セキュリティフォーラム2025
JSSEC利用部会成果発表

フィッシング＆フェイク！
実体験に基づいた解説ガイドリリースについて

2025年 2月18日（火）

一般社団法人　日本スマートフォンセキュリティ協会
利用部会 部会長　　兼　利用ガイドラインWGリーダー
松下 綾子（ALSIアルプスシステムインテグレーション）

JSSECとは？

一般社団法人 日本スマートフォンセキュリティ協会

略称：JSSEC＝じぇいせっく

代表理事・会長　佐々木 良一

（東京電機大学 名誉教授 兼 サイバーセキュリティ研究所 客員教授）

スマートフォンの**安全な利活用を図り普及を促進**するために、
2011年5月に任意団体としてスタート
2012年4月より一般社団法人として活動
その他、**IoTやICTの安心安全な**普及啓発活動

JSSEC が目指すもの

スマートフォンは社会のさまざまな場所において利活用が進んでおり、今や社会と人をつなぐ有用な役割を果たしています。
IoT（モノのインターネット）の拡大により、従来では考えられなかったあらゆる「モノ」がインターネットに繋がる世界となり、さらに社会を変革しようとしています。その**社会と人の接点になるのが、スマートフォンなどのスマートデバイス**です。JSSECは、この人との接点となるスマートフォンなどを中心に、この新たな社会での更なるセキュリティの重要性について普及啓発してまいります。

利用部会　活動紹介

部会紹介：目的と目指す成果

利用部会	**利用者視点**の活動	安心・安全なスマートフォン利用のために情報収集と課題を整理し、情報発信を行う。 又、**近年のスマートフォン利用形態の変化に合わせ、たとえば、IoTの導入など利用企業の共通的 な経営課題を中心にテーマを選定**し、利用事例の調査や新しい技術の調査・研究の成果 を発信する。
技術部会	**提供者視点**の活動	スマートフォンを安全に利用するための**技術的な調査・研究・議論**を行う。 具体的には4ワークグループで構成し成果物を公開する事で、日本におけるスマートフォン利用の安全性向上に寄与する。
啓発事業部会	**学生への啓発**活動	JSSECが**スマートフォンの安全利用を推進し広く社会に貢献**するため、積極的に啓発活動展開を行うことを目的とする。 特に、中高生など学生向けの啓発活動に注力する。
ＰＲ部会	JSSECの**PR活動**	JSSECが行うすべての活動について**普及啓発するための情報配信**を行う。 例）・メディア対応/各種成果物、JSSEC活動に関する情報配信 ・イベント・セミナーの企画・運営 ・他団体との連携

利用部会体制

部会体制

部会長　　：松下　綾子　（ALSI/アルプスシステムインテグレーション株式会社）
副部会長　：北村　裕司　（サイバートラスト株式会社）
副部会長　：本間　輝彰　（KDDI株式会社）

■WG体制

利用ガイドライン　ＷＧリーダー：松下　綾子 (アルプスシステムインテグレーション株式会社) 兼務
　　サブリーダー：本間　輝彰 (KDDI株式会社) 兼務

IoT事例研究　　ＷＧリーダー：中村　丈洋 (株式会社SHIFT SECURITY)

利用ガイドラインWG

JAPAN SMARTPHONE SECURITY ASSOCIATION

活動成果物

① スマートフォンやタブレットを組織で利用する際の留意点をまとめた、ガイドラインとチェックシートⅠ作成

① 対策チェックシートⅡの作成と啓発活動

利用ガイドライン本体のダウンロードはこちら

対策チェックシートⅡのダウンロードはこちら

■ **「対策チェクシートⅡ」とは？　～2021年6月発行～**

「スマートフォン＆タブレット（以下スマートフォン）の業務利用に関するセキュリティガイドライン【第二版】」（2014年3月）巻末に付属の 「特性別／利用シーン別対策チェックシート」について、昨今の社会情勢を考慮しつつ、NIST-CSFに合わせて再検討したチェックシート。

■ **特長**

① スマートフォンの導入・運用・利用停止の各段階における、セキュリティの考慮点を集約。項目は、「50」で簡潔！すぐ読める！

② NIST-CSFの分類で網羅的にチェック可能！
(5機能：識別/防御/検知/対応/復旧)

③ 従来チェックシートの不足項目を追加/補充！(テレワークや Webアプリ、クラウドサービス活用の増加、経営層の視点、サプライチェーンへの配慮、等)

④ 用途レベル毎に推奨項目あり！
（簡易的な利用/一般的な社内業務/重要な本業ビジネス）

⑤ 自社の状況も一覧記入できて、すぐ使える！

IoT-事例研究WG

活動成果物

① IoTセキュリティチェックシート　第2.1版の外部発信、啓発活動

■ **「IoTセキュリティチェックシート 第2.1版」とは？　～2020年2月発行～**

NIST-CSFの分類をベースに、一般企業がIoTを利用（導入）する時、セキュリティ面で考慮すべきことを網羅的にまとめています。「社内IoT導入推進者の検討のベース」、「社内の経営層などへの報告時の指標」、「IoT構築ベンダーとの確認用」などに活用。

JSSECホームページよりダウンロードすることができます。https://www.jssec.org/iot

② 動画セミナー「IoTセキュリティチェックシート入門」

■ **「YouTube」に解説動画をUPしています。**

▶https://www.jssec.org/iot-youtube

第１回　セミナーの構成と受講の進め方
第２回　チェックシートの特長とセキュリティの重要性
第３回　チェック項目「識別」の解説
第４回　チェック項目「防御」の解説
第５回　チェック項目「検知・対応・復旧」の解説
第６回　チェックシートの活用例

IoT-事例研究WG

活動成果物

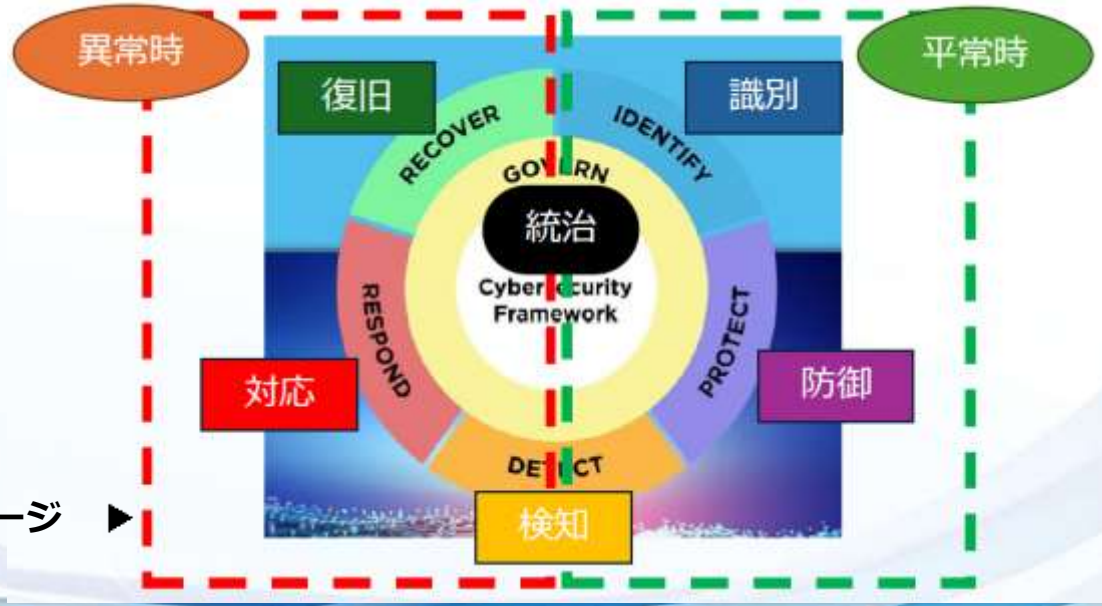
① IoTセキュリティチェックシート　第2.1版の外部発信、啓発活動

■ **「IoTセキュリティチェックシート 第2.1版」とは？　～2020年2月発行～**

NIST-CSFの分類をベースに、一般企業がIoTを利用（導入）する時、セキュリティ面で考慮すべきことを網羅的にまとめています。「社内IoT導入推進者の検討のベース」、「社内の経営層などへの報告時の指標」、「IoT構築ベンダーとの確認用」などに活用。
JSSECホームページよりダウンロードすることができます。https://www.jssec.org/iot

