JNSA PKI相互運用WG・電子署名WG共催セミナー
PKI Day 2015 サイバーセキュリティの要となるPKIを見直す

SSL/TLS生誕20年、脆弱性と対策を振返る

2015年4月10日(金) 13:40-14:15
於：ヒューリックカンファレンス秋葉原ROOM1

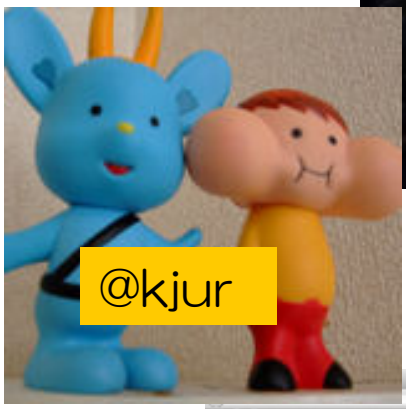
富士ゼロックス株式会社　漆嶌　賢二, CISSP

FUJI Xerox

自己紹介: 漆嶌 賢二(うるしま), CISSP

- 経歴
  - 富士ゼロックス(2010~)
  - エントラストジャパン(2005~2010)
  - セコム(1988~2005)
- 興味：

  PKI, TLS, 電子署名, SSO, 認証, 暗号,
  CSIRT, 脆弱性検査, フォレンジック,
  スマホ, プログラミング, ビットコイン
- 別名
  - 証明書ハンター
  - (TLS)暗号スイートウォッチャー
- 委員、標準化、認定基準、実証実験、普及啓蒙
  - CRYPTREC, 日本データ通信協会
  - 旧ECOM, PKI-J, JNSA, 欧州ETSI
  - PKI, 長期署名, タイムスタンプ, TLS



ブログ：自堕落な技術者の日記

jsrsasign –
JavaScript 実装暗号ライブラリ

FUJI Xerox

アジェンダ

- SSL/TLSとは
- SSL/TLSの歴史
  - プロトコルの歴史
  - クライアントの歴史
  - サーバーの歴史
  - ライブラリの歴史
- 脆弱性の歴史
- 脆弱性への対応の整理(4つの分類)
- TLSやPKIの脆弱性対策技術の最新動向

SSL/TLSとは

アマゾンでの商品購入例とSSL/TLS

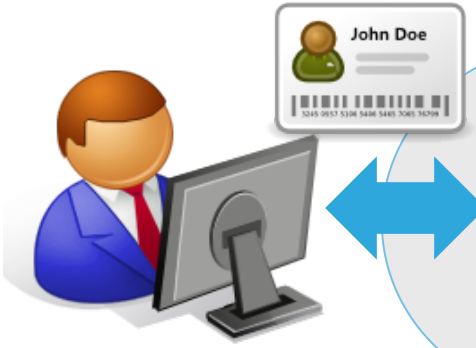
出典：アマゾン(www.amazon.co.jp)

FUJI Xerox

HTTPS暗号通信はなぜ必要なのか

アマゾンでの商品購入例

amazon.com



クレジットカード番号
住所・氏名
秘密にしたい買い物

SSL/TLSが守る

「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

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。

今のネットに必須の機能

途中で「届け先住所」を書き換えて商品を騙し取られたくない。

FUJI Xerox

SSL/TLSの3つの機能

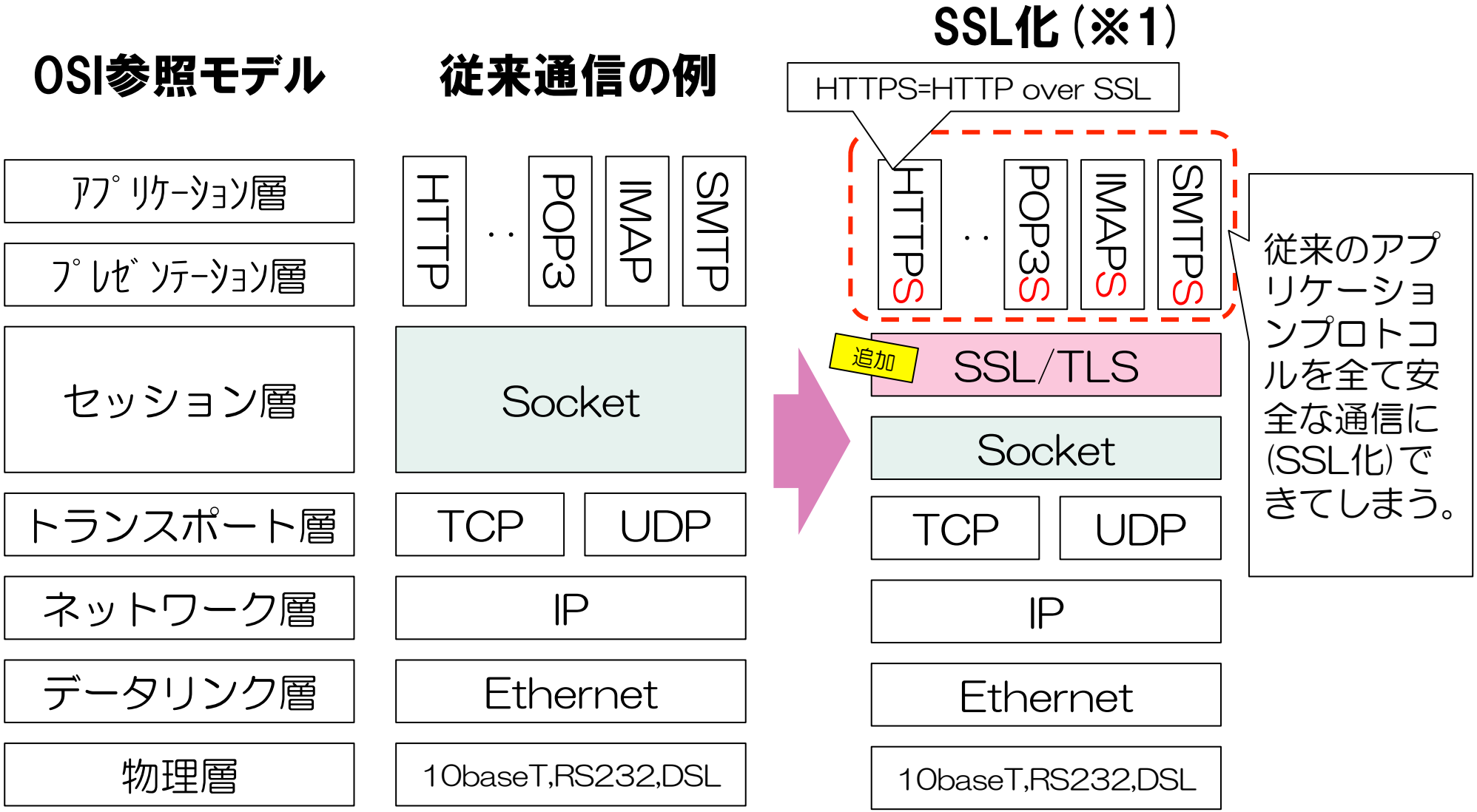
「カード番号、住所、氏名、買い物の内容」を途中で見られたくない

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。

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。

機密性	相手認証	完全性
暗号通信により通信相手以外に通信内容を盗み見(盗聴)されないようにする	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する	通信の途中でデータが書き換え(改ざん)されないよう、改ざん検知できる
覗き見(盗聴)防止	なりすまし防止	改ざん防止
共通鍵暗号を使う	*PKI(公開鍵暗号)、パスワード、Kerberos認証を使う*	*MAC(メッセージ認証コード)を使う*

SSL/TLSの特徴(HTTPでも何でも乗る)



※1：他にLDAPS, FTPS, TELNETSとか

FUJI Xerox

SSL/TLSの歴史

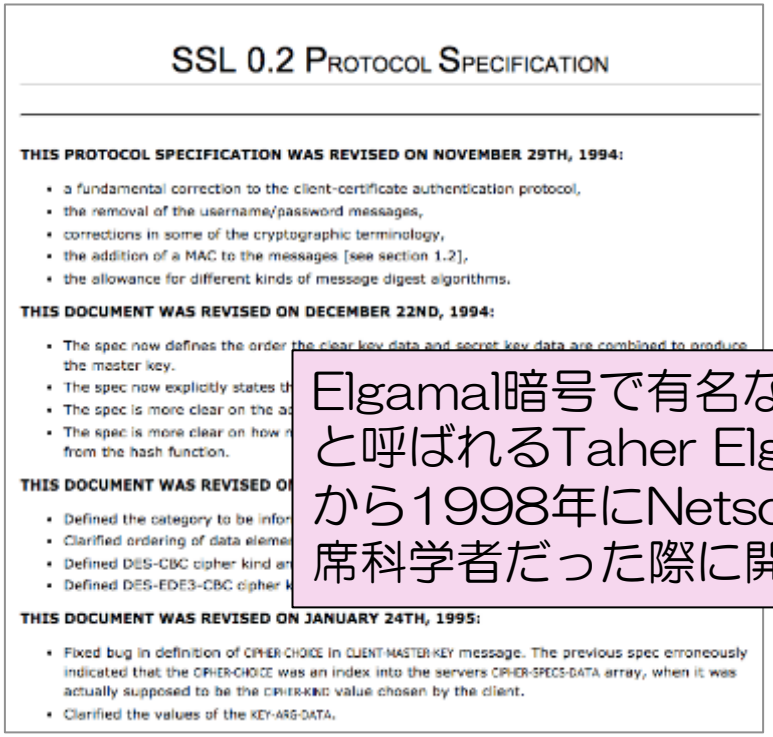
そもそもの始まり(SSL 2.0、SSL 3.0) 1995年

SSL 1.0

1995年

SSL 2.0 Protocol Specification
1995年2月
Kipp E.B. Hickman / Netscape

SSL Protocol 3.0
1996年11月18日
Alan O. Freier / Netscape
Philip Karlton / Netscape
Paul C. Kocher


SSL 0.2 PROTOCOL SPECIFICATION

THIS PROTOCOL SPECIFICATION WAS REVISED ON NOVEMBER 29TH, 1994:

- a fundamental correction to the client-certificate authentication protocol,
- the removal of the username/password messages,
- corrections in some of the cryptographic terminology,
- the addition of a MAC to the messages [see section 1.2],
- the allowance for different kinds of message digest algorithms.

THIS DOCUMENT WAS REVISED ON DECEMBER 22ND, 1994:

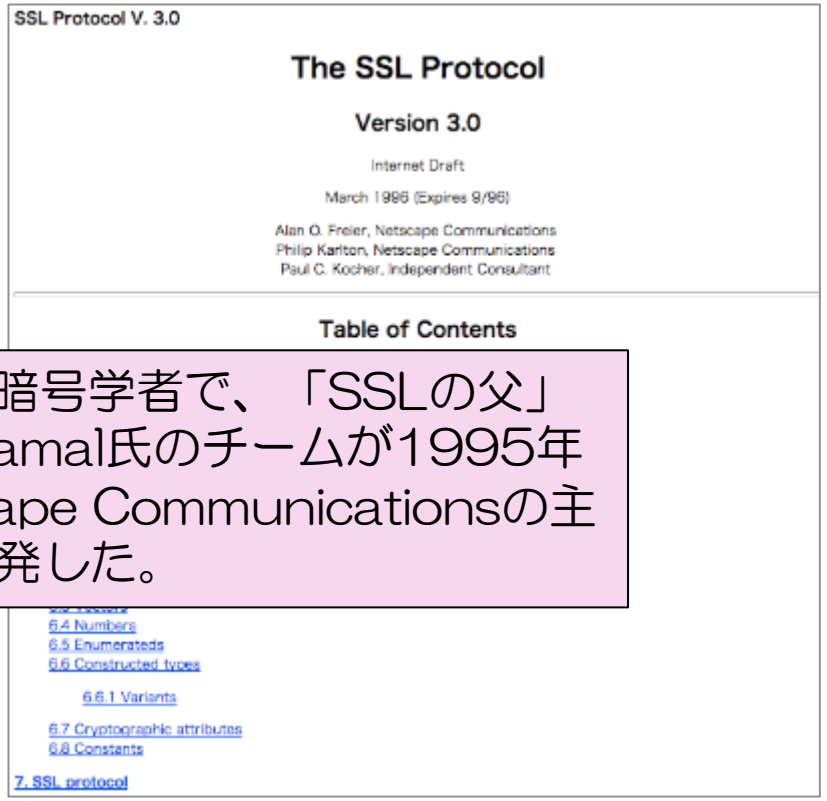
- The spec now defines the order the clear key data and secret key data are combined to produce the master key.
- The spec now explicitly states th
- The spec is more clear on the ac
- The spec is more clear on how
from the hash function.

