1. 違反を示すが，CA に次の監査まで運用を続けることを許す。
2. 失効の前に問題の是正を最大 30 日間保留し，その間の CA の運営の続行を許す。
3. CA の証明書を失効する。（注：サービスを中断させるおそれがあるので，CA を停止することはできない。）

これらのいずれの処置をとるべきかに関する決定は，違反の重大さに基づくものとする（SHALL)。

欠陥カテゴリ － 危機的

認証局が CA 認定団体（このような認定が CA が営業する管轄区域内に存在する場合）によって決定された認証業務運用規程の不可欠なセクションに従うことができなかった場合は，危機的な欠陥として分類されるものとする（SHALL)。たとえば，認証局が費用のかかる手続きを省略したために証明書が危殆化したことが検出された場合は，危機的な欠陥として分類されるものとする（SHALL)。

CA がその管轄区域で認定されていた場合，認定がただちに撤回されることが推奨される（RECOMMENDED)。CA の証明書が上記の項目 1 と同様に失効されることが推奨される（RECOMMENDED)。

欠陥カテゴリ － 重度

認証局が認証業務運用規程の重要な要素に従わず，それが保証プロセスの一部と評価されていた場合には，重度な欠陥として分類されるものとする（SHALL)。たとえば，事業の十分な連続性を維持していない認証局が識別された場合は，重度な欠陥として分類されるものとする（SHALL)。

同時に追加のイベントが認証局に影響を与えた場合，または CA が数日以内に準拠性問題を改善できなかった場合には，問題の危機的な欠陥への格上げが課されるものとする（SHALL)。

欠陥カテゴリ － 部分的

認証業務運用規程への準拠違反は，保証プロセスの一部として評価され，重大な欠陥になる十分な可能性はないが，認証局の運用の完全性に影響を与える可能性がある場合，部分的な欠陥として分類されるものとする（SHALL)。たとえば，時代遅れのセキュリティポリシー及び手続きは，部分的な失敗として分類されるものとする（SHALL)。

このカテゴリ内の追加の欠陥が検出された場合，または CA が 30 日以内に準拠性問題を改善できなかった場合には，問題の重度な欠陥カテゴリへの格上げが課されるものとする（SHALL)。

欠陥カテゴリ － 軽度

部分的な欠陥になるおそれはないと見られるが，認証局の運用の完全性に対する全体的な影響を軽減するために対処すべきである準拠違反は，部分的な欠陥として分類されるべきである。たとえば，管理上の欠陥（不正確な料金請求など）は，軽度な欠陥として分類されるべきである。

このカテゴリ内の追加の欠陥が検出された場合，または CA が次の定期監査までに準拠性問題を改善できなかった場合には，問題の部分的な欠陥への格上げが課されるものとする（SHALL)。

２．７．６．　監査結果

監査者によって欠陥が発見された CA または RA は，証明書利用者及び検証者にただちに通知するものとする（SHALL)。

2．8．　秘密保持

2．8．1．　秘密扱いとする情報

1．　本人確認の目的で収集されたが，証明書に含まれない証明書所有者及び登録局の個人情報は，秘密に保たれるものとする（SHALL）（身分証明書，経歴調査，自宅住所，連絡先の詳細など）。この情報の一部は，証明書利用者の同意を得て，その証明書利用者のディレクトリリスティングに含めてよい（MAY）。

2.　秘密鍵

2．8．2．　秘密扱いとしない情報

1. 公開鍵

2. 医療専門家の役割

3. ヘルスケアの専門性

2．8．3．　証明書失効及び一時停止情報の開示

CAは，証明書利用者の証明書失効または停止の理由に関する情報を秘密に保つものとする（SHALL)。

2．8．4．　法的執行機関への情報開示

秘密情報は，証明書利用者の明白な同意に基づいて，またはCAあるいはRAの国の法律の下での要求に従ってだけ公開されるものとする（SHALL)。

2．8．5．　民事手続き上の情報開示

秘密情報は，証明書利用者の明白な同意に基づいて，またはCAあるいはRAの国の法律の下で認められた法廷からの命令の提示によってだけ公開されるものとする（SHALL)。

2．8．6．　証明書利用者の要求に基づく情報開示

秘密情報は，要求している証明書利用者からの（証明書利用者のデジタル署名のある）認証された電子メール，または署名付き文書による要求に従って，証明書利用者によって指名された関係者に開示されるものとする（SHALL)。

2．8．7．　その他の理由に基づく情報開示

秘密情報は，CAまたはRAの国の法律の下で認められた法廷からの命令の提示に従ってだけ開示されるものとする（SHALL)。

3．　利用者の識別方法と本人確認方法

3．1．　新規発行時での利用者の本人確認方法

3．1．1．　名前の形式

このポリシに基づいて発行される証明書に使用されるサブジェクト名は，このガイドラインのＸＸＸＸに従うものとする（SHALL)。

3．1．2．　名前の表す意味に対する要求

証明書を効果的に使用するには，証明書に現われる相対識別名が検証者によって理解され，使用される必要がある。これらの証明書で使用される名前は，それらが割り当てられた証明書利用者を意味を持つ方法で識別するものとする（SHALL)。これは，患者/消費者に発行される証明書でのペンネームの使用を妨げない。

3．1．3．　各種の名前形式を解釈する為の規則

本ガイドラインＸＸＸＸＸによる。

3．1．4．　名前の一意性

証明書に記載されるサブジェクト識別名は，あいまいさがなく，CA の個別の証明書利用者に一意であるものとする（SHALL)。

3．1．5．　利用者の名前を決定する際の問題の解決

CP は，名前クレーム紛争が発生した状況で適用される名前クレーム紛争解決手続きを持つものとする（SHALL)。

3．1．6．　登録商標を含んだ認識・認証・役割

本規程では，さらなる規定をしない。

3．1．7．　秘密鍵の所有を証明するための方法

鍵利用者は，CA に対して行う申請への電子的署名，あるいは CA からのチャレンジへの署名を定期的に要求されることによって，秘密鍵の所有を証明するように要求されるものとする（SHALL)。

