サイバーセキュリティニュース（平成30年9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

○ 北海道　ＳＮＳでデマ拡散

胆振東部地震に関連して、根拠のない誤情報が交流サイト（ＳＮＳ）や無料対話アプリを中心に拡散し、被災者に不安が広がっている。投稿は自衛隊などの情報として「数時間後に大地震が来る」などと記され、一見、信ぴょう性が高いものだった。苫小牧市危機管理室には無料対話アプリ「ＬＩＮＥ」などの投稿を見た市民から「本当に大地震が来るのか」「避難すべきか」などの問い合わせが相次ぎ、２時間ほど電話が鳴りやまないほどの対応に追われた。市危機管理室は「情報の発信源は分からない」とし、市のホームページとフェイスブックで「全て根拠のないものですので冷静な行動をお願いいたします」と呼びかけた。このほか地震後には「大規模な断水が始まる」などの誤った情報も流れたため札幌市や函館市、帯広市などもホームページやＳＮＳで注意喚起している。法政大の藤代准教授は「災害時は確実ではない情報を発信したり、情報を流した後に状況が変わってしまったりするなど、悪意がなくても結果的に多くのデマが生まれる。被災地の状況が刻々と変わるなかデマかどうか受け手側が見極めるのは難しい。情報を拡散する前に一呼吸置き、発信元が本当に信頼できるのか確かめてほしい」と話している。

２　新たな脅威（手口）・技術

○ チケット買い占め自動プログラム　購入手続きの９割

入手困難なコンサートチケットをめぐり、ネット販売サイトでチケットを買い占めるプログラムの実態が明らかになった。大量のアカウントを使い、人になりすまして購入手続きを繰り返すプログラムは、ロボットに見立てて「ボット」と呼ばれる。チケット販売会社などが長年対応に追われていた。５月12日土曜日、この日は、大手販売サイト「イープラス」（東京）がチケット購入の買い占めプログラムをチェックするシステムを導入後、販売が集中する初の土曜日。午前10時の販売開始と同時に複数のビジュアル系バンドへの購入アクセスが集中した。この購入アクセスのほとんどがシステムにより買い占めプログラムとみなされ、購入手続きが無効扱いとなった。買い占めプログラムは国内480か所から一斉にアクセスし、人の操作をまねてクリックやキーボード入力をしていた。販売開始から30分、購入手続き約50万件のうち、９割の約45万件が買い占めプログラムによるものと見なされた。

後日調べると、同一人物が作った約800個のアカウントを使い、480か所から繰り返しアクセスして買い占めを図っていたことが判明した。購入アクセ

スがプログラムによるものか、人の操作によるものかの判別は、サイト画面のマウスクリックやキーボード入力の規則性を読み取り、ＡＩ（人工知能）が担う。

イープラスが導入したのは、米通信サービス大手「アカマイ・テクノロジーズ」のシステム。アカマイ社の中西一博氏は「プログラムで一気に買い占めができてしまう。企業のビジネスに深刻な影響を与える迷惑行為。サイバー攻撃と同等の対策が必要」と語る。イープラスでは買い占めプログラムの存在が明らかとなった後も改良型とみられるプログラムによるアクセスが続いた。その都度対策を講じ、８月22日以降、プログラムのアクセスはなくなったという。

○ 車種判別・不審者発見に人工知能活用 警察庁が実証実験へ

人工知能（ＡＩ）を犯罪捜査や警備にどこまで使えるか。警察庁が来年度からこんな実験を始める。実証実験の内容は「自動車の車種判別」「疑わしい取引の分析」「不審者・不審物の抽出」の３項目。警察庁が本格的にＡＩの実験に取り組むのは初めて。自動車の実験は、不鮮明だったり、一部しか映っていなかったりする防犯カメラの画像から、車種や年式を特定するのが目標。あらかじめ大量の車両データを学習させる。事故現場付近を通った車が分かれば容疑者や目撃者を捜しやすくなる。金融取引などで犯罪やマネーロンダリング（資金洗浄）の疑いがあるものを判断できるかも調べる。現在金融機関などが「疑わしい取引」として警察に届ける通報は年間約40万件。ＡＩに過去の摘発事例などを学習させ、犯罪の可能性があるものを絞り込むことができれば捜査が効率化する。大規模なイベントの際に、不審な人物や物を判別できるかどうかも実験する。いずれも実際の捜査現場に投入できるかは未知数だが、実験の成果を踏まえながらほかの捜査や警備への応用も検討する。

○ 破壊型サイバー攻撃 国内でも 情報・業務妨害目的か

社内パソコンの基本ソフト（ＯＳ）を一斉に起動できなくする新手のサイバー攻撃が国内企業に対して行われたことが、情報セキュリティ会社「サイバーリーズン」（東京）への取材で分かった。情報を盗み取るほか、業務を妨害する目的があった可能性があり、一度に数百台のパソコンが使えなくなった企業もある。被害に遭ったのは、都内の大手サービス業者。昨年春頃、社内のシステム担当者がメールに添付されたファイルを開いたことで、パソコンを遠隔操作できるプログラムが送り込まれた。添付されていたのは、パスワードをかけて圧縮したデータをやり取りする際に使われる「ｚｉｐファイ

