内容

- 連携アイデンティティ
- SAML　2.0概要

RSA SECURITY

2

連携アイデンティティ

RSA SECURITY

連携アイデンティティ（Federated Identity）とは？

技術的定義

The agreements, standards, and technologies that make identity and entitlements portable across autonomous domains.
The Burton Group

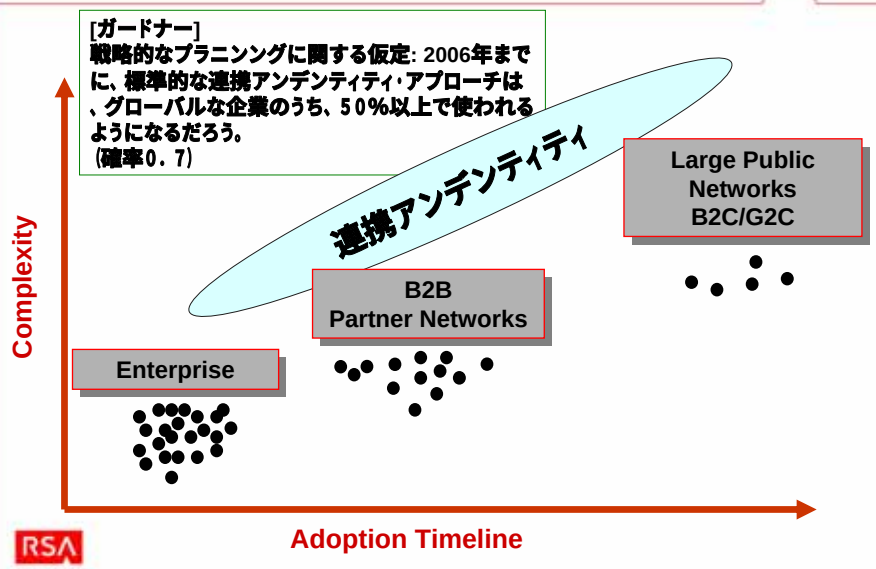
アイデンティティと権限を、ドメイン間に渡って利用可能にするための同意、標準、テクノロジー

ビジネス上の定義

取引先や顧客に対して、アイデンティティを取り扱うことによって生じるコスト、リスク、新たな負荷を持つことなく、Webアプリケーションへのより効果的で安全なアクセスを提供することによって、大規模な組織が直面する困難な問題を解決するためのアイデンティティに関する標準化手法

RSA SECURITY

連携アイデンティティ
Scope of Current Deployments



RSA SECURITY

5

標準と仕様

	SAML	Liberty ID-FF	WS-Federation
概要	The purpose of SAML is to define, enhance, and maintain a standard XML-based framework for creating and exchanging authentication and authorization information	Aims to provide open standard and business guidelines for federated identity management spanning all network devices	One of the WS-* specifications that defines mechanisms to allow different security realms to federate by allowing and brokering trust of identities, attributes, authentication between participating Web services.
スポンサー	OASIS	150 consumer and technologies companies, including BofA, AmEx, Fidelity, GM, Sony, Vodafone, Sun, RSA	Microsoft, IBM, RSA, BEA, VeriSign
履歴	SAML 1.0 (Q2 '02) SAML 1.1 (Q2 '03) SAML 2.0 (Q1 '05)	Liberty 1.1 (Q1 '03) Liberty ID-FF 1.2 (Q4 '03)	WS-Fed (TBD)

