Internet Week2019, D2-2, Asakusa-bashi, Tokyo, Japan

TLS1.3概要と現状
～移行に向けた情報提供～

セキュリティ本部セキュリティ情報統括室
須賀祐治
2019-11-27

自己紹介

- CRYPTREC 暗号技術活用委員会 委員
- CRYPTREC **TLS暗号設定ガイドライン**WG 主査
- 暗号プロトコル評価技術コンソーシアム 幹事
- Cryptoassets Governance TF SecWG member
- 電子情報通信学会 ISEC研究会 幹事補佐
- 情報処理学会 CSEC研究会 運営委員

（ちょい前だと）

- IPSJ 論文誌ジャーナル編集委員(NW)
- IWSEC2015 Program co-chair
- SSR2015 General co-chair
- CSS2017，CyberSciTech2019 Program co-chair
- ECC2018，IWSEC2019 実行委員

CRYPTREC

Cryptography Research and Evaluation Committees

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

- 電子政府推奨暗号の安全性を評価・監視し暗号技術の適切な実装法・運用法を調査・検討するプロジェクト
- 2013年にリスト改訂

電子政府における調達のために参照すべき暗号のリスト
（CRYPTREC暗号リスト）

平成25年3月1日
総務省
経済産業省

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

技術分類		名称
	署名	DSA
		ECDSA

今年度WG再設置して全面改正

SSL/TLS暗号設定ガイドライン

ガイドライン (2018年5月8日第2.0版公開)

- SSL/TLS暗号設定ガイドライン （全83ページ、5.02MB）
- SSL/TLS暗号設定ガイドライン チェックリスト（PDF形式 794KB）
- SSL/TLS暗号設定ガイドライン チェックリスト（Excel形式 1.49MB）

参考資料

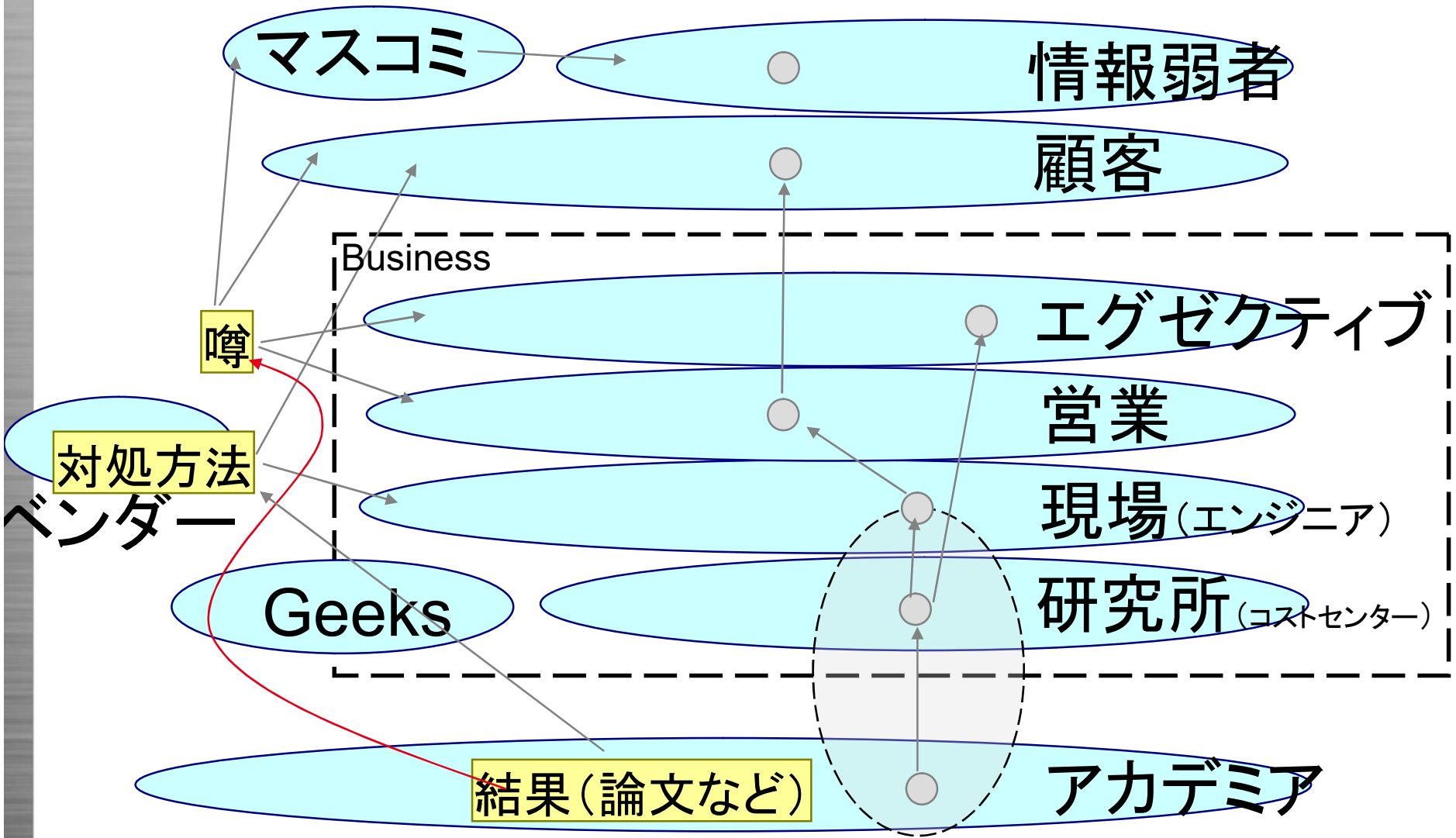
- SSL/TLS暗号設定 サーバ設定編（全15ページ、343KB）
- SSL/TLS暗号設定 暗号スイートの設定例（全7ページ、257KB）

一括ダウンロード

- SSL/TLS暗号設定ガイドライン・参考資料一式（ZIPファイル、7.58MB）

https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

「技術翻訳者」連携の必要性



2012年3月総合大会「セキュリティプロトコル仕様の脆弱性事例と世代交代困難性」

「技術翻訳者」の役割

- 正しい情報をわかりやすく「上」に伝える
  - 落としてよい情報と肝の情報
- 誤りがあればそれを正す
  - 噂が広まるのは早い
- どう解釈しているのか「横」に伝える

2012年3月総合大会「セキュリティプロトコル仕様の脆弱性事例と世代交代困難性」

須賀執筆のIIR記事（抜粋）

- Vol.43 (2019-09) ブロックチェーン技術を
  ベースとしたアイデンティティ管理・流通の動向
- Vol.39 (2018-06) ROCA(RSA実装問題)
- Vol.33 (2016-12) TLS1.3
- Vol.31 (2016-06) 耐量子暗号
- Vol.30 (2016-03) Let's Encrypt
- Vol.26 (2015-02) ID管理技術
- Vol.25 (2014-11) POODLE attack
- Vol.21 (2013-11) 仮想通貨 Bitcoin
- Vol.18 (2013-02)
  暗号技術を用いたプロトコル・実装に
  多発している問題の整理とあるべき姿

https://www.iij.ad.jp/dev/report/iir/

今回のプレゼン方針

- 昨日（11/25），2階ホールで聴講してみて
  あまりインタラクションが無い→悲しみをry)
- とりあえず40-50分話せる分量は準備
  - URL等メモしないと！という各種情報は
    事前資料にできるだけ埋め込んだつもり
  - 会場のいらっしゃる皆様の反応を伺いつつ
    話をやめたり脱線させるかもしれません
- 発表中でも都度ご質問お受けします
  - マイク経由でもなんでもよかです

事前資料 is NOT 事後資料

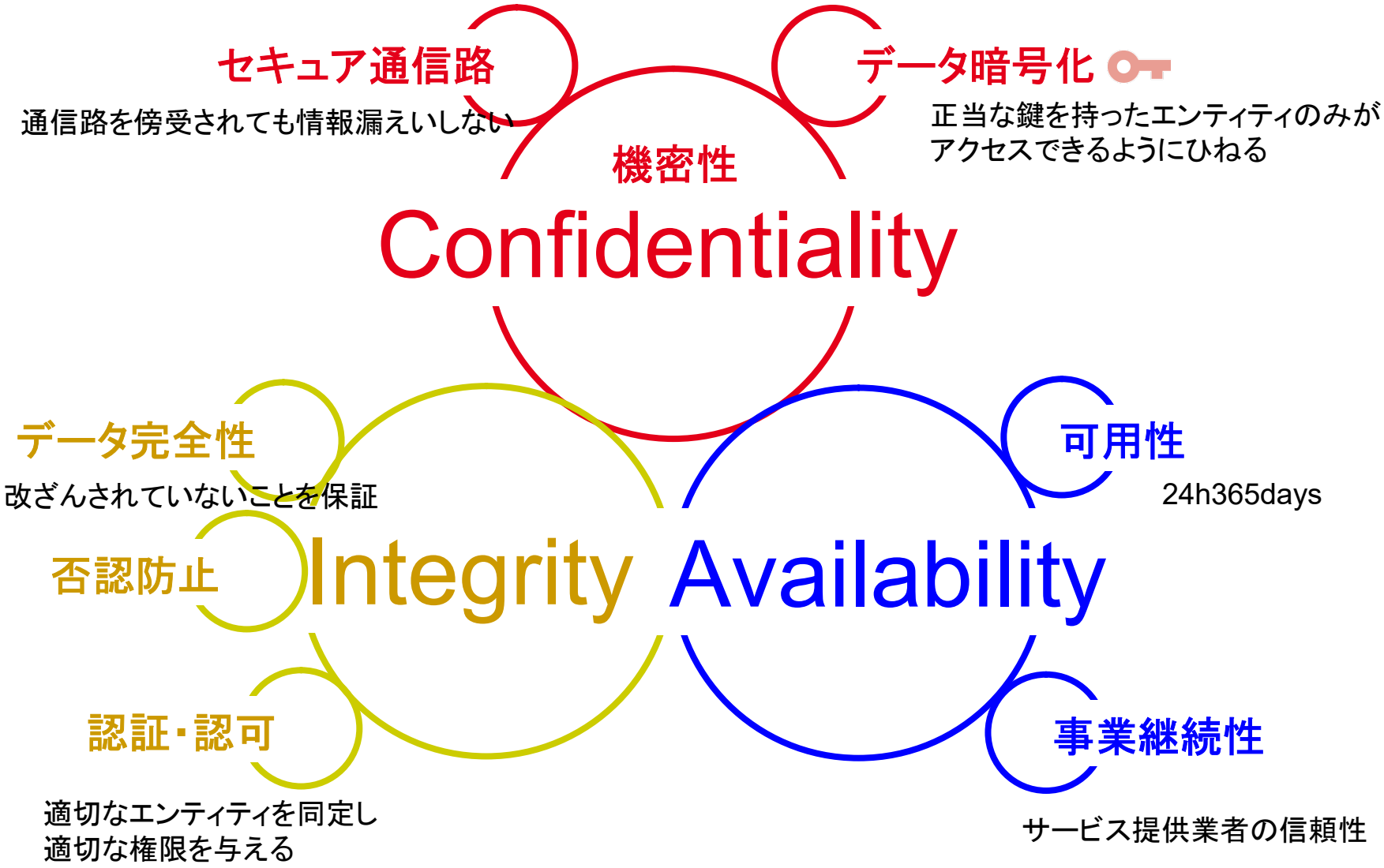
- 事前資料はご参加頂いた皆様への特典
  - クローズドな場と理解

- 事後資料はスパースにする予定
  （可能でしょうか？ > プログラム委員会）

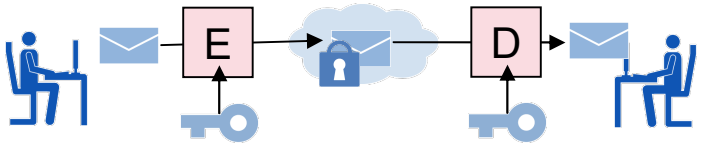
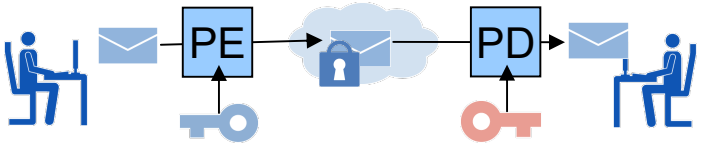
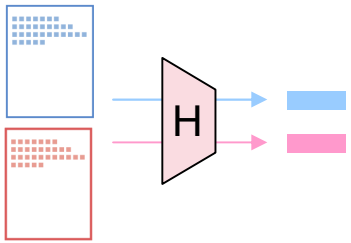
脱線1
念のため黒塗り

Introduction（そもそも論）

一般的なセキュリティ要件

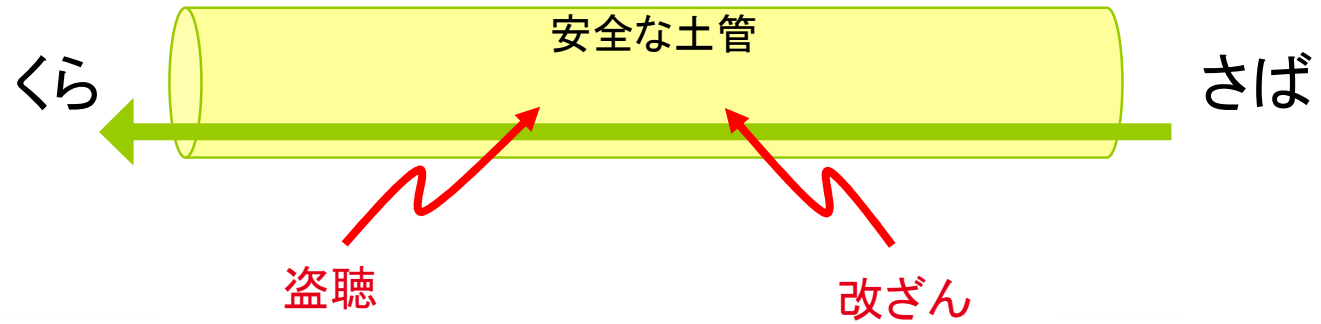


参考：暗号アルゴリズムの分類

暗号プリミティブ	特徴・用途	アルゴリズム例
共通鍵暗号	暗号化と復号で同じ鍵を用いて秘匿 	ブロック暗号 AES, DES, Camellia ストリーム暗号 RC4, MUGI
公開鍵暗号 Confidentiality	対になる2つの鍵を用いて 守秘(暗号化)，署名，鍵共有 	素因数分解 RSA 離散対数 DSA，DH 楕円離散対数 ECDSA, ECDH
Integrity		
ハッシュ関数	衝突しない固定長データに圧縮  (デジタル署名 タイムスタンプ 等で利用)	専用(dedicated) 関数 MD5, SHA-1/SHA-256 ブロック暗号ベース ISO 10118-2

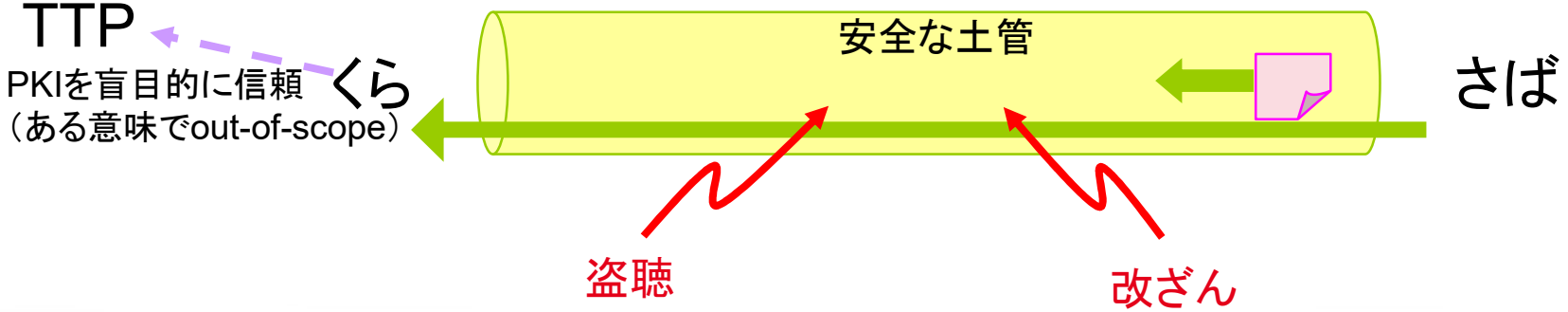
SSL/TLSでやりたかったこと(基本機能)

- 盗聴防止(機密性保持) confidentiality
  - フラグメント暗号化
- 改ざん防止(データ完全性保持) data integrity
  - デジタル署名やMAC付与
- サーバ認証(+optional:クライアント認証) authentication
  - PKI(X.509証明書検証)と連動



SSL/TLSでやりたかったこと(基本機能)

- 盗聴防止(機密性保持) confidentiality
  - フラグメント暗号化
- 改ざん防止(データ完全性保持) data integrity
  - デジタル署名やMAC付与
- サーバ認証(+optional:クライアント認証) authentication
  - PKI(X.509証明書検証)と連動



