# 大分県医師国民健康保険組合における情報セキュリティ基本方針

平成28年1月1日制定

## 第1章　情報セキュリティポリシー等について

大分県医師国民健康保険組合（以下「組合」という。）では、組合員及び被保険者の健康にかかわる個人情報をはじめ、部外に漏洩、改ざん等した場合には、極めて重大な結果を招く情報を多く取り扱っている。これらの情報を安全に取り扱っていくためには、情報の重要性を認識し、厳格に管理・運用して情報を保護することが重要と考えられる。

さらには、利便性を向上させつつ安全性を追求し、情報管理の枠組みを明確に定め、実践していくことが組合のこれからの重点項目である。

従って組合では、情報のセキュリティを保持するため、統一方針として「大分県医師国民健康保険組合　情報セキュリティポリシー」を策定することとする。

### 第1節　情報セキュリティポリシー

情報セキュリティポリシーは、情報資産の安全を守るために定められる規則やルールであり、情報セキュリティ基本方針（以下「基本方針」という。）と情報セキュリティ対策基準（以下「対策基準」という。）からなる。セキュリティポリシーは公開することができる。

(1)　基本方針

組合は、組合の情報の管理および情報セキュリティ対策についての基本的な考え方や方向性を定めた基本方針を定める。

(2)　対策基準

組合は、基本方針に基づいた情報セキュリティ対策を講ずるに当たって遵守すべき行為、判断等の基準を統一的に定めるために、必要となる基本要件を明記した対策基準を定める。

### 第2節　情報セキュリティポリシーの改訂

組合は、情報セキュリティを取り巻く状況の変化に速やかに対応するため、情報セキュリティ監査の結果等も踏まえ、情報セキュリティポリシーおよび実施手順は定期的に見直し、必要に応じて改訂する。

### 第3節　実施手順

組合は、情報セキュリティポリシーを遵守して情報セキュリティ対策を実施するため、個々の部署や情報システムについて基本方針に基づき具体的な手順を明記した実施手順を定める。

実施手順は、公にすることにより組合の運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

## 第４節　用語定義

(1) ネットワーク
　組合において相互に接続するための通信網、その構成機器（ハードウェアおよびソフトウェア）および記録媒体で構成され、処理を行う仕組み。

(2) 情報システム
　ネットワーク、ハードウェア、ソフトウェアおよび記録媒体で構成された情報を処理する仕組み。

(3) 情報セキュリティ
　情報資産の機密の保持および正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持すること。

(4) 情報資産
　組合が保有する全ての文書および電磁的データ、および本組合が保有する情報システムとネットワーク。

(5) 役職員
　組合の役員、正職員、嘱託職員、臨時職員およびパート職員。

(6) 情報セキュリティ責任者
　組合における情報セキュリティ対策の責任者。原則として常務理事（コンプライアンス担当理事）、不在の場合は、事務長が代行する。

(7) 運用管理者
　組合情報システムを総括的に管理している事務長。

(8) 業務委託会社社員
　組合における業務を委託され、組合の情報資産を使用して業務を行う者。

# 第２章　基本的な考え方

## 第１節　情報資産の範囲

本基本方針が対象とする情報資産は次のとおりである。

(1) 組合の業務で取扱う情報
(2) 組合が保有する情報システム、ネットワーク
(3) 組合の情報システム、ネットワークで取扱う入出力媒体（印刷した文書を含む）

## 第２節　情報資産に関する脅威

情報資産に対する脅威の発生度合や発生した場合の影響の大きさを考慮すると、特に認識すべき脅威は次のとおりである。

(1) 役職員および業務委託会社社員または外部による組合の文書類の盗難、改ざん、消去等

(2) 外部からの不正アクセスまたは不正操作によるデータまたはプログラムの持ち出し・盗聴・改ざん・消去、機器および媒体の盗難等

(3) 役職員および業務委託会社社員による誤操作、不正アクセスまたは不正操作によるデータまたはプログラムの持ち出し・盗聴・改ざん・消去、機器および媒体の盗難および規定外の端末接続によるデータ漏洩等

