DIR SOC Quarterly

2023 spring vol.4

わが国の政策・法制度の動向

金融庁と業界団体との意見交換会の実施

トピックス

ChatGPT が サイバーセキュリティにもたらす影響

大和総研
Daiwa Institute of Research

目次

はじめに

本冊子は、サイバーセキュリティに関する動向をタイムリーにお伝えすることを目的としています。今回は、2022 年度第 4 四半期の話題を取り上げます。

本冊子は三部構成となっています。第 1 部はサイバー攻撃対策が国家主導の下に行われており、それを指揮する行政機関の動向をウォッチすることが不可欠であるため、この点にフォーカスしています。また実際のインシデント事例は、組織がさらされているサイバー攻撃の状況を端的に示すと同時に、組織の対策のあるべき姿を浮かび上がらせるものです。第 2 部はこの点に注目しています。また第 3 部では、注目度の高いサイバーセキュリティ関連の話題をトピックスとして詳しく説明します。

本冊子にて取り扱っている話題について、いくつかご紹介します。

サイバーセキュリティ対策を行うために経営層の関与は非常に重要です。経営層の関与の重要性については、本レポートでも継続して取り扱っている話題となりますが、本号では、第 1 部で金融庁が 2023 年 1 月 26 日に開催した主要行等に対する『業界団体との意見交換会において金融庁が提起した主な論点』についてご紹介します。併せてサイバーセキュリティ対策の予算確保の取り組みの参考として、IPA が公開しているセキュリティ関連費用の可視化ツールもご紹介しています。

日々のニュースでも取り上げられることが多いように、ランサムウェア攻撃は現在のビジネスにとっては深刻な問題です。攻撃により重要なデータが失われたり、ビジネス活動が中断したりすることがあります。ランサムウェア攻撃の対策として、警察庁の取り組みを第 2 部で、ランサムウェア対策として重要なデータ保護の考え方、バックアップの最新動向について第 3 部でご紹介します。

また、最近 OpenAI 社が開発したチャットボットサービスである ChatGPT が注目を集めています。ChatGPT はその多機能性から、ビジネス・医療・学術・エンターテインメントなど様々なジャンルで活用が期待されていますが、サイバーセキュリティの観点ではどのようなことが議論されているかについて、第 3 部でご紹介しています。

上記トピックスのいずれかが皆様の日々の活動に関連する何らかの「気づき」や「きっかけ」となれば幸いです。

2023 年 4 月　株式会社大和総研執筆者一同

1. 金融庁と業界団体との意見交換会の実施

意見交換会の概要

金融庁は 2023 年 1 月 26 日に開催した主要行等に対する『業界団体との意見交換会において金融庁が提起した主な論点』を公表しました (*1)。本意見交換会の内容の一つに金融機関に対するセキュリティ強化についての記載があり、金融庁が金融機関に実施したサイバーセキュリティに関する検査・モニタリング結果として以下の事例をあげています。

基本的な対策が講じられていない事例
セキュリティパッチが迅速に適用されていない事例
OS が更新されていない、または、サポート切れのまま使用を継続している事例
リモートワークなどの導入に伴い、外部ネットワークから内部ネットワークへのアクセスが可能となっているにもかかわらず、アクセス制御や認証機能が十分に堅牢なものとなっていない事例
アクセス権が一元管理されておらず、その付与・抹消を含め、管理状況の把握が困難となっている事例
特権アカウントについては更に厳格な管理が必要であるが、一元管理が行われていなかったり、そのログの監視・分析が行われていなかったりする事例
ガバナンスや内部統制
中期経営計画、年次計画上のサイバーセキュリティの施策が進捗していないにもかかわらず、経営層が看過している事例
外部委託先を一元的に管理しておらず、サイバーセキュリティの観点から評価していない事例
サイバーセキュリティに関する監査が形式的な確認にとどまっており、実効的な検証がなされていない事例

出典：本意見交換会の内容を基に大和総研作成

上記の事例などを踏まえ、より一層の対策が必要となることから、単なる技術上のリスクとして情報システム部門に任せきりにすることなく、経営陣が率先して関与し、予算・人材育成を含めて組織全体で対応を推進することを金融庁は求めています。

本意見交換会からの示唆

本意見交換会で金融庁が指摘しているサイバーセキュリティに関する検査・モニタリング結果の事例は、特段金融機関に限ったものではなく、あらゆる業界で必要となるセキュリティ対策についてあげていると言えます。

昨今のサイバー攻撃の情勢を鑑みると、事業規模にかかわらず、企業が事業を継続する上で十分なセキュリティ対策を確保することは必要不可欠であり、必要な予算を含めて対策を推進することが求め

(*1) https://www.fsa.go.jp/common/ronten/202301/01.pdf

られます。一方、サイバー攻撃の発生を防止するために、自社のセキュリティ対策としてセキュリティ製品やサービスの導入を検討する際、どの程度の予算をかければよいか根拠立てて試算することが困難と感じている企業も多いのではないでしょうか。

独立行政法人情報処理推進機構（IPA）ではこのような問題に対して、各種サイバー攻撃の被害が発生した際にその被害額を見積もることができるツールを提供しており、セキュリティ対策にかける予算を算出する際の参考になると思われます。

IPA がセキュリティ関連費用の可視化ツールを公開

IPA は 2023 年 1 月 20 日、セキュリティ関連費用を可視化するためのお助けツール「NANBOK」を公開しました (*1)。本ツールは Excel で作成されており、各種業界に分けて IPA の『情報セキュリティ 10 大脅威 2022』に関わる事象が発生した場合の自社の事情に則った想定損失額を算出できます。

「NANBOK」で選択可能な『情報セキュリティ 10 大脅威』
ランサムウェアによる被害
標的型攻撃による機密情報の窃取
サプライチェーンの弱点を悪用した攻撃
テレワーク等のニューノーマルな働き方を狙った攻撃
内部不正による情報漏えい
脆弱性対策情報の公開に伴う悪用増加
修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
ビジネスメール詐欺による金銭被害

×

「NANBOK」で選択可能な業界
製造業
サービス業（金融業・建設業を含む）
インフラ（エネルギー・交通）
IT（ベンダー・SIer・情報通信）

図：「NANBOK」で選択可能な『情報セキュリティ 10 大脅威』と業界の組み合わせ

出典：本ツールの内容を基に大和総研作成

本ツールでは選択した情報セキュリティ 10 大脅威と業界に合わせて、簡単な質問に回答することで算出が可能となる形式となっています。

IPA は企業のセキュリティ担当者が経営者に対してセキュリティ対策を遂行するための予算確保を行う際に利用してもらうことを想定して本ツールを作成しており、損害の合計金額だけでなく、事故対応や賠償損害といった項目ごとの内訳を確認できるので、これらの項目も必要となる対策を洗い出す際に活用できると思われます。

(*1) https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project/visualization-costs.html

2. NICTER 観測レポートの公開および サイバーセキュリティ対策分科会の設置

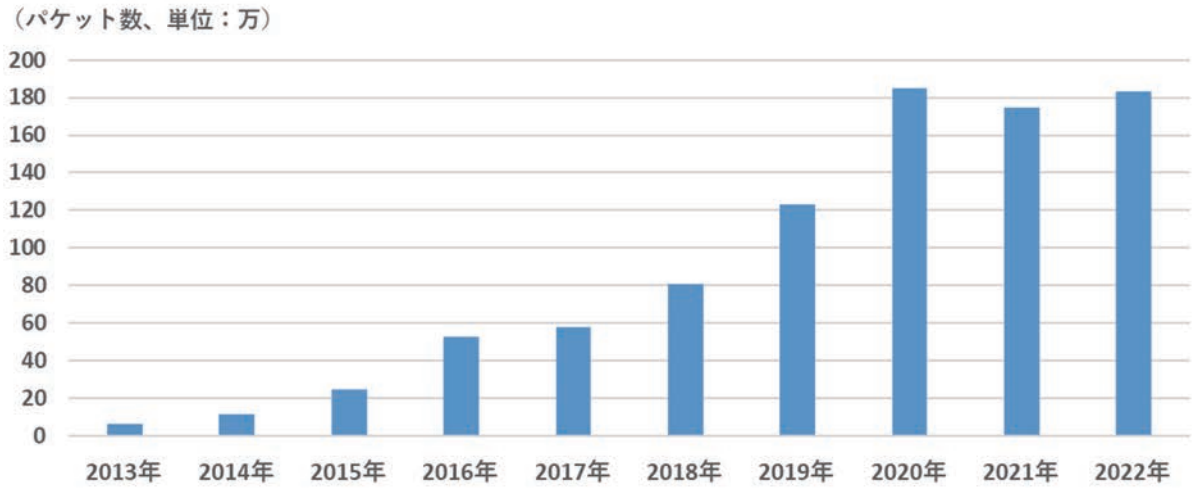
IoT 機器における課題

IoT 機器が一般家庭だけでなく企業においてもあらゆる業界で幅広く使用され、ビジネスにおいて重要かつ不可欠な存在となってきており、市場規模が拡大を続けています。その一方で IoT 機器はサイバー攻撃の標的として狙われるケースも多く、安全性の確保が課題となっています。

