

現場でもオフィスでも在宅でも快適PCログオン

多要素認証 活用事例



SmartOn® シリーズ

累計約4600社・約370万ライセンス。デバイス認証ツール分野・20年連続シェアNo.1※

※ 出展「2004～2023ネットワークセキュリティビジネス調査総覧デバイス認証ツール」富士キメラ総研

□ 目次

- P4 **産業機械メーカー** 「工場の共有PCで、負荷をかけない利用者認証」
- P5 **BPO大手** 「強固な本人認証で、大規模な緊急国策事業にもスピーディーに対応」
- P6 **流通系金融** 「顧客情報もOAクラウド基盤も、束ねて守る」 
- P7 **研究開発機関** 「急なテレワークでも安心、プラス国産EDRで日本の研究開発情報を守る」 
- P8 **クレジットカード会社** 「テレワークでも、PCI DSSに準拠したセキュリティ認証」
- P9 **独立行政法人** 「Smart Secure Client×顔認証で、業務データを漏らさない」
- P10 **ガス機器メーカー** 「たった一度の顔認証で、あらゆる業務システムをパスワードレス利用」
- P11 **医療機器メーカー** 「いつでもどこからでも、VDI×顔認証で医療研究データに安心アクセス」 

□ 目次

- P12 **TV放送事業者** 「一分一秒を争う報道現場、個人情報 は 仕組みで守る」
- P13 **旅行会社大手** 「顔認証でヘルプデスク工数を低減、新常態でも高セキュリティ」
- P14 **関東地区 市役所** 「分離環境でも、顔認証で職員の安全なリモートアクセスを実現」 
- P15 **中核市 教育委員会** 「拡張性の高い認証基盤に刷新、教職員の利便性も向上」
- P16 **政令市 水道局** 「24/365で稼働する重要インフラを、国産ソフトウェアで守る」 
- P17 **損害保険会社** 「ノートPCの利便性を損なわないセキュリティ」

産業機械メーカー 「工場の共有PCで、負荷をかけない利用者認証」

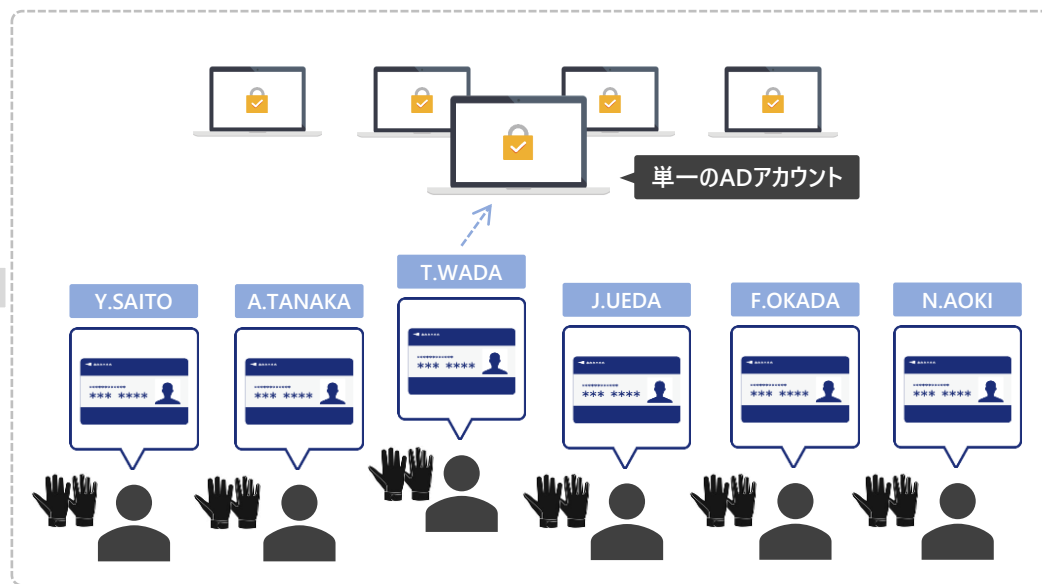
☑ ICカード認証 / 約3千ユーザー

導入背景

- 工場のPCは、同一のADアカウントを複数人で共有しており、いつ・誰がPC利用していたのかが特定できていない課題があった。
作業者の生産性を落とさず、利用者認証を実施する必要があった。

