II．業務機能および技術要件：基盤

II. 業務機能および技術要件：基盤

用語と概念

RA 登録局 (Registration Authority)
証明書発行申請者の本人確認および登録を行い, 証明書発行のもととなる登録原簿を持つ.

CA 認証局 (Certification Authority)
証明書の発行・更新・失効, 鍵の生成・保護, および公開鍵証明書所有者の登録を行う.
なお本書で CA という場合, 登録局業務および認証局業務の双方を含むことがある. また, 単に証明書と記述した場合には, 公開鍵証明書をいうものとする.

AA 属性認証局 (Attribute Authority)
属性証明書の発行局. CAの発行する公開鍵証明書とは証明書所有者 (エンドエンティティ) の特定に利用されるのに対し, 属性証明書はエンドエンティティのアクセス権制御に用いられる.

PM 権限管理局 (Privilege Management Service)
発行された属性証明書の属性内容に応じて, 事前に設定されたルールまたはルール・カテゴリに従いアクセス権限制御を行う.

DS ディレクトリサービス (Directory Service)
ディレクトリサービスには公開鍵証明書や属性情報等が保管され, 照会検索業務に利用される.

TSA 時刻証発行局 (Time Stamp Authority)
対象情報が, その時刻以前に存在し・かつその後改竄されていないことを証明するために用いるタイムスタンプを発行する.

II. 業務機能および技術要件：基盤

1 公開鍵認証

1-1 CA

1-1-1 証明書の発行要求と失効要求

1-1-1-1 RA は, 証明書発行要求クライアントからの証明書発行要求を受け取り, これを保管すること.

1-1-1-2 RA は, 証明書発行要求クライアントからの証明書失効要求を受け取り, これを保管すること.

1-1-1-3 RA は, 各医療施設からの証明書発行要求および失効要求も受け付け, これを保管すること.

1-1-2 証明書の発行

1-1-2-1 RA は, 本人性確認が為されたエンドエンティティに対して私有鍵と公開鍵との組を作成すること.

1-1-2-2 CA は, 作成された公開鍵に対して署名を施し, 証明書を発行すること.

1-1-2-3 CA は, 発行した証明書を利用者に配布できること.

1-1-2-4 CA は, 発行した証明書をディレクトリサービスに登録すること.

1-1-2-5 CA の私有鍵は, 真正性を確保でき詐称危険性のない安全な方法で管理すること.

1-1-3 証明書の失効

1-1-3-1 CA は, 利用者の要求または証明書発行者のポリシーに基づき, 証明書を失効すること.

1-1-3-2 CA は, 私有鍵の危殆化, 証明書記載事項の変化, 利用者から申告に基づき, 証明書を失効させること.

1-1-3-3 CA は, 証明書の失効を利用者に通知できること.

1-1-3-4 CA は, 証明書の失効をディレクトリサービスに登録すること.

1-1-4 失効リストの発行

1-1-4-1 CA は, 利用者の要求または証明書発行者のポリシーに基づき, 失効された証明書の証明書失効リストを作成すること.

1-1-4-2 CA は, 証明書の失効, 証明書失効リストの有効期限切れにより, 証明書失効リストを発行すること.

1-1-4-3 CA は, 発行した証明書失効リストをディレクトリサービスに登録すること.

1-2 公開鍵証明に関するDS

1-2-1 証明書の登録

1-2-1-1 ディレクトリサービス・クライアントの認証を行うこと.

1-2-1-2 CA の要求を受けて証明書を登録すること.

1-2-1-3 ディレクトリサービス・クライアントとのセッションを終了すること.

1-2-2 証明書の検索

1-2-2-1 ディレクトリサービス・クライアントの認証を行うこと.
1-2-2-2 指定された条件に基づき, ディレクトリサービス・サーバから証明書を検索し, ディレクトリサービス・クライアントに対して検索結果を提供すること.
1-2-2-3 ディレクトリサービス・クライアントとのセッションを終了すること.

1-2-3 証明書の削除

1-2-3-1 ディレクトリサービス・クライアントの認証を行うこと.
1-2-3-2 CA の要求を受けて証明書の削除を行うこと.
1-2-3-3 ディレクトリサービス・クライアントとのセッションを終了すること.

