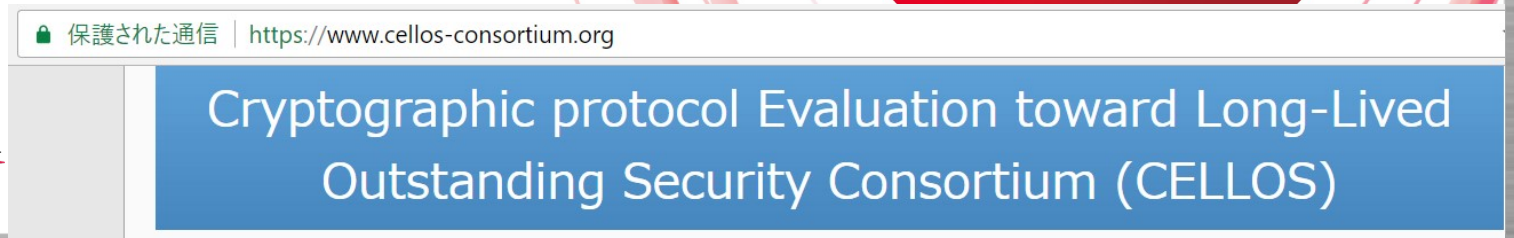
JANOG39 meeting, Kanazawa, January 20, 2017

EVSSL証明書が泣いている「検索窓問題」～ブラウザのセキュリティインディケータを意識していますか～

須賀祐治

2017-01-20

Ongoing Innovation



2014年10月

POODLE attack 概要

2014年10月

- CVE-2014-3566
- 日本時間10月15日に公開
  - https://www.openssl.org/~bodo/ssl-poodle.pdf
- 仕様そのものの問題
  - SSLv3にてCBC暗号モード利用時のみ影響
    - SSLv2は以前から脆弱
- 問題：Padding Oracle Attack の一種.
  サーバのパディングチェック機能を悪用し
  ブラウザから大量のリクエストをサーバに
  送りつけてトライ＆エラーを繰り返し，暗号化
  された攻撃対象データを1バイトずつ復号

POODLE attack への対策

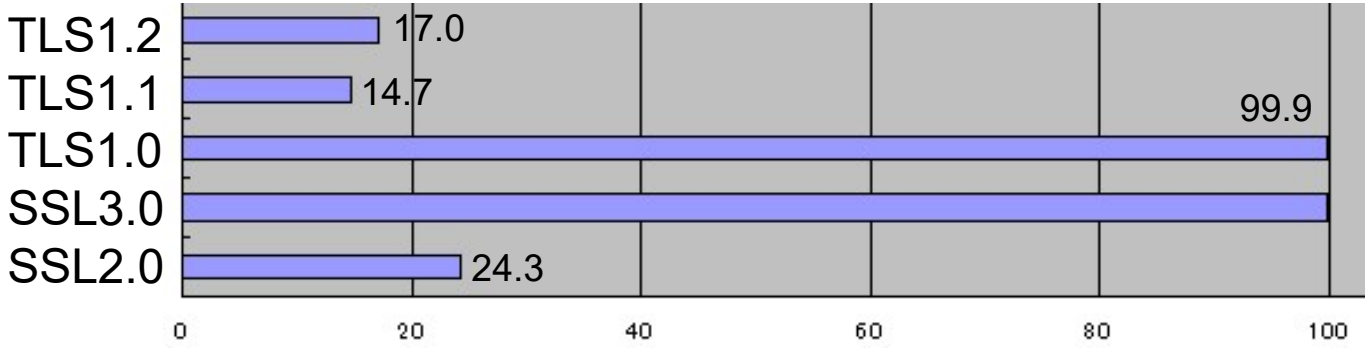
- **（1）SSLv3を捨てる** [=機会損失]
  - Twitterなどで即座に対応が行われた
  - www.iij.ad.jp, help.iij.ad.jp 等でも対策済
- （2）TLS_FALLBACK_ SCSVの導入
  - OpenSSL 10月アップデートで実装済

