■『セキュリティフォーラム2023 オンライン』資料

【新発表】
スマートフォン利用シーンに潜む脅威 Top10 2023

2023年 3月1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　松下 綾子　（ALSI）

はじめに～

JSSEC 利用部会　活動紹介

活動紹介：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する。又、**近年のスマートフォン利用形態の変化に合わせて、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、事例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

「スマートフォン利用シーンに潜む脅威 Top10　2023」選出までの道のり

JAPAN SMARTPHONE SECURITY ASSOCIATION

2020年度・2021年度、
コロナ禍でワークショップ活動は縮小せざるを得ない状況
各種施策を手探り⇒YouTube活用など実践

↓

2022年度、人の輪と知恵をつなぐ機会をもっと創出しよう！

↓

脅威選出のワークショップを開催！ ※オンライン

①第一回WS　2022年9月開催～**身近な脅威の洗い出し**
②第二回WS　2023年1月開催～**意見交換と投票**

参考～第一回ワークショップのコラム

JAPAN SMARTPHONE SECURITY ASSOCIATION

第一回WSのコラムはこちら。

https://www.jssec.org/column/20221222.html

第二回目のコラムも
準備中！お楽しみに！

スマートフォン利用シーンに潜む脅威
Top10　2023

新発表

その前に・・・
JSSEC「2013年スマホ5大ニュース」

JAPAN SMARTPHONE SECURITY ASSOCIATION

覚えてますか～

2013年12月25日発表

順位	JSSEC選出の5大ニュース	
1	**スマートフォン プライバシー イニシアティブ**（総務省がまとめたスマートフォンでプライバシーを取り扱うための指針）	＜選出理由＞ **スマートフォンのプライバシーに関する多大な貢献をした**
2	**スマートフォンを狙った標的型攻撃が現実の脅威に**	＜選出理由＞ **昨年に発表されたスマートフォンを狙った標的型攻撃が現実のものとなった**
3	**シニア層に対するスマホ訴求が激しくなる**	＜選出理由＞ **テレビ番組でシニア層向けのスマートフォン使い方番組が始まった**
4	**トラブル続出！歩きスマホ族の横行**	＜選出理由＞ **ながらスマホの危険性を告知する鉄道各社がキャンペーンを開始した**
5	**iOSでも起こるヒヤリ・ハット**	＜選出理由＞ **Apple IDを狙ったフィッシング詐欺が急増した**

第一回WSで洗い出した脅威項目

JAPAN SMARTPHONE SECURITY ASSOCIATION

- 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詐取
- 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

皆さんの経験から「利用シーン」毎に選出

投票結果発表

JAPAN SMARTPHONE SECURITY ASSOCIATION

投票結果発表

JAPAN SMARTPHONE SECURITY ASSOCIATION

ディープフェイク

投票結果発表

なりすまし契約と
アカウント詐取

ディープフェイク

投票結果発表

依然猛威を振るう
スミッシング詐欺

なりすまし契約と
アカウント詐取

ディープフェイク

第一回WSで洗い出した脅威項目

JAPAN SMARTPHONE SECURITY ASSOCIATION

スマートフォン利用シーンに潜む脅威 Top10 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 （同率）	提供元不明アプリによるマルウェア感染
	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