NIST-CSF2.0公開を受け、チェックシート更改に着手

※次ページ参照



NIST-CSF2.0イメージ ▶

IoT-事例研究WG

③IoTセキュリティチェックシート更改

意見交換のためのワークショップを実施（2024年11月、2025年1月）

■ **手順**

・NIST-CSF1.1と２.0を比較しながら、現在のチェックシートを見直すための意見交換を実施。
・チェックシート各項目を見直しつつ、追加修正を行い再分類。

➡2025年度の活動へとつなげていきます。

▼作業シートイメージ①

NIST-CSF1.1と2.0の項目を比較して確認

▼作業シートイメージ②

チェックシート側の項目について分類や追加修正を議論

啓発活動

①コラムによる情報発信

すぐ読めるコラムや資料を作成　➡最新ニュースを発信

▼「iOS18でのパスワード機能強化」（11月）

資料公開「強化された！～ iOS18のパスワード管理」 | JSSEC

▼「QRコード詐欺」（10月）

そのQRコード大丈夫？フードコートで増えるQRコード詐欺（クイッシング）に注意！　～ スマートフォン利用シーンに潜む脅威 Top10 2023 番外編 ～ | JSSEC

②外部との交流・セミナー登壇・取材対応

- **総務省や警察庁、県警等との情報交換（4月～5月）**
- **NHK「あさいち」への取材協力（5月放送済）＋民放も・・・**
- **JAPANSecuritySummit 2024（10月）**
- **JPAAWG 7th General Meeting（11月）**

スマートフォン利用シーンに潜む脅威 Top10

「スマホ利用シーンに潜む脅威 Top10」作成背景

JAPAN SMARTPHONE SECURITY ASSOCIATION

■背景

- 2011年のJSSEC設立以来、スマートフォンはこの10年で幅広く普及
  ※ スマホ所有率（29.3%/2011年→88.6%/2021年）
- ビジネスやコンシューマの生活にとって重要な役割
- 利用者視点でのセキュリティに対して検討を行う中で、JSSEC発足当時に問題視されていた脅威がこの**10年超の月日を経てどのように変化しているか見直す**ことが重要

↓

「スマートフォン利用シーンに潜む脅威 Top10/2023」をワークショップで選定

2019年までの利用部会は、**勉強会＋懇親会**

↓

2020年以降、コロナ禍で中止・・・
2022年度、人の輪と知恵をつなぐ機会を創出したい

2022年・2023年は、ワークショップを中心に活動
「スマートフォンが絡む脅威を選出してみよう」

■ニュースリリースと解説
https://www.jssec.org/news/news20230228.html
https://www.jssec.org/smartphone-use-10threats2023

■ご参考：【利用会活動レポート】
JSSECワークショップ「利用部会が選ぶ5大脅威」作成に向けて
～異業種の方と意見交換する楽しみと気づきが満載～
https://www.jssec.org/column/20221222.html

ワークショップ全体からの考察

■ワークショップ全体からの考察：キーワード

- JSSEC発足当時から問題となっている、フィッシングメールなどによる「**メールを狙った様々な攻撃**」
- ここ数年大きな問題となっている「**スミッシング詐欺**」と、技術の進化によって新たに課題となるであろう「**ディープフェイク**」
- SNSなどの普及で顕著になった問題「**SNSフェイクニュース**」「**誹謗・中傷**」
- コロナ禍による巣籠需要により、ますます増えているネット通販を狙った「**不正通販サイト**」
- もしかしたらあまり知られていない、「**検索エンジンの汚染**」

✶驚異の多くは、その**回避に利用者のリテラシー**が求められる。
利用者一人一人が脅威について十分理解した上で安全に利用する必要がある。
さらには、議論を行っている過程で、**若い世代に対して両親や教育関係者が適切な指導が出来ず、相談すべき相手が友人しかいないという問題も明らか**になった

【参考】ワークショップでの内容は、コラムとして公開
【利用部会活動レポート】 JSSECワークショップ「利用部会が選ぶ5大脅威」　作成に向けて
～異業種の方と意見交換する楽しみと気づきが満載～
https://www.jssec.org/column/20221222.html
【利用部会活動レポート】 JSSECワークショップ「利用部会が選ぶ5大脅威」　作成に向けて 【第2回】
～異業種の方と意見交換する楽しみと気づきが満載（2）～
https://www.jssec.org/column/20230306.html

「スマホ利用シーンに潜む脅威 Top10」

JAPAN SMARTPHONE SECURITY ASSOCIATION

■ワークショップで挙がった脅威一覧

- ■アカウント乗っ取りと誤ったアカウント登録
- ■なりすまし契約とアカウント搾取
- ■スマホカメラの悪用
- ■不正通販サイト
- ■SNS フェイクニュース
- ■短縮 URL 問題
- ■検索エンジンの汚染
- ■メールを狙った様々な攻撃
- ■依然猛威を振るうスミッシング詐欺
- ■アプリストアのマルウェア感染
- ■提供元不明アプリによるマルウェア感染
- ■誹謗・中傷
- ■盗難・紛失
- ■不適切なパスワード管理
- ■ディープフェイク

投票結果

スマートフォン利用シーンに潜む脅威 TOP 10/2023	
第１位	依然猛威を振るうスミッシング詐欺
第２位	なりすまし契約とアカウント詐取
第３位	ディープフェイク
第４位	メールを狙った様々な攻撃 ～フィッシングメール・ビジネスメール詐欺、 ランサムウエアの脅威など～
第５位	提供元不明アプリによるマルウェア感染
第５位	誹謗・中傷
第７位	SNSフェイクニュース
第８位	アカウント乗っ取りと誤ったアカウント登録
第９位	検索エンジンの汚染
第10位	不正通販サイト
ランク外	不適切なパスワード管理
	アプリストアのマルウェア感染
	スマホカメラの悪用
	短縮URL問題
	盗難・紛失

右表の色分けは ➤
同種の脅威を分類したもの

「スマホ利用シーンに潜む脅威 Top10」

JAPAN SMARTPHONE SECURITY ASSOCIATION

依然猛威を振るうスミッシング詐欺

なりすまし契約とアカウント搾取

ディープフェイク

解説ガイド作成

スマートフォンを安全に利用するにあたっては、**技術的対策で100%防ぐことは不可能**であり、利用者一人一人がスマートフォン利用時の**危険性を十分理解し、適切な判断を行うことが重要**。
また、若い世代に対して企業や組織、両親や教育関係者が適切な指導ができず、相談すべき相手が友人しかいないという問題も課題と認識。

- Top10をグループ分け
- 関心の高かった２点をピックアップ
  - 「フィッシング」
  - 「フェイクニュース」

JSSEC会員企業の有志とワークショップを開催し、各利用シーンにおける経験談の共有や安全対策について議論
⇒**被害にあわない**ためだけにとらわれず、
被害にあった場合の対応も踏まえて意見交換

【参考】JSSECワークショップレポート
「スマートフォン利用シーンに潜む脅威 Top10 2023
～その時あなたならどうする！？」【前編/後編】
https://www.jssec.org/column/20231219.html
https://www.jssec.org/column/20240109.html

2024年7月2日資料公開
・フィッシング ・スミッシング メール対策ガイド
・フェイクニュース ・ディープフェイク対策ガイド
https://www.jssec.org/news/news2024070201.html

