長野市民病院　情報セキュリティ基本方針

1. 目的

長野市民病院が取り扱う診療情報その他の情報には、患者、市民、職員等に関する個人情報その他の重要な情報が含まれている。これらの情報及び情報を取り扱うために必要な情報システム、ネットワーク、施設、機器等を、災害、事故、故意又は過失による漏えい、滅失、毀損、改ざん、不正利用その他の脅威から保護することは、患者等の権利利益を守り、安全で質の高い医療を継続的に提供し、病院運営を安定的に遂行するために不可欠である。

本基本方針は、当院が保有し、又は管理する情報資産の機密性、完全性及び可用性を確保するため、情報セキュリティ対策に関する基本的事項を定め、組織的かつ計画的にこれを推進することを目的とする。

２．情報セキュリティポリシーの構成

当院の情報セキュリティポリシーは、情報セキュリティ対策に継続性、統一性及び実効性を持たせるため、次の 3 層により構成する。

(1)

情報セキュリティ基本方針

情報セキュリティ対策に関する基本理念、適用範囲、管理体制その他の基本的事項を定める。

(2)

情報セキュリティ対策基準

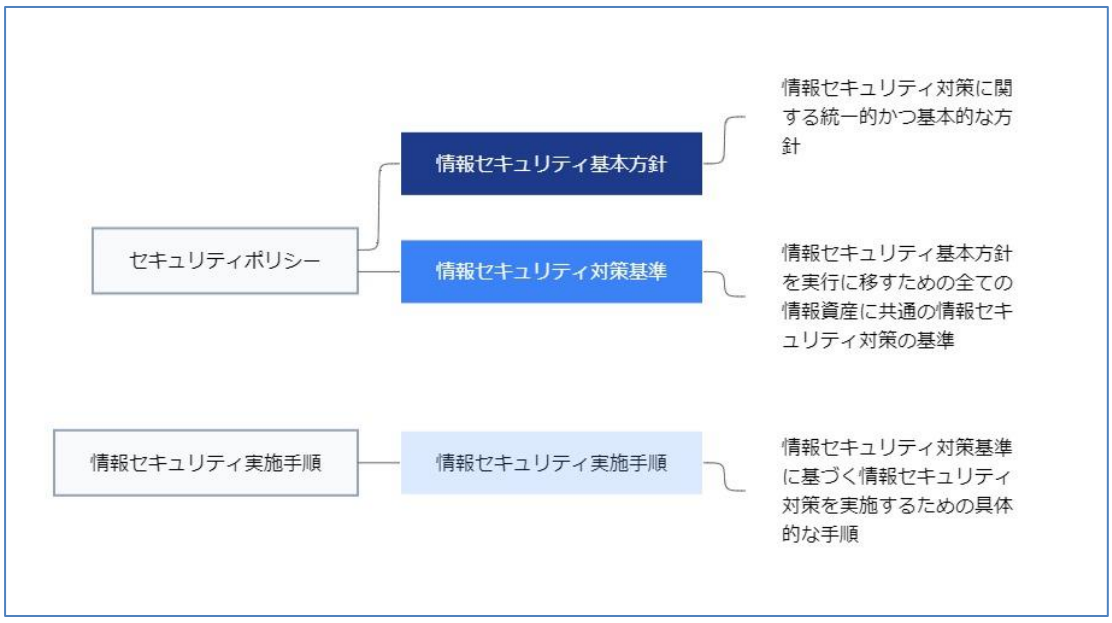
本基本方針を実行に移すため、当院において共通して適用すべき情報セキュリティ対策の判断基準及び遵守事項を定める。

(3)

情報セキュリティ実施手順

情報セキュリティ対策基準に基づき、各部門、各業務、各情報システム等において実施すべき具体的な手順を定める。

2　前項第 2 号及び第 3 号に定める文書は、公にすることにより当院の安全な運営に支障を及ぼすおそれがあるため、原則として非公開とする。



３．用語の定義

本基本方針において、次に掲げる用語の意義は、当該各号に定めるところによる。

⑴情報資産

診療情報その他当院の業務に関して取り扱う全ての情報並びにこれらを取り扱う情報システム、ネットワーク、機器、記録媒体、施設、関連文書及び委託先又は外部サービス上に保管もしくは処理される情報をいう。

