Hitachi Solutions Create

HITACHI

認証管理ソリューション「SECUREMATRIX」説明資料

株式会社 日立ソリューションズ・クリエイト

目次

1. はじめに

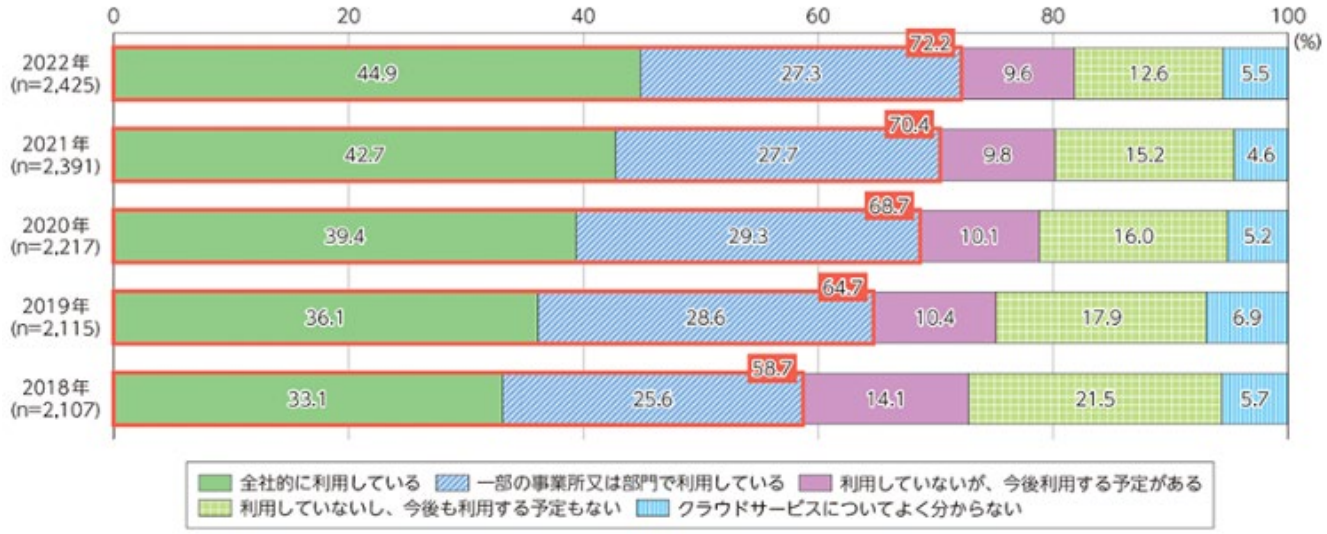
HITACHI

1.1 働き方改革におけるIT活用の課題①

多くの企業でマルチデバイスでの業務が拡大、また、クラウドサービスの利用が増加
しかし、セキュリティ問題から利用サービスは制限される傾向

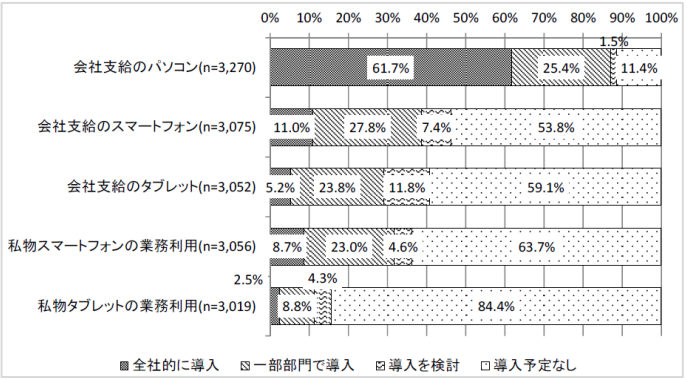
働き方改革やテレワークが推進される中、ITデバイス（端末）は進化を続け、
PCだけでなく、スマートフォンやタブレットを活用し、いつでも、どこでも仕事ができる
ワークスタイルが定着してきました
一方で、不正アクセスや情報漏えいが後を絶たず、外部からのアクセスを大幅に制限した
セキュリティポリシーで運用するなど、IT投資が有効に機能していない状況でもあります

■ クラウドサービスの利用状況



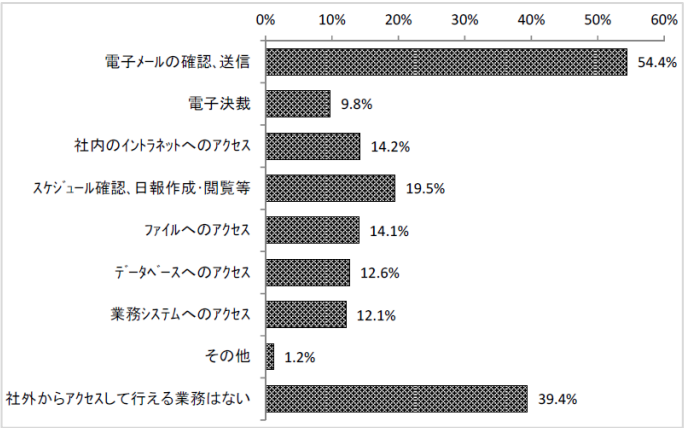
出典:令和5年版 情報通信白書 総務省　2023年

■ 業務へのデバイスの導入状況



出典:2017年3月ICT利活用と社会的課題解決に関する調査研究（総務省）
「情報端末の導入状況」

■ 社外から自社のシステムにアクセスして行える業務の状況
（複数回答）



出典:2017年3月ICT利活用と社会的課題解決に関する調査研究（総務省）
「社外から自社のシステムにアクセスして行える業務」

HITACHI

1.1 働き方改革におけるIT活用の課題②

法令・ガイドラインでも強固なセキュリティ対策が推奨されるように

そんな中、2021年5月31日公表の「テレワークセキュリティガイドライン第5版（総務省）」では、クラウドサービスの活用やゼロトラストセキュリティに関する考え方が示されました
テレワークでの社内システムやクラウドサービス利用時の留意点として、適切な管理ルールの設定、多要素認証など、より強固なアカウント・認証管理が推奨されています

