サイバーセキュリティニュース（平成31年4月分）

（発出：令和元年5月　函館方面サイバーセキュリティ連絡会議事務局）

【目次】

１　脅威（手口）

○ まだまだ続く偽佐川
次の手口はｉＯＳ端末に構成プロファイル

情報処理推進機構（ＩＰＡ）は公式ホームページ（ＨＰ）で、佐川急便をかたる偽ＳＭＳの新たな手口を公開した。佐川急便をかたる手口は、これまでｉＰｈｏｎｅなどのｉＯＳ端末でアクセスした場合フィッシングサイトに誘導し「電話番号と認証番号」や「ＡｐｐｌｅＩＤとパスワード」を入力させる手口だったが、本年３月ごろから、不審な構成プロファイル（※）をインストールさせてからフィッシングサイトに誘導する手口が確認されるようになったという。不審な構成プロファイルをインストールした場合「端末内の設定が変更される」「端末の固有情報が外部に送信される」といった可能性が考えられるが、それによる具体的な被害や影響は現時点で判明していない。

ただ、その後の誘導先フィッシングサイトでＡｐｐｌｅＩＤとパスワードを入力してしまうと、ＡｐｐｌｅＩＤで利用できるサービスを悪用される危険性がある。

※構成プロファイル～ｉＰｈｏｎｅの各種設定を自動で行うためのファイル

【被害に遭わないために、ＩＰＡでは下記の対策を挙げています。】

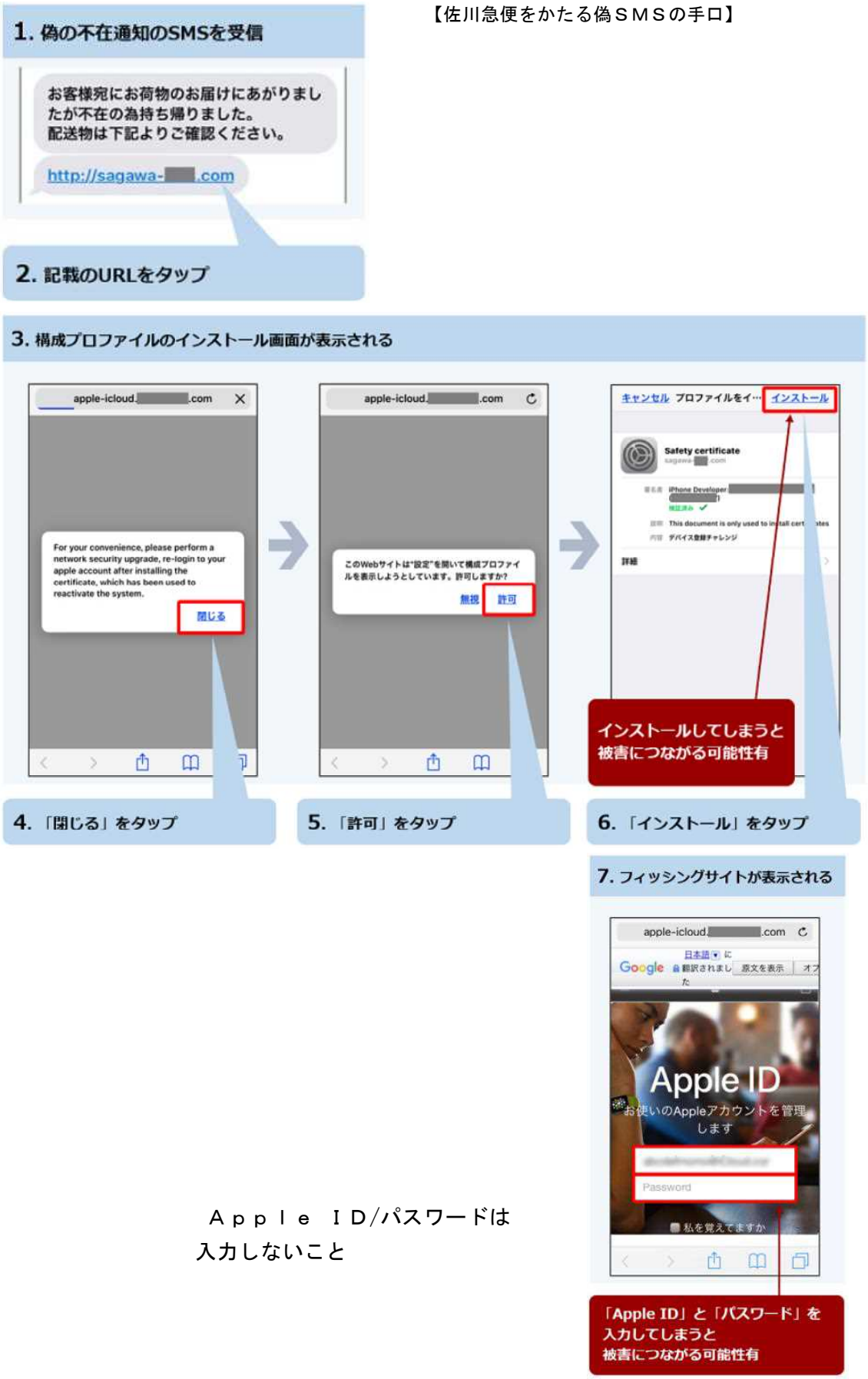
○　佐川急便をかたる不在通知のＳＭＳが届いた場合はＵＲＬリンクをタップしない。（佐川急便ではＳＭＳによる案内を行っていないとＨＰで公表している。）