- 両方の対策ともレガシーな製品（特にフィーチャーフォンやゲーム機器など）からサイトが閲覧できなくなったりするケースも考えられる

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-02

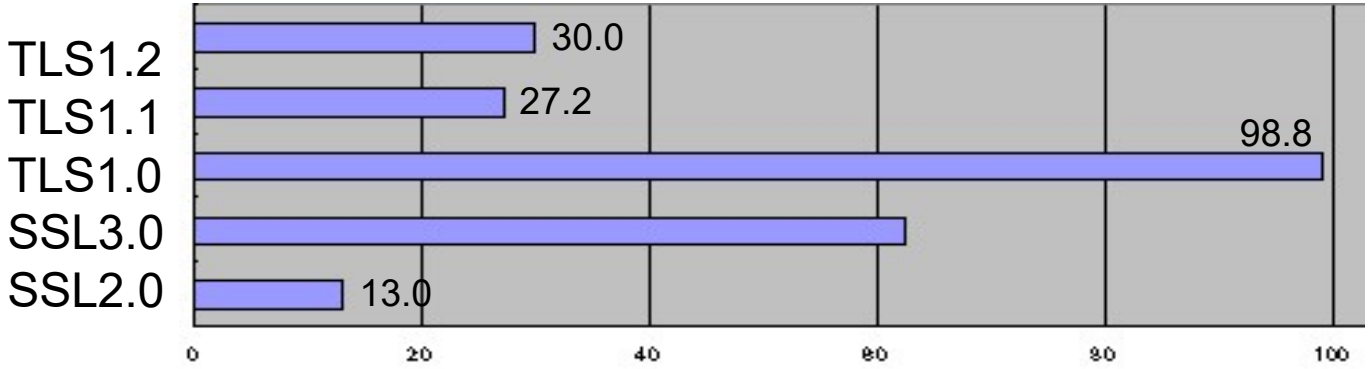
SSL/TLSサーバのバージョン移行状況（2014年）

- 4月15日 SSL-enable sites=5677



99.9%

- 11月26日 SSL-enable sites=5620



62.3%

SSLv3を無効にするサイトが大幅に増加している

Alexa top 100M sites に記載されている .jp ドメイン17988サイトを調査
両日ともに同じURLリストを利用

2015年1月

FREAK attack 概要

- CVE-2015-0204
- 2015年 日本時間3月3日にサイト公開（再認識）
  - https://freakattack.com/
- 脆弱なバージョン：
  - 2015年1月のUpdateで修正済
  - クライアント

    各系列 1.0.1j以下，1.0.0o以下，0.9.8zd 以下
- 問題：クライアントの指定したCipherSuitesではなくExport-grade（輸出可能な弱い）暗号を意図せず利用されてしまう

Freakattack.com

- これまでにも「サーバ設定の不備が風評被害になりうる」と言ってた→今回わりと現実的に
  - 技術的に理解していない方でもブラックリストのように見えるわけで，実際Twitterなどでいくつかの日本のサーバが名指しされている.
- さすがにもうこの時期に輸出規制時代のCipherSuitesをサポートすることは後方互換性の確保のため，という理由にはならないか

ブラックリスト（のように見える）

https://freakattack.com/vulnerable.txt

sleazyneasy.com,68.169.101.206,rsa-export katestube.com,64.188.53.206,rsa-export
indiocasino.com,212.64.147.151,rsa-export googleping.com,208.109.97.183,rsa-export
kohls.com,23.202.240.45,rsa-export vente-privee.com,185.45.180.3,rsa-export
lan.com,67.15.147.205,rsa-export delfi.lv,62.63.137.4,rsa-export
adplxmd.com,205.186.187.178,rsa-export alltop.com,184.106.130.115,rsa-export
leparisien.fr,95.131.142.225,rsa-export doctissimo.fr,85.116.34.4,rsa-export
dinodirect.com,184.173.225.136,rsa-export wannonce.com,188.165.15.58,rsa-export
4shared.com,208.88.224.138,rsa-export tribalfusion.com,204.11.109.195,rsa-export
suntimes.com,64.94.90.42,rsa-export hola.com,62.22.171.50,rsa-export
santander.com.br,172.224.248.145,rsa-export ets.org,144.81.88.152,rsa-export
wowhead.com,23.6.67.58,rsa-export sidereel.com,173.247.105.225,rsa-export
umich.edu,141.211.243.44,rsa-export itv.com,193.35.9.65,rsa-export
honda.com,164.109.25.194,rsa-export nordstromrack.com,23.193.174.147,rsa-export
giga.de,80.86.80.168,rsa-export lolking.net,23.6.67.58,rsa-export
gocomics.com,66.6.101.183,rsa-export eltiempo.com,200.41.9.39,rsa-export
trafficholder.com,64.111.214.2,rsa-export estadao.com.br,23.6.72.37,rsa-export
ppomppu.co.kr,110.45.151.210,rsa-export delfi.lt,91.234.200.110,rsa-export
wiocha.pl,195.225.138.230,rsa-export draftkings.com,23.203.3.237,rsa-export
twitcasting.tv,202.234.23.144,rsa-export e-rewards.com,63.241.211.118,rsa-export
propellerads.com,78.140.145.202,rsa-export ziddu.com,84.45.63.57,rsa-export
topshop.com,23.194.147.74,rsa-export alice.it,217.169.121.227,rsa-export
syosetu.com,111.64.91.10,rsa-export trafficshop.com,78.140.142.21,rsa-export
sec.gov,23.203.5.89,rsa-export 337.com,174.36.254.166,rsa-export
epnet.com,140.234.254.41,rsa-export backlinkwatch.com,74.204.189.20,rsa-export
refinery29.com,50.22.34.142,rsa-export ohmyzip.com,216.176.192.139,rsa-export ……..

2015年9月

FIT2015（第 14 回情報科学技術フォーラム）

L-034

Export-grade な暗号アルゴリズムを用いたダウングレード攻撃に対する SSL/TLS サーバの対処状況について

SSL/TLS servers status survey against down-grade attacks with export-grade cipher algorithm

須賀 祐治 *
Yuji SUGA

2015年6月に再調査

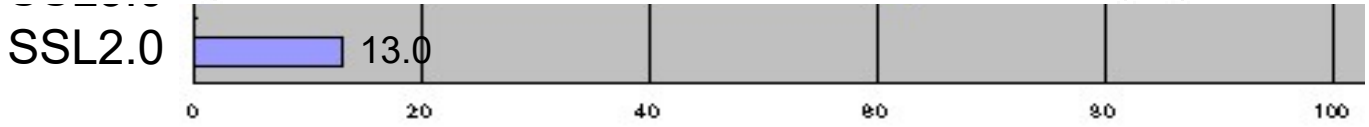
- Alexa提供のリストから抽出
  - α）.jp ドメイン**17988** サイト
  - β）Alexa top sites の上位**20000** サイト
- クローリング 2015年6月27日から28日

- 最終的にSSL-enable サイトは
  - α）.jp ドメイン5518 サイト
  - β）Alexa top sites 6431 サイト

SSL/TLSサーバのバージョン移行状況

version	2014-04-27	2014-11-26	2015-01-07	2015-06-27
SSL2.0	24.08	12.91	12.12	09.30
SSL3.0	99.91	62.32	57.44	49.89
TLS1.0	99.86	98.84	98.63	99.64
TLS1.1	15.61	27.27	28.94	36.96
TLS1.2	17.86	29.98	31.67	40.36

