

Vista, PKI, IE7

Kiyoshi Watanabe

Security Center of Excellence

Microsoft

はじめに

- Vistaは現在Beta2段階であり、本日の情報は最終リリース時と異なる可能性があります。

アジェンダ

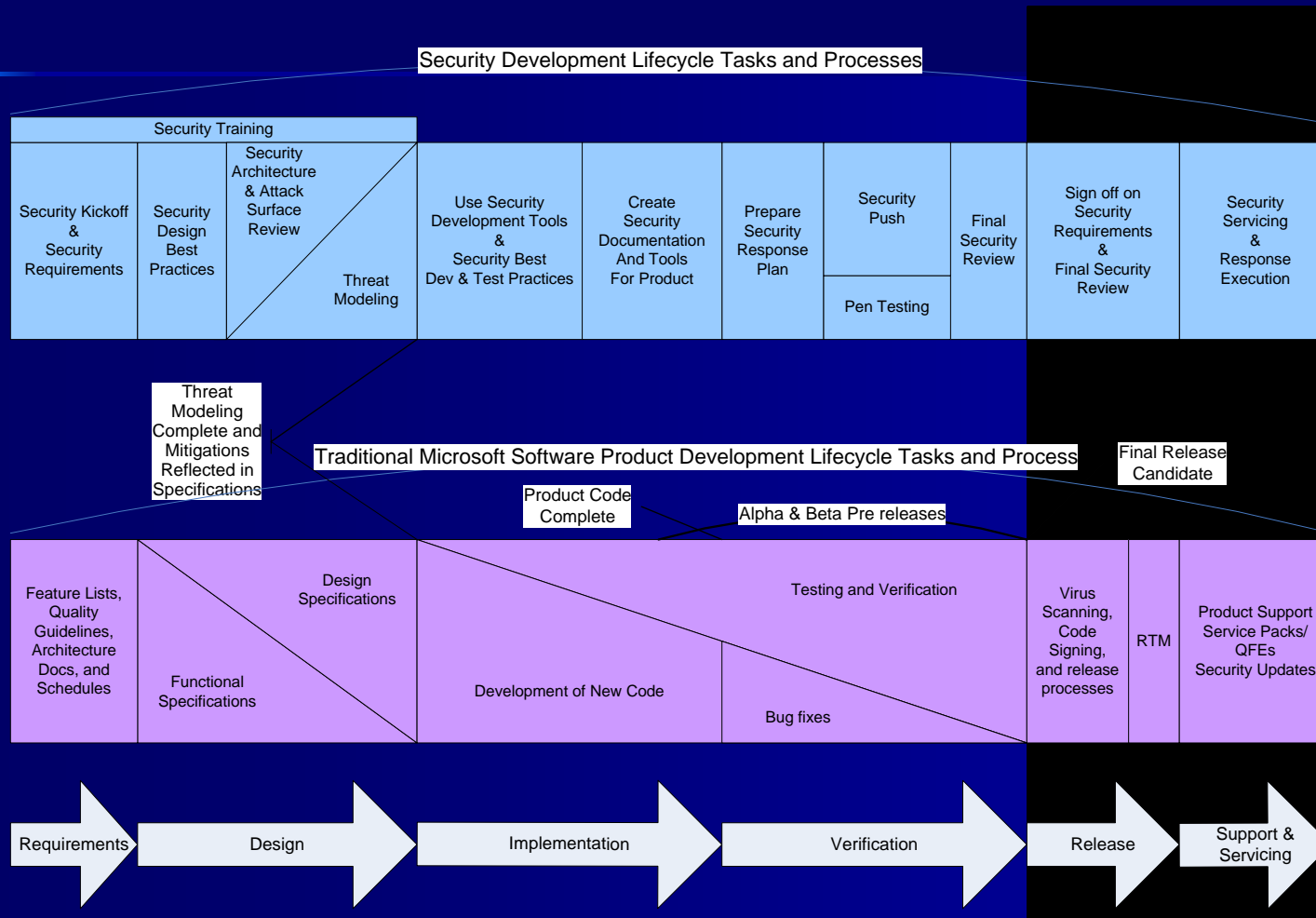
- Vista, IE7, PKI
- ルート証明書
- 失効機能
- Enrollment
- Credential ローミング
- 証明書サービス
- CNG

- Bit Locker
- Certificate Lifecycle Manager
- NAP
- IE7

Vistaの開発

- Engineering Excellence と SDL
 - セキュリティトレーニング
 - Security Advisorの設置
 - Threat Modelingの実施
 - セキュリティツールの利用
 - 最終セキュリティレビューの実施
 - その他

Vistaの開発



IE7の開発

■ Engineering Excellence と SDL



PKI

- PKI単体はソリューションではない
- PKIは要素技術
- アプリケーションを定義する必要あり

マイクロソフトのPKI 方向性

- PKIアプリケーションを可能とする製品の提供
 - S/MIME
 - ワイヤレスネットワーク
 - VPN
 - IPsec
 - EFS (Encrypting File System: 暗号ファイルシステム)
 - スマートカード
 - SSL/TLS
 - 電子署名

マイクロソフトのPKI 方向性

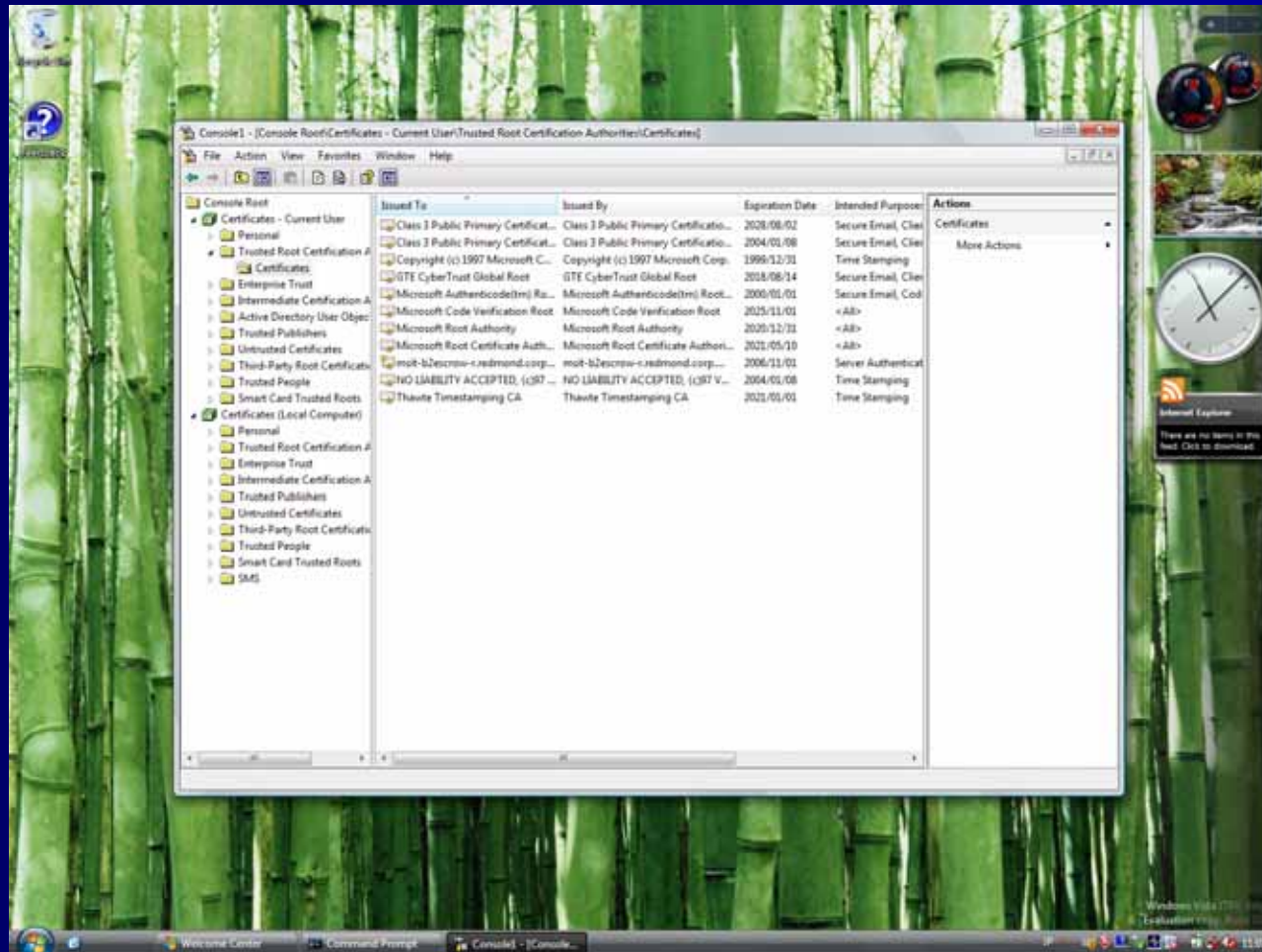
- クレデンシャル管理の向上
- 新しい\Certificate Enrollment APIとUI
- 証明書サービスの管理と展開の向上
- 失効機能の向上

