vFORUM 2019

NS419

仮想化環境にもパスワードレスを！
多要素認証で実現する
エンドポイントセキュリティ

石川 竜雄

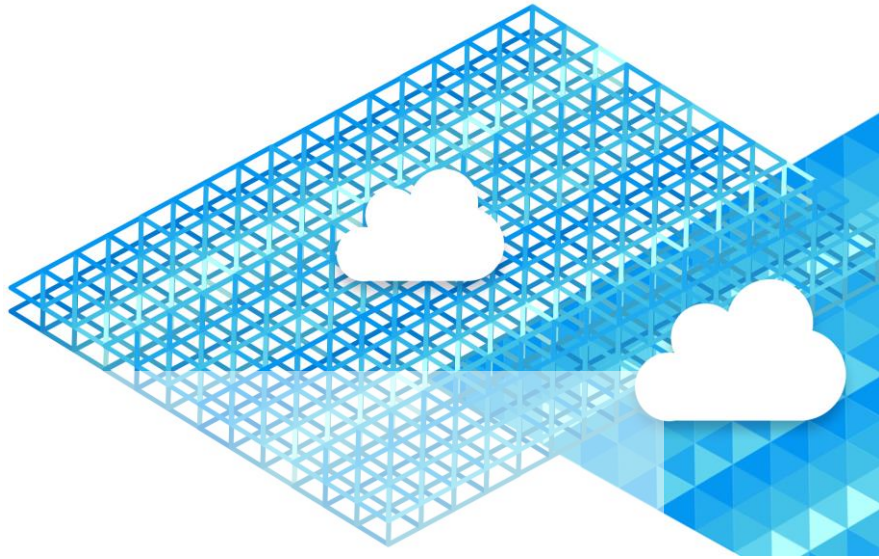
株式会社ディー・ディー・エス

営業本部 販売促進部

部長

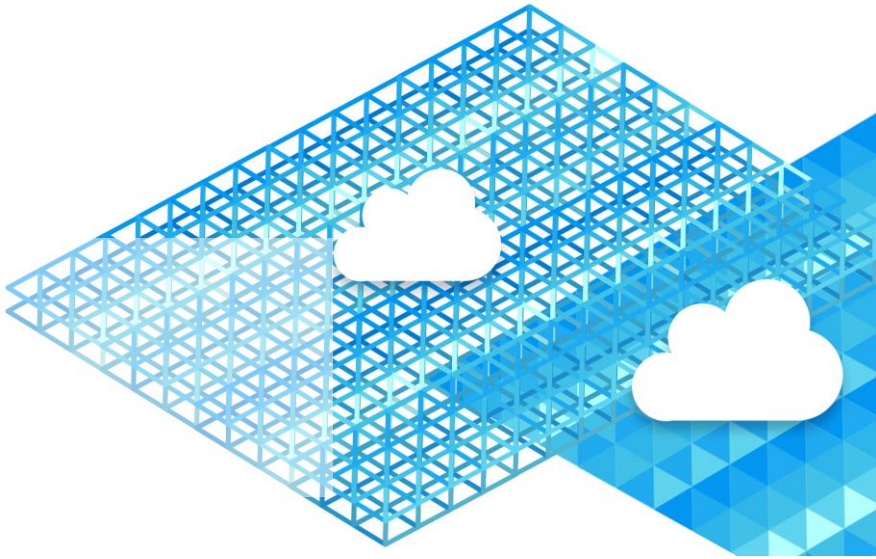
vmware

Agenda



- DDSはどんな会社？
- デジタルトランスフォーメーション
- 仮想化セキュリティの盲点
- パスワードだけに頼る認証との決別
- 多要素認証基盤のアップデート情報

