セキュリティ機能との付き合い方

- Windows PKI を例にして -

2003-03-22 NT-Committee2

緊急コンピュータセキュリティ研究会
りょうわあきら@Cookies.to
(E-mail: ryowa@cookies.to)

ところで PKI て、何ですか？

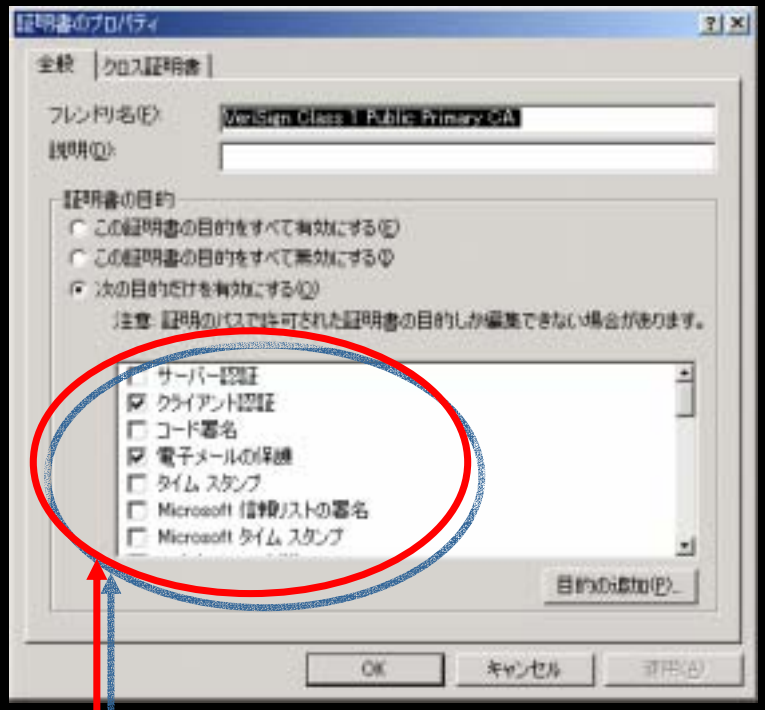
- PKI = Public Key Infrastructure
  - 公開鍵暗号技術を使用して、盗聴・改ざん・なりすましなどの危険を回避して安全なデジタル情報交換を行うためのインフラ
  - デジタル証明書の発行・流通・利用の為の規格、ハード/ソフト、制度等が一体となったものを指す
  - 代表的なPKIコンポーネント
    - X.509: デジタル証明書フォーマットの標準仕様。
    - 認証局 (CA) : 加入者を識別し、証明書を発行する組織。
    - ディレクトリ: デジタル証明書を格納し、配布するシステム。
    - 公開鍵暗号ライブラリ: 暗号化・証明書検証などの機能を実装するソフトウェア (CryptoAPIなど) 。
    - スマートカード: 加入者の秘密鍵を安全に保管するハードウェア。

で、Windows PKI とは？

- もう少し狭い範囲
  - Windows へのPKIコンポーネント（ソフトウェア）の実装
  - Windows における、公開鍵暗号技術の応用の枠組み
- ところで…
  - Windows PKI が、どこでどのように使われているか把握していますか？
  - Windows PKI が、どんな仕組みで機能しているか理解できていますか？
  - もし知らないとして、あなたは Windows を安全な使い方で使っているといえますか？

Windows で PKI が使われている主な局面

- SSL/TLS 通信
  - IE によるサーバ認証/IIS によるクライアント認証
- S/MIME メール検証
  - Outlook / OutlookExpress の署名検証
- コード署名の検証
  - ActiveXコンポーネントのダウンロードインストール
  - オフラインコード検証
  - Windows ファイル保護 (WFP)
  - ソフトウェア制限ポリシー
- タイムスタンプ検証
- スマートカードログオン認証
- 暗号化ファイルシステム (EFS)
- 802.1x EAP/TTLS 認証
- IPsec / IKE 認証



