

Windows, Internet Explorer セキュリティのいま



日本マイクロソフト
セキュリティ レスポンス チーム
セキュリティ プログラム マネージャー
村木 由梨香



村木 由梨香

日本マイクロソフト セキュリティ レスポンス チーム
セキュリティ プログラム マネージャー

• 略歴

- Active Directory, Network, Crypto, PKI 関連を専門とした Windows エンジニアを経て現職。
- セキュリティの意識向上活動、インシデント対応に従事
- CRYPTREC 暗号技術活用委員会運用ガイドライン WG 委員

• 執筆・講演

- 日本のセキュリティ チーム 公式ブログ
 - <http://blogs.technet.com/b/jpsecurity/>
 - セキュリティ、証明書、脆弱性緩和ツール EMET など、セキュリティについて解説
- マイクロソフト セーフティとセキュリティ センター「ゆりか先生のセキュリティひとくち講座」
 - <http://www.microsoft.com/ja-jp/security/msy/default.aspx>
 - 身近なセキュリティ問題を取り上げ、安全な IT 生活を送るためのヒントを提供
- MSN「ゆりか先生の早わかりセキュリティ」
 - <http://www.msn.com/ja-jp/news/microsoft/information>
 - 初心者が気軽に楽しめるようなセキュリティのコラム
- 翔泳社 エンタープライズジン 連載「間違いだらけのサイバー攻撃対策」
 - <http://enterprisezine.jp/article/corner/280/>
 - IT プロ向けにセキュリティ運用について解説したコラム



Agenda

- **SSL/TLS & 証明書 in Windows/Internet Explorer**
- **安全性を高める機能**
 - ルート証明書更新プログラム・証明書信頼リストの自動更新
 - SmartScreen と Bing Webmaster Tool による不正証明書の検出強化
- **より安全な環境へ**
 - 危殆化したアルゴリズムからの移行推奨
- **まとめ**

Agenda

- **SSL/TLS & 証明書 in Windows/Internet Explorer**
- **安全性を高める機能**
 - ルート証明書更新プログラム・証明書信頼リストの自動更新
 - SmartScreen と Bing Webmaster Tool による不正証明書の検出強化
- **より安全な環境へ**
 - 危殆化したアルゴリズムからの移行推奨
- **まとめ**

HTTPS サイトを閲覧する

ブラウザー
アクセス
(Internet Explorer)

SSL/TLS
(Windows, Schannel)

証明書検証
(Windows, Crypto)

- 信頼チェーン検証
- 失効確認(CRL, OCSP)

