１．１．２　国内における情報セキュリティインシデント状況

国内における情報セキュリティインシデントの発生状況について、以下の資料を参照して解説する。

・三井物産セキュアディレクション株式会社（以下、ＭＢＳＤ社）による集計情報
・トレンドマイクロ社：２０１９年年間セキュリティラウンドアップ
・一般社団法人ＪＰＣＥＲＴコーディネーションセンター（ＪＰＣＥＲＴ／ＣＣ：Ｊａｐａｎ　Ｃｏｍｐｕｔｅｒ　Ｅｍｅｒｇｅｎｃｙ　Ｒｅｓｐｏｎｓｅ　Ｔｅａｍ　Ｃｏｏｒｄｉｎａｔｉｏｎ　Ｃｅｎｔｅｒ）：インシデント報告対応レポート
・フィッシング対策協議会：月次報告書

（１）情報セキュリティインシデントの発生状況

ＭＢＳＤ社が集計した結果によると、２０１９年度に報道された情報セキュリティインシデントの件数は２０１８年度の３０６件から４５８件に増加した（図１－１－７）。インシデントの種類別に見ても、いずれも前年度比で４割以上増加した。２０１８年度同様、最も件数が多いのは「不正アクセス」、最も件数が少ないのは「改ざん」だが、「改ざん」は前年度比で２倍以上に増加している。「不正アクセス」件数の増加は、ＩＰＡへの届出件数の増加にも表れている（「付録」の「資料Ｂ　２０１９年のコンピュータ不正アクセス届出状況」参照）。報道数や届け出件数が増加していることから、社会のインシデントへの意識や関心は高まっていると考えられる。

（２）Ｗｅｂサイト改ざんによる被害

２０１９年度にＪＰＣＥＲＴ／ＣＣへ報告されたＷｅｂサイトの改ざん総件数は９７６件であった。ここ数年の傾向を見ると、２０１６年度までは毎年３，０００件を超えていたが、２０１７年度は１，２５９件と大幅に減少し、２０１８年度、２０１９年度も減少傾向が続いている（図１－１－８）。なお、前項の図１－１－７における「改ざん」の件数は増加しているが、この件数にはデータベースやプログラムの改ざんも含まれているため、Ｗｅｂサイト閲覧者からの報告を集計した図１－１－８とは増減の傾向が異なるものと考えられる。

ＪＰＣＥＲＴ／ＣＣは、Ｗｅｂサイト改ざんの傾向について、２０１８年度に続き、不正に埋め込まれたスクリプトによって特定ブランドを扱うｅコマースサイトやアダルトサイト等、閲覧者が意図しないサイトに転送させる事例を報告している。２０１９年度に目立った手口として、ＷｏｒｄＰｒｅｓｓやＭａｇｅｎｔｏといった広く利用されているＣＭＳ（Ｃｏｎｔｅｎｔｓ　Ｍａｎａｇｅｍｅｎｔ　Ｓｙｓｔｅｍ）の脆弱性を悪用したものが確認されている（「１．２．４（２）ＣＭＳの脆弱性を悪用した攻撃」参照）。Ｗｅｂサイト改ざんの目的はウイルスの配布、特定のＷｅｂサイトへの誘導、クレジットカード情報等の個人情報や他の攻撃の手掛かりになるシステム情報の窃取等、多岐にわたる。減少傾向にあるとはいえ今後も継続的な対策が必要である。

（３）フィッシングによる被害

個人情報やクレジットカード番号、キャッシュレス決済等の各種サービスの認証情報等の詐取を目的としたフィッシングが継続している。ここ数年のフィッシング対策協議会への報告件数は、２０１７年度が１万１，２０５件、２０１８年度が２万２，５０３件と倍増し、２０１９年度には前年度の３倍超の７万３，５７６件と急増している（図１－１－９）。

ＪＰＣＥＲＴ／ＣＣで集計したフィッシングサイトの業界別件数の推移を見ると、２０１７年度以降「Ｅコマース」が最多で急増を続けており、２０２０年１～３月期に過去最多の１，７３９件を記録した、「金融機関」は２０１８年から緩やかな増加傾向にあったが、２０２０年１～３月期には急減し、２０１９年に入ってから増加し始めた「企業」に追い抜かれた（図１－１－１０）。今後は企業の偽サイトにも注意が必要となる。

また、ＪＰＣＥＲＴ／ＣＣが収集したフィッシングサイトのプロトコルについて、２０１７年からＨＴＴＰＳを使用したサイトが増加し始め、２０１８年には全体の４５％、また２０１９年には全体の５１％と半数以上のフィッシングサイトがＨＴＴＰＳを使用していたことが報告された。メールに記載されたＵＲＬがｈｔｔｐｓで始まるものでも簡単に信用してはならないことを認識したい。

