NAD MonthlyReport.

MarketFlash

サイバーリスクマネージメント
～最近のサイバー攻撃～

2018.06

日本アルプス電子株式会社
NIHON ALPS ELECTRONICS CO.,LTD.

サイバーリスクマネージメント
サイバー攻撃の最新動向

近年のIOTやAIの発展により、インターネットは益々ビジネスには欠かせないものとなっている。一方で、サイバー攻撃による被害は年々増加している。その攻撃による被害は、個人情報などの漏洩に限らず、ウイルス感染やDOS攻撃による企業活動そのものが停止するなどの損害が発生している。そして、企業売上、収益の減少ばかりでなく、企業の信用失墜、ブランドイメージの毀損など経営に大きなダメージを与えることになる。
企業経営者としては、年々深化するサイバー攻撃の手口などの情報を収集することはもちろんのこと、それらに備える社内体制の構築に努めることが重要な経営課題となっている。

独立行政法人情報処理推進機構が公表した「情報セキュリティ10大脅威2017」によると、第1位は、「標的型攻撃による情報流出」である。2014年のベネッセによる約3500万人の個人情報漏洩、2016年においても日本年金機構やJTBなどの大規模な情報漏洩インシデントが発生している。第2位は、「ランサムウェアによる被害」である。これは、標的型攻撃とは違って、個人も含めて広く拡散するウィルス型の攻撃であり、その被害は広範にに及んでいる。この「ランサムウェア」の攻撃は前年においては第7位であったが、2017年においては、その攻撃が急増するリスクが高まっている。

順位	脅威	昨年順位
1	標的型攻撃による情報流出	1
2	ランサムウェアによる被害	7
3	ウェブサービスからの個人情報の窃取	3
4	サービス妨害攻撃にゆるサービスの停止	4
5	内部不正による情報漏洩とそれに伴う業務停止	2
6	ウェブサイトの改ざん	5
7	ウェブサービスへの不正ログイン	9
8	IOT危機の脆弱性の顕在化	ランク外
9	攻撃のビジネス化（アンダーグランドサービス）	ランク外
10	インターネットバンキングやクレジットカード情報の不正利用	8

このような標的型攻撃やランサムウェアによる広範囲型攻撃など、サイバー攻撃の手口は年々巧妙化かつ多様化してきている。
AIやIOTの普及が進むと、それに利用されるデバイスの数は増加し、情報もますます複雑化する。サイバーリスクマネジメントは今や企業経営の重要課題である。しかし、そのセキュリティ対策は完全ではなく安全なものではなく完璧な解決法はないということを踏まえ、環境は常に侵害されることを前提にサイバーリスクに対する対策を立てる必要がある。
社内におけるサイバー攻撃に対する危機管理体制をどのように構築していくか検討していく必要がある。また、自社だけで手に負えないリスクに対しては、サイバー保険を利用することも有効である。

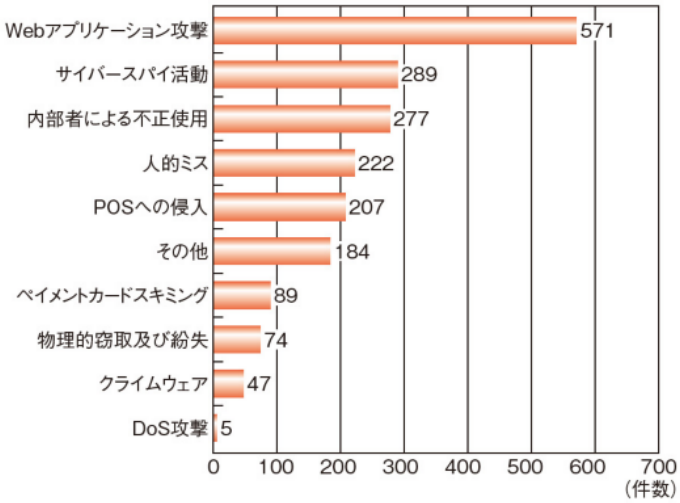
次ページ以降、最近のサイバー攻撃の動向・手口などについての情報をまとめてみた。

サイバーリスクマネージメント 情報セキュリティ白書2017

情報セキュリティインシデントは世界各国で発生しており、その規模や影響は年々拡大している。2016年においても、大規模な情報漏えい、サイバー攻撃を許すきっかけとなるスパムメールや脆弱性の放置、フィッシングサイト、またランサムウェアやビジネスメール詐欺等の金銭被害に直結する事象が確認されている。国内においても、ランサムウェアが検出された機器の台数が最大となり、AppleInc.やMicrosoftCorporation（以下、Microsoft社）等の身近なサービスをかたったフィッシングサイトが増加する等、サイバー攻撃の脅威が増している。

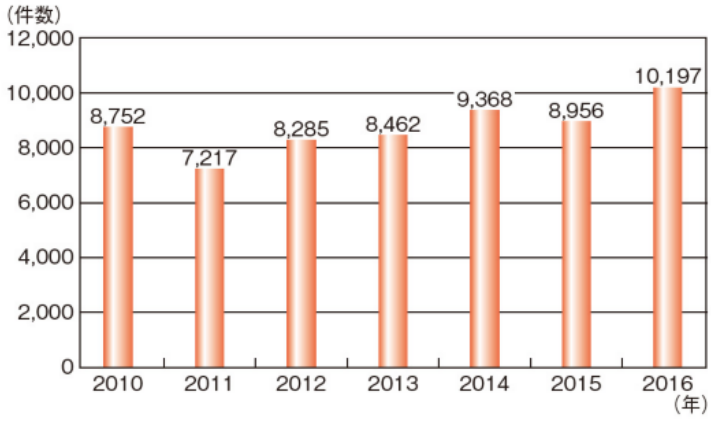
(1)情報漏えいインシデントの状況

2016年4月、パナマの法律事務所であるMossackFonsecaから流失した、1,150万件の租税回避に関する文書、並びに関与する21万4,000社の企業名や首脳等の著名人の情報（日本在住者・企業約400を含む）が公開された。2016年12月には、米国Yahoo!が2013年に10億人、2014年に5億人のアカウント情報が情報漏えいしたことを公表し、単一組織からの漏えい件数としては過去最悪となった。IBM社によると、漏えいしたデータ件数は、2014年は約10億件、2015年は約6億件と減少し、2016年は約40億件と急増した。Symantec社でも、2014年は約12.2億件、2015年は約5.6億件と減少し、2016年に約11.2億件と、2016年に再び増加したと報告している。Symantec社によると、情報漏えいインシデントが発生した件数を業種別に見ると、最も件数が多い業種は「サービス」で452件、次いで「金融、保険、不動産」が226件、「製造」が116件、「小売業」が84件となっている。Verizon社が1,935件の情報漏えいインシデントの攻撃方法を分析した結果を見ると、2015年と同様に2016年も「Webアプリケーション攻撃」が571件と最も多い（2015年は908件）。2015年に2位であった「POSへの侵入」（525件）が2016年は207件と大幅に減少している（図1-1-1）。



■図1-1-1　情報漏えい事件の分類

（出典）Verizon社「2017 Data Breach Investigations Report」を



■図1-1-2脆弱性の公開件数の推移

（出典）IBM社「IBMX-ForceThreatIntelligenceIndex2017」を基にIPAが編集

(2)脆弱性情報の公開件数

サイバー攻撃の足がかりとなるOSやアプリケーションの脆弱性の動向を示す。IBM社によると、脆弱性の公開件数は増加傾向にあり、2016年には1万件を超え過去最多となった(図1-1-2)。

(3)メールを介したサイバー攻撃

Symantec社によると、全世界のメール中のスパムの割合は2014年から2016年にかけて50%以上で推移している。また、マルウェアが添付されたメールを受信する頻度は増加傾向にあり、2014年は244通に1通、2015年は220通に1通、2016年は131通に1通であった。主な要因として、Symantec社はメール配信へのボットネット(ウイルス感染等により攻撃者の自由に操られる状態となったパソコン等の機器(「ボット」と呼ばれる)を束ねたネットワークのこと。DDoS攻撃やスパムメールの送信等に悪用される。)の活用を挙げた。トレンドマイクロ社は国内でも1台のボットから1ヵ月にマルウェアが添付されたスパムメール総計約25万件の配信を確認しており、今後もサイバー攻撃の突破口として、ボットネットから自動配信されるメールの割合が高まることが推測される。

