「製造業者による医療情報セキュリティ開示書」ガイド　Ver.3.0a に関するQ&A

（「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」対応）

2018年11月

JIRA -JAHIS　合同開示説明書WG

目次

はじめに

本書は「製造業者による医療情報セキュリティ開示書」（以下、MDS とする。）関連セミナー」で寄せられた質問を中心にまとめたものです。

※Q における「質問ｎ」の”ｎ”は MDS Ver.3.0a における番号を指します。
※本書では厚生労働省の「医療情報システムの安全管理に関するガイドライン」を「安全管理ガイドライン」と記します。
※本書並びに本書に基づいたシステムの導入・運用についてのあらゆる障害や損害について、本書作成者は何ら責任を負わないものとします。

「全体」

Ｑ１．ある病院様より「弊社より納入した医療情報パッケージシステムは、医療情報システムの安全管理に関するガイドラインに対応しているのか？」と回答を求められています。
本ガイドラインについては、どこまでがパッケージシステムに該当し、対応可否の回答をすれば良いのかが判別できない状況にいます。
「製造業者による医療情報セキュリティ開示書」ガイドに「5.2 チェックリスト（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版対応）」がありますが、本チェックリストにある項目が、医療情報システムの安全管理に関するガイドラインの中でパッケージシステムとして対応可否の回答をすべき事項が全て網羅されており、それ以外の項目はパッケージシステムとして関係が無く、対応可否の回答をせずとも良いとの考えで宜しいのでしょうか。

Ａ１．まず大前提ですが「医療情報システムの安全管理に関するガイドライン」（以下「安全管理ガイドライン」という。）に対応すべき対象は、システムベンダーやその医療情報システムではなく医療機関等であるということです。
医療機関等で誤解されている場合があるのですが、医療情報システムが安全管理ガイドラインに対応するのではなく、医療機関等がシステムの持つ機能（技術的対策）とそれに相応した運用的対策を組み合わせて安全管理ガイドラインに対応するものです。必ずしも技術的対策が必須となる訳ではありません。

「製造業者による医療情報セキュリティ開示書」（以下「MDS」と略す。）では安全管理ガイドラインのＣ項「最低限のガイドライン」の中で、製造業者が提供する個々の医療情報システムの持つ機能(技術的対策)に関して抜粋したものとなっています。
そのため、「MDS」のチェックリストに御社のシステムについて回答したものを提出されれば、基本的には質問された病院様のニーズに応えた事になると思われます。
しかしながら、「MDS の全項目を回答すれば他は考慮しなくてよい」とは言えません。

MDS は「C 項に関して技術的対策で対応可能と考えられる項目」をピックアップしたものであり、D 項「推奨されるガイドライン」については対象外としています。
厚生労働省が MDS の使用を推奨していますが、完全網羅性が保証されている訳ではありません。
なぜなら、システムの使用条件が運用に制約を与える場合、その制約により安全管理ガイドラインの運用要件（C 項）が影響を受ける場合があり、医療機関から見れば、その部分も考慮ポイントとなりえます。

Q2．MDS チェックリストの使い方が今一つしっくりきません。医療機関から求められてチェックリストを提出していますが同じ製品であっても、納品先によって詳細な機能の使い方が異なるため、チェックリストの内容が変わってしまいます。どのように使用すればよろしいのでしょうか？

A2． MDS チェックリストは納品仕様書ではなく、製品の機能リストです。「安全管理ガイドライン」の技術的対策の実装の有無を「はい」、「いいえ」、「対象外」で表しています。
そのため機能を有していて、納品先との調整の結果、設定で機能をオフにしていても MDS チェックリストとしては「はい」という回答になります。
例えば、案件段階で医療機関等が採用を検討する製品のセキュリティ対応状況を説明する際等に MDS を使用することができます。

Q3．質問の後ろの括弧の中の番号は何を示すのか。

A3．質問項目の括弧内に記載されている番号は、安全管理ガイドライン第5版の各章番号に対応するものです。

Q4．MDS は医療機関から請求されて提出する物なのか、製造業者側から積極的に提出するものなのか。

A4．MDS は製造業者から自発的に開示することを想定したものです。統一フォーマットを使用することにより、製造業者からの医療情報システムのセキュリティ対応状況の説明、医療機関側の情報収集が効率よく行えるようになることを期待しています。

Q5．ホームページでの MDS の公開等を考えるとマイナーバージョン毎の修正は避けたいが、バージョンは「ｘｘｘ以上」という表現でもよいか。

A5．MDS はお客様に対して納品する製品のチェックリストを提供するものです。それぞれのお客様に

対して納品する製品のバージョンを記載した MDS を提供してください。ホームページで公開する場合はバージョンの記載方法について医療機関が混乱しないよう各製造業者で判断してください。

