SSL/TLS 暗号設定ガイドライン改訂及び鍵管理ガイドライン作成のための調査・検討

― 調査報告書 別紙 1 ―

本文に係る改訂案

2018 年 6 月

IPA 独立行政法人 情報処理推進機構
技術本部 セキュリティセンター

目次

SSL/TLS 暗号設定ガイドライン本文改訂案

I.　本文に係る記述のアップデート

本文に係る記述の改訂案を SSL/TLS ガイドライン v1.1 の節項の昇順に示す。
記載例は、以下のとおりである。

- 改訂前
  改訂前の SSL/TLS ガイドライン v1.1 の記述である。
  改訂する箇所を黄色いマーカーで示す。
- 改訂後
  SSL/TLS 暗号設定ガイドライン改訂及び鍵管理ガイドライン作成のための調査・検討報告書（以下、報告書）の調査結果を受けて作成した改訂案である。
  改訂した箇所を水色のマーカーで示す。
- 調査根拠
  SSL/TLS ガイドライン v1.1 の記述から差分が発生し、改訂が必要であると判断した調査結果の報告書の項番を調査根拠として示す。

なお、本改訂案には、“本ガイドラインの公開時点（2015 年 5 月）”という記述に関する改訂案は含まないこととする。

- 2.1.1　SSL/TLS の歴史
  - P9　表 2　SSL/TLS のバージョン概要
  - 改訂前

バージョン	概要
SSL2.0 （1994）	● いくつかの脆弱性が発見されており、なかでも「ダウングレード攻撃（最弱のアルゴリズムを強制的に使わせることができる）」と「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）」は致命的な脆弱性といえる ● SSL2.0 は利用すべきではなく、実際に 2005 年頃以降に出荷されているサーバやブラウザでは SSL2.0 は初期状態で利用不可となっている
SSL3.0 （RFC6101） （1995）	● SSL2.0 での脆弱性に対処したバージョン ● 2014 年 10 月に POODLE[1]攻撃が発表されたことにより特定の環境下での CBC モードの利用は危険であることが認識されている。POODLE 攻撃は、SSL3.0 におけるパディングチェックの仕方の脆弱性に起因しているため、この攻撃に対する回避策は現在のところ存在していない ● POODLE 攻撃の発表を受け、必要に応じてサーバやブラウザの設定を変更し、SSL3.0 を無効化にするよう注意喚起されている [2]
TLS1.0	● 2015 年 3 月時点では、もっとも広く実装されているバージョンであり、実装率はほ

[1] POODLE: Padding Oracle On Downgraded Legacy Encryption
[2] SSL3.0 の脆弱性対策について、https://www.ipa.go.jp/security/announce/20141017-ssl.html

バージョン	概要
（RFC2246） （1999）	ぼ 100% ● ブロック暗号を CBC モードで利用した時の脆弱性を利用した攻撃（BEAST 攻撃など）が広く知られているが、容易な攻撃回避策が存在し、すでにセキュリティパッチも提供されている。また、SSL3.0 で問題となった POODLE 攻撃は、プロトコルの仕様上、TLS1.0 には適用できない ● 暗号スイートとして、より安全なブロック暗号の AES と Camellia、並びに公開鍵暗号・署名に楕円曲線暗号が利用できるようになった ● 秘密鍵の生成などに擬似乱数関数を採用 ● MAC の計算方法を HMAC に変更
TLS1.1 （RFC4346） （2006）	● ブロック暗号を CBC モードで利用した時の脆弱性を利用した攻撃（BEAST 攻撃等）への対策を予め仕様に組み入れるなど、TLS1.0 の安全性強化を図っている ● 実装に関しては、規格化された年が TLS1.2 とあまり変わらなかったため、TLS1.1 と TLS1.2 は同時に実装されるケースも多く、2015 年 3 月時点でのサーバやブラウザ全体における実装率は約 50%
TLS1.2 （RFC5246） （2008）	● 暗号スイートとして、より安全なハッシュ関数 SHA-256 と SHA-384、CBC モードより安全な認証付暗号利用モード（GCM、CCM）が利用できるようになった。特に、認証付暗号利用モードでは、利用するブロック暗号が同じであっても、CBC モードの脆弱性を利用した攻撃（BEAST 攻撃等）がそもそも適用できない ● 必須の暗号スイートを TLS_RSA_WITH_AES_128_CBC_SHA に変更 ● IDEA と DES を使う暗号スイートを削除 ● 擬似乱数関数の構成を MD5/SHA-1 ベースから SHA-256 ベースに変更 ● 本格的に実装が始まったのは最近であり、2015 年 3 月時点でのサーバやブラウザ全体における実装率は約 55%

➢ 改訂後

バージョン	概要
SSL2.0 （1994）	● いくつかの脆弱性が発見されており、なかでも「ダウングレード攻撃（最弱のアルゴリズムを強制的に使わせることができる）」と「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）」は致命的な脆弱性といえる ● SSL2.0 は利用すべきではなく、実際に 2005 年頃以降に出荷されているサーバやブラウザでは SSL2.0 は初期状態で利用不可となっている
SSL3.0 （RFC6101） （1995）	● SSL2.0 での脆弱性に対処したバージョン ● 2014 年 10 月に POODLE[3]攻撃が発表されたことにより特定の環境下での CBC モードの利用は危険であることが認識されている。POODLE 攻撃は、SSL3.0 におけるパ

[3] POODLE: Padding Oracle On Downgraded Legacy Encryption

バージョン	概要
	ディングチェックの仕方の脆弱性に起因しているため、この攻撃に対する回避策は現在のところ存在していない ● POODLE 攻撃の発表を受け、必要に応じてサーバやブラウザの設定を変更し、SSL3.0 を無効化にするよう注意喚起されている [4]
TLS1.0 （RFC2246） （1999）	● 2018 年 3 月時点では、もっとも広く実装されているバージョンであり、実装率はほぼ 88% ● ブロック暗号を CBC モードで利用した時の脆弱性を利用した攻撃（BEAST 攻撃など）が広く知られているが、容易な攻撃回避策が存在し、すでにセキュリティパッチも提供されている。また、SSL3.0 で問題となった POODLE 攻撃は、プロトコルの仕様上、TLS1.0 には適用できない ● 暗号スイートとして、より安全なブロック暗号の AES と Camellia、並びに公開鍵暗号・署名に楕円曲線暗号が利用できるようになった ● 秘密鍵の生成などに擬似乱数関数を採用 ● MAC の計算方法を HMAC に変更
TLS1.1 （RFC4346） （2006）	● ブロック暗号を CBC モードで利用した時の脆弱性を利用した攻撃（BEAST 攻撃等）への対策を予め仕様に組み入れるなど、TLS1.0 の安全性強化を図っている ● 実装に関しては、規格化された年が TLS1.2 とあまり変わらなかったため、TLS1.1 と TLS1.2 は同時に実装されるケースも多く、2018 年 3 月時点でのサーバにおける実装率は約 85%
TLS1.2 （RFC5246） （2008）	● 暗号スイートとして、より安全なハッシュ関数 SHA-256 と SHA-384、CBC モードより安全な認証付暗号利用モード（GCM、CCM）が利用できるようになった。特に、認証付暗号利用モードでは、利用するブロック暗号が同じであっても、CBC モードの脆弱性を利用した攻撃（BEAST 攻撃等）がそもそも適用できない ● 必須の暗号スイートを TLS_RSA_WITH_AES_128_CBC_SHA に変更 ● IDEA と DES を使う暗号スイートを削除 ● 擬似乱数関数の構成を MD5/SHA-1 ベースから SHA-256 ベースに変更 ● 本格的に実装が始まったのは最近であり、2018 年 3 月時点でのサーバにおける実装率は約 91%
TLS1.3 （draft23）	● 共通鍵暗号は認証付き暗号：AEAD（Authenticated Encryption with Associated Data）のみ採用した結果、AES GCM/CCM と ChaCha20-Poly1305 のみになった ● 鍵交換は、DHE/ECDHE のみで楕円曲線を指定した ● 署名は、RSA-PSS、RSASSA-PKCS1-v1_5、ecdsa_secp256r1 が必須になった ● ハッシュは SHA-256 以上になった

