

特定個人情報の取扱いに関する
基本方針及び取扱規程について
<後期高齢者医療広域連合>

(調整中)

内 容

1. 特定個人情報の取扱いについて
2. 個人情報保護方針
3. 情報セキュリティ基本方針
4. 運用管理規程
5. 機密文書管理規程

特定個人情報の取扱いについて

後期高齢者医療広域連合は、個人番号及び特定個人情報の適正な取扱いの確保について組織として取り組むために、付録 4「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」を遵守して、個人番号及び特定個人情報の安全管理に関する基本方針を策定し、職員及び関係者に明示します。また、策定された基本方針に基づき、取扱規程等を策定します。

また、特定個人情報に関し、番号法に特段の規定がなく個人情報保護法が適用される部分については、「健康保険組合等における個人情報の適切な取扱いのためのガイドライン」¹が遵守されていることを前提としています。

ここでは、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」に基づいて、既存の取扱規程等の見直しのポイントを示します。なお、見直しのポイントを反映した「個人情報保護方針」、「情報セキュリティ基本方針」、「運用管理規程」及び「機密文書管理規定」の雛形を示しますので、必要であれば参考としてご利用ください。なお、雛形は各保険者の実状に合わせて追記・修正してください。既存の規定等を有していない場合は、雛形を参考にして、実状に合わせて新規策定してください。

用語の定義については、（付録 4「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」 P3~4 参照してください。

1. 見直しのポイント

・番号法で定められた業務以外は個人番号を利用することができない

個人番号は、番号法があらかじめ限定的に定めた事務の範囲の中から、具体的な利用目的を特定した上で、利用するのが原則となっております。

・医療保険者は「番号法別表 1 を根拠にした医療保険事務」で個人番号を利用することができる

別添資料 9 個人番号を利用できる具体的な手続（帳票）一覧にて確認できる事務において、個人番号が利用できます。

・本人の同意があっても定められた事務以外で利用できない

個人情報保護法とは異なり、本人の同意があつたとしても、例外として認められる場合を除き、これらの事務以外で個人番号を利用することはできません。

・死者の個人番号は安全管理措置の対象に含まれる

個人情報保護法においては、保護の対象は、「生存する」個人情報であり、死者に関する情報については、保護の対象とはなりません。番号法における特定個人情報についても同様の取扱いとなります。一方、特定個人情報のうち、個人番号については、生存者の個人番号であることが要件ではありませんので、死者の個人番号も安全管理措置の対象に含まれます。

¹ 健康保険組合等における個人情報の適切な取扱いのためのガイドライン、平成 16 年 12 月 27 日 厚生労働省

<http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/161227kenpo.pdf>

・ 個人番号記入欄を有す帳票は特定個人情報と同様な安全管理措置を講ずる

特定個人情報の定義に従えば、同じ帳票であっても、個人番号の記入の有無で特定個人情報と個人情報に区別されることになります。今後省令で指針が示されますが、既存の業務への影響を抑えるため、帳票への個人番号の記入は任意になることが想定されます。しかし、同じ手続のエビデンスとして保管・管理する帳票を個人番号の記入の有無で分けて管理することは、連番管理が困難になることによって、返って盗難・紛失に関するリスクを増大させることになります。

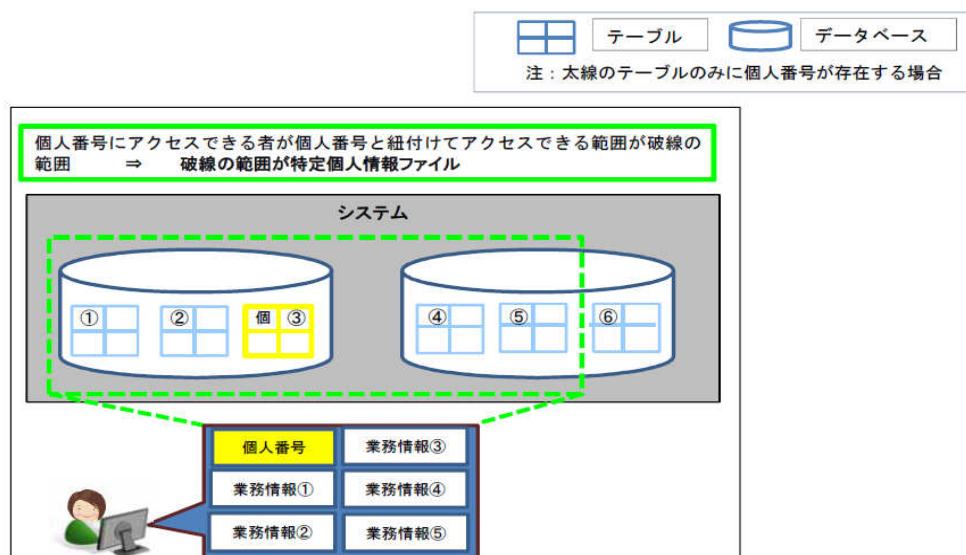
このため、同じ手続の帳票を一元管理するため、個人番号の記入欄のある帳票は、すべて特定個人情報と同様に取り扱うことが望まれます。

2. 情報システムにおける特定個人情報ファイルの範囲の明確化

特定個人情報ファイルとは、単に個人番号が含まれているテーブルのみを意味するのではなく、個人番号にアクセスできる者が、個人番号と紐付けてアクセスできる情報を意味しており、これが特定個人情報ファイルとなります。（番号法第2条第9項）

そのため、レセプト（現物給付）業務等、個人番号が利用できない業務の情報でも、システム上個人番号と紐づけがされている場合、特定個人情報ファイルとなりますので、特定個人情報ファイルと同等の安全管理措置が必要となります。現在の医療保険の給付・徴収関係のデータベース及びファイルはすべて記号番号が入っており、特定個人情報に紐付けられる可能性のあるファイルとして、特定個人情報ファイルとして扱うことが懸念されます。そのため、適切なアクセス制御が望まれます。

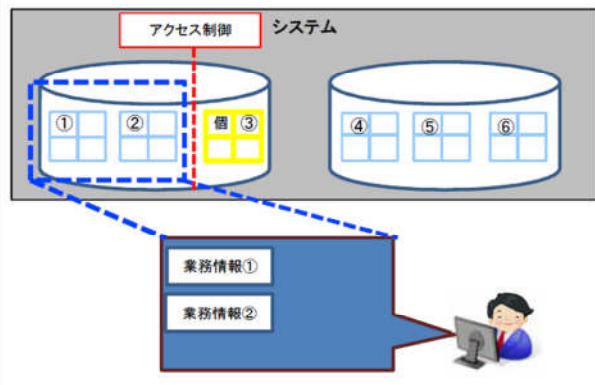
図表 1 特定個人情報ファイルの考え方



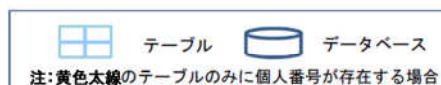
- アクセス制御等により、不正アクセスを行わない限り、個人番号を含むテーブルにアクセスできない場合は、原則、特定個人情報ファイルには該当しない。



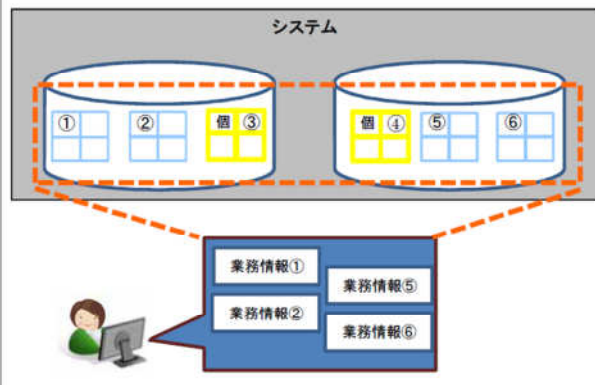
破線のテーブルにアクセスできる者は、アクセス制御により個人番号にアクセスできない ⇒ 破線の範囲は特定個人情報ファイルではない



- 個人番号が画面上表示されない場合であっても、システム上で個人番号にアクセスし、システム内部で検索キーとして個人番号を利用する場合などは、特定個人情報ファイルに該当する。