本記事では近年、急速に普及が進む IoT 機器に対するサイバー攻撃について、国立研究開発法人情報通信研究機構（NICT）のダークネットの観測結果と、総務省による対策への取り組みを紹介します。

NICTER 観測レポート 2022 の公開

2023 年 2 月に NICT は、『NICTER 観測レポート (*1) 2022』を公開しました (*2)。2022 年の 1 IP アドレス当たりの年間総観測パケット数は、前年の 2021 年から僅かな増加を見せたものの、ほぼ同じ水準で推移しています。



図：1 IP アドレス当たりの年間総観測パケット数（過去 10 年間）

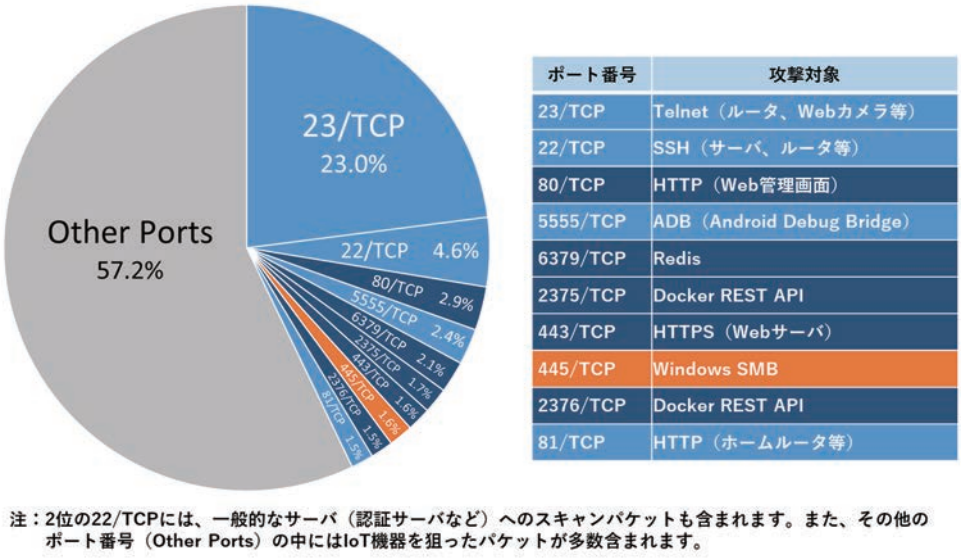
出典：『NICTER 観測レポート 2022』を基に大和総研作成

特徴として、以前から IoT 機器で使用されている Telnet（23/TCP）を狙った攻撃の割合が、2021 年の 11.0%から 23.0%へと増加したことがあげられます。 IoT 機器が使用する特徴的なポート番号はこれまでにもボットネットの攻撃対象として多く観測されていましたが、2022 年は特に 23/TCP を含むポート宛の攻撃が活発に観測されました。

(*1) NICT によるダークネットや各種ハニーポットによって観測したサイバー攻撃について、毎年の状況をまとめたレポート。

(*2) https://www.nict.go.jp/press/2023/02/14-1.html

下図の円グラフの水色の部分（23/TCP、22/TCP、5555/TCP、81/TCP）が、Web カメラやホームルータなどの IoT 機器に関連したサイバー攻撃関連通信です。



ポート番号	攻撃対象
23/TCP	Telnet（ルータ、Webカメラ等）
22/TCP	SSH（サーバ、ルータ等）
80/TCP	HTTP（Web管理画面）
5555/TCP	ADB（Android Debug Bridge）
6379/TCP	Redis
2375/TCP	Docker REST API
443/TCP	HTTPS（Webサーバ）
445/TCP	Windows SMB
2376/TCP	Docker REST API
81/TCP	HTTP（ホームルータ等）

注：2位の22/TCPには、一般的なサーバ（認証サーバなど）へのスキャンパケットも含まれます。また、その他のポート番号（Other Ports）の中にはIoT機器を狙ったパケットが多数含まれます。

図：宛先ポート番号別パケット数分布（調査目的のスキャンパケットを除く）

出典：『NICTER 観測レポート 2022』を基に大和総研作成

情報通信ネットワークにおけるサイバーセキュリティ対策分科会の設置

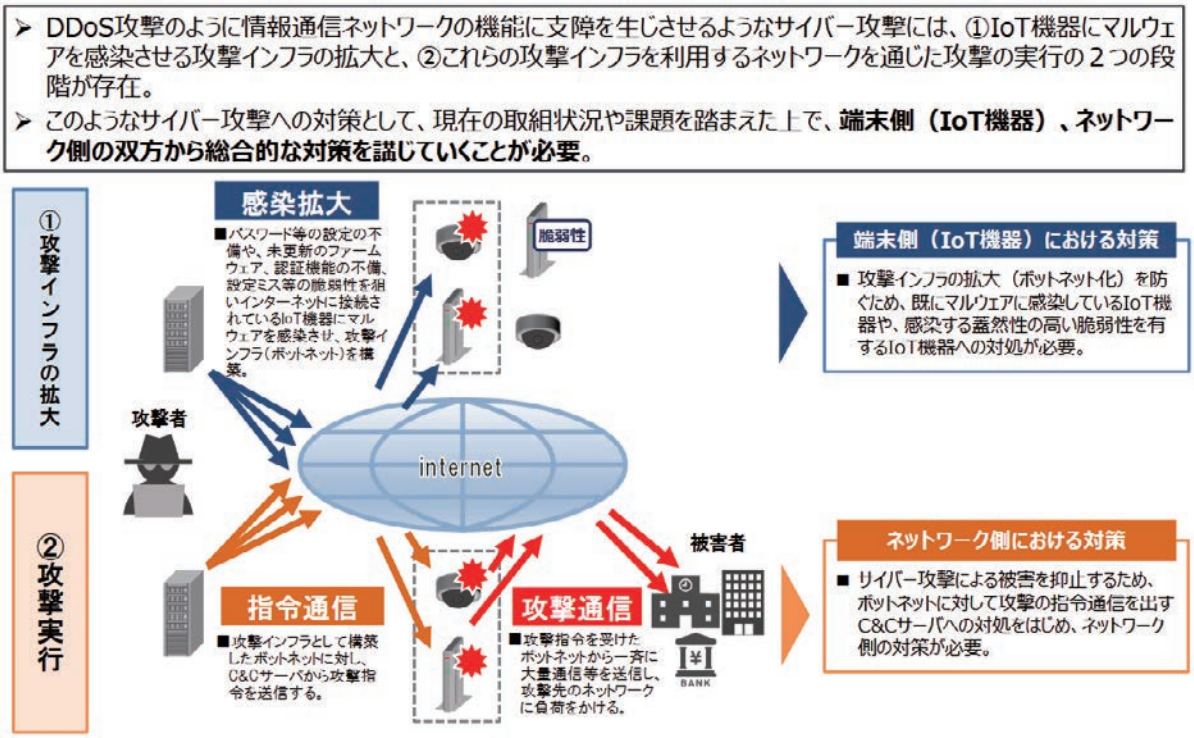
上記の IoT 機器を狙ったサイバー攻撃が多く発生している状況などに対応するため、総務省のサイバーセキュリティタスクフォースは 2023 年 1 月に「情報通信ネットワークにおけるサイバーセキュリティ対策分科会」を新たに設置することを公表しました (*1)。同分科会は 2022 年 8 月に取りまとめられた「ICT サイバーセキュリティ総合対策 2022」を踏まえ、以下の検討を行うこととしています。

