SSL/TLS証明書の現状について

～安全なWebサイト運営のために～

2020年1月28日（火）

KAGOYA JAPAN

©2020 KAGOYA JAPAN Inc. All rights reserved.

目次

1．SSL/TLSとは
2．SSL証明書の役割
3．なぜSSL化が求められているのか
4．SSL/TLS暗号化の変遷
5．各ブラウザでの表示について
　①GoogleChrome
　②Microsoft Edge
　③Firefox
　④Safari
　⑤スマートフォン（iPhone）
　⑥スマートフォン（Android）
6．当社サービスのご紹介
7．質疑応答

©2020 KAGOYA JAPAN Inc. All rights reserved.

◎SSLとは

Secure Socket Layerの略で、インターネット上でデータを暗号化して通信する方法のひとつです。
通常インターネットでは暗号化されずに通信されます。
通信途中でデータを傍受されると、情報が漏洩する可能性があります。
そのため、個人情報などを扱うWebサイトの多くは情報漏洩を防ぐ目的でSSLを導入しています。

©2020 KAGOYA JAPAN Inc. All rights reserved.

◎TLSとは？

TLSはTransport Layer Securityの略で、SSLが発展した規格です。
現在使われている暗号化通信はほとんどがTLSですが、SSLの名前が広く浸透しているので一般的にSSLといわれています。

どちらも暗号化通信の名称であると認識いただければと思います。

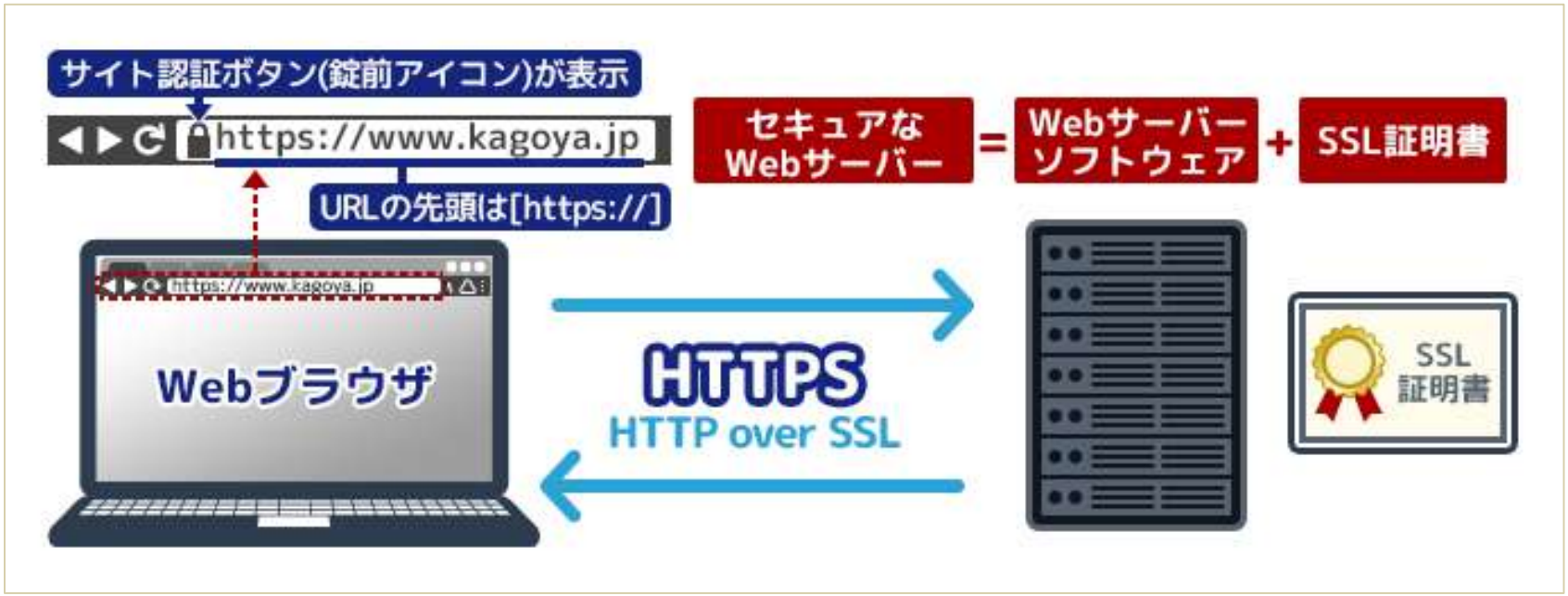
©2020 KAGOYA JAPAN Inc. All rights reserved.

◎SSLの通信ができているかは

○Webサイトのアドレスが「https://」 からはじまる

○ブラウザに鍵マークのアイコンが表示される

といったことで確認ができます。



©2020 KAGOYA JAPAN Inc. All rights reserved.

◎SSL証明書とは？

SSLの通信を行うには一般的に認証局が発行するSSL証明書をWebサーバーに設定します。

認証局とは信頼された第三者機関のことで「デジサート」「ジオトラスト」「サイバートラスト」などがあります。
日本国内では「セコムトラストシステムズ」が有名です。

Webサイト運営者は直接、もしくはレンタルサーバー会社を通して、認証局から証明書を購入します。
なぜ認証局が発行するSSL証明書が必要なのでしょうか。

©2020 KAGOYA JAPAN Inc. All rights reserved.

