事　務　連　絡
令和６年６月 11 日

認定認証事業者　各位

特定認証業務の基準の改正スケジュール等の周知について

デジタル庁　デジタル社会共通機能グループ　参事官（トラスト担当）
法務省　民事局商事課

平素からデジタル行政にご理解とご協力を賜り、厚く御礼申し上げます。

先般、デジタル庁・総務省・経済産業省において「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」を策定したところですが、電子署名及び認証業務に関する法律施行規則（平成 13 年総務省・法務省・経済産業省令第２号）第２条及び電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成 13 年４月 27 日総務省・法務省・経済産業省告示第２号）第３条に規定する特定認証業務の基準につきまして、別添の通り「電子署名法特定認証業務の基準における暗号移行方針」を策定しましたので、電子署名法第 33 条の規定に基づき情報提供します。認定認証事業者各位におかれましては、本方針を踏まえ、円滑な暗号移行へのご協力をお願いいたします。

【問合せ先】
デジタル庁　デジタル社会共通機能グループ
電子署名法担当
電話：03-6891-2720
e-mail：digitaltrust@digital.go.jp

法務省　民事局商事課
電子認証係
電話：03-3580-4111（内線：2375）
e-mail：denshi-ninsho@i.moj.go.jp

（別添）

令和６年６月 11 日

電子署名法特定認証業務の基準における暗号移行方針

デジタル庁　デジタル社会共通機能グループ　参事官（トラスト担当）
法務省　民事局商事課

１．特定認証業務の基準の改正スケジュール及び改正内容

電子署名及び認証業務に関する法律施行規則（平成 13 年総務省・法務省・経済産業省令第２号）第２条及び電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成 13 年４月 27 日総務省・法務省・経済産業省告示第２号）第３条に規定する特定認証業務の暗号アルゴリズム及び暗号強度に係る基準については、令和 15 年（2033 年）末を目途に改正する。

現行は 112 ビットセキュリティ強度以上を規定しているが、改正後は 128 ビットセキュリティ強度[1]以上を規定することを想定している。

これは、認定認証業務が発行する電子証明書の有効期限、認定認証事業者の事業の安定性及び利用者への影響、認定認証業務であることを民間認証局の相互認証基準の条件の一つとしている GPKI ブリッジ認証局の暗号移行対応スケジュール等を踏まえ、使用する暗号技術の解法アルゴリズムに係る進展、量子コンピュータの性能向上等の急速な危殆化等特別の事情が認められない場合に限り、令和 15 年末（2033 年末）まで現行の暗号強度を特定認証業務に利用することを許容するものである。

したがって、現行の暗号技術が急速に危殆化するおそれが生じた場合等、暗号技術の動向等を踏まえ、必要に応じて上記スケジュール及び改正内容を見直すことがある。

２．暗号移行に係る留意点

認定認証業務の暗号移行の対応にあたっては、以下の点に留意することとする。

＜暗号危殆化時の対応＞

112 ビットセキュリティの安全性指標を持つ暗号技術が急速に危殆化するおそれが生じた場合には、これらを利用した電子証明書については、CRYPTREC による注意喚起や主務省庁からの情報提供等を踏まえ、電子証明書の失効の請求や有効期限の短い電子証明書の発行等の対応を行い、電子署名に対する信頼性の低下を最小限とするように努めること。

---

[1] 112 ビットセキュリティ強度を持つ暗号技術の例としては、2048 ビットの RSA 暗号及び 224 ビットの楕円曲線暗号（P-224）、128 ビットセキュリティ強度を持つ暗号技術の例としては、3072 ビットの RSA 暗号及び 256 ビットの楕円曲線暗号（P-256）が挙げられる。

＜利用者への周知＞

電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成 13 年４月 27 日総務省・法務省・経済産業省告示第２号）第８条に定める利用申込者に対する説明に関する規定の通り、暗号危殆化時の取扱いについて利用申込者に説明を行うこと。

特に、令和 13 年（2031 年）以降に有効期限を迎える電子証明書の利用申込者に対しては、電子証明書の失効の請求や有効期限の短い電子証明書の発行等の取扱いが発生する可能性を説明に含める等、その時点における暗号危殆化の状況を踏まえ、利用申込者への説明をより一層明確な形とすること。

＜新暗号への対応開始時期＞

GPKI ブリッジ認証局との相互認証を行う認定認証業務については、GPKI ブリッジ認証局の新暗号対応予定時期である、令和 10 年（2028 年）中を目途に新暗号に対応した認証局の運用を開始すること。

＜移行先の暗号アルゴリズム及び暗号強度＞

移行先の暗号技術の強度については、128 ビットセキュリティ以上の安全性指標を持つ暗号技術を利用すること。

なお、認定認証事業者であることを民間認証局の相互認証基準の一つ[2]としている GPKI ブリッジ認証局においては、現時点において次の暗号アルゴリズム及び鍵長に対応予定である。[3]

・ECDSAWithSHA384（1.2.840.10045.4.3.3）

※ECDSA の曲線は鍵長が 384 ビットである NIST P-384（secp384r1、OID：1.3.132.0.34）とする。

＜暗号移行に係る調整について＞

GPKI ブリッジ認証局の暗号移行時期の周辺においては、多数の認証局の暗号移行対応時期が重なると考えられる。そのため、認定に係る調査のスケジュールについては、主務省庁及び指定調査機関による調整に協力すること。

また、GPKI ブリッジ認証局についても、相互認証を実施している認定認証業務以外の認証局を含め、暗号移行対応の時期が重なるため、円滑な相互認証の実施のため、相互認証の審査に係るスケジュールについてデジタル庁による調整に協力すること。

