1.3.3.2. LANにおけるPC設置・変更・撤去の標準

本標準は、当保健医療機関LAN環境へのPC（サーバ、クライアント等）接続において発生し得る各種の問題を未然に防ぎ、情報資産を保護することを目的とする。

1.3.3.3. リモートアクセスサービス利用標準

本標準は、ダイヤルアップ等により保健医療機関内ネットワークを利用してリモートアクセスサービス利用にあたり、当保健医療機関の情報資産を外部から守ることを目的とする。

1.3.3.4. 専用線及びVPNに関する標準

本標準は、当保健医療機関とその取引先等が円滑かつ効率よく業務を遂行するために構築されたVPN及び専用線によるネットワークにおいて、接続される両端の組織のお互いがネットワーク犯罪の被害者や加害者、あるいは踏み台にならないことを目的とする。

1.3.4. 物理的対策

1.3.4.1. サーバルームに関する標準

本標準は、サーバルームの設置によってサーバ等を保護し、それらに格納する情報の安全性を確保することを目的とする。

1.3.4.2. 物理的対策標準

本標準は、当保健医療機関の敷地・建物・機器・設備等を保護し、それらの損傷や利用の妨害、許可されていないアクセスを防止することを目的とする。

1.3.4.3. 職場環境におけるセキュリティ標準

本標準は、職場環境におけるセキュリティリスクを低減し、情報漏えい等のセキュリティ事故を防止することを目的とする。

1.3.4.4. 媒体の取扱に関する標準

本標準は、クライアントPC 等の修理時、並びに媒体の処分時に関するルールを定め、機密性の高い情報の漏洩を未然に防ぐことを目的とする。

1.3.5. セキュリティ運用対策

1.3.5.1. システム維持に関する標準

本標準は、当保健医療機関におけるシステムのセキュリティレベルを維持するためのパッチ等の適用ルール及びバックアップルールについて規定する。

1.3.5.2. 監視に関する標準

本標準は、当保健医療機関が利用している情報システムの監視について規定し、システム障害、不正アクセスの兆候、情報の流出、不正利用等をいち早く検知し、それらの原因究明が円滑に行われることを目的とする。

1.3.5.3. セキュリティインシデント報告、対応標準

本標準は、セキュリティインシデントが発生した場合に迅速に対応し、情報システム環境の復旧が円滑になされることを目的とする。

また、当保健医療機関においてセキュリティインシデントとは次の事態を指す。

（1）情報セキュリティに対する侵害

例：不正アクセスによる情報漏洩、従業員による情報漏洩、ウイルス感染、なりすまし、使用不能攻撃、ハードウエア紛失　等

（2）システム・ネットワークの故障、損壊

例：電源異常、熱暴走、天災による機器損壊　等

1.3.6.　その他対策

1.3.6.1.　監査標準

本標準では、セキュリテイマネジメントシステムの内部監査及び、個人情報保護の監査にかかわる事項を規定する。

1.3.6.2.　セキュリティ・個人情報保護の教育に関する標準

本標準では、セキュリティ及び個人情報保護の教育、訓練に関わる事項を規定する。

教育、訓練の対象者は、当センターのコンピュータに携わっているすべての人、またはそれを運用、管理し、業務に携わっているすべての人を対象とする。

教育対象者：

(1)経営者層、管理部門の長、管理部門担当者、

(2)情報システム管理者、オペレータ、派遣入力者、派遣プログラマ等

(3)外部の研究員(研究管理者･研究者　等)

(4)その他外部からの派遣者（庶務･受付等)

(5)第三者利用者（外部のＷｅｂ利用者等)

1.3.6.3.　委託時の契約に関する標準

本標準は、当保険医療機関の業務を外部の業者に委託し、実施する場合の契約における問題および委託作業時の問題、特に個人情報の保護に関する問題を未然に防ぐことを目的とする。

