

[SmartSESAME
PCログオン システムのご紹介

株式会社シーイーシー
営業本部 首都圏営業部
2024年4月22日更新

多要素・二要素認証とは	2
PCログオンシステムとは	3
SmartSESAME 自治体の導入実績	4
導入実績の高いセキュリティサービス	5
SmartSESAME PCログオンとは	
PCログオンの特長	7
選べる認証方式	8
選べる管理方式	9
選べる管理方式	10
かんたん登録	11
かんたん登録	12
柔軟な運用	13
柔軟な運用	14
救済措置	15
ログオン履歴管理	16
PIN運用	17
ICカード認証機能	18
生体認証機能	19
ポリシー設定	20
スタンドアローン版／AD版の違い	21
動作仕様	22

Azure AD版

Azure AD版 エディション概要	24
クラウド上の管理機能	25
PCへの展開やログオン認証	26
動作環境	27

シングルサインオン（オプション機能）

シングルサインオンによる自動サインオン	29
スタンドアローン版／AD版の違い	30
シングルサインオンのシステム構成例	31
シングルサインオンの対象範囲	32

appendix AI顔認証システムについて

AI顔認証システムの特長	34
各種システムポリシー	35
利用シーン	36

2つの要素を組み合わせることでセキュリティを強化

多要素・二要素認証とは、PCを起動してIDとパスワードを入力し、さらに別の要素を組み合わせなければ認証できない方式のことです。認証するための“要素”は大きく下記の3つに分けられます。



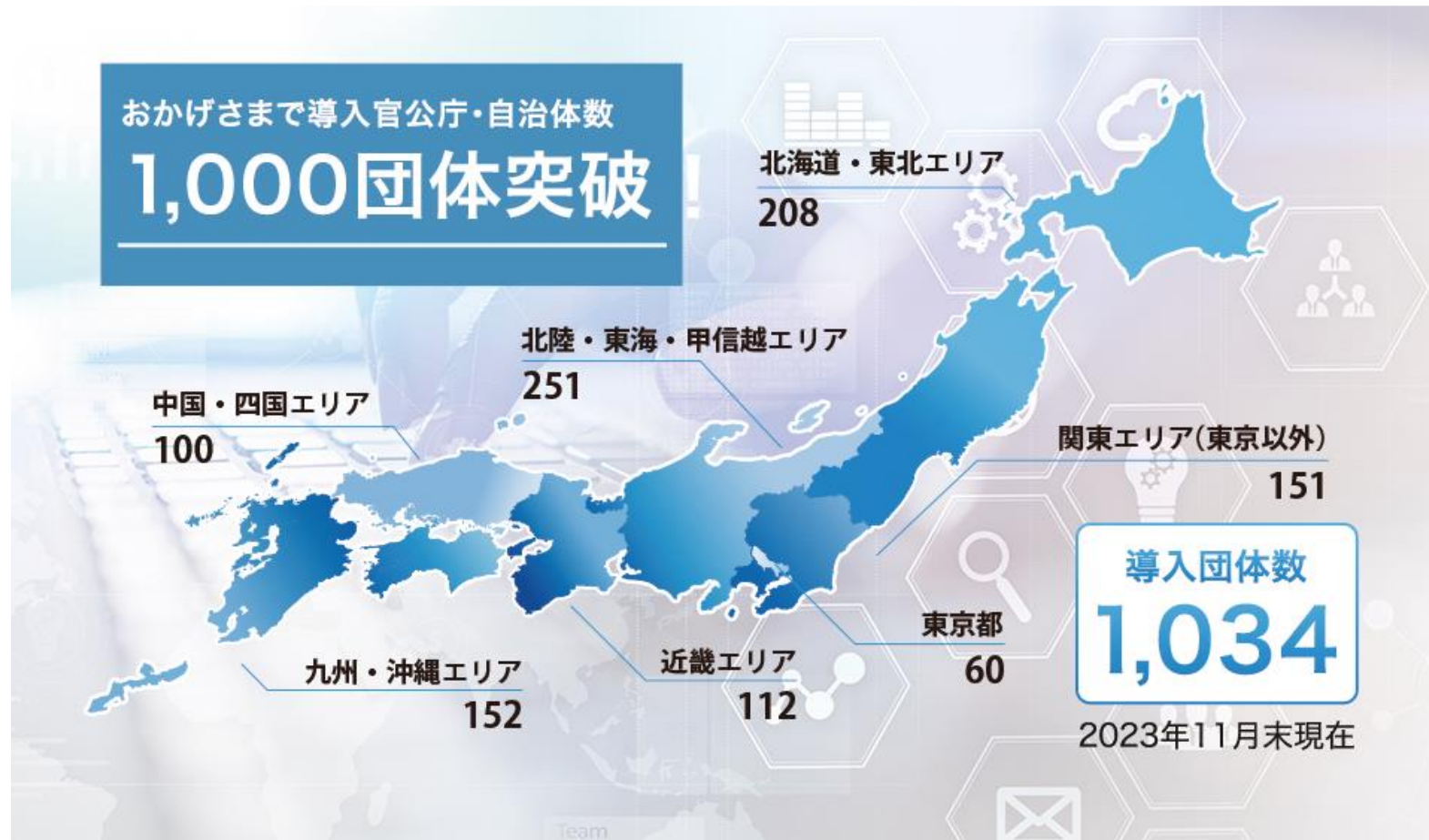
クライアントPCの不正利用と画面からの情報漏えいを防止

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。ICカードや生体認証でPCへログオンすることで、なりすましや不正操作による情報漏えいを防ぎます。



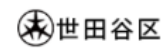
2015年3月に総務省が発表した『地方公共団体における情報セキュリティポリシーに関するガイドライン』の二要素認証にも対応できます。

SmartSESAME 自治体の導入実績



総務省

京都府



墨田区



安曇野市



お客様のセキュリティを支えるシーイーシーの **No.1** シリーズ

累計導入団体数と売上
2年連続 **No.1**

[SmartSESAME
PCログオン



売上シェア **70%**

[SmartSESAME
SecurePrint!



EDR対応メーカー数 **No.1**
(当社調べ)

Security Operation Center
CEC SOC[®]



SmartSESAME PCログオンとは



選べる認証方式・管理方式

- ICカードや顔・指紋・静脈など生体認証による二要素認証に対応
- Active Directory対応の集中管理、ワークグループ環境下のスタンドアローンにも対応

認証サーバー、ログサーバーレスで導入可能

- 集中管理する場合でも、Active Directory内で生体・カード番号の管理が可能
- 専任のサーバー担当者を設ける必要がないため管理負荷を軽減

登録・管理もラクラク

- 初期登録は、ユーザーが自分のPCで生体・Windowsアカウントを登録
- 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導入、管理負荷軽減を実現

