サイバーセキュリティニュース（令和元年5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）

○ ユニクロ、ＧＵ 不正アクセス被害 顧客情報流出の可能性も

ユニクロを運営するファーストリテイリングは５月１４日、ネット通販サイト「ユニクロ公式オンラインストア」と「ＧＵ（ジーユー）公式オンラインストア」に不正アクセスがあったと発表した。同社によると、４月２３日から５月１０日までの間、顧客のアカウント４６万１０９１件に不正なログインがあり、顧客の名前、住所、電話番号、クレジットカード情報の一部などが閲覧された可能性があるという。同社では、閲覧された可能性がある顧客のパスワードを無効化し、パスワードの再設定と登録内容の確認を求めるメールを送付した。不正アクセスの手法は、他社サービスから流出した可能性のあるユーザＩＤ・パスワードを利用した「リスト型アカウントハッキング（リスト型攻撃)」と推測されている。

○ コジマ通販サイトもリスト型攻撃被害 カード情報の流出は無し

株式会社コジマは５月２３日、ネット通販サイト「コジマネット」に、リスト型攻撃と思われる不正アクセスがあったことを明らかにした。同社によると、顧客のアカウントに不正なログインがあり、氏名、住所、連絡先、メールアドレス、購入履歴などの情報が第三者に閲覧された可能性があるという。同社では、不正アクセスされたと思われるアカウントのパスワードを無効化し、パスワードの再設定を求めるメールを個別に送付した。今回の不正アクセスによって閲覧されたと思われる顧客情報には、クレジットカード情報は含まれていないとしている。

【リスト型アカウントハッキング（リスト型攻撃)】

ウェブサービスなどから流出したＩＤ・パスワードのリストを使って、他のサービスでログインを試みる攻撃手法のこと。利用者がとるべき対策は、ＩＤ・パスワードを使い回さないことです。同一のＩＤ・パスワードを複数のサービスで使い回していると、このＩＤ・パスワードが流出した場合リスト型攻撃によって、すべてのサービスに不正アクセスされる危険性があります。サービスごとに異なるＩＤ・パスワードを設定することで、仮にＩＤ・パスワードが流出しても当該サービスのＩＤ・パスワードを変更するだけで以後の不正アクセスを防ぐことができます。

○ 通販サイト 偽の決済画面でクレカ情報窃取、１．５万人分流出

正規の通販サイト上で偽のクレジットカード決済画面を表示させ、利用者が入力したカード情報を盗み取る手口が相次いでいることが分かった。電子書籍など少なくとも７つのサイトで偽画面が表示され、流出した可能性のあるカード情報は合計で約１万５千人分に上るという。被害は昨年から本年にかけて確認されており、このうち電子書籍販売「ディー・エル・マーケット」のサイトからは７７４１件、タオル販売「伊織」のサイトからは２１４５件のカード情報が流出した。流出したカード情報の一部は不正利用されていたという。今回の手口では、利用者が正規の通販サイトで商品を選び終え、支払いにクレジットカードを選択すると、本物そっくりの偽画面が表示される。偽画面にカード情報を入力するといったんエラーメッセージが表示されるが、前画面に戻ると、今度は正規のカード決済画面が表示される。再びカード情報を入力すると買い物が完了するが、偽画面に入力したカード情報はすでに犯人に送信されている。購入した商品は手元に届くため、利用者が被害に気付くのは非常に難しいという。犯人はサイトの欠陥を悪用して通販サイトのサーバに侵入し偽画面を仕込む。被害を受けたサイトの多くは、通販サイト構築用の無償ソフト「ＥＣ－ＣＵＢＥ（イーシーキューブ）」を使っており、同ソフト開発会社によると、ソフト自体の欠陥ではなく、設定の不備から生じた欠陥が狙われたという。このような手法でクレジットカード情報を盗み取る手口は「フォームジャッキング」「ウェブ版スキミング」などとも呼ばれる。

○ 札幌国際プラザ メールハッキングされ、迷惑メール大量送信

札幌市の公益財団法人「札幌国際プラザ」は５月１４日、同法人のメールアカウントに不正アクセスがあったことを発表した。同法人によると、本年４月２８日、代表メールアカウントが不正に使用され、約２２００件の迷惑メールが同アカウントから送信されたという。迷惑メールは英語で書かれ、出会い系サイトへ誘導する内容だった。送信に伴う被害は確認されていない。不正アクセスされたメールアカウントのパスワードは比較的推測しやすいものとなっており、パスワードが解析されて悪用されたとみられる。メールサーバの管理会社が４月２８日夜、短時間に大量のメールが送信されていることを検知し、発覚に至った。

