

digicert®

EV 証明書に関する 顧客の知識強化コンテンツキット



EV 証明書に関する顧客の知識強化コンテンツキット

EV SSL 証明書をご利用いただきありがとうございます。

企業ブランドや個人のアイデンティティ、オンラインでの顧客体験の毀損を防ぐために EV SSL をお選びいただき、ありがとうございます。EV SSL はアイデンティティとブランドに最高レベルの保護を提供します。

しかし、個人情報や財務内容を保護するために EV SSL が最適である理由とその仕組みを理解することは、顧客にとって容易ではありません。このコンテンツの目的は、お客様がオンライン保護への積極的な取り組みを示すことで、顧客やウェブサイト訪問者との間に信頼を築き上げられるようにすることです。ウェブサイトとそれを提供する企業のアイデンティティについて、真正であることを認識していただくことの重要性を理解する上でお役に立てれば幸いです。このキットに含まれるコンテンツは自由に編集して、顧客やウェブサイト訪問者と共有していただけます。

お客様のウェブチームがご利用できるよう、コンテンツにはさまざまなテキストや画像が含まれています。これらを編集し、ウェブページ、ブログ記事、メールキャンペーン、ソーシャルメディアなどで 사용할 ことができます。このキットで提供するファイルはすべて、こちらからダウンロードできます。セキュリティとプライバシーについてはすでに通知されているので、このキットでは、ウェブサイトアイデンティティが真正であることの重要性を顧客とウェブサイト訪問者に伝える方法をご紹介します。

敬具

デジサートチーム

目次

- I. メインコンテンツ
 - A. 違いはどこにある？
 - B. すべてのセキュリティやウェブサイト暗号化が同じであるとは限りません
 - C. ウェブサイト所有者を明確に把握するための情報提供
 - D. お客様の信頼と弊社ブランドのアイデンティティを最優先に
 - E. 弊社の取り組み
- II. その他の補足資料
 - A. 強化されたオンラインセキュリティ
 - B. ソーシャルメディアコンテンツ
 - C. 認証済みサイトを確認するための詳しい手順
 - D. 適切なウェブブラウザの選択

違いはどこにある？

表示しているウェブサイトが真正であることを見分ける方法

各位

平均的な人は、毎日7時間もオンラインで時間を費やしており、その半分は携帯電話の使用によるものであることをご存知でしたか。つまり、1年に106日間も費やしていることになります。¹

直接誰かと会うのとは違い、特定のウェブサイトが正当または真正であると確認することは、たとえブラウザに「安全」と表示されていても、簡単ではありません。

そこで、デスクトップコンピューターからウェブサイトのSSLサーバ証明書の見え方を考察して、そのブランド名のセキュリティが侵害されていないことを確認する方法をご紹介します。

1 EV SSL によるセキュリティ

アドレスバーの鍵マークアイコンをクリックし、SSLサーバ証明書を表示します。弊社のウェブサイトは、デジサートが提供するEV SSL証明書によってセキュリティ保護されています。高度なブランド保護を提供するこの証明書は、弊社がこのウェブサイトのドメインを正式に所有し、ウェブサイトが示す企業であることに間違いのないことを証明します。証明書の詳しい確認方法は、こちらをご覧ください。

2 ルート証明書の確認

証明書の詳細情報で、EVルートを確認します。これは、そのブランドが、SSLサーバ証明書を保護するための18の手順からなる認証および審査プロセスに合格したことを意味しています。

3 サイトシールのチェック

サイトがEV証明書を使用していない場合は注意が必要です。DigiCert サイトシールや Norton サイトシールなど、その他の信頼できるマークを探します。

¹ <https://thenextweb.com/tech/2019/01/31/study-shows-were-spending-an-insane-amount-of-time-online/>

すべてのセキュリティやウェブサイト暗号化が同じであるとは限りません

私たちは、お客様のデータプライバシーとセキュリティを守るために一切の妥協を許しません。このため、弊社のウェブサイトをデジサートによる EV SSL 証明書で保護しています。

