文書番号	HPCI-CA03-002-08

HPCI 認証局
証明書/CRL プロファイル設計書
Ver1.7

2022.05.13

HPCI 認証局ポリシー管理委員会

改訂履歴

発行年月日	Ver.	改訂内容
2011.12.28	1.0	新規作成
2012.08.31	1.1	「1．1 CA 証明書プロファイル」、「1．2 クライアント証明書プロファイル」、「1．3 ホスト証明書プロファイル」、「1．4 サービス証明書プロファイル」、「2． CRL プロファイル」の signature の設定内容を SHA-2 対応として変更
2014.03.24	1.2	「1．1 CA 証明書プロファイル」にて、秘密鍵の長さを追記 「1．2 クライアント証明書プロファイル」、「1．3 ホスト証明書プロファイル」、「1．4 サービス証明書プロファイル」にて、秘密鍵の長さを追記、有効期限を「毎年 4 月 24 日」に修正、MICS プロファイルの OID を追記、cRLDistributionPoints の値を変更 「2． CRL プロファイル」にて、issuingDistributionPoint の記載を削除
2015.03.12	1.3	「1．4 サービス証明書プロファイル」にて、subjectAltName の値を変更
2016.05.12	1.4	「1．2 クライアント証明書プロファイル」「1．3 ホスト証明書プロファイル」「1．4 サービス証明書プロファイル」にて、Authority Information Access を追加 「1．5 OCSP レスポンダ証明書プロファイル」を追加
2016.08.10	1.5	OID の区切り文字を半角スペースからピリオドに修正 「1．2 クライアント証明書プロファイル」「1．3 ホスト証明書プロファイル」「1．4 サービス証明書プロファイル」にて、Extended Key Usage を追加 「1．2 クライアント証明書プロファイル」「1．3 ホスト証明書プロファイル」「1．4 サービス証明書プロファイル」「1．5 OCSP レスポンダ証明書プロファイル」にて、HPCI 認証局証明書ポリシーの OID を修正

2017.09.25	1.6	「1．2 クライアント証明書プロファイル」にて、有効期限を「発行してから 395 日後」に変更 「1．4 サービス証明書プロファイル」にて、「issuer」と「subject」の不要なスペースを削除。なお、発行済みのサービス証明書にはこの不要なスペースは含まれていない。 「2． CRL プロファイル」にて、「issuer」の不要なスペースを削除。なお、発行済みの CRL にはこの不要なスペースは含まれていない。
2022.05.13	1.7	「1．1 CA 証明書プロファイル」にて、CA 証明書の有効期間の記載を「有効期間は20年間を超えないものとする」に変更

目次

1. 証明書プロファイル **5**

1．1 CA 証明書プロファイル 5

1．2 クライアント証明書プロファイル 6

1．3 ホスト証明書プロファイル 8

1．4 サービス証明書プロファイル 10

1．5 OCSP レスポンダ証明書プロファイル 12

2. CRL プロファイル **14**

1. 証明書プロファイル

CA 証明書、クライアント証明書、ホスト証明書、サービス証明書の各プロファイルは、以下の通りとする。

1．1 CA 証明書プロファイル

名称	クリティカルフラグ	設定値又は設定内容
証明書基本領域		
version	－	V3
serialNumber	－	ユニークな値
signature	－	sha256WithRSAEncryption (2048bit) (OID=1.2.840.113549.1.1.11)
validity	－	
notBefore		有効期間は 20 年間を超えないものとする (UTCTime)
notAfter		
issuer	－	C=JP,O=NII,OU=HPCI,CN=HPCI CA (PrintableString でエンコードする)
subject	－	C=JP,O=NII,OU=HPCI,CN=HPCI CA (PrintableString でエンコードする)
subjectPublicKeyInfo	－	
algorithmIdentifier		rsaEncryption (2048bit) (OID=1.2.840.113549.1.1.1)
public key		公開鍵値
証明書拡張領域		
authorityKeyIdentifier	F	認証局鍵識別子
keyIdentifier		ユニークなバイト列
subjectKeyIdentifier	F	ユニークなバイト列
keyUsage	T	keyCertSign, CRLSign
basicConstraints	T	
cA		TRUE

