JAHIS

ＪＡＨＩＳ標準　１３－００３

Japanese Association of Healthcare Information Systems Industry

製造業者による医療情報セキュリティ開示説明書

２０１３年４月

一般社団法人 保健医療福祉情報システム工業会

セキュリティ委員会

JAHIS-JIRA 合同開示説明書 WG

製造業者による医療情報セキュリティ開示説明書

ま　え　が　き

JAHIS と JIRA にて医療情報セキュリティ開示説明書に関する合同ワーキングを立ち上げた。合同ワーキングとなる前に JIRA で 2011 年 12 月に第 1 版の文書が発行されている。本文書は JIRA セキュリティ委員会にて作成された第 1 版を JAHIS 標準として採用したものである。
以下の序文以降は JIRA で発行された第 1 版と書式以外は同一であるが、団体名が「JAHIS」となっている箇所は JIRA 版では「JIRA」と記載されていた箇所である。

2013 年 4 月

一般社団法人　保健医療福祉情報システム工業会
セキュリティ委員会
JAHIS－JIRA 合同開示説明書 WG

序文

近年の情報技術の進歩は目覚しく、社会的にも情報化の要請は一層高まりつつあります。医療情報においても、医療情報システムの導入及びそれに伴う外部保存を行う場合の取扱いに関し、個人情報保護法や e-文書法への適切な対応の総合的な指針として，厚生労働省から「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略す）が発行されています。

各製造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には標準的記載方法の定めがなく、その記載レベルもさまざまであるのが現状です。このことは、医療機関内のトータルシステムの構築を担う担当組織においては、各システム間の整合性を取る際の支障であり、各医療機関で独自に策定した書式にその都度製造業者が対応することもまた、業務の効率化を妨げることにもなります。

そこで、JIRA 医用画像システム部会セキュリティ委員会は、製造業者による製品のセキュリティに関する説明を、日本での標準書式とすることを想定して「製造業者による医療情報セキュリティ開示説明書(略称：開示説明書)」を作成しました。この標準的な書式を用いることにより、製造業者と医療機関の双方にとって効率的なシステム構築が進むことを目的としています。

本書の意図は、医療機関が医療情報システムによって送信され維持される健康情報に関するリスクアセスメントおよびリスクマネージメントを行うとき、それを支援できる重要な情報を提供することにあります。製造業者は、標準化された書式を使用することにより、自らが製造する医療情報システムのセキュリティ関連機能に関して、医療機関から情報提供を要求されたとき迅速に答えることができます。一方、医療機関は、標準化された書式の記載により、製造業者によって提供されるセキュリティ関連情報のレビューを行い易くなります。

この文書は、安全管理ガイドライン 4.1 版(2010.2 発行)に基づく開示説明書と、この書式の記入方法の解説とからなっています。また、読者の知識としては、安全管理ガイドライン(特に第 6 章)の理解を前提にしています。

2011 年　12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

第１章　適用範囲

本書にて規定する書式の記載内容は、製品説明の一部として製造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を支援するため、以下の用途を想定しています。

（1）製造業者が提供する医療情報システムのセキュリティ機能に関して、安全管理ガイドラインの第6章への技術的な適合性を示すことにより、医療機関側において必要な運用的対策の理解を容易にすること。

（2）安全管理ガイドラインに適応しなければならない医療機関にとって有用な情報を提供すること。
当該システム導入医療機関においてセキュリティマネジメントを実施するにあたって、製造業者により提供される情報をリスクアセスメントの材料とすること。

（3）各製造業者にとって、安全管理ガイドラインへの適合性の自己評価手段として利用すること。

（4）医療機関が製造業者にセキュリティ機能の説明を求める際の、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です。例えば、ある型名の製品とそのオプションとして一まとまりに提供される機能の一式です。その中に他製造業者の品(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めます。

さらに、本書の書式は、個々の医療情報システムにおける技術的セキュリティ関連機能の具体的内容の記載を可能としています。

本書式の使用は強制されるものではありませんが、多くの箇所で利用されて標準となることを目指し、さらには各製造業者がホームページなどで公表することを期待しています。

本書式を作成したJAHISは、製品設計・設置・保守等の認証・試験・検査等は行わず、特定の医療機関における特定の目的･ニーズを満たすこと、あるいは個々の製品またはサービスの性能を保証するものではありません。この書式への記入内容は、記入した製造業者が全責任を負います。