1-2-4 失効および失効リストの登録

1-2-4-1 ディレクトリサービス・クライアントの認証を行うこと.
1-2-4-2 CA の要求を受けて失効した証明書もしくは証明書失効リストの登録を行うこと.
1-2-4-3 ディレクトリサービス・クライアントとのセッションを終了すること.

1-2-5 失効および失効失効リストの検索

1-2-5-1 ディレクトリサービス・クライアントの認証を行うこと.
1-2-5-2 指定された条件に基づき, ディレクトリサービス・サーバから失効した証明書もしくは証明書失効リストを検索し, ディレクトリサービス・クライアントに提供すること.
1-2-5-3 ディレクトリサービス・クライアントとのセッションを終了すること.

1-2-6 失効および失効失効リストの削除

1-2-6-1 ディレクトリサービス・クライアントの認証を行うこと.
1-2-6-2 ディレクトリサービス・サーバに対して, 失効した証明書もしくは証明書失効リストの削除を行うこと.
1-2-6-3 ディレクトリサービス・クライアントとのセッションを終了すること.

1-3 ＩＣカードの発行

1-3-1 証明書発行要求リストの作成

1-3-1-1 証明書発行端末は, 証明書発行要求内容を入力できること. また, RA から証明書発行要求を受信できること. そしてこの証明書発行要求を保持すること.
1-3-1-2 証明書発行端末は, 証明書発行要求をICカードに送信すること.
1-3-1-3 IC カードは, その内部において, 証明書発行要求に基づきつつ公開鍵および私有鍵を生成すること.
1-3-1-4 IC カードは, 証明書発行要求をハッシュし, 生成した私有鍵で暗号化すること. すなわち証明書発行要求にデジタル署名すること.
1-3-1-5 IC カードは, 公開鍵および署名を証明書発行端末に送信すること.
1-3-1-6 証明書発行端末は, 証明書発行要求リストを生成すること.
証明書発行要求リストは, 証明書発行要求とその署名から構成されること.
1-3-1-7 証明書発行端末は, 証明書発行要求リストおよび公開鍵を CA に送信すること.

1-3-2 公開鍵証明書の発行

1-3-2-1 CA は, 証明書発行要求リストを受信すること.
1-3-2-2 CA は, 公開鍵に対して署名し, 証明書を生成すること.
1-3-2-3 CA は, 生成した証明書を, 証明書発行端末に返信すること.

1-3-3 IC カードの発行

1-3-3-1 証明書発行端末は生成された証明書を受信し, これが当該ICカードの証明書であること

を検証すること.

1-3-3-2 検証された証明書を IC カードに格納すること.

1-4 サーバ間認証

1-4-1 施設間でのサーバ間認証

1-4-1-1 医療施設のサーバ ID および鍵ペアは, データセンタで発行し支給することが望ましい. ただし医療施設のサーバで生成した鍵にも対応できること.

1-4-1-2 各サーバの私有鍵は, 真正性を確保でき, かつ詐称の危険性がない安全な方法で管理する機構を提供すること.

1-4-1-3 データセンタのサーバとその他のデータ交換を行う対象となる医療施設のサーバ間で SSL 相互認証を行い, セッションを確立すること.

1-5 施設認証

1-5-1 証明書の扱い

1-5-1-1 施設 ID は, データセンタで管理発行すること. なお個人 ID とは別系列の ID として設計すること.

1-5-1-2 施設の証明書の個人識別子には, 当該施設の施設 ID を格納すること.

1-5-1-3 証明書の検証では通常の検証に加え, サーバ ID と施設 ID の照合も行うことが望ましい.

1-5-1-4 施設 PKC を用いるモジュールの起動や動作は, 妥当な認証ポリシーに基づいた手順であること.

1-5-2 認証手順

1-5-2-1 施設間認証および検証は, 以下の手順によること.

