



## XS40 XMLセキュリティ・ゲートウェイ による認証ゲートウェイの構築

2005年9月13日 XMLコンソーシアムセミナー

東京エレクトロン株式会社  
コンピュータネットワーク事業部 マーケティング グループ  
松永 豊 matsu@kabuki.tel.co.jp

Distributed by



## サービス指向エンタープライズ

? **ビジネス・パートナー連携**

Webサービスによるビジネス連携に  
必要なセキュリティ、認証、データ検証、  
データ変換を提供します。

? **メッセージ・ハブ(ESB)**

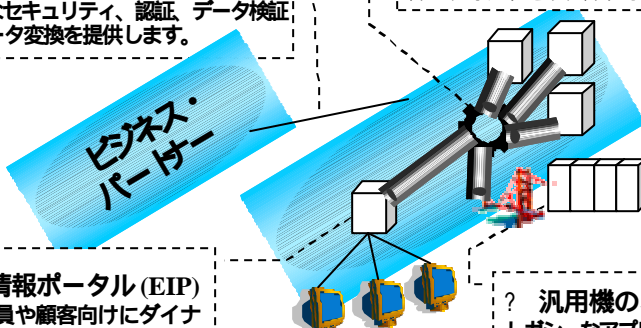
アプリケーション統合にはデータ変換、  
ルーティングをリアルタイムで行います。

? **情報ポータル(EIP)**

従業員や顧客向けにダイナ  
ミックに的確な情報提供を  
行うには、膨大なデータ処  
理が必要です。

? **汎用機のオープン化**

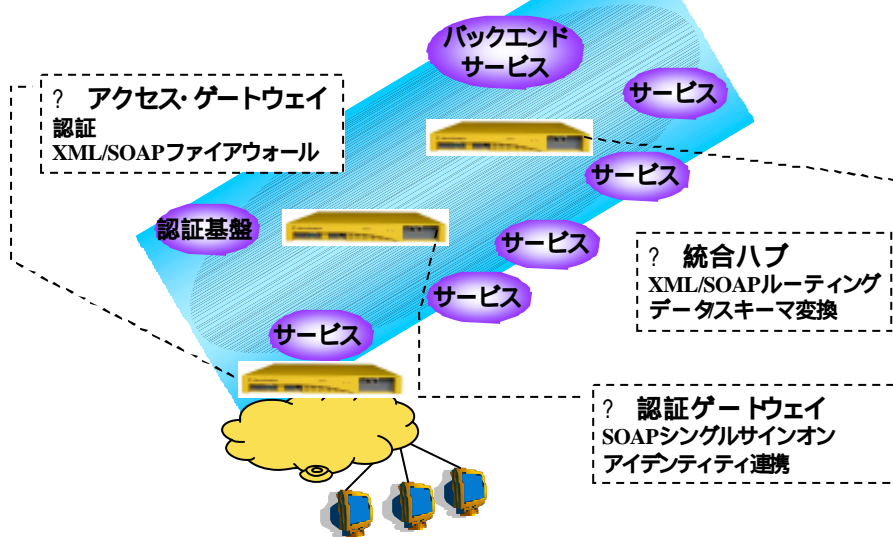
レガシーなアプリケーションをサ  
ービス化して新たな活用を行う  
為に、データとメッセージ形式の  
変換を行います。



Distributed by



# サービス基盤でのAON



Distributed by



3

# DataPowerの製品

## XA35 XMLアクセラレータ



- XMLアプリケーション性能を10倍以上改善 (実測最大100倍)
- XML処理の集約で開発コストを大幅に削減

## XS40 XMLセキュリティゲートウェイ



- Webサービスに必要なセキュリティを超高速に提供
- XMLセキュリティ機能を全てビルトインで提供
- 柔軟な設計 新規格、ポリシー、アプリケーションを常に反映