RSA SECURITY

6

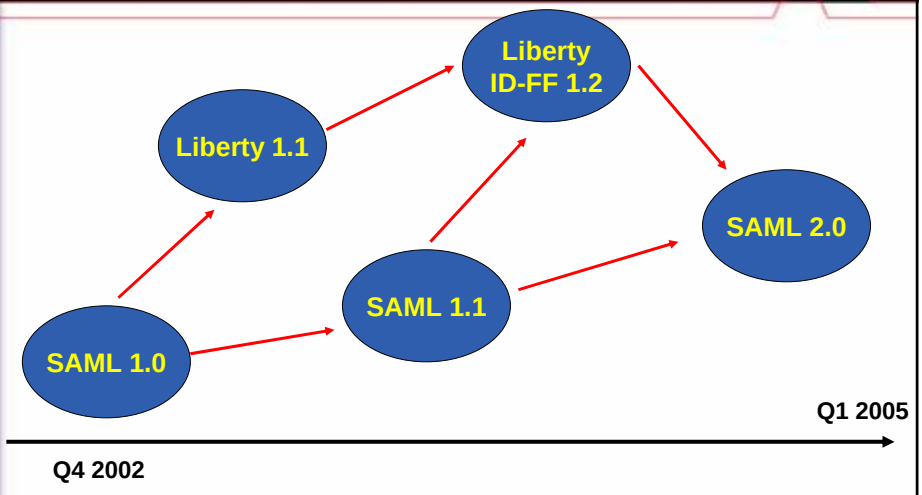
標準と仕様

	SAML	Liberty ID-FF	WS-Federation
ベンダ	Many implementations available, including open source toolkits	Sun, Ping Identity, Phaos, Trustgenix RSA has announced intent to support by Q4 2004	Microsoft, IBM, RSA, and a few other vendors have announced intent to support and produced prototypes
利用例	• Web SSO • Attribute Exchange • Authentication Query • Authorization Query	• Enhanced Web SSO (e.g. acct. linking, privacy, session mgmt.) • Other specs (ID-WSF and ID-SIS) support additional use cases • Smart client (LECP)	• Web SSO (passive requestor profile) • Smart client (active requestor profile)
推奨採用時期	• 現在 -	• 現在-6ヵ月後	• 12-18 ヵ月後

RSA SECURITY

7

SAML と Liberty



RSA SECURITY

(注意)SAML 2.0とLiberty ID-FF1.2の実装レベルのコンパチビリティはない

8

SAML 2.0概要

RSA SECURITY

9

SAMLとは

- SAML (Security Assertion Markup Language)
- 信頼するパーティ間のセキュリティ関連情報の交換のためのフレームワーク
- 連携アイデンティティを機能させるための鍵となる標準
- 現実のビジネスシナリオをサポート
- ドメインをまたがるSSOサービスに広く採用されている
- XMLを基盤にした標準仕様

  XMLを用いているためセキュリティ標準との親和性

  XML署名、XML暗号、XACML

RSA SECURITY

10

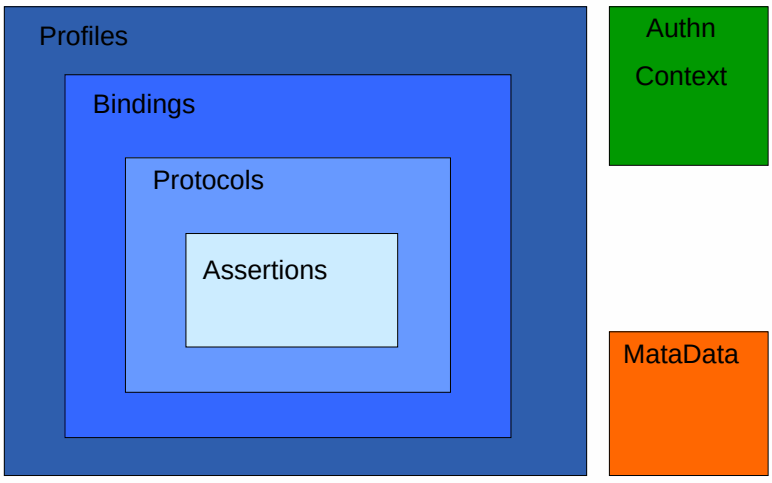
SAMLの代表的用途

- 連携アイデンティティ
- シングル・サイン・オン
- 属性サービス
- シングル・ログアウト
- WEBサービスメッセージの保護

RSA SECURITY

11

SAML標準の概念



RSA SECURITY

12

SAMLの基本的用語

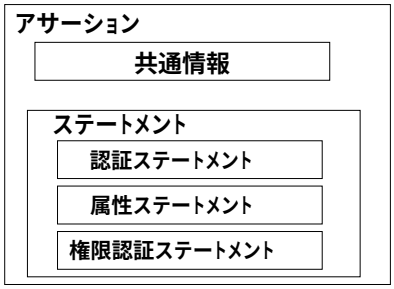
- **アサーション** (Assertion)
  - 具体的なサブジェクトに関してセキュリティデータを含んだXMLのメッセージ
  - 例： ユーザIDと認証方式
- Relying **パーティ**
  - SAMLアサーションを要求したり、受けたりするシステム
- Asserting **パーティ**
  - SAMLアサーションを作り出すシステム