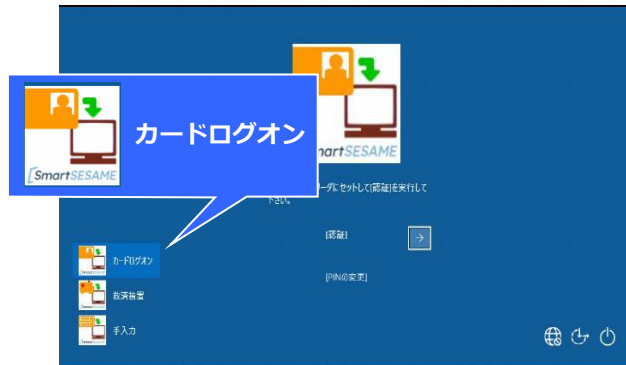
マイナンバーカードにも対応

- 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オンにも対応
※JPKIシリアル方式は現在開発中

ICカードや生体認証による多要素・二要素認証に対応

ICカードや顔・静脈・指紋などの生体認証で多要素・二要素認証の仕組みを取り入れることができます。テレワーク時にも、PCに多要素認証が入っていることでPCの紛失・盗難時の情報漏えいのリスクを解消。安心して作業を行うことが可能です。

ICカード認証



【ICカード認証】

登録済みカード以外は使用できません。

【本人認証】

PIN（暗証番号）による認証チェックを実施します。

※PIN(暗証番号) の入力を必要としないことも可能です。

生体認証



【本人認証】

生体情報による認証チェックを実施します。

顔認証はPC内蔵のWebカメラ及び外付けのWebカメラが利用可能です（WebカメラはSVGA以上が必要）。

指静脈認証または指紋認証が利用可能です（当社指定の認証リーダー以外は事前検証が必要）。

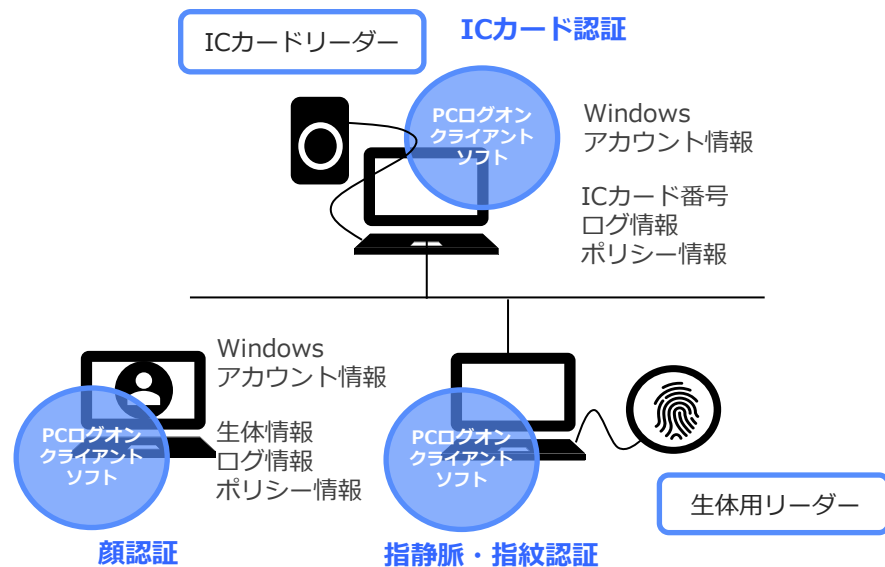
※顔認証はPIN(暗証番号) による認証も可能です。

Active Directory版、スタンドアローン版にも対応

Active Directory対応の集中管理、ワークグループ環境下のスタンドアローンにも対応しています。

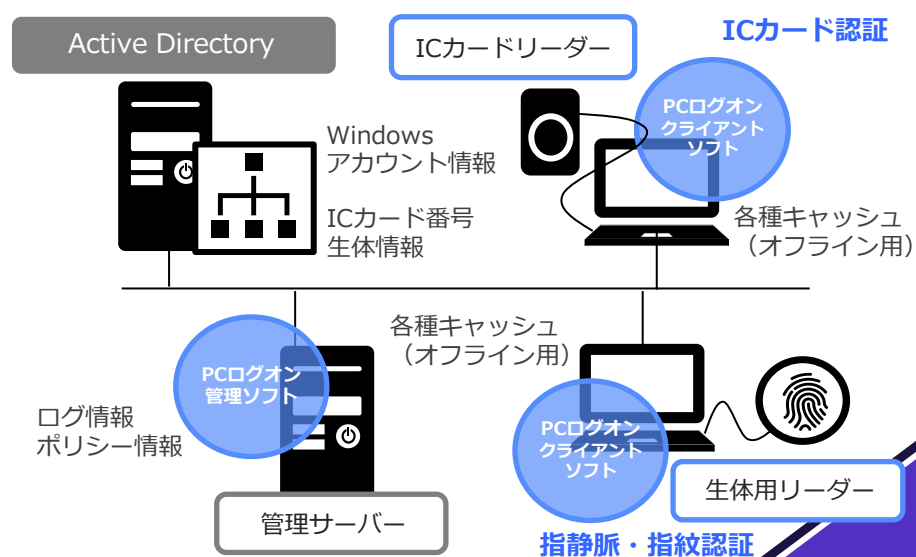
スタンドアローン版

全ての情報が利用者PC上で管理されます。各PC上でICカード番号/生体情報やポリシー情報を設定する必要があります。なお、PC単位に登録情報を変えることができます。
ログオン履歴はパソコンのWindowsイベントログに出力され、パソコンごとに管理・閲覧することができます。



Active Directory版

Active Directory内でICカード番号/生体情報を集中管理し、管理ソフトウェアにてICカード番号/生体データの登録、編集、削除などを行います。登録されている認証情報はドメイン傘下のどのPCでも利用可能です。各クライアントPCから出力されたログオン履歴を管理ソフトにて集中管理・閲覧することができます。



※Active Directory版であっても、正常接続時に保存されたキャッシュを使用して外出時やネットワーク断線時でもログオン可能です。

認証サーバー、ログサーバーレス

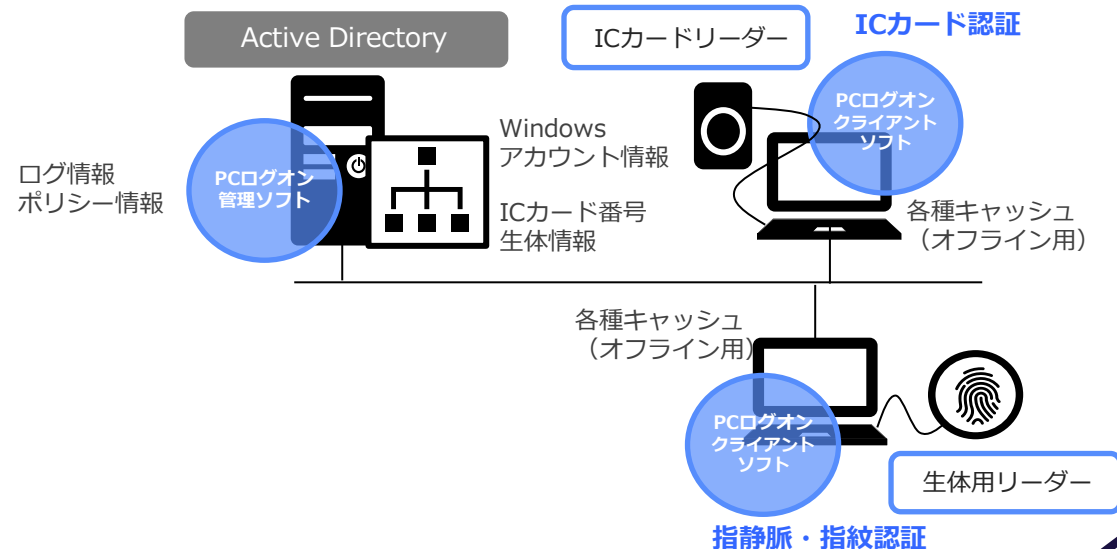
集中管理する場合でも、サーバーレスで導入できます。

管理ソフトウェアはADサーバーにもインストール可能です。
ログ情報・ポリシー情報は管理ソフトウェアをインストールしたサーバーで管理されます。

Active Directory版

Active Directory内でICカード番号/生体情報を集中管理し、管理ソフトウェアにてICカード番号/生体データの登録、編集、削除を行います。登録されている認証情報はドメイン傘下のどのPCでも利用可能です。

