必要です。そして、中間CA証明書を発行するのはさらに信頼性の高い認証機関になります。このように PKIは階層構造で連鎖的に信頼を提供します。そして階層構造の最上位に位置するCAがルートCAです。ルートCAも証明書を持っていますが、自組織で署名して発行しているため自己証明の証明書です。ルートCAはWebTrust[iii]やETSI[iv]などの監査機関の厳格な基準によって認められます。

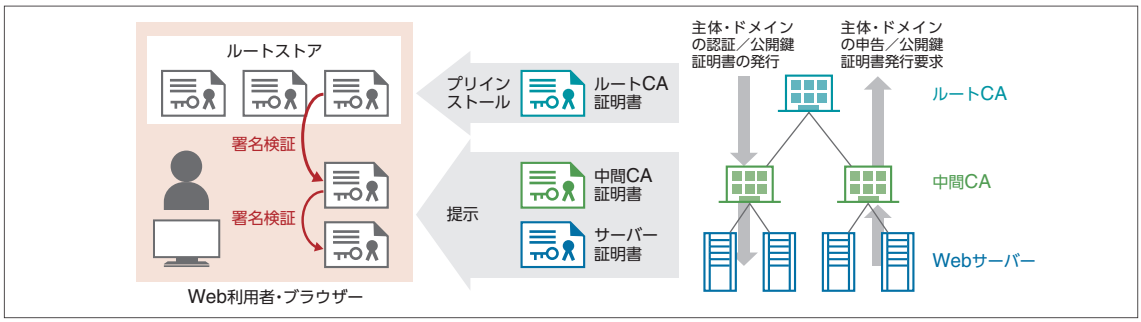

図 6-3　PKIの階層構造

OSやブラウザーのベンダーは自製品のルートプログラムあるいはルートストアポリシーと呼ばれる基準を公開しており、基準を満たすルートCAが発行するルートCA証明書はOSやブラウザーのルートストアと呼ばれる領域にプリインストールされています。例として図 6-4にWindows 10のルートストアの確認方法を示しました。OS、ブラウザーベンダーはルートプログラムと業界任意団体のガイドラインを通して認証局の信頼性を担保しています。これらの製品を信頼して使用することは、ルートストアを通してルートCA証明書を間接的に信頼していることになります。OS、ブラウザーはPKIの信頼性について重要な鍵を握っていると言っても良いでしょう。

図 6-4　Windows 10のルートストアの確認方法

iii　米国公認会計士協会とカナダ勅許会計士協会による監査プログラム

iv　欧州電気通信標準化機構

6.3.　信頼性の危機と向上策の歴史

PKIの運用が本格的に始まってから 20年以上の年月が経ちましたが、その歩みは常に順風満帆だったわけではありません。特に 2011年には PKIの危機と呼べるような事件が立て続けに発生しました。その中でも有名な事件が、オランダのルートCAであるDigiNotarへComodoHackerと名乗る人物が不正にアクセスし、不正な証明書を大量に発行した事件です。[4] 証明書はGoogle社やMicrosoft社、Facebook社などの大手サイトのドメインを騙ったもので正確な数は不明ですが少なくとも 500枚以上は発行されたようです。[5] 不正証明書の失効には 2ヶ月弱を要し、その間に不正証明書を利用した Gmail ユーザーへの中間者攻撃も発生しました。この事件で DigiNotarは廃業しましたが、厳格な基準で運用されていたはずのルートCAが完全に侵害されたことは、それまでの安全神話の崩壊を意味しており、もはや手放しで認証局を信頼することはできないという認識が共有されました。
事件以後は技術と運用の両面から信頼性向上のための取り組みが始まります。以下に主だった取り組みを挙げます。

●Baseline Requirementsの策定

CAやブラウザーベンダーの組織する任意団体であるCA/Browser Forum[6](以下CABF)は、2011年に証明書の発行に関する基本的要件(Baseline Requirements)[7]に合意します。過去の監査基準の曖昧性を解消し、すべての認証局を対象に監査基準を定義しました。監査機関のWebTrustもBaseline Requirementsに沿って基準を改定しました。

●Certificate Transparency(CT｜証明書の透明性)

