

NEWS RELEASE

報道関係者各位

2014年6月10日
日本セーフネット株式会社

SafeNet、認証ソリューション利用調査結果を発表 多要素認証でアクセス管理セキュリティの強化が進む

クラウドベースの認証サービスと、社員のモバイル化に対応するためのモバイル多要素認証の採用が増加している事が判明

米国ボルチモア発(2014年5月21日) – データ保護ソリューションのグローバルリーダーである [SafeNet, Inc \(以下、SafeNet\)](#) は、昨今のセキュリティリスクの高まりと、あらゆるデバイスからいつでもシームレスに安全なアクセスを行うことへの需要増加に伴い、企業の認証ソリューションの採用が拡大している事を発表しました。「[2014年度 認証ソリューショングローバル調査\(2014 Global Annual Authentication Survey\)](#)」によれば、多要素認証(以下、MFA)の採用は2013年から増加し、現在3分の1以上の企業が多数のデバイスや様々な場所からシームレスかつセキュアなアクセスのために、[多要素認証\(MFA\)](#)を使用していることがわかりました。

調査結果によると、多要素認証を採用して従業員に幅広く利用を促す企業が増加傾向にあります。この結果は、米調査会社である451リサーチ社が公表した[レポート](#)^[1]にて「IT事業者は、アクセスコントロールと認証が弱点で、最優先で解決すべき課題」と提言している点と共通しています。2013年に発生したデータ漏えい全体の57%が悪意ある部外者によるものです。MFAを利用することで認証を受けていないユーザーが機密情報にアクセスするリスクを減らすだけでなく、従業員は必要な時に適切な方法で確実に企業リソースにアクセスできます。

調査結果のハイライト

多要素認証(MFA)の採用が大幅に増加

- ・現在、37%の企業が大多数の社員がMFAを利用していると回答し、昨年の30%から増加
- ・56%の大半の企業が、2016年までにMFAを利用すると予想

クラウド認証の受け入れが進む

- ・33%の企業がクラウドベースの認証を選んでおり、昨年の21%から50%分増加
- ・33%の企業が認証の導入にクラウドを活用することに前向き

モバイルデバイス向けMFA

- ・53%以上は、モバイルデバイスのユーザーが企業リソースへのアクセスを制限されていると回答

[1] 451リサーチ「2014年企業の情報セキュリティ組織(The enterprise information security organisation in 2014)」
<https://451research.com/report-short?entityId=80256>

- ・モバイルユーザー向けの MFA を利用する人のうちの 22% は、2016 年までに利用者が全体の 33% に増えると予想(前回調査より 30% 分増加)

SafeNet のクラウド認証ソリューション部門バイスプレジデントの Jason Hart は次のように述べています。「複数の IT 部門で、新技術による急速な変化への対応に苦慮していることは明白です。課題として従業員がアクセスできるようにするための安全な認証がないため、企業は仕事に必要なシステムへの全面的なアクセス権を従業員に与えられません。実際、ほぼ 2 週に 1 度はハッキングされたことや情報が漏えいした可能性があるという企業の話を目にします。つまり、急速な技術の進展を把握し、企業を保護し、セキュリティのリスクを抑えようとする長きにわたる挑戦があります」。

コストと予算の優先順位について

451 リサーチ社は、認証と ID アクセス管理はセキュリティの計画で最優先事項であることを示すレポートを発表しました。しかし、SafeNet の認証調査では、ほぼ 40% の回答者が 1 年のユーザー当たりの認証ソリューションのコストを把握していませんでした。これは企業にとって最もコスト効果が良いソリューションに対する意識の欠如があるといえます。MFA に追加費用を使わないことでコストを節約しているという認識は、IT 予算編成の担当者の誤解を招く可能性があります。実際には、MFA ソリューションは認証費用を引き下げるとともに、利便性を向上させることを目指しています。

クラウドベースの認証 と オンプレミスベースの認証比較

個人のデバイスで社内ネットワークにアクセスする従業員からの需要の高まりに伴い、企業はクラウドベースの認証を拡大することで対応しています。今年の調査では、クラウドベースの認証を選ぶ企業は 33% となり、昨年の 21% から 50% 増加しました。

Hart はさらに次のように述べています。「企業は許可の有無に関わらず従業員がモバイルデバイスを使って企業データにアクセスすることを最終的に受け入れざるを得ない段階に来ています。企業の資源を保護するとともに、社員の生産性やパフォーマンスも維持するためにはアクセスを制限するのではなく、IT 部門の意思決定者は MFA を展開する必要があります」。

モバイルデバイスからの認証

企業のリソースにアクセスするモバイルデバイスに対して強固な認証を利用することについては、回答者の大半は二極化し、偏りがあることがわかります。ほぼ 40% の回答者は、強固な認証を利用する必要のあるユーザーは 10% 未満であると回答したのに対し、20% 以上の回答者は今やユーザーの 90~100% には強固な認証が必要であると答えました。この数字は大きく変化する見込みで、今後 2 年間では 33% の回答者がユーザーの 90~100% には強固な認証が必要になると予想し、強固な認証を利用する必要のあるユーザーは 10% 未満という回答者はわずか 15% にすぎませんでした。これによりモバイル認証の重要性が高まることがわかります。