各クライアントPCから出力されたログオン履歴を管理ソフトにて集中管理・閲覧することができます。

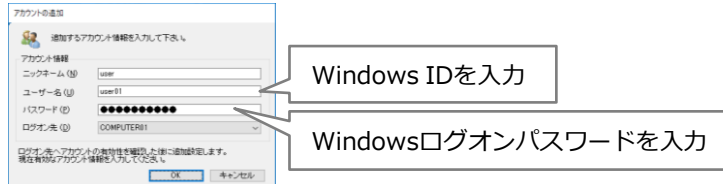


簡単な導入

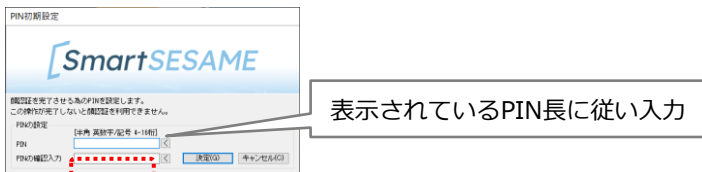
初回ログオン時（認証データ未登録時）は、自動的に認証データの登録処理となり、クライアントPC上で利用者自身が認証データを登録します。カード番号は管理者による一括登録も可能です。

Active Directory版

- ① 管理ソフトウェアで管理者がICカード番号を登録
- ② カードリーダードライバーをインストール
- ③ クライアントソフトをインストール
- ④ 「アカウントの追加」画面でログオンに必要なWindowsユーザーID/パスワードを入力



- ⑤ 「PIN初期設定」画面でPIN設定

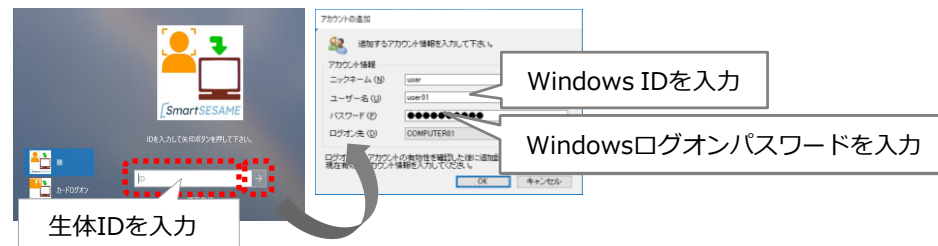


PINの最小桁数は管理者がSmartSESAME ポリシーにより0～16桁で設定します。
0桁のPINが設定されているカードの場合、PINを使用しない選択も可能
(空欄のまま [OK] 押下)

[決定] ボタン押下で初回登録完了

指静脈／指紋認証

- ① 管理ソフトウェアで管理者が生体ID（社員番号等）を登録
- ② 指静脈／指紋リーダードライバーをインストール
- ③ クライアントソフトをインストール
- ④ 生体IDを入力後、「アカウントの追加」画面でログオンに必要なWindowsユーザーID/パスワードを入力



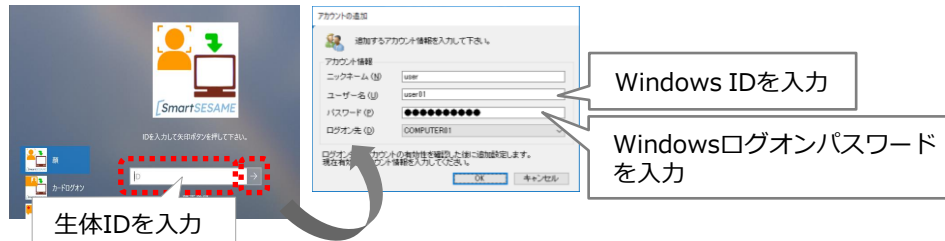
- ⑤ 生体情報を登録（最大5指まで）



[OK] ボタン押下で初回登録完了

顔認証

- ① 管理ソフトウェアで管理者が生体ID（社員番号等）を登録
- ② クライアントソフトをインストール
- ③ 生体IDを入力後、「アカウントの追加」画面でログオンに必要なWindows ユーザーID/パスワードを入力



- ④ 生体情報を登録

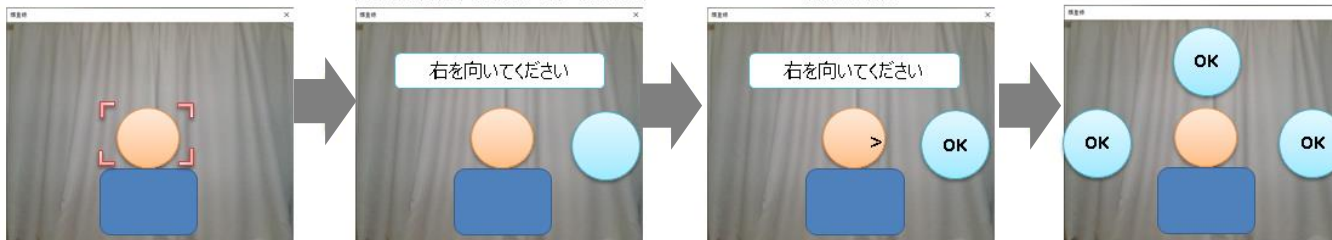
表示されるキャプチャ画面中央に顔を映す

画面に表示される指示に従い「右」を向く

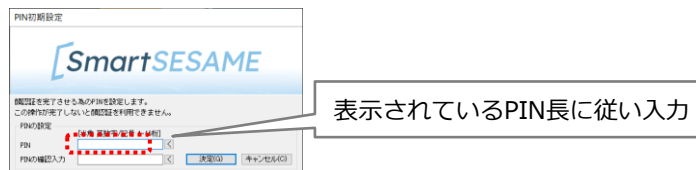
「右」向き判定OK

同様に画面の指示に従い「左」「上」「下」を向く

顔情報登録完了



- ⑤ 「PIN初期設定」画面でPIN設定



PINの最小桁数は管理者がSmartSESAME ポリシーにより0～16桁で設定します。0桁のPINが設定されているカードの場合、PINを使用しない選択も可能（空欄のまま[OK] 押下）

