サイバーセキュリティニュース（平成30年11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　道内のサイバーセキュリティ関連ニュース

○ 正義のハッカー育成、「セキュリティ・ミニキャンプ」道内で開催

独立行政法人・情報処理推進機構（ＩＰＡ）などは１１月３日、次世代を担うセキュリティ人材を育成する「セキュリティ・ミニキャンプ」を北海道大学で開催し、小学生から大学院生までの２２人が参加した。参加者が取り組んだのは、インターネットとモノをつなぐ先端技術「ＩｏＴ」を活用してミニカーを動かすプログラムの作成。ＩｏＴが社会に広まる中、電力や鉄道などを狙ったサイバー攻撃への対策は緊急の課題となっており、１泊２日のセキュリティ・ミニキャンプでも特に時間を割いて講義が行われた。

ＩＰＡでは２００４年からこうしたハッカー育成合宿を開催しており、今回は、道警サイバーセキュリティ対策本部の警察官も講義に参加し、ネット犯罪の事例紹介を交えながら倫理教養も行った。

経済産業省は、サイバー攻撃に対応できる情報セキュリティの人材は、２０年には全国で約１９万人が不足すると推計。道内のＩＴ企業を対象とした「北海道ＩＴ推進協会」のアンケート（２０１７年）でも、今後力を入れたい分野として「クラウド」「ＡＩ（人工知能）」「ＩｏＴ」に続き、１３．９％の企業が「情報セキュリティ」と回答するなど、人材不足への危機感は高まっている。

こうした現状から、道警では今年３月、苫小牧高専と情報セキュリティ人材育成に関する連携協定を締結し、セキュリティ分野に詳しい講師がお互いの組織に出前授業を実施しているほか、地元企業に意識調査を行い、今後の人材育成に役立てる。

○ スマホで家電を遠隔操作、北電 来年から新サービス

北海道電力は、スマホで電気使用量の確認や家電の遠隔操作ができる契約者対象のサービス「エネモＬＩＦＥ（ライフ）」を来年中にも本格的に始めると発表した。このサービスでは、家にスマートメーター（次世代電力計）や家電をまとめて操作できる赤外線リモコン、各種センサーなどを設置し、スマホの無料通信アプリＬＩＮＥ（ライン）で電気使用量や室内の温度などを確認できたり、スマホでエアコンや照明などを遠隔操作できるようになるという。

２　新たな脅威（手口）・技術

○ ＧＰＳ位置情報を偽造し来店ポイント詐取、容疑の男を逮捕

イオン九州アプリのＧＰＳを用いた「チェックイン」機能で偽の位置情報を送信して約２６９万回来店したように装い、不正にポイントを得ようとしたとして、福岡県警は１１月１２日、北海道石狩市の男を私電磁的記録不正作出・同供用などの容疑で逮捕した。逮捕容疑は、自宅のノートパソコン内でイオン九州の公式アプリを起動し、ＧＰＳ情報を偽造して７０店にチェックイン。ＷＡＯＮポイント１４０円相当を不正に得た疑い。その後、同様の手口で７１店に約２６９万回にわたって来店したように装い、約５３８万円相当のポイントを得ようとした疑い。さらに福岡県警は、男が同様の手口で生活雑貨店「無印良品」の店舗にも約５６２回来店したように装って来店ポイント１０８万円相当を詐取したとして、１１月２８日に男を電子計算機使用詐欺容疑で再逮捕した。

福岡県警によると、男は無印良品の公式アプリで約３００のアカウントを作成し、自宅のパソコン４５台を使って国内や北米、欧州などの計９０９店舗を毎日訪れたように装っていたという。

○ 「アダルトサイト閲覧姿を録画」偽メール、大量送信続く

「アダルトサイトを閲覧している姿を録画した」などとの偽メールを送りつけて仮想通貨をだまし取る手口について、１０月中も約５万２千通のメールが送信され、国内で約１千万円相当の被害が発生していることが情報セキュリティ会社トレンドマイクロの調査でわかった。

トレンドマイクロによると、当初は偽メールの件名に「緊急対応！」「あなたの心の安らぎの問題」などの文言が使われていたが、１０月下旬からは「あなたのパスワードが侵害された」などの文言とともに、利用者が過去に使っていたパスワードなどが表示されるパターンが主流になってきているという。パスワードはネット上に流出した個人情報が悪用されているとみられるが、被害者はサイバー攻撃で自分のパソコンを乗っ取られたと思い込み、要求に応じているとみられている。１１月に入ってからも偽メールの大量送信が続いているという。

