2024 年 9 月 26 日
デジタルアーツ株式会社

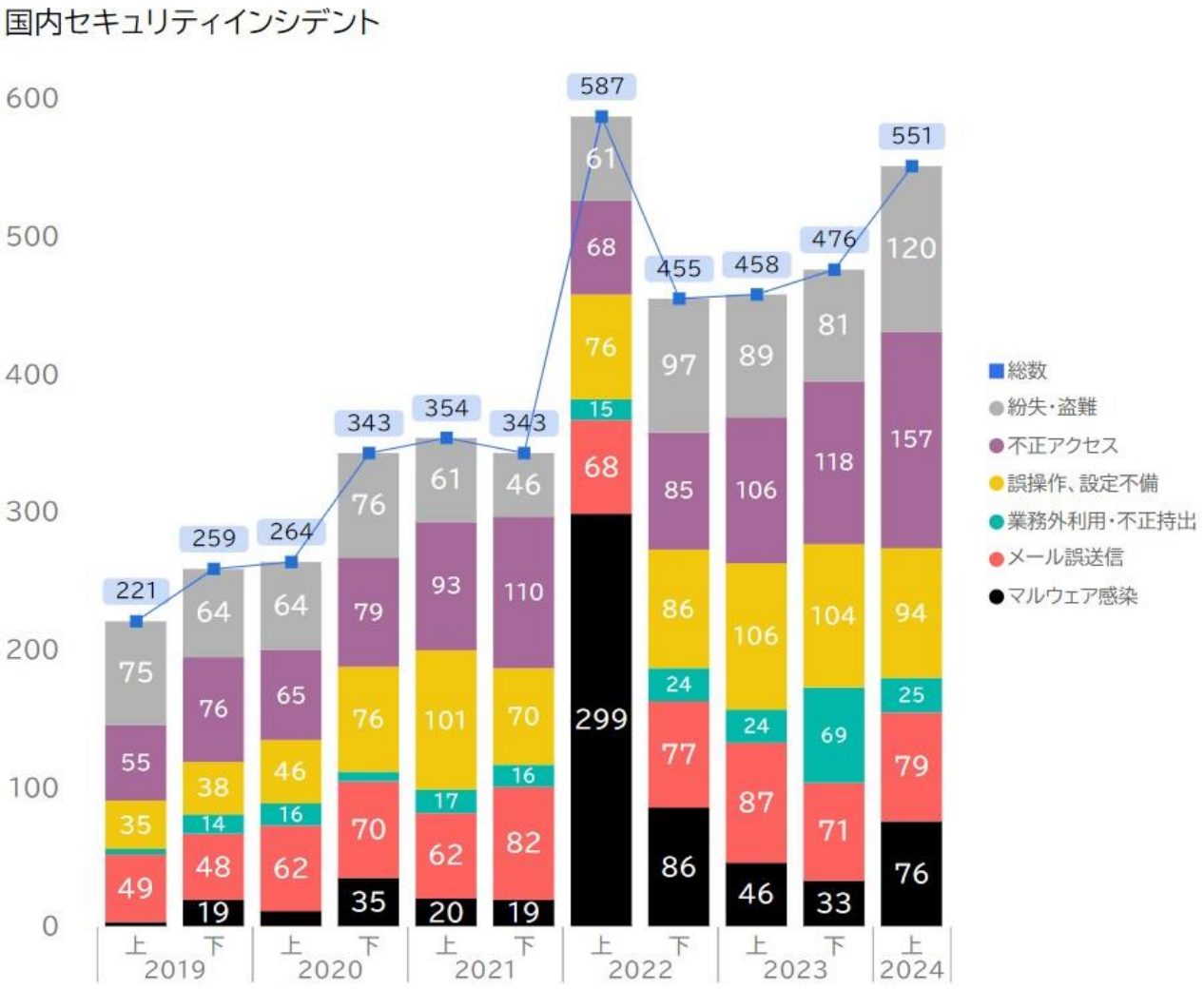
PRESS RELEASE

【セキュリティレポート】2024 年上半期の国内セキュリティインシデントを集計
ランサムウェア被害が増加　マルウェア感染の 9 割以上を占める

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、2024 年上半期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します。

