運用ガイドラインWG活動報告

主査　菊池　浩明

明治大学

CRYPTREC
Cryptography Research and Evaluation Committees

背景1: スノーデン事件とフォワードセキュリティ

- **Edward Joseph Snowden**
  - 元米中央情報局CIA職員、米国家安全保障局NSAへ出向していた
  - 2013年6月13日、香港英文紙に、米国政府が世界中の数万の標的を対象に電話記録やインターネット利用を極秘裏に監視していたことを暴露
- **Perfect Forward Secrecy (PFS)の重要性が再認識**
  - PFS: ある時刻に長期鍵が漏洩しても、それ以前の暗号通信の解読に影響を与えないこと

    RSA: PFSでない
    DH: PFSでない
    DHE (DH Ephemeral): PFSを満たす
    ECDHE (楕円版DHE): PFSを満たす

CRYPTREC
Cryptography Research and Evaluation Committees

背景2: BEAST, POODLE攻撃

■BEAST攻撃

- CBCモードの脆弱性。ブロックの一部を解読。メッセージの分割などにより対処可

■POODLE攻撃

- SSL 3.0のパディングの脆弱性。2014年12月に発見

SSL/TLS への攻撃方法に対する耐性	TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
ダウングレード攻撃（最弱の暗号アルゴリズムを強制的に使わせることができる）	安全	安全	安全	安全	脆弱
バージョンロールバック攻撃（SSL2.0 を強制的に使わせることができる）	安全	安全	安全	安全	脆弱
ブロック暗号の CBC モード利用時の脆弱性を利用した攻撃（BEAST/POODLE 攻撃など）	安全	安全	パッチ適用要	脆弱	脆弱