3．1．8．　組織の認証

ヘルスケア組織，支援組織，または組織あるいは装置に代わって活動する個人は，国，州，または地方政府に対応した適切な文書によって，自らの存在とヘルスケアでの役割の証拠を RA に提示するものとする（SHALL)。CA，RA，及び適用可能な場合は AA も，申請側代表者の認証および組織の名において行動する代表者の認証すると同様にこの情報を検証するものとする（SHALL)。

3．1．9．　個人の認証

医療専門家，非資格ヘルスケア従業員，派遣ヘルスケア提供者，支援組織従業員，及び患者/消費者を含めて，個人は，証明書発行に先立ち，自分のアイデンティティを RA に認証するものとする（SHALL)。

本規程では，このような個人がパスポートの発行を受ける場合，または同等の厳格さを持つ手続きの際に必要とされるものと同じ身分証明書を推奨する。
医療専門家がヘルスケア免許，役割，及び専門（ある場合）を認証するためには，管轄区域の職業登録または認定団体によって確立された職業上の身分証明書をRAに提示するものとする（SHALL)。
非資格ヘルスケア従業員が雇用を立証し，ヘルスケアでの役割を認証するためには，派遣している医療組織または派遣している医療専門家からの派遣または雇用の証明書をRAに提示するものとする（SHALL)。
派遣ヘルスケア提供者がヘルスケアコミュニティで活動していることを立証し，ヘルスケアでの役割を認証するためには，派遣している医療組織または派遣している医療専門家からの派遣の証明書をRAに提示するものとする（SHALL)。
支援組織従業員が雇用を立証し，ヘルスケアでの役割を認証するためには，支援医療組織による雇用証明書をRAに提示するものとする（SHALL)。

3．2．　証明書の更新

3．2．1．　認証局の証明書の更新

認証局情報のルーチンの鍵更新は，元の記録が作成されたときに使用された元の文書に基づいて行われるものとする（SHALL)。

3．2．2．　登録局の証明書の更新

登録局情報のルーチンの鍵更新は，元の記録が作成されたときに使用された元の文書に基づいて行われるものとする（SHALL)。

3．2．3．　証明書利用者の証明書の更新

証明書所有者情報のルーチンの鍵更新は，元の記録が作成されたときに使用された元の文書または記録を再び参照することによって行われるものとする（SHALL)。
元の文書が無効になっているか廃棄されていた場合は，代替文書を使用してよい。

3．3．　失効後の再発行

3．3．1．　認証局の失効後の再発行

証明書が鍵危殆化以外の理由で失効された後の情報の鍵の再発行は，認証局を認定するために使用された元の情報の再提出を必要とするものとする（SHALL)。

3．3．2．　登録局の失効後の再発行

証明書が鍵危殆化以外の理由で失効された後の情報の鍵の再発行は，登録局を認定するために使用された元の情報の再提出を必要とするものとする（SHALL)。

3．3．3．　証明書利用者の失効後の再発行

証明書が鍵危殆化以外の理由で失効された後の情報の鍵の再発行は，証明書利用者情報の元の記録が作成されたときに使用された元の文書の提出，または使用された元の記録の参照を必要とするものとする（SHALL）。元の文書が無効になっているか廃棄されていた場合は，代替文書を使用してよい。

3．4．　証明書の失効申請

3．4．1．　認証局

ヘルスケア公開鍵基盤内の認証局が別の認証局に失効申請を行うときには，次のようにするものとする（SHALL）。

1. 証明書を特定する。
2. 証明書が失効されるべき理由を述べる。

申請書に秘密鍵で署名して，メッセージを暗号化し，関連するドメインCAに送信する。

3．4．2．　登録局

ヘルスケア公開鍵基盤内の登録局が認証局に失効申請を行うときには，次のようにするものとする（SHALL）。

1. 失効を要求する証明書を特定する。
2. 証明書が失効されるべき理由を述べる。
3. 申請書に秘密鍵で署名して，メッセージを暗号化し，関連するドメインCAに送信する。

3．4．3．　証明書利用者

ヘルスケア公開鍵基盤内の証明書利用者が認証局に失効申請を行うときには，次のようにするものとする（SHALL）。

1. 失効を申請する証明書を特定する。
2. 証明書が失効されるべき理由を述べる。
3. 申請に秘密鍵で署名して，メッセージを暗号化し，関連したドメインCAに送信する。

署名付き失効申請を必要とすることは，鍵危殆化が疑われる場合でも矛盾しないことに注目すべきである。失効申請は，本当に証明書利用者からのものであるか，または，第三者が危殆化した鍵を使用して要求を開始したかのどちらかであり，いずれにしても鍵は失効されるべきである。
秘密鍵を含んでいるトークンが紛失または盗まれた場合（したがって，証明書利用
者がデジタル署名付きの要求を開始できない場合）は，他の何らかの手段を用い，証明書を取得するために提供したものと同等のアイデンティティ証明を添える。