活用メリット

- 作業用手袋をつけたままでも、**キーボード操作をする必要がなく** ログオンが完了
- 作業員に**PCログオン操作の負荷をかけることなく**、共有PCの利用者認証が**実施でき**、セキュリティが強化できた
- SmartOnサーバーは **IaaS 上にも導入し**、**BCP 対策も実現**



BPO大手 「強固な本人認証で、大規模な緊急国策事業にもスピーディーに対応」

☑ ICカード認証 / 約1万ユーザー

導入背景

- 2020年「休業要請に伴う各給付金の対応デスク」を大量受注。SmartOnは元々、BPOのセキュリティ体制のルールとして採用されており、対応職員とクライアントPCの増設にもスピーディーに対応。

活用メリット

- 業務上センシティブな情報が含まれるが、職員にリテラシーに依存せずに高い安全性を維持（＝セキュアな認証とログ）
- 需要増による急な拠点新設でも、素早く、即時に業務を開始できた（＝ポリシーの一元管理＆サイレント展開）
- 人員の入れ替えが多い現場でも、ユーザー情報とログを一元管理することができ、管理漏れによる情報漏えいを確実に防止

セキュリティ体制

物理的対策

入退室管理設備、無停電電源設備

技術的対策

アクセス制御、暗号化、**ユーザ認証 & 証跡ログ**
マルウェア対策

運用管理対策

情報セキュリティ方針・基準の策定と運用、
セキュリティ教育の実施、セキュリティ監査

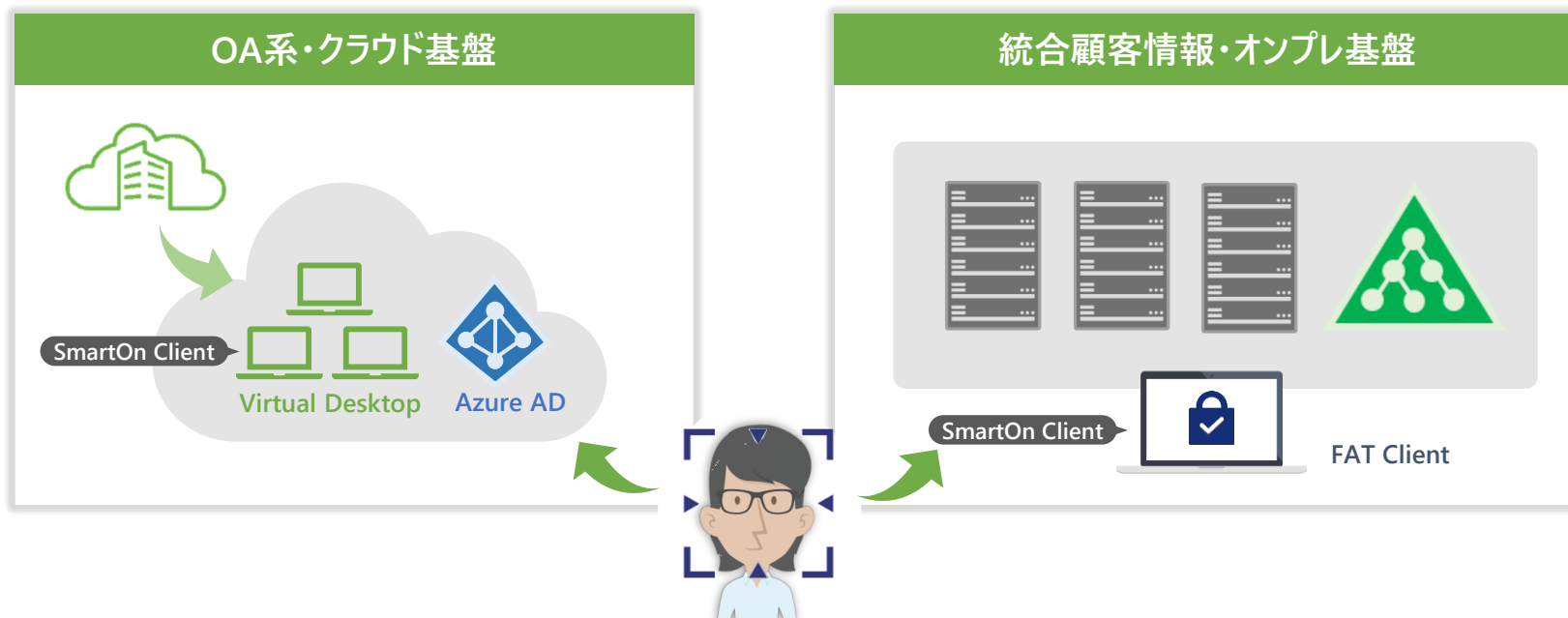


導入背景

- 指紋認証を利用していたが、精度が悪く、デバイス管理に手間がかかっていた為、**SmartOn 顔認証に切り替え**。
端末のリプレースに伴い、OA系の基盤を「VMware Horizon Cloud on Microsoft Azure」に刷新した。

