ThemiStruct（テミストラクト）(OpenAM) で実現する端末認証の実際

株式会社オージス総研

八幡 孝

自己紹介

八幡 孝（やはた たかし）

- 株式会社オージス総研
- ThemiStructソリューション開発 リードアーキテクト
- ThemiStruct関連サービスの東日本エリア責任者
- OpenAMコンソーシアム 活動メンバー
- OpenIDファウンデーション・ジャパン
  Enterprise Identity WG 技術TF リーダー

@paoneJP

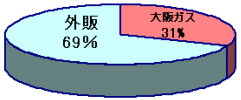
- OpenAM, Apache Modules, Python, Android, …
- OpenID Connect, JWT, OAuth, … , 周辺の実験をいろいろと。
- https://paonejp.github.io/

オージス総研です

株式会社オージス総研

- 代表者： 代表取締役社長　西岡　信也
- 設　立： 1983年6月29日
- 資本金： 4.４億円　（大阪ガス株式会社100%出資）
- 事業内容： システム開発、プラットフォームサービス、
  コンピュータ機器・ソフトウェアの販売、
  コンサルティング、研修・トレーニング

- 主な事業所
  - 本　社： 大阪府 大阪市西区千代崎3-南2-37 ICCビル
  - 東京本社： 東京都 港区港南2-15-1 品川インターシティA棟
  - 千里オフィス： 大阪府 豊中市新千里西町１－２－１
  - 名古屋オフィス： 愛知県 名古屋市中区錦1-17-13 名興ビル
- 売上実績： 582億円（連結）　308億円（単体）　(2014年度)
- 従業員数： 3,126名（連結）　1,279名（単体）
- 関連会社： さくら情報システム（株）、（株）宇部情報システム、（株）システムアンサー、
  OGIS International, Inc. 、上海欧計斯軟件有限公司（中国）
- オージス総研グループ 売上構成比（連結）



取得許可認定

Chapter I

これまでのおさらい

認証基盤を作る狙いは何か？

認証基盤を作るメリット

- ① 利用者が便利になる
- ② セキュリティレベルのばらつきがなくなる
- ③ システム開発がしやすい
- ④ 認証方式の変更がやりやすい

① 利用者が便利になる

- 作業効率の向上
- IT活用の促進

② セキュリティレベルのばらつきがなくなる

- 開発者に依存したばらつき
- ユーザーに依存したばらつき

③ システム開発がしやすい

- アプリ毎の認証機能開発は不要
- サブシステムに分割した開発の実現

④ 認証方式の変更がやりやすい

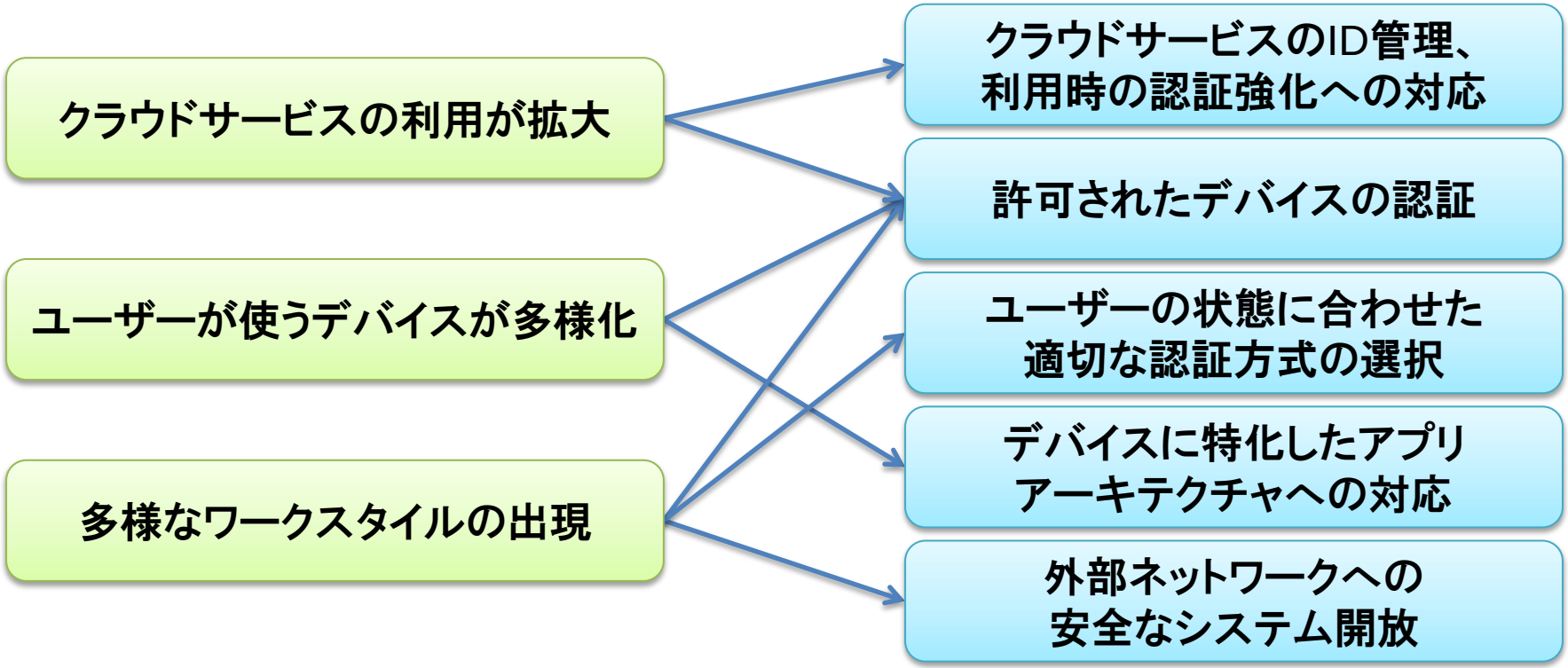
- ID/パスワードを使った認証
- 多要素認証への対応
- 新しい方式への対応

