■ファイル概要

「1.2.1.5 主要ブラウザでのSSL/TLSに関するサポート状況の調査」をまとめたもの。

■シート一覧

No.	シート名	内容
1	調査結果(5)	1.2.1.5に対する調査結果。各ブラウザのセキュリティサポート状況。
2	公式サイト一覧 (5)	公式サイトとして扱うサイトの一覧。

■Google Chrome

項目	調査結果	記載内容	信頼度	URL	備考
プロトコルバージョン	TLS1.0, TLS1.1, TLS1.2 設定方法： UIは用意されていない。 コマンドラインオプションから、バージョンの指定(Max, Min)はできるようだが推奨していない。	SSLv3はサポートされない [引用：SSLv3 is no longer supported in Chrome.]	高	http://www.chromium.org/Home/chromium-security/education/tls	
		Chrome 39からデフォルトでSSLv3は使用不可 [引用：In Chrome 39 (the next version), fallback to SSLv3 will be disabled by default.]	中	https://groups.google.com/a/chromium.org/forum/#!topic/security-dev/Vnhy9aKM_I4	GoogleグループのSecurity-devフォーラムの1トピック内での記述なので、一応信頼度は「中」にしている
		Chrome 40からSSLv3を完全に使用できないようにする [引用：In Chrome 40, we plan on disabling SSLv3 completely, although we are keeping an eye on compatibility issues that may arise.]	中		
		Chrome 44からSSLv3のサポート停止 [引用：SSLv3 support will be entirely removed from Chrome in version 44 (around July 2015) after which the setting "ssl3" will be ignored in favor of the then-current default.)	中	https://bugs.chromium.org/p/chromium/issues/detail?id=436391	バグチケット
		SSLVersionMaxポリシに「tls1.2」が指定できる [引用：(SSLVersionMaxポリシの項目) it may be set to one of the following values: "tls1.2" or "tls1.3". When set, Google Chrome will not use SSL/TLS versions greater than the specified version. An unrecognized value will be ignored.]	高	http://www.chromium.org/administrators/policy-list-3	
		指定しない場合はSSLの最大のバージョンを使用 [引用：If this policy is not configured then Google Chrome uses the default maximum version.]	高		
		ChromeはSSL/TLSオプションを設定するUIを意図的に提供していない。コマンドラインオプションからできるが、その使用は推奨しない。(※) [引用：Chrom[e/ium] intentionally does not provide UI to configure SSL/TLS options (we previously did). There are a set of command-line options for testing, but those are not 'supported', in that we don't recommend users use these (invariably, when people use these, it's to weaken security, unfortunately).]	中	https://bugs.chromium.org/p/chromium/issues/detail?id=391955	
		コマンドラインオプション一覧に--ssl-version-max/minがある。 [引用：List of Chromium Command Line Switches] [引用：--ssl-version-max … Specifies the maximum SSL/TLS version ("tls1", "tls1.1", "tls1.2", or "tls1.3"). --ssl-version-min … Specifies the minimum SSL/TLS version ("tls1", "tls1.1", "tls1.2", or "tls1.3").]	低	https://peter.sh/experiments/chromium-command-line-switches/	個人のページのようだが、自動更新しているとのこと。 (Last automated update occurred on 2018-01-16.)
暗号スイート	追加・削除：不可 優先度変更：不可 設定方法： 追加削除、優先度変更のインタフェースはない。	SSL/TLSの暗号スイートの優先度を変更するインタフェースがない [引用：there is no interface today to prioritize individual SSL/TLS cipher suites.]	中	https://bugs.chromium.org/p/chromium/issues/detail?id=58833	バグチケット
		SSL/TLSの暗号スイートの使用・不使用を変更するインタフェースがない [引用：Currently, Chrome does not offer any interface for enabling or disabling individual SSL/TLS cipher suites, either through the UI or through the administrative policies.]	中	https://bugs.chromium.org/p/chromium/issues/detail?id=58831	バグチケット
	起動時オプションで禁止できるが、上記(※)よりコマンドラインオプションは推奨されていない	特定のアルゴリズムを禁止 アプリケーション起動時のオプションで、ブラックリストをHex表記で記述する。 "C:¥Program Files¥Google¥Chrome¥Application¥chrome.exe" --cipher-suite-blacklist=0xc007,0xc011,0x0005,0x0004	低	http://d.hatena.ne.jp/tosi29/20140720/1405854774	個人サイト
		Chrome 6からWindowsで設定した暗号スイート設定が反映されなくなった [引用：In Chrome 5 and earlier, this could be managed on Windows by configuring the Schannel cipher suites (http://msdn.microsoft.com/en-us/library/bb870930(VS.85).aspx). Since Chrome 6, which saw the switch to NSS as the default SSL library, this is no longer possible, unless either "--use-system-ssl" is specified on the command-line (an unsupported option), or the server requests client certificate authentication (which will cause Chrome to fall back to Schannel).]	中	https://bugs.chromium.org/p/chromium/issues/detail?id=58831	・Chrome 5まではWindowsの設定を流用していて、6からはChromeが採用したライブラリの設定を使っている模様（一つ下の情報も参照）
		Chrome 5まではCryptoAPI/CNG (WindowsのAPI) を使用していて、6でNSSに移行した [引用：Windows版のGoogle Chromeの暗号モジュールがCryptoAPI/CNGからMozillaのNSSに変更になったそうで、そのおかげでCamelliaを使ったCipher Suitesにも対応するようになったそうです。]	低	http://blog.livedoor.jp/k_urushima/archives/1489528.html	個人サイト
サーバ証明書の利用期間	SHA-1証明書は使用不可	Chrome 56からSHA-1証明書のサポートをやめる [引用：We are planning to remove support for SHA-1 certificates in Chrome 56, which will be released to the stable channel around the end of January 2017.]	高	http://www.chromium.org/Home/chromium-security/education/tls/sha-1	
		[引用： Step 1: Blocking new SHA-1 certificates Starting in early 2016 with Chrome version 48, Chrome will display a certificate error if it encounters a site with a leaf certificate Step 2: Blocking all SHA-1 certificates Starting January 1, 2017 at the latest, Chrome will completely stop supporting SHA-1 certificates.]	高	https://security.googleblog.com/2015/12/an-update-on-sha-1-certificates-in.html	
表示方法の変更	(Chrome 63) ・緑の錠前：保護された通信 ・〇の中に「i」：情報、または保護されていない通信 ・赤三角に「!」：保護されていない通信、または危険	「安全性を示すアイコンの意味」の節に説明がある	高	https://support.google.com/chrome/answer/95617?hl=ja	
	(Chrome 46) ①緑の錠前：Secure HTTPS ②白紙：HTTP、HTTPS with minor errors ③灰色の錠前＋ばつ印＋httpsに取り消し線：Broken HTTPS [参考]mixedコンテンツ：②白紙になることを確認済み https://www.noble-system.com/~ssl/?product=geotrust-true-businessid-san-ev%EF%BC%88%EF%BC%91%E5%B9%B4%EF%BC%89-2	アイコンの説明がある HTTPからHTTPSの移行の間、mixedコンテンツになることがあるがほとんどの場合安全性は低くならないので、黄色三角警告バッジを削除した [引用：(Not) Warning About Mixed Content This change will mainly affect HTTPS pages that contain certain mixed content, such as HTTP images. Site operators face a dilemma: Switching an HTTP site to HTTPS can initially result in mixed content, which is undesirable in the long term but important for debugging the migration. During this process the site may not be fully secured, but it will usually not be less secure than before. Removing the yellow “caution triangle” badge means that most users will not perceive a warning on mixed content pages during such a migration. We hope that this will encourage site operators to switch to HTTPS sooner rather than later.]	高	https://security.googleblog.com/2015/10/simplifying-page-security-icon-in-chrome.html	・Chromeのセキュリティアイコンの単純化 (Simplifying the Page Security Icon in Chrome) というページ ・Chrome 63でデザインは変わっても、アイコンの区別は変わっていないと思われる
EV-SSL証明書の取り扱い方法	・Certificate Transparency(CT)に準拠している必要がある ・有効の場合はグリーンバーで表示される	2015年1月1日からEV証明書にCertificate Transparencyを要求 [引用：From 1 January 2015, Google Chrome requires all EV certificates to use Certificate Transparency.]	高	http://www.chromium.org/Home/chromium-security/root-ca-policy	Certificate Transparency(CT)は、Google社が提唱したSSL/TLSの信頼性を高めるための技術(RFC6962) ・Symantecによる解説 (https://www.symantec.com/ja/jp/page.jsp%3Fid=ssl-certificate-transparency) ・CTの公式ページ (http://www.certificate-transparency.org/ev-ct-plan)
EV-SSL証明書でグリーンバーにならない条件	Certificate Transparency(CT)がない場合	証明書やステープルされたOCSP応答にCTが含まれない場合、Chromeにグリーンバーを表示しない [引用：If a CT proof is not included either in the Certificate or as part of an OCSP stapled response, the EV certificate will not display the green address bar in Chrome.]	低	https://www.digicert.com/blog/certificate-transparency-required-ev-certificates-show-green-address-bar-chrome/	Digicert社のブログ

