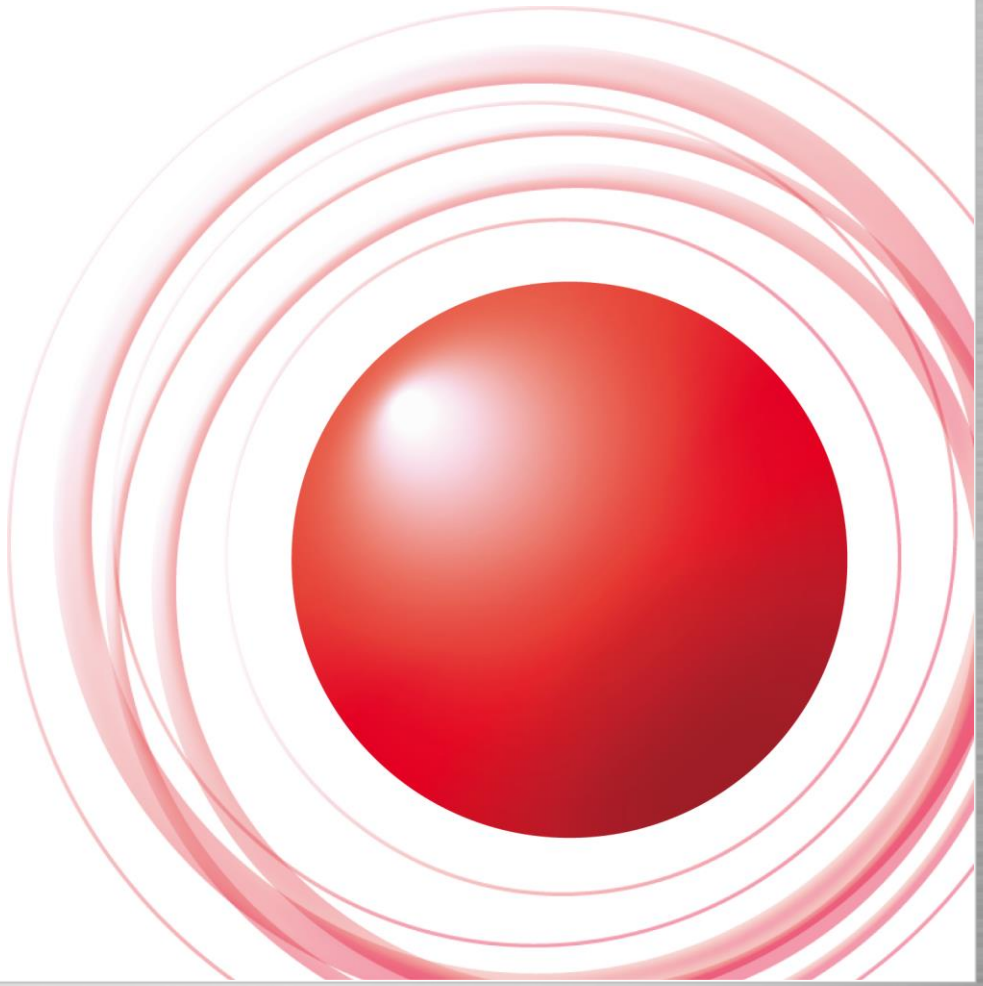
IIJ Technical WEEK 2014, November 27th, Iidabashi, Tokyo, Japan

セキュリティ動向2014 後編



株式会社インターネットイニシアティブ
セキュリティ情報統括室
須賀祐治
2014-11-27

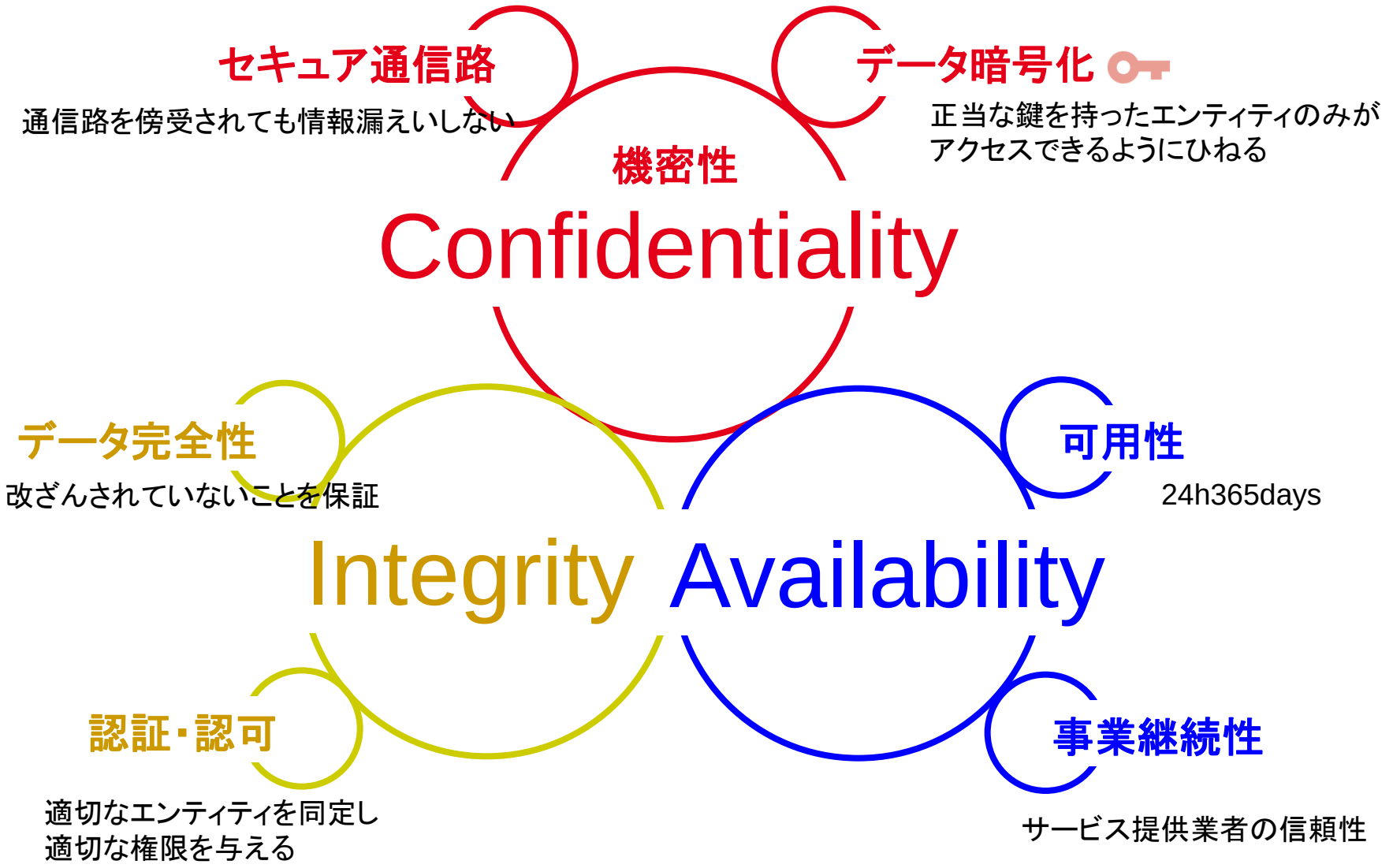
後編の概要

- 暗号技術に関わる脆弱性について紹介
- 「安全と思っていたけどそうじゃなかった」
  事例が今年も相変わらず多発した
- 脆弱性の影響と対策方法だけでなく…
- 何が本質的な問題なのか技術的な側面を
  (できるだけわかりやすく)解説したい

