Hitachi Solutions Create

HITACHI

「侵入させないこと」が最初のランサムウェア対策

ID・パスワードの漏えいを前提とした、最初にとるべき侵入防止対策とは

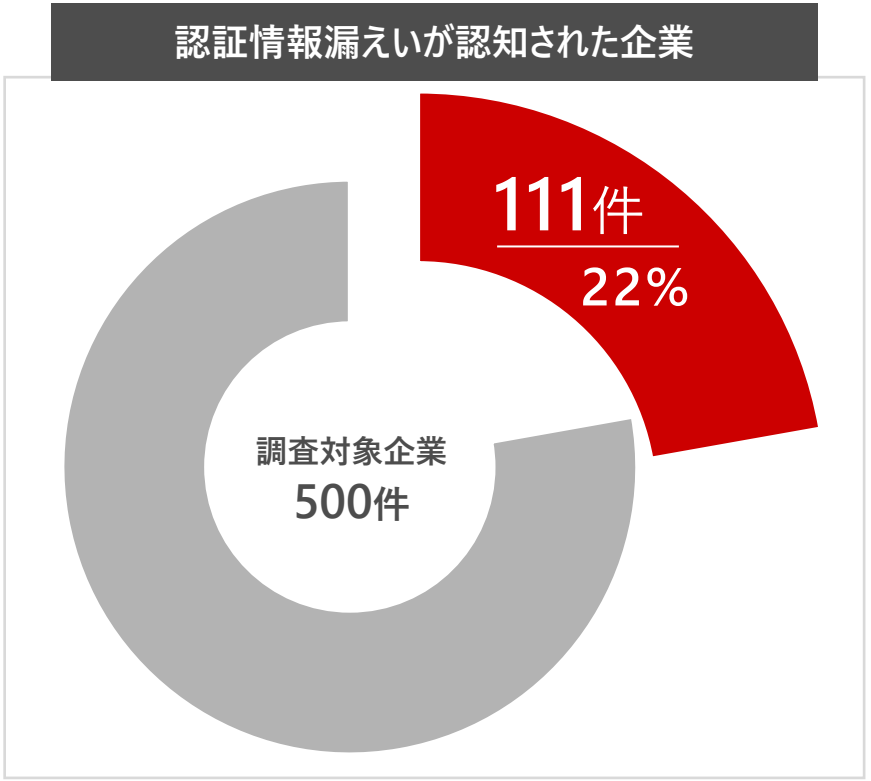
株式会社 日立ソリューションズ・クリエイト

1. 認証情報漏えいの実態

HITACHI

1-1. 認証情報の漏えいは目前に迫る脅威

認証情報の漏えいは、もはや一部の企業の問題ではなく、全ての企業が現実に直面している問題です。多くの企業の認証情報が秘密裏に窃取され、攻撃者側へと渡っています。認証情報の漏えいを前提とした対策が求められます。



約5社に1社が認証情報漏えいのリスク有

インフォスティーラー（情報窃取型マルウェア）による、認証情報の漏えい状況を調査。
国内企業500社のうち、**22%の企業の認証情報漏えいが検知**されました。

業種	漏えい検知企業数	業種	漏えい検知企業数	業種	漏えい検知企業数
製造・メーカー	14社	金融	4社	飲食・サービス	11社
エネルギー	10社	建設・設備	17社	IT・メディア	20社
運輸・輸送	14社	販売・商社	8社	医療・福祉	4社
				不動産	9社

出典：SOMPO CYBER SECURITY　2024年度 我が国における認証情報の実態調査

HITACHI

1-2. 認証情報の窃取手段と目的とは

膨大な認証情報漏えいの背景には、フィッシング攻撃に加え「インフォスティーラー」による感染した端末の情報を外部へ送信するマルウェア攻撃の拡大があります。窃取された情報はダークウェブなどで売買され、実際の攻撃に利用されています。

