アクセスマネジメント・ソリューション

かんたんセキュリティモデル

特許出願済※1　新商品

特　長

- 1台の手のひら静脈認証で全PCのセキュリティを強化します。
- PCやサーバの設定変更が不要(※2)なため、導入時のリスクを回避できます。
- PCやサーバ毎の認証ソフト・生体認証機器が不要な為、低コスト、短期導入できます。

(※2) スタンドアロンでご利用の場合、ActiveDirectoryへ参加する必要があります

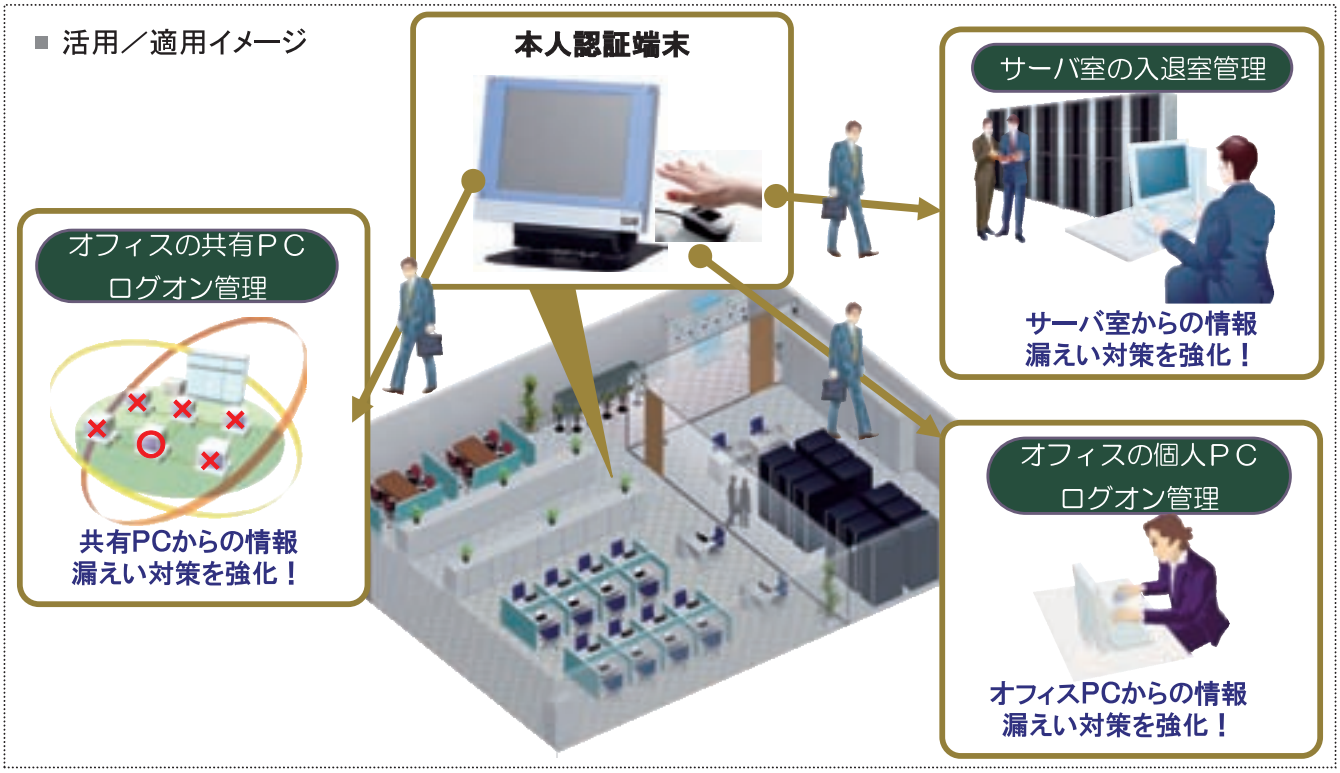
概要

PCやサーバからの情報漏えいを抑止するためには、ログイン認証に本人を特定できる本人認証の導入が有効です。『アクセスマネジメント・ソリューション　かんたんセキュリティモデル』では、既存のPC・サーバのログイン認証環境はそのままに、事務所やサーバ室の入り口に専用の本人認証装置を設置しユーザーアカウント情報と連携させるだけで強固なセキュリティ対策を実現できます。

