

Internet Week 2014

サイト管理者が知っておくべきSSLの秘孔(ツボ)

SSL/TLSで使われる 暗号技術のキモチ

菅野 哲(かんの さとる)

NTTソフトウェア株式会社

2014年11月20日

この人は誰？

- **名前**

- 菅野 哲 (かんの さとる)

- **所属**

- NTTソフトウェア 株式会社

- セキュリティ事業部

- 人事部 人材開発部門 兼務

- マーケティングやプロモーションも...

- **その他の所属**

- ISOC Japan Chapter (Program Committee)

- MIT-KIT Japan Chapter (窓口？)

本講演の目的

- 日頃のサーバ管理でギモンに思っていることを解消するためのきっかけに！
 - 暗号って種類が多くて面倒ですよ？
 - なぜこの設定なのか？判断する足掛かりがほしい
 - 専門用語が意味わからない・・・

日頃のギモンとして...

安全な暗号って？

暗号って
どれもいっしょでしょ？

脆弱性対応って？

危殆化対策？



〇〇ビット
セキュリティ？

みんなのSSL/TLSと脅威

SSL/TLSが利用されるまで様々な工程がある

現実的なもの

サービス／システム

実装物の
バグ

暗号製品



仕様上の
欠陥

SSL/TLSプロトコル



暗号技術

危殆化



理想的なもの

SSL/TLSにおける暗号技術

- 認証や経路上を暗号化するために、複数の暗号技術を組合せで実現

➤ **Ciphersuite**で組合せがわかる！

具体例：

0x00,0xBA	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	Y	[RFC5932]
0x00,0xBB	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256	Y	[RFC5932]
0x00,0xBC	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256	Y	[RFC5932]
0x00,0xBD	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256	Y	[RFC5932]
0x00,0xBE	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	Y	[RFC5932]
0x00,0xBF	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xC0	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xC1	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xC2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xC3	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xC4	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xC5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xC6	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xC7	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xC8	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xC9	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xCA	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xCB	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xCC	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xCD	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xCE	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x00,0xCF	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0x01-BF,*	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	Y	[RFC5932]
0xC0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA	Y	[RFC4492]
0xC0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	N	[RFC4492][RFC6347]
0xC0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	Y	[RFC4492]
0xC0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	Y	[RFC4492]
0xC0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	Y	[RFC4492]

鍵交換

暗号利用モード

TLS **DHE** **RSA** WITH **CAMELLIA_256** **CBC** **SHA256**

認証

共通鍵

MAC

SSL/TLSで利用してる暗号技術：公開鍵暗号

- **どんな特徴？**
 - 異なる一対の鍵を駆使して暗号化／復号（または、署名／検証）を行う
 - 公開できる鍵がある
 - 処理速度は低速
- **SSL/TLSでは何が使えるの？**
 - 鍵交換
 - RSA, DH, ECDH
 - 認証
 - RSA, ECDSA
- **安全性を考えるときの着眼点**
 - 十分な鍵長かどうか？

SSL/TLSで利用してる暗号技術：共通鍵暗号

- **どんな特徴？**
 - 共通な鍵を用いて暗号化／復号を行う
 - 処理処理は高速
- **SSL/TLSでは何が使えるの？**
 - 共通鍵暗号
 - DES, 3DES, AES, Camelliaなど
 - 暗号利用モード
 - CBC, GCMなど
- **安全性を考えるとときの着眼点！**
 - 危殆化したアルゴリズムじゃないか？
 - 十分な鍵長かどうか？