ルート証明書

ルート証明書

- 最小限のルート証明書がプレインストール(crypt32.dll)
- 他の”認定”されたルート証明書は、証明書検証時にWUサイトへアクセスし、サイレントインストール
 - XP時でもこの動作は同様
- オフライン用に完全ルート証明書セットも用意される

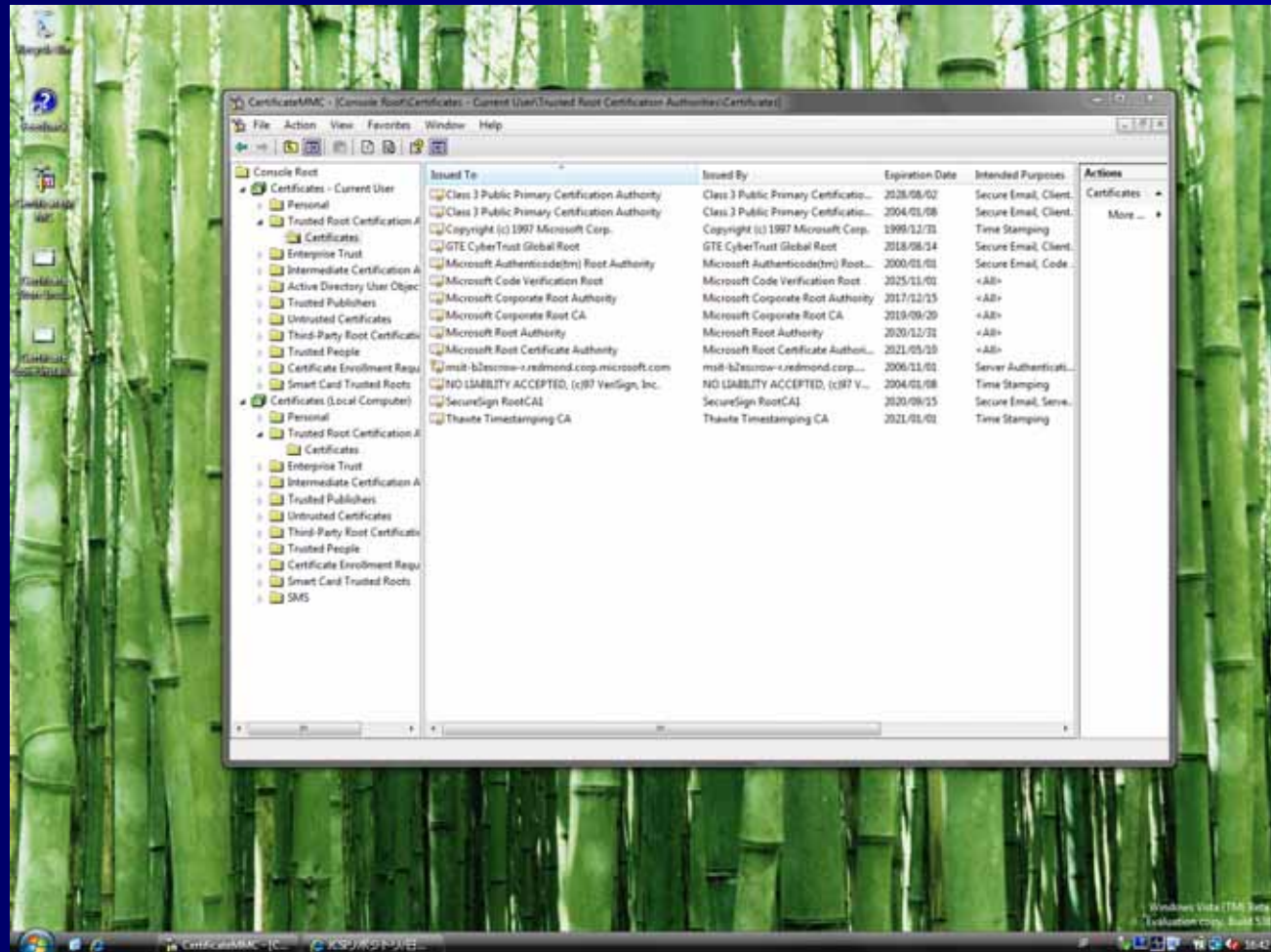
ルート証明書 (インストール直後)



2006/06/07

12

ルート証明書 (SSLサイト利用時)



2006/06/07

ルート証明書

■ 理由

– Visibilityの向上

■ 受け付けるルート証明書のみユーザに提示

- 200以上のルート証明書から、自分のルート証明書を目視でチェックするのは手間。例えばルート証明書のインポート時の目視チェック

– パフォーマンス

■ 200以上のルート証明書をメモリにロードするのを防ぐ

- 200ルート証明書は、1証明書2Kとし、20プロセス走るとし、4Mバイト何もしないのに、消費する

ルート証明書

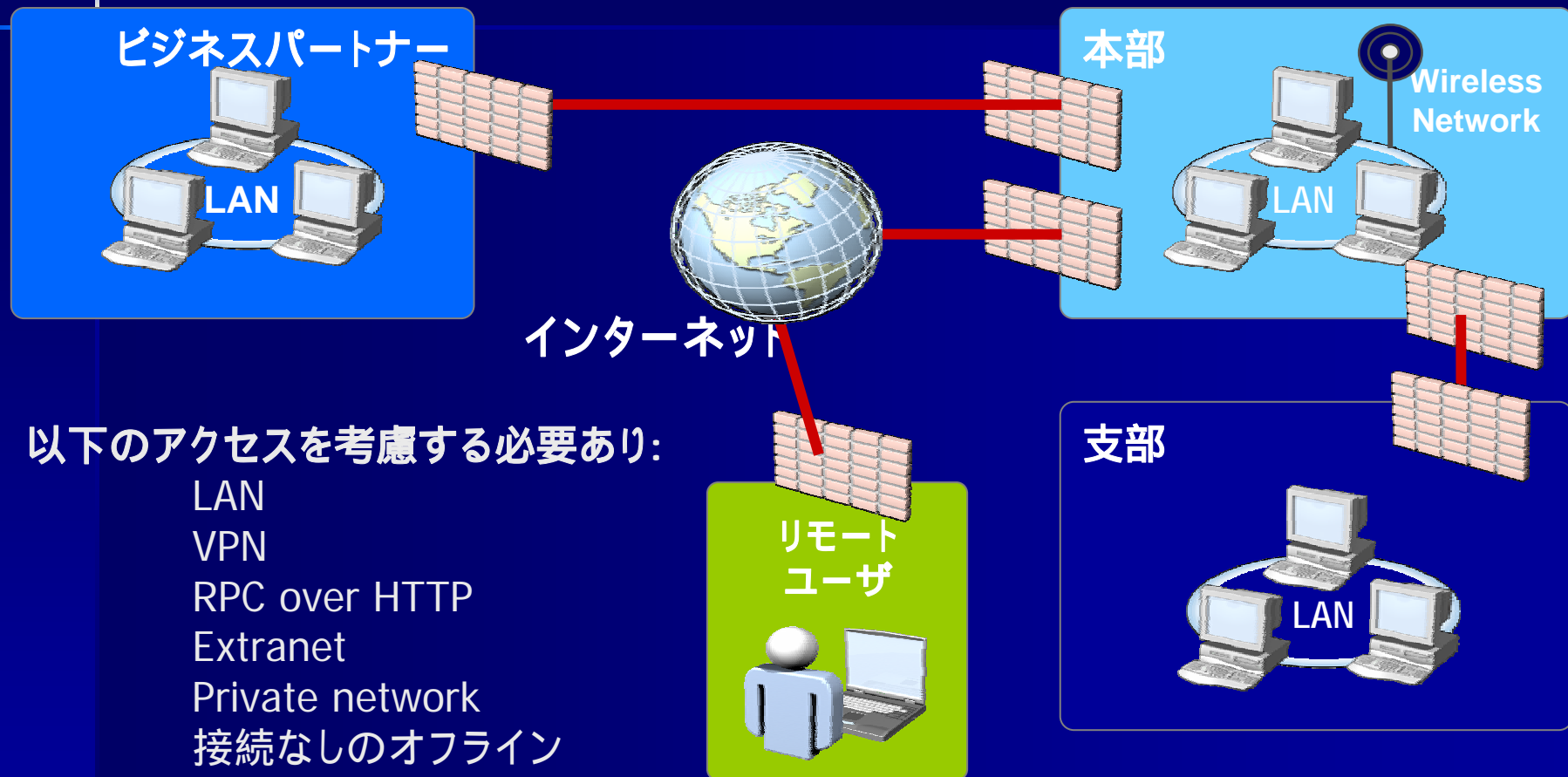
- Vista用にWindows Root Certificate Requirement が改定される
- 今後アナウンスされる予定