○ ビジネスメール詐欺 世界中で横行、被害１兆円超す

取引先や会社役員などの関係者を装ったメールで金銭をだまし取る「ビジネスメール詐欺（Ｂｕｓｉｎｅｓｓ Ｅｍａｉｌ Ｃｏｍｐｒｏｍｉｓｅの頭

文字をとって『ＢＥＣ』とも呼ばれる）」が世界中で横行している。ここ５年間の被害は世界で１兆円を超えるといわれ、日本の企業も標的となっているという。米国の非政府組織（ＮＧＯ）がだまされて送金した９３００万円を不正に引き出したとして、仙台市で中古車輸出会社を経営する日本人の男が今年７月、組織犯罪処罰法違反などの疑いで警視庁に逮捕された。詐欺グループは、ＮＧＯパキスタン支部の職員が使っているメールのアカウント情報を事前に入手し、この職員になりすまして米国の経理担当者に「太陽光パネルを購入する」とメールを送って１億円余りの支払いを要求した。送金先として指定されたのが、逮捕された男の会社名義の邦銀口座だった。男の関連口座には、他にも米国やアジアなど８か国１０社から詐取したと思われる６２００万円の入金があった。警視庁幹部は「詐欺グループ詐取金の送金先を世界中に持っており、その一つが男の口座だったようだ」と話す。ビジネスメール詐欺の代表的な手口は、本物と酷似したアドレスや不正入手したアカウントを使って企業の幹部・同僚、取引先になりすまし、虚偽の名目で送金を指示する。事前に標的周辺のパソコンやメールをのぞき見し、数か月にわたって業務内容などを監視したうえで犯行に及んだとみられるケースもある。メール詐欺の被害は日本でも１４年ころから報告されるようになり、１７年には日本航空が取引先を装う相手に約３億８千万円をだまし取られた。

トレンドマイクロが今年６月に行った調査では、日本の企業や行政機関で経理責任者などを務める課長級以上の約１千人の約４割に、詐欺メールの受信経験があることが明らかとなった。虚偽の送金依頼を受けたことがあるのは２５３人で、メールを信じて送金した人が２２人もいた。狙われたのは金だけでなく、２０９人は従業員の個人情報や非公開の決算、新製品情報を求められ、１７人が実際に送信してしまったという。

情報処理推進機構（ＩＰＡ）セキュリティセンターの伊藤氏は「これまで詐欺メールは英文が主だったが、１８年に入ってから日本語で書かれたメールも確認されている。国際的に活動している企業だけでなく、国内でビジネスをしている日本企業、日本人も狙われ始めている」と警告している。

○ 津波警報を装う不正メール出回る、気象庁がＨＰで注意喚起

気象庁の津波警報を装った不正メールが１１月に入って大量に出回っており、気象庁にはこのメールに関する問い合わせが全国から寄せられている。メールのリンクにあるサイトを閲覧するとウイルス感染し、パソコンの中の情報が抜き取られるおそれがある。メールは「津波警報発表」などの件名で届く。発信者のアドレスの末尾は、省庁が使う「．ｇｏ．ｊｐ」となってい

るが、偽装の可能性が高い。「津波警報が出され、緊急避難必要」として、サイトにアクセスして避難対象地域を確認するよう求める内容となっている。サイトを閲覧すると「ファイルのダウンロードを許可する」という表示が現れ、「実行」をクリックしてダウンロードすると、パソコン内のデータを削除したり、情報を流出させるウイルスに感染する。

気象庁はウェブサイトで「気象庁を含め、政府機関は原則として「．ｇｏ．ｊｐ」で終わる名前のドメインを使っています。『ｊｍａ－ｇｏ．ｊｐ』など、正規の政府機関とまぎらわしいドメインを使用したＵＲＬは気象庁とまったく関係がありません。アクセスしないでください」と注意喚起している。

