PRESS RELEASE
2020 年 10 月 27 日
タレス DIS CPL ジャパン株式会社

タレス、アクセス管理に関する国際調査「タレス アクセス管理インデックス2020 APAC版」を発表

リモートワークによって需要が高まるクラウドアプリケーションに対するサイバー攻撃への脅威と保護対策の促進状況を顕在化

- アクセス管理ソリューションの導入要因は、パスワードの脆弱性を含むセキュリティへの懸念（APAC:81%、日本:75%）、ならびに大規模なデータ漏洩への脅威（APAC・日本:78%）
- クラウドアプリケーションの利用拡大がサイバー攻撃のリスクを高める（APAC:58%、日本:42%）
- IT 意思決定者の中で、セキュリティに関する経営陣からの賛同の獲得が、昨対（APAC:34%、日本:38%）で上昇（APAC:55%、日本:51%）

香港（2020 年 10 月 27 日）---デジタルセキュリティの世界的リーダー企業であるタレスは本日、アクセス管理に関するグローバル調査「タレス アクセス管理インデックス 2020 APAC（アジア太平洋）版」[(1)]の調査結果を発表しました。APAC および日本の IT 意思決定者 500 人を対象とした本調査は、サイバー攻撃の脅威に対する懸念の高まりや、調査対象国内の企業が保護対策を強化させていることを顕在化させました。また、アクセス管理ソリューションの導入を拡大させる大きな要因として、「パスワードの脆弱性を含むセキュリティへの懸念」（APAC:81%、日本:75%）、さらには「大規模なデータ漏洩への脅威」（APAC・日本:78%）という結果を報告しました。

『Access Management and Authentication Trends in the Asia-Pacific Region（APAC におけるアクセス管理と認証のトレンド）』と題したウェビナーを 11 月 18 日に開催し、タレスは本グローバル調査の詳細説明を行います。詳細はこちらをご覧ください。

調査対象全地域においてリモートワークの導入により、企業のクラウド導入は拡大している一方、クラウドアプリケーションの利用増加がサイバー攻撃増加の要因になると懸念（APAC:58%、日本:42%）しています。先日タレスが発表した「2020 年 タレス データ脅威レポート グローバル市場版」では、1 社平均 29 種類のクラウドサービスを利用していることを明らかにしています。今日のような状況下において、クラウドサービスはあらゆるビジネスで不可欠となっています。

潜在的脅威を減少させながらクラウドへのアクセス管理を簡素化するために、企業（APAC:89%、日本:87%）はスマート・シングルサインオン（SSO）の利用拡大を推進しています。SSO が提供する安全性については、機密データ保護（APAC:57%、日本:54%）、アプリケーション保護（APAC:45%、日本:20%）と回答しています。また、データ漏えい防止（APAC:47%、日本:41%）、および顧客データの安全性（APAC:44%、日本:33%）に対する利点があるとも回答しています。

APAC 地域内の IT 意思決定者が抱えるサイバー攻撃への脅威は、依然として払拭されていません。その理由として、クラウド全体のセキュリティ保護に関する一貫性の不足（APAC: 57%、日本:46%）、適切な保護対策を実行できる強力なサイバーセキュリティソリューションの欠如（APAC: 56%、日本:50%）、さらにはクラウドアプリケーションのセキュリティを確保するための社内のスキル不足（APAC: 53%、日本:65%）を挙げています。さらに、非効果的なクラウドのアクセス管理がクラウドアプリケーションのセキュリティ問題につながることを指摘（APAC: 50%、日本:39%）しています。

タレスのデータ保護ソリューション担当 APAC 地域バイスプレジデントであるラナ・グプタ（Rana Gupta）は、「無類な時代となった今、従業員や顧客、パートナー企業への支援を必要とする組織において、アクセス管理の必要性が以前よりも高まっています。複雑性と事業規模がともに増大している環境下であっても、自社オフィス外からのリモートアクセスの安全性の確保が、最重要事項になっています。サイバーセキュリティの必要性が、経営会議でも議論されるべき課題であることを認識すべきです。また現在の状況は、導入決定者や管理者といった IT リーダーにデジタルトランスフォーメーション（DX）計画だけでなく、堅牢なクラウド環境を迅速に構築する機会にもなります。」と述べています。

