

# Windows VISTAでの スマートカード



**Microsoft®**

2007/6/25

Microsoft Consulting Services

Satoshi Kayama, CISSP

# Agenda

- はじめに
  - 用語の確認
- エンタープライズセキュリティアーキテクチャーにおけるスマートカードの位置づけ
  - シングルサインオンの課題
- ケルベロス認証におけるスマートカードの役割
- ドライバーの新アーキテクチャー概念
  - 概念図
  - 対応OSについて
- VISTA新機能のご紹介
  - OSに統合されたPIN変更機能
  - EFS証明書のスマートカード対応
    - EFS証明書の発行の方法
    - カードがない場合のファイルアクセス時のUI
  - ルート証明書の格納
  - ドライバー認定

# はじめに

—用語の確認 スマートカード:ICカード

# スマートカード : Smartcard



- アメリカを中心にICカードのことをスマートカードと呼びます。
  - ICチップ内にCPUがあり、「頭脳をもった」カードという意味からスマートカードと呼びます
- ヨーロッパ、日本ではICカードと呼びます
  - ISOの記述などでもICカードを ICC=IC Cardとなっています。
- マイクロソフトはアメリカの会社であるため、ICカードといわずスマートカードと呼んでいます
- 本セミナーでも、ICカードとスマートカードは同じ意味で表現します。
  - ISO7816：接触式ICカードをベースとします。



# エンタープライズセキュリティにおける PKI / スマートカードの位置づけ

# 2つのCIA

## ● セキュリティのCIA

- C・・・Confidentiality (機密性)
- I・・・Integrity (完全性)
- A・・・Availability (可用性)

## ● PKIのCIA

- C・・・Confidentiality (機密性)
- I・・・Integrity (完全性)
- A・・・Authentication (認証)



# ひとつの要素技術で3大要素に対応

## セキュリティ3大要素

Confidential

Integrity

Available

Confidential

機密性の例

EFS S/MIME

IPSec

認証後のアクセス制御

SSL認証後の通信

Integrity

署名の例

S/MIME MS-WORD

認証要求データの署名

Authentication

認証の例

SSL認証,

スマートカードログオン

ワイヤレスLAN認証

IPSec

PKI3大要素



交通費の清算と確認

出張申請  
稟議申請

座席表と顔写真の確認  
電話番号の確認

給与明細の  
Web閲覧

専門分野での仲間集め  
キーマンの確認

ワイヤレスLANによる会議室でのネット接続(メール確認や会議内容の速報)

ADにログオン

(社員と確認されたら)

会議開催通知と会議室予約

作成したドキュメントのアクセス権の設定

部門で共有すべきデータの提出  
(部門内のみ閲覧可能)

ICカードを利用したVPN接続による社外からのデータアクセス

人事考課の入力・閲覧

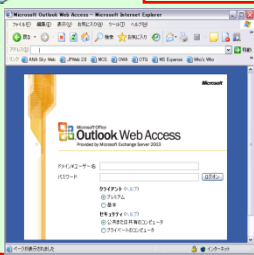
社外からは

社外Webからのメール確認(OWA)

Windows Mobile

メール確認

すべてのシステムの本人確認  
Active Directoryを利用



# シングルサインオンの整理

- 一度の認証でネットワーク資源を網羅的にアクセスする手段
  - メリット
    - ユーザはパスワードをひとつだけ記憶すればよい
  - デメリット: リスク
    - 単一障害ポイント(論理的)
      - パスワードが不正利用されるとネットワーク全体に被害が及ぶ

デメリットが転じて・・・単一「監視」ポイントになるメリットに  
最初の認証を強化することが全体のセキュリティ向上につながる



# シングルサインオン環境における 認証強化の必要性

- シングルサインオンのリスクを低減するため、初期の認証を二重化
  - 2因子認証 (Two factor authentication)
- アカウンタビリティ
  - ネットワーク上の行為について、自分が実施したことを確実に主張できる
    - ルールに則ったこと以外はしていない
  - セキュリティ・コンプライアンスの前提

# お城の守り方とシングルサインオン

単一監視ポイント



単一障害ポイント

# 生産性原則とセキュリティ原則の確認



本人  
確認

ICカードにも  
CPUとOSが実装

情報共有

ファイル共有、ポータルサイトなど

一元管理

AD環境、アカウントの集約

知識分離

Windows外のOSに本人確認情報を格納

二重管理

カード(証明書)所有とPINの記憶

# ケルベロス認証での スマートカードの役割

## ～Windows上の代表的PKIアプリケーション

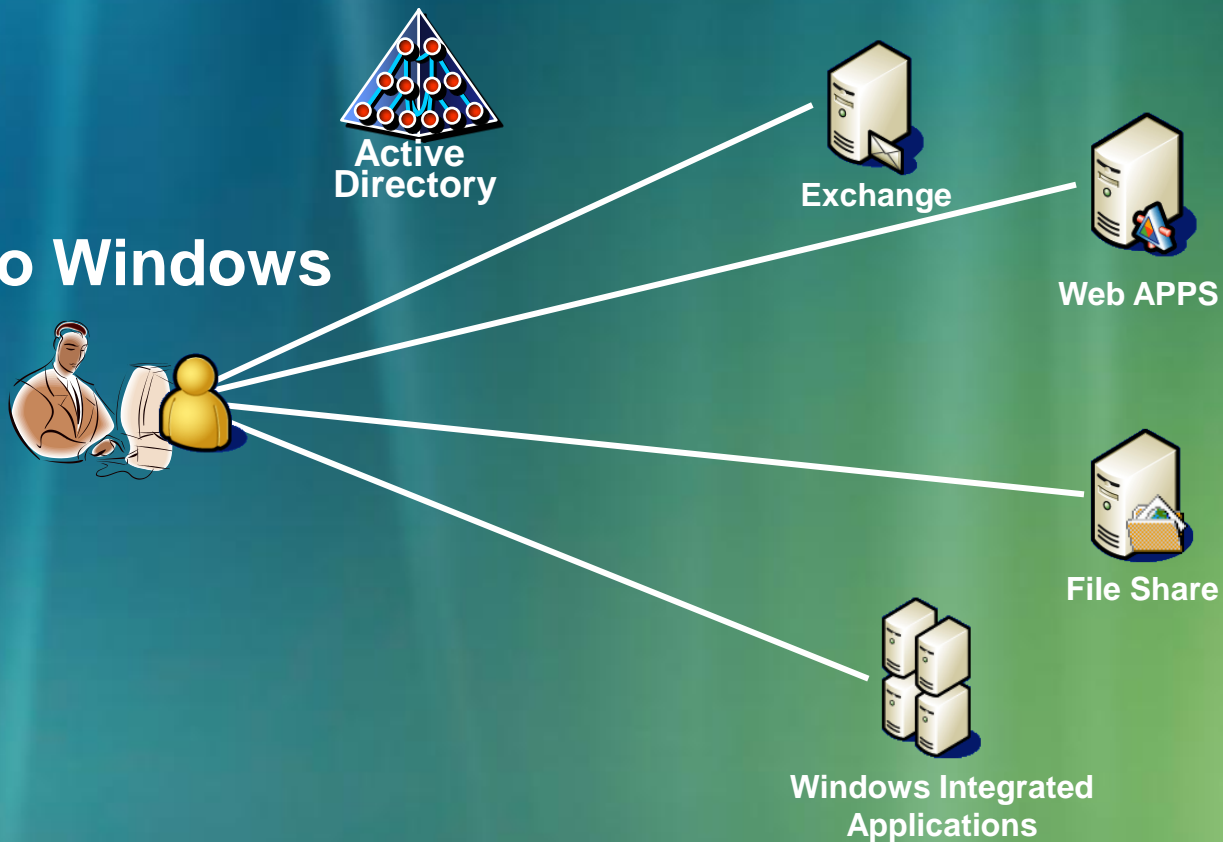
ケルベロス認証：  
ギリシャ神話に出てくる黄泉の国の入口を守る  
3つの頭をもつ番犬の名前であるから転じて