①データの盗聴を防ぐ

SSLでは通信が暗号化され、通信経路上で盗聴されても
解読できないため情報の漏洩を防ぐことが可能です。

©2020 KAGOYA JAPAN Inc. All rights reserved.

②データの改ざんを防ぐ

データの暗号化と複合化の際に照合を行う機能を持たせ、
経路上で改ざんされた場合には、検知、破棄できる仕組みとなっています。
（※複合化＝暗号化したデータを元に戻すこと）

©2020 KAGOYA JAPAN Inc. All rights reserved.

③なりすましを防ぐ

Webサイトの運営者が存在し、利用しているドメインの正しい所有者であることを証明します。

認証局がSSL証明書を発行する際にWebサイト運営者を審査することで信頼性を担保しています。
審査内容は発行されるSSL証明書の種類により異なります。

©2020 KAGOYA JAPAN Inc. All rights reserved.

KAGOYA JAPAN

◎SSL証明書の種類
ドメイン認証型、企業認証型、EVタイプの３つがあります。

SSLサーバー証明書の種類

次に、審査内容の程度によって取得可能なSSL証明書について、比較検討してみましょう。

	ドメイン認証型	企業認証型	EVタイプ
審査内容	登録ドメインの確認のみ	企業の実在性を認証	・企業の実在性を厳格に認証 ・なりすまし対策可
信頼性	中	高	最高
実在性確認※	無	有	有
手続き	簡単	煩雑	より煩雑
デメリット	安全性がやや弱い	費用と時間がかかる	費用と時間が大いにかかる
費用	低	中	高
対象	主に個人	企業	企業
その他			ブラウザのアドレスバーに利用者の名称を表示する

©2020 KAGOYA JAPAN Inc. All rights reserved.

KAGOYA JAPAN

◎スノーデン氏の発表による国家的な盗聴の事実

2013年6月、元NSA職員のエドワード・スノーデン氏により、アメリカ国家安全保障局（NSA）の国家的な盗聴の事実が明らかになりました。

NSAは通信キャリアの協力を受けて、インターネットを平文で流れる膨大なデータの傍受、改ざんの仕組みを設置していました。

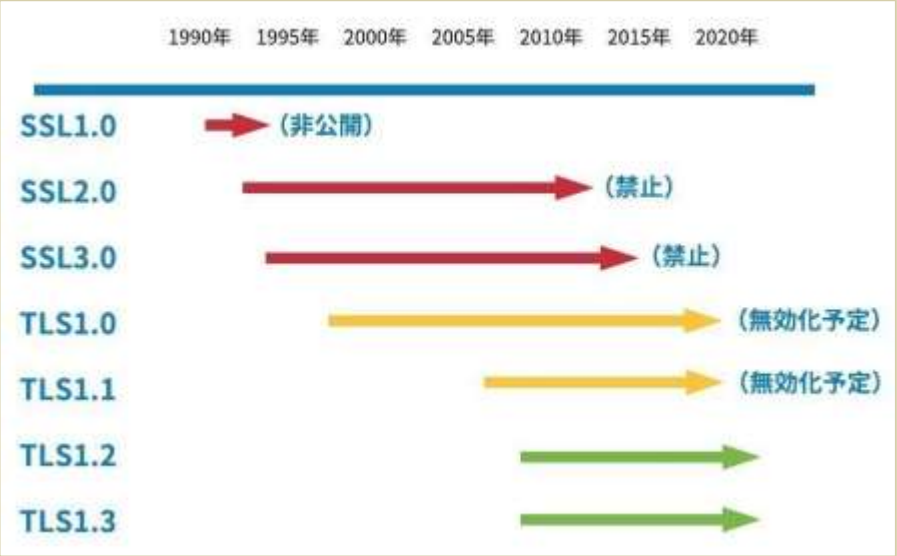
この事態を受け主要のブラウザ開発元はインターネットに流れるデータの暗号化を進める動きが大幅に加速しました。

©2020 KAGOYA JAPAN Inc. All rights reserved.

◎SSL/TLSの暗号化の変遷

SSLは初期バージョンでは脆弱性の問題があったため、
SSL1.0 → SSL2.0 → SSL3.0 → TLS1.0 → TLS1.1→…
と改良が加えられ、現在は「TLS1.2」が主流です。

前バージョンのTLS1.1までは脆弱性が存在していることが確認されています。
しかし、依然としてTLS1.0 / 1.1を利用しているWebサーバーは多く存在している状況です。



©2020 KAGOYA JAPAN Inc. All rights reserved.