認証基盤への要求の変化

企業ITを取り巻く環境の変化

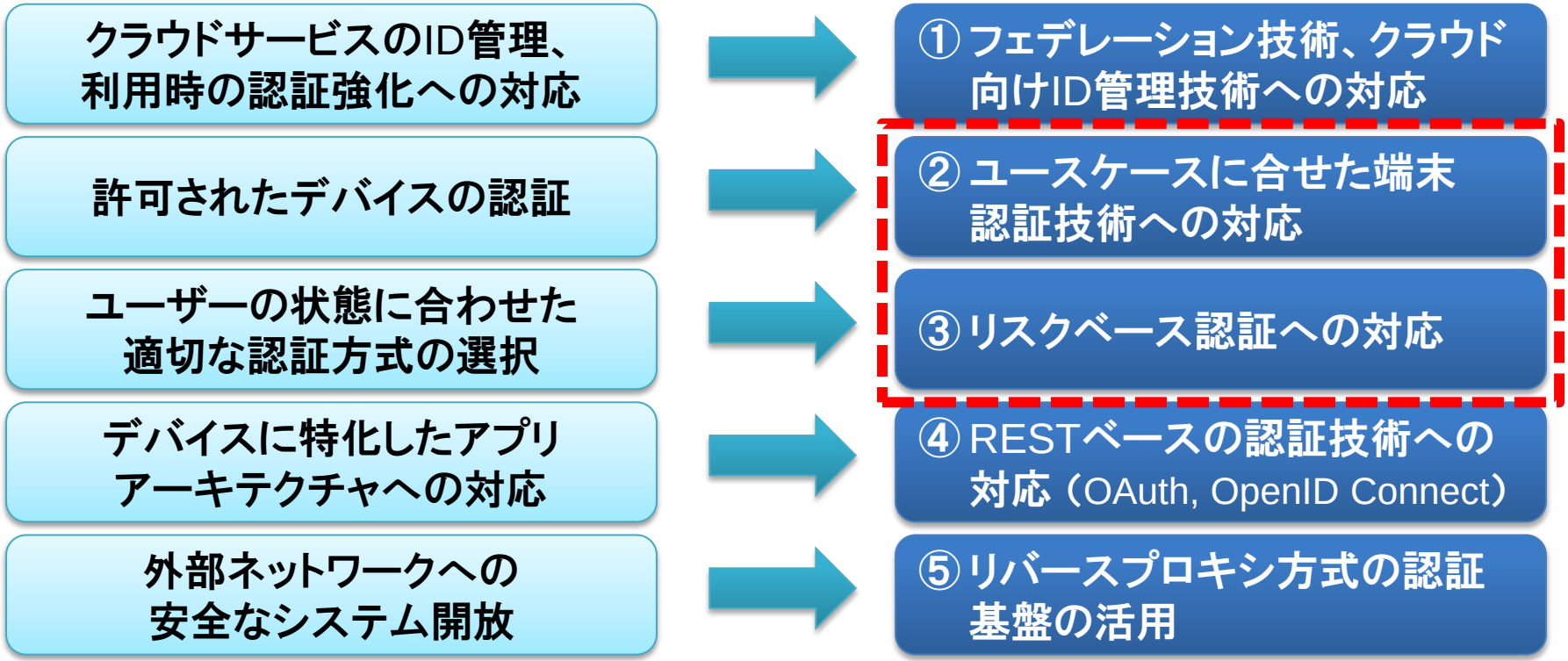
社内にあるシステムを	→	クラウドサービスの利用が拡大
社員用のPCから	→	ユーザーが使うデバイスが多様化
社内ネットワークの中で	→	多様なワークスタイルの出現

