

Information Card と Windows CardSpace のご紹介

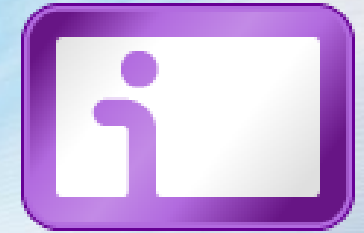
マイクロソフト株式会社
田辺 茂也

<http://blogs.technet.com/stanabe/>

パスワードの次の一手

⇒ Information Card

- ⇒ 個人の Identity 情報を「カード」として表現し、ネットワーク上で使えるようにしたもの

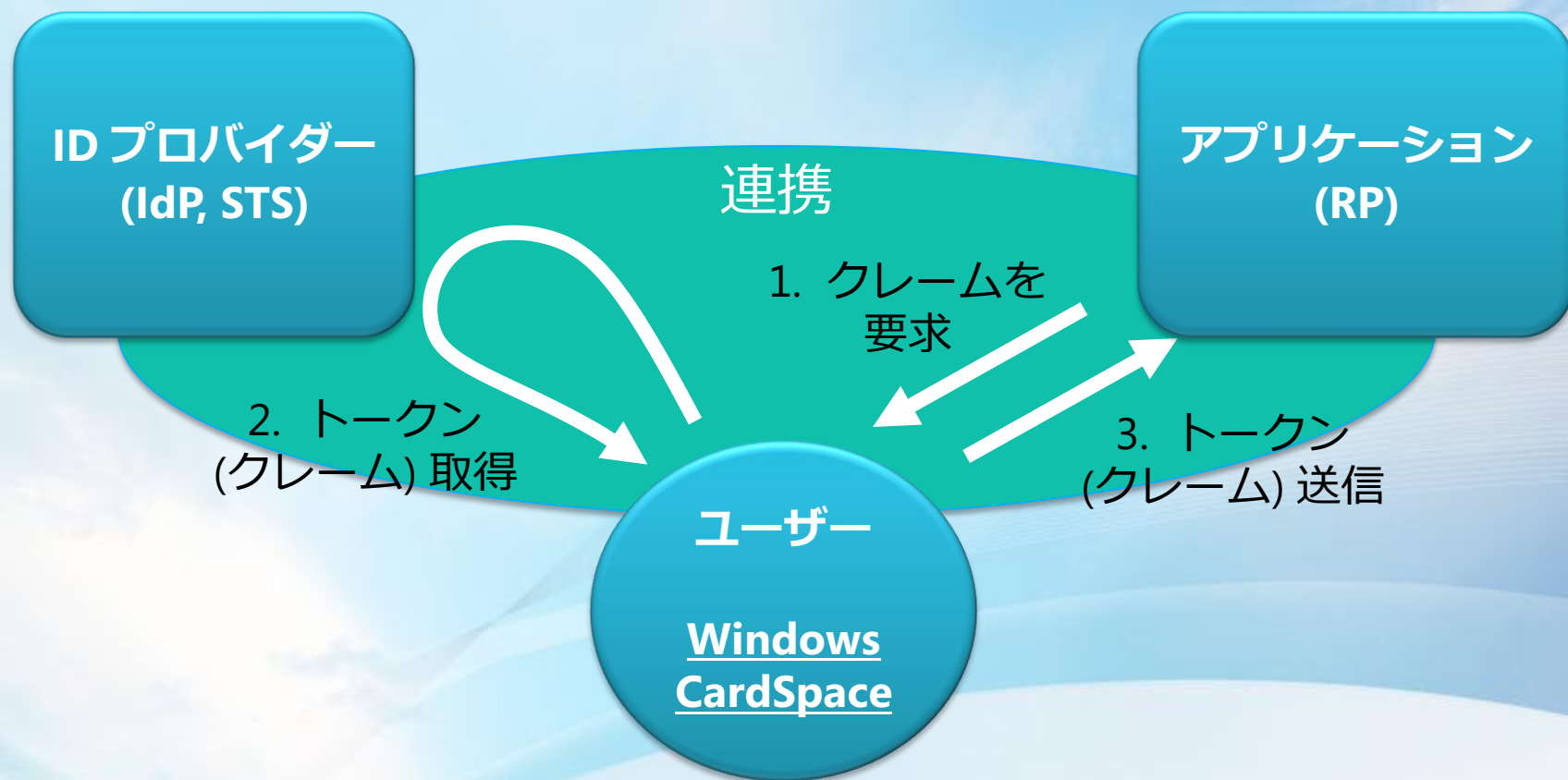


⇒ Windows CardSpace

- ⇒ Information Card セレクタの実装



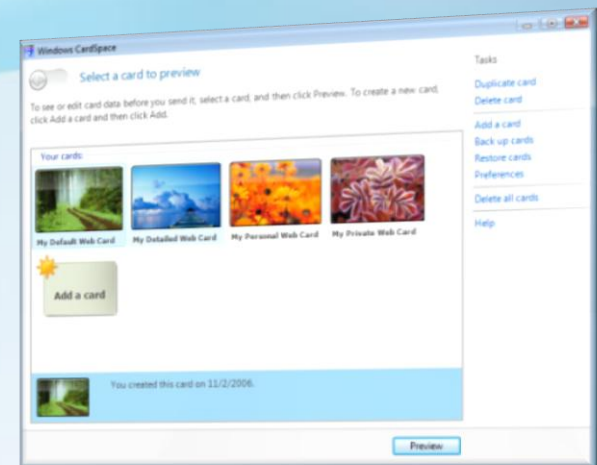
認証の流れ



- ⇒ アプリケーション: ユーザーを特定するためにクレームを利用
- ⇒ ID プロバイダー: クレームを含むトークンを発行
- ⇒ 連携: 信頼関係のもと、クレームが渡される

Windows CardSpace = Identity セレクター

- ④ 「カード」を選択する、
簡単で一貫した操作性を提供
- ④ カードの利用、クレーム (ユーザの属性情報) の
提供をユーザがコントロール
- ④ ユーザ名・パスワードの使用を低減
- ④ フィッシングからの防御
- ④ WS-* による通信
- ④ 必要システム
 - ④ .NET Framework 3.0 以降
(現行の Windows CardSpace)