活用メリット

- 2020年 突如降りかかったテレワーク環境でも、**利便性を損なうことなく、セキュアに業務開始**できる環境が用意できた
- なりすましを防止できる、**精度の高い認証システムを実現**（＝SmartOnの首ふり認証）
- OA系と顧客情報系で異なる端末環境であったが、**共通認証基盤でコスト低減を実現**



研究開発機関 「急なテレワークでも安心、プラス国産EDRで日本の研究開発情報を守る」

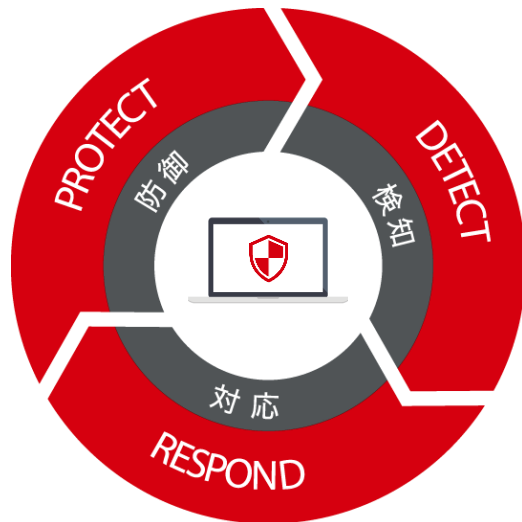
☑ VDI×多要素認証 ☑ 顔認証 / 約3千ユーザー

導入背景

- OA環境のシステム更改において、リモートワークにも適したモバイルPCの調達とセキュリティの向上を目的とした、**エンドポイントでのセキュリティ対策**を検討。情報資産を保全しつつ、研究に集中できる環境を整備する必要があった。

活用メリット

- PC内蔵カメラに顔を向けるだけの簡単ログオンで、利用者に**セキュリティを意識させない**運用を実現 ▶ **SmartOn**
- 不審なシステム動作を監視し **脅威を検知**、サイバー攻撃と内部不正を同時に対処することが可能に ▶ **InfoTraceMark II**
- リモートワーク時の端末状況も**ログにより可視化**、**インベントリ取得**や**ファイル配布**によりアップデート適用漏れも防止 ▶ **InfoTraceMark II**



クレジットカード会社 「テレワークでも、国際基準に準拠した認証セキュリティ」

☑ 顔認証 / 約5千ユーザー

導入背景

- ノートPCへのリプレイスに伴い ICカード認証から、Webカメラを利用できる顔認証に切り替えを実施。
働き方改革の一環で、**時短・自宅勤務者でも安全に業務ができる認証環境**が必要であった。

活用メリット

- クレジットカード情報を扱うためのセキュリティ基準である、**多要素認証要件**を満たすことができた
- 勤務環境に応じた柔軟なポリシー適用（**離席ロックの有無等**）により、**顧客情報を扱う社員にも安心を提供**
- 業務ポータルとSSO連携、**社員はシステム毎のパスワード管理から解放され生産性も向上**



