**フィッシングメールやランサムウェア被害が拡大した2017年、マカフィーが10大セキュリティ事件ランキングを発表**

* 磯谷 智仁

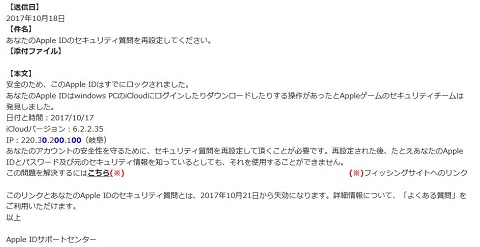
2017年12月20日 11:58

　マカフィー株式会社は10日、日本国内の企業を調査対象としたセキュリティ意識調査に基づく「2017年の10大セキュリティ事件ランキング」を発表した。

　調査は2014年から実施しているもので、今年が4回目。2016年10月から2017年10月に発生したセキュリティ事件に関して、日本国内の企業経営者や情報システム部門の従業員および一般従業員など22歳以上の男女1552人を対象に、認知度をインターネットで調査したもの。調査期間は2017年11月24日～28日。

**急増するフィッシングメール、標的は通販利用者**

　今年はフィッシングメールの拡散が多く確認された。フィッシングメールが誘導する偽サイトではHTTPSが利用されるなど、手口も巧妙化している。日本の電子商取引の市場規模は2016年に15.1兆円規模に上り、常に利益率の高い標的を模索している攻撃者にとって、通販利用者は格好の餌食となっている。ランキングではAmazonをかたるフィッシングメールが2位、Appleをかたるフィッシングメールが6位に入っており、「誰もが攻撃対象になる時代」として、マカフィー株式会社の櫻井秀光氏（セールスエンジニアリング本部本部長）は警告する。

[](https://internet.watch.impress.co.jp/img/iw/docs/1097/619/html/01.jpg.html)

Appleをかたるフィッシングメールの一例（一般財団法人日本サイバー犯罪対策センターの注意喚起情報より）

**Wi-Fi通信の盗聴などが可能なWPA2の脆弱性「KRACKs」**

　Wi-Fiの暗号化技術であるWPA2/WPAの脆弱性「KRACKs（Key Reinstallation Attacks）」も話題となった。KRACKsは、クライアント（Wi-Fi子機）がWi-Fiアクセスポイントに接続する際の暗号化通信のハンドシェイク処理に起因するもの。CVE番号ベースで10件の脆弱性「CVE-2017-13077～13088」からなる。これを悪用することで、ペア暗号鍵（PTK-TK）、グループ鍵（GTK）、整合性グループ鍵（IGTK）の再インスト―ルなどが可能になる。

　脆弱性を悪用するためには、電波の到達範囲内にいる制約があるなど実行は困難だが、ユーザー側も油断せず、VPNやHTTPS（SSL）で通信を暗号化して盗聴を防ぐことが推奨される。さらに、電波出力の調整が可能な機器では、電波の到達範囲を最小限にして、脆弱性を悪用できる範囲を狭めることも必要だ。

**世界中で猛威を振るったランサムウェア「WannaCry」**

　なお、5月から世界的な感染の拡大が確認されたランサムウェア「WannaCry」は1位にランクインした。ランサムウェアへの対抗策としては、1）OSやアプリを常に最新の状態にすること、2）マルウェア対策ソフトを活用する、3）疑わしいファイルやメール・リンクを開かない、4）常にデータのバックアップを取ることなどを推奨している。

　櫻井氏は、「昨年の予測ではランサムウェアの被害は減少するとしていたが、予想を裏切られた」とコメント。しかし、ランサムウェアは優れた検体を使いまわしているため、種類自体は減少しているという。

[](https://internet.watch.impress.co.jp/img/iw/docs/1097/619/html/a1.jpg.html)