カードの種類

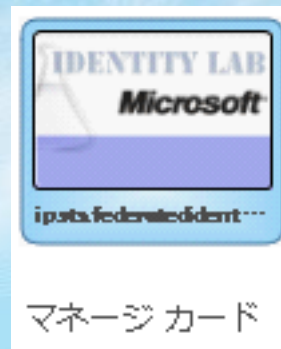
個人用カード



個人用カード

- ④ 自己署名型のカード
- ④ ローカルに保存
- ④ ユーザー名・パスワードに対する、より安全な代替手段

マネージカード



マネージカード

- ④ Identity Provider により発行
- ④ ローカルにデータは保存せず、Identity Provider から取得
- ④ STS が必要

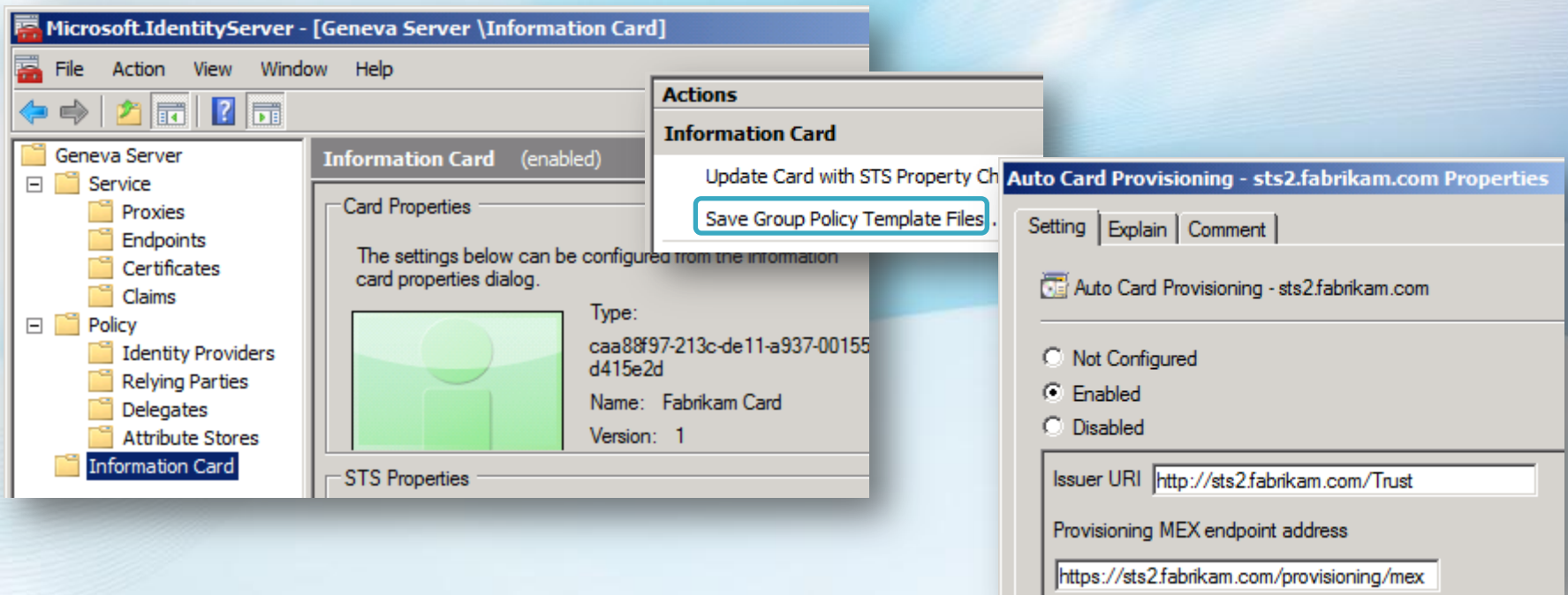
Windows CardSpace “Geneva”

[Windows CardSpace]

- ④ Windows CardSpace の次期バージョン
- ④ Beta 2 公開中 (<http://www.microsoft.com/geneva/>)
 - ④ 年内に完成予定 (Forefront ブランド)
 - ④ 7/14 正式名称発表 ([] 内が正式名称)
- ④ 特徴
 - ④ 軽量なインストーラー、セレクター
 - ④ エンタープライズシナリオにも対応
- ④ “Geneva” framework [Windows Identity Foundation]
 - ④ クレーム対応のプログラミングフレームワーク
- ④ “Geneva” server [Active Directory Federation Services]
 - ④ Active Directory フェデレーションサービスの後継
 - ④ Information Card の STS
 - ④ WS-Trust, WS-Federation
 - ④ SAML 2.0 protocol (範囲未定)

