2025 年 9 月 9 日
デジタルアーツ株式会社

PRESS RELEASE

2025 年上半期の国内セキュリティインシデント、集計以来過去最多の 1027 件に

突出する不正アクセス、サプライチェーン起因が増勢／実被害額は機会損失を含め巨額化

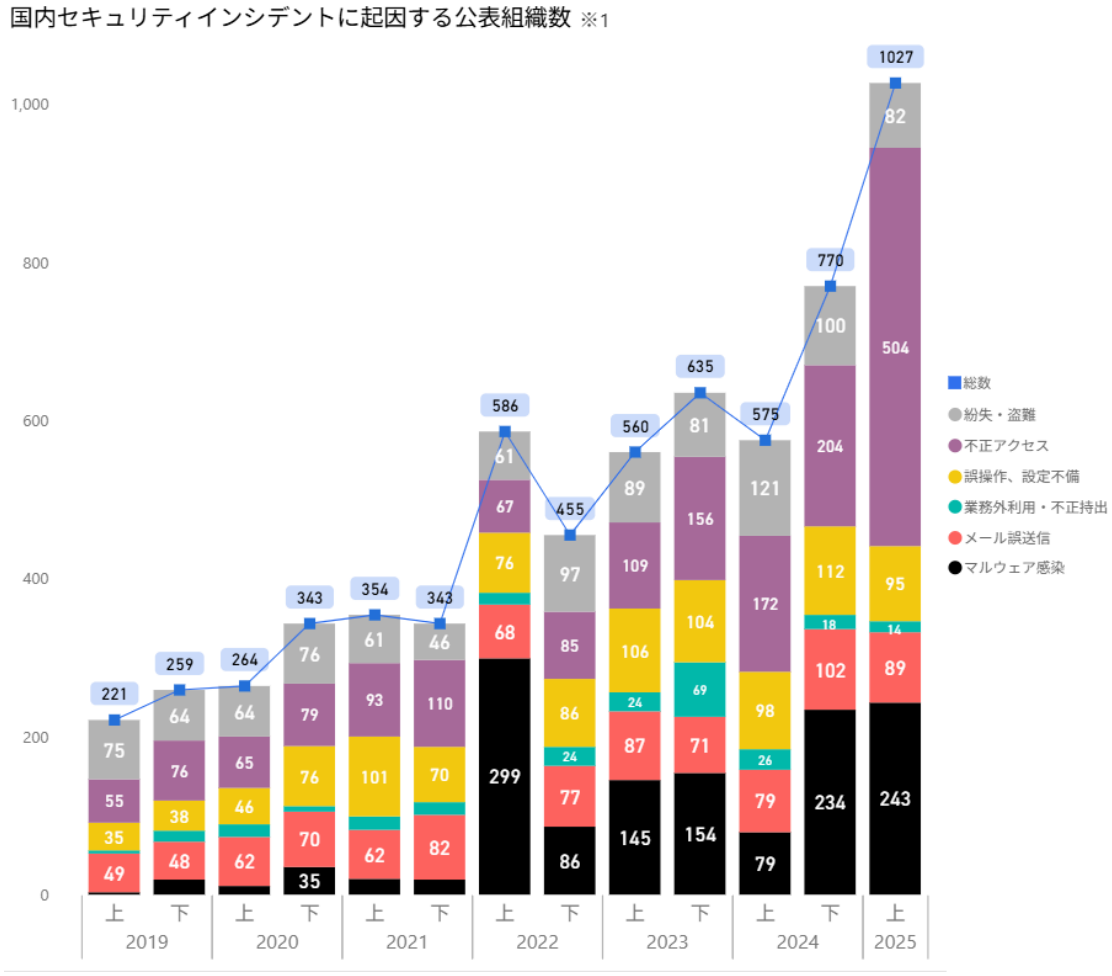
情報セキュリティメーカーのデジタルアーツ株式会社（本社：東京都千代田区、代表取締役社長：道具　登志夫、以下デジタルアーツ、証券コード 2326）は、2025 年上半期（1～6 月）国内組織におけるセキュリティインシデントを、対象組織による公開報告書およびマスメディアによる報道資料をもとに独自に集計し、その結果を発表いたします。

詳細のセキュリティレポートはこちら

2025 年上半期国内セキュリティインシデント集計

セキュリティインシデントは “過去最多”を更新

デジタルアーツが発表した「2025 年上半期 国内セキュリティインシデント動向」によると、2025 年上半期の総数は集計以来過去最多の 1027 件を記録しました。中でも不正アクセスが最も多く、次いでマルウェア感染が多くを占める結果となりました。総数は前年同期比で約 1.8 倍になっており、サプライチェーン起因のインシデント増加が主な要因です。