THIS DOCUMENT WAS REVISED O

- Defined the category to be infor
- Clarified ordering of data eleme
- Defined DES-CBC cipher kind ar
- Defined DES-EDE3-CBC cipher k

THIS DOCUMENT WAS REVISED ON JANUARY 24TH, 1995:

- Fixed bug in definition of CIPHER-CHOICE in CLIENT-MASTER-KEY message. The previous spec erroneously indicated that the CIPHER-CHOICE was an index into the servers CIPHER-SPECS-DATA array, when it was actually supposed to be the CIPHER-KIND value chosen by the client.
- Clarified the values of the KEY-ARG-DATA.


SSL Protocol V. 3.0

The SSL Protocol

Version 3.0

Internet Draft

March 1996 (Expires 9/96)

Alan O. Freier, Netscape Communications
Philip Karlton, Netscape Communications
Paul C. Kocher, Independent Consultant

Table of Contents

6.4 Numbers
6.5 Enumerateds
6.6 Constructed types
6.6.1 Variants
6.7 Cryptographic attributes
6.8 Constants
7. SSL protocol

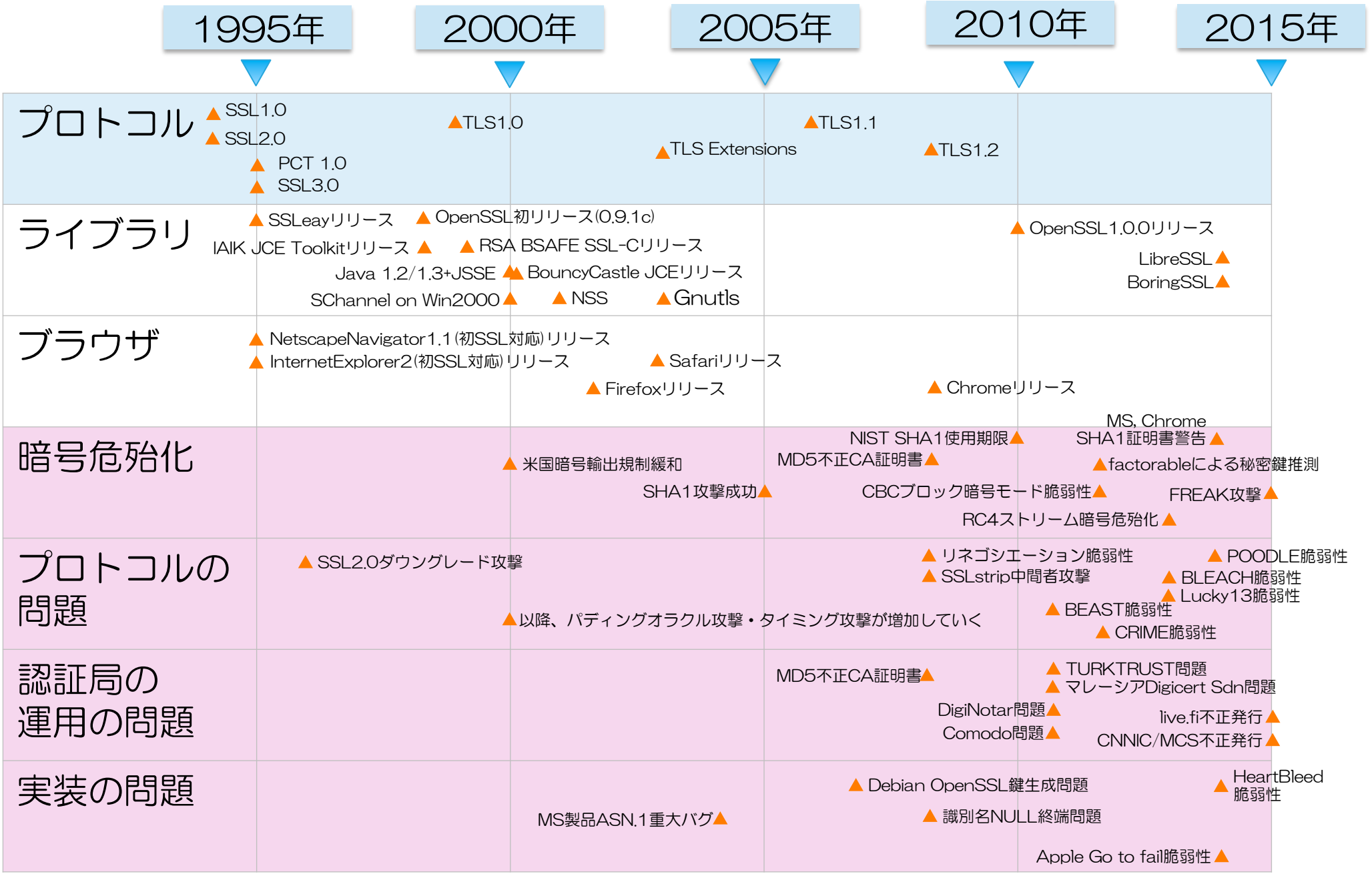
幾つかの致命的な設計上の欠陥が発見されリリースされなかった

Elgamal暗号で有名な暗号学者で、「SSLの父」と呼ばれるTaher Elgamal氏のチームが1995年から1998年にNetscape Communicationsの主席科学者だった際に開発した。

出典：http://www-archive.mozilla.org/projects/security/pki/nss/ssl/draft02.html
http://www.freesoft.org/CIE/Topics/ssl-draft/INDEX.HTM

