NEMA，COCIR，JIRA による承認のレビュー

マシン認証証明書の管理

この文書は
NEMA-MITA／COCIR／JIRA セキュリティ及びプライバシー合同委員会（SPC）
によって作成されたものである。

この文書は MITA (Medical Imaging & Technology Alliance, a Division of NEMA)-USA,
COCIR（欧州放射線・医療電子機器産業連合会），
JIRA（日本画像医療システム工業会）の承認を受けている。

2007 年 5 月

Secretariat: NEMA (National Electrical Manufacturers Association) www.nema.org
1300 North 17th Street, Suite 1847, Rosslyn, VA 22209 USA tel: 703-841-3200 fax: 703-841-5900
Secretary: Stephen Vastagh tel:703-841-3281 fax:703-841-3381 E-mailto:ste_vastagh@nema.org

NEMA，COCIR，JIRA による承認のレビュー

1. 概要／序文

この文書は、医療提供者と医療機器製造組織がマシン間の通信を安全にするためにデジタル証明を使う方法を決めるのを助けます。

医療ではプライバシー及びセキュリティが注目されている。過去５年以上の間のセキュリティの違反は、内部のセキュリティなしでファイアウォールの“堀”アプローチを使うことが効果的でないことを示しました。ネットワーク環境の適切な安全確保には，機密データの受信又は送信を行うマシン（例えば、画像機器、PACS アーカイブ、ラップトップ、IHE プロファイルを実装しているシステム、インターネット・キオスク）の識別が必要である。このため，マシン識別及び個人識別の両方を認証する必要性が生じる。マシン識別の管理がこの文書の焦点である。

米国（HIPAA），欧州（電子通信プライバシー指令），日本（個人情報保護法）などのデータ保護規制は，病院情報ネットワークの保護を要求している。ひとつの方法として，厳密なネットワーク分離によるセキュリティの採用がある。医療専門家は医薬品情報などイントラネット／インターネット設備にアクセスする必要があるため，これは実用的ではない。マシン及び個人の認証は実用的な解決法である。個人認証に関する問題は，公開鍵暗号基盤（PKI）のようなテーマで，他所で広く議論されている。

医療で用いられる主な通信基準（DICOM，HL7，IPSEC，TLS 及び HTTPS）はすべて，私有鍵及び公開証明書を用いたマシン認証方法を定めている。IPSEC，TLS 及び HTTPS は医療以外の場でも広く用いられている。インテグレーティング ヘルスケア エンタープライズ（IHE）統合プロファイルの“監査証跡とノード認証（ATNA）”は，これらの基準及び他の基準が安全な医療ネットワークの一部としてどのように用いられるべきかについて，その技術的詳細を述べている。商業基準及び医療基準はすべて，様々な PKI インフラシステムとの併用が可能な認証メカニズムに基づく証明書を用いている。

既にマシン認証インフラを整備した施設，又は別の方法をとることでベンダーと合意した施設もあるかもしれない。そのような場合には，この文書及びガイドラインは適用されない。そのような施設は自身のインフラによって定義済みの手順及び管理要件に従わなければならない。

この文書は、医療システムの異なる構成要素の間で規定を決めることや確立されなくてはいけない信用関係などのはるかに大きい問題は議論しません。それらは、ローカルな規制強制、操作上の関係、専門家の関係などを含みます。マシン認証は、それらのポリシー決定を適切に管理して実施するためのポリシー実施メカニズムの共通構成要素です。使っているマシン認証は、適当なポリシーを確立するための代用品ではありません、それは、ポリシーを実施するのを助けるメカニズムです。

この文書のガイドラインは，マシン認証に PKI インフラを用いることに決めた施設及びベンダーを対象としている。この文書は実装仕様を提供しません。人のための PKI イン

フラを備え，それをマシンにも適用できるよう拡張したいと考えている施設には，この文書が役立つかもしれない。この文書はマシン認証及び関連インフラに関するガイドラインを提供する。これらのガイドラインに従えば，ベンダー及び顧客は取得，開発及び運営にかかる費用を削減することができるだろう。

人の認証メカニズムには，マシンでは発生しない法律，プライバシー，認定，雇用，解雇，任務／職務及び許可に関する複雑な問題がたくさんある。マシンの管理は IT 組織内で処理することができ，人的組織を必要としない。マシンには在庫，サービス及び修理の問題があるが，これらは IT 組織内で管理することができる。

これらのマシン認証に関するガイドラインは，多くのセキュリティ文献に見られる PKI 管理提言より簡素であるが，これはマシン認証の管理は個人認証よりはるかに簡素であるからである。

証明書によるマシン認証を用いる場合，医療提供者は以下を行わなければならない。

- *IT 管理組織の一部としての認証権限部門の提供。鍵及び証明書付きのマシンの提供を単純にベンダーに依存することはできない。このネットワークインフラは第三者契約による提供が可能である。*
- *後述の認証方法のうちどれを使用するかの決定。*
- *選択した方法に必要な，証明書失効リスト（CRL）サーバなど他のサーバ及びサービスの設置及び維持。*

