■資料概要

「1.2.1.8 設定・実装状況に係る調査」の結果をまとめたもの。

■シート一覧

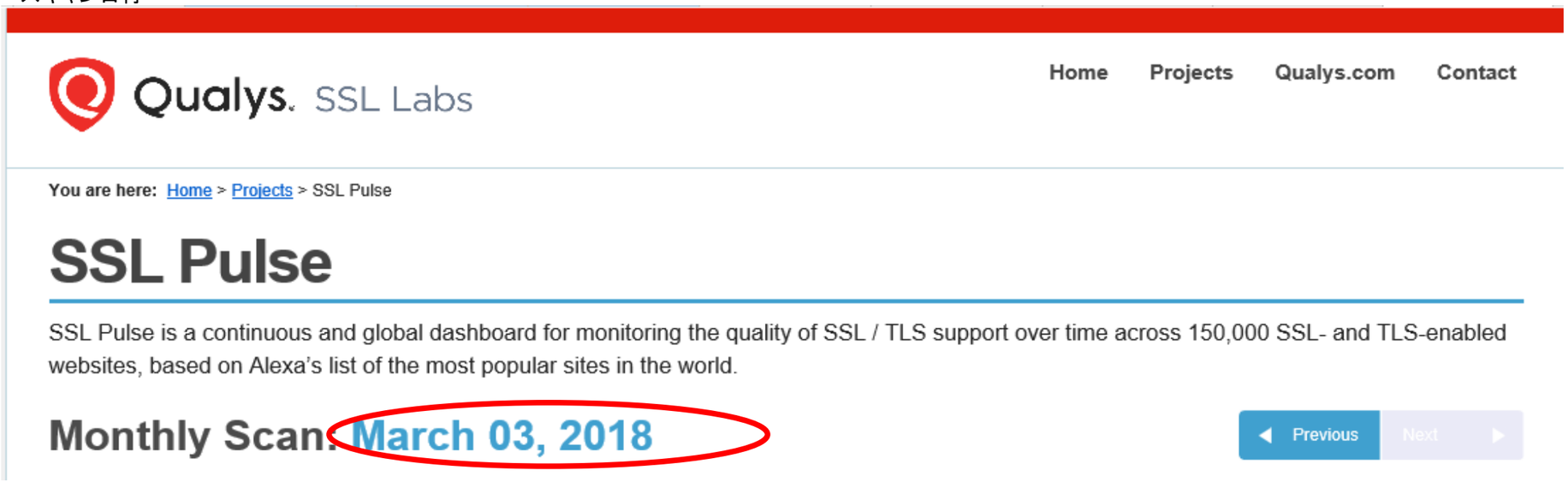
No.	シート名	内容
1	調査結果(8) (TLS実装率)	1.2.1.8に対する調査結果。調査サイトからTLS実装率を記入。
2	調査結果(8) (HSTSなど)	1.2.1.8に対する調査結果。HSTS/PKP/OCSP staplingの実装状況を記入。
3	調査結果(8) (OS)	1.2.1.8に対する調査結果。OSのサポート状況を記入。
4	調査結果(8) (ブラウザ)	1.2.1.8に対する調査結果。ブラウザのサポート状況を記入。
5	公式サイト一覧 (8)	公式サイトとして扱うサイトの一覧。

■TLS実装率

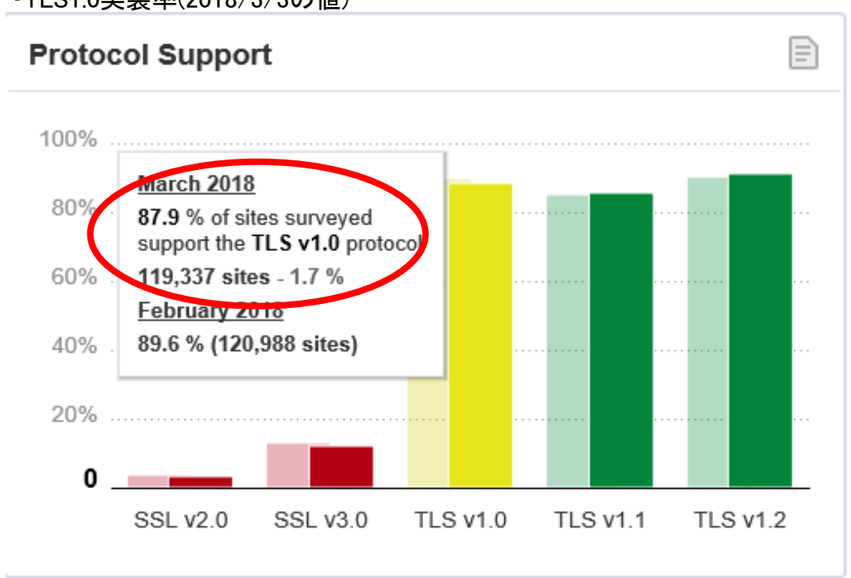
バージョン	実装率	出典・ページタイトル	URL	備考
TLS1.0	87.9%	SSL Pulse Monthly Scan: March 03, 2018	https://www.ssllabs.com/ssl-pulse/	SSL Pulseの調査結果 119,337サイト中の値
TLS1.1	85.3%			SSL Pulseの調査結果 115,767サイト中の値
TLS1.2	91.0%			SSL Pulseの調査結果 123,569サイト中の値