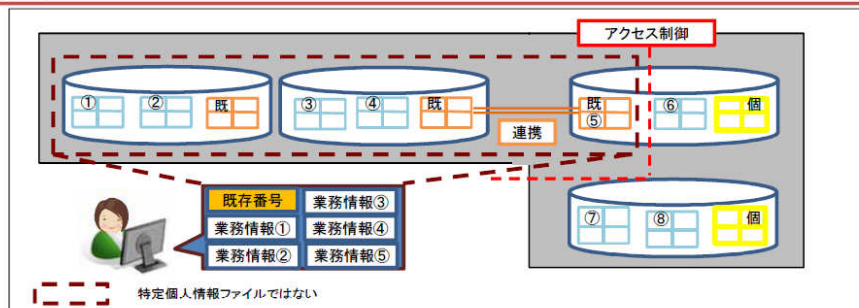


個人番号にアクセスできないが、システム内部で個人番号が検索キーとして利用され、個人番号により紐付けてアクセスできる ⇒ 破線の範囲は特定個人情報ファイル

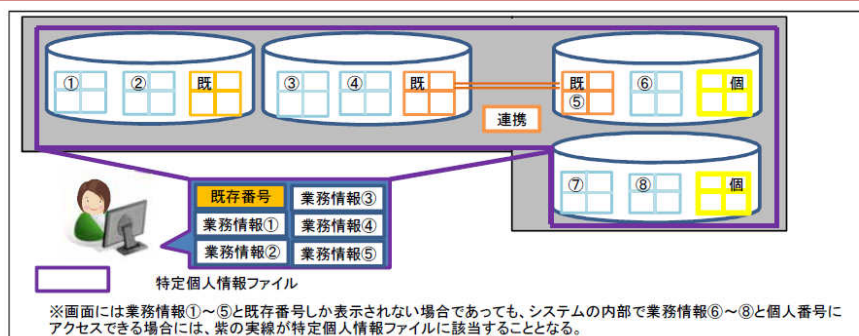


既存番号で連携している場合の特定個人情報ファイルの考え方

既存番号で連携している場合であって、アクセス制御等により個人番号そのものにはアクセスできず、個人番号以外の情報のみアクセスできるように制御されている場合は、特定個人情報には該当しない。



既存番号で連携している場合であっても、アクセス制御がされておらず、個人番号そのものにアクセスできる場合は、特定個人情報ファイルに該当する。



出典：内閣府、特定個人情報保護委員会、平成26年6月3日：特定個人情報保護評価に関する都道府県・指定都市説明会配布資料

【雛形】 個人情報保護方針

改 訂 履 歴

版数	改訂年月日	改訂内容
1.0	20xx 年 xx 月 xx 日	新規制定

※ 版数は新規制定を第 1.0 版とし、改訂が発生した際は第 1.1 版とする。

※ 改訂があった場合は、必ず改訂内容を記載すること。

目次

1. 基本理念	1
2. 個人情報の範囲.....	1
3. 個人情報の取扱いについて.....	1
4. 法令等の遵守について.....	1
5. 安全管理措置について.....	1
6. 問い合わせ窓口.....	1
7. 個人情報保護の仕組みの改善	2

1. 基本理念

〇〇〇〇（以下「当〇〇」という。）は、常日頃より加入者の視点に立ち、よりよい加入者サービスの提供を目標として、医療保険業務を営んでいます。加入者に応じて迅速で的確なサービスを提供させていただくためには、加入者に関する様々な情報が必要です。加入者と確かな信頼関係を築き上げ、安心してサービスを受けていただくために、加入者の個人情報の安全な管理は必須です。当〇〇では下記の方針に基づき、個人情報保護に厳重な注意を払います。

本方針は、加入者の個人情報のみならず、当の職員情報など、当〇〇が取り扱う全ての個人情報についても適用します。

2. 個人情報の範囲

当〇〇の取扱う個人情報は、適用・給付・徴収に係る医療保険業務、健診・検診に係る保健業務、〇〇当の人事・給与、資産管理、財務会計等に係る業務に必要な個人に係る情報のすべてを指します。個人情報は、特定個人情報も含みます。特定個人情報は、個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報を指します。法令の定める業務範囲の手続において、個人番号の記入欄のある様式を用いて得られた情報については、様式に個人番号の記入がない個人情報も特定個人情報と同様に取り扱います。

3. 個人情報の取扱いについて

当〇〇は、個人情報の取得にあたって、健康保険法等で取得が義務付けられている場合を除き、予め利用目的を明確にし、同意を頂いた上で取得します。

個人情報の利用及び提供については、同意を頂いた利用目的の達成に必要な範囲内において利用及び提供を行います。また、法令等で定められた場合を除き、目的外利用や第三者提供を行わないこととし、そのための措置を講じます。

特定個人情報については、下記の場合以外の場合は、利用目的の範囲を超えて、利用しません。

①行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）（以下「番号法」という。）第 9 条第 4 項の規定に基づく場合

②人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意があり、又は本人の同意を得ることが困難であるとき。

また、特定個人情報については、番号法第 19 条各号のいずれかに該当する場合を除き、提供しません。

4. 法令等の遵守について

当〇〇は、個人情報保護及び特定個人情報保護に関する日本の法令、国が定める指針その他の規範を遵守します。

5. 安全管理措置について

当〇〇は、加入者の個人情報への不正アクセス、紛失、破壊、改ざん及び漏えいを防止し、安全で正確な管理に努めます。

外部委託事業者に対して、適切な監督を行います。

6. 問い合わせ窓口

当〇〇における個人情報の取扱いに関するお問い合わせは下記の相談窓口で受けます。

個人情報保護相談窓口 電話 xxx-xxx-xxxx
e-mail privacy@xxxx.jp

7. 個人情報保護の仕組みの改善

当〇〇は、個人情報保護のための運用ルールを整備し、それに基づいて加入者の情報を管理します。また、この運用ルールは適宜見直し、継続的な改善を図ります。

制定日 〇〇年〇月〇日

改定日 〇〇年〇月〇日

〇〇〇〇
理事長 ××××

【雛形】 情報セキュリティ基本方針

改 訂 履 歴

版数	改訂年月日	改訂内容
1.0	20xx 年 xx 月 xx 日	新規制定

※ 版数は新規制定を第 1.0 版とし、改訂が発生した際は第 1.1 版とする。

※ 改訂があった場合は、必ず改訂内容を記載すること。

目 次

1. 総則	1
1. 1 目的	1
1. 2 適用範囲	1
1. 3 定義	1
2. 基本原則	2
3. 管理運営体制	2
3. 1 ポリシーの管理体制	2
3. 2 情報システムの運用体制	2
3. 3 苦情・質問窓口の設置	2
4. 管理方法	4
4. 1 情報の管理	4
4. 2 保管期間	4
4. 3 利用者識別	4
4. 4 監督及び教育	4
4. 5 事故の予防と対応	4
4. 6 罰則規程	4
5. ポリシーの維持管理	4
5. 1 ポリシーの改訂及び公開	4
5. 2 監査及び是正措置	5

1. 総則

1. 1 目的

本規程は、〇〇（以下、「当〇〇」という）の取り扱う個人情報、故意、過失、偶然の区別に関係なく、改ざん、破壊、漏洩から保護すると共に、個人情報を利用する役職員に対して、情報システムに関する安全管理の重要性、及び個人情報の適切な取り扱いと保護についての認識を高め、医療保険者としての信頼感と安心感の向上を図る事を目的として制定する。

1. 2 適用範囲

1) 適用対象者

情報セキュリティ基本方針（以下、「ポリシー」という）は、役員、職員、契約社員、嘱託社員、出向社員、派遣社員、パート、ボランティア及び実習生等（以下、「役職員」という）の雇用形態、職位、資格、勤務地を問わず、全役職員に対して適用する。ただし、ポリシーの対象となる業務を外部に委託する場合には、別途、本ポリシーに準拠した内容の外部委託契約を締結する。

2) 適用情報

ポリシーは、情報システムで取り扱う電子情報だけでなく、情報システムへ入力する前の紙媒体の情報や、役職員の履歴書等全ての個人情報に対して適用する。当〇〇が遵守すべき具体的な事項は、ポリシーに基づいた物理的、組織的、技術的及び人的な対策を、情報システムに関する「運用管理規程」及び紙媒体の情報に関する「機密文書管理規程」にまとめる。