◎TLS1.0 / 1.1 利用Webサイトの非表示化

主要ブラウザ開発元は、2020年3月から上半期にかけて、TSL1.0 / 1.1のサポート終了を発表しました。
TLS1.0 / 1.1を利用しているWebサイトは表示ができなくなります。

■ブラウザベンダ各社の方針

・ Google Chrome
Google社は、2020年3月(予定)リリース予定のChrome 81において、TLS1.0および1.1のサポートを終了する予定を発表しております。
https://security.googleblog.com/2019/10/chrome-ui-for-deprecating-legacy-tls.html

・ Mozilla Firefox
Mozillaは、2020年3月(予定)またはこれ以前に、FirefoxにおけるTLS1.0および1.1のサポートを終了する予定を発表しております。
https://blog.mozilla.org/security/2018/10/15/removing-old-versions-of-tls/

・ Microsoft Edge
Microsoft社は、2020年上半期(予定)において、EdgeならびにInternet ExplorerにおけるTLS1.0および1.1のサポートを終了する予定を発表しております。
https://blogs.windows.com/msedgedev/2018/10/15/modernizing-tls-edge-ie11/

・ Apple Safari
Apple社は、2020年3月(予定)またはこれ以降において、SafariにおけるTLS1.0および1.1のサポートを終了する予定を発表しております。
https://webkit.org/blog/8462/deprecation-of-legacy-tls-1-0-and-1-1-versions/

©2020 KAGOYA JAPAN Inc. All rights reserved.

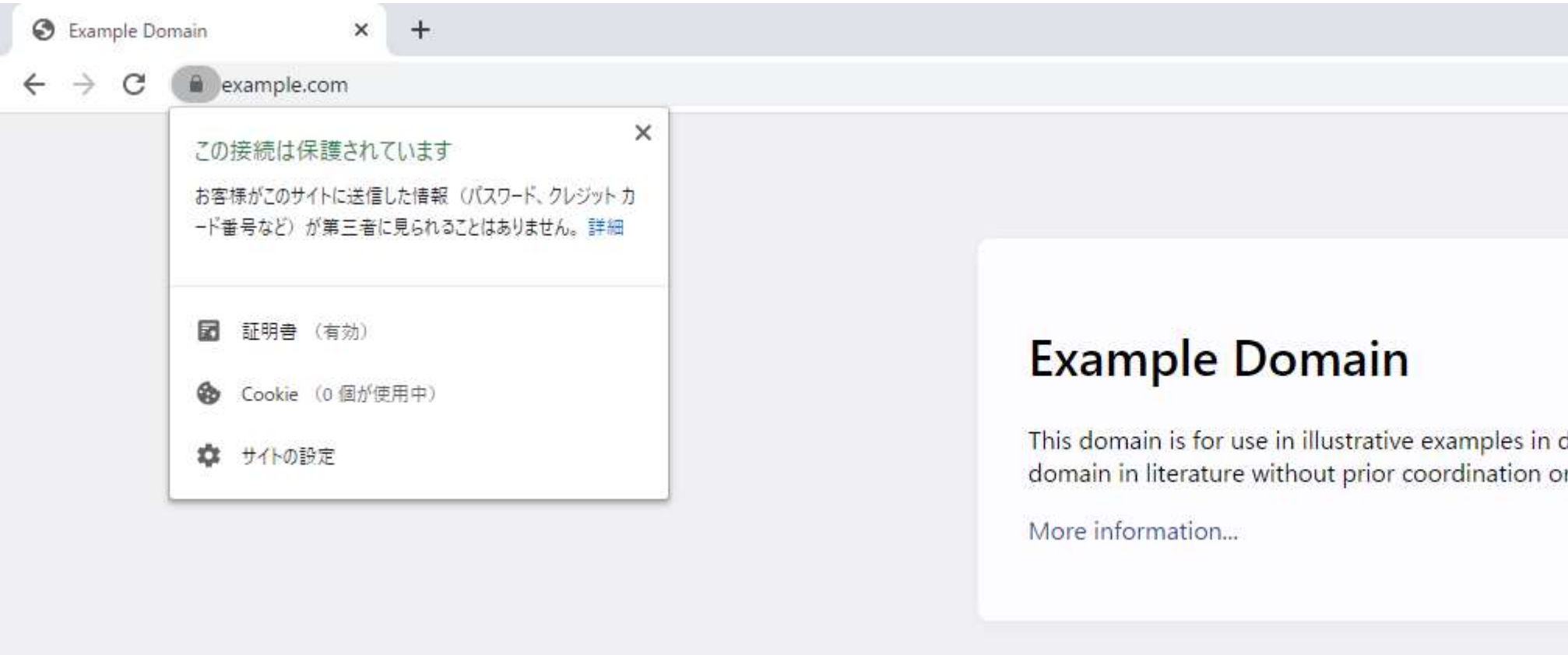
5. 各ブラウザの対応状況 ①GoogleChrome(1)

・Google Chrome68（2018年7月リリース）
http://で始まる全てのWebサイトで「このサイトへの接続は保護されていません」と警告メッセージ（黒字）が表示されるようになりました。

©2020 KAGOYA JAPAN Inc. All rights reserved.

5. 各ブラウザの対応状況 ①GoogleChrome(2)

・Google Chrome69（2018年9月リリース）
これまではhttps://で始まるWebサイトは「保護された通信」と緑の文字で表示されていましたが、灰色の文字と鍵マークになりました。https://が非表示となりました。



©2020 KAGOYA JAPAN Inc. All rights reserved.