CRYPTREC
Cryptography Research and Evaluation Committees

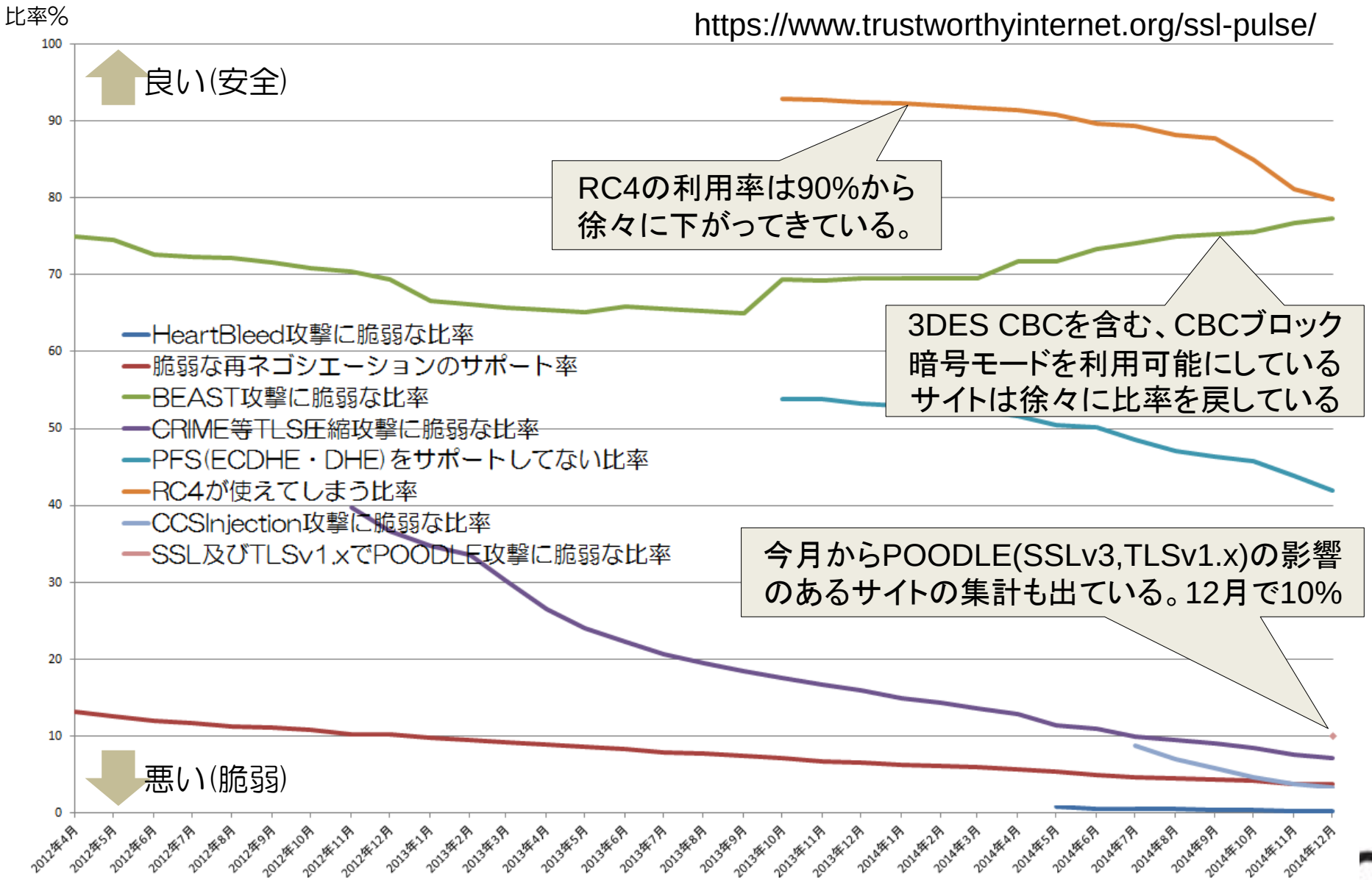
背景3: 新しいプロトコル

- **TLS 1.2 (RFC5246, 2008)**
  - SHA-256, SHA-384のサポート
  - CBCに代わる認証付暗号利用モード(GCM, CCM)をサポート
  - 必須暗号スイート
    TLS_RSA_WITH_AES_128_CBC_SHA
  - 普及はそれほど進んでいない (54.5%, 2015年2月)

利用できる暗号アルゴリズム	TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
128 ビットブロック暗号（AES, Camellia）	可	可	可	不可	不可
認証付暗号利用モード（GCM, CCM）	可	不可	不可	不可	不可
楕円曲線暗号	可	可	可	不可	不可
SHA-2 ハッシュ関数（SHA-256, SHA-384）	可	不可	不可	不可	不可

CRYPTREC
Cryptography Research and Evaluation Committees

SSL Pulseによる脆弱性影響推移



漆嶌 賢二委員調査・作成

ウェブサーバ管理者の苦悩

- BEAST、POODLEなどの攻撃が次々に出てきて、自分のサイトは安全に運用されてだろうか?
- PFSは重要らしいが、どうしたらそれを満たされるだろうか?
- 携帯電話やゲーム機などのSSLしか話せないブラウザの利用者を無視できない。セキュリティとのトレードオフをどうしたらよいか
- 上司がセキュリティ技術を理解してくれない。最新のTLS1.2の重要性を納得してもらうにはどうしたらよいか

