医療機関向け
『Cybozu.com』対応セキュリティリファレンス

2019年7月10日

Version 1

作成者：
株式会社三菱総合研究所（MRI）

Copyright (C) MRI All Rights Reserved.

更新日	版番号	改版内容
2019/7/10	Version 1	初版作成

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.1-01	6	6.1	（安全管理措置） 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。 （従業者の監督） 個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。 （委託先の監督） 個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。 （個人情報保護法第20 条第21 条第22 条）	「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ドライン」において、個人情報保護に関する方針を定め公表することが求められている。本ガイドラインが対象とする情報システムの安全管理も、個人情報保護対策の一部として考えることができるため、この方針の中に情報システムの安全管理についても言及する必要がある。	個人情報保護に関する方針を策定し、公開していること。	最低限	–	以下のウェブページで個人情報保護に関する方針を公開しております。 個人情報に関する問い合わせ窓口についても、本文書の中に記載しております。 https://cybozu.co.jp/privacy/privacy-policy/	適合可能	文献[15]にてサイボウズ社の個人情報の取り扱いに関する方針が定められており、外部に公開されていることを確認した。	公開文書	文献[15]	–	–	–	利用者及びSI事業者は個人情報保護に関する方針を策定し、公開する必要がある。
6.1-02					個人情報を取り扱う情報システムの安全管理に関する方針を策定していること。その方針には、少なくとも情報システムで扱う情報の範囲、取扱いや保存の方法と期間、利用者識別を確実に行い不要・不法なアクセスを防止していること、安全管理の責任者、苦情・質問の窓口を含めること。	最低限	–		適合可能	文献[15]には、個人情報を取り扱う部門ごとに管理責任者を置き、個人情報の適切な管理に努めること、個人情報データベース等に対し、合理的な技術的施策、および従業員に対する啓発活動を行なうことにより、情報の紛失、改ざん、漏洩等の防止に努めることが明記されている。また、同文献には個人情報に関する問い合わせ窓口が記載されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[15]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は個人情報を取り扱う情報システムの安全管理に関する方針を策定する必要がある。またその方針には、少なくとも情報システムで扱う情報の範囲、取扱いや保存の方法と期間、利用者識別を確実に行い不要・不法なアクセスを防止していること、安全管理の責任者、苦情・質問の窓口を含める必要がある。
6.2-01		6.2	（安全管理措置） 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。 （個人情報保護法第20 条）	安全管理を適切に行うための標準的なマネジメントシステムがISO（ISO/IEC27001:2005）ならびにJIS（JIS Q 27001:2006）によって規格化されている。適切なマネジメントシステムを採用することは、安全管理の実践において有用である。	情報システムで扱う情報をすべてリストアップしていること。	最低限	–	各事業部のセキュリティ施策を推進する「情報責任者」が、情報資産のリストアップを行い、台帳管理しております。情報資産に対して「情報区分」と呼ばれる「機密レベル」を設定し、設定された機密レベルに応じた情報の管理方法を内規にて定めています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は情報システムで扱う情報をすべてリストアップする必要がある。
6.2-02					リストアップした情報を、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持していること。	最低限	–		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者はリストアップした情報を、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持する必要がある。
6.2-03					このリストは情報システムの安全管理者が必要に応じて速やかに確認できる状態で管理していること。	最低限	–		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者はこのリストアップした情報を情報システムの安全管理者が必要に応じて速やかに確認できる状態で管理する必要がある。
6.2-04					リストアップした情報に対してリスク分析を実施していること。	最低限	–		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者はリストアップした情報に対してリスク分析を実施する必要がある。
6.2-05					この分析により得られた脅威に対して、6.3 章～6.12 章に示す対策を行っていること。	最低限	–	対策を行っております。詳細につきましては、各管理策に対する回答内容をご参照ください。	適合可能	6.3～6.12の通り。	–	–	–	–	–	利用者及びSI事業者は上記分析により得られた脅威に対して、適切な対策を実施する必要がある。
6.2-06					上記の結果を文書化して管理していること。	推奨	–	「情報セキュリティ規則」と呼ばれる文書にて管理しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は上記の結果を文書化して管理する必要がある。
6.3-01		6.3	-	安全管理について、従業者の責任と権限を明確に定め、安全管理に関する規程や手順書を整備運用し、その実施状況を日常の自己点検等によって確認しなければならない。これは組織内で情報システムを利用するかどうかにかかわらず遵守すべき事項である。組織的安全管理対策には以下の事項が含まれる。 ① 安全管理対策を講じるための組織体制の整備 ② 安全管理対策を定める規程等の整備と規程等に従った運用 ③ 医療情報の取扱い台帳の整備 ④ 医療情報の安全管理対策の評価、見直し及び改善 ⑤ 情報や情報端末の外部持ち出しに関する規則等の整備 ⑥ 情報端末等を用いて外部から医療機関等のシステムにリモートアクセスする場合は、その情報端末等の管理規程 ⑦ 事故又は違反への対処	情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。ただし小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。	最低限	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．4．1．1【推奨】） ・各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるよう、定期的にレビュー及び見直しを行うこと。（Ⅱ．4．3．1【基本】） ・情報システム運用責任者を明確に定めて、合意すること。	cybozu.com におけるデータの取り扱い方法については、以下のウェブページで公開しております。 cybozu.com サービスご利用規約 https://www.cybozu.com/jp/terms/ プライバシーポリシー https://cybozu.co.jp/privacy/privacy-policy/ クラウドデータポリシー https://cybozu.co.jp/privacy/cloud-data-policy/ また以下の責任者を定め、文書化しております。 情報責任者：情報資産の責任者 情報セキュリティ管理責任者：cybozu.com のセキュリティに関する責任者	適合可能	文献[15]にて、取り扱う情報資産の利用に関する許容範囲（利用可,能者、利用目的、利用方法、および廃棄）が明記されており、情報のライフサイクルという観点では問題ないと考える。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[15]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行う必要がある。（ただし小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。）
6.3-02					個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること。	最低限	・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅱ．4．4．1【基本】） ・重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること。（Ⅱ．4．4．3【基本】） ・受託した個人情報を参照可能な事務室等における入退室管理のルールが、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	最低限	サイボウズ社内の運用体制については、下記ウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html	適合可能	文献[05]にて、運用メンバーは一般社員とは分離された執務スペースで業務を行い、運用メンバーの執務スペースは監視カメラを設置し、入退室等が管理されていることが明記されている。	公開文書	文献[05]	–	–	–	利用者及びSI事業者は個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定める必要がある。
6.3-03					情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。	最低限	・従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること。（Ⅱ．5．3．1【基本】） ・ASP・SaaSサービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．7．1．2【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．3．1．2【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】） ・運用しているアクセス管理に関する規程類が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・自社の規程類の情報を医療機関に対して開示する範囲・条件等について、医療機関等と合意すること。	最低限	cybozu.com におけるアクセス管理に関する文書は、以下のウェブページで公開しております。 不正ログイン対策 https://www.cybozu.com/jp/security/bad_login/index.html 不正アクセス対策 https://www.cybozu.com/jp/security/illegal_access/index.html 以下の文書も併せてご参照ください。 cybozu.com セキュリティチェックシート https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf ネットワーク図についても作成しております。	適合可能	文献[01]にて、システムアカウントについては当社規定に則り、各個人に一意の識別子が付与されている。またシステムにアクセスする際にはVPN網を利用し、さらにアクセスが許可されていない者がアクセス、ログオンできないように制御している旨が明記されている。 文献[03]で不正アクセス対策がされていること、また文献[04]で不正ログイン対策（なりすまし対策）がされていることが明記されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]文献[03]文献[04]	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成する必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.3-04					個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。	最低限	・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．５．１．２【基本】） ・自社で定める個人情報保護指針等に基づいて、委託業務を実施する旨を、契約内容に含めること。 ・自社で定める個人情報保護指針等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・個人情報保護法の対象に満たない件数(5,000件未満)、対象外（死者に関する情報）等であっても、医療情報の重要性から個人情報保護法における運用に準じて取り扱う旨が含まれていることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	情報セキュリティに関する基本方針を定め、以下のウェブページで公開しております。 ISMS 基本方針 https://www.cybozu.com/jp/terms/security.html cybozu.com におけるデータの取り扱い方法については、以下のウェブページで公開しております。 cybozu.com サービスご利用規約 https://www.cybozu.com/jp/terms/ プライバシーポリシー https://cybozu.co.jp/privacy/privacy-policy/ クラウドデータポリシー https://cybozu.co.jp/privacy/cloud-data-policy/ また内規にて情報の管理方法および、秘密保持に関する条項を定め、運営いたしております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は契約者情報などの個人情報について、公開している個人情報保護指針を利用者が見て、不足なら利用者側で契約に盛り込むよう交渉するなど、利用者側の責務とする必要がある。
6.3-05					運用管理規程等において次の内容を定めること。 (a) 理念（基本方針と管理目的の表明）	最低限	・経営陣は、情報セキュリティに関する組織的取組についての基本的な方針を定めた文書を作成すること。また、当該文書には、経営陣が承認の署名等を行い、情報セキュリティに関する経営陣の責任を明確にすること。（Ⅱ．１．１．１【基本】） ・自社で定める情報セキュリティに関する組織的取組における基本方針が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	適合可能	文献[15]に「取り組み」として、取り扱う情報資産の基本方針および利用に関する許容範囲（利用目的）が明記されている。	公開文書	文献[15]	–	–	–	利用者及びSI事業者は、運用管理規程を適切に定める必要がある。
6.3-06					(b) 医療機関等の体制	最低限	・医療機関等の体制に対応する事業者の体制を明らかにすることを、医療機関等と合意すること。	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	利用者及びSI事業者は、運用管理規程を適切に定める必要がある。
6.3-07					(c) 契約書・マニュアル等の文書の管理	最低限	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaSサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３【基本】） ・マニュアル等の文書管理に関して、開示できる文書等の範囲、事業者の役割等を医療機関等と合意すること。	情報セキュリティに関する文書は、文書管理いたしております。 cybozu.comは、ISO/IEC27001:2013／JIS Q 27001:2014 の要求事項に適合し、 認証を取得する過程で、本文書は第三者による審査を受けております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、運用管理規程を適切に定める必要がある。
6.3-08					(d) リスクに対する予防、発生時の対応の方法	最低限	・全ての従業員に対し、業務において発見あるいは疑いをもった情報システムの伝い弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続きを定め、実施を要求すること。報告を受けた後に、迅速に整然と効果的な対応ができるよう、責任体制及び手順を確立すること。（Ⅱ．６．１．１【基本】） ・自社で定めるリスク等に対する予防措置及び事故等の発生時の対応等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	脆弱性に対する対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html 内規にてセキュリティインシデント発生時には、管理責任者に報告する手続きを定め、運用しております。当事者・発見者からの報告は、全て記録しております。	適合可能	文献[05]にて、サイボウズ製品の脆弱性への取り組みおよびコンピュータのOSや他社のソフトウェア等の脆弱性への取り組みに関して明記されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[05]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、運用管理規程を適切に定める必要がある。
6.3-09					(e) 機器を用いる場合は機器の管理	最低限	・連携ASP・SaaS 事業者が提供するASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．３．１．２【基本】） ・ASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。（Ⅲ．２．１．２【基本】） ・自社で定める機器の管理等の運用管理の規程等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	ユーザ数の増加傾向や売り上げ計画に基づき、ハードウェアの増強計画を毎年実施しています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、運用管理規程を適切に定める必要がある。
6.3-10					(f) 個人情報の記録媒体の管理（保管・授受等）の方法	最低限	・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．５．３．１【基本】） ・自社で定める個人情報を記録した媒体の運用管理規程等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・個人情報保護法の対象に満たない件数(5,000件未満)、対象外（死者に関する情報）等であっても、医療情報の重要性から個人情報保護法における運用に準じて取り扱うこと。	内規にて書類・記録メディアの保管・管理ルールを定めております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、運用管理規程を適切に定める必要がある。
6.3-11					(g) 患者等への説明と同意を得る方法	最低限	・医療機関等の管理者が患者等への説明及び同意を得る際に、事業者が提供する情報の範囲、事業者の役割等について医療機関等と合意すること。	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	利用者及びSI事業者は、運用管理規程を適切に定める必要がある。
6.3-12					(h) 監査	最低限	・連携ASP・SaaS事業者が提供するASP・SaaSサービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．３．１．２【基本】） ・ASP・SaaSサービスの提供に用いる情報システムが、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に点検・監査すること。（Ⅱ．４．３．２【基本】） ・自社において実施するシステム監査等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・監査記録等を医療機関等に開示する情報の範囲・条件等について合意すること。	cybozu.comは、ISO/IEC27001:2013／JIS Q 27001:2014 の要求事項に適合し、 認証を取得する過程で、内部監査および審査機関による審査を受けております。 認証登録番号 IS 577142	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、運用管理規程を適切に定める必要がある。
6.3-13					(i) 苦情・質問の受付窓口	最低限	・ASP・SaaSサービスの提供に支障が生じた場合には、その原因が連携ASP・SaaS事業者に起因するものであったとしても、利用者と直接契約を結ぶASP・SaaS事業者が、その責任において一元的にユーザサポートを実施すること。（Ⅱ．８．１．１【基本】） ・医療機関等の管理者側からの問合せ窓口を設けること。また受付の時間帯等について、医療機関等と合意すること。	各サービスごとに問い合わせ窓口を設けております。 詳細は以下のウェブページで公開しております。 https://www.cybozu.com/jp/inquiry/	適合可能	文献[15]にて、お問い合わせ窓口が明記されていることを確認した。	公開文書	文献[15]	–	–	–	利用者及びSI事業者は、運用管理規程を適切に定める必要がある。
6.4-01		6.4	-	物理的安全対策とは、情報システムにおいて個人情報が入力、参照、格納される情報端末やコンピュータ、情報媒体等を物理的な方法によって保護することである。具体的には情報の種別、重要性と利用形態に応じて幾つかのセキュリティ区画を定義し、以下の事項を考慮し、適切に管理する必要がある。 ① 入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理） ② 盗難、窃視等の防止 ③ 機器・装置・情報媒体等の盗難や紛失防止も含めた物理的な保護	個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。	最低限	・サーバルームやラックの鍵管理を行うこと。（Ⅲ．４．４．６【基本】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．５．３．１【基本】） ・バックアップ媒体も含め、個人情報を含むサーバ以外の機器・媒体等の保管場所を施錠管理すること。	電子媒体の保管・破棄などの管理方法につきましては、以下の文書をご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf 運用メンバーは「入室制限エリア」と呼ばれる、一般社員とは隔離された執務スペースで業務を行っています。 詳細は以下の Web ページを参照ください。 https://www.cybozu.com/jp/security/vulnerabili	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者にて個人情報を格納している機器や媒体がある場合、個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠する必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目									Cybozu.com における対応							
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類	総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
6.4-02				及び措置	個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規程に基づき許可された者以外立ち入ることが出来ない対策を講じること。 ただし、本対策項目と同等レベルの他の取りうる手段がある場合はこの限りではない。	最低限	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．７．１．３【基本】） ・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅱ．４．４．１【基本】） ・重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像を予め定められた期間保存すること。（Ⅱ．４．４．２【推奨】） ・委託業務に基づき受託する個人情報の内容を参照する必要が生じる場合には、データアクセスが可能な端末が設置されている部屋に対する入退出の施錠管理及び入退出管理を行うこと。	by/index.html 「入室制限エリア」は、IC 又は生体認証によって自動的に施錠監視されています。また監視カメラを用いて入退室を管理しております。 お客様からお預かりしたデータは、利用規約の定めに従って取り扱います。 詳細は以下のウェブページで公開しております。 https://www.cybozu.com/jp/terms/ https://cybozu.co.jp/privacy/cloud-data-policy/	適合可能	執務スペースには監視カメラを設置し、入退室が管理されていることが文献[05]に記載されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[05]	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、個人情報を入力、参照できる端末が設置されている区画について、適切な物理対策を講じる必要がある。
6.4-03					個人情報の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。 ・入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。 ・入退者の記録を定期的にチェックし、妥当性を確認する。	最低限	・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅱ．４．４．１【基本】）		適合可能	文献[05]にて、運用メンバーは一般社員とは分離された執務スペースで業務を行い、運用メンバーの執務スペースは監視カメラを設置し、入退室等が管理されていることが明記されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[05]	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者にて個人情報を格納している機器や媒体がある場合、物理的セキュリティ境界を設け、個人情報の物理的保存を行っている区画への入退管理を実施する必要がある。また入退者の記録を定期的にチェックし、妥当性の確認を実施する必要がある。
6.4-04					個人情報が存在するPC 等の重要な機器に盗難防止用チェーンを設置すること。	最低限	・サーバルームやラックの鍵管理を行うこと。（Ⅱ．４．４．６【基本】） ・受託する個人情報を保守に用いる端末に保存しない旨、自社の運用管理規程等に定めること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者にて個人情報を格納しているPC等がある場合、個人情報が存在するPC 等の重要な機器に盗難防止用チェーンを設置する必要がある。
6.4-05					覗き見防止の対策を実施すること。	最低限	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．７．１．３【基本】）		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者にて個人情報を格納しているPC等がある場合、覗き見防止フィルターを利用する必要がある。
6.4-06					防犯カメラ、自動侵入監視装置等を設置すること。	推奨	・重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像を予め定められた期間保存すること。（Ⅱ．４．４．２【推奨】）		適合可能	文献[05]にて、運用メンバーは一般社員とは分離された執務スペースで業務を行い、運用メンバーの執務スペースは監視カメラを設置し、入退室等が管理されていることが明記されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[05]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者にて個人情報を格納している機器や媒体がある場合、物理的セキュリティ境界を設け、個人情報の物理的保存を行っている区画への入退管理を実施する必要がある。また重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像を予め定められた期間保存する必要がある。
6.5-01		6.5	-	技術的な対策のみで全ての脅威に対抗できる保証はなく、一般的には運用管理による対策との併用は必須である。 しかし、その有効範囲を認識し適切な適用を行えば、技術的な対策は強力な安全対策の手段となりうる。ここでは「6.2.3 リスク分析」で列挙した脅威に対抗するために利用できる技術的な対策として下記の項目について解説する。 （1）利用者の識別及び認証 （2）情報の区分管理とアクセス権限の管理 （3）アクセスの記録（アクセスログ） （4）不正ソフトウェア対策 （5）ネットワーク上からの不正アクセス	情報システムへのアクセスにおける利用者の識別と認証を行うこと。	最低限	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】）	cybozu.com における不正アクセス対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/illegal_access/index.html cybozu.com における不正ログイン対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/bad_login/index.html	適合可能	文献[03]にて不正アクセス対策が実施されている旨を確認した。 また文献[04]にて不正ログイン対策が実施されている旨を確認し、パスワードの有効期限が設定可能である旨を確認した。 サイボウズ側では文献[05]にて、運用メンバーは一般社員とは分離された執務スペースで業務を行い、運用メンバーの執務スペースは監視カメラを設置し、入退室等が管理されていることが明記されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[03]文献[04]文献[05]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は情報システムへのアクセスにおける利用者の識別と認証を行う必要がある。
6.5-02					本人の識別・認証にユーザID とパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。	最低限	・同上		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者が本人の識別・認証にユーザID とパスワードの組み合わせを用いる場合、それらの情報を本人しか知り得ない状態に保つよう対策を行う必要がある。
6.5-03					本人の識別・認証に IC カード等のセキュリティ・デバイスを用いる場合には、IC カードの破損等、本人の識別情報が利用できない時を想定し、緊急時の代替手段による一時的なアクセスルールを用意すること。	最低限	–	運用メンバーは「入室制限エリア」と呼ばれる、一般社員とは隔離された執務スペースで業務を行っています。 詳細は以下の Web ページを参照ください。 https://www.cybozu.com/jp/security/vulnerability/index.html	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者が本人の識別・認証に IC カード等のセキュリティ・デバイスを用いる場合、IC カードの破損等、本人の識別情報が利用できない時を想定し、緊急時の代替手段による一時的なアクセスルールを用意する必要がある。
6.5-04					入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力の恐れがある場合には、クリアスクリーン等の防止策を講じること。	最低限	・受託情報を扱う運用端末に、クリアスクリーン等の防止策を講じることを、自社の運用管理規程等に定めること。	内規にて対策を定めています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力の恐れがある場合には、クリアスクリーン等の防止策を講じる必要がある。
6.5-05					動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意すること。	最低限	・データベースに格納されたデータの暗号化を行うこと。（Ⅲ．２．２．２【推奨】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。（Ⅲ．３．２．２【推奨】） ・受託した情報の処理に必要な、システムに関する動作確認に際し、原則個人情報を含むデータを使用せず、テスト用のデータを使用すること ・システムに関する動作確認に際し、やむを得ず受託した個人情報を使用する場合には、医療機関等の管理者と十分協議の上、必要な措置を講じて使用すること。	cybozu.com ではデータを保管する際には、データを暗号化しております。	適合可能	文献[09]にて、手動オペレーションによる操作は、すべて手順書を整備しており、手順書に従って実施することを徹底している旨が記載されている。また、全ての操作はログを自動記録しており、ルールが守られているかチェックできる体制となっている旨が記載されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[09]	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、動作確認等で個人情報を含むデータを使用するときは、暗号化を行うなど、漏えい等に十分留意する必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.5-06					医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。また、アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行うよう、運用管理規程で定めていること。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある。	最低限	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・提供するサービスにおいて、医療機関等の利用者の職種、担当業務等に応じたアクセス制御が可能な機能を含めること。 ・医療機関等の利用者の職種等に応じたアクセス制御の設定に関しては、医療機関等の管理者と協議の上、実際に設定する作業に関する役割も含めて合意すること。 ・医療機関等のアクセス管理に関する運用管理規程の内容に従った運用を行い、医療機関等の求めに応じて資料を提出できるようにすること。	cybozu.com における不正アクセス対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/illegal_access/index.html cybozu.com における不正ログイン対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/bad_login/index.html 内規にて運用管理規定を設け、アクセス可能範囲を定めております。 操作記録は運用管理者および、アクセスが許可された者のみがアクセスできる場所に保管しております。 以下のドキュメントについてもご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[03]にて不正アクセス対策が実施されている旨を確認した。 また文献[04]にて不正ログイン対策が実施されている旨を確認し、パスワードの有効期限が設定可能である旨を確認した。 文献[20]、文献[21]、文献[22]、文献[23]にて、医療従事者や関係職種ごとに利用するアプリケーションやデータへのアクセスおよび削除等の操作など、適切にアクセス管理が出来るような仕組みが提供されていることを確認した。	公開文書	文献[03]文献[04]文献[20]文献[21]文献[22]文献[23]	–	–	–	利用者及びSI事業者は、医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を実施する必要がある。
6.5-07					アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、ならびにログイン中に操作した患者が特定できること。 情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容等）を必ず行うこと。	最低限	・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。（Ⅲ．１．１．５【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】※ベストプラクティス(i)を実施すること。）		適合可能	文献[01]にて、監査ログが取得され、日次で該当のログについて確認をしている旨が記載されている。また該当のログについては運用管理者及びアクセスが許可されたものがアクセスできる場所に保管している旨が記載されている。	公開文書	文献[01]	–	–	–	利用者及びSI事業者は、アクセスの記録及び定期的なログの確認を行う必要がある。
6.5-08					アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じること。	最低限	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】） ・運用管理者とログのレビュー者のアクセス権を分離する等の、アクセスログの改ざん等に対する措置を講じること。		適合可能	文献[01]にて、ログについては運用管理者及びアクセスが許可されたものがアクセスできる場所に保管している旨が記載されている。	公開文書	文献[01]	–	–	–	利用者及びSI事業者は、システム管理権限を持つアカウントを適切に保護する必要がある。
6.5-09					アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある。	最低限	・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。（Ⅲ．１．１．５【基本】※ベストプラクティスの(i)～(iv)を実施すること）	NTP を利用して OS、ネットワーク機器等、正確な時刻源と時刻同期を実施しています。 以下のドキュメントについてもご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、NTP を利用してオペレーティングシステム・ネットワーク機器等、正確な時刻源と時刻同期を実施している旨が記載されている。	公開文書	文献[01]	–	–	–	利用者及びSI事業者は、医療情報システムにおける時刻同期を適切に行う必要がある。
6.5-10					システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（たとえばパターンファイルの更新の確認・維持）を行うこと。	最低限	・ASP・SaaS サービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。（Ⅲ．１．１．６【基本】） ・ASP・SaaS サービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。（Ⅲ．２．２．１【基本】）	脆弱性に対する対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html 下記ドキュメントもご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[05]にて、品質保証チームにおける脆弱性検証の実施、さらに信頼性を高めるため外部の調査機関による監査、有識者による脆弱性発見の取り組みを実施している旨が記載されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[05]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、構築した医療情報システムについて、脆弱性対策およびウイルス対策を適切に行う必要がある。
6.5-11					パスワードを利用者識別に使用する場合 システム管理者は以下の事項に留意すること。 (1) システム内のパスワードファイルでパスワードは必ず暗号化（可能なら不可逆変換が望ましい）され、適切な手法で管理及び運用が行われること。また、利用者識別にIC カード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること。 (2) 利用者がパスワードを忘れたり、盗用されたりするおそれがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類等のコピーを添付）し、本人以外が知り得ない方法で再登録を実施すること。 (3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること（設定ファイルにパスワードが記載される等があってはならない）。 また、利用者は以下の事項に留意すること。 (1) パスワードは定期的に変更し（最長でも2 ヶ月以内※D.5 に規定する 2 要素認証を採用している場合を除く。）、極端に短い文字列を使用しないこと。英数字、記号を混在させた8 文字以上の文字列が望ましい。 (2) 類推しやすいパスワードを使用しないこと、かつ類似のパスワードを繰り返し使用しないこと。類推しやすいパスワードには、自身の氏名や生年月日、辞書に記載されている単語が含まれるもの等がある。	最低限	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・自社において定めたパスワードポリシーが、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・利用者のパスワード発行等に関する手続及び業務範囲について、医療機関等と合意すること。	・内規にてパスワードを暗号化して保存すること、複雑性や管理方法を定めております。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf ・cybozu.com における不正アクセス対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/illegal_access/index.html ・cybozu.com における不正ログイン対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/bad_login/index.html	適合可能	システム利用者に対しては文献[03]にてクライアント証明書によるセキュアアクセスが実施されていることが明記されている。 文献[04]にて、パスワードの文字数・複雑さ・再利用制限・有効期間が利用者にて設定可能であることが明記されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[03]文献[04]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者は、cybozu.comにおけるパスワードポリシーが、医療機関等が求める内容を含むものであることを確認する必要がある。 利用者は、2要素認証を行っている場合を除き、パスワードを定期的に変更させる必要がある。 利用者は、類推しやすいパスワードの使用や、類似のパスワードの繰り返しの利用を行わないように周知する必要がある。
6.5-12					無線LAN を利用する場合 システム管理者は以下の事項に留意すること。 (1) 利用者以外に無線LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY 接続拒否等の対策をとること。 (2) 不正アクセスの対策を施すこと。少なくともSSID やMAC アドレスによるアクセス制限を行うこと。 (3) 不正な情報の取得を防止すること。例えばWPA2/AES 等により、通信を暗号化し情報を保護すること。 (4) 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、医療機関等の施設内で利用可能とする場合には留意すること。 (5) 無線LAN の適用に関しては、総務省発行の「安心して無線LAN を利用するために」を参考にすること。	最低限	・医療機関等がASP・SaaSの利用に際して無線LANを利用する場合に、医療機関等の無線LANが必要なセキュリティ対策について、事業者の役割、範囲等について合意すること。	cybozu.com 運用環境では、無線ネットワークは利用しておりません。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者がcybozu.comの利用に際して無線LANを利用する場合には、適切なセキュリティ対策を実施する必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.5-13					13．IoT 機器を利用する場合 システム管理者は以下の事項に留意すること。 (1) IoT 機器により患者情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。 (2) セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置のIoT 機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクについて患者等へ説明し、同意を得ること。また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。 (3) IoT 機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、適用すること。 (4) 使用が終了した又は不具合のために使用を停止した IoT 機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を講じること。	最低限	–	IoT機器は利用しないため、対象外。	対象外	IoT機器は利用しないため、対象外。	–	–	–	–	利用者及びSI事業者は、IoT機器の管理を適切に行う必要がある。
6.5-14					情報の区分管理を実施し、区分単位でアクセス管理を実施すること。	推奨	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１【基本】） ・組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。（Ⅱ．４．２．１【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・医療情報について、医療機関等が行う情報資産分類の区分に従い、アクセス制御を行うこと。	情報資産の利用に関する許容範囲については、以下のウェブページで公開しております。 プライバシーポリシー https://cybozu.co.jp/privacy/privacy-policy/ クラウドデータポリシー https://cybozu.co.jp/privacy/cloud-data-policy/ また内規にて情報オーナーを定め、アクセス制御方針に基づいて情報資産を管理しております。	適合可能	文献[15]にて、取り扱う情報資産の利用に関する許容範囲（利用可,能者、利用目的、利用方法、および廃棄）が明記されており、情報のライフサイクルという観点では問題ないと考える。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[15]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は情報の区分管理を実施し、区分単位でアクセス管理を実施する必要がある。
6.5-15					離席の場合のクローズ処理等を施すこと（クリアスクリーン：ログオフあるいはパスワード付きスクリーンセーバー等）。	推奨	・最低限3.と同様の対応を行う。	内規にて、離席時には第三者が容易に操作および閲覧ができないようスクリーンロック等の対策を講じることを定め、運用しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、医療機関等の利用者側の施設における、適切な端末管理（スクリーンロック等）を行う必要がある。
6.5-16					外部のネットワークとの接続点やDB サバ等の安全管理上の重要部分にはファイアウォール（ステートフルインスペクションやそれと同等の機能を含む）を設置し、ACL(アクセス制御リスト)等を適切に設定すること。	推奨	・データベースに格納されたデータの暗号化を行うこと。（Ⅲ．２．２．２【推奨】） ・外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。（Ⅲ．３．１．４【基本】） ・不正な通過パケットを自動的に発見、もしくは遮断する措置（IDS/IPSの導入等）を講じること。（Ⅲ．３．１．５【推奨】）	cybozu.com ではデータを保管する際には、データを暗号化しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、利用者側の施設等における外部ネットワークとの接続点において、適切なセキュリティ対策を実施する必要がある。
6.5-17					パスワードを利用者識別に使用する場合以下の基準を遵守すること。 （1） パスワード入力が不成功に終わった場合の再入力に対して一定不応時間を設定すること。 （2） パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない機構とすること。	推奨	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・自社において定めたパスワードポリシーが、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	cybozu.com における不正アクセス対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/illegal_access/index.html cybozu.com における不正ログイン対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/bad_login/index.html ネットワーク図を作成し、内規にて運用管理規定を設け、アクセス可能範囲を定めております。 操作記録は運用管理者および、アクセスが許可された者のみがアクセスできる場所に保管しております。 以下のドキュメントについてもご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[04]にて、パスワード再入力の失敗が一定数を超えた際のロックアウトが設定可能であること、またロックアウトを解除するまでの時間指定が設定可能であることを確認した。	公開文書	文献[04]	–	–	–	利用者は、cybozu.com におけるパスワードポリシーが、医療機関等が求める内容を含むものであることを確認する必要がある。
6.5-18					認証に用いられる手段としては、ID・パスワード＋バイオメトリクス又はICカード等のセキュリティ・デバイス＋パスワード若しくはバイオメトリクスのように 2 つの独立した要素を用いて行う方式（2 要素認証）等、より認証強度が高い方式を採用すること。ただし、情報システムを利用する端末に 2 要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め 2 要素以上（記憶・生体計測・物理媒体のいずれか 2 つ以上）の認証がなされていれば、2 要素認証と同等と考えてよい。	推奨	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・採用する認証手段・方式について、医療機関等と合意すること。	クライアント証明書を用いた認証（セキュアアクセス）を提供しております。詳細は以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/illegal_access/index.html	適合可能	文献[03]にてクライアント証明書およびID/パスワードの二要素認証が利用されていることを確認した。	公開文書	文献[03]	–	–	–	利用者及びSI事業者は、必要に応じて2要素認証などを導入する必要がある。
6.5-19					無線LAN のアクセスポイントを複数設置して運用する場合等は、マネジメントの複雑さが増し、侵入の危険が高まることがある。そのような侵入のリスクが高まるような設置をする場合、例えば802.1x や電子証明書を組み合わせたセキュリティ強化をすること。	推奨	・医療機関等がASP・SaaSの利用に際して無線LANを利用する場合に、医療機関等の無線LANが必要なセキュリティ対策についての、事業者の役割、範囲等について合意すること。	cybozu.com 運用環境では、無線ネットワークは利用していません。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、無線LANの管理を適切に行う必要がある。
6.5-20					IoT 機器を含むシステムの接続状況や異常発生を把握するため、IoT 機器・システムがそれぞれの状態や他の機器との通信状態を収集・把握し、ログとして適切に記録すること。	推奨	–	IoT機器は利用しないため、対象外。	対象外	IoT機器は利用しないため、対象外。	–	–	–	–	–	利用者及びSI事業者は、IoT機器の管理を適切に行う必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応						SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.6-01		6.6	-	医療機関等は、情報の盗難や不正行為、情報設備の不正利用等のリスク軽減をはかるため、人による誤りの防止を目的とした人的安全対策を策定する必要がある。これには守秘義務と違反時の罰則に関する規定や教育、訓練に関する事項が含まれる。 医療情報システムに関連する者として、次の5 種類を想定する。 (a) 医師、看護師等の業務で診療に関わる情報を取扱い、法令上の守秘義務のある者 (b) 医事課職員、事務委託者等の医療機関等の事務の業務に携わり、雇用契約の下に医療情報を取扱い、守秘義務を負う者 (c) システムの保守業者等の雇用契約を結ばずに医療機関等の業務に携わる者 (d) 見舞い客等の医療情報にアクセスする権限を有しない第三者 (e) 診療録等の外部保存の委託においてデータ管理業務に携わる者	（1） 従業者に対する人的安全管理措置 医療機関等の管理者は、個人情報の安全管理に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること。 1. 法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。	最低限	従業員の雇用時に社内規定（情報セキュリティ規則等）への遵守について同意確認を取っています。 雇用時および雇用後も必要に応じてセキュリティ・コンプライアンスに関する教育を実施しています。 以下の文書も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、自身の管理下にある従業員等については、適切に管理する必要がある。
6.6-02					2. 定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。	最低限	・全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。（Ⅱ．５．２．１【基本】）	個人情報データベース等に対し、合理的な技術的施策、および従業員に対する啓発活動を行なうことにより、情報の紛失、改ざん、漏洩等の防止に努めております。 以下のウェブページもご参照ください。 プライバシーポリシー https://cybozu.co.jp/privacy/privacy-policy/	適合可能	文献[15]にて従業員に対する啓発活動を行なう旨が記載されている。	公開文書	文献[15]	–	–	–	利用者及びSI事業者は、定期的に従業者に対し個人情報の安全管理に関する教育訓練を実施する必要がある。
6.6-03					3. 従業者の退職後の個人情報保護規程を定めること。	最低限	・従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること。（Ⅱ．５．３．１【基本】）	内規にて従業員の退職・休職時は、全てのシステムのアカウントを削除または使用停止すること、アクセス権・リモートアクセス権は削除または使用停止すること、業務PC・鍵・カードキー等を回収することを情報セキュリティ規則で明記していることを定めています。また退職時には従業員との秘密保持の合意書を締結しています。 以下の文書も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、従業員の退職・休職時は、全てのシステムのアカウントを削除または使用停止すること、アクセス権・リモートアクセス権は削除または使用停止すること、業務PC・鍵・カードキー等を回収することを情報セキュリティ規則で明記していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は従業者の退職後の個人情報保護規程を定める必要がある。
6.6-04					サーバ室等の管理上重要な場所では、モニタリング等により従業者に対する行動の管理を行うこと。	推奨	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、罰告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．７．１．３【基本】） ・重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること。（Ⅲ．４．４．３【基本】）	サイボウズ社内の運用体制については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html 運用メンバーは一般社員とは分離された執務スペースで業務を行っています。 運用メンバーの執務スペースは監視カメラを設置し、入退室等が管理されています。	適合可能	文献[05]にて、運用メンバーは一般社員とは分離された執務スペースで業務を行い、運用メンバーの執務スペースは監視カメラを設置し、入退室等が管理されていることが明記されている。	公開文書	文献[05]	–	–	–	–
6.6-05					医療機関等の事務、運用等を外部の事業者に委託する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。 ① 受託する事業者に対する包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結すること	最低限	・従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．２【基本】） ・雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。（Ⅱ．５．１．１【基本】）	従業員の雇用時に内規（情報セキュリティ規則等）への遵守について同意確認を取っています。 雇用時および雇用後も必要に応じてセキュリティ・コンプライアンスに関する教育を実施しています。 セキュリティ違反を犯した従業員は、懲戒の対象になることを情報セキュリティ規則にて定めております。 以下の文書も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者は、医療情報システムを提供する事業者に対する包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結する必要がある。
6.6-06					② 保守作業等の医療情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認を行うこと。	最低限	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】）	保守作業の体制については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/human_error/index.html 全ての作業内容を自動記録し、ルールが順守されていることをチェックできる体制となっています。	適合可能	文献[09]にて、手動オペレーションによる操作は、すべて手順書を整備しており、手順書に従って実施することを徹底している旨が記載されている。また、全ての操作はログを自動記録しており、ルールが守られているかチェックできる体制となっている旨が記載されている。	公開文書	文献[09]	–	–	–	利用者は、利用者自身のユーザーによるアクセスを制御し、そのようなアクセスを適切に確認するとともに、作業内容等を確認する必要がある。
6.6-07					③ 清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。	最低限	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．７．１．３【基本】） ・重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること。（Ⅲ．４．４．３【基本】）	手動オペレーションに伴うミスの防止策は、以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/human_error/index.html	適合可能	文献[09]にて、手動オペレーションによる操作は、すべて手順書を整備しており、手順書に従って実施することを徹底している旨が記載されている。また、全ての操作はログを自動記録しており、ルールが守られているかチェックできる体制となっている旨が記載されている。	公開文書	文献[09]	–	–	–	利用者は、利用者側の施設等における入退室管理を適切に実施する必要がある。
6.6-08					④ 委託事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託事業者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こと。	最低限	・外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること。（Ⅱ．２．２．１【基本】） ・情報資産へのアクセスが可能となる外部組織との契約においては、想定される全てのアクセスについて、その範囲を規定すること。（Ⅱ．２．２．２【基本】） ・連携ASP・SaaS 事業者が提供するASP・SaaS サービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携ASP・SaaS 事業者によって確実に実施されることを担保すること。（Ⅱ．３．１．１【基本】） ・連携ASP・SaaS 事業者が提供するASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．３．１．２【基本】） ・外部組織に対して再委託等を行う場合には、事前に医療機関等の管理者に対して説明を行い、契約において体制を明確にすること。 ・外部組織に対して、自社と同等の個人情報保護指針等について遵守させること。 ・外部組織においても表３－９（外部と個人情報を含む医療情報を交換する場合の安全管理におけるASP・SaaS事業者への要求事項）について遵守させること。	内規にて外部に関するセキュリティ要求事項を定めております。 ISMS 認証対象業務について、再委託は行っておりません。 従業員の雇用時に社内規定（情報セキュリティ規則等）への遵守について同意確認を取っています。 雇用時および雇用後も必要に応じてセキュリティ・コンプライアンスに関する教育を実施しています。 内規にて従業員の退職・休職時は、全てのシステムのアカウントを削除または使用停止すること、アクセス権・リモートアクセス権は削除または使用停止すること、業務PC・鍵・カードキー等を回収することを内規で定めています。また退職時には従業員との秘密保持の合意書を締結しています。 以下の文書も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	–
6.6-09					プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏づけられた守秘契約等の秘密保持の対策を行うこと。	推奨	・従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．２【基本】） ・外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること。（Ⅱ．２．２．１【基本】） ・情報資産へのアクセスが可能となる外部組織との契約においては、想定される全てのアクセスについて、その範囲を規定すること。（Ⅱ．２．２．２【基本】） ・雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。（Ⅱ．５．１．１【基本】）		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者が構築する環境については、利用者及びSI事業者は、外部保守要員が個人情報にアクセスする際は、守秘契約等の秘密保持の対策を行う必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.7-01		6.7	-	医療に係る電子情報は破棄に関しても安全性を確保する必要がある。破棄は確実に行う必要がある。しかし、例えばデータベースのように情報が互いに関連して存在する場合は、一部の情報を不適切に破棄したために、その他の情報が利用不可能になる場合もあり、注意しなくてはならない。 実際の破棄に備えて、事前に破棄の手順を明確化しておくべきである。	「6.1 方針の制定と公表」で把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めること。	最低限	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．4．1．1【基本】） ・組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。（Ⅱ．4．2．1【基本】） ・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．7．1．1【基本】） ・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．5．3．2【基本】） ・自社において定めた情報の破棄手順が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	内規にて手順を定めております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者は、医療に係る電子情報の破棄について、手順等を定める必要がある。
6.7-02					情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認すること。	最低限	・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．5．3．2【基本】）	内規にて手順を定めております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認する必要がある。 外部保存を受託する機関に破棄を委託した場合は、「6.6 人的安全対策（2）事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する医療機関等が確実に情報の破棄が行われたことを確認すること。
6.7-03					外部保存を受託する機関に破棄を委託した場合は、「6.6 人的安全対策（2）事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する医療機関等が確実に情報の破棄が行われたことを確認すること。	最低限	・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．5．3．2【基本】） ・情報の破棄を実施した場合に、電磁記録媒体の消磁、物理的破壊等、情報の削除方法を含む実施内容を医療機関等に対して報告し、破棄記録等を提出すること。	内規にて手順を定めております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	
6.7-04					運用管理規程において下記の内容を定めること。 (a) 不要になった個人情報を含む媒体の破棄を定める規程の作成	最低限	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．4．1．1【基本】） ・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．7．1．1【基本】） ・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．5．3．2【基本】） ・自社において定めた情報の破棄手順が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	内規にて手順を定めております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	
6.8-01		6.8	-	医療情報システムの可用性を維持するためには定期的なメンテナンスが必要である。メンテナンス作業には主に障害対応や予防保守、ソフトウェア改訂等があるが、特に障害対応においては、原因特定や解析等のために障害発生時のデータを利用することがある。この場合、システムのメンテナンス要員が管理者モードで直接医療情報に触れる可能性があり、十分な対策が必要になる。具体的には以下の脅威が存在する。 ・個人情報保護の点では、修理記録の持ち出しによる暴露、保守センター等で解析中のデータの第三者による覗き見や持ち出し等 ・真正性の点では、管理者権限を悪用した意図的なデータの改ざんや、オペレーションミスによるデータの改変等 ・見読性の点では、意図的なマシンの停止や、オペレーションミスによるサービス停止等 ・保存性の点では、意図的な媒体の破壊及び初期化や、オペレーションミスによる媒体の初期化やデータの上書き等	動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うとともに、終了後は確実にデータを消去する等の処理を行うことを求めること。	最低限	・連携ASP・SaaS 事業者が提供するASP・SaaS サービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携ASP・SaaS 事業者によって確実に実施されることを担保すること。（Ⅱ．3．1．1【基本】） ・雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。（Ⅱ．5．1．1【基本】） ・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．5．1．2【基本】） ・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．5．3．2【基本】） ・受託した情報の処理に必要な、システムの動作確認に際し、原則個人情報を含むデータを使用せず、テスト用のデータを使用すること ・システムに関する動作確認に際し、やむを得ず受託した個人情報を使用する場合には、医療機関等の管理者と十分協議の上、必要な措置を講じて使用すること。	個人情報を含む運用データを試験に利用してはならない旨、内規にて定めております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	テストデータ・個人情報の使用については利用者及びSI事業者の責任にて実施する必要がある。
6.8-02					メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、及びアクセスした場合は対象個人情報を含む作業記録を残すこと。これはシステム利用者を模して操作確認を行うための識別・認証についても同様である。	最低限	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．7．1．2【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．2．1．3【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．3．1．2【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】）	保守作業の体制については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/human_error/index.html	適合可能	文献[09]にて、手動オペレーションによる操作は、すべて手順書を整備しており、手順書に従って実施することを徹底している旨が記載されている。また、全ての操作はログを自動記録しており、ルールが守られているかチェックできる体制となっている旨が記載されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[09]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者は、オペレーション実行時の運行状況を確認し、オペレーションを記録する必要がある。 利用者が使用する端末における不正プログラムへの防御対策については、利用者が対策する必要がある。 利用者は、利用者自身のユーザーによるアクセスを制限し、そのようなアクセスを適切に確認するとともに、自らが定めた監査ポリシーに従って記録されたログなどを、定期的に確認する必要がある。 ネットワーク構成図は利用者側にて作成する必要がある。
6.8-04					保守要員の離職や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えておくこと。	最低限	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．3【基本】） ・外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること。（Ⅱ．2．2．1【基本】） ・従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること。（Ⅱ．5．3．1【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・保守等の体制変更が生じた場合に、医療機関等に行う報告の範囲、内容等について合意すること。	サイボウズ社員以外が関与することはないため、対象外。	対象外	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者が使用する端末における不正プログラムへの防御対策については、利用者が対応を講じる必要がある。 ネットワーク構成図は利用者側にて作成する必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応						SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.8-05					保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認すること。	最低限	・サービス提供に必要な保守業務を行うに際して、医療機関等の管理者に対して書面等により作業の事前及び事後に通知を行うこと、及び事前の了解を必要とする作業等について医療機関等と合意すること。	サイボウズではデータセンターを運営する外部事業者に、サーバラックの施錠管理などの業務を委託しております。データセンターのラックは施錠および鍵管理をデータセンター事業者に依頼しております。施錠を含めた鍵の利用はデータセンター事業者にて記録が取られています。 サイボウズ社員以外が、cybozu.com 運用環境にログインすることはありません。 システムの運用担当者の作業についてはすべて記録を残しております。また作業を実施する際には変更管理に則り、作業内容について責任者の承認を得てから実施しております。	適合可能	文献[09]にて、手動オペレーションによる操作は、すべて手順書を整備しており、手順書に従って実施することを徹底している旨が記載されている。また、全ての操作はログを自動記録しており、ルールが守られているかチェックできる体制となっている旨が記載されている。	公開文書	文献[09]	–	–	–	利用者及びSI事業者の責任者は、保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求め、それらの書類を逐一承認する必要がある。
6.8-06					保守会社と守秘義務契約を締結し、これを遵守させること。	最低限	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３【基本】） ・サービス提供に際して、医療機関等と守秘義務契約を締結すること。	内規にて委託業者と損害賠償上限を明記した秘密保持契約を結ぶことを定め、遵守しております。	対象外	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者が外部の保守会社を利用する場合、保守会社と守秘義務契約を締結し、これを遵守させる必要がある。
6.8-07					保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること。	最低限	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３【基本】） ・情報の持ち出しに関する自社において定めた運用管理規程が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	サイボウズ社員以外が関与することはないため、対象外。	対象外	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者が外部の保守会社を利用する場合、保守会社が個人情報を組織外に持ち出さなければならない場合には、運用管理規程を定めることを求め、責任者が逐一承認する必要がある。
6.8-08					リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること。	最低限	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】） ・サービス提供に必要なシステムの保守をリモートメンテナンスで行う場合の医療機関等の管理者に対する報告、承認等について、医療機関等と合意すること。	保守作業の体制については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/human_error/index.html 全ての作業内容を自動記録し、ルールが順守されていることをチェックできる体制となっています。	適合可能	リモートに限らずすべてのメンテナンスに関して、文献[09]に、手動オペレーションによる操作はすべて手順書を整備しており、手順書に従って実施することを徹底していること、また全ての操作はログを自動記録しており、ルールが守られているかチェックできる体制となっている旨が記載されている。	公開文書	文献[09]	–	–	–	利用者及びSI事業者が外部の保守会社を利用し、リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに作業内容を責任者が確認する必要がある。
