

OpenAM は OpenID Connect Ready. ThemiStructでエンブラ系へどう広めるか？

テ ミ ス ト ラ ク ト

株式会社オージス総研
サービス事業本部

八幡 孝

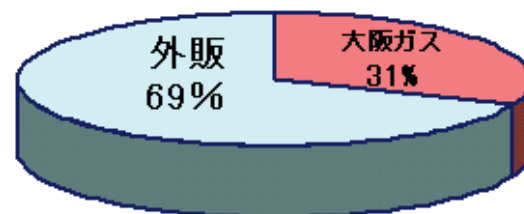
2014年3月7日



オービス総研です

株式会社オービス総研

- 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
- 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
 - 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: 550億円(連結) 283億円(単体) (2012年度)
- 従業員数: 3,064名(連結) 1,268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、上海欧計斯软件有限公司(中国)
- オービス総研グループ 売上構成比 (連結)



Design Your Energy 夢ある明日を



大阪ガス
GROUP

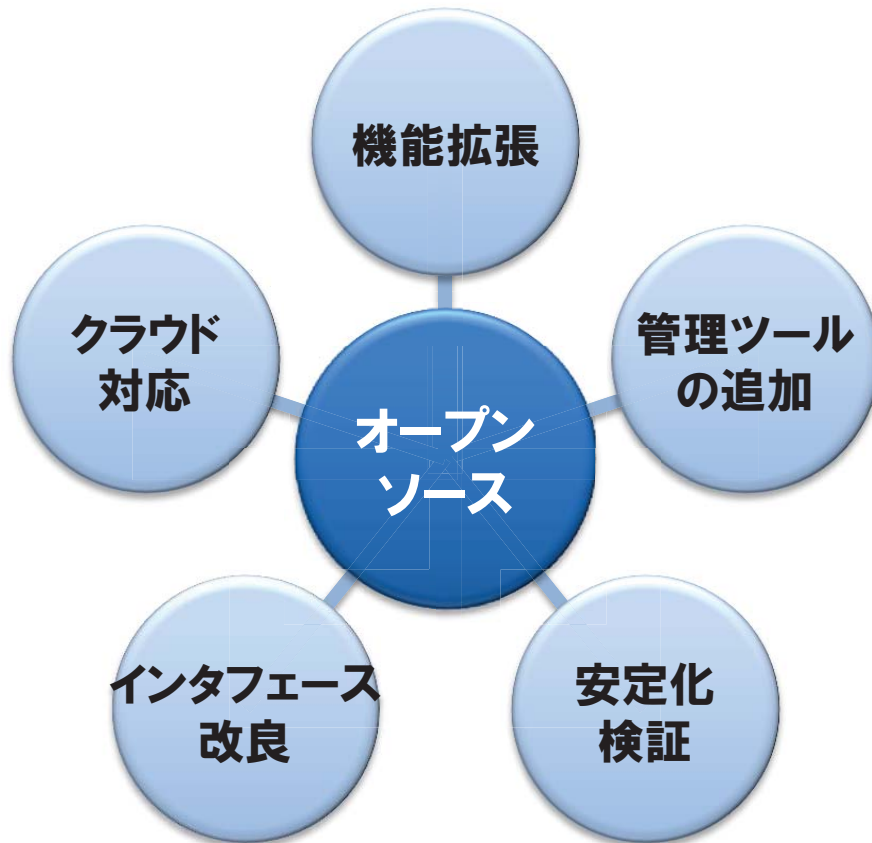


取得許可認定



ThemiStruct はOSS活用IT基盤ソリューション

テ ミ ス ト ラ ク ト



- **ThemiStruct-WAM** (OpenAM)
 - シングルサインオン認証基盤ソリューション
- **ThemiStruct-IDM** (OpenIDM)
 - ID管理ソリューション
- **ThemiStruct-CM** EJBCA
PKI BY PRIMEKEY
 - 電子証明書発行・管理ソリューション
- **ThemiStruct-OTP**
 - ワンタイムパスワードソリューション
- **ThemiStruct-WorkFlow**
 - 申請承認ワークフローソリューション
- **ThemiStruct-MONITOR** **ZABBIX**
 - システム監視ソリューション
- **ThemiStruct for Office365**
 - Microsoft Office365認証強化ソリューション