4．　業務手続き

4．1．　証明書の発行申請

本規程では，さらなる規定をしない。

4．2．　証明書の発行

本規程では，さらなる規定をしない。

4．3．　証明書の受理

本規程では，さらなる規定をしない。

4．4．　証明書の一時停止と失効

4．4．1．　証明書の失効事由

発行 CA は，次の場合に証明書を失効するものとする（SHALL)。

1. 証明書利用者，雇用者（非資格従業員または支援組織従業員の場合），または派遣者（派遣ヘルスケア提供者の場合）が，このポリシ，適用可能な認証業務運用規程，またはその他の契約，規制，あるいは，証明書に適用され，施行されている法に基づく義務を満たさなかった場合。
2. 秘密鍵の危殆化が認識されたか，妥当な疑いがある場合。
3. 証明書に含まれる該当のサブジェクト情報が正確でなくなった場合。
4. 証明書利用者の所属組織が変更された場合（たとえば，医療専門家が特定の組織から退職した場合）。
5. CA が，このポリシ及び/または適用可能な認証業務運用規程に従って証明書が適切に発行されなかったと判断した場合。
6. いかなる理由でも，証明書利用者または派遣ヘルスケア提供者の派遣者の要求があった場合。

証明書利用者，RA，及び派遣者は，証明書のサブジェクト情報が不正確であることに気づいた場合には，CA に知らせる義務がある。

4．4．2．　証明者の失効申請者

証明書の失効は，次の 1 つ以上の者によって申請されるものとする（SHALL)。

1．　の名前で証明書が発行された証明書利用者。
2．　装置またはアプリケーションに代わって証明書の申請を行った個人または組織。
3．　派遣されたヘルスケア提供者の派遣者。
4．　発行 CA の人員。
5．　発行 CA に関連する RA の人員。

4．4．3．　失効申請手続き

失効申請が CA によって受領されたとき，セクション 3.4 に従って，CA は次のようにするものとする（SHALL)。

1. 失効を要求しているエンティティが失効される証明書に帰されている証明書利用者であることを確認する。
2. 申請者が証明書利用者の代理人として行動している場合は，申請者が失効をもたらす十分な権限を持っていることを確認する。
3. 失効申請の理由を確認し，それが真実であると実証された場合は，証明書を失効する。

4．4．4．　効の猶予期間

証明書の失効要求の結果として取られる処置は，受領後ただちに開始されるものとする（SHALL)。

4．4．5　一時停止事由

ヘルスケアPKI内のCAは，停止をサポートしてもよい（MAY)。証明書の停止を正当化する識別された状況には，次のものが含まれる。

1．　秘密鍵の危殆化の疑いがある場合。停止は，調査中に行われる。
2．　証明書に関する情報が明確化されるまで。
3．　証明書利用者が停止を要求した場合。
4．　ローカルのヘルスケアPKIドメイン内で決定されたその他の状況。

4．4．6．　一時停止申請者

CA が停止をサポートする場合，証明書の停止は，次の 1 つ以上の者によって要求されるものとする（SHALL)。

1. その名前で証明書が発行された証明書利用者。
2. 装置またはアプリケーションに代わって証明書の申請を行った個人または組織。
3. 委託ヘルスケア提供者の委託者。
4. 発行CAの人員。
5. 発行CAに関連するRAの人員。
6. 検証者。

4．4．7．　一時停止申請手続き

停止要求がCAによって受領されたときには，セクション7.4.4.5に従って，CAは次のようにするものとする（SHALL)。

1. 停止要求が証明書利用者から，または装置あるいはアプリケーションに代わって申請を行った個人または組織から，または委託ヘルスケア提供者の委託者からであると主張されている場合，要求者のアイデンティティを確認する。
2. 停止要求が装置またはアプリケーションに代わって証明書の申請を行った個人または組織からであると

主張されている場合，要求者のアイデンティティを確認する。

3. 要求者が証明書利用者の委託者として行動している場合，要求者が停止をもたらす十分な権限を持っていることを確認する。

停止要求の理由を確認して，それが真実であると実証された場合は，証明書を停止する。

４．４．８．　一時停止期間の上限

証明書の停止期間は，（情報の確認などに）必要な調査の期間に限られるものとする（SHALL)。停止は10営業日を超えないことが推奨される。

４．４．９．　失効リスト発行の頻度

失効通知は，（発行当日に）すみやかに公開され，CRLが変更されたときには常に更新されるものとする（SHALL)。

４．４．１０．　失効リスト確認要件

検証者は，別のエンティティの公開鍵を使い始めるときは常に，CRLをチェックすべきである。CRLは，少なくとも毎日失効の有無をチェックされるべきである

４．４．１１．　オンラインでの失効確認に対する可用性

CAは，利用者の営業時間に合わせてCRLチェックサービスを使用できるようにすべきである。

４．４．１２．　オンラインでの失効確認要件

オンライン失効チェックには，証明書所有者が，応答に署名する機能を備えたオンライン証明書状態チェックサーバーとの安全な通信を確立する必要がある。これはCAでもよい（MAY)。このようにして，CAの真正性は検証される。発行CAではなく，検証機関または外注ディレクトリを使用することも可能かもしれない。

４．４．１３．　その他利用可能な失効確認公表手段

本規程では，さらなる規定をしない。

４．４．１４．　その他利用可能な失効確認公表手段における確認要件

本規程では，さらなる規定をしない。

４．４．１５．　鍵の危殆化に関する特別な要件

CA署名鍵の危殆化の際には，CAは相互証明書を発行したCAにただちに通知するものとする(SHALL)。

４．５．　セキュリティ監査の手順

セキュリティ監査手続きは，ISO 17799:2000と同等以上の規格に従うものとする（SHALL)。

4．6．　アーカイブ

記録は，ISO 17799-1:2000 と同等以上の規格に従って保管されるものとする（SHALL)。

4．7．　鍵の更新

証明書所有者が公開鍵を別の公開鍵に円滑に切り替えることができるように，CA は，切り替え日の 30 日前に新しい証明書を発行して，その日以降は新しい証明書を使用する必要がある日付を証明書保有者に明確に知らせなければならない。