脱線２

念のため黒塗り

脱線2
念のため黒塗り

土管は土管でしかない（ここに入力できますか？）

- 「安全な土管を」通して流したものが
  どう扱われるかはサーバ次第

念のため黒塗り

脱線2
念のため黒塗り

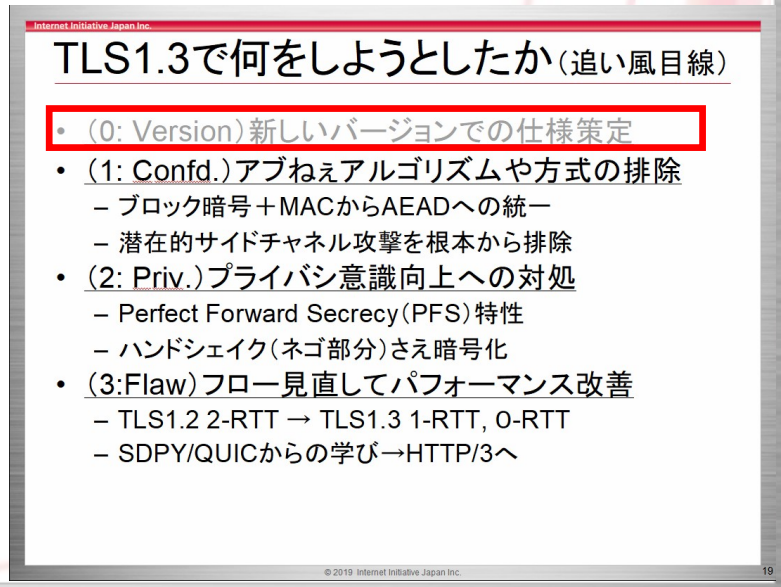
TLS1.3で何をしようとしたか（追い風目線）

- （0: Version）新しいバージョンでの仕様策定
- （1: Alg.）アブねぇアルゴリズムや方式の排除
  - ブロック暗号＋MACからAEADへの統一
  - 潜在的サイドチャネル攻撃を根本から排除
- （2: Priv.）プライバシ意識向上への対処
  - Perfect Forward Secrecy（PFS）特性
  - ハンドシェイク（ネゴ部分）さえ暗号化
- （3:Flaw）フロー見直してパフォーマンス改善
  - TLS1.2 2-RTT → TLS1.3 1-RTT, 0-RTT
  - SDPY/QUICからの学び→HTTP/3へ

- これらを通して「外的要因の整理」をしましょう

0. Version

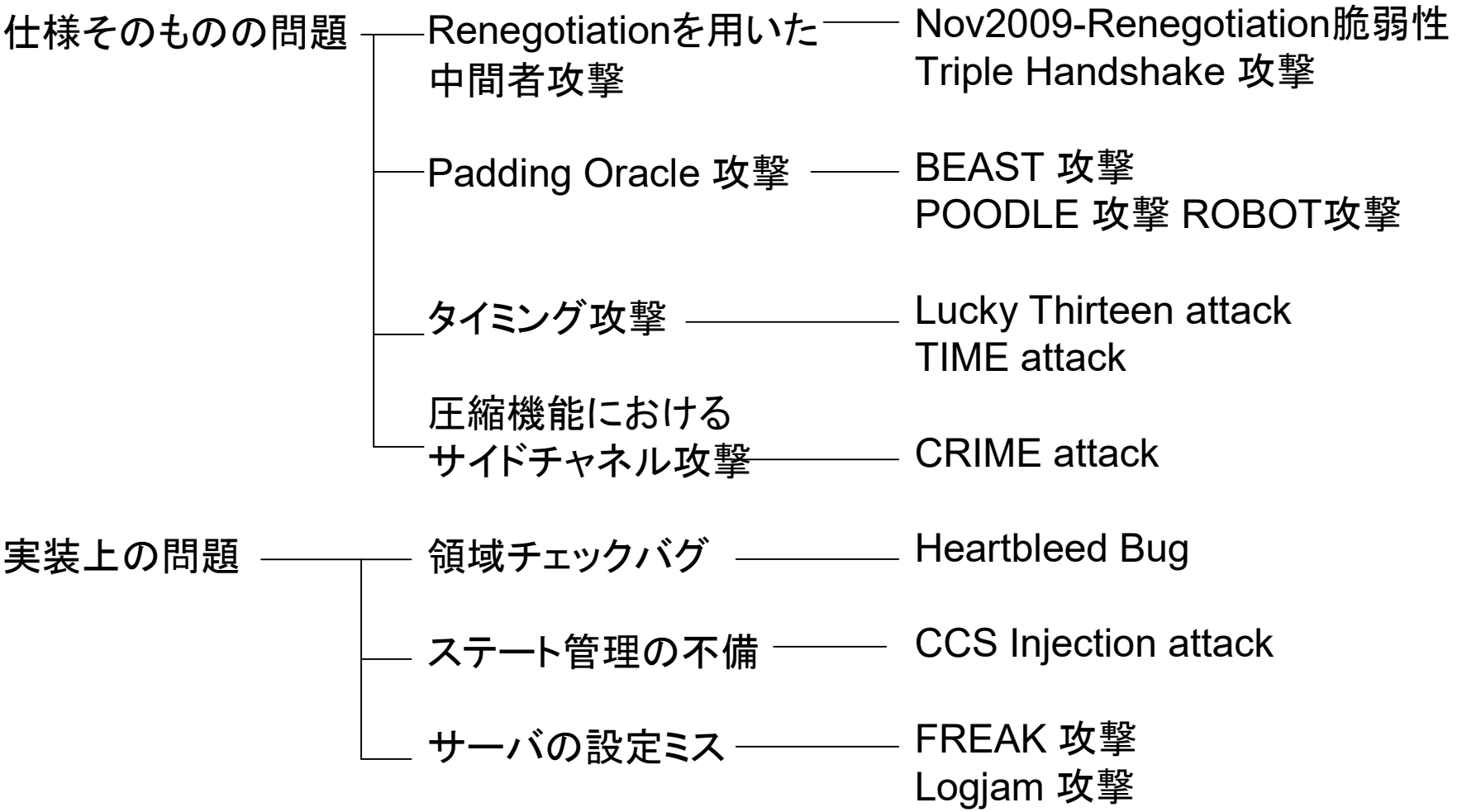
TLS1.3における再設計（TLS1.2までの変遷）



SSL/TLSの経緯

- Netscape Communicationsから1995年にInternet draft が公開された時期と同じくして当時のブラウザNetscape NavigatorにSSL2.0が実装
- 2014年10月に発表されたPOODLE攻撃はSSL3.0における根本的な問題を露呈
- SSLの後継でありIETFで策定されたTLSは1.0/1.1/1.2が1999/2006/2008年にそれぞれRFCとして公開
- 2014年4月からTLS1.3ドラフト策定開始．28版の改訂後，2018年8月ついにTLS1.3がRFCとして公開

SSL/TLSに対する攻撃の分類



SSL/TLSバージョンごとの状況

プロトコル	バージョン	ステータス	ワークアラウンド	根拠
SSL	2.0	脆弱	なし	RFC6167
	3.0	脆弱	なし	RFC7568
				POODLE攻撃

IETFがSSL2.0/3.0を無効化

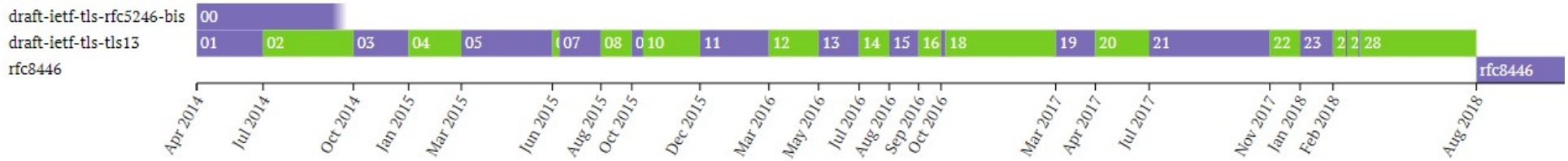
（トップダウン的な措置）

- 2011年3月
  - RFC 6176：Prohibiting Secure Sockets Layer（SSL）Version 2.0
- 2015年6月
  - RFC 7568：Deprecating Secure Sockets Layer Version 3.0
  - http://disablessl3.com/ by Michele Spagnuolo

SSL/TLSバージョンごとの状況

プロトコル	バージョン	ステータス	ワークアラウンド	根拠
SSL	2.0	脆弱	なし	RFC6167
	3.0	脆弱	なし	RFC7568
				POODLE攻撃
TLS	1.0	問題はあるが回避策あり （ただし回避策がないものもある）	Renegotiation機能を利用しない	RFC5746
			圧縮機能を利用しない	CRIME攻撃
			1/n-1分割法	BEAST攻撃
			リスク受容	Lucky13攻撃
	1.1	問題はあるが回避策あり （ただし回避策がないものもある）	圧縮機能を利用しない	CRIME攻撃
			リスク受容	Lucky13攻撃
	1.2	問題はあるが回避策あり	圧縮機能を利用しない	CRIME攻撃
			暗号モードとしてGCM, CCMのみを利用	Lucky13攻撃
	1.3	安全に設計したと信じられている		

2018年8月 TLS1.3 RFC発行



- ドラフト更新の経緯を参照可能
  - https://tools.ietf.org/html/draft-ietf-tls-tls13
- IETFとは異なるリポジトリで頻繁に更新
  - https://tlswg.github.io/tls13-spec/

参考：フォーマルメソッドで設計中のプロトコルの穴を見つける

- 米山一樹，セキュリティプロトコル安全性検証の理想と現実，CRYPTRECシンポジウム2016
  - https://www.cryptrec.go.jp/symposium/20160627_invited1.pdf
- レピダムBlog, 祝RFC！Transport Layer Security (TLS) 1.3 発行の軌跡 ～熟成された4年間の安全性解析～
  - https://lepidum.co.jp/blog/2018-10-01/tls1_3security/

2018年9月 TLS1.0/1.1排除の初動

- SSL3.0などと同様の die-die-die ドラフト発行
  - https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate
  - “Deprecating TLSv1.0 and TLSv1.1”
  - 移行状況に関する数値的根拠も紹介されている（-00 draft：Webサーバの対応状況は以下の通り）

Name/Ref	Date	SSLv3	TLSv1.0	TLSv1.1	TLSv1.2	TLSv1.3
! Alexa [1]	20180226	-	2.0	<0.1	97.9	-
Cloudflare [2]	20180518	0.0	9.3	0.2	84.9	5.5
Firefox [3]	20180709	-	1.0	-	94.0	5.0
Chrome [4]	20180711	-	0.4	<0.1	-	-

バージョン移行動向（2019-06）

https://www.ssllabs.com/ssl-pulse/

- 毎月レポートが発出
  - プロトコル種別などの先月との差分表示

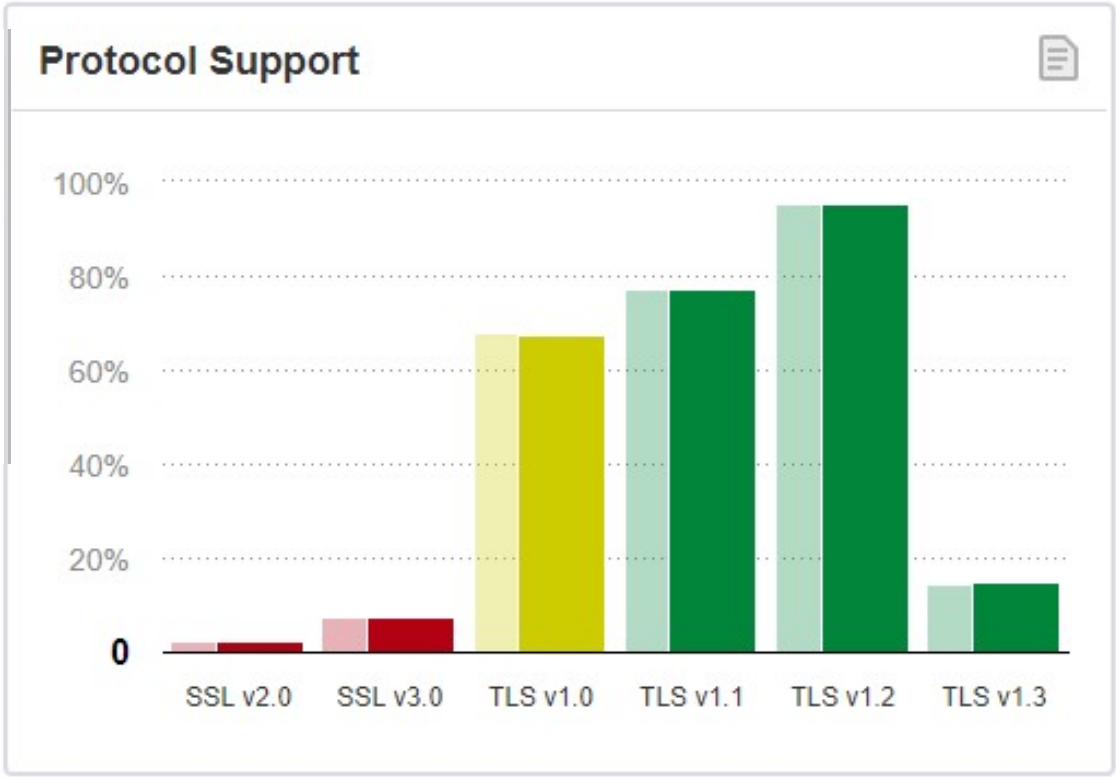
June 2019

14.8 % of sites surveyed support the **TLS v1.3** protocol

20,661 sites + 0.6 %

May 2019

14.2 % (19,821 sites)

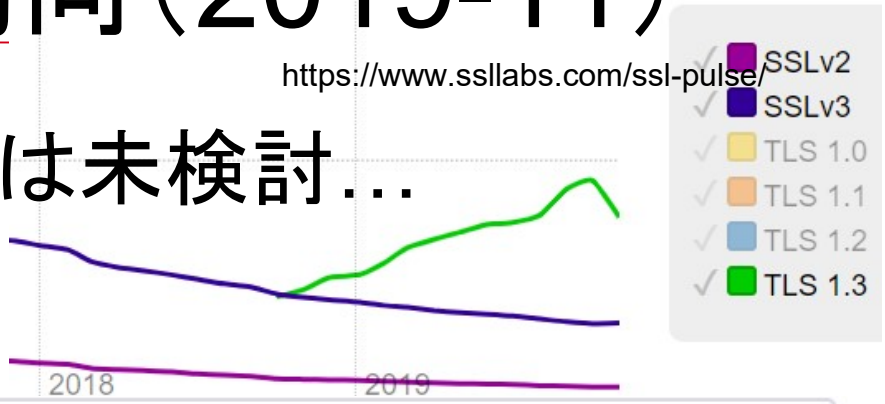


参考：K. Urushimaさん http://blog.livedoor.jp/k_urushima/archives/1786599.html

バージョン移行動向（2019-11）

https://www.ssllabs.com/ssl-pulse/

- 対応率が下がった要因は未検討…



June 2019

14.8 % of sites surveyed support the **TLS v1.3** protocol

20,661 sites + 0.6 %

May 2019

14.2 % (19,821 sites)

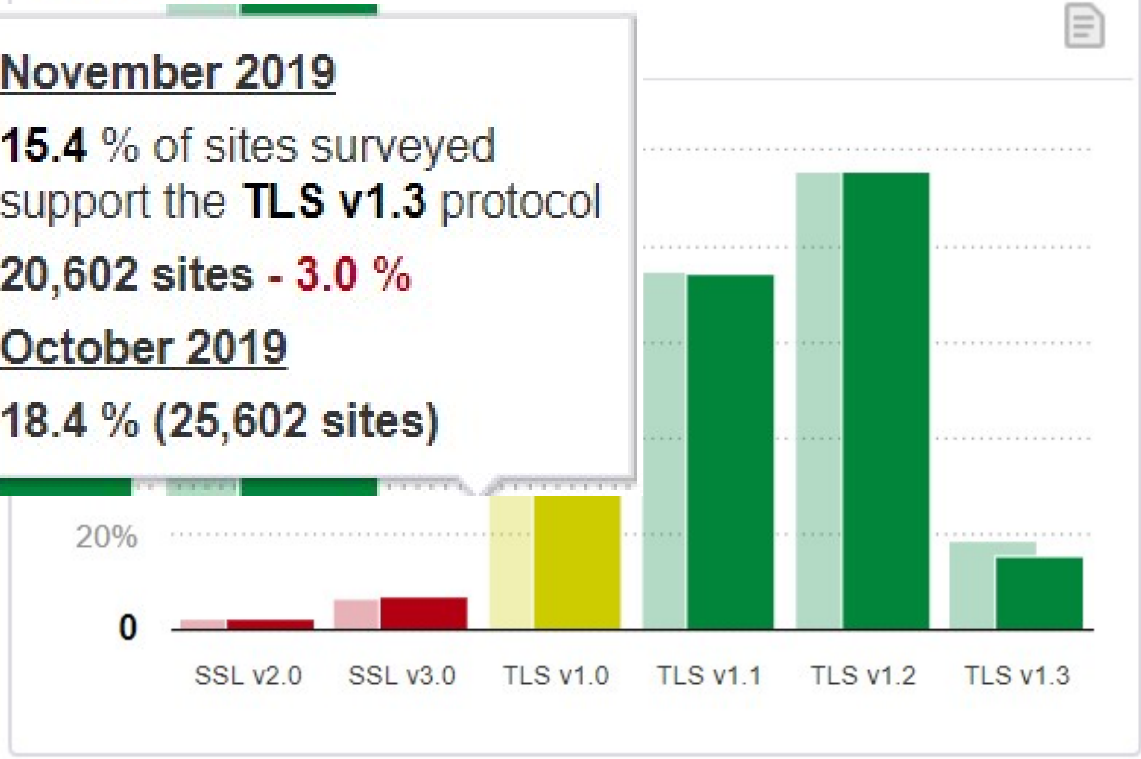
November 2019

15.4 % of sites surveyed support the **TLS v1.3** protocol

20,602 sites - 3.0 %

October 2019

18.4 % (25,602 sites)



