サイバーセキュリティニュース（平成31年2月分）

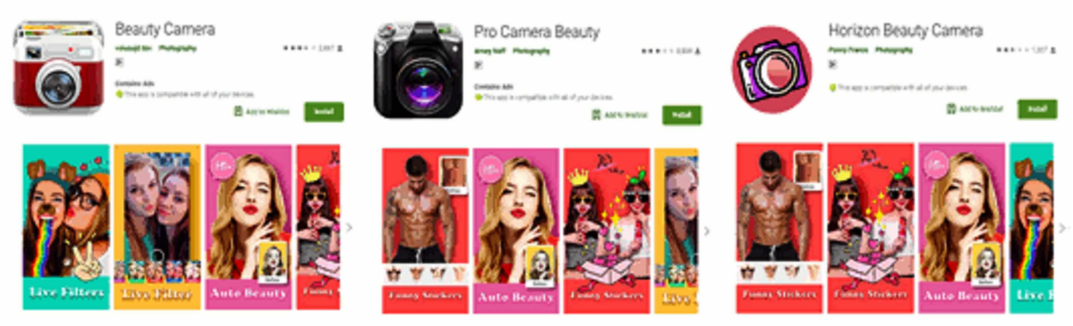
（発出：函館方面サイバーセキュリティ連絡会議事務局）

【目次】

１　脅威（手口）

○ カメラアプリを装う不正アプリ　ＧｏｏｇｌｅＰｌａｙで確認

トレンドマイクロによると、カメラアプリに偽装した複数のＡｎｄｒｏｉｄ端末向け不正アプリがＧｏｏｇｌｅＰｌａｙにあるのを確認したという。これらの不正アプリをスマホにインストールしてしまうと、ポップアップ広告が表示されるようになり、広告をタップするとフィッシングサイトやポルノアプリに誘導される。カメラアプリのほかにも、ユーザがアップロードした画像を窃取する、画像加工アプリに偽装した不正アプリも確認された。これらの不正アプリはＧｏｏｇｌｅＰｌａｙから削除されているが、すでに百万回以上ダウンロードされたものもあるという。



GooglePlay で確認された不正なカメラアプリ
画像はトレンドマイクロウェブサイトから引用（https://www.is702.jp/）

○ ＳＮＳを悪用した薬の不正取引 東京都が公開警告へ

ツイッターやフリマサイト（フリーマーケットサイト）を悪用して、処方箋が必要な向精神薬や避妊薬などを売買する不正取引が横行している。手口は、販売者がツイッターを通じて購入者を募り、実際の取引はフリマアプリで別の商品を装って行うというもの。販売者はまずツイッターに宣伝を投稿し、ダイレクトメッセージ機能を使って購入希望者と売買交渉を行う。実際の取引はフリマサイトを利用して別の商品の出品を装って医薬品代を決済させた後、医薬品を発送するという流れ。今年１月、この手口を使って未承認の緊急避妊薬（アフターピル）を無許可販売したとして、仙台市の男が医薬品医療機器法違反容疑で警視庁に逮捕された。フリマサイト運営各社では不正取引の監視を強め、問題のある出品者のアカウントを凍結するなどの対策を続けているが、学生や主婦など若い世代を中心に、口コミで不正取引の手口が拡散しているという。また、フリマサイト側がツイッター社に繰り返し

投稿の削除などの対応を求めているが「削除の判断はグローバルで検討している。個別の判断は難しい」として、削除などの対策が速やかに講じられていないという。こうした問題を受け、東京都ではフリマサイトと連携し新たな取組を始める。取組は、都がツイッターに警告用の公式アカウントを開設。フリマサイトが不正取引の宣伝投稿を発見した場合、都に情報提供し、都がツイッターの当該投稿へのリプライ（返信）機能を使って「法律に抵触する」「投稿を削除するように」といった警告をツイッター上で発信する。削除に応じない場合は、ツイッター社に情報提供し、投稿の削除や投稿者のアカウント凍結などを要請するという。都は現在、ツイッター側と調整しながら、警告用の公式アカウントの開設準備を進めており、手続きが整い次第、取組を始めるとしている。