FUJI Xerox

SSL/TLSの20年の歴史のまとめ

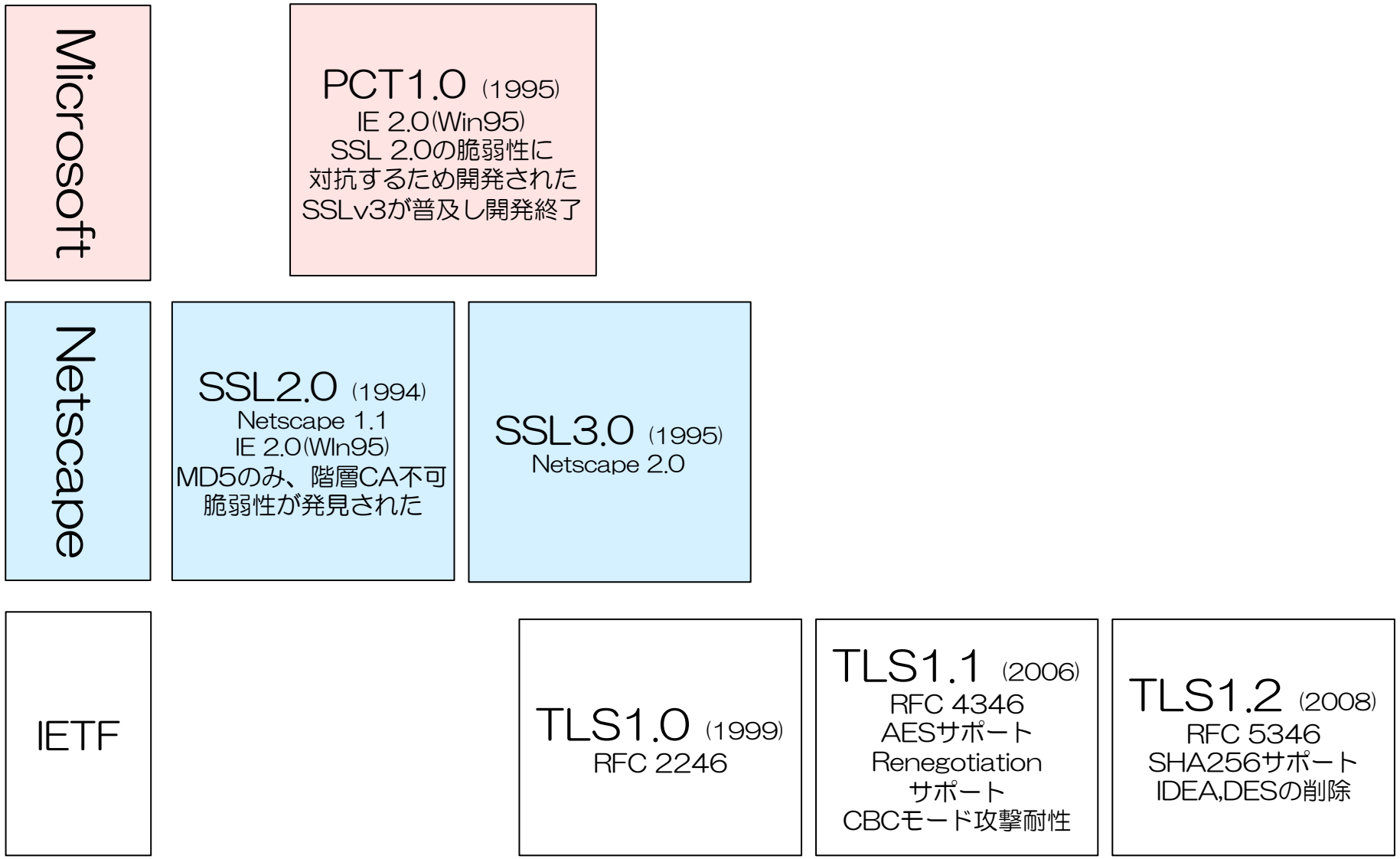


FUJI Xerox

SSL/TLSプロトコルの歴史

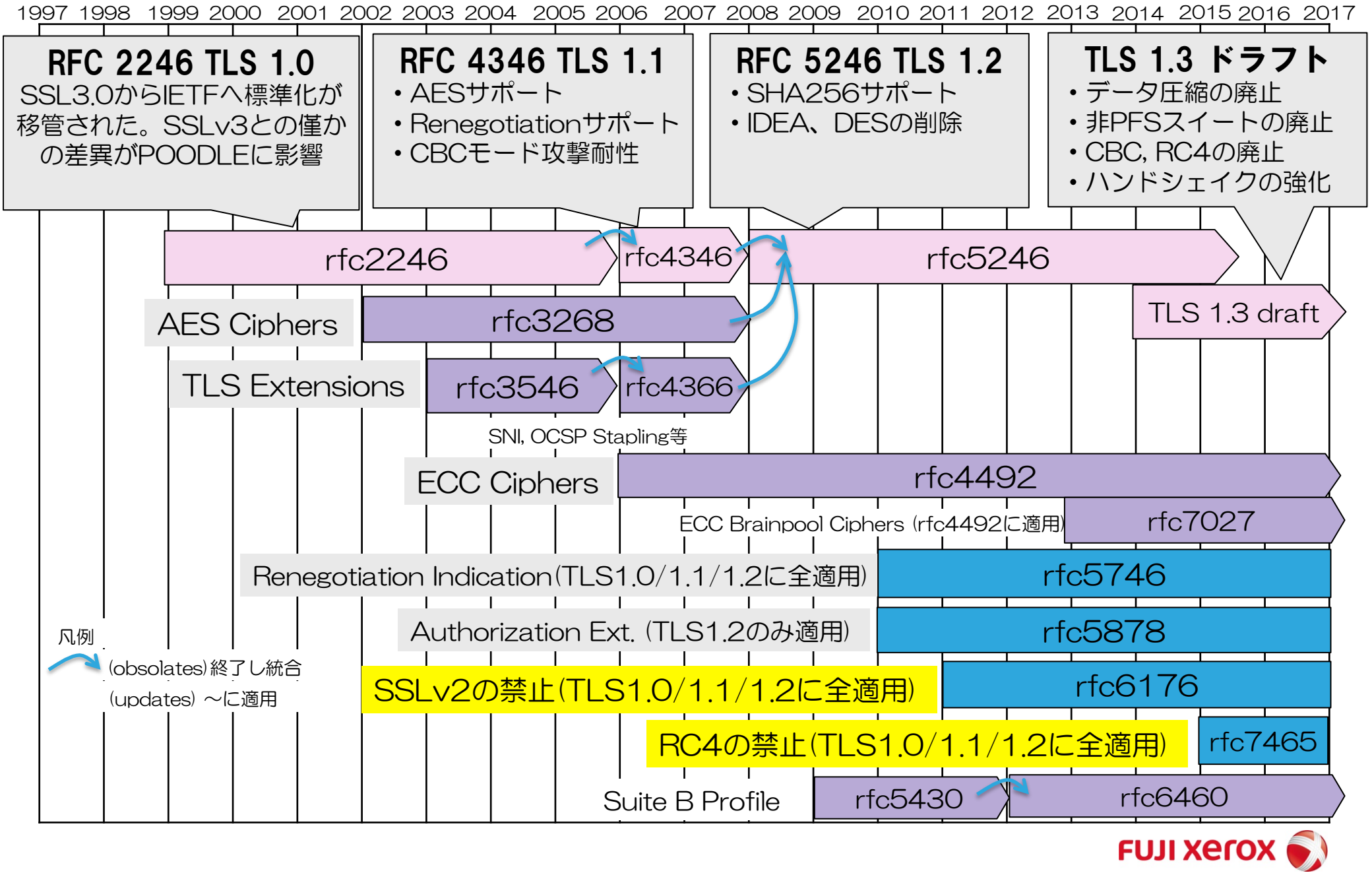
FUJI Xerox

SSL/TLSの標準仕様の歴史の概要



FUJI Xerox

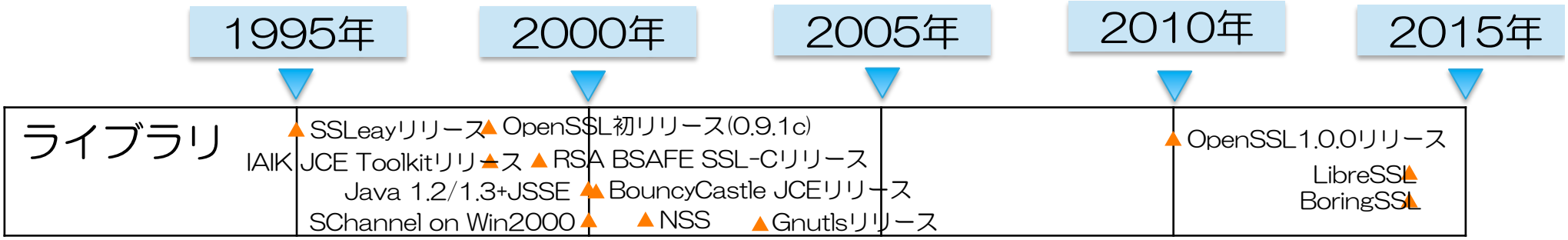
IETF RFCのSSL/TLS標準仕様



SSL/TLSライブラリの歴史

FUJI Xerox

SSL/TLSライブラリの歴史



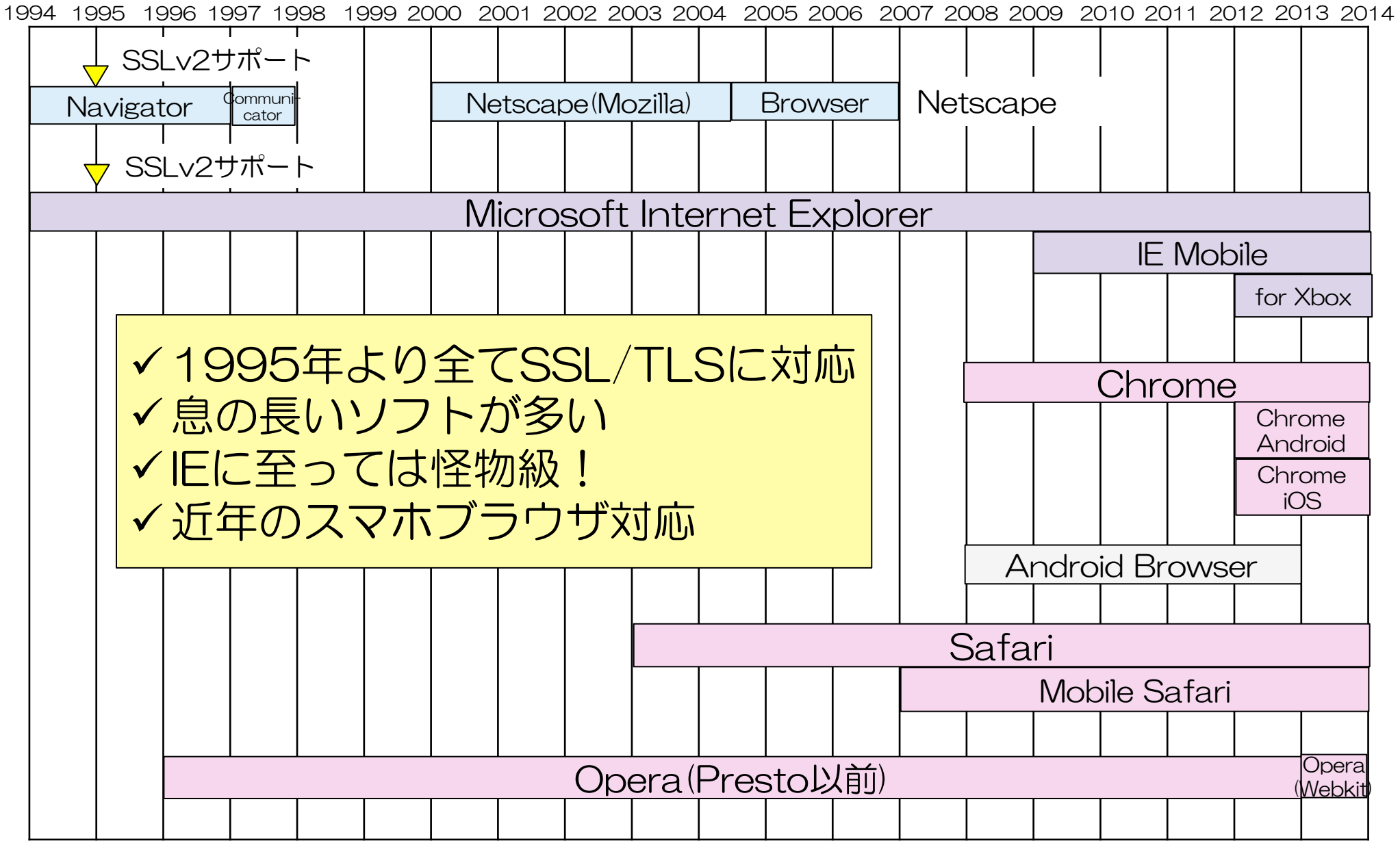
- 1995年、世界最初のSSLライブラリSSLeayリリース
- 1998年、SSLeayの後継としてOpenSSL 0.9.1c発リリース
- 1999年、SSLeayを元に商用ライブラリRSA BSAFE SSL-Cリリース
  - 以降、ゲーム機や組込みブラウザなど組込み製品には数多く利用されている
- 2000年、WindowsのSSL実装Schannel on Win2000リリース
- Javaでは暗号API(JCE)とSSL拡張(JSSE)の共通API仕様を策定
  - Sun 標準JCE、JSSE
  - 1998年、IAIK JCE Toolkit (商用ライブラリ 研究無償、企業有償)
  - 2000年、BouncyCastle JCEライブラリ(オープンソースライブラリ)
- 2001年、MozillaがNSSライブラリをリリース
- 2003年、GNUがgnutls 1.0をリリース
- OpenSSLのソースコードのメンテナンス性の低さ、脆弱性によりブランチ
  - 2014年、OpenBSDによりLibreSSLが、GoogleによりBoringSSLがリリース

