JAHIS

ＪＡＨＩＳ技術文書　１７－１０５

Japanese Association of Healthcare Information Systems Industry

ＪＡＨＩＳ
セキュアトークン実装
ガイド・ノード認証編
Ver.1.1

２０１７年６月

一般社団法人 保健医療福祉情報システム工業会

医療システム部会　セキュリティ委員会

セキュアトークンWG

ＪＡＨＩＳ　セキュアトークン実装ガイド
・ノード認証編　Ver.1.1
ま　え　が　き

本ガイドは、保健医療福祉分野における医療機関等の識別及び認証に用いられるセキュアトークン及びセキュアトークンの利用環境に対する要求事項をまとめたものである。

同一医療圏内、さらには医療圏を超えた医療機関等のネットワークを通じた電子的な手段による連携が重要な課題の一つになっている。ネットワークを通じて医療関連サービスを行うためには、医療機関等の間で電子的に患者情報を含む重要かつ機微な情報を交換することが必要であり、その際には事前に正しい医療機関等の間での情報交換であることを保証するための医療機関等の識別及び認証が必要となる。セキュアトークンは、識別及び認証に用いられる施設のクレデンシャルを安全に格納すると共に、クレデンシャルを利用するための媒体である。本ガイドは、医療サービスを行う施設・設備等のノードを識別・認証するためのクレデンシャルを格納するセキュアトークンに関して、ユースケース、セキュアトークンの要件、運用上の要件、相互運用の要件を明らかにしている。

JAHIS は、産業界の業界団体として医療機関等の連携基盤の普及促進を図るためには医療関連機関等の識別・認証の基盤の普及、セキュアトークンの実装・相互運用性の確保を図ることが重要な役割であるとの判断から、「JAHIS セキュアトークン実装ガイド」として JAHIS 技術文書としてまとめた。その後、情報技術発達によって、様々な機器を無線技術によって接続する例が増えてきている。医療機関等の施設内で利用する医療機器等においても、医療機器等の設置の容易性や可搬性の確保のために Wi-Fi によって施設内ネットワークに接続する例が見られるようになっている。このような状況のため、「JAHIS セキュアトークン実装ガイド･機器認証編」を発行した。この機器認証編との差異を明確にし、参照するガイドラインの更新に対応させ、本書をノード認証編として改訂する。

本ガイドは、JAHIS 会員各社の意見を集約し、「JAHIS 技術文書」の一つとして発行したものである。本ガイドで扱う医療機関等の識別・認証を行うノード認証の要件は、参照規格及び技術動向にあわせて変化する可能性がある。JAHIS としても継続的に本技術文書のメンテナンスを重ねてゆく所存であるが、本ガイドの利用者はこのことにも留意されたい。

本ガイドが、医療機関等の認証基盤の普及・推進に貢献できれば幸いである。

２０１７年６月

一般社団法人 保健医療福祉情報システム工業会
医療システム部会 セキュリティ委員会
セキュアトークンＷＧ

目　　次

1 適用範囲

同一医療圏内、さらには医療圏を超えた医療機関等の連携が、重要な課題の一つになっている。そのような状況の下で適切な医療サービスを行うためには、医療機関等の間で電子的に患者情報を交換することが必要であり、その際には正しい医療機関等の間での情報交換であることを保証するための医療機関等の識別及び認証が、重要な意味をもつ。セキュアトークンは、識別及び認証に用いられる施設のクレデンシャルを安全に格納すると共に利用するための媒体である。

本ガイドでは、ノード認証に用いられるセキュアトークンに必要とされる機能、相互運用で必要となる仕様を明らかにすると共に、運用上で要求される事項をまとめることによって、医療機関等の施設認証の基盤が円滑に導入・運営されることを目標とする。本ガイドで対象とするセキュアトークンは、医療機関等の設備間の認証にも利用可能なものを目指す。

ノードとは、ネットワークに接続され、ネットワークを介して通信を行うネットワークを構成するコンピュータ、ルータ、サーバ等の要素を指す。本ガイドにおいてノード認証は、ノードと関連付けられているエンティティを識別及び認証することを指す。対象となるエンティティは、医療機関等及びその配下の部署等の組織が該当する場合、医療機器等の機器が該当する場合、コンピュータ等を利用する医療従事者等の人が該当する場合等、ノードの利用形態に応じて定まる。本ガイドの目的とするセキュアトークンは、ノード認証のために必要となる各エンティティに対して発行されたクレデンシャルの格納のために利用される。

本ガイドでは、医療サービスを行う施設・設備等のノードを識別・認証するためのクレデンシャルを格納するセキュアトークンに関して、

- セキュアトークンを利用するユースケースを明らかにする。
- セキュアトークンの要件を明確にし、必要な機能を定める。
- セキュアトークンを利用する際に必要となる相互運用性を確保するための仕様を定める。
- セキュアトークンを利用する際に要求される運用上の要求事項を明らかにする。

識別及び認証に用いるクレデンシャルの内容は規定しない。

2 引用規格・引用文献

厚生労働省　医療情報システムの安全管理に関するガイドライン第5版　平成29年X月（予定）

ISO/IEC 19790 Information technology – Security techniques – Security requirements for cryptographic modules

Integrating the Healthcare Enterprise　IHE IT Infrastructure (ITI) Technical Framework Volume 1 (ITI TF-1) Revision 13.0　Sep. 9, 2016

保健医療福祉情報システム工業会　リモートサービスセキュリティガイドライン Ver.3.0　2016年6月

保健医療福祉情報システム工業会　JAHIS シングルサインオンにおけるセキュリティガイドライン Ver.1.0　2016年6月

保健医療福祉情報システム工業会　HPKI対応ICカードガイドライン第2版　2010年6月

3 用語の定義

エンティティ

情報システムを利用するクレデンシャルの対象となる主体。医療分野であれば、患者や医療従事者等の自然人の他、一定の権限をもった病院の代表者や医療機関等の組織、機能範囲によって決められるネットワークに接続される医療機器及びサーバなどの機器及びルータ、GW などのネットワーク機器等が該当する。

クレデンシャル

認証においてエンティティの身元と関連する属性を識別するための情報オブジェクト。一般的なクレデンシャルの例としては、X.509 公開鍵身元識別情報証明書、X.509 属性証明書等がある。

トークン

クレデンシャルを格納するハードウェア。本ドキュメントにおいては、ソフトウェア技術によって仮想的にトークンを実現したソフトウェアトークンと呼ぶものも含む。

セキュアトークン

クレデンシャルを格納し一定の物理的耐タンパー性をもったデバイス。外部からの要求に従ってクレデンシャルへのアクセス、暗号演算等を行って結果を返すことによって、識別及び認証の機能の一部を構成する。

識別

情報システム内で、エンティティを一意に特定するための情報の有効性を検証するプロセス。

認証

電子的な手段によって利用者が情報システムに提示する利用者の身元識別情報に関する信用を確立するプロセス。

ノード

エンティティがネットワークに接続される点。

機器認証

ネットワークに接続された機器の認証。物理的な医療機器等のネットワーク接続の確認に対応する。

ノード認証

ネットワークに接続されたノードの認証。論理的なノードのネットワーク接続の確認に対応する。

4 記号及び略語

このガイドでは、次の略語を用いる

CA	認証局（Certification Authority）
HCF	医療施設（Health Care Facility）
HPKI	保健医療福祉分野公開鍵基盤（Healthcare Public Key Infrastructure）
IA	発行機関（Issuer Authority）
IHE ITI-ATNA	IHE – IT インフラストラクチャ – 監査証跡とノード認証（IHE – IT Infrastructure – Audit Trail and Node Authentication）
JPKI	公的個人認証サービス （Japanese Public Key Infrastructure）
PIN	暗証番号/個人識別番号 （Personal Identification Number）
PKI	公開鍵基盤（Public Key Infrastructure）
RSC	リモートサービスセンタ（Remote Service Center）

5 概説

5.1 ノード認証の必要性

医療情報システムにおいては、機微な情報を取り扱うために、安全の確保されたノード間で情報の交換を行う必要がある。ここでノードとは、ネットワークに接続され、ネットワークを介して通信を行うネットワークを構成する要素（例：コンピュータ、ルータ、サーバ等）である。ノードは物理的な存在であるだけでなく、責任分界点になる。

安全性が確立されている組織内のエンティティが組織外のエンティティと接続する場合には、相手が信頼できる接続先であることを確認する必要がある。そのためには、接続元と接続先の各ノード間で相互にクレデンシャルによって識別して信頼性を確認するノード認証が必須となる。特に機微な情報を取り扱う医療情報システムにおいては、相手が目的の組織に属した信頼できるノードであることを確認することが安全な情報交換が可能なのか否かを判断する最初のステップとなる。

医療情報分野では次のような例が考えられる。

a) 医療機関等の間の地域医療連携サービス
   ・医療機関等内の端末から医療従事者が「地域医療連携システムのサーバにアクセスして必要な患者情報を取得する、あるいは医療従事者の指示に従って必要な患者情報を医療機関等内の情報システムから「地域医療連携システムのサーバに登録・更新する例
b) 医療機関等及び支払い基金
   ・医療機関等内の端末から医療機関等の職員が支払い基金のサーバにアクセスし、レセプトをオンラインで送付する例
c) 医療施機関の医療機器メンテナンスを行うサービス提供者
   ・医療機関内に設置された医療機器が、医療機器のメンテナンスを行うサービス提供者のサーバに対して稼働状況及びエラー状況などの情報を送付する例
   ・医療機器のメンテナンス担当者がサービス提供者内の端末から医療機関内の管理対象機器にアクセスし、メンテナンスに必要となる作業を行う例
d) 医療機関及び薬局
   ・医師の指示によって発行された電子処方箋を医療機関から電子処方箋管理サーバに送付し、薬局からその処方箋を参照して処方する例
e) 遠隔機器間の連携
   ・緊急車両等に設置された医療機器から搬送先になる医療機関のサーバに測定した患者情報を送付する例

図 5-1 に全体像のモデルを示す。丸はネットワークに接続される各ノードを示す。端末・コンピュータ、サーバ、機器等は、それ自身が責任範囲となる。ルータ/ゲートウェイ（GW）は、外部から見ると組織又はサブシステム全体の入り口となるので、組織又はサブシステムが責任範囲となる。

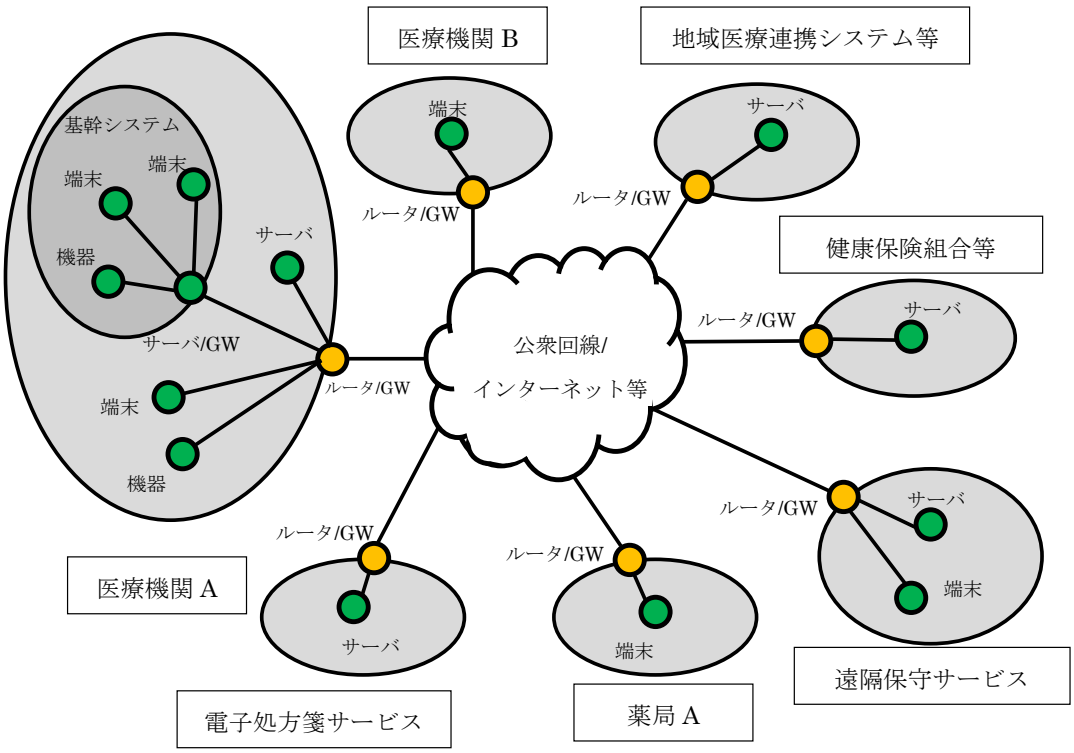

図 5-1　全体モデル

前記 a)に示した地域医療連携サービスの場合には、患者情報の機密性及び完全性を保った状態で施設間のデータ交換を行う必要がある。そのためには、正しい施設であることの識別及び認証が必要となる。施設においては、施設内部のネットワークの入り口/アクセスポイントとなるサーバ、ルータ等のノードとなる接続機器を設置するのが一般的であり、施設の入り口/アクセスポイントとなるノードの識別及び認証を行うことで正しい施設であることを確認することが可能となる。