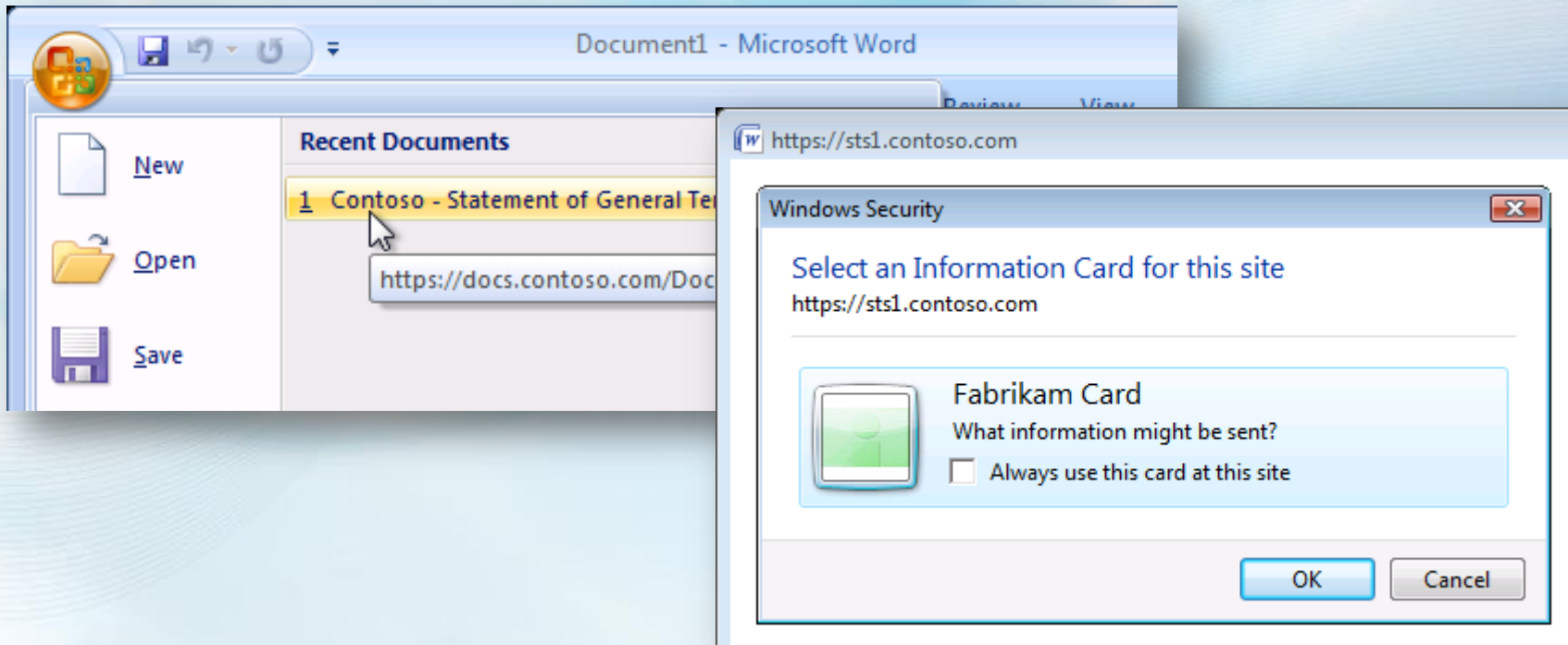
エンタープライズへの適用

- ➡ グループポリシーによる、Information Card の自動プロビジョニング
- ➡ 特定のサイトへのアクセスに自動的に使用



業務アプリケーションでの利用

- ④ Web (ブラウザ) や Web サービス (クライアントアプリケーション) で、
簡単な操作・確実な認証



事例: InfoCard プロジェクト



AAA Discount Reminders



ChoixVert Information Card



The Equifax Over 18 I-Card



The Minuteman Library Network Information Card



Student Advantage RemindMe



The U.S. General Services Administration (GSA) I-Card



WebCard Loyalty from fun communications

事例: ユーザーの確認



U.S. General Services Administration

- 検証中
- 簡単にアクセス
- 本人確認
- アクセスレベル
- フィッシングの防止

事例: 最新情報を含めた認証

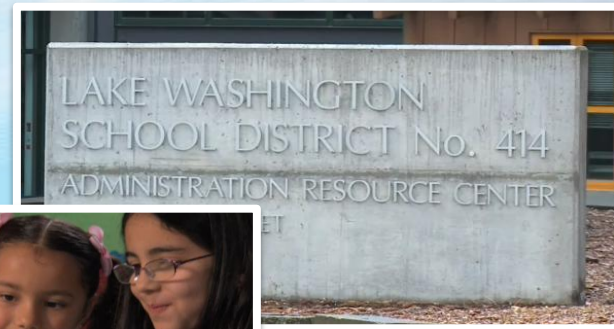
- ➡ Minuteman Library Network
- ➡ 最新在庫情報
- ➡ Azigo.com (Higgins) のセレクトタ利用
- ➡ 図書館用の情報 + 書籍情報