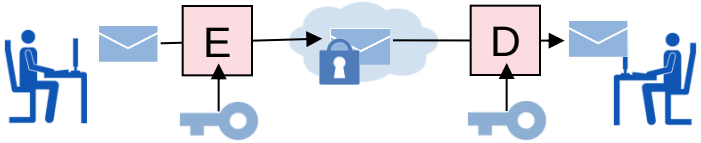
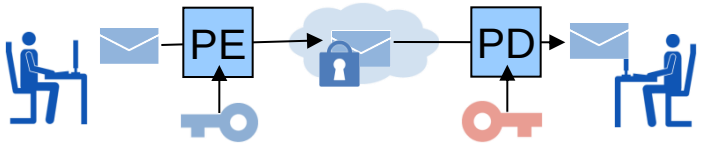
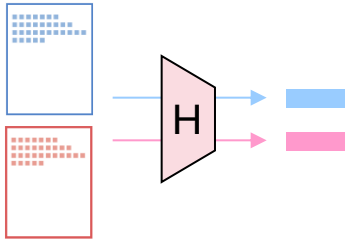
暗号技術に関わる最近の話題

- 2013年 3月/8月 RC4における複数の攻撃
- 2013年 6月 NSAによる諜報活動の報道
- 2013年 9月 Dual_EC_DRBG 問題
- 2013年11月 IETF-88 にてPervasive Surveillance（広域監視）がメイントピックに
- 2014年 4月 OpenSSLにHeartbleed 発覚
- 2014年 6月 OpenSSLにCCS Injection 発覚
- 2014年 9月 Mozilla NSSに署名検証不備の脆弱性
- 2014年10月 POODLE attack SSLv3仕様そのものの問題

一般的なセキュリティ要件



暗号アルゴリズムの分類

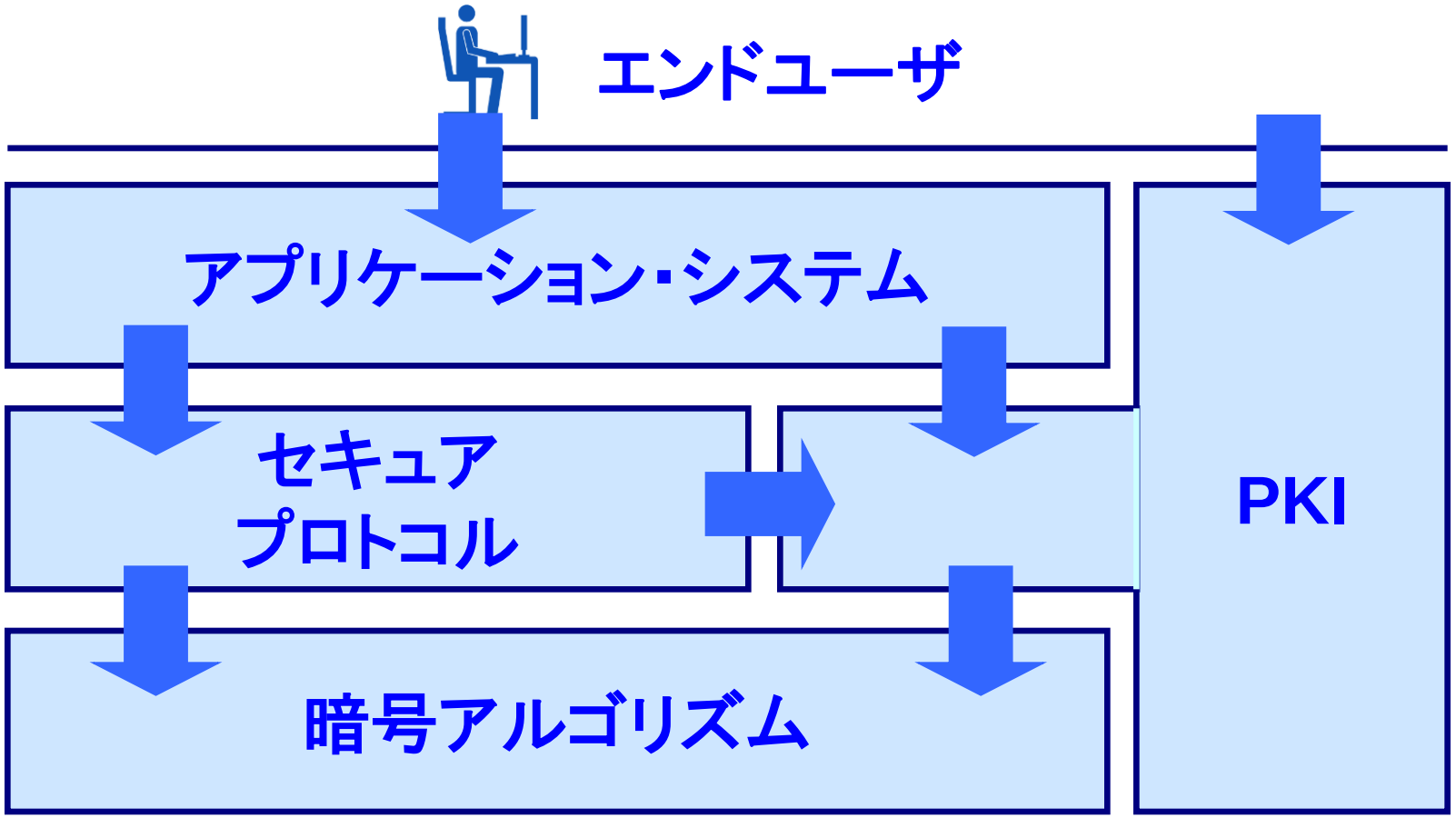
暗号プリミティブ	特徴・用途	アルゴリズム例
共通鍵暗号	暗号化と復号で同じ鍵を用いて秘匿 	ブロック暗号 AES, 3DES, Camellia ストリーム暗号 RC4, KCipher-2,ChaCha
公開鍵暗号 Confidentiality	対になる2つの鍵を用いて 守秘(暗号化)，署名，鍵共有 	素因数分解 RSA 離散対数 DSA，DH 楕円離散対数 ECDSA, ECDH
Integrity		
ハッシュ関数	衝突しない固定長データに圧縮  (デジタル署名 タイムスタンプ 等で利用)	専用(dedicated) 関数 MD5, SHA-1/SHA-256 ブロック暗号ベース ISO10118-2

暗号アルゴリズムの危殆化

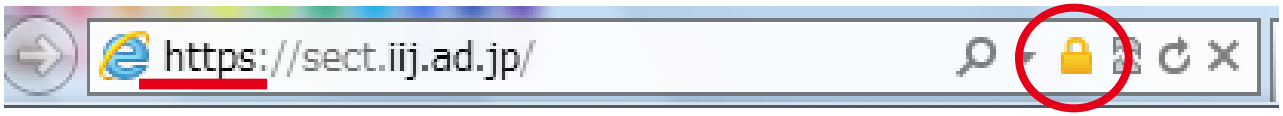
- アルゴリズム自体に欠陥が生じる問題
  - 設計当時は安全と思われていた
  - しかしアルゴリズムに内在していた欠陥が近年の暗号解析研究によって明らかになった「設計ミス」
- 対処方法：暗号アルゴリズムを差し替える
  - 移行コスト，社会的インパクトが大きい
    - 1976年に策定されたDESはTDES（Triple DES）として現在も使われており**2030年まで**利用を容認
  - 既に脆弱であると認識されているアルゴリズム
    - 共通鍵暗号：DES（, **RC4**）
    - ハッシュ関数：MD2, MD4, MD5（, **SHA-1**）

