

安心安全に医療介護福祉情報を利用するために

## セキュリティ要件報告書

株式会社 佐野医療介護ICTビジネスクリエイト

1. はじめに
2. 考慮すべき判断指標
3. コミュニケーションツール候補評価
4. 今後の考慮、実施が必要なこと
5. まとめ
6. 報告者

令和7年12月9日、社会保障審議会医療保険部会より

令和8年度診療報酬改定の基本方針が示され、

「2040年頃を見据えた医療機関の機能の分化・連携と地域における医療の確保、地域包括ケアシステムの推進」について下記文言が記載されました。

「医療提供体制の構築に当たっては、更なる生産年齢人口の減少に伴って医療従事者確保の制約が増す中で、ICT、AI、IoT等の利活用の推進等により医療従事者の業務効率化・負担軽減等を行う」(4項)

今回の本協議会「医療福祉情報プラットフォームプロジェクト」の推進は、まさに国の基本方針に沿ったプロジェクトと考えます。

一方、医療介護福祉情報は個人情報（要配慮個人情報）取扱考慮が必須であるとともにオンライン上でのデータやりとりに伴う利便性享受の代償としてサイバーセキュリティ対策が事業者自身の事業継続性及び地域への医療介護福祉サービス提供継続性の観点から必須となります。

本報告書は協議会参加者に、

安心安全に医療介護福祉情報を利用頂くための指針をご提供することを趣旨とします。

医療介護福祉情報は個人情報（要配慮個人情報）の取扱いに関して、病院、一般診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者は、その規模の大小に関係なく、3省2ガイドラインに準拠することが要求されています。



2023年度医療法改正より、**病院、診療所、助産所**は医療法施行規則 第十四条2項「サイバーセキュリティ基本法」が規程されました。毎年、**3省2ガイドライン**を根拠に作成される「サイバーセキュリティ対策チェックリスト」に対する回答、必要時監査を受ける状況になりました。

チェックリストは3省2ガイドラインを根拠に作成されています

資料2-2		令和7年度版	医療機関確認用	
医療機関におけるサイバーセキュリティ対策チェックリスト				
*1 入力検査時、本チェックリストを確認します。令和7年度中にすべての項目で「はい」にマルが付くよう取り組んでください。 *2 「いいえ」の場合、令和7年度中の対応目標日を記入してください。				
1	体制構築	チェック項目	確認結果 (日付)	備考
2	医療情報システム の管理・運用	医療情報システム安全管理責任者を設置している。(1-(1))	はい/いいえ/ ( )	
		医療情報システム全般について、以下を実施している。 サーバ、端末PC、ネットワーク機器の危機管理を行っている。(2-(1))	はい/いいえ/ ( )	
		リモートメンテナンス(保守)を利用している機器の有無を事業年度に確認した。(2-(2)) ※事業者と契約していない場合には、記入不要	はい/いいえ/ ( )	
		事業者から製造業者/サービス事業者による医療情報セキュリティ開示書(MDS/SDS)を提出してもらった。(2-(3)) ※事業者と契約していない場合には、記入不要	はい/いいえ/ ( )	
		利用者の職種・担当業務等の情報区分別のアクセス利用権限を設定している。 ※ 監査者権限等の権限を行っていない(2-(4))	はい/いいえ/ ( )	
		監査者や使用していないアカウント等、不要なアカウントを廃棄または無効化している。(2-(5))	はい/いいえ/ ( )	
		セキュリティパッチ(脆弱性ソフトウェアや更新プログラム)を適用している。(2-(6))	はい/いいえ/ ( )	
		パスワードは英数字、記号が混合した8文字以上とし、定期的に更新している。 ※ 二要素認証、または13文字以上の場合は定期的な更新は不要(2-(7))	はい/いいえ/ ( )	
		パスワードの使い回しを禁止している。(2-(8))	はい/いいえ/ ( )	
		アクセスログを管理している。(2-(9))	はい/いいえ/ ( )	
バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(10))	はい/いいえ/ ( )			
端末PCについて、以下を実施している。 バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(11))	はい/いいえ/ ( )			
ネットワーク機器について、以下を実施している。 接続先制御を実施している。(2-(12))	はい/いいえ/ ( )			
3	インシデント発生に 対応した対応	インシデント発生時における院内および外部関係機関(事業者、厚生労働省、警察等)への連絡体制がある。(3-(1))	はい/いいえ/ ( )	
		インシデント発生時に対応を継続するために必要な情報を確認し、データやシステムのバックアップの高度と復旧手順を確認している。(3-(2))	はい/いいえ/ ( )	
		サイバー攻撃を想定した事業継続計画(BCP)を策定している。(3-(3))	はい/いいえ/ ( )	
4	規程等の整備	上記1-3のすべての項目について、具体的な実施方法を運用管理規程等に定めている。(4-(1))	はい/いいえ/ ( )	