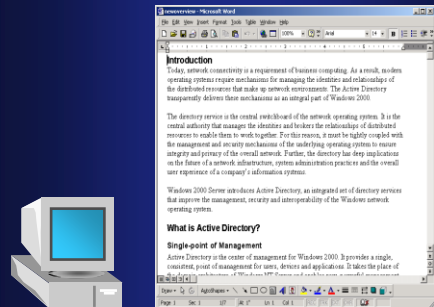
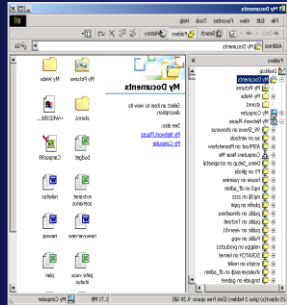
# Active Directory環境での シングルサインオン 概念

Logon to Windows



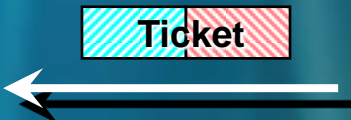


# ケルベロス認証の基本



クライアント

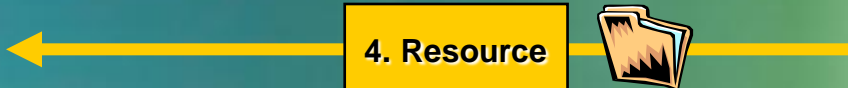
1. ドメイン  
コントローラー  
認証



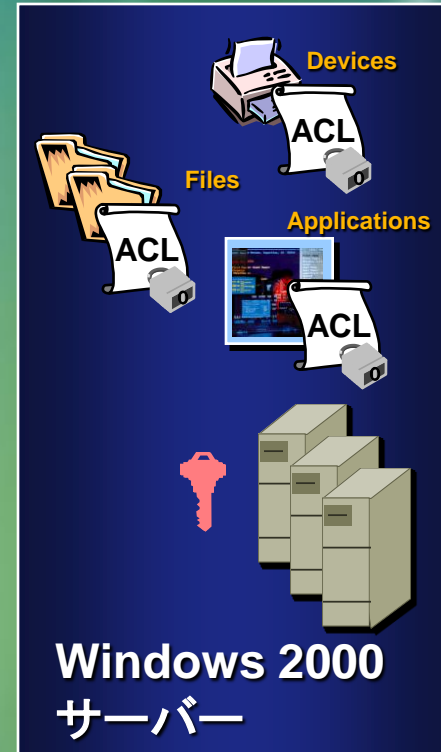
2. クライアントへ  
チケットを付与

(認可)

