サイバーセキュリティニュース（平成31年3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）

○　ＳＭＳから偽サイトへ誘導　「宅配業者」の次は「携帯会社」

トレンドマイクロは公式ブログで「継続する偽造ＳＭＳ：今度は携帯電話事業者サイトの偽装とｉＯＳを狙う不正プロファイル」と題する記事を公開した。このブログによると、昨年国内で拡散した「宅配業者を装うＳＭＳを送りつけ、偽サイトに誘導する手口」に、新たなものが確認されたという。一つ目は「宅配業者」ではなく「携帯電話事業者」を装ったＳＭＳの出現。さらに二つ目として、誘導先の偽サイト上でｉＯＳ端末（ｉＰＨＯＮＥ等）の固有情報を窃取するために、不正な構成プロファイル（※）をインストールさせる新たな手口が確認された。この手口は、これまで同様にアクセスした端末のＯＳを判定し、Ａｎｄｒｏｉｄ端末だった場合には携帯電話事業者の偽サイトに誘導して不正アプリをインストールさせる。ｉＯＳ端末だった場合には、これまでは電話番号等の入力を求めていたところ、新たな手口では「ネットワークセキュリティのアップグレード」と称して不正な構成プロファイルをインストールさせ、端末やＳＩＭカードの固有情報、ＯＳバージョン等の情報を盗み取り、最終的にアップル社を装ったフィッシングサイトへ誘導するという。

※　iOS端末の設定情報が書き込まれたファイル。iOS端末にインストールすると、その設定が適用される。利用される例として、iOS端末でインターネットを使えるようにする初期設定のほか、学校の教材端末や会社の業務用端末で、特定のアプリ以外を起動できないようにしたり、勝手にアプリをインストール・アンインストールできないようにしたりもできる。

○　サポート詐欺に新手口　ＳＮＳで正規企業になりすまし

トレンドマイクロは公式ブログで「『サポート詐欺』の手口が変化、ＳＮＳの投稿を検索結果に表示させ詐欺ページに誘導」と題する記事を公開した。ブログでは、ツイッターやフェイスブック等のＳＮＳに、不正なウェブサイトへのリンクを投稿するという新しいサポート詐欺の手口を解説している。トレンドマイクロによると、犯人はＳＮＳ上でセキュリティ関連企業やオフィス機器製造企業等になりすました偽アカウントを作成し、そこに不正なウェブサイトへのリンクや偽のサポート電話番号を載せた内容を投稿する。ユーザがセキュリティやオフィス機器に関する情報を検索すると、正規企業の

情報のほか、犯人の投稿も検索結果に表示される。ユーザが偽物と気づかず利用してしまった場合、被害を受けることになる。投稿に記載された電話番号は「１－８８８」「１－８００」「１－８７７」で始まっており、米国の無料通話サービスで利用されているという。また、同一の電話番号で、セキュリティ企業、ウェブメールサービス、プリンタの顧客サービス・サポート、ブラウザのサポートなどさまざまなサポート詐欺に利用されているという。

○ 高○名人もびっくり！？ボタン連打で仮想通貨詐取少年を摘発

仮想通貨「モナコイン」を顧客から預かるサービス「モナッピー」にサイバー攻撃を仕掛けてモナコイン約１５００万円相当を詐取したとして、警視庁は３月１４日、栃木県少年（１８歳）を電子計算機使用詐欺と組織的犯罪処罰法違反（犯罪収益の隠匿）の疑いで書類送検した。少年は平成３０年８月、モナッピー運営会社が行ったＰＲイベントで、少額のモナコインを受け取れるギフトコードを入手した。サイトにコードを入力し、受取ボタンをクリックしてモナコインを受け取るという仕組みだったが、ボタンを短時間に何度もクリックすると、送金システムが誤作動を起こし、複数回受け取ることができる欠陥があったという。この欠陥に気づいた少年は、スマホやパソコンで計８２５４回、手動でボタンを連打し、自らが取得していた１３３回分のコードで６４２回分受け取ったという。不正に受け取ったモナコインは海外の仮想通貨交換業者に開設した匿名口座に送金。その際、送金元の追跡を困難にする匿名化ソフトを利用していたという。

