「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」

Ver. 5. 0

医療機関等向けユーザーズガイド

（「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」対応）

２０２４年　１２月

JIRA - JAHIS 合同開示説明書 WG

目次

「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」とは

「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」（以下、MDS/SDS とする。）とは、各製造業者/サービス事業者の医療情報システムのセキュリティ機能に関する説明の標準的記載方法（書式）を JIRA /JAHIS で定めたものです。

製品/サービスの説明の一部として製造業者/サービス事業者によって作成され、セキュリティマネジメントを実施する医療機関等を支援するため、以下の用途に用いられることを想定しています。

（1） 製造業者が提供する医療情報システム、又はサービス事業者が提供する医療情報システムを用いたサービス（以下、「対象とするシステム/サービス」とする。）のセキュリティに関して、厚生労働省から発行されている「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」とする。）への適合性を示すことにより、医療機関等側において必要な対策の理解を容易にすること。

（2） 安全管理ガイドラインを遵守しなければならない医療機関等にとって有用な情報を提供すること。当該システム/サービスを導入する医療機関等においてセキュリティマネジメントを実施する際に、製造業者/サービス事業者により提供される情報がリスクアセスメントの材料となること。

（3） 各製造業者/サービス事業者が、安全管理ガイドラインへの適合性への自己評価手段として利用すること。

（4） 医療機関等が、製造業者/サービス事業者にセキュリティの説明を求める際に、要求のベースとして利用すること。

・本書式での記載対象の単位は、製造業者の製品として提供される医療情報システム、又はサービス事業者による医療情報システムを用いたサービスです。例えば、ある型式の製品及びそのオプション、または、ある名前のサービス及びそのオプションとして提供される機能の一式です。その中に他の製造業者の製品（例えば OS やミドルウェア）を含むならば、それによって実現される機能も記載対象に含まれています。

・チェックリストの項目は以下の通りになっています。

チェックリスト（製造業者編）

1	～	12	個人情報を含むデータを扱うすべての医療機関等で参照されるべき内容です。
13	～	29	保存義務のある診療録等を電子的に保存する場合の内容です。
30	～	31	診療録等をスキャナ等により電子化して保存する場合の内容です。

チェックリスト（サービス事業者編）

1			医療機関等とサービス事業者の契約に関する内容です。
2	～	76	個人情報を含むデータを扱うすべての医療機関等で参照されるべき内容です。
77	～	104	保存義務のある診療録等を電子的に保存する場合の内容です。
105	～	106	診療録等をスキャナ等により電子化して保存する場合の内容です。

「安全管理ガイドライン」の経営管理編、企画管理編及びシステム運用編の各章の「遵守事項」には、技術的対応項目と運用も含めた対応項目とが含まれています。ＭＤＳについては、技術的対応項目の中で製品に関連する内容が、一方、ＳＤＳについては、運用に関する対応項目も含むサービス事業者に関する内容も記載されています。

関連する機能に関しては「該当」、「非該当」で回答し、それ以外の質問では「はい」、「いいえ」、「対象外」で回答する形になっています。また、対象とするシステム/サービスが未対応で回答が「いいえ」となっている場合には、備考にて運用による代替手段を記載するか、補足事項を追記する形にしています。

MDS/SDS の書式は、JIRA/JAHIS 合同の開示説明書 WG にて作成し、記述方法、解説を加えた JESRA/JAHIS 標準「「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」ガイド」（以下、ガイド）、Q&A 集と共に JIRA/JAHIS のホームページにて公開しています。

なお、「安全管理ガイドライン」や厚生労働省通知「医療機器のサイバーセキュリティの確保に関するガイダンスについて」等において、情報セキュリティを適切に管理する際に、参考にする文書として取り上げられており、HELICS 指針としても採択されています。

