サイバーセキュリティレポート

2025.03

NTT セキュリティ・ジャパン株式会社
プロフェッショナルサービス部　OSINT モニタリングチーム

目次

【1 ページサマリー】

当レポートでは 2025 年 3 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『山形銀行に偽装した「ビッシング」による被害』

- 2024 年秋から、電話音声を使用したフィッシングである、「ビッシング」（ボイスフィッシングの略）による法人向けネットバンキング口座の不正送金被害が急増している。2025 年 3 月には山形県において、山形銀行に偽装したビッシングにより複数の企業で不正送金被害が発生した。
- 自動音声でかかってきた電話から、ネットバンキングに偽装したフィッシングサイトにアクセスするよう誘導するといった手口が確認されている。
- 山形県での被害発生以降も、このようなビッシングは全国の都道府県で続いている。企業は多額の損失を防止するため、銀行を名乗る自動音声電話に応じないといった、慎重な対応をするための手順を定めてネットバンキング担当者に周知することが急務である。

第 2 章『セキュリティ要件適合評価及びラベリング制度（JC-STAR）」の運用開始』

- 経済産業省および独立行政法人情報処理推進機構（IPA)は、IoT (Internet of Things)製品のセキュリティレベルを可視化する制度として、「セキュリティ要件適合評価及びラベリング制度（JC-STAR)」の運用を開始した。
- 製品を利用する企業は、本体やパッケージに掲示された JC-STAR のラベルを確認することで、客観的なセキュリティ水準を満たした製品を選定できるようなる。
- IoT 製品の導入にあたっては、自社でのガイドラインの策定やリスク分析を行い、セキュリティパッチの適用など適切な運用管理が求められる。

第 3 章『未成年者によるサイバー犯罪』

- 不正に入手した ID とパスワードで楽天モバイルのサーバーにアクセスし、通信回線の新規契約をしたとして、警視庁は中高生 3 人を逮捕した。この事件では、「ChatGPT」で自作した犯罪用のプログラムをハッキング活動に使い、約 750 万円相当の暗号資産を得ていた。
- 他にも、岩手県の男子高校生が他人になりすまして携帯電話の回線を追加で契約したとして逮捕された事件も発生している。高校生はその回線を使い、ライブ配信サービスで不正を行っていた。
- 昨年度の不正アクセス禁止法違反の検挙者のうち、10 代は 3 割近くを占める。未成年者がサイバー犯罪に走る主な動機には、金銭獲得以外に技術的な好奇心からの腕試しもあるとみられている。

1. 山形銀行に偽装した「ビッシング」による被害

1.1. 概要

ビッシング(Vishing) はボイスフィッシング (Voice Phishing)の略で[1]、電話等での音声のやり取りで行われるフィッシング攻撃である[2]。

最近、日本国内で、ネットバンキング等の利用者を電話音声で巧みにフィッシングサイトに誘導するビッシングが多発している。警察庁の『令和６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』（2025 年３月 13 日発表）[3]によれば、2024 年秋から、ビッシングによる法人向けネットバンキング口座の不正送金被害が急増している。2025 年３月には、山形銀行に偽装したビッシングが複数の組織に対し行われ、１企業だけで約１億円もの被害が発生したことが明らかになった。

1.2. 山形銀行を装ったビッシング

【山形銀行を装ったビッシングの手口】 [4,5]