  - 広く使われていてもいずれは捨てる覚悟が必要

エンドユーザと「暗号技術」の距離



SSL/TLS概要



- アプリケーション層のデータにセキュアなチャネルを提供（暗号化・認証・データ完全性）

- Phase1: ハンドシェーク
  - 暗号アルゴリズムの決定
  - PKI経由でノード認証（通常はサーバ認証のみ）
  - 暗号化とデータ完全性保持のための鍵交換
- Phase2: アプリケーションレイヤのデータ送受信
  - 暗号化＋MAC（Message Authentication Code）

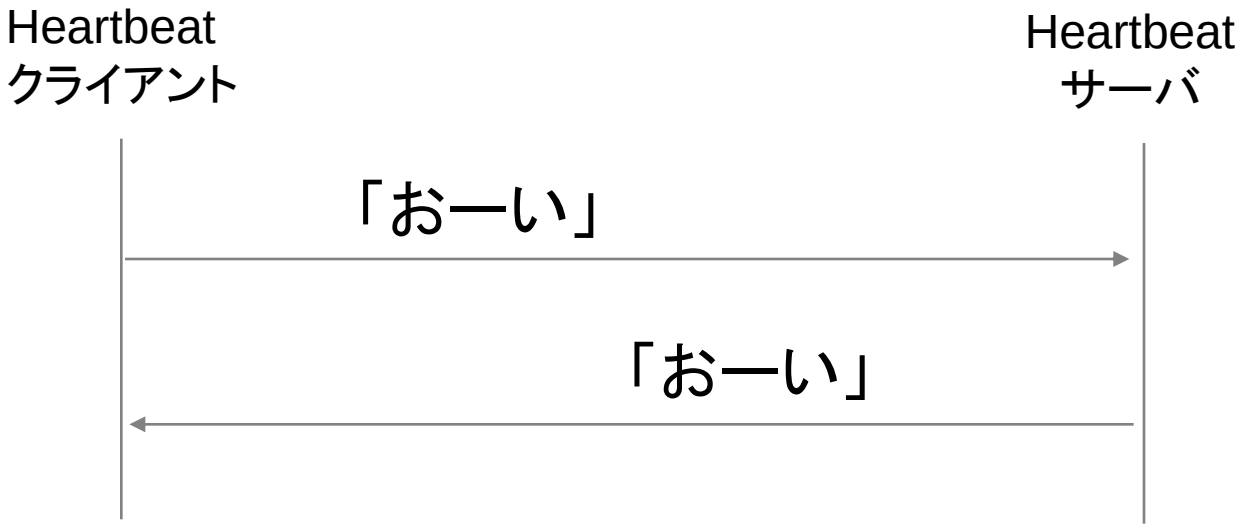
Heartbleed Bug 概要

2014年4月

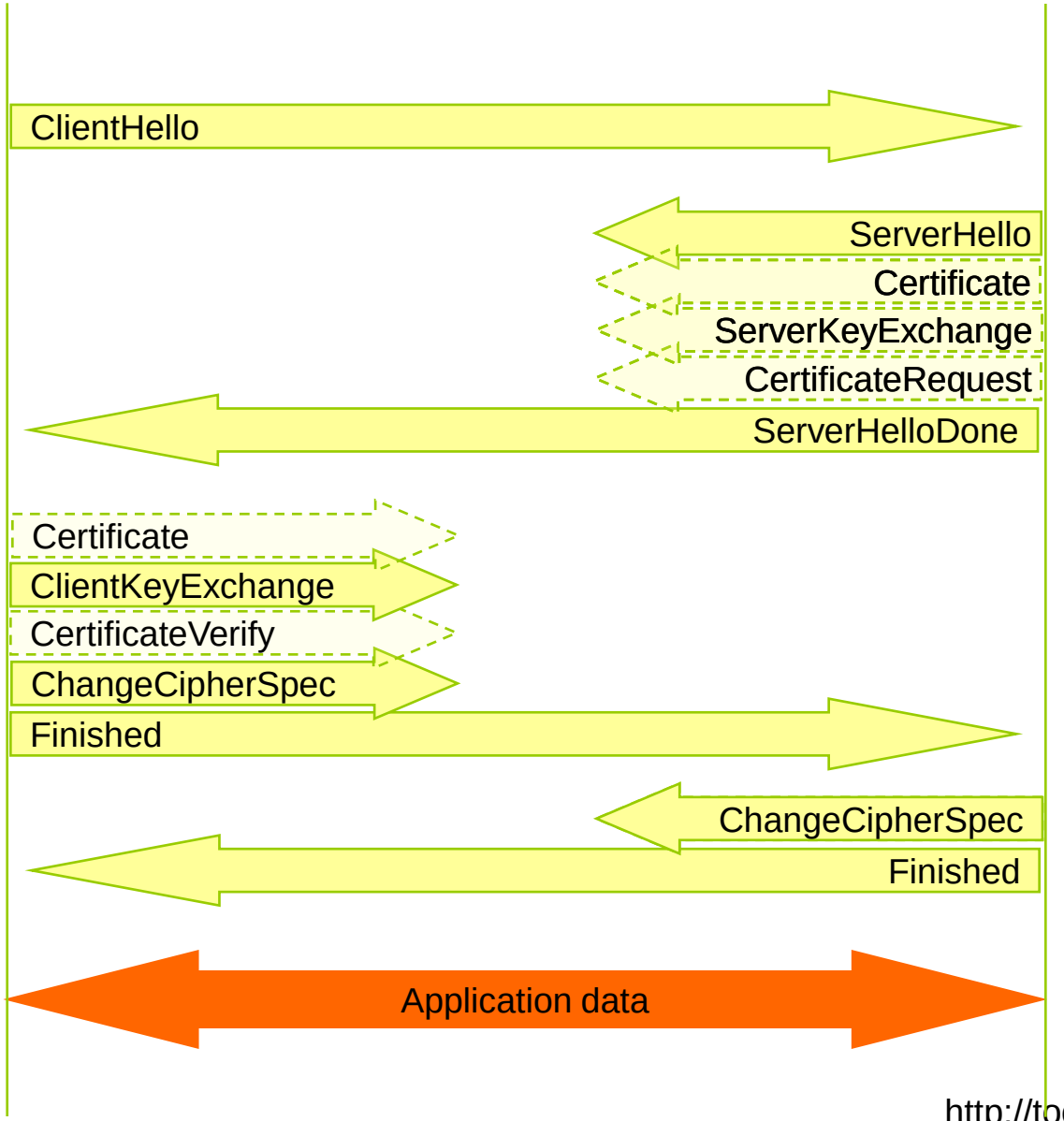
- CVE-2014-0160
- 日本時間4月8日未明に公開
  - http://heartbleed.com/
- 脆弱なバージョン：OpenSSL
  1.0.1 から 1.0.1f および 1.0.2beta1
- 問題：OpenSSL が動作しているマシンの
  メモリ情報を取得可能な状態にあった
- 対策：(1) 1.0.1g にアップデート or
  (2) Heartbeat 無効にして再コンパイル

Heartbeat プロトコル

- RFC6520 で策定
- リクエスト-レスポンス型の
  2-way で完結する簡易なプロトコル
  - 「やまびこ」のようなもん
- SSL/TLS の Record レイヤで送受信