[4] SSL3.0 の脆弱性対策について、https://www.ipa.go.jp/security/announce/20141017-ssl.html

バージョン	概要
	● ハンドシェイク性能の向上のため、1-RTT、0-RTT（Round Trip Time）になるようにシーケンスが簡素化された ● ハンドシェイクのデータを暗号化して保護した ● TLS1.2 互換に配慮し、ClientHello、ServerHello、ChangeCipherSpec が規定された まだ draft であるが、サーバやブラウザで実装が始まっている

- 調査根拠
  - ✓ 4.1①（1）
  - ✓ 4.1②
  - ✓ 4.1③（2.1.1 節）SSL/TLS の各バージョンでのサーバ及びブラウザでの実装状況

- 新規　2.1.3　TLS1.3 の特徴
  - 改訂前

    なし。
  - 改訂後

    TLS1.3 は、TLS1.2 策定以降に見つかった新たな脆弱性や攻撃手法への対策を施すと共に、QUICK などのプロトコルに対応するための性能向上を狙いとして、プロトコルとアルゴリズムの抜本的な再設計が行われた。TLS1.2 との互換性などの課題があり、2018 年 1 月現在標準化作業は続いている。2018 年 1 月現在の最新仕様は、draft23 である。

    TLS1.2 との差異の観点から見た主な特徴を以下に示す。

    （1） 脆弱なアルゴリズムとして、TripleDES、DSA、RC4、MD5、SHA-1、SHA-224、静的な RSA が削除された。また、認証付き暗号（AEAD）でない AES の CBC モードが削除された。

    （2） NIST 規定でないアルゴリズムとして、共通鍵暗号の ChaCha20 と署名の EdDSA が追加された。

    （3） 鍵交換は、DHE、ECDHE が必須になった。楕円曲線として secp256r1 が必須になった。

    （4） 脆弱なハンドシェイク機能として、リニゴーシエーション、圧縮、セッション回復が削除された。

    （5） ServerHello 以降のハンドシェイクパラメータを暗号化して保護する。

    （6） HMAC ベースの導出関数を使った鍵導出に変更された。

    （7） 性能向上のため、1-RTT でハンドシェイクが完了するようにメッセージおよび拡張が見直された。

    （8） QUICK 等の上位アプリへの適用を考慮し、0-RTT でアプリデータを送信する機能が追加された。

（9） ClientHello、ServerHello、ChangeCipherSpec の TLS1.2 互換性を保つことにより、中間ノードによる接続性を向上した。

- 調査根拠
  - ✓ 4.1①（1）

- 新規　2.1.4　TLS プロトコルの最新動向
  - 改訂前

    なし。
  - 改訂後

    2015 年 5 月以降に発行された SSL/TLS に関する RFC の一覧である。TLS1.3 が規格化されているところだが、既存の TLS1.2 までのプロトコルに対して、SSL3.0 の無効化や RC4 の無効化など、プロトコルの脆弱性の排除に関するものが規格化されている。

RFC	**タイトル**	**概要**
7465	Prohibiting RC4 Cipher Suites	RC4 を含む暗号スイートの禁止
7507	TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks	SSL/TLS プロトコルのダウングレード攻撃を防ぐための TLS Fallback Signaling Cipher Suite Value (SCSV)暗号スイートの追加
7525	Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)	SSL2、SSL3 リニゴーシエーションの禁止 TLS1.0、TLS1.1 リニゴーシエーションの非推奨
7568	Deprecating Secure Sockets Layer Version 3.0	SSL3 の禁止
7905	ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS)	ChaCha20-Poly1305 を含む暗号スイートの追加

  - 調査根拠
    - ✓ 4.1①（2）

- 2.2.1　CRYPTREC 暗号リスト
  - 改訂前

    「政府機関の情報セキュリティ対策のための統一基準（平成 26 年度版）」（平成 26 年 5 月 19 日、情報セキュリティ政策会議） では以下のように記載されており、政府機関における情報システムの調達及び利用において、CRYPTREC 暗号リストのうち「電子政府推奨暗号リスト」が原則的に利用される。

    政府機関の情報セキュリティ対策のための統一基準（抄）

    6.1.5 暗号・電子署名－遵守事項(1)(b)

情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム及び運用方法について、以下の事項を含めて定めること。

（ア） 行政事務従事者が暗号化及び電子署名に対して使用するアルゴリズムについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。

（イ） 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズムを採用すること。

（以下、略）

- 改訂後

「政府機関の情報セキュリティ対策のための統一基準（*平成28年度版*）」（平成28年8月31日） では以下のように記載されており、 政府機関における情報システムの調達及び利用において、CRYPTREC 暗号リストのうち「電子政府推奨暗号リスト」が原則的に利用される。

政府機関の情報セキュリティ対策のための統一基準（抄）

6.1.5 暗号・電子署名－遵守事項(1)(b)

情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定めること。

(ア) 行政事務従事者が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。

(イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。

（以下、略）

- 調査根拠
  - ✓ 4.1②

- 2.2.2　異なる暗号アルゴリズムにおける安全性の見方
  - P12　NIST SP800-57 Part 1 Revision 3
  - 改訂前

例えば、NIST SP800-57 Part 1 revision 3[5]では、表 3 のように規定している。

- 改訂後

例えば、NIST SP800-57 Part 1 revision 4[6]では、表 3 のように規定している。

- 調査根拠
  - ✓ 4.1②

- 3.1 実現すべき設定基準の考え方
  - P16 表 4 安全性と相互接続性についての比較
  - 改訂前

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	扱う情報が漏えいした際、組織の運営や資産、個人の資産やプライバシー等に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、極めて高い安全性を確保して SSL/TLS で通信するような場合に採用する設定基準 **※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を対象としており、非常に高度で限定的な使い方をする場合の設定基準である。一般的な利用形態で使うことは想定していない** ＜利用例＞ 政府内利用（G2G 型）のなかでも、限定された接続先に対して、とりわけ高い安全性が要求される通信を行う場合	本ガイドラインの公開時点（2015 年 5 月）において、標準的な水準を大きく上回る高い安全性水準を達成	最近提供され始めたバージョンの OS やブラウザが搭載されている PC、スマートフォンでなければ接続できない可能性が高い また、PC、スマートフォン以外では、最新の機器であっても一部の機器について接続できない可能性がある
推奨セキュリティ型	扱う情報が漏えいした際、組織の運営や資産、個人の資産やプライバシー等に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 SSL/TLS での通信を行うための標準的な設定基準	本ガイドラインの公開時点（2015 年 5 月）における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（8.1.2 節）が搭載されている PC、スマートフォンなどでは問題な