失効機能

失効機能の難しさ

- 失効機能は以前から悩ましい問題
 - XPまでのIEでは、失効はオフ
 - PKI屋からしてみれば、愚の骨頂と見える？
 - マイクロソフト、PKI知らないんじゃないの？
 - SEからしてみれば、懸案事項の種が飛躍的に増加する
 - 何のアプリケーションのためにどこに置けばいいの、どうやって管理するの、どうやって同期するの？ イントラ、インターネット、VPN、エキストラネット、パートナーネットワーク

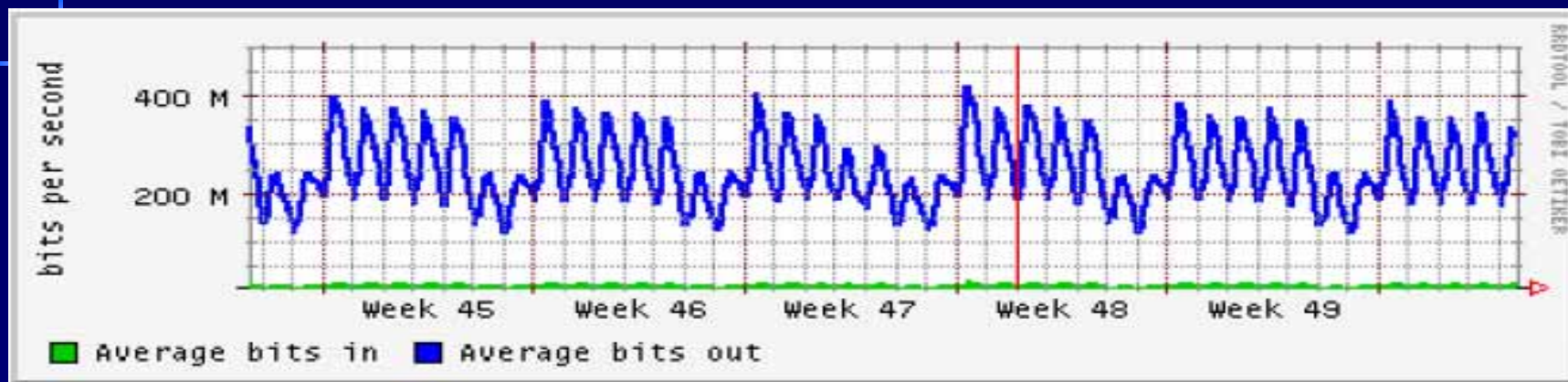
典型的なアクセスパターン



以下のアクセスを考慮する必要あり:

- LAN
- VPN
- RPC over HTTP
- Extranet
- Private network
- 接続なしのオフライン

失効機能の難しさ



参考資料: VeriSign (RSA 2005)

- コード署名用が90%
- リトライが発生するとサービスが悪化する
- OCSPは、CRLより、少ないバンド幅となるが、常に真ではない

マイクロソフトの経験

- IE3.02、オンにしたところ、IEが固まる
- Outlook 2000 S/MIME、オンにしたところ、しばしばフリーズする経験
 - 90秒のURLタイムアウトは長すぎる、15秒にしても長すぎる、但し短くすると、取得失敗回数が増加
 - 原因：
 - 署名検証をバックグラウンドで行い、署名検証が終了するまで、ブロックする
 - サーバがオフライン、サーバに到達が出来なかった、サーバにCRLがなかった等の運用ミス
 - CDPに複数記述され、イントラ用とインターネット用が併用して記述されている

マイクロソフトの経験

- Authenticate Code 対策としては、失効機能は、非常に重要なセキュリティ対策
- しばし署名検証時に問題が発生
 - アンチウイルスソフトが独自に定期的にチェック
 - プライベートネットワーク時にCRLが取得できない

デフォルトで有効にする？

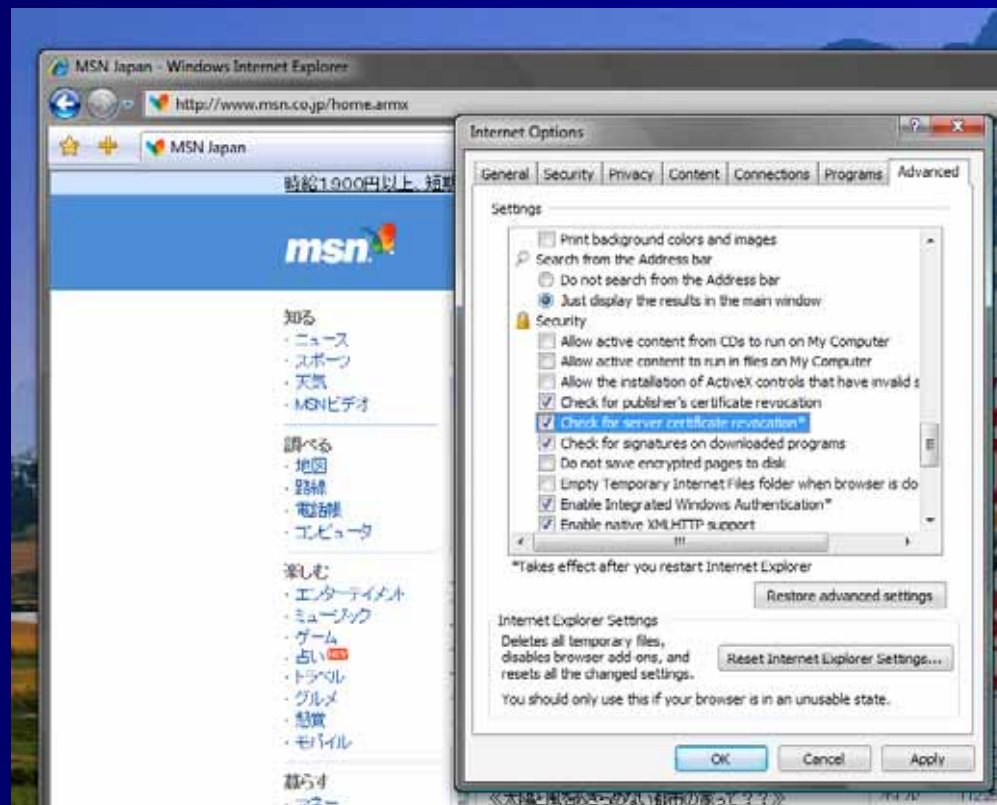
- ネットワークインフラとユーザのコスト増加
- OCSPを必須とするのか？
 - ブート時の検証は可能か？
 - オフラインユーザシナリオは？
 - ユーザがアクセス出来ない状況を許してくれるだろうか？
 - ユーザに対する保証レベルはどれぐらいにするのがよいのだろうか？

デフォルトで有効にする？

- 失効は、様々なソリューションが複雑に関与する不完全な世界での、完全なソリューションを求めている
- 鍵失効は、どれくらいCAにレポートされるのだろうか？
- 現行のHTTPSで危惧される“脅威”とは何だろうか？
- そもそもGrace Periodが存在するので、今起きている失効脅威からユーザを守ることはできるのだろうか？

Vistaでのゴール

■ デフォルト、オン(有効)



