MKI 三井情報

セキュリティソリューション

フィッシング耐性のある多要素認証ソリューション

Beyond Identity

Beyond Identityが求められる背景

認証をめぐるセキュリティリスク

企業のデータ漏洩の大多数は
ID・パスワードを狙った認証
ベース攻撃やソーシャルエンジ
ニアリングが原因といわれます。

認証情報が、企業全体の
セキュリティ強化に
直結します。

多要素認証（MFA）があればセキュリティは万全か？

従来の認証は IDとパスワード に依存していました。しかし、パスワードは使い回しや漏えい、推測のしやすさなど多くのリスクを抱えています。
そこで複数の認証を組み合わせた多要素認証（MFA: Multi-Factor Authentication） による認証強化が図られています。

知識情報
（パスワードなど）

所持情報
（端末やICカード）

生体情報
（指紋や顔認証）

従来のMFAでは様々な課題が残る

従来のMFA	問題
ショートメッセージ／メールコード	フィッシング・傍受リスク
プッシュ通知	誤承認（無意識タップ）の可能性
2つ目のデバイスが必要	手間・煩雑・業務効率低下
パスワード＋追加要素	結局パスワードに依存 → 根本解決にならない

Beyond Identityとは？

Beyond IdentityはFIDO2/WebAuthn準拠の公開鍵暗号方式を用いたパスキーという認証技術を採用しています。
非常にセキュアな認証であるFIDO2認証に準拠してSSOやMFAの導入が出来るソリューションです。

ポイント パスキーを使った多要素認証で高度なフィッシングも防ぐ

ポイント パスワード入力が不要となり、パスワードの使い回しや盗難リスクを排除

ポイント デバイスポスチャによる端末レベルのセキュリティも提供

最新のサイバー脅威からBeyond Identityで守る

高度化するフィッシング攻撃への対策はできていますか？

■対策が求められる理由

フィッシング被害は年々増えており、特にMicrosoft365のログイン情報を狙う「AitM（Adversary in the middle）」攻撃が問題になっています。この攻撃はセッションCookieを盗む手口です。

■影響

AitM攻撃は認証後のデータ（セッションCookie）を盗みます。そのため、SSOやMFAだけでは防ぐことができません。

■Beyond Identityでの対策

Beyond Identityは公開鍵暗号方式のパスキーを使い、ユーザーのデバイスで署名された安全なデータだけをやりとりします。これにより、攻撃者がCookieを盗むことができず、安全に認証できます。

MKI 三井情報
www.mki.co.jp
〒105-6215 東京都港区愛宕2-5-1 愛宕グリーンヒルズMORIタワー

【本製品サービスに関するお問い合わせ先】
共創営業本部マーケット推進部
E-mail： beyond-id-dg@mki.co.jp

20201130_1 MKI