○　ＵＲＬリンクをタップし、構成プロファイルのインストール画面が表示された場合は、「無視」または「キャンセル」をタップして画面を閉じる。

○　構成プロファイルをインストールしてしまった場合は、外部への情報送信の可能性を考慮し、すぐにスマホを機内モード（ＷｉＦｉもオフ）にした後、端末を初期化する。（推奨）

○　フィッシングサイトにＡｐｐｌｅＩＤとパスワードを入力してしまった場合は、速やかにパスワードを変更する。

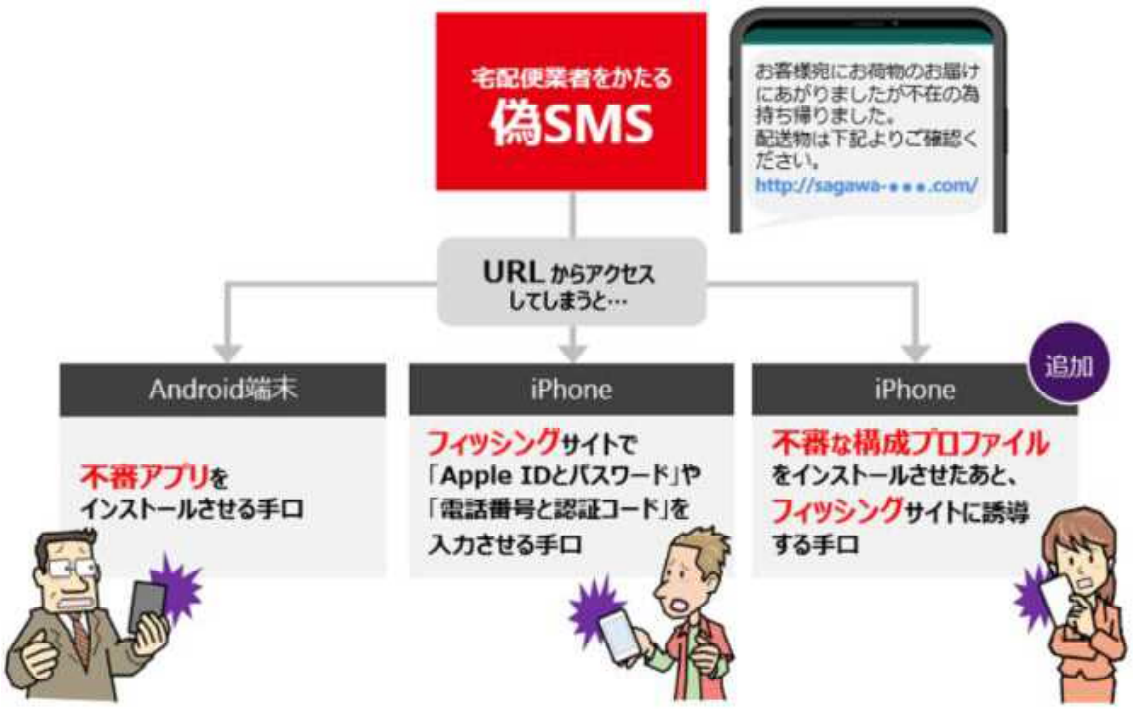
【佐川急便をかたる偽ＳＭＳの手口】



Ａｐｐｌｅ ＩＤ/パスワードは
入力しないこと

【不審な構成プロファイルのインストールまでの流れ】

画像引用元：ＩＰＡのＨＰ（https://www.ipa.go.jp）



○ 新元号に便乗　携帯大手３社をかたる偽メール

新元号「令和」が発表された４月１日以降、携帯大手３社をかたった「新元号に伴う新プラン」などと称する偽メールが出回っているとして、携帯大手３社はＨＰやツイッターで注意喚起した。偽メールは「新元号に伴い新プランへ移行となる」（ＮＴＴドコモ）、「新元号に伴い全額キャッシュバックキャンペーンを実施する」（ソフトバンク、ＫＤＤＩ）といった内容で、いずれもメール本文中のＵＲＬリンクから別のサイトへ誘導する手口となっている。携帯大手３社では、こうしたメールを配信しておらず、偽メールを受信した場合は本文中のＵＲＬリンクをクリックしないよう注意喚起している。

道警に寄せられた警察相談では、大手通販サイトアマゾンをかたり、新元号に伴うセキュリティの更新名目で、個人情報やクレジットカード情報の入力を求めるＳＭＳが確認されています。

「新元号に伴う○○」という内容のメールやＳＭＳが届いた場合の対処法

○安易にＵＲＬリンクをクリック（タップ）しない。

○個人情報やクレジットカード情報等を入力しない。

○正規のホームページ等でメールの真偽を確認する。

○ ネット闇市場で流通するクレカ情報 限度額高いほど高値で取引

デロイトトーマツサイバーセキュリティ先端研究所（東京）は平成３０年末、ダークウェブ上で５万件近くのクレジットカード情報を販売する闇市場サイトを発見した。カード情報は、カード番号、国、発行会社、有効期限、限度額、セキュリティコードなどの項目で整理され、検索することも可能だった。売られているカード情報の国は米国や欧州、アジアなど様々だが、日本が半数の約２万５千件を占めていた。