ある組織の端末が別の組織のサーバ等にアクセスする場合には、各組織の入り口となるルータ/GW 間で組織レベルでの確認が行われ、続いて最終的な目的となる端末とサーバ等の間で接続される必要がある。図 5-2 に概要を示す。

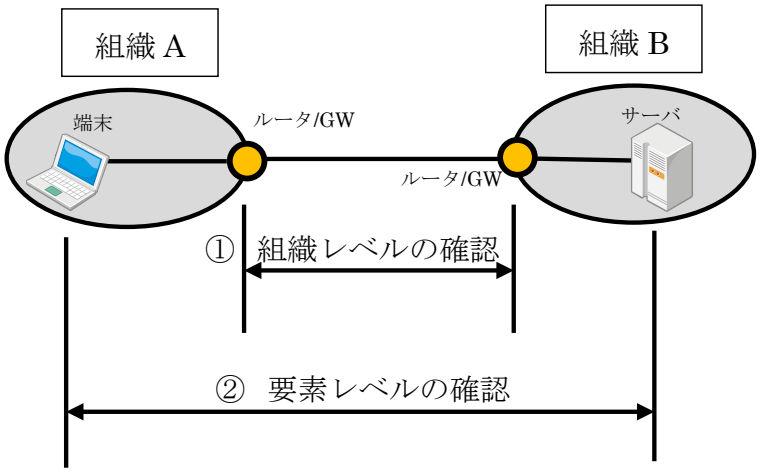

図 5-2　組織間のノードの接続

次に具体的な接続の例を示す

a) 医療従事者が外部のサーバにアクセスする場合

医療機関から地域医療連携のサーバへの情報参照、薬局からの電子処方箋参照等が該当する。図 5-3 にその概要を示す。

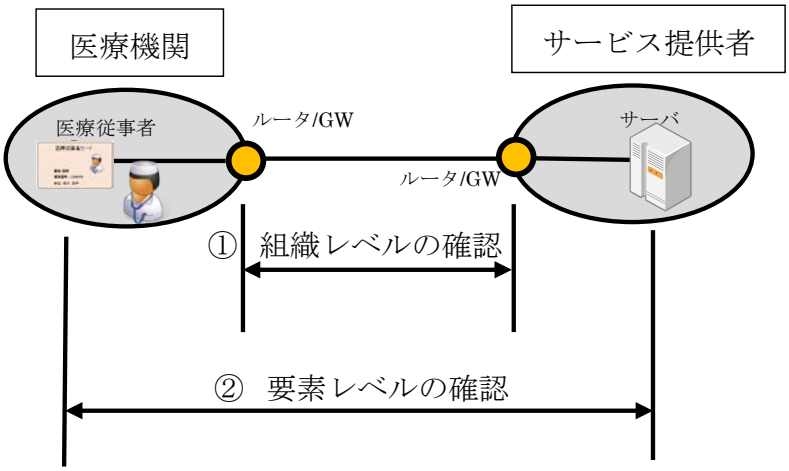

図 5-3 医療機関とサービス提供者間のノードの接続 1

医療機関内とサービス提供者となる地域医療連携サービス、電子処方箋サービスとのノード認証を行い、組織レベルの認証を行う。続いて利用者である医療従事者とサービスを提供するサーバ間でノード認証を行い、認証のプロセスが完了する。その後、医療従事者が必要な情報を参照する。

b) 患者が医療機関内から外部のサーバにアクセスする場合

患者カードを使った医療保険の資格確認、電子処方箋サービスの処方箋参照等が該当する。図 5-4 にその概要を示す。

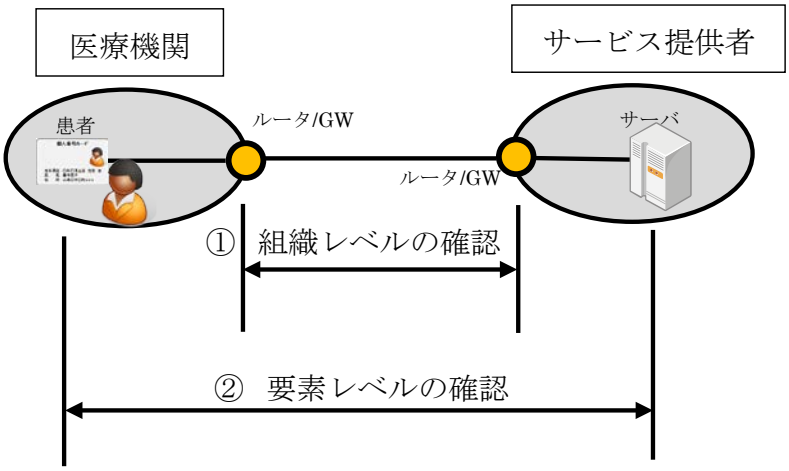

図 5-4 医療機関とサービス提供者間のノードの接続 2

医療機関とサービス提供者となる地域医療連携サービス、電子処方箋サービスとのノード認証を行い、組織レベルの認証を行う。続いて利用者である患者とサービスを提供するサーバ間でノード認証を行い、認証のプロセスが完了する。

c) 医療機関内のサーバと外部サーバが連携する場合

レセプトの審査請求、病院情報システムから地域医療連携サービスへの情報提供などの例が該当する。図 5-5 にその概要を示す。

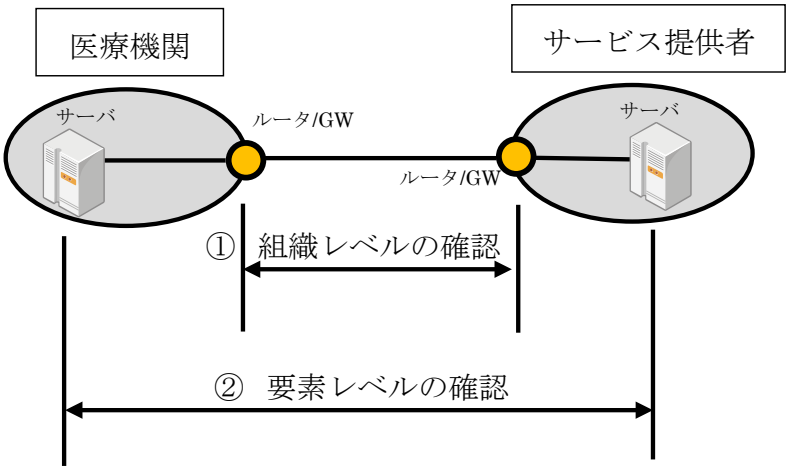

図 5-5　医療機関とサービス提供者間のノードの接続 3

医療機関とサービス提供者となる健康保険組合等、地域医療連携サービスとのノード認証を行い、組織レベルの認証を行う。続いて医療機関内の病院情報システムのサーバと各サービスを提供するサーバ間でノード認証を行い、認証のプロセスが完了する。その後サーバ間で必要な情報が提供される。

d)　リモートメンテナンスのサービス（サーバ/サービスマン）が医療機関内の機器にアクセスする場合

医療機関内の医療機器からリモートメンテナンスを行うサーバに管理情報を送付する場合、リモートメンテナンスサービスから医療機関内の医療機器にアクセスして保守操作を行う場合等が相当する。図 5-6 にその概要を示す。

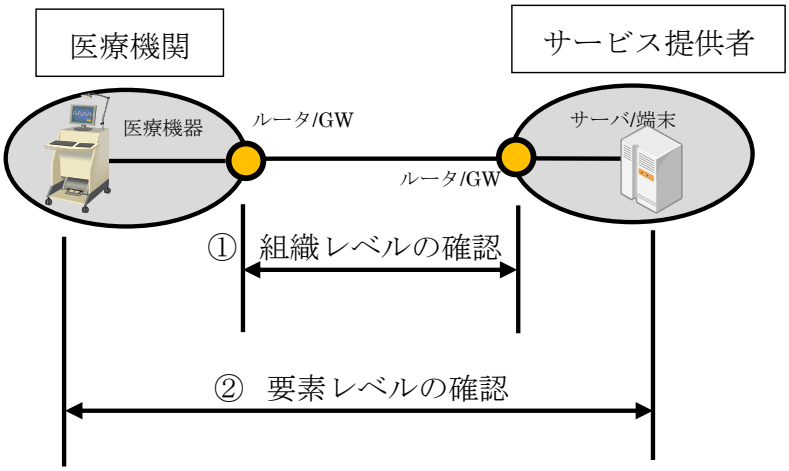

図 5-6　医療機関とサービス提供者間のノードの接続 4

医療機関とサービス提供者となるリモートメンテナンスサービスとのノード認証を行う。続いて医療機関内の機器と各リモートメンテナンスサービスを実施するサーバ又は端末間のノード認証を行う。その後医療機器とリモートメンテナンスサービスを行うサーバ/端末間で必要な情報が提供される。

e)　外部の機器から利用施設のサーバに計測データを送信する場合

緊急車両内の機器から医療機関内の病院情報システムに情報を送信するなどの例が該当する。図 5-7 にその概要を示す。

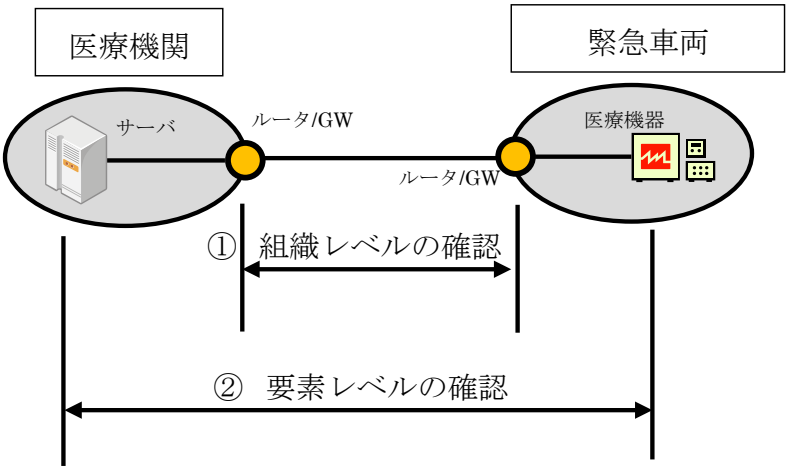

図 5-7　医療機関とサービス提供者間のノードの接続5

医療機関とサービス提供者となる緊急車両とのノード認証を行い、組織レベルの認証を行う。続いて医療機関内の病院情報システムのサーバと緊急車両内の医療測定機器等の間でノード認証を行い、認証のプロセスが完了する。その後医療機器とサーバ間で必要な情報が提供される。