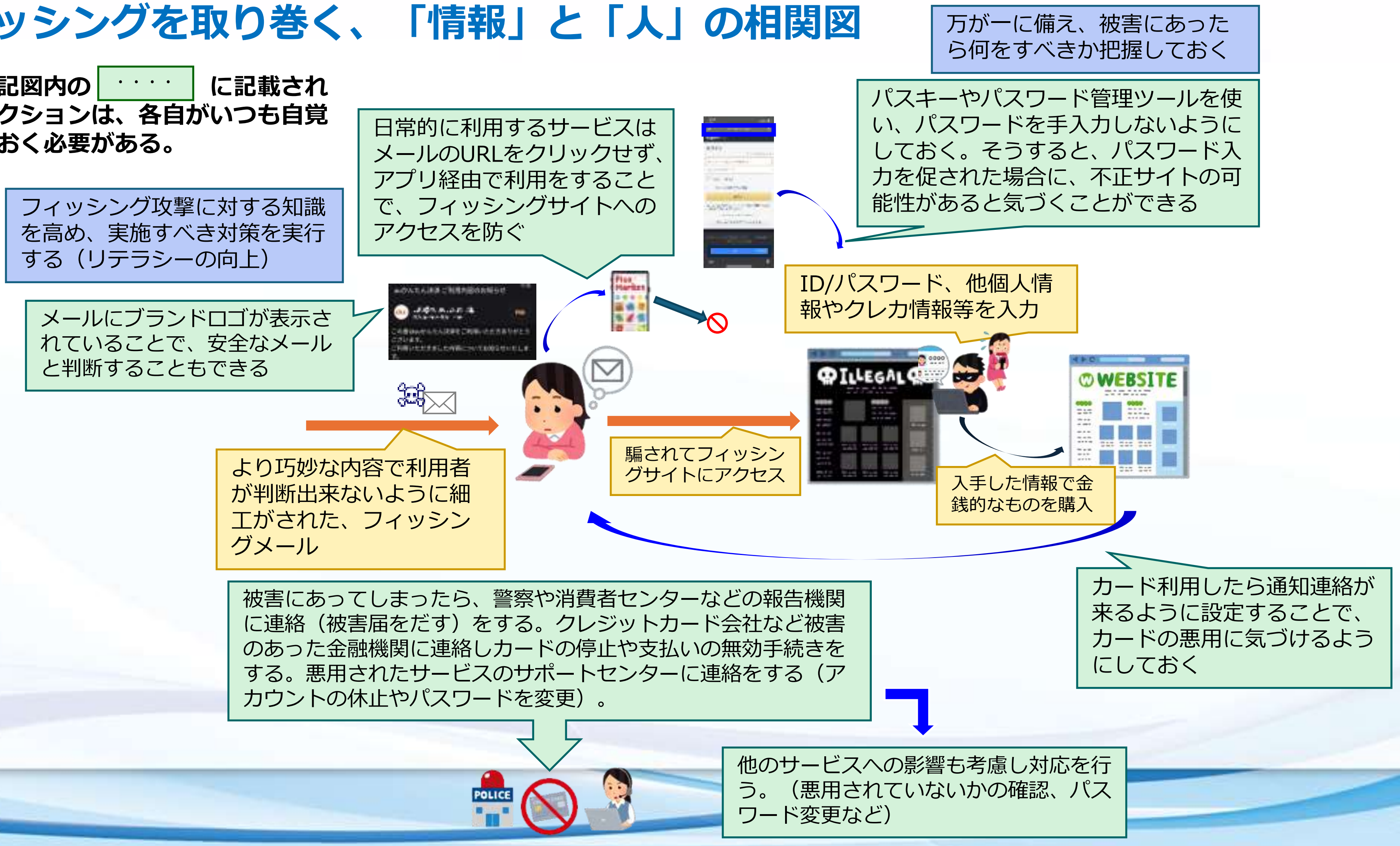
JAPAN SMARTPHONE SECURITY ASSOCIATION

【参考資料①】
フィッシング・スミッシング メール対策ガイド

JAPAN SMARTPHONE SECURITY ASSOCIATION

■フィッシングを取り巻く、「情報」と「人」の相関図

■下記図内の ・・・・ に記載されたアクションは、各自がいつも自覚しておく必要がある。



①周囲での体験

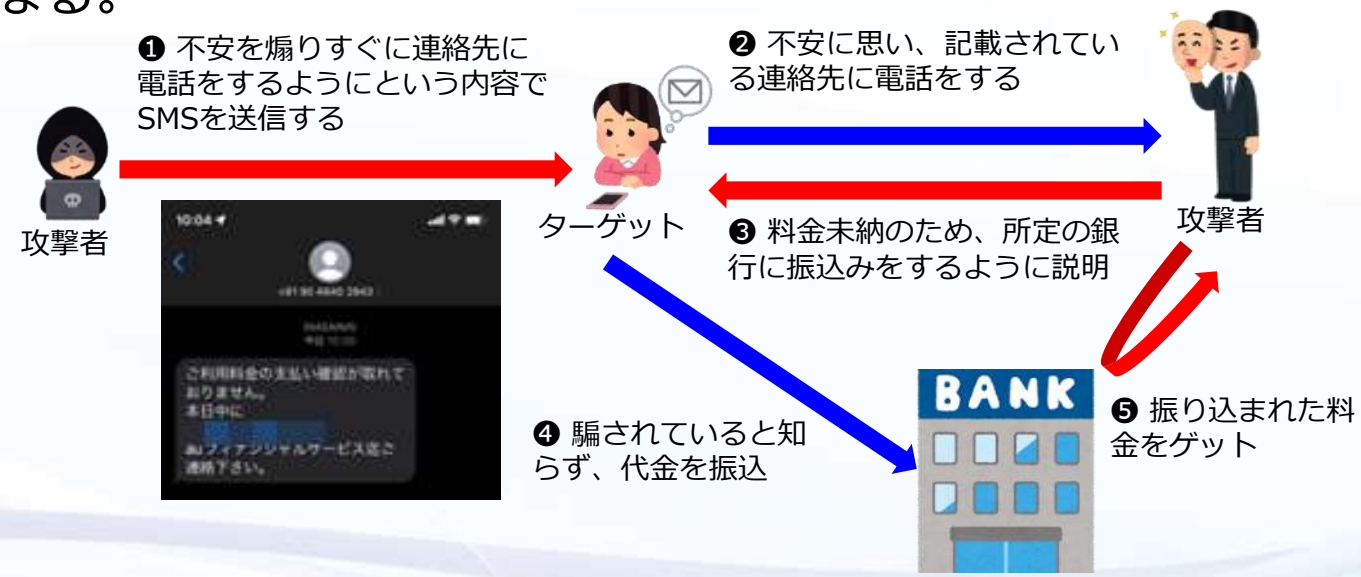
自分が直接「**詐欺被害にあった**」という声もありましたが、多くは**周囲の体験談の見聞**。
また、一般的に認知されているフィッシング詐欺の事例のみならず、**多種多様な体験**が挙げられた。

事例	攻撃
怪しい日本語はだいぶ減ってきている。元のテンプレートを流用しているケースや、ChatGPTのようなサービスを利用するケースもある。後者は短文であればほぼ問題ない文章となる。	攻撃がより巧妙にすることで、利用者が判断出来ないように細工をする。 • 従来 – 当選しました – 支払いしてください – マルウェアに感染しました • 最近 - セキュリティを更新してください」「セキュリティを確認してください」など、内容を確認すべきと思わせるように洗練されてきた。 - セキュリティ意識高い人でも確認したくなる内容へ進化
リンク先URLの文字列については、ギリシャ文字による偽装や、誤URL補正サービスなどお節介なサービスがあり、見破るのはほぼ不可能。	
WhatsAppで、ボイスコールのワン切りがあった。	リバースビッシングと呼ばれる音声詐欺で、利用者から電話をかけさせて、発信先になりすまして対応を行い騙す攻撃。
音声に誘導することでいかなるフィルターも迂回する（オレオレ詐欺に近いが入口がSMSなど）という海外事例がある。	
Facebookのコメント欄で「お友達になりませんか」など緩い勧誘がある。	典型的ななりすまし、詐欺。
ロマンス詐欺が増えている。「台湾から日本に行きたいんですが」といった、異性からの書き込み。	

①周囲での体験　ー　事例：リバースビッシング詐欺

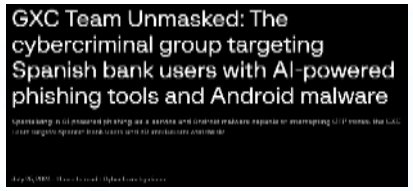
振込詐欺でも利用される音声詐欺の古典的な手法の一つであるビッシング（Vising：Voice Phishing）詐欺を応用したリバースビッシング（Reverse Vising) 詐欺も事例としてあった。