第２章　引用規格・引用文献

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4.1版
http://www.mhlw.go.jp/shingi/2010/02/s0202-4.html

HIMSS/NEMA Standard HN 1-2008 Manufacturer Disclosure Statement for Medical Device Security
http://www.jira-net.or.jp/commission/system/04_information/information.html#02-05

（財）医療情報システム開発センター・医療情報システム安全管理評価制度（PREMISS）　自己評価ファイル（様式6）
http://premiss.medis.or.jp/download.html

第３章　用語の定義

e-文書法
「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」の通称

生体認証
人間の身体的特徴の情報を用いて個人の認証を行う行為のことを言う。バイオメトリクス(biometrics)認証 とも呼ばれる。

管理区域
情報資産を守るために、医療機関によって定められた特別な管理を必要とされる区域。

経路制御
ルーティングとも呼び、ネットワーク上で IP パケットを目的地に転送するための、パケットの通り道（経路）についての情報を管理し、最適な経路を選択する仕組み。

プロトコル制御
標準規格などで定められた通信手順などの各種プロトコル(ネットワークを介してコンピュータ同士が通信を行う上で、相互に決められた約束事の集合）を実装した機器やソフトウェアにおいて、プロトコルに従った処理手順を適切に実行できるようにするために組み込まれた仕組みのこと。

特定認定認証局
電子署名法にて定められている認定認証事業者により運用される電子認証局。

真正性
正当な権限において作成された記録に対し、虚偽入力、書き換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であることである。なお、混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性を誤ったりすることをいう。(安全管理ガイドラインより引用)

クリアスクリーン
個人端末のセキュリティ管理に関する概念。機密漏えいの防止、情報等に対する不正操作の防止を目的とした対策で、離席時に端末の表示を見られないようにログオフ等をすること。

機密性
正当な人間のみ対象資源にアクセスできるよう、管理されている状態を指す。

オブジェクト・セキュリティ
情報資産に対する安全対策のこと。例えばファイルの暗号化や改ざん検知のための電子署名付与などの対策を指す。

チャネル・セキュリティ
通信経路に対する安全対策のこと。VPN や IPSec などの対策を指す。

セキュリティターゲット
″ISO/IEC　15408:情報セキュリティ評価基準（CC ： Common Criteria）″にて用いられている概念。情報システムが備えるべきセキュリティに関する目標を記載したセキュリティ設計仕様書のことを指す。

タイムスタンプ
電磁的な情報に対し、ある時点で存在したことやその時点から改ざんされていないことを証明するために、第三者機関の発行した日時情報を電子署名化して添付したもの。

第４章　記号および略語

本開示文書では、次の記号および略語・表記を用います。

CAdES	CMS Advanced Electronic Signatures
HPKI	Health Public Key Infrastructure
IPSec	Security Architecture for Internet Protocol
JIRA	Japan Industries Association of Radiological Systems
OSI	Open Systems Interconnection
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Socket Layer
VPN	Virtual Private Network
XAdES	XML Advanced Electronic Signatures

第５章　チェックリスト

５．１　チェックリストの書き方

チェックリストは二部構成となっています。最初のパートはチェックリストそのものであり、もう一つのパートは、チェックリストの過不足を記載する備考欄です。チェックリストは質問に対する項目を選択する形式、備考欄は自由記述形式になっております。チェック項目の後ろにある括弧内の数字は、対応する安全管理ガイドラインの各章番号を表しています。

チェックリストの項目は以下の通りとなります。

（1）基本情報

製造メーカ　：対象となる製品の製造業者の名称を記述する。
製品名称　：製品の名称・型名を記述する。
バージョン　：製品のバージョン（版番号）を記述する。
作成日　：チェックリストの記載日を記述する。

（2）質問項目

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4.1 版の各章番号に対応するものです。

はい　：質問に対応している場合に選択する。オプションの場合は備考欄にその旨を記述する。
いいえ　：質問に対応していない場合に選択する。
対象外　：製品の対応する機能でない場合に選択する。
備考　：”備考記載欄”に対応する番号を記述する。実際の内容は”備考記載欄”に記述する。
備考欄には、機能の補足説明や”はい””いいえ””対象外”では説明しきれない内容等を自由に記述ください。