SSL/TLS handshake



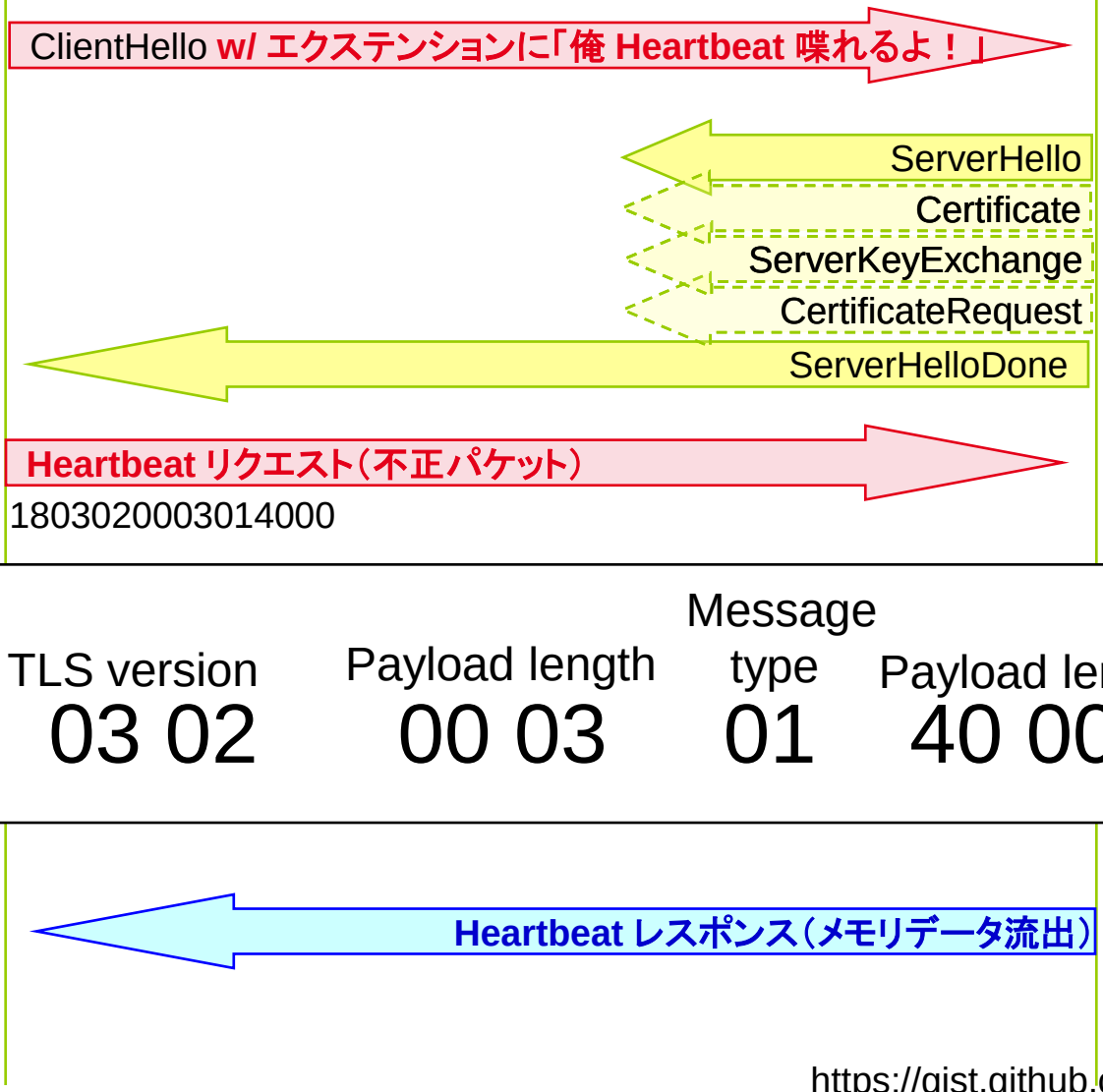
http://tools.ietf.org/html/rfc5246

ハンドシェイク中にHeartbeatすると…

- SSL/TLSクライアント/サーバのどちらが
  トリガー（リクエスタ）になってもいい
- ハンドシェイク中にいきなり
  Heartbeat リクエストを送りつけると…

→それを受け取った OpenSSL ライブラリは
境界チェックのバグを誘発
→メモリ領域のデータをレスポンス

ssltest.py (攻撃ツール)



https://gist.github.com/sh1n0b1/10100394

そのほかのOpenSSL実装のまずさ

- Heartbeatメッセージの中身を見て処理できなければ無視
  →OpenSSLでは不幸なことに0バイトメッセージを受け取ったときに，この「無視」が効いていない
  ＝0バイトのときの処理が不明瞭(仕様の問題？)
- リクエスト ではデータ長エリアのあと，その分のデータを格納するはず
  → OpenSSL ではそれが入っているかどうか完全に無視.
- Heartbeatメッセージは最大 2^{14}のはず
  → OpenSSLではこのチェックを怠ってしまい
  最大2^{16}-1ビットのデータを返すはめに

メモリへの不正アクセスの深刻度

- システム上のメモリ領域データ奪取により

ID/パスワード	成りすましによる不正アクセス
セッションID (例：Cookie)	セッションハイジャック
サーバ証明書の秘密鍵	暗号化通信の復元
	本物と判断可能な偽サーバへの誘導