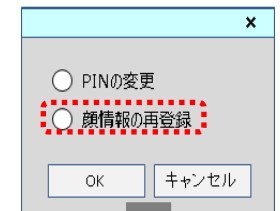
[決定] ボタン押下で初回登録完了

顔データの再登録

- ① 通常の顔認証 + PIN認証処理後、顔再登録の確認画面で「顔情報の再登録」を選択し、「OK」を押下



- ② 顔再登録の確認画面で「顔情報の再登録」を選択し、「OK」を押下



顔データの登録処理へ

ICカード認証と生体認証の併用

用途に応じて認証方法を柔軟に切り替えることができます。

通常の業務で使用するPC : ICカード認証 | セキュアな業務PC : 生体認証

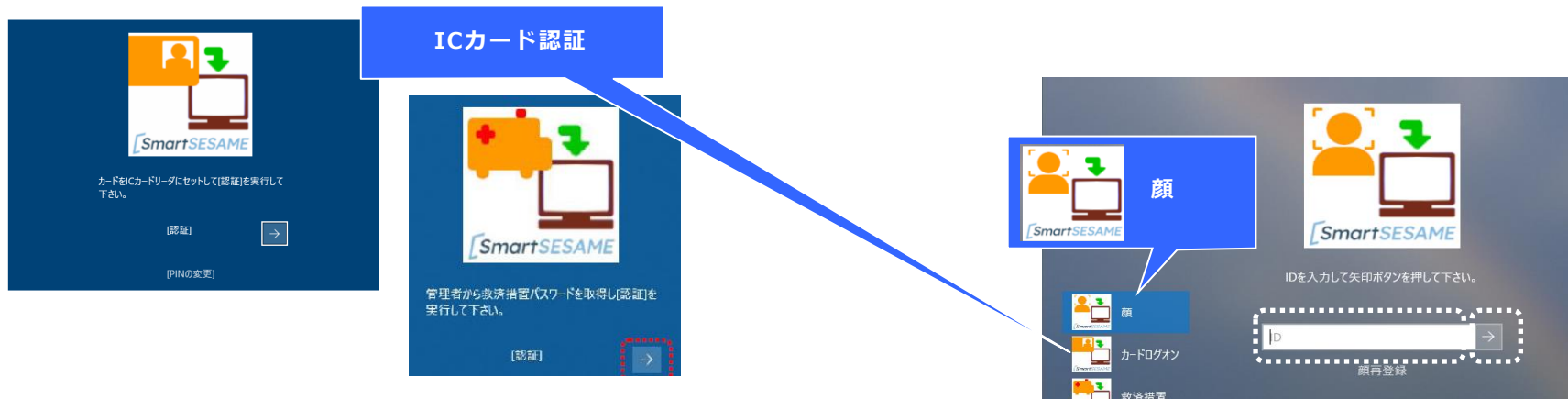
ICカード認証

1. ICカードのみ
2. ICカード + Windowsパスワード
3. ICカード + PIN (暗証番号)
4. ICカード + PIN (暗証番号) + Windowsパスワード

生体認証

1. 生体ID + 生体認証 (※)
 2. 生体ID + 生体認証 (※) + Windowsパスワード
 3. 生体ID + 顔認証 + PIN (暗証番号)
- ※生体認証 : 顔、指静脈、指紋

<ICカード認証と生体(例：顔) 認証併用イメージ>



ログイン画面左下の一覧より利用したいログイン方法を選択すると各認証画面に切り替わります。

スクリーンロック・ロック解除

- ・スクリーンロックの解除時にも「ICカード認証」や「生体認証」が必要となります。
- ・ロック後指定時間を経過すると強制ログオフを行うポリシー設定が可能です。ICカード認証においてカードを外してもロックしない運用および生体認証利用環境では、スクリーンセーバー解除後にPCがロック状態に遷移する設定を推奨します。

複数Windowsユーザーに対応

- ・1利用者（カードまたは生体ID）あたり、最大で5アカウントまで利用できます。
- ・複数の利用者が共有するアカウントも利用できます。

手入力ログオン

- ・[手入力]はポリシー設定により許可されたPCでのみ表示されます。



救済措置

- 手入力ログオンの利用を救済措置パスワード認証に成功した場合のみ利用可能とします。
- 救済措置パスワードは管理者により条件(コンピュータ名またはドメイン傘下共通、使用期間)を指定して 生成され、利用範囲や期間を限定した運用が可能です。(1ヵ月有効)
- 救済措置パスワードの生成と利用にはネットワークが繋がっている必要はなく、完全なオフライン環境でも運用が可能です。
- 生成された救済措置パスワードを利用者に通知し、利用者が救済措置パスワード認証に成功すると手入力ログオン画面が表示されます。



救済措置パスワード認証

管理者から通知されたパスワードを入力してください。

コンピュータ名 COMPUTER01

パスワード

OK キャンセル



管理者より通知された
救済措置パスワードを入力

アカウント情報を入力してログオンして下さい。

ユーザ名

パスワード

COMPUTER01

PCのログオン履歴を記録

- 「誰が」「どのPCから」「いつ」などのログオン履歴をログに記録します。
- 「PIN間違い」「カードロック」などの履歴をログに記録します。
- 「ICカード番号」または「生体ID」がログに記録される為、同一のWindowsユーザを複数の利用者で使用している場合でも本人を特定できます。
- 記録されたログは、Active Directory版では管理ソフトウェアに収集され、スタンドアロン版ではPC上のWindowsイベントログ(Applicationログ)に保存されます。
- 履歴の保持期間は任意に設定できます。

管理ソフトウェアのログオン履歴確認画面

The screenshot displays the 'SmartSESAME PCログオン マネージャ' (SmartSESAME PC Logon Manager) application. The main window shows a list of logon events for the date 2017/11/08. The list includes columns for '区分' (Category), '日付' (Date), 'ソース' (Source), 'ユーザ' (User), 'コンピュータ' (Computer), and '内容' (Content). A search filter dialog is open, allowing users to filter logs by '区分' (Category), '日付' (Date), 'ソース' (Source), 'ユーザ' (User), and 'コンピュータ' (Computer). The dialog also includes a 'ログ表示設定' (Log Display Settings) section with checkboxes for '詳細' (Detailed), '警告' (Warning), and 'エラー' (Error). A curved arrow points from the search filter dialog to the main log list.

ログの表示設定で絞り込み・検索が可能

CSVファイルへのエクスポートが可能

PIN（暗証番号）間違いによるロック

- 複数回連続でPIN（暗証番号）を間違えた場合、ICカード／生体情報がロックされ使用できなくなります。
- ロックされたICカード／生体情報は管理機能よりロック解除が行えます。

柔軟なPIN運用が可能

- PINには最小桁数や複雑さ、失敗許容回数、履歴数などのルールを設けることができます。
- PINを使用しない設定も可能です。
- PINには有効期限を設定する事ができ、PINの残された有効期間が設定する警告日数より短くなった場合、PIN の変更を促すメッセージを表示できます。
- 利用者がPINを失念した場合、管理機能によるリセット操作を行います。