○ ＳＮＳで広がる「個人間融資」 違法な高金利、条件に性行為も

見知らぬ人同士で金の貸し借りをする「個人間融資」のＳＮＳ投稿がネット上で広がっている。「＃（ハッシュタグ）個人間融資」で検索すると、貸し手、借り手双方のツイッター投稿が大量に現れるほか、双方が連絡先などを書き込める電子掲示板もあるという。ＳＮＳの投稿から個人間融資で金を借りたことのある男性によると、８万円を借りて利息は１か月４万円。金銭のやりとりは対面で行われ、人家の少ない見通しのよい橋などで待つように言われた。取引ごとに違う人物が現れ、自宅まで男がついてきたこともあった。傷だらけの男性の写真を見せられたこともあり「逃げたらこうなる」と感じたという。また、別の経験者（女性）によると、借金を重ねて正規の貸金業者から借りられない状態だったが、個人間融資の掲示板に「借りたい」と書

き込んだところ、男から連絡があった。男とはＬＩＮＥでやりとりを始め、金を貸す条件として、定期的な性行為と、性行為中の動画撮影を求められた。違法な高金利も提示され「返済を怠れば動画を流出させる」と脅されたという。都内の某法律事務所には、こうした個人間融資の被害相談が年間３００件ほど寄せられるという。

○ パソコンソフトで高級車窃盗１５６件繰り返す 容疑の男逮捕

高級車窃盗を繰り返したとして、大阪市内に居住する男が窃盗容疑で大阪府警に逮捕された。男は平成３０年９月までの約１年半の間に、高級車を狙った窃盗を１５６件（被害額約７億１７６０万円）繰り返していたという。被害車両はレクサス、ランドクルーザーなどの高級車が大半を占める。車には制御コンピュータが特定の電子キーの電波を感知しないとドアの解錠やエンジン始動ができない装置「イモビライザー」が搭載されている。男はドアを電動ドリルなどの工具でこじ開け、車内の制御コンピュータにパソコンを接続し、電子キーがなくてもエンジンを始動できるソフトを使って車を動かしたという。男が使ったパソコンソフトは電子キーの紛失対応に鍵業者が使うソフトで、海外のインターネットサイトなどからダウンロードできるという。

○ 標的型メール、手口巧妙化 心の隙を突く

公的機関や企業を狙った標的型メールは近年、件数が増え続けるとともに、その手口も巧妙になっている。平成３０年７月に国内メディア関連企業等に送られた標的型メールは、題名に「自民党海洋総合戦略小委員会が政府に提言申入れ」や、グアテマラ大使の「講演会案内状」など実在する組織やイベントが使われたほか、ウイルスを仕込んだワード形式の案内文や資料が添付され、対策ソフトで簡単に検知されないようパスワードで保護されていた。また、「先着５０名まで」という文言を使い、熟考の余地を与えないよう細工していたという。平成３０年１月に仮想通貨交換業者コインチェックから約５８０億円相当の仮想通貨が流出した事件では、半年前に研究者を装った人物からコインチェックにメールが届き、その後断続的にやり取りを重ねた上、事件の数週間前にウイルス感染につながるＵＲＬをメールで送られた。コインチェックでは、これまでやり取りをしてきた人物だったため、疑うことなくＵＲＬをクリックしてしまい、ウイルス感染したという。警察庁によると、平成３０年に確認された標的型メール攻撃は６７４０件に上り、前年に続き

過去最多を更新した。メールの文体も、かつては自動翻訳したような単語の誤用や不自然な言い回しも多かったが、近年では自然なものになっている。また、取引先のふりをして偽の注文書を添付するなど、業務を装った内容が目立つという。セキュリティの技術的な弱点を突くのではなく、人間の心理的な隙やミスにつけ込むこうした手口は「ソーシャルエンジニアリング」と呼ばれ、さまざまなサイバー攻撃に使われている。情報セキュリティ会社Ｓ＆Ｊ（東京）の三輪氏は「言葉遣いなどに少しでも違和感を覚えたら、相手に電話するなど慎重に対応することが必要」としている。