(4)ビジネスメール詐欺の脅威

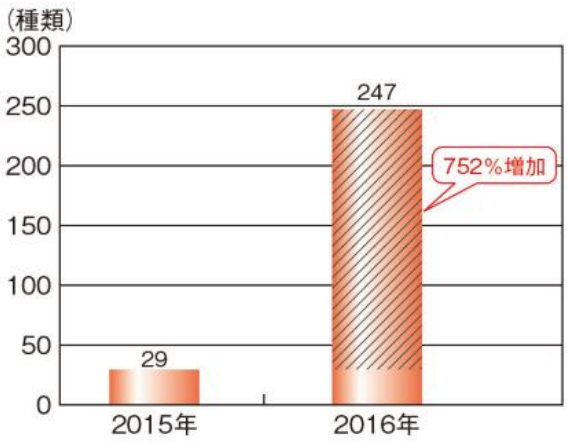
トレンドマイクロ社によると、取り引き先になりすました偽メールの指示に従い金銭を騙し取られるビジネスメール詐欺(BusinessEmailCompromise:BEC)による被害が増加しており、世界92ヵ国において詐欺メールの受信が確認された。受信件数の上位国は、米国(37.55%)、英国(9.61%)、香港(2.85%)、日本(2.75%)、インド(2.39%)の順となる。ドイツの自動車用配線メーカであるLeoniAGが約51億円、米国の金融系ITサービス企業SS&CTechnologies,Inc.が約6.8億円を騙し取られる等、世界において、一企業あたり平均約1,590万円の被害が報告された。NRIセキュア社の米国とシンガポールにおける調査では、米国企業の87%、シンガポール企業の86.5%がBECの詐欺メールを受信し、米国企業の45.6%、シンガポール企業の24.6%が金銭被害に遭っている。

FBI(FederalBureauofInvestigation:米国連邦捜査局)は2013年よりBECについて注意喚起しており、2017年2月には、届け出された被害総額が約30億ドルを超えたと発表した。BECの特徴として、攻撃者は出張や会議等で多忙な経営層や財務責任者を装う場合が多く、すぐに電話で連絡が取れなくても不自然でないことや、緊急を装う等により攻撃対象者の心理を巧妙に操り金銭を詐取するという。

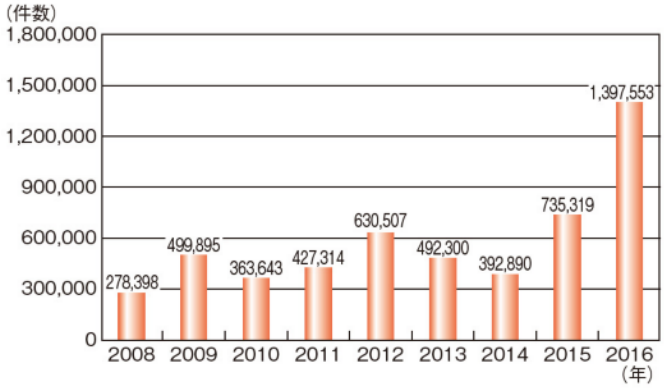
(5)ランサムウェアの巧妙化

利用者の意図に反しパソコンやスマートフォンに保存した電子データを暗号化し、復号するための身代金を請求する「ランサムウェア」も増加傾向にある。トレンドマイクロ社によると、2016年に観測された新種のランサムウェア(新ファミリー※14)は247種類と前年の29種類から急増した(図1-1-4)。その要因として、教育目的で公開された「HiddenTear」「EDA2」等のオープンソースのウイルスの悪用や、Ransomware-as-a-Service(RaaS)の普及を挙げている。

サイバーリスクマネージメント
情報セキュリティ白書2017



■図1-1-4新種のランサムウェア数（新ファミリー数）
（出典）トレンドマイクロ社「2016年年間セキュリティラウンドアップ」を基にIPAが編集



■図1-1-5　世界における届け出されたフィッシングサイト件数
（出典）APWG「Phishing Activity Trends Report」（2008年～2016年）を基にIPAが作成

Symantec社によると、ランサムウェアの亜種は2014年に6.8万種、2015年に34.2万種、2016年には24.1万種が確認された。2016年の感染者の割合は、一般利用者が69%、企業が31%と、一般利用者がより被害に遭う傾向にある。また、身代金の平均額は1,077米ドルで、2015年の294米ドルから大幅に上昇しており、被害者の34%が身代金を支払ったという。こうしたランサムウェアによる被害を低減するために、2016年7月、オランダ警察や欧州刑事警察機構（Europol）、セキュリティ企業が「TheNoMoreRansomProject※16」を立ち上げ、2017年4月現在、世界各国の官民89組織が加盟している。本プロジェクトでは、ランサムウェアへの感染低減施策として、ランサムウェアの解説やデモビデオの公開、対策の助言や復号ツール（2017年4月現在38種類の復号ツールを公開）等を提供している。ランサムウェアは今後も増え続けることが推測されるため、どのような新しい攻撃があるかを常に把握し、対策をとることが重要である。

（6）フィッシングサイトの増加

APWGによると、2016年のフィッシングサイトの総数は約140万件であり、2015年と比較し90%増加し、過去最大となった（図1-1-5）。Verizon社によると、攻撃キャンペーンごとのフィッシングのリンクや添付ファイルをクリックした業種別の割合は、「製造業」が13.4%と最も高く、次いで「情報通信」「小売り」「ヘルスケア」の順に高い。
また、Symantec社が2016年度にファイルレスマルウェア（マルウェアの一種。ハードディスクにファイルを残さず悪意のあるコードをメモリやOSのレジストリなどに埋め込むことで不正な活動を行うマルウェアのこと）が増加傾向にあると指摘していることや、多くの報告書で世界的にビジネスメール詐欺等の広まりが指摘されていることから、2017年においては、巧妙化するサイバー攻撃だけでなく、ITを巧みに悪用した詐欺にも留意することが重要である。

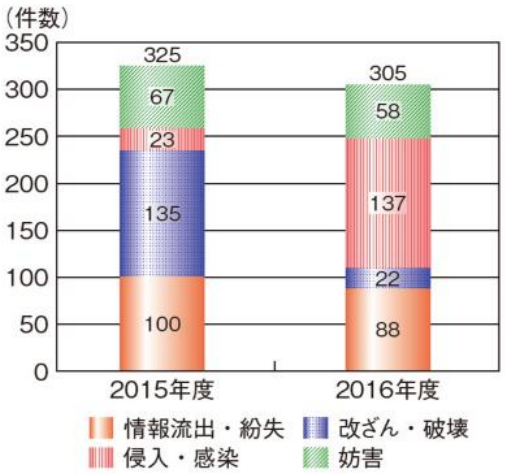
サイバーリスクマネージメント 情報セキュリティ白書2017

国内における情報セキュリティインシデント状況

(1)情報セキュリティインシデントの発生状況

MBSD社が2016年度に報道された情報セキュリティインシデントを集計した結果、2015年度の325件から305件に減少した(図1-1-6)。内訳を見ると、「妨害」行為の内容はフィッシング攻撃が大半を占めており、金融機関やクレジットカード会社が引き続き注意喚起を行っている。「侵入・感染」では、中央官庁や自治体等の公的機関を狙った意図的攻撃による不正アクセスが目立った。また、大学等の専門の管理者が不足がちな組織のサーバを踏み台として悪用される事例が複数報告された。

NRIセキュア社の調査では、過去1年間に発生した情報セキュリティに関する事件・事故で最も多かったのは2015年度に引き続き「誤送信・誤配送」(35.6%)であった。しかし、「サイバー攻撃」に分類される「標的型メール攻撃」(34.1%)、「マルウェア感染」(31.0%)がいずれも大幅に増加しており、2015年度に2位だった「情報機器、外部記憶媒体の紛失・置き忘れ・棄損」(28.9%)を超えた。「ランサムウェアによる金銭等の要求」も32.5%と高い割合となっている(図1-1-7)。