Symantec発行の証明書の信頼を破棄	経緯 ・2015年、2014年9月にSymantec子会社がgoogleドメインのEV証明書をテスト目的で不正に発行したことが、Certificate Transparency(CT)ログから判明した。 ・Chromeが不正に発行された証明書を無効として扱うようにした	[引用：Improved Digital Certificate Security　（September 18, 2015の記事） On September 14, around 19:20 GMT, Symantec's Thawte-branded CA issued an Extended Validation (EV) pre-certificate for the domains google.com and www.google.com. This pre-certificate was neither requested nor authorized by Google. We discovered this issuance via Certificate Transparency logs, which Chrome has required for EV certificates starting January 1st of this year. The issuance of this pre-certificate was recorded in both Google-operated and DigiCert-operated logs. During our ongoing discussions with Symantec we determined that the issuance occurred during a Symantec-internal testing process. We have updated Chrome's revocation metadata to include the public key of the misissued certificate. Additionally, the issued pre-certificate was valid only for one day.]	高	https://security.googleblog.com/2015/09/improved-digital-certificate-security.html	
		[引用：Sustaining Digital Certificate Security (October 28, 2015の記事） Therefore we are firstly going to require that as of June 1st, 2016, all certificates issued by Symantec itself will be required to support Certificate Transparency.]	高	https://security.googleblog.com/2015/10/sustaining-digital-certificate-security.html	
	経緯（続き） ・2017年1月、mozilla.dev.security.policy newsgroupへの投稿で、Symantec PKIがCA/Browser Forum Baseline Requirementsに準拠していない証明書を多数発行していることが判明した。 現状 ・Chrome 66以降、2016年6月1日以前に発行されたSymantecの証明書は無効 ・Chrome 70以降、すべてのSymantecの証明書は無効	Chrome 66 以降、Symantec によって 2016 年 6 月 1 日より前に発行された証明書に対する信頼が破棄されます。 [引用：(September 11, 2017の記事） Symantec's PKI business, which operates a series of Certificate Authorities under various brand names, including Thawte, VeriSign, Equifax, GeoTrust, and RapidSSL, had issued numerous certificates that did not comply with the industry-developed CA/Browser Forum Baseline Requirements. This incident, while distinct from a previous incident in 2015, was part of a continuing pattern of issues over the past several years that has caused the Chrome team to lose confidence in the trustworthiness of Symantec's infrastructure, and as a result, the certificates that have been or will be issued from it. Starting with Chrome 66, Chrome will remove trust in Symantec-issued certificates issued prior to June 1, 2016.]	高	https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html	(2017/12/22:ARK) TODO:「なぜSymatecの署名書の信頼を破棄するか」という内容を報告に追加する (2017/12/25:ARK) ・左記URLのページ内で「Symantecの証明を信頼できなくなった」というコメントがあり、その理由も記載されているため、そのあたりを中心にまとめる予定。
		Symantec の古いインフラストラクチャとそれらが発行したすべての証明書に対する信頼が完全に破棄される Chrome 70 は、2018 年 10 月 23 日の週前後にリリースされる予定です。 [引用：Around the week of October 23, 2018, Chrome 70 will be released, which will fully remove trust in Symantec's old infrastructure and all of the certificates it has issued.]	高		
		Google ChromeやMozilla Firefox：信頼しない Microsoft（Internet ExplorerやEdge）やApple（Safari）：発表なし [引用：Chromeで信頼されなくなるSymantec発行のSSL証明書かどうか判定・確認する方法（2017年12月01日の記事） 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。 　Mozilla Firefoxも多少の違いはあるものの、同様のスケジュールでSymantec発行の証明書を信頼しなくなる予定だ。 　一方、Microsoft（Internet ExplorerやEdge）やApple（Safari）については、本件について特に発表はない。]	低	http://www.atmarkit.co.jp/ait/articles/1712/01/news033.html	@ITの記事
ブラウザサポート終了時	調査中（なし？）				

