FUJITSU THE POSSIBILITIES ARE INFINITE

電子認証基盤の技術動向

2004年12月9日

富士通株式会社

目次（内容）

1．電子認証基盤の概観

電子認証基盤の定義

電子認証基盤とは、下記3A（4A）のセキュリテイ機能を実現するための仕組み、機構

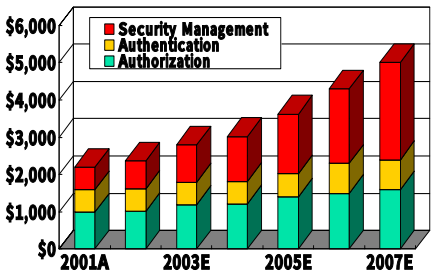
■ **認証(Authentication)**
- 情報システムにおいて利用者や機器・プログラム等の構成要素が、情報システム提供者等の他の当事者にとって想定した正しい対象・環境であることを確認する機能あるいは行為

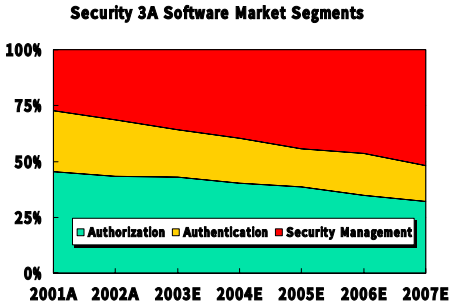
■ **認可(Authorization)**
- 認証された利用者や・機器・プログラム等の構成要素が、プログラム、又は、データに対するアクセスを許可するための機構

■ **管理 (Administration)**
- 上記、認証・認可のための利用者情報・機器・プログラム情報やアクセス制御情報を管理する機能

（■ **監査・監査証跡　(Audit & Audit Trail)**）
- 利用者・機器・プログラムがログイン。ログアウトした日時や操作履歴を管理する機構
- セキュリティ・ポリシーに従った運用が行われているかをチェックし監査レポートにまとめる機能

市場予測





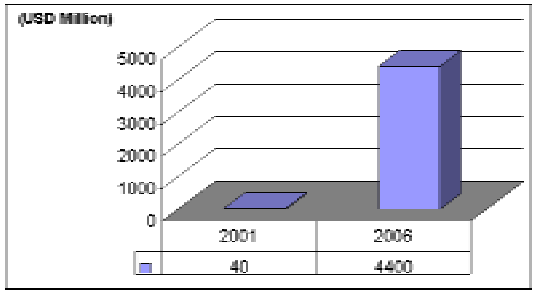
3Aソフトウェア市場全体は、World Wide で
2007年度　＄5Billion
2002年度 2.1 Billionから2007年度まで
年平均市場成長率　15.3% が見込まれる。

管理の3Aに占める割合が増加傾向。
次期、最も市場成長率の高いセグメントは、
管理であり、　年平均市場成長率は、
28% と予測されている。

(Source: WACHOVIA SECURITIES)

XML Security関連市場予測

- XML/Web ServicesのSecurityに関する市場サイズ予測(製品･サービス込み)
  - $40M(2001年)から$4.4B(2006年)に成長
  - なお、$4.4B(2006年)という数値は、全AAA(Authentication, Authorization and Administration) Security市場の65%を占める



