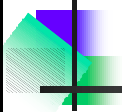




XML Consortium

WebSAM SECUREMASTER ActiveGlobe WebOTX



2005年9月13日
日本電気株式会社

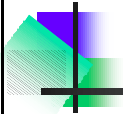
© NEC Corporation 2005



アジェンダ

- 統合認証基盤
WebSAM SECUREMASTERについて
- サービス実行基盤
ActiveGlobe WebOTXについて
- まとめ
NECの今後の取り組みについて

XML Consortium



統合認証基盤

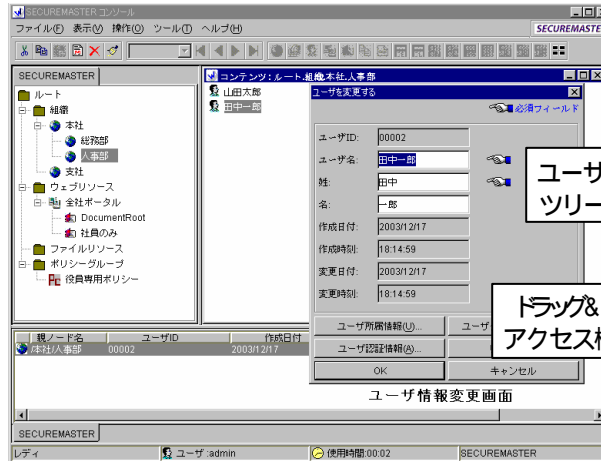


WebSAM SECUREMASTER

- Webサーバセキュリティ運用管理製品
 - セキュリティ管理情報を一元管理
 - ユーザ情報
 - 複数Webサーバのリソース情報、アクセス制御情報
 - パスワード、証明書といった認証情報
 - 認証・アクセス制御・SSOを実現するモジュールの提供
 - エージェントモジュール形式(リバースProxy型も開発中)
 - 認証機能の一元化、分散化どちらも可能



ユーザ管理操作画面



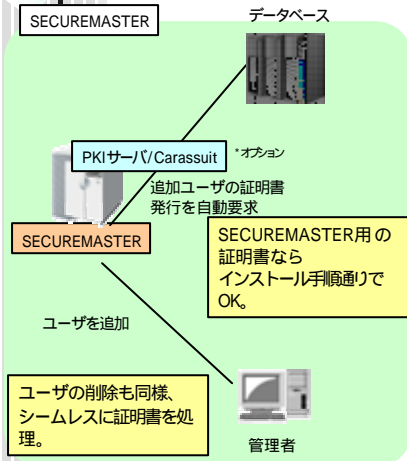
ユーザを組織
ツリーで管理

ドラッグ&ドロップで
アクセス権を設定

ユーザ情報変更画面



PKIサーバとの連携



- ユーザの追加で証明書を自動発行
- SECUREMASTER上で管理しているユーザのユーザ属性をそのまま証明書のフィールドとして申請可能
- 多量のユーザの証明書もバッチコマンドで一括発行可能
- ユーザの削除時も同様に証明書の失効まで自動申請