発行済みICカードに対応

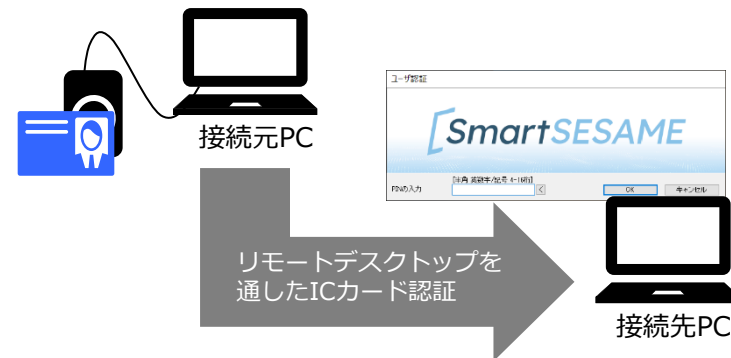
- ・マイナンバーカードや社員証等の発行済みのICカードも利用できます。詳細はご相談ください。
- ・ICカードを一意に認識する番号として、ICカードの中に書き込まれた社員番号等も利用できます。

失効処理・カード忘れ対応・有効期限設定

- ・ICカードの紛失や盗難時にも利用停止処理で、ICカードの悪用を防ぎます(Active Directory版のみ)。
- ・利用者がICカードを忘れた場合は、2通りの方法で対応できます（併用可）。
 - ① **救済措置パスワード方式**：緊急時の救済措置パスワード認証を経てアカウントを指定してログオン
 - ② **スポットカード方式**：スポットカードで認証
- ・事前に利用期間が分かる場合は、ICカードの有効期限を設定することで、安全に利用管理できます。

リモートデスクトップを通したICカード認証が可能

- ・PCログオンがインストールされたPCにリモートデスクトップでログオンする際、接続元のPCに接続されたICカードリーダーを使用して接続先のPCに対するICカード認証を行うことができます。
(指静脈・指紋認証は使用できません)



利用可能な生体認証及びデバイス

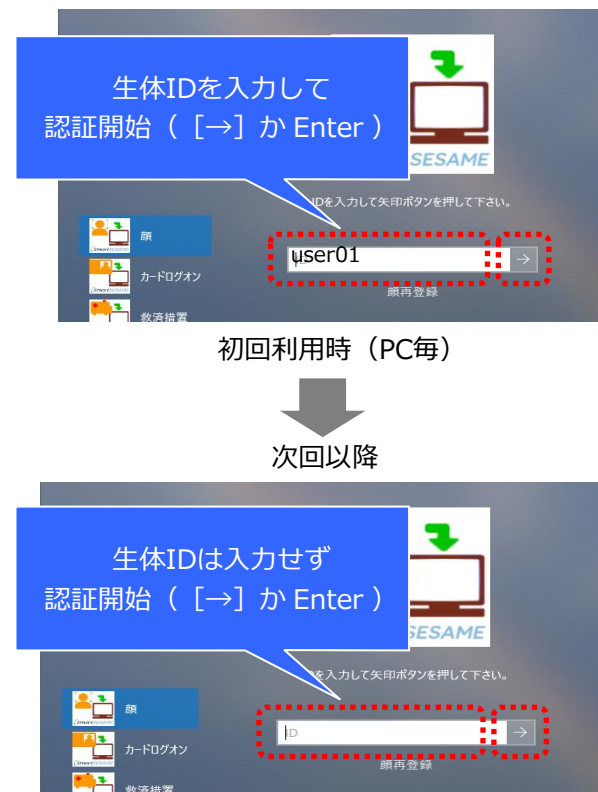
- 顔認証には、SVGA以上のWebカメラを使用します。認証情報には特徴点を抽出した独自のデータを利用します。また、顔写真等によるなりすまし防止対策やマスク対応も行っています。
- 指紋または指静脈を使用した生体認証が可能です。
(当社指定以外の指紋センサーを利用する場合、評価用ソフトウェアを使用して事前に検証いただく必要があります)

利用者の識別

- 利用者ごとに一意となる識別子(生体ID)を付与し、これに生体情報やログオンに使用するアカウントを紐づけます。
- 生体情報登録時や認証時はこの生体IDを画面に入力して登録/認証を行います。過去そのPCで認証された生体IDは入力を省略することができます。

生体情報の登録や更新

- 利用者の生体情報登録は初回利用時にクライアントPC上で行います。
- 認証しづらくなった場合、クライアントPC上での利用者による再登録や、管理機能からクリアすることが可能です。
- 生体情報をクリアした場合、次回利用者による再登録を行います。



ポリシー設定

- PCログオンの各種動作を決めるポリシーを設定します。
- システムポリシー(Active Directory版のみ)にはシステム全体に一律に適用するポリシーを設定、ローカルポリシーにはPC個別に対して適用するポリシーを設定します。
- システムポリシーとローカルポリシーがマージされたものがPCに適用されます。

●ポリシーの例

項目	設定内容
ICカード認証でログオンした後、カードをICカードリーダーから外した時の動作	ロックする or ロックしない
ICカード認証や生体認証を行わない手入力によるログオン	許可する or 許可しない
同じアカウントを紐づけた別のカード(利用者)によるロック解除	許可する or 許可しない
PINに関する条件	最小桁数や複雑さ、PIN履歴の記録有無(再利用制限)、ロックするまでのPIN認証失敗回数 etc.
生体情報の条件	認証時の厳しさを1~3段階(低~高)で指定できます。指紋/指静脈を登録する最低指数 etc.
Active Directory版におけるキャッシュに関する条件	キャッシュ保存最大数、有効期間 etc.

スタンドアローン版／AD版の違い

項目	スタンドアローン版	Active Directory版
利用者情報の管理	各クライアントPCのHDD上	Active Directoryに作成する専用領域内 (スキーマ拡張必要なし)
ログオン可能PC	利用者情報を事前に登録したPCのみ	ドメイン環境内であればどのPCでも可能
ログの管理場所	PCのWindowsイベントログ (Applicationログ) へと出力	管理ソフトにて集中管理
Active Directory環境	任意	必須

クライアントOS	Microsoft Windows 10 Pro(32/64bit) Ver.21H2以降22H2まで Microsoft Windows 10 Enterprise(32/64bit) Ver.20H2以降22H2まで Microsoft Windows 11 Pro(64bit) Ver.21H2以降23H2まで Microsoft Windows 11 Enterprise (64bit) Ver.21H2以降23H2まで ※ 法人（ビジネス）向けの日本語版OSのみサポート対象です。 ※ Microsoft Windows 10 Education、Enterprise LTSC 2015/2016、LTSC 2019等、上記に記載のないOS、 及びシンクライアント環境についてはお問合せください。 ※ Microsoft Windows RTはサポート対象外です。 ※ 顔認証における対象OSは64bitのみとなります。
管理ソフトOS	Microsoft Windows Server 2012 Standard/Datacenter(64bit) Microsoft Windows Server 2012 R2 Standard/Datacenter(64bit) Microsoft Windows Server 2016 Standard/Datacenter(64bit) Microsoft Windows Server 2019 Standard/Datacenter(64bit) Microsoft Windows Server 2022 Standard/Datacenter(64bit) ※ 日本語版OSのみサポート対象です。 ※ 上記に記載のないOSについてはお問い合わせください。
ICカード	Sony社規格FeliCa（IDm、ユーザエリア[セキュリティ領域除く]） NXPセミコンダクタ社規格Mifare Standard 1K/4K（UID、ユーザエリア）
ICカードリーダー	Sony PaSoRi RC-S380/S、RC-S300/S、RC-S300/S1
指静脈センサー	mofiria FVA-U4ST、日立 PC-KCA110
指紋センサー	弊社指定外付け指紋リーダー（パソコン内蔵指紋リーダーについてはお問い合わせください）
顔認証用カメラ	Webカメラ（SVGA以上の解像度、30fps以上のフレームレート、カラー）
シングルサインオン対応ブラウザ	Internet Explorer、Microsoft Edge、Google Chrome