1．2 クライアント証明書プロファイル

名称	クリティカルフラグ	設定値又は設定内容
証明書基本領域		
version	－	V3
serialNumber	－	ユニークな値
signature	－	sha256WithRSAEncryption (2048bit) (OID=1.2.840.113549.1.1.11)
validity	－	
notBefore		有効期限は発行してから 395 日後とする (UTCTime)
notAfter		
issuer	－	C=JP,O=NII,OU=HPCI,CN=HPCI CA (PrintableString でエンコードする)
subject	－	C=JP,O=NII,OU=HPCI,CN=ユーザ氏名 HPCI ID (PrintableString でエンコードする)
subjectPublicKeyInfo	－	
algorithmIdentifier		rsaEncryption (2048bit) (OID=1.2.840.113549.1.1.1)
public key		公開鍵値
証明書拡張領域		
authorityKeyIdentifier	F	認証局鍵識別子
keyIdentifier		ユニークなバイト列
subjectKeyIdentifier	F	ユニークなバイト列
keyUsage	T	digitalSignature, Key Encipherment
certificatePolicies	F	
policyIdentifier		
certPolicyId		HPCI 認証局証明書ポリシー (OID=1.3.6.1.4.1.32264.2.2)
(policyIdentifier)		
(certPolicyId)		MICS プロファイルの OID (OID=1.2.840.113612.5.2.2.5)
basicConstraints	T	

名称	クリティカルフラグ	設定値又は設定内容
cA		FALSE
cRLDistributionPoints	F	http://www.hpci.nii.ac.jp/ca/hpcica_crl.der
Authority Information Access	F	
OCSP - URI		http://ocsp.hpci.nii.ac.jp
Extended Key Usage	F	PKIX-IDKP-ClientAuth (OID=1.3.6.1.5.5.7.3.2)

1．3 ホスト証明書プロファイル

名称	クリティカルフラグ	設定値又は設定内容
証明書基本領域		
version	－	V3
serialNumber	－	ユニークな値
signature	－	sha256WithRSAEncryption (2048bit) (OID=1.2.840.113549.1.1.11)
validity	－	
notBefore		有効期限は毎年 4 月 24 日とする (UTCTime)
notAfter		
issuer	－	C=JP,O=NII,OU=HPCI,CN=HPCI CA (PrintableString でエンコードする)
subject	－	C=JP,O=NII,OU=HPCI,CN=ホスト名 (FQDN)
subjectPublicKeyInfo	－	
algorithmIdentifier		rsaEncryption (2048bit) (OID=1.2.840.113549.1.1.1)
public key		公開鍵値
証明書拡張領域		
authorityKeyIdentifier	F	認証局鍵識別子
keyIdentifier		ユニークなバイト列
subjectKeyIdentifier	F	ユニークなバイト列
keyUsage	T	digitalSignature, Key Encipherment
certificatePolicies	F	
policyIdentifier		
certPolicyId		HPCI 認証局証明書ポリシー (OID=1.3.6.1.4.1.32264.2.2)
(policyIdentifier)		
(certPolicyId)		MICS プロファイルの OID (OID=1.2.840.113612.5.2.2.5)
subjectAltName	F	ホスト名 (FQDN)
basicConstraints	T	
cA		FALSE

名称		クリティカルフラグ	設定値又は設定内容
	cRLDistributionPoints	F	http://www.hpci.nii.ac.jp/ca/hpcica_crl.der
	Authority Information Access	F	
	OCSP - URI		http://ocsp.hpci.nii.ac.jp
	Extended Key Usage	F	PKIX-IDKP-ServerAuth (OID=1.3.6.1.5.5.7.3.1)
			PKIX-IDKP-ClientAuth (OID=1.3.6.1.5.5.7.3.2)