1）要求元モジュールと要求先モジュールは，施設証明書を相互に交換すること.
2）要求元モジュールは，要求先モジュールの施設証明書の真正性と有効性を確認すること.
3）要求元モジュールは，被署名用文字列を生成し，ハッシュすること.
4）要求元モジュールは，ハッシュ値に署名すること.
5）要求元モジュールは，署名データを要求先モジュールに送る.
6）要求先モジュールは，署名データを検証すること.
7）要求先モジュールは，要求元モジュールの施設証明書の真正性と有効性を確認すること.
8）要求先モジュールは，被署名用文字列を生成し，ハッシュすること.
9）要求先モジュールは，ハッシュ値に署名データを作成すること.
10）要求先モジュールは，署名データを要求元モジュールに送る.
11）要求元モジュールは，署名データを検証すること.

2 属性登録と権限認証

2-1 属性の形式

2-1-1 attributeType

2-1-1-1 attributeType には, 本調達システムに適合した OID を用いること.
本調達システムが想定する属性には，個人属性と施設属性との二種がある.

2-1-2 attributeValue

2-1-2-1 attributeValue には, 本調達システムに適合した形式にて属性情報を格納すること.

2-2 PM

2-2-1 利用者認証

2-2-1-1 利用者と証明書の交換を行うこと.

2-2-1-2 利用者の証明書ポリシ ID と PM の証明書ポリシ ID との一致を確認すること.

2-2-1-3 利用者の証明書が, 本調達システムの CA が発行した危殆でない証明書であることを確認すること.

2-2-1-4 利用者の証明書が失効リストに登録されていないことを確認すること.

2-2-1-5 利用者の属性および権限を取得すること.

2-2-2 私有鍵の管理

2-2-2-1 PMの私有鍵は, 真正性を確保でき, かつ詐称の危険性がない安全な方法で管理すること.

2-3 属性情報管理

2-3-1 属性情報の管理

2-3-1-1 PM は, 権限管理クライアントまたは他施設からの要求に応じて, その利用者の属性ならびに権限に見合った範囲内で, 属性情報の管理を行うこと.

2-3-2 属性の登録要求

2-3-2-1 PM は, 利用者の証明書および登録対象属性を AA に送り, その属性の登録要求を行うこと.

2-3-2-2 登録された権限属性情報は AA による属性証明書の作成に利用されること.

2-3-2-3 PM は, AA の処理結果を受け取り, 引き続く必要な処理を行うこと.

2-3-3 属性証明要求の発行要求

2-3-3-1 PM は, 利用者の証明書を AA に送り, その属性証明書の発行要求を行うこと.

2-3-3-2 PM は, AA の処理結果を受け取り, 引き続く必要な処理を行うこと.

2-4 権限管理

2-4-1 権限ルールの管理

2-4-1-1 権限管理クライアントから権限ルールの管理を行えること.

2-4-1-2 属性情報と権限ルールの関連付けを登録すること.

2-4-1-3 属性情報に応じて, 必要となる権限を取り出すこと.

2-4-2 利用者権限の制御

2-4-2-1 利用者の属性証明書を取得し, 属性情報から利用者の権限を取得し, 利用者の権限制御を行うこと.

2-4-2-2 AA から返送された属性証明書を受け取ること.

2-4-2-3 受け取った属性証明書の真正性を検証すること.

2-4-2-4 属性証明書から属性情報を取り出すこと.

2-4-2-5 属性情報をキーにして権限ルールを検索し, 利用者権限を取り出すこと.

2-4-2-6 取り出した利用者権限に応じて利用者の権限制御を行うこと.

2-4-3 施設権限の制御

2-4-3-1 要求先モジュールは, 要求元モジュールから送られた施設証明書を元にして施設権限の制御を行うこと.

2-4-3-2 要求先モジュールは, AA に要求元モジュールの施設証明書を送ること.

2-4-3-3 AA は, 要求先モジュールの施設証明書を使って属性情報ディレクトリサーバから属性情報を取り出すこと.

2-4-3-4 AA は, 取り出した属性情報を元にして属性証明書を作成し, 要求先モジュールに返送すること.

2-4-3-5 要求先モジュールは, 受け取った属性証明書の真正性を確認し, 属性証明書から属性情報を取り出すこと.

2-4-3-6 要求先モジュールは, 属性情報をキーにして権限ルールを検索し, 施設権限を取り出すこと.