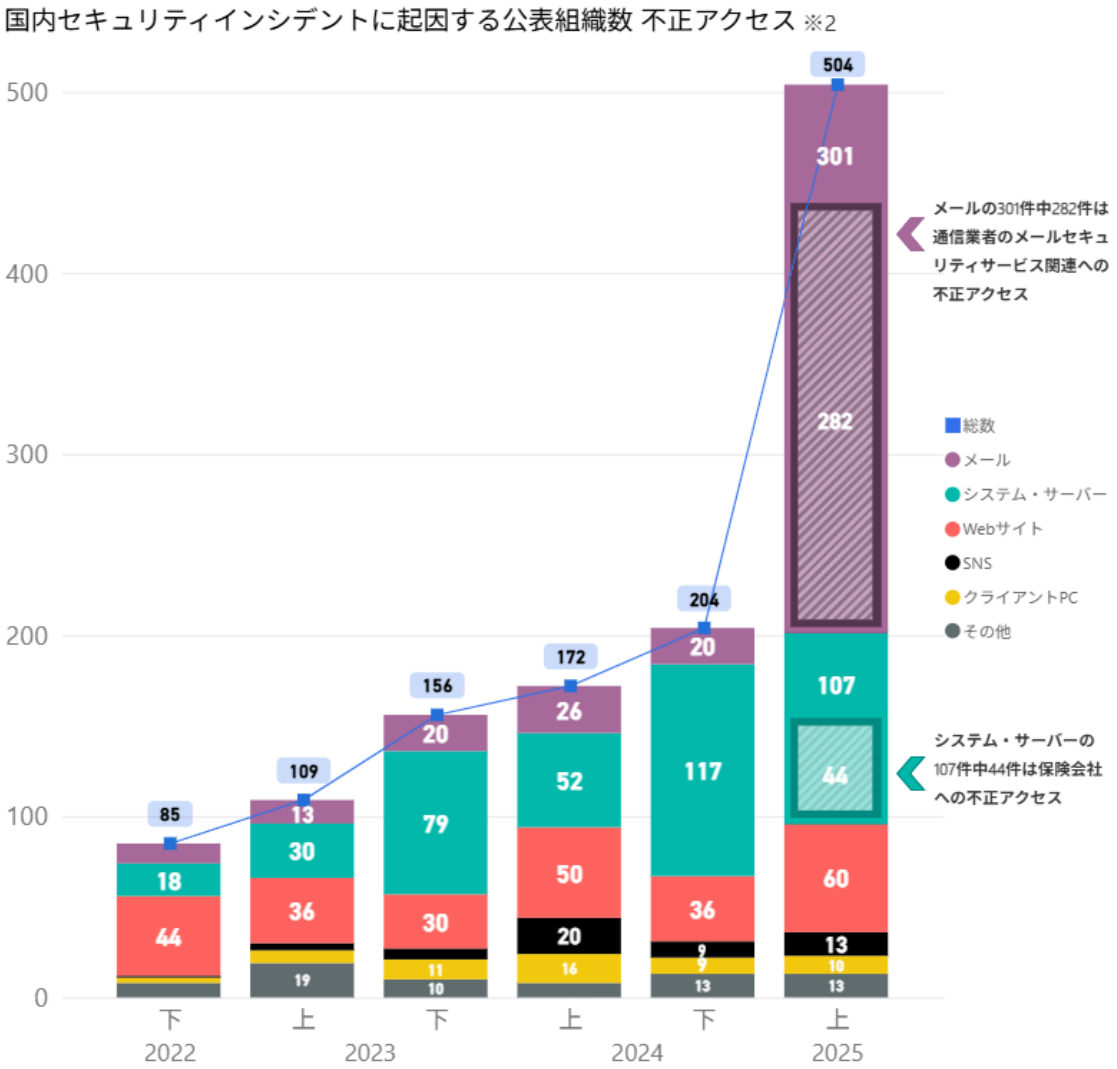


※1‥本集計では、インシデントの連鎖的影響を個別に計上しています。
例えば、業務委託先企業がランサムウェア被害を受け、情報漏えい報告があった場合、それを 1 件として計上します。
さらに、その被害により影響を受けた委託元企業からの情報漏えい報告も、それぞれ独立したインシデントとして計上しています。

不正アクセス突出の要因は大規模なインシデント

不正アクセスの分野では、個人情報やカード情報が漏えいした事例が増加しています。特に、一件の不正アクセスから連鎖的に広がる大規模なインシデントが報告されており、保険会社関連では 44 件、通信業者のメールセキュリティサービス関連では 282 件に及ぶ事案が確認できました。