ル」。パスワード付きファイルは、中身の安全性をチェックするセキュリティ対策をすり抜けてしまうため悪用されたとみられる。送り込まれたプログラムは、本来はシステム管理者が離れた場所にあるパソコンの障害に対応する際のものだった。パソコンが起動するたびに動き出すよう細工されており、これを悪用して社内ネットワークに侵入した。その後、数か月かけてネットワーク内の情報を窃取。最終的にシステム管理者になりすまし、社員のパソコンにソフトウェアのインストールを指示する機能を使い、ＯＳを起動できなくするウイルスに感染させた。その結果、昨年秋、社内の約1,000台のパソコンのうち４割が、真っ黒な画面に「ファイルを復元するには連絡を」などと赤い文字でメールアドレスなど数行の英文が表示されたまま起動できなくなった。パソコンは初期化して復旧に当たったが、データが破壊されるなどして業務に大きな支障が出たという。

サイバーリーズンによると、同様の被害は国内数社で確認。被害に遭ったパソコンを解析した結果、ウイルスのコード（設計図）にはロシア語が含まれていたという。こうした攻撃は、デンマークや米国で数百億円単位の被害をもたらすなど各国で確認されており、同社は「破壊型攻撃」として警戒を強めている。

○ 水産研機構 グーグルと連携 密漁船監視システムを運用へ

国立研究開発法人「水産研究・教育機構」が、米ＩＴ大手グーグルなどと連携して密漁監視システムの運用に乗り出すことが分かった。近年、サンマなどが不漁に見舞われることがあるのは、日本近海で外国船の違法操業が増えたことが一因とされ、密漁の実態把握を強化する。グーグルなどが開発した「グローバル・フィッシング・ウォッチ」と呼ばれるシステムを活用する。船舶に搭載された「船舶自動識別装置（ＡＩＳ）」から発信される針路や位置情報を、人工衛星や地上の基地局でとらえ、船の位置や航路を地図上に表示する。これにより、漁獲が禁止されている海域での操業や、海産物が運ばれた港を一目で判別できると期待される。水研機構はグーグル側に漁船の画像データなどを提供する一方、グーグル側は航路などを記した地図データを提供。まず太平洋沖での違法操業を調べる。

水研機構は、グーグルが参加するシステム運用団体と、豪州の研究機関の３者で協定を締結した。10月以降に今後の作業計画をつくる会合を開き、水産庁とも連携して違法漁船の共同監視を始める見通しだ。

３ 国内外のサイバーセキュリティ関連ニュース

○ 偽サイト誘導 今年上半期 過去最多の290万人

クレジットカードなどの情報を盗むために電子メールを送りつけて偽サイトを開かせる「フィッシング」詐欺の手口で、偽サイトに誘導された人が、日本国内で今年上半期に過去最多の約290万人に上ることがわかった。情報セキュリティ大手トレンドマイクロが調査結果を公表した。

最近の傾向として、パソコンやスマートフォンでアップルやアマゾン、楽天、ＬＩＮＥなど有名企業のサービスを利用する際に使われるアカウントを盗もうとする攻撃が増えたという。トレンドマイクロによると、同社は製品利用者を対象に偽サイトを遮断した数の統計を平成26年から取り始め、これまでは同年下半期の約136万人が最多。その後100万人前後で推移していたが、今年上半期は昨年下半期と比べて2.7 倍に急増した。また、大量のフィッシングメールが送られた27件の攻撃を分析したところ、リンク先の偽サイトはクレジットカード情報を盗み取ろうとするものが20件、アカウントを狙うものが15件あり、うち13件は両方を狙っていた。これらのアカウントは、個人情報と結び付けられ、複数のサービスで使えることから、思わぬ形で悪用されるおそれがある。

トレンドマイクロの岡本勝之氏は「カード情報やアカウントを入力させるようなメールが来たら、もう一度本物かどうか確かめてほしい」と注意を呼び掛けている。

○ ｄポイント不正利用 原因は加盟サイトへの不正アクセス

ＮＴＴドコモは９月12日、８月末から同社の共通ポイントサービス「ｄポイント」で第三者による不正利用の被害が発生している件について、原因を特定したことを明らかにした。被害拡大を防ぐため、不正利用の可能性がある約３万5,000件のｄポイントの利用を停止し、同日該当する利用者にメールで通知した。８月25日ころから、ｄポイントを第三者に不正に利用されたという被害の声がインターネット上などに出ていた。９月11日までに約300件の被害申告があったという。

ドコモによると、今回の不正利用被害は、ｄポイントに加盟しているウェブサイトが不正アクセスを受けて、ｄポイントのカード番号や残高が第三者に漏えいしたことが原因だった。