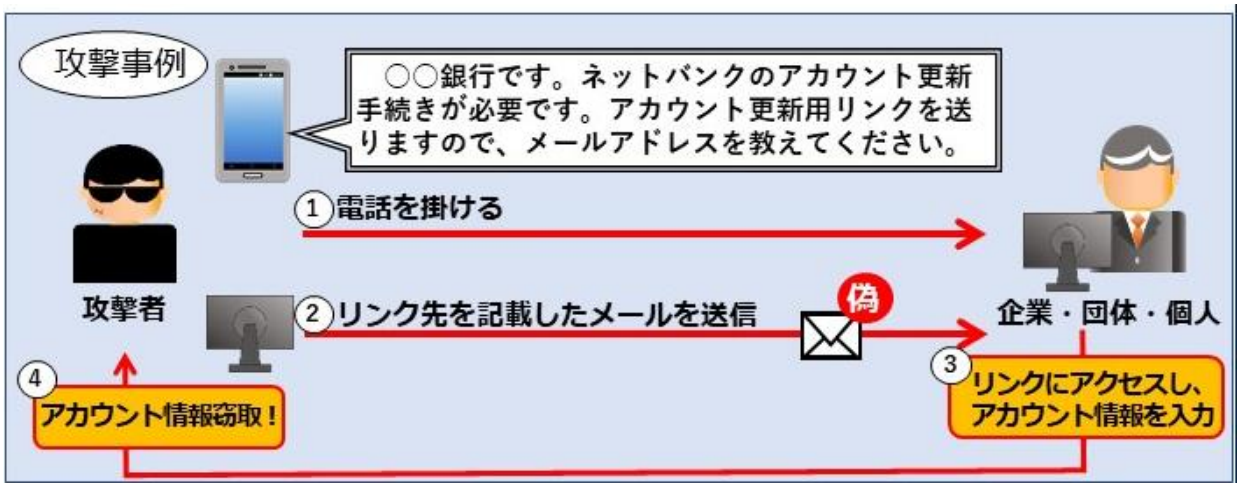

図 1 山形銀行を装ったビッシングの流れ
（隣県の秋田県警察の注意喚起より）[6]

---

[1] 出典：Proofpoint『用語集 ビッシングとは？』
https://www.proofpoint.com/jp/threat-reference/vishing

[2] 出典：警察庁『サイバー警察局便り R6Vol.15「今、企業の資産（法人口座）がねらわれている！！」』
https://www.npa.go.jp/bureau/cyber/pdf/R6_Vol.15cpal.pdf

[3] 出典：警察庁『令和６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/R6/R06_cyber_jousei.pdf

[4] 出典：朝日新聞『山形銀行かたる不正送金詐欺、山形鉄道が１億円被害　不審電話相次ぐ』
https://www.asahi.com/articles/AST3D3H8MT3DUZHB003M.html

[5] 出典：山形銀行『当行を騙る「ボイスフィッシング」による不正送金に関する注意喚起について』
https://www.yamagatabank.co.jp/release/pdf/20250310.pdf

[6] 出典：X『@AkitaCyber_Info』
https://x.com/AkitaCyber_Info/status/1902269013084033484

山形県内では 3 月 10 日に集中してビッシングが発生した[7]。山形県の地銀である山形銀行のネットバンキングのサポートを装った、企業を狙った自動音声の電話が複数確認された。国際電話による発信もあったとみられている。また、企業が公表していない電話番号への着信も確認されている[8]。

この自動音声では法人向けネットバンキングについて、「契約者情報の更新が必要」といった要求がアナウンスされる。電話に応答すると、対応が銀行員になりすました攻撃者に替わる。攻撃者は電話でメールアドレスを聞き出して、フィッシングサイトの URL が記載されたメールを企業のネットバンキング担当者に送る。担当者が、誘導されたフィッシングサイトでネットバンキングの認証情報を入力すると、ワンタイムパスワードの詐取も行われ、ネットバンキングの不正利用がリアルタイムで進められる。これにより、攻撃者は自らの口座へと不正送金を行うとみられている。

【明らかになった被害】[9]

一連の山形銀行等に偽装したビッシングでは、山形県内で複数の組織が被害に遭ったと発表されており、被害総額は合計で数億円とみられている。中でも、第三セクターのフラワー長井線を運行する山形鉄道は 3 月 12 日、約 1 億円の被害に遭ったと発表した。これには、老朽化した信号施設の更新のために自治体から受けていた交付金も含まれていた。

