

カード代替電磁的記録用 CWT Signer 運用規程

第 1.0 版
2026 年 10 月 20 日

地方公共団体情報システム機構
デジタル庁

発行/改訂履歴

版数	改訂履歴	改訂箇所
1.0	初版	

カード代替電磁的記録用 CWT Signer.....	0
運用規程	0
1 はじめに.....	4
1.1 概要.....	4
1.2 文書名と識別	4
1.3 関係者	4
1.4 カード代替電磁的記録の MRL としての CWT 利用用途.....	5
1.5 ポリシー運用管理.....	6
1.6 定義と略語.....	6
2 公開と公開手法の責任.....	9
2.1 公開手法	9
2.2 カード代替電磁的記録に関する情報の公開	9
2.3 公開の時期又はその頻度.....	9
2.4 アクセス管理	9
3 識別と認証	10
3.1 名称決定	10
3.2 カード代替電磁的記録の MRL の識別と認証.....	10
3.3 鍵更新時の識別と認証	11
3.4 失効申請時の識別と認証.....	11
4 . MRL に関する運用上の要件.....	12
4.1 MRL のライフサイクル	12
4.2 MRL の発行.....	12
4.3 MRL の公開.....	12
4.4 MRL の真正性の確認	12
5 実装面、管理面、運用面のセキュリティ管理.....	13
5.1 実装面のセキュリティ管理	13
5.2 手続面のセキュリティ管理	14
5.3 認証局における人事管理面のセキュリティ管理	16
5.4 監査ログの手続	17
5.5 記録の保管（アーカイブ）	18
5.6 認証局の鍵の更新.....	19
5.7 鍵の危殆化と災害復旧	19
5.8 CWT Signer の運営の終了	20
6 技術面のセキュリティ管理.....	21
6.1 鍵ペアの生成とインストール	21
6.2 秘密鍵の保護と暗号モジュールの技術管理	21
6.3 鍵ペア生成管理に関する他の局面	22
6.4 活性化データ	23
6.5 コンピュータセキュリティ管理.....	23

6.6 ライフサイクルセキュリティ管理	23
6.7 ネットワークセキュリティ管理	23
6.8 タイムスタンプ	24
7 電子証明書のプロファイル	25
7.1 電子証明書のプロファイル	25
8 MRL のプロファイル	26
8.1 MRL のプロファイル	26
8.2 CWT 形式の失効情報のプロファイル	26
9 準拠性監査	27
9.1 監査人	27
9.2 監査の頻度	27
9.3 監査人の要件	27
9.4 監査人と被監査組織の関係	27
9.5 監査項目	27
9.6 監査指摘事項への対応	27
9.7 監査結果の取扱い	27
10 他の業務上及び法的事項	28
10.1 手数料	28
10.2 財務上の責任	28
10.3 事業情報の秘匿性	28
10.4 個人情報の保護	28
10.5 知的財産権	29
10.6 表明保証	29
10.7 保証の免責事項	30
10.8 責任の制限	30
10.9 補償	30
10.10 有効期間と終了	30
10.11 関係者との個別通知と伝達	30
10.12 改訂	31
10.13 紛争解決手順	31
10.14 準拠法	31
10.15 適用可能な法への準拠性	31
10.16 雑則	31
10.17 他の条項	31

1 はじめに

本運用規程は、「行政手続における特定の個人を識別するための番号の利用等に関する法律」（以下「法」という。）で定める「カード代替電磁的記録」によって、移動端末設備及び確認用プログラムの連携により法上の本人確認等を可能にするため、移動端末設備上に個人番号カードの情報を格納し、発行・管理するシステムのうち、カード代替電磁的記録の MSO Revocation List（以下「MRL」という。）に電子署名を付与するエンティティ（以下「カード代替電磁的記録用 CWT Signer」という。）について、そのセキュリティと運用の実務を記述する証明書ポリシー（CP）及び認証実務規定（CPS）である。

住民と国又は地方公共団体の機関等との間の申請・届出等手続時の本人確認の電子化並びに民間企業のサービスへの活用に資することを目的として、法に基づき、地方公共団体情報システム機構（以下「機構」という。）は発行主体として、カード代替電磁的記録を発行する役割を担う。

本運用規程は、このカード代替電磁的記録用 CWT Signer におけるカード代替電磁的記録の MRL の発行、管理、並びにカード代替電磁的記録利用者と検証者によって充足されるべき要件と責任について説明する。

なお、本運用規程の構成は、IETF（Internet Engineering Task Force）の PKIX（Public-Key Infrastructure X.509）Working Group による RFC（Request For Comments）3647 「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。ただし、他の規程を参照する部分は見出しだけを残し参照内容を明示することとする。

1.1 概要

本運用規程は、その実務と管理がどのように実施されるか、以下の標準を基に示す。

- ・ RFC 3647 -Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework 【RFC3647】
- ・ RFC 5280 - Internet X.509 PKI - Certificate and CRL Profile 【RFC5280】
- ・ ISO/IEC 18013-5（第2版、2026年内に発行見込み）- Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence（mDL） application 【ISO/IEC 18013-5】
- ・ IETF RFC8392 CBOR Web Token（CWT） 【RFC8392】

カード代替電磁的記録用 CWT Signer は、CP 及び CPS をそれぞれ独立したものとして、本運用規程をカード代替電磁的記録用 CWT Signer の運営方針として位置付ける。

本運用規程では、運用に関するセキュリティポリシーを規定し、運用の詳細は、運用手順書等に規定する。

1.2 文書名と識別

本運用規程は、カード代替電磁的記録用 CWT Signer 運用規程である。

1.3 関係者

1.3.1 カード代替電磁的記録用 CWT Signer

CWT Signer は、カード代替電磁的記録における Mobile Security Object（以下「MSO」という。）の失効情報を MSO ステータストークンとして格納する CBOR Web Token（以下「CWT」という。）に対して、電子署名を付与するエンティティを指し、X.509 における下位認証局相当の機能を持つ。CWT への電子署名時に、ルート認証局が発行する CWT Signer の電子証明書（以下「CWT 電子証明書」と

いう。)は、検証者が Digital Trust Service (以下「DTS」という。)から CWT をダウンロードする際に CWT の protected header に格納されているため同時にダウンロードされる。

1.3.2 DTS

検証者に対して、カード代替電磁的記録の IACA における Root 証明書、Root 認証局の CRL 及び MRL、CWT 電子証明書等の情報を検証者に公開するためのサービス。

1.3.3 登録局

登録局 (RA) は、カード代替電磁的記録・失効時の登録機関として機能する。また MRL への登録確認後、MRL への署名要求をカード代替電磁的記録用 CWT Signer に対して行う。

1.3.4 カード代替電磁的記録利用者

カード代替電磁的記録利用者とは、法第 18 条の 2 第 6 項の規定により、カード代替電磁的記録の発行を受けた者をいう。カード代替電磁的記録利用者は、カード代替電磁的記録を利用する。

1.3.5 検証者

検証者とは、法第 18 条の 2 第 7 項の規定により、カード代替電磁的記録の送信を受け、確認用プログラムを利用して、カード代替電磁的記録利用者が行った電子署名を検証し、当該カード代替電磁的記録が当該送信を行った者のものであること、また DTS へ当該カード代替電磁的記録の失効情報を確認して失効していないことを確認し、開示されたデータの真正性を確認する者をいう。

検証者は、DTS から当該の CWT をダウンロードして、MSO が失効していないことを検証する。

1.3.6 その他の関係者

1.3.6.1 カード代替電磁的記録用 CWT Signer の運営に関する意思決定機関

カード代替電磁的記録用 CWT Signer の運営に関する意思決定は機構及びデジタル庁が行い、法第 18 条の 2 第 13 項より、カード代替電磁的記録発行及び運用に関する状況の管理の事務は機構が行う。