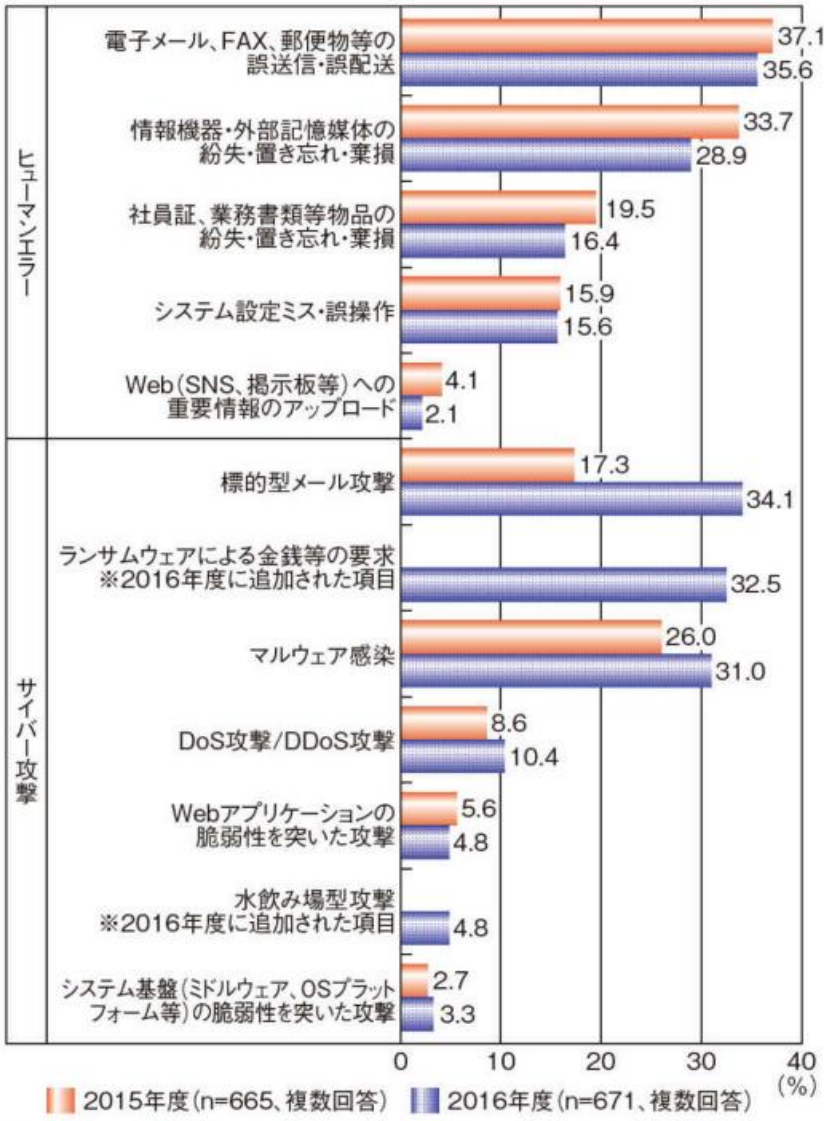
■図1-1-6 情報セキュリティインシデントの事象分類

(出典) MBSD社「サイバーセキュリティ事件簿」を基にIPAが

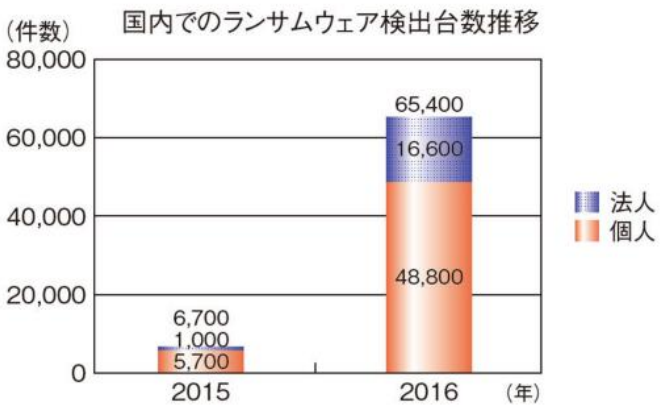
NRIセキュア社は、「標的型メール攻撃」の増加の一因として、各社の対策が強化されたことで今まで見過ごされていた攻撃が検知されていることを挙げている。また、ヒューマンエラーに起因する事件・事故がわずかながらも減少傾向にあることについては、情報セキュリティへの関心の高まりを受けて、セキュリティ対策が意識して取り組むべきことから、当たり前に実施すべきことへと変わってきているのではないかと考察している。トレンドマイクロ社は、日本でのランサムウェア検出台数、被害報告件数が過去最大となった2016年を「日本におけるサイバー脅迫元年」と称している。2016年のランサムウェア検出台数は2015年の9.8倍の6万5,400件、被害報告件数は2015年の3.5倍の2,810件と急増している(図1-1-8)。検出台数の割合の少なさに比べ、法人利用者からの被害報告件数が全体の8割以上を占めていることから、ランサムウェアによるネットワーク上のファイルを含めたデータの暗号化が、法人の業務継続に深刻な被害を与えていると述べている。

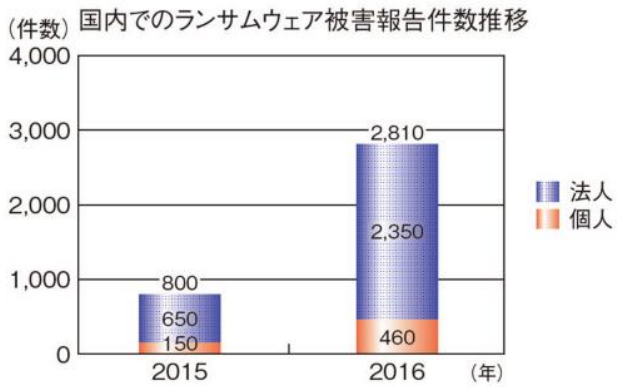
サイバーリスクマネージメント
情報セキュリティ白書2017

。



■図1-1-7　過去1年間で発生した事件・事故の対比



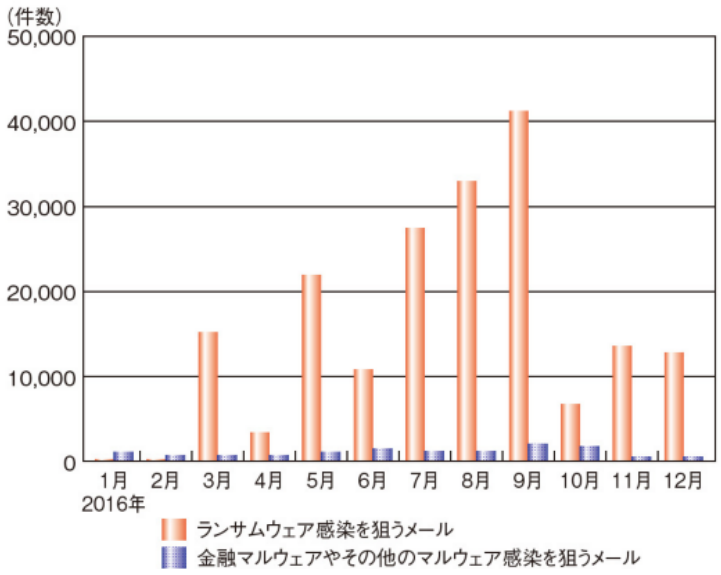


■図1-1-8　国内でのランサムウェアの検出台数と被害報告件数の推移

サイバーリスクマネージメント 情報セキュリティ白書2017

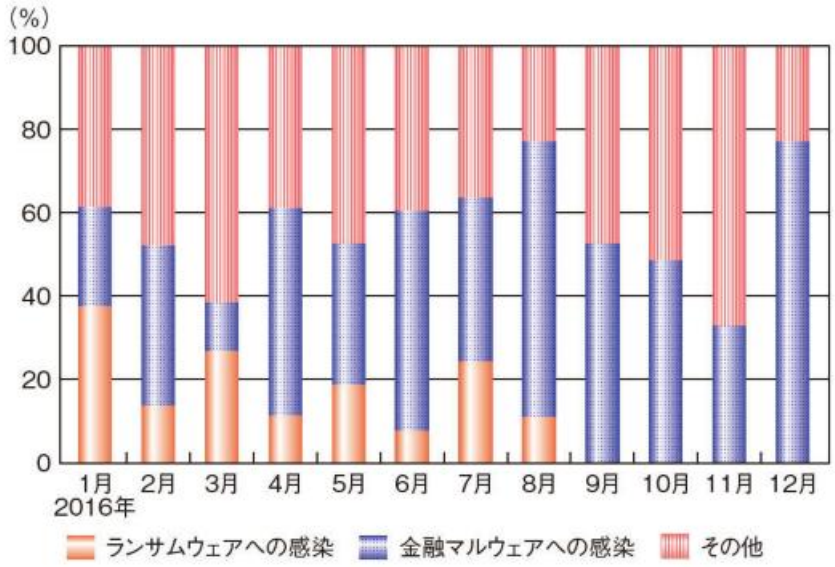
日本IBM社は、2016年下半期（7～12月）にTokyoSOCで検知した悪意のあるファイルが添付されたメール（図1-1-9）の94.9%がランサムウェア「Locky」への感染を狙ったものであり、残りは不正送金ウイルスやその他のウイルスへの感染を狙うものだったと報告している。

TokyoSOCで2016年に検知したランサムウェアへの感染を狙ったメールで、件名や添付ファイル名に日本語が利用されていたのは、2016年4月前半に検知された「CRYPTOLDESH」への感染を目的とした攻撃のみだった。一方、トレンドマイクロ社では2016年10月から11月に、法人利用者を狙う日本語のメールを使用したランサムウェアを確認している。日本IBM社によると、2016年8月まではランサムウェアへの感染を示す通信があったが、9月以降は確認されていない（図1-1-10）。ただし、図1-1-9に示したとおり、ランサムウェアの感染を試みる攻撃は継続して確認されており、引き続き注意する必要がある。



■図1-1-9悪意のあるファイルが添付されたメールの検出数推移

メールを悪用したランサムウェアの大規模拡散の増加や新たなランサムウェアの登場、日本語のメールで日本法人を狙うランサムウェア攻撃等により、被害が更に拡大する恐れがあり、対策の強化が求められる



■図1-1-10　クライアントPCへのマルウェア感染種別の内訳の割合

サイバーリスクマネージメント
個人情報を狙った攻撃

情報セキュリティインシデント別の状況と事例

＜個人情報の大量取得を狙った攻撃による情報漏えい＞

サーバを狙った不正アクセスや、パスワードリスト攻撃（脆弱なWebサイトなどから窃取したIDとパスワードの組み合わせ情報を用い、他のWebサービスにログインを試みる攻撃）、アカウント情報を不正利用した事例のほか、株式会社ジェイティービー（以下、JTB）の事例のような、内部端末を狙った標的型攻撃による大規模な情報漏えいの可能性がある事例も報告された。