## XI50 XML統合アプライアンス



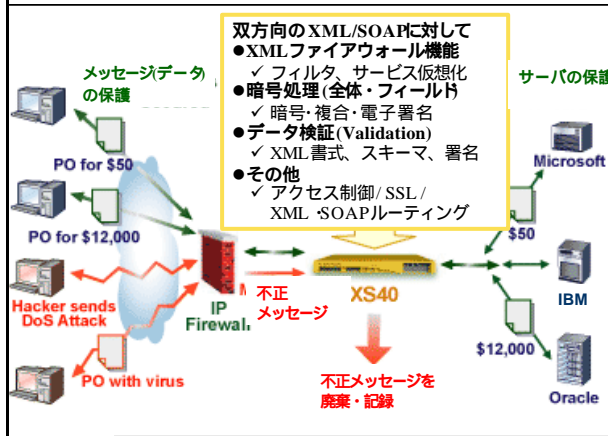
- XML以外のトラフィックに対応
- 汎用機のオープン化
- データ指向プログラミング (DOP)
- メッセージレベルのセキュリティ

Distributed by



4

# XS40 XMLセキュリティ・ゲートウェイ



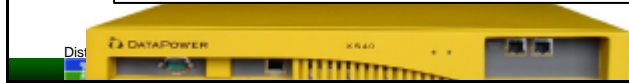
## □特許取得XMLエンジン

- XMLアクセラレータ+暗号処理とセキュリティ

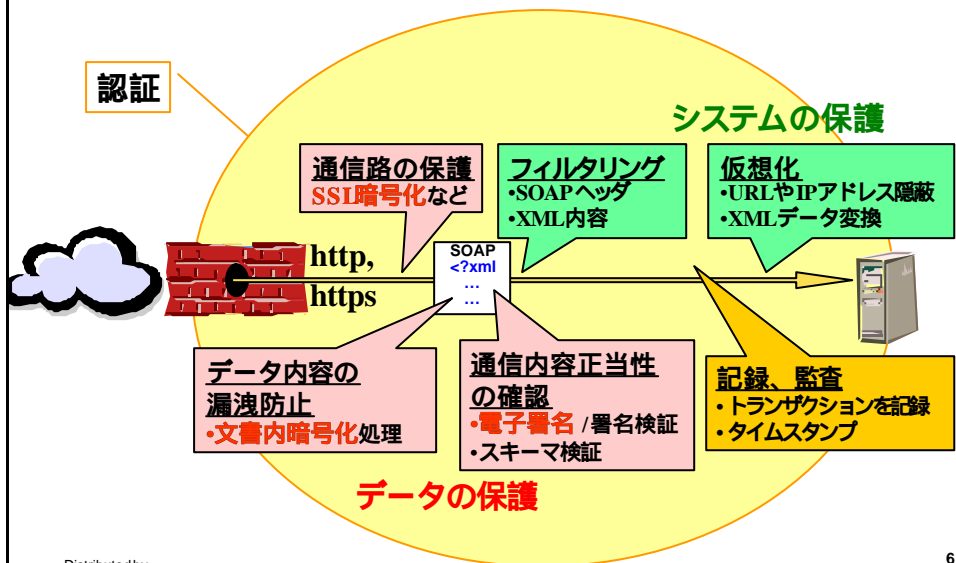
## □メリット

- XMLセキュリティ機能をゲートウェイで一括提供
- セキュリティ機能と性能を両立
- 常に最新のWebサービス・セキュリティ規格を提供
- セキュリティの為の開発工数を削減