■Firefox

項目	調査結果	記載内容	信頼度	URL	備考
プロトコルバージョン	TLS1.0, TLS1.1, TLS1.2 設定方法： TLSバージョンの最小・最大をabout:configから設定可能	Firefox 34.0でSSL3.0 が利用できなくなった [引用：SSLv3 が利用できなくなりました。]	高	https://www.mozilla.jp/firefox/34.0/releasenotes/	
		Firefox 39.0でSSL3.0のサポート終了 [引用：安全上の問題があるため SSLv3 のサポートを終了しました]	高	https://www.mozilla.jp/firefox/39.0/releasenotes/	
		SSL3.0、TLS1.0がサポートされているが、SSL3.0を不使用に、TLS1.0～TLS1.2を使用できる(about:config) [引用：SSL 3.0 and TLS 1.0 are currently supported by default.] [引用：You can disable SSL 3.0 or enable TLS 1.1/1.2 by using these preferences, or enforce the use of a specific protocol version.]	中	http://kb.mozillazine.org/Security.tls.version.%2A	Mozillazineはユーザコミュニティによってつくられたもののようだが、MDNがMozillazineをリンクしているため信頼度は「中」にしている。
暗号スイート	追加・削除：可 設定方法： about:configから設定可能	「security. (ssl2 or ssl3). (cipher suite)」メソッドで使用・不使用を設定できる	中	http://kb.mozillazine.org/About:config_entries	同上
サーバ証明書の利用期間	・SHA-1証明書に対して信頼できない接続のエラーを表示する	2017年1月1日から、SHA-1証明書に対しては信頼できない接続のエラーを表示する [引用：We plan to add a security warning to the Web Console to remind developers that they should not be using a SHA-1 based certificate.]	高	https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/	
	・Firefox 36で、1024-bit RSAのルート証明書は無効	Firefox 36で、1024-bit RSAのルート証明書は削除された [引用：In the previous post about certificates with 1024-bit RSA keys we said that the changes for the second phase of migrating off of 1024-bit root certificates were planned to be released in Firefox in early 2015. These changes have been made in Firefox 36, in which the following 1024-bit root certificates were either removed, or their SSL and Code Signing trust bits were turned off.]	高	https://blog.mozilla.org/security/2015/01/28/phase-2-phasing-out-certificates-with-1024-bit-rsa-keys/	
表示方法の変更	(Firefox 42) ①緑の錠前：DV証明書 ②緑の錠前＋組織名：EV証明書 ③灰色の錠前＋赤い斜線：能動的な混在コンテンツ(そのHTTPS ページのすべて、ないしは DOM の一部にアクセスできるコンテンツ)がある ④灰色の錠前＋黄色三角の中に!：受動的な混在コンテンツ(HTTPS の web ページの中で HTTP 経由で送信されるコンテンツ)がある	Firefox 42での表示変更(Updated Firefox Security Indicators)	高	https://blog.mozilla.org/security/2015/11/03/updated-firefox-security-indicators-2/	
	(Firefox 57) 上記と同じ(デザインが変わっている) [参考]mixedコンテンツ：④灰色の錠前＋黄色三角の中に! になることを確認済み https://www.noble-system.com/~ssl/?product=geotrust-true-businessid-san-ev%EF%BC%88%EF%BC%91%E5%B9%B4%EF%BC%89-2	アイコンの説明がある	高	https://support.mozilla.org/ja/kb/how-do-i-tell-if-my-connection-is-secure https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure	「ウェブサイトへの接続が安全かどうかはどうすればわかりますか？(How do I tell if my connection to a website is secure?)」というヘルプページ
EV-SSL証明書の取り扱い方法	・グリーンバーで表示される	緑色の錠前に会社または組織名が緑色で表示されているのは、そのサイトがEV証明書を使用していることを表す。 [引用：A green padlock plus the name of the company or organization, also in green, means this website is using an Extended Validation (EV) certificate.]	高	https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure	
Symantec発行の証明書の信頼を破棄	October 2018 (Firefox 63)：Symantec ルート証明書を無効にする	[引用：CA:Symantec Issues Following the investigation documented below, a consensus proposal was reached among multiple browser makers for a graduated distrust of Symantec roots. The dates in that proposal and how they apply to Mozilla's Root Program and Firefox are as follows: ①December 1st, 2017: Symantec to implement "Managed CA" proposal ②January 2018 (Firefox 58): Notices in the Developer Console will warn about Symantec certificates issued before 2016-06-01, to encourage site owners to migrate their TLS certs. ③May 2018 (Firefox 60): Websites will show an untrusted connection error if they have a TLS cert issued before 2016-06-01 that chains up to a Symantec root. ④October 2018 (Firefox 63): Removal/distrust of Symantec roots, with caveats described below.]	高	https://wiki.mozilla.org/CA:Symantec_Issues	