Carassuit以外のPKIサーバから発行された証明書も認証用途として問題なく利用できます。



バッチ機能

使いやすさではGUIが便利。
しかし、数千人のユーザを入力するのは非現実的

すでに運用済みのマスターデータベースがある
自動的に反映できるようにしたい

人事異動の時期に更新処理が集中。
一括処理できないか



バッチコマンドを用意

リソース、ユーザ、組織情報の追加・削除・更新
パスワード更新、通知など、コマンドで処理可能



イベント通報

同一ユーザIDで連続して認証失敗

短時間の間に、多数のユーザ名を使用した
大量の認証失敗

など

不正アクセスの可能性大



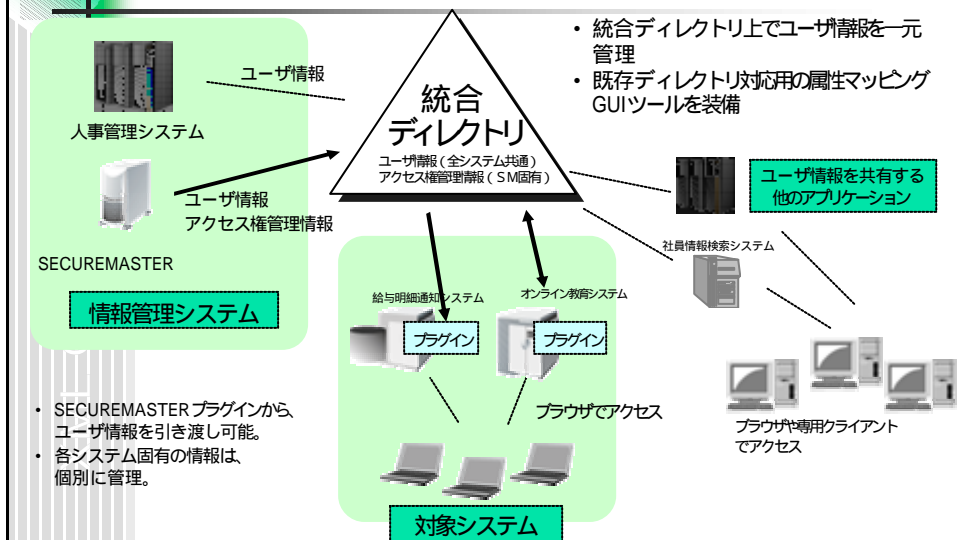
イベントログ・syslogに記録



監視運用製品と連携

- SNMPトラップ
- メール通報
- パトライト

既存のユーザ管理ディレクトリを利用可能

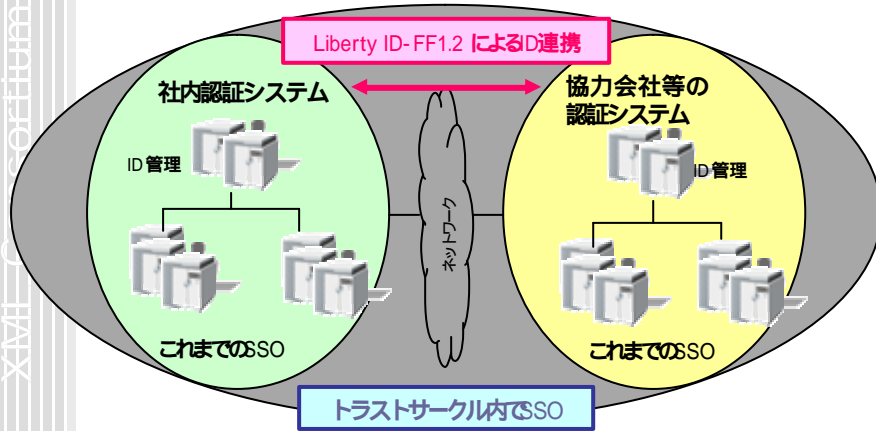


マッピング操作画面紹介



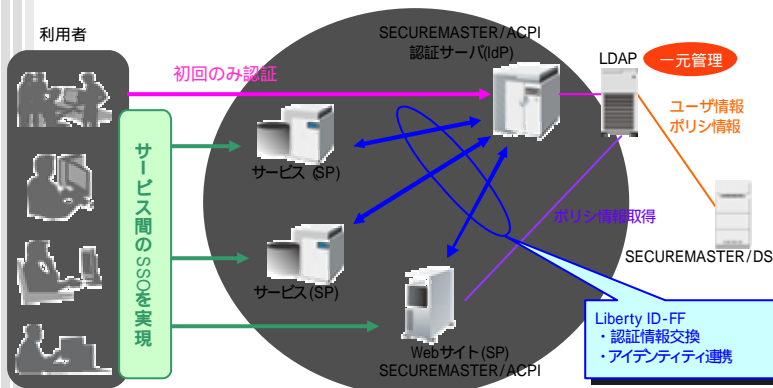
