阿伎留病院企業団
サイバーセキュリティ基本方針

阿伎留病院企業団

公立阿伎留医療センター

令和８年４月

(初 版)

目　次

序文

阿伎留病院企業団（以下「当企業団」という。）が保有する情報資産には、患者さん及び住民の個人情報をはじめ、極めて機微な医療情報（診療記録等）が多数含まれている。これらの情報資産を適切に管理し、高度化・巧妙化するサイバー攻撃や予期せぬ災害、人的要因による情報漏えい等の脅威から保護することは、安全で質の高い医療サービスを持続的に提供し、継続的な信頼を得るために不可欠である。 このような認識のもと、当企業団は情報セキュリティ対策に組織的かつ体系的に取り組むため、「阿伎留病院企業団 サイバーセキュリティ基本方針」を策定する。 本方針は、地方自治法（昭和22年法律第67号）第244条の6第1項の規定に基づき、当企業団におけるサイバーセキュリティを確保するための基本的な考え方を定めるものである。

１．目的

本方針は、当企業団が保有する情報資産の機密性、完全性及び可用性を維持し、サイバーセキュリティを確保することにより、行政運営の安定化並びに安全で質の高い医療サービスの継続的提供を実現することを目的とする。

２．定義

本方針における用語の定義は、以下のとおりとする。

（１）ネットワーク：コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（２）情報システム：コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう（電子カルテシステム等の医療情報システムを含む）。

（３）情報資産：ネットワーク、情報システム及びこれらに関わる全ての情報並びに情報システムの仕様書等の関連資料をいう。

（４）職員等：当企業団の組織に所属し業務に従事する全ての者（管理者、派遣職員、並びに会計年度任用職員等の非常勤職員を含む。）をいう。

（５）機密性：情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（６） 完全性：情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（７）可用性：情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（８）CSIRT（Computer Security Incident Response Team）：情報システム等におけるセキュリティ侵害等の問題が発生した場合に、被害の最小化、原因解析や影響範囲の調査等を行う体制（外部専門業者等との連携を含む。）をいう。

３．対象とする脅威

情報資産に対する脅威として、以下の事項を想定し、情報セキュリティ対策を講じる。

（１）外部からのサイバー攻撃（不正アクセス、ランサムウェア等のマルウェア感染、標的型攻撃等）

（２）内部要因による脅威（職員等の意図的な情報の持ち出し、誤操作による漏えい等）

（３）物理的脅威（機器の盗難、紛失、破壊、故障等）

（４）環境的脅威（地震、落雷、火災等によるサービス停止）

４．適用範囲

本方針は、当企業団の全ての執行機関（管理者、議会等）並びに当企業団のネットワーク及び情報システムを利用する全ての職員等に適用する。

５．職員等の遵守義務

職員等は、サイバーセキュリティの確保について不断の注意を払い、業務に当たること。また、当企業団が保有する情報資産に対し、業務目的外のアクセス又は利用を行ってはならない。その上で、地方公務員法、本方針及び情報セキュリティに関する各種規程（対策基準、実施手順等）を厳格に遵守しなければならない。これらに違反した場合は、同法、「阿伎留病院企業団職員の懲戒処分等に関する規程」及び「阿伎留病院企業団職員の分限に関する規程」に基づき、処分等の対象となり得る。

６．情報セキュリティ管理体制

当企業団のサイバーセキュリティを確保するため、以下の体制を構築する。

（１）最高責任者： 管理者を最高情報セキュリティ責任者(CISO)とし、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

（２）推進体制： 総括的な権限・責任を有する統括情報セキュリティ責任者を置き、各部門に情報セキュリティ責任者等を配置する。また、組織的な対策を推進するため、個人情報保護委員会等の既存の会議体を情報セキュリティに関する意思決定機関として位置づけ、重要事項を協議し、経営会議において審議・決定する。

（３）権限の最小化： 情報資産へのアクセス権限は、業務上必要最小限の範囲で付与する（最小権限の原則）。

７．情報セキュリティ対策の実施

脅威から情報資産を保護するため、総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」及び厚生労働省「医療情報システムの安全管理に関するガイドライン」に準拠し、以下の多層的な対策を講じる。

（1） 情報資産の分類と管理 情報資産の重要度（機密性・完全性・可用性）に応じた分類を行い、データ最小化の原則に基づき適切に管理する。

（2）物理的セキュリティ サーバ室等への入退室管理の徹底、情報機器の盗難・破壊防止、災害対策等の物理的な保護措置を講じる。

（3）人的セキュリティ 職員等に対し、情報セキュリティに関する権限と責任を明確化し、採用時から退職時に至るまでの遵守事項を定める。また、継続的な教育・訓練を実施し、リテラシーの向上を図る。

（4）技術的セキュリティ 不正アクセスやマルウェア感染を防止するため、ネットワークの分離、アクセス制御、通信の暗号化、ログの取得と長期間の保存等、技術的な防御措置を講じる。

（5）機器の廃棄・データ消去 情報機器等を廃棄又はリース返却する際は、内部データが復元不可能な状態となるよう、物理的破壊、磁気的破壊、又は確実なソフトウェア消去を実施し、委託先等から作業完了証明書を取得・確認する措置を講じる。

8．業務委託及び外部サービスの利用

（1） 業務委託における対策 情報システムの開発、運用、保守等を外部に委託する場合は、委託事業者において当企業団と同等以上のセキュリティ対策が確保されるよう、契約等においてセキュリティ要件を明記し、その実施状況を定期的に確認する。

（2）外部サービス（クラウド等）の利用 クラウドサービス等の外部サービスを利用する場合は、国が示す基準等（ISMAP等）を参考とし、利用規程を整備した上で安全性を評価し利用する。ソーシャルメディアの利用にあたっては、運用責任者を定め、発信内容の承認ルールを構築する

９．情報セキュリティインシデントへの対応

情報セキュリティインシデント（サイバー攻撃による被害、情報の漏えい、システムの停止等）が発生した場合、又はその予兆を検知した場合には、被害の拡大防止、速やかな復旧、原因究明及び再発防止を行うため、緊急時対応計画（BCP等）に基づく迅速な対応体制（CSIRT等との連携を含む）を整備する。

１０．サイバーセキュリティに関する監査及び自己点検の実施

本方針及び関連規程の遵守状況を確認するため、定期的に自己点検を実施するとともに、情報セキュリティ対策の実効性を検証するための監査体制を段階的に整備し、定期的又は必要に応じて内部監査を実施する。

１１．本方針の見直し及び下位規程等の整備

情報技術の進展、新たな脅威の発生、関連法令や国等のガイドラインの改定、並びに監査結果等を踏まえ、本方針を定期的に評価し、必要に応じて見直しを行う。また、本方針に基づき、具体的な遵守事項や判断基準を定めた「情報セキュリティ対策基準」及び「情報セキュリティ実施手順」等を整備する。なお、情報セキュリティ実施手順は、公にすることにより当企業団の運営に重大な支障を及ぼすおそれがあることから非公開とする。

附則

１．本方針は、令和8年4月20日から施行し、令和8年4月1日から適用する。

２．第4項に定める適用範囲のうち、議会等に関する部分については、当該機関における決定が行われた日から適用する。