付録 A　証明書の属性値

KS Solutions ルート認証局証明書

フィールド名	値
バージョン	V3
シリアル番号	ユニークな値
署名アルゴリズム	sha256RSA
有効期限の開始	2015 年 7 月 14 日 18:33:49
有効期限の終了	2045 年 7 月 14 日 18:56:49
発行者	CN = KSSOLrootCA02 O = KandenSystemSolutionsCoInc C = jp
サブジェクト	CN = KSSOLrootCA02 O = KandenSystemSolutionsCoInc C = jp
公開キー	RSA (2048 Bits)
機関キー識別子	5b 6a 5b ee bc 5b f9 ed f0 5a 5c 9b fd 8c 6e b0 c2 48 9d 75
サブジェクト キー識別子	5b 6a 5b ee bc 5b f9 ed f0 5a 5c 9b fd 8c 6e b0 c2 48 9d 75
CRL 配布ポイント	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://pki3.kanden.ne.jp/crl/KSSOLrootCA02/Latestcrl.crl URL=http://CDPSERVER/crl/KSSOLrootCA02/Latestcrl.crl
キー使用法	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
基本制限	Subject Type=CA Path Length Constraint=1

KS Solutions ユーザ証明書認証局証明書

フィールド名	値
バージョン	V3
シリアル番号	ユニークな値
署名アルゴリズム	sha256RSA
有効期限の開始	2015 年 7 月 21 日 17:03:30
有効期限の終了	2045 年 7 月 14 日 18:56:55
発行者	CN = KSSOLrootCA02 O = KandenSystemSolutionsCoInc C = jp
サブジェクト	CN = KSSOLsubCA0201 O = KandenSystemSolutionsCoInc C = jp
公開キー	RSA (2048 Bits)
Netscape 証明書の種類	SSL CA, SMIME CA (06)
機関キー識別子	KeyID=5b 6a 5b ee bc 5b f9 ed f0 5a 5c 9b fd 8c 6e b0 c2 48 9d 75
サブジェクト キー識別子	89 e4 38 7f c3 08 fa b1 10 b2 0e cd df 08 83 ea f3 82 bf b1
CRL 配布ポイント	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://pki3.kanden.ne.jp/crl/KSSOLrootCA02/Latestcrl.crl URL=http://CDPSERVER/crl/KSSOLrootCA02/Latestcrl.crl URL=ldap://pki3.kanden.ne.jp/OU=KSSOLrootCA02,O=KandenSystemSolutionsCoInc,C=jp?authorityRevocationList URL=ldap://CDPSERVER/OU=KSSOLrootCA02,O=KandenSystemSolutionsCoInc,C=jp?authorityRevocationList
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=file:////svpk66-1/CertEnrollsvpk66-1_KSSOLrootCA02(1).crt
キー使用法	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
基本制限	Subject Type=CA Path Length Constraint=0

・ユーザ証明書

フィールド名	値
バージョン	V3
シリアル番号	ユニークな値
署名アルゴリズム	sha256RSA
有効期限の開始	yyyyMMdd HHmmss
有効期限の終了	2045 年 7 月 14 日 18:56:55
発行者	CN = KSSOLsubCA0201 O = KandenSystemSolutionsCoInc C = jp
サブジェクト	CN = 証明書利用者のユーザ ID OU = 証明書発行回数 O = 利用企業名 C = jp
公開キー	RSA (2048 Bits)
証明書ポリシー	[1]Certificate Policy: Policy Identifier=1.2.392.200174.2.1.1
拡張キー使用法	クライアント認証 (1.3.6.1.5.5.7.3.2) 電子メールの保護 (1.3.6.1.5.5.7.3.4) スマート カード ログオン (1.3.6.1.4.1.311.20.2.2)
Netscape 証明書の種類	SSL クライアント認証, SMIME (a0)
機関キー識別子	中間認証局公開鍵の SHA-2 ハッシュ値
サブジェクト キー識別子	利用者公開鍵の SHA-2 ハッシュ値
CRL 配布ポイント	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://pki3.kanden.ne.jp/crl/KSSOLsubCA0201/Latestcrl.crl URL=http://CDPSERVER/crl/KSSOLsubCA0201/Latestcrl.crl URL=ldap://pki3.kanden.ne.jp/OU=KSSOLsubCA0201,O=KandenSystemSolutionsCoInc,C=jp?authorityRevocationList URL=ldap://CDPSERVER/OU=KSSOLsubCA0201,O=KandenSystemSolutionsCoInc,C=jp?authorityRevocationList
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=file:////svpk68-1/CertEnroll/svpk68-1_KSSOLsubCA0201(5).crt
キー使用法	Digital Signature, Non-Requdiation, Key Encipherment (e0)