アドレスバーに「安全」鍵マークのついたウェブサイトであっても、セキュリティがそれぞれ異なることをご存知でしたか？

ブラウザに表示される「安全」というウェブサイトメッセージが意味するのは、そのサイトが暗号化を使用しているということだけです。お客様がご自分の情報を送信しているウェブサイトが、第三者による確認もされていない偽のウェブサイトだったとしたらどうなるでしょうか。EV SSL 証明書を取得している弊社は、18 の手順からなる認証プロセスに合格しているので、URL が真正かつ正当な所有者のものであることが確認されています。

3 種類の SSL サーバ証明書によって、ウェブサイトの真正性がどの程度認証されているのかを確認してみましょう。

1 DV SSL

安価で迅速な、暗号化とドメインの認証のみを行う SSL サーバ証明書です。ウェブサイトから連想される企業が所有者とは異なる可能性がありますがあるので、使用には注意が必要です

2 OV SS

ウェブサイトの管理者が公に知られた本当の企業であることが確認されています。認証されるのは、企業の実在性と名称です

3 EV SSL

高度な手段を用いて、企業の真正性と正当性が認証されています。

オンラインセキュリティの重要性が高い場合は、最高レベルの SSL でブランド保護された正当なウェブサイトであることを確認することをお勧めします。

安全なウェブサイトの確認方法について詳しくは、こちらをご覧ください。

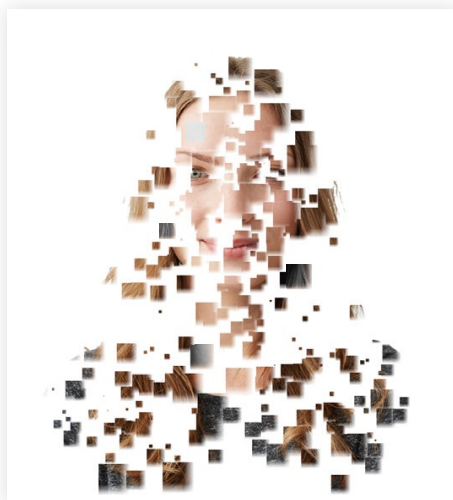
ウェブサイト所有者を明確に把握するための情報提供

お客様のオンラインセキュリティは、私たちが最も大切にしているものの1つです。そのため、当社のウェブサイトでは、(社名) が実在する (社名) であることを確実にお知らせできるように、EV SSL 証明書を使用しています。3 種類の SSL サーバ証明書について簡単に紹介し、オンラインにおける企業ブランドのアイデンティティ保護を重視する企業に、EV SSL が最善の保護を提供する理由を説明します。



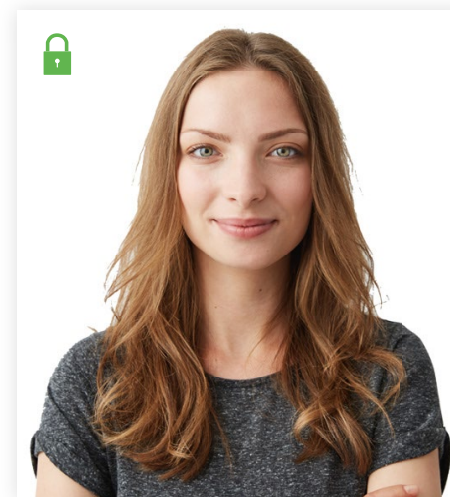
ドメイン認証 SSL (DV)

証明書が提供するのは最低限の認証なので、匿名の組織でも証明書を取得できます。サイト所有者は不確かで、名称も明かされません。



企業認証 SSL (OV)