FUJI Xerox

SSL/TLSブラウザの歴史

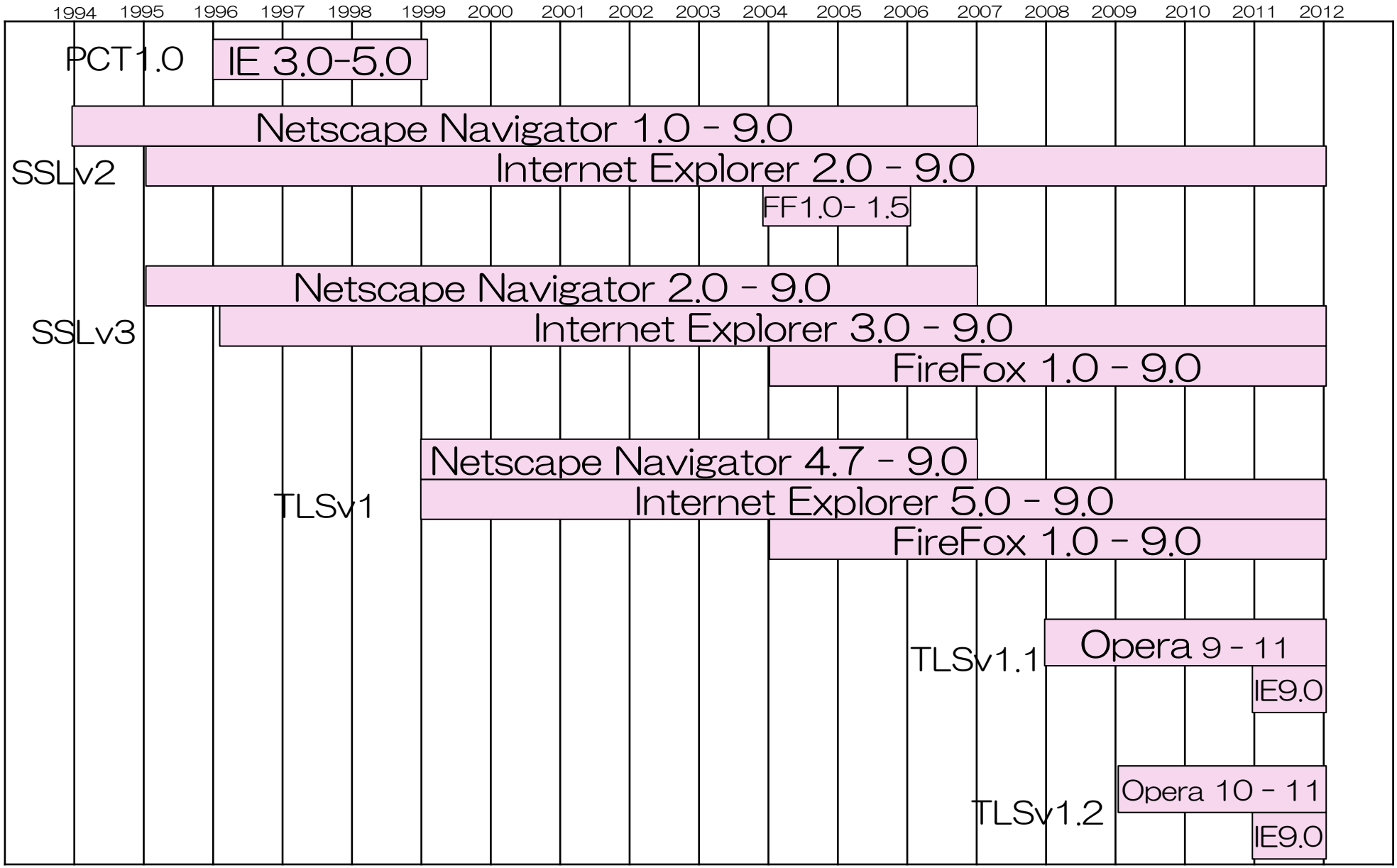
FUJI Xerox

ブラウザの歴史



FUJI Xerox

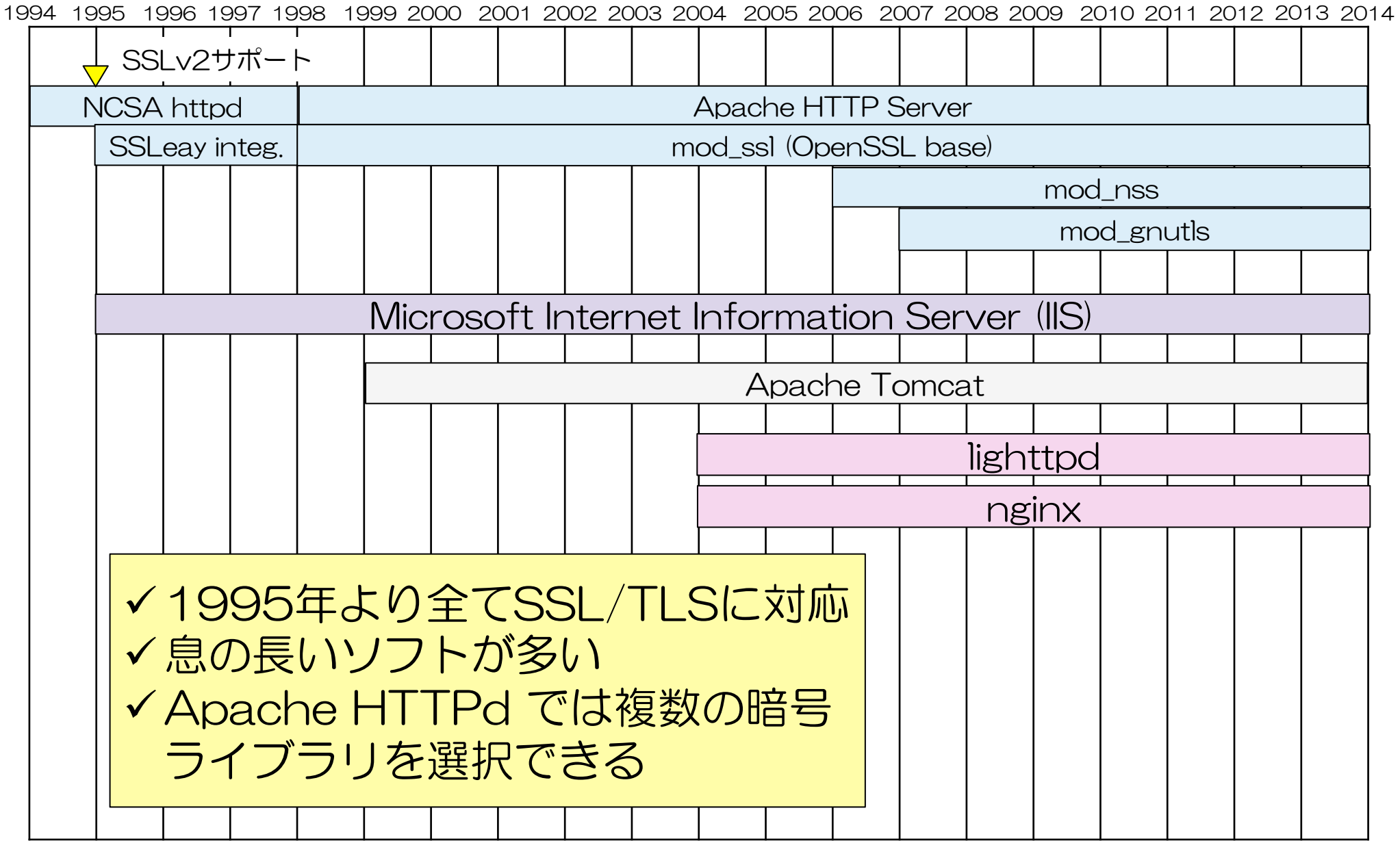
SSL/TLSバージョン対応とブラウザ(参考：2012年まで)



FUJI Xerox

SSL/TLS対応
ウェブサーバーの歴史

SSL対応ウェブサーバー、コンテナの歴史



- ✓1995年より全てSSL/TLSに対応
- ✓息の長いソフトが多い
- ✓Apache HTTPd では複数の暗号ライブラリを選択できる

FUJI Xerox

SSL/TLS関連の脆弱性の歴史と脆弱性対応の整理

FUJI Xerox

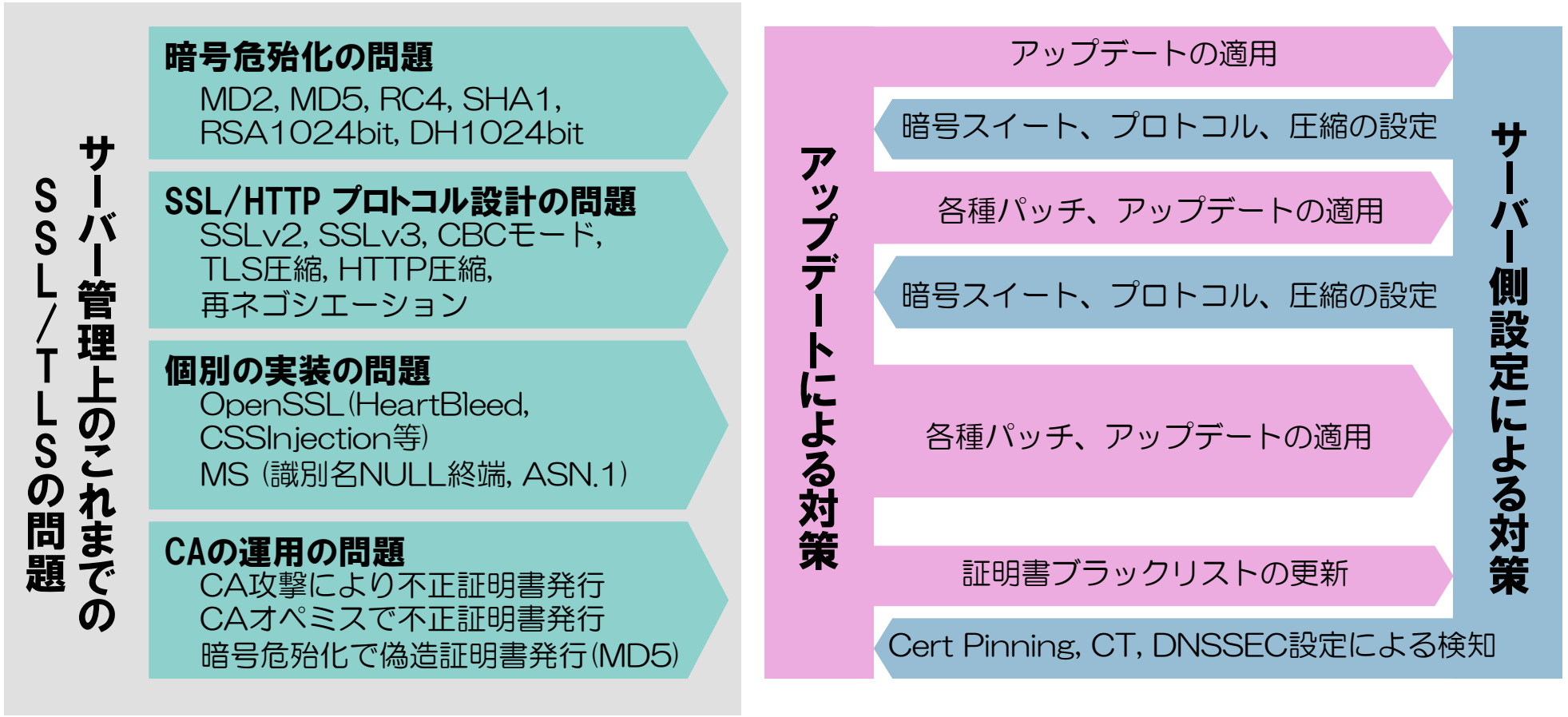
SSL/TLSの過去の主要な問題と対応

サーバー設定で回避し続けならないものも多数

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

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(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)とPFS	暗号スイート/プロトコル設定(ECDHE,DHE使用)
2014.02	Apple OSX, iOS goto fail 問題 ★	アップデート
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)
2015.03	FREAK攻撃	暗号スイート(非EXPORT)
2015.03	live.fi、CNNIC/MCS不正証明書発行(運用不備)	アップデートやPinning(CABF BR要件に課題も)
2015.03	パスワード盗聴可能なRC4暗号スイート攻撃	暗号スイート設定(非RC4)

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

第６位：個別の実装の問題から
Apple Mac OS X、iOSのgoto fail脆弱性(2014年2月)

```
        ：中略
if (err = Hash.update(値1)) != 0)
        goto fail;
        goto fail;
if (err = Hash.final(ハッシュ結果) != 0)
        goto fail;
err = VerifySignature(公開鍵, データ,署名値)

fail:
        メモリの開放等後処理
        return err;
```

この部分は処理せずに
即ち、公開鍵で認証せずに
すべて成功して

値を返す

- Apple Secure Transportライブラリのバグ
- 多分、コピペミス？
- DHE、ECDHEを使いSSLv3～TLSv1.1で影響有
- iOSは 6.0.0 ～ 7.0.5までが脆弱
- Mac OS X Mavericks は 10.9.2 で修正
- 2013年10月からあったらしい