フィッシング攻撃

不正なメール・SNSから、リンク先にある偽サイトへ誘導して、ID・パスワードなどの認証情報を盗み取る方法

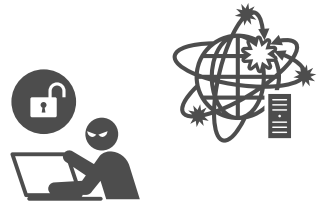
情報窃取型マルウェア攻撃

マルウェア（インフォスティーラー）に感染させ、ID・パスワードなどの機密情報を外部C2サーバーへ送信する方法

闇市場

ダークウェブ
ディープウェブ
リークサイト
etc

窃取した認証情報は闇市場で攻撃グループに販売され、ランサムウェア攻撃などに利用



2024年度に窃取された認証情報

約 **32億件**

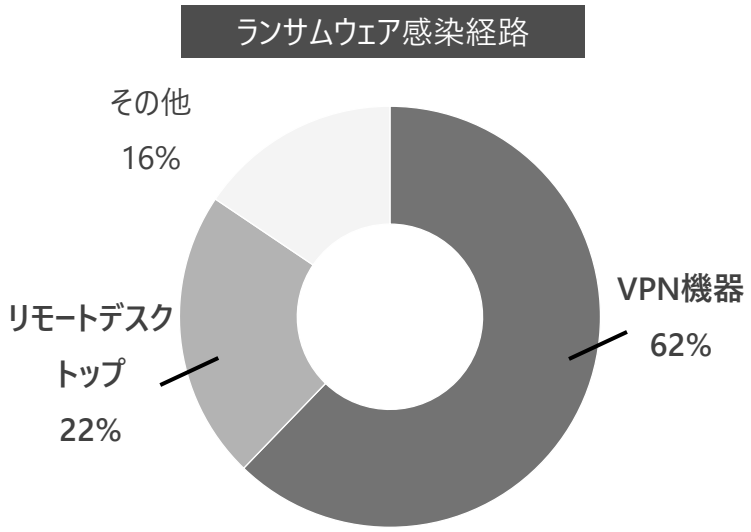
ダークウェブやディープウェブなどの闇サイトを監視し、企業向けのリスクインテリジェンス（脅威情報）を提供するFlashpoint社の調査によると、2024年度に窃取された認証情報の総件数は約**32億件**に達しました。
そのうち**75％がインフォスティーラー**によるものであり、世界中で2,300万台以上のデバイスが感染被害にあっています。

HITACHI

1-3. ランサムウェア攻撃対策において「初期侵入リスクの低減」は最優先事項

本質的なランサムウェア攻撃対策は「侵入後の対応」ではなく、「侵入させないこと」にあります。攻撃者の多くが利用する侵入経路に対して大きなハードルを設けることが、事業継続性を高めるための最優先事項といえます。

Phase 1. 情報収集 ▶ **Phase 2. 初期侵入** ▶ Phase 3. 内部展開 ▶ Phase 4. 情報窃取・暗号化 ▶ 目的遂行



■VPN・RDPからの侵入が84%

ランサムウェアの感染経路とは、依然として外部環境との接続点である「VPN」や「リモートデスクトップ」が標的となっています。IPAの情報セキュリティ10大脅威2025組織編でも、機器のぜい弱性の放置に加えて、**窃取・推察された認証情報の悪用について大きなリスクと位置付けられています。**

出典：警視庁「令和7年度上半期におけるサイバー空間をめぐる脅威の情報等について」

ランサムウェアを攻撃フェーズごとに分解した場合、最優先事項は「初期侵入」のリスクを低減させることと考えられます。攻撃を成立させないブロックを実現することが重要です。

HITACHI

1-4.「多要素認証」による認証強化が求められています

多要素認証とはID・パスワードの「記憶認証」に加え「所持認証」、「生体認証」の3つの認証要素から2つ以上を組み合わせて本人確認を行う、セキュアな認証方式です。多くのガイドラインや指針で義務化・推奨化が進められています。