○ フィッシング詐欺 巧妙化する手口の変遷

実在する企業などを装ったメールやメッセージを送りつけ、偽サイトに誘導し、ＩＤ・パスワードやクレジットカード情報などを盗み取るフィッシング詐欺について、「フィッシング対策協議会」の駒場一民氏によると、手口の変遷から詐欺グループの狙いが見えるという。フィッシング詐欺は、国内では２００４年頃から広がり始め、当初はヤフーアカウントやオンラインゲームのアカウントなどのＩＤ・パスワードが狙いだった。２０１４年頃になると、銀行を装ったメールから偽サイトに誘導してネットバンキングのＩＤ・パスワードを盗み取る手口が急増した。盗み取ったＩＤ・パスワードを使ってネットバンキング口座から勝手に送金する手口で、被害額も膨大になった（２０１５年の不正送金被害額は約３０億７３００万円 警察庁公表）。銀行側の対策として、一定時間で切り替わる「ワンタイムパスワード」を導入すると、今度はクレジットカードが標的となった。カード会社を装って偽サイトに誘導し、カード番号や有効期限などを入力させて盗み取る手口が出回った。２０１７年末になると、米アップルや通販大手アマゾンなどを装った偽サイトも登場した。クレジットカード情報を盗み取り、換金性の高い商品を購入して現金化するのが主な狙いで、その手口も、偽サイトに情報を入力させた後、正規サイトに誘導するなど巧妙化している。最近では、スマホのＳＭＳ（ショートメッセージサービス）を使ったフィッシングが増えている。宅配業者の不在通知を装ったＳＭＳで偽サイトに誘導し、アップルＩＤ・パスワードや、キャリア決済に必要な認証情報を盗み取る。フィッシング対策協議会には昨年、偽メールや偽サイトについて、前年比２倍超となる１万９９６０万件の相談が寄せられたという。次々と新たな手口を使うフィッシング詐欺に対処するために、フィッシング対策協議会では次のポイントを挙げている。

① 銀行やカード会社がメールでログイン情報などの確認を求めることはない。
② メールにリンクされたアドレスは開かず、サービスの専用アプリでアクセスする。
③ 詐欺メールを検知するセキュリティソフトを導入する。
④ 不審メールが届いた場合に備え、銀行やカード会社の問合せ先リストを用意する。

※ フィッシング対策協議会はフィッシングに関する最新情報を提供しています。
フィッシング対策協議会ＨＰ ： https://www.antiphishing.jp

○トレンドマイクロ、不正アクセス被害　機密情報の一部が流出

ウイルス対策ソフト「ウイルスバスター」で知られるトレンドマイクロは５月２０日、同社のコンピュータシステムが不正アクセスを受け、一部の機密情報が外部に流出したと発表した。不正アクセスを受けたのは、研究分析を行うテストラボ環境という領域で、ウイルスなどによってソフトウェアの不具合が生じた際、原因を突き止めるために作成するファイルの情報が流出したという。顧客情報や、ウイルス対策プログラムなど製品の根幹に関わる情報の漏えいはないとしている。発覚のきっかけは、米セキュリティ会社「アドバンスト・インテリジェンス」による調査だった。同調査によると、米国に拠点があるセキュリティ企業３社がロシア系とみられるハッカー集団のサイバー攻撃を受けたとしており、そのうち１社が米国に現地法人を持つトレンド社だったという。アドバンス・インテリジェンス社によると、ハッカー集団は「Ｆｘｍｓｐ」と名乗り、各国政府や企業から盗み取った情報を販売し、これまでに１００万ドル近い利益を得ているという。本年３月には、インターネット掲示板を介して接触してきた相手に、ロシア語で「大手ウイルス対策企業３社から盗み取った情報を独占的に提供する」と持ちかけ、不正アクセスの手口と合わせて「３０万ドル以上で販売する」と提案したという。

○ 東京五輪関連装う偽サイト続々、アドレスに注意

２０２０年東京五輪と関係があるかのように装った偽サイトが多数存在することが、トレンドマイクロと朝日新聞の調べで分かった。東京五輪公式サイトに接続されるアドレスは「tokyo2020.org」と「tokyo2020.jp」、オフィシャル商品販売サイトの「tokyo2020shop.jp」がある。調べによると、こうした公式サイトで使われている「tokyo2020」の単語を組み合わせた別のサイトが複数見つかり、少なくとも二つのアドレスが不正なサイトと確認できた。不正なサイトに接続すると「システム警告」「セキュリティシステムが破損しています」「最新ソフトをインストール」などのメッセージとともに偽のセキュリティソフト購入を求める画面が表示されたという。トレンドマイクロの岡本勝之氏は、正しいサイトかどうかアドレスをよく確認するよう呼びかけている。