1. 3 定義

1) 情報セキュリティポリシー（以下、「ポリシー」という）

ポリシーとは、組織内にある情報を安全に運用するための規約を文書化したものである。本規程のポリシーは、当〇〇の「個人情報保護方針」に基づいて、当〇〇の情報システムに関する安全管理についての基本姿勢を示したものである。

2) 個人情報

個人情報とは、氏名、住所、生年月日、性別等の個人を特定できる情報または他の情報と組合せて個人を特定できる情報を含んだ情報をいう。なお、個人情報は、特定個人情報も含む。特定個人情報は、個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報を指す。

個人情報保護法においては、保護の対象は、「生存する」個人情報であり、死者に関する情報については、保護の対象とならない。番号法における特定個人情報についても同様の取扱いとなるが、特定個人情報のうち、個人番号については、生存者の個人番号であることが要件でないため、死者の個人番号も保護の対象となる。

法令の定める業務範囲の手続において、個人番号の記入欄のある様式を用いて得

られた情報については、様式に個人番号の記入がない個人情報も特定個人情報と同様に取り扱う。

3) 情報システム

情報システムとは、当〇〇で運用する適用、給付、徴収に係る医療保険業務に適用する医療保険システム、健診、検診に係る保健業務に適用する保健システム及び当〇〇の人事・給与、資産管理、財務会計等に係る業務に適用する業務システム並びにこれらのシステムへの接続機器などをいう。

2. 基本原則

当〇〇の情報システムは、次に掲げる基本原則により運用する。

- 1) 保存義務のある情報の電子媒体による保存については、情報の真正性、見読性、保存性を確保する。
- 2) 情報システムの利用に当たっては、守秘義務を遵守し、加入者個人の情報を保護する。
- 3) 情報システムへのコンピュータウィルスの侵入及び外部からの不正アクセスに対して必要な対策を講じる。原則、ソフトウェアのインストール及びUSBメモリ等の外部記憶媒体の接続を禁止する。

3. 管理運営体制

3. 1 ポリシーの管理体制

- 1) ポリシーは、情報システム管理委員会（以下、「委員会」という）を設置して、委員会が維持管理を行う。
- 2) 委員会は、委員長を置き、理事長をもってこれに充てる。
- 3) 各部署の長は、委員会の指示を受け、各部署に置いてポリシーが遵守されるように指導、教育を行う。

3. 2 情報システムの運用体制

- 1) 情報システムについては、運用責任者を置き、理事長、又は事務長をもってこれに充てる。
- 2) 運用責任者は、情報システムの安全管理に必要な、組織的、人的、技術的、物理的対策を実施し、維持し、かつ、改善するために不可欠な資源を用意する。
- 3) 運用責任者は、情報システムを円滑に運用するため、情報システムに関する運用を担当するシステム管理者を内部の者から指名することができる。

3. 3 苦情・質問窓口の設置

個人情報の取扱い及び情報システムの運用に関して、本人及びシステム利用者からの苦

情及び質問を受け付け、適切かつ迅速な対応を行うために、苦情・質問を受け付ける窓口（ヘルプデスク）を設ける。

4. 管理方法

4. 1 情報の管理

情報システムで取扱う情報は、情報の取得から利用・保管・廃棄までの情報の取扱いの流れに沿ったリスク分析を実施し、リスクに対応した適切な取り扱い方法を運用管理規程、機密文書管理規程、他各種手順書等に規定して、適切に管理・運用する。

4. 2 保管期間

情報システムで取扱う情報は、法令に定められた保管期間を基本として別途定める。また、情報システムへのアクセスログを記録し、その記録を最低〇年保管する。

4. 3 利用者識別

情報システムの利用者の登録を管理し、そのアクセス権限を規定し、不正な利用を防止する。

4. 4 監督及び教育

委員会は、全ての役職員に対して、情報セキュリティの重要性と、個人情報の適切な取り扱い、及び安全管理について意識面及び技術面の向上を目的として、必要かつ適切な監督及び継続的な教育を行う。

4. 5 事故の予防と対応

当〇〇は、ポリシーの遵守により、情報漏えい事故等の発生の予防に努める。万一、事故が発生した場合には、その事実を速やかに公表し、再発防止策を含む適切な対策を速やかに講じる。

4. 6 罰則規程

委員会は、役職員がポリシーに違反して、当〇〇の情報セキュリティに重大な影響を与えた場合、又はそれに準ずる悪質な行為などが認められた場合、当〇〇の就業規則に基づいた処罰を勧告することができる。

5. ポリシーの維持管理

5. 1 ポリシーの改訂及び公開

- 1) ポリシーは、以下のような場合等を想定して、委員会の決議・承認及び運用責任者の承認を経て改訂する。
 - a) IT 技術の発展とポリシーの整合性を維持する必要がある場合
 - b) 社会環境の変化とポリシーの整合性を維持する必要がある場合
 - c) 法令及び標準規格等とポリシーの整合性を維持する必要がある場合
- 2) 各部門で作成した運用規程については部門長の承認を経て改訂することができる。
- 3) 改訂されたポリシー並びに運用管理規程は、改訂後即時に役職員に向けて公開する。

原則として、当〇〇の外部に向けては公開しない。

5. 2 監査及び是正措置

- 1) 情報システムの適正な運用とその有効性を維持するために、毎年1回内部監査を実施する。ただし、高度な技術を要する監査が必要な場合は、外部の専門家による外部監査を導入する。
- 2) 運用責任者は、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じる。

以上

【雛形】 運用管理規程

改 訂 履 歴

版数	改訂年月日	改訂内容
1.0	20xx 年 xx 月 xx 日	新規制定

※ 版数は新規制定を第 1.0 版とし、改訂が発生した際は第 1.1 版とする。

※ 改訂があった場合は、必ず改訂内容を記載する。

目次

1. 総則	1
1. 1 目的	1
1. 2 適用対象	1
1. 3 標準規格	1
2. 組織的な対策	1
2. 1 管理運営体制	1
2. 1. 1 体制及び責任者	1
2. 1. 2 管理者及び利用者の責務	2
2. 2 具体的な対策	3
2. 2. 1 予防処置及び是正処置	3
2. 2. 2 事故への対応	4
2. 2. 3 非常時の対策	4
2. 2. 4 監査	5
2. 2. 5 苦情・質問受付	5
2. 3 守秘契約	5
2. 4 業務委託	5
2. 4. 1 委託契約	5
2. 4. 2 再委託	6
2. 4. 3 作業確認	6
3. 人的な対策	6
3. 1 マニュアルの整備	6
3. 2 研修の内容	6
3. 3 職員への周知	6
4. 物理的な対策	7
4. 1 立入り領域の制限	7
4. 1. 1 立入り領域の定義	7
4. 1. 2 執務室等	7
4. 1. 3 サーバー室等	7
4. 2 情報システム	7
4. 2. 1 サーバー室等管理	7
4. 2. 2 端末管理	7
4. 2. 3 ネットワーク管理	8
4. 2. 4 外部機関との情報交換	8
4. 2. 5 電子媒体の管理	8
4. 2. 6 文書管理	8
4. 3 情報及び情報機器の持出し及びリモートアクセス管理	9
4. 3. 1 対象となる情報及び情報機器	9
4. 3. 2 情報の持出し管理	9
4. 3. 3 情報機器の持出し管理	9

4. 3. 4 情報機器のリモートアクセス管理	9
4. 3. 5 盗難、紛失時の対応	10
5. 技術的な対策	10
5. 1 利用者の登録・認証	10
5. 2 サーバー管理	11
5. 2. 1 サーバーの運用	11
5. 2. 2 アクセス管理	11
5. 2. 3 情報のバックアップ	12
5. 2. 4 リスク対応（障害対策）	12
5. 3 端末管理	13
5. 4 ネットワーク管理	13
5. 4. 1 LAN 管理	13
5. 4. 2 インターネットの利用・管理	13
5. 4. 3 電子メールの利用・管理	13
5. 4. 4 無線 LAN の管理	14
5. 5 一般的な運用事項	14
5. 5. 1 セキュリティパッチの適用	14
5. 5. 2 ウィルス対策	14
5. 5. 3 電子媒体の管理	15
5. 5. 4 電子署名・タイムスタンプ	15
6. その他	15

