デジサート認定資格プログラム
SSL/TLS トレーニングガイド

はじめに

このトレーニングガイドは「デジサート認定資格プログラム：SSL/TLS」認定試験の準備のためにデザインされています。試験は 50 問の選択式/択一式の問題で構成されます。制限時間は 1 時間です。

この試験は、技術的な役割で SSL/TLS に関わるあらゆる方(例えばテクニカルサポートや SSL/TLS 証明書を扱うサーバー管理者など)を受験者として想定しています。

試験項目

「デジサート認定資格プログラム：SSL/TLS」認定試験を受験する前に、以下の知識・能力を習得しておくことが望まれます。

- SSL/TLS の主な目的と機能
- SSL/TLS の歴史およびバージョン
- 対象鍵暗号方式および非対称鍵暗号方式
- 電子署名の仕組み
- SSL/TLS 証明書の詳細(例えば拡張子、ファイルフォーマット等)
- DV、OV、EV ならびにプライベートの各カテゴリの証明書
- EV 証明書の利点
- SAN ならびにワイルドカード証明書
- ドメイン名利用権確認ならびに組織認証の方法論
- SSL/TLS の「ハンドシェイク」の仕組み(例えばルート証明書、中間証明書、End-Entity 証明書ならびにクロスルート証明書の役割等
- CRL および OCSP による失効確認の仕組み(例えば OCSP ステイプリング等)
- TLS 鍵交換、暗号化、署名ならびにハッシュで用いられる一般的なアルゴリズム

- 前方秘匿性(forward secrecy)
- TLS における楕円曲線暗号(ECC)の利点
- 不適切な証明書の使用の危険性(例えば期限切れ証明書、自己署名証明書ならびにサーバー機器の出荷時に設定されているデフォルト鍵を用いた証明書等
- 廃止されたプロトコルにおける脆弱性(例えば Heartbleed 等)
- フィッシングサイトの目的と仕組み
- SNI(Server Name Indication)
- CT(Certificate Transparency)
- CAA(Certificate Authority Authorisation)
- 証明書ピニング
- HSTS(HTTP Strict Transport Security)
- HTTP/2
- 「常時 SSL(Always-on SSL)」の目的と仕組み
- CA/ブラウザフォーラムの役割
- セキュリティおよびパフォーマンスの観点での SSL/TLS のベストプラクティス
- ACME プロトコル
- Google AMP (Accelerated Mobile Pages)、SXG(Signed HTTP Exchange)ならびに Delegated Credentials
- 一般的な SSL/TLS ツール(例えば OpenSSL、Java Keystore 等)

トレーニングガイド

試験を受けていただく前に上述の試験項目に対して十分な復習していただくことを推奨します。もし追加の準備が必要と感じる場合は、該当の項目に対して、さらに詳細なリサーチをいただくことを推奨します。

この試験でカバーする項目が詳細に紹介されている E-ラーニングサイト、資料のダウンロードページおよび関連するウェブサイトへのリンクを以下にご紹介します。これらのリソースはあくまで一例であり、この試験のために十分な知識・能力を習得いただくためにはより広い範囲でのリサーチをいただくことを推奨します。推奨するリサーチには、例えばインターネット上の情報の収集(例えば Wikipedia 等)や、デジサートが提供する製品・ツール類を用いたハンズオントレーニング等が含まれます。

また、ここでご紹介した自己学習に加えて、デジサートの専門家がインストラクターとして、この試験でカバーするトピックをより深く解説するワークショップにご参加いただくことが可能です。詳細についてはデジサートまでお問合せください。

（参考）自己学習のためのリンク集(リンク先のコンテンツは英語となります)

SSL Best Practice Workshop Student Guide	https://www.digicert.com/digicert-tls-ssl-certified-expert/#downloads
NIST SP 1800-16: Securing Web Transactions: TLS Server Certificate Management	https://csrc.nist.gov/publications/detail/sp/1800-16/final
TLS Best Practice eBook	https://www.digicert.com/resources/tls-best-practices.pdf
SSL/TLS and PKI History	https://www.feistyduck.com/ssl-tls-and-pki-history/

ウェブサイト

CA ブラウザーフォーラム Baseline Requirement	https://cabforum.org/baseline-requirements-documents/
CA ブラウザフォーラム EV ガイドライン	https://cabforum.org/extended-validation/
TLS 1.2 (RFC 5246)	https://tools.ietf.org/html/rfc5246
TLS 1.3 (RFC 8446)	https://tools.ietf.org/html/rfc8446
OCSP (RFC 6960)	https://tools.ietf.org/html/rfc6960
SNI (RFC 6066)	https://tools.ietf.org/html/rfc6066#section-3
CAA (RFC 6844)	https://tools.ietf.org/html/rfc6844 https://www.digicert.com/blog/new-caa-requirement-2/
HSTS (RFC 6797)	https://tools.ietf.org/html/rfc6797
HTTP/2 (RFC 7540)	https://tools.ietf.org/html/rfc7540
ACME (RFC 8555)	https://tools.ietf.org/html/rfc8555
AMP & SXG	https://www.digicert.com/google-amp-security-solutions/ https://www.digicert.com/blog/googles-signed-http-exchange-solution-displays-publisher-urls-for-amp-pages-via-tls/
Delegated Credentials	https://blog.cloudflare.com/keyless-delegation/
Certificate Transparency	https://www.certificate-transparency.org/
US Government Compliance Guide	https://https.cio.gov/guide/#compliance-and-best-practice-checklist
常時 SSL(Always-on SSL)	https://otalliance.org/resources/always-ssl-aossl https://casecurity.org/2016/09/30/always-on-ssl/ https://www.digicert.com/always-on-ssl.htm
OpenSSL	www.openssl.org https://www.feistyduck.com/books/openssl-cookbook/
一般的な CSR 作成方法	https://www.digicert.com/csr-creation.htm
一般的な SSL/TLS 証明書のインストール方法	https://www.digicert.com/ssl-certificate-installation.htm

証明書のファイルフォーマット	https://knowledge.digicert.com/generalinformation/INFO4448.html

E-ラーニング (YouTube)

Cryptography Overview (8:31)
Symmetric vs. Asymmetric Encryption (4:18)
Public Keys and Private Keys (4:10)
Session Keys (4:22)
Block vs. Stream Ciphers (3:13)
Hashing (3:30)
Perfect Forward Secrecy (3:38)
Cryptographic Hash Functions (7:04)
Symmetric Encryption Ciphers (6:42)
Asymmetric Cryptography Algorithms (2:36)
Certificate Authorities (2:52)
Key Revocation (3:31)
Digital Certificates (3:01)
Public Key Infrastructure (3:33)