KS Solutions サーバ証明書認証局証明書

フィールド名	値
バージョン	V3
シリアル番号	ユニークな値
署名アルゴリズム	sha256RSA
有効期限の開始	2015 年 7 月 21 日 17:04:47
有効期限の終了	2045 年 7 月 14 日 18:56:55
発行者	CN = KSSOLrootCA02 O = KandenSystemSolutionsCoInc C = jp
サブジェクト	CN = KSSOLsubCA0202 O = KandenSystemSolutionsCoInc C = jp
公開キー	RSA (2048 Bits)
Netscape 証明書の種類	SSL CA (04)
機関キー識別子	KeyID=5b 6a 5b ee bc 5b f9 ed f0 5a 5c 9b fd 8c 6e b0 c2 48 9d 75
サブジェクト キー識別子	1e 34 ea 59 01 cc 54 c8 ec a1 c2 d5 19 7d 5a ca c3 73 12 ad
CRL 配布ポイント	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://pki3.kanden.ne.jp/crl/KSSOLrootCA02/Latestcrl.crl URL=http://CDPSERVER/crl/KSSOLrootCA02/Latestcrl.crl URL=ldap://pki3.kanden.ne.jp/OU=KSSOLrootCA02,O=KandenSystemSolutionsCoInc,C=jp?authorityRevocationList URL=ldap://CDPSERVER/OU=KSSOLrootCA02,O=KandenSystemSolutionsCoInc,C=jp?authorityRevocationList
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=file:////svpk66-1/CertEnrollsvpk66-1_KSSOLrootCA02(1).crt
キー使用法	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
基本制限	Subject Type=CA Path Length Constraint=0

サーバ証明書

フィールド名	値
バージョン	V3
シリアル番号	ユニークな値
署名アルゴリズム	sha256RSA
有効期限の開始	yyyyMMdd HHmmss
有効期限の終了	yyyyMMdd HHmmss
発行者	CN = KSSOLsubCA0202 O = KandenSystemSolutionsCoInc C = jp
サブジェクト	CN = 証明書利用者のユーザ ID OU = 証明書発行回数 O = 利用企業名 L = 市区町村 C = jp
公開キー	RSA (2048 Bits)
証明書ポリシー	[1]Certificate Policy: Policy Identifier=1.2.392.200174.2.1.1
拡張キー使用法	クライアント認証 (1.3.6.1.5.5.7.3.2) 電子メールの保護 (1.3.6.1.5.5.7.3.4) スマート カード ログオン (1.3.6.1.4.1.311.20.2.2)
Netscape 証明書の種類	SSL サーバー認証 (40)
機関キー識別子	中間認証局公開鍵の SHA-2 ハッシュ値
サブジェクト キー識別子	利用者公開鍵の SHA-2 ハッシュ値
CRL 配布ポイント	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://pki3.kanden.ne.jp/crl/KSSOLsubCA0202/Latestcrl.crl URL=http://CDPSERVER/crl/KSSOLsubCA0202/Latestcrl.crl URL=ldap://pki3.kanden.ne.jp/OU=KSSOLsubCA0202,O=KandenSystemSolutionsCoInc,C=jp?authorityRevocationList URL=ldap://CDPSERVER/OU=KSSOLsubCA0202,O=KandenSystemSolutionsCoInc,C=jp?authorityRevocationList
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=file:////svpk68-1/CertEnroll/svpk66-1_KSSOLsubCA0202(5).crt

付録 B　CRL の属性値

KS Solutions ユーザ証明書認証局 CRL

フィールド名	値
バージョン	V2
署名アルゴリズム	sha256RSA
有効期限の開始	yyyyMMdd HHmmss
有効期限の終了	yyyyMMdd HHmmss
発行者	CN = KSSOLsubCA0201 O = KandenSystemSolutionsCoInc C = jp
更新日	yyyyMMdd HHmmss
次回更新日	yyyyMMdd HHmmss
機関キー識別子	中間認証局公開鍵の SHA-2 ハッシュ値