また、サイバーセキュリティ対策チェックリストにおいて、MDS/SDS の授受について確認する質問が設けられています。

「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）の入手と利用

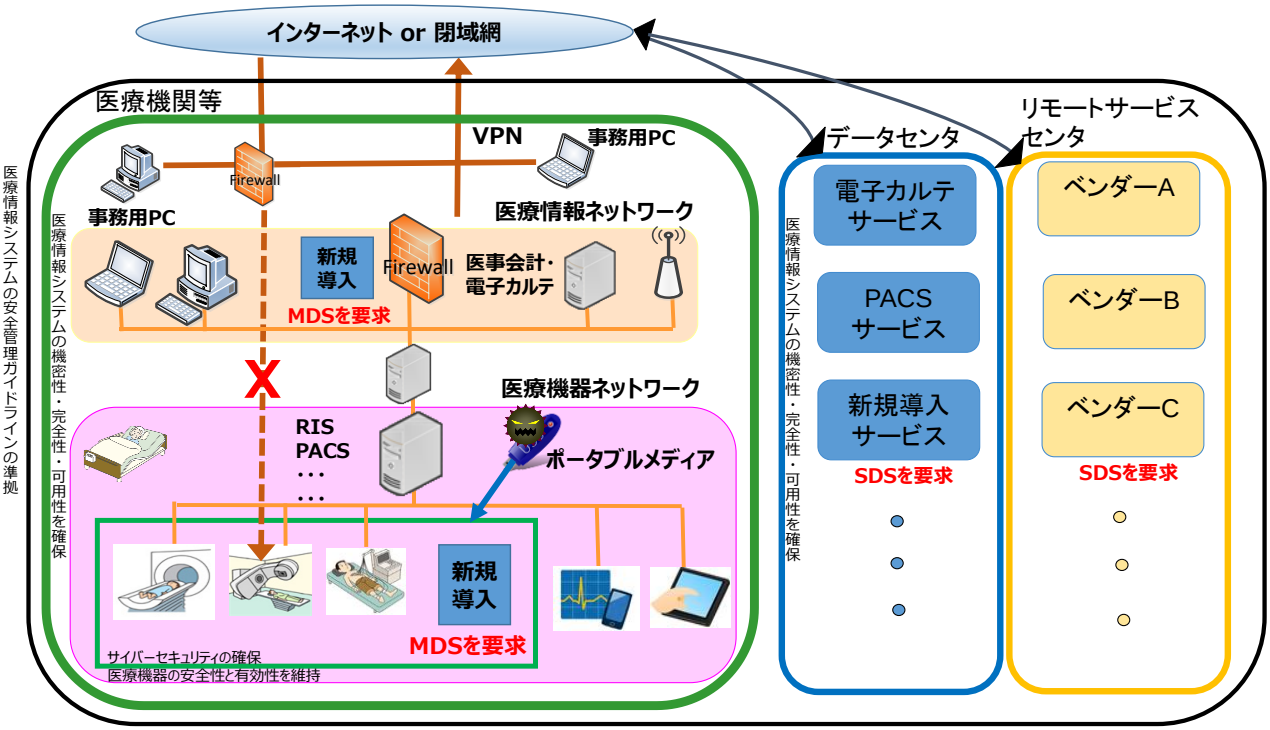
医療機関等は製造業者/サービス事業者に対し、対象とするシステム（医療機器を含む）/サービス毎にMDS/SDSを要求し入手してください。なお、オンプレミスのシステムでリモートメンテナンスを受けている場合は、リモートメンテナンスに関するSDSを要求し入手してください。対象とするシステム/サービスのMDS/SDSが未作成の場合は、作成するよう要求してください。

医療機関等は「安全管理ガイドライン」の遵守が求められており、医療機関等全体としては医療機関等が主体となって、医療情報システムの製造業者/サービス事業者の協力を受けつつ、安全管理ガイドラインに則って機密性・完全性・可用性を確保するために対象とするシステム/サービスの安全管理を行う必要があります。

一方、医療機器に関しては、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（以下、薬機法という。）における製造販売業者が厚生労働省通知「医療機器におけるサイバーセキュリティの確保について」に則ってサイバーセキュリティの確保を行う必要があります。

さらに、医療法施行規則の改正により、病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティを確保するために必要な措置を講じなければならないとされました。