4．8．　危殆化と災害からの復旧

セキュリティ監査手続きは，ISO 17799:2000 と同等以上の規格に従うものとする（SHALL)。

4．8．　認証業務の終了

CA が運営を停止する場合には，運営の終了時にただちに証明書利用者に通知し，CA の鍵と情報の継続的な保管を手配するものとする（SHALL)。また，相互認証しているすべての CA にも通知するものとする（SHALL)。

CA の運営が別の CA に譲渡され，より低い保証レベルで運営される場合には，運営が譲渡される CA によって発行された証明書は，譲渡に先立ち，その CA によって署名された CRL を通じて失効されるものとする（SHALL)。

CA が終了する場合には，その CA の記録の安全な保管または廃棄を確実にするための取り決めが行われるものとする。

5．　建物・関連設備、運用、要員のセキュリティ管理

これらは，ISO 17799 : 2000 と同等以上の規格，または認可された認定あるいは免許基準に従うものとする（SHALL)。これは，セクション 5 に適用され，次の項目をカバーする。

5．1．　建物及び関連設備管理

物理的管理は，ISO 17799:2000 と同等以上の規格に従うものとする（SHALL)。

5．2　運用面の管理

手続き的管理は，ISO 17799:2000 と同等以上の規格に従うものとする（SHALL)。

5．3．　要員管理

人事的管理は，ISO 17799:2000 と同等以上の規格に従うものとする（SHALL)。

6．　技術的なセキュリティ管理

6．1．　鍵ペアの生成とインストール

6．1．1．　鍵ペアの生成

証明書利用者の公開鍵/秘密鍵のペアは，次のものによって生成されるものとする（SHALL)。

1. CA，または
2. CA によって指名された別の信頼できる第三者，または
3. CA によって承認された鍵管理機能またはアプリケーションを使用して，証明書利用者。

鍵ペアが第三者によって生成される場合，鍵ペアの改変と生成された秘密鍵の危殆化を防止するためのセキュリティ措置（ハードウェアトークンなど）の採用を必須とするものとする（SHALL)。

6．1．2．　利用者への秘密鍵の送付

私有復号鍵が証明書所有予定者によって生成されない場合は，IETF RFC 2511「証明書管理プロトコル」に従ってオンライントランザクションで，または同様に安全な方法によって，証明書所有者に引き渡されるものとする（SHALL)。CA または信頼できる第三者の鍵生成エンティティは，オリジナルの私有鍵を引き渡した後は私有鍵のコピーを所有していないことを証明できるものとする（SHALL)。ただし，このようなコピーがセクション 7.6.2.4 に従って鍵のバックアップの目的で保持される場合を除く。

6．1．3．　認証局への公開鍵の送付

公開暗号化鍵が CA によって生成されない場合は，IETF RFC 2511「証明書管理プロトコル」に従ってオンライントランザクションで，または同様に安全な方法によって，CA に引き渡されるものとする（SHALL)。

6．1．4．　証明書利用者および検証者への CA 公開鍵の配付

公開鍵は証明書に結合されるので，公開鍵は，作成後ただちに証明書とともに証明書利用者に送られるものとする（SHALL)。公開鍵の引渡しには，証明書の引渡しと同じ手続きが適用されるものとする（SHALL)。これらは，RFC2527，セクション 4.2 で規定されている。

6．1．5．　鍵の長さ

鍵の最小サイズは，使用されるアルゴリズムに依存する。CA 証明書の鍵の最小サイズは，RSA アルゴリズムの場合，2048 ビットとする（SHALL)。他のアルゴリズムを使用する CA 証明書の鍵の最小サイズは，同等のセキュリティを提供するサイズとする（SHALL)。CA 以外の証明書の鍵の最小サイズは，RSA アルゴリズムまたは技術的に同等のアルゴリズムの場合，1024 ビットとする（SHALL)。他のアルゴリズムを使用する CA 以外の証明書の鍵の最小サイズは，同等のセキュリティを提供するサイズとする（SHALL)。

6．1．6．　公開鍵のパラメータ生成

公開鍵パラメータは，CA または信頼できる第三者の鍵生成組織によって生成されるものとする(SHALL)。

6．1．7．　パラメータ品質の検査

パラメータの品質チェックは，監査組織の役割とする（SHALL)。

6．1．8．　ハードウェア又はソフトウェアによる鍵ペア生成

鍵の生成は，安全な方法で行われるものとする（SHALL)。

6．1．9．　鍵の使用目的

認証鍵及びデジタル署名鍵は，身元確認及び/または否認防止目的のためだけに使用されるものとする（SHALL)。暗号化目的のための別個の鍵ペアがあるものとする（SHALL)。

6．2．　秘密鍵の保護

本規程では2つの鍵ペアが存在すべきことを推奨する。1つは，暗号化のためのペアであり，CAは秘密鍵をバックアップすることができる。もう1つは，認証またはデジタル署名鍵であり，私有鍵はエスクロウされない。

6．2．1．　暗号モジュールに関する標準

CA署名鍵は，US FIPS 140-1レベル2と同等以上の規格に準拠するものとする（SHALL)。
他の証明書は，US FIPS 140-1レベル1と同等以上の規格に準拠するものとする（SHALL)。

6．2．2．　複数人による秘密鍵の管理

証明書利用者がヘルスケア組織または支援組織である場合，秘密鍵は，複数に分割され，複数の人の管理下に置かれてよい（MAY)。

6．2．3．　秘密鍵のエスクロウ

認証またはデジタル署名のために使用される私有鍵は，法律によって必要される場合を除き，エスクロウされないものとする（SHALL)。

6．2．4．　秘密鍵のバックアップ

可能な場合，証明書利用者は秘密鍵をバックアップすることが推奨される（RECOMMENDED)。(秘密鍵がソフトウェアトークンに格納されている場合など。)
秘密認証鍵またはデジタル署名鍵は，証明書利用者の管理の下で全体としてバックアップされるものとする（SHALL)。バックアップされた鍵は，証明書利用者の環境（仕事場，部課，または組織）内に保持されるものとする（SHALL)。
証明書利用者は，CAが自分の秘密復号鍵をバックアップし，保有することに同意してよい（MAY)。このようなバックアップは，保証されたプロセスによって実行されるものとする（SHALL)。秘密鍵は，主要なコピーとして必要なレベルより低くない保護レベルでバックアップされるものとする（SHALL)。

