JAHIS

健康で豊かな国民生活を保健医療福祉情報システムが支えます

サイバーセキュリティ対応活動報告

2022年9月5日

一般社団法人保健医療福祉情報システム工業会
医療システム部会　セキュリティ委員会
委員長　茗原　秀幸

サイバーセキュリティに対するJAHISの対応

近年は医療機関に対するランサムウェアによる重篤な被害が発生し、マスコミでも大きく報道されている。JAHISセキュリティ委員会としても厚生労働省等と協力し各種啓発活動を実施している。

セキュリティ関連のJAHIS標準類を発行

詳細については次スライド以降にて詳述

会員向け啓発活動や支援活動

医療機関に対するリモート保守のリスクアセスメントを支援するための「ISMS準拠リスクアセスメントテンプレート」を公開

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GL」）の適合性を示す開示書（後述）の書き方セミナーの開催による会員への啓発

毎年6月に開催するセキュリティ標準化セミナーにてJAHIS標準類の啓発活動を実施

毎年3回開催の新人教育セミナーのセキュリティ教材にバックアップの考え方を詳述

関係各所への協力や支援活動

医療セプターオブザーバーとして重要インフラレターなど会員各社へ情報発信

社会保険診療報酬支払基金のオンライン資格確認等に対するリスクアセスメント支援

日本薬剤師会による薬剤師啓発用eラーニングコンテンツ開発への協力

医機連サイバーセキュリティTFに対する委員派遣による医療機器のサイバーセキュリティ対応への協力

セキュリティ関連のJAHIS標準類

発行済みJAHIS標準【番号は発行年度（西暦下2桁） ー 発行順（000番台）】

22-007 保存が義務付けられた診療録等の電子保存ガイドライン

電子保存・外部保存システムにおける技術的対策としてベンダーが整備すべきものを規定

（2022年6月改定の際に安全管理GL5.2版の内容を反映し、サイバーセキュリティ対策も具体化）

22-001 リモートサービスセキュリティガイドライン

リモート保守などのリモートサービスを実施する際のサービサーとして考慮すべき事項を規定

（2022年4月改定の際に安全管理GL5.2版との整合を確認）

21-001 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

医療情報システムにおける監査証跡としての監査ログのメッセージを規定

20-005 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

医療情報システム/サービスの安全管理GL対応状況を自ら説明するためのフォーマットを規定

（安全管理GL5.2版対応に向け改定作業を実施中・HELICS申請を実施）

18-006 ヘルスケアPKIを利用した医療文書に対する電子署名規格

HPKIを利用して否認防止のための電子署名を行う際の手続きを規定

（FHIR対応に向けてJSON長期署名フォーマット対応の改定作業を実施中）

セキュリティ関連のJAHIS標準類

18-004　シングルサインオンにおけるセキュリティガイドライン	病院内の複数システムにおいてシングルサインオンを実現するための要求事項とリスクアセスメントの考え方を記載

（FHIR対応を意識し、OpenIDconnect、OAuth2.0への対応を含めた改定作業を実施中）

18-001　HPKI対応ICカードガイドライン	HPKI証明書をICカードに格納した場合のHPKIへのアクセスメソッドを規定
14-005　HPKI電子認証ガイドライン	HPKIを利用して本人確認などの認証を行う際の考慮すべき事項を規定

発行済みJAHIS技術文書【番号は発行年度（西暦下2桁）　―　発行順（100番台）】

16-103　セキュアトークン実装ガイド・機器認証編	医療機関内における無線接続機器の機器認証のためのクルデンシャルをセキュアに格納・利用するための考慮事項を記載（IEEE802.1Xなど）
17-105　セキュアトークン実装ガイド・ノード認証編	医療機関内、施設間におけるノード認証のためのクルデンシャルをセキュアに格納・利用するための考慮事項を記載（TLSクライアント認証など）

セキュリティ委員会のJAHIS標準類策定における考え方と対応例

レギュレーションにおいては、厚生労働省の安全管理GLを遵守することを念頭に置き、安全管理GLと整合性を取った規約、ガイドラインを制定する

スタンダードにおいては、ISOとの整合性を確保するため、JAHIS標準類のISOへの提案や、ISO規格のJAHIS標準類への取り込みを実施する

工業会組織であるため、視点はあくまでベンダーの視点であり、医療サービサーや情報システムサービサーの視点ではない。

近年の課題

JAHIS会員が情報システムサービサーとなる事例が多く、クラウドに関する安全管理GLへの準拠性を示す開示書の策定要望やリモート保守における適正な対応が求められている。

課題を受けた対応

JAHIS標準「製造業者による医療情報セキュリティ開示書ガイド」を「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」に改定しHELICS申請を実施

課題を受けた対応

JAHIS標準「リモートサービスセキュリティガイドライン」に基づくリスクアセスメントの普及啓発活動を実施し、リモート保守のみならず様々なサービスのリスクアセスメントに活用

