2025 年 1 月 10 日
株式会社ドリーム・アーツ

2025 年 1 月 9 日　セキュリティ調査に関する記者説明会　質疑応答集

2025 年 1 月 9 日（木）に開催した「ドリーム・アーツ　セキュリティ調査に関する記者説明会」において、参加者からいただいたご質問とそれに対する回答をまとめましたので、以下の通りお知らせいたします。なお、ご理解いただきやすいよう、一部内容の加筆・修正を行なっております。

●説明会の内容：情報セキュリティ調査レポートへのリンク
大企業の情報システム部門 500 名に聞いた“情報セキュリティ”に関する調査
【危険な過信！経営層のセキュリティ盲点が企業をリスクに晒す】
https://lp.dreamarts.co.jp/rs/068-CBO-389/images/da_dl_DIR_vol12.pdf

---

Q1　事業会社においては、具体的にどのようなセキュリティ対策を講じるべきでしょうか。

A1　IT ベンダーに依存するのではなく、自社が抱えるリスクやデータ資産を適切に把握し、自ら評価・コントロールする姿勢が求められます。そのためには、脅威の本質を理解し、最新の技術動向を継続的に把握することが重要です。ベンダーの安全宣言をそのまま受け入れるのではなく、自らの責任で安全性を検証する必要があることを、まず認識することが最初の一歩となります。

Q2　役職別の階層における回答傾向を示す表（調査レポート p7）によれば、上位の役職者ほど「十分に対策している」と回答した割合が概ね高くなっておりますが、5 段階の役職のうち、どの階層が情報セキュリティ対策について最も適切に、あるいは切実に把握しているとお考えでしょうか。また、「非管理職（3 年以上）」の階層では、「十分に対策している」と回答した割合が、その上下の階層と比較して例外的に高くなっております。この背景にはどのような要因があるとお考えでしょうか。

A2　「おおむね十分」までを含めると例外的に高いとは言えませんが、あえて考察を加えると、非管理職層については、現場で発生するインシデントに慣れてしまい、それが常態化することで危険性に対する認識が薄れている可能性があると推察されます。「5 段階の役職のうち、いずれの階層が情報セキュリティ対策を最も適切に（あるいは切実に）把握してい

るか」とのご質問に対しては、残念ながらどの階層も十分に対策できていないという見解です。ただし、非管理職層が「危険だ」と認識している割合が相対的に高いことは、調査結果から明らかであると考えられます。

Q3　ドリーム・アーツ社の製品におけるセキュリティ対策について、どのような対策が講じられているのでしょうか。

A3　ドリーム・アーツの製品におけるセキュリティ対策として、「監査ログ機能」を備えており、ユーザーの行動証跡を詳細に確認できる仕組みが整っています。また、特定の権限を持つユーザーが特定の経路を通じてアクセスした場合にのみ情報を閲覧可能とする「権限制御機能」を提供しています。さらに、データにアクセスしているネットワークが社内か社外か、あるいはどの認証方式を経由してログインしているかに応じて、データへのアクセスを制限する機能も実装されています。加えて、ユーザー自身の鍵を用いてサーバー上のデータ内容を暗号化する「BYOK（Bring Your Own Key）」機能も提供しています。

Q4　今回の調査において、ユーザークレデンシャルの窃取や不正利用によるアクセス権限の不正取得、データ侵害などに関する質問や分析は行われておりますでしょうか。また、計算中の暗号化処理について、例えばメインフレーム等での実行が可能とのことですが、その他にどのようなシステムで実行が可能とされているのでしょうか。

A4　特定の不正アクセスに関する調査までは、踏み込んで実施しておりません。暗号化された計算処理については、メインフレーム以外にも、インテル製CPUを使用している場合、「Intel SGX（Software Guard Extensions）」という機能が利用可能です。この機能に対応したソフトウェアでは、OSや仮想化ハイパーバイザーからも内部データを保護する仕組みが提供されています。また、計算中のデータ暗号化の概念においては、データを細分化し、複数のサーバーで分散処理を行うことで、各サーバーの内部情報だけではデータ内容を特定できないように構築する手法も実現されています。

Q5　発表の中で「計算中の暗号化は極めて難しい」とのご発言があったかと存じます。技術的な内容となりますが、その理由についてご教示いただけますでしょうか。

A5　A4の回答と重複いたしますが、Intel SGXを利用する場合、専用のソフトウェア開発が必要となります。このため、技術的難易度が高く、対応するプログラムの開発には相応の

コストが伴います。現状では、こうした高いコストをかけてでも保護すべき重要なデータに限定して活用されるのが一般的です。例えば、鍵管理システム（KMS：Key Management System）などは、計算中も暗号化された状態で利用されているケースが多いです。一方、それ以外のデータに関しては、ここまでのコストをかけて対応する企業は少数にとどまります。ただし、現時点での状況に過ぎず、将来的にはテクノロジーの進歩により、こうした技術が一般的に普及する可能性も十分に考えられます。

Q6　「BYOK（Bring Your Own Key）」について、ドリーム・アーツ社のサービスにおけるユーザーの利用実態についてご教示いただけますでしょうか。

A6　ドリーム・アーツの製品「SmartDB（スマートデービー）」において「BYOK」の対応は 2023 年 12 月に開始し、約 1 年が経過しました。初の導入事例は JCB 社でしたが、それ以降の採用は限定的な状況にあります。その背景には、ユーザー企業側が「BYOK」の仕組みや運用方法について十分に理解していないという課題があり、これはある種のリスクとも言えます。この点については、ドリーム・アーツとユーザー企業の双方に責任があると考えています。ユーザー企業側には、設定を適切に行い、何を守るべきかを明確にした上で取り組む責務があり、ドリーム・アーツ側には、技術や運用方法に関する啓発活動を強化する必要があります。海外、特にアメリカでは既に「BYOK」が一般的な存在となりつつありますが、日本国内では依然として認識や導入状況に差があると感じています。この技術が国内でも標準的なものとして普及するよう、努力を重ねる必要があると考えています。

参考）BYOK についてのプレスリリース（2023 年 12 月 20 日）

ドリーム・アーツ、クラウドセキュリティソリューション第一弾「BYOK」を発表
米シリコンバレー IT ベンチャーFortanix 社と技術提携を開始
1st ユーザー JCB はセキュアな社内 OA 基盤として採用
https://www.dreamarts.co.jp/news/press-release/pr231220/

以上