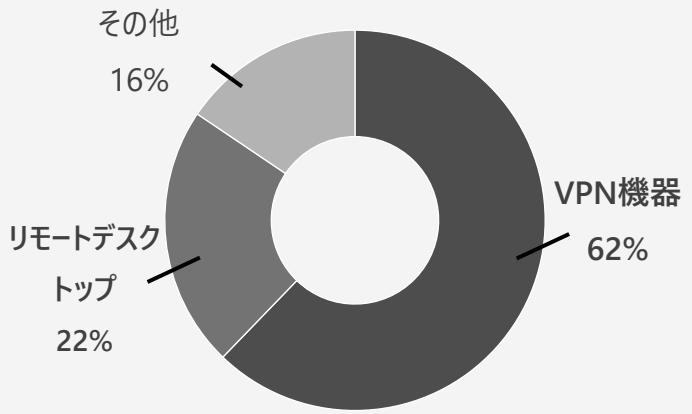
国内ガイドライン・指針

- 医療情報システムの安全管理に関するガイドライン（厚生労働省）
- 金融商品取引業者等向けの総合的な監督指針（金融庁）
- インターネット取引における不正アクセス等防止に向けたガイドライン（日本証券業協会）
- 地方公共団体における情報セキュリティポリシーに関するガイドライン（総務省）
- **サプライチェーン強化に向けたセキュリティ対策評価制度（経産省）※2026年下期制度開始予定**

HITACHI

1-5. 多要素認証導入による効果

ランサムウェア対策



ランサムウェアの多くが、VPNやリモートデスクトップなど外部環境との接続点を通した侵入・攻撃が行われています。多要素認証システム導入による認証情報の強化はこれらの攻撃に対して、有効な対策手段となり得ます。

出典：警視庁「令和7年度上半期におけるサイバー空間をめぐる脅威の情報等について」

不正アクセス対策

98.6% パスワード漏えい時の、攻撃阻止確率

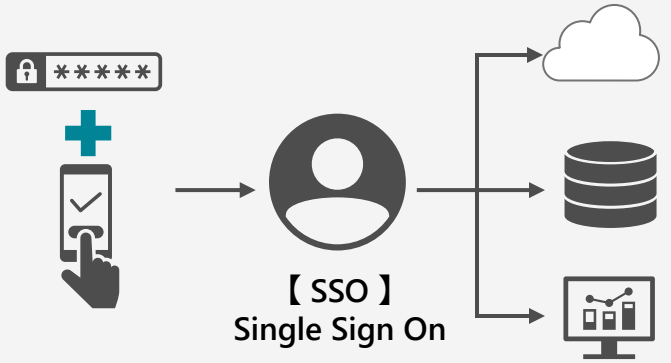
99.2% アカウント侵害のリスク低減割合

99.1% 侵害されたアカウントの99.17%がMFAを使用していなかった

Microsoftの研究論文において、多要素認証の実装によるアカウント保護の有効性が実証されています。Microsoft Active Directoryなどの商用アカウントを対象にした調査では、**パスワードが漏えいした場合でも、98.56%の攻撃を防止できたとの調査結果がでています。**

参考：MictosoftMFA-Microsoft-Research-Paper-update.pdf

SSOによる管理業務効率化



SSO導入による効果は、ポリシーの一元的な適用やぜい弱なパスワードの使いまわしリスクの軽減などのセキュリティリスクの軽減のみにとどまりません。**パスワードに関連する問い合わせ数や、管理負担の低減になど、IT管理部門の業務負担軽減に大きな成果が確認できます。**

2. 当社の提供製品の紹介

HITACHI

2-1. 多要素認証システム導入における課題

日本企業の多要素認証（MFA）導入率は20％と低い水準にとどまっています。（※）。特に中堅・中小企業では従来型のID/パスワード認証への依存度が高く、クラウドサービスの利用やリモートワークの拡大に伴いセキュリティリスクが高まっています。