マシン供給者（ベンダー）は以下を用意しなければならない。

- *後述の方法で通信を認証できるようにすること。*
- *それらマシンのローカル私有鍵の維持手段の提供。*
- *安全な通信を必要とする全アプリケーションに必要な，アプリケーション及び管理インターフェースの提供。*

2. シナリオ

医療環境では，関係者の認証とは独立して通信するマシンの認証が必要なことが多い。以下のシナリオは，一般的な医療ワークフローにおいて，セキュリティを強化するためにマシン認証が行われなければならない場合を示す。

2.1 職員が配置されたマシン

マシン認証としては，職員が配置されたマシンのユーザ認証では不十分である。マシンは機密データの送信又は受信の前に認証されなければならない。例えば，認証されたユーザはインターネットカフェのコンピュータを使っているかもしれない。公共のコンピュータはアクセスを拒否されるだろう。これは個人認証とは無関係である。ユーザ認証

は，そのユーザの動作に関連するアクセス制御及び監査証跡のために必要である（他の文書で扱われる）。

2.1.1 画像作成モダリティ

職員が配置されたマシンの典型的なものは，例えば、血管造影システムなどの画像作成モダリティである。しばしば、マシンオペレータの認証が行われます、しかし外科チームは休んでいません。以下のようなときに双方向的なマシン認証が必要である：

- ユーザ認証は、いくつかの状況には適しません。例えば、血管造影システムが PACS に送信しなければならない検査を所有している場合，正しい PACS への送信を保証するために PACS システムの認証が必要である。ユーザ認証は、この場合適当な認証ではありません。
- マシンが患者情報を取得するためにワークリストに問い合わせを行う場合，HIS／RIS システムはこの問い合わせに対する回答がなされるべきかどうか知る必要がある。患者のスケジュール情報は病院のどのマシンにも送信されるのではなく，認可されたマシンにのみ送信されなければならない。
- 自動セキュリティシステムは，産科ナースステーションからの血管造影スケジュールの問い合わせなど例外的なワークリストへの問い合わせには記録し警告を与え，血管造影からの血管造影スケジュールの問い合わせなど通常の問い合わせには警告を与えない。同様に，血管造影システムはそれが HIS システムに到着し，なりすましなど認可されていないマシンには到着しなかったことの保証を必要とする。
- 血管造影システムが終了済みの検査を送信してワークリストの状態を更新する場合も，やはり個人よりマシンの識別のほうが重要である。上述のように，セキュリティシステムは信頼できる血管造影システム以外から送信された血管造影結果を保存しようとすると，警告を与える。

マシン認証メカニズムはこれらの問題を解決する。

2.1.2 放射線医のワークステーション

私たちの例では，CT 結果を読影する放射線医は個人として認証及び許可される。マシンはそれとは関係なく認証される。放射線医が正しく識別され，マシンがデータの受信を許可されてそれを保護すれば，CT 結果の閲覧を続行することができる。放射線医師が到着し、ログインする前に、マシン認証は、放射線医師のワークステーション上へ検査の安全なプリロードすることを許します。

2.1.3 病院 LAN に直接アクセスするサービスラップトップ

サービスラップトップ周辺のセキュリティ問題は，ラップトップのマシン認証の範囲を超える。それは、ベンダーと医療提供者とその他の間の複雑な委託契約によります。この文書はこの状況に関連して生じる他の問題は一切扱わない。ここで述べるマシン通信認証はその解決法の一部となるだろう。

NEMA，COCIR，JIRA による承認のレビュー

2.2 サーバへのアクセス

私たちの例では，医師は患者の情報を得るためにブラウザを用いてウェブサーバにアクセスする。ユーザは適切に識別，認証及び許可されると仮定する。医師は正しいウェブサーバに接続し，それが認証されたことを保証しなければならない。サーバが医師のマシンを認証できるように，あまり用いられないメカニズムがある。

ウェブサーバ，ブラウザ及び PC はローカルマシンのクライアント証明書を用いるように設定されなければならない。これに関する指示は個々の製品の付属文書に記載されている。

「単に見るだけ」のブラウザの使用はマシン認証は必要ないという、一般的な誤解があります。これは、通信を傍受するマルウェア(例えば画面収集とキーボード・ロガー)の脅威を無視しています。ブラウザは、完全に消去されていないキャッシュページを維持し、また個人情報をさらします。これは、SSL または VPN 技術で通信を保護したかどうかにかかわらず真実です。The machine authentication information can be used to identify whether the connection is from a machine that is known to be taking all of the extra steps needed to protect privacy.

It can also be used to ensure that unknown machines are treated differently. There may be good reasons to permit limited access from public access kiosks. The machine authentication can be used to enable granting limited access to authorized staff from such machines. The limited access can be designed with the assumption that these unknown machines are likely to have malware or maintain caches that will expose the information that is delivered.