被害発生を受け山形銀行は 3 月 10 日、法人インターネットバンキングサービスでの、他行に宛てた即時振込の停止を発表した[10]。

【各地で続くビッシング】

地方銀行に偽装したビッシングは、日本各地で続いている。3 月末には埼玉県の武蔵野銀行への偽装、4 月には沖縄県の琉球銀行、徳島県の阿波銀行、茨城県の筑波銀行への偽装による、法人向けインターネットバンキングを狙ったビッシングが確認されている。その被害は億円単位とみられている[11]。

1.3. まとめ

山形銀行に偽装したビッシングの電話では自動音声が使われていた。自動音声はネットバンキングでよく使われており、受けた側も違和感が少ないことから、今回の詐欺でも使われたと考えられる。

各企業は、ビッシングによる多額の損失を防止するため、セキュリティ対策強化の指示を、ネットバンキング担当者に行う必要がある。まず、銀行を名乗る自動音声電話には対応しないよう周知する。また自動音声に限らず、銀行等から口座に関する電話があった際には、真偽を確認するため銀行の代表電話番号へ問い合わせるよう定める。[12]

---

[7] 出典：読売新聞『山形鉄道、フィッシング詐欺で 1 億円被害…山形銀行かたる自動音声電話で偽サイトに誘導』
https://www.yomiuri.co.jp/national/20250312-OYT1T50149/

[8] 出典：NHK『山形 NEWS WEB「山形鉄道 被害の約 1 億円には新しい信号機システム導入費も」』
https://www3.nhk.or.jp/lnews/yamagata/20250312/6020023443.html

[9] 出典：NHK『山形 NEWS WEB「山形鉄道 被害の約 1 億円には新しい信号機システム導入費も」』
https://www3.nhk.or.jp/lnews/yamagata/20250312/6020023443.html

[10] 出典：山形銀行『当行を騙る「ボイスフィッシング」による不正送金に関する注意喚起について』
https://www.yamagatabank.co.jp/release/pdf/20250310.pdf

[11] 出典：産経ニュース『地銀装う「ボイスフィッシング詐欺」各地で猛威 企業口座狙い電話、億単位の実害も』
https://www.sankei.com/article/20250406-UZ3MAQYR4JJ7NLUQZ57O2O23BA/

[12] 出典：警察庁『サイバー警察局便り R6Vol.15「今、企業の資産（法人口座）がねらわれている！！」』
https://www.npa.go.jp/bureau/cyber/pdf/R6_Vol.15cpal.pdf

攻撃者は企業のインターネットバンキング担当者をフィッシングサイトへ誘導しようと狙っている。今回の地方銀行に偽装したビッシングはその一種であり、今後、ビッシングの成功率が下がったとしても、他の様々な方法で狙い続けるものと考えられる。突然の攻撃に動じない、慎重な対応をするための手順を定めて周知することが急務である。

2.「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」の運用開始

2024 年 3 月 25 日、経済産業省および独立行政法人情報処理推進機構（IPA）は、IoT (Internet of Things)製品のセキュリティレベルを可視化する制度として、「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」の運用を開始した[13]。製品を利用する企業は、本体やパッケージに掲示された JC-STAR のラベルを確認することで、客観的なセキュリティ水準を満たした製品を選定できるようになる。

本章では、JC-STAR の概要を整理し、制度導入の背景となる IoT 製品のセキュリティ課題について述べる。

2.1.「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」について

ルーターやネットワークカメラなどの IoT 製品は 2030 年までに 320 億台に達すると見込まれる一方[14]、IoT 製品を狙ったサイバー攻撃が急増している[15]。このような中、「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」は、セキュリティ対策が講じられた IoT 製品が広まる仕組みの構築を目指したものである。

図 2 JC-STAR のロゴ

JC-STAR では、下表のような★1~4 (レベル 1~4)の 4 段階のレベルでラベルが付与され、数値が高いほど高度なセキュリティ要件が求められる[16]。

レベル	基準概要	評価手順
★1	IoT 製品共通の最低限の適合基準を満たす	IoT ベンダーによる自己宣言
★2	製品類型ごとの特徴に対応する基本的な適合基準を満たす	
★3	政府機関、重要インフラ事業者、大企業の重要なシステムでの利用を想定した製品類型ごとの特徴に対応する汎用的な適合基準を満たす	第三者評価機関による評価
★4		

