東京桑野会ホームページのSSL化

情報の保護や通信の安全性は向上したのか

2023年 9月 21日

東京桑野会　ホームページ委員会
委員長　　芳賀　雅美

1. サーバー証明書とは

1−1 サーバー証明書の必要性 ⇒ 「**脅威**」への対策

利用者(クライアント)とホームページサイト(サーバー)を、公開された空間であるインターネットを通じ通信回線によって、データを送受信する。このデータは通常では、誰でも傍受し閲覧が可能である。

（1） 盗聴、盗み見、個人情報や秘密データの盗み取り の脅威
（2） データの改ざん、画像の差替え の脅威
（3） なりすまし の脅威

⇒ **「サーバー証明書」が効果あり**

1−2 SSLサーバー証明書の役割

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送受信する仕組み(プロトコル)のひとつ。暗号化だけでなく、組織の実在証明を兼ねる役割もある。

（1） 暗号化通信

2つの暗号キーを使用し、クライアントとサーバー間のデータ通信を秘密化する。第三者には解読が不可能となり、データが守られる。

（2） 実在証明

「実在するサイトの運営者(組織)によって正しく運営されているホームページ」であることを証明。

⇒ **ただし、「ドメイン認証SSL」**の証明書は「ドメインの実在」しか証明できない。

※)最近のフィッシング詐欺サイトは、無料ドメイン認証SSL(Let’s Encrypt)を利用する例が増加。

⇒ この1～2年で、詐欺サイトの90%以上が採用していると言われている。

1. サーバー証明書とは（続き）

1－3 SSLサーバー証明書の種類

SSLサーバー証明書には3つの種類がある。

（1）**「ドメイン認証SSL」… DV（Domain Validation）**

無料の「 Let’s Encrypt 」や、認証局が発行する有料型もある。有料型は審査がやや厳しい。
誰でも（流通するドメインを所有していれば）、簡単に（無料では5分で）、新規取得できる。

（2）**「実在認証SSL」… OV（Organization Validation） 「企業認証SSL」とも言う**

金銭のやり取りが無いコーポレートサイトは、ほぼ全部これである。大手企業のホームページは、米国 DigiCert Inc の証明書を利用している例が多い。認証局による適正審査がある。

（3）**「EVSSL」… EV（Extended Validation）**

銀行、証券会社、クレジットカード会社、インターネットショッピングなどの金銭を扱う場合や、高度の機密情報を扱う場合に発行する証明書である。企業の業態や経営状態など厳しい審査がある。

1－4 SSLの歴史

現在の形、世界スタンダード化したのは2012年と、つい最近である。25ヶ国、browser8社、日本はGMOグローバルサイン社とセコムトラストシステムズ社の2社が参加。