CTはCAが発行した証明書の情報を第三者のCTログサーバーに記録し監視できるようにする取り組みで、Google社が2011年に提案、2013年に標準化され現在はVersion 2.0が公開されています。[8,9] CTは不正な証明書の発行を防ぐことはできませんが、サーバー管理者が運用中に常に監視できるようにすることで不正を早期に発見するのが目的です。Google Chromeは証明書のCT準拠の検証を行っておりWebサーバー証明書は事実上CT準拠が必須化されています。[10]

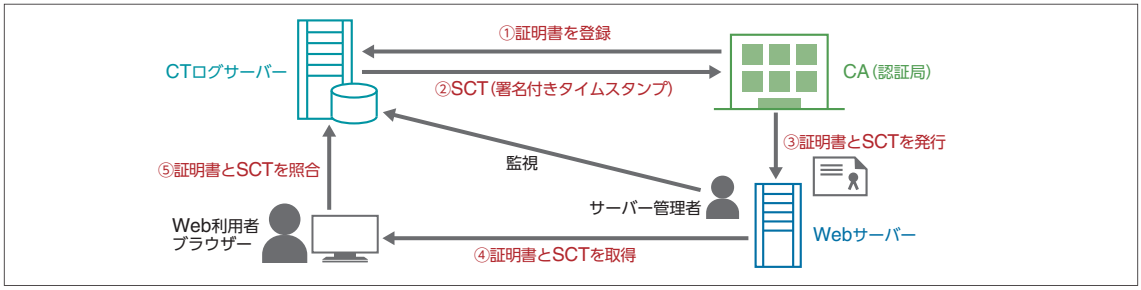

図 6-5　Certificate Transparency の仕組み

●Certificate Authority Authorization(CAA)

CAAはドメインの所有者がDNSサーバーのCAAレコードに、そのドメインの証明書を発行できるCAの名称を設定できる仕組みで、2013年に標準化され[11]2019年に改訂されました[12]。CABFはCAに対しCAA検証を義務付けています。CAは証明書発行が申請された際にドメインのCAAレコードを検証し、設定されていた場合は従わなければなりません。これを参照することでCAは証明書の誤発行を防ぐことができます。CAAはあくまでCAが利用するレコードであり、サイト閲覧者(ブラウザー)は利用してはいけません。その場合は次のDANEを利用します。

●DNS-based Authentication of Named Entities（DANE）

DANEはCAA同様にドメインに対して証明書を発行できる中間CA証明書の情報や階層の最上位のルートCA証明書の情報をDNSサーバーのTLSAレコードに設定する機能で、2011年に要求仕様が公開され2012年に標準化されました。[13] クライアントはサーバーから受け取った証明書がDNSサーバーのTLSAレコードに記載されていることを確認することで、不正な証明書を排除できます。ただ、現時点でDANEは普及が進んでいません。[14] さまざまな理由が考えられますがDANEを使うにはDNSSEC[v]が必須で設定の要求が高いことも普及が進まない一因かもしれません。

これらの取り組みは10年以上を経て明暗は分かれましたが、不正証明書発行の減少に一定の役割を果たしたと言えそうです。ただし、これらはPKIの信頼性にまつわる課題の一部を解決するものであり、まだ多くの課題が残されています。解決のための取り組みは現在も続けられています。

6.4.　近年のPKIの動向

PKIを取り巻く環境は変化し続けており、それに呼応してPKI自身も形を変えています。2022年もさまざまな動きがありましたので目立ったトピックを紹介します。

●コード署名鍵の流出事件

PKIや証明書はWebだけにとどまらずソフトウェアに対する「コード署名」の検証にも利用されています。

Androidは公式アプリストアで配布するアプリをインストールする際に、開発者の署名を証明書で検証できるようになっています。12月の報道によれば、大手スマートフォンメーカーの署名鍵が流出し長期間マルウェアの署名に使用されていたことが判明し、PKI関係者に衝撃を与えました。[15] ほかにもMicrosoft社の認定を受けたドライバー用署名がランサムウェアに使用された事件や[16]、半導体メーカーのインシデントでコード署名鍵が流出し、証明書が失効された事件[17]などコード署名の侵害が多発しています。