1. 総則

1. 1 目的

運用管理規程（以下、「本規程」という）本規程は、〇〇〇〇（以下、「当〇〇」という）の情報セキュリティ基本方針（以下、「ポリシー」という）に従い、当〇〇の業務を取り扱うシステム（以下、「情報システム」という）の安全かつ合理的な運用を図り、併せて法令に保存が義務付けられている書類の電子媒体による運用（電子保存システム）の適正な管理を図るために必要な事項を定めることを目的とする。

1. 2 適用対象

1) 情報システム

情報システムとは、当〇〇で運用する適用、給付、徴収に係る医療保険業務に適用する医療保険システム、健診、検診に係る保健業務に適用する保健システム及び当〇〇の人事・給与、資産管理、財務会計等に係る業務に適用する業務システム並びにこれらのシステムへの接続機器などをいう。

2) 適用する情報

管理対象となる情報は、情報システムで取り扱う電子情報だけでなく、情報システムへ入力する前の紙媒体の情報や、従業者の履歴書等全ての個人情報を適用対象とする。なお、個人情報には、特定個人情報も含む。特定個人情報は、個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報を指す。

個人情報保護法においては、保護の対象は、「生存する」個人情報であり、死者に関する情報については、保護の対象とならない。番号法における特定個人情報についても同様の取扱いとなるが、特定個人情報のうち、個人番号については、生存者の個人番号であることが要件でないため、死者の個人番号も保護の対象となる。

法令の定める業務範囲の手続において、個人番号の記入欄のある様式を用いて得られた情報については、様式に個人番号の記入がない個人情報も特定個人情報と同様に取り扱う。

1. 3 標準規格

システム管理者は、システム変更・改定時の対象とするため、当〇〇でフォローすべき法令及び標準規格の列挙を行い、変更状況を確認し維持する。

2. 組織的な対策

2. 1 管理運営体制

2. 1. 1 体制及び責任者

- 1) ポリシーの遵守及び本規程の実施に必要な事項について、情報システム管理委員会（以下、「委員会」という）の審議を経て、本運用管理規程に定める。
- 2) 運用責任者は、情報システムを安全に運用並びに改善するために必要な資源を用意する。
- 3) 情報システムの運用管理者またはシステム管理者（以下、「運用管理者等」という）

は、本規程に定められた組織的、人的、技術的、物理的対策を実施して、情報システムを円滑に運用できるようにする。

- 4) 委員会は、情報システムを複数の部門で運用する必要がある場合、情報システム部門管理者（以下、「部門管理者」という）を各部門に任命して、情報システムを円滑に管理運営できるようにすることができる。
- 5) 委員会は、情報システムを監査するため、公平かつ客観的な立場にある情報システム監査責任者（以下、「監査責任者」という）を置き、内部の者から指名する。

2. 1. 2 管理者及び利用者の責務

1) 運用責任者の責務

- a) 情報システムの機能要件に挙げられている機能が支障なく運用される環境を整備する。
- b) 加入者又は利用者からの、情報システムについての苦情を受け付ける窓口を設ける。
- c) 監査責任者に監査を実施させ、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な処置を講じる。

2) システム管理者の責務

- a) 情報システムに用いる機器及びソフトウェアを導入するに当たって、システムの機能を確認する。
- b) 個人情報の安全性を確保し、常に利用可能な状態に置いておく。
- c) 機器やソフトウェアに変更があった場合においても、情報が継続的に使用できるよう維持する。
- d) 情報システムの利用者の登録を、人事異動等による利用者の担当業務の変更等に併せて管理し、そのアクセス権限を規定し、不正な利用を防止する。
- e) 情報システムを正しく利用させるため、作業手順書の整備を行い利用者の教育と訓練を行う。
- f) 情報システムの安全管理の見直し及び改善の基礎として、運用責任者に情報システムの運用状況を報告する。

3) 監査責任者の責務

- a) 監査責任者は、監査計画を立案し、監査を指揮し、監査報告書を作成し、運用責任者に報告する。
- b) 監査責任者は、情報システムの監査を円滑に実施するため、情報システムに関する監査を担当する監査員を置くことができる。
- c) 監査員の選定及び監査の実施においては、監査の客観性及び公平性を確保する。
- d) 監査員は自らの所属する部門を監査しない。

4) 情報システム部門管理者の責務

- a) 情報システム部門管理者（以下、「部門管理者」という）は、自部門のシステムの運に管理に責任を持つ。

- b) 部門管理者は、自部門のマスタを管理する。
- c) 自部門のマスタに変更・追加が生じた場合には、速やかに書面をもって関連部署部門管理者ならびにシステム管理者に提出する。
- d) 制度改正が生じる場合、改正事項の解析とプログラム修正計画書を情報システム管理委員会に提出し、承認を得る。
- e) マスタの変更の際に、過去の情報に対する内容の変更が起こらない機能を備える。

5) 利用者の責務

- a) 利用者は、情報システムの情報の参照や入力（以下「アクセス」という。）に際して、認証番号やパスワード等によって、システムに自身を認識させる。
- b) 利用者は、自身の認証番号やパスワードを管理し、これを他者に利用させない。
- c) 利用者が、正当な認証番号及びパスワード等の管理を行わないために生じた事故や障害に対しては、その利用者が責任を負う。
- d) 利用者は、情報システムへの情報入力に際して、確定操作（入力情報が正しい事を確認する操作）を行って、入力情報に対する責任を明示する。
- e) 利用者は、与えられたアクセス権限を越えた操作を行わない。
- f) 利用者は、情報システム及び参照した情報を、目的外に利用しない。
- g) 利用者は、加入者等のプライバシーを尊重し、職務上知ることが必要な情報以外の情報にアクセスしてはならない。
- h) 利用者は、法令上の守秘義務の有無に関わらず、アクセスにより知り得た情報を目的外に利用し、又は正当な理由なしに漏らしてはならない。異動、退職等により職務を離れた場合においても同様である。
- i) 利用者は、システムの異常を発見した場合、速やかに運用責任者に連絡し、その指示に従う。
- j) 利用者は、不正アクセスを発見した場合、速やかに運用責任者に連絡し、その指示に従う。
- k) 利用者は、離席する際は、窃視防止策を実施する（ログアウトまたはスクリーンロック等）。尚、不特定多数の者が出入する部署においては、必要に応じて偏光フィルム等による窃視防止処置を講ずる。
- l) ウィルスに感染又はその恐れを発見した場合は、ネットワークから端末を切り離すとともに、システム管理者へ連絡し、指示を仰ぎ、その指示に従う。

2. 2 具体的な対策

2. 2. 1 予防処置及び是正処置

- 1) 委員会は、加入者、システム利用者等からの苦情、緊急事態の発生、監査報告、外部審査機関等からの指摘で、システムの機能、運用状況等に問題がある場合には、問題に対する予防処置及び是正処置（以下、「処置等」という）のための責任及び権限を定め、処置等の手順を定めて、これを実施させる。
- 2) 運用責任者は、適切な情報システムの運用を維持するため、少なくとも年に1回、本

規程に関わる次の事項を委員会に報告して、本規程の見直しについて審議する。

- a) 監査及びシステム管理者の運用状況に関する報告
- b) 苦情を含む外部からの意見
- c) 前回までの見直しの結果に対するフォローアップ
- d) 安全管理 GL 等の標準規格や法令等の規範の改正状況
- e) 社会の情勢等の変化、国民の認識の変化、技術の進歩などの諸環境の変化
- f) 情報システムの運用状況の変化
- g) 内外から寄せられた改善のための提案

3) 処置等は、以下のような手順で行う。

- a) 発生した問題の内容を確認して、問題の原因を特定する。
- b) 発生した問題の処置等を立案する。
- c) 立案された処置等について、期限を定めて実施して、実施結果を確認する。
- d) 実施された処置等の有効性を確認する。
- e) 発生した問題について、問題の内容、原因、実施した処置等の実施結果及び有効性を記録する。

