

講談社様 ThemisStruct-WAM (OpenAM) 導入事例
**クラウドサービスと複数の社内システムを
対象にSSO連携を実現**
～シームレスにシステム間を接続し、業務を効率化～

株式会社オージス総研
IT基盤ソリューション第一部

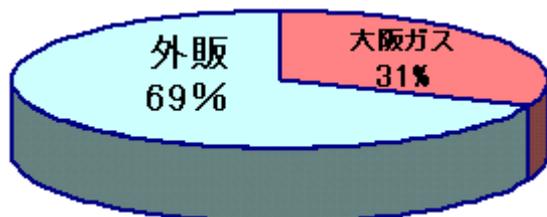
八幡 孝

2012年10月19日



株式会社オージス総研

- 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
- 名古屋オフィス： 愛知県名古屋市中区錦1-17-13 名興ビル
- 代表者： 代表取締役社長 平山 輝
- 設 立： 1983年6月29日
- 資本金： 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
- 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.、上海欧計斯软件有限公司(中国)
- 従業員数： 3,068名(連結) 1,264名(単体)
- 売上実績： 535億円(連結) 288億円(単体)
- オージス総研グループ 売上構成比（連結）



取得許可認定



我々はどこへ行くのか？

しっかりした基本構造

モデリング アーキテクチャ
オープンソース・ソフトウェア

変化への適応力

SOA、クラウドインテグレーション
アジャイル開発

持続可能な企業情報システムの実現

百年アーキテクチャ

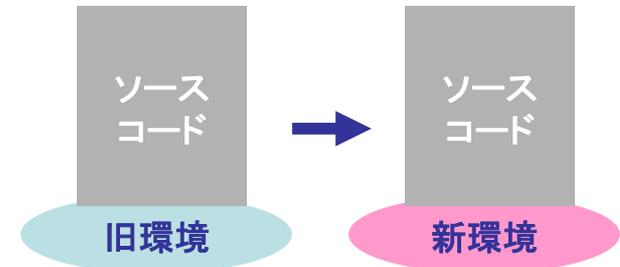
オープンソース・ソフトウェア

耐久性のある材料

なぜ耐久性があるのか？

ソースコードが公開

- 新環境へ移動可能
- カスタマイズ可能
- 使用継続可能



サポート打ち切り ベンダーロックイン

リスクからの開放

なぜ今オープンソースか？

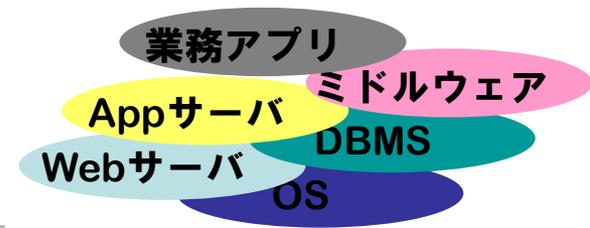
高価なライセンス料 バージョンアップ

質・量が飛躍的に向上

- 高機能、高品質
- あらゆるジャンル

低コスト

- サポートは必要



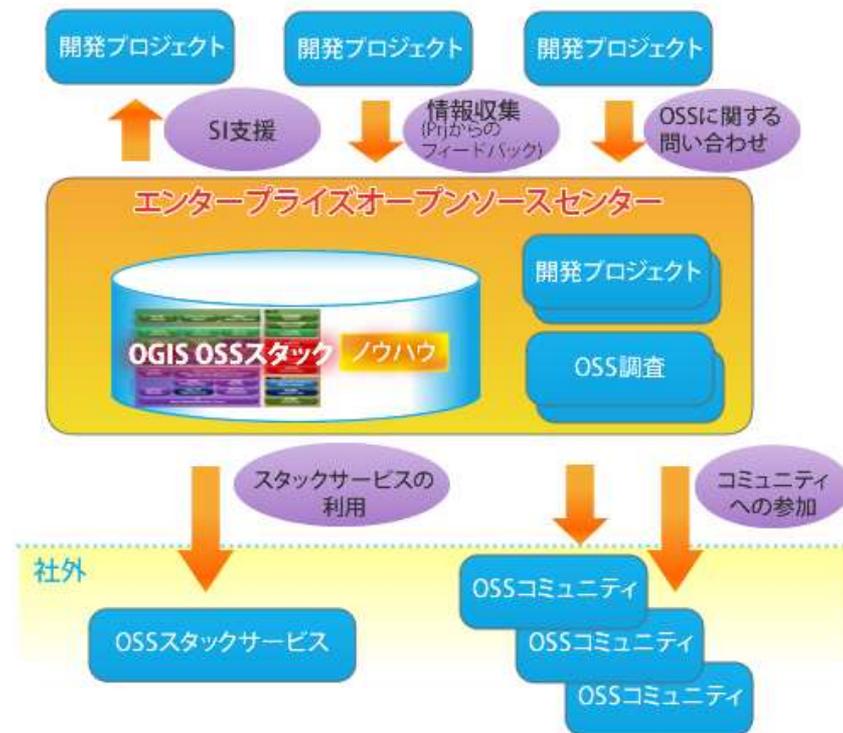


ミッション

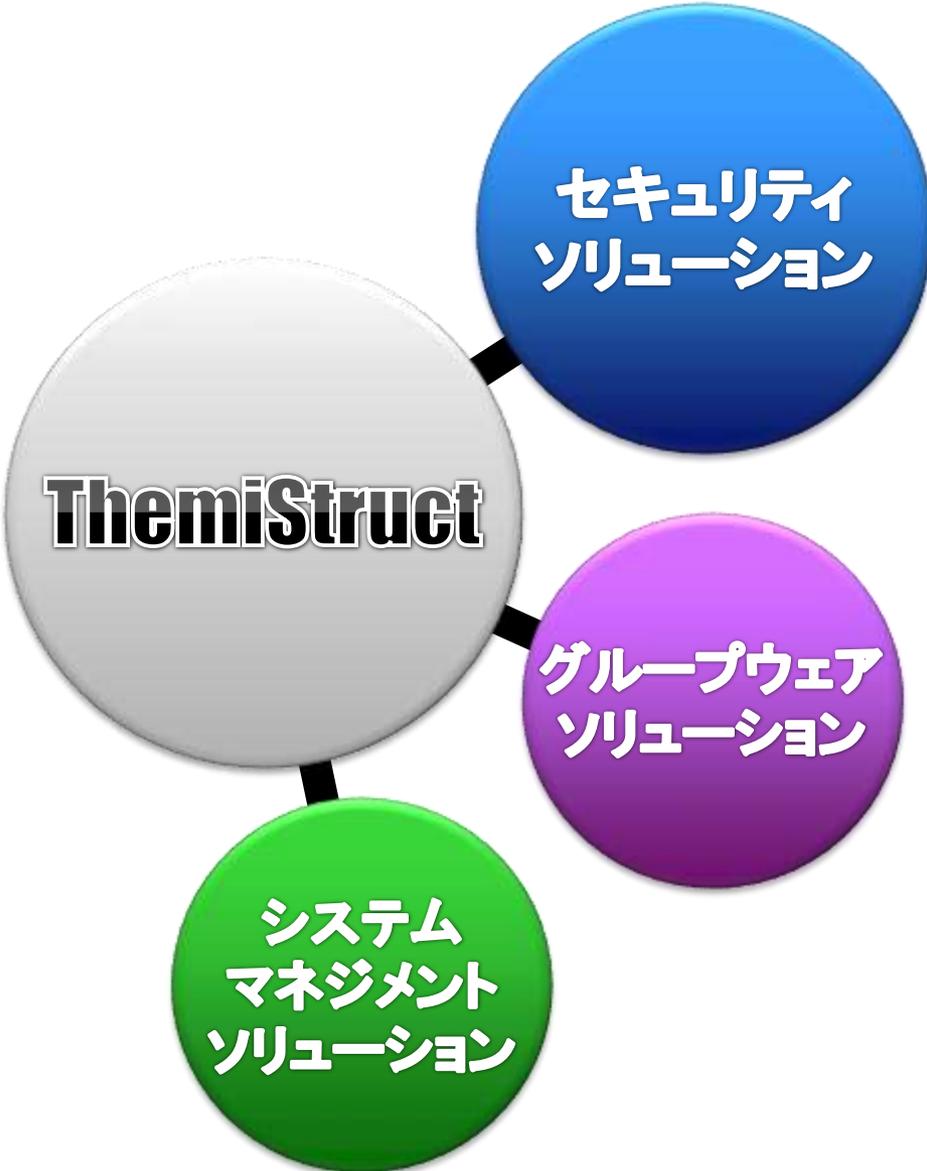
- SIやサービスビジネスなどへのOSS利用実績、ノウハウの蓄積
- オージス総研におけるOSS活用の促進、先端技術の提供
- コミュニティ活動を通してのOSS活用推進への貢献

取り組み

- OSSの動向調査
- OSSリファレンススタックの整備
- 商用プロダクトとの相互運用性検証
- オープンソースコミュニティへの貢献
- 次世代ソリューションへのOSS適用技術開発
- OSSライセンスに関する正しい知識の啓蒙



2009年4月設立



The diagram features a central grey circle with the text 'ThemiStruct'. Four colored circles are connected to it by black lines: a blue circle at the top right labeled 'セキュリティソリューション', a purple circle at the bottom right labeled 'グループウェアソリューション', a green circle at the bottom left labeled 'システムマネジメントソリューション', and a blue circle at the top left labeled 'セキュリティソリューション'.