独立行政法人「Smart Secure Client + 顔認証で 業務データを漏らさない」

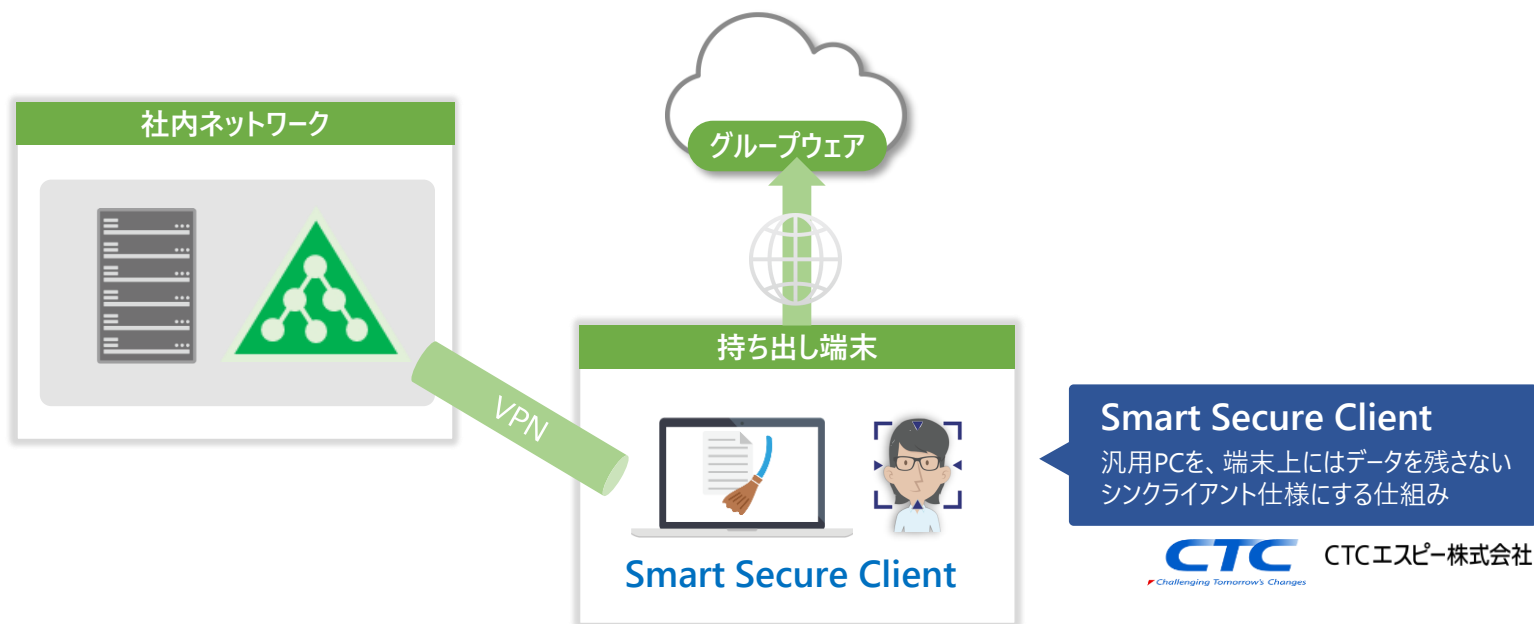
☑ 顔認証 / 約2千ユーザー

導入背景

- PC更改と持ち出し用端末の導入に伴い、**業務データを漏らさない仕組み**が必要だった。
社内ネットワークやグループウェアへの接続を許可した端末が、不正利用されないよう**二要素認証**が要件としてあった。

活用メリット

- 万が一、PCの盗難や紛失があっても、**第三者は端末にログオンできず、ローカルディスクにも業務データは一切残らないため、**情報漏えいを確実に防止できる
- 移動中や出先においても、**カメラに顔を向けるだけで、**どこでも即・業務開始でき、生産性も向上している