2.3 自律マシン

医療では多くの種類の自立マシンを使用します。コンピュータ診断支援と携帯型患者モニタのような計測システムはどちらも分析的なシステムです。例えば、携帯型患者モニタが患者の様々な健康測定を自動的に行い，アラームを発し，さらに他のシステムからの指示を受信する。医療提供者が同席していることもあるが，システムは職員が同席していなくても作動しなければならない。

モニタが病院記録保管庫にデータを送信すると，保管庫はどのモニタがデータを送信しているのかを明確に認識しなければならず，モニタは正しい保管庫にデータを送信していることを認識しなければならない。これは安全の重要性に関わるセキュリティ問題である。識別を誤ると，警報又はレポートの表示の誤り，又は間違った場所に送信されればデータの損失を招く恐れがある。

また，携帯型患者モニタは移動し，移動中も十分に作動することができる。そのため，モニタがローカルネットワーク間を移動できる場合は，ネットワークアドレスの使用という単純な管理上の解決法ではうまくいかないか，又は非常に手間がかかってエラーが発生しやすくなる。モニタ認証は移動性の動作を許可しなければならないが，多大な管理労力を要求してはならない。マシン認証はこれらの問題を解決する。

NEMA，COCIR，JIRA による承認のレビュー

2.4 非認証マシン

ルーチンの通信すべてがマシン認証を用いれば，非認証マシンがアクセスしようとしてもすべて拒否され，報告される。これらの中で最も重要な通信は、個人的なデータを運ぶものです。

205 Communications like cafeteria schedules and other public data should be minimized or eliminated from machines that also are used for personal data. These communications might be with unauthorized machines.

3 マシン認証の動作方法

210 医療プロトコルにおいてマシン認証に用いられる方法は，以下を要求する：

- 各マシンの私有鍵／公開鍵のペアの作成

  これらの鍵はマシン内部で作成される場合，又は外部で作成されてマシンに提供されなければならない場合がある。私有鍵はマシン識別の主要な手段であるため，複製又は変更がなされないよう慎重に保護されなければならない。

215 - 公開証明書の配布

  公開証明書は私有鍵とペアになる公開鍵を含む。これらの証明書は自身の有効期限を含み，一定期間ごとに交換されなければならず，他のシステムに公に配布されることができる。公開証明書の所有者は，別のマシンがそれに対応する私有鍵を所有していることを検証することができる。用いられる検証は主に以下の二種類である。

220 - 直接比較（3.1 参照）
  - 信頼できる署名連鎖（3.2 参照）

- 通信チャネルの安全確保

  チャネル設定は私有鍵及び公開鍵を用いるチャレンジレスポンストークンを含む。セッション開始中は TLS，IPSEC，SSL 及び他の安全なトランスポートプロトコル
225 がこれを処理する。医療のデータ交換に利用される高水準プロトコル HTTP、DICOM と HL 7 は、すべて TLS を使用する定義をサポートしています。それらは、使われるサイトのために適当な証明書で形成される必要があります。

3.1 直接比較

この方法はマシン 1 台当たりの通信パートナーが少ないネットワークに適する。このネ
230 ットワークの使用が許可されるマシンすべてに対し，各マシンに事前に公開証明書が与えられる。パートナーを認証するため，マシンは着信した接続情報をそのリスト上の証明書と比較する。

図 1 は直接比較に必要なインストール手順を示す。

1. 私有鍵／公開鍵のペアが作成され，公開証明書が発行される。これは自己署名でも
235 又は CA による署名でもよい。

NEMA，COCIR，JIRA による承認のレビュー

2. 公開証明書が他のマシンに配布される。これは手動配布でも，メディア上でも，又は LDAP 若しくは OCSP などのサービス経由でもよい。配布メカニズムは信頼できるものでなければならない。
3. 他のマシンの公開証明書が新しいマシンにインストールされる。これは手動配布でも，メディア上でも，又は LDAP 若しくは OCSP などのサービス経由でもよい。配布メカニズムは信頼できるものでなければならない。

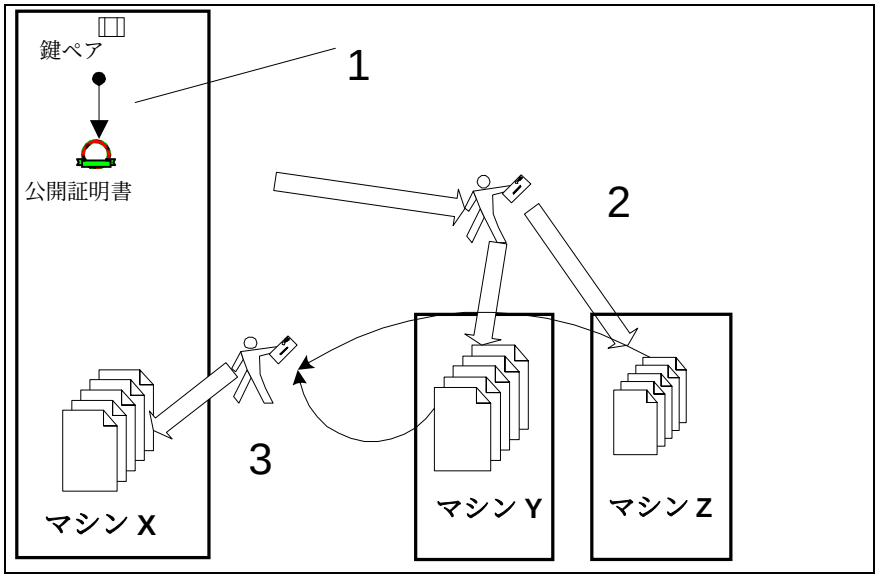

図 1 直接比較のインストールプロセス

マシンが削除された場合，私有鍵が危殆化した場合，証明書の有効期限が切れた場合，及びマシンへの接続が適切でなくなった場合は，それに対応する公開証明書は他のマシンから削除されなければならない。これは失効と同等の直接比較である。