[5] NIST SP800-57, Recommendation for Key Management – Part 1: General (Revision 3)
[6] NIST SP800-57, Recommendation for Key Management – Part 1: General (Revision 4)

設定基準	概要	安全性	相互接続性の確保
	※ほぼすべての一般的な利用形態で使うことを想定している ＜利用例＞ • 政府内利用（G2G 型）や社内システムへのリモートアクセスなど、特定された通信相手との安全な通信が要求される場合 • 電子申請など、企業・国民と役所等との電子行政サービスを提供する場合 • 金融サービスや電子商取引サービス、多様な個人情報の入力を必須とするサービス等を提供する場合 • 既存システムとの相互接続を考慮することなく、新規に社内システムを構築する場合		く相互接続性を確保できる 本ガイドラインが対象としない、バージョンが古い OS やブラウザの場合や発売開始からある程度の年月が経過している一部の古い機器（フィーチャーフォンやゲーム機など）については接続できない可能性がある
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 SSL/TLS での通信を行う場合に許容しうる最低限度の設定基準 **※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している** ＜利用例＞ • 利用するサーバやクライアントの実装上の制約、もしくは既存システムとの相互接続上の制約により、推奨セキュリティ型（以上）の設定が事実上できない場合	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、本ガイドラインの公開時点（2015 年 5 月）において許容可能な最低限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できる

➢ 改訂後

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	扱う情報が漏えいした際、組織の運営や資産、個人の資産やプライバシー等に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、極めて高い安全性を確保して SSL/TLS で通信するような場合に採用する設定基準 **※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を対象としており、非常に高度で限定的な使い方をする場合の設定基準である。一般的な利用形態で使うことは想定していない** ＜利用例＞ 政府内利用（G2G 型）のなかでも、限定された接続先に対して、とりわけ高い安全性が要求される通信を行う場合	本ガイドラインの公開時点（2015 年 5 月）において、標準的な水準を大きく上回る高い安全性水準を達成	本ガイドラインで対象とするブラウザ（8.1.2 節）が搭載されている PC、スマートフォンなどでは問題なく相互接続性を確保できる 本ガイドラインが対象としない、バージョンが古い OS やブラウザの場合や発売開始からある程度の年月が経過している一部の古い機器（フィーチャーフォンやゲーム機など）については接続できない可能性がある
推奨セキュリティ型	扱う情報が漏えいした際、組織の運営や資産、個人の資産やプライバシー等に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 SSL/TLS での通信を行うための標準的な設定基準 **※ほぼすべての一般的な利用形態で使うことを想定している** ＜利用例＞	本ガイドラインの公開時点（2015 年 5 月）における標準的な安全性水準を実現	ほとんどのすべての機器について相互接続性を確保できる。 ※すでにサポートが切れているなどかなり古い機器などで接続できない場合があるが、この種の機器は本来

設定基準	概要	安全性	相互接続性の確保
	• 政府内利用（G2G 型）や社内システムへのリモートアクセスなど、特定された通信相手との安全な通信が要求される場合 • 電子申請など、企業・国民と役所等との電子行政サービスを提供する場合 • 金融サービスや電子商取引サービス、多様な個人情報の入力を必須とするサービス等を提供する場合 • 既存システムとの相互接続を考慮することなく、新規に社内システムを構築する場合		接続させるべきではない。
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 SSL/TLS での通信を行う場合に許容しうる最低限度の設定基準 **※推奨セキュリティ型への早期移行を求めるものであり、すでに最低限の安全性水準を満たしているとは言えない状況になっている** ＜利用例＞ • 利用するサーバやクライアントの実装上の制約、もしくは既存システムとの相互接続上の制約により、推奨セキュリティ型（以上）の設定が事実上できない場合	本ガイドラインの公開時点（2015 年 5 月）において、すでに最低限の安全性水準を満たしているとは言えない状況になっている。速やかな推奨セキュリティ型への移行を強く求める	ほとんどのすべての機器について相互接続性を確保できる

- 調査根拠
  - ✓ 4.1①（4）
  - ✓ 4.1①（5）
  - ✓ 4.1②
  - ✓ 4.2③

- 5.4.3　サーバ証明書で利用すべき鍵長
  - P30　CRYPTREC Report 2013
  - 改訂前

    詳細については、CRYPTREC Report 2013[7] 図 3.1、図 3.2 を参照されたい。
  - 改訂後

    詳細については、CRYPTREC Report 2016[8] 図 3.3、図 3.4 を参照されたい。
  - 調査根拠
    - ✓ 4.1②
- 5.4.5　サーバ証明書の有効期間に関する注意点
  - 改訂後

    5.4.5　サーバ証明書の有効期間に関する注意点

    サーバ証明書については、CA/ブラウザフォーラムによる「Baseline Requirement」で要件が規定されている。2017 年 4 月 22 日以降、既存の鍵ペアを使う場合は、有効期間は 825 日までと規定されており、さらに、2018 年 3 月 1 日以降は、新規鍵ペアでも有効期間は 825 日までと規定されている。したがって、サーバ証明書の有効期間について、このような規定についても考慮されたい。
  - 調査根拠
    - ✓ 4.1①（4）
- 6.2　暗号スイートで利用可能な候補となる暗号アルゴリズム
  - P35　NIST SP800-52 revision 1 (draft)
  - 改訂前

    [9]NIST SP800-52 revision 1 (draft), Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
  - 改訂後

    [10]NIST SP800-52 revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
  - 調査根拠
    - ✓ 4.1②
- 6.3.3　DHE/ECDHE での鍵長の設定状況についての注意
  - P38　図 4　DHE/ECDHE の鍵長の設定状況（Alexa の調査結果を加工）
  - 改訂前

---

[7] http://www.cryptrec.go.jp/report/c13_eval_web_final.pdf
[8] http://www.cryptrec.go.jp/report/cryptrec-rp-0002-2016.pdf
[9] NIST SP800-52 revision 1 (draft), Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
[10] NIST SP800-52 revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

図 4 の 2015 年 1 月の Alexa の調査結果[11]によれば、約 47 万の主要なサイトについて、DHE が利用できるのは約 52.3%であり、そのうちの約 87.5%（全体では約 45.8%）が鍵長 1024 ビットを採用している。一方、ECDHE が利用できるのは約 62.7%であり、そのうちの約 98%（全体では約 61.5%）が鍵長 256 ビットを採用している。

➢ 改訂後

図 4 の 2017 年 1 月の Alexa の調査結果[12]によれば、約 47 万の主要なサイトについて、DHE が利用できるのは約 55.7%であり、そのうちの約 64.7%（全体では約 36.0%）が鍵長 2048 ビットを採用している。一方、ECDHE が利用できるのは約 92.2%であり、そのうちの約 92.7%（全体では約 85.4%）が鍵長 256 ビットを採用している。