[13] 出典：経済産業省『IoT 製品に対するセキュリティラベリング制度（JC-STAR）の運用を開始しました』
https://www.meti.go.jp/press/2024/03/20250325007/20250325007.html

[14] 出典：Statista『Number of Internet of Things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2033』
https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[15] 出典：SonicWall『2025 Cyber Threat Report: The Need For Speed and Strong Allies to Overcome the Cybersecurity Battlefield』
https://www.sonicwall.com/resources/white-papers/2025-sonicwall-cyber-threat-report

[16] 出典：経済産業省『IoT 製品に対するセキュリティ適合性評価制度構築方針』
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20240823_1.pdf

2025 年 3 月時点では★1 のみ申請受付が開始しており、★2 以上は 2026 年 1 月以降の受付を予定している。ラベルを付与された IoT 製品には「適合ラベル」が発行され、製品やそのパッケージ等に掲示することができる。

IoT 製品の購入者・調達者は、適合ラベルを確認することで、客観的なセキュリティ水準を満たした製品を選定できるようになる。

図 3 適合ラベル（イメージ）

2.2. IoT 製品のセキュリティ課題

【運用におけるセキュリティ課題】

このようなセキュリティ水準が設定される背景として、IoT 製品が性能などの制約から、強固なセキュリティ機能を有さないものが多く、ID とパスワードだけの弱い認証方式しか備えないものもあることが挙げられる。

また、IoT 製品は様々な方法でネットワークに接続できることから、組織として設置場所や台数を把握することが難しく、シャドーIT の温床となったり、セキュリティパッチの適用を管理できなかったりすることがある。さらに、IoT 製品は長いライフサイクルで利用されることが多く、セキュリティパッチがリリースされなくなった後も利用されている場合がある。

このような弱い認証や放置された脆弱性を突かれることで、IoT 製品がマルウェア感染や DDoS 攻撃の踏み台[17]になったり、侵入経路[18]として悪用されたりする被害が多数発生している。

IoT 製品には、一般の PC のようにエンドポイントセキュリティ製品を導入することが難しいため、IT 資産の管理、ログの収集、ネットワークの監視など間接的に管理する方法が推奨されている[19]。加えて、JC-STAR に準拠することで、単体でもマルウェアの感染や外部からの侵入に対して強固になり、サポート期間が明示されることで新機種への交換計画が立てやすくなるなどの改善が見込まれる。

【サプライチェーンにおけるセキュリティ課題】

ここまでの IoT 製品の運用上の課題に加えて、製造ライン、流通経路、アップデート配布時などサプライチェーンの上流から下流までの間に、ソフトウェアコンポーネントに対する悪意のある改ざん、不正なコードの埋め込みなどが発生する恐れもある。

製造ラインや流通経路での改ざんにつながる恐れがあった事例として、2025 年 3 月 6 日に明らかになった、中国の半導体

[17] 出典：トレンドマイクロ『2024 年末からの DDoS 攻撃被害と関連性が疑われる IoT ボットネットの大規模な活動を観測』
https://www.trendmicro.com/ja_jp/research/24/l/iot-botnet-activity-ddos-attacks.html

[18] 出典：トレンドマイクロ『Raspberry Pi から侵入 ～NASA の事例から学ぶ IoT 時代のセキュリティ～』
https://www.trendmicro.com/ja_jp/research/19/f/breaking-through-raspberrypi.html

[19] 出典：総務省『IoT セキュリティガイドライン ver 1.0』
https://www.soumu.go.jp/main_content/000428393.pdf

メーカ Espressif Systems が製造するマイクロコントローラー「ESP32」の隠しコマンド[20]の問題が挙げられる。

同マイクロコントローラーは、Wi-Fi と Bluetooth の接続機能を提供している[21]。2023 年時点で累計 10 億個以上の出荷実績があり、様々な IoT 製品に組み込まれている[22]。物理的なアクセスが可能な状態で同マイクロコントローラーの隠しコマンドを悪用すると、信頼されたデバイスへのなりすまし、機密情報の窃取、ネットワーク内の他のデバイスへの攻撃などが可能となる。