参考：K. Urushimaさん http://blog.livedoor.jp/k_urushima/archives/1786599.html

定点観測55地点

version	2016-10	2017-04	2019-01	2019-06
SSL2.0	0	0	0	0
SSL3.0	8	3	2	2
TLS1.0	55	55	55	55
TLS1.1	18	23	23	39
TLS1.2	36	37	53	53
TLS1.3	-	-	0	0

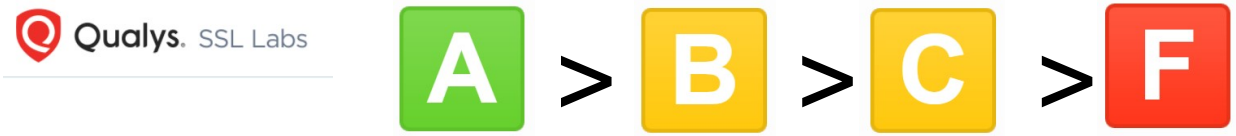
表 1: SSL/TLS バージョン対応状況

- SSL3.0/TLS1.0のみ対応というサイトも存在
  - おそらく機会損失を恐れてか？
- ROBOT攻撃に脆弱という判定：2サイト（Fラン）

Qualys SSLTEST の利用

- （以前は独自にクロールしてたんだけど
  怒られたので調査中止．世知辛い世の中 orz）

- Qualys サイトでのチェック
  - https://www.ssllabs.com/ssltest/
  - **TLSサーバ設定**を独自の方針に基づきランク付け



  - SSL3.0 利用でC ランク，DES等の56 ビット暗号利用でF ランクのように決められている．
  - しかもちょくちょく更新される（独自目線）

ランク一覧とBランク下落に関して

rank	2019-01	2019-06
A	3	4
B	48	47
C	2	2
D	0	0
F	2	2

表 2: ランクの変化状況

reason	2019-01	2019-06
noFS	44	41
noAEAD	35	33
weakDH	8	9

表 3: B ランク下落要因の変化

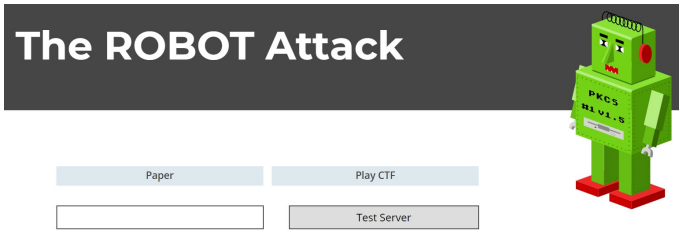
- noFS :Forward Secrecy 対応のアルゴリズムに未対応
- noAEAD:TLS1.3 で義務化されたAEAD 暗号の未サポート
- weakDH:鍵長の短いDiffie-Hellman 方式の利用

あくまで私見ですが…

- F ランク2 サイトはBleichenbacher 攻撃の亜種であるROBOT 攻撃に脆弱であると判断
  - ROBOT 攻撃はBEAST やPOODLE と同様に何度もトライ＆エラーを繰り返しリクエストを送ることで，過去の暗号メッセージを復元するという類の攻撃
- ROBOT 攻撃のリスクを許容するかどうかは意見が分かれるところではあるが…
- 通常のユーザがランクを確認できることからこのようなランクが表示されることはミスリーディングを起こしやすいため，速やかな対策が必要

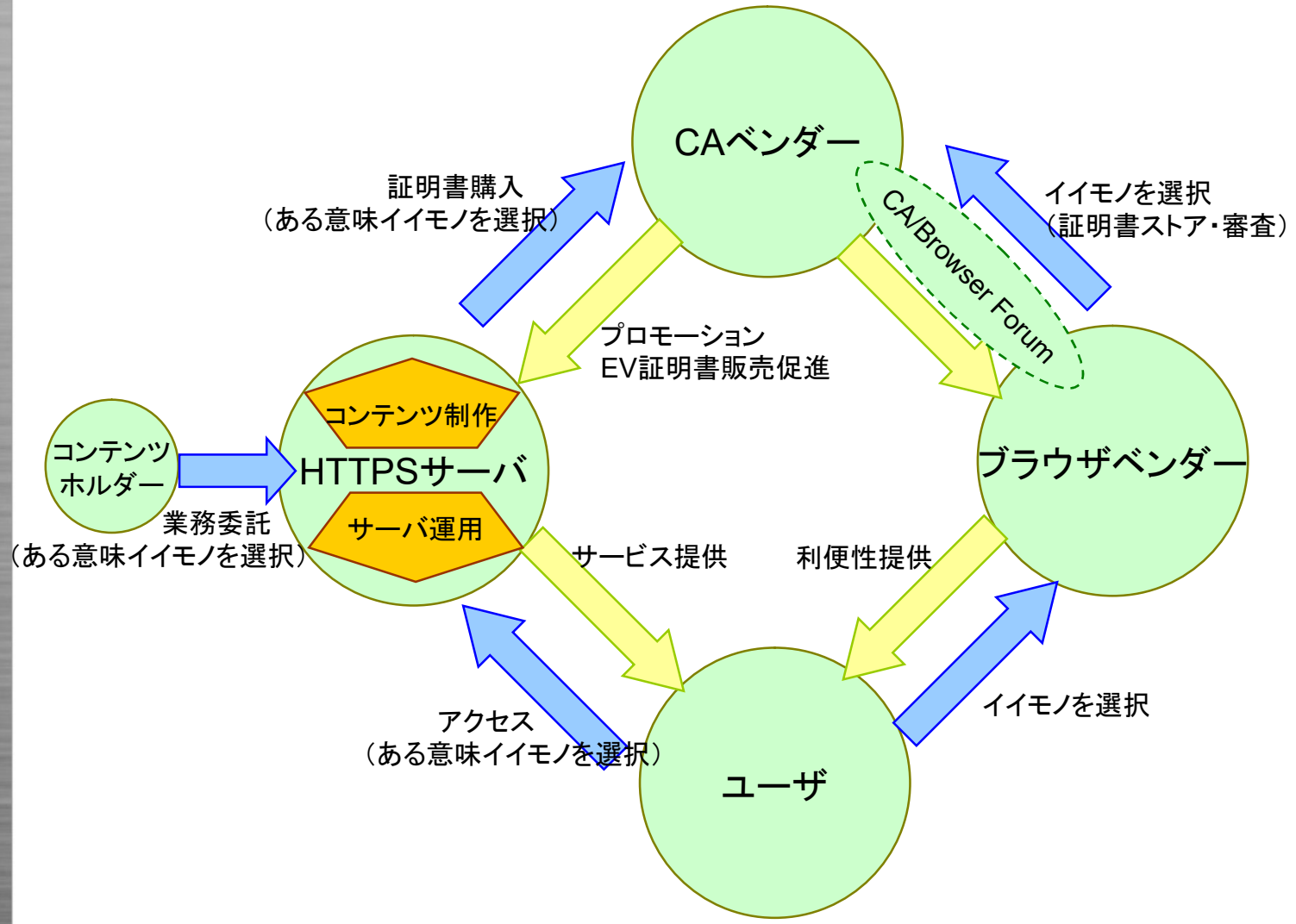
「評価軸」を知っておこう

- ブラウザの判断を信じるか
  - 誤検知事例



- 世の中のサーバテストサイトを信じるか
  - ROBOT攻撃のリスクを受容するか？
    - 技術の正しい理解＝継続的なウォッチと勉強が必要
  - もう少し前だとRC4リスク受容するか？
    - IETFでRC4排除RFCがある中で怒られた
      - Asiacrypt2014 Rump session
      - https://asiacrypt.2014.rump.cr.yp.to

ステークホルダーの関係



2018年10月 TLS1.0/1.1排除の本格化

- 主要ブラウザベンダーが<u>同時に</u>
  2020年前半に無効化するアナウンス
  - Chrome, Edge/IE, Firefox, Safari

2020 年 IE, Edge で TLS 1.0, 1.1 での接続無効化。確認を！

Rate this article ★★★★★

YURIKAM 2018/10/16

Share 139 | 0 | in 0

こんにちは、垣内ゆりかです。

マイクロソフトでは、Transport Layer Security (TLS) 1.0, 1.1 の利用を廃止し、より安全なプロトコルである TLS 1.2 以降への移行を推奨しています。(参考: 過去ブログ [IT 管理者向け] TLS 1.2 への移行を推奨しています)

2020 年 前半、Internet Explorer 11, Microsoft Edge にて、 TLS 1.0 および TLS 1.1 を既定で無効化する措置を行う予定です。

https://blogs.technet.microsoft.com/jpsecurity/2018/10/16/tlsdeprecation/

NISTトライアル（2018年）
“By 2020-01-01”

SP 800-52 Rev. 2(Draft)

⚠ Obsoleted on October 15, 2018 by SP 800-52 Rev. 2 (Draft).

Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

Date Published: November 2017
Comments Due: February 1, 2018 (public comment period is CLOSED)
Email Questions to: sp80052-comments@nist.gov

Author(s)
Kerry McKay (NIST), David Cooper (NIST)

Announcement

NIST announces the release of draft Special Publication 500-52 Revision 2, ***Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations***. Transport Layer Security (TLS) provides mechanisms to protect data during electronic dissemination across the Internet. This Special Publication provides guidance to the selection and configuration of TLS protocol implementations while making effective use of Federal Information Processing Standards (FIPS) and NIST-recommended cryptographic algorithms. It requires that TLS 1.2 configured with FIPS-based cipher suites be supported by all government TLS servers and clients and recommends that agencies develop migration plans to support TLS 1.3 by January 1, 2020. This Special Publication also provides guidance on certificates and TLS extensions that impact security.

DOCUMENTATION

Publication:
Draft SP 800-52 Rev. 2

Supplemental Material:
Comments received (pdf)

Document History:
11/15/17: SP 800-52 Rev. 2 (Draft)
10/15/18: SP 800-52 Rev. 2 (Draft)
08/29/19: SP 800-52 Rev. 2 (Final)

TOPICS

Security and Privacy
cryptography; general security & privacy; public key

https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/archive/2017-11-15

結局“By 2024-01-01”

Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations: NIST SP 800-52 Rev. 2

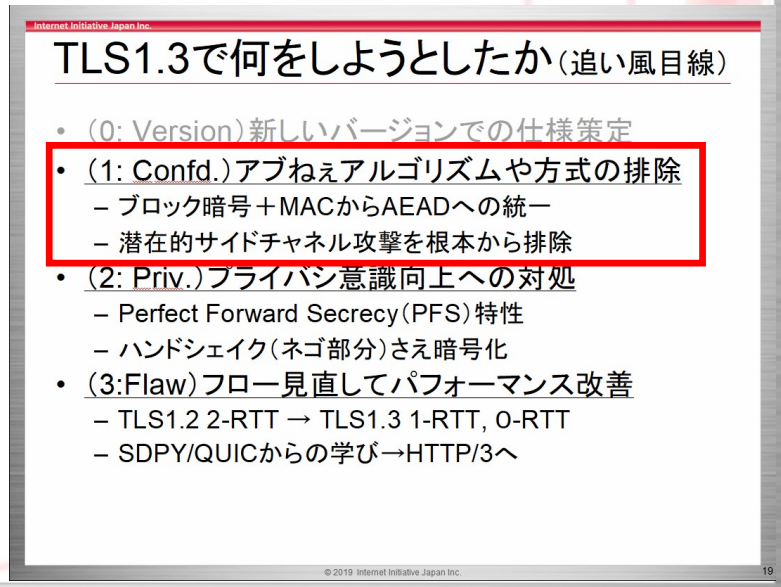
August 29, 2019

NIST announces the publication of **NIST Special Publication (SP) 800-52 Revision 2**, ***Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations***, which provides guidance for selecting and configuring TLS protocol implementations while making effective use of Federal Information Processing Standards (FIPS) and NIST-recommended cryptographic algorithms. It requires that all government TLS servers and clients support TLS 1.2 configured with FIPS-based cipher suites and recommends that agencies develop migration plans to support TLS 1.3 by January 1, 2024. This Special Publication also provides guidance on certificates and TLS extensions that impact security.

https://csrc.nist.gov/News/2019/nist-publishes-sp-800-52-revision-2

1: Confd.

TLS1.3 における再設計
（危ないアルゴリズムの排除）



懐かしいね　2011年は Padding Oracle Attackの当たり年

- 9月：BEAST攻撃（CVE-2011-3389）
  - SSL 3.0/TLS 1.0 を使用しているブラウザの CBC モードに対して選択平文攻撃を行うことでブラウザ内の Cookie を入手するツールを公開
  - ブロックごとではなく**バイトごとの全数検索**だとうまくいく例を示し，実際にPayPalからのセキュアなCookieを奪取してログイン権限を不正に得るというデモを公開
- 10月：XML暗号化仕様
  - Webサービスの実装物をplaintext validity oracle として利用
  - XML Parser のエラーの意味を解釈しながらトライ＆エラー
- 12月：TLS1.2における Truncated HMAC利用時の問題
  - RFC6066で規定された拡張機能のひとつであるTruncated HMACを用いたTLS1.2通信における脆弱性が公開
  - 通常のHMACではなく、80ビットに切り詰めたデータをMAC(データの完全性を保証する認証子)として利用する拡張方式の原理的な問題

CRIME攻撃（2012年9月）

- SSL/TLSで**Compression(圧縮)機能**を有効にしているケースでCookie を搾取するデモが公開
- 例え同じ長さのデータを圧縮したとしても，圧縮前に同じ文字を含むかどうかで辞書の長さが変わるという事実を用いてトライ＆エラーで暗号化データを復元する

Lucky13攻撃（2013年2月）

- SSL/TLSへのタイミング攻撃．演算速度の違いから情報を搾取するサイドチャネル攻撃の１種をネットを介して行う手法
- CBCモードを使わない，もしくはMACとしてHMAC-SHA1などではなく**AEAD**(暗号化と認証子付与を同時に行う方式)を用いる．例えば GCMモードやCCMモードなど．

2013年の問い「CBCを捨てますか？」

- 単純な対策方法：CBCを使わない
  - Lucky13（2月5日）の風潮：RC4使おう！
    - Lucky Thirteen: Breaking the TLS and DTLS Record Protocols
    - http://www.isg.rhul.ac.uk/tls/Lucky13.html
- しかしRC4も死亡（3月13日）
    - Breaking the TLS and DTLS Record Protocols
    - http://www.isg.rhul.ac.uk/tls
- AEADの普及率が課題…

代替手段があるかどうか？＋相互接続性を確保できるか？

2013年3月 第3回神保町暗号ワークショップ「CBCモードの現在（いま）～CBCモードに何が起こっているか？」

USENIX SEC 2019で再来

https://www.usenix.org/conference/usenixsecurity19/presentation-21

Scalable Scanning and Automatic Classification of TLS Padding Oracle Vulnerabilities

Authors:
Robert Merget and Juraj Somorovsky, *Ruhr University Bochum;* Nimrod Aviram, *Tel Aviv University;* Craig Young, *Tripwire VERT;* Janis Fliegenschmidt and Jörg Schwenk, *Ruhr University Bochum;* Yuval Shavitt, *Tel Aviv University*

Abstract:
This paper is under embargo and will be released to the public on the first day of the symposium, August 14, 2019.

The TLS protocol provides encryption, data integrity, and authentication on the modern Internet. Despite the protocol's importance, currently-deployed TLS versions use obsolete cryptographic algorithms which have been broken using various attacks. One prominent class of such attacks is CBC padding oracle attacks. These attacks allow an adversary to decrypt TLS traffic by observing different server behaviors which depend on the validity of CBC padding.

We present the first large-scale scan for CBC padding oracle vulnerabilities in TLS implementations on the modern Internet. Our scan revealed vulnerabilities in 1.83% of the Alexa Top Million websites, detecting nearly 100 different vulnerabilities. Our scanner observes subtle differences in server behavior, such as responding with different TLS alerts, or with different TCP header flags.

TLS Padding Oracles

The TLS protocol provides encryption, data integrity, and authentication on the modern Internet. Despite the protocol's importance, currently-deployed TLS versions use obsolete cryptographic algorithms which have been broken using various attacks. One prominent class of such attacks is CBC padding oracle attacks. These attacks allow an adversary to decrypt TLS traffic by observing different server behaviors which depend on the validity of CBC padding.

We evaluated the Alexa Top Million Websites for CBC padding oracle vulnerabilities in TLS implementations and revealed vulnerabilities in 1.83% of them, detecting nearly 100 different vulnerabilities. These padding oracles stem from subtle differences in server behavior, such as responding with different TLS alerts, or with different TCP header flags. We suspect the subtlety of different server responses is the reason these padding oracles were not detected previously.

The currently identified and fixed vulnerabilities are:

- OpenSSL. CVE-2019-1559. OpenSSL Security Advisory: 0-byte record padding oracle
- Citrix. CVE-2019-6485. TLS Padding Oracle Vulnerability in Citrix Application Delivery Controller (ADC) and NetScaler Gateway.
- F5. CVE-2019-6593. TMM TLS virtual server vulnerability CVE-2019-6593.
- SonicWall SonicOs. CVE-2019-7477. SonicOS & SonicOSv CBC Cipher TLS Padding Vulnerability.