EV-SSL証明書でグリーンバーにならない条件	・特にないと思われる(情報なし) ・CT (Google Chrome参照) はサポートしていない	2016/11/4にCertificate Transparency(CT)対応検討のため、Googleグループのフォーラム上にトピックがつくられた [引用：CT is coming to Firefox. As part of that, Mozilla needs to have a set of CT policies surrounding how that will work.]	中	https://groups.google.com/forum/#!msg/mozilla.dev.security.policy/VJYX1Wnnhiw/ZaJBaKfKBQAJ	サポート時期は明記されていないので、未対応と考えられる
ブラウザサポート終了時期	非公表と思われる(情報なし)				

■Internet Explorer

項目	調査結果	記載内容	信頼度	URL	備考
プロトコルバージョン	SSL3.0, TLS1.0, TLS1.1, TLS1.2 ただし、SSL3.0はデフォルトで不使用 設定方法： インターネットオプションから可能	SSL3.0, TLS1.0, TLS1.1, TLS1.2の仕様をレジストリに設定するサブキーが記載されている	高	https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings	「Transport Layer Security (TLS) registry settings」というページ
		Windows 10 (v1607) 以降はSSL3.0はデフォルトで無効 [引用：Beginning with Windows 10, version 1607 and Windows Server 2016, SSL 3.0 has been disabled by default. For SSL 3.0 default settings, see Protocols in the TLS/SSL (Schannel SSP).]	高		
		この更新プログラムはIE11においてSSL 3.0フォールバックを無効にする設定をオンにする。 [引用：(2017/1/8の記事)This update turns on the setting that disables SSL 3.0 fallback in Internet Explorer 11. Internet Explorer 11 will now block the connections to websites that fall back from TLS 1.0 or a later version to SSL 3.0 or an earlier version. By default, this update turns on this setting only for protected mode sites in Internet Explorer 11. By default, Internet sites and restricted sites run under protected mode in Internet Explorer 11.]	高	https://support.microsoft.com/ja-jp/help/3038778/update-turns-on-the-setting-to-disable-ssl-3-0-fallback-for-protected	
暗号スイート	追加・削除：可 優先順位の変更：可 設定方法： グループポリシーエディタの、コンピューターの構成＞管理用テンプレート＞ネットワーク＞SSL構成設定＞SSL暗号の順位から設定可能	暗号スイートを追加する方法 [引用：To add cipher suites, either deploy a group policy or use the TLS cmdlets: * To use group policy, configure SSL Cipher Suite Order under Computer Configuration > Administrative Templates > Network > SSL Configuration Settings with the priority list for all cipher suites you want enabled. * To use PowerShell, see TLS cmdlets.]	高	https://msdn.microsoft.com/ja-jp/library/windows/desktop/mt813794.aspx	
サーバ証明書の利用期間	SHA-1証明書の鍵アイコンは表示されない	SHA-1証明書の鍵アイコンは表示されない [引用：Windows 10 Anniversary Update 以降、Microsoft Edge と Internet Explore は SHA-1 証明書で保護された Web サイトを信頼から除外し、これらのサイトのアドレス バーから鍵アイコンを外します。]	高	https://blogs.technet.microsoft.com/jpsecurity/2016/05/06/sha-1_deprecation_roadmap/	
		IEからSHA-1証明書によってプロテクトされたサイトのアドレスバーの錠前アイコンを削除する [引用：Lock icon removed from Address bar of sites that are protected by SHA-1	高	https://support.microsoft.com/en-us/help/3180315/lock-icon-removed-from-address-bar-of-sites-that-are-protected-by-sha	
	Phase2で、SHA-1証明書は、警告を表示する Phase3(現在) さらに警告	Phase 1 The first phase of our plan is to indicate to users that browse to TLS-secured websites that SHA-1 is less secure than SHA-2. Previously, when customers use Microsoft Edge or Internet Explorer 11 to browse to a TLS site that uses a SHA-1 end-entity certificate or issuing intermediate, customers will notice that the browser no longer displays a lock icon. Phase 2 On May 9, 2017, Microsoft released an update to Microsoft Edge and Internet Explorer that will prevent sites that are protected with a SHA-1 certificate from loading and will display an invalid certificate warning. Additionally, the Windows 10 Creators Update blocks SHA-1 by-default in the browser Phase 3 – Today Today, we intend to do more to warn consumers about the risk of downloading software that is signed using a SHA-1 certificate. Our goal is to develop a common, OS-level experience that all applications can use to warn users about weak cryptography like SHA-1. Long-term, Microsoft intends to distrust SHA-1 throughout Windows in all contexts. Microsoft is closely monitoring the latest research on the feasibility of SHA-1 attacks and will use this to determine complete deprecation timelines.	高	https://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-sha1-certificates.aspx	