**特長： 性能 一元管理 迅速・容易 柔軟**

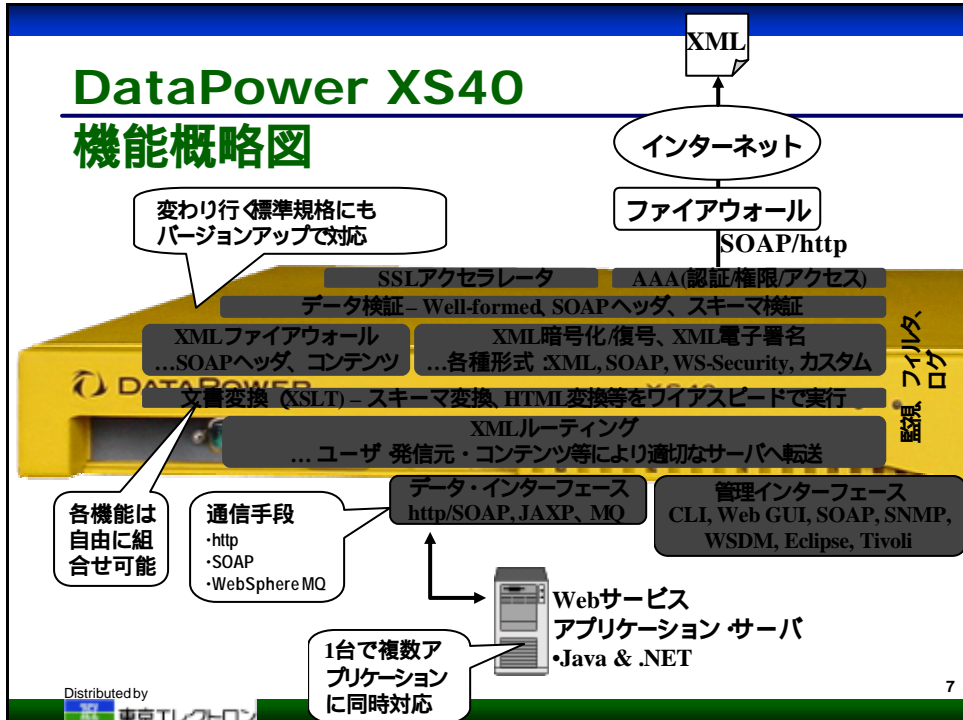


# データ保護とシステムの保護



# DataPower XS40

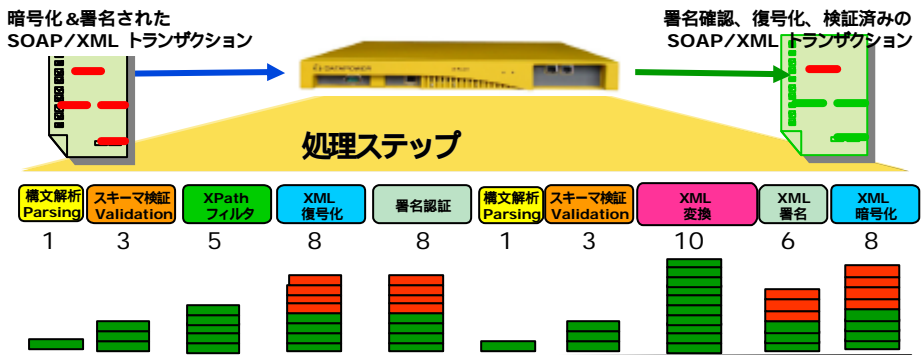
## 機能概略図



Distributed by



# XS40 性能 : XMLセキュリティを現実に



**XML WebサービスのセキュリティではXML処理能力がカギになる**

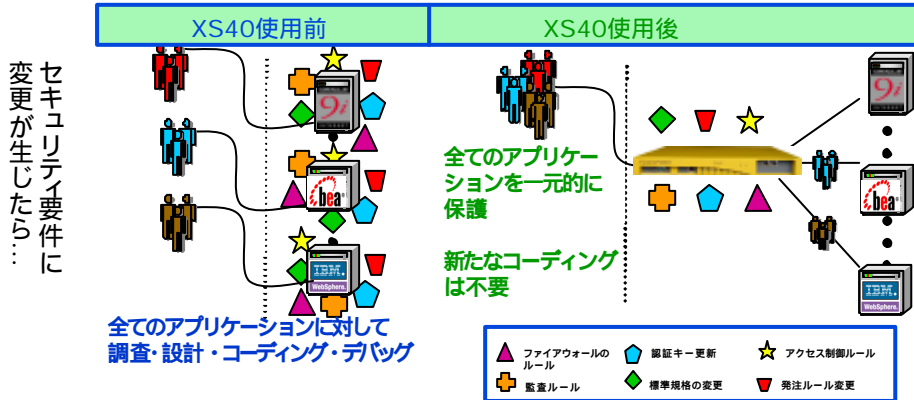
- XG3 はセキュアなXML処理を念頭において設計
- SOAP/XMLレベルでの脆弱性を回避 (XDoS=XMLサービス拒否攻撃)
- セキュリティ実装における妥協に訣別 (セキュリティ設定⇔性能)