■補足：スクリーンショット

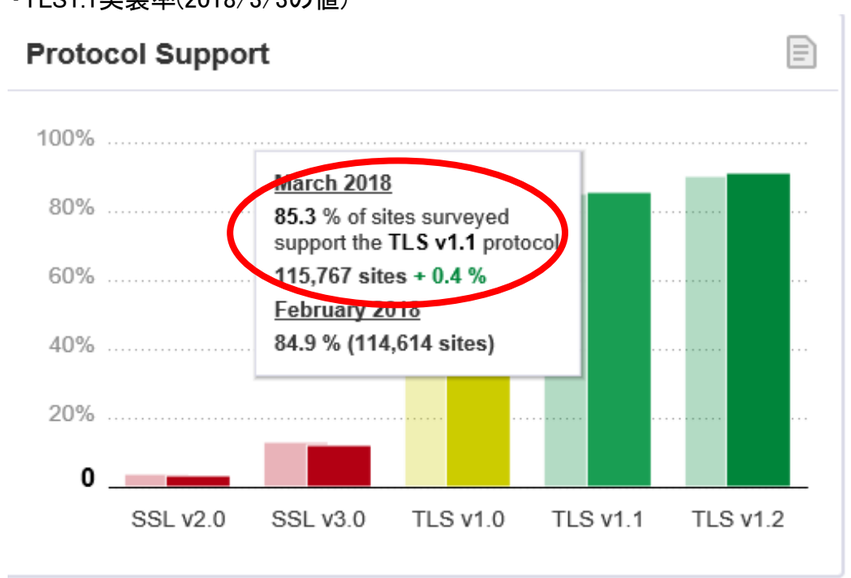
・スキャン日付



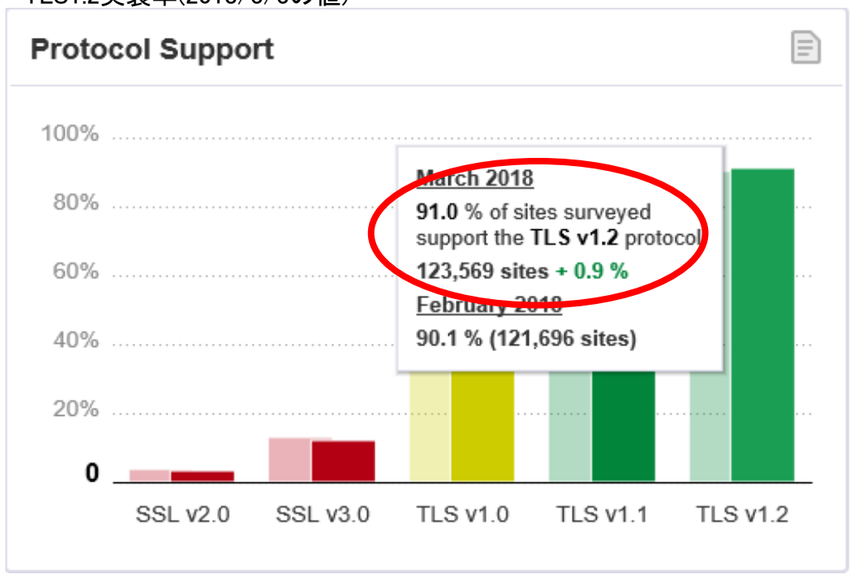
・TLS1.0実装率(2018/3/3の値)



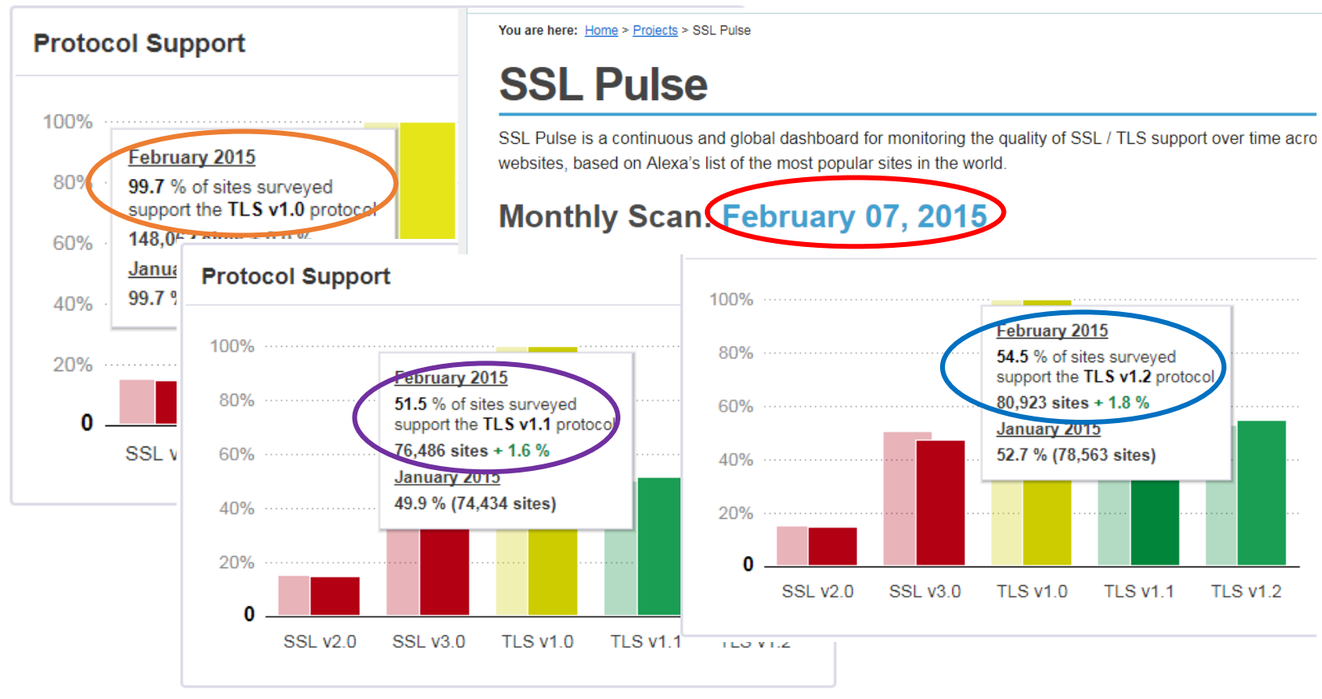
・TLS1.1実装率(2018/3/3の値)