（3）備考記載欄

左欄に”備考”にて明示した番号を記述し、右欄に内容の記述を行います。安全管理ガイドラインの改定などにより、本書式が最新の安全管理ガイドラインに対応していない場合、JAHIS が本書式の改訂を行うまでの間、不整合箇所について本備考記載欄にて記載することにより対応を行うこととしてください。

５．２　チェックリスト

製造メーカ　：	作成日　：
装置名称　：	バージョン　：

医療機関における情報セキュリティマネジメントシステムの実践（6.2）

1　扱う情報のリストを提示してあるか？（6.2.C1）　はい　いいえ　対象外　備考____

物理的安全対策（6.4）

2　窃視防止の機能があるか？（6.4.C5）　はい　いいえ　対象外　備考____

技術的安全対策（6.5）

3　不正入力防止の機能があるか？（6.5.C3）　はい　いいえ　対象外　備考____

4　アクセス管理の機能があるか？（6.5.C1、6.5.C5）　はい　いいえ　対象外　備考____

４．１　アクセス管理の認証方式は？（6.5.C1）

・パスワード認証　はい　いいえ　対象外　備考____

・生体認証　はい　いいえ　対象外　備考____

・物理媒体認証　はい　いいえ　対象外　備考____

・二要素認証　はい　いいえ　対象外　備考____

・その他（具体的な方法を備考に記入してください）　はい　いいえ　対象外　備考____

４．１．１　パスワードを利用者認識手段として利用している場合、パスワード管理は可能か？
（6.5.C10-1～6.5.C10-3）　はい　いいえ　対象外　備考____

４．２　アクセスログを出力する機能があるか？（6.5.C6）　はい　いいえ　対象外　備考____

４．２．１　アクセスログを利用者が確認する機能があるか？（6.5.C6）
はい　いいえ　対象外　備考____

４．２．２　アクセスログへのアクセス制限が出来るか？（6.5.C7）
はい　いいえ　対象外　備考____

5　時刻情報の正確性を担保する仕組みがあるか？（6.5.C8）　はい　いいえ　対象外　備考____

6　不正ソフトウェア対策を行っているか？（6.5.C9）　はい　いいえ　対象外　備考____

7　無線 LAN を利用する場合のセキュリティ対策機能はあるか？（6.5.C.11）
はい　いいえ　対象外　備考____

情報および情報機器の持ち出しについて（6.9）

８　ソフトウェアのインストールを制限する機能があるか？（6.9.C9）　はい　いいえ　対象外　備考____

９　外部入出力装置の機能を無効にすることができるか？（ 6.9 ）　はい　いいえ　対象外　備考____

１０　管理区域外への持ち出しの際、起動パスワード等のアクセス制限を設定できるか？（6.9.C6、6.9.C7）
はい　いいえ　対象外　備考____

災害等の非常時の対応（6.10）

１１　非常時機能又は、非常時アカウントを持っているか？（6.10.C1）　はい　いいえ　対象外　備考____

外部と個人情報を含む医療情報を交換する場合の安全管理（6.11）

１２　外部と個人情報を含む医療情報を通信する機能やリモート保守機能を有するか？（6.11.C1）
はい　いいえ　対象外　備考____

１２．１　なりすましの対策（認証）機能を有するか？（6.11.C3）　はい　いいえ　対象外　備考____

１２．２　データの暗号化（SSL、S/MIME、ファイル暗号化など）が可能か？（6.11.C5）
はい　いいえ　対象外　備考____

１２．３　ネットワークの経路制御・プロトコル制御に関わる機能を有しているか？（6.11.C4）
はい　いいえ　対象外　備考____

１２．３．１　ネットワークの経路制御・プロトコル制御に関わる機能は、安全管理ガイドラインを満たす設定が可能か？（6.11.C4）　はい　いいえ　対象外　備考____

１２．３．２　ネットワークの経路制御・プロトコル制御に関わる機能の適正さを証明できる文書があるか？（6.11.C4）　はい　いいえ　対象外　備考____

１２．４　リモートメンテナンス機能を有するか？（6.11.C7）　はい　いいえ　対象外　備考____

１２．４．１　リモートメンテナンスサービスに関し、不必要なリモートログインを制限する機能があるか？（6.11.C7）　はい　いいえ　対象外　備考____

法令で定められた記名・押印を電子署名で行うことについて（6.12）

１３　記名・押印が義務付けられた文書を扱っているか？（6.12.C.(1)）　はい　いいえ　対象外　備考____

１３．１　HPKI 対応もしくは特定認定認証局が発行する証明書対応の署名機能があるか？（6.12.C.(1)）
はい　いいえ　対象外　備考____

１３．２　HPKI 対応もしくは特定認定認証局が発行する証明書対応の検証機能があるか？（6.12.C.(1)）
はい　いいえ　対象外　備考____

１３．３　日本データ通信協会認定のタイムスタンプが付与可能か？ (6.12.C.(2))

