

## クイック認証SSL (SKIP申込サービス含む)

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 2011年6月27日午前9:00以降発行分	旧証明書 2011年6月27日午前6時以前発行分
バージョン	V3	V3
シリアル番号	自動割当	自動割当
署名アルゴリズム	Sha1RSA	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 Domain Validation CA - G2	CN=GlobalSign Domain Validation CA
	O=GlobalSign nv-sa	O=GlobalSign nv-sa
	OU=項目削除	OU=Domain Validation CA
	C=BE	C=BE
サブジェクト	CN=コモンネーム	CN=コモンネーム
	O=項目削除	O=コモンネーム
	OU=Domain Control Validated	OU=Domain Control Validated
	C=国名	C=国名
公開キー	RSA 2048bit	RSA 2048bit
Netscape 証明書の種類	項目削除	SSL client, SMIME
機関キー識別子	KeyID=96 ad fa b0 5b b9 83 64 2a 76 c2 1c 8a 69 da 42 dc fe fd 28	KeyID=36 12 4e 9e 71 c4 26 41 f1 fa f1 29 4c bf 17 a4 53 28 b6 eb
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/gc/gsdomainvalg2.crl	http://crl.globalsign.net/DomainVal1.crl
キー使用法	Digital Signature, Key Encipherment (a0)	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment
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) 不明なキー使用法 (1.3.6.1.4.1.311.10.3.3)	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/gsdomainvalg2eku.crt	[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.net/cacert/dvhe1.crt
証明書ポリシー	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.4146.1.10 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.globalsign.com/repository/	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.4146.1.10 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.globalsign.net/repository/
基本制限	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
拇印	自動割当	自動割当