これには、機構及びデジタル庁の認証局管理責任者と、カード代替電磁的記録用 CWT Signer の運用管理及びセキュリティ運用を担当するスタッフが含まれる。

1.3.6.2 操作要員

カード代替電磁的記録用 CWT Signer の運用を実施する操作者のこと

1.3.6.3. 監査人

カード代替電磁的記録用 CWT Signer の運用を監査する人のこと

1.4 カード代替電磁的記録の MRL としての CWT 利用用途

1.4.1 適切なカード代替電磁的記録の CWT の利用用途

カード代替電磁的記録用 CWT Signer の署名する対象の種類及び用途は、次のとおり。

- ・ 対象の種類：失効したカード代替電磁的記録の MSO に格納されている Device Key 公開鍵の先頭 4 文字(Hex)が同じである MSO 失効 ID(デバイス鍵識別子)が格納された CWT
- ・ 用途：本人確認等実現時にカード代替電磁的記録が失効していないことを確認する手段の提供

1.4.2 禁止されるカード代替電磁的記録の CWT 利用用途

法で制限されている用途や、「1.4.1 適切なカード代替電磁的記録の CWT の利用用途」以外の目的に利用してはならない。

1.5 ポリシー運用管理

1.5.1 文書を管理する組織

本運用規程の責任者は、機構及びデジタル庁とする。

1.5.2 連絡先

本運用規程に関する照会は、機構を窓口とする。

窓口の連絡先は、以下の URL に掲示する。

URL : <https://www.j-lis.go.jp/pn/mdociaca.html>

1.5.3 運用規程承認手続

カード代替電磁的記録用 CWT Signer 運用規程は、機構及びデジタル庁の決定をもって有効なものとする。

1.6 定義と略語

単語、略語、頭字語	意味
CA (Certification Authority : 認証局)	電子証明書の発行・更新・失効、MSO への署名・更新・失効、認証局等秘密鍵の生成・保護を行う機関。
CC (Common Criteria)	ISO/IEC15408 で定める情報セキュリティのための国際評価規格を指す。
CP (Certificate Policy : 証明書ポリシー)	認証局が各電子証明書を発行する際及び MSO へ署名する際の運用方針を定めた文書。
CPS (Certification Practices Statement : 認証実施規程)	認証実施規程。認証局の信頼性、安全性を対外的に示すために、認証局の運用、証明書ポリシー、鍵の生成、管理、責任等に関して定めた文書。CP が何を運用方針にするかを示すのに対して、CPS は運用方針をどのように適用させるかを示す。
CWT (CBOR Web Token)	CBOR Web Token の略。JSON Web Token(JWT) の CBOR ベースのバージョン。認証情報やクレームをバイナリ形式で表現している。CWT は、RFC 8392 で規定されているデータ構造を指す。
CWT Signer 証明書	RootCA で証明された MRL への署名用の電子証明書。電子証明書に格納されている公開鍵は、CWT の署名検証に利用される。
ECDSA (Elliptic Curve Digital Signature Algorithm)	「楕円曲線暗号方式」参照。

FIPS140-3	NIST（National Institute of Standards and Technology：米国標準技術研究所）が策定した米国連邦情報処理標準のうち、暗号技術に関するセキュリティ要件を規定しているもの。 コンピュータと通信システムの暗号モジュールに対して暗号技術に関する汎用要件を網羅しており、最低レベル 1 から最高レベル 4 までのセキュリティレベルが設定されている。
HSM（Hardware Security Module）	不正アクセスに備えるための機能（耐タンパ機能）を保有した秘密鍵の管理装置。耐タンパ機能とは、不正アクセスに対してその侵入の痕跡を残したり、データを消去する機能であり、不正アクセスの証拠を残す不正検知機能、不正アクセスからデータを防護する不正防護機能、不正アクセスに対してデータを消去する対抗動作を行う不正対抗機能等がある。
MRL（MSO Revocation List）	IACA システム内にて構築・稼働する MSO 失効登録・公開機能。 利用者操作、カードの失効等のイベントにより失効要求を受け MSO 失効登録を行い、失効済み MSO 情報を MSO ステータストークンとして CWT 形式で検証者向けに公開する。
MSO（Mobile Security Object）	カード代替電磁的記録内で各データ項目の情報のハッシュ値を配列として格納する Mobile Security Object をいう。カード代替電磁的記録に存在する各データ要素のメッセージダイジェストを計算し、全てのダイジェスト及びカード代替電磁的記録利用者の Device Key 公開鍵を MSO に含める。カード代替電磁的記録用 Document Signer は、カード代替電磁的記録用 Document Signer の秘密鍵を使用して MSO に電子署名する。
RA（Registration Authority：登録局）	次の機能の 1 つ又は複数を担うエンティティ：カード代替電磁的記録申請者の識別と認証、カード代替電磁的記録申請の承認又は拒否、特定の状況下でのカード代替電磁的記録の失効の申立、カード代替電磁的記録の失効を求めるカード代替電磁的記録利用者の要求処理、鍵更新を伴うカード代替電磁的記録の更新を求めるカード代替電磁的記録利用者の要求の承認又は拒否。ただし、RA はカード代替電磁的記録への署名や電子証明書の発行は行わない（すなわち、RA は認証局の代わりに特定のタスクを委任される）。
移動端末設備	電気通信事業法（昭和五十九年法律第八十六号）第 12 条の 2 第 4 項第 2 号ロに規定する移動端末設備。

鍵ペア	公開鍵暗号方式における公開鍵と秘密鍵のペア。一方の鍵から他方の鍵を導き出せない性質を持つため、一方（秘密鍵）を秘密にすることで、他方（公開鍵）を公開することができる。
確認用プログラム	法第 18 条の 4 第 1 号から第 3 号に規定する機能を有するプログラムをいう。
カード代替電磁的記録用 CWT Signer	CWT 形式の MSO ステータストークンに対して、電子署名を付与するエンティティを指し、X.509 における下位認証局相当の機能を持つ。
ガバメントクラウド	政府共通のクラウドサービスの利用環境。国の全ての行政機関や地方公共団体が共同で行政システムをクラウドサービスとして利用できるようにした IT 基盤。
キーセレモニー	認証局の鍵ペアを生成するために実行される一連の手続のこと。
危殆化	信頼性が喪失された可能性のある事態の発生をいう。認証局の場合、認証局の秘密鍵が危殆化することによって、発行した全ての電子証明書及び署名した全ての MSO の信頼性が失われる。
公開鍵	公開鍵暗号方式において用いられる鍵ペアの一方。秘密鍵に対応する、公開されている鍵。
個人番号カード	氏名、住所、生年月日、性別、個人番号、その者の写真その他その者を識別する事項のうち政令で定める事項が記載されたカード。 公的個人認証サービスが発行する署名用電子証明書と利用者証明用電子証明書が格納される。
自己署名電子証明書	自認証局の公開鍵に対して、自認証局の秘密鍵で署名した電子証明書。
楕円曲線暗号方式	楕円曲線上で定義された加減演算を使用して計算を行う暗号方式。パラメータを変えることにより、強度を保つ必要がある。
プロファイル	カード代替電磁的記録に含まれるデータの内容を定義したもの。【ISO/IEC18013-5】にて準拠すべきカード代替電磁的記録のプロファイルが定義されている。
リンク証明書	認証局の鍵更新に伴い同時に存在することとなる新しい認証局の鍵ペアと古い認証局の鍵ペアの関係を保証するための電子証明書。