Liberty ID-FF1.2対応

- 分散化したID管理環境においてもSSOを実現し、ID管理の統合が困難な企業間、組織間に対してもシステム統合を簡易に。



Webサービスとの連携が可能に

- SECUREMASTERで認証を行い、各サービス(Webサービス)とのID連携や認証情報の交換をすることで、サービス間のSSOを実現。

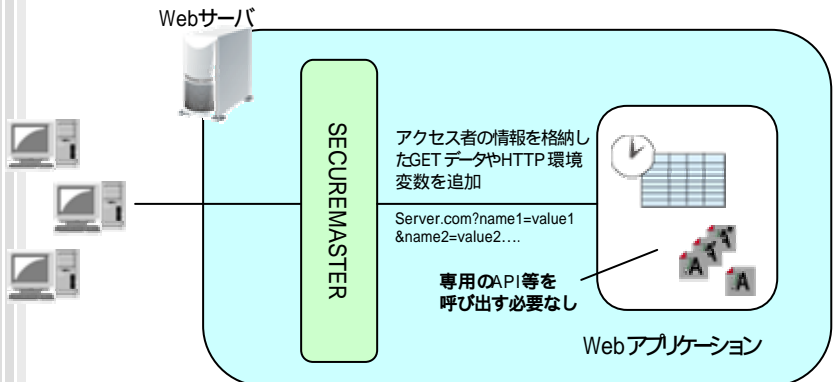




アプリケーションへの属性引渡し

WebアプリケーションがHTTP環境変数や、通常のGETデータを取得するようにアクセス者の属性を取得することができます。

XML Consortium



(参照) 適用事例



導入されているお客様の業種

XML Consortium

金融機関、教育機関、製造業、保険業、運輸業、電力
 と言った幅広い業種のお客様にご利用頂いています。

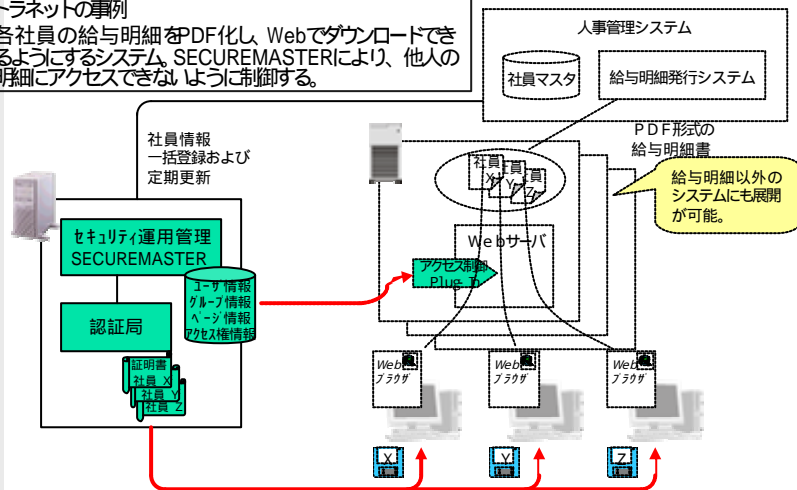
また最近では官公庁、ISP、モバイルキャリアの分野のお客様
 からもお問い合わせを頂いております。