1. IoT におけるサイバーセキュリティの確保に向けた取組（NOTICE (*2) 等）の現状と課題
2. 情報通信ネットワークにおけるサイバーセキュリティ対策の現状と課題（総合実証の検討等）
3. 上記課題の解決に向けた必要な方策

同分科会は今後、月 1 回ペースで実施され、本年 6 月頃に取りまとめ案ができる予定となっています。

(*1) https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00155.html

(*2) 総務省、NICT 及びインターネットプロバイダが連携し、IoT 機器へのアクセスによる、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起を行う取り組み。



図：情報通信ネットワークに対するサイバー攻撃の対策の方向性

出典：情報通信ネットワークにおけるサイバーセキュリティ対策分科会（第１回）資料１−２　事務局資料 (*1)

まとめ

サイバー攻撃に悪用される恐れのある IoT 機器に関する注意喚起（NOTICE 注意喚起）等の取り組みによって、国内における IoT 機器の注意喚起対象数は減少傾向にあるものの、依然としてマルウェアへの感染リスクが高い若しくは感染している IoT 機器が多数存在しているものとみられます。自社の IoT 機器がマルウェアに感染した場合、自社のネットワークが侵害されるだけでなく、ボットネットの一部として DDoS 攻撃に悪用されるなど、知らぬ間に加害者の立場になる恐れもあります。

「情報通信ネットワークにおけるサイバーセキュリティ対策分科会」が設置され、国として IoT 機器に対するサイバー攻撃対策の検討が進められているところですが、各企業においても自社で保有する IoT 機器を単なるハードウェアと認識せず、ソフトウェアが内蔵されたパソコンやサーバーと同様、適切な認証、セキュリティパッチの更新、意図しないポートの確認など、セキュリティ対策に十分配慮したうえで運用することが大切です。

(*1) https://www.soumu.go.jp/main_content/000856809.pdf

3. 『防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律案』の、民間企業への影響

概要

2023 年 2 月 10 日、防衛省から国会に『防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律案(*1)』が提出されました。これは日本の安全保障環境が厳しくなっていることや装備品が高度化している状況において、防衛装備品の調達をスムーズに行うことを目的として作成されています。

要綱では、防衛装備品の製造企業などに対して、サイバーセキュリティの強化を求めることが含まれており、その中でも「装備品製造等事業者」という言葉が全 21 項中 23 回登場し、ほぼ全項で語られていることから、サプライチェーンリスク管理が重要であることを示唆しています。

法律案の大枠	対象箇所	要約
防衛産業の位置付けの明確化	第 1 条 第 3 条	・装備品等の開発及び生産のための基盤を強化することが一層重要となっていることを明確化 ・防衛大臣が基盤の強化に関する基本方針を定め、公表
基盤強化の措置	第 4 条～ 第 7 条	任務に不可欠な装備品を製造する企業を対象に、防衛装備品等の製造に資する企業の取組について、サプライヤーも含め、経費を直接的に支払
サプライチェーン調査	第 8 条	任務に不可欠な装備品を製造する企業を対象に ・調査により、防衛省がサプライチェーンリスクを直接把握 ・企業は防衛省の調査に対して回答の努力義務
装備移転円滑化措置	第 9 条～ 第 25 条	装備移転を行う企業を対象に、装備品等の仕様・性能等を変更する費用に対する助成金の交付
資金の貸付け	第 26 条	装備品を製造する企業を対象に、貸付けを配慮
装備品等契約における秘密の保全措置	第 27 条 第 28 条	装備品等の機微情報の保全強化
製造施設等の国による保有	第 29 条～ 第 33 条	任務に不可欠な装備品を製造する企業を対象に、上記の措置を講じてもなお、他に手段がない場合、国自身が製造施設等を保有し、企業に管理・運営させることを可能とする

出典：第２１１回国会（常会）提出法案『防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律案』に掲載の図(*1)から大和総研が作成

(*1) 第２１１回国会（常会）提出法案『防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律案』

概要（ https://www.mod.go.jp/j/presiding/houan/pdf/211_230210/01.pdf ）

要綱（ https://www.mod.go.jp/j/presiding/houan/pdf/211_230210/02.pdf ）

サイバーセキュリティ体制の強化となる基準

これまでわが国は、サイバーセキュリティ体制の強化のための施策を促進するため、先行する米国の取り組みを参考に防衛装備品などに関連する重要情報をサイバー攻撃から守るための『防衛産業サイバーセキュリティ基準（2023 年度の契約から適用）(*1)』を整備してきました。具体的には、米国が採用するセキュリティガイドライン『NIST SP800-171(*2)』を参考にしています。NIST SP800-171 は調達から販売・供給まで一連のサプライチェーンに存在する、業務委託先や関連企業のすべてに対するセキュリティ対策についての方針を示しています。

軍事産業と自社は関係ない？

「軍事産業と自社は関係ない」と考える企業が多いかもしれませんが、サプライチェーンすべてに適用される上に、今後は他の業界にも広く展開されていく可能性が考えられます。なぜなら、前号でも取り上げたように経済産業省は『サイバーセキュリティ経営ガイドライン Ver3.0（案）に対する意見公募手続（2022 年 10 月）(*3)』、経団連は『経団連サイバーセキュリティ経営宣言 2.0（2022 年 10 月）(*4)』においてサプライチェーン管理について触れ、経営者に対してサプライチェーン全体を俯瞰したサイバーセキュリティを強化すべきと指示しているためです。

『DIR SOC Quarterly 2022 the first issue(*5)』でも取り上げた『経済安全保障推進法（2022 年 5 月 11 日成立）(*6)』においても、安全保障を確保するため「基幹インフラ役務の安定的な提供の確保（基幹インフラのサイバーセキュリティ確保）」を施策の一つにおいています。これにより、基幹インフラ事業者は重要設備（ハードウェア、ソフトウェア、クラウドサービスなど）の導入・維持管理等の委託について政府の事前審査を受けなければならず、また審査結果に基づいて勧告・命令などを受ける可能性があります。今後、具体化される内容について十分注意を払う必要があります。

(*1) 防衛装備庁　防衛産業サイバーセキュリティ基準の整備について（ https://www.mod.go.jp/atla/cybersecurity.html ）

(*2) SP800 シリーズで保護する情報には、政府の機密情報とされる CI（Classified Information）とそれ以外の重要情報と位置付けられる CUI（Controlled Unclassified Information）の 2 種類があります。米国では CI を SP800-53 で、CUI を SP800-171 で管理すると定められています。

(*3) https://public-comment.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595222069&Mode=0

(*4)『経団連サイバーセキュリティ経営宣言 2.0』（ https://www.keidanren.or.jp/policy/2022/087.html ）

(*5) 大和総研『DIR SOC Quarterly 2022 the first issue』（ https://www.dir.co.jp/publicity/publication/socquarterly2210.html ）

(*6) 正式名称は、『経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律』です。

経済安全保障推進法案の概要（ https://www.cas.go.jp/jp/houan/220225/siryou1.pdf ）

4. IPA『2022 年度情報セキュリティに対する意識調査【倫理編】【脅威編】』報告書の公表

情報セキュリティに対する意識調査

独立行政法人情報処理推進機構（IPA）は 2023 年 2 月 16 日、『2022 年度情報セキュリティに対する意識調査【倫理編】【脅威編】』の結果報告書を発表しました(*1)。「情報セキュリティに対する意識調査」は、一般国民のネットモラルに対する現状を把握するための「倫理調査」を 2013 年から実施し、サイバーセキュリティにおける脅威の認識と対策の実施状況を把握するための「脅威調査」を 2005 年から実施しています。「倫理調査」は 13 歳以上の SNS 等における投稿経験者 5,000 名に対して、「脅威調査」は 13 歳以上の PC あるいはスマートフォン利用者 10,000 名に対して行われています。下表は「倫理調査」、「脅威調査」の質問項目です。以降では、結果報告書のポイントを取り上げます。（下線の質問）