・ P38　図 4　DHE/ECDHE の鍵長の設定状況（Alexa の調査結果を加工）

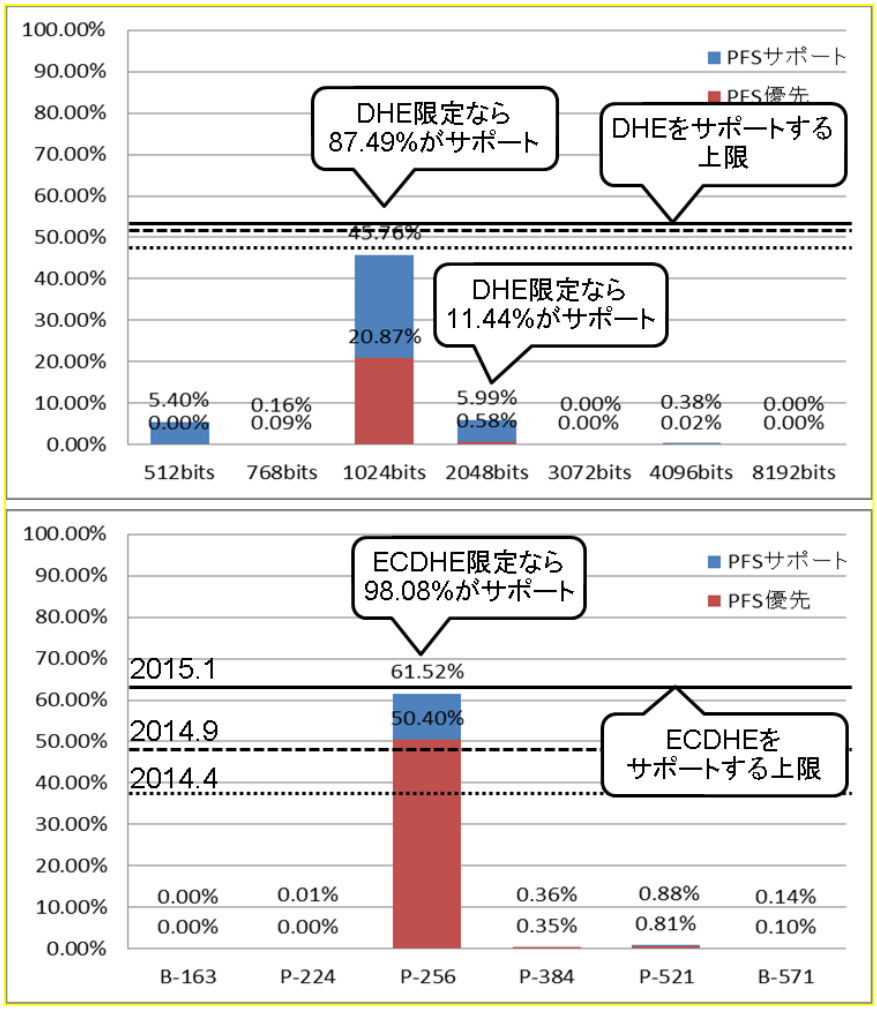


図 4　DHE/ECDHE の鍵長の設定状況（Alexa の調査結果を加工）

➢ 改訂後

[11] https://securitypitfalls.wordpress.com/2015/02/01/january-2015-scan-results/
[12] https://securitypitfalls.wordpress.com/2017/04/17/january-2017-scan-results/

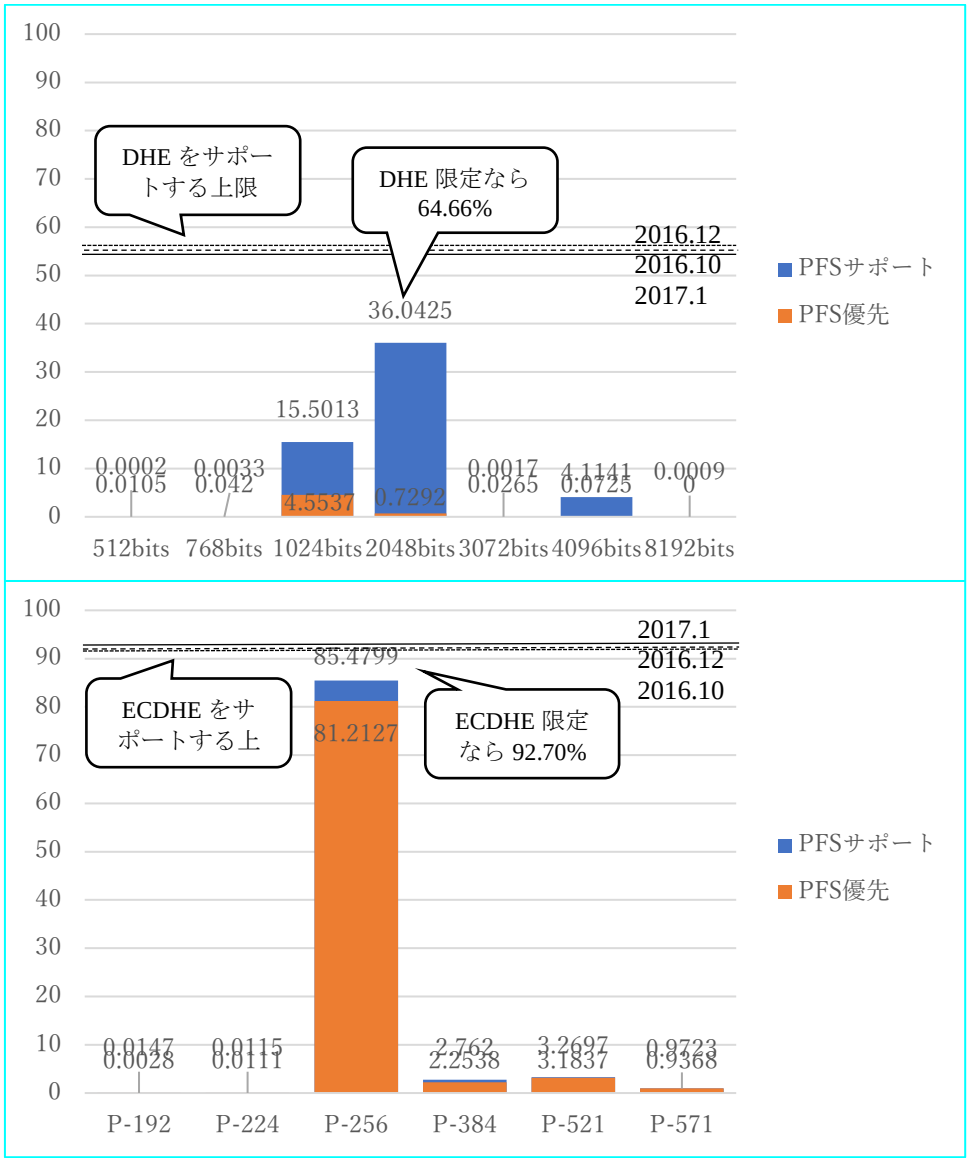


図 4　DHE/ECDHE の鍵長の設定状況（Alexa の調査結果を加工）

- 調査根拠
  - ✓ 4.1③（6.3.3 節）DHE での鍵長 2048 ビットの設定に係る実装状況

- 7.1.1　サーバ証明書での脆弱な鍵ペアの使用の回避
  - P45　既知の解読可能な鍵ペアでないことを確認するサービス
  - 改訂前

    [13]例えば https://factorable.net/keycheck.html がある。ただし、安全性を 100%証明するものではないことに注意されたい
  - 改訂後