2006/06/07

24

Vistaでのゴール

- “It just works”
 - デフォルトオンは、望ましい設定であるが、すべてのシナリオに対応するため最適化されてはいない
- 脅威対策と使い勝手のバランス
- 通常バンド幅の考慮が必要となる (CA, インフラ担当)
- 例外時や緊急時の対応も必要

Vistaでの失効機能

デフォルトオンからの次のレベル

- OCSP クライアント
- TLS stapling 拡張
- HTTP 1.1 cache proxies
- Pre-fetch機能
- CRL, OCSPをメモリキャッシュからフラッシュするツール
- OCSP サーバ(Longhorn)

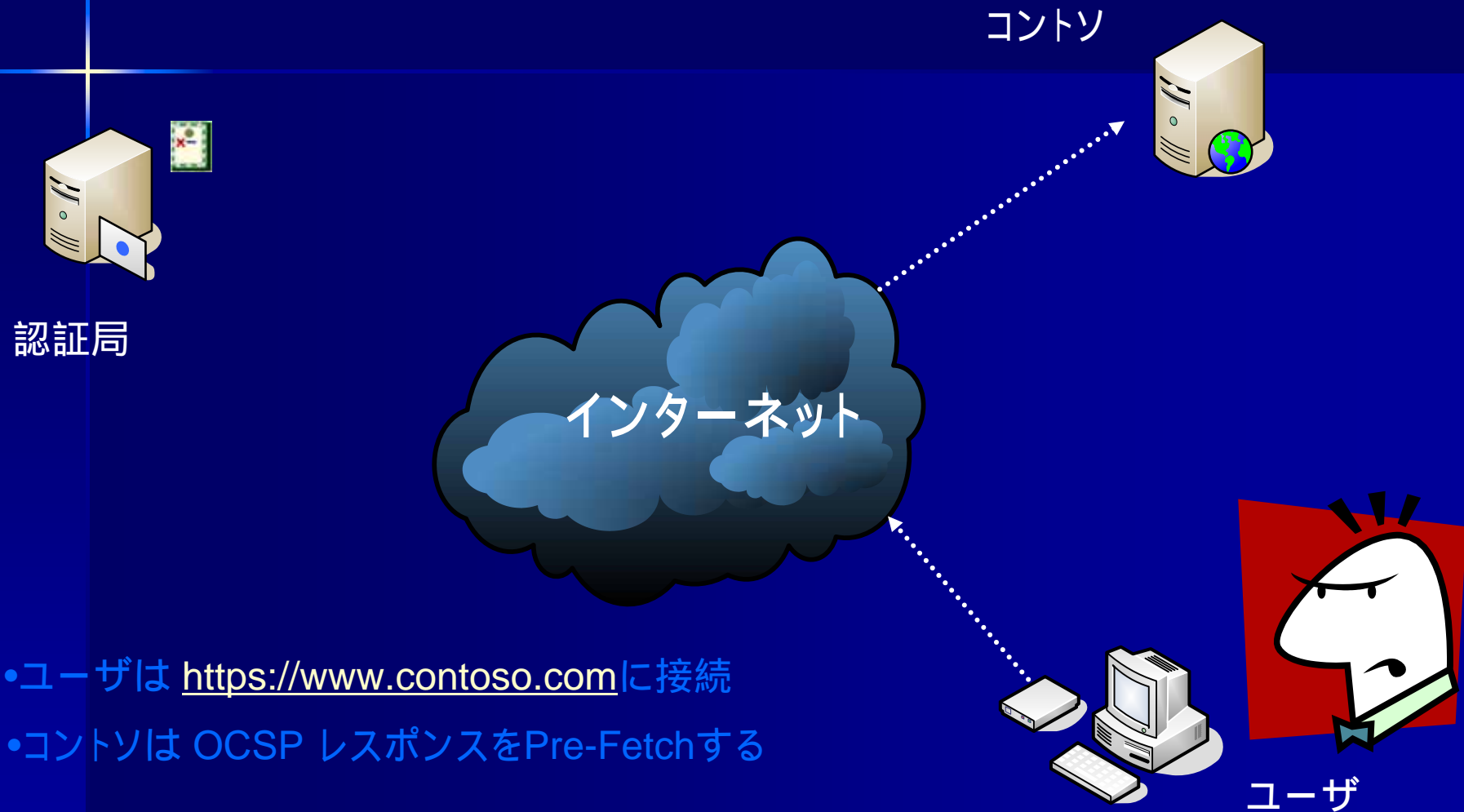
Vistaでの失効機能

■ TLS Stapling

- ステープリング(ホッチキス止め)？
 - RFC 3546 section 3.6
- TLSサーバが失効サーバとしての役割
- ユーザは、CA局に問い合わせるのではなく、TLSのハンドシェイク通信で、証明書リストとOCSPレスポンスを受け取る

Vistaでの失効機能

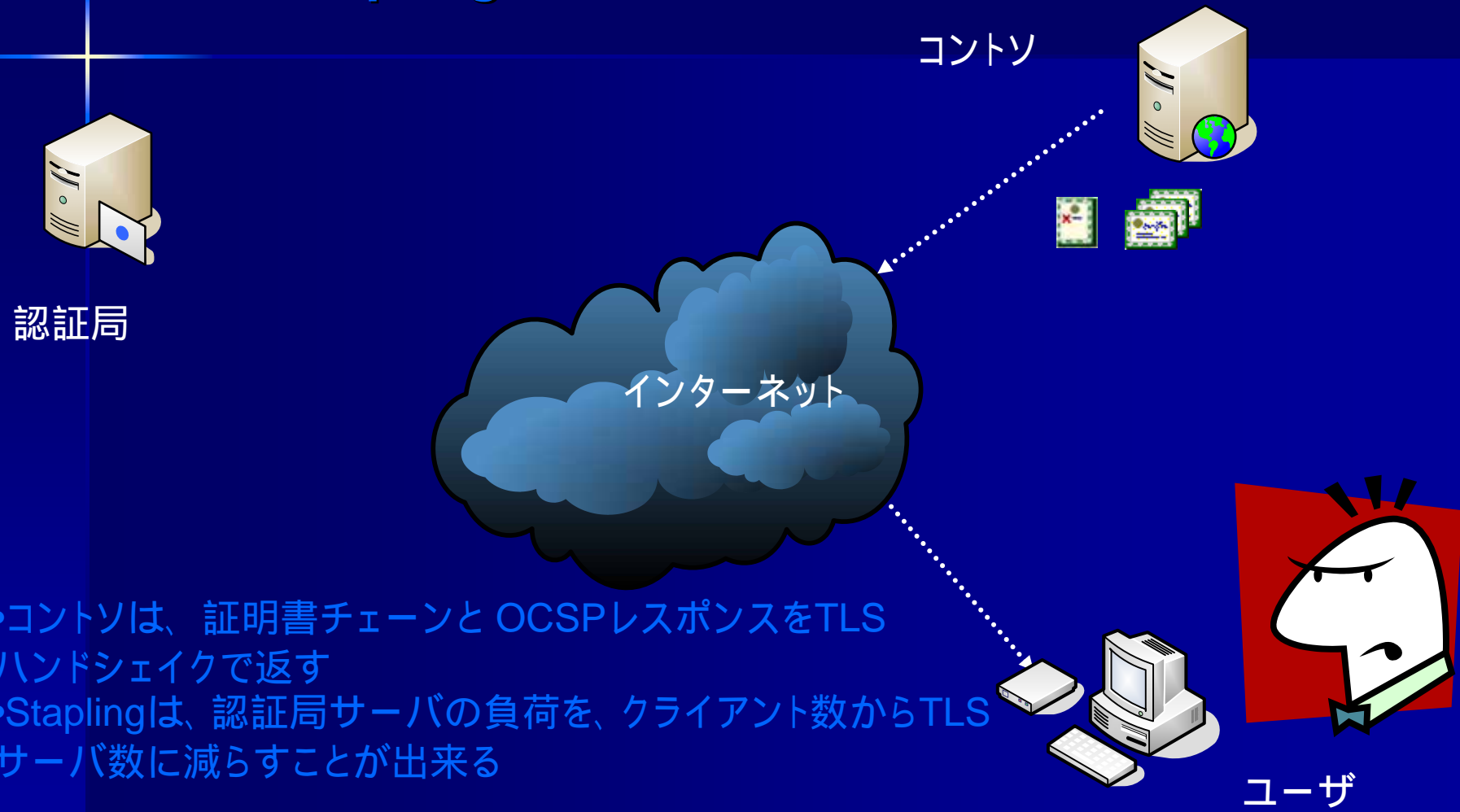
TLS “Stapling” 例



- ユーザは <https://www.contoso.com> に接続
- コントソは OCSP レスポンスをPre-Fetchする

Vistaでの失効機能

TLS “Stapling” 例



Vistaでの失効機能

TLS “Stapling” 例

- 注意点は、中間証明書は、取得できない。バックグラウンドでCA(CDP等の場所)から取得する必要がある。但し、中間証明書の失効情報は、少なく失効期間も長くなる。
 - 運用としての失効期間を考慮