価格はおおむね１件当たり１０～６０米ドルで、５ドル以下の格安品から１００ドル以上の高級品まであった。国や発行会社の信用度、利用限度額が高いほど高額になり、有効期限が迫ったものは安価になるなど値付けも工夫されているという。同研究所では「盗んだカード情報を自分で使うより他人に売った方が摘発されるリスクは低く、世界各地のハッカーが情報を持ち込む場となっている」とみている。カード情報を盗み取る手口には、企業のシステムに不正侵入して顧客情報をまとめて盗み出す手口のほか、フィッシングサイトに誘導してカード情報を入力させる手口もある。セキュリティ大手シマンテックによると、「フォームジャッキング」という新たな手口が最近目立つという。通販サイトを外部から改ざんし、利用者が入力した情報を外部に送信する手口で、平成３０年９月には、英国の航空会社のサイトが改ざんされ、カード情報など約３８万件の顧客情報が流出した。そのほか、店舗のレジにあるカード読み取り機器に不正プログラムを仕込み、読み取った情報を外部送信する「ＰＯＳマルウェア」という手口もあるという。

クレジットカードを利用するに当たっては

〇不審なサイトで不用意に情報を入力しない

〇利用明細をよく確認して身に覚えのない支払いがあればカードを停止する

といった対策のほか、「３Ｄセキュア」と呼ばれるネット決済専用のパスワードを設定することで安全性が高まるという。

○ 中国で偽ＱＲコードを使った詐欺が横行

飲食店の支払いや飛行機の搭乗手続きなど、日本でも様々なところで使われるようになってきたＱＲコード。ＱＲコード先進国といわれる中国で偽造ＱＲコードを使った詐欺が横行している。中国北京では、交通違反の反則金の納付方法の一つとして、ＱＲコード決済が取り入れられている。警察官が違反者に交付する違反切符にＱＲコードが付されており、スマホ等でこのＱＲコードをスキャンすることで反則金を納付することができる。中国で横行し

ているのは、ＱＲコードが付された偽物の違反切符を利用した手口で、駐車違反の車両に偽物の違反切符を貼り付け、ＱＲコードをスキャンして反則金の納付を求める。違反者が偽物と気付かずＱＲコード決済すると、犯人のアカウントに送金することになる。違反切符のほかにも、ＱＲコード決済が普及する中国では、街中の青果店や屋台などでも店先に決済用のＱＲコードを掲示しており、店先のＱＲコードを偽物のＱＲコードにすり替え、店の売上げをだまし取る手口もあるという。