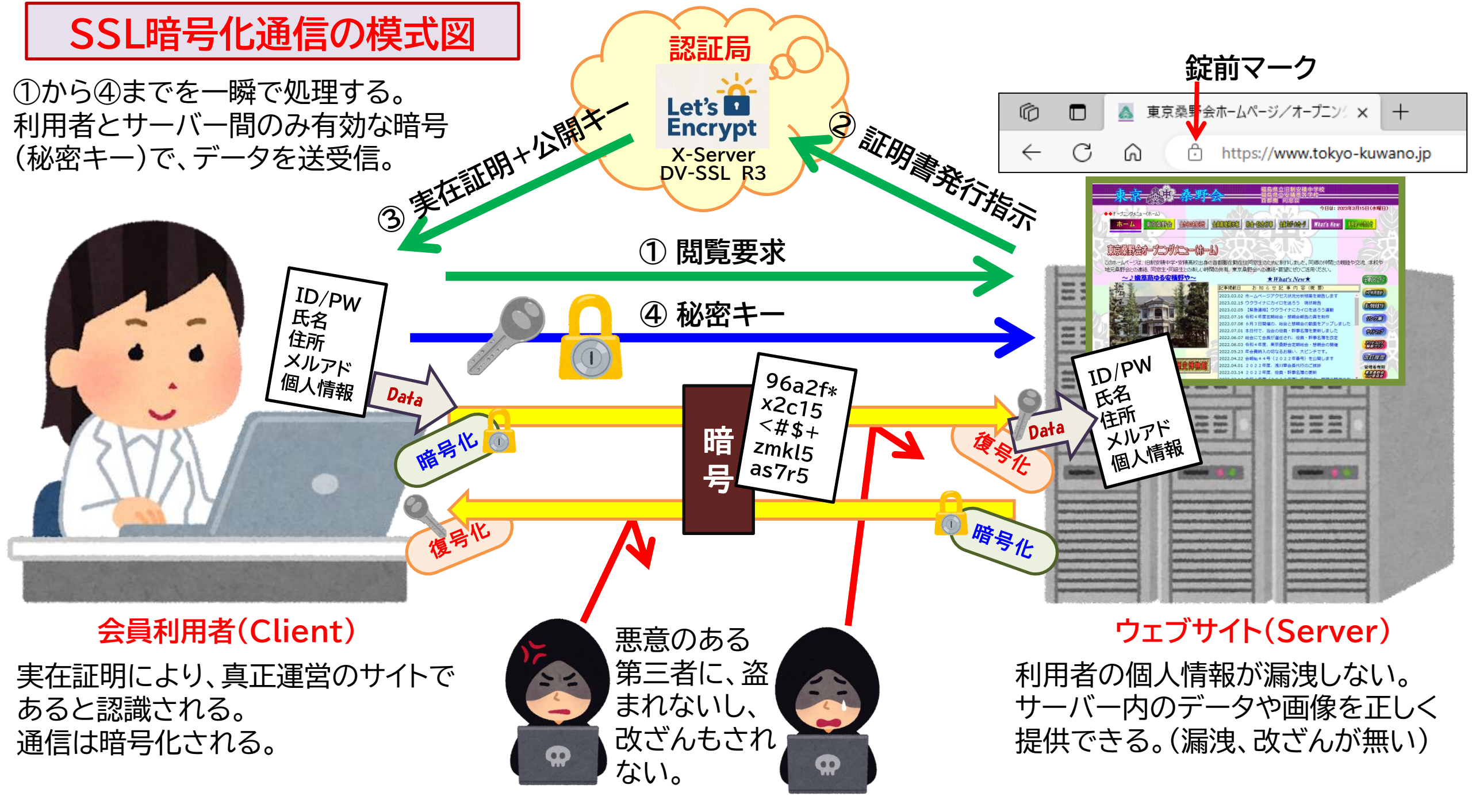
（1） 1995年頃から、サーバー証明業者が登場。当初は「OV型」の考え方しかなかった。

（2） 2005年にマイクロソフト社を中心として、規格の統一化を開始。

（3） 2007年頃より、より高度なEV要件の要求が高まり、一気にSSL化の気運が高まった。

SSL暗号化通信の模式図

①から④までを一瞬で処理する。
利用者とサーバー間のみ有効な暗号（秘密キー）で、データを送受信。



会員利用者（Client）

実在証明により、真正運営のサイトであると認識される。
通信は暗号化される。

悪意のある第三者に、盗まれないし、改ざんもされない。

ウェブサイト（Server）

利用者の個人情報が漏洩しない。
サーバー内のデータや画像を正しく提供できる。（漏洩、改ざんが無い）

2.　東京桑野会ホームページのSSL証明書

2－1　SSLサーバー証明書の種類

エックスサーバー株式会社の無料**DVSSL（ドメイン認証SSL）**を採用した。また、特定頁のSSL化とせず、全体を**常時SSL化**とした。2023年9月16日（土）早朝に移行した。

（1）　利　点

永久無料、証明書インストールはサーバー操作パネルから簡単に設定や解除ができる。

（2）　欠　点

実在証明としては不充分、有効期限が90日と短い（自動更新可能）。暗号化強度が弱い。
ホスティング先である、「エックスサーバー社」のサーバー内でしか有効でない。セキュリティ診断が付帯されていない。SSLサイトシール（認証局ブランド表示）が無い。