コード署名の証明書についてはCABFによる基本的要求事項が整備されています。用途に限らず秘密鍵は厳格な管理が要求されますが、現状の運用ルールだけでベンダーの発行する証明書を信頼できるのかも課題となっています。

●CNの禁止とSANへの統一

証明書は組織や個人の認証、役割の証明などさまざまな用途で発行されますが、最も多いのがWebのドメイン認証です。証明書のX.509勧告ではサイトのFQDNは証明書主体者のCommon Name（CN）と呼ばれる属性に記述するよう定められていますが、1つしか設定できないためSubject Alternative Name（SAN）と呼ばれる拡張領域にも記載可能となっています。近年はクラウド普及によるマルチドメイン化の流れも後押しし、SANを使用するケースが一般化していました。

また、CNは記載の自由度が高く曖昧性があり、検証処理の実装を困難にするなど、安全上の懸念も指摘されていたので、SANの利用が推奨されていました。しばらくはCNとSANを併用する形が続いていましたが、2022年にはWebの暗号化通信のCN検証が禁止され、SANへの対応が必須となりました。[18,19] 今後発行するWebの証明書はSANの記述がなければ、ブラウザーで検証エラーとなる可能性があるので注意が必要です。

v　DNS問い合わせ時にキャッシュサーバーがDNS応答の出自と完全性を検証する技術

●HPKP廃止

DigiNotar事件後の不正証明書発行対策の1つとして提案・実装されたのがHTTP Public Key Pinning(HPKP)です。これはWebサイトから提示された証明書が、正しい証明書かどうかをブラウザー側で検証できるようにする機能です。[20] 具体的には正常な通信で得た証明書の公開鍵のハッシュ値をブラウザーに保存(ピン止め)し、以後の通信でハッシュ値を比較して検証します。この手法は不正防止の強力な助けとなりますが、証明書の流動的な環境では運用が難しく、失敗すれば長期間サイトにアクセスできなくなる障害が発生するリスクや敵対的なピン止めのリスクも指摘されていました。[21] 結果的に普及しなかったため2022年には主要ブラウザーから削除されました。[22]

証明書は発行した後も適切に管理しなければなりません。日々大量に発行され増加し続ける証明書の安全なライフサイクル管理は長年の課題です。近年では証明書管理に関する指針やトレンドにも変化が見られます。

●証明書の有効期間の短縮

運転免許証のような物理的証明書と同様にデジタル証明書にも必ず有効期間が必要です。有効期間が長ければ更新の手間が省けて便利ですが、長すぎれば鍵の漏えいや暗号の危殆化[vi]などのリスクが増えていきます。初期のサーバー証明書は2、3年程度が一般的で、CABFが2015年に定めた上限は3年3ヶ月でした。これが2018年に2年3ヶ月に変更され[23]、2020年には主要なブラウザーで399日以上の証明書は信頼されないことが決定されています。一部で既に90日に短縮する案も出ており検討が続いています。有効期間短縮トレンドの背景にはセキュリティ向上の意図もありますが、無料証明書を発行するCAであるLet's Encryptの台頭などにより証明書の自動更新が普及していることも関係しています。

●ブラウザー独自のルートストア

従来のInternet ExplorerやGoogle Chromeなどのブラウザーはルート CA証明書についてOSが管理するルートストアに従う方式を採用していました。[vii]ルートストアを独自に管理することはコストもかかるためこれは合理的な選択ですが、プラットフォームへの依存はクロスプラットフォームにおけるブラウザー挙動の一貫性を損なう恐れがあります。Google社はWeb PKIのエコシステムへの参画と改善を謳っており、その一環としてプラットフォームから独立する方針を打ち出していました。そして2022年に独自のルートストアの配布を開始しています。[24]ちょうどInternet Explorerのサポート終了も重なったことで、このトレンドは決定的となっています。

●証明書失効検証の課題とブラウザー独自CRLの拡大

証明書は特別な理由により有効期間内に失効するケースがあります。その場合、CAは失効した証明書の状態をCRL(Certificate Revocation List｜証明書失効リスト)と呼ばれるファイルに記載して配布し、検証者(ブラウザー)に知らせなければなりません。