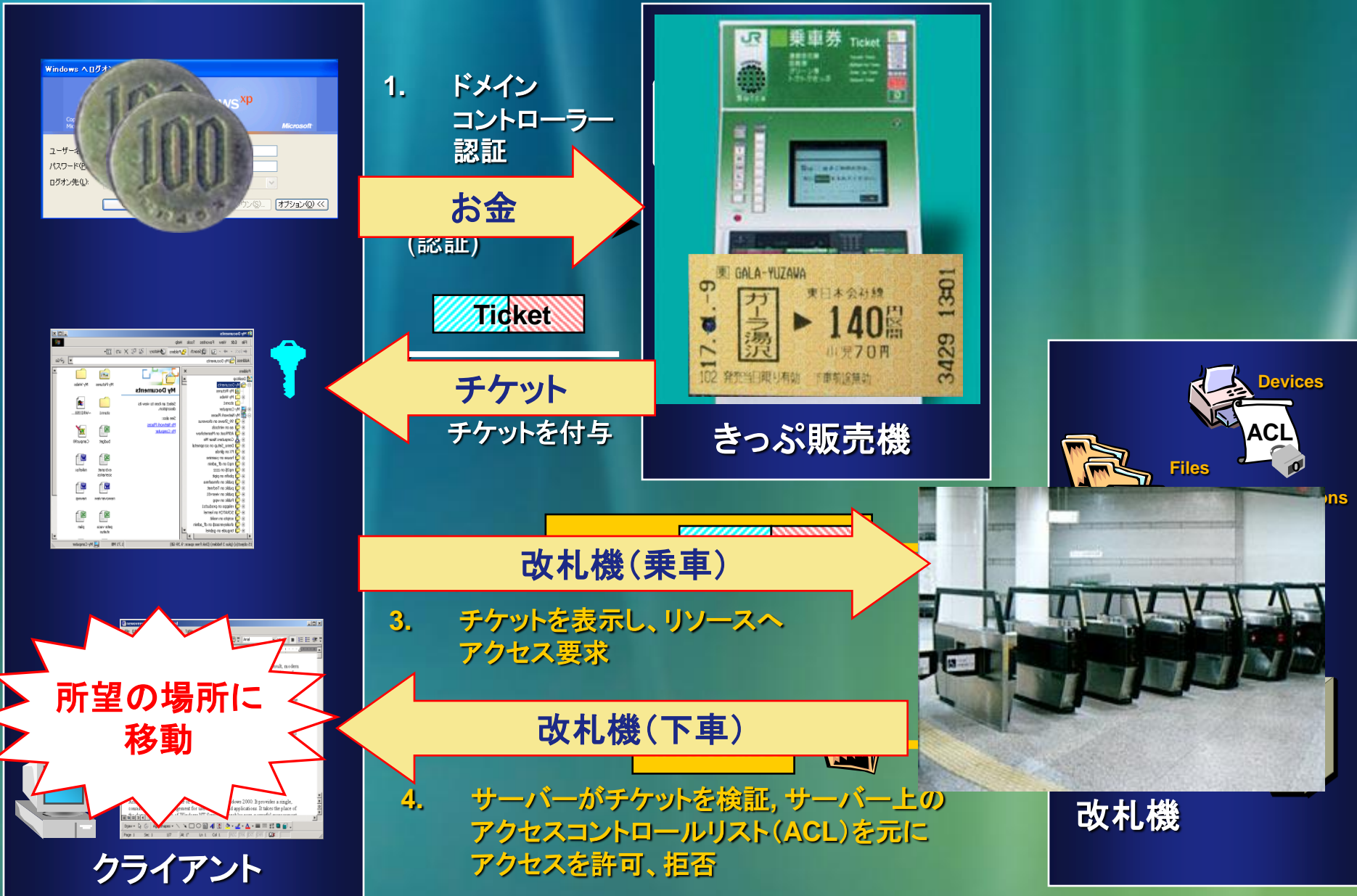
3. チケットを表示し、リソースへ  
アクセス要求



4. サーバーがチケットを検証、サーバー上の  
アクセスコントロールリスト(ACL)を元に  
アクセスを許可、拒否



# 切符, 券売機, 自動改札機の利用で比喻すると・



# スマートカードログオンは・・・



1. ドメイン  
コントローラー  
認証

お金と南京錠  
(認証)

Ticket

施錠されたキップ  
チケットを付与

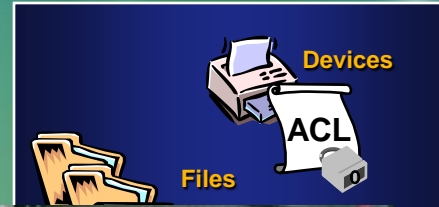
きっぷ販売機

改札機(乗車)

3. チケットを表示し、リソースへ  
アクセス要求

改札機(下車)

4. サーバーがチケットを検証、サーバー上の  
アクセスコントロールリスト(ACL)を元に  
アクセスを許可、拒否



改札機



# 技術仕様

- Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)
- <http://www.ietf.org/rfc/rfc4556.txt>