Distributed by



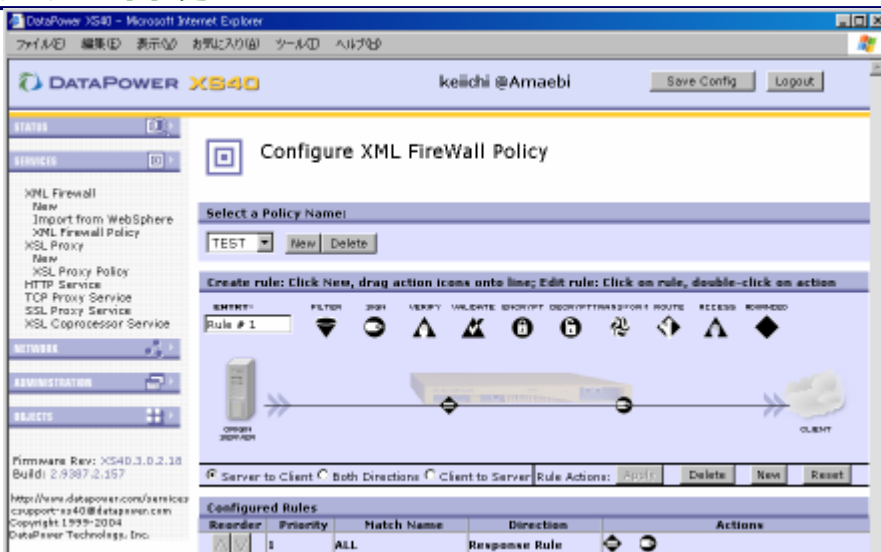
# 一元管理 :XS40 がシステムを変える

- XMLネットワークによるセキュリティの集約
  - 多数のアプリケーションを一元的に保護
  - コストと工数を劇的に削減
  - 新しいビジネスを圧倒的なパフォーマンスで実現



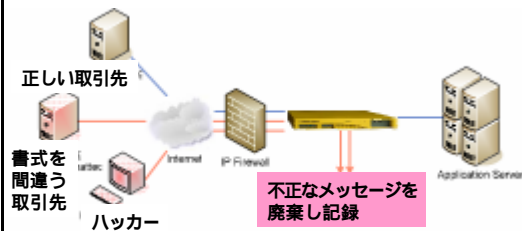
Distributed by

# 迅速・容易 : XS40 Web GUI



Distributed by

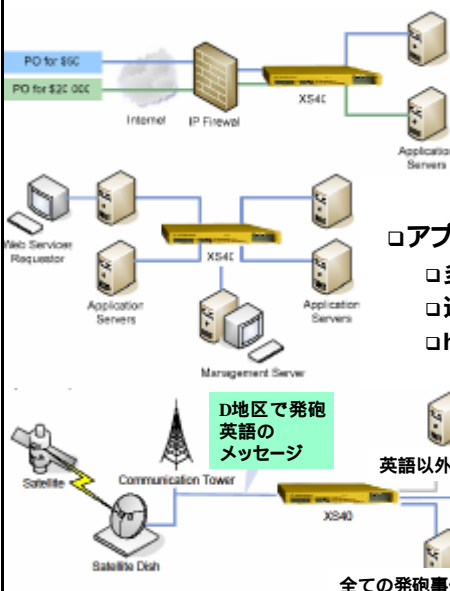
## XS40用途1 :XMLファイアウォール



- ファイアウォールを抜けてくる SOAP メッセージを検査
- XMLを悪用する不正通信や書式の間違いによる異常動作を回避
- バイナリ添付、サイズ、受信頻度なども制限可能
- メリット:DataPowerのノウハウ活用、開発工数削減、処理性能、一元管理

XML整形形式チェック	異常なメッセージを除外しサーバのメモリ領域障害やシステム侵入、DoS攻撃を回避
XMLスキーマ検証	処理性能を気にすることなく必要なスキーマのみを通し、不要なメッセージの侵入や処理エラーを回避
バッファオーバーフロー検査	データの検査によりバッファオーバーフローを防止
WSDLメソッド・フィルタ	メソッド毎の許可設定によりサービスへのアクセスを制限
XMLフィルタ	Xpathでの指定により特定部分のデータによるフィルタ
サービス仮想化	URLやエンドポイントを隠蔽して内部構造の露出を回避
メッセージモニター	メッセージ頻度などを監視して攻撃防御とサービス・レベルの確保

## XS40用途2 :XML/SOAPルーティング



- 会員制商取引のゲートウェイ
- 仮想化により内部構成を隠蔽
- 注文額や会員属性などにより適切なサーバへ転送 (サービス・レベル確保)
- トランザクションのログ
- 返信メッセージを適切な宛先へ転送