5. 各ブラウザの対応状況 ①GoogleChrome(3)

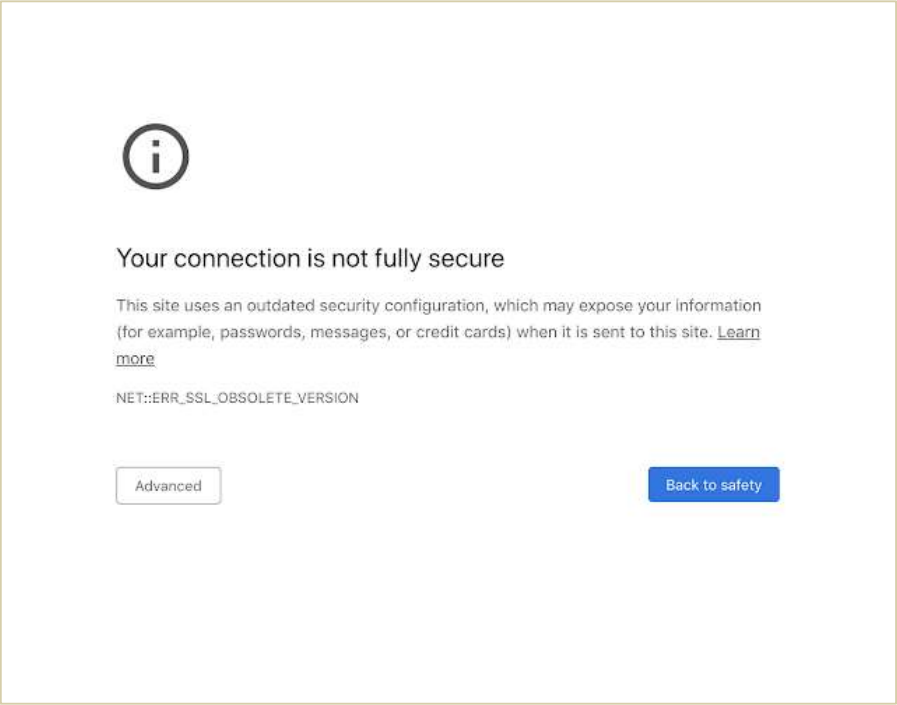
・Google Chrome79（2020年1月リリース）
「TLS1.0」「TLS1.1」を利用したWebサイトでは、
https://でアクセスしても「このサイトへの接続は完全には保護されていません」と表示されるようになりました。

©2020 KAGOYA JAPAN Inc. All rights reserved.

5. 各ブラウザの対応状況 ①Google Chrome(4)

そして今後・・・

・Google Chrome81（2020年3月リリース予定）
「TLS1.0」「TLS1.1」を利用したWebサイトはアクセスを完全にブロックされる予定です。
https://security.googleblog.com/2019/10/chrome-ui-for-deprecating-legacy-tls.html



©2020 KAGOYA JAPAN Inc. All rights reserved.

☆SEO対策にもなる！？

開発元のGoogleは2014年の時点で、SSLによる暗号化が実施されたサイトをSEO的に優遇することを公式ブログで発表しています。

※SEOとは…Webの検索結果で上位に表示させる取り組みのことです。

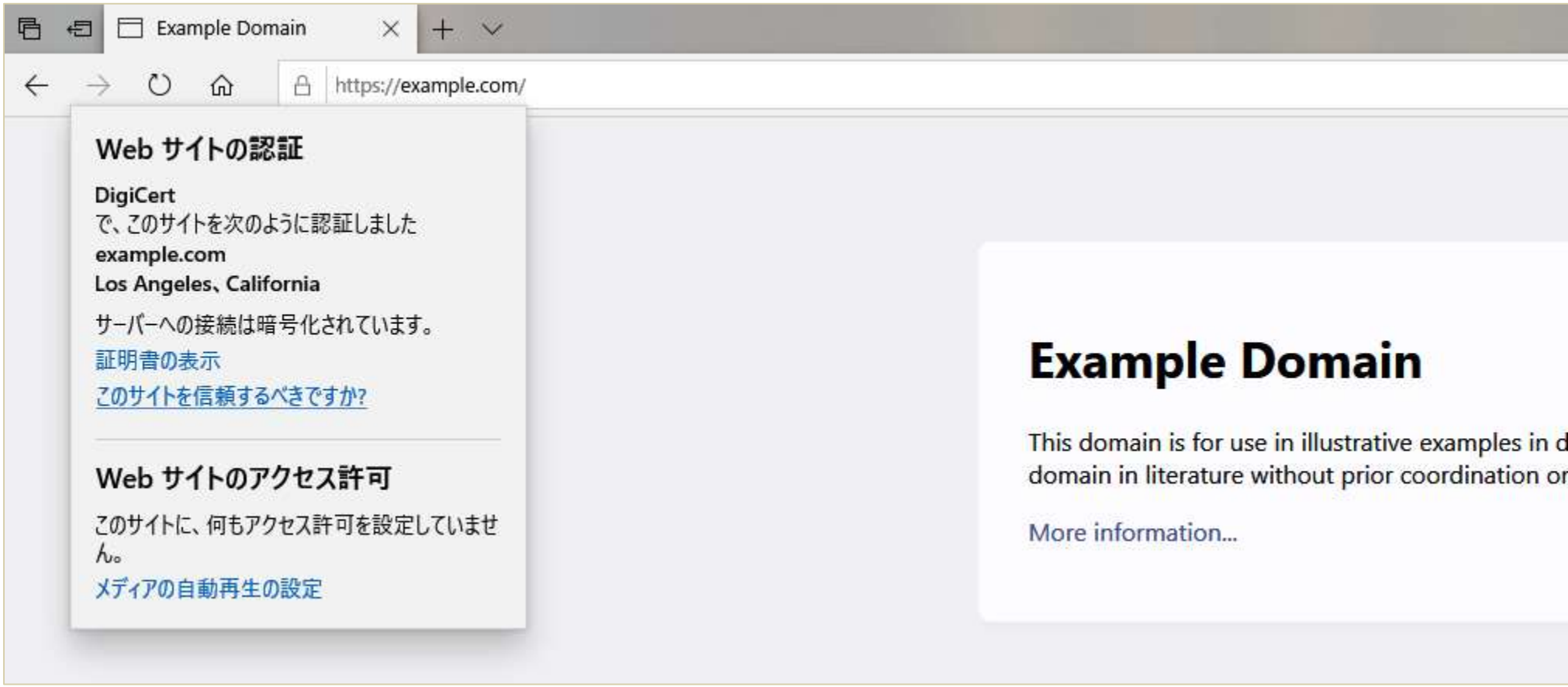
さらに同じドメインでSSL暗号化が実施されたページ(https://からはじまるページ)、暗号化が行なわれていないページ(http://からはじまるページ)が存在した場合に、暗号化されたページが先にインデックス化され検索結果に表示されるようになるとも語っています。