RSA SECURITY

13

SAMLアサーション

- セキュリティ情報のアサーション
- 3種類のアサーション
  - Authentication Assertion (認証)
  - Attribute Assertion (属性)
  - Authorization Decision Assertion (権限承認)
- 各アサーションには、デジタル署名を付加できる



RSA SECURITY

14

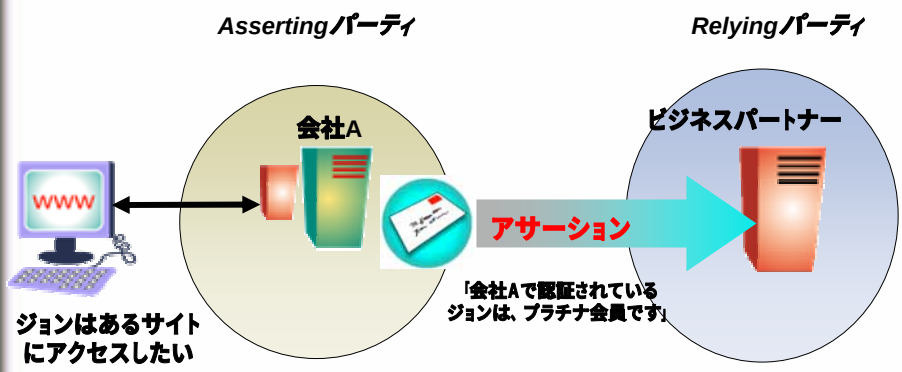
SAML アサーション例

```
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  Version="2.0"
  IssueInstant="2005-01-31T12:00:00Z">
  <saml:Issuer>
    www.acompany.com
  </saml:Issuer>
  <saml:Subject>
    <saml:NameID
  Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
      j.doe@company.com
    </saml:NameID>
  </saml:Subject>
  <saml:Conditions
    NotBefore="2005-01-31T12:00:00Z"
    NotOnOrAfter="2005-01-31T12:00:00Z">
  </saml:Conditions>
    ... statements go here ...
</saml:Assertion>
```