3 月 8 日、これらの隠しコマンドは脆弱性 CVE-2025-27840 として登録され、製造元の Espressif Systems はこれらの隠しコマンドについて、開発用のコマンドであるとし、将来的に無効化するパッチを提供する方針であることを発表した[23]。

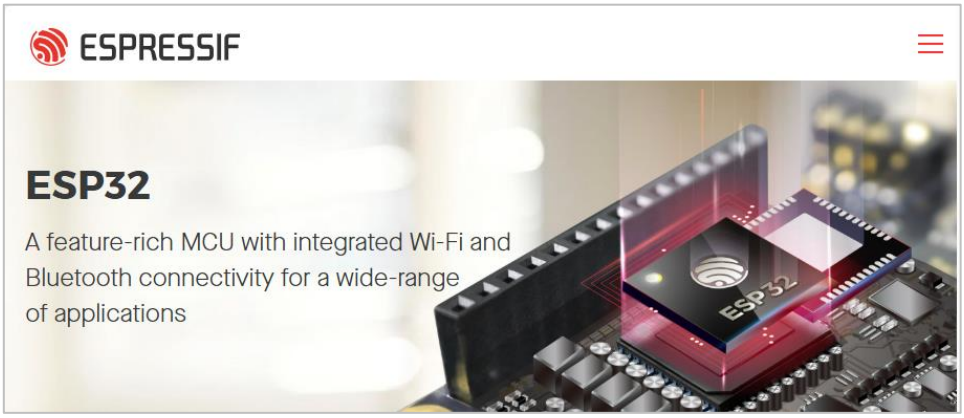

図 4 ESP32 の製品イメージ

このようなサプライチェーンの問題は、IoT 製品を利用する企業だけで対応するのは難しい。製品を製造する企業が、JC-STAR のような評価基準を満たした製品を生産・販売・サポートし、評価基準を満たした製品が市場競争力を生むことが期待される。

2.3. まとめ

利用増加が見込まれる IoT 製品は、今後もサイバー攻撃の格好の標的となり得る。IoT 製品の導入にあたっては、自社でのガイドラインの策定やリスク分析を行い、セキュリティパッチの適用など適切な運用管理が求められる。

加えて、事前に信頼できるベンダー・調達先を選定することも必要である。JC-STAR のような制度を活用して、調達時のセキュリティ要件を整理し、選定の基準を設けることを推奨する。

---

[20] 出典：Tarlogic『Tarlogic detects a hidden feature in the mass-market ESP32 chip that could infect millions of IoT devices』
https://www.tarlogic.com/news/hidden-feature-esp32-chip-infect-ot-devices/

[21] 出典：Espressif Systems『ESP32』
https://www.espressif.com/en/products/socs/esp32

[22] 出典：Espressif Systems『Espressif Leads the IoT Chip Market with Over 1 Billion Shipments Worldwide』
https://www.espressif.com/en/news/1_Billion_Chip_Sales

[23] 出典：Espressif Systems『Espressif's Response to Claimed Backdoor and Undocumented Commands in ESP32 Bluetooth Stack』
https://www.espressif.com/en/news/Response_ESP32_Bluetooth

3. 未成年者によるサイバー犯罪

3.1. 概要

未成年者によるサイバー犯罪への関与の増加が懸念されている。不正に入手した他人の ID とパスワードで楽天モバイルのサーバーにアクセスし、通信回線を新規に契約したとして、2 月 27 日に岐阜、滋賀、東京の中高生 3 人が逮捕された[24]。また、3 月 11 日には、岩手の 15 歳の高校生が不正に回線を契約し、その回線を使ったライブ配信で自らへ投げ銭を行って利益を得たとして逮捕されている[25]。