表 2: SSL/TLS バージョン対応状況 - (α) .jp ドメイン



Alexa top 100M sites に記載されている .jp ドメイン17988サイトを調査
両日ともに同じURLリストを利用

Alexa Top sites の結果

version	2014-04-27	2014-11-26	2015-01-07	2015-06-27
SSL2.0	05.23	01.73	01.62	01.23
SSL3.0	98.57	37.42	33.78	23.67
TLS1.0	99.48	99.69	99.75	99.39
TLS1.1	56.66	72.66	74.46	80.83
TLS1.2	60.66	76.42	78.37	83.98

表 3: SSL/TLS バージョン対応状況 - (β) Alexa top sites

Export-grade暗号の利用状況

6431　　5518

サーバリスト種別 / 観測日	(α) Alexa top sites 2015-01-07	(α) Alexa top sites 2015-06-27	(β) .jp ドメイン 2015-01-07	(β) .jp ドメイン 2015-06-27
EXP-RC2-CBC-MD5	756	230	1414	932
EXP-RC4-MD5	802	251	1437	962
EXP-EDH-RSA-DES-CBC-SHA	182	96	1128	779
EXP-EDH-DSS-DES-CBC-SHA	0	0	0	0
EXP-DES-CBC-SHA	771	229	1293	853
EXP-RC2-CBC-MD5	756	230	1414	932
EXP-RC4-MD5	802	251	1437	962
(40 ビット暗号アルゴリズム総計)	808	255	1444	970
DES-CBC-SHA	943	709	2648	2267
DES-CBC-MD5	122	71	682	509
EDH-RSA-DES-CBC-SHA	408	276	2277	1960
(56bits 暗号アルゴリズム総計)	947	711	2648	2268

表 1: Export-grade な暗号アルゴリズムの SSL/TLS サーバにおける対応状況

2016年3月

DROWN attack

- そもそも SSLv2やExport-grade の暗号アルゴリズムの利用は危険であるという認識
- 今回，現在安全と認識されている 128ビット以上の鍵長を持つ共通鍵暗号アルゴリズムを用いて暗号化した場合でも解読可能
- 攻撃条件
  - 中間者攻撃が可能な環境であること
    （攻撃対象となる暗号化通信を観測できること）
  - その暗号化通信に用いられたRSA鍵ペアを利用して運用されており、**かつ SSL2.0** が利用可能なSSLサーバにアクセスできること

ここまでのサーマリ
（小難しいこと考えなければこんな感じ）

- どうせSSL2.0使ってたって40ビット暗号使ってたって，最新のブラウザにしとけば，そんな危ないの選択されることないし大丈夫っしょ！

- もはやSSL/TLSサーバはその組織体の「顔」なんだから，キレイにしときなよ．減るもんじゃないし．ただしSSL3.0は微妙．
  - Thanks to mixi吉野さん（Janogサーバはキレイ）

今回

再々調査

2016年10月に再調査

- Alexa提供のリストから抽出
  - α）.jp ドメイン17988 サイト
  - β）Alexa top sites の上位20000 サイト
- クローリング 2016年10月24日から25日

- 最終的にSSL-enable サイトは
  - α）.jp ドメイン~~5518~~ **5407** サイト
  - β）Alexa top sites ~~6131~~ **6265** サイト

α）.jp ドメイン17988 サイト

version	2014-04-27	2014-11-26	2015-01-07	2015-06-27	2016-10-24
SSL2.0	24.08	12.91	12.12	09.30	04.2
SSL3.0	99.91	62.32	57.44	49.89	30.6
TLS1.0	99.86	98.84	98.63	99.64	99.2
TLS1.1	15.61	27.27	28.94	36.96	62.8
TLS1.2	17.86	29.98	31.67	40.36	65.9

表 2: SSL/TLS バージョン対応状況 - (α) .jp ドメイン

β）Alexa top sites の上位20000 サイト

version	2014-04-27	2014-11-26	2015-01-07	2015-06-27	2016-10-24
SSL2.0	05.23	01.73	01.62	01.23	00.4
SSL3.0	98.57	37.42	33.78	23.67	09.3
TLS1.0	99.48	99.69	99.75	99.39	97.1
TLS1.1	56.66	72.66	74.46	80.83	90.8
TLS1.2	60.66	76.42	78.37	83.98	93.4

表 3: SSL/TLS バージョン対応状況 - (β) Alexa top sites

β）Alexa top sites の上位20000 サイト

JPドメインサイトの対応状況は芳しくない

version	2014-04-27	2014-11-26	2015-01-07	2(JP	2016-10-24
SSL2.0	05.23	01.73	01.62	04.2	00.4
SSL3.0	98.57	37.42	33.78	30.6	09.3
TLS1.0	99.48	99.69	99.75	99.2	97.1
TLS1.1	56.66	72.66	74.46	62.8	90.8
TLS1.2	60.66	76.42	78.37	65.9	93.4