・TLS1.2実装率(2018/3/3の値)



・【参考】2015/2/7のTLS1.0～1.2の実装率



TLS1.0 （RFC2246） （1999）	● 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%

※現行ガイドラインの実装率(2015年3月時点と表記)に近い値

『SSL/TLS暗号設定ガイドラインVer.1.1』

■HSTS

サーバ名	実装状況	記載内容	信頼度	URL	備考
Apache	○	設定方法が記載されている [引用：Edit your apache configuration file (/etc/apache2/sites-enabled/website.conf and /etc/apache2/httpd.conf for example) and add the following to your VirtualHost: # Optionally load the headers module: LoadModule headers_module modules/mod_headers.so <VirtualHost 67.89.123.45:443> Header always set Strict-Transport-Security "max-age=63072000; includeSubdomains;" </VirtualHost>]	低	https://raymii.org/s/tutorials/HTTP_Strict_Transport_Security_for_Apache_NGINX_and_Lighttpd.html	個人のサイト？
		Strict-Transport-Security HTTPレスポンスヘッダを応答すればよい [引用：Strict Transport Security の有効化 この機能を Web サイトで有効化する方法は、HTTPS でアクセスを受けた際に Strict-Transport-Security HTTP レスポンスヘッダを応答することです: Strict-Transport-Security: max-age=expireTime [; includeSubDomains] [; preload]]	低	https://developer.mozilla.org/ja/docs/Web/Security/HTTP_Strict_Transport_Security	MDNによるHSTSの一般的な設定方法
		Headerディレクティブはレスポンスヘッダを置換、追加、削除できる [引用：This directive can replace, merge or remove HTTP response headers. The header is modified just after the content handler and output filters are run, allowing outgoing headers to be modified.]	中	http://httpd.apache.org/docs/2.4/mod/mod_headers.html	Ver.2.4(安定版)で、レスポンスヘッダを追加できることはわかる
		MDRequireHttpsディレクティブで半年間Strict-Transport-Securityヘッダを含むレスポンスヘッダが返される [引用：All answers to https: requests will carry the header Strict-Transport-Security with a life time of half a year.]	中	http://httpd.apache.org/docs/trunk/mod/mod_md.html	Ver.2.5(安定版でない)では、HSTSを設定するためのディレクティブが追加されている

Lighttpd	○	設定方法が記載されている [引用：The lighttpd variant is just as simple. Add it to your Lighttpd configuration file (/etc/lighttpd/lighttpd.conf for example): server.modules += ("mod_setenv") $HTTP["scheme"] == "https" { setenv.add-response-header = ("Strict-Transport-Security" => "max-age=63072000; includeSubdomains; ") }]	低	https://raymii.org/s/tutorials/HTTP_Strict_Transport_Security_for_Apache_NGINX_and_Lighttpd.html	個人のサイト？
		Strict-Transport-Security HTTPレスポンスヘッダを応答すればよい [引用：Strict Transport Security の有効化 この機能を Web サイトで有効化する方法は、HTTPS でアクセスを受けた際に Strict-Transport-Security HTTP レスポンスヘッダを応答することです: Strict-Transport-Security: max-age=expireTime [; includeSubDomains] [; preload]]	低	https://developer.mozilla.org/ja/docs/Web/Security/HTTP_Strict_Transport_Security	MDNによるHSTSの一般的な設定方法
		setenv.add-response-headerでレスポンスヘッダを追加できる [引用：Adds a header to the HTTP response sent to the client:]	中	https://redmine.lighttpd.net/projects/1/wiki/Docs_ModSetEnv	レスポンスヘッダを追加できることはわかる
nginx	○	“add_header Strict-Transport-Security max-age=31536000;” とすれば設定できる [引用：Currently HSTS is "enabled" like this (according to https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security): add_header Strict-Transport-Security max-age=31536000;]	中	https://trac.nginx.org/nginx/ticket/289	明記されているがチケットなので参考レベル
		add_headerでレスポンスヘッダを追加できる [引用：Adds the specified field to a response header provided that the response code equals 200, 201 (1.3.10), 204, 206, 301, 302, 303, 304, 307 (1.1.16, 1.0.13), or 308 (1.13.0). The value can contain variables.]	中	http://nginx.org/en/docs/http/ngx_http_headers_module.html	
IIS	○	<site>の<hsts>要素は、IIS 10.0, ver.1709以降のサイトに対するHSTSを設定できる属性を含む [引用：The <hsts> element of the <site> element contains attributes that allow you to configure HTTP Strict Transport Security (HSTS) settings for a site on IIS 10.0 version 1709 and later.]	高	https://docs.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/site/hsts	
		IIS 10.0 ver.1709以前は複雑な設定が必要。Strict-Transport-Securityヘッダは、HTTPSサイトのweb.configのCustom Headersで追加できる(のでそれで設定する)。 [引用：Before IIS 10.0 version 1709, enabling HSTS on an IIS server requires complex configuration.] [引用：The STS header can be added through Custom Headers by configuring the web.config of the HTTPS site.]	高	https://docs.microsoft.com/ja-jp/iis/get-started/whats-new-in-iis-10-version-1709/iis-10-version-1709-hsts	
Google Web Server		(非公開)			