The screenshot shows the Amazon.com product page for the book "The Aerobics Program For Total Well-Being: Exercise, Diet, And Emotional Balance (Paperback)" by Kenneth H. Cooper. The page includes a search bar, navigation links, and product details. A blue arrow points to a "minuteman LIBRARY NETWORK" badge in the bottom left corner of the product page, which includes a "Check Catalog" button and a "No Thanks" link.

<http://informationcard.net/card-projects/minuteman>

事例: Lake Washington 学区

- ④ ワシントン州で6番目に大きい学区
50校に24,000人以上の生徒
- ④ 生徒を“Future ready”にするビジョンと、
グローバルな職場への準備
- ④ ネットブックでいつでも
どこからでも
リソースにアクセス
できる環境の整備を計画



事例: Lake Washington 学区 ユーザーとアプリケーション

- ④ さまざまなカテゴリーのユーザー
 - ④ 教職員 (スタッフ)
 - ④ 生徒、保護者 (顧客)
 - ④ Active Directory のアカウントあり
- ④ さまざまな別個のアプリケーションが数多くのベンダーから提供中 (主にクラウドベース)
 - ④ E ラーニング
 - ④ 教材
 - ④ 校務

事例: Lake Washington 学区

アプリケーションの展開

- ④ 数多くの課題: さまざまなデバイスから、いつでも、どこからでも、安全なアクセスの提供
 - ④ 認証: フェデレーションを実装するか?
 - ④ 認可: クラウドベースのアプリケーションはロールの判断のために内部システムにアクセスする必要がある
 - ④ 管理コスト (ID ライフサイクルなど)
 - ④ すべてを限られた IT スタッフでカバー
- ④ ソリューションには “In-Person-Proofing” と、クレームベースのアクセスを含む

事例: Lake Washington 学区

In Person Proofing イベント

- ⇒ 実社会の信頼関係を、オンライントランザクションの信頼性に延長
- ⇒ IPP イベントにてオンライン ID を作成
 - ⇒ 生徒と保護者が、学校に出向いて担当の職員に書類を提出
 - ⇒ 職員は本人確認、書類確認を行う
 - ⇒ 確認後マネージドのデジタル ID を発行
 - ⇒ ID は Information Card のマネージカードで生徒のコンピューターにインストールされる