(4) 地震、落雷、火災、風水害等の災害によるサービスの停止

(5) 事故、故障、障害等によるサービスの停止

## 第３節　情報資産区分

前節で示した脅威から情報資産を保護するために、情報が不当に他者に漏洩しない（機密性）、情報が改ざんされない（完全性）、障害発生時にも継続して提供できる（可用性）の３つの側面から、その重要度に応じて情報資産区分を設定する。
情報資産区分に基づき、情報資産の保護管理要件を明確にし、想定されるリスクおよびその対策を明確にする。

## 第４節　情報セキュリティ対策

前節で示した３つの側面から情報資産の重要性を検討し、組合は次の情報セキュリティ対策を講ずるものとする。

(1) 人的対策
情報セキュリティに関する権限および責任を定め、役職員および業務委託会社社員に基本方針および情報セキュリティに関する法令等の内容を周知徹底する等、十分な教育および啓発が行われるよう必要な対策を講ずる。

(2) 物理的対策
情報システムおよびネットワークを設置する施設への不正な立ち入り、並びに情報システム、ネットワークおよび情報資産への損傷・妨害等から保護するための物理的な対策を講ずる。

(3) 技術的対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策を講ずる。

(4) 開発・運用上の対策

情報システム開発の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等、開発・運用面の対策を講ずる。

また、緊急事態が発生した場合に速やかな対応を可能とするための危機管理対策を講ずる。

## 第３章　情報資産

### 第１節 情報資産の分類

情報セキュリティ責任者は、所管部で管理している情報資産をそれぞれの重要度に応じた情報資産区分に分類しなければならない。

### 第２節 保護管理要件の決定

情報セキュリティ責任者は、情報資産区分をその情報を使用している使用者や運用管理者に明示する。また必要に応じて追加の保護管理要件を設定し、想定されるリスクおよびその対策を明確にしなければならない。

### 第３節　情報資産の取扱い

情報資産の使用者や運用管理者は、その情報資産に定められた情報資産区分に従って取り扱わなければならない。さらに、情報セキュリティ責任者が追加して定めた保護管理要件に従わなければならない。

## 第４章　人的対策

### 第１節　職掌上の役割と責任

組合は、通常の業務の中で情報セキュリティを確保するために、職掌上の役割と責任を定める。

理事長および役員は、組合における情報セキュリティを確実にするために必要な支援を行い、また自ら情報を使用する際は情報セキュリティポリシーを遵守しなければならない。

情報セキュリティ責任者は、情報セキュリティ確保の責任を負い、職員や業務関係者が情報セキュリティポリシーを理解し、遵守することを徹底しなければならない。

職員および業務委託会社社員は情報セキュリティポリシーや情報セキュリティ責任者の指示を遵守し、情報を不正に使用されることを防止しなければならない。

## 第２節　情報セキュリティ上の役割と責任

情報セキュリティ確保のため、組合内横断的に、情報セキュリティ責任者、運用管理者、使用者の３つの役割と責任を定める。

情報セキュリティ責任者は、自らが保有する情報資産を把握し、その重要度の判断を行い、情報資産区分を決定し、いかに管理するかを決定した上で運用管理者に通知しなければならない。

運用管理者は、職員および業務委託会社社員が情報システム上で情報を取り扱う上で、組合情報セキュリティポリシーを理解し、遵守していることを管理しなければならない。また、情報セキュリティ責任者の指示に基づき所属部での情報資産の保護・管理を行わなければならない。

使用者は、情報セキュリティ責任者および運用管理者の指示に基づいて情報資産を使用しなければならない。

## 第３節　情報セキュリティ管理組織

組合は、組合全般における情報セキュリティの方針を決定し、情報セキュリティ対策を計画、実施するために、情報セキュリティ管理組織を設ける。情報セキュリティ管理組織は、情報セキュリティ統括責任者、情報セキュリティ委員会および情報セキュリティ委員会事務局で構成する。