○ ネットに広がる中傷・嘘・迷惑投稿

ツイッター 道知事選への中傷６５０件

道知事選（４月７日投開票）について、北海道新聞社がツイッターの書き込みを分析したところ、両候補者に対する根拠に乏しい批判や中傷を含む投稿が相次いでいたことが分かった。ＳＮＳの情報解析を行う企業に委託し、投開票日までの１か月間、道知事選に関する書き込み約１２万件の中から、書き込みを引用して転載するリツイートを除いた１万２千件を分析したところ、「犯罪者」「売国奴」など候補者を中傷する書き込みだけで６５０件も確認された。なかには、コンピュータプログラム「ＢＯＴ（ボット）」によって、中傷などの書き込みを繰り返し発信、拡散させたとみられるものも約１６０件あったという。

ＹｏｕＴｕｂｅ（ユーチューブ） 渋谷スクランブル交差点にベッド

渋谷スクランブル交差点にベッドを置く様子を撮影した動画が、動画投稿サイト「ユーチューブ」に投稿された。動画には、歩行者用の信号が青のときに、男性が寝そべった状態のベッドを別の男性４人が持ち上げて運ぶ様子が映されていた。警視庁渋谷署が道交法違反容疑で捜査に乗り出したところ、投稿した人気ユーチューバーが出頭したという。

ツイッター 地下鉄の閉まるドアに何度も手を挟み発車を妨害

名古屋市営地下鉄で、高齢男性が地下鉄の閉まるドアに繰り返し手を挟むなどし、発車を遅らせる様子を撮影した動画がツイッターに投稿された。市交通局によると、男性は７、８回にわたり、手を挟んだり、足でドアが閉まるのを妨げたりした。この影響で発車が約１分遅れたという。

ツイッター 「人が刺された」嘘動画

「人が刺された」と嘘の動画をツイッターに投稿したとして、警視庁町田署は軽犯罪法違反（虚偽申告）の容疑で町田市内の男女４人を書類送検した。

容疑は、暗闇で人が倒れている様子が映った動画とともに「人が刃物で刺されたみたいです。犯人はまだ捕まっていません」などと嘘の内容をツイッターに投稿した。ツイッターを見た人から１１０番通報があったほか、ネット上では情報提供を呼びかける内容が拡散されたという。

２　技術

○　警視庁開発　無料防犯アプリ「デジポリス」　２２万件ＤＬ

警視庁が開発したスマホ用無料防犯アプリ「Ｄｉｇｉ　Ｐｏｌｉｃｅ（デジポリス）」が、平成２８年３月の配信開始から約２２万件ダウンロードを突破した。「痴漢撃退」や「防犯ブザー」などの機能が評判となり人気を集めている。痴漢撃退機能を起動し、画面をタップすると「やめてください！」とスマホから大声が出る。画面には「痴漢です 助けてください」の文字が表示され、怖くて声が出せなくても助けを求めることができる。防犯ブザー機能は、画面のベルの絵を一度タップするだけで、スマホの最大音量で電子音が鳴り響く。どちらの機能も、あらかじめ登録したメールアドレスに通知や位置情報を送ることができ、家族や保護者にも身の危険を伝えることできる。

そのほか、事前登録した地域の犯罪発生情報の表示や、「子どもと女性の安全」コーナーとして現在地から最寄りの警察署や交番、周囲のコンビニ店への道筋も表示できる。

交番や犯罪発生情報は都内に限られるが、痴漢撃退機能や防犯ブザー、防犯対策のページは誰でも活用できる。デジポリスは、当初は詐欺被害への注意喚起や不審者情報が主な内容だったが、大学教授で作る有識者会議から「子どもや女性の安全対策として更なる普及・改善を図ることが望ましい」との指摘を受け、スマホ世代の若年層が利用しやすいよう全面改修した。

都内の企業から「女性社員のスマホにアプリを入れたい」との問合せもあったという。

【痴漢撃退機能や防犯対策などの機能が備わっている。】

デジポリスは、警視庁ＨＰ（https://www.keishicho.metro.tokyo.jp）などからダウンロードできます。

３ 国内外のサイバーセキュリティ情勢

○ サイバー攻撃情報を官民共有 サイバーセキュリティ協議会発足

政府は４月１日、サイバー攻撃に関する情報を官民で共有する新組織「サイバーセキュリティ協議会」を発足した。東京五輪などの国際イベントを控え、重要インフラや政府機関などを狙ったサイバー攻撃への対処能力を強化する。協議会は、国の行政機関に加え、教育研究機関、地方公共団体、重要インフラ事業者、サイバーセキュリティ事業者などで構成され、サイバー攻撃があれば、専門機関や企業による「タスクフォース」が中核となって攻撃の手口や対応策を話し合い、構成メンバーに情報提供する。攻撃を受けた疑いがある早い段階から情報共有することで初動対応や予防能力の向上を図る。