２０１９年９月から１１月にかけて、フィッシングによるものと思われる不正送金被害が急増し、注意喚起が行われた。２０１９年１２月には同年８月の水準に戻ったものの、被害急増を背景として多要素認証の突破や、不正アプリ

をインストールさせて被害を拡大させる手口等、フィッシングの巧妙化が指摘されており、また、フィッシングサイトを手軽に作成・運用するツールも出回っているため、引き続き注意が必要である（フィッシングについては「１．２．６　個人をターゲットにした騙しの手口」参照）。

（４）注目された新たな脅威

トレンドマイクロ社の調査によると、２０１９年後半に「Ｅｍｏｔｅｔ」と呼ばれるウイルスの検出数が急増し、２０１９年第１～３四半期に毎期３００件未満だった検出数は２０１９年第４四半期（１０～１２月）に１万件を超えた。Ｅｍｏｔｅｔは２０１９年２月ごろから日本語のばらまき型メールで拡散されるようになり、日本の商習慣を利用する等、その手口も巧妙化してきた。２０１９年１０月からは、多数の法人組織で感染被害が公表され、被害件数が急増した（図１－１－１１）。２０１９年のＥｍｏｔｅｔ感染による国内での被害は情報漏えいや幹線端末から窃取した情報を元にしたなりすましメール送信が中心となっている（Ｅｍｏｔｅｔについては「１．２．５　ばらまき型メールによる攻撃」参照）。

国内におけるランサムウェア感染を目的とした攻撃の検出数は２０１７年以降、減少傾向にある（図１－１－１２）。しかし、法人での被害報告は２０１９年上半期にピークとなった（図１－１－１３）。法人被害報告の増加の要因として、これまで標的型攻撃（「１．２．１　標的型攻撃」参照）で用いられてきたような事前調査を伴う計画的な手口が用いられるようになったことが指摘されている。２０２０年６月に本田技研工業株式会社に対して行われたランサムウェアＳＮＡＫＥ（別名、ＥＫＡＮＳ）による攻撃では、目的のシステムにランサムウェアを感染させるためにネットワーク偵察等の事前調査や感染経路の確保等が計画的に行われた可能性があるとされる。その他、標的型攻撃にも利用されている攻撃ツールやサーバ等の脆弱性を悪用してランサムウェアに感染させる手口、海外では前述のＥｍｏｔｅｔを利用してランサムウェアに感染させる手口が確認されている。

２０１３年前後から表面化してきたパスワードリスト攻撃は２０１９年度も継続しており、２０１９年７月にはキャッシュレス決済サービス「７ｐａｙ（セブンペイ）」（以下、７ｐａｙ）における大規模な不正利用が発生した。

７ｐａｙは２０１９年７月１日よりサービスを開始したが、翌日から身に覚えのない取引があった旨の相談が寄せられ、株式会社セブン＆アイ・ホールディングス及び株式会社セブン・ペイが外部の情報セキュリティ会社とともに調査した結果、第三者がパスワードリスト攻撃により不正ログインしていた可能性が高いことが明らかになった。被害に遭ったアカウントは同月末の時点で８０８人分、被害総額は３，８６１万５，４７３円と発表されており、同年９月３０日には７ｐａｙのサービス自体が廃止された。

被害が継続している背景には、様々な要因によるＩＤとパスワードの漏えいと、それらの情報が蓄積されたリストの流通、そしてユーザのパスワードの使い回しがある。リストはダークウェブで販売される等、攻撃者の間で広く流通して悪用されるため、ユーザがパスワードを使い回している場合、ＩＤとパスワードのみによる認証ではセキュリティの担保にならない。サービス提供者には複数の端末からのログインの制限や多要素認証等の追加のセキュリティ対策の実施が求められ、同時にユーザにも、複数のサービスにおいてパスワードの使い回しをしない、サービス側から提供される追加のセキュリティ機能を利用する、または追加のセキュリティ機能があるサービスを選ぶといった対策が求められる。

２０２０年１月より、ウィルスやフィッシング、詐欺等の攻撃メールにおいて新型コロナウイルス感染症（以下、新型コロナウイルス）の流行に便乗した文面が確認されている。また、新型コロナウイルスの感染拡大を防ぐ目的で、テレワークや個人が所有する端末を業務で利用するＢＹＯＤ（Ｂｒｉｎｇ　Ｙｏｕｒ　Ｏｗｎ　Ｄｅｖｉｃｅ）といった業務形態が急速に普及しており、使用するシステムや端末のセキュリティ対策強化の必要性が指摘されている（「１．３．１　（３）リモートデスクトップサービスに関連する脆弱性について」参照）。今後も新型コロナウイルスの流行や対策に伴う政策やサービスに便乗した新たな詐欺の手口や攻撃の出現が懸念され、引き続き警戒が必要である。

出典：情報セキュリティ白書２０２０（Ｐ１１～Ｐ１３）

独立行政法人情報処理推進機構