SSL/TLSで利用してる暗号技術: ハッシュ関数

- **どんな特徴？**

- 任意の長さを固定長のデータに変換できる
- MACやデジタル署名に利用する

- **SSL/TLSでは何が使えるの？**

- MD5, SHA-1, SHA-256など

- **安全性を考えるときの着眼点！**

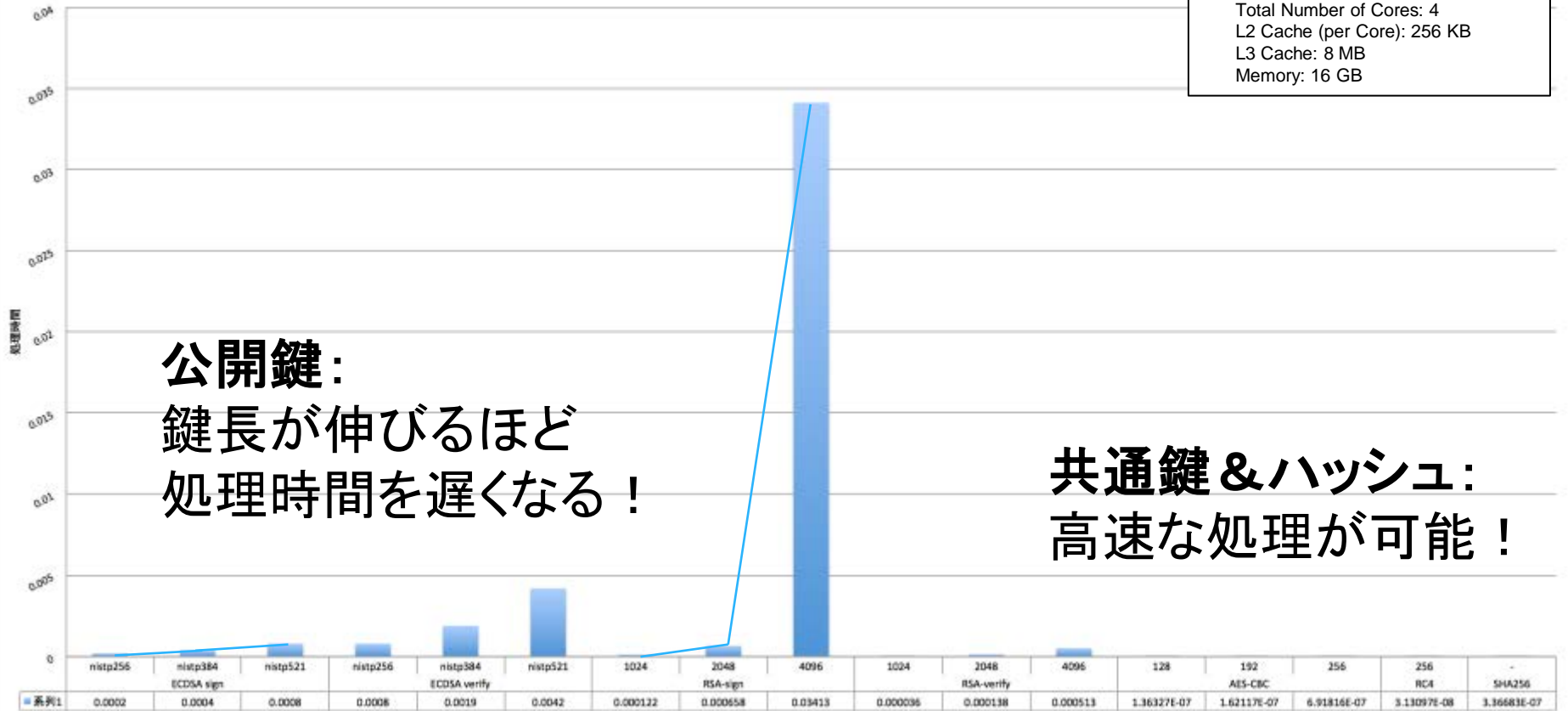
- 危殆化しているアルゴリズムを利用していないか？
- どんな用途で使うのか？
 - デジタル署名？ HMAC？

性能で見るSSL/TLSで利用される暗号技術

測定環境:

Model Name: MacBook Pro
 Model Identifier: MacBookPro10,1
 Processor Name: Intel Core i7
 Processor Speed: 2.7 GHz
 Number of Processors: 1
 Total Number of Cores: 4
 L2 Cache (per Core): 256 KB
 L3 Cache: 8 MB
 Memory: 16 GB

OpenSSL 1.0.1j 性能測定 (各アルゴリズム)



公開鍵:
 鍵長が伸びるほど
 処理時間を遅くなる！

共通鍵 & ハッシュ:
 高速な処理が可能！

公開鍵暗号

共通鍵 & ハッシュ

暗号技術の安全性: 鍵長的な側面(1/2)

- 「RSA-1024はAES-128 はどっちが安全？」という質問をよく受ける...

ECDH-P256 ECDSA-P521
Camellia-256 SHA-256
RSA-1024 AES-128 DH-1024

疑問!

異なる鍵長をどう判断するの？

「等価安全性」という概念!

暗号技術の安全性: 鍵長的な側面 (2/2)

- 等価安全性とは？

- 異なる種類の暗号技術に対して、
同一の評価尺度で安全性を表したもの

- 例: 80 bit セキュリティ

- 解読に必要な計算量が 2^{80} 乗相当である

・・・と言われても・・・わかりにくし
どうやって判定するの??

