

第4回「2017年のセキュリティ事件に関する意識調査」を実施 マカフィー、2017年の10大セキュリティ事件ランキングを発表

世界中に影響を与えたランサムウェアの被害や、無線 LAN の脆弱性が上位にランクイン、若年層のサイバー犯罪が目立った一年に

第4回「2017年のセキュリティ事件に関する意識調査」を実施。マカフィー、2017年の10大セキュリティ事件ランキングを発表

世界中に影響を与えたランサムウェアの被害や、無線 LAN の脆弱性が上位にランクイン、若年層のサイバー犯罪が目立った一年に

今年は、第1位に日本でも被害をもたらしたランサムウェア「WannaCry (ワナクライ)」の事件がランクインしました。この WannaCry の事件では、端緒となった欧州を中心に世界中の企業に感染が拡大し、日本でも製造業や運輸などの主要業界で被害が報告されるなど、世界規模で影響を及ぼした事件として、ランサムウェアの名前を知らしめる結果になりました。またその他にも、無線 LAN の暗号化技術の脆弱性や有名人の個人情報への不正アクセスなど、高度情報化社会における個人のプライバシーに関する脅威がさらにクローズアップされた一年でした。また、注目の事件として、今年は例年以上に中学生や高校生によるマルウェアの作成やフリーマーケット アプリでのマルウェア関連情報の出品など、若年層のサイバー犯罪が強く印象に残った年となりました。

2017年の10大セキュリティ事件ランキングに関するマカフィーの主な見解

マカフィーが従来から指摘してきた通り、世界中のあらゆる組織がインターネットに接続して事業活動を行っているため、WannaCry のように海外で発生した事件であっても、インターネットを介して瞬間に日本にも影響が及ぶことを十分に念頭に置いた速やかな対策がこれまで以上に求められます。さらに日本ではこれまで、言語の違いがサイバー攻撃に対する障壁になり得ると考えられていましたが、今後は攻撃側の機械学習の活用などにより言語の壁は低くなると想定されるため、日本に対する攻撃がさらに活発化することも考えられます。

個人向けの脅威では、普段利用している無線 LAN の脆弱性や個人情報への不正アクセス事件など、今や生活の一部となっているインターネットの利便性だけでなく、そこに潜むプライバシーの問題について改めて考え直す一年になりました。

若年層によるサイバー犯罪の摘発は、日常がデジタル化された世界では、以前は限られた専門家のみが利用できたサイバー犯罪に関する情報に、場所や年齢を問わず誰でもアクセスできるようになったことを示しています。今後も情報化の流れはさらに進むものと思われませんが、教育などを通じた情報リテラシーの向上がもはや喫緊の課題となっていると考えています。

調査概要

- 調査名: 「2017年のセキュリティ事件に関する意識調査」
- 調査対象者: 日本国内に在住する企業経営者、企業に勤務する情報システム担当者、
- 一般従業員など 22 歳以上の男女 1,552 人
- 調査方法: インターネットによるアンケート調査
- 調査項目: 第3回調査後の2016年10月から今回の調査を開始した2017年10月までに報道された
- セキュリティ事件に対する認知度 (複数回答)
- 調査期間: 2017年11月24日～2017年11月28日
- 調査主体: マカフィー株式会社 (マクロミル モニタを利用)

<https://www.mcafee.com/jp/about/news/2017/q4/1211-01.aspx>

レポート

調査結果を基にランク付けした 2017 年の 10 大セキュリティ事件は以下の通りです。なお、当ランキングは、昨年実施した 3 回目の調査 (2016 年 10 月) から今回の調査を開始した 2017 年 10 月までに報道されたセキュリティ事件に対するビジネスパーソンの認知度 (複数回答) を調査した結果によるものです。

| 順位 | セキュリティ事件 (時期) | 認知度 |
|----|--|-------|
| 1 | ランサムウェア「WannaCry / WannaCrypt (ワナクライ)」の大規模な攻撃が世界中で確認され、国内でも製造や運輸などの業界で被害が発生 (2017 年 5 月) | 36.7% |
| 2 | Amazon をかたるフィッシングメール / 「Amazon」の利用者を狙ったフィッシング攻撃が発生 / 大手宅配業者の商品の発送や宅配便のお知らせを装った偽メールが増加 (2016 年 11 月～2017 年 1 月) | 36.2% |
| 3 | 無線 LAN の暗号化規格である WPA2 の脆弱性 (KRACK / KRACKs) が発見される (2017 年 10 月) | 32.8% |
| 4 | 米 Yahoo! で、不正アクセスにより最終的に 30 億人以上のユーザー個人情報に漏えいしていたことが判明 (2017 年 10 月) | 32.3% |
| 5 | ランサムウェアや遠隔操作ウイルスの作成、フリーマーケット アプリへのマルウェア関連情報の出品など、中高生によるサイバー犯罪で逮捕者が続出 (2017 年 6 月～9 月) | 27.2% |
| 6 | Apple を装い、アカウント情報を詐取するフィッシング攻撃が確認される (2017 年 2 月) | 26.0% |
| 7 | 女優や女性アイドルなどの芸能人が画像を保存するなどしていたインターネットサーバーに不正にログインしたとして、無職の男を書類送検 (2017 年 4 月) 23.0% | 23.0% |
| 8 | 防衛省と自衛隊の情報基盤がサイバー攻撃を受けたとの報道 (2016 年 11 月) | 20.4% |
| 9 | 女性タレントや女性アイドルらの電子メールサービスなどに不正接続したとして、大手新聞社の社員を逮捕 (2016 年 11 月) 19.3% | 19.3% |
| 10 | 日本マクドナルドのシステムがマルウェアに感染し、外部に向けて大量のパケットを発信して通信を圧迫、商品購入時のポイントサービスが利用不能に (2017 年 6 月) | 18.8% |

