2024 年 4 月 3 日

サイバートラスト株式会社

代表取締役社長 北村 裕司

東証グロース：4498

端末認証サービス「サイバートラスト デバイス ID」がキヤノン ITS の クラウド型統合 ID 管理サービスと連携

～ ID 管理やシングルサインオンなどの一元管理を可能にする IDaaS「ID Entrance」で 厳格な端末のアクセス制御を実現 ～

サイバートラスト株式会社（本社：東京都港区、代表取締役社長：北村 裕司　以下、サイバートラスト）は、端末認証サービス「サイバートラスト デバイス ID（以下、デバイス ID）」とキヤノンマーケティングジャパングループのキヤノン IT ソリューションズ株式会社（本社：東京都港区、代表取締役社長：金澤 明　以下、キヤノン ITS）が 2023 年 12 月より提供しているクラウド型統合 ID 管理サービス（IDaaS）「ID Entrance（アイディ エントランス）」が連携したことを発表します。

「ID Entrance」は、IT インフラサービスである「SOLTAGE」サービスの一つで、ID 管理、シングルサインオンやアクセス制御などの一元管理が可能であり、「ID Entrance」のクライアント証明書発行オプションを利用して、デバイス ID と連携します。この連携により、端末固有情報に紐づけてクライアント証明書の発行が可能となり、管理者が許可した端末だけにインストールできるため、厳格な端末のアクセス制御と多要素認証を可能にします。セキュリティリスクに対するリソースが十分に確保できない組織、団体や中堅中小企業に向けて、テレワークなどでのクラウドサービスの活用において、組織が許可した端末からのみ情報資産や機密情報へのアクセスを可能とすることで、ガバナンス強化と外部への情報漏えい対策を実現します。

＜背景＞

昨今では、デジタル ID の増加に伴って ID ベースのサイバー攻撃である「アイデンティティベース攻撃（ID ベース攻撃）」[※1] による脅威が増加しています。Identity Defined Security Alliance（IDSA）が公表する「2023 Trends in Securing Digital Identities」[※2] によると、実際に組織が受けた攻撃の中で最も多かったのは「フィッシング（Phishing）」が 62%で、2 位の「クレデンシャルスタッフィング（Credential Stuffing）」[※3] などを含む「ブルートフォース攻撃（総当たり攻撃）」[※4] が 31%を占め

ています。フィッシング攻撃の経路としては、「メールによるフィッシング」が 93%と最も多く、アカウント情報が攻撃者によって乗っ取られることで、機密情報などが外部に漏えいする危険性があります。 この増加する ID ベース攻撃の対策としては、証明書ベースによる多要素認証が有効です。また、クラウドサービスの利用率が高まるとともに、ID/パスワードの認証情報の漏えいやパスワードの使い回しによる不正アクセスが急増するなか、総務省の「テレワークセキュリティガイドライン」[※5] では、「テレワーク勤務者からの社内システムにアクセスするための利用者認証について、多要素認証方式を用いたり、電子証明書を併用したりするなどの技術的基準を明確に定め、適正に管理・運用する必要がある」と推奨されています。

デバイス ID と連携した「ID Entrance」ならびにクライアント証明書発行オプションは、キヤノン ITS より購入いただけます。

今後、サイバートラストとキヤノン ITS は、両社サービスの連携をさらに強化することにより、幅広いお客様のニーズに応え、安心・安全なサービス利用環境の構築を推進します。

サイバートラスト デバイス ID について

「サイバートラスト デバイス ID」 は、端末識別情報を確認し、管理者が許可した端末にのみデバイス証明書を登録することによって、厳格な端末認証を可能にするデバイス証明書発行管理サービスです。Windows デバイス、iPhone、iPad、Android 搭載端末や Chromebook などの幅広い端末に対応しています。管理者が発行申請したデバイス証明書を該当端末に確実に配付し、デバイス証明書を登録した端末のみを接続先のネットワークにアクセス可能にすることで、不正アクセスを防ぎ安全なサービス利用環境を構築できます。
「サイバートラスト デバイス ID」についての詳細は、こちらをご参照ください。
https://www.cybertrust.co.jp/deviceid/

ID Entrance について

「ID Entrance」は、 各種クラウドサービスへのログインに使用している ID/パスワードなどの情報を統合管理し、シングルサインオン機能により、複数のアプリケーションやサービスを、1 つの ID/パスワードで利用できるサービスです。また、多要素認証や認証ポリシー機能も備えた認証・認可機能をクラウド上で提供します。
クラウド型統合 ID 管理サービス「ID Entrance」についての詳細は、こちらをご参照ください。
https://www.canon-its.co.jp/products/identrance/

※1 アイデンティティベース攻撃（ID ベース攻撃）とは：攻撃者が何らかの方法で入手した、サービスやシステムの ID とパスワードを利用し、企業や組織の Web サイトへの不正アクセスを試みる攻撃方法で、代表的な例として ID ベースのフィッシング攻撃やクレデンシャルスタッフィングが挙げられます。
※2 2023 Trends in Securing Digital Identities
https://www.idsalliance.org/white-paper/2023-trends-in-securing-digital-identities/
※3 クレデンシャルスタッフィングとは：攻撃者が盗んだアカウント情報で Web サービスなどのシステムのユーザーアカウントへの不正アクセスを試みるサイバー攻撃の一種です。
※4 ブルートフォース攻撃とは：暗号解読方法の一つで、ID/パスワードの組み合わせを総当たりで試みるサイバー攻撃の一種です。
※5 総務省「テレワークセキュリティガイドライン 第 5 版」
https://www.soumu.go.jp/main_content/000752925.pdf

- **キヤノン IT ソリューションズ株式会社について**

キヤノン ITS は、キヤノン MJ グループの中期経営計画で掲げている ITS 事業拡大を主導する会社として、システムインテグレーションモデル・サービス提供モデル・ビジネス共創モデルの拡大に向けた取り組みを推進しています。 IT インフラに関するすべての領域に対応するサービス「SOLTAGE」ブランドのもと、クラウドセキュリティ領域をはじめとするサービスラインアップの拡充に継続して取り組むとともに、今後もセキュリティ対策や情報漏えい対策に課題を抱えるお客さまをワンストップで支援する体制を強化してまいります。

- **サイバートラスト株式会社について**

サイバートラストは、日本初の商用電子認証局として 25 年以上にわたり提供している認証・セキュリティサービスと、ミラクル・リナックスのカーネル技術やオープンソースソフトウェア（OSS）の知見を応用したオンプレミス、クラウド、組込み領域向けの Linux/OSS サービスを展開しています。また、これらの技術や実績を組み合わせ、IoT をはじめとする先端分野に向けて、「ヒト・モノ・コト」の正しさを証明し、お客様のサービスの信頼性を支えるサービスを推進しています。
「すべてのヒト、モノ、コトに信頼を」。サイバートラストは、IT インフラに関わる専門性・中立性の高い技術で、安心・安全な社会を実現します。

当リリースに関するお問い合わせ先
サイバートラスト株式会社
メール：IR 担当(ir@cybertrust.co.jp)、広報担当（ press@cybertrust.co.jp ）