情報セキュリティ統括責任者は常務理事（コンプライアンス担当）とする。

情報セキュリティ統括責任者は組合における情報資産の管理及び情報セキュリティ対策に関する責任を有する。

情報セキュリティ統括責任者は情報セキュリティ委員会のメンバーを任命する。

## 第４節　情報セキュリティに関する教育

組合は、役職員および業務委託会社社員への情報セキュリティポリシーの浸透と情報セキュリティ意識向上のため、情報セキュリティに関する教育を実施する。

## 第５節　第三者による情報資産使用に関する方針

組合が業務委託会社社員等第三者に、組合の重要情報資産を使用させる場合は、事前に情報セキュリティ委員会の承認を必要とする。また、情報セキュリティ上必要な事項については予め契約に定めておかなければならない。

### 第６節　識別と認証

使用者は、情報システムを使用する上で識別子（ID、カード等）と固有の認証子（パスワード等）を使用しなければならない。識別子と認証子の他の使用者との共有はできる限りしないものとする。また、識別・認証を確実に行えるように設定間隔、誤入力の取扱いを定め、管理された状態に置かなければならない。

## 第５章　物理的対策

### 第１節　セキュリティエリア

情報セキュリティ責任者は、不正侵入や業務への割り込みを防御するために、重要情報資産をもつ情報システムが存在するフロアには物理的な保護エリアを設定し、エリアを管理する責任者を定めた上で管理を行わなければならない。

### 第２節　情報機器管理

情報セキュリティ責任者および運用管理者は、情報機器の設置、廃棄、および移動については、適切な管理を行わなければならない。

## 第６章　技術的対策

### 第１節　コンピュータおよびネットワーク管理

運用管理者は、情報資産に関する脅威から情報資産を守るために、コンピュータやネットワークを適切に設定し、管理しなければならない。

### 第２節　不正ソフトウェアからの保護

運用管理者は、悪意のあるソフトウェアから保護するための検出および防止の管理を行わなければならない。

### 第３節　アクセス制御

運用管理者は、情報資産の情報資産区分に従い、承認された者のみが情報システムに対してアクセスが可能であるように制御しなければならない。

## 第７章　開発・運用上の対策

### 第１節　情報システム運用管理

情報システムの運用手順、事故管理手順を文書化し、その手順に基づいて適切に管理運用しなければならない。

## 第２節　情報システム開発および保守

### １．開発・保守手順等

運用管理者は、情報システムを開発する前には情報セキュリティ要件を明確にし、その要件に基づいて開発を行わなければならない。また、開発保守にあたっては、手順を明確にしなければならない。

### ２．情報システム開発・保守環境

システム開発者は、情報システムの開発環境および保守環境について、運用システムの環境と分離しなければならない。

# 第８章　緊急時対応計画の策定

情報セキュリティ責任者は、主要業務毎に情報資産区分に基づいた、非常時の手順、バックアップ手順、業務再開手順等を含む緊急時対応計画を策定しなければならない。

緊急時対応計画は定期的にテストを行い、計画の有効性を確認し、適宜見直さなければならない。

# 第９章　遵守

## 第１節　ポリシーおよび法令の遵守

役職員は、組合の情報資産を使用して職務を遂行するにあたり、情報セキュリティポリシーおよび関連する法令等を遵守し、これに従わなければならない。

## 第２節　点検

情報セキュリティ責任者は、情報セキュリティポリシーに沿った情報セキュリティ対策が実施されているかどうか、定期的に点検を行わなければならない。

## 第３節　情報セキュリティ監査

情報セキュリティ委員会は、情報セキュリティポリシーが遵守されていることを検証するため、定期的に監査を行わなければならない。

## 第４節　情報セキュリティポリシーに違反した場合の対応

役職員が、情報セキュリティポリシーに違反した場合は、その重大性、発生した事案の状況に応じて別に定める懲戒処分等の対象とする。

業務委託会社社員が、情報セキュリティポリシーに違反した場合の対応については、予め契約に定めておかなければならない。

附　則

この基本方針は、平成２８年１月１日から施行する。