ただ、CRLは証明書の発行数増加や大量失効による肥大化の問題があるため、その後、検証者がオンデマンドで個別の証明書失効状態を確認できるプロトコルOCSP(Online Certificate Status Protocol)も標準化されました。OCSPはCRLの運用負荷の問題を解消できますが、妨害のリスクやプライバシーの問題も指摘されています。

2022年には大きな動きがありました。膨大な証明書を発行し規模を拡大しているCAであるLet's Encryptは、従来OCSPのみ利用可能でしたが、9月にCRLをブラウザーに対してプッシュするインフラを構築したことを明らかにしました。このインフラは2億枚の証明書の同時失効も扱えるよう設計されているとのことです。[25]

vi　計算機の計算能力の向上や脆弱性の発見により暗号の強度が弱くなっていくこと

vii　MozillaのFirefoxは当初から独自のルートストアを管理・利用していました

実は現在のWeb証明書の失効検証ではブラウザーベンダーが独自に開発した「要約されたCRL」の機能が普及しています。これは大量のCRLを個々のブラウザーが独自に取得するのではなく、ブラウザーベンダーがCAから一元的に収集しそれを独自のフォーマットに圧縮して高頻度でブラウザーにプッシュする機能です。[26,27]この機能は一部の登録済みのCAが対象でしたが、小規模サイトを含む膨大な証明書を抱えるLet's Encryptの方針転換はPKIエコシステムに大きな影響を及ぼすかもしれません。

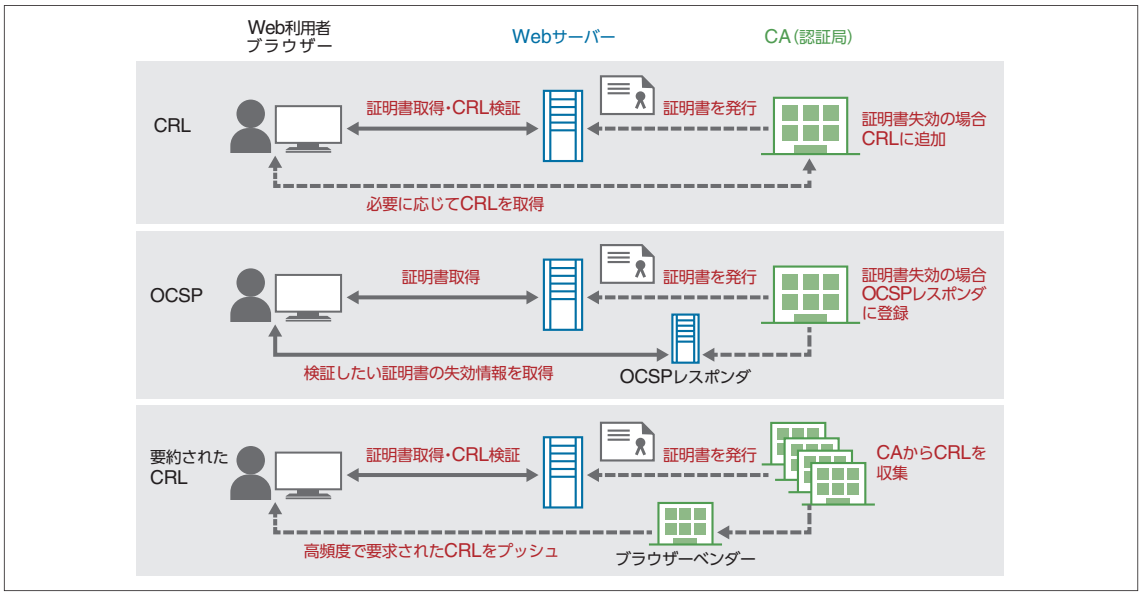

図 6-6　証明書の失効検証の違い

6.5.　認証レベルの扱いの変化

証明書には発行時の確認内容によって異なる認証レベルがあります。その違いは証明書の信頼性にもかかわるためWebサイト管理者にとっては気になるところです。表 6-1に認証レベルの種類と違いを示しました。

表 6-1　証明書の認証レベル

認証レベル	呼称	確認内容
ドメイン認証	Domain Validation (DV証明書)	対象ドメインと所有者の関係
実在認証	Organization Validation (OV証明書)	企業等実在組織と対象ドメインの関係
拡張された実在認証	Extended Validation (EV証明書)	登記情報などに基づく厳格な組織の実在と対象ドメインの関係