表 3: SSL/TLS バージョン対応状況 - (β) Alexa top sites

Export-grade暗号の利用状況

6431

~~5518~~ 5407

サーバリスト種別	(α) Alexa top sites		(β) .jp ドメイン	
観測日	2015-01-07	2015-06-27	2015-01-07	2015-06-27
EXP-RC2-CBC-MD5				932
EXP-RC4-MD5				962
EXP-EDH-RSA-DES-				779
EXP-EDH-DSS-DES-CBC-SHA	0	0	0	0
EXP-DES-CBC-SHA	771	229	1293	853
EXP-RC2-CBC-MD5	756	230	1411	932
EXP-RC4-MD5	802	251	1437	962
(40 ビット暗号アルゴリズム総計)	808	255	1444	970
DES-CBC-SHA	943	709	2648	2267
DES-CBC-MD5	122	71	682	509
EDH-RSA-DES-CBC-SHA	408	276	2277	1960
(56bits 暗号アルゴリズム総計)	947	711	2648	2268

仮調査した状態だが
まだまだ多くのサイトがダメな状況

2016-10-24

475

1609

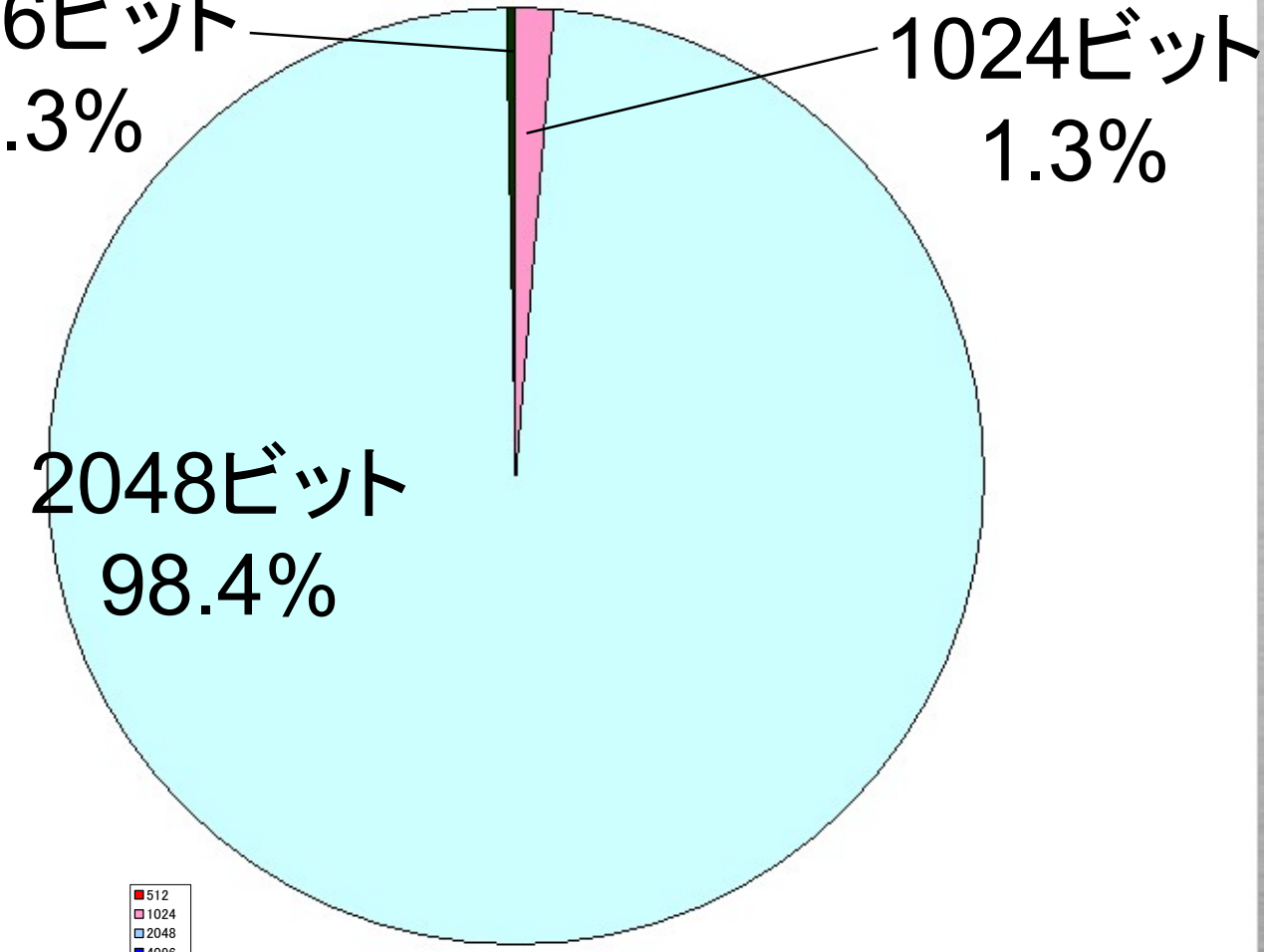
220

1416

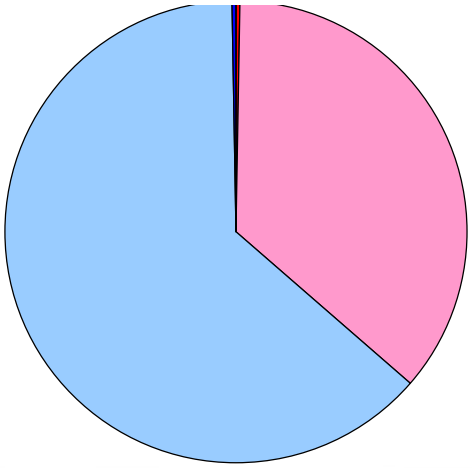
1609

表 1: Export-grade な暗号アルゴリズムの SSL/TLS サーバにおける対応状況

JPサイト:RSA鍵長の割合



参考データ
2012年5月（地方自治体サーバの調査）



4096ビットRSA利用サイトの例

4096ビットはオーバースペックだが
ちゃんと運用されているケースもあり

1024ビットRSA利用サイト

ちゃんと使っているところでも…

昔の証明書が残ったままに…

10年以上前のオレオレ証明書が今でも観測されている

今回…

再々調査&

追加調査

※ 次ページのBGMはこれ： http://commons.nicovideo.jp/material/nc148600

こんな再調査、しなければよかった

予測（期待を込めて）

- 一般的なJPサイトに比べれば きっと
  「いい設定」がされているのではないか？

具体的事例紹介

- EVSSL**2**証明書
  - EVSSL証明書なのに
- リダイレクト残念系
  - HTTP→HTTPSなのに
- 検索窓問題
  - 自身の能力を発揮できずにいるサーバ証明書