ガス機器メーカー「たった一度の顔認証で、あらゆる業務システムをパスワードレス利用」

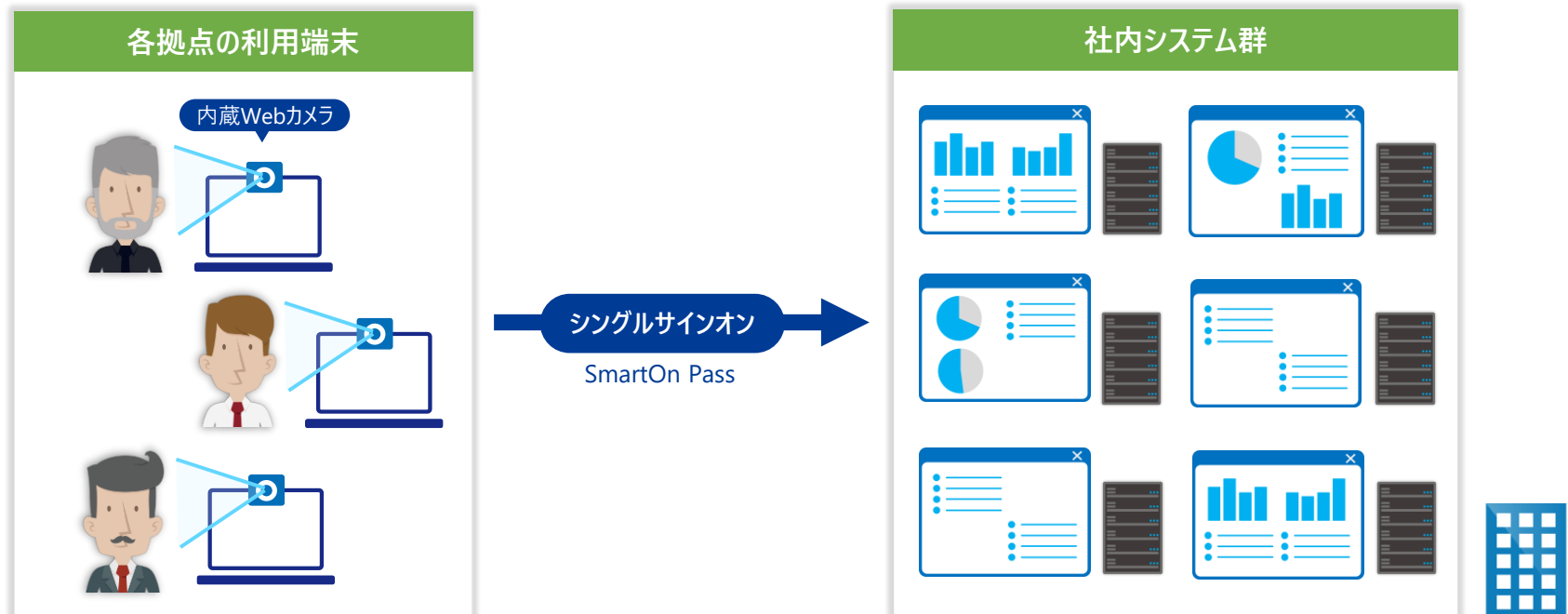
☑ 顔認証 / 約2千ユーザー

導入背景

- 業務システムの増加に伴い、パスワードの使い回しによる形骸化やパスワード忘れによる再発行手続きの労力が課題となっていた。パスワードを従業員に教えたくないという強い要望があった。

活用メリット

- PCログオンから各業務システムへのログインまで、一貫したパスワードレスを実現（= SmartOn Passによるシングルサインオン）
- 認証方式を顔認証に移行したことで、**利用者の利便性**とともに、**管理者の運用性**も向上した



医療機器メーカー「いつでもどこからでも、VDI×顔認証で医療研究データに安心アクセス」

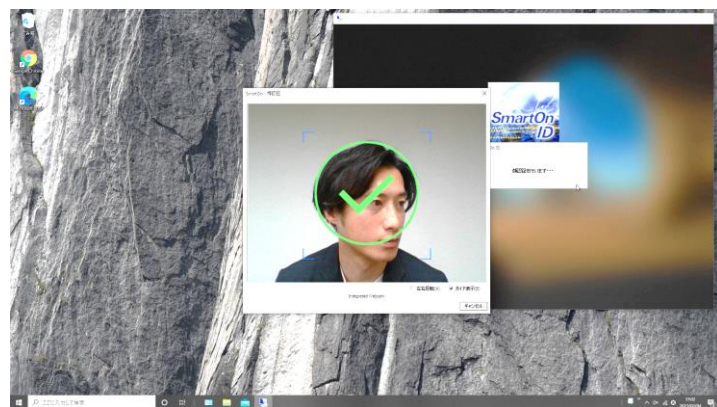
☑ VDI×多要素認証 ☑ 顔認証 / 約2千ユーザー

導入背景

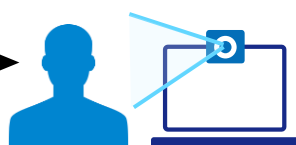
- デスクトップPCから移行し、仮想デスクトップを導入。シンクライアント端末の導入に合わせ、従来のICカード認証から、Webカメラを利用した顔認証へ移行。

活用メリット

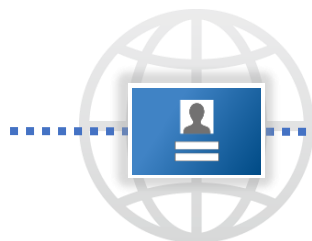
- 仮想環境上で、医療研究データをはじめとする機密情報を扱うため、仮想環境の入り口の本人認証を強化する必要があったが、SmartOn for リモートアクセスにより、**仮想デスクトップ ログオン時の顔認証**が適用できた