システム・セキュリティ管理者が実施すべき対策	
管理者H-1 基本対策	テレワーク時にアクセスする社内システムやクラウドサービスへのアクセスで必要となる利用者認証機能について、技術的な基準（**多要素認証**方式の利用、**パスワードポリシー**の規定等）を明確に定める。
管理者H-2 基本対策	社内システムやクラウドサービスへのアクセス時の利用者認証機能として、可能な限り**多要素認証を強制**する。
管理者H-3 基本対策	テレワーク端末がオフィスネットワークやクラウドサービスに接続する際は、接続先のサーバの正当性（**サーバ証明書**等）と、接続元のテレワーク端末の正当性（**パスワードやクライアント証明書**）を相互に認証する仕組みを備えたものとする。
管理者H-4 基本対策	テレワーク端末へのログインパスワードや、オフィスネットワークやクラウドサービスにアクセスする際のパスワードは、**強力なパスワードポリシーの適用**を強制する。
管理者H-5 基本対策	テレワーク端末やアプリケーションの初期パスワードが強制的に変更されるか、**十分な強度のある個別のパスワード**が個々に設定されるようにする。
管理者H-6 基本対策	**利用者認証に一定回数失敗した**場合、テレワーク端末の**一定時間ロック**や、テレワーク端末上のデータ消去を行うよう設定する。
管理者H-7 基本対策	異動や担当変更等を適切に把握し、**不要なアカウントの削除やアカウント権限の更新**等を実施する。

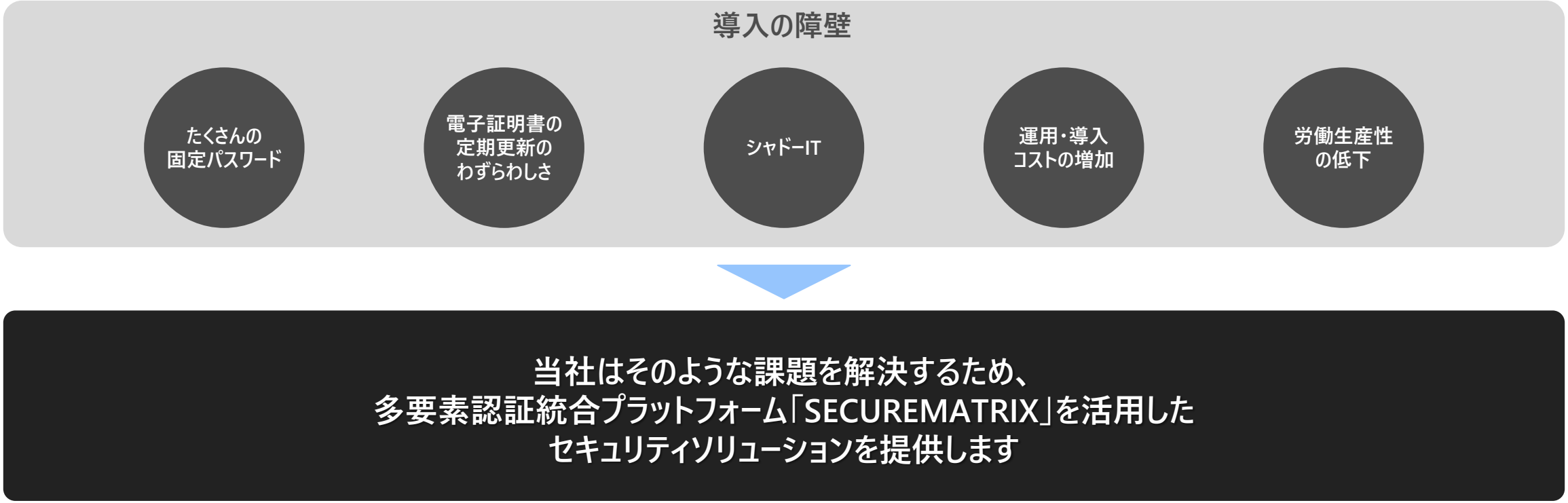
出典：テレワークセキュリティガイドライン 第5版（令和3年5月）　https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

HITACHI

1.2 セキュリティ強化における企業側の課題

セキュリティ強化における企業側の課題

クラウドサービスやWebアプリケーションごとに類推できない複数のID・パスワードの厳重な管理に加えて、会社支給のデバイスと私物デバイス（BYOD）を適切に管理するには限界があります
また、その認証を多要素化すると複数のソリューションの導入が必要となり、運用の手間や導入コストが増え、
さらには労働生産性も落としかねません



2. 認証管理ソリューション

HITACHI

2.1 パスワード時代の終わり

パスワード管理は過去の遺物になろうとしています

パスワードは予測可能になり、強力なパスワードでさえフィッシングされ、乗っ取られてしまいます

事例①　テレワーク

プライベートで利用しているネットショップと同じパスワードをテレワークでも利用しており、ネットショップでパスワードの流出事故が発生、
勤務先にも不正アクセスされてしまった

出典：総務省「テレワークセキュリティガイドライン」　第4版（2018年4月）から

事例②　ネットワークサービス

脆弱な他サービスから取得したID・パスワードによる、パスワードリスト攻撃が発生、約16万件の不正ログイン、およびアカウント情報が流出した
その後、ユーザーには、改めて二段階認証の利用など、セキュリティ対策を依頼

出典：任天堂株式会社ホームページより

**パスワードは漏えいすることを前提に、
ワンタイム化（一度きりの使い捨て）と二要素認証がおすすめです**

HITACHI

2.2 課題

お客さまのシステムにおいて、このようなお悩みはありませんか？

課題	**認証セキュリティを強化したい　効果的な認証セキュリティに向けて、支援してほしい**
解決	まずは、お気軽にご相談ください 導入・運用支援、トレーニングサービスまで、お客さまの状況に合わせて、ソリューションを**ワンストップ**で提供します
課題	**多要素認証システムの運用負荷が大きい**
解決	本ソリューションは、専用のアプリケーションや認証デバイスが不要なため、 **配布管理・故障対応が不要、紛失のリスクも少なく**、運用負荷は最小限です
課題	**テレワーク推進にあたり、私用端末（BYOD）を活用したいが、適切に管理できるか不安**
解決	本ソリューションは、デバイス依存がなく、一つのIDと一つのパスワードで、マルチデバイスからのアクセスを可能にします **私用端末（BYOD）**を活用しやすくなります
課題	**認証は強化したいが、既存のシステムと連携できるか心配**
解決	**クラウド認証連携サーバー**により、利便性を損なうことなく、セキュリティレベルを強固にします

HITACHI

2.3 認証管理ソリューションの特長①

多要素認証で高いセキュリティを実現

多要素認証とは

認証の三要素である「記憶」「所持」「生体」のうち、二つ以上の要素を組み合わせて認証を行う方式です
複数の要素を組み合わせることで、第三者からの不正ログインを防止し、セキュリティを強化できます