NEMA，COCIR，JIRA による承認のレビュー

図 2 は通信中にマシン認証を確立するときの方法を示す。

1. 発信マシン（マシン X）がその私有鍵からトークンを作成すし、トークンが受信マシンに送信される。
2. 受信マシン（マシン Y）は既知のマシン認証として保存された各公開証明書と比較して，トークンを確認する。
3. 認証されたマシン識別がシステムアクセス制御メカニズムと比較して確認され，接続を続行すべきかどうかが決定される。

発信マシンが受信マシンを認証できるように，このプロセスが反対方向で繰り返される。

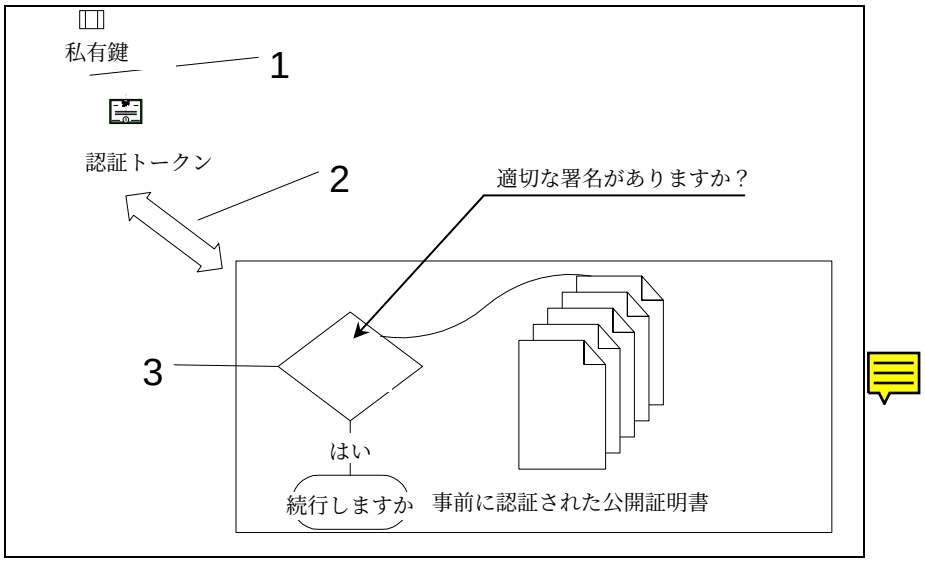

図2 直接比較の認証プロセス

NEMA，COCIR，JIRA による承認のレビュー

3.2 信頼できる署名連鎖の比較

この方法には，認証権限部門（CA）として機能する，つまり IT 管理組織に信頼される第三マシンが関与する。この CA は私有鍵の署名入り公開証明書を作成する。ネットワークの他のシステムは，これらの署名を用いて，これらがネットワーク使用を許可されたマシンの証明書であることを保証する。

図 3 は新しいマシンがインストールされるときの手順を示す。

1. 信頼できる CA の公開証明書が新しいマシンにインストールされる。
2. 新しいマシンは公開鍵／私有鍵のペアを作成する（又は CA に作成してもらう）。
3. 新しいマシンと CA が交信し，新しいマシンが認証に用いる署名入り公開証明書を作成する。
4. この新しい公開証明書は今後の使用のために新しいマシンに返信される。ただし，前述の直接比較とは違って，他のマシンでの動作は必要ない。

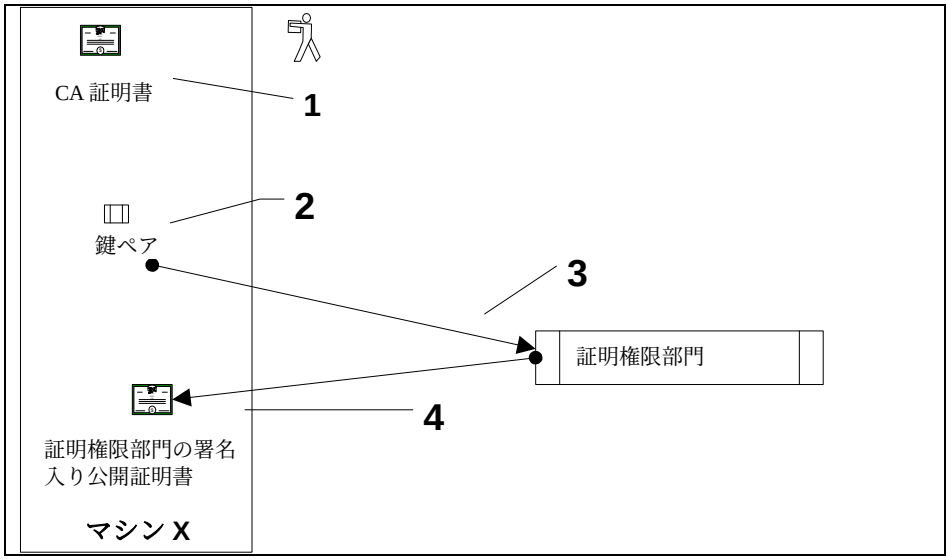

図3 信頼できる署名連鎖のインストールプロセス

マシンが削除された場合，私有鍵が危殆化した場合，証明書の有効期限が切れた場合，及びマシンへの接続が適切でなくなった場合は，それに対応する公開証明書は失効されなければならない。この結果，最終的には失効リストが拡張する。証明書有効期限は、このリストを整理することを許されます、しかし、拡張された期間の間、満了過ぎの取り消された証明書をリストに維持することは、普通です。