ここを一覧してみると…

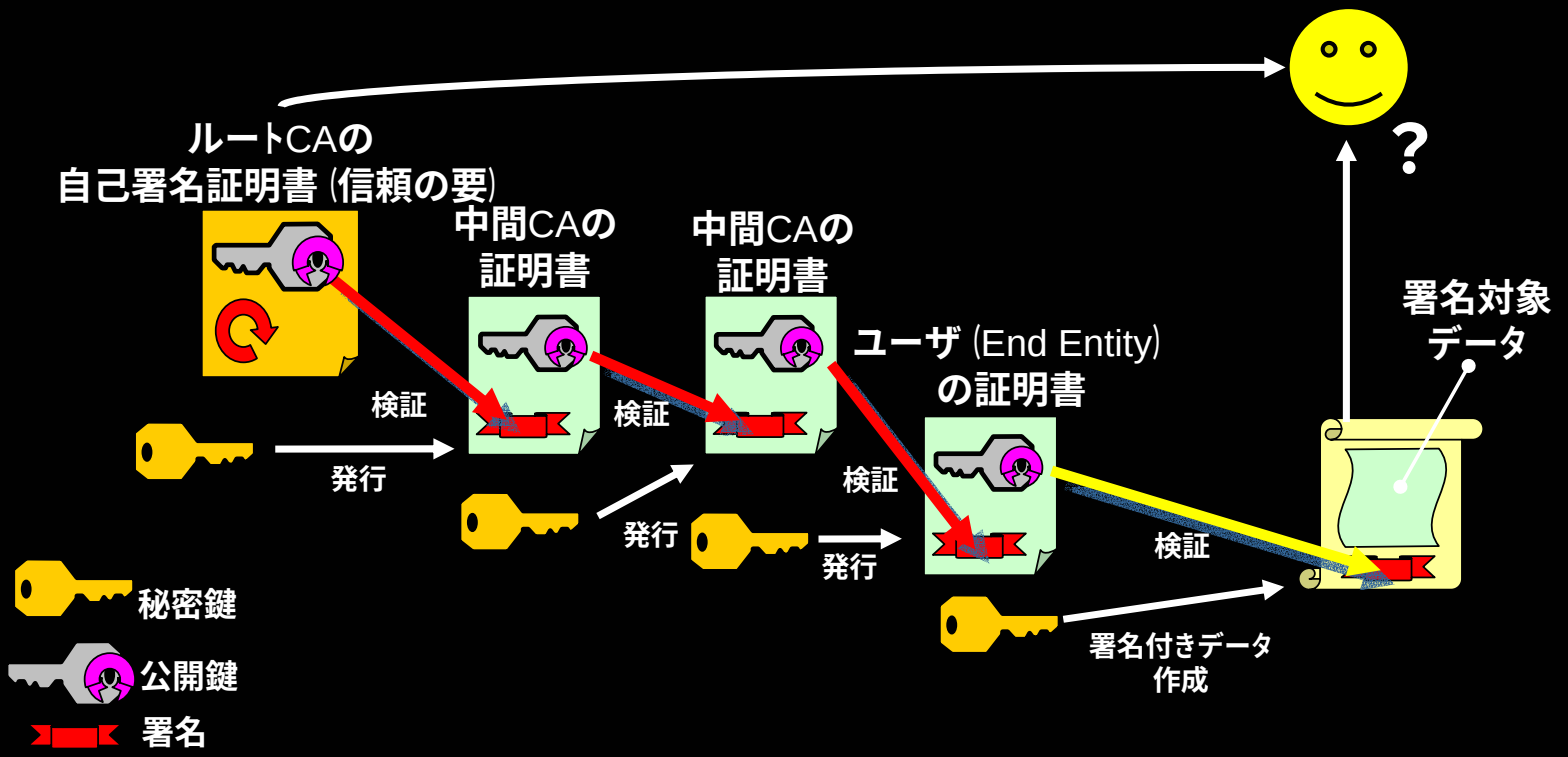
その他、実はこんなところにも PKIの仕掛けが… (いっぱい)

- サーバー認証
- クライアント認証
- コード署名
- 電子メールの保護
- タイムスタンプ
- Microsoft 信頼リストの署名
- Microsoft タイムスタンプ
- IP セキュリティ末端システム
- IP セキュリティ トンネル終端
- IP セキュリティ ユーザ
- 暗号化ファイルシステム
- Windows ハードウェア ドライバの確認
- Windows システム コンポーネントの確認
- OEM Windows システム コンポーネントの確認
- 埋め込み Windows システム コンポーネントの確認
- キーパックライセンス
- ライセンスサーバの確認
- スマート カード ログオン
- デジタル権限
- 限定従属
- キー回復
- ドキュメントの署名
- IP セキュリティ IKE 中間
- ファイル回復
- ルートリスト署名者
- すべてのアプリケーションポリシー
- ディレクトリ サービス電子メール複製
- 証明書の要求エージェント
- キー回復エージェント
- CA 暗号化証明書
- ライフタイム署名