○ 日本ハッカー協会設立 善玉ハッカー発掘し企業に紹介

コンピュータへの不正アクセスなど、サイバー攻撃に立ち向かう「ホワイトハッカー」となる人材を発掘し、企業に橋渡しをしようと「日本ハッカー協会」が９月13 日、設立された。素質がありながら、社会に出る自身がない人たちの就業支援などを通じて、ハッカーが活躍できる社会を目指すという。代表理事に就任する杉浦隆幸氏はかつて、海賊版動画の流通や企業の内部情報流出で問題となったファイル共有ソフト「ウィニー」の仕組みを解読し、監視ソフトを作るなど、日本を代表するホワイトハッカーとして知られる。

杉浦氏の会社は以前、専門知識と技量が試される問題をネット上で公開し、解いた人を採用する試みをしたことがある。そこで見えたのは「とびきり優秀だが社会になじめない人がいる」こと。若い人がネットの闇に陥ってサイバー犯罪に関与した結果、警察に摘発されて社会復帰が困難になるケースもある。協会の狙いは、こうした「とがった人材」の発掘。仕事を求めるハッカーが技術力や実績を登録し、協会のスタッフと面談やメールのやりとりをして紹介先を決めていく方針。家電製品や自動車などがネットにつながる時代を迎え、セキュリティ業界は慢性的な人手不足となっており、杉浦氏は「ハッカーが活躍する場がますます増える」とみる。当面はホワイトハッカーを目指す人の就業支援をメインに、人材をＰＲするするためのブログを立ち上げる。ゆくゆくは個人で活動するハッカーを支援するため、法的トラブルに巻き込まれた際の弁護士紹介などの業務も目指すという。

○ 「ｚａｉｆ」不正アクセス被害 仮想通貨67億円流出

仮想通貨交換業者「テックビューロ」（大阪市）は９月20日、運営する仮想通貨交換サイト「ｚａｉｆ（ザイフ）」が不正アクセスを受け、「ビットコイン」「ビットコインキャッシュ」「モンコイン」の３種類の仮想通貨計67億円相当が外部に流出したと発表した。同社によると、９月14日午後５時から同７時ころ、ザイフに不正アクセスがあり、顧客との入出金のためにインターネット接続した状態で保管していた仮想通貨が流出した。９月17日にサーバの異常を検知して18日に流出を確認、金融庁や大阪府警に届け出た。テックビューロは2014 年６月に設立。2017 年９月、金融庁から仮想通貨交換業者として認められた。近年の仮想通貨取引の急拡大に伴い会社も急成長した。しかし、金融庁への登録後もザイフで売買が一時出来なくなるなどのトラブルが頻発。今年２月には、仮想通貨を０円で販売するシステムトラブルが発生するなど、セキュリティ対策の不備を露呈した。金融庁は「顧客の資産を守るための対策が万全ではない」などとして、今年３月と６月の２回、同社に対し業務改善命令を出していた。今回の仮想通貨流出は、金融庁が改善命

令を出した３月以降、同社に対して実効性のあるリスク管理体制の構築を求め、提出された改善計画が実行されているか検証作業に入ろうとした矢先だった。

４ その他

○ サイバー損害 事前査定 ＮＴＴなど16社連合 モデル開発

ＮＴＴなど16 社で組織する日本サイバーセキュリティ・イノベーション委員会（ＪＣＩＣ、東京・港区）は、過去のサイバー攻撃で受けた被害の実例などを分析して、サイバー攻撃による損失額を事前に割り出す算出式（サイバーリスクの事前算定モデル）を作った。

これまで国内企業は具体的な被害額がわかりづらかったため、経営課題としての優先度は低かった。損失額を把握できるようにすることで防御ソフトの導入や専門の技術者確保などの投資を企業に促す。事前算定モデルでは、サイバー攻撃の被害で発生する損失額を「直接被害」と「間接被害」に分けて算出する。直接被害は個人情報の漏えいによる金銭被害や、事故対応費用といった４項目から構成する。間接被害は純利益の減少と時価総額への影響の２項目からなる。直接被害のなかの「個人情報漏えいによる金銭被害」を算出する場合、漏えいした個人情報の価値に、個人の特定しやすさや企業の社会的責任の大きさ、事後対応の適切さといった各要素に、被害状況に応じた度合いを掛け合わせて損害額を割り出す。度合いを示す係数は通信事業会社など約220社が参加する日本ネットワークセキュリティ協会が過去の情報漏えい被害の原因や判例の賠償額を調査して算出した数値を参考にした。

大量の個人情報の漏えいや数億円の金額を詐取されたりするサイバー攻撃の被害が国内でも相次いでいるが、サイバー対策に十分な予算を確保する国内企業は少ない。売上高500億円以上の企業に行った調査（2017年）によると、サイバーセキュリティ対策に１年間で3,000万円以上投資する企業は19.2%。47%の企業の投資額は1,000万円未満だった。投資が少ない原因について、ＪＣＩＣの梶浦代表理事は「災害などほかの経営リスクと比べて、どの程度対策に力を入れるべきかが判断できないため」と指摘する。このため、ＪＣＩＣは簡単に損害額を試算できるモデルを開発し、サイバー対策への取組を促すことにした。サイバー攻撃による被害額を算定する場合の標準モデルとして国内企業への普及・採用を働きかける。