### □ アプリケーション・ルーティング/ブローカー

- 多種のメッセージを変換し適切なサーバへ転送
- 運用一元化、コスト削減、高速処理に貢献
- http, https, SOAP, MQ, JMSに対応

### □ コンテンツに依存したメッセージ配信

- イベント配信、市場取引情報、信用情報照会など

全ての発砲事件を担当

# XS40用途3 :XMLデータ保護

## ■部分暗号化



- 販売店は受注時に暗号化されたカード番号を復号
- 中間の顧客管理サーバでは必要な情報だけ参照し、機密データの漏洩を防止
- 返信時には暗号化処理をゲートウェイで実行

## ■パートナー間のデータ保護



- 顧客は注文書に署名し、口座情報を銀行の鍵で暗号化
- 銀行が口座を確認し、署名
- 販売店が両者の署名を確認し、受注成立

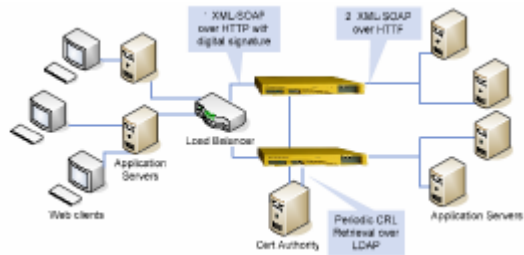
Distributed by

13

# XS40用途4 :Webサービスアクセス制御



- 外部Webサービスのゲートウェイ
  - 社内アプリを顧客やパートナーに公開する
  - SSOサーバ(ClearTrust等)への認証をゲートウェイで行う



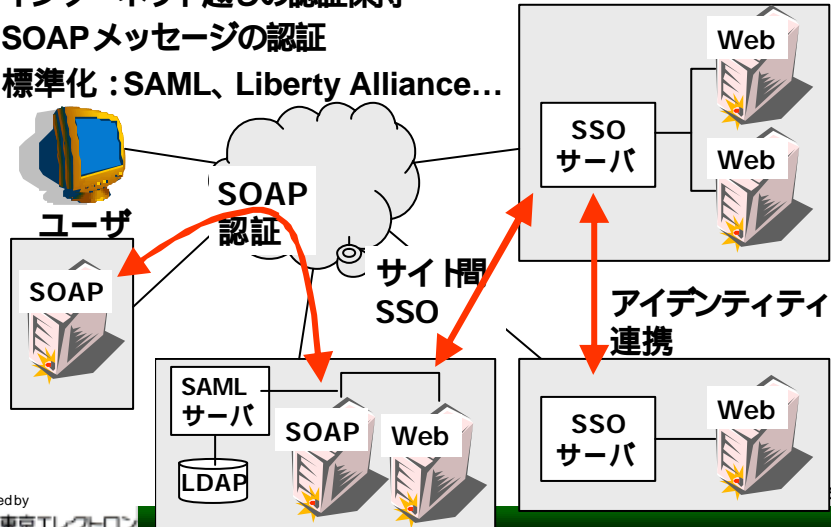
- 社内Webサービスのハブ
  - 機密性の高いサービスを保護
  - クライアントからのリクエストは電子署名の検証が成功しない限り通過させない
- どちらの場合も認証ログをゲートウェイにおいて記録可能

Distributed by

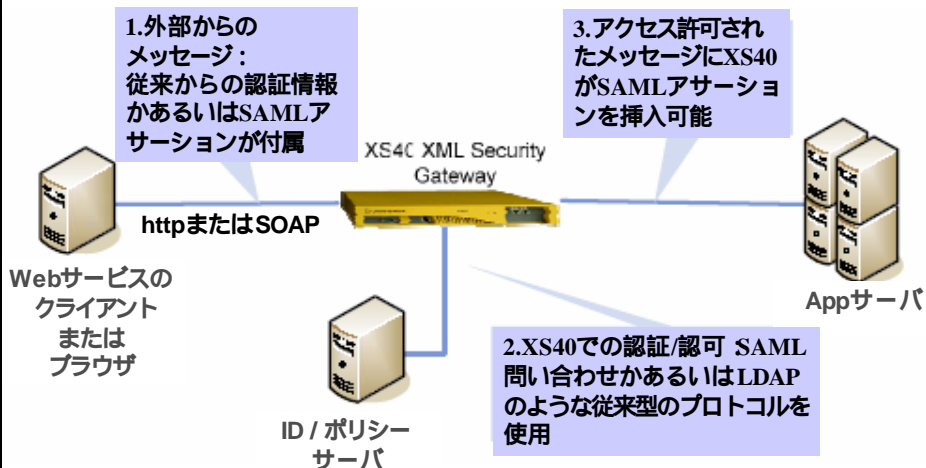
14

# 認証: セキュリティの中核

- Webサービスによる認証のチャレンジ
  - インターネット越しの認証保持
  - SOAPメッセージの認証
  - 標準化 : SAML、Liberty Alliance...