経営陣がサイバー攻撃を問題視

状況変化に対応する中、企業では徐々にセキュリティファーストのアプローチを重要視するという意識変化が起こっています。APAC 地域の IT 意思決定者は、経営陣に対して IT セキュリティの必要性を訴えやすくなったと感じています。IT 意思決定者の半数以上（APAC:55%、日本:51%）が以前に比べて理解を得やすくなったと回答し、昨年の結果（APAC: 34%、日本:38%）から大きく上昇しています。企業は自社の安全性を維持しながら、リモートワークの従業員が何処からでも効率的に仕事ができるようにする方法を模索中ではありますが、アクセス管理は今後ますます重要な役割を担うようになると考えられます。本調査では、特定のデータへのアクセス制御がコンプライアンス遵守に貢献する（APAC:99%、日本:100%）と回答しています。

セキュリティ意識の向上という点から、APAC 地域ではセキュリティやアクセス管理に関する従業員トレーニングを実施している企業は約半数（APAC:53%、日本:50%）という結果になり、2 年前（APAC:49%日本:37%）よりも明らかな増加を示しています。同様に、アクセス管理への支出（APAC:47%、日本:40%）も、2 年前（APAC:45%、日本:33%）よりも上昇しています。さらに、専任の CISO を設置する割合が 2 年前（APAC:41%、日本:32%）から増加し、今回の結果（APAC:47%、日本:42%）となっています。しかしながら、シャドーIT のような問題が内在（APAC:75%、日本:67%）しているにも関わらず、ユーザー名とパスワードによる認証の拡大を予定しているなど、依然として課題は山積していると言えます。

グプタはさらに、「企業はコロナ禍における事業継続の方法を模索しています。認証情報の乗っ取りに関連する脅威がサイバー攻撃の拡大を助長させる中、多くの人がリモートワークを強いられているため、セキュリティリスクが高まることは避けられません。多数のユーザーがリモートロケーションから、各システムへのアクセスが必要となるため、多岐にわたるクラウドプラットフォームの導入拡大が、セキュリティへの懸念を作り出すことは必然です。今まさに必要とされていることは、アクセスポリシーの強化以外にも、多要素認証によってセキュリティレベルを向上できるスマートアクセス管理ツールに投資することです。パスワードなどの欠点が内在するシステム利用を拡大することは、問題をさらに深刻化させます」と結論付けています。

(1)「タレス アクセス管理インデックス 2020 APAC 版」: IT およびデータ・セキュリティに関して責任や影響力を持つ APAC5 カ国・地域（オーストラリア、香港、インド、日本、シンガポール）の IT 意思決定者 500 名を対象とした調査です。本調査結果および分析は、タレスが **Vanson Bourne** に業務委託によって実施したものです。

タレスについて

タレス（本社：フランス・パリ、Euronext Paris: HO）は、コネクティビティ、ビックデータ、人工知能、サイバーセキュリティ、量子コンピューティングといったデジタルやディープテックのイノベーションに注力

するテクノロジーのグローバルリーダーとして、社会の発展に向けた基盤形成により、誰もが信頼できる未来の構築を目指しています。
意思決定者への支援に注力するタレスは、防衛、航空、宇宙、陸上交通、デジタルアイデンティティ&セキュリティ市場向け製品・サービスを提供すると共に、企業・団体・政府機関などあらゆる組織の重要性が高い業務遂行に貢献しています。
68 カ国に 8 万 3000 人の従業員を擁するタレスの 2019 年度売上高は、190 億ユーロを記録しています（ジェムアルトの 12 カ月間分を含む）。

https://cpl.thalesgroup.com/about-us/newsroom/news-releases/asia-pacific-organisations-implement-access-management-to-protect-cloud-threats

PRESS CONTACT

Thales Japan PR 事務局（プラップジャパン）
担当： 松本／沖山
Tel： 03-4580-9134
Email： Thales@prap.co.jp

タレスについて、下記もご覧ください

タレスグループ
セキュリティ

@Thalesgroup