Q6．製造する会社と販売する会社が異なる場合はどうすればよいか。

A6．一般的には製造する会社が作成します。例外として OEM の場合、製造受託側ではなく、製造委託側の型式番号を持っている会社が発行する場合があります。

Q7．オプションの考え方（定義）が良くわからない。

A7．MDS におけるオプションの定義は、自社製品である必要はなく、動作確認が取れており、保守問合せ等の一次窓口になれる製品やサービスになります。単純に市販品等を調達して納品するだけではオプションとはみなせません。

Q8．ユーザの意向に応じて設定で機能がオン/オフできる場合、「はい」と回答して良いか？

A8．「はい」で結構です。デフォルト設定で機能がオフになっている場合は、備考にその旨を記載してください。

Q9．ユーザの要望により機能を追加する場合は「はい」と回答して良いでしょうか？

A9．「はい」とは回答できません。現時点で実装されていない機能については「いいえ」となります。

Q１０．MDS のチェックリストは安全管理ガイドラインのＣ項を網羅しているのか？

A１０．MDS のチェックリストは、安全管理ガイドラインのＣ項の項目の中で製造業者が提供する個々の医療情報システムのセキュリティ機能に関して抜粋して記載しています。これにより、医療機関側でＣ項を網羅したセキュリティマネジメントを実施するための材料となります。

Ｑ１１．質問の内容に対して部分的に未対応な場合は「はい」と回答して、備考に未対応内容を記せば良いか？

Ａ１１．一部でも未対応な場合は「いいえ」と回答し、備考に対応/未対応内容に関して記述してください。「はい」と回答する場合は全てについて対応できている場合になります。

Ｑ１２．オプションで対応可能な場合は「はい」と回答してよいか？

Ａ１２.「はい」で結構です。そのオプションの内容を備考に記載してください。

「安全管理ガイドライン６章　情報システムの基本的な安全管理」関係

Ｑ１３.「質問１」の「扱う情報のリスト」とは、どういう物か。

Ａ１３. 患者情報の項目のリストです。例えば患者の氏名、ID、住所などです。扱う情報に関しては基本情報だけでなく、検査データや画像情報等も漏れなく記載してください。システムにもよりますがDICOM Conformance Statement 等でリストの代用も可能な場合があります。

Ｑ１４.「質問１」の「はい」、「いいえ」の判断基準は、どう考えれば良いか。

Ａ１４. MDS のチェックリストは医療機関がリスクアセスメントを実施するための資料となる物です。リスト化され提示している場合は「はい」となります。リスト化されずに取扱説明書に記載されているだけでは「いいえ」となります。また、医療機関からの要求に応じて作成する場合も「いいえ」となりますが、備考欄にその旨記載してください。

Ｑ１５.「質問１」に関して顧客が入力する任意の情報を扱うシステムで、情報の項目が製造業者側で把握できない場合はどう考えれば良いか。

Ａ１５. 顧客が入力する任意の情報は該当しません。チェックリストが問う対象は製造業者が製品に定義し扱う情報についてのみです。

Ｑ１６.「質問１」のリストのデータは複数の情報で構成されていても良いですか？

Ａ１６. 医療機関による情報の見落としを防止するためには、データはまとまっていることが望ましいです。

Ｑ１７.「質問４．１」に関して、例えば「パスワード認証」と「生体認証」が「はい」となる場合、「二要素認証」が「はい」となるか。

Ａ１７.「パスワード認証」と「生体認証」を組み合わせて使用可能であれば「はい」と、いずれか片方のみが使用可能であれば「いいえ」になります。

Q１８.「質問4．１．１」で書かれているパスワード管理とは何ですか。

Ａ１８．安全管理ガイドラインの6.5C11 システム管理者の留意事項⑴から⑶及び利用者の留意事項⑴、⑵で記載されている内容のことです。但しシステム管理者の留意事項⑵ の「本人確認に関する内容の台帳記載」に関しては一般的には運用でカバーする内容となりますので除外して回答いただいても結構です。

Q１９.「質問4．１．１」の備考に「パスワードの登録・暗号化にのみ対応しています。パスワードの変更や類推性他の要素は運用でカバーしてください。」と記述された事例を見たことがあるが、なぜ、そのような記述になっているのですか？

Ａ１９．技術面で求められているのはＡ１８．にある通り５点あります。技術的にカバーしているのが全てでない場合は何がカバーできているのか、いないのかを備考にて記述してください。

Q２０.「質問4．３」において、どのレベルが要求されているのか分からない。

Ａ２０.「JAHIS ヘルスケア分野における監査証跡のメッセージ標準規約　Ver.2.0」※を参考にしていただくと安全管理ガイドラインの要求事項と産業界としての標準フォーマットの両方を参照いただけます。
※https://www.jahis.jp/standard/detail/id=136