認証の三要素

記憶の認証　本人だけが知っている情報による認証

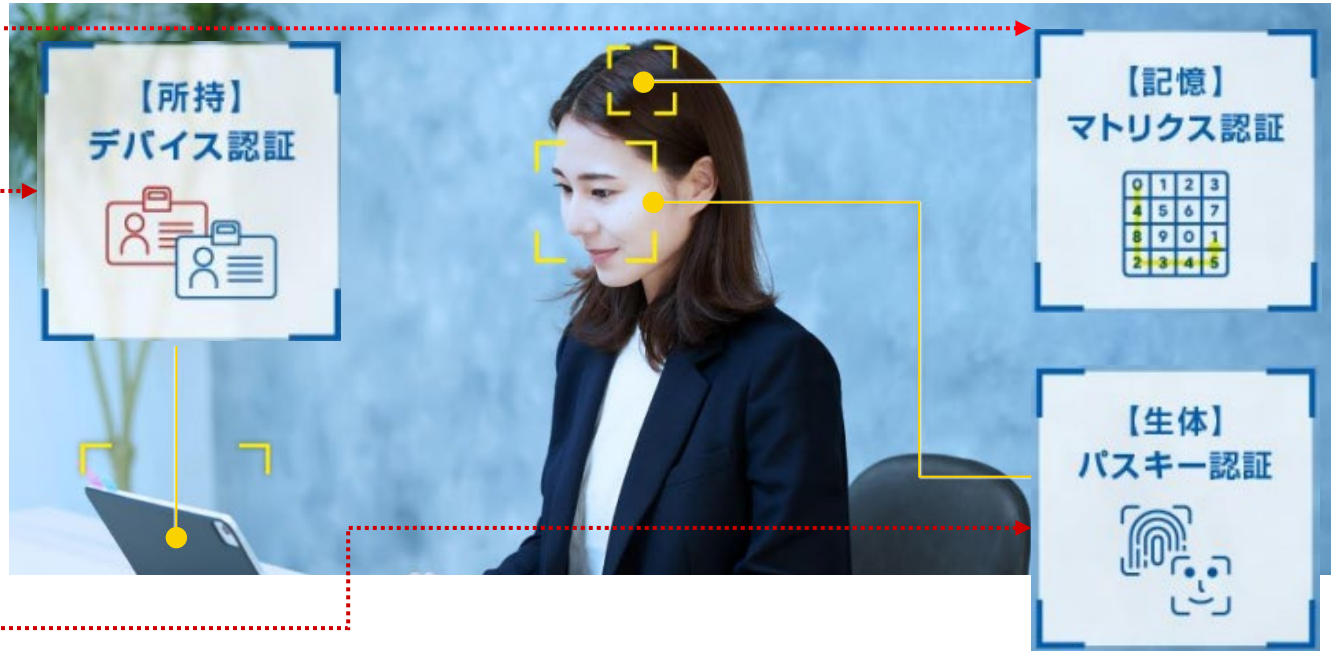
- 固定パスワード、PIN
- ソフトトークン（ワンタイムパスワード）
- **イメージ型ワンタイムパスワード**（マトリクス認証など）

所持の認証　本人だけが持っている情報による認証

- ICカード
- ハードトークン（ワンタイムパスワード）
- デバイス認証（機体番号式）
- デバイス認証（電子証明書）
- **デバイス認証**（ワンタイム証明書）

生体の認証　本人の身体的特徴による認証

- **パスキー認証**（指紋・顔・静脈・網膜）

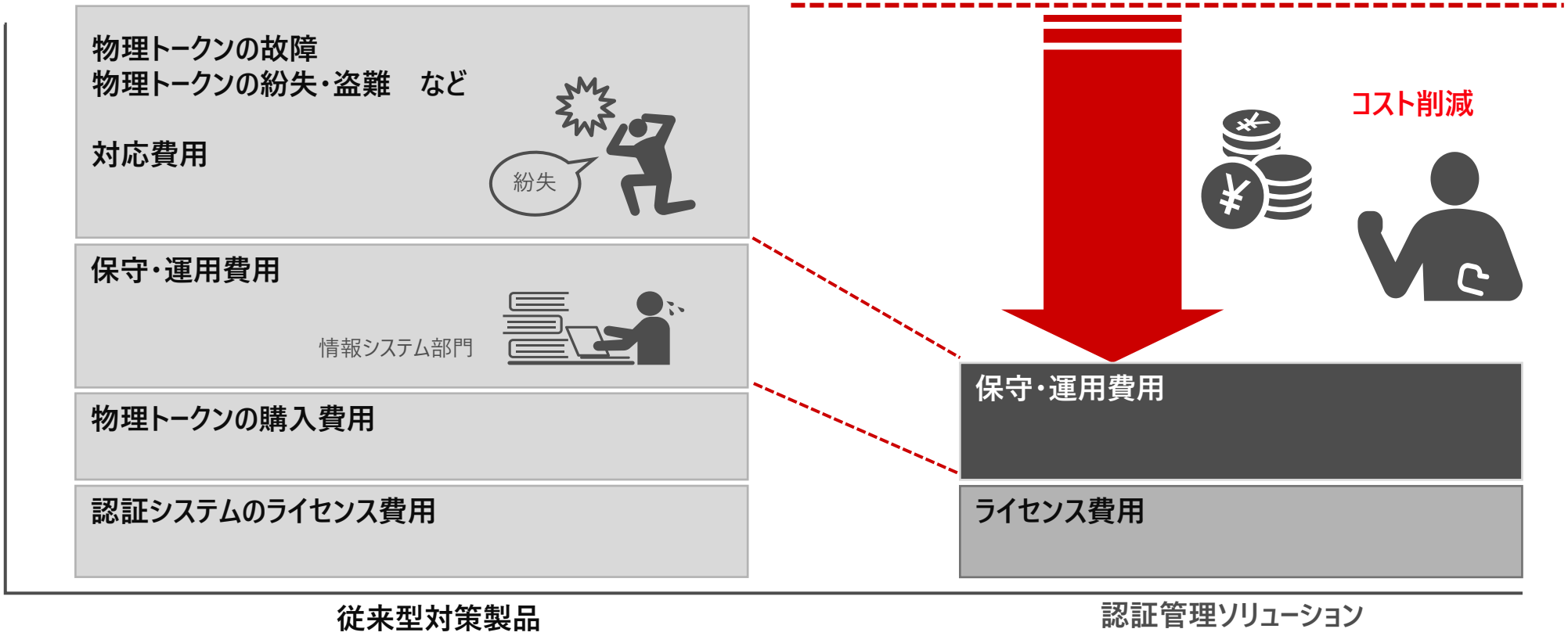


HITACHI

2.3 認証管理ソリューションの特長②

運用負荷を最小限に、認証セキュリティを強化

ブラウザーのみで利用できるため、**物理トークンの配布や故障対応が不要**
紛失のリスクもないため、運用負荷を最小限に抑えられます



HITACHI

2.3 認証管理ソリューションの特長③

多様な認証連携に対応しており、働き方改革の仕組みを支援

主要な連携動作確認済み製品

例に記載のない製品や、お客さま独自のシステムとの連携についてはご相談ください

利用目的	例
クラウドサービスへの認証	対象：クラウドサービス **Microsoft Office 365 , Google Workspace , Salesforce.com**
Webアプリケーションへの認証	対象：各種アプリケーションソフトウェア **Citrix StoreFront ，eセールスマネージャー**
ネットワークへの認証	対象：VPN機器、認証VLAN機器 **Pulse Secure , Cisco ASA , F5 BIG-IP APM , Array AG, FortiGate**
仮想化環境への認証	対象：仮想化基盤 **VMware Horizon , Citrix NetScaler**
Windowsデスクトップへの認証	対象：Microsoft Windows **Windows 10 , Windows 11**

