openssl.cnfの変更点

2020年6月　初版

OpenSSLの設定ファイル（openssl.cnf）のデフォルト設定からの変更箇所は下記の通りです。

■ 証明書のsubjectの重複を許可

【変更前】
#unique_subject = no # Set to 'no' to allow creation of
【変更後】
unique_subject = no # Set to 'no' to allow creation of

■ CA署名時にSAN(Subject Alternative Name)を渡す
複数のDNS名(ホスト名)を扱う場合に利用するx.509証明書のオプション

【変更前】
copy_extensions = copy
【変更後】
copy_extensions = copy

■　装置の証明書の有効期限を20年、署名アルゴリズムをSHA256に変更
　★装置の証明書の有効期限はお客様の運用に合わせて適切に変更お願いします。

【変更前】
default_days = 365 # how long to certify for
…
default_md = default # use public key default MD
【変更後】
default_days = 7300 # how long to certify for
…
default_md = sha256 # use public key default MD

■ どのようなCSR(証明書要求)に対して証明書を発行するか「ポリシー」を設定

【変更前】
countryName = match
stateOrProvinceName = match
organizationName = match
【変更後】
countryName = supplied
stateOrProvinceName = optional
organizationName = supplied

■ extendedKeyUsageを追加(サーバー認証)

extendedKeyUsage = 1.3.6.1.5.5.7.3.1