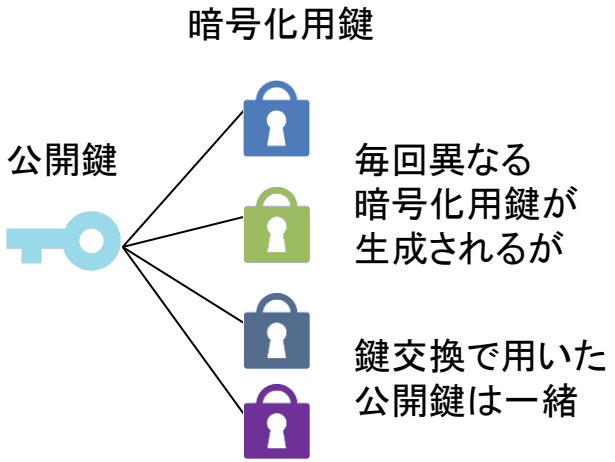
が可能になっていた

- 秘密鍵の更新と証明書の再発行が推奨された

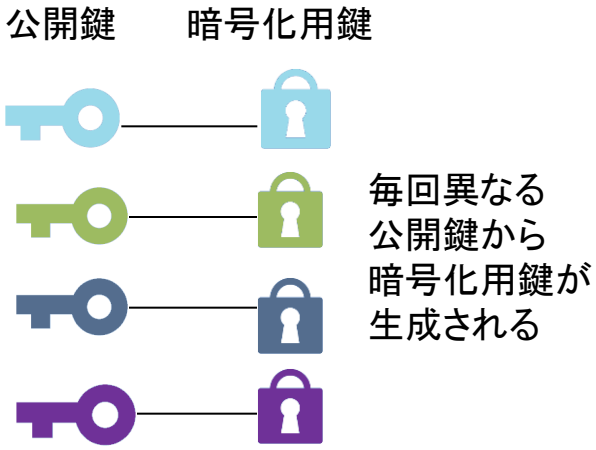
（Perfect）Forward Secrecyへの注目

「一時的に用いた鍵は捨ててもよい」

- サーバ証明書のRSA公開鍵を使わずに
  その都度，ECDH/DHで暗号化して捨てる



RSA、DH_RSA、ECDH_RSA利用時

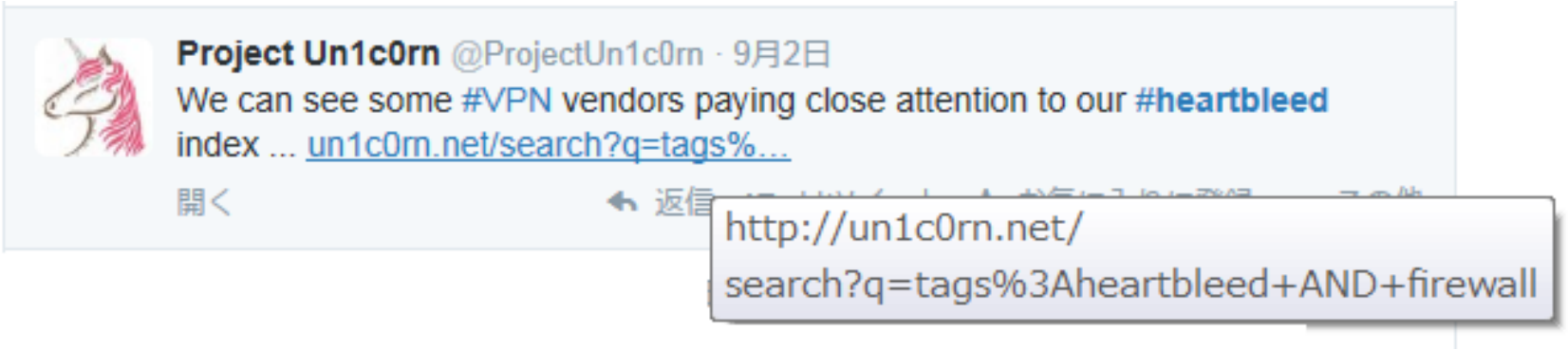


DHE_RSA、ECDHE_RSA利用時
（Forward Secrecy 適用）

http://www.iij.ad.jp/company/development/report/iir/022.html

Project Un1cr0n

- Heartbleedバグがそのままになっているサーバに関する情報提供



- Bitcoinで情報を購入可能

CCS Injection 概要

2014年6月

- CVE-2014-0224
- 日本時間6月6日に公開
  - http://ccsinjection.lepidum.co.jp/ja.html
- 脆弱なバージョン:
  - サーバ OpenSSL 1.0.1 系列:1.0.1g以下
  - クライアント

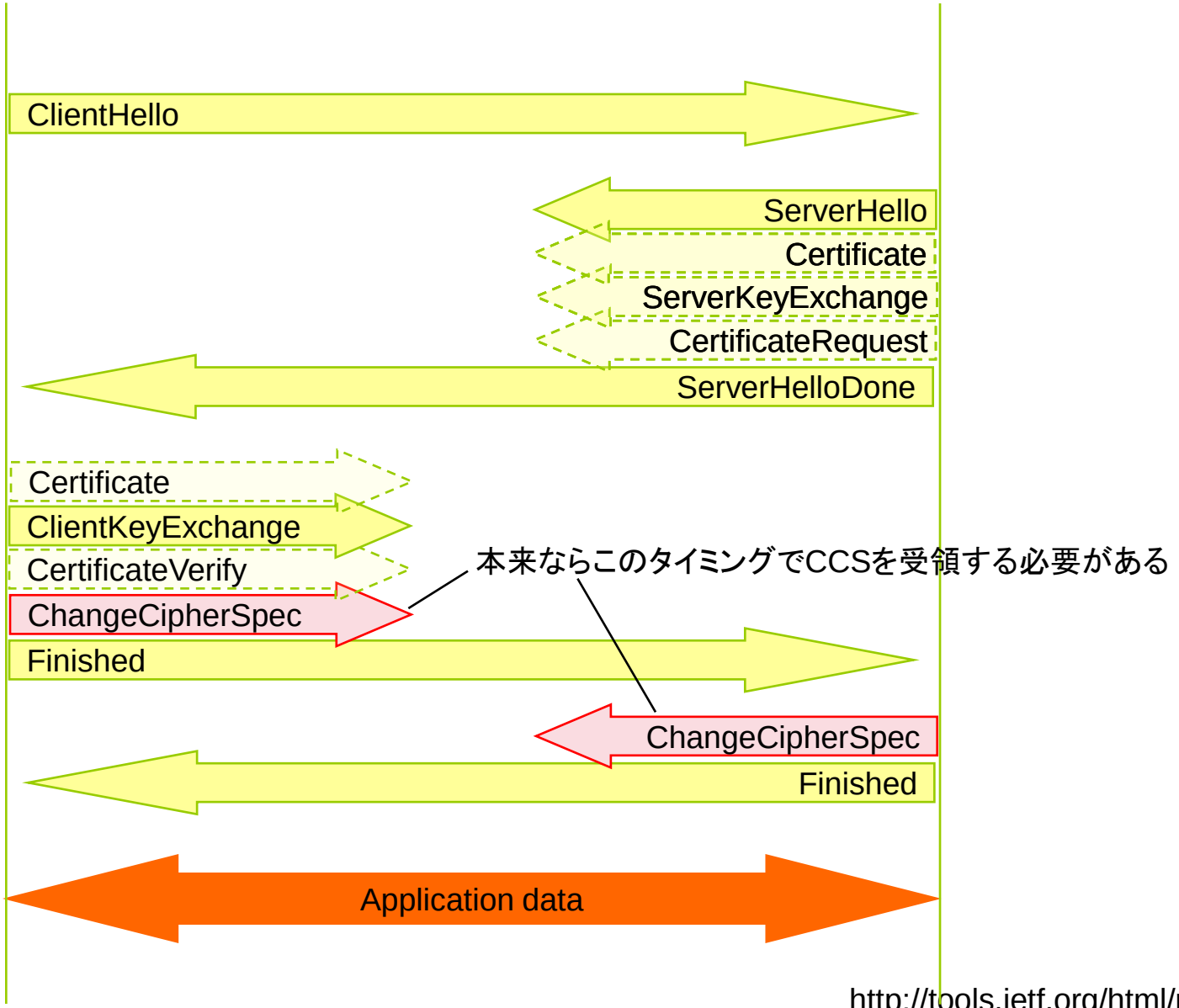
    各系列 1.0.1g以下, 1.0.0以下, 0.9.8y 以下
- 問題:ChangeCipherSpecメッセージの処理の欠陥により暗号化データの漏洩

ポイント

- 受け入れてはいけないタイミングでCCSメッセージを受領してしまう
  - CCS =「セッション鍵をリフレッシュしよう！」
- サーバだけでなくクライアントもOpenSSLを利用している際にだけ起こる