はい　　いいえ　　対象外　　備考____

１３．４　日本データ通信協会認定のタイムスタンプが検証可能か？ (6.12.C.(2))

はい　　いいえ　　対象外　　備考____

１３．５　保存期間中の文書の真正性を担保する仕組みがあるか？ (6.12.C.(2))

はい　　いいえ　　対象外　　備考____

備考記載欄	

第６章　チェックリストの解説

６．１　「１　扱う情報のリストを提示してあるか？（6.2.C1)」

本項目は、安全管理ガイドライン「6.2.2　取扱い情報の把握」の考え方に基づいてシステムにおけるリスク分析を行うため、扱う情報をすべてリストアップしているかを確認するものです。

情報システムで扱う情報をすべてリストアップしている場合は、「はい」、そうでない場合は「いいえ」と回答してください。「対象外」である場合や、リストが一部不足している等、補足説明が必要な場合は備考に記載してください。

６．２　「２　窃視防止の機能があるか？（6.4.C5)」

本項目は、安全管理ガイドライン「6.4　物理的安全対策」の考え方に基づいて窃視防止対策を有するかを確認するものです。

窃視防止の対策がされている場合には「はい」、そうでない場合には「いいえ」、対象機器が本項目に該当しない場合は「対象外」と回答してください。補足事項がある場合は、備考に記載してください。

６．３　「３　不正入力防止の機能があるか？（6.5.C3)」

本項目は、不正入力を防止する対策を有するかを確認するものです。

長時間離籍の際に不正入力の恐れがある場合は、クリアスクリーン等の対策がされている場合には「はい」、そうでない場合には「いいえ」、対象機器が本項目に該当しない場合は「対象外」と回答してください。補足事項がある場合は、備考に記載してください。

６．４　「４　アクセス管理の機能があるか？（6.5.C1、6.5.C5)」

医療情報システムの利用者の識別、認証が可能である場合は”はい“、出来ない場合は”いいえ“としてください。アクセス管理を機能的な面から必要としない場合は “対象外”としてください。
なお、本項への回答は安全管理ガイドライン”6.5 技術的安全対策”の”B. 考え方“をよく理解してください。

６．４．１　「４．１　アクセス管理の認証方式は？（-)」

アクセス管理の認証方式として利用可能なものを以下の中からお答えください。(複数回答可)

パスワード、生体計測(生体認証)、物理媒体、その他の場合は具体的な認証方式を備考に記載してください。

６．４．１．１　「４．１．１　パスワードを利用者認識手段として利用している場合、パスワード管理は可能か？（6.5.C10-1～6.5.C10-3)」

パスワードを利用者認識手段として利用している場合、パスワードが管理可能である場合は“はい”、出来ない場合は”いいえ“としてください。本項目に記載されているパスワード管理においては、パスワードが暗号化されていることと、安易に類推されないための手段の両方を有する必要があります。

６．４．２　「４．２　アクセスログを出力する機能があるか？（6.5.C6)」

製品にアクセスログを出力する機能がある場合は“はい”としてください。

６．４．２．１　「４．２．１　アクセスログを利用者が確認する機能があるか？（6.5.C6)」

アクセスログにおいて操作者、アクセスした時間(ログイン時刻、操作時間)、アクセスした個人情報を特定し、確認を行う手段がある場合は“はい”としてください。

６．４．２．２　「４．２．２　アクセスログへのアクセス制限が出来るか？（6.5.C7)」

個人情報を含むアクセスログに対して、アクセスする操作者を制限することが可能であり、かつ不当な削除／改ざん／追加等を防止する機能を有している場合は“はい”としてください。