※ 既にPCログインを運用中の環境における各OSバージョンに対する当製品のサポート期限について、Microsoftによるサポートが終了してから1年後までとします。尚、Microsoftによるサポート終了後に新たに確認されたOSの不具合など、内容によっては上記期限内でも対応できない場合があります。

Azure AD版

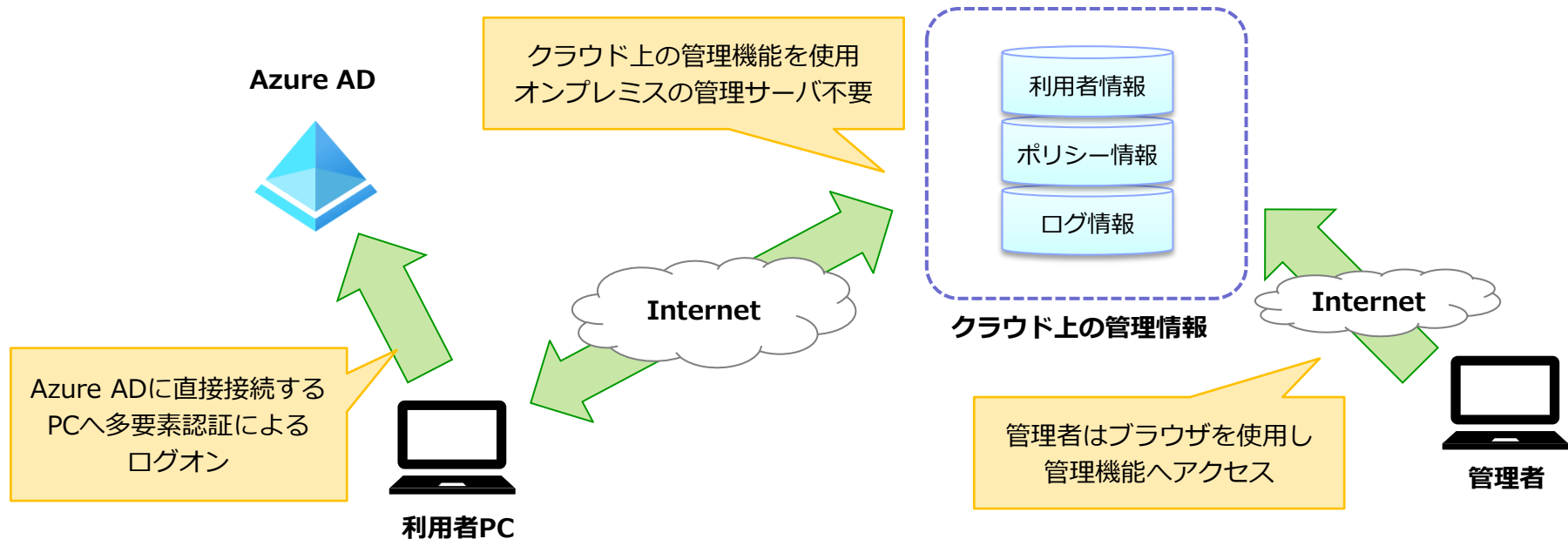
Azure ADに直接接続するPCに多要素認証によりログイン

Azure ADに直接接続するPC環境(Azure AD Join)に多要素認証を使用してログインします。

管理機能はクラウド上に用意される管理機能を使用し、オンプレミスの管理サーバは必要ありません。

管理者やブラウザを使用し、クラウド上の管理機能を利用します。

エージェントをインストールするだけでクラウド上の管理情報と連携し多要素認証によるPCへのログインを開始できます。

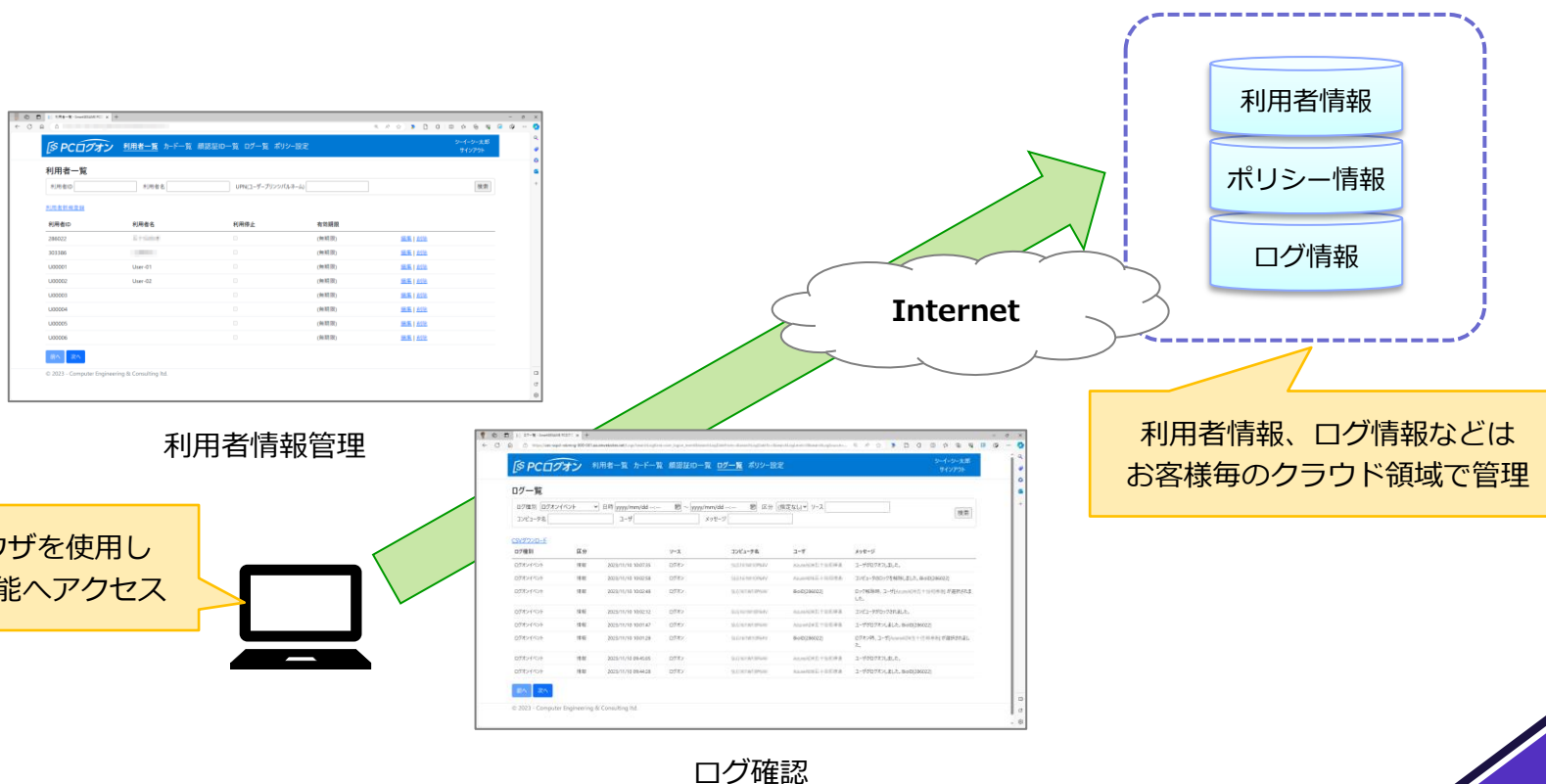


クラウド上の管理コンソールを使用し管理業務を実施

クラウド環境上にお客様用の管理コンソール、管理情報領域を用意します。

管理者はブラウザを使用して管理コンソールにアクセスし、利用者情報の登録やポリシーの設定などをします。

PCへ多要素認証によりログオンした結果も管理コンソール上でログとして確認できます。



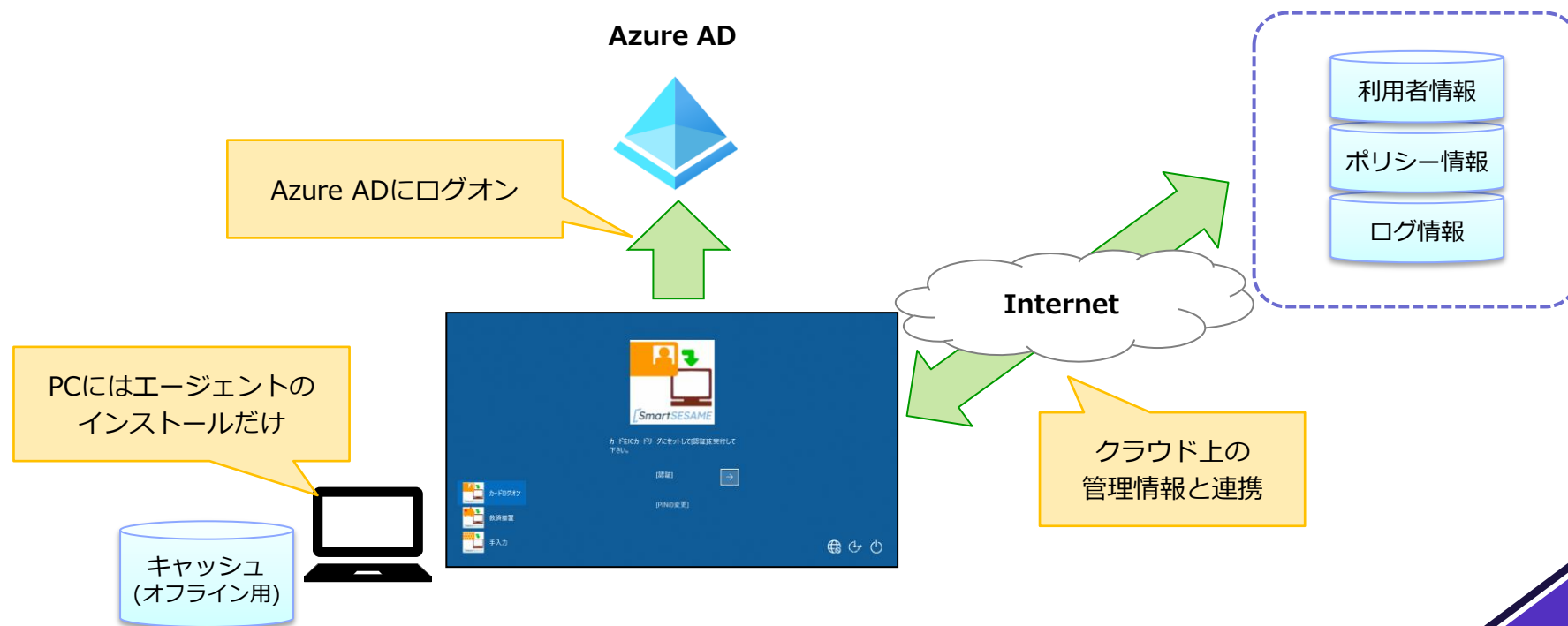
簡単なPCへの展開、Azure ADへのログオン

PCへはエージェントをインストールだけでセットアップは完了し、複雑な手順は必要ありません。

クラウド上の管理情報を参照し多要素認証によりお客様の用意するAzure ADにログオンします。

ログオンに関する履歴はクラウド上に収集されます。

カード認証+知識要素、または顔認証+知識要素に対応します。(今後、指紋や指静脈へも拡張予定)



Microsoftのサポートするブラウザ、Windows 11環境をサポート

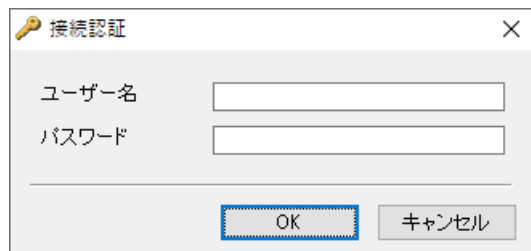