OpenAM/OpenIDM、本気でやっています

- オージス総研、IT基盤ソリューション「ThemiStruct(R) (テミストラクト)」を大幅リニューアル (2014年1月28日)

http://www.ogis-ri.co.jp/news/1212304_6734.html

実績のある
オープンソース
ソフトウェア



独自の機能拡張
や管理ツールの
追加



1,000項目以上の
徹底的なテストや
検証などを実施

継続的に実行可能な開発・テストプロセスを整備



お客様に安心してお使い
いただけるソフトウェアと
サポートをご提供



開発コミュニティへ
バグフィックス等の成果を
フィードバック

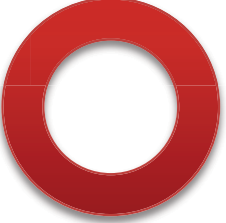
OpenAM は OpenID Connect Ready!

Released	Released	2014	2015
OpenAM 10.1	OpenAM 11.0	OpenAM 12.0	OpenAM 13.0
<u>Standards:</u> ▪ OAuth 2.0 Provider ▪ OATH OTP AuthN module ▪ REST: Identity Management JSON based <u>Core:</u> ▪ New Session Failover ▪ OpenAM now bundles OpenDJ 2.4.6	<u>Cloud:</u> ▪ Multi-Tenant Phase 1 – Core Architecture ▪ Cloud Dashboard - Preview <u>Standards:</u> ▪ OpenID Connect ▪ REST Enhancements <u>Core:</u> ▪ Risk Based AuthN includes Device-print ▪ OpenAM IPv6 support ▪ OpenAM Java 7 support ▪ Varnish Policy Agent	<u>Cloud:</u> ▪ Multi-Tenant Phase 2 - Scale and Management ▪ Cloud Dashboard and Connector Wizards (SF, Google, Webex, Office 365, Facebook) <u>Standards:</u> ▪ Entitlements Policy Editor <u>Core:</u> ▪ Core Token Service Phase 2 ▪ Risk Based AuthN scripting engine (for adding custom parameters)	<u>Cloud:</u> ▪ Multi-Tenant Phase 3 - Elasticity <u>Standards:</u> ▪ OAuth 2.0 End User Console <u>Core:</u> ▪ REST Secure Token Service Enhancements ▪ Agent and OpenIG Configuration Wizards ▪ Monitoring Dashboard

Note: The roadmap is subject to changes

出典: ForgeRock OpenAM Roadmap <https://wikis.forgerock.org/confluence/display/openam/OpenAM+Roadmap>

実装があるだけでは広がらない

	for Consumer	for Enterprise
Business Use Cases, Applications		
Integration Patterns, Architecture		
Implementations		

