【プレスリリース】

マカフィー株式会社
2020 年 12 月 15 日

マカフィー、2020 年の 10 大セキュリティ事件ランキングを発表
第 7 回「2020 年のセキュリティ事件に関する意識調査」を実施

オンラインサービスや AI を悪用した攻撃のリスクに注目が集まった一年に

デバイスからクラウドまでを保護するサイバーセキュリティ企業であるマカフィー株式会社（本社：東京都渋谷区、代表取締役社長：田中 辰夫、以下、マカフィー）は、本日、2020 年の 10 大セキュリティ事件を発表しました。これは、日本国内の経営層や情報システム部門などのビジネスパーソンを対象に実施した「2020 年のセキュリティ事件に関する意識調査」の結果を基にしています。

今年は、第 1 位に携帯電話会社が運営する電子決済サービスを通じて、利用者の預貯金が何者かに不正に引き出された事件がランクインしました。この事件は、利用者の本人確認を厳重に行う安全性と利便性のバランスについて改めて考えるきっかけとなりました。またその他にも、当社の 2020 年の脅威予測にも含まれていた AI を悪用したディープフェイク関連の事件や、新型コロナウイルス感染症に便乗したフィッシングサイトの登場など、進化する技術や人々の混乱に乗じた脅威にも注目が集まった一年でした。

2020 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

- 今年はコロナ禍におけるリモートワークや外出自粛によって、オンラインサービスの利用が急増しニーズが多様化しました。さまざまなサービスがオンラインで提供されることで利便性は高まりますが、サービス提供者と利用者の双方が十分な安全性を確保する必要があります。特に、DX の推進を急ぐあまり、セキュリティ観点でのガバナンスが不十分であったことが要因の一つと思われる事案もいくつか見られ、セキュリティ人材の確保と併せ、今後の課題になると考えられます。またコロナ禍で情報を求める人々を騙す、自治体などのホームページを模倣したフィッシングサイトの登場や、オンライン会議システム「Zoom」の機能における潜在的なリスクなどについても注目される一年となりました。
- 国内の大企業を狙ったサイバー攻撃も複数報道され、不正アクセスによる情報流出が発生していたことが明らかになりました。インシデントの詳細については未発表のものもあり断定はできませんが、ロシアや中国など、国家を背景としたハッカー集団の関与が噂されるなど、これまでは重要インフラをターゲットとしていた攻撃が、一般企業まで広がってきているように感じられます。また攻撃の手法も、サプライチェーンなどの脆弱性を突いた標的型攻撃に加え、「二重脅迫型ランサムウェア」や、PowerShell などを用いた「環境寄生型攻撃」の増加など、その内容に関しても注目が集まりました。

調査結果を基にランク付けした 2020 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 6 回目の調査後（2019 年 12 月）から今回の調査を開始した 2020 年 11 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	携帯電話会社の電子決済サービスを通じて、利用者の預金が何者かに不正に引き出されたことが判明（9 月）	59.2
2	ゲームメーカーが 11 月 16 日、サイバー犯罪集団からの不正アクセスを受け、顧客や取引先に関する情報が最大で 35 万件流出した可能性があると発表（11 月）	37.7
3	AI を使ってポルノ動画に写った人物の顔を芸能人の顔にすり替えた“ディープフェイクポルノ動画”を公開したとして、男性 2 人を名誉毀損と著作権法違反の疑いで逮捕（10 月）	36.5
4	新型コロナウイルス感染症対策として 10 万円の特別定額給付金の給付が各自治体で始まるなか、自治体などのホームページを模倣したフィッシングサイトが相次いで確認（5 月）	35.4
5	米海軍はサイバーセキュリティ上の懸念を理由に、政府支給のモバイルデバイスで中国製アプリ「TikTok」を使用することを禁止した（2019 年 12 月）	35.1
6	総合電機メーカーがサイバー攻撃を受け、個人情報や機密情報が流出したおそれがあると発表（1 月）	33.5
7	総合電機メーカーへのサイバー攻撃で、防衛関係の機密情報が同社から漏えいした疑いがあることが判明（5 月）	32.9
8	納税などに関する大量の個人情報や秘密情報を含む地方自治体の行政文書が蓄積されたハードディスク（HDD）が、ネットオークションを通じて転売され、流出していた（2019 年 12 月）	31.4
9	「Zoom」の「Windows」版クライアントについて、攻撃者がグループチャットのリンク共有機能を悪用した場合、リンクをクリックした人の Windows のネットワーク認証情報が漏えいする可能性があることが明らかに（4 月）	30.9
10	電気通信事業者等を傘下に置く持株会社の機密情報を不正に取得したとして、同社元社員を逮捕。容疑者が取得した機密情報は在日ロシア通商代表部の職員らに譲渡されたとみられる（1 月）	30.2

2020 年を代表する事件“電子決済サービスを通じて不正預金引き出し”

今年を代表する事件としてランキングの第 1 位に登場したのは電子決済サービスを通じて、利用者の預金が何者かに不正に引き出された事件でした。ユーザーはサービス口座と銀行口座を容易に紐付けることができ、利便性の高さから注目が集まっていました。利便性のみを追求した結果、セキュリティの甘さを狙われたこの事件は、世間に大きな衝撃を与えました。

進化する技術や人々の混乱に乗じた脅威のリスクについて考える一年に

今年のランキングの第 3 位にランクインした AI を悪用したディープフェイク、第 4 位の新型コロナウイルス感染症に便乗したフィッシングサイト、第 9 位のオンライン会議システムの潜在的リスクなど、2020 年は進化する技術や人々の混乱に乗じた脅威のリスクについて考える一年となりました。新たな日常に適応したサービスの利用者が増える中、企業や個人は真偽を見極めることが求められます。

マカフィー株式会社の代表取締役社長である田中 辰夫は次のように述べています。

「今年は新型コロナウイルス感染症の影響で在宅時間が長くなり、さまざまなオンラインサービスの利用が増えた一年だったと思います。数多くのオンラインサービスが存在していますが、容易に利用できる便利さとリスクは表裏一体であり、セキュリティにも意識を向ける必要があります。今後も我々のビジネスや生活において、ますますデジタル化が進んでいくことが予想されますが、そのような環境で企業や個人の大切な情報や資産を守っていく方法について、より一層、理解を深め対策を強化していく必要がると考えています。」

【調査概要】

調査名：　「2020 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 6 回調査後の 2019 年 12 月から今回の調査を開始した 2020 年 11 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：　2020 年 11 月 26 日～2020 年 11 月 27 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）

マカフィーについて

マカフィーはデバイスからクラウドまでを保護するサイバーセキュリティ企業です。業界、製品、組織、そして個人の垣根を越えて共に力を合わせることで実現するより安全な世界を目指し、マカフィーは企業、そして個人向けのセキュリティ ソリューションを提供しています。
詳細は https://www.mcafee.com/enterprise/ja-jp/home.html をご覧ください。

＜本情報のお問い合わせ＞

マカフィー株式会社（ https://www.mcafee.com/enterprise/ja-jp/home.html ）
広報担当 戸田
Tel: 070-2680-0731
hiromi_toda@mcafee.com

マカフィー広報担当
ウィタンアソシエイツ 担当：中根／桑村
mcafee-pr@witan.co.jp