https://webmaster-ja.googleblog.com/2014/08/https-as-ranking-signal.html

©2020 KAGOYA JAPAN Inc. All rights reserved.

5. 各ブラウザの対応状況 ②Microsoft Edge(1)

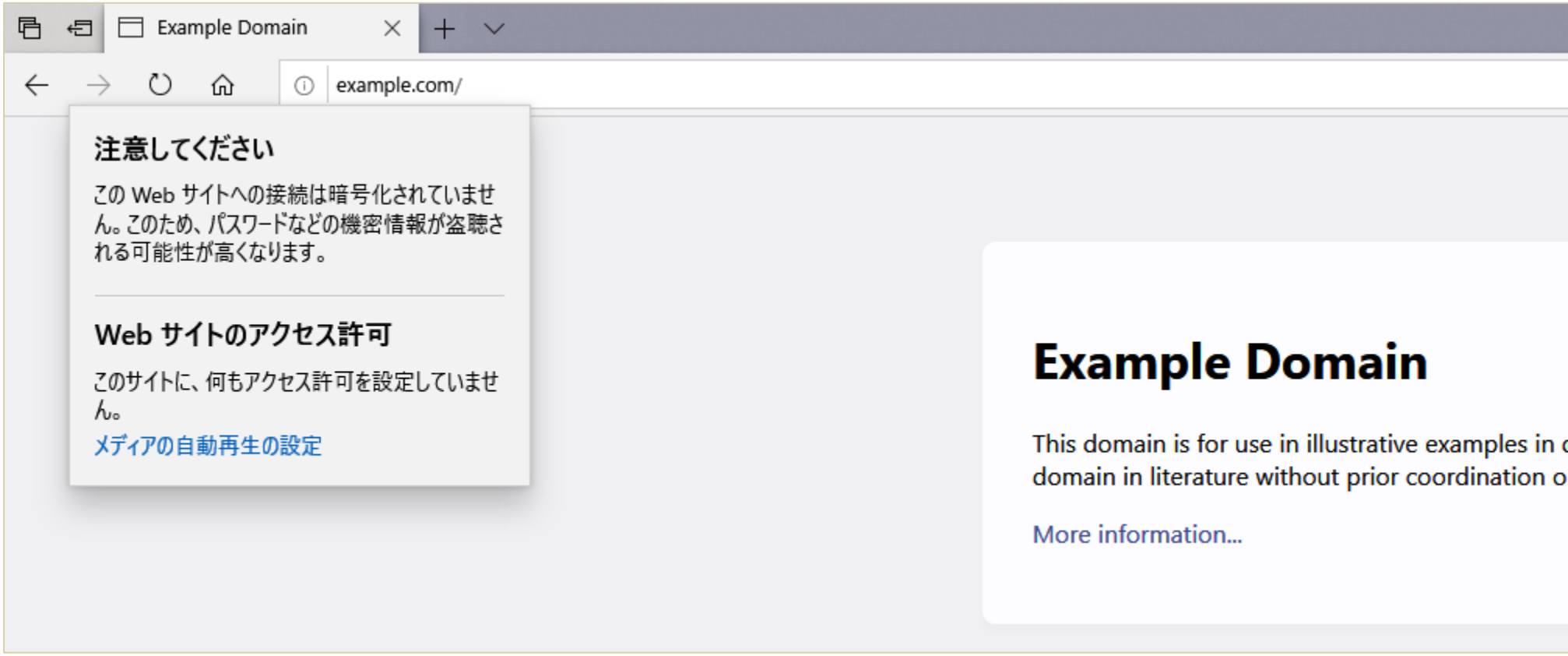
・Microsoft Edge44
https://で始まるWebサイトは「サーバーへの接続は暗号化されています」と表示されます。



©2020 KAGOYA JAPAN Inc. All rights reserved.