これからの認証基盤への要求

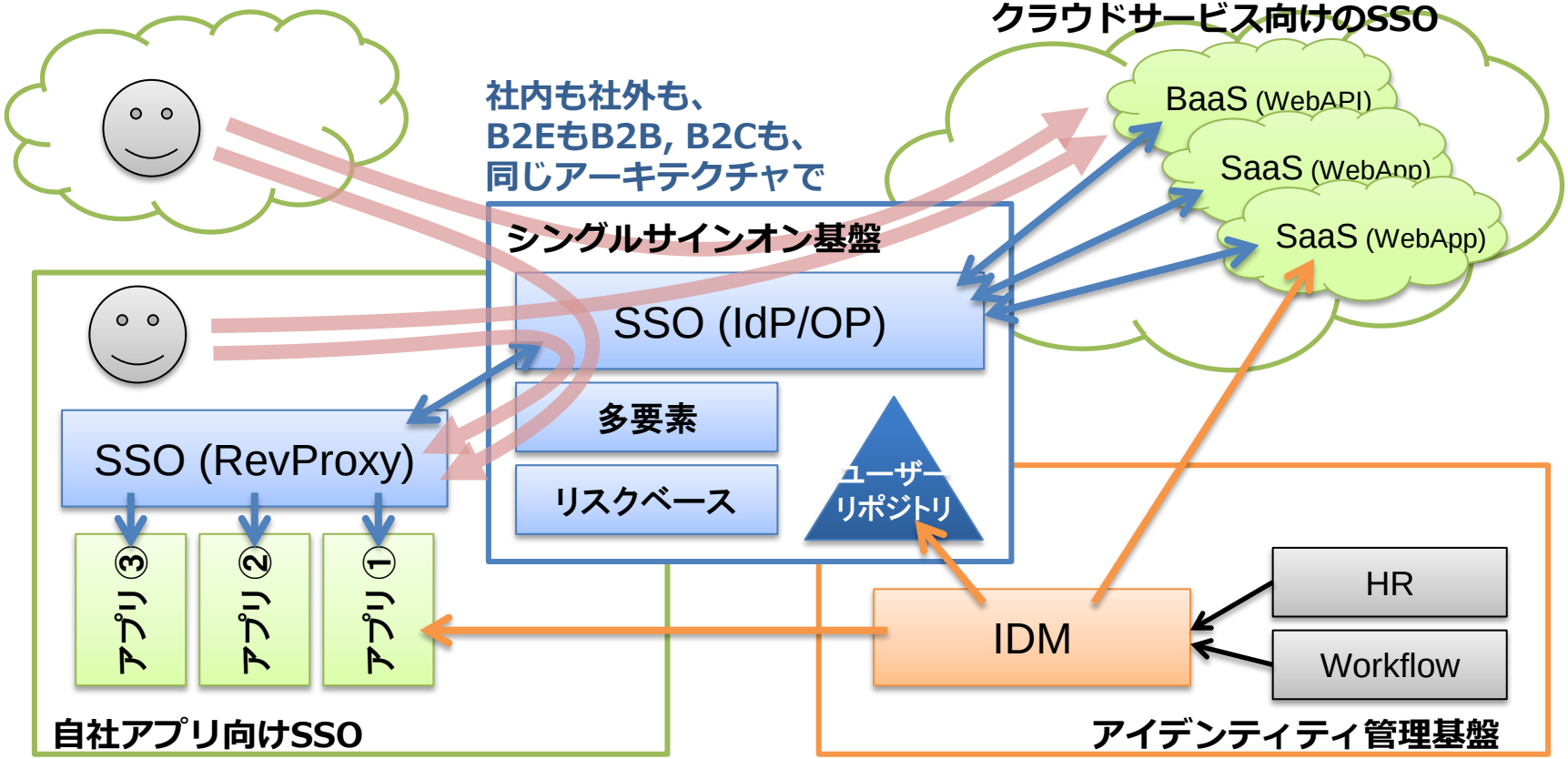


企業の認証基盤ではどう対応すべきか

企業の認証基盤の目指す方向性



認証基盤コアアーキテクチャ 2015年版 r2



認証基盤への要求が変わった今がチャンス

- まず認証基盤を作る
- アプリに仕様を提示し、認証基盤に繋がってもらう
- アプリを徐々に集める・増やす

- 先に認証基盤を作ればメリットを最大限享受できる

Chapter II

端末認証のユースケース

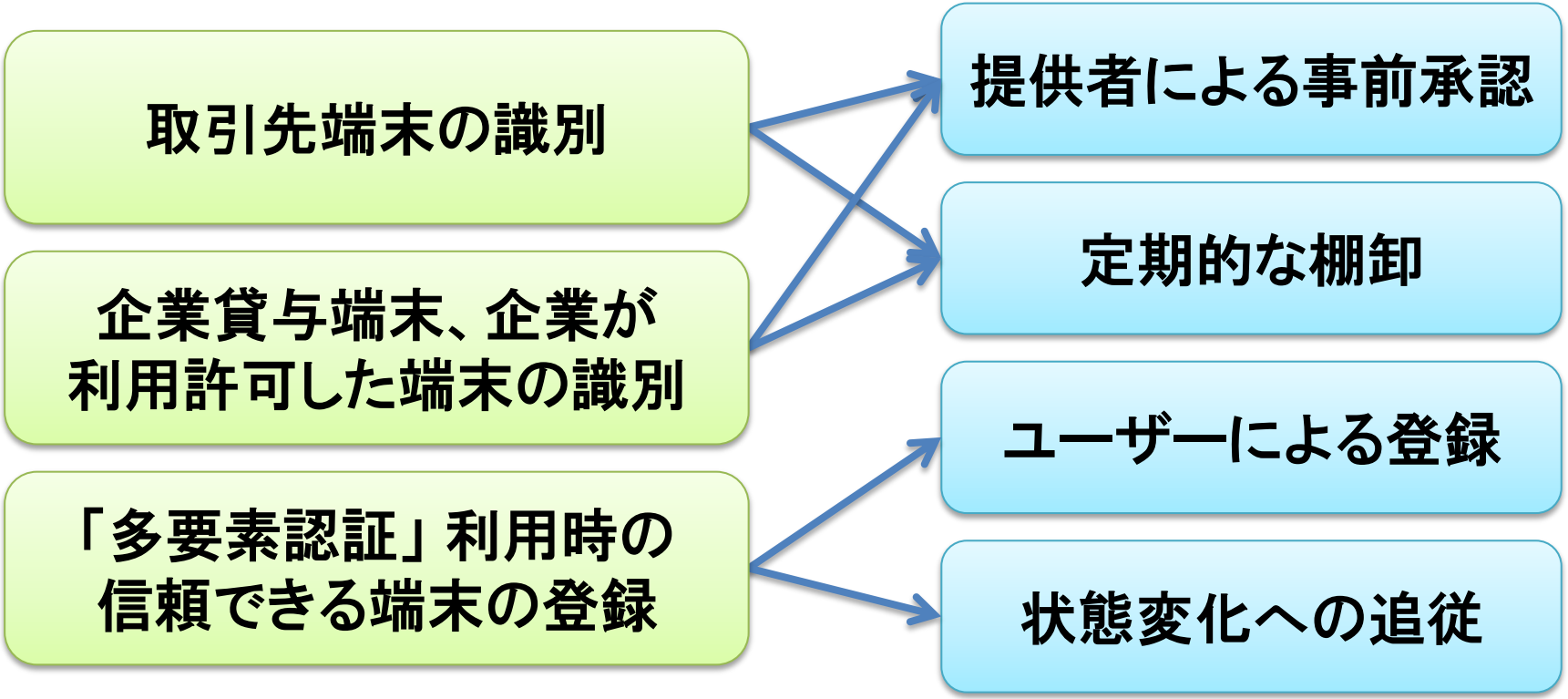
端末認証のユースケース

取引先端末の識別

企業貸与端末、企業が利用許可した端末の識別

「多要素認証」利用時の信頼できる端末の登録

端末認証に求められる特性



Chapter III

端末認証の技術・方式

端末認証の技術・方式

- アクセス元IPによる認証
- 電子証明書を用いた認証
- デバイスID認証 for **OpenAM**
- [New!] インベントリ認証 for **ThemiStruct-WAM**

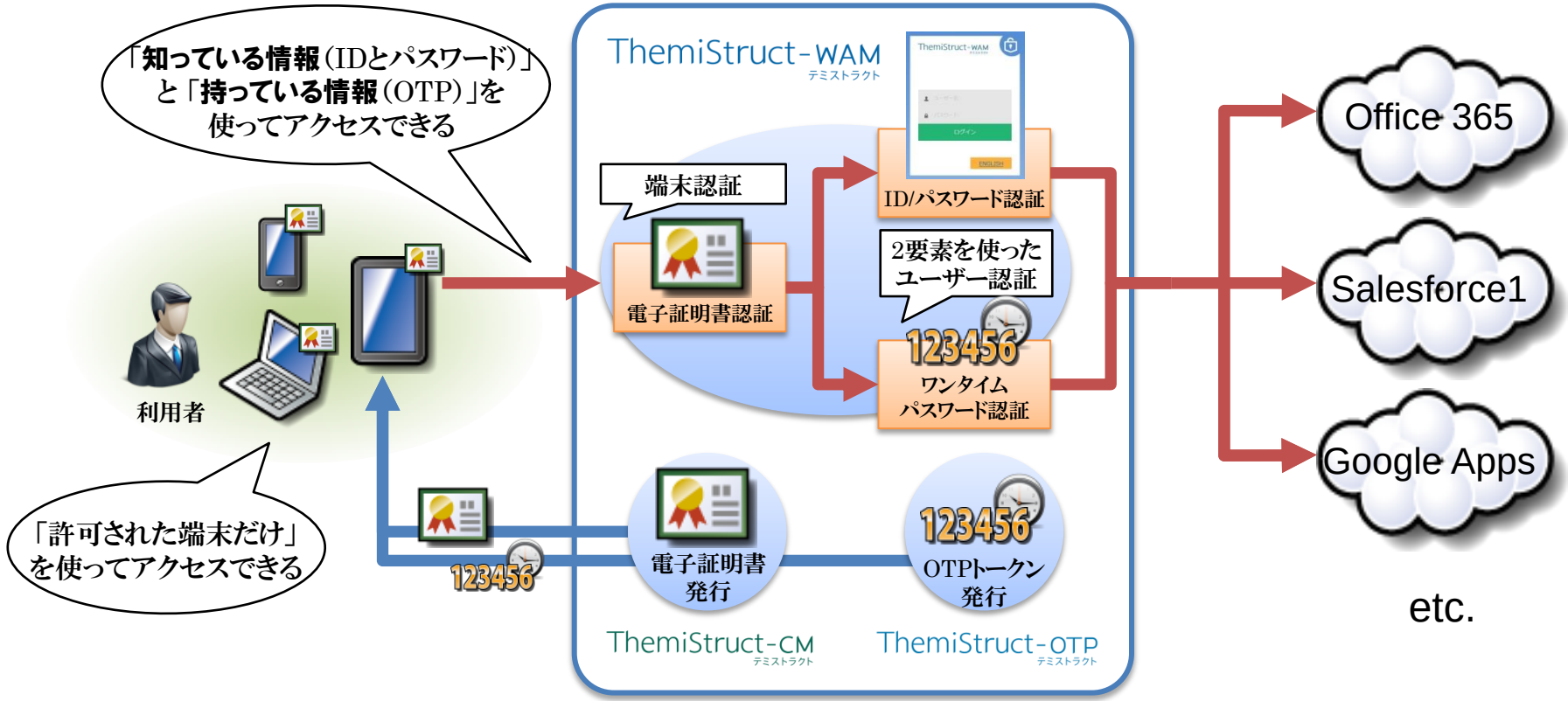
アクセス元IPによる認証

- サーバーから見たクライアントのIPアドレスを利用
- 固定IPが必要
- 端末と言うよりは、組織を認証する方式
- 実装、運用が簡単
- 固定IPが使えるケースでは現在でも有効の方式