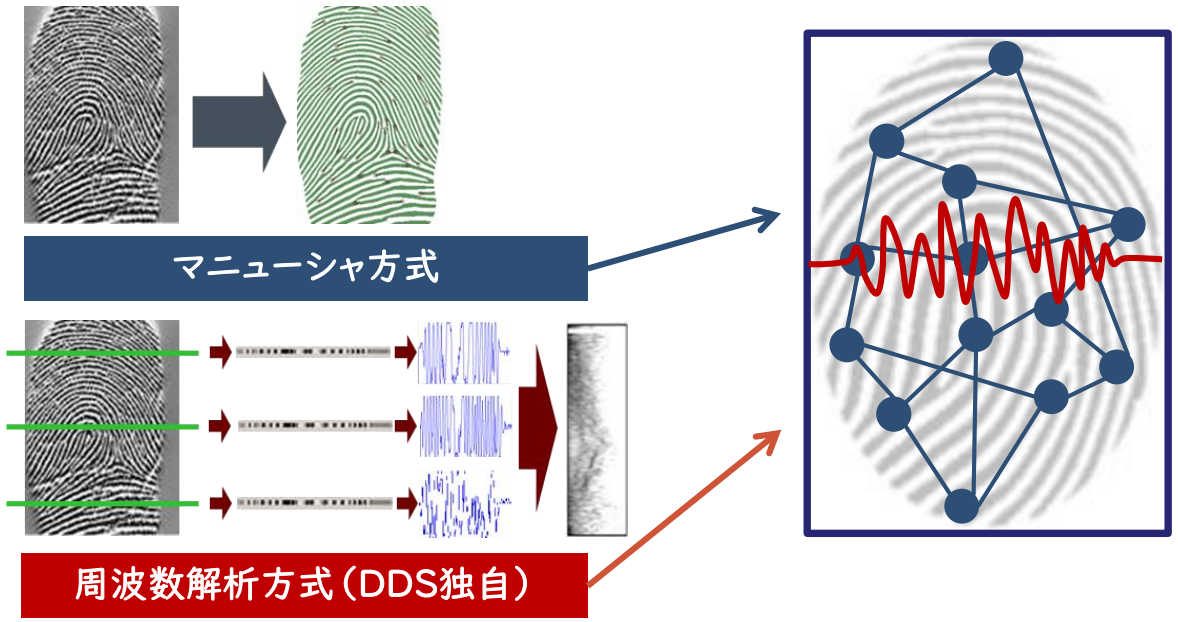
DDSはどんな会社？



DDSとはどんな会社？

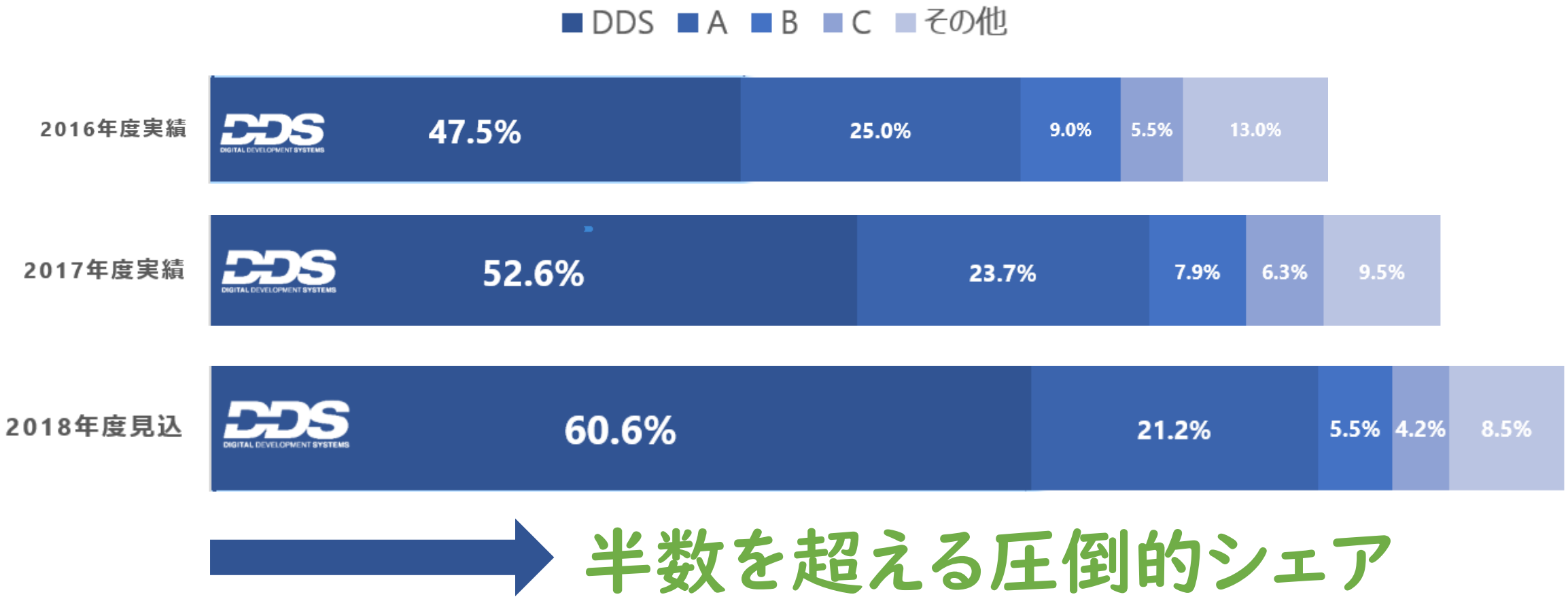
指紋認証アルゴリズムと多要素認証ソリューションを開発・販売する会社

ハイブリッド指紋認証方式



多要素認証ソリューション

こんなに使われてます（PC向け指紋認証シェア推移）

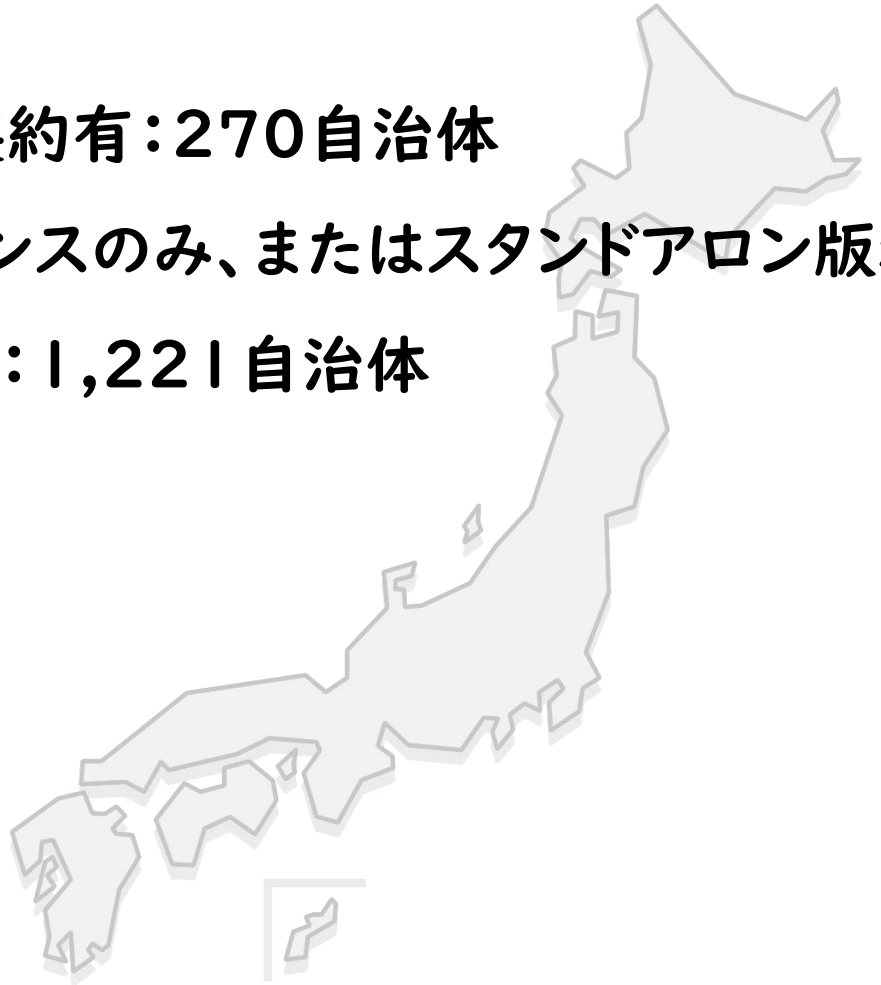


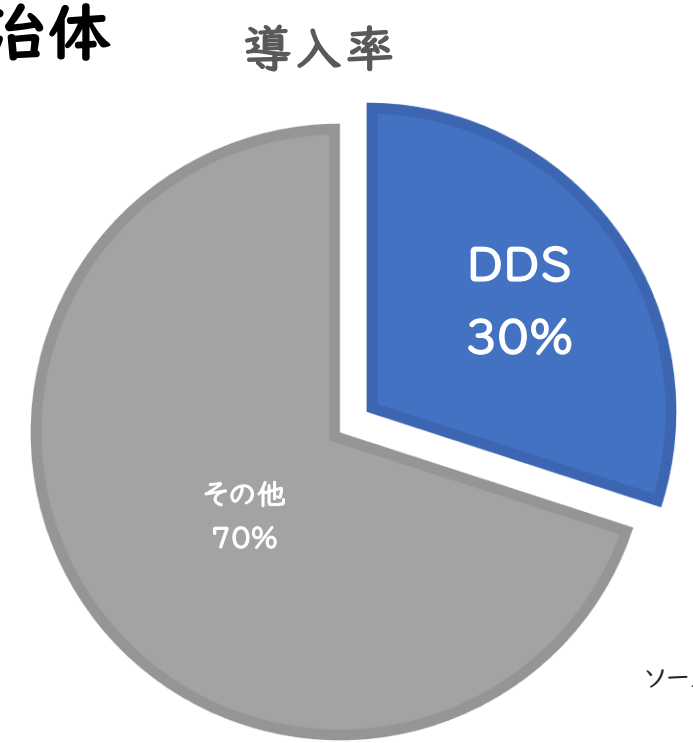
半数を超える圧倒的シェア

出典：富士キメラ総研『2018ネットワークセキュリティビジネス調査総覧』（2016年実績は『2017ネットワークセキュリティビジネス調査総覧』）

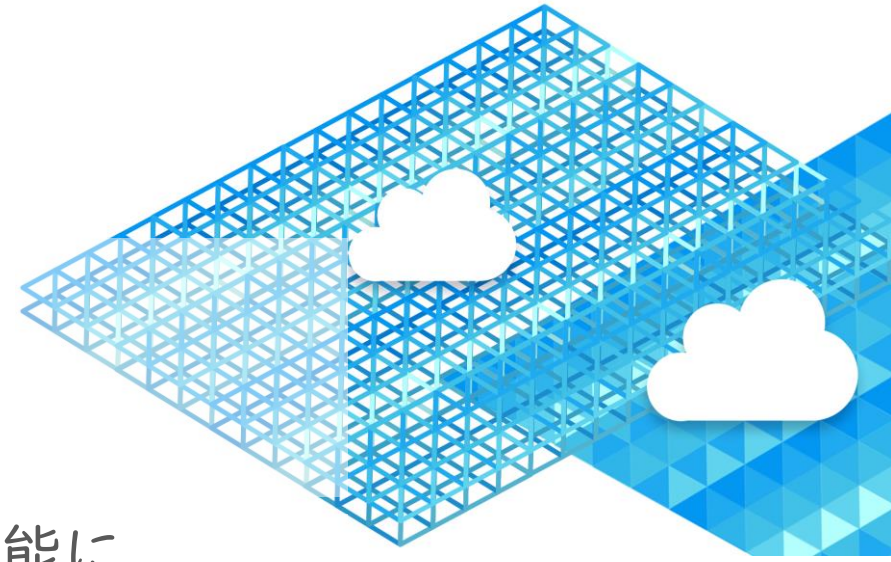
こんなに使われてます（自治体での市場占有率）

- 保守契約有：270自治体
- ライセンスのみ、またはスタンドアロン版利用：250自治体
- その他：1,221自治体





ソース：DDS調べ



デジタルトランスフォーメーション

DXにより、いつでも、どこでも、どのデバイスでも仕事が可能に

DX → いつでも、どこでも、どのデバイスでも

モバイルワーク

在宅勤務

サテライトオフィス

- 働く場所: オフィス→どこでも
- さまざまなデバイスの利用
- 雇用形態の多様化

デジタルトランスフォーメーションによって「いつでも、どこでも、どのデバイスでも」仕事ができる環境が整えば、テレワークなど多様な働き方が可能に

セキュリティ対策が考慮されていないDXはリスク大

アクセスするデータには、極めてセンシティブな個人情報や機密情報が含まれることもあり、不正アクセスや漏えいなどから守る厳重なセキュリティ対策を確立しておくことが必須要件。