６．５　「５　時刻情報の正確性を担保する仕組みがあるか？（6.5.C8)」

医療情報システムが、アクセス記録に使用される時刻情報に対して、標準時刻と時刻同期手段を有している場合は“はい”としてください。

６．６　「６　不正ソフトウェア対策を行っているか？（6.5.C9)」

不正ソフトウェア対策（たとえばコンピュータウイルスの検出機能と駆除機能）を有している場合は“はい”としてください。コンピュータウイルス対策ソフトを使用する場合、定期的にパターン定義ファイルの更新が必要になります。具体的な対策や制約等がある場合は備考に記載してください。

６．７　「７　無線LANを利用する場合のセキュリティ対策機能はあるか？（6.5.C.11)」

無線LANを使用している場合にセキュリティ対策機能がある場合は“はい”としてください。なお、無線LANの使用を認めていない場合は“対象外”としてください。具体的な利用可能なセキュリティ機能に関しては備考に記載してください。

※　総務省発行の「安心して無線LAN を利用するために」を参考に記載してください。最新は平成19年に改訂されています。

６．８　「８　ソフトウェアのインストールを制限する機能があるか？（6.9.C9)」

本項目は、システムとしてソフトウェアのインストールを制限する機能が有するかを確認するものです。例えば、ファイル交換ソフト（Winny等）のような不適切な設定のされた外部ソフトウェアにより情報が漏えいする可能性があるため、外部から持ち込まれたソフトウェアのインストールを制限する等の情報漏えい対策が必要となります。

システム側で、ソフトウェアのインストールを制限する機能がある場合には「はい」、制限する機能が無い場合には「いいえ」、ソフトウェアのインストール自体が出来ない場合には「対象外」としてください。

６．９　「９　外部入出力装置の機能を無効にすることができるか？（ 6.9)」

本項目は、外部入出力装置（DVDドライブ、USBメモリー等）の機能を無効にすることが出来るかを確認するものです。外部入出力装置の機能を無効にすることで、コンピュータウィルスなどの進入防止や情報漏洩防止等の情報の持ち出しを制限することが可能となります。

外部入出力装置の機能を無効にすることができる場合には「はい」、出来ない場合には「いいえ」、外部入出力装置を持たない場合には「対象外」としてください。

６．１０　「１０　管理区域外への持ち出しの際、起動パスワード等のアクセス制限を設定できるか？(6.9.C6、C7)」

本項目は、ノートパソコンのような情報端末や心電系のようなポータブル機器等の情報記録可搬媒体を管理区域外へ持ち出す際に、起動パスワード等のアクセス制限の設定で使用制限が可能かを確認するものです。情報端末やポータブル機器の場合には、盗難、紛失、置忘れ等のリスクが存在するため、これらのリスクに対応した情報漏えい対策が必要となります。

情報端末やポータブル機器等に、起動時パスワード等のアクセス制限を設定できる機能がある場合には「はい」、無い場合には「いいえ」、物理的に管理区域外へ持ち出しができない場合や情報を保有していない場合には「対象外」としてください。

６．１１　「１１　非常時機能又は、非常時アカウントを持っているか？（6.10.C1)」

本項目は、自然災害やＩＴ障害等の非常時に、システムとして医療サービスを提供できる機能が有するかを確認するものです。非常時には、システムとして正常なユーザ認証が不可能な場合の対応（非常時アカウントによる患者データへのアクセス機能）や、災害時の受付での患者登録を経ないような非常時の運用に対応した機能等が求められます。

上記のような非常時機能又は非常時アカウントがある場合には「はい」、無い場合には「いいえ」、システムとして該当しない場合（アカウント管理機能等が無い場合）には「対象外」としてください。

６．１２　「１２　外部と個人情報を含む医療情報を通信する機能やリモート保守機能を有するか？(6.11.C1)」

本項目は標準機能、オプション機能を問わず、外部のシステムと個人情報を含む医療情報を通信する機能あるいはリモート保守機能を有するかを確認するものです。１方向のみの場合も含まれます。「外部のシステムと個人情報を含む医療情報を通信」とは、医療機関、薬局、検査会社等間での診療情報の交換、医療機関の従事者がモバイル型端末で外部から医療機関内の情報システムに接続、患者等による外部からのアクセスなどのケースのことを言います。

上記のような通信機能がある場合には「はい」、無い場合には「いいえ」としてください。「はい」の場合は、１２．１～４の質問に回答してください。

６．１２．１　「１２．１　なりすましの対策（認証）機能を有するか？（6.11.C3)」

外部との情報交換の際に、機密性保持のために送信元および送信先が正しいことが担保されなくてはなりません。送信元および送信先を偽装するなりすましの対策として、認証機能を有するかどうかを回答してください。