このような、未成年者による類似の犯罪は後を絶たない。昨年度の不正アクセス禁止法違反の検挙者のうち、3 割近くを 10 代が占めていた。未成年者によるサイバー犯罪は以前からあったが、生成 AI 等の最新技術により犯罪のハードルが下がり、中高生が多額の金銭を得るという事件が増えている[26]。

3.2. 楽天モバイルへのハッキング

楽天モバイルのサーバーへのハッキングで 2 月 27 日に逮捕されたのは、オンラインゲーム仲間であった岐阜県大垣市の高校生 1 名と滋賀県米原市と東京都立川市の中学生 2 名である。容疑は、不正アクセス禁止法違反と電子計算機使用詐欺。2023 年 12 月より、彼らは楽天モバイル及び様々な他サービスの ID とパスワードのセット約 33 億件を、通信アプリ「テレグラム」で知り合った人物から購入した。その中から、大垣市の高校生が楽天モバイルの ID とパスワードを抽出し、同サービスのシステムに不正なログインを行った。この高校生は、回線契約を機械的に行うプログラムを ChatGPT で自作しており、これを使用して昨年 5 ～ 8 月の間に計 105 回線を契約した疑いが持たれている。高校生は、「犯罪スキームを考案して注目を集めたかった」などと供述しているという[27]。

楽天モバイルでは、最初の回線契約以降 15 回線までは本人確認が不要であるため、同サービスは狙いやすかったとみられる[28]。3 人はテレグラムを通じて不正に契約した回線を犯罪グループに転売し、約 750 万円相当の暗号資産を手に入れていた。これをゲームやオンラインカジノ等に使ったとされる。

後に、大垣市の高校生と立川市の中学生は、米国の違法サイトから約 1 万 1000 件のクレジットカード情報を入手し、不正に契約した回線でゲーム機等、約 350 万円分の買い物をした疑いで、3 月 18 日に再逮捕された[29]。

---

[24] 出典：読売新聞オンライン『楽天モバイルへの不正ログイン容疑で中高生３人逮捕、他人のＩＤ・パスワード３３億件購入か』
https://www.yomiuri.co.jp/national/20250227-OYT1T50083/

[25] 出典：岩手日報『不正に回線契約疑い、北上の高校生を逮捕　他人名義で投げ銭』
https://www.iwate-np.co.jp/article/2025/3/11/181207（公開終了記事、3 月 19 日閲覧）

[26] 出典：総務省『不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況』
https://www.soumu.go.jp/main_content/000997024.pdf

[27] 出典：朝日新聞『ID･PW 入手し AI 悪用　楽天に不正アクセス容疑で少年 3 人逮捕』
https://www.asahi.com/articles/AST2W3PLJT2WUEFT00KM.html

[28] 出典：毎日新聞『楽天モバイル回線を不正契約疑い　17 歳逮捕　売却金で中傷活動か』
https://mainichi.jp/articles/20250321/k00/00m/040/287000c（公開終了記事、3 月 23 日閲覧）

[29] 出典：読売新聞オンライン『楽天モバイル不正接続、中高生２人を再逮捕…他人の通信回線と１万件のクレカ情報でスマホなど購入か』
https://www.yomiuri.co.jp/national/20250318-OYT1T50074/

図 5 押収されたスマートフォンやパソコンなど[30]

3.3. 岩手の 15 歳少年が不正に回線契約、自らへ投げ銭

未成年者のサイバー犯罪の事例としては、3 月 11 日、岩手県北上市の男子高校生が電子計算機使用詐欺の疑いで逮捕された事件もあった。この高校生は、昨年 5 月に SNS を通じて、携帯電話を契約するための QR コードを不正に入手し、他人になりすまして回線を追加契約した。高校生はその回線を使い、何らかの方法で得たとみられる約 100 万円相当の金銭を、ライブ配信サービスでの「投げ銭」により自分自身に対して送金していた。投げ銭とはライブ配信者を応援するため、視聴者が配信者に金銭等を送る機能で、YouTube の「スーパーチャット（スパチャ）」、TikTok の「LIVE Gifting」等がこれに当たる。他者ではなく自身へ投げ銭をしたのは、資金洗浄を狙ったものとみられている。高校生は、100 万円から配信サービス手数料が差し引かれた約 50 万円を手に入れていた。逮捕に関連して押収されたスマートフォンには、不正に入手した ID やパスワードが 3 万件以上、QR コードは数百件含まれていた[31, 32]。