エンブラでもマルチデバイス・BaaS活用が進む



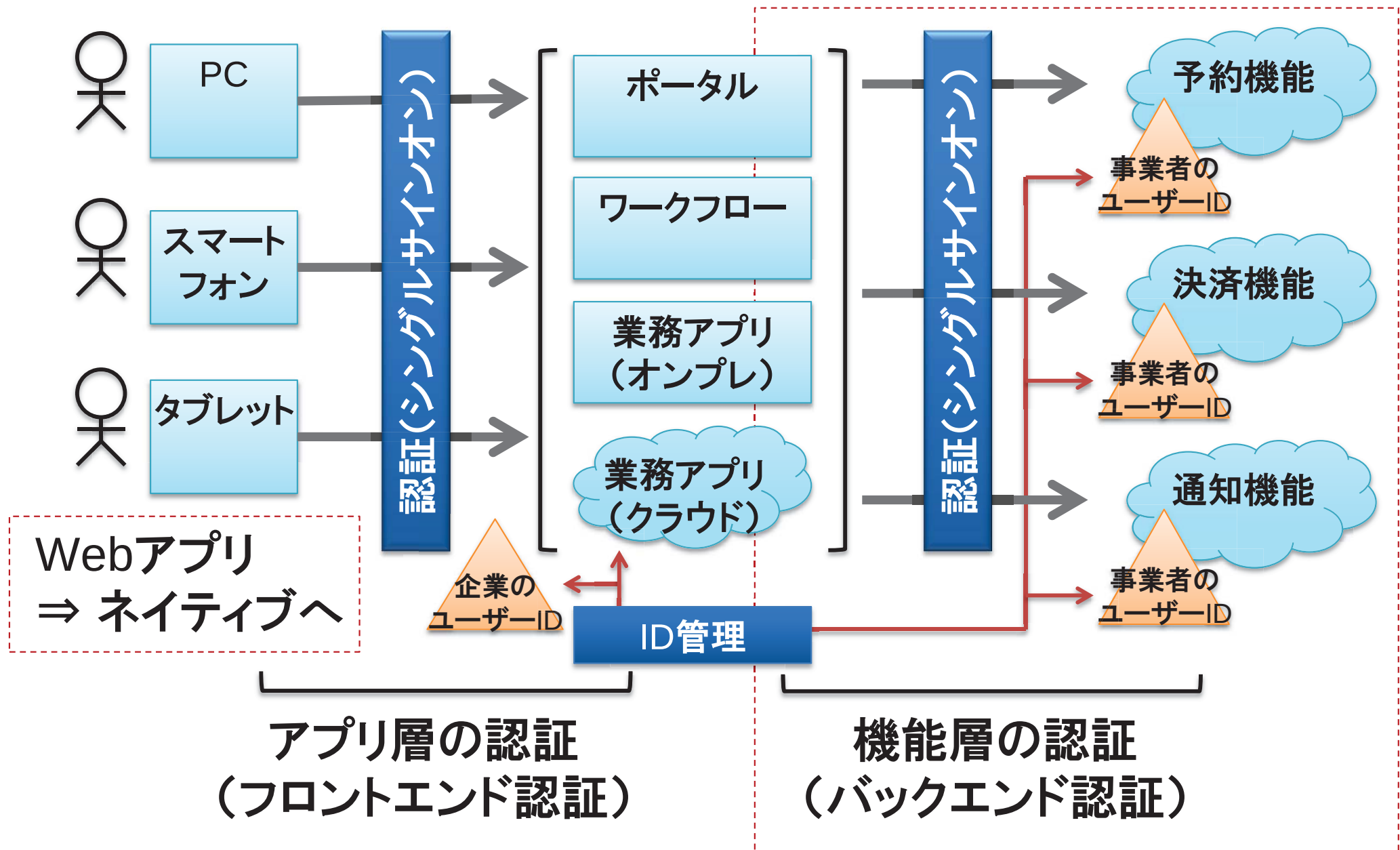
内部・外部境界型セキュリティ（ファイアウォール、etc）

ID統合・認証統合・ネットワークゾーニング
（ディレクトリ、ID管理、シングルサインオン）

クラウド利用時の認証・アクセス管理
（認証連携、多要素認証、デバイス認証、
リスクベース）

アプリ層・機能層の2層
での認証・アクセス管理
（属性連携、認可管理）

アプリケーションのアーキテクチャが変わる



アプリケーションのアーキテクチャが変わる

機能層の認証のための技術への対応が必要

- OAuth2.0, OpenID Connect, JIT Provisioning, SCIM, ...

アプリ層・機能層の透過的認証、アクセス権限の統制のための技術への対応が必要

- ... (これから何が来るか?)