手元のWebカメラを利用し
仮想PCへ顔認証ログオン



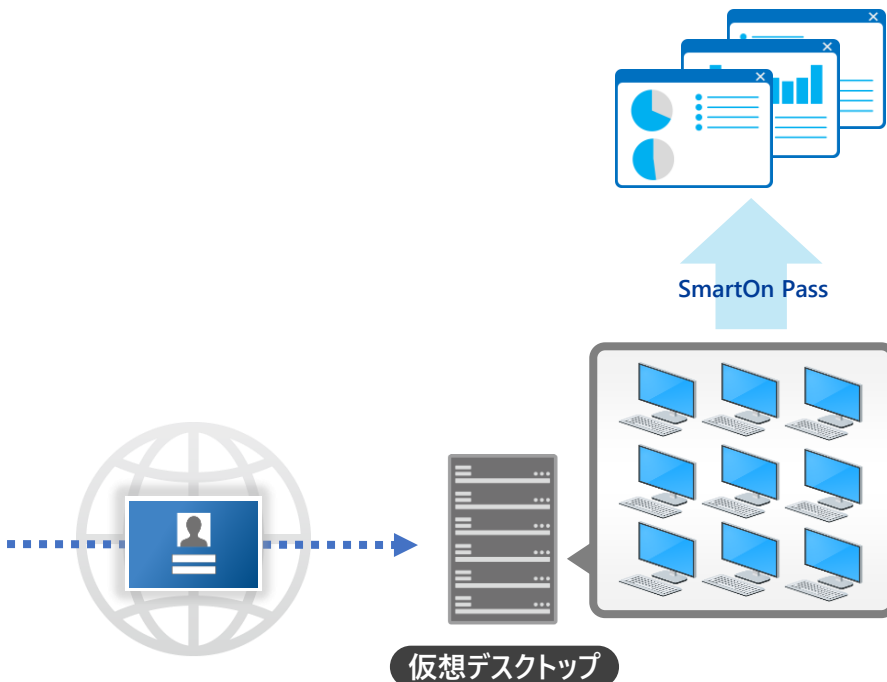
シンクライアント



仮想デスクトップ



SmartOn Pass



導入背景

- 持ち出し用PCの運用において、業務を優先させざるを得ない現場でのセキュリティ対策に課題を抱えていた。
不特定多数の人が出入りする現場でも、安全に情報を収集・活用できる仕組みが必要であった。

活用メリット

- PCのカメラを使って 顔認証することで、素早く安全に業務を開始できる
- ルールではなく システムで制限することにより、社員のITリテラシーに依存せずにセキュリティレベルを強化



導入背景

- パスワードの定期変更を実施していたが、社員の増加に伴い、パスワード忘れやアカウントロックへの対応工数も増加していた。Webカメラ付きノートPCの調達に合わせ、パスワードの定期変更ルールを廃止し、**SmartOn顔認証を導入**。

活用メリット

- パスワードの定期変更を廃止でき、**セキュリティレベルの向上とヘルプデスク工数の低減を同時に実現**
- 強固な本人認証で **なりすましによる内部不正を防止し、大量の個人情報を扱うシステム端末の安全性も向上**