1.3.6.4.　プライバシーに関する標準

本標準は、情報主体の個人情報を適切に収集・維持・破棄に取り扱う際に注意するべき事項をまとめ、発生しうる問題を未然に防ぐことを目的とする。

特に個人情報における検体提供者の個人情報（以下「臨床情報」とする）については、遺伝子に関わる情報を含む場合があり、関連する法律・規範（医療法・三省指針等）に基づいて適切に管理する。

本標準の実施の細則は「個人情報保護規定」を参照すること。

1.3.6.5.　罰則に関する利用標準

本標準は、当保険医療機関のセキュリティ違反及び個人情報保護違反に対する罰則の適用手順及びそれに関わる遵守事項を規定する。

本標準は、セキュリティ方針および個人情報保護標準が適用されるすべての人を対象とする。罰則事項の執行は、セキュリティ違反および個人情報保護違反に対する罰則の適用に関わる委員会のメンバー、部門長及び人事部門の担当者を対象とする。

1.4.　リスク評価手順書

1.5.　情報資産管理シート

1.6.　リスク評価シート

1.7. リスク管理シート
1.8. 適用宣言書

## 2．プライバシポリシ

### 2.1. 個人情報保護基本方針

XXX 保健医療機関（以下、XXX）は保健医療機関であり、保健医療情報を取り扱っている。

#### 2.1.1 基本方針

個人情報は個人の重要な財産である。XXX で業務に従事するすべての者は、個人情報保護に関するコンプライアンス・プログラム(CP)を遵守し、個人情報を正確かつ、安全に取り扱うことにより、検体を提供する人の個人情報を守り、その信頼にこたえなければならない。

#### 2.1.2 目的

XXX に収集される個人情報が、適切な方法で収集され利用されることを保証するために、CP を定め、これに基づき実施し･維持し、さらに継続的にこれを改善してゆくことを目的とする。

### 2.2. 個人情報保護基本規程

この規程は、XXX 保健医療機関（以下、「XXX」という。）の管理規程の基本規程に定める。

#### 2.2.1 目的

この規程は、個人情報を保護するために、体系的で XXX 全体として統合されたコンプライアンス・プログラム（以下、「CP」という。）を定め、CP に基づき実施し、維持し、継続的にこれを改善してゆくことを目的とする。

#### 2.2.2 適用

この規程は、XXX 内において処理されるすべての個人情報に関して適用される。

当該の個人情報の一部もしくは全部が、コンピュータシステムにより処理されているか書面などにより処理されているかには関わらない。

#### 2.2.3 用語の定義

この規程で用いる主な用語の定義は次による。

（1）個人情報

個人に関する情報であって、当該情報に含まれる氏名、生年月日とその他の記述、または個人別につけられた番号、記号その他の符号、画像もしくは音声によって当該個人を識別できるもの（当該情報だけでは識別できないが、他の情報と容易に照合することができ、それによって当該個人を識別できるものを含む)。

（2）情報主体

一定の情報によって識別される、又は識別されうる個人。

（3）業者

事業を営む法人、その他の団体または個人。

（4）管理者

事業者の内部において代表者によって指名されたものであって、コンプライアンス･プログラムの実施及び運用に関する責任と権限を持つもの。

（5）受領者

個人情報の提供を受ける法人、その他の団体または個人。

（6）監査責任者

事業者の代表者によって示されたものであって、公平、かつ、客観的な立場にあり、

監査の実施及び報告を行う権限を持つもの。

（7）情報主体の同意

情報主体が、収集、利用又は提供に関する情報を与えられた上で、自己に関する個人情報の収集、利用又は提供について承諾する意思表示。情報主体が子供の場合は、保護者の同意も得るべきである。