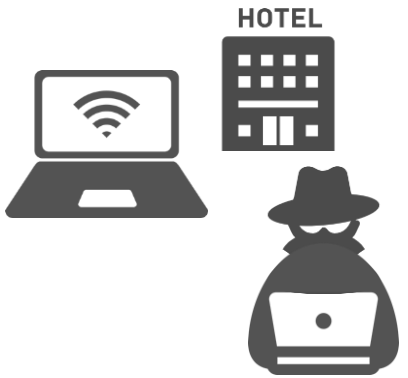
不正アクセスや漏えいのリスク

オフィス外からの情報システム利用に対する脅威 は、オフィス内での利用とは異なり、

上司・同僚の目が届かず、**利用者（社員）個人の注意やモラルに依存**

端末の紛失・盗難

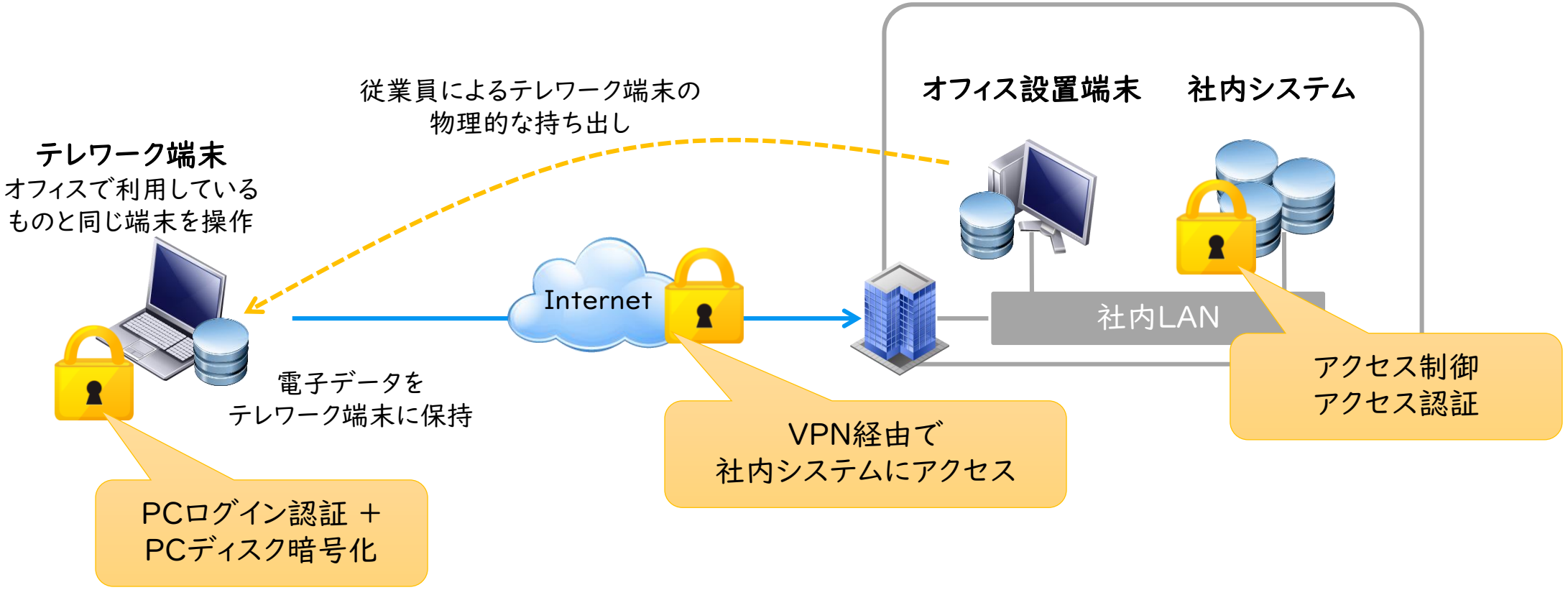
ファイルのローカル保存



Wi-Fi環境の悪用

共有ソフトの利用

セキュリティ強化ポイント（端末持ち出し）



VDI導入を検討する背景

働き方改革への取り組み
（テレワーク推進）

業務システム延命

情報漏えい対策

デスクトップ
仮想化

Windows 7／
Windows Server
2008のサポート終了

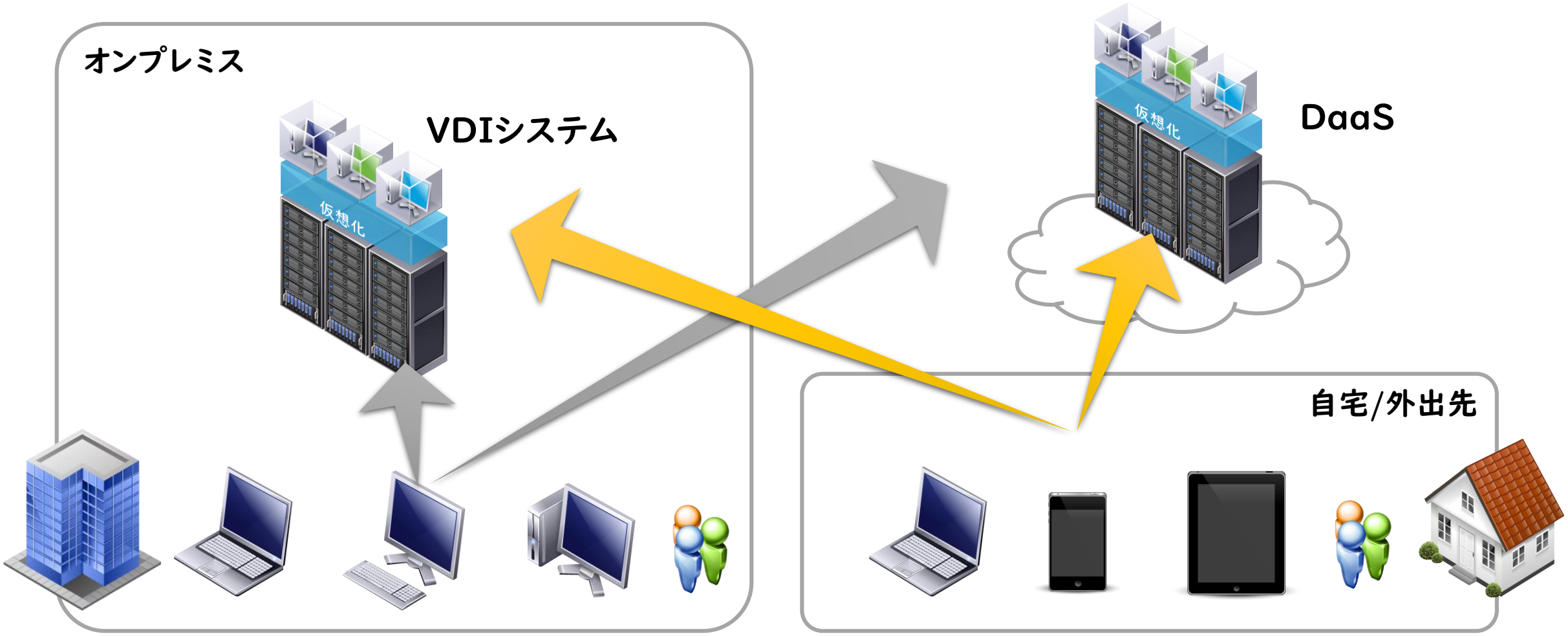
個人情報保護対策として、
ネットワークの分離

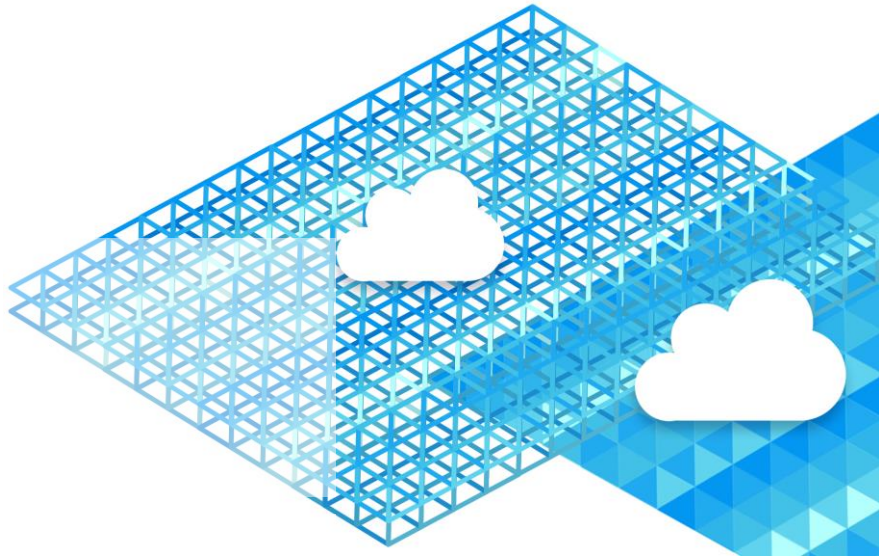
PC管理作業＆
コストの削減・

法規制／
ガイドライン対策

事業継続性対策

オフィスからの解放を現実にするデスクトップ仮想化

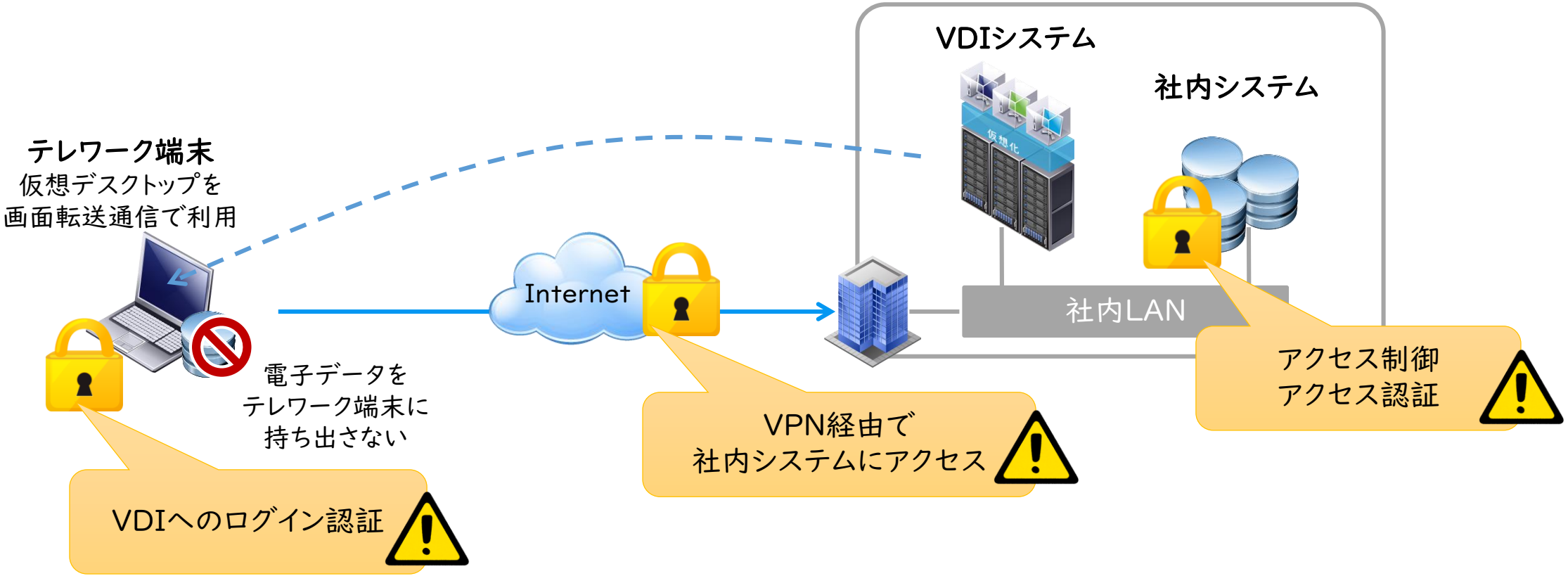




仮想化セキュリティの盲点

仮想化の進展で浮かび上がるパスワード認証の課題

VDI方式なら安全？ 仮想化のセキュリティ盲点



利用者のID／パスワードが破られたり、漏えいした場合、
様々な情報システムへの侵入を許し、大量の情報が外部へ流出することに。

パスワードによる認証

パスワードに対する攻撃手法

- 総当たり攻撃・フレーズ推測攻撃
- リスト攻撃
- システム脆弱性を利用したパスワード漏えい
- ネットワークの盗聴
- ソーシャルハッキング・ショルダーハッキング

企業が現実的にとれる対策

- ソフトウェア更新・設定の見直し
- セキュリティソフトの導入
- 安全性の高いネットワークの利用
- 従業員の教育、パスワードポリシーの徹底

強度の高いパスワード
- ランダム性
- 文字・数字・記号を混在
- 長い文字数

パスワードの運用
- 使いまわさない
- 紙などに記録しない
- 定期的に変更 (と言われていた)