ノード認証に近い考え方に、機器認証がある。機器認証の詳細は、「セキュアトークン実装ガイド・機器認証編」を参照するとよい。機器認証はクレデンシャル及び機器が物理的に１対１に対応するもので、機器を識別・認証するために用いられる。例えば、医療機器のリモートメンテナンスを行う際には、サービス提供者が機器認証によって特定の機器であることを識別し、認証することが重要となる。これに対してノード認証は、ネットワーク上に設置されたノード及びクレデンシャルが論理的に１対１に対応するもので、特定の機器及びクレデンシャルが１対１に対応するとは限らない。例えば、クラウドサービス等の場合には、物理的な機器及びネットワーク上のノードは１対１に対応しない場合が存在する。また、ノードとなる機器が故障した場合には代替の機器とクレデンシャルを論理的に結びつけることによって迅速な復旧を図ることも可能となる。

機器認証の場合には、機器の設置された物理的な場所にかかわらず機器を識別認証することが可能となるので、機器をトレースする観点で重要となる。ノード認証は、医療機関又はその内部の組織等の存在する物理的な場所と関連付けることが可能であり、資産管理等の観点から重要となる。

5.2 ノード認証とセキュアトークン

医療機関等及びその中に設置されている端末（コンピュータ）、サーバ、機器等の数は膨大な数になる。また関連するサービスも、医療情報連携、健康保険の審査請求、電子処方箋、機器のリモートメンテナンス等多岐にわたる。そのため、事前にアクセスを許可する端末を確定して登録しておくなどということは現実的でない。そのため、各ノードに対して発行されたクレデンシャルを用いて相手の正当性を確認する方法が重要となる。ここで、クレデンシャルの中には、ノードを唯一に識別するための識別情報及び関連属性情報が含まれるものとする。

クレデンシャルは、責任をもつべきエンティティに対して発行される。次に一例を示す。

a) 組織：医療関連機関であることを示す。第三者が病院、薬局、関連機関（地域医療連携など）を確認し、保証する必要がある。
b) 人：医療従事者であることを示す。HPKI によって実現できる。
c) 機器：正しい機器であることを示す。製造業者が責任をもつ。
d) サービス提供者：医療機関等の外部にあるサービス一般を指す。保険請求の支払い基金へのレセプ

ト請求、電子処方箋、機器のリモートメンテナンス等のサービスが該当し、正しいサービスであることを示す。

各エンティティに対しては、クレデンシャルが 1 対 1 に紐付けされる。IHE ITI TF-1 では、双方向の証明書に基づいた機器認証を各ノード間の接続のために使用することが要求されている。

トークンは、組織、人、機器等の各エンティティに対して発行されたクレデンシャルを格納し、識別・認証の際に利用可能にするものである。

図 5-8 及び図 5-9 にトークンを利用するノードのイメージを示す。図 5-8 は、ネットワーク機器や医療機器等に埋め込まれたトークンの例である。機器内のトークンに格納されたクレデンシャルによってノード認証を行う。図 5-9 は、トークンが機器から取り外し可能なトークンの例である。医療従事者等の自然人がノードとなる場合には、人に対して発行されたクレデンシャルを例えば IC カードに格納して端末に挿す（結びつける）ことによってクレデンシャルを利用する。機器の場合には、ノードに対して発行されたクレデンシャルを例えば USB トークンに格納して機器に挿す（結びつける）ことによってクレデンシャルを利用する。

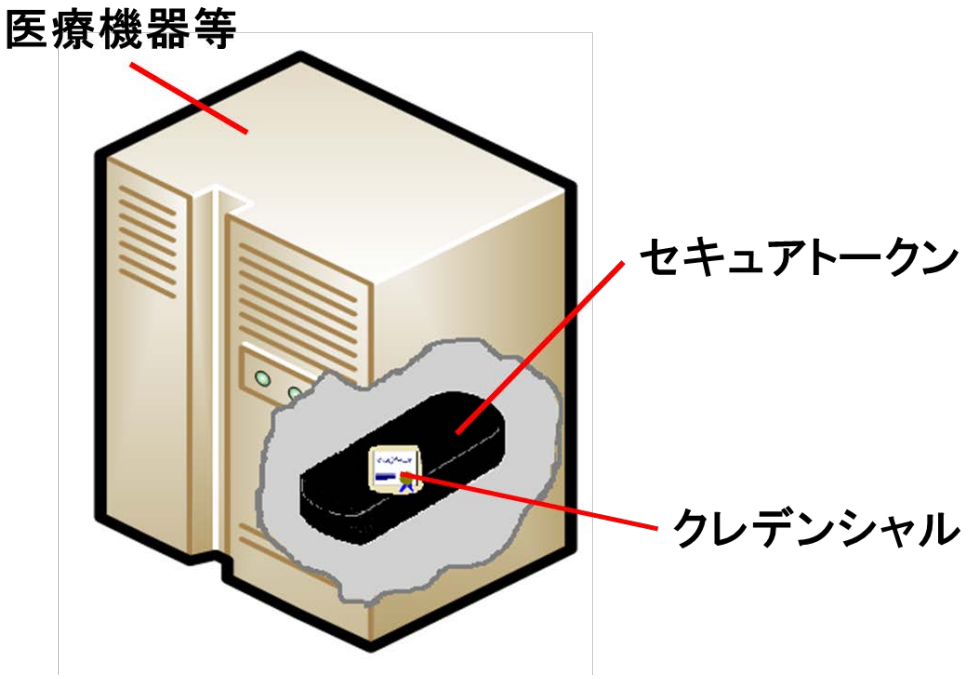

図 5-8　クレデンシャル及びセキュアトークン：機器等の埋め込み型の場合

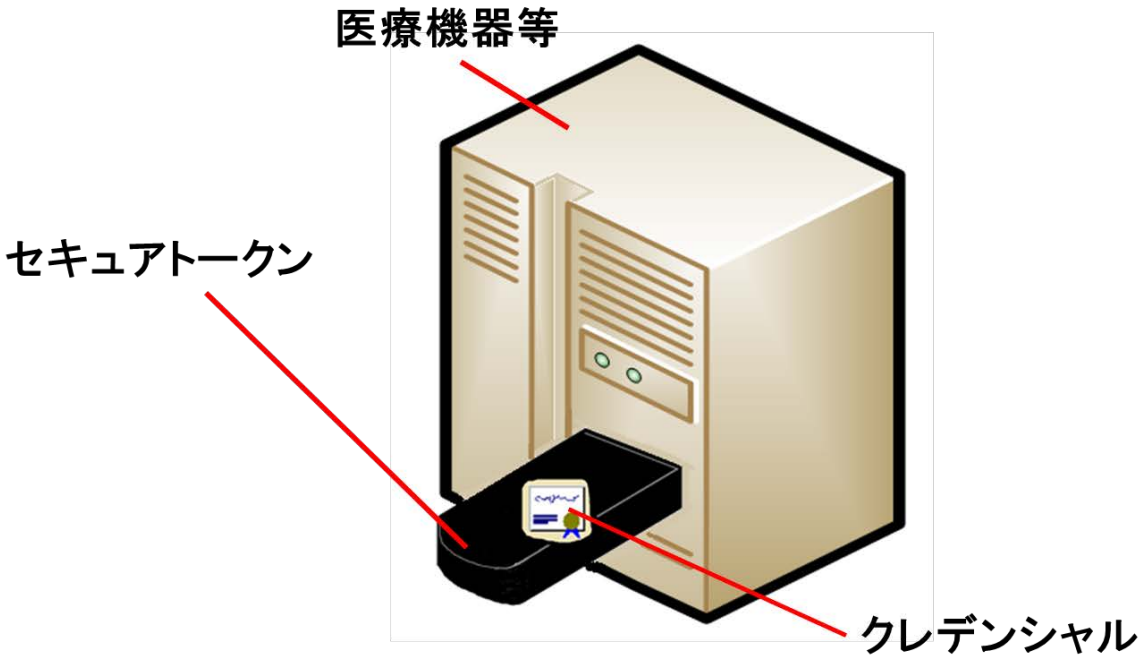

図 5-9　クレデンシャル及びセキュアトークン：人等の取り外し型の場合

識別及び認証においては、クレデンシャルの信頼性検証が重要となる。信頼できる機関から発行されたクレデンシャル [1]が偽造されること及び悪用されることを防がなくてはならない。トークンに対する要求は、7.2 で説明する。

[1] 本ガイドでは、クレデンシャルのコンテンツの信頼性確保及び信頼できるクレデンシャルを発行するためのスキム等についてはスコープ外とする

6 ユースケース

6.1 医療機関等の間の連携にかかわるユースケース

6.1.1 地域医療連携システム

地域医療連携システムとは、医療機関同士をネットワーク接続することによって情報共有を行い、高度な治療をスムーズに地域医療と連携させるシステムである。このユースケースは, 5.1 a) の「医療従事者が外部のサーバにアクセスする場合」の一例である。

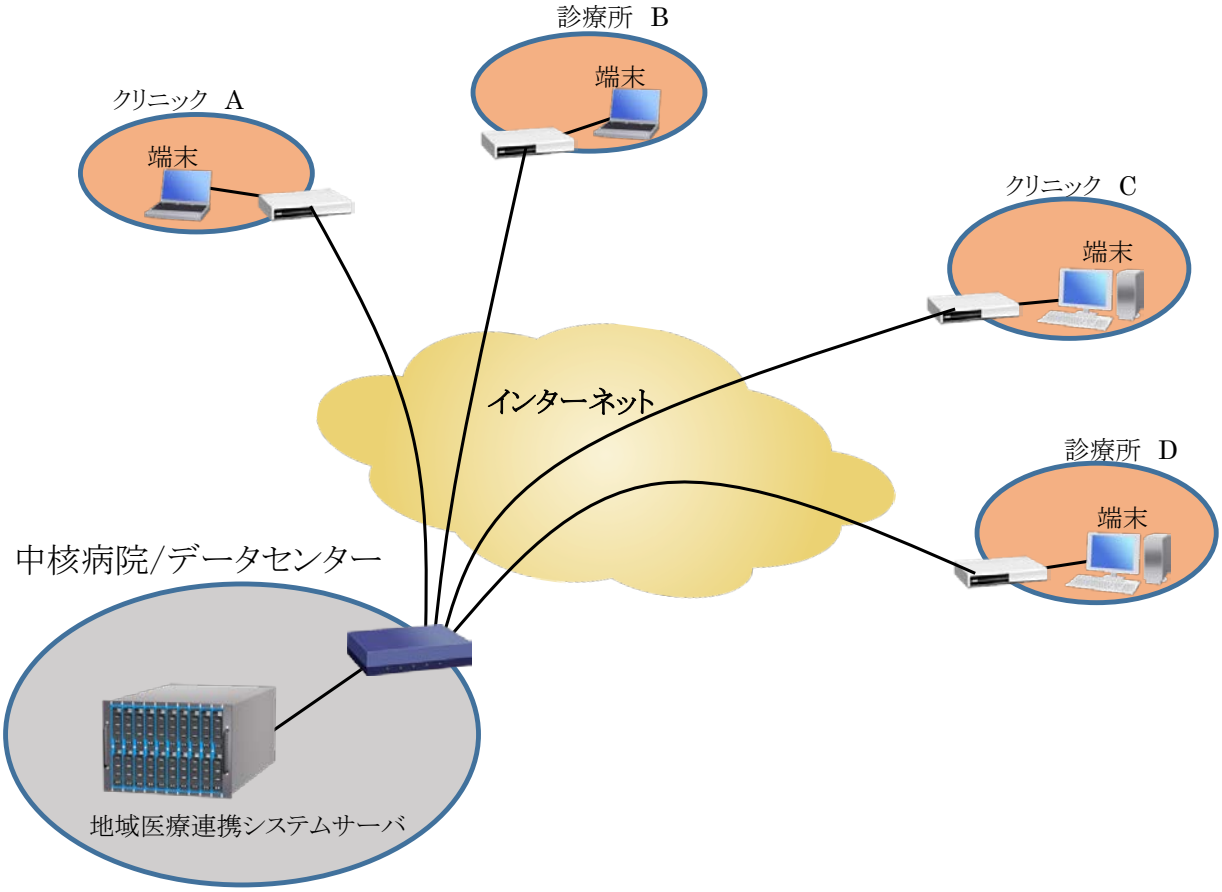

図 6-1 地域医療連携システム イメージ図

その形態としては、図 6-1 に示すとおり中核病院又はデータセンター及び地域のクリニック、診療所を接続するケース、在宅医療を支援するためのケース等さまざまであるが、いずれも医療機関外を通過するため、その経路にはセキュリティが担保される必要がある。