（8）コンプライアンス･プログラム（CP）

事業者が、自ら保有する個人情報を保護するための方針、組織、計画、実施、監査及び見直しを含むマネジメントシステム。

（9）収集目的

個人情報の利用および提供の範囲を定め、情報主体の同意の対象となるもの。

（10）利用

事業者が当該事業者内で個人情報を処理すること。

（11）提供

事業者が当該事業者外のものに自ら保有する個人情報を利用可能にすること。

（12）預託

事業者が当該事業者外のものに情報処理を委託するなどのために自ら保有する個人情報を預けること。

2.2.4　個人情報保護方針）

XXX の代表者は、次の事項を含む個人情報保護方針を定めるとともに、これを実行し維持する。

（1）事業内容および規模を考慮した適切な個人情報の収集、利用及び提供に関すること。

（2）個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えいなどの予防並びに是正に関すること。

（3）個人情報に関する法令およびその他の規範を遵守すること。

（4）コンプライアンス･プログラムの継続的改善に関すること。

XXX の代表者はこの方針を文書化し、役員および従業員に徹底させるとともに一般の人が入手可能な措置を講じる。

2.3.　入退室管理規程

本規程は、XXX の施設・各部屋（以下「施設・各部屋」という。）の入退管理に関する事項を定める。

2.4.　臨床情報を預託される場合の細則

本細則は、XXX の個人情報保護規程（以下「規程」という。）に基づき、情報主体以外の者（人または法人）から臨床情報（研究者が臨床現場から収集した治験等、臨床研究用の検体、およびそれらより測定した検体情報。遺伝子情報を含む場合がある。）を預託される場合の措置（手続き）について定める。

## 3．認証局実施規程

3.1.　本認証実施規程の適用範囲

XXX 認証実施規程（Certification Practice Statement、以下 CPS という）は、XXX 認証局が行う証明書発行、失効、及び証明書を基礎とする公開鍵基盤(PKI：Public Key Infrastructure)の運用維持に関する諸手続きおよび証明書発行、利用にかかわる主体の責任を記述したものである。XXX 認証局では、証明書所有者の私有鍵や証明書の格納媒体として IC カードを用いる。

XXX 認証局は、ルート認証局より CA 証明書の発行を受け、ルート認証局の下位認

証局として活動する。

本 CPS は、医療従事者用公開鍵証明書、患者・保健医療福祉サービス利用者用公開鍵証明書および医療機関・保健医療福祉サービス供給組織用公開鍵証明書を発行する「ヘルスケア PKI 認証局」証明書ポリシ(以下 CP という)に従い、XXX 認証局が発行するすべての証明書に適用されるものとする。ヘルスケア PKI とは、保健医療福祉分野において医療情報を地域で連携して利用するための PKI である。

本 CPS と CP が抵触する場合には、CP が優先する。

3.2. 本規程が依拠する文書

ISO/DTS17090-1 保健医療情報 □ 「公開鍵基盤 パート 1: フレームワーク、概観」

ISO/DTS17090-2 保健医療情報 □ 「公開鍵基盤 パート 2: 証明書プロファイル」

ISO/DTS17090-3 保健医療情報 □ 「公開鍵基盤 パート 3: 認証局のポリシ管理」

3..3. 本規程が参照する文書

ISO 17799-1:2000 情報技術 － 情報セキュリティ管理の運用規程

IETF/RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols

IETF/RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework

IETF/RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP

IETF/RFC 3280 Internet X.509 Public Key Infrastructure: Certificate and CRL Profile

US FIPS 140-1 、 140-2(Federal Information Processing Standard) : Security Requirements for Cryptographic Modules (http://csrc.nist.gov/cryptval/)

JIS X 5080:2002 : 情報技術－情報セキュリティマナジメントの実践のための規範 (ISO/IEC17799:2000)

電子署名及び認証業務に関する法律（平成 12 年 5 月 31 日　法律第 102 号）

電子署名及び認証業務に関する法律施行規則（平成 13 年 3 月 27 日　総務省・法務省・経済産業省令第 2 号）

電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成 13 年 4 月 27 日　総務省・法務省・経済産業省告示第 2 号）