出典：ZapThink

2．認証

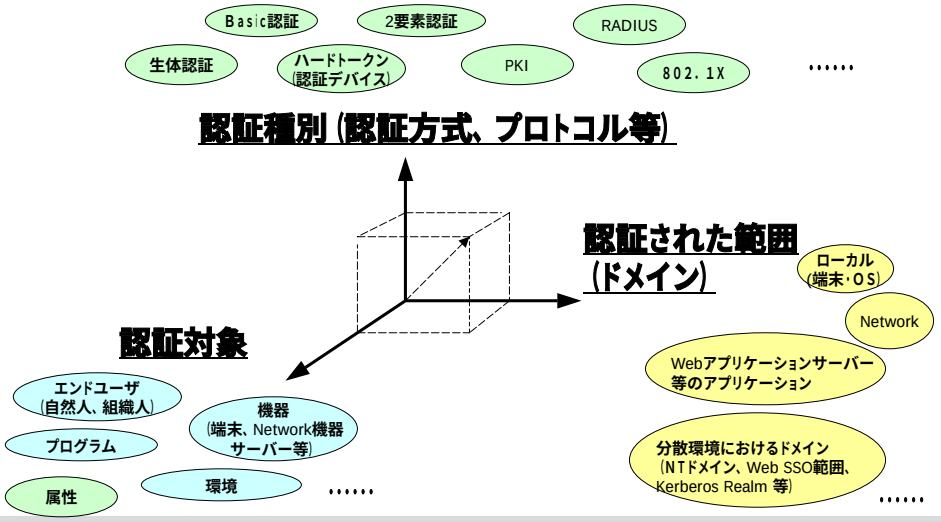
認証に求められる要件

- 認証に対する要件と、それに対する要素技術

種別		要件	要素技術
共通		様々な認証の操作や管理を簡易にしたい。	SSO、認証統合
ユーザ認証	本人認証	なりすましの脅威を防止するために確実な本人認証を行いたい。	生体認証、スマートカード、USB Token 、 PKI 、二要素認証、802.1X(EAP-TLS), etc.
	属性認証	ユーザ（又は機器）の持つ属性によって認証したい。（例： 個人の持つ資格）	証明書への属性情報の格納、属性証明書、SAML属性Assertion等
Networkでの認証		特定の機器のみNetworkへの接続を許可したい。 認証した人のみ Networkの通過を許可したい。	アドレスチェック、 認証VLAN, ＶＰＮ etc.
機器の認証		機器を特定したい。	TCG PKI
環境の認証		最新のSecurity パッチが適用されている持込ノートＰＣのみ接続を許可したい。（ウィルス感染防止）	検疫ネットと 認証サーバーの連携
		プログラムの身元保証を行いたい。 （不正なプログラムの動作を防止したい。）	NGSCB (Next Generation Secure Computing Base)

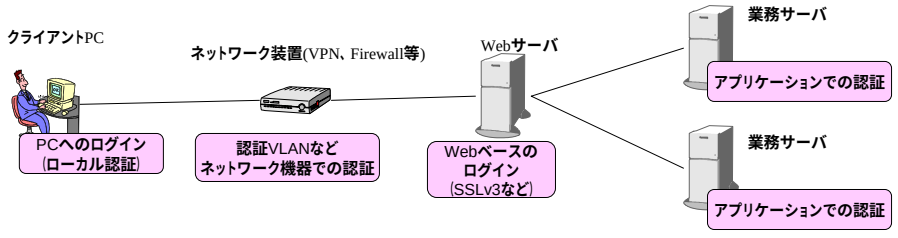
認証の多様性（1／2）

- 認証を考える際に「対象」「ドメイン」「種別」の明確化が必要。



認証の多様性（2／2）

- 認証が必要な場所や目的、方式も多様。
  例えば、以下のように端末利用時の認証(ローカル)から、ネットワークやWebアプリケーションまで、複数の箇所で認証が必要な場合もある。



属性認証

属性認証とは

利用者の認証やサービスの提供(認可など)の際に確認する属性を保証する仕組み。
(利用者と属性との結び付き、属性情報の内容など)

属性の分類と例

分類の観点	分類内容	属性の例	属性利用に際し考慮すべき点
更新頻度	更新間隔が長い(静的)	氏名、生年月日、住所	静的な属性のうち、ID情報の更新間隔が長いものについては、ID情報(例えば証明書)に埋め込むことも可能。 動的な属性については、属性の利用時にその都度、状態を確認する必要がある。
	更新間隔が短い(動的)	位置情報、所持ポイント	
用途	権限確認(アクセス制御)	資格、肩書、役職、年齢	第3者による検証が必要かどうかは、属性の内容だけでなく、用途による場合もある。 例えば、アンケート等の場合は本人申告のみで十分だが、権限確認などに利用する場合は、検証が必要。 また検証したことを保証する必要がある場合もある。
	情報流通(付加価値提供)	購買履歴、趣味、年齢、職業	
保証	本人の申告に基づく	ニックネーム、趣味	
	第3者による検証を行う	国家資格、住所、年齢	