どれかひとつにでも抜け道があると安全性は担保されません

安全なパスワードは難し過ぎて自分さえログインできない

強度の高いパスワード
- ランダム性
- 文字・数字・記号を混在
- 長い文字数

8桁　大小英字、数字、記号混在パスワード

mK2+phVy	,Dx4FSq(	E9h|%KPZ	qK6/+_,e
i)X7*P9L	(Tv4$9~K	%8kYy$xV	s,T9mvbN

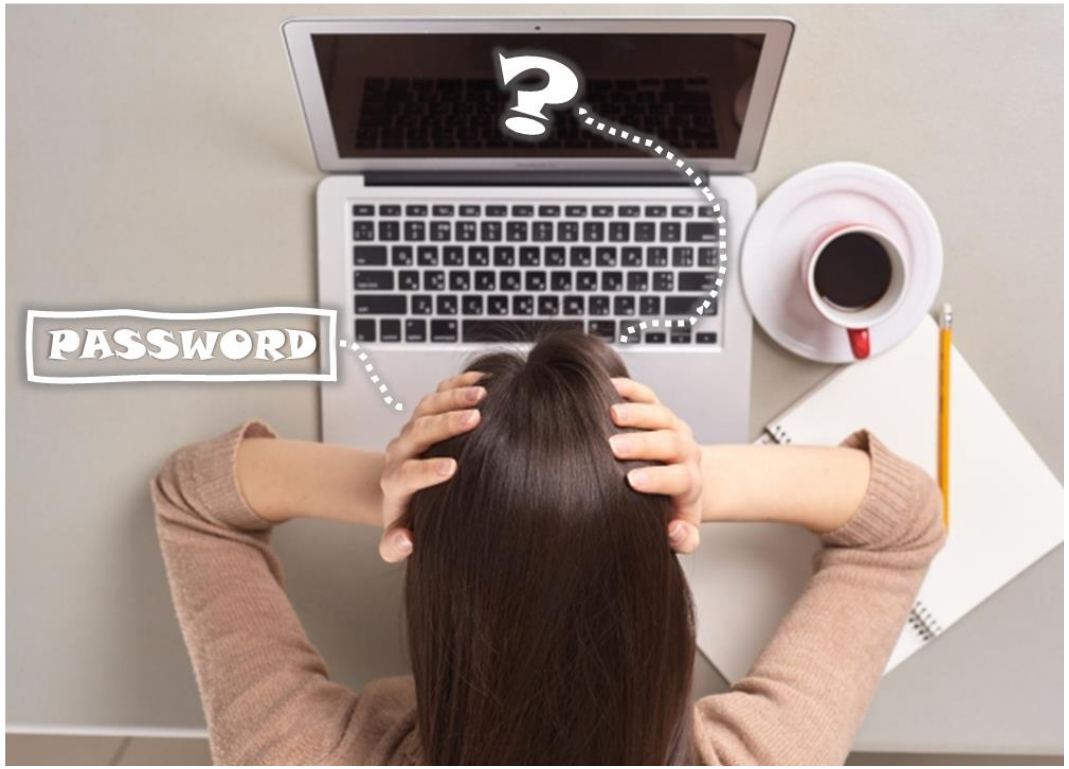
こういうパスワードを
こんなふうに運用する
できますか？

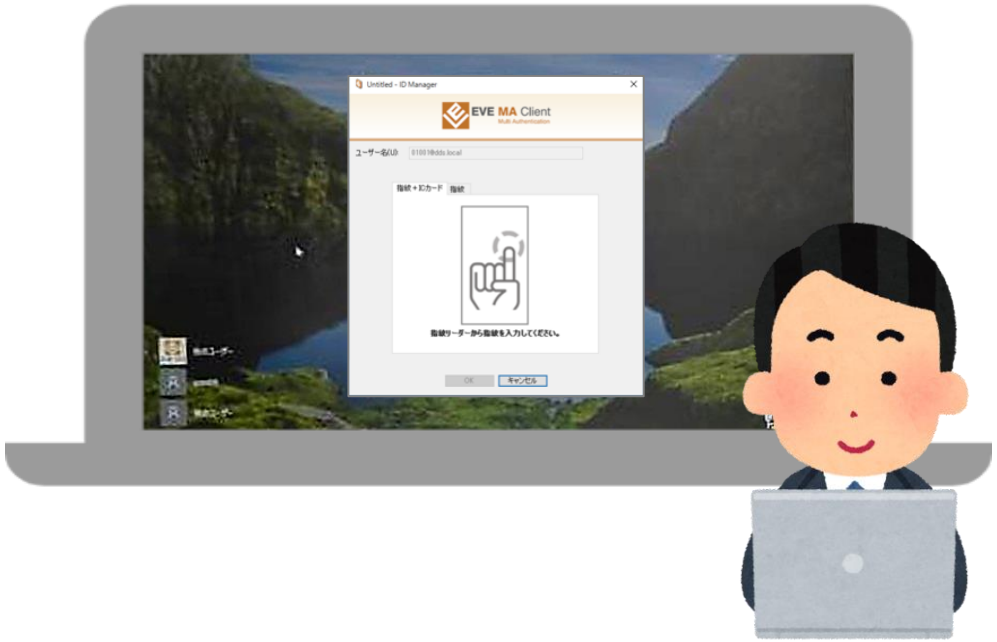
パスワードの運用
- 使いまわさない
- 紙などに記録しない
- 定期的に変更 (と言われていた)

全従業員にこのパスワードポリシーを遵守させることが
本当に可能でしょうか？

パスワードだけに頼る認証との決別

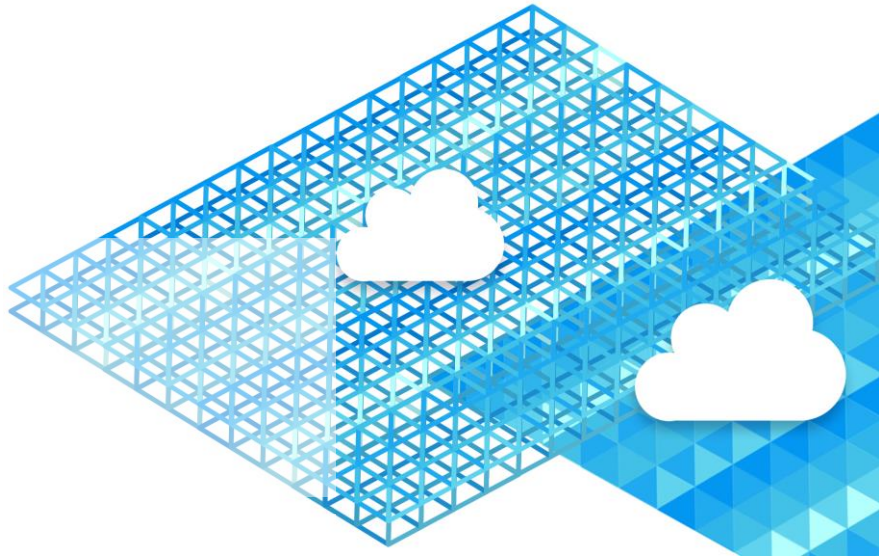
多要素認証でパスワード認証と決別しませんか？





パスワードだけに頼る認証との決別

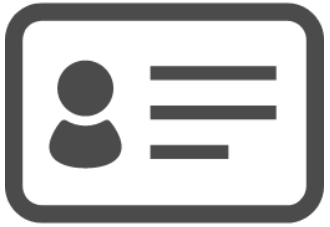
エンドポイントのセキュリティを強固にする多要素認証



個人を識別する認証要素は3種類

ユーザが知っていること
Something You Know

パスワード、暗証番号、秘密の質問



ユーザが持っているもの
Something You Have

ICカード、マトリクス、
ワンタイムパスワード、SMS、SIM

ユーザ自身の特徴
Something You Are

生体(バイオメトリクス)認証
指紋、顔、虹彩、静脈、・・・

認証要素ごとに、長所・短所がある
よりセキュアな認証が必要なシーンでは2種類以上の要素を組み合わせる(多要素認証)