以下、詳細は添付資料に示す。

## D. 考察

本研究では、電子署名を実運用する際に必要となる規程類の開発を行った。研究に際しては、全体を網羅することを試みたが、非常に広範囲にわたり、また、その作業量が膨大であることが判明したため、一部は項目を洗い出すに留めたところもある。しかしながら、今後、各医療機関で認証業務および電子署名を行う際には、これらの規程類は必ず必要となる。今年度の研究で判明したとおり、これらの規程類の策定作業は非常に作業量を必要とするものであり、これをそれぞれの医療機関で行うには、その負担が大きすぎると考えられる。今後は本研究で開発したようなテンプレートを充

実すると共に、これらの規程類の策定を支援するソフトウェアの開発も必要ではないかと考える。

なし。

E．結論

電子署名や認証局の実際の運用に際しては、さまざまな運用手順書や規程類が必要となる。そこで、本研究では、これらの規程類のうち、すべての基本となる、情報セキュリティポリシとプライバシポリシ、さらには認証局実施規程を開発した。そして、今後保健医療機関で電子署名を活用する際の一助となるようにすると共に、今年度の実証実験においてもこれらの規程類に基づいて検証が行った。

来年度以降、これらの規程類をさらに充実し、他の保険医療機関でも使用可能なテンプレートして開発していく予定である。

F．健康危険情報

なし。

G．研究発表

1．論文発表

なし。

2．学会発表

なし。

H．知的財産権の出願・登録状況

1．特許取得

なし。

2．実用新案登録

なし。

3．その他

厚生労働科学研究費補助金（医療技術評価総合研究事業）
分担研究報告書

# 情報セキュリティポリシ、認証局実施規程に関する研究

## 添付資料１

## 情報セキュリティポリシ

# 情報セキュリティポリシ

代表者:XXX 病院長

１．【情報セキュリティの定義と基本方針策定の目的】

保健医療機関 XXX(以下「XXX」と称する)においては、個人の機微な情報を含むデータベースが、施設の内外のネットワークに接続されたコンピュータシステムにより運営されている。

XXX 内部でのリスク対策を確実に行うことで、医療従事者が自らの業務を継続することはもとより、医療受給者が安心して診療、研究を任せられる環境を提供するために「情報セキュリティ基本方針」を定める。

本情報セキュリティ基本方針は、XXX 建屋内にある、臨床情報データベースや仕様書等の情報資産、業務ソフトウエア等のソフトウエア資産、コンピュータ機器やネットワーク機器等の物理的資産、電源・空調等のサービスを適用範囲とする。

２．【情報セキュリティの目標】

XXX では、そこで働く人々の取り扱う保健医療情報が、不当に暴露されたり、内容を改竄されたり、処理を妨害されたりしないようにすることを目標とし、必要な管理策をとる。また、臨床情報のような個人情報の利活用には、提供者のインフォームドコンセントによる意向が反映されることを目標とする。

３．【情報資産の管理方針】

(1)基本方針の徹底のためのセキュリティ教育と違反者の罰則

XXX では、人的な誤り・盗難・不正行為・設備の誤用を防止するため、適宜セキュリティ教育を実施し、違反者には罰則を課する。このセキュリティに関する審査・契約・罰則は、外部から登録された研究者にも適用する。

(2)機密性・完全性・可用性の確保

研究内容の重要性・機密性への要求の高さを考慮して、業務施設及び業務情報に対する認可されていないアクセス、損傷及び妨害を防止するため、セキュリティ区域内で厳重に管理される。さらに、XXX と外部の協力研究機関等の組織間で交換される、情報の紛失・盗聴・改竄又は誤用からの保護にも、管理策を策定し維持する。

許可されていない利用者のアクセスを防止するための管理策を策定する一方、許可された利用者の運用を損なうことの無いよう、ウイルス等の悪意のあるソフトウエアからの保護策も講じる。