ブラウザ名	実装状況	記載内容	信頼度	URL	備考
Chrome	○	Chromeの新機能のひとつがHSTSの追加である [引用：One of the several new features in Chrome is the addition of HTTP Strict Transport Security.]	高	http://www.chromium.org/hsts	
Firefox	○	FirefoxはVersion 4からHSTSをサポートしている [引用：Firefox has supported HSTS since version 4; we think it’s about time your site did too. You can learn more about HSTS and how to implement it in this article on MDN.]	高	https://blog.mozilla.org/security/2012/12/26/http-strict-transport-security-2/	
Opera	○	HSTSはOperaでサポートされている [引用：HSTS allows a site to request that it always be contacted over HTTPS. HSTS is supported in Google Chrome, Firefox, Safari, Opera, and IE is planning support (caniuse.com has a compatibility matrix).]	低	https://www.chromium.org/hsts	Chromiumに記載 ※caniuseという調査サイト引用
		OperaはVer.12からサポートされている [引用：ブラウザ実装状況/Opera/12]	低	https://developer.mozilla.org/ja/docs/Web/Security/HTTP_Strict_Transport_Security	Mozillaのドキュメントに記載
Safari	○	HSTSはSafariでサポートされている [引用：HSTS allows a site to request that it always be contacted over HTTPS. HSTS is supported in Google Chrome, Firefox, Safari, Opera, and IE is planning support (caniuse.com has a compatibility matrix).]	低	https://www.chromium.org/hsts	Chromiumに記載 ※caniuseという調査サイト引用
		SafariはVer.7 (on Maverics) からサポートされている [引用：ブラウザ実装状況/Safari/7 on Maverics]	低	https://developer.mozilla.org/ja/docs/Web/Security/HTTP_Strict_Transport_Security	Mozillaのドキュメントに記載
IE	○	HSTSはWin10上のInternet Explorer 11で利用できる [引用：HSTS is also available in both Internet Explorer 11 and Microsoft Edge on Windows 10.]	高	https://support.microsoft.com/en-us/help/3071338/internet-explorer-11-adds-support-for-http-strict-transport-security-s	
Edge	○	HSTSはWin10上のEdgeで利用できる [引用：HSTS is also available in both Internet Explorer 11 and Microsoft Edge on Windows 10.]	高	https://support.microsoft.com/en-us/help/3071338/internet-explorer-11-adds-support-for-http-strict-transport-security-s	

■OCSP Stapling

サーバ名	実装状況	記載内容	信頼度	URL	備考
Apache	○	SSLUseStaplingが有効ならば、OCSP応答を格納するキャッシュを設定する [引用：Configures the cache used to store OCSP responses which get included in the TLS handshake if SSLUseStapling is enabled.]	高	http://httpd.apache.org/docs/2.4/ja/mod/mod_ssl.html#sslstaplingcache	[2.4 current version]
		OCSP staplingを有効にするには、httpdの設定を少し変えるだけでよい。 [引用：Once general SSL support has been configured properly, enabling OCSP Stapling generally requires only very minor modifications to the httpd configuration — the addition of these two directives: SSLUseStapling On SSLStaplingCache "shmcb:ssl_stapling(32768)"]	高	http://httpd.apache.org/docs/trunk/ssl/ssl_howto.html	[2.5 develop version]
nginx	○	OCSP staplingを有効にするには、ssl_stapling onと設定する [引用：Enables or disables stapling of OCSP responses by the server. Example: ssl_stapling on; resolver 192.0.2.1;]	高	http://nginx.org/en/docs/http/ngx_http_ssl_module.html	
IIS	○	自動的にOCSP stapleが行われるように設定する方法 [引用：Applies To: Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows Vista] [引用：This support topic for the IT professional shows you how to configure OCSP stapling for Kerberos so that stapling does automatically occur.]	高	https://technet.microsoft.com/en-us/library/hh826044(v=ws.10).aspx	
Google Web Server		(非公開)			

ブラウザ名	実装状況	記載内容	信頼度	URL	備考
Chrome	○	ChromiumにはOCSPステープルなどのシステムのNSSインストールに必須ではない高度な機能をサポートする独自のNSSパッチがある [引用：Note that Chromium has its own NSS patches which support some advanced features which aren't necessarily in the system's NSS installation, such as support for NPN, False Start, Snap Start , OCSP stapling, etc.]	高	http://www.chromium.org/developers/design-documents/network-stack/	
		ChromiumはOCSP staplingをサポートしている [引用：Chromium has supported OCSP stapling on (Windows Vista+, Linux, ChromeOS), and that's always been enabled (independent of the checkbox).]	高	https://bugs.chromium.org/p/chromium/issues/detail?id=361820#c7	
Firefox	○	OCSP staplingが使えるようになった [引用：OCSP Stapling has landed in the latest Nightly builds of Firefox!]	高	https://blog.mozilla.org/security/2013/07/29/ocsp-stapling-in-firefox/	
IE	○	自動的にOCSP stapleが行われるように設定する方法 [引用：Applies To: Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows Vista] [引用：This support topic for the IT professional shows you how to configure OCSP stapling for Kerberos so that stapling does automatically occur.]	高	https://technet.microsoft.com/en-us/library/hh826044(v=ws.10).aspx	
Edge	○	自動的にOCSP stapleが行われるように設定する方法 [引用：Applies To: Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows Vista] [引用：This support topic for the IT professional shows you how to configure OCSP stapling for Kerberos so that stapling does automatically occur.]	高	https://technet.microsoft.com/en-us/library/hh826044(v=ws.10).aspx	

