

[SmartSESAME

PCログオン

多要素・二要素認証で PCセキュリティを強化

多要素・二要素認証 / 利用者履歴管理

PCや業務アプリケーションの利用が増える一方で、セキュリティ事故が後を絶ちません

PCの情報漏えいの原因には、サイバー攻撃や不正アクセスなど外部からの攻撃や、社員によるミスや盗難・流出などが多く占めています。PCログオンは、今や政府のセキュリティガイドラインでも推奨されている多要素認証に対応。外部からの攻撃防止に大きく貢献します。

PCログオンができること

生体認証やICカードによる多要素・二要素認証

顔や指紋・静脈などの生体認証やICカードによる多要素認証を取り入れることができます。マイナンバー関連業務を行うためのセキュアな共有PCが必要な場合にも、低コストで多要素認証を導入できます。

ICカードに関しては、FeliCaやMifareなどのICカードはもちろんのこと、マイナンバーカードによるログインにも対応しています。

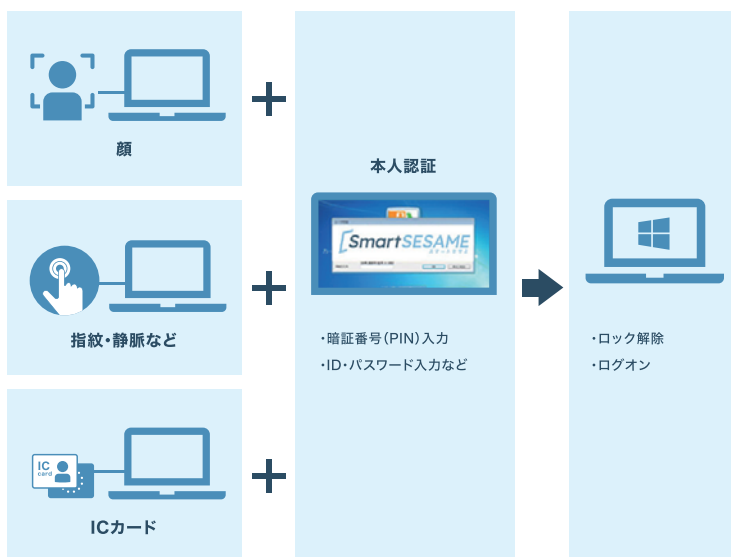
※詳細はお問い合わせください。

ロック解除には再度認証が必要

スクリーンロック後の解除には再度本人認証が必要です。離席時の不正アクセスや覗き見を防ぎます。

利用者履歴の収集管理

「いつ」「誰が」「どのPCを」利用したかログオン履歴を保存し、実際に利用したユーザーを特定することができます。



PCログオンが選ばれる3つの理由

- ✓ **業界最安値**
サーバーレス、PC単位のライセンスでコストを抑えて導入

Active Directoryサーバーの中に認証データ、管理ソフト、ログソフトを格納できるため、新規にサーバーを導入する必要がありません。

※ログやポリシーの設定を管理するマネージャーソフトは、Active Directoryサーバー以外にもインストールできます。

- ✓ **機能特化で**
運用負荷を軽減しながら
しっかり管理

徹底したスリム設計で余分な機能を外し、PCの“ログオン”に特化。管理項目が少なく簡単に導入、管理ができます。

また、共有端末へのログオンも個人の特定ができ、利用履歴もしっかりと管理できます。

- ✓ **緊急時における**
業務を止めない運用

ICカード盗難や紛失における失効処理、ワンタイムパスワードを利用したログオンなど、さまざまな運用に対応できます。

オプション機能

シングルサインオン

覚えきれないIDやパスワードをICカード、生体でログオン認証

勤怠管理連携

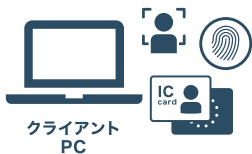
PCのログオン・ログオフ履歴で勤怠を管理

UEBA

ユーザーおよびPCの稼働可視化、攻撃の早期検知

製品ラインアップ

スタンドアローン版

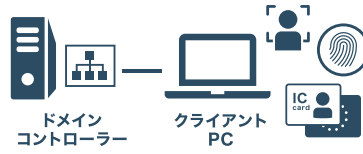


PC内でカード情報および生体情報を管理します。ログオンを行うPCに登録されているICカードあるいは生体データがないとログオンすることができません。管理サーバーが必要なく、カード情報および生体情報の登録からシステムの設定、ログオン履歴の管理までを1台でできます。