（1）サーバを狙った不正アクセスによる情報漏えい

管理や対策が不十分なサーバに存在する脆弱性を狙った外部からの不正アクセスによる情報漏えい被害が多発した。被害の中には、氏名や生年月日、住所等の情報だけでなく、クレジットカード情報まで窃取された事例もある。GMOペイメントゲートウェイ株式会社の事例では、運営受託している複数のサイトにおいてApacheStruts2の脆弱性を悪用した不正アクセスにより、メールアドレスやクレジットカード情報、最大延べ約72万件の情報が流出した可能性がある。他にも、同脆弱性を悪用した攻撃による情報流出被害が複数確認されている。株式会社J-WAVEの事例では、Webサーバで利用しているソフトウェア「ケータイキットforMovableType」の脆弱性を悪用したOSコマンドインジェクション攻撃（脆弱なサーバーに対して、OSコマンドを埋め込んだ要求を送信し、不正にコマンドを実行させる攻撃）により、氏名、住所、メールアドレス、電話番号等、約64万件の個人情報が流出した可能性がある。同ソフトウェアを利用していた他企業においても、個人情報が流出した被害が複数確認されている。株式会社ザ・キッスの事例では、運営するサイト「THEKISSONLINESHOP」に不正アクセスの痕跡が見つかったことから調査を実施したところ、原因となるプログラムを特定し削除することができた。しかし、後日、犯人と思われる者から連絡があったため、再度調査を実施したところ、最大で約20万件の会員登録情報（ユーザID、暗号化パスワード、氏名、住所、電話番号、メールアドレス等）、及びクレジットカードを利用した顧客の延べ537件の個人情報（氏名、クレジットカード番号、セキュリティコード等）が流出した可能性が判明した。株式会社SynaBizの事例では、運営するサイト「NETSEA」のWebサーバの脆弱性を突いた攻撃により、約13万件の情報が流出した可能性がある。流出した可能性のある情報には、氏名、住所、電話番号、メールアドレス等の個人情報のほか、約7,000件のクレジットカード情報が含まれる。その他、サーバに対する外部からの不正アクセスによる情報漏えいが発生した事例を表1-2-1に示す。

（2）パスワードリスト攻撃による情報漏えい

株式会社サイバーエージェントを狙ったパスワードリスト攻撃では、同社が運営するブログサービス「Ameba」に対して、2016年4月29日から5月7日にかけて約220万回の不正ログイン試行が確認されている。そのうち約5万件のアカウントで不正ログインが成功していた。これにより、メールアドレスや生年月日等の情報を不正に閲覧された可能性があることが判明した。更に、同サービスにおいては2016年11月25日から11月28日にかけても約3,755万回の不正ログイン試行があり、そのうち約59万件で不正ログインの成功が確認された。株式会社ディー・エヌ・エーを狙った攻撃では、2016年1月9日から4月1日までの約3ヵ月にわたり、最大約10万件の不正ログインが確認され、生年月日、性別、地域等の情報を不正に閲覧された可能性があることが判明した。その他のパスワードリスト攻撃が原因とされる事例を表1-2-2に示す。

サイバーリスクマネージメント
個人情報を狙った攻撃

。

運営会社	公表日	被害内容
日本テレビ放送網株式会社[*55]	2016年4月21日	同社のWebサイトで利用しているソフトウェアの脆弱性を悪用したOSコマンドインジェクションにより、氏名、住所、電話番号、メールアドレス等の情報、最大42万8,138件の漏えいの可能性がある。
エイベックス・グループ・ホールディングス株式会社[*56]	2016年4月28日	同社のWebサイトで利用しているソフトウェアの脆弱性を悪用したOSコマンドインジェクションにより、氏名、住所、電話番号、メールアドレス等の情報、約64万件の漏えいの可能性がある。
株式会社講談社[*57]	2016年6月22日	同社が株式会社ウェアハートと共同運営している通販サイト「NET ViVi Coordinate Collection」のサイトにおいて、外部からの不正アクセスにより、氏名、住所、メールアドレス、電話番号等の情報、1万946件の漏えいが判明した。
公益財団法人東京動物園協会[*58]	2016年7月7日	同協会が運営するWebサイトにおいて、外部からの不正アクセスにより掲載記事が改ざんされ、更に同協会が発行するメールマガジンの登録者等に関するメールアドレス、2万1,688件の漏えいが判明した。
株式会社エフエム愛知[*59]	2016年7月25日	同社が管理しているサーバに対する外部からのSQLインジェクション[*60]により、電話番号、メールアドレス等の情報、11万4,581件の漏えいが確認された（うち、電子メールアドレス及びパスワードが流出した可能性のあるのは5万4,148件）。
軒先株式会社[*61]	2016年8月26日	同社が運営するWebサイト「軒先パーキング」において、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報、最大11万1,959件と、クレジットカード情報（セキュリティコードを含む）、最大3万8,201件の漏えいの可能性がある。
株式会社アドプリント[*62]	2016年9月15日	同社が運営するWebサーバ、データベースサーバにおいて、外部からの不正アクセスにより、住所、電話番号、メールアドレス、クレジットカード情報、最大1万4,627件の漏えいの可能性がある。
カゴヤ・ジャパン株式会社[*63]	2016年9月16日	同社が管理しているデータベースサーバの脆弱性を悪用したOSコマンドインジェクションにより、氏名、住所、電話番号、メールアドレス等の情報、最大4万8,685件の漏えいの可能性がある。そのうち、最大2万809件はクレジットカード情報の漏えいの可能性がある。
株式会社エンファクトリー[*64]	2016年10月3日	同社が運営しているオンラインショップ「STYLE STORE」及び「COCOMO」の2サイトにおいて、脆弱性を悪用した攻撃により、氏名、住所、電話番号、メールアドレス、クレジットカードの情報、最大3万8,313件の漏えいの可能性がある。
株式会社椿本チエイン[*65]	2016年11月14日	同社が運営するWebサイト「TT-net」において、外部からの不正アクセスにより、氏名、メールアドレス、ログインユーザ名、パスワードが最大6万4,742件漏えいした可能性がある。
株式会社帆風[*66]	2016年12月29日	同社が運営するオンラインショップ「パンフーオンラインショップ」において、外部からの不正アクセスにより氏名、住所、生年月日等の個人情報、最大1万6,084件と、クレジットカード情報、最大835件の漏えいの可能性がある。
日販アイ・ピー・エス株式会社[*67]	2017年1月5日	同社が管理するサーバに外部からのSQLインジェクションにより、会員ID、メールアドレス等、最大延べ13万1,936件の情報流出の可能性がある（うち、38件の暗号化前のパスワード、30件のクレジットカード情報を含む）。
クラウドゲームス株式会社[*68]	2017年1月13日	同社が運営するWebサーバにおいて、外部からの不正アクセスによりユーザ名、ユーザID、パスワード、メールアドレス等の個人情報、計14万408件の漏えいの可能性がある。
ロングランプランニング株式会社[*69]	2017年1月27日	同社が運営するWebサイトにおいて、外部からの不正アクセスにより、氏名、住所、電話番号、メールアドレス等の情報、最大2万2,276件の漏えいの可能性がある（うち、2,523件のIDとパスワードを含む）。
株式会社Flavor[*70]	2017年2月22日	同社が運営するオンラインショップ「Re:CENO公式オンラインショップ」において、Webアプリケーションの脆弱性を悪用した外部からの不正アクセスによりクレジットカード情報、最大1万7,085件の漏えいの可能性がある。
学校法人法政大学[*71]	2017年3月10日	同学が管理するサーバにおいて、外部からの不正アクセスにより、氏名、メールアドレス、パスワード（暗号化されている）等、最大4万3,103件の情報流出の可能性がある。
独立行政法人日本貿易振興機構[*72]	2017年3月10日	同機構が運営しているWebサイトにおいて、Apache Struts2の脆弱性を悪用した不正アクセスにより、メールアドレス2万6,708件の情報が流出した可能性がある。
日本郵便株式会社[*73]	2017年3月14日	同社が運営しているWebサイト「国際郵便マイページサービス」において、Apache Struts2の脆弱性を悪用した不正アクセスにより、送り状1,104件、メールアドレス2万9,116件の情報が流出した可能性がある。