かなりコアに組み込まれている

詳しくは、「Windows XP Professional と Windows Server 2003 の PKI 拡張機能」
http://www.microsoft.com/japan/windowsxp/pro/techinfo/planning/pkiwinxp/default.asp

PKIの基本のきほん (署名と証明書の検証)



◆CAは、秘密鍵を死守して、適切な対象 (加入者) に適切な手続で、証明書を発行

◆加入者 (証明書所有者) は、秘密鍵を死守して、秘密鍵を適切な用途に使用

◆署名検証者 (証明書の検証者) は、信頼するCAの自己署名証明書を、信頼できる場所から改ざんされない方法で入手・保管し、検証の基点とする

◆署名検証者 (証明書の検証者) は、証明書を正しく検証する

PKIの弱点は？

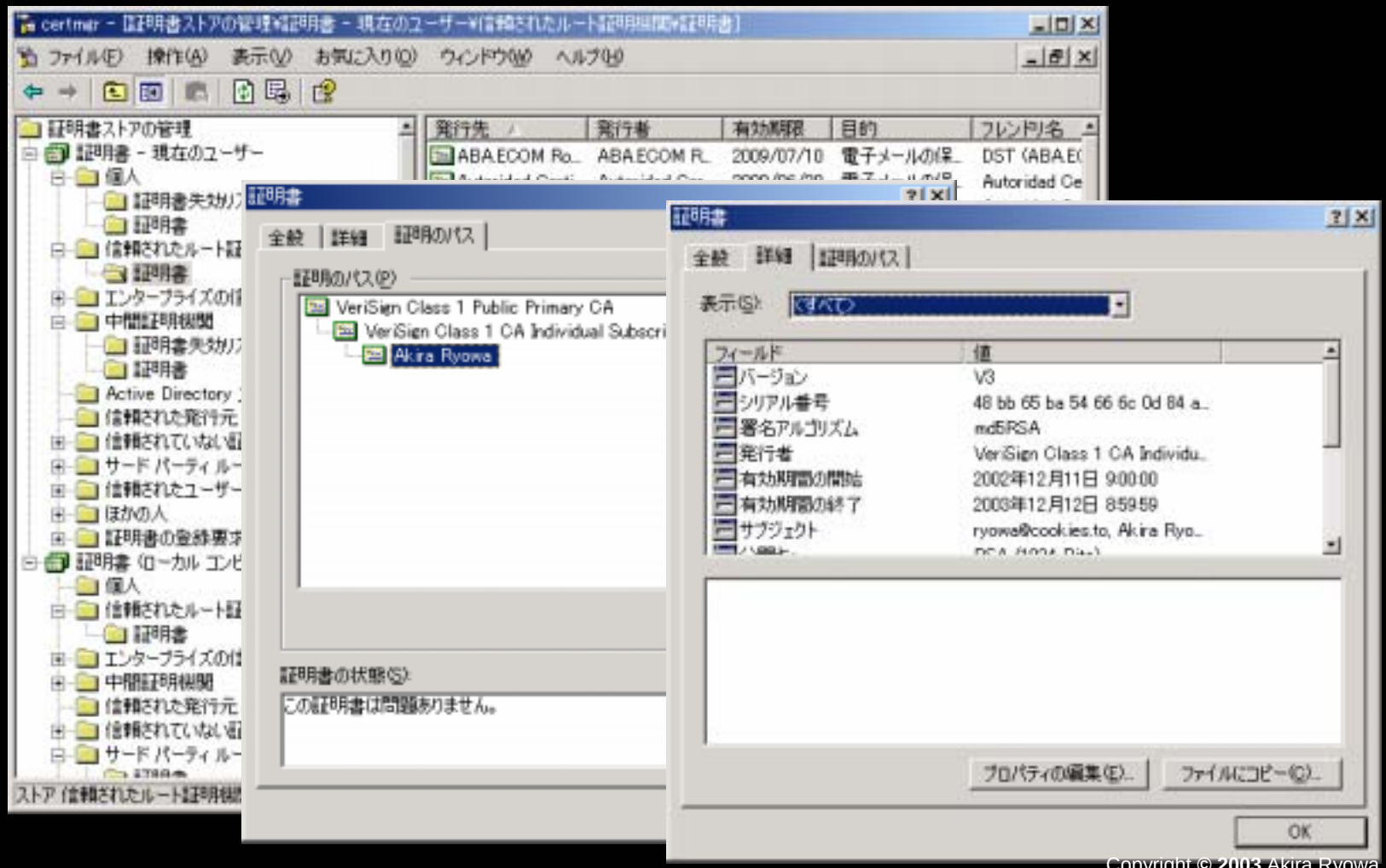
- PKIを攻略したいときには…
  - 秘密鍵を入手（あまりにも当然なので今日はパス）
    - ユーザ秘密鍵 → 不正ログオン、不正な署名付データの作成
    - 中間CA秘密鍵 → 不正なユーザ証明書を発行
    - ルートCA秘密鍵 → 信頼モデル崩壊
  - ルートCA証明書（信頼の要）のすり替え（ポイント1）
    - 複数のルートCA証明書を信頼している場合が危ない（すり替え・追加があっても正常時と変わらずに使えてしまう）→ Windows PKI は該当している
    - 悪意あるルートCA証明書を信頼させる → Windows では、たくさんのセキュリティ機能がPKIを応用しているため、大きな影響が出そう
  - 証明書検証・署名検証機構の穴を攻略（ポイント2）
    - 適切な（あるいは期待通りの）動作をしてくれない → 思い込みで使われている機能はないか？