PC、サーバ毎の認証ソフトが不要になるため、室内で何台ものPCやサーバを運用するコールセンターやサーバルーム、重要情報を扱うオフィスルームなどで、強固なセキュリティを低コスト・短期で導入したいお客様に最適です。

特許出願済

■ 活用／適用イメージ



※1　本資料中、特許出願済 表示箇所については特許出願済の技術を含みます。

かんたんセキュリティモデルの特長

サーバに影響を与えずユーザー認証を強化

・サーバへの特別なソフトや機器の導入はなし。

・Active Directory経由でログイン権限を操作。

・Windows以外のOSや特殊なOSを搭載した機器でも、ディレクトリサービス（Active Directoryなど）と　認証可能なOSであれば対応可能。

手のひら静脈認証連携しユーザー認証を強化

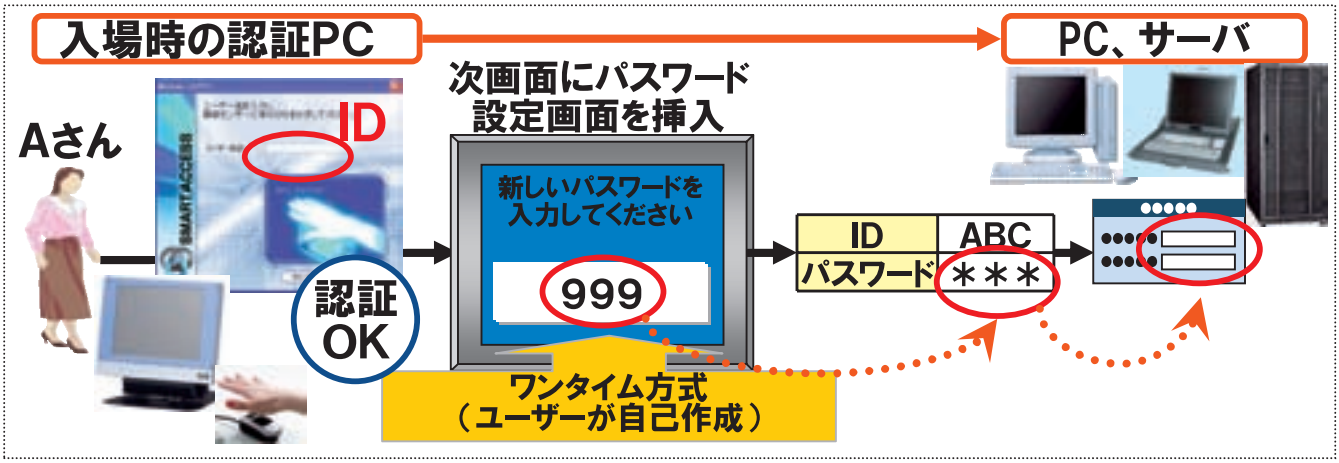
・ログイン権限があるユーザーでも、手のひら静脈認証をしないとログインできません。

・第三者が共連れ入室でき、かつ、正規利用者のログイン情報を入手できていても、本人の認証履歴がないため悪用できません。

想定される利用シーン

共有PC、サーバのパスワード定期変更で不正アクセスを抑止

手のひら静脈認証による個人識別後に、ユーザー自身が任意にかんたんなパスワードを設定できます。
⇒アカウントが「有効」な状態でも、パスワードが盗まれにくく、不正ログインを防止できます。
⇒退場時または一定時間経過後にアカウントを「無効」にするため、かんたんなパスワードでも安心です。
共有端末、サーバの運用ではユーザーに徹底が困難だった「パスワードの定期変更」が実現でき、高度なセキュリティを確保できます。



Green Policy Innovation　環境貢献への取組みはこちら：http://jp.fujitsu.com/about/csr/eco/green-it/index.html

株式会社富士通エフサス
販売推進統括部
〒105-0011 東京都港区芝公園4-1-4　メソニック38MTビル
フリーダイヤル：0120-860-242
詳細をご覧いただけます。 http://jp.fujitsu.com/fsas/

2009．5