2017 年を代表する脅威“WannaCry”

今年を代表する脅威としてランキングの第 1 位に登場したのはランサムウェア「WannaCry」でした。ランサムウェアは、感染したシステムを暗号化するなどして使用不能にした後、再度アクセスすること引き換えに被害者に対して身代金 (ランサム) の支払いを要求するタイプのマルウェアです。今回ランキングのトップになった WannaCry は、ハッカー集団が公開した脆弱性を悪用するもので、その被害は 150 カ国以上に及ぶと報告されており、その中には日本の企業なども含まれています。WannaCry の詳細についてはマカフィーのブログでも解説されていますが、今回の WannaCry の事件で顕著だったのはその感染力で、自己増殖するワーム型の特徴を備えたランサムウェアであったことが、感染を世界規模に拡散させた要因であることが指摘されています。マカフィーでは 2018 年の脅威予測でランサムウェアが今後はより収益性の高い企業などを標的とし、またその目的も従来の身代金による金銭目的から、サイバー上の破壊攻撃や妨害活動へ拡大すると考えています。今年のランキングではランク外だったランサムウェア「Petya」(6 月) による攻撃キャンペーンは金銭よりも破壊活動を目的としたものであったと考えられており、韓国の Web ホスティング会社への攻撃は APT 攻撃

レポート

とランサムウェアの組み合わせにより、ホスティング契約していた顧客データを暗号化し、被害者に対して身代金支払いを要求する攻撃も発生しました。本格的な標的型ランサムウェア時代の幕開けに伴い、企業におけるランサムウェア対策はこれからも最優先事項の1つとなるとマカフィーでは考えています。

ランサムウェアへの対策として、ソフトウェアを常に最新のものに更新する、マルウェア対策ソフトウェアを活用する、疑わしいファイルやメール、リンクを開かない、常にデータのバックアップを取る、などを推奨しているほか、警察機関やその他のサイバーセキュリティ企業などと協力して、ランサムウェアに関する啓発や復号ツールの提供などを目的としたWebサイト「No More Ransom!」を開設し、ユーザーを支援しています。

サイバー空間における個人のプライバシーについて認識を新たにする一年に

今年のランキングで第7位と第9位にランクインした不正アクセスによる有名人の個人情報の取得に加え、第3位にランクインした無線LANのデータ暗号化機能であるWPA2の脆弱性など、2017年はユーザーの個人情報やプライバシーへの脅威が顕在化した一年となりました。現在、SNSや個人向けクラウドサービスなど、私達の日常はさまざまな場面でインターネットのメリットを受けていますが、そこで送信・保存されている個人情報やプライバシーについてはあまり気にしていない方も多いと思います。一方で、サイバー犯罪者は、そのようなユーザー心理を悪用し、重要な個人情報やプライバシー情報を不正に入手するための技術やテクニックを進化させています。マカフィーでは、デジタル時代のユーザーの心得として、自身に関する情報の場所や保存方法、そして使用方法などを十分に意識すると同時に、信頼できるサービスやインターネット回線であるかどうかを見極められるだけのリテラシーを備えていく必要があると考えています。そして、まだ個人情報の窃取やプライバシー侵害の被害に遭っていないユーザーでも、明日起こるかもしれない危険を意識してセキュリティ対策に取り組むことを強く推奨しています。私達の生活のデジタル化の流れは不可避のものとなるなか、改めて個人レベルで情報やプライバシーの問題について考え直す時期になっています。

サイバー空間はすでに若年層の格好の遊び場に

今年マカフィーが注目したセキュリティ事件として、第5位に中高生によるサイバー犯罪がランクインしました。昨年の調査でも若年層によるサイバー犯罪がランクインしましたが、今年はさらに多くの事件が話題を集めました。また、若年層によるサイバー犯罪も従来のような不正アクセスによる情報の窃取だけでなく、マルウェアの作成からフリーマーケットアプリ上へのマルウェア関連情報の出品など、その手口がさらに多様化してきているのも今年の特徴です。今や場所や年齢を問わず、インターネット上でサイバー犯罪に関する情報を手に入れられる時代になっています。デジタル化が進み、若年層によるサイバー犯罪を抑止することがますます難しくなるなか、家庭や教育課程でサイバー空間との付き合い方について話し合うなど、情報リテラシーを若年層の“必修科目”の一つとして採用する時代になっていると、マカフィーでは考えています。