ThemiStruct

セキュリティ
ソリューション

グループウェア
ソリューション

システム
マネジメント
ソリューション

- **ThemiStruct-IDM**
ID管理ソリューション
- **ThemiStruct-WAM**
Web統合認証管理ソリューション
(シングルサインオンソリューション)
- **ThemiStruct-CM**
電子証明書発行ソリューション
- **ThemiStruct-OTP**
ワンタイムパスワードソリューション
- **ThemiStruct-Portal**
企業情報ポータルソリューション
- **ThemiStruct-WorkFlow**
申請承認ワークフローソリューション
- **ThemiStruct-MONITOR**
システム監視ソリューション
- **ThemiStruct-TM**
チケット・インシデント管理ソリューション

- I. 講談社様導入事例のご紹介
- II. 適用したテクノロジー&ノウハウ
- III. クラウドサービス活用時代のシングルサインオン基盤
- IV. ThemisStructシリーズのご紹介

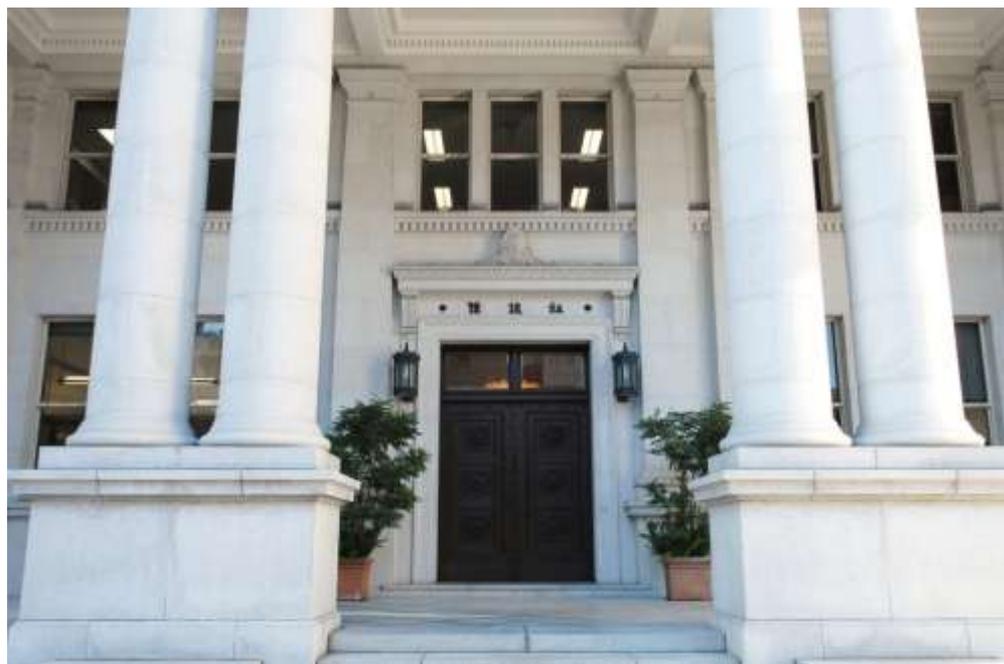
I. 講談社様導入事例のご紹介

1. 講談社事例の概要

講談社
KODANSHA

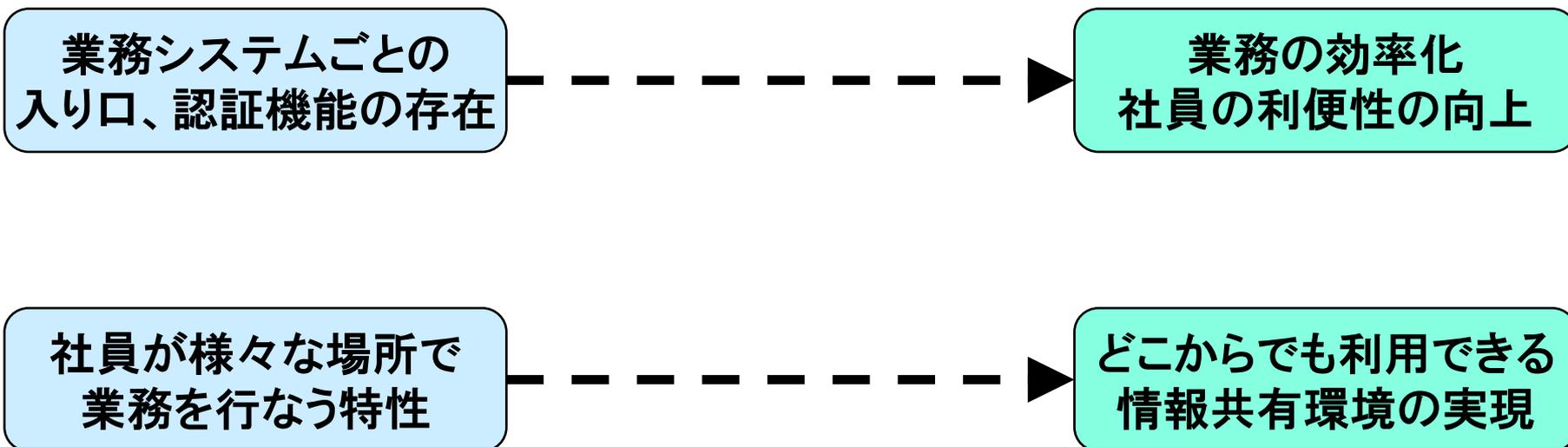
講談社様は「おもしろくて、ためになる」を基本理念とし、創業より100年という長い歴史を重ねてこられた日本を代表する出版社。出版事業を中心に、電子書籍事業、コンテンツを生かした映像化やアニメ化するライセンス事業など、様々な事業に取り組まれておられます。

事業の発展と共に複雑化するシステム環境の中で、認証環境の統合管理を実現する為のシングルサインオン環境を構築されるにあたり、当社ThemiStruct-WAMをご採用いただきました。



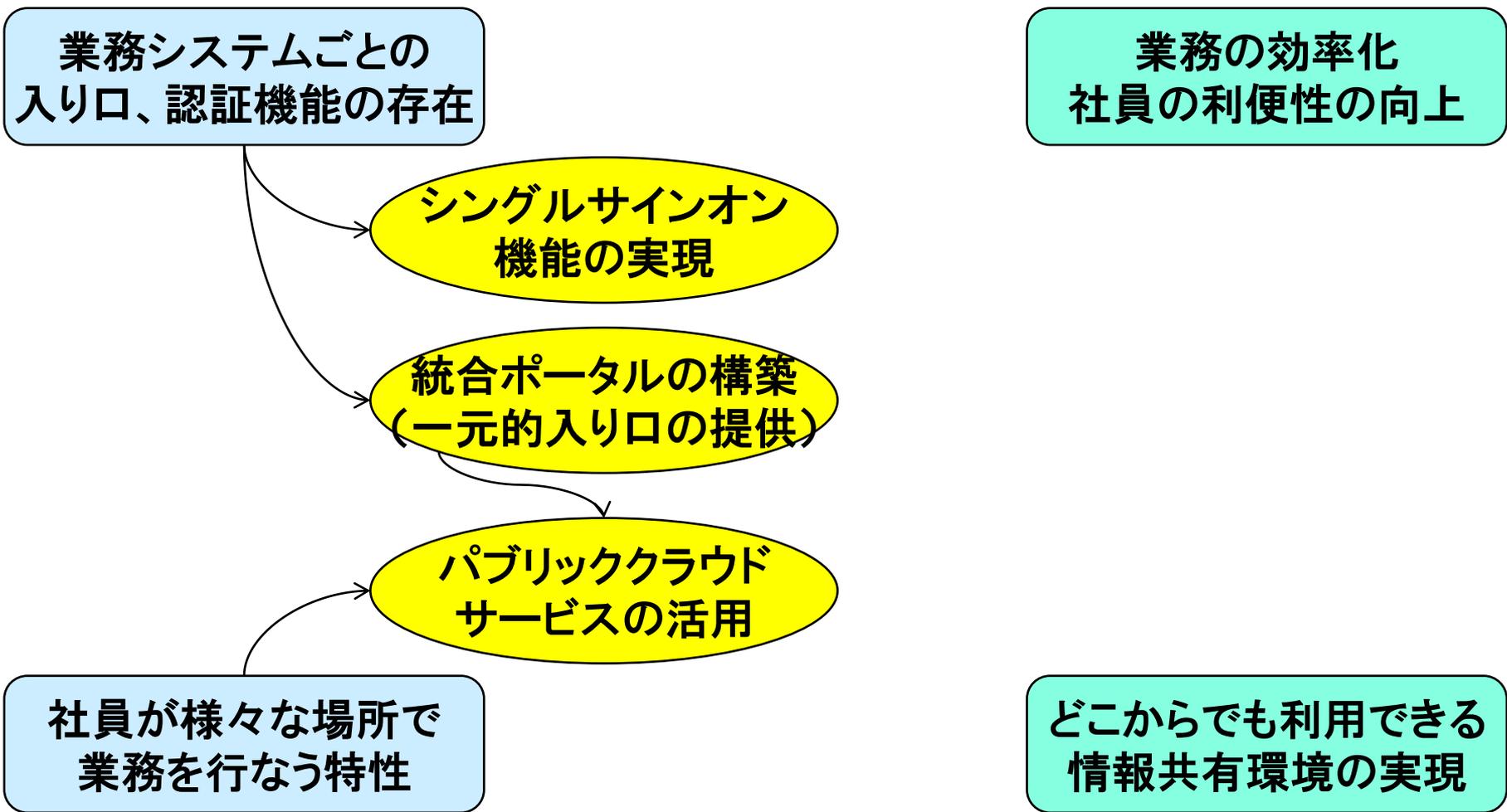
2. 統合ポータル導入の狙いと課題①

- 業務システムの入り口が作られて、わかりにくい、使いにくいという現状を改善するために、統合ポータルの導入を検討。
- どこからでも使える情報共有環境としての機能も持たせる。