等価安全性に関するお助けサイト



In most cryptographic functions, the key length is an important security parameter. Both academic and private organizations provide recommendations and mathematical formulas to approximate the minimum key size requirement for security. Despite the availability of these publications, choosing an appropriate key size to protect your system from attacks remains a headache as you need to read and understand all these papers.

This web site implements mathematical formulas and summarizes reports from well-known organizations allowing you to quickly evaluate the minimum security requirements for your system. You can also easily compare all these techniques and find the appropriate key length for your desired level of protection. The lengths provided here are designed to resist mathematic attacks; they do not take algorithmic attacks, hardware flaws, etc. into account.



Choose a Method

- Lenstra and Verheul Equations (2000)
- Lenstra Updated Equations (2004)
- ECRYPT II Recommendations (2012)
- NIST Recommendations (2012)
- ANSSI Recommendations (2010)
- Fact Sheet NSA Suite B Cryptography (2013)
- Network Working Group RFC3766 (2004)
- BSI Recommendations (2014)

Compare all Methods

Date	Minimum of Strength	Symmetric Algorithms	Asymmetric	Discrete Logarithm Key	Elliptic Curve Group	Elliptic Curve	Hash (A)	Hash (B)
2010 (Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1** SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
2011 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
> 2030	128	AES-128	3072	256	3072	256	SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
>> 2030	192	AES-192	7680	384	7680	384	SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512
>>> 2030	256	AES-256	15360	512	15360	512	SHA-512	SHA-256 SHA-384 SHA-512

This kind authorization and comments.
to Law Survey / Digital Signature Law Survey.
Copyright | Release Notes

<http://www.keylength.com/>

危殆化対策

- 危殆化とは

- 当初期待していた安全性を担保できない状態になっていること



でも、忙しくてそんな情報を収集してられないよ・・・

危殆化対策を行う際の情報源

- 正直，日々の運用を実施していると暗号アルゴリズムやプロトコルの状況監視している余裕がない...



暗号アルゴリズムと暗号プロトコルに関する監視／評価している組織があり，信頼のおける情報を発信している

暗号アルゴリズム

CRYPTREC

暗号プロトコル

CELLOS

暗号アルゴリズムに関する有益な情報

- 日本にはCRYPTRECという暗号技術の評価／監視している組織がある

<http://www.cryptrec.go.jp/>



安全なアルゴリズム

危険なアルゴリズム

暗号プロトコルに関する有益な情報

- 信頼できるプロトコルに関する脆弱性情報などを公開してくれるサイトってないの？

Cryptographic protocol Evaluation toward Long-Lived Outstanding Security Consortium



CELLOS

Cryptographic protocol Evaluation toward Long-Lived Outstanding Security

HOME 概要 体制 公開情報 調査対象 関連サイト English

HOME

CELLOSとは
What's New!

概要

活動内容
発起人

体制

構成
規約
役員
会員

公開情報

連絡
報告書
Protocol zoo

調査対象

イベント
アーティクル

関連サイト

FrontPage

HOME

CELLOSとは

暗号プロトコル評価技術コンソーシアム(Cryptographic protocol Evaluation toward Long-Lived Outstanding Security (CELLOS) Consortium)について紹介します。

近年のネットワークの発展は、単なるコミュニケーション促進だけでなく、モバイルネットワークやクラウドコンピューティングなど、我々の生活の向上に向けて、新たな情報通信の可能性を開こうとしています。この新たな情報通信の可能性に併せて、プライバシー保護など、高度な安全性が要求されるようになっており、単に通信内容の暗号化や認証を行うだけでは不十分となっています。

それに対して、暗号化や認証を始め、多種多様な暗号技術を組み合わせた「暗号プロトコル」が精力的に研究開発され、現在400を超える暗号プロトコルが国際標準化されています。しかし、無線LAN用暗号プロトコルWEPに次々と脆弱性が発見されるなど、これらの暗号プロトコルが現実のICTシステムに用いた高度な安全性を実現していることの評価は、これまで十分に行われていませんでした。とりわけ、世界レベルかつ最新の安全性情報を集約し、専門家による議論を促す、幅広く技術的に詳細な安全性情報を社会に公開する活動は、これまで国際的に見てもありませんでした。一方で、日本は、ISO/IECにおいて主導的に安全性評価指標の標

本コンソーシアムは、このような活動を通じ、ネットワークセキュリティの向上に大きく貢献し、今後のネットワーク利用の安心・安全に繋がるよう先導的かつ主導的役割を果たしていきます。

What's New!