※ Yubico：「グローバル認証状況調査2025」より

このような課題はありませんか？

IT基盤に関するお悩み

課題1

全従業員にスマートフォンを貸与しておらず、多要素認証で多く採用されているスマートフォンを利用した認証方式を採用することが難しい。

管理体制に関するお悩み

課題2

スマートフォンやハードウェアトークン、ICカードなどの専用機器に関して、資産管理・紛失への備えなどの運用プロセスがIT管理部門の負担となる。

業務効率化実現への懸念

課題3

ID/パスワードの入力に加えて他の要素が加わることで、ログインの手間が増え、業務効率の低下、現場の反発が起きる可能性がある。

HITACHI

2-2. SECUREMATRIXの紹介

SECUREMATRIX

SECUREMATRIXが解決

IT基盤に関するお悩み

認証用追加デバイス不要

特許技術を用いた方式で、既存のIT環境への影響を最小限に抑えつつ、強固な多要素認証の実装が可能です。

管理体制に関するお悩み

運用負担の軽減

認証用機器の管理負担削減に加え、独自技術により、電子証明書の有効期限管理やパスワード再発行手続きなどの業務負担を軽減できます。

業務効率化実現への懸念

ユーザービリティの高いSSO

PCのみでもセキュアな多要素認証が実現でき、スムーズな運用開始を実現できます。また、オンプレミス・クラウド環境の双方に一度の認証作業でアクセス可能です。

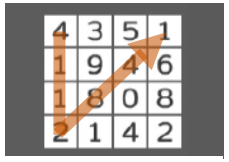
HITACHI

2-3. SECUREMATRIX 3つの認証要素

お客さまの組織環境に合わせて、3要素全てを利用した多要素認証や、「**マトリクス認証＋デバイス認証**」、「**デバイス認証＋パスキー認証**」などを組み合わせてご利用いただけます。

【記憶】

マトリクス認証



乱数表から記憶した【形】に当てはまる数字ワンタイムパスワードとして認証する「**パスワードレス認証方式**」

【所持】

デバイス認証

サインインのたびに新しい電子証明書を発行する「**ワンタイム身分証方式**」

【生体】

パスキー認証

FIDO2に準拠したパスキーを利用する「**パスワードレス認証方式**」

HITACHI

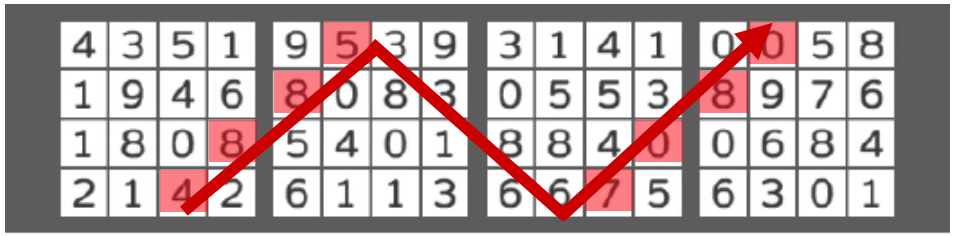
2-4.【記憶】マトリクス認証

ユーザーにしか分からない**【形】の記憶で認証を行います。**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）であらかじめ設定した位置・順番をもとに、ワンタイムパスワードを入力します。

■ マトリクス認証： ユーザーしか知らない「形」を利用したパスワードレス認証

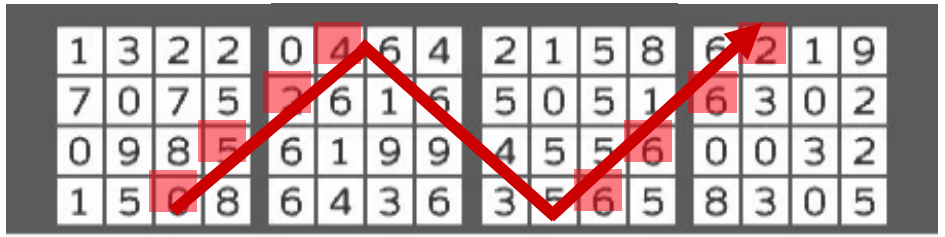
ログインごとに乱数表（マトリクス表）が変化。記憶した形をなぞり、使いきりのワンタイムパスワードを発行