注目すべきは、通信業者のメールセキュリティサービス関連の多数のインシデント報告です。この事例は外部サービスの脆弱性を突かれたものであり、その規模の大きさからもサプライチェーンインシデントにおけるリスクの深刻さを象徴しています。加えて、このような多数の報告は、形式的な委託先評価による管理手法ではリスクを防ぎきれない現状を示しています。組織は取引先ごとのリスクを重点的にチェックし、事故発生時の影響を想定した対応策も準備することが重要です。



※2‥ 本集計では、不正アクセスを受けた対象別に公表組織数を集計しています。

インシデントの被害額は軽視できない規模に

被害の重さはインシデント被害額からも読み取れます。2024 年（および一部 2024 年以前）に発生したインシデントごとの被害額および年間売上額について、対象企業の決算書や決算説明資料などをもとにデジタルアーツが独自に算出したところ、機会損失を含めた被害額が約 130 億円に達した製造業のケース、約 105 億円にのぼったメディア関連のケースなど、高額事例が複数確認されました。機会損失を含めない公表でも、最大で約 10 億円の被害額が発生した事例もあり、軽視できない規模です。

インシデント被害額（機会損失を含む）

業種	年間売上額	営業損益	被害額
電機・精密機器メーカー	2617億円	142億円	約130億円
出版・映像メディア企業	2582億円	184億円	105億円
小売・流通業者	4711億円 ※3	314億円 ※3	42億円
物流・倉庫運営企業	152億円	△4700万円	12億3100万円
包装資材・化学製品メーカー	1500億円	101億円	10億円
ITソフトウェア開発企業	26億3900万円	3億4800万円	2億6100万円

インシデント被害額（機会損失を含まない）

業種	年間売上額	営業損益	被害額
建設コンサルタント企業	683億円 ※4	32億円 ※4	約10億円
自動車販売業者	4132億円	167億円	1億3000万円
機械・部品製造業者	676億円	6億9000万円	7600万円
ITソフトウェア開発企業	13億円	△1億7900万円	3200万円
包装資材メーカー	180億円	3億3800万円	2389万円
繊維製品メーカー	208億円	4億3000万円	1960万円

※3・4・・被害額が複数年度に渡る事案については、参考としてインシデントが発生した年度の売上額と営業損益を表に記載しています。

本表からも明らかなように、インシデント発生時の被害額は直接的なコストだけにとどまらず、**機会損失が大きな影響**を与えています。機会損失を含めると、想定以上の被害が発生する可能性も考慮しなければなりません。さらに、営業損益と比べてみると、被害額が営業損益の 8 割～9 割を占めるケースも多く、最悪の場合、被害額が営業損益を上回り、企業の業績にも影響を与えることが読み取れます。こうした実際のインシデント被害額を踏まえると、セキュリティ対策の強化は一層不可欠であると言えます。

サプライチェーンに起因するインシデントが増加要因に

2025 年上半期において、公表されたセキュリティインシデント件数は集計以来過去最多を更新し、特に不正アクセスやマルウェア感染においてサプライチェーンに起因するインシデントが増加要因となっていました。また、単に公表組織数が増加しているだけでなく、個々のインシデントが組織の経営に与える被害額も甚大であり、機会損失を含めた被害は想定以上の影響を及ぼしています。

今後サイバーリスクはさらに多様化し、あらゆる業種・組織にとって無視できない経営課題となることが予想されます。そのために、各組織における現状の対策を見直し、実効性あるセキュリティ対策の強化が不可欠となるでしょう。

■デジタルアーツの Web セキュリティ「i-FILTER」

デジタルアーツでは日々様々な情報をもとにデータの収集を行っています。
「i-FILTER」Ver.10 では、フィッシングサイト URL はフィルターデータベースへと迅速に配信され、
[脅威情報サイト][違法ソフト・反社会行為][不確定サイト（※）] カテゴリにてブロックすることが可能です。

※[不確定サイト] カテゴリは、弊社でカテゴリ精査を行った結果、コンテンツや URL などの付随情報では利用用途が判断できない URL が含まれます。用途が判明した場合は別のカテゴリへと修正されます。

■シングルサインオン・ID 管理「StartIn」

「StartIn」は IDaaS 製品です。通常の IDaaS 製品でできる ID 管理やシングルサインオン、多要素認証に加え、位置（GPS）を利用した「位置情報認証」、第三者（上長など）を認証要素に加える「第三者認証」、定期的にアプリケーションでの認証を実施する「定期認証」の独自認証により、強度の高い認証と安心・安全な ID 管理を実現します。

■安全な Web セキュリティの新定番「ホワイト運用」とは

フィルターデータベースに反映されていない URL についても「ホワイト運用」を行うことで、デジタルアーツが安全を確認した URL にのみアクセスを許可し未知のフィッシングサイトや悪性 URL をブロックすることができます。

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