事例: Lake Washington 学区

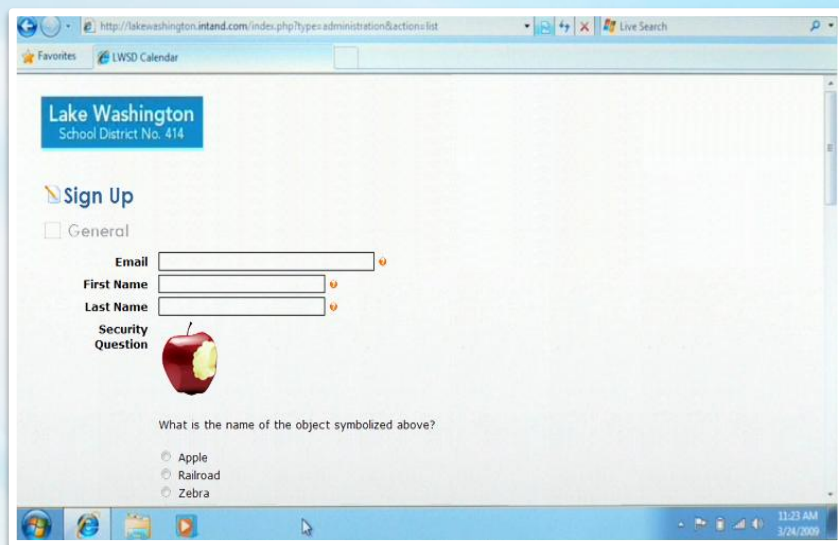
Intand's School Calendar アプリケーション

- ④ Intand 社によるアプリケーション学区にサービスとして提供
- ④ アプリケーションは、ユーザーのロールに応じてカスタマズされる
 - ④ コンテンツのカスタマイズ
 - ④ プライベートなイベントやデータの保護
 - ④ イベント作成の可・不可



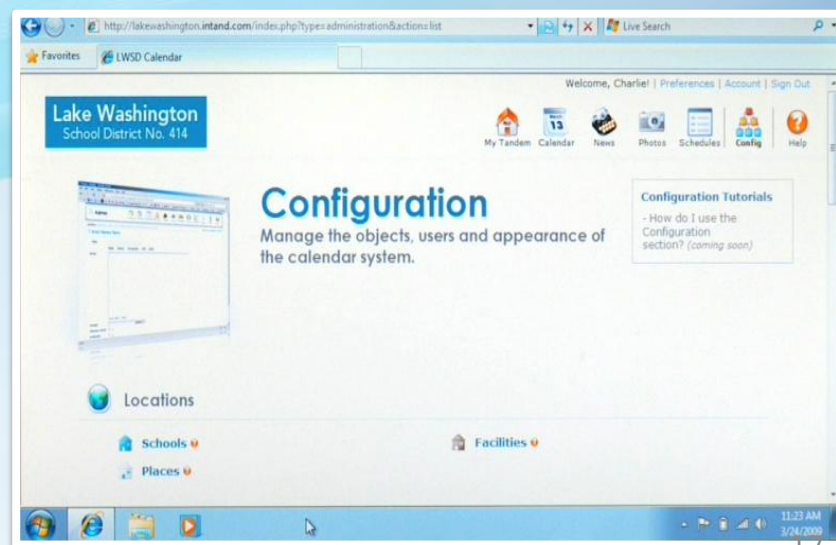
事例: Lake Washington 学区 以前のバージョン

⇒ ユーザー登録



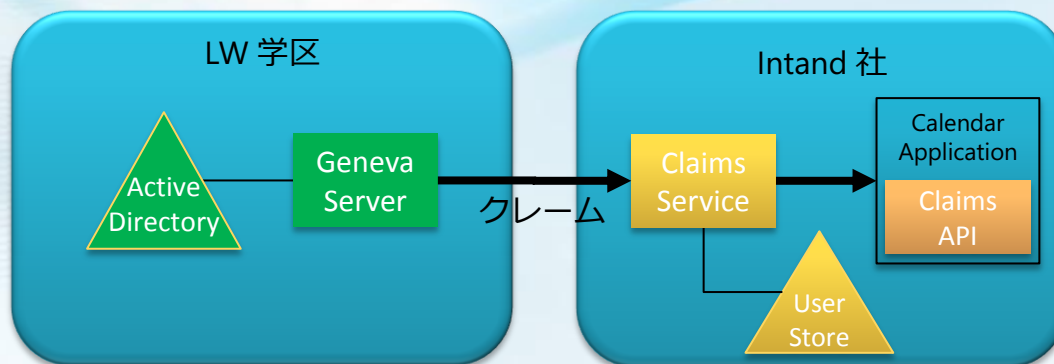
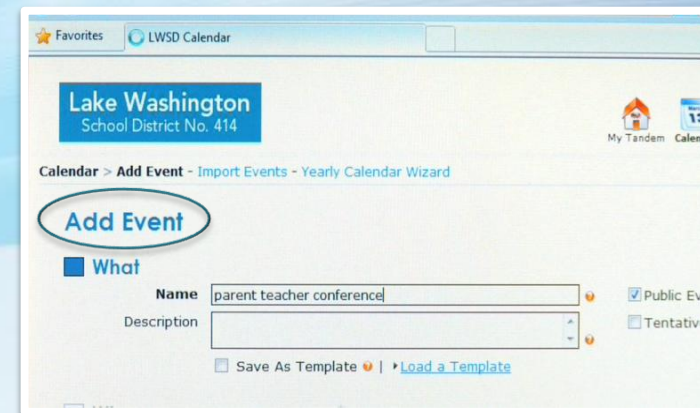
A screenshot of a web browser showing the user registration page for Lake Washington School District No. 414. The page has a blue header with the district name. Below the header, there is a "Sign Up" section with a "General" checkbox. The registration form includes fields for "Email", "First Name", and "Last Name", each with a dropdown arrow. A "Security Question" section features an image of a red apple with a bite taken out of it. Below the image, the text asks "What is the name of the object symbolized above?" and provides three radio button options: "Apple", "Railroad", and "Zebra". The browser's address bar shows the URL "http://lakewashington.intand.com/index.php?type=administration&actions=list". The Windows taskbar at the bottom shows the time as 11:23 AM on 3/24/2009.