⑵診療情報

診療録、看護記録、検査結果、画像情報、処方情報その他患者の診療に関して作成又は取得される情報をいう。

⑶医療情報システム

診療情報その他当院の業務に関する情報を取り扱うための情報システム、ネットワーク、端末、ソフトウェア及びこれらに附帯する設備をいう。

⑷情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

⑸情報セキュリティインシデント

情報資産の漏えい、滅失、毀損、改ざん、不正利用、利用不能その他情報セキュリティを侵害し、又は侵害するおそれのある事象をいう。

⑹職員等

当院の役員、職員、非常勤職員、派遣職員、研修生、実習生、委託事業者及び当院の情報資産を利用する全ての者をいう。

４．適用範囲

本基本方針は、当院が保有し、又は管理する全ての情報資産並びにこれを取り扱う全ての職員等に適用する。

2　前項の適用範囲には、情報資産の取得、作成、利用、保存、移送、提供、外部委託、保守、廃棄その他これらに関連する一切の取扱いを含む。

５．法令等の遵守

当院は、情報セキュリティ対策の実施に当たり、関係法令、関係省庁の指針、医療分野における関連ガイドライン、契約上の義務及び院内諸規程を遵守する。

６．対象とする脅威

当院は、情報資産に対する脅威として、特に次に掲げる事象を想定し、必要な対策を講ずる。

⑴　不正アクセス、マルウェア感染、ランサムウェア攻撃、サービス妨害攻撃その他のサイバー攻撃

⑵　職員等による誤操作、設定不備、情報機器の紛失、無断持出し、内部不正、権限の不適切な利用その他人的又は運用上の要因による事故

⑶　委託先、保守事業者、クラウドサービスその他外部サービスに起因する事故又は管理不備

⑷　機器故障、ソフトウェア障害、停電、通信障害その他のインフラ障害

⑸　地震、風水害、火災、感染症のまん延その他の災害等による業務継続への影響

７．情報セキュリティ管理体制の整備

当院は、情報セキュリティ対策を総合的かつ継続的に推進するため、医療情報システムに関する責任者、情報統括責任者、情報セキュリティ責任者その他必要な責任者

を置き、全院的な管理体制を整備する。
2　前項の管理体制においては、役割及び責任を明確にし、必要に応じて情報セキュリティインシデントに対応する体制を整備する。

８．リスクアセスメントの実施
　当院は、情報資産の重要性、想定される脅威、脆弱性、業務への影響等を踏まえ、情報セキュリティに関するリスクを適切に把握し、評価し、その結果に応じて必要な対策を講ずる。
2　前項の評価は、情報システムの新規導入、更改、構成変更、外部委託又は外部サービス利用その他必要な場合に実施し、又は見直すものとする。

９．情報資産の分類及び保護
　当院は、情報資産をその重要性に応じて分類し、当該分類に応じた人的、物理的、技術的及び運用上の対策を講ずる。
2　特に診療情報及び個人情報については、その重要性に鑑み、厳格な管理を行う。

１０．総合的な情報セキュリティ対策の実施
　当院は、情報資産を保護するため、次に掲げる対策を総合的に実施する。
(1) 組織的対策
(2) 人的対策
(3) 物理的対策
(4) 技術的対策
(5) 運用上の対策
(6) 業務継続及び復旧に関する対策

１１．外部委託及び外部サービスの管理
　当院は、業務の全部又は一部を外部委託し、又はクラウドサービスその他の外部サービスを利用する場合には、当院自らが負うべき責任を明確にした上で、委託先又はサービス提供事業者との責任分界を定め、必要な情報セキュリティ対策が講じられるよう管理する。
2　外部委託及び外部サービスの利用に当たっては、契約、監督、点検その他必要な措置を講ずる。

１２．教育及び訓練
　当院は、全ての職員等に対し、情報セキュリティに関する教育、啓発及び訓練を継続的に実施し、情報セキュリティ意識の向上及び事故防止を図る。

１３．情報セキュリティインシデントへの対応
　当院は、情報セキュリティインシデントが発生し、又は発生するおそれがある場合には、速やかに報告、連絡及び初動対応を行い、被害の拡大防止、原因究明、復旧及び再発防止を図る。
2　当院は、必要に応じて関係機関への報告、患者その他関係者への説明、公表その他の対応を適切に実施する。

１４．監査及び自己点検
　当院は、情報セキュリティポリシーの遵守状況及び対策の有効性を検証するため、

定期的又は必要に応じて、情報セキュリティ監査及び自己点検を実施する。

１５．評価及び見直し

当院は、情報セキュリティ監査、自己点検、リスクアセスメント及びインシデント対応の結果並びに社会的環境、技術的環境及び脅威の変化を踏まえ、本基本方針及び対策基準等を定期的に評価し、必要に応じて見直す。