2022 年 2 月 24 日
デジタルアーツ株式会社

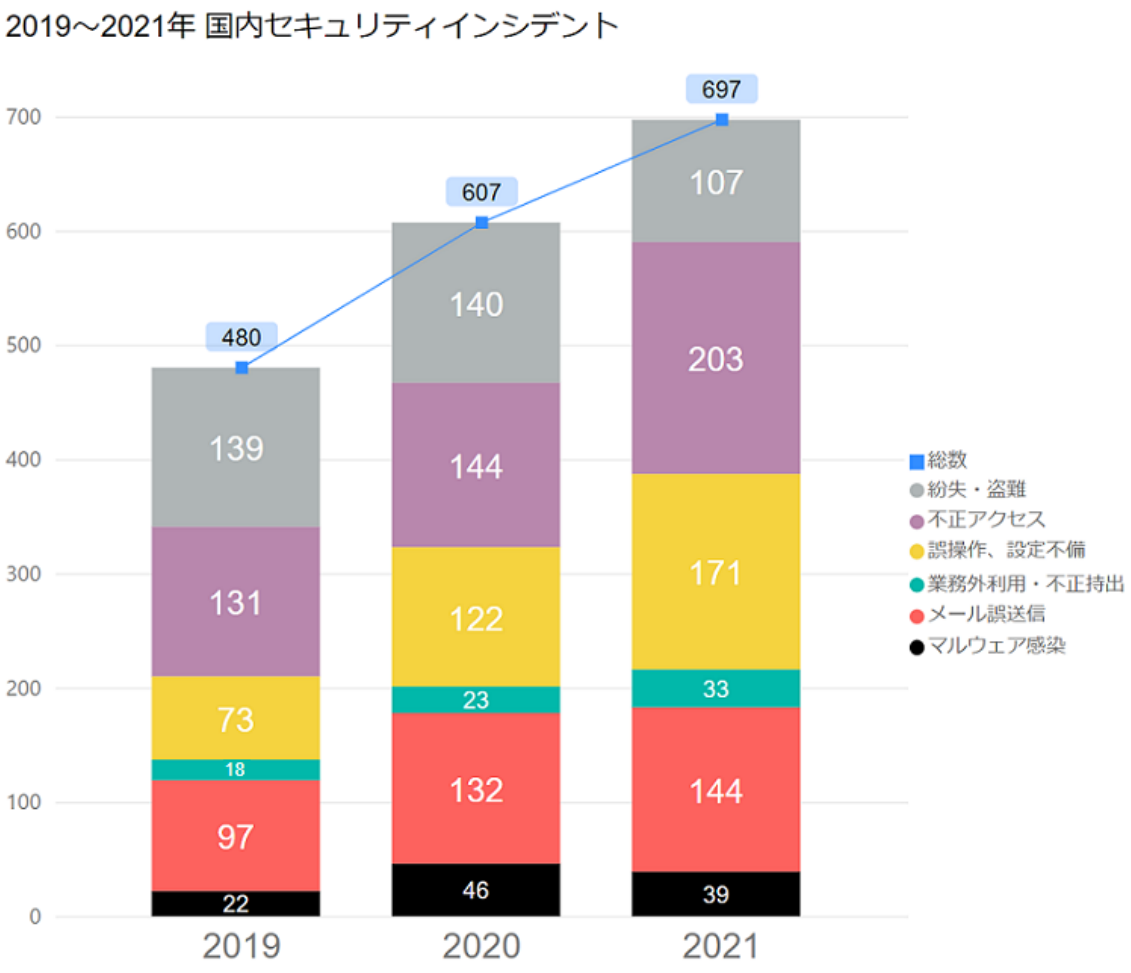
PRESS RELEASE

【セキュリティレポート】
過去３年間の国内セキュリティインシデントを集計、インシデント最多は「不正アクセス」
～2021 年からランサムウェアが急増　マルウェア感染のうち 8 割を占める結果に～

情報セキュリティメーカーのデジタルアーツ株式会社（本社：東京都千代田区、代表取締役社長：道具　登志夫、以下 デジタルアーツ、証券コード 2326）は、過去 3 年分の国内セキュリティインシデントを集計したセキュリティレポートを公開したことを発表いたします。