■表1-2-1　不正アクセスによる情報漏えい

サイバーリスクマネージメント
個人情報を狙った攻撃

運営会社	公表日	被害内容
株式会社ディノス・セシール[※76]	2016年9月1日	同社が運営する「セシールオンラインショップ」において、第三者によるログイン試行が2016年8月31日に50回、同9月3日に30回確認された。そのうち、計15件のアカウントで不正ログインが確認された。
株式会社マーケティングアプリケーションズ	2016年10月24日	同社が運営するアンケートリサーチサイト「アンとケイト」において、第三者によるログイン試行が2016年10月5日から10月7日にかけて20万9,003回確認された。そのうち、96件のアカウントで不正ログインされ、メールアドレスの改ざんや不正なポイント交換が確認された[※77]。
東北電力株式会社[※78]	2016年11月16日	同社が運営するWebサービス「よりそうeねっと」において、2016年11月10日から11月15日にかけて第三者による大量のログイン試行が確認された。これにより、約1,400件のアカウントで不正ログインされ、そのうち540件で不正なポイント交換が確認された。
ピクシブ株式会社[※79]	2016年12月2日	同社が運営する「pixiv」において、2016年11月29日から12月2日にかけて第三者によるログイン試行が確認された。これにより、3,646件のアカウントで不正ログインが確認された。
ポケットカード株式会社	2016年12月15日	同社が運営する会員専用ネットサービス「ネットカウンター」において、2016年12月上旬ごろより、第三者によるログイン試行が確認された。これにより、118名の会員が不正ログインされ、不正なポイント交換が確認された[※80]。
DeSCヘルスケア株式会社[※81]	2017年2月10日	同社が運営する「KenCoM」において、第三者による大量のログイン試行が確認された。これにより、435件のアカウントで不正ログインが確認され、総額2万4,400円相当のポイントが不正取得された可能性がある。

■表1-2-2　パスワードリスト攻撃による情報漏えい

(3)アカウント情報の不正利用による情報漏えい

アカウント情報を不正利用されたことによる情報漏えい被害も発生している。株式会社優良住宅ローンの事例では、同社が管理するメールサーバの管理者権限のIDとパスワードを何らかの方法で第三者が取得、その情報を用いて不正ログインされた。このとき、役職員5名のメール設定を変更されたことで、2016年9月10日から9月30日までの間に当該役職員が受信したメールが外部に転送されていた。氏名、住所、電話番号、生年月日、メールアドレス、勤務先、年収、口座情報等が含まれる約3万7,000名の顧客情報がメール転送により漏えいした。パスワードリスト攻撃やアカウントの不正利用等による情報漏えい被害を防止するために、サーバの脆弱性対策だけでなく、管理者及び利用者の適切なパスワード管理も不可欠である。

(4)標的型攻撃による情報漏えい

2016年6月、JTBは、グループ会社である株式会社i.JTBが管理するサーバから約678万件の情報が流出した可能性があると公表した。流出した情報には、利用者の氏名、生年月日、住所、電話番号、メールアドレス、メールアドレス、パスポート番号等の情報が含まれる。公表された内容によれば、取り引き先になりすましたメールの添付ファイルを社員が開いたことで社内のパソコンがウイルスに感染し、その後、外部からの遠隔操作によって内部感染が広がりサーバに侵入されたという。

2015年度の日本年金機構の情報漏えい被害と同様に、サーバの脆弱性等を突いた攻撃ではなく、巧妙なメールにより、内部のパソコンをウイルスに感染させる標的型攻撃であった。

サイバーリスクマネージメント
個人情報を狙った攻撃

(5)内部者の故意による情報漏えい

2014年に発生した内部不正による大規模情報漏えい事件をきっかけに、企業では内部不正対策の重要性が認識されるようになった。しかし2016年度も、退職者による技術情報流出や従業員による不正な情報持ち出し等が相次いでいる状況は変わっていない。内部不正は、持ち出された情報が競合他社に盗用される、または別の犯罪の足掛かりにされる等によって、組織の信用や利益に直接影響を与える重大な脅威である。
2016年度に発生した国内の主な内部不正事件を表1-2-5に示す。

(a)個人的利得を目的とした内部者による事例

事例4、7は、公的機関の契約・臨時職員が、業務のために与えられたシステムへのアクセス権限を悪用し、個人情報を盗み見た事例である。契約・臨時職員は、内部不正により得られた情報を基に、女性へのストーカー行為や住居侵入を行っている。このような個人的な事情(動機)を組織が把握することは困難である。この場合には、「捕まるリスクを高める(やると見つかる)」対策が有効である。具体的には、「システムのアクセスログを記録する」「監視カメラを設置する」等の監視を強化する対策が挙げられる。また、取得した「ログの内容を確認する」こと、及びログの取得を周知することも重要である。ログ監視ツールを導入した企業の例では、導入の周知前と周知後を比較すると、周知後には情報の持ち出しが減っていたという。監視を周知することは不正抑止効果があるといえる。

事例番号	報道時期	不正行為者	概要
1	2016年5月	役員	北海道のプロパイダ代理店「日本ネットワーク」役員が、インターネットサービスプロバイダ株式会社DEXから不正に持ち出された約8万7,000人分の顧客情報を購入し、勧誘目的で使用したとして不正競争防止法違反(営業秘密の使用)の容疑で逮捕された[*118]。
2	6月	退職者	岐阜県岐阜市内のプロパンガス会社の社員(当時)が、同社の営業秘密である顧客情報等を不正に取得し同業他社に開示したとして、不正競争防止法違反(営業秘密の領得、開示)の容疑で逮捕された。社員は会社に不満を持っていたことから、顧客情報等を会社のパソコンから不正に入手し、情報を封筒に入れて県内の同業他社に送っていたが、「この情報を使って会社をつぶせ」という不審な内容のメモが添付されていたことから、受け取った会社がすべての情報をこの会社に返却した[*119]。
3	6月	退職者	愛媛県松山市の元職員が、同市が管理する特定健康診断の対象者名簿等、約13万件の個人情報を不正に持ち出したとして、同市個人情報保護条例違反の容疑で逮捕された。持ち出された名簿データの二次流出や、不正利用による被害等は確認されていない[*120]。
4	7月	退職者	日本年金機構静岡年金事務所の元契約職員が、女性にストーカー行為をする目的で日本年金機構の持つ個人情報を不正取得したとして、独立行政法人個人情報保護法違反の疑いで逮捕された[*121]。
5	11月	委託先社員	中日本高速道路株式会社の業務委託先である株式会社片平エンジニアリング社員が、同社発注工事2件の設計金額に関する情報を株式会社ゼンテックに漏えいし、同社が落札していた。株式会社片平エンジニアリング社員と株式会社ゼンテックの役員及び法人としての株式会社ゼンテックは、不正競争防止法違反で略式起訴された[*122]。
6	11月	退職者	三井住友トラストクラブ株式会社の元契約社員が、顧客のクレジットカード情報を不正に使用し、利益(合計約270万円)を得たとして、不正競争防止法違反及び電子計算機使用詐欺の容疑で逮捕された。同社は自ら疑義のある取り引きを発見、内部調査を進めるとともに、警察に通報し、捜査に全面的に協力した。元契約社員は、2016年8月に懲戒解雇された[*123]。
7	2017年1月	退職者	東京都中野区役所の元臨時職員が、勤務中に住民情報システムに接続し、個人情報を盗み見て女性宅に侵入したとして、同区個人情報保護条例違反と住居侵入の疑いで逮捕された[*124]。
8	2月	退職者	オンラインショップのプラットフォームを提供しているGMOメイクショップ株式会社の元社員が、ネットショップの運営者情報を含む3万2,800件の個人情報及び営業関連データを無断で社外に持ち出していたことが判明した。退職した元社員が個人で業務を請け負っていた会社の関係者より、上記の情報を持ち込んでいる可能性があると通報を受け、発覚した[*125]。
9	2月	退職者	特殊鋼メーカ愛知製鋼株式会社の元専務と元社員が、営業秘密にあたる磁気センサーの技術情報を漏えいしたとして、不正競争防止法違反(営業秘密侵害)容疑で逮捕された。2人は磁気技術製品の開発販売会社を設立しており、磁気センサーの製造販売を自ら手掛けるため、無断で関係先(電子部品会社の従業員)に技術情報を流したとされる[*126]。

■表1-2-5　2016年度に報道された内部不正事件(報道または公表された事例を基にIPAが作成)

(b)情報を大量に持ち出せる環境があった事例

事例3、8は、退職者が勤務先から大量の個人情報を持ち出した事例である。事例8では、外付けハードディスクドライブに個人情報等を保存していた。外部記憶媒体の利用についてルール等が定められていたかは不明だが、情報を大量に持ち出せる環境であったことが推測される。情報を持ち出しにくくするためには、「犯行を難しくする」対策が有効である。具体的には、システムからの「重要情報のダウンロードの制限」や「上司等に通知される」よう設定することが考えられる。また業務上外部記憶媒体を利用するときには「持ち込み・業務利用のルールを定め、徹底する」ことが求められる。

(c)情報の流出先から流出元へ通報された事例

事例2、8は、情報の流出先から流出元に持ち出された個人情報等の返却あるいは通報があった事例である。個人情報保護委員会の「個人情報の保護に関する法律についてのガイドライン(第三者提供時の確認・記録義務編)」では、第三者から個人情報を取得する場合には、当該個人情報が適法に入手されていることを確認することを求めている。不正に取得された可能性があると判断し、個人情報を返却あるいは通報した流出先の対応は適切である。個人情報取扱事業者が遵守すべき義務を果たすことが、不正対策の一つといえる。第三者から提供された個人情報は、正規の手続きで入手した情報であるか「取得の経緯を確認する」必要がある。不正に取得した個人情報を取得または利用した場合は、個人情報保護法違反、あるいは不正競争防止法違反の可能性があることを教育等の機会を通じて従業員・職員等に周知徹底させることが重要である。