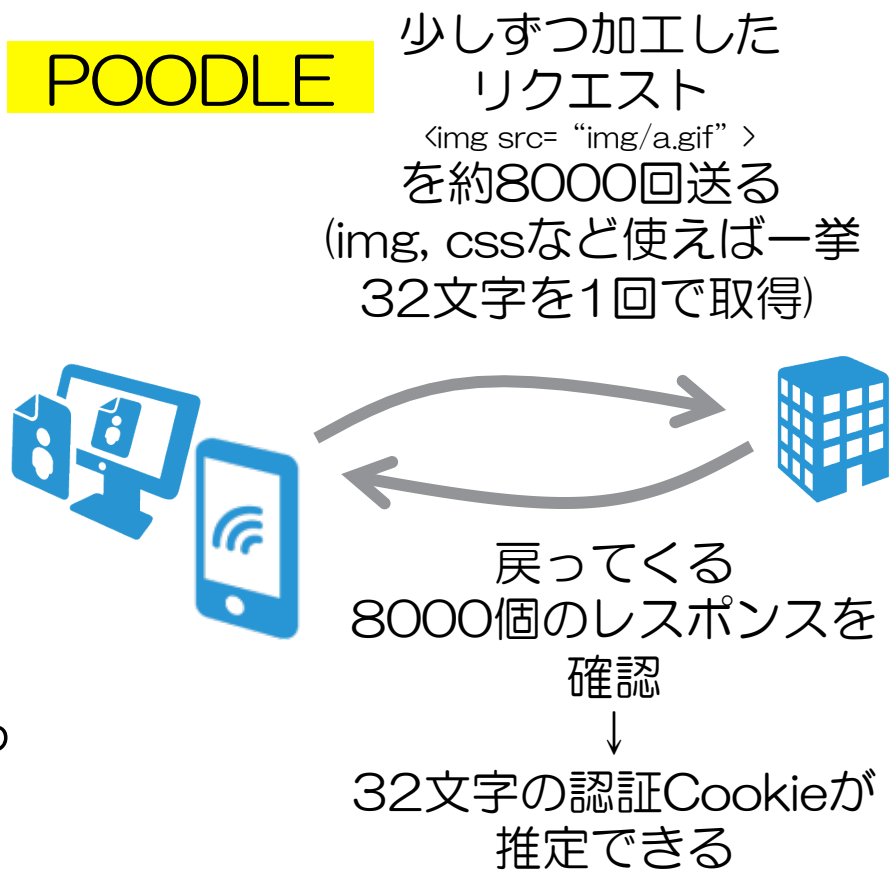
第５位：個別の実装の問題から(2009年7月)
NULL終端による証明書ホスト名一致確認不備

① 攻撃対象のドメインが shop.com だったとする。
② 適当なドメイン foo.co.jp を取得する。
③ CN=“shop.com¥0.foo.co.jp”の証明書をCSRを作り発行要求
④ CNの文字種を確認しないCAはそのまま証明書を発行
⑤ C言語では ¥0 は文字列の終端記号なので誤った実装では、¥0 を文字列終端として扱うために、④で発行された証明書を shop.com 用の証明書として利用できてしまう。

⑥ 実際にMicrosoftやFirefoxなど幾つかの実装に影響があり、アップデートが公開された。

第４位：プロトコル設計の問題から
POODLE攻撃(2014年10月)、BEAST(2011年9月)攻撃など

- BEAST
  - CBCモードの不備を突いて、クッキーを盗む
  - デモではJavaアプレットの脆弱性を突いて実施した。
  - FlashでもWebSocketでも何でも良かった
- POODLE
  - CBCモードとSSLv3のパディング検証をしない事を利用して、BEASTより格段に効率的にクッキを盗むことができるようになった



参考：SSL v3.0の脆弱性「POODLE」ってかわいい名前だけど何？？Padding Oracle On Downgraded Legacy Encryptionの仕組み
http://developers.mobage.jp/blog/poodle

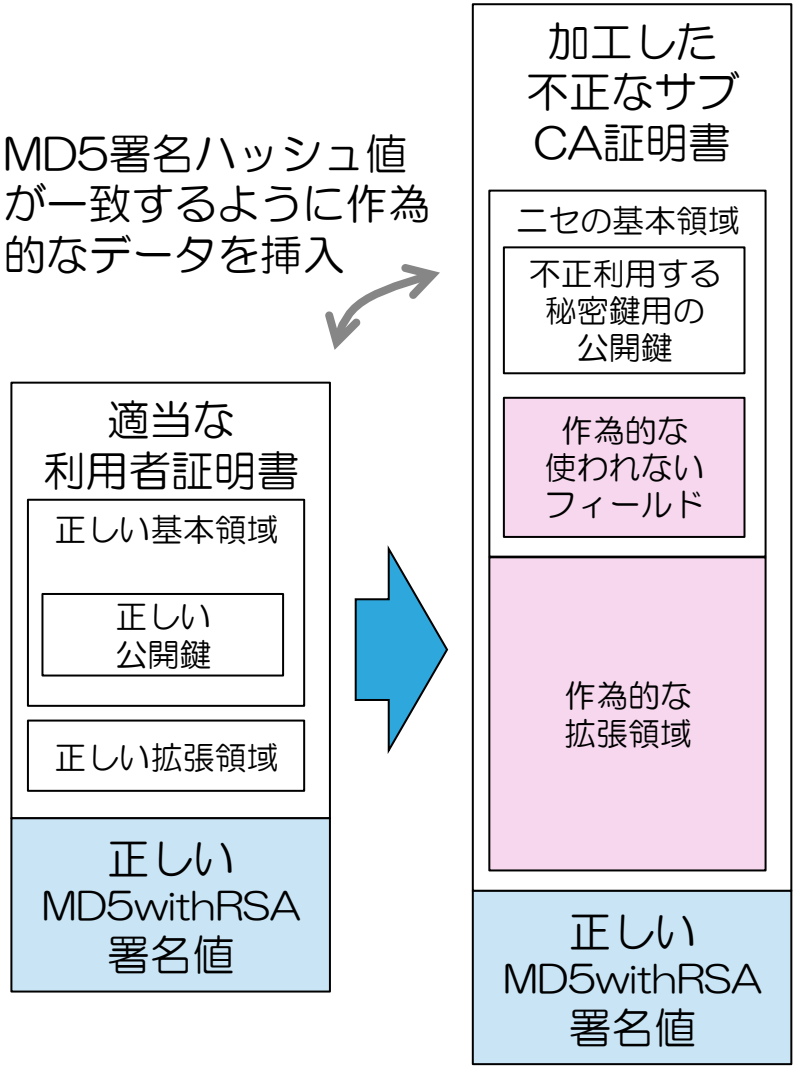
FUJI Xerox

第３位：認証局の運用の問題から
認証局の問題による不正証明書発行
(Comodo、DigiNotar、TURKTRUST、CNNICなど)

- 登録局(RA)のソフトウェアの脆弱性をつかれて証明書を不正発行
  - 2011年3月、ComodoはRA Windowsアプリの脆弱性を突かれた
  - 2011年8月、DigiNotarも同様にRAの攻撃により不正発行
- 運用のオペレーションミスにより不正発行
  - 2013年1月、トルコのTURKTRUST
- 弱い鍵により
  - 2011年11月、マレーシアDigicert SdnはRSA512bit CAだった
- ガイドラインの不備により
  - 2015年3月、Comodoはドメイン管理者と勘違いし*.live.fiを発行
- 暗号を破るより簡単に低コストで有効なサーバー証明書が入手できる
- *.google.com、*.gmail.com、*.yahoo.com、*.microsoft.comなどメジャーなサイトのワイルドが人気があり、盗聴に使われる。

第２位：暗号危殆化から MD5ハッシュ衝突による証明書偽造 (RapidSSL 2009年1月, FRAMEマルウェア2012年5月)

- RapidSSL
  - 2009年元旦あたり、本物の認証局(RapidSSL)を使って不正サブCA証明書が作れることを示したグループ。
  - 200台のPS3クラスタ
  - 2日以下でできた
- FLAMEマルウェア
  - Windows Terminalサーバー用の証明書から不正証明書を作った
  - 実際にFLAMEマルウェアのコード署名、*.google.comのサーバー証明書を作成
  - イラクISPの通信が盗聴
- 今は暗号破るよりRA攻撃が簡単？



第１位：個別の実装の問題から HeartBleed脆弱性(2014年4月 CVE-2014-0160)

RFC 6520 TLS HeartBeat拡張という死活監視機能を悪用して、OpenSSLのサーバーでは、誰でもメモリの一部を取り出すことができ、運が良ければ認証クッキーやIDパスワードなどの情報が盗めた。

- OpenSSLだけの問題
- HeartBeat要求に対し任意の長さを受け付けるようになっていたので、バッファオーバーランしてサーバーのメモリにある情報が盗めた。
- 運が良ければ認証クッキーやアカウント情報が通常のHTTPSアクセスで誰でも盗めた。