The disclosure process is still running with a handful of vendors. Some of them consider to disable or even completely remove CBC cipher suites from their products.

https://github.com/RUB-NDS/TLS-Padding-Oracles

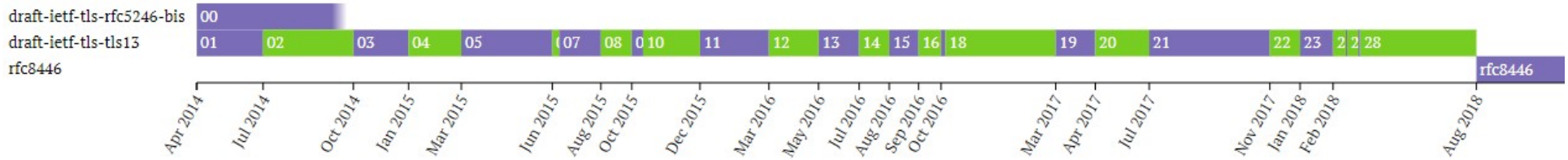
これあれやん（CVE-2019-1559）

- OpenSSL Security Advisory [26 February 2019]
  0-byte record padding oracle (CVE-2019-1559)
  ==========
- Severity: Moderate
- If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data.
- In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway).

AEAD ciphersuites are not impacted.

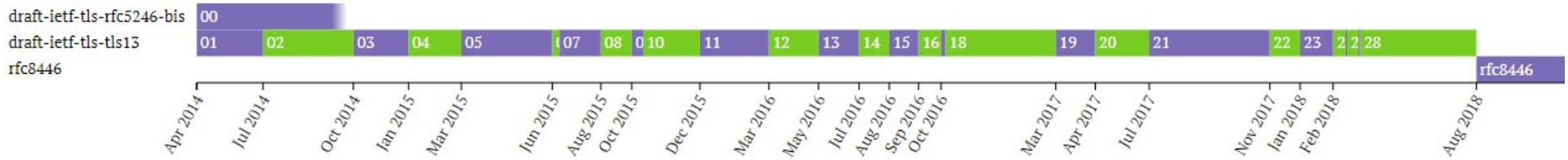
https://www.openssl.org/news/secadv/20190226.txt

Rev重ねるごとに落選していく

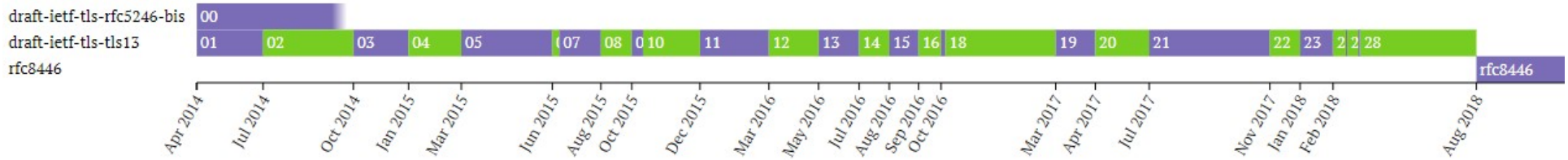


- draft-02
  - Remove custom DHE groups.
  - Remove support for compression.
  - Remove support for static RSA and DH key exchange.
  - Remove support for non-AEAD ciphers.
- draft-03
  - Remove the unnecessary length field from the AD input to AEAD ciphers.
- draft-06
  - Prohibit RC4 negotiation for backwards compatibility.

https://tlswg.org/tls13-spec/draft-ietf-tls-tls13.html



- draft-07
  - Integration of semi-ephemeral DH proposal.
  - Remove resumption and replace with PSK + tickets.
  - Move to HKDF.
- draft-08
  - Remove support for weak and lesser used named curves.
  - Remove support for MD5 and SHA-224 hashes with signatures.



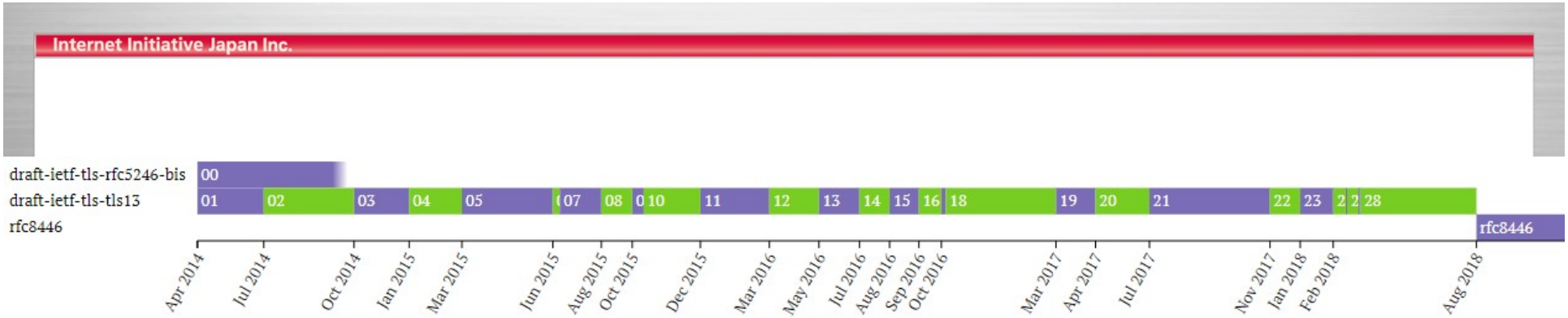
- draft-09
  - Change to RSA-PSS signatures for handshake messages.
  - Remove support for DSA.
  - Deprecate SHA-1 with signatures.
- draft-11
  - Port the CFRG curves & signatures work from RFC4492bis.

2016年1月の時点の様子

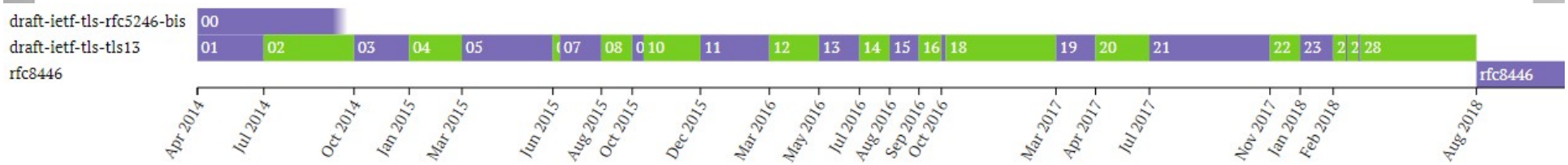
- https://tlswg.github.io/tls13-spec/#rfc.appendix.A.4

Cipher Suite Name	Value	Specification
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	{0x00,0x9E}	[RFC5288]
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	{0x00,0x9F}	[RFC5288]
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	{0xC0,0x2B}	[RFC5289]
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	{0xC0,0x2C}	[RFC5289]
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	{0xC0,0x2F}	[RFC5289]
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	{0xC0,0x30}	[RFC5289]
TLS_DHE_RSA_WITH_AES_128_CCM	{0xC0,0x9E}	[RFC6655]
TLS_DHE_RSA_WITH_AES_256_CCM	{0xC0,0x9F}	[RFC6655]
TLS_DHE_RSA_WITH_AES_128_CCM_8	{0xC0,0xA2}	[RFC6655]
TLS_DHE_RSA_WITH_AES_256_CCM_8	{0xC0,0xA3}	[RFC6655]
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	{TBD,TBD}	[I-D.ietf-tls-chacha20-poly1305]
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	{TBD,TBD}	[I-D.ietf-tls-chacha20-poly1305]
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	{TBD,TBD}	[I-D.ietf-tls-chacha20-poly1305]

TLS_（鍵共有）_（署名）_（AEADのアルゴリズム）_（ハッシュ関数）



- draft-13
  - Require DH public keys and secrets to be zero-padded to the size of the group.
- draft-14
  - Define ecdsa_sha1 (*).
- draft-15
  - Remove old PRNG text.



- draft-16
  - Change RSASSA-PSS and EdDSA SignatureScheme codepoints for better backwards compatibility (*)
- draft-23
  - Add some text on the security of static RSA.

共通鍵暗号

- DESはTLS1.2で既に排除済み
- RC4についてもRFC7465が2015年2月に発行されたことを受けて排除済み

- CBC暗号モード排除．共通鍵暗号としてはAEAD（Authenticated Encryption with Associated Data）のみの利用に統一
  - ChaCha20-Poly1305がAES-GCMと並んで実装必須（Mandatory Algorithms）

ハッシュ関数

- MD5, SHA-224 を排除（MUST NOT）
- SHA-1 は SHOULD NOT
  - 後方互換性のためのSHA-1サポート
    - 特にSHA-1署名での証明書検証はサポート

CipherSuitesの簡略化

- 5つのCipherSuitesのみを規定
  - （これまでのCipherSuitesと同じ呼び方でいいのか？）
- これまでの反省のもと「記載」をかなり簡略化

Description	Value	
TLS_AES_128_GCM_SHA256	{0x13,0x01}	**MUST**
TLS_AES_256_GCM_SHA384	{0x13,0x02}	**SHOULD**
TLS_CHACHA20_POLY1305_SHA256	{0x13,0x03}	**SHOULD**
TLS_AES_128_CCM_SHA256	{0x13,0x04}	
TLS_AES_128_CCM_8_SHA256	{0x13,0x05}	

TLS_（**AEADのアルゴリズム**）_（**ハッシュ関数**）

IANAで規定の各種パラメータ

Transport Layer Security (TLS) Parameters

Created
2005-08-23
Last Updated
2019-04-22
Available Formats

Registries included below

- TLS ClientCertificateType Identifiers
- TLS Cipher Suites
- TLS ContentType
- TLS Alerts
- TLS HandshakeType
- TLS Supported Groups
- TLS EC Point Formats
- TLS EC Curve Types
- TLS Supplemental Data Formats (SupplementalDataType)
- TLS UserMappingType Values
- TLS SignatureAlgorithm
- TLS HashAlgorithm
- TLS Exporter Labels
- TLS Authorization Data Formats
- TLS Heartbeat Message Types
- TLS Heartbeat Modes
- TLS SignatureScheme
- TLS PskKeyExchangeMode

https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

CCM_8_SHA256 推奨の変化

Value	Description	DTLS-OK	Recommended	Reference
0x13,0x01	TLS_AES_128_GCM_SHA256	Y	Y	[RFC8446]
0x13,0x02	TLS_AES_256_GCM_SHA384	Y	Y	[RFC8446]
0x13,0x03	TLS_CHACHA20_POLY1305_SHA256	Y	Y	[RFC8446]
0x13,0x04	TLS_AES_128_CCM_SHA256	Y	Y	[RFC8446]
0x13,0x05	TLS_AES_128_CCM_8_SHA256	Y	N	[RFC8446][IES

6.3 TLS registry updates (Benjamin Kaduk)

The management issue was discussed. The IESG agreed to use IESG Action to effect a "Y"->"N" change in the value of the "Recommended" column for the following TLS registry entries:

- o TLS_AES_128_CCM_8_SHA256 in the TLS Cipher Suites registry
- o truncated_hmac in the TLS ExtensionType Values registry

Internet Engineering Steering Group
Area Director of Security Area

https://www6.ietf.org/iesg/minutes/2018/minutes-2018-08-16.txt

署名・鍵交換

- DSA排除（ただし現時点で脆弱ではない）して
  ECDSA利用に完全シフト
- もちろん署名としてはECDSAだけではなく
  RSA-PSSも利用可能

- 一方で鍵交換に使われるDHは排除されることなく
  ECDHと共に残留
- 毎回異なる鍵（Ephemeral keys）を生成する
  Forward secrecy を満たす方式のみ

1軍（電子政府推奨暗号リスト）

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH

- いずれもリストに掲載されており安全であると認識されている
- レガシーな暗号であるという論理だけで移行が進められているという問題がある（私見）
  - 傷もついていないのに…

B.3.1.3. Signature Algorithm Extension

```
enum {
    /* RSASSA-PKCS1-v1_5 algorithms */
    rsa_pkcs1_sha256(0x0401),
    rsa_pkcs1_sha384(0x0501),
    rsa_pkcs1_sha512(0x0601),

    /* ECDSA algorithms */
    ecdsa_secp256r1_sha256(0x0403),
    ecdsa_secp384r1_sha384(0x0503),
    ecdsa_secp521r1_sha512(0x0603),

    /* RSASSA-PSS algorithms with public key OID rsaEncryption */
    rsa_pss_rsae_sha256(0x0804),
    rsa_pss_rsae_sha384(0x0805),
    rsa_pss_rsae_sha512(0x0806),

    /* EdDSA algorithms */
    ed25519(0x0807),
    ed448(0x0808),

    /* RSASSA-PSS algorithms with public key OID RSASSA-PSS */
    rsa_pss_pss_sha256(0x0809),
    rsa_pss_pss_sha384(0x080a),
    rsa_pss_pss_sha512(0x080b),

    /* Legacy algorithms */
    rsa_pkcs1_sha1(0x0201),
    ecdsa_sha1(0x0203),

    [redacted]

} SignatureScheme;
```

MUST for certificates

MUST

MUST for CertificateVerify and certificates

Edwards曲線上の Schnorr 署名ライクな EdDSA

4.2.7. Supported Groups

When sent by the client, the "supported_groups" extension indicates the named groups which the client supports for key exchange, ordered from most preferred to least preferred.

```
enum {

    /* Elliptic Curve Groups (ECDHE) */
    secp256r1(0x0017), secp384r1(0x0018), secp521r1(0x0019),
    x25519(0x001D), x448(0x001E),

    /* Finite Field Groups (DHE) */
    ffdhe2048(0x0100), ffdhe3072(0x0101), ffdhe4096(0x0102),
    ffdhe6144(0x0103), ffdhe8192(0x0104),

    /* Reserved Code Points */
    ffdhe_private_use(0x01FC..0x01FF),
    ecdhe_private_use(0xFE00..0xFEFF),
    (0xFFFF)
} NamedGroup;
```

MUST

SHOULD

secp256r1, secp384r1, secp521r1: Standards for Efficient Cryptography Group, SEC 2: "Recommended Elliptic Curve Domain Parameters“ http://www.secg.org/sec2-v2.pdf

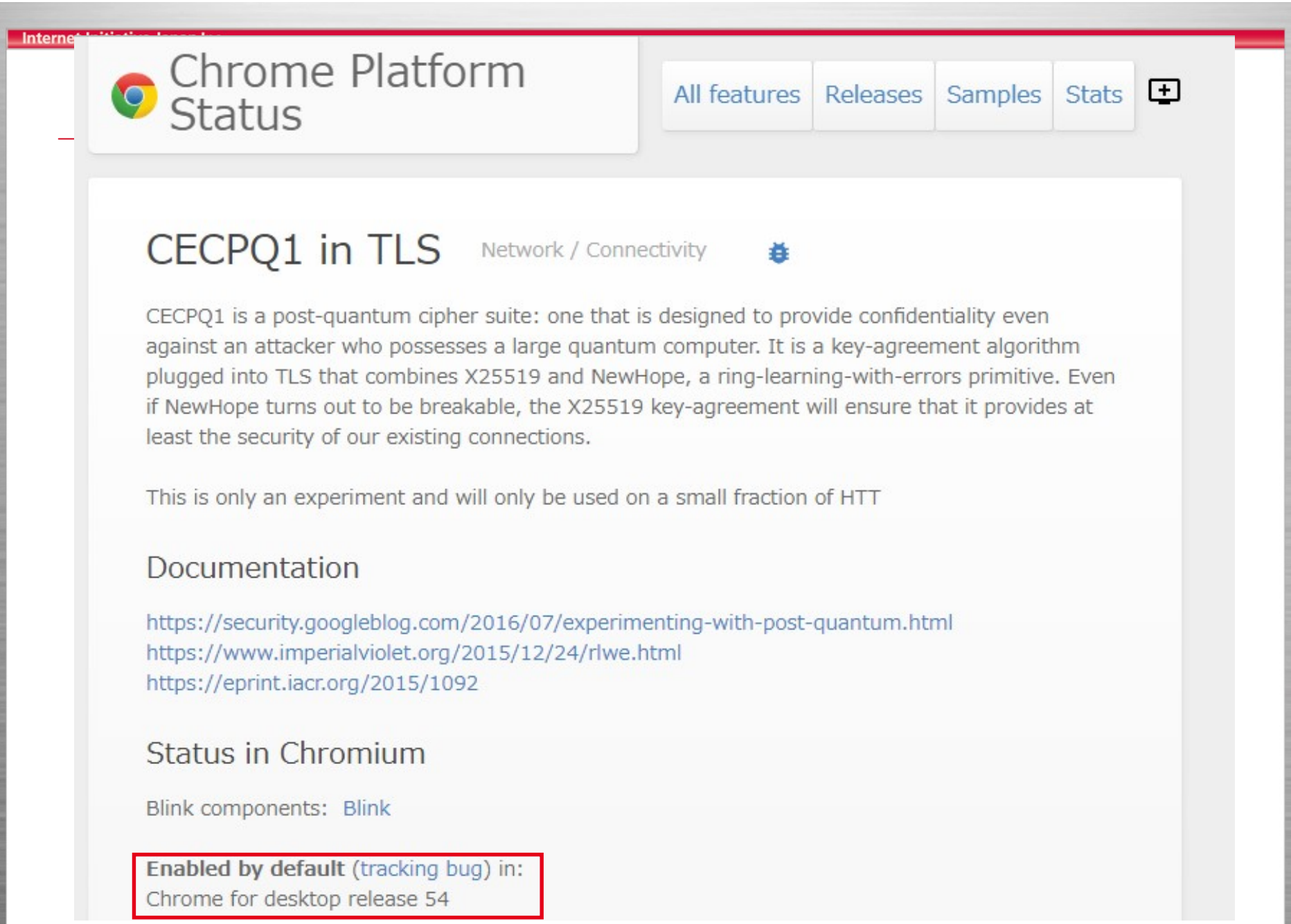
x25519, x448：”Elliptic Curves for Security”, https://datatracker.ietf.org/doc/rfc7748/

1. Alg. 追加情報

Beyond TLS1.3

2016年7月TLSに PostQなアルゴリズム載っけるぜ報道

念のため黒塗り



https://www.chromestatus.com/feature/5749214348836864

いくつかの先駆的な取り組み

- Microsoft Research, Open Quantum Safe library
  - https://github.com/open-quantum-safe/
  - https://qtesla.org/
- Google, Post-quantum confidentiality for TLS
  - https://www.imperialviolet.org/2018/04/11/pqconftls.html
- CloudFlare, Introducing CIRCL: An Advanced Cryptographic Library
  - https://blog.cloudflare.com/introducing-circl/

PQC Standardization Process: Second Round Candidate Announcement

January 30, 2019

After over a year of evaluation, NIST would like to announce the candidates that will be moving on to the 2nd round of the NIST PQC Standardization Process.