- ・管理業務を行うブラウザMicrosoft Edge
(Chromium対応版以降)
- ・クライアント
Windows 11 Pro/Enterprise 64bit (MSサポートバージョン下限～23H2)

※ 「Azure AD」は2023年夏以降で「Microsoft Entra ID」に名称を変更していますが当製品に影響はありません。

シングルサインオン（オプション機能）

サイト／アプリケーションへの自動サインオン

シングルサインオンに登録されたアプリ／サイトのログイン画面が表示された際、PCへのログインユーザーに対して登録されたサインオン情報より自動的にアプリ／サイトの入力フィールドへの自動入力とログイン操作を行います。（※サインオン情報：対応するアプリ／サイトに対するユーザーID、パスワード等）

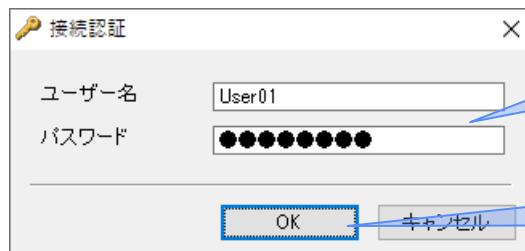


接続認証

ユーザー名

パスワード

OK キャンセル



接続認証

ユーザー名 User01

パスワード ●●●●●●●●

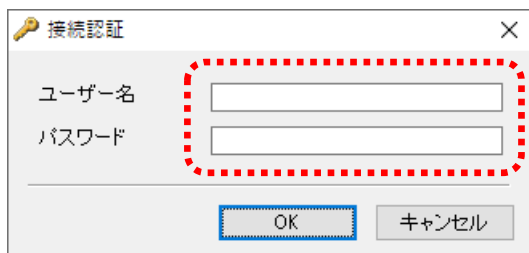
OK キャンセル

入力フィールドへの自動入力

ログインボタンの自動押下

入力フィールドのロック（Edge、Chromeは非対応）

対象アプリケーションが起動された際、入力フィールドを無効化し、手入力による不正なサインオンを防ぎます。

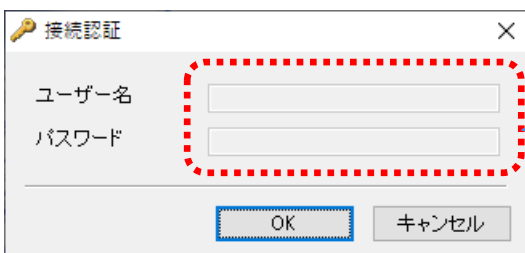


接続認証

ユーザー名

パスワード

OK キャンセル



接続認証

ユーザー名

パスワード

OK キャンセル

入力フィールドのロック

スタンドアローン版／AD版の違い

項目	スタンドアローン版	Active Directory版
アプリ／サイト情報の管理	各クライアントPCのHDD上	管理ソフトウェアにて集中管理 各クライアントPCのHDD上 ※併用可
サインオン情報の管理	各クライアントPCのHDD上	Active Directoryに作成する専用領域内 (スキーマ拡張必要なし)

