



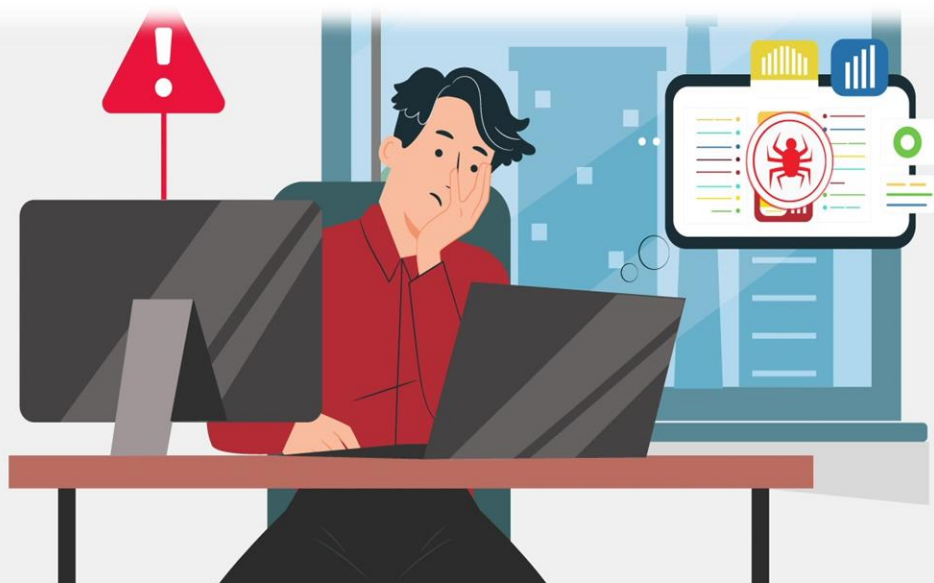
Unified Identity Platform

Securing the most secure.

安全なIDセキュリティをさらにプラス

突然ですが質問です！

次の5つの質問の答えが気になる方は、ぜひ次のページをご覧ください



パスワードのセキュリティリスクを知っていますか？

ID認証はパスワード以外にもあることを知っていますか？

退職者のアカウントがそのままになっていませんか？

クラウドサービスを複数利用していますか？

ゼロトラストの対策はできていますか？

セキュリティを第一に考えたIDaaS ソリューション

パスワードのセキュリティリスクを知っていますか？

現状

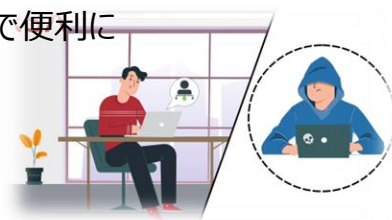
- パスワードは狙われやすく、フィッシングなど大きなリスクを伴います。
- 攻撃者の不正アクセスの実に50%以上の原因は「認証情報の窃取または侵害」と報告されています。*1
- 複雑なパスワードを覚えることはユーザーにとって大きな負担であり、パスワード忘れて生産性の低下も懸念されています。
- 最近では定期的にパスワードを変更してもAIで解析される可能性があり、むしろ定期的な変更をすることで、パスワードの作り方がパターン化し簡単なものになることや、使い回しをするようになることの方が問題となります。流出時に速やかに変更する旨が示されています。*2

RSAでは

パスワードだけではなく、ID PlusのMFA（多要素認証）でより安全で便利にパスワードレスとして企業向けパスキーで対応 FIDO対応

*1：2023のVerizon DBIRレポート

*2：NIST SP800-63B（電子的認証に関するガイドライン）



ID認証はパスワード以外にもあることを知っていますか？

現状

- パスワード（「知識」）だけでなく、「所持」「生体」といった認証方式があります。
- 複数を組み合わせた、多要素認証（MFA）でより安全な認証をすることができ、PCI-DSSなど様々なルールで、多要素認証の利用が必須になっています。

RSAでは

スマートフォン以外にもハードウェアトークンを活用

QRコードや生体情報でも認証可能となり、安全でかつ利便性も向上



退職者のアカウントがそのままになっていませんか？

現状

- 人材市場の流動化が進み、中途採用が活性化しています。
- IDの作成、退職による削除といったIDの管理を適切に行うことが重要です。
- 削除されていない退職者のアカウントが悪用されることがあります。