図 6-2 のワークフローは地域医療連携システムの実装の一例である。

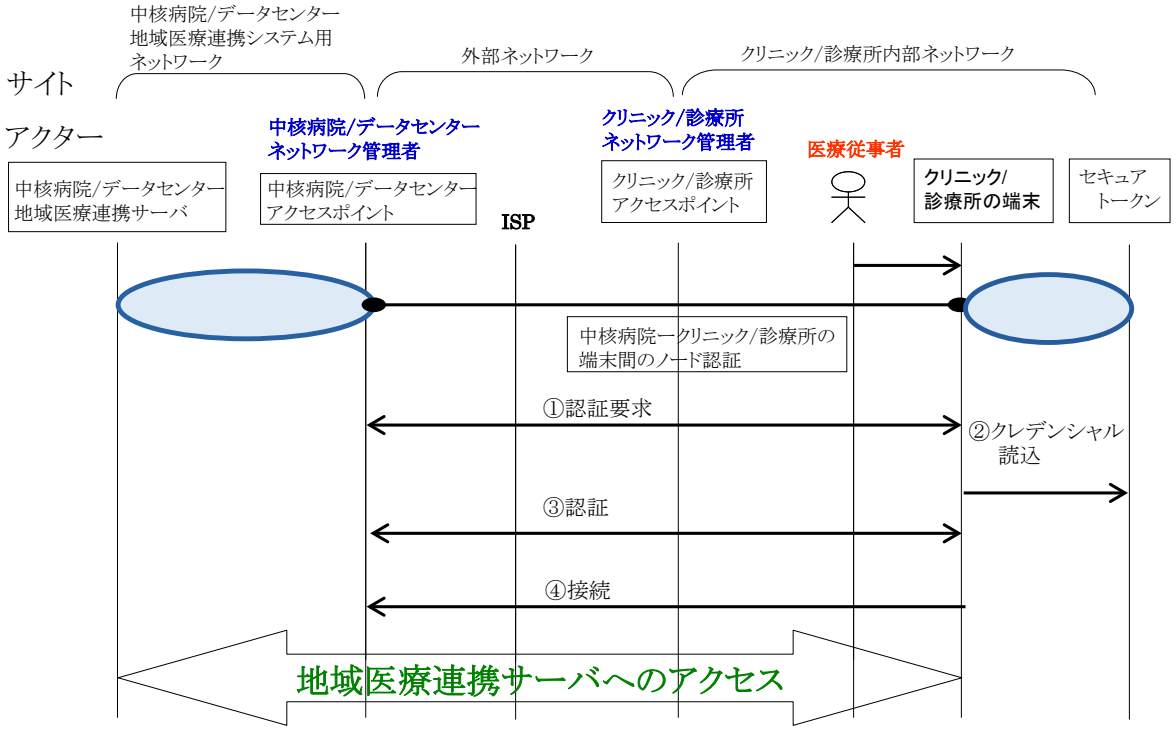

図 6-2　地域医療連携システムを利用する場合のワークフロー

地域医療連携システムを利用するクリニック/診療所の医療従事者は地域医療連携システムを管理する中核病院あるいはデータセンターから配付されたセキュアトークンを利用する端末に取り付ける。

① クリニック/診療所の端末から中核病院/データセンターのアクセスポイントに接続要求を行う。
② 端末はセキュアトークンからクレデンシャルを読み出し、認証要求を受けたアクセスポイントに引き渡す。
③ 中核病院/データセンターのアクセスポイントは、セキュアトークンから読みだされたクレデンシャル情報を利用して認証を行う。
④ 認証に成功した場合、接続を許可する。認証に失敗した場合は、接続を許可しない。

6.1.2　リモートメンテナンス

6.1.2.1 概要

保守作業のために、医療機関等の外部であるリモートサービスセンタからアクセスする場合のワークフローは図 6-3 のようになる。リモートサービスセキュリティの詳細については、JAHIS リモートサービスセキュリティガイドライン Ver.3.0 を参照すること。また、図 6-3 のワークフロー図は、リモートサービスセキュリティガイドラインに基づいて作成したものである。

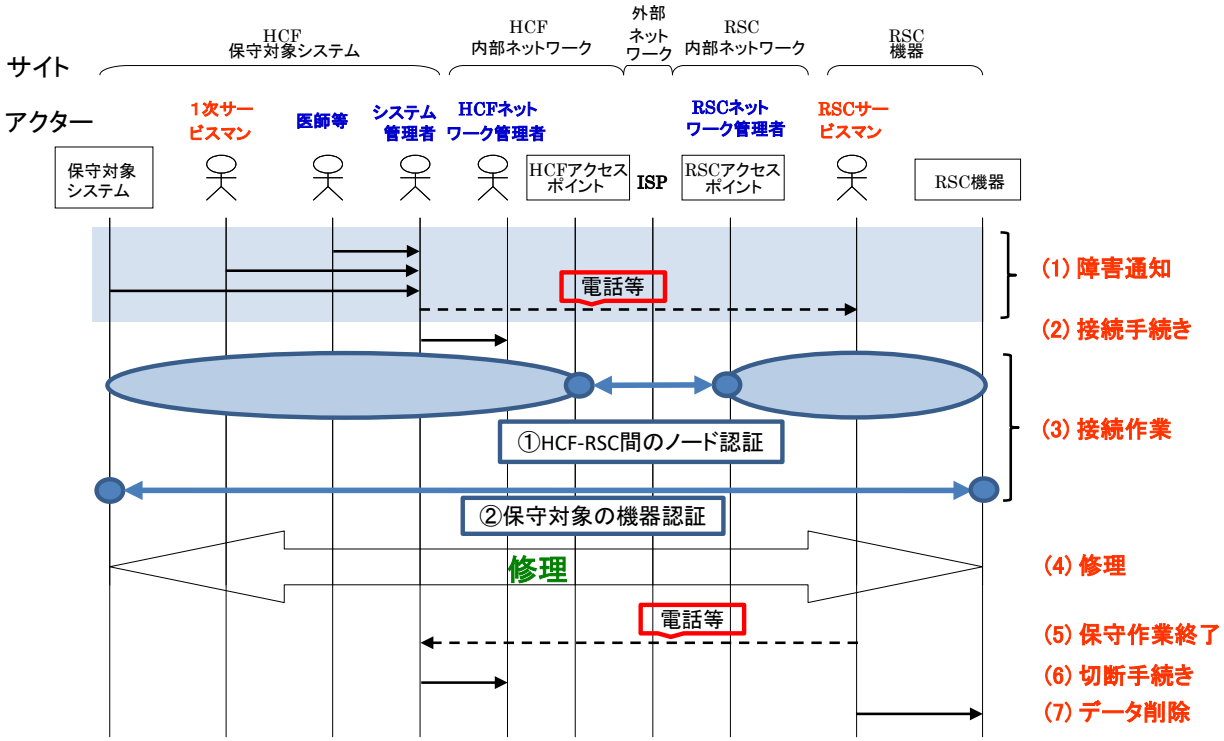

図 6-3　リモートサービスセンタからアクセスする場合のワークフロー

6.1.2.2 組織間のノード認証

組織間のノード認証は　図 6-4 のようなフローとなる。

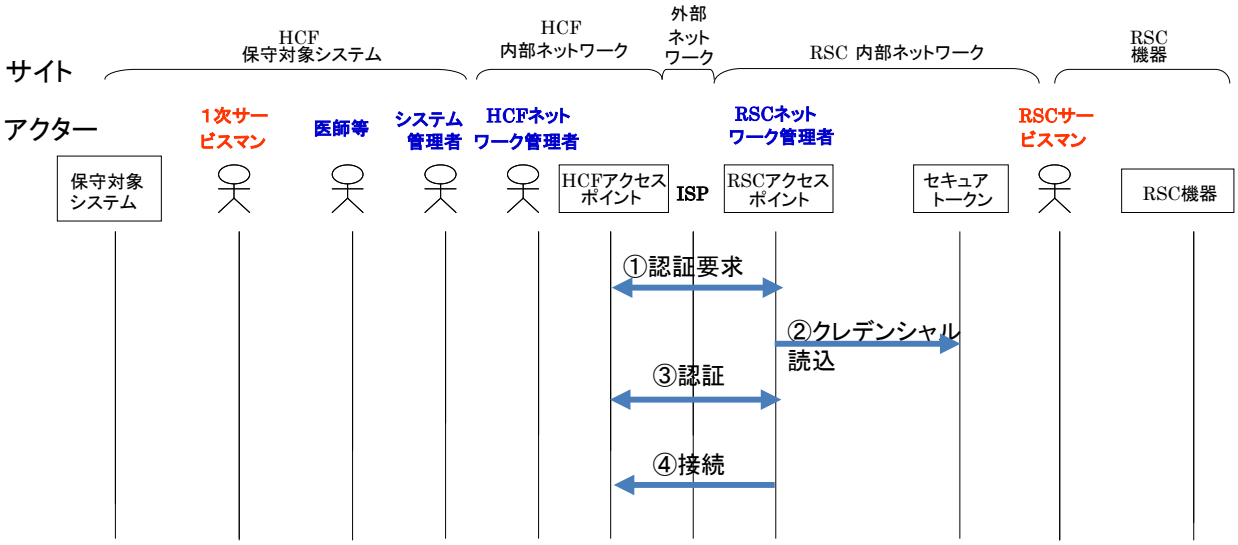

図 6-4　組織間のノード認証

① リモートサービスセンタは、HCF によって指定されたセキュアトークンを RSC アクセスポイントに取り付け、HCF に接続要求を行う（HCF-RSC 間の接続の際にはリモートサービスセキュリティガイドラインに従うこと）。HCF 側は、RSC 側からの接続要求に対して、認証の要求を行う。
② 認証要求を受けた RSC アクセスポイントは、セキュアトークンからクレデンシャル情報を読み出す。
③ RSC アクセスポイントは、セキュアトークンから読みだしたクレデンシャル情報を利用して認証を行

う。認証する際には、シングルサインオン実装ガイド等に従う。
④ 認証に成功した場合、接続を許可する。認証に失敗した場合は、接続を許可しない。

6.1.2.3 リモートメンテナンス機器の機器認証

機器のノード認証は、図 6-5 のようなフローとなる。6.1.2.2 によって、組織間のノード認証は既に行われているため、必要があれば保守対象機器の認証を行う。

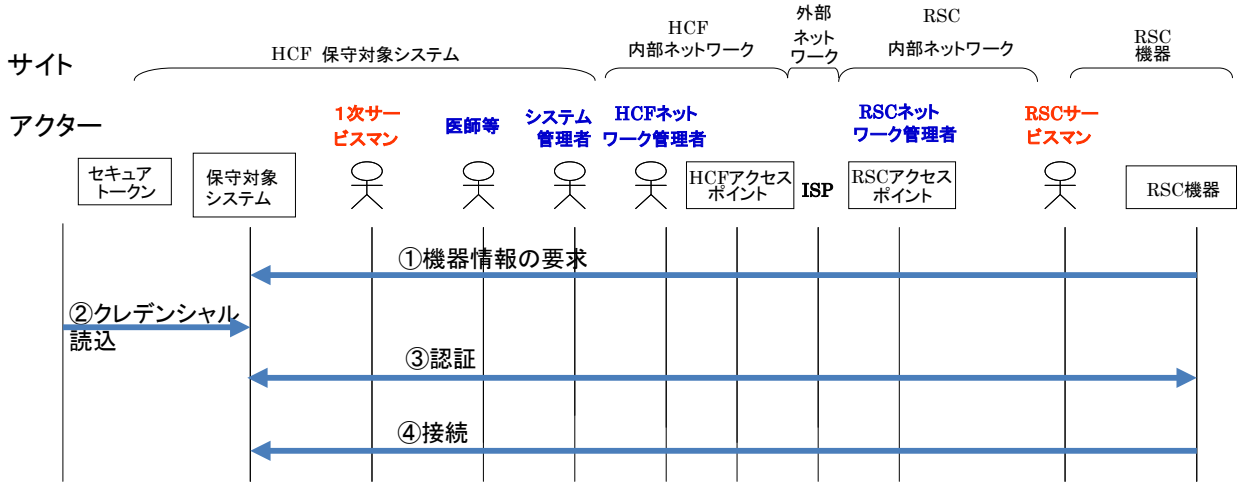

図 6-5　機器のノード認証

① リモートサービスセンタの RSC 機器から、保守対象の機器に対して機器情報の取得要求を行う。
② 保守対象の機器は、要求があった場合、セキュアトークン等から機器の識別を取得する。
③ 保守対象の機器は、取得した保守対象の機器の識別情報を利用して認証を行う。
④ 認証に成功した場合、保守作業を開始する。