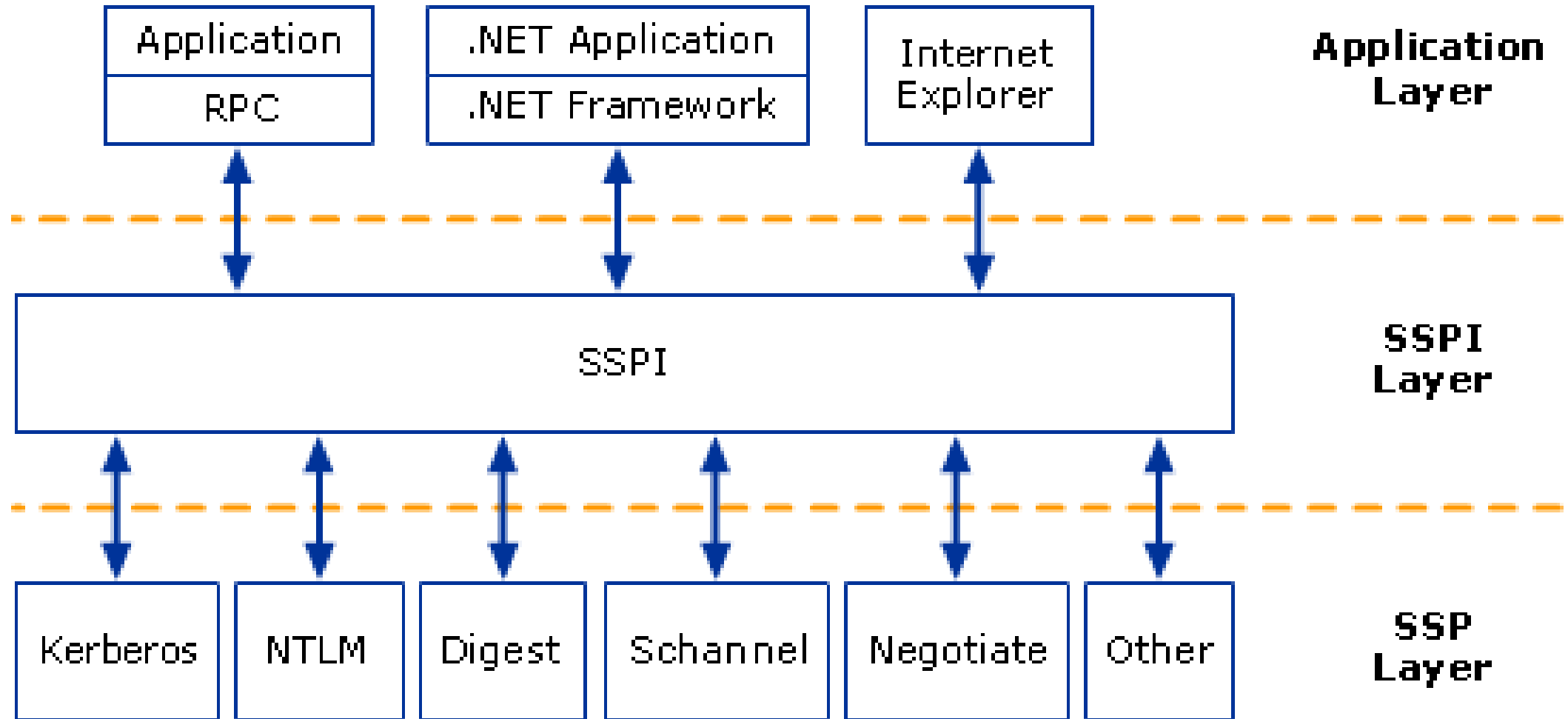


- SSL/TLS
- Cipher Suites



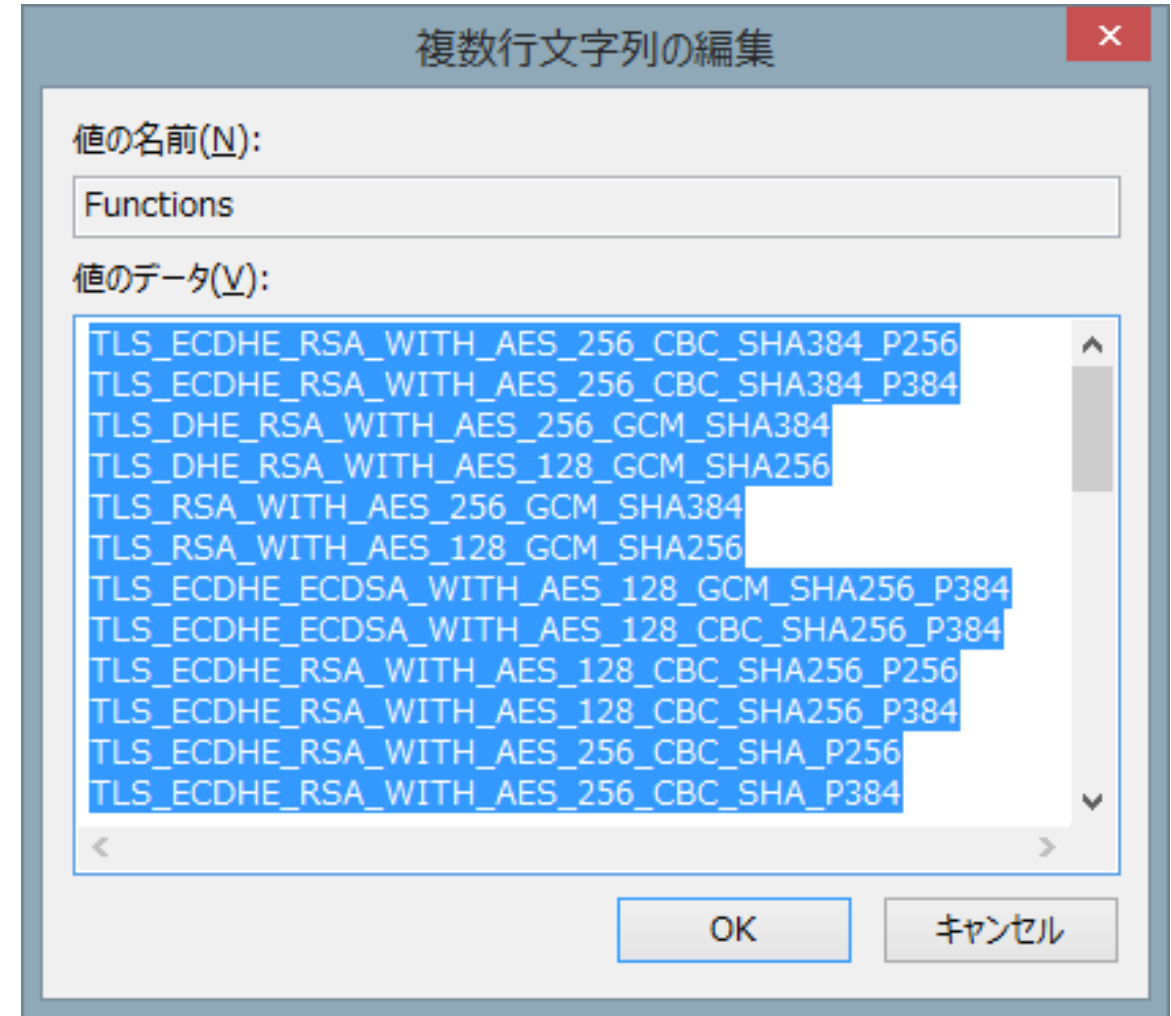
Security
Response
Team

SSL/TLS Architecture



利用している暗号スイートを確認する方法

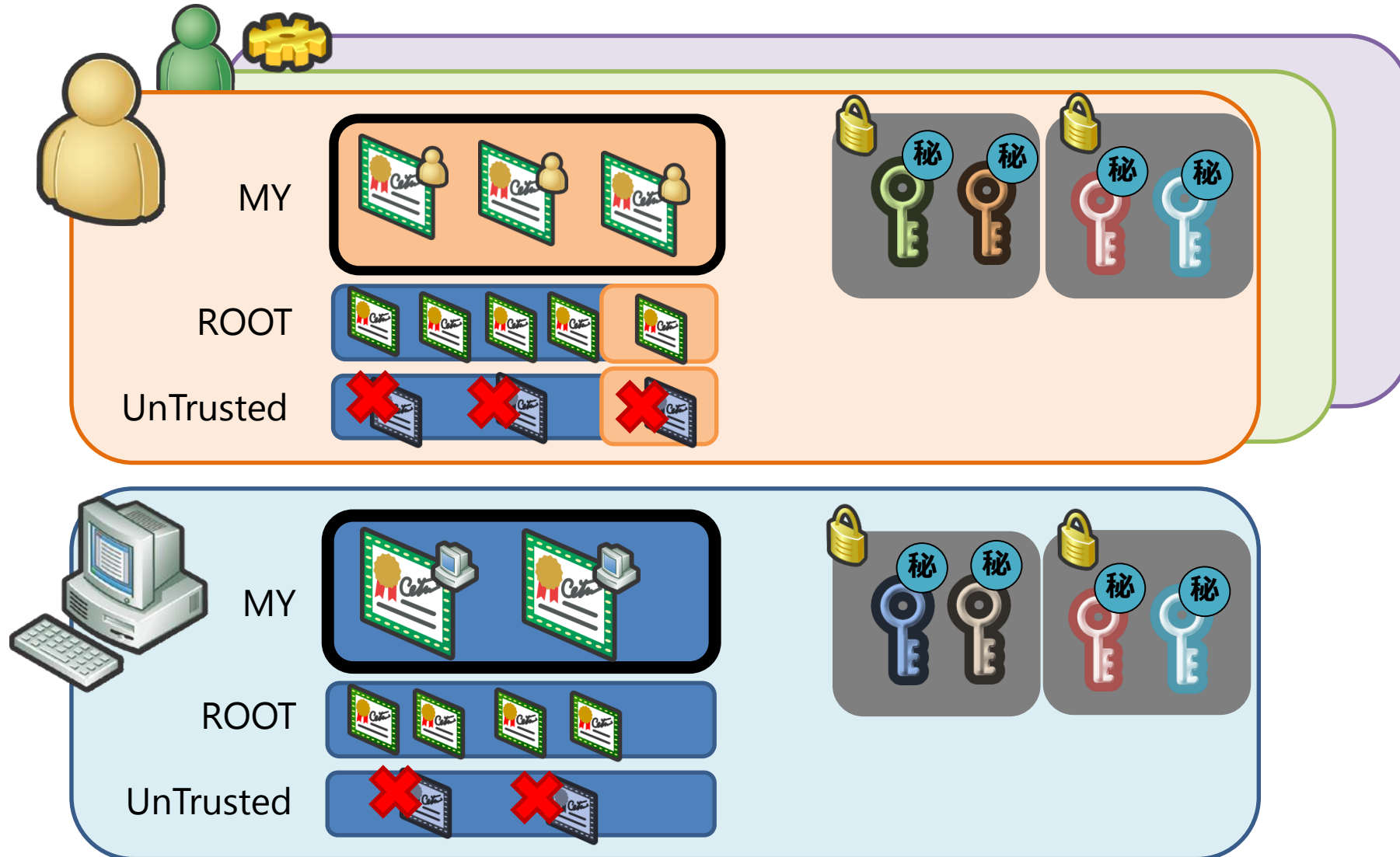
- 対象: Windows Vista/Windows Server 2008 以降
- レジストリ:
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Cryptography¥Configuration¥Local¥SSL¥00010002¥Functions
- 参考: Cipher Suites in Schannel
([http://msdn.Microsoft.com/en-us/library/windows/desktop/aa374757\(v=vs.85\).aspx](http://msdn.Microsoft.com/en-us/library/windows/desktop/aa374757(v=vs.85).aspx))