資料3-1		令和6年度版	医療機関確認用	
医療機関におけるサイバーセキュリティ対策チェックリスト				
*以下項目は令和6年度中にすべての項目で「はい」にマルが付くよう取り組んでください。 *1 1回目の確認で「いいえ」の場合、令和6年度中の対応目標日を記入してください。				
1	体制構築	チェック項目	確認結果 (日付)	備考
2	医療情報システム の管理・運用	医療情報システム安全管理責任者を設置している。(1-(1))	はい/いいえ/ ( )	
		医療情報システム全般について、以下を実施している。 サーバ、端末PC、ネットワーク機器の危機管理を行っている(1)	はい/いいえ/ ( )	
		リモートメンテナンス(保守)を利用している機器の有無を等に確認した。(2-(1)) ※事業者と契約していない場合には、記入不要	はい/いいえ/ ( )	
		事業者から製造業者/サービス事業者による医療情報セキュリティ開示書(MDS/SDS)を提出してもらった。(2-(2)) ※事業者と契約していない場合には、記入不要	はい/いいえ/ ( )	
		利用者の職種・担当業務等の情報区分別のアクセス利用権限を設定している。 ※ 監査者権限等の権限を行っていない(2-(3))	はい/いいえ/ ( )	
		監査者や使用していないアカウント等、不要なアカウントを廃棄または無効化している。(2-(4))	はい/いいえ/ ( )	
		セキュリティパッチ(脆弱性ソフトウェアや更新プログラム)を適用している。(2-(5))	はい/いいえ/ ( )	
		パスワードは英数字、記号が混合した8文字以上とし、定期的に更新している。 ※ 二要素認証、または13文字以上の場合は定期的な更新は不要(2-(6))	はい/いいえ/ ( )	
		パスワードの使い回しを禁止している。(2-(7))	はい/いいえ/ ( )	
		アクセスログを管理している。(2-(8))	はい/いいえ/ ( )	
バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	はい/いいえ/ ( )			
端末PCについて、以下を実施している。 バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(10))	はい/いいえ/ ( )			
ネットワーク機器について、以下を実施している。 接続先制御を実施している。(2-(11))	はい/いいえ/ ( )			
3	インシデント発生に 対応した対応	インシデント発生時における院内および外部関係機関(事業者、厚生労働省、警察等)への連絡体制がある。(3-(1))	はい/いいえ/ ( )	
		インシデント発生時に対応を継続するために必要な情報を確認し、データやシステムのバックアップの高度と復旧手順を確認している。(3-(2))	はい/いいえ/ ( )	
		サイバー攻撃を想定した事業継続計画(BCP)を策定している。(3-(3))	はい/いいえ/ ( )	
4	規程等の整備	上記1-3のすべての項目について、具体的な実施方法を運用管理規程等に定めている。(4-(1))	はい/いいえ/ ( )	