(d)自己点検・内部監査の重要性を示す事例

事例6は、不正行為が発生したものの、自社で疑わしい取り引きを発見、自主的に調査を実施することで被害を食い止めることができた事例である。
内部不正の防止・抑止の観点から、情報の管理や取り扱いが適切か、定期的及び不定期な確認や監査を実施すべきである。そのほか、技術的・社会的な状況の変化に応じて対策を見直すことが必要である。

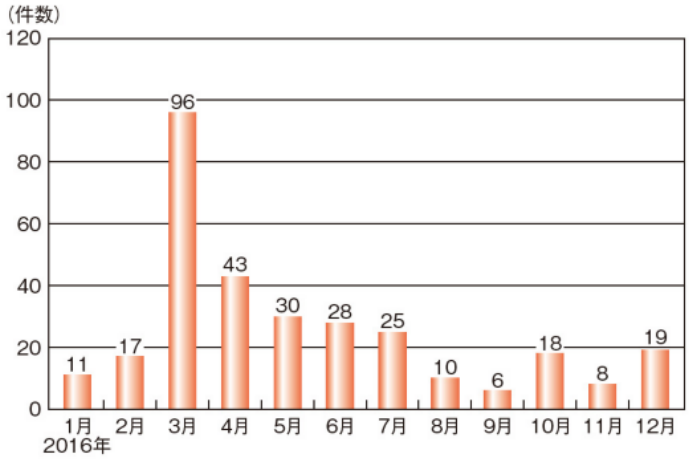
(e)退職者により営業秘密が漏えいした事例

事例9は、所属先企業が開発した製品の製造技術を元役員らが漏えいした事例である。この製造技術は、社内規定で機密に指定されていた。不正競争防止法では、企業内の情報を営業秘密として管理することで、法的保護を受けることが可能となる。

(6)ランサムウェアによる被害

ランサムウェアとは「ransom」(身代金)と「software」(ソフトウェア)を組み合わせた造語で、画面ロック等によりパソコンを使用不可にする、またはパソコン内のファイルを暗号化するウイルスの総称である。それらの復旧を条件に身代金を支払うように促す脅迫メッセージ(図1-2-14)を表示することから、ランサムウェアと呼ばれている。
2016年3月には、ばらまき型メールによってランサムウェアが拡散され、IPAへの相談件数が急増した。それ以降もIPAへのランサムウェアに関する相談は多く寄せられており、ランサムウェアの被害は継続して発生している(図1-2-15)。セキュリティベンダによると、2016年の日本国内でのランサムウェア検出台数は6万5,000件を超え、2015年の検出台数と比較して9.8倍の急増となった(図1-2-16)。

サイバーリスクマネージメント
個人情報を狙った攻撃



■図1-2-15　ランサムウェアに関する月別相談件数推移

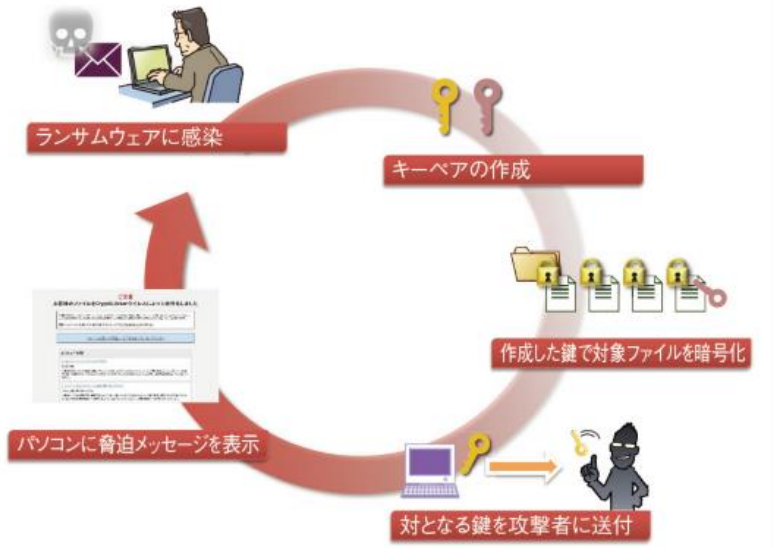
■図1-2-16　国内でのランサムウェア検出台数推移

2016年5月には、2015年12月に話題となったランサムウェア「TeslaCrypt」の作成者が攻撃活動を停止し、暗号化されたファイルを復号するための鍵を無料で公開した。また、2016年7月には、ランサムウェアの復号用の鍵を競合する他のランサムウェア攻撃者の組織がリークするという事例も確認されている。リークされた複合用の鍵を使用して、セキュリティベンダからファイルを復元するためのツールが公開された。ファイル暗号化型のランサムウェアが主流であることは変わらず、被害内容についてはおおむね共通であるが、攻撃に使用されるランサムウェアは次々と新しいものへと移行している。2016年は「Locky」「CryptXXX」「CERBER」等様々なランサムウェアが登場した。このように新たなランサムウェアが登場し続ける要因の一つとして、「DarkWeb」におけるランサムウェアの販売や、ランサムウェアによる攻撃のサポート等を行うWebサイトの存在が挙げられる。こうした環境により、ある程度の知識があれば誰でもランサムウェアを利用した攻撃者になり得る状況にあるといえる。しかし、ランサムウェアの販売やランサムウェアを利用して脅迫することは犯罪であることを十分に認識し、興味本位でそれらにアクセスしないようにすべきである。

サイバーリスクマネージメント
多様化するサイバー攻撃

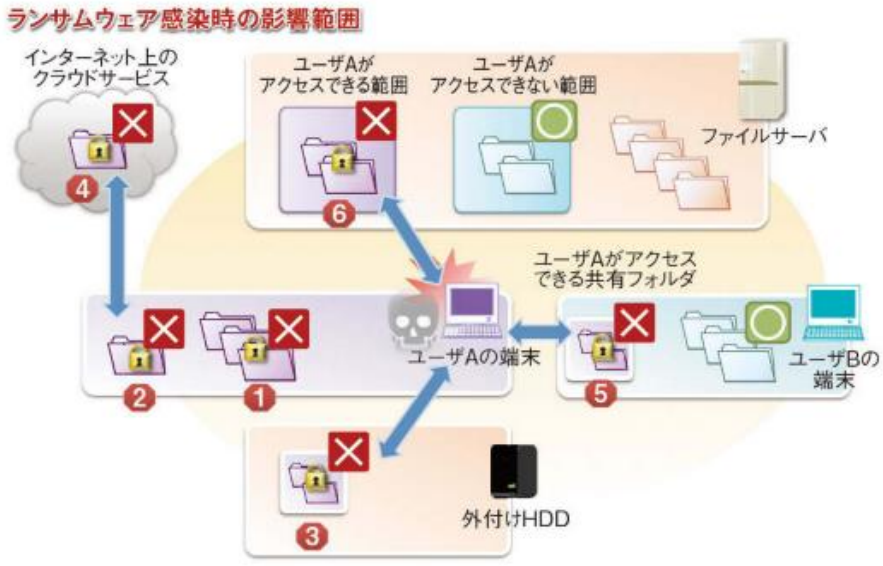
1. ランサムウェアによる攻撃

2016年はランサムウェアによる被害が著しく増加した。主流となっているランサムウェアは前年度と同様、パソコン内のファイルを暗号化する、ファイル暗号化型のランサムウェアである（図1-3-22）。



■図1-3-22　ランサムウェアのファイル暗号化の動作のイメージ

このようなランサムウェアに感染した場合の影響範囲は、感染したパソコンのみにとどまらず、ネットワーク経由でアクセス可能な端末へも影響を及ぼす可能性がある（図1-3-23）。



■図1-3-23　ファイル暗号化型のランサムウェア感染時の影響範囲

サイバーリスクマネージメント
多様化するサイバー攻撃

(1)ランサムウェアを感染させる手口

ランサムウェアは、メールに添付された不正なプログラムの実行、改ざんされたWebサイトの閲覧や不正広告表示によるドライブバイダウンロード攻撃で感染する。メールを使った手口では、ばらまき型メールによってランサムウェアがばらまかれた事例が確認されている。IPAに寄せられた相談に「不審なメールの添付ファイルを開いてしまった」という内容が多かったことから、ばらまき型メールが主な感染経路と考えられる。IPAへの相談で最も多く感染被害が確認されたランサムウェアが「Locky」であり、2016年2月から3月にかけてばらまき型メールで拡散された※224。また、2016年6月には「Zepto」と呼ばれるランサムウェアがばらまき型メールによって感染を広げた※225。Zeptoは、ばらまき型メールによる拡散手法やファイルを暗号化する動作においてLockyと類似していることが指摘されている。また、Zepto以降もLockyと動作が類似しているランサムウェアは確認されており、今後も様々な亜種が発生する懸念がある。2016年9月にはWebサイトを閲覧することで「CERBER」と呼ばれるランサムウェアに感染する事例が確認された※226。この事例ではAdobeFlashPlayer等の脆弱性が悪用され、感染させられていた※227(「1.3.2(1)クライアントソフトウェアの脆弱性を悪用した攻撃」参照)。更にその1ヵ月後にも、複数の脆弱性を悪用した攻撃によりWebサイトを閲覧するだけでCERBERに感染する事例が発生した