■Public Key Pinning

サーバ名	実装状況	記載内容	信頼度	URL	備考
Apache	○	[引用：次のような行を web サーバの config に追加すると Apache で HPKP が有効になります。mod_headers モジュールがインストールされている必要があります。 Header always set Public-Key-Pins "pin-sha256=¥"base64+primary==¥"; pin-sha256=¥"base64+backup==¥"; max-age=5184000; includeSubDomains"]	低	https://developer.mozilla.org/ja/docs/Web/Security/Public_Key_Pinning	MDNによる設定方法
		Headerディレクティブはレスポンスヘッダを置換、追加、削除できる [引用：This directive can replace, merge or remove HTTP response headers. The header is modified just after the content handler and output filters are run, allowing outgoing headers to be modified.]	中	http://httpd.apache.org/docs/2.4/mod/mod_headers.html	Ver.2.4(安定版)で、レスポンスヘッダを追加できることはわかる
Lighttpd	○	[引用：鍵に関する次のような情報（pin-sha256="..." フィールドなど）を含む行を追加すると、lighttpd で HPKP が有効になります。 setenv.add-response-header = ("Public-Key-Pins" => "pin-sha256=¥"base64+primary==¥"; pin-sha256=¥"base64+backup==¥"; max-age=5184000; includeSubDomains")]	低	https://developer.mozilla.org/ja/docs/Web/Security/Public_Key_Pinning	MDNによる設定方法
		setenv.add-response-headerでレスポンスヘッダを追加できる [引用：Adds a header to the HTTP response sent to the client:]	中	https://redmine.lighttpd.net/projects/1/wiki/Docs_ModSetEnv	レスポンスヘッダを追加できることはわかる
nginx	○	[引用：次のような行を追加し、適切な pin-sha256="..." の値を設定すると nginx で HPKP が有効になります。ngx_http_headers_module がインストールされている必要があります。 add_header Public-Key-Pins 'pin-sha256="base64+primary=="; pin-sha256="base64+backup=="; max-age=5184000; includeSubDomains' always;]	低	https://developer.mozilla.org/ja/docs/Web/Security/Public_Key_Pinning	MDNによる設定方法
		add_headerでレスポンスヘッダを追加できる [引用：Adds the specified field to a response header provided that the response code equals 200, 201 (1.3.10), 204, 206, 301, 302, 303, 304, 307 (1.1.16, 1.0.13), or 308 (1.13.0). The value can contain variables.]	中	http://nginx.org/en/docs/http/ngx_http_headers_module.html	レスポンスヘッダを追加できることはわかる

IIS	○	[引用:IIS から Public-Key-Pins ヘッダを送信するには、以下のような数行を Web.config ファイルに追加してください。 <system.webServer> ... <httpProtocol> <customHeaders> <add name="Public-Key-Pins" value="pin-sha256="base64+primary=="; pin-sha256="base64+backup=="; max-age=5184000; includeSubDomains" /> </customHeaders> </httpProtocol> ... </system.webServer>]	低	https://developer.mozilla.org/ja/docs/Web/Security/Public_Key_Pinning	MDNによる設定方法
		カスタムHTTPヘッダを追加できる [引用:<httpProtocol> 要素の <customHeaders> 要素は、インターネット インフォメーション サービス (IIS) 7.0 で Web サーバーから HTTP 応答内で返されるカスタム HTTP ヘッダーを指定します。]	中	https://technet.microsoft.com/ja-jp/library/ee431580.aspx	レスポンスヘッダを追加できることはわかる
Google Web Server		(非公開)			