※東京五輪チケットの当落に関する偽メールにも注意！

東京五輪チケットの抽選申込みが締め切りとなり、大会組織委員会では、当落に関する詐欺目的の偽メールが横行する可能性について注意喚起しています。組織委は抽選の当落に関する連絡について、申込者がＩＤ登録した際のメールアドレスに

対し、tokyo2020 のドメインで送付するとしています。また、メールにはリンクとなるＵＲＬは付さないとしています。これらと異なるメールは偽物の可能性が高く、注意が必要となります。

２ 国内外のサイバーセキュリティ情勢

○ ＩＰＡ 情報発信のためのツイッターアカウント開設

情報処理推進機構（ＩＰＡ）は５月９日、「情報セキュリティ安心相談窓口」の公式ツイッターアカウントを開設した。「情報セキュリティ安心相談窓口」は、ＩＰＡが一般向けに開設している窓口で、コンピュータウイルスや不正アクセス等に対する情報セキュリティについて相談を受け付け、技術的なアドバイスを行っている。よく寄せられる相談に対するＱ＆Ａ、タイムリーなテーマを取り上げた「安心相談窓口だより」等のコンテンツをＩＰＡのＨＰで公開している。今回新たに開設されたツイッターアカウント「@ＩＰＡ＿ａｎｓｈｉｎ」では、窓口に寄せられた相談内容をもとに、脅威に関する対策情報等を発信するとしている。すでに、２０１９年４月に寄せられた相談トップ３の内容がツイートされている。

【情報セキュリティ安心相談窓口公式ツイッター】　https://twitter.com/ipa_anshin

○ 防衛省 サイバー攻撃対策 反撃ウイルス作成へ

政府は、日本の安全保障を揺るがすようなサイバー攻撃を受けた場合に反撃するとして、防衛省でコンピュータウイルスを作成、保有する方針を固めた。相手の情報通信ネットワークを妨害するためのウイルスを防衛装備品として保有するのは初めてで、サイバー空間における新たな対処策となる。防衛省は、例として、政府機関や自衛隊の陸海空のネットワークシステムがサイバー攻撃を受け、部隊運用に支障を来すような事態を想定する。ウイルスによる反撃で相手軍のシステム利用を妨げ、陸海空による攻撃をさせにくくすることを狙うとみられる。関係者によると、ウイルスは最新技術を持つ複数の民間企業に委託し、共同で作成する。攻撃側に侵入を図るため、ネットワーク上に裏口を設けることができる「バックドア」と呼ばれるソフトなどが検討されているという。サイバー攻撃について政府は、武力行使３要件を満たすなら自衛権が発動され、ウイルスによる反撃ができるとの立場を示す。サイバー攻撃を未然に防ぐための先制攻撃としての使用は想定せず、あくまでも専守防衛の範囲内としている。

３ その他

○ 災害情報をＬＩＮＥで提供 政府、２１年にも開始

政府は、地震や大雨の災害発生時に無料対話アプリＬＩＮＥを使い、避難場所などの情報を提供する仕組みをつくる。被災者らが発信するメッセージをＡＩ（人工知能）が分析し、必要な物資の確保なども効率化する。国内利用者数７千万人を超えるＬＩＮＥを活用することで、多数の人と同時にやりとりし、個人の状況に合わせて必要な情報を届けることができる。防災科学研究所、情報通信研究機構、ＬＩＮＥなどは昨年１２月から神戸市で実証実験を始めた。「状況はどうですか」などチャットボット（自動応答システム）の問いかけに対し「家が倒壊した」などとメッセージや写真を送信してもらうことで、詳細な被災状況を大量に集める。被災者の位置情報をもとに、被害状況を一覧できる地図なども作成できるようになる。被災者が負傷している場合は、自治体がすぐに救護に向かう体制も整えるという。大規模災害が発生すると、デマ情報が錯綜し、正確な情報が被災者に届かないことがある。そのため、情報の整理にＡＩを活用し、情報の精度を向上させるほか、対応すべき情報の優先順位を決めるのに役立てる。災害に関する情報は政府や自治体の防災公式ＨＰなどで発信しているが、認知度は低く、一方的な情報提供が中心となっている。被災状況の把握に時間がかかっているほか、被災者へのきめ細やかな対応も課題となっており、ＳＮＳとＡＩを活用することで

災害対応の効率化を図るという。政府は２０２１年にもサービスの開始を目指す。