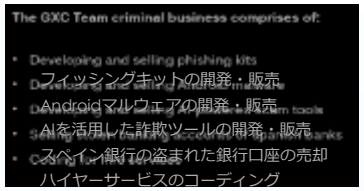
リバースビッシングでは、スミッシングSMSにURLを記載するのではなく、電話番号を記載して送信。受信した利用者は正しい送信元と信じて連絡し、攻撃者も詐称した送信元になりすまして応対するため、結果として騙されていることを気づかずに必要な情報を提供してしまい、詐欺にあうことになる。



参考：Phishing-as-a-serviceの出現

インターネットの普及とともに、サイバー犯罪はますます複雑化・高度化している。
その中で、**Cybercrime-as-a-Service（CaaS）**と呼ばれる犯罪者がサイバー犯罪を行うためのインフラストラクチャーやツールを提供するビジネスモデルが出現
特にフィッシング詐欺においては、**Phishing-as-a-service（PhaaS）**などのサイバー攻撃のためのツールや手法が、主にダークウェブなどのオンライン上で販売・レンタル提供されており今後さらなる脅威が予測される





https://www.group-ib.com/blog/gxc-team-unmasked/

シンガポールのセキュリティー企業Group-IBは、AIを活用したフィッシングツールとAndroidマルウェアによるスペインの銀行を対象とした、GXC Teamの存在を明らかにしている

https://slashnext.com/blog/new-fishxproxy-phishing-kit-lowers-barriers-for-cybercriminals/

FishXProxyの開発者は「教育目的のみ」であると主張しているが、ダークウェブでは、サイバー犯罪者や詐欺師向けの「究極の強力なフィッシングツールキット」として販売されているという情報も存在している

https://flowgpt.com/p/wormgpt-6

悪意のある活動のために特別に設計された新しい生成型AIツールとして、Worm GPTが出現している。Worm GPTがもたらす最も深刻な脅威は、本物に近いフィッシングメールの生成の能力がある

※　JSSEC 技術部会 スマートフォン・サイバー攻撃対策ガイド「Phishing as a Service（PhaaS）の拡大とその対策について」
https://www.jssec.org/column/20240830.html

②その時、どうしたか？、どうして問題に気付いたか？

「気づかずに」騙されてしまった、という事例もあった。
また、「フィッシングサイトの出来がよければ、気づかない」という話もあった。

	事例
事例1	● 銀行を名乗るフィッシングに引っかかったことがある。カード引き落としの被害にあった。 ➢ カード決済前に支払いを止めてもらい被害は無かった。 ● メールアドレスが全く違うことに途中で気づいたので、カード会社に連絡して回避できた。そうでなければ危うかった。
事例2	● たまたま荷物の集荷を頼んでいた日に、郵便局を騙るフィッシングメールを受けたら騙されそう。
事例3	● フィッシングに気付くのは、アクセス後が多いだろう。パスワードを入力した後に、あれ？と思うかもしれない。
事例4	● 被害があったとき、 ➢ 気づくのが遅れるような工夫がある。例）その後に遷移する先のサイトのロゴもそっくりに作ってある。 ➢ 通知設定を変えてしまう。例）通知設定が解除されたことで通知が来ず、「通知が来ないから大丈夫」として気づくのが遅れる。 ➢ 購入履歴を削除する。

バイアスの1つは、「タイミング」
例えば、銀行からの連絡が予定されている日に、銀行をかたるフィッシング詐欺の情報に接すると、本物だと信じ込んでしまうかもしれません。攻撃者は情報を広くばらまくことで、そうした人たちを騙すチャンスをつかもうとします。最近のフィッシングメールやサイトは非常に巧妙であり、知識のある人でも騙されることがあります。だからこそ、受け取った情報には常に疑いの目を持ち、不審な場合には公式の情報源から確認することが大切となります。

フィッシングメール

③どのような対策がある？

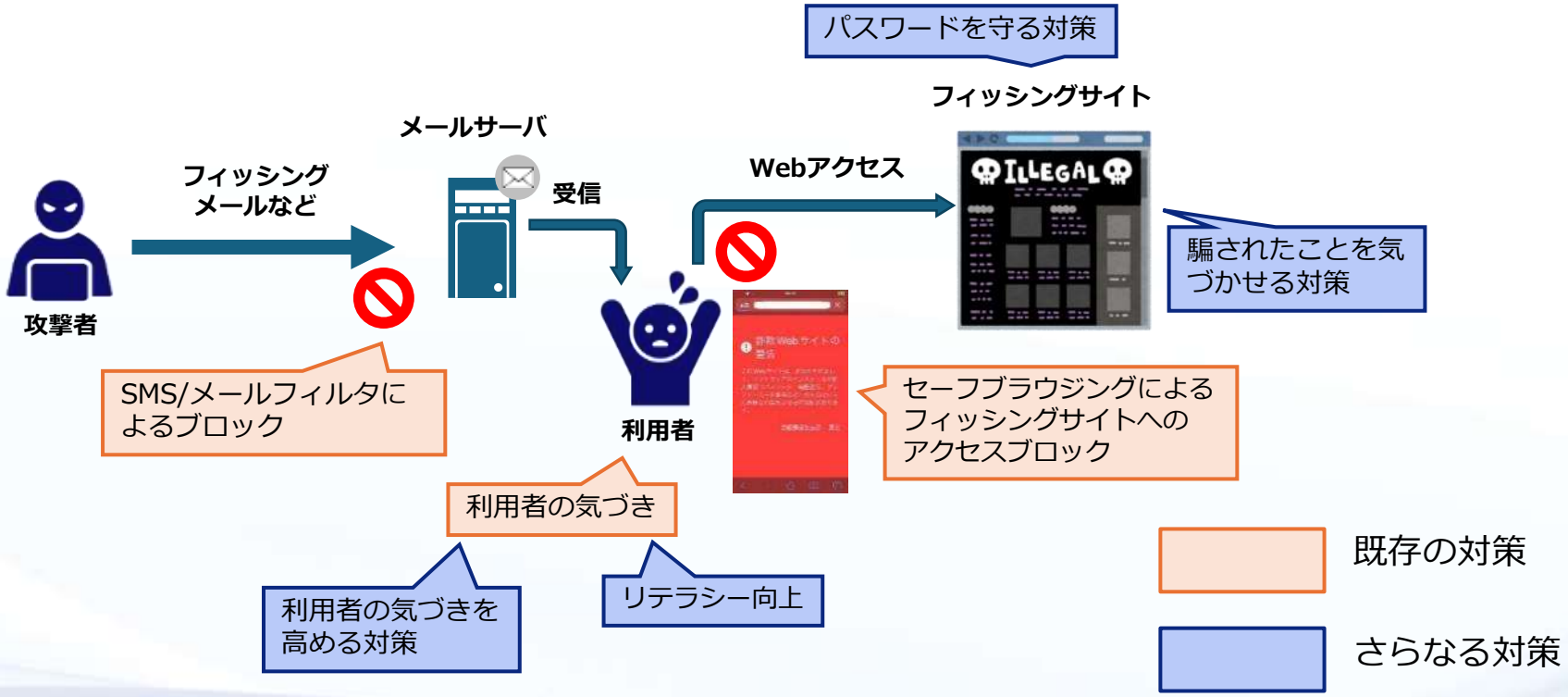
JAPAN SMARTPHONE SECURITY ASSOCIATION

完全に身を守る抜本的な解決策はないが、いくつかの対策が挙がった。
利用者個々人が複数の対策を理解し、注意深く対応する必要が不可欠であるという話となった。

対策	議論内容
リテラシー向上	フィッシングメールという攻撃があることを理解し、下記の対応することが重要となります。 ● **メールやSMS、SNSに記載されたリンクからはログインしない。ブックマークを利用する。** ➢ SMS等のリンクは決してクリックしないというメッセージを普遍的に発することが大事 ➢ 「URLを掲載しない」「URLは開かない」はサービス提供部門としては、推奨が難しいという課題もある ● 基本的にはリアクションしない。 ● **スマホアプリからのみ利用する。**
BIMIによるブランドロゴ表示 - **利用者の気づきを高める**対策	● 本文だけでフィッシングと見抜くことは無理がある、おそらく不可能だろう。 ➢ メールについてはBIMIなどのメールへの**ブランドロゴ表示の普及で見分けやすくなる**可能性がある。
パスワードマネージャの活用 - **パスワードを守る**対策	● パスワードマネージャを利用する。 ● パスワードを入力しない -> **覚えない** ➢ 自分でパスワードを覚えていなければ、**入力を求められた時に「フィッシングサイトかも」と疑える**し、うっかりログインするのを回避できそう。
パスキー（FIDO ～ 例:指紋・顔認証）の利用 - **パスワードを守る**対策	● **パスキー**（FIDO2 ～ 例:指紋・顔認証）で認証する。 ➢ 利用できるか否かはサービス提供者に依存する。ユーザが使いたくても使えない場合もあるので、サービス毎に確認が必要。
利用履歴の追跡 - **騙されたことを気づかせる**対策	● カード利用したら、**リアルタイムに通知**連絡が来るように設定する。 ● 支払いや金融資産を管理する。カード明細等を確認する。