2019 年から 2021 年の国内組織における情報漏洩等のセキュリティインシデントを独自に集計

デジタルアーツは、2019 年から 2021 年の国内組織における情報漏洩等にかかるセキュリティインシデントを、対象組織による公開報告書とマスメディアによる報道資料をもとに独自に集計しました。2021 年の国内セキュリティインシデントは 697 件と、前年の 607 件を上回っており、最多は「不正アクセス」の 203 件、次いで「誤操作、設定不備」によるインシデントが 171 件でした。また、「ランサムウェア」によるインシデントは 2021 年に急増し、「マルウェア感染」インシデントは 39 件のうち、32 件と大半を占める結果となりました。



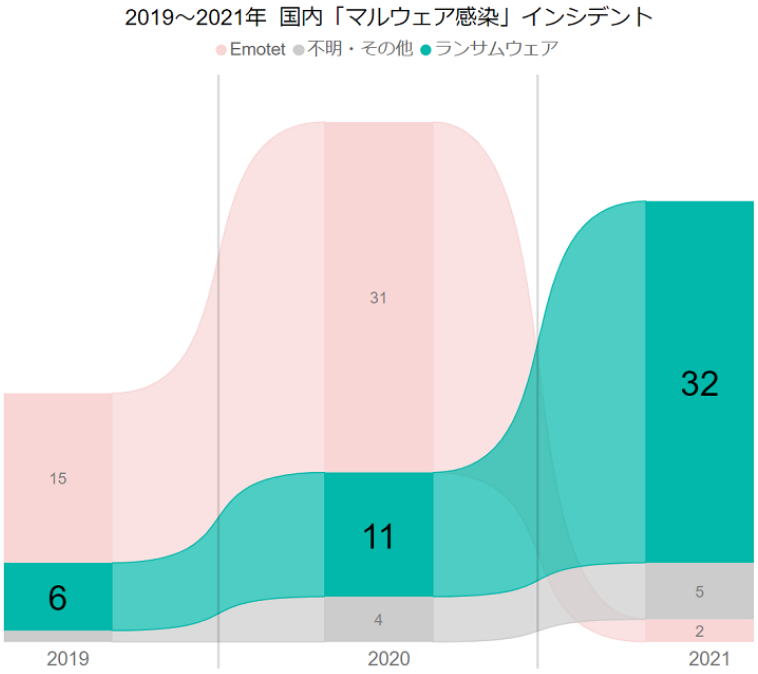
最多のセキュリティインシデントは「不正アクセス」、その主な原因は「脆弱性」

まず、2021 年の「不正アクセス」の例としては、プロジェクト情報共有ツールへの不正アクセスにより、政府機関など約 130 の組織に影響を与えたものがありました（ただし本稿での集計では公開された組織のみカウント）。他にも、EC サイトの運営・委託組織が被害に遭い、多数の委託元が影響を受けたといったものもありました。

「不正アクセス」のうち 2021 年のインシデントにおいて何が原因となっていたのか分類した結果、「不正アクセス」インシデントは「脆弱性」が原因であったものが 48%とおよそ半数を占めていることがわかりました。この中で特に被害が多かった組織は、EC サイト（通販サイト）を運営している組織でした。

「マルウェア感染」インシデントはランサムウェアが大半を占める結果に

2021 年下半期もランサムウェア被害は増加し続け、2021 年の「マルウェア感染」インシデントは 39 件で、そのうち「ランサムウェア」が 32 件と大半を占める結果となりました。



2021 年 10 月には徳島県の町立病院がランサムウェアに感染し、電子カルテが使用不能となり新規患者や救急搬送の受け入れを停止するなど、生命にもかかわる非常にショッキングなインシデントも発生しました。

感染したランサムウェアは「LockBit 2.0」だといわれています。データを盗みかつ暗号化し、金銭を支払わなければ盗み出したデータを公開するという「二重脅迫型のランサムウェア」です。被害を受けた同病院では、犯人との交渉はしないことを決断し支払いを拒否しました。