2 公開と公開手法の責任

2.1 公開手法

カード代替電磁的記録用 CWT Signer で署名を行った MRL は、DTS で公開する。

2.2 カード代替電磁的記録に関する情報の公開

カード代替電磁的記録用 CWT Signer は、機構の Web 上で次の情報を公開する。

- ・ 本運用規程
- ・ MRL を公開するための DTS の URL
- ・ カード代替電磁的記録用 CWT Signer の秘密鍵の危殆化に係る情報等

なお、失効事由の詳細は公表しない。また、カード代替電磁的記録の失効情報である MRL としての CWT は検証者等に DTS 上で公開して提供する。

2.3 公開の時期又はその頻度

公開する情報の更新頻度は次のとおりとする。

- ・ 法、関係法令、本運用規程等は最新版を機構の Web 上に掲載する。

2.4 アクセス管理

機構の Web 上で公表する情報については、特段のアクセス制御は行わない。

3 識別と認証

3.1 名称決定

3.1.1 名称の種類

カード代替電磁的記録用 CWT Signer が署名する CWT は、【ISO/IEC 18013-5】及び【RFC8392】の形式に従って設定する。

3.1.2 名称の意味に関する要件

規定しない。

3.1.3 カード代替電磁的記録利用者の匿名性又は仮名性

カード代替電磁的記録利用者の匿名、仮名を利用することはできない。

3.1.4 名称形式を解釈するための規則

カード代替電磁的記録の MRL 及び CWT は、【ISO/IEC 18013-5】及び【RFC8392】の規定に従い処理する。

3.1.5 名称の一意性

規定しない。

3.1.6 商標の認識・認証・役割

規定しない。

3.2 カード代替電磁的記録の MRL の識別と認証

3.2.1 MRL の真正性を証明する方法

MSO に格納されている Device Key 公開鍵の先頭 4 文字(Hex)が同じである MSO 失効 ID(デバイス鍵識別子)をまとめて 1 つの CWT として、MSO 内にリファレンス先の URL を格納する。CWT が CWT Signer によって正しく電子署名されていることを「3.2.3 CWT の認証」に準じて確認する。

3.2.2 組織の認証

規定しない。

3.2.3 CWT の認証

検証者は、CWT 証明書に記録された公開鍵を用いて CWT の電子署名で真正性の確認を行うと同時に payload に記述されたクレームについても検証する。

3.2.4 検証されない CWT の情報

規定しない。

3.2.5 権限の正当性確認

権限の正当性確認は、「3.2.3 CWT の認証」に準じる。

3.2.6 相互運用の基準

規定しない。

3.3 鍵更新時の識別と認証

3.3.1 通常の鍵更新時の識別と認証

① 通常の更新業務の場合

「3.2.3 CWT の認証」に準じる。

② カード代替電磁的記録自動更新業務の場合

規定しない。

3.3.2 カード代替電磁的記録失効後の鍵更新時の識別と認証

「3.2.3 CWT の認証」に準じる。

3.4 失効申請時の識別と認証

3.4.1 サービスの利用をやめるための失効申請

カード代替電磁的記録利用者は、スマートフォンアプリケーションのマイナポータルアプリからカード代替電磁的記録の失効申請を行う。カード代替電磁的記録利用者の実在性確認は、失効申請のカード代替電磁的記録利用者による署名を検証することで行う。

カード代替電磁的記録の失効申請が行われた場合、当該のスマートフォン上に保持されている有効なすべてのカード代替電磁的記録の MSO は、MRL に登録される。

3.4.2 カード代替電磁的記録利用者の移動端末設備紛失時の届出

カード代替電磁的記録利用者は、電話で移動端末設備を紛失した旨の届出を行う。カード代替電磁的記録利用者の実在性確認は、基本 4 情報を使用して行う。

3.4.3 カード代替電磁的記録利用者の移動端末設備紛失時のカード代替電磁的記録の失効

移動端末設備紛失時に届出があった場合には、カード代替電磁的記録を失効する。紛失した旨の届出が行われた場合、当該のカード代替電磁的記録の MSO は MRL に登録される。

3.4.4 一時停止の届出

カード代替電磁的記録利用者より一時利用停止の届出があった場合には、カード代替電磁的記録の利用を一時停止する。一時利用停止の届出が行われた場合、当該のカード代替電磁的記録の MSO は、MRL に登録される。

4. MRL に関する運用上の要件

4.1 MRL のライフサイクル

4.1.1 RA から MRL に対する当該 MSO の登録

MRL へ登録できる事象は以下のとおりである。

- ・ カード代替電磁的記録利用者から端末の紛失による一時停止、または停止の申請があった場合
- ・ Device Key 秘密鍵が漏洩し、滅失し、若しくは毀損した失効事由で MSO 失効の申請があった場合
- ・ 個人番号カードや個人番号カード用署名用電子証明書が失効した場合

4.1.2 MRL の当該 MSO が有効な期間

MRL の MSO 失効情報は、当該の MSO が MRL に登録されてから MSO の有効期限切れまでが有効な期間である。

4.1.3 MRL の削除

MRL に載っている失効したカード代替電磁的記録の MSO の有効期間が切れた場合、MRL から当該の MSO のデバイス公開鍵の識別子（SHA256 ハッシュ値）を MRL から削除する。

また、カード代替電磁的記録利用者から端末の紛失による一時停止からの解除の申請があった場合も MRL から当該の MSO のデバイス公開鍵の識別子（SHA256 ハッシュ値）を MRL から削除する。。

4.1.4 失効記録発行頻度

CWT 形式の MSO ステータストークンは、24 時間毎に発行する。

4.2 MRL の発行

4.2.1 MRL 発行手続き

MRL は、24 時間毎に MSO が失効している状態を確認して発行処理を行う。

4.2.2 MRL の形式

MRL は、8. MRL のプロファイルに従って発行する。

4.3 MRL の公開

4.3.1. MRL の公開場所

MRL は、カード代替電磁的記録の DTS により公開する。

4.4 MRL の真正性の確認

4.4.1. MRL の電子署名

MRL は、CWT Signer により電子署名される。

4.4.2. MRL の署名検証

MRL は、CWT Signer の公開鍵により署名検証することで真正性を確認することができる。

5 実装面、管理面、運用面のセキュリティ管理

5.1 実装面のセキュリティ管理

5.1.1 立地場所及び構造

カード代替電磁的記録用 CWT Signer は、水害、地震、火災その他の災害や不正侵入を考慮した立地及び構造とする。

5.1.2 物理的アクセス

カード代替電磁的記録用 CWT Signer の施設内の各室内において行われる業務の重要度に応じ、複数のセキュリティレベルで入退室管理を行う。入退室管理の認証は、操作権限者が識別できる IC カード及び生体認証装置により行う。全ての要員は、目に見える位置に身分証明書を着用し、着用していない者に注意することが奨励される。

各室への入退室権限は、本運用規程「5.2. 手続面のセキュリティ管理」において定める各要員の業務に応じて、「5.2.1.1 認証局管理責任者」で規定する認証局管理責任者が付与する。

当該施設には、監視員を配置し、監視システムにより 24 時間 365 日監視を行う。

またカード代替電磁的記録用 CWT Signer の運用施設を収容する建物の外部ドアを保護するため、侵入検知システムが設置し、定期的に試験する。

カード代替電磁的記録の発行・失効はシステムで実施されるため、操作者の認証については定めない。

5.1.3 電源、電力、通信及び空調

カード代替電磁的記録用 CWT Signer は、機器等の運用のために十分な容量の電源を確保するとともに、瞬断、停電、電圧・周波数の変動に備えた対策を講じる。商用電源が供給されない事態においては、一定時間内に発電機による電源供給に切り替える。

