Internet Week 2014　セッションS14

サーバーのSSL/TLS設定のツボ

(配布資料)

2014年11月20日(木) 13:45-14:15
於：富士ソフトアキバプラザ

富士ゼロックス株式会社　漆嶌 賢二

SSL/TLSの過去の問題と対応方法

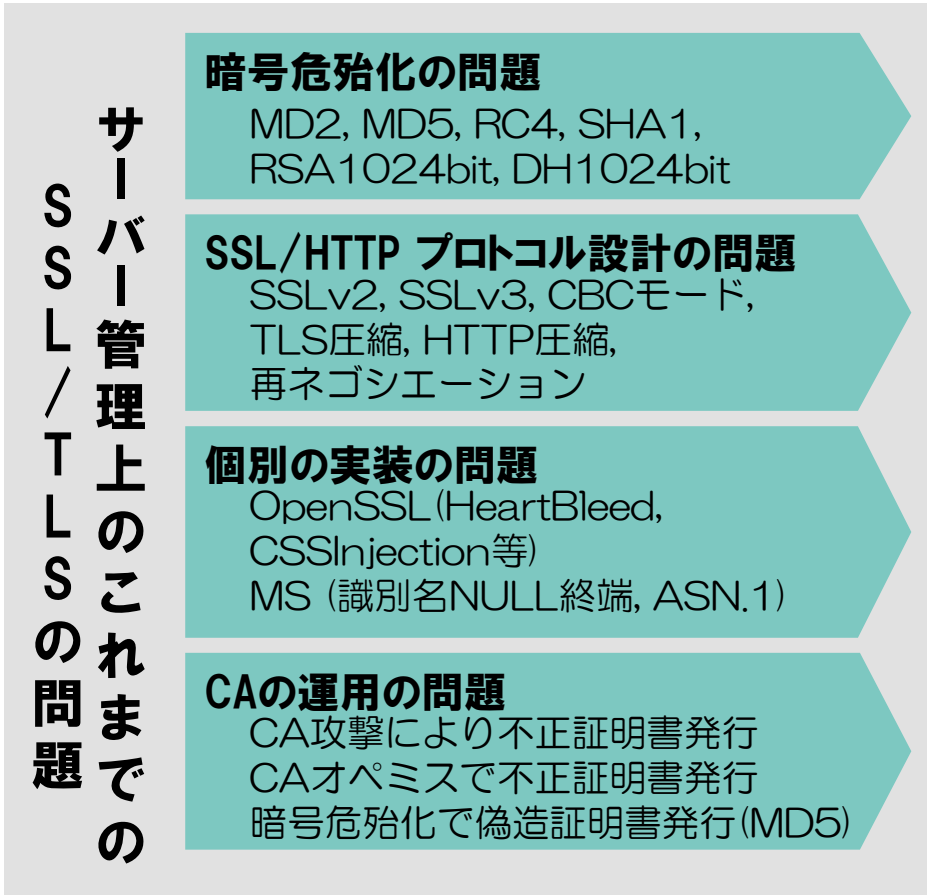
サーバー設定で回避し続けならないものも多数

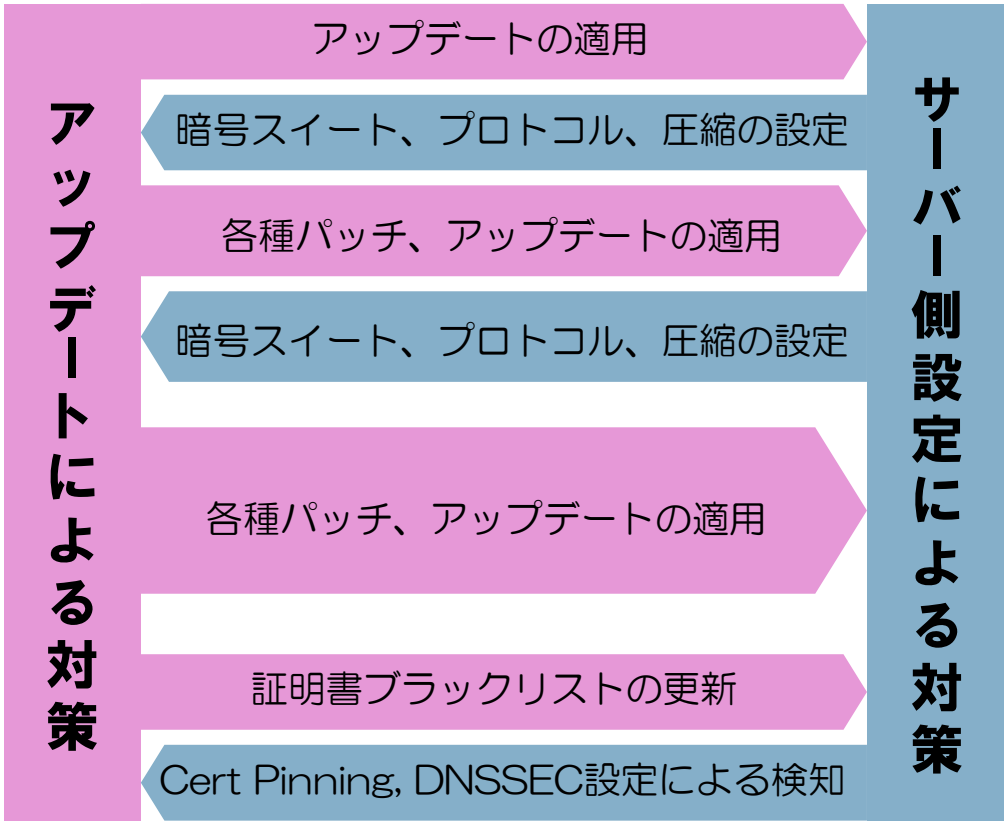
時期	問題・事件	対策
2005.11	OpenSSL SSLv2バージョンロールバック	アップデート
2009.01	RapidSSL MD5衝突偽造中間CA	アップデートやPinning
2009.07	NULL終端による証明書ホスト名一致不備	アップデートやPinning
2009.11	再ネゴシエーション脆弱性	アップデート
2011.03	Comodo不正証明書発行(RA攻撃)	アップデートやPinning
2011.08	DigiNotar不正証明書発行(RA攻撃)	アップデートやPinning
2011.09	BEAST攻撃	暗号スイート/プロトコル設定(非CBC)
2011.11	Digicert Sdn不正証明書発行(RSA512)	アップデートやPinning
2012.05	FLAMEマルウェア用Windows Terminal ServerによるMD5衝突偽造中間CA, Windows Update攻撃	アップデートやPinning
2012.09	CRIME攻撃	圧縮解除設定(SSL)
2013.01	Lucky13攻撃	暗号スイート/プロトコル設定(GCM利用)
2013.01	TURKTRUST不正証明書発行(オペミス)	アップデートやPinning
2013.03	SSLにおけるRC4暗号危殆化	暗号スイート/プロトコル設定(非RC4)
2013.03	TIME攻撃	圧縮解除設定(SSL)
2013.06	BREACH攻撃	圧縮解除設定(HTTP gzip)
2013.06	スノーデン氏暴露(NSAの全SSL通信保管)	暗号スイート/プロトコル設定(ECDHE,DHE使用)
2014.04	HeartBleed攻撃	アップデート
2014.06	CSSInjection攻撃	アップデート
2014.10	POODLE攻撃	暗号スイート/プロトコル設定(非SSLv3,CBC)