2-4-3-7 要求先モジュールは施設権限を使用して要求元サーバへのサービス内容を制御すること.

2-5 医療施設の権限管理

2-5-1-1 D 型, W 型医療施設の場合, データセンタの権限管理機構の制御下におかれること.

2-5-1-2 I 型医療施設の場合, 当該内では独自ルールによる権限管理を行うことができるが, データセンターの情報を利用する場合には, データセンタの権限管理機構の制御下におかれること.

2-5-1-3 I 型医療施設は, データセンタの権限管理機構が要求する属性を満たさなければ, 権限付与されないこと.

3 属性認証

3-1 属性の寿命管理

3-1-1 attrCertValidityPeriod と Revocation

3-1-1-1 attrCertValidityPeriod ならびに Revocation は, 属性の寿命, 管理コスト, システム全体のパーフォマンスを勘案して, それらの管理手法を決定すること.

3-2 AA

3-2-1 利用者認証

3-2-1-1 クライアントと証明書の交換を行うこと.

3-2-1-2 クライアントの証明書ポリシ ID と PM の証明書ポリシ ID との一致を確認すること.

3-2-1-3 クライアントの証明書が, 本調達システムの CA が発行した危殆でない証明書であることを確認すること.

3-2-1-4 クライアントの証明書が失効リストに登録されていないことを確認すること.

3-2-1-5 クライアントの属性および権限を取得すること.

3-2-1-6 AA の私有鍵は, 真正性を確保でき, かつ詐称の危険性がない安全な方法で管理すること.

3-2-2 属性の登録

3-2-2-1 PM から送られた属性登録要求 (変更・削除要求を含む) を受け付けること.

3-2-2-2 属性登録の対象となっている利用者の証明書の情報をキーにして, ディレクトリサービスに属性保持者として存在しているか否かを検索すること.

3-2-2-3 属性登録の対象となっている利用者がディレクトリサービスに属性保持者として存在している場合, 属性登録 (変更・削除) 要求に応じた処理をディレクトリサービスに対して要求すること.

3-2-2-4 属性登録の対象となっている利用者がディレクトリサービスに属性保持者として存在していない場合には, 属性保持者の登録を行った後に属性登録 (変更・削除) 要求に応じた処理をディレクトリサービスに対して要求すること. .

3-2-3 属性認証書の発行

3-2-3-1 PM から送られた属性証明書作成要求を受け付けること.

3-2-3-2 属性証明書作成の対象となっている利用者の証明書の情報をキーにして, ディレクトリサービスから属性情報を取得すること.

3-2-3-3 ディレクトリサービスから取得した属性情報を元にして属性証明書を作成すること.

3-2-3-4 作成した属性証明書を PM に返送すること.

3-2-3-5 AA の私有鍵は, 真正性を確保でき, かつ詐称の危険性がない安全な方法で管理すること. (再掲)

3-2-4 属性認証書の有効期間

3-2-4-1 属性証明書作成要求に記された有効期限の妥当性を確認すること.

3-2-4-2 属性証明書作成要求に記された有効期限を属性証明書に登録すること.

3-3 属性証明に関するＤＳ

3-3-1 属性の登録

3-3-1-1 ディレクトリサービス・クライアントの認証を行うこと.
3-3-1-2 AA は, 属性をディレクトリサーバに登録すること.
3-3-1-3 ディレクトリクライアントとのセッションを終了すること.

3-3-2 属性の検索

3-3-2-1 ディレクトリサービス・クライアントの認証を行うこと.
3-3-2-2 指定された条件に基づき, ディレクトリサーバから属性を検索し, ディレクトリサービス・クライアントに提供すること.
3-3-2-3 ディレクトリクライアントとのセッションを終了すること.

3-3-3 属性の削除

3-3-3-1 ディレクトリサービス・クライアントの認証を行うこと.
3-3-3-2 AA は, ディレクトリサーバより, 属性を削除すること.
3-3-3-3 ディレクトリクライアントとのセッションを終了すること.