6.8-09					再委託が行われる場合は、再委託する事業者にも保守会社の責任で同等の義務を課すこと。	最低限	・外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること。（Ⅱ．２．２．１【基本】） ・連携ASP・SaaS 事業者が提供するASP・SaaS サービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携ASP・SaaS 事業者によって確実に実施されることを担保すること。（Ⅱ．３．１．１【基本】） ・連携ASP・SaaS 事業者が提供するASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．３．１．２【基本】）	内規にて委託業者と損害賠償上限を明記した秘密保持契約を結ぶことを定め、遵守しております。また再委託は行っておりません。	対象外	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者が外部の保守会社を利用し、外部の保守会社から再委託が行われる場合は、再委託する事業者にも保守会社の責任で同等の義務を課す必要がある。
6.8-10					詳細なオペレーション記録を保守操作ログとして記録すること。	推奨	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２【基本】）	保守作業の体制については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/human_error/index.html 全ての作業内容を自動記録し、ルールが順守されていることをチェックできる体制となっています。	適合可能	文献[09]にて、手動オペレーションによる操作はすべて手順書を整備しており、手順書に従って実施することを徹底していること、また、全ての操作はログを自動記録しており、ルールが守られているかチェックできる体制となっている旨が記載されている。	公開文書	文献[09]	–	–	–	利用者及びSI事業者が外部の保守会社を利用する場合、詳細なオペレーション記録を保守操作ログとして記録させる必要がある。
6.8-11					保守作業時には医療機関等の関係者立会いのもとで行うこと。	推奨	・サービス提供に必要な保守業務を医療機関施設内で行う際に、医療機関等の立会いの下で実施する旨を、医療機関等と合意すること。	サイボウズは cybozu.com の運用に関して ISMS 認証を受けております。 認証登録番号：IS 577142 内規に基づき内部監査を実施し、ISMS 認証審査の過程で外部からの審査を受けております。 また cybozu.com 運用基盤上で動作するアプリケーションについては、年に１回脆弱性診断を受け、その結果を以下のウェブページで公開しております。 https://www.cybozu.com/jp/productsecurity/ 上記内容をもち、医療機関の立ち合いの元作業を行うことの代替とさせていただいております。	適合可能	保守作業に関しては、出来る限り自動化され、またすべての手動オペレーションの作業記録がされていることが文献[09]にて確認出来た。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[09]	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者が外部の保守会社を利用する場合、保守作業時には立会いを行う必要がある。
6.8-12					作業員各人と保守会社との守秘義務契約を求めること。	推奨	・従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．２【基本】） ・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．５．１．２【基本】）	従業員の雇用時に社内規定（情報セキュリティ規則等）への遵守について同意確認を取っています。 雇用時および雇用後も必要に応じてセキュリティ・コンプライアンスに関する教育を実施しています。 内規にて従業員の退職・休職時は、全てのシステムのアカウントを削除または使用停止すること、アクセス権・リモートアクセス権は削除または使用停止すること、業務PC・鍵・カードキー等を回収することを内規で定めています。また退職時には従業員との秘密保持の合意書を締結しています。 cybozu.com をご利用いただくにあたり、利用規約に同意をいただくことになっております。 利用規約内に、当社とお客様との間でセキュリティ要求事項を満たすための契約事項を締結する旨定めております。 cybozu.com 利用規約 https://www.cybozu.com/jp/terms/ 以下の文書も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者が外部の保守会社を利用する場合、作業員各人と保守会社との間の守秘義務契約締結を求める必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応						SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.8-13					保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、詳細な作業記録を残すことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。	推奨	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】） ・個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、医療機関等の管理者による監査の内容、範囲について、医療機関等と合意すること。	サイボウズ社員以外が関与することはないため、対象外。	対象外	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者が外部の保守会社を利用する場合、保守会社が個人情報を組織外に持ち出さなければならない場合には、運用管理規程を定めることを求め、責任者が逐一承認する必要がある。
6.8-14					保守作業に関わるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べて表示し、かつ指定時間内でどの患者に何回のアクセスが行われたかが確認できる仕組みが備わっていること。	推奨	・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】）	保守作業の体制については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/human_error/index.html 全ての作業内容を自動記録し、ルールが順守されていることをチェックできる体制となっています。	適合可能	文献[09]にて、全ての操作はログを自動記録しており、ルールが守られているかチェックできる体制となっている旨が記載されている。	公開文書	文献[09]	–	–	–	患者情報に対するアクセスの記録は利用者側もしくはSI事業者側にて対応する必要がある。
6.9-01		6.9	-	昨今、医療機関等において医療機関等の従業者や保守業者による情報及び情報機器の持ち出しにより、個人情報を含めた情報が漏えいする事案が発生している。 一方で、在宅医療、訪問診療等の増加、モバイル端末の発展により医療情報を持ち出すニーズや機会が増加していることも事実である。 情報の持ち出しについては、ノートパソコン、スマートフォンやタブレットのような情報端末やCD-R、USB メモリのような情報記録可搬媒体が考えられる。また、情報をほとんど格納せず、ネットワークを通じてサーバにアクセスして情報を取り扱う端末（シンクライアント）のような情報機器も考えられる。 まず重要なことは、「6.2 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）の実践」の「6.2.2 取扱情報の把握」で述べられているように適切に情報の把握を行い、「6.2.3 リスク分析」を実施することである。 その上で、医療機関等において把握されている情報もしくは情報機器を持ち出しておいのか、持ち出してはならないかの切り分けを行うことが必要である。切り分けを行った後、持ち出してよいとした情報もしくは情報機器に対して対策を立てなくてはならない。 適切に情報が把握され、リスク分析がなされていれば、それらの情報や情報機器の管理状況が明確になる。例えば、情報の持ち出しについては許可制にする、情報機器は登録制にする等も管理状況を把握するための方策となる。 一方、自宅等の医療機関等の管轄外のパソコン（情報機器）で、可搬媒体に格納して持ち出した情報を取り扱う時に、コンピュータウイルスや不適切な設定のされたソフトウェア（Winny 等）、外部からの不正アクセスによって情報が漏えいすることも考えられる。この場合、情報機器が基本的には個人の所有物となるため、情報機器の取り扱いについての把握や規制は難しくなるが、情報の取り扱いについては医療機関等の情報の管理者の責任において把握する必要性はある。 このようなことから、情報もしくは情報機器の持ち出しについては組織的な対策が必要となり、組織として情報もしくは情報機器の持ち出しをどのように取り扱うかという方針が必要といえる。また、小規模な医療機関等であって、組織的な情報管理体制を行っていない場合でも、可搬媒体や情報機器を用いた情報の持ち出しは想定されることからリスク分析を実施し、対策を検討しておくことは必要である。 ただし、この際留意すべきは、可搬媒体や情報機器による情報の持ち出し特有のリスクである。情報を持ち出す場合は、可搬媒体や情報機器の盗難、紛失、置き忘れ等の人による不注意、過誤のリスクの方が医療機関等に設置されている情報システム自体の脆弱性等のリスクよりも相対的に大きくなる。 従って、情報もしくは情報機器の持ち出しについては、組織的な方針を定めた上で、人的安全対策をさらに施す必要がある。	組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること。	最低限	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１【基本】） ・情報の持ち出しに関する自社において定めた運用管理規程が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	組織としてリスク分析を行い、内規にて以下を定めております。 - 情報および、情報機器の持ち出しに関する方針 - 情報資産の管理方法 - 情報資産の盗難、紛失時の対応	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定める必要がある。
6.9-02					運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。	最低限	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３【基本】） ・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１【基本】） ・情報の持ち出しに関する自社において定めた運用管理規程が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者が定める運用管理規程では、持ち出した情報及び情報機器の管理方法を定める必要がある。
6.9-03					情報を格納した可搬媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程に定めること。	最低限	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３【基本】） ・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１【基本】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。 （Ⅲ．５．３．１【基本】） ・自社において定めた機器・媒体の盗難、紛失が生じた際の対応についての手順等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、情報を格納した可搬媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程に定める必要がある。
6.9-04					運用管理規程で定めた盗難、紛失時の対応を従業者等に周知徹底し、教育を行うこと。	最低限	・全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。（Ⅱ．５．２．１【基本】） ・従業員が、情報セキュリティポリシーもしくはASP・SaaS サービス提供上の契約に違反した場合の対応手続を備えること。（Ⅱ．５．２．２【基本】）		適合可能	文献[15]には、個人情報を取り扱う部門ごとに管理責任者を置き、個人情報の適切な管理に努めること、および従業員に対する啓発活動を行なうことにより、情報の紛失、改ざん、漏洩等の防止に努めることが明記されている。	公開文書	文献[15]	–	–	–	利用者及びSI事業者にも啓発活動を実施する必要がある。
6.9-05					医療機関等や情報の管理者は、情報が格納された可搬媒体若しくは情報機器の所在について台帳を用いる等して把握すること。	最低限	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１【基本】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。 （Ⅲ．５．３．１【基本】）	内規にて情報資産の責任者として「情報責任者」を定め、責任者の指示の元、 情報資産を「情報資産台帳」に登録、管理しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者においても情報が格納された可搬媒体若しくは情報機器の所在について台帳を用いる等して把握する必要がある。
6.9-06					情報機器に対して起動パスワード等を設定すること。設定に当たっては推定しやすいパスワード等の利用を避けたり、定期的にパスワードを変更する等の措置を行うこと。	最低限	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３【基本】）	パスワードは推測を困難にすべく、複雑度が高いものを設定するよう内規で義務付けています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者においても情報機器に対して起動パスワード等を設定する必要がある。設定に当たっては推定しやすいパスワード等の利用を避けたり、定期的にパスワードを変更する等の措置を行う必要がある。
6.9-07					盗難、置き忘れ等に対応する措置として、情報に対して暗号化したりアクセス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こと。	最低限	・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。 （Ⅲ．５．３．１【基本】）	内規にて書類・記録メディアの保管・管理ルールを定めております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、盗難、置き忘れ等に対応する措置として、情報に対して暗号化したりアクセス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必要がある。
6.9-08					持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入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こと。なお、ネットワークに接続する場合は「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」の規定を順守すること。特に、スマートフォンやタブレットのようなモバイル端末では公衆無線 LAN を利用できる場合があるが、公衆無線LAN は6.5 章C-11 の基準を満たさないことがあるため、利用できない。ただし、公衆無線 LAN しか利用できない環境である場合に限り、利用を認める。利用する場合は6.11 章で述べている基準を満たした通信手段を選択すること。	最低限	・運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行うこと。技術的せい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。 （Ⅲ．５．２．１【基本】） ・受託した情報を可搬媒体により外部に持ち出し、受託情報の処理を行わない旨を、自社の運用管理規程等に含め、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	業務端末のウイルス対策、プログラムのインストール、媒体持ち出しについて内規に基づいて対策しています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応						SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.9-09					持ち出した情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールすること。業務に使用しないアプリケーションや機能については削除あるいは停止するか、業務に対して影響がないことを確認して用いること。	最低限	–		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者にて情報機器を持ち出す場合、持ち出した情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールする必要がある。業務に使用しないアプリケーションや機能については削除あるいは停止するか、業務に対して影響がないことを確認して用いる必要がある。
6.9-10					個人保有の情報機器（パソコン、スマートフォン、タブレット等）であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、管理者は1～5 の対策を行うとともに、管理者の責任において上記の6．7．8．9 と同様の要件を順守させること。	最低限	・全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。（Ⅱ． 5． 2． 1【基本】） ・従業員が、情報セキュリティポリシーもしくはASP・SaaS サービス提供上の契約に違反した場合の対応手続を備えること。（Ⅱ． 5． 2． 2【基本】）	モバイル端末を含む、私物の業務端末を社外から利用する場合のルールを内規にて定めております。内規では「覗き見防止フィルターを利用すること」などを定めております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者が個人所有の情報機器（パソコン、スマートフォン、タブレット等）を利用する場合、個人保有の情報機器であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、管理者は1～5の対策を行うとともに、管理者の責任において上記の6、7、8、9 と同様の要件を順守させる必要がある。
6.9-11					外部での情報機器の覗き見による情報の露見を避けるため、ディスプレイに覗き見防止フィルタ等を張ること。	推奨	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ． 7． 1． 3【基本】）		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者が外部で情報機器を利用する場合、外部での情報機器の覗き見による情報の露見を避けるため、ディスプレイに覗き見防止フィルタ等を張る必要がある。
6.9-12					情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせて用いること。	推奨	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ． 3． 1． 3【基本】）	サイボウズ社内の運用体制については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html 運用メンバーは一般社員とは分離された執務スペースで業務を行っています。 運用メンバーの執務スペースは監視カメラを設置し、入退室等が管理されています。	適合可能	文献[05]にて、情報へアクセスするには操作端末へのID/パスワードでの認証とは別に運用メンバーの執務スペースへ入るための入退室が管理されている旨が記載されている。	公開文書	文献[05]	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-13					情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること。	推奨	・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ． 5． 3． 1【基本】）	内規にて書類・記録メディアの保管・管理ルールを定めております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者が情報格納用の可搬媒体や情報機器を利用する場合、全て登録し、登録されていない機器による情報の持ち出しを禁止する必要がある。
6.9-14					スマートフォンやタブレットを持ち出して使用する場合、以下の対策を行うこと。 ・BYODは原則として行わず、機器の設定の変更は管理者のみが可能とすること。 ・紛失、盗難の可能性を十分考慮し、可能な限り端末内に患者情報を置かないこと。やむを得ず患者情報が端末内に存在するか、当該端末を利用すれば容易に患者情報にアクセスできる場合は、一定回数パスワード入力を誤った場合は端末を初期化する等の対策を行うこと。	推奨	–	モバイル端末を含む、私物の業務端末を社外から利用する場合のルールを内規にて定めております。紛失・盗難の可能性を考慮し、MDM サービスの導入を義務付け、一定回数以上のログイン施行があった場合に端末を初期化する設定としております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.10-01		6.10	-	災害時、中でも大規模災害時には医療情報システム だけでなく、医療機関の様々な機能や人的能力に変化が生じる。その一方で、そのような事態では医療の需要が高まり、平常時以上の対応が求められることもある。このような事態に可能な限り対応するためには、普段からあらゆるレベルの異常時を想定し、対策を立て、文書化し、訓練を繰り返すことが有用である。このような対策を事業継続計画(BCP：Business Continuity Plan)と呼ぶ。 我が国は大規模な自然災害が比較的多く見られ、事例の蓄積も多い。そのため適切なBCPの作成と訓練は可能であり、必須の事項と考えられる。医療機関全体のBCP は本ガイドラインの範疇を超えるため、ここでは「6.2.3 リスク分析」の「⑦医療情報システム」に掲げる自然災害やサイバー攻撃によるIT 障害等の非常時に、医療情報システムが通常の状態で使用が出来ない事態に陥った場合における医療情報システムのBCP や留意事項について述べる。ただし、医療機関全体のBCP の一部として医療サービスの提供が最優先されるように、整合性のある対策にならなければならないことは言うまでもない。 「通常の状態で使用できない」とは、システム自体が異常動作または停止になる場合と、使用環境が非定常状態になる場合がある。前者としては、医療情報システムが損傷を被ることにより、システムの縮退運用あるいは全面停止に至り、医療サービス提供に支障発生が想定される場合である。後者としては、自然災害発生時には多数の傷病者が医療サービスを求める状態になり、医療情報システムが正常であったとしても通常時のアクセス制御下での作業では著しい不都合の発生が考えられる場合である。この際の個人情報保護に関する対応、「生命、身体の保護のためであって、本人の同意を得ることが困難であるとき」に相当すると解せられる。	医療サービスを提供し続けるためのBCP の一環として"非常時"と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。	最低限	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ． 2． 1． 3【基本】） ・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ． 4． 1． 1【基本】） ・組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。（Ⅱ． 4． 2． 1【基本】） ・自社において定めた非常時におけるBCPに関する運用手順等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	cybozu.com における災害対策については、以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/disaster_control/index.html 事業継続計画において想定される緊急事態を列挙し、リスク対策を行っています。非常時には対策本部を設置し、復旧に向けた作業を行います。	適合可能	文献[07]にて災害対策が記載されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[07]	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者が医療サービスを提供し続けるためのBCP の一環として"非常時"と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておく必要がある。
6.10-02					正常復帰後に、代替手段で運用した間のデータ整合性を図る規約を用意すること。	最低限	同上	cybozu.com の災害対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/disaster_control/ cybozu.com の保証範囲については、利用規約に定めがございます。 https://www.cybozu.com/jp/terms/	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、正常復帰後に代替手段で運用した間のデータ整合性を図る規約を用意する必要がある。
6.10-03					非常時の情報システムの運用 ・「非常時のユーザアカウントや非常時用機能」の管理手順を整備すること。 ・非常時機能が定常時に不適切に利用されることがないように、もし使用された場合には使用されたことが多くの人にわかるようにする等、適切に管理及び監査をすること。 ・非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用が出来ないように変更しておくこと。 ・標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、関係先への連絡手段や紙での運用等の代替手段を準備すること。	最低限	・自社において定めた非常時におけるアクセス管理の対応方法の内容（非常時用のユーザアカウントに関する内容含む）が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	事業継続計画および、事業継続計画における手順書にて、非常時の管理手順を整備しております。事業継続計画については、年次で有効性を試験しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、利用者が使用する端末については、障害時・災害時に利用者自身が実施すべきコンピュータシステムの復旧手順を明確にする必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.10-04					サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、“非常時”と判断した上で所管官庁への連絡を行うこと。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。 連絡先 厚生労働省 医政局研究開発振興課医療技術情報推進室（03-3595-2430） ※独立行政法人等においては、各法人の情報セキュリティポリシー等に基づき所管課へ連絡すること。 なお、情報処理推進機構は、マルウェアや不正アクセスに関する技術的な相談を受け付ける窓口を開設している。標的型メールを受信した、Webサイトが何者かに改ざんされた、不正アクセスを受けた等のおそれがある場合は、下記連絡先に相談することが可能である。 連絡先 情報処理推進機構 情報セキュリティ安心相談窓口（03-5978-7509）	最低限	・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を行うこと。稼働停止を検知した場合は、利用者に速報を通知すること。（Ⅲ．１．１．１【基本】） ・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の障害監視（サービスが正常に動作していることの確認）を行うこと。障害を検知した場合は、利用者に速報を通知すること。（Ⅲ．１．１．２【基本】） ・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を行うこと。また、利用者との取決めに基づいて、監視結果を利用者に通知すること。（Ⅲ．１．１．３【推奨】） ・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）に係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告を利用者に対して行うこと。（Ⅲ．１．１．８【基本】） ・外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報すること。（Ⅲ．３．２．５【推奨】） ・所管官庁に対して法令に基づく資料を円滑に提出できるよう、ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等は国内法の適用が及ぶ場所に設置すること。	障害発生時には cybozu.com の利用者の方に以下のサイトにて適宜通知を行っております。 https://cs.cybozu.co.jp/cybozucom/ 各ドメインの障害発生状況については、以下のサイトで確認することが出来ます。 cybozu.com 稼働状況 https://status.cybozu.com/status/ サービスを構成するプラットフォームはすべて日本国内（東日本・西日本）のデータセンターで管理しています。 https://www.cybozu.com/jp/security/data_loss/index.html	適合可能	文献[13]にて、利用者へ適宜通知がされていることを確認した。	公開文書	文献[13]	–	–	–	所管官庁への連絡は利用者側で実施する必要がある。 利用者が使用する端末については、利用者が対策する必要がある。また必要に応じて、情報共有機関やセキュリティベンダー等と連携する必要がある。 利用者は、各種資源の能力及び使用状況の確認を行い、システムの性能強化や機能強化、組み合わせの再検討等を行う必要がある。
6.11-01		6.11	-	ここでは、組織の外部と情報交換を行う場合に、個人情報保護及びネットワークのセキュリティに関して特に留意すべき項目について述べる。ここでは、双方向だけではなく、一方向の伝送も含む。外部と診療情報等を交換するケースとしては、地域医療連携で医療機関、薬局、検査会社等と相互に連携してネットワークで診療情報等をやり取りする、診療報酬の請求のために審査支払機関等とネットワークで接続する、ASP・SaaS 型のサービスを利用する、医療機関等の従事者がノートパソコンの様なモバイル型の端末を用いて業務上の必要に応じて医療機関等の情報システムに接続する、患者等による外部からのアクセスを許可する、等が考えられる。 医療情報をネットワークを利用して外部と交換する場合、送信元から送信先に確実に情報を送り届ける必要があり、「送付すべき相手に」、「正しい内容を」、「内容を覗き見されない方法で」送付しなければならない。すなわち、送信元の送信機器から送信先の受信機器までの間の通信経路において上記内容を担保する必要があり、送信元や送信先を偽装する「なりすまし」や送受信データに対する「盗聴」及び「改ざん」、通信経路への「侵入」及び「妨害」等の脅威から守らなければならない。	ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策を行うこと。 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を行うこと。 セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策を行うこと。 上記を満たす対策として、例えばIPsec とIKE を利用することによりセキュアな通信路を確保することが挙げられる。 チャネル・セキュリティの確保を閉域ネットワークの採用に期待してネットワークを構成する場合には、選択するサービスの閉域性の範囲を事業者に確認すること。	最低限	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。（Ⅲ．３．１．４【基本】） ・不正な通過パケットを自動的に発見、もしくは遮断する措置（ID/IPSの導入等）を講じること。（Ⅲ．３．１．５【推奨】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。（Ⅲ．３．２．１【基本】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。（Ⅲ．３．２．２【推奨】） ・第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。（Ⅲ．３．２．３【基本】） ・医療機関等がASP・SaaSを利用するネットワークにつき、ウイルスや不正なメッセージの混入等による改ざんに対する防止措置についての事業者の役割の範囲について医療機関等と合意すること。	cybozu.com における不正アクセス対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/illegal_access/index.html cybozu.com における不正ログイン対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/bad_login/index.html cybozu.com では、IP アドレス制限とクライアント証明書を用いた認証機能を用いることで、 セキュリティ対策を補完しております。詳細は以下のウェブページで公開しております。 https://www.cybozu.com/jp/service/option/	適合可能	文献[03]にてクライアント証明書によるセキュアアクセスが実施されていること、文献[04]にてなりすまし対策が実施されていることを確認した。また文献[18]にてIPアドレス制限によるIPアドレス許可への対策が実施されていることを確認した。 cybozu.com における不正ログイン対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/bad_login/index.html cybozu.com では、IP アドレス制限とクライアント証明書を用いた認証機能を用いることで、 セキュリティ対策を補完しております。詳細は以下のウェブページで公開しております。 https://www.cybozu.com/jp/service/option/	公開文書	文献[03]文献[04]文献[18]	–	–	–	所管官庁への連絡は利用者側で実施する必要がある。 ネットワーク構成図は利用者側にて作成する必要がある。 端末側で使用する暗号鍵は、第三者に解読されたり漏洩することを、利用者が対策を講じる必要がある。 利用者が使用する端末で独自に使用する暗号鍵の保護については、利用者が対策する必要がある。 リバースプロキシサーバ等の対策については必要に応じて利用者もしくはSI事業者にて構築する必要がある。
6.11-02					データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、採用する認証手段を決めること。認証手段としてはPKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等の容易に解読されない方法を用いるのが望ましい。	最低限	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。（Ⅲ．３．２．３【基本】） ・ASP・SaaSを利用するネットワークで用いられる医療機関等の送受信の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、医療機関等から事業者までの確認を行うこと（但し事業者が保守業務を再委託している場合には、事業者と再委託先との接続では本項の対応を適用せず、別途なりすましを防止する策を講じること）。 ・厚生労働省ガイドラインに基づいて医療機関等が採用する通信方式認証手段が妥当なものであることを確認することにつき、事業者の役割と範囲を、医療機関等と合意すること。	サービスを提供する各サーバーにはサーバー証明書を導入しております。 cybozu.com では、IP アドレス制限とクライアント証明書を用いた認証機能を用いることで、 セキュリティ対策を補完しております。詳細は以下のウェブページで公開しております。 https://www.cybozu.com/jp/service/option/	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者は、利用者自身のユーザーによるアクセスを制御し、そのアクセスを適切に確認する必要がある。
6.11-03					施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策を行うこと。これに関しては、「6.5技術的安全対策」で包括的に述べているので、それを参照すること。	最低限	表３-３参照のこと	cybozu.com における不正アクセス対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/illegal_access/index.html cybozu.com における不正ログイン対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/bad_login/index.html cybozu.com では、IP アドレス制限とクライアント証明書を用いた認証機能を用いることで、 セキュリティ対策を補完しております。詳細は以下のウェブページで公開しております。 https://www.cybozu.com/jp/service/option/	適合可能	文献[03]にてなりすまし対策が実施されていることを確認した。またIPアドレス制限やクライアント証明書によるセキュアアクセスにより許可機器へのなりすましを防ぐ対策が実施されていることを確認した。	公開文書	文献[03]	–	–	–	利用者及びSI事業者は、施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策を行う必要がある。
6.11-04					ルータ等のネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶVPN の間で送受信ができないように経路設定されていること。安全性が確認できる機器とは、例えば、ISO15408 で規定されるセキュリティーゲートもしくはそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。	最低限	・不正な通過パケットを自動的に発見、もしくは遮断する措置（IDS/IPSの導入等）を講じること。（Ⅲ．３．１．５【推奨】） ・ASP・SaaSを利用するネットワークで用いられるルータ等のネットワーク機器が厚生労働省ガイドラインで求める安全性が確認されているものであること、ASP・SaaSを利用するネットワークで用いられる医療機関等の施設内のルータについて、これを経由して医療機関等の施設間を結ぶVPNの間で送受信ができないように経路設定されていること等に関して、事業者の役割、範囲を医療機関等と合意すること。	ネットワーク機器は安全性が確認できる機器を利用しております。 以下のウェブページも併せてご参照ください。 障害検知・復旧対策 https://www.cybozu.com/jp/security/fault_detection/index.html	適合可能	文献[08]にてDoS, DDoS対策が記載されていることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[08]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、ルータ等のネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶVPN の間で送受信ができないように経路設定されていること。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.11-05					送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。たとえば、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。	最低限	・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。（Ⅲ．３．２．２【推奨】） ・ASP・SaaSにおいて送受信されるデータに対して、電子政府推奨の暗号を用いた暗号化等によるセキュリティ対策を講じること。 ・暗号化によるセキュリティ対策が、医療機関等が求める水準を満たすものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	cybozu.com における不正アクセス対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/illegal_access/index.html cybozu.com における不正ログイン対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/bad_login/index.html cybozu.com では、IP アドレス制限とクライアント証明書を用いた認証機能を用いることで、 セキュリティ対策を補完しております。詳細は以下のウェブページで公開しております。 https://www.cybozu.com/jp/service/option/	適合可能	文献[03]にてなりすまし対策が実施されていること、またクライアント証明書を利用したセキュアアクセスに関する記載を確認した。	公開文書	文献[03]	–	–	–	–
6.11-06					医療機関等の間の情報通信には、医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等多くの組織が関連する。 そのため、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。 ・診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に関わる操作を開始する動作の決定 ・送信元の医療機関等がネットワークに接続できない場合の対処 ・送信先の医療機関等がネットワークに接続できなかった場合の対処 ・ネットワークの経路途中が不通または著しい遅延の場合の対処 ・送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処 ・伝送情報の暗号化に不具合があった場合の対処 ・送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処 ・障害が起こった場合に障害部位を切り分ける責任 ・送信元の医療機関等または送信先の医療機関等が情報交換を中止する場合の対処 また、医療機関内においても次の事項において契約や運用管理規程等で定めておくこと。 ・通信機器、暗号化装置、認証装置等の管理責任の明確化。外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結。 ・患者等に対する説明責任の明確化。 ・事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置。 ・交換した医療情報等に対する管理責任及び事後責任の明確化。 個人情報の取扱いに関して患者から同意等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項。	最低限	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３【基本】） ・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１【基本】） ・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２【基本】） ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。（Ⅲ．３．２．４【基本】） ・通常運用時、緊急時の医療機関等と事業者との起点から終点までの通信手順を明確にし、事業者の負う責任の範囲、役割等について、医療機関等と合意すること。 ・医療機関等の管理者において発生する患者等に対する説明責任、管理責任等、各種責任に関し、事業者が負う責任の範囲、役割等について、医療機関等と合意すること。	cybozu.com サービスにおけるサイボウズの責任については、利用規約の定めるところに依ります。 https://www.cybozu.com/jp/terms/ cybozu.com サービスの運用に関する具体的な実施基準や手順は、内規に定め文書化しております。	適合可能	文献[10]において、保証範囲や責任の制限等についてCybozu社の見解が明示されていることを確認した。	公開文書	文献[10]	–	–	–	利用者は、対象業務の重要度、要求事項と提供されるサービスレベルを照らし合わせ、利用可否を決定する必要がある。 利用者は、cybozu.com の契約書および使用条件を確認し、cybozu.com の責任が及ばない範囲については、自ら対策を施す必要がある。
6.11-07					リモートメンテナンスを実施する場合は、必要に応じて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こと。 また、メンテナンス自体は「6.8 情報システムの改造と保守」を参照すること。	最低限	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。 （Ⅲ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。（Ⅲ．３．１．４【基本】）	運用担当者には各個人に一意の識別子を付与し、アクセスが許可されていない者が運用環境にログインおよび、アクセスできないように制御しております。 またネットワーク図を作成し、サービスを提供するネットワークを適切に分離し、管理責任の範囲を明確にしております。 cybozu.com の不正ログイン対策は、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/bad_login/index.html 以下の資料も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	アクセス制御方針に関しては文献[01]にて、各個人に一意の識別子を付与しており、またシステムにアクセスする際にはVPN網を利用し、さらにアクセスが許可されていない者がアクセス、ログオンできないように制御していることが明記されている。 文献[05]にて運用環境が分離され、データセンターへの接続は専用端末のみからしか行えないことが明記されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]文献[05]	–	詳細はサイボウズ社とのNDAにより開示。	–	ネットワーク構成図は利用者側にて作成する必要がある。
6.11-08					回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。 また上記1 及び4 を満たしていることを確認すること。	最低限	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１【基本】） ・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。（Ⅲ．２．１．４【推奨】） ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。（Ⅲ．３．２．４【基本】） ・サービスを提供する際に用いる回線の管理責任、品質等に対する事業者の責任の範囲、役割等について、医療機関等と合意すること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者は、対象業務の重要度、要求事項と提供されるサービスレベルを照らし合わせ、利用可否を決定する必要がある。
6.11-09					患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信のTLS暗号化、PKI 個人認証等の技術を用いた対策を実施すること。 また、情報の主体者となる患者等へ危険性や提供目的についての納得できる説明を行い、IT に係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にすること。	最低限	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。（Ⅲ．３．１．４【基本】） ・患者が情報を閲覧する情報システムの安全性に関する説明責任等において、事業者は責任の範囲、役割等について、医療機関等と合意すること。	cybozu.com における不正アクセス対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/illegal_access/index.html cybozu.com における不正ログイン対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/bad_login/index.html アクセス制御については、以下の資料も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	アクセス制御方針に関しては、文献[01]にて各個人に一意の識別子を付与しており、またシステムにアクセスする際にはVPN網を利用し、さらにアクセスが許可されていない者がアクセス、ログオンできないように制御していることが明記されている。 また文献[01]ではパスワードが情報セキュリティ規則、情報システム運用マニュアルに則り管理されていることが明記されている。 文献[04]で不正ログイン対策（なりすまし対策）が明記されており、またパスワード有効期限が設定可能であることが明記されている。 文献[03]にて不正アクセス防止に関して明記されている。	公開文書	文献[01]文献[03]文献[04]	–	–	–	利用者及びSI事業者は、医療情報システムへのアクセスを患者に提供する際には、適切に対応する必要がある。
6.11-10					オープンなネットワークを介して HTTPS を利用した接続を行う際、IPsec を用いた VPN 接続等によるセキュリティの担保を行っている場合を除いては、SSL/TLS のプロトコルバージョンを TLS1.2 のみに限定した上で、クライアント証明書を利用した TLS クライアント認証を実施すること。その際、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行うこと。いわゆる SSL-VPN は偽サーバへの対策が不十分なものが多いため、原則として使用しないこと。また、ソフトウェア型の IPsec 若しくは TLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃からの防護について、適切な対策を実施すること。	最低限	–	cybozu.com は NTTコミュニケーションズ様が提供する「Arcstar Universal One Multi-Cloud Connect」に対応しています。こちらを利用することで、VPN 接続によって通信経路を保護できます。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、すべてVPNを使用して頂く必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応						SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.11-11					やむを得ず、従業者による外部からのアクセスを許可する場合は、PC の作業環境内に仮想的に安全管理された環境をVPN 技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに運用等の要件を設定すること。	推奨	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法，特定の場所及び装置からの接続を認証する方法等により，アクセス制御しなければ対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。（Ⅲ．３．２．４【基本】） ・医療機関等の利用者が、医療機関の外部からASP・SaaSを利用する場合に、事業者は、医療機関の利用者が用いるPCの作業環境内に仮想的に安全管理された環境をVPN技術と組み合わせて実現する仮想デスクトップ等の技術導入に関する事業者の役割、範囲等を医療機関等と合意すること。	外部から作業する場合には、EDR などのクライアントにおけるセキュリティ対策を用いて保護された端末から、IPVPN 経由でオペレーション専用端末にアクセスし作業いたしております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、やむを得ず従業者による外部からのアクセスを許可する場合は、PC の作業環境内に仮想的に安全管理された環境をVPN 技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに運用等の要件を設定する必要がある。
6.12-01		6.12	「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。 一 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。 二 当該情報について改変が行われていないかどうかを確認することができるものであること。 （電子署名及び認証業務に関する法律（平成12 年法律第102 号）第2 条1 項）	平成11 年4 月の「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関する通知」においては、法令で署名または記名・押印が義務付けられた文書等は、「電子署名及び認証業務に関する法律」（以下「電子署名法」という。）が未整備の状態であったために対象外とされていた。 しかし、平成12 年5 月に電子署名法が成立し、また、e-文書法の対象範囲となる医療関係文書等として、e-文書法省令において指定された文書等においては、「A．制度上の要求事項」に示した電子署名によって、記名・押印にかわり電子署名を施すことで、作成・保存が可能となった。 ただし、医療に係る文書等では一定期間、署名を信頼性を持って検証できることが必要である。電子署名は紙媒体への署名や記名・押印と異なり、「A．制度上の要求事項」の一、二は厳密に検証することが可能である反面、電子証明書等の有効期限が過ぎたり失効させた場合は検証ができないという特徴がある。さらに、電子署名の技術的な基礎となっている暗号技術は、解読法やコンピュータの演算速度の進歩につれて次第に脆弱化が進み、中長期的にはより強固な暗号アルゴリズムへ移行することも求められる。例えば現在、電子署名に一般的に用いられている暗号方式のRSA 1024bitや、ハッシュ関数のSHA1は、政府機関の情報システムからの移行スジュールが決まっており、2008年4月の情報セキュリティ政策会議が決定した「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA1及びRSA1024に関する移行指針」によれば、2014年度以降，RSA 2048bitやSHA2等へ移行される予定となっている。 従って、電子署名を付与する際はこのような点を考慮し、電子証明書の有効期間や失効、また暗号アルゴリズムの脆弱化の有無によらず、法定保存期間等の一定の期間、電子署名の検証が継続できる必要がある。また、対象文書は行政の監視等の対象であり、施した電子署名が行政機関等によっても検証できる必要がある。近年、デジタルタイムスタンプ技術を利用した長期署名方式の標準化が進み、長期的な署名検証の継続が可能となり、JIS規格としても制定された（JIS X 5092:2008 CMS利用電子署名(CAdES)の長期署名プロファイル、JIS X 5093:2008 XML署名利用電子署名(XAdES)の長期署名プロファイル）。 長期署名方式では、下記により、署名検証の継続を可能としている。 （1） 署名に付与するタイムスタンプにより署名時刻を担保する（署名に付与したタイムスタンプ時刻以前にその署名が存在していたことを証明すること）。 （2） 署名当時の検証情報（関連する証明書や失効情報等）を保管する。 （3） 署名対象データ、署名値、検証情報の全体にタイムスタンプを付し、より強固な暗号アルゴリズムで全体を保護する。	（1） 厚生労働省の定める準拠性監査基準を満たす健医療福祉分野PKI 認証局若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こと 1． 保健医療福祉分野PKI 認証局は、電子証明書内に医師等の保健医療福祉に係る資格を格納しており、その資格を証明する認証基盤として構築されている。従ってこの保健医療福祉分野PKI 認証局の発行する電子署名を活用することが推奨される。 ただし、当該電子署名を検証しなければならない者の全てが、国家資格を含めた電子署名の検証が正しくできることが必要である。	最低限	・法令で定められた記名・押印を電子署名で行うものとされた情報に対する電子署名の方式等について、医療機関等と合意すること。 ・合意した電子署名の方式等が、保健医療福祉分野PKI認証局の発行する電子証明書、もしくは電子署名法の規定に基づく**認定特定認証事業者の発行する電子証明書**によるものであることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	利用者様にて適切に実施いただく必要があります。	対象外	–	医療機関に対する要求事項のため、対象外。	–	–	–	–	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-02					2． 電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いなくてもＡの要件を満たすことは可能であるが、同等の厳密さで本人権限を行い、さらに、監視等を行う行政機関等が電子署名を検証可能である必要がある。	最低限	同上	利用者様にて適切に実施いただく必要があります。	対象外	–	医療機関に対する要求事項のため、対象外。	–	–	–	–	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-03					3．「電子署名に係る地方公共団体の認証業務に関する法律」（平成14 年法律第153号）に基づき、平成16 年1 月29 日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、行政機関以外に当該電子署名を検証しなければならない者がすべて公的個人認証サービスを用いた電子署名を検証できることが必要である。	最低限	同上	利用者様にて適切に実施いただく必要があります。	対象外	–	医療機関に対する要求事項のため、対象外。	–	–	–	–	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-04					（2） 電子署名を含む文書全体にタイムスタンプを付与すること。 1． タイムスタンプは、「タイムビジネスに係る指針 －ネットワークの安心な利用と電子データの安全な長期保存のために－」（総務省、平成16 年11 月）等で示されている時刻認証業務の基準に準拠し、財団法人日本データ通信協会が認定した時刻認証事業者のものを使用し、第三者がタイムスタンプを検証することが可能であること。	最低限	・法令で定められた記名・押印を電子署名で行うものとされた情報に対する電子署名の方式等について、医療機関等と合意すること。 ・合意した電子署名の方式等が、保健医療福祉分野PKI認証局の発行する電子署名もしくはこれと同等の仕様を含むものであることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	利用者様にて適切に実施いただく必要があります。	対象外	–	医療機関に対する要求事項のため、対象外。	–	–	–	–	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-05					2． 法定保存期間中のタイムスタンプの有効性を継続できるよう、対策を講じること。	最低限	同上	利用者様にて適切に実施いただく必要があります。	対象外	–	医療機関に対する要求事項のため、対象外。	–	–	–	–	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-06					3． タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を講じる必要がある。	最低限	同上	利用者様にて適切に実施いただく必要があります。	対象外	–	医療機関に対する要求事項のため、対象外。	–	–	–	–	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-07					（3） 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こと。 1． 当然ではあるが、有効な電子証明書を用いて電子署名を行わなければならない。 本来法的な保存期間は電子署名自体が検証可能であることが求められるが、タイムスタンプが検証可能であれば、電子署名を含めて改変の事実がないことが証明されるために、タイムスタンプ付与時点で、電子署名が検証可能であれば、電子署名付与時点での有効性を検証することが可能である。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が必要である。	最低限	・法令で定められた記名・押印を電子署名で行うものとされた情報に対する電子署名の方式等について、医療機関等と合意すること。 ・合意した電子署名の方式等が、保健医療福祉分野PKI認証局の発行する電子署名もしくはこれと同等の仕様を含むものであることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	利用者様にて適切に実施いただく必要があります。	対象外	–	医療機関に対する要求事項のため、対象外。	–	–	–	–	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
7.1-01	7	7.1	電磁的記録に記録された事項について、保存すべき期間中における当該事項の改変又は消去の事実の有無及びその内容を確認することができる措置を講じ、かつ、当該電磁的記録の作成に係る責任の所在を明らかにしていること。 （e-文書法省令第4 条第4 項第2 号） ② 真正性の確保 電磁的記録に記録された事項について、保存すべき期間中における当該事項の改変又は消去の事実の有無及びその内容を確認することができる措置を講じ、かつ、当該電磁的記録の作成に係る責任の所在を明らかにしていること。 (ア) 故意または過失による虚偽入力、書換え、消去及び混同を防止すること。 (イ) 作成の責任の所在を明確にすること。 （施行通知第2 2（3）②） 「診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。」 （外部保存改正通知第2 1（1））	真正性とは、正当な権限において作成された記録に対し、虚偽入力、書き換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であることである。なお、混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性を誤ったりすることをいう。 また、ネットワークを通じて外部に保存を行う場合、委託元の医療機関から委託先の外部保存施設への転送途中で、診療録等が書き換えや消去されないように、また他の情報との混同が発生しないよう、注意する必要がある。 従って、ネットワークを通じて医療機関の外部に保存する場合は、医療機関等に保存する場合の真正性の確保に加えて、ネットワーク特有のリスクにも留意しなくてはならない。	【医療機関等に保存する場合】 （1） 入力者及び確定者の識別及び認証 a. 電子カルテシステム等でPC 等の汎用入力端末により記録が作成される場合 1． 入力者及び確定者を正しく識別し、認証を行うこと。	最低限	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】）	cybozu.com における不正アクセス対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/illegal_access/index.html cybozu.com における不正ログイン対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/bad_login/index.html 運用担当者の各個人に一意の識別子を付与しており、またシステムにアクセスする際にはVPN網を利用し、さらにアクセスが許可されていない者がアクセス、ログオンできないように制御していることが明記されている。 また文献[04]で不正ログイン対策（なりすまし対策）が明記されており、入力者及び確定者を正しく識別し、認証を行うことが出来ることを確認した。 アクセス制御については、以下の資料も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf 利用者のアカウントを管理する方法は、以下のウェブページで公開しております。 https://jp.cybozu.help/ja/general/admin/list_useradmin.html	適合可能	文献[01]にて、各個人に一意の識別子を付与しており、またシステムにアクセスする際にはVPN網を利用し、さらにアクセスが許可されていない者がアクセス、ログオンできないように制御していることが明記されている。 また文献[04]で不正ログイン対策（なりすまし対策）が明記されており、入力者及び確定者を正しく識別し、認証を行うことが出来ることを確認した。	公開文書	文献[01]文献[04]	–	–	–	利用者及びSI事業者は、電子カルテシステム等でPC 等の汎用入力端末により記録が作成される場合入力者及び確定者を正しく識別し、認証を行う必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
7.1-02					2.　システムへの全ての入力操作について、対象情報ごとに入力者の職種や所属等の必要な区分に基づいた権限管理（アクセスコントロール）を定めること。また、権限のある入力者以外による作成、追記、変更を防止すること。	最低限	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・提供する電子カルテシステム等に関するサービスにおいて、医療機関等の職務権限等に応じたアクセス制御が可能であることを含め、仕様内容について、医療機関等と合意すること。	cybozu.com における不正アクセス対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/illegal_access/index.html cybozu.com における不正ログイン対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/bad_login/index.html システムへのアクセス権限の追加・削除・変更方法は文書化しております。 特権については、利用者を cybozu.com の運用担当者のみに制限しております。 アクセス制御については、以下の資料も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[20]、文献[21]、文献[22]、文献[23]にて、適切にアクセス管理が出来るような仕組みが提供されていることを確認した。	公開文書	文献[20]文献[21]文献[22]文献[23]	–	–	–	利用者及びSI事業者は、権限のある入力者以外による作成、追記、変更を防止する必要がある。
7.1-03					3.　業務アプリケーションが稼動可能な端末を管理し、権限を持たない者からのアクセスを防止すること。	最低限	・同上	cybozu.com では、IP アドレス制限とクライアント証明書を用いた認証機能を用いることで、 社外からアクセスする端末可能な端末を制限する機能を提供しております。詳細は以下のウェブページで公開しております。 https://www.cybozu.com/jp/service/option/	適合可能	文献[18]にて、社外からはユーザーごとに発行・管理されているクライアント証明書をインポートしたモバイル端末のみアクセス可能であることが明記されている。	公開文書	文献[18]	–	–	–	利用者及びSI事業者は、業務アプリケーションが稼動可能な端末を管理し、権限を持たない者からのアクセスを防止する必要がある。
7.1-04					b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合 1.　装置の管理責任者や操作者が運用管理規程で明確にされ、装置の管理責任者、操作者以外による機器の操作が運用上防止されていること。	最低限	・臨床検査システム、医用画像ファイリングシステム等との連携におけるインターフェースの構築に関し、事業者の役割、範囲について医療機関等と合意すること。	cybozu.com の各製品を操作するための API については、以下のウェブページで公開いたしております。 https://developer.cybozu.io/hc/ja API を利用する際に出力されるログ情報については、各製品のマニュアルをご参照ください。 https://manual.cybozu.co.jp/ API を用いてサービスを操作する端末の管理はお客様にて実施いただく必要があります。	対象外	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、医用画像ファイリングシステム等の装置を適切に管理する必要がある。
7.1-05					2.　当該装置による記録は、いつ・誰が行ったかがシステム機能と運用の組み合わせにより明確になっていること。	最低限	・同上		対象外	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、医用画像ファイリングシステム等の装置からの入力を適切に記録する必要がある。
7.1-06					（2）　記録の確定手順の確立と、作成責任者の識別情報の記録 a. 電子カルテシステム等でPC 等の汎用入力端末により記録が作成される場合 1.　診療録等の作成・保存を行おうとする場合、システムは確定された情報を登録できる仕組みを備えること。その際、作成責任者の氏名等の識別情報、信頼できる時刻源を用いた作成日時が含まれること。	最低限	・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。（Ⅲ．１．１．５【基本】） ・電子データの原本性確保を行うこと。（Ⅲ．５．１．１【推奨】）	NTP を利用して OS、ネットワーク機器等、正確な時刻源と時刻同期を実施しています。 以下のドキュメントについてもご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、NTPを利用した時刻同期が実施されていることを確認した。	公開文書	文献[01]	–	–	–	電子データの原本性確保は利用者側で実施する必要がある。 利用者及びSI事業者は、医療情報システムにおける時刻同期を適切に行う必要がある。
7.1-07					2.　「記録の確定」を行うにあたり、作成責任者による内容の十分な確認が実施できるようにすること。	最低限	・入力された内容が記録の確定前に作成責任者によって確認できる仕様とすることを、医療機関等と合意すること。	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	利用者及びSI事業者は、医療情報システムにおける電磁的記録の確定において、作成責任者による確認が可能な機能を構築する必要がある。
7.1-08					3.「記録の確定」は、確定を実施できる権限を持った確定者が実施すること。	最低限	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	利用者及びSI事業者は、記録の確定を、適切な権限を持った確定者が実施するよう業務の設計を行う必要がある。
7.1-09					4.　確定された記録が、故意による虚偽入力、書き換え、消去及び混同されることの防止対策を講じておくこと及び原状回復のための手順を検討しておくこと。	最低限	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３【基本】） ・連携ASP・SaaS 事業者が提供するASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．３．１．２【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】） ・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．２．３．１【基本】）	利用者の利用状況は、「監査ログ」機能にて確認できます。 詳細は以下のウェブページをご確認ください。 https://jp.cybozu.help/ja/general/admin/audit cybozu.com のデータ消失対策は、以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/data_loss/index.html	適合可能	文献[01]にて、利用者の利用状況（アクセスログ）が取得され、また記録（ログ等）の保存期間が無期限であることが明記されている。 また、文献[01]および文献[06]にて定期的なバックアップが実施されている旨が明記されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]文献[06]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は必要に応じて、データ回復のための手順を検討する必要がある。
7.1-10					5.　一定時間後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを策定し運用管理規程に明記すること。	最低限	–	ご利用者様にてバッチ処理などを作成いただく場合、利用者様にて適切な運用管理を実施いただく必要があります。 サービス内の一部として、一定時間後に記録が自動確定する機能がございます。 詳細は弊社マニュアルをご参照ください。 https://manual.cybozu.co.jp/	対象外	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者が入力処理がバッチ処理等により自動確定するような仕組みを実施する場合には、利用者側での適切な運用管理を実施する必要がある。
7.1-11					6.　確定者が何らかの理由で確定操作ができない場合、例えば医療機関等の管理責任者が記録の確定を実施する等のルールを運用管理規程で定め、記録の確定の責任の所在を明確にすること。	最低限	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	利用者は、確定者が何らかの理由で確定操作ができない場合、代替策の例やルールを運用管理規程で定め、記録の確定の責任の所在を明確にする必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
7.1-12					b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合 1. 運用管理規程等に当該装置により作成された記録の確定ルールが定義されていること。その際、当該装置の管理責任者や操作者の氏名等の識別情報（又は装置の識別情報）、信頼できる時刻源を用いた作成日時が記録に含まれること。	最低限	・臨床検査システム、医用画像ファイリングシステム等との連携におけるインターフェースの構築に関し、事業者の役割、範囲について医療機関等と合意すること。	cybozu.com の各製品を操作するための API については、以下のウェブページで公開いたしております。 https://developer.cybozu.io/hc/ja API を利用する際に出力されるログ情報については、各製品のマニュアルをご参照ください。 https://manual.cybozu.co.jp/ API を用いてサービスを操作する端末の管理はお客様にて実施いただく必要があります。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、臨床検査システム、医用画像ファイリングシステム等の装置の管理は利用者側で実施する必要がある。
7.1-13					2. 確定された記録が、故意による虚偽入力、書き換え、消去及び混同されることの防止対策を講じておくこと及び原状回復のための手順を検討しておくこと。	最低限	・同上	改ざんおよび原状回復のための機能として、変更履歴を提供いたしております。 https://jp.cybozu.help/ja/k/user/history ※ 製品機能（kintone）	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、故意による虚偽入力、書き換え、消去及び混同されることの防止対策を利用者にて実施する必要がある。
7.1-14					（3） 更新履歴の保存 1. 一旦確定した診療録等を更新した場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合せることができること。	最低限	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３【基本】） ・連携ASP・SaaS 事業者が提供するASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．３．１．２【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】） ・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．２．３．１【基本】） ・一旦確定した診療録等を更新した場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合せられる機能を含めること。 ・更新管理の仕様について、医療機関等と合意すること。	利用者の利用状況は、「監査ログ」機能にて確認できます。詳細は以下のウェブページをご確認ください。 https://jp.cybozu.help/ja/general/admin/audit また一部の製品内機能として、更新前と更新後の内容を照らし合わせる仕組みがございます。 詳細は以下のウェブページをご確認ください。 https://jp.cybozu.help/ja/k/user/history	適合可能	文献[01]にて、利用者の利用状況（アクセスログ）が取得されることより、更新履歴が保存されることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、故意による虚偽入力、書き換え、消去及び混同されることの防止対策を利用者にて実施する必要がある。