HITACHI

2.4 認証管理ソリューションメニュー

効果的な認証セキュリティ対策をワンストップで提供

認証管理ソリューションは、SECUREMATRIXと、
セキュリティ領域で培ってきた当社の経験とを組み合わせたセキュリティソリューションです

項目	内容
SIサービス	要件定義・ヒアリング
	設計
	構築
	テスト
SE保守サービス	問い合わせ対応
	システム変更対応など
トレーニングサービス	運用者・管理者を対象としたトレーニング

2020年 2 月21日、㈱シー・エス・イー殿主催の「パートナー協創セミナー2020」にて、
「2019年SECUREMATRIXの新規ユーザー獲得実績No.1パートナー」として当社が表彰されました！

豊富な導入実績とノウハウを基に、要件定義から運用まで、
お客さまのニーズに合わせた効果的な認証セキュリティ対策をワンストップで提供します

3. SECUREMATRIXの特長と機能

HITACHI

3.1 SECUREMATRIXが解決できる企業課題

SECUREMATRIXは、貴社のセキュリティ課題を解決し、働き方改革を推進します

たくさんの
固定パスワード

認証は
これ一つでOK！

SECUREMATRIXに認証を集約できるので、ユーザーは一組のIDとパスワードを覚えるだけ
パスワードはワンタイム（使い捨て）のため、認証ごとに使い分けなくても安全です