表示方法の変更	・アドレスバーが緑→EV証明書あり ・錠前→SSL暗号化あり	アドレスバーの錠前アイコンの説明 [引用：アドレス バーにロックが表示されている場合は、その Web サイトが SSL (Secure Socket Layer) 暗号化を使用していることを意味し、さらにステータス バーに Web サイトの追加識別情報が表示されるため、これによって適切な Web サイトを閲覧していることを確認できます。]	高	https://www.microsoft.com/ja-jp/safety/online-privacy/cybersquatting.aspx	
		IE7以上で、EV証明書ありのサイトはアドレスバーが緑になる [引用：Internet Explorer で EV証明書がインストールされたサイトにアクセスした場合にアドレスバーを緑色に表示する機能は、Internet Explorer7 以上が対応しています。]	低	https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?vproductcat=V_C_S&vdomain=VERISIGN.JP&page=content&id=SO25544&actp=RSS&viewlocale=ja_JP&locale=ja_JP&redirected=true	
EV-SSL証明書の取り扱い方法	グリーンバーで表示される。 ただし、以下条件を満たす場合 ・SmartScreenフィルタが有効 ・ツール→インターネットオプション→詳細設定タブ 内の「サーバーの証明書失効を確認する」設定が有効	アドレスバーが緑色になるときの説明 [引用：緑のアドレス バー は、そのサイトが完全な文書化プロセスを完了し、現在のビジネス ライセンスおよび法人設立のための書類が確認されていることを意味します。]	高	https://www.microsoft.com/ja-jp/safety/online-privacy/cybersquatting.aspx	
		IE7以上で、EV証明書ありのサイトはアドレスバーが緑になる [引用：Internet Explorer で EV証明書がインストールされたサイトにアクセスした場合にアドレスバーを緑色に表示する機能は、Internet Explorer7 以上が対応しています。]	低	https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?vproductcat=V_C_S&vdomain=VERISIGN.JP&page=content&id=SO25544&actp=RSS&viewlocale=ja_JP&locale=ja_JP&redirected=true	Symantec社の情報
		EV証明書ありのアドレスバーが緑色に表示されるための設定 [引用：対応バージョンの Internet Explorer で、アドレスバーを緑色に表示するためには、Internet Explorer の以下の設定が有効になっている必要があります。 設定を変更した場合は、ブラウザを再起動してください。 ・Smart Screen フィルター機能（IE8以降）またはフィッシング詐欺防止機能（IE7） ・IEメニュー：ツール→インターネットオプション→詳細設定タブ 内の「サーバーの証明書失効を確認する」設定]	低		Symantec社の情報
EV-SSL証明書でグリーンバーにならない条件	・特にないと思われる ・ただし、ブラウザ側で必要な設定がされていな場合はグリーンバーにならない ・CT（Google Chrome参照）は未サポートと思われる（情報なし）	EV証明書ありのアドレスバーが緑色に表示されるための設定 [引用：対応バージョンの Internet Explorer で、アドレスバーを緑色に表示するためには、Internet Explorer の以下の設定が有効になっている必要があります。 設定を変更した場合は、ブラウザを再起動してください。 ・Smart Screen フィルター機能（IE8以降）またはフィッシング詐欺防止機能（IE7） ・IEメニュー：ツール→インターネットオプション→詳細設定タブ 内の「サーバーの証明書失効を確認する」設定]	低	https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?vproductcat=V_C_S&vdomain=VERISIGN.JP&page=content&id=SO25544&actp=RSS&viewlocale=ja_JP&locale=ja_JP&redirected=true	Symantec社の情報
		CTの言及はされているが、サポートはされていないと思われる。 [引用：Public Key Pinning, Perspectives や Convergence, Certificate Transparency (CT) など、業界で実現化へ向けて進められている対策や、一歩先を行くための保護策は多く検討されています。]	中	https://blogs.technet.microsoft.com/jpsecurity/2014/05/27/internet-explorer-11-smartscreen-2612/	IEと関連するCTの情報は、いまのところこのページしか見つかっていない
ブラウザサポート終了時期	インストールしたOSのサポート終了まで	OSのサポート終了までサポートされる [引用：最新バージョンの Internet Explorer は引き続きコンポーネント ポリシーに従います。つまり、インストールされている Windows オペレーティング システムのサポート ライフサイクルに従い、同じ期間だけサポートされます。]	高	https://support.microsoft.com/ja-jp/help/17454/lifecycle-faq-internet-explorer	