電子証明書を用いた認証

- 企業が承認する端末向けに電子証明書を発行
- アクセス時に電子証明書を用いて端末を認証
- 証明書有効期限を用いた棚卸、再承認運用が可能
- 証明書の配布方法によって、証明書インストール端末の妥当性確認が課題となる場合あり

電子証明書を使った端末認証と多要素認証の例

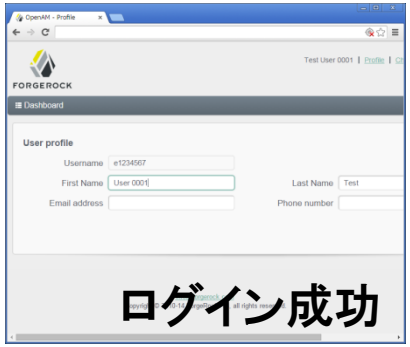


デバイスID認証 for OpenAM

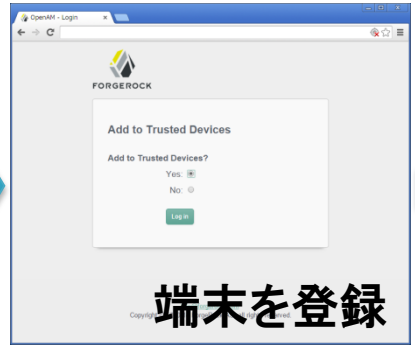
- OpenAMの認証モジュールとして提供されるもの
  - Device Id (Match) と Device Id (Save) を組合せて構成
- ブラウザ上でJavaScriptを実行して判定
  - ブラウザ名、フォント、ブラウザに組み込まれたフォント、画面サイズ、色数、タイムゾーン、などの情報を利用
- 多要素認証の利便性向上が主たるユースケース
  - 一度目は、多要素認証を用いて認証、端末を登録すれば、2回目以降はID/パスワードだけで認証、という使い方

デバイスID認証の例

登録済み端末ならシンプルに



未登録端末 or 端末状態が変わったら確実に



認証連鎖設定

(4 項目)

追加 削除 並べ替え

	インスタンス	条件
	DataStore	必須
	DeviceIdMatch	十分
	OATH	必須
	DeviceIdSave	必要

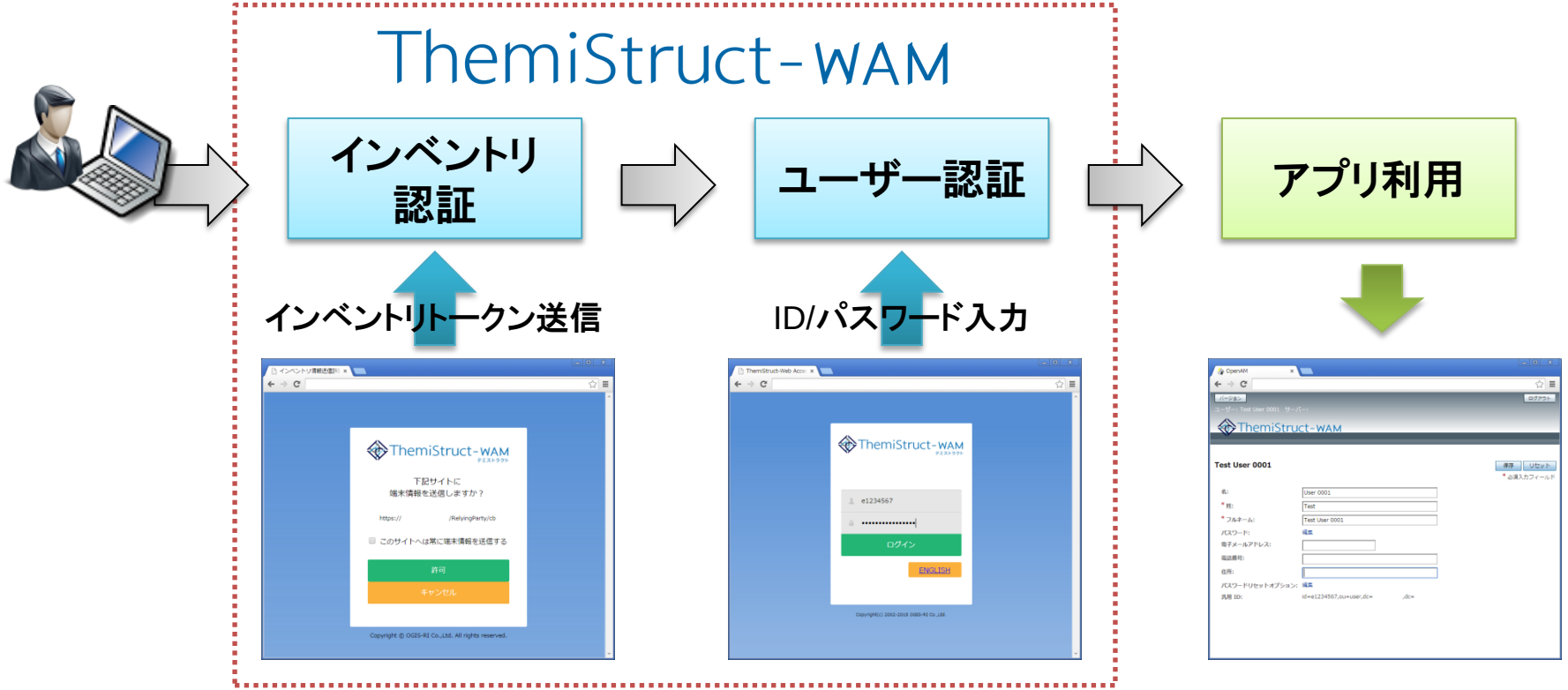
[New!]