マカフィー株式会社の櫻井秀光氏（セールスエンジニアリング本部本部長）

**便利なサービス・製品に存在する問題、2018年の脅威予測**

　櫻井氏は、10大セキュリティ事件ランキングに加えて、2018年以降に起こる脅威予測についても発表した。

　まず、防御者と攻撃者の間で機械学習を活用したツールの開発競争が激化することを挙げた。「機械学習の活用を売りにしたセキュリティ製品が出てきているが、攻撃側でも機械学習が使われ始めている」という。

　同氏によると、機械学習で検知力・防御力は高まるが、誤検知もあり得るため、最終的に判断を行う人間の手間がなくなることはないと補足し、機械学習と人手による対策の組み合わせが今後の主流になるとの見方を示した。

[](https://internet.watch.impress.co.jp/img/iw/docs/1097/619/html/02.jpg.html)

　ランサムウェアに関しては、今後は多くの収益が見込める特定の「お金持ち」を標的にしたり、破壊行為やビジネスの妨害を目的とした攻撃パターンに変化することが予想されている。これは、各セキュリティベンダーが連携して立ち上げたランサムウェア対策プロジェクト「No More Ransom」による活動も影響しているという。最新の危機、対策に関する情報が共有されやすい体制が整ったことで、従来の脅迫型の攻撃では攻撃者の収益性が下がるそうだ。そのため、収益性の高い企業などを標的としたサイバー上の破壊攻撃や、妨害活動へ拡大することが考えられている。

[](https://internet.watch.impress.co.jp/img/iw/docs/1097/619/html/03.jpg.html)

　クラウドサービスが普及することで、起こりうるネットワークセキュリティの問題も懸念される。従来のオンプレミス型からクラウド型に移行することで、導入までの時間とコストを節約できるようになったが、データが複数のプロバイダーやサーバーを介するため、ネットワークからの脅威の対象となる。脆弱なまま運用されたサーバーがある場合、ブルートフォース攻撃やDos攻撃の対象となりやすい状況となっている。そのため、ユーザーは現在使用しているサービスのセキュリティ面を見直す必要があるとしている。

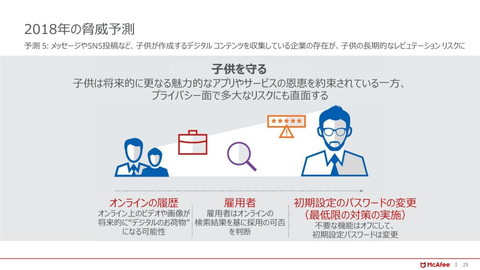
[](https://internet.watch.impress.co.jp/img/iw/docs/1097/619/html/04.jpg.html)

　企業による個人情報の収集に関して、欧州では個人データの処理と移転に関するルールを定めた「EU一般データ保護規則（GDPR）」が制定され、日本でも改正個人情報保護法が施工された。しかし、収益を追求するあまり、一部企業がユーザーの同意の有無を問わず個人データを収集する例は後をたたないという。今後はIoTデバイスが普及することで、個人情報が収集される機会もさらに増えてくると予測される。

　「多少罰金を支払ってもユーザー情報を取る恩恵を捨てるとは思わないので、リスクを犯しながらも収集を継続するとみている」（櫻井氏）

[](https://internet.watch.impress.co.jp/img/iw/docs/1097/619/html/05.jpg.html)

　子どものSNS投稿などによる情報発信がプライバシーの危険性に繋がることも指摘。これからも子どもが使いやすいアプリが登場し、情報発信を行う年齢層が下がる可能性が考えられる。しかし、オンライン上の履歴に残ることで、他人から私生活を覗き見られたり、企業の採用活動の際に過去に投稿していたコンテンツを検索され、採用の可否を判断される可能性もある。そのため、マカフィーでは子どものリテラシーを向上させるための支援に力を入れていくとしている。

[](https://internet.watch.impress.co.jp/img/iw/docs/1097/619/html/06.jpg.html)