■Edge

項目	調査結果	記載内容	信頼度	URL	備考
プロトコルバージョン	SSL3.0, TLS1.0, TLS1.1, TLS1.2 ただし、SSL3.0はデフォルトで不使用 設定方法： インターネットオプションから可能	SSL3.0, TLS1.0, TLS1.1, TLS1.2の仕様をレジストリに設定するサブキーが記載されている	高	https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings	「Transport Layer Security (TLS) registry settings」というページ
		Windows 10 (v1607) 以降はSSL3.0はデフォルトで無効 [引用：Beginning with Windows 10, version 1607 and Windows Server 2016, SSL 3.0 has been disabled by default. For SSL 3.0 default settings, see Protocols in the TLS/SSL (Schannel SSP).]			
暗号スイート	追加・削除：可 優先順位の変更：可 設定方法： グループポリシーエディタの、コンピューターの構成＞管理用テンプレート＞ネットワーク＞SSL構成設定＞SSL暗号の順位から設定可能	TLS暗号スイートの順番を設定するために、SSL Cipher Suite Order Group Policy settingsが使用できる。 [引用：You can use the SSL Cipher Suite Order Group Policy settings to configure the default TLS cipher suite order.]	高	https://docs.microsoft.com/en-us/windows-server/security/tls/manage-tls#configuring-tls-cipher-suite-order	
		暗号スイートを追加する方法 [引用：To add cipher suites, either deploy a group policy or use the TLS cmdlets: * To use group policy, configure SSL Cipher Suite Order under Computer Configuration > Administrative Templates > Network > SSL Configuration Settings with the priority list for all cipher suites you want enabled. * To use PowerShell, see TLS cmdlets.]	高	https://msdn.microsoft.com/ja-jp/library/windows/desktop/mt813794.aspx	
サーバ証明書の利用期間	SHA-1証明書の錠前アイコンは表示されない	[引用：Windows 10 Anniversary Update 以降、Microsoft Edge と Internet Explore は SHA-1 証明書で保護された Web サイトを信頼から除外し、これらのサイトのアドレス バーから鍵アイコンを外します。]	高	https://blogs.technet.microsoft.com/jpsecurity/2016/05/06/sha-1 deprecation roadmap/	
		IEからSHA-1証明書によってプロテクトされたサイトのアドレスバーの錠前アイコンを削除する [引用：Lock icon removed from Address bar of sites that are protected by SHA-1	高	https://support.microsoft.com/en-us/help/3180315/lock-icon-removed-from-address-bar-of-sites-that-are-protected-by-sha	
	Phase2で、SHA-1証明書は、警告を表示する Phase3(現在) さらに警告	Phase 1 The first phase of our plan is to indicate to users that browse to TLS-secured websites that SHA-1 is less secure than SHA-2. Previously, when customers use Microsoft Edge or Internet Explorer 11 to browse to a TLS site that uses a SHA-1 end-entity certificate or issuing intermediate, customers will notice that the browser no longer displays a lock icon. Phase 2 On May 9, 2017, Microsoft released an update to Microsoft Edge and Internet Explorer that will prevent sites that are protected with a SHA-1 certificate from loading and will display an invalid certificate warning. Additionally, the Windows 10 Creators Update blocks SHA-1 by-default in the browser Phase 3 – Today Today, we intend to do more to warn consumers about the risk of downloading software that is signed using a SHA-1 certificate. Our goal is to develop a common, OS-level experience that all applications can use to warn users about weak cryptography like SHA-1. Long-term, Microsoft intends to distrust SHA-1 throughout Windows in all contexts. Microsoft is closely monitoring the latest research on the feasibility of SHA-1 attacks and will use this to determine complete deprecation timelines.	高	https://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-sha1-certificates.aspx	
表示方法の変更	・灰色の錠前：Webサイトが暗号化されていることを確認済み ・緑色の錠前：EV証明書が使われている	アイコンの説明がある [引用：灰色のロックは Web サイトが暗号化されていて確認済みであることを意味し、緑のロックは Web サイトが正規である可能性が高いと考えられることを意味します。これは、EV (Extended Validation) 証明書が使われているためです。]	高	https://support.microsoft.com/ja-jp/help/4027268/windows-how-to-know-whether-to-trust-a-website-in-microsoft-edge	「Microsoft Edge で Web サイトを信頼するかどうかを知る方法」というページ
EV-SSL証明書の取り扱い方法	緑色の錠前が表示される	アイコンの説明がある（文章） [引用：緑のロックは Web サイトが正規である可能性が高いと考えられることを意味します。これは、EV (Extended Validation) 証明書が使われているためです。]	高	https://support.microsoft.com/ja-jp/help/4027268/windows-how-to-know-whether-to-trust-a-website-in-microsoft-edge	
EV-SSL証明書でグリーンバーにならない条件	・特にないと思われる（情報なし） ・CTに関する情報もない				
ブラウザサポート終了時	・非公表と思われる（情報なし）				