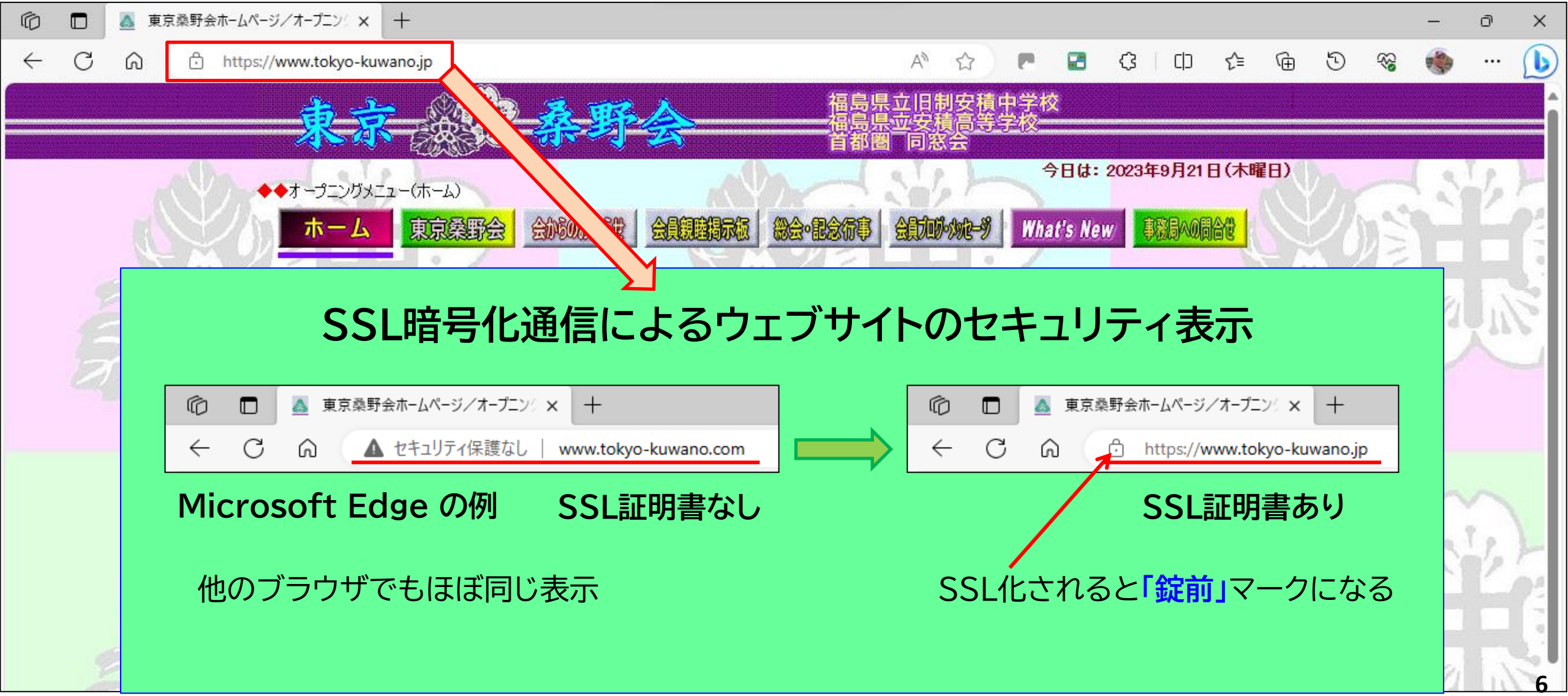
（3）　認証局

実在証明書は**「tokyo-kuwano.jp」**ドメインに対して、米国の非営利団体である**「Internet Security Research Group（ISRG）」**により運営されている認証局のSSL証明書が付与されている。証明書の有効期間は90日であり、60日を経過するごとにドメインの再審査を実施して更新される仕組みである。通常**「Let ‘s Encrypt R3」**と呼ばれている2021年10月にリリースされた証明書のバージョン3である。この公的認証局による当会ホームページサイトの認証は2023年9月14日に承認された。