3-3-4 属性保持者の登録

3-3-4-1 ディレクトリサービス・クライアントの認証を行うこと.
3-3-4-2 AA は, 証明書の情報に基づき, 属性保持者をディレクトリサーバに登録すること.
3-3-4-3 ディレクトリクライアントとのセッションを終了すること.

3-3-5 属性保持者の検索

3-3-5-1 ディレクトリサービス・クライアントの認証を行うこと.
3-3-5-2 指定された条件に基づき, ディレクトリサーバから属性保持者を検索し, ディレクトリサービス・クライアントに提供すること.
3-3-5-3 ディレクトリクライアントとのセッションを終了すること.

3-3-6 属性保持者の削除

3-3-6-1 ディレクトリサービス・クライアントの認証を行うこと.
3-3-6-2 AA は, ディレクトリサーバより, 属性保持者を削除すること.
3-3-6-3 ディレクトリサービス・クライアントとのセッションを終了すること.

4 電子署名

4-1 署名付与

4-1-1 ＩＣカード内私有鍵による署名

4-1-1-1 ドキュメントをハッシュすること.

4-1-1-2 IC カードにハッシュ値を転送し, 私有鍵による暗号化を施して署名を作成すること.

4-1-1-3 ドキュメントに, 署名データ, 署名情報, タイムスタンプレスポンスを付与して署名付きドキュメントを生成すること. なお XML signature を行う際には, その規格に則ること.

4-1-2 ＩＣカード内 PKC による HTTPS セッションの確立

4-1-2-1 IC カード内 PKC, PK, SK による HTTPS セッションの確立が必要な場合, 以下の手順によること.

1）HTTPS サーバの証明書と利用者の IC カード内の証明書を交換し，双方で証明書の検証を行い相互認証すること.

2）利用者側のクライアントはセッション鍵を生成するための情報（プリマスタシークレット）を生成し，HTTPS サーバの公開鍵で暗号化して HTTPS サーバに送ること.

3）HTTPS サーバはプリマスタシークレットを取得すること.

4）双方でプリマスタシークレットを使ってセッション鍵を生成すること.

5）HTTPS サーバから受信した Hello メッセージに対して，IC カード内の私有鍵を使った署名を生成し，サーバに返信すること.

6）HTTPS サーバは利用者の証明書を用いて署名の検証を行うこと.

7）検証確認後，セッションを確立すること.

8）セッションが確立している間，通信データをセッション鍵で暗号化し，セッションがクローズした時点でセッション鍵は破棄すること.

4-2 署名検証

4-2-1-1 署名付きドキュメントから, 署名データ, 署名情報, タイムスタンプレスポンスと, 署名前のドキュメントを取り出すこと.

4-2-1-2 署名者の証明書および公開鍵により, ドキュメント署名者の真正性を検証すること.

4-2-1-3 署名者の証明書または公開鍵がない場合は, CA のディレクトリサービスから署名者の証明書を取得し, 証明書から公開鍵を取り出すこと.

4-2-1-4 署名情報に従って署名データを復号し, 署名前のドキュメントのハッシュ値と比較して, ドキュメントの真正性を検証すること.

4-2-1-5 ＴＳＡの証明書をディレクトリサービスから取得し, 公開鍵を取り出すこと.

4-2-1-6 タイムスタンプレスポンスを検証し, タイムスタンプを取り出すこと.

5 時刻認証

5-1 ＴＳＡ

5-1-1 リクエストの受信

5-1-1-1 クライアントから送られたハッシュ値を受け取ること.

5-1-2 レスポンスの送信

5-1-2-1 受け取ったハッシュ値にサーバの管理する時刻を付与し, これに署名すること.

5-1-2-2 署名済みデータをタイムスタンプレスポンスとしてクライアント機能に返送すること.

5-2 クライアント機能

5-2-1 リクエストの送信

5-2-1-1 ドキュメントのハッシュ値をサーバに送信すること.

5-2-2 レスポンスの受信

5-2-2-1 サーバ機能からタイムスタンプレスポンスを受け取ること.

6 属性の収集と公開

6-1 属性情報の保管形態

6-1-1 D型およびW型医療施設

6-1-1-1 属性情報はデータセンタの属性管理機能に保管すること.