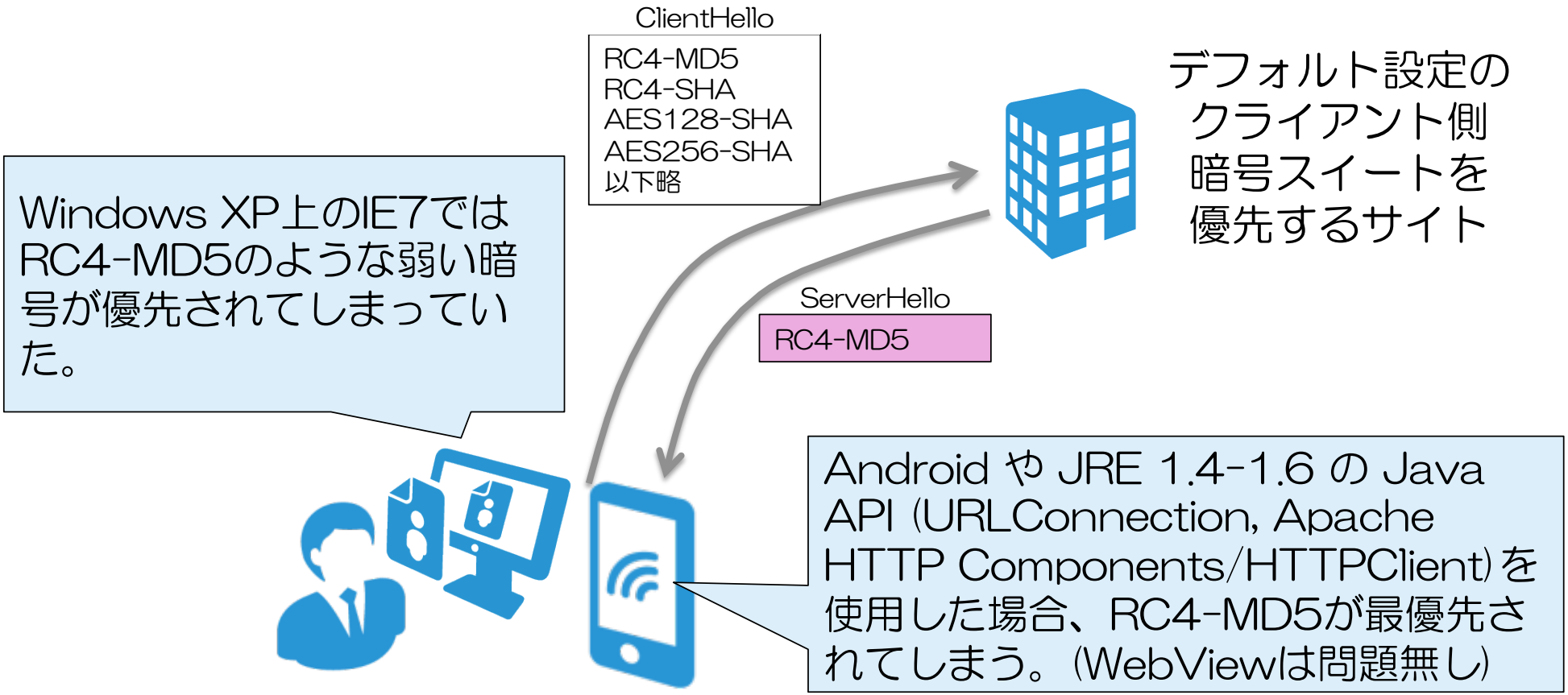
FUJI Xerox

SSL/TLS関連の脆弱性への対策技術の最新動向

FUJI Xerox

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

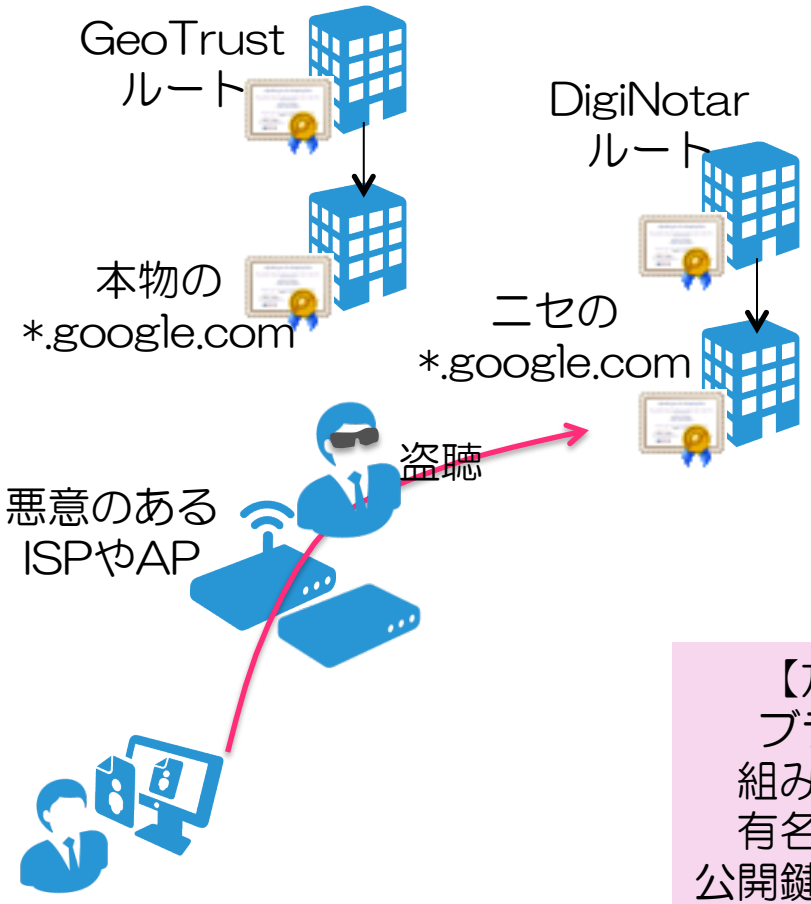
参考　PKIDay 2011 NTT武藤氏：SSLにおける暗号危殆化サンプル調査の報告　http://www.jnsa.org/seminar/pki-day/2011/data/03_mutoh.pdf
自堕落な技術者の日記 JRE 1.4-1.6やAndroidのAPIを使ったHTTPS接続のCipherSuitesのRC4-MD5優先　http://blog.livedoor.jp/k_urushima/archives/1727793.html

