Windows VISTAでのスマートカード

Microsoft®

2007/6/25

Microsoft Consulting Services
Satoshi Kayama,CISSP

Windows Vista™

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

ー用語の確認 スマートカード:ICカード

スマートカード :Smartcard

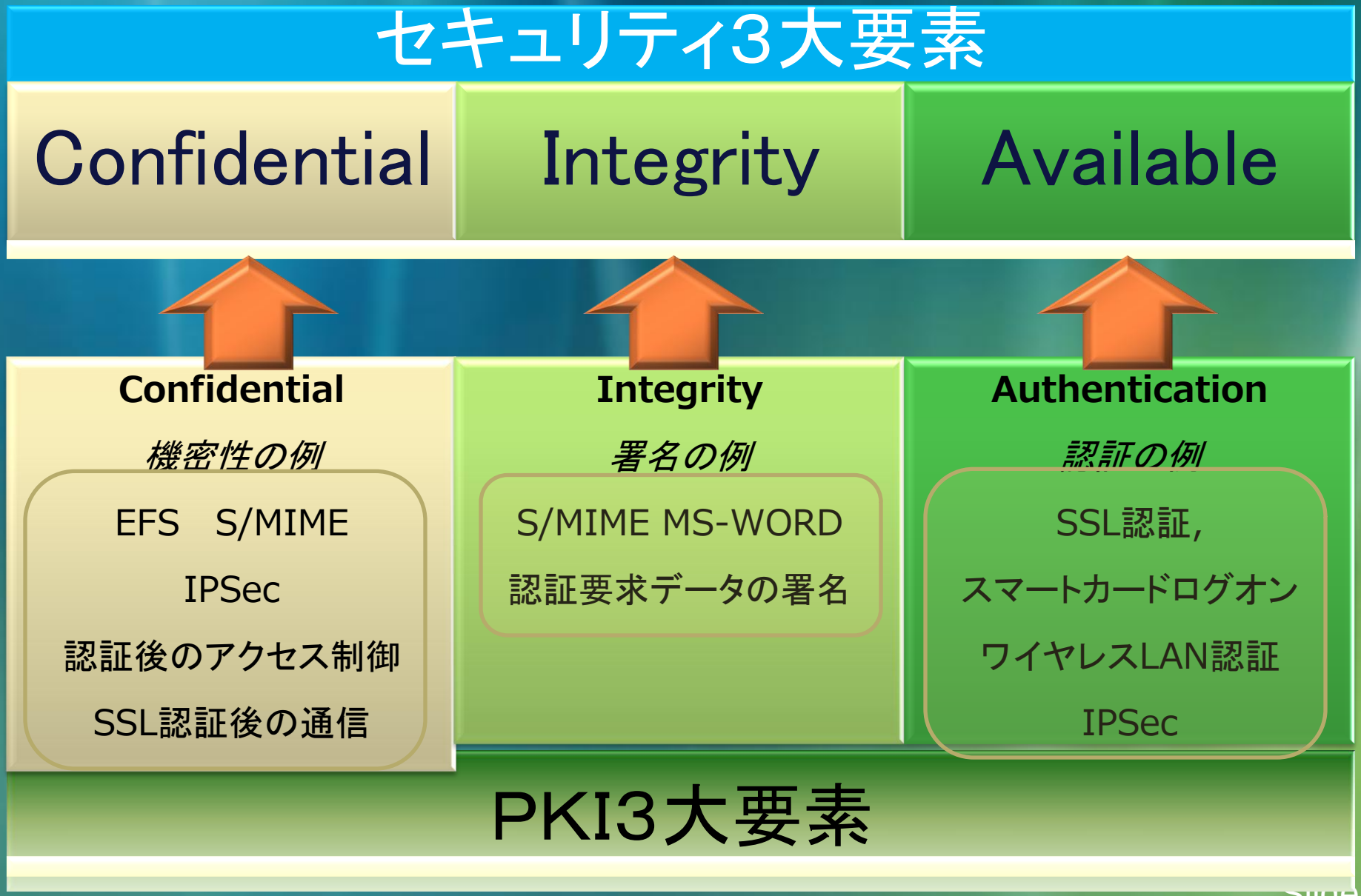
- アメリカを中心にICカードのことをスマートカードと呼びます。
  - ICチップ内にCPUがあり、「頭脳をもった」カードという意味からスマートカードと呼びます
- ヨーロッパ、日本ではICカードと呼びます
  - ISOの記述などでもICカードを　ICC＝IC　Cardとなっています。
- マイクロソフトはアメリカの会社であるため、ICカードといわずスマートカードと呼んでいます
- 本セミナーでも、ICカードとスマートカードは同じ意味で表現します。
  - ISO7816：接触式ICカードをベースとします。

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

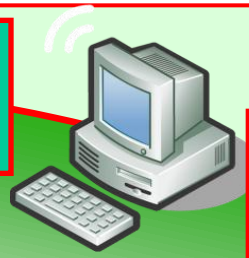


マイクロソフト内での利用可能なサービス　主な例

Microsoft

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

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

部門で共有すべき
データの提出
(部門内のみ閲覧可能)