その他PKIの代表的なリスクに関しては、
Ten Risks of PKI - http://www.counterpane.com/pki-risks.pdf 等を参照

(ポイント1) Windows PKI で、信頼の要は攻略可能？

- ルートCA証明書が不正操作を受ける危険性と可能な防衛策を評価するためには、以下のことを知っておく必要がある。
  - どこにあるか？
  - どのような形式で保存され、保護されているか？
  - どうすれば操作できるのか？
- 実際に確認してみる。

証明書はどこにある？ -
MMC証明書スナップインによる証明書ストアの確認



証明書はどこにある？- 実体は、

- スナップインからの操作によるシステムの変更を監視すると…
- 証明書ストア「信頼されたルート証明機関」の実体はレジストリにあることがわかる
  - スタンドアロン環境では以下のレジストリキー
    - [HKCU¥SOFTWARE¥Microsoft¥SystemCertificates¥ROOT¥Certificates¥] の配下（ユーザ）
    - [HKLM¥SOFTWARE¥Microsoft¥SystemCertificates¥ROOT¥Certificates¥] の配下（ローカルコンピュータ）
  - ActiveDirectory環境ではグループポリシーに

(参考) レジストリ中の証明書

SystemCertificates配下のサブキー	概　　要
AddressBook	Outlook のS/MIME証明書
AuthRoot	(Microsoftに)認証された信頼されたルートCA
CA	中間CA証明書
Disallowed	無効とする証明書
My	ローカルコンピュータの秘密鍵と関連した証明書 (ユーザ証明書のストアはユーザプロファイル配下に。 %USERPROFILE%¥Application Data¥Microsoft¥SystemCertificates¥My)
ROOT	信頼されたルートCA
SPC	ソフトウェア発行者証明書
Trust	エンタープライズの信頼
TrustedPeople	ルートによらず個別に信頼されたユーザ証明書 (EFS用証明書など)
TrustedPublisher	ルートによらず個別に信頼されたソフトウェア発行者証明書

詳細はこちらを参照

http://msdn.microsoft.com/library/en-us/security/security/system_store_locations.asp