Vistaでの失効機能

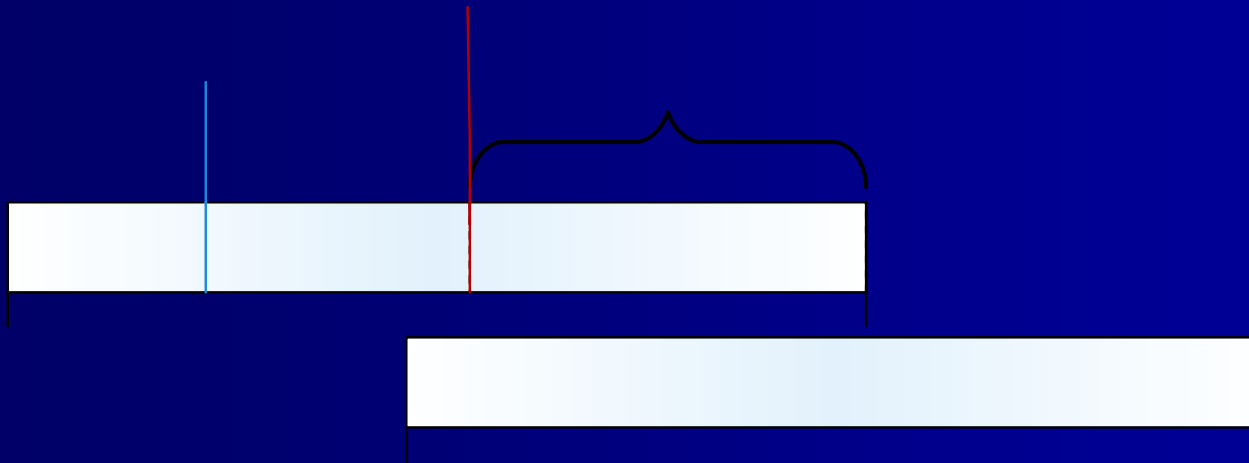
■ HTTP1.1 Proxy サポート

- Etag, cache control:max-age
- Expire, Last Modified(HTTP1.0)
- Etag:
 - クライアントがサーバに対して、条件クエリを送信することが可能(いつもダウンロードする必要がない)
- Max-age:
 - キャッシュの満期期間を記述
 - Pre-fetchを可能とする

Vistaでの失効機能

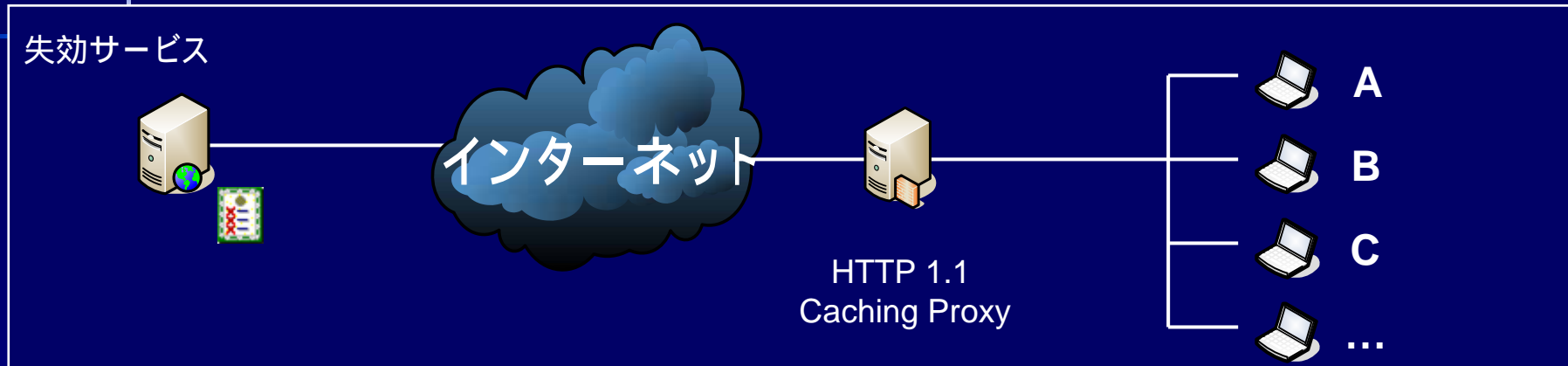
Pre-Fetch の仕事

- バックグラウンドで、クライアントは、nextの期待する発行時間と失効期間の間で、ランダムな時間を設定し、Pre-Fetchする



Vistaでの失効機能

HTTPS 1.1 Proxyサポート



1.6/7/2006, 8:00amにCRL要求

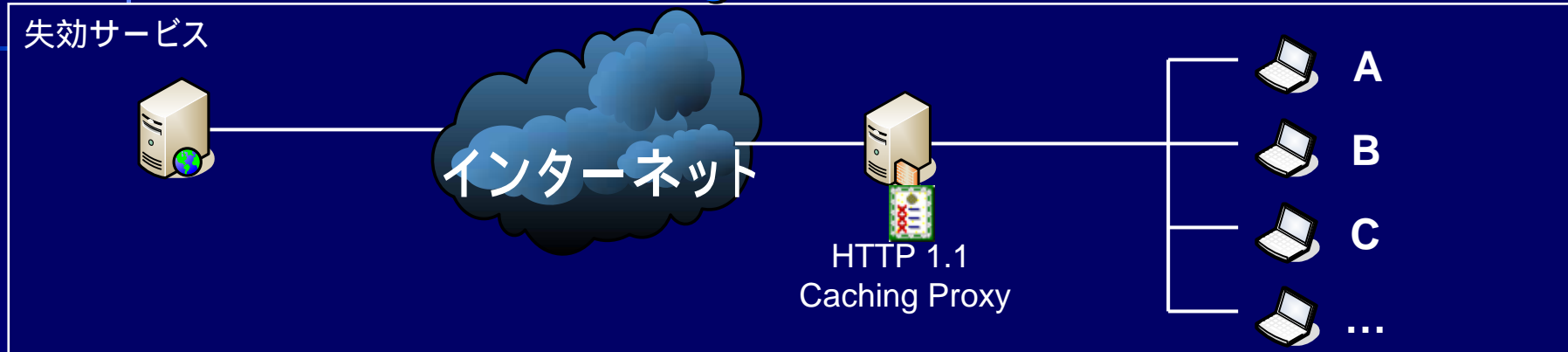
2.失効Revocationサービスは次のヘッダをHTTP responseとして返す:

```
HTTP/1.1 200 OK
Content-Length: 1653
Date: Wed, 07 Jun 2006 08:00:00GMT
Content-Type: application/pkix-crl
Last-Modified: Wed, 07 Jun 2006 00:00:00 GMT
ETag: "39a0-28d-4029bce7"
Expires: Tue, 13 Jun 2006 23:59:59 GMT
Cache-Control: Max-age = 86400
```