このように医療機関等は対象とするシステム/サービスのリスクアセスメントを行うことが必要となります。MDS/SDSはリスクアセスメントを行う際に利用でき、安全管理ガイドラインに対する準拠性が確認できます。対象とするシステム/サービスの情報セキュリティに関する情報を入手することによって、効果的にリスクアセスメントを実施し、有効な技術的対策や運用的対策を立てることができます。



医療機関等が、製造業者/サービス事業者にセキュリティ対応状況を確認する際に、独自のフォーマットを使用することに比べて、MDS/SDS を利用することには以下のメリットがあります。

- 製造業者/サービス事業者に依存せず、標準化された書式で情報が記載されているため、セキュリティ対応状況の比較や把握が容易になる。
- 医療機関等内の各部門で使用している対象とする全てのシステム/サービスのセキュリティ状況の把握が容易になる。
- 独自のフォーマットに比べて、比較的迅速な回答が得られる。

その結果、安全管理ガイドラインに適合した運用管理規程の作成や改訂が容易になり、運用に大いに役立つことが期待されます。

- JIRA/JAHIS は本ドキュメントの作成、メンテナンス、普及活動を実施しています。

- MDS/SDS の記載内容は各製造業者/サービス事業者の自己宣言となります。記載された内容については、情報を記載した製造業者/サービス事業者が全責任を負います。

- MDS/SDS の書式及びガイドを作成した JIRA/JAHIS は、各製造業者/サービス事業者の情報を記載した MDS/SDS に関して認証・試験・検査等は行っておりません。
また、MDS/SDS は特定の医療機関等における特定の目的・ニーズを満たすこと、又は個々の製品もしくはサービスの性能を保証するものではありません。

Annex　Q&A 集

はじめに

本 Q&A 集は MDS/SDS に関して医療機関等から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 /SDS Ver.5.0 における番号を指します。
※本書並びに本書に基づいたシステム/サービスの導入・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．　この開示書を利用する上での前提は？

Ａ1．　安全管理ガイドラインを理解されている事です。
なお、MDS/SDS には医療情報システム/サービスを利用する医療機関等における運用的手段で行うように求められている要件の質問は含まれておりませんのでご注意ください。

Ｑ2．医療機関等が立入検査及び個別指導等を受ける際の資料として MDS/SDS が使用できるか？

Ａ2．　はい。サイバーセキュリティ対策チェックリストにおいて、MDS/SDS を入手しているか否かが確認されていますので、各システムの MDS./SDS そのものが必要です。また、MDS/SDS は立入検査等への対応資料を作成するための材料として活用いただけます。ただし、そのままでは使用できません。MDS/SDS は安全管理ガイドラインが求める機能/サービスを提供しているかどうかを示す物であり、それらを医療機関等が実際に運用していることを示すものではないためです。

例えば、MDS/SDS で二要素認証が「はい」となっていても、実際に使用されているかどうかは医療機関等の運用となり、機能又はサービスを有していることと、医療機関等で運用されているかどうかは別の問題となります。

Ｑ3．ガイドの質問の後ろの括弧の中の番号は何を示すのか？

Ａ3．ガイドの質問項目の後ろの括弧内に記載されている番号は、対応する安全管理ガイドラインの各章番号です。

Q4．MDS/SDS は医療機関等から請求して提出されるものなのか、製造業者/サービス事業者側から積極的に提出するものなのか？

A4．MDS/SDS は製造業者/サービス事業者から自発的に開示することを想定したものですが、業者から自発的な開示が無い場合は請求してください。

Q5．MDS/SDS の具体的なメリットは何ですか？

A5．統一フォーマットを使用することにより、医療機関等における各製造業者/サービス事業者からの医療情報システム/サービスのセキュリティ対応状況の把握、情報収集が効率よく行えるようになります。