A社殿人事システム

イントラネットの事例

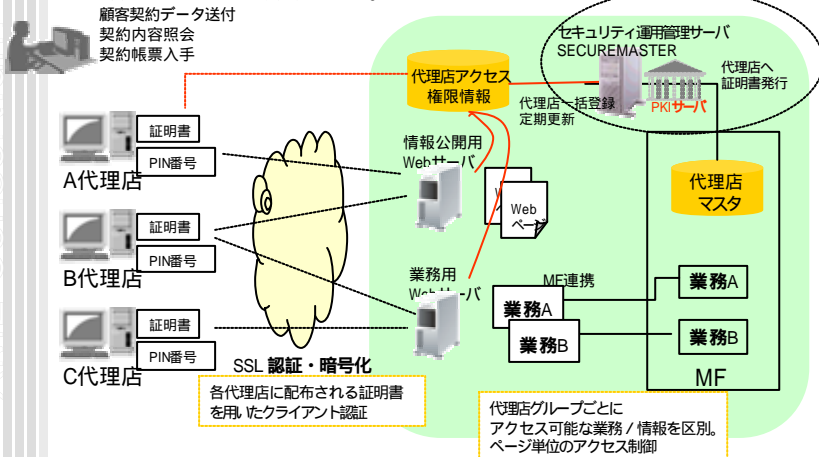
- 各社員の給与明細をPDF化し、Webでダウンロードできるようにするシステム、SECUREMASTERにより、他人の明細にアクセスできないように制御する。



XML Consortium

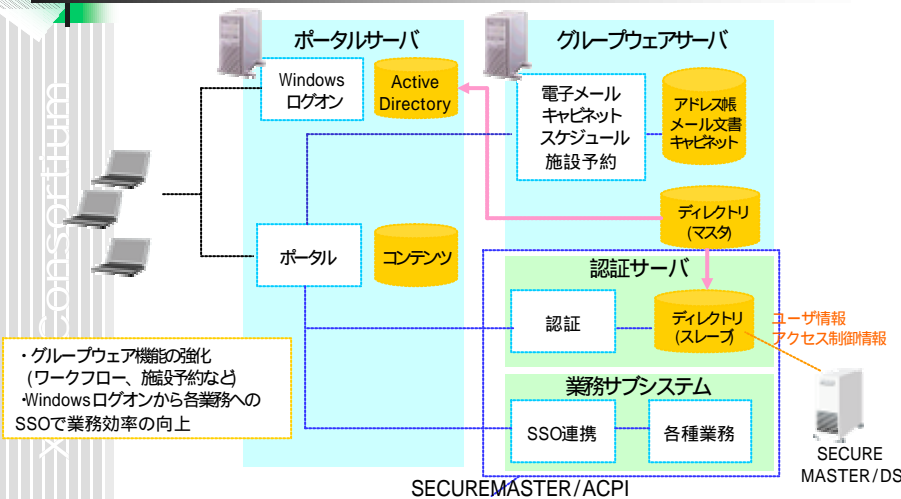
B 損保会社代理店システム

- ・取引先の業務メニュー、情報提供業務のWeb化。
- ・業務の効率化とサービス拡大をはかる。



XML Consortium

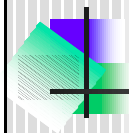
C 銀行様 新業務システム



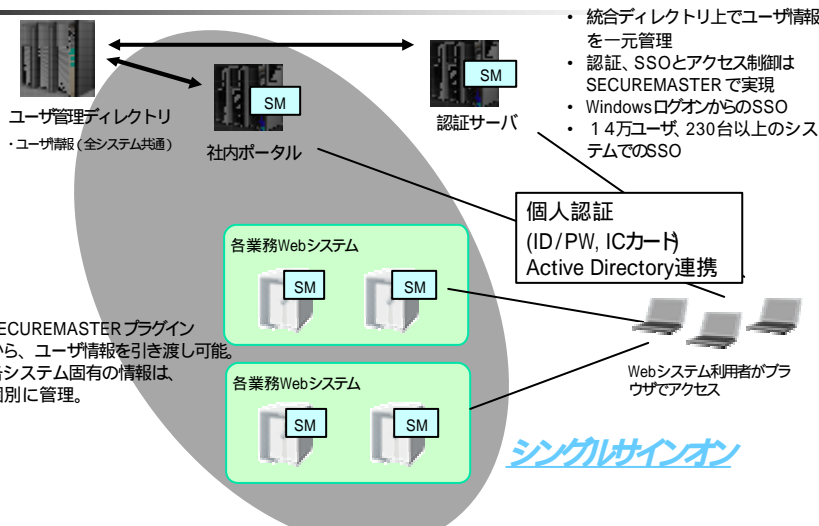
- ・グループウェア機能の強化 (ワークフロー、施設予約など)
- ・Windows ログオンから各業務への SSO で業務効率の向上

