【セキュリティフォーラム2026】資料

利用部会 活動報告

～ スマホ脅威Top10 ＆ IoTセキュリティチェックシート改訂 ～

2026年 2月6日（金）

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　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）

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発信**を行う。 ・メディア対応／各種成果物ならびにJSSEC活動の情報配信（Web／SNS） ・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

利用部会の体制

JAPAN SMARTPHONE SECURITY ASSOCIATION

体制

利用部会

部会長　：松下綾子(ALSI)
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）

利用ガイドライン WG

WGリーダー ※兼務
松下綾子(アルプスシステムインテグレーション(株))

IoT事例研究 WG

WGリーダー
小林幸司（株式会社SHIFT SECURITY）
サブリーダー
中村丈洋（株式会社SHIFT SECURITY）

スマートフォン利用シーンに潜む脅威検討 WG

WGリーダー　※兼務
本間輝彰（KDDI株式会社）

具体的な活動内容①

JAPAN SMARTPHONE SECURITY ASSOCIATION

スマートフォン利用シーンに潜む脅威 Top10 2023 解説ガイド

2023年、最近の傾向として 「スマートフォン利用シーンに潜む脅威 Top10 2023」を発表。2024年7月にはTop10 に基づいた「フィッシング」と「フェイク」の解説ガイドを発表するなど、続々と解説資料/コラムを公開中！

<Top 10 の特長>

- ここ数年大きな問題となっている「スミッシング詐欺」
- 技術の進化によって新たに課題となると予測される「ディープフェイク」
- JSSEC発足当時（2011年）から問題視されていた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」
- SNSなどの普及により顕著になった問題である「SNSフェイクニュース」や「誹謗・中傷」
- コロナ禍を経て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」

「フィッシング対策」
「フェイク対策」 など
Top10に関する資料

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	アプリストアのマルウェア感染
	不適切なパスワード管理
	スマホカメラの悪用
	短縮 URL 問題
	盗難・紛失

https://www.jssec.org/smartphone-use-10threats2023

具体的な活動内容②資料の例

JAPAN SMARTPHONE SECURITY ASSOCIATION

挿絵や画面ショットを交え、ガイドやコラムで分かりやすく解説！

● Top10 解説ガイド（No.1：フィッシング）

スマートフォン利用シーンに潜む脅威Top10 解説ガイド（No.1：フィッシング） | JSSEC

※資料抜粋

【第一回】フィッシング・スミッシング メール対策

JSSECの利用部会では、2023年2月に「スマートフォン利用シーンに潜む脅威 Top10 2023」を公開しました。このTop10の中から、特に注目度の高い内容について「初動」や「気付き」に重点を置いて解説したガイドを作りましたので、ぜひご参照ください。

第一回は、「フィッシング・スミッシング メール対策」です。

本ガイドは、「人」と「情報」に焦点を当て、「被害にあわないための対策と被害にあった時の対応」で構成されています。具体的には、それぞれの脅威に遭遇したことがあるか、その時どうしたのか、なぜその問題に気付いたのか、本当はその時どうすれば良かったのか、など、「スマートフォン利用シーンに潜む脅威 Top10 2023」の選出のために開催されたワークショップで挙がった、日ごろの経験や初動、その時の気付きを中心にまとめています。
そしてガイドの締めくくりは、今後わたしたちはどのような点に注意してスマートフォンを利用すれば良いのか、利用者視点の分かりやすい提言で結んでいます。

■「スマートフォン利用シーンに潜む脅威 Top10 2023」ガイド 【第一回】フィッシング・スミッシング メール対策
https://www.jssec.org/dl/jssec_PhishingCountermeasureGuide_20240625.pdf