1回目



4 8 8 5 7 0 8 0

2回目以降



0 5 2 4 6 6 6 2

パスワードは一度きりの使い捨て

多くのパスワード攻撃に有効な防御手段

パスワードリスト攻撃、キーロガー、辞書攻撃などパスワードを狙った攻撃を実質的に無効化

パスワードに関する社内問い合わせを減少

【形】で記憶する認証方式のため、パスワードの失念などが原因となる再発行手続きの負担を軽減

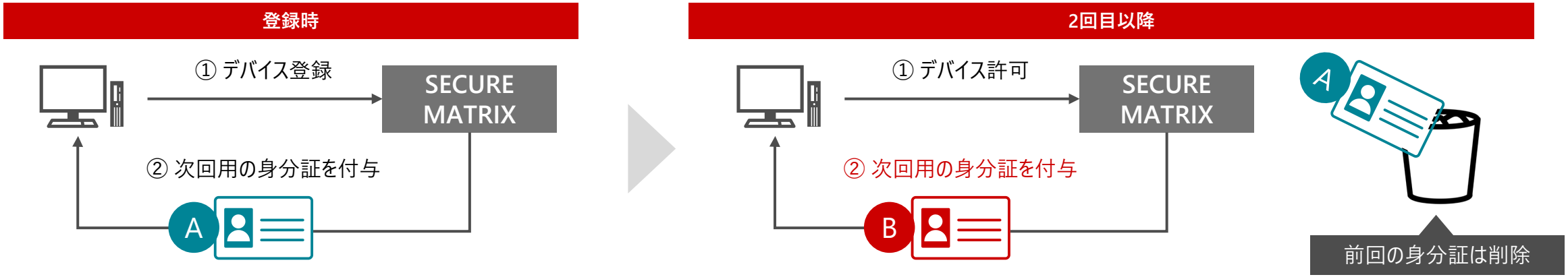
HITACHI

2-5.【所持】デバイス認証

電子証明書として機能する、特許技術の【ワンタイムデジタル身分証】をデバイスに付与して所有の認証を実施。
デジタル身分証はサインインのたびに新しく付与されるため、有効期限管理の必要もありません。

■ デバイス認証： サインインするたびに新しく発行されるワンタイムデジタル身分証

サインインのたびに"次回用の身分証"を付与することによって、身分証のないデバイスからのアクセスをシャットアウトします。



電子証明書を狙った攻撃を無効化

電子証明書を窃取した「なりすまし行為」や「不正アクセス」などのリスク軽減

電子証明書の管理負担を軽減

使いきり方式のため、電子証明書の管理や有効期限管理などの運用負担を軽減

HITACHI

2-6. ハイブリッドシングルサインオン（Hybrid SSO）

境界型でも、ゼロトラスト型ネットワークでも、ハイブリッドなシングルサインオンを実現します。
多要素認証およびシングルサインオンでのセキュアなアクセスを可能にし、境界型・ゼロトラスト型どちらでも、安全で利便性の高いワークスペースを提供します。

■ ハイブリッドシングルサインオン：一度のセキュアな認証で複数システムへアクセス

セキュリティ強化

一元的なパスワードポリシーによるセキュアな運用管理
許可のないデバイスからの利用制限（シャドーIT対策）

ユーザービリティ向上

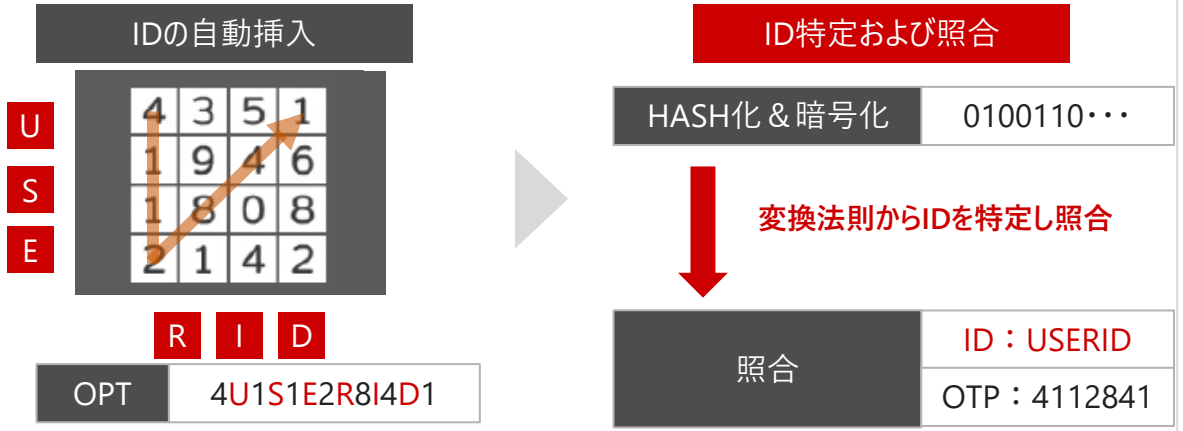
一度の認証で複数システムへのアクセス
アカウント管理の一元管理による業務負担軽減

