

セキュアメールID 製品仕様等変更点

分類1	分類2	～2023/8/29	～2024/6/26	変更後2024/6/27～
証明書	ルート	DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	DigiCert Assured ID Root G2
	中間CA証明書	DigiCert Assured ID SMIME RSA2048 SHA256 2021 CA1	DigiCert Assured ID SMIME RSA2048 SHA256 2021 CA1	DigiCert Assured G2 SMIME RSA4096 SHA384 2024 CA1
	End Entity証明書	(次頁参照)	(次頁参照)	(次頁参照)
端末対応率	各種メーラ	変更なし	変更なし	変更なし (* 1)
階層構造 オプション	ハッシュアルゴリズム	SHA-2	SHA-2	SHA-2

*1 DigiCert Assured ID Root G2は2013年に作成され、既に10年以上の運用実績があるルート認証局である。現在使用されているソフトウェア環境においては原則として信頼されている状態にある。

セキュアメールID END-ENTITY 証明書プロファイルの比較

項目	～2023/8/29	～2024/6/26	変更後 2024/6/27～
Subejct: (証明書サブジェクト)	CommonName = [申請団体名] Organizationa Unit = [申請団体 部署名] Organization = [申請団体名] Locality = [市区町村] State = [都道府県] Country = JP	CommonName = [申請団体名] Organization = [申請団体名] Locality = [市区町村] State = [都道府県] Country = JP 2.5.4.97 = [OrgnizationIdentifier/組織の法人登録番号]	CommonName = [申請団体名] Organization = [申請団体名] Locality = [市区町村] State = [都道府県] Country = JP 2.5.4.97 = [OrgnizationIdentifier/組織の法人登録番号]
Subject Alternative Name: (サブジェクト代替名)	[セキュアメールID Eメールアドレス]	[セキュアメールID Eメールアドレス]	[セキュアメールID Eメールアドレス]
Key Usage: (鍵用途)	critical Digital Signature, Key Encipherment	critical Digital Signature, Key Encipherment	critical Digital Signature, Key Encipherment
CRL Distribution Points: (CRL 配布点)	http://crl3.digicert.com/DigiCertAssuredIDSMIME RSA2048SHA2562021CA1.crl http://crl4.digicert.com/DigiCertAssuredIDSMIME RSA2048SHA2562021CA1.crl	http://crl3.digicert.com/DigiCertAssuredIDSMIMERSA2048S HA2562021CA1.crl http://crl4.digicert.com/DigiCertAssuredIDSMIMERSA2048S HA2562021CA1.crl	http://crl3.digicert.com/DigiCertAssuredG2SMIMERSA4096S HA3842024CA1.crl http://crl4.digicert.com/DigiCertAssuredG2SMIMERSA4096S HA3842024CA1.crl
Extended Key Usage : (拡張された鍵用途)	TLS Web Client Authentication, E-mail Protection	TLS Web Client Authentication, E-mail Protection	TLS Web Client Authentication, E-mail Protection
Certificate Policies: (証明書ポリシー)	2.16.840.1.114412.4.1.2	2.23.140.1.5.2.1	2.23.140.1.5.2.1
Authority Key Identifier: (Authority 鍵識別子)	E7:02:23:80:00:4F:D8:D7:BC:94:0B:D9:3F:74: 39:49:32:3C:8A:79	20:33:96:D3:66:66:DF:1D:DC:01:26:2B:DD:E2:E0:E2:76: C9:40:0C	F7:9B:A2:4E:D3:97:C5:F4:34:0F:43:0E:81:85:CE:91:93:3 2:AF:F9
Authority Information Access: (Authority 情報アクセス)	OCSP - URI:http://ocsp.digicert.com CA Issuers - URI:http://cacerts.digicert.com/DigiCertSHA2Ass uredIDCA.crt	OCSP - URI:http://ocsp.digicert.com CA Issuers - URI:http://cacerts.digicert.com/DigiCertAssuredIDSMIMERS A2048SHA2562021CA1.crt	OCSP - URI:http://ocsp.digicert.com CA Issuers - URI:http://cacerts.digicert.com/DigiCertAssuredG2SMIMERS A4096SHA3842024CA1.crt