古い脆弱性であっても、アップデートだけでは解決しない問題が多数残っている

FUJI Xerox

サーバー管理上のこれまでのSSL/TLSの問題と対策の整理





古い脆弱性であっても、アップデートだけでは解決しない問題が多数残っている
デフォルト設定でなく、きめ細かい設定で問題に対処する必要がある

FUJI Xerox

とはいえ、SSL/TLSの設定はわかりにくい

- 設定だってよくわからん

```
SSLCipherSuite
RC4-SHA:AES128-SHA:HIGH:MEDIUM:!aNULL:!MD5
```

- もう、こりゃ呪文かと・・・

- どんなサーバー証明書にすればいいの？

今日説明する設定のポイント(アジェンダ)

- SSL/TLSの設定ポイント
  - 暗号の設定(暗号スイートの設定)
  - 暗号スイートの順序のサーバー優先
  - 使用プロトコルバージョン
  - 圧縮設定の解除
  - 証明書の設定
  - オプション：Certificate/Public Key Pinning
  - オプション：OCSPステープリング
  - オプション：HSTS(HTTPSの強制)
- 今後のSSLサーバー証明書の購入ポイント

利用者環境/サービス提供環境の想定

利用者はどんな環境を使うのか
そしてサービス提供側の要件
によって設定は変わる

利用者環境/サービス提供側環境の想定

利用者側

- ✓スマートフォン, PCなど最新のブラウザが使えるか
- ✓どのようなブラウザ、OSを使っているか
- ✓Javaなどのクライアントがあるか
- ✓フィーチャーフォンのユーザがいるか
- ✓Windows XP SP3より前の環境をサポートするか
- ✓サポート終了になったクライアント環境(WinXP SP3等)をサポートするか
- ✓ゲーム機、専用機、専用アプリなどが想定されるか
- ✓APIからの利用があるか、また言語は何か

サービス提供側

- ✓サポートするブラウザやOSは何か
- ✓最新のブラウザだけにサービスを限定するか
- ✓サーバー側のOS、ソフトウェアは何か
- ✓HTML5や最新のJavaScriptに限定するか
- ✓専用機、SSLアクセラレータ、SSL-VPNなどか
- ✓クラウド環境から提供されるものか(AWS Elastic LB等)
- ✓一般に広く提供するサービスか、組織内(社内,省庁内)のサービスか

想定される対象によって有効な設定が変わってくる

FUJI Xerox

想定環境の大まかな分類

高セキュリティ

低セキュリティ

A. 最新環境をサポート

- HTML5や最新のJavaScript, CSSなど最新環境でしか動作しない
- 最新のPCやスマホのブラウザを必須とする

B. 幅広くサポート

- 幅広い環境をサポートしなければならない場合
- 何をサポートしなければならないのかよくわからない場合

C. レガシーサポート

- XP、ガラケー、ゲーム機、APIなどレガシーな環境をサポートする場合
- 政官系の専用アプリ
- ICカードによるクライアント認証
- SSLアクセラレータ、SSL-VPN等の専用ハードで設定内容が制限される場合

FUJI Xerox

SSL/TLSサーバー設定のポイント

SSL/TLSサーバー設定のポイント(概要)

① 暗号の設定(暗号スイートの設定)
② 暗号スイートの順序のサーバー優先
③ 使用プロトコルバージョン
④ 圧縮設定の解除
⑤ サーバー証明書の設定

以下は、できれば

オプション①：Certificate Pinning
オプション②：HSTS(HTTPSの強制)
オプション③：OCSPステープリング

SSL/TLSサーバー設定のポイント①
暗号スイートの設定

SSL/TLSの3つの機能

ニセのアマゾンサイトに「カード番号、住所」なんかを送りたくない。

「カード番号、住所、氏名、買い物の内容」を途中で見られたくない

途中で「届け先住所」を書き換えて商品を騙しとられたくない。

相手認証	機密性	完全性
証明書(PKI)などを使い**通信相手が正しい相手であるか認証**	暗号通信により相手以外に内容を**盗み見(盗聴)されない**	通信途中でデータが**書換え(改ざん)されない**よう検知できる
なりすまし防止	覗き見(盗聴)防止	改ざん防止
PKI(公開鍵暗号)を使う	*共通鍵暗号を使う*	*MAC(メッセージ認証コード)を使う*

CipherSuiteとは？

標準(RFC)では
318種以上規定されている

ClientHello, ServerHelloでウェブブラウザとウェブサーバーが合意する暗号のセット

ClientHello
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_DES_CBC_SHA
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
をサポートしてますけど、どうしまっか？

ServerHello
ほな、これでお願いしま
TLS_RSA_WITH_DES_CBC_SHA

通信暗号強度が決まるのでサーバー側では注意が必要

(例)

TLS_RSA_WITH_AES128_CBC_SHA　値0x0010

TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA　値0x0010

鍵交換と(公開鍵暗号を使った)認証のアルゴリズム	データの共通鍵暗号のアルゴリズム	メッセージ認証(MAC)のアルゴリズム
		※ハッシュ関数SHA1でなくMAC関数 HmacSHA1
相手認証	**データ暗号化**	**改ざん防止**

FUJI Xerox

じゃぁ、どの暗号スイートを選ぶか (参考)

鍵交換	認証	暗号化	MAC
ECDHE ECDH DHE DH SRP NULL	RSA ECDSA DSS KRB5 PSK anon NULL RSA_EXPORT DSS_EXPORT GOST341094 GOST341001	AES_(128|256)_CBC AES_(128|256)_GCM AES_(128|256)_CCM(_8) 3DES_EDE_CBC DES_CBC RC4_(40|128) CAMELLIA_(128|256)_CBC IDEA_CBC ARIA_256_(CBC|GCM) SEED_CBC CHACHA20_POLY1305 GOST28147 NULL	SHA SHA256 SHA384 MD5 IMIT_GOST28147 HMAC_GOST3411 NULL

組み合わせの数が多すぎて選びようがない

暗号スイートを選定する際のポイント

① 2つ以上のメジャーなブラウザがサポートしている
(KRB5, PSK, SRP, CCMなど除外)
② 最近のなるべく多くの脆弱性や問題に対応したい
a. BEAST,POODLE対策 (CBC除外)
b. Lucky13対策 (GCM利用)
c. RC4危殆化 (RC4除外)
d. 多くのDHE,DH実装の鍵長不足(1024bit以下) (DHE,DH除外)
e. 米NSAの監視とPFS (ECDHE,DHE利用)
f. SHA1危殆化 (SHA除外)
③ 暗号機能が無効になってるものは選ばない(NULL,anon除外)
④ 輸出用の弱い暗号を選ばない(EXPORT除外)
⑤ 証明書に関しては商用サービスが対応するもの(DSS除外)
⑥ 明らかに弱い暗号は除外(MD5, RC2, DES除外)
⑦ サーバー側のパフォーマンスにも配慮する
(AES128で十分、DHEはやめる、RSA4096ならECDSA)
⑧ 必要があればレガシーな環境にも配慮する
(3DESかRC4ぐらいしか選択肢がない)