# ゲートウェイでの認証処理





# ゲートウェイでのSAML利用例

1. Webサービスのアクセス制御
  - XS40は受け取ったXML/SOAPメッセージからID情報を入手、認証
2. SAML以外のアクセス制御をSAMLに変換する
  - XS40がメッセージからID情報を入手、認証サーバに問い合わせ
  - SAMLの認証アサーションをメッセージに挿入し、転送
3. 属性を利用した詳細な認証(役割や職種、権限、位置情報等)
  - XS40がSAMLの属性問い合わせを認証サーバに対して発行
  - 属性情報と定義済みのルールを照合しアクセスを許可を判断
4. Webシングルサインオン
  - XS40はSAMLブラウザ・アーティファクトを処理するプロキシとして動作
  - WebサービスとWebアプリケーションの認証をXS40で一元化
5. アイデンティティ連携
  - XS40を使って異なるドメインの企業同士を連携

# XS40 AAA機能の設定

- AAA: 認証、権限認可、アクセス制御

Configure XML FireWall Policy

Select a Policy Name:  
demo [New] [Delete] [View Log] [View Object Status]

Create rule: Click New, drag action icons onto line. Edit rule: Click on rule, double-click on action

Entry: Rule # 1 [Filter] [Sign] [Verify] [Validate] [Encrypt] [Decrypt] [Transform] [Route] [AAA] [Advanced]

SERVER <--- [Rule # 1] ---> CLIENT

Server to Client  Both Directions  Client to Server  Error Rule Actions: [Apply] [Delete] [New] [Reset]

Reorder	Priority	Match Name	Direction	Actions
[Up] [Down]	1	ALL	Request Rule	[Rule # 1] [AAA]



Configure an Access Control Policy

Help

AAA Policy Name: demo1

Define how to extract a user's identity from an incoming request.

httpヘッダ

WS-Securityヘッダ内の  
トークン

SAMLアサーション

Identification methods

SAMLアーティファクト

クッキー

- HTTP's Authentication header
  - UserName element from WS-Security header
  - BinarySecurityToken element from WS-Security header
  - WS-SecureConversation Identifier
  - WS-Trust Base or Supporting Token
  - Kerberos ticket from WS-Security header
  - Subject DN from SSL client certificate
  - Name from SAML attribute assertion
  - Name from SAML authentication assertion
  - SAML artifact
  - Client IP address
  - Subject DN from certificate in the message's signature
  - Token extracted from the message
  - Token extracted as Cookie value
  - Custom template
- \*

Configure an Access Control Policy

Help

Define how to authenticate the user.

- Method
- Use DataPower AAA Info file
  - Bind to specified LDAP server
  - Contact Tivoli Access Manager
  - Contact Netegrity SiteMinder
  - Contact Oblix server
  - Contact ClearTrust server
  - Use specified RADIUS server
  - Validate the client SSL certificate
  - Accept a SAML assertion with a valid signature
  - Retrieve SAML assertions corresponding to a SAML browser artifact
  - Contact a SAML server for a SAML Authentication statement
  - Use an established WS-SecureConversation security context
  - Pass identity token to the authorize step
  - Validate a Kerberos ticket for the correct server principal
  - Custom template

SAMLアサーション (署名確認)

SAMLブラウザ・  
アーティファクト



## Configure an Access Control Policy

Hel

Define how to authorize a request.