NEMA，COCIR，JIRA による承認のレビュー

図 4 は通信中にマシン認証を確立するときの手順を示す。

1. 発信マシンがその私有鍵からトークンを作成する。
2. トークンが受信マシンに送信される。
3. 受信マシンは，トークンが承認済みの認証権限部門に署名された私有鍵によって署名されたかどうかを確認する。
4. 受信マシンは，この個々の公開証明書が失効されたかどうかを確認する。通常これは，一般的に CA によって提供される機能である，失効サーバを用いた確認によって行われる。
5. 認証されたマシン識別がシステムアクセス制御メカニズムと比較して確認され，接続を続行すべきかどうかが決定される。

発信マシンが受信マシンを認証できるように，このプロセスが反対方向で繰り返される。

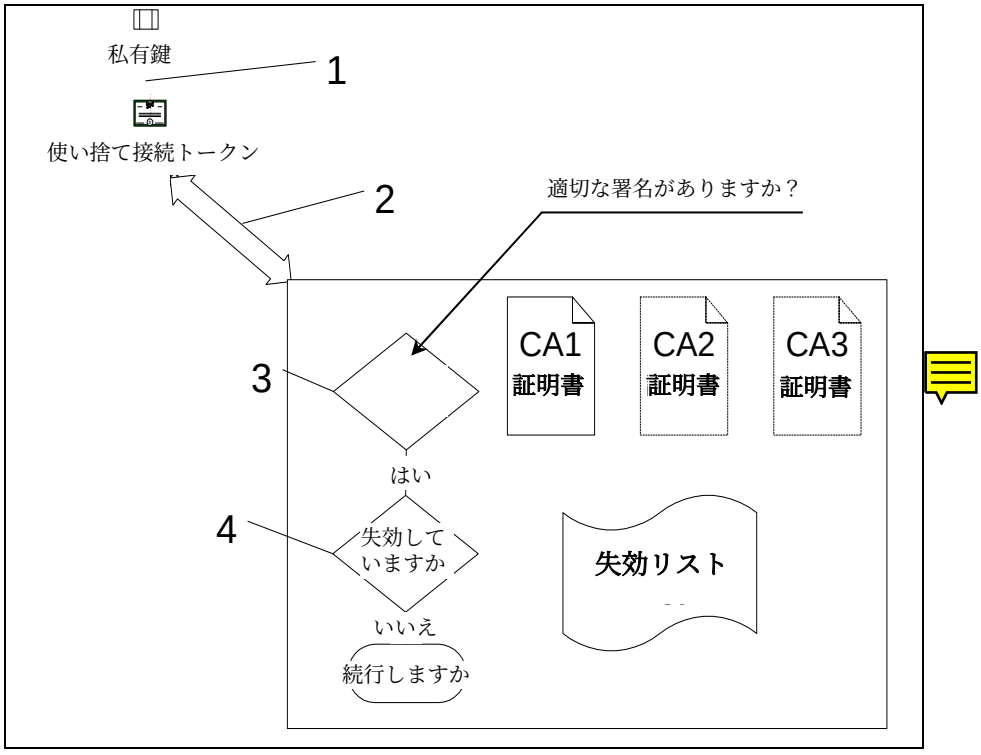

図 4 信頼できる署名連鎖の認証プロセス

3.3 直接比較又は信頼できる署名連鎖の決定

直接比較又は信頼できる署名連鎖比較のどちらを用いるかの決定は，IT 管理組織によってなされるべき重要な選択である。認証の目的ではいずれも等しく有効であり，いずれも医療システムへの適合が可能である。様々な種類のネットワーク設備をインストール

しなければならないか，又は動作を維持するために様々な種類のルーチンの管理労力が要求されるかの兼ね合いである。一般的には，ネットワーク設備が比較的小規模であれば直接比較法を，比較的大規模であれば署名比較法を選択する。しかし，どちらかが望ましくなる単一の規模があるわけではない。そのため，SPC は機器ベンダーが両方の環境の準備をすることを推奨する。

TLS, SSL, and IPSEC all support both approaches, and support a hybrid that combines them. The higher level protocols like HTTP, DICOM, and HL7 that are used for medical data exchange, all have support defined for using TLS. They need to be configured with the appropriate certificates for the sites where they are used.