多要素認証＝ID不正利用からの保護

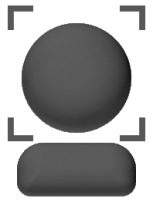
多要素認証は、確認方法の2つ以上を必須とすることで機能します。

ユーザが
知っている
こと

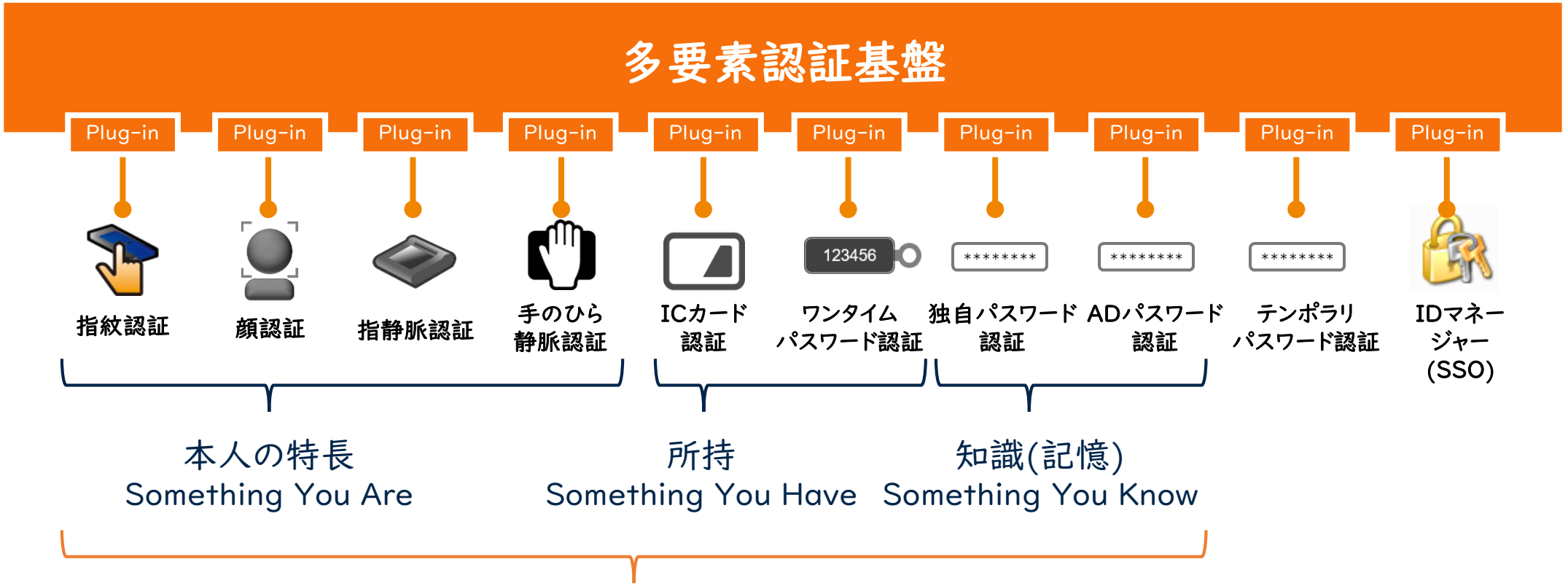
AND

ユーザ
自身の特徴

認証OK



様々な認証要素を自由に組み合わせ

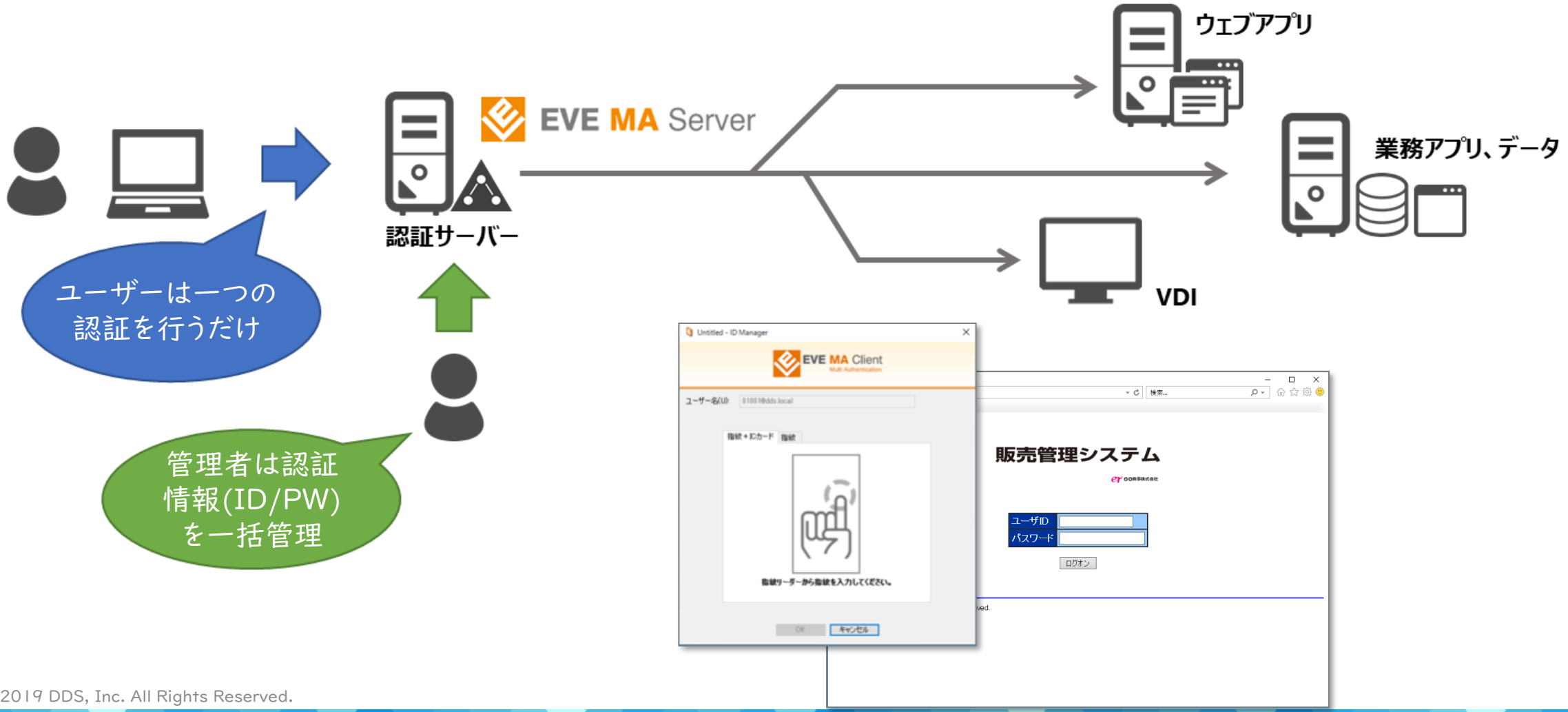


デバイスログオン（Windowsログオン）

サインイン画面を独自のものに置き換え

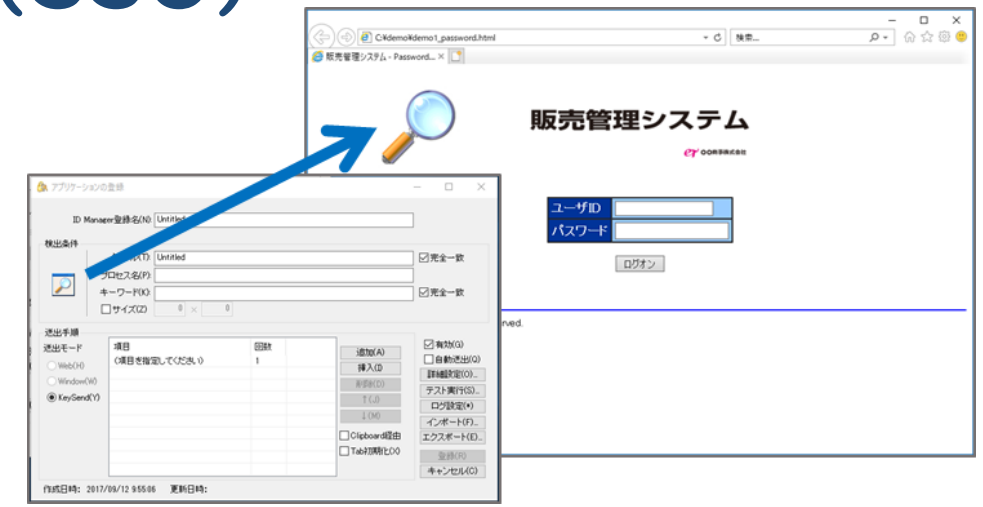
- Windows Helloのようにサインインオプションを表示せず、特定の認証しか受け付けないようにすることが可能
- AND/ORで認証要素の設定が可能。
  アクセスユーザーやPCによって細かい設定も可能