(3)システムの開発及びメンテナンス

業務用システム開発および保守時の情報のセキュリティ保持のために、変更管理手順を

厳格に実施する。

(4)事業継続管理

セキュリティ障害及びサービス喪失に伴う影響を分析(リスクアセスメント)し、事業継続に対する計画を、試験・維持し、定期的に再評価を行う。

(5)情報セキュリティの管理体制

XXX においては、XXX 病院長の責任の元に、情報セキュリティの維持、管理を行うための委員会を設置する。また、個人情報管理室という専門の部門を設置し、セキュリティ・個人情報保護には特段の配慮を行う。情報の公開に関しては情報セキュリティ管理委員会において詳細を定める。

セキュリティ上の要求事項および知的所有権、個人情報の収集・利用に関し、適用法令を識別し、違反を避けるよう留意する。

4.【関連する法律・規範】

セキュリティ上の要求事項および知的所有権、個人情報の収集・利用に関し、適用法令を識別し、尊重する。以下に、関連する法令を掲げる。

(1)医薬品の臨床試験の実施の基準(GCP:Good Clinical Practice)

(2)遺伝子に関連する指針等

「ヒトゲノム・遺伝子解析研究に関する倫理指針」(平成 13 年 3 月 29 日　文部科学省　厚生労働省、経済産業省:いわゆる三省指針)、およびこれに関連する法令・規範

(3)プライバシー保護関連

a. 国家公務員法・地方公務員法・労働安全衛生法・医療法　等に定める「秘密を守る義務」

b. 個人情報保護法案:3 月 31 日現在　国会にて検討中

(4)海外の法律・規範

a. FDA 規則 21CFR　PART11

b. HIPPA プライバシー&セキュリティ

5.　【見直し及び評価】

本情報セキュリティ基本方針は、定例的に見直すと共に、その必要が発生した場合には、システムセキュリテイ統括責任者が情報セキュリティ管理委員会に諮って、定められた手続きに則って速やかに修正・追加を行う。

—以上—

厚生労働科学研究費補助金（医療技術評価総合研究事業）
分担研究報告書

情報セキュリティポリシ、認証局実施規程に関する研究
添付資料 2
プライバシポリシ

# プライバシポリシ

XXX 保健医療機関（以下、XXX）は保健医療機関であり、保健医療情報を取り扱っている。

1．　基本方針

個人情報は個人の重要な財産である。 XXX で業務に従事するすべての者は、個人情報保護に関するコンプライアンス・プログラム(CP)を遵守し、個人情報を正確かつ、安全に取り扱うことにより、検体を提供する人の個人情報を守り、その信頼にこたえなければならない。

2．　目的

XXX に収集される個人情報が、適切な方法で収集され利用されることを保証するために、CP を定め、これに基づき実施し･維持し、さらに継続的にこれを改善してゆくことを目的とする。

3．　組織活動

基本方針を具体化するために、以下の活動を行う。

（1） XXX の職員および XXX を利用する研究員は、個人情報に関する法令及びその他の規範を遵守する。

（2） 個人情報保護管理者を選任し、CP の実施及び運用に関する責任を与え、業務を行わせる。

（3） 監査責任者を選任し、監査を実施する。

（4） 監査に基づき、社内の規定、運用の仕方を改善する。

（5） 取引のある企業･機関及び個人に対し、規程の目的達成のための協力を要請する。

（6） 本基本方針は、ホームページに掲載し、随時閲覧可能とする。

（7） CP は定期的・継続的に改善する。

4．　個人情報の取り扱い

（1） 個人情報の収集・提供・預託・利用について

XXX は個人情報の収集に当たり、収集目的を明らかにし、収集した個人情報の使用範囲を限定し、適正に取り扱う。

（2） 権利の尊重

XXX は個人情報に関する個人の権利を尊重し、自己の個人情報に対し、開示、訂正、削除を求められたときは、合理的な期間、妥当な範囲内でこれに応ずる。

（3） 安全対策の実施

XXX は、個人情報が外部に流出する、不当に改竄されるなどといったトラブルを引き起こさないよう、セキュリテイポリシーを策定し、内部規定を整備し、安全対策を実施する。