# VISTAのスマートカード 「変わること」 「変わらないこと」



# Windowsとスマートカードの関係

- スマートカードは電子証明書と秘密鍵のストアの位置づけ 変わらないこと
- ~~カードベンダーのCSPを必要とします~~

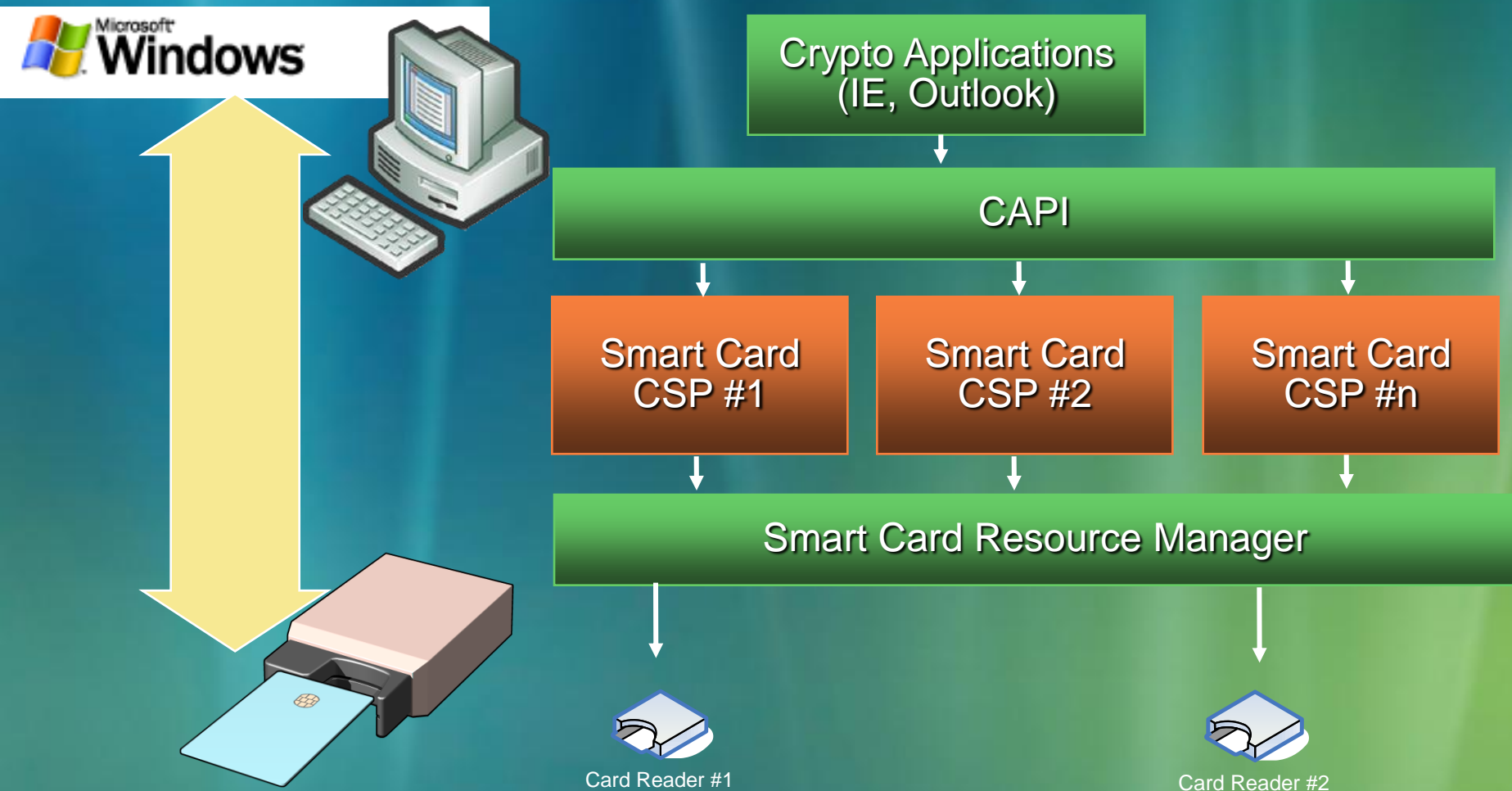


変わること  
CSP  
WindowとICチップ間の  
通信を行う

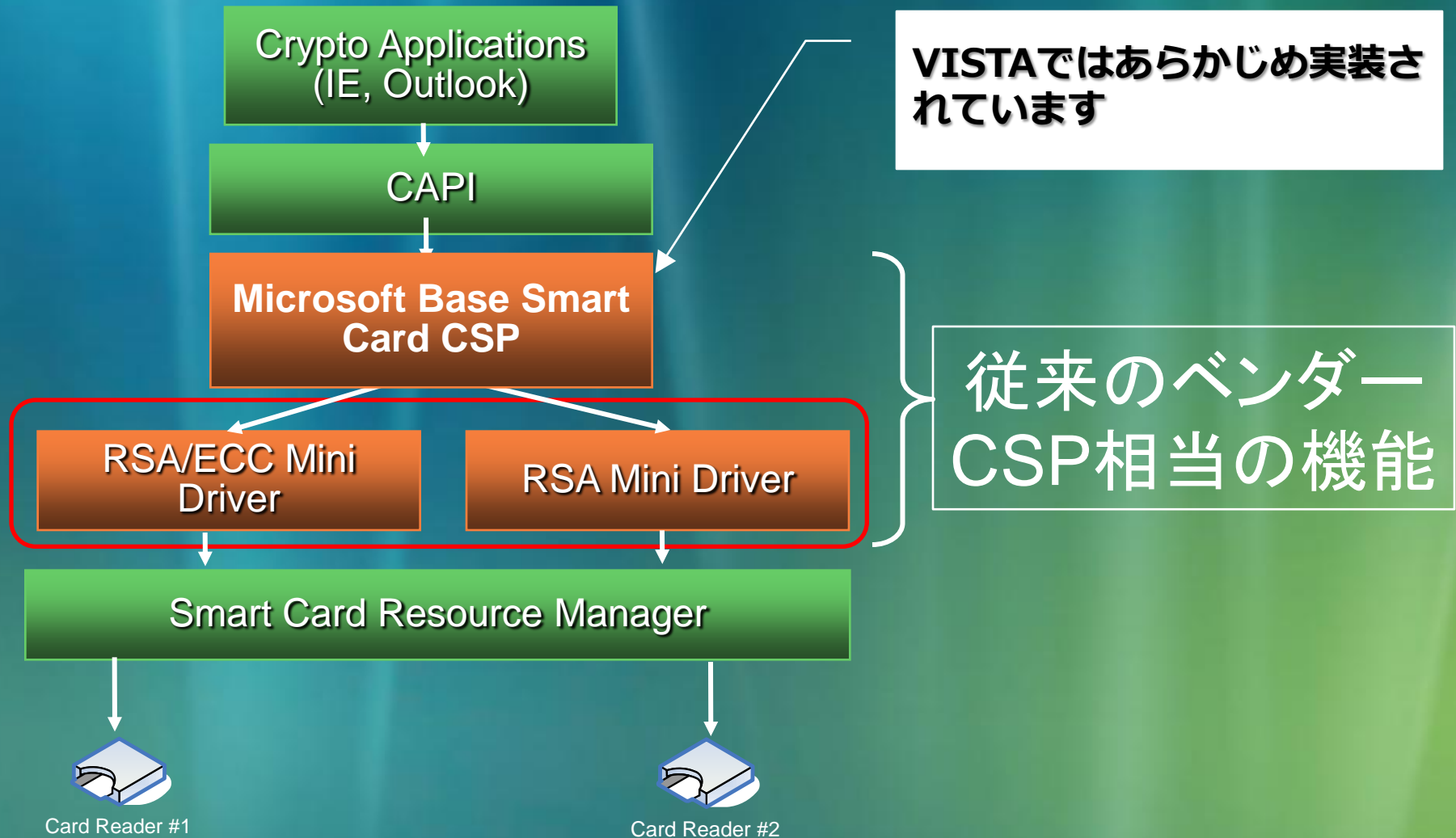
A screenshot of the Windows Certificate Manager window titled '証明書'. The window shows a list of certificates under the '個人' (Personal) tab. The selected certificate is issued to 'Satoshi Kayama' by 'Microsoft Intranet Le...'. The '目的' (Intended purposes) field is circled in red and contains the text 'スマートカード ログオン クライアント認証'. A red arrow points from the '変わること' text in the bottom left to this circled text. To the right of the window is an illustration of a desktop computer with a monitor, keyboard, and mouse.

発行先	発行者	有効期限	フレンド
Satoshi Kayama	Microsoft Personnel ...	2008/04/...	<なし>
Satoshi Kayama	Microsoft Corp Enter...	2008/04/...	<なし>
Satoshi Kayama	Microsoft Intranet Le...	2008/03/...	<な

# XP, 2000までのアーキテクチャー



# VISTA以降のアーキテクチャー



# 新旧ドライバーのカバー範囲

VISTAの新機能



XPまでのSmartcard機能



**Microsoft**  
**Base Smart Card CSP**  
(ダウンロードセンタ)KB909520

Mini Driver

Smart Card  
CSP

# インストール対象OSについて

- 旧Smartcard CSP はVISTAにインストール可能
  - ただし、VISTAの新機能は使えずXPの機能のみ
- MS Base CSP + Mini DriverはVISTAだけでなく、XP,2000,2003にもインストール可能
  - ただし、そのOSの持つ機能が適用されるのみ
    - スマートカード利用のEFSやOSからのPIN変更はできない
  - **サポートされているオペレーティング システム**
    - Windows 2000 Service Pack 4;
    - Windows Server 2003;
    - Windows XP Service Pack 1;
    - Windows XP Service Pack 2
    - Windows Server 2003 Service Pack 1



# インストール対象 補足

- 各ドライバーは相互にインストール可能
- ただし、OS,ドライバーの機能範囲での動作

Microsoft  
Base Smart Card CSP  
(ダウンロードセンタ)KB909520

Mini Driver

Smart Card CSP

VISTA



Windows Vista

XP



# Mini Driverの動作例

## Smart Card CSP

### スマート カード 証明書の登録ステーション

#### 登録のオプション:

証明書テンプレート: スマート カード ユーザー  
証明機関: MSCA  
暗号化サービスプロバイダ: Schlumberger Cryptogra  
管理者の署名証明書: Administrator

#### スマート カードの PIN の確認

暗証番号 (PIN) を入力してください(P)

確認後 PIN を変更する(C)

OK

キャンセル

Schlumberger

## Microsoft Base Smart Card CSP

### スマート カード 証明書の登録ステーション

#### 登録のオプション:

証明書テンプレート: スマート カード ユーザー  
証明機関: MSCA  
暗号化サービスプロバイダ: Microsoft Base Smart C  
管理者の署名証明書: Administrator

#### 登録するユーザー:

Paul@skayama01.private

ユーザーの選択

#### スマート カードの暗証番号 (PIN)



暗証番号(P):