○ ウラン、ネットオークションで売買 警視庁が出品者らを聴取

ヤフーのオークションサイトで「ウラン９９．９％」と記載された物質が出品されているのを原子力規制庁が発見し、警視庁に通報した。警視庁では、出品者と購入者から物質を押収して成分分析を進めるとともに、原子炉等規制法違反容疑（譲渡など）を視野に、いずれも日本人の出品者の男性と複数の購入者の男性から任意で事情を聴くなど捜査を進めている。出品されていたのは、固形状と粉末状の物質で、劣化ウランやウラン精鉱の可能性があうという。いずれも微量とみられ、密閉されたガラスケースに入れられていた。線量計による簡易検査の結果、微量の放射線が検出されており、警視庁は「日本原子力研究開発機構」に鑑定を依頼した。出品者の男性は警視庁の事情聴取に「海外のサイトで購入した」と説明。警視庁では入手経路や購入理由を調べている。劣化ウランやウラン精鉱が放出する放射線は微量で、長期間そばに置いたり経口摂取したりしない限り、人体への影響は少ないとされる。ただ、劣化ウランを水と反応させた場合、毒性のあるフッ化水素ガスを放出するという。原子炉等規制法では、許可を受けた事業者以外による核燃料物質の譲り渡しなどを禁止している。

２ 技術

○ 警察庁 視覚障害者の事故を防ぐ 音で信号知らせるアプリ導入

視覚障害者が交通事故に遭うのを防ぐため、警察庁は来年度にも、視覚障

害者らに音声で青信号を伝えるスマホアプリを導入する方針とした。昨年１２月に東京都内で行われた実証実験では「まもなく豊洲駅交差点です」「進行方向の信号は青です」などと地図が表示されたスマホから音声が流れ、実験に参加した視覚障害者の９割が「アプリを利用したい」と回答したという。警察庁は２０１５年から、スマホを使った視覚障害者の安全対策の検討を始めた。アプリは通信装置がある信号機とも連動して青信号の時間を延長することもでき、横断に時間のかかる高齢者らの利用も想定されるという。「ピヨピヨ」「カッコー」などの音で青信号を伝える音響信号機は昨年３月末時点で、全国に２万３１４９基（全信号機の１１％）あるが、その多くは近隣住民に配慮して、早朝、深夜には音が鳴らない設定になっている。昨年１２月には都内で視覚障害者の男性が交差点で車にはねられ死亡する事故が起きており、警察庁では「悲惨な事故の減少につなげたい」としている。

○ 架空請求の被害を防ぐアプリやサイトが登場

公的機関などを装ったはがきや封書による架空請求の被害を防ごうと、架空請求を見破るアプリや、実際に届いた封書などを掲載したサイトが登場している。写真を撮って無料通信アプリ「ＬＩＮＥ」で送信するだけで、架空請求かどうかを判別するサービス「Ｓｃａｍ Ｄｅｔｅｃｔｏｒ（スカム・ディテクター）」は、埼玉弁護士会所属の川目武彦弁護士が開発した。専用サイトを開き、ＬＩＮＥの「友だち」に追加すると無料で利用できる。このサービスでは、送信された写真をＡＩ（人工知能）が判別。「架空請求の可能性が濃厚です！」などと返信されるという。また、東京都はホームページ（ＨＰ）に、実際に届いた架空請求のはがきやメールなどを掲載し事業者名も公表している。

○ 国交省 目的地への交通手段検索・予約・支払いをアプリで完結

国土交通省は、マイカー以外で目的地に行く最適な交通手段を検索し、予約や決済まで完了できるシステムの構築に乗り出す。２０１９年度に課題を整理し、２０年をめどに具体的な導入計画の策定を目指すという。国交省が目指すのは、自家用車以外のすべての移動手段を1 つのサービスとして提供する仕組み。利用者がアプリに出発地と到着地を入力すると、電車やバス、カーシェアリングなど様々な交通手段から最適な組み合わせが表示され、予約から料金の支払いまでスマホで完結する。すでに大手私鉄などが沿線地域での実証実験に取り組んでおり、国交省ではこうした実験への支援を通じて課題を整理し、全国規模でサービスを展開できるシステムをつくる。