PKIの初期は厳密な認証レベルは存在しませんでしたが、CABFが発足して以降はCAによる審査基準のばらつきを是正するために認証レベルと統一的な審査基準が定められました。[28,29]特に EV証明書は厳しい審査基準があるので、フィッシングサイトなど悪意のある管理者は取得が難しくなります。

EV証明書が定義されて以降、主要ブラウザーではEV証明書を提示するサイトをアドレスバーでわかるように組織名を

表示し、背景を緑色にしていました。ユーザーはブラウザーのアドレスバーを確認すれば、サイトが EV証明書を保有していることを確認できました。しかし、近年ブラウザーはEV証明書に対する特別扱いを止めつつあります。Google Chromeは2018年にEV証明書保有サイトのアドレスバーを緑背景にするのを止め、その後、組織名表示も止めて、鍵マークをクリックして確認する仕様に変更しました。[30] また、他のブラウザーもこの動きに追従しています。[31]

変更理由の 1つとして Webの主役がモバイルへ移行していることが挙げられます。モバイルブラウザーはアドレスバーの表示スペースが小さいため、そもそも組織名表示は困難です。デスクトップとモバイルで表示に差異があるとユーザーが混乱するため、モバイル表示に統一する意図があるとも言われています。[32] もう1つの消極的理由として、実態としてユーザー側も EV証明書かどうかを確認する習慣がないため、UI表示の差別化によるフィッシング防止効果は限定的という主張もありますが、真偽ははっきりしません。

図 6-7はアクセス数の多い主要サイトにおける EV証明書保有率の推移を表していますが、2016年頃まで増加傾向だったEV証明書の保有率はその後減少に転じています。[33] 一方で Let's Encryptに代表されるように自動的に発行・更新可能な無料の CAの登場で、DV証明書の数は爆発的に増加しています。現在は膨大な DV証明書をいかに安全に運用するかに焦点が移っており、証明書発行の自動化と有効期間の短縮が進められています。