安全性

SAFETY



利便性

USABILITY

関東地区 市役所 「分離環境でも、顔認証で安全なリモートアクセスを実現」

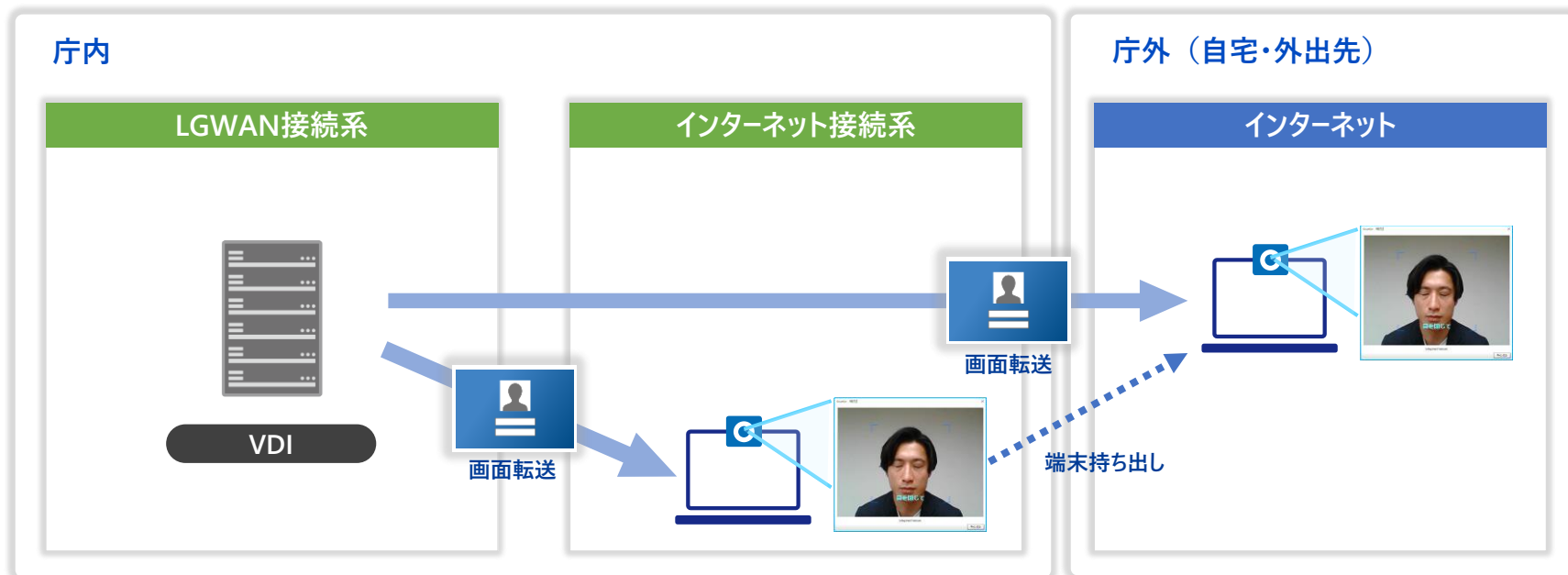
☑ VDI×多要素認証 ☑ 顔認証 / 約800ユーザー

導入背景

- 「地方公共団体におけるテレワーク推進」の流れを受け、スモールスタートでスタンドアロン端末の貸出を行っていた。リモートワークの拡大とともに、許可された職員が、庁外から庁内の端末にアクセスできる環境が必要であった。

活用メリット

- 庁内でも、庁外でも、LGWAN接続系のVDIログオン時に顔認証することで、強固な本人認証を実現
- 最新の顔認証エンジンで、マスクを外さなくても認証。瞬き検知により、画像による「なりすまし」も抑止