倫理調査の質問			
Q1	倫理教育の受講経験	Q14	家族や友人などの許可を得ず投稿したことのある情報
Q2	SNS 等で拡散したことのある情報・内容	Q15	家族や友人などの許可を得ず投稿した理由
Q3	SNS 等で拡散したことのあるリスクある内容	Q16	家族や友人などの許可を得ず投稿しない理由
Q4	SNS 等で拡散する理由（モチベーション）	Q17	自分の個人情報を許可なく投稿された経験
Q5	SNS 等での拡散時の心がけ	Q18	許可なく自分の個人情報を公開されたことに対する気持ち
Q6	自身のネガティブな投稿経験	Q19	SNS での写真・動画の共有範囲
Q7	自身のネガティブな投稿経験の理由	Q19SQ	SNS での写真・動画の共有時の抵抗感
Q8	自身のネガティブな投稿後の感情	Q20	動画、ソフトウェア、楽曲などのコピーや公開に対する意識
Q9	自身のネガティブな投稿後に発生したこと	Q21	SNS 等で知り合った人と 1 対 1 で会った経験の回数
Q10	自身のネガティブな投稿の公開範囲	Q22	1 対 1 で会うきっかけとなった SNS 等のツール
Q11	自身のプライベートや個人の情報の公開経験	Q23	1 対 1 で会うことになった理由
Q12	プライベートや個人の情報の公開に対する考え	Q24	1 対 1 で実際に会った結果発生したこと
Q13	プライベートや個人の情報を公開しない理由	Q25	自身の投稿や SNS に関して受けた経験
脅威調査の質問			
Q1	セキュリティ教育の受講経験	Q7	パスワード設定における対策状況
Q2	脅威の認知度	Q8	パスワード管理方法
Q3	脅威の特徴、手口、被害例等の理解度	Q9	脆弱性対策の必要性認知
Q4	脅威との遭遇経験	Q10	脆弱性対策状況
Q5	被害経験	Q11	セキュリティ対策状況
Q6	アカウント保有数		

表：『 2022 年度情報セキュリティの倫理と脅威に対する意識調査−【倫理編】−』(*2)『 2022 年度情報セキュリティの倫理と脅威に対する意識調査−【脅威編】−』(*3)を基に大和総研作成

(*1) https://www.ipa.go.jp/security/economics/ishikichousa2022.html

(*2) https://www.ipa.go.jp/files/000108322.pdf

(*3) https://www.ipa.go.jp/files/000108321.pdf

倫理に対する意識調査の結果

「Q11 自分の個人情報やプライベートな情報の公開経験」では、「趣味・関心」「性別」を公開した経験がある割合がほぼ同じ 52%超と最も多い回答でした。続けて「居住している都道府県」（47%）、「生年月日・年齢」（35.3%）となっています。「Q12 自分の個人情報やプライベートな情報の公開に対する考え」では、「第三者に知られても問題ない」「公開範囲を限定している」「今まで問題なかった」の割合が高い結果となっています。「家族や友人しか見に来ないので大丈夫」の回答割合が平均（23.2%）より高いのは 10 代（33.3%）、20 代（29.5%）となっています。

脅威に対する意識調査の結果

「Q1 セキュリティ教育の受講経験」では、10 代、20 代の順に受講割合が高く、この傾向は 2020 年、2021 年と同じ結果となっています。

「Q7 パスワード設定における対策状況」では、10 代、20 代の「推測しにくいパスワード」「できるだけ長いパスワード」の実施率が他の年代に比べ低くなっています。全年代で実施率が低いのは「パスワードの使い回しをしない」で、使い回す人の割合は 4 割から 5 割となっています。「Q11 セキュリティ対策状況（多要素認証や OS アップデートなど）」でも全体的に 10 代、20 代の実施率は他の年代に比べ低くなっています。全年代で「リモートロック」「紛失時のデバイス探索設定」の実施率は 3 割程度と低い結果となっています(*1)(*2)。

報告書からの示唆

インターネット上ではたびたび誹謗中傷、ネットストーカー、不正アクセスなどの事件が発生しています。SNS 等での情報発信についてどのようなリスクがあるのかを知ることでトラブルから自身を遠ざけることができます。しかし「倫理調査」結果から、公開範囲を限定しているといった対策が取られているものの、今まで問題なかったから、友人だから大丈夫という回答もあり、個人情報が意図せず洩れるリスクがあります。また「脅威調査」結果から、パスワードを使い回す人の割合が 4 割から 5 割と多いこと、特に 10 代、20 代で短く簡易なパスワード設定が行われているだろうことから、なりすまされるリスクがありえます。このような個人情報の公開や推測されやすいパスワードが原因となって SNS が乗っ取られた場合、自身が被害者のみならず、加害者になりかねず、情報倫理やセキュリティに関して学ぶことはとても重要であると言えます。第 2 部「SNS の投稿内容からパスワードを推測し不正ログイン」にて、そのような事例を紹介していますので、併せてご参照ください。

(*1) 独立行政法人情報処理推進機構『2022 性別・年代軸_脅威調査 PC』（https://www.ipa.go.jp/files/000108301.pdf）

(*2) 独立行政法人情報処理推進機構『2022 性別・年代軸_脅威調査 SP』（https://www.ipa.go.jp/files/000108302.pdf）

5. 安心安全なメタバース空間の実現に向けたセキュリティガイドラインを一部公開

メタバースのセキュリティガイドラインを一部公開

日本スマートフォンセキュリティ協会（JSSEC）、メタバース推進協議会、セキュア IoT プラットフォーム協議会（SIOTP 協議会）は 2023 年 2 月 17 日、メタバース(*1)空間における『セキュリティガイドライン（一部公開版）』を公開しました(*2)。これは、メタバース推進協議会が設置したセキュリティ分科会において 2022 年 6 月から進められてきた検討の成果を公開したものです。本ガイドラインは、メタバースがより世間に普及し、新たな課題の抽出やセキュリティ技術が進む過程において随時更新される予定です。

メタバースがまだ普及していない現状において個別のセキュリティ課題を検討するのは難しいため、本ガイドラインは、ユーザー・プラットフォームなど、メタバース事業に関わる機能別レイヤーの整理から始めています。その上で、機能別レイヤー毎のバリューチェーン(*3)を分解しています。分解したバリューチェーンに対し、ユースケースを想定しセキュリティ課題を洗い出します。最後にそれぞれのセキュリティ課題に対する対策、法的観点での補足・留意事項を検討しています。

ガイドライン作成ステップ	作業内容
（Step1）機能別レイヤーの整理	・ユーザー、コンテンツ、プラットフォームなどのメタバース事業に関わる機能別レイヤーを整理
（Step2）バリューチェーン分解	・Step1 で整理した機能別レイヤー毎にバリューチェーンを分解 例：ユーザーレイヤーの場合は、デバイスの登録、個人情報の登録、本人認証、決済情報の登録、アバターの作成、仮想空間へのアクセス、仮想空間での消費活動、仮想空間での生産活動 に分解
（Step3）ユースケースを想定した課題の整理	・Step2 で分解したバリューチェーン毎にユースケースを想定した課題を整理 例：ユーザーの本人認証の場合は、他人が本人になりすます行為などが課題
（Step4） セキュリティ対策の検討	・Step3 で整理した各課題に対して考えられるセキュリティ対策の方向性を整理
（Step5） 法的観点での整理	・Step3 の課題や Step4 の対策における法的観点での補足・留意事項などを整理

表：『セキュリティガイドライン（一部公開版）』を基に大和総研作成

メタバースにおけるセキュリティ課題と対策

今回の一部公開版では「利用者の本人確認・本人認証」「利用者へのコンテンツ販売」「デバイスの設計・制作」におけるセキュリティ課題・留意点・対策が公開されています。

(*1) 明確な定義はなくコンピューターの中に作られた仮想空間のことを指します。仮想空間の中で利用者はアバターを作成しコミュニケーションしながらゲームや買い物などを行うことができます。語源は Meta(超越)と Universe(宇宙)を組み合わせた造語です。

(*2) https://jmpc.jp/wp-content/uploads/2023/02/47cfadf4f713ce549607cdf764adbdcb-2.pdf