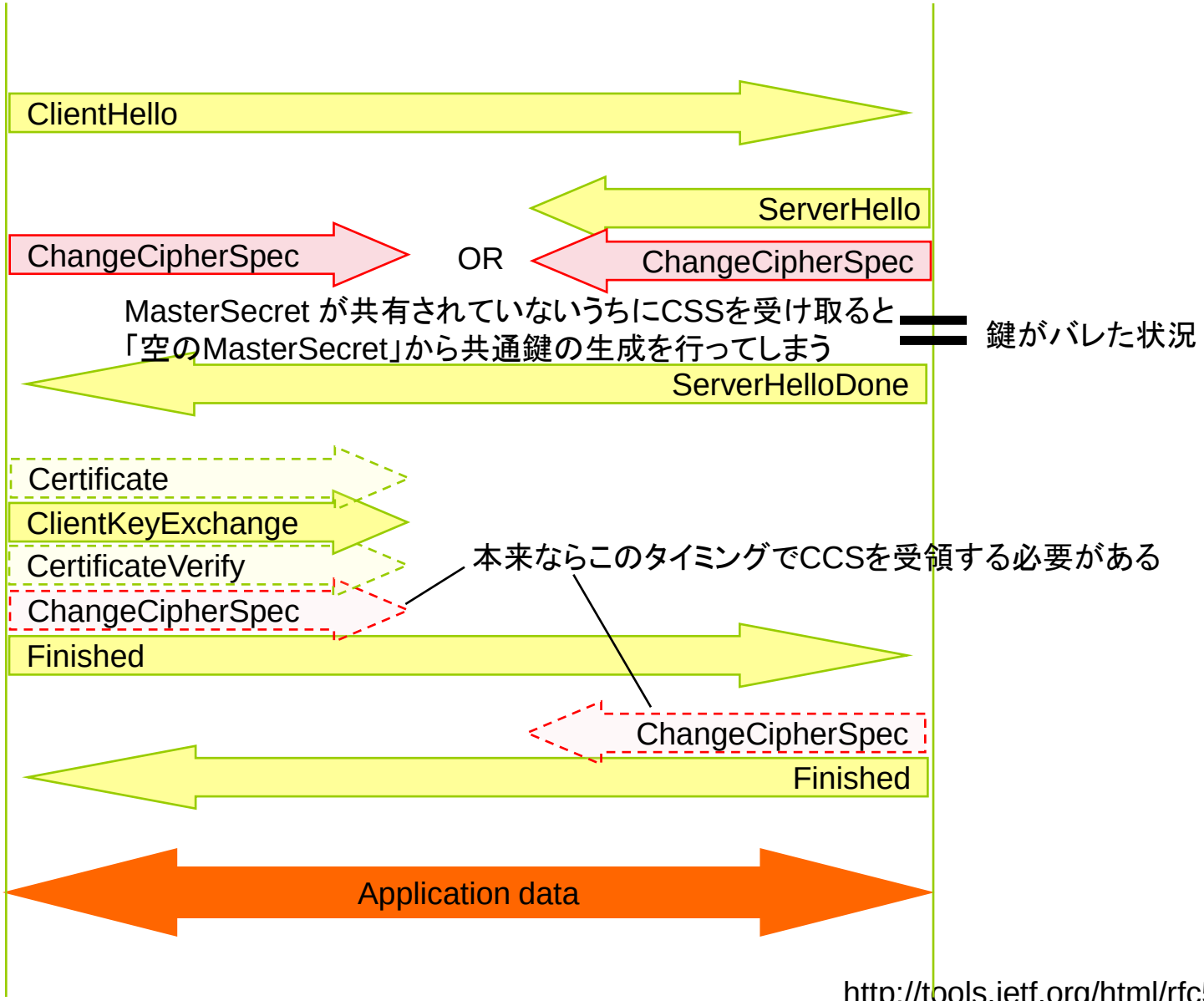
  → 環境によっては放置しても大丈夫な状況もありえる
- 枯れた技術神話が崩壊した
  - 「0.98系は大丈夫だろう」 v.s 意識の高い管理者（パッチ信者）
  - 1998年12月からエンバグしていた

SSL/TLS handshake



http://tools.ietf.org/html/rfc5246

SSL/TLS handshake



http://tools.ietf.org/html/rfc5246

2014年9月

NSSにおける署名検証不備

- CVE-2014-1568
- 日本時間9月24日に公開
  - http://www.mozilla-japan.org/security/announce/2014/mfsa2014-73.html

- 問題：NSSにおけるパーサの問題によりRSA署名検証をすり抜けて，偽造された文書が正当な署名であると返却される場合がある

今回の攻撃手法のポイント

- （1）2006年のBleichenbacher attack ライクな攻撃手法
- （2）DigestInfo のパーザ時の問題を突いている
- （3）"signature malleability" - 署名データの揺れを利用
- （4）RSA署名かつ e=3 のときに適用可能

現実的な問題としてはX.509証明書の署名部分の偽造が考えられるが，現在はあまり使われていないパラメータ（e=3）にのみ有効な攻撃手法と考えられるため，現実的な攻撃とは認められない

2006年のBleichenbacher attack

- 署名偽造が成功するための前提条件は，RSAアルゴリズムで用いられる公開鍵(N,e)のうち e=3 の場合のみ
- 「実装上の問題」とはPKCS#1で規定されたパディングフォーマットに沿っていない場合でも署名を受け入れている，という点
- 本来以下のようなフォーマットがパディング方式に使われる

  00 01 FF FF …FF 00 || ALG || H(M)

http://www.imc.org/ietf-openpgp/mail-archive/msg06063.html

- しかし一部の実装では

00 01 FF FF …FF 00 || ALG || H(M) || gomi

のように後ろにゴミデータを含む場合，本来ならエラーとして処理すべきなのに署名を受理してしまうことがあった

malleability

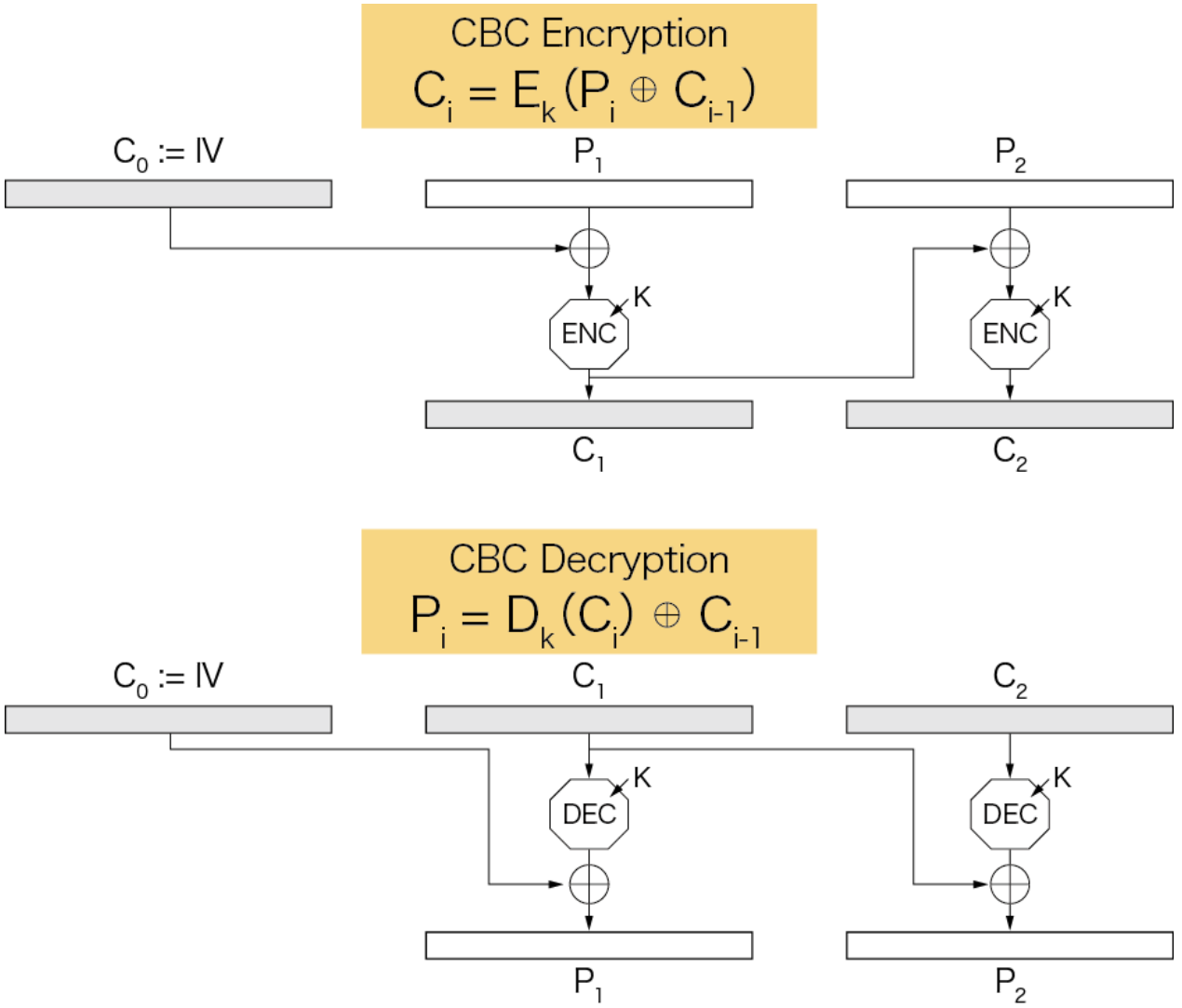
- Bitcoin 交換所Mt.Goxへの攻撃でも利用された手法に似ている http://arxiv.org/abs/1403.6676
  - Christian Decker, Roger Wattenhofer, “Bitcoin Transaction Malleability and MtGox”
- セマンティカリに同じ内容のデータをエンコーディングしても複数のデジタルデータで表現可能になるという「揺れ」を利用
  - BER v.s DER encoding