ブラウザ名	実装状況	記載内容	信頼度	URL	備考
Chrome	○ (PKP, HPKP)	Chrome 46から、HPKPのレポート機能ができた [引用：To help you roll out a stricter form of SSL, Chrome 46 ships with a feature called HPKP reporting.]	高	https://developers.google.com/web/updates/2015/09/HPKP-reporting-with-chrome-46	
		2018/5/29にリリースする予定のChrome 67でHPKPのサポートをやめる予定 [引用：This will first remove support for HTTP-based PKP (“dynamic pins”), in which the user-agent learns of pin-sets for hosts by HTTP headers. We would like to do this in Chrome 67, which is estimated to be released to Stable on 29 May 2018.]	高	https://groups.google.com/a/chromium.org/forum/#!msg/blink-dev/he9tr7p3rZ8/eNMwKPmUBAAJ	
		built-in PKPのサポートをやめる予定。ただし、その時期は未定 [引用：2017/10/28 This will first remove support for HTTP-based PKP (“dynamic pins”), in which the user-agent learns of pin-sets for hosts by HTTP headers. We would like to do this in Chrome 67, which is estimated to be released to Stable on 29 May 2018. Finally, remove support for built-in PKP (“static pins”) at a point in the future when Chrome requires Certificate Transparency for all publicly-trusted certificates (not just newly-issued publicly-trusted certificates). (We don’t yet know when this will be.)]	高		Edge: Currently does not support key pinning. Firefox: No official signals yet. Safari: Currently does not support key pinning. Opera: If Opera wishes to continue to support pinning, they will need to carry a patch that reverts our diff(s).
Firefox	○ (PKP, HPKP)	Firefoxはbuilt-in PKPをサポートしている [引用：Firefox now supports built-in public key pins, which means that a shortened list of acceptable certificate authorities (CAs) for participating sites is built into Firefox.]	高	https://blog.mozilla.org/security/2014/09/02/public-key-pinning/	
		(HPKPは) ver.35からサポートされている [引用：ブラウザ実装状況 Firefox (Gecko): 35 (35)]	高	https://developer.mozilla.org/ja/docs/Web/Security/Public Key Pinning	
		[引用：SecurityEngineering/Public Key Pinning]	高	https://wiki.mozilla.org/SecurityEngineering/Public_Key_Pinning	
IE	×	(HPKPは)IE11でサポートされていない [引用：Not Supported in Internet Explorer 11]	高	https://developer.microsoft.com/en-us/microsoft-edge/platform/status/publickeypinningextensionforhttp/	
		EMET (ver 4.0)を導入すれば、公開鍵の情報を用いてサーバ証明書の正当性を検証することは可能。 [引用：2.2.4 証明書信頼 (ピン設定) の設定] [引用：PublicKey Match (公開キーの照合): このオプションが選択された場合、サブジェクト名、およびシリアル番号を照合することなく、ピン設定に存在するルート証明機関内の公開キー コンポーネントのみを確認します。]	中	http://download.microsoft.com/download/B/F/B/BFBFDAB1-225C-4ECD-906F-C1DF61D7DB64/EMET Users%20Guide J.pdf	・現行ガイドラインにEMET導入で設定可能という記述があるが、EMETのサポートが2018/7/31で終了する ・Windows Server2016とWindows 10 1703ではEMETはテストされず、5.2以前のバージョンは公式にはサポートされない(https://support.microsoft.com/ja-jp/help/2458544/the-enhanced-mitigation-experience-toolkit) ・EMET4.0や5.5では、証明書の正当性を検証する仕組みはあるが、4.0のときのように公開鍵の情報単体で正当性は証明できないようになっていると思われる
		EMET ver5.5では、公開鍵だけで正当性を証明できないようになった？ [引用：(これは、証明書のサブジェクト名とシリアル番号、または公開キーのハッシュと一致という以前のバージョンの EMET からの変更点ですので、ご注意ください。)]	中	http://download.microsoft.com/download/B/F/B/BFBFDAB1-225C-4ECD-906F-C1DF61D7DB64/EMET%205.5%20User's%20Guide J.pdf	
		EMETは2017/1/27でサポート終了の予定だったが、2018/7/31まで延長された [引用：2017 年 1 月 27 日に EMET のライフ サイクルが終了することに関してお客様からのフィードバックを受け、サポート終了日が 18 か月間延長されることを発表します。新しいサポート終了日は 2018 年 7 月 31 日です。2018 年 7 月 31 日以降、EMET に関するサポートおよびセキュリティ更新プログラムを提供する予定はありません。]	高	https://technet.microsoft.com/ja-jp/security/jj653751.aspx	

Edge	×	(HPKPは)Edgeでの実装は検討中である [引用：Under Consideration in Microsoft Edge on Desktop, Mixed Reality, Mobile and Xbox]	高	https://developer.microsoft.com/en-us/microsoft-edge/platform/status/publickeypinningextensionforhttp/	
Safari, iOSSafari	×	各ブラウザの対応状況 Safari:Not Supported iOS Safari:Not Supported	低	https://caniuse.com/#search=HPKP	個人のサイト

■OS

OS名	サポート状況	サポート終了	記載内容	信頼度	URL	備考
Windows Vista Service Pack 2	×	2017/4/11	(製品のライフサイクルの検索)	高	https://support.microsoft.com/ja-jp/lifecycle/search	当該OSを検索してサポート終了日を調査
Windows 7 Service Pack 1	○	2020/4/11				
Windows 8	×	2016/1/12				
Windows 8.1	○	2023/1/10				
Windows 10	○	2025/10/14				
OS X 10.9	–	最終アップデート 2016/7/18	(Appleセキュリティアップデート)	高	https://support.apple.com/ja-jp/HT201222	当該OSを最新セキュリティアップデートを調査 ・OSのサポートは最新3バージョンだけと考えられる ・左記URLのセキュリティアップデートの対象OSをみるとそう見える ・Apple社が公式に発表している情報ではない
OS X 10.10 Yosemite	–	最終アップデート 2017/7/19				
OS X 10.11 El Capitan	–	最終アップデート 2017/12/6				
macOS X 10.12 Sierra	–	最終アップデート 2017/12/6				
macOS X 10.13 High Sierra	–	最終アップデート 2017/12/6				

■OS(モバイル)