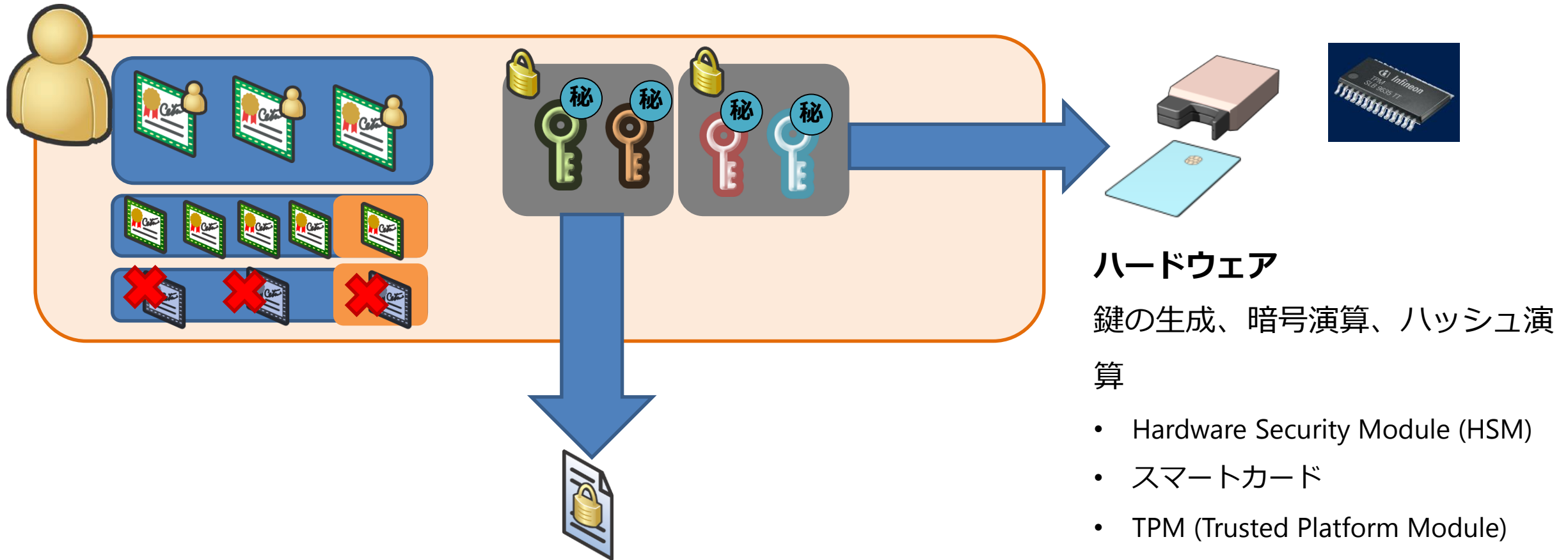
SSL/TLS の暗号化スイートを管理するには

- **グループ ポリシーで利用順位を決める**
 - 対象: Windows Vista, Windows Server 2008 以降
 - [コンピューターの構成]、[管理用テンプレート]、[ネットワーク] の順に展開し、[SSL 構成設定] [SSL 暗号化スイートの順序]
 - 注意: 1023 文字まで
- **レジストリで利用可能なアルゴリズムを制限する**
 - 対象: Windows Server 2003 以降
 - HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Ciphers¥
 - 参考: 特定の暗号化アルゴリズムおよび Schannel.dll のプロトコルの使用を制限する方法 (<http://support.microsoft.com/ja-jp/kb/245030>)