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

Windows Active Directory

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

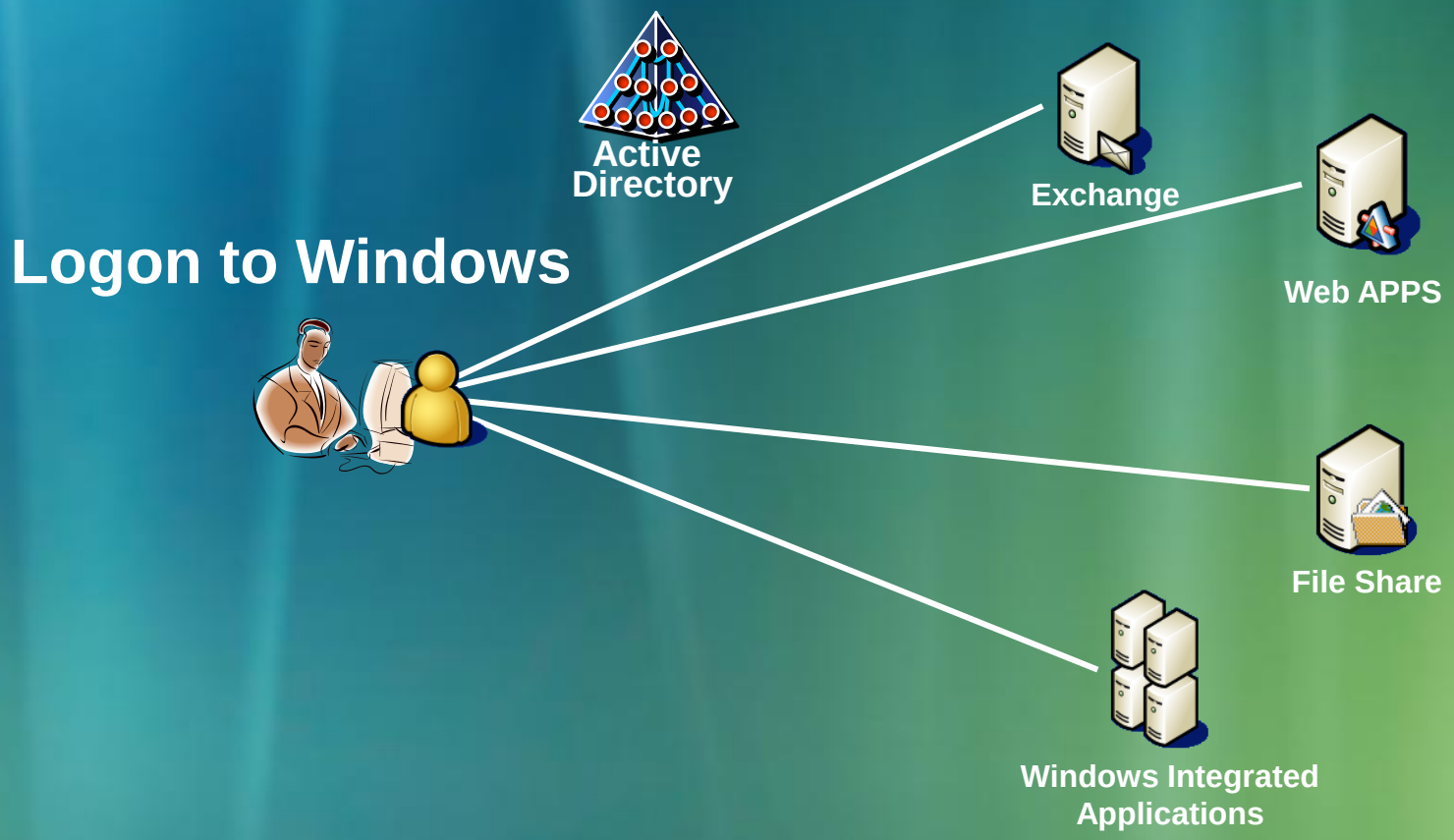
カード（証明書）所有とPINの記憶

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

T16.2 Herakles, Kerberos, Hekate

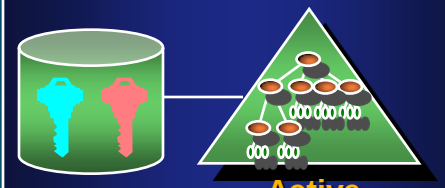
Active Directory環境でのシングルサインオン 概念



ケルベロス認証の基本

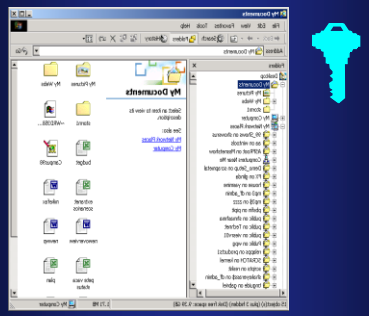
1. ドメイン コントローラー 認証

(認証)

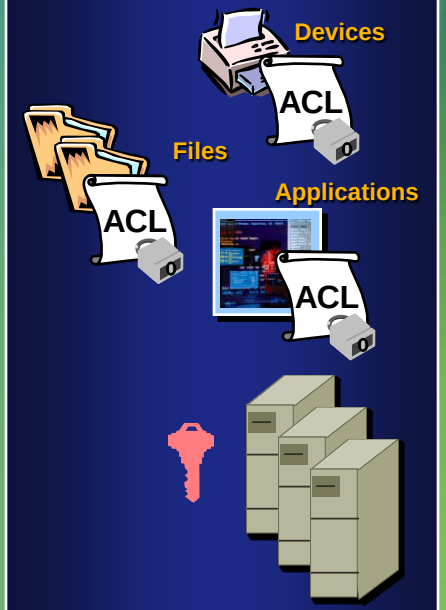


Windows 2000 ドメインコントローラー

Ticket



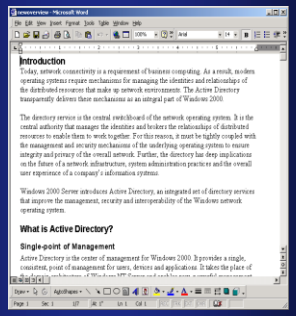
2. クライアントへ チケットを付与



Request Ticket

(認可)

3. チケットを表示し、リソースへ アクセス要求



4. Resource

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

クライアント

Windows 2000 サーバー

切符,券売機,自動改札機の利用で比喩すると・

1. ドメイン コントローラー 認証

お金

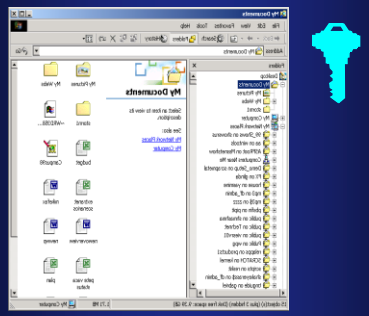
(認証)

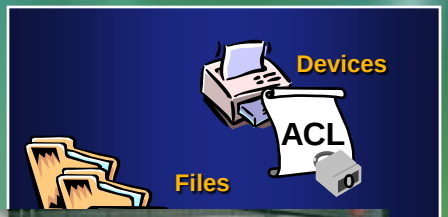
きっぷ販売機

Ticket

チケット

チケットを付与





改札機(乗車)