FUJI Xerox

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

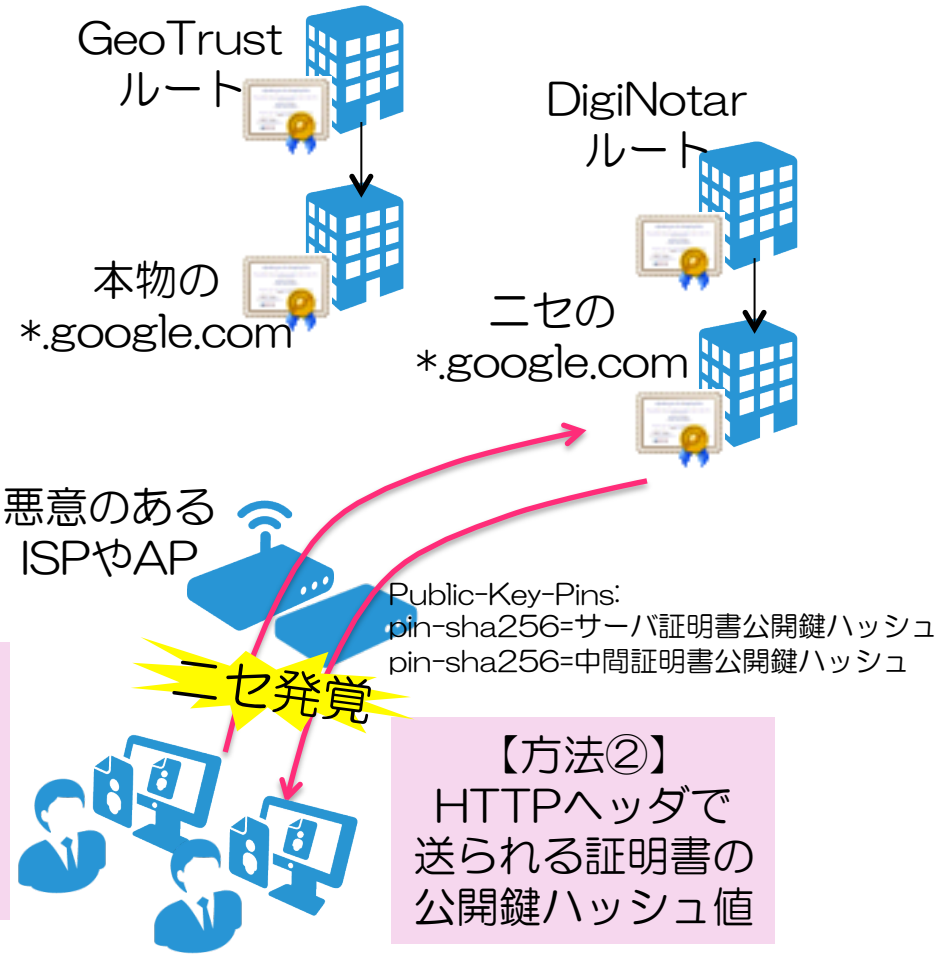
Pinningはニセ証明書対策に効果がある

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

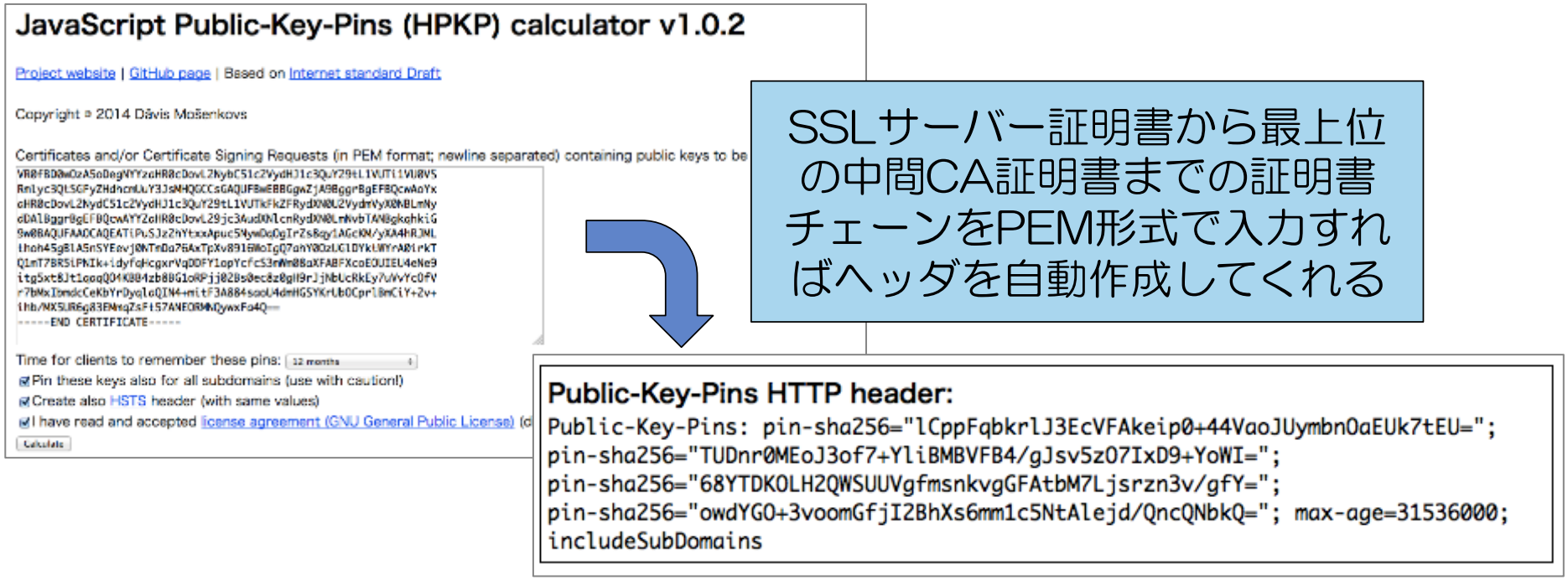


【方法②】
HTTPヘッダで
送られる証明書の
公開鍵ハッシュ値

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

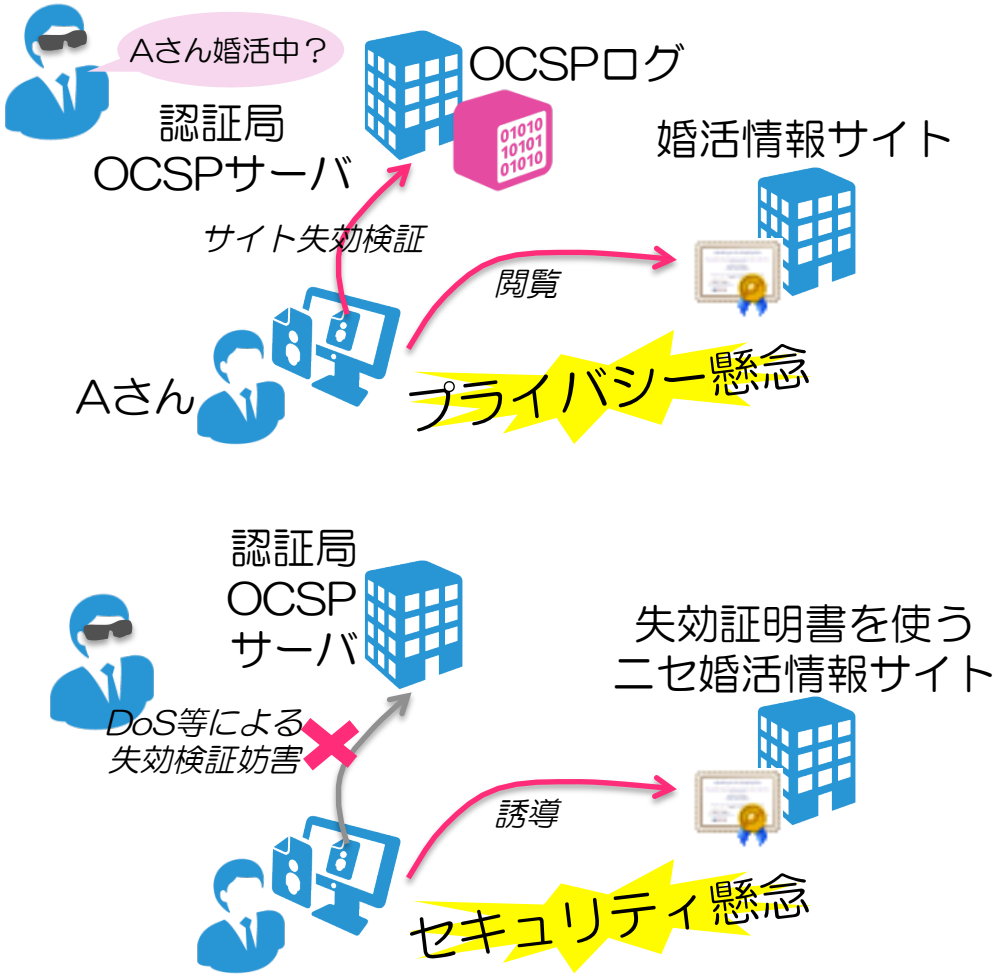


FUJI Xerox

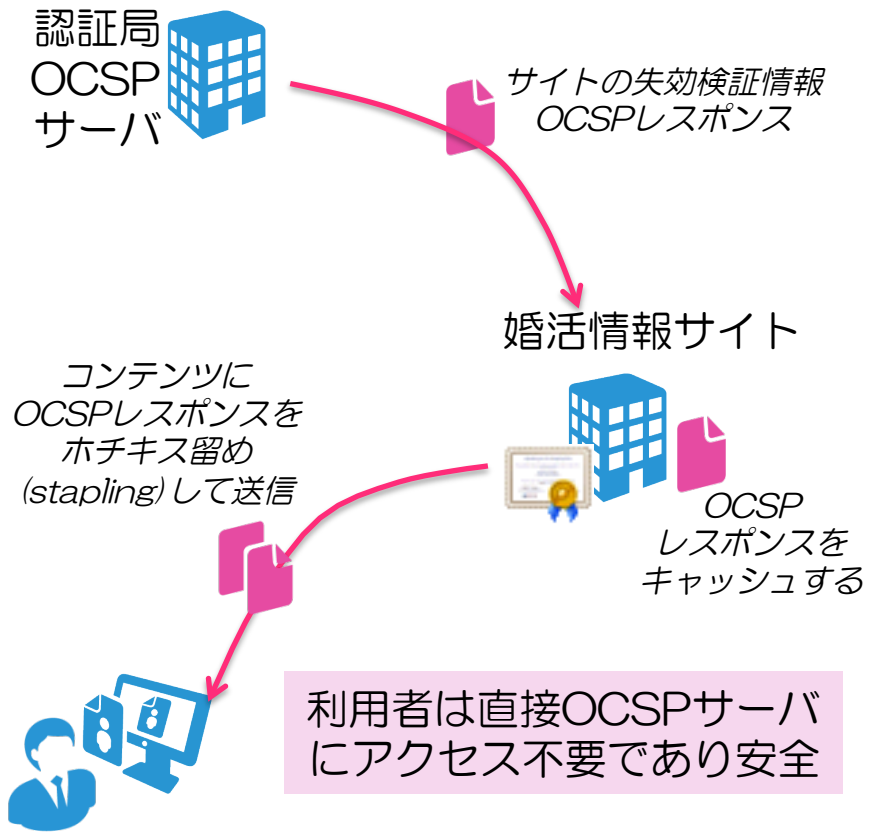
OCSP Stapling(RFC 6066TLS拡張8章)の意義と仕組み

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



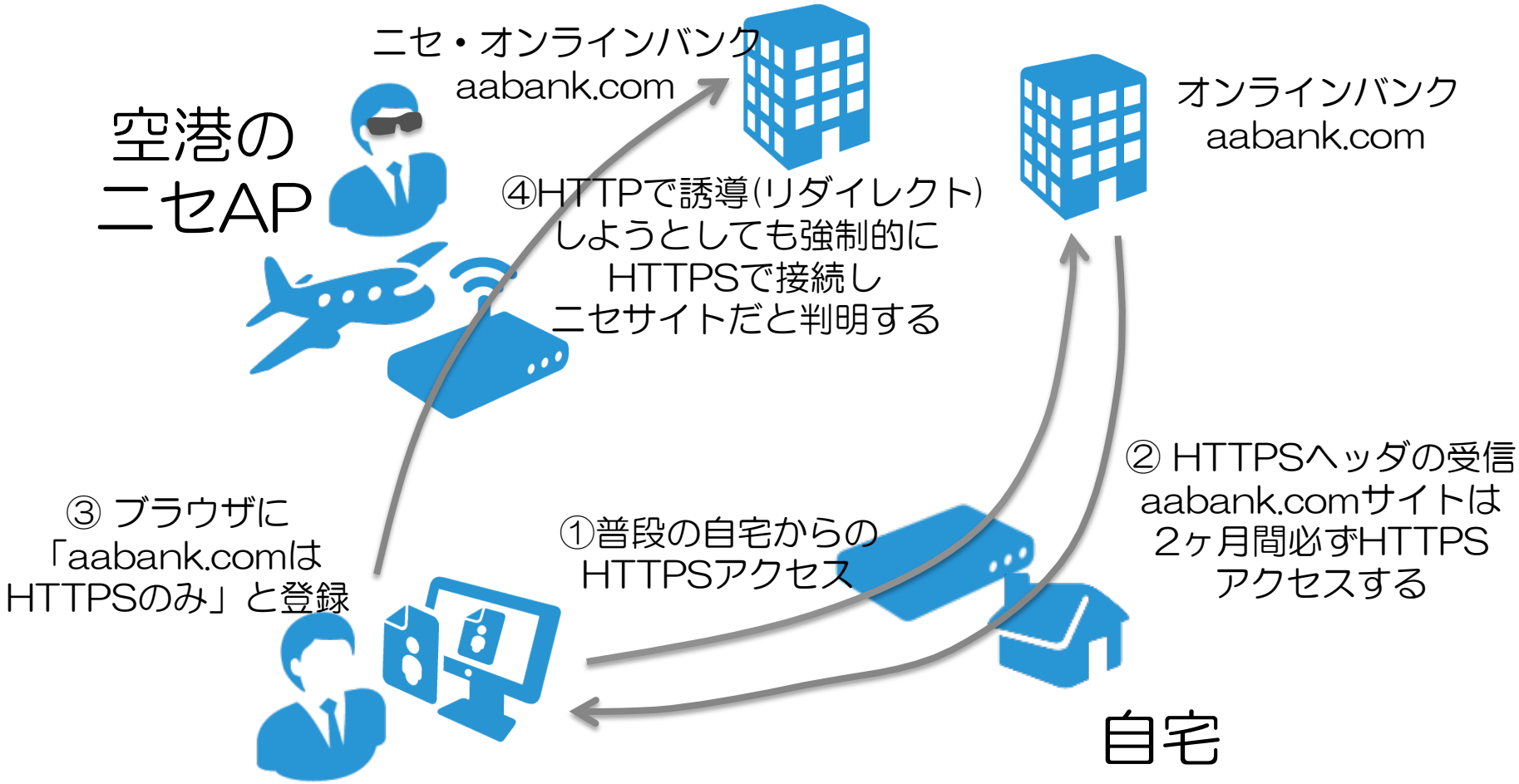
OCSP Staplingがある場合



FUJI Xerox

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。



Microsoft製品、Google ChromeのSHA1証明書からの移行(1/2)

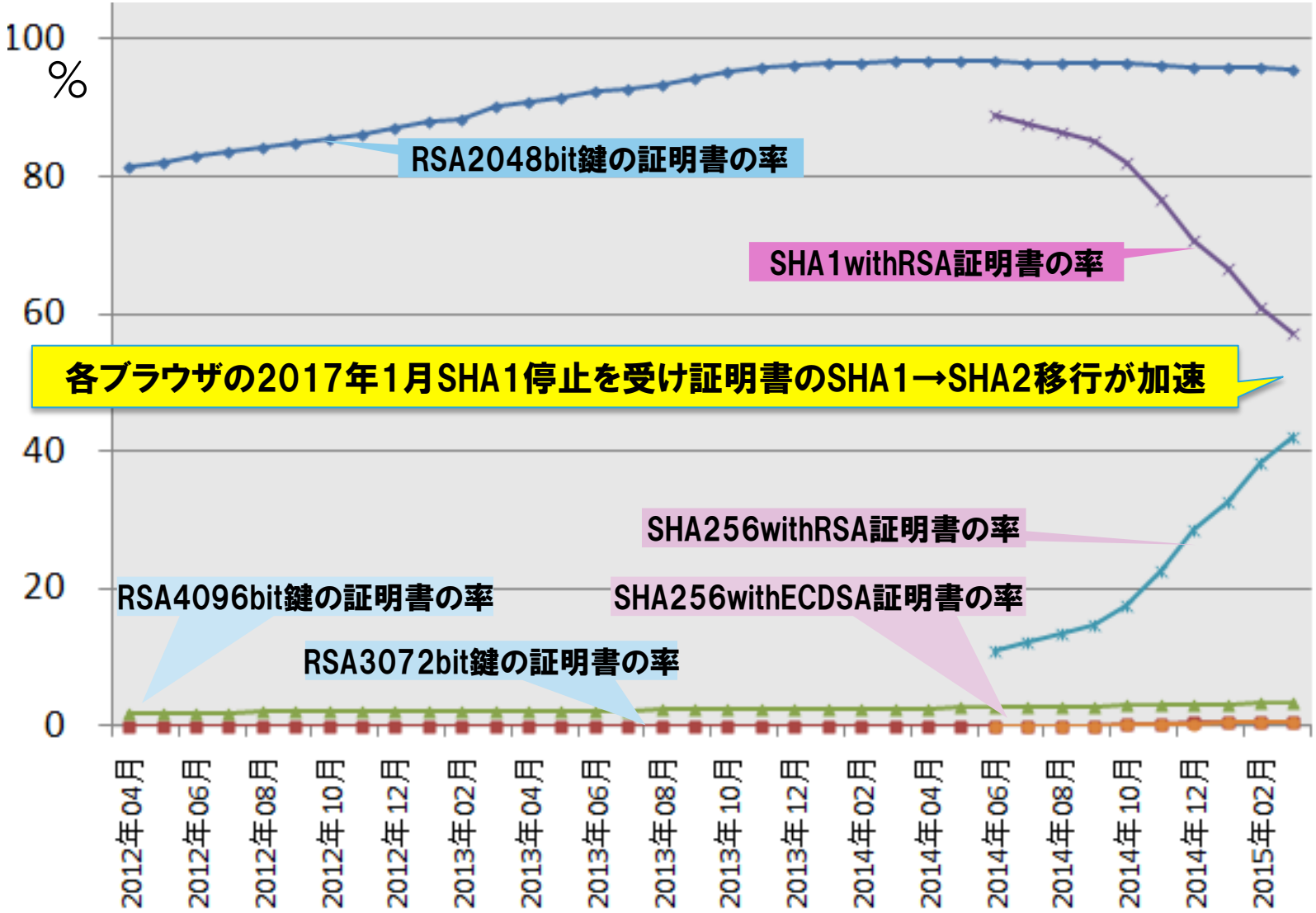
- Windowsルート証明書プログラムのルートCA配下は2016年1月1日以降、SHA1証明書を発行できない。
- Windows製品では有効期限が2017年1月1日以降の証明書を受理しないためエラーとなる。
- Google ChromeはSHA1証明書の有効期限により、2015年1月以降のリリース版より下表の警告表示を開始し、2017年1月以降は受理しない。

Google Chrome		SHA1証明書の有効期限			
Chrome バージョン	安定版 リリース日	2015.12.31 まで	2016.05.31 まで	2016.12.31 まで	2017.01 以降
38	2014.10.08	https://	https://	https://	https://
39	2014.11.18	https://	https://	https://	https://
40	2015.01.21	https://	https://	https:// ☆	https:// ☆
42	2015.04中旬	https://	https:// ☆	https:// ☆	~~https~~:// ☆
2017.01直後	2017.01中旬	~~https~~:// ★	~~https~~:// ★	~~https~~:// ★	~~https~~:// ☆