＜「フィッシング・スミッシング メール対策」ガイドから抜粋＞

図 2-1 フィッシングを取り巻く、「情報」と「人」の相関図

● 強化された！～ iOS18 のパスワード管理

資料公開「強化された！～ iOS18のパスワード管理」 | JSSEC

※資料抜粋

さらに図 5 で示す通り、「すべて」の画面のアカウントを選択すると、各アカウントのパスワードの設定方法も確認できます。サービス登録時に、パスワードを自動設定した場合は「強力なパスワード」、利用者が個別に設定した場合は「カスタムパスワード」、Apple アカウントを使ってログインなら「Apple でサインイン」、と表示されます。

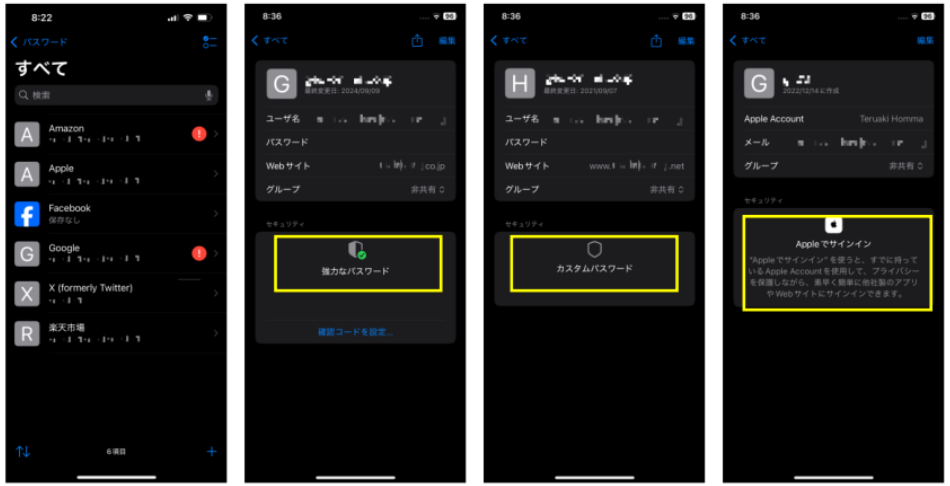

図 5　iOS18 各パスワード画面

また、設定しているパスワードにセキュリティ上の問題があると考えられる場合には、図 6 の「すべて」の画面で黄

具体的な活動内容③
セキュリティチェックシート

NIST-CSF2.0
対応へ改訂中！

JAPAN SMARTPHONE SECURITY ASSOCIATION

組織へIoTを導入する場合のセキュリティ検討事項

JSSEC IoTセキュリティチェックシート

- NIST-CSFの分類：5機能 23カテゴリ（識別/防御/検知/対応/復旧）
- 企業のIoT推進者や管理者の視点で検討すべき点：60項目
- IoT用途レベル毎の推奨項目：3つの重要度に分類
- 各社の検討内容　採用理由／追加項目：検討結果の見える化
- 検討主体（IT又はOT）及び、連携（ITとOT）が重要な項目を明記

動画セミナー「IoTセキュリティチェックシート入門」公開中

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徴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

https://www.jssec.org/iot-youtube

スマートフォンセキュリティ

スマートフォンセキュリティ対策チェックシートⅡ

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 ～50 項目で簡潔！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WGからのご案内

JAPAN SMARTPHONE SECURITY ASSOCIATION

参加者募集！

■**概要：**IoTセキュリティチェックシート更新のためのメンバーを募集中です。

■**日時：**日程: 2026年02月下旬 ~ 3月上旬ころを予定

■**場所：**調整中

■**内容：**IoTセキュリティチェックシートCSF2.0対応のための意見交換

・第一回WSの議論を反映した既存項目分類案に対する意見交換

・現行の項目見直し、および、新規項目案に対する意見交換（メイン）

例）CSF2.0機能毎のサブカテゴリ（例: GV.OC-01）ベースでの議論を想定

■**ご連絡先：**ご参加希望の方はこちらまでお願いします。➡ **sec@jssec.org**

議論の進め方：例）統治(GOVERN)