6.1.3　医療機関における医療保険の資格確認

医療機関による保険証の即時資格確認については、社会保障サブワーキングによる「医療等の現場での利用を念頭に置いた社会保障カード（仮称）の活用シナリオ」を参考にして JPKI を用いる方式における一例を記載する。

ここでは、PIN なし確認を実施するに当たり、医療機関職員を医療機関内のシステムで認証した上で、医療機関からのリクエストを医療機関認証によって確認することとしており、医療機関のノードに認証用のクルデンシャル（認証用 HPKI など）が利用されることを想定している。
医療機関にて被保険者本人が提示した JPKI を用いて医療機関職員が医療保険の資格確認を行う場合には、暗証番号を入力できない場合が想定されるので、

① 医療機関職員が、券面の情報により正しいカードであること、及び提示した本人のカードであることを確認する。
② 医療機関の保険資格確認システムが職員の認証を行う。
③ 被保険者の IC カード内の証明書情報を取得する。
④ 保険資格確認サービス提供者が医療機関の認証を行う。
⑤ 保険資格確認サービス提供者が被保険者の JPKI の証明書情報を確認する。
⑥ 保険資格確認サービス提供者が保険資格情報を医療機関のシステムに回答する。
⑦ 医療機関職員が資格確認を行う。

という手順によって、資格確認を実現できる（図 6-6）。

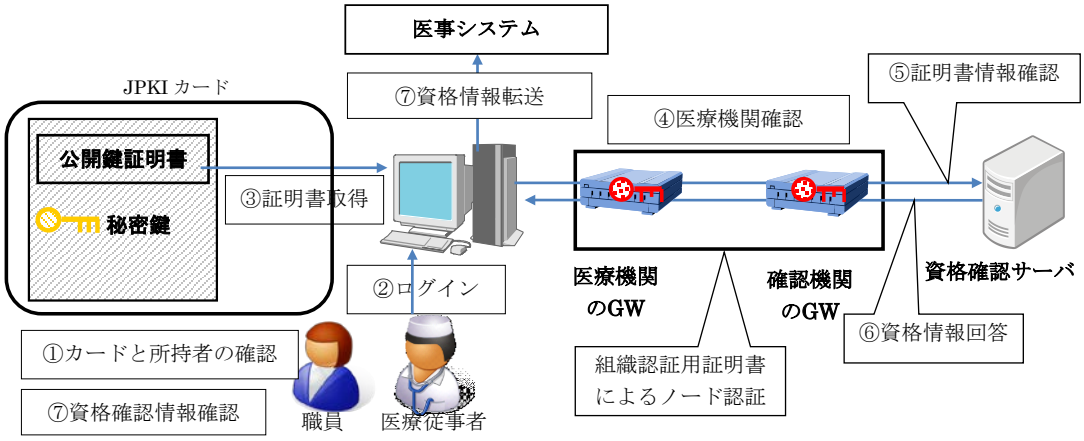

図 6-6　医療保険の資格確認

本人の管理する暗証番号を利用せずに医療保険資格の確認を行う場合には、主に職員が券面の内容に基づいて本人確認を実施するため、暗証番号によって本人確認を行う場合と比較して本人確認の程度が異なる。そのため、暗証番号を入力しないでシステム的に本人性を確実に確認する仕組みが別途構築されていることが期待される。

実現に当たっては、例えば暗証番号の入力を必要とする PKI の仕組みと、暗証番号の入力を必要としない PKI の仕組みをカード上の機能としてもつことをなどが考えられる。

6.2 医療機関等の間の連携に関わる機能要件

ユースケースに関わる主なセキュリティ機能要件として、厚生労働省が発行している「医療情報システムの安全管理に関するガイドライン」から主な該当箇所を抜粋する。詳細はガイドライン参照のこと。（ ）内はガイドライン本文の「最低限のガイドライン」の該当番号を示す。

a)　送信元及び送信先の確認

データ送信元及び送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行う必要がある。採用する通信方式及び運用管理規程によって、採用する認証手段を決めること。認証手段としては PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等の容易に解読されない方法を用いるのが望ましい。

（６．１１．Ｃ．２）

b)　チャネルセキュリティ

ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策を行うこと。

施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を行うこと。

セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策を行うこと。

（６．１１．Ｃ．１）

c)　オブジェクトセキュリティ

送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。例えば、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。

（６．１１．Ｃ．５）

d)　施設内でのなりすまし防止

施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策を行うこと。（６．１１．Ｃ．３）

情報システムへのアクセスにおける利用者の識別及び認証を行うこと。（6．5．C．1）
アクセスの記録及び定期的なログの確認を行うこと。
アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、並びにログイン中に操作した患者が特定できること。（6．5．C．6）

e) リモートメンテナンスにおける不必要なログインの防止
リモートメンテナンスを実施する場合は、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止すること。
（6．11．C．7）
リモートメンテナンスによるシステムの改造又は保守が行われる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること。（6．8．C．8）
メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、及びアクセスした場合は対象個人情報を含む作業記録を残すこと。これはシステム利用者を模して操作確認を行うための識別・認証についても同様である。（6．8．C．2）

7 セキュアトークンの機能

7.1 セキュアトークンの具体例

一般的にセキュアトークンは図 7-1 のような構成を取る。

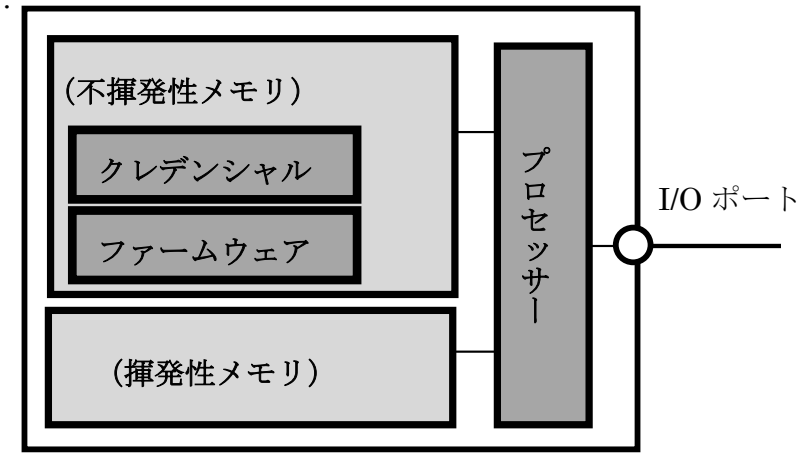

図 7-1　ハードウェアトークンのイメージ

セキュアトークンの具体的な例としては次が挙げられる。

a) USB タイプトークン
USB で接続するタイプのトークンで、取り外しが可能である。トークンは機器又は PC の USB インタフェースに挿入して利用する。内部に図 7-1 に示した機能をもつ IC チップを搭載しており、外部からの要求に従って、クレデンシャルに関する入出力及び暗号演算を行う。

b) IC カード
カード形状のトークンで、ISO/IEC 7816 又は ISO/IEC 14443 等の標準で定められたインタフェースをもつカードリーダを通じて利用する。内部に図 7-1 に示した機能をもつ IC チップを搭載しており、標準で定められたプロトコルを用いて外部からの要求を受け付け、クレデンシャルに関する入出力及び暗号演算を行う。人の認証等に利用される場合が多い。

c) SD カードタイプトークン
SD カードの形状をしたトークンで、取り外しが可能である。SD カード形状のトークンに IC カードと同等のセキュリティ機能を搭載したもので、Advanced Security SD（ASSD）と呼ばれている。トークンは、機器又は PC の SD インタフェースに挿入して利用する。内部に図 7-1 に示した機能をもつ IC チップを搭載しており、外部からの要求に従ってクレデンシャルに関する入出力及び暗号演算を行う。

d) 埋め込み型
IC チップのパッケージの形状をしており、基盤に直付けされて利用される。CPU からは内部バスを通じてアクセスし、IC チップ内部に格納されたクレデンシャルに対する入出力及び暗号演算を行う。例えば、セキュリティチップ（TPM）を内蔵したルータがこれに該当する。

e) ソフトウェアトークン
ソフトウェアだけで構成する暗号モジュールで、暗号演算する機能、クレデンシャル及び暗号鍵の保管機能、及びアクセス制御等の管理機能をもつ。定められた API によって、内部に格納されるクレデンシャルに対する入出力及び暗号演算を行う。

上記 a), b)及び c)は、取り外し可能なタイプのトークン、d)は機器の中に埋め込まれて機器と一体になったトークンであり、それぞれ表 7-1 に示すようなメリット及びデメリットをもつ。選択する際にはこれらを考慮の上、どちらのタイプのトークンを利用するか決定する必要がある。

表 7-1　トークンの形態とメリット及びデメリット

	メリット	デメリット
機器埋め込み型	・設置環境の物理的セキュリティを極端に高める必要はない	・機器の故障が生じると、クレデンシャルは再発行する必要があり、機器の入替と再発行・登録が完了するまで運用が停止する可能性がある
取り外し型	・ハードウェアが故障してもトークンを差換えるだけで済むので、運用停止が最小限で済む可能性がある	・持ち去られる危険性もあるので、設置環境の物理的セキュリティ及び管理に配慮する必要がある
ソフトウェアトークン	・特別なハードウェアを必要としないので、安価で実現することができる ・バックアップを作成することが可能	・物理的な保護がなく、クレデンシャルの複製が作成されてしまう可能性があるので、コピーによって成りすまされる危険性がある ・ハードウェアよりも悪意あるソフトウェアによって攻撃されるおそれが高い

暗号機能のセキュリティレベルは、ISO/IEC 19790 でセキュリティレベル１から４の４つのレベルで規定されている。セキュリティレベル１及び２の要求事項は、次による。

セキュリティレベル１：　基本的な要求事項を超える特別な物理的セキュリティのメカニズムは要求されない。

セキュリティレベル２：タンパー証跡をもつコーティング若しくはシール、又は暗号モジュールがもつ除去可能なカバー若しくはドアに対してこじ開け耐性のある錠を含むタンパー証跡機能をもつ。暗号鍵又はクリティカルセキュリティパラメータ（CSP）への物理的なアクセスがあった場合には、そのコーティング若しくはシールが破壊される。

何らかの物理的な保護がされるのはレベル２であり、セキュアトークンはレベル２以上の物理的な保護が要求される。

7.2 セキュアトークンに要求される機能

7.2.1　概要

セキュアトークンには、通常利用時とライフサイクル管理時(証明書の更新等)で異なる機能が要求される。7.2.2及び7.2.3に各運用時に要求される機能を示す。またそれぞれの機能の「Mandatory」(必須)、「Optional」（任意)、「Conditional」（条件付き）も示す。