6-1-2 I型医療施設

6-1-2-1 一次属性情報は当該医療施設自身が保管し, データセンタは二次的にデータセンタの属性管理機能に保管すること前提とすること.

6-2 コンテンツの生成

6-2-1 コンテンツ作成要求の受付

6-2-1-1 利用者クライアントから, コンテンツ作成要求を受け付けること.

6-2-1-2 利用者の証明書ならびに属性証明書を検証すること.

6-2-1-3 利用者の権限に応じて, 収集すべき属性情報を決定すること.

6-2-2 医療施設属性の取得

6-2-2-1 データセンタまたは医療施設から, 必要とする属性証明書または属性を収集すること. その手法は, 後述する「属性の授受」に則ること.

6-2-2-2 属性証明書を検証し, 真正性と有効性を検証すること.

6-2-2-3 属性証明書から属性情報を取り出すこと.

6-2-3 コンテンツ生成

6-2-3-1 取得した属性情報をもとにしてコンテンツを生成すること.

6-2-3-2 生成するコンテンツは, 利用者の権限の範囲内とすること.

6-2-3-3 コンテンツを要求元クライアントに送信すること.

7 属性の授受

7-1 静的属性の公開

7-1-1 D型医療施設の属性情報の登録と属性証明書の発行

7-1-1-1 D型医療施設の利用者クライアントから属性情報を登録できること.

7-1-1-2 属性情報はデータセンタ内に登録し, 属性証明書を発行すること.

7-1-1-3 属性証明書の有効期限は属性証明書のアトリビュートごとに設定された有効期限を使用して発行すること.

7-1-2 W型医療施設の属性情報の登録と属性証明書の発行

7-1-2-1 データセンタから定期的に W 型施設が公開している情報提供コンテンツを取得すること. さらに, 上記の方法も併用できること.

7-1-2-2 取得したコンテンツを解析して, 属性情報を取り出すこと.

7-1-2-3 属性情報はデータセンタ内に登録し, 属性証明書を発行すること.

7-1-2-4 属性証明書の有効期限は属性証明書のアトリビュートごとに設定された有効期限を使用して発行すること.

7-1-3 I型医療施設の属性情報の登録と属性証明書の発行

7-1-3-1 I 型医療施設内のディレクトリサービスから属性情報を登録できること. さらに上記二種の方法も併用できること.

7-1-3-2 属性情報はデータセンタ内に登録し(二次保管), 属性証明書を発行すること.

7-1-3-3 属性証明書の有効期限は属性証明書のアトリビュートごとに設定された有効期限を使用して発行すること.

7-1-4 属性証明書の保存と提供

7-1-4-1 属性証明書はディレクトリサービスに保管すること.

7-1-4-2 前述した「属性の収集と公開」からの要求に応じて属性情報を提供すること.

7-2 静的属性の更新

7-2-1 D型医療施設

7-2-1-1 D型医療施設の利用者クライアントから新たな属性情報を登録できること.

7-2-2 W型医療施設

7-2-2-1 データセンタから定期的に W 型施設が公開している情報提供コンテンツを取得すること.

7-2-2-2 取得したコンテンツから取り出した属性情報が更新されていた場合, 新たな属性情報を登録すること.

7-2-3 I型医療施設

7-2-3-1 I型医療施設内のディレクトリサービスから新たな属性情報を登録できること.

7-2-4 属性証明書の更新

7-2-4-1 更新前の当該属性情報の属性証明書を失効させ, 同時に新たな属性情報について新たな属性証明書を発行すること.

7-2-4-2 属性証明書の有効期限は属性証明書のアトリビュートごとに設定された有効期限を使用して発行すること.

7-2-4-3 属性証明書はディレクトリサービスに保管すること.
7-2-4-4 更新内容はログとして記録すること.
7-2-4-5 前述した「属性の扱い」からの要求に応じて属性情報を提供すること.

7-3 動的属性の公開

7-3-1 D 型医療施設

7-3-1-1 D 型医療施設の利用者クライアントからデータセンタへ属性情報を登録できること.
7-3-1-2 データセンタ内に登録されている属性情報を参照すること.