各種アプリ利用やデータアクセス時のSSO

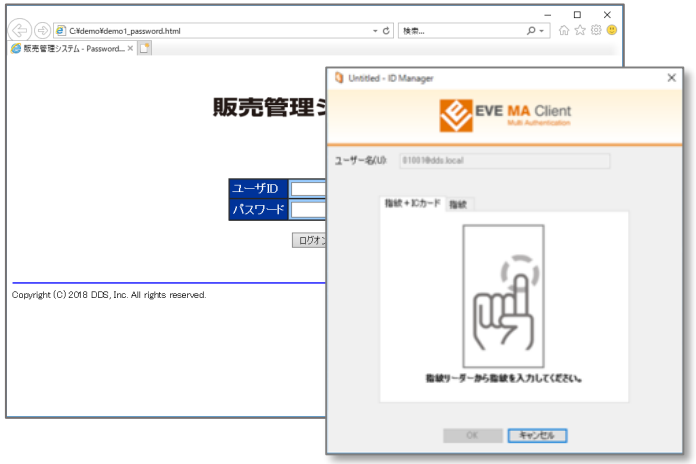


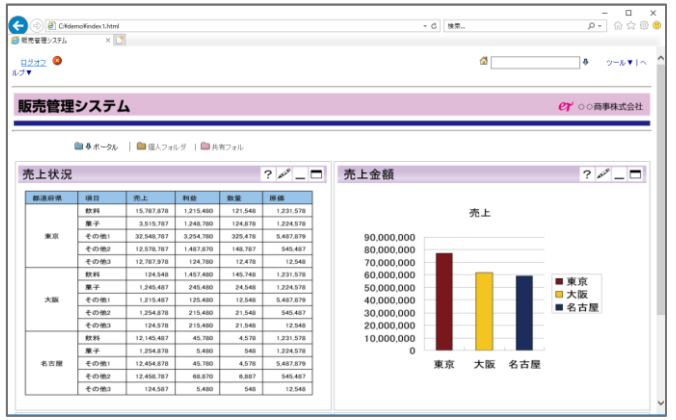
開発不要＆簡単登録のアプリ認証（SSO）

- ウェブアプリケーション
- デスクトップアプリケーション
- VDIクライアントアプリケーション



様々なアプリに対し認証画面を表示 ＞ IDマネージャーで自動ログイン





連携検証済みのアプリケーション・サービス

医療（電子カルテ）

シーエスアイ株式会社『MI・RA・Is／AZ』，『MI・RA・Is／PX』

富士通株式会社『HOPE EGMAIN-GX』

ファイル無害化・ファイル交換

株式会社プロット『Smooth File（スムースファイル） ネットワーク分離モデル』

ファイル暗号化

株式会社ネスコ『DataClasys』

操作ログ収集・管理

株式会社ラネクシー『MylogStar』

会計・人事給与

スーパーストリーム株式会社『SuperStream-NX』

ピー・シー・エー株式会社『PCA DXシリーズ』

簡単登録
API開発不要

文教（校務支援）

株式会社EDUCOM『EDUCOMマネー ジャC4th』

株式会社システム ディ『School Engine』

勤怠管理

ソニーネットワークコミュニケーションズ株式会社
『AKASHI』

特権ID管理

ManageEngine PasswordManager Pro

ゾーホージャパン株式会社
『ManageEngine Password Manager Pro』

コミュニケーション

株式会社エイジア『WEBCAS』

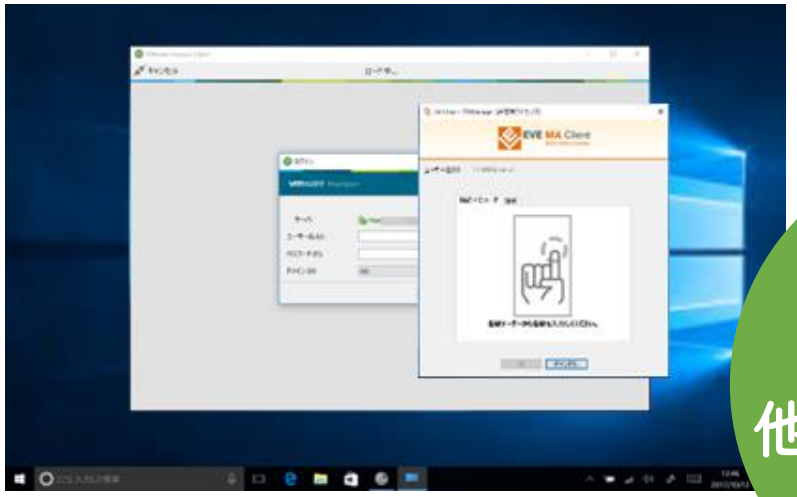
シンクライアント

株式会社サスライト『SASTIK Ⅲ Thin-Client Layer』
『SASTIK Network Isolation』

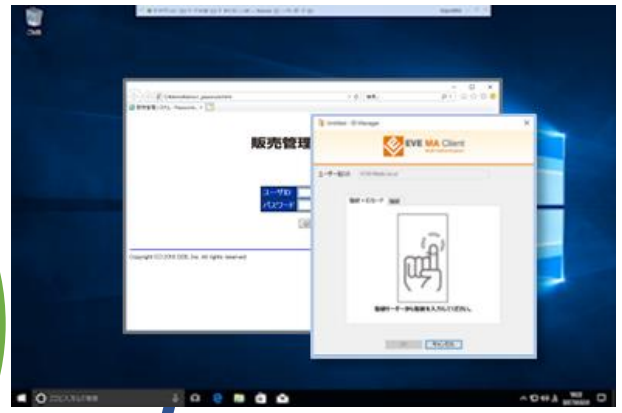
他多数

デスクトップ仮想化環境への適用

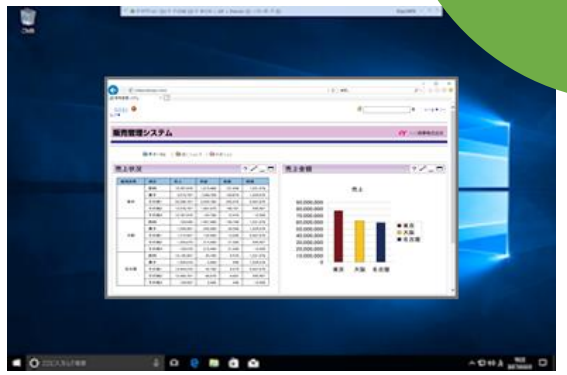
