2025 年 10 月 2 日
デジタルアーツ株式会社

PRESS RELEASE

【セキュリティレポート】国内のインシデント集計データからサプライチェーンリスクを分析

-リスク低減に向けた取り組みは急務に、保険、自治体、教育など各分野で規制強化進む-

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、国内組織における情報漏えい等のセキュリティインシデント集計データをもとに、外部委託先や取引先に起因するインシデントの拡大傾向を分析し、サプライチェーンリスクの可視化や、保険・自治体・教育分野で進む規制強化の流れ、ならびに実効性ある対策の方向性を示すセキュリティレポートを公開しました。

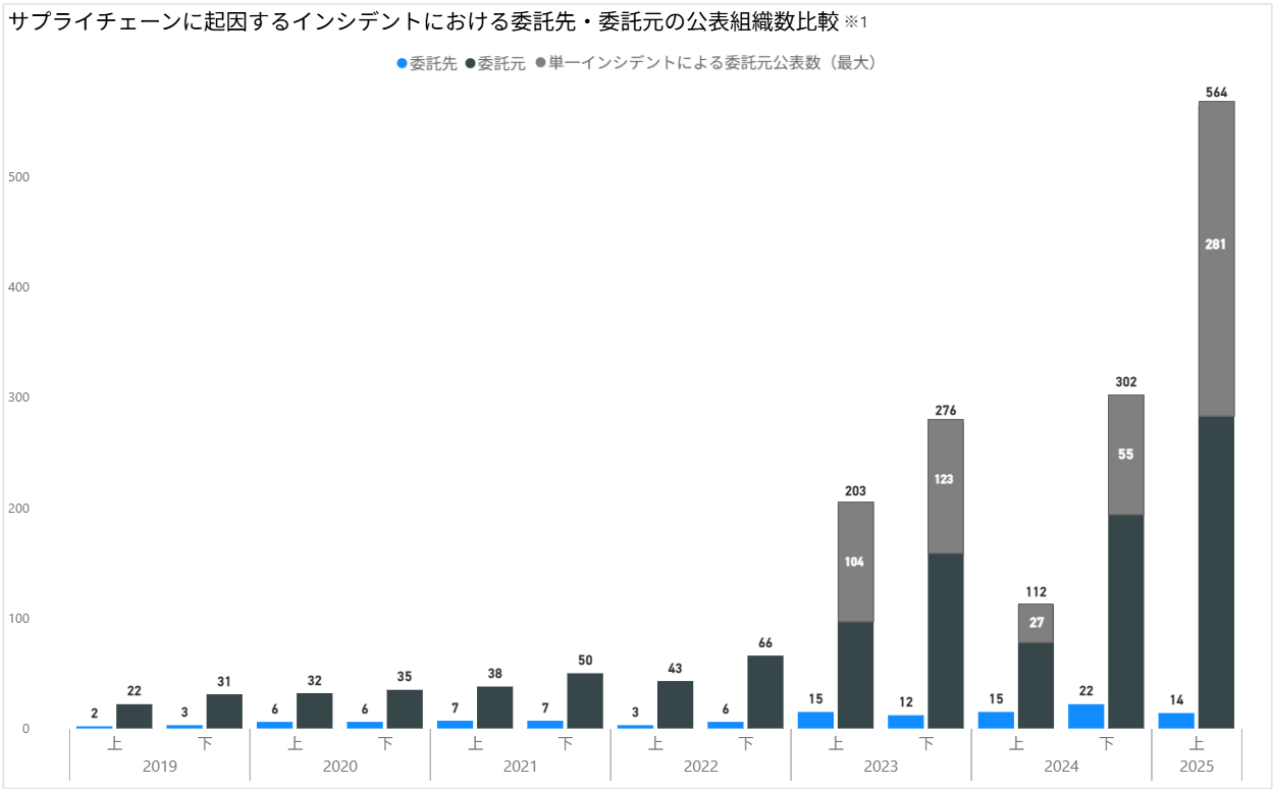
詳細のセキュリティレポートはこちら

サプライチェーンリスクの可視化：国内インシデント集計データから分析

サプライチェーンリスクの傾向とセキュリティ強化の課題

国内組織における情報漏えい等のセキュリティインシデントの集計結果から、サプライチェーンリスクについて分析しました。2019 年以後の半期ごとの国内インシデントの公表組織数を対象に、サプライチェーンを起因とする事案のみを抽出し、委託元組織と委託先組織のそれぞれが公表した件数を集計・比較したところ、両者の公表数には大きな乖離が生じていることが明らかになりました。