OK

キャンセル

# 新機能の紹介

# ログイン先頭画面の変化 -PIN入力の方法の改善

# ログオン画面の変化 XP

- PC/SC規格のICカード読取装置がWindowsで認識され、Scardsvrと呼ばれるサービスが稼動している環境では自動的に以下のように表示が変更されます



このキーの組み合わせを使用すること  
詳細は [ヘルプ] を参照してください。





# VISTAのログオン画面

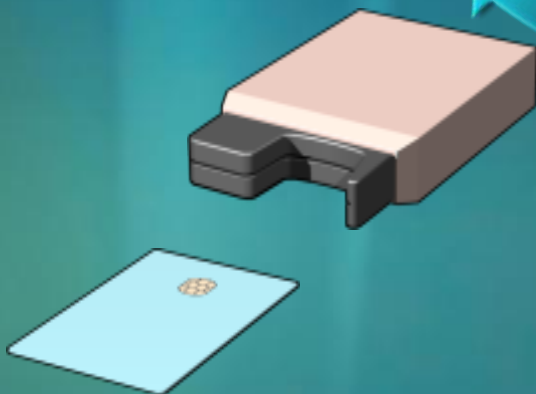


# XPまでのPIN入力

- スマートカードの挿入動作でPIN入力画面に推移



操作ミスをする  
とカードを一度抜い  
て、再度セットし  
なければならない



# VISTAのPIN入力画面の変化

マウスクリックでPIN入力画面に推移



# PIN（暗証番号）変更 OSメニュー統合



# OSメニューからの暗証番号変更



パスワード変更画面

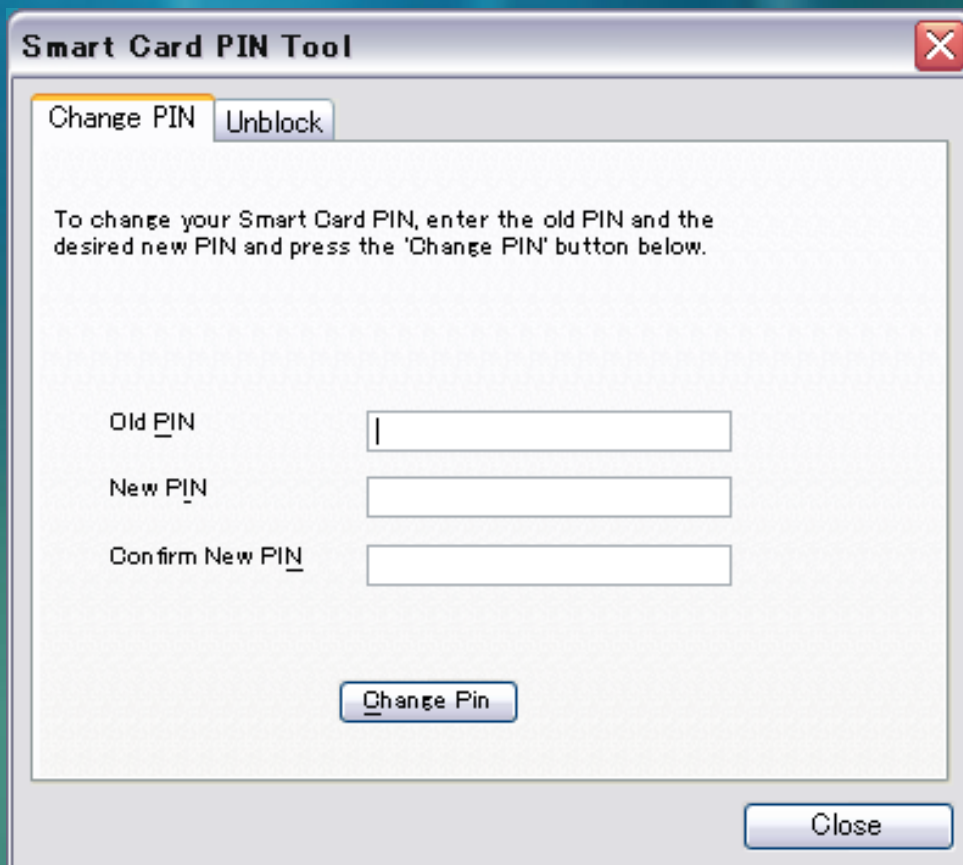


PIN 変更画面



# 従来の暗証番号変更ツール

- スマートカードベンダーが独自に開発し、PIN変更ツール配布が必要だった



The image shows a screenshot of a Windows-style dialog box titled "Smart Card PIN Tool". The dialog has a close button (X) in the top right corner. Inside the dialog, there are two tabs: "Change PIN" (which is selected) and "Unblock". Below the tabs, there is a text instruction: "To change your Smart Card PIN, enter the old PIN and the desired new PIN and press the 'Change PIN' button below." There are three input fields: "Old PIN", "New PIN", and "Confirm New PIN". Below these fields is a "Change Pin" button. At the bottom right of the dialog is a "Close" button.

MSのPIN 変更画面

# スマートカードログオン証明書 複数格納

# 複数ユーザのログオン対応



LONGHORN B3¥billg



他のユーザー



Steve Ballmer  
スマートカード ログオン



Bill Gates  
スマートカード ログオン

キャンセル

# 想定される活用例

- 日米欧など国別ドメインへのログオン
  - グローバル企業
  - 事業部、分社化された環境への対応
- 「管理者」としての作業、「一般ユーザ」としての作業の切換え
- ✓ スマートカードのPINは共通なので、あくまで同じユーザに用途別に複数証明書を発行した場合の利用を前提

# EFS証明書 スマートカード格納

EFS・・・Encrypted File System

暗号化ファイルシステム

Windows2000以降の機能、NTFSフォーマットが条件



# EFSのスマートカード対応

The screenshot shows a Windows XP user account control dialog box titled "暗号化ファイル システム" (Encrypted File System). The dialog is open over a user account page for "Bill Gates". The user account page has a sidebar with navigation links: "タスク" (Tasks), "ネットワークパスワードの管理" (Manage network passwords), "ファイル暗号化証明書の管理" (Manage file encryption certificates), "ユーザー プロファイルの詳細 プロパティの構成" (Configure user profile details properties), and "環境変数の変更" (Change environment variables). The "ファイル暗号化証明書の管理" link is highlighted with a red box. The dialog box contains the following text and options:

暗号化ファイル システム

ファイル暗号化の証明書の選択または作成

既存のファイル暗号化の証明書を選択するか新しい証明書を選択してください。暗号化されたファイルが既にある場合は、この証明書を使用してファイルを更新することができます。