(参考) レジストリ中の証明書

SHA1 Fingerprint

MD5 Fingerprint

Certificate

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates
            \ROOT\Certificates\E3356D0519052056F957C8D62F4574F87F087032]
"Blob"=hex:0f,00,00,00,01,00,00,00,14,00,00,00,8c,6a,ac,20,48,2b,5a,42,7b,1f,\
  a1,01,d4,ab,a3,35,ba,e8,36,68,14,00,00,00,01,00,00,00,14,00,00,00,d1,de,13,\
  3d,30,dd,13,40,24,c6,c8,d8,dd,02,de,19,53,46,bf,22,03,00,00,00,01,00,00,00,\
  14,00,00,00,e3,35,6d,05,19,05,20,56,f9,57,c8,d6,2f,45,74,f8,7f,08,70,32,04,\
  00,00,00,01,00,00,00,10,00,00,00,98,6b,5e,a6,4c,38,07,c1,54,93,a7,70,12,f0,\
  be,0d,19,00,00,00,01,00,00,00,10,00,00,00,ca,d0,81,13,a2,63,0c,2d,97,6b,91,\
  b0,b5,d5,06,c5,20,00,00,00,01,00,00,00,bb,01,00,00,30,82,01,b7,30,82,01,61,\
  a0,03,02,01,02,02,01,01,30,0d,06,09,2a,86,48,86,f7,0d,01,01,05,05,00,30,42,\
  31,0b,30,09,06,03,55,04,06,13,02,55,53,31,12,30,10,06,03,55,04,0a,13,09,4d,\
  69,63,72,6f,73,6f,66,74,31,1f,30,1d,06,03,55,04,03,13,16,4d,69,63,72,6f,73,\
  6f,66,74,20,2e,4e,45,54,20,52,6f,6f,74,20,43,41,30,1e,17,0d,30,33,30,32,30,\
  39,30,37,35,39,30,31,5a,17,0d,30,33,30,32,31,36,30,37,35,39,30,31,5a,30,42,\
  31,0b,30,09,06,03,55,04,06,13,02,55,53,31,12,30,10,06,03,55,04,0a,13,09,4d,\
  69,63,72,6f,73,6f,66,74,31,1f,30,1d,06,03,55,04,03,13,16,4d,69,63,72,6f,73,\
  6f,66,74,20,2e,4e,45,54,20,52,6f,6f,74,20,43,41,30,5c,30,0d,06,09,2a,86,48,\
  86,f7,0d,01,01,01,05,00,03,4b,00,30,48,02,41,00,a6,2a,01,7b,f5,36,fc,fa,f2,\
  eb,14,99,fa,f3,95,ef,1d,f7,8a,e8,b3,a5,3d,8e,c9,81,b4,12,ca,77,7b,1f,9b,40,
  3e,36,c3,2b,d0,c2,00,7b,af,5e,3f,f3,bb,3c,a3,d3,54,5f,9f,bd,29,09,6d,15,b2,\
  42,5f,b1,ee,8f,02,03,01,00,01,a3,42,30,40,30,0f,06,03,55,1d,13,01,01,ff,04,\
  05,30,03,01,01,ff,30,0e,06,03,55,1d,0f,01,01,ff,04,04,03,02,01,c6,30,1d,06,\
  03,55,1d,0e,04,16,04,14,d1,de,13,3d,30,dd,13,40,24,c6,c8,d8,dd,02,de,19,53,\
  46,bf,22,30,0d,06,09,2a,86,48,86,f7,0d,01,01,05,05,00,03,41,00,31,2c,86,f4,\
  2d,ca,e0,a0,7a,72,70,d5,d9,b2,83,57,f3,cb,c4,05,78,9b,51,3a,36,e6,23,df,73,\
  e6,67,d7,50,35,c7,f1,e2,8b,06,d8,a2,88,3b,90,64,24,2f,e3,8e,c3,1e,3e,34,ee,\
  72,a8,2e,06,01,6f,53,c5,f5,41
```

証明書ストアは、どうすれば操作できるのか？（1）

- ルートCA証明書の追加や更新
  - アプリケーションからのユーザ操作による追加や更新
    - 証明書ダイアログやMMC証明書スナップインから
    - 追加する場合、CryptoAPI経由の場合には証明書を信頼するかどうか、確認を求められる
  - その他 Windows Update と連動したルート証明書の自動更新機能による追加や更新
    - http://www.microsoft.com/japan/windowsxp/pro/techinfo/administration/manageautoupdate/ManagingDL.doc
    - Microsoftによって信頼されたルート証明書は自動的に信頼される

しかし、実体がレジストリであれば、レジストリを直接操作しても同じことが可能ではないか？