JAPAN SMARTPHONE SECURITY ASSOCIATION

（Govern）

- **論点：組織の「共通ルール」と「現場の制約」の合意**

  既存のチェックシートは「現場での対策」に寄せているが、
  それを支える組織の方針がITとOTで食い違うことが多い。

- **リスク許容度の定義（GV.RM-02）：**

  「安全」を優先してラインを止めるのか、「稼働」を優先してパッチ適用を遅らせるのか、その判断基準を経営層と合意する。

- **サプライチェーンの出口戦略（GV.SC-01）**

  IoT機器は利用期間が長いため、ベンダー倒産やサービス終了時に
  どう事業を継続するかという長期的な戦略。

- **リソースの適正化（GV.RR-03）**

  導入予算だけでなく、5年後・10年後のメンテナンスや廃棄にかかるコスト・人員が確保されているか。

スマホ脅威Top10 2026 選出について

JAPAN SMARTPHONE SECURITY ASSOCIATION

■背景

- 2011年のJSSEC設立以来、スマートフォンはこの15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

↓

「3年毎の見直し」として2026版を選定中

【方法：ワークショップ＆投票】

本日、
特別に投票受付中！

Top10 選出候補20①

JAPAN SMARTPHONE SECURITY ASSOCIATION

候補１：フィッシング・偽メール詐欺

個人のメールアドレスに偽のメールやSMSが届き、リンクや添付ファイルをクリックさせて情報を盗む手口。特にAIの技術進歩により、精巧な偽物が作成されやすくなっている。

候補２：スミッシング（SMSを利用したフィッシング）

宅配便や荷物受取を装ったSMSを送り、リンクをクリックさせて偽サイトに誘導。巧妙な偽QRコードや短縮URLを用いた攻撃がある。

候補３：ビッシング（電話を用いた詐欺）

警察などの公共機関や金融機関を名乗る偽の電話をかけ、個人情報や口座情報を引き出す。AIや偽番号を使った巧妙な手口が増加。

候補４：ロマンス詐欺・投資詐欺・リクルーティング詐欺（SNSを使った詐欺）

SNSやマッチングアプリを通じて知り合った相手を騙し高額な投資や金銭を要求。生成AIを活用しよりリアルな偽の人物やシナリオを作成。

候補５：生成AIによるフェイク動画・音声）

有名人や関係者の声や顔を模倣したフェイク動画や音声を生成し、誤情報や詐欺に利用。生成AIを使ったディープフェイクの進歩により、見分けがより困難になっている。

候補６：QRコードを用いた詐欺（クイッシング）

偽のQRコードを貼り付けるなど、不審なサイトへアクセスさせて不正送金を誘導。巧妙な偽造や貼り替えにより見抜くのが困難。

10

Top10 選出候補20②

JAPAN SMARTPHONE SECURITY ASSOCIATION

候補７：盗撮・プライバシー侵害

スマートフォンのカメラや位置情報を悪用した盗撮や監視。学校や公共の場での盗撮動画が拡散。

候補８：オレオレ詐欺・なりすまし

電話やSMSを用いたオレオレ詐欺やなりすまし。電子音声やAIによるなりすましも増加。

候補９：悪意ある広告・偽商品販売

偽の投資広告や商品詐欺、タイムリーな偽情報をSNSやYouTubeで拡散。偽のコマースサイトや投資サイトに誘導。

候補１０：セクストーション・リベンジポルノ

個人の私的な画像や動画を脅しや悪用により流布。スマホの便利さとともに、被害の拡大や心理的影響が深刻化。

候補１１：アプリの提供元不明・非正規マーケットからのマルウェア感染

正規のアプリストア以外からDLしたアプリにマルウェアが仕込まれるケース。審査を通過したアプリも、穴をついて不正コードを埋め込む例が増えている。

候補１２：正規マーケットからのマルウェア感染

正規マーケット(AppStore/GooglePlay)の審査を掻い潜り、マルウェアをインストールさせる攻撃。ユーザの知らないうちに感染し情報盗取や遠隔操作される。

