医療機関向け
『cybozu.com』対応セキュリティリファレンス

概要説明資料

2019年7月10日

セキュリティリファレンスの概要（1）

■医療機関向けクラウドサービス対応セキュリティリファレンスとは？

近年、クラウドサービスは急速に普及しつつあり、大企業、中堅企業、中小企業の様々なビジネスシーンにおいて活用されています。ただし、病院等を含む医療機関においては、取り扱う個人情報の性質や非常時を想定した医療情報システムの可用性確保、および高解像度・大容量化が進む医療画像の取扱などの観点から、特に日本国内でのクラウドの利活用はあまり進んでいない状況です。

そこで、医療業界におけるクラウドサービスの利活用促進を目的として、医療機関に対する次の4ガイドライン（以下、「3省4ガイドライン」という。）に対して、対象とするクラウドサービスの対応状況を確認・整理しました。整理した結果を、ここでは「医療機関向けクラウドサービス対応セキュリティリファレンス」と呼んでいます。

① 厚生労働省「医療情報システムの安全管理に関するガイドライン　第5版」（平成29年5月）
https://www.mhlw.go.jp/stf/shingi2/0000166275.html

② 総務省「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）
http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/asp_saas/

③ 総務省「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　第1.1版」（平成22年12月）
http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_01000009.html

④ 経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」（平成24年10月）
https://www.meti.go.jp/policy/it_policy/privacy/iryouglv2.pdf

■医療機関向け『cybozu.com』対応セキュリティリファレンスとは？

今回公開する「医療機関向け『cybozu.com』対応セキュリティリファレンス」（以下、cybozu.com対応セキュリティリファレンス」という。）は、サイボウズ株式会社（以下、「サイボウズ」という。）のクラウドサービスである cybozu.com に関して、主に医療機関・SI事業者等が cybozu.comが提供するシステム基盤上に医療情報システムを構築・利用する場合を想定して、3省4ガイドラインの各項目に対する対応状況を調査したものです。調査は、株式会社三菱総合研究所が実施しました。