モバイル認証への動きは、ハードウェアベースの認証トークンからソフトウェアベースの認証トークンへの動きを促進しています。今回の調査では、ソフトウェアベースの認証の利用が 2013 年の 27% から 2014 年には 40% に増え、2016 年には 50% まで増える見込まれています。一方ハードウェアベースの認証の利用は、2013 年の 60% から 2014 年には 41% に低下しました。

Hart は、このことについて次のように述べています。「IT 企業がモバイル化の高まりに対応し、ソフトウェアベースの認証を増やしているのは明らかです。しかし、モバイルを活用したいという要望とモバイル化への動きを把握しつつ外部の脅威から資源やデータを保護するという目的は両立しにくいものです。さらに、クラウド・コンピューティングの採用が増えるにつれ、セキュリティの向上が極めて重要となります。クラウドは認証やアプリケーションに様々なメリットをもたらしますが、クラウドを支えるセキュリティがなければ脅威を拡大するだけだからです」。

本調査について

SafeNet の調査は、世界中の IT 部門における意思決定権をもつ 350 人以上を対象にアンケート調査を実施しました。地域別では、アジア太平洋地域が 29%、欧州・中東・アフリカが 42%、北米が 29%でした。今回のレポートでは、データを 2013 年の同様のレポートと比較しています。要旨は[こちら](#)をご覧ください。

SafeNet のデータ保護ソリューションについて

SafeNet の[データ保護ソリューション](#)は、マルチレイヤの暗号化や、鍵とストレージの中央管理を可能とします。SafeNet は、セキュリティ専門家がデータセンターや仮想データセンター、プライベートクラウドおよびパブリッククラウド環境にて機密データを安全に保つための包括的な暗号化プラットフォームを提供しています。

SafeNet のソリューションによって、ストレージやファイル、仮想インスタンス、データベース、アプリケーションレイヤなど、さまざまな環境内の機密データが暗号化できると共に、暗号化に関するセキュリティポリシーの管理や暗号鍵の中央管理が可能となります。また、SafeNet では、幅広い種類のデータフォーマットを維持したままデータを匿名化するための[トークン化\(トークナイゼーション\)](#)もサポートしています。こうした SafeNet のマルチレイヤへのアプローチにより、以下のことが可能となります。

- ・システムやアプリケーションの管理と、そのインフラ層の中で保存または処理されたデータに対する管理を分けることが可能です。こうすることで、管理者権限を持つユーザーが機密データを閲覧することはできなくなります。
- ・低コスト運用モデルを活用しつつ、確実にセキュリティポリシーが施行できます。
- ・物理環境、仮想環境、パブリッククラウド環境など、さまざまな環境にわたる[中央集中管理](#)が可能で、内部および外部監査員に対し詳細なログやコンプライアンスレポートを効率的に提示できます。
- ・暗号化されたデータの所有権を完全に自社で保持し管理するために、データセンターおよびマルチテナントの両環境に於いて、暗号鍵の保管とセキュアな暗号化を実現します。

こうした SafeNet のソリューションにより、企業は徹底的な防御戦略を策定できます。別の管理場所でセキュリティ侵害が起こった場合でも、機密データが置かれた場所はそれがどこであろうと高いレベルで安全に保つことができるのです。

SafeNet, Inc.について

1983 年設立。[SafeNet](#) は情報セキュリティ業界の世界的なトップ企業で、グローバル企業の最も重要なデータを保護し、信頼を得ています。SafeNet は、お客様の貴重な情報を、データセンターからクラウドまで、情報ライフサイクル全般にわたり保護しています。現在、25,000 を超える企業や政府機関が[情報セキュリティの保護](#)、リスク管理、[コンプライアンス管理](#)、仮想化・クラウド環境の保護を SafeNet に委ねています。

日本セーフネットについて

日本セーフネット株式会社 (<http://jp.safenet-inc.com> 代表取締役社長:酒匂 潔、本社:東京都港区)は、米国 SafeNet, Inc.の日本法人で、2001 年の設立以来、ネットワークやアプリケーションのセキュリティ製品の日本国内での販売、マーケティング、サポートを提供しています。

[Twitter](#), [LinkedIn](#), [Facebook](#), [YouTube](#), [Google+](#) をご覧いただくと SafeNet の詳細情報を入手できます。

SafeNet、SafeNet ロゴは SafeNet, Inc.の登録商標です。その他の商標はすべて、各所有者の財産です。

©2010 SafeNet, Inc. All rights reserved. SafeNet is a registered trademark of SafeNet, Inc. All other products and brand names mentioned in this document are trademarks or registered trademarks of their respective owners.

本件に関するお客様からのお問い合わせ先

日本セーフネット株式会社

TEL: 03-5776-2751

E-Mail: jp-info@safenet-inc.com

本件に関する報道関係者からのお問い合わせ先

日本セーフネット PR デスク

(株式会社アクティオ内)

TEL : 03-5771-6426 FAX : 03-5771-6427

E-mail: safenet-pr@actioinc.jp