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

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）を定めた物。最新版 Ver 4.0。

構成　・チェックリスト（はい、いいえ、対象外で回答し、説明は備考欄に記載）
・チェック項目に関する記入方法の解説（Q＆A集も別途用意）

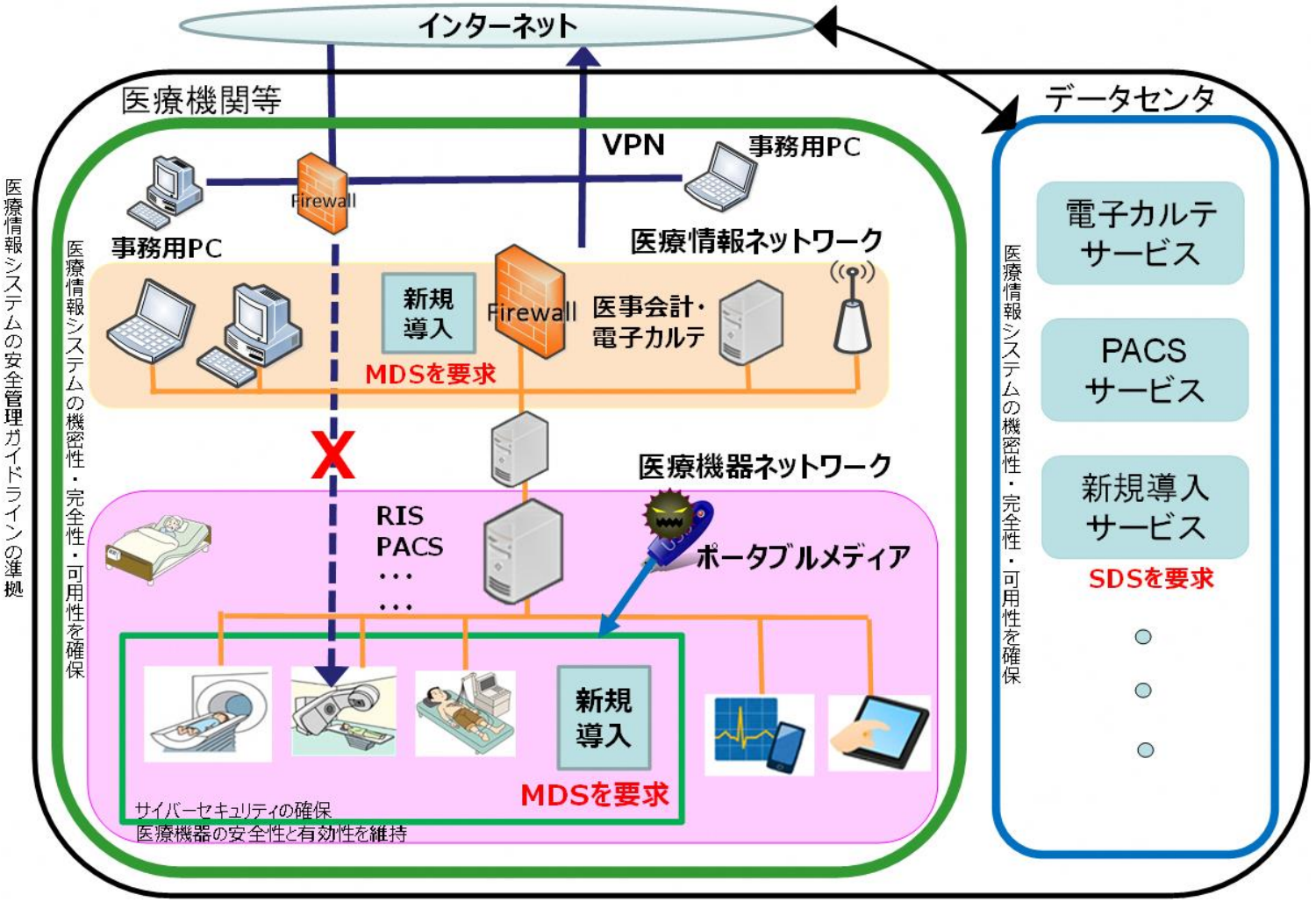
製造事業者向けMDS(Manufacturer Disclosure Statement)は、安全管理GLの各章の「C. 最低限のガイドライン」の技術的対策項目について、サービス事業者向けSDS:(Servicer Disclosure Statement) は、運用も含めた対策項目について、対応状況を記載する。

策定にあたっては、JAHIS/JIRAの合同WGにオブザーバとしてJEITA、ASPICのメンバーを加え、医療情報システム関連の業界団体が結集して検討を実施している。
（JIRA：日本画像医療システム工業会、JEITA：電子情報技術産業協会、ASPIC：日本クラウド産業協会）

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　覗き見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　離席時の不正入力防止の機能があるか？（6.5.C4）	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）	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）					
・記憶(ID・パスワード等)	はい	いいえ	対象外	備考	-
・生体認証(指紋等)	はい	いいえ	対象外	備考	-
・物理媒体（ICカード等）	はい	いいえ	対象外	備考	-

「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

医療機関等が新規システムやサービスを導入する際に安全管理GL準拠のために必要な事項を
MDS（製造業者向け）、SDS（サービス事業者向け）を用いて確認する。



リモートサービスセキュリティガイドライン

本ガイドラインでは、医療機関内の情報機器・システムを遠隔保守するケースのモデル化を行い、そのモデルに対して ISMS（Information Security Management System）の手法に従ったリスクマネジメントの実施例を示す。それにより、医療機関の管理者、および遠隔保守を行うベンダが、実施例を参考にリスクアセスメントを実施することにより、情報資産を安全かつ効率的に保護することができるようになることを期待している。

策定にあたっては、JIPDEC（一般財団法人日本情報経済社会推進協会）と連携し、JAHIS標準改定作業の際にはISMSの最新動向・規格の内容の確認などで連携を実施。

ポイント：
・標準的なリモート保守モデルを定義（予防保守、ソフトウェア改定、故障対応、監視）
・JISQ27001：2014ならびにJISQ27002：2014に対応したリスクアセスメントを実施
・汎用的なリモートサービスのリスクアセスメントに利用可能なテンプレートを作成