7-3-2 W 型医療施設

7-3-2-1 データセンタから定期的に W 型施設が公開している情報提供コンテンツを取得すること. さらに, 上記の方法も併用できること.
7-3-2-2 取得したコンテンツから属性情報を取り出すこと.

7-3-3 I 型医療施設

7-3-3-1 I 型医療施設内のディレクトリサービスから属性情報を取得すること. さらに, 上記二種の方法も併用できること.

7-3-4 属性証明書の扱い

7-3-4-1 コンテンツ作成時に属性証明書を発行すること.
7-3-4-2 属性証明書の有効期限はコンテンツ作成終了までの寿命とすること.
7-3-4-3 コンテンツ作成終了と同時に属性証明書は破棄すること. ただし, ログとして保存すること.

8　属性情報提供者以外による動的属性更改要求の扱い

8-1　受付機能

8-1-1　更改要求の受付

8-1-1-1　公開コンテンツを介して利用者から送られた動的属性の更改要求を受け付けること.

8-1-1-2　利用者の証明書ならびに属性証明書の真正性と有効性を検証すること.

8-1-2　更改要求の割振

8-1-2-1　I型およびW型医療施設から供給された動的属性が対象とされている場合は, 該当施設へ転送すること. このとき, 動的属性更改要求はログとして保管すること.

8-1-2-2　D型医療施設から供給された動的属性が対象とされている場合は, データセンタに動的属性更改要求を保管すること.

8-2　D型医療施設における対応

8-2-1-1　PM にデータセンタに動的属性更改要求が保管されたことを通知すること.

8-2-1-2　PM は AA と協同して動的属性更改要求を元にして属性情報を更改すること.

8-2-1-3　公開コンテンツ作成機能は更改された属性情報を利用者に返信すること.

8-3　W型およびＩ型医療施設における対応

8-3-1　更改要求の通知と確認

8-3-1-1　医療施設に対して, データセンタに動的属性更改要求が保管されたことを通知すること.

8-3-1-2　医療施設は, 先の通知により, 保存された動的属性更改要求の存在を確認できること.

8-3-2　更改要求内容の送信

8-3-2-1　本調達システムとW型およびI型医療施設とが動的属性更改要求内容を授受するために必要となるインターフェイスを那覇市が無償で公開できるよう, 当該インターフェイスの仕様ならびにコードを提供すること.

8-3-2-2　データセンタは動的属性更改要求を医療施設に送信すること.

8-3-3　更改処理

8-3-3-1　動的属性更改要求に応じた属性更改･または要求拒否は医療施設側で行い, 医療施設側はその応答をデータセンタに返信し, データセンタはその応答を受け取ることができること.

8-3-3-2　医療施設側が動的属性更改要求に応じる場合, 当該施設の公開コンテンツまたはディレクトリサービスを更改すること.

8-3-3-3　データセンタは前述した「属性の収集と公開」および「属性の授受」に拠りつつ, PM と AA ならびに「公開コンテンツ作成機能」が協同して, 当該属性情報の公開内容を更改すること.

8-3-3-4　更改された属性情報を利用者に返信すること.

9 ログ管理

9-1 ログ記録

9-1-1 オペレーションログ

9-1-1-1 各利用者が利用者認証を行った際, ユーザ情報, 日時, 端末情報などをログとして保管すること.

9-1-2 データフローログ

9-1-2-1 エンドユーザが情報の参照を行った際のユーザ情報, コンテンツ情報をログとして保管すること.

9-1-2-2 登録を行った際のユーザ情報, 登録内容情報をログとして保管すること.

9-1-3 属性情報登録ログ

9-1-3-1 各施設, データセンタにある属性情報を変更した際にユーザ情報, 変更内容をログとして保管すること.

9-2 ログの閲覧

9-2-1 ログの検索，閲覧画面

9-2-1-1 ログ情報を各種条件で検索することができること.

9-2-1-2 検索した結果を一覧表に表示することができること.

9-2-2 ログのＣＳＶ出力

9-2-2-1 ログ情報を各種条件で検索することができること.

9-2-2-2 検索した結果を CSV ファイルに出力することができること.

以上