○ 盗んだクレカ情報 現金化の手段は「自分に寄付」

不正入手したクレジットカード情報を現金にする手段として、インターネットで寄付を募る「クラウドファンディング（ＣＦ）」サイトが悪用されていることが分かった。ＣＦサイトは、資金を調達したい人が、映画制作やイベント開催などの使い道と目標額を投稿し、寄付を呼びかける。寄付をする人は、クレジットカード決済や銀行振込などの方法で寄付をする。目標額に達すれば、手数料を引いた分を寄付の呼びかけ人が受け取る仕組み。犯人はまず、フィッシングなどの手口でクレジットカード情報や氏名などの個人情報を盗み取る。次に、寄付の呼びかけ人を装ってＣＦサイトに登録し、盗み取ったクレジットカード情報を決済手段として自分に寄付することで現金を手にする。ＣＦサイトを運営する都内の会社によると、こうしたクレジットカードの不正利用に関する問合せが増えているという。ＣＦサイトのほかにも、特技を活かしてサービスを提供する「スキルシェア」の仲介サイトも悪用された事例もある。スキルシェアは、イラストなど自分の特技や技術を、仲介サイトを介して利用者に提供するサービスで、利用代金から手数料を引いた金額を仲介サイトから受け取る仕組み。犯人は、架空のサービスを登録し、自らサービスを利用して盗み取ったクレジットカード情報で決済し現金を手にする。不正入手したクレジットカード情報は、これまで換金性の高い商品を購入して転売する方法で現金化されていたが、カード会社が高額商品の大量購入などを自動検知するシステムを導入するなどしたため、こうしたサイトが悪用され始めたという。

２ 技術

○ ＡＩで不審客発見 サツドラ子会社 新システム開発

サツドラホールディングス（札幌）の子会社で、人工知能（ＡＩ）のシステム開発を手がけるアウル（東京）は、店舗内の防犯カメラ映像から万引き

目的の不審な客をＡＩで瞬時に特定する新システムを開発した。新システムの開発では、万引き犯の心理に詳しい警察ＯＢらの話を参考に不審者の店内での行動パターンをＡＩに学習させた。周囲をしきりに気にしたり、売場の一角に長い間とどまったりするなど犯罪リスクが高いとＡＩが判断すると、各店員にメールで通知する仕組みとなっている。ＡＩは映像から性別、年齢も推定する。化粧品コーナーで黒い服を着た男性が不審な動きをしているといった情報も判断できる。過去の映像の検索も可能で、不審者の行動を継続して監視できる。不審者の位置や問題行動の内容も短い文章で教えてくれる。アウルは平成３０年夏から、札幌市内の複数店舗で本格的な実証実験を重ね、システムを確立した。導入する店側は設置済みの防犯カメラや付属の機器を活用できるという。

○ ネットで民事裁判、法廷出向かずウェブ会議　２２年度を目標

法務省が最高裁と連携し、ネットで民事裁判ができるよう法改正を目指していることが分かった。争点整理や口頭弁論をウェブ会議などでできるようにするほか、証拠もネットで共有できるようにする。現在の日本の民事裁判手続きは書面の提出や対面での協議が原則で、原告・被告ともに多大な手間や時間がかかる。法務省が検討しているのは一連の裁判手続きでＩＴを使うこと。書類を電子データでやりとりし、対面の弁論をウェブ会議に切り替えれば、当事者には大きな負担減となる。原告・被告双方がネット上での裁判を望めば、出廷しないまま結審させることもできるようになる。法務省がこうした改革を目指すのは、経済界などからの強い要望があるからだ。知的財産をめぐる紛争の増加やビジネスの複雑化で企業の訴訟リスクは大きくなっている。争点が明確で判決の見通しが立ちやすい場合や、当事者同士が早期和解を目指す場合などは、速やかに裁判を終えたいというのが企業の本音。法務省は１９年度に一部の裁判所へのウェブ会議用設備の導入を始める。早ければ２１年秋の臨時国会で民事訴訟法改正案を提出し、２２年度ころの本格運用を目指す。法改正後は裁判期日の調整や証拠の提出、弁論もネットでできるようになる。証拠などは電子データとしてネットで閲覧できる。ただし、訴状や証拠は個人情報や企業情報を含むため十分な秘密保全対策が必要になる。