構成メンバーには情報提供を義務づけ、秘密情報を不当に外部に漏らすと１年以下の懲役または５０万円以下の罰金とする罰則も設けた。タスクフォースへの外資系企業の参加は原則認めないとしている。

政府がサイバー攻撃に関する官民の情報共有体制の強化に動き出す契機となったのは平成２９年に１５０か国で感染が確認されたコンピュータウイルス「ワナクライ」だった。日本では、日立製作所やＪＲ東日本、川崎市など自治体でもワナクライの被害が確認された。被害が拡大した背景には、企業がワナクライの感染防止できる可能性のある対処方法に気づきながらも、対処方法が間違っていた場合の責任追及のリスクや風評被害をおそれ、情報共有が遅れたという。こうした反省が協議会の設置につながった。

○ 中小企業・ＮＰＯ向け情報セキュリティ指南書を公開 ＮＩＳＣ

内閣サイバーセキュリティセンター（ＮＩＳＣ）は４月１９日、「小さな中小企業とＮＰＯ向け情報セキュリティハンドブック」を公開した。これまでＮＩＳＣでは、一般向けに「インターネットの安全・安心ハンドブック」を作成・公開していたが、今回、セキュリティ担当者を置くことが難しい小規模企業やＮＰＯ（特定非営利法人）に焦点を当て、サイバーセキュリティを解説するガイドブックを作成した。

ガイドブックは、サイバー攻撃の説明から始まり、機器ごとの対処方法、対策の仕方、災害や海外渡航での備え、コストの捻出方法までを指南する内容となっている。

ＮＩＳＣでは、各組織の取組推進に使えるよう、ＰＤＦ・コピー・製本の無料配布、作業実費での販売、ページ単位・イラスト単位での利用、分割しての配布等についても対応しており、ＮＩＳＣの公式サイトでダウンロードできる。

【ＮＩＳＣ公式サイト】

(https://www.nisc.go.jp/security-site/files/blue_handbook/index.html

○ サイバー攻撃で流出した個人情報 平成３０年 ２６８万件

共同通信の集計によると、平成３０年にサイバー攻撃の被害を公表した国内企業などから流出、または流出したおそれがある個人情報が少なくとも２６８万件に上ることが分かった。国内１０４組織と、日本のホテルの予約サイト業務を受託しているフランス企業１社が被害を発表している。流出件数が最も多かったのは、コンサルティング会社エムエス・アンド・コンサルティング（東京）で、顧客のメールアドレスやパスワード、電話番号の計約５７万件が流出した可能性がある。

フランスのファストブッキングからは、日本のホテル各社関連で３２万５７１７件が流出した。名前や国籍、電話番号、利用日などが流出したという。

大学では弘前大、横浜市立大、立命館大、沖縄県立看護大など１４校から流出した。ＩＤ・パスワードが盗まれ、教員らのメールが外部に勝手に転送されたり、閲覧されるなどした。

三菱地所・サイモンや山梨県忍野村観光協会の被害では、流出した情報が海外の掲示板サイトに掲載されているのが見つかった。集計とは別に、米フェイスブックが平成３０年１０月、２９００万人分の情報流出を発表し、この中にも日本人の情報は含まれるとみられる。国内組織でも公表したのは一部であり、実際の流出件数はもっと多いとみられる。

○ サイバー攻撃の武力認定「米基準を参考」 防衛相初見解

岩屋防衛相は４月２６日、日本がサイバー攻撃を受けた場合の武力攻撃の認定について「物理的手段による攻撃と同様の極めて深刻な被害が発生し、国や国に準じる組織であろうと判断できる相手から組織的・計画的に行われた場合であれば、武力攻撃に当たり得る」とした上で、米国の認定基準も参考にする見解を示した。

米政府は、サイバー攻撃が武力攻撃に該当し得る事例として

〇原子力発電所のメルトダウン

〇人口密集地域でのダムの決壊
〇航空管制システムの不具合による航空機の墜落
を挙げている。

サイバー攻撃への対処としては、自衛隊がサイバー反撃することになるが、サイバー反撃だけでは敵の攻撃を止めることが不可能な場合、物理的手段も排除されないという。日本は敵基地攻撃能力を政策判断として保有していないため、ミサイルなどによる物理的な敵基地への反撃は、日米同盟に基づき米国が担う。