Method

認証に使った  
SAMLトークンの属性

SAML属性  
問い合わせ

- Allow any authenticated client
- Always allow
- Contact Tivoli Access Manager
- Contact Netegrity SiteMinder
- Contact Oblix server
- Contact ClearTrust server
- Custom template
- Check for membership in an LDAP group
- Generate a SAML authorization query
- Generate a SAML attribute query
- Use SAML attributes from authentication
- Use Datapower AAA Info file

Back

Next

Advanced

Cancel

21

## XS40における認証ログ

- 成功 失敗それぞれのログレベルやカウントを設定
- エントリーに電子署名可能、各種通知方法をサポート



System Log for Transaction 5463

target:   filter:

time	category	level	trans#	client	message
Thu Jul 14 2005					
15:25:26	multistep	error	5463	192.168.0.199	xmlfirewall (TestA3): Event-Code(0xd30003) - Rejected by filter; SOAP fault sent
15:25:26	multistep	error	5463	192.168.0.199	xmlfirewall (TestA3): request TestA3_1_Rule_0 #1 aaa: 'INPUT TestA3_3 stored in OUTPUT' failed; Rejected by policy.
15:25:26	aaa	warn	5463	192.168.0.199	xmlfirewall (TestA3): Policy(TestA3_3): Message rejected
15:25:26	aaa	warn	5463	192.168.0.199	xmlfirewall (TestA3): Policy(TestA3_3): anyauthenticated authorization failed with credential "" for resource 'POST'
15:25:26	aaa	warn	5463	192.168.0.199	xmlfirewall (TestA3): Policy(TestA3_3): ldap authentication failed with (wssec-username, username='userAAA', password='*****')

# DataPower導入事例

通信	Bell Canada、仏通信会社、T-mobile	金融 (銀行・投資・ 保険・証券)	カナディアン・インペリアル銀行 (CIBC)
旅行	Cendant		JPMorgan Chase Bank
製薬	ファイザー(Pfizer)		Principal Financial Group
製造・国防	BAE		RBC
	Northrop Grumman		UBS
SI・コンサルティング	ブーズ・アレン・ハミルトン (Booz Allen Hamilton)		Wachovia
政府機関	マサチューセッツ州政府 収税部門		AIG
	米国退役軍人省		GFKL (独リース会社)
その他サービス	Leader Technologies (電話会議サービス)		ハートフォード(The Hartford)
	Hemscott (英株式情報サイト)		ADP (Automatic Data Processing, Inc.)
		電子商取引	Navio
			RouteOne (自動車ローン)
			Vesta

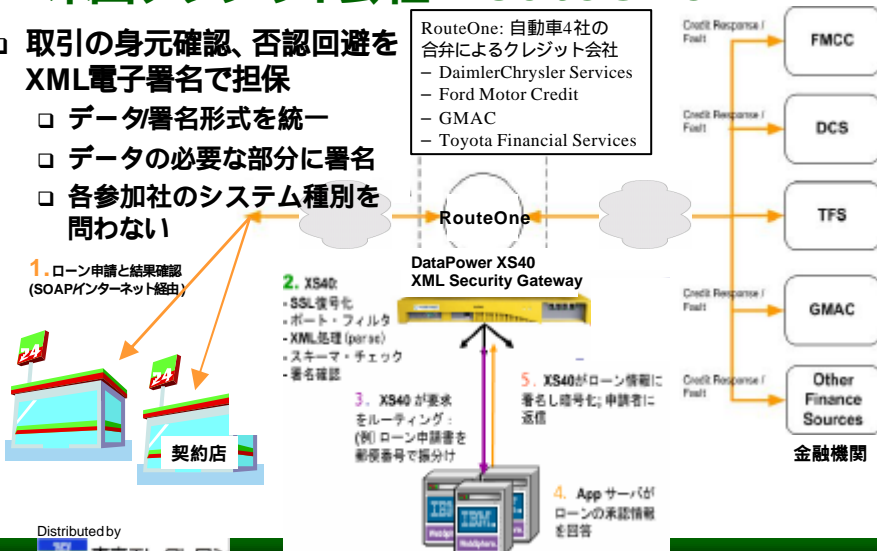
Distributed by

# XS40 XML電子署名事例： 米国クレジット会社 RouteOne

## 取引の身元確認、否認回避をXML電子署名で担保

- データ署名形式を統一
- データの必要な部分に署名
- 各参加社のシステム種別を問わない

RouteOne: 自動車4社の合併によるクレジット会社  
 - DaimlerChrysler Services  
 - Ford Motor Credit  
 - GMAC  
 - Toyota Financial Services