3.4. 未成年者によるサイバー犯罪

昨年（令和 6 年）は 259 人が、他人の ID やパスワードを使ってサーバーにログインする「不正アクセス禁止法」違反により検挙された。そのうち 10 代の検挙者は、20 代の次に多い 72 人となっている[33]。

---

[30] 出典：X『@MPD_yokushi』
https://x.com/MPD_yokushi/status/1896468400362439040

[31] 出典：岩手日報『不正に回線契約疑い、北上の高校生を逮捕　他人名義で投げ銭』
https://www.iwate-np.co.jp/article/2025/3/11/181207（公開終了記事、3 月 15 日閲覧）

[32] 出典：ロケットボーイズ『岩手県の高校生、他人名義で回線契約し「投げ銭」で逮捕』
https://rocket-boys.co.jp/security-measures-lab/iwate-highschool-student-arrested-fraudulent-contract/

[33] 出典：総務省『不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況』
https://www.soumu.go.jp/main_content/000997024.pdf

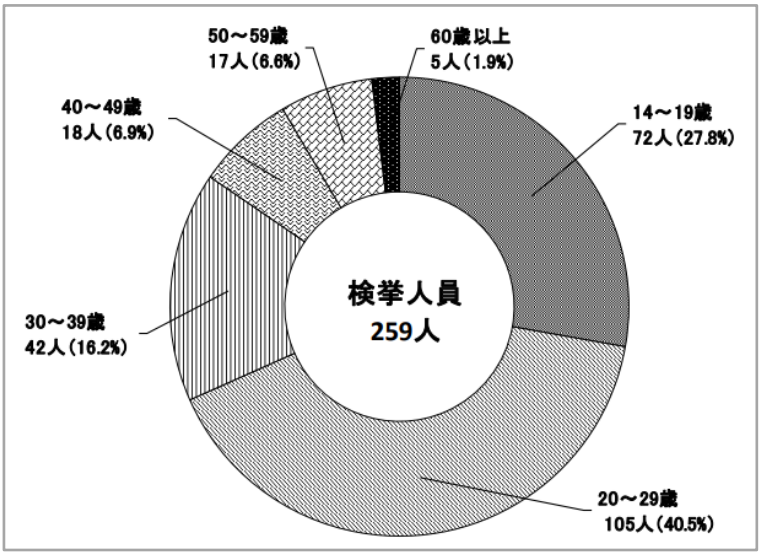

図 6 不正アクセス禁止法違反事件の年齢別被疑者数（令和６年 [警察庁資料より]）[34]

犯行手口は SNS（コミュニティサイト）やショッピングサイト等でのパスワードの管理や設定の甘さを利用した不正アクセスが多い[35]。警察庁は被害を防ぐため、簡単なパスワードの設定や使いまわしをしないよう注意を呼び掛けている。