機器認証

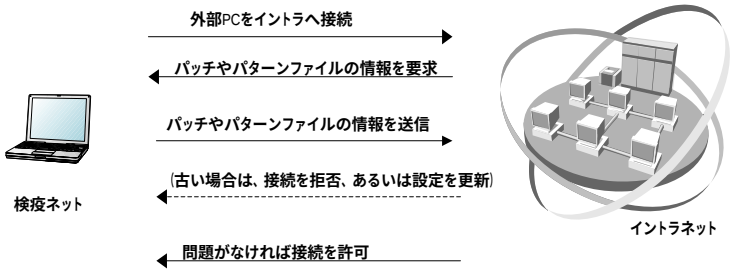
- **機器認証とは**
  - **利用者が操作している(あるいは操作しようとしている)機器を特定するための認証。**
    - あらかじめ登録されている機器であることが確認でき、利用者の認証と組み合わせることで、より高セキュアな認証が実現できる。
    - TCG(Trusted Computing Group)が規定するTPM(Trusted Platform Module)の利用などが挙げられる。

- **TCG(Trusted Computing Group)とは**
  - **目的**
    情報機器のセキュリティ面での信頼性確保を目標としたハードウェアベースのセキュリティ技術の標準化(ハードウェア仕様, ソフトウェアAPI の仕様策定)
  - **設立**
    2003年4月　AMD, HP, IBM, Intel, Microsoft により設立
  - **参加メンバ**
    79社 (2004年9月現在)
    - 業種：PC/サーバ, 周辺機器, 半導体, ソフトウェア (OS/アプリケーション), 携帯電話サービス,等

URL：http://www.trustedcomputinggroup.org/

環境の認証（例：「検疫ネット」）

- 機器をネットワークに接続する際、検疫ネット上で、セキュリティパッチやウィルスパターンファイルの更新などの状態を検証し、ポリシーに従った適切な設定となっている機器だけ接続を許可する



認証の技術動向

認証の高度化

複数の要素技術をインテグレーションすることで Security 強度を高める方向性へ技術が進化。
同時に認証の運用形態も目的に応じて多様になる。

- **機器認証＋本人認証＋属性認証などの複数の要素による高度な認証が可能に**
- **複数の認証種別のインテグレーション**
  - 例：ＰＫＩ＋生体認証等
- **環境の認証**
  - 最新のセキュリテイパッチがあたっているPCのみ Networkへの接続を許可
  - 身元保証されたセキュアなプログラムだけがプログラム実行を許可する機能を持つPCのみ Network への接続を許可（理想形）

3. 認可

認可に求められる要件

- 認可に対する要件と、それに対する要素技術

種別	要件	要素技術
シングルサインオン	エンドユーザに一度の認証で複数の業務のアクセスを認めることによりサービス性を向上させたい。	Web SSO, Kerberos, NT Domain, DCE, etc.
連携SSO	複数のID管理ドメイン間でIDを連携したい。	連携SSO、SAML、Liberty, eAuthentication
	複数のID管理ドメイン間で、属性に応じたダイナミックなアクセス制御を行いたい。	
木目の細かなアクセス制御	ユーザの資格、職位、所属組織に応じたアクセス制御を行いたい。	RBAC, XACML
再認証の設定	重要な業務の操作を行う際に再認証の処理をエンドユーザに行わせたい。	Ruleベースのアクセス制御