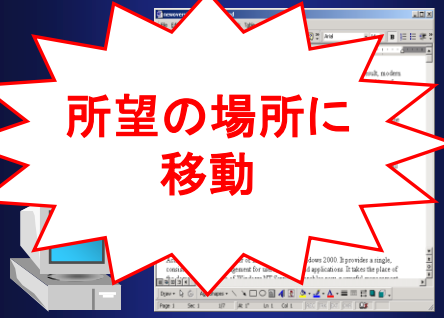
3. チケットを表示し、リソースへ アクセス要求

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

所望の場所に 移動



クライアント

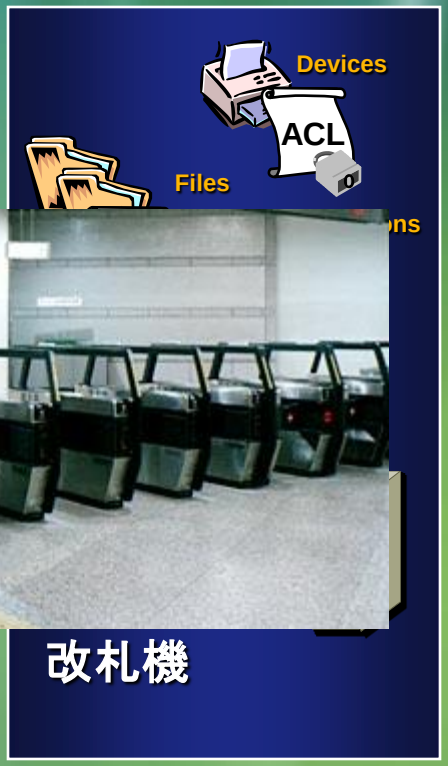
スマートカードログオンは・・・

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



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

所望の場所に移動

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」

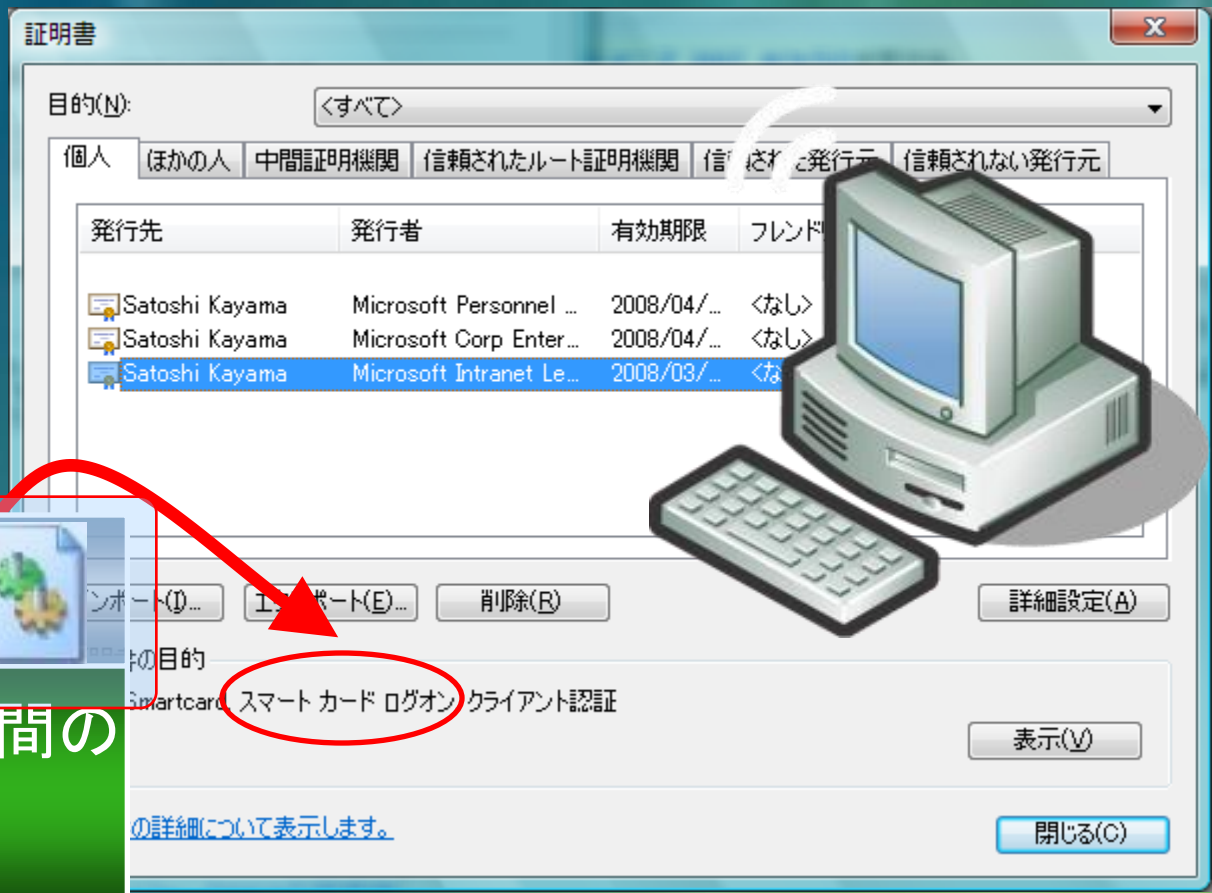
Windowsとスマートカードの関係

- 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~~

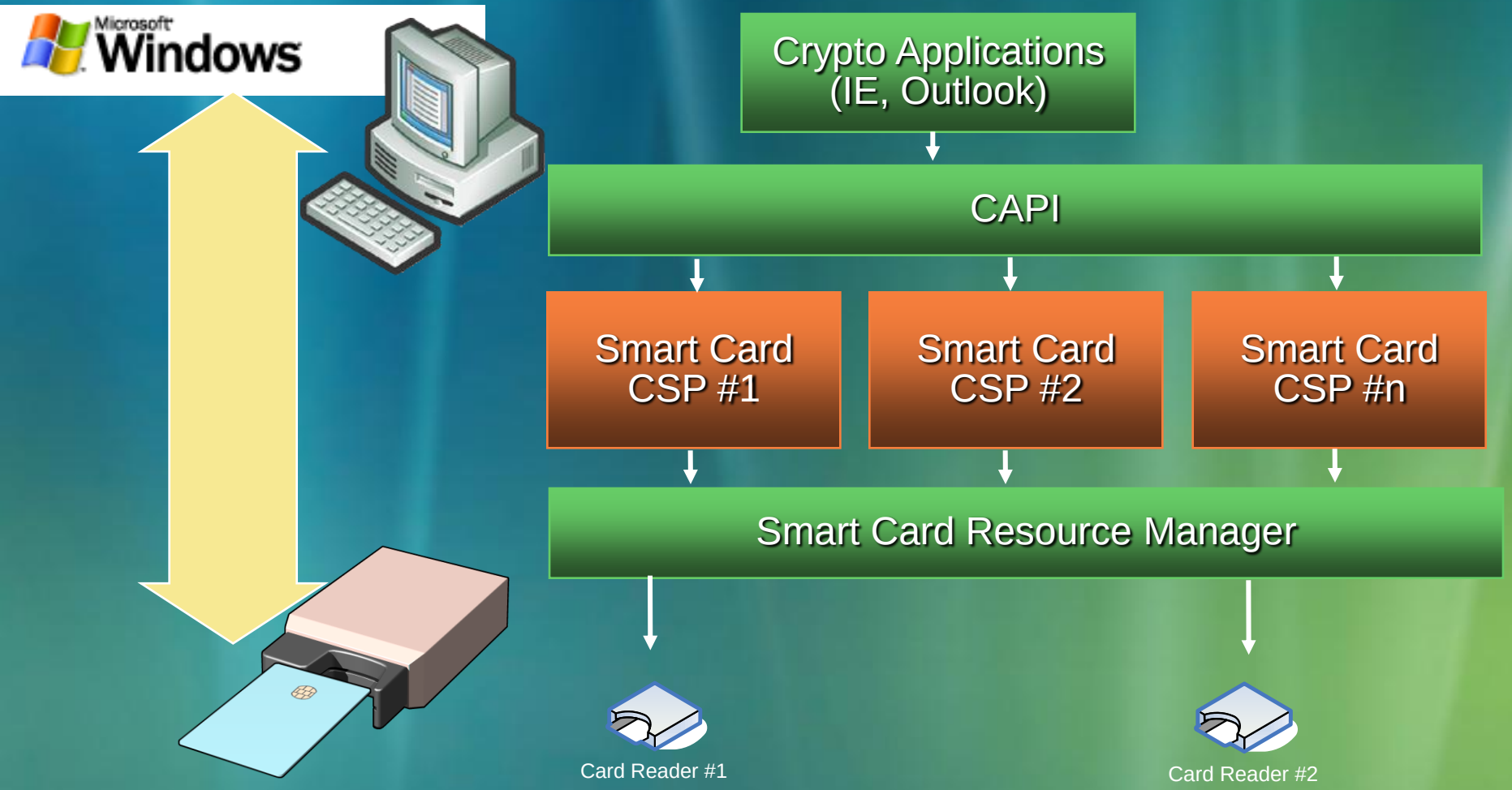