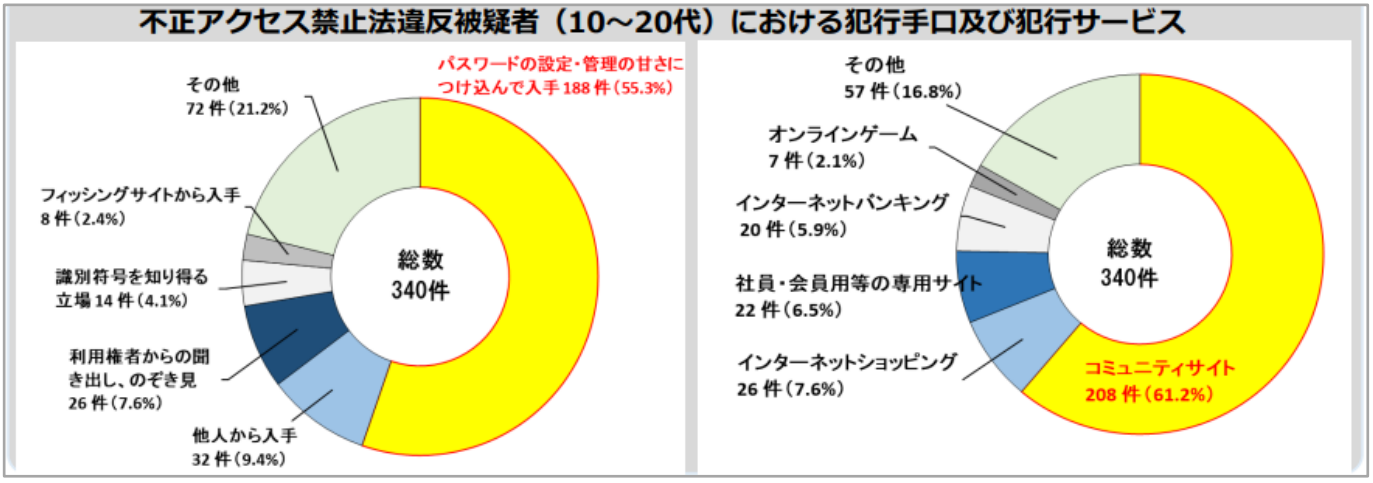

図 7 不正アクセス禁止法違反被疑者（10～20 代）における犯行手口及び犯行サービス（令和 5 年 [警察庁資料より]）[36]

【海外での事例】

海外では、未成年者がサイバー攻撃に関与する事例はより多く見られ、以前から課題となっている。

---

[34] 出典：総務省『不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況』
https://www.soumu.go.jp/main_content/000997024.pdf

[35] 出典：朝日新聞『不正アクセス摘発最多 259 人 他人の SNS ログイン、学生目立つ』
https://www.asahi.com/articles/AST3D3SFHT3DUTIL026M.html

[36] 出典：警察庁『サイバー警察庁便り R6(2024) Vol.13「サイバー犯罪（不正アクセス）行為者の実態」』
https://www.npa.go.jp/bureau/cyber/pdf/R6_Vol.13cpal.pdf

例えば 2018 年には、オーストラリアの 13 歳の少年が、Apple 社のネットワークをハッキングし、90GB の内部ファイルをダウンロードした事件があった[37]。

2023 年 7 月には、DDoS 攻撃を請け負う闇サイトの運営者が米英の法執行機関の協働により摘発された。当該サイトの利用者約 3800 名の多くは未成年者であり、彼らはゲーム感覚で DDoS 攻撃を行っていた[38]。この事件は、サイバー犯罪の軽減のため、未成年者へ適切な対策を講じることの重要性を、国を越えて認識するきっかけのひとつとなった。

3.5. まとめ

未成年者のサイバー犯罪の多くはいたずらレベルのものである。しかし、取り締まりが行われた最近の事案からは、生成 AI やサイバー犯罪の分業化によって、高度な攻撃が比較的容易に実現できるようになっている状況が示された。犯罪に関する情報は動画、SNS など若年層がアクセスしやすい形で蓄積されており、未成年者のサイバー犯罪は今後も増え、高度化する恐れがある。また、ICT 教育の整備が進んだ反面、若年層でサイバー犯罪に転用可能な技術力が強化されている可能性も考えられる。情報モラル教育もそれ以上に強化することが新たな犯罪者を生み出さないために必要と考える。

以上

[37] 出典：BBC『Apple files stored by teen in 'hacky hack hack' folder』
https://www.bbc.com/news/technology-45219895

[38] 出典：日本経済新聞『サイバー攻撃に酔う「未成年者」たち、国際連携で抑止へ』
https://www.nikkei.com/article/DGXZQOUE229HX0S4A820C2000000/

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

お問い合わせ先：NTT セキュリティ・ジャパン株式会社

プロフェッショナルサービス部　OSINT モニタリングチーム
メールアドレス：nsj-co-osint-monitoring@security.ntt