証明書は、ブランドを保護するための追加チェックを提供します。100% ではありませんが、サイト所有者の実在をある程度確認できます。



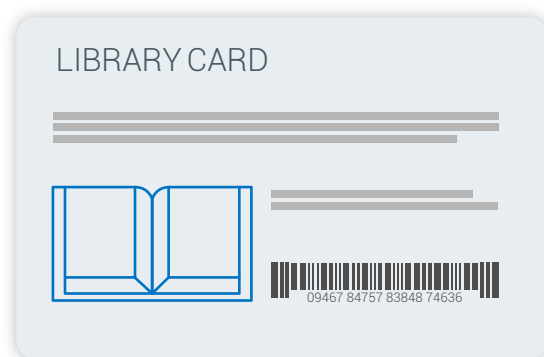
拡張認証 SSL (EV)

証明書は最高水準のブランド保護を提供します。EV の取得により、安全な取引への積極的な取り組みを顧客に知らせることができます。自分の機密情報を共有するサイト所有者について全面的に把握できます。

お客様の信頼とブランドのアイデンティティを最優先に

顧客が期待する真正性のレベル

当社は、私たちがオンラインで表明しているとおりの実在企業であることを証明することができます。当社のウェブサイトは、デジサートによる EV SSL 証明書で保護されているので、顧客の不正行為とアイデンティティ盗難を防ぐ最高レベルのセキュリティ保護が提供されています。また、お客様のデータがウェブサイト上で安全に暗号化されることが立証されています



ドメイン認証 SSL (DV) 証明書

DV SSL 証明書が保証するのは、一般的な図書館カードと似たような最低限のアイデンティティ真正性なので、匿名に近い状態です。



企業認証 SSL (OV) 証明書

OV SSL 証明書の審査には、運転免許証などの標準的な ID 形式と同じように、もう少し複雑な取得手順が必要になります



EV SSL 証明書

パスポートは最も価値の高い ID です。EV SSL 証明書と同じように、より高度で厳格な取得プロセスが必要なので、外国政府からもアイデンティティを認められ、信頼してもらうことができます。

弊社の取り組み

オンラインでのお客様情報のセキュリティ

弊社のウェブサイトでは、お客様データのセキュリティを守るために特別な予防策を講じています。さらに、お客様ご自身がオンラインで情報を保護するためのヒントを紹介します。



鍵マークを見つけよう

表示しているウェブサイトが SSL (Secure Sockets Layer) 証明書によって暗号化されていることを確認します。ウェブサイトに「安全ではありません」というメッセージが表示される場合、お客様のデータが危険にさらされているおそれがあります。



詳しく調査

ブラウザに表示された鍵マークをクリックし、「詳細」を表示します。企業の所在地と法人組織が特定できるかを確認します。自分の情報を誰と共有しているのかを把握することは非常に重要です。



企業の真正性を確認

ハイアシュアランス (高い保証レベル) の EV SSL 証明書を取得している企業は、会社名、カテゴリ、所在地に関する詳細情報を提供して、正当な企業を代表したウェブサイトであることを証明します。



直感だけに頼らない

鍵マークが付いており、ブラウザで「安全」と表示される場合でも、フィッシングサイトである可能性は残っています。DV SSL 証明書は簡単に取得できるので、オンライン詐欺に悪用されることがよくあります。

弊社は SSL/TLS サーバ証明書の業界最大手のデジサートの EV SSL 証明書を使用することで、弊社ウェブサイト上のすべてのトランザクションを暗号化して保護しています。アイデンティティと暗号化に関するデジサートの専門性は、Fortune 500 企業の 89% と世界のトップ 100 銀行の 97% をはじめとする多くの革新的な企業から選ばれています。¹ SSL サーバ証明書の詳細と、SSL がインターネットセキュリティ全体にとって果たす重要な理由については、こちらをご覧ください。

¹ DigiCert Internal Customer Analysis 2017 10 Forbes Fortune 500 & Global 2000 2017 Publication