6．2．5．　秘密鍵のアーカイブ

CA が証明書所有者の同意の下に私有鍵をバックアップした場合，この鍵は，少なくとも，CA 管轄区域での個人医療記録の必須保管期間と同じ期間にわたって保管されるものとする。

6．2．6．　暗号モジュールへの秘密鍵の格納

私有復号鍵がエンティティの暗号モジュールで生成されない場合は，IETF RFC 2511「証明書管理プロトコル」に従って，または同様に安全な方法で，モジュールに入力されるものとする（SHALL)。

6．2．7．　秘密鍵の活性化方法

ヘルスケア PKI においては，証明書所有者だけが私有鍵を活性化することができる。証明書所有者は，私有鍵の活性化の前に，私有鍵を保護している暗号モジュールまたはアプリケーションに認証されるものとする（SHALL)。この認証は，パスワード，パスフレーズ，またはバイオメトリックの形式を取ってよい（MAY)。非活性化された私有鍵は，暗号化された形式でだけ保管されるものとする（SHALL)。

6．2．8．　秘密鍵の非活性化方法

鍵が非活性化されるときには，メモリが割り当て解除される前に，鍵がメモリから消去されるものとする（SHALL)。鍵が格納されていたディスク領域は，その領域がオペレーティングシステムに解放される前に上書きされるものとする（SHALL)。暗号モジュールは，事前設定された非活動期間の後に自動的に私有鍵を非活性化するものとする（SHALL)。

6．2．9．　秘密鍵の廃棄方法

私有鍵の使用の終了時には，コンピュータメモリ及び共有ディスク領域内の私有鍵のすべてのコピーは，複数回上書きすることによって確実に破壊されるものとする（SHALL)。私有鍵破棄手続きは，CPS または公的に入手可能な文書で記述するものとする（SHALL)。

6．3．　鍵ペア管理に関するその他の配慮

6．3．1．　公開鍵の履歴保管

公開鍵は，未来の日付での署名の検証を可能にするために，信頼できる第三者によって保管される必要がある。CA は，公開鍵が保管されたことを確認する責任があるものとする（SHALL)。

6．3．2．　秘密鍵と公開鍵の有効期間

CA 以外の公開鍵と秘密鍵の使用は，3 年を超えないものとし（SHALL)，その後に新しい鍵ペアが発行されるものとする(SHALL)。属性証明書は，事業の必要に応じて，より短い有効期間を持ってよい(MAY)。CA の公開鍵と秘密鍵の使用は，10 年を超えないものとし，その後に新しい鍵ペアが発行されるものとする（SHALL)。

6．4．　活性化用データ

活性化データは，一意で予想不能なものとし，証明書所有者に安全に伝えられるものとする（SHALL)。

6．5．　コンピュータのセキュリティ管理

これらは，ISO 17799-1：2000と同等以上の規格，または認可された認定あるいは免許基準に従うものとし（SHALL)，また，次の問題をカバーするものとする（SHALL)。

[IETF RFC 2527 セクション 6.5.1 特定のコンピュータセキュリティの技術的な要件

[IETF RFC 2527 セクション 6.5.2 コンピュータセキュリティの評価基準

6．6．　情報システムのライフサイクル管理

これらは，ISO 17799-1：2000と同等以上の規格，または認可された認定あるいはライセンス基準に従うものとし（SHALL)，また，次の問題をカバーするものとする（SHALL)。

[IETF RFC 2527 セクション 6.6.1 システム開発の管理

[IETF RFC 2527 セクション 6.6.2 セキュリティマネジメントの管理

[IETF RFC 2527 セクション 6.6.3 ライフサイクルのセキュリティ評価

6．7．　ネットワークのセキュリティ管理

これは，ISO 17799-1：2000と同等以上の規格，または認可された認定あるいはライセンス基準に従うものとする（SHALL)。

6．8．　暗号モジュールの技術管理

これは，ISO 17799-1：2000と同等以上の規格，または認可された認定あるいはライセンス基準に従うものとする（SHALL)。

7．　証明書と失効リストのプロファイル

7．1．　証明書のプロファイル

ガイドラインＸＸＸＸＸによる。

7．2．　証明書失効リストのプロファイル

ガイドラインＸＸＸＸＸによる。

8．　本ポリシの管理

8．1．　改定手続き

この証明書ポリシに対するいかなる変更にも先立って，CA統制責任部門は，CAと直接相互認証しているすべてのCAに通知し，コメントを求めるものとする（SHALL)。ポリシの変更は，CA統制責任部門

によって承認されるものとする。

8．2．　公表ポリシ

CA の公認の代表者によってデジタル署名された証明書ポリシ文書の電子コピーが，次のように入手可能にされなければならない。

1．　すべての検証者が利用できる Web サイト上で，または

2．　電子メールでの要求によって。

8．3．　CPS 承認手続き

認証業務運用規程は，CA サービスの実装と鍵ライフサイクル管理の手続きを正確に詳述する。それは CP より詳細であり，CA のセキュリティを確保するために秘密に保たれる必要があってもよい（MAY）情報を含んでいる。