4 動作の失敗及び継続

認証システムが失敗すると，医療サービスの提供が妨げられる可能性がある。信頼できる署名連鎖を用いた場合，これは CRL サービス，他のサービス又はこれらのサービスを用いたネットワーク通信の障害を含む。手順，障害迂回及びバックアップのメカニズムは，このような失敗が必要なサービスを妨げないように計画されなければならない。

災害の後，災害中に発生した損失から回復するため，緊急の，及び一時的なマシン交換が相次いで起こることがよくある。認証制御の手順及び設備計画はこれを考慮しなければならない。これらのマシンは認証サービスを必要とする。ブレークグラス白書はこれらの問題のいくつかについて論じている（www.nema.org/medical/SPC）。Special care is needed to establish backup and local alternatives to deal with loss of network access during disasters.

直接比較及び信頼できる署名連鎖のどちらを用いるかについては，全システムの災害及び障害の間の動作維持の方法と災害及び障害からの回復方法を考慮したうえで決定しなければならない。

5 Conclusion

The certificate management procedures needed for identifying and authenticating machines are different from those used for people. The software provided for most systems can accommodate both, but the documentation often only covers personnel. The vendors and healthcare providers can meet the needs of machine identification as well.

When using machine authentication by certificates, healthcare providers must:

• decide which of the authentication approaches to use (see section 3 above).

• if using a trusted signature chain approach, provide a certificate authority. They cannot simply depend on their vendors to provide machines with keys and certificates. This network infrastructure can be provided through third party contracts.

• if using direct comparison, obtain certificates for manual installation. This can be from any certificate authority, internal or external.

• establish and maintain the other servers and services, e.g., Certificate Revocation List (CRL) servers, needed for their selected approach.

NEMA，COCIR，JIRA による承認のレビュー

To meet the variety of needs worldwide, the vendors must:

• be able to authenticate communications by the different approaches described above.

• provide a means of maintaining a local private key on those machines.

• provide applications and administrative interfaces necessary for all the applications that need secured communications.

Technical Annex　証明書の使用に関するガイドライン

これらのガイドラインは医療の運営責任とベンダーの製品要求事項を区別し，その両方に対する技術的詳細を提供する。

A.1　組織責任

ローカル手順を確立する場合は，施設の IT 組織及び機器ベンダーの両方がそれに取り組まなければならない。

A.1.1　施設の IT 組織

組織は認証方法を選択しなければならない。この組織は以下を行わなければならない。

a) 方針，手順，サーバ及び選択した認証システムの管理の確立及び維持。Particular care must be taken to ensure that certificate management for authentication purposes is controlled to protect against unauthorized modifications.

b) 認証情報の適切な記録及びバックアップの維持。

c) ローカル証明書失効システムの維持。直接比較では，これは信頼できない証明書を各マシンから削除するための手動プロセスを要求する。信頼できる署名連鎖では，これは失効リストの手動配布又は失効サービス管理のいずれでもよい。

d) 紛失又は危殆化した鍵及び証明書の看護の遅延を最小限にするタイムリーな交換手順の策定。

e) 証明書の有効期限の管理。

1. 医療運営を妨げることがないよう，古い証明書の有効期限が切れる前に新しい証明書が設定されなければならない。
2. 有効期限は 2 年間とすることが推奨されるが，これは現場の意見によって変更することができる。
3. 交換用の証明書を作成するときは，新しい証明書の作成と同じ手順に従う。

f) 認証情報を生かしたマシンアクセス方針の策定。これらの方針は非認証マシンの拒否，マシン認証の失敗の調査などを含む。

g) 障害及び災害の間の動作継続を考慮した設計。この作業をベンダーと調整する。災害時は，ネットワークの接続及びサーバアクセスは失敗することがあると考えられる。4 章参照。

h) 認証手順の一部として運営責任を負う可能性のある他部門との調整。例えば，生物医学工学部門は機器の修理に責任を負う可能性があるため，認証プロセスに関係すると考えられる。これは一時的に交換される可能性のあるローカルスペアの認証を含まなければならない。

A.1.2 医療機器ベンダー

機器ベンダーは以下を行う製品及びサービス手順を設計しなければならない。

- 直接比較及び信頼できる署名連鎖のどちらの方法にも使用可能な製品サービスサポートツールの提供。
- アップグレード，有効期限及びマシン交換を管理するための，サービス文書の提供及び施設の IT 組織とのサービス手順の調整。これはローカル機器の交換などの作業のサポートに十分なツール及び文書を含む。
- アップグレード，有効期限及び交換についての，施設の IT 組織及び他のベンダーとの手順の調整。直接比較を用いる場合は，サービス活動の結果として他のベンダーのマシンの証明書リストの更新が必要となることがある。
- 遠隔サービス活動が認証体系をどのように利用するかの検討。
- マシン認証に影響を与える遠隔サービス活動が施設の IT 組織及び他のベンダーとどのように調整されるかの検討。
- Problems with machine authentication are detected and correctable in such a way that they do not affect patient safety.