7.2.2　通常利用時に要求される機能

a)　クレデンシャル保管機能：「Mandatory」

エンティティ（機器、組織等）の正当性を保証するためのクレデンシャル（電子証明書）を安全に（耐タンパー性＋(必要に応じて)アクセス制御機能）保管する。

b)　セキュアトークンとエンティティ間の認証機能：「Mandatory」

セキュアトークン及び装着されているエンティティがお互いに相手が正当であることを確認する。エンティティが機器の場合は、エンティティ及びセキュアトークンはお互いに正当な相手が保有しているべき暗号鍵を相手側が保有していることを、メッセージのやり取りによって確認する（図 7-2)。

エンティティが自然人の場合は、認証方法として PIN 認証が想定される（図 7-3)。

セキュアトークン内のデータの読み出し、書込み、演算等の前に実行する。

c) 秘密鍵を用いた署名生成機能：「Conditional」

当機能は、エンティティがインターネット等のセキュアでない経路を通り外部接続して利用される場合に必須となる。IHE ITI-ATNA では、エンティティと対向ノードは TLS を用いて相互に認証する。このため、エンティティは下記手順で認証する。

1) クレデンシャルを対向ノードに送信する。

2) 対向ノードから送られてきたチャレンジ（乱数）をクレデンシャル内の公開鍵と対になる秘密鍵を用いて暗号化（署名生成）して対向ノードへ返信する。

d) 利用者データ保管機能：「Optional」

セキュアトークンの利用者が任意の情報を保管する。

利用者データの一例として、機器識別情報が想定される。エンティティが機器の場合、医療機器の不良時にトレーサビリティを行うために、機器製造業者及び機器自体を認識するための機器識別情報を保管する。機器識別情報は、読み出し自由な情報でありかつ、変更が必要な場合は認証行為の正常完了後に行えることとする。

ただし、取り外し型トークンの場合は、運用面で問題（異なるエンティティにセキュアトークンを移し変える場合）がある。

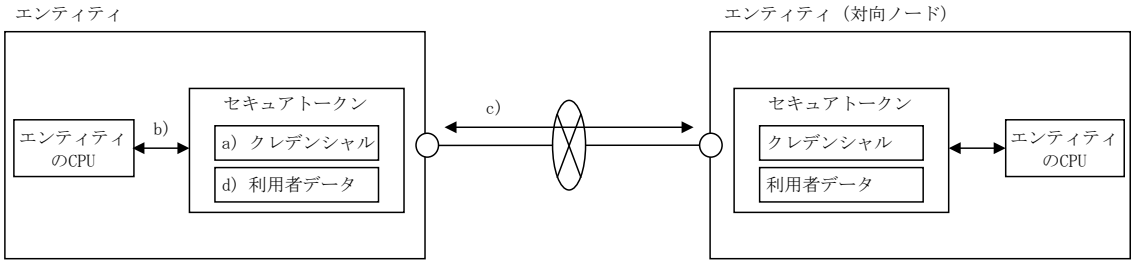

図 7-2 通常利用時のイメージ図（ノード認証）

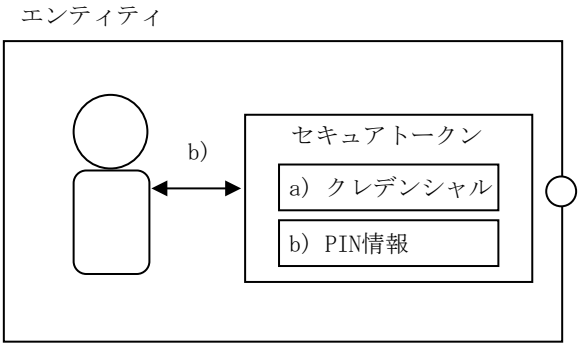

図 7-3 通常利用時のイメージ図（セキュアトークンの所有者認証）

7.2.3 ライフサイクル管理時に要求される機能

a) クレデンシャル保管機能：「Mandatory」

エンティティ（機器、組織等）の正当性を保証するためのクレデンシャル（電子証明書）を安全に（耐タンパー性＋(必要に応じて)アクセス制御機能）保管する。

b) セキュアトークンとエンティティ間の認証機能：「Mandatory」

セキュアトークン及び装着されているエンティティがお互いに相手が正当であることを確認する。エンティティが機器の場合は、エンティティ及びセキュアトークンはお互いに正当な相手が保有しているべき暗

号鍵を相手側が保有していることを、メッセージのやり取りによって確認する。
エンティティが自然人の場合は、認証方法として PIN 認証が想定される。
セキュアトークン内のデータの読み出し、書込み、演算等の前に実行する。

c) 発行サーバの認証機能：「Mandatory」
クレデンシャルの書込み・更新及び、セキュアトークン内のアプリケーションの更新サービスを提供する発行サーバを認証する。認証方法としては、b) と同様の方法で行ってもよい。

d) クレデンシャルの書込み・更新機能：「Mandatory」
クレデンシャルを書込み・更新する。オフラインで書込み・更新を行う場合は、エンティティを PC などの情報処理端末に接続して行う方法と、エンティティから取出したセキュアトークンを情報処理端末に接続する方法が想定される（図 7-4）。

e) 鍵生成機能：「Optional」
クレデンシャルの書込み・更新する際に、トークン内にてクレデンシャルを構成する鍵ペア(公開鍵及び、秘密鍵)を生成する。

f) リモート書込み・更新機能：「Conditional」
厳密な安全性の確保されていない環境でクレデンシャルを書込み・更新する場合に必須となる。IC カードにおけるセキュアメッセージングのように、外部とセキュアトークンの間の通信の安全性を保障する機能を提供する。（図 7-5）。

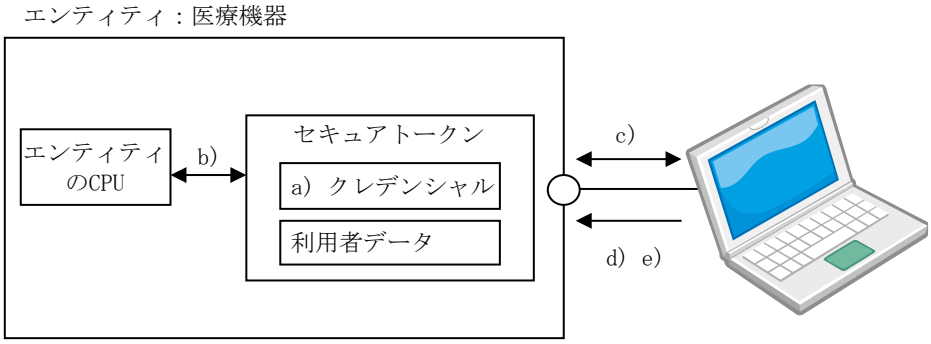

図 7-4　オフラインによるライフサイクル管理時のイメージ図

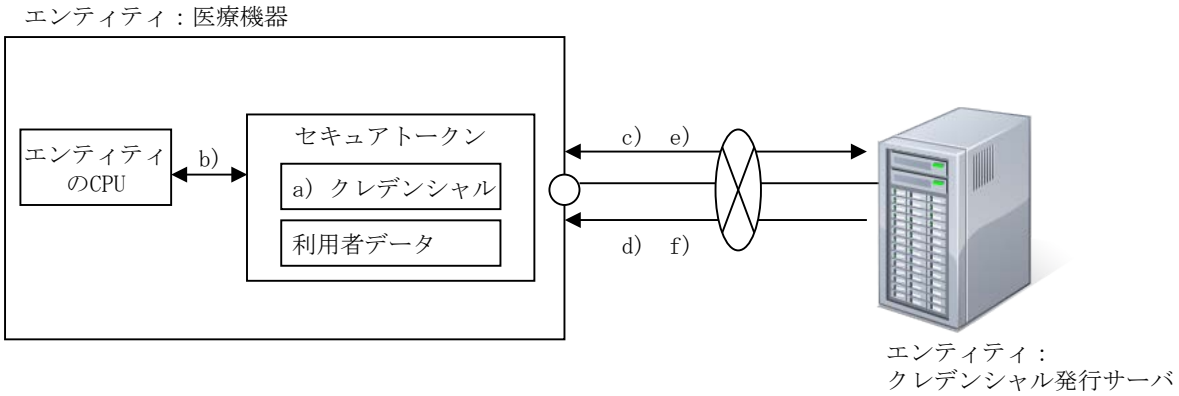

図 7-5 インターネット経由によるライフサイクル管理時のイメージ図

7.3 セキュアトークンの運用

組織認証を行うノードを構成する要素は、組織を識別・認証するためのクレデンシャル、クレデンシャルを安全に格納するトークン、そして実際の通信を行うノード（機器）である。クレデンシャルを発行及び更新する際には発行されたクレデンシャルをトークンに格納することになるが、その際には厳密な安全性が確

保された環境で行われる必要がある。

実際の運用では、クレデンシャル、トークン及びノードのライフサイクルが異なっているので、運用に際しては注意が必要である。図 7-6 に典型的なライフサイクルの例を示す。

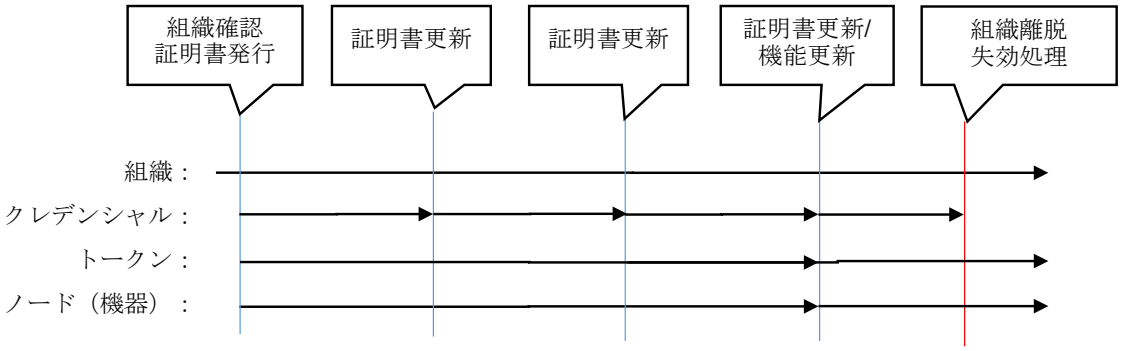

図 7-6　組織認証に関連するライフサイクルモデル(1)：正常系

組織は申請によってクレデンシャルの発行を受け、クレデンシャルをノードとなる機器（GW 等のネットワーク機器）内のトークンに格納し、利用する。トークンが製造された際には組織のクレデンシャルは発行されていないため、機器を医療機関等に設置する際にトークン内にクレデンシャルを格納する必要がある。証明書の有効期限が来ると、再発行を受け、トークンに格納して継続運用する。そのため、トークンにはクレデンシャルを更新する機能が求められる。ノードとなる機器も耐用年数があるので、一定期間で新しい機器に入れ替える。組織がトラストゾーンから離脱する場合には、クレデンシャルが失効する。

次に、ノードを構成する機器（ネットワーク機器）にトークンが埋め込まれている場合で、ノードを構成する設備に障害等が発生した場合を想定したライフサイクルを図 7-7 に示す。