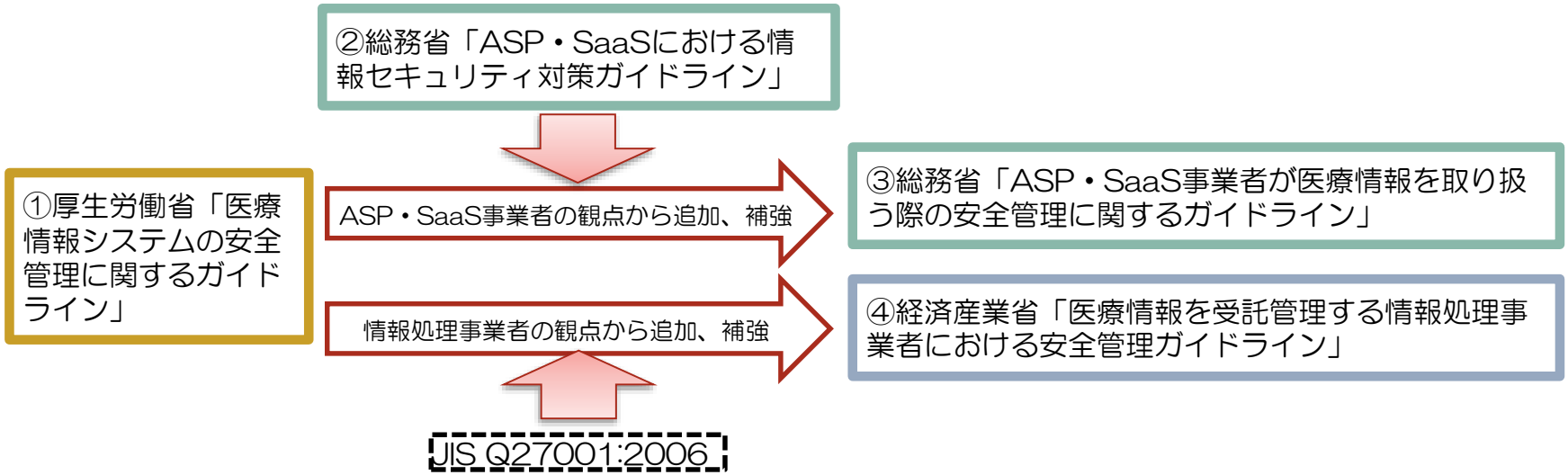
セキュリティリファレンスの概要（2）

■cybozu.com対応セキュリティリファレンスの構成

3省4ガイドラインの関連は下図の通りです。厚生労働省のガイドライン（①）を中心に、それらを補強するものとして総務省（②、③）および経済産業省（④）のガイドラインが位置づけられます。

総務省のガイドライン（②、③）については、③の第3章において、①の要求事項の対応関係が示されています。そこで、厚生労働省のガイドライン（①）および総務省のガイドライン（②、③）における要求事項は一体として整理して、「医療機関向け『cybozu.com』対応セキュリティリファレンス（厚生労働省・総務省版）」（以下、「cybozu.com対応セキュリティリファレンス（厚生労働省・総務省版）」という。）として取りまとめました。

一方、経済産業省のガイドライン（④）については、他のガイドラインとの関連性は高いものの、独自の要求事項が設定されているため、単独で整理して、「医療機関向け『cybozu.com』対応セキュリティリファレンス（経済産業省版）」（以下、「cybozu.com対応セキュリティリファレンス（経済産業省版）」という。）として取りまとめました。



出所）総務省「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　第1.1版」に基づき作成

セキュリティリファレンスの概要（3）

■cybozu.com対応セキュリティリファレンスの使い方

cybozu.com対応セキュリティリファレンスは、医療機関等（利用者）が自らcybozu.comを使用したり、SI事業者（システムインテグレータ）等がcybozu.comを利活用して医療機関機関にサービスを提供する場合に、3省4ガイドラインにどのように適合しうるかをセルフチェックするためのツールとして利用することを想定しています。

cybozu.com対応セキュリティリファレンスでは、3省4ガイドラインの要求事項に対して、「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」（「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」を示しています。

利用者やSI事業者が「SI事業者・利用者で必要な対応」に示した対応を自らが実施することと、「cybozu.comにおける対応」に示した状況の両方の結果により、3省4ガイドラインに適合できると考えています。

■cybozu.com対応セキュリティリファレンスの利用許諾について

cybozu.com対応セキュリティリファレンスは、「医療機関向け『cybozu.com』対応セキュリティリファレンス　利用許諾契約書」（以下、「利用許諾契約書」）を読み、その内容に同意した方のみに利用を許諾しています。詳細な利用条件等については、cybozu.com対応セキュリティリファレンスと同時に公開される利用許諾契約書をご覧ください。

