

企業認証SSL (SKIP申込サービス、SSLマネージドサービス含む)

フィールド名はInternetExplorerで表示される証明書を参考にしてしています。変更箇所は黄色で表示しています。

フィールド名	新証明書	旧証明書
バージョン	2017年11月6日午後14:00以降発行分 V3	2011年6月27日午前9:00以降発行分 V3
シリアル番号	自動割当	自動割当
署名アルゴリズム	sha256RSA	Sha1RSA
有効期限の開始	自動割当	自動割当
有効期限の終了	自動割当	自動割当
発行者	CN=GlobalSign Organization Validation CA - SHA256 - G2 O=GlobalSign nv-sa C=BE	CN=GlobalSign Organization Validation CA - G2 O=GlobalSign nv-sa C=BE
サブジェクト	CN=コモンネーム O=組織名 OU=部署名 L=市区町村 S=都道府県 C=国名	CN=コモンネーム O=組織名 OU=部署名 L=市区町村 S=都道府県 C=国名
公開キー	RSA 2048bit	RSA 2048bit
機関キー識別子	KeyID=96 de 61 f1 bd 1c 16 29 53 1c e0 cc 7d 3b 83 00 40 e6 1a 7c	KeyID=5d 46 b2 8d c4 4b 74 1c bb ed f5 73 b6 3a b7 38 8f 75 9e 7e
サブジェクト キー識別子	自動割当	自動割当
CRL 配布ポイント	http://crl.globalsign.com/globalsign.com/globalsignvalsha2g2.crl	http://crl.globalsign.com/globalsign.com/globalsignvalg2.crl
キー使用法	Digital Signature, Key Encipherment (a0)	Digital Signature, Key Encipherment (a0)
サブジェクトの別名	自動割当	自動割当
拡張キー使用法	サーバー認証 (1.3.6.1.5.5.7.3.1) クライアント認証 (1.3.6.1.5.5.7.3.2)	サーバー認証 (1.3.6.1.5.5.7.3.1) クライアント認証 (1.3.6.1.5.5.7.3.2) 不明なキー使用法 (1.3.6.1.4.1.3.11.10.3.3)
機関情報アクセス	[1]Authority Info Access Access Method=証明機関の発行者 (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://secure.globalsign.com/cacert/globalsignvalsha2g2r1.crt [2]Authority Info Access Access Method=オンライン証明書状態プロトコル (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp2.globalsign.com/globalsignvalsha2g2	[1]Authority Info Access Access Method=証明機関の発行者 (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://secure.globalsign.com/cacert/globalsignvalg2eku.crt
証明書ポリシー	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.4146.1.20 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.globalsign.com/repository/ [2]Certificate Policy: Policy Identifier=2.23.140.1.2.2	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.4146.1.20 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.globalsign.com/repository/
基本制限	Subject Type=End Entity Path Length Constraint=None	Subject Type=End Entity Path Length Constraint=None
1.3.6.1.4.1.11129.2.4.2	自動割当	
拇印アルゴリズム	sha1	sha1
拇印	自動割当	自動割当