最近の脆弱性に配慮した暗号スイートの選定と順序

	最近のブラウザのみ対応		レガシーを含む幅広い環境に対応	
	【最新1】 NSA等による監視にも対応	【最新2】 NSA等による監視は無視	【レガシー1】 RC4危殆化に配慮	【レガシー2】 CBC関連の攻撃に配慮
暗号スイートと順序	① ECDHE+AES+GCM+SHA2	①+ ②AES+GCM+SHA2	①+②+ ③AES+CBC+SHA2 AES+CBC+SHA1 3DES+CBC+SHA1	①+②+ ④RC4+SHA1
対応する問題	POODLE,BEAST,Lucky13,RC4,DH,PFS,SHA1	POODLE,BEAST,Lucky13,RC4,DH,SHA1	RC4,DH	POODLE,BEAST,Lucky13,DH
非対応の問題		PFS	POODLE,BEAST,Lucky13,SHA1	RC4,SHA1
注意点	新しいブラウザしか対応しない	やや新しいブラウザ以降しか対応しない	最も幅広いクライアントに対応するが、CBC関係の攻撃に対抗しない	CBC関連攻撃に対抗し、レガシーを広くカバーするが古IEなど非対応

前述4ケースのための暗号スイート一覧と順序（参考）

【最新1】グループ①のみ
【最新2】グループ①＋②
【レガシー1】グループ①＋②＋③
【レガシー2】グループ①＋②＋④

■暗号スイート グループ①
ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE_RSA_WITH_AES_256_GCM_SHA384

■暗号スイート グループ②
RSA_WITH_AES_128_GCM_SHA256
RSA_WITH_AES_256_GCM_SHA384

好みの暗号スイートを加えて
構いませんが、これが基本形です。

■暗号スイート グループ③
ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
RSA_WITH_AES_128_CBC_SHA256
RSA_WITH_AES_256_CBC_SHA256

ECDHE_ECDSA_WITH_AES_128_CBC_SHA
ECDHE_ECDSA_WITH_AES_256_CBC_SHA
RSA_WITH_AES_128_CBC_SHA
RSA_WITH_AES_256_CBC_SHA

RSA_WITH_3DES_EDE_CBC_SHA

■暗号スイート グループ④
RSA_WITH_RC4_128_SHA

Apache HTTP Server/lighttpd/nginx+OpenSSLの暗号スイート設定 (参考)

OpenSSL系のサーバーでは、個別の省略した名称で暗号スイートを記載し指定することもできるが、パータンを表す式により指定することもできる。前述４ケースにほぼ近いパターン式を紹介する。

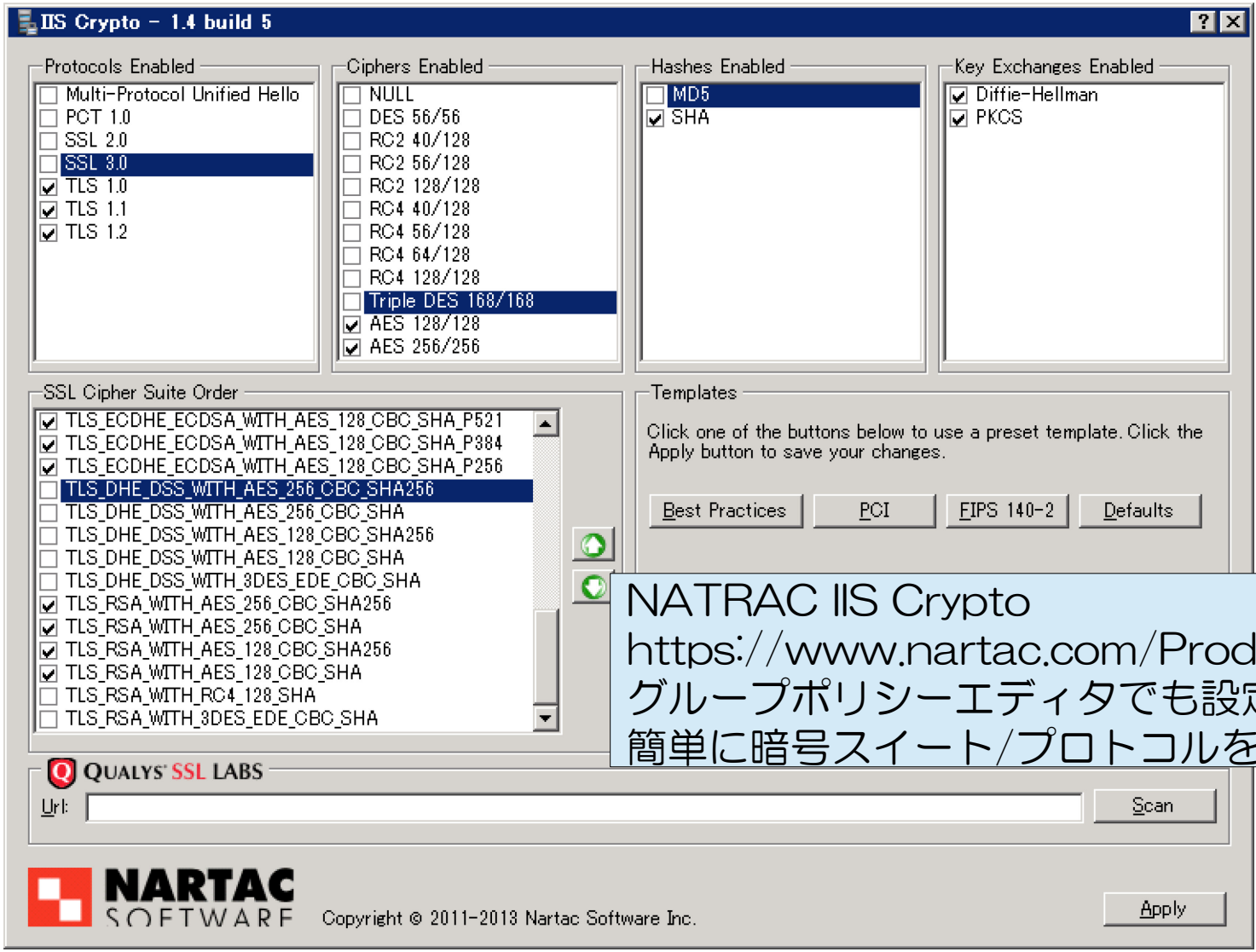
■【最新1】最新のブラウザ用でPFSを気にする場合
EECDH+AESGCM:!DSS:!DH
課題：AES256>AES128になってしまう

■【最新2】最新のブラウザ用でPFSを気にしない場合
EECDH+AESGCM:RSA+AESGCM:!DSS:!DH

■【レガシー1】レガシーを含め最も幅広くサポートし、RC4危殆化に対抗する場合
EECDH+AESGCM:RSA+AESGCM:EECDH+AES:AES:DES-CBC3-SHA:!DSS:!DH:!PSK:!SRP:!MD5:!AECDH:!kECDH

■【レガシー2】レガシーを含め幅広くサポートし、古いIE環境は無視し、BEAST等のCBC系攻撃に対抗する場合
EECDH+AESGCM:RSA+AESGCM:RC4-SHA:!DSS:!DH:!PSK:!SRP:!MD5:!AECDH:!kECDH

Microsoft IISの暗号スイート/プロトコル設定
オススメIISの暗号スイート/プロトコルの設定ツール(参考)



NATRAC IIS Crypto
https://www.nartac.com/Products/IISCrypto/
グループポリシーエディタでも設定可能だが、
簡単に暗号スイート/プロトコルを設定できるフリーウェア