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,EV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

SOUPS 2016

usenix

Twelfth Symposium On Usable Privacy and Security

JUNE 22–24, 2016 • DENVER, CO

実は，この論文が大きな影響を与えている

usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

Rethinking Connection Security Indicators

Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, and Max Walker, *Google;*
Christopher Thompson, *University of California, Berkeley;* Mustafa Embre Acer,
Elisabeth Morant, and Sunny Consolvo, *Google*

概要（かなり意訳）

- Google提供ブラウザChromeのセキュリティインディケータの再考.
  

  - 表記上のミスリードを避けたい
- 1300を超えるユーザにアンケート
  - 40種の表記方法に関してどう感じ取るか調査
    - 40 = 8型×5色
- 最終的によさげな3つを選択しChrome実装にバージョン53以降に反映予定
  - （12月に54でアイコンだけ採用，55で文言も）
  - 他のブラウザも我々と同様に変えてみたら？

インディケータの種類（2つの大分類）

- Connection security
  - Valid HTTPS
  - HTTPS with minor errors
    - HTMLコンテンツにHTTPで指し示された画像がある等
  - HTTPS with major errors
    - 証明書チェーンが辿れない
  - HTTP
- Website trustworthiness
  - EV（Extended Validation）HTTPS
  - Malware and phishing
    - ブラックリストで検知（Google Safe Browsing, M$ SmartScreen）
    - HTTPSだったとしても安全ではない（←信頼できない）

Chrome48時代のインディケータ

Browser	HTTPS	HTTPS minor error	HTTPS major error	HTTP	EV	Malware
Chrome 48 Win	https://www	https://mixe	https://wro	www.examp	Symantec Co	https://dow
Edge 20 Win	example.	https://mix	wrong.host.badss	example.com	Symantec Co	Unsafe website den
Firefox 44 Win	https://www.e	https://mixed	https://expire	www.example	Symantec Corpo	https://spacet
Safari 9 Mac	example.com	mixed.badssl.c	*URL hidden*	example.com	Symantec Cor	downloadgam
Chrome 48 And	https://v	https://mixe	https://v	www.examp	https://v	https://spac
Opera Mini 14 And	www.examp	mixed.badssl.(	wrong.host.ba	www.example	www.syma	*Unavailable*
UC Mini 10 And	Example D	mixed.badss	*Blocked*	Example D	Endpoint, C	*Blocked*
UC Browser 2 iOS	Example Do.	mixed.badss..	wrong.host..	Example Do.	Endpoint, C.	*Unavailable*
Safari 9 iOS	example.c	mixed.badss	wrong.host	example.com	Symantec	*Unavailable*

UC Mini and UC Browser (http://www.ucweb.com/company/about/)

アイコン セレクション

Secure connection.

- Colorblindでも判断できるべき
- 鍵マークがよいという結果を従来研究の引用

Insecure connection.

- 色によらずよい結果がでてる

Slightly insecure connection.

- Negativeグループから選択はするけれど，とても危ないというイメージではいけない
- ISOシンボルの「Information」に似てる

Mixed Contents に関する指針

- Firefox：2013年4月(ff23)からブロック開始
  - https://support.mozilla.org/ja/kb/mixed-content-blocking-firefox
  - https://blog.mozilla.org/tanvi/2013/04/10/mixed-content-blocking-enabled-in-firefox-23/
- Chrome: 直し方指南書公開済
  - https://developers.google.com/web/fundamentals/security/prevent-mixed-content/what-is-mixed-content
  - https://developers.google.com/web/fundamentals/security/prevent-mixed-content/fixing-mixed-content

安全なウェブサイトの作り方 改訂第7版 https://www.ipa.go.jp/files/000017316.pdf

検索窓問題

このEVSSL証明書は泣いている

SHA-1利用で署名した証明書に対する挙動の変化

- **SHA1 & Google Chrome Checker**
  - http://sha1affected.com/

Results for [redacted]

The certificates for [redacted] will be affected by Google Chrome's SHA1 deprecation policy.

Chrome 39	Chrome 40	Chrome 41+
November 2014	January 2015	April 2015
https://www.	https://www.	https://www.