○ 防犯カメラ画面から外れた人物をＡＩが追跡　位置や色で判断

慶應義塾大学とパナソニックは、防犯カメラなどに映っている人物が途中で画面から外れても再度認識をして追跡する手法を共同で開発した。ＡＩと位置や色の情報を組み合わせて人を区別する精度を高めた。体全体の特徴を捉えるため粗い画像でも使えるという。これまでも映像で人を追跡する技術はあったが、画像内の間だけだったり、事前に追いかけたい人物の動きの特徴を学ばせたりする必要があった。新システムでは他の人の陰に隠れて見えなくなったり、カメラの範囲から一度外れてもリアルタイムで続けられるという。画像中のどこに人がいるか探し、各人物について１フレーム前の画像と比較して似ている人を探し出して追跡する。一度見失った人物の場合、最初は新たな人物として認識するが、数秒で過去に認識していた人物と同一人物であると判断する。人物の判定は、ＡＩが上半身と下半身の洋服の色などの特徴で見分けている。複数のカメラ映像に適応することも可能で、店舗などの広い範囲での人の行動も追跡できるという。同大学では２年以内の実用化を目指している。

３ 国内外のサイバーセキュリティ情勢

○ 平成３０年サイバー犯罪統計公表、警察庁

警察庁は３月７日、平成３０年のサイバー犯罪統計を公表した。統計によると、全国警察が摘発したサイバー犯罪は９０４０件（前年比＋２６件）で過去最高を更新。内訳は、児童買春・ポルノ禁止法違反が２０５７件と最多で、次いで詐欺９７２件、青少年保護育成条例違反９２６件と続いた。被害相談は減少したが、１２万６８１５件（前年１３万１１件）と高水準で推移した。仮想通貨を狙った不正アクセス事件の認知件数は１６９件（前年比＋２０件）で、被害総額は約６７７億円に上った。このうちの６割超となる１０８件は、利用者が仮想通貨交換業者に登録したＩＤ・パスワードを別のウェブサービスでも使用していたという。また、警察庁が運用しているリアルタイム検知ネットワークシステムで検知した不審なアクセスは平成３０年中、一日平均約２７５２．８件（前年比４５．４％増）と大幅に増加。このうち１７０２．８件は、ネットに接続できる家電のＩｏＴ機器や仮想通貨などを標的にしているという。これらの発信元は、ロシアが２０．８％と最も多く、次いで中国が１４．１％、米国が１２．６％と続いた。警察庁では、発信元を偽装するため「踏み台」にしている可能性があるとしている。

○ サイバー保険 加入率は１割 企業対象調査

日本損害保険協会が発表した企業対象調査の結果によると、サイバー攻撃

の被害に備える「サイバー保険」の加入率が１割程度にとどまっていることがわかった。事業規模の小さい中小企業ほど加入が限られ、サイバー攻撃への危機意識が低いという。今回の調査は、損保協会がインターネットで調査し、国内の１１１３社から回答を得た。サイバー攻撃による顧客情報流出などが相次いでいるため、損保大手は事故時の賠償責任やシステム復旧費などを補償するサイバー保険の販売を強化しているが、今回の調査で判明した加入率は１２％で、「検討したこともない」との回答が７３％に上ったという。従業員規模別の加入率は、１０００人以上の企業が３０％だったのに対し、５０人未満の企業は５％と低くかった。また、自社がサイバー攻撃の対象になるかどうかについては「可能性がない」「わからない」を合わせて６１％に達した。損保協会は、今後保険加入を促していきたいとしている。

４ 道内関連

○ ノーマップス 平成３１年は釧路でも開催

音楽や映画、ＩＴ産業の複合イベント「ＮｏＭａｐｓ（ノーマップス）」の実行委員会は、平成３１年のイベントを札幌市のほか、釧路市でも開催する方針を明らかにした。４月に新設する「ＮｏＭａｐｓ釧路実行委員会（事務局：大地みらい信用金庫）」が主催し、９月中旬に地場産業とＩＴの融合をテーマにした会議などを開く。ＡＩやＩｏＴを使って一次産業の強化などをテーマに、専門家を招いた会議などを開く方針。高校生がアイデアを披露するコンテストや、東京や札幌からの来場者を対象とした釧路・根室地方のショートツアーも設定する。初年度は音楽や映画などの文化イベントは実施しない。ＮｏＭａｐｓは、「初音ミク」で知られるクリプトン・フューチャー・メディアの伊藤博之社長が中心となって立ち上げ、２０１６年から札幌中心部で最新のＩＴを紹介するイベントなどを行ってきた。ＮｏＭａｐｓ実行委員会は、民間企業、北海道や札幌市などの官公庁、北大や札幌市立大などの教育機関で構成されている。２０１７年のイベントでは大通公園周辺の公道で自動運転の実証実験が行われたほか、「チ・カ・ホ」ではＩＴ企業がブース出展し、新たな技術の体験会などが行われた。