認証業務運用規程は，CA 統制責任部門によって承認されるものとする。

医療用公開鍵基盤ガイドライン　ドラフト　v006　Feb. 5

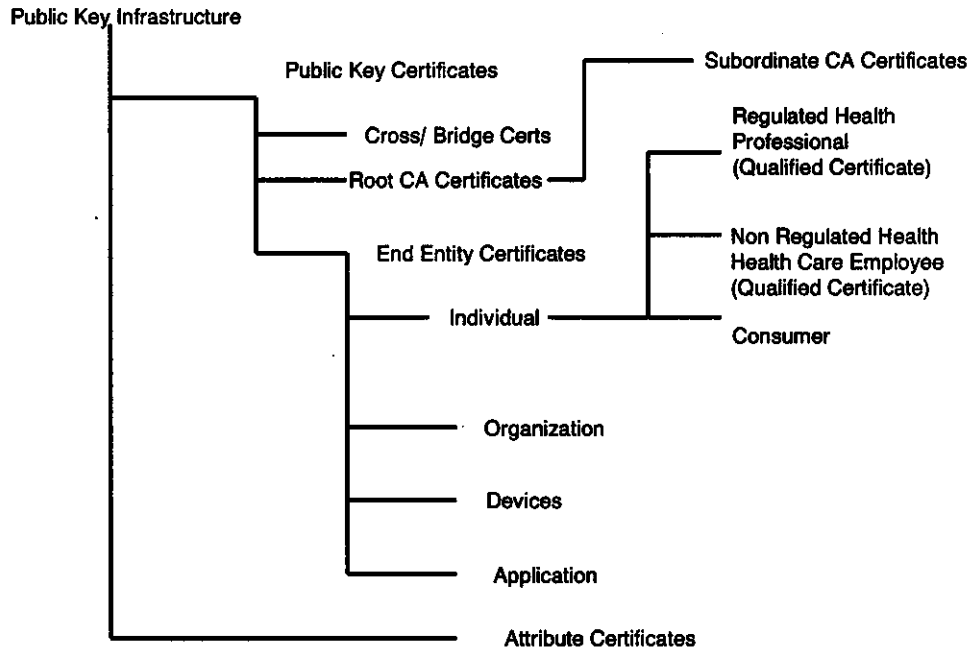
1．保健・医療・福祉分野と公開鍵基盤

2．基本的な方針と注意点

2－1．医療とＰＫＩ

ITU-T X.509 で規定される公開鍵基盤(PKI)を医療で用いる場合、その目的はいくつか考えられます。ISO-TS 17090 には以下の図が示されています。

Figure 1 – Health Care Certificate Types



この中で End Entity Certificates の Individual、Organization、それから Attribute Certificates は適応分野で運用や証明書の型式をある程度定めることが必要になります。このドキュメントは主にこれらの証明書の保健・医療・福祉分野で用いる場合の運用と証明書型式について、主に技術的な観点からガイドラインを示しています。Device や Application に PKI を用いる場合、保健・医療・福祉分野で特別に考慮することはなく、また SSL/TLS や PKI-VPN のように各方面で応用されている例があり、それらを参考にすればよいでしょう。

２－２．電子署名と完全性

End Entity Certificatesの中でIndividual、つまり医療従事者や患者などのサービス受給者に証明書を発行する場合と、Organization、つまり医療機関や保健者などの組織に証明書を発行する場合、その用途はいくつか考えられます。

用途の１つ目は「署名」で、これには法律や規則で定められている署名・捺印を電子的に行う場合と、法律や規則で定められてはいないが、情報作成・編集の責任者を明確にするために行う場合があります。また電子署名は通常，署名の対象となる情報のダイジェストに対して行われますので、もとの情報の完全性（真正性）の保証のための１つの手段としての意味がありますが、完全性については後であらためて取り上げます。法律や規則で定められている場合はわが国では「電子署名法」に準拠した証明書と署名方法が必要です。電子署名法では電子署名に用いる証明書は署名の目的のためだけに用いることが定められていますので、署名に用いる証明書およびそのペアの署名鍵は他の用途に用いてはいけません。法律・規則で定められていない署名に同じ証明書や署名鍵を用いるかどうかは、運用で定めなければなりませんが、今後の連携医療の発展を考えると、あまり狭い範囲だけで通用する証明書を用いることは推奨されません。また証明書の数が増えるとそれだけ運用に負担がかかりますので、法的に有効な署名と同じものを用いると良いでしょう。

２－３．資格認証

保健・医療・福祉分野では情報を扱う人の資格や役割が重要な場面が多くあります。PKIで資格や役割をあらわすためには２つの方法があります。１つは公開鍵証明書に資格や役割を示すフィールドを定義して使う方法で、もう１つは属性証明書を使う方法です。この２つの方法にはそれぞれ特徴があり、使い分けを工夫する必要があります。属性証明書は公開鍵が含まれていなくて、通常は短い有効期間で使用します。また公開鍵がないために署名との関連付けは属性証明書自体ではできませんので、対応する公開鍵証明書を一緒に用いる必要があります。

属性証明書と公開鍵証明書の使い方を検討するためにＡ病院の内科外来を担当するＸ医師が紹介されて受診した患者の過去の診療記録について紹介元のＢ医療機関に問い合わせる場合を考えてみます。Ｘ医師はＢ医療機関に対して問い合わせ書を作成して送りますが、Ｂ医療機関は問い合わせて来た人の身元や属性を確認することなしに、患者情報を返送することはできません。Ａ病院の内科に患者を紹介したことはわかっていますので、問い合わせて来た人がＡ病院の内科担当の医師であることを確認すればよいことになります。

２－３－１．公開鍵証明書による資格認証

最初に公開鍵証明書だけですべての属性を証明する場合を考えてみます。この場合証明書にはＸという人で、医師であって、Ａ病院の従業員で、内科外来担当であることが記載されることになります。そしてこの証明書はＢ医療機関で信頼できるものであると判断さ