XML Consortium

NEC社内認証システム



XML Consortium



- 統合ディレクトリ上でユーザー情報を一元管理
- 認証、SSOとアクセス制御はSECUREMASTERで実現
- WindowsログインからのSSO
- 14万ユーザー、230台以上のシステムでのSSO

- SECUREMASTERプラグインから、ユーザー情報を引き渡し可能。
- 各システム固有の情報は、個別に管理。

シングルサインオン



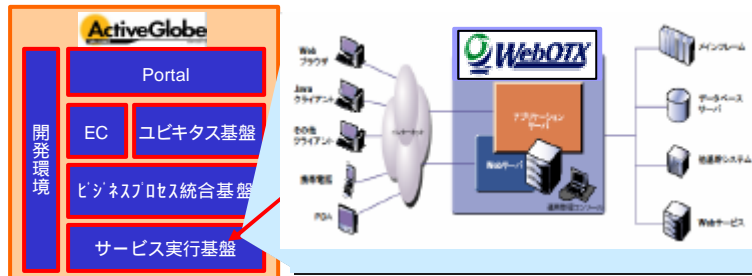
サービス実行基盤



ActiveGlobe WebOTX

XML Consortium

- サービス構築基盤の中核として、最新の標準技術を採用したミッションクリティカルな業務を支えるアプリケーションサーバ



ActiveGlobe WebOTXの特徴

XML Consortium

▶ ビジネスを止めない 高性能、高信頼

24時間365日の無停止運用を実現する堅牢なトランザクション製品。
ハイパフォーマンス、スケーラビリティ、高負荷耐性を持った
高信頼なビジネスロジック実行基盤。

◀ ビジネスを回す 最新のデファクトスタンダード技術

IT開発投資を無駄にしない、将来に渡って保証された
最新オープン技術に基いたコンポーネント設計。

- J2EE1.4準拠
- 最新Webサービス仕様に対応 (SOAP1.2, UDDI3.0, WSDL1.1, WSS 1.0)
- CORBA2.3/3.0(一部準拠)

DOPGやユーザ先で実証された相互接続実績
(CORBA/EJB/Webサービス相互接続)。



▼ コストを下げる 高い生産性

J2EE APを効率よく開発しデバッグできるJava™統合開発環境。
既存資産を有効活用できるEAJ基盤を実装。
(ACOS : VISコネクタ, IBM : MQコネクタ, UNIX : TUXEDOコネクタ)

ActiveGlobe WebOTXのオープン性

? J2EE1.4仕様準拠のアーキテクチャ

? **ビジネスロジック層の新しい基礎サービス**

- ▷ EJB2.1 コンテナ管理によるタイマーサービス
- ▷ WSEE1.1 WebサービスがEnterprise Java Beansに統合



? **サービス層の向上**

- ▷ Servlet 2.4 ELによる可読性と保守性を向上
- ▷ JSTL 1.1 フィルタによるコンポーネント化
- ▷ タグライブラリによるXMLの簡便な記述

? **サーバ運用環境の標準化**

- ▷ JMX 1.2配備方法、監視方法、監視ツール

Point

J2EE1.4では、システムの柔軟性と再利用性を高めるWebサービスの統合、開発生産性を向上させる強化、運用を効率化するサーバ管理環境の標準化が図られています。

Webサービス先進サケ

? **セキュアなサービス間の情報交換**

- ? UDDI3.0電子署名に**主要ベンダー**で初めて対応、XML署名
- ? Web Services Security SAML Token P
- ? Web Services Security Ver1.0



? **柔軟かつ迅速**

- ? ビジネス

? **標準仕様でサービスを定義・公開・発見**

- ? Webサービス基本標準(SOAP1.2/WSDL1.1/UDDI2.0)のサポート

? **高い相互接続性**

- ? Webサービス相互接続性の保証(WS-I Basic Profileに国内初対応)
- ? 導入を容易にするビジネスプロトコル(ebXML、RosettaNet)のサポート