The 17 Second-Round Candidate public-key encryption and key-establishment algorithms are:

- BIKE
- Classic McEliece
- CRYSTALS-KYBER
- FrodoKEM
- HQC
- LAC
- LEDAcrypt (merger of LEDAkem/LEDApkc)
- NewHope
- NTRU (merger of NTRUEncrypt/NTRU-HRSS-KEM)
- NTRU Prime
- NTS-KEM
- ROLLO (merger of LAKE/LOCKER/Ouroboros-R)
- Round5 (merger of Hila5/Round2)
- RQC
- SABER
- SIKE
- Three Bears

The 9 Second Round Candidates for digital signatures are:

- CRYSTALS-DILITHIUM
- FALCON
- GeMSS
- LUOV
- MQDSS
- Picnic
- qTESLA
- Rainbow
- SPHINCS+

https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates

AWSさんも今月Blogで反応

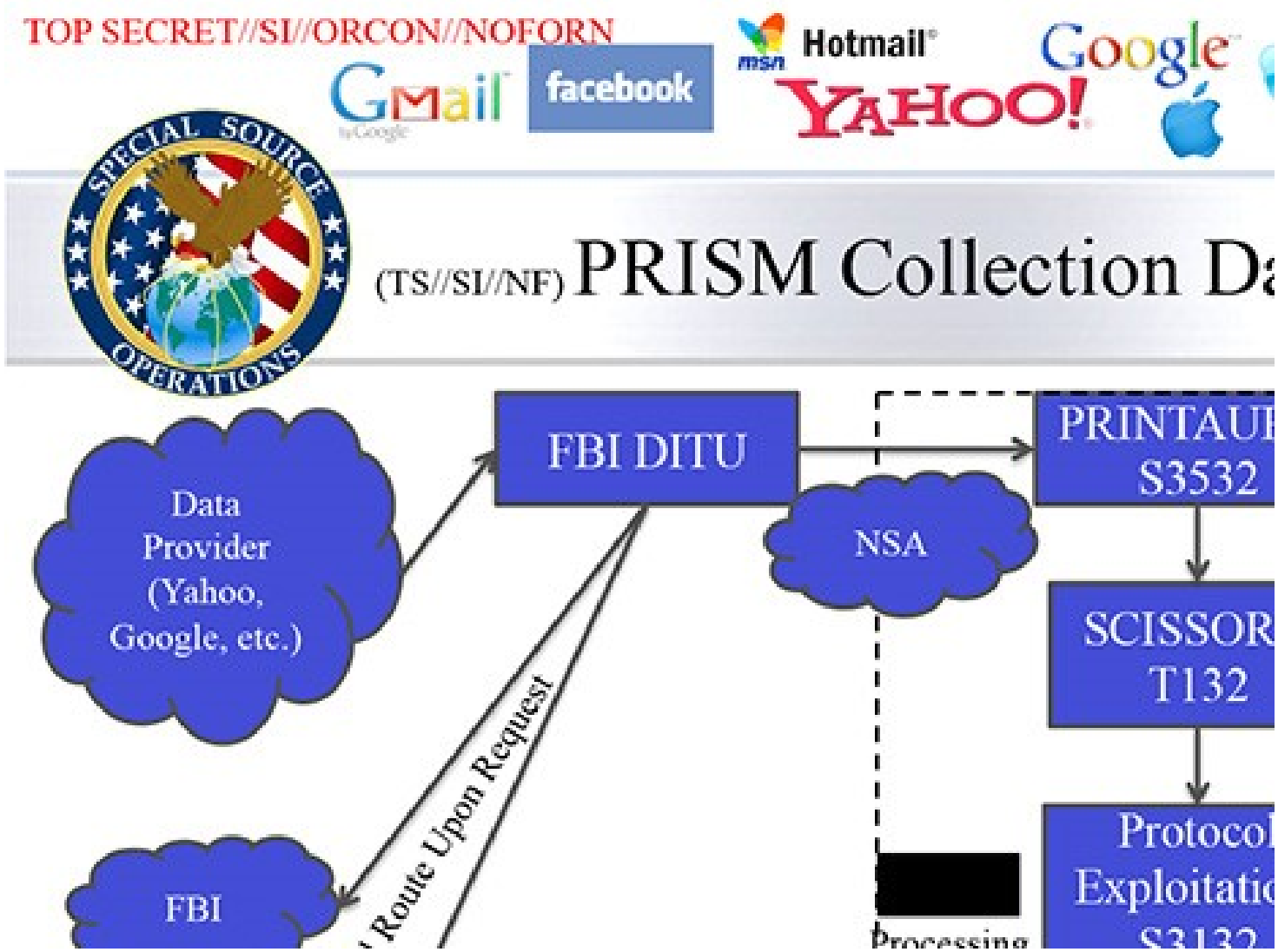
- Post-quantum TLS now supported in AWS KMS by Andrew Hopkins（04 NOV 2019）
  - https://aws.amazon.com/jp/blogs/security/post-quantum-tls-now-supported-in-aws-kms/
  - BIKE, SIKE

2. Priv.

TLS1.3における再設計（プライバシ・常時HTTPS（Always On SSL））

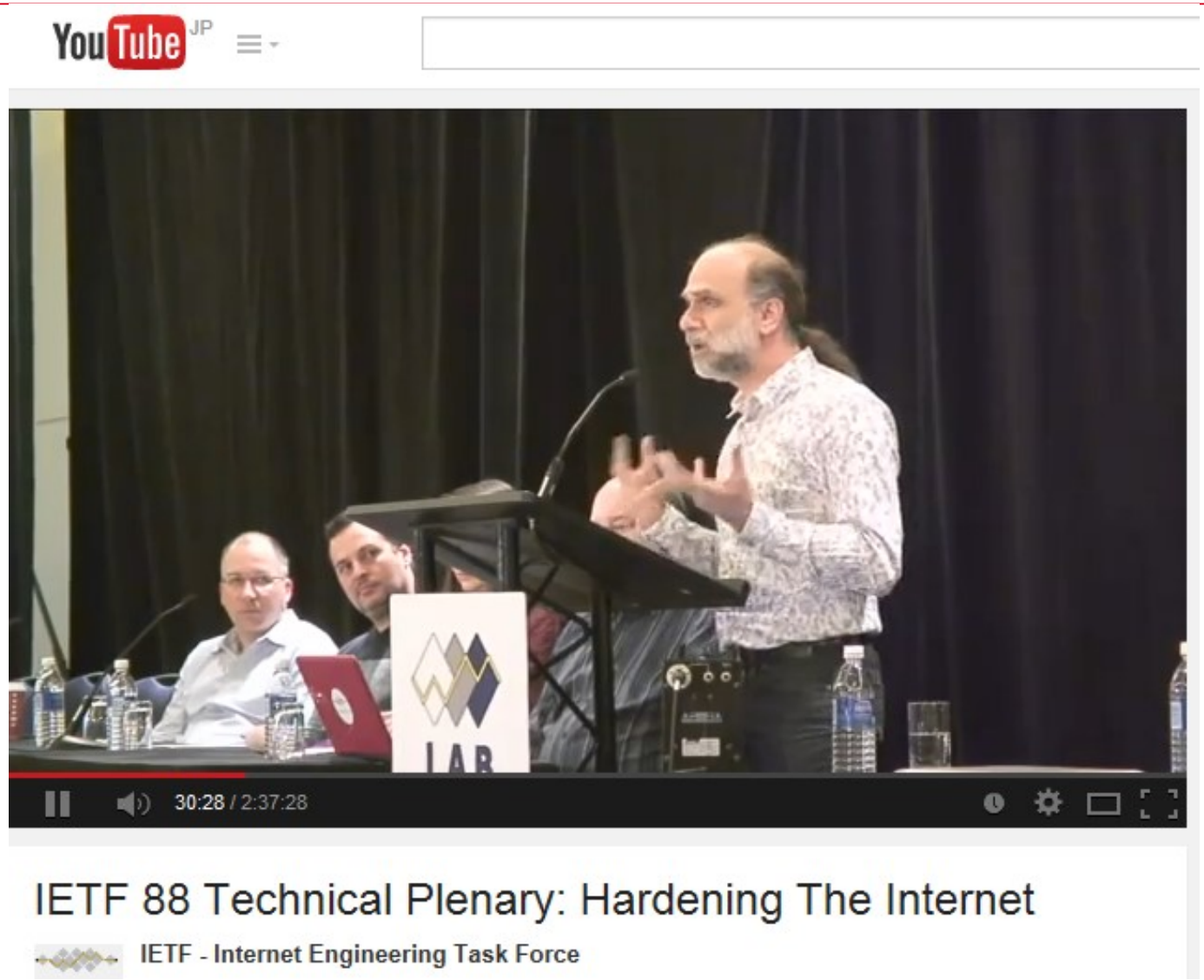
マーケティング用語？

PRISM



http://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)

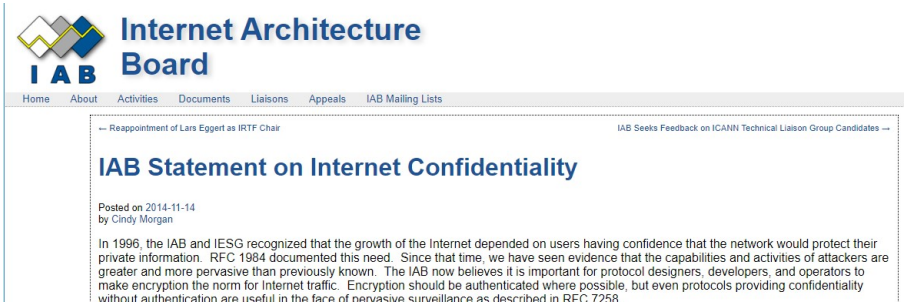
IETF 88 – Pervasive Surveillance



http://www.youtube.com/watch?v=oV71hhEpQ20

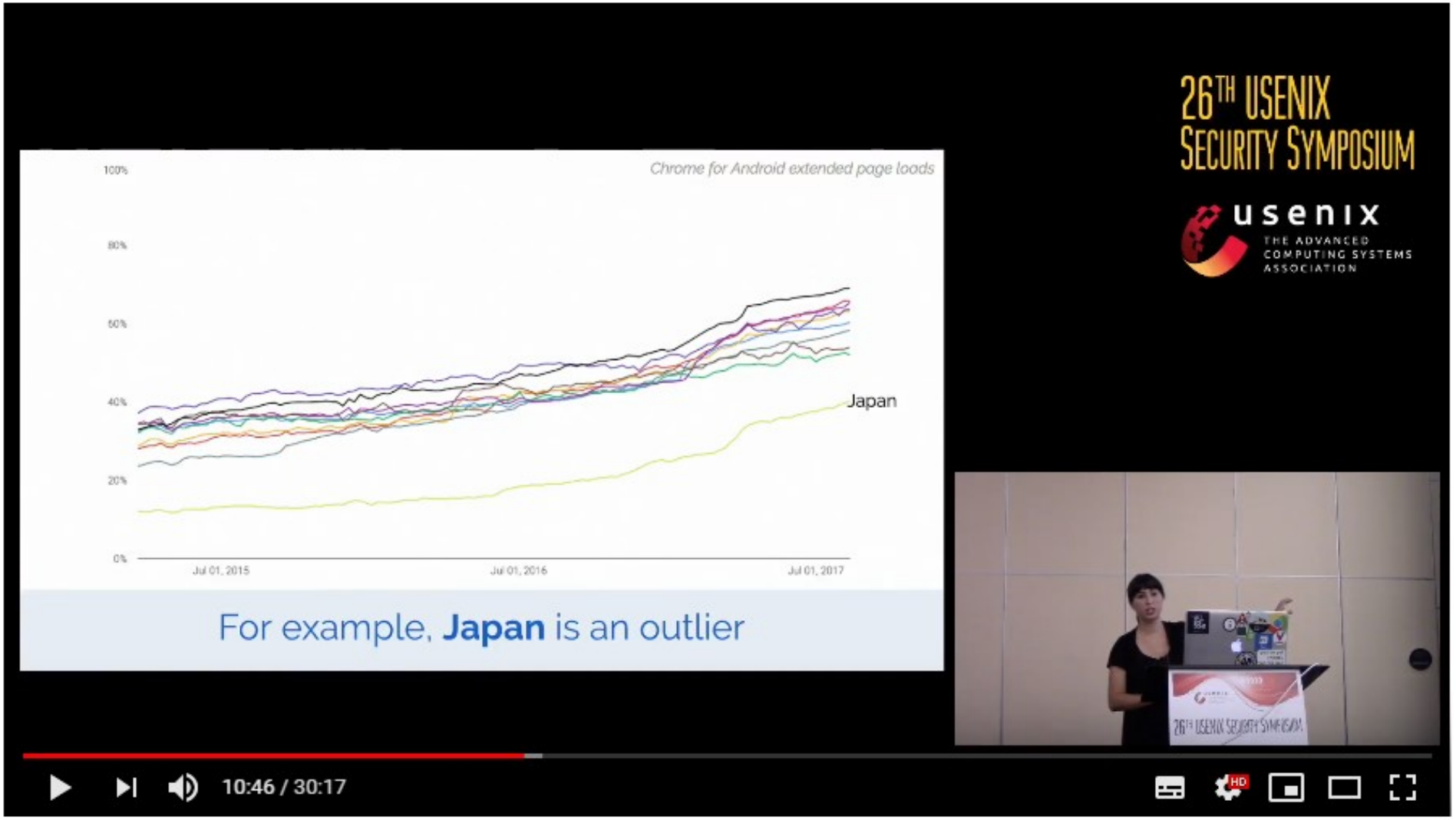
E.J. Snowden 後

- 2014年11月IAB声明
  - https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/



- 「超」短絡的な解決を選択したんだけど…
  - 全部暗号せな なにもかも抜かれてしまうで.
  - せや！全ての通信を暗号化したらええやん.

- でも，それTLSじゃなくてよくね？
  - E2E的）IPsecなどの より下のレイヤでカバー
  - C2C的）S/MIME, GnuPGなどでカバー



USENIX Security '17 - Measuring HTTPS Adoption on the Web

359 回視聴

3 0 共有 保存 ...