Q２１.「質問5」の解説の「標準時刻」は何を持って「標準」とすべきか分からない。

Ａ２１．日本での標準時刻は NICT が決定・維持を行っている日本標準時である JST（UTC+9）となります。日本標準時との時刻同期をいかに行うかについては NTP サーバの利用等にて適宜対応してください。

Q２２.「質問6」に関して、モダリティの中には、不要なソフトウェアはインストールしない（できない）ため、インターネットに未接続であれば不正ソフトウェア対策は不要ではないか。こういった場合は「対象外」として良いか。

Ａ２２．必ずしも「対象外」として良いとは言えません。2015/4/28 の厚生労働省からの通知（http://www.mhlw.go.jp/file/05-Shingikai-11121000-Iyakushokuhinkyoku-Soumuka/0000090664.pdf）でサイバーセキュリティ対応が要求されていることもあり、リスクアセスメントの結果、受容可能でないリスクがあれば不正ソフトウェア対策は必要となります。
また、院内 LAN や USB メモリ等を経由して感染する可能性があるためインターネットに未接続であっても必ずしも安全であるとは言えません。
パターンファイル、ふるまい検知等を使用する不正ソフトウェア対策ソフトウェアをインストールすると過負荷となり画像のロスト等の運用に支障が発生する場合はホワイトリスト方式等の採用をお勧めします。
「ホワイトリスト方式」等を含むウィルス対策ソフト等の不正ソフトウェア対策がされていれば「はい」となり、採用されている不正ソフトウェア対策について備考に記述してください。
また ROM 上で動作する機器で書き込みが不可能であれば「対象外」として結構です。

Ｑ２３．「質問７」でオプションとして無線 LAN を準備している場合、「はい」、「いいえ」どちらになるか。

Ａ２３．オプションで準備している無線 LAN にセキュリティ機能がある場合は、「はい」で結構です。
※オプションの考え方については Ａ７．をご参照ください。

Ｑ２４．オプションとして無線 LAN を用意しているのではなく、ユーザ指定で無線 LAN を納品する場合は、どのような回答になるか。

Ａ２４．「いいえ」としてください。
※オプションの考え方については Ａ７．をご参照ください。

Ｑ２５．「質問７」は、物によって違うのでは。サーバとかクライアントで回答が変わるかもしれないのだが。

Ａ２５．MDS のチェックリストは販売するシステム単位や製品型番がある物に対して記入するものです。一部でも未対策の場合は「いいえ」としてください。

Ｑ２６．「質問８」で通常の操作ではソフトウェアのインストールできなければ、「はい」で良いか。

Ａ26.「はい」で結構です。

Q27.「質問１２」で医事コンシステムにレセプトオンラインを含む場合は、どうなるか。

Ａ27．外部との個人情報のやりとりがあるので「はい」としてください。

Q28.「質問１２．１」において、クライアントまで含めたシステムのチェックという認識で良いか。

Ａ28．クライアントが製品に含まれる場合は、クライアントも含みます。
※「質問１２．１」に限らず、クライアントまで含みます。

Q29.「質問１２．１」において、クライアントに対してもなりすまし対策がなされているという理解で良いか。

Ａ29．クライアントが製品に含まれる場合は、その理解で結構です。

Q30.「質問１２．３」でネットワークも含んで納品する場合、どう回答すれば良いか。

Ａ30.「はい」と回答し、備考欄に具体的な内容を記載してください。

Q31.「質問１２」と「質問１２．４」は同じことを問うているのか。

Ａ31.「質問１２」では「通信機能」または「リモートメンテナンス機能」などのネットワークで個人情報を含む医療情報を交換する機能があるかを問うており、「質問１２．４」では「リモートメンテナンス機能」に限定して問うています。

Q32.「質問１２．４．１」において、何を持って不必要とするか。製造業者と医療機関の間でギャップがありうるので両者間で協議しないと回答できないのでは。

Ａ３２．製造業者側で作成する物なので、医療機関との協議は不要です。製造業者の判断で記入してください。

Ｑ３３．「質問１３」においてモダリティは対象となるか。

Ａ３３．記名・押印が義務付けられた文書を生成する機能を有するモダリティの場合は対象となります。

Ｑ３４．「質問１４．１」において「区分」の意味する詳細な分類方法が分からない。「所見」と「処方」の違いも「区分」に入るのか。

Ａ３４．安全管理ガイドラインにおいては具体的な区分に関する規定はありません。例えばアクセス制御の際に、「所見」と「処方」に対する個別の権限管理が行われている場合には「区分」に入ります。「所見」と「処方」が区分されていなくても、システムとして適切なアクセス制御が可能な区分管理がされていれば「はい」で結構です。

