News Release

2022 年 10 月 13 日
SCSK株式会社

SCSK、Beyond Identity とアジア初の戦略的パートナーシップを締結
～ゼロトラスト時代に向けた先進的なユーザー認証を実現～

SCSK株式会社（本社：東京都江東区、代表取締役　執行役員　社長　最高執行責任者：當麻　隆昭、以下　SCSK）は Beyond Identity Inc.（以下　Beyond Identity 社）と、アジア初の戦略的パートナーシップを締結し、ゼロトラスト認証ソリューション「Beyond Identity」（ビヨンド　アイデンティティ）の販売を開始します。
「Beyond Identity」は、ランサムウェアやアカウント乗っ取りなど、急速に拡大するサイバー攻撃を阻止するために設計された、先進的な多要素認証ソリューションです。SCSK は、今回のパートナーシップ締結により、SSO（シングルサインオン）[1]や IDaaS[2]などの認証基盤を利用しているユーザーに、より高度な認証ソリューションを提供し、2026 年度に 10 億円の販売を目指します。

1. 背景
セキュリティインシデントの 70%以上[3]が、盗まれたパスワードや推測されたパスワードを使用してコンピューターにアクセスすることから始まっています。攻撃者がアクセスに成功すると、ランサムウェア攻撃や、データの不正取得等を行います。従来、パスワードの盗難から始まる攻撃を防ぐための方法は、多要素認証（MFA）[4]を実装することでしたが、攻撃者の手法も巧妙化しており、より強固な認証プロセスが求められています。

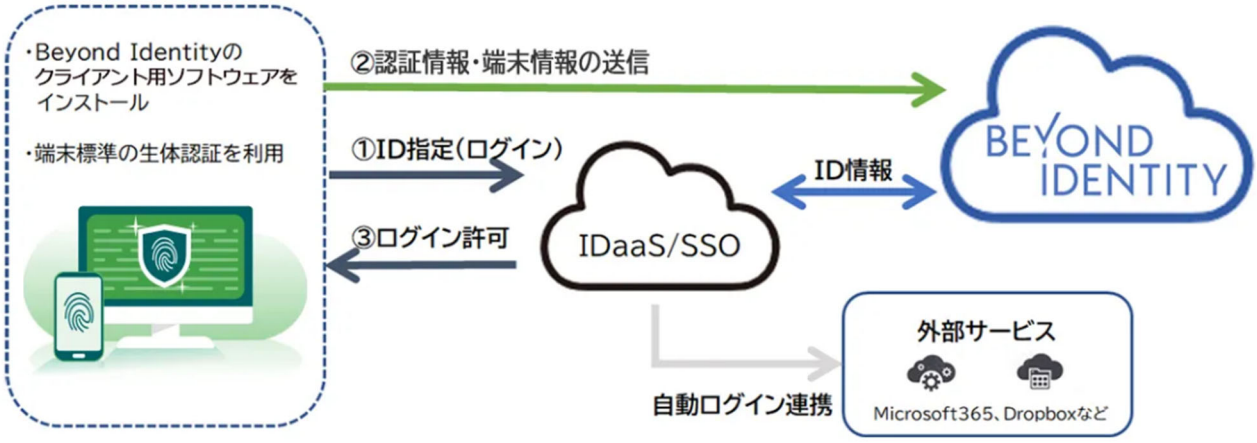
2. Beyond Identityの特徴
「Beyond Identity」は、クラウドベースの認証サービスとクライアント用ソフトウェアの組み合わせで提供します。以下 3 点のアプローチにより、認証されたユーザーとセキュリティポリシーを満たすデバイスのみに重要なシステムやデータへのアクセスを許可します。

① パスワードレス認証によるセキュアな認証
パスワードによる認証を、ユーザーデバイスに内蔵されている生体認証と公開鍵暗号方式に置き換え、より安全な認証を提供します。

② クライアント用ソフトウェアによる端末情報の収集と精査
クライアント用ソフトウェアは、ユーザーデバイスにおけるファイアウォールの有無や暗号化設定、実行されているアプリケーションやファイルの有無、プロセスの存在など、様々なデバイス情報を収集し、認証の条件に加えることができます。Windows、MacOS、iOS、Android、Linux など、主要なプラットフォームで利用可能です。

③ 他のセキュリティソリューションとの連携
MDM[5]や EDR[6]などの端末管理ソリューションと連携することで、それらの情報を活用した、より高度な認証への拡張が可能です。

<Beyond Identity 利用イメージ図>



3.Beyond Identity 社からのエンドースメント

Beyond Identity 社の戦略・事業開発担当副社長である Kurt Johnson は、「SCSK と協業できることを大変うれしく思います。SCSK は、日本における高度なサイバーセキュリティ技術の導入で非常に高い評価を得ており、アジアで初のパートナーシップとなる今回の提携も大きな成功を収めるものと確信しています。」と述べています。

4.Beyond Identity社について

Beyond Identity 社は、Silicon Graphics や Netscape などを設立した伝説的なシリコンバレーのパイオニアである Jim Clark によって設立されました。Netscape では、初の商用ブラウザを導入しただけでなく、SSL[7]を開発した会社を率いました。Beyond Identity は、何十億ドルものオンラインビジネスの取引に日々使用されている SSL と同じコアテクノロジー(公開鍵暗号方式と証明書)を使用しています。Jim は、Silicon Graphics 社で共に働き、その後、Home Network の CEO としてブロードバンド通信の普及に貢献した TJ Jermoluk を Beyond Identity 社の CEO として迎えました。

本件に関するお問い合わせ先

【製品・サービスに関するお問い合わせ先】
SCSK株式会社　プラットフォーム事業グループ
IT プロダクト＆サービス事業本部
セキュリティプロダクト部　　栗井
TEL:03-5859-3037
E-mail:　beyondidentity-info@ml.scsk.jp

【報道関係お問い合わせ先】
SCSK株式会社
企画本部　広報部　井上
TEL:03-5166-1150

[1] 一度システムのユーザー認証を行うと、他のシステムを利用する際にも毎回認証を行う必要がないという仕組み。

[2] 複数のサービスの ID・パスワードをクラウド上で一元的に管理するソリューション。

[3] セキュリティインシデントの発端のなかで、50%が資格情報の奪取、20%がフィッシング攻撃といわれている。
https://www.beyondidentity.com/blog/what-know-2022-verizon-data-breach-investigations-report-dbir

[4] 以下 3 種類の情報のうち 2 つ以上を組み合わせて認証を行う方法。
① 知識情報(例:ID・パスワード)
② 所持情報(例:YubiKey 等のセキュリティキー)
③ 生体情報(例:指紋・顔・静脈)

[5] 「Mobile Device Management(モバイルデバイス管理)」の略。モバイル端末を一元的に監視、管理するためのサービス。

[6] Endpoint Detection and Response」の略。端末の状態を把握して問題発生時に迅速な対応を行う。

[7] セキュア・ソケット・レイヤー、今日では TLS またはトランスポート・レイヤー・セキュリティとして知られている。
インターネット上でやりとりされるデータの「盗聴」「改ざん」「なりすまし」を防止するための暗号化プロトコル。