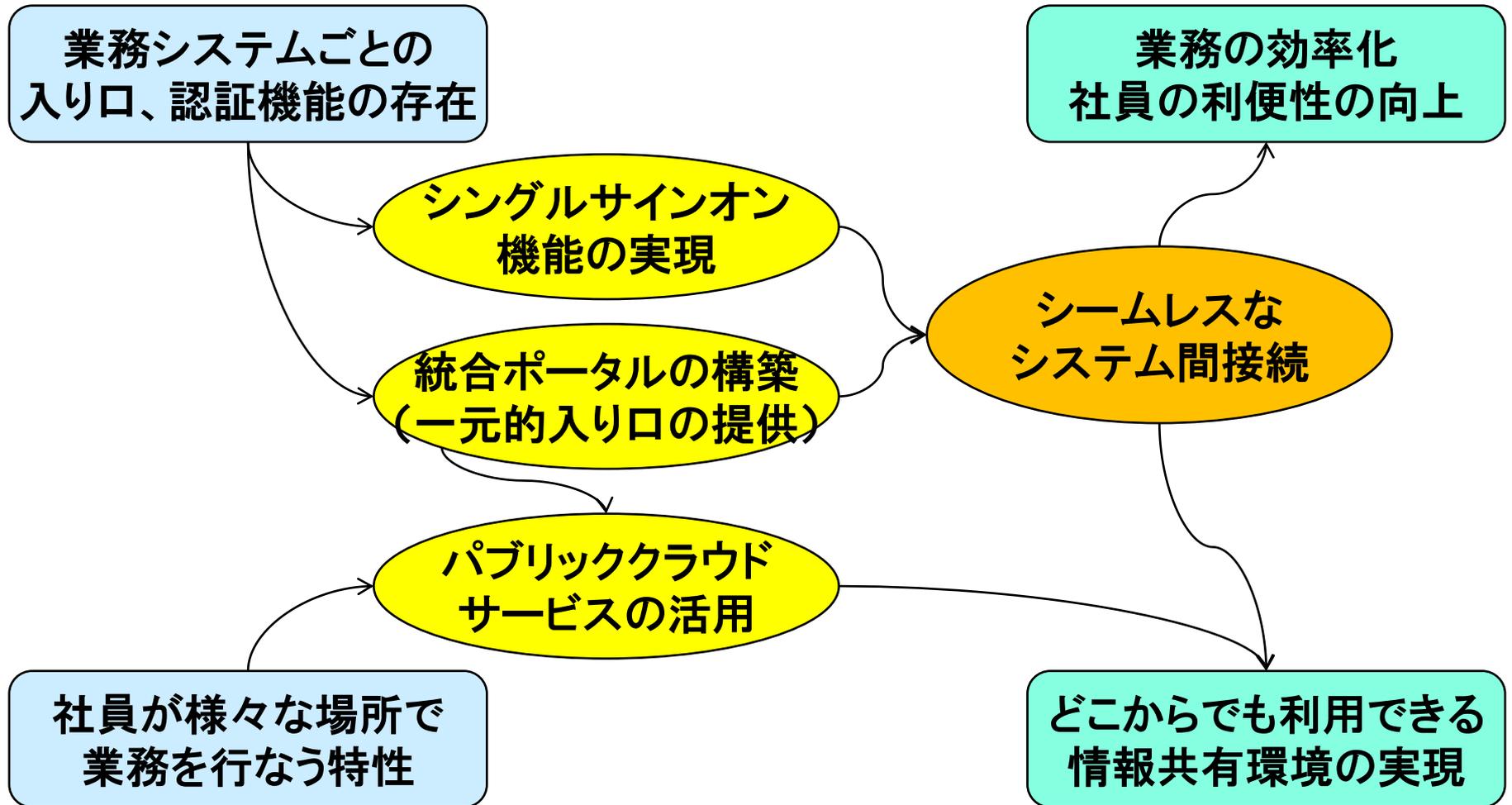
2. 統合ポータル導入の狙いと課題②

- 業務でシステムを使う時の一元的入り口として、統合ポータルを導入する。
- どこからでも使えるように、パブリッククラウドサービスを活用する。
- システム利用毎に認証をしないで済むよう、シングルサインオンを実現する。



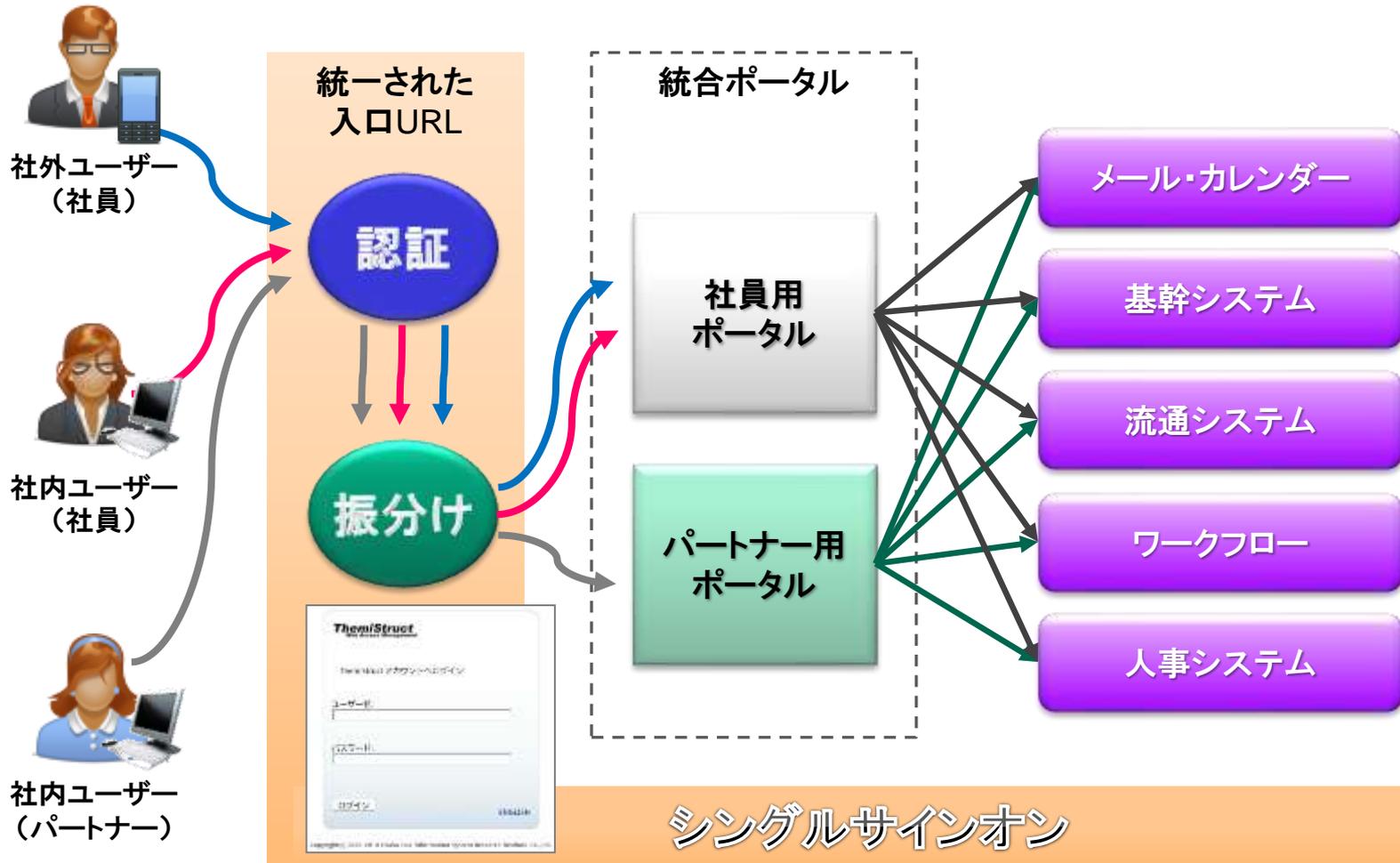
2. 統合ポータル導入の狙いと課題③

- シームレスなシステム間接続を実現することが、システム化を行なう上での重要ポイントとなる。



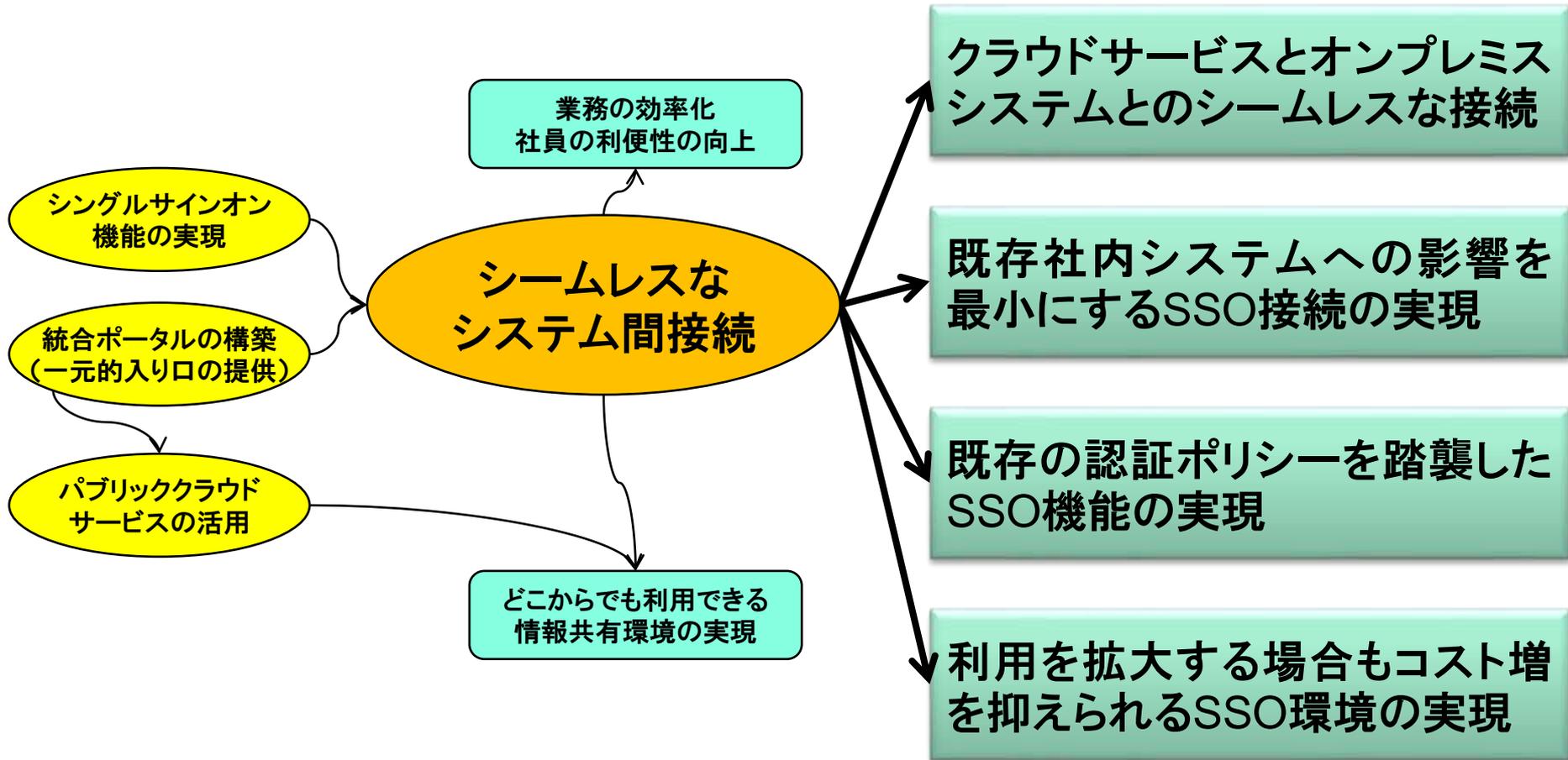
3. 構築された統合ポータル全体の全体像

- パブリッククラウドサービス上に、統合ポータルを構築。
- 統一された入り口URLでユーザーロールに合わせたポータル画面を表示。
- 統合ポータル、既存の業務アプリケーション間でシングルサインオンを実現。



4. シングルサインオン基盤への要求事項①

- OpenAMを使ってクラウド-オンプレミス間でのシングルサインオンを実現してほしいというシンプルな要求。
- 本質的課題は、認証ポリシーの実現、既存アプリの接続方法の部分にある。



