セキュリティフォーラム2024
JSSEC利用部会成果発表

「スマホ利用シーンに潜む脅威 Top10/2023」解説編リリースについて

2024年 3月6日（水）

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　ガイドラインWGリーダー
松下 綾子（ALSI）

https://www.jssec.org

JSSECとは？

JAPAN SMARTPHONE SECURITY ASSOCIATION

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。

部会紹介：目的と目指す成果

JAPAN SMARTPHONE SECURITY ASSOCIATION

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

https://www.jssec.org/activities

JAPAN SMARTPHONE SECURITY ASSOCIATION

利用部会　活動紹介

2023年度 利用部会の方針

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) 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：三池　聖史　(ユニアデックス株式会社)
　　サブリーダー：中村　丈洋 (株式会社SHIFT SECURITY)

利用ガイドラインWG

利用ガイドラインWG　活動報告

**①スマートフォンやタブレットを組織で利用する際に、留意して
いただきたい点についてまとめたガイドラインとチェックシートⅠ作成**

②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

IoT-事例研究WG　活動内容

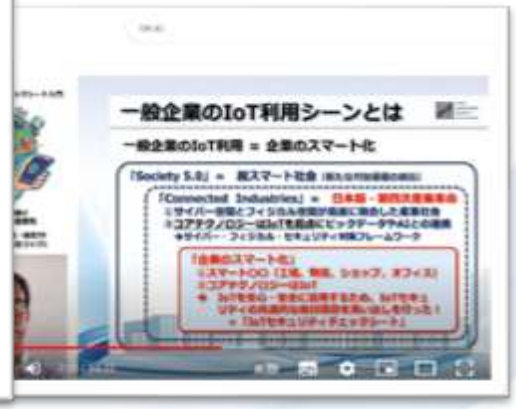
①IoTセキュリティチェックシート　第2.1版の外部発信、啓発活動

■「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～

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」

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



動画サイト「YouTube」を視聴することができます▶https://www.jssec.org/iot-youtube

2023年度　利用部会の活動方針

JAPAN SMARTPHONE SECURITY ASSOCIATION

今年度の活動方針

①オンライン/オフラインを融合させた活動
～ハイブリッドなＷＧ開催と、外部への情報発信

・ワークショップによるJSSEC会員の意見交換の場の設定
・外部に向けたオンラインセミナーと実地ワークショップの同時展開

②ワーキンググループの成果物を活用した啓発活動と情報発信

・「利用ガイドラインセキュリティチェックシートⅡ」の普及啓発、「解説書」執筆
・「IoTセキュリティチェックシート第二版」の普及啓発、事例研究　：
EU 動向の確認：サイバーレジリエンス法案（CRA）が　Proposal（法案）として公開➡IoTセキュリティチェックシートとの項目比較など検討

2023年度の主な活動内容

主な活動内容

①コラムによる情報発信

・右図のような**コラム**を作成

②ワークショップの開催

・**オンラインとオフラインのハイブリッドを実現**

➡参加者からは、今後もハイブリッド対応の声が多かった。
「オンラインなら遠方からも参加可能」、「現地にいると意思疎通がしやすい」

③ワークショップ議論の成果物を活用した啓発活動と情報発信

・2023年3月にリリースした「スマートフォン利用シーンに潜む脅威 Top10/2023」を活用した**ワークショップ開催と解説書作成**

スマホ利用シーンに潜む脅威 Top10/2023

解説書について

「スマホ利用シーンに潜む脅威 Top10」とは①

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
・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