－以上－

厚生労働科学研究費補助金（医療技術評価総合研究事業）
分担研究報告書

情報セキュリティポリシ、認証局実施規程に関する研究
添付資料 3
認証局実施規程

XXX 病院

# 認証局認証実施規程

Ver1.0

平成 15 年 4 月 1 日

# 目次

# 1. はじめに

## 1.1. 概要

### 1.1.1. 本認証実施規程の適用範囲

XXX 病院（以下、XXX という）認証実施規程(Certification Practice Statement、以下 CPS という)は、XXX 認証局が行う証明書発行、失効、及び証明書を基礎とする公開鍵基盤(PKI：Public Key Infrastructure)の運用維持に関する諸手続きおよび証明書発行、利用にかかわる主体の責任を記述したものである。XXX 認証局では、証明書所有者の私有鍵や証明書の格納媒体として IC カードを用いる。

XXX 認証局は、ルート認証局より CA 証明書の発行を受け、ルート認証局の下位認証局として活動する。

本 CPS は、医療従事者用公開鍵証明書、患者・保健医療福祉サービス利用者用公開鍵証明書および医療機関・保健医療福祉サービス供給組織用公開鍵証明書を発行する「ヘルスケア PKI 認証局」証明書ポリシ(以下 CP という)に従い、XXX 認証局が発行するすべての証明書に適用されるものとする。ヘルスケア PKI とは、保健医療福祉分野において医療情報を地域で連携して利用するための PKI である。

本 CPS と CP が抵触する場合には、CP が優先する。

### 1.1.2. 本規程が依拠する文書

ISO/DTS17090-1 保健医療情報 – 「公開鍵基盤 パート 1: フレームワーク、概観」
ISO/DTS17090-2 保健医療情報 – 「公開鍵基盤 パート 2: 証明書プロファイル」
ISO/DTS17090-3 保健医療情報 – 「公開鍵基盤 パート 3: 認証局のポリシ管理」

### 1.1.3. 本規程が参照する文書

ISO 17799-1:2000　情報技術 － 情報セキュリティ管理の運用規程
IETF/RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols
IETF/RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework
IETF/RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP

IETF/RFC 3280 Internet X.509 Public Key Infrastructure: Certificate and CRL Profile
US FIPS 140-1、140-2(Federal Information Processing Standard) : Security Requirements for Cryptographic Modules (http://csrc.nist.gov/cryptval/)
JIS X 5080:2002：情報技術－情報セキュリティマナジメントの実践のための規範(ISO/IEC17799:2000)
電子署名及び認証業務に関する法律（平成 12 年 5 月 31 日　法律第 102 号）
電子署名及び認証業務に関する法律施行規則（平成 13 年 3 月 27 日　総務省・法務省・経済産業省令第 2 号）
電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成 13 年 4 月 27 日　総務省・法務省・経済産業省告示第 2 号）

## 1.2. 本 CPS の名称と関連するオブジェクト識別子

本 CPS の名称を、「XXX 認証局認証実施規程」とする。XXX 認証局にて発行する証明書及び関連サービスに割り当てられたオブジェクト識別子（OID）を以下に示す。

XXX 認証局の OID：????. ????. ????. ????. ????

## 1.3. 本証明書が流通するコミュニティと証明書の適用範囲

### 1.3.1. 認証局（Certification Authority）

XXX 認証局（以下、本 CA という）は、運用管理する機関として証明書発行局（以下 IA）と登録局（以下 RA）により構成される。
IA は証明書の作成、発行、失効及び失効情報の開示及び保管の各業務を行う。

### 1.3.2. 登録局（Registration Authority）

RA は、適切な申請者の本人確認、登録の業務を行う。IA への証明書登録の業務は、ヘルスケア PKI のインタフェースを用いて安全に IA にオンラインでアクセスする。なお、証明書登録の業務は、発行、失効の作業を含む。

### 1.3.3. エンドエンティティ（End Entity）