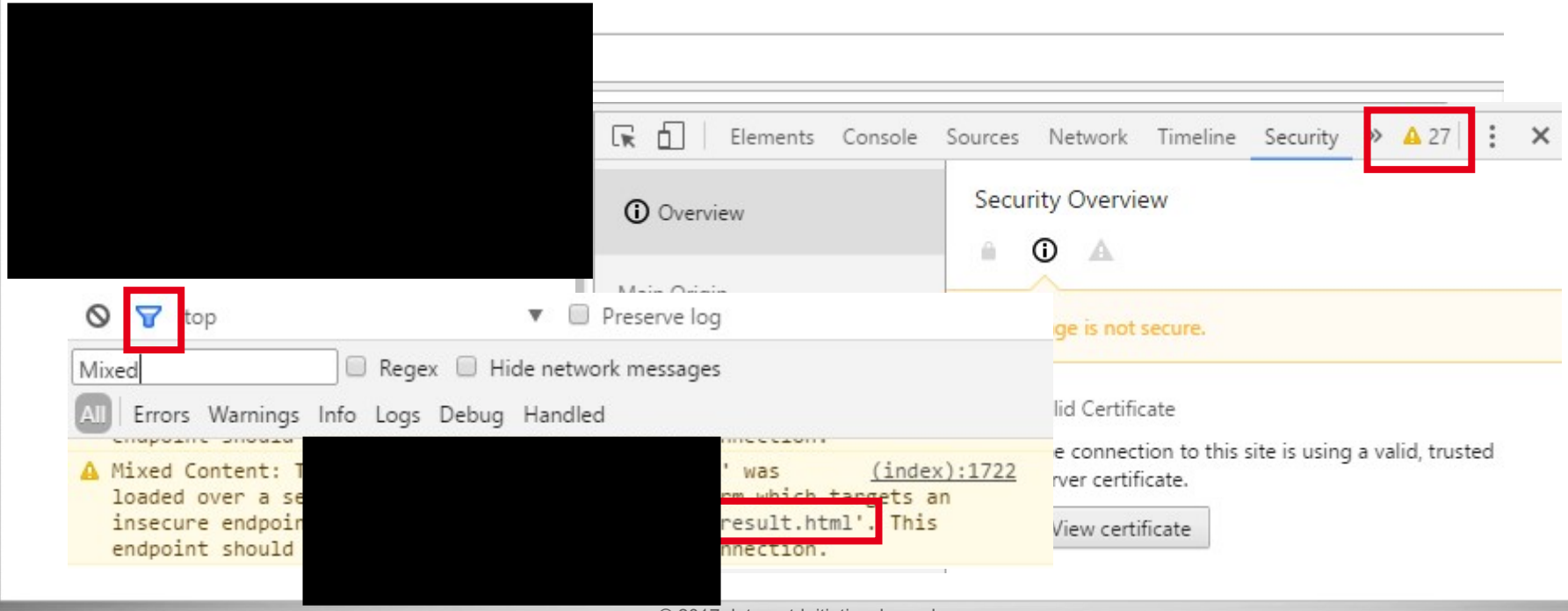
Certificate Summary

Type	Valid For	Expiry Date	Signature Algorithm
End Identity	[redacted]		
Intermediate			
Root			

自分のところを確認してみよう

Chromeでの調査手順

- ググって当該サイトを表示
- セキュリティインディケータを押下
- ページエラー ⚠ の中から “Mixed”でフィルタ



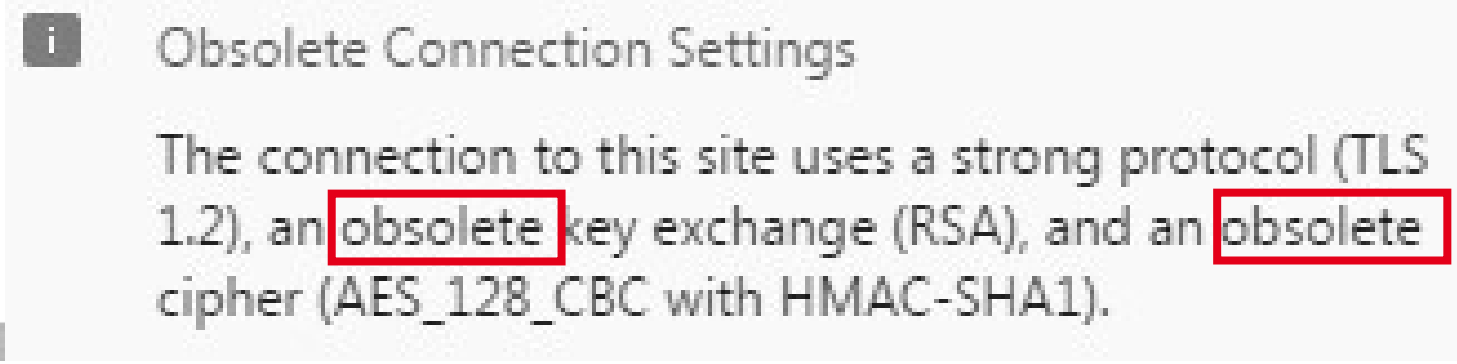
日常生活においても

- 「どうやって金沢来たの？」
- [redacted]はどこの業者さん？

まとめ

やらないといけないこと（私見）

- バンキングサイト（ID/PASS入力）とは別FQDNであることが多い→飛んだ先での再調査
- .jsファイルのレンダリング（誤検知）
  - httpとhttpsでは異なるコンテンツを用意してる？
- 調査の自動化
- Chrome判断の暗号アルゴリズム強度の可否
  - Googleさんに判断を任せていいの？



皆さんと一緒に考えたいこと

- どういうWebページ設計ならうまくいくのか？
  - 知見・ベストプラクティスの共有
- 常時SSL化時代に突入した場合に起きそうな問題を事前に予見できるか？
  - HTTPサイトのブラウザでの見え方
- ブラウザ以外のU/Iでも同様の問題は生じえるか？
  - 証明書の価値とサイトのレピュテーション
    - Let’s Encrypt証明書 v.s. EVSSL証明書

SSL/TLSサーバ設計の「一般論」例

- HTTP(→HTTPS)フォームは使わない

1)
☞ 重要な情報を取り扱うウェブページでは、通信経路を暗号化する

ウェブサイトで通信を暗号化する手段として、SSL(Secure Socket Layer)や TLS(Transport Layer Security)を用いた HTTPS 通信があります。パスワードでログインするページや、個人情報を登録するページ、また、秘密にするべき情報を表示する画面のページは、https:// で始まる URL として、通信経路を暗号化することをお勧めします。