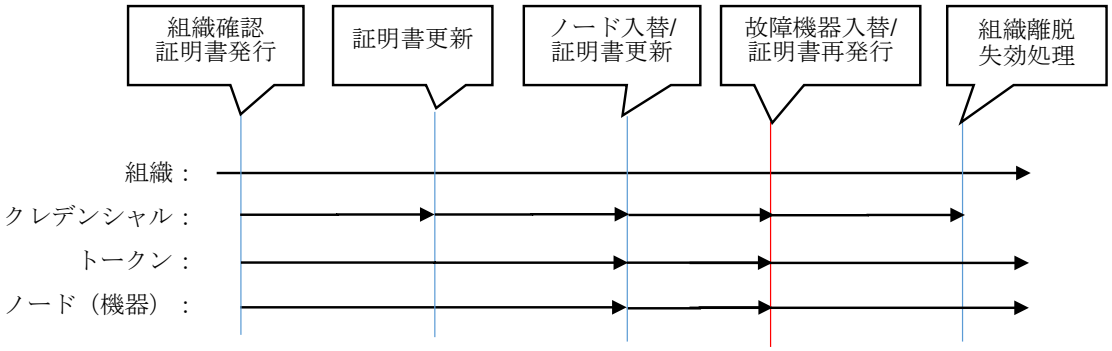

図 7-7　組織認証に関連するライフサイクルモデル(2)：　機器埋め込み型トークン

組織は申請によってクレデンシャルの発行を受け、クレデンシャルをノードとなる機器（GW のネットワーク機器）内のトークンに格納し、利用する。トークンが製造された際には組織のクレデンシャルは発行されていないため、機器を医療機関等に設置する際にトークン内にクレデンシャルを格納する必要がある。証明書の有効期限が来ると、再発行を受け、トークンに格納して継続運用する。そのため、トークンにはクレデンシャルをアップデートする機能が求められる。ノードの設備も耐用年数があるので、一定期間で新しい設備に入れ替える。組織がトラストゾーンから離脱する場合には、クレデンシャルが失効する。

次に、トークンとして取り外しが可能なものを用いた場合に、ノードを構成する設備及びトークンに障害が発生した場合を想定したライフサイクルを図 7-8 に示す。

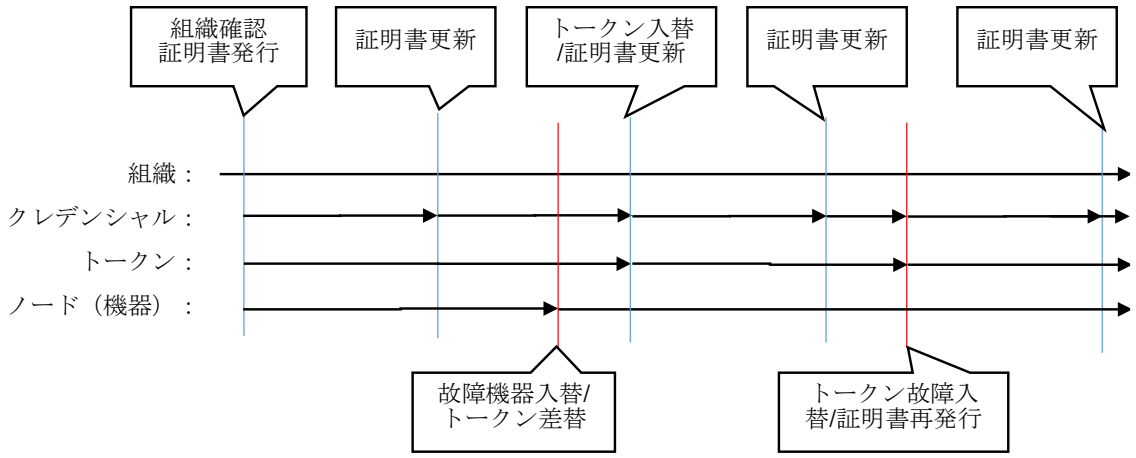

図 7-8　組織認証に関連するライフサイクルモデル(3)：取り外し型・異常系

組織は申請によってクレデンシャルの発行を受け、クレデンシャルをノードとなる機器（GW 等のネットワーク機器）内のトークンに格納し、利用する。証明書の有効期限が来ると、再発行を受け、トークンに格納して継続運用する。ノードの機器が故障すると、新しい設備にトークンを差替えて運用を再開する。トークンが故障した場合は、クレデンシャルは取り出すことができないので、トークンを入れ替えるとともに、クレデンシャルの再発行を受け、運用を再開する。

システム全体の可用性を重視するのであれば、ノードが使用不能となる時間が少なくなる取り外し型トークンが好ましい。ただし、その場合には何らかの物理的安全性の確保等の対策が必要となる。

ISO/IEC 19790 では、マルチチップスタンドアロン型暗号モジュールのキュリティレベル２の場合の物理的セキュリティは、次のように定められている。

1) 金属製又は硬いプラスチック製の製品グレードの囲い内に完全に含まれていなければならない。これらは、ドア又は除去可能なカバーを含んでもよい。（レベル１）
2) 暗号モジュールの囲いは、可視光領域内において不透明でなければならない。（レベル２）
3) 暗号モジュールの囲いが、ドア又は除去可能なカバーを含む場合には、ドア又はカバーは、物理的若しくは論理的な鍵を用いたこじ開け耐性のある機械的錠が掛けられているか、そのドア又はカバーはタンパー証跡を残すシール（例えば証跡性テープ又はホログラムシール）で保護されていなければならない。（レベル２）

以上を参考にすると、医療機関等に設置された機器に取り外し型トークンを適応した場合には、例えば次の対策が必要となる。

a) 機器の鍵が掛かるラック等への設置
b) 開閉の記録管理及び不正な開閉が分かる仕組みの導入
c) 管理者及び操作者の適切な教育及び運用の徹底

このような対策の実施が難しい場合には、機器埋め込み型を選択する必要がある。

8　相互運用性確保の要件

8.1 相互運用性

7.2 で示したように、セキュアトークンには、通常利用（ノードの識別及び認証を行う利用）及び、ライフサイクル管理時(証明書等のクレデンシャルの更新を行う利用)の利用が存在する。また、差替え可能なトークンを利用した場合には、トークンを次の機器に差し替えたり、別のトークンに変更したりする可能性がある。他方、対象となる組織は、規模も想定されるノードに対する負荷も様々であり、組織の入り口となる機器を特定の機器に限定することは難しい。そのため、ノードとして利用する機器でセキュアトークンを利用する際には、トークン及びノード（機器）によらない共通の仕様を定めて相互運用を図ることが必要となる。

a)　通常利用時における仕様

7.2.2 で示したクレデンシャル保管機能、認証機能、署名生成機能、利用者データ保管機能の 4 つの機能に対して、相互運用性の確保が必要となる。特にトークンが取り外し型の場合には、図 8-1 に示すとおり、ノード内からトークンへのアクセスを実現するトークンドライバがインタフェースレベルで互換性をもつ必要がある。これによって、ノードを構成する機器が入れ替わった場合、及びセキュアトークンが入れ替わった場合でも、通信アプリケーションから共通のインタフェースを通じてセキュアトークン内のクレデンシャルを利用することができる。

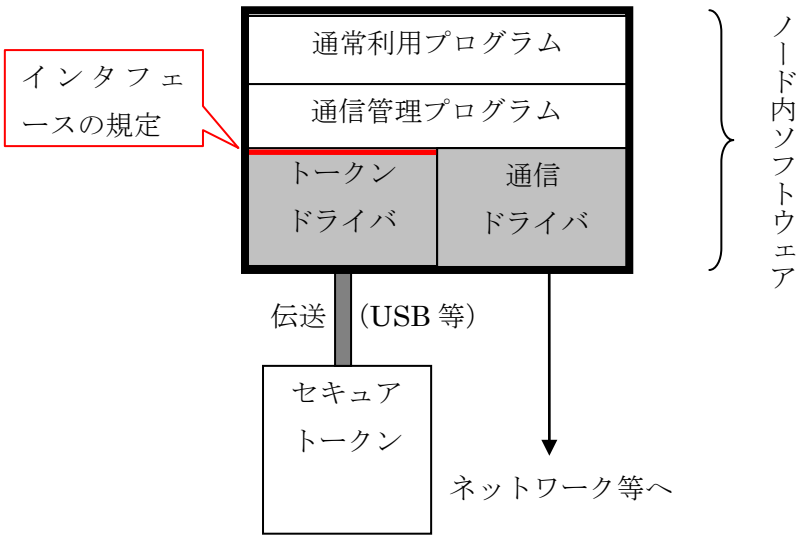

図 8-1　ノード内のソフトウェア構成

図 8-2 にノードを構成する機器が入れ替わった場合のトークンの利用の概念を示す。旧ノードに挿入されていたトークンは、新ノードに導入されて利用される。新ノード内の通信制御プログラムは、相互運用が確保されたトークンドライバのインタフェースを通じてセキュアトークン内のクレデンシャルにアクセスする

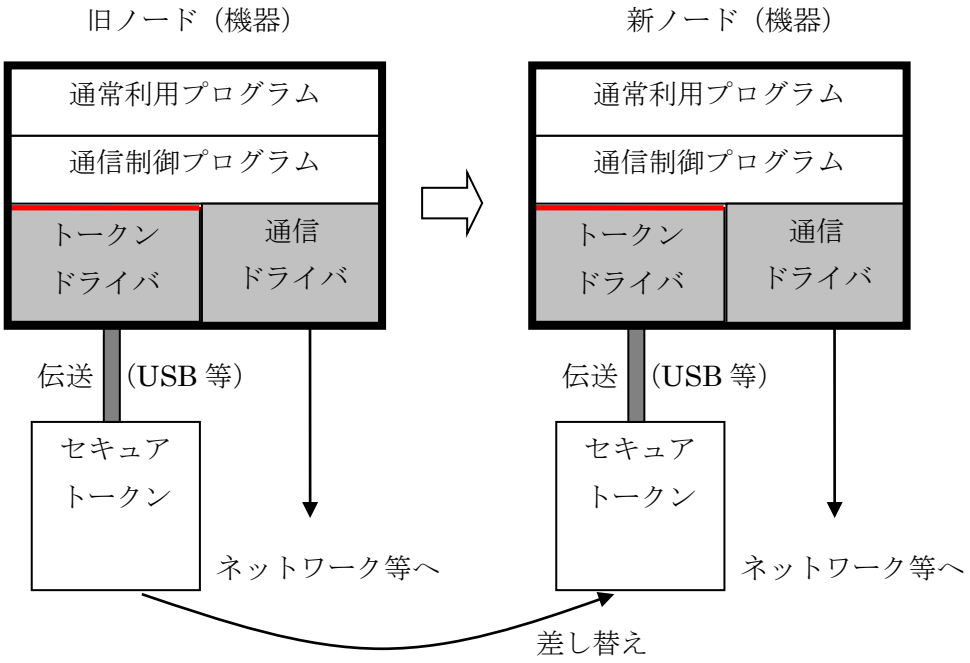

図 8-2　ノード(機器)を交換した際のトークンの利用

b)　ライフサイクル管理における仕様

7.2.3 で示したクレデンシャル保管機能、認証機能、発行サーバ認証機能、クレデンシャル書き込み・更新機能、鍵生成機能、リモート書込み・更新機能の 6 つの機能に対して、相互運用性の確保が必要となる。CA（クレデンシャル発行組織）が発行したクレデンシャルをノード内のクレデンシャル管理アプリケーションプログラムが受け取り、トークンに対して処理を依頼する。そのため、ノードを構成する機器及びトークンが交換されることを前提にすると、トークンに対するインタフェースだけでなく、CA からクレデンシャルを受け取るためのプロトコル及びフォーマット等のインタフェース仕様にも相互運用性が必要となる。図 8-3 にその概念を示す。機器埋め込み型のトークンの場合にも、クレデンシャル管理のためのインタフェースの相互運用性確保が必要となる。クレデンシャルは、IA から直接ノードに設定される場合と、施設の管理者が IA からクレデンシャルを受け取り設定する場合が考えられる。