7.1-15					2. 同じ診療録等に対して更新が複数回行われた場合にも、更新の順序性が識別できるように参照できること。	最低限	・同上	利用者の利用状況は、「監査ログ」機能にて確認できます。詳細は以下のウェブページをご参照ください。 https://jp.cybozu.help/ja/general/admin/audit NTP を利用して OS、ネットワーク機器等、正確な時刻源と時刻同期を実施しています。 更新の順序を適切に識別することは可能です。 以下のドキュメントについてもご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、NTPを利用した時刻同期が実施されていることから、更新の順序は時刻で識別できると判断する。	公開文書	文献[01]	–	–	–	データの履歴バックアップを作成すること、その他のフォールト トレランスを提供するための追加の手順を実施する責任は利用者側にある。 更新履歴について、更新の順序性が識別できるように参照できる機能を備える必要がある。
7.1-16					（4） 代行入力の承認機能 1. 代行入力を実施する場合、具体的にどの業務等に適用するか、また誰が誰を代行してよいかを運用管理規程で定めること。	最低限	・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・代行操作を実施するIDや運用方法について、予め医療機関等の管理者と内容を合意すること。	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	代行操作に関するルールを運用管理規程で定めることは利用者側で行う必要がある。
7.1-17					2. 代行入力が行われた場合には、誰の代行が誰によっていつ行われたかの管理情報が、その代行入力の都度記録されること。	最低限	・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】）	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	代行操作に関する機能の整備は利用者側で行う必要がある。
7.1-18					3. 代行入力により記録された診療録等は、できるだけ速やかに確定者による「確定操作（承認）」が行われること。この際、内容の確認を行わずに確定操作を行ってはならない。	最低限	・代行操作された際の、データの確定に関する仕様について、医療機関等の管理者と内容を合意すること。	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	代行操作に関する機能の整備は利用者側で行う必要がある。
7.1-19					（5） 機器・ソフトウェアの品質管理 1. システムがどのような機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかが明らかにされており、システムの仕様が明確に定義されていること。	最低限	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１【基本】） ・機器、ソフトウェア構成について、医療機関等と合意をとること。 ・機器、ソフトウェア構成について文書化を行い、医療機関等の管理者に対して報告できる内容とすること。	cybozu.com におけるデータの取り扱い方法については、以下のウェブページで公開しております。 cybozu.com サービスご利用規約 https://www.cybozu.com/jp/terms/ プライバシーポリシー https://cybozu.co.jp/privacy/privacy-policy/ クラウドデータポリシー https://cybozu.co.jp/privacy/cloud-data-policy/ また不要・不法なアクセスを防止するために、内規にてアクセス制御に関する規則を定め、運用しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	医療機関との合意は契約など（利用規約？）で別途行う必要がある。
7.1-20					2. 機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスが規定されていること。	最低限	・提供するサービスにおけるシステムの導入プロセスについて、文書化を行うこと。 ・システムの構成管理内容を示す資料の開示内容・範囲・条件について、医療機関等と合意すること。	内規にて運用管理規定（変更管理および、構成管理）を定め、運用いたしております。 各種規定については、社内規程の変更の都度、全従業員に通知し、周知いたしております。 また、教育・研修を実施し、セキュリティ、コンプライアンス等に関する教育についても必要に応じて実施しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者は、医療情報システム全体の機器及びソフトウェアの構成を管理し、文書化する必要がある。
7.1-21					3. 機器、ソフトウェアの品質管理に関する作業内容を運用管理規程に盛り込み、従業者等への教育を実施すること。	最低限	・運用・操作に関する利用者教育における事業者の役割、範囲等について、医療機関等と合意すること。	以下のドキュメントについてもご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	従業者への教育は、文献[01]にて雇用する従業員に対して入社オリエンテーションの一環で、コンプライアンス研修を実施しており、社内規程の教育を行っている旨が記載されている。また、社内規程の変更の都度、全従業員に通知し、周知を行っており、さらに、教育・研修を実施し、セキュリティ、コンプライアンス等に関する教育についても必要に応じて実施している旨が記載されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、従業者の教育は利用者様の責任の下実施する必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
7.1-22					4． システム構成やソフトウェアの動作状況に関する内部監査を定期的に実施すること。	最低限	・システム構成やソフトウェアの動作状況に関する内部監査について、事業者の役割、範囲等について医療機関等と合意すること。	サイボウズは cybozu.com の運用に関して ISMS 認証を受けております。 認証登録番号：IS 577142 内規に基づき内部監査を実施し、ISMS 認証審査の過程で外部からの審査を受けております。 また cybozu.com 運用基盤上で動作するアプリケーションについては、年に 1 回脆弱性診断を受け、その結果を以下のウェブページで公開しております。 https://www.cybozu.com/jp/productsecurity/	適合可能	文献[25]に記載のあるCy-PSIRTにて、製品のセキュリティ品質の管理および向上を目的とした取り組みが実施されていることを確認した。 また、万が一製品に脆弱性が発見された場合には、文献[14]に則り、適切に管理されていることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[14]文献[25]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者は、医療情報システム全体の機器及びソフトウェアに関する内部監査を定期的に実施する必要がある。
7.1-23					【ネットワークを通して医療機関等の外部に保存する場合】 医療機関等に保存する場合の最低限のガイドラインに加え、次の事項が必要となる。 （1） 通信の相手先が正当であることを認識するための相互認証を行うこと診療録等のオンライン外部保存を受託する機関と委託する医療機関等が、お互いに通信目的とする正当な相手かどうかを認識するための相互認証機能が必要である。	最低限	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・第三者が当該事業者のサーバになりすまして（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。（Ⅲ．３．２．３【基本】）	cybozu.com における不正アクセス対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/illegal_access/index.html cybozu.com における不正ログイン対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/bad_login/index.html 運用担当者の各個人に一意の識別子を付与しており、またシステムにアクセスする際にはVPN網を利用し、さらにアクセスが許可されていない者がアクセス、ログオンできないように制御しています。 アクセス制御については、以下の資料も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、システムアカウントについては当社規定に則り、各個人に一意の識別子が付与されている旨が明記されている。またシステムにアクセスする際にはVPN網を利用し、さらにアクセスが許可されていない者がアクセス、ログオンできないように制御している旨が明記されている。 文献[03]で不正アクセス対策がされていること、また文献[04]で不正ログイン対策（なりすまし対策）がされていることが明記されている。	公開文書	文献[01]文献[03]文献[04]	–	–	–	利用者は、医療機関など利用者側の認証が必要な機器等について、適切に設定・管理を行う必要がある。
7.1-24					（2） ネットワーク上で「改ざん」されていないことを保証すること ネットワークの転送途中で診療録等が改ざんされていないことを保証できること。 なお、可逆的な情報の圧縮・解凍並びにセキュリティ確保のためのタグ付けや暗号化・平文化等は改ざんにはあたらない。	最低限	・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。（Ⅲ．３．２．１【基本】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。（Ⅲ．３．２．２【推奨】）	cybozu.com システムの運用管理担当者がシステムにアクセスする際には暗号化されているVPN網を利用しております。 利用者様クライアント環境から cybozu.com への転送経路は、SSL にて暗号化しております。 暗号形式は Qualys SSL Labs スコアで高ランクを維持するよう、日々方式を見直しております。 以下の資料も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf https://www.cybozu.com/jp/security/disaster_control/index.html	適合可能	文献[01]にて、cybozu.com システムの運用管理担当者がシステムにアクセスする際には暗号化されているVPN網を利用する旨が明記されている。 また文献[03]にて、クライアント証明書を利用したセキュアアクセスの機能を提供していることを確認した。	公開文書	文献[01]文献[03]	–	–	–	利用者は、医療機関などの利用者側のネットワーク上での改ざん対策を行う必要がある。
7.1-25					（3） リモートログイン機能を制限すること 保守目的等のどうしても必要な場合を除き行うことができないように、適切に管理されたリモートログインのみに制限する機能を設けなければならない。なお、これらの具体的要件については、「6.11 外部と診療情報等を含む医療情報を交換する場合の安全管理」を参照すること。	最低限	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法の環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・ASP・SaaS提供に必要なシステムの保守をリモートメンテナンスで行う場合の、医療機関等への報告対象とするシステムの範囲、そのシステムに対するリモートメンテナンスの実施条件、報告内容等について、医療機関等と合意すること。	cybozu.com システムの運用管理担当者がシステムにアクセスする際には暗号化されているVPN網を利用しております。 ネットワーク管理者の権限は cybozu.com システム運用担当者の身に制限されており、許可されていない者がアクセス・ログオンできないように制御されております。 以下の資料も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、ネットワーク管理者の権限については、cybozu.com システムの運用管理担当者のみとされており、アクセスする際にはVPN網を利用し、またアクセスが許可されていない者がアクセス、ログオンできないように制御されている旨が記載されている。	公開文書	文献[01]	–	–	–	利用者は、医療情報システム全体の機器及びソフトウェアに対するリモートアクセスについて、その要否を含めて適切に管理する必要がある。
7.2-01		7.2	必要に応じ電磁的記録に記録された事項を出力することにより、直ちに明瞭かつ整然とした形式で使用に係る電子計算機その他の機器に表示し、及び書面を作成できるようにすること。 （e-文書法省令第4 条第4 項第1 号）	電子媒体に保存された内容を、権限保有者からの「診療」、「患者への説明」、「監査」、「訴訟」等の要求に応じて、それぞれの目的に対し支障のない応答時間やスループットと操作方法で、肉眼で見読可能な状態にできることである。e-文書法の精神によれば、画面上での見読性が確保されていることが求められているが、権限保有者の要求によっては対象の情報の内容を直ちに画面に表示できることが求められることもあるため、必要に応じてこれに対応することを考慮する必要がある。	（1） 情報の所在管理 紙管理された情報を含め、各種媒体に分散管理された情報であっても、患者毎の情報の全ての所在が日常的に管理されていること。	最低限	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１【基本】）	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	利用者及びSI事業者は、外部電子媒体への書き出し、それを参照するデバイスなどを整えて頂く必要がある。
7.2-02			① 見読性の確保 必要に応じ電磁的記録に記録された事項を出力することにより、直ちに明瞭かつ整然とした形式で使用に係る電子計算機その他の機器に表示し、及び書面を作成できるようにすること。 (ア) 情報の内容を必要に応じて肉眼で見読可能な状態に容易にできること。 (イ) 情報の内容を必要に応じて直ちに書面に表示できること。 （施行通知第2 2 （3） ①）	電子媒体に保存された情報は、紙に記録された情報と違い、以下の理由によりそのままでは見読できない場合がある。 ・電子媒体に格納された情報を見読可能なように画面に呼び出すために何らかのアプリケーションが必要であること ・記録が、他のデータベースやマスター等を参照する形で作成されることが多く、データの作成時点で採用したマスター等に依存しなければ、正しい記録として見読できないこと ・複数媒体に分かれて記録された情報の相互関係が、そのままでは一瞬して判りにくいこと これらに適切に対応することにより、紙の記録と同等と言える見読性を確保しなければならない。 また、何らかのシステム障害が発生した場合においても診療に重大な支障が無い最低限の見読性を確保するための対策も考慮に含める必要がある。 ネットワークを通じて外部に保存する場合は、これらのことに適切に対応することに加えて、外部保存先の機関の事情により見読性が損なわれることを考慮に含めた十分な配慮が求められる。その際には、「4.2 責任分界点について」を参考にしつつ、予め責任を明確化しておき、速やかなる復旧が図られるように配慮しておく必要もある。 これらのことに配慮していても万が一、保存していた情報が き損した場合等は、可能な限り速やかな復旧に努め、「診療」、「患者への説明」、「監査」、「訴訟」等の要求に応える見読性の確保を図らなければならない。	（2） 見読化手段の管理 電子媒体に保存された全ての情報とそれらの見読化手段は対応づけて管理されていること。また、見読手段である機器、ソフトウェア、関連情報等は常に整備されていること。	最低限	・見読性を保証するサービス仕様について、医療機関等と合意すること。	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	電子媒体に関する見読化手段の管理は利用者側で対応する必要がある。
7.2-03			「診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。」 （外部保存改正通知第2 1 （1） ）		（3） 見読目的に応じた応答時間 目的に応じて速やかに検索表示もしくは書面に表示できること。	最低限	・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を行うこと。稼働停止を検知した場合は、利用者に速報を通知すること。（Ⅲ．１．１．１【基本】） ・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を行うこと。また、利用者との取決めに基づいて、監視結果を利用者に通知すること。（Ⅲ．１．１．３【推奨】） ・ASP・SaaS サービスを利用者に提供する時間帯を定め、この時間帯におけるASP・SaaSサービスの稼働率を規定すること。また、アプリケーション、プラットフォーム、サーバ・ストレージの定期保守時間を規定すること。（Ⅲ．２．１．１【基本】） ・見読性を保証するサービス仕様について、医療機関等と合意すること。	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	検索表示に関するアプリケーションの機能は利用者側で確保する必要がある。
7.2-04					（4） システム障害対策としての冗長性の確保 システムの一系統に障害が発生した場合でも、通常の診療等に差し支えない範囲で診療録等を見読可能とするために、システムの冗長化（障害の発生時にもシステム全体の機能を維持するため、平常時からサーバやネットワーク機器等の予備設備を準備し、運用すること）を行う又は代替的な見読化手段を用意すること。	最低限	・障害等が生じた場合等を想定し、冗長性を確保する仕様等について医療機関等と合意すること。	cybozu.com におけるデータ消失対策は以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/data_loss/index.html cybozu.com の災害対策は以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/disaster_control/index.html cybozu.com の障害検知・復旧対策は以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/fault_detection/index.html	適合可能	文献[08]にて、各種サービスのプログラムやWebサーバーが稼働している仮想サーバーの障害に備えて、「自律分散エージェントシステム」を構築している旨が明記されている。 文献[06]にてデータを管理するストレージサーバーがRAID 6の冗長化手法を採用している旨が明記されている。 文献[07]にて、電源や回線、ネットワークが冗長化されている旨が明記されている。	公開文書	文献[06]文献[07]文献[08]	–	–	–	利用者は、利用者側のネットワークや端末などの冗長性を確保する必要がある。
7.2-05					【医療機関等に保存する場合】 （1） バックアップサーバ システムが停止した場合でも、バックアップサーバと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。	推奨	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．２．３．１【基本】） ・事業者は、障害等が生じた場合の稼動に関するサービスの品質について医療機関等の管理者と合意する。	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	利用者及びSI事業者は、日常診療に必要な最低限の診療録等を見読することができるよう準備が必要である。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
7.2-06					（2） 見読性確保のための外部出力 システムが停止した場合でも、見読目的に該当する患者の一連の診療録等を汎用のブラウザ等で見読ができるように、見読性を確保した形式で外部ファイルへ出力することができること。	推奨	・事業者は、障害等が生じた場合の稼動に関するサービスの品質について医療機関等の管理者と合意する。	製品内に含まれるお客様情報の出力形式については、各製品のマニュアルに記載されております。詳細は以下のウェブページをご参照ください。 https://manual.cybozu.co.jp/	適合可能	文献[20]、文献[21]、文献[22]、文献[23]にて、CSV形式, テキスト形式, ZIP形式等、汎用的なファイル形式にて入出力可能である記載が確認できた。	公開文書	文献[20]文献[21]文献[22]文献[23]	–	–	–	利用者及びSI事業者は、出力した外部ファイルを利用して見読目的に該当する患者の一連の診療録等を汎用のブラウザ等で見読ができるようにしておく必要がある。
7.2-07					（3） 遠隔地のデータバックアップを使用した見読機能 大規模火災等の災害対策として、遠隔地に電子保存記録をバックアップし、そのバックアップデータと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。	推奨	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．２．３．１【基本】） ・事業者は、障害等が生じた場合の稼動に関するサービスの品質について医療機関等の管理者と合意する。	利用者様にて適切に実施いただく必要があります。	対象外		–	–	–	–	–	利用者及びSI事業者は、遠隔地に電子保存記録をバックアップし、そのバックアップデータと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができるようにしておく必要がある。
7.2-08					【ネットワークを通じて外部に保存する場合】 医療機関等に保存する場合の推奨されるガイドラインに加え、次の事項が必要となる。 （1） 緊急に必要になることが予測される診療録等の見読性の確保 緊急に必要になることが予測される診療録等は、内部に保存するか、外部に保存しても複製又は同等の内容を医療機関等の内部に保持すること。	推奨	・緊急時の医療機関等における診療録等の見読性の確保を支援する機能(例えば画面の印刷機能、ファイルダウンロードの機能等)をASP・SaaSにおいて含めることについて、医療機関等の管理者と協議し、合意すること。	利用者様にて適切に実施いただく必要があります。	対象外		–	–	–	–	–	利用者及びSI事業者は、緊急に必要になることが予測される診療録等が想定される場合、利用者にてファイルを保存しておく必要がある。
7.2-09					（2） 緊急に必要になるまではいえない診療録等の見読性の確保 緊急に必要になるまではいえない情報についても、ネットワークや外部保存を受託する機関の障害等に対応できるような措置を行っておくこと。	推奨	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．２．３．１【基本】） ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラック変動が重要）及び管理上の要求事項を特定すること。（Ⅲ．３．２．４【基本】） ・障害等が生じた場合の責任分界を明確にし、稼動を保証するサービスの品質について医療機関等と合意すること。	利用者様にて適切に実施いただく必要があります。	対象外		–	–	–	–	–	利用者及びSI事業者は、緊急に必要になることが予測される診療録等が想定される場合、利用者にてファイルを保存しておく必要がある。
7.3-01		7.3	電磁的記録に記録された事項について、保存すべき期間中において復元可能な状態で保存することができる措置を講じていること。 （e-文書法省令第4 条第4 項第3 号） ③ 保存性の確保 電磁的記録に記録された事項について、保存すべき期間中において復元可能な状態で保存することができる措置を講じていること。 （施行通知第2 2（3）③） 「診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。」 （外部保存改正通知第2 1（1））	保存性とは、記録された情報が法令等で定められた期間に渡って真正性を保ち、見読可能にできる状態で保存されることをいう。 診療録等の情報を電子的に保存する場合に、保存性を脅かす原因として、下記のものが考えられる。 （1） ウイルスや不適切なソフトウェア等による情報の破壊及び混同等 （2） 不適切な保管・取扱いによる情報の滅失、破壊 （3） 記録媒体、設備の劣化による読み取り不能または不完全な読み取り （4） 媒体・機器・ソフトウェアの整合性不備による復元不能 （5） 障害等によるデータ保存時の不整合 これらの脅威をなくすために、それぞれの原因に対する技術面及び運用面での各種対策を施す必要がある。	【医療機関等に保存する場合】 （1） ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止 1. いわゆるコンピュータウイルスを含む不適切なソフトウェアによる情報の破壊・混同が起こらないように、システムで利用するソフトウェア、機器及び媒体の管理を行うこと。	最低限	・ASP・SaaS サービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。（Ⅲ．２．２．１【基本】）	内規にてクライアント PC に関する遵守事項（ウイルス対策など）を定め、運用いたしております。運用環境のサーバには HIDS を導入し、不正なプログラムが動作しないように制御いたしております。 以下の資料も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止をと必要がある。
7.3-02					（2） 不適切な保管・取扱いによる情報の滅失、破壊の防止 1. 記録媒体及び記録機器の保管及び取扱いについては運用管理規程を作成し、適切な保管及び取扱いを行うように関係者に教育を行い、周知徹底すること。また、保管及び取扱いに関する作業履歴を残すこと。	最低限	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．２．１．３【基本】） ・全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。（Ⅱ．５．２．１【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】）	内規にて運用管理規定（記録媒体および、記録機器の保管・取り扱い）を定め、運用いたしております。 各種規定については、社内規程の変更の都度、全従業員に通知し、周知いたしております。 また、教育・研修を実施し、セキュリティ、コンプライアンス等に関する教育についても必要に応じて実施しております。 以下のドキュメントについてもご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[15]にて従業員に対する啓発活動を行なう旨が記載されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[15]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、記録媒体及び記録機器の保管及び取扱いについては運用管理規程を作成し、適切な保管及び取扱いを行うように関係者に教育を行い、周知徹底する必要がある。また、保管及び取扱いに関する作業履歴を残す必要がある。
7.3-03					2. システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能用量（サイズ、期間）、リスク、レスポンス、バックアップ頻度、バックアップ方法等を明示すること。これらを運用管理規程としてまとめて、その運用を関係者全員に周知徹底すること。	最低限	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．４．１．１【基本】） ・組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。（Ⅱ．４．２．１【基本】） ・情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。 また、ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークの運用・管理に関する手順書を作成すること。（Ⅲ．１．１．９【基本】） ・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．２．３．１【基本】）	cybozu.com のデータ消失対策は、以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/data_loss/index.html	適合可能	文献[06]にて、バックアップ頻度が日時であること、14日分の差分バックアップが取得されていること、また東日本および西日本のデータセンターにてバックアップが実施されていることが明記されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[06]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者が医療情報等を内部で保存する場合、システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能用量（サイズ、期間）、リスク、レスポンス、バックアップ頻度、バックアップ方法等を明示する必要がある。これらを運用管理規程としてまとめて、その運用を関係者全員に周知徹底する必要がある。
7.3-04					3. 記録媒体の保管場所やサーバの設置場所等には、許可された者以外が入室できないような対策を施すこと。	最低限	・情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。 また、ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークの運用・管理に関する手順書を作成すること。（Ⅲ．１．１．９【基本】） ・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅲ．４．４．１【基本】） ・重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること。（Ⅲ．４．４．３【基本】）	内規にて記録媒体を保管することができるエリアとして、「セキュリティエリア」を定めております。 当該エリアは許可された従業員のみアクセス可能です。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者が医療情報等を内部で保存する場合、記録媒体の保管場所やサーバの設置場所等には、許可された者以外が入室できないような対策を施す必要がある。
7.3-05					4. 電子的に保存された診療録等の情報に対するアクセス履歴を残し、管理すること。	最低限	・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】）	利用者の利用状況は、「監査ログ」機能にて確認できます。 詳細は以下のウェブページをご参照ください。 https://jp.cybozu.help/ja/k/admin/audit_logs	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者が医療情報等を内部で保存する場合、電子的に保存された診療録等の情報に対するアクセス履歴を残し、管理する必要がある。
7.3-06					5. 各保存場所における情報が き損した時に、バックアップされたデータを用いて き損前の状態に戻せること。もし、き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしておくこと。	最低限	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．２．３．１【基本】） ・バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認すること。（Ⅲ．２．３．２【推奨】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．５．３．１【基本】） ・バックアップのき損箇所の確認に関する仕様、方法等ついて、医療機関等と合意すること	サーバー上のディスクは多重障害にも耐えられるようにしております。 cybozu.com のデータ消失対策は、以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/data_loss/index.html	適合可能	文献[06]にて、バックアップ頻度が日次であること、また復元のためのリストア試験を毎日実施している旨が明記されている。	公開文書	文献[06]	–	–	–	利用者及びSI事業者が医療情報等を内部で保存する場合、各保存場所における情報が き損した時に、バックアップされたデータを用いて き損前の状態に戻せる必要がある。もし、き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしておく必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応						SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
7.3-07					（3） 記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止 1． 記録媒体が劣化する以前に情報を新たな記録媒体又は記録機器に複写すること。記録する媒体及び機器ごとに劣化が起こらずに正常に保存が行える期間を明確にして、使用開始日、使用終了日を管理して、月に一回程度の頻度でチェックを行い、使用終了日が近づいた記録媒体又は記録機器については、そのデータを新しい記録媒体又は記録機器に複写すること。これらの一連の運用の流れを運用管理規程にまとめて記載し、関係者に周知徹底すること。	最低限	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ． 2． 1． 3【基本】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。 （Ⅲ． 5． 3． 1【基本】）		適合可能	文献[06]より、利用者のデータを管理するディスクはすべて多重障害にも耐えられるように暗号化している、リストア試験も実施しているので適合可能と判断する。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[06]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者が記録媒体を利用する場合、記録媒体が劣化する以前に情報を新たな記録媒体又は記録機器に複写すること。記録する媒体及び機器ごとに劣化が起こらずに正常に保存が行える期間を明確にして、使用開始日、使用終了日を管理して、月に一回程度の頻度でチェックを行い、使用終了日が近づいた記録媒体又は記録機器については、そのデータを新しい記録媒体又は記録機器に複写する必要が。これらの一連の運用の流れを運用管理規程にまとめて記載し、関係者に周知徹底する必要がある。
7.3-08					（4） 媒体・機器・ソフトウェアの不整合による情報の復元不能の防止 1． システム更新の際の移行を迅速に行えるように、診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能を備えること。	最低限	・入出力するデータ項目の形式ついて、標準形式を採用する、標準形式にすることができない場合には、妥当なデータ項目の形式について医療機関等と合意すること。	製品内に含まれるお客様情報の出力形式については、各製品のマニュアルに記載されております。詳細は以下のウェブページをご参照ください。 https://manual.cybozu.co.jp/	適合可能	文献[20]、文献[21]、文献[22]、文献[23]にて、CSV形式, テキスト形式, ZIP形式等、汎用的なファイル形式にて入出力可能である記載が確認できた。	公開文書	文献[20]文献[21]文献[22]文献[23]	–	–	–	データ形式の選択・設定は、利用者が対応する必要がある。
7.3-09					2． マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えていること。	最低限	・マスターテーブルの変更に際してのレコード管理方法・とるべき措置等について、移行に際して情報内容の変更が生じない機能及び検証方法を備える。本機能を備えることが困難な場合には、妥当な提案を行い、医療機関等と合意すること。	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	利用者及びSI事業者は、マスターデータベースの変更の際に、過去の診療録等の情報に対する変更が起こらないように行う必要がある。
7.3-10					【ネットワークを通じて医療機関等の外部に保存する場合】 医療機関等に保存する場合の最低限のガイドラインに加え、次の事項が必要となる。 （1） データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと 保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられる。その場合、外部保存を受託する機関は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持しなくてはならない。	最低限	・ASP・SaaSによりデータ保存する際に用いるデータ形式及び転送プロトコルを変更する場合、変更前の方式との互換性の確保等について、医療機関等と合意する。	データセンターと接続する通信経路は暗号化しており、暗号化方式はQualys SSL Labs スコアで高ランクを維持するよう、日々見直しております。 以下のドキュメントも併せてご参照ください。 https://www.cybozu.com/jp/security/disaster_control/index.html 製品内に含まれるお客様情報の出力形式については、各製品のマニュアルに記載されております。詳細は以下のウェブページをご参照ください。 https://manual.cybozu.co.jp/	適合可能	文献[13]にて、顧客影響の大きなケースには、事前に通知する仕組みがあることを確認した。 また、文献[21]、文献[22]、文献[23]にて、医療機関等に保存する場合にはCSV形式で保存する方法が明記されていることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[13]文献[21]文献[22]文献[23]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者は、医療情報システムで使用するデータ形式及び転送プロトコルについて、バージョン管理と継続性の確保を行う必要がある。
7.3-11					（2） ネットワークや外部保存を受託する機関の設備の劣化対策を行うこと ネットワークや外部保存を受託する機関の設備の条件を考慮し、回線や設備が劣化した際にはそれらを更新する等の対策を行うこと。	最低限	・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等の稼働監視、障害監視、パフォーマンス監視の結果を評価・総括して、管理責任者に報告すること。（Ⅲ． 1． 1． 4【推奨】） ・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。 （Ⅲ． 2． 1． 2【基本】） ・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。（Ⅲ． 2． 1． 4【推奨】） ・ASP・SaaSに用いる回線もしくは施設等のサービスレベル維持を満足するための更新計画について、医療機関等と合意すること。	内規でサービス運用管理規定を策定し、運用いたしております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、設備の劣化対策を行う必要がある。
7.3-12					【医療機関等に保存する場合】 （1） 不適切な保管・取扱いによる情報の滅失、破壊の防止 1． 記録媒体及び記録機器、サーバの保管は、許可された者しか入ることができない部屋に保管し、その部屋の入退室の履歴を残し、保管及び取扱いに関する作業履歴と関連付けて保存すること。	推奨	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ． 7． 1． 3【基本】） ・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。 （Ⅲ． 4． 4． 1【基本】） ・サーバルームやラックの鍵管理を行うこと。（Ⅲ． 4． 4． 6【基本】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。 （Ⅲ． 5． 3． 1【基本】）	利用者様にて適切に実施いただく必要があります。	対象外	–	–	–	–	–	利用者及びSI事業者にて、記録媒体及び記録機器、サーバの保管は、許可された者しか入ることができない部屋に保管し、その部屋の入退室の履歴を残し、保管及び取扱いに関する作業履歴と関連付けて保存する必要がある。
7.3-13					2． サーバ室には、許可された者以外が入室できないように、鍵等の物理的な対策を施すこと。	推奨	・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。 （Ⅲ． 4． 4． 1【基本】） ・サーバルームやラックの鍵管理を行うこと。（Ⅲ． 4． 4． 6【基本】）	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	利用者及びSI事業者は、サーバ室には許可された者以外が入室できないように、鍵等の物理的な対策を施す必要がある。
7.3-14					3． 診療録等のデータのバックアップを定期的に取得し、その内容に対して改ざん等による情報の破壊が行われていないことを検査する機能を備えること。	推奨	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ． 2． 3． 1【基本】） ・バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認すること。（Ⅲ． 2． 3． 2【推奨】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。 （Ⅲ． 5． 3． 1【基本】） ・バックアップされたデータに対して、内容が改ざんされていないことを確認できる仕様について、医療機関等と合意すること。	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	利用者及びSI事業者は、診療録等のデータのバックアップを定期的に取得し、その内容に対して改ざん等による情報の破壊が行われていないことを検査する機能を備える必要がある。
7.3-15					（2） 記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止 診療録等の情報をハードディスク等の記録機器に保存する場合は、RAID-1 若しくはRAID-6 相当以上のディスク障害に対する対策を行うこと。	推奨	・医療情報のデータを格納するサーバのディスクの障害対策について、医療機関等と合意する。	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	利用者及びSI事業者は、診療録等の情報をハードディスク等の記録機器に保存する場合は、RAID-1 若しくはRAID-6 相当以上のディスク障害に対する対策を行う必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
7.3-16					【ネットワークを通じて医療機関等の外部に保存する場合】 （1） ネットワークや外部保存を受託する機関の設備の互換性を確保すること 1．回線や設備を新たなものに更新した場合、旧来のシステムに対応した機器が入手困難となり、記録された情報を読み出すことに支障が生じるおそれがある。従って、外部保存を受託する機関は、回線や設備の選定の際は将来の互換性を確保するとともに、システム更新の際には旧来のシステムに対応し、安全なデータ保存を保証できるような互換性のある回線や設備に移行すること。	推奨	ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。（Ⅲ．２．１．２【基本】） ・ASP・SaaSに用いる回線もしくは施設等のサービスレベル維持を満足するための更新計画について、医療機関等と合意すること。	内規にて運用管理規定（変更管理）を定め、運用いたしております。 お客様のデータに関しては、利用規約の定めにある例外事項を除き、サイボウズが閲覧・変更・削除をすることはございません。 以下のドキュメントについてもご参照ください。 cybozu.com サービスご利用規約 https://www.cybozu.com/jp/terms/ プライバシーポリシー https://cybozu.co.jp/privacy/privacy-policy/ クラウドデータポリシー https://cybozu.co.jp/privacy/cloud-data-policy/	適合可能	文献[13]にて、以下を確認した。 ・データベースへのフィールドの追加等、下位互換性が図れないような場合には、利用者へのアップデート前のアナウンスを実施し、必要であれば利用者に先行動作環境を提供する準備があること。 ・顧客影響の大きなケースには、事前に通知する仕組みがあること。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[13]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、サービス提供ポリシーおよびブラウザサポートポリシーをお客様に開示し、合意して頂く必要がある。
8.1-01	8	8.1	電気通信回線を通じて外部保存を行う場合にあっては、保存に係るホストコンピュータ、サーバ等の情報処理機器が医療法第1 条の5 第1 項に規定する病院又は同条第2 項に規定する診療所その他これに準ずるものとして医療法人等が適切に管理する場所、行政機関等が開設したデータセンター等、及び医療機関等が民間事業者等との契約に基づいて確保した安全な場所に置かれるものであること。 （外部保存改正通知第2 1 （2）） 本来、医療に関連した個人情報の漏えいや不当な利用等により、個人の権利利益が侵害された場合には、被害者の苦痛や権利回復が困難であることが多く、医療機関等や関係各者に対し、法律や各種ガイドライン等により格別の安全管理措置を講じることが求められている。従って、診療録等のネットワークを通じた医療機関等以外の場所での外部保存については、通常求められる安全管理上の体制と同等以上の体制を確保した上で、患者に対する保健医療サービス等の提供に当該情報を利活用するための責任を果たせることが原則である。 上記に対応するためには「C．最低限のガイドライン」で定める、「②行政機関等が開設したデータセンター等に保存する場合」と「③医療機関等が民間事業者等との契約に基づいて確保した安全な場所」に該当する機関を選定する場合には、「C．最低限のガイドライン」で定める事項を厳守し、また、データセンター等の情報処理関連事業者が経済産業省が定めた「医療情報を受託管理する情報処理事業者向けガイドライン」や総務省が定めた「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」の要求事項を満たしていることを確認の上、契約等でその遵守状況を明らかにしなくてはならない。	ネットワークを通じて医療機関等以外の場所に診療録等を保存することができれば、システム堅牢性の高い安全な情報の保存場所の確保によるセキュリティ対策の向上や災害時の危機管理の推進、保存コストの削減等により医療機関等において診療録等の電子保存が推進されることが期待できる。しかし、外部保存には保存機関の不適切な情報の取り扱いにより患者等の情報が瞬時に大量に漏えいする危険性も存在し、その場合、漏えいした場所や責任者の特定が困難になる可能性がある。そのため、常にリスク分析を行いつつ万全の対策を講じなければならず、医療機関等の責任が相対的に大きくなる。 さらには、情報の保存を受託する機関等もしくは従業者による、利益を目的とした不当利用の危惧があるのも事実である。その一方で金融情報、信用情報、通信情報は実態として保存・管理を当該事業者以外の外部事業者に委託しており、合理的に運用されている、金融・信用・通信に関わる情報と医療に関わる情報を一概に同様に扱うことはできないが、一般に実績あるデータセンター等の情報の保存・管理を受託する事業者は慎重で十分な安全対策を講じており、医療機関等が自ら管理すること比べても厳重に管理されていることが多い。	(1) 病院、診療所、医療法人等が適切に管理する場所に保存する場合 (ア) 病院や診療所の内部で診療録等を保存すること。	最低限	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	–
8.1-02					(イ) 保存を受託した診療録等を委託した病院、診療所や患者の許可なく分析等を目的として取り扱わないこと。	最低限	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	–
8.1-03					(ウ) 病院、診療所等であっても、保存を受託した診療録等について分析等を行う場合は、委託した病院、診療所及び患者の同意を得た上で、不当な営利、利益を目的としない場合に限ること。	最低限	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	–
8.1-04					(エ) 匿名化された情報を取り扱う場合においても、匿名化の妥当性の検証を検証組織で検討するとか、取り扱いをしている事実を患者等に掲示等を使って知らせる等、個人情報の保護に配慮した上で実施すること。	最低限	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	–
8.1-05					(オ) 情報を保存している機関に患者がアクセスし、自らの記録を閲覧するような仕組みを提供する場合は、情報の保存を受託した病院、診療所は適切なアクセス権を規定し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないように配慮すること。	最低限	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	–
8.1-06					(カ) 情報の提供は、原則、患者が受診している医療機関等と患者間の同意で実施されること。	最低限	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	–
8.1-07					② 行政機関等が開設したデータセンター等に保存する場合 (ア) 法律や条例により、保存業務に従事する個人もしくは従事していた個人に対して、個人情報の内容に係る守秘義務や不当使用等の禁止が規定され、当該規定違反により罰則が適用されること。	最低限	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	–
8.1-08					(イ) 適切な外部保存に必要な技術及び運用管理能力を有することを、システム監査技術者及びCertified Information Systems Auditor（ISACA 認定）等の適切な能力を持つ監査人の外部監査を受ける等、定期的に確認されていること。	最低限	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	–
8.1-09					(ク) 医療機関等は保存された情報を、外部保存を受託する事業者が分析、解析等を実施しないことを確認し、実施させないことを明記した契約書等を取り交わすこと。	最低限	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	–
8.1-10					(ケ) 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等が起こらないようにさせること。	最低限	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	–
8.1-11					③ 医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合 (ア) 医療機関等が、外部保存を受託する事業者と、その管理者や電子保存作業従事者等に対する守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取り扱いに対して監督を行えること。	最低限	・従業員が、情報セキュリティポリシーもしくはASP・SaaS サービス提供上の契約に違反した場合の対応手続を備えること。（Ⅱ．５．２．２【基本】） ・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１【基本】） ・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２【基本】） ・守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わすこと。	就業規則にて、以下の事例に対して罰則を設けております。 ①セキュリティ事件・事故を故意に起こそうとした場合 ②情報セキュリティに関する重大な過失を犯した場合 ③情報セキュリティに関する過失を繰り返した場合	適合可能	文献[10]にて、cybozu.com上に入力・保存したデータ（入力データ）についての管理責任は顧客にあることが明記されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[10]	–	–	詳細はサイボウズ社とのNDAにより開示。	医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合には、医療機関等が、外部保存を受託する事業者と、その管理者や電子保存作業従事者等に対する守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取り扱いに対して監督を行える必要がある。
8.1-12					(イ) 医療機関等と外部保存を受託する事業者を結ぶネットワーク回線の安全性に関しては「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守していること。	最低限	・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。（Ⅲ．３．２．１【基本】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。（Ⅲ．３．２．２【推奨】） ・第三者が当該事業者のサーバになりすまして（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。（Ⅲ．３．２．３【基本】） ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。（Ⅲ．３．２．４【基本】） ・外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報すること。（Ⅲ．３．２．５【推奨】） ・ネットワーク回線を含めてASP・SaaS事業者がサービスを提供する場合、そのネットワークの安全性に関しては、「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守すること。 ・自社で属しるネットワークの安全対策が、医療機関等が定めるネットワーク回線の安全性に関する基準を満たしていることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	利用者様クライアント環境から cybozu.com への転送経路は、SSL にて暗号化しております。 暗号形式は Qualys SSL Labs スコアで高ランクを維持するよう、日々方式を見直しております。 以下の資料も併せてご参照ください。 https://www.cybozu.com/jp/security/disaster_control/index.html	適合可能	文献[07]にて、データセンターと接続する回線には、Qualys SSL Labs スコアで高ランクを維持するよう、日々暗号化方式を見直している旨が記載されている。 文献[03]にて、クライアント証明書を利用したセキュアアクセスの実現、また悪意のあるサイトによる情報流出を防ぐ機能を有していることが明記されている。	公開文書	文献[03]文献[07]	–	–	–	医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合には、医療機関等と外部保存を受託する事業者を結ぶネットワーク回線の安全性に関しては「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守している必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応						SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
8.1-13					(ウ) 受託事業者が民間事業者等に課せられた経済産業省の「医療情報を受託管理する情報処理事業者向けガイドライン」や総務省の「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」等を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等で確認をすること。	最低限	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１【基本】） ・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２【基本】） ・ASP・SaaSにおける情報セキュリティ対策ガイドライン（平成20年1月30日総務省）及びホガイドラインを遵守すること。 ・遵守すべきガイドラインの範囲及びこれを遵守している旨の報告につき、その内容・範囲等を、医療機関等と合意すること。	サイボウズは cybozu.com の運用に関して ISMS 認証を受けております。 認証登録番号：IS 577142 内規に基づき内部監査を実施し、ISMS 認証審査の過程で外部からの審査を受けております。 また cybozu.com 運用基盤上で動作するアプリケーションについては、年に１回脆弱性診断を受け、その結果を以下のウェブページで公開しております。 https://www.cybozu.com/jp/productsecurity/	適合可能	サイボウズでは、文献[17]に則り、ISMSで適切に管理されている旨が記載されていることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[17]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者側でも適切な管理を実施する必要がある。
8.1-14					(エ) 保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと。なお保守に関しては、「6.8 情報システムの改造と保守」を遵守すること。	最低限	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１【基本】） ・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．７．１．３【基本】） ・受託した医療情報を、保守作業に必要な範囲での閲覧を超えて閲覧しないこと。 ・許可されていない受託データの閲覧を禁止することにつき、その方法等を含め、医療機関等と合意すること。	外部への業務委託については、内規にて運用管理規定（外部委託）として、以下の事項を定め、運用しております。 - 情報の取扱いを委託する場合、委託する情報の安全管理が当社で規定する水準以上であることを確認し、適切な管理を行うこと - 委託の担当者は、秘密保持に関する条項および秘密情報漏えい等の場合の損害賠償を含む契約を締結すること	適合可能	文献[10]にて、cybozu.com上に入力・保存したデータ（入力データ）については入力データに関するいかなる権利も有さないことが明記されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[10]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者は、医療情報システム提供事業者が提供するサービス内容及び約款等について、保守作業に必要な範囲を超えた閲覧の禁止に関して確認する必要がある。
8.1-15					(オ) 外部保存を受託する事業者が保存した情報を分析、解析等を実施してはならないこと。匿名化された情報であっても同様であること。これらの事項を契約に明記し、医療機関等において厳守させること。	最低限	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１【基本】） ・受託した医療情報は、匿名化されたものを含めて、医療機関との契約に基づくことなく、分析、解析等を実施しないこと。 ・医療機関との契約に基づくことなく、受託したデータの分析・解析を実施しないことにつき、その方法等を含め、医療機関等と合意すること。		適合可能	また文献[10]にて、cybozu.com上に入力・保存したデータ（入力データ）については入力データに関するいかなる権利も有さないことが明記されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[10]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者は、医療情報システム提供事業者が提供するサービス内容及び約款等について、保存した情報の分析、解析の禁止に関して確認する必要がある。
8.1-16					(カ) 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等が起こらないようにさせること。	最低限	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】）		適合可能	文献[10]にて、cybozu.com上に入力・保存したデータ（入力データ）については入力データに関するいかなる権利も有さないことが明記されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[10]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者は、医療情報システム提供事業者が提供するサービス内容及び約款等について、外部保存を受託する事業者が保存された情報の提供を行わないよう確認する必要がある。
8.1-17					(キ) 医療機関等において（ア）から（カ）を満たした上で、外部保存を受託する事業者の選定基準を定めること。少なくとも以下の4 点について確認すること。 （a） 医療情報等の安全管理に係る基本方針・取扱規程等の整備 （b） 医療情報等の安全管理に係る実施体制の整備 （c） 実績等に基づく個人データ安全管理に関する信用度 （d） 財務諸表等に基づく経営の健全性	最低限	・契約に先立ち、医療機関等の管理者から、選定に必要な情報の提供を求められた場合に、速やかに提出すること。	サイボウズでは情報セキュリティに係る基本方針を定め、取り扱い規定を整備し、運用体制を構築しております。 また ISMS 審査を 2011 年から取得し、更新・維持しております。 経営状況については、IR 情報などのウェブページをご参照ください。 https://cybozu.co.jp/company/ir/	適合可能	本項目は基本的に医療機関側で実施すべき事項である。 ただし、確認すべき事項については、以下を確認することが出来た。 ・ISMSサーベランスを7年間連続で審査に合格しており、信用度に関しては問題ないと判断する。 ・文献[30]および文献[31]にて公開されていることから、経営の健全性は問題ないと判断した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[30]文献[31]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者は、外部保存を受託する事業者の選定基準を定める必要がある。
8.1-18					(ア)「①病院、診療所、医療法人等が適切に管理する場所に保存する場合」のうち、医療法人等が適切に管理する場所に保管する場合、保存を受託した機関全体としてのより一層の自助努力を患者・国民に示す手段として、それぞれ個人情報保護及び情報セキュリティマネジメントの認定制度である、プライバシーマークやISMS 認定等の第三者による認定を取得すること。	推奨	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	–
8.1-19					(イ)「②行政機関等が開設したデータセンター等に保存する場合」においては、制度上の監視や評価等を受けることになるが、更なる評価の一環として、（ア）で述べた第三者による認定を受けること。	推奨	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	–
8.1-20					(ウ)「②行政機関等が開設したデータセンター等に保存する場合」及び「③医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合」では、技術的な方法としては、例えばトラブル発生時のデータ修復作業等緊急時の対応を除き、原則として委託する医療機関等のみがデータ内容を閲覧できることを担保すること。	推奨	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】）	お客様のデータに関しては、利用規約の定めにある例外事項を除き、サイボウズが閲覧・変更・削除をすることはございません。 以下のドキュメントについてもご参照ください。 cybozu.com サービスご利用規約 https://www.cybozu.com/jp/terms/ プライバシーポリシー https://cybozu.co.jp/privacy/privacy-policy/ クラウドデータポリシー https://cybozu.co.jp/privacy/cloud-data-policy/	適合可能	文献[10]の15.4にて以下の記載を確認した。 サイボウズは、以下の目的によるとサイボウズが判断した場合を除き、入力データに対し、アクセスを行うことはありません。 ・サービスシステムの安全な運営のため ・本サービスまたは本サービスのシステム上の問題を防止するため ・本サービスのサポート上の問題に関連してお客様からサイボウズに要請があった場合に、当該サポート上の問題を解決するため	公開文書	文献[10]	–	–	–	利用者は、医療情報システム提供事業者が提供するサービス内容及び約款等を確認する必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するサイボウズの見解	Cybozu.com における対応						SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
8.1-21					(エ) 外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、外部保存を受託する事業者の管理者といえども通常はアクセスできない制御機構をもつこと。具体的には、「暗号化を行う」、「情報を分散保管する」という方法が考えられる。その場合、非常時等の通常とは異なる状況下でアクセスすることも想定し、アクセスした事実が医療機関等で明示的に識別できる機構を併せ持つこと。	推奨	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅱ．３．１．１【基本】） ・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。（Ⅲ．３．１．２【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．３．１．３【基本】） ・システム管理者のデータアクセスの制限の方法について、医療機関等と合意する。	以下のドキュメントについてもご参照ください。 cybozu.com サービスご利用規約 https://www.cybozu.com/jp/terms/ プライバシーポリシー https://cybozu.co.jp/privacy/privacy-policy/ クラウドデータポリシー https://cybozu.co.jp/privacy/cloud-data-policy/	適合可能	文献[07]にて、データセンターとの接続する回線は暗号化通信を利用していることが明記されている。 また文献[10]にて、cybozu.com上に入力・保存したデータ（入力データ）については入力データに関するいかなる権利も有さないことが明記されている。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[07]文献[10]	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、外部保存を受託する事業者の管理者といえども通常はアクセスできない制御機構をもたせる必要がある。
8.2-01		8.2	患者のプライバシー保護に十分留意し、個人情報の保護が担保されること。 （外部保存改正通知第2 1（3））	ネットワークを通じて外部に保存する場合、医療機関等の管理者の権限や責任の範囲が、自施設とは異なる他施設や通信事業者にも及ぶために、より一層、個人情報の保護に配慮が必要となる。 なお、患者の個人情報の保護等に関する事項は、診療録等の法的な保存期間が終了した場合や、外部保存を受託する事業者との契約期間が終了した場合でも、個人情報が存在する限り配慮される必要がある。また、バックアップ情報における個人情報の取扱いについても、同様の運用体制が求められる。	（1）診療録等の外部保存委託先の事業者内における個人情報保護 ① 適切な委託先の監督を行うこと 診療録等の外部保存を受託する事業者内の個人情報保護については本ガイドライン6 章を参照し、適切な管理を行う必要がある。	最低限	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１【基本】） ・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．７．１．２【基本】） ・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．７．１．３【基本】） ・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．５．１．２【基本】） ・自社で定める個人情報保護を記録した媒体の運用管理規程等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・個人情報保護法の対象に満たない件数(5,000件未満）対象外（死者に関する情報）等であっても、医療情報の重要性から個人情報保護法における運用に準じて取り扱う旨が含まれていることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	個人情報の保護に関しては、以下のウェブページをご参照ください。 プライバシーポリシー https://cybozu.co.jp/privacy/privacy-policy/	適合可能	文献[15]にて、外部委託先（サイボウズ社）が個人情報を取り扱う部門ごとに管理責任者を置き、個人情報の適切な管理に努めることが記載されている。	公開文書	文献[15]	–	–	–	利用者及びSI事業者は、診療録等の外部保存を受託する事業者内の個人情報保護については本ガイドライン6 章を参照し、適切な管理を行う必要がある。監督責任は利用者である。
8.2-02					(2) 外部保存実施に関する患者への説明 診療録等の外部保存を委託する施設は、あらかじめ患者に対して、必要に応じて患者の個人情報が特定の外部の施設に送られ、保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得る必要がある。 ① 診療開始前の説明 患者から、病態、病歴等を含めた個人情報を収集する前に行われるべきであり、外部保存を行っている旨を、院内掲示等を通じて説明し理解を得た上で診療を開始すること。	最低限	・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．５．１．２【基本】） ・医療機関等が患者等に対して行う個人情報等の外部保存に関する説明に必要な資料の提供とその範囲、役割分担等について、医療機関等と合意すること。	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	利用者は、個人情報を外部保存を行っている旨を患者に説明し理解を得た上で診療を開始する必要がある。
8.2-03					② 患者本人に説明をすることが困難であるが、診療上の緊急性がある場合 意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は必ずしも事前の説明を必要としない。意識が回復した場合には事後に説明を行い、理解を得る必要がある。	最低限	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	利用者は、意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は、意識が回復した時点で事後に説明をし、理解を得る必要がある。
8.2-04					③ 患者本人に説明することが困難であるが、診療上の緊急性が特にない場合 乳幼児の場合も含めて本人に説明し理解を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得ること。 ただし、親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。	最低限	–	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	利用者は、乳幼児の場合も含めて本人に説明し理解を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得る必要がある。 ただし、親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。
8.3-01		8.3	外部保存は、診療録等の保存の義務を有する病院、診療所等の責任において行うこと。 また、事故等が発生した場合における責任の所在を明確にしておくこと。 （外部保存改正通知第2 1（4））	本項の記載は、「4 電子的な医療情報を扱う際の責任のあり方」及び「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」へ考え方を集約したため、それらを参照されたい。	–	–	–	–	–	–	–	–	–	–	–	–
8.4-01		8.4	外部保存を行う病院、診療所等の管理者は、運用管理規程を定め、これに従い実施すること。 （外部保存改正通知第3 1）	外部保存に係る運用管理規程を定めることが求められており、考え方及び具体的なガイドラインは、「6.3 組織的安全管理対策」の項を参照されたい。 また、その際の責任のあり方については、「4 電子的な医療情報を扱う際の責任のあり方」を参照されたい。 なお、すでに電子保存の運用管理規程を定めている場合には、外部保存に対する項目を適宜修正・追加等すれば足りると考えられる。	診療録等が機微な個人情報であるという観点から、外部保存を終了する場合には、医療機関等及び受託する事業者双方で一定の配慮をしなくてはならない。 診療録等の外部保存を委託する医療機関等は、受託する事業者に保存されている診療録等を定期的に調べ、外部保存を終了しなければならない診療録等は速やかに処理した上で、当該処理が厳正に執行行われたかを監査しなくてはならない。また、外部保存を受託する事業者も、医療機関等の求めに応じて、保存されている診療録等を厳正に取扱い、処理を行った旨を医療機関等に明確に示す必要がある。 これらの廃棄に関わる規定は、外部保存を開始する前に委託契約書等にも明記をしておく必要がある。また、実際の廃棄に備えて、事前に廃棄プログラム等の手順を明確化した規定を作成しておくべきである。 これらの厳正な取扱い事項を双方に求めるのは、同意した期間を超えて個人情報を保持すること自体が、個人情報の保護上問題になり得るためであり、そのことに十分に留意しなければならない。 ネットワークを通じて外部保存する場合は、外部保存システム自体も一種のデータベースであり、インデックスファイル等も含めて慎重に廃棄しなければならない。また電子媒体の場合は、バックアップファイルについても同様の配慮が必要である。 また、ネットワークを通じて外部保存している場合は、自ずと保存形式が電子媒体となるため、情報漏えい時の被害は、その情報量の点からも甚大な被害が予想される。従って、個人情報保護に十分な配慮を行い、確実に情報が廃棄されたことを、外部保存を委託する医療機関等と受託する事業者とが確実に確認できるようにしておかなくてはならない。 （厚労省ガイドラインでは「B.考え方」の枠に記載されている内容だが、総務省ガイドラインでは要求事項として扱われているためここに記載）	–	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．７．１．１【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．２．１．３【基本】） ・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．５．１．２【基本】） ・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．５．３．２【基本】） ・事業者の都合により医療機関等に対してASP・SaaSの提供を終了する場合の事前通知の方法、終了が認められる理由、及び終了に向けての対応について、医療機関等と合意すること。 ・情報の破棄の実施に際し、報告の内容・範囲・提出すべき資料等について、医療機関等と合意すること。 ・ASP・SaaSの提供を終了する場合に、受託しているデータ及びこれに関連する資料の内容、範囲、条件等について、医療機関等と合意すること。 ・受託データを医療機関に引き渡す際には、厚生労働省ガイドライン「5 情報の相互運用性と標準化について」に従って行うことし、その内容について医療機関等と合意すること。	内規にて運用管理規定（情報区分と情報区分に応じた資産の取り扱い方法）を定め、運用いたしております。 媒体を破棄する場合には、物理的に破壊して廃棄しております。 サービス終了時には、cybozu.com 利用規約の定めに沿ってお客様にご連絡し、利用終了後には一定の期間を経てデータを削除いたします。 以下のウェブサイトも併せてご参照ください。 https://www.cybozu.com/jp/security/disaster_control/index.html https://www.cybozu.com/jp/terms/	適合可能	文献[07]にて、媒体の廃棄は物理的に破壊して廃棄することが明記されていることを確認した。 また、サービス終了時の取り決め及び終了時のデータの取り扱いについて、文献[10]（cybozu.com利用規約）に記載されており、cybozu.comの利用はこの規約に基づき利用されるものであることから、医療機関との間にて合意が得られているものと考えられる。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[07]文献[10]	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、診療録等の外部保存を受託する医療機関等は、受託する事業者に保存されている診療録等を定期的に調べ、外部保存を終了しなければならない診療録等は速やかに処理した上で、当該処理が厳正に執行行われたかを監査しなくてはならない。また、外部保存を受託する事業者も、医療機関等の求めに応じて、保存されている診療録等を厳正に取扱い、処理を行った旨を医療機関等に明確に示す必要がある。