認証機能を有する場合は「はい」、無い場合は「いいえ」としてください。補足説明が必要な場合は、どのような仕様の認証機能かを備考欄に記載記入してください。

６．１２．２　「１２．２　データの暗号化（SSL、S/MIME、ファイル暗号化など）が可能か？（6.11.C5)」

「データの暗号化」とはOSI４層以上のレイヤにて暗号化を施すものを言います。外部との情報交換の際に、機密性保持のためにデータ自体の暗号化（オブジェクト・セキュリティ）機能を有するかを回答してください。その際、IPSecなどOSI３層以下による暗号化（チャネル・セキュリティ）のことでは無いことに注意してください。

データの暗号化が可能な場合は「はい」、機能を有しない場合は「いいえ」としてください。補足説明が必要な場合は、使用している暗号の仕様を備考欄に記入してください。

６．１２．３　「１２．３　ネットワークの経路制御・プロトコル制御に関わる機能を有しているか？(6.11.C4)」

本項目は、施設内のルータを経由して異なる施設間を結ぶVPN の間で送受信ができないように経路設定されていることを確認するものです。「ネットワークの経路制御・プロトコル制御」とはネットワーク機器（ルータ、スイッチ、ファイアーウォールなど)、もしくはそれと同等の機能を持つことを指しています。特に情報セキュリティリスクを極小化するために接続経路を限定したり、回り込みを禁止したりすることを指します。

有する場合は「はい」、無い場合は「いいえ」としてください。もし、有する場合は、１２．３．１、１２．３．２の質問に回答してください。

６．１２．３．１　「１２．３．１　ネットワークの経路制御・プロトコル制御に関わる機能は、安全管理ガイドラインを満たす設定が可能か？（6.11.C4)」

可能な場合は「はい」、設定できない場合は「いいえ」としてください。

６．１２．３．２　「１２．３．２　ネットワークの経路制御・プロトコル制御に関わる機能の適正さを証明できる文書があるか？（6.11.C4)」

本項目は、外部との情報交換用のネットワーク機器に対し、安全管理ガイドラインの要求事項に適合していることを確認できる文書を添付しているかを確認するものです。例えば、ISO15408 で規定されるセキュリティターゲット、もしくはそれに類するセキュリティ対策が規定された文書のことを指します。

添付している場合は「はい」、していない場合は「いいえ」としてください。

６．１２．４　「１２．４　リモートメンテナンス機能を有するか？（6.11.C7)」

本項目は、装置に対し保守会社によるリモートメンテナンスサービスを提供しているかを確認するものです。提供している場合、１２．４．１の質問にも回答してください。

提供している場合は「はい」、していない場合は「いいえ」としてください。

６．１２．４．１　「１２．４．１　リモートメンテナンスサービスに関し、不必要なリモートログインを制限

する機能があるか？（6.11.C7）」

本項目は、リモートメンテナンスサービスにおいて、利用者側がアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なリモートログインを防止することが可能かを確認するものです。

有する場合は「はい」、しない場合は「いいえ」としてください。

６．１３　「１３　記名・押印が義務付けられた文書を扱っているか？（6.12.C.(1)）」

本項目は、当該ソフトウェアが記名・押印を義務付けられた文書の作成、参照、保存などを行っているかどうかを確認するものです。記名・押印を義務付けられた文書の例としては、診断書、紹介状、放射線照射録などが挙げられます。

「はい」の場合は、１３．１以降の５項目の質問に回答してください。これらを電子的に作成する場合には電子署名法に適合する電子署名が必要です。また、電子署名、タイムスタンプが付された文書を参照する場合には、電子署名、タイムスタンプの検証が必要になる場合があります。さらに電子文書をタイムスタンプの有効期限（一般的には 10 年程度）を超えて長期保存する場合には、真正性の確保のための長期署名技術、もしくはそれに準ずる措置を行う必要があります。

６．１３．１　「１３．１　HPKI 対応もしくは特定認定認証局が発行する証明書対応の署名機能があるか？（6.12.C.(1)）」

本項目は、記名・押印を義務付けられた文書の作成機能を有するかを確認するものです。安全管理ガイドラインにおいて HPKI 証明書もしくは特定認定認証局が発行する証明書を用いることが求められており、電子署名を付与するために必須の機能です。

