文書番号	HPCI-CA03-002-01

HPCI 認証局
証明書/CRL プロファイル設計書
Ver1.0

2011.12.28

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

目次

1.　証明書プロファイル.....4

1．1 CA証明書プロファイル.....4

1．2 クライアント証明書プロファイル.....5

1．3 ホスト証明書プロファイル.....7

1．4 サービス証明書プロファイル.....9

2.　CRLプロファイル.....11

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	－	sha1WithRSAEncryption (OID=1 2 840 113549 1 1 11)
validity	－	
notBefore		有効期間は 10 年間とする (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 (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	－	sha1WithRSAEncryption （OID=1 2 840 113549 1 1 11）
validity	－	
notBefore		有効期限は発行年度末＋1ヶ月とする （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 （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 32264 2 2）
(policyIdentifier)		
(certPolicyId)		MICS の OID（APGridPMA から MICS 準拠の承認を得た場合追加する。）

名称		クリティカルフラグ	設定値又は設定内容
	basicConstraints	T	
	cA		FALSE
	cRLDistributionPoints	F	http://www.hpci.nii.ac.jp/ca/hpcica.crl

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	－	sha1WithRSAEncryption （OID=1 2 840 113549 1 1 11）
validity	－	
notBefore		有効期限は発行年度末＋1ヶ月とする （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 （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 32264 2 2）
(policyIdentifier)		
(certPolicyId)		MICS の OID（APGridPMA から MICS 準拠の承認を得た場合追加する。）
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

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	－	sha1WithRSAEncryption （OID=1 2 840 113549 1 1 11）
validity	－	
notBefore		有効期限は発行年度末＋1ヶ月とする （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 （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 32264 2 2）
(policyIdentifier)		
(certPolicyId)		MICS の OID （APGridPMA から MICS 準拠の承認を得た場合追加する。）
subjectAltName	F	サービス名（サービス名/FQDN）

名称		クリティカルフラグ	設定値又は設定内容
	basicConstraints	T	
	cA		FALSE
	cRLDistributionPoints	F	http://www.hpci.nii.ac.jp/ca/hpcica.crl

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	－	sha1WithRSAEncryption (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
issuingDistributionPoint	F	http://www.hpci.nii.ac.jp/ca/hpcica.crl