2. 2. 2 事故への対応

- 1) 委員会は、事故が発生した場合は、再発防止策を含む適切な対策を速やかに講じる。事故については、発生の実態及び再発防止策等の事実を速やかに公表する。
- 2) 運用責任者等は、事故等発生予防に努めるため、情報システムの扱う情報について、予見されるリスクを洗い出して、事故発生時の危険度を明確にして、リスクを回避する方法を提示するリスク分析を行う。リスクには、事業継続性を考慮して、災害及び障害も含める。
- 3) 運用責任者等は、リスク分析の結果は、台帳に記入して維持・管理する。
- 4) 運用管理者等は、緊急時及び災害時の連絡、復旧体制並びに回復手順を文書に定め、利用者に周知の上で常に利用可能な状態におく。

2. 2. 3 非常時の対策

- 1) 運用管理者は、災害、サイバー攻撃などにより医療保険サービスの提供体制に支障が発生する「非常時」の場合を想定して、非常時と判断するための基準、手順、判断者等の判断する仕組み、システムの閉塞及び縮退運用等の手順（以下、「非常時運用」という）及び正常状態への復帰手順を定めた事業継続計画（以下、「BCP」という）を策定する。
- 2) 運用管理者は、BCP を利用者に周知の上、常に利用可能な状態におく。
- 3) システム管理者は、非常時は BCP に則って、非常時運用を行う。
- 4) システム管理者は、正常状態への復帰後に、非常時運用した間の情報整合性を図る等、必要な処置を実施する。
- 5) 非常時に異常状態を通知する必要がある機関の連絡先一覧を準備して、非常時には速やかに連絡を取る。

2. 2. 4 監査

- 1) 当〇〇は、本運用管理規程の「医療情報システムの安全管理に関するガイドライン」への準拠状況及び情報システムの運用状況を毎年3月に監査する。
- 2) 運用責任者は、監査責任者から監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な処置等を講じる。
- 3) 監査の内容については、監査責任者が定める。
- 4) 運用責任者は必要な場合、臨時の監査を監査責任者に命ずることができる。

2. 2. 5 苦情・質問受付

- 1) 苦情・質問の受付窓口（以下、「受付窓口」という）は、個人情報の取扱い及び情報システムの運用に関して、加入者及びシステム利用者からの苦情及び質問を受け付ける。
- 2) 受付窓口は、直接または間接的に苦情を受けた際に、別途定められた手順に則って速やかに対応しなければならない。
- 3) 受付窓口は、受付けた苦情・質問を整理して、運用責任者に報告しなければならない。
- 4) 運用責任者は、受付窓口の報告を受け、問題点の指摘等がある場合には、直ちに必要な処置等を講じる。

2. 3 守秘契約

- 1) 当〇〇の業務従事者は在職中のみならず、退職後においても業務中に知った個人情報に関する守秘義務を負う。
- 2) 法令上の守秘義務のある者以外を採用する場合は、雇用及び契約時に守秘・非開示契約を締結する。

2. 4 業務委託

2. 4. 1 委託契約

業務を当〇〇外の所属者に委託する場合は、以下の処置を実施する。

- 1) 守秘事項を含む業務委託契約を結ぶ。契約の署名者は、その部門の長とする。
- 2) 各担当者は委託作業内容が個人情報保護の観点から適正に且つ安全に行われていることを確認する（委託先が、許可無く個人情報を含む情報を組織外に持出すことは禁止する）。
- 3) 業務委託の契約書には、次に示す事項を規定し、十分な個人情報の保護水準を担保する。
 - a) 個人情報の安全管理に関する事項
 - b) 事業所内からの個人情報の持出しの禁止
 - c) 個人情報の目的外利用の禁止
 - d) 再委託に関する事項（再委託する場合は、再委託の許諾を要件とする。また、再委託する事業者にも委託先と同等の義務を課すこと）
 - e) 個人情報の取扱状況に関する委託者への報告の内容及び頻度
 - f) 契約内容が遵守されていることを委託者が確認できる事項

- g) 契約内容が遵守されなかった場合の処置
- h) 事件・事故が発生した場合の報告・連絡に関する事項
- i) 漏えい事案等が発生した場合の委託先の責任に関する事項
- j) 一連の委託業務終了後に関する事項（終了報告、確実に情報を消去する等）
- k) 確実に削除又は破棄したことを証明書等により確認できる事項
- l) 保守要員のアカウント情報の管理に関する事項（適切に管理することを求める）
- m) 従業者に対する監督・教育

2. 4. 2 再委託

委託先事業者が再委託を行う場合は、当〇〇による再委託の許諾を要件とする。さらに、委託先と同等の個人情報保護に関する対策及び契約がなされていることを条件とする。さらに、当〇〇との業務委託の契約書に再委託での安全管理に関する事項を加える。

2. 4. 3 作業確認

- 1) システム管理者は、作業の管理・監督のため、システムの改修及び保守において、以下のような確認を実施する。
 - a) 保守要員用のアカウントの確認（保守要員個人の専用アカウントを使用すること）。
 - b) 保守作業等の情報システムに直接アクセスする作業の際には、作業中・作業内容・作業結果の確認（原則として日単位）。
 - c) 清掃等、直接情報システムにアクセスしない作業の場合の定期的なチェック。
 - d) 保守契約における個人情報保護の徹底。
 - e) 保守作業の安全性についてログによる確認。
- 2) システム管理者は、必要と認めた場合は適時監査を行う。

3. 人的な対策

運用責任者及び情報システム管理者は、情報セキュリティの重要性と、個人情報の適切な取り扱い、及び安全管理について意識面及び技術面の向上を目的として、必要かつ適切な監督及び継続的な教育を行う。

3. 1 マニュアルの整備

情報システム管理者は、情報システムの取扱いについてマニュアルを整備し、利用者に周知の上、常に利用可能な状態におく。

3. 2 研修の内容

情報システム管理者は、情報システムの利用者に対し、定期的に情報システムの取扱い及びプライバシー保護に関する研修を行う。また、研修時のテキスト、出席者リストを残す。

3. 3 職員への周知

- 1) システム管理者は、情報及び情報機器の持出しについてマニュアルを整備し、利用者

に周知の上、常に利用可能な状態におく。

- 2) システム管理者は、利用者に対し、情報及び情報機器の持出しについて研修を行う。
また、研修時のテキスト、出席者リストを残す。

4. 物理的な対策

4. 1 立入り領域の制限

4. 1. 1 立入り領域の定義

1) 執務室等

当〇〇の職員が執務する場所また部屋を執務室等という。

2) サーバー室等

スタッフの常駐または施錠できるセキュリティが保たれた管理領域を「サーバー室等」という。ただし、いずれも難しい場合は防犯カメラを設置する。

4. 1. 2 執務室等

部外者が執務室等に立ち入る場合は、その執務室の管理レベルに合わせた入退室記録の作成、同伴等の管理を実施する。

4. 1. 3 サーバー室等

- 1) システム管理者は、個人情報が保管されている機器（以下、「サーバー」という）及び記録媒体をサーバー室等に設置する。
- 2) システム管理者は、サーバー室等の出入口は常時施錠管理し、その入退室を記録・管理する。
- 3) サーバー室等への出入りは、システム管理者の承認を得て行う。サーバー室等への入退者は、全て名札を着用し、入退室の記録を残す。
- 4) システム管理者は、入退室の記録を定期的に確認して、問題があれば運用責任者に報告する。

4. 2 情報システム

4. 2. 1 サーバー室等管理

- 1) システム管理者は、サーバー室等における火災、その他の災害、盗難に備えて、非常電源装置、無停電装置、自動消火装置、監視カメラ、入退制限装置などによる必要な保安処置を講じなければならない。
- 2) システム管理者は、サーバー室等の温度、湿度等の環境を適切に保持する。

4. 2. 2 端末管理

- 1) 盗難の恐れがある端末（ノート PC 等）は、盗難防止用ワイヤーロックで固定するか、使用しない際は鍵のかかる保管庫に保管管理する。

- 2) 端末の使用に際しては、画面を廊下側に向けない、窃視防止フィルムを貼るなどの、窃視防止に努める。
- 3) PC の廃棄及びレンタル・リース切れによる PC の返却等に当たっては、ハードディスク等の既存情報を上書処理により書き換え、その後情報を消去する。
- 4) 情報を削除または廃棄した記録を保存する。
- 5) 情報の消去処理を外部業者に委託することができるが、その場合は、消去証明書を受領するものとする。