POODLE attack 概要

画像ナシ

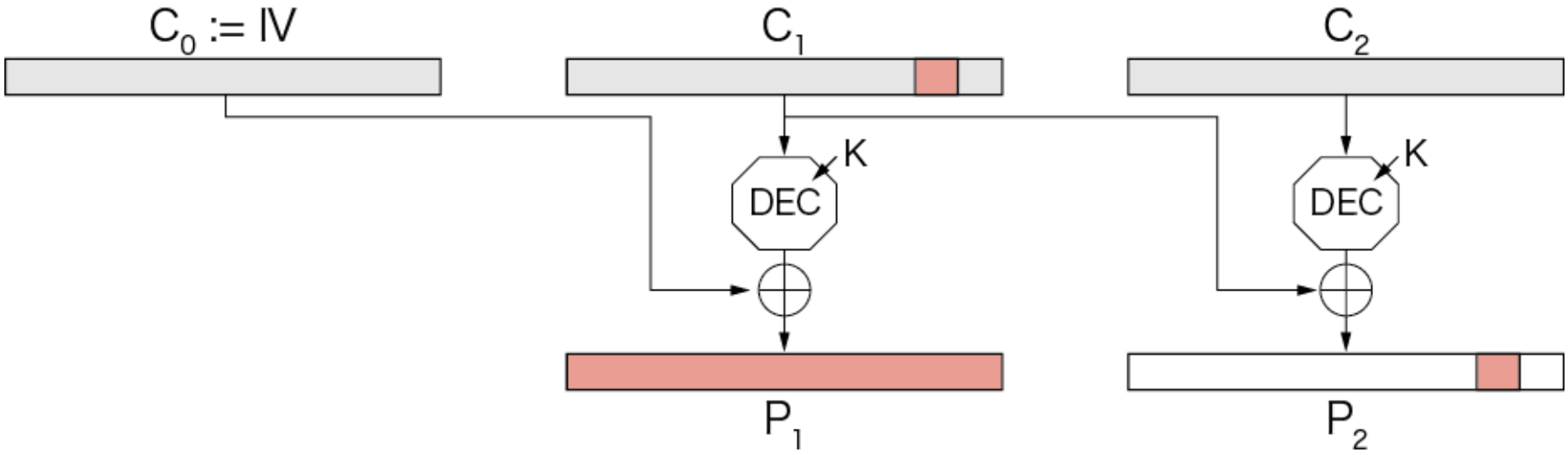
- CVE-2014-3566
- 日本時間10月15日に公開
  - https://www.openssl.org/~bodo/ssl-poodle.pdf
- 仕様そのものの問題
  - SSLv3にてCBC暗号モード利用時のみ影響
    - SSLv2は以前から脆弱
- 問題：Padding Oracle Attack の一種.
  サーバのパディングチェック機能を悪用し
  ブラウザから大量のリクエストをサーバに
  送りつけてトライ＆エラーを繰り返し，暗号化
  された攻撃対象データを1バイトずつ復号

CBC（Cipher Block Chaining）モード概要



http://www.iij.ad.jp/company/development/report/iir/025.html

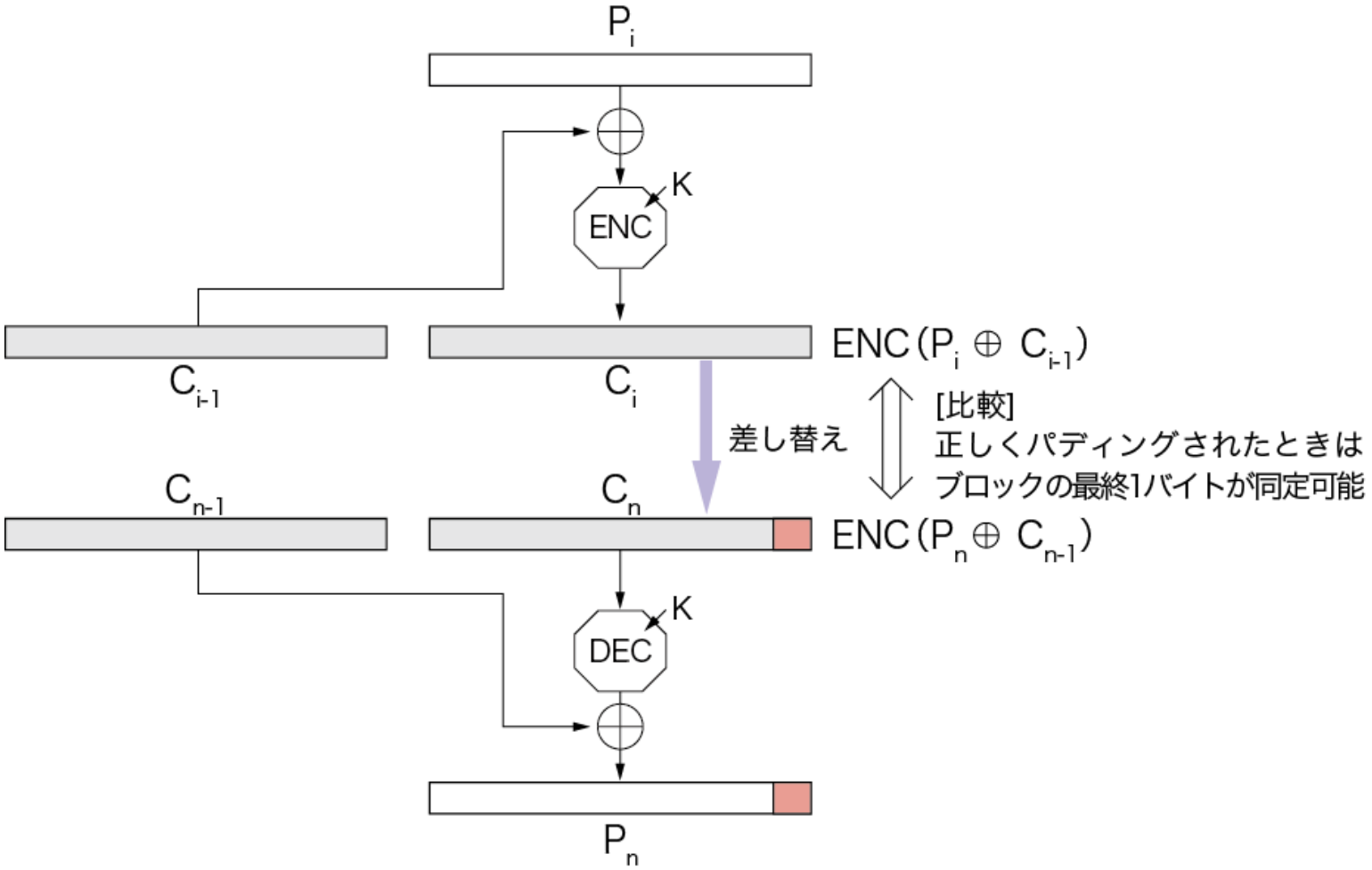
CBCモードにおける暗号文が改ざんされた場合の波及範囲



※暗号文の1バイトを改ざんして復号処理した場合には、当該ブロックの平文はブロック全体に渡って影響が及ぶが、次ブロックにおける平文において意図した箇所を改ざんすることが可能である。