証明書ストアは、どうすれば操作できるのか？（2）

- 実際に検証したところ、レジストリを操作する権限さえあれば、不正な証明書を信頼させることができた。
  - regコマンド等でルート証明書データを直接注入
  - CryptoAPI経由の場合と違い、ユーザへの確認はされない
  - レジストリ保護手段 → OSによるアクセス権設定のみ
  - アクセス権設定を迂回できれば容易に攻略可能
    - 他の脆弱性を攻略して…
    - 受動的攻撃（レジストリ変更は警告なしに行われる。安易にAdministrator で作業してはいないか？）
    - インストールにAdministrator権限を要求するアプリケーション（レジストリ変更は警告なしに行われる。安易に信頼してはいないか？）

Windows PKI を
安全に活用するためには

- 心がけること
  - 不注意な操作一つで、信頼の要が攻略されることを認識
  - Administrator権限での操作は最小に
  - 必要ならレジストリのACLを強化（操作失敗への対策）
  - 必要ならレジストリを監視（セキュリティ監査ログ・3rd Party ツール）
  - エンドユーザによるルート証明書取り込みは極力しない
  - 証明書を信頼する目的には十分注意（特に手動組み込みだとデフォルトが＜すべて＞なので、必ず変更）

(ポイント2) 仕様/実装に問題はないか？ 過去の事例

- 仕様/実装上の問題があると…
- 過去に指摘されている代表的な問題
  - 証明書確認の問題により、ID が偽装される (Q329115) (MS02-050)
    - 実は、**誰でも中間CAになれた**ヽ(;´Д`)ノ
  - Windows File Protection Arbitrary Certificate Chain Vulnerability
    - 実は、WFPは**厳密にはMicrosoftの署名を確認しているわけではなかった**
- 機能の検証をしないまま使って、安全だと考えられますか？

Windows ファイル保護 (WFP) の場合 (1)

- Windows ファイル保護 (WFP)
  - Windows 2000 以降で導入されたシステムファイル保護機構
  - 動作は、次のように説明されている
    - WFP は、保護されたファイルが正しい Microsoft バージョンのものであるかどうかを確認する
    - 確認には、コード署名によって生成されたファイル署名及びカタログファイルを使う
  - Administrator であっても出来ることを制限しているという点で、評価できる機能

しかし、実際には次のような問題点が指摘されている

Windows File Protection Arbitrary Certificate Chain Vulnerability
http://www.science.org/secalert/WFP_Arbitrary_Certificate_Chain_Vulnerability.txt

Windows ファイル保護 (WFP) の場合 (2)

- これも実際に問題の動作を検証してみると…
  - 保護対象ファイルの置き換えを検知すると、WFP はファイルに付与された Authenticode 署名を検証する。
  - 署名が正しく、かつ署名検証に用いた証明書の「コード署名」＋「Windows システムコンポーネントの確認」が有効な場合、置き換えを許す。
  - 「コード署名」＋「Windows システムコンポーネントの確認」で検証できるカタログファイルに、一致するハッシュ値が存在した場合、置き換えを許す。
  - [時間があればちょっと実演]
  - 実際の検証の過程は、http://archives.jwntug.or.jp/public/index.html?ng=jwntug%2Epublic%2Esecurity&t=%3Cmid%2D241%2Dsecurity%40jwntug%2Eor%2Ejp%3E のスレッドを参照してみてください。
- 着目点はよいけれど、今の仕様ではセキュリティ機能とはいえないかな

詳しくは「WFPとデジタル署名」http://www.port139.co.jp/csir_wfp.htm

その他の関連しそうな機能では…

- セキュリティ機能に見え隠れする怪しい挙動
  - ソフトウェアの制限ポリシー (SRP) のハッシュ規則に存在する問題
    - レジストリに次の値が登録されることで規則が有効に
      - [MD5 or SHA1 hash value]:[file length]:[hash algorithm id]
    - ところがSHA1ハッシュ値が登録された場合、規則が有効にならない ヽ(;´Д`)ノ
    - Authenticode署名付きファイルだと、自動的にSHA1ハッシュ値が選択されるのだが…
    - [時間があればちょっと実演]

Windows PKI を調べてみた感想
(愚痴ともいう…)

- エンドユーザ向け・管理者向けに、きちっと各機能の仕組みまで含めて説明したドキュメントが少ない
  - MSDNを読めば、APIレベルでは、仕組みも含めてそれなりに詳しく書かれているけど、エンドユーザには不親切
  - 特にPKI関連は英語ばっかりだし
- エンドユーザ＝認証される側、という造りになっている感が随分する
  - もっと「認証する側」としてのエンドユーザへ配慮した造りになっていてもいいのでは
- 怪しい動作もみられるので、機能としてイマイチ信用しきれない感もある
  - 例えば、SRPのハッシュ計算の不具合などは、あまりにお粗末
  - 仕様が明示されていないから余計そう感じるのかも

セキュリティ機能との付き合い方

- 原則・仕組みを理解しよう