変わること

CSP

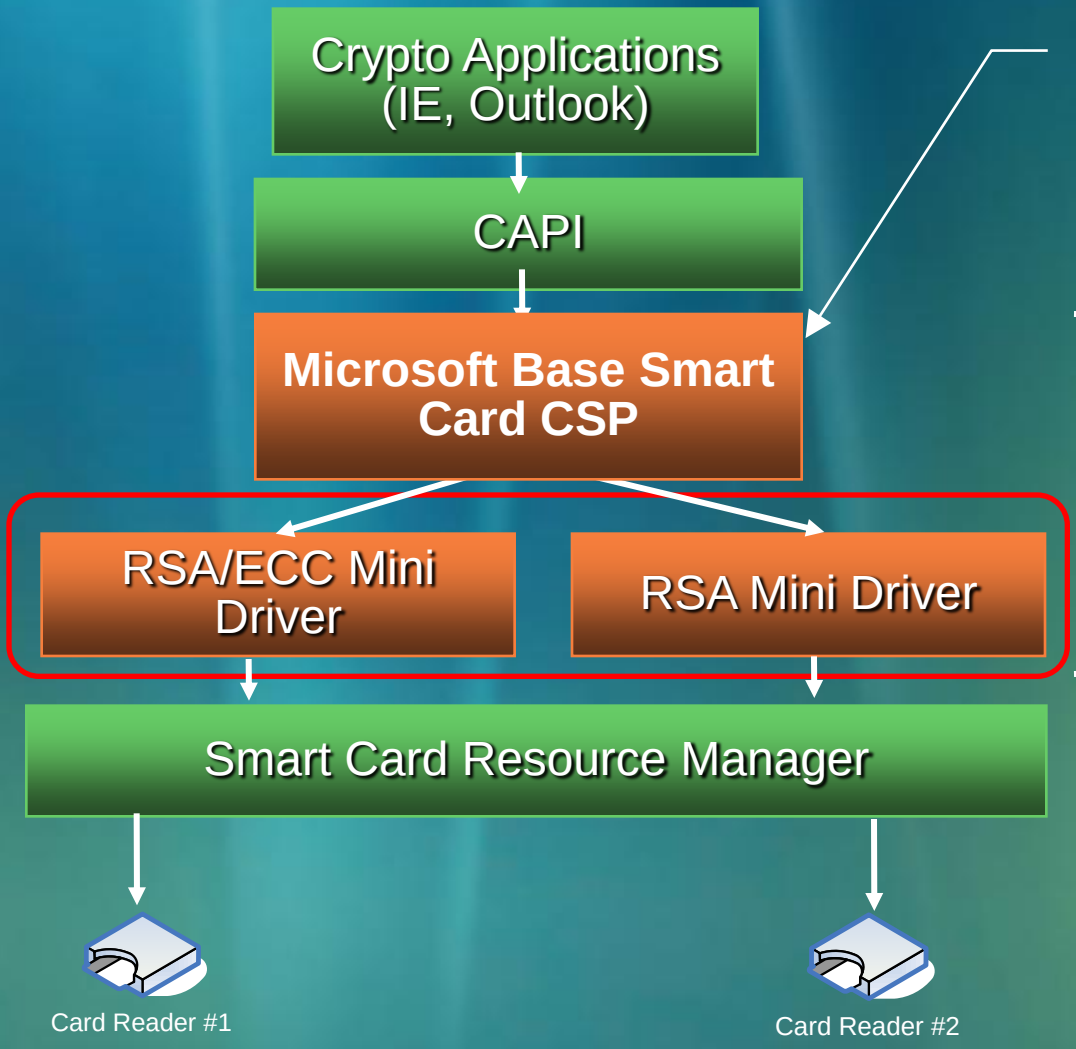
WindowとICチップ間の通信を行う



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



VISTAではあらかじめ実装されています

従来のベンダーCSP相当の機能

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

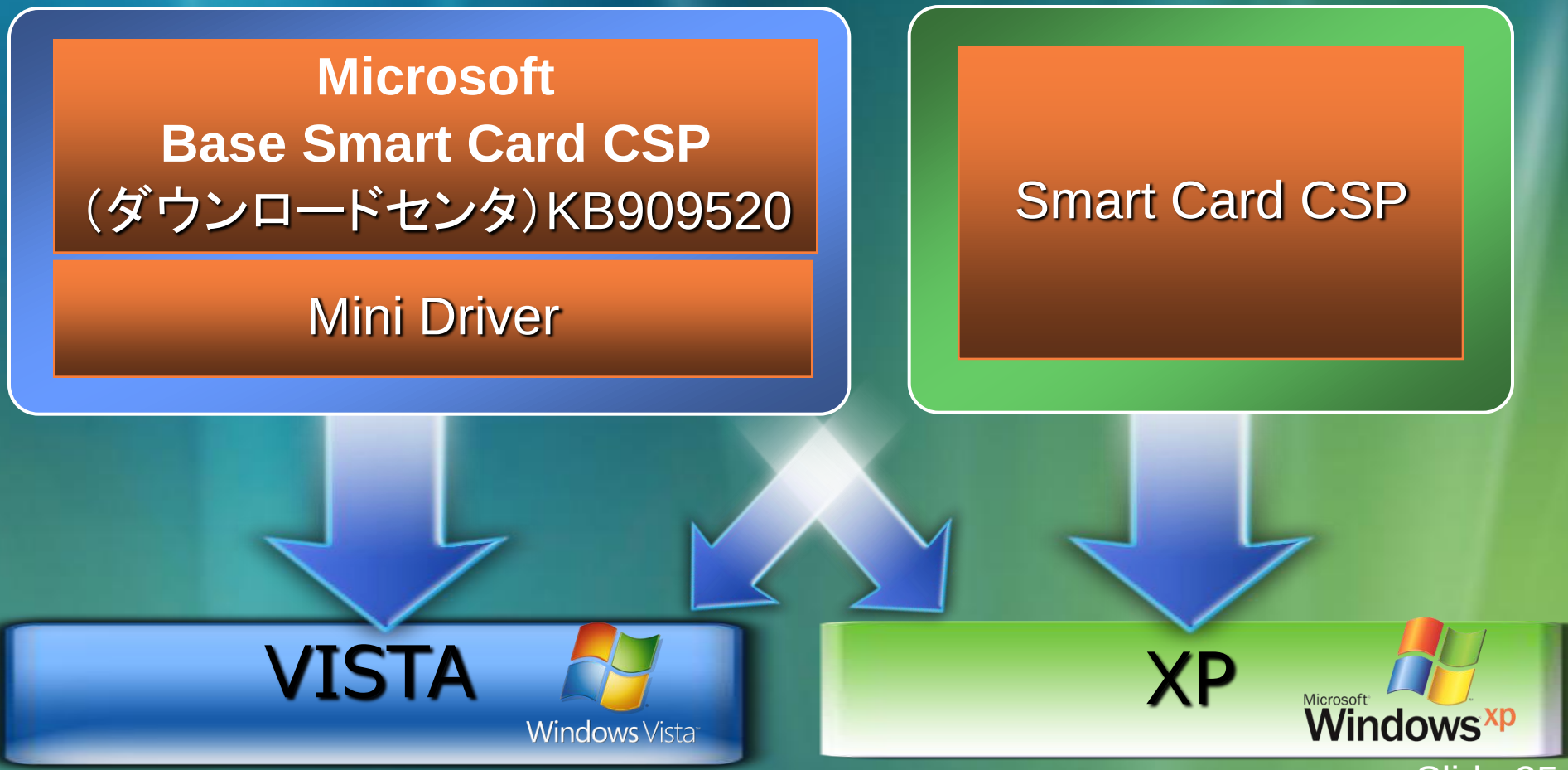
Smart Card
CSP

インストール対象OSについて

- 旧Smartcard CSP はVITSA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

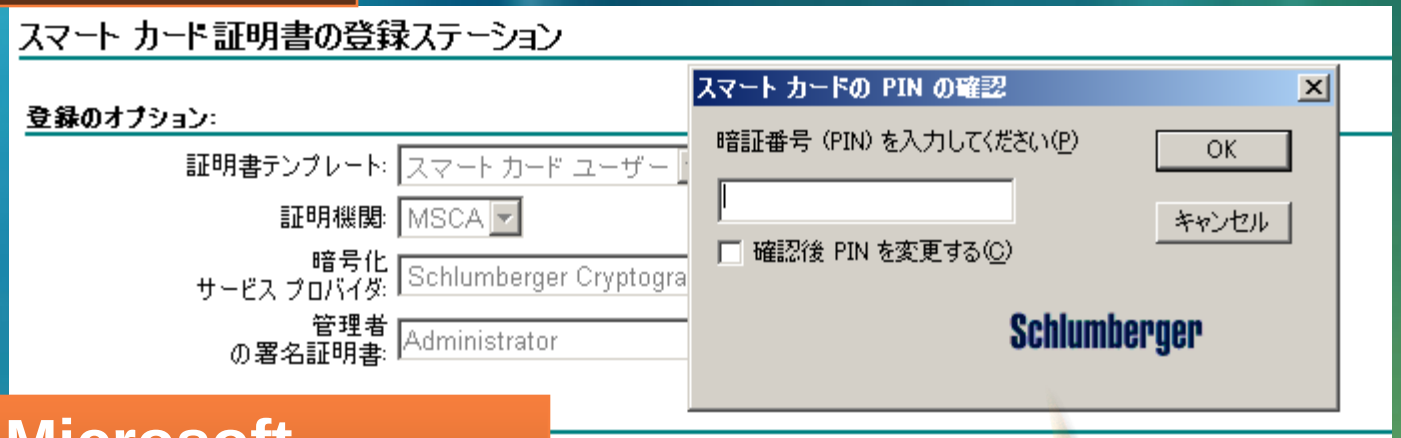
インストール対象　補足

- 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



Mini Driverの動作例

Smart Card CSP