(2)ランサムウェアに対する対策

ランサムウェアは様々な種別が確認されているが、対策については共通である。IPAではランサムウェアの概要や対策を解説したテクニカルウォッチを公開している。対策を大別すると、ランサムウェアに感染しないための対策とランサムウェアの感染に備えた対策とがある。ランサムウェアに感染しないための対策としては以下の点が挙げられる。

- OS及びソフトウェアを常に最新の状態に保つ。
- セキュリティソフトを導入し、定義ファイルを常に最新の状態に保つ。
- メールの添付ファイルや本文に記載されたURL、SNSにアップロードされているファイルや掲載されているURLを不用意に開かないように注意する。

IPAに寄せられる相談の中では、ばらまき型メールに添付されたファイルを開くことでランサムウェアに感染しているケースが多い。巧妙に作られたばらまき型メールを見分けることは、困難であることから注意が必要である。

ランサムウェアの感染に備えた対策としては、重要なファイルをバックアップしておくことが有効である。なお、図1-3-23で示したように、ランサムウェアの影響範囲は感染したパソコンのみにとどまらず、このパソコンがアクセス可能な同一ネットワーク上の装置にも及ぶため、バックアップにおいては以下に留意する必要がある。

- バックアップに使用する装置
- 媒体は、バックアップ時のみパソコンと接続する。
- バックアップに使用する装置・媒体は複数用意する。バックアップのルールの例としては、「3-2-1ルール(データをコピーして三つ持ち一2つはバックアップ一、2種類の媒体一例えば、ハードディスクとDVD-R一で保存し、バックアップデータのうち一つは違う場所で保管するというルール)」と呼ばれるものがある。
- バックアップの妥当性(バックアップが正常に取得できているか、現状のバックアップ手法がランサムウェアに対して有効か)を定期的に確認する。

ランサムウェアに感染してファイルが暗号化されてしまった場合、身代金を支払ったとしても復号できる保証はない。ランサムウェア対策情報を提供しているWebサイト「TheNoMoreRansomProject」やセキュリティベンダは、複数の復号ツールを提供している。これらのツールは全てのランサムウェアに対して有効ということではないが、暗号化されたファイルを復号できる可能性がある。

サイバーリスクマネージメント
多様化するサイバー攻撃

2. ばらまき型メールによる攻撃

特定の組織や個人ではなく、不特定多数の一般利用者を狙った、ウイルス感染を目的としたメールを「ばらまき型メール」と呼ぶ。以前より「Invoice」（請求書）といった件名等の英語のばらまき型メールは確認されていたが、2015年10月以降は日本語のばらまき型メールも多数確認されている。「御請求書」「発注依頼書」等の件名で、不自然さを感じる日本語の本文であるケースもあるが、実在する企業や組織をかたり、送信者のアドレスや本文の日本語にも不自然さを感じない、非常に巧妙で見分けることが困難なばらまき型メールも確認されている（図1-3-8）。

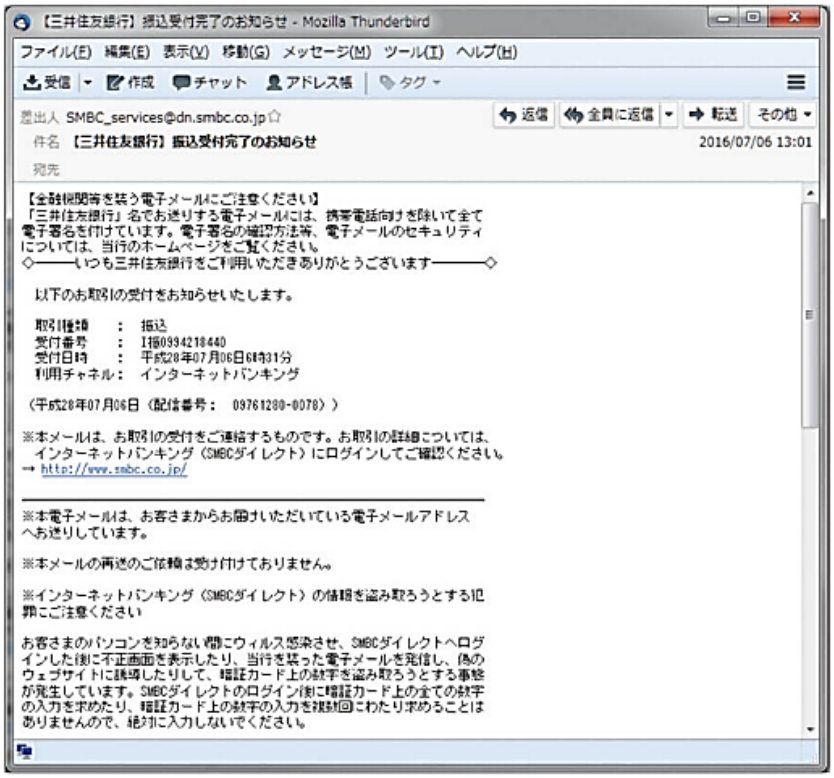


図1-3-8　三井住友銀行をかたったばらまき型メールの例

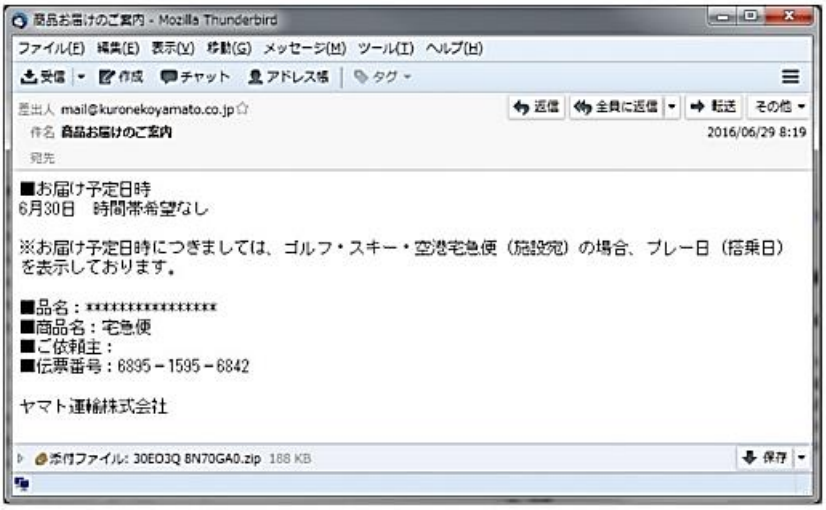
（1）ヤマト運輸の名前をかたったばらまき型メール

2016年6月、ヤマト運輸の名前をかたったばらまき型メールが確認され、IPAにも多数の相談や情報が寄せられた。それらの相談や情報から、次のようなメールであったことが確認できている（図1-3-9）。

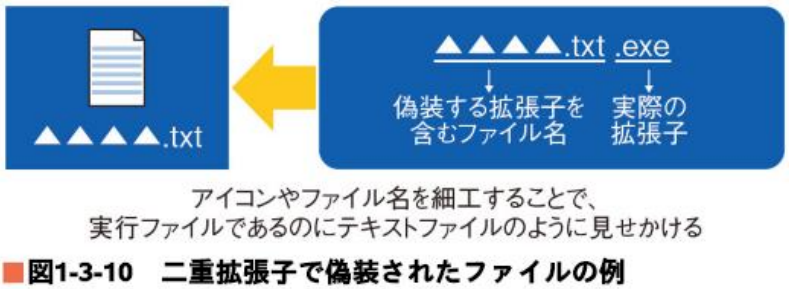
- 件名は「商品お届けのご案内」や「宅急便お届けのお知らせ」等
- 送信者は「mail@kuronekoyamato.co.jp」
- 本文に「ヤマト運輸株式会社」と記載
- 添付ファイルはランダムな英数字の名称のzipファイル本文中の品名が「*****」となっている箇所を除けば、送信者も実際にヤマト運輸から送信されるメールアドレスメールアドレスと同一である等、同社が実際に使っているメールと酷似している。

また、メールヘッダにもヤマト運輸のサーバから送信されたように見せかけている等、不審なメールと見抜くことを困難にするための細工がされている。セキュリティベンダによると、当該メールに添付されているzipファイルには二重拡張子でtxtファイルに偽装されたexeファイルが格納されており（図1-3-10）、当該ファイルを実行すると「Bebloh」と呼ばれるインターネットバンキングの情報を盗み取るウイルスに感染し、不正送金被害の恐れがあるという