フィッシングとスミッシング

JAPAN SMARTPHONE SECURITY ASSOCIATION

■違いは・・・下記表参照

■対策は・・・比較的認知度の低いスミッシングに要注意！
キャリアでもフィルターしているが、個人での用心が大切。

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

なりすまし契約とアカウント詐取

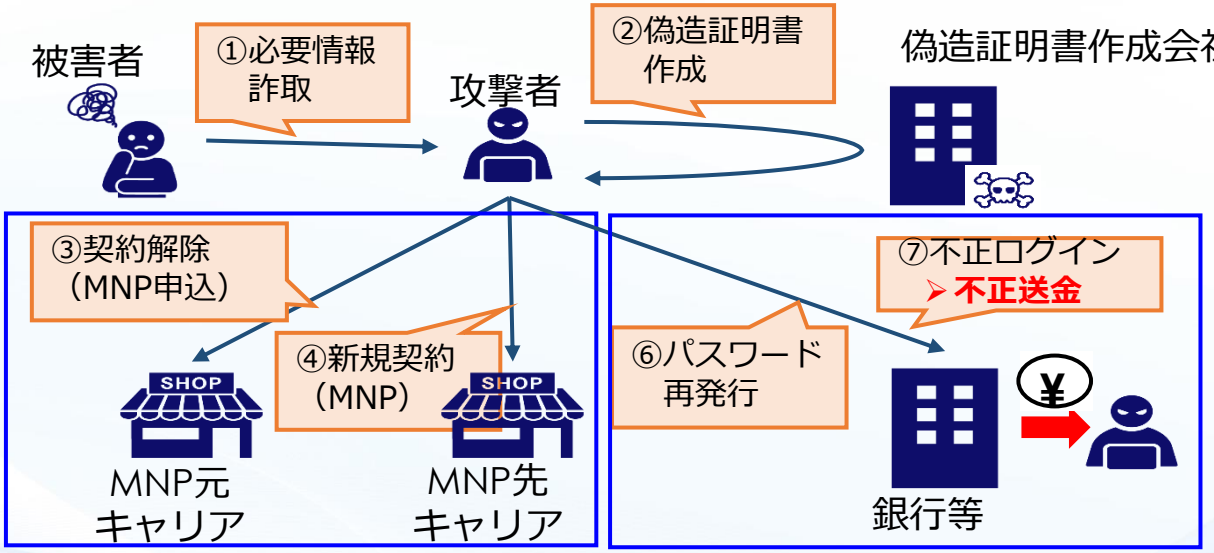
JAPAN SMARTPHONE SECURITY ASSOCIATION

■手法は・・・例えばMNPの悪用

なりすましのターゲットとする人の情報を入手し、入手した情報で偽造証明書を作成し、偽造証明書を使ってなりすまして契約を行う。

■対策は・・・

キャリアはマイナンバーカードのJPKIを利用して本人確認を厳格にする。
サービス提供者は、パスワードをSMSではない別の手段も考える必要あり。

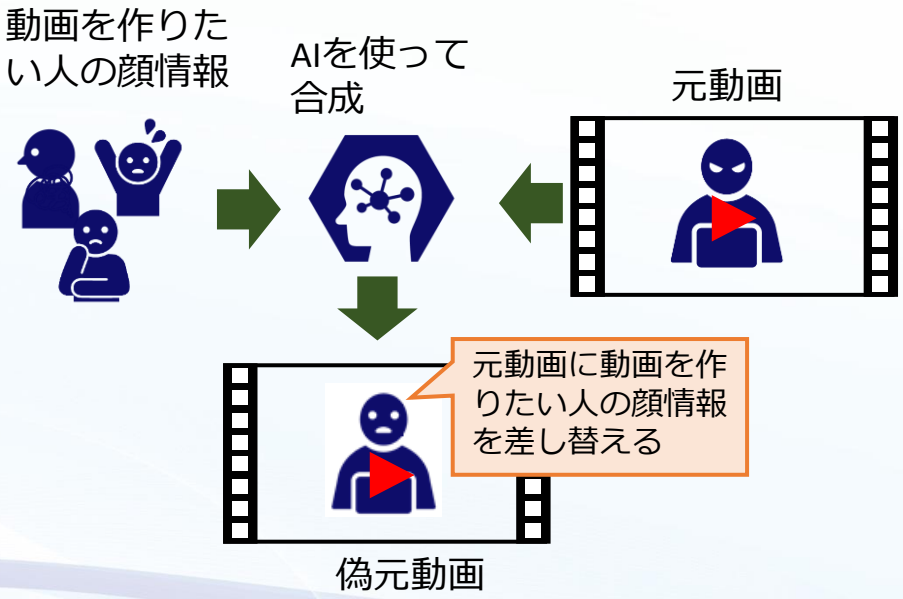


ディープフェイク

■手法は・・・動画や音声の合成技術。作成アプリも流通している。

主に著名人の人物画像を合成し、あたかも本人が発言したように発信したり、発生していない事象を現実に起きた事象のように発信したりして、不特定または特定の人を狙って騙す。

■対策は・・・技術的対策が期待される。さらに、法的対策も注目されている。



ワンポイント考察

JAPAN SMARTPHONE SECURITY ASSOCIATION

選定された脅威の背景は・・・

■**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**手法**「スミッシング詐欺」

■**技術の進化によって新たに課題となってくる**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」

■**多くの利用者がご存知ないかもしれない**「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**が求められるため、
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。

意見交換内容の一例

JAPAN SMARTPHONE SECURITY ASSOCIATION

■「フィッシング・スミッシング」については、やはり重大な問題であることが共通の認識だった。**家族などに注意喚起をしておく**と、怪しいメールを受け取った際に確認の連絡をもらるので、啓発して危機感を持ってもらうことは重要。

■なりすまし契約や不正アプリと同様に、**一人で生活していると「フィッシングかどうかの判断」が難しい**という指摘があった。

■「検索エンジンの汚染」については、人に言えないキーワードで引っかかるケースが多いので相談しにくいという意見がある一方で、**正しいキーワード**でも起きるという話もあった。これに関連して、マルウェアサイトなどに誘導する**怪しい広告**も話題に上った。**怪しい広告は、SNSでも表示される**ので、根深い問題。

■「短縮URL」は悪いことではないが、そもそも**URLが表示されないスマホ**も増えている。**果たしてそのサイトから新規ID登録をしていいのか、正しいサイトかどうかの見極めが難しい**という意見があった。スミッシングと合わせて考えると非常に大きな問題。

その他のご意見は、ぜひ
第二回ワークショップコラムをご参照ください。

ありがとうございました。

ぜひ一緒に活動してみませんか！
お待ちしております。

JSSEC 事務局
sec@jssec.org

JAPAN SMARTPHONE SECURITY ASSOCIATION

成果物一覧はこちら➡

https://www.jssec.org/report