RSA SECURITY

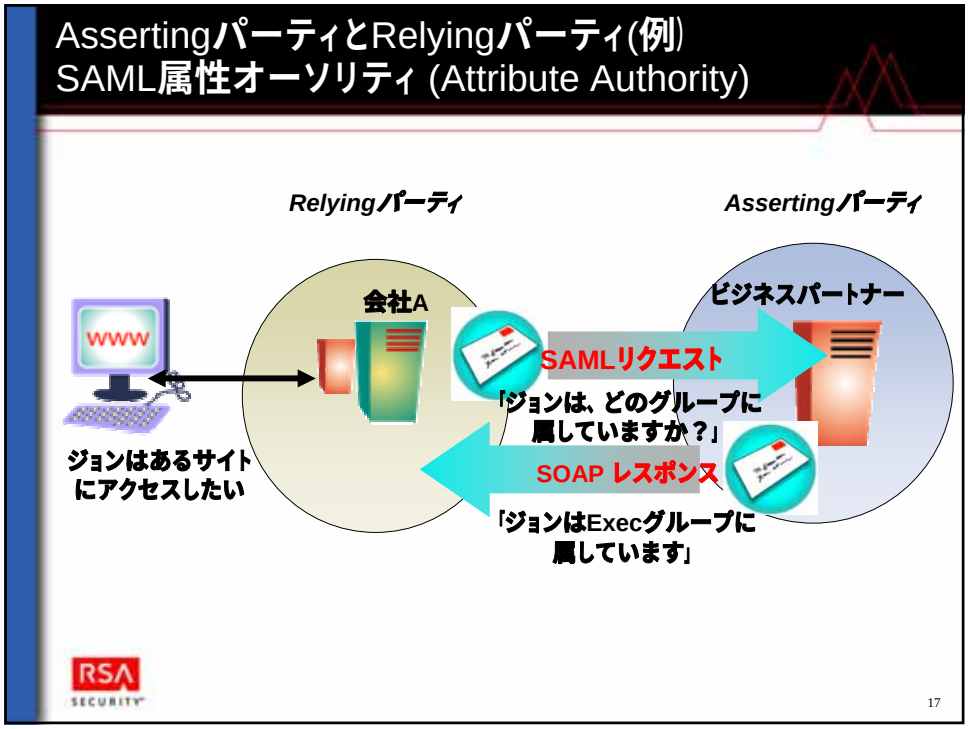
15

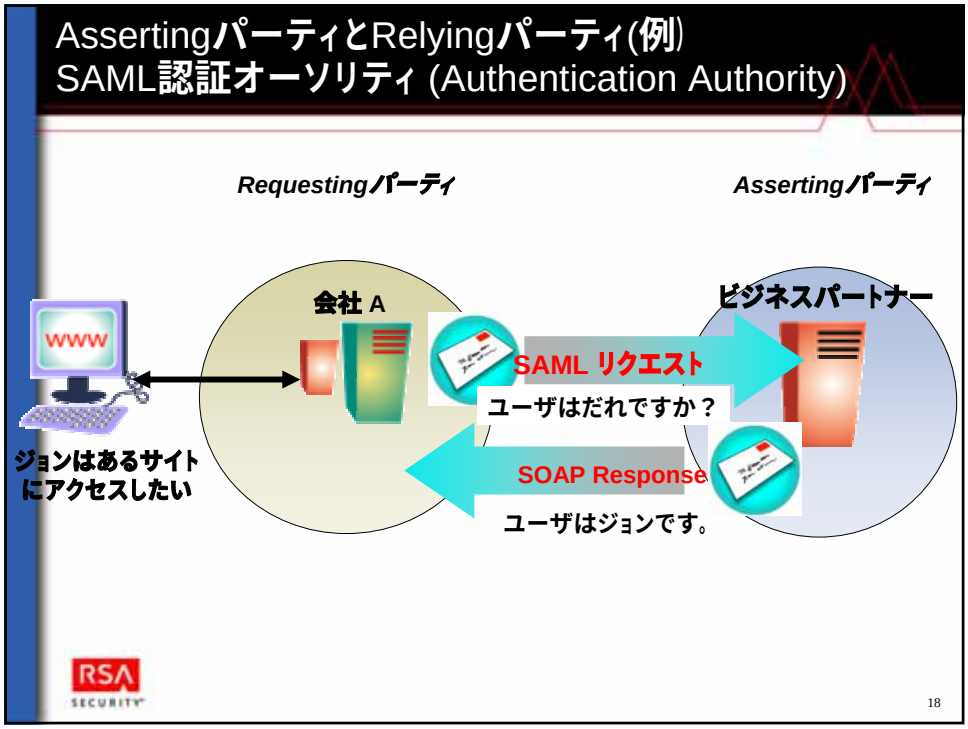
AssertingパーティとRelyingパーティ(例) SAML Web シングル・サインオン



RSA SECURITY

16


AssertingパーティとRelyingパーティ(例)
SAML属性オーソリティ (Attribute Authority)
Relyingパーティ
Assertingパーティ
会社A
ビジネスパートナー
www
SAMLリクエスト
「ジョンは、どのグループに
属していますか？」
SOAP レスポンス
「ジョンはExecグループに
属しています」
ジョンはあるサイト
にアクセスしたい
RSA
SECURITY
17


AssertingパーティとRelyingパーティ(例)
SAML認証オーソリティ (Authentication Authority)
Requestingパーティ
Assertingパーティ
会社 A
ビジネスパートナー
www
SAML リクエスト
ユーザはだれですか？
SOAP Response
ユーザはジョンです。
ジョンはあるサイト
にアクセスしたい
RSA
SECURITY
18

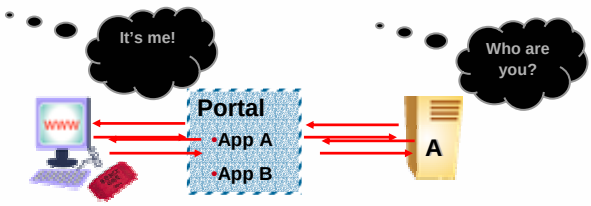
BAP (Browser Artifact Profile) と、BPP (Browser Post Profile) との違い