2006/06/07

Vistaでの失効機能

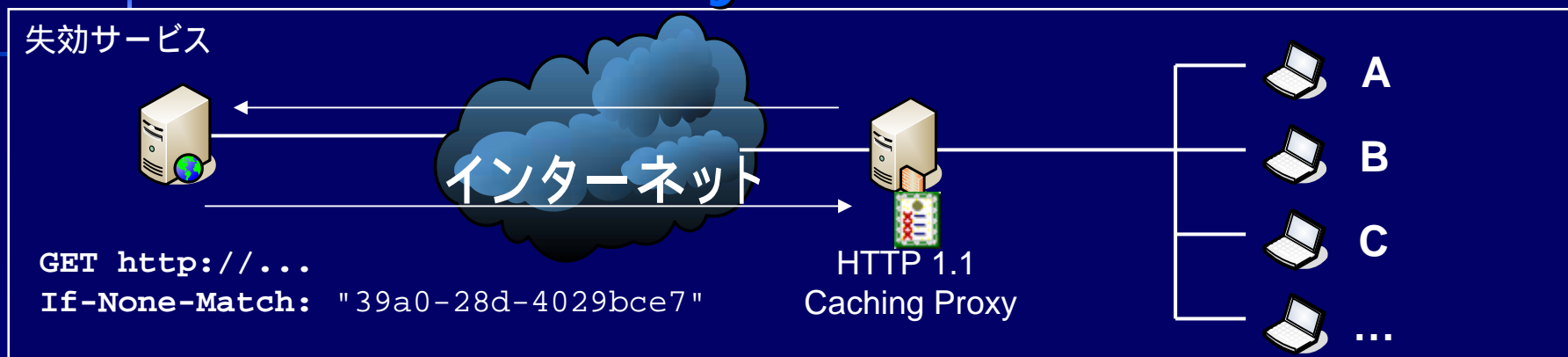
HTTPS 1.1 Proxyサポート



3. HTTP ProxyはCRLをキャッシュし Aに戻す
4. Bは、CRLを1時間後に要求、Proxyは、CRLを1日以下キャッシュするので、proxyは、そのキャッシュコピーをBに返答し、失効サービスにはアクセスしない。

Vistaでの失効機能

HTTPS 1.1 Proxyサポート



5. C は2日後にCRLをリクエスト。失効サービスに問い合わせしてから1日以上経っているため、proxyは、失効サービスに対して条件GETを送信

6.失効サービスは、CRLが更新されていなかったため、更新されたヘッダのみ返信

```
HTTP/1.1 304 Not Modified  
Date: Fri, 09 Jun 2006 9:00:00GMT  
ETag: "39a0-28d-4029bce7"  
Cache-Control: Max-age = 86400
```

Vistaでの失効機能

CRL vs. OCSP

- Windowsは常にキャッシュされたもの、又はStapled OCSP Responseを優先
- ネットワーク接続が必要とされ、CRL及びAIAが存在すると、
 - 全てのOCSP URLにアクセス、そして全てのCRL URLにアクセス
 - Networkタイムアウトは、1URL,15秒

Vistaでの失効機能

Call for Action

- HTTPを利用(LDAPではなく...)
- KISSの原則、1OCSP,1CRLで何処からでもアクセス可能なインフラデザイン
- 失効期間をオーバーラップさせ、Pre-fetchの利用
- Light-weight OCSPの利用
- ブラウザやサーバでのStaplingの対応

Enrollment

Advanced Enrollment

- Xenroll と Scrdenrl はリタイヤ
 - 使いにくい
 - メンテナンスしにくい
 - コスト高

Advanced Enrollment

- 明快な定義されたクラス階層、生成と管理インターフェイスが含まれる

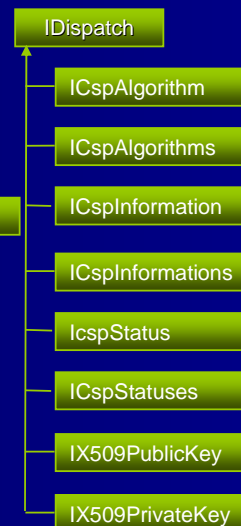
Request Classes



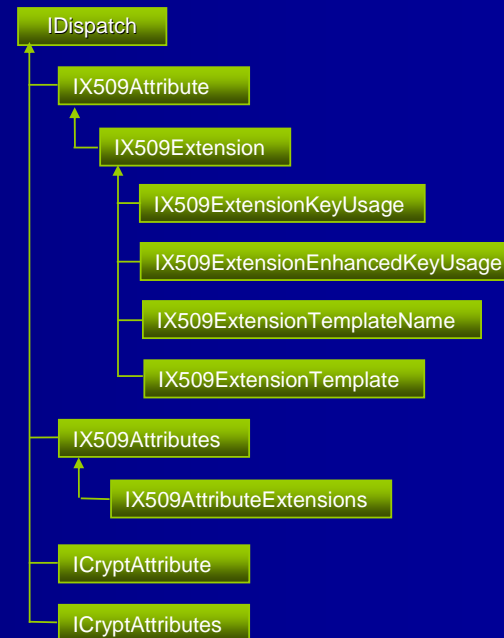
Enrollment Classes



Crypto Classes



Attribute Classes



Credential ローミング

Credential ローミング

■ PKIの痛いところ

- 証明書と秘密鍵は、マシーンと紐づくため、違うマシーンで、ログオンすると？
 - 違うマシーンで行うためには、改めて証明書と秘密鍵をインストールする必要あり

■ 現状のオプション

- スマートカード
- User Profileのローミング

Credential ローミング

解決方法

- Credential ローミングサービスで全てのクレデンシャルをアクティブディレクトリ (AD)機能で配信
 - 以下のアプリケーション展開を助ける
 - S/MIME
 - クライアント認証
 - スマートカード
 - クラスタサーバに対する展開も助ける

証明書サービス

証明書サービス

- SCEPのサポート
- MOMとの統合(2005 Management pack)
 - Events
 - Perfmon Counters
 - MOM scripts
- UI向上

CNG

CryptoNextGen

CAPIの次バージョン

- AES
- ECC
- SHA2ファミリー
- CNGは、FIPSやCommon Criteriaの Requirementsを満たす(Strong IsolationとAuditing)

Bit Locker

Full Volume Encryption

<http://www.microsoft.com/technet/windowsvista/security/bitlockr.mspx>

BitLocker

■ 脅威

- ラップトップが盗まれるたり、失くす可能性あり -> そこから情報漏えい
- SYSKEY (他の鍵を作るためのWindows Key)がアタックを受ける

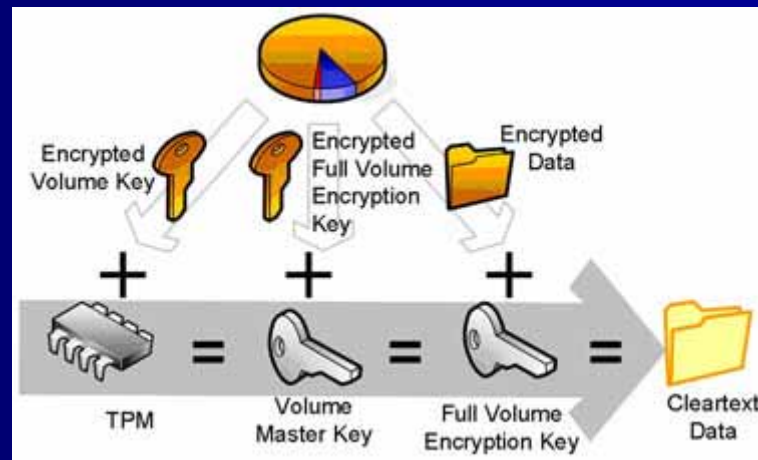
■ 解決方法

- TMP1.2を利用(無くてもよい)し、以下を実現
 - Full-Volume暗号
 - 初期ブートコンポーネント完全性検証

BitLocker

■ 通常の利用

- TPMk (StorageRootKey)がTPMに格納される
- VMk (Volume Master Key)がTPMのTPMkを利用し Seal/Unsealされる
- FVEk (Full Volume Encryption Key)がVMkを利用して、取り出される
- FVEkを利用して、Full Volume暗号を行う