れなくてはいけません。したがって証明書の発行者はB医療機関が信頼できる組織が発行したものである必要があります。A病院が大阪にあり、B医療機関が東京であることもありえますし、それ以外の医療機関とも同様な場合が起こりうることを考えると、事実上日本中ですべての医療機関から信頼される組織が証明書を発行する必要があります。

仮に財団法人医療情報システム開発センター（MEDIS-DC）が証明書を発行すると仮定します。MEDIS-DC はXが医師であることは厚生労働省に問い合わせることで理論的には確認することが可能です。またA病院が存在することも地方自治体等に問い合わせることで確認できます。これらは手間ではありますが、仕組みをうまく作れば現実にも可能でしょう。X医師がA病院に勤務していることも保険医登録情報などを用いればなんとかできるかも知れません。しかしX医師が内科外来担当であることはA病院に問い合わせる以外に確認の方法がありません。証明書発行の要請があるたびにその医療機関に勤務形態を確認しなければなりませんので、証明書発行の運用は複雑になります。これは証明内容に責任を持つ組織が 1 つの証明書に対して多数存在するための複雑さです。また、もし発行したとしても内科外来担当から救急外来担当に変わった場合や、A病院からB病院に転勤した場合には証明書を廃棄して、新しい証明書を発行しなければなりません。電子証明書は単なるファイルですので、いくつでもコピーできます。したがって電子証明書そのものをすべて廃棄することは不可能ですので、証明書廃棄リスト（CRL）を発行し、証明書を使う人は常に最新の CRL を参照して、その証明書は廃棄されていないかどうかを確認する必要があります。転勤や担当部署の変更は全国的に見れば日常的に起こっていますので、大量の CRL が常に存在することになり、PKI 全体の運用に大きな負担になります。

つまり医療で必要なすべての属性を 1 つの公開鍵証明書に盛り込むことは現実には不可能といえます。複数の公開鍵証明書を組み合わせて使う方法も考えられますが、もとの情報と証明書を関連付けるためには電子署名を行う必要があり、公開鍵証明書の数だけ電子署名を重ねる必要があります。そのため電子署名の順序など複雑な取り決めをしなければなりませんし、CRL が大量に発生する問題は解決できません。

２－３－２．属性証明書による資格認証

属性証明書は技術的には公開鍵証明書の簡略版であり、比較的簡単に発行できますし、通常は数時間～数日といった短期間で無効になるようにしますので、資格や役割の変更があっても CRL を発行する必要性はほとんどありません。一方、属性証明書には公開鍵がありませんので、電子署名と直接対応付けることはできません。公開鍵証明書と組み合わせて用いる必要があります。つまり属性証明書で資格認証を行うということは、公開鍵証明書を属性証明書の使い分けを考えることにほかなりません。

２－３－１の公開鍵証明書だけで資格認証を行う場合にうまくいかない理由は証明内容に責任を持つ組織が複数存在することと、CRL が大量に発生することでした。従ってこれらの障害を取り除くことができるような属性証明書と公開鍵証明書の使い分けを考えれば

よいことになります。公開鍵証明書は基本的には公開鍵が誰のものか証明するものです。この「誰」に対して責任を持つ組織が単純であり、「誰」があまり変化しなければ公開鍵証明書の運用は単純になり、それ以外の属性を属性証明書で証明すればよいことになります。このような「誰」の定義には2つの場合を考えることができます。

1つ目は個人や法人といった人格を「誰」として扱う場合です。このような公開鍵証明書に対する署名は個人「実印」や法人の「公印」に相当します。証明に責任を持つ組織は住民票情報を管理している地方自治体や法人登記または医療機関登録を管理している組織になります。これは電子政府計画で整備されつつあり、制度的な問題は別として技術的には比較的容易に運用可能です。先の例で言えばXさんとA病院、B医療機関がそれぞれ公開鍵証明書を 1 つもつことになります。Xさんが医師であること、A病院の勤務医であること、内科外来担当医であることはすべて属性証明書で運用することになります。この方法ではCRLはほとんど発生しませんし、属性証明書を証明内容ごとに複数使うことにすれば、証明内容に対する責任組織も単純です。ただし一般には属性証明書は有効期間が短いものですので、しばしば必要になる医師の資格を示す属性証明書もその都度、発行を要求しなければなりません。医師の資格に責任を持つのは厚生労働省ですから、たとえ地方自治体に業務を委託するとしても医師資格属性証明書の要求は多数が集中することになり、運用上の負荷になる可能性があります。医師のような公的資格は変更が極めて少ないので、属性証明書の有効期間を長くすることも考えられます。しかしこの場合は少ないとはいえ、資格喪失などがありますので、属性証明書のCRLの発行を考えなければなりません。CRLの発行はそれほど難しいことではありませんが、属性証明書を使うシステムがすべてCRLを検索しなければならなくなり、実装上の負荷になる可能性があります。また属性証明書は公開鍵証明書に関連付ける必要がありますが、属性証明書の有効期間が公開鍵証明書の有効期間を超えることはできないために、公開鍵証明書の有効期間が残り少なくなっている場合などは属性証明書の有効期間を変えなければならず、発行自体も複雑になります。

2つ目は公的な資格を含めた個人を「誰」として扱う場合です。法人や組織は一つ目の場合と同じです。先の例では「医師であるXさん」を公開鍵証明書で資格認証し、「A病院の勤務医」、「A病院の内科医外来担当医」を属性証明書で資格認証します。この場合は運用がもっとも単純になります。公的資格はほとんど変化しませんので、CRLの発生は少なく、証明内容の責任の所在も単純で明確です。唯一の問題はXさんが医師として署名する場合と、個人として署名する場合に証明書や署名鍵を使い分ける必要があることですが、あまり大きな問題にはならないでしょうし、心情的にはかえって好まれるかも知れません。公的資格には「医師」のような国家資格や「保険医」のような地方自治体に対する登録資格があり、現在の管理体制では責任の所在が異なる以上は証明書を分ける必要がありますが、これは制度的な整備や「保険医」の属性証明を医療機関や医師会などに委任することで、解決することが可能です。