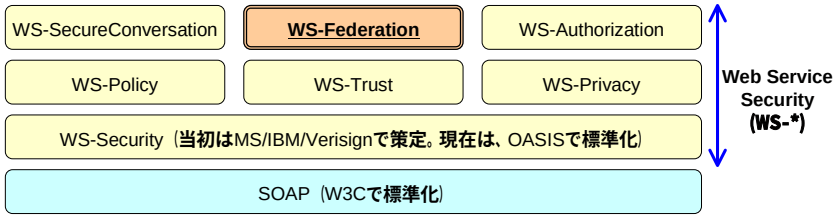
連携SSO：「Liberty仕様」

- Liberty Alliance Project とは
  - Liberty Alliance Projectは、インターネット上での新しい水準の信頼、商取引、通信を推進するために結成された産業団体。
  - Libertyは、Identity情報のプライバシーやセキュリティを考慮しつつ、広域なネットワークIDベースのやりとりをオープンな技術仕様で策定する。
    - 利便性の向上 ：
      Single-Sign-On, Single-Log-Out
    - プライバシの考慮 ：
      許可ベースのID連携と属性情報交換、匿名サービス
    - Identityの流通 ：
      認証アサーションや属性情報のプロファイルの定義
  - 技術仕様策定だけでなく、具体的なサービス実現のための普及促進も図る。
    - 相互接続テストの実施
    - Identity関連サービスの検討

ID-FF	複数のIDを連携しSSOを実現する仕組みを定義。
ID-WSF	Webサービス上で利用者の同意の基で、利用者情報を交換する方式を定義。
ID-SIS	具体的なサービスモデルを想定し、メッセージやインターフェイスを定義。

連携SSO：「WS-Federation仕様」

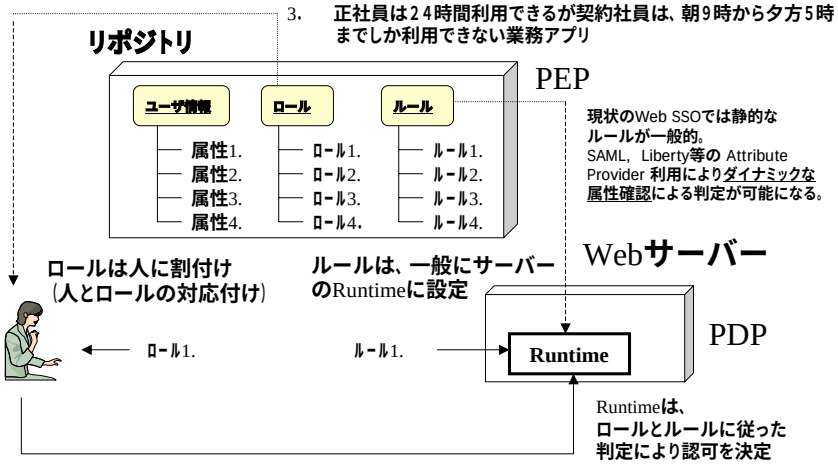
- WS-Federationとは
  - ドメインを越えて、Single-Sign-Onを実現する技術。
  - Microsoft、IBM、Verisignにより2003年7月に公開。
  - Web Service Securitiy仕様のひとつとして位置づけられる。
- Web Service Securitiyとは
  - 2002年4月に、Microsoft、IBM、Verisignがロードマップを発表したWebサービスにおけるセキュリティフレームワークのための仕様群。
  - “Web Services Security”は、1つの基本プロトコル「WS-Security」と6つの補助プロトコル、計7つの仕様群で構成される。
    構成の概念を以下に示す。



RBAC と Rule Base のアクセス制御

ロールの例
1. 職位を表すロール
2. 属している組織を表すロール
3. その人が持っている資格を表すロール

ルールの例
1. Basic認証でしか認証されていないユーザは、PKIで再認証しないと利用できない業務アプリケーション (in B)
2. ユーザ属性で20歳以上でないと受けられないサービス (例えば B2C での酒屋のサービス)
3. 正社員は24時間利用できるが契約社員は、朝9時から夕方5時までしか利用できない業務アプリ



XACML

- XACMLとはアクセス制御ポリシーのためのXMLベースの言語2003年2月にOASISで標準化
- アクセス制御のためのポリシー(認可条件)などをXMLで表現。条件確認のための要求･応答プロトコルも規定。
- XACMLにより、アクセス制御ポリシーの一貫性保持を図れ、相互接続性も期待できる。XACMLの標準化動向
  - XACML 1.0 (2003年2月)
  - XACML 1.1 (2003年8月)
  - XACML 2.0 (2004年)
    - 階層化されたリソースへの対応
    - time zoneへの対応
    - プロファイルの提供 (RBAC, LDAP, 再帰構造の設定, 管理の代行, 電子署名)