4. 2. 3 ネットワーク管理

- 1) 情報システムのネットワーク（以下、「LAN」という）は、インターネット等の当〇〇外と情報交換ができるネットワークとは技術的な対策を適用した上で接続する。
- 2) LAN へ接続を行う場合、利用者はシステム管理者に申請し、承認を得る。
- 3) 私有の PC を持込み、LAN に接続することは、原則禁止とする。業務上やむを得ず接続を要する場合は、システム管理者の許可を得て行うこととする。ただし、この場合、PC の使用にあたっては、業務用端末に準じた取扱いとする。
- 4) システム保守のため委託先等の部外者が PC を持込み LAN へ接続する場合は、システム管理者に申請し、許可を得てから行うこととする。

4. 2. 4 外部機関との情報交換

- 1) 医療保険者等、保守会社等、通信事業者、運用委託業者等の外部機関と医療保険情報を交換する場合、相手外部機関との間で、責任分界点や責任の所在を契約書等で明確にする。
- 2) システム管理者は、外部機関と医療保険情報を交換する場合、リスク分析を行い、安全に運用されるように技術的及び運用的対策を講じる。
- 3) リスク分析及びその技術的及び運用的対策の内容を文書化して、維持・管理する。
- 4) 定期的に監査を行って、外部機関との契約事項、技術的対策及び運用的対策が適切に実施されていることを確認する。

4. 2. 5 電子媒体の管理

- 1) 特に許可した場合を除き、情報のバックアップ業務以外には外部記憶媒体への個人情報情報の複写を禁止する。
- 2) 電子媒体の廃棄は、原則粉碎処理とする。
- 3) 個人情報を記録した可搬型記録媒体（FD、CD-ROM、DVD、USB メモリ等）は、施錠できるキャビネットに保管し、その所在を台帳に記録し、管理する。
- 4) 個人情報を可搬型記録媒体で授受する場合は、授受の記録を残す。
- 5) 個人情報を記した電子媒体の廃棄に当たっては、安全かつ確実に行われることを、システム管理者が作業前後に確認し、結果を記録に残す。

4. 2. 6 文書管理

- 1) 当〇〇は、以下の技術的と運用的対策の分担を定めた文書の管理を実施する。
- 2) 各システムはその設計時、運用開始時に技術的対策と運用による対策を、基準適合チ

チェックリストに記載し、必要時には第三者への説明に使える状態で保存する。

- 3) システムの保守時には、基準適合チェックリスト記載にしたがっていることを確認する。
- 4) システム改造時は、最新の基準適合チェックリストに従って、技術的対策と運用による対策の分担を見直す。

4. 3 情報及び情報機器の持出し及びリモートアクセス管理

4. 3. 1 対象となる情報及び情報機器

- 1) 委員会は、情報及び情報機器の持出しに関してリスク分析を実施し、持出し対象となる情報及び情報機器を規定し、それ以外の情報及び情報機器の持出しを禁止する。
- 2) 委員会は、持出し対象となる情報及び情報機器をまとめて、利用者に公開する。

4. 3. 2 情報の持出し管理

- 1) 情報は、所属、氏名、連絡先、持出す情報の内容、格納する媒体、持出す目的、期間をシステム管理者に承認を得て持出す。
- 2) 持出す情報については、暗号化、パスワードを設定する等、容易に内容を読み取られないようにする。

持出した情報は、例えばファイル交換ソフト（Winny 等）がインストールされた情報機器で取り扱わない。

4. 3. 3 情報機器の持出し管理

- 1) 情報機器は、所属、氏名、連絡先、持出す情報の内容、格納する媒体、持出す目的、期間をシステム管理者に承認を得て持出す。
- 2) 持出す情報機器については、以下のような対策を施す。
 - a) 起動パスワードを設定する。起動パスワードは、推定しやすいものは避け、また定期的に変更する。
 - b) ウィルス対策ソフトをインストールしておく。
 - c) 別途定められている以外のアプリケーションはインストールしない。
- 3) 持出した情報機器には、別途定められている以外のアプリケーションをインストールしない。
- 4) 持出した情報機器をネットワークに接続、または他の外部媒体を接続する場合は、ウィルス対策ソフトやパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施す。
- 5) システム管理者は、情報が格納された可搬媒体及び情報機器の所在について台帳に記録する。システム管理者は、その内容を定期的にチェックし、所在状況を把握する。

4. 3. 4 情報機器のリモートアクセス管理

- 1) 外部からアクセスを許容する情報機器（以下、「リモート端末」という）については、以下の内容を別に定める。
 - a) リモート端末及びリモートアクセス要件
 - b) リモート端末がリモートアクセス要件を保持していることを確認する手順

- c) 情報システムに不正な侵入等の攻撃を防止する技術的対策
 - 2) b) リモート端末がリモートアクセス要件を保持していることを定期的に確認する。
4. 3. 5 盗難、紛失時の対応
- 1) 持出した情報及び情報機器の盗難、紛失時には、速やかにシステム管理者に届け出る。
 - 2) 届け出を受け付けたシステム管理者は、その情報及び情報機器の重要度に従って対応する。
5. 技術的な対策
5. 1 利用者の登録・認証
- 1) システム管理者は、職員等の採用時、異動時、退職時に合わせ、速やかに利用者の認証情報の登録、変更、削除及び認証情報の発行の処置を取る。
 - 2) システム管理者は、情報システムの利用者等の申請を受け、情報システムへのアクセス権限を審査して、利用者登録を実施する。利用者登録実施後、利用者の認証に必要なデバイスまたは認証情報（以下、「認証情報等」という）を利用者に交付する。
 - 3) 利用者の認証は、以下の2つのいずれかの認証方式を用いることとする。
 - a) 公開鍵基盤（以下、「PKI」という）の秘密鍵及び PKI 証明書が格納された IC カードを用いる認証方式（以下、「IC カード認証」という）。
 - b) 利用者の ID とパスワードを用いる認証方式（以下、「ID・パスワード認証」という）。情報システムの重要度に応じて、生体認証等を用いた二要素認証を用いる。
 - 4) IC カード認証は、以下の要件とする。
 - a) IC カード及び PKI の鍵と証明書の交付は、個人単位とし共有することはない。
 - b) IC カードには、PKI の秘密鍵を安全な方法で格納する。
 - c) IC カードには、暗証番号を設定する。
 - d) 利用者は、IC カードの盗難・紛失の事実を知った後、速やかに IC カードの再発行依頼を提出する。システム管理者は、盗難・紛失した IC カードによるアクセスができないようにするため、当該 PKI の認証情報をシステムから削除する。システム管理者は、利用者に対して新しい PKI 情報の格納された IC カードを交付する。
 - e) 利用者は、盗難・紛失した IC カードが発見された場合は、速やかにシステム管理者に当該 IC カードを返却する。
 - 5) ID・パスワード認証
 - a) 利用者 ID の付与は、個人単位とし共有することはない。Administrator 等の OS のデフォルト ID は使用せず、個別 ID とする。
 - b) パスワードは8桁以上の英数記号を組み合わせたものとする。
 - c) パスワードの有効期限は、原則2ヶ月以内とし、利用者が更新する。システム管理者は、2ヶ月以上パスワードを更新しない利用者に対し、警告を与え、速やかに更新させるものとする。
 - d) 利用者が、パスワードの盗難・紛失の事実を知った後、システム管理者へ速や

かにパスワードの初期化依頼を提出する。システム管理者は、利用者からのパスワード紛失の申請書を受け、利用者登録の確認後、パスワードの初期化を行ない、利用者へ知らせることとする。

e) 利用者は、パスワードの初期化の通知後は、速やかにパスワードを変更することとする。

f) 利用者登録時は、システム管理者の登録処理による初期値のパスワードとし、その後速やかに、利用者が個々のパスワードへ変更する手順とし、システム管理者であってもパスワードを推定できない仕組みとする。