BitLocker

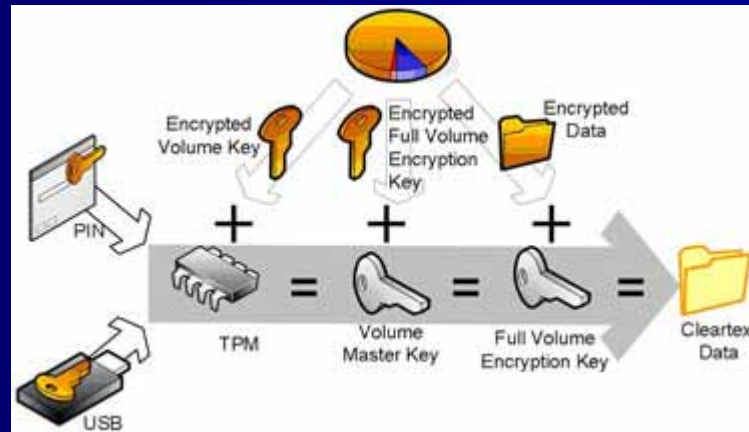
■ 認証を利用

– PIN

■ SHA256でハッシュ化。

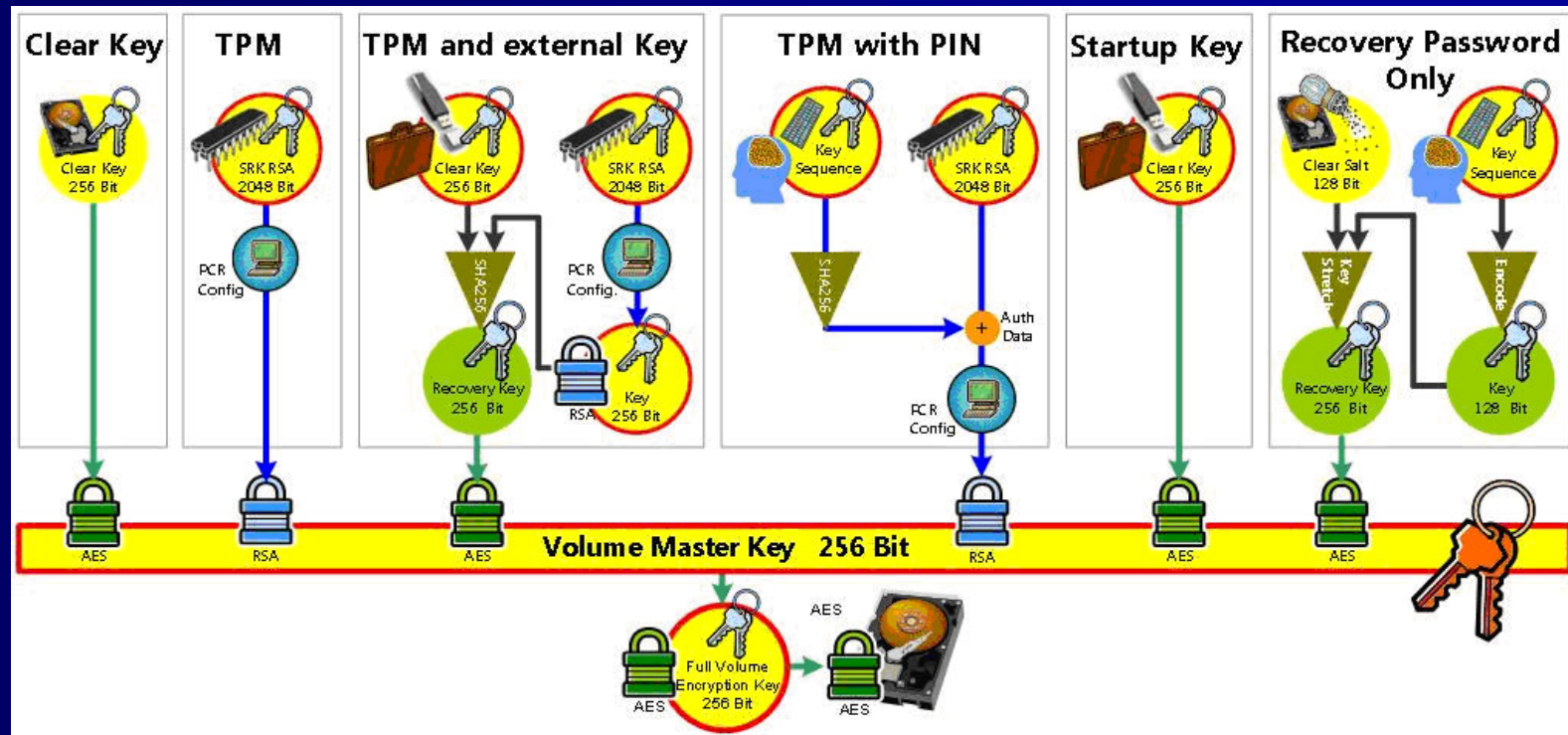
■ TPMでVMKをUnsealするため

– USBにStart-up Keyを保存しておく



BitLocker

■ 違う種類の鍵の関係

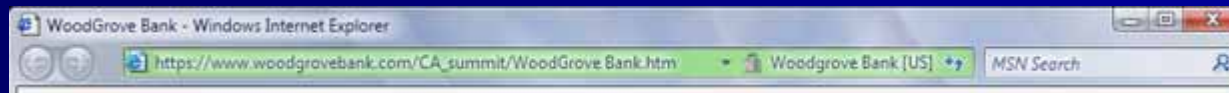


IE7

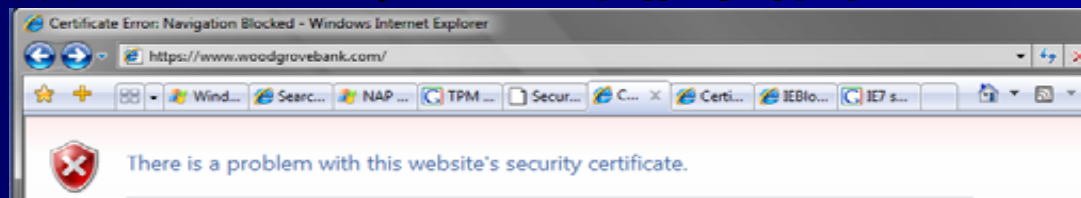
- SSL2.0はデフォルト、オフ
- HTTPSサイトにHTTPコンテンツがある場合、ブロック
- ユーザエクスペリエンスの向上
 - サイトのバックグラウンドチェックがどの程度で、SSL証明書が発行されるのかレベルがない
 - ABA
 - 認証局であるGeotrust, Verisign, Identrus, Comodo, Cybertrust, Go Daddy and X-Rampとも協調を図る

IE7

- high-assurance SSL certificate (OID)
 - グリーンバー



- ルート証明書が無い場合、
 - 続けるかどうかの確認画面



- 続けた後、赤いバーとなる



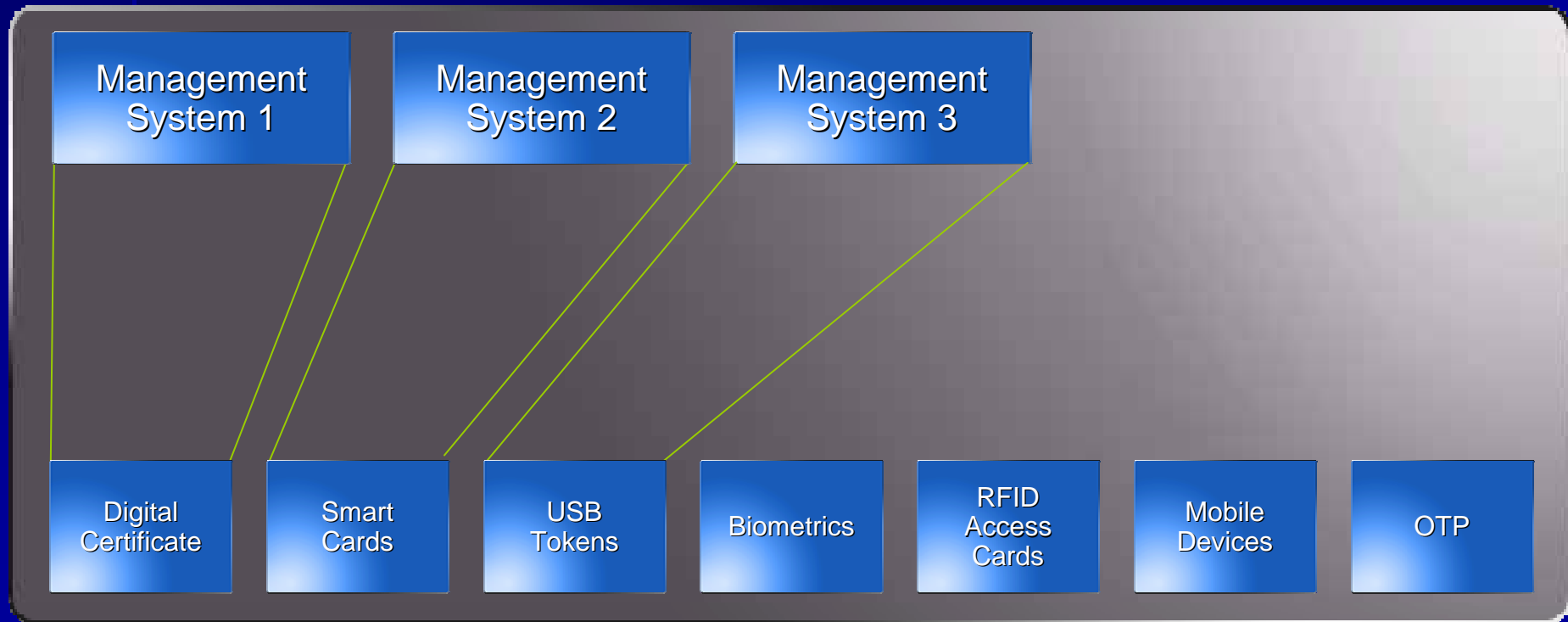
IE7

- **セキュリティユーザエクスペリエンス向上の関連記事**
 - **Web Browser Developers Work Together on Security (KDE)**
 - <http://dot.kde.org/1132619164/>
 - Internet Explorer, Mozilla/FireFox, や Opera development teams, KDE 4's Konqueror
 - **The business of CAs (Mozilla)**
 - <http://www.hecker.org/mozilla/business-of-cas>