また施設内の電力及び通信設備において、データを伝送又はカード代替電磁的記録用 CWT Signer が提供するサービスに使用するケーブルは、傍受や損害から保護する。

空調設備を設置することにより、機器類の動作環境及び要員の作業環境を適切に維持する。

5.1.4 水害対策

カード代替電磁的記録用 CWT Signer を設置する建物、室、天井、床には防水対策を講じる。

5.1.5 地震対策

カード代替電磁的記録用 CWT Signer を設置する建物は制震構造とし、機器・什物の転倒及び落下を防止する対策を講じる。

5.1.6 火災防止及び火災保護対策

カード代替電磁的記録用 CWT Signer を設置する建物は耐火構造、室は防火区画とし、消火設備を備える。

5.1.7 媒体保管場所

保管情報、バックアップデータを含む媒体は、適切な入退室管理が行われている室内に設置された施設可能な場所に保管するとともに、所定の手続に基づき適切に搬入出管理を行う。本運用規程「5.5.1 アーカイブ記録の種類」に関わる書類は、適切な場所に保管する。

5.1.8 廃棄物処理

秘密扱いとする情報を含む書類・記憶媒体及び端末等については、所定の手続により適切に廃棄処理

を行う。

5.1.9 オフサイトバックアップ

規定しない。

5.1.10 電磁波対策

カード代替電磁的記録用 CWT Signer の施設内の各室内において行われる業務の重要度に応じて、電磁波攻撃及び電磁波からの情報漏えいを防ぐ設備を備える。

5.2 手順面のセキュリティ管理

5.2.1 信頼すべき役割

カード代替電磁的記録用 CWT Signer における役割は、次のとおりとする。なお、「5.2.1.5 システム技術担当者」「5.2.1.6 PKI 技術担当者」「5.2.1.7 運用保守担当者」「5.2.1.9 施設スタッフ」はカード代替電磁的記録用 CWT Signer の機能ごとに複数存在する可能性がある。

5.2.1.1 認証局管理責任者

認証局管理責任者は、カード代替電磁的記録用 CWT Signer の運営に関する責任者であり次の業務を行う。

- ・ カード代替電磁的記録用 CWT Signer に係るシステムの統括
- ・ キーセレモニーにおける総責任者として、作業の正常完了の承認
- ・ インシデント対応における、鍵や電子証明書の危殆化判断と再発行手続の承認
- ・ カード代替電磁的記録用 CWT Signer 監査対応における現場責任者としての実行

5.2.1.2 運用保守責任者

運用保守責任者は、システム運用保守業務の責任者であり次の業務を行う。

- ・ カード代替電磁的記録用 CWT Signer に関するインシデント対応における、問題管理、リリース管理における更新の承認
- ・ カード代替電磁的記録用 CWT Signer 運用保守業務の責任者として、システムのインストール、設定及び保守
- ・ カード代替電磁的記録用 CWT Signer 運用保守業務の責任者としての各ステークホルダーの窓口
- ・ 年間、月次の活動計画の策定及び遂行
- ・ 各ステークホルダーとの会議開催及び活動計画の承認とその遂行実績の報告
- ・ カード代替電磁的記録用 CWT Signer 設備の管理
- ・ 定常運用・保守、インシデント対応における運用保守担当者への業務指示及び必要に応じて、各ステークホルダーへのエスカレーション
- ・ キーセレモニーを含むカード代替電磁的記録用 CWT Signer の鍵・電子証明書発行業務の実行・報告

5.2.1.3 秘密鍵管理者

認証局の秘密鍵管理者は、カード代替電磁的記録用 CWT Signer の秘密鍵等を使用する業務に関する責任者であり、次の業務を行う。

- ・ カード代替電磁的記録用 CWT Signer の秘密鍵等生成、自己署名電子証明書発行時の鍵管理装置と HSM に対する操作
- ・ カード代替電磁的記録用 CWT Signer の秘密鍵等の更新時における鍵管理装置と HSM に対する操作

5.2.1.4 認証局電子証明書発行者

認証局電子証明書発行者は、次の業務を行う。

- ・ キーセレモニーの進行に立会い、手順書通りに作業が行われていることを確認
- ・ カード代替電磁的記録用 CWT Signer における電子証明書の生成、失効及び停止の承認

5.2.1.5 システム技術担当者

システム技術担当者は、次の業務を行う。

- ・ カード代替電磁的記録用 CWT Signer システム（ハードウェア、ソフトウェア）の保守、メンテナンス
- ・ 問題管理・インシデント対応、変更管理、リリース管理、構成管理

5.2.1.6 PKI 技術担当者

PKI 技術担当者は、次の業務を行う。

- ・ カード代替電磁的記録用 CWT Signer 業務
- ・ キーセレモニーにおける PKI システム操作
- ・ 各種電子証明書の登録、公開

5.2.1.7 運用保守担当者

運用保守担当者は、次の業務を行う。

- ・ 定常業務におけるシステム運転管理、運用ログの取得
- ・ 問い合わせ対応、定期的な報告書の作成
- ・ 手順書に定められる監査対応業務
- ・ 監査に必要なとなる文書、運用保守実績、ログデータに関する、定められた様式での記録
- ・ 運用手順書の維持管理

5.2.1.8 施設スタッフ

施設スタッフは、次の業務を行う。

- ・ キーセレモニー参加者の入退室の立会い

5.2.2 職務ごとに必要とされる人数

カード代替電磁的記録用 CWT Signer の秘密鍵管理者及び操作要員は、「5.2.1 信頼すべき役割」において定める各作業を複数人で行う。

5.2.3 個々の役割に対する識別と認証

各要員がシステム操作を行う際、システムは操作要員が正当な権限者であることの識別・認証を行う。各要員がその役割に応じてアクセスできる秘密情報は最小限に抑え、各要員の認証は IC カード又は役割を認証する認証装置やパスワードを用いて実施する。パスワードは定期的に変更する。

5.2.4 職務権限の分離が必要な役割

各要員が行う職務権限の分離と作業の指示方法につき次のように定める。

① 権限の分離

人的セキュリティの観点から所定の手続に基づき、職務を分離した上で、権限を付与された複数人の要員によって、施設の運用・管理を行う。

② 認証局管理責任者の権限

重要な業務の指示は、認証局管理責任者が各要員に対して、所定の手続により指示する。

③ 運用保守責任者の権限

運用保守責任者は各担当者等に対し、所定の手続に基づいた各種作業に対する指示及び結果の確認を行う。また要員の権限に応じた登録及び電子証明書を発行する。

5.3 認証局における人事管理面のセキュリティ管理

5.3.1 経歴、資格、経験等に関する要求事項

カード代替電磁的記録用 CWT Signer の業務に従事する者は、役割と責任に応じて、PKI、セキュリティ等の業務遂行に必要な知識、経験を有する者とする。

5.3.2 要員の個人の背景のチェックと認可手順

信頼すべき役割を担う全ての要員は、所要の審査手順に従い、雇用前に書類（履歴書、推薦状等）検査により経歴調査を実施する。

5.3.3 各要員に対する教育訓練要件

教育訓練計画書に従い、各要員に必要な訓練を実施する。教育訓練計画書では教育訓練要件、教育訓練の周期について規定する。

デジタル庁は、教育計画及び実施、訓練計画及び実施を担う。

5.3.4 各要員に対する教育訓練の周期

定期的に訓練を実施し、要員の知識とプロセスを継続的に更新する。これは（少なくとも 12 カ月毎の）新たな脅威と現行のセキュリティ慣行に関する更新を含む。また、業務内容、手順、指揮命令系統、責任及び権限の変更が行われた場合にも訓練を行う。