2024 年上半期の国内組織における情報漏えいなどのセキュリティインシデントを独自に集計

2024 年上半期（1～6 月）国内組織における情報漏えい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およびマスメディアによる報道資料をもとに独自に集計※1 しました。



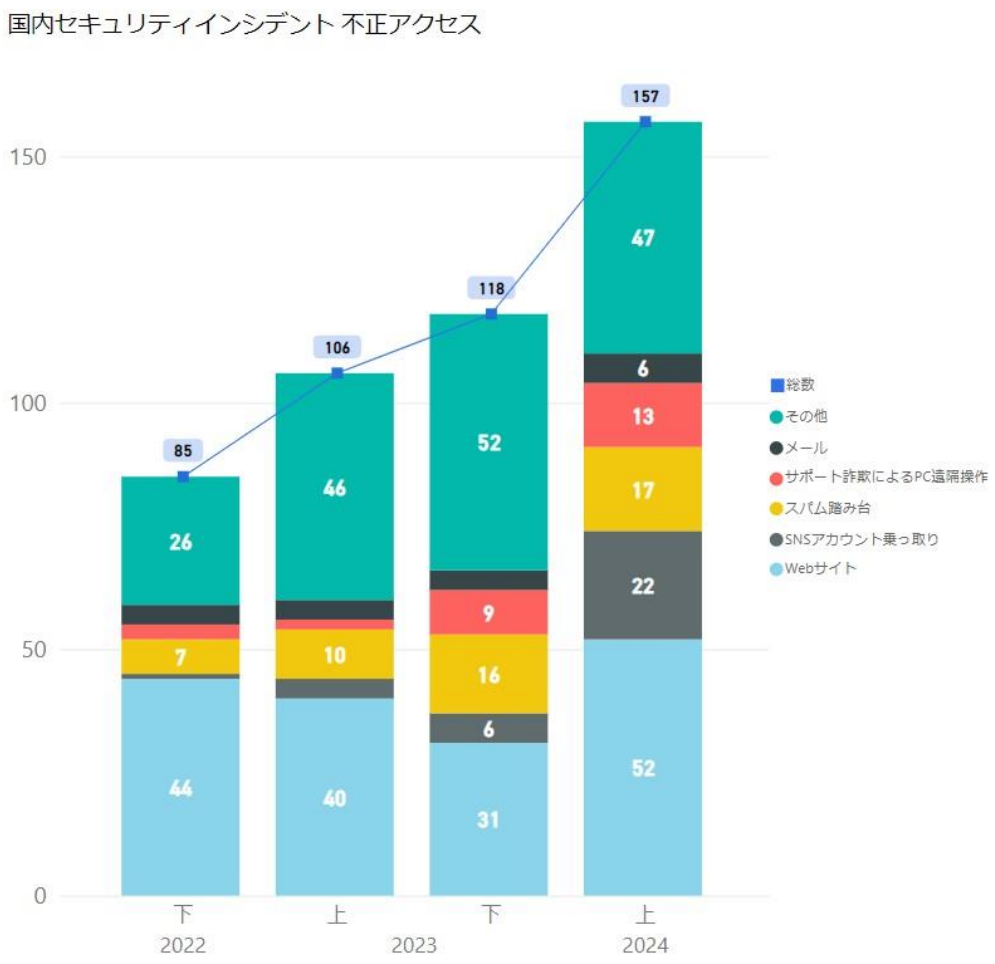
2024年上半期のセキュリティインシデント総数は、551 件で、「不正アクセス」が 157 件で最多となり、2023 年下半期と比較して「業務外利用・不正持出」が 25 件とおおよそ 1/3 に減少しました。「業務外利用・不正持出」が減少した要

因は 2023 年下半期に発生した、大手グループ会社の元派遣社員による顧客情報の不正持ち出しに関連するインシデントでの一時的な増加が落ち着いたことによります。

また 2023 年上半期と比較すると、「マルウェア感染」が 46 件から 76 件となり、大幅に増加しました。

2019 年からのセキュリティインシデント総数は、Emotet が猛威を振るった 2022 上半期を除くと増加傾向にあります。また今回の調査でセキュリティインシデント総数が増加した外的な要因の 1 つに、2024 年 4 月 1 日から個人情報保護法の施行規則及びガイドラインの改正が考えられます。これにより、漏えい等発生時の報告・通知義務と安全管理措置を講じる義務、保有個人データに関する事項の公表等の対象範囲が拡大し、委託先等の第三者に対する不正アクセス等によって生じた漏えい等も報告の対象となりました。