記号：☆：Googleのポリシにより、★：証明書期限切れにより

FUJI Xerox

Microsoft製品、Google ChromeのSHA1証明書への警告(2/2)



データ出典：SSL Pulse(https://www.trustworthyinternet.org/ssl-pulse/)

2015年6月頃にはSHA1証明書とSHA256証明書の利用数が逆転しそう

FUJI Xerox

Certificate Transparency(1)

- ✓ 2011年、DigiCertやComodoなどで google.comドメイン不正証明書が 発行されイラクの通信が盗聴 その対策の一環として提案。
- ✓ 証明書発行の公開監査情報として、 証明書チェーンと登録日時を追記し署名される
- ✓ 2011年のGoogleの人の論文に基づく
- ✓ 実験RFC 6962になった
- ✓ Google Chromeのみが実験に対応
- ✓ ChromeはEV証明書の発行要件にした
- ✓ DigiCert, GlobalSignが先行対応
- ✓ 他の海外認証ベンダも対応中

CT対応のサイト(=GlobalSign or DigiCert)

鍵を右クリック

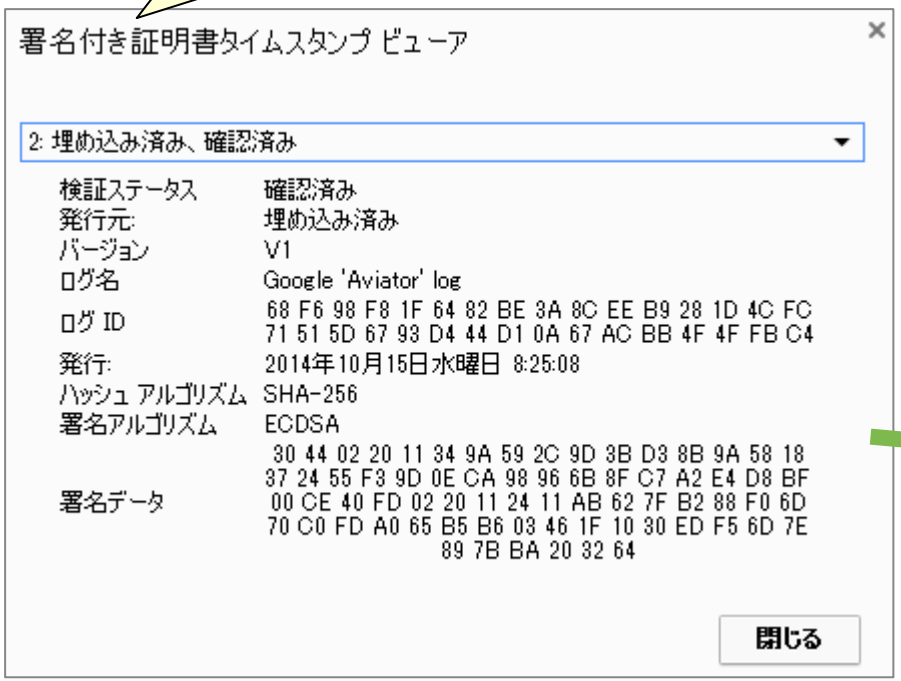
例の出典
https://www.digicert.com/

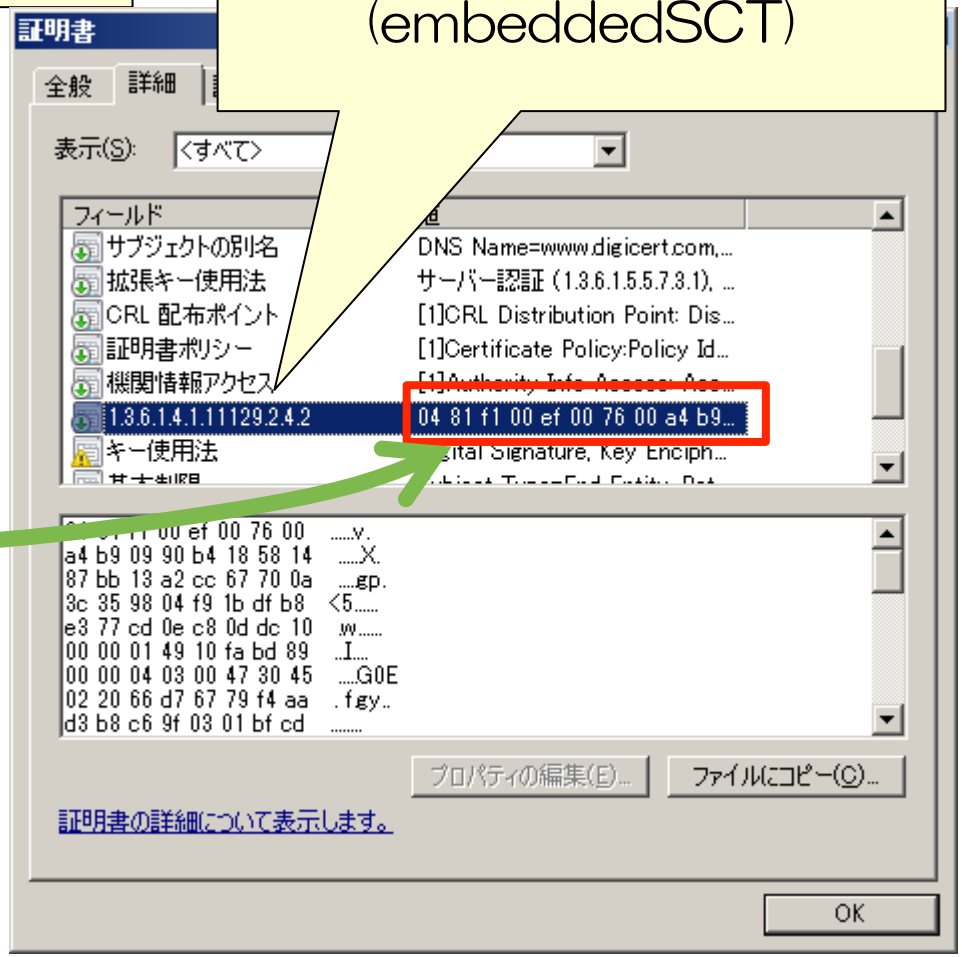
「公開監査が可能」
＝
Certificate Transparency
対応のサイト

CT対応のサイト(=GlobalSign or DigiCert)

Signed Certificate Timestamp (SCT)
(RFC 3161とは無関係の
CTログエントリに対する署名情報)

DigiCert、GlobalSignには
見慣れない拡張が！！
(embeddedSCT)

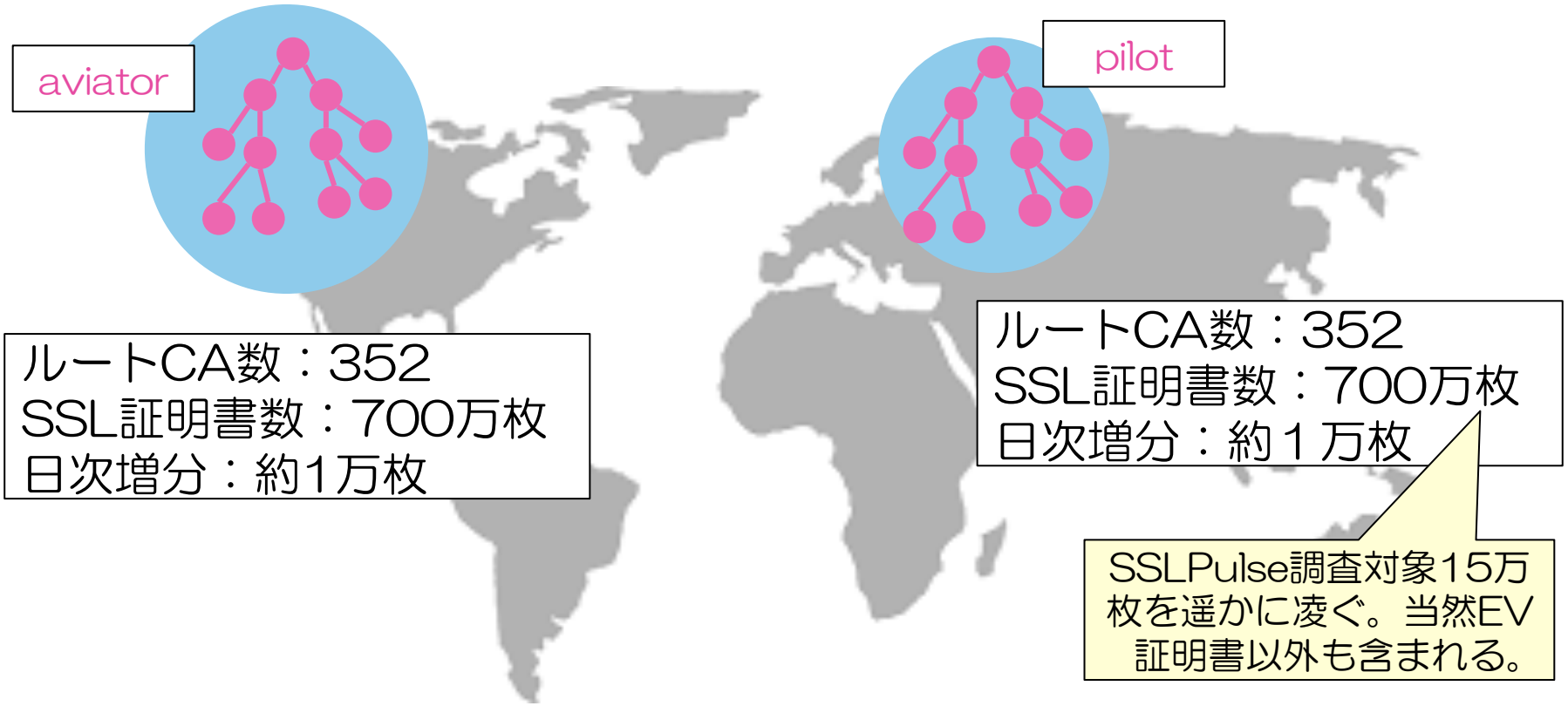




FUJI Xerox

Certificate Transparencyログサーバー(2015年4月2日時点)

Googleは世界2拠点でログサーバーをテスト運用している



Googleは3拠点を計画、他の組織がログサーバーを提供してもよい

FUJI Xerox

まとめ

まとめ

- SSL/TLS生誕20周年でその歴史を振返った
  - プロトコル、ライブラリ、ブラウザ、サーバー
- SSL/TLSの脆弱性の歴史
- SSL/TLSの脆弱性対策の整理
  - 4種類に分類できる、種類毎に対策方法も違う
    - 暗号期危殆化の問題
    - TLS/HTTPSプロトコル設計の問題
    - 個別の実装の問題(OpenSSL、Windows、Java(JSSE, JCE))
    - CA運用上の問題
- SSL/TLSの脆弱性対策技術の最新動向
  - HSTS, OCSP stapling, Certificate Transparency等の解説

20歳になり成人して、社会の荒波に揉まれているかのようです。
この1年、SSL/TLSやPKIに関して脆弱性が数多く出ている傾向にありますが、一つ一つ手当をして今後も使われていくでしょう。

PKI Day 2015の私の講演とパネルの補足情報ページは以下にあります。
http://www9.atwiki.jp/kurushima/pages/123.html
本講演後、リンク等補足情報を提供する予定です。参考になさってください。