証明書・鍵 Architecture



鍵の保存

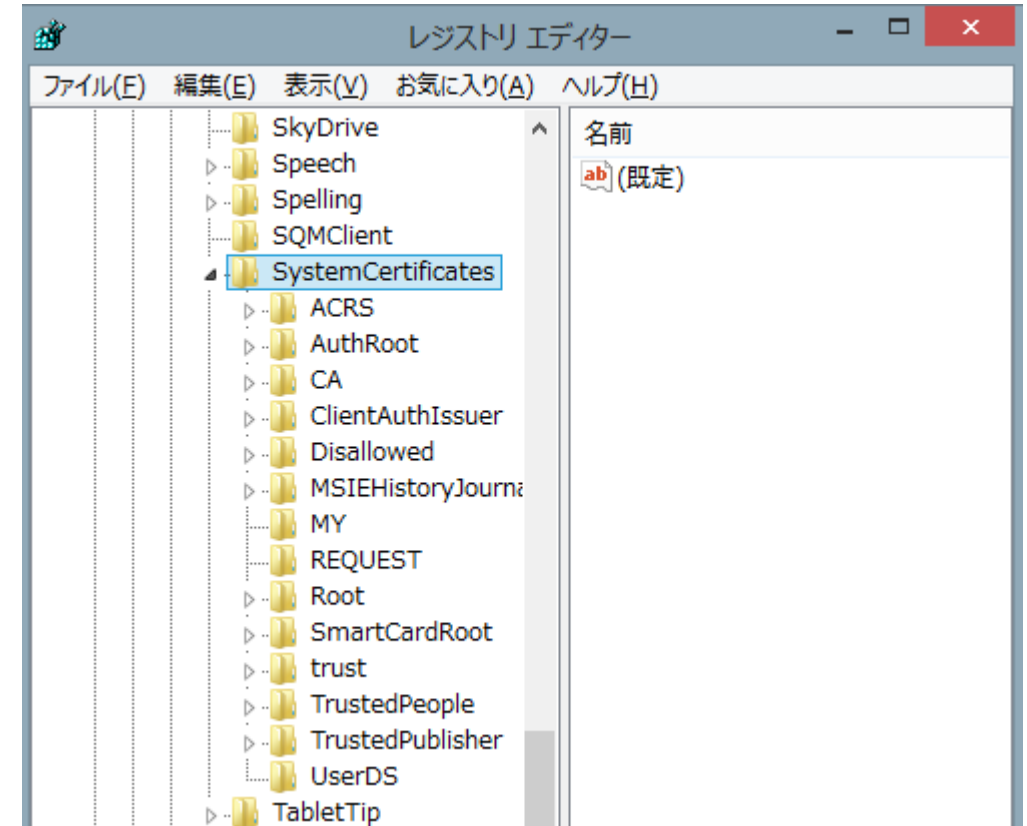
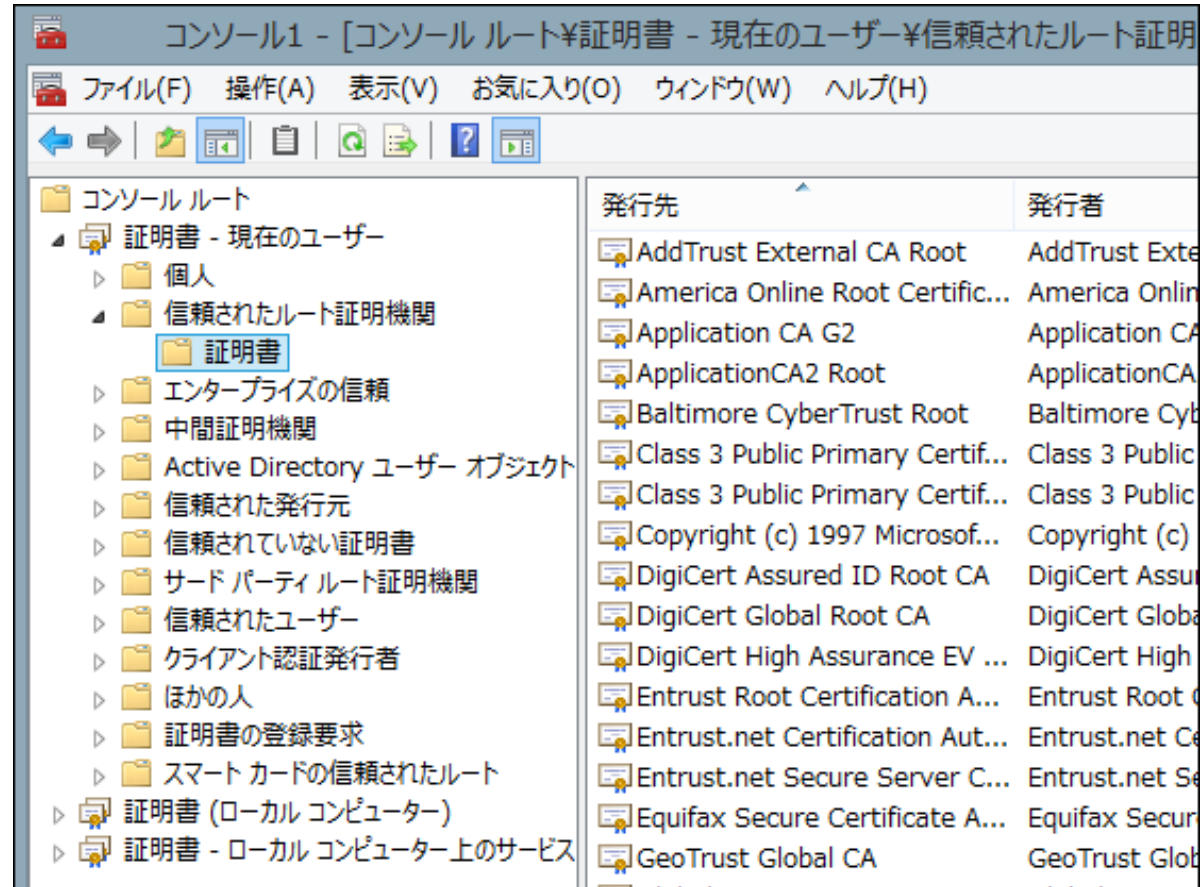