電子証明書の
定期更新の
わずらわしさ

ワンタイム証明書で更新の手間なし！

通常の証明書は期間に定めがあるため定期更新が必要ですが、ワンタイム（使い捨て）証明書は認証のたびに新たな証明書が発行されるため、更新の必要がありません

シャドーIT

ポリシーの適切化でリスクを防止！

外部からの安全なアクセスを可能にし、適切なセキュリティポリシーと快適な業務環境に整えることで、従業員の管理外IT活用＝シャドーITによるリスクを根本的に防ぎます

運用・導入
コストの増加

低コストで運用・導入を実現！

デバイスレスなので、導入・運用双方のコストが抑えられます
また、ユーザーによるセルフパスワードリセットやデバイス登録機能により、運用管理者のコストも削減できます

労働生産性
の低下

いつでもどこでも社内情報にアクセス！

時間と場所を選ばない安心・安全なワークスペースへのアクセスを実現することで、従業員の労働生産性向上はもちろん、ITデバイスやITリソースの有効活用を最大化します

3.2 SECUREMATRIXとは

いつでも、どこでも、快適＆安全に「働き方改革」を実現できる「認証セキュリティ製品」

“ワークスペース“

自宅でも　電車でも　カフェでも　オフィスでも

マルチデバイス対応

アプリケーション不要
認証デバイス不要

SECUREMATRIX

多要素認証

「記憶」「所持」「生体」の三要素を全て利用した認証や任意の組み合わせでの認証が可能です

1IDで99台まで利用可能

ユーザーはID・パスワードを一つ覚えるだけで複数デバイス・複数サービスの認証をセキュアに行えます
ユーザーによって台数を制限・追加することも可能です

ブラウザーのみで利用可能

デバイス・ソフト配布の必要がない上、PC、シンクライアント、スマートフォンなど利用機器を選びません

“ワークスペース“

クラウド

- Office 365
- Google Workspace
- Salesforce
- その他 SaaS

Web

- グループウエア
- ポータルサイト
- 業務アプリケーション

社内

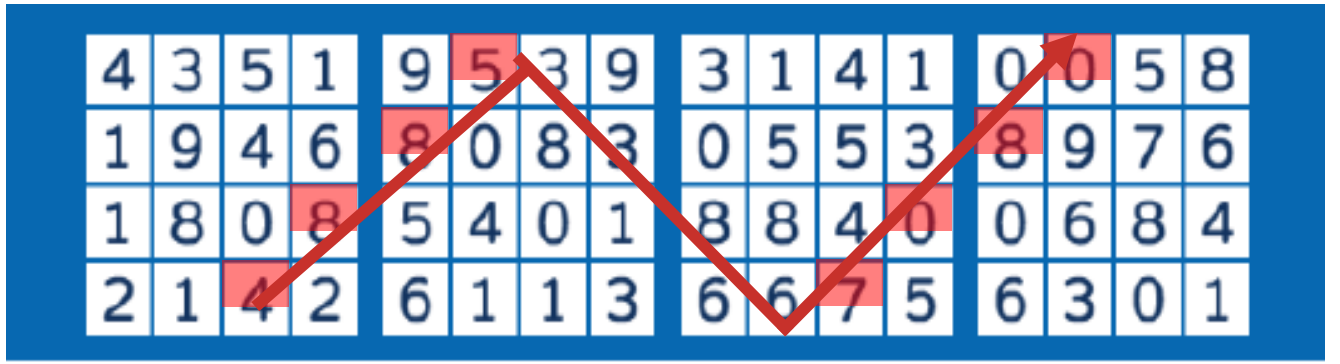
- 社内LAN
- ファイルサーバー
- メールサーバー

HITACHI

3.3 マトリクス認証とは

形で覚えるパスワード

アクセスのたびに異なる数字が表示されるマトリクス表（乱数表）
あらかじめ設定した位置・順番を基に、毎回異なるパスワードを入力するため、覚えやすくて安全です

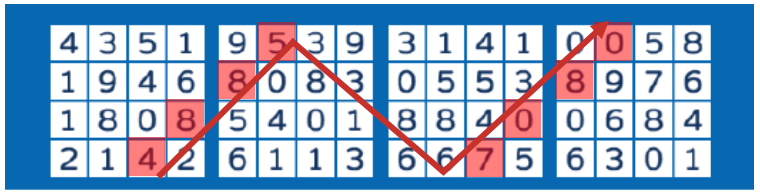


※パスワードは一度きりの使い捨て

■マトリクス表からの入力例

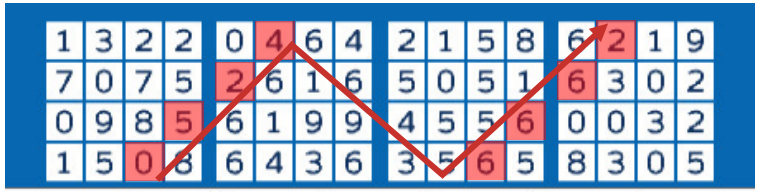
1回目

入力するパスワード：
4 8 8 5 7 0 8 0



2回目

入力するパスワード：
0 5 2 4 6 6 6 2



HITACHI

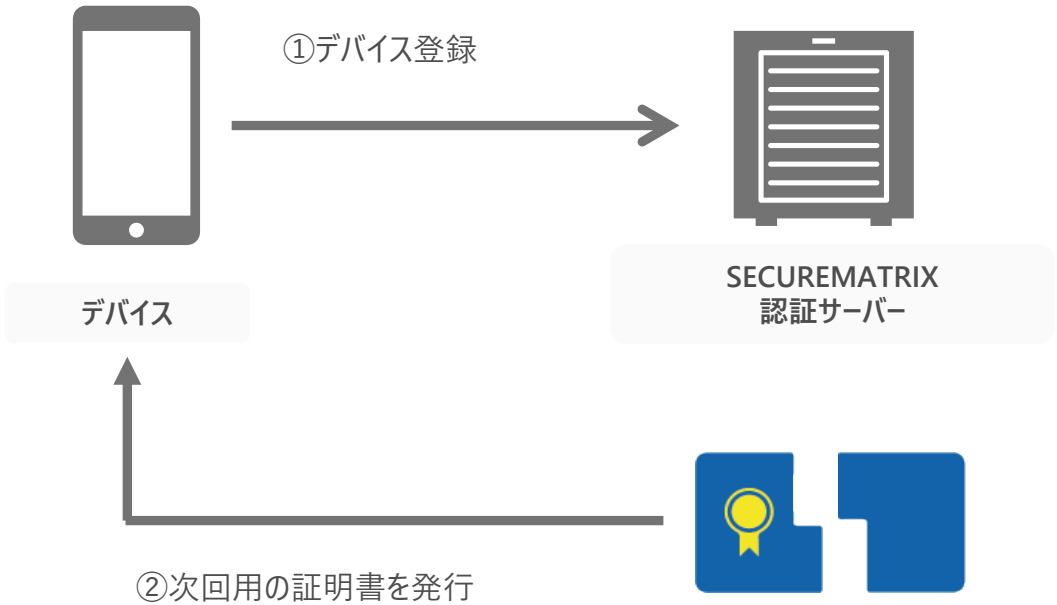
3.4 デバイス認証とは

証明書を毎回生成する独自のワンタイム方式

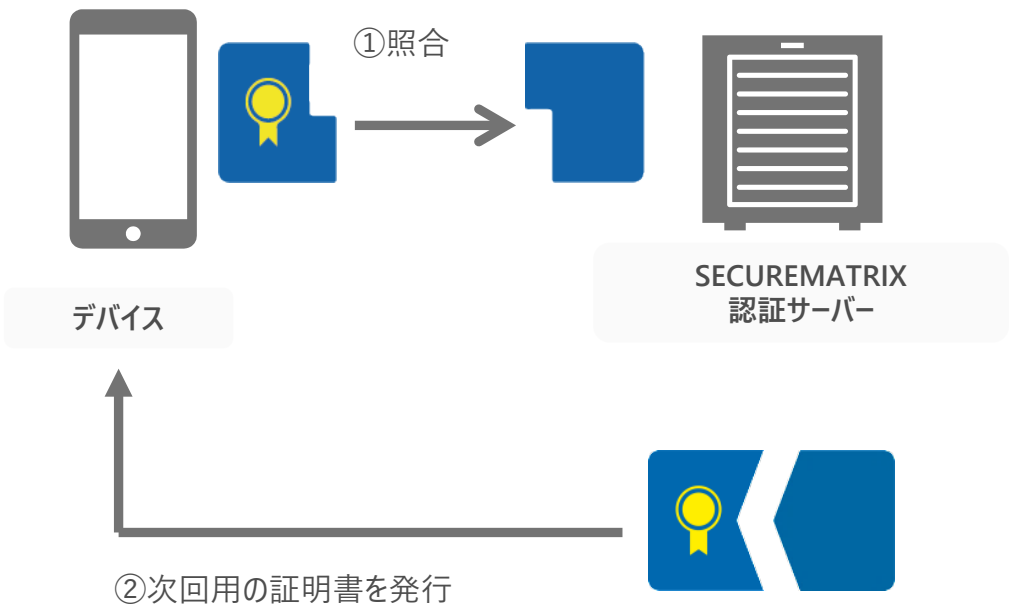
登録時、証明書を分解して、片方をデバイスに配布し、
2回目以降はログインごとに次回認証に利用する証明書を発行します

※証明書は一度きりの使い捨て

1回目（登録時）



2回目以降

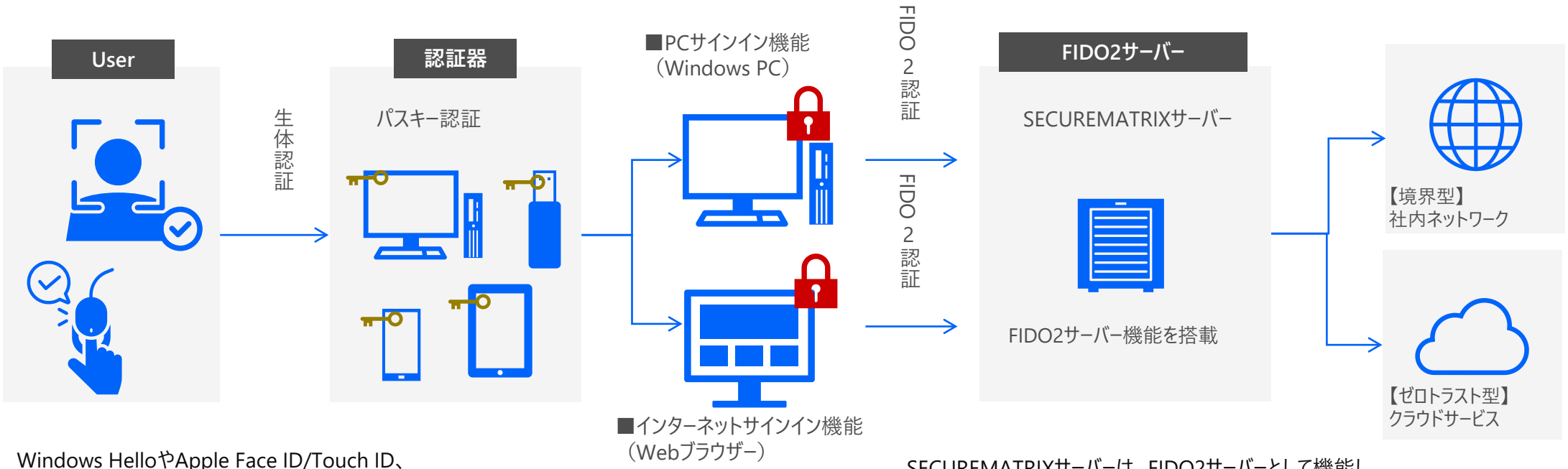


HITACHI

3.5 パスキー認証とは

「パスキー」を利用して「パスワードレス」の生体認証を行います

デバイスに標準装備されているWindows HelloやApple Face ID/Touch ID、
外付型のFIDO2認証器などを利用できます
PCサインイン機能とインターネットサインイン機能の双方で認証強化します



