歯科情報セキュリティ，サイバーセキュリティ及びプライバシー保護 情報セキュリティマネジメントシステム 要求事項

DISC 27001：2025

2025年4月1日 制定

一般社団法人歯科情報セキュリティ協議会

著作権法により無断での複製、転載等は禁止されております。

目　次

0 序文 2
0.1 概要 2
1 適用範囲 2
2 参照規格およびガイドライン 2
3 用語及び定義 2
3.1 クリアスクリーン 3
3.2 クリアデスク 3
3.3 要配慮個人情報 3
4 情報セキュリティマネジメントシステムの適用範囲の決定 3
5. リーダーシップ 3
5.1. 情報セキュリティ基本方針 3
5.2. 役割及び責任 3
6. 保有する情報の整理 3
7. 支援のための資源 3
7.1. 教育 3
7.2. 文書管理 3
8. 実行 4
8.1. 情報セキュリティ活動 4
8.2. ルールブック 4
9. 評価 4
9.1. 年間評価 4
9.2. 経営者への報告 4
10. 改善 4
11. 詳細管理策 4
解説 8

著作権法により無断での複製、転載等は禁止されております。

歯科情報セキュリティ，サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項

Dental information security, cybersecurity and privacy protection-Information security management systems-Requirements

0 序文

この規格は，日本国内の歯科医療機関において，個人情報保護法を遵守した個人情報の適切な取り扱い、サイバーセキュリティを含む医療情報システムの管理並びに歯科医療機関が保有する情報資産の適切な管理を行うことを目的としている。

0.1 概要

この規格は，歯科医院において情報セキュリティマネジメントシステム（以下，ISMS という。）を確立し，実施し，維持し，継続的に改善するための要求事項を提供するために作成された。ISMS の採用は，組織の戦略的決定である。組織の ISMS の確立及び実施は，その組織のニーズ及び目的，セキュリティ要求事項，組織が用いているプロセス，並びに組織の規模及び構造によって影響を受ける。影響をもたらすこれらの要因全ては，時間とともに変化することが見込まれる。

1 適用範囲

この規格は、「一般社団法人歯科情報セキュリティ協議会」が制定し、情報セキュリティを確立し、実施し、維持し、継続的に改善するための要求事項について規定する。この規格が規定する要求事項は、適用するすべての組織に適用できることを意図している。組織がこの規格への適合を宣言する場合には、箇条 4～箇条 10 及び、箇条 11 詳細管理策すべての要求事項を実施しなければならない。

2 参照規格およびガイドライン

この規格は、次の規格及びガイドラインを参照する。

・ISO/IEC27001:2022

・JIS Q 15001:2023

・医療情報システムの安全管理に関するガイドライン

3 用語及び定義

この規格で用いる主な用語及び定義は，JIS Q 27000:2019 に準拠する。JIS Q 27000:2019 に定義のない用語について以下に示す。

著作権法により無断での複製、転載等は禁止されております。

3.1 クリアスクリーン

離席する際に、パソコンの画面を他人がのぞき見したり、操作できる状態のまま放置しないこと。

3.2 クリアデスク

離席や業務の終了時に机の上に個人情報が記載された書類や、USB メモリなどの記憶媒体を放置しないこと。

3.3 要配慮個人情報

本人の人種、信条、社会的身分、病歴（身体・知的・精神障害、健康診断/遺伝子検査結果、保健指導、診療・調剤情報など）、前科・前歴、犯罪被害情報のほか、本人に不当・偏見が生じないよう、特に配慮が必要な情報。（引用 改正個人情報保護法）

4 情報セキュリティマネジメントシステムの適用範囲の決定

組織における情報セキュリティの必要性を整理し、適用範囲を定義しなければならない。

5. リーダーシップ

5.1. 情報セキュリティ基本方針

経営者により承認された情報セキュリティ基本方針があり、公開されていなければならない。情報セキュリティ基本方針には情報セキュリティに関連する法令を遵守することへのコミットメントを含まなければならない。

5.2. 役割及び責任

著作権法により無断での複製、転載等は禁止されております。

10. 改善

組織内規定に違反する事項が発生した場合、情報セキュリティインシデント改善シートにより改善処置が考案され、実行されなければならない。この結果は記録され、保存されなければならない。