[13] 例えば https://factorable.net/keycheck.html がある。ただし、安全性を 100%証明するものではないことに注意されたい

[14]例えば https://keytester.cryptosense.com/や https://keychest.net/roca がある。ただし、安全性を 100%証明するものではないことに注意されたい

- 調査根拠
  - ✓ 4.1②

- 7.2.1 HTTP Strict Transport Security（HSTS）の設定有効化
  - 改訂前

    以上のように、HTTPS で安全にサービスを提供したい場合などでは、ユーザに意識させることなくミスを防止でき、ユーザの利便性を向上させることができるので、HSTS の機能を持っているならば有効にすることを推奨する。参考までに、いくつかの設定例を Appendix B.4 で紹介する。

    ただし、HSTS が実際に機能するためには、サーバだけでなく、ブラウザも対応している必要があることに注意されたい。また、一度も接続したことがないサーバ（例外的に Firefox 17 以降ではあらかじめ登録されているサーバもある）や、HSTS の期限切れになったサーバの場合にも、HTTPS への変換は行われない。

    2014 年 9 月時点での主要な製品の HSTS へのサポート状況は以下の通りである。

    - サーバ
      - Apache 2.2.22 以降：設定により可能
      - Lighttpd 1.4.28 以降：設定により可能
      - nginx 1.1.19 以降：設定により可能
      - IIS：設定により可能
    - クライアント（ブラウザ）
      - Chrome：4.0.211.0 以降でサポート
      - Firefox：Firefox 17 以降でサポート
      - Opera：Opera 12 以降でサポート
      - Safari：Mac OS X Mavericks 以降でサポート
      - Internet Explorer：Windows 10 IE 以降でサポート予定
  - 改訂後

    以上のように、HTTPS で安全にサービスを提供したい場合などでは、ユーザに意識させることなくミスを防止でき、ユーザの利便性を向上させることができるので、HSTS の機能を持っているならば有効にすることを推奨する。

    なお、HSTS はサーバ、クライアント（ブラウザ）ともに、2018 年 3 月時点の最新バージョンではすべてサポートされている。
  - 調査根拠
    - ✓ 4.1③（7.2.1 節）HTTP Strict Transport Security（HSTS）に係る実装状況

---

[14] 例えば https://keytester.cryptosense.com/や https://keychest.net/roca がある。ただし、安全性を 100%証明するものではないことに注意されたい

- 7.2.4　OCSP Stapling の設定有効化
  - 改訂前

    なお、OCSP Stapling は 2014 年 9 月時点で以下の環境においてサポートされている。参考までに、いくつかの設定例を Appendix B.5 で紹介する。

    - サーバ
      - Apache HTTP Server 2.3.3 以降
      - nginx 1.3.7 以降
      - Microsoft IIS on Windows Server 2008 以降

      など
    - クライアント（ブラウザ）
      - Mozilla Firefox 26 以降
      - Microsoft Internet Explorer （Windows Vista 以降）
      - Google Chrome
  - 改訂後

    なお、OCSP Stapling はサーバ、クライアント（ブラウザ）ともに、2018 年 3 月時点の最新バージョンではすべてサポートされている。
  - 調査根拠
    - ✓ 4.1③（7.2.4 節）OCSP Stapling に係る実装状況
- 7.2.5　Public Key Pinning の設定有効化
  - 改訂前

    2014 年 9 月時点で、Public Key Pinning をサポートしている環境は以下の通りである。
    - サーバ
      - HTTP ヘッダを追加可能な任意のサーバ
    - クライアント
      - Google Chrome 13 以降
      - Mozilla Firefox 32 以降（デスクトップ版）、34 以降（Android 版）
      - Internet Explorer： マイクロソフト脆弱性緩和ツール（EMET[15]） を導入することで設定可能（EMET バージョン 4.0 以降よりサポート）

    期待されるハッシュ値の提供方法には 2 通りある。

    1) ブラウザのソースコードに主要なサイトの SPKI フィールドの情報のハッシュ値リストを保持し、これと比較して SSL サーバ証明書が正当であるかを調べるもの。2014 年 9 月時点では Google Chrome や Mozilla Firefox がサポートしている。

    2) サイトから送られる HTTP ヘッダに含まれる、SSL サーバ証明書の SPKI

[15] http://technet.microsoft.com/ja-jp/security/jj653751

フィールドの情報のハッシュ値を元に正当性を比較するもの。IETF において、Public Key Pinning Extension for HTTP として発行された。参考までに、いくつかの設定例を Appendix B.6 で紹介する。

- ➢ 改訂後

  ただし、導入が進んでいない。

  - ➢ Google Chrome 67 からサポートをやめる予定
  - ➢ Mozilla Firefox 35 からサポートされている

- ➢ 調査根拠
  - ✓ 4.1③（7.2.5 節）Public Key Pinning に係る実装状況

● 8.1 本ガイドラインが対象とするブラウザ

・ P55 8.1.1 対象とするプラットフォーム

- ➢ 改訂前
  - ● デスクトップ向け OS
    - ✓ Windows Vista Service Pack 2 （2017 年 4 月 11 日サポート終了）
    - ✓ Windows 7 Service Pack 1 （2020 年 4 月 11 日サポート終了）
    - ✓ Windows 8 （2016 年 1 月 12 日サポート終了）
    - ✓ Windows 8.1 （2023 年 1 月 10 日サポート終了）
    - ✓ Mac OS X 10.9
  - ● スマートフォン向け OS
    - ✓ 当該端末で利用できる最新の Android（もっとも古いもので Android4.x）
    - ✓ iOS 8
- ➢ 改訂後
  - ● デスクトップ向け OS
    - ✓ Windows 7 Service Pack 1 （2020 年 4 月 11 日サポート終了）
    - ✓ Windows 8.1 （2023 年 1 月 10 日サポート終了）
    - ✓ Windows 10（2025 年 10 月 14 日サポート終了）
    - ✓ OS X El Capitan（10.11）（2017 年 12 月 6 日最終アップデート）
    - ✓ macOS Sierra（10.12）（2017 年 12 月 6 日最終アップデート）
    - ✓ macOS High Sierra（10.13）（2017 年 12 月 6 日最終アップデート）
  - ● スマートフォン向け OS
    - ✓ 当該端末で利用できる最新の Android（2018 年 3 月時点で最新 ver.は Android 8.x）
    - ✓ 当該端末で利用できる最新の iOS（2018 年 3 月時点で最新 ver.は iOS 11.x）
- ➢ 調査根拠
  - ✓ 4.1①（5）

- ✓ 4.1②
- ✓ 4.1③（8.1.1 節）主要 OS に係るサポート状況

・ P55　8.1.2　対象とするブラウザのバージョン

➢ 改訂前

● Microsoft Internet Explorer

2016 年 1 月 12 日以降は、サポートされるオペレーティングシステムで利用できる最新バージョンの Internet Explorer のみがテクニカルサポートとセキュリティ更新プログラムを提供されるようになる（表 1）。詳細は、以下を参照のこと。