http://www.iij.ad.jp/company/development/report/iir/025.html

Padding Oracle Attack の原理

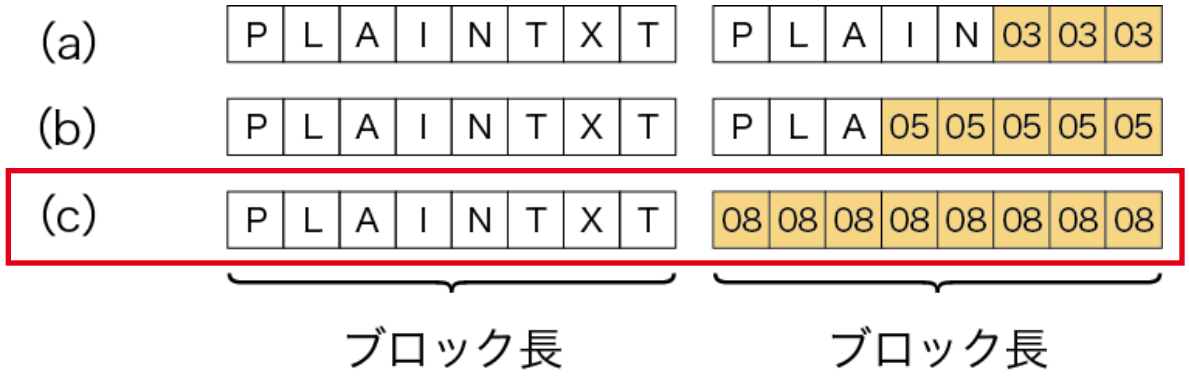


※サーバのPaddingチェック機能においてPaddingが正しい場合にはアクセプトされるが誤っている場合にはエラーが返却される。

http://www.iij.ad.jp/company/development/report/iir/025.html

POODLE attack 攻撃の条件

- SSLv3でCBCモードを利用
  - RC4 では影響なし
  - TLSv1 でも潜在的な攻撃はあるが無視できる
- 暗号化したデータの最終ブロックが
  パディングデータのみで埋め尽くされる状態



パディングデータを改ざんされたとしてもMAC の検証外なので
改ざんを検知することができない

http://www.iij.ad.jp/company/development/report/iir/025.html

POODLE attack への対策

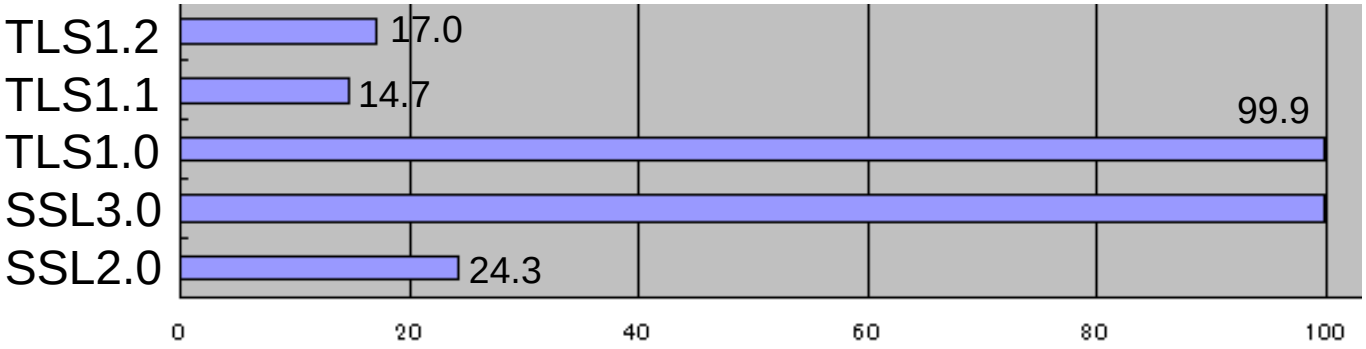
- （1）SSLv3を捨てる
  - Twitterなどで即座に対応が行われた
  - www.iij.ad.jp, help.iij.ad.jp 等でも対策済
- （2）TLS_FALLBACK_ SCSVの導入
  - OpenSSL 10月アップデートで実装済

- 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

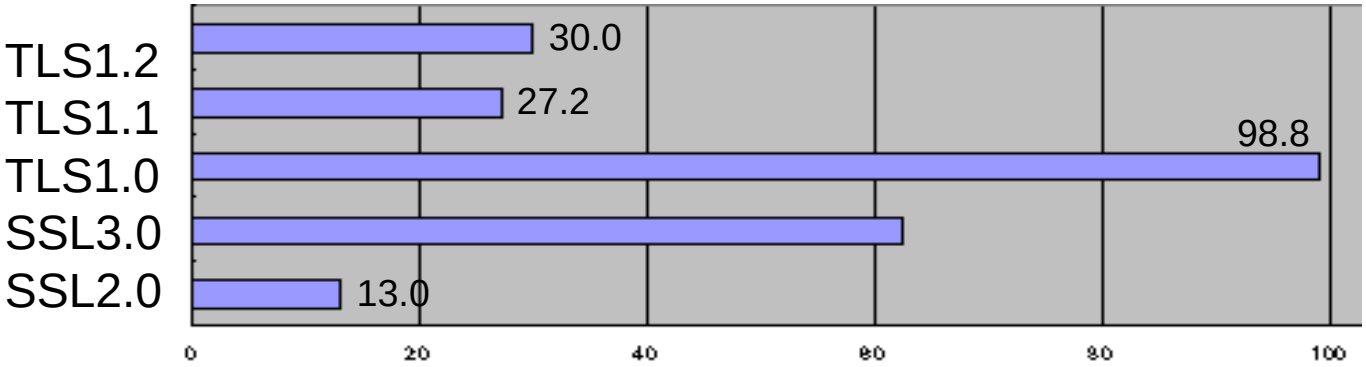
- 4月15日 SSL-enable sites=5677



99.9%

- 11月26日 SSL-enable sites=5620

SSLv3を無効にするサイトが
大幅に増加している



62.3%

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

SSLv3でRC4利用することの可否

- 2013年3月/8月に複数の攻撃が発表済
- CRYPTREC暗号リストにおいては
  運用監視暗号リスト（戦力外通知）に
  - 互換性維持以外の目的での利用は推奨しない

- どうしても SSLv3 を利用せざるを得ない状況の場合，RC4とTripleDES-CBC のどちらを利用すべきだろうか？

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

インターネットの先にいます。

IIJはこれまで、日本のインターネットはどうあるべきかを考え、
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ました。
インターネットの未来を想い、イノベーションに挑戦し続けることで、世界を塗り変えていく。
それは、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/