Microsoft
Base Smart Card CSP

新機能の紹介

ログオン先頭画面の変化
-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

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

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

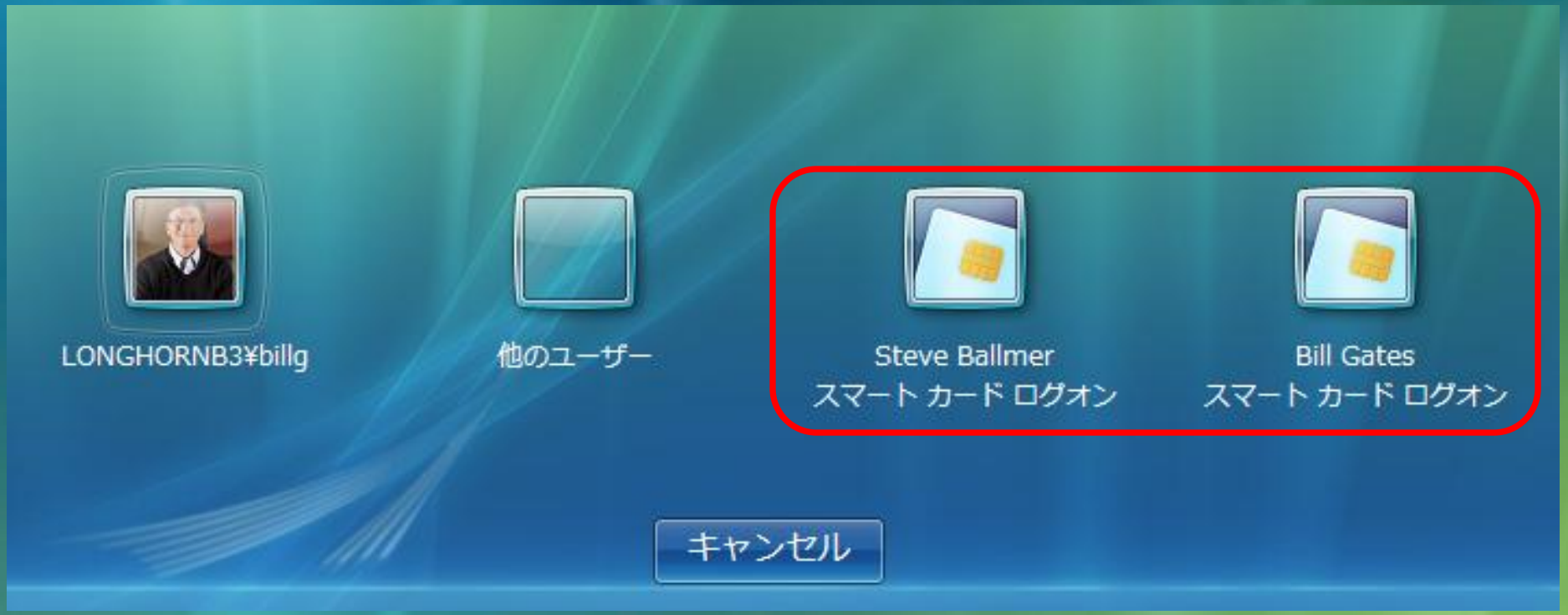
従来の暗証番号変更ツール

- 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

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



想定される活用例

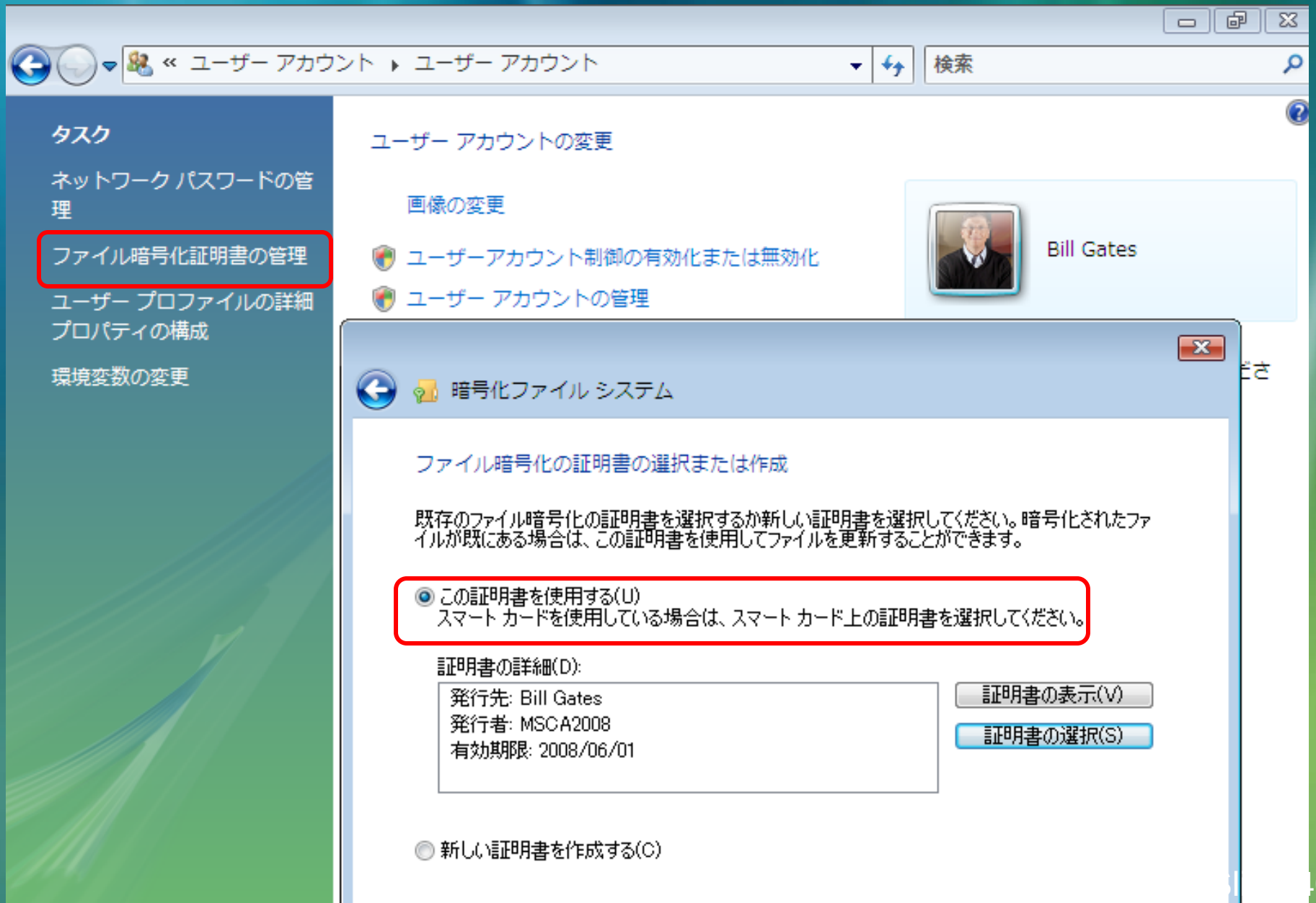
- 日米欧など国別ドメインへのログオン
  - グローバル企業
  - 事業部、分社化された環境への対応
- 「管理者」としての作業、「一般ユーザ」としての作業の切換え