○ ｉＰｈｏｎｅ「ＡｉｒＤｒｏｐ」悪用、サイバー痴漢相次ぐ

ｉＰｈｏｎｅなどに搭載されたデータ通信機能「ＡｉｒＤｒｏｐ（エアドロップ）」。近距離無線通信を利用し、半径１０メートル程度の距離にあるｉＰｈｏｎｅやｉＰａｄなどの端末同士で画像や動画などのデータを送受信し共有することができる。この機能を悪用し、電車内などで居合わせた女性のｉＰｈｏｎｅにわいせつ画像を表示させる悪質行為が相次いでいるという。女性の困惑する姿をのぞき見ることなどが狙いで、会員制交流サイト（ＳＮＳ）で「エアドロップ痴漢」と呼ばれるなど社会問題化している。

エアドロップの送信側は端末画面に表示される通信圏内の端末の名前リストから送信先を選択すればよく、例えばスマホのカメラで撮影した集合写真をその場で共有することが可能となる。この便利さにつけ込み、わいせつ画像を見知らぬ女性に送りつける事件が続発。リストから女性と推定される名前の端末を選択し送信しているとみられる。これまでの事例として、

・兵庫県で今年７月、電車内で向かいに座っていた女性にわいせつ画像を送りつけたとして、県迷惑防止条例違反で男を逮捕
・大阪府で今年８月、電車内で周囲の乗客にわいせつ画像を送りつけたとして、府迷惑防止条例違反で男を書類送検

がある。この二つの事例では、乗客がたまたま犯行の様子を目撃していたため摘発につながったが、混雑した場所で送り主を特定するのは難しい。

短文投稿サイト・ツイッターには「私もされたことがある」「急に見たくもない画像が送られてきた」などと、体験談を報告する書き込みが多数寄せられているという。

○ 正規ソフトを利用した新たなサイバー攻撃

米国の情報セキュリティ会社「パロアルトネットワークス」は、パソコン

の動画再生ソフトの更新やインストールを持ちかけて、利用者が応じると正規ソフトの更新等を実際に行いながら、別の不正なソフトを入り込ませる新手のサイバー攻撃を発見した。不正の隠れみのとして、正規ソフトのインストールを行う手口が確認されたのは初めて。

発見された手口は、攻撃相手のパソコンに、仮想通貨のマイニングを実行するソフトを入り込ませ、パソコンの所有者が知らない間にその計算処理能力を使わせることを目的としている。

こうした攻撃は今年３月ころから、米国や台湾など海外で約１０００件確認されているといい、日本に来るのも時間の問題だという。

パロアルトネットワークスによると、マイニングのためのソフトの代わりに、より悪質なコンピュータウイルスを忍び込ませることも技術的に難しくなく、このようなウイルスの侵入を許せば、個人情報を盗まれたり、パソコンを他のサイバー攻撃に使われたりする恐れもある。動画再生ソフト以外のインストールや更新を装うこともできるといい、どの利用者も注意が必要となる。

○ グーグルマップにヘイト書き込み

グーグルの地図サービス「グーグルマップ」で、朝鮮総連東京都本部や社民党旧本部所在地が「犯罪者」などと表記されていた。何者かが書き込んだものとみられている。

朝鮮総連東京都本部は「朝鮮進駐軍犯罪者」などと書き込まれ、「東京　犯罪者」と入力して検索した場合でも表示された。

社民党旧本部所在地は「朝鮮労働党日本支部」、在日本大韓民国民団三重県地方本部も「反日韓国基地」と書き込まれた。

グーグルマップには利用者が情報を追加できる機能があり、不適切な表現が書き込まれることがあるという。２０１５年には原爆ドームに「核実験場」などと書き込まれた事件で、大学生ら３人が軽犯罪法違反で書類送検された。グーグル広報部は、誤りがある場合は修正や削除をするとして、グーグルへの通報を求めている。

○ 空き巣グループ　インスタの投稿から狙いを決める

愛知県警は今年１月、県内のアパートの一室に侵入して金品を盗んだとして、飲食店の客引きなどの男５人を逮捕した。この事件で被害に遭った部屋の住人は男子大学生。狙われたきっかけはインスタグラムだったという。大学生はしばしば、高級ブランド品を身につけたり、高級車を運転する様子をインスタグラムに投稿。「羽振りの良さそうな投稿をしている大学生がいる」

などと評判になり、口コミで広がっていった。この事件で中心的な役割を担った客引きは「いつか盗みに入ろう」と、この大学生の投稿に目を付けており、投稿写真の景色やコメントを手がかりに、知人らに聞き込みし、最終的に大学生が住むアパートを特定したという。