4. シングルサインオン基盤への要求事項②

- OpenAMを使ってクラウド-オンプレミス間でのシングルサインオンを実現してほしいというシンプルな要求。
- 本質的課題は、認証ポリシーの実現、既存アプリの接続方法の部分にある。

クラウドサービスとオンプレミスシステムとのシームレスな接続

- **統合ポータルへのSAMLフェデレーション**
 - SSOログインIDと、統合ポータルログインID（メールアドレス）のマッピングへの対応

既存社内システムへの影響を最小にするSSO接続の実現

- **エージェント型でのSSOの実現**
 - IIS配下で動作するシステムへのSSOの実現
 - 改修困難なパッケージアプリケーションの円滑な移行
 - アプリケーションの修正必要箇所の早期提示と検証

既存の認証ポリシーを踏襲したSSO機能の実現

- **認証ポリシーの実現**
 - パスワード有効期限の確認、強制変更
 - アクセス元によるログイン可否の判定
 - 運用の手間を低減できる、パスワード忘れ時のセルフリセットへの対応

利用を拡大する場合もコスト増を抑えられるSSO環境の実現

- **OSSの活用**
 - ユーザー数、接続システム数によらず、一定の費用で構築、利用できる、OSS活用したSSO基盤の実現

5. Why OpenAM ?

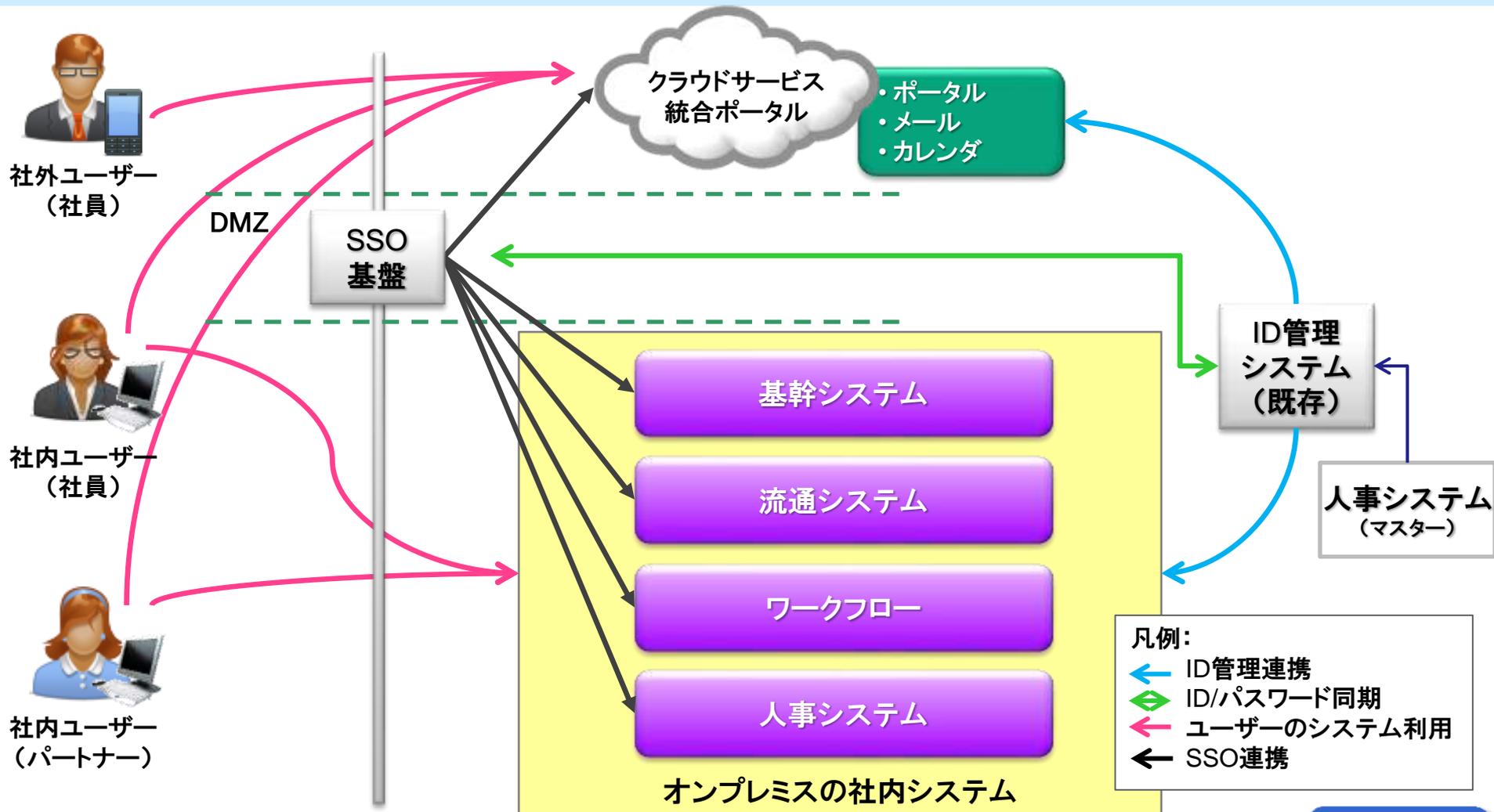
- お引合いをいただいた段階で、お客様自身がOpenAMの導入を検討されていた。
- SAML標準技術への対応
- 多様なエージェントの提供
- OSSであることから、ユーザー数、接続システム数によらない費用でのシステム実現が可能。

6. Why ThemisStruct-WAM ?

- OpenAMをコアとして、当社応用ノウハウや独自モジュールを加えてソリューションパッケージ化したThemisStruct-WAMを適用することで、お客様要求に応えるシングルサインオン基盤を実現。
- OpenAMをコアとしたソリューションパッケージ
- 当社ノウハウに基づく、アプリケーション連携方法の具体的なガイドランスの提供
- 多様な認証連鎖モジュールの提供
 - パスワード有効期限チェック、強制変更モジュール、
 - アクセス元IPを用いた認証可否チェックモジュール、など
- 独自修正を施したIISエージェントの提供
 - 属性情報のCookie連携への対応
 - 他のISAPIフィルターと組み合わせた利用への対応、など
- 独自要件に対応できる、モジュールやエージェントの開発力
 - ユーザー種別に合わせた表示サイト振分け対応用モジュール、など

7. 構築されたシングルサインオン基盤の全体像

- クラウドとのSSOはSAMLで、社内システムとのSSOはエージェント型で。
- 認証ポリシーの適用、ポータル画面の振分け等を認証連鎖モジュールで実現。
- ID管理は既存の仕組みを流用しつつ、パスワード変更機能をSSO側で実現。



8. 統合ポータル、シングルサインオンの導入によって得られた効果

- 統合ポータルとSSO実現は、利用者からも「判りやすい」との評価を得る。
- 同時に認証機能を標準化したことで、今後のシステム導入においても、一層のID管理、アクセス管理の品質が向上することが期待される。

■ ユーザービリティの向上

- 新ポータルにアクセスし、そこでログイン認証を行えば、必要な社内各システムにアクセスができ、個別認証が不要となったことで、「シンプルで判りやすい」と利用者から高い評価をいただいている。

■ セキュリティの向上

- システムのフロントにSSO環境を構築する事で、利用可能なアプリケーション制限や、パスワード変更管理などが集中管理できる為、セキュリティ面での統制が容易な環境が実現できた。

■ 認証環境の統合と標準化

- 社内の全システムの認証環境のデザインを整理し、標準化したことで、今後、新たなシステムを導入する際も、ID管理、アクセス管理への考慮が単純化される上、管理品質が一層向上することが期待できる。

II. 適用したテクノロジー&ノウハウ

主要要件をどう実現したか？

1. 認証ポリシーの実現
2. 既存アプリケーションのSSO接続
(早く、できるだけ変更なく)

1. 認証ポリシーの実現

- 実現したい認証ポリシーは、どのお客様からのご要望をいただくもの。

実現した認証ポリシー

認証は統一されたユーザーID、パスワードを使って行なう。

パスワードには有効期限を設定し、有効期限が切れている場合は強制的に変更させる。

社外からのシステム利用を想定するが、利用できる人は、事前に許可された人に限定する。

認証後は、ユーザー種別(社員、パートナー)に応じたポータル画面を表示する。

パスワード忘れ時の対応は、自分自身で行なえるようにし、システム担当者の手間を削減する。

1. 認証ポリシーの実現

- 実現したい認証ポリシーは、どのお客様からのご要望をいただくもの。
- OpenAMの標準機能で実現できることは限定的。
- 積極的に認証連鎖モジュールを開発することで、要求を実現。