✓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

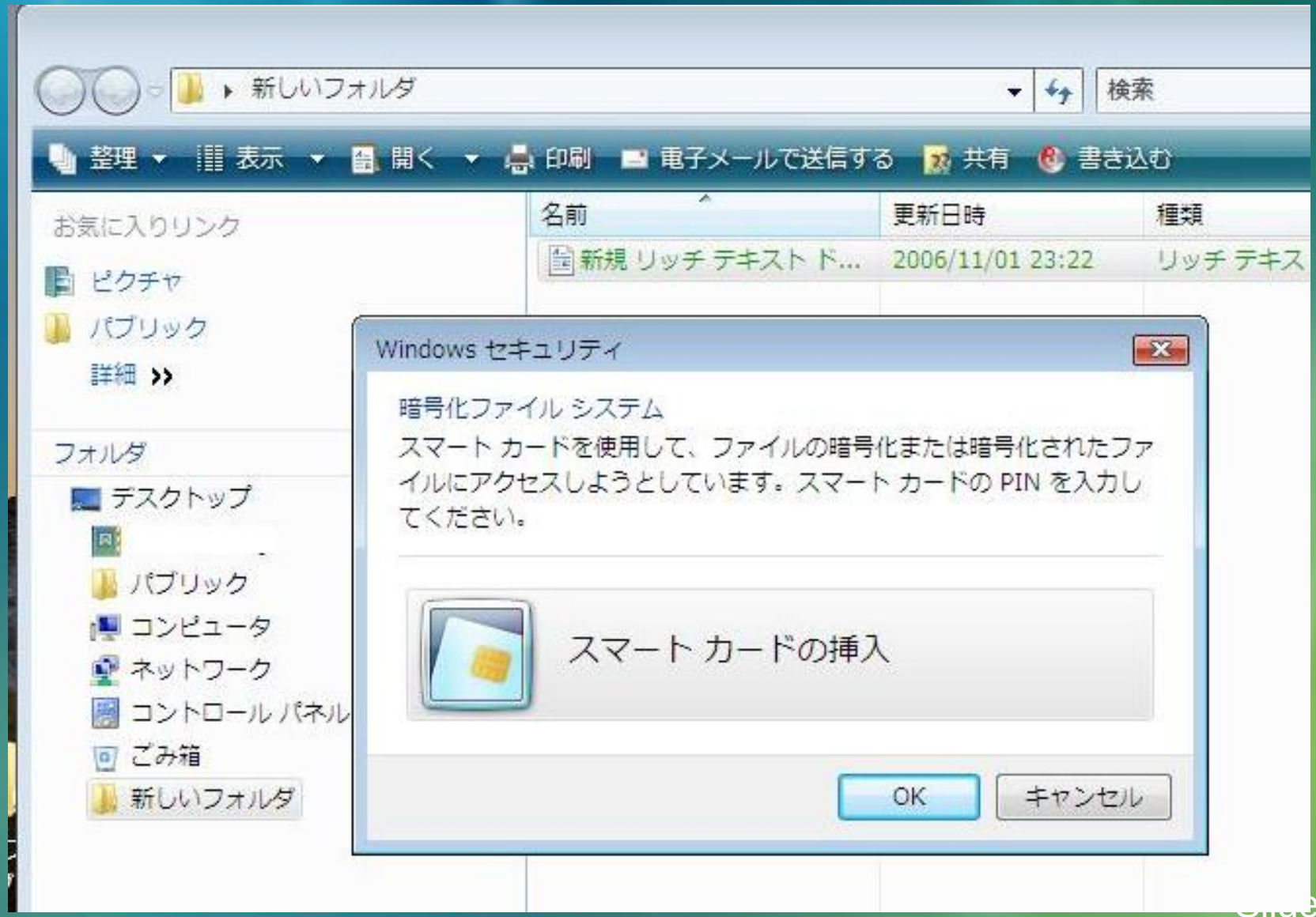
EFS証明書
スマートカード格納

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

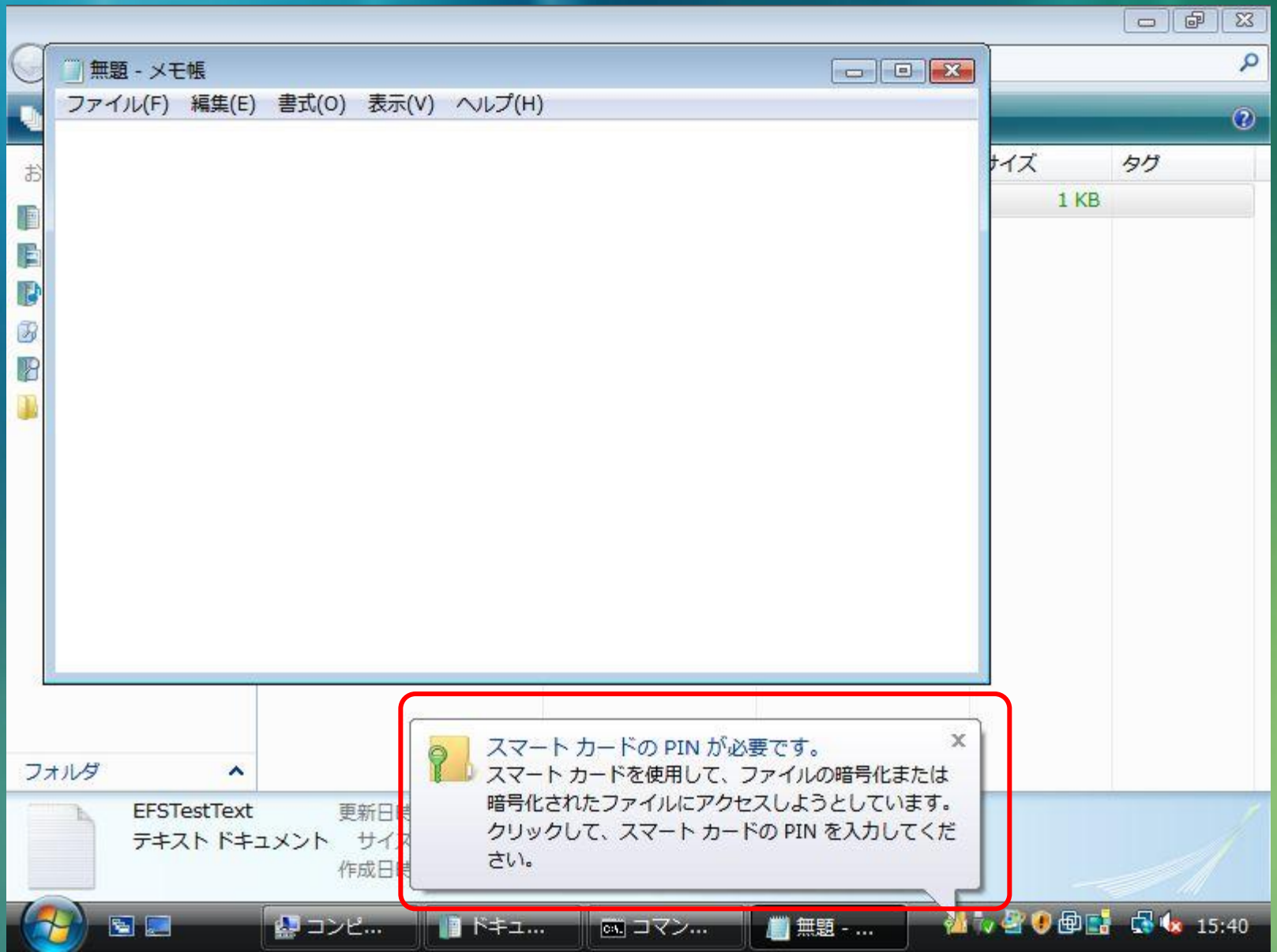
EFSのスマートカード対応



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

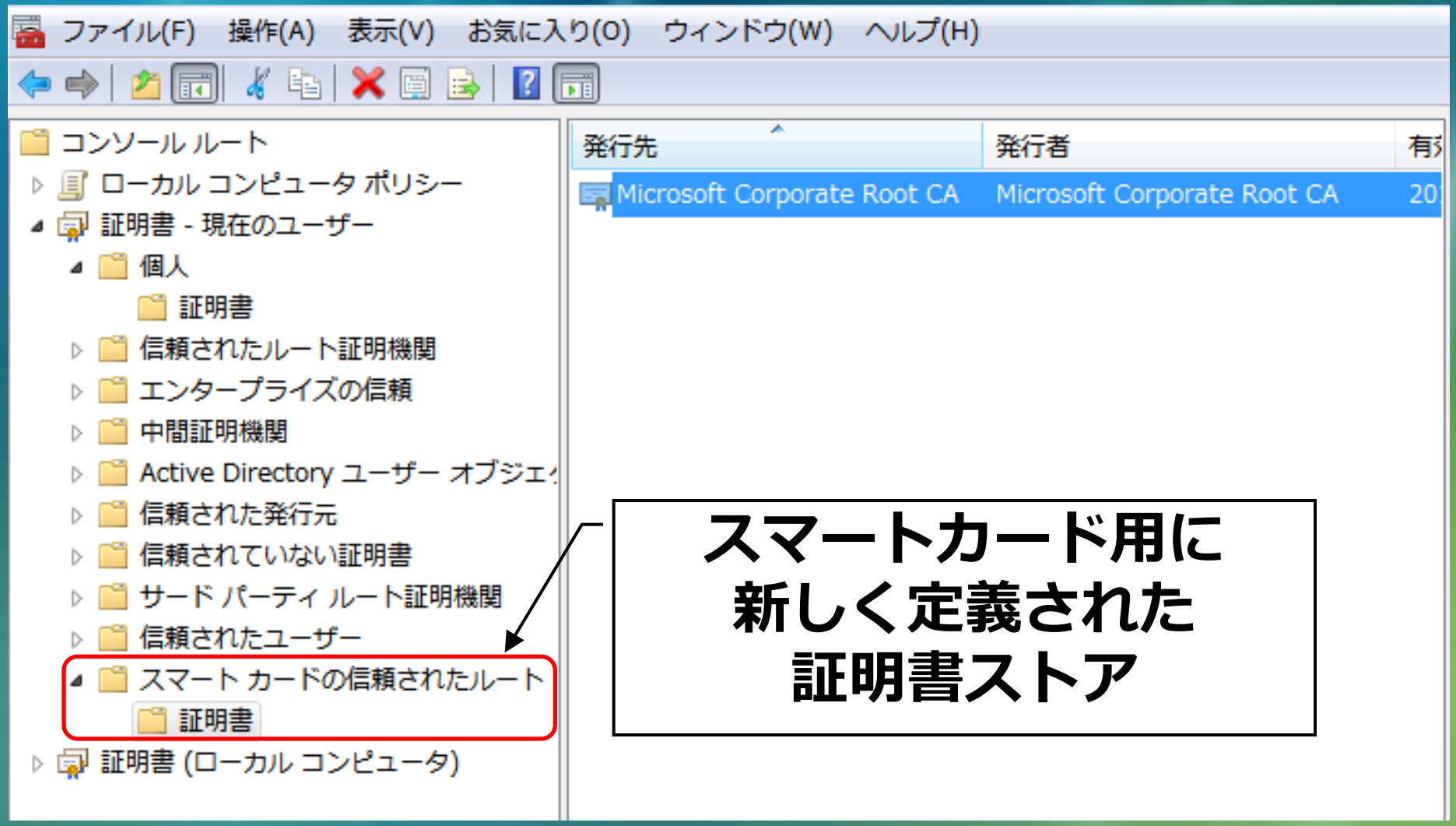


EFSスマートカード対応の意義

- 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

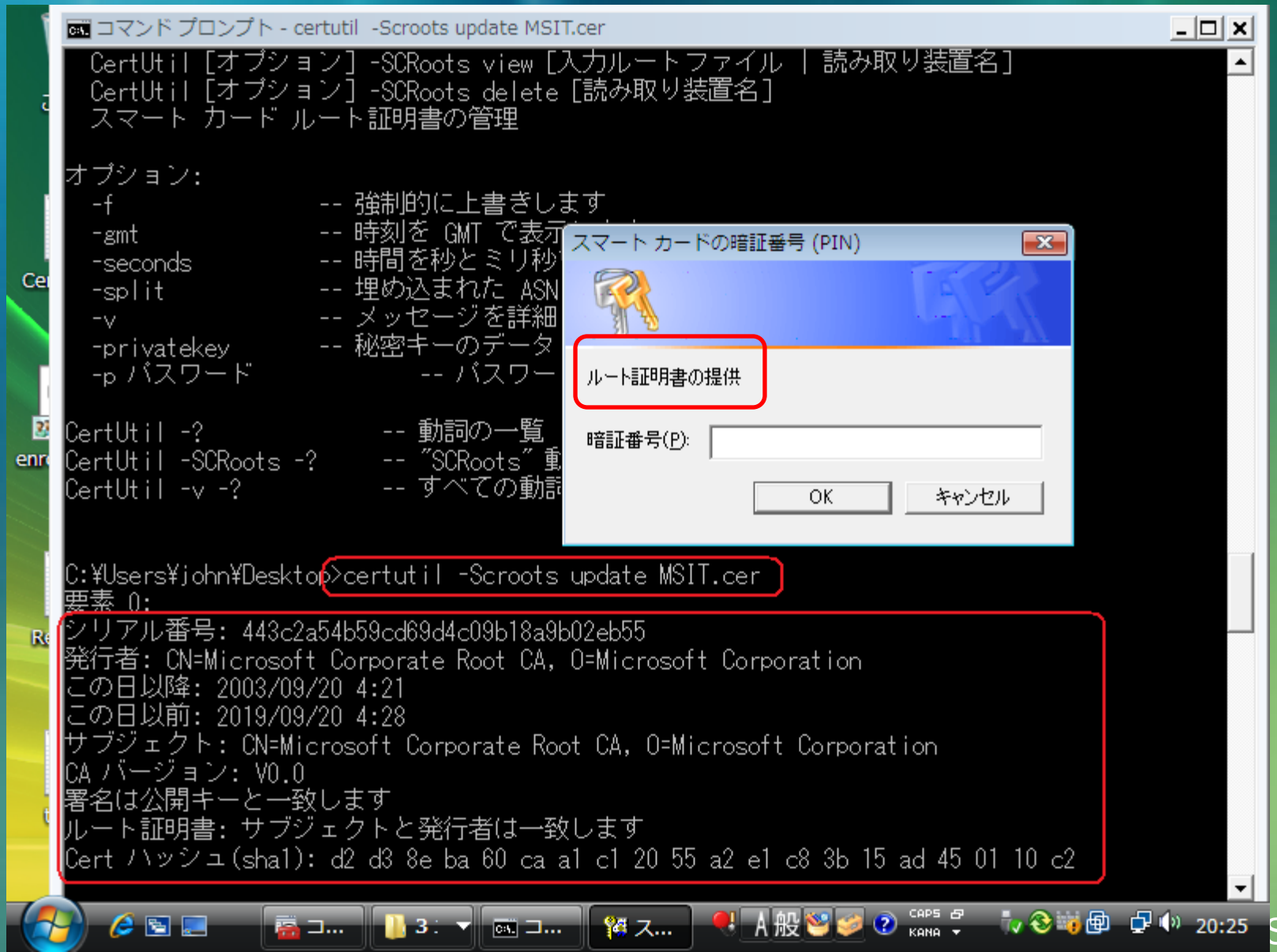
拡張された証明書ストア