5. 各ブラウザの対応状況 ②Microsoft Edge(2)

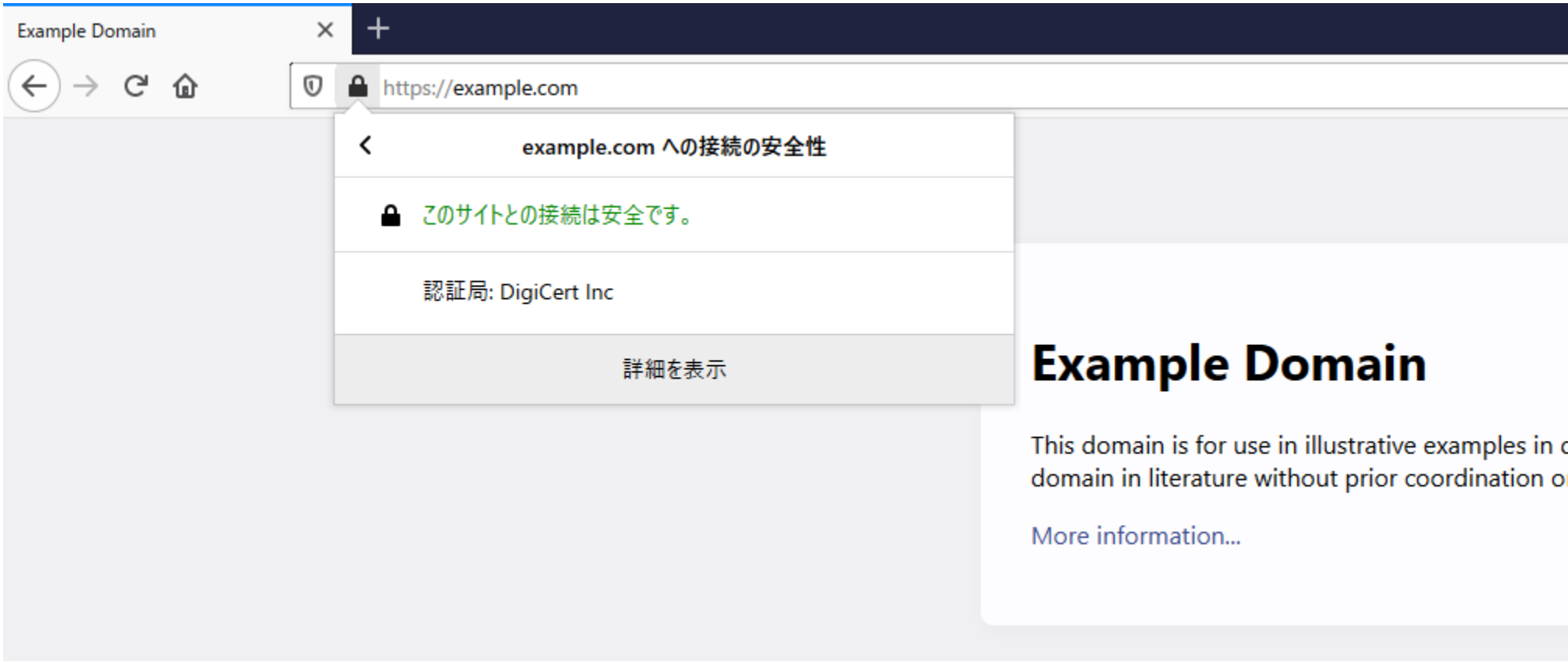
・Microsoft Edge44
http://で始まるWebサイトで「注意してください..」と警告メッセージが表示されます。



©2020 KAGOYA JAPAN Inc. All rights reserved.

5. 各ブラウザの対応状況 ③Mozilla Firefox(1)

・Mozilla Firefox72
https://で始まるWebサイトは鍵マークと「このサイトとの接続は安全です。」と表示されます。



©2020 KAGOYA JAPAN Inc. All rights reserved.

5. 各ブラウザの対応状況 ③Mozilla Firefox(2)

・Mozilla Firefox72
http://で始まるWebサイトは鍵マークに赤の斜め線が入り、「このサイトとの接続は安全ではありません。」と表示されます。

©2020 KAGOYA JAPAN Inc. All rights reserved.