6) 利用者には、原則として利用者権限を付与し、管理者権限は付与しない。

5. 2 サーバー管理

5. 2. 1 サーバーの運用

1) システム管理者は、サーバーへのアクセス状況・稼動状況を定期的（月 1 回以上）に確認し、問題がある場合は、速やかに処置を講じる。

2) システム管理者は、個々のサーバー及び端末機のクロックを定期的（月 1 回以上）に確認するとともに、誤差が生じている場合は標準時間に設定し直す。

5. 2. 2 アクセス管理

1) システム管理者は、職務により定められた権限による情報アクセス範囲を定め、以下の内容に沿って、ハードウェア及びソフトウェアの設定を行う。

a) 情報区分とアクセス権限に基づくアクセスできる情報の範囲を定め、アクセス管理を行う。

b) 利用者のアクセスにおいては、利用者の認証を行う。利用者の認証には、「第 5. 1 節 利用者の登録・認証」にある原則に依らず、システム管理者の承認の上で、管理者権限を付与する。管理権限は、原則 2 名以下とする。

2) システム管理者は、情報システム、情報への使用状況を監視するため、以下の事項を含むアクセスログを取得する。

a) 利用者 ID

b) 端末 ID

c) 操作の日時

d) 情報へのアクセス結果（誰が、いつ、誰の情報に、どのようなアクセスをしたか）

3) 異常なアクセスを検知したときは警告を発して、ネットワークを切断する等の対処をする。

4) システム管理者は、取得したアクセスログを情報システムの重要度に合わせ定期的（月 1 回以上）に検証し、問題のないことを確認する。問題がある場合は、速やかに適切な処置を講じる。

5) システム管理者は、管理状況を運用責任者に報告をする。

6) アクセスログは、重要度に合わせ定めた方法・場所・期間に従い保管する。

7) アクセスログを廃棄する場合は、「第 4. 2. 5 節 電子媒体の管理」に準じて実施する。

- 8) アクセスログは、特定の担当者以外アクセスできない仕組みとする。また、アクセスログへのアクセス確認を別人が実施する。

5. 2. 3 情報のバックアップ

- 1) 情報システムの重要度に応じて、システムファイル及び情報のバックアップを定期的
に取得する。
- 2) バックアップの作業に当たる者は、その作業の記録を残し、部門管理者の承認を得る。
- 3) バックアップ媒体は、施錠できるキャビネット、耐火金庫等に保管し、その所在を台
帳に記録し、管理する。
- 4) バックアップ媒体は1年間に1回新品に交換する。媒体に品質の劣化が予想される場
合や、劣化原因と思われる障害が発生した場合は、直ちに新品に交換を行う。
- 5) 部門管理者は、記録媒体及び機器のログを確認し、記録媒体の劣化や機器の不具合を
確認する。エラー・警告のログが発見された場合は、直ちに新品の記録媒体に記録を
複写する。
- 6) 情報がき損した時に、バックアップされた情報を用いてき損前の状態に戻せることを
確認し、リストア手順を規定する。

5. 2. 4 リスク対応（障害対策）

- 1) システム管理者は、情報システムに係る障害が発生した場合には、事態の掌握・收拾
及び被害を最小限に止め、復旧作業の軽減、時間の短縮等を図るため、次の処置を講
じなければならない。
- 2) 緊急時及び災害時の連絡、復旧体制並びに回復手順を定め、非常時においても参照で
きるような媒体に保存し保管する。
- 3) 利用者に対し事故発生時には、速やかに報告することを周知させる。
- 4) 業務上において情報漏えいなどのリスクが予想されるものに対し、運用ルール等の見
直しを実施する。
- 5) 基幹システム以外の部門システムで障害が発生した場合は、当該部門の部門管理者に
報告し、部門管理者は、担当 SE と連携して復旧対策を講じるとともに、障害内容を
システム管理者に報告する。
- 6) 部門管理者は、障害内容が部門間インターフェイスの要因であると判断した場合は、
関係部門に報告するとともに、システム管理者に報告し、復旧対策の指示を待つ。そ
の際は、状況に応じて伝票での運用に切り替え、通常業務の稼働に努める。

5. 3 端末管理

- 1) 離席時など、特定の時間（5分以内）使用しなかった場合は、なりすましによる使用を防ぐため、パスワード付きスクリーンロック又は、自動ログオフ機能を設定する。
- 2) 持出した情報機器には、別途定められている以外のアプリケーションをインストールしない。
- 3) 全端末の時刻情報はサーバー時刻と同期させる。

5. 4 ネットワーク管理

5. 4. 1 LAN 管理

- 1) 個人情報にアクセスするための当〇〇の情報システムネットワーク（以下、「LAN」という）は、インターネット等の当〇〇外と情報交換ができるネットワークとは物理的に遮断する。
- 2) LANを利用できる情報システムを制限・管理し、許可されていない情報機器の接続を制御する。
- 3) 外部のネットワークとLANを接続する場合は、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。

5. 4. 2 インターネットの利用・管理

- 1) インターネット利用は、業務上必要な場合に限られ、私的利用は禁止とする。情報及びソフトウェア等のダウンロード、インストール等が業務上必要なインターネットサイトは、原則ホワイトリストで指定して通信先を限定する。
- 2) システム管理者は、ホームページを含む不正アクセスや改ざんの防止のため、インターネットに係る各サーバー、ルータ等に適切な管理策等の処置を講じ、ファイアウォール及びプロキシサーバーを設置し、許可された通信以外の通信を遮断すると共に許可された通信の状況を記録する。システム管理者は、定期的（月1回以上）に通信状況を監査する。
- 3) 当〇〇の情報を、ホームページを用いてインターネットへ公開、又は公開情報を変更・削除する場合は、システム管理者へ申請する。システム管理者は、内容の確認後に、登録・変更を実施する。
- 4) システム管理者は、ホームページの利用状況を監視し、不正アクセスやホームページの改ざんの有無を確認し、問題がある場合は、適切な処置（予防・是正）を講じる。

5. 4. 3 電子メールの利用・管理

- 1) システム管理者は、メールアカウントを申請に基づいて発行する。
- 2) システム管理者は、職員の退職時に当該職員のメールアカウントを速やかに削除する。
- 3) 電子メールの私的利用は、禁止とする。
- 4) 受信メールの自動転送については、組織外へのメール転送を原則禁止とする。ただし、業務の遂行のために予め許された指定メールアドレスへの転送は、信頼のおける転送方法をもって実施する場合のみ可能とする。
- 5) 個人情報を含む情報を電子メールで送信する場合、個人情報を含む情報に暗号化処置

等を講ずるなど、情報の安全性に留意して、ファイルとして添付して送信することとする。この場合、復号用パスワードは別に送信し、紛失または誤送に備える。

- 6) 電子メールに個人情報が含まれる場合は、送信・受信した後に速やかに削除することとする。

5. 4. 4 無線 LAN の管理

- 1) 無線 LAN のセキュリティ対策については、総務省発行の「安心して無線 LAN を使用するために」を参考にして対策を実施する。
- 2) システム管理者は、不正アクセスの対策として、以下のような設定を施す。
 - a) 少なくとも SSID や MAC アドレスによるアクセス制限を行う。
 - b) ステルスモード、ANY 接続拒否を利用者以外のアクセスを排除する。
 - c) 不正な情報の取得を防止するため、通信を WPA2/AES 等の手法を用いて暗号化する。
- 3) 電波を発する機器（携帯ゲーム機等）によって電波干渉が起こり得るため、無線 LAN 利用規則を情報システムの利用者へ説明する。
- 4) システム管理者は、無線 LAN アクセスポイントの設定状態を適宜確認する。

5. 5 一般的な運用事項

5. 5. 1 セキュリティパッチの適用

- 1) 情報システムのサーバー及び端末には、ベンダーからの保証がない限り、原則として修正プログラムは適用しない。
- 2) インターネットへの接続を許可された端末については、オペレーティングシステムやパッケージソフト等のパッチなどの修正プログラムがメーカーより発行された場合、既存システムの影響を考慮してシステム管理者の指示に基づいて実施する。

5. 5. 2 ウィルス対策

- 1) 悪意のあるソフトウェア等から保護するため、全てのサーバー、端末にアンチウィルスソフトを導入し、パターンファイルは常に最新のものを使用する。
- 2) 定期的にソフトウェア等のウィルスチェックを行ない、感染の有無を確認する。
- 3) アンチウィルスソフトは、常に稼働させておくこととする。
- 4) 業務上許された情報取得分については、ウィルスチェックを行い、問題のないことを確認後に使用する。
- 5) 電子メールサーバーは、すべての着信メールについてウィルスチェックを行ない、感染の有無を確認する。
- 6) ネットワークに接続するサーバーと端末は、配信型のアンチウィルスソフトの利用を可能とし、パターンファイルの更新は自動更新で行う。
- 7) ネットワークに接続していない PC は、PC の利用者が常に更新情報の入手に努め、最新パターンファイルを入手し更新する。
- 8) インターネットに接続していない LAN は、最新のパターンファイルを、インターネットに接続したウィルスサーバーにより取得し、情報システムのウィルスサーバーに