機器構成	概要
PCごとの利用者管理	PCごとに利用者管理を行い、カード情報、生体情報の登録、編集、削除ができます。
PCごとのログ管理	ログオン履歴がPCのWindowsイベントログに出力され、PCごとに管理・閲覧することができます。
ローカルポリシーの設定	PCごとにSmartSESAMEポリシー（ローカルポリシー）の設定機能があり、適用されているポリシーの確認や設定を行うことができます。

※ログやポリシーの設定を管理するマネージャソフトは、Active Directoryサーバー以外にもインストールできます。※ライセンスはPC台数単位となります。スタンドアローン版、Active Directory版ともに最低販売ライセンスは10ライセンスとなります。

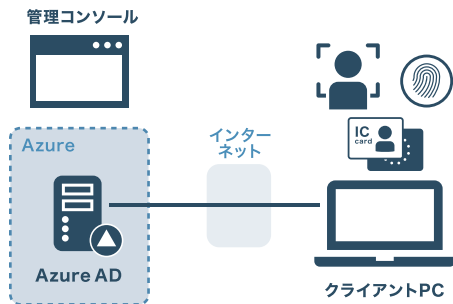
Active Directory版



Active Directory内でカード情報および生体情報を集中管理します。登録されているICカードまたは生体データがないとログオンすることができません。管理サーバーにおいてカード情報、生体情報、ポリシーなどの設定を行い、ログオン履歴を閲覧できます。

機器構成	概要
Active Directory内で集中管理	Active Directory内でカード情報、生体情報を集中管理し、管理サーバーよりカードまたは生体データの登録、編集、削除などを行います。
ログの集中管理	各クライアントPCから出力されたログオン履歴を集中で管理・閲覧することができます。また、管理PCの操作ログも管理することができます。
ローカルポリシーの設定	PCごとにSmartSESAMEポリシー（ローカルポリシー）の設定機能があり、適用されているポリシーの確認や設定を行うことができます。また、Active Directory版においては、管理サーバーより各PCのポリシーの確認、設定を行うことができます。
システムポリシーの配信	管理サーバーからSmartSESAMEポリシー（システムポリシー）を配信することができ、運用開始後もシステム全体で統一されたポリシーで運用を行うことができます。

Azure AD版



Azure ADに参加するクライアントPCに多要素認証でログオンします。Azure ADと連携した管理コンソールにより、カード情報、生体情報、ポリシーなどの設定とログオン履歴の閲覧ができます。

動作環境

	クライアントソフト
対応OS	Microsoft Windows 10 (32bit/64bit) Microsoft Windows 11 (64bit) ※詳細なエディションやバージョンはお問い合わせください。
	管理ソフト
対応OS	Microsoft Windows Server 2012 (64bit) Microsoft Windows Server 2012 R2 (64bit) Microsoft Windows Server 2016 (64bit) Microsoft Windows Server 2019 (64bit) Microsoft Windows Server 2022 (64bit) ※詳細なエディションやバージョンはお問い合わせください。

導入事例



官公庁・自治体

京都府庁 様

京都府セキュリティ基盤の認証システムに「PCログオン」を導入。セキュアかつ利便性を損なわず、庁内システム・業務アプリケーションのログオン管理を実現。



官公庁・自治体

倉敷市役所 様

職員証ICカード認証とID/パスワードを組み合わせ「PCログオン」で二要素認証を実現。簡単操作の端末認証とログの証跡管理で、なりすましなど不正利用を防止。



企業

株式会社DMM.com証券 様

マイナンバー専用PCのセキュリティを高めるため、二要素認証のSmartSESAME PCログオンを導入。



企業

九州電力株式会社 様

セキュリティ強化のため、社員それぞれが使用するすべてのPCおよびシステム専用のPCを含めて約1万5000台以上の端末にSmartSESAME PCログオンを使用した二要素認証を導入。

お問い合わせ



株式会社シーイーシー
Computer Engineering & Consulting

〒108-6012 東京都港区港南 2-15-1 品川インターシティA棟12F
TEL:03-5783-3162 FAX:03-5783-3165
Email: cec-marketing@cec-ltd.co.jp
URL: https://www.cec-ltd.co.jp/

販売代理店