2025 年 12 月 17 日
デジタルアーツ株式会社

PRESS RELEASE

デジタルアーツ、セキュリティインシデント年間表 2025 を発行

-「システム」「人」「サプライチェーン」3 つの観点から対策を-

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 年に発生した主なセキュリティインシデントを独自に選定し、月別に整理したセキュリティレポート「セキュリティインシデント年間表 2025」を公開しました。

2025 年の主要インシデントを月別にピックアップ

本レポートでは、2025 年 1 月から 11 月までに公表された国内外のインシデントの中から、当社リサーチャーが特に注目した事案を月ごとに整理しています。

2025 年	デジタルアーツのリサーチャーが選定したトピック
1 月	バイオテック企業が BEC（ビジネスメール詐欺）被害 生々しい攻撃手法が明らかに ・ 取引先アカウントの乗っ取りを悪用した BEC 被害。信頼関係や過去の取引履歴を踏まえた、長期観察型の巧妙な手口が明らかに。
2 月	テーマパーク運営会社がランサムウェア被害 最大約 200 万件の情報漏えい可能性 ・ 最大約 200 万件の情報漏えい可能性に加え、オンライン予約やチケット購入などのサービス停止が長期化し、復旧まで約 6 か月を要した。
3 月	証券会社で不正取引が多発 ・ 証券会社利用者のアカウントが乗っ取られ、不正取引による被害が急増。 ・ フィッシングやインフォスティーラーにより窃取された認証情報が悪用された可能性が指摘。
4 月	法人向けメールセキュリティサービスに不正アクセス メールアカウント約 31 万件情報漏えい ・ 法人向けメールセキュリティサービスへのゼロデイ攻撃により、不正アクセスが発生。
5 月	プレスリリース配信サービスに不正アクセス 発表前情報の漏えい可能性 ・ 1,182 社分・1,682 件の発表前情報と、最大約 90 万件の個人情報が流出した可能性が判明。
6 月	保険会社が不正アクセス受け約 1,748 万件の情報漏えい可能性 ・ 顧客・代理店関連のデータなど約 1,748 万件の情報漏えい可能性を公表。Web アプリケーションの脆弱性リスクが改めて浮き彫りに。
7 月	保険事故調査会社がランサムウェア被害 委託元 30 社以上に影響 ・ 同社に業務委託していた保険会社など 30 社以上が相次いで情報漏えいの可能性を公表し、サプライチェーン全体に影響する事案となった。
8 月	CRM サービス上のデータ窃取と恐喝が流行 ・ CRM サービスを狙ったソーシャルエンジニアリング攻撃が流行。電話で IT サポートを装い、認証情報や接続アプリを承認させ、クラウド上の顧客データを窃取・恐喝する手口が多数確認された。

9 月	酒類事業を展開する企業がランサムウェア被害 EDR も検知できず ・ EDR を含む既存対策をすり抜ける形でシステム障害が発生。出荷停止や品薄、同業他社の供給ひっ迫など、業界全体に影響が広がった。
10 月	オフィス用品通販を手掛ける企業がランサムウェア被害 ・ 物流システムを中心に障害が発生。自社のみならず、受託していた他社通販サイトにも影響が及び、法人・個人を問わず生活インフラに近い領域で混乱が生じた。
11 月	新聞社が利用するチャットツールに不正ログイン マルウェア感染で認証情報が流出 ・ 社員の個人 PC がマルウェアに感染し、チャットツールの認証情報が窃取されたことが原因と推定。

3 つの観点から読み解く、2025 年のセキュリティトレンド

本レポートでは、これらのインシデントを踏まえ、2025 年のセキュリティトレンドを次の 3 つの観点から整理しています。

システムの「わずかな隙」を突かれる現実

ゼロデイ脆弱性や設定不備、古いリモートアクセス設定など、システム上の小さな隙が侵入の起点となる事案が目立ちました。EDR など高度な検知製品を導入していても、運用・設計の死角を突かれると攻撃を防ぎきれないことが明らかになっています。

「人」を起点とした攻撃の拡大

ビジネスメール詐欺やフィッシング、偽の IT サポートからの電話など、人の信頼や油断を狙う攻撃が高度化しました。システムだけでなく「人」を起点としたリスクが、より身近な脅威となっています。

サプライチェーン全体に波及するリスク

保険業界や物流関連など、委託先・取引先企業での被害が原因となり、多数の企業や生活インフラにまで影響が及ぶ事案が相次ぎました。自社の対策だけでは不十分であり、サプライチェーン全体を見据えたリスク管理の必要性が一層高まっています。

「システム」「人」「サプライチェーン」3 つの観点で対策の見直しを

2025 年は、ランサムウェアや情報窃取マルウェア、認証情報を狙う攻撃が引き続き深刻さを増すとともに、被害がサプライチェーンや社会インフラにまで広がる構造が改めて浮き彫りになった 1 年でした。

詳細なインシデントの概要や当社リサーチャーによるコメントは、セキュリティレポート本編「セキュリティインシデント年間表 2025」をご覧ください。

詳細のセキュリティレポートはこちら

以下、当社コーポレートサイトにて公開しております。詳細はこちらからご覧ください。

URL：https://www.daj.jp/security_reports/51/

■安全な Web セキュリティの新定番「ホワイト運用」とは

「ホワイト運用」は、従来の“通してはいけないものをブロックする”とは真逆の発想です。攻撃やリスクと“接触しない”前提で、安全が確認された通信だけを許可する運用設計により、未知の脅威にもさらされない、予防的で持続可能なセキュリティを実現します。

■SSE + IDaaS ソリューション「Z-FILTER」

「Z-FILTER」は、Web やクラウド通信を許可リスト方式で制御し、URL・ドメイン・アプリケーション単位のポリシー適用、SaaS などのクラウドサービス利用時に機能単位でアクセスや操作を制御する機能、通信の可視化とログ分析を備えた国産 SSE（Security Service Edge）＋IDaaS（Identity as a Service）ソリューションです。

■Web セキュリティ「i-FILTER」

「i-FILTER」は、Web セキュリティ製品です。有害情報や業務に関係のない Web サイトの閲覧を防ぐフィルタリングに加え、外部からの攻撃、内部からの情報漏えいも防ぎます。国内で検索可能な URL を網羅したデータベースにより、危険な Web サイトや未知の脅威へのアクセスをブロックし、デジタルアーツが安全と判定した Web サイトのみアクセスできる環境を実現しています。

■メールセキュリティ「m-FILTER」 Ver.5

メールセキュリティ「m-FILTER（エムフィルター）」 Ver.5 は、電子メールフィルタリング（送受信制御）による誤送信対策、全保存（メールアーカイブ）・検索機能による内部統制・コンプライアンス強化、スパムメール対策・メールセキュリティの推進を実現します。

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