1．4 サービス証明書プロファイル

名称	クリティカルフラグ	設定値又は設定内容
証明書基本領域		
version	－	V3
serialNumber	－	ユニークな値
signature	－	sha256WithRSAEncryption (2048bit) (OID=1.2.840.113549.1.1.11)
validity	－	
notBefore		有効期限は毎年 4 月 24 日とする (UTCTime)
notAfter		
issuer	－	C=JP,O=NII,OU=HPCI,CN=HPCI CA (PrintableString でエンコードする)
subject	－	C=JP,O=NII,OU=HPCI,CN=サービス名（サービス名/FQDN）
subjectPublicKeyInfo	－	
algorithmIdentifier		rsaEncryption (2048bit) (OID=1.2.840.113549.1.1.1)
public key		公開鍵値
証明書拡張領域		
authorityKeyIdentifier	F	認証局鍵識別子
keyIdentifier		ユニークなバイト列
subjectKeyIdentifier	F	ユニークなバイト列
keyUsage	T	digitalSignature, Key Encipherment
certificatePolicies	F	
policyIdentifier		
certPolicyId		HPCI 認証局証明書ポリシー (OID=1.3.6.1.4.1.32264.2.2)
(policyIdentifier)		
(certPolicyId)		MICS プロファイルの OID (OID=1.2.840.113612.5.2.2.5)
subjectAltName	F	ホスト名（FQDN）
basicConstraints	T	

名称	クリティカルフラグ	設定値又は設定内容
cA		FALSE
cRLDistributionPoints	F	http://www.hpci.nii.ac.jp/ca/hpcica_crl.der
Authority Information Access	F	
OCSP - URI		http://ocsp.hpci.nii.ac.jp
Extended Key Usage	F	PKIX-IDKP-ServerAuth (OID=1.3.6.1.5.5.7.3.1)
		PKIX-IDKP-ClientAuth (OID=1.3.6.1.5.5.7.3.2)

1．5 OCSP レスポンダ証明書プロファイル

名称	ｸﾘﾃｨｶﾙﾌﾗｸﾞ	設定値又は設定内容
証明書基本領域		
version	－	V3
serialNumber	－	ユニークな値
signature	－	sha256WithRSAEncryption (2048bit) (OID=1.2.840.113549.1.1.11)
validity	－	
notBefore		有効期限は毎年 4 月 24 日とする (UTCTime)
notAfter		
issuer	－	C=JP,O=NII,OU=HPCI,CN=HPCI CA (PrintableString でエンコードする)
subject	－	C=JP,O=NII,OU=HPCI,CN=ホスト名 (FQDN)
subjectPublicKeyInfo	－	
algorithmIdentifier		rsaEncryption (2048bit) (OID=1.2.840.113549.1.1.1)
public key		公開鍵値
証明書拡張領域		
authorityKeyIdentifier	F	認証局鍵識別子
keyIdentifier		ユニークなバイト列
subjectKeyIdentifier	F	ユニークなバイト列
keyUsage	T	digitalSignature, Key Encipherment
certificatePolicies	F	
policyIdentifier		
certPolicyId		HPCI 認証局証明書ポリシー (OID=1.3.6.1.4.1.32264.2.2)
(policyIdentifier)		
(certPolicyId)		MICS プロファイルの OID (OID=1.2.840.113612.5.2.2.5)
subjectAltName	F	ホスト名 (FQDN)
basicConstraints	T	
cA		FALSE

名称		ｸﾘﾃｨｶﾙﾌﾗｸﾞ	設定値又は設定内容
	cRLDistributionPoints	F	http://www.hpci.nii.ac.jp/ca/hpcica_crl.der
	Extended Key Usage	F	OCSP Signing (OID=1.3.6.1.5.5.7.3.9)

2. CRL プロファイル

CRL のプロファイルは、以下の通りとする。

名称	クリティカルフラグ	設定値又は設定内容
CRL 基本領域		
version	－	V2
signature	－	sha256WithRSAEncryption (OID=1.2.840.113549.1.1.11)
issuer	－	C=JP,O=NII,OU=HPCI,CN=HPCI CA (PrintableString でエンコードする)
thisUpdate	－	CRL の更新日(UTCTime)
nextUpdate	－	thisUpdate＋30 日(UTCTime)
revokedCertificates	－	
userCertificate		証明書シリアル番号
revocationDate		失効日時
CRL 拡張部		
authorityKeyIdentifier	F	認証局鍵識別子
keyIdentifier		ユニークなバイト列
authCertSerialNumber		ユニークな整数
cRLNumber	F	ユニークな整数