cybozu.com対応セキュリティリファレンスの読み方

cybozu.com対応セキュリティリファレンスには、ガイドラインの各項目に対して、以下の表に示した項目が記載されています。

cybozu.com対応 セキュリティリファレンスの項目		項目の説明
ガイドラインの要求事項		厚生労働省ガイドラインの要求事項（「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、経済産業省ガイドラインの要求事項を記載した。
ガイドラインに対するサイボウズの見解		ガイドラインの要求事項に対するサイボウズの見解を記載した。
cybozu.com における対応	ガイドラインへの適合性	「本調査で確認した内容」ならびに「SI事業者・利用者で必要な対応」からガイドラインへの適合性を次の分類で整理した。 「適合可能」：cybozu.comの状況に加えて、SI事業者・利用者が必要な対応を行うことで適合可能。 「対象外」　：cybozu.comにおける対応の対象外であり、必要に応じてSI事業者・利用者が対応。
	本調査で確認した内容	本調査で確認したcybozu.comの対応状況。 確認にあたっては、公開文書の確認、第三者認証等からの類推に加えて、サイボウズに対するインタビューや、サイボウズとのNDA締結により入手できる文書等を用いた。
	確認文書等の開示レベル	内容の確認に用いた文書等の開示レベルを次の分類で整理した。 「公開文書」：公開文書に記載されている公開情報 「要NDA」：サイボウズとのNDA締結により入手できる文書等に記載されている情報
	確認した公開文書	確認に使用した公開文書への参照を記載した。 文献番号に対応する公開文書の情報は「参照文書リスト」に示した。
	第三者認証等から類推した内容	cybozu.comが取得済みの第三者認証の認証状況から対応状況を類推した内容を記載した。
	サイボウズへのインタビューで確認した内容	サイボウズに対するインタビューにより確認した内容を記載した。
	NDAに基づき確認した資料	サイボウズとのNDA締結により入手した資料への参照を記載した。
SI事業者・利用者で必要な対応		ガイドラインの要求事項に適合するために、SI事業者・利用者での対応が必要な項目について、その対策例を示した。

参照文書リスト（1）

ID	名称・URL
01	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
02	cybozu.com 製品セキュリティ https://www.cybozu.com/jp/productsecurity/
03	cybozu.comで実施しているクラウドサービスを安全に使うために重要な7つの対策 – 不正アクセス対策 https://www.cybozu.com/jp/security/illegal_access/index.html
04	cybozu.comで実施しているクラウドサービスを安全に使うために重要な7つの対策 – 不正ログイン対策 https://www.cybozu.com/jp/security/bad_login/index.html
05	cybozu.comで実施しているクラウドサービスを安全に使うために重要な7つの対策 – 脆弱性対策 https://www.cybozu.com/jp/security/vulnerability/index.html
06	cybozu.comで実施しているクラウドサービスを安全に使うために重要な7つの対策 – データ消失対策 https://www.cybozu.com/jp/security/data_loss/index.html
07	cybozu.comで実施しているクラウドサービスを安全に使うために重要な7つの対策 – 災害対策 https://www.cybozu.com/jp/security/disaster_control/index.html
08	cybozu.comで実施しているクラウドサービスを安全に使うために重要な7つの対策 – 障害検知・復旧対策 https://www.cybozu.com/jp/security/fault_detection/index.html
09	cybozu.comで実施しているクラウドサービスを安全に使うために重要な7つの対策 – ヒューマンエラー対策 https://www.cybozu.com/jp/security/human_error/index.html
10	cybozu.com利用規約 https://www.cybozu.com/jp/terms/
11	CSIRT記述書（Description） https://www.cybozu.com/jp/security/management/cysirt.html
12	脆弱性報奨金制度 https://cybozu.co.jp/products/bug-bounty/
13	サイボウズからのお知らせ – cybozu.com https://cs.cybozu.co.jp/cybozucom/
14	脆弱性情報ハンドリングポリシー https://www.slideshare.net/slideshow/embed_code/30074325

参照文書リスト（2）

ID	名称・URL
15	プライバシーポリシー https://cybozu.co.jp/privacy/privacy-policy/
16	クラウドデータポリシー https://cybozu.co.jp/privacy/cloud-data-policy/
17	ISMS基本方針 https://www.cybozu.com/jp/terms/security.html
18	サービス一覧　セキュアアクセス https://www.cybozu.com/jp/service/option/
19	各サービスのマニュアル一覧 https://www.cybozu.com/jp/support/manual/
20	サイボウズOfficeのマニュアル https://help.cybozu.com/ja/o/index.html
21	Garoonのマニュアル https://help.cybozu.com/ja/g/index.html
22	kintoneのマニュアル https://help.cybozu.com/ja/k/index.html
23	メールワイズのマニュアル https://help.cybozu.com/ja/m/index.html
24	サービス環境　運用環境（SLO） https://www.cybozu.com/jp/service/slo.html
25	Cy-PSIRTの取り組み https://www.slideshare.net/Mtikutea/cypsirt