特に 2023 年以降はその乖離幅が急拡大しており、2025 年上半期には単一の委託先（またはサービス事業者）における大規模なインシデントが連鎖的に波及し、委託元組織 281 社が影響を公表したケースを確認しています。



この傾向は、1 件のインシデントが多くの委託元組織に連鎖的影響を及ぼす**サプライチェーンリスクの顕在化**を示しており、外部委託やクラウドサービスの活用が進む中で、企業・組織には自社のセキュリティ対策だけでなく、委託先・取引先を含む広範なサプライチェーン全体のセキュリティ管理が不可欠となっています。

こうした背景を踏まえて、サプライチェーン全体のセキュリティを強化する上で課題となるのが委託先管理の複雑性です。委託先ごとに異なる対策レベルや統制方法が存在するため、対策基準の統一が難しく、実務上の大きな課題となっています。このような状況における効果的な管理としては、十分なリスク分析やリスクの大きさに応じた重点的なチェック、事故発生時の影響を想定した対応策を準備しておくことなどが重要です。

※1‥前回のレポート「2025 年上半期国内セキュリティインシデント集計」（https://www.daj.jp/security_reports/49/）の集計を基に、サプライチェーン起因のみを抽出・分類。本集計では委託元と委託先の関係が全件で明確に特定できるわけではなく、委託元のみが公表し対応する委託先の公表が確認できない事例も含みます。

委託元のインシデント対応コストは多岐にわたる

サプライチェーンリスクが顕在化するなかで、委託元など連鎖的に影響を受ける企業・組織は、法的責任や社会的信頼への影響を回避するため、迅速かつ適切な対応が求められます。個人情報保護委員会への報告や影響を受けた本人への通知、プレスリリース・Web サイト等での公表、関係省庁・所轄官庁への連絡、再発防止策の策定など、透明性確保と再発防止の観点から必要な初動は多岐にわたり、金融や教育などの分野では所轄官庁への報告義務が定められている場合もあります。委託先に起因するインシデントであっても、委託元が保有する個人情報が対象となる場合には、これらの対応コストが委託元側で発生することに留意が必要です。

保険業界や自治体・教育機関の動向と規制強化の流れ

業界別の傾向とその対策状況を見ていくと、保険業界では内部不正やサイバー攻撃による顧客情報流出の報告が相次いでおり、金融庁による業務改善命令に加えて各種ガイドラインの整備が進んでいます。

個人情報保護委員会・金融庁が策定した「金融分野における個人情報保護に関するガイドライン」では、アクセス制御の徹底や暗号化の活用などの技術的対策が推奨され、個人データを委託先に提供する際は委託元である金融機関が委託先を継続的に監督する責任が明確化されました。また、一般社団法人生命保険協会の「業務品質評価基準 ガイドライン」では、個人データ管理台帳の整備や委託先管理の徹底が求められています。

自治体や教育機関でも、複数の卒業アルバム制作企業におけるランサムウェア被害を契機として、外部委託業者の選定や委託契約時の個人情報保護対策の見直しが広がっています。

