

従業員が個人で使用しているデバイスやオンラインアカウントに保管されている企業データがリスクに晒されていることが、ワインマジックの調査によって明らかに



業務用のファイルや電子メールにアクセスするときに個人のアカウントやデバイスを使用している英国のオフィスワーカーで、データを常に暗号化しているのはわずか 18% という結果が明らかに。

個々のユーザーの IT セキュリティ習慣を向上するために、一層の教育および啓蒙が必要

2017 年 1 月 16 日（月）東京発—ディスク暗号化ソフトウェアの先進企業、WinMagic Inc. の日本法人であるワインマジック・ジャパン株式会社（本社：東京都港区、カントリーマネージャー：石山 勉、以下ワインマジック）は本日、YouGov によってオンラインで実施された新しい調査結果を公表し、暗号化への対策が不十分であること、そして承認されておらず十分な保護対策が講じられていないデバイスを従業員が使用しているために企業データがリスクに晒されているという結果を明らかにしました。英国のオフィスワーカーを対象としたこの調査では、42% の従業員が企業から提供されていない個人のデバイスを企業の電子メールやファイルへのアクセスに使用していることが判明しました。回答者の約半数（52%）は、EFSS（企業向けファイル共有/同期）などの個人用オンラインアカウントを使用して、業務ファイルを保存または利用していました。一方で、これらのアカウントを使用したことないと答えた従業員は、わずか 34% でした。

オフィスワーカーは、業務用のファイルを保存したり企業のシステムにアクセスしたりするために、ノート PC（30%）、スマートフォン（22%）、USB ストレージデバイス（17%）など、さまざまな個人デバイスを使用しています。オフィスワーカーが業務用のファイルを保存およびアクセスするために使用する個人用オンラインアカウントの上位には、Hotmail（14%）、Gmail（13%）、Dropbox（10%）がランクインしています。

しかし、これらの個人デバイスは、会社から支給されるデバイスと同等のセキュリティレベルが確保されていないことが多い、企業のデータを危険にさらす恐れがあります。たとえば、すべてのデバイスを最新のセキュリティソフトウェアで保護していると回答したのはわずか 52% でした。個人で所有するデバイスのセキュリティを保護することは従業員の責任ですが、移動および保管される企業データを安全に管理および保護するために、多くの対策が従業員に求められます。適切な対策を講じなければ、データが適切に保護されず、企業の外部に保管されることになります。ファイアウォールの外側に企業データある場合であっても、常に保護することが必要となります。

アクセスされる無防備な企業データ

個人デバイスからアクセスされるファイルや個人のオンラインアカウントに保存されたファイルを企業が常に暗号化していると回答したのは、調査を受けたオフィスワーカーのわずか 18%

でした。リモートからデータにアクセスできれば、従業員のワークスタイルが広がり生産性は向上します。一方、デバイスの紛失によって、データが漏洩するケースが多く発生しています。企業データが暗号化されないまま保存されており、十分な保護対策がデバイスに講じられていないと、これらのデバイスに保存されるクレジットカード、医療データ、他の顧客データ、機密の企業データやシステムが、権限を持たないユーザーにアクセスされる恐れがあります。紛失したり、保護機能が不十分である場合、アイデンティティ詐欺につながる恐れがあり、Information Commissioner's

Office (ICO) のような規制当局が定める標準に準拠できなくなることもあります。英国は EU から離脱することになっていますが、その決定にも関わらず、EU 一般データ保護規制 (EU GDPR) は、EU 市民の個人データを管理または処理する英國企業に 2018 年から適用されることとなっています。アカウント番号や IP アドレスなどの情報が含まれる個人データの管理については厳格な規則が適用され、適切にデータを管理していない場合、データの漏洩やセキュリティインシデントにつながる問題について、重大な罰金が科せられます。

ワインマジックの COO、Mark Hickman は次のようにコメントしています。「IT 部門は、従業員が業務を遂行するために必要としている柔軟な環境と企業データのセキュリティ確保とのバランスを慎重に検討する必要があります。優れたバランスを確保するためには、適切なソフトウェアを導入しながら従業員を教育および啓蒙し、企業では管理できない各ユーザーの IT

セキュリティ習慣を向上させることが求められます。暗号化によってもたらされるセキュリティ効果はさまざまですが、クラウドやリモートデバイス、個人アカウント、企業アカウントに保存されたデータを保護できるため、現在の企業環境における要件に最適な効果を発揮できます。暗号化は、オンラインアカウントが侵害されたり、デバイスが紛失したりする場合の最後の防衛線となるのです」

いまだにリスクとなっているパスワード

公開されるデータ侵害はごく僅かであり、ハッキング組織によって数百万のユーザー名およびパスワードが漏洩しています。26%

のオフィスワーカーが、業務用と個人用のオンラインアカウントで同じパスワードを使い回していることを認めているため、個人用のアカウントのパスワードが漏洩する場合、ハッカーは会社と個人の両方のアカウントに直接アクセスできることになります。また、同じパスワードをすべての会社用と個人用のアカウントで使用していると述べた回答者も5% に上ります。

個人用のアカウントでは十分なセキュリティ対策が講じられていないと認識しているにも関わらず、オフィスワーカーの 20%

が、十分なセキュリティソフトウェアをインストールしている場合、個人用のアカウントの使用と業務用ファイルに個人のデバイスを使用してアクセスすることを企業が許可していると述べています。さらに、35%

の回答者が個人用のアカウントは本来使用するべきではなく、使用するハードウェアは会社のポリシーに準ずるものでなければならぬと考えていることも明らかになりました。

Hickman

は、次のように述べています。「従業員はできる限り効率的に業務を遂行したいと考えているだけなのですが、会社に対して与える恐れがあるリスクについては十分に認識していない場合があります。効果的なデバイスおよび暗号化管理の戦略を導入することで、IT 部門は、従業員の生産性を低下させることなく、透過的で円滑なデータ保護を実現できます」

【ワインマジックについて】

ワインマジックは、あらゆる暗号化に対応するインテリジェントな鍵管理機能を備え、堅牢で管理も容易な使いやすいデータセキュリティソリューションを提供しています。ワインマジックのSecureDoc

は、保存場所を問わずデータの安全を確保し、あらゆるオペレーティングシステムにわたり、エンタープライズグレードのデータ暗号化およびアプリケーションアウェアのインテリジェントな鍵管理ポリシーを提供します。SecureDoc

はワールドワイドで多くの企業や政府系機関に採用されており、ビジネスリスクの低減、プライバシーおよび規制コンプライアンス要件への準拠、また不正アクセスからの貴重な情報資産の保護を実現しています。

ワインマジックもしくは SecureDoc製品に関する詳しい情報は、Web サイト

www.winmagic.com/jp をご覧いただくな、お電話（03-5403-4642））、または E メール（sales.jp@winmagic.com）にてお問い合わせください。

本プレスリリースに関するお問合わせ先：

ワインマジック・ジャパン株式会社

〒105-0022 [東京都港区海岸 1-2-3](#)

汐留芝離宮ビルディング 21 階

<http://www.winmagic.com/jp>

(製品情報に関するお問合わせ先)

Email : sales.jp@winmagic.com

Tel : 03-5403-6950

(取材のお申込先)

Tel : 03-3537-1108

Email : winmagic@mlrev.co.jp

Generated by ぶれりりプレスリリース

<https://www.prerele.com>