候補１３：生体情報の窃取・悪用

指紋、顔写真、声などの生体情報を不正に取得し、生成AIで声や顔を複製。これを用い、スマホの生体認証を突破したり、詐欺やなりすましに利用する。

ワークショップ考察①

JAPAN SMARTPHONE SECURITY ASSOCIATION

➢ 社外を名乗る巧妙なフィッシングと新たな入口、見抜きにくい時代

・フィッシング／スミッシングが最大脅威。認証情報の窃取や情報漏洩が現実劇なリスク。
・文面が自然で“**もっともらしい人物像**（例：社長、警察、行政）”を装うケースが増加。
・SMSは**差出人判別が困難**で、メール以上に見抜きづらい。
・ロマンス詐欺はチャネル増加により成立しやすくなっている。
・多忙な現場に緊急性を装うなど、心理を利用したり隙をつく“**それっぽいシナリオ**”も巧妙。
・古い業務端末（例：古いWindows環境）が狙われやすいとする議論も。
・QRコード詐欺（クイッシング）は**生活導線にQRが浸透**しているため被害リスクが高い。
・偽広告・偽商品は**意図しないタップやスクロールが“入口”に**なりうる。
・生成AIによるフェイク動画・音声で被害が加速する可能性。
・規制緩和による**正規ストア由来アプリによるマルウェア混入**の懸念。

➡AIの活用と接触チャネルの増加で見抜きにくい嘘、詐欺。時代にあった意識改革と対策を。

詐欺が“自然すぎる”時代――想像を超える手段と入口の増加で見抜き難易度UP

ワークショップ考察②

JAPAN SMARTPHONE SECURITY ASSOCIATION

➢ フィッシングは生成AIで高度化。複合型詐欺へ発展

・スマホ脅威の中心は、以前「フィッシング」
・認証情報窃取・不正送金など**被害が大きく**なる傾向
・**入口は多様化**＝メール、SMS、SNS・・・
・**生成AI**により文面や偽サイトが自然になり、見抜きづらさが増大。
・オレオレ詐欺が多角化。AI音声・SNS・ビデオ通話をフル活用してBtoBの指示型詐欺に発展。
・LINEグループ誘導など、**企業統制の外で詐欺が進行**するケースへの懸念。
・パスワード使い回し、多要素認証未利用など**“古い弱点”が依然残る**。
・パスキーなど仕組みによる防御の重要性。
・ブラウザ拡張の悪用、ダークパターン、サイドロード、マイナカード搭載など新しい視点も。

➡複合的な手口（アナログ×デジタル）が増加。利用者・企業双方で備えの更新が必要

生成AIで“見抜けない”フィッシングへ――スマホ起点の複合型詐欺に備える

ワークショップ考察③

JAPAN SMARTPHONE SECURITY ASSOCIATION

➢ 攻撃者の心理を読む。「低コスト×高成功率」＋利用シーン

・攻撃者は、コストと成功率を基準に手法を選ぶ。
・フィッシングは**生成AIにより低コストかつ巧妙化**しており、最優先の脅威。
・メールを起点にApple ID等の重要アカウントを奪うインフォスティーラー(認証情報窃取)の増加。
・SNS広告や偽QRなど、**日常導線に攻撃が紛れ込む形**が増えている。
・サイドロード、アプリ審査すり抜け、iOSショートカット悪用など**多様な入口**。
・会社端末はMDMで統制、個人端末はフィルタリング／通信監視／アップデートが現実的。
・**認証基盤（Apple ID等）保護**が重要。