「不正アクセス」157 件のうち 1/3 が Web サイトの改ざんやショッピングサイトへの不正アクセスによる情報漏えい



2024 年上半期の「不正アクセス」157 件のうち 52 件は Web サイトに起因するものであり、Web サイトが改ざんされたケースやショッピングサイトへの不正アクセスにより顧客情報が流出したことがわかりました。

そのほか、SNS アカウント乗っ取りやスパム踏み台、サポート詐欺による PC 遠隔操作の順で続き、特に SNS アカウント乗っ取りは 2023 年下半期と比較して 3 倍以上に増加しました。

SNS アカウント乗っ取りは、企業やファッションブランド、Web メディアやイベントの X（旧 Twitter）や Instagram の公式アカウントなどを乗っ取り、外部サイトに誘導する URL が付いた不審なダイレクトメッセージ（DM）の送信や、アカウント運営者の意図しない投稿をするといった事象が確認されました。

マルウェア感染の 9 割以上はランサムウェア被害

2024 年上半期の「マルウェア感染」76 件のうち、ランサムウェア被害によるものが 74 件と 9 割以上を占めており、その件数は 2023 年上半期と比べて倍増しました。また、ランサムウェア被害の 74 件中 27 件が、多数の組織が印刷業を委託する企業で発生したランサムウェア被害に起因する情報漏えいインシデントで※2、同社に業務を委託していた多数の組織が情報漏えいの可能性を公表しており、自治体から金融機関まで多岐にわたっていることから、影響が広範囲に及ぶインシデントであることがうかがえます。
さらに、「マルウェア感染」の半数がサプライチェーンに起因するインシデントであり、この印刷業務の委託先企業の事例がその主な要因となっています。

今後もランサムウェアの脅威は続く可能性があり、サプライチェーンの多様化・煩雑化により、委託先や取引先などでのインシデントも考えられます。被害者・加害者の両方にならないために、自組織が実施するセキュリティ対策はもちろん、委託先や取引先やクラウドサービス提供者における情報セキュリティ対策の確認や監査を検討するなど、サプライチェーン全体を視野に入れた対策を行うことが重要であると考えられます。

※1　過去に公開済みの記事と比較すると分類項目によっては数値の増減があります。これは新たに見つかったインシデントの追加や既存インシデントの更新情報の反映/分類の見直し、等を行ったことによります。
※2　本集計は 6 月末までの公表分を対象としていますが、7 月以降も当該委託先企業関連のインシデントが継続して確認されています。

詳細のセキュリティレポートはこちら
2024 年上半期国内セキュリティインシデント集計

ランサムウェアの攻撃傾向はこちら
ランサムウェアを知る　そして、対策する

「D アラート発信レポートサービス」は、マルウェアの脅威検知・対処方法をお伝えするレポートです。「いつ」「どのユーザーに」「どんな脅威が発生したか」レポートを見るだけで把握が可能で、「今後どのように対処すれば良いか」の明瞭な対処方法をご提示します。

新オプション「Anti-Virus & Sandbox」のご紹介
デジタルアーツが提供する新オプション「Anti-Virus & Sandbox」は安全な Web サイト・メールからの安全なファイルのダウンロード・受信をリアルタイムに実現し、セキュリティレベルを向上させます。

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。

「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。

IDaaS ソリューション StartIn(スタートイン)
安全な「Login」で業務を快適に「Start」できる世界を実現する StartIn(スタートイン)は多要素認証、シングルサインオン、ID 管理、ログ管理に対応する IDaaS（Identity as a Service）ソリューション です。

DLP・ファイル転送サービス「f-FILTER」
DLP・ファイル転送サービス「f-FILTER」は重要情報が入ったファイルを確実に選別、セキュアな状態で正しい相手に受け渡しします。

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、情報漏えい対策や標的型攻撃をはじめとするサイバー攻撃対策を実現する最先端の製品を、企業・官公庁・学校・家庭向けに提供しています。

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 広報課 関 TEL : 03-5220-1670/ E-mail : press@daj.co.jp