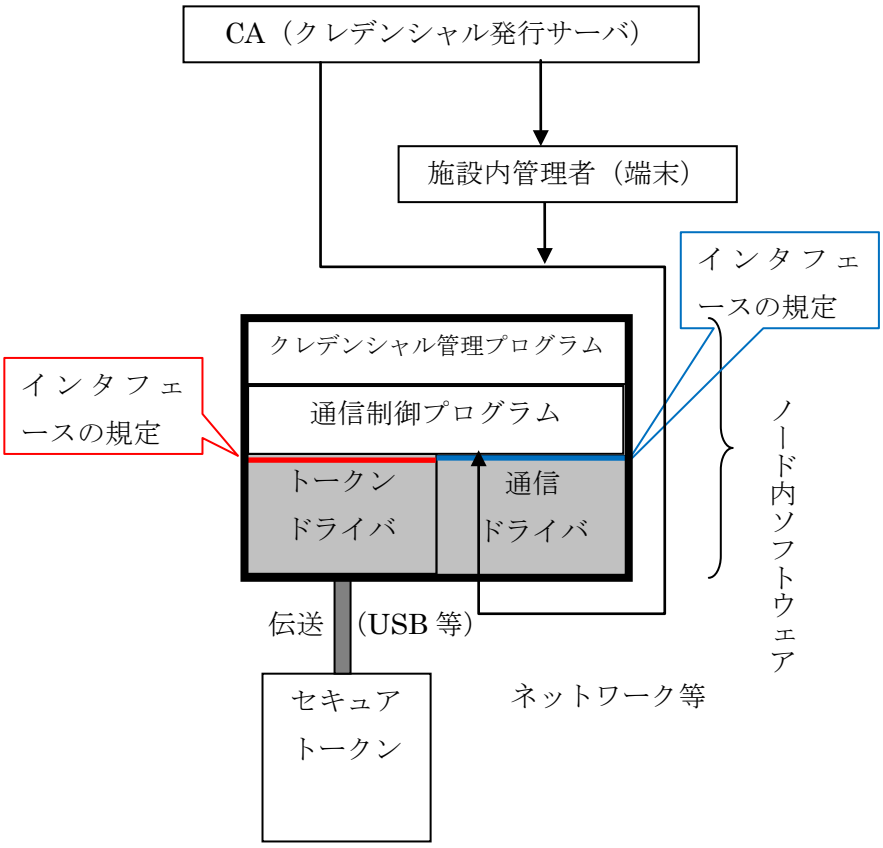

図 8-3　クレデンシャルの管理

トークンを共通利用するためインタフェースの互換性確保の仕様の一例としては、JAHIS 標準「HPKI 対応 IC カードガイドライン」がある。しかしながら、本ドキュメントの検討時点で対象とする医療機関等・設備等のノード認証を行うための詳細な仕様を定めるのは難しいため、8.2 節においては、ノード内でセキュアトークンを利用する際に必要となる機能に対応したインタフェースを列挙することとする。[2]

8.2 インタフェース要件

8.2.1　概要

IHE ITI-ATNA（TF-19）において、公衆回線及びインターネット回線を利用するトラステッド・ドメインを含まないノード間通信では、TLS を利用することが要求されている。TLS は、暗号化通信プロトコルであり、通信開始時に接続元と接続先の各ノードで相互に相手をクレデンシャル（証明書）によって識別して、信頼性を確認することが必須となる。そのために、先ずクレデンシャルである証明書のライフサイクルを整理したうえで、セキュアトークンでサポートすべき機能概要及びインタフェース要件を示す。

なお、セキュアトークンと上位装置間で利用する暗号化通信プロトコルとしてセキュアメッセージングがあるが、本ガイドではノード間通信におけるインタフェース要件となることから対象外とした。

[2] 将来本ドキュメントを改定する際には、必要となる具体的な仕様を記述する予定である。

8.2.2 証明書のライフサイクル

セキュアトークンのライフサイクルは格納媒体によって異なるため、クレデンシャルとなる証明書のライフサイクルを次に示す。

① 証明書の発行
鍵ペア及び証明書を生成してセキュアトークンへの書き込みまでのフェーズ

② 証明書の利用
利用者が発行された証明書を用いて PKI サービスを利用するフェーズ

③ 証明書の失効
紛失又は破損などの理由で証明書を失効させ、証明書失効リスト（CRL）を発行し、利用を中止するフェーズ

④ 証明書の更新
セキュアトークンを有効期限切れ後も引き続き利用するために、証明書の有効期限満了前に、発行サーバへアクセスして証明書を更新するフェーズ

8.2.3 セキュアトークンの機能概要

7.2 に示したセキュアトークンを利用するために必要な機能概要を Mandatory（必須）、Conditional（条件付き）、Optional（任意）に分け次に示す。

a) 通常利用時に要求される機能（8.2.2 ②）
書類への電子署名及び TLS 認証においての利用

「Mandatory」	・クレデンシャル保管機能（7.2.2 a)）
	・セキュアトークンとエンティティ間の認証機能(7.2.2 b))
「Conditional」	・秘密鍵を用いた署名生成機能（7.2.2 c)）
「Optional」	・利用者データ保管機能（7.2.2 d)）

b) ライフサイクル管理時に要求される機能（8.2.2 ①及び④）
鍵ペア及び証明書の生成、及び証明書の有効期限内更新においての利用

「Mandatory」	・クレデンシャル保管機能（7.2.3 a)）
	・セキュアトークンとエンティティ間の認証機能（7.2.3 b)）
	・発行サーバとの認証機能（7.2.3 c)）
	・クレデンシャルの書込み・更新機能（7.2.3 d)）
「Conditional」	・リモート書込み・更新機能（7.2.3 f)）
「Optional」	・鍵生成機能（7.2.3 e)）

8.2.4 インタフェースの例

クライアント側のソフトウェアは、PKI アプリケーション層、ミドルウェア層、トークンへのドライバ層に分かれる。本ガイドでは、HPKI に特化しない汎用的な PKI 機能を提供するミドルウェアとして、CryptoAPI インタフェース及び PKCS#11 インタフェースの2種類のインタフェースについて例を示す。IC カードで実現した場合の具体例は、HPKI 対応 IC カードガイドラインを参照のこと。

a) CryptoAPI インタフェース
セキュアトークンに求められる API 概要は、表 8-1、表 8-2 及び表 8-3 のとおりとなる。なお、詳細（戻り値、構造体等）は、CryptoAPI の仕様を参照のこと。

表 8-1 CryptoAPI で要求されるインタフェース(1) 「Mandatory」

No	API 名	概要
1	CryptAcquireContext	指定されたコンテナに対する鍵ハンドルを取得する
2	CryptCreateHash	ハッシュオブジェクトを生成する
3	CryptDecrypt	データの復号を行う
4	CryptDeriveKey	ハッシュデータを使ってセッション鍵を生成する
5	CryptDestroyKey	鍵オブジェクトを破棄する
6	CryptEncrypt	データを暗号化する
7	CryptGenRandom	乱数を生成する
8	CryptGetHashParam	ハッシュオブジェクトのパラメータを取得する
9	CryptGetKeyParam	鍵オブジェクトのパラメータを取得する
10	CryptGetProvParam	プロバイダーオブジェクトのパラメータを取得する
11	CryptGetUserKey	不揮発な鍵ペアのハンドルを取得する
12	CryptHashData	ハッシュオブジェクトにデータをセットする
13	CryptHashSessionKey	ハッシュオブジェクトに鍵をセットする
14	CryptImportKey	鍵をインポートする
15	CryptReleaseContext	CryptAquireContext で生成したコンテキストを破棄する
16	CryptSetProvParam	プロバイダーオブジェクトにパラメータをセット
17	CryptVerifySignature	デジタル署名データの検証を行う

表 8-2 CryptoAPI で要求されるインタフェース(2) 「Conditional」

No	API 名	概要
1	CryptDestroyHash	ハッシュオブジェクトを破棄する
2	CryptSetKeyParam	鍵オブジェクトにパラメータをセット する
3	CryptSetHashParam	ハッシュオブジェクトにパラメータをセット する
4	CryptSignHash	ハッシュオブジェクトにデジタル署名する

表 8-3 CryptoAPI で要求されるインタフェース(3)「Optional」

No	API 名	概要
1	CryptGenKey	鍵を生成する

b) PKCS#11 インタフェース

セキュアトークンに求められる API 概要は表 8-4、表 8-5 及び表 8-6 のとおりとなる。なお、詳細(戻り値、構造体等)は、PKCS#11 の仕様を参照のこと。

また、「Conditional」と「Optional」は、「Mandatory」との差分として記載する。

表 8-4 PKCS#11 で要求されるインタフェース(1)「Mandatory」

No	API 名	概要
1	C_GetFunctionList	関数ポインタリストを取得する
2	C_Initialize	PKCS#11 ライブラリを初期化する
3	C_Finalize	PKCS#11 ライブラリを終了する
4	C_GetInfo	ライブラリ情報を取得する
5	C_GetSlotList	スロットリストを取得する
6	C_GetSlotInfo	スロット情報を取得する
7	C_GetTokenInfo	トークン情報を取得する

8	C_WaitForSlotEvent	スロットのイベント(トークンの挿抜など)の発生を待つ
9	C_GetMechanismList	サポートメカニズム（アルゴリズム）を取得する
10	C_GetMechanismInfo	メカニズム（アルゴリズム）情報を返す
11	C_OpenSession	メカニズム（アルゴリズム）情報を返す
12	C_CloseSession	セッションを切断する
13	C_GetSessionInfo	セッション状態を取得する
14	C_Login	トークンをログイン状態にする
15	C_Logout	トークンをログアウト状態にする
16	C_CreateObject	新規オブジェクトの生成を行う
17	C_GetObjectSize	オブジェクトサイズをバイト単位で取得する
18	C_FindObjectsInit	オブジェクトの検索を開始する
19	C_FindObjects	オブジェクトの検索を行う
20	C_FindObjectsFinal	オブジェクトの検索を終了する
21	C_GetAttributeValue	オブジェクトの属性値を取得する
22	C_SetAttributeValue	オブジェクトの属性値を変更する
23	C_EncryptInit	暗号処理の初期設定を行う
24	C_Encrypt	単数ブロックの暗号化を行う
25	C_EncryptFinal	複数ブロックの暗号化を終了する
26	C_VerifyInit	検証処理の初期設定を行う
27	C_Verify	単数ブロックの署名検証を行う
28	C_VerifyFinal	複数ブロックの署名検証を終了する
29	C_Decrypt	データの復号を行う

表 8-5 PKCS#11 で要求されるインタフェース(2)「Conditional」

No	API 名	概要
1	C_DigestInit	メッセージダイジェスト化処理の初初期化を行う
2	C_DigestUpdate	複数ブロックのメッセージダイジェスト化を継続する
3	C_DigestFinal	複数ブロックのメッセージダイジェスト化を終了する
4	C_SignInit	署名処理を初期化する
5	C_Sign	データに署名を行う

表 8-6 PKCS#11 で要求されるインタフェース(3)「Optional」

No	API 名	概要
1	C_GenerateKeyPair	公開鍵・プライベート鍵の鍵ペアを生成する

9 付録：作成者名簿

作成者（社名五十音順）

下野　兼揮	㈱グッドマン
松本　泰	セコム㈱
半田　富己男	大日本印刷㈱
浅野　之治	凸版印刷㈱
遠藤　方洋	凸版印刷㈱
平田　泰三	(一社)日本画像医療システム工業会(ＪＩＲＡ)
小出　一希	日本光電工業㈱
藤咲　喜丈	日本光電工業㈱
別府　嗣信	日本光電工業㈱
梶山　孝治	㈱日立製作所
山岡　弘明	富士通㈱
喜多　紘一	(一社)保健医療福祉情報安全管理適合性評価協会(HISPRO)
茗原　秀幸	三菱電機㈱
太田　英憲	三菱電機インフォメーションシステムズ㈱
酒巻　一紀	三菱電機インフォメーションシステムズ㈱
清水　可奈子	三菱電機インフォメーションシステムズ㈱
谷内田　益義	㈱リコー

改定履歴		
日付	バージョン	内容
2015/02/10	Ver. 1.0	初版
2017/6/14	Ver. 1.1	機器認証編が発行されるのに合わせたタイトルの変更と整合性確保、及び引用規格・引用文献の更新

（ＪＡＨＩＳ技術文書　17－１０５）
２０１７年6月発行

ＪＡＨＩＳ　セキュアトークン実装ガイド・ノード認証編　Ver.1.1

発行元　一般社団法人　保健医療福祉情報システム工業会
〒１０５－０００４　東京都港区新橋２丁目５番５号
（新橋２丁目ＭＴビル５階）

電話　03-3506-8010　　FAX　03-3506-8070