RSAでは

ガバナンス＆ライフサイクルでID管理を適切に実施

また入退社だけでなく、異動などによるアクセス権の変更も可能



クラウドサービスを複数利用していますか？

現状

- 利用するクラウドサービスが増えてくると、その都度ログイン・アクセスのアカウントを管理しないといけません。
- しかしID・パスワードを使いまわしや、使われていないアカウントがなどセキュリティリスクが増えてきます。
- システム障害やネットワーク障害などでクラウドサービスが利用できないときに業務継続が難しくなることがあります。

RSAなら

シングル・サインオン（SSO）で、リスクを軽減して利便性を向上
オンプレミスと併用してフェイルオーバー対策をすることで業務の継続が可能



ゼロトラストの対策はできていますか？

現状

- ゼロトラストセキュリティと言われて久しいですが、なかなかできていないのが現実です。
- クラウドやモバイルの活用、働き方の多様性に合わせて、境界型セキュリティからゼロトラストセキュリティへの移行における情報資産アクセスのリスク対策が必要です。
- 認証を無条件を信頼せず、アクセスの信頼性を都度適切にチェックするリスクベースによる判定や、必要最小限にアクセスする権限を付与して資産を保護することが大切です。



RSAなら

多要素認証（MFA）とRisk AIでアクセスの状況に合わせて本人確認を取ることで安全性を高めます。



Mobile Lockでスマホも
安全に ID認証を保護
QRコード、生体認証、
OTPでも認証可能



iShield Key2シリーズ
デバイスバウンドパスキー
でキーを共有しない
シンクドパスキーも対応



DS100でFIDO2に対応
OTPにも対応しており、ス
マホでの認証が使えな
い環境でも利用可能

ID Plus 4つのラインナップで

- C1: 安価で使いやすいクラウドSSO専用エントリーライセンス
E1: オンプレミスとクラウドをMFAで統合するスタンダードライセンス
E2: あらゆる環境のシステムとネットワークのIDをセキュアに統合するプレミアムライセンス
E3: ID Plusのすべての機能を提供するハイエンドライセンス

機能 プラン	C1	E1	E2	E3
環境	クラウドのみ	クラウド・オンプレ・ハイブリッド	クラウド・オンプレ・ハイブリッド	クラウド・オンプレ・ハイブリッド
多要素認証 (MFA)	クラウドのみ	ハイブリッド	ハイブリッド+SDK	ハイブリッド+SDK
シングル・サインオン (SSO)	ベーシック (10アプリケーションまで)	-	エンハンスト (無制限)	エンハンスト (無制限)
Contextual Access	Static	Static	Static + Adaptive	Static + Adaptive + リスクベース
インテグレーション	Web Standards	Web+Agents/RADIUS	Web+Agents/RADIUS	All Integrations
ワークフロー	Standard	Standard	Advanced	Advanced
ディレクトリ	クラウドのみ	Cloud/On-Prem	Cloud/On-Prem/Custom	Cloud/On-Prem/Custom
Mobile Lock	オプション	オプション	オプション	標準搭載

- 多様なワークスタイルを支援するMFA (多要素認証)
- クラウドからオンプレミスまで多数のシステムやアプリケーションと柔軟に連携 (RSA Ready)
- ハイブリッド構成によりクラウド認証サービス停止時でも認証を継続させることで高可用性を実現 (フェイルオーバー)
- セキュリティ向上とユーザ利便性の両立を実現するリスクベース認証

RSAが選ばれる理由

暗号化鍵をサードパーティに委ねない企業向けのパスキー

- パスワードを利用しない新たなID認証で安全で便利に
- FIDOアライアンスのボードメンバーとして業界をリード

ゼロトラスト対策はID認証から

- 多様な働き方に安全に柔軟に対応
- 豊富な実績でゼロトラストの実現

MFA (多要素認証) の導入実績多数

- ワンタイムパスワード (OTP) や、生体認証、QRコードなどスマートフォンを使った認証はもちろん、ハードウェアトークンを利用すればスマートフォン持ち込み禁止エリアや通信が利用できないところでも認証可能
- モバイルセキュリティでBYODでも安心

シングルサインオン (SSO) で安全で便利に

- ガバナンス&ライフサイクルで適切かつ効率的に安全にIDを管理

認証ソリューションで40年以上の実績

- 日本国内テナントでクラウドに環境構築
- オンプレミスにも対応でき、ハイブリッドでフェイルオーバー対策が可能に