(*3) サービスの設計・制作から利用者に提供するまでの一連の流れの中で付加価値を生む工程がなにかを分析するフレームワーク。

■（本人確認・本人認証）アバター乗っ取りによるなりすまし行為

【課題・留意点】

・ヘッドマウントディスプレイ(*1)を被った際に多要素認証など従来の方法が困難となる場合がある

・犯罪収益移転防止法に定められる特定取引の場合、本人確認など同法の定めを遵守する必要がある

【対策】

・利便性の高い本人確認およびセキュアな認証が必要

・高い機密性が求められる利用用途ではマイナンバーカードによる公的個人認証の仕組み等が必要

■（コンテンツ販売）コンテンツが偽物の空間へデリバリーされるリスク

【課題・留意点】

・メタバースにおける仮想空間においてもフィッシング、コピー、偽物のリスクがある

・メタバースのプラットフォーム側が安全性に対する審査が不十分だと利用者に損害を与えるコンテンツが流通してしまう

【対策】

・利用者による安全確認を可視化し投票等によって健全性を保つ

・メタバースのプラットフォーム側が仮想空間に対して審査・認証を行って保護する

■（デバイスの設計・制作）デバイスの脆弱性を狙った攻撃や不適切なデバイスによる健康被害

【課題・留意点】

・センサーの小型化により身体的特徴や利用者の位置情報などプライベート情報の取得が可能となる

・デバイスによる健康被害のリスクがあることに留意したデバイス開発が求められる

【対策】

・デバイスの設計から利用、廃棄まで、ライフサイクル全体を考慮したセキュリティ対策が必要

・健康被害のリスクに対しては厚生労働省などによる安全基準が求められる可能性がある

本ガイドラインからの示唆

メタバースは新たなコミュニケーション手段として注目されており、エンターテインメント分野だけでなくビジネス分野における活用も増えています。しかし、ルールや規制の整備、セキュリティ対策は十分に行われていると言えない状況であり、利用者はセキュリティリスクを意識して利用する必要があります。また、メタバースでビジネス展開を行う場合は、利用者に安心してサービスを利用してもらうために、メタバースの特性を理解したセキュリティ対策を行うことが求められます。

(*1) ゴーグルのように頭に装着するディスプレイのことです。装着することで大画面で映画やゲームを楽しむことができます。

1. 警察庁による LockBit 暗号化済みデータの復元成功

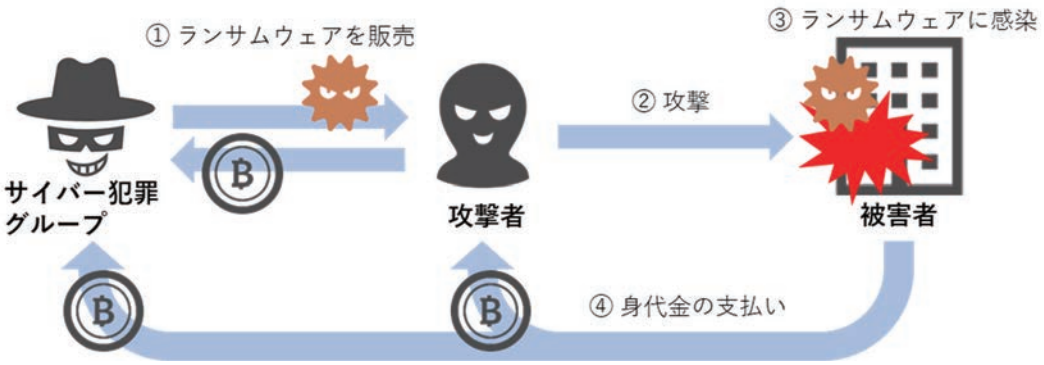
概要

2022 年 12 月 28 日、複数の報道機関において警察庁のサイバー特別捜査隊がランサムウェアである「LockBit」により暗号化されたデータの復元に成功したと報じられました (*1)。同隊ではすでに LockBit の被害にあった国内企業 3 社においてデータの復元に成功しており、複数の国の捜査機関に対して復元方法の情報提供が行われているとされています。

また、報道機関による取材に対して警察庁の関係者は、被害回復に至った事例は複数あるが具体的な内容については差し控える、と回答をしています。

LockBit とは

LockBit は 2019 年 9 月頃に存在が確認されたランサムウェアの一種で、感染すると被害者のデータを暗号化し、復号するための鍵と引き換えに身代金を要求するもので、数あるランサムウェアの中でも現在、特に被害の発生が多いものの一つです。このランサムウェアはサイバー犯罪グループによって開発・管理されており、同グループが攻撃者に対してパッケージ化した製品として提供することで、被害者から支払われた身代金を同グループと攻撃者で分配する RaaS（Ransomware as a Service）というビジネスモデルを形成しています。これにより、高度な技術を持たない攻撃者であっても同グループに対価を支払うことで容易に攻撃を実行できるため、被害が拡大しているのが現状です。



図：RaaS のイメージ

出典：大和総研作成

(*1) 日本経済新聞　身代金ウイルス、警察庁が暗号解除成功　支払い未然防止
(https://www.nikkei.com/article/DGXZQOUE062930W2A201C2000000/)

読売新聞　ランサムウェアで暗号化された企業データ復元に成功、身代金支払い防ぐ…警察庁サイバー特捜隊
(https://www.yomiuri.co.jp/national/20221228-OYT1T50190/)

産経新聞　ランサム被害のデータ復元成功　警察庁、暗号化を強制解除
(https://www.sankei.com/article/20221228-RLMXVY5SPBNPZP3K4T4M4SOQYE/)

LockBit はこれまでに複数回にわたってバージョンアップされており、 2021 年 6 月頃に LockBit2.0、2022 年 6 月頃に LockBit3.0 の存在が確認されています。この過程において複数の機能の追加やデータを暗号化する仕組みの変更が行われています。

特に注意すべきこととして、外部にデータを送信する機能が追加されたことによって、暗号化されたデータを復号するための身代金要求だけでなく、窃取した情報を公開すると脅す「二重脅迫」という手法が用いられるようになっており、被害者をより身代金の支払いに応じざるを得ない状況に追い込むよう仕向けられています。

報道内容の考察

今回報道された内容においては、サイバー特別捜査隊がデータの復元に用いた手法や復元に成功した LockBit のバージョンなどの情報が明かされていないため、バージョンの違いにかかわらず、暗号化されたデータをすべて復元可能かどうかは不明です。しかし、少なくとも被害にあった国内 3 社においてデータを元に戻すことに成功したと報じられており、今後、新たに被害を回復できる企業が現れることが期待できます。

その一方で、LockBit には外部にデータを送信する機能が含まれているため、この機能により外部にデータが送信された場合、情報漏洩の被害を回復することはできません。また、今回の報道を受けて、LockBit を開発する犯罪グループが暗号を解読できないように何らかの改修を加える可能性もあり、今後新たに LockBit に感染した場合、データを復元できる可能性が低くなることが懸念されます。

以上のことから、やはりあらかじめランサムウェアへの感染を防止する対策を講じておくことが最も重要と言えます。しかし、感染リスクを完全に回避することは事実上不可能であるため、ランサムウェアによる被害が発生した場合を想定して被害の早期検知と早期対処の仕組みを構築し、適切に取得したバックアップからデータを復元できる体制を確保しておく必要があります。データのバックアップについては第 3 部のトピックス『データ保護の「3-2-1 ルール」と最新動向』で触れていますのでご参照ください。

2. Web スキミングによるクレジットカード情報の窃取

ソースネクスト・サイト不正アクセスの概要

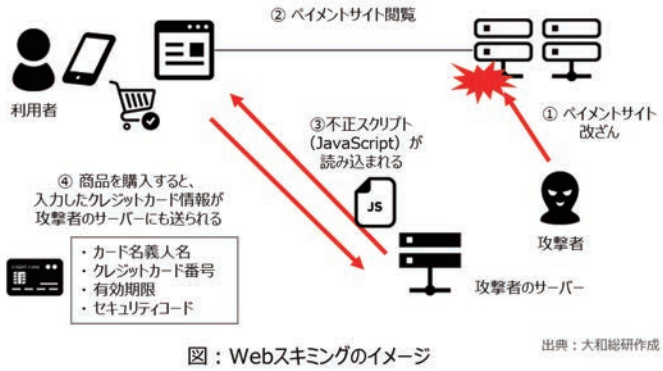
PC ソフト・スマートフォンアプリなどの開発、販売を事業展開する「ソースネクスト株式会社」は 2023 年 2 月 14 日、第三者の不正アクセスによる個人情報の漏洩について発表しました。漏洩した情報には顧客のクレジットカード情報 112,132 件が含まれる可能性があります。同社は、同年 1 月 4 日にクレジット会社から当サイトを利用した顧客のクレジットカード情報漏洩の懸念について連絡を受け、翌 1 月 5 日に当サイトのカード決済を停止しています。しかし一部の顧客のクレジットカード情報は不正利用された可能性があることが確認されています。