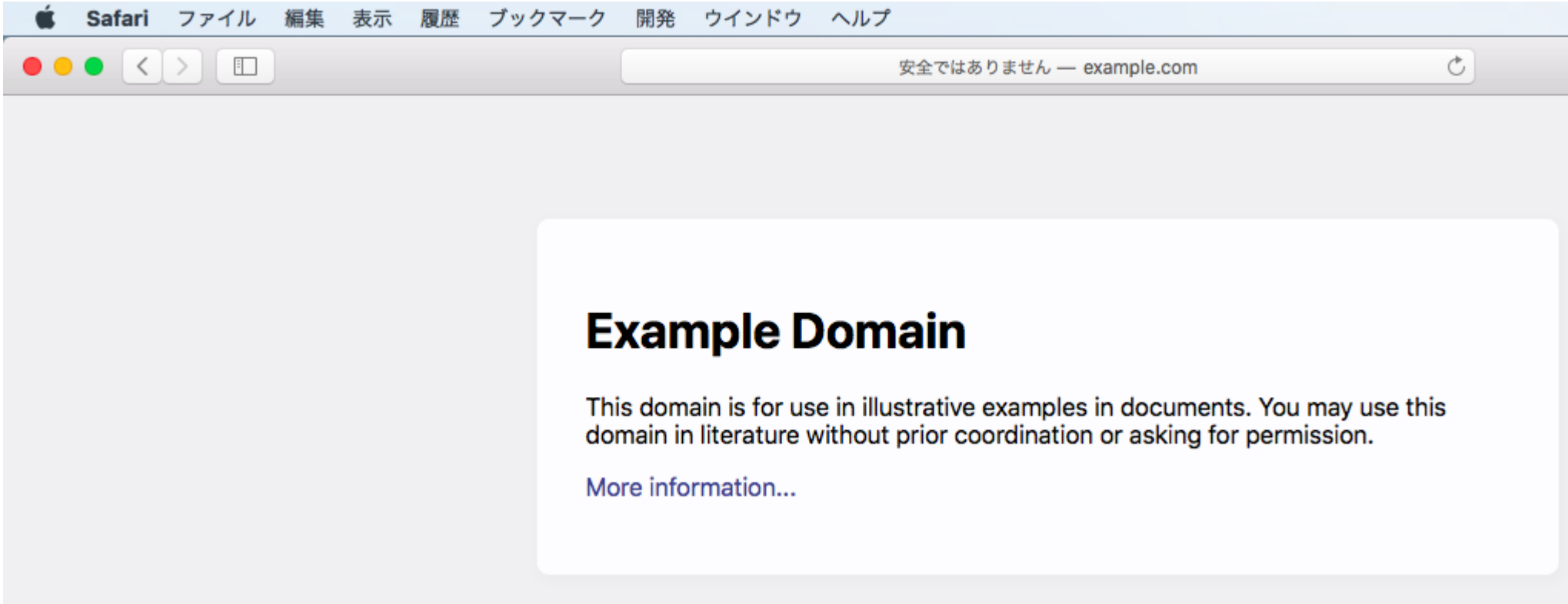
5. 各ブラウザの対応状況 ④Apple Safari(1)

・Apple Safari13
https://で始まるWebサイトは鍵マークが表示されます。

©2020 KAGOYA JAPAN Inc. All rights reserved.

5. 各ブラウザの対応状況 ④Apple Safari(2)

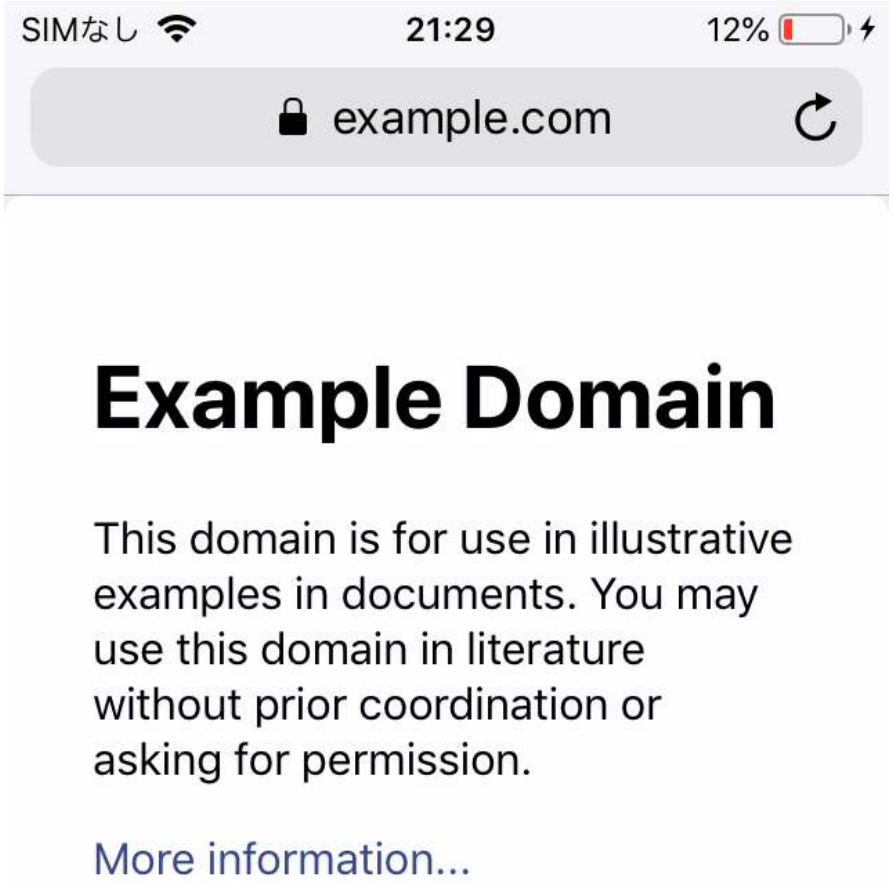
・Apple Safari13
http://で始まるWebサイトは「安全ではありません」と表示されます。



©2020 KAGOYA JAPAN Inc. All rights reserved.