FUJI Xerox

Apache Tomcatの暗号スイート設定（参考）

Tomcatで使用するJavaがどのバージョンかで、設定できる暗号スイートやその名称が決まるため、サポートする暗号スイート一覧が簡単に得られると有り難い。
このような時、SSLInfoというツールを使用している。

https://gist.github.com/MikeN123/8810553

コンパイルしてTomcatで使うJavaで実行すれば暗号スイート一覧が得られる。

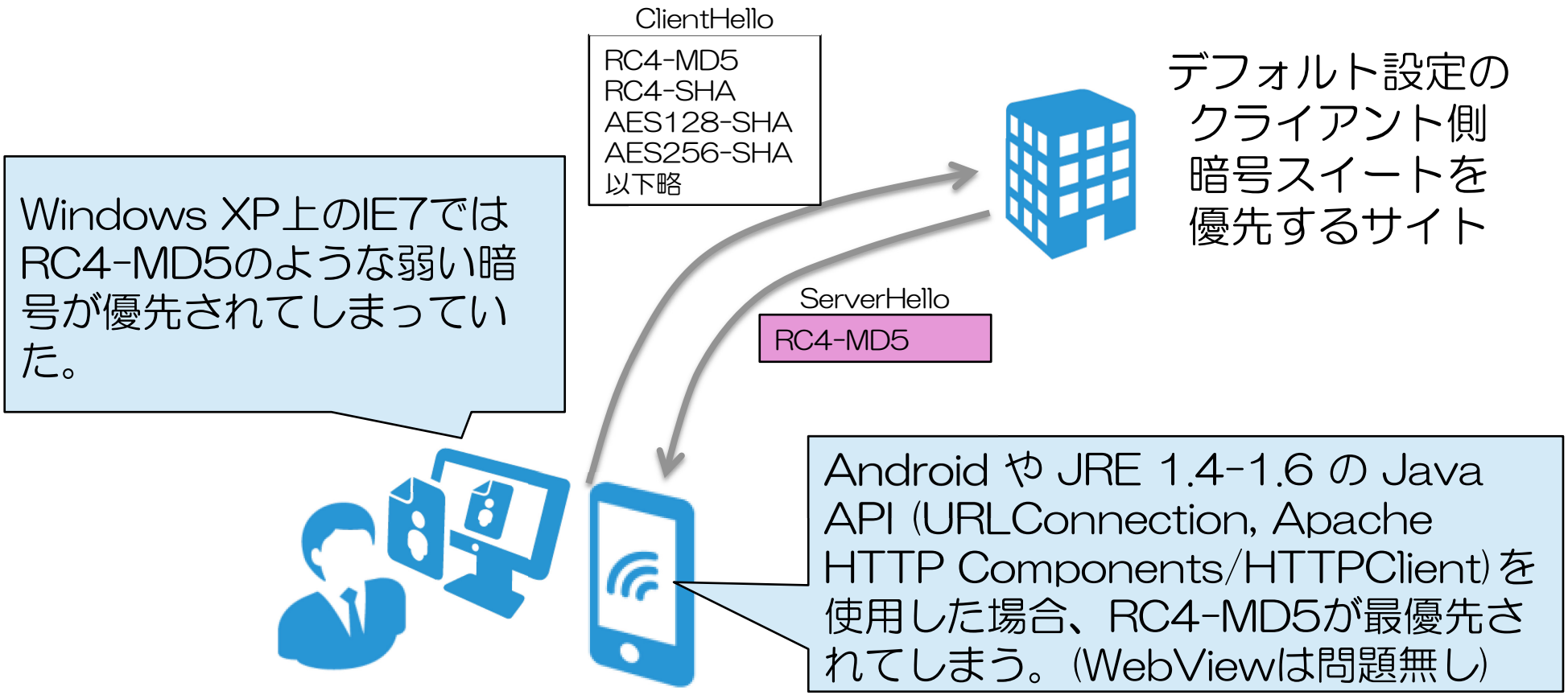
※ J2SE 1.6.0_65のサポートするCipherSuites一覧
Default Cipher
* SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
* SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
* SSL_DHE_DSS_WITH_DES_CBC_SHA
* SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
* SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
* SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
SSL_DH_anon_WITH_DES_CBC_SHA
SSL_DH_anon_WITH_RC4_128_MD5
* SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
* SSL_RSA_EXPORT_WITH_RC4_40_MD5
* SSL_RSA_WITH_3DES_EDE_CBC_SHA
* SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
* SSL_RSA_WITH_RC4_128_MD5
* SSL_RSA_WITH_RC4_128_SHA
* TLS_DHE_DSS_WITH_AES_128_CBC_SHA
* TLS_DHE_DSS_WITH_AES_256_CBC_SHA
* TLS_DHE_RSA_WITH_AES_128_CBC_SHA
* TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
* TLS_EMPTY_RENEGOTIATION_INFO_SCSV
TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5
TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA
TLS_KRB5_EXPORT_WITH_RC4_40_MD5
TLS_KRB5_EXPORT_WITH_RC4_40_SHA
TLS_KRB5_WITH_3DES_EDE_CBC_MD5
TLS_KRB5_WITH_3DES_EDE_CBC_SHA
TLS_KRB5_WITH_DES_CBC_MD5
TLS_KRB5_WITH_DES_CBC_SHA
TLS_KRB5_WITH_RC4_128_MD5
TLS_KRB5_WITH_RC4_128_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA
* TLS_RSA_WITH_AES_256_CBC_SHA
※ ‘*’印はデフォルトで提供されるCipherSuites

FUJI Xerox

SSL/TLSサーバー設定のポイント②
暗号スイートのサーバー優先

暗号スイートのサーバー側優先

クライアントから送る暗号スイート一覧の順序を優先して接続すると弱い暗号が使われることがある



SSLHonorCipherOrder On等設定してサーバー側を優先する設定を

参考　PKIDay 2011 NTT武藤氏：SSLにおける暗号危殆化サンプル調査の報告　http://www.jnsa.org/seminar/pki-day/2011/data/03_mutoh.pdf
自堕落な技術者の日記 JRE 1.4-1.6やAndroidのAPIを使ったHTTPS接続のCipherSuitesのRC4-MD5優先　http://blog.livedoor.jp/k_urushima/archives/1727793.html