CRYPTREC
Cryptography Research and Evaluation Committees

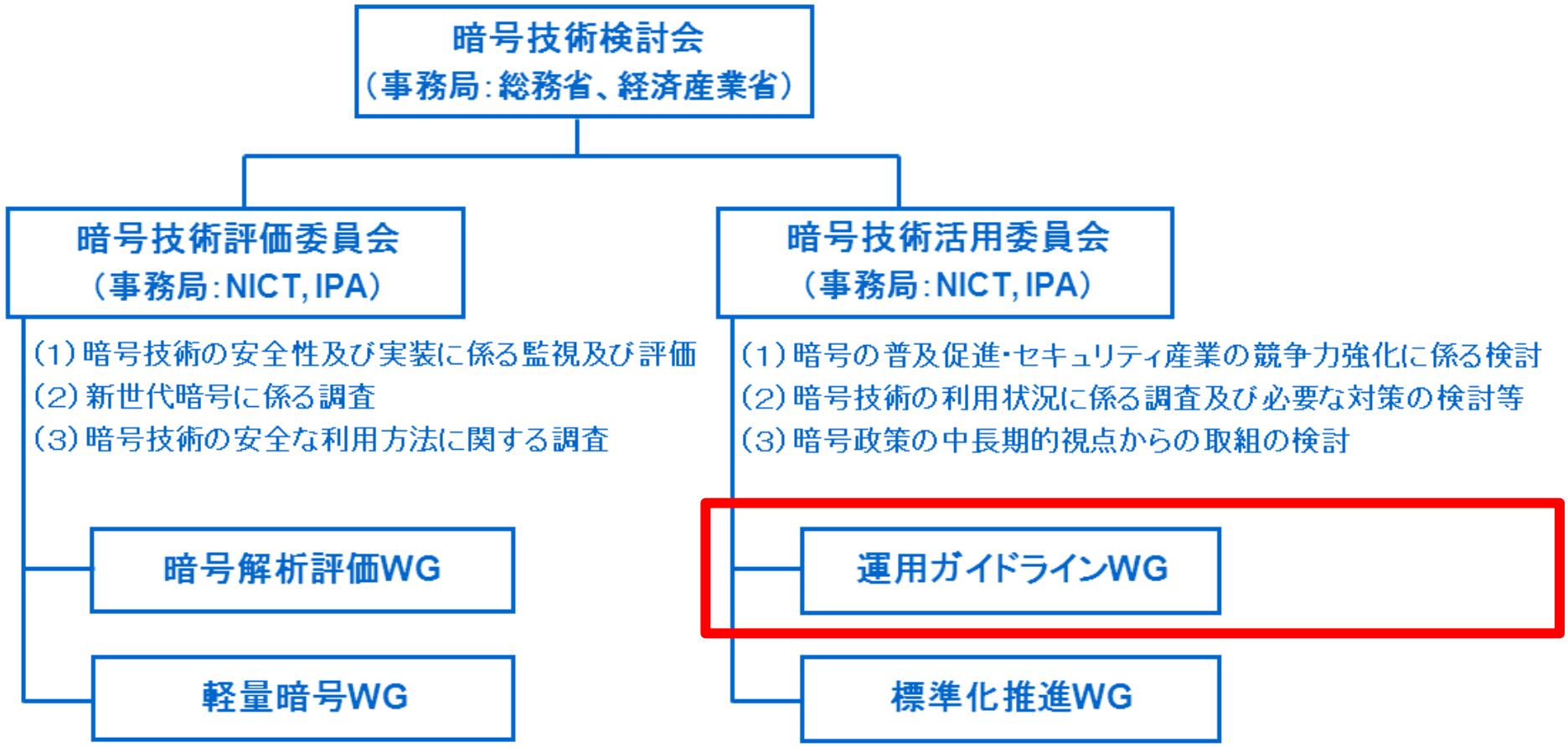
運用ガイドラインが目指したもの

- **暗号に関する一定水準以上の知識・リテラシーがあることを前提とせずに、暗号システムとして安全に利用できるようにするための運用ガイドラインを作成**
  - 「暗号技術解説書」ではなく「Best Practiceを集める」
  - 「暗号技術以外の様々な利用上の判断材料も加味した合理的な根拠」を重視して利用方法をまとめる

- **利用者が非常に多く、また暗号に関するリテラシーのレベルにも大きな差がある「SSL/TLS」を対象**

CRYPTREC体制

CRYPTREC体制図



CRYPTREC
Cryptography Research and Evaluation Committees

運用ガイドラインWG委員

主査	菊池 浩明	明治大学　総合数理学部 先端メディアサイエンス学科　教授
委員	阿部 貴	株式会社シマンテック　SSL製品本部　SSLプロダクトマーケティング部 マネージャー
委員	漆嶌 賢二	富士ゼロックス株式会社　新規事業開発部　SkyDeskサービスセンター マネージャー
委員	及川 卓也	グーグル株式会社　エンジニアリング　シニアエンジニアリングマネージャー
委員	加藤 誠	一般社団法人 Mozilla Japan　技術部　テクニカルアドバイザ
委員	佐藤 直之	株式会社イノベーションプラス　Director
委員	島岡 政基	セコム株式会社IS研究所　コミュニケーションプラットフォームディビジョン 暗号・認証基盤グループ　主任研究員
委員	須賀 祐治	株式会社インターネットイニシアティブ　サービスオペレーション本部 セキュリティ情報統括室　シニアエンジニア
委員	高木 浩光	独立行政法人産業技術総合研究所　セキュアシステム研究部門 主任研究員
委員	村木 由梨香	日本マイクロソフト株式会社　セキュリティレスポンスチーム セキュリティプログラムマネージャ
委員	山口 利恵	東京大学　大学院　情報理工学系研究科　ソーシャルICT研究センター 特任准教授