手動で更新・配信する。

5. 5. 3 電子媒体の管理

- 1) 媒体使用時は、必ずウィルス等の不正なソフトウェアの混入がないか確認する。

5. 5. 4 電子署名・タイムスタンプ

- 1) 法令で署名または記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行う。
 - a) 厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野 PKI 認証局もしくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施す。
 - b) 電子署名を含む文書全体にタイムスタンプを付与する。
 - c) 上記タイムスタンプを付与する時点で有効な電子証明書を用いる。
- 2) システム管理者は、電子的に受領した文書に電子署名が有る場合の、署名検証手順を定める。具体的には、電子署名が有効である間に、電子署名の検証に必要となる情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値とともにその全体に対してタイムスタンプを付与する等の対策を実施する。

6. その他

本規程は 20xx 年 xx 月 xx 日より施行する。

以上

【雛形】機密文書管理規程

改 訂 履 歴

版数	改訂年月日	改訂内容
1.0	20xx 年 xx 月 xx 日	新規制定

※ 版数は新規制定を第 1.0 版とし、改訂が発生した際は第 1.1 版とする。

※ 改訂があった場合は、必ず改訂内容を記載すること。

目 次

1. 総則	1
1. 1 目的	1
1. 2 機密文書の定義	1
1. 3 機密区分	1
1. 4 適用範囲	1
1. 5 個人情報の取扱い	1
2. 機密文書管理体制	1
2. 1 管理組織	1
2. 2 機密保持	2
2. 3 非常持出	2
3. 3. 機密文書管理方法	2
3. 1 機密文書の作成および指定	2
3. 2 機密文書の表示	2
3. 3 機密文書の保管	3
3. 4 機密文書の指定の変更、解除	3
3. 5 保管文書の引継ぎ	3
3. 6 機密文書の廃棄	3
4. その他	3
4. 1 改廃	3
4. 2 施行	3

1. 総則

1. 1 目的

本規程は、〇〇〇〇（以下、「当〇〇」という）の情報セキュリティ基本方針に従い、当〇〇で取り扱う文書の中で、特に機密性の高い文書（以下、機密文書という）の適正な管理を図ることを目的とする。

1. 2 機密文書の定義

機密文書とは、秘密保全の必要性が特に高く、当該文書が漏洩することによって、当〇〇に甚大な損害や損失を与える虞がある文書であって、機密度を規定する区分（以下、「機密区分」という）を指定した文書と定義する。

1. 3 機密区分

機密文書の機密区分は以下の通りとする。

- 1) 指定された者以外に開示してはならない機密文書を「極秘」と指定する。
- 2) 取扱い部署以外に開示してはならない機密文書を「秘密」と指定する。
- 3) 当〇〇の役職員以外に開示してはならない機密文書を「社外秘」と指定する。

1. 4 適用範囲

適用範囲は、以下の通りとする。

- 1) （情報システムから出力された帳票類を含む）当〇〇が作成及び編集した文書
- 2) 申請・届出及び添付書類等の加入者及び事業主から受領した文書
- 3) 他の地域公共団体、医療保険者、その他の機関から入手した文書または情報を文書化したもの（メモを含む）

1. 5 個人情報の取扱い

- 1) 個人情報が記入、又は記載された文書は、機密区分として「秘密」以上を指定する。
- 2) 特定個人情報が記入、又は記載された文書は、機密区分として「極秘」を指定する。
- 3) 個人情報、又は特定個人情報の記入欄のある帳票、又は文書（以下、指定帳票という）において、個人情報、又は特定個人情報が記入されたものは、管理責任者の指定を得ずに上記文書に準じて取り扱う。

2. 機密文書管理体制

2. 1 管理組織

- 1) 理事長が任命した者を機密文書管理の統括責任者（以下、統括責任者という）とする。
- 2) 機密文書を保有する部署の長を機密文書管理責任者（以下、「管理責任者」という）とする。

2. 2 機密保持

- 1) 機密文書の開示を受けた役職員は、知り得た機密情報を、関係する業務以外に使用してはならない。
- 2) 機密文書の開示を受けた役職員は、知り得た機密情報を、機密区分に基づく開示可能な範囲外の者に開示、又は漏洩してはならない。
- 3) 機密文書の開示を受けた役職員は、知り得た機密情報を、業務上で開示可能な範囲外の者に開示する必要がある場合には、予め管理責任者に報告して、その指示に従って行わなければならない。
- 4) 役職員は、業務上必要な場合に限り、予め管理責任者に報告して、その指示に従って機密文書を最低必要部数に限って複写することができる。複写した文書を配布する場合は、連番を付与して配布先が特定できる情報を管理する。また、使用終了後は当該文書をすべて回収して破棄する。
- 5) 役職員は、当〇〇外に機密文書を持ち出すことを原則禁止する。業務上、やむをえない場合には、管理責任者に申請して、承認を得なければならない。

2. 3 非常持出

- 1) 火災または天災等により、滅失毀損した場合、業務上著しく支障をきたす恐れのある文書は、専用の容器に入れ、「非常持出」の表示をする。
- 2) 「非常持出」の文書の保管場所は、火災盗難の予防並びに非常の際に搬出の容易なことを考慮して定める。

3. 3. 機密文書管理方法

3. 1 機密文書の作成および指定

- 1) 機密文書の作成及び入手は、必要最低限に留める。
- 2) 管理責任者は、指定帳票を除く、機密文書の内容を評価して、機密区分を指定する。
- 3) 管理責任者は、指定帳票を除く、「極秘」及び「秘密」指定の機密文書について、開示可能な者の範囲及び開示期間を定める。
- 4) 管理責任者は、指定帳票を除く、「極秘」及び「秘密」指定の機密文書を統括責任者に報告する。
- 5) 統括責任者は、報告を受けた機密文書に機密文書指定番号を付与する。

3. 2 機密文書の表示

- 1) 機密文書は、指定帳票を除き、上記文書個人情報、又は特定個人情報の記入欄のある帳票、又は文書を除き、少なくとも以下の事項を表紙、又は文書の見える部分に明記する。
 - a) 機密区分
 - b) 機密文書指定番号
 - c) 機密取扱期間
 - d) 作成担当部署名

- 2) 指定帳票は、個別の文書について上記記載事項を省略することができる。ただし、指定帳票を綴じるファイル、バインダー等の表紙に上記の事項を明記することとする。

3. 3 機密文書の保管

- 1) 機密文書は、原則として、当該機密文書を作成、又は入手した部署で所在を明示して、法令の定めた保存期間、又は法令に定められているものの他は別に定めた保存期間の間保存・管理する。
- 2) 保存期間が経過した文書において、引き続き保存する必要があるものについては、改めて保存期間を定めて保存・管理する。
- 3) 「極秘」および「秘密」の機密文書は、機密文書管理台帳を作成して、保存・管理の状況が確認できるようにする。
- 4) 「極秘」および「秘密」の機密文書は、キャビネット等の施錠可能な場所に、常時施錠して保管・管理する。

3. 4 機密文書の指定の変更、解除

管理責任者は、機密文書の指定に変更事由が生じた場合、指定の変更、又は解除などの適切な措置を講じる。

3. 5 保管文書の引継ぎ

改組、業務委譲等によって保存文書を他部署に引継ぐ場合は、文書引継書を作成して、受領を明確にしなければならない。

3. 6 機密文書の廃棄

- 1) 保存期間が経過して廃棄すべき文書、又は使用後回収した複写した文書は、原則として、保管の所管部において廃棄処分する。
- 2) 廃棄する文書は、シュレッダー等で破砕処理または溶融処理する。

4. その他

4. 1 改廃

本規定の改廃については、統括管理者が立案し、役員会が決議する。

4. 2 施行

本規定は平成〇〇年〇〇月〇〇日から施行する。