インベントリ認証 for ThemiStruct-WAM

- 専用エージェントソフトウェアを用いる方式
- 端末固有の情報をインベントリトークンとして提示することで端末認証を実現

built on OpenID Connect standard！

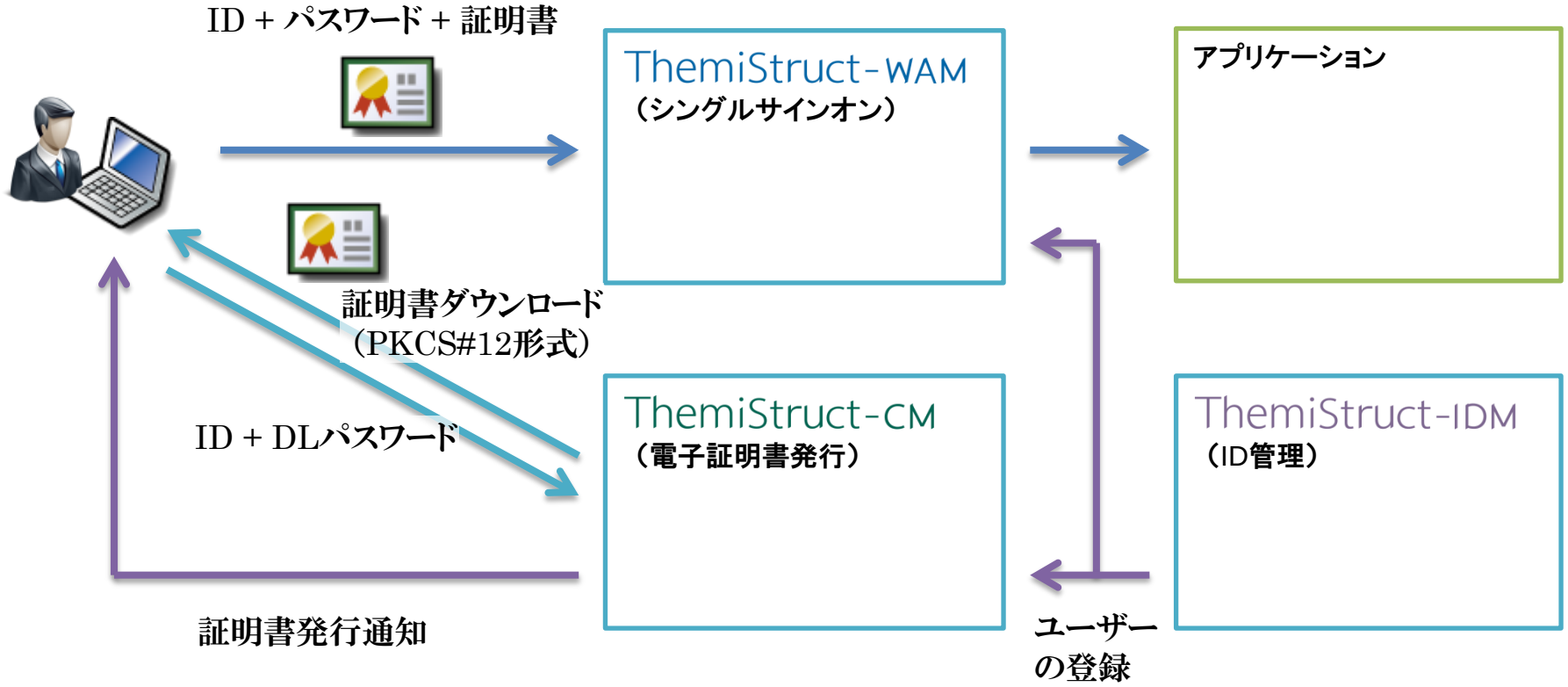
インベントリ認証の概要



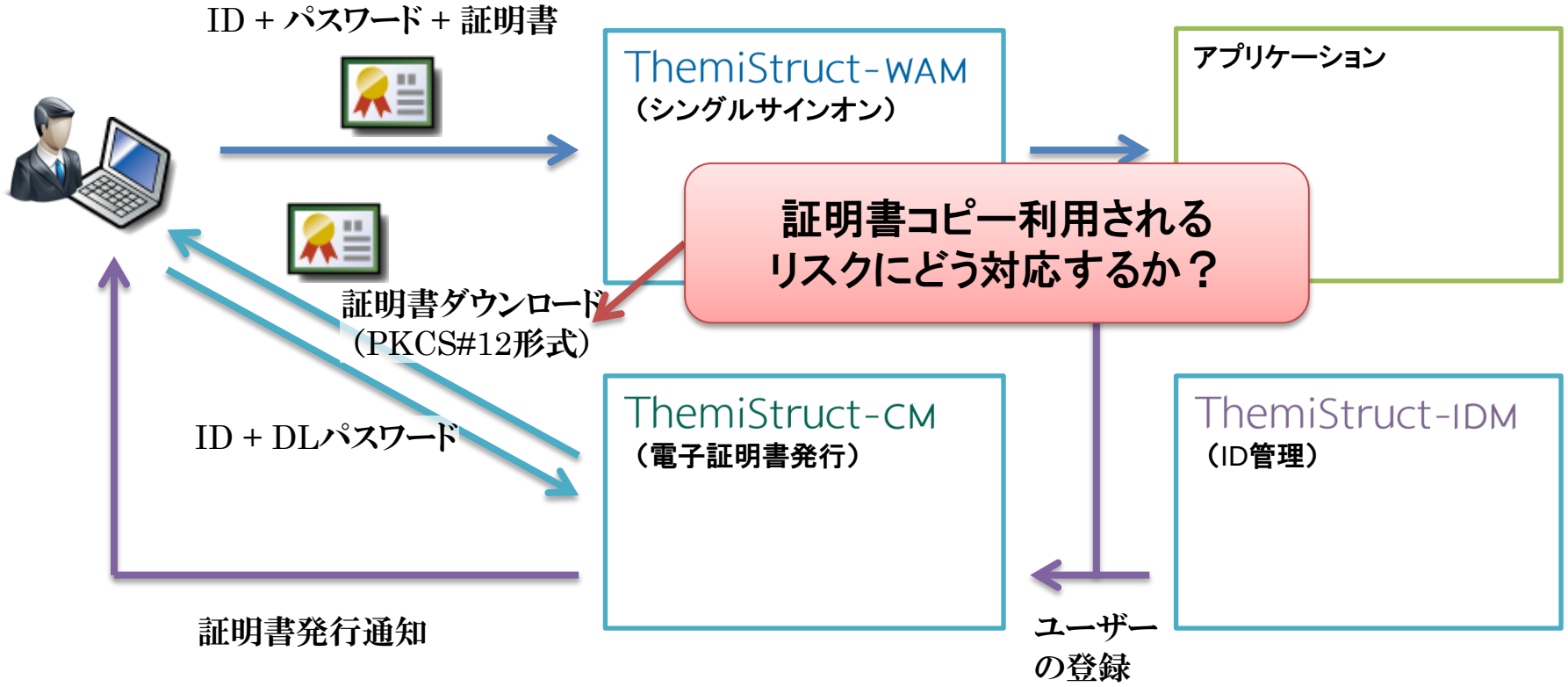
Chapter IV

企業向け端末認証構成例

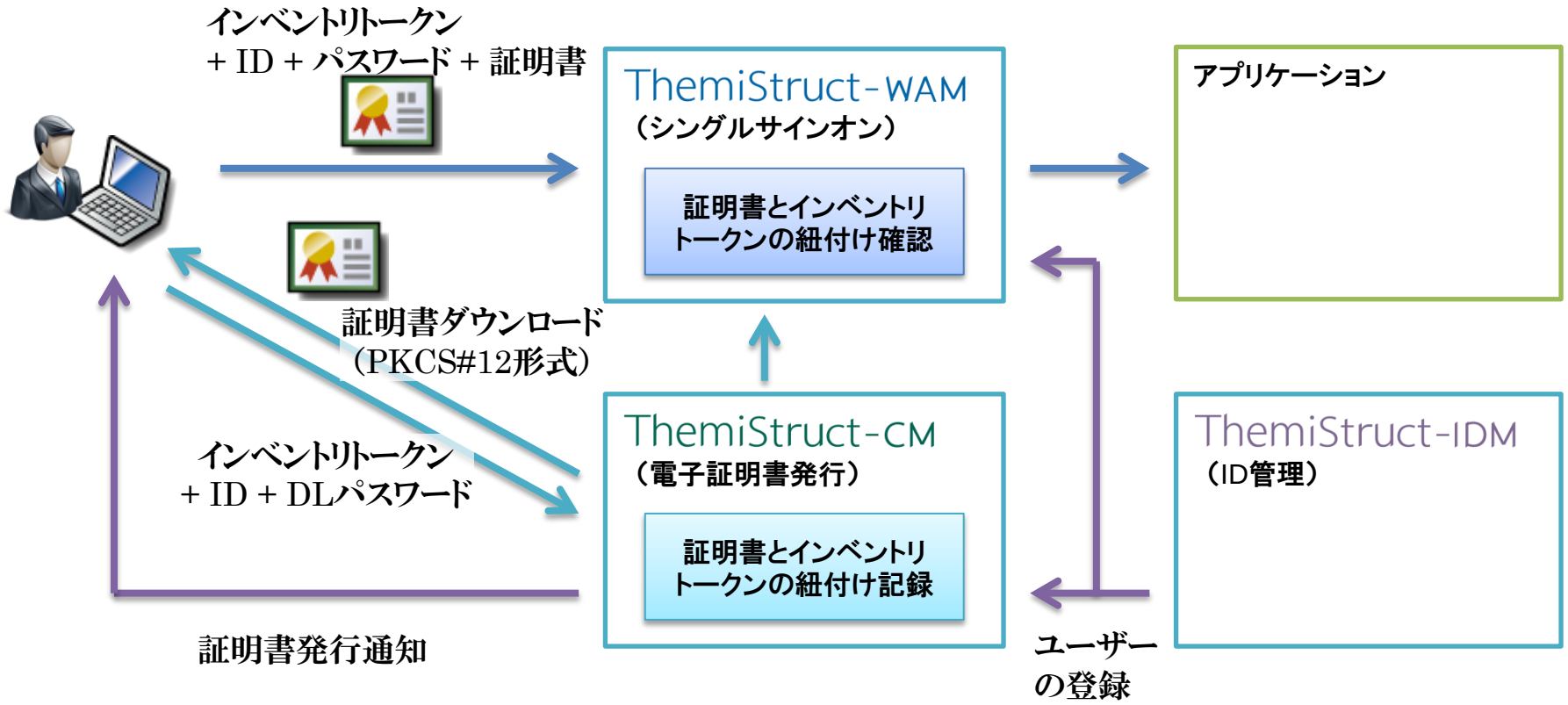