○ 自動車事故 過失割合をＡＩが判定

損保ジャパン日本興亜は、自動車事故の過失割合を人工知能（ＡＩ）が自動算出するシステムを年内にも導入するとした。保険契約者のうちドライブレコーダーを搭載している約１０万台がサービスの対象となる。ドライブレコーダーの映像とＧＰＳのデータをもとに車両の動きや道路状況など事故を再現し、ＡＩが学習した過去の事故データと過失認定に関する判例を踏まえ、事故当事者の過失割合を導き出す。判定には速度違反の有無なども加味する。事故の過失判定は従来、調査や示談交渉などに２か月近く要していたが、自動算出システムの導入により１～２週間に短縮でき、保険金の支払いも円滑に行えるという。

３ 国内外のサイバーセキュリティ情勢

○ ＩＰＡ 「情報セキュリティ１０大脅威 ２０１９」決定

独立行政法人情報処理推進機構（ＩＰＡ）は、「情報セキュリティ１０大脅威２０１９」を決定した。「情報セキュリティ１０大脅威２０１９」は、２０１８年に発生した社会的影響が大きかったと考えられる情報セキュリティにおける事案から、ＩＰＡが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者などで構成された「１０大脅威選考会」の投票により、個人・組織それぞれのランキングとして選出したもの。個人の１位から４位、６位、７位はいずれも、利用者をだまして金銭や情報を詐取する手口であり、“だましによる手口”が顕著となっている。

■「情報セキュリティ10大脅威 2019」

NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
1位 (*3)	クレジットカード情報の不正利用	1位	標的型攻撃による被害	1位
1位	フィッシングによる個人情報等の詐取	2位	ビジネスメール詐欺による被害	3位
4位	不正アプリによるスマートフォン利用者の被害	3位	ランサムウェアによる被害	2位
NEW	メールやSNSを使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW
3位	ネット上の誹謗・中傷・デマ	5位	内部不正による情報漏えい	8位
10位	偽警告によるインターネット詐欺	6位	サービス妨害攻撃によるサービスの停止	9位
1位	インターネットバンキングの不正利用	7位	インターネットサービスからの個人情報の窃取	6位
5位	インターネットサービスへの不正ログイン	8位	IoT機器の脆弱性の顕在化	7位
2位	ランサムウェアによる被害	9位	脆弱性対策情報の公開に伴う悪用増加	4位
9位	IoT 機器の不適切な管理	10位	不注意による情報漏えい	12位

画像はIPAウェブサイトから引用

（https://www.ipa.go.jp/security/vuln/10threats2019.html）

○ 総務省　ＩｏＴ機器２億台の調査を開始 対策不備を洗い出し

総務省は２月２０日、インターネットにつながったＩｏＴ機器の安全性を確かめるための調査「ＮＯＴＩＣＥ（Ｎａｔｉｏｎａｌ Ｏｐｅｒａｔｉｏｎ Ｔｏｗａｒｄｓ ＩｏＴ Ｃｌｅａｎ Ｅｎｖｉｒｏｎｍｅｎｔ）」を開始した。通信事業者（プロバイダ）の協力も得て、国内約２億台の機器にアクセスし、パスワード設定などを点検する。パスワードが初期設定のままなど不正アクセスの「侵入口」となりかねない機器を洗い出し、通信事業者を通じて利用者に設定変更などを促すという。調査の主な対象は、ネットに接続されているウェブカメラやルータ、ＤＶＤレコーダーなど。日常的にソフトウェアをアップデートするスマホやパソコンなどと違い、セキュリティ対策が手薄になりがちとされている。実際に海外では、ＩｏＴ機器を踏み台にしたサイバー攻撃で大規模な通信障害が起きたケースもある。今回の調査は、総務省所管の情報通信研究機構（ＮＩＣＴ）が国内約２億個のＩＰアドレスに対し、過去のサイバー攻撃で使われた約１００通りのＩＤ・パスワードの組み合わせを入力してログインできるかを試す。パスワードが容易に推測できる場合などは通信業者に通知し、通信事業者から利用者に電子メールなどで改善を促すという。本来こうしたアクセス行為は違法とされるが、政府は昨年５月に関連法を改正し、５年間限定で合法的な特例として調査が可能となった。ただ、ＳＮＳ上では「防犯のために人の家に勝手に入るのと変わらない」など避難の声も多い。総務省では、調査に関する情報を集めたサイト（https://notice.go.jp/）を開設し、理解を求めている。