資料3-2		令和5年度中	医療機関確認用	
医療機関におけるサイバーセキュリティ対策チェックリスト				
*以下項目は令和5年度中にすべての項目で「はい」にマルが付くよう取り組んでください。 *2 (2)及び2(3)については、事業者と契約していない場合には、記入不要です。 *1 1回目の確認で「いいえ」の場合、令和5年度中の対応目標日を記入してください。				
1	体制構築	チェック項目	確認結果 (日付)	備考
2	医療情報システム の管理・運用	医療情報システム安全管理責任者を設置している。(1)	はい/いいえ/ ( )	
		医療情報システム全般について、以下を実施している。 サーバ、端末PC、ネットワーク機器の危機管理を行っている(1)	はい/いいえ/ ( )	
		リモートメンテナンス(保守)を利用している機器の有無を等に確認した。(2-(1)) ※事業者と契約していない場合には、記入不要	はい/いいえ/ ( )	
		事業者から製造業者/サービス事業者による医療情報セキュリティ開示書(MDS/SDS)を提出してもらった。(2-(2)) ※事業者と契約していない場合には、記入不要	はい/いいえ/ ( )	
		利用者の職種・担当業務等の情報区分別のアクセス利用権限を設定している。 ※ 監査者権限等の権限を行っていない(2-(3))	はい/いいえ/ ( )	
		監査者や使用していないアカウント等、不要なアカウントを廃棄または無効化している。(2-(4))	はい/いいえ/ ( )	
		セキュリティパッチ(脆弱性ソフトウェアや更新プログラム)を適用している。(2-(5))	はい/いいえ/ ( )	
		パスワードは英数字、記号が混合した8文字以上とし、定期的に更新している。 ※ 二要素認証、または13文字以上の場合は定期的な更新は不要(2-(6))	はい/いいえ/ ( )	
		パスワードの使い回しを禁止している。(2-(7))	はい/いいえ/ ( )	
		アクセスログを管理している。(2-(8))	はい/いいえ/ ( )	
バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))	はい/いいえ/ ( )			
端末PCについて、以下を実施している。 バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(10))	はい/いいえ/ ( )			
ネットワーク機器について、以下を実施している。 接続先制御を実施している。(2-(11))	はい/いいえ/ ( )			
3	インシデント発生に 対応した対応	インシデント発生時における院内および外部関係機関(事業者、厚生労働省、警察等)への連絡体制がある。(3-(1))	はい/いいえ/ ( )	
		インシデント発生時に対応を継続するために必要な情報を確認し、データやシステムのバックアップの高度と復旧手順を確認している。(3-(2))	はい/いいえ/ ( )	
		サイバー攻撃を想定した事業継続計画(BCP)を策定している。(3-(3))	はい/いいえ/ ( )	
4	規程等の整備	上記1-3のすべての項目について、具体的な実施方法を運用管理規程等に定めている。(4-(1))	はい/いいえ/ ( )	

経済産業省は全業種向けに昨今のランサムウェア被害の発生原因より「サプライチェーン強化に向けたセキュリティ対策評価制度構築」を2026年度からの制度運用を目指す旨HP上に記載しています。

The screenshot shows the homepage of the Ministry of Economy, Trade and Industry (METI) with a news article titled "「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針（案）」（SCS評価制度の構築方針（案））を公表しました". The article is dated December 26, 2025. A green arrow points from a text box on the right to the article title.

サプライチェーン攻撃は最初にセキュリティー対策が脆弱な事業者より侵入し、次に、サプライチェーン情報経路より脆弱性対応済取引関係者にも侵入し、被害をもたらす。

今後、公的ガイドラインを準拠しない医療介護福祉事業者は、地域へのサービス提供の「サプライチェーン」に参加できない事態になりかねません。

## 1. サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針（案）について

### 制度検討の背景

近年、取引先に影響を与えるようなサイバー攻撃事案が顕著化しており、サプライチェーン全体でのサイバーセキュリティ対策の強化が求められています。そうした中、取引先のセキュリティ対策状況を外部から判断することが難しいといった発注元企業側の課題や、複数の取引先から様々な対策を要求されるといった委託先企業側の課題が生じています。こうした課題に対応するため、経済産業省及び内閣官庁国家サイバー統括室では、サプライチェーンにおける重要性を踏まえた上で満たすべき各企業の対策を提示しつつ、その対策状況を可視化する仕組み（「サプライチェーン強化に向けたセキュリティ対策評価制度」）の検討を進めるべく、産業サイバーセキュリティ研究会ワーキンググループ1「サプライチェーン強化に向けたセキュリティ対策評価制度に関するサブワーキンググループ」において、制度の目的や位置付け、要求項目・評価基準の内容、制度の普及のために必要な施策等について有識者・産業界とも継続して議論を進め、本年4月に本制度構築に向けた「中間取りまとめ」を公表しました。

各社IT製品サービスは、各社が様々な自社セキュリティーポリシーに基づいて製品サービスを提供されており、一定レベルの水準は担保できていると考えますが、利用する医療介護福祉事業者は各社の様々なセキュリティーポリシーでは比較、判断が困難です。

上記課題を解決する判断指標として  
医療介護福祉業界向に公的なガイドラインとして下記が制定されています。

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6.0版」  
経済産業省・総務省 「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理 ガイドライン第2.0版」