**これらの新技術に追従できる認証基盤の実現が
エンタープライズでも求められる。**

(フロントエンド認証)

(バックエンド認証)

エンブラ系で使える認証基盤の実現を目指して

ユーザーIDの作成

あらかじめプロビジョニングするか？
使い始めるときにプロビジョニングするか？

ユーザーIDの削除

異動・退職などに合わせて適切にユーザーIDを無効化・削除する。

企業としてAPI利用認可

個人の判断で許可をさせるのではなく、
企業として許可を与える。

適切な認可の取り消し

異動・退職などに合わせて適切にAPI利用を取り消す。

ロギング

クラウドで提供される API へのアクセスを
どう記録するか？ 監査するか？

ThemiStructでの対応を進めています

テ ミ ス ト ラ ク ト

ThemiStruct-WAM (OpenAM)

&

ThemiStruct-IDM (OpenIDM)

&

Mule ESB



マルチデバイス・クラウド(BaaS)活用時代の
認証基盤を実現します。

そして

OpenIDファウンデーション・ジャパン
エンタープライズ・アイデンティティ
・ワーキンググループ

での活動を通じて、
OpenID Connectの普及・発展に貢献
していきます。

ご清聴ありがとうございました

【お問合せ先】

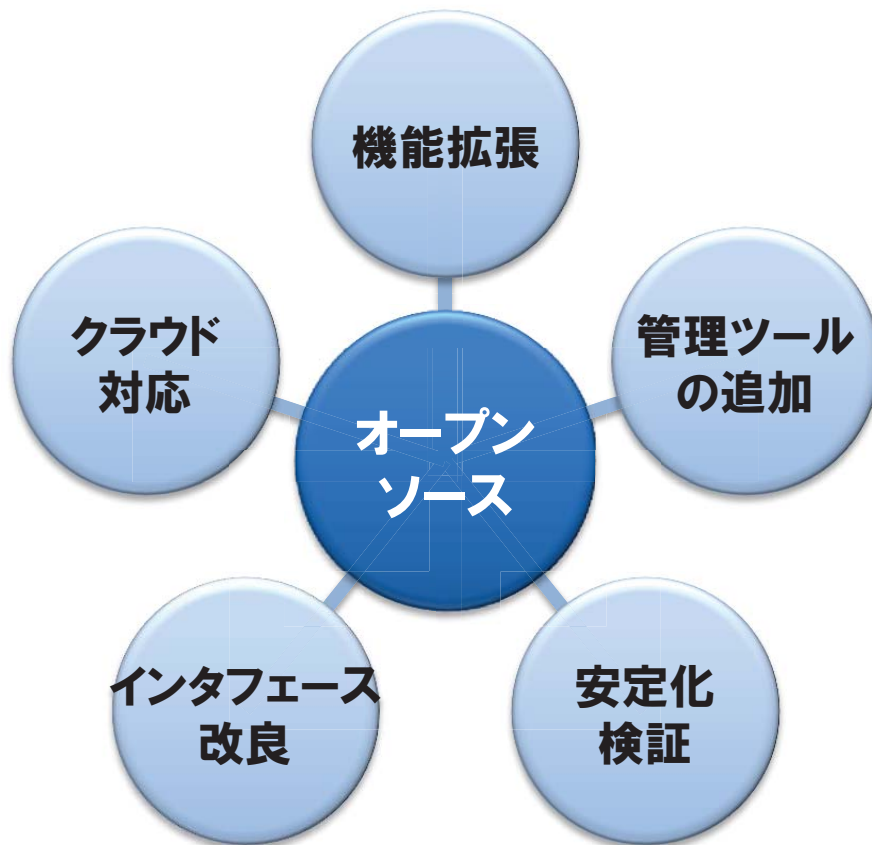
株式会社オージス総研
ソリューション営業部

TEL 03-6712-1201

E-mail info@ogis-ri.co.jp

ThemiStruct ラインナップ

テ ミ ス ト ラ ク ト



- **ThemiStruct-WAM** (OpenAM)
 - シングルサインオン認証基盤ソリューション
- **ThemiStruct-IDM** (OpenIDM)
 - ID管理ソリューション
- **ThemiStruct-CM** EJBCA
PKI BY PRIMEKEY
 - 電子証明書発行・管理ソリューション
- **ThemiStruct-OTP**
 - ワンタイムパスワードソリューション
- **ThemiStruct-WorkFlow**
 - 申請承認ワークフローソリューション
- **ThemiStruct-MONITOR** **ZABBIX**
 - システム監視ソリューション
- **ThemiStruct for Office365**
 - Microsoft Office365認証強化ソリューション

ThemiStruct ラインナップ

テ ミ ス ト ラ ク ト

- オージス総研、IT基盤ソリューション「ThemiStruct(R) (テミストラクト)」を大幅リニューアル (2014年1月28日)

http://www.ogis-ri.co.jp/news/1212304_6734.html

実績のある
オープンソース
ソフトウェア



独自の機能拡張
や管理ツールの
追加



1,000項目以上の
徹底的なテストや