ルート証明書格納コマンド

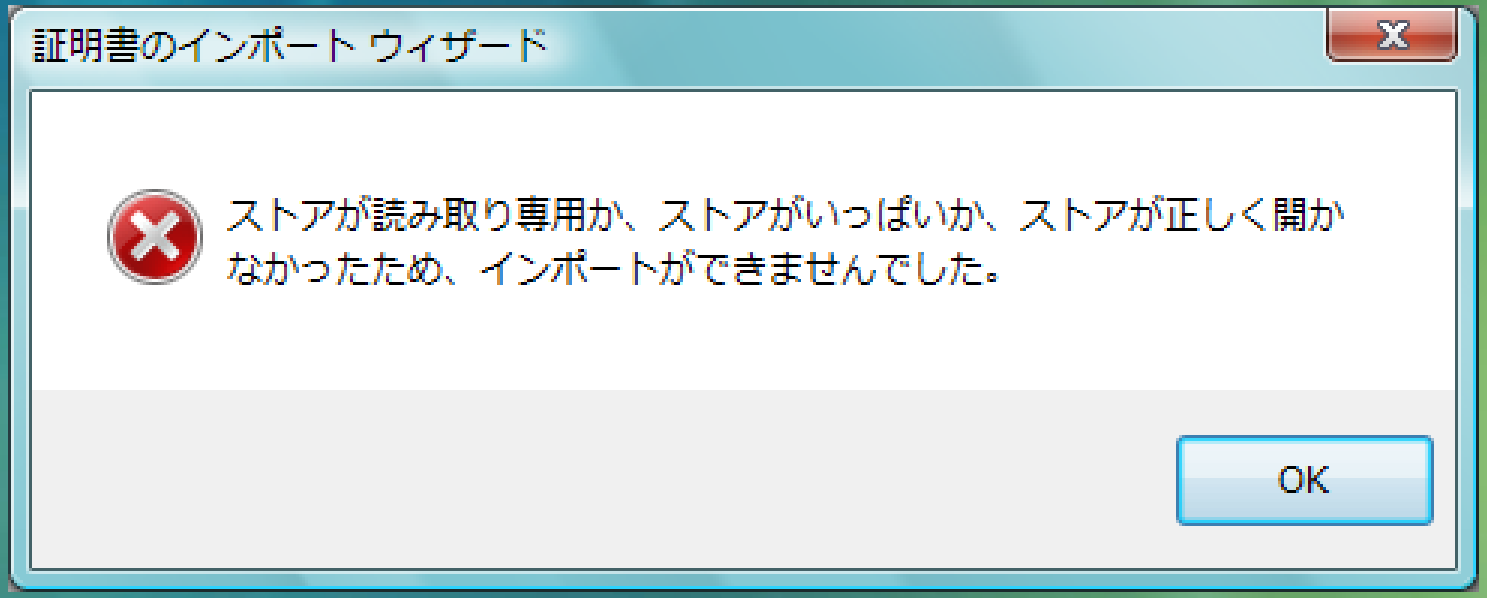
```
C:¥Users¥skayama>certutil -scroots -?
使用法:
  CertUtil [オプション] -SCRoots update [+][入力ルートファイル] [読み取り装置名]

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

コマンドの適用例

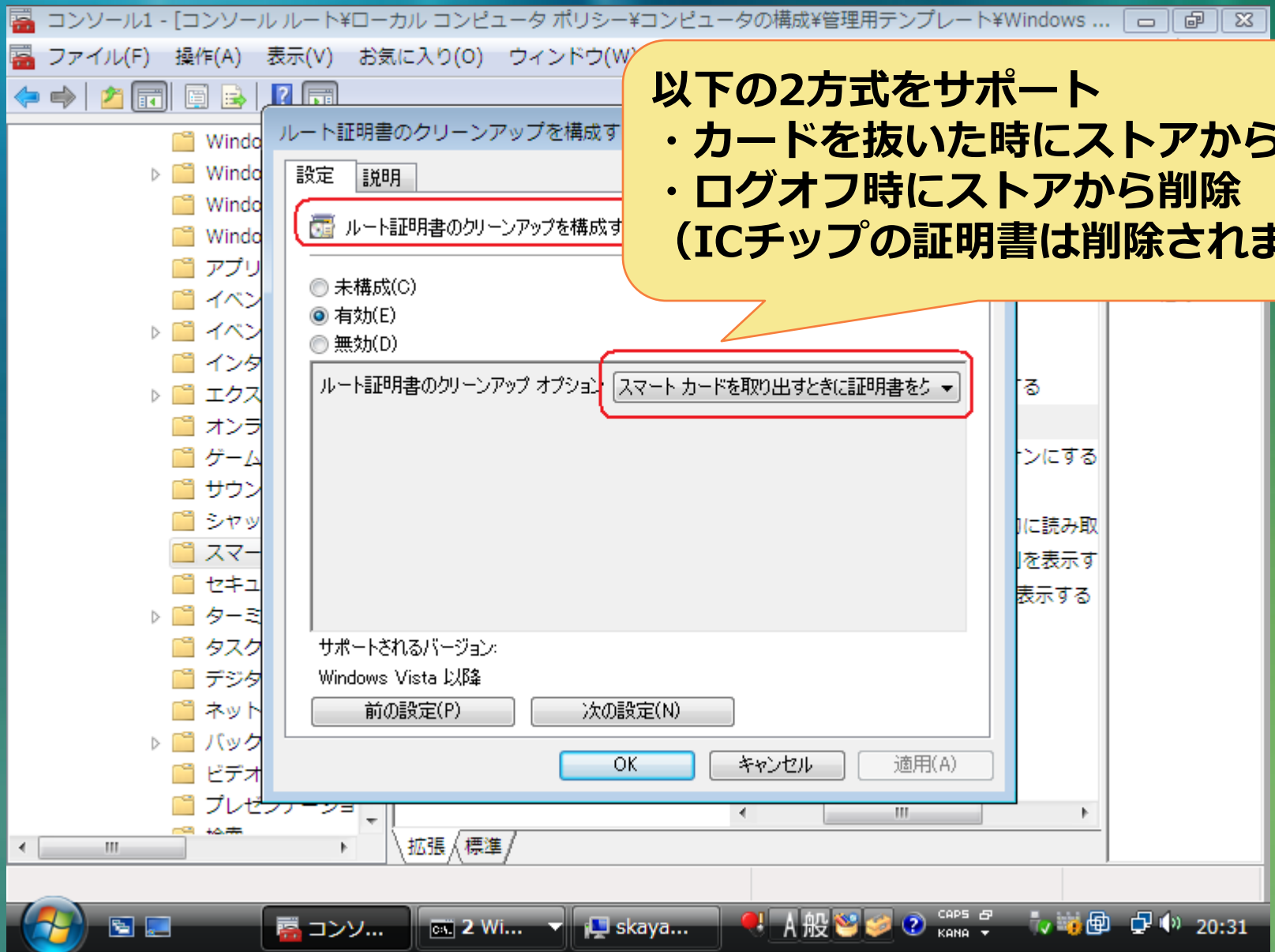

コマンド プロンプト - certutil -Scroots update MSIT.cer
CertUtil [オプション] -SCRoots view [入力ルートファイル | 読み取り装置名]
CertUtil [オプション] -SCRoots delete [読み取り装置名]
スマート カード ルート証明書の管理
オプション:
-f -- 強制的に上書きします
-gmt -- 時刻を GMT で表示
-seconds -- 時間を秒とミリ秒
-split -- 埋め込まれた ASN
-v -- メッセージを詳細
-privatekey -- 秘密キーのデータ
-p パスワード -- パスワー
CertUtil -? -- 動詞の一覧
CertUtil -SCRoots -? -- "SCRoots" 動
CertUtil -v -? -- すべての動詞
スマート カードの暗証番号 (PIN)
ルート証明書の提供
暗証番号(P):
OK
キャンセル
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
20:25

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
- 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®

Your potential. Our passion.™