5.3.5 要員間の業務交代と周期、順序

認証局管理責任者が文書により、業務のローテーション方法を規定する。

5.3.6 許可されていない行動に対する罰則

各要員が職務権限に違反する行動を行った場合には、所定の手続に基づき処分を行う。

一時的な契約スタッフを配備する場合、委託先と運用責任を持つデジタル庁間の契約において、契約スタッフがセキュリティポリシーに違反した場合はデジタル庁が措置を講じることを許可する旨を明示する。措置には以下のものが含まれる。

- ① 契約スタッフに対する保証要件
- ② 契約スタッフの故意の有害行為による損害の補償
- ③ 金銭的な罰則

リスク評価に基づいて必要な場合には、脅迫をうける可能性のある従業員が脅迫警報を発報することが考えられるが、本システムではサポートしないこととする。

5.3.7 各要員に対する契約要件

業務の一部を委託する場合は、委託先との間で委託業務に関する機密保持義務等を含む適切な契約を締結する。デジタル庁は外部委託先の要員が本運用規程で規定される要件に照らして十分な要件を満たしていることを事前に確認する。

5.3.8 各要員に提供される文書

各要員は、それぞれのアクセス権に応じて文書（構築手順書、運用設計書、運用手順書、情報セキュ

リティポリシー等）を閲覧することが可能である。

5.4 監査ログの手続

内部監査人は、カード代替電磁的記録用 CWT Signer におけるセキュリティに関する重要な事項を対象としたアクセスログや操作ログ等の発生事象の記録（以下「監査ログ」という。）を業務実施記録等と照合し、不正操作等異常な事象を確認するセキュリティ監査を行う。

5.4.1 監査ログに記録する情報

カード代替電磁的記録用 CWT Signer は、以下の監査ログを記録する。

- ・ 発行手続に関する操作・稼動ログ
- ・ 失効手続に関する操作・稼動ログ
- ・ 有効性確認に関する全てのアクセス・稼動ログ
- ・ 認証局の鍵ペア生成に関する操作ログ
- ・ システム、各種帳簿等に対するアクセスログ
- ・ 認証局の設備への入退室記録

監査ログには次の情報を含める。

- ・ 一意性のある端末 ID
- ・ 事象又は処理の種類
- ・ 発生日時
- ・ 処理の結果

ただし監査ログは、いかなる形式（例えば、平文又は暗号化されたもの）においてもカード代替電磁的記録利用者の Device Key 秘密鍵を記録しない。

5.4.2 監査ログの検査周期

監査人はセキュリティ監査を定期的に行う。

5.4.3 監査ログの保管期間

1 年間保管する。

5.4.4 監査ログの保護

監査ログは、改ざん防止対策として電子署名を施す。また、定期的に監査ログのバックアップを取得し、監査ログの閲覧及び削除は監査人が適切に行う。

監査ログの署名用秘密鍵は、他の目的に使用されない。

5.4.5 監査ログのバックアップ手順

規定しない。

5.4.6 監査ログの収集システム

監査ログの収集機能は、カード代替電磁的記録用 CWT Signer の一機能とし、セキュリティに関する重要な事象をシステムの起動時から監査ログとして収集する。

5.4.7 監査ログ検査の通知

監査ログの検査は、その事象を発生させた者に通知することなく行う。

5.4.8 脆弱性評価

定期的に、運用面及びシステム面におけるセキュリティ上の脆弱性を評価する。

5.5 記録の保管（アーカイブ）

5.5.1 アーカイブ記録の種類

5.5.1.1 紙で保管する情報

デジタル庁は次の情報を保管する。ただし、キーセレモニーの実施等に関する書類については最新版のみ紙で保管するものとし、最新でなくなった情報はデジタルデータに変換して保存する。

5.5.1.1.1 カード代替電磁的記録用 CWT Signer

- ・ 本運用規程の作成に関する書類
- ・ キーセレモニーの実施等に関する書類
- ・ 監査報告書等
- ・ 設備及び安全対策に関する書類

5.5.1.1.2 RA

紙で保管する情報は規定しない。

5.5.1.2 デジタルデータとして保管する情報

デジタル庁は次の情報を保管する。

5.5.1.2.1 カード代替電磁的記録用 CWT Signer

- ・ 検証者等との取決めに関する書類
- ・ CWT Signer の運営情報の開示・訂正等に関する書類
- ・ 失効情報及び失効情報ファイルの提供状況の報告書
- ・ 失効申請書（デジタル庁へのオンライン申請の場合）
- ・ MSO 失効申請情報等
- ・ CWT 電子証明書
- ・ 失効情報
- ・ 失効記録
- ・ 失効情報ファイル提供履歴
- ・ 各種ログ（監視用ログ、起動停止ログ、操作ログ）等

5.5.1.2.2 RA

- ・ カード代替電磁的記録の失効申請書

5.5.2 アーカイブ保存期間

5.5.2.1 紙で保管する情報

別途定める期間、保管する。

5.5.2.2 デジタルデータとして保管する情報

別途定める期間、保管する。

5.5.3 アーカイブの保護

情報の取り扱い及び保管に関する手順を定めた「情報セキュリティポリシー」に従い、ビジネス上の必要性及び影響を踏まえて情報をラベリングし保護する。

カード代替電磁的記録用 CWT Signer は、アーカイブ化された監査ログを、リスク評価及び法的要求事項によって決定された所定の期間、保管する。また電子証明書及びカード代替電磁的記録の主体以外の関係者からの要求による、アーカイブからの情報開示は、機構の承認を必要とする。

5.5.3.1 紙で保管する情報

認証局に保管する情報は、適切な入退出管理が行われている室内に設置された施錠可能な場所に保管し、温度、湿度等環境に配慮した保護対策を施す。

アーカイブは、紛失、承認されていない破棄及び改ざんへの対策が講じられる。

5.5.3.2 デジタルデータとして保管する情報

保管情報には、アクセス制御を施す。保管情報は、定期的に外部記憶媒体等に取得し、適切な入退室管理が行われている室内に設置された施錠可能な保管庫に保管する。

アーカイブは、紛失、承認されていない破棄及び改ざんへの対策が講じられる。

5.5.4 アーカイブのバックアップ手続

5.5.4.1 デジタルデータとして保管する情報

保管情報は、定期的にバックアップする。

5.5.5 記録に付与するタイムスタンプの要件

5.5.5.1 デジタルデータとして保管する情報

保管情報には、タイムスタンプ（時刻情報）を付与する。

タイムスタンプの日付と時刻は、定期メンテナンス時の校正、および、ガバメントクラウドで提供される機能を用いて補正される。

5.5.6 アーカイブ収集システム

規定しない。

5.5.7 保管情報の検証

5.5.7.1 紙で保管する情報

保管情報が記載された紙の保管環境の記録を行い、紙の状態の確認を年 1 回行う。

5.5.7.2 デジタルデータとして保管する情報

保管情報が記録された外部記憶媒体等の可読性の確認を、年 1 回行う。

5.6 認証局の鍵の更新

2 年毎にカード代替電磁的記録用 CWT Signer の鍵ペアの更新を行う。

5.7 鍵の危殆化と災害復旧

5.7.1 事故及び危殆化の取扱手続

認証局は事故及び危殆化が発生した場合に速やかに業務を復旧できるよう、以下を含む事故及び危殆化に対する対応手続（以下「緊急時対応計画」という。）を策定する。

- ・ ハードウェア、ソフトウェア、データ等の破損、故障
- ・ 認証局秘密鍵の危殆化
- ・ 火災、地震等の災害

「緊急時対応計画」は適切なリスクアセスメントに基づいて策定され、セキュリティ事故報告の正式

な手順及び事故報告の受領時に取るべき措置を定めている。これには、責任の割り当てとエスカレーション手順が定義され文書化されている。緊急時は、認証局管理責任者に報告する。