⇒ 学校の職員が 手作業で ユーザー毎の パーミッションを設定



事例: Lake Washington 学区 クレームベースのバージョン

- ④ シングルサインオン
 - ④ Information Card でのサインオンをサポート
- ④ ロール(クレーム)ベースのアクセス制御
 - ④ 生徒、教師、職員、保護者に
応じたコンテンツ
 - ④ 個人情報全部ではなく
認可に必要な属性だけを
やり取りすればよい



まとめ

- ④ Information Card は簡単でセキュアな認証手段です
- ④ Windows CardSpace により、ユーザーの操作性も向上します
- ④ Windows CardSpace “Geneva” によりより多くの実用的なシナリオに対応
- ④ プラットフォーム・ブラウザへの対応も広がってきています
- ④ ぜひ検証をお願いします！

参考情報

参考資料 (1)

④ 情報サイト

- ④ ユーザー向けサイト (英語)

<http://www.microsoft.com/windows/products/winfamily/cardspace/default.aspx>

- ④ 開発者向けサイト (英語)

<http://msdn.microsoft.com/CardSpace>

- ④ 開発者コミュニティサイト (英語)

<http://netfx3.com/content/WindowsCardspaceHome.aspx>

- ④ Windows CardSpace の紹介

<http://www.microsoft.com/japan/msdn/net/general/IntroInfoCard.aspx>

④ ビジョンに関する文書

- ④ The Laws of Identity (英語)

<http://msdn.microsoft.com/en-us/library/ms996456.aspx>

- ④ Microsoft's Vision for an Identity Metasystem (英語)

<http://msdn.microsoft.com/en-us/library/ms996422.aspx>

④ Identity Lab

- ④ 各種 Information Card の発行、利用実験のためのサイト

- ④ <http://www.federatedidentity.net/>

④ Identity Selector Interoperability Profile

- ④ <http://download.microsoft.com/download/1/1/a/11ac6505-e4c0-4e05-987c-6f1d31855cd2/Identity-Selector-Interop-Profile-v1.pdf>

参考資料 (2)

