

## 時刻監査証明書のデータ形式

フィールド	意味	値
Version		
AttCertVersion	時刻監査証明書の、属性証明書としてのバージョン 型:INTEGER	1
Holder		
Holder	時刻監査証明書の所有者	
entityName	時刻監査証明書の所有者名	
directoryName		
countryName	時刻監査証明書所有者の国名	
type	国名のオブジェクト ID 型:OID	2.5.4.6
value	国名の値	時刻監査証明書所有者の公開鍵証明書のサブ ジェクト名に従う
organizationName	時刻監査証明書所有者の組織名	
type	組織名のオブジェクト ID 型:OID	2.5.4.10
value	組織名の値	時刻監査証明書所有者の公開鍵証明書のサブ ジェクト名に従う
organizationalUnitName	時刻監査証明書所有者の部門名	
type	部門名のオブジェクト ID 型:OID	2.5.4.11
value	部門名の値	時刻監査証明書所有者の公開鍵証明書のサブ ジェクト名に従う
commonName	時刻監査証明書所有者の固有名称	
type	固有名称のオブジェクト ID 型:OID	2.5.4.3
value	固有名称の値	時刻監査証明書所有者の公開鍵証明書のサブ ジェクト名に従う
objectDigestInfo	オブジェクトのダイジェスト値の情報	
digestedObjectType	オブジェクトのダイジェスト値の型 型:ENUMERATED	1
digestAlgorithm	オブジェクトのダイジェストに使用されたハッシュアル ゴリズムの識別子	
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID	1.3.14.3.2.26 (SHA1)
parameters	暗号アルゴリズムの引数 型:NULL	なし
objectDigest	オブジェクトのダイジェスト値 型:BIT STRING	公開鍵証明書のハッシュ値
Issuer		
AttCertIssuer	時刻監査証明書の発行者	
v2Form	バージョン2の記述形式	
issuerName	時刻監査証明書の発行者名	

directoryName	時刻監査証明書発行者の国名	
countryName	国名のオブジェクト ID	
type	型:OID	2.5.4.6
value	国名の値	時刻監査証明書発行者の公開鍵証明書のサブ ジェクト名に従う
organizationName	時刻監査証明書発行者の組織名	
type	組織名のオブジェクト ID 型:OID	2.5.4.10
value	組織名の値	時刻監査証明書発行者の公開鍵証明書のサブ ジェクト名に従う
organizationalUnitName	時刻監査証明書発行者の部門名	
type	部門名のオブジェクト ID 型:OID	2.5.4.11
value	部門名の値	時刻監査証明書発行者の公開鍵証明書のサブ ジェクト名に従う
commonName	時刻監査証明書発行者の固有名称	
type	固有名称のオブジェクト ID 型:OID	2.5.4.3
value	固有名称の値	時刻監査証明書発行者の公開鍵証明書のサブ ジェクト名に従う
signature		
AlgorithmIdentifier	時刻監査証明書への署名に使用された暗号アルゴリズムの識別子(公開鍵暗号とハッシュ関数)	
algorithm	暗号アルゴリズムのオブジェクト ID 型:OID	1.2.840.113549.1.1.5 (SHA1withRSA)
parameters	暗号アルゴリズムの引数 型:NULL	なし
serialNumber		
CertificateSerialNumber	時刻監査証明書のシリアル番号 型:INTEGER	ユニークな正の整数
attrCertValidityPeriod		
AttCertValidityPeriod	時刻監査証明書の有効期間	
notBeforeTime	開始日時 型:GeneralizedTime	値:YYYYMMDDHHMMSSZ
notAfterTime	終了日時 型:GeneralizedTime	値:YYYYMMDDHHMMSSZ
attributes		
[attribute: TimingMetrics]	属性情報	
type	型:OID	
value		1.3.6.1.4.1.601.10.4.1
ntpTime	時刻監査が行われた時刻	
major	時刻監査が行われた時刻の整数部 型:INTEGER	時刻監査が行われた時刻の整数部
fractionalSeconds	時刻監査が行われた時刻の小数部 型:INTEGER	時刻監査が行われた時刻の小数部
offset	上位時刻認証サーバとの時刻のずれ(オフセット)	
major	上位時刻認証サーバとの時刻のずれの整数部 型:INTEGER	上位時刻認証サーバとの時刻のずれの整数部

fractionalSeconds	上位時刻認証サーバとの時刻のずれの小数部 型: INTEGER	上位時刻認証サーバとの時刻のずれの小数部
sign	上位時刻認証サーバとの時刻のずれの符号 型: INTEGER OPTIONAL	上位時刻認証サーバとの時刻のずれが負の値の場合: -1 それ以外の場合: 本項目は時刻監査証明書に含まれない
delay	時刻監査時のネットワーク遅延	
major	ネットワーク遅延の整数部 型: INTEGER	ネットワーク遅延の整数部
fractionalSeconds	ネットワーク遅延の小数部 型: INTEGER	ネットワーク遅延の小数部
expiration	時刻監査証明書の有効期間	
major	時刻監査証明書の有効期間の整数部 型: INTEGER	時刻監査証明書の有効期間の整数部
fractionalSeconds	時刻監査証明書の有効期間の小数部 型: INTEGER	時刻監査証明書の有効期間の小数部
leapEvent	うるう秒設定情報(※うるう秒設定時のみ含まれる)	
leapTime	うるう秒設定日時	
major	うるう秒設定日時の整数部 型: INTEGER	うるう秒設定日時の整数部
fractionalSeconds	うるう秒設定日時の小数部 型: INTEGER	うるう秒設定日時の小数部
action	うるう秒の設定方法 型: INTEGER	挿入の場合: 1 削除の場合: -1
attributes		
[attribute: TimingPolicy]	属性情報	
type	型: OID	
value		1.3.6.1.4.1.601.10.4.2
policyID	時刻監査証明書ポリシー 型: OID	時刻監査証明書ポリシーのOIDの値
maxOffset	時刻監査規格(オフセット)	
major	時刻監査規格(オフセット)の整数部 型: INTEGER	時刻監査規格(オフセット)の整数部
fractionalSeconds	時刻監査規格(オフセット)の小数部 型: INTEGER	時刻監査規格(オフセット)の小数部
maxDelay	時刻監査規格(ネットワーク遅延)	
major	時刻監査規格(ネットワーク遅延)の整数部 型: INTEGER	時刻監査規格(ネットワーク遅延)の整数部
fractionalSeconds	時刻監査規格(ネットワーク遅延)の小数部 型: INTEGER	時刻監査規格(ネットワーク遅延)の小数部