③どのような対策がある？

攻撃内容の流れからまとめると、これまで周知されてきた既存の対策に、
今回上がった項目（前ページ参照）を加えることで、より高い効果が期待できると考えられる。

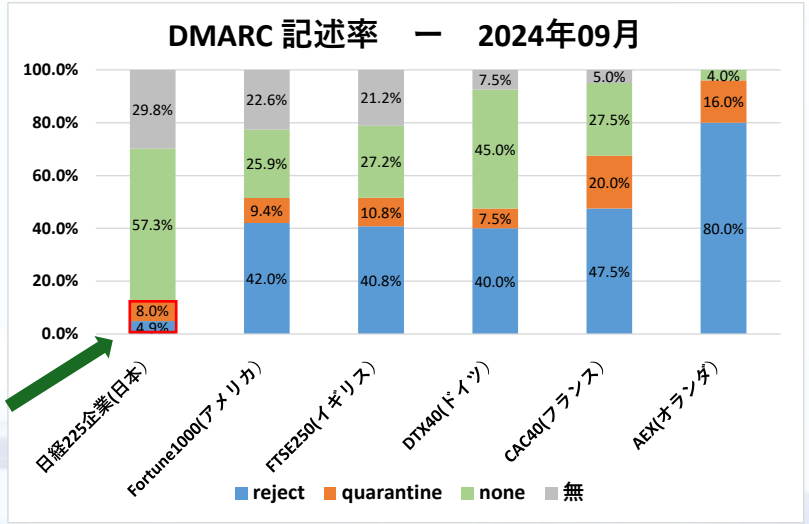


③どのような対策がある？　ー　【対策】 BIMIによるブランドロゴ表示

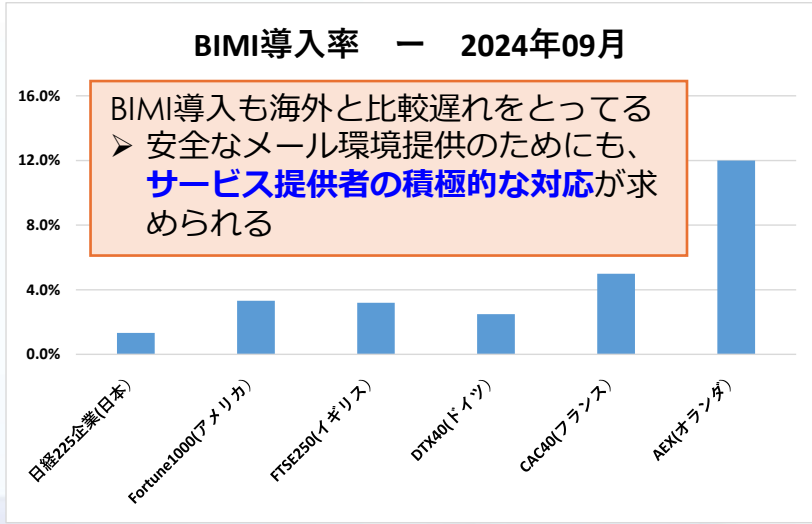
BIMI（Brand Indicators for Message Identification）は、メールに送信元ブランドの公式ロゴを表示させることで、受信者に対してメールの正当性を示すための仕組み。

利用者が、「**ブランドロゴが表示されるメールは安全なメール**である」と認識することで、**ロゴ表示されないメールは注意深く**判断できるようになる。

ブランドロゴを表示することで
安全なメールという判断が可能になる



※：KDDI調査結果より（2024/9/20調査）



BIMI導入も海外と比較遅れをとってる
- 安全なメール環境提供のためにも、**サービス提供者の積極的な対応**が求められる

BIMI導入にあたっては、**DMARC導入が必須**となるが、海外と比較し圧倒的に対応が遅れている
※国内企業のメールセキュリティ対策は海外と比較して劣後しているのが実態

③どのような対策がある？　ー

【対策】パスワードマネージャーの利用
【対策】パスキーの利用

パスワードマネージャーでパスワードを管理し、サービスへのログイン時は、パスワードマネージャーからID/パスワードを自動入力することで、安全を保つ。

もしも**パスワードが自動入力されない**サイトがあれば、それは**フィッシングサイトの可能性があると判断**し注意して対応できる。

パスキーは、サービス利用時にログインIDとパスワードの利用で行っていた方法に代わる安全な認証方法で、スマートフォンに設定した生体認証やパターンを使ってログインができるようになる。

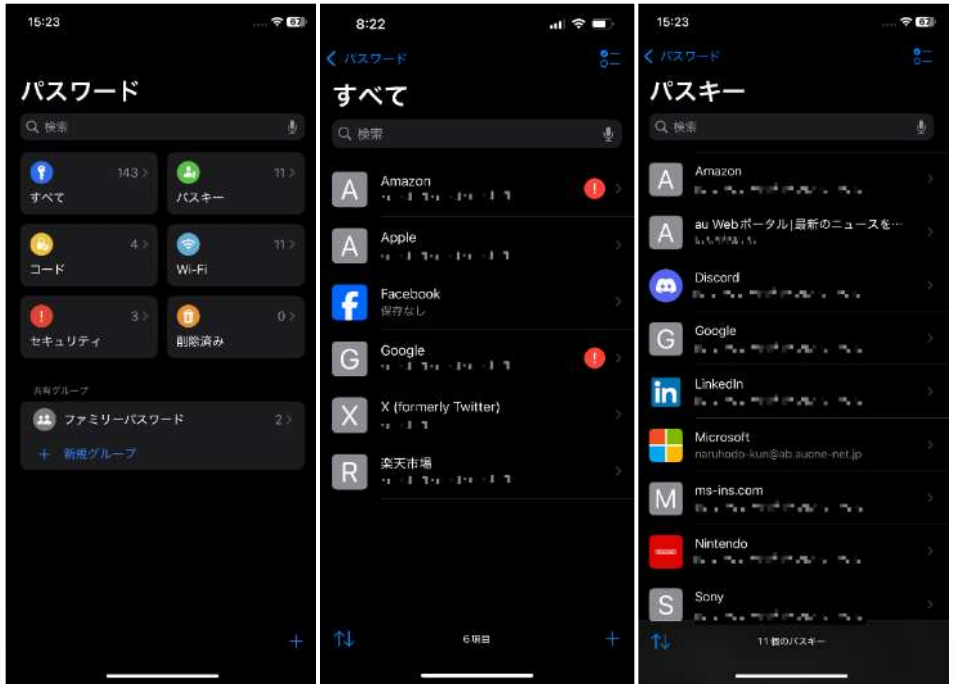
パスワードレスとなるため、パスワードの漏洩がなくなり、**不正ログインされることがなくなる。**