「安全管理ガイドライン7章　電子保存の要求事項について」関係

Q35.「質問16」において、確定機能とはデータベースにデータを登録することなのか、変更不可にすることなのか。

A35. どちらとも言えません。記録の確定については、安全管理ガイドライン 7.1B-2⑵を参照ください。

Q36.「質問18」で、システム更新（リプレース）で製造業者が変わる場合は「いいえ」で良いか。

A36.「いいえ」で結構です。マイグレーションの場合は、新システムとしてはデータが入力されるだけであり、以前のシステムの履歴は無関係となります。

Q37.「質問18」では、製造業者が変わる場合、旧システムの履歴は対象外だが安全管理ガイドライン的にはどうか。

A37. 安全管理ガイドラインには明言されていませんが、移行時には標準形式のデータを使用することが推奨されています。

Q38.「質問21．1」で、「ネットワークの冗長化」についてはネットワークを納品しない場合は「対象外」として良いか。

A38.「対象外」として結構です。

Q39.「質問21．1」で、ネットワークI/F を複数有していれば「ネットワークの冗長化」を「はい」として良いか。

A39. 冗長動作をする機能を有していれば「はい」で結構です。

Q４０.「質問２１．２」において、外部保存サービスを利用した参照であっても「はい」で良いか。

Ａ４０.「はい」で結構です。

Q４１.「質問２１．２」において、PDF 形式で保存されているが検索機能が用意されていない場合の回答はどうなるか。

Ａ４１．SS-MIX のようにフォルダ単位である程度、分別されている場合は「はい」と答えてください。全ファイルが押しなべて同一階層に保存されていて、ファイルを開かないと内容が確認できない場合は「いいえ」としてください。

「安全管理ガイドライン８章　診療録及び診療諸記録を外部に保存する際の基準」関係

Q４２．安全管理ガイドライン８章（外部保存）の質問がチェックリストにありませんが、今後追加されるのか。

Ａ４２．検討の結果、製造業者が担保すべき事項がなかったため該当項目がありません。８ 章に関しては外部保存サービスを行っているサービサー側の内容となります。そのため、ASPIC（ASP/SaaS・クラウド　コンソーシアム）等での検討事項かと考えています。
「クラウドサービス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版)」の「ガイドラインに基づく SLA 参考例及びサービス仕様適合開示書第１版」をご使用ください。

「安全管理ガイドライン９章　診療録等をスキャナ等で電子化して保存する場合について」関係

Q４３．システムにスキャナが入っている場合、「質問１６．１」で入力者／確定者とあるがスキャナを使っている人が作成責任者となるのか。

Ａ４３．責任者と作業者が異なる場合もあるので、必ずしもスキャナを使っている人が作成責任者になるとは限りません。医療機関の運用に依ります。

Q４４.「質問２９」において、参照の利便性を目的としてスキャナによる電子化を行った場合は、どう回答すれば良いか。

A４４.「いいえ」と回答してください。電子保存を目的とする場合のみ「はい」と答えてください。

「その他」

Q４５. モダリティ、機器に製造番号がある物が本チェックリストの対象とあるが、広域で利用される地域連携ネットワークは対象となるか。

A４５. 地域連携ネットワークのように大規模なものは運用面が係ってくることもあり、MDS の対象とすることは難しいです。地域連携ネットワークを構成する個々の製品に対して各々の MDS を用意してください。

Q４６. 地域連携ネットワークにおいても、参加する医療機関から MDS の提出が求められそうだがどう対応すればよいか。

A４６. 地域連携ネットワークを構成する個々の製品に対して各々の MDS を用意してください。
MDS は個別製品用のものです。複数の製品を組み合わせて構築する地域連携システムにおいては要求仕様において三省ガイドライン（厚生労働省、経済産業省、総務省）に準拠することを求める場合が多くあり、運用も含めた対策を提案書等で提示する必要があります。厚労省の安全管理ガイドラインが求める技術的対策については MDS で説明可能ですが、それだけでは不完全なため別途個別に対応表を作成する必要があります。

Q４７. システムに外部保存の機能がある場合、「質問１２」で回答すれば良いか。

A４７. 該当する製品（システム）に含まれる場合は、通信に関する機能については「質問１２」で回答してください。外部保存サービスを提供する場合、サービスそのものは MDS の対象ではありません。経済産業省・総務省のガイドラインに適合している必要があります。

Q.４８.　MDS で言うところの製造業者とは「薬機法」における製造業の会社のことか？

A.４８.　いいえ。　医療情報システム、医療情報機器を製造している業者を指しています。

改訂履歴

2016 年９月	初版	Ver.2.0 対応
2017 年 10 月	第２版	Ver.3.0(a)対応
2018 年１月	第３版	Q&A の追加（医療機関からの問合せ対応）
2018 年 11 月	第4版	Q&A の追加（製造業者からの問合せ対応）