検証などを実施

継続的に実行可能な開発・テストプロセスを整備



お客様に安心してお使い
いただけるソフトウェアと
サポートをご提供



開発コミュニティへ
バグフィックス等の成果を
フィードバック

プロダクト		コアOSS	概要
認証ソリューション	シングルサインオン認証基盤ソリューション ThemiStruct-WAM テミストラクト ワム	OpenAM	Webアプリケーションの統合認証 - 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 - クラウドサービスへのシングルサインオンにも対応
	ID管理ソリューション ThemiStruct-IDM テミストラクト アイディーエム	OpenIDM	アカウント情報を一元管理するID管理 クラウドサービスへのプロビジョニングにも対応
	電子証明書発行・管理ソリューション ThemiStruct-CM テミストラクト シーエム		電子証明書を利用したプライベート端末認証 - 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 - スマートフォンやタブレットなど外部からアクセスする端末の増加に対応可能
	ワンタイムパスワードソリューション ThemiStruct-OTP テミストラクト オーティーピー	Google Authenticator	端末IDから生成するワンタイムパスワードを発行 スマートフォンやタブレットなどを利用したソフトウェアトークン方式なので、専用ハードウェア方式と比較して低コストかつ容易な維持管理が可能
申請承認ワークフローソリューション ThemiStruct-WorkFlow テミストラクト ワークフロー		jBPM	必要かつ十分な機能を備えたワークフロー 申請書(フォーム)と経路(フロー)が担当で自由にデザインできるエンジンを標準装備
システム監視ソリューション ThemiStruct-MONITOR テミストラクト モニター			システム監視 - サーバや仮想基盤における稼働(死活、プロセス、サービスログなど)やパフォーマンスの監視が可能 - リアルタイムの統計や履歴データへのアクセスが可能
Microsoft Office365認証強化ソリューション ThemiStruct for Office365 テミストラクト フォー オフィス365		—	Microsoft Office365認証強化 ThemiStruct-WAMおよびCMを活用し、Office365のセキュリティ(認証機能)を強化するための多要素認証を低コストで実現

ThemiStruct ラインナップ

テ ミ ス ト ラ ク ト

ThemiStruct で提供する3つのサービス

テ ミ ス ト ラ ク ト

テクニカルサポート サービス

- 利用方法等の問合せに回答
- 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
- PoC、技術検証の支援
- 自社で実施する開発、構築の技術支援