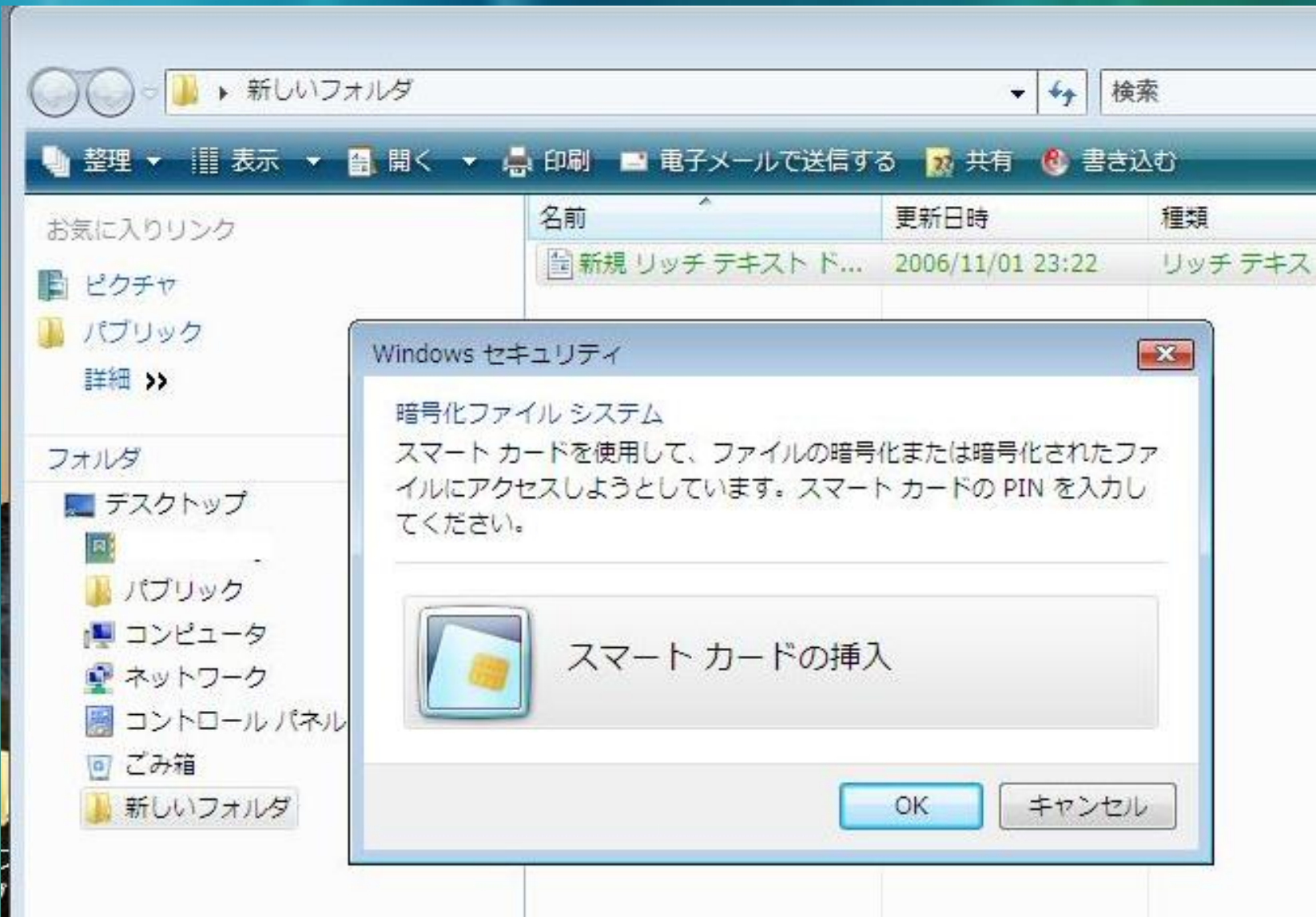
この証明書を使用する(U)  
スマート カードを使用している場合は、スマート カード上の証明書を選択してください。

証明書の詳細(D):

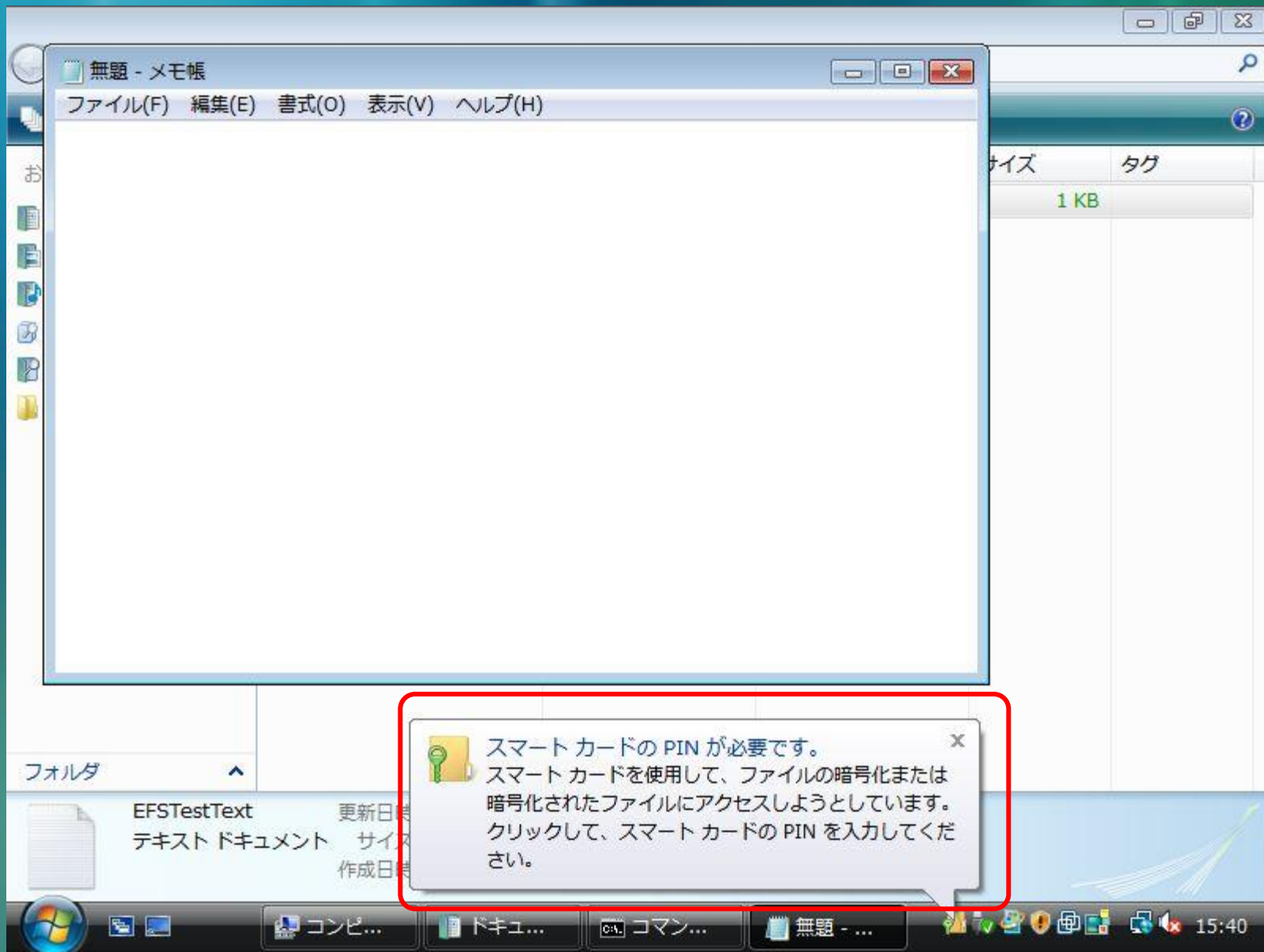
発行先: Bill Gates
発行者: MSCA2008
有効期限: 2008/06/01