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
2.1 医療情報に係る情報処理事業を受託する上で推奨される認証及び認定			医療情報に係る情報処理事業を受託する機関においては、医療情報の安全確保を目的として、合理的・客観的な基準による公正な第三者認証を取得すること。	cybozu.comは、ISO/IEC27001:2013／JIS Q 27001:2014の要求事項に適合し、認証を取得しております。 認証登録番号 IS 577142	適合可能	文献[01]にて、cybozu.comは、ISO/IEC27001:2013／JIS Q 27001:2014の要求事項に適合し、認証登録を取得していることを確認した。	公開文書	文献[01]	ISO/IEC 27001	–	–	–
2.2.情報資産管理			医療情報が完全な状態にあることを保証するために、資産台帳等を適切に維持管理することを目的として、以下の管理策を適用すること。なお、資産台帳等の媒体は、紙文書、電子ファイルのいずれでも良いが、媒体特有の脅威について把握し、適切な管理策を追加すること。	電子ファイルにて情報資産台帳を作成し、管理しております。	適合可能	文献[10]にて、サイボウズでは、情報の種類を区分して管理方法を決めている。情報の種類とは、(1)お客様がcybozu.comに登録・入力・保存した「入力データ」、(2)お客様がcybozu.comにアクセスした「利用データ」、(3)お客様の「契約者情報」、(4)入力データの「バックアップデータ」である。 文献[06]にて、お客様がcybozu.comに登録・入力・保存した「入力データ」はサイボウズで権利を取得しないこととしているため、対象外である。 以下の各項目は、「利用データ」「契約者情報」「バックアップデータ」を対象に確認する。	公開文書	文献[06] 文献[10]	–	–	–	利用者およびSI事業者は、自らがcybozu.comに登録・入力・保存した医療情報データを適切に管理する必要がある。
	2.2.1.資産台帳	(1)	医療機関等から預かる情報を管理するための管理台帳の整備について文書化して管理すること。	各事業部のセキュリティ施策を推進する「情報責任者」が、情報資産に対して「情報区分」と呼ばれる機密レベルを設定します。 設定された機密レベルに応じた情報の管理方法を定めており、 「データ利用者」は「情報責任者」の指示に従って資産を利用します。	適合可能	文献[01]にて、サイボウズでは、情報資産管理台帳にて、情報資産を明確にし、各情報資産の利用許容範囲の文書を作成しており、ISMSにおいて定期的に見直し・更新していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らがcybozu.comに登録・入力・保存した医療情報データを管理台帳で管理するよう文書化する必要がある。
		(2)	預託された情報の全てを資産台帳に記録すること。	お客様からお預かりした情報は、cybozu.com利用規約の定めに従って分類し、資産管理しております。 https://www.cybozu.com/jp/terms/	適合可能	文献[01]にて、サイボウズでは、情報資産管理台帳にて、各資産名、管理責任者、C.I.Aレベル、利用許可範囲、情報コンテナ、保存期間ごとに分類して記載していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らがcybozu.comに登録・入力・保存した医療情報データの分類を適切に実施する必要がある。
		(3)	必要に応じて資産台帳の閲覧が速やかに行うことができる状態で管理しておくこと。	電子ファイルは社内システムに保管し、アクセス権を付与されたものが速やかに閲覧可能としております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、自らがcybozu.comに登録・入力・保存した医療情報データを管理台帳により適切に管理する必要がある。
		(4)	資産台帳等へのアクセスについては、閲覧・編集が必要な作業者に制限すること。	社内ポリシーに準じて制限をしています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らがcybozu.comに登録・入力・保存した医療情報データを管理台帳により適切に管理する必要がある。
		(5)	資産台帳等を電磁的記録として管理する場合には、資産台帳等へのアクセス制限を侵害する行為について記録すること。	社内システムのアクセスログを取得、保管しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、自らがcybozu.comに登録・入力・保存した医療情報データを管理台帳により適切に管理する必要がある。
	2.2.2.情報の分類	(1)	情報を分類するための指針を決定し、情報の所有者、管理責任者が指針に従って適切な分類を行うことができるようにしておくこと。	各事業部のセキュリティ施策を推進する「情報責任者」が、情報資産に対して「情報区分」と呼ばれる機密レベルを設定します。 設定された機密レベルに応じた情報の管理方法を定めており、 「データ利用者」は「情報責任者」の指示に従って資産を利用します。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らがcybozu.comに登録・入力・保存した医療情報データの分類を適切に実施する必要がある。
		(2)	情報の所有者、管理責任者は情報の分類が正しく行われていることを定期的に確認すること。	「情報責任者」の責務として、情報資産の棚卸を監督することを定めております。通常、年に１度資産の棚卸を行います。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らがcybozu.comに登録・入力・保存した医療情報データの分類を適切に実施する必要がある。
		(3)	預託される情報に対して分類にもとづいたリスク分析を実施すること。	現状把握とリスク評価を組み合わせたリスク分析を行っております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らがcybozu.comに登録・入力・保存した医療情報データの分類に基いてリスク管理を適切に実施する必要がある。
		(4)	リスク分析の結果に応じて、リスク低減に必要な管理策を実施すること。	リスク分析の結果検出されたリスクは、情報資産の「情報責任者」がリスクマジメントを行い、「リスク対応計画」として文書化されます。本計画は、代表取締役によるマネジメントレビューにて承認されます。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らがcybozu.comに登録・入力・保存した医療情報データの分類に基いてリスク管理を適切に実施する必要がある。
		(5)	分類がわかるように情報にラベルをつけること（電磁的な記録にラベルをつける方式には様々なものが考えられるので、実装する方式の詳細及び安全性について、医療機関等側の確認、承認を得ること）。	各事業部のセキュリティ施策を推進する「情報責任者」が、情報資産に対して「情報区分」と呼ばれる機密レベルを設定します。 設定された機密レベルに応じた情報の管理方法を定めており、 「データ利用者」は「情報責任者」の指示に従って資産を利用します。	適合可能	文献[01]にて、サイボウズでは、情報のCIAレベルごとに分類して台帳管理していることをHPで公開しており、cybozu.com利用者はそれを参照した上で、cybozu.comを利用していただいていることを確認した。	公開文書	文献[01]	–	–	–	利用者およびSI事業者は、自らがcybozu.comに登録・入力・保存した医療情報データの分類に基いてリスク管理を適切に実施する必要がある。