---

[2] 政府認証基盤におけるブリッジ認証局の相互認証基準について（平成 13 年 4 月 25 日行政情報化推進各省庁連絡会議幹事会了承。最終改定令和 3 年 12 月 9 日デジタル社会推進会議関係課長等連絡会議了承。）

https://www.gpki.go.jp/cross/cross.pdf

[3] 仕様の詳細等については、令和６年８月に公表予定である次期システムに係る相互運用性仕様書を参考にされたい。

加えて、電子証明書の暗号移行においては、認定認証業務のみならず、認定認証業務の電子証明書を受け入れている電子申請システム等署名検証側における対応も同時に行う必要があるため、関係システムを運営している行政機関及び民間組織との調整及び相互運用性の確保に努めること。

＜参考１＞電子署名法施行規則（抄）
第２条　法第２条第３項の主務省令で定める基準は、電子署名の安全性が次のいずれかの有する困難性に基づくものであることとする。
一　ほぼ同じ大きさの二つの素数の積である 2048 ビット以上の整数の素因数分解
二　大きさ 2048 ビット以上の有限体の乗法群における離散対数の計算
三　楕円曲線上の点がなす大きさ 224 ビット以上の群における離散対数の計算
四　前三号に掲げるものに相当する困難性を有するものとして主務大臣が認めるもの

＜参考２＞特定認証業務の認定に係る指針（抄）
第３条　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。
一　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 11 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
二　RSA-PSS 方式（オブジェクト識別子 1 2 840 113549 1 1 10）であって、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
三　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
四　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

＜参考３＞CRYPTREC 暗号リスト（電子政府推奨暗号リスト）（抜粋）
https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf

暗号技術検討会[4]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[5]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

なお、利用する鍵長について、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[6]の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

[4] デジタル庁統括官、総務省サイバーセキュリティ統括官及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、デジタル庁、総務省及び経済産業省における施策の検討に資することを目的として開催。

[5] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

[6] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html

＜参考４＞暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準（抜粋）
https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022.pdf

2.2.1　公開鍵暗号の推定セキュリティ強度

表２　公開鍵暗号の推定セキュリティ強度[7]

セキュリティ強度（ビットセキュリティ）	IFC RSA-PSS RSASSA-PKCS1-v1.5 RSA-OAEP RSAES-PKCS1-v1_5	FFC DSA DH	ECC ECDSA ECDH PSEC-KEM
112	k = 2048	(L, N) = (2048, 224)	P-224 B-233 K-233
128	k = 3072	(L, N) = (3072, 256)	P-256 B-283 K-283 W-25519 Curve25519 Edwards25519
192	k = 7680	(L, N) = (7680, 384)	P-384 B-409 K-409 W-448 Curve448 Edwards448
256	k = 15360	(L, N) = (15360, 512)	P-521 B-571 K-571

[7] P: curve over Prime fields（素体曲線）、B: curve over Binary fields（拡大体（バイナリ）曲線）、K: Koblitz-curve（コブリッツ曲線）、W: Weierstrass-curve（ワイエルシュトラス曲線）、Curve: Montgomery-curve（モンゴメリ曲線）、Edwards: Edwards-curve（エドワード曲線）

3.2　セキュリティ強度要件の基本設定方針

表 5　セキュリティ強度要件の基本設定方針

<table>
<tr><th colspan="2">想定運用終了・廃棄年／
利用期間</th><th>2022～2030</th><th>2031～2040</th><th>2041～2050</th><th>2051～2060</th><th>2061～2070</th></tr>
<tr><td rowspan="2">112 ビット
セキュリティ</td><td>新規生成
((a)参照)</td><td rowspan="2">移行完遂
期間
((c)参照)</td><td>利用不可</td><td rowspan="2">利用不可</td><td rowspan="2">利用不可</td><td rowspan="2">利用不可</td></tr>
<tr><td>処理
((b)参照)</td><td>許容</td></tr>
<tr><td rowspan="2">128 ビット
セキュリティ</td><td>新規生成
((a)参照)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">移行完遂
期間
((c)参照)</td><td>利用不可</td><td rowspan="2">利用不可</td></tr>
<tr><td>処理
((b)参照)</td><td>許容</td></tr>
<tr><td rowspan="2">192 ビット
セキュリティ</td><td>新規生成
((a)参照)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td></tr>
<tr><td>処理
((b)参照)</td></tr>
<tr><td rowspan="2">256 ビット
セキュリティ</td><td>新規生成
((a)参照)</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td><td rowspan="2">利用可</td></tr>
<tr><td>処理
((b)参照)</td></tr>
</table>

(a)　　新規に暗号保護を適用する（例えば、暗号化や署名生成を実行する）際は、原則として、2040 年までは 128 ビット以上のセキュリティ強度のものを選択すべきである。2041 年以降は 192 ビット以上のセキュリティ強度のものを選択すべきである。

(b)　　保護済みのデータに対して処理を実行する（例えば、復号や署名検証を実行する）際は、2040 年までは 128 ビット以上、2041 年以降は 192 ビット以上のセキュリティ強度のものを選択すべきである。ただし、保護済みのデータに対する正当性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合に、2031 年以降も 2040 年までの必要な範囲内で 112 ビットセキュリティ強度のものを選択することを許容する。同様に、2051 年以降も 2060 年までの必要な範囲内で 128 ビットセキュリティ強度のものを選択することを許容する。

(c)　　移行完遂期間内に、よりセキュリティ強度の高い暗号技術又は鍵長への移行を完遂させることを前提として、利用する暗号処理が短期間で完結する場合（例：エンティティ認証）、又は既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持などの必要がある場合には、2030 年までは 112 ビットセキュリティ強度のものを、2050 年までは 128 ビットセキュリティ強度のものを選択することを許容する。

（別添）

＜参考５＞GPKI ブリッジ認証局の暗号移行予定（令和６年３月時点）