ソフトウェア

- プロファイル内に格納
- 「鍵コンテナ」はファイル
- データ保護 API による保護



信頼する証明書・信頼しない証明書とは



証明書の管理

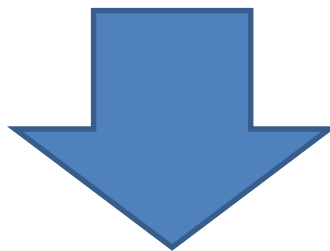
- **グループ ポリシーを利用する**
 - [コンピューターの構成] - [Windows の設定] - [セキュリティの設定] - [公開キーのポリシー]
- **Certutil コマンドを利用する**
 - Windows Vista/Windows Server 2008 以降標準
 - 信頼されるルート CA 証明書を追加する
 - Certutil -addstore root 証明書ファイル名
 - 信頼されるルート CA 証明書を表示する (コンピューター)
 - Certutil -store root

Agenda

- SSL/TLS & 証明書 in Windows/Internet Explorer
- 安全性を高める機能
 - ルート証明書更新プログラム・証明書信頼リストの自動更新
 - SmartScreen と Bing Webmaster Tool による不正証明書の検出強化
- より安全な環境へ
 - 危殆化したアルゴリズムからの移行推奨
- まとめ

多層のセキュリティ機能

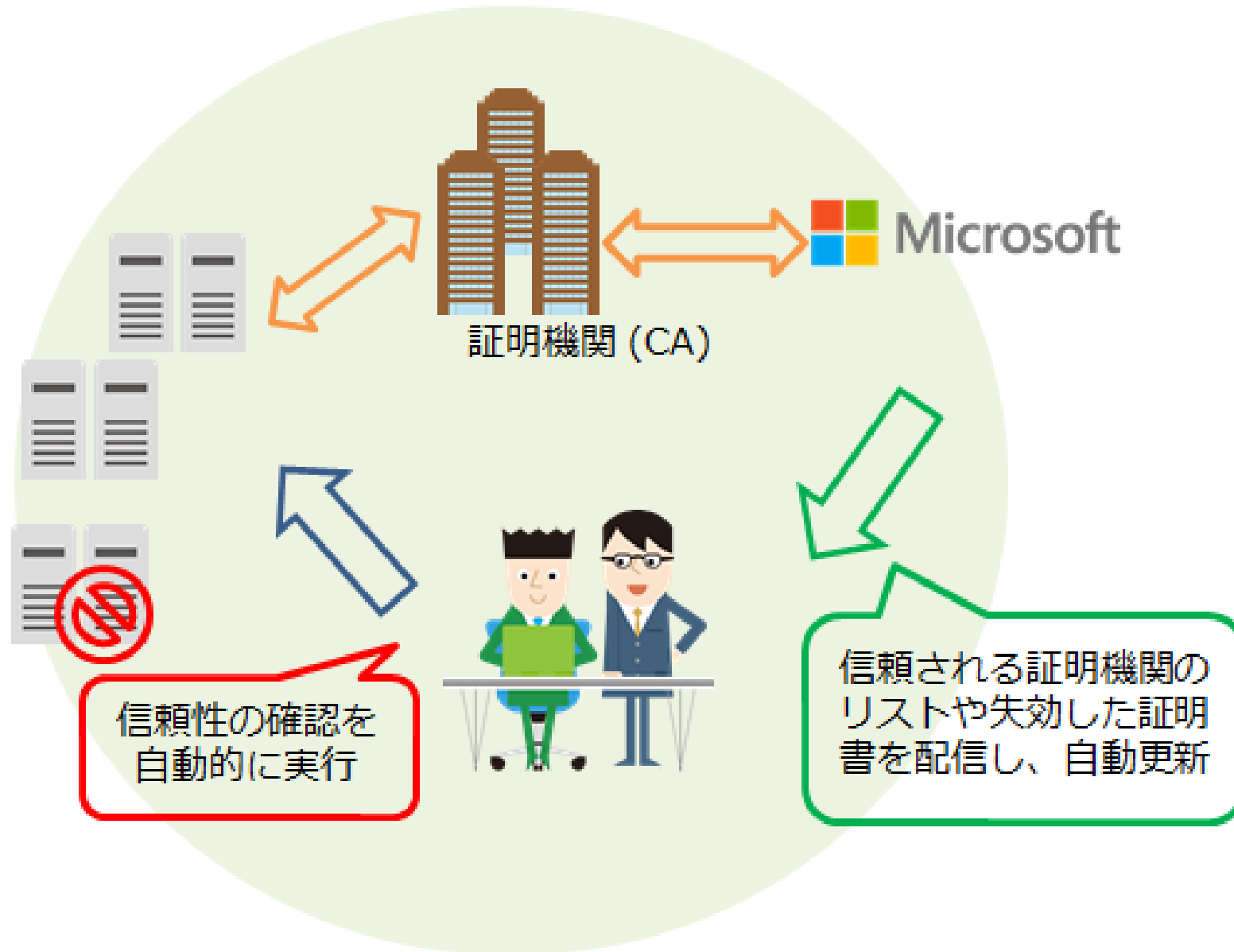
- 「信頼できる証明機関」とは？
- 不正証明書な証明書から保護するには？
- 複雑化する脅威から保護するには？



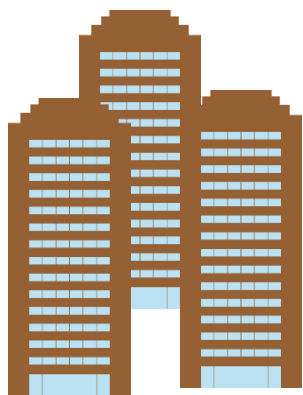
様々な機能や連携により多層的に安全性を高めていく必要がある



パブリック証明書の配布



ルート証明書プログラム・信頼リストの更新



証明機関 (CA)