Microsoft Internet Explorer サポート ライフサイクル ポリシーに関する FAQ
http://support2.microsoft.com/gp/microsoft-internet-explorer

● Microsoft Internet Explorer 以外のブラウザ

- ✓ Apple Safari 最新版
- ✓ Google Chrome 最新版
- ✓ Mozilla Firefox 最新版
- ✓ Mobile Safari（iOS）：iOS 8 に搭載する Mobile Safari

表 1　Internet Explorer のサポート期間

ブラウザバージョン	OSバージョン	サポート期間（ライフサイクルポリシー@2014年11月10日時点）
		2015 / 2016 / 2017 / 2018 / 2019 / 2020 / 2021 / 2022 / 2023
Internet Explorer 7	Windows Vista SP2	2016/1/12
Internet Explorer 8	Windows Vista SP2	2016/1/12
	Windows 7 SP1	2016/1/12
Internet Explorer 9	Windows Vista SP2	2017/4/11
	Windows 7 SP1	2016/1/12
Internet Explorer 10	Windows 7 SP1	2016/1/12
	Windows 8	2016/1/12
Internet Explorer 11	Windows 7 SP1	2020/1/14
	Windows 8.1	2023/1/10

➢ 改訂後

● Microsoft Internet Explorer 11

● Microsoft Edge

- ● Apple Safari 最新版
- ● Google Chrome 最新版
- ● Mozilla Firefox 最新版
- ● Mobile Safari（iOS）

➢ 調査根拠

- ✓ 4.1①（5）

✓ 4.1③（8.1.2 節）Microsoft Internet Explorer 及び Edge のサポート状況

- 8.2 設定に関する確認項目

・ P56 8.2.2 設定項目 設定項目を標準機能で提供していないブラウザ

➢ 改訂前

以下のブラウザは、設定変更オプションが提供されておらず、そもそも設定変更ができない。

- PC 版 Web ブラウザ
  - ➢ Apple Safari
  - ➢ Google Chrome
- スマートフォンに含まれる Web ブラウザ
  - ➢ Android 標準ブラウザ

Mobile Safari (iOS)

➢ 改訂後

以下のブラウザは、設定変更オプションが提供されておらず、そもそも設定変更ができない。

- PC 版 Web ブラウザ
  - ➢ Apple Safari
  - ➢ Google Chrome
- スマートフォンに含まれる Web ブラウザ
  - ➢ Google Chrome
  - ➢ Mobile Safari (iOS)

➢ 調査根拠

✓ 4.1①（5）

・ P56 8.2.2 設定項目 設定項目を標準機能で提供しているブラウザ

➢ 改訂前

- Microsoft Internet Explorer

他のブラウザとは異なり、Internet Explorer では、

“ツール”→“インターネットオプション”→“詳細設定”

を選択すると多数の設定項目が表示され、ユーザが細かく設定できるようになってはいる。

しかし、安全性を考慮してデフォルト設定が行われていることから、特段の理由がない場合には“プロトコルバージョンの設定を除いて”設定を変更することは推奨しない。

なお、Internet Explorer のセキュリティ機能及びデフォルト設定については、以下に一覧としてまとめられている。

バージョン別 IE のセキュリティ機能

http://msdn.microsoft.com/ja-jp/ie/cc844005.aspx

【プロトコルバージョンの設定】

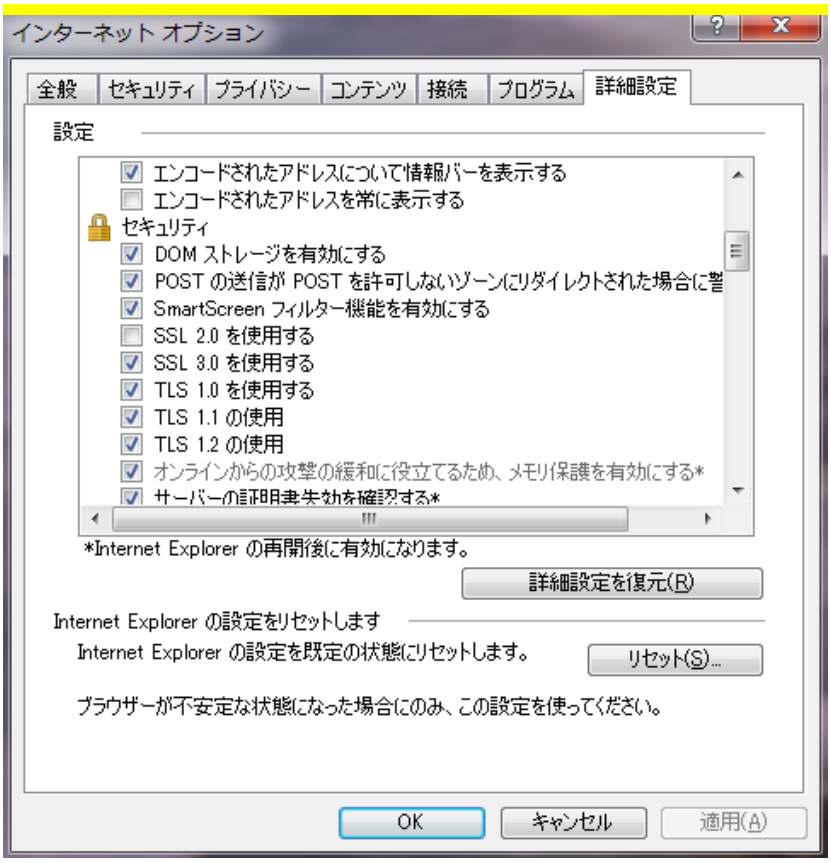
“ツール”→“インターネットオプション”→“詳細設定”を選択した後、設定項目を“セキュリティ”までスクロールさせると、「SSL2.0 を使用する」「SSL3.0 を使用する」「TLS1.0 を使用する」「TLS1.1 を使用」「TLS1.2 を使用」といったチェックボックスが表示される。ここでのチェックボックスにチェックが入っているプロトコルバージョンが、ブラウザが使うことができるプロトコルバージョンとなる。

本ガイドライン公開時点（2015 年 5 月）のデフォルト設定では、IE6 では「SSL2.0 を使用する」にチェックが入っている一方、IE8 以降では TLS1.1 や TLS1.2 をサポートしているものの「TLS1.1 を使用」「TLS1.2 を使用」にはチェックが入っていない。

このように、Internet Explorer は使うバージョンによって利用できるプロトコルバージョンが異なるので、プロトコルバージョンについてのみ、適切な設定になっているかを確認し、必要に応じて設定変更することを推奨する。

	TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
IE6（参考）	×	×	▲	○	○
IE7	×	×	○	○	▲
IE8	▲	▲	○	○	▲
IE9	▲	▲	○	○	▲
IE10	▲	▲	○	○	▲
IE11	▲	▲	○	○	▲