このガイドラインはPKIを保健・医療・福祉分野に応用するための技術的な指針ですの

で、運用面の断定はしていませんが、公的な資格を公開鍵証明書で運用し、それ以外の属性は属性証明書で運用することを推奨しています。またその前提で証明書の形式などを規定しています。また当面は国家資格だけを公的な資格としてガイドラインに取り入れています。これは制度的な整備などが整えば改定される可能性があります。

2－4．暗号化

PKI は暗号化に用いることもできます。PGP や S/MIME でも暗号化を行うことができます。アプリケーションやライブラリも数多く存在し、また保健医療福祉分野で特別な要素もありませんので、PKI を暗号化に用いること自体は簡単です。しかしただ 1 つ注意しなければならないことは、法的に有効であることが求められる署名に用いる証明書や署名鍵は暗号化に使ってはいけないということです。また保健医療福祉分野の情報は利用できなければ意味がありません。暗号化によって万が一にも利用性が阻害されることがないように注意する必要があります。通信途中のような一時的な暗号化は問題がありませんが、データベースそのものを暗号化するような場合は、事故などがおこっても必要なときに速やかに復号できる必要があります。

2－5．電子保存の真正性と長期にわたる署名の確認

PKI は公開鍵暗号を基礎においていますが、公開鍵暗号の安全性は時間的に有限とされています。例えば 1024 ビットの RSA 暗号を用いる場合は 1 年程度の安全期間を前提に運用されることが多いでしょう。単純な情報交換やある時点での資格認証には問題がありませんが、保存された情報の署名の有効性を長期にわたって確認する必要がある場合には問題が生じます。法的に保存が義務付けられた情報は 3 ～ 5 年、あるいはそれ以上の間、真正性を保って保存しなければなりません。1 年の寿命の公開鍵暗号を用いる場合、公開鍵が作成され証明書が発行された直後に署名を行っても、その署名が確認できる、つまり PKI で真正性が保証されるのは高々1 年です。したがって PKI を利用して電子保存の真正性を求める場合は工夫が必要です。

1 つは署名そのものの有効期間を延長する方法です。簡単に言えば有効期間が切れる前に新しい署名鍵と公開鍵証明書を作成し、再署名します。この方法は単純ですが、署名者ごとに署名の有効期間を管理し、再署名を依頼する必要があり、個別に再署名する限り、ほとんど不可能と考えてよいでしょう。システムで自動的に再署名する方法も考えられますが、署名鍵をシステムがアクセスできる必要があり、事実上不可能です。

2 つ目は署名の確認者を置く方法です。例えばすべての署名は有効期間が 1 ヶ月以上ある書名鍵および公開鍵証明書を用いて行うことと決めておき、すべての署名を一ヶ月に一度確認します。そして有効であった署名のなされた情報のリストを作り、そのリストに確認者が署名を行います。これを確認済みリストとし、さらに確認者の署名の有効期間が過ぎる前に確認済みリストの署名確認を行い、そのリストを作成し、署名を行います。これを

何度か繰り返せば一定期間の真正性は確認者に信頼性のもとに保証されます。

2つ目の方法の応用として、確認リストを作成した時点で機能上および運用上で改ざん不可能な媒体（例えば第三者が監査可能な金庫保管したCD-ROMなど）に固定して厳重に管理することも可能です。

いずれにしても単純に電子署名をしたから長期の保存の真正性が確保されるとかんが得てはいけません。

2－6．タイムスタンプ

電子署名によって署名時点での真正性が証明可能であり、また前節にのべたような工夫を行えば一定期間の真正性も確保できると説明しましたが、保健医療福祉分野の場合、情報が作成された時刻や、順番が重要です。虫垂炎と診断した時点と虫垂炎の手術を行った時点がこの順か、逆の順かで大きく意味が変わってきます。したがって一般に保健医療福祉分野では電子署名を行った時刻が大変重要で、信頼性のある時刻情報を付加する必要があります。訴訟等で証明力を確保しようと思うと、時刻の信頼性は第三者にとっても信頼できるものでなければなりません。本ガイドラインでも第 7 章でタイムスタンプについて述べていますが、基本的にはすべての署名にタイムスタンプがあることが求められます。

第三者に信頼される時刻情報を付加するためにはタイムスタンプ発行局は保健医療福祉機関から独立した信頼できる第三者機関（Trusted Third Party：TTP）が行うことが理想ですが、しっかりした監査によって信頼性が説明可能であれば、保健医療福祉機関内部やそのグループ内に置くことも可能です。

3．公開鍵証明書と証明書失行リストのプロファイル

3－1．全体的な方針

保健・医療・福祉分野での公開鍵証明書プロファイルはITU-T X.509推奨規格第3版に準拠するものとします。すなわちRFC2459に規定されているプロファイルに従うものとします。ITU-T X.509推奨規格はRFC2459以外にもISO/IEC9594-8として登録されていますが、このガイドラインで参照した文書はRFC2459です。このガイドラインではRFC2459自体にも触れていますが、日本の保健・医療・福祉分野で公開鍵基盤を用いるための制限や追加項目を中心に記載しています。実装に際してはRFC2459を参照してください。また原則としてISO TS 17090に準拠しています。

3－2．文字コードセット

名前などの文字コードセットは RFC2459 で PrintableString, BMPString および UTF-8String を使用することが定められています。(2003 年以降は UTF-8String のみ。)