? **携帯電話対応Javaアプリケーション開発効率化**

- ? 携帯JavaからバックエンドWebサービスの呼び出しを容易に実現

? **Webサービス統合&運用管理能力を高めるJ2EE1.4対応**

- ? WSEEによりEJBをシームレスにWebサービス化(国内初対応)



Webサービスセキュリティ対応一覧

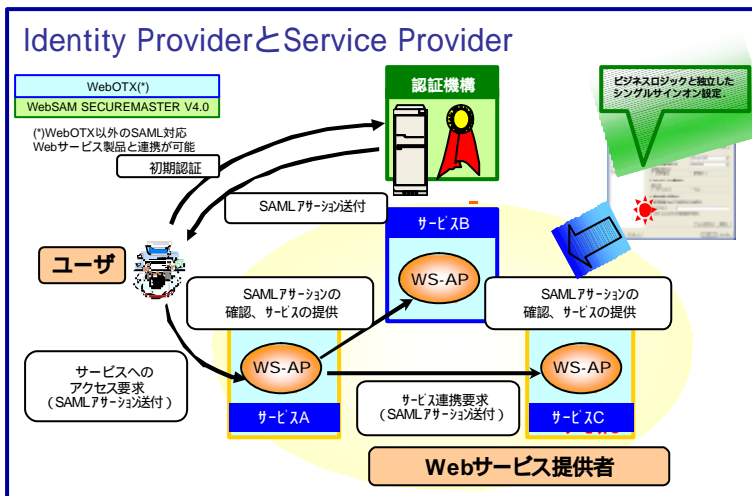
XML Consortium

仕様名称	概要
Web Services Security: SOAP Message Security V1.0	SOAPメッセージへのXML署名、XML暗号の適用方法、認証情報(Token)の利用方法に関する仕様。
Web Services Security: Username Token Profile V1.0	ユーザ名、パスワードを用いた認証情報の利用方法に関する仕様。
Web Services Security: X.509 Token Profile V1.0	X.509証明書を用いた認証情報の利用方法に関する仕様。
Web Services Security: SAML Token Profile	OASIS SAML仕様に準拠したセキュリティトークンの利用方法に関する仕様。



Webサービス間連携モデル

XML Consortium

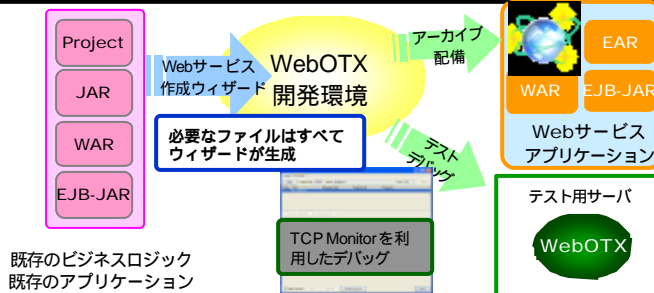




Webサービスの開発

XML Consortium

- ? Developer's Studioが提供するWebサービス作成ウィザード
- ? 既存のビジネスロジックやアプリケーションを簡単にWebサービス化
- ? J2EE 1.4に対応し、ポータビリティの高いWebサービスを開発
- ? Webサービスセキュリティのきめ細かな設定が可能
- ? WebOTX開発環境だけで充実したデバッグ環境が整う
- ? 設定なしですぐデバッグできるテスト用のJ2EEサーバを同封
- ? テスト用サーバのコントロールはすべてDeveloper's Studioに統合