認可の技術動向

認可の高度化

- Web SSOから連携SSOへ
  (Hub型モデルからスポーク型モデルへ)
- Web SSOや複数の連携SSO方式が共存可能な
  e-Authentication アーキテクチャにおけるプロトコル変換
  やAA/CS統治の機構が考えられ始めている。
- アクセス制御方式の進化
  - RBAC(: Role Based Access Control)
  - Rule base のアクセス制御（静的なルール）
  - Rule base のアクセス制御（動的な属性判定によるアクセス制御）

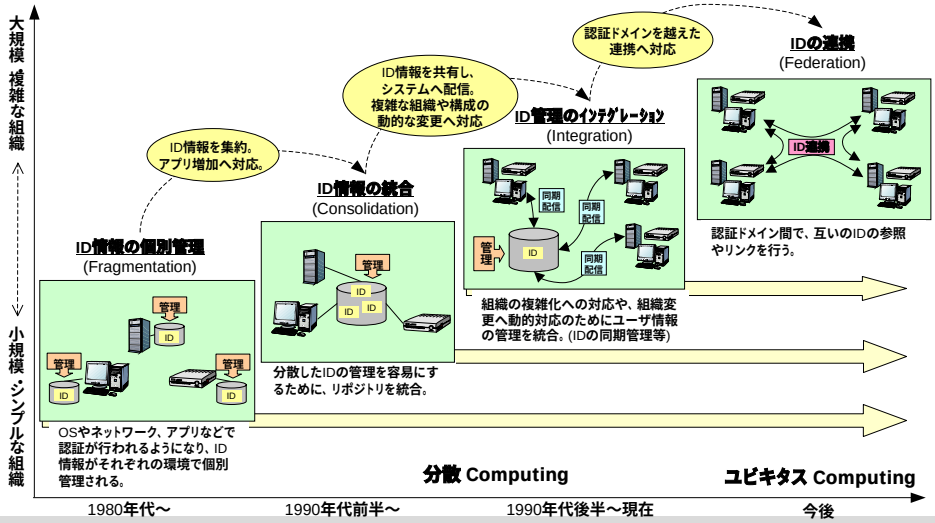
4．管理

管理に求められる要件

種別	要件	要素技術
ID管理 ID Life Cycle管理	C/S, Web SSO, パッケージアプリや機器を含む様々な種別のIDのライフサイクル管理を行いたい。 IDの申請、承認を行いIDの追加、削除に関して承認ログを残したい。	ID Provisioning、SPML、ワークフロー制御
管理者権限の分散	認証。認可情報の管理者権限を階層化し分散させたい。（二階層目として、管理権限ドメインを限定）	管理者Role
ID連携	複数のID管理ドメイン間での連携を管理したい。 複数のID管理ドメイン間で認可の連携を管理したい。	eAuthentication 連携SSO、SAML、Liberty
属性管理	属性に応じたダイナミックなアクセス制御のために属性を管理。	SAML、Liberty (Attribute Provider)
権限付与管理 （Entitlement Management）	認証・認可に用いる利用者や機器の属性情報、ネットワーク情報の関係付けを管理したい。	X.500, LDAP, RDB等のリポジトリ技術
アクセス制御ポリシーの管理（Role,Rule等）	アクセス制御の条件の設定や更新などの管理を行いたい。	RBAC制御、 ルールベース制御、 XACML

ID管理(ID管理手法の変遷)

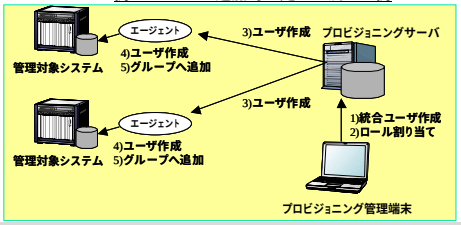
- アプリケーションの多様化や管理対象IDの増加、組織構成の複雑化などに伴い、ID管理技術のコンセプトは、以下のように推移してきた。



