項番	施行規則	指針	適合例	必要書類	措置状況	認証業務規程	事務取扱要領等	調査結果／特記事項等
3421	電子証明書には、その発行者を確認するための措置であって第二条の基準に適合するものが講じられていること。（第六条第六号）	規則第二条の基準を満たす電子署名の方式は、次の各号のいずれかとする。 ① ＲＳＡ方式であって、ハッシュ関数としてＳＨＡ－２５６を使用するもの（オブジェクト識別子 １ ２ 840 113549 1 1 11）、ＳＨＡ－３８４を使用するもの（オブジェクト識別子 １ ２ 840 113549 １ １ 12）又はＳＨＡ－５１２を使用するもの（オブジェクト識別子 １ ２ 840 113549 １ １ 13）のうち、モジュラスとなる合成数が2048ビット以上のもの ② ＲＳＡ－ＰＳＳ方式（オブジェクト識別子 １ ２ 840 113549 １ １ 10）であって、ハッシュ関数としてＳＨＡ－２５６（オブジェクト識別子 ２ 16 840 1 101 3 4 2 1）、ＳＨＡ－３８４（オブジェクト識別子 ２ 16 840 1 101 3 4 2 2）又はＳＨＡ－５１２（オブジェクト識別子 ２ 16 840 1 101 3 4 2 3）を使用するもののうち、モジュラスとなる合成数が2048ビット以上のもの ③ ＥＣＤＳＡ方式であって、ハッシュ関数としてＳＨＡ－２５６を使用するもの（オブジェクト識別子 １ ２ 840 10045 4 3 2）、ＳＨＡ－３８４を使用するもの（オブジェクト識別子 １ ２ 840 10045 4 3 3）又はＳＨＡ－５１２を使用するもの（オブジェクト識別子 1 2 840 10045 4 3 4）のうち、楕円曲線の定義体及び位数が224ビット以上のもの ④ ＤＳＡ方式であって、ハッシュ関数としてＳＨＡ－２５６を使用するもの（オブジェクト識別子 ２ 16 840 1 101 3 4 3 2）であり、かつ、モジュラスとなる素数が2048ビット以上のもの （指針第三条）	(1) 以下の(2)の事項に関して、認証業務規程及び事務取扱要領等に明確かつ適切に規定し、実施している。	・認証業務規程 ・事務取扱要領				
3422			(2) 電子証明書の発行に利用する電子署名方式は、以下のいずれかの方式を用いている。 ① RSA方式であって、ハッシュ関数としてSHA-256を使用するもの（オブジェクト識別子 1 2 840 113549 1 1 11）、SHA-384を使用するもの（オブジェクト識別子 1 2 840 113549 1 1 12）又はSHA-512を使用するもの（オブジェクト識別子 1 2 840 113549 1 1 13）のうち、モジュラスとなる合成数が2048ビット以上のもの ② RSA-PSS方式（オブジェクト識別子 1 2 840 113549 1 1 10）であって、ハッシュ関数としてSHA-256（オブジェクト識別子 2 16 840 1 101 3 4 2 1）、SHA-384（オブジェクト識別子 2 16 840 1 101 3 4 2 2）又はSHA-512（オブジェクト識別子 2 16 840 1 101 3 4 2 3）を使用するもののうち、モジュラスとなる合成数が2048ビット以上のもの ③ ECDSA方式であって、ハッシュ関数としてSHA-256を使用するもの（オブジェクト識別子 1 2 840 10045 4 3 2）、SHA-384を使用するもの（オブジェクト識別子 1 2 840 10045 4 3 3）又はSHA-512を使用するもの（オブジェクト識別子 1 2 840 10045 4 3 4）のうち、楕円曲線の定義体及び位数が224ビット以上のもの ④ DSA方式であって、ハッシュ関数としてSHA-256を使用するもの（オブジェクト識別子 2 16 840 1 101 3 4 3 2）であり、かつ、モジュラスとなる素数が2048ビット以上のもの					

		3.5 認定認証業務と他の業務との誤認を防止するための措置						
3511	認証業務に関し、利用者その他の者が認定認証業務と他の業務を誤認することを防止するための適切な措置を講じていること。(第六条第七号)	規則第六条第七号に規定する利用者その他の者が認定認証業務と他の業務を誤認することを防止するための適切な措置には、次の各号に掲げる措置が含まれるものとする。(指針第十条) 発行者署名符号を認定認証業務以外の業務のために使用しないこと。ただし、次に掲げる場合を除く。(指針第十条第一号) イ　他の認定認証業務その他認定認証業務と同程度以上の基準に従って国又は地方公共団体等が実施する認証業務との相互認証の実施のための使用(指針第十条第一号イ) ロ　当該認証業務の維持管理のために必要な場合における使用(指針第十条第一号ロ)	(1) 以下の(2)、(3)の事項に関して、認証業務規程及び事務取扱要領等に明確かつ適切に規定し、実施している。	・認証業務規程 ・事務取扱要領				
3512			(2) 発行者署名符号の用途は認証業務の発行する電子証明書への電子署名のみに使用される。 上記以外に発行者署名符号を使用する場合は、以下の項目内に限定される。 ① 他の認定認証業務その他認定認証業務と同程度以上の基準に従って国又は地方公共団体等が実施する認証業務との相互認証証明書への電子署名 ② 当該認証業務の電子証明書への電子署名(自己署名) ③ 当該発行者署名符号の更新処理のため、新しい当該認証業務の電子証明書への電子署名 ④ 当該発行者署名符号の更新処理のため、古い当該認証業務の電子証明書への電子署名 ⑤ 当該認証業務用設備およびそれを操作する者に対して発行する電子証明書への電子署名 ⑥ 電磁的に記録する失効に関する情報への電子署名 ⑦ 電子証明書失効情報および当該認証業務に関する情報等を開示する設備に対して発行する電子証明書への電子署名					
3513		発行者署名検証符号に係る電子証明書の値をＳＨＡ－２５６、ＳＨＡ－３８４又はＳＨＡ－５１２のうちいずれか一以上で変換した値によって認定認証業務を特定すること。(指針第十条第二号)	(3)当該発行者署名符号に対応した発行者署名検証符号に係る電子証明書の値をSHA-256、SHA-384又はSHA-512のうちいずれか1以上で変換した値(フィンガープリント)を記録し、改ざん防止措置を講じて公開している。	・電子証明書の値をSHA-256、SHA-384又はSHA-512のうちいずれか1以上で変換した値				