その他の補足資料



強化されたオンラインセキュリティ

お客様に最も安全なオンライン体験を提供するため、弊社は EV 証明書を使用してウェブサイトを保護しています。

ドメイン認証 SSL (DV) 証明書は、
ブランドのアイデンティティ認証を
提供しない最低限の証明書です。

DV

企業認証 SSL (OV) 証明書は、
企業の名称、状況、事業種別を
認証する追加チェックを提供します。
商業用途以外の一般ウェブサイト
に最適です。

OV

拡張認証 SSL (EV) 証明書は、
最高レベルの審査と顧客が安心して
取引できる真正性を必要とする
全面的なアイデンティティ証明書です。

EV

ソーシャルメディアコンテンツのサポート

次のソーシャルメディア記事を自社チャンネルで共有することで、フィッシング攻撃のリスクに関する顧客の理解を促します。

フィッシング攻撃により、
毎分
17,700ドル
の損失が発生しています

[Top cybersecurity facts, figures and statistics for 2020, March 2020](#)

フィッシング攻撃は、
報告されるセキュリティ
インシデントの
80%以上を
占めています

[Top cybersecurity facts, figures and statistics for 2020, March 2020](#)

現在では、ほぼすべての企業が鍵マークと何らかの暗号化を使用しています。このため、弊社のように、ブランド名とお客様のセキュリティの保護を大切にする企業は、EV SSL 証明書を使用しています。

EV SSL 証明書はフィッシング攻撃の防止に最適な手段です。このため、弊社のように、ブランド名とお客様のセキュリティの保護を大切にする企業は、EV SSL 証明書を使用しています。

認証済みサイトを確認するための詳しい手順

ウェブブラウザで SSL/TLS サーバ証明書を表示する方法を紹介します。ご使用のブラウザ (Firefox, Safari, Chrome) 向けの手順をご参照ください。

Firefox

ステップ 1
ブラウザの
鍵アイコンを
クリックします

ステップ 2
矢印をクリックして
次のウィンドウを
表示します

ステップ 3
「詳細を表示」をクリックして
証明書情報ウィンドウを展開します



ドメイン認証 SSL (DV) 証明

証明書

www.DV-certificate-example.com	Organization Validated Server	Organization Validated Root
Subject Name Common Name www.DV-certificate-example.com		
Issuer Name Country US Organization DigiCert Inc Common Name DigiCert Global CA G2		
Validity Not Before 3/3/2020, 5:00:00 AM (Mountain Daylight Time) Not After 8/1/2020, 6:00:00 AM (Mountain Daylight Time)		

ドメイン認証 SSL (DV) 証明

証明書

www.DV-certificate-example.com	Organization Validated Server	Organization Validated Root
Subject Name Country or Region US State/Province California Locality San Francisco Organization OV Certificate Example Common Name www.OV-certificate-example.com		
Issuer Name Country US Organization DigiCert Inc Common Name DigiCert Global CA G2		
Validity Not Before 3/3/2020, 5:00:00 AM (Mountain Daylight Time) Not After 8/1/2020, 6:00:00 AM (Mountain Daylight Time)		

ドメイン認証 SSL (DV) 証明

証明書

www.EV-certificate-example.com	Extended Validated Server	Extended Validated Root
Subject Name Business Category Private Organization Inc. Country/Region US Inc. State/Province California Serial Number 5299537-0142 Country or Region US State/Province California Locality San Francisco Organization EV Certificate Example Organizational Unit DCG-PSG Common Name www.EV-certificate-example.com		
Issuer Name Country US Organization DigiCert Inc Organizational Unit www.EV-certificate-example.com Common Name DigiCert Global CA G2		
Validity Not Before 3/3/2020, 5:00:00 AM (Mountain Daylight Time) Not After 8/1/2020, 6:00:00 AM (Mountain Daylight Time)		