Q6．オプションの考え方（定義）がよく分からない。

A6．MDS/SDS 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。

Q7．医療機関等の要望により機能を追加する場合、MDS/SDS の回答が変わるのでしょうか？

A7．その医療機関等向けにカスタマイズしたものは、MDS/SDS には原則として反映されません。（カスタマイズが汎用機能としてパッケージやサービスに取り込まれる場合を除く）個別のカスタマイズの安全管理ガイドラインへの対応については納品仕様書等を確認の上、ご判断ください。

Q8．MDS/SDS のチェックリストは安全管理ガイドラインの遵守事項を網羅しているのか？

A8．MDS/SDS のチェックリストは、安全管理ガイドラインの遵守事項の項目の中で製造業者/サービス事業者が提供する個々の医療情報システム/サービスのセキュリティに関わる項目に関して抜粋して記載しています。よって医療機関等での運用のみによる項目等に関しては除外されています。

各ベンダーの MDS/SDS を集めることにより、医療機関等全体のリスクアセスメントを実施するための材料としてご使用いただけます。

Q9．質問の内容に対して部分的に未対応な場合でも「はい」と回答され、備考に未対応内容が記されているのか？

A9．一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するルールとなっています。「はい」と回答されている場合は全てについて対応できている場合になります。

Q10．　安全管理ガイドラインで技術的対応が求められている事項に「いいえ」の回答がされている事項には、医療機関等はどうすれば良いのか？

A10．　医療情報システムを利用するに当たっては技術的対応を求められている項目ですので、例えば他の製品やサービスと組み合わせて実現したり、カスタマイズ開発によって実現したりすることが求められます。
MDS/SDS においては「いいえ」の場合は備考に代替手段を記載することを求めております。それを参考にしてご対応いただいても結構ですし、記載されていない場合や、記載されていても他の代替手段の方が有効なことも考えられますので、当該製品/サービスの採否を含め医療機関等にてご判断ください。

Q11．オプションで対応可能な場合は「はい」と回答されているのか？

A11．オプションの内容が備考に記載されていれば、「はい」とされています。

Q12．　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？

A12．　いいえ、医療情報システム、医療情報機器を提供している業者を指しています。

「MDS/SDS の対象システムへの該当・非該当について」

Q13．モダリティ機器等、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。

A13．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関わってくることもあり、全体を単一の MDS/SDS で網羅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/サービスに対して各々の MDS/SDS を入手してください。

Q１４.【医療機関より】CT の製造販売会社とリモートメンテナンスなどのセキュリティ対策や責任分界点の協議を行っています。その製造販売会社は CT は医療機器であり、医療情報システムではないため「医療情報システムの安全管理に関するガイドライン」や「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」の対象ではないため対応しないでよい、と回答されました。

Ａ１４. 厚生労働省から発行されている「医療情報システムの安全管理に関するガイドライン」は、薬機法上の医療機器であるかどうかにかかわらず、医療情報を扱うシステムを対象としています。厚生労働省から発行された「医療機関における医療機器のサイバーセキュリティ確保のための手引書について」※1において、医療に関する患者情報（個人識別情報）を含む情報を取り扱う医療機器であれば「医療情報システムの安全管理に関するガイドライン」の対象範囲内にあることが示されています（図 1 参照）。