5.7.2 ハードウェア、ソフトウェア又はデータが破壊された場合の対処

ハードウェア、ソフトウェア又はデータが破壊された場合、バックアップ用のハードウェア、ソフトウェア又はデータにより、速やかに復旧作業を行う。

5.7.3 認証局の秘密鍵が危殆化した場合の手順

カード代替電磁的記録用 CWT Signer の秘密鍵が危殆化した場合、緊急時対応計画に従い対処する。主な対処は次のとおり。

- ① 危殆化したカード代替電磁的記録用 CWT Signer の公開鍵を含む CWT 電子証明書をルート認証局が発行する失効記録（CRL）に記録し、情報公開レポジトリである DTS 上で公開する。
- ② 新規のカード代替電磁的記録の MSO ステータストークンの生成を停止する。
- ③ カード代替電磁的記録用 CWT Signer の CWT 電子証明書を再発行して、カード代替電磁的記録用 CWT Signer の環境設定を行う。
- ④ 新規のカード代替電磁的記録発行の MSO ステータストークンの発行業務を再開する。

カード代替電磁的記録の失効手続については、本運用規程「4.9 カード代替電磁的記録の失効と一時停止」に規定する。

5.7.4 災害発生時の設備の確保

災害等により設備が被害を受けた場合は、緊急時対応計画に従い運用を行う。「緊急時対応計画」には下記の事項を含む。

- ① デジタル庁は、障害発生時の障害修正（障害切り分け窓口と連携して障害修正を緊急で実施）、機構へのエスカレーション等を実施する。機構は、対応状況の確認を実施する。
- ② デジタル庁は、緊急時運用（パンデミック、大規模地震等）、大規模システム故障への対応を実施する。
- ③ デジタル庁は、インシデント管理に関する実績集計の計画立案、インシデントに関する実績集計、定期報告、インシデントの受付・応急措置、インシデント管理のモニタリング、苦情/問合せ対応、作業依頼の実施、インシデントに関する改善検討・実施を担う。

5.8 CWT Signer の運営の終了

規定しない。

6 技術面のセキュリティ管理

6.1 鍵ペアの生成とインストール

6.1.1 鍵ペアの生成

6.1.1.1 カード代替電磁的記録用 CWT Signer の鍵ペア

カード代替電磁的記録用 CWT Signer の鍵ペアは、複数人の秘密鍵管理者が FIPS140-3 レベル 3 相当の HSM を用いて生成する。

6.1.2 検証者への認証局公開鍵の配布

カード代替電磁的記録用 CWT Signer の CWT 電子証明書は、CWT 発行の際に CWT の protected header に格納して検証者(verifier)に交付する。また、カード代替電磁的記録の発行の際に MSO に CWT の参照先の URL を格納し、安全かつ確実な手段で検証者等が DTS から CWT をダウンロードできる手段を提供することで配付する。

6.1.3 鍵サイズ

鍵サイズは次のとおりとし、デジタル庁はセキュリティ強度に関する年次レビューにおいて鍵サイズの変更の必要性を確認する。変更の必要性があった場合には機構へ報告を実施し、変更の承認を得る。

6.1.3.1 カード代替電磁的記録用 CWT Signer の鍵ペア

ES256 ビットの鍵を使用する。

6.1.4 公開鍵パラメータの生成及び品質検査

規定しない。

6.1.5 鍵の利用目的 (X.509 v3 Key Usage Field)

6.1.5.1 カード代替電磁的記録用 CWT Signer の鍵ペア

CWT に電子署名するために使用される。

6.2 秘密鍵の保護と暗号モジュールの技術管理

6.2.1 暗号モジュールの標準及び管理

6.2.1.1 カード代替電磁的記録用 CWT Signer の秘密鍵

カード代替電磁的記録用 CWT Signer の秘密鍵を HSM へ格納し、FIPS140-3 レベル 3 相当の HSM により保護する。

6.2.2 秘密鍵の複数人制御

6.2.2.1 カード代替電磁的記録用 CWT Signer の秘密鍵

カード代替電磁的記録用 CWT Signer の秘密鍵は、複数人の秘密鍵管理者により制御する HSM で秘密鍵を保護する。

6.2.3 秘密鍵の預託 (エスクロー)

6.2.3.1 カード代替電磁的記録用 CWT Signer の秘密鍵の預託

カード代替電磁的記録用 CWT Signer の秘密鍵の預託は行わない。

6.2.4 秘密鍵のバックアップ

6.2.4.1 カード代替電磁的記録用 CWT Signer の秘密鍵

カード代替電磁的記録用 CWT Signer の秘密鍵のバックアップは、実施しない。秘密鍵の危殆化、または、HSM の故障等で利用できなくなった場合、別の秘密鍵を利用する。

6.2.5 秘密鍵のアーカイブ

秘密鍵のアーカイブは行わない。

6.2.6 秘密鍵の暗号モジュールへの転送

秘密鍵の転送は行わない。

6.2.7 暗号モジュールへの秘密鍵の格納

6.2.7.1 カード代替電磁的記録用 CWT Signer の秘密鍵

カード代替電磁的記録用 CWT Signer の秘密鍵は、複数人の秘密鍵管理者による操作で HSM の中で生成し、HSM 内の暗号モジュールで秘匿性を担保する。

6.2.8 秘密鍵の活性化方法

6.2.8.1 カード代替電磁的記録用 CWT Signer の秘密鍵

カード代替電磁的記録用 CWT Signer の秘密鍵は HSM に格納されており、常にオンラインだが、システム起動時は複数人の操作により活性化する。リスクアセスメントに基づき、必要に応じて多要素認証を使用する。

6.2.9 秘密鍵の非活性化方法

6.2.9.1 カード代替電磁的記録用 CWT Signer の秘密鍵

カード代替電磁的記録用 CWT Signer の秘密鍵は複数人の操作により非活性化する。

6.2.10 秘密鍵の破棄方法

6.2.10.1 カード代替電磁的記録用 CWT Signer の秘密鍵

暗号モジュール内のカード代替電磁的記録用 CWT Signer の秘密鍵の破棄は、複数人の秘密鍵管理者により暗号モジュールを初期化する等の方法により、完全に利用できない状態にする。

6.2.11 暗号モジュールの評価

本運用規程「6.1.1.鍵ペアの生成」及び「6.2.1.暗号モジュールの標準及び管理」において定める。

6.3 鍵ペア生成管理に関する他の局面

6.3.1 公開鍵のアーカイブ

6.3.1.1 カード代替電磁的記録用 CWT Signer の公開鍵

カード代替電磁的記録用 CWT Signer の公開鍵は CWT 電子証明書に含まれている。

6.3.2 カード代替電磁的記録の有効期間と鍵ペアの使用期間

6.3.2.1 カード代替電磁的記録用 CWT Signer の公開鍵証明書の有効期間と鍵ペアの使用期間

カード代替電磁的記録用 CWT Signer の CWT 電子証明書の有効期間は 2 年とする。カード代替電磁的記録用 CWT Signer の秘密鍵の使用期間は 2 年とし、鍵を生成した日から起算して 2 年以内に鍵更新を行う。ただし、暗号方式が脆弱になったと判断した場合は、暗号方式の変更又は鍵長の変更を検討その時点で鍵更新を行う場合がある。