2. 東京桑野会ホームページのSSL証明書（続き）

2−2 SSL証明の見分け方

全体を**常時SSL化**としており、ブラウザ画面の左上にセキュリティ表示が掲載されている。



2. 東京桑野会ホームページのSSL証明書（続き）

2－3 SSL化して何が変わったのか

（1）URLの表記が変更

【旧】 http://www.tokyo-kuwano.com

【新】 https://www.tokyo-kuwano.jp

※） **http** の後に **s** が付き、最後が「**.jp**」になった。ほかの頁も同じ。

（2）サイトの画面は変化なし

見掛けは何も変わらない。旧URLに接続すると、当面の間は自動的にSSL化された新URLにつながるようにプログラムしてある。年内に旧URLは閉鎖の予定である。

（3）会員の皆さまへのお願い

ブラウザの「お気に入り」を、新URLに更新してください。

※） サーバーを別会社に移管し、ドメインを変更したため。

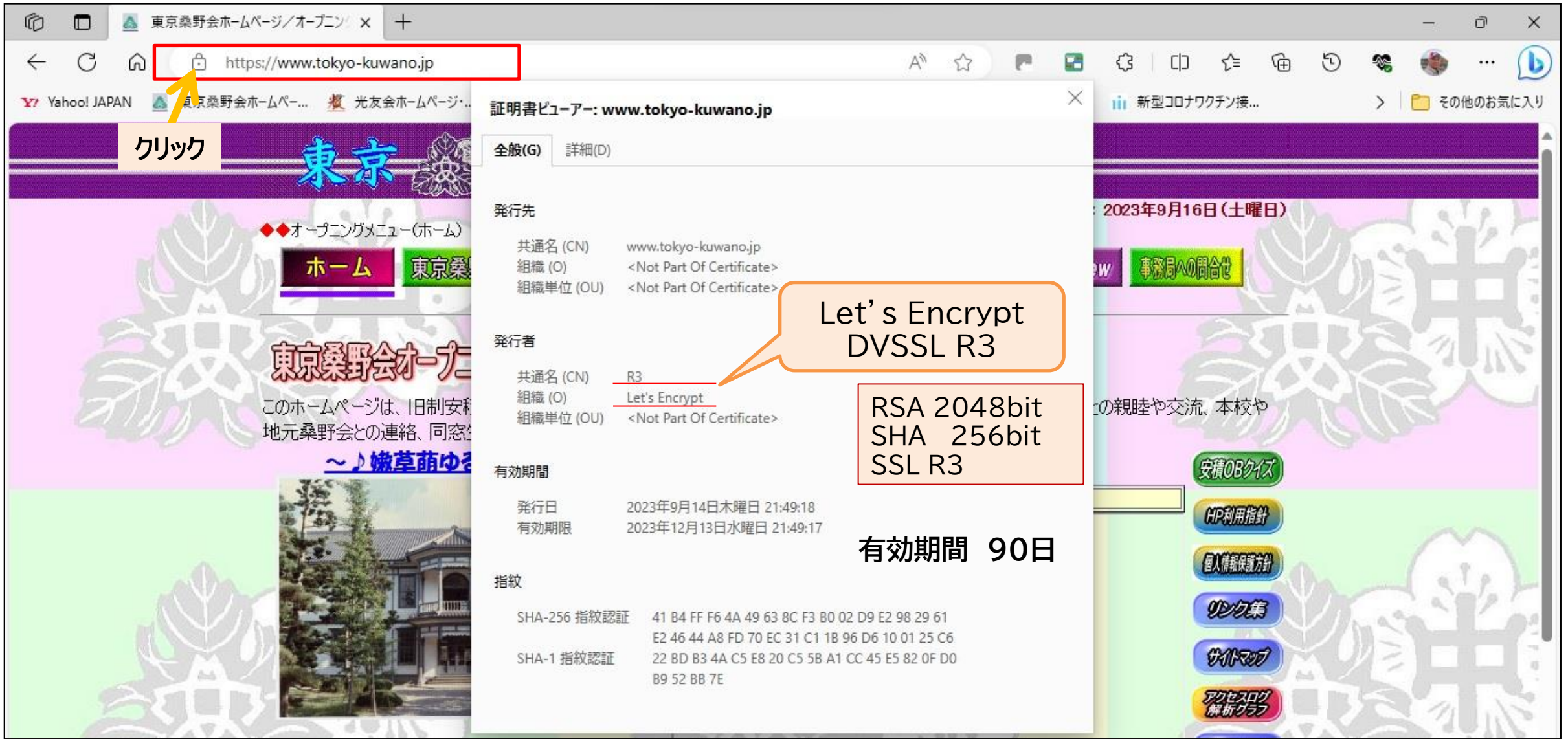
（4）**最大の違い**は

通信が暗号化され、悪意のある第三者によるデータの「盗み見」、「改ざん」、「差替え」 等のリスクが大きく低減された。特に個人情報の漏洩を防止できる。

※） 元々サーバー内には、会員の個人情報は保存していない。「会員情報登録・変更届」頁の入力データは、**サーバーには保存されない**。