  - セキュリティ機能のもとになっている、原則・仕組みを知る
  - セキュリティ機能の正しい仕様を知る
  - 弱点を知って、うまく回避する
- 機能を信頼する前に、まず評価・検証
  - 本当に期待通りに動いてくれるかは、自分で試してみなくちゃ、わからない
  - セキュリティ機能だからこそ、欠陥の可能性を前提にした評価・検証を

END

用語（PKI一般）

- PKI (Public Key Infrastructure)
  - 公開鍵暗号技術を使用して、盗聴･改ざん･なりすましなどの危険を回避して安全なデジタル情報交換を行うためのインフラ。
- デジタル証明書（Digital Certificate）
  - 公開鍵暗号技術を使用したデジタル署名により、記載データの正当性の検証を可能としている証明書。通常にX.509で規格化されているデジタル証明書を指す。PKI関連の文章では、単に証明書と言うことが多い。
- 自己署名証明書（Self-sign Certificate）
  - デジタル証明書のうち、自分の公開鍵に自分の秘密鍵でデジタル署名を施した証明書。ルート CA のデジタル証明書は自己署名証明書。自己署名証明書の正当性は単体では確認できないので、自己署名証明書データ以外で発行主体を確認できる手段で受け渡す必要がある。
- CA (Certification Authority)
  - 認証局、認証機関などと訳される、デジタル証明書を発行する組織･機関。文脈によっては、証明書発行関連システムを指す意味で使われるため、注意が必要。
- ルートCA (Root CA)
  - ルート認証局。証明書を検証するユーザは、信頼するルート認証局の自己署名証明書を信頼の基点として証明書連鎖を検証することで、デジタル署名の信頼性を確認できる。ルートCA は、中間 CA 及びエンドエンティティに対して証明書を発行する。
- 中間CA (Intermediate CA)
  - 中間認証局。ルート CA 以外のすべての CA は、上位の CA から発行されたデジタル証明書を有する。中間 CA は、さらに下位の中間 CA 及びエンドエンティティに対して証明書を発行する。エンドエンティティのみに証明書を発行するCAを下位CA（Subordinate CA）として区別することもある。

用語 (PKI一般)

- エンドエンティティ (End Entity)
  - 証明書を発行しない、末端の証明書所有者。SSLクライアント証明書、S/MIME 証明書、IPsec 証明書等は、すべてエンドエンティティの証明書に分類される。
- デジタル署名
  - 公開鍵暗号技術を使用した、あるデータに対して特定の秘密鍵所有者だけが作成可能なデジタルデータ。特定の秘密鍵に対応した公開鍵による検証を行うことで、署名対象データが特定の秘密鍵によって署名されていることを確認できる。
- ハッシュ関数/ハッシュ値(Hash function/Hash Value)
  - 任意長データから、固定長無作為なデータを生成する一方向性関数をハッシュ関数といい、ハッシュ関数により生成される値をハッシュ値という。ハッシュ値は、意味のあるデータに対して重複する確率がほぼないことがわかっており、データ正当性の検証に応用される。あるデータに対するハッシュ値を、そのデータのフィンガープリント/拇印ともいう。
- 証明書の検証
  - 検証対象証明書に付与されたデジタル署名をルートCAの証明書まで検証し、検証対象証明書が正当なものであることを確認する作業。現在が有効期限内にあることや使用目的をはじめとした、パラメータのチェックなども行う。
- 証明書の有効性確認
  - CAが提供する情報を元に有効性確認対象証明書が、現時点で有効であることを確認する作業。証明書は、有効期限内であっても、記載事項の変更や秘密鍵の漏洩など様々な理由で効力を失う。CAはこうした証明書の失効リスト等を提供することで、発行証明書の信頼性を維持する。
- 加入者 (Subscriber)
  - CAから証明書の発行を受けた主体。
- 証明書の検証者 (Relying Party)
  - 加入者の証明書に依存して、加入者のデジタル署名を検証する主体。依拠する当事者、依存者とも言われる。

用語 (Windows PKI)

- CryptoAPI
  - Windows ファミリーにおいて、デジタル証明書の取り扱いなどの暗号化関連機能を提供する API 。
- Windows 証明書ストア
  - Windows 2000 以降では、各種証明書は Windows 証明書ストアと呼ばれる共通の格納場所に保存され、さまざまな用途に使用される。CryptoAPI の各種関数を使用することで ストアに対する操作や、ストア内の証明書を利用した処理を行うことができる。
- Windowsファイル保護 (Windows File Protection)
  - Windows 2000 以降に搭載されたシステムファイル保護機構。WFP と略される。WFP は登録されたシステムファイル (SYS, DLL, EXE, OCX ファイルと一部のフォントファイル) の書き換えを監視し、書き換えが行われた場合にはファイルのデジタル署名または登録されたカタログファイルのデジタル署名を検証して、書き換えの可否を制御する。
- ソフトウェアの制限ポリシー (Software Restriction Policy)
  - Windows XP 以降に搭載された、ソフトウェア実行制限･インストール制限を実現する機能。ハッシュの規則、パスの規則、証明書の規則、インターネットゾーンの規則などが利用できる。

参考URL (PKI一般)

- PKI～技術概要と利用の実際～ (IW2002チュートリアル: 松本 泰/稲田 龍)