新しい鍵ペアのための電子証明書は、利用期限が切れる 1 ヶ月前を発行開始期限とする。

6.4 活性化データ

6.4.1 活性化データの生成及び設定

6.4.1.1 カード代替電磁的記録用 CWT Signer の秘密鍵

カード代替電磁的記録用 CWT Signer の秘密鍵を格納する HSM の活性化データは、管理鍵により設定する。

6.4.2 活性化データの保護

6.4.2.1 カード代替電磁的記録用 CWT Signer の秘密鍵

カード代替電磁的記録用 CWT Signer の秘密鍵を格納する HSM の活性化に必要な管理鍵は安全に保管する。

6.4.3 活性化データの他の考慮点

規定しない。

6.5 コンピュータセキュリティ管理

6.5.1 コンピュータセキュリティに関する技術的要件

カード代替電磁的記録用 CWT Signer に係るシステムには、信頼される OS の使用、アクセス制御、各要員の識別と認証機能、監査ログ及びアーカイブデータの収集機能及びシステムのリカバリ機能等を備える。また使用する機器は、メーカーの指示及び/又は他の文書化された手順に従って保守される。

6.5.2 コンピュータセキュリティ評価

システムのセキュリティ評価を定期的に実施する。

6.6 ライフサイクルセキュリティ管理

6.6.1 システム開発管理

サービスに係るシステムの開発、修正又は変更に当たっては、所定の手続に基づき、信頼できる組織及び環境下において作業を実施する。開発、修正又は変更したシステムは、テスト環境において検証を行い、認証局管理責任者の承認を得たうえで導入する。また、システム仕様及び検証報告については、文書化し保管する。

6.6.2 セキュリティ運用管理

サービスに係るシステムを維持管理するため、OS 及びソフトウェアのセキュリティチェックを定期的に行う。また、この検証結果を文書化し保管する。また、適宜ウイルス対策及び不正プログラム対策を行う。

6.6.3 ライフサイクルのセキュリティ管理

デジタル庁は、カード代替電磁的記録用 CWT Signer のシステム開発、運用、保守が適切に行われていることについて監査等を通じて適宜評価し、機構及びデジタル庁は、必要に応じて改善を行う。

6.7 ネットワークセキュリティ管理

カード代替電磁的記録用 CWT Signer の各コンポーネントに対しては、不正アクセスを防止するため、外部ネットワークの通過を許可するネットワークサービスは必要最小限とする。また、不正侵入検

知等の十分なセキュリティ保護対策を行う。

6.8 タイムスタンプ

カード代替電磁的記録用 CWT Signer は、信頼される時刻源を使用してシステムの時刻同期を行い、システム内で記録される重要な情報に対しレコード単位でタイムスタンプを付与する。

7 電子証明書のプロファイル

7.1 電子証明書のプロファイル

電子証明書のプロファイルは、技術資料に定める。なお、CWT 電子証明書は【ISO/IEC 18013-5】に準拠し、「7.1.2 電子証明書拡張」の情報を記載する。

7.1.1 バージョン番号

【ISO/IEC 18013-5】より、バージョン番号は「3」とする。

7.1.2 CWT 電子証明書/拡張

- ・ バージョン番号 (X.509 電子証明書フォーマットのバージョン番号)
- ・ シリアル番号 (ルート認証局内で発行済み電子証明書を識別するための番号)
- ・ 署名アルゴリズム (ルート認証局が当該 CWT 電子証明書へ署名する際に用いたアルゴリズム情報)
 - ・ 発行者情報 (当該 CWT 電子証明書を発行した機構名が X.500 識別名で記述される)
 - ・ 有効期間の開始日 (当該 CWT 電子証明書の発行日)
 - ・ 有効期間の終了日 (発行日の2年後)
 - ・ 公開鍵 (カード代替電磁的記録用 CWT Signer の公開鍵)
 - ・ 拡張情報

7.1.3 アルゴリズム Object Identifier

ルート認証局では、次の署名アルゴリズムが使用される。

- ・ CWT 電子証明書：ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3)

7.1.4 名称形式

「3.1.1 名称の種類」に準じる。

7.1.5 名称の制約

【ISO/IEC 18013-5】より、name constraints 拡張子を使用してはならない。

7.1.6 証明書ポリシー Object Identifier

証明書ポリシーの OID は、【ISO/IEC 18013-5】で定義された電子証明書プロファイルに従い、電子証明書では記載しない。

7.1.7 ポリシー制約拡張の使用用途

【ISO/IEC 18013-5】より、policy constraints 拡張子を使用してはならない。

7.1.8 ポリシー修飾子の構文とセマンティクス

規定しない。

7.1.9 Critical な証明書ポリシー拡張の処理セマンティクス

検証者は、検証者が認識できない Critical な拡張又は検証者が処理できない情報を含む Critical な拡張を見つけた場合、電子証明書を拒否しなければならない。

8 MRL のプロファイル

8.1 MRL のプロファイル

MRL (MSO Revocation List) は、ISO/IEC18013-5 で規定される Identifier List 方式により、CWT が Identifier list の MSO の失効情報として提供される。

8.2 CWT 形式の失効情報のプロファイル

MRL は、RFC 8392 に規定する CWT 形式とし、RFC 9052 第 4.2 節に規定されている COSE_Sign1 構造を使用する。MRL は CWT を COSE_Sign1 で CWT Signer が署名する。COSE_Sign1 の構造を以下に示す。

```
COSE_Sign1 [  
    protected,    // 署名で保護されるヘッダー  
    unprotected,  // この署名の保護対象には含まれないヘッダー  
    payload,      // CWT Claims Set：失効情報、有効期限など  
    signature     // 署名値  
]
```

格納先	項目	設定内容
Protected header	alg (1)	使用する署名アルゴリズムの COSE 識別子
Protected header	typ (16)	application/identifierlist+cwt
Protected header	x5chain (33)	RFC 9360 に従う CWT Signer 証明書または証明書チェーン
Payload	sub (2)	MSO 内の失効情報参照 URI と一致する MRL の URI
Payload	iat (6)	MRL の発行時刻
Payload	exp (4)	MRL の有効期限
Payload	IdentifierList (65530)	identifiers に失効した MSO の識別子を格納
Payload	TTL(65534)	TTL の時間

上記項目は必須とし、署名は、CWT Signer の署名用秘密鍵を用い、RFC 9052 4.4 に従って生成する。

9 準拠性監査

9.1 監査人

監査人は、次の業務を行う。

- ・ 定期的な監査
- ・ キーセレモニー進行への立会い及び手順書通りに作業が行われていることの確認

9.2 監査の頻度

デジタル庁は監査人により年次又は隔年次で定期的準拠性監査を実施する。また、定期監査以外に随時監査を必要に応じて実施する。デジタル庁は監査の結果を機構に報告する。

9.3 監査人の要件

カード代替電磁的記録用 CWT Signer の監査は、監査業務及び認証局の運営に精通した者が行う。

9.4 監査人と被監査組織の関係

デジタル庁は、カード代替電磁的記録用 CWT Signer と利害関係を有しない者を監査人として選定する。

9.5 監査項目

認証局の運営が本運用規程等に準拠して実施されていることの監査を実施する。

9.6 監査指摘事項への対応

デジタル庁は監査指摘事項を確認し、重要性又は緊急性に応じて適切な是正措置を行う。デジタル庁は重要な是正措置を行う場合には、機構に報告して承認を得る。

9.7 監査結果の取扱い

監査結果は、監査人からデジタル庁に対して監査報告書として提出される。デジタル庁は監査法人から提出された監査報告書を機構へ提出する。

認証局管理責任者は、カード代替電磁的記録用 CWT Signer の運営に関する意思決定機関に監査結果を報告する。

10 他の業務上及び法的事項

10.1 手数料

規定しない。

10.2 財務上の責任

規定しない。

10.3 事業情報の秘匿性

10.3.1 秘密情報の範囲

カード代替電磁的記録用 CWT Signer は、漏えいすることによってカード代替電磁的記録用 CWT Signer の運営の信頼性が損なわれる恐れのある情報は機密扱いとする。