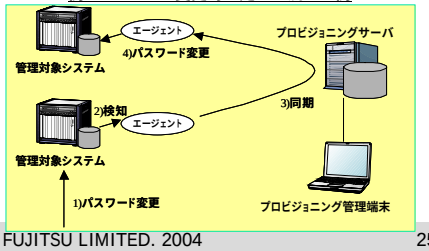
IDライフサイクル管理（ユーザプロビジョニング）

- ユーザプロビジョニングについて
  - ユーザプロビジョニングの特徴
    - ユーザ情報を個々のシステムに設定するエージェントを利用することで、OSや既存システムなどのユーザ情報の一元化が可能。（OS、DB、Webアクセス、ビジネスアプリケーションなど）
  - ユーザプロビジョニングが管理するユーザ情報
    - アカウント、クレデンシャル、属性、エンタイトルメント、ロール等
  - ユーザプロビジョニングが対象とする主な操作
    - アカウントの追加や削除、アカウントのロック、パスワードの変更、ロールや属性の変更等
  - ユーザプロビジョニングの問題点
    - 対象システムごとにエージェントを作成する必要がある。
      （ただし、OSやメジャーなアプリに関しては、プロビジョニング製品からエージェントが提供される場合がある）

例1：アカウント追加時の処理の流れの例



例2：パスワード変更時の処理の流れの例

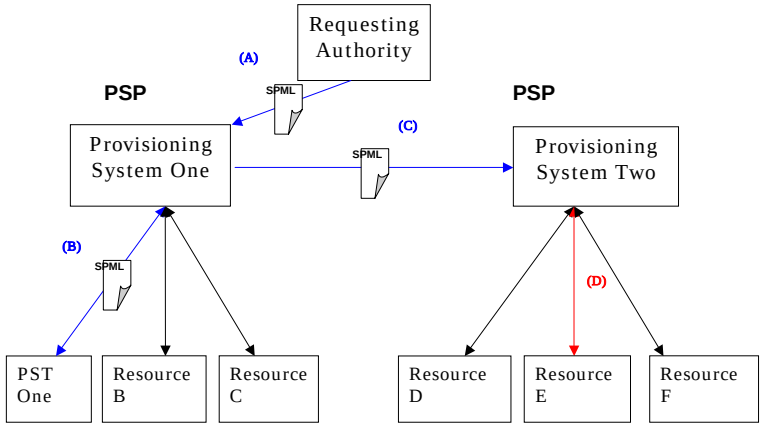


（参考）SPML標準化動向（1／2）

- SPML（Service Provisioning Markup Language）
  - ユーザプロビジョニングを実現するためにOASIS Provisioning Services TC(PSTC)で標準化。
  - ユーザプロビジョニングを行う際のリクエストとレスポンスをXMLで表現。
- SPMLのOASIS承認までの流れ
  - **2001年末** OASISにPSTC(Provisioning Services Technical Committee)発足。
    - メンバはAccess360, BMC, Business Layers, CA, Entrust, Netegrity, Novell, Oblix, OpenNetwork Technologies, Sun/Waveset
  - **2003年7月** Catalystカンファレンスで相互接続デモ
    - 参加ベンダは10社、BMC, Business Layers, Critical Path, Entrust, OpenNetwork Technologies, PeopleSoft, Sun, Thor Technologies, TruLogica, Waveset
  - **2003年8月** Sun/Waveset が、SPMLツールキット公開
  - **2003年10月** IBMがSPML2.0への推奨をWS-Provisioning仕様に記載
  - **2003年11月** SPML1.0承認
  - **2004年末** SPML2.0承認予定

(参考) SPML標準化動向 (2／2)