CRYPTREC
Cryptography Research and Evaluation Committees

WG開催日程

- 2013年 10月 10日(木) 15:00 ～ 18:00
- 2013年 12月　4日(水) 17:30 ～ 21:15
- 2014年　3月 12日(水) 17:00 ～ 20:00
- 2014年 10月 17日(金) 17:30 ～ 22:00
- 2014年 12月 16日(水) 16:30 ～ 21:45
- 2015年　2月 25日(水) 16:00 ～ 18:30

この他に、多数のメールでの議論あり！

3時間、4時間当たり前の
白熱した議論を戦わせた
集大成！

CRYPTREC
Cryptography Research and Evaluation Committees

できあがったガイドラインはこんなもの

- **タイトル**
  「SSL/TLS暗号設定ガイドライン」と「チェックリスト」
- **主な想定読者**
  - SSL/TLSサーバの具体的な構築・設定を行うサーバ構築者
  - サーバ管理やサービス提供に責任を持つサーバ管理者
  - SSL/TLSサーバの構築を発注するシステム担当者
- **2015年3月時点における、SSL/TLS通信での安全性と可用性（相互接続性）のバランスを踏まえた暗号設定方法をガイドラインとして取りまとめた**
  - 電子政府だけでなく、一般でも利用可能なガイドライン
  - ユースケースに応じた3段階の設定基準
  - 現在の利用環境の実態も考慮した設定を採用

CRYPTREC
Cryptography Research and Evaluation Committees

3段階の設定基準

設定基準	概要	安全性	相互接続性の確保
高セキュリティ型	漏えいすると**致命的または壊滅的な悪影響を及ぼす**と予想される情報を通信するような場合に採用 ※**とりわけ高い安全性を必要とする明確な理由があるケース**が対象で、**非常に高度で限定的な使い方**	標準的な水準を**上回る高い安全性水準**を達成	**最近のOSやブラウザ**でなければ接続できない可能性が高い
推奨セキュリティ型	漏えいすると**何らかの悪影響を及ぼす**と予想される情報を、安全性確保と利便性実現をバランスさせて通信するような場合に採用 ※ほぼすべての**一般的な利用形態で使う**ことを想定	**標準的な安全性水準**を実現	**本ガイドラインで対象とするブラウザ**であれば問題なく**相互接続性を確保**
セキュリティ例外型	脆弱なプロトコルバージョンや暗号が使われるリスクを受容したうえで、**安全性よりも相互接続性に対する要求をやむなく優先**させて通信するような場合に採用 ※推奨セキュリティ型への**早期移行を前提**として、**暫定的に利用継続**するケースを想定	推奨セキュリティ型への移行完了までの**短期的な利用を前提に許容可能な最低の安全性水準**を満たす	最新ではない**フィーチャーフォンやゲーム機**などを含めた、**ほとんどのすべての機器**について相互接続性を確保

推奨セキュリティ型の要求設定

■プロトコルバージョン

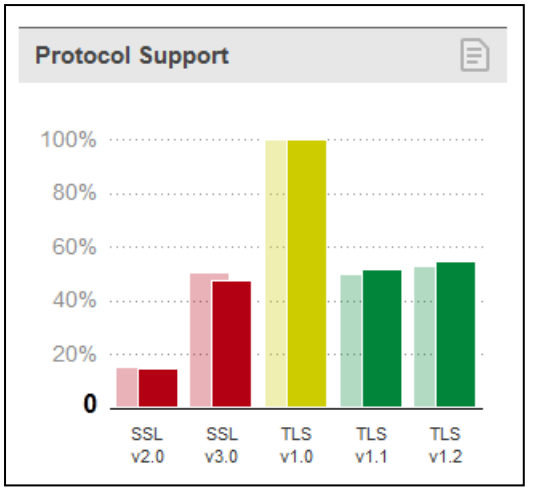
○：設定有効（◎：優先するのが望ましい）　×：設定無効化　－：実装なし

TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
◎	○	○	×	×
－	◎	○	×	×
－	－	◎	×	×