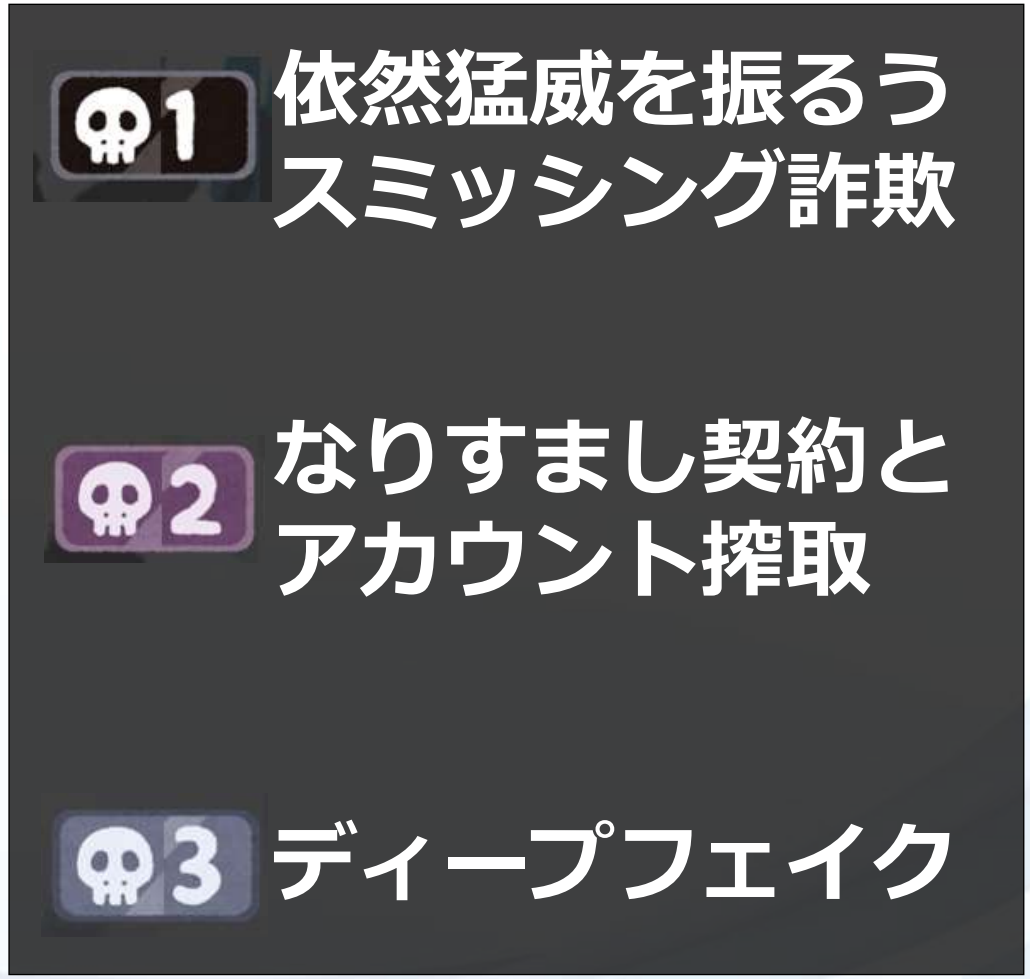
「スマホ利用シーンに潜む脅威 Top10」とは②

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



「スマホ利用シーンに潜む脅威 Top10」とは③

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

■解説書の作成手順

・Top10をグループ分け

・関心の高かった以下２点をピックアップ
- 「フィッシング」（右表の黄色）
- 「フェイクニュース」（右表の薄緑）

・ワークショップで議論した下記を記述
- 事例
- 技術背景
- インシデント時の初動（暫定策）
- 恒久策

➡今春リリース予定で作成中

ワークショップ全体からの考察

JAPAN SMARTPHONE SECURITY ASSOCIATION

■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。

フィッシング	項目	スミッシング
インターネットに接続されていれば、**どこからでも送信可能**	環境	携帯網と接続している環境が必要
１通あたりの**送信コストが安価**	コスト	送信するのに大きな費用が発生
迷惑メールの危険性について利用者の理解が浸透しており、比較的クリック率が低い	**リスク**	SMSへの不審な通知に対する利用者の理解が低く、比較的**クリック率が高い**
フィッシングで送信する文章には文字数の制限がなく、HTMLメールなど、精度の高い詐称が可能	文字数条件	送信文字数に制約があり、表現が限られる
短縮URLを使うケースも多々あるが、HTMLメールによりURLを隠蔽したり、送信者を識別するコードを埋め込むなど多彩	手法	誘導するURLに短縮URLを使うケースが多い
ファイル添付が可能 （マルウェアの添付も可能）	仕様	ファイル添付が不可能

【解説編】フィッシング・スミッシングについて

■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。

日常的に利用するサービスはメールのURLをクリックせず、アプリ経由で利用をすることで、フィッシングサイトへのアクセスを防ぐ

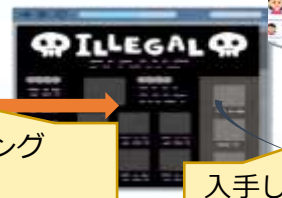
万が一に備え、被害にあったら何をすべきか把握しておく

パスキーやパスワード管理ツールを使い、パスワードを手入力しないようにしておく。そうすると、パスワード入力を促された場合に、不正サイトの可能性があると気づくことができる

フィッシング攻撃に対する知識を高め、実施すべき対策を実行する（リテラシーの向上）

メールにブランドロゴが表示されていることで、安全なメールと判断する
こともできる

ID/パスワード、他個人情報やクレカ情報等を入力



より巧妙な内容で利用者が判断出来ないように細工がされた、フィッシングメール

騙されてフィッシングサイトにアクセス

入手した情報で金銭的なものを購入

カード利用したら通知連絡が来るように設定することで、カードの悪用に気づけるようにしておく

被害にあってしまったら、警察や消費者センターなどの報告機関に連絡（被害届をだす）をする。クレジットカード会社など被害のあった金融機関に連絡しカードの停止や支払いの無効手続きをする。悪用されたサービスのサポートセンターに連絡をする（アカウントの休止やパスワードを変更）。

他のサービスへの影響も考慮し対応を行う。
（悪用されていないかの確認、パスワード変更など）

【解説編】フィッシング・スミッシングについて②

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。	

【解説編】ディープフェイク・フェイクニュースについて

■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

おわりに～いま私たちにできること

JAPAN SMARTPHONE SECURITY ASSOCIATION

■フィッシング・スミッシング

1．情報収集は、インターネットだけに頼らないようにしよう。
2．平素から、インターネットの情報は、すべて正しいわけではないという認識を常に持っておこう。
3．インターネットの情報を利用する／発信（リツイート）する場合は、いったん立ち止まり、
　情報元を精査した上で、出典も合わせて記載しよう。
4．もし誤った情報を拡散してしまったと分かったら、勇気と責任を持って訂正しよう。

※フェイクを取り巻く現状に、法整備が追い付いていない現実があるので、情報収集には最善の注意を払いましょう。

■ディープフェイク・フェイクニュース

1．SNS、メール、SMSで届いたURLは、なるべくクリックせずに自分のブックマークやアプリからアクセスしよう。
　特に、メール本文にログインを促す記述があったら要注意！
2．各サービスサイトが、パスキーや多要素認証機能等を提供していれば導入しよう。
3．パスワードは、パスワード管理ツール使って「自動入力設定」をしておこう。
　※iOSのパスワードマネージャ、Google Authenticator、Microsoft Authenticatorなど。
4．もし不安に思ったら、サービス提供者（カード会社、銀行など）や、消費者センターなどの公共機関に相談して
　被害を最小限に留めよう。友人や家族にも影響が考えられる場合は、直ちに伝えよう。
5．同じIDやパスワードを別のサイトでも使っていないか見直して、少しでも不安があればパスワードを変更し、
　二次被害を防ごう。

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