④ 関連ブログ

④ Kim Cameron's Identity Weblogs

④ <http://identityblog.com/>

④ Windows CardSpace のアーキテクト

④ CardSpace を中心に、アイデンティティに関するさまざまな話題を取り上げている

④ CardSpace: Behind The Code

④ <http://blogs.msdn.com/card/>

④ Windows CardSpace の開発チームによる技術情報

④ Vibro.NET

④ <http://blogs.msdn.com/vbertocci/>

④ “Understanding Windows CardSpace” (Addison Wesley) の著者 Vittorio Bertocci のブログ

④ 開発者向けの、実装方法を中心としたトピック

④ Mike Jones: self-issued

④ <http://self-issued.info/>

④ CardSpace を中心に、アイデンティティの相互運用や業界動向などを幅広く取り上げている

ICF: Information Card Foundation

- ④ <http://informationcard.net>
- ④ 2008年6月発足
- ④ 参加メンバー
 - ④ Board Members
 - ④ Equifax, Google, Microsoft, Novell, Oracle, PayPal
 - ④ Launch members
 - ④ Arcot Systems, Aristotle, A.T.E. Software, BackgroundChecks.com, CORISECIO, FuGen Solutions, Fun Communications, Gemalto, IDology, IPcommerce, ooTao, Parity Communications, Ping Identity, Privo, Wave Systems, WSO2
 - ④ Fraunhofer Institute, Liberty Alliance
 - ④ Daniel Bartholomew, Sid Sidner



各種 Identity セレクター

- ⇒ Windows CardSpace を利用するもの
 - ⇒ Internet Explorer 6/7/8
 - ⇒ Firefox
 - ⇒ Identity Selector
<http://www.codeplex.com/IdentitySelector>
 - ⇒ カードの一元管理が可能、Windows のみ対応

Identity セレクター

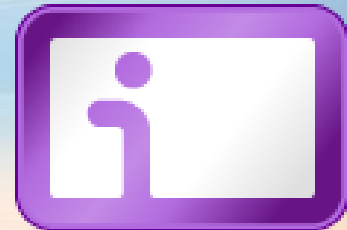
- ⇒ 独自のセレクターを利用するもの
 - ⇒ Higgins
 - ⇒ <http://www.eclipse.org/higgins/>
 - ⇒ Firefox, GTK, Cocoa, Eclipse RCP, AIR, iPhone
 - ⇒ Bandit Project
 - ⇒ <http://cards.bandit-project.org>
 - ⇒ Firefox, SuSE Linux, Mac OSX
 - ⇒ OpenCardSpace
 - ⇒ <http://code.google.com/p/openinfocard/>
 - ⇒ FireFox の組み込みセレクター
 - ⇒ Xmlldap.org のプロジェクト
 - ⇒ Infocard Selector For Safari
 - ⇒ <http://www.hccp.org/safari-plug-in.html>
 - ⇒ Mac OSX

Relying Party

- ⊕ IIS, HTML, ASP.NET 2.0:
 - ⊕ “Geneva” Framework [Microsoft Identity Foundation]
 - ⊕ クレームを扱うフレームワーク
 - ⊕ <http://www.microsoft.com/geneva/>
- ⊕ PHP: <http://www.codeplex.com/informationcardphp>
- ⊕ Java: <http://www.codeplex.com/informationcardjava>
- ⊕ Ruby: <http://www.codeplex.com/informationcardruby>
- ⊕ C: <http://www.codeplex.com/InformationCard>
- ⊕ Python: <http://code.google.com/p/py-self-issued-rp/>
- ⊕ Higgins Project
- ⊕ Bandit Project
- ⊕

Web ページへの組み込み例

- ④ Web 開発者が追加する項目
 - ④ データベースに、ユーザ ID フィールド・テーブルを追加
 - ④ ブラウザチェックのための JavaScript
 - ④ Information card のアイコンと利用条件表記
 - ④ ログインフォームに、カード対応部分を追加
 - ④ トークン処理のためのコード (“Zermatt” などのフレームワーク)
 - ④ カード管理のページ



```
<form name="Login Page" method="post">  
...  
<object type="application/x-informationcard" name="xmlToken">  
  <param name="tokenType" value="urn:oasis:names:tc:SAML:1.0:assertion">  
  <param name="requiredClaims"  
    value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier">  
</object>  
...  
</form>
```

Microsoft[®]

Your potential. Our passion.[™]

© 2009 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.