日本がフルボッコにあったから？
（もしそうなら消極的では？）

USENIX Security '17 - Measuring HTTPS Adoption on the Web

358 回視聴

https://www.youtube.com/watch?v=toaR0uSabK8

TLS_*_anon_WITH_*

- 暗号化ONLY CipherSuitesの復活は？
  - TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
- と思ったら同じこと考えてるヒト居た（嬉）

TLS 1.3 Authentication and Integrity only Ciphersuites

draft-camwinget-tls-ts13-macciphersuites-04

Status | IESG evaluation record | IESG writeups | Email expansions | History

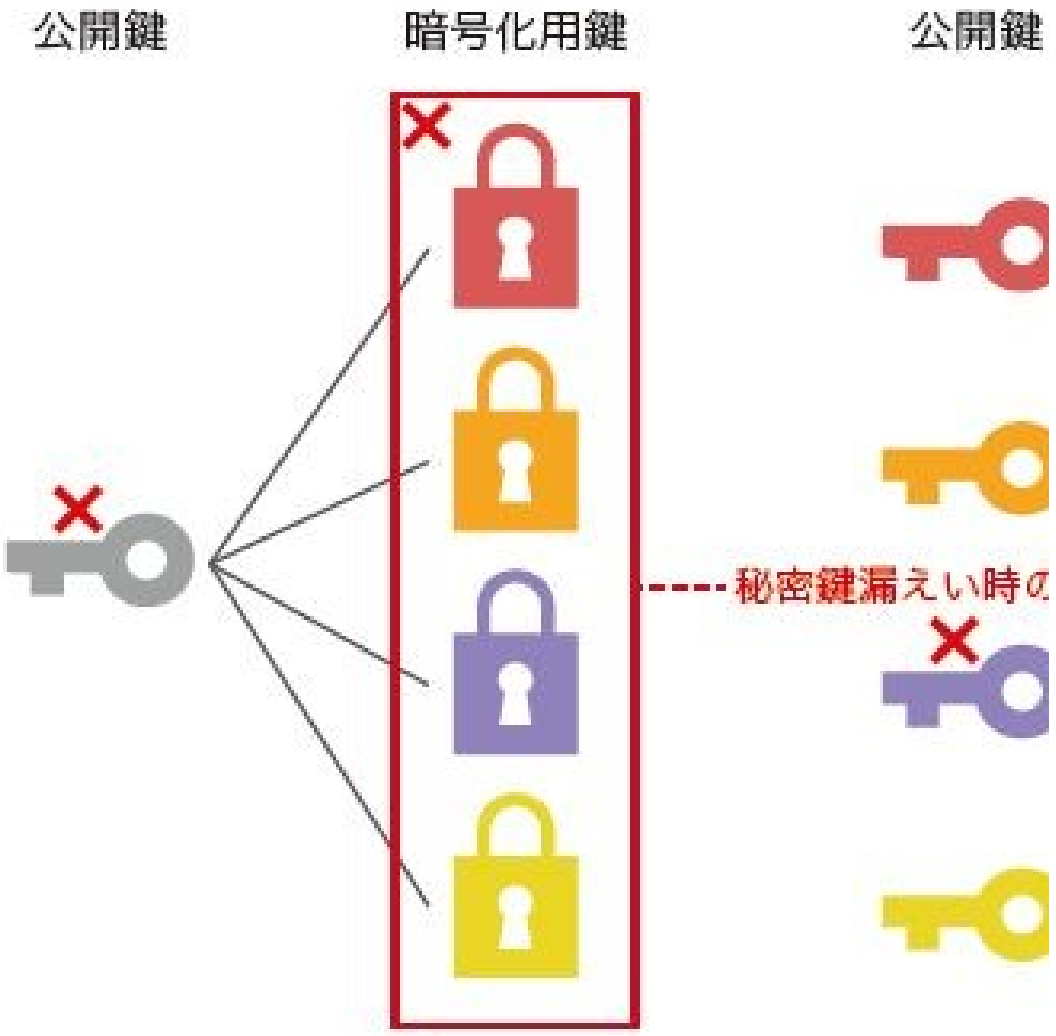
Versions 00 01 02 03 04

Document **Type** Active Internet-Draft (individual)

Last updated 2019-07-08 https://datatracker.ietf.org/doc/draft-camwinget-tls-ts13-macciphersuites

PFS特性

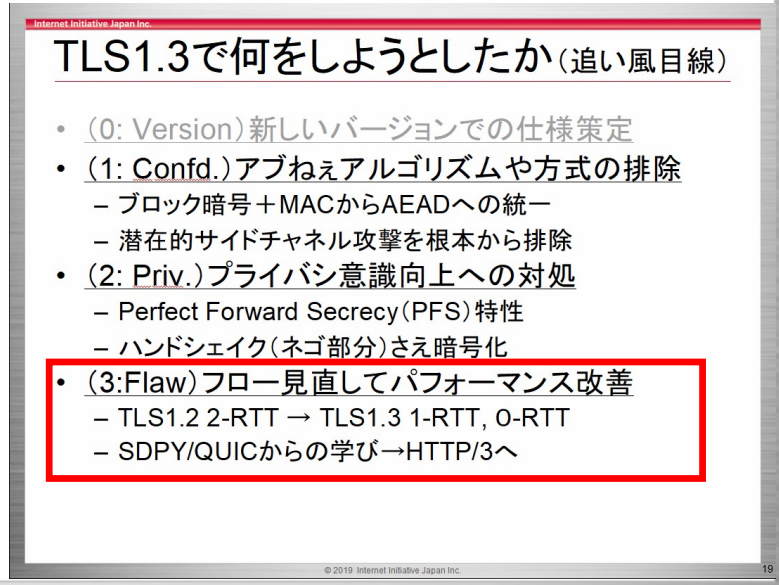
- 基本機能として
  否認防止を
  あえて
  外してましたが．．．



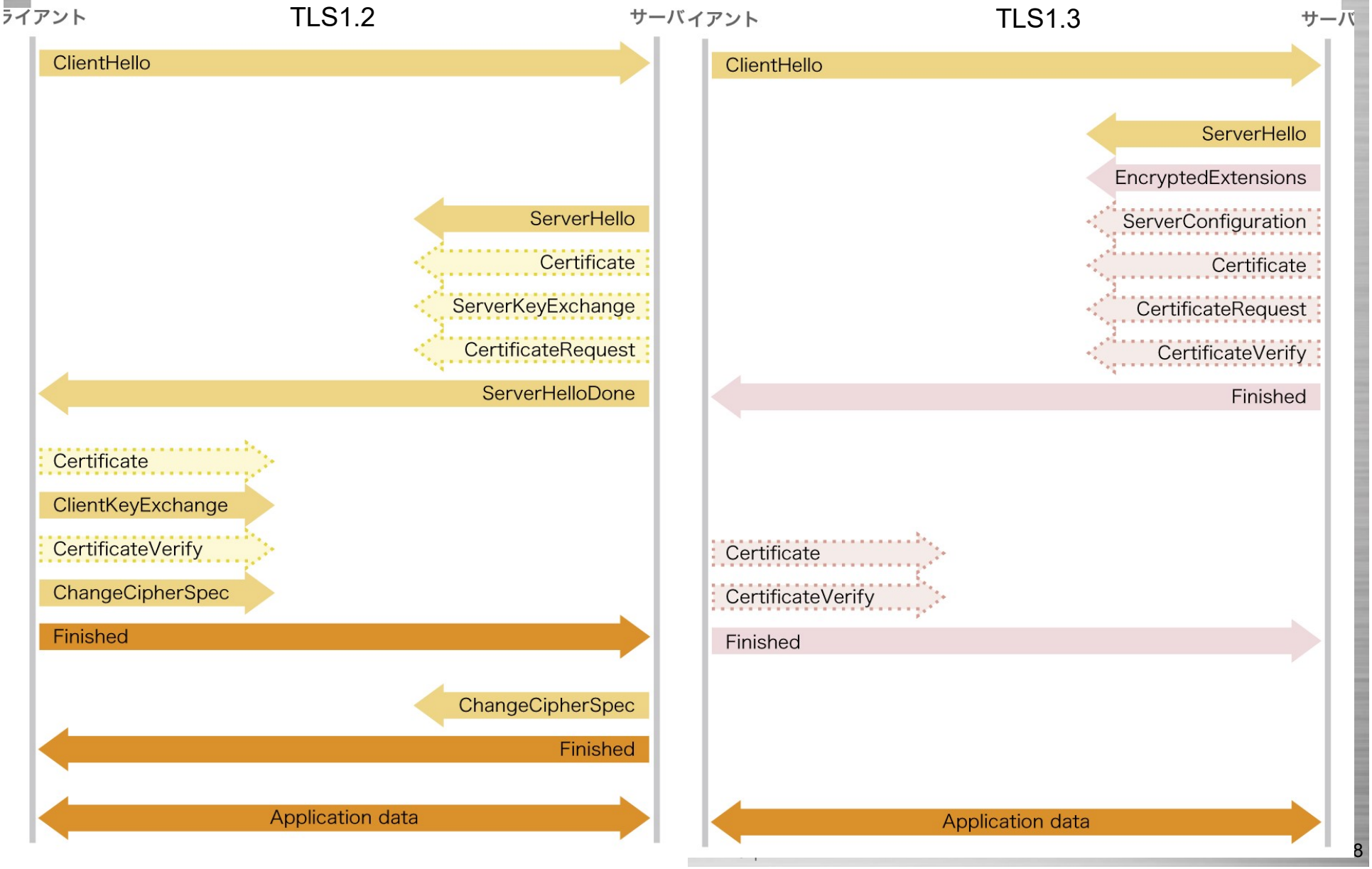
https://www.iij.ad.jp/dev/report/iir/022/01_04.html

3. Flaw

TLS1.3における再設計
（フロー フロー & フロー）

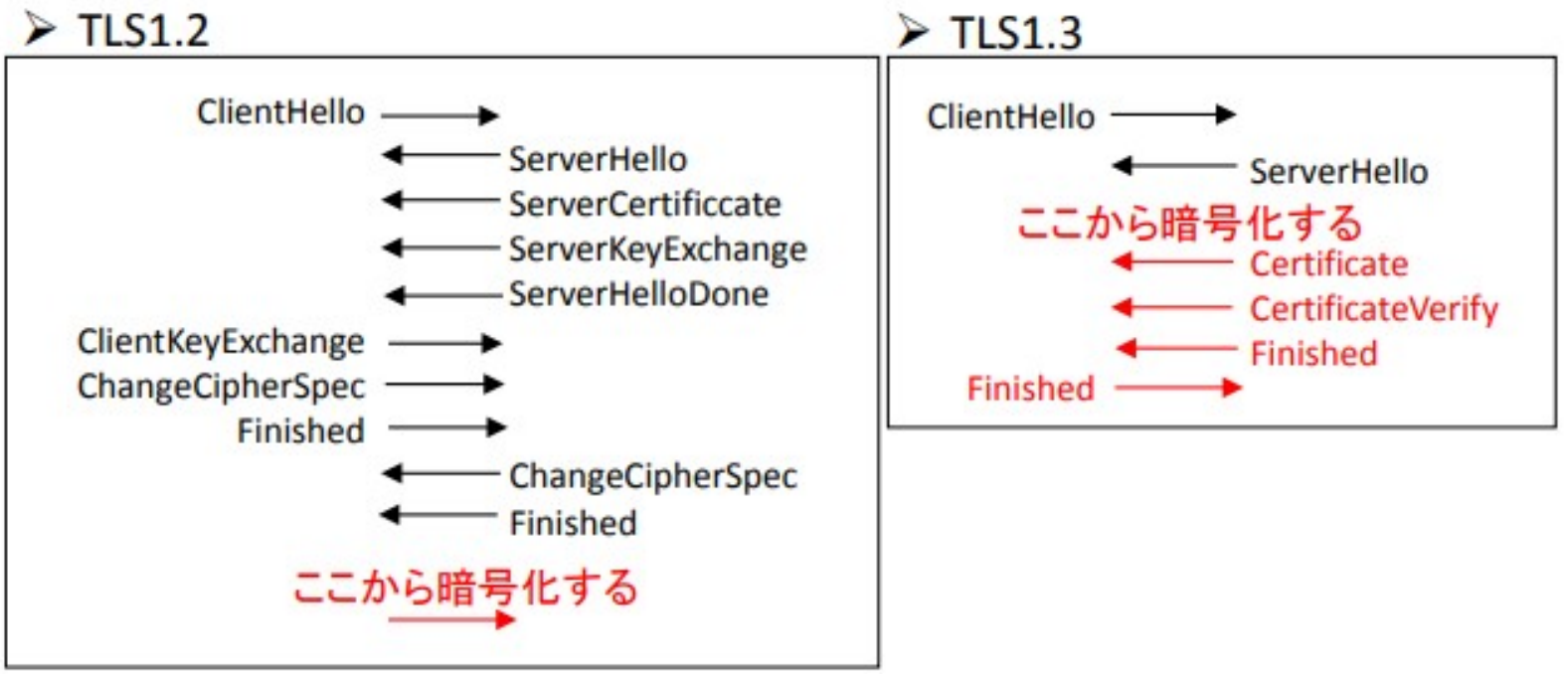


フローの違い（Full Handshake）



シーケンス変化のポイント（1）

ハンドシェイク時から暗号化開始

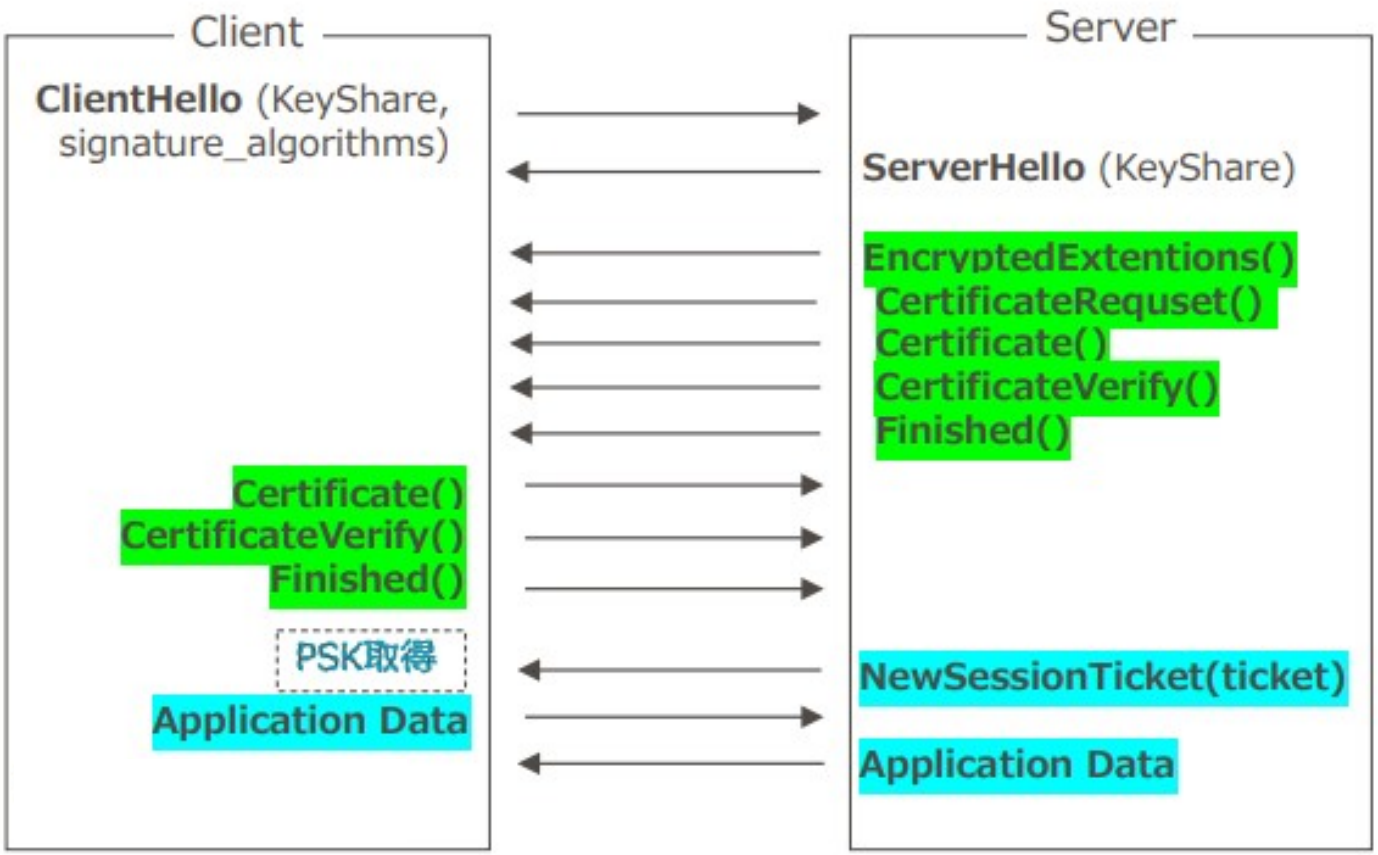


TLS1.2 と TLS1.3 との暗号化開始個所の比較

SSL/TLS 暗号設定ガイドラインは. 第 2.0 版
https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3001-2.0.pdf

シーケンス変化のポイント(2)

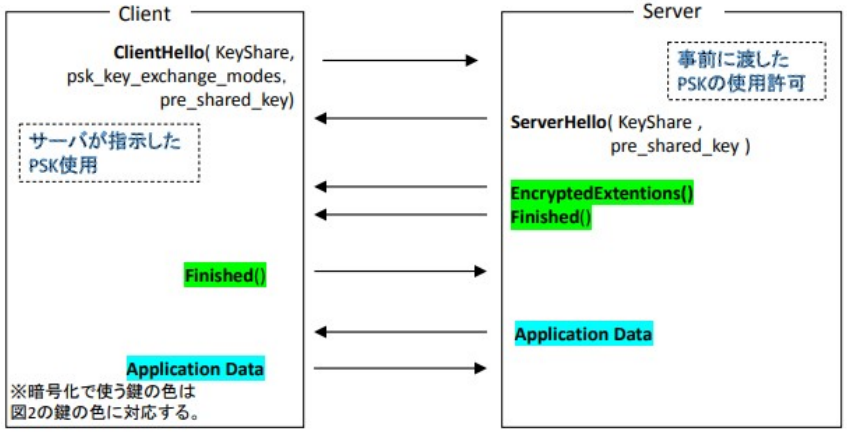
アプリケーションデータの暗号鍵だけではなく2種の鍵を導出



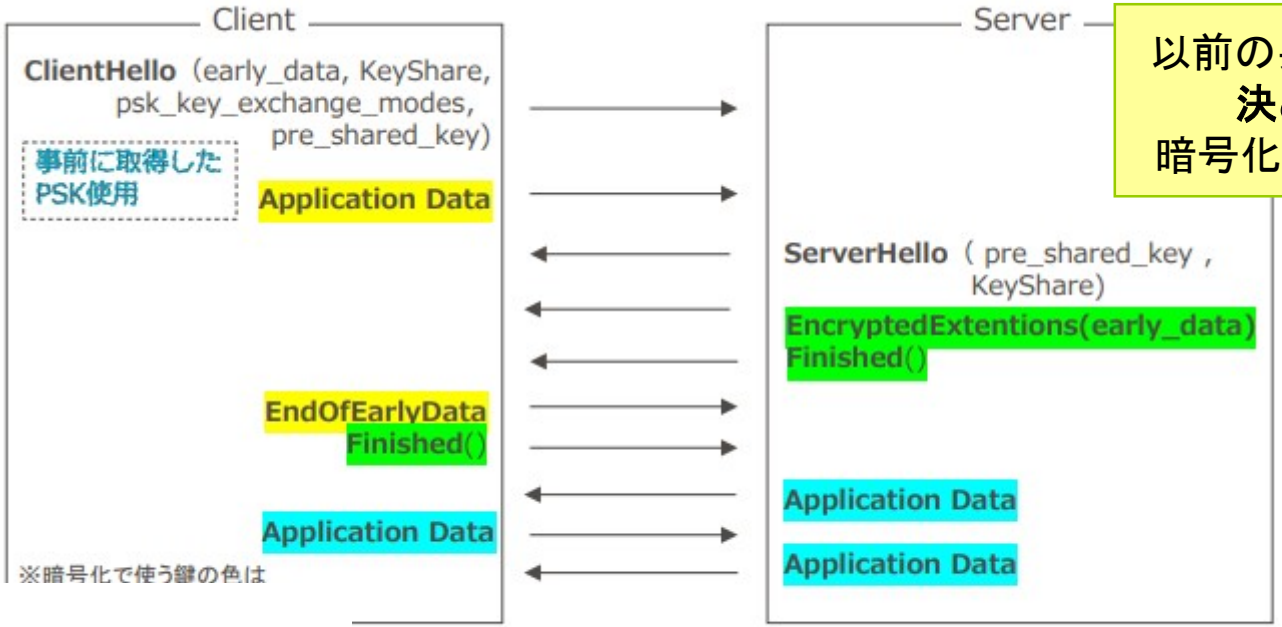
TLS1.3 のシーケンス図

シーケンス変化のポイント(3)