設定無効化

【判断根拠】

SSL/TLSへの攻撃方法に対する耐性	TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
ダウングレード攻撃（最弱の暗号アルゴリズムを強制的に使わせることができる）	安全	安全	安全	安全	脆弱
バージョンロールバック攻撃（SSL2.0を強制的に使わせることができる）	安全	安全	安全	安全	脆弱
ブロック暗号のCBCモード利用時の脆弱性を利用した攻撃（BEAST/POODLE攻撃など）	安全	安全	パッチ適用要	脆弱	脆弱
利用できる暗号アルゴリズム	**TLS1.2**	**TLS1.1**	**TLS1.0**	**SSL3.0**	**SSL2.0**
128ビットブロック暗号（AES, Camellia）	可	可	可	不可	不可
認証付暗号利用モード（GCM, CCM）	可	不可	不可	不可	不可
楕円曲線暗号	可	可	可	不可	不可
SHA-2ハッシュ関数（SHA-256, SHA-384）	可	不可	不可	不可	不可



SSL Pulse – 2015.2.7

https://www.trustworthyinternet.org/ssl-pulse/

CRYPTREC
Cryptography Research and Evaluation Committees

3つのセキュリティ型の整理

要件		高セキュリティ型	推奨セキュリティ型	セキュリティ例外型
想定対象		G2G	一般	レガシー携帯電話を含む
暗号スイートの（暗号化の）セキュリティレベル		①256 bit ②128 bit	①128 bit ②256 bit	① 128 bit ② 256 bit ③ RC4, Triple DES
暗号アルゴリズム	鍵交換	DHE 2048 bit ECDHE 256 bit	DHE 1024 bit以上 ECDHE 256 bit RSA 2048 bit ECDH 256 bit	DHE 1024 bit以上 ECDHE 256 bit RSA 2048 bit ECDH 256 bit
	暗号化	AES 256, 128 CAMELLIA 256, 128	AES 256, 128 CAMELLIA 256, 128	AES 256, 128 CAMELLIA 256, 128 RC4 DES CBC3
	モード	GCM	GCM, CBC	
	ハッシュ関数	SHA384, SHA256	SHA384, SHA256, SHA1	
プロトコルバージョン		TLS1.2のみ	TLS1.2 ～ TLS1.0	TLS1.2～1.0, SSL 3.0
証明書鍵長		鍵長2048ビット以上のRSA または 鍵長256ビット以上のECDSA		
証明書でのハッシュ		SHA256		SHA256, SHA1

推奨セキュリティ型の要求設定

■サーバ証明書の設定

暗号アルゴリズムと鍵長	RSAとSHA-256の組合せで鍵長は2048ビット以上、またはECDSAとSHA-256の組合せで鍵長は256ビット以上、を必須
発行・更新時の鍵情報の生成	● 発行・更新時に、既存の鍵情報は再利用せず、必ず新たに公開鍵と秘密鍵の鍵ペアを生成しなければならない ● 上記の指示をサーバ管理者への仕様書、運用手順書、ガイドライン等に明示しなければならない
クライアントでの警告表示の回避	● 全てのクライアントに対して、警告表示が出ないようにするか、警告表示が出るブラウザはサポート対象外であることを明示しなければならない

【判断根拠】

- CRYPTREC暗号リストに準拠。ただし、DSAはほとんど利用されておらず、RSAやECDSAと比較して大きなメリットがないため、積極的には勧めない
- 信頼できないサーバ証明書の利用は止めるべき
- 公開鍵と秘密鍵の鍵ペアを正しく生成・運用していないと、暗号化された通信データが復号されるなどのリスクがある。特に、デフォルト設定での利用や秘密鍵漏えい時の使いまわしを避ける必要がある

推奨セキュリティ型の要求設定

■暗号スイートの設定

【判断根拠】

- CRYPTREC暗号リストに掲載されているアルゴリズムのみで構成
- 暗号化として128ビット安全性以上を有する
- Triple DESよりも安全でかつ高速な共通鍵暗号としてAESやCamelliaが利用可能であることから、Triple DESは除外
- 上記以外の暗号スイートは利用除外

- 優先順位
  - 通常の利用形態において、128ビット安全性があれば十分な安全性を確保できることから128ビット安全性を優先
  - 鍵交換に関しては、Perfect Forward Secrecyの特性の有無と実装状況に鑑み、DHE/ECDHE、RSA、ECDHの優先順位とする

- 楕円曲線暗号の利用についてはオプトイン型を採用

どんなことを議論したか①

- **ガイドラインの対象範囲をどうするか**
  - 電子政府だけをターゲットにするか、民間（一般）も含めるか
  - フィーチャーフォンなどもクライアントの対象に含めるか
  - ユースケースをどう考えるか
  - 想定読者を誰に置くか
  - 設定基準をいくつ置くか
- **プロトコルバージョンの設定をどうするか**
  - BEAST, POODLE攻撃などの影響をどう判断するか