暗号化したい情報を入力させる画面では、送信先の URL を https:// とするだけでなく、入力画面も https:// の URL としておく必要があります。そうしなければ、入力画面が盗聴者に改ざんされている可能性があり、利用者が改ざんに気づかずに入力すれば、差し替えられた別のサイトに送信されてしまったり、暗号化されずに送信されて盗聴される危険があるからです。利用者は入力画面が https:// になっていることを確認してから入力しますので、ウェブサイト運営者は、そのような確認ができるようにしてください。

安全なウェブサイトの作り方 改訂第7版 https://www.ipa.go.jp/files/000017316.pdf

設定に関する思想

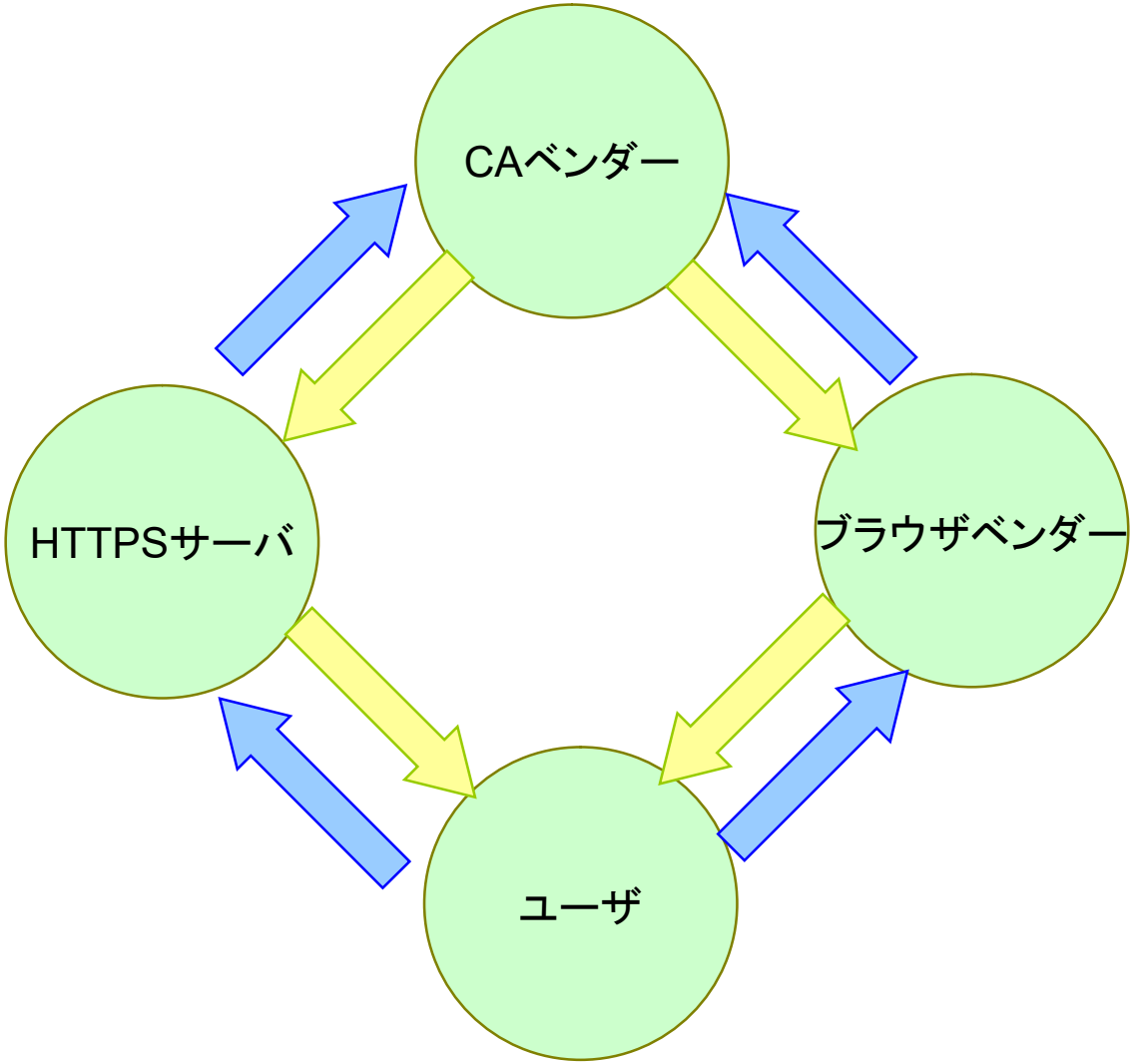
- 後方互換性の確保：SSL/TLSバージョン
  - 機会損失とのせめぎ合い（〇〇サイトがその一例）
- 暗号アルゴリズム：Qualys等テストサイト
  - リスク受容しているケースをどう考えるか
- リダイレクト
  - HTTP→HTTPS　常時SSL時代，HSTS利用
  - HTTPS→HTTP　Webサイト負荷軽減

