「製造業者による医療情報セキュリティ開示書」ガイドに関するQ&A

平成 28 年9月

（社）日本画像医療システム工業会
医用画像システム部会 セキュリティ委員会
製造業者による医療情報セキュリティ開示説明書に関するWG

目次

はじめに

本書は「MDS 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「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。） Ver.2.0 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．質問の後ろの括弧の中の番号は何を示すのか。

Ａ1．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 4.2 版の各章番号に対応するものです。

Ｑ2．MDS は医療機関から請求されて提出する物なのか、ベンダー側から積極的に提出するものなのか。

Ａ2．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医療情報システムのセキュリティ対応状況に関する説明がベンダー側も医療機関側も効率よく行えるようになることを期待しています。

Ｑ3．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。

Ａ3．結構です。受け取った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。

Q4．製造メーカと販売会社が異なる場合はどうすればよいか。

A4．一般的には製造会社が作成します。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。

「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

Q5.「質問1」の「扱う情報のリスト」とは、どういう物か。

A5．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。DICOM Conformance Statement 等でリストの代用も可能です。

Q6.「質問1」の「はい」、「いいえ」の判断基準は、どう考えれば良いか。

A6．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、公開されておらず医療機関からの要求に応じて提出する場合も「いいえ」となりますが、備考欄にその旨記載してください。

Q7.「質問1」に関して顧客が入力する PDF 等を扱うシステムで、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。

A7．顧客が入力する PDF 等は該当しません。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。

Q8.「質問1」のリストのデータはバラバラで良いか。

A8．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。

Q9.「質問4．1」に関して、例えば「パスワード認証」と「生体認証」は「はい」となる場合、「二要素認証」が「はい」となるか。

A9.「パスワード認証」と「生体認証」の両方が同時に選択できるものであれば「はい」と、いずれか片方のみが選択できるようになっているものであれば「いいえ」になります。

Q10.「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。

A10. 安全管理ガイドラインの 6.5C10-1 から 6.5C10-3 までで求められている機能が全て実装されていることです。3つ全て実装していない場合は「いいえ」となります。1つまたは2つ実装している場合は備考欄に明記してください。

Q11.「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？

A11．技術面で求められているのはA10．にある通り3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。

Q12.「質問4．2」において、どのレベルが要求されているのか分からない。

A12.「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

Q13.「質問5」の「標準時刻」は何を持って「標準」とすべきか分からない。

A13．日本での標準時刻は一般的に JST となります。

Q１４.「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。

Ａ１４. 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。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「いいえ」としてください。その場合はホワイトリスト方式等の採用をお勧めします。
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。
※JIRA から医療機器の不正ソフトウェア対策に関する文書が発行されていますので参考にしてください。
「画像診断ワークステーションのウィルス対策ソフトに関するガイドライン」
http://www.jira-net.or.jp/commission/houki_anzen/03_topics/file/20100930_JESRA_TR-0035-2010.pdf
さらに安全管理ガイドライン 6.5C9 では、システム構築時のメディアによる不正ソフトウェア混入も示しているため注意してください。

Q１５.「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。

Ａ１５. 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。

Q１６. オプションとして無線 LAN を用意しているのではなく、ユーザー指定で無線 LAN を納品する場合は、どのような回答になるか。

Ａ１６.「いいえ」としてください。

Q１７.「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。

Ａ１７. 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。

Q１８.「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。

Ａ１８.「はい」で結構です。

Q１９.「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。

Ａ１９. 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。

Q２０.「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。

Ａ２０. 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。

Q２１.「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。

Ａ２１. その理解で結構です。

Q２２.「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。

Ａ２２.「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。

Q２３.「質問１２」と「質問１２．４」は同じことを問うているのか。

Ａ２３.「質問１２」では「通信機能」または「リモート保守機能」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」に限定して問うています。

Q２４.「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。

Ａ２４．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。

Q２５.「質問１３」においてモダリティは対象となるか。

Ａ２５．一般的にはモダリティは対象外となります。ただし例外として記名・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。

Q２６.「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。

Ａ２６．入ります。

「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

Q27.「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。

A27. 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-2(2)を参照ください。

Q28.「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。

A28.「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。

Q29.「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。

A29. 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。

Q30.「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。

A30.「対象外」として結構です。

Q31.「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。

A31. 冗長動作をするように設定されていれば「はい」で結構です。

Q３２.「質問２２」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。

Ａ３２.「はい」で結構です。

Q３３.「質問２２」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。

Ａ３３. 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

Q３４. 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。

Ａ３４. 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。

「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

Q３５. システムにスキャナが入っている場合、「質問１６」で確定責任者／作成責任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。

Ａ３５. 紙の原本をスキャンして、それを原本とした場合にはそうなります。

Q３６.「質問３０」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。

Ａ３６.「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」

Q３７. 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。

Ａ３７. 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。

Q３８. 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。

Ａ３８. 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。

Q３９. 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。

Ａ３９. 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は経済産業省・総務省のガイドラインに適合している必要があります。

改訂履歴

初版	Ver.2.0 対応