- [2014年10月15日] SSLv3仕様そのものに対する POODLE attack について
- [2014年8月08日] Black Hat 2014 USAで発表されたSSL/TLSへの複数の新たな攻撃手法について
- [2014年6月06日] OpenSSLに関する7つの問題点とその対策について
- [2014年6月05日] GnuTLSの暗号ライブラリにおける問題について
- [2014年4月18日] OpenSSLにおける Heartbleed Bugと呼ばれる脆弱性について
- [2014年3月13日] TLSに関する新たな攻撃の報告
- [2013年12月06日] 設立総会開催

暗号プロトコルの
脆弱性の解説を公開！

<https://www.cellos-consortium.org/jp/>

Copyright(c) 2014 NTT Software Corporation. All rights reserved.

SSL/TLSにおける禁じ手？

- CRYPTRECやCELLOSで情報監視していれば万全なの？



SSL/TLSの利用の観点からだと不十分・・・

過去の遺産三兄弟



古い環境だと**デフォルト**で**ON**になっている

知っていると便利かもしれない情報

自分のサーバ設定を確かめるには・・・？

- **QUALYS SSL LABS**

The screenshot shows the Qualys SSL Labs website. At the top, there is a red navigation bar with the logo and the text "QUALYS SSL LABS". To the right of the logo are links for "Home", "Projects", "Qualys.com", and "Contact". Below the navigation bar, the breadcrumb "You are here: Home > Projects > SSL Server Test" is visible. The main heading is "SSL Server Test". A paragraph of text explains the service: "This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used for the test results, and we never will." A blue callout box with white text says "調査したいサーバを入力！" (Enter the server you want to investigate!). Below this is a form with a "Domain name:" label, a text input field, and a "Submit" button. There is also a checkbox labeled "Do not show the results on the boards". At the bottom, there are three columns of results: "Recently Seen" (listing eu1.badoo.com, bancofalabella.cl, rp-l.com), "Recent Best" (listing meu1.badoo.com with grade A, authorize.net with grade A, owa.fondsfinanz.de with grade A-), and "Recent Worst" (listing mgi-aperio.myriad.com with grade F, imagepeaksystems.com with grade F, mail.downing-downing.com with grade F).

<https://www.ssllabs.com/ssltest/index.html>

手軽に調査できちゃう！

SSL Report: [google.co.jp](https://www.google.co.jp) (74.125.239.119)

Summary

Overall Rating



主要なブラウザとの
接続可能かも判定！

Visit our [documentation page](#) for more information, configuration, and more.

This server uses SSL 3, with POODLE mitigated. Still, it is not recommended to use SSL 3.

Certificate uses SHA1. When renewing, please use SHA256.

This server supports TLS_FALLBACK_SNI, which helps prevent downgrade attacks.

Handshake Simulation

Client	Protocol	Cipher Suite	Score
Android 2.3.7	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
Android 4.0.4	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Android 4.1.1	TLS 1.0	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) FS RC4	128
Android 4.2.2	TLS 1.0	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007) FS RC4	128
Android 4.3	TLS 1.0	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007) FS RC4	128
Android 4.4.2	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) FS	128
BingBot Dec 2013	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS	128
BingPreview Jun 2014	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
Chrome 37 / OS X R	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) FS	128
Firefox 24.2.0 ESR / Win 7	TLS 1.0	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007) FS RC4	128
Firefox 32 / OS X R	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) FS	128
Googlebot Jun 2014	TLS 1.0	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007) FS RC4	128
IE 6 / XP	SSL 3	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
IE 7 / Vista	TLS 1.0	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) FS	128
IE 8 / XP	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128

日頃のギモンが解決？！

安全な...って？

...って？
どれもいつ...でしょ？

脆弱性...って？

危殆化...対策？

...って？
セキュリティ？



まとめ

- Ciphersuiteの構成を読み解くことができる！
 - SSL/TLSで利用される暗号技術
- サーバ設定時に耳にする用語を把握した！
- デフォルト設定だと危険なことがある！という事実
- 安全にSSL/TLSを利用するには暗号～システム構築まで広い範囲で注意が必要！
- 情報収集に関する便利なサイト
 - ドンドン活用して負荷を軽減！

CONTACT

- **E-mail**

- kanno.satoru@po.ntts.co.jp

- **SNS**

- Twitter (satorukanno)

- Facebook (satoru.kanno)

- LinkedIn

お気軽にご連絡ください！