FUJI Xerox

SSL/TLSサーバー設定のポイント ③④⑤

③使用プロトコルバージョン
④圧縮設定の解除
⑤サーバー証明書の設定

SSLサーバー設定のポイント③～⑤

③ 使用プロトコルバージョン

- POODLE対策としてSSLv3を無効化できるか？
- レガシーな環境ではSSLv3を残す必要があるかも

④ 圧縮設定の解除

- CRIME攻撃、TIME攻撃対策としてSSL圧縮を無効化する

⑤ サーバー証明書の設定

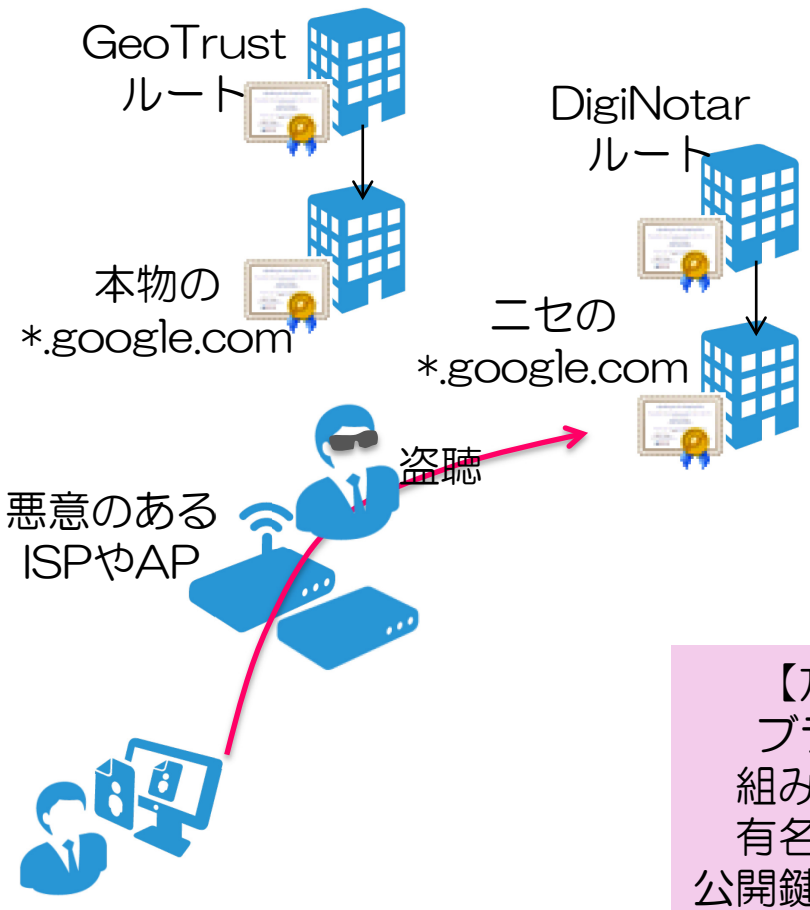
- OpenSSL系のサーバー(Apache、lighttp、nginx)の場合には、中間CA証明書の設定を忘れずに！
- 設定方法は証明書発行サービスのヘルプをよくご覧ください

SSL/TLSサーバー設定のポイント
オプション①
Certificate Pinning

Certificate Pinning/Public Key Pinning (不正証明書の拒否)

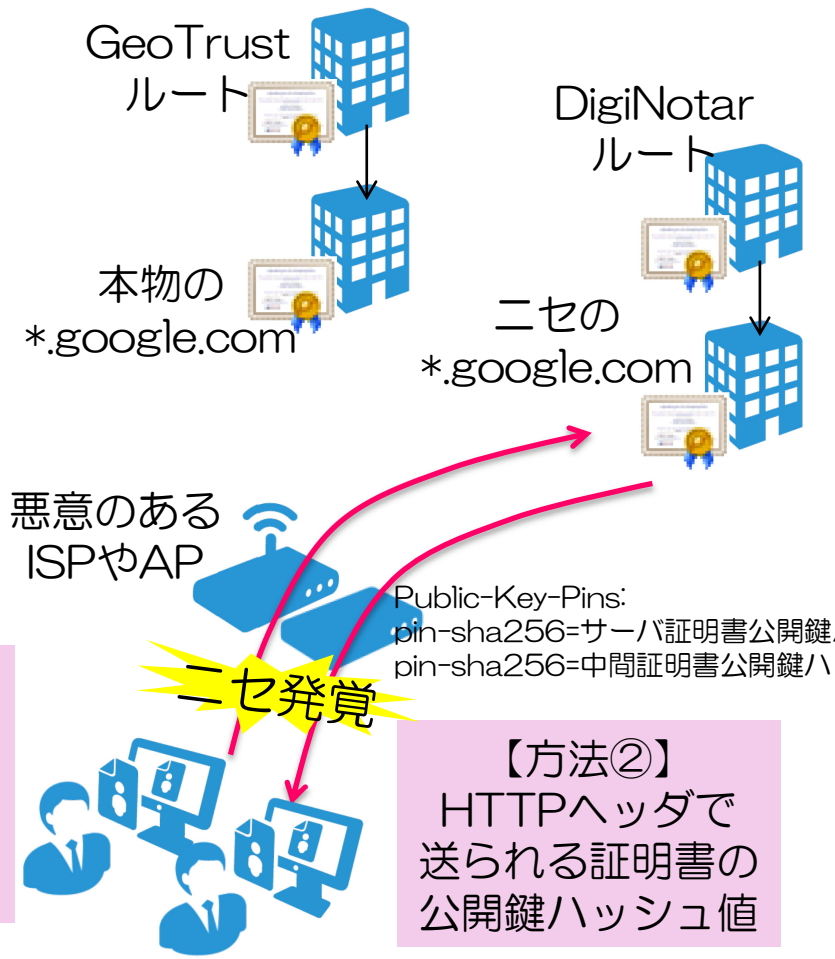
Pinningはニセ証明書対策に効果がある

Pinningがない場合



【方法①】
ブラウザに
組み込まれた
有名サイトの
公開鍵ハッシュ値

Pinningがある場合

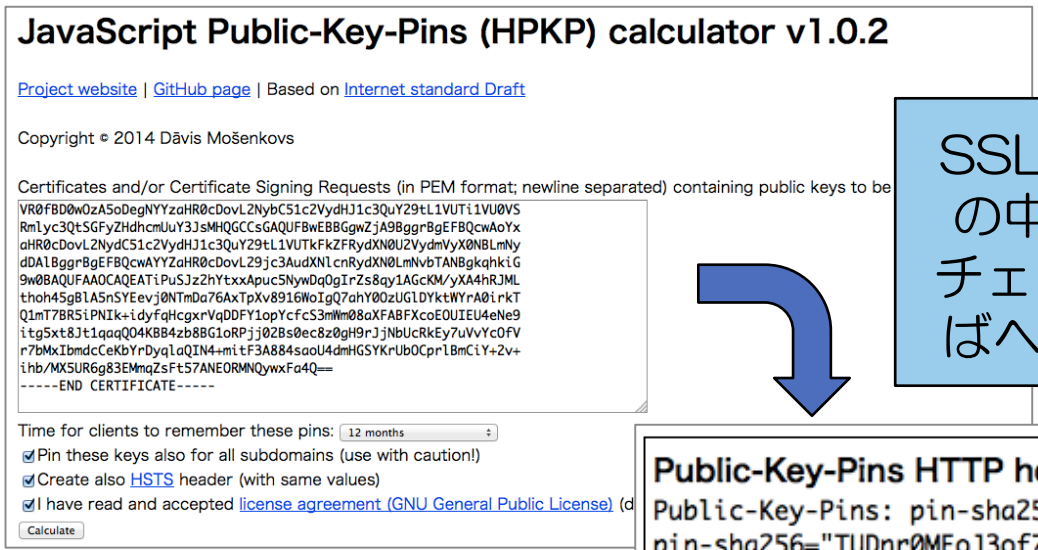


【方法②】
HTTPヘッダで
送られる証明書の
公開鍵ハッシュ値

FUJI Xerox

Certificate Pinning/Public Key Pinning (不正証明書の拒否)

- インターネットドラフトで規定されている
  https://tools.ietf.org/html/draft-ietf-websec-key-pinning-21
- HTTPヘッダを追加することで使用する証明書チェーンの不正入替を防ぐ
- ヘッダのキー：Public-Key-Pins
- ヘッダの値(例)：pin-sha256=証明書の公開鍵のSHA256ハッシュ値のBase64値
- ヘッダを作成してくれるサイトを活用するとよい
  https://projects.dm.id.lv/s/pkp-online/calculator.html



SSLサーバー証明書から最上位の中間CA証明書までの証明書チェーンをPEM形式で入力すればヘッダを自動作成してくれる

Public-Key-Pins HTTP header:

```
Public-Key-Pins: pin-sha256="lCppFqbkrlJ3EcVFAkeip0+44VaoJUymbnOaEUk7tEU=";
pin-sha256="TUDnr0MEoJ3of7+YliBMBVFB4/gJsv5zO7IxD9+YoWI=";
pin-sha256="68YTDKOLH2QWSUUVgfmsnkvgGFAtbM7Ljsrzn3v/gfY=";
pin-sha256="owdYGO+3voomGfjI2BhXs6mm1c5NtAlejd/QncQNbkQ="; max-age=31536000;
includeSubDomains
```