Safari

ステップ 1

ブラウザの
鍵アイコンを
クリックします

ステップ 2

「証明書を表示」をクリックして
ウィンドウを展開します

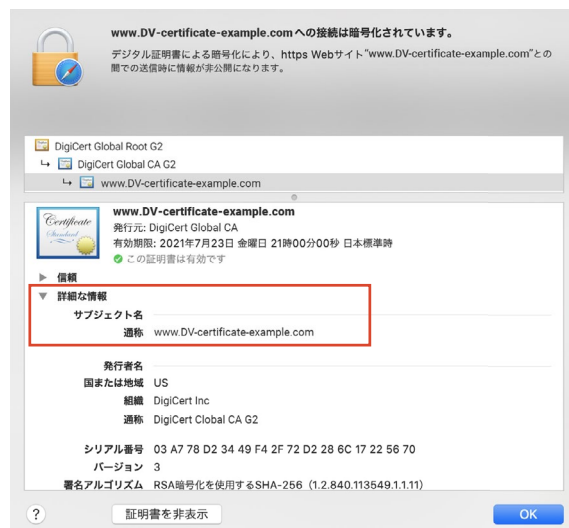


ステップ 3

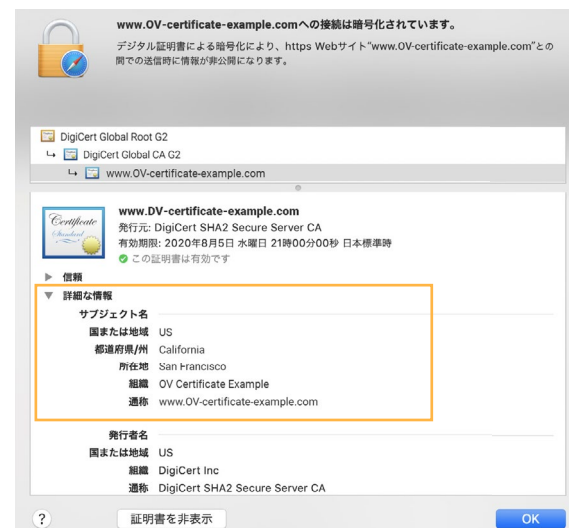
グレーの三角形をクリックして
詳細を表示します



ドメイン認証 SSL (DV) 証明書



企業認証 SSL (OV) 証明書



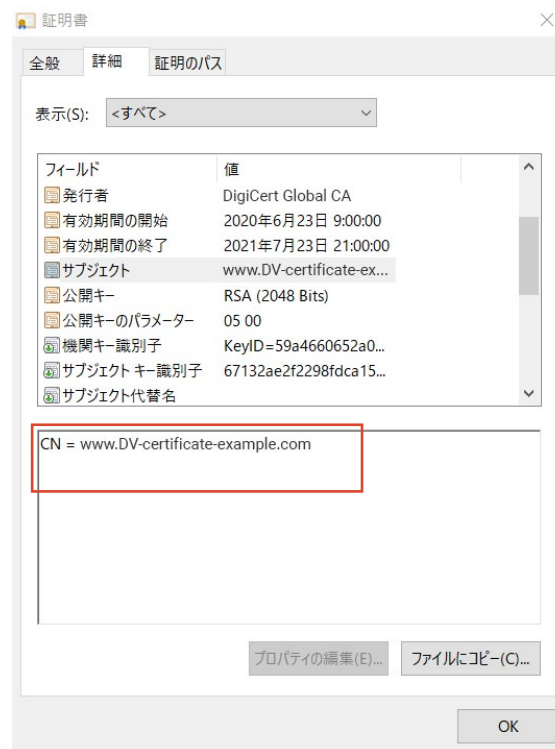
拡張認証 SSL (EV) 証明書



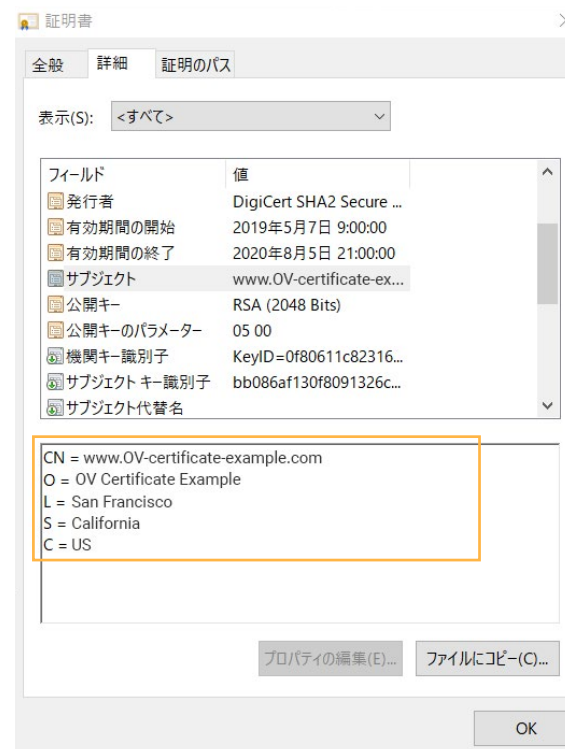
Chrome



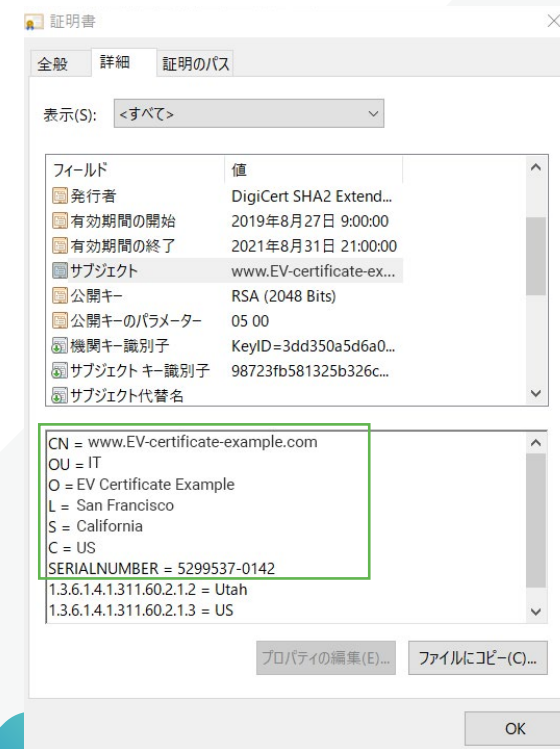
ドメイン認証 SSL (DV) 証明書



企業認証 SSL (OV) 証明書



拡張認証 SSL (EV) 証明書



安全なウェブブラウジング

すべてのウェブブラウザが、同じように作られているわけではありません。オンラインでのプライバシーとセキュリティに関して言うと、一部のウェブブラウザはセキュアであっても、インターネット上のユーザーのアクティビティを追跡して利用するために、より多くのデータを収集します。最大限のプライバシーとセキュリティを確保するために次の3種類のブラウザを使用することを推奨しています。

1. **Firefox** – クッキーとデータ収集をブロックするように設定できます
2. **Brave** – すべてのウェブサイトに強制的にセキュアな HTTPS 暗号化を適用します
3. **Tor** – このブラウザはユーザーの現在地を隠すことができます



複数のブラウザの使用

たとえば、個人アカウントは Safari のみで使用し、インターネットブラウジングには Firefox を使用する、またはその逆など。



SSL サーバ証明書の確認

アドレスバーの鍵マークアイコンをクリックし、詳細を表示します。表示しているウェブサイトが認証済みであることを確認します。



「安全ではない」ウェブサイトの回避

「安全ではありません」とメッセージが表示されるウェブサイトは、SSL サーバ証明書を使用していないので、入力するデータがハッカーに傍受されるおそれがあります。

弊社はお客様のオンラインセキュリティ保護に積極的に取り組んでいます。そのため、弊社ウェブサイトには、デジサートによるハイアシュアランスの EV SSL 証明書を導入しています。SSL サーバ証明書の重要性について詳しくは、[こちら](#)をご覧ください。