0-RTT(QUIC)でさらに高速処理



1-RTT のシーケンス図



以前の共有情報から
決め打ちで
暗号化データを送信

0-RTT のシーケンス図

自己責任で

4. Trust

やっぱり信頼点が問題なのよ
（PKI・証明書・トラスト厨 歓喜）

あらゆることが原因で EVSSL証明書が泣いている事例たち

- Mixed-Content
- 証明書OID処理バグ

- クロスルート証明書 ← **new!**
  - フィーチャーフォン等のレガシー対応とも関連

参考：サーバ証明書発行時の確認レベル

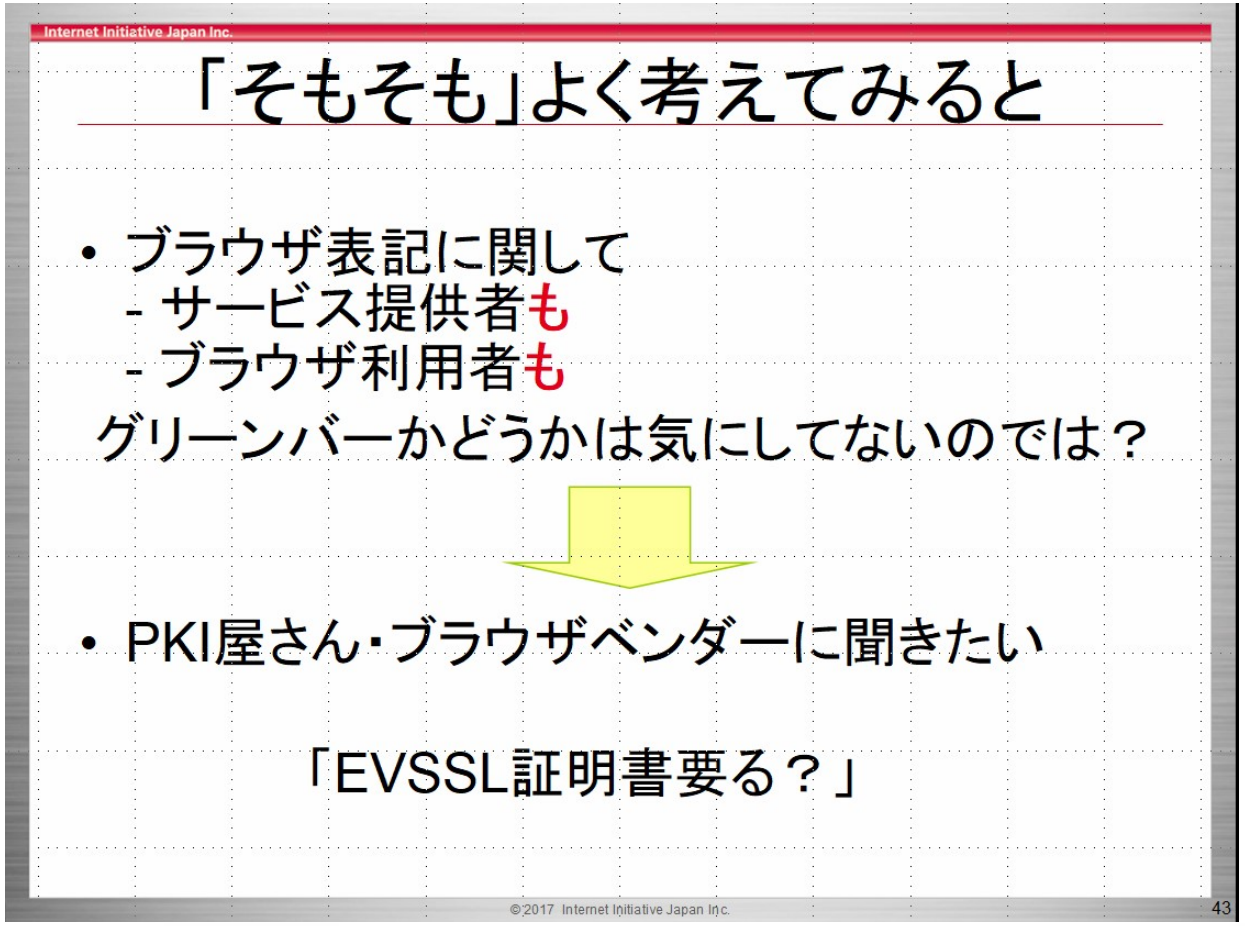
DV（Domain Validated）証明書	ドメイン名の所在のみを確認して証明書を発行。
OV（Organization Validation）証明書	組織の所在（実在性）を確認をして証明書を発行。
EV（Extended Validation）証明書	CA/Bowser Forum で規定された手順に則り証明書を発行。ブラウザでURL記載部分が緑色になるなど、DV/OV証明書との更なる差別化が図られている。

- OV,DVでは登記事項証明書との突き合わせをやることでリアルな「実在性」も確認.
  - 加えて電話等で申請の意思確認も.

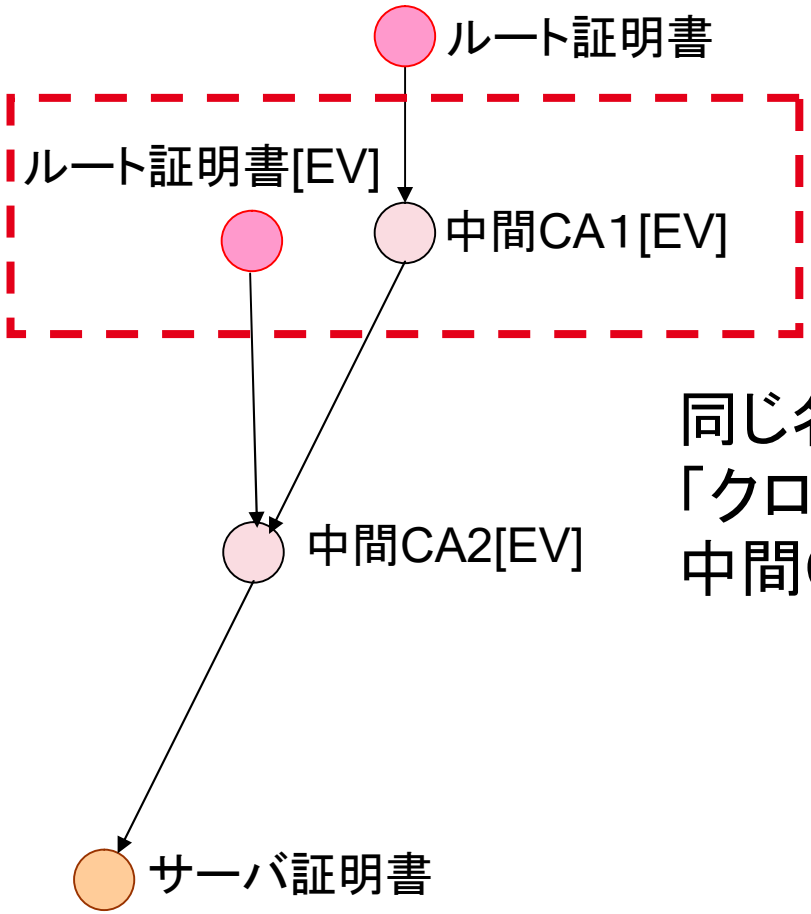
IIJ, IIRvol.30, 1.4.2 Let's Encryptプロジェクトと証明書自動発行のための ACMEプロトコル
http://www.iij.ad.jp/company/development/report/iir/030/01_04.html