Microsoft



Windows Update サイトから同期し
自動更新

インターネット環境



Windows Update サイト
から同期

DMZ



FILE/HTTP で
リストを配布し
自動更新

非インターネット環境



Security
Response
Team



証明書リストの更新機能

	インターネット環境		非インターネット環境 (*4)	
	信頼証明書	非信頼証明書	信頼証明書	非信頼証明書
Windows Server 2003	△	△ *1	△	△ *1
Windows Vista/ Windows Server 2008	○	○ *2	○ *3	○ *2 *3
Windows 7/ Windows Server 2008 R2	◎	◎ *2	◎ *3	◎ *2 *3
Windows 8/ Windows Server 2012	◎	◎	◎ *3	◎ *3
Windows 8.1/ Windows Server 2012R2	◎	◎	◎	◎

◎ 24 時間以内に更新
(KB3004394 適用)

○ 1 週間以内に更新

△ 不定期

*1: セキュリティ アドバイザリを適用

*2: KB2677070 または KB2813430 の適用が必要

*3: KB2813430 の適用が必要

*4: windowsupdate.com のサイトへアクセス不可の環境

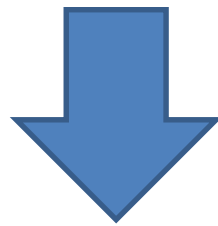


Security
Response
Team



不正な証明書の検出強化

- 不正な証明書発行の発見シナリオ
 - 利用者・証明機関からの申し出があった場合
 - 証明機関での失効処理が行われた場合
- 利用者・証明機関も気づく前に不正利用が行われているケースも。



マイクロソフト側でも検出し、証明機関と連携できないか？

SmartScreen を利用した不正な証明書検出

- Internet Explorer 11 より実装
- 攻撃に利用されている場合は、大規模から小規模まで様々なシナリオを想定

SmartScreen 収集

- アクセスしているサイトのサーバー証明書



攻撃の検出

- 中間者攻撃 (Man-In-The-Middle) に利用されている不正な証明書
- 不正に発行されていると推察される証明書



証明機関との連携

- 情報の伝達
- 対応方針の協議



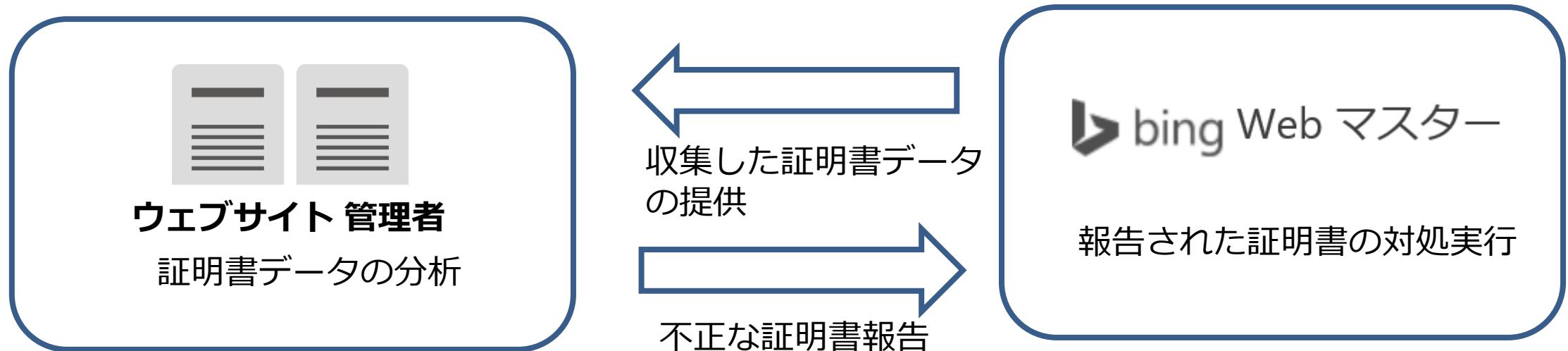
措置の実行

- 証明機関における失効
- マイクロソフトからの自動更新



ウェブサイト管理者への情報提供

- ウェブサイトのドメイン管理者に収集した証明書データを提供
 - 管理者においても証明書データの分析が可能
 - 不正な証明書の発見をより強化
 - 管理するドメインに対する証明書データのみ提供
- Windows 10 (Technical Preview) で提供中



Track Certificates (Preview)

収集された証明書一覧

収集された証明書
ダウンロード
X.509 バイナリ DER
(PKCS#7 提供予定)