NEMA，COCIR，JIRA による承認のレビュー

A.2　技術的ガイドライン

A.2.1　医療提供者のためのガイドライン

A.2.1.1 認証権限部門

医療機関はこれの一部又はほとんどを外注することができるが，この責任を回避することはできない。医療機関は単に国の認証階層とは無関係の自己署名機関になることを選択してもよい。この場合，その自己署名機関は他のコンピュータネットワークには認識されないことがある。

医療機関の認証権限部門は医療機関の管理下にあるすべてのマシンについて，私有鍵及び公開証明書の提供又は少なくとも認可を行わなければならない。医療機関が直接比較を選択した場合，使用する鍵及び証明書はマシン自身が作成したものか，又はマシンのベンダーが作成したものかを選択することができる。この方法では署名機関の識別は重要ではなく，自己署名証明書は受諾可能である。医療機関自身は証明書のコピーをネットワーク上の他のマシンに提供し，この動作が認証セキュリティを提供する。医療機関は古い有効期限が切れたマシンの鍵及び証明書の両方を提供することができなければならないので，ベンダーが提供したものを扱うのではなく自身の鍵及び証明書を提供することを選択するほうがよいかもしれません。

医療機関が信頼できる署名連鎖に基づく方法を選択した場合，公開証明書は医療機関の認証権限部門によって署名されなければならない。これは多くのベンダーから利用可能でその医療機関によって運営される，独立した証明機関でもよい。この任務も外注が可能であるが，その信託はこの特定の医療機関に割当てられたサブルートに制限されなければならない。

医療機関の CA は国または地域の CA のチェーンの一部でも，又は自身の権限で運営する私有の CA でもよい。これらの要求事項はすべての CA 製品及びサービスの標準的な特徴である。

A.2.1.2 メディア配布

鍵，証明書及び CRL はメディア上での移動が可能である。そのメディアは使用後，慎重に保護されるか，又は安全に破棄されなければならない。X.509 証明書はわずか数千バイトと小さいため，メディアの選択はその配布，使用及び安全確保という運営上の必要性によって決定される。CD-ROM メディアは安価であり，一般的に使用，配布，管理及びシュレッダー破棄が容易である。Portable flash memory devices can also be used, but special procedures must be used to ensure 100% erasure when their use is complete.

A.2.1.3 ネットワーク配布

直接比較に必要な証明書の送信に必要とされる労力は，証明書サーバの使用によって減少させることができる。証明書サーバを使用すると，個々のマシンは公開証明書を取得するために，信頼できるサーバに問い合わせを行うことができる。個々のマシンは信頼

できるサーバの位置及びその公開証明書を取得するだけでよい。公開証明書は公知となりうるため，個々のクライアントマシンと証明書サーバの間の通信は暗号化される必要がない。

証明書サーバを使用すると，信頼性及び性能が損なわれる可能性が生じる。

A.2.1.4 有効期限及び交換に関する方針

- 有効期限は 2 年間とすることが推奨されるが，これは現場の意見により変更することができる。
- 交換用の証明書を作成するときは，新しい証明書の作成と同じ手順に従う。古い証明書の有効期限を修正しての再発行は安全性に欠ける。

ほとんどの医療機器は脅威の低い環境にあるため，鍵データ長の設定は 1024 ビットでよい。

A.2.2 ベンダーのためのガイドライン

A.2.2.1 公開鍵／私有鍵のペアの管理

マシンは私有鍵の保護だけでなく，その作成又は受諾の手段を提供しなければならない。マシンによっては，適切な乱数発生器を備えているために自身の私有鍵を作成することができる。そのようなマシンは，病院の認証権限部門から公開証明書を要求するために PKCS#8 を用いなければならない。すべてのマシンは PKCS#12 を用いて認証権限部門から公開鍵／私有鍵のペアを取得できなければならない。

マシンは認可されたサービススタッフから新しい鍵を受け取り，紛失又は危殆化した鍵と交換しなければならない。

A.2.2.2 Certificate Contents

The certificate may contain additional information describing the system that is used by field service and other staff to understand the purpose of a particular certificate. The key size selection and expiration are the only mandatory fields.

A.2.2.2.1 鍵サイズ

機器は最小 512 ビットから最大 4096 ビットまでの鍵データ長をサポートしなければならない。実際に用いられる鍵データ長は施設の方針によって定められる。For financial and other purposes, as of September 2006 the Web Services Interoperability (WS-I) organization recommends a length of 1024.

NEMA，COCIR，JIRA による承認のレビュー

A.2.2.2.2 Machine Identification

It can be useful to encode the machine serial number, asset tag identifier, and similar information into the descriptive fields of the certificate. This helps operational users to identify the correct certificate for use on other systems. This should only be done for information that is not likely to change.

A.2.2.2.3 Network Identification

Hostname and similar information can be useful, and can be encoded into the certificate.

This should not be done with information that is likely to change during network reconfigurations, because that could invalidate certificates.

A.2.2.2.4 Organization Information

Organization name and related information can be encoded into the certificate.

A.2.2.2.5 Certificate Purpose

These certificates can be used for encryption, signature, and node authentication. A different certificate must be used for digital signatures by people. This signature only implies that this machine created the data.

A.2.2.2.6 Expiration

The recommended expiration policy is to assign certificates a two-year life. Local risk analysis may change this. Longer validity periods increase the risks of theft and exposure. Shorter periods increase the maintenance costs of replacing expired certificates.

A.2.2.2.7 Encoding

The system should support both BER and DER encoding because both are commonly found.