HSTS（HTTP Strict Transport Security）：2012 年に RFC 6797 で策定済

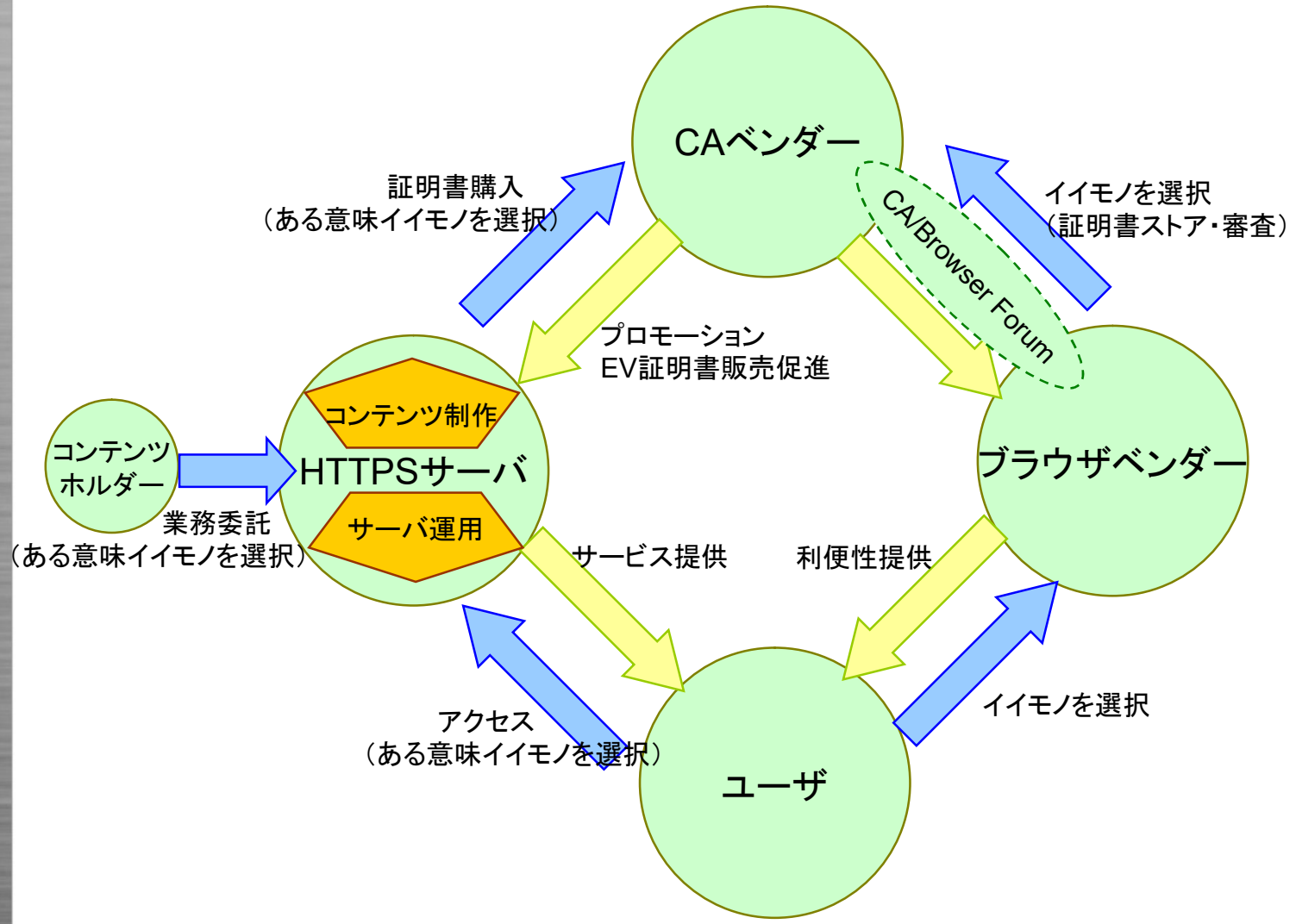
信頼に関する思想

- サーバ証明書の格差拡大
  - どうせ同じように見えるなら… コスト重視？
  - CAベンダー選定はどのようにすべきか
    - 微妙にOSごとに証明書ストアが異なる点も配慮
- とても小さな U/I しか持たないIoT製品
  - EVSSL証明書利用サイトのスマホでの表記

ステークホルダーの関係



サーバ運用時のカバレッジ問題？



そのほか

設定に関するTIPS

- CRYPTREC,SSL/TLS 暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～
  - https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html
- Mozilla, “Security/Server Side TLS”
  - https://wiki.mozilla.org/Security/Server_Side_TLS
- [Renegotiation対策]と[圧縮機能無効化]

暗号プロトコル課題検討WG

https://www.cryptrec.go.jp/report/c15_prom_web.pdf

- CRYPTREC Report 2015
  - 暗号技術活用委員会報告

4. 2016 年度活動計画について

4.1 暗号技術活用委員会の活動計画について

「CRYPTREC 暗号技術活用委員会の今後の活動に向けて（第 2 回重点課題検討タスクフォースでの議題）」のうち、重点課題検討タスクフォースにて決定された活動方針を基に、2016 年度活動計画を定めた。

⑥ その他

必要に応じて、暗号技術活用委員会として検討テーマを新たに設けることがある。2016 年度は、 CRYPTREC として暗号プロトコルをどのように扱うかを重点的に検討するため、「暗号プロトコル課題検討 WG」を設置する。

情報共有・意見交換の場として

CELLOS

Cryptographic protocol Evaluation toward
Long-Lived Outstanding Security

- 暗号プロトコル評価技術コンソーシアム
  - セキュアプロトコルに関わる脆弱性のピックアップ
  - ショートサーマリ・速報の発行
    - 要因の精査（実装 or 仕様そのもの），対策方法
  - より踏み込んだディスカッション
    - 報告書の発行

https://www.cellos-consortium.org/

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

お問い合わせ先 IIJインフォメーションセンター
TEL 03-5205-4466（9:30～17:30 土/日/祝日除く）
info@iij.ad.jp
http://www.iij.ad.jp/