【プレスリリース】

マカフィー株式会社
2019 年 5 月 8 日

※当資料は、米国時間 2019 年 4 月 30 日に米国で発表されたプレスリリースの抄訳です。

マカフィー、データ漏洩の実態と動向に関する調査結果を公開
IT 担当者の 61%が深刻なデータ漏えいを経験

深刻化するデータ漏えいのリスクを低減するために
セキュリティソリューションと社員トレーニングの連携が重要

ニュースハイライト

- 侵入経路の多くはデータベース漏えい、クラウドアプリケーション、USB ドライブ
- データ漏えいの約 4 分の 3 が公表を要するため、ブランドイメージ損傷の恐れ
- IT 担当者の 81%が CASB と DLP のポリシーと管理コンソールを分けていると回答
- 個人情報と結びつくペイメントカードデータよりも、知的財産が窃盗犯の最大の標的に

デバイスからクラウドまでを保護するサイバーセキュリティ企業である米国マカフィー（McAfee LLC、本社：米国カリフォルニア州）は、データ漏えいの実態と動向についてまとめた調査レポート「Grand Theft Data II – The Drivers and Changing State of Data Breaches」を発表しました。同レポートでは、サイバー犯罪や脅威に対する対策は向上しているものの、IT セキュリティ担当者の 61%がデータ漏えいを経験したと回答しており、データ漏えいを完全に防御することに苦戦を強いられていることが明らかになりました。さらに、サイバー犯罪者は知的財産を標的として執拗な攻撃を仕掛けるようになったため、データ漏えいはさらに深刻な問題になっており、会社のブランドイメージや金銭的ダメージへのリスクが増大しています。

マカフィーの調査結果から、将来的にデータ漏えいのリスクを低減するには、包括的なセキュリティソリューションと社員トレーニング、そして企業全体のセキュリティ意識向上を含むサイバーセキュリティの戦略が必要であることが明らかになりました。

マカフィーのバイスプレジデント兼チーフテクニカルストラテジストのキャンディス・ウォーリー（Candace Worley）は次のように述べています。「脅威はこれからもますます巧妙化していくでしょう。企業全体にセキュリティ意識を確立し、IT チームだけでなく全社員がセキュリティへの責任を担っていると理解させ、セキュリティ対策を強化する必要があります。脅威に打ち勝つためには、企業がセキュリティソリューションを利用するだけでなく、適切なセキュリティ管理を実施するなど、より包括的なアプローチを取ることが重要なのです」

マカフィーのレポート「Grand Theft Data II – The Drivers and Changing State of Data Breaches」 の主なポイントは、以下のとおりです。

- **攻撃者はさらに狡猾に：**最近のデータ窃盗は単一な手法ではなく、多様な手法により行われています。データ窃盗のための侵入経路として最も多いのは、 データベース漏えい、クラウドアプリケーションおよび USB ドライブです。
- **知的財産が標的に**：回答者の 43%は、 個人情報と知的財産が最もダメージを与える可能性があるデータカテゴリと回答しました。 特に、個人情報はヨーロッパで最も懸念されてお

り（49%）、おそらく一般データ保護規則（GDPR）の施行が要因と考えられます。 アジア太平洋諸国では、知的財産の盗難が個人情報よりも大きな関心事（51%）となっています

- **漏えいの発生原因：**回答者の 52%が、データ漏洩の最大の原因は IT であると主張し、 続いて、事業運営（29%）が挙げられています。財務（12%）および法務（6%）などの厳しく規制された内部部署は、安全です。
- **個別管理による弊害：**回答者の 81%が、CASB と DLP に別々のポリシーおよび管理コンソールを使用していると回答しています。引き続き、それぞれ別途で運用していくため、検知と修復に遅れが生じています。
- **責任の取り方：**アカウンタビリティについて、IT 担当者の 55%が深刻なデータ漏えいの際には経営陣が解任されるべきだとしています。一方、61%が自分達に対しては、経営陣はもっと寛容なセキュリティポリシーを採用して欲しいと期待しています。
- **将来に備えて：**IT 担当者の約 3 分の 2 が、過去 12 ヶ月の間に DLP、 CASB およびエンドポイントでの検知ソリューションを追加購入するなどの対処を行なっています。彼らはこのようなシステムがあらかじめインストールされていたら、過去のデータ漏えいの 65 〜80 %はおそらく防止できただろうと考えています。

サイバー犯罪者は個人情報や知的財産を狙って様々な攻撃方法を用いるようになってきているため、より危険になっています。また、データ漏えい発生の際にその事実を公表せざるを得なくなっていることから、 IT セキュリティ担当者は外部からの脅威によってネットワークが破壊されることを恐れています。データ漏えいを公表することは、財政面のダメージだけでなく、ブランドイメージやレピュテーション（評判）の損傷につながります。

参考情報：

- レポート（英語）
- エグゼクティブサマリー（英語）
- インフォグラフィック（英語）
- McAfee MVISION Cloud
- McAfee Data Protection
- McAfee Database Security
- McAfee MVISION EDR
- McAfee Secure Web Gateway

調査方法

この調査はマカフィーの委託を受け MSI-ACI Europe が実施しました。調査対象者は深刻なデータ漏えいのインシデントを経験したことのある IT 担当者に限定しています。データは 2018 年 12 月 12 日〜31 日の間にオンラインでのインタビューを通じて収集されました。また、調査対象は千名以上の従業員を有する企業の中から、企業レベル（1,000〜5,000 人）とエンタープライズレベル（5,000 人以上）の半々としました。結果として、オーストラリア、カナダ、フランス、ドイツ、インド、シンガポール、米国、イギリスの様々な業界のグローバル企業が本調査対象になっています。

マカフィーについて

マカフィーはデバイスからクラウドまでを保護するサイバーセキュリティ企業です。業界、製品、組織、そして個人の垣根を越えて共に力を合わせることで実現するより安全な世界を目指し、マカフィーは企業、そして個人向けのセキュリティ ソリューションを提供しています。詳細は https://www.mcafee.com/ja-jp/ をご覧ください。

* McAfee、McAfee のロゴは、米国およびその他の国における McAfee, LLC の商標です。
* その他の製品名やブランドは、該当各社の商標です。

＜本情報のお問い合わせ＞

マカフィー株式会社（ https://www.mcafee.com/ja-jp/ ）
広報担当 戸田
東京都渋谷区道玄坂 1-12-1 渋谷マークシティウエスト 20 階
Tel: 03-5428-1226 Fax: 03-5428-1480
hiromi_toda@mcafee.com

マカフィー広報担当
ウィタンアソシエイツ
担当：住川／中根
Tel: 03-4570-3169
mcafee-pr@witan.co.jp