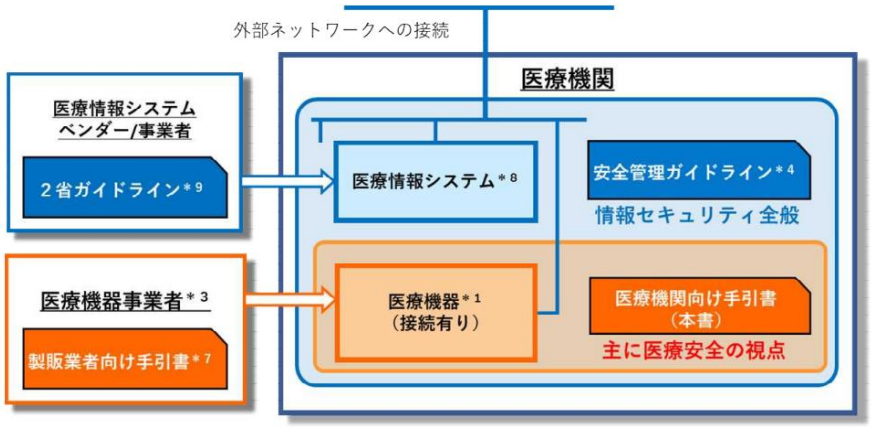


図 1　医療機関向け手引書と安全管理ガイドライン等の位置付け（イメージ）

（※1）出典：厚生労働省「医政参発 ０３３１ 第1号　医療機関における医療機器のサイバーセキュリティ確保のための手引書について」からの引用
https://www.mhlw.go.jp/content/11120000/001094637.pdf

Q１５.　当院では、Office や Google Workspace(GWS)などの表計算ソフトや文章作成ツール(Word など)で患者情報のデータベース作成や院内共有を行っています。

- マイクロソフト社→Office 購入→利用
- Google 社→代理店→GWS 利用

この場合、MDS や SDS はどこに提出依頼したらよいでしょうか？

Ａ１５. Office や Google workspace(GWS)は、製造業者の製品として提供される医療情報システム又はサービス事業者による医療情報システムを用いたサービスではありませんので MDS/SDS の対象外となります。

医療情報を扱うシートなどの作成を医療機関自らが行っている場合は、MDS/SDS の作成は不要です。

医療情報を扱うシートなどの作成を外注している場合、

・準委任契約（いわゆる委託）のケースでは、医療機関の責任であるため不要

・請負契約のケースでは、受託事業者に作成責任が発生するのでMDSあるいはSDSの提出が必要と考えます。

「医療機関等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」関係

Q１６．MDSの「質問１」、SDSの「質問２」の「扱う情報のリスト」とは、どういうものか？

Ａ１６．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あります。システムにもよりますがDICOM Conformance Statement等をリストとしている場合があります。

但し、予め製品に定義されている項目を対象としており、医療機関等で任意に扱う項目は該当しません。

Q１７．MDSの「質問１」、SDSの「質問２」の「はい」、「いいえ」の判断基準は、どう考えれば良いか？

Ａ１７．判断基準は取り扱う情報がリスト化されているか否かです。リスト化されている場合は、情報の集約が容易に行え、「はい」と回答されます。一方、リスト化されていない場合は、医療機関等が取扱説明書・仕様書等から情報を集約する必要があり、「いいえ」と回答されます。

また、機能のカスタマイズ等により医療機関等からの要求に応じてリストを個別に作成する場合は「いいえ」となります。この場合、MDS/SDS上では「いいえ」ですが、医療機関等としての個別のリストの入手はできているため安全管理ガイドライン上は問題ありません。

「技術的安全対策」関係

Q１８．MDSの「質問４．１」、SDSの「質問１７．１」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？

Ａ１８．「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」、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。

Q１９．MDS の「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？

Ａ１９．安全管理ガイドラインの システム運用編１４ ②⑥で記載されている内容のことです。但し⑥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される場合があります。

Q２０．MDS の「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？

Ａ２０．技術面で求められている内容は安全管理ガイドラインのシステム運用編１４ ②⑥で記載されている通り５点あります。技術的にカバーしている項目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確認してください。

Q２１．MDS の「質問5」、SDS の「質問１８」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．MDS の「質問7」、SDS の「質問２２」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？

Ａ２２．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」となります。
※オプションの考え方については A6．をご参照ください。

Q２３．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っているか？

Ａ２３．「いいえ」という回答になっています。
※オプションの考え方については A6．をご参照ください。

「見読性の確保について」関係

Q２４．MDSの「質問２１．２」、SDSの「質問９５．２」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？

Ａ２４．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」となります。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」となります。

「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

Q２５．システムにスキャナが入っている場合、MDSの「質問１６．１」、SDSの「質問８１．１」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。

Ａ２５．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。医療機関等の運用に依ります。

改訂履歴

２０２１年　５月	初版	Ver.４．０対応
２０２３年　９月	第２版	Ver.４．１対応
２０２４年 １２月	第3版	Ver.５．０対応