原因については「弊社が運営するサイトのシステムの一部の脆弱性を利用した第三者の不正アクセスにより、ペイメントアプリケーションの改ざんが行なわれたため。(*1) 」に留まり、それ以上は公表されていません。しかし「アプリケーションの改ざん」「漏洩した情報がセキュリティコード(*2) を含むクレジットカード情報」であることから、国内 EC サイトの被害が確認されている「Web スキミング」と同類の攻撃を受けた可能性が考えられます。

Web スキミング

Web スキミング自体は新しい攻撃手口ではありません。攻撃者は EC サイト上に不正なコードを挿入して、顧客が EC サイト上で入力した決済情報を窃取する攻撃です。

Web スキミングは多くが JavaScript の改ざんによって行われます。改ざんされた EC サイトから利用者が商品を購入すると、正規の EC サイト上で正常に決済が完了すると同時に、商品購入時に入力したクレジットカード情報（カード名義人名、クレジットカード番号、有効期限、セキュリティコード）が攻撃者のサーバーにも送信されます。



図：Webスキミングのイメージ

(*1) ソースネクスト株式会社　当サイトへの不正アクセスによる個人情報漏えいに関するお詫びとお知らせ
https://www.sourcenext.com/support/i/2023/0214_info/?i=gtnews

(*2) カード情報保護のための国際的な基準である PCI DSS では、セキュリティコードは、加盟店のみならず決済代行事業者も処理後に直ちに削除することが求められており、保存すること自体が禁止されています。

被害に遭っても気づきにくい特徴

Web スキミングは、2022 年 3 月に日本サイバー犯罪対策センター（JC3：Japan Cybercrime Control Center）が注意喚起(*1) を行い、 JPCERT/CC は 2023 年 1 月に四半期ごとに発表しているインシデント報告対応レポート(*2) の中で、2022 年 10 月 1 日～12 月 31 日に確認された事例として紹介しています。

Web サイトの改ざんというと、攻撃者が挑発的で利用者に不快感を与えるデータを挿入したり、悪意をもって Web ページの外観を変更する場合がイメージされます。 しかしながら、JC3 および JPCERT/CC のレポートによると、改ざんされた Web サイトは見た目では判断できず、難読化された JavaScript が Web サイトに挿入されていることが確認されています。その結果、気づかないうちにクレジットカード情報が窃取されるという特徴があります。

インシデントからの示唆

このようなケースでは、EC サイト側は被害者である立場でもありますが利用者からみると責任は EC サイトにあるとみられます。実際に、利用者はセキュリティコードを含むクレジットカード情報が漏洩されているわけなのでクレジットカードの再発行を余儀なくされます。電子決済やクレジットカード決済が日常に浸透しつつある中で利用者への影響は大きいと考えます。また、今後、当該サイトでの購入に抵抗を覚えることや企業の信頼性が低下することは免れないでしょう。

Web スキミングに対する完璧な対策は難しいと言われています。JavaScript は Web ブラウザに動きを加えることができ、利用者に使いやすさと快適さを提供します。利用者の集客を望む EC サイトでは JavaScript を利用しない選択は考え難いのではないでしょうか。そのため、サイトを運営する側は JavaScript の特徴やそのメリット・デメリット、長短についてもっと知る必要があると考えます。

運営する Web サイトに悪意のある JavaScript が挿入される可能性について認識し、脆弱性管理はもちろんのこと定期的なセキュリティ診断や Web 改ざん検知ソリューションの導入等を検討してはいかがでしょうか。

(*1) 日本サイバー犯罪対策センター（JC3） 脅威情報のトピックス https://www.jc3.or.jp/threats/topics/

(*2) JPCERT/CC インシデント報告対応レポート［2022 年 10 月 1 日～2022 年 12 月 31 日］
https://www.jpcert.or.jp/pr/2023/IR_Report2022Q3.pdf

3. SNS の投稿内容からパスワードを推測し不正ログイン

概要

2023 年 1 月 18 日、警視庁は他人のインスタグラムのアカウントを乗っ取ったとして、男を不正アクセス禁止法違反容疑などで逮捕しました(*1)。被害に遭ったのは東京、埼玉、神奈川などに住む 20 代の女性 9 人です。男は 2020 年 8 月から 2021 年 10 月にわたり 59 回の不正ログインを行い、個人情報をのぞき見したり、アカウントのパスワードを書き換えてアカウントを乗っ取ったりした疑いがあります。動機は「自分の生活にコンプレックスがあり嫌がらせをしようと思った」と説明しています。

SNS 乗っ取りの手口

警視庁によると、男はターゲットにしたインスタグラムのアカウントを数日間にわたり観察し、誕生日パーティーなどの投稿内容を元に誕生日を推測しパスワードを割り出していました。今回被害に遭った 9 人のほとんどがアカウント名と誕生日を組み合わせた推測されやすいパスワードを使っていました。さらにアカウントの乗っ取りに成功すると、本人になりすまし、乗っ取ったアカウントのフォロワーに「テーマパークのチケットを受け渡すために SNS のパスワードが必要だ」などとメッセージを送り、パスワードを聞き出していました。そのため特定の人物しか見ることのできない非公開アカウントも被害に遭いました。

出典：大和総研作成

SNS の不正ログイン被害

最近の SNS の不正ログイン被害の事例としては、次の表のようなものがあります。

(*1) 朝日新聞デジタル　「リア充の 20 代女性に嫉妬して」　インスタ乗っ取り容疑で男を逮捕
(https://www.asahi.com/articles/ASR1L3TJXR1LUTIL00D.html)

発生時期	対象 SNS	事例内容
2022 年 1 月	インスタグラム等	女子大生・タレントの SNS に不正アクセス 約 2000 人分の ID とパスワードを保管していた (*1)
2022 年 11 月	YouTube	歌手が乗っ取り被害　Tesla 社の YouTube チャンネルになりすまし 登録していたメールアドレスパスワードは全て変更されていた(*2)
2022 年 11 月	YouTube	東急電鉄の公式 YouTube チャンネルが乗っ取り被害 東急電鉄の YouTube に無関係の動画がアップロードされた(*3)
2022 年 12 月	インスタグラム	友人女性のアカウントを乗っ取り 本人になりすましメッセージを送信していた(*4)
2023 年 2 月	Twitter	ドトールコーヒー公式 Twitter アカウントが乗っ取り被害 アイコンやヘッダー画像の削除や関係のない投稿が見つかった(*5)

表：各種報道資料等を基に大和総研作成

SNS の不正ログイン被害は以前からたびたび発生しています。また総務省や IPA などから SNS 利用時の注意事項に関する情報(*6)を発信しているにもかかわらず、推測されやすいパスワードの設定やパスワードを使い回していたために不正ログインの被害に遭うケースも多く発生しています。最近ではマーケティングや採用活動などで SNS を利用する企業も増えているため、個人アカウントだけでなく企業アカウントも被害に遭うケースが増えています。企業アカウントが不正ログイン被害に遭った場合、乗っ取りにより不適切な投稿をされ、ブランドイメージなどに影響を与える可能性があります。

インシデントからの示唆

推測されやすいパスワードの設定やパスワードの使い回しなどにより個人や企業、公開や非公開アカウント、誰もが SNS の不正ログイン被害に遭う可能性があります。被害に遭わないために、利用している環境のセキュリティ上のリスクや留意点を知っておく必要があります。また SNS が多要素認証やログイン履歴などを提供している場合はそれらを利用しセキュリティ対策を行うことも必要です。企業アカウントは特に被害が大きくなる可能性があるため、SNS の運用ルールを策定しておくことも必要です。

(*1) https://www.yomiuri.co.jp/national/20220107-OYT1T50005/

(*2) https://www.itmedia.co.jp/news/articles/2211/08/news102.html

(*3) https://www.j-cast.com/2022/11/04449652.html?p=all

(*4) https://news.yahoo.co.jp/articles/11e1d667ce17134e88b136d931f5bfe2bf3576ad

(*5) https://www.itmedia.co.jp/news/articles/2302/14/news107.html

(*6)（総務省）『SNS を利用する際の情報セキュリティ対策』
（ https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/16.html ）

（IPA）『不正ログイン対策特集ページ』（ https://www.ipa.go.jp/security/anshin/account_security.html ）

1. ChatGPT がサイバーセキュリティにもたらす影響

ChatGPT とは

ChatGPT は米国の AI 研究開発企業である OpenAI 社が開発したチャットボットサービスです。名前後半の「GPT」は Generative Pre-trained Transformer という AI 技術を利用した言語モデルの名前に由来しています。インターネット上のテキストを大量に読み込ませ、自然な文章を生成できるように訓練してあります。