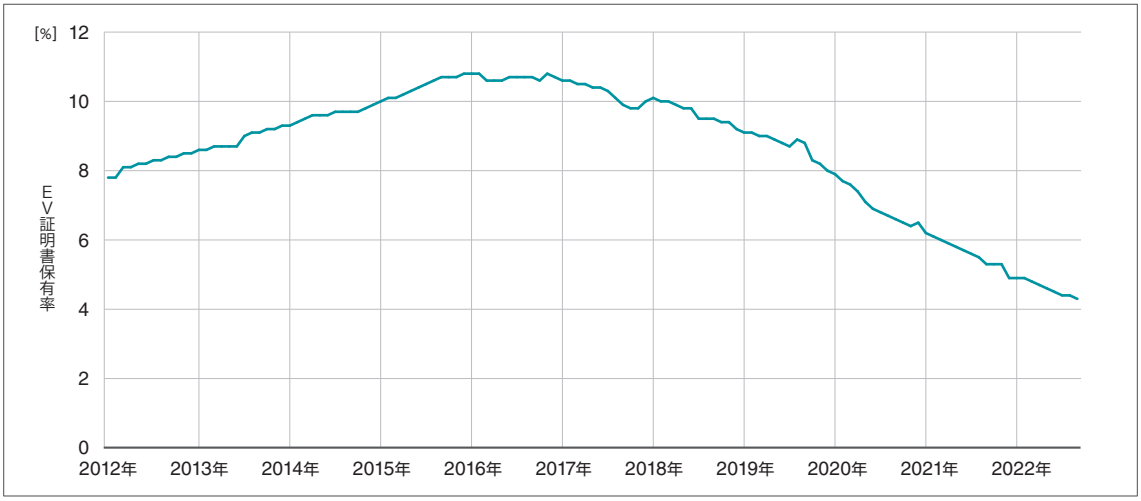

図 6-7　EV証明書保有率の推移状況（SSL Pulse[viii]データより筆者作成）

現状ではEV証明書だけで信頼性を判断するには限界があることも事実です。サイトの信頼性を判断する別の手段はないのでしょうか。例えばEUはeIDAS規制[ix]の一環で身元確認の取れた信頼できる個人、法人を認証する証明書であるQWACs (Qualified Web Authentication Certificates)を提案しています。[34] 政府機関による証明ということで信頼性は高いですが、EV証明書に考え方が近く、特定の政府機関が審査し発行する証明書をインターネットで無条件に信頼できるのかについてはブラウザーベンダーも含めた議論が続いています。悪質サイトや信頼できるサイトを拒否リスト、許可リストにして、アクセス制限する機能は、高い防御効果があるので現状における現実的な選択肢でしょう。ただし、現在のフィッシングは短時間・高頻度化が顕著であるため、リスト管理による対策も完璧ではありません。運用性、透明性、実効性の高い Webサイトの信頼性判断方法が求められていますが、決定的な解決策はないため今後も新しい提案や議論を必要としています。

viii　Qualys社が公表するAlexaトップ20万アクセス数サイトのTLSに関する統計情報(https://www.ssllabs.com/ssl-pulse/)

ix　EU域内電子取引のための電子署名やID、トラストサービスに関する規制の標準

6.6.　今後の展望

PKIは Webサイトを中心に発展しましたが、現在ではその用途や環境は多様化しています。前述の Let' s Encryptは大量の証明書が自動で発行・更新できるため、短期間でインターネット全体の暗号化を進める推進力となりました。クラウドの拡大がサーバーの仮想化や運用の自動化を促進したことは、証明書運用についても例外ではありません。Google社やAmazon社、Microsoft社などのクラウドプロバイダーは独自の認証局サービスを展開しており、証明書発行枚数でも存在感を放つようになりました。証明書の活用はサーバーだけでなく増え続ける IoT[X]機器にも広がっています。IoT機器は数も多いため、多数の証明書を高頻度に発行し展開できる仕組みが必要です。

これらのトレンドを踏まえると今後はますます証明書の用途の多様化・細分化が進み、運用管理の自動化、サービス化が当たり前になっていくことが予想されます。人手の必要な EV証明書は手動によるオペレーションミスのリスクもありそれを完全に排除することは困難です。そうなれば議論の中心はライフサイクル管理システムの充実と個別サイト単位の信頼性計測の方法に移行していくのではないでしょうか。

サイトの信頼性に関して現時点での答えはありませんが、レピュテーション（評判）による信頼性の数値化やユーザーによる認証機関の選別などの興味深い提案はいくつか見られます。これらの中から PKIや Webの信頼をつくる技術が生まれてくるかもしれません。

一方でインフラの安全性、信頼性を追求するためにどこまでのコストを負担できるのか、バランスについても検討が必要でしょう。高い効果が期待できる施策でも、投じる労力・コストが直面するリスクとベネフィットに見合ったものでなければ必要とされません。安全を一元的に考えるのではなく個別の運用環境に応じた適切なレベルの PKIサービスを柔軟に選択できる環境整備が進められることを期待したいと思います。

1　フィッシングレポート2022 ｜ フィッシング対策協議会 技術・制度検討ワーキンググループ
https://www.antiphishing.jp/report/phishing_report_2022.pdf

2　ITU-T Recommendation database
https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14033

3　RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
https://datatracker.ietf.org/doc/html/rfc5280

4　プロフェッショナルSSL/TLS ｜ Ivan Ristić著、齋藤孝道 監訳（2017）ラムダノート

5　Black Tulip Report of the investigation into the DigiNotar Certificate Authority breach
https://www.researchgate.net/publication/269333601_Black_Tulip_Report_of_the_investigation_into_the_DigiNotar_Certificate_Authority_breach

6　CAB Forum – Certificate Issuers, Certificate Consumers, and Interested Parties Working to Secure the Web
https://cabforum.org/

X　Internet of Things（モノのインターネット）

7 Baseline Requirements – CAB Forum
https://cabforum.org/baseline-requirements/

8 Certificate Transparency(証明書の透明性) | DigiCert
https://www.websecurity.digicert.com/ja/jp/theme/ssl-certificate-transparency

9 RFC 9162: Certificate Transparency Version 2.0
https://www.rfc-editor.org/rfc/rfc9162.html

10 CertificateTransparency/ct_policy.md at master GoogleChrome/CertificateTransparency
https://github.com/GoogleChrome/CertificateTransparency/blob/master/ct_policy.md