新しい証明書を作成する(C)

# EFSファイルアクセス時 スマートカードがない場合のUI



# EFSファイルアクセス時 スマートカードがない場合のUI



# EFSスマートカード対応の意義

- 知識分離・二重管理の原則
  - PCとスマートカードを同時に紛失・盗難しな  
いかぎり安全・・・
- PINを規定回数間違えるとスマートカード  
の機能設定によりロックをかけることが  
できる
  - オフライン環境での安全性の向上
- 1人が複数台PCを利用する場合EFSファイ  
ルのローミングが可能になる



# ルート証明書 スマートカード格納

# 拡張された証明書ストア

The screenshot shows the Windows Certificate Manager application. The left pane displays a tree view of certificate stores. The 'Smart Card Trusted Root Certificates' folder is highlighted with a red box. An arrow points from this box to a text box on the right. The right pane shows a table of certificates in the selected store.

発行先	発行者	有効期限
Microsoft Corporate Root CA	Microsoft Corporate Root CA	20...

**スマートカード用に  
新しく定義された  
証明書ストア**

# ルート証明書格納コマンド

```
C:¥Users¥skayama>certutil -scroots -?
```

使用法:

```
CertUtil [オプション] -SCRoots update [+][入ルートファイル] [読み取り装置名]
```

```
CertUtil [オプション] -SCRoots save @ 出ルートファイル [読み取り装置名]
```

```
CertUtil [オプション] -SCRoots view [入ルートファイル | 読み取り装置名]
```

```
CertUtil [オプション] -SCRoots delete [読み取り装置名]
```

スマートカード ルート証明書の管理

# コマンドの適用例

The screenshot shows a Windows command prompt window titled "コマンド プロンプト - certutil -Scroots update MSIT.cer". The window displays the help text for the 'certutil' command, including options like '-f', '-gmt', '-seconds', '-split', '-v', '-privatekey', and '-p'. A dialog box titled "スマートカードの暗証番号 (PIN)" is overlaid on the command prompt, with a red box around the "ルート証明書の提供" (Provide root certificate) option. The dialog box also has a text input field for the PIN and "OK" and "キャンセル" (Cancel) buttons. Below the dialog box, the command prompt shows the execution of the command: "C:\Users\john\Desktop>certutil -Scroots update MSIT.cer". The output of the command is displayed below the command line, showing details of the root certificate update, including the serial number, issuer, validity dates, subject, CA version, and SHA1 hash. A red box highlights the output text.

```
certutil [オプション] -Scroots view [入力ルートファイル | 読み取り装置名]
certutil [オプション] -Scroots delete [読み取り装置名]
スマートカード ルート証明書の管理

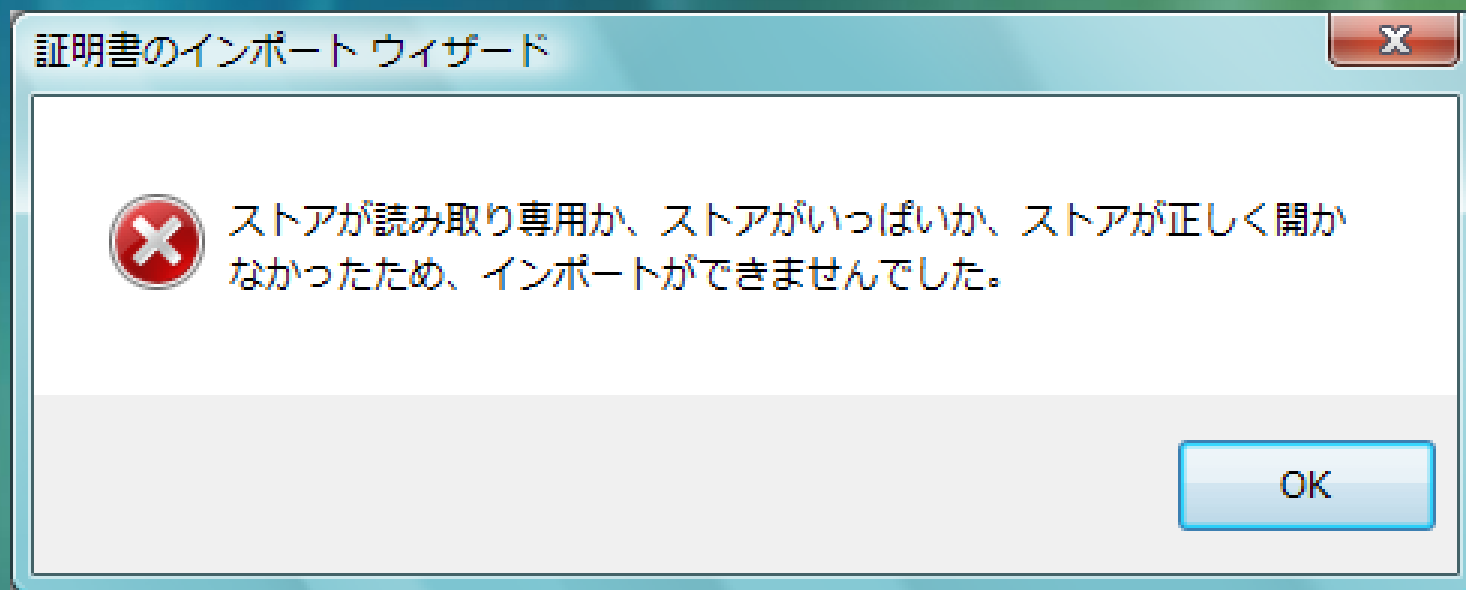
オプション:
-f          -- 強制的に上書きします
-gmt       -- 時刻を GMT で表示
-seconds   -- 時間を秒とミリ秒
-split     -- 埋め込まれた ASN
-v         -- メッセージを詳細
-privatekey -- 秘密キーのデータ
-p パスワード -- パスワード

certutil -?          -- 動詞の一覧
certutil -Scroots -? -- "Scroots" 重
certutil -v -?      -- すべての動詞

C:\Users\john\Desktop>certutil -Scroots update MSIT.cer
要素 0:
シリアル番号: 443c2a54b59cd69d4c09b18a9b02eb55
発行者: CN=Microsoft Corporate Root CA, O=Microsoft Corporation
この日以降: 2003/09/20 4:21
この日以前: 2019/09/20 4:28
サブジェクト: CN=Microsoft Corporate Root CA, O=Microsoft Corporation
CA バージョン: V0.0
署名は公開キーと一致します
ルート証明書: サブジェクトと発行者は一致します
Cert ハッシュ(sha1): d2 d3 8e ba 60 ca a1 c1 20 55 a2 e1 c8 3b 15 ad 45 01 10 c2
```