中核市 教育委員会 「拡張性の高い認証基盤に刷新、教職員の利便性も向上」

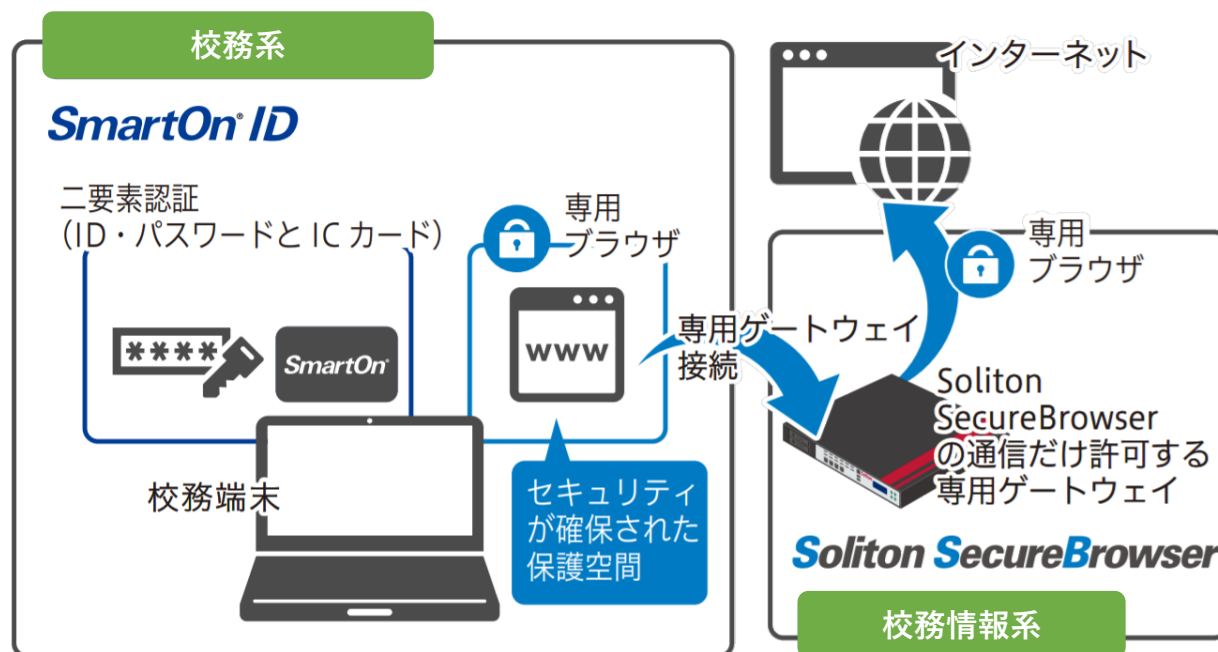
☑ ICカード認証 / 約6千ユーザー

導入背景

- 他社の多要素認証システムからリプレイス。以前のシステムは、シングルサインオン機能の対応ブラウザが限られていたり、ドメインを跨ぐ利用ができなかったりと、運用面で課題が出ていた。教育委員会でも導入実績が多い、SmartOnの導入に至った。

活用メリット

- 拡張性の高い 多要素認証システム にすることで、運用面の課題を解決し、教職員の利便性も向上
- 既存の職員証を利用。初回ログオン時に教職員自身に登録させることで、スムーズな移行を実現
- ガイドラインに則したソリューションを Soliton でまとめて導入、ワンストップのサポートサービスを実現



☑ VDI×多要素認証 ☑ 顔認証 / 約2千ユーザー

導入背景

- 2020年6月に米国で起きた「**水道における産業用制御系システムを対象とした不正アクセス**」の事案を受け、制御システムへの入り口となる **VDI環境利用時の認証** をより強固なものにすることが求められた。

活用メリット

- VDIログオン時に多要素認証（顔認証×パスワード）を利用、**重要インフラへの不正アクセスを許容しないシステム**を構築
- 不特定多数の職員が利用する共有PCでも、VDIの利用ログをしっかり記録することにより、**内部不正を抑止**
- 今後は、**テレワークの利用や同自治体への導入を検討**

水道業務システム



制御システム

設備制御



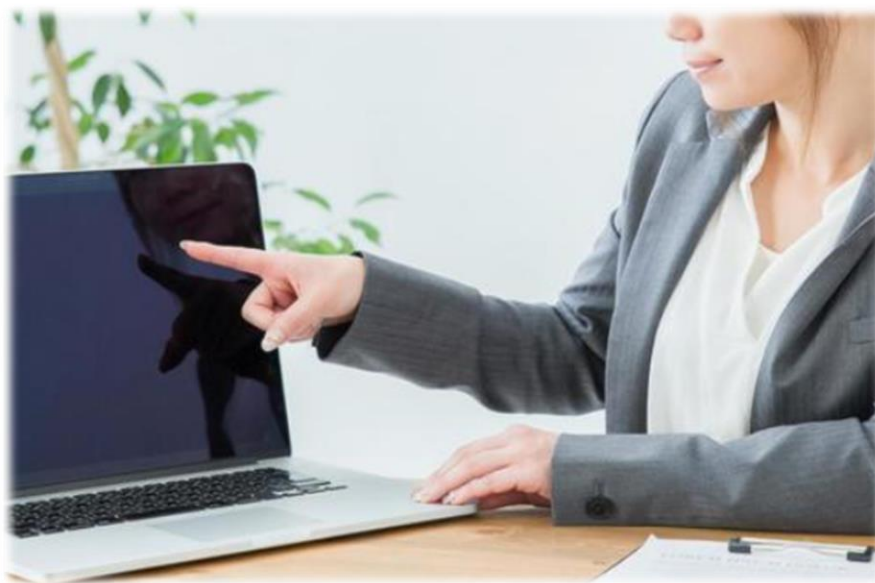
浄水場

導入背景

- クラウドシフトに伴い、認証基盤を刷新。保障プランのシミュレーションや 契約情報の照会などで PCの画面を見せる際、お客様の前でログオン／ロック解除といった動作が発生するため、パスワードを入力しない運用方法を採用する必要があった。

活用メリット

- 顔を向けるだけで PCログオン、顧客情報や基幹システムへも パスワード入力不要で すぐアクセス
- PC を安全に有効活用でき、ペーパーレス化を促進。より円滑な お客様対応が可能に
- Active Directoryと連携し、人事異動による アカウントの追加／変更／削除を自動化し、運用管理も効率化





お問合せ

ITセキュリティ営業部 netsales@soliton.co.jp

for your information

Soliton
自治体情報セキュリティチャンネル 

自治体情報セキュリティ対策のポイントとは。具体的な情報を交えてご紹介いたします。

[▶ くわしくはこちらから](#)