■Safari

項目	調査結果	記載内容	信頼度	URL	備考
プロトコルバージョン	・~~SSL3.0~~, TLS1.0～TLS1.2と思われる	(OS X 10.9で) TLS1.2がサポートされた。それ以前はSSL3.0とTLS1.0だけだった [引用：For the first time Apple OS X is now enabling TLS 1.2, which is a more recent and more secure implementation of transport layer security. Prior to the Mavericks release, OS X only supported the SSLv3 and TLS 1.0 versions of SSL.]	低	https://www.esecurityplanet.com/mac-os-security/apple-secures-mac-os-x-with-mavericks-release.html	QuinStreet社が提供するセキュリティニュースサイトのページ。参考程度。
		SSL3.0, TLS1.0～1.2による通信を行うAPIがある [引用：The Security.SecureTransport API gives you access to Apple's implementation of Secure Sockets Layer version 3.0 (SSLv3), Transport Layer Security (TLS) versions 1.0 through 1.2, and Datagram Transport Layer Security (DTLS) version 1.0.]	中	https://developer.apple.com/documentation/security/secure_transport	
		iOS 10, macOS 10.12でSSLv3は廃止予定 [引用：Changes coming with iOS 10 The SSLv3 cryptographic protocol and the RC4 symmetric cipher suite will be deprecated in iOS 10, macOS 10.12, tvOS 10, and watchOS 3.]	高	https://support.apple.com/en-us/HT206871	
	TLS 1.3 (draft)は実験的に利用可能	macOS High SierraおよびiOS 11では実験的にTLS 1.3 (draft)の利用が可能に。	低	https://applech2.com/archives/20170621-high-sierra-and-ios-11-experiment-with-tls-1-3-	実験的なので参考程度
暗号スイート	追加・削除・優先順位の変更：不可と思われる（情報なし）	「知る限り暗号スイートの優先順位を変更する方法はない」 [引用：Unfortunately, AFAIK, this setting does not exist. (It doesn't exist in another WebKit browser, either: Google Chrome. You can do this in Firefox, though, using 'about:config'.)]	低	https://apple.stackexchange.com/questions/32125/setting-safari-ssl-tls-cipher-suites	ユーザが答えただけ
		RC4 対称暗号スイートが非推奨。利用できる暗号スイートが RC4 しかない場合は、接続不可。 [引用：iOS 11 January 2018 TLS The RC4 symmetric cipher suite is deprecated in iOS 10 and macOS Sierra. By default, TLS clients or servers implemented with SecureTransport APIs don't have RC4 cipher suites enabled, and are unable to connect when RC4 is the only cipher suite available. To be more secure, services or apps that require RC4 should be upgraded to use modern, secure cipher suites.]	高	https://www.apple.com/business/docs/iOS_Security_Guide.pdf	iOSのセキュリティ文書内にmacOSの記載あり
サーバ証明書の利用期間	SHA-1証明書は警告を表示	SHA-1証明書は警告を表示 [引用：macOS Sierra 10.12.4 以降および iOS 10.3 以降では、SHA-1 で署名された証明書を使って TLS 接続を確立しようとする Web ページにアクセスすると、Safari に通知が表示されます。通知をクリックしないとサイトが読み込まれません。読み込み後、サイトは安全でない接続として Safari に表示されます。]	高	https://support.apple.com/ja-jp/HT207459	
		SHA-1と2048より短い鍵のRSAは、禁止 [引用：iOS 11 January 2018 TLS As of iOS 11 and macOS High Sierra, SHA-1 certificates are no longer allowed for TLS connections unless trusted by the user. Certificates with RSA keys shorter than 2048 bits are also disallowed.]	高	https://www.apple.com/business/docs/iOS_Security_Guide.pdf	iOSのセキュリティ文書内にmacOSの記載あり
表示方法の変更	・灰色の錠前→標準的な証明書で暗号化 ・緑色の錠前＋組織名→EV証明書あり	[引用：グレイのアイコンは、標準的な証明書であることを示しています。] [引用：緑色のアイコンは、EV 証明書（より詳細な識別情報の検査が行われます）であることを示しており、EV 証明書の所有者の名前が表示されます。]	高	https://support.apple.com/ja-jp/guide/safari/sfri40697/mac	
EV-SSL証明書の取り扱い方法	アドレスバーに緑色の錠前と組織名が緑色で表示される	Ver.3.2からEV-SSL証明書に対応 [引用：米Appleは11月13日（米国時間）、Webブラウザ「Safari」の最新版「Safari 3.2」を公開した。] [引用：新版では、Safari 3.1.2以前に見つかった脆弱性を修正するとともに、次世代サーバー証明書「EV SSL」に対応した。]	低	https://enterprise.watch.impress.co.jp/cda/security/2008/11/17/14329.html	インプレス社のニュースページ。参考程度
		[引用：緑色のアイコンは、EV 証明書（より詳細な識別情報の検査が行われます）であることを示しており、EV 証明書の所有者の名前が表示されます。]	高	https://support.apple.com/ja-jp/guide/safari/sfri40697/mac	
EV-SSL証明書でグリーンバーにならない条件	・特にないと思われる（情報なし） ・CTに関する情報もない				
ブラウザサポート終了時期	・非公表と思われる（情報なし）				