A.2.2.2 メディア配布

機器は公開鍵／私有鍵のペア，公開証明書及び CRL をメディアから受け取ることができなければならない。機器は証明書要求及び 公開証明書の両方をメディア上でエクスポートできなければならない。

4.2.2.3 ネットワーク配布

クライアントマシンは，それが信頼できる公開証明書の発信元と通信していることを保証しなければならないことがあるため，サーバの公開鍵はクライアントマシンに手動でインストールされなければならない。DICOM 設定管理サービスは，DICOM 機器の公開証明書の提供に LDAP サーバを使用するよう定めている。HL7 及びウェブサービスの証明書要求に関する同等の基準は記載されていない。LDAP サービスは人及びマシン両方の公開証明書の提供に有効な手段である。

性能及び信頼性に関する問題を避けるため，クライアントマシンは公開証明書及び CRL をキャッシュに格納するか，又は公開証明書及び CRL を手動でローカルに保存する手段を提供しなければならない。このキャッシュは，問題が発生したため又はクライアントマシンが移動環境で使用中のために，証明書サーバが使用できないときに用いることができる。

4.2.2.3 私有鍵の使用

マシンは私有鍵を保護するために強力な内部セキュリティを備えなければならない。この達成手段は様々であるが，私有鍵の公開は他のシステムによる不適切な使用及びなりすましを許容することになるため，私有鍵はコピー又は閲覧されないよう保護されなければならない。

実用的な場合，アプリケーションはマシンの私有鍵を共有しなければならない。機能上，異なる通信プロトコル及び異なるアプリケーションのマシン認証には異なる証明書を用いなければならないということはない。例えば，HL7 通信及び DICOM 通信の両方を実装するアプリケーションは，両方に同じ鍵を共有することができる。しかし，一つのシステムにインストールされたソフトウェアの一部には，一つの鍵の共有が実用的ではないことがある。証明書の管理を簡素化するため，マシン 1 台当たりの私有鍵の数を制限することを推奨する。鍵及び証明書の数を削減すると，認証権限部門及び IT 管理組織にかかる記録保管の負担が低減する。

4.2.2.4 アクセス制御と認証の分離

マシンはマシン認証証明書をアクセス制御の代わりとして用いてはならない。例えば，クライアントマシンはサーバマシン上で使用可能な多くのサービスのうち，一つのみのアクセスに制限されることがある。アクセス制御の手順の詳細はこの白書には記載されていない。

4.2.2.5 認証メカニズム

医療提供者が認証方法を選択するため，機器は直接比較及び信頼できる署名連鎖の両方をサポートしなければならない。

4.2.2.6 継続の保証

認証メカニズムは災害及び他の問題による変更に対応するよう設定可能でなければならない。このリストに沿って，すべて速やかに再設定できなければならない。全機器は以下の 3，4 及び 5 をサポートしなければならない。1 及び 2 はベンダーの自由裁量で行う。

1. 連鎖署名，遠隔失効サービスへのアクセス‐問題が発生した場合，速やかに段階 3 に格下げしなければならない。
2. 直接，信頼できる証明書のサーバ配布‐問題が発生した場合，速やかに段階 4 に格下げしなければならない。
3. 連鎖署名，失効リストの手動配布。

NEMA，COCIR，JIRA による承認のレビュー

4. 直接，信頼できる証明書の手動配布。
5. 認証無効化（ブレークグラス）

NEMA，COCIR，JIRA による承認のレビュー

マシンは格下げモードでの動作期間の後，正常な動作への回復をサポートするためのツールを備えなければならない。

頭字語

BER ASN.1 オブジェクトをバイト列に変換する基本的なエンコード規則。

CA 認証権限部門

CAD コンピュータ支援診断

CRL 証明書失効リスト

CT コンピュータ断層撮影

DER ASN.1 オブジェクトをバイト列に変換する簡略化されたエンコード規則。

DICOM デジタル医用画像通信（標準開発組織）。 (http://medical.nema.org)

HIPAA 医療保険の相互運用性と説明責任に関する法律

HIS 病院情報システム

HL7 Health Level 7 （標準開発組織）。(http://www.hl7.org)

HTTP ハイパーテキスト トランスポート プロトコル，RFC-2616

HTTPS ハイパーテキスト トランスポート プロトコル(secure). The TLS protected version of HTTP

IHE インテグレーティング ヘルスケア エンタープライズ

IPSEC インターネット プロトコル セキュリティ

IT 情報技術

LAN ローカル エリア ネットワーク

LDAP ライトウェイト ディレクトリ アクセス プロトコル

OCSP オンライン証明書状態プロトコル

PACS 医用画像保管通信システム 参照 http://www.rsasecurity.com/rsalabs/node.asp?id=2124

PKI 公開鍵基盤

RIS 放射線部門情報システム

SOAP シンプル オブジェクト アクセス プロトコル

SPC セキュリティ及びプライバシー委員会

SSL セキュア ソケット レイア

TLS トランスポート レベル セキュリティ，RFC-2246

NEMA，COCIR，JIRA による承認のレビュー

ATNA 監査証跡とノード認証（IHE プロファイル）

WS-I ウェブ・サービス相互運用性(http://www.ws-i.org/)