実現した認証ポリシー

認証は統一されたユーザーID、パスワードを使って行なう。

パスワードには有効期限を設定し、有効期限が切れている場合は強制的に変更させる。

社外からのシステム利用を想定するが、利用できる人は、事前に許可された人に限定する。

認証後は、ユーザー種別(社員、パートナー)に応じたポータル画面を表示する。

パスワード忘れ時の対応は、自分自身で行なえるようにし、システム担当者の手間を削減する。

実現の方針

OpenAM標準の機能で実現

当社オリジナルの認証連鎖モジュールを適用して実現

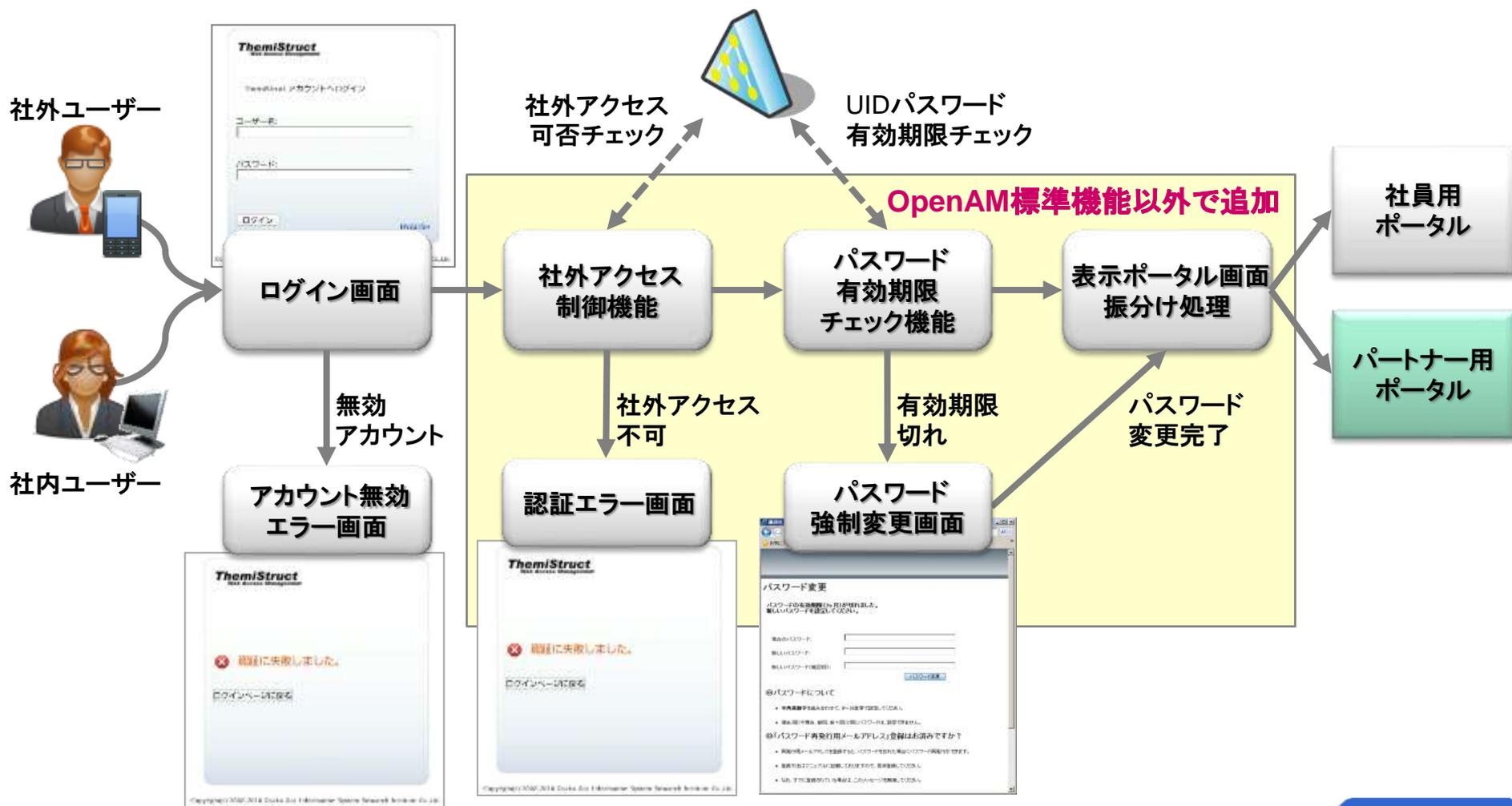
- ・ パスワード有効期限チェックモジュール
- ・ パスワード強制変更モジュール
- ・ アクセス元IPを用いた認証可否チェックモジュール、等

お客様専用の認証連鎖モジュール類を開発して実現

- ・ セカンダリーメールアドレスを用いたパスワード再発行アプリケーション
- ・ パスワード変更画面へのセカンダリーメールアドレスメンテナンス機能の統合
- ・ 表示サイト振分け対応用モジュール、等

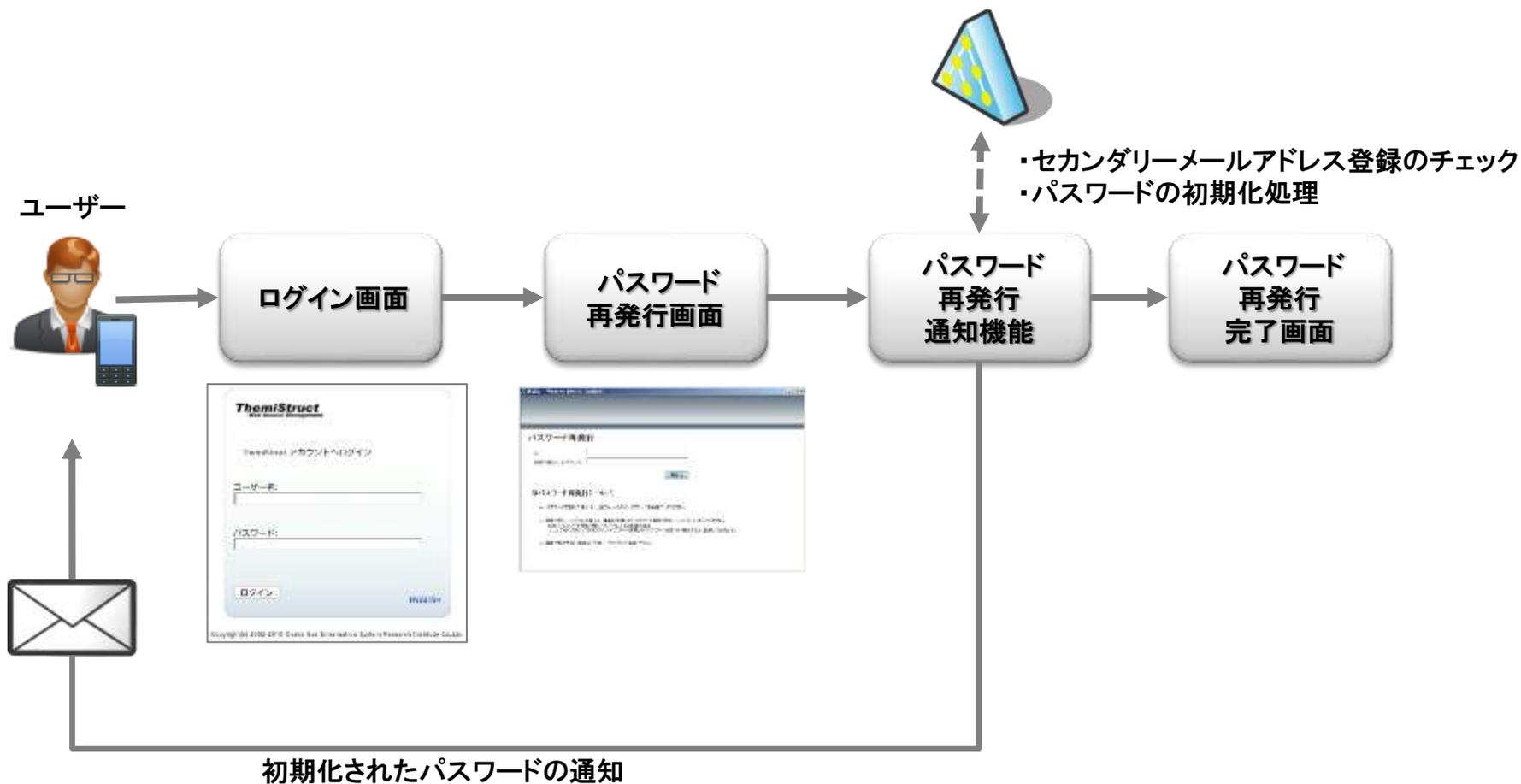
1.1 実現された認証フロー

- 認証連鎖モジュールを開発、組合せることで要求通りの認証ポリシーを実現。
- 特にポータル画面振分けの機能は、ユーザーへ知らせるURLの単一化と、簡略化（サーバー名だけでよい）に大きく役立った。



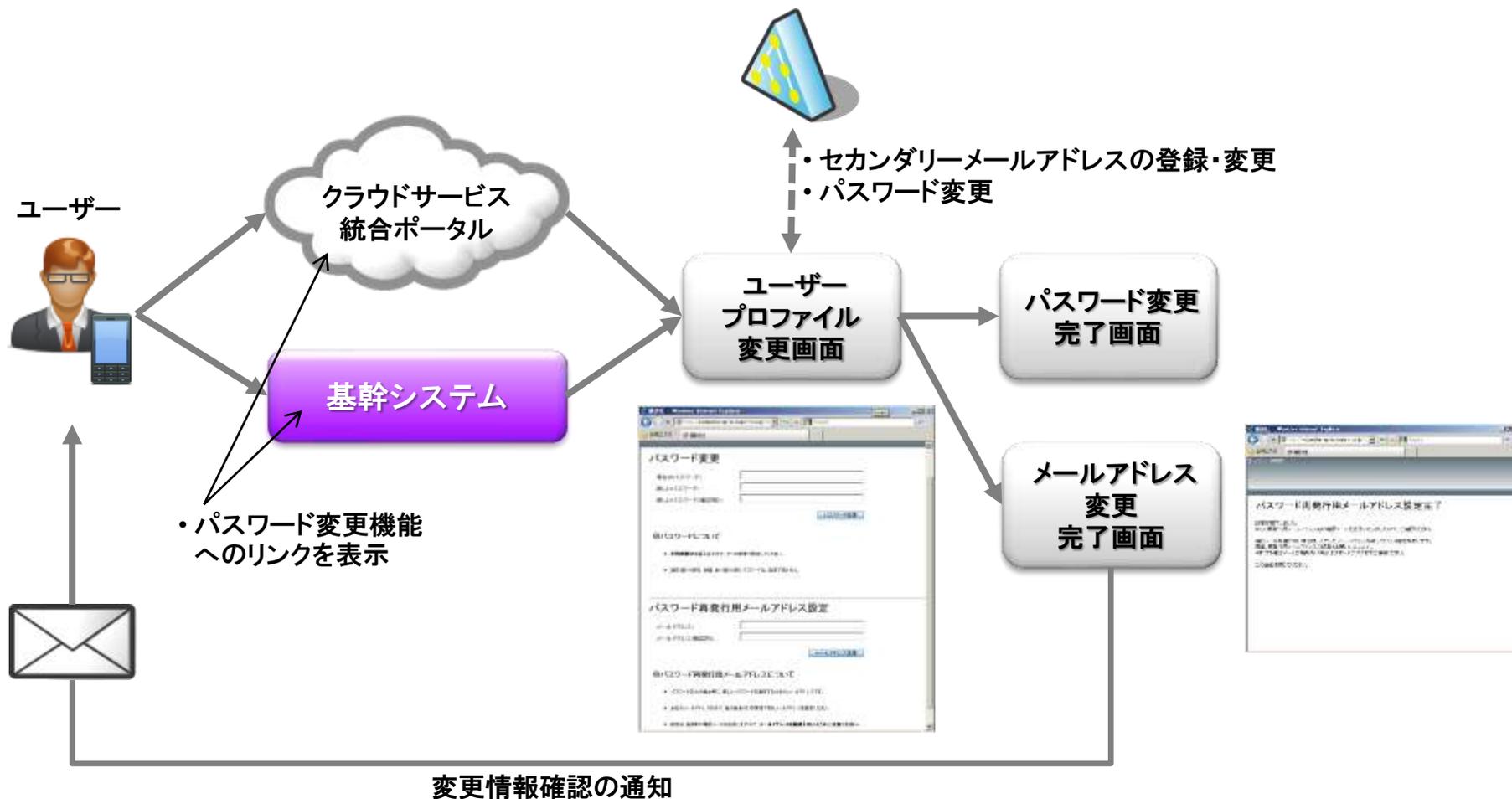
1.2 パスワード忘れ時のセルフリセット

- セカンダリーメールアドレスを使用する方式をお客様にご提案。
- お客様と具体的な処理フローを検討し、専用のセルフリセットの仕組みを実現。



1.3 パスワード変更・セカンダリーメールアドレス登録・変更

- セカンダリーメールアドレスの登録、最新化を意識づけられるように、パスワード変更画面と統合した画面として実装。



2. 既存アプリケーションのSSO接続(早く、できるだけ変更なく)