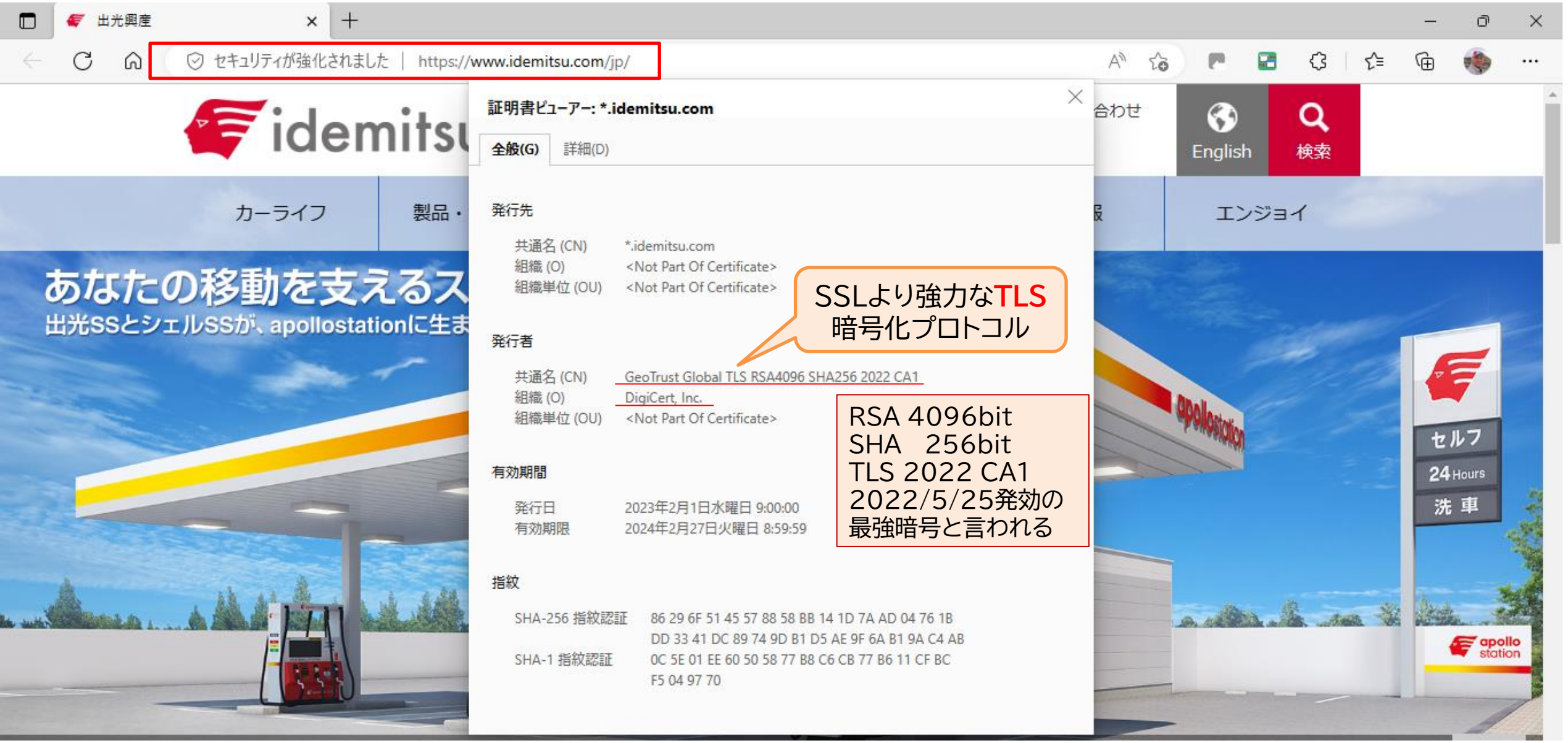
ブラウザに表示される証明書

ブラウザの画面から、光友会が導入したSSL証明書の内容を読み取ることができる。
ブラウザ画面左上のセキュリティ表示「**錠前マーク**」を、クリックしてポップアップから入る。



【例示】出光興産株式会社ホームページのSSL証明書

米国DigiCert社の企業認証型を採用し、暗号化強度が高い。



3. 【結論】 情報の保護や通信の安全性は向上したのか

3－1 SSL証明書の効果

「無料ドメイン認証SSL」 とは言え

（1） 暗号化強度の程度は劣るが、情報は保護され通信の安全性は向上した。

（2） 実在証明としてはSSL証明書だけでは弱いが、従来の証明書なし非SSL通信と比較すると格段に高いレベルが維持されている。

3－2 運用実務

従来型非SSLホームページの運用となんら変化はないが、SSL証明書の有効期限に注意を払う必要がある。有効期間90日間で、更新は自動であるがドメインの実在確認チェックが入る。また、大手のプロバイダーに乗り換えたことで、より良い運用管理サービスを甘受できるようになった。

3－3 結　論

「大手企業や金融機関のホームページ」ほどではないものの・・・・

情報の保護や通信の安全性は、
大きく向上した！！

以　上