OS名	サポート状況	サポート終了	記載内容	信頼度	URL	備考
iOS 8	–	最終アップデート 2015/8/13	(Appleセキュリティアップデート)	高	https://support.apple.com/ja-jp/HT201222	当該OSを最新セキュリティアップデートを調査
iOS 9	–	最終アップデート 2016/8/25				
iOS 10	–	最終アップデート 2017/7/19				
iOS 11	–	最終アップデート 2018/1/23				
Android 5 Lollipop	–	最終アップデート 2018/1/1	(Androidセキュリティアップデート)	高	https://source.android.com/security/bulletin/2018-01-01?hl=ja	当該OSを最新セキュリティアップデートを調査 (Androidはマイナーバージョンを含める)
Android 6 Marshmallow	–	最終アップデート 2018/1/1				
Android 7 Nougat	–	最終アップデート 2018/1/1				
Android 8 Oreo	–	最終アップデート 2018/1/1				

■ブラウザ

OS名	サポートブラウザ	バージョン		信頼度	URL	備考
		最新	確認日			
Windows 7 Service Pack 1	Internet Explorer	11	2017/12/22	高	https://support.microsoft.com/ja-jp/help/17454/lifecycle-faq-internet-explorer https://docs.microsoft.com/ja-jp/internet-explorer/ie11-deploy-guide/system-requirements-and-language-support-for-ie11	
	Chrome	63	2018/1/29	高	https://support.google.com/chrome/answer/95346?co=GENIE.Platform%3DDesktop&hl=ja	
	Firefox	58	2018/1/26	高	https://www.mozilla.org/en-US/firefox/58.0/system-requirements/	
					https://www.mozilla.org/en-US/firefox/3.0/system-requirements/	
					https://www.mozilla.org/en-US/firefox/4.0/system-requirements/	
Windows 8.1	Internet Explorer	11	2018/1/26	高	https://docs.microsoft.com/ja-jp/internet-explorer/ie11-deploy-guide/system-requirements-and-language-support-for-ie11	
	Chrome	63	2018/1/29	高	https://support.google.com/chrome/answer/95346?co=GENIE.Platform%3DDesktop&hl=ja	
	Firefox	58	2018/1/26	高	https://www.mozilla.org/en-US/firefox/58.0/system-requirements/	
Windows 10	Internet Explorer	11	2018/1/26	高	https://docs.microsoft.com/ja-jp/internet-explorer/ie11-deploy-guide/system-requirements-and-language-support-for-ie11	
	Edge	41	2018/1/29	高	https://docs.microsoft.com/ja-jp/microsoft-edge/deploy/hardware-and-software-requirements	
	Chrome	63	2018/1/29	高	https://support.google.com/chrome/answer/95346?co=GENIE.Platform%3DDesktop&hl=ja	
	Firefox	58	2018/1/26	高	https://www.mozilla.org/en-US/firefox/58.0/system-requirements/	
OS X 10.9 Mavericks	Safari	9.1.3	2018/1/26	高	https://support.apple.com/ja-jp/HT201222	
	Firefox	58	2018/1/26	高	https://www.mozilla.org/en-US/firefox/58.0/system-requirements/	
	Chrome	63	2018/1/29	高	https://support.google.com/chrome/answer/95346?co=GENIE.Platform%3DDesktop&hl=ja&oco=1 OS X Mavericks 10.9 以降	
OS X 10.10 Yosemite	Safari	10.1.2	2018/1/26	高	https://support.apple.com/ja-jp/HT201222	
	Firefox	58	2018/1/26	高	https://www.mozilla.org/en-US/firefox/58.0/system-requirements/	
	Chrome	63	2018/1/29	高	https://support.google.com/chrome/answer/95346?co=GENIE.Platform%3DDesktop&hl=ja&oco=1 OS X Mavericks 10.9 以降	
OS X 10.11 El Capitan	Safari	11.0.3	2018/1/26	高	https://support.apple.com/ja-jp/HT201222	
	Firefox	58	2018/1/26	高	https://www.mozilla.org/en-US/firefox/58.0/system-requirements/	
	Chrome	63	2018/1/29	高	https://support.google.com/chrome/answer/95346?co=GENIE.Platform%3DDesktop&hl=ja&oco=1 OS X Mavericks 10.9 以降	
macOS X 10.12 Sierra	Safari	11.0.3	2018/1/26	高	https://support.apple.com/ja-jp/HT201222	
	Firefox	58	2018/1/26	高	https://www.mozilla.org/en-US/firefox/58.0/system-requirements/	
	Chrome	63	2018/1/29	高	https://support.google.com/chrome/answer/95346?co=GENIE.Platform%3DDesktop&hl=ja&oco=1 OS X Mavericks 10.9 以降	
macOS X 10.13 High Sierra	Safari	11.0.3	2018/1/26	高	https://support.apple.com/ja-jp/HT201222	
	Firefox	58	2018/1/26	高	https://www.mozilla.org/en-US/firefox/58.0/system-requirements/	
	Chrome	63	2018/1/29	高	https://support.google.com/chrome/answer/95346?co=GENIE.Platform%3DDesktop&hl=ja&oco=1 OS X Mavericks 10.9 以降	