- シングルサインオン基盤は、アプリケーションへのSSOができるようになって初めて完成する。そのための対応をお客様は要望される。

既存アプリケーションのSSO接続に 関するお客様のご要望

統合ポータルとのSAML連携の実現に関する具体的な方式を提示すること。

既存アプリケーションへのSSO接続実現に関する具体的な方式を提示すること。

プロジェクト開始後、早い段階で、アプリケーション担当者への技術的説明、役割分担の実施し、アプリケーションの対応を早期に開始させられること。

2. 既存アプリケーションのSSO接続(早く、できるだけ変更なく)

- シングルサインオン基盤は、アプリケーションへのSSOができるようになって初めて完成する。そのための対応をお客様は要望される。
- 10年以上認証基盤構築を行ってきた当社ノウハウで、ご要望に応える。

既存アプリケーションのSSO接続に 関するお客様のご要望

対応の方針

統合ポータルとのSAML連携の実現に関する具体的な方式を提示すること。

OpenAM標準の機能での実現方式を提示。

既存アプリケーションへのSSO接続実現に関する具体的な方式を提示すること。

当社のノウハウをベースとしたSSO接続方式の具体的な説明の実施。

- ・ どの方法が一番うまく動くか？
- ・ どの方法が一番費用がかからないか？
- ・ どの方法が一番早くできるか？

プロジェクト開始後、早い段階で、アプリケーション担当者への技術的説明、役割分担の実施し、アプリケーションの対応を早期に開始させられること。

アプリケーション担当者向け開発ガイドのテンプレートを用いた、プロジェクト初期段階での説明会の実施。

2.1 選択したSSO接続方式

- SSO側は標準的な連携方式とする方針で、接続方式を選択した。
- アプリケーション側でのいくらかの改修をしていただけたため、シンプルな方式でSSO接続ができた。

アプリケーション名	サーバー	SSO接続方式	選択のポイント
統合ポータル	クラウド	SAML連携	クラウドサービスを利用するため、標準であるSAML連携を使用。
基幹システム	IIS	エージェント型 HTTP Header連携	スクラッチ開発されたアプリ。保守ベンダーがアプリ改修で対応。
流通システム	IIS	エージェント型 Cookie連携	既存のパッケージアプリケーション。仕様上アプリ改修不要で対応ができそうであったため、Cookie連携方式を選択。
ワークフロー	IIS	エージェント型 Cookie連携	
人事システム	IIS	エージェント型 HTTP Header連携	パッケージを利用したアプリ。ベンダーにてカスタマイズをして対応。

2.2 パッケージアプリケーションへのCookie連携例

- パッケージ固有のSSO連携仕様との互換性の実現が課題。

統合ポータル効果を最大化するためには、このパッケージアプリケーションへのSSO実現が必須。しかし、プロジェクトの期間・コストの観点から、アプリケーションの改修が要らない方式の方が望ましい。



アプリの円滑な移行のための検討事項

IISでの構成に対応が行なえること。

既存アプリが使用しているIIS用フィルターと共存ができること。

- これができない場合、Agent型での構成ができず、サーバー構成を大きく見直す必要がある。

パッケージのSSO連携仕様と同等の情報をCookieで渡すことができること。

- SSO連携仕様との互換性の実現により、アプリを修正することなく接続することを狙う。

2.2 パッケージアプリケーションへのCookie連携例

- パッケージ固有のSSO連携仕様との互換性の実現が課題。
- 当社にてカスタマイズ済みのIISエージェントを提供することで機能実現。
- 統合ポータル導入効果の向上を実現するとともに、コスト削減にも貢献。

統合ポータルの効果を最大化するためには、このパッケージアプリケーションへのSSO実現が必須。しかし、プロジェクトの期間・コストの観点から、アプリケーションの改修が要らない方式の方が望ましい。



アプリの円滑な移行のための検討事項

対応の方針

IISでの構成に対応が行なえること。

OpenAM標準エージェントで対応可能

既存アプリが使用しているIIS用フィルターと共存ができること。

当社カスタマイズ済みのIISエージェントを提供して実現。

- ・ これができない場合、Agent型での構成ができず、サーバー構成を大きく見直す必要がある。

- ・ 既存のフィルターと共存してエージェント導入ができたため、サーバー構成を変更せず対応ができた。

パッケージのSSO連携仕様と同等の情報をCookieで渡すことができること。

当社カスタマイズ済みのIISエージェントを提供して実現。

- ・ SSO連携仕様との互換性の実現により、アプリを修正することなく接続することを狙う。

- ・ アプリケーションが要求するSSO連携仕様を調査・確認し、同等の機能を実現した。

2.3 使用した当社カスタマイズ済みIISエージェントの特徴

- 当社にてIIS向けエージェントをISAPIフィルター型で実装したものの。
- Apache用エージェントに近い実装としている。
- Cookie連携、入力パスワードの連携などの機能に修正を加えている。

機能	標準エージェント	当社エージェント
バージョン	3.0.4	—
実装アーキテクチャ	モジュール型	ISAPIフィルター型
IIS6/IIS7のサポート	○	○
HTTPヘッダでの属性連携	○	○
Cookieでの属性連携	△ 同一キーの変数のオーバーライドができない制限あり。	○
他のISAPIフィルターと組み合わせた利用	×	○
入力パスワードの連携 (パスワードリプレイ)	×	○
長いパスワード長への対応	—	○

III. クラウドサービス活用時代の シングルサインオン基盤

1. クラウドサービスを活用するうえでの課題

- クラウド上のサービスは、誰でもどこからでも利用できるのが最大の特徴。

クラウド上のサービスの特性

アカウントがあれば誰でも

各サービス毎に管理された
IDとパスワードで

組織内のネットワークからでも

組織外のネットワークからでも

組織で管理された端末でも

個人の端末でも

利用できる

クラウドサービス

Google Apps

Salesforce

Office365

App1



1. クラウドサービスを活用するうえでの課題

- クラウド上のサービスは、誰でもどこからでも利用できるのが最大の特徴。
- 各組織で要求される認証ポリシーをクラウド上のサービス側で実現できないケースもしばしばある。