10.3.2 秘密情報の範囲外の情報

CWT 電子証明書、CWT 電子証明書の失効情報、本運用規程等に加え、法の規定に基づき公表する情報等は機密扱いとしない。

10.3.3 秘密情報を保護する責任

機構及びデジタル庁は、機密扱いとする情報について、当該情報を含む書類及び電磁的記憶媒体の管理責任者を定め、安全に管理する。またこれらの情報が不要となった際又はカード代替電磁的記録用 CWT Signer が運用終了した際は、適切に制限される。

10.4 個人情報の保護

10.4.1 個人情報保護計画

機構及びデジタル庁は、「個人情報保護基本方針」に基づき個人情報を適切に保護する。

10.4.2 個人情報として扱われる情報

規定しない。

10.4.3 個人情報としてみなされない情報

規定しない。

10.4.4 個人情報を保護する責任

機構及びデジタル庁、市町村の長、検証者は、関係法令に基づき個人情報を適切に保護する。

機構及びデジタル庁は、当該個人情報を含む書類及び電磁的記憶媒体の管理責任者を定め安全に管理する。

10.4.5 個人情報の使用に関する個人への通知及び承諾

CWT Signer は、MSO 及びカード代替電磁的記録の発行には関与しないため個人情報の使用に関する個人への通知及び承諾を行うことは無い。

10.4.6 司法手続又は行政手続に基づく公開

司法機関、行政機関の決定、命令、勧告等があった場合は、機構及びデジタル庁は情報を開示することができる。

10.4.7 他の情報公開の場合

規定しない。

10.5 知的財産権

カード代替電磁的記録用の MRL は機構に帰属するものとする。本運用規程及び関連するプログラム等の知的財産権は、デジタル庁に帰属するものとする。

資料やソフトウェア製品の使用にあたり、知的財産権に関わる法令を遵守する。

10.6 表明保証

10.6.1 認証局の表明保証

10.6.1.1 カード代替電磁的記録用 CWT Signer の表明保証

カード代替電磁的記録用 CWT Signer は、CWT Signer の運営に関して次の内容を表明し、保証する。

- ・ 本運用規程に基づき、カード代替電磁的記録の MRL を発行、更新、失効すること。
- ・ 「2.2 カード代替電磁的記録の MRL に関する情報の公開」に定める情報を公表すること。
- ・ カード代替電磁的記録に紐づく鍵ペアについて、失効記録を「4.1.4 失効記録発行頻度」に定める期間ごとに発行すること。
- ・ カード代替電磁的記録用 CWT Signer の秘密鍵を安全に管理すること。
- ・ カード代替電磁的記録用 CWT Signer の秘密鍵が危殆化した場合は、速やかに危殆化に関する情報を公表すること。
- ・ カード代替電磁的記録の発行、更新、失効等に関する監査ログ及びアーカイブを必要な期間保管すること。
- ・ システムの稼動監視を行うこと。

10.6.2 RA の表明保証

RA は、RA の業務に関して次の内容を表明し、保証する。

- ・ カード代替電磁的記録利用者からのカード代替電磁的記録の失効申請に際して、MRL に対して当該のカード代替電磁的記録の MSO の登録を確実に行うこと。
- ・ マイナンバーカード又は JPKI 署名用電子証明書の失効に際して、MRL に対して当該のカード代替電磁的記録の MSO の登録を確実に行うこと。

10.6.3 カード代替電磁的記録利用者の表明保証

申請者/カード代替電磁的記録利用者は、「4.5.1 カード代替電磁的記録利用者による秘密鍵及びカード代替電磁的記録の使用」に定める内容及び以下に定める内容を遵守することについて表明し、保証する。

- ・ 機構に対し、カード代替電磁的記録を発行及び失効するために本人の署名用電子証明書を用いて申請すること。
- ・ カード代替電磁的記録の記載事項が変更となる場合は、速やかに機構に申請すること。

10.6.4 検証者の表明保証

検証者は、「4.5.2 検証者による公開鍵及びカード代替電磁的記録の使用」に定める内容を遵守することについて表明し、保証する。

10.6.5 その他の関係者の表明保証

10.6.5.1 カード代替電磁的記録用 CWT Signer の運営に関する意思決定機関の表明保証

機構及びデジタル庁は、カード代替電磁的記録用 CWT Signer の運営に当たり以下の事項を保証する。

- ・ 法の規定に基づき、CWT Signer の運営業務を適切に行うこと。
- ・ カード代替電磁的記録及びその失効は本運用規程の定めに基づくこと。
- ・ カード代替電磁的記録用 CWT Signer の役割及び各機能の一部を別の事業者へ委譲することを選択した場合、機構及びデジタル庁は、委譲された機能の完了及びその CPS に関する表明の定義と維持に関する責任を持つこと。

10.7 保証の免責事項

規定しない。

10.8 責任の制限

機構及びデジタル庁は、カード代替電磁的記録用 CWT Signer に責を帰すべき事由のない行為によって発生した損害については、一切損害賠償責任を負わないものとする。

10.9 補償

規定しない。

10.10 有効期間と終了

10.10.1 有効期間

本運用規程は、機構及びデジタル庁の認証局管理責任者の承認により有効となる。「10.10.2 終了」に規定する終了以前に本運用規程が無効となることはない。

10.10.2 終了

本運用規程は、「10.10.3 終了の効果と効果継続」に規定する内容を除きカード代替電磁的記録用 CWT Signer を終了した時点で無効となる。

10.10.3 終了の効果と効果継続

カード代替電磁的記録利用者がカード代替電磁的記録の利用を終了する場合又はカード代替電磁的記録用 CWT Signer の業務を終了する場合であっても、「10.3 事業情報の秘匿性」、「10.4 個人情報の保護」及び「9.14 準拠法」の規定は、終了の事由を問わずカード代替電磁的記録利用者、検証者、機構及びデジタル庁に適用されるものとする。

10.11 関係者との個別通知と伝達

本運用規程上必要とされ又は許容されるカード代替電磁的記録用 CWT Signer に対する通知、請求、要求、依頼その他の連絡は機構を窓口とする。連絡先は「1.5.2 連絡先」に規定する。

10.12 改訂

10.12.1 改訂手続

機構及びデジタル庁は、本運用規程を必要に応じて変更する。

10.12.2 通知方法及び機関

本運用規程を変更した場合には、機構及びデジタル庁は速やかに変更した本運用規程を機構の Web 上で公表する。これをもってカード代替電磁的記録利用者、検証者等への通知とする。

10.12.3 オブジェクト識別子の変更されなければならない場合

規定しない。

10.13 紛争解決手続

本運用規程に関して生じた訴訟の際、全ての当事者は東京地方裁判所を第一審の専属管轄裁判所とする。

10.14 準拠法

日本国の法令に準拠する。

10.15 適用可能な法への準拠性

日本国の法令に準拠する。

10.16 雑則

規定しない。

10.17 他の条項

規定しない。