11 RFC 6844: DNS Certification Authority Authorization (CAA) Resource Record
https://www.rfc-editor.org/rfc/rfc6844.html

12 RFC 8659 - DNS Certification Authority Authorization (CAA) Resource Record
https://datatracker.ietf.org/doc/html/rfc8659

13 RFC 6698: The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA
https://www.rfc-editor.org/rfc/rfc6698

14 DNSセキュリティ機構の普及状況調査:現状と今後の課題
https://dnsops.jp/event/20220624/20220624_yajima_v2.pdf

15 Major Android Security Leak: Manufacturer Signing Keys Used To Validate Malware Apps - CPO Magazine
https://www.cpomagazine.com/cyber-security/major-android-security-leak-manufacturer-signing-keys-used-to-validate-malware-apps/

16 Microsoft-signed malicious Windows drivers used in ransomware attacks
https://www.bleepingcomputer.com/news/microsoft/microsoft-signed-malicious-windows-drivers-used-in-ransomware-attacks/

17 Security Notice: NVIDIA Response to Security Incident - March 2022 | NVIDIA
https://nvidia.custhelp.com/app/answers/detail/a_id/5333/~/security-notice%3A-nvidia-response-to-security-incident---march-2022

18 RFC 9110: HTTP Semantics
https://www.rfc-editor.org/rfc/rfc9110.html

19 HTTPS 証明書の Common Name の検証がしれっと禁止されていた件について | IIJ Engineers Blog
https://eng-blog.iij.ad.jp/archives/14820

20 RFC 7469: Public Key Pinning Extension for HTTP
https://www.rfc-editor.org/rfc/rfc7469

21 自堕落な技術者の日記：HPKP(HTTP Public Key Pinning)公開鍵ピニングについて考える - livedoor Blog(ブログ)
http://blog.livedoor.jp/k_urushima/archives/1811745.html

22 Remove HTTP-Based Public Key Pinning - Chrome Platform Status
https://chromestatus.com/feature/5903385005916160#details

23 Ballot 193 – 825-day Certificate Lifetimes – CAB Forum
https://cabforum.org/2017/03/17/ballot-193-825-day-certificate-lifetimes/

24 Google Developers Japan: Chrome Root Program 開始に向けてのお知らせ
https://developers-jp.googleblog.com/2022/10/chrome-root-program.html

25 A New Life for Certificate Revocation Lists - Let's Encrypt
https://letsencrypt.org/2022/09/07/new-life-for-crls.html

26 ImperialViolet - Revocation checking and Chrome's CRL
https://www.imperialviolet.org/2012/02/05/crlsets.html

27 Introducing CRLite: All of the Web PKI's revocations, compressed - Mozilla Security Blog
https://blog.mozilla.org/security/2020/01/09/crlite-part-1-all-web-pki-revocations-compressed/

28 Information for the Public – CAB Forum
https://cabforum.org/info-for-consumers/

29 EV SSL Certificate Guidelines – CAB Forum
https://cabforum.org/extended-validation/

30 Chromium Docs - EV UI Moving to Page Info
https://chromium.googlesource.com/chromium/src/+/HEAD/docs/security/ev-to-page-info.md

31 「Chrome」と「Firefox」のアドレスバーでEV証明書の情報表示を変更へ - ZDNET Japan
https://japan.zdnet.com/article/35141280/

32 TLSとWebブラウザの表示のいまとこれから～EV証明書の表示はどうなるのか～
https://www.nic.ad.jp/ja/materials/iw/2018/proceedings/d1/d1-1-okuda.pdf

33 SSL Pulseデータの推移（SSL Pulse Trends）
https://kjur.github.io/www/sslpulsetrend/index_j.html#ovdvev

34 Commission runs a pilot project on Qualified Web Authentication Certificates (QWACs) | FUTURIUM | European Commission
https://ec.europa.eu/futurium/en/blog/commission-runs-pilot-project-qualified-web-authentication-certificates-qwacs.html

CYBERSECURITY REPORT 2022 ― 編集・発行 キヤノンマーケティングジャパン株式会社

Canon キヤノンマーケティングジャパン株式会社

〒108-8011 東京都港区港南2-16-6 CANON S TOWER

CSR2303CMJ_PDF