Windows HelloやApple Face ID/Touch ID、
外付型のFIDO2認証器などでパスキーを利用して生体認証を行います

SECUREMATRIXサーバーは、FIDO2サーバーとして機能し、
FIDO2認証を行います

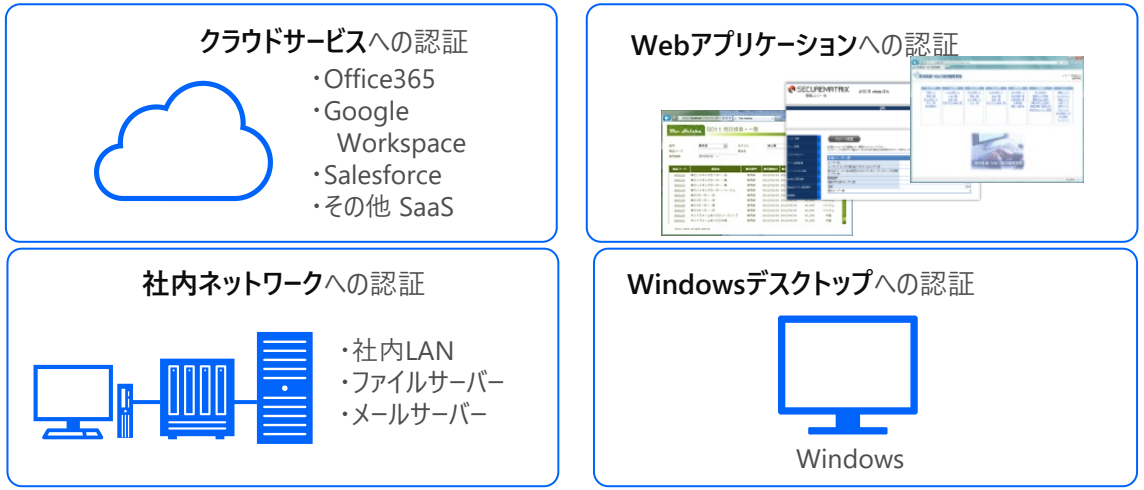
3.6 利用可能デバイス・利用用途

統一されたUI、覚えやすく簡単な操作

PC・タブレット・スマートフォンなど、各種デバイスに対応しています
また、デバイスごとに異なっていた認証画面インターフェースを統一し、
デバイスに依存しない認証インターフェースと操作性を確立
小さなスマートフォンの画面でも同じ操作で認証が可能です

さまざまなアプリケーション・サービスの認証にご利用いただけます

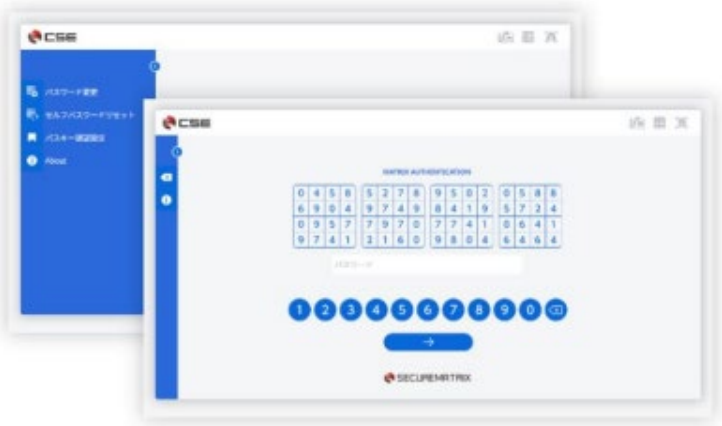
クラウドサービス・Webアプリケーション・ネットワーク・仮想化環境・
Windowsデスクトップなど、さまざまな認証との連携機能を持っています



3.7 ログオンの種類

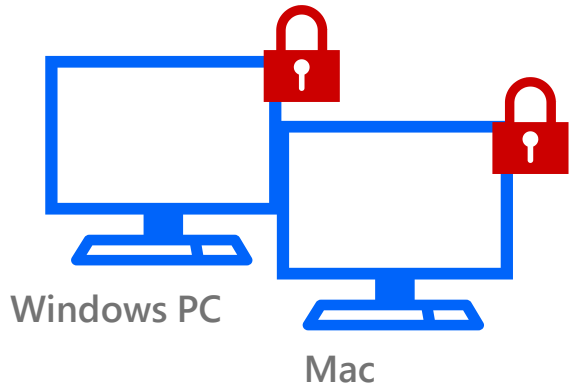
インターネットサインイン機能

（ネットワーク/仮想化環境、Webアプリケーション、クラウドサービスへの認証）



- 社外からのリモートアクセス、Webアプリケーションアクセスの認証を強化
- RADIUSプロトコルが利用可能な機器との連携が可能
- リバースプロキシにより、機密性の高い情報を扱うWebアプリケーションを安全なネットワーク領域で保護が可能
- シングルサインオンにより、マトリクス認証のみでリモートアクセス・Webアプリケーションへのログインが可能
- ユーザーのグループやユーザーの権限に応じた柔軟なアクセスコントロールが可能
- SSL-VPN機器ベンダーなど、さまざまなベンダーとのアライアンスによる豊富な連携実績
- SAML2.0 とマトリクス認証で利便性とセキュリティ強化を両立し、クラウドサービスの展開を促進

PCサインイン機能（Windows PC/Mac）



- Windows PC サインインの認証を強化
- コンピューターロック解除にも適用可能
- Active Directoryとの連携をサポート
- VDI環境へ適用することでシンクライアントからの接続時の認証を強化
- ネットワークがオフライン時にもマトリクス認証を使用してWindowsサインインが可能
- マトリクス/デバイス/パスキー認証を組み合わせた多要素認証によってセキュリティを強化
  ※MacOSはPCサインイン時のパスキー認証に未対応

HITACHI

3.8 他の認証ソリューションとの比較

総務省「テレワークセキュリティガイドライン」に準拠した認証セキュリティ

SECUREMATRIXは、認証の三要素（「記憶の認証」「所持の認証」「生体の認証」）として、
「記憶の認証」の**『イメージ型ワンタイムパスワード（マトリクス認証など）』**、「所持の認証」の**『デバイス認証（ワンタイム証明書）』**、
「生体の認証」の**『パスキー認証（指紋・顔・静脈・網膜）』**を採用しました