FUJI Xerox

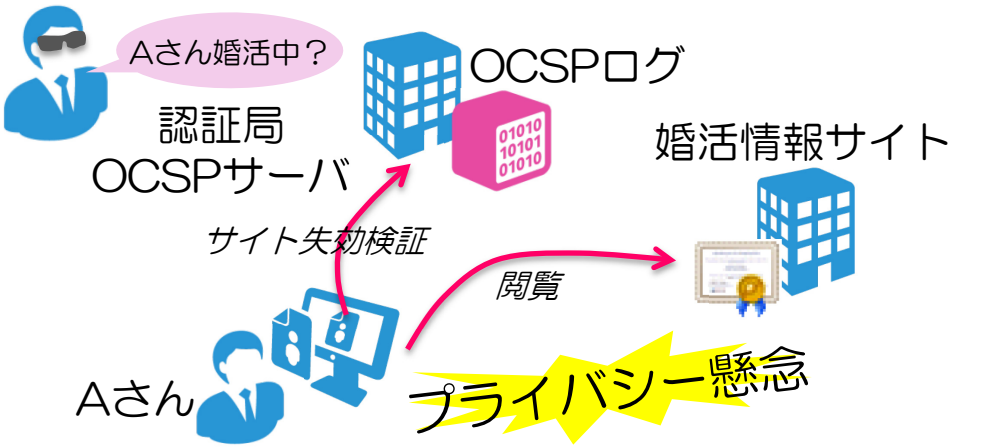
SSL/TLSサーバー設定のポイント
オプション②
OCSPステープリング

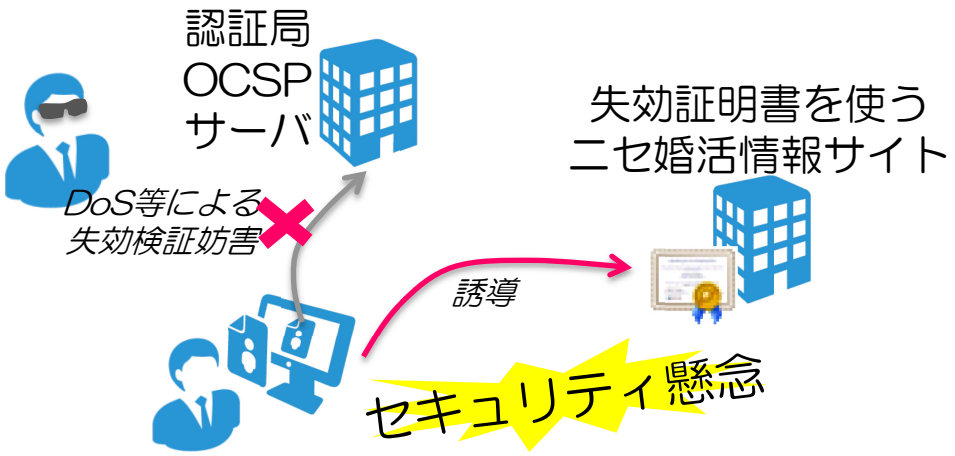
FUJI Xerox

OCSP Stapling(RFC 6066TLS拡張8章)の意義と仕組み

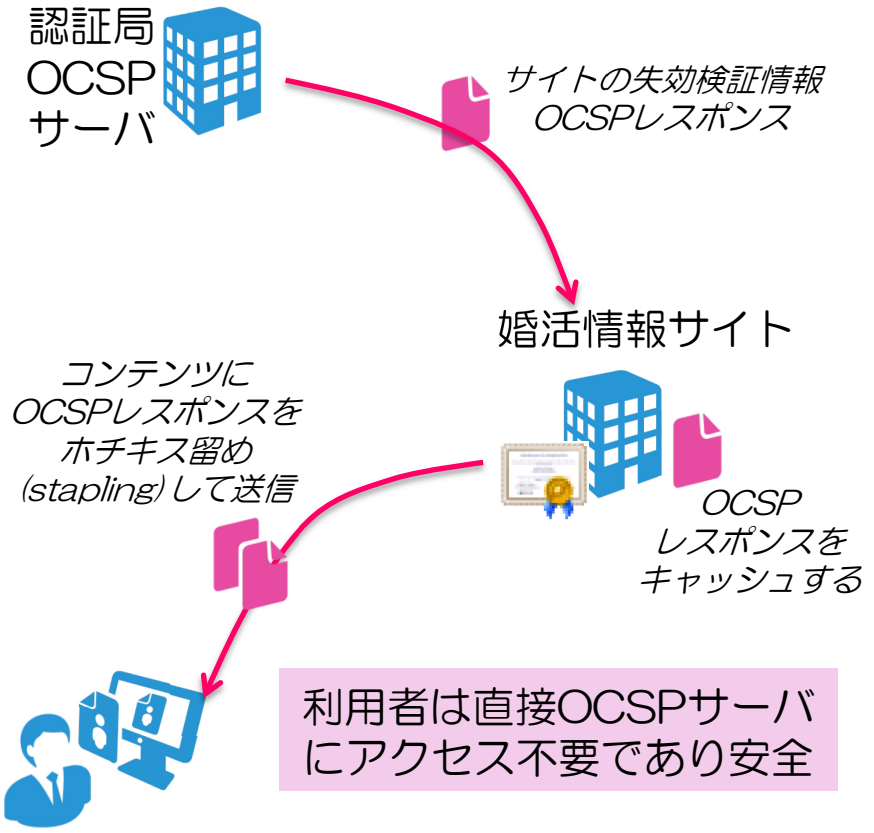
① 近年、CRLは数十MBまで膨大しモバイル/組込み環境の失効検証に向かずOCSPを使う方向に
② ブラウザがOCSPに接続できないと失効如何にかかわらず証明書有効になってしまう
③ OCSPサーバのログで、どのIPの人がどのサイトを閲覧したかという情報を認証局も知ってしまう
→→ OCSP Staplingでこれを解決