NOTICEによる利用者への注意喚起は、ユーザが契約するプロバイダ以外からは行いません。また、プロバイダからの注意喚起や、NOTICEサポートセンターでの案内にあたり、費用の請求や、設定しているパスワードを聞き出すことは絶対にありません。NOTICEを装う架空請求やフィッシング詐欺などの発生も考えられることから注意しましょう。不明な点があれば、NOTICEサポートセンターへ連絡しましょう。

○ 政府 クラウドの安全基準を策定、認証制度導入へ

政府は、インターネットを通じてデータを保管する「クラウド」の安全性を認証する制度を導入するとした。クラウドは、自社で情報システムを作る手間や費用を省け、効率的にデータを管理できることから導入する企業が急増している。政府も、税金など国民のデータを保管する情報システムを含め、政府系機関では原則、クラウドの利用を進める方針を打ち出している。ただ、クラウドの安全性が低いと、サイバー攻撃でデータが外部に漏えいする危険がある。そこで政府は、クラウドサービスの事業者の安全性を審査し、安全

基準を満たしたクラウドに認証を与え、優先的に使う仕組みを整えることにした。安全基準は３段階にランク分けする。最も厳しい「レベル３」では、データセンターの防御態勢の確立や、使用する情報通信機器の安全の確認が必要になる。安全保障関連など最も機密性が高いデータを扱う機関は、こうした基準を満たした事業者のクラウドしか使わないようにするほか、電力や鉄道とった重要インフラ企業にも安全なクラウドの利用を求めるという。政府は、１９年中に安全基準を策定して試験運用を始め、２０年から制度を本格的に導入するとしている。

○ 自衛隊 超一流技術者の技能を活用、サイバー職場内訓練導入

防衛省は、自衛隊のサイバー防衛隊の隊員を急速に養成するため、民間の超一流技術者の技能を活用した職場内訓練を導入する。現行で１１０人態勢のサイバー防衛隊は中朝露の部隊に比べ桁違いに少なく、人材拡充と能力向上を急ピッチで進める狙いがある。技術者を派遣する民間専門業者との契約を今夏に交わし、来春から訓練を始める。サイバー防衛隊は、陸海空の統合部隊として平成２６年に発足し、防衛省・自衛隊の全体のネットワーク監視とサイバー攻撃対処を１１０人態勢で担う。一方、他国部隊のネットワークを妨害する攻撃能力を強化している中国のサイバー部隊は約１３万人、ロシアが約千人、軍事機密を盗む攻撃技術を持つ北朝鮮の部隊も約７千人に上るとされており、自衛隊のサイバー防衛隊の人員の少なさが顕著となっている。防衛省は来年度から、サイバーセキュリティ業者でトップレベルの知見を持つ技術者に業務を委託し、攻撃の監視や分析、防御で支援を受ける予定で、それを機に職場内訓練の指導役も技術者に担わせることにした。目の前で技術者に対処法を示してもらい、隊員が実践してみることで通常の育成より格段のスピードで能力を向上させる効果が期待できるという。