三要素	認証要素	マルチデバイスに対応	利便性 専用機器やソフトが不要	セキュリティ強度	漏えい紛失 盗難リスク	インストールや配布の手順	低コスト
記憶の認証	固定パスワード、PIN	○	○	×	×	○	○
	ソフトトークン（ワンタイムパスワード）	△	×	○	○	△	△
	イメージ型ワンタイムパスワード（マトリクス認証など）	○	○	○	○	○	△
所持の認証	ICカード	×	×	○	×	×	×
	ハードトークン（ワンタイムパスワード）	○	○	○	×	×	×
	デバイス認証（機体番号式）	△	○	△	×	×	○
	デバイス認証（電子証明書）	△	○	○	×	×	×
	デバイス認証（ワンタイム証明書）	○	○	○	○	○	△
生体の認証	パスキー認証（指紋認証）	×	×	○	○	○	×
	パスキー認証（顔認証）	×	×	○	○	○	×
	パスキー認証（静脈・網膜認証）	×	×	○	○	○	×

3.9 SECUREMATRIX非導入の場合との比較

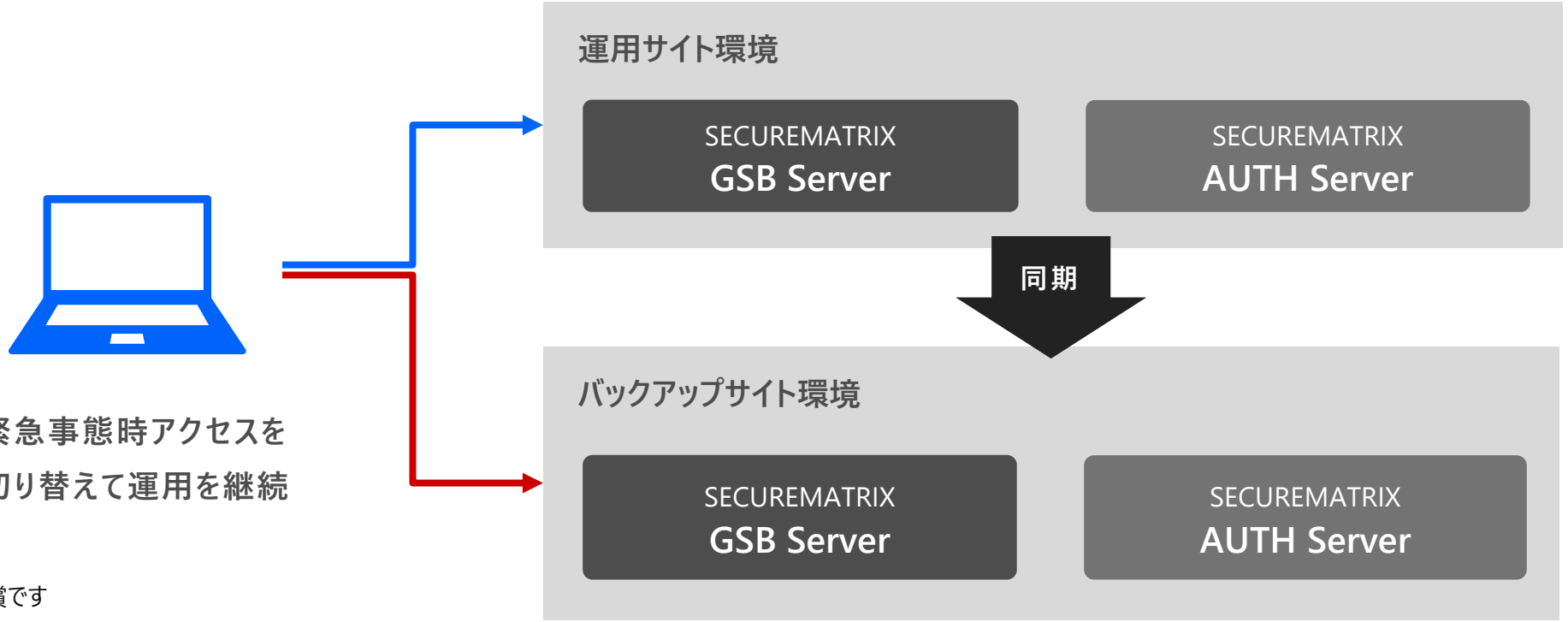
	SECUREMATRIX V13導入	SECUREMATRIX 非導入 ※固定パスワード認証の場合
セキュリティ強度	◎ 多要素認証（マトリクス・デバイス・パスキー） ワンタイム証明書を採用しているため 流出しても次回悪用の危険性なし	× なりすまし・ブルートフォースアタック・ スニッフィングなどの被害に遭う危険性あり
ユーザビリティ	◎ • 管理者の手を介さずにデバイスの登録や パスワードのリセットがいつでも可能 • デバイス間のインターフェース統一	× • 固定パスワードを正確に覚えられない • 失念した際の手続きが煩雑
コスト	◎ • 「覚えやすい」ためパスワードを失念するリスクを大幅に削減 • 管理者によるデバイスの登録やパスワードのリセットが不要になることで運用のコストを削減 • AWS/Azure上での構築が可能なため、サーバーの導入・運用コストを削減	× • セキュリティ被害に遭った場合、 多大な損害が発生 • 固定パスワードを失念した場合の問い合わせ対応など多大な運用コストが発生 • デバイス資産の有効利用が不可能でムダが発生

HITACHI

3.10 DRオプション

万一の事態でも、SECUREMATRIXは運用を止めません
お客さまの事業継続を支援します

運用サイトからバックアップサイトにユーザーデータ、設定情報を定期的に同期することにより、
緊急事態発生時でも運用を継続できます



※本オプションは有償です

4. SECUREMATRIXのライセンス・保守サポート

4.1 ライセンス提供方法

SECUREMATRIXのライセンスには「ソフトウェアライセンス」と「サブスクリプションライセンス」の2種類があり、
「ソフトウェアライセンス」は、ソフトウェア費用と保守サポート費用を別々に購入する形態です

ライセンスの種類

ライセンス種別	概要
ソフトウェアライセンス	ソフトウェア費用と保守サポート費用を別々に購入するライセンス 初年度：ソフトウェア費用と年間保守サポート費用が必要 次年度以降：年間保守サポート費用のみで更新
サブスクリプションライセンス	初年度から一定の費用で利用可能な保守サポート込みのライセンス
評価ライセンス ※	30日間無償で評価できるライセンス