上記ガイドラインを評価基準にすることで  
統一的な尺度を得て、各社IT製品サービスを統一的に評価することができます。

逆に、公的ガイドライン準拠を評価基準にしなかった場合、  
「製品サービスの不具合が原因」で、個人情報漏洩またはサイバーセキュリティ被害にあった場合、選定した事務局は管轄行政に対して  
公的ガイドラインに準拠しない製品サービスを選定した理由、根拠の説明責任が発生するリスクがあると考えます。

ガイドライン準拠状況について、今回トライアル対象4社のサービスについて評価を実施しました。前提事項は下記です。

**1. 評価時期**：2025年11月時点

**2. 想定利用者**：本協議会参加法人所属職員(\*1)、協議会事務局職員  
(\*1)特別養護老人ホーム、グループホーム、障害者支援施設、  
訪問看護ステーション、薬局、歯科診療所、医科診療所、病院

**3. 対象情報**：介護サービス利用者、患者に関する  
個人情報（要配慮個人情報）含むコミュニケーション情報

**4. 評価基準**：

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6.0版」  
経済産業省・総務省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理 ガイドライン第2.0版」

**5. 評価方法**：各社ホームページ公開情報を確認した上で  
候補ベンダー4社に対して「情報提供依頼書」を  
次項の文面で送付し、回答を求める。

<各社ガイドライン準拠及びセキュリティポリシーについての公開URL>

「MedicalCare STATION」

<https://about.medical-care.net/html/service/security.html>

「カナミックネットワーク」

<https://aspicjapan.org/nintei/%e5%8c%bb%e7%99%82-0001-1712/>

「LINE WORKS」

<https://line-works.com/privacycenter/security/certification/>

「チャットワーク」

[https://go.chatwork.com/ja/solutions/careworkers/?utm\\_source=chatgpt.com](https://go.chatwork.com/ja/solutions/careworkers/?utm_source=chatgpt.com)

2025年11月吉日

ベンダー様各位

長崎県西海市  
医療福祉情報プラットフォーム  
プロジェクト協議会情報提供依頼

拝啓、時下ますますご清栄のことお慶び申し上げます。当協議会では来年度末に向けて、医療福祉情報プラットフォーム構築において有効な製品・サービスの情報収集を実施します。今回、セキュリティ要件について情報提供いただきたくご案内させていただきました。

ご多忙のところ大変恐縮ではございますが、ご協力の程よろしくお願い申し上げます。

敬具

## 記

## ■依頼内容

1. 御社製品・サービスが下記ガイドライン準拠の根拠とされている説明資料をご提出ください。  
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6.0版」、  
経済産業省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第2.0版」
2. ガイドライン記載上、2027年度から必須準拠とされている「2要素認証」を機能提供しているか  
現在「2段階認証」の場合には対応計画をご回答ください。
3. システム利用者のアクセスログをシステム管理者が定期的に確認できる仕組みになっているか  
ご回答ください。
4. ネットワーク要件として、IPsecによるVPN接続を利用しない場合でHTTPSを利用する場合  
TLSプロトコルはTLS1.3以上に限定して、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しているか、回答してください。
5. 御社雛形SLAをご提出して打合せを実施し、責任分界点について合意形成可能か回答してください。

## ■回答方法

本メールに情報提供資料添付にてご返信ください。添付ファイル容量が大きい場合はディスク転送サービス等をご利用ください。

■提出締切希望日 2025/11/21(金)迄

以上

## 候補ツールベンダー向 情報提供依頼書 内容

各社回答結果および各社提出資料は  
別途納品します。

## 3.4

## コミュニケーションツール候補評価

	MedicalCare STATION	カナミック ネットワーク	LINE WORKS	チャットワーク
ガイドライン準拠	準拠	準拠	非準拠	非準拠
判定根拠	公開準拠情報[有] 個別回答にも準拠 に該当する回答有。	公開準拠情報[無] 個別回答提出資料 内に「ガイドライ ン準拠」を明言す る。	公開準拠情報[無] 個別回答「汎用的な サービスであるため、 ガイドラインへの準 拠については弊社側 判断することはでき ません。」	公開準拠情報[無] 個別回答「準拠し ておりません。」
判定結果	制限付推奨	制限付推奨	推奨しない	推奨しない
補足	追加質疑は1回4万 円の有料対応とし、 追加質問回答無。 <u>顧客要件に柔軟に 対応する姿勢無。</u>	提出資料内に準拠 を明言しているが、 <u>根拠公開無。</u> また <u>個別質疑で、準拠 していない回答が 複数有。</u>	多数の医療介護施 設向導入実績より、 準拠に等価する情 報を追加で確認す るも提出無。	自社サイト内に、介 護事業者向けにガイ ドライン準拠情報を 公開している。準拠 しているとは記載し ていないが、あたか も準拠していると誤 認しかねない。