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(6)	各ラベルに応じた処理方式（保存、配送、閲覧、廃棄等）を定めること。	各事業部のセキュリティ施策を推進する「情報責任者」が、情報資産に対して「情報区分」と呼ばれる機密レベルを設定します。 設定された機密レベルに応じて、情報の保存、配送、閲覧、廃棄などの管理方法を定めています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、自らがcybozu.comに登録・入力・保存した医療情報データの分類に基いてリスク管理を適切に実施する必要がある。
2.3.組織的安全管理策（体制、運用管理規程）		(1)	医療情報の安全管理に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。	お客様からお預かりした情報は、cybozu.com利用規約の定めに従って分類し、管理しております。 https://www.cybozu.com/jp/terms/ 下記文書も併せてご参照ください。 プライバシーポリシー https://cybozu.co.jp/privacy/privacy-policy/ クラウドデータポリシー https://cybozu.co.jp/privacy/cloud-data-policy/ ISMS基本方針 https://www.cybozu.com/jp/terms/security.html	適合可能	文献[03]、文献[04]、文献[05]、文献[06]、文献[07]、文献[08]、文献[09]、文献[14]、文献[15]にて、サイボウズでは、医療情報に関する管理方針を策定しており、HPで公開していることを確認した。	公開文書	文献[03] 文献[04] 文献[05] 文献[06] 文献[07] 文献[08] 文献[09] 文献[14] 文献[15]	–	–	–	利用者およびSI事業者は、cybozu.comで取り扱う医療情報データの安全管理に関する方針を策定する必要がある。
		(2)	個人情報保護に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。	お客様が個人情報の照会、訂正、削除、利用停止等を希望される場合には合理的範囲内で速やかに対応いたします。 詳細は以下の文書をご参照ください。 プライバシーポリシー https://cybozu.co.jp/privacy/privacy-policy/	適合可能	文献[15]にて、お客様が個人情報の照会、訂正、削除、利用停止等を希望される場合には合理的範囲内で速やかに対応することを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[15]	–	–	詳細はサイボウズ社とのNDAにより開示。	–
		(3)	個人情報保護に関しては、医療機関等の監督の下に行うこと。	cybozu.comは、ISO/IEC27001:2013／JIS Q 27001:2014の要求事項に適合し、認証を取得する過程で、第三者による審査を受けております。またサービスに関する脆弱性の有無を第三者機関に診断を受けており、結果は下記ウェブページで公開しております。 https://www.cybozu.com/jp/productsecurity/	適合可能	文献[02]にて、cybozu.comの脆弱性の有無をHPで公開していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[02]	–	–	詳細はサイボウズ社とのNDAにより開示。	–
		(4)	情報処理の安全管理に関わる手順書、運用管理規程を整備すること。	cybozu.comは、ISO/IEC27001:2013／JIS Q 27001:2014の要求事項に従い、手順書および、運用管理規定を定めております。 セキュリティに関する基本方針については、以下からご参照いただくことが可能です。 https://www.cybozu.com/jp/terms/security.html https://cybozu.co.jp/company/internal-control/ また情報セキュリティの体制を強化することを目的として、2011 年に Cy-SIRT を設立し、サイバーセキュリティリスクへの対応を行っております。 https://www.cybozu.com/jp/security/management/cysirt.html セキュリティに関する問い合わせ窓口については、下記をご利用ください。 脆弱性のご連絡 https://www.cybozu.com/jp/support/security.html 情報セキュリティ・インシデント連絡窓口 https://contact.cybozu.co.jp/security/	適合可能	文献[01]にて、cybozu.comは、ISO/IEC27001:2013／JIS Q 27001:2014の要求事項に適合し、認証登録を取得していることを確認した。 文献[09]にて、手動オペレーションによる操作は全て手順書を整備し、手順書に従って実施することを徹底していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01] 文献[09]	ISO/IEC 27001	–	詳細はサイボウズ社とのNDAにより開示。	–
		(5)	運用管理規程には、情報セキュリティに対する組織的取組方針、情報処理事業者内の体制及び施設、医療機関及び清掃事業者等の外部事業者との契約書の管理、情報処理に関わるハードウェア・ソフトウェアの管理方法、リスクに対する予防、リスク発現時の対応、医療情報を格納する媒体の管理（保管・授受等）、第三者による情報セキュリティ監査、医療機関等の管理者からの問い合わせ窓口の設置、対応等について記載しておくこと。		適合可能	文献[01]にて、cybozu.comは、ISO/IEC27001:2013／JIS Q 27001:2014の要求事項に適合し、認証登録を取得していることを確認した。 文献[05]および文献[09]にて、情報セキュリティ体制強化のためにCSIRT（Cy-SIRT）を設立・活動していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01] 文献[05] 文献[09]	ISO/IEC 27001	–	詳細はサイボウズ社とのNDAにより開示。	–
2.4.医療情報の伝達経路におけるリスク評価			医療情報の取扱いに際しては高い機密性が求められていることに配慮しなければならない。機密性を確保するためには、医療情報の移動する範囲を限定することが必要である。情報の入り口から保管場所、電子媒体であれば適切な保護機能と一定の強度を備えた保管庫、電磁的記録であれば適切なアクセス管理を施されたデータベース、ファイルサーバ等に保存されるまでの経路、及び医療機関等に医療情報を提供する経路、最終的に情報を廃棄する経路を認識し、その経路上に存在する脅威を列挙してリスク評価を行うこと。	リスク分析の結果検出されたリスクは、情報資産の「情報責任者」がリスクマジメントを行い、「リスク対応計画」として文書化されます。本計画は、代表取締役によるマネジメントレビューにて承認されます。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	—	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comに登録・入力・保存した医療情報データの伝送経路についてリスク評価を適切に実施する必要がある。
2.5.物理的安全対策	2.5.1.医療情報処理施設の建物に関する要求事項		情報処理事業者の専有する領域に医療情報システムを設置する場合には、以下に示す物理的安全管理策を施すこと。外部事業者が運用するデータセンター及びサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合においても、同等の措置がとられていることを確認すること。	外部事業者のデータセンターを利用しております。 サーバーラックはサイボウズが占有する領域を利用しております。	適合可能	以下の項目にて確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
		(1)	医療情報が保存されるサーバ機器等への不正アクセスを防止するため、サーバラックの施錠管理、鍵管理が行われていること。	サーバーラックの施錠管理を行っております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	–