OCSP Staplingがない場合





OCSP Staplingがある場合

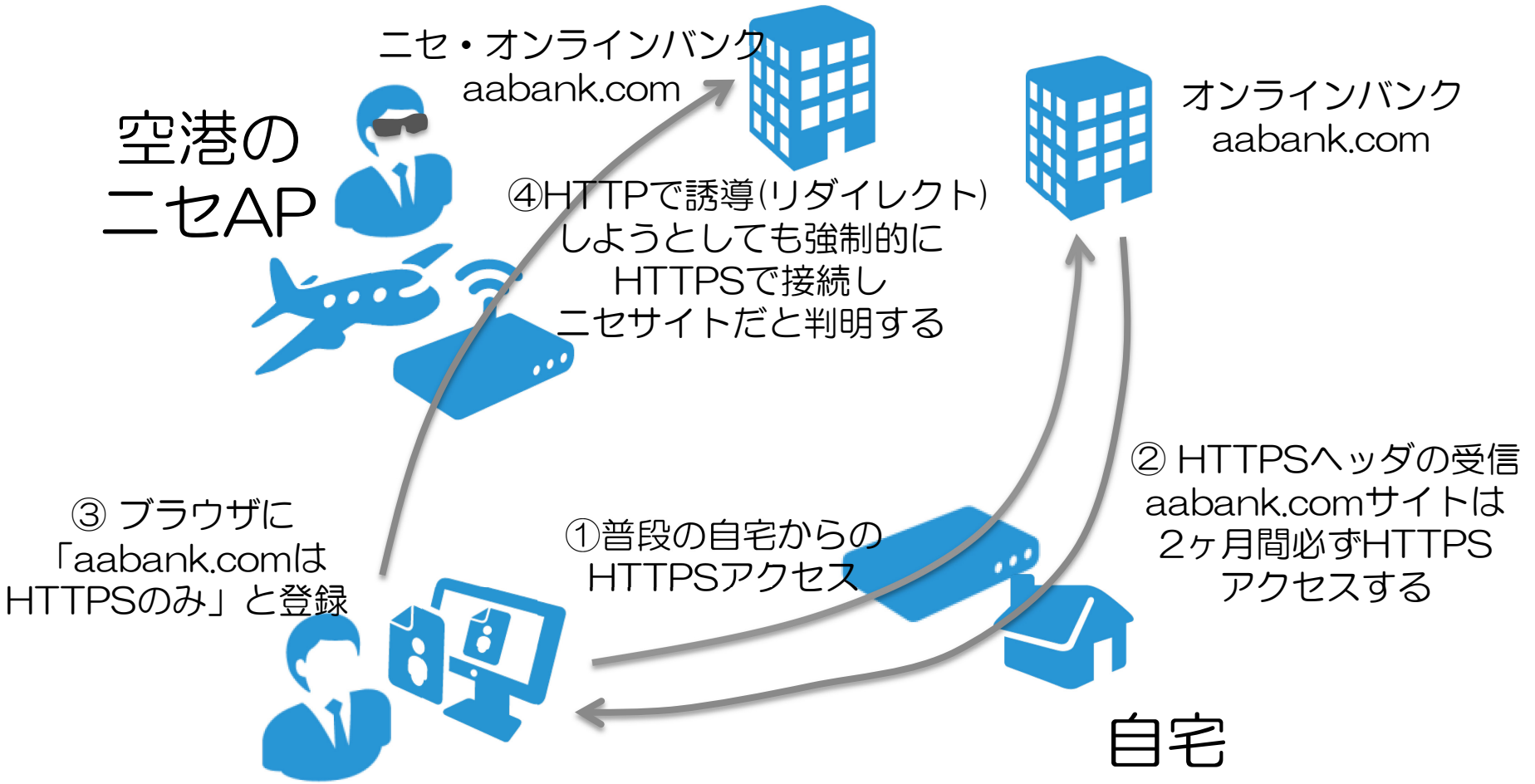


FUJI Xerox

SSL/TLSサーバー設定のポイント
オプション③
HSTS(HTTPSの強制)

HSTSによる強制的なHTTPS接続

RFC 6797 HTTP Strict Transport Secuirty（HSTS）
普段、HTTPSでアクセスしているオンラインバンキングサイトに、空港など外出先でアクセスした場合、そのアクセスポイントが不正APで、ニセのHTTPで作ったサイトに誘導しようとしても、HSTS機能が有効であれば、二回目以降の接続は自動的にHTTPSサイトへ接続します。



今後当面の
SSLサーバー証明書の購入ポイント

SSLサーバー証明書の購入時のチェックポイント

①鍵長(RSA 2048bit以上、ECDSA 256bit以上)
(NIST: RSA1024bitは2013年末まで)

②SHA2証明書への移行を検討を
Googleは2014年11月頃からSHA1だと警告がでる
Microsoftは2017年1月からSHA1証明書をサポートしない

③OCSPに対応している所がよい

④フィーチャーフォン、ゲーム機、VoIPの対応が必要ならベンダーによく確認を(鍵長,SHA2,パス長で問題になることも)

⑤ワイルドカード証明書、マルチドメイン証明書は鍵の運用もよく考えて導入を

⑥必要であればアドレスバーが緑になるEV証明書を

まとめ

まとめ

デフォルト設定のままでは昨今のSSL脆弱性に対抗できない
面倒でも、きめ細かいウェブサーバーのSSL設定を！

- SSL/TLSの設定ポイント
  - 暗号の設定(暗号スイートの設定)
  - 暗号スイートの順序のサーバー優先
  - 使用プロトコルバージョン
  - 圧縮設定の解除
  - 証明書の設定
  - オプション：Certificate/Public Key Pinning
  - オプション：OCSPステープリング
  - オプション：HSTS(HTTPSの強制)
- 今後のSSLサーバー証明書の購入ポイント

講演「サーバーのSSL/TLS設定のツボ」補足ページ
http://www9.atwiki.jp/kurushima/pages/108.html
本講演後、設定ファイル例、暗号スイートリストなどの補足情報を提供予定

「最新環境」と「レガシーを含む幅広い環境」のサーバー設定まとめ

		最新環境のみを サポートする場合	レガシーな環境を含む、 幅広い環境をサポートする場合
サーバー SSL設定	証明書設定	必要があれば中間CA証明書を忘れずに設定する	
	暗号スイート	ECDSA,AES,GCM, SHA2をメインに	ECDSA,AES,GCM,SHA2メイン+レガシーをサポートできるもの 1) POODLE, BEAST攻撃をあきらめるなら3DES,RSA-AES128を追加 2) RC4の危殆化をあきらめるならRC4を追加
	プロトコルバージョン	TLSv1.1, TLSv1.2	TLSv1.2, TLSv1.1, TLSv1, SSLv3
	暗号スイートサーバー優先	サーバー優先を有効に	
	圧縮設定	圧縮設定を解除する	
	Certificate Pinning	Certificate Pinningを設定	
	HSTS(HTTPSの強制)	HSTSを有効に	パフォーマンスを考慮してHSTSの導入を検討する
	OCSPステープリング	なるべくOCSP ステープリング有効に	パフォーマンスに配慮してOCSPステープリングの導入を検討 (レガシーのパフォーマンスダウンに配慮して止めた方がいい)
SSL サーバー 証明書	鍵と鍵長	RSA2048bitか ECDSA256bit以上	RSA2048bit (2048bitに対応しないレガシーに配慮するが 今やほとんどの認証局は1024bitを発行してくれない)
	ハッシュ関数	SHA2	・2017年1月までにはレガシーを捨ててSHA2へ移行 ・有効期間を考えると2016年1月頃までにはSHA2へ移行 ・SHA1しかサポートしないレガシーのためには 短い有効期間のSHA1で繋いでいくしかない
	ルート認証局	注意点なし	レガシー環境のサポートが必要な場合、特に証明書発行サービスによく相談を (信頼するルート認証局のリスト、鍵長、アルゴリズム、拡張、識別名、パス長など)
	その他	EV、マルチドメイン、ワイルドはお好みで(運用要件に合わせて)	

Apache HTTP ServerのSSL設定例

```
<VirtualHost *:443>
中略
SSLEngine on
SSLCertificateFile /etc/ssl/chain+ecparam.crt
SSLCertificateKeyFile /etc/ssl/server.key
SSLCipherSuite "暗号スイート設定例は別紙"
SSLProtocol All -SSLv2 -SSLv3
SSLHonorCipherOrder On
SSLCompression off
Header always set Public-Key-Pins "max-age=3000; ¥
  pin-sha256=EE中略; ¥
  pin-sha256-IM1中略; ¥
  includeSubDomains"
Header always set Strict-Transport-Security
  'max-age=63072000; includeSubDomains'
SSLUseStapling On
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"
</VirtualHost>
```

証明書チェーンファイル
(中間CAを忘れずに。
ECDH*, DH*の鍵長も設定可)