どんなことを議論したか②

- **サーバ証明書の取り扱いをどうするか**
  - サーバ証明書で使う暗号アルゴリズムを何にするか
  - 鍵長をどうするか
  - サーバ証明書の種類（EV, OV, DV）をどう使い分けるか
  - パブリック認証局とプライベート認証局の扱いを分けるか
  - いわゆる「オレオレ証明書」の扱いをどうするか
- **暗号スイートの選択をどうするか**
  - 暗号スイートとして認める暗号アルゴリズムを何にするか
  - 鍵交換での暗号アルゴリズムの優先順位をどうするか
  - 鍵交換時の鍵長をどうするか
  - 暗号化での暗号アルゴリズムの優先順位をどうするか
  - 楕円曲線暗号アルゴリズムの利用可否についてどのように考えるか

どんなことを議論したか③

- **実装に起因する問題をどこまで取り上げるか**
  - 乱数生成器の脆弱性
  - 鍵ペアの使いまわし問題
  - 実装攻撃に対する対処
  - 認証局自身の危殆化への対処
- **サーバ以外についてどこまで取り上げるか**
  - ブラウザ設定の考え方
  - リモートアクセスVPN（いわゆるSSL-VPN）

推奨セキュリティ型の要求設定

■暗号スイートの設定

	楕円曲線暗号なし	楕円曲線暗号分
グループA	DHE-DSS-AES128-GCM-SHA256	ECDHE-ECDSA-AES128-GCM-SHA256
	DHE-RSA-AES128-GCM-SHA256	ECDHE-RSA-AES128-GCM-SHA256
	DHE-DSS-CAMELLIA128-GCM-SHA256	ECDHE-ECDSA-CAMELLIA128-GCM-SHA256
	DHE-RSA-CAMELLIA128-GCM-SHA256	ECDHE-RSA-CAMELLIA128-GCM-SHA256
	DHE-DSS-AES128-SHA256	ECDHE-ECDSA-AES128-SHA256
	DHE-RSA-AES128-SHA256	ECDHE-RSA-AES128-SHA256
	DHE-DSS-CAMELLIA128-SHA256	ECDHE-ECDSA-CAMELLIA128-SHA256
	DHE-RSA-CAMELLIA128-SHA256	ECDHE-RSA-CAMELLIA128-SHA256
	DHE-DSS-AES128-SHA	ECDHE-ECDSA-AES128-SHA
	DHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA
	DHE-DSS-CAMELLIA128-SHA	
	DHE-RSA-CAMELLIA128-SHA	
グループB	AES128-GCM-SHA256	該当なし
	CAMELLIA128-GCM-SHA256	
	AES128-SHA256	
	CAMELLIA128-SHA256	
	AES128-SHA（RFC必須）	
	CAMELLIA128-SHA	
グループC	該当なし	ECDH-ECDSA-AES128-GCM-SHA256
		ECDH-RSA-AES128-GCM-SHA256
		ECDH-ECDSA-CAMELLIA128-GCM-SHA256
		ECDH-RSA-CAMELLIA128-GCM-SHA256
		ECDH-ECDSA-AES128-SHA256
		ECDH-RSA-AES128-SHA256
		ECDH-ECDSA-CAMELLIA128-SHA256
		ECDH-RSA-CAMELLIA128-SHA256
		ECDH-ECDSA-AES128-SHA
		ECDH-RSA-AES128-SHA