○ 五輪競技団体、サイバー標的 予算や人手に限界 対策不十分

２０２０年東京五輪に向けて、セキュリティ対策が手薄な競技団体へのサイバー攻撃が危惧されている。団体に被害が生じるだけでなく、五輪の中枢組織を攻撃する足がかりとなり、より深刻な被害につながるおそれもある。昨年７月、日本セーリング連盟のオリンピック強化委員会のＨＰ（ホームページ）が改ざんされ、ＨＰを閲覧すると有害サイトに強制移動させられる状態となった。すぐにＨＰを閉鎖して調べたところ、管理に使っていたサーバ

内に不審なデータが見つかり、ＨＰが丸ごと改ざんされた可能性があると判明したが、侵入経路は特定できなかった。五輪に向けて大会組織委員会など中枢組織を狙ったサイバー攻撃への対策が進む一方、十分な対策をしていない個人端末でサイト運営や情報管理をしている競技団体もある。ある競技団体によると、五輪開催に向けて補助金は増えているがその多くは選手の強化用となるほか、試合の調整や広報業務などにより、セキュリティ強化に取り組む予算や人員の余裕がないという。１８年平昌五輪では、開会式中に会場のＷｉ－Ｆｉやチケット印刷に障害が発生。競技団体などの外部の端末が不正プログラムに感染し、ネットワークを介して中枢システムに侵入したとみられている。内閣サイバーセキュリティセンター（ＮＩＳＣ）では競技団体向けの勉強会を定期的に開催。警視庁も各団体の情報システム担当者と合同で標的型メール対策訓練を実施した。大会警備関係者は「定期的なウイルスチェック、不審メールへの警戒と感染拡大を防止する対応など、資金や人手をかけなくてもできる対策はある。狙われているという意識を持って、基本に徹底してほしい」と話している。

４　その他

○　自然災害への備え　セキュリティの観点から

○災害に便乗した詐欺に注意

自然災害発生後は、それに便乗した詐欺が横行する。昨年９月には大手インターネットサービスをかたって「平成３０年７月豪雨緊急災害支援募金」を呼びかける詐欺メールが拡散された。これは、西日本豪雨の緊急支援を募る「ネット募金」の偽サイトへ誘導し、クレジットカード情報や金銭をだまし取ることが目的とされている。そのほか、災害情報に見せかけた内容の偽メールを送りつけ、偽サイトのＵＲＬをクリックさせたり、添付ファイルを開かせることでウイルス感染させる手口もあるという。

【被害に遭わないためのポイント】

１　メールのＵＲＬリンクや添付ファイルを不用意に開かない。

２　寄付や送金に関わる正規のウェブサイトのＵＲＬを確認し、真偽を確かめる。

○デマ情報に注意

被災状況、避難場所の状況、支援物資の供給などの災害情報を収集、発信する手段としてネットは有効な手段といえるが、事実とは異なる情報や、悪意をもって加工されたデマなどがネット上を飛び交うこともある。ネット上

の誤った情報やデマに踊らされることがないよう、また、事実かどうかわからない情報の拡散に加担しないようにする。

【ネットで災害情報を収集するときのポイント】
　首相官邸や消防庁、各自治体などの公式のツイッターアカウントをフォローし、信頼できる情報を入手する。フォローする際は、アカウントが本物であることを示すブルーのチェックマーク（ツイッターが発行する認証バッジ）が表示されていることを確認する。

〇無料公衆Ｗｉ－Ｆｉの利用

大規模災害時には「００００００ＪＡＰＡＮ（ファイブゼロジャパン）」というＳＳＩＤ（ネットワーク名）を持つ公衆Ｗｉ－Ｆｉが無料開放される場合がある。利用方法は、スマホなどの端末のＷｉ－Ｆｉ機能をオンにし、利用可能なＳＳＩＤの一覧から００００００ＪＡＰＡＮを選択するだけで利用できる。ただし、００００００ＪＡＰＡＮは誰でも利用できるように認証を設けておらず、通信内容が暗号化されていないことから、悪意の第三者に通信内容を盗み見られてしまうおそれがある。

【公衆Ｗｉ－Ｆｉを安全に利用するためのポイント】
　ＩＤ・パスワードの入力や、個人情報、クレジットカード情報などの重要な情報のやり取りはしない。