SIサービス

- お客様の要求に応じたシステムの実現を責任を持ってお引受け

当社サービスの活用事例

顧客(業種)	提供サービス	ユーザー数	実施内容	プロダクト
インフラ	SIサービス	約20,000	・グループ認証基盤構築 (商用製品からオープンソースへの移行)	WAM
インフラ	SIサービス	数万	・取引先向け電子証明書発行	CM
インフラ	SIサービス	数万	・顧客向けポータルID管理	IDM/WAM
文教	SIサービス	約30,000	・教員・学生向けWeb-SSO基盤構築	WAM
製造	SIサービス	約2,000	・EDI向けユーザー認証システム構築	WAM/CM
製造	SIサービス	約20,000	・B2Bシステム用Web-SSO/ID管理 ・認証基盤の構築	WAM/IDM
製造	SIサービス	約17,000	・全社統合ID基盤の構築 (既存のID管理システムの連携部分をThemiStruct-IDMでリプレイス)	IDM
インフラ	SIサービス	約5,000	・グループ共用Web-SSO/証明書発行 ・認証基盤の構築	WAM/CM
文教	SIサービス	約16,000	・教員・学生向けシステム向け ・統合ID管理基盤の構築 ・サーバ、NW機器監視基盤の構築	IDM/MONITOR
金融	SIサービス	約20,000	・基幹業務システム再構築に伴う、グループ共通認証基盤の構築	IDM/WAM /WorkFlow
製造	SIサービス	約200	・B2Bシステム向け電子証明書発行基盤の構築	CM
金融	SIサービス	約5,000	・電子証明書発行基盤の構築	CM
インフラ	SIサービス	約8,000	・BPO進捗管理システムとして新設 ・社内電子決裁システムリプレイス ・グループ企業横断決裁フローを実現	WorkFlow
サービス	SIサービス	約1,500	・社内向けID管理システム構築	IDM
製造	SIサービス		・社内SSOリプレイス	WAM
公共	SIサービス	約3,000		CM
サービス	SIサービス	約7,000	・派遣登録者向けポータルシステムのためのSSO基盤構築	WAM
製造	SIサービス	約1,500	・ID管理とSSOの実現。大手商用パッケージを使用していたが、 管理が常駐パートナー依存のため、それを改善。	IDM/WAM
製造	SIサービス	監視約80台	・大手商用パッケージからのリプレイス。監視システム構築。	MONITOR

当社サービスの活用事例

顧客(業種)	提供サービス	ユーザー数	実施内容	プロダクト
流通	SIサービス	約4,000 監視約10台	・MONITORは大手商用パッケージからのリプレース。 ・全部署及びグループ向けの決裁システムのエンジン ・電子決裁システムリプレイス(SAP連携)	MONITOR/WorkFlow
マスコミ	SIサービス		・ポータルへの導入がトリガー(社外からアクセス出来ず) ・大手商用パッケージからのリプレイス	WAM
製造	SIサービス	監視約150台	・大手商用パッケージからのリプレース。監視システム構築。	MONITOR
製造	プロフェッショナルサービス		・ワールドワイドの製造拠点のSSO/ID管理共通基盤の構築にOpenAM、ThemiStruct-IDMを利用 ・企画、検証、導入支援 ・WAM/IDMサポートサービス提供	WAM/IDM
公共	プロフェッショナルサービス		・自治体のシステムのOSS化に伴い、OSSサポートの依頼を受けたOSSサポートサービス提供	OSS全般
製造	プロフェッショナルサービス		・Liferayを使ったB2B2Cポータルシステムの構築における技術支援	Portal
製造	プロフェッショナルサービス		・Liferay(ポータル)、OpenAM(シングルサインオン)の導入・設定支援サポートサービス提供	Portal/WAM
製造	プロフェッショナルサービス		・OpenAMの導入設定支援	WAM
流通	プロフェッショナルサービス		・ESBを利用した認証システム連携機能開発の技術支援	WAM
製造	プロフェッショナルサービス		・グループ共用のID管理システムの企画検討支援	IDM
インフラ	プロフェッショナルサービス		・病院システム用の認証システムとしてOpenAMを採用 ・システムの導入設定技術支援	WAM
製造	プロフェッショナルサービス		・将来3,000台規模の監視を行なう為のサーバ構築設計支援	MONITOR