作成機能がない場合は「対象外」となります。作成機能がある場合、「はい」の場合は備考に対応している証明書を記載してください。また、「いいえ」の場合は、電子署名を付与するための別の手段を提供する必要がありますので、可能ならば備考に当該システムと連携可能な署名機能の提供方法を記載してください。

６．１３．２　「１３．２　HPKI 対応もしくは特定認定認証局が発行する証明書対応の検証機能があるか？（6.12.C.(1)）」

本項目は、記名・押印を義務付けられた文書の検証機能を有するかを確認するものです。安全管理ガイドラインにおいて HPKI 証明書もしくは特定認定認証局が発行する証明書の検証が求められており、電子署名付き文書を参照するために必須の機能です。

参照機能がない場合は「対象外」となります。検証機能がある場合、「はい」の場合は備考に対応している証明書を記載してください。また、「いいえ」の場合は、電子署名を検証するための別の手段を提供する必要がありますので、可能ならば備考に当該システムと連携可能な署名検証機能の提供方法を記載してください。

６．１３．３　「１３．３　日本データ通信協会認定のタイムスタンプが付与可能か？（6.12.C.(2)）」

本項目はタイムスタンプの付与を確認するものです。安全管理ガイドラインにおいて日本データ通信協会認定のタイムスタンプの利用が求められているためです。電子文書作成においては、電子署名を行った後、タイムスタンプを付与する必要があります。

記名・押印を義務付けられた文書の作成機能がない場合は「対象外」となります。作成機能がある場合、「はい」の場合は対応するタイムスタンプサービスを記載してください。また、「いいえ」の場合は、タイムスタンプを付与するための別の手段を提供する必要がありますので、可能ならば備考に当該システムと連携可能なタイムスタンプの付与方法を記載してください。

６．１３．４　「１３．４　日本データ通信協会認定のタイムスタンプが検証可能か？（6.12.C.(2)）」

本項目はタイムスタンプの検証を確認するものです。安全管理ガイドラインにおいて日本データ通信協会認定のタイムスタンプの利用が求められているためです。参照時には検証が必要となる場合があります。

記名・押印を義務付けられた文書の参照機能がない場合は「対象外」となります。参照機能がある場合はタイムスタンプの検証機能が必要になります。「はい」の場合は対応するタイムスタンプサービスを記載してください。また、「いいえ」の場合は、タイムスタンプを検証するための別の手段を提供する必要がありますので、可能ならば備考に当該システムと連携可能なタイムスタンプの検証方法を記載してください。

６．１３．５　「１３．５　保存期間中の文書の真正性を担保する仕組みがあるか？（6.12.C.(2)）」

本項目は保存機能を確認するものです。法定保存期間が 10 年を超えるものや、法定保存期間を越えて 10 年以上保存するものについてはタイムスタンプ単独では真正性を確保できません。タイムスタンプの有効期限を越えた際に長期保存するための JIS 規格である CAdES、XAdES などの機能、もしくはそれと同等の真正性を確保する機能があるかどうかの確認を行います。

記名・押印を義務付けられた文書の保存機能がない場合は「対象外」となります。「はい」の場合は備考に具体的な実現方式を記載してください。「いいえ」の場合は、真正性を確保するための別の手段を提供する必要がありますので、可能ならば備考に当該システムと連携可能な真正性確保手段を記載してください。

付録：作成者名簿

作成者（五十音順）

五十嵐　隆史（コニカミノルタエムジー）
下野　兼揮　（グッドマン）
西田　慎一郎（島津製作所）
野津　勤　　（システム計画研究所）
葉賀　功　　（コニカミノルタエムジー）
平田　泰三　（シーメンス・ジャパン）（主査）
茗原　秀幸　（三菱電機）

改定履歴		
日付	バージョン	内容
2013/03/XX	Ver. 1.0	初版

（ＪＡＨＩＳ標準　１３－００３）
２０１３年４月発行

～製造業者による医療情報セキュリティ開示説明書～

発行元　一般社団法人　保健医療福祉情報システム工業会
〒１０５－０００４　東京都港区新橋２丁目５番５号
（新橋２丁目ＭＴビル５階）

電話　03-3506-8010　　FAX　03-3506-8070