Webサービスセキュリティの開発

XML Consortium

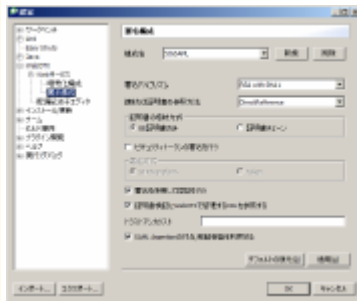
- Step 0 ? 認証機構(SAMLオーソリティ)を準備
 - ? SAMLアサーションを発行するSAMLオーソリティ(WebSAM SECUREMASTER/ACPI)を準備します。
- Step 1 ? キーストア、証明書を作成
 - ? 署名、暗号化のために鍵を含んだキーストアを作成します。
- Step 2 ? 署名構成、暗号化構成の設定
 - ? WebOTX Developer's StudioのWebOTX|Webサービス設定で、署名構成、暗号化構成を設定します。
- Step 3 ? Webサービス作成ウィザード
 - ? WebOTX Developer's StudioのWebサービスウィザードでWebサービスを作成します。Webサービスアプリケーションのセキュリティに対する設定は本ウィザードで行います。
- Step 4 ? CallbackHandlerの実装
 - ? ユーザ名(またはエイリアス)、パスワード、SAMLアサーションを取得するロジックをクライアントサーバと各用途別に生成されたCallbackHandlerの雛形に実装します。



Webサービスセキュリティの開発

XML Consortium

Step 2 署名構成、暗号化構成の設定



暗号化	データアルゴリズム
	鍵暗号化アルゴリズム
署名	鍵または証明書の参照方法
	署名アルゴリズム
	鍵または証明書の参照方法
	証明書格納方式
	セキュリティトークンの署名有無
	署名を使用しての認証有無
	SAML Assertionの付与/検証機能の有無

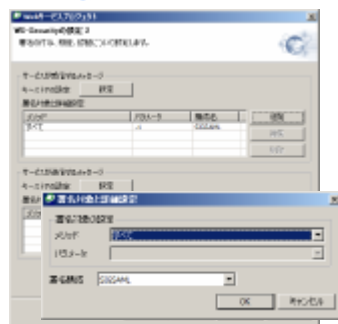
Webサービスの設定は、WebOTX Developer's Studioからウィンドウ「設定」設定ダイアログを開き、WebOTX/Webサービスの下にある署名構成 / 暗号化構成で行ないます。



Webサービスセキュリティの開発

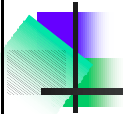
XML Consortium

Step 3 Webサービス作成ウィザード作成



Webサービス設定項目	
Web Services Security	ユーザー名トークンの認証機能
	署名の付与、検証、認証 (キーストア指定 設定参照)
	暗号化 (キーストア指定 設定参照)
	タイムスタンプ付与、検証
	SOAP role(actor)属性

Webサービス作成ウィザードの詳細設定において、Webサービスセキュリティの設定を行います。

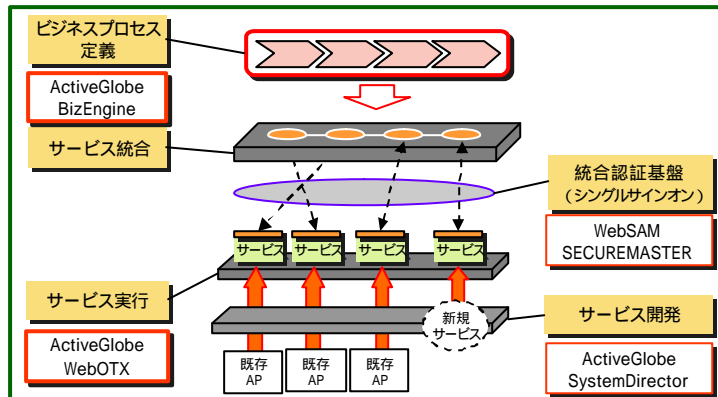


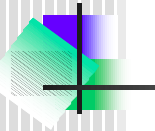
まとめ



NECの今後の取り組み

長年にわたり蓄積したオープンミッションクリティカルシステムの構築ノウハウとWebサービス技術の融合により、高度な生産性と高い品質を兼ね備えSOA対応システムの実現をサポートしていきます。





XML Consortium

Empowered by Innovation

NEC