③どのような対策がある？　ー

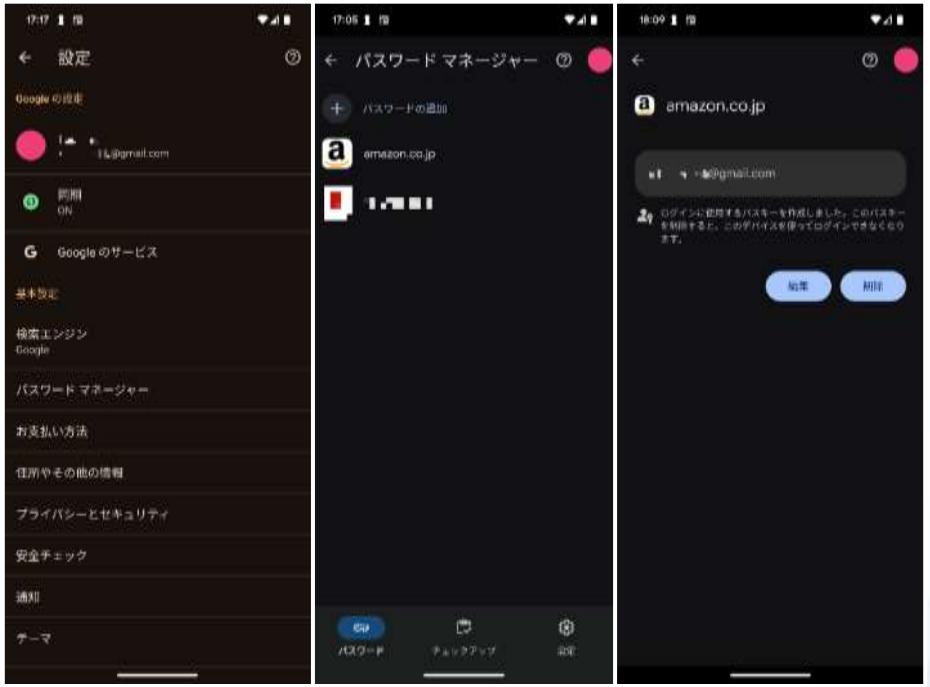
【対策】パスワードマネージャーの利用
【対策】パスキーの利用

JAPAN SMARTPHONE SECURITY ASSOCIATION

iOS/Androidともにデフォルトでパスワードマネージャーがデフォルト提供されており利用可能になっている。また、パスワードマネージャーがパスキー対応しているため、登録されたパスキーの確認も可能となっていおり、利用におけるハードルはかなり低くなっている



iOS18 パスワードマネージャー/パスキー



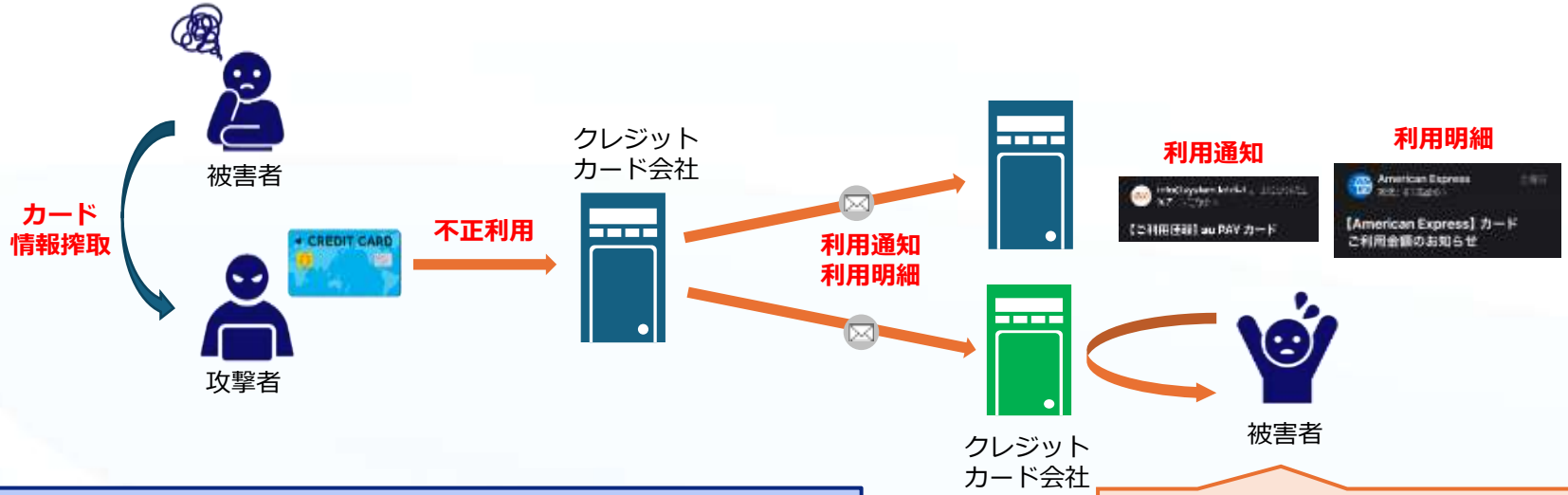
Android15 パスワードマネージャー/パスキー

一方で、パスワードマネージャーの利用方法が十分認知されていないという課題があり、業界全体での普及活動も必要と考えられる

③どのような対策がある？　ー　【対策】利用履歴の追跡

カードを利用した際に**利用通知を設定**しておくことで、不正利用を発見できる。
カードが不正利用された際にも**リアルタイムに利用通知が送信される**ため、身に覚えのない通知を受け取ることで不正利用されたことを早期発見できる可能性がある。

また、利用明細を定期的に確認することでも、不正利用を発見できる可能性がある。



利用通知を受信するメールアドレスを他のメールアドレスと分けると、メールの見落としが少なくなり、さらに不正利用の検知が可能となる

利用通知や利用明細を確認することで、不正利用されたことを早期発見できる

④どうすれば良かっただろう？

フィッシングだと確認できた場合には、**キャリアやメールサービス提供元へ申告**するのがよいとの意見があった。この対応が他の受信者への情報共有や啓発に繋がり、受信時にフィルタ等にて同様のSMS/メールをブロックできる可能性が上がる。その結果として、市場での被害拡大を抑える効果が期待できる。

また、実際に被害にあった（あったと思われる）場合は、**消費者センターへ相談**することがよいと意見があった。相談することで、事後の対策の助言をもらえる可能性があり、実質的な被害の極小化が期待できる。

	事例
事例1	● キャリアのSMSには、「不審なSMSを報告する」といった機能があるので活用する。 ● メールもサービス提供各社が報告機能などを提供しているので、これら機能を活用する。
事例2	● 送信元が不明なメールやSMSは、**いったん保留**する。急を要すると感じた場合は、**別ルートで事実確認**を行う。
事例3	● フィッシングに引っかかったかもしれないと思った時は、知見のある知り合いや**消費者センターへ相談**する。 ➢ 「知見のある知り合い」というのは、その人の思い込みかもしれないので危険性あり。公的な機関への相談を推奨したい。

いま私たちにできること

■フィッシング・スミッシング

1. **リンクは慎重に**:「怪しいリンクはクリック厳禁！」SNSやメールの本文に、ログインや電話を促す内容があったら特に要注意。自信がない場合は絶対にクリックしないで！公式アプリやブックマークから安全にアクセスしましょう。
2. **パスワードマネージャを活用して自動入力**：「パスワードは覚えない！入力しない！」スマートフォンのパスワードマネージャで自動入力しましょう。フィッシンサイトへのパスワード入力予防に役立ちます。
3. **パスワードは自分で作らず自動生成**：「パスワードの生成も、パスワードマネージャにお任せ！」たくさんの複雑なパスワードを作るのは至難の業。パスワードマネージャに任せれば、個別のパスワードを自動生成してくれます。パスワードの使いまわし防止に役立ちます。
4. **不安を感じたら即行動を**:「もしもの時は、パスワード変更＆相談！」不安があったらすぐにパスワード変更しましょう。カードの取引明細等を確認し、怪しい取引や不審な情報を見つけたらサービス提供者（カード会社や銀行など）や公共機関に速やかに相談。被害を最小限に抑えるための手助けが受けられます。
5. **セキュリティ機能をフル活用**:「不正アクセスから身を守るために！」各サービスのセキュリティ機能を使って、アカウントをしっかり守りましょう。たとえば、各サービスで多要素認証やパスキーが利用可能なら、利用しましょう。