クラウド上のサービスの特性

アカウントがあれば誰でも

各サービス毎に管理された
IDとパスワードで

組織内のネットワークからでも

組織外のネットワークからでも

組織で管理された端末でも

個人の端末でも

利用できる

組織での認証ポリシー例

アカウントは全員分作成し

パスワードは定期的に変更して

N回認証失敗の場合は
アカウントをロックして

組織内からはIDとパスワードで

組織外からのアクセスの場合は
ワンタイムパスワードを併用して

組織から貸与した端末を使って

個人の端末の使用は禁止して

利用させる

クラウドサービス

Google Apps

Salesforce

Office365

App1



2. シングルサインオン基盤による課題解決

- 認証ポリシーの実現はシングルサインオン基盤で、アプリケーションの機能はクラウドサービスで、という役割分担で課題を解決する。

組織での認証ポリシー例

アカウントは全員分作成し

パスワードは定期的に変更して

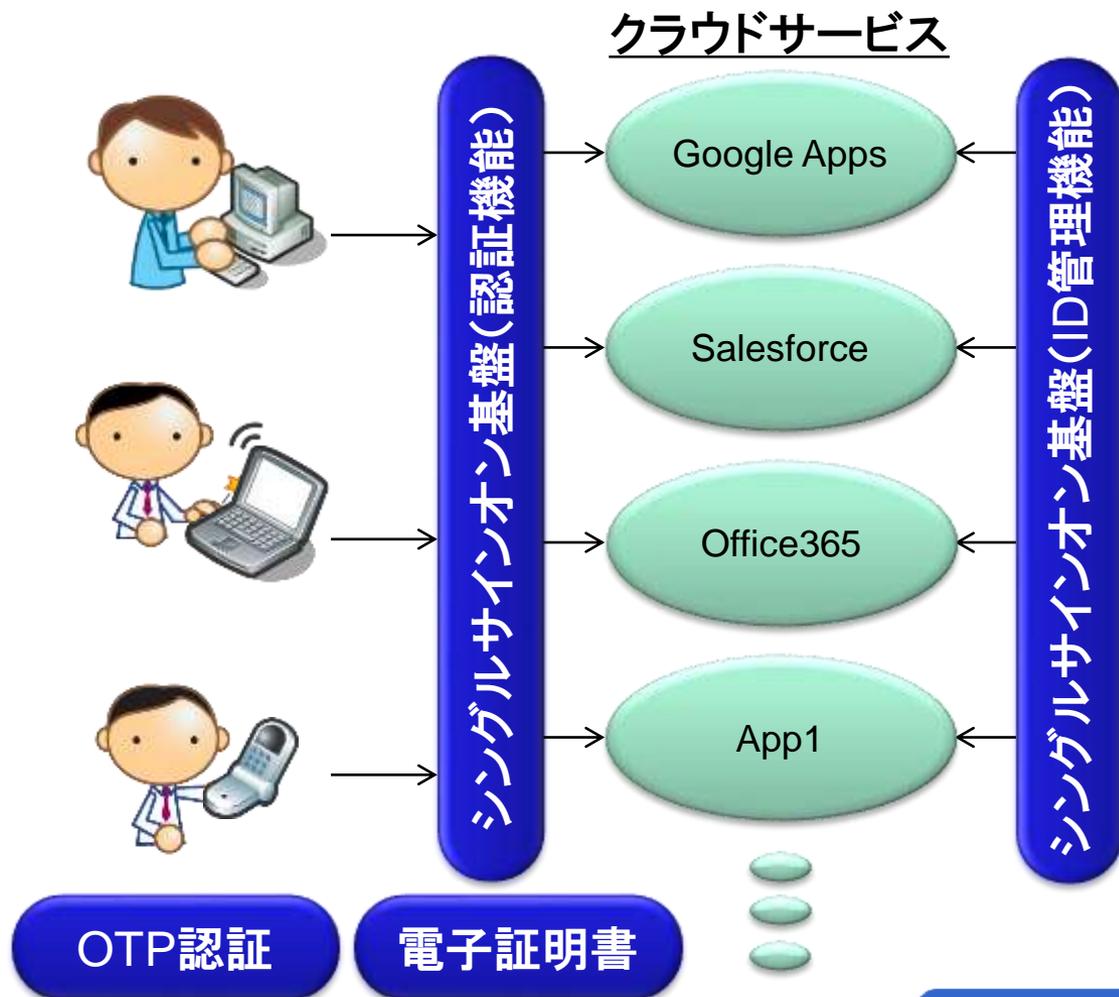
N回認証失敗の場合は
アカウントをロックして

組織内からはIDとパスワードで

組織外からのアクセスの場合は
ワンタイムパスワードを併用して

組織から貸与した端末を使って

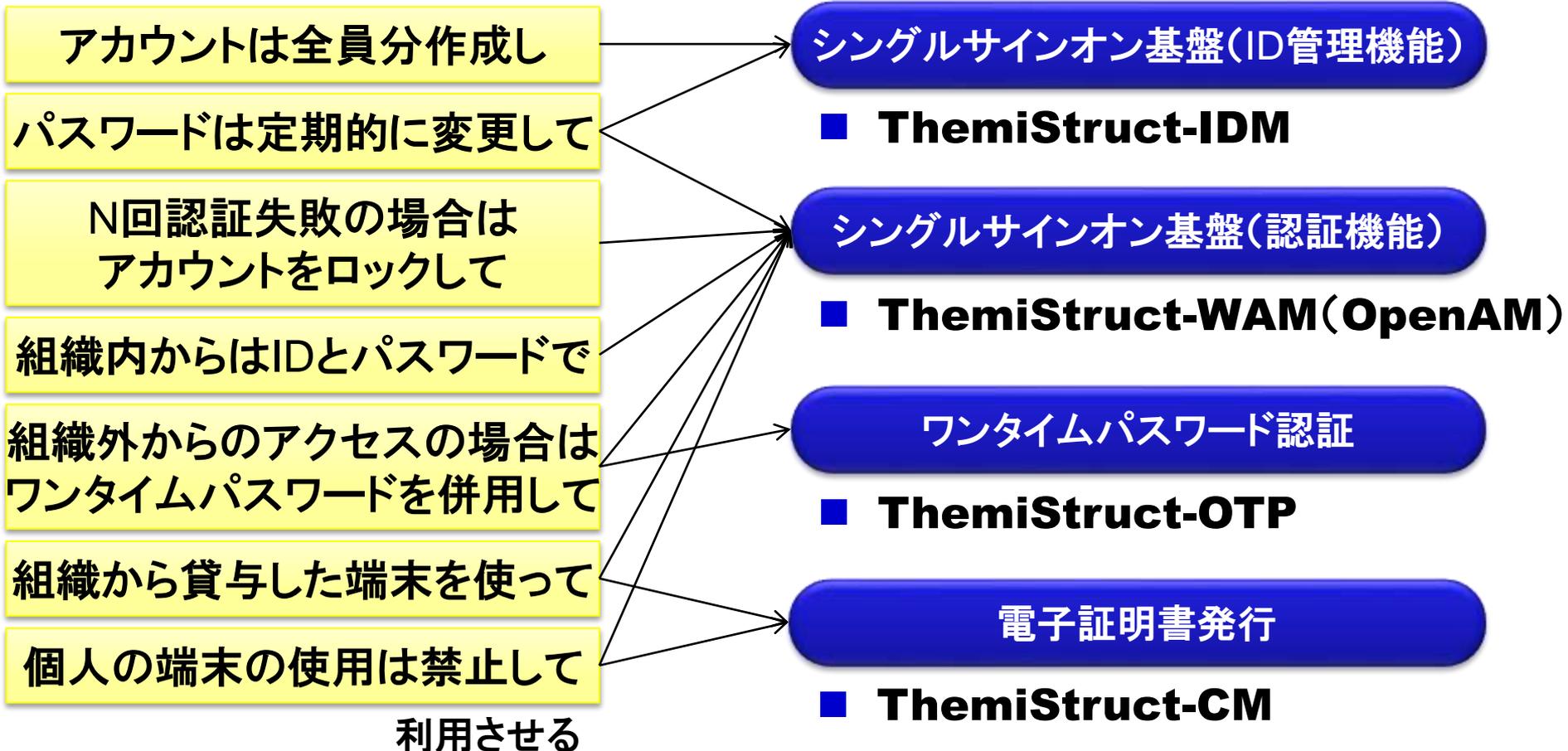
個人の端末の使用は禁止して
利用させる



2. シングルサインオン基盤による課題解決

- 認証ポリシーの実現はシングルサインオン基盤で、アプリケーションの機能はクラウドサービスで、という役割分担で課題を解決する。
- 認証機能を提供するシングルサインオンソリューションを中心として構成。

組織での認証ポリシー例



3. クラウドサービスのワンタイムパスワード認証対応 x ThemisStruct

- ThemisStruct-OTPを使うことで、携帯電話、スマートフォンをトークン生成器として利用可能。



アプリケーションのインストール、QRコードの取込みだけで、携帯電話、スマートフォンがワンタイムパスワードのトークンに。

3. クラウドサービスのワンタイムパスワード認証対応 x ThemisStruct

- ThemisStruct-OTPを使うことで、携帯電話、スマートフォンをトークン生成器として利用可能。
- ThemisStruct-OTP連携用認証連鎖モジュールを組み込めばOTP認証対応に。

カメラを利用してQRコードからユーザー個別のキーをセットすることができる。

IDとパスワードでの認証

ワンタイムパスワードの入力

SSO環境でアプリケーションの利用

アプリケーションのインストール、QRコードの取込みだけで、携帯電話、スマートフォンがワンタイムパスワードのトークンに。



4. クラウドサービスの電子証明書認証対応 x ThemisStruct

- ThemisStruct-CMで、PCのブラウザやスマートフォンへ電子証明書を発行。

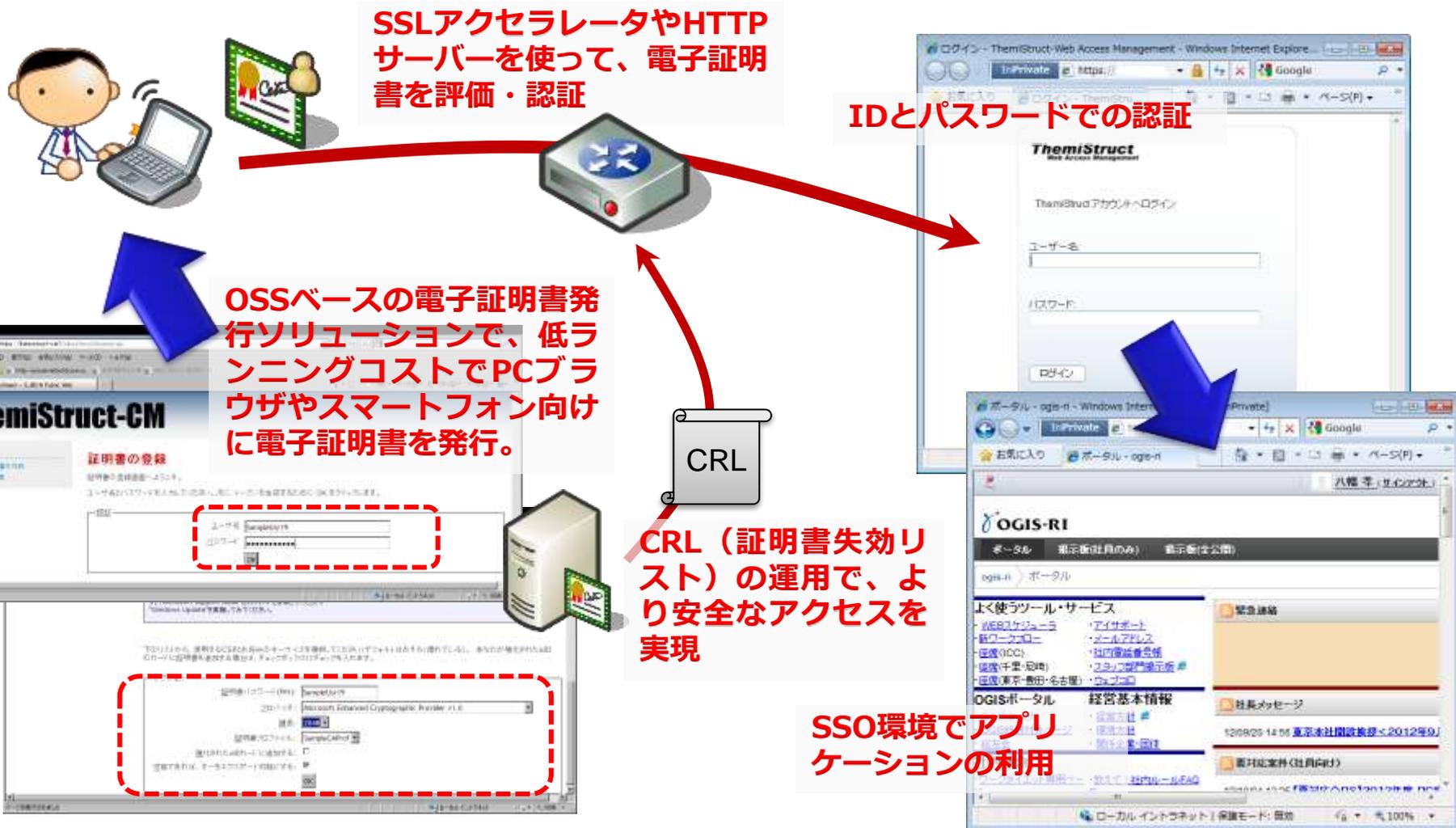


OSSベースの電子証明書発行ソリューションで、低ランニングコストでPCブラウザやスマートフォン向けに電子証明書を発行。

A screenshot of the ThemisStruct-CM web interface. The page title is "ThemisStruct-CM". There is a section titled "証明書の登録" (Certificate Registration). Below this, there are input fields for "ユーザID" (User ID) and "パスワード" (Password). A red dashed box highlights these fields. Below the input fields, there is a section for "証明書情報" (Certificate Information) with a red dashed box around it. This section includes a dropdown menu for "証明書タイプ" (Certificate Type) set to "Microsoft Enhanced Cryptographic Provider #1.0", a "検索" (Search) button, and a "証明書ID" (Certificate ID) field. There is also a small icon of a server tower and a digital certificate icon to the right of the screenshot.