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(2)	傍受、盗撮等の不正な行為を防止するため、部屋を区切る壁面、天井、床部分においては、十分な厚みを持たせ、監視カメラでの常時監視及び画像記録の保存、不正に取り付けられた装置の定期的な検出等の対策を施すこと。	運用メンバーは「入室制限エリア」と呼ばれる、一般社員とは隔離された執務スペースで業務を行っています。 詳細は以下の Web ページを参照ください。 https://www.cybozu.com/jp/security/vulnerability/index.html	適合可能	文献[05]にて、運用メンバーは一般社員と分離された執務スペースで業務を行い、運用メンバーの執務スペースは監視カメラで入退出を管理していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[05]	–	詳細はサイボウズ社とのNDAにより開示。	–	–
		(3)	建物、部屋に対する不正な物理的な侵入を抑止するため、侵入検知装置を導入すること。	「入室制限エリア」は、IC 又は生体認証によって自動的に施錠監視されています。また監視カメラを用いて入退室を管理しております。 cybozu.com のサーバーを管理しているデータセンターは、高度なファシリティ要件が求められる金融機関向けの「FISC安全対策設備基準」を満たしています。また、日本データセンター協会が制定しているデータセンターファシリティスタンダードでほぼ全ての項目でティア4を満たしております。	適合可能	文献[05]にて、運用メンバーは一般社員と分離された執務スペースで業務を行い、運用メンバーの執務スペースは監視カメラで入退出を管理していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[05]	–	–	詳細はサイボウズ社とのNDAにより開示。	–
		(4)	自然災害、人的災害による損傷を避けるため、建物自体の防災対策を適切に実施すること。		適合可能	文献[07]にて、災害発生時の影響を最小化するべく、電源・回線・ネットワークを冗長化していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[07]	–	詳細はサイボウズ社とのNDAにより開示。	–	–
	2.5.2.医療情報処理施設への入退館、入退室等に関する要求事項	(1)	情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合 ・医療情報システムを設置、医療情報を保管する部屋の出入りを制限するため、有人の受付、機械式の認証装置のいずれか、あるいは双方を設置して、入退館及び入退室者の確実な認証を行うこと。	データセンタについて、有人受付を設置しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
			・有人受付を置かずに機械式の認証装置により入退室者を管理する場合には、生体認証を一つ以上含む複数要素を利用した認証装置を利用すること。	データセンタについて、有人受付を設置しております。	対象外	詳細はサイボウズ社とのNDAにより開示。	–	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
			・有人受付、機械式入退管理のいずれの場合も認証履歴を取得し、定期的に履歴を検証して、不審な活動が無いことを確認すること（履歴の保全については「2.6.12.ログの取得及び監査」を参照）。	データセンタ入館は特定業務に従事する社員に限定しており、採用・異動・退職のタイミングにデータセンターの入館アクセス権の見直しを実施しており、不審な活動が発生しない運用としております。 認証履歴の定期検証は対応検討段階です。	未適合	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
			・情報処理事業者の専有する領域での職務中においては、職員の顔写真を券面に記録した情報処理事業者の職員証を外部から目視で確認できる状態で携帯することを義務付け、情報処理事業者の職員で無い者が領域内に立ち入っていた場合に識別できるようにしておくこと。	顔写真付の職員証を目視できるよう携帯することを規則にて定めております。また職員ではないと識別した場合には、声掛けなど身分確認を行っております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
			・情報処理事業者の職員は、情報処理事業者の専有する領域にて、情報処理事業者の職員で無い者を識別した際には声掛け等を行い、身分を確認すること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
			・職員証を紛失あるいは不正利用された疑いを持った際には、ただちに管理者に連絡する、情報処理事業者の職員の退職時には確実に職員証を回収・廃棄する等、職員証の厳密な発行及び失効管理を行うこと。	内規およびシステムにおいて、職員証の紛失時の連絡、執務室内の滞在時間の制限を定めています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
			・情報処理事業者の職員の業務に応じて執務室内に滞在できる時間を指定すること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
			・医療情報処理施設内への業務遂行に関係のない個人的所有物の持ち込みを認めないこと。	データセンターには通信可能な電子機器の持ち込みが制限されております。 また「入室制限エリア」には、業務遂行に関係のない個人所有物の利用が禁止されています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
		(2)	外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合 ・データセンターを運営する外部事業者が、(1)と同等な安全管理策を実施する等、情報処理事業者の管理外にある者の物理的な不正操作に対する十分な安全性が確保されていることを確認すること。	cybozu.com は、本項目の運用に該当します。データセンターを運営する外部業者が安全管理策を実施しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
			・医療情報システムの設置されるサーバラックには施錠を行い、定められた情報処理事業者の職員以外が鍵を扱わないよう、確実な鍵管理を行うこと。	データセンターのラックは施錠および鍵管理をデータセンター事業者に依頼しております。施錠を含めた鍵の利用はデータセンター事業者にて記録が取られています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
			・情報処理事業者が医療情報システムの設置されるサーバラックを解錠して行う作業については、作業者、作業開始時刻、作業終了時刻、作業内容等について記録すること。	システムの運用担当者の作業についてはすべて記録を残しております。また作業を実施する際には変更管理に則り、作業内容について責任者の承認を得てから実施しております。 下記ドキュメントもご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、システムの運用担当者の作業はすべて記録を残していることを確認した。	公開文書	文献[01]	–	–	–	–
			・データセンターを運営する外部事業者がサーバラックを解錠して作業を行う場合には、事前連絡を原則とし、医療情報システム、医療情報に影響を与えないことを確認すること。	データセンターを運営する外部事業者がラックを解錠して作業を実施する場合は、サイボウズに事前連絡をいただいています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
			・医療情報システムであることが、同じデータセンター内に立ち入る他事業者にわからないよう、扱う情報の種類、システムの機能等が識別できるような情報を外部から見える状態にしないこと。	ラック内に格納されている情報は、目視で確認できないよう管理されています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
		(3)	外部事業者の運営するサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合 ・サーバ環境を運営する外部事業者が、(１)及び(２)と同等な安全管理策を実施する等、情報処理事業者の管理外にある者の不正なアクセスに対する十分な安全性が確保されていることを確認すること。	対象外	対象外	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
	2.5.3.情報処理装置のセキュリティ	(1)	不正な装置を識別するため、医療情報システム内で利用する情報処理装置を登録したリストを作成・維持すること。	サイボウズでは、情報資産台帳をISMSにおいて定期的に見直し・更新しています。 下記ドキュメントもご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]により、サイボウズでは、情報資産台帳をISMSにおいて定期的に見直し・更新していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らの端末やネットワーク機器で使用する情報処理装置のリストの作成・維持を適切に行う必要がある。
		(2)	医療情報システムに用いる装置には、必要のないアプリケーション等をインストールしないこと。	不要なアプリケーションのインストールを制限しています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、自らの端末やネットワーク機器に必要のないアプリケーション等をインストールしないように権限管理やルールの設定を行う必要がある。
		(3)	医療情報等が表示される端末画面等をアクセス権限の無いものが閲覧することが無い様に室内の機器レイアウトを行うこと。このようなレイアウトが難しい場合には、端末画面に覗き見防止用フィルターを設置する等の対策を行うこと。	利用者様にて適切に実施いただく必要があります。	対象外	文献[06]にて、お客様がcybozu.comに登録・入力・保存した「入力データ」はサイボウズで権利を取得しないこととしているため、対象外である。	公開文書	文献[06]	–	–	–	利用者およびSI事業者は、cybozu.comに接続する端末を、アクセス権限の無いものが閲覧することが無い様に室内の機器レイアウトを行う必要がある。このようなレイアウトが難しい場合には、端末画面に覗き見防止用フィルターを設置する等の対策を行う必要がある。
		(4)	医療情報はサーバ機器のみに保存し、表示のための一時的な保存等を除き、端末上に保存されることがないようにすること。	利用者様にて適切に実施いただく必要があります。	対象外	cybozu.com利用者の端末に関する内容であるため、対象外である。	–	–	–	–	–	利用者およびSI事業者は、医療情報データが自らの端末上に保存されないように措置を講じる必要がある。
		(5)	火災発生時の消火設備が機器に損傷を与えないよう配慮すること。	ガス系の消火設備を整備しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
		(6)	医療情報システムを配置する室内での喫煙、飲食を禁止すること。	データセンターでは、喫煙および飲食は禁止されております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
		(7)	医療情報システムを配置する室内に可燃物及び液体を置く場合には、装置との間に十分な距離を保ち、専用の収納設備を設ける等、装置に悪影響を及ぼさないよう配慮すること。	データセンターでは、可燃物および液体の持ち込みは禁止されております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
		(8)	それぞれの装置は製造元又は供給元が指定する間隔及び仕様に従って保守点検を行い、必要であれば交換を行うこと。	情報処理装置は定期的に点検いたしております	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応						SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(9)	保守点検で障害不良等が発見された際の対応作業等を行う際には情報処理事業者の管理する領域にて行うこととし、外部に持ち出すことが無いようにすること。必要により外部に持ち出しての作業が必要な場合には、装置内の電磁的記録を確実に消去してから持ち出すこと。記憶装置等、障害により情報の消去が不可能となっている装置については、補修ではなく物理的な破壊を行ってから廃棄を選択すること。	HDDの保守および破棄（物理破壊）はデータセンター内で実施しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
		(10)	医療情報システムを設置するサーバラックについては、以下の安全管理策を実施すること。 ・震災時に転倒することが無いよう確実に設置すること。	データセンターはFISCの設備基準を満たし、JDCCのデータセンターファシリティスタンダードでほぼ全ての項目でティア4を満たしています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
			・熱による障害を防ぐため十分な空調設備を保有し、サーバラック内が十分に換気されていること。	空調設備を冗長化し、十分に換気しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
			・扉には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮すること。	データセンターのラックは施錠および鍵管理をデータセンター事業者に依頼しております。施錠を含めた鍵の利用はデータセンター事業者にて記録が取られています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
		(11)	起動パスワードを設定しても合理的に運用が可能な情報処理装置に対しては起動パスワードを設定すること。設定されるパスワードの品質、管理については「2.6.14.作業者アクセス及び作業者ＩＤの管理」に従うこと。	情報処理装置に対しては起動パスワードを設定しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、自らの端末の起動について、パスワードを適切に管理する必要がある。
		(12)	情報処理装置の障害発生時においても業務を継続できるよう、代替機器の準備、冗長化、バックアップ施設の設置等の対策を実施すること。	お客様データを守るためのバックアップ体制については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/data_loss/index.html また災害対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/disaster_control/index.html	適合可能	文献[06]にて、お客様のデータを管理するストレージサーバを構成するハードディスクはRAID-6を採用しており冗長化されていることを確認した。 文献[06]にて、バックアップ専用のストレージサーバも用意されており、日次でバックアップを取得していることを確認した。 文献[07]にて、災害発生時の影響を最小化するべく、電源・回線・ネットワークを冗長化していることを確認した。	公開文書	文献[06] 文献[07]	–	–	–	–
		(13)	不正な情報処理装置がネットワークに接続されることの悪影響を避けるため、登録されたネットワークアドレスとの整合性、悪意のあるプログラムに未感染であること、脆弱性パッチが適用されていること等を接続前に検査を行う仕組みを整備運用すること	脆弱性に対する対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html 弊社従業員の端末については、ウイルス対策ソフトなどのシステム的な対策を導入しております。また PC の管理方法などを定めた遵守事項を策定し、定期的なセキュリティ教育を行うことで、管理面での対策を行っております。	適合可能	文献[01]にて、技術的脆弱性に関する情報を定期的に収集し、定期的にクライアントPCおよびcybozu.comのアプリケーション、オペレーションシステム、サーバー、ネットワーク機器にパッチを適用していることを確認した。 文献[01]にて、クライアントPCでは利用者の遵守事項（ウイルス対策等）を定め、遵守していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らの端末やネットワーク機器について、ネットワークに不正な装置が接続されないように対策を講じる必要がある。
	2.5.4.情報処理装置の廃棄及び再利用に関する要求事項	(1)	ハードディスク等を医療情報システム内の別の機器で再利用する場合には、再利用前に、複数回のデータ書き込みによる元データの消去等の確実な方法でデータを消去し、再利用前に情報が消去されていることを確認すること。	ハードディスクの再利用を、システム内の別の機器で再利用することは行っておりません。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comに接続する端末を、一時的に外部からレンタルして調達するような場合は、確実な方法でデータを消去する必要がある。
		(2)	サーバ等のＢＩＯＳパスワード、ハードディスクパスワード等のハードウェアに対するパスワードを設定している場合には、それらを消去すること。	データ暗号化と論理削除による安全策を実施しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
		(3)	ハードディスクを機器に接続する際には、再利用であるかどうかに関わらず、検証用の機器で不正なプログラム等が記録されていないことを検証すること。	プログラム動作の制限を実施しています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comに接続する端末でリムーバブルハードディスクを利用する場合、不正なプログラム等が記録されていないことを検証する必要がある。

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応						SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(4)	ハードディスクの廃棄については、再利用及びデータの読み出しが不可能となるよう、複数回のデータ書き込みによる元データの消去、強磁気によるデータ消去措置、物理的な破壊措置（高温による融解、裁断等）等を適用し、当該装置に実施した措置の概要の記録（対象機器の形式、管理番号、作業担当者、作業実施日時、作業内容等）について、医療機関等の求めに応じ、速やかに提出できるよう整備すること。	外部事業者に委託してハードディスクの廃棄を実施し、廃棄記録については証明書を作成し、サイボウズにおいて保管しています。	適合可能	文献[07]にて、cybozu.comで利用していたハードディスクが不要になった場合は物理的に破壊して廃棄するなど、情報漏えい対策を含めた徹底した情報管理を行っていることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[07]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comに接続する端末を、一時的に外部からレンタルして調達するような場合は、確実な方法でデータを消去する必要がある。
	2.5.5.情報処理装置の外部への持ち出しに関する要求事項		利用中の情報処理装置を外部に持ち出す行為は原則として禁止するが、製造元でのみ可能な補修が必要な場合など、止むを得ない事情により外部への持ち出しを行う場合には、以下の管理策を適用すること。	クライアントPCの外部持ち出しは原則として禁止されています。 持ち出す場合には、複数の条件を満たす必要があります。	適合可能	以下（1）（2）にて適合可能であることを確認済。	–	–	–	–	–	–
		(1)	情報処理装置が設置されている室内及び情報処理事業者の管理する領域から持ち出す場合に備え、適切な持ち出し手順を策定すること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comに接続する端末の持ち出し・再設置に関して適切な手順を策定する必要がある。
		(2)	持ち出した機器を再度設置するための適切な検証手順を策定すること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、cybozu.comに接続する端末の持ち出し・再設置に関して適切な手順を策定する必要がある。
2.6.技術的安全対策	2.6.1.情報処理装置及びソフトウェアの保守	(1)	保守に伴う情報処理装置及びソフトウェアの変更がもたらす影響の評価を行うこと。	ソフトウェアの変更管理プロセスを定め、事前に変更による提供調査を実施しております。また、事前にバックアップを取得し、切り戻しを行うことが可能としております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、cybozu.comのホームページで提示された情報を元に、自らの医療情報システムへの影響有無を検討する必要がある。
		(2)	変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため、影響を最小限に抑える方策を検討すること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comのホームページで提示された情報を元に、安全なデータの保存を保証するため、自らの医療情報システムへの影響を最小限に抑える方策を検討する必要がある。
		(3)	医療情報を保存・交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する間、以前のデータ形式、プロトコルの利用をサポートすること。	データ形式・プロトコルのサポートについては、サービスのサポートポリシーとして文書化し、ポリシーに従ってサポート期間を定めております。また、利用ブラウザのサポートポリシーについても同様に定めております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、サイボウズから提示するデータ形式やプロトコルのサポート情報に従い、自らの端末やネットワークを適切に変更する必要がある。
		(4)	情報処理装置及びソフトウェアの保守作業については、情報処理業務の停止時間を最小限に留めるように計画を立てて実施すること。	日本時間の毎月第2日曜日午前1時~7時は定期メンテナンスのため利用ができなくなります。メンテナンスについては、2週間前を目処に以下のウェブページにて公開しています。 https://cs.cybozu.co.jp/maintenance/ またソフトウェアの変更管理プロセスを定め、事前に変更による提供調査を実施しております。また、事前にバックアップを取得し、切り戻しを行うことが可能としております。	適合可能	文献[13]にて、保守作業はcybozu.comへログインした後のトップページおよびサイボウズHPで適時開示していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[13]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、自らの端末の保守作業については、情報処理業務の停止時間を最小限に留めるように計画を立てて実施する必要がある。
		(5)	情報処理装置及びソフトウェアの適切な変更手順を策定すること。保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受けること。		適合可能	文献[13]にて、保守作業はcybozu.com利用者に極力早めに開示されていることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[13]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らの端末やアプリケーション等の保守を適切に実施する必要がある。
		(6)	不正な改ざんを受けていないことを検証するため、定期的にソフトウェアの整合性検査（改ざん検知）を実施すること。	脆弱性に対する対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html 人為的なミスによるトラブルへの対策について、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/human_error/index.html 改ざん検知の対策として、侵入検知・防止システムを備えています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	ー	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、自らの端末が不正の改ざんを受けていないことを検証するため、定期的にソフトウェアの整合性検査（改ざん検知）を実施する必要がある。

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(7)	医療情報システムに関連する技術的脆弱性については台帳等を利用して管理すること。	脆弱性に対する対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html	適合可能	文献[01]にて、定期的に第三者機関から脆弱性監査を受けており、また、脆弱性を報告いただいた方に報奨金を支払う「脆弱性報奨金制度」を運営することでより多くの外部の目でcybozu.comの脆弱性をチェックできていることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、構築する医療情報システムの技術的脆弱性について台帳等で管理する必要がある。
		(8)	潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定すること。		適合可能	文献[01]にて、技術的脆弱性に関する情報を定期的に収集し、定期的にクライアントPCおよびcybozu.comのアプリケーション、オペレーションシステム、サーバー、ネットワーク機器にパッチを適用していることを確認した。	公開文書	文献[01]	–	–	–	利用者およびSI事業者は、自らの端末に脆弱性が特定された場合には、リスク分析を行った上で必要な措置（windows update等）を実施する必要がある。
		(9)	修正パッチの適用前にパッチが改ざんされていないこと及び有効性を検証すること。	修正パッチは本番環境適用前に必ず開発環境に適用してテストを実施することが、変更管理規定にて定められております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らの端末に修正パッチを適用する前に、パッチが改ざんされていないこと及び有効性を検証する必要がある。
		(10)	保守作業を外部事業者に再委託する場合には、上記要件を満たしていることを確認して選定し、「2.6.5.第三者が提供するサービスの管理」の管理策を実施すること。選定した外部事業者について医療機関等に報告し、合意を得ること。	サイボウズ社員以外が関与することはないため、対象外。	対象外	上記(1)～(9)に関連する保守は、外部委託していないため、対象外である。 詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者は、医療情報システムの保守作業を外部事業者に再委託する場合は、外部事業者の選定及び医療機関への報告を適切に行う必要がある。
	2.6.2.開発施設、試験施設と運用施設の分離	(1)	情報処理に供するアプリケーションについては、情報処理事業者自身で開発したアプリケーションを用いること。外部開発事業者が開発したアプリケーションを用いる場合には、事前に安全性を十分に検証した上で用いること。	cybozu.com のアプリケーションに関しては、全てサイボウズで開発しております。 脆弱性に対する対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html	適合可能	文献[01]にて、cybozu.com にて提供する各サービスは、年間少なくとも１回、第三者機関に脆弱性監査を実施しており、脆弱性の監査結果をサイボウズHPで公開していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、医療情報システムを用いる場合は、事前に安全性を十分検証する必要がある。
		(2)	ソフトウェア開発を行う際には、ソフトウェア障害の影響を避けるため、運用施設とは直接に接続されていない開発用の情報処理施設（以下、「開発施設」という。）を用いて行うこと。	脆弱性に対する対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html 人為的なミスによるトラブルへの対策について、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/human_error/index.html	適合可能	文献[05]にて、運用環境と開発環境を分離しており、運用環境は一般社員はもちろん開発者もアクセスできないことを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[05]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、構築する環境について、開発環境と運用環境を分けて管理する必要がある。
		(3)	開発施設では、悪意のあるコードが混入することを避けるため、不特定多数が利用するネットワーク（インターネット等）と接続を持つ場合には「2.6.3.悪意のあるコードに対する管理策」に従うこと。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、構築する環境について、開発環境と運用環境を分けて管理する必要がある。
		(4)	不正なソフトウェアの書き換えリスクを避けるため、開発したソフトウェアを運用施設に導入する際、ソフトウェアに対する改ざん防止、検知策を実施すること。	人為的なミスによるトラブルへの対策について、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/human_error/index.html 変更管理規定を定め、ソフトウェアに対する改ざん防止、検知策を実施しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、構築する医療情報システムの変更時は、変更プログラムの改ざん防止、検知策を実施する必要がある。
		(5)	運用施設に保存されている医療情報を開発施設及び試験施設にコピーしないこと。	個人情報を含む運用データを試験に利用してはならない旨、規定にて定めております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、構築する環境について、開発環境と運用環境を分けて管理し、開発環境には医療情報をコピーしないようにする。
		(6)	医療情報を開発及び試験用データとして直接、利用しないこと。利用する場合には、個人情報の消去及び元のデータを復元できないように一部データのランダムデータとの入れ替え等のデータ操作を定め、十分な安全性が保証されていることを医療機関に示し、了解を得た上で利用すること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、構築する環境について、開発環境と運用環境を分けて管理し、開発環境には医療情報をコピーしないようにする。
	2.6.3.悪意のあるコードに対する管理策	(1)	最新の脅威についての情報収集に努め、導入している悪意のあるコード対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認すること。対応すべき脅威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）等がある。	脆弱性に対する対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html	適合可能	文献[01]にて、技術的脆弱性に関する情報を定期的に収集し、定期的にクライアントPCおよびcybozu.comのアプリケーション、オペレーションシステム、サーバー、ネットワーク機器にパッチを適用していることを確認した。 また同文献にて、クライアントPCでは利用者の遵守事項（ウイルス対策等）を定め、遵守していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、最新の脅威についての情報収集に努め、自らの端末やネットワーク機器での対策漏れがないことを確認する必要がある。