Site ▼
contoso.com

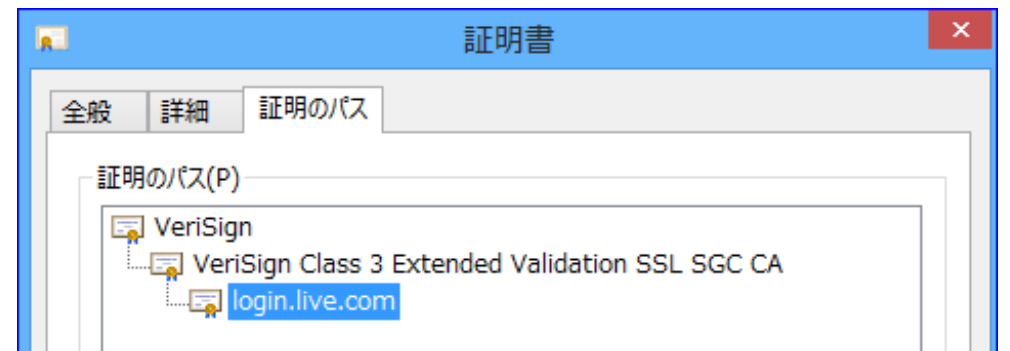
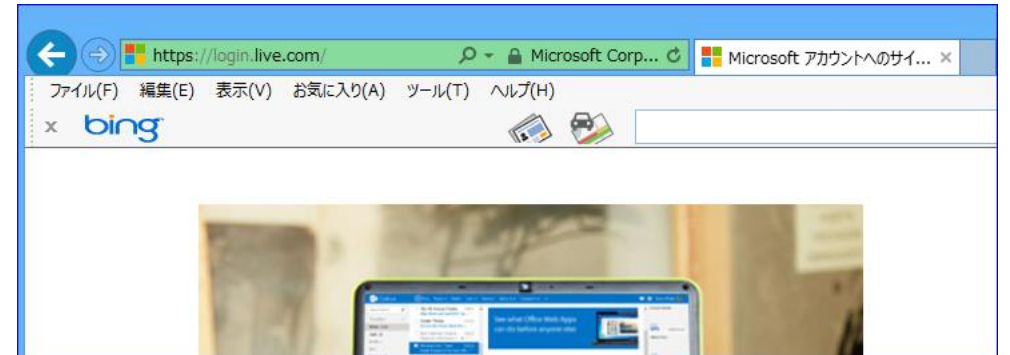
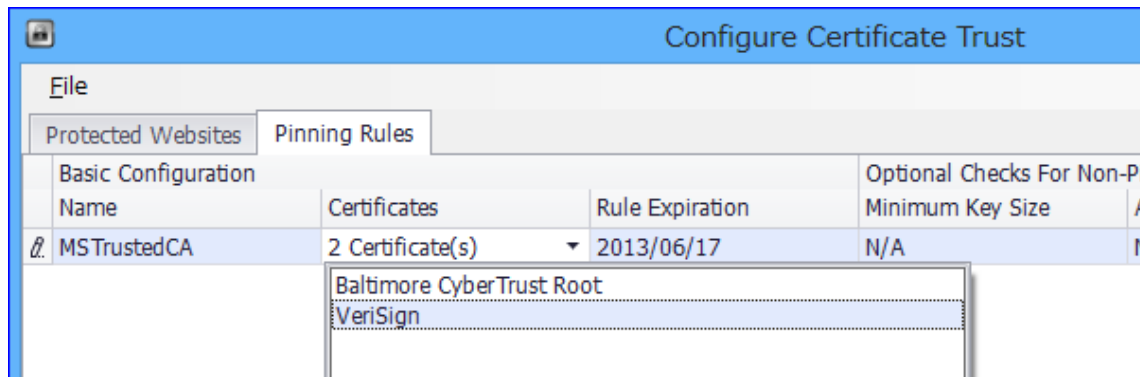
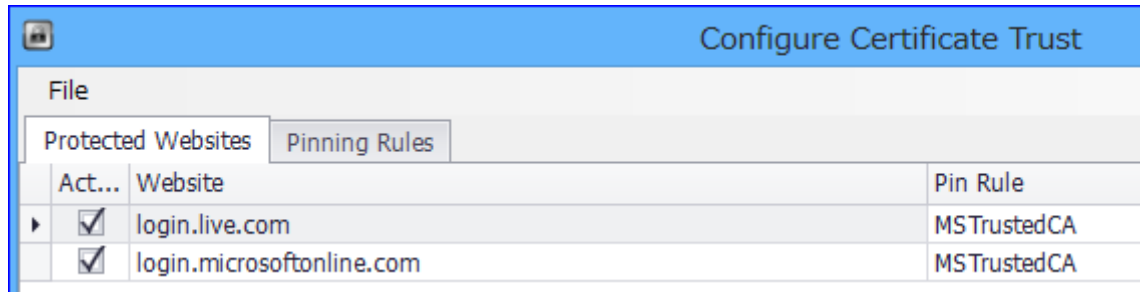
Track Certificates (Preview) ⓘ

HOST	ISSUED TO	ISSUED BY	FIRST SEEN	LAST SEEN	EXPIRY DATE	DOWNLOAD	REPORT TO MICROSOFT
*.contoso.com	*.contoso.com	Cybertrust Public SureServer SV CA	8/31/2014 12:32:51 PM	2/13/2015 8:44:26 AM	4/17/2015	Download	Report
*.contoso.com	*.contoso.com	Verizon Akamai SureServer CA G14-SHA1	12/5/2014 11:18:17 PM	3/4/2015 12:56:03 AM	12/5/2015	Download	Report
*.contoso.com	*.contoso.com	Verizon Akamai SureServer CA G14-SHA1	1/6/2015 8:50:39 AM	1/16/2015 9:35:05 PM	12/5/2015	Download	Report
*.contoso.com	*.contoso.com	Verizon Akamai SureServer CA G14-SHA1	12/20/2014 7:41:20 AM	12/20/2014 7:41:20 AM	12/5/2015	Download	Report

報告フォーム

Certificate Pinning

- 脆弱性緩和ツール EMET (無償ツール) にて提供
- 対象のサイト (ドメイン) と、証明書を紐づけ



Agenda

- SSL/TLS & 証明書 in Windows/Internet Explorer
- 安全性を高める機能
 - ルート証明書更新プログラム・証明書信頼リストの自動更新
 - SmartScreen と Bing Webmaster Tool による不正証明書の検出強化
- より安全な環境へ
 - 危殆化したアルゴリズムからの移行推奨
- まとめ

危殆化したアルゴリズムの排除

	概要	対象 OS	タイムライン	アドバイザリ
RSA 鍵長	1024 ビット未満の RSA 鍵を利用した証明書を無効化	Windows XP, Windows Server 2003 以降	2012 年 8 月アドバイザリ公開 2012 年 10 月自動更新で配布	マイクロソフト セキュリティ アドバイザリ (2661254)
MD5 ハッシュ	ルート証明書プログラムに参加している証明機関は以下で利用されている証明書において、SHA-1 ハッシュ アルゴリズムを無効化	Windows Vista/Windows Server 2008 以降	2013 年 8 月更新プログラム公開 2014 年 2 月自動更新で配布	マイクロソフト セキュリティ アドバイザリ (2862973)
SHA-1 ハッシュ	ルート証明書プログラムに参加している証明機関は以下で利用されている証明書において、SHA-1 ハッシュ アルゴリズムを無効化	Windows Vista/Windows Server 2008 以降	2016 年 1 月証明機関にて新規の SHA-1 証明書発行停止 2016 年 1 月 SHA-1 コード署名証明書無効化を自動更新で配布 2017 年 1 月 SHA-1 SSL 証明書無効化を自動更新で配布	マイクロソフト セキュリティ アドバイザリ (2880823)
RC4	SSL/TLS にて RC4 を利用しないよう構成を推奨 * レジストリによる無効化が必要	Windows 7, Windows Server 2008 R2 以降	2013 年 11 月更新プログラム公開 2014 年 5 月 .NET 用の更新プログラムを公開	マイクロソフト セキュリティ アドバイザリ (2868725) マイクロソフト セキュリティ アドバイザリ (2960358)