○ 警察庁 自動運転事故の捜査手法を研究 ノウハウ確立へ

警察庁は来年度から、自動運転事故の原因を捜査するための技術的研究を始める。自動運転車の事故は、操作ミスやシステムトラブルだけでなく、サイバー攻撃の可能性も指摘されている。従来の捜査手法だけでは対応は難しく、研究でノウハウを確立するという。研究では実際の自動運転車のシステムを使い、車両のどこにデータが残っているかや、データを取り出して解析する手法を調べる。

今後、自動車メーカー側にも協力を求める考えで、解析のノウハウは各県警に伝え、自動運転車が絡む事故捜査に役立てる。これまでも自動運転車に対するサイバー攻撃のリスクは指摘されており、トレンドマイクロの実証実験では、インターネットにつながったカーナビのアップデートを装って不正プログラムを感染させ、ライトを点滅したり、クラクションを鳴らしたりすることができたという。

同社担当者は「車が不正プログラムに感染し、遠隔操作される可能性も考えられる」と指摘する。車を乗っ取り、身代金を要求するような犯罪が起きる可能性もあり、セキュリティ対策が急務となっている。

○ ブリヂストン ＩｏＴ活用、タイヤにセンサーで走行分析

あらゆるモノがネットにつながるＩｏＴ時代で、タイヤ世界首位のブリヂストンは自動運転やカーシェアリングの普及をにらんだ経営にカジを切る。注力するのは、タイヤにセンサーを付けて走行状況を分析するデータビジネスで、保守などのサービスで稼ぐ基盤を整える。

自動車の必需品であるタイヤは新車販売の浮き沈みがあっても、交換用の需要を背景に市場の拡大基調が続いてきた。その自動車産業は「ＣＡＳＥ（つながる車、自動運転、シェアリング、電気自動車）」と略される新たなビジネスが台頭し、大きな転機を迎えている。車の「保有」から「利用」へのシフトで２０２３年以降は年１億台程度の世界新車販売台数のうち約２％にあたる２００万台規模の需要が「カーシェアなどの普及で消える」と調査会社の

英ＩＨＳマークイットは分析している。
　タイヤはというと、自動運転やカーシェアの普及で車の稼働率が高まり、タイヤの交換頻度が増えるとみられる。ただブリヂストン最高経営責任者は「１０年前の最先端製品は今の汎用品。将来への投資で車両の進化についていかないと稼げない」として、従来の売り切り型を脱し、事業モデルや開発体制を変える。注力するのはタイヤを軸にしたデータ分析。タイヤにセンサーを付け、走行距離や稼働状況のデータを蓄積すれば、点検・修理の時期を事前に察知できる。タイヤ販売後も保守、サービス事業の拡大につながる。すでに鉱山用機械向けでノウハウを蓄積している。こうしたデジタル化の動きはライバル会社にもある。世界２位の仏ミシュランは、物流事業者向けにトラックのタイヤに取り付けたセンサーから空気圧や内部温度を把握し、基準値を下回ると管理担当者へ通知するサービスを展開している。１７年にはＧＰＳでトラックの安全運転を管理する米国企業を買収した。世界４位の独コンチネンタルも、タイヤに付けたセンサーで路面状態を判別し、自動運転システムに役立てる技術を開発するという。

３　国内外のサイバーセキュリティ関連ニュース

○　経産省　中小企業のサイバー攻撃対策を強化する方針

　経済産業省は、２０１９年度からＩＴ企業等と協力し、中小企業がサイバー攻撃を受けた際の相談窓口の設置や、外部の専門家チームがすぐに対応できる体制を整備し、中小企業のサイバー攻撃対策を強化する方針を固めた。相談窓口は、ＩＴ企業やサイバー保険を販売する損保会社に設け、サイバー攻撃を受けたと疑われる中小企業からの連絡や相談を受け付ける。専門家による調査や復旧が必要と判断すれば、新たに設置される「サイバーセキュリティお助け隊」の派遣を要請する。お助け隊には、普段は他の仕事に従事するシステムエンジニア等を非常勤として登録するという。
　経産省は、２０１９年度から２年間、相談窓口の運営日やお助け隊の報酬等を補助するという。中小企業が集積しており、サイバー攻撃を受けると部品供給に大きな影響が出やすい国内５か所程度で行う方針だといい、大阪府や愛知県の一部地域などが対象となる見込み。

４　その他

なし