推奨セキュリティ型の要求設定

■暗号スイートの設定（続）

	楕円曲線暗号なし	楕円曲線暗号分
グループD	DHE-DSS-AES256-GCM-SHA384	ECDHE-ECDSA-AES256-GCM-SHA384
	DHE-RSA-AES256-GCM-SHA384	ECDHE-RSA-AES256-GCM-SHA384
	DHE-DSS-CAMELLIA256-GCM-SHA384	ECDHE-ECDSA-CAMELLIA256-GCM-SHA384
	DHE-RSA-CAMELLIA256-GCM-SHA384	ECDHE-RSA-CAMELLIA256-GCM-SHA384
	DHE-DSS-AES256-SHA256	ECDHE-ECDSA-AES256-SHA384
	DHE-RSA-AES256-SHA256	ECDHE-RSA-AES256-SHA384
	DHE-DSS-CAMELLIA256-SHA256	ECDHE-ECDSA-CAMELLIA256-SHA384
	DHE-RSA-CAMELLIA256-SHA256	ECDHE-RSA-CAMELLIA256-SHA384
	DHE-DSS-AES256-SHA	ECDHE-ECDSA-AES256-SHA
	DHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA
	DHE-DSS-CAMELLIA256-SHA	
	DHE-RSA-CAMELLIA256-SHA	
グループE	AES256-GCM-SHA384	該当なし
	CAMELLIA256-GCM-SHA384	
	AES256-SHA256	
	CAMELLIA256-SHA256	
	AES256-SHA	
	CAMELLIA256-SHA	
グループF	該当なし	ECDH-ECDSA-AES256-GCM-SHA384
		ECDH-RSA-AES256-GCM-SHA384
		ECDH-ECDSA-CAMELLIA256-GCM-SHA384
		ECDH-RSA-CAMELLIA256-GCM-SHA384
		ECDH-ECDSA-AES256-SHA384
		ECDH-RSA-AES256-SHA384
		ECDH-ECDSA-CAMELLIA256-SHA384
		ECDH-RSA-CAMELLIA256-SHA384
		ECDH-ECDSA-AES256-SHA
		ECDH-RSA-AES256-SHA
除外事項	**グループA～グループF以外のすべての暗号スイートを利用除外とする**	

推奨セキュリティ型のチェックリスト

		参照章	済
①要求設定確認	チェック項目なし		
②プロトコルバージョン設定	②-1) TLS1.0を設定有効にしたか	4.1節	□
	②-2) SSL2.0及びSSL3.0を設定無効（利用不可）にしたか	4.1節	□
	□ ②-3) TLS1.2が実装されている場合には左の□と以下の項目をチェック		
	②-4) TLS1.2について設定を有効にしたか	4.1節	□
	□ ②-5) TLS1.1が実装されている場合には左の□と以下の項目をチェック		
	②-6) TLS1.1について設定を有効にしたか	4.1節	□
	□ ②-7) プロトコルバージョン優先順位を設定できる場合には左の□と以下の項目をチェック		
	②-8) 設定有効になっているプロトコルバージョンのうち、もっとも新しいバージョンによる接続を最優先にしたか。接続できない場合に、順番に一つずつ前のプロトコルバージョンでの接続するようにしたか	4.1節	□
③サーバ証明書設定	③-1) SHA256withRSAで鍵長2048ビット以上、またはSHA256withECDSAで鍵長256ビット以上のサーバ証明書を利用したか （もしくは、現時点で利用中のSHA256withDSAで鍵長2048ビット以上のサーバ証明書をそのまま継続利用したか）	5.1節	□
	③-2) サーバ証明書の発行・更新をした際に、鍵情報のペアを新たに生成したか	5.1節	□
	③-3) サーバ証明書の発行・更新をする際に、鍵情報のペアを新たに生成する旨の指示を仕様書・運用手順書等に記載したか	5.1節	□
	③-4) 接続することが想定されている全てのクライアントに対して、警告表示が出ないように対策するか、警告表示が出るブラウザはサポート対象外であることを明示したか	5.1節	□