※ 2015 年 4 月時点での状況です。今後の予定は変更になる可能性があります。



マイクロソフト SHA-1 廃止に向けた措置

① 2016 年 1 月 1 日以降
証明機関は SHA-1 を利用
した証明書を発行不可



マイクロソフト ルート更新プログラムに
参加しているルート証明機関
(ルート CA)



中間証明機関
(中間 CA)



中間証明機関
(中間 CA)

コード署名証明書



SHA1

SSL 証明書



SHA1

② コード署名証明書は 2016 年 1 月 1 日以降
のタイムスタンプで署名された証明書
およびアプリケーション・コードは利用不可

(2015 年 12 月 31 日以前に署名されたコードは、
SHA-1 の脅威状況に応じて利用不可の措置が
実施される可能性があります)

SSL 証明書は 2017 年 1 月 1 日以降
SHA-1 を利用した証明書は利用不可

※ 2015 年 4 月時点での状況です。今後の予定は変更になる可能性があります。



Security
Response
Team



POODLE 対応予定

- セキュリティ アドバイザリ 3009008 「SSL 3.0 の脆弱性により、情報漏えいが起こる」
 - <https://technet.microsoft.com/ja-jp/library/security/3009008>
- 対応タイムライン
 - 2014 年 10 月 21 日: セキュリティ アドバイザリを公開
 - 2014 年 10 月 29 日: Internet Explorer の設定で SSL3.0 無効化するための Fix IT ツールを公開
 - 2014 年 12 月 1 日: Azure および Office 365 にて、SSL 3.0 を無効化
 - **2015 年 4 月 13 日自動更新にて Internet Explorer の既定の設定で SSL3.0 を無効化**
 - IE のみで SSL3.0 が無効化
 - その他の SSL/TLS 利用時には影響を受けない



参考: Internet Explorer 設定一覧

	SSL3.0	TLS1.0	TLS1.1	TLS1.2
Internet Explorer 6	○	△	×	×
Internet Explorer 7	○	△	×	×
Internet Explorer 8 (Windows Server 2003, Windows Vista, Windows Server 2008)	○	△	×	×
Internet Explorer 8 (Windows 7, Windows Server 2008 R2)	○	○	△	△
Internet Explorer 9 (Windows Vista, Windows Server 2008)	○	△	×	×
Internet Explorer 9 (Windows 7, Windows Server 2008R2)	○	○	△	△
Internet Explorer 10	○	○	△	△
Internet Explorer 11	○	○	○	○

○ 既定で有効 △既定で無効だが利用可 ×利用不可

セキュリティ アドバイザリでお知らせ

マイクロソフト セキュリティ アドバイザリ

<https://technet.microsoft.com/ja-jp/library/security/dn631936.aspx>

公開月	アドバイザリ番号	タイトル
2013/1	2798897	不正なデジタル証明書により、なりすましが行われる
2013/6	2854544	Windows の暗号化とデジタル証明書の処理を改善するための更新プログラム
2013/6	2813430	管理者が、接続されていない Windows 環境で信頼されている CTL と許可されていない CTL を更新できるようにする更新プログラム
2013/8	2862966	Windows の弱い証明書暗号化アルゴリズムの管理を向上させる更新プログラム
2013/8	2862973	マイクロソフト ルート証明書プログラムでの MD5 ハッシュ アルゴリズム廃止用の更新プログラム
2013/11	2868725	RC4 を無効にするための更新プログラム
2013/11	2880823	マイクロソフト ルート証明書プログラムでの SHA-1 ハッシュ アルゴリズムの廃止
2013/12	2915720	Windows Authenticode 署名検証の変更
2013/12	2916652	不適切に発行されたデジタル証明書により、なりすましが行われる
2014/7	2982792	不適切に発行されたデジタル証明書により、なりすましが行われる
2014/5	2960358	.NET TLS で RC4 を無効化するための更新プログラム
2014/10	2949927	Windows 7 および Windows Server 2008 R2 で SHA-2 ハッシュ アルゴリズムを利用可能
2014/10	2977292	TLS の使用を可能にする Microsoft EAP 実装用の更新プログラム
2014/10	3009008	SSL 3.0 の脆弱性により、情報漏えいが起こる



Agenda

- **SSL/TLS & 証明書 in Windows/Internet Explorer**
- **安全性を高める機能**
 - ルート証明書更新プログラム・証明書信頼リストの自動更新
 - SmartScreen と Bing Webmaster Tool による不正証明書の検出強化
- **より安全な環境へ**
 - 危殆化アルゴリズムの移行推奨
- **まとめ**

まとめ

- 単一の機能や仕組みだけではなく、様々な機能や連携により多層的に安全性を高めていく必要がある
- より安全な環境のために、新機能や推奨される移行などを活用し運用していくことが大切
- ぜひ、活用していただけると幸いです

参考情報

マイクロソフトが提供する信頼できる証明書利用基盤～ルート証明書更新プログラムと更新ツール～

<http://blogs.technet.com/b/jpsecurity/archive/2013/01/17/3546357.aspx>

セキュリティ アドバイザリ 2854544 (KB2813430) ～ルート証明書更新プログラムの管理強化

<http://blogs.technet.com/b/jpsecurity/archive/2013/06/12/3578245.aspx>

Certificate Reputation for website owners

<http://blogs.msdn.com/b/ie/archive/2015/03/10/certificate-reputation-for-website-owners.aspx>

Technet EMET ツール

<http://technet.microsoft.com/ja-jp/security/jj653751>



© 2015 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.