- Browser/Artifact Profileはプルモデルと呼ばれている。Asserting パーティからReplying パーティに、リファレンスでSSOアサーションを渡す。この渡し方は、バックチャネルのメッセージ交換で行われる。（Replyingパーティから Asserting パーティにアサーションが「プル」される）
  - ブラウザでアサーションを受け渡すので比較的軽い処理。
- Browser/POST Profileは、プッシュモデルと呼ばれる。BAPと比較して、値でSSOアサーションを渡す。この場合は、バックチャネルのコミュニケーションの必要はない。実際には、Assertingパーティがアサーションを Replyingパーティに「プッシュ」する。
  - PKI/デジタル署名必須

RSA SECURITY

19

SAMLの働きー Web SSO (BAP)

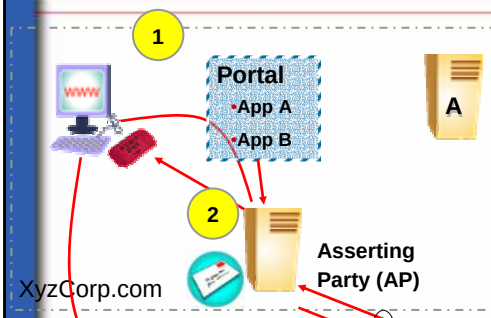


XyzCorp.com

RSA SECURITY

20

SAMLの働きー Web SSO (BAP), continued

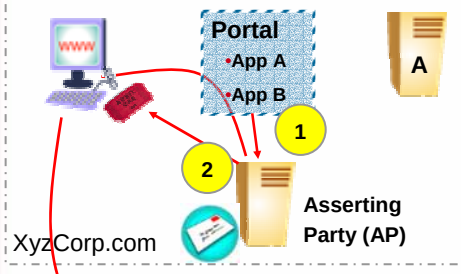


1. ユーザが、アプリケーションBにアクセスしようとします。
2. チケット (クッキー) を読み、アサーションを生成する。
3. アサーションが利用可能なことを示す"アーティファクト"とともに、そのリクエストをRPにリダイレクトする。
4. RPは、アーティファクトと"要求"アーサーションを復号化する。APは、アーサーションを返す。
5. RPは、アーサーションを復号化して、"ローカルな"クッキーを生成し、ユーザをアプリケーションBにリダイレクトする。

◆BPPと比べて、ブラウザーには
コンパクトな処理
◆FIMの大部分なユーザがBAPを使っている

21

SAML の働きー Web SSO (BPP)



1.ユーザがアプリケーションBにアクセスしようとします。
2.チケット (クッキー) を読み、アサーションを生成する。
3. アサーションをサインして、RPのアサーション・コンシューマ・サービスに直接送る。
4. RPは、アサーションを復号化して、ローカルなチケット (クッキー) を作成して、ユーザをアプリケーションB にダイレクションを行う。

ブラウザー経由
SAMLアサーションが攻撃される可能性あり

BPPでSSOを実現した時には、
SAML complianceでは
デジタル署名は必須。(SAML1.1仕様)

22

SAML 2.0の目的

- SAML 1.1までの実装経験とSAMLベースのセキュリティ・アーキテクチャを反映。
- SAML 1.1までに組み込まれなかった機能追加
- 連携アイデンティティモデルの統一

RSA SECURITY

23

SAML 2.0の構成

- Conformance Requests
- Assertions and Protocol
- Bindings
- Profiles
- Metadata
- Authentication Context
- Security and Privacy Considerations
- Glossary

RSA SECURITY

24

SAML 2.0の新機能

- 強固な連携アイデンティティと管理
- シングル・サイン・オンプロファイルの改良
- アイデンティティ・プロバイダー探索
- 基本的セッション管理とグローバル・ログアウト
- 属性共有プロファイル
- 認証機構の詳細な記述
- 簡易構成のためのMetadata
- Enhanced Client or Proxy(ECP)プロファイル

RSA SECURITY

25

SAML 2.0まとめ

- OASIS標準として、SAML1.X、Liberty ID-FFその他を統合
- 利用を促進する新機能
  - 管理・展開コスト削減
  - 法規制に準拠するIDデータコントロール向上
  - Webユーザオンライン利用形態の向上
  - IDデータの管理と保護向上
- 完全な連携アイデンティティのソリューション

RSA SECURITY

26


RSA
SECURITY
Confidence Inspired™