EVSSL証明書の再考

- 2017年7月 Janog40 meeting の資料から
  - 当時はまだグリーンバーによるメリットがあった



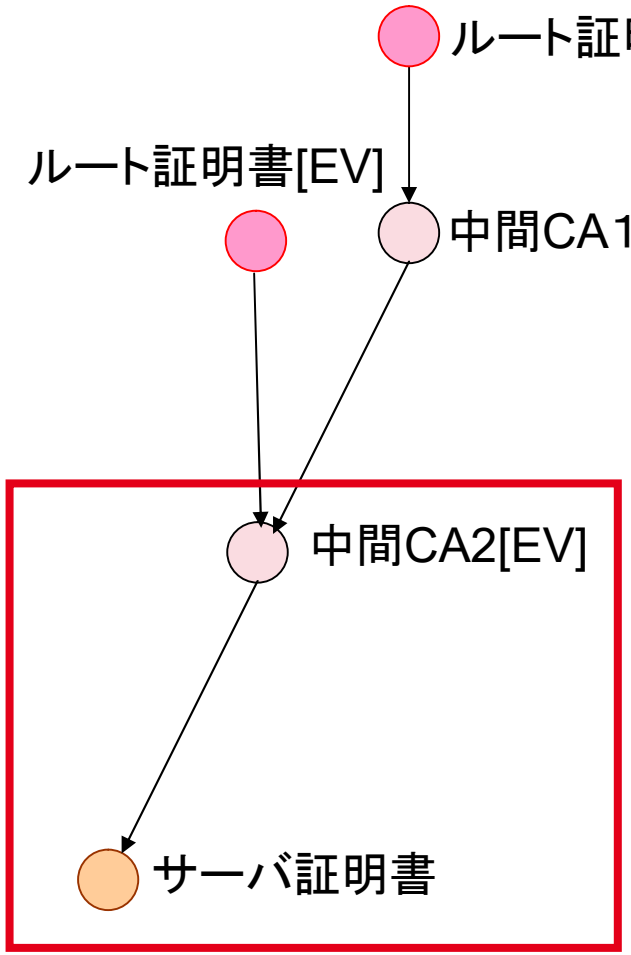
別のEVSSL証明書 不活性問題



ブラウザのトランスアンカーに
入っている

同じ名前でルート証明書でない
「クロスルート証明書」と呼ばれる
中間CA証明書(1)が存在するという状況

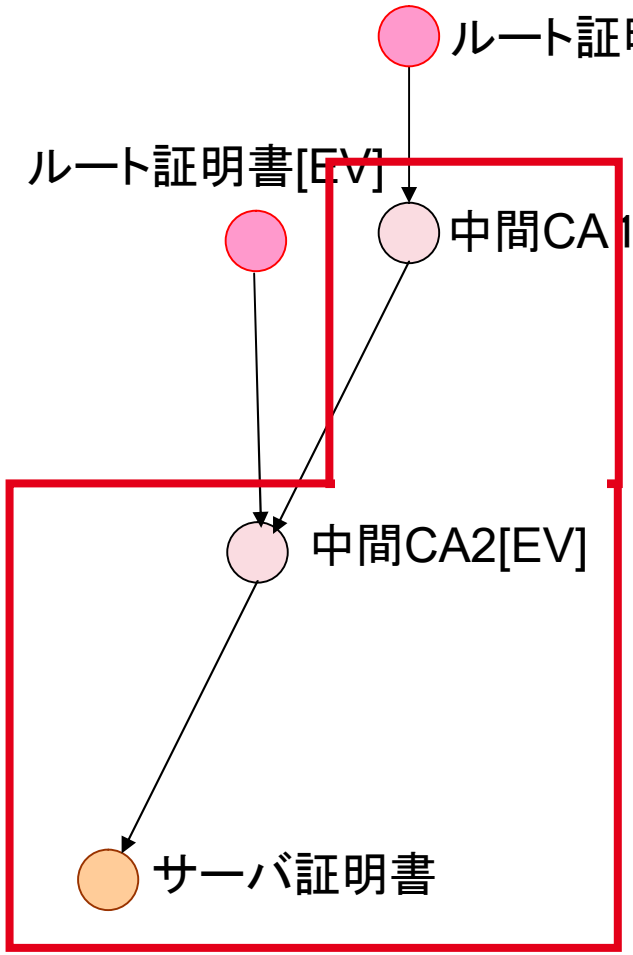
別のEVSSL証明書 不活性問題



ブラウザのトランスアンカーに
入っている

SSL/TLS接続した際にサーバから
この2枚の証明書を送りつける場合は
セーフ

別のEVSSL証明書 不活性問題

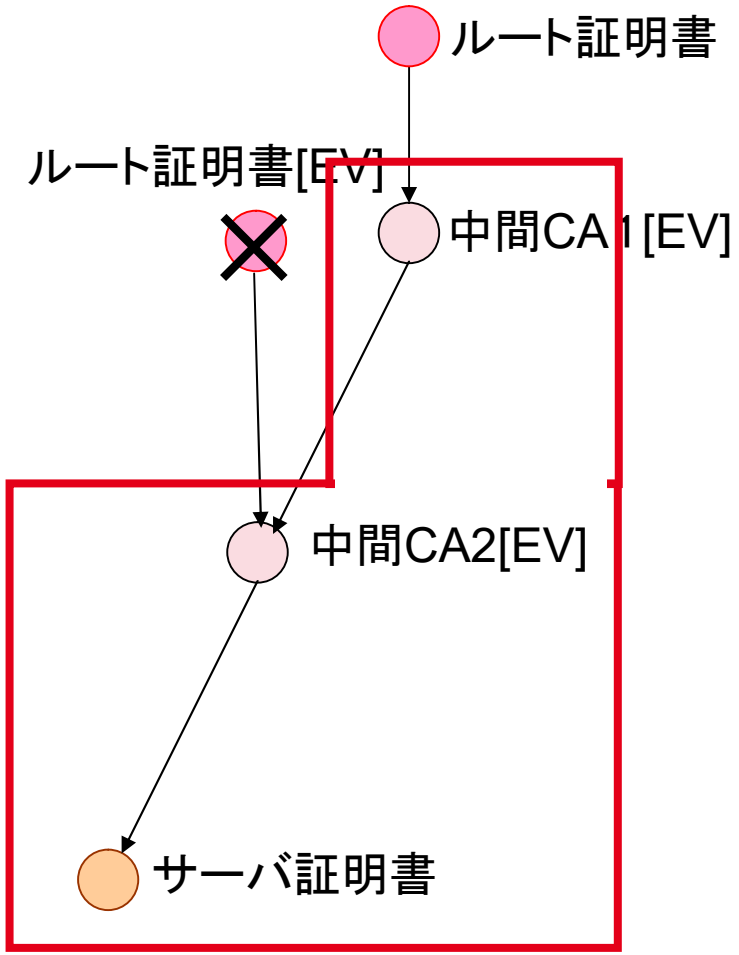


ブラウザのトランスアンカーに入っている

SSL/TLS接続した際にサーバから
この3枚の証明書を送りつける場合は
アウト

本来な左の ● に
パスが伸びる実装が素直では？

これフィーチャーフォン対策でした



- 中間CA1を送らないとルート証明書までのパスを辿れない
- 泣く泣くEV不活性にしている実情

- ある業界：10 / 55

EVSSL証明書利用時
セキュリティインディケータの表記変化

https://www.antiphishing.jp/news/info/_ssl_20191021.html

信頼点って重要だと知らされた事例

- GPKIに関する混乱
- LGPKI：民間に委託

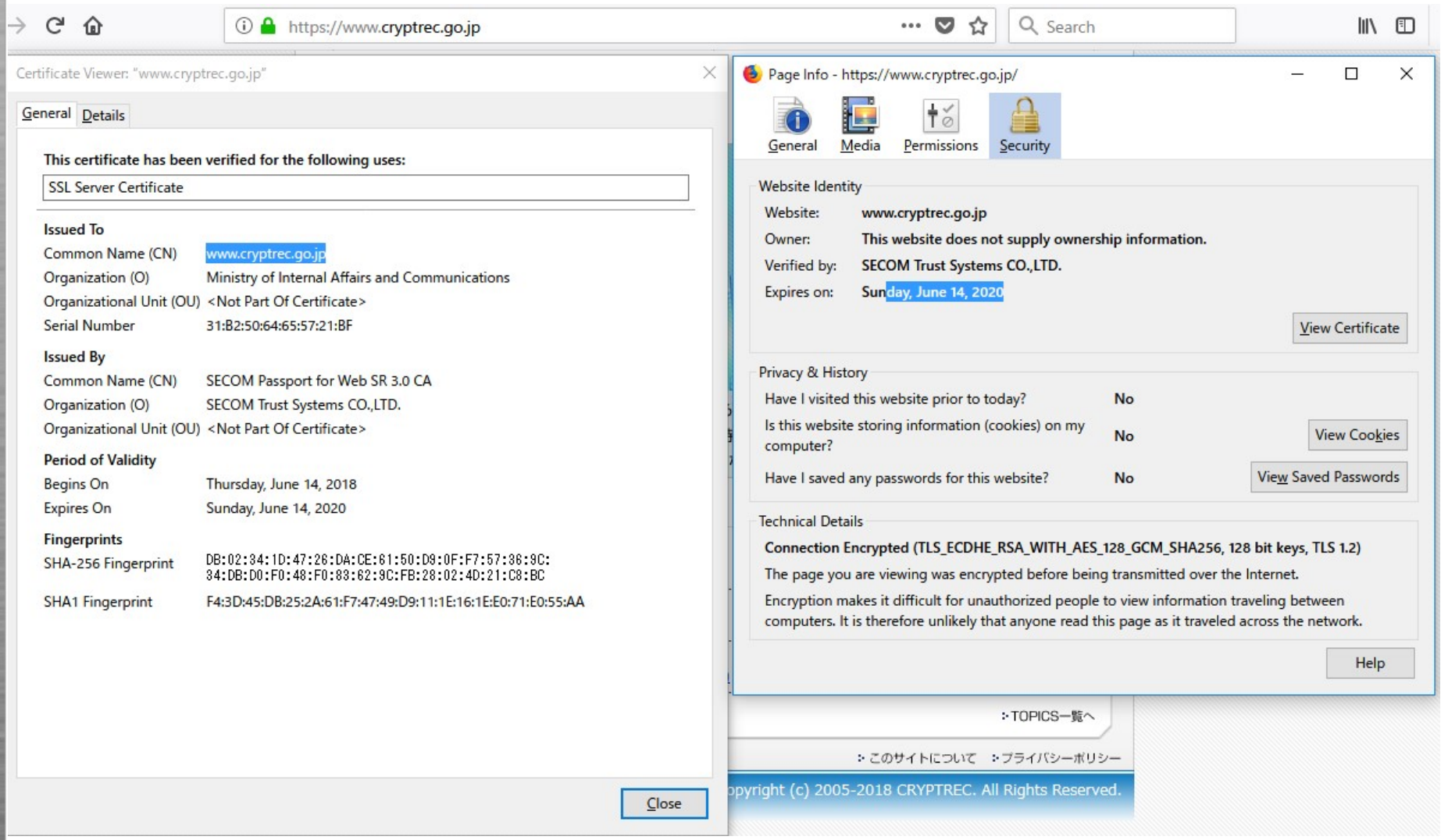
証明書での見え方

Chromeからのスナップショット（2018年6月5日）

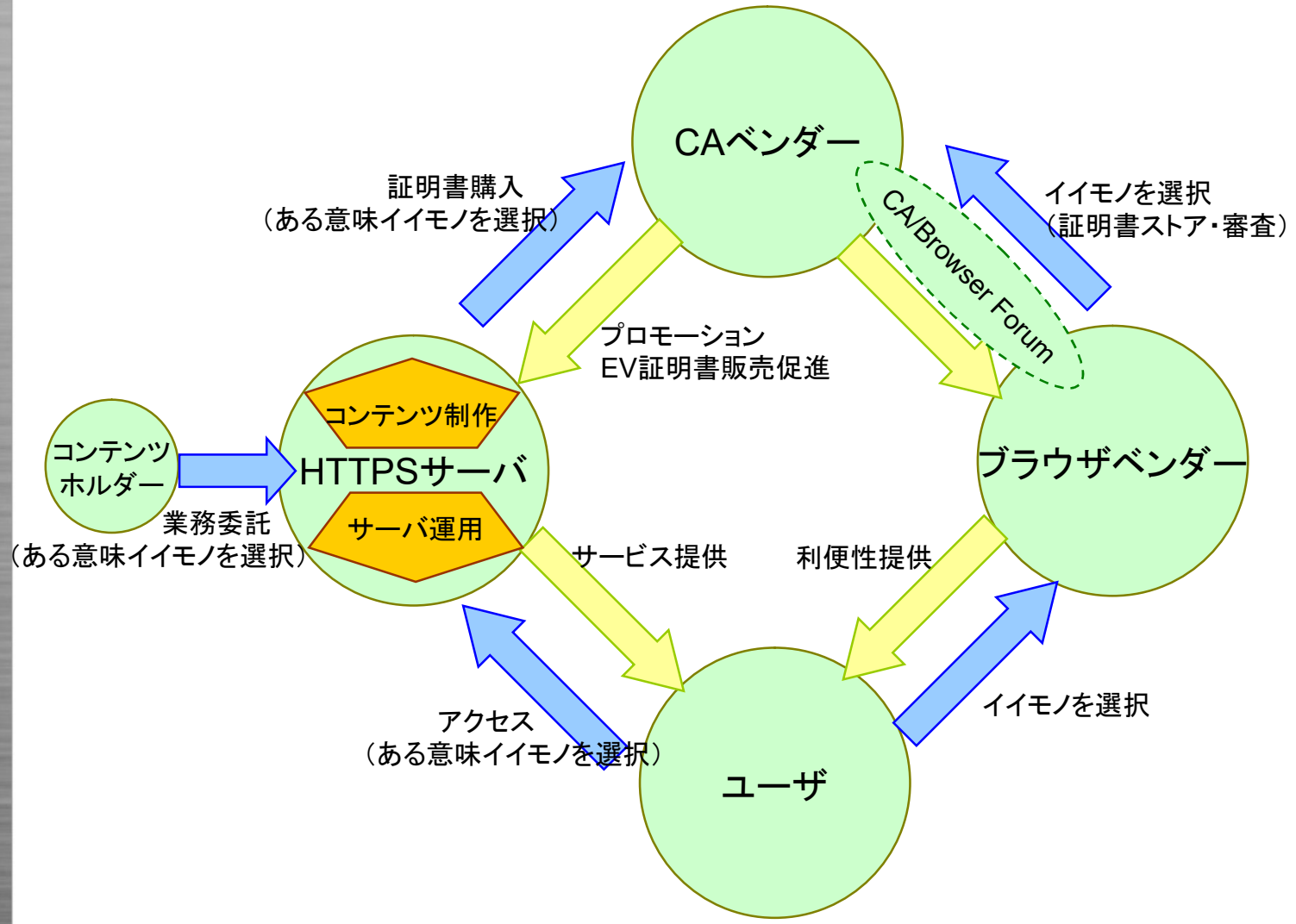
証明書での見え方

Firefoxからのスナップショット（2018年6月5日）

再発行後のFirefoxから



ステークホルダーの関係



Certificate Transparencyの課題

脱線3
念のため黒塗り

脱線3
念のため黒塗り

脱線3
念のため黒塗り

脱線3
念のため黒塗り

5. Others

そのほかの参考情報

2018年10月時点での TLS1.3実装状況

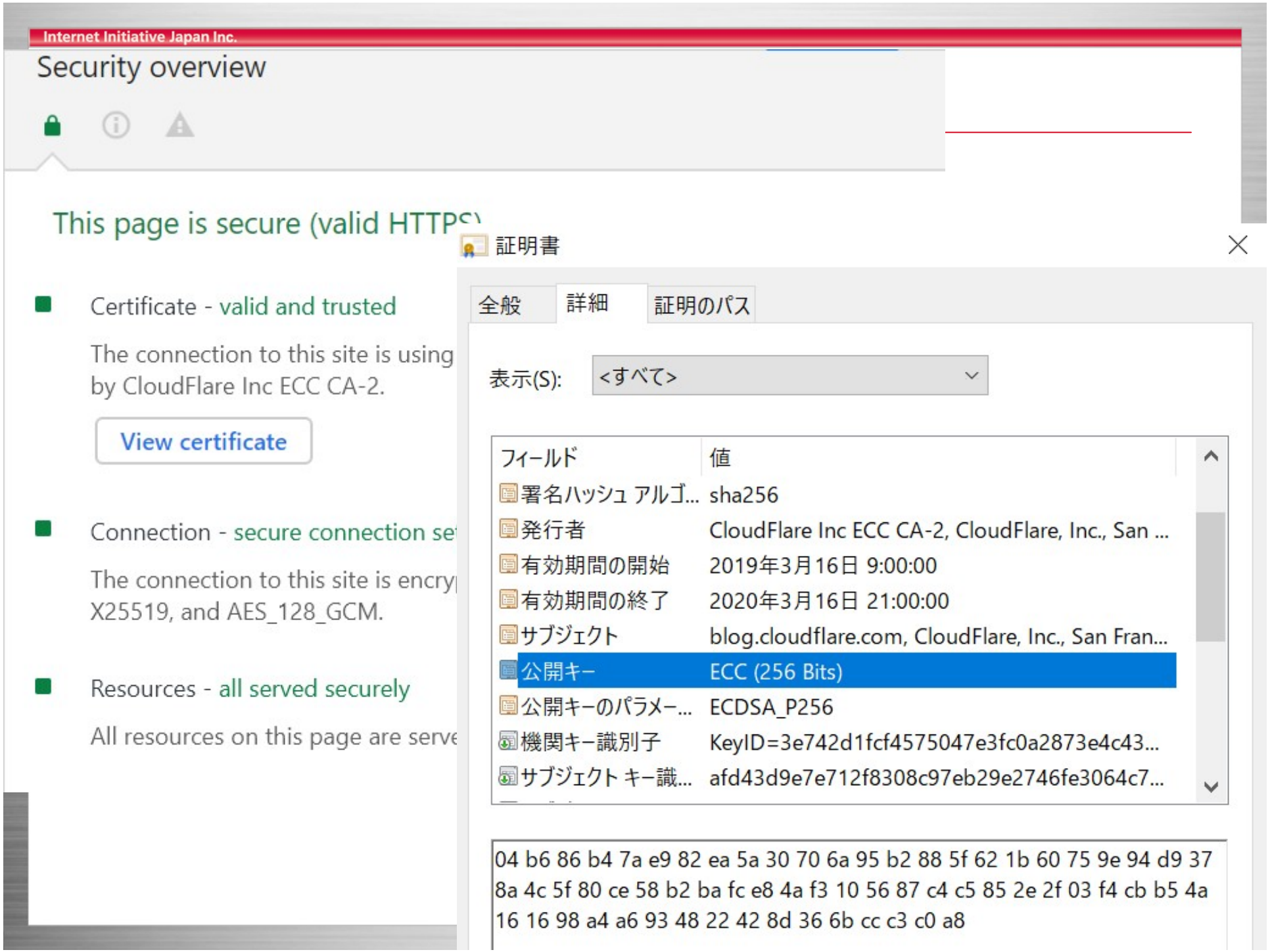
https://github.com/tlswg/tls13-spec/wiki/Implementations

name	language	role(s)	version	features/limitations
fizz	C++	C/S	-28	Based on libsodium, includes secure design abstractions. Zero-copy for advanced pe
NSS	C	C/S	RFC 8446	Almost everything, except post-handshake auth and X448
Mint	Go	C/S	-18	PSK resumption, 0-RTT, HRR
nqsb	OCaml	C/S	-11	PSK/DHE-PSK, no EC*, no client auth, no 0RTT -- live server at tls13test.nqsb.io por ping @hannesm, contains a static PSK/DHE_PSK token: id: 0x0000secret:
ProtoTLS	JavaScript	C/S	-13	EC/DHE/PSK, no HelloRetryRequest
miTLS	F*	C/S	RFC 8446	EC/DHE/PSK/0-RTT, no RSA-PSS, no post-HS-auth, no ESNI
Tris	Go	C/S	RFC 8446	ECDHE/PSK/0-RTT, no HelloRetryRequest
BoringSSL	C	C/S	-23, -28, RFC 8446	P-256, X25519, HelloRetryRequest, resumption, 0-RTT, KeyUpdate
Wireshark	C	other	-18 to -28, RFC 8446	Full decryption and dissection support for drafts 19-21 since 2.4.0 (keylog format). Su since 2.4.3, -23 since 2.4.5, -24 to -28 (+0RTT trial decryption) since 2.6.0. Tracking l
picotls	C	C/S	-18,-21,-23,-26	P-256, X25519, HelloRetryRequest, resumption, 0-RTT
rustls	Rust	C/S	-28 (final on branch)	P-256/P-384/curve25519, HRR, resumption, 0-RTT client
Haskell tls	Haskell	C/S	-28	ECDHE w/ P* and X*, full, HRR, PSK, 0RTT
Leto	C#	S	-18	DHE, X25519, AES, no PSK no 0RTT. Tested against NSS
OpenSSL	C	C/S	RFC 8446	P-256, P-384, P-521, X25519, X448, Ed25519, Ed448, HelloRetryRequest, resumptio stateless server, Post-handshake auth, KeyUpdate, RSA-PSS certs, no FFDHE
wolfSSL	C	C/S	-18/-22/-23/-26/-28	P-256, P-384, X25519, Ed25519, HelloRetryRequest, resumption, PSK, 0-RTT, CCS Post-Handshake Auth, KeyUpdate
GnuTLS	C	C/S	-28	P-256, P-384, X25519, FFDHE, RSA-PSS (keys and certs), HelloRetryRequest, Keyl
tlslite-ng	Python	C/S	RFC 8446	ECDHE (all), EdDHE (X25519, X448), FFDHE (all), AES-GCM, Chacha20, HelloRetr and certificate signatures, cookie extension, CCS, PSK, resumption, no ECDSA certi
tlsfuzzer	Python	C	RFC 8446	ECDHE (all), EdDHE (x25519, X448), FFDHE (all), AES-GCM, Chacha20, RSA, Hell

TLS1.3ライブラリはRFC8446ではなくInternetDraft（中途）版も存在

- 先に挙げたライブラリ群は対応済のものが多いが，未実装の機能・アルゴリズムもあるので注意

BoringSSL	-23, -28, RFC 8446	P-256, X25519, HelloRetryRequest, resumption, 0-RTT, KeyUpdate
OpenSSL	RFC 8446	P-256, P-384, P-521, X25519, X448, Ed25519, Ed448, HelloRetryRequest, resumption, PSK, 0-RTT, CCS, cookies, stateless server, Post-handshake auth, KeyUpdate, RSA-PSS certs, no FFDHE
NSS	RFC 8446	Almost everything, except post-handshake auth and X448


Internet Initiative Japan Inc.
Security overview
This page is secure (valid HTTPS)
Certificate - valid and trusted
The connection to this site is using
by CloudFlare Inc ECC CA-2.
View certificate
Connection - secure connection se
The connection to this site is encry
X25519, and AES_128_GCM.
Resources - all served securely
All resources on this page are serve
証明書
全般
詳細
証明のパス
表示(S):
<すべて>
フィールド
値
署名ハッシュ アルゴ...
sha256
発行者
CloudFlare Inc ECC CA-2, CloudFlare, Inc., San ...
有効期間の開始
2019年3月16日 9:00:00
有効期間の終了
2020年3月16日 21:00:00
サブジェクト
blog.cloudflare.com, CloudFlare, Inc., San Fran...
公開キー
ECC (256 Bits)
公開キーのパラメー...
ECDSA_P256
機関キー識別子
KeyID=3e742d1fcf4575047e3fc0a2873e4c43...
サブジェクト キー識...
afd43d9e7e712f8308c97eb29e2746fe3064c7...
04 b6 86 b4 7a e9 82 ea 5a 30 70 6a 95 b2 88 5f 62 1b 60 75 9e 94 d9 37
8a 4c 5f 80 ce 58 b2 ba fc e8 4a f3 10 56 87 c4 c5 85 2e 2f 03 f4 cb b5 4a
16 16 98 a4 a6 93 48 22 42 8d 36 6b cc c3 c0 a8

参考：TLS1.3サーバ構築の一例

- 2017年5月 OpenSSLでの構築方法公開
  - https://www.openssl.org/blog/blog/2017/05/04/tlsv1.3/
  - 設定の注意点など細かい内容まで記載
- 2018月9月11日 OpenSSL1.1.1リリースで正式サポート
  - https://www.openssl.org/blog/blog/2018/09/11/release111/
- 2018年10月Apache 2.4.37 リリース mod_ssl で OpenSSL1.1.1対応
  - https://httpd.apache.org/download.cgi
  - enable-tls1_3 フラグでコンパイルすることで簡単に構築可能

参考：Apache2.4系での拡張ログ対応

https://httpd.apache.org/docs/current/mod/mod_ssl.html#logformats

- クライアントがどのバージョン，CipherSuitesで接続されたかを別のログファイルに追記

Custom Log Formats

When mod_ssl is built into Apache or at least loaded (under DSO situation) additional functions exist for the Custom Log Format {*varname*}x" eXtension format function which can be used to expand any variables provided by any module, especially those pro table.

For backward compatibility there is additionally a special ``%{*name*}c" cryptography format function provided. Information about th

Example

```
CustomLog "logs/ssl_request_log" "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%
```

These formats even work without setting the StdEnvVars option of the SSLOptions directive.

Environment Variables

This module can be configured to provide several iter default for performance reasons. (See SSLOptions available under different names, too. Look in the Com

Variable Name:	Value Type:
HTTPS	flag
SSL_PROTOCOL	string
SSL_SESSION_ID	string
SSL_SESSION_RESUMED	string
SSL_SECURE_RENEG	string
SSL_CIPHER	string
SSL_CIPHER_EXPORT	string
SSL_CIPHER_USEKEYSIZE	number
SSL_CIPHER_ALGKEYSIZE	number

その他様々な情報を残すことが可能→

参考：TLS1.3チュートリアル

- Kennyは話がむっちゃ上手
  - https://crypto.iacr.org/2018/affevents/cwtls/medias/Kenny_Paterson.pdf
- EricによるRFC出た直後の話@CRYPTO2018
  - https://crypto.iacr.org/2018/affevents/cwtls/medias/Eric_Rescorla.pdf
- やっぱCBCダメな話
  （特にEnc-then-MACの実装の難しさ）
  - https://crypto.iacr.org/2019/affevents/wac/medias/Merget-ScalableScanningPaddingOracles.pdf

IIJ Internet Initiative Japan

Lead Initiative

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ――――――――――IIJはいつもはじまりであり、未来です。

Ongoing Innovation