ただし、新システムの構築費用や、被害を受けた後の患者や職員のケア、様々な事務処理対応などかかったコストは少なくありません。ランサムウェアの侵入経路ははっきりと公開されていませんが、メディアからの取材に対し同病院は、遠隔保守用の通信回線から不正アクセスされた能性がある旨を述べています。

また、2022 年 1 月に情報処理推進機構（IPA）が公開した情報セキュリティ 10 大脅威 2022 では、「ランサムウェアによる被害」が昨年と同様に組織部門 1 位に選出されました。今年も引き続き警戒すべき脅威といえます。

「Emotet」のインシデントは 2 件でした。Emotet は 2021 年 1 月末にテイクダウンされたことにより、しばらくの間は新たな被害は出ていませんでしたが、2021 年 11 月に復活しました。日本では同年 12 月ころに本格的に活動をし始め、すでに Emotet に感染した組織からの報告も確認しています。翌 2022 年 2 月の執筆時点でも活動は衰えておりません。今後、さらに Emotet によるインシデントが増加する可能性が高いでしょう。

この数値は公開されたインシデントのみであり実際はもっと多いと考えられる、より一層のセキュリティ対策が必要

注意していただきたいことは、ここまでに述べてきた数値は「公開されたインシデントのみ」だということです。情報を公開する組織が増えてきていますが、発生してしまったセキュリティインシデントを公開できている組織はごく一部のみでしょう。表面化していないだけで「不正アクセス」や「マルウェア感染」、その他の被害に遭ってしまった、もしくは現在遭っている組織が多数存在しているということは間違いありません。

セキュリティ対策はどの組織でも行っているかと思いますが、攻撃者はその対策をあの手この手で潜り抜けてきます。今後もより一層、組織におけるセキュリティ対策が必要となるでしょう。

▼デジタルアーツが提案するセキュリティ対策

■「i-FILTER」Ver.10 ・「m-FILTER」Ver.5 – セキュリティ対策の新定番 ホワイト運用

受信したすべてのメールを開け、アクセスしたい Web をクリックできる。情報システム部門の運用負荷も削減できる。デジタルアーツの「ホワイト運用」がセキュアな世界を実現します。 https://www.daj.jp/bs/ifmf/

■「FinalCode」

ファイル暗号化・暗号化ソフトなら「FinalCode（ファイナルコード）」。重要ファイルを暗号化して、利用状況を追跡、遠隔削除もできる究極のファイルセキュリティです。ファイル暗号化による情報漏洩対策には、FinalCode をご活用ください。
https://www.finalcode.com/jp/

■「ZIP 暗号化」運用（PPAP）は効果がないのか？Emotet や IcedID などの外部攻撃対策にはデジタルアーツの『脱 ZIP 暗号化』運用

メールでファイルを送る際に、日本の多くの企業・団体で慣例化された「ZIP 暗号化」運用（PPAP）ですが、セキュリティレベルを担保するための暗号化ではないため様々なインシデントリスクを抱えてきました。弊社ではこれら「ZIP 暗号化」運用のリスクに対していち早く警鐘を鳴らし、解決しています。 https://www.daj.jp/bs/lp/zipencryption/

▶過去 3 年分の国内セキュリティインシデント集計についてのレポートはこちら

以下、弊社コーポレートサイト上にて公開しております。
セキュリティレポート　https://www.daj.jp/security_reports/220224_1/

デジタルアーツ株式会社　概要

Web、メール、ファイルなどのセキュリティソフトウェアの提供を核に事業展開する情報セキュリティメーカーです。
1995 年の創業以来、「より便利な、より快適な、より安全なインターネットライフに貢献していく」を企業理念とし、有害情報の閲覧を制限する Web フィルタリングソフトを開発、以来企業・公共・家庭向けに情報セキュリティ製品を提供しております。

東京都千代田区大手町 1-5-1 大手町ファーストスクエア　ウエストタワー14F　▶URL: https://www.daj.jp/
＜本リリースに関するお問い合わせ＞
デジタルアーツ株式会社　広報担当　石井　　TEL　: 080-8750-0425　/ E-mail : press@daj.co.jp
※新型コロナウイルス感染症拡大に伴う在宅勤務実施中のため、お電話でのお問い合わせは上記とさせていただきます