現在は研究プレビュー版のため無償で公開されており、ユーザー登録すれば誰でも利用できます。公開日は 2022 年 11 月 30 日でしたが、公開当初から世界中で話題となり、2 カ月後の 2023 年 1 月には月間アクティブユーザーが 1 億人(*1)に達しました。これはユーザー数が 1 億人に達するのに 9 カ月を要した TikTok や 2 年半を要したインスタグラムよりも大幅に速い記録です。

これほど急速にユーザーを獲得している理由の一つはその優れた会話能力です。これまでのチャットボットはユーザーの意図を誤解したり、内容の乏しい回答をしたりするものも少なくありませんでした。しかし、この ChatGPT はユーザーの意図や文脈をこれまでのチャットボットと比較すると桁違いと言えるまでに高度に推定・把握し、回答を返してくれます。また、会話能力だけでなく、その多機能性にも注目が集まっています。たとえば、以下のようなこと(*2)も実行してくれます。

- 履歴書の作成や添削
- 文章の要約
- 専門用語の解説
- 外国語への翻訳
- プログラミング（ソースコードの生成や添削）
- エッセイや物語の生成

しかし、その優れた性能ゆえに、サイバーセキュリティの領域においても大きな影響を与えそうだと考える有識者が多く、活発な議論がなされています。以降では、どのような議論がなされているかを紹介します。

(*1) REUTERS 『ChatGPT sets record for fastest-growing user base - analyst note』
(https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/)

(*2) TechRader『What can ChatGPT do? Here's 11 fun and useful ways it can boost your life』
(https://www.techradar.com/features/what-can-chatgpt-do-heres-11-fun-and-useful-ways-it-can-boost-your-life)

サイバーセキュリティに対する脅威

まず多くの有識者が指摘するのはサイバーセキュリティに与える悪影響です。ChatGPT はたとえば以下のようなことに悪用可能だと指摘(*1)されています。

- フィッシング詐欺に利用可能なメールを作成
- マルウェアのソースコードを生成
- SNS 上でソーシャルエンジニアリングに活用（偽プロフィールを作成するなど）

もちろんこのような利用方法は OpenAI 社の利用規約で禁じられていますし、このような利用ができないようにコンテンツフィルターも設定されています。しかし、コンテンツフィルターは完全ではなく、やり方によってはこのような利用ができてしまうため、実際にマルウェアのソースコードを生成できたとの報告が多くなされています。

またサイバー攻撃者による悪用ではないですが、機密データが流出する危険性もあります。ChatGPT に入力したデータは ChatGPT の学習に利用されるため、たとえば ChatGPT に業務上の機密データを入力してしまうとその機密データは意図せずに第三者の目に触れてしまう可能性があります。実際に業務上の機密データを ChatGPT に入力してしまう事案は既に発生(*2)しているようです。

逆に ChatGPT が学習した機密データや個人情報を意図的に抜き出すという攻撃も考えられます。これは「トレーニングデータ抽出攻撃」（training data extraction attacks）(*2)と呼ばれています。

なお、このようなリスクを考慮してのことかどうかは明確になっていませんが、海外の金融機関では ChatGPT の社内利用を禁止する動き(*3)が広がっています。

(*1) ZDNET 『ChatGPT and more: What AI chatbots mean for the future of cybersecurity』
(https://www.zdnet.com/article/chatgpt-and-more-what-ai-chatbots-mean-for-the-future-of-cybersecurity/)

(*2) Dark Reading 『 Employees Are Feeding Sensitive Biz Data to ChatGPT, Raising Security Fears』
(https://www.darkreading.com/risk/employees-feeding-sensitive-business-data-chatgpt-raising-security-fears)

(*3) Bloomberg 『Wall Street Banks Are Cracking Down on AI-Powered ChatGPT』
(https://www.bloomberg.com/news/articles/2023-02-24/citigroup-goldman-sachs-join-chatgpt-crackdown-fn-reports)

サイバーセキュリティに対する利点

一方、ChatGPT がサイバーセキュリティにもたらす良い影響については、たとえば以下のような点が指摘(*1)(*2)されています。

- セキュリティインシデントの分析自動化
- ペネトレーションテストの効率化（ツールやレポート作成）
- 脆弱性検査の効率化

またマルウェア作成と同じく、実際に ChatGPT を利用してセキュリティインシデントの分析が可能であったとの報告(*3)もあります。

まとめ

ChatGPT は現時点（2023 年 4 月現在）で公開からまだ 4 カ月程度しか経過しておらず、様々な人が様々な検証や考察を行っている段階と言えるでしょう。新しい技術が登場した際に賛否両論が巻き起こるのは世の常です。また「技術」はそれを使う人間次第で利用も悪用もできます。

現時点の情報を見る限り、ChatGPT によって全く新しいサイバー攻撃が可能になるとか、誰でも簡単にサイバー攻撃が可能になるということはなさそう(*4)です。ただサイバー攻撃の「効率化」をもたらしそうだということは確かです。ChatGPT を悪用した攻撃に関する動向に注意を払いながらも、やはりサイバーセキュリティ対策の基本動作（セキュリティコントロールの実装やインシデントレスポンス体制の構築など）を確実に実行することが重要であると言えるでしょう。

(*1) Nuspire 『ChatGPT in Cybersecurity: Benefits and Risks』(https://www.nuspire.com/blog/chatgpt-in-cybersecurity-benefits-and-risks/)

(*2) CRN 『5 Big Pros And Cons Of ChatGPT For Cybersecurity』(https://www.crn.com/news/security/5-big-pros-and-cons-of-chatgpt-for-cybersecurity)

(*3) SECURELIST 『IoC detection experiments with ChatGPT』(https://securelist.com/ioc-detection-experiments-with-chatgpt/108756/)

(*4) MalwareTech 『A Realistic Look at Implications of ChatGPT for Cybercrime』(https://malwaretech.com/2023/02/a-realistic-look-at-chatgpt-cybercrime.html)

2. データ保護の「3-2-1 ルール」と最新動向

3-2-1 ルールとは何か？

米国国土安全保障省配下の米国コンピューター緊急事態対応チーム（US-CERT: United States Computer Emergency Readiness Team）が 2012 年に「3-2-1 ルール」を公表(*1)しました。これは重要なデータのバックアップに関する有名なベストプラクティスなのですが、セキュリティ最後の砦であるバックアップの重要性が見直される中、昨今、注目を集めています。

3-2-1 ルール

> **3** – 重要なファイルは 3 つのコピーを保持すべし：1 つのプライマリと 2 つのバックアップ
>
> **2** – 異なる種類の危険から守るために 2 つの異なる媒体に保存すべし
>
> **1** – 1 つのコピーはオフサイトに保存すべし（たとえば自宅やオフィス以外の場所）

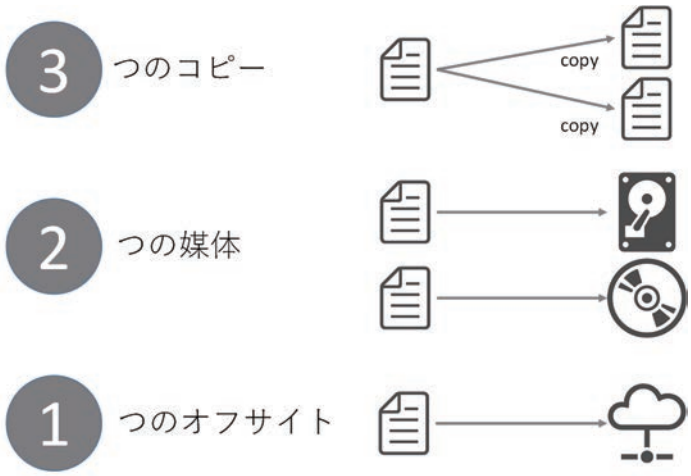


図 1：3-2-1 ルール

出典：大和総研作成

3-2-1 ルールが注目される背景

このルールは前述のとおり 10 年以上も前に公表されたものですが、このルールがあらためて注目されている背景には猛威を振るっているランサムウェアがあげられます。ランサムウェアは PC やサーバーに感染し、業務データを暗号化します。そして、ランサムウェアを仕掛けた攻撃者は暗号化されたデータを元に戻す対価として金銭を要求してきます。

(*1) US-CERT『Data Backup Options』（https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf）