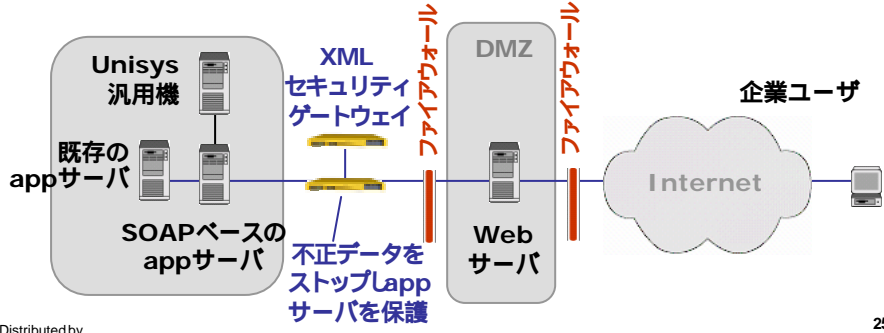


Distributed by

# XMLファイアウォール事例

## マサチューセッツ州政府 税金システム

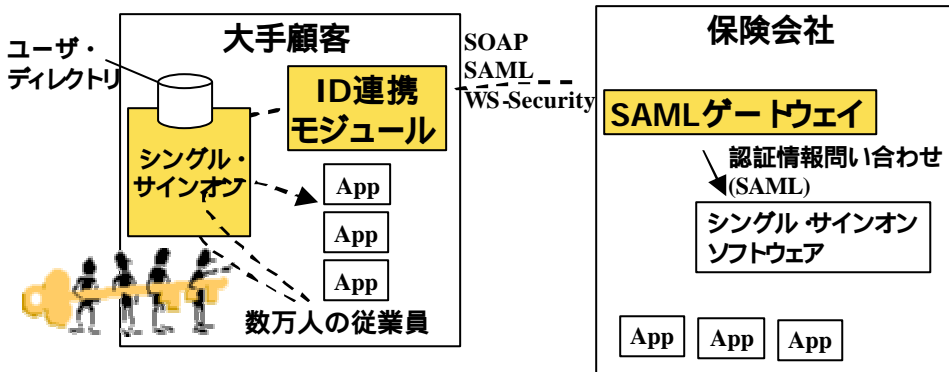
- XML+SOAPを使ったオンライン収受システム
  - 20億ドルの赤字を解消するためにオンライン化
  - 既存の汎用機システムをインターネットに接続
  - 稼動中 週間10億円のトランザクション
- ネットワーク管理者がXML/SOAPの内容を検査する必要があった



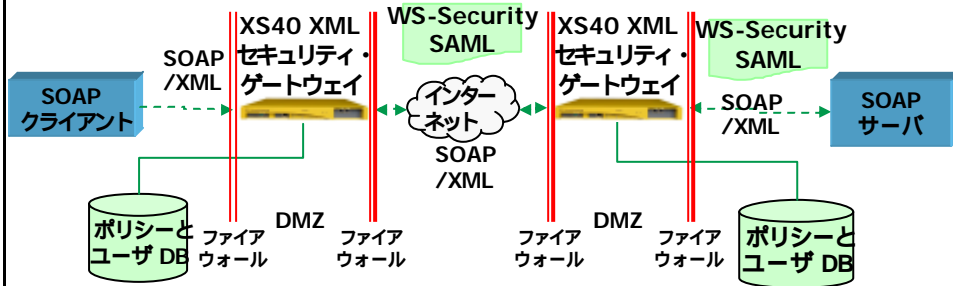
# XS40 SAML事例

## 米国保険会社での顧客認証

- 顧客サービスのためのエクストラネット
- 顧客のユーザ・ディレクトリは一箇所で管理
- 送信中の情報は暗号化・署名して保護



# XS4O SAML事例： 米国防省 - 部門間の相互アクセス



- フェデレーション (D連携)により、認証と権限の管理は独立したまま
- ユーザはローカルで認証され、リモートにアクセスする際はWS-Security/SAML でID情報を伝達
- サーバはSAMLトークンでアクセスを認可

Distributed by

東京エレクトロン

27



# DATAPOWER

INTELLIGENT XML-AWARE NETWORK INFRASTRUCTURE

お問い合わせは：

東京エレクトロン株式会社 コンピュータ ネットワーク事業部  
貴社担当営業

または

東京：〒107-8481 東京都港区赤坂5-3-6 TBS放送センター 03 (5561) 7190

大阪：〒532-0003 大阪市淀川区宮原3-4-30 ニッセイ新大阪ビル 06 (6399) 0244

Webサイト <http://www.tel.co.jp/cn/product/datapower/>