プロトコル例(SSLv3無効)

暗号スイート・サーバー側優先

SSL圧縮OFF(CRIME,TIME攻撃対策)

Certificate Pinning
(不正/偽造証明書の検知)

HSTS(強制HTTPS)

OCSP Stapling(OCSP貼付け)

FUJI Xerox

SSLサーバー設定のチートシート(apache/nginx/lighttpd/IIS/Tomcat)(参考)

	Apache HTTP	nginx	lighttpd	IIS	Tomcat
証明書と鍵	2.4.8から SSLCertificateFile (EE>IM2>IM1) SSLCertificateKeyFile PRVKEY	ssl_certificate (EE>IM2>IM1) ssl_certificate_key PRVKEY	ssl.pemfile=(PRVKEY,EE) ssl.ca-file=(IM2>IM1)	ウィザードで選択	証明書ストア(JKS,PKCS12)で提供。keystoreFileとkeystorePassで設定
暗号スイート	SSLCipherSuite OSSLパターン	ssl_ciphers "OSSLパターン";	ssl.cipher-list = "OSSLパターン"	グループポリシーで列挙し設定	属性ciphers="列挙"
プロトコルバージョン	SSLProtocol All -SSLv2 -SSLv3	ssl_protocols TLSv1 TLSv1.1 TLSv1.2	ssl.use-sslv2 = "disable" ssl.use-sslv3 = "disable"	レジストリ設定だがNARTAC SoftのIIS Cryptoツールで簡単設定	6.0.39以降はsslEnabledProtocols、それ以前はprotocolsで指定。 protocols="TLSv1,TLSv1.1,TLSv1.2"
暗号スイートサーバー優先	SSLHonorCipherOrder On	ssl_prefer_server_ciphers on;	ssl.honor-cipher-order = "enable"	設定不能	非サポート 設定不能
圧縮フラグOFF	SSLCompression off	1.1.6+/1.0.9+かつOpenSSL 1.0.0+の場合、もしくは1.3.2+ /1.2.2+の場合デフォルトOFF	ssl.use-compression = "disable"	IIS 7.5/Server 2008 R2以降でも圧縮非サポートのため設定不要	圧縮非サポート 設定不能
ヘッダ設定方法	Header always set キー 値	add_header キー 値	setenv.add-response-header = (キー1=>値1, キー2=>値2…)	「IISマネージャー>機能ビュー>HTTPレスポンスヘッダ」で追加	
Certificate Pinningヘッダ	キー:Public-Key-Pins 値(例):pin-sha256="B64鍵ハッシュEE", pin-sha256="B64鍵ハッシュIM1", max-age=3000				非サポート 設定不能
HSTSヘッダ	キー:Strict-Transport-Security 値(例):'max-age=63072000; includeSubDomains'				非サポート 設定不能
OCSP Stapling	Apache 2.3.3以降 SSLUseStapling On SSLStaplingCache パス(時間)	ssl_stapling on; ssl_stapling_verify on; ssl_trusted_certificate パス;	非サポート 設定不能	WinSrv2008以降はデフォ有効	非サポート 設定不能
DH,DHEの鍵長設定	SSLCertificateFile指定ファイルにDH鍵パラメータを追記	ssl_dhparam DH鍵パラ	ssl.dh-file=DH鍵パラ	設定不能	設定不能
ECDH,ECDHEの鍵長の設定	SSLCertificateFile指定ファイルにEC鍵パラメータを追記	ssl_ecdh_curve 曲線名	ssl.ec-curve=曲線名	設定不能	設定不能

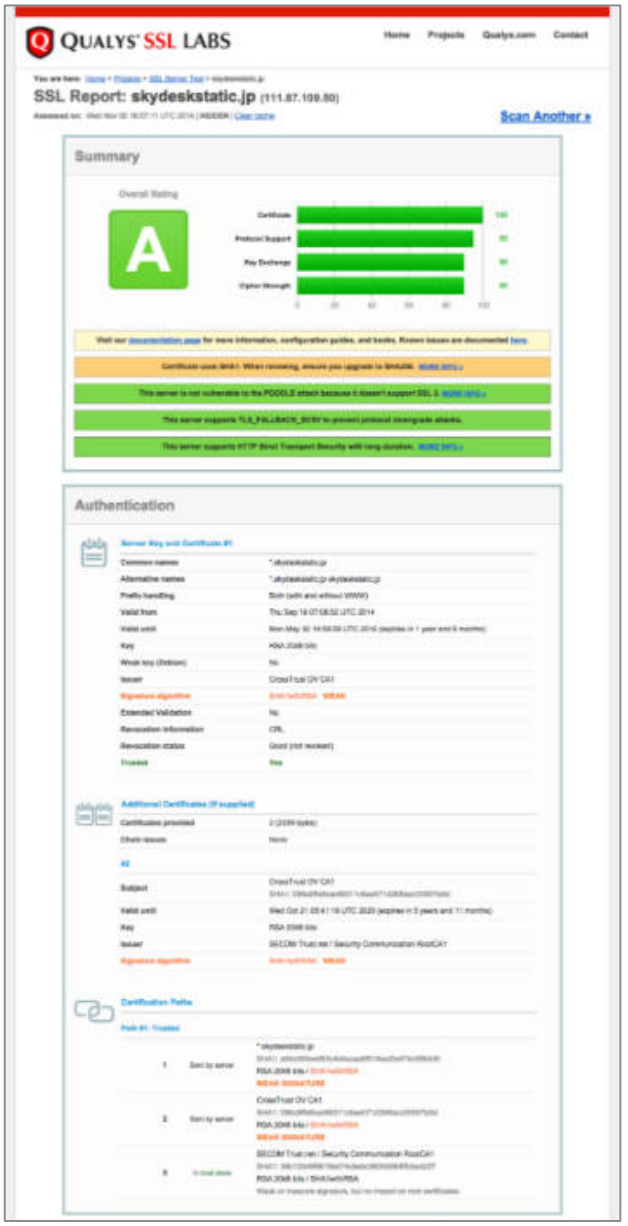
※略号:OSSLパターン:OpenSSLによる暗号スイート指定パターン文字列

FUJI Xerox

最後にQualys SSLLabsで設定を確認しましょう

https://www.ssllabs.com/ssltest/ を開きあなたのサイトのドメインを入力し「Do not show the results on the boards」をチェックしボタンを押します。

- あなたのサイトのSSL設定を様々な観点からチェックしてくれます。
- 対応している暗号スイート、プロトコルの確認
- 主要クライアントで選択される暗号スイート
- 証明書チェーン、OCSP、HSTS、Stapling
- 最近の脆弱性や設定項目の対応状況
  - POODLE
  - BEAST
  - ダウングレード攻撃
  - TLS圧縮の設定
  - RC4
  - CSSInjection
  - Forward Secrecy
  - HeartBleed
  - セキュアな再ネゴシエーション



FUJI Xerox

参考資料

■SSLの設定

https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices_1.3.pdf

SSL/TLS Deployment Best Practices

設定内容、解説等とてもオススメ。QualysのIvan Ristic氏著

■暗号アルゴリズムの選定

http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

NIST SP800-131A Transitions: Recommentation for Transitioning the Use of Cryptographic Algorithm and Key Lengths

http://www.cryptrec.go.jp/list.html

CRYPTREC暗号リスト

■個々の技術解説

http://d.hatena.ne.jp/jovi0608/20140902/1409635279

ぼちぼち日記：不正なSSL証明書を見破るPublic Key Pinningを試す