➡端末の位置づけと利用シーンを考慮した対策が現実解。”鍵”となる認証基盤保護は重要

攻撃者は「低コスト×高成功率」を選ぶ――フィッシング優位と導線型リスク

ワークショップ考察④

JAPAN SMARTPHONE SECURITY ASSOCIATION

➢ 中高生の“リアルな被害”から見える現在地

・若年層の生活は**スマホ中心**
・SNSアカウント乗っ取りなど**“なりすまし”が身近**な脅威。
・占いアプリなど**非典型の入口**も存在。
・いずれにしても**認証情報奪取**がランサム被害につながる。パスキー普及は重要。
・SMSやSNSのDM誘導（怪しいバイト、脅し（写真から住所を匂わせる））への**耐性が低い**。
・知らない人と繋がる**心理的抵抗が低い**。
・親世代が実態を理解しづらい**ギャップ**が課題。アンケート調査も有効。
・APKサイドロード、root化、AI音声悪用、画像生成悪用など**新旧の脅威が混在**。
・私的情報の拡散(復讐的ポルノ、いじめ動画)等、“撮れる/送れる”という**スマホ特性が被害を助長**
・生体認証依存のリスク、企業利用での内部不正（カメラ・録音等）も論点。

➡世代間の心理的抵抗感や理解度の違い、企業での不正利用。人と運用を考慮した対策が必要

中高生の“ヒヤリハット”が映す、スマホ脅威のいま―なりすまし・DM誘導・AIの影

ワークショップ考察⑤

JAPAN SMARTPHONE SECURITY ASSOCIATION

➢ AIが詐欺を産業化する現実と「通信の秘密」のジレンマ

・**AI技術の悪用**による詐欺全般（スミッシング・ビッシング・ロマンス詐欺等）の**質・量の拡大**
・**手口の多様化**～スミッシング（SMS）、ビッシング（電話）、ロマンス／投資／リクルーティング詐欺、オレオレ詐欺・なりすまし。
・個人のみならず企業もターゲット。CEO詐欺のように、**なりすまし成功で一気に被害拡大。**
・AIによる半自動化により、**利用者が真偽を見抜きにくい**状況が加速。
・将来的にはフェイク動画・偽音声により**本人確認自体が揺らぎかねない。**
・防御側は、通話アプリの対策が限定的（過去の詐欺番号通知程度）
・AIで通話解析を行う方向性はあるが**「通信の秘密」が壁**に（法的/倫理的）
・社会全体がAI生成コンテンツ多数派になる「インプレッションゾンビ」状態も懸念。

➡AI悪用や倫理的課題への対処として、政策提言等も含めた社会的ルール作りが必要。
技術と社会の両面から備えを更新。

AIが詐欺を“産業化”する――高度化する手口と「通信の秘密」「法」「倫理」

ワークショップ考察：まとめ①

今どんな状況？

➡生成AIがエンジンとなり詐欺技術を底上げして、特にフィッシングが大進化

- フィッシング／スミッシングが依然として脅威の中心。
- 心理を利用するなど成功率UP。
- 目的は認証情報奪取、アカウント乗っ取り、不正送金
- 入口はメール・SMS・SNS・広告・QR・アプリなど多様化し、見抜きづらくなっている。
- 「アナログ＋デジタル」で詐欺が巧妙化
- 個人被害だけでなく、組織へのなりすまし・指示型詐欺も増加。
- 若年層はSNS乗っ取り・DM誘導が中心、世代によって“刺さる入口”が異なる。
- **生成AI**により、詐欺の「自然さ」「大量展開」「多様性」が強化されている。

ワークショップ考察：まとめ②

JAPAN SMARTPHONE SECURITY ASSOCIATION

対策は？

➡「リアルな生活とデジタルは融合している」ことの世代別啓発
＋技術＋社会制度

- 意識の**更新**：啓発➡「過去といまの違い」
- 技術の**更新**：パスキー／多要素認証、MDM、アップデート、
  通信監視などの多層防御、AI悪用対策
- 制度の**更新**：AIによる新しい脅威に対する制度面の整備（通信の秘密、社会ルール）

※啓発・・・利用シーン別、世代別のアプローチ
古くから指摘されているパスワード運用などの再啓発も必要
典型と非典型の手口があることの認識

JSSECは、各種活動を通して貢献していきます。

ご清聴ありがとうございました。

JAPAN SMARTPHONE SECURITY ASSOCIATION

詳細はこちら

JSSEC

https://www.jssec.org