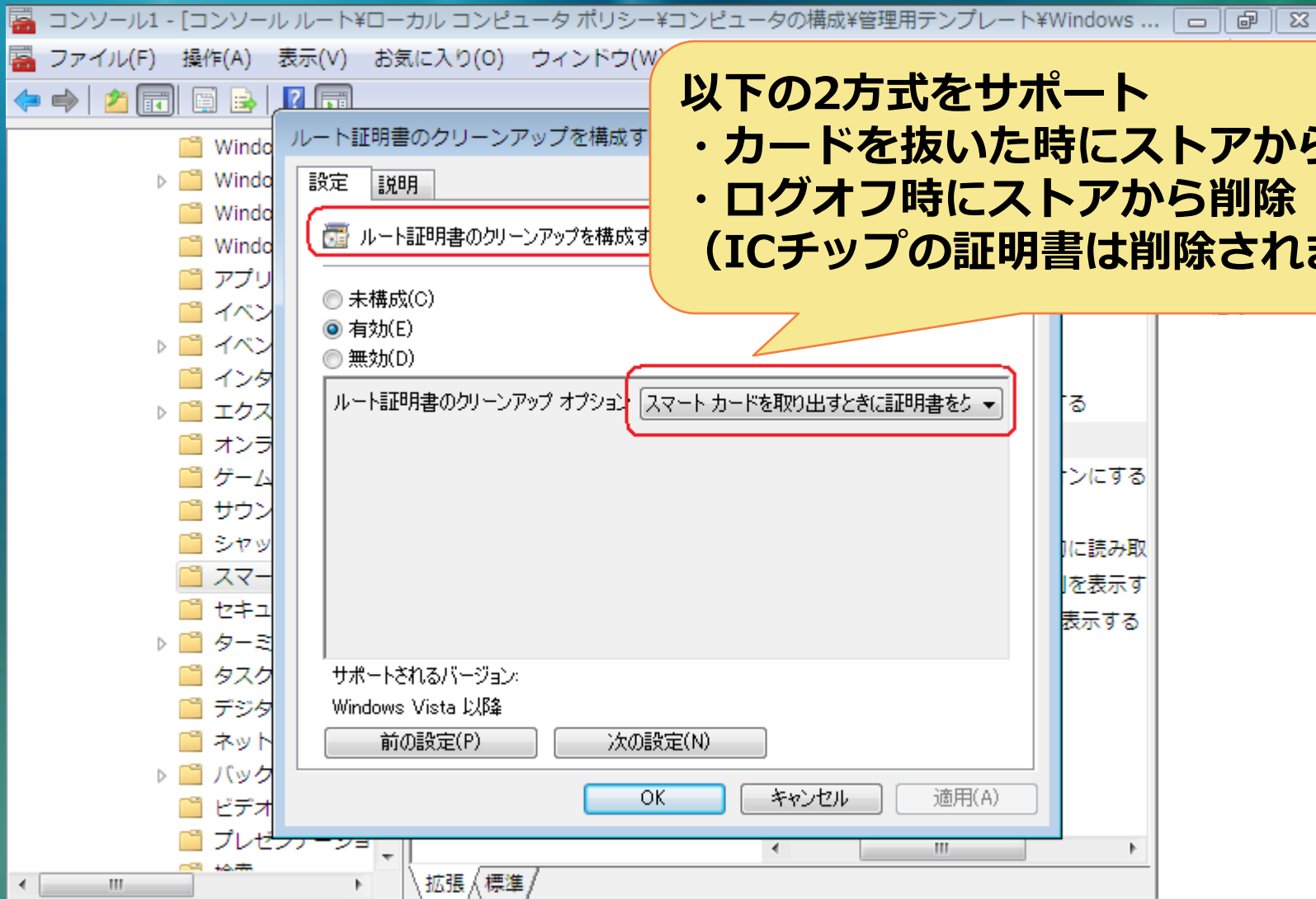
# ファイルからルート証明書の インポート結果

- スマートカードではなく、ファイルから手動操作でルート証明書をインポートしたときのエラーメッセージ
  - スマートカード以外からのインポートは禁止されています





# スマートカードの信頼されたルート証明書 ストアからのクリーンアップ方法



以下の2方式をサポート

- ・ カードを抜いた時にストアから削除
- ・ ログオフ時にストアから削除  
(ICチップの証明書は削除されません)

# ルート証明書 スマートカード格納の意義

- ルート証明書をスマートカードに格納できるので  
証明書の検証がオンスポットで可能
  - カードを抜くことでルート証明書のクリーンアップも可能
- セキュリティ媒体でのルート証明書配布
  - 電子デバイスの特性を生かしたルート証明書の配布と保護

# Mini Driver

## ドライバー認定の予定

# ドライバー認定

- 従来のCSPはMSへ署名される必要があった。これは暗号製品の管理が趣旨
  - 周辺機器(NICやプリンタ等) のドライバ署名とは性格が異なっていた。
- 新しいアーキテクチャーである Mini Driver を対象として2007年秋をメドにドライバ認定スキームが決定

# ドライバー認定されると…

- 動作認定ではなく、関数レベルのアタックをチェック（他のソフトに影響を与えないことを認定）
- インストール時の警告が表示されない
- Windows Update によりインターネット経由で mini driver のダウンロード可能
  - インターネットに接続できる環境で、カードをセットしたとき、対応するmini Driver がない場合自動でダウンロードされる（予定）
  - Windows Update にmini Driver を登録するかどうかはカードベンダーの選択



# 参考資料

- スマート カード ミニドライバの認定要件
  - [http://www.microsoft.com/japan/whdc/device/input/smartcard/sc-minidriver\\_certreqs.mspx](http://www.microsoft.com/japan/whdc/device/input/smartcard/sc-minidriver_certreqs.mspx)
- Windows Logo Program Requirements V. 3.0(mini-driver要件は、次のバージョンに含まれる予定)
  - <http://www.microsoft.com/japan/whdc/winlogo/hwrequirements.mspx>

# ***Microsoft***<sup>®</sup>

*Your potential. Our passion.*<sup>™</sup>

© 2006 Microsoft Corporation. All rights reserved.

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.