HITACHI

2-7. 特許技術による認証強度の向上

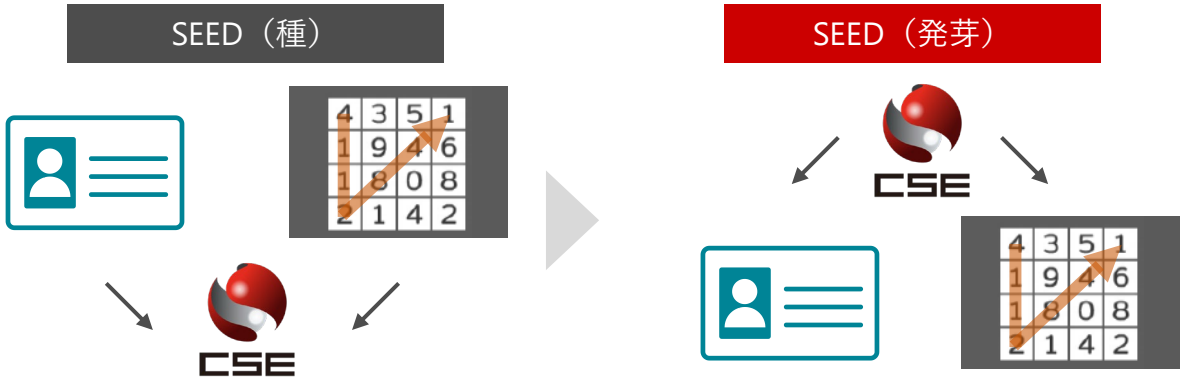
■ ステルスID方式：IDの秘匿化

ワンタイムパスワードにIDや属性情報を**自動挿入**します。
ワンタイムパスワードからIDを特定できるため、ID入力を省略して、**ID情報の漏えいも防ぎます。**



■ SEED方式：通信の暗号化

認証に必要な情報を直接通信経路に流さず、SEEDと呼ばれるデータに置き換えて送受信します。通信経路上に直接IDやワンタイムパスワードの情報を流さないため、**盗み見や通信傍受などを無力化し、安全に認証ができます。**



デジタル身分証情報やマトリクス表を
生成するための乱数をSEEDに置き換えます

アクセスのたびに、SEEDから
デジタル身分証とマトリクス表を抽出します

HITACHI

2-8. 導入事例

SECUREMATRIXは、国産の多要素認証システムとして20年以上にわたり堅ろうなセキュリティ基盤として多くの企業に採用されてきました。国内大手企業、自治体、大学、医療機関など多種多様な業界に多数の導入実績があります。

■ 導入事例　製造業：2,500ID（運用数）

NEED

**海外赴任・出張者が安全に社内システムへ
アクセスできるICT環境の整備**

課題1　ハードウェアトークンなどの故障時の敏速な対応が困難で、業務に支障が生じる可能性がある

課題2　数か月に一度、大幅な社員情報のメンテナンスが必要で、その運用負担も大きな課題

OUTCOME

**人事・経理システムなどの
社内の他業務システムへも利用拡大**

解決1　PCのみでもセキュアな利用者認証が可能。外部デバイスの故障・紛失による業務停滞のリスクと管理コストを軽減

解決2　標準機能でID管理システムと連携させることができたため、社員情報メンテナンス作業の効率化を実現

より詳しいご相談、お問い合わせ

HITACHI

ご相談・お問い合わせ

ご相談・お問い合わせは専用メールアドレス宛にお問い合わせください。
ご不明点やご要望も受け付けています。
お客さまの環境に最適なご提案をいたします。

hsc-contact@mlc.hitachi-solutions.com

株式会社 日立ソリューションズ・クリエイト
所在地:東京都品川区東品川四丁目12番6号
（品川シーサイドキャナルタワー）
https://www.hitachi-solutions-create.co.jp/

■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
- 「Microsoft」、「Windows」、「Active Directory」は、米国、その他の国における米国Microsoft Corp.の登録商標です。

■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。

■サービス・製品の仕様に関する表示

本資料に記載しているサービス・製品の仕様は、2026年2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

わくわくをあなたと

想像を超える明日を創造する

当社はITを通じ 安心・快適を提供し、社会とともに持続的に成長します。
確かな技術力と深い知見で、想像を超える価値の創造に挑戦します。
協創を通じて すべての人が充実し、わくわくする明るい未来づくりに貢献します。

HITACHI