○：デフォルト設定 ON　▲：デフォルト設定 OFF　×：サポートしていない



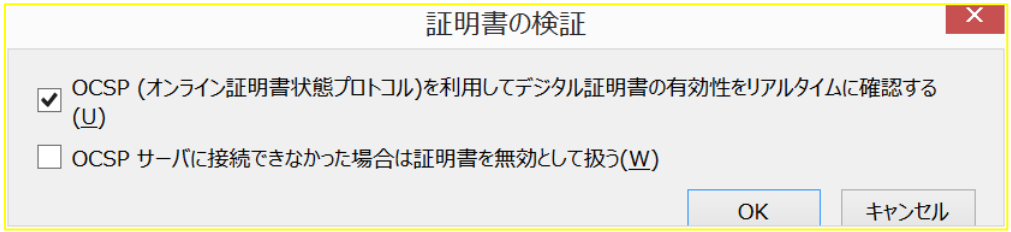
- Firefox

  Firefox では、サーバ証明書の検証、失効機能においてどのように処理するかの動作についてのみ設定方法を提供している。この設定については、

  “メニュー” → “オプション” → “詳細” → “証明書” → “検証(V)…”

  を選択することで設定方法へのダイアログが表示される。

  デフォルトの設定は以下のようになっており、特段の理由がない場合に変更することは推奨しない。



➢ 改訂後

- Microsoft Internet Explorer

  他のブラウザとは異なり、Internet Explorer では、

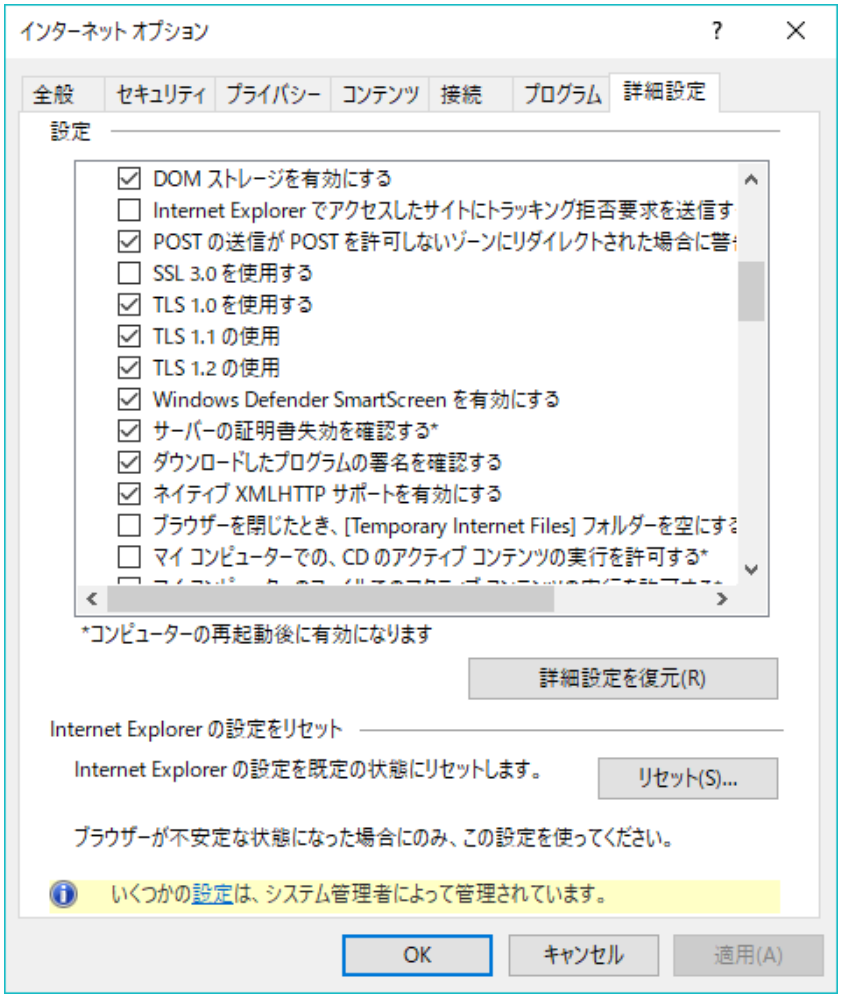
  “ツール” → “インターネットオプション” → “詳細設定”

  を選択すると多数の設定項目が表示され、ユーザが細かく設定できるようになってはいる。

しかし、安全性を考慮してデフォルト設定が行われていることから、特段の理由がない場合には、設定を変更することは推奨しない。

【プロトコルバージョンの設定】

“ツール”→“インターネットオプション”→“詳細設定”を選択した後、設定項目を“セキュリティ”までスクロールさせると、「SSL3.0 を使用する」「TLS1.0 を使用する」「TLS1.1 を使用」「TLS1.2 を使用」などといったチェックボックスが表示される。ここでのチェックボックスにチェックが入っているプロトコルバージョンが、ブラウザが使うことができるプロトコルバージョンとなる。以下は、windows10 IE11 の設定画面である。



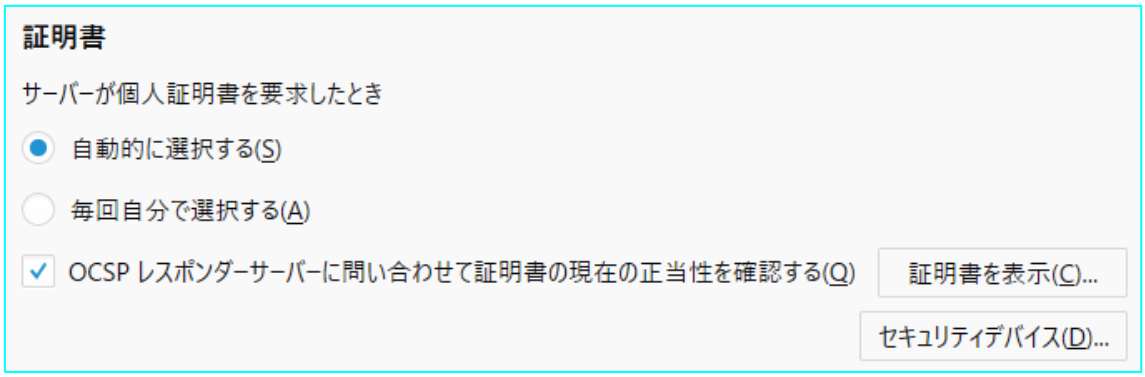
- Firefox

Firefox では、サーバ証明書の検証、失効機能においてどのように処理するかの動作についてのみ設定方法を提供している。この設定については、

“メニュー”→“オプション”→“プライバシーとセキュリティ”→“証明書”で選択することで設定のチェックボックスが表示される。

デフォルトの設定は以下のようになっており、特段の理由がない場合に変更

することは推奨しない。



- 調査根拠
  - ✓ 4.1①（5）

- 8.3.1　鍵長 1024 ビット、SHA-1 を利用するサーバ証明書の警告表示
  - 改訂前

    8.3.1　鍵長 1024 ビット、SHA-1 を利用するサーバ証明書の警告表示

    CA/Browser Forum にて、サーバ証明書の有効期限が 2014 年 1 月 1 日以降の場合、RSA の鍵長を最小 2048 ビットにすると決められている。このため、ブラウザベンダ各社では、RSA の鍵長が 2048 ビット未満のものは順次無効にする対処がされている。また、SHA-1 についても、順次無効化する対処が予定されている。