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(2)	悪意のあるコード対策ソフトウェアにおいて次の設定が行われていること。 ・リアルタイムスキャン（ディスク書き出し・読み込み、ネットワーク通信） ・リスク評価の結果として必要であれば定期的にスキャンを実施 ・電子媒体へのデータ書き出し・読み込み時におけるオンデマンドスキャン ・定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新 ・管理者以外による設定変更やアンインストールの禁止	サイボウズ社内の運用体制については、下記ウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、自らの端末やネットワーク機器にセキュリティ対策を適切に行う必要がある。
		(3)	一定期間、悪意のあるコードのチェックが行われていない場合や定義ファイル、スキャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止又は隔離措置をとるといった対策が行われていること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、自らの端末やネットワーク機器にセキュリティ対策を適切に行う必要がある。
	2.6.4.ウェブブラウザを使用する際の要求事項		医療情報システム内で必要とする、ネットワーク監視ソフトウェア、サーバ制御ソフトウェア等でユーザインタフェースとしてウェブブラウザを使用する場合は、以下の要求事項を満足する体制を確立すること。	利用者様にて適切に実施いただく必要があります。	対象外	cybozu.comは、ネットワーク監視ソフトウェア・サーバ制御ソフトウェア等ではないため、対象外である。	–	–	–	–	–	利用者およびSI事業者は、自らの端末やネットワーク機器にセキュリティ対策を適切に行う必要がある。
		(1)	ウェブブラウザの接続するサーバを業務上必要なサーバに限定すること。	利用者様にて適切に実施いただく必要があります。	対象外	cybozu.comは、ネットワーク監視ソフトウェア・サーバ制御ソフトウェア等ではないため、対象外である。	–	–	–	–	–	利用者およびSI事業者は、自らの端末やネットワーク機器にセキュリティ対策を適切に行う必要がある。
		(2)	ウェブブラウザの設定で、認可していないサイトから、ActiveX、Java アプレット、Flash 等のコードをダウンロード及び実行することができない設定になっていること（管理ソフトウェアが実行されるサーバのみを認可する。）。	利用者様にて適切に実施いただく必要があります。	対象外	cybozu.comは、ネットワーク監視ソフトウェア・サーバ制御ソフトウェア等ではないため、対象外である。	–	–	–	–	–	利用者およびSI事業者は、自らの端末やネットワーク機器にセキュリティ対策を適切に行う必要がある。
		(3)	認可したサイトからダウンロードされるコードについても「2.6.3.悪意のあるコードに対する管理策」に即して検査されること。	利用者様にて適切に実施いただく必要があります。	対象外	cybozu.comは、ネットワーク監視ソフトウェア・サーバ制御ソフトウェア等ではないため、対象外である。	–	–	–	–	–	利用者およびSI事業者は、自らの端末やネットワーク機器にセキュリティ対策を適切に行う必要がある。
	2.6.5.第三者が提供するサービスの管理		医療情報システムが設置される領域において、有人監視、機械監視、保守点検作業、清掃作業等については、外部の事業者に作業依頼をすることが考えられる。このような第三者が提供するサービスの利用に関して、以下の管理策を実施すること。	データセンター保守業務について、外注いたしております。 以下、データセンター事業者の運営について回答します。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
		(1)	第三者により提供されるサービスの安全管理策及びサービスレベルが十分であることを確認すること。	データセンターの安全管理対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/disaster_control/index.html より詳細な事項については、以下のコンテンツをご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者は、cybozu.comに入力する情報の重要度に応じて、cybozu.comで提供されるサービスレベルが十分であることを確認する必要がある。
		(2)	サービスの実施、運用、維持について定期的に検証すること。	ISMS 認証更新手続きの中で、定期的に実地調査を行っております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者は、cybozu.comのサービス実施、運用、維持について定期的に検証する必要がある。
		(3)	サービス実施について事前、事後報告を義務づけ、報告内容を点検確認すること。	データセンター事業者のサービス実施については、オンライン上で依頼し、実施の履歴を残しています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者は、サイボウズが報告したcybozu.comのサービス実施記録を照会し確認する必要がある。
		(4)	サービスを実施する人員は予め届け出を行い、サービス実施時に不正な人員を受入れないこと。	不正な人員の受け入れを防ぐべく、責任者の承認を受けた人員のみが入館できるようにしています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
		(5)	サービス実施中に第三者が管理区域に立ち入る場合は顔写真を券面に入れた身分証明を携帯すること。	データセンターでは、第三者は身分証に基づき発行されたセキュリティカードを携帯しています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
		(6)	サービス実施にともなう処理施設内への立ち入り手順に関しては、情報処理事業者の職員の入室、退室手順に準ずること。	データセンターの立ち入りは、データセンターのセキュリティ施策に基づく手順に準じます。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(7)	サービスの変更時には、引き続き安全性が維持されていることについて適切な検証を行うこと。	第三者が提供するサービスについては、社内でサービスレベルが低下しないように管理・検証し、議論・承認の履歴を残しています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、構築する医療情報システムの変更時に対策が維持されていることを検証する必要がある。
		(8)	医療情報システムの保守点検作業を外部事業者に委託する場合には、「医療情報システムの安全管理に関するガイドライン第４．１版（厚生労働省、平成２２年２月）」６．８章Ｃ項の管理策を実施すること。	サイボウズ社員以外が関与することはないため、対象外。	対象外	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	–
	2.6.6.ネットワークセキュリティ管理	(1)	セキュリティゲートウェイ（ネットワーク境界に設置したファイアウォール、ルータ等）を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行うこと。ホスティング利用時等、ネットワーク境界にセキュリティゲートウェイを設置できない場合は、個々の情報処理装置（サーバ）にて、同様のアクセス制御を行うこと。	接続先を限定する方法として、IP アドレス制限やクライアント証明書を用いた認証（セキュアアクセス）を提供しております。 詳細は以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/illegal_access/index.html	適合可能	文献[01]にて、cybozu.comではIPアドレス制限、BASIC認証、クライアント証明書認証の機能を提供していることを確認した。 文献[03]にて、cybozu.comにアクセスできるIPアドレスを限定する機能が提供されていることを確認した。 文献[03]にて、cybozu.comにアクセスするためのBasic認証用のユーザ名・パスワードの入力した上で、cybozu.comへのログイン名・パスワードを入力することで二重でアクセス制限を実施するための機能を提供していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01] 文献[03]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、構築する医療情報システムに関し、不正侵入を防止するため、適切にネットワークACLを設定する必要がある。また、ファイアウォールによる通信の送受信の確認や、WAFによるWebアプリケーションの保護など、必要性に応じて判断し構成する必要がある。
		(2)	セキュリティゲートウェイでは、不正なＩＰアドレスを持つトラフィックが通過できないように設定すること（接続機器類のＩＰアドレスをプライベートアドレスとして設定して、ファイアウォール、ＶＰＮ装置等のセキュリティゲートウェイを通過しようとするトラフィックをＩＰアドレスベースで制御する等。）。		適合可能	文献[01]にて、cybozu.comではIPアドレス制限、BASIC認証、クライアント証明書認証の機能を提供していることを確認した。 文献[03]にて、アクセスできるIPアドレスを限定していること、クライアント証明書によって接続元を認証するセキュアアクセスの機能を提供していることを確認した。	公開文書	文献[01] 文献[03]	–	–	–	
		(3)	ルータ等のネットワーク機器は、安全性が確認できる機器を利用すること。	機材調達は、関係者が調達要件ごとに安全性の定義を行い、社内レビューを行い、要件を満たしたことを確認して発注するプロセスとなっています。発注に至る過去の議論の履歴はすべて記録されており、あらたに調達する際の参考情報として活用されています。	未適合	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	
		(4)	ネットワーク機器及びサーバ、端末の利用していないネットワークポートへの物理的な接続を制限すること。	サイボウズ社内の運用体制については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	
		(5)	医療機関等との接続ネットワーク境界には侵入検知システム（以下、「ＩＤＳ」という。）及び侵入防止システム（以下、「ＩＰＳ」という。）を導入してネットワーク上の不正なイベントの検出、あるいは不正なトラフィックの遮断を行うこと。ホスティング利用時等、ネットワーク境界に装置を設置できない場合は、個々の情報処理装置にて、同様の制御を行うこと。	各ホストに HIDS を導入しております。	適合可能	文献[08]にて、自動侵入検知・防止システムを備えていることを確認した。	公開文書	文献[08]	–	–	–	
		(6)	侵入検知システム等が、常に最新の攻撃・不正アクセスに対応可能なように、シグネチャ・検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行うこと。	脆弱性に対する対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html 下記ドキュメントもご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、技術的脆弱性に関する情報を定期的に収集し、定期的にクライアントPCおよびcybozu.comのアプリケーション、オペレーションシステム、サーバー、ネットワーク機器にパッチを適用していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	–	詳細はサイボウズ社とのNDAにより開示。	
		(7)	侵入検知システム等が、緊急度の高い攻撃・不正アクセス行為を検知した際は、監視端末への出力や電子メール等を用いて直ちに管理者に通知する設定にしていること。	各ホストに HIDS を導入し、ログを保管しております。 侵入検知システムで攻撃を検知した場合、運用管理区画のモニタに表示、運用管理者へメール通知しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	
		(8)	侵入検知の記録には不正アクセス等の事後処理に必要な項目が含まれていること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応						SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(9)	医療情報システムにおいて、インターネット等のオープンネットワーク上のサービスとの接続について、以下にあげるサービスとの接続に限定すること。他に必要なサービスがある場合には、医療機関等の合意を得てから利用すること。 ・外部からの医療情報システムの稼働監視・遠隔保守 ・セキュリティ対策ソフトウェアの最新パターンファイル等のダウンロード ・オペレーティングシステム及び利用アプリケーションのセキュリティパッチファイル等のダウンロード ・電子署名時の時刻認証局へのアクセス、電子署名検証における失効リスト等認証局へのアクセス ・ファイアウォール、ＩＤＳ・ＩＰＳなどのセキュリティ機器に対する不正アクセス監視 ・時刻同期のための時刻配信サーバへのアクセス ・これらのサービスを利用するために必要なインターネットサービス（ドメインネームサーバへのアクセス等） ・その他の医療情報システムの稼動に必要なサービス（外部認証サーバ、外部医療情報データベース等）	接続先を限定する方法として、IP アドレス制限やクライアント証明書を用いた認証（セキュアアクセス）を提供しております。 詳細は以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/illegal_access/index.html サイボウズ社内の運用体制については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html データセンターと接続する回線には、Qualys SSL Labs スコアで高ランクを維持するよう、日々暗号化方式を見直しています。	適合可能	文献[01]にて、cybozu.comではIPアドレス制限、BASIC認証、クライアント証明書認証を提供していることを確認した。 文献[03]にて、cybozu.comにアクセスできるIPアドレスを限定していることを確認した。 文献[05]にて、運用環境には運用メンバーしかアクセスできない（一般社員および開発者はアクセス不可）ことを確認した。 文献[07]にて、データセンターと接続する回線には、Qualys SSL Labs スコアで高ランクを維持するよう日々暗号化方式を見直していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01] 文献[03] 文献[05] 文献[07]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者は、cybozu.comへのインターネット接続に関するポリシーや構成等を検討し、適切に実装する必要がある。
		(10)	医療情報システムのサーバ機器等への同時ログオンユーザ数（ＯＳアカウント等）に適切な上限を設けること。	cybozu.com 運用環境には、弊社内のオフィスネットワークとは論理的に隔離された、専用のオペレーション端末からのみ接続可能としています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者は、cybozu.comへの同時アクセスユーザ数を適切に設定する必要がある。
		(11)	ネットワーク接続のログ（認証ログ及び接続ログ）を記録すること。	利用者の活動および、セキュリティ事象は監査ログを取得し、 ユーザが閲覧できるようにしています。 運営環境の接続ログについても保管しております。	適合可能	文献[01]にて、利用者の活動、例外処理およびセキュリティ事象を記録した監査ログを取得し、日次でログの確認を実施していることを確認した。	公開文書	文献[01]	–	–	–	利用者は、サイボウズから提供されるcybozu.comの監査ログを定期的に検証し不審な活動が行われていないことを検証する必要がある。
		(12)	ネットワーク接続ログを定期的に検証し不審な活動が行われていないことを検証すること。	運用環境の接続ログについては、長時間ログインしているアカウントを監視しています。規定時間を超えるアカウントについては、上長が長時間ログインの理由を確認する運用としています。	適合可能	文献[01]にて、利用者の活動、例外処理およびセキュリティ事象を記録した監査ログを取得し、日次でログの確認を実施していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者は、サイボウズから提供されるcybozu.comの監査ログを定期的に検証し不審な活動が行われていないことを検証する必要がある。
		(13)	2.6.1	cybozu.com 運用環境では、無線ネットワークは利用していません。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、cybozu.comへの接続時に無線ネットワークLANを使用しない。
		(14)	ＶＰＮ接続を行う場合には以下の事項に従うこと。 ・接続時にＶＰＮ装置間で相互に認証を行うこと。	クライアント証明書を用いた認証（セキュアアクセス）を提供しております。詳細は以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/illegal_access/index.html cybozu.com 運用環境にアクセスする際にはVPN網を利用し、またアクセスが許可されていない者がアクセス、ログオンできないように制御しております。	適合可能	文献[01]にて、システムにアクセスする際にはVPN網を利用し、さらにアクセスが許可されていない者がアクセス、ログオンできないように制御していることを確認した。 文献[03]にて、cybozu.com接続時には、クライアント証明書によるセキュアアクセスの機能があることを確認した。	公開文書	文献[01] 文献[03]	–	–	–	利用者およびSI事業者は、VPNを使用する場合は、VPNの構成や使用する暗号鍵、自らのネットワーク機器等を適切に管理する必要がある。
			・傍受、リプレイ等のリスクを最小限に抑えるために、「2.6.11.暗号による管理策」に従い、適切な暗号技術を利用すること。	データセンターとオフィス間の通信は専用線を用いており、通信内容は暗号化いたしております。暗号化方式は、Qualys SSL Labs スコアで高ランクを維持するよう日々見直しております。	適合可能	文献[07]にて、データセンターと接続する回線には、Qualys SSL Labs スコアで高ランクを維持するよう日々暗号化方式を見直していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[07]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、VPNを使用する場合は、VPNの構成や使用する暗号鍵、自らのネットワーク機器等を適切に管理する必要がある。
			・インターネット上のトラフィックがＶＰＮチャンネルに混入しないように、プライベートネットワークインタフェースとインターネットインタフェースの間に直接の経路を設定しないこと。	利用者様にて適切に実施いただく必要があります。	対象外	医療機関に対する要求事項のため、対象外。	–	–	–	–	–	利用者およびSI事業者は、VPNを使用する場合は、VPNの構成や使用する暗号鍵、自らのネットワーク機器等を適切に管理する必要がある。
			・複数の医療機関等から情報処理業務を受託している場合には、医療機関等の間で情報が混同するリスクを避けるためＶＰＮチャンネルを医療機関等別に構築する等の対策を実施すること。	cybozu.com 運用環境のアカウントは各個人に一意の識別子を付与しています。運用環境にアクセスする際は、VPN網を利用し、アクセスが許可されていない者がアクセス、ログオンできないように制御しています。 「入力データ」については利用されている顧客以外はアクセスできないようにデータベースの分離やアクセス制限を行っています。「入力データ」の取り扱いについては、cybozu.com 利用規約をご参照ください。 https://www.cybozu.com/jp/terms/	適合可能	文献[01]には、登録されたデータについては利用されている顧客以外はアクセスできないようにデータベースの分離やアクセス制限が行われていることが記載されている。	公開文書	文献[01]	–	–	–	利用者およびSI事業者は、VPNを使用する場合は、VPNの構成や使用する暗号鍵、自らのネットワーク機器等を適切に管理する必要がある。

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
	2.6.7.電子媒体の取扱	(1)	電子媒体について情報処理事業者施設外への不要な持ち出しを行わないこと。ＣＤ、ＤＶＤ、ＭＯ等の電子媒体については、追記のできない光学メディア（ＣＤ－Ｒ、ＤＶＤＲ等）を用い、情報交換作業終了後、電子媒体を（９）に示す方式にて確実に廃棄処分すること。	電子媒体の保管・破棄などの管理方法につきましては、以下の文書をご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf 電子媒体の外部持ち出しは原則として禁止されています。 持ち出す場合には、以下の条件を満たす必要があります。 - 電子媒体が暗号化されていること - 利用者の所属する部長の許可を得ていること また、電子媒体を破棄する際には、物理的破壊もしくは、完全消去を行っています。	適合可能	文献[01]にて、電子媒体の情報取扱方法（保管、破棄）は情報セキュリティ規則に定めて適切に扱っていることを確認した。 文献[07]にて、cybozu.comで利用したハードディスクが不要になった場合は、物理的に破壊して破棄することを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01] 文献[07]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らの端末で使用する電子媒体を施設外に不要に持ち出さない。電子媒体は追記のできない光学メディアを用い、使用後は確実に破棄処分する必要がある。
		(2)	情報交換目的やバックアップ目的でＭＴ、ＤＡＴ、半導体記憶装置、ハードディスク等の大容量の電子媒体を用いる場合には、その管理を厳重に行うこと。これらの電子媒体に複数回の情報記録を行う場合には、単に上書きするのではなく、確実な情報消去等の情報漏洩対策を行うこと。	大容量の記憶媒体は施錠管理し、破棄する場合には媒体を破壊しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、自らの端末で電子媒体を使用する場合は管理を厳重に行う必要がある。電子媒体に複数回の情報記録を行う場合は、確実に情報消去する等の情報漏洩対策を行う必要がある。
		(3)	電子媒体は台帳を作成して管理すること。台帳と電子媒体を定期的に検証し、盗難、紛失の発生を検証すること。台帳においては利用に関する記録を行い、電子媒体の廃棄後も一定期間にわたり記録を維持すること。	電子媒体については情報資産台帳および、ハードウェア構成管理台帳を作成し、台帳を維持・管理しております。	適合可能	文献[01]により、サイボウズでは、情報資産台帳をISMSにおいて定期的に見直し・更新していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、自らの端末で使用する電子媒体を適切に管理する必要がある。
		(4)	電子媒体を保存するキャビネット等には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮すること。	電子媒体は施錠されたキャビネット、引き出しに保管しております。施錠に用いる鍵は、最小限の人員のみが使用するように管理しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らの端末で使用する電子媒体を適切に管理する必要がある。
		(5)	電子媒体の損傷等による情報喪失のリスクを最小限にするため媒体の製造者により指定される保管環境にて保管すること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らの端末で使用する電子媒体を適切に管理する必要がある。
		(6)	製造者の定める有効利用限度期間を超過することがないよう、電子媒体の有効利用限度期間が近づいた場合は、他媒体に複写すること。	ハードウェア構成管理台帳にて有効期限を管理し、適宜機材の入れ替えを行っています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、自らの端末で使用する電子媒体を適切に管理する必要がある。
		(7)	情報を保管するためにハードディスク装置を用いる場合には、ＲＡＩＤ－１もしくはＲＡＩＤ－６相当以上のディスク障害に対する対策を取ること。	ディスク障害など、データ消失対策の詳細は、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/data_loss/index.html	適合可能	文献[06]にて、ハードディスク装置の10台（全12台）はRAID-6を採用し、残りの2台が同時に故障してもデータが消失することはないことを確認した。	公開文書	文献[06]	–	–	–	利用者およびSI事業者は、自らの端末で使用する電子媒体を適切に管理する必要がある。
		(8)	全ての電子媒体には格納される情報の機密レベルを示すラベル付けを行うこと。	「情報区分」と呼ばれる機密レベルを設定し、情報資産ごとに機密ラベルを設定しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らの端末で使用する電子媒体を適切に管理する必要がある。
		(9)	電子媒体を廃棄する場合には、物理的な破壊措置（高温による融解、裁断等）を適用し、情報の読み出しが不可能であることを確認すること。	大容量の記憶媒体は施錠管理し、破棄する場合には媒体を破壊しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自らの端末で使用する電子媒体を適切に管理する必要がある。
	2.6.8.情報交換に関するセキュリティ	(1)	医療機関等と情報処理事業者間の情報交換に関して、次の事項を予め合意しておくこと。 ・情報を電子媒体に記録して交換する際の手順 ・情報をネットワーク経由で文書ファイル形式にて交換する際の手順 ・情報をネットワーク経由でアプリケーション入力にて交換する際の手順 ・情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順	cybozu.com 上で提供される各サービスのマニュアルにて、 操作手順を整備し公開いたしております。 https://www.cybozu.com/jp/support/manual/	適合可能	文献[19]、文献[20]、文献[21]、文献[22]、文献[23]にて、サイボウズは、ファイルアップロード・ダウンロードのマニュアルを整備し、医療機関が利用できるよう公開されていることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[19] 文献[20] 文献[21] 文献[22] 文献[23]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、サイボウズから提供されるcybozu.comのマニュアルにて操作手順を確認する必要がある。

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応						SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(2)	情報交換手順では搬送の形態によらず次の事項を確実にすること。 ・発送者、受領者を識別し記録すること。	接続先を限定する方法として、IP アドレス制限やクライアント証明書を用いた認証（セキュアアクセス）を提供しております。このセキュアアクセスにNTTコミュニケーションズの提供するVPNサービスである Multi-Cloud Connect for cybozu.com を利用することが前提条件です。 詳細は以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/illegal_access/index.html https://www.ntt.com/business/services/network/vpn/vpn/op/cybozu.html	適合可能	文献[01]にて、cybozu.comではIPアドレス制限、BASIC認証、クライアント証明書認証の機能を提供していること、アクセスログの保管を行っていることを確認した。 文献[03]にて、cybozu.comにアクセスできるIPアドレスを限定する機能を提供していることを確認した。 文献[04]にて、cybozu.com利用者は、監査ログ（日時、接続元、ユーザ等の情報）を閲覧・ダウンロードすることができることを確認した。	公開文書	文献[01] 文献[03] 文献[04]	–	–	–	利用者およびSI事業者は、cybozu.comから提供される機能（セキュアアクセス）を用い、クライアント認証する必要がある。
			・発送者の行為を後に否定できないように、発送伝票の保存、文書ファイルへの電子署名付与、アプリケーションログオン時の確実な認証等、否認防止策を行うこと。	監査ログを提供しております。お客様環境にて、ID を一意に採番いただくことで、不正行為の監査に利用できます。 https://www.cybozu.com/jp/security/bad_login/index.html また cybozu.com へのアクセスログにつきましては無制限に保管し、運用管理者および、アクセスが許可された者がアクセスできる場所に保管しております。詳細は以下の文書をご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、cybozu.com利用者の活動、例外処理及びセキュリティ事象を記録した監査ログを取得し、日次で該当のログについて確認をしていることを確認した。 文献[04]にて、cybozu.com利用者は、監査ログ（日時、接続元、ユーザ等の情報）を閲覧・ダウンロードすることができることを確認した。	公開文書	文献[01] 文献[04]	–	–	–	利用者は、サイボウズから提供されるcybozu.comの監査ログを定期的に検証し不審な活動が行われていないことを検証する必要がある。
			・交換する情報の機密レベルに関して合意すること（受領側で機密レベルが低くならないこと。）。	サイボウズの情報の取り扱い方法に関する詳細につきましては、以下の文書をご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、cybozu.com 利用者がcybozu.comに登録した情報については、その情報の内容を問わず、サイボウズでは最善の注意を持って管理していることを確認した。	公開文書	文献[01]	–	–	–	利用者は、cybozu.comに入力した情報は利用者側の管理責任であり、情報の取扱を管理する必要がある。
			・交換された情報に悪意のあるコードが含まれていないことを確実とすること。	交換されうる情報（cybozu.comに対する「入力データ」）の扱いについては以下の文書をご参照ください。 https://www.cybozu.com/jp/terms/	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者は、cybozu.comに入力する情報に悪意のあるコードが含まれていないことを確実とする必要がある。
		(3)	物理的に情報を搬送する際には以下の対策を実施すること。 ・医療機関等が合意する基準にもとづいて信頼できる配送業者を選択すること。	サイボウズ社員以外が関与することはないため、対象外。	対象外	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、医療情報システムにおける物理的な情報の搬送について、適切に取り扱う必要がある。
			・配送時の作業者については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐこと。	サイボウズ社員以外が関与することはないため、対象外。	対象外	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、医療情報システムにおける物理的な情報の搬送について、適切に取り扱う必要がある。
			・配送業者等による電子媒体の抜き取り等を防ぐため、交換する電子媒体の数と種類について、予め情報交換して受領時に欠損が無いことを確認すること。	サイボウズ社員以外が関与することはないため、対象外。	対象外	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、医療情報システムにおける物理的な情報の搬送について、適切に取り扱う必要がある。
			・配送業者等による電子媒体からの情報の抜き取りを防ぐため、不正な開封を検出することのできるコンテナ等を利用すること。	サイボウズ社員以外が関与することはないため、対象外。	対象外	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、医療情報システムにおける物理的な情報の搬送について、適切に取り扱う必要がある。
			・電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さないこと。	サイボウズ社員以外が関与することはないため、対象外。	対象外	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、医療情報システムにおける物理的な情報の搬送について、適切に取り扱う必要がある。
			・電子媒体により情報を交換する場合、移送中の安全管理上のリスクがある場合には電子媒体内のデータに暗号化を施すこと。	顧客のデータをデータセンター外に持ち出す場合は、弊社規則に従って運用しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、医療情報システムにおける物理的な情報の搬送について、適切に取り扱う必要がある。
		(4)	電子的に情報を転送する際には以下の対策を実施すること。 ・送信者、受信者は相互に電子的に認証を行って相手の正当性を検証すること。認証方式は接続形態、転送に利用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。	接続先を限定する方法として、IP アドレス制限やクライアント証明書を用いた認証（セキュアアクセス）を提供しております。 詳細は以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/illegal_access/index.html	適合可能	文献[03]にて、cybozu.comでは、クライアント証明書によって接続元を認証するセキュアアクセスの機能により、相手の正当性を検証できることを確認した。	公開文書	文献[03]	–	–	–	利用者およびSI事業者は、cybozu.comから提供される機能（セキュアアクセス）を用い、クライアント認証する必要がある。
			・送受信する経路は適切な方法で傍受のリスクから保護されていること。	お客様環境と cybozu.com とのデータ通信内容は暗号化いたしております。暗号化方式は、Qualys SSL Labs スコアで高ランクを維持するよう日々見直しております。	適合可能	文献[03]にて、cybozu.comでは、クライアント証明書によって接続元を認証するセキュアアクセスの機能により、傍受のリスクから保護されていることを確認した。	公開文書	文献[03]	–	–	–	利用者およびSI事業者は、cybozu.comから提供されている機能を用い、傍受のリスクから保護する必要がある。

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応						SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
			・受信した情報について経路途中での損傷、改ざんが無いことを検証する対策を講じること。		適合可能	文献[03]にて、cybozu.comでは、クライアント証明書によって接続元を認証するセキュアアクセスの機能により、経路途中での損傷や改ざんを検証できることを確認した。	公開文書	文献[03]	–	–	–	利用者およびSI事業者は、cybozu.comから提供されている機能を用い、情報経路途中での損傷、改ざんがないことを検証する対策を講じる必要がある。
			・送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施すること。	SLO としてサービス提供時間を24時間365日と定めております。サービス提供時間帯の全てにおいて、障害検知および対応を実施いたしております。詳細につきましては、以下のウェブページをご参照ください。 https://www.cybozu.com/jp/service/slo.html	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、cybozu.comへの情報の送受信に失敗する場合は、サイボウズで提供しているサポート窓口に連絡し、必要な対応を実施する必要がある。
	2.6.9.医療情報システムに対するセキュリティ要求事項	(1)	運用システムの混乱を避けるため、開発用コード又はコンパイラ等の開発ツール類を運用システム上に置かないこと。	サイボウズ社内の運用体制については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html 本番環境には、サービス提供に不要なファイルは設置いたしておりません。ステージング環境は、本番環境とは論理的に独立した環境を構築しております。	適合可能	文献[05]にて、本番環境と開発環境を分離しており、運用環境は一般社員はもちろん開発者もアクセスできないことを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[05]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、医療情報システムの運用環境に、開発中のプログラム等を置かないよう、適切に管理する必要がある。
		(2)	情報処理に不必要なファイル等を運用システム上におかないこと。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、医療情報システムの運用環境に、不要なファイルを置かないよう、適切に管理する必要がある。
		(3)	業務に供するソフトウェア及びオペレーティングシステムソフトウェアについて、十分な試験を行った上で導入すること。	サイボウズ社内の運用体制については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、医療情報システムについて、利用者への提供前に事前に十分検証を行う必要がある。
		(4)	運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得すること。	本番環境で行われた操作については、すべて記録しております。システムの使用状況については、定期的に監視しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、医療情報システムのログ取得・確認する必要がある。
		(5)	システム運用情報（システム及びサービス設定ファイル等）の複製及び利用については監査証跡とするためにログを取得すること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者及びSI事業者は、医療情報システムのログ取得・確認する必要がある。
	2.6.10.アプリケーションに対するセキュリティ要求事項	(1)	提供するアプリケーションについては、アプリケーションの種別による特定の脆弱性検出を含む安全性診断を定期的に行い、その結果に基づいて対策を行うこと。医療機関等とのデータ送受信の際にはデータの完全性を検証する機構を導入すること。	脆弱性に対する対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html またクライアント証明書を用いた認証（セキュアアクセス）を提供しております。詳細は以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/illegal_access/index.html	適合可能	文献[01]にて、技術的脆弱性に関する情報を定期的に収集し、定期的にクライアントPCおよびcybozu.comのアプリケーション、オペレーションシステム、サーバー、ネットワーク機器にパッチを適用していることを確認した。 文献[03]にて、cybozu.com接続時には、クライアント証明書によるセキュアアクセスの機能にて相互認証することによりデータの完全性を担保していることを確認した。	公開文書	文献[01] 文献[03]	–	–	–	利用者およびSI事業者は、構築する医療情報システムの脆弱性検査を実施する必要がある。
		(2)	アプリケーション及びアプリケーション稼動に利用する第三者のソフトウェア（ライブラリ、サーバプロセス等）については、公開される最新の脆弱性情報を参照し、迅速に対応策をとること。	脆弱性に対する対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/vulnerability/index.html	適合可能	文献[01]にて、技術的脆弱性に関する情報を定期的に収集し、定期的にクライアントPCおよびcybozu.comのアプリケーション、オペレーションシステム、サーバー、ネットワーク機器にパッチを適用していることを確認した。	公開文書	文献[01]	–	–	–	利用者およびSI事業者は、構築する医療情報システムの脆弱性検査を実施する必要がある。
		(3)	アプリケーションにて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行うこと。	クライアント証明書を用いた認証（セキュアアクセス）を提供しております。詳細は以下のウェブページをご参照ください。 https://www.cybozu.com/jp/security/illegal_access/index.html 以下の文書も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、cybozu.comではIPアドレス制限、BASIC認証、クライアント証明書認証を提供していることを確認した。 文献[03]にて、アクセスできるIPアドレスを限定していることを確認した。 文献[03]にて、クライアント証明書によって接続元を認証するセキュアアクセス機能により相互認証できることを確認した。	公開文書	文献[01] 文献[03]	–	–	–	利用者およびSI事業者は、医療情報システムを利用するユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行う必要がある。
		(4)	アプリケーションにて医療事業者側の作業者を認証する情報（ＩＤ／パスワード認証の際のパスワード）は、十分な強度を持ったハッシュ関数の出力値として保存する、あるいは暗号化して保存すること。	パスワードを暗号化して保存することを、社内規定にて定めております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、医療情報システム利用者の認証情報は、十分な強度を持ったハッシュ関数の出力値として保存する、あるいは暗号化して保存する必要がある。
		(5)	アプリケーションによる情報操作については、医療機関等の職務権限に応じたアクセス管理を可能とし、正当なアクセス権限を持たないものによる情報の生成、編集、削除等を防止すること。	利用企業ごとにシステム管理権限を付与することが出来ます。 詳細は、cybozu.com 上で提供される各サービスのマニュアルにて、操作手順を整備し公開いたしております。 https://www.cybozu.com/jp/support/manual/	適合可能	文献[20]、文献[21]、文献[22]、文献[23]にて、cybozu.comの利用企業（団体）ごとに、システム管理者権限を付与でき、管理者がアクセス制御を設定できることを確認した。	公開文書	文献[20] 文献[21] 文献[22] 文献[23]	–	–	–	利用者およびSI事業者は、医療情報システム利用者は職務権限に応じたアクセス管理を実施する必要がある。