ここで鍵となる対策がバックアップです。バックアップがあれば金銭を攻撃者に差し出す必要もなく、暗号化される前の状態にデータを復元できます。しかし、バックアップを取得していても暗号化される前のデータを復元できなかったケースが相次いでいます。

警察庁が 2022 年 9 月に公表した『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』(*1)によると被害企業・団体等に対するアンケート調査の結果、86%の企業・団体等でバックアップを取得していたものの、78%の企業・団体等がバックアップから復元できなかったと回答しています。復元できなかった詳しい理由については明らかにされていませんが、バックアップデータも含めて暗号化されてしまった可能性が考えられます。

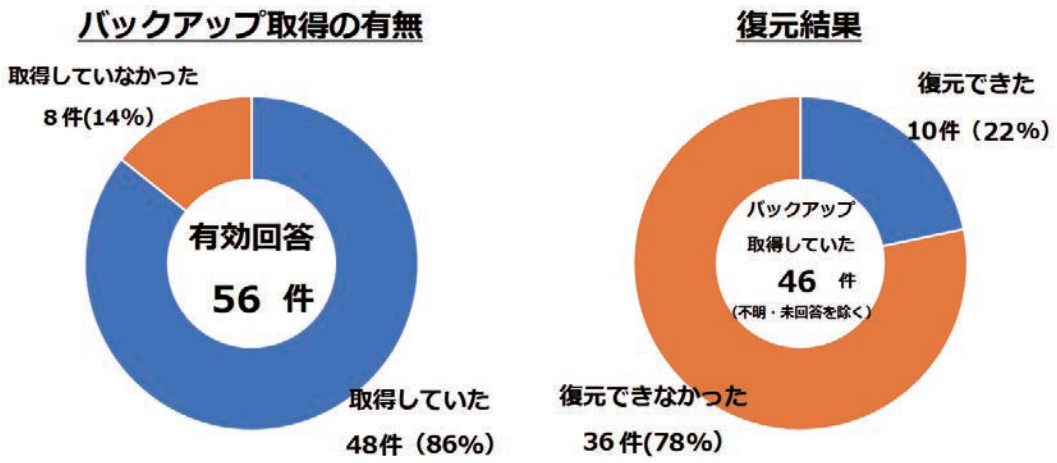


図 2：被害企業・団体等のバックアップの取得・活用状況

出典：警察庁『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』

ランサムウェア対策としては不十分

したがって単にバックアップを取得すれば良いのではなく、前述の「3-2-1 ルール」にしたがって適切にバックアップを取得することがますます重要になってきています。しかし一方で、従来の「3-2-1 ルール」にしたがうだけではランサムウェア対策としては不十分になってきています。たとえば、「3-2-1 ルール」にしたがって二つの媒体や一つのオフサイト(*2)でバックアップを保持していたとしてもそれがランサムウェアに感染した PC やサーバーからアクセス可能であれば、バックアップも含めて暗号化されてしまいます。

(*1) https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

(*2) ここでの「オフサイト」とは文字通り離れた場所という意味です。オフィスから離れた場所にあるオフサイトバックアップでもオフィスにある PC やサーバーとネットワークでつながっている場合もあります。

ランサムウェア対策としてのバックアップ最新動向

有効なランサムウェア対策としては、業務システムとは完全に切り離されたオフラインのバックアップを保持することです。ただし、オフラインでバックアップを保持することの難点はどうしてもデータ鮮度が落ちてしまうことと、データの復元に要する時間が長くなりがちであるということです。

そこでその他の有効なランサムウェア対策として、ストレージベンダーやクラウドベンダーの多くが提供する「WORM ストレージ」（不変ストレージ）を利用することがあげられます。クラウドベンダーによってはオブジェクトロック機能と呼んでいる場合もあります。

WORM とは Write Once Read Many の頭文字をつなげた略語で、文字通り一度データを書き込んだらそのデータは何度も読み取りができるが二度と変更ができないような機能のことを指します。WORM ストレージ（不変ストレージ）にバックアップデータを保存すれば、このデータをランサムウェアが暗号化しようとしても暗号化できません。なお、クラウドベンダーがストレージサービスにおいてこのような WORM 機能を提供する場合、基本的には標準機能であり、WORM 機能自体は追加料金不要で利用可能であることが多いです。

またバックアップソリューションベンダーも進化してきており、OS（オペレーティングシステム）が認識できない独自プロトコルを用いてバックアップを取得する製品やストレージの使用量などを監視してランサムウェア攻撃を検知できる製品も一般的になりつつあります。さらに近年は SaaS アプリケーションの利用が一般的になっていることから、オンプレミスのデータだけでなく SaaS アプリケーションのデータも統合的にバックアップできる製品も増えています。

最後に

以上述べてきたようにバックアップを取得することはとても大切なことですが、実際のランサムウェア被害発生時にバックアップからデータをリストア（復元）できなければ意味がありません。バックアップは日々取得しているが実はリストア手順が整備されていない、あるいはそのリストア手順を一度も実行したことがないというようではリストア時間が長引く恐れや、最悪の場合、リストアできないかもしれません。日ごろからセキュリティインシデント対応訓練の一環としてバックアップからのリストア訓練も実施しておくことが重要です。

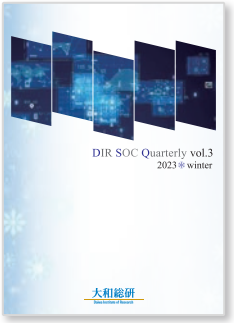
バックナンバーはこちら

DIR SOC Quarterly 2022 the first issue （2022 年 9 月 29 日発行）

https://www.dir.co.jp/publicity/publication/socquarterly2210.html

DIR SOC Quarterly 2022 vol.2 （2022 年 11 月 21 日発行）

https://www.dir.co.jp/publicity/publication/socquarterly2211.html



DIR SOC Quarterly vol.3 2023 winter （2023 年 1 月 30 日発行）

https://www.dir.co.jp/publicity/publication/socquarterly2301.html

DIR SOC Quarterly vol.4 2023 spring
2023 年 4 月 7 日発行

著者　大和総研
発行所　株式会社大和総研　フロンティア研究開発センター
印刷・製本　セキ株式会社

お問い合わせ先　https://www.dir.co.jp/contact/solution/input.php

大和総研が運営する、AI・データサイエンスなど先端技術に特化した用語解説サイト「WORLD」（ワード）を開設しました。

大和総研の用語解説サイト

WORLD

キーワードから、みえる、つながる、未来の日常（Life）

「WORLD」（ワード）は、大和総研が運営する、AI・データサイエンスなど先端技術に特化した用語解説サイトです。
大和総研にはシステム、リサーチ、コンサルティング分野のスペシャリストが連携して、多くのお客様の幅広いニーズに応えてきた実績があります。用語解説サイト「WORLD」では、大和総研がこれまでに培ってきた豊富な経験をもとに、未来を築く新ソリューション創出の礎となる情報を、わかりやすく、深くご紹介していきます。
大和総研は先端テクノロジーやAI・データサイエンス技術を駆使し、デジタル社会を牽引するビジネスパートナーであり続けます。

CONTENTS

キーワードから　旬のIT用語が一目でわかるトレンドワードクラウド

国内約50のIT関連ニュースサイトで掲載された記事の中から、トレンドのワードをピックアップして視覚化。今押さえるべきIT用語が一目でわかるトレンドワードクラウドです。

みえる　AI・データサイエンスなど4分野の用語を解説

よく耳にする頻出用語から最新の用語まで、先端技術の研究・開発を通じてテクノロジーの可能性を追求しつづける大和総研の知見を活かした用語解説ページです。

解説用語例

AI・データサイエンス	セキュリティ	IT全般	ブロックチェーン
●MLOps	●eKYC	●マルチクラウド	●暗号資産（仮想通貨）
●マルチモーダルAI	●ゼロトラスト	●データマネジメントプラットフォーム	●セキュリティ・トークン・オファリング（STO）
●ニューラルネットワーク		●ノーコード開発/ローコード開発	

つながる　IT技術とビジネスをつなぐ深掘り解説

ビジネスでの活用が見込まれる技術を深掘り。技術発展の背景、関連技術の紹介や導入における注意点など、未来を築く新ソリューション創出の礎となる情報をわかりやすく解説します。

大和総研の用語解説サイト
WORLD

https://www.dir.co.jp/world/

大和総研
Daiwa Institute of Research