4. クラウドサービスの電子証明書認証対応 x ThemisStruct

- ThemisStruct-CMで、PCのブラウザやスマートフォンへ電子証明書を発行。
- ThemisStruct-WAMへのSSLアクセスで、証明書がある端末だけをアクセス許可することで、認証された端末を使うユーザーのみを認証可能。



IV. ThemisStructシリーズのご紹介

オージス総研が提供する、
**OSS（オープンソースソフトウェア）を活用した
IT基盤ソリューション全体を指すブランド名です。**

■ **Themis**

- テミス。ギリシャ神話上の法・掟の女神。「不変なる掟」との意味も。

■ **Struct**

- ストラクチャ。構造。(IT)基盤の意味。



合わせてIT基盤上の掟(=ガバナンス、セキュリティ)を守るものという意味を込めています。

■ セキュリティリスクの軽減

- ID管理、認証処理の一元管理
- システム単位でのアクセス制御の一元管理
- アカウントポリシー、パスワードポリシーの一元管理
- システムへのアクセス記録の一元管理

■ 開発のコスト削減

- 認証機能、アクセス制御機能の個別実装が不要
 - 特にID管理、認証処理
- セキュリティポリシー変更時の個別開発が不要
 - 認証方式の変更

■ ユーザーの利便性向上

- ユーザーID/パスワードが統一される
- 一度のログインで複数アプリケーションをシームレスに利用可能
- ユーザーサポートコストの低減

3. 認証基盤を活用する

ねらい
メリット

セキュリティリスクの軽減
開発コストの削減
ユーザーの利便性の向上

広げる・永く使い続ける

アプリケーションを集める

アプリケーションをつなぐ

認証基盤を作る

- システム活用が進む、動線の提供
- スマートデバイスなどの新しい技術、UIへの対応
- ロケーションを問わないシステム利用環境の提供

- 共通基盤としての利用ルール整備
- 接続方式のパターン化・標準化
- 開発担当向けガイドの提供
- レビュー等による標準外構成の除外

- 接続方式の決定・設定
- アプリケーションの修正
- 認証基盤側でのカスタマイズ対応

- SSO製品の導入
- IDM製品の導入

4. なぜOSS活用なのか？

■ コスト削減

- ユーザー数増加によるライセンス費用、保守費用の増加が抑制できる。

➡ コンシューマー向けサイト運用においても費用負担を大幅軽減

■ 構成の柔軟性

- オープンソースソフトウェアの活用により、特定のソフトウェア、ハードウェアへの依存度が減り、構成の柔軟性が確保される。

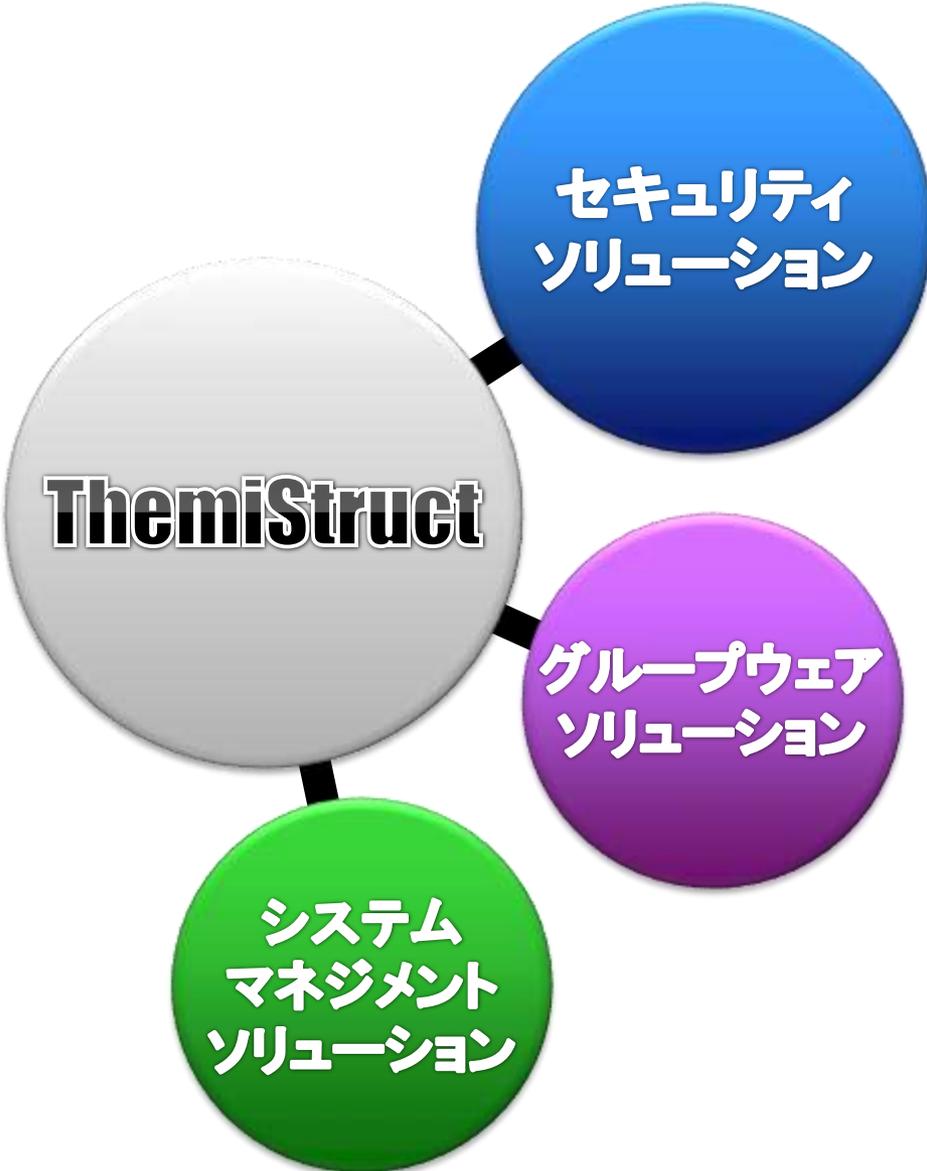
➡ 商用UNIXサーバーからLinuxサーバーへの変更、集約へ道筋

■ 長期間サポート

- オープンソースであるため、徹底的な原因究明が可能。
- ソースコードを使った長期間サポートが可能。

➡ 長い目で見た信頼性向上の実現

5. ThemisStructシリーズラインナップ



The diagram features a central grey circle with the text 'ThemisStruct'. Four colored circles are connected to it by black lines: a blue circle at the top right labeled 'セキュリティソリューション', a purple circle at the bottom right labeled 'グループウェアソリューション', a green circle at the bottom left labeled 'システムマネジメントソリューション', and a white circle at the top left which is empty.

ThemisStruct

セキュリティ
ソリューション

グループウェア
ソリューション

システム
マネジメント
ソリューション

- **ThemisStruct-IDM**
ID管理ソリューション
- **ThemisStruct-WAM**
Web統合認証管理ソリューション
(シングルサインオンソリューション)
- **ThemisStruct-CM**
電子証明書発行ソリューション
- **ThemisStruct-OTP**
ワンタイムパスワードソリューション
- **ThemisStruct-Portal**
企業情報ポータルソリューション
- **ThemisStruct-WorkFlow**
申請承認ワークフローソリューション
- **ThemisStruct-MONITOR**
システム監視ソリューション
- **ThemisStruct-TM**
チケット・インシデント管理ソリューション

6. ThemisStructシリーズラインナップ一覧

ソリューション		コアOSS	概要
セキュリティ	ThemisStruct-WAM (Web統合認証管理ソリューション)	OpenAM	<ul style="list-style-type: none"> Webアプリケーションの統合認証ソリューション リバースプロキシ型とエージェント型の両方式に対応可能 SalesforceやGoogle Appsへのシングルサインオンにも対応
	ThemisStruct-IDM (ID管理ソリューション)	Mule ESB	<ul style="list-style-type: none"> ユーザーのアカウント情報を一元管理し、アカウントの作成、更新、削除を自動化(プロビジョニング)するID管理ソリューション SalesforceやGoogle Appsへのプロビジョニングにも対応
	ThemisStruct-CM (電子証明書発行ソリューション)	EJBCA	<ul style="list-style-type: none"> 電子証明書を利用したプライベート端末認証ソリューション 外部認証局方式と比較して安価で必要十分なセキュリティ スマホなど外部アクセス端末の増加に対応可能
	ThemisStruct-OTP (ワンタイムパスワードソリューション)	Google Authenticator	<ul style="list-style-type: none"> 端末IDから生成するワンタイムパスワード発行ソリューション スマートフォンを利用するため、専用ハードウェアの購入・維持管理費用が不要
グループウェア	ThemisStruct-Portal (企業情報ポータルソリューション)	Liferay	<ul style="list-style-type: none"> 各種ポートレットを利用し企業内情報ポータルソリューション 既存のIT資産を最大限活用するプラットフォームとして活用 Web統合認証を利用しポータルとしての連携対応可能
	ThemisStruct-WorkFlow (申請承認ワークフローソリューション)	jBPM	<ul style="list-style-type: none"> 必要かつ十分な機能を備えたワークフローソリューション 申請書(フォーム)と経路(フロー)がユーザーで自由にデザインできるエディタを標準装備
システム マネジメント	ThemisStruct-TM (チケット・インシデント管理ソリューション)	OTRS	<ul style="list-style-type: none"> 様々な「問い合わせ」業務の管理の効率化や知識の共通化を支援 コールセンターでの対応の記録から、ITILを活用した業務最適化コンサルティングまで対応可能
	ThemisStruct-MONITOR (システム監視ソリューション)	ZABBIX	<ul style="list-style-type: none"> システムの稼働監視(サーバー、プロセス、サービスなど)、パフォーマンス監視、ログ監視をする機能を提供。 クラウドサービスの安定稼働を実現するSOA基盤監視に対応予定

- クラウドサービスと社内システムとの間をシームレスに接続した、講談社様のSSO導入事例を紹介。
- クラウドサービスとのSSO実現の際には、SAML等の認証連携方式に対応しているか、ということに目が行きがち。
- お客様の要求は、①自組織の認証ポリシーをいかに実現するか、②既存アプリケーションへの影響を最小限にSSOを実現するか、の2点にあった。
- 当社の約10年にわたる認証基盤の構築、運用の経験とノウハウ、OpenAM向けのオリジナルモジュール類を適用して、お客様の要求にお応えするシングルサインオン基盤を構築した。
- こうした経験とノウハウを**ThemiStruct**シリーズとして提供しています。

ご清聴ありがとうございました

【お問合せ先】

**株式会社オージス総研
東日本営業部**

TEL 03-6712-1201
E-mail info@ogis-ri.co.jp