レポート

2017年の身の回りの脅威ランキング

また、マカフィーでは、2017年の10大セキュリティ事件ランキングに関連して、2017年に企業や個人を問わず影響を及ぼしたセキュリティ上の一般的な脅威に関する調査も実施しました。この調査は、調査対象時期全体を通じて、特定の事件には関連しないものの、一般的なセキュリティ上の脅威として注意すべきものに対するビジネスパーソンへの認知度（複数回答）を基にランク付けしたものです*。2017年の注目すべき一般的な脅威は以下の通りです。

* 昨年までは下記の一般的な脅威もセキュリティ事件ランキングに含まれていましたが、今年からは個別のセキュリティ事件とは別のランキングとして発表するものです。

| 順位 | セキュリティ上の脅威 | 認知度 |
|----|-------------------------------|-------|
| 1 | 振り込め詐欺／迷惑電話による被害 | 52.6% |
| 2 | ランサムウェア（身代金ウイルス）の被害 | 45.0% |
| 3 | 大手金融機関やクレジットカード会社などをかたるフィッシング | 41.0% |
| 4 | 公共無線 LAN のセキュリティ問題 | 35.1% |
| 5 | ビジネスメール詐欺の被害 | 25.2% |

マカフィーの過去の調査では、振り込め詐欺／迷惑電話による被害、金融機関などをかたるフィッシング、公共無線 LAN のセキュリティ問題などが毎年上位にランクインしていましたが、今年の調査ではランサムウェアの被害が2位にランクインしました。これは今年発生した WannaCry による被害者数と被害を拡大させるスピードがこれまでのランサムウェアとは桁違いであったことで、情報セキュリティ関連組織による啓発活動や報道機関の注目度が増し、社会でのランサムウェアに対する理解や意識が高まったことによるものとマカフィーでは考えています。サイバー犯罪者は技術や手法を進化させながら、ビジネスや自宅など日常のあらゆる場面でサイバー上の脅威を拡大させており、インターネットに接続されているあらゆるものがサイバー攻撃の標的となることを認識すべきです。

マカフィー株式会社の代表取締役社長である山野 修は次のように述べています。

「やはり今年は WannaCry の1年と言える年だったと思います。欧州で発生し、瞬く間に世界、そして日本へと拡大したこのランサムウェアは、標的となった企業だけでなく、社会全体にサイバー上の脅威の潜在力を再認識させる出来事でした。私達のビジネスや生活がますますデジタル化していくことは明らかですが、そのような環境で企業や個人の大切な情報や資産をどのように守っていくのか、改めて考え直す必要があると考えています。日本が2020年という節目の年を迎えるにあたって、もはや日常となった情報セキュリティ上の脅威について、あらゆる組織や個人が次のステージへと歩みを進めなければならない時期に来ていると考えています」

McAfee について

McAfee は、世界で最先端のサイバーセキュリティ企業です。McAfee では、より安全なデジタル世界を構築するため、個々の力を結集し、企業と個人を保護するソリューションを提供しています。他社の製品と連携するソリューションを構築することで、真に統合されたサイバーセキュリティ環境を整備し、脅威の対策、検出、修復を連動して行うことができます。McAfee の個人向けのソリューションは、すべての種類のデバイスに対応しています。自宅でも外出先でも、安心してデジタル ライフを楽しむことができます。McAfee では、他のセキュリティ企業との連携を強化し、力を合わせてサイバー犯罪者と戦っています。

www.mcafee.com/jp

McAfee Labs について

McAfee Labs は世界で最先端の脅威研究機関で、脅威情報やサイバーセキュリティに関する最新の情報を提供しています。世界各地に配備した数百万台のセンサーからデータを収集し、ファイル、Web、メール、ネットワークなどに対する脅威を研究・調査し、脆弱性の報告を行っています。McAfee Labs は、リアルタイムで脅威情報、重要な分析結果、専門的な情報を提供し、保護対策の向上とリスクの軽減に貢献しています。

<https://www.mcafee.com/jp/mcafee-labs.aspx>



〒150-0043
東京都渋谷区道玄坂 1-12-1
渋谷マークシティウエスト 20F
www.mcafee.com/jp

本資料は弊社の顧客に対する情報提供を目的としています。本資料の内容は予告なしに変更される場合があります。本資料は「現状のまま」提供するものであり、特定の状況あるいは環境に対する正確性および適合性を保証するものではありません。McAfee および McAfee のロゴは米国法人 McAfee, LLC またはその関係会社の登録商標です。その他すべての登録商標および商標はそれぞれの所有者に帰属します。Copyright © 2018 McAfee, LLC