■モバイル版Safari

項目	調査結果	記載内容	信頼度	URL	備考
プロトコルバージョン	TLS v1.0, TLS v1.1, TLS v1.2	iOS 11は、TLS v1.0, TLS v1.1, TLS v1.2をサポート。Safariも自動的に使用する。 APIは、SSLv3禁止。 [引用：iOS 11 January 2018 TLS iOS supports Transport Layer Security (TLS v1.0, TLS v1.1, TLS v1.2) and DTLS. It supports both AES-128 and AES-256, and prefers cipher suites with perfect forward secrecy. Safari, Calendar, Mail, and other Internet apps automatically use this protocol to enable an encrypted communication channel between the device and network services.High-level APIs (such as CFNetwork) make it easy for developers to adopt TLS in their apps, while low-level APIs (SecureTransport) provide fine-grained control. CFNetwork disallows SSLv3, and apps that use WebKit (such as Safari) are prohibited from making an SSLv3 connection.]	高	https://www.apple.com/business/docs/iOS_Security_Guide.pdf	
暗号スイート	・情報なし（MacOS版Safariと同じと思われる）	RC4 対称暗号スイートが非推奨。利用できる暗号スイートが RC4 しかない場合は、接続不可。 [引用：iOS 11 January 2018 TLS The RC4 symmetric cipher suite is deprecated in iOS 10 and macOS Sierra. By default, TLS clients or servers implemented with SecureTransport APIs don't have RC4 cipher suites enabled, and are unable to connect when RC4 is the only cipher suite available. To be more secure, services or apps that require RC4 should be upgraded to use modern, secure cipher suites.]	高	https://www.apple.com/business/docs/iOS_Security_Guide.pdf	
サーバ証明書の利用期間	SHA-1証明書は警告を表示	SHA-1証明書は警告を表示 [引用：macOS Sierra 10.12.4 以降および iOS 10.3 以降では、SHA-1 で署名された証明書を使って TLS 接続を確立しようとする Web ページにアクセスすると、Safari に通知が表示されます。通知をクリックしないとサイトが読み込まれません。読み込み後、サイトは安全でない接続として Safari に表示されます。]	高	https://support.apple.com/ja-jp/HT207459	
		SHA-1と2048より短い鍵のRSAは、禁止 [引用：iOS 11 January 2018 TLS As of iOS 11 and macOS High Sierra, SHA-1 certificates are no longer allowed for TLS connections unless trusted by the user. Certificates with RSA keys shorter than 2048 bits are also disallowed.]	高	https://www.apple.com/business/docs/iOS_Security_Guide.pdf	
表示方法の変更	・情報なし（MacOS版Safariと同じと思われる）				
EV-SSL証明書の取り扱い方法	・情報なし（MacOS版Safariと同じと思われる）				
EV-SSL証明書でグリーンバーにならない条件	・特にないと思われる（情報なし） ・CTに関する情報もない				
ブラウザサポート終了時期	・非公表と思われる（情報なし）				

■公式サイト一覧

- 「調査結果(5)」

ブラウザ	概要	公式サイト
Chrome	chromiumから確認可能	http://www.chromium.org/
		https://developer.chrome.com/home
		https://developers.google.com/web/
		https://blog.chromium.org/
		https://bugs.chromium.org/
		https://groups.google.com/a/chromium.org
		https://security.googleblog.com
		https://support.google.com/
Firefox	mozillaのセキュリティブログ等で確認可能	https://blog.mozilla.org/security/
		https://www.mozilla.org/
		https://www.mozilla.jp
		https://developer.mozilla.org
		https://wiki.mozilla.org/
		https://kb.mozillazine.org
		https://support.mozilla.org
		https://groups.google.com/forum/#!msg/mozilla.dev.security.policy
Safari	iOSでの設定を調査する	https://www.apple.com/
		https://developer.apple.com/
		https://support.apple.com/
IE	公式サイトで確認可能	https://docs.microsoft.com/
		https://blogs.windows.com
		https://technet.microsoft.com
		https://blogs.msdn.microsoft.com
		https://support.microsoft.com/
		https://developer.microsoft.com
		http://download.microsoft.com
		https://msdn.microsoft.com
		https://blogs.technet.microsoft.com/
		https://social.technet.microsoft.com
		https://www.microsoft.com
Edge	公式サイトで確認可能	(IEと同じ)