

## HTTPSサイトだからといって 油断していませんか？

インターネットをするとき、「HTTPS」のサイトだから大丈夫だと油断していませんか？

HTTPSサイトで使われている「SSL/TLSサーバ証明書」の認証レベルの違いを知って、偽サイトやフィッシングサイトの被害に遭わないようにしましょう。

### HTTPSサイトについて

HTTPSサイトでは、SSL/TLSサーバ証明書を用いてサーバの認証や通信の暗号化を行うことで、なりすましや盗聴などを防いでいるため、HTTPSサイト＝安全なサイトと思ってしまうがちですが、一概にそう言うことはできません。

そこで参考になるのがSSL/TLSサーバ証明書の認証レベルです。

SSL/TLSサーバ証明書には、証明書発行の審査が簡易なものから厳格なものまで3つの認証レベルがあり、サイトの用途などによって使い分けられています。

### SSL/TLSサーバ証明書の認証レベルについて

#### 認証レベル1：DV証明書（ドメイン認証・Domain Validation）

ドメインの登録者のみを確認して発行される証明書。  
個人情報や決済情報などの重要な情報を入力しないサイト、誰が運営しているか確認する必要のないサイトなどで使われている。

#### 認証レベル2：OV証明書（企業認証・Organization）

ドメインの登録権の他に、ウェブサイトの運営組織が実在するかどうかなどを審査した上で発行される証明書。  
企業の実在性が証明されており、会員制サイトなど個人情報の入力が必要なサイトなどで使われている。

#### 認証レベル3：EV証明書（Extended Validation）

OV証明書より更に厳格な審査を基に発行される証明書。  
申請組織が法的にも物理的にも存在するかなど、審査方法が最も厳格であり、ネットバンクなど決済情報の入力が必要なサイトなどで使われている。

# SSL/TLSサーバ証明書の認証レベル確認方法

最も厳格な審査を受けて発行されるEV証明書を用いているサイトについては、**アドレスバーが緑色に変わる** など一目で分かるようになっているものもありますが、DV証明書とOV証明書については、アドレスバーの表示だけでは見分けがつかないことが多いです。

証明書の種類ごとの各ブラウザのアドレスバー表示

ブラウザ	証明書なし	DV証明書	OV証明書	EV証明書
Google Chrome (Windows) Ver. 65.0.3325.162				
Google Chrome (Android) Ver. 65.0.3325.109				
Microsoft Edge Ver. 41.16299.15.0				
Firefox Ver. 59.0.1				
Safari (Mac) Ver. 11.0.3				
Safari (iOS) Ver. 11.0.3				

画像引用：フィッシング対策協議会 ([https://www.antiphishing.jp/news/info/\\_ssllooks\\_20180327.html](https://www.antiphishing.jp/news/info/_ssllooks_20180327.html))

DV証明書とOV証明書の見分け方については、証明書の内容を確認することで判別することができますが、以下のチェックサイトを利用することで簡単に判別することもできます。

チェックサイト <https://cryptoreport.websecurity.symantec.com/checker/>

**Symantec.CryptoReport** Pick a tool

Check your SSL/TLS certificate installation

www.symantec.com **Check**

CryptoReport is moving!  
Symantec CryptoReport is moving to DigiCert SSL Tools. The new home offers improved scan selection and report results. Don't forget to bookmark the new address!

**Certificate information**  
**DV** This server uses a Domain Validated (DV) certificate. Your data is protected, but exchanging personal information is not.

**Common name:** www.symantec.com  
**SAN:** www.symantec.com

**Valid from:** 2018-Jul-27 00:19:02 GMT  
**Valid to:** 2018-Oct-25 00:19:02 GMT

**Certificate status:** Valid  
**Revocation check method:** OCSP

**Certificate information**  
**OV** This server uses an Organizationally Validated (OV) certificate, validated by Cybertrust Japan Co., Ltd. to help protect your data.

**Common name:** www.symantec.com  
**SAN:** www.symantec.com, www.symantec.com

**Valid from:** 2017-Sep-01 07:04:40 GMT  
**Valid to:** 2020-Sep-30 14:59:00 GMT

**Certificate status:** Valid  
**Revocation check method:** OCSP

**Certificate information**  
**EV** This server uses an Extended Validation (EV) certificate, validated by DigiCert Inc to help secure personal and financial information.

**Common name:** www.symantec.com  
**SAN:** www.symantec.com

**Valid from:** 2018-Jun-18 00:00:00 GMT  
**Valid to:** 2019-Aug-19 12:00:00 GMT

**Certificate status:** Valid  
**Revocation check method:** OCSP

偽サイトやフィッシングサイトの中には、認証が比較的容易なDV証明書を利用したHTTPSサイトのところもあります。

HTTPSサイトだからといって安心せず、サイトに記載されている内容に不審な点はないかなどしっかりチェックして、被害に遭わないようにしましょう。