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
	2.6.11.暗号による管理策		アプリケーション及び情報処理装置で暗号を利用する場合には、以下の管理策を適用すること。	–	適合可能	以下（1）（2）（3）（4）（5）にて適合可能であることを確認済。	–	–	–	–	–	利用者およびSI事業者は、構築する医療情報システムの暗号化を適切に管理する必要がある。
		(1)	暗号アルゴリズムは十分な安全性を有するものを使用すること。選択基準としては電子政府推奨暗号リスト等を用いること。	開発責任者が集まる「Tech Lead Meeting」と呼ばれる会議体にて、採用する暗号技術を策定しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、医療情報システムで使用する暗号化アルゴリズムを適切に選択する必要がある。
		(2)	暗号鍵が漏洩した場合に備えた対応策を策定しておくこと。	暗号鍵の漏洩時の対応策を策定しています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、医療情報システムにおける暗号鍵の漏洩対策を講じる必要がある。
		(3)	電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとすること。	伝送データは全てSSL通信で暗号化しています。SSLサーバ証明書は、認証局にて発行されたものを利用しています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、必要に応じて信頼された電子証明書を使用する必要がある。
		(4)	暗号アルゴリズム及び暗号鍵の危殆化に備え、暗号アルゴリズムを切り替えることができるように配慮すること。	開発責任者が集まる「Tech Lead Meeting」と呼ばれる会議体にて、採用する暗号技術を策定しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者及びSI事業者は、医療情報システムで使用する暗号化アルゴリズムの危殆化について、対策を講じる必要がある。
		(5)	医療機関等から受け付けるデータを検証するためのルート認証機関の公開鍵証明書は安全な経路で入手し、別の経路で入手したフィンガープリントと比較して、真正性を検証すること。	利用者様にて適切に実施いただく必要があります。	対象外	文献[06]にて、cybozu.com利用者がcybozu.comに登録・入力・保存した「入力データ」はサイボウズで権利を取得しないこととしているため、データの真正性検証はcybozu.com利用者の責務となる。	公開文書	文献[06]	–	–	–	利用者及びSI事業者は、公開鍵証明書の真正性の確認を適切に実施する必要がある。
	2.6.12.ログの取得及び監査	(1)	作業者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録した監査ログを作成し管理すること。	利用者の活動、例外処理およびセキュリティ事象を記録した監査ログをcybozu.com 共通管理画面にて出力しております。 詳細は以下のウェブページで公開しております。 https://jp.cybozu.help/ja/general/admin/audit	適合可能	文献[01]にて、利用者の活動、例外処理およびセキュリティ事象を記録した監査ログ（アクセスログ、システムログ、システムエラー）を取得し、日次でログの確認を実施していることを確認した。	公開文書	文献[01]	–	–	–	利用者は、サイボウズから提供されるcybozu.comの監査ログを定期的に検証し不審な活動が行われていないことを検証する必要がある。
		(2)	監査ログを定期的に検証して不正な行為、システムの異常等を検出すること。		適合可能	文献[01]にて、利用者の活動、例外処理およびセキュリティ事象を記録した監査ログ（アクセスログ、システムログ、システムエラー）を取得し、日次でログの確認を実施していることを確認した。	公開文書	文献[01]	–	–	–	利用者は、サイボウズから提供されるcybozu.comの監査ログを定期的に検証し不審な活動が行われていないことを検証する必要がある。
		(3)	ログを利用して正確に事故原因等を検証するため、医療情報システムのすべてのサーバ機器等の時刻を時刻サーバ等の提供する標準時刻に同期しておくこと。	NTP を利用して、オペレーティングシステム、ネットワーク機器等、正確な時刻源と時刻同期しております。 以下の文書も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、NTP を利用して、オペレーティングシステム、ネットワーク機器等、正確な時刻源と時刻同期していることを確認した。	公開文書	文献[01]	–	–	–	利用者およびSI事業者は、自らの端末やネットワーク機器の時刻は信頼できる機関が提供する標準時刻に同期する必要がある。
		(4)	標準時刻に同期するための時刻提供元は信頼できる機関を利用すること。		適合可能	文献[01]にて、NTP を利用して、オペレーティングシステム、ネットワーク機器等、正確な時刻源と時刻同期していることを確認した。	公開文書	文献[01]	–	–	–	利用者およびSI事業者は、自らの端末やネットワーク機器の時刻は信頼できる機関が提供する標準時刻に同期する必要がある。
		(5)	ログ情報を不正なアクセスから適切に保護するため以下の管理策を適用すること。 ・ログデータにアクセスする作業者及び操作を制限すること。	監査ログは「cybozu.com 共通管理」の管理者のみがアクセス可能な領域に保管されます。 詳細は以下のウェブページで公開しております。 https://jp.cybozu.help/ja/general/admin/admin_common	適合可能	文献[01]にて、監査ログは、運用管理者及びアクセスが許可されたもののみがアクセスできる場所に保管してあることを確認した。 文献[01]にて、アプリケーションの監査ログの保存期間や保存形式、閲覧はアプリケーションの運用管理者での管理を定めていることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者は、サイボウズから提供されるcybozu.comの監査ログにアクセスできる作業者および操作を制限する必要がある。
			・容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとること。	アクセスログは無期限に保存しております。 クラウドサービスの利用状況の推移から容量増強・増設の計画を立て、文書化しております。 以下の文書も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、アクセスログは無期限に保存していることを確認した。 文献[01]にて、クラウドサービスの利用状況の推移から容量増強・増設の計画を立て、その内容については文書を作成していることを確認した。	公開文書	文献[01]	–	–	–	利用者及びSI事業者は、医療情報システムにおけるログ管理を適切に実施する必要がある。

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
			・ログデータに対する不正な改ざん及び削除行為に対する検出・防止策を施すこと。	監査ログは「cybozu.com 共通管理」の管理者のみがアクセス可能な領域に保管されます。 詳細は以下のウェブページで公開しております。 https://jp.cybozu.help/ja/general/admin/admin_common アプリケーションが出力するアクセスログや、エラーログはネットワーク管理責任者およびネットワーク管理者のみがアクセスできるようアクセス制御しています。	適合可能	文献[01]にて、利用者の活動、例外処理およびセキュリティ事象を記録した監査ログ（アクセスログ、システムログ、システムエラー）を取得し、日次でログの確認を実施していることを確認した。また、監査ログは、運用管理者及びアクセスが許可されたもののみがアクセスできる場所に保管してあることを確認した。	公開文書	文献[01]	–	–	–	利用者及びSI事業者は、医療情報システムにおけるログ管理を適切に実施する必要がある。
	2.6.13.アクセス制御方針	(1)	情報処理に用いる情報処理装置それぞれのセキュリティ要求事項を整理すること。	機器の運用管理の手順書を整理し、操作方法および機材の追加・変更都度で更新しております。	適合可能	文献[01]にて、アプリケーション、OS、サーバー、ネットワーク機器の運用管理の手順書を整理し、操作方法および機材の追加・変更都度で更新するルールであることを確認した。	公開文書	文献[01]	–	–	–	利用者およびSI事業者は、自らの端末やネットワーク機器に対するセキュリティ要求事項を適切に整理する必要がある。
		(2)	情報処理に用いるソフトウェアそれぞれのセキュリティ要求事項を整理すること。	同上	適合可能	文献[01]にて、アプリケーション、OS、サーバー、ネットワーク機器の運用管理の手順書を整理し、操作方法および機材の追加・変更都度で更新するルールであることを確認した。	公開文書	文献[01]	–	–	–	利用者およびSI事業者は、自らの端末やネットワーク機器に対するセキュリティ要求事項を適切に整理する必要がある。
		(3)	アクセス権限の登録申請、変更申請、廃棄申請、及びそれらの承認、定期的な検証プロセスを規定すること。	システムへのアクセス権限の追加・削除・変更の方法については手順書を作成し、cybozu.com システムの運用管理担当者のみにアクス権限を付与するルールとしています。従業員が雇用の終了または変更となった場合のアクセス権限の手続きについても規定しております。	適合可能	文献[01]にて、システムへのアクセス権限の追加・削除・変更の方法については手順書を作成し、cybozu.com システムの運用管理担当者のみにアクセス権限を付与するルールであることを確認した。 文献[01]にて、従業員の雇用の終了または変更となった場合のアクセス権限の手続きが規定されていることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comにおけるアクセス権限の管理を適切に実施する必要がある。
		(4)	それぞれの情報にアクセスする権限を持つ作業者を最小限に抑えるよう、適切に情報のグルーピングを行い、情報のグループに対するアクセス制御を行うこと。		適合可能	文献[01]にて、ネットワーク管理者の権限は、cybozu.comのシステム運用管理担当者のみに付与していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comにおけるアクセス権限の管理を適切に実施する必要がある。
		(5)	業務内容を考慮した必要最小限のアクセス権限を設け、アプリケーションやオペレーションシステムでの権限を設定すること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comにおけるアクセス権限の管理を適切に実施する必要がある。
	2.6.14.作業者アクセス及び作業者ＩＤの管理	(1)	作業者は情報処理装置上においてユニークな作業者ＩＤにより識別されること。	cybozu.com 運用環境のアカウントは各個人に一意の識別子を付与しています。また、重複発行は禁止しています。 以下の文書も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、システムアカウントは各個人に一意の識別子を付与していることを確認した。	公開文書	文献[01]	–	–	–	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(2)	作業者ＩＤを発行する際に、既存のＩＤとの重複を排除する仕組みを導入すること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(3)	複数作業者で共用するためのグループＩＤの利用は原則として行わず、業務上必要であれば、ログ上で操作の実施者が特定できるように、作業者ＩＤでログオンしてからグループＩＤに変更する仕組みを利用すること。	原則として共有アカウントは利用しないことにしております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(4)	作業者ＩＤの発行は医療情報システムの管理に必要な最小限の人数に留めること。	社内規定に基づきアクセス権を設定しています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(5)	作業者が変更あるいは退職した際には、ただちに当該作業者ＩＤを利用停止とすること。	従業員が雇用の終了または変更となった場合のアクセス権限の手続きについて規定しております。 以下の文書も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、従業員の雇用の終了または変更となった場合のアクセス権限の手続きが規定されていることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(6)	監視ログの監査時に作業者を確実に特定するため、作業者ＩＤは過去に使われたものを再利用しないこと。	作業IDは過去重複を排除しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(7)	不要な作業者ＩＤが残っていないことを定期的に確認すること。	システムへのアクセス権限の追加・削除・変更の方法については手順書を作成し、cybozu.com システムの運用管理担当者のみにアクス権限を付与するルールとしています。従業員が雇用の終了または変更となった場合のアクセス権限の手続きについても規定しております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(8)	特権ＩＤの発行は必要な最小限のものに留めること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(9)	特権使用者に昇格可能な作業者ＩＤを制限すること。	特権ID使用には、都度社内規定に基づく承認手続きが必要であり、承認手続きはシステムにて記録している。事前に登録された特権IDのみが作業者IDへ昇格できるよう設定している。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(10)	特権の使用時には作業実施内容を記録すること。	特権操作に限らず、cybozu.com 運用環境における全ての作業内容は記録されております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(11)	管理端末以外からの特権ＩＤによる直接ログオンを禁止すること。	cybozu.com 運用環境には、弊社内のオフィスネットワークとは論理的に隔離された、専用のオペレーション端末からのみ接続可能としています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(12)	情報処理装置及びソフトウェアを使用する前に、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等、必要のないアカウントについては削除あるいはパスワード変更を行うこと。	デフォルトのパスワードは必ず変更することを内規にて定めております。 以下の文書も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、パスワードは情報セキュリティ規則、情報システム運用マニュアルで規定していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(13)	医療情報システムへのログオン用パスワードはハッシュ値での保存、暗号化等、パスワードを容易に復元できない形で情報を保管すること。	内規にてパスワードは暗号化して保存することを定めております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(14)	医療情報システムへのログオン用パスワードには有効期限の設定を行い、定期的な変更を作業者に強制すること。	ログオン用パスワードは共通のIDではなく、運用者別に個別のパスワードを利用しています。 NIST SP800-63B（電子的認証に関するガイドライン）にもあるよう、定期的なパスワード変更をしない運用としていますが、パスワードは推測を困難にすべく、複雑度が高いものを設定するよう内規で義務付けています。	適合可能	文献[04]にて、利用者によるパスワード設定機能を提供しており、有効期間を含め設定が可能であることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[04]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(15)	医療情報システムへのログオン用パスワードの履歴管理を導入し、変更時には一定数世代のパスワードと同じパスワードを再設定することができないようにすること。	NIST SP800-63B（電子的認証に関するガイドライン）にもあるよう、定期的なパスワード変更をしない運用としていますが、履歴管理機能は導入されています。 https://jp.cybozu.help/general/ja/admin/list_security/passwordpolicy.html	適合可能	文献[04]にて、利用者によるパスワード設定機能を提供しており、パスワード再利用制限回数を含め設定が可能であることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[04]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(16)	パスワード変更時には変更前のパスワードの入力を要求し、変更前のパスワード入力を一定回数以上失敗した場合には、パスワード変更を一定期間受けつけない機構とすること。	cybozu.com 運用環境に接続するために利用する専用のオペレーション端末は、一定の回数以上パスワードの入力に失敗する場合、アカウントをロックするようにしております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(17)	パスワード発行時には、乱数から生成した仮の医療情報システムへのログオン用パスワードを発行し、最初のログオン時点で強制的に変更させる等パスワード盗難リスクに対する対策を実施すること。	システムの重要度に併せて、適切な文字長および、強度を持つパスワードを設定することを内規にて定めております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(18)	パスワードの満たすべき品質の基準を策定し、すべてのパスワードが品質基準を満たしていることを確実とすること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(19)	パスワードをシステムに記憶させる自動ログオン機能を利用しないよう作業者に徹底すること。	パスワードのブラウザ記憶は利用せず、パスワード管理ツールを利用するようにしております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(20)	パスワードに関連するデータを保存するファイルの真正性及び完全性を保つために、ファイルのハッシュ値の取得及び検証、ファイルに対するデジタル署名の付与及び検証、ファイルを暗号化して保存する等の保護策を採用すること。また、一般の作業者による閲覧を制限すること。	cybozu.com 運用環境に接続するために利用する専用のオペレーション端末は、運用管理者ごとに一意のIDを採番し、十分な複雑度をもったパスワードを設定しています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(21)	端末又はセッションの乗っ取りのリスクを低減するため、作業者のログオン後に一定の使用中断時間が経過したセッションを遮断、あるいは強制ログオフを行うこと。	cybozu.com 運用環境に接続するために利用する専用のオペレーション端末は、一定使用中断時間が経過したセッションは、強制ログオフを実施しています。長時間ログインしているアカウントがないかを監視しており、内規にて管理者が当該アカウントの保持者に長時間ログインの理由を確認することとしております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
		(22)	パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定すること。連続してログオンが失敗した場合は再入力を一定期間受付けない機構とすること。この場合には、警告メッセージをシステムの管理者に送出する仕組みを導入すること。	セキュリティインシデント発生時の対応プロセスが定められています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、cybozu.comにおけるID管理を適切に実施する必要がある。
	2.6.15.作業者の責任及び周知		各作業者に対しては、自己の責任範囲を認識し、責任を果たすことを周知することが必要である。以下の管理策について作業者に対し周知し、理解したことを確認すること。	–	適合可能	以下（1） （2） （3）にて確認を実施した。	–	–	–	–	–	利用者およびSI事業者は、自社社員のセキュリティ教育を適切に実施する必要がある。
		(1)	各作業者は自身のパスワードを秘密にし、パスワードを記録する必要がある場合は、安全な場所に保管して、他者による閲覧、修正、廃棄等のリスクから保護すること。	システムの重要度に併せて、適切な文字長および、強度を持つパスワードを設定することを内規にて定めております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者およびSI事業者は、自社社員のセキュリティ教育を適切に実施する必要がある。 アカウント管理を適切に実施する必要がある。
		(2)	システムに許可なくアクセスされた疑いがあるとき又はパスワードが第三者に知られた可能性がある場合には、直ちにパスワードを変更あるいはアカウントを無効化し管理者に通知すること。	セキュリティインシデント発生時の対応プロセスが定められています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、自社社員のセキュリティ教育を適切に実施する必要がある。 アカウント管理を適切に実施する必要がある。
		(3)	離席時及び非利用時には、端末をロックする、あるいはログオフして第三者の利用を未然に防ぐこと。	離席時は、第三者が容易に操作及び閲覧ができないようスクリーンロック等の対策を定め、実施しております。	適合可能	文献[01]にて、離席時は、第三者が容易に操作及び閲覧ができないようスクリーンロック等の対策を定め、実施していることを確認した。	公開文書	文献[01]	–	–	–	利用者およびSI事業者は、離席時および非利用時には端末をロックする、あるいはログオフして第三者の利用を未然に防ぐ必要がある。
2.7.人的安全対策			医療情報処理を受託する情報処理事業者において医療情報処理に関する管理を的確に行うため、医療情報に触れる機会を持つ情報処理事業者職員は、原則として情報処理事業者の正規職員に限ることを原則とするが、雇用形態が多様化している実態を踏まえ、派遣従業員等の非正規職員についても、秘密保持契約や情報セキュリティ教育等の履行に万全を期し、正規職員のみによる管理と同等レベルの管理が行われることを前提として、認めることとする。	cybozu.comの開発および、運用はデータセンターの運営事業を除き、全てサイボウズ社員が実施しております。	適合可能	以下（1） （2） （3） （4） （5）にて適合可能であることを確認済。 詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、医療情報を操作する可能性のある職員の全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約への署名を求める必要がある。
		(1)	医療情報を操作する可能性のある情報処理事業者職員の全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約への署名を求めること。派遣従業員については秘密保持義務及び継続的な情報セキュリティ教育を課すことを条件に選定、派遣することを求めること。	従業員の雇用時に社内規定（情報セキュリティ規則等）への遵守について同意確認を取っています。 雇用時および雇用後も必要に応じてセキュリティ・コンプライアンスに関する教育を実施しています。 以下の文書も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、雇用時に社内規定（情報セキュリティ規則等）へ遵守について署名・押印で明確に同意確認を取っていることを確認した。 文献[01]にて、サイボウズの従業員は雇用時および雇用後も必要に応じてセキュリティ・コンプライアンスに関する教育を実施していることを確認した。	公開文書	文献[01]	–	–	–	利用者およびSI事業者は、医療情報を操作する可能性のある職員の全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約への署名を求める必要がある。
		(2)	医療情報を操作する可能性のある情報処理事業者職員の全てに情報セキュリティに関する教育を行い、一定水準の理解を得たものだけを選定すること。派遣従業員に関しては、派遣元に対し、情報セキュリティに関する一定水準の知識、理解を持つ、あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行うこと。この教育は新しい脅威や情報セキュリティ技術の推移に合わせて定期的に行うこと。		適合可能	文献[01]にて、サイボウズの従業員は雇用時および雇用後も必要に応じてセキュリティ・コンプライアンスに関する教育を実施していることを確認した。	公開文書	文献[01]	–	–	–	利用者およびSI事業者は、医療情報を操作する可能性のある職員の全てに情報セキュリティに関する教育を行い、一定水準の理解を得たものだけを選定する必要がある。
		(3)	情報処理事業者職員による安全管理策違反の疑いが発生した際には、ただちに医療情報へのアクセス権を停止し、改ざん又は破壊等の行為が行われていないことを検証すること。	内部不正への対策として、「内部不正通報窓口」を設置しております。同窓口では、通報者の匿名性の確保や関係者以外への報告等を考慮した通報を行うことが出来ます。また不正の原因、事後的な影響等を調査する体制、再発防止策や事後対策を検討する体制、自社内外へ報告する体制も整備しています。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、職員による安全管理策違反の疑いが発生した際には、ただちに医療情報へのアクセス権を停止し、改ざん又は破壊等の行為が行われていないことを検証する必要がある。

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応						SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(4)	医療情報を操作する情報処理事業者職員が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続きを予め規定しておくこと。また、業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求めること。派遣従業員については、派遣契約解除時に同等の合意書への署名を求めること。	内規にて従業員(派遣・契約社員含む)の退職・休職時は、全てのシステムのアカウントを削除または使用停止すること、アクセス権・リモートアクセス権は削除または使用停止すること、業務PC・鍵・カードキー等を回収することを情報セキュリティ規則で明記することを定めています。また退職時には従業員との秘密保持の合意書を締結しています。 以下の文書も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、従業員の退職・休職時は、全てのシステムのアカウントを削除または使用停止すること、アクセス権・リモートアクセス権は削除または使用停止すること、業務PC・鍵・カードキー等を回収することを情報セキュリティ規則で明記していることを確認した。 詳細はサイボウズ社とのNDAにより開示。	要NDA	文献[01]	–	詳細はサイボウズ社とのNDAにより開示。	–	利用者およびSI事業者は、医療情報を操作する職員が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳および返却確認手続きを予め規定しておく必要がある。 利用者およびSI事業者は、業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求める必要がある。派遣従業員については、派遣契約解除時に同等の合意書への署名を求める必要がある。
		(5)	医療機関等との委託契約において、情報処理事業者職員との秘密保持契約を結ぶこと、情報セキュリティ教育を受けさせること、及び、規定に反して預託情報を不正に扱った際の懲罰規定等、預託情報の機密管理に関する条項を設けること。	従業員の雇用時に社内規定（情報セキュリティ規則等）への遵守について同意確認を取っています。 雇用時および雇用後も必要に応じてセキュリティ・コンプライアンスに関する教育を実施しています。 セキュリティ違反を犯した従業員は、懲戒の対象になることを情報セキュリティ規則にて定めております。 以下の文書も併せてご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	文献[01]にて、雇用時に社内規定（情報セキュリティ規則等）へ遵守について署名・押印で明確に同意確認を取っていることを確認した。 文献[01]にて、サイボウズの従業員は雇用時および雇用後も必要に応じてセキュリティ・コンプライアンスに関する教育を実施していることを確認した。 文献[01]にて、セキュリティ違反を犯した従業員は、当社就業規則に規定された懲戒の対象となることが、情報セキュリティ規則に明記されていることを確認した。	公開文書	文献[01]	–	–	–	–
2.8.情報の破棄		(1)	ＣＤ－Ｒ等の廃棄については「2.6.7.電子媒体の取扱」を参照すること。	電子媒体の保管・破棄などの管理方法につきましては、以下の文書をご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf 電子媒体の外部持ち出しは原則として禁止されています。 持ち出す場合には、以下の条件を満たす必要があります。 - 電子媒体が暗号化されていること - 利用者の所属する部長の許可を得ていること また、電子媒体を破棄する際には、物理的破壊もしくは、完全消去を行っています。	適合可能	「2.6.7.電子媒体の取扱」にて確認済	–	–	–	–	–	利用者およびSI事業者は、医療情報システムの利用に当たり外部電子媒体を使用する場合、「2.6.7.電子媒体の取り扱い」に準拠した対応を行う必要がある。
		(2)	ハードディスク等の廃棄については「2.5.4.情報処理装置の廃棄及び再利用に関する要求事項」を参照すること	大容量の記憶媒体は施錠管理し、破棄する場合には媒体を破壊しております。 cybozu.com ではデータを保管する際には、データを暗号化しております。データを削除する際には、暗号化する際に利用した「秘密鍵」を論理削除（削除ソフトウェアを用いてゼロもしくは、乱数の１回以上の書き込みを行うことで、論理的に削除する）しております。	適合可能	「2.5.4.情報処理装置の廃棄及び再利用に関する要求事項」にて確認済	–	–	–	–	–	利用者およびSI事業者は、医療情報システムの利用に当たりリムーバブルハードディスク等を使用する場合、「2.5.4.情報処理装置の廃棄および再利用に関する要求事項」に準拠した対応を行う必要がある。
		(3)	情報処理事業者は「医療情報システムの安全管理に関するガイドライン」に従って情報の破棄を行った記録を提出すること。	サービス解約の翌日から30日後にデータを消去いたします。消去に関してはログを取得し、要望があれば削除証明を発行可能です。詳細は以下のウェブページをご参照ください。 https://www.cybozu.com/jp/terms/ 下記ドキュメントもご参照ください。 https://www.cybozu.com/jp/support/data/cybozucom_securitysheet.pdf	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	詳細はサイボウズ社とのNDAにより開示。	詳細はサイボウズ社とのNDAにより開示。	–
2.9.医療情報システムの改造と保守			オペレーティングシステムのアップグレード、セキュリティパッチの適用を行う場合、医療情報システムに対する影響を評価し、試験結果を確認してから実施すること。	対象外	対象外	cybozu.comは、医療情報システムと接続していないため対象外。 ただし、文献[13]にて、サイボウズ側で実施する保守作業をcybozu.com利用者向けに事前告知していることを確認した。	公開文書	文献[13]	–	–	–	利用者およびSI事業者は、サイボウズから提供されるcybozu.comの保守作業を確認する必要がある。
2.10.医療情報処理に関する事業継続計画	2.10.1.要求事項の識別	(1)	医療情報処理に関わる業務プロセス（プロセスを実施するための作業員を含む）、情報処理設備等について識別すること。	利用者様にて適切に実施いただく必要があります。	対象外	cybozu.comを用いた業務プロセスは、cybozu.com利用者で整備するため、対象外。	–	–	–	–	–	利用者は、医療情報処理に関わる業務プロセスを識別する必要がある。 利用者およびSI事業者は、医療情報処理に関わる情報処理設備等について識別する必要がある。
		(2)	業務プロセス間の相互関係を評価すること。	利用者様にて適切に実施いただく必要があります。	対象外	cybozu.comを用いた業務プロセスは、cybozu.com利用者で整備するため、対象外。	–	–	–	–	–	利用者は、業務プロセス間の相互関係を評価する必要がある。
		(3)	事業を継続するための業務プロセスの優先順位を明確にすること。	利用者様にて適切に実施いただく必要があります。	対象外	cybozu.comを用いた業務プロセスは、cybozu.com利用者で整備するため、対象外。	–	–	–	–	–	利用者は、事業を継続するための業務プロセスの優先順位を明確にする必要がある。
		(4)	医療情報システムに発生するハードウェア及びソフトウェアの障害が業務プロセスに与える影響について識別すること。	利用者様にて適切に実施いただく必要があります。	対象外	cybozu.comを用いた業務プロセスは、cybozu.com利用者で整備するため、対象外。	–	–	–	–	–	利用者は、医療情報システムに発生するハードウェアおよびソフトウェアの障害が業務プロセスに与える影響について識別する必要がある。

Copyright (C) MRI All Rights Reserved.

経済産業省ガイドラインの評価項目				ガイドラインに対するサイボウズの見解	Cybozu.com における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	サイボウズ社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(5)	医療情報システムに発生するハードウェア及びソフトウェアの障害が他のハードウェア、ソフトウェアに及ぼす影響、相互作用について認識し、影響度の大きなハードウェア及びソフトウェアを識別すること。	cybozu.com の障害検知・復旧対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/fault_detection/index.html 以下のウェブページも併せてご確認ください。 https://www.cybozu.com/jp/service/slo.html	適合可能	文献[08]にて、cybozu.comでは各種サービスのプログラムやWebサーバーが稼働する仮想サーバーの障害に備え、自動分散エージェントシステムを構築しており、異常検知を素早く行うためサーバー同士が相互に監視し合い、障害の場合は自動復旧プロセスが開始され通常5分以内に回復する仕組みになっていることを確認した。 文献[24]にて、サイボウズは、cybozu.comの利用稼働状況は公開しており、サイボウズの目標値は99.99%としている。cybozu.com利用者は本情報を元に、自社のシステムへの影響有無を検討できる。	公開文書	文献[08] 文献[24]	–	–	–	利用者は、医療情報システムに発生するハードウェアおよびソフトウェアの障害が他のハードウェア、ソフトウェアに及ぼす影響、相互作用について認識し、影響度の大きなハードウェアおよびソフトウェアを識別する必要がある。
		(6)	ハードウェア及びソフトウェアの持つ影響度の大きさを評価し、影響度が大きすぎる部分については、該当システム部分の冗長化や、システムに障害が発生して情報の閲覧が不可能となった際に備え、汎用のブラウザ等で閲覧が可能となるよう、見読性が確保される形式（PDF、JPEG 及びPNG 等のフォーマット）で外部ファイルに出力可能とすることなどの方策を検討すること。	ストレージのデータ消失対策については、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/data_loss/index.html 利用者の方が保管したデータはローカルに出力することが出来ます。詳細は cybozu.com 上で提供される各サービスのマニュアルにて、操作手順を整備し公開いたしております。 https://www.cybozu.com/jp/support/manual/	適合可能	文献[06]にて、お客様のデータを管理するストレージサーバを構成するハードディスクはRAID-6を採用しており冗長化していることを確認した。 文献[06]にて、バックアップ専用のストレージサーバも用意されており、日々バックアップを取得していることを確認した。 文献[20]、文献[21]、文献[22]、文献[23]にて、cybozu.comの各機能にはエクスポート機能があり、それを用いてcybozu.com利用者はローカルに保存できることを確認した。	公開文書	文献[06] 文献[20] 文献[21] 文献[22] 文献[23]	–	–	–	利用者およびSI事業者は、ハードウェアおよびソフトウェアの持つ影響度の大きさを評価し、影響度が大きすぎる部分については、方策を検討する必要がある。
		(7)	医療機関等に提供する情報処理サービスの継続に必要であれば、受託する医療情報のバックアップ施設等、情報処理サービスを継続するための代替情報処理施設を設置し、それらの施設に対しても本ガイドラインで提示する物理的安全対策を施すこと。	東日本エリアのデータセンターでバックアップ専用のストレージサーバーを保有し、災害時に備え、西日本エリアのデータセンターで遠隔バックアップを実施しています。 詳細につきましては、以下のウェブページで公開しております。 https://www.cybozu.com/jp/security/disaster_control/index.html	適合可能	文献[06]にて、東日本エリアのデータセンターでバックアップ専用のストレージサーバーを保有し、災害時に備え、西日本エリアのデータセンターで遠隔バックアップを実施していることを確認した。	公開文書	文献[06]	–	–	–	利用者およびSI事業者は、医療情報システムを用いた業務継続性を考慮し、必要に応じた冗長構成を検討する必要がある。
	2.10.2.事業継続計画の立案及びレビュー	(1)	医療情報システムのサービス提供における業務プロセス及び医療情報システムの優先順位にもとづいて、医療情報処理に関する事業継続計画として策定すること。	事業継続計画書および事業継続計画手順書を整備しております。また計画の有効性を測定するための試験を実施しております。訓練の結果は経営者によってレビューされ、適宜見直しを行っております。	適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者は、医療情報システムのサービス提供における業務プロセスおよび医療情報システムの優先順位にもとづいて、医療情報処理に関する事業継続計画として策定する必要がある。
		(2)	策定した事業継続計画について模擬試験を含めた適切な方法でレビューすること。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者は、策定した事業継続計画について模擬試験を含めた適切な方法でレビューする必要がある。
		(3)	事業継続計画について定期的に見直しを行うこと。		適合可能	詳細はサイボウズ社とのNDAにより開示。	要NDA	–	–	–	詳細はサイボウズ社とのNDAにより開示。	利用者は、事業継続計画について定期的に見直しを行う必要がある。

Copyright (C) MRI All Rights Reserved.