サプライチェーンに起因するインシデントが顕著となるなか、各分野・機関において規制強化と運用の見直しが着実に進展している状況です。

サプライチェーン全体に及ぶセキュリティ管理が求められる時代に

これらの分析から、近年は委託先のインシデントが委託元を含む広範な企業・組織へと波及し、その影響が拡大している実態が明らかとなりました。

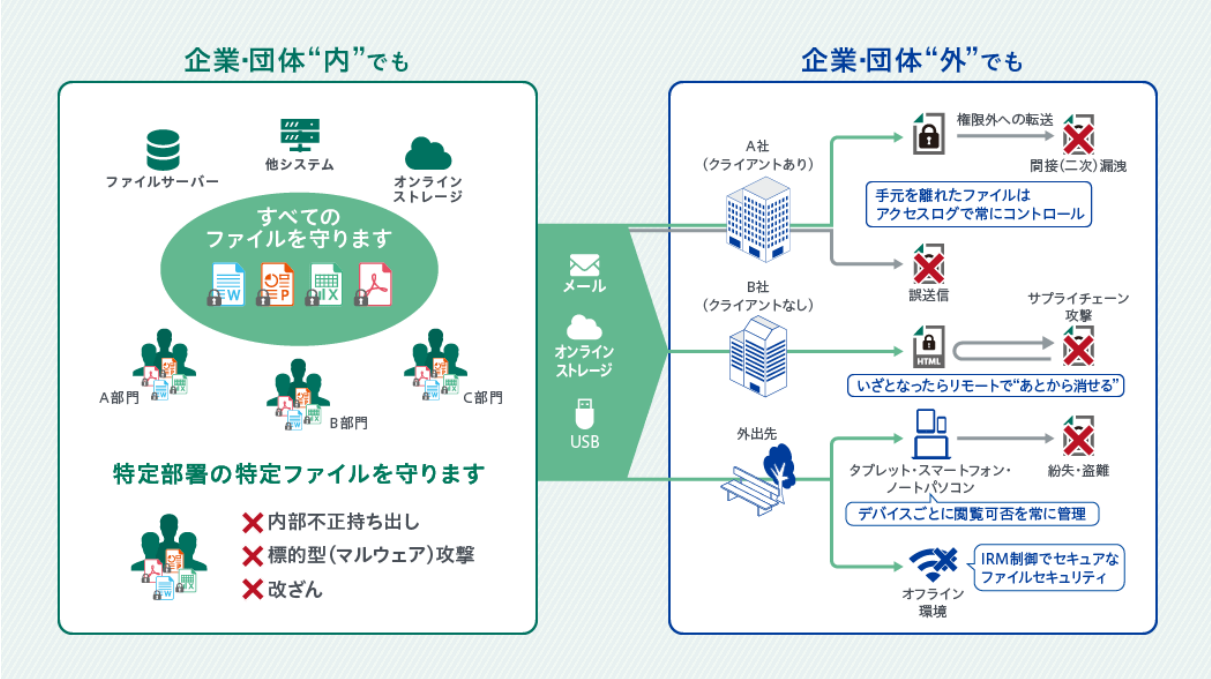
このような状況下においては、もはや自社単体のセキュリティ対策だけでは不十分であり、委託先や取引先も含めた「サプライチェーン全体のセキュリティ管理」が求められています。また、規制や各種ガイドラインの整備が進む中で、企業・組織は情報管理体制の強化とともに、IRM 製品のような情報そのものに権限設定を与え制御する手法や、IDaaS 製品のような統合的な ID 管理と認証基盤によるアクセス制御手段の導入といったリスク低減に向けた具体的な取り組みが急務です。

サプライチェーンリスクが顕在化する中、今後委託元としての責任を果たす上でも、単なる委託先の監督を超えた実効性あるセキュリティ対策と、インシデント発生時に迅速に対応するための体制整備が一層重要となるといえます。

デジタルアーツでは

■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えい対策には、FinalCode をご活用ください。



「FinalCode」の特徴

- **ファイルを暗号化し、自動で追跡・制御**
  暗号化されたファイルは、委託先に送信された後も閲覧・編集・印刷の可否を制御できます。
- **アクセスログで行動を可視化**
  「誰がいつどのファイルを開いたか」を記録します。許可されていないユーザーがアクセスすると、そのタイミングでアラート通知を送ることも可能で、不正アクセスを検知できます。
- **閲覧権限設定により、万が一流出しても閲覧不可**
  暗号化されたファイルが流出した場合にも、閲覧権限を制限することで閲覧をさせず、情報の漏えいを防ぎます。
- **遠隔削除で“あとからでも守れる”**
  プロジェクト終了時等の場面では、委託先企業からリモートで送付した暗号化ファイルを削除することができ、情報漏えいの可能性を防げます。
- **委託先でも、リスクを抑えて業務が可能**
  暗号化されたままファイルを渡せるため、業務委託先や代理店連携時のセキュリティレベルを均一に保てます。

■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。

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