推奨セキュリティ型のチェックリスト

		参照章	済
④暗号スイート設定	□ ④-i) 楕円曲線暗号を利用しない場合は左の□と以下の項目をチェック		
	④-i-1) 表2記載の暗号スイート（網掛けを除く）の全部または一部を設定したか	6.1節／6.5.2節	□
	④-i-2) 表2記載のグループA及びグループBそれぞれの暗号スイート（網掛けを除く）から少なくとも一つずつは設定したか	6.1節／6.5.2節	□
	□ ④-i-3) 金融サービスや電子商取引サービスなど、不特定多数に公開されるサービス等において使用されるサーバである場合には左の□と以下の項目をチェック		
	④-i-4) AES128-SHAの暗号スイートを設定したか	6.1節／6.5.2節	□
	④-i-5) 表2記載の暗号スイートのグループ順番（グループAの暗号スイートの次にグループBの暗号スイートが並ぶ、以下同様）を守っているか	6.1節／6.5.2節	□
	④-i-6) 表2記載の暗号スイート以外は、すべて利用不可の設定をしたか	6.1節／6.5.2節	□
	□ ④-ii) 楕円曲線暗号を利用する場合は左の□と以下の項目をチェック		
	④-ii-1) パテントリスクを考慮したうえで楕円曲線暗号を利用すると決めたか	6.1節	□
	④-ii-2) 表2記載の暗号スイート（網掛けを含む）の全部または一部を設定したか	6.1節／6.5.2節	□
	④-ii-3) 表2記載のグループA及びグループBそれぞれの暗号スイート（網掛けを含む）から少なくとも一つずつは設定したか	6.1節／6.5.2節	□
	□ ④-ii-4) 金融サービスや電子商取引サービスなど、不特定多数に公開されるサービス等において使用されるサーバである場合には左の□と以下の項目をチェック		
	④-ii-5) AES128-SHAの暗号スイートを設定したか	6.1節／6.5.2節	□
	④-ii-5) 表2記載の暗号スイートのグループ順番（グループAの暗号スイートの次にグループBの暗号スイートが並ぶ、以下同様）を守っているか	6.1節／6.5.2節	□
	④-ii-6) 表2記載の暗号スイート以外は、すべて利用不可の設定をしたか	6.1節／6.5.2節	□

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術として特に論点となったモノ

- **「セキュリティ例外型」の利用環境を想定した時、Triple DESとRC4のどちらを優先すべきか**
  - セキュリティ例外型を選択したサーバでは、SSL3.0が使われる可能性が高い。少なくとも、SSL3.0を切ることができないと判断したと考えるべき
  - 新しいブラウザやセキュリティパッチを当てることができるブラウザほどSSL3.0は使わない。SSL3.0を使うのはむしろセキュリティパッチなどを当てるのが困難なレガシーなブラウザと考えるべき
  - 現状ではSSL3.0を完全に除外する（＝セキュリティ例外型をなくす）ことは現実的ではない

上記の利用形態では、現時点では、POODLE攻撃によるTriple DESの脆弱性のほうがRC4の脆弱性よりもリスクが高いと判断

暗号技術として特に論点となったモノ

■ 鍵長1024ビットDHE vs. 鍵長2048ビットRSA

- 実際の秘密鍵の漏えいは暗号解読によるものよりも、実装脆弱性や運用ミス等に起因して漏えいする場合が多いため、秘密鍵の漏えい対策になるPFSを優先すべき
- DHEは電子政府推奨暗号、RSAは運用監視暗号
- 鍵長2048ビットDHEのサポートが増えてきているものの、現状では鍵長1024ビットDHEのサポートが圧倒的に多い

現時点では、
「高セキュリティ型」は鍵長2048ビットDHEのみを必須、
「推奨セキュリティ型」「セキュリティ例外型」は
鍵長1024ビットDHEを鍵長2048ビットRSAより優先

そのほかに・・・

- **SSL/TLSを安全に使うために考慮すべきこと**
  - チェックリストの対象ではないが、安全性を高めるために考慮すべき項目を列挙
    - サーバ証明書の取り扱い
    - 実装脆弱性への対処
    - 安全性を高めるために新しく実装されるようになった設定の情報
- **ブラウザについての情報**
  - IEのサポート期間の情報
  - サーバ証明書の警告表示についての動向
  - SSL3.0の取り扱いの動向
- **Appendix**
  - サーバでの具体的な各種設定方法の提示

おわりに

- **SSL3.0の利用は薦めない**
  - どうしても利用するとき（セキュリティ例外型）は、RC4, DES CBC3の順で設定し、推奨セキュリティ型への移行を検討
- **推奨セキュリティ型は、安全性と広い相互接続性のバランスを重要視した**
  - より安全なTLS1.2が優先利用できる設定が望ましい
- **高セキュリティ型では、PFSを必須とした**
  - DHEは明示的に鍵長2048ビットが設定できる場合に限る。それ以外はECDHEを利用すべき
- **暗号設定以外の安全性について考慮すべき事項はガイドライン7章にまとめた**
- **チェックリストは暗号設定の確認用**

おわりに

運用ガイドラインWGに参加いただいた委員の知見が
十分に反映された、実用性の非常に高いガイドラインに
仕上がりました

「SSL/TLS暗号設定ガイドライン」と「チェックリスト」が
公開されましたら、
SSL/TLSサーバの安全性向上のために
是非とも本ガイドラインをご活用ください