- SPMLのプロビジョニングシステムモデル



（A）RAがPSPに処理要求を提出

（B）PSPが管理下のPSTに処理を依頼

（C）PSPが他のPSPに要求を転送し、管理外のリソースに要求を依頼

（D）転送を受けたPSPが管理下にあるリソースに処理を行う

ID連携

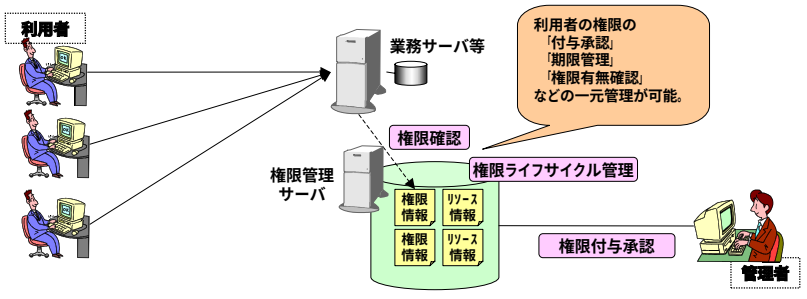
- 「ID連携」のためのとは
  - ドメイン内の事業者がそれぞれ個別に管理しているIdentityを、事業者を越えて相互に共有することを実現するための管理の仕組み
- 「ID連携」の実現のための要素
  - 「ドメインを越えたSSOの実現」
    - 認証Assertionとセッション管理によるSSO
  - 「IDのマッピング」
    - 認証ドメイン間でアカウントをリンク（プライバシー保護は必要）
    - アカウントと属性をリンク
      （アカウント管理と属性管理とを分離した上で、必要に応じてリンク）
  - 「ドメインを越えた認証、認可などの情報の共有」
    - 認証ドメインを超えてPDPからPEPへ認可Assertionを提供
    - 認証ドメインを超えて属性Assertionを提供（プライバシー保護は必要）
  - 「運用面の管理」
    - ビジネス面、法律面のアグリーメント、信頼関係の構築
    - 監査の実施

米e-Authentication

- 概要
  - e-Authenticationとは、アメリカの公的サービスを受ける際のID検証サービス。(e-Governmentの一環で検討中)
    - 連邦政府の全ての認証作業を連邦政府ポータルサイト「FirstGov.gov」経由で一元的に行えるようにしようとする。
    - 認証情報の連携(Federate)により、民間サービスと公的サービスとを連続的に利用することも可能とする。
- 目的
  - 利用者の利便性を向上させることでe-Governmentの普及を促進させる。
  - 認証ポリシーやリスク分析手順、製品やサービスの認定などを共通化することで、民間企業、市民、政府の負担の軽減させる。
- e-Authenticationの主な作業
  - サービスのリスクと認証方式の対応づけ
    サービスのリスク分析手法整備、クレデンシャルサービスの認定など
  - 認証コンセプトの整備と実証
    Identity Federation技術を実装。
  - 相互接続の検討および実験システムの運用
    Interoperability Labによりプロダクトやサービスの相互運用性を検証

権限付与管理(Entitlement Management)

- 権限付与管理(Entitlement Management)とは、システム内の資源(データやファイルなど)に対してアクセスの可否の権限を付与し管理する仕組み。
  - 権限付与の承認フローの管理
  - 権限の期限の管理
  - 権限情報の提供
    (予め利用者に付与した資格だけでなく、IPアドレスや機器情報などの組合せを含めて権限を管理することで、動的な条件に基づく権限情報の提供も可能)



5. まとめ

まとめ

技術動向からみた次世代認証基盤に求められる要件

- 認証の多様性に対応可能に
  - 機器認証＋人の認証＋Network認証といった複合的で高度な認証が可能
  - 属性認証への対応が可能
  - 複数の認証方式に対応可能な柔軟性、拡張性
- 複数ドメイン間での認可、ダイナミックなアクセス制御
  - 複数のドメイン間での連携SSO機能を実装すること
  - ダイナミックなアクセス制御の判定が可能な機構を実装すること
- 管理系の高度化
  - ID数の Scalability、ID Provisioning, ID ライフサイクル管理
  - 属性管理、Entitlement management
  - 連携SSOにおける統治
  - e-Authentication モデルの Portal におけるリダイレクション管理


FUJITSU
THE POSSIBILITIES ARE INFINITE