iOS 8	Safari	8	2018/1/29	低	https://ja.wikipedia.org/wiki/Safari	
	Firefox	58	2018/1/29	高	https://support.mozilla.org/ja/kb/firefox-available-iphone-or-ipad-my-language iOS 版 Firefox は、iOS 8.2 以降と互換性のある iPhone、iPad、iPod touch デバイスで利用できます。	
iOS 9	Safari	9	2018/1/29	高	https://developer.apple.com/library/content/releasenotes/General/WhatsNewInSafari/Articles/Safari_9_0.html#//apple_ref/doc/uid/TP40014305-CH9-SW5	
	Firefox	58	2018/1/29	高	https://support.mozilla.org/ja/kb/firefox-available-iphone-or-ipad-my-language	
iOS 10	Safari	10	2018/1/29	高	https://developer.apple.com/library/content/releasenotes/General/WhatsNewInSafari/Articles/Safari_10_0.html#//apple_ref/doc/uid/TP40014305-CH11-SW39	
	Chrome	63	2018/1/29	高	https://support.google.com/chrome/answer/95346?co=GENIE.Platform%3DiOS&hl=ja&oco=1 iOS 10 以降	
	Firefox	58	2018/1/29	高	https://support.mozilla.org/ja/kb/firefox-available-iphone-or-ipad-my-language	
iOS 11	Safari	11.1	2018/1/29	高	https://developer.apple.com/library/content/releasenotes/General/WhatsNewInSafari/Articles/Safari_11_1.html#//apple_ref/doc/uid/TP40014305-CH14-SW1	
	Chrome	63	2018/1/29	高	https://support.google.com/chrome/answer/95346?co=GENIE.Platform%3DiOS&hl=ja&oco=1	
	Firefox	58	2018/1/29	高	https://support.mozilla.org/ja/kb/firefox-available-iphone-or-ipad-my-language	
Android 5 Lollipop	Chrome	63	2018/1/29	高	https://support.google.com/chrome/answer/95346?co=GENIE.Platform%3DAndroid&hl=ja&oco=1 Android 4.1（Jelly Bean）以上	
	Firefox	58	2018/1/29	高	https://support.mozilla.org/ja/kb/will-firefox-work-my-mobile-device	
Android 6 Marshmallow	Chrome	63	2018/1/29	高	https://support.google.com/chrome/answer/95346?co=GENIE.Platform%3DAndroid&hl=ja&oco=1	
	Firefox	58	2018/1/29	高	https://support.mozilla.org/ja/kb/will-firefox-work-my-mobile-device	
Android 7 Nougat	Chrome	63	2018/1/29	高	https://support.google.com/chrome/answer/95346?co=GENIE.Platform%3DAndroid&hl=ja&oco=1	
	Firefox	58	2018/1/29	高	https://support.mozilla.org/ja/kb/will-firefox-work-my-mobile-device	
Android 8 OREO	Chrome	63	2018/1/29	高	https://support.google.com/chrome/answer/95346?co=GENIE.Platform%3DAndroid&hl=ja&oco=1	
	Firefox	58	2018/1/29	高	https://support.mozilla.org/ja/kb/will-firefox-work-my-mobile-device	

■公式サイト一覧

・「調査結果(8)（TLS実装率）」

プロトコルバージョン	概要	公式サイト
TLS1.0	調査サイトSSL Pulseの結果を利用予定	https://www.ssllabs.com/ssl-pulse/
TLS1.1		
TLS1.2		

・「調査結果(8)（HSTSなど）」(※サーバ)

サーバ	概要	公式サイト	現行バージョン
Apache	公式サイトでサーバーの設定の有無を確認可能	http://httpd.apache.org/	2.4
		https://wiki.apache.org/general	
Lighttpd	redmineのチケットに情報があるが、まとまっていない情報。	https://www.lighttpd.net/	1.4.48 November 11, 2017
		https://redmine.lighttpd.net/	
nginx	公式サイトでサーバーの設定の有無を確認可能	http://nginx.org/	2017-11-21 nginx-1.13.7 mainline version has been released.
		https://trac.nginx.org/	
IIS	公式サイトで確認可能	https://support.microsoft.com/	IIS 10.0 Windows 10 と Windows Server 2016 に付属するバージョン。
		https://docs.microsoft.com/	
		https://technet.microsoft.com/	
Google Web Server	確認不可 Googleが自前のサービスを動かしているサーバー。 情報は公開されていない。		

・「調査結果(8)（HSTSなど）」(※ブラウザ)

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
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://developer.mozilla.org
		https://wiki.mozilla.org/
Opera	Opera blogsで検索できる	http://www.opera.com/
Safari	iOSでの設定を調査する	https://www.apple.com/safari/
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
Edge	公式サイトで確認可能	(IEと同じ)

・「調査結果(8)（OS）」

OS	概要	公式サイト
Windows	公式サイトで確認可能 Microsoftの「製品のライフサイクルの検索」(右記URL)で検索して調査	https://support.microsoft.com/ja-jp/lifecycle/search
OS X/macOS/iOS	サポート終了期日は公開されていない。 各バージョン(MacOS X 10.13, 10.12, …)の最終アップデートの日付を調査	https://support.apple.com/
Android	サポート終了期日は公開されていない。 各バージョン(Android 8, 7, …)の最終アップデートの日付を調査	https://source.android.com/

・「調査結果(8)（ブラウザ）」

ブラウザ	概要	公式サイト
Mobile Safari (iOS)	サポートページなどから情報を取得	https://support.apple.com/
Chrome	サポートページなどから情報を取得	https://support.google.com/chrome/
Firefox	サポートページなどから情報を取得	https://www.mozilla.org/
		https://support.mozilla.org/
Safari	サポートページなどから情報を取得	https://support.apple.com/
		https://developer.apple.com/
IE	サポートページなどから情報を取得	https://docs.microsoft.com/
		https://support.microsoft.com/
Edge	サポートページなどから情報を取得	https://docs.microsoft.com/