    詳しくは以下のとおりである。

    - Microsoft Internet Explorer

      2017 年 1 月 1 日より SHA-1 で署名されたサーバ証明書を受け付けない [16]。詳細は別途追記予定

    - Google Chrome

      Chrome 39 より順次、SHA-1 で署名されたサーバ証明書については、アドレスバーの鍵アイコンが別表記になる [17,18]。以下のようにサーバ証明書の有効期限によって表記は変化する。

バージョン	サーバ証明書の有効期限	アドレスバーの鍵アイコンの表記
39	2017 年 1 月 1 日以降	黄色い三角アイコン
40	2016 年 6 月 1 日～12 月 31 日	黄色い三角アイコン
	2017 年 1 月 1 日以降	HTTP と同様の表示
42	2016 年 1 月 1 日～12 月 31 日	黄色い三角アイコン
	2017 年 1 月 1 日以降	赤い×アイコン

    - Firefox

[16] http://blogs.technet.com/b/pki/archive/2013/11/12/sha1-deprecation-policy.aspx
[17] http://blog.chromium.org/2014/09/gradually-sunsetting-sha-1.html
[18] https://groups.google.com/a/chromium.org/forum/#!topic/security-dev/QNVVo4_dyQE

2014 年以降、SSL/TLS で利用される RSA の鍵長が 2048 ビットに満たないルート証明書は順次無効になり、2015 年の中頃までにはすべてで無効になる [19]。

また SHA-1 で署名されたサーバ証明書についても、2015 年以降にリリースされる最新版の Firefox では、以下のように変更をする予定である [20]。

バージョン	サーバ証明書の有効期限	アドレスバーの鍵アイコンの表記
2015 年以降のバージョン	2017 年 1 月 1 日以降	警告表示をする UI を追加
2016 年以降のバージョン	2017 年 1 月 1 日以降	“接続の安全性を確認できません”と表示
2017 年以降のバージョン	すべて	“接続の安全性を確認できません”と表示

- 改訂後

8.3.1　SHA-1 を利用するサーバ証明書に対する無効化

CA/Browser Forum では、2016 年 1 月 1 日以降、商用 CA は SHA-1 のサーバ証明書を発行しないことが決められている。このため、ブラウザベンダ各社では、SHA-1 のサーバ証明書は無効化する対処がされている。

詳しくは以下のとおりである。

- Microsoft Internet Explorer

  2017 年 5 月 9 日に公開した更新版で、IE11、Edge で SHA-1 を無効化している [21]が、サポートはしている。

- Google Chrome

  Chrome56 から SHA-1 を無効化している [22]が、サポートはしている。

- Firefox

  Firefox36 から SHA-1 を無効化している [23]が、サポートはしている。

- 調査根拠
  - ✓ 4.1①（5）

- 8.3.2　SSL3.0 の取り扱い
  - 改訂前

[19] https://wiki.mozilla.org/CA:MD5and1024
[20] https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signaturealgorithms/
[21] https://technet.microsoft.com/ja-jp/library/security/4010323
[22] https://security.googleblog.com/2016/11/sha-1-certificates-in-chrome.html
[23] https://www.fxsitecompat.com/en-CA/docs/2016/sha-1-certificates-issued-by-public-ca-will-no-longer-be-accepted/

8.3.2　SSL3.0 の取り扱い

POODLE 攻撃の公表を受け、各ブラウザベンダは順次 SSL3.0 を利用不可とする対処を取り始めている。

- Internet Explorer

  セキュリティ情報 MS15-032「Internet Explorer 用の累積的なセキュリティ更新プログラム （3038314）」により、Internet Explorer 11 では SSL3.0 がデフォルトで無効になっている。

  それ以外のバージョンの Internet Explorer では、設定を変更することにより、SSL3.0 を無効化することができる。詳しくは、下記 URL のマイクロソフトセキュリティアドバイザリを参照のこと。

  マイクロソフト セキュリティ アドバイザリ 3009008

  https://technet.microsoft.com/ja-jp/library/security/3009008.aspx

- Google Chrome

  Chrome 40 からデフォルトで SSL3.0 が無効化されている。

- Firefox

  Firefox 34 および Firefox ESR 31.3.0 からデフォルトで SSL3.0 が無効化されている。

➢ 改訂後

（全削除）

➢ 調査根拠

✓ 4.1①（5）

● 新規　8.3.3　RC4 と TripleDES の取り扱い

➢ 改訂前

なし。

➢ 改訂後

8.3.3　RC4 の取り扱い

RC4、および、TripleDES の危殆化の状況を受け、各ブラウザベンダでは、RC4 を利用不可とする対処を取り始めている。

➢ 調査根拠

✓ 4. 1①（5）

II.　コラムに係る記述のアップデート

SSL/TLS 暗号設定ガイドライン v1.1 に掲載されている 4 つのコラムのうち、

➢ 【コラム③】　輸出規制時代の名残－FREAK 攻撃

➢ 【コラム④】　DigiNotar 認証局事件

について、以下の内容に改訂することを提案する。

- 改訂案 1　Measuring HTTPS Adoption on the Web
  26th USENIX Security Symposium August 16–18, 2017 • Vancouver, BC, Canada
  - ✓ 2017 年 8 月 16 から 18 日の 26th　USENIX Security Symposium で、Measuring HTTPS Adoption on the Web という論文が発表された
  - ✓ 東アジア諸国は特に HTTPS の普及率が低く、インターネット利用率の高い 13 ヵ国のうち、韓国と日本が HTTPS の普及率の最下位 2 ヵ国である調査結果が掲載されていた
  - ✓ インターネットプライバシーを強化するためにも、HTTPS の普及を進めるべきであると言及されていた
- 改訂案 2　Symantec のサーバ証明書が Chrome と Firefox で無効化
  - ✓ @IT で、Symantec のサーバ証明書が Chrome と Firefox で無効化されるという記事が掲載されている。

    Symantec の証明書発行事業における一部のパートナー企業が、明らかに不正なドメイン名をコモンネーム（共通名）に持つ証明書を発行していたなど、不適切な証明書の取り扱いが発覚したことだ。パートナーと言っても、証明書の発行には Symantec のシステムが用いられ、また同社の認証局が信頼の連鎖におけるルートとなっていた。
    この事態を重く見た Google と Mozilla は、Symantec との協議を経て、Symantec のシステムから発行された全ての証明書を丸ごとごっそり、将来的に Google Chrome や Mozilla Firefox などで信頼しないようにすることを決定した。
    ---
    http://www.atmarkit.co.jp/ait/articles/1712/01/news033.html
  - ✓ Google Security Blog で、Chrome は 2018 年 3 月（Chrome 66）に 2016 年 6 月 1 日より前に発行された Symantec の証明書を無効化し、2018 年 10 月（Chrome 70）には Symantec のすべての証明書を無効化することを公表している。
    https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html
  - ✓ mozilla wiki で、Firefox は 2018 年 5 月（Firefox 60）に 2016 年 6 月 1 日より前に発行された Symantec の証明書を無効化し、2018 年 10 月（Firefox 63）には Symantec のすべての証明書を無効化することを公表している。
    https://wiki.mozilla.org/CA:Symantec_Issues
- 調査根拠
  - ✓ 4.1④

III. 付録・脚注に係る記述のアップデート

付録に係る記述の改訂案は、別紙 2 として添付した。