電子証明書を用いた端末認証



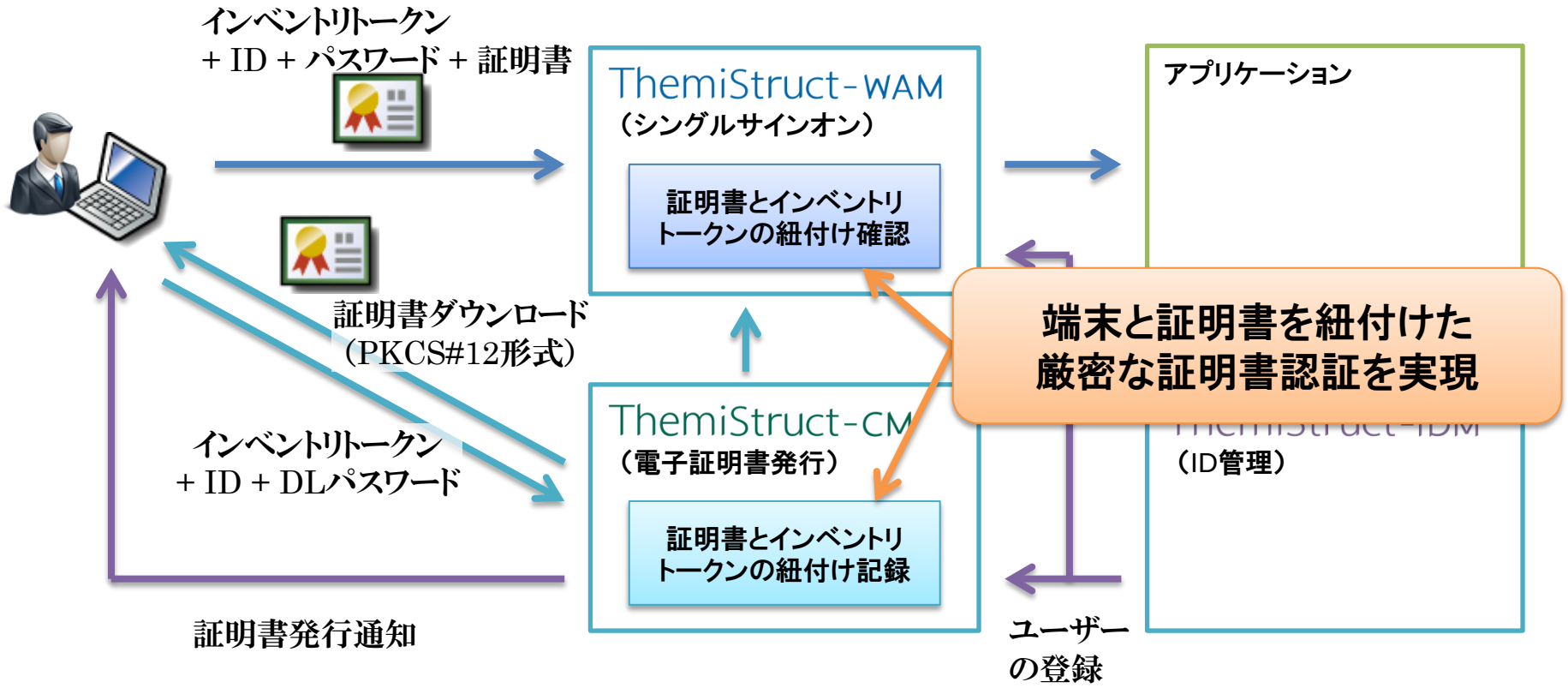
電子証明書を用いた端末認証構成例



より厳密な電子証明書を用いた端末認証



より厳密な電子証明書を用いた端末認証



Chapter V

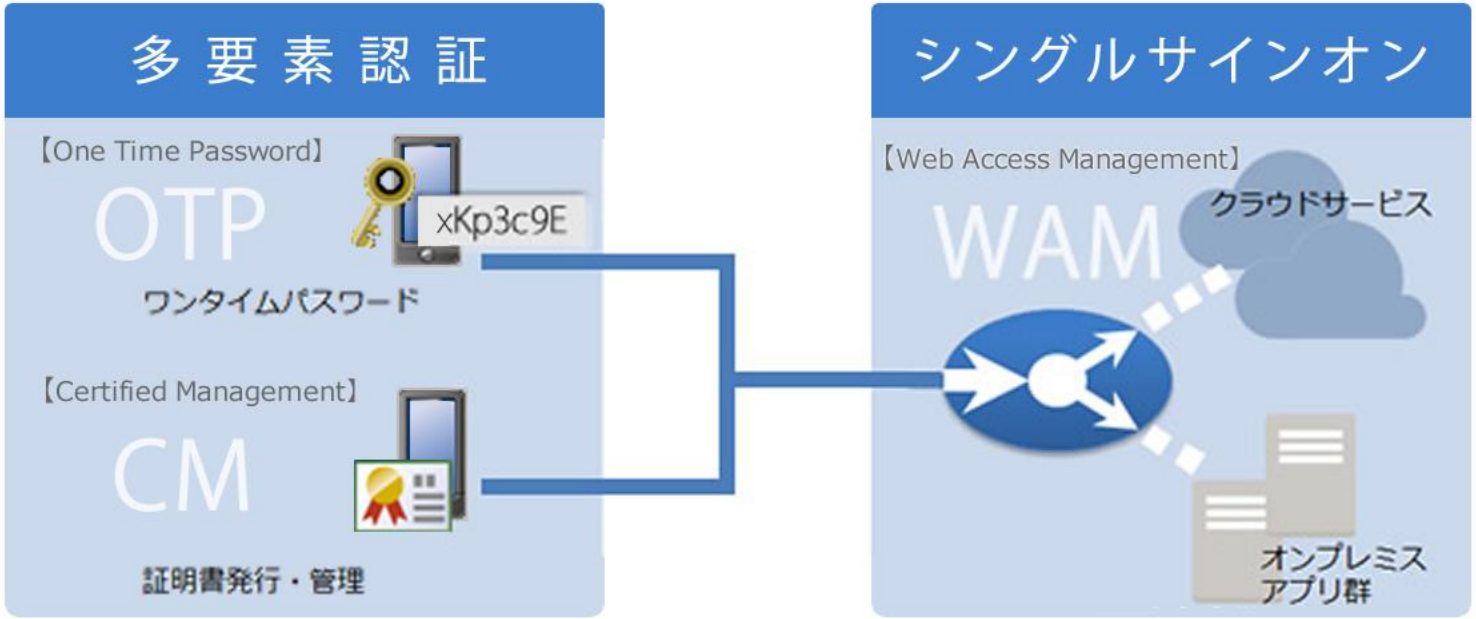
当社ソリューションの紹介

ThemiStruct（テミストラクト）は統合認証ソリューション

多要素認証やシングルサインオンなどアクセスマネジメント

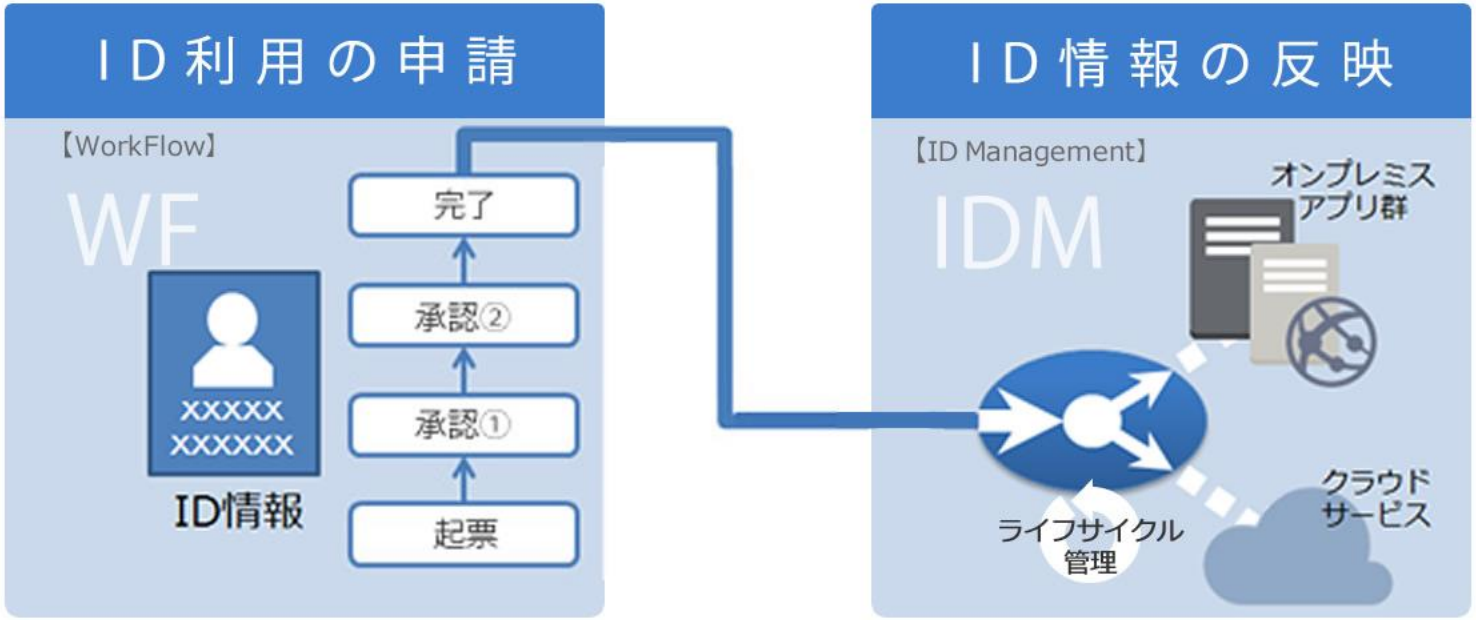
1. 認証基盤ソリューション

クラウド×スマートデバイスを多要素認証でセキュリティ強化し
シングルサインオンで利便性を向上します



2. ID管理ソリューション

ID情報を申請フローを用いて収集し対象システム群へ反映
有効期限による管理および人事異動などにスマートに対応可能です



5つのソリューションを提供

ThemiStruct-WAM	シングルサインオン 認証基盤ソリューション
ThemiStruct-IDM	ID管理ソリューション
ThemiStruct-CM	電子証明書発行・管理 ソリューション