KS Solutions サーバ証明書認証局 CRL

フィールド名	値
バージョン	V2
署名アルゴリズム	sha256RSA
有効期限の開始	yyyyMMdd HHmmss
有効期限の終了	yyyyMMdd HHmmss
発行者	CN = KSSOLsubCA0202 O = KandenSystemSolutionsCoInc C = jp
更新日	yyyyMMdd HHmmss
次回更新日	yyyyMMdd HHmmss
機関キー識別子	中間認証局公開鍵の SHA-2 ハッシュ値

付録 C　用語

用語	定義
CPS ［Certification Practice Statement］	認証局が、証明書の発行、管理、失効の際に採用する運用手続を規定した文書。
認証局（CA） ［Certification Authority］	証明書の発行、管理、失効を行う機関。発行局、登録局、リポジトリで構成される。
ルート認証局 ［Root Certification Authority］	信頼の基点となる認証局。自己の秘密鍵で、自己の公開鍵に対して電子署名を行った証明書を発行する機関。また認証局として、他の認証局に対して証明書を発行する。
中間認証局 ［Intermediate Certification Authority］	ルート認証局によって認証され、自己の公開鍵に対して電子署名を行った認証局証明書を発行された機関。認証局として、他者に対して証明書を発行する。
公開鍵証明書 ［Public Key Certificate］	公開鍵に対して電子署名を行った電子データ。
証明書 ［Certificate］	公開鍵証明書と同じ。
発行局（IA） ［Issuing Authority］	認証局の中で、登録局の指示により証明書の発行、失効、管理を行う機関。
登録局（RA） ［Registration Authority］	認証局の中で、利用企業からの証明書発行・失効申請の受け付け、証明書利用者に対する鍵ペアの生成、発行局への証明書発行・失効指示、鍵ペアと証明書のセキュリティデバイスへの格納を行う機関。
リポジトリ ［Repository］	認証局の中で、証明書、失効情報（CRL/ARL）、認証局に関する規定文書、通知等を公開するための機関。
CRL ［Certificate Revocation List］	認証局が発行した利用者の証明書のうち、失効したものに関する情報を掲載したリスト。
利用企業	本認証局との契約により、自己の社員等のための証明書の発行･失効の申請を登録局に対して行う企業。
利用法人規約	利用企業が本サービスを利用する上で、利用企業の義務・責任を記載した文書。
利用企業担当者	利用企業が本サービスを利用する上で、申請等の処理を一手に担当する者。
証明書利用者 ［End Entity、Subscriber］	利用企業の社員等で、本認証局の発行するセキュリティデバイスを保有し、その秘密鍵を利用する者。
依拠当事者 ［Relying Party］	証明書利用者との通信等で証明書を受け取り、その証明書の正当性を確認し、証明書に依拠するもの。

鍵ペア ［Key Pair］	秘密鍵と、それに対応する公開鍵の組。
CSR ［Certificate Signing Request］	サーバ証明書を発行するための署名要求。
セキュリティデバイス	IC チップが埋め込まれたカードあるいはＵＳＢトークン等の電子証明書を格納するためのデバイス。
作業用ＩＣカード	本認証局において、RA 業務用設備を操作する際に利用するＩＣカード。
記録アーカイブ	本認証局がその業務遂行において発生する、書類および電子データの集まり。
秘密鍵 ［Private Key］	当該本人だけが所有し、使用することのできる電子データ。対応する公開鍵と、関連している。電子署名を行ったり、暗号化されたメッセージの復号化を行うことができる。
PIN ［Personal Identification Number］	証明書利用者を識別するために必要な情報のこと。
危殆化 ［Compromise］	秘密鍵が、その正当な所有者以外の第三者によって利用可能になる状態。
識別名（DN） ［Distinguished Name］	証明書中で、証明書発行対象者あるいは証明書の発行者を一意に識別するための名称。
活性化 ［Activation］	秘密鍵が格納されているセキュリティデバイス等の暗号装置が利用可能になること。
FIPS ［Federal Information Processing Standards］	米国の定めた、情報処理に関する基準。FIPS140-1 は、暗号装置に関する基準である。
ITU ［International Telecommunication Union］	国際電気通信連合のこと。ITU-T は、特に電気通信に関連した標準を策定する。
PKCS#12 ［Public Key Cryptography Standers #12］	PKCS は、米国 RSA Security 社が提唱する暗号に関する業界標準規格。PKCS#12 は、秘密鍵と対応する証明書の出力データ形式、および、パスワードを用いた暗号化方式に関する規程。