11. 詳細管理策

A001	個人情報管理	管理策 個人情報保護法の適用範囲について、安全管理を行わなければならない。
A002	従業者の責任	管理策 正規雇用または臨時雇用を問わず、全従業員に対して次を実施しなければならない。 雇用時：雇用期間中及び雇用終了後の情報セキュリティ責任を明示した誓約書への署名。 雇用終了時：診療所から提供した情報資産の返却。
A003	情報の取り扱い	管理策 重要な書類は識別され、施錠管理されなければならない。

著作権法により無断での複製、転載等は禁止されております。

A022	事業継続のための備え	**管理策** 災害、サイバー攻撃、システム障害、ネットワーク障害等によって院内の情報システムが利用できなくなった場合の対応事項を定め、実行できるようにしておかなければならない。

参考文献

[1] 医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス
個人情報保護委員会・厚生労働省

[2] 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン
経済産業省

著作権法により無断での複製、転載等は禁止されております。

歯科情報セキュリティ，サイバーセキュリティ及びプライバシー保護
－情報セキュリティマネジメントシステム－要求事項

解説

この解説は，規格に規定・記載した事柄を説明するものであり，規格の一部ではない。

1 発行の経緯

この規格は，日本国内の歯科医療機関における情報セキュリティマネジメントシステム（ISMS）の構築及び運用を行うための要求事項として検討し、取りまとめたものである。あらゆる組織に対応するための情報セキュリティマネジメントシステム規格としては ISO27001:2022（JIS Q 27001:2023）が発行されているが、国内歯科医療機関においては多くの組織と比較して情報システムの規模が小さく、複雑さも低い。さらに関連する要員を含めた組織規模も小さいことから、ISO27001:2022（JIS Q 27001:2023）の要求事項及び管理策を基本として組織の特徴に合わせた必要かつ充分な要求事項及び管理策を策定したものである。検討に当たっては、医療機関としての特性である個人情報保護法における要配慮個人情報の取り扱いおよび厚生労働省が発行する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対応も考慮した。

規格の構造は ISO/IEC 専門業務用指針 第 1 部 統合版 ISO 補足指針の附属書 SL Appendix 2, MSS（マネジメントシステム規格）のための調和させる構造を参考とし、全体として Plan-Do-Check-Act（PDCA）サイクルの実行を意図している。

2 要求事項の内容

4 情報セキュリティマネジメントシステムの適用範囲の決定

この規格に基づいた情報セキュリティマネジメントシステムの適用範囲は組織の決定による。決定に当たっては組織を取り巻く社会的要求事項や患者を含む利害関係者の潜在的及び顕在的要望を考慮することになるであろう。

5.1 情報セキュリティ基本方針

経営者は情報セキュリティに関わる取り組みの方向性を定める。また関連法令の遵守について組織

著作権法により無断での複製、転載等は禁止されております。

3 詳細管理策の内容

A001

この規格が個人情報保護法に対応することが明示されている。歯科医療機関においては特に要配慮個人情報を保有していることに留意しなければならない。

A002

情報セキュリティに関わる組織のルールを遵守することについて雇用時に誓約書を取り交わす。誓約書には雇用終了後の遵守事項も含めなければならない。雇用終了時には退職者は情報資産を返却し、その後も誓約書に定められた事項を遵守する。

A003

カルテを含む診療に関わる文書や経営上の重要文書は施錠管理を行う。業務時間中や業務時間外、あるいは有人による監視下にある場合や無人となる場合等、文書の機密性に応じて施錠の要否を組織で決定する。書庫単位や管理区域単位での施錠管理も視野に入れる。

A004

機密事項が記載された文書は第三者の目に触れないように管理する。特に記載の個人が特定できる状態での放置がなされないよう管理する。執務机のみならず診療チェアのテーブルや患者の動線にある棚にも配慮することが必要である。

A005

紙媒体の廃棄に関わる一切の業者による共断な溶解処理を行うこと。

著作権法により無断での複製、転載等は禁止されております。

歯科情報セキュリティ，サイバーセキュリティ及びプライバシー保護
情報セキュリティマネジメントシステム 要求事項
DISC 27001：2025

制定・発行 一般社団法人歯科情報セキュリティ協議会
東京都江東区東陽 3-23-3 立川ビル 3F

監修 ビューローベリタスジャパン株式会社

著作権法により無断での複製、転載等は禁止されております。