サイバーリスクマネージメント
多様化するサイバー攻撃



■図1-3-9　ヤマト運輸をかたったばらまき型メール



アイコンやファイル名を細工することで、
実行ファイルであるのにテキストファイルのように見せかける

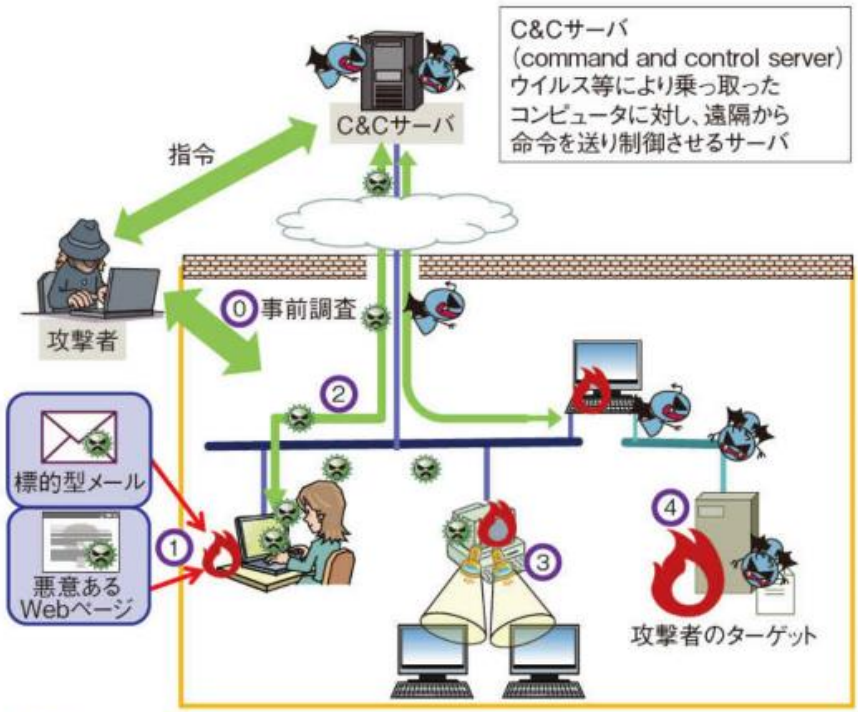
■図1-3-10　二重拡張子で偽装されたファイルの例

3. 標的型攻撃

標的型攻撃とは、特定の組織や企業等を狙うサイバー攻撃のことである。無差別かつ不特定多数の相手にウイルスメール等を送りつける攻撃や、社会的・政治的主張を目的とする攻撃、また愉快犯による攻撃とは異なり、機密情報の窃取やシステムの破壊・停止といった明確な目的を攻撃者が持ち、特定の組織や業界に対して攻撃を行う。標的型攻撃における攻撃者は、狙った組織に対して複数の段階を経て長期的に攻撃を継続するという特徴を持っている。IPAは、過去の事例等から、標的型攻撃を図1-3-11に示すような五つの段階に分類している。まず、「事前調査」段階において、標的とした組織や業界の情報を調査する。このとき、標的となる組織と外部とのメールのやり取りを盗聴する等により収集した情報を足掛かりとして、侵入の方法を画策することもある。次に、「初期潜入段階」では、事前調査によって得られた情報を基に、標的とした組織のパソコンにウイルスを感染させようとする。手口としては、ウイルスを添付したメール（標的型攻撃メール）を送りつけることが多く、標的とした組織に合わせたメール文面や、セキュリティソフトでウイルスを検知しにくくさせる細工が施されている。初期潜入に成功した攻撃者は、「攻撃基盤構築段階」に移り、組織内ネットワークで攻撃活動を行うための下準備をする。パソコンをリモート操作可能にするため、遠隔操作ウイルス（RemoteAccessTrojan：RAT）に新たに感染させる。遠隔操作を確実かつ継続的に行えるよう、複数の遠隔操作ウイルスに感染させることもある。

サイバーリスクマネージメント
多様化するサイバー攻撃

「システム調査段階」に移行すると、遠隔操作によって組織内ネットワークの攻撃に必要なウイルスを送り込み、組織内のネットワークの調査や、管理者権限の奪取、窃取する情報の探索等を行う。「攻撃最終目的の遂行段階」では、標的とした組織の情報の窃取等の活動を行う。標的型攻撃の手口は、典型的にはこのような流れをたどるが、異なる手口が使われることもある。また、攻撃者の目的は、機密情報や個人情報だけとは限らず、海外では、企業内システムの破壊や工場・発電所の停止を狙った事例も報告されている。



0 [事前調査]
ターゲットとなる組織を攻撃するための情報を収集する。

1 [初期潜入段階]
標的型メールや、Webサイト閲覧を通してウイルスに感染させる。

2 [攻撃基盤構築段階]
侵入したPC内でバックドアを作成し、外部のC&Cサーバと通信を行い、新たなウイルスをダウンロードする。

3 [システム調査段階]
情報の存在箇所特定や情報の取得を行う。
攻撃者は取得情報を基に新たな攻撃を仕掛ける。

4 [攻撃最終目的の遂行段階]
攻撃専用のウイルスをダウンロードして、攻撃を遂行する。

■図1-3-11　標的型攻撃の流れ

サイバーリスクマネージメント
多様化するサイバー攻撃

(2)標的型攻撃メールの手口

標的型攻撃メールは、「初期潜入段階」で攻撃者から標的とした組織に対して送付されるものである。このメールは非常に巧妙に偽装され、かつ多様であるため、開封を完全に防ぐことは難しい。しかし、標的型攻撃メールに関する教育により、攻撃手口をよく知ることで開封リスクを低減することや、システム的な対策を行うことで攻撃に備えることが可能である。ここでは、標的型攻撃メールの手口の例を示す。

(a)送信者偽装の手口メールソフトでは、メールの送信者が表示されるが、これは容易に偽装することができる。例えばJTBの事例では、これまでにJTBと取り引き実績のある航空会社系列のドメイン名のメールアドレスに偽装されていた。また、標的型攻撃メールは海外から送付されることが多いが、送信者の表示に日本人のありふれた名前を使用することによって、受信者に不審なメールであると気付きにくくさせる場合もある。

(b)件名や本文の内容標的型攻撃メールの件名や本文は、一見しただけではそれが攻撃だと気付きにくい内容となっている。例えば、日常的に発生する問い合わせや、標的とした組織の業務に関連した内容を詐称している。また、本文では添付ファイルの開封や、本文中のURLリンクをクリックするように仕向け、ウイルスに感染させる。以前の標的型攻撃メールは、日本語として不自然な点があったが、現在では一般的な定型文の挨拶や業務に関する連絡等が使用され、文面に不自然な点は少ない。更に、実在する組織名等を詐称する署名が使われることもある。添付ファイルについても、件名や本文の内容と関連するファイル名が多く、目視だけで不審なメールを見分けることは難しい

(c)添付ファイルによるウイルス感染の手口標的型攻撃メールの添付ファイルは、受信者に攻撃であると気付きにくくさせるため、攻撃者が添付ファイルに細工を施す場合がある。例えば、アイコンの偽装等による拡張子の偽装、ショートカット(LNK)ファイルの悪用、MicrosoftOfficeのマクロ機能や脆弱性の悪用等がある。これらの手口は、2016年も引き続き多数確認されたが、MicrosoftOfficeのOLE(ObjectLinkingandEmbedding)オブジェクトを悪用する手口も新たに確認された。以下では二つの手口を紹介する。

・圧縮ファイルを使用する手口標的型攻撃メールの多くは圧縮形式のファイルを添付している。富山大学の事例でもZIP形式の圧縮ファイルが添付された標的型攻撃メールが使用された。パスワードで保護された圧縮形式のファイルは、メールの配送経路上にあるメールサーバのフィルタ等でウイルスを検出することが難しい。パスワード付きの圧縮ファイルは日常のメールのやり取りで多用する利用者も多く、パスワード付きの圧縮ファイルを開く場合の危険性について周知することが重要である。

・MicrosoftOfficeのOLEを悪用する手口Office文書ファイルを用いた標的型攻撃においては、マクロ機能の悪用、脆弱性の悪用が多く観測されてきたが、MicrosoftOfficeのOLEオブジェクトを悪用した添付ファイルが攻撃として用いられることもある。Office文書ファイルにはパスワードを設定できるが、これにより、圧縮形式のファイルと同様にメールの配送経路上でのウイルスチェックの回避を試みる手口も確認されている

(d)使用されるウイルス標的型攻撃では、メールにウイルスを添付して感染させる場合や、「初期潜入段階」で感染したウイルスから、更に別のウイルスに感染させる場合がある。メールに添付されるウイルスの種類として、JTBや経団連の事例では、「PlugX」と「Elirks」と呼ばれるトロイの木馬型のウイルス(ユーザに対して、悪質ではないプログラムのように見せかけるウイルス)が使用された。特にPlugXは、2012年に確認されて以降、政府系機関や主要産業を狙った事例で使用されているRATである。