### 1. 教育

1) なぜ対応実施が必要なのかの理解

「事業者自身の事業継続性」、「地域への医療介護福祉サービス提供継続性」

2) 個人情報の適切な取り扱いの理解

「医療・介護関係事業者における 個人情報の適切な取扱いのためのガイダンス」

厚労省 個人情報保護委員会

3) サイバーセキュリティ対策の理解

費用対効果より対応優先度を考えて順番に実施

### 2. 運用環境整備

運用ルール（情報管理規定）作成

認証方式（二要素認証）

パスワード強度（13桁以上の英数記号混在推奨、管理者の共通パスワードは不可）

外部通信環境整備（可視化、集約化、ログ管理、定期的脆弱性対応ファーム更新）

USBメモリー取扱い（法人配布の暗号化・パスワード付き以外利用禁止。台帳棚卸管理）

無線利用セキュリティー強化（管理者パスワード、暗号化方式、ファーム更新）

BYOD（私物機器の業務利用）原則禁止

### 3. 支援体制構築

各協議会参加者が個別に対応することは現実的に困難

協議会参加者に対して集約して支援するための体制構築が現実的な対応

そのための人員、予算確保が必要

便利なICTサービス&機器は業務効率・品質面で非常に大きなメリットがありますが  
メリットがあれば必ずデメリットがあります。

デメリットとは具体的には一瞬にして大量の個人情報が漏洩するリスク、  
オンラインゆえのサイバー攻撃によるデータを暗号化されてしまうリスクがあります。

本協議会参加者の事業継続性、地域への医療介護福祉サービス提供継続性観点から  
本プロジェクト推進にはセキュリティー対策が必須と考えます。

ランサムウェア被害の約7割はリモートメンテラターの脆弱性を狙われての  
経由ルートです。また被害者はパスワードが簡易で共通利用の運用が特徴的です。  
攻撃者もビジネスです。侵入コストが高いとターゲットから外れる可能性が高いです。  
基本的かつ安価な対応だけでも侵入コストを上げる事が可能です。

公的ガイドライン準拠に沿ってセキュリティー対策を整備・実施していく方針の元に、  
優先度を考慮し、コストパフォーマンスが高い施策から順番に実施していくことが  
最も有効な施策と考えます。

本報告書によって協議会参加者が、安心安全に医療介護福祉情報を利用頂くための  
指針になれば幸いです。



## 佐野医療介護 ICTビジネスクリエイト



<b>拠点</b>	大阪府豊中市
<b>事業</b>	医療情報システムコンサルティング



創業：2014年9月

代表取締役：佐野 祐宏

種別	サービス名
①選定導入	<ul style="list-style-type: none"> <li>電子カルテ、部門システム 選定導入支援業務</li> <li>医療情報系ネットワーク 選定導入支援業務</li> <li>院内仮想統合サーバ 選定導入支援</li> <li>院内勤怠、勤務表システム 選定導入支援業務</li> </ul>
②運用企画	<ul style="list-style-type: none"> <li>月次院内システム会議運営業務</li> <li>中長期IT投資計画立案、実行フォロー業務</li> </ul>
③DBツール開発	<ul style="list-style-type: none"> <li>医療情報系クローズドNW内 Accessツール開発 (開発実績：未収金管理、地域係室紹介管理、多職種連携 専門学会報告データ管理)</li> </ul>

資格：医療情報技師（日本医療情報学会認定番号 20141046）  
 第二種情報処理技術者（第22962305号）  
 VBAエキスパート Standard Crown (MOS試験 Odyssey社認定)  
 VBA Expert Microsoft Access VBA Standard  
 VBA Expert Microsoft Excel VBA Standard  
 Microsoft Access Expert (Office 2019)



### ひと言 アピール

2040年に向け、中小規模病院生き残りのIT施策を、社会保障制度の方向性考慮し、コスパ優先で推進します。