

EV SSL ( SSLマネージドサービス含む )



フィールド名はInternet Explorerで表示される証明書を参考にしています。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 ( SHA-1 ) 2014年12月24日午前0時以降発行分	新証明書 ( SHA256 ) 2014年12月24日午前0時以降発行分	旧証明書 2014年12月24日午前0時以前発行分
バージョン	V3	V3	V3
シリアル番号	自動割当	自動割当	自動割当
署名アルゴリズム	Sha1RSA	sha256RSA	Sha1RSA
署名ハッシュアルゴリズム	sha1	sha256	
有効期限の開始	自動割当	自動割当	自動割当
有効期限の終了	自動割当	自動割当	自動割当
発行者	CN=GlobalSign Extended Validation CA - G2	CN = GlobalSign Extended Validation CA - SHA256 - G2	CN=GlobalSign Extended Validation CA - G2
	O=GlobalSign nv-sa	O=GlobalSign nv-sa	O=GlobalSign nv-sa
	なし	なし	OU=項目削除
	C=BE	C=BE	C=BE
サブジェクト	CN=コモンネーム	CN=コモンネーム	CN=コモンネーム
	O=組織名	O=組織名	O=組織名
	OU=部署名	OU=部署名	OU=部署名
	STREET=住所	STREET=住所	STREET=住所
	L=市区町村	L=市区町村	L=市区町村
	S=都道府県	S=都道府県	S=都道府県
	C=国名	C=国名	C=国名
	1.3.6.1.4.1.311.60.2.1.3=登録管轄地	1.3.6.1.4.1.311.60.2.1.3=登録管轄地	1.3.6.1.4.1.311.60.2.1.3=登録管轄地
	SERIALNUMBER=会社法人等番号 または Government Entities	SERIALNUMBER=会社法人等番号 または Government Entities	SERIALNUMBER=会社法人等番号 または Government Entities
2.5.4.15=事業種別	2.5.4.15=事業種別	2.5.4.15=事業種別	
公開キー	RSA 2048bit	RSA 2048bit	RSA 2048bit
Netscape 証明書の種類	項目削除	項目削除	項目削除
機関キー識別子	KeyID=b0 b0 4a fd 1c 75 28 f8 1c 61 aa 13 f6 fa c1 90 3d 6b 16 a3	KeyID=cda 40 77 43 65 1c f8 fe a7 e3 f4 64 82 3e 4d 43 13 22 31 02	KeyID=b0 b0 4a fd 1c 75 28 f8 1c 61 aa 13 f6 fa c1 90 3d 6b 16 a3
サブジェクト キー識別子	自動割当	自動割当	自動割当
CRL 配布ポイント	http://crl.globalsign.com/gs/gxextendvalg2.crl	http://crl.globalsign.com/gs/gxextendvalsha2g2.crl	http://crl.globalsign.com/gs/gxextendvalg2.crl
キー使用法	Digital Signature, Key Encipherment (a0)	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	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)	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 (1.3.6.1.4.1.311.10.3.3)
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/gxextendvalg2.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/gxextendvalg2	[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/gxextendvalsha2g2.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/gxextendvalsha2g2	[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/gxextendvalg2eku.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/gxextendvalg2
証明書ポリシー	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.4146.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.globalsign.com/repository/	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.4146.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.globalsign.com/repository/	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.4146.1.1 [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	Subject Type=End Entity Path Length Constraint=None
拇印アルゴリズム	sha1	sha1	sha1
拇印	自動割当	自動割当	自動割当
1.3.6.1.4.1.11129.2.4.2	自動割当	自動割当	