  - http://www.nic.ad.jp/ja/materials/iw/2002/proceeding/index.html
- PKI: 基礎と応用 (IW2001チュートリアル: 稲村 雄)
  - http://www.soi.wide.ad.jp/iw2001/slides/16/16-1/
- PKI関連技術情報 (IPA)
  - http://www.ipa.go.jp/security/pki/pki.html
- PKI関連RFC (IPA)
  - http://www.ipa.go.jp/security/rfc/RFC.html#13
- PKI相互運用技術WG「Challenge PKI 2002 とマルチドメインPKI」
  - http://www.jnsa.org/seminar/active/CPKI2002.pdf
- CACAnet福岡ー研究会の資料や認証関連のリンクー
  - http://cvs.cacanet.org/doc/index.html
- 5分で絶対に分かるPKI (@IT)
  - http://www.atmarkit.co.jp/fsecurity/special/02fivemin/fivemin00.html
- 電子署名導入指南 (@IT)
  - http://www.atmarkit.co.jp/fsecurity/rensai/elesign01/elesign01-1.html
- PKI基礎講座 (@IT)
  - http://www.atmarkit.co.jp/fnetwork/rensai/pki01/pki01.html

参考URL (Windows PKI関連)

- Windows 2000 Server ドキュメント (日本語)
  - http://www.microsoft.com/windows2000/ja/server/help/
- Windows 2000 公開キー基盤 (英語)
  - http://www.microsoft.com/windows2000/techinfo/howitworks/security/pkiintro.asp
- 暗号化 と PKI の基本 (英語)
  - http://www.microsoft.com/windows2000/techinfo/howitworks/security/cryptpki.asp
- Windows 2000 証明書サービス (英語)
  - http://www.microsoft.com/windows2000/techinfo/howitworks/security/windows2000csoverview.asp
- Windows XP Professional と Windows Server 2003 の PKI 拡張機能 (日本語)
  - http://www.microsoft.com/japan/windowsxp/pro/techinfo/planning/pkiwinxp/default.asp

参考URL (Windows PKI関連)

- Windows XP における自動更新およびダウンロード テクノロジの管理（日本語）
  - http://www.microsoft.com/japan/windowsxp/pro/techinfo/administration/manageautoupdate/
- The Cryptography API, or How to Keep a Secret（英語）
  - http://msdn.microsoft.com/library/en-us/dncapi/html/msdn_cryptapi.asp
- MSDN Library SDK Documentation “Cryptography”（英語）
  - http://msdn.microsoft.com/library/en-us/security/security/cryptography_portal.asp
- [MS02-050]証明書確認の問題により、ID が偽装される (Q329115)
  - http://www.microsoft.com/japan/technet/security/bulletin/MS02-050.asp
- Windows File Protection Old Security Catalog Vulnerability
  - http://www.science.org/secalert/WFP_Old_Security_Catalog_Vulnerability.txt
- Windows File Protection Arbitrary Certificate Chain Vulnerability
  - http://www.science.org/secalert/WFP_Arbitrary_Certificate_Chain_Vulnerability.txt

参考書籍

- 「PKI 公開鍵インフラストラクチャの概念、標準、展開」
  - C・アダムズ/S・ロイド 著、鈴木 優一 訳 ピアソン・エデュケーション ISBN 4-89471-248-2
- 「PKIハンドブック」
  - 小松 文子 他著 SRC ISBN 4-88373-142-1
- 「企業システムのためのPKI」
  - 塚田 孝則 著 日経BP ISBN 4-8222-8117-5
- 「Windows 2000 Server リソースキット3 分散システムガイド 上」
- 「Windows 2000 Server リソースキット4 分散システムガイド 下」
  - Microsoft Corporation 著 日経BPソフトプレス 多摩ソフトウェア（有）訳 NRIラーニングネットワーク（株）監修 ISBN 4-89100-156-9/ISBN 4-89100-168-2