Microsoft Certificate Lifecycle Manager

現状

- 各クレデンシャルに管理システムが必要

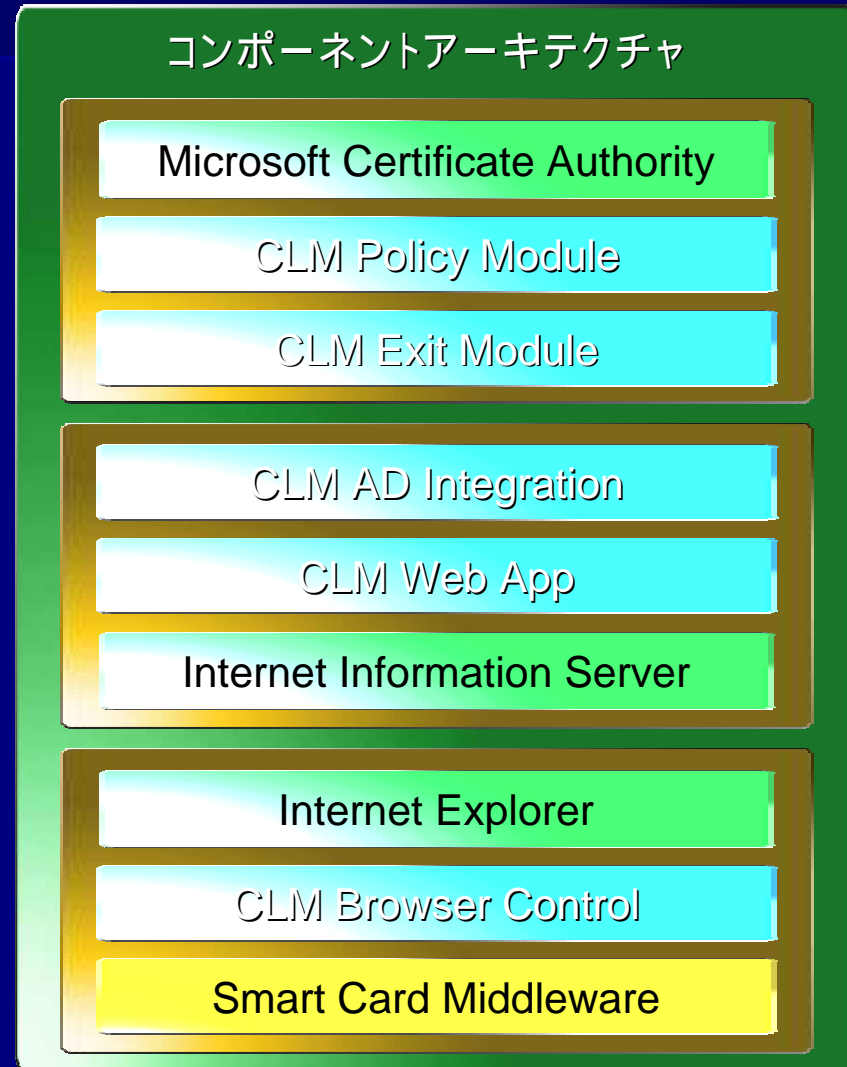
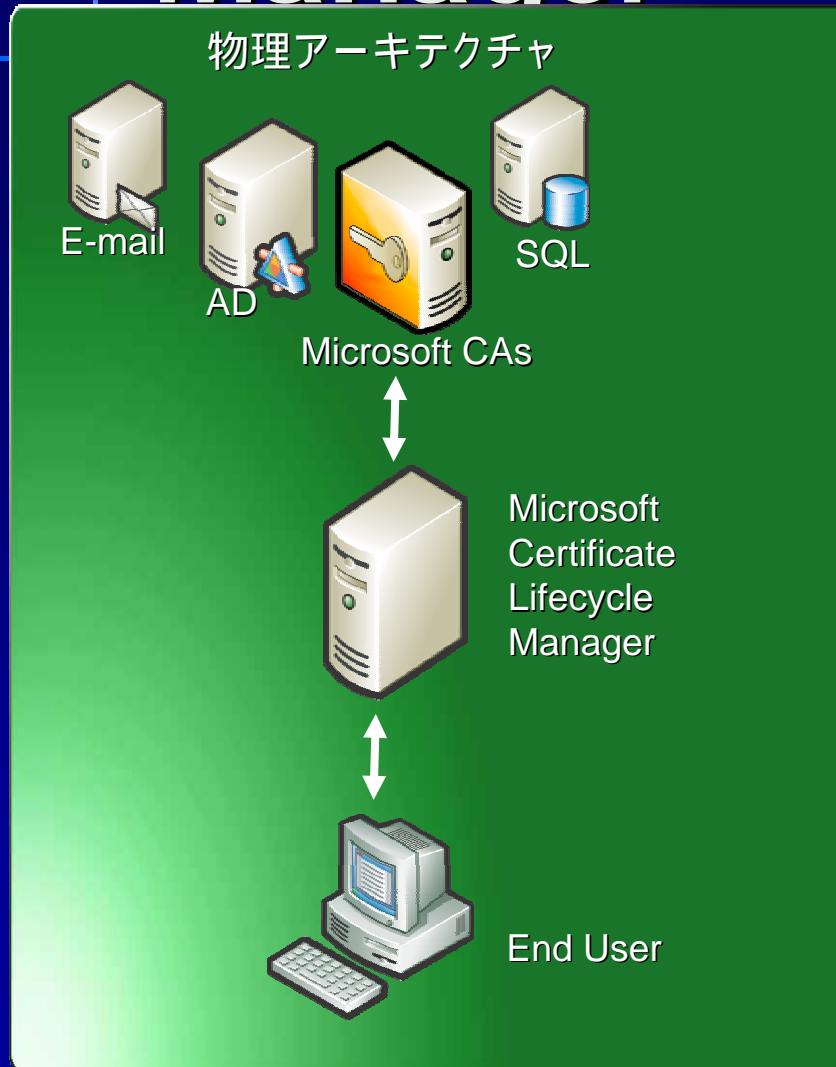


Certificate Lifecycle Manager

■ 機能

- 証明書とスマートカードの統一管理システム
- ワークフローに基づく管理機能
- 監査機能
- 既存のシステムと連携(AD, MSCA)

Certificate Lifecycle Manager



NAP

ネットワークアクセス保護

<http://www.microsoft.com/technet/itsolutions/network/nap/naparch.mspx>

■ PKIはどこに利用

- Health Certificateを発行し、システムの健康状態(☺)の検証後、アクセス許可用に発行される
- IPsecの認証用

リリースまでの道

Beta1

- ▶ 限られた方へレビュー
- ▶ 最小限の広報

Beta2

- ▶ 公開ベータ
- ▶ 何万のダウンロード
- ▶ お客様への展開広げる
- ▶ パートナー、フィールドのイベント

RTM

▶ リリース

関連資料

- <http://www.microsoft.com/japan/windowsvista/default.aspx>
- <http://download.microsoft.com/download/4/a/b/4abb4432-5b51-4de2-a0e5-f69b1f250c51/SEC305.ppt>

Q&A

2006/06/07

64

Microsoft[®]

Your potential. Our passion.[™]

© 2006 Microsoft Corporation. All rights reserved.

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