※ログやポリシーの管理およびActive Directory環境要否についてはPCログオンと同じです。

対応ログイン画面

- Windows 32bit/64bitアプリケーション
- Webページ (ブラウザはInternet Explorer、Edge、Chromeが対象)
- Web基本認証や「Windows セキュリティ」画面

【注意事項】

SingleSignOnの適用には各アプリ／サイトへの事前検証が必要になります。

ログイン画面の構成によっては対応できない場合があります、以下については特に注意が必要です。

- 画面が動的に変わるような画面
- 入力欄にカスタムコントロールが使用されている画面
- 入力欄へのフォーカスイベント／入カイベントで処理を制御をしている画面
- Adobe Acrobat関連ソフトウェアのログイン画面 等

また、以下については対応できません。

- Java/Javaアプレットのログイン画面
- コンソールアプリケーション画面
- Active Xコントロール内の入力欄

appendix

- ・ AI顔認証システムについて

1

認識精度となりすまし防止

本人認識率99.73%、マスク着用時も98.5%と高い認識精度を実現します。顔写真を使用したなりすまし防止が可能になり、マスク着用時のなりすまし防止にも対応します。

2

PC内蔵Webカメラに対応

PC内蔵のWebカメラおよび外付けのWebカメラが利用できます。認証用のリーダーを用意する必要がなく、低コストで顔認証を導入できます。

※カメラはSVGA以上の解像度が必要となります。

3

顔認証 + PIN (PW) の二要素認証

利用者個人のみが知るPIN番号を必要とする認証も可能です。一定回数PIN間違いをすると認証情報がロックされ、以後ログオンできません。

4

ICカード認証との併用可

顔認証の端末とICカード認証の端末が混在する環境でも一元管理可能です。



顔認証レベル

生体認証における顔認識のレベルを[1～3]で指定します。
数値が大きいほど厳しくなります。



なりすまし防止レベル

生体認証におけるなりすまし防止のレベルを[1～3]で指定します。
数値が大きいほど厳しくなります。



顔登録モード

顔登録時における顔の撮影モードを指定します。

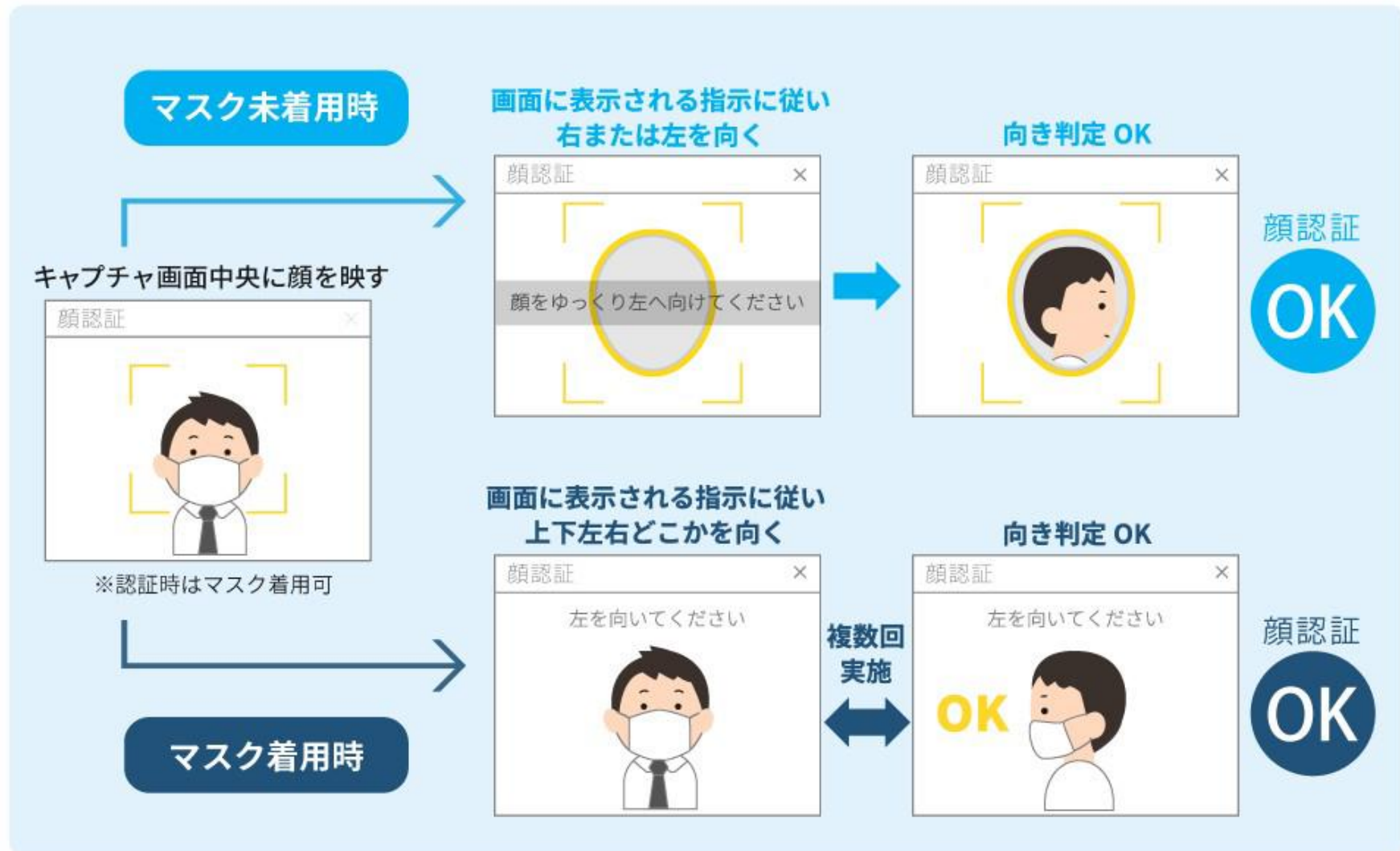
[標準]正面、上下左右(5個)
[簡易]正面のみ(1個)



マスク認証許可

マスクを着用した顔認証を許可するか否かを指定します。







Computer Engineering & Consulting

【 お問い合わせ先 】

株式会社シーイーシー

営業本部

首都圏営業部

連絡先: 03-5783-3162