※購入をご検討のお客さまには、評価ライセンスの提供が可能です。必要な場合は、ご相談ください

保守サポートとは別に、「SIサービス」や「SE保守サービス」「トレーニングサービス」などのソリューションサービスを用意しています
詳細はお問い合わせください

4.2 ライセンスについて

ライセンス形態

	ソフトウェアライセンス	サブスクリプションライセンス
ライセンスの形態	買い切り型	年間更新型
利用者の数（ユーザーIDの数）	購入する際に指定（利用者数により料金が異なります）	
保守サポート	別途、年間サポート料金が必要	サブスクリプションライセンスの料金に包含
バージョンアップ	年間サポート料金に包含　※	サブスクリプションライセンスの料金に包含　※

※ V10.x.xおよびV11.x.x、V12.x.xからV13へのバージョンアップは無償です。V9以前のバージョンをご使用の場合は、お問い合わせください

参考価格（税別）

利用者数	ソフトウェア価格	サブスクリプション価格（年間）
25ユーザー	¥ 215,000	¥ 110,000
100ユーザー	¥ 710,000	¥ 379,000

参考価格は一例です。詳細はお問い合わせください

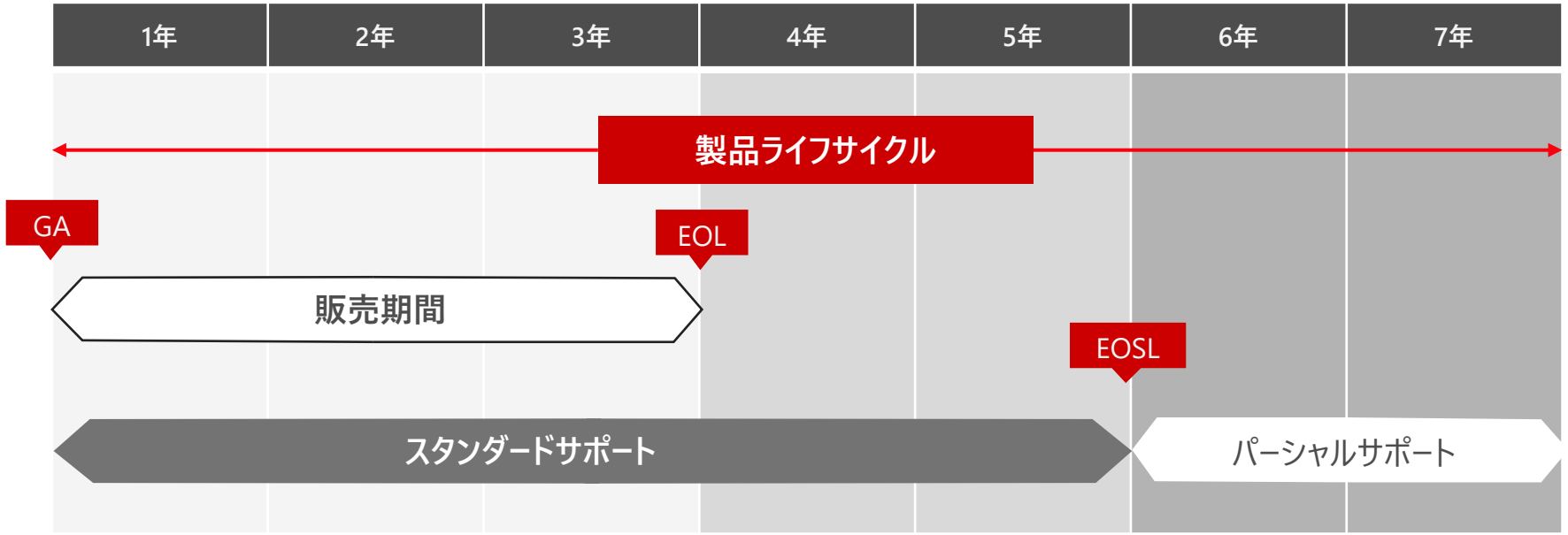
4.3 保守サポートについて

製品出荷後5年間はスタンダードサポートを、
スタンダードサポート終了後2年間は、パーシャルサポートを提供します

	スタンダードサポート	パーシャルサポート
お問い合わせ受付	○	○
障害解析	○	△ 既知の問題のみ対応
セキュリティ 脆弱性対応	○	×
パッチ	○	×

4.4 ライフサイクル（EOSL）

SECUREMATRIX V13では、以下のように製品ライフサイクルとサポートポリシーを定めます



EOL/EOSLの定義

販売終了（EOL : End-of-Life）・・・・・・・・・・・・・・・・・・・・・・ 該当バージョンの販売終了とします

サポート終了（EOSL : End-of-Support-Life）・・・・・・・・・・ 製品出荷開始後5年でスタンダードサポートを終了します

パーシャルサポート終了・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 製品出荷開始後7年でパーシャルサポートを終了します

※製品出荷開始（GA）後3年でEOLとなります
※既存の複数年保守は本EOSLの対象外とし、締結済みの保守契約に基づく保守サービスを契約期間提供します
※SECUREMATRIX V13の販売終了日は2027年1月31日、スタンダードサポート終了日は2029年1月31日です

お問い合わせ先

■お問い合わせ先

株式会社 日立ソリューションズ・クリエイト

- **Webでのお問い合わせ**
  www.hitachi-solutions-create.co.jp/contact/solution.html

  お問い合わせページより、商品・サービスをお選びください。
- **メールでのお問い合わせ**
  hsc-contact@mlc.hitachi-solutions.com

■お問い合わせ情報について

ご相談、ご依頼いただいた内容は回答などのため、当社の関連会社（日立ソリューションズグループ会社）および株式会社日立製作所に提供（共同利用含む）することがあります。
取り扱いには充分注意し、お客さまの許可なく他の目的に使用することはありません。

表示に関する注意事項

HITACHI

■他社商品名、商標などの引用に関する表示

- 「SECUREMATRIX」、「マトリクス認証」は株式会社シー・エス・イーの登録商標です。
- Windows、Windows Hello、 Microsoft Office、Active Directory、Azureは、Microsoft Corporationの登録商標です。
- Google Workspace は、Google LLC の登録商標です。
- Salesforceは、salesforce.com,Inc.の登録商標です。
- eセールスマネージャー は、ソフトブレーン株式会社の登録商標です。
- Citrix、StoreFront、NetScalerは、Citrix Systems, Inc.の登録商標です。
- Ciscoは、Cisco System, Inxの登録商標です。
- F5、BIG-IPは、F5, Inc.の商標もしくは登録商標です。
- FortiGateは、Fortinet, Inc.の登録商標です。
- Array AGは、Array Networks,Incの商標です。
- Pulse Secureは、オージー技研株式会社の登録商標です。
- VMware Horizonは、Broadcom Inc.の商標です。
- Apple、Face ID、Touch IDは、Apple Inc.の登録商標です。

表示に関する注意事項

HITACHI

■サービス・製品の仕様に対する表示

本資料に記載しているサービス・製品の仕様は、2025年11月現在のものです。
サービス・製品の改良などにより予告なく記載されている仕様が変更になることがあります。


HITACHI