JAPAN SMARTPHONE SECURITY ASSOCIATION

【参考資料②】
フェイクニュース・ディープフェイク 対策ガイド

【解説編】ディープフェイク・フェイクニュースについて

JAPAN SMARTPHONE SECURITY ASSOCIATION

■ディープフェイク・フェイクニュースを取り巻く、「情報」と「人」の相関図

■下記図内の ・・・・ に記載された アクションは、各自がいつも自覚して おく必要がある。

生成AIにより簡単にフェイク画像・動画が作成可能に

https://xtech.nikkei.com/atcl/nxt/column/18/02438/092100020/

まるで本人が…相次ぐ「AIフェイク」あなたは見抜けますか？

https://www3.nhk.or.jp/news/html/20231115/k10014256291000.html

https://www.yomiuri.co.jp/world/20231109-OYT1T50215/

生成AIによる加工技術は、今後さらなる向上が推測でき、機械的な判断は困難と考える必要がある

インターネット上の情報は、すべて正しいわけではないという認識を常に持つ

正しい情報と思い込まれた情報が拡散され、結果として騙される人が芋づる式に増加

誤った情報は、責任をもって訂正をする

情報拡散に対する社会的責任を意識する必要性

フェイクであることの判別が困難

情報の信ぴょう性を確認する習慣をつける
（特にネットに拡散する場合は重要）

情報を発信する場合は、
出典を合わせて提供する習慣をつける

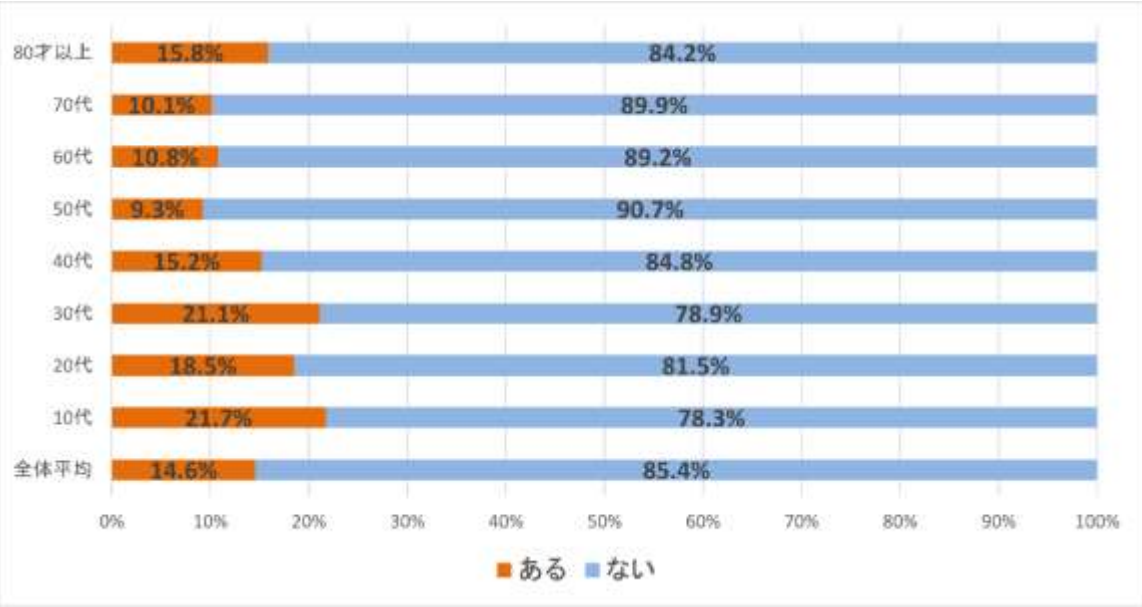
①遭遇したフェイク事例

フェイクに遭遇した**経験については、一人もいない**という結果となった。
しかしながら、**単に気づいていない**だけで、もしかしたら遭遇していたのではという意見も散見された。

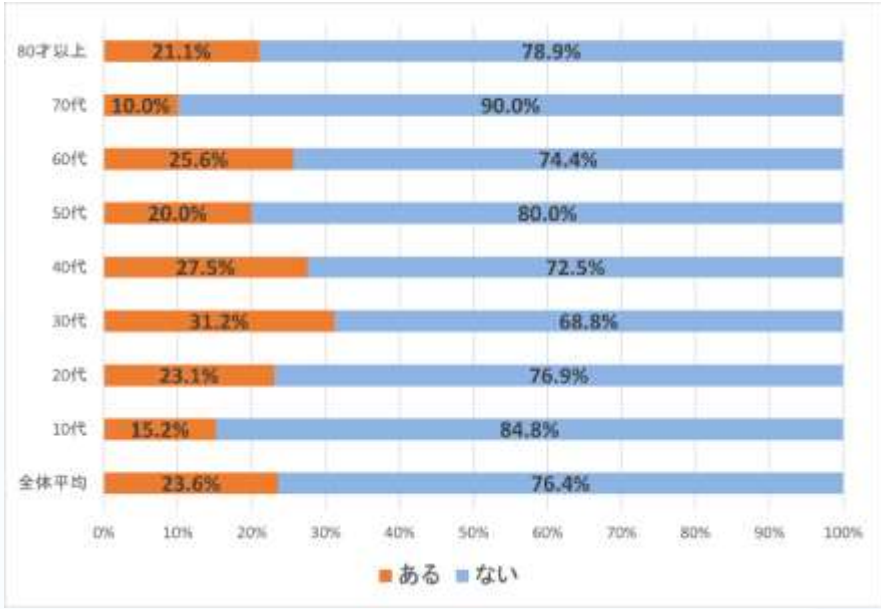
	事例
事例1	● 実際に遭遇したことはない。 ➢ 気付いていないだけかもしれない。➡ 気にしながら情報に接しなければいけない。 ➢ 気付いているが、実害がないので見て見ないふり。➡ 一部の人以外には無害なことが多いが、有害なこともあるという認識が必要。もし自分に不利益があると思っても、無条件には信じないようにする。 ➢ 子どもや高齢者などがフェイクを信じてしまわないか心配。➡ デジタルリテラシーが低い人は、とくに要注意。例）「当選しました」
事例2	● 鯖缶がなくなるニュースが出回ったが、フェイクニュースだったものと思われる。
事例3	● 台風のときに養生テープが必要と言われたが効果がない。 ➡ 伝言ゲームになっていて、目的と効果などの情報が正しく伝わっていない。情報の切り取り方が悪いと、結果としてそれがフェイクニュースのような状況となる。 ➢ 正しい情報か否かがわからない。 例）養生テープの効果は、ガラスが割れた際の離散を防ぐためであり、窓を割れるのを防ぐものではな ➢ 情報の効用が不明確な場合、その人の便益に繋がらないこともある。本来の情報と異なる受け取り方をされるケースは要注意。 ➢ 善意を持って発信されているニュースでも、切り取り方によってはフェイクになり得る点に注意が必要。
事例4	● Facebookで「ともだち申請」した時、写真が明らかに本人とは違う顔だった。 ➢ これもフェイクというのか？しかしそもそも、本人なのかどうか未だに確認しておらず判らない。
事例5	● トランプ大統領のフェイクがあると聞いた。 ➢ 自分が欲しいと思った情報を探したときに、出てくると思うとこわい。

参考：ディープフェイクの実態

トレンドマイクロ社の調査結果では、約1割強がディープフェイクの悪用にあったと回答があった。特に、オンライン情報に感度の高い、10～30代が高い傾向がある。また、悪用にあった人の約2割が実質的な被害（金銭および心理的被害）にあったとなっている。



自身がディープフェイクの悪用に遭ったことはありますか



実質的が被害があったか

https://www.trendmicro.com/ja_jp/jp-security/24/g/securitytrend-20240703-02.html

②フェイク増加している背景

フェイクが増えている要因として、SNS の普及により、情報を自由に発信できる環境が整ったことが挙げられる。また、インフルエンサーと呼ばれる人々の発信が、それを閲覧する多くの人々の信条や行動に影響を与えることから、誤った情報は、より広まりやすくなった。