5. 各ブラウザの対応状況 ⑤スマートフォン iPhone(1)

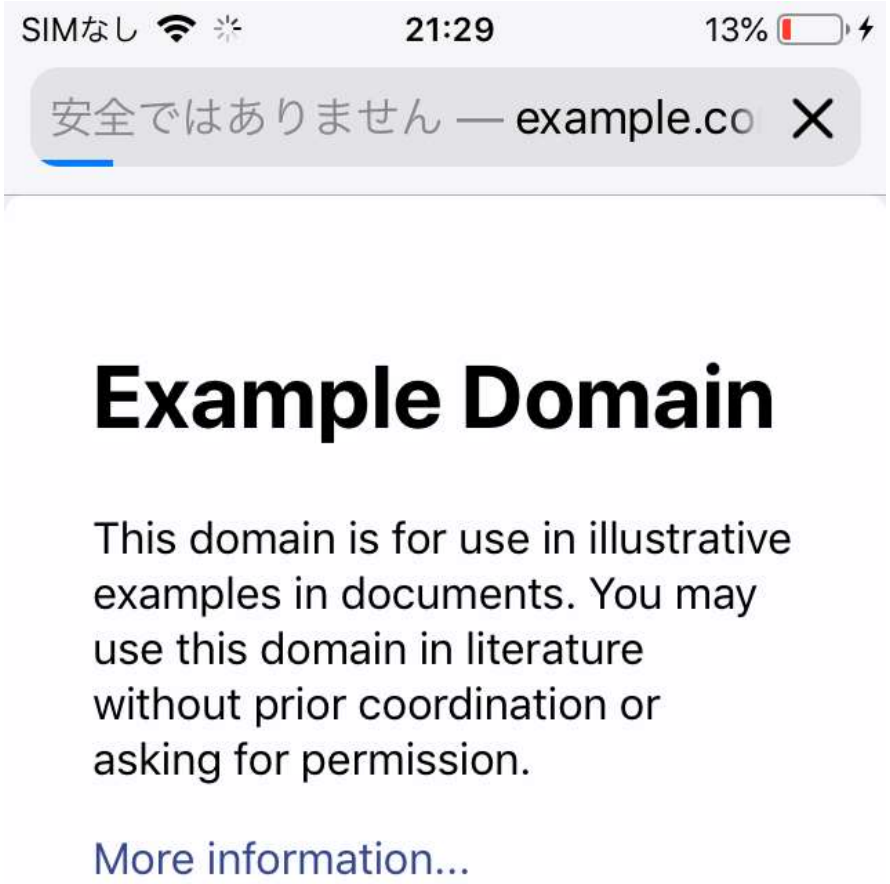
・スマートフォン iPhone
https://で始まるWebサイトは鍵マークが表示されます。



©2020 KAGOYA JAPAN Inc. All rights reserved.

5. 各ブラウザの対応状況 ⑤スマートフォン iPhone(2)

・スマートフォン iPhone
http://で始まるWebサイトは「安全ではありません」と表示されます。



©2020 KAGOYA JAPAN Inc. All rights reserved.

5. 各ブラウザの対応状況 ⑥スマートフォン Android(1)

・スマートフォン Android
https://で始まるWebサイトは鍵マークが表示され、
そちらをタップすると「この接続は保護されています」と
表示されます。

©2020 KAGOYA JAPAN Inc. All rights reserved.

5. 各ブラウザの対応状況 ⑥スマートフォン Android(2)

・スマートフォン Android
http://で始まるWebサイトは「i」のマークが表示され、そちらをタップすると「このサイトへの接続は保護されません」と表示されます。

©2020 KAGOYA JAPAN Inc. All rights reserved.

6. 当社サービスのご紹介

・ドメイン認証型
RapidSSL
ジオトラストクイックSSLプレミアム

・企業認証型
セコムパスポート for Web
シマンテック セキュア・サーバID

・EVタイプ
セコムパスポート for Web EV
シマンテック グローバル・サーバID EV

■参考URL：カゴヤのサーバー研究室
https://www.kagoya.jp/howto/rentalserver/ssl/

©2020 KAGOYA JAPAN Inc. All rights reserved.

◎無償SSL証明書「Let’s Encrypt」

https://letsencrypt.org/ja/
インターネット・セキュリティ・研究グループ (Internet Security Research Group; ISRG) という非営利団体が提供する無償SSL証明書です。

「自動発行、自動更新が可能」という特徴を持っています。

更新忘れの心配がなく安全にWebサイト運営が可能です。

©2020 KAGOYA JAPAN Inc. All rights reserved.

Thank you

カゴヤ・ジャパン株式会社
https://www.kagoya.jp/

【本社】〒604-8166 京都市中京区三条通烏丸西入御倉町85-1 KDX烏丸ビル 8F
TEL：075-252-9355（代表）　FAX：075-252-9356
【カゴヤ梅田ファクトリー】〒530-0057 大阪市北区曽根崎2-12-7 清和梅田ビル 4F
TEL：06-6809-7381　FAX：06-6809-7359
【東京営業所】〒104-0031 東京都中央区京橋2-11-4 カクトビル宝町 9F
TEL：03-3538-2007　FAX：03-3538-2008

問い合わせ

Tel：0120-022-234
受付時間　平日9:30～17:45（土日祝・当社指定休日を除く）
Mail：support@kagoya.com

©2020 KAGOYA JAPAN Inc. All rights reserved.