ワンタイムパスワードソリューション

ThemiStruct-OTP

システム監視ソリューション

ThemiStruct-MONITOR

ThemiStruct-WAM

- OpenAM (trunk) **がベース**
- **専用のインストーラー**
- **当社オリジナルの日本語マニュアル**
- **スマートデバイスに対応するレスポンシブUI**
- **パスワード管理強化のためのアドオンモジュール群**
- **高度なリスクベース認証を実現するインベントリ認証オプション**
- …

ThemiStruct-IDM

- OpenIDM (trunk) **がベース**
- **専用のインストーラー**
- **当社オリジナルの日本語マニュアル**
- **権限委譲に対応した専用の**WebUI (SSI)
- **組織、グループ、ロールの管理**
- **プロビジョニングのスケジューリング、予約への対応**
- **…**

ThemiStruct-CM

- EJBCA (Enterprise版) がベース
- 当社オリジナルの日本語マニュアル
- 証明書の一括登録、一括ダウンロード
- 秘密鍵がエクスポートできない証明書発行への対応
- デバイスアクセスコントロールへの対応
- …

EJBCA
PKI by PrimeKey

当社は PrimeKeySolutions AB 社の
パートナー です。

OSSを活用するメリット

- 技術標準の早期実装
- 公開されている仕様
- ソースコードを使った問題調査、修正

ThemiStructで提供する3つのサービス

テクニカルサポートサービス

- 利用方法などの問合せへの回答
- 障害時の調査、回避策や代替案の提示、復旧の技術支援

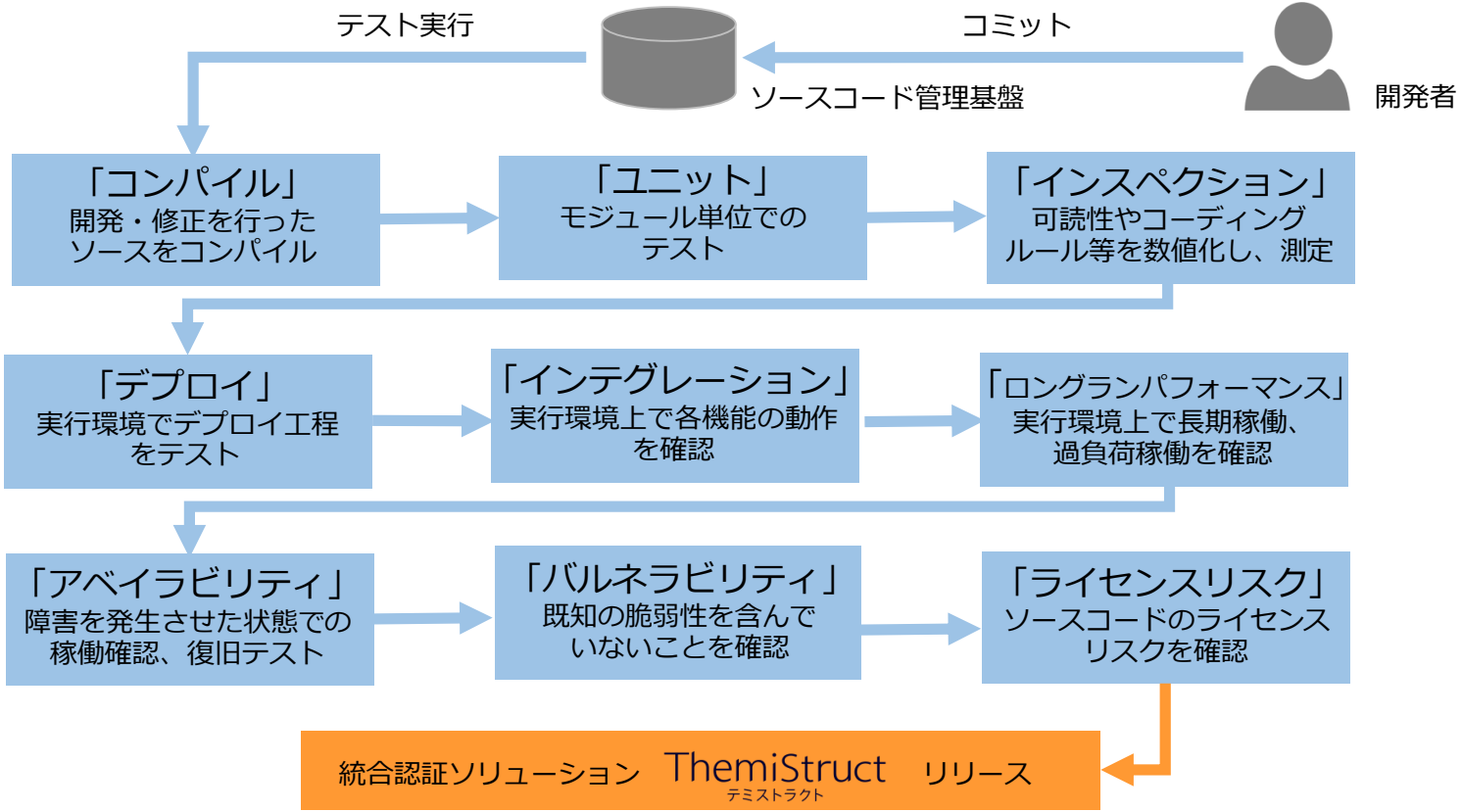
プロフェッショナルサービス

- 要件実現方法の相談、回答
- 技術検証の支援
- 自社で実施する開発、構築の技術支援

システムインテグレーションサービス

- お客様の要望に応じたシステムを構築

OSSを安心して活用いただくための取り組み



AWS上に展開されたテスト基盤

- テストターゲットの自動デプロイによる
  クリーンなテスト環境の構築
- 自動化インテグレーションテスト
  - 自動化率向上のための取り組みを継続
- スポットインスタンスを活用した
  パフォーマンステスト
- etc…

当社は APN (AWS Partner Network)
コンサルティングパートナー です。

ライセンスリスクの確認

- 使用しているOSS、著作権者、ライセンス条件を正しく把握
- 権利の瑕疵の発生を予防
- OSS自動検出ツール「Palamida™」を使用

PALAMIDA™
Application Security for Open Source Software

当社は 米国PALAMIDA社の
パートナー です。

サポート力向上のための更なる挑戦

- ソースコード静的解析ツール「コベリティ®」を使った、不具合発見と修正へトライ中。
  - クラッシュ
  - リソースリーク
  - 脆弱性
  - …

当社は 米国シノプシス社（旧：コベリティ社）の販売代理店 です。

本日紹介した当社ソリューション

ThemiStruct
テミストラクト

PALAMIDA™
Application Security for Open Source Software

COVERITY®
BY SYNOPSYS

ご清聴ありがとうございました。

ThemiStruct
テミストラクト

【お問合せ先】
株式会社オージス総研
TEL: 03-6712-1201 / 06-6871-7998
E-mail: info@ogis-ri.co.jp

OGIS-RI