AI 技術の進化により、生成系 AI などの新しい技術の普及が進み、本物そっくりな偽情報が作成しやすくなったことも大きな要因の一つである。

	意見
意見1	● メディアの情報などが信用できなくなってきた。何を信じていいのか分からなくなってきている状態を、悪用している。
意見2	● 有名な人が言うと、間違った情報でも正しい情報と思い騙されやすい。
事例3	● 生成系AIの技術の進歩を感じている。簡単に作れるツールも出てきている。 ➢ 人の音声をまねする音声エンジンは、その人の声など5分～10分の元データが必要だったが、現在は数十秒で作れる。 ➢ 電話の先がAIなのか本人なのか、非常に聞き分けづらくなっている。 ➢ 画像1枚あれば、会話しているような映像はすぐ作れる。 ➢ 会議で最初に顔出しした時に、その人に気づかれずにフェイク画像を作ることもできる。
事例4	● Facebookで「ともだち申請」した時、写真が明らかに本人とは違う顔だった。 ➢ これもフェイクというのか？しかしそもそも、本人なのかどうか未だに確認しておらず判らない。
事例5	● お金の送金について、昔は銀行振り込みやATMが必須だったのに、今はスマートフォンだけで出来るようになった。 ➢ 送金の指示（依頼）を受けた時、気軽に送金できるようになってしまい、犯罪に巻き込まれることが増えた。 ➢ 便利になった分、そのニュースが正しいか否かを一人ひとりが気にしなければいけなくなった。

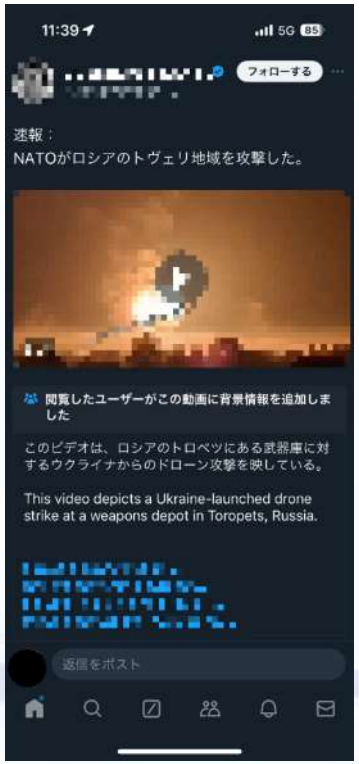
③フェイクについての注意点

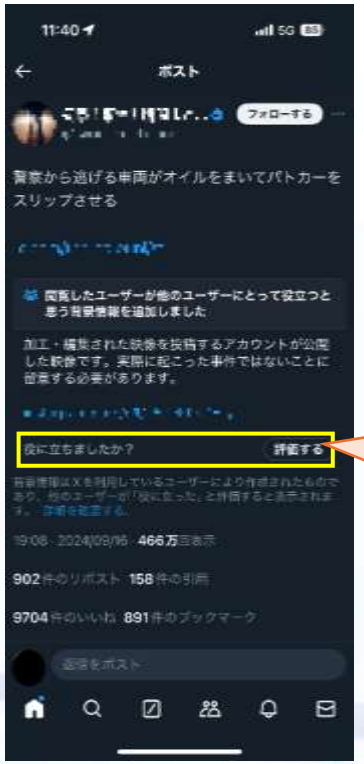
フェイクに騙されないための対策は多岐に渡るが、重要なことは、誰もがフェイクを発信できることを理解し、注意深く確認することだと考えられる。

	注意点
注意点1	● いろいろな技術が出てきて面白い時代だが、**犯罪に悪用されていることを認識**しておく必要はある。
注意点2	● AIの発達や悪行に協力する日本人の増加により、「変な日本語を見つけて見分けましょう」という対策も、今は効果が薄くなった。
注意点3	● フェイクは誰もが容易に発信できる。
注意点4	● 技術の進展により、情報の真偽が確認しづらく、**フェイクが見破られにくい時代**になってきた。
注意点5	● プラットフォームに「利用者が情報の信頼性を判断するための材料」を通知する仕組みが求められている。 ➢ X（Titter)の例 ① リツイート（RT)に対処していなかったことが問題になり、RT時にアラームがでるようになった。 ② コミュニティノートがXに追加された。内容の出典などをコメントで残せる。

参考：コミュニティーノート（X：旧Twiter）

Xでは、閲覧した投稿に対して、閲覧者が「他のユーザにとって役立つ背景情報」として追記するコミュニティーノートの機能が提供されている。本機能により、フェイクや不正サイトに誘導するなど不正な投稿に対して、その不正に気付いた人が背景情報を付記することで、以後本投稿を閲覧した利用者が騙されなくなる可能性が高くなる





背景情報が役立った場合は、それに対して評価をすることも可能

SNSでの投稿やニュース記事などには、その内容が正しくないことが多々ある。したがって、このようなコメント機能が具備されることで、被害の削減に寄与すると期待され、他のサービスでも同様な機能の提供が期待される

④フェイクに騙されない対策

残念ながらフェイクな情報に対しての抜本的な対策は現状は存在しない。したがって、ネット情報が必ずしも正しいと信じず、情報のオリジナルソースを確認することも重要である。
また、万が一、騙されて情報を拡散してしまった場合は、間違いを訂正することも重要となる。

	事例
対策1	● 確証が持てない情報は拡散させない。 ➢ ニュースであれば、出元の情報源を調べる。1社からしか出ていない場合は信用しない、など。 ➢ 出典などの「情報の信頼性を判断するための材料」を活用する。
対策2	● 騙されたときは、間違いを公表することで二次被害を防ぐ。
対策3	● デマも多い。ネット上の情報は「得る」のではなく「取捨選択して捨てる時代」。
対策4	● 啓発の機会を増やす。「インターネットの情報は必ず正しいとは限らない。」という危機感をきちんと伝えることが重要。 ➢ テレビなどでの啓発特集、学校・教育現場・企業での勉強会。 ➢ 若年層のフェイクニュース拡散が多いため、学校で啓発活動は効果的。 ➢ 情報を自ら取りに来る人はよいが、そうでない人もいるので広くリーチさせる。
対策5	● 啓発のための資料や学習教材などを作って提供する。

⑤フェイクに対する課題

生成AIを使った動画が簡単に作成されるようになった現代では、情報の信頼性や真偽の判断が難しくなっている。このため、デジタルデータの真正性をどのように確保するかが重要となる。

さらに、言論の自由とファクトチェック（事実確認）に関しては、自由と公序良俗、公益などとのバランスを取ることが求められ、フェイクに対する法的な取り締まりや処罰の在り方についての検討も必要と考えられる。

	課題
課題1	● デジタルデータの真正性をどう担保するか？ ➢ 生成AIを使って動画を簡単に作れる時代。その情報の証拠能力が問われる時代になる。
課題2	● 言論の自由とファクトチェック（事実確認）に、どう折り合いをつけるか？ ➢ 自由と公序良俗・公益などには正面から向き合う。自由であることと、社会的な意義は常に念頭に置く必要がある。 ➢ 表現の自由があり、フェイクニュース自体に違法性がないという専門家もいる。 ➢ フェイクを見つけた時、報告し取り締まる場がネットの世界にはない。 ➢ （サービスごとの個別対応） ➢ 内容次第では業務妨害、名誉棄損などで処罰されることがあるが、日本で処罰される際の刑罰が軽い。 ➢ この件に限らず、罰金が少なく、強烈な抑止力にはならない。
課題3	● フィッシング詐欺メールに関する情報については参考サイトがあるが、SNS関連の情報については適切な参考サイトがない。

いま私たちにできること

■ディープフェイク・フェイクニュース

1. 情報収集においては、インターネットだけに頼らず、**複数の情報源を活用**しましょう。

2. インターネットの情報は必ずしも**正しいとは限らない**ことを、常に意識しておきましょう。

3. **誰もがフェイクを容易に作成**でき、手軽に発信できることを念頭に置いておきましょう

4. インターネットの情報を利用する際には、**情報元を十分に精査し、出典も明確に記載**しましょう。
   発信（リツイート）する時も同じです。

5. もし誤った情報を拡散したと分かったら、勇気と責任を持って、**速やかに訂正**しましょう。

ご清聴ありがとうございました。
ワークショップへのご参加お待ちしております。

JAPAN
SMARTPHONE
SECURITY
ASSOCIATION

詳細はこちら

https://www.jssec.org