VDI接続アプリを起動し、
多要素認証で本人確認



VDI環境へログオンし
業務アプリケーションを起動



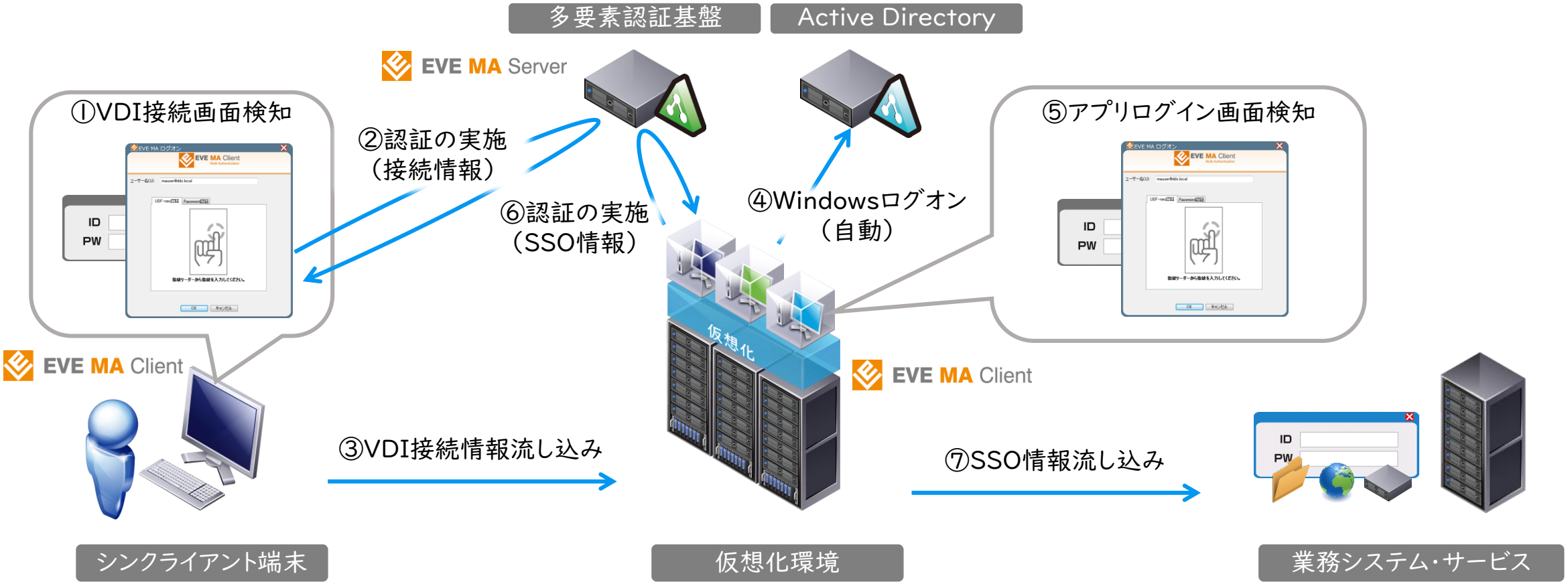
簡単・安心
他にない利便性

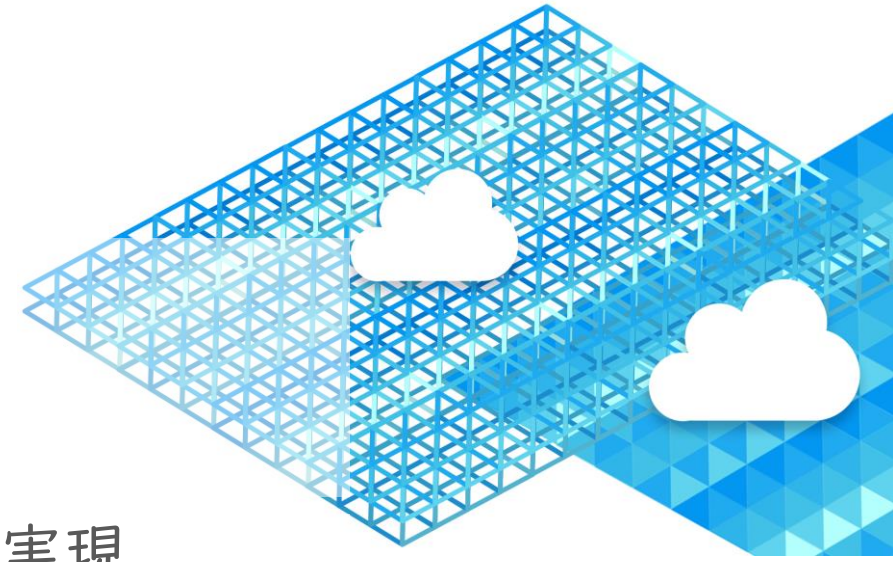


VDI内のアプリケーション認証でも多要素
認証を利用

仮想化（シンクライアント）でのログイン認証

Windows 10 IoT（多要素）や HP ThinPro（指紋・パスワード）でログイン



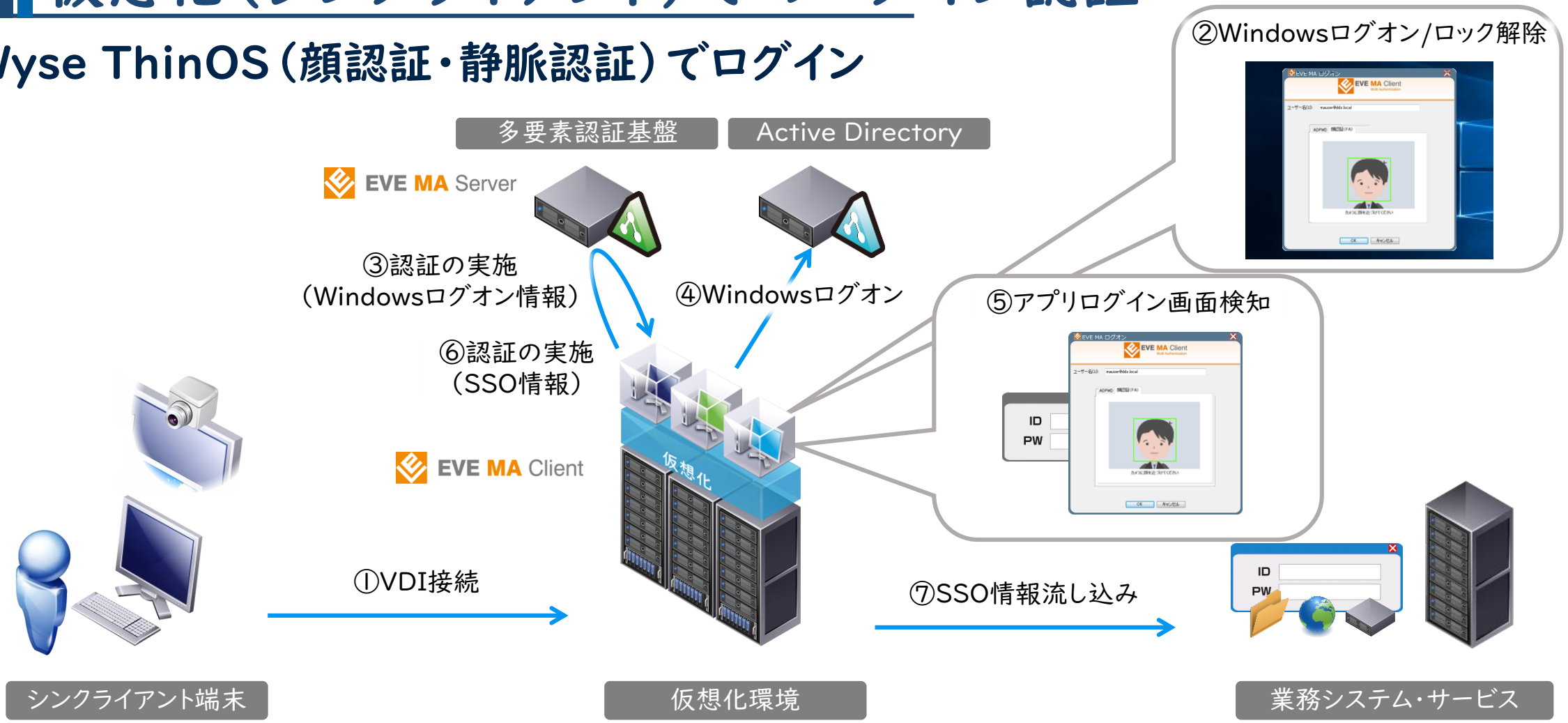


多要素認証基盤のアップデート情報

ゼロクライアント（Wyse ThinOS）における多要素認証の実現

仮想化（シンクライアント）でのログイン認証

Wyse ThinOS（顔認証・静脈認証）でログイン



Wyse ThinOS（顔認証）でログイン

以下動画でご確認いただけます。

出典：DELL社公式ページ（Dell Technologies Wyse ThinOS -FaceAucentification/顔認証）
https://youtu.be/wbkCpoqBxHs

まとめ

デジタルトランスフォーメーション（DX）

↳「いつでも、どこでも、どのデバイスでも」仕事が可能（例えばテレワーク）

テレワークにおける代表的な環境＝VDI

仮想化のセキュリティ盲点＝脆弱なパスワード認証

↳パスワード認証の脆弱性をつかれ、企業データへのアクセスを許す結果に

パスワードだけに頼る認証との決別

↳VDIでも利用可能な多要素認証でセキュリティ&利便性UP

株式会社ディー・ディー・エス

本社
〒460-0002
名古屋市中区丸の内三丁目6番41号 DDSビル 7F
営業本部
TEL:052-955-6600 FAX:052-955-6610

東京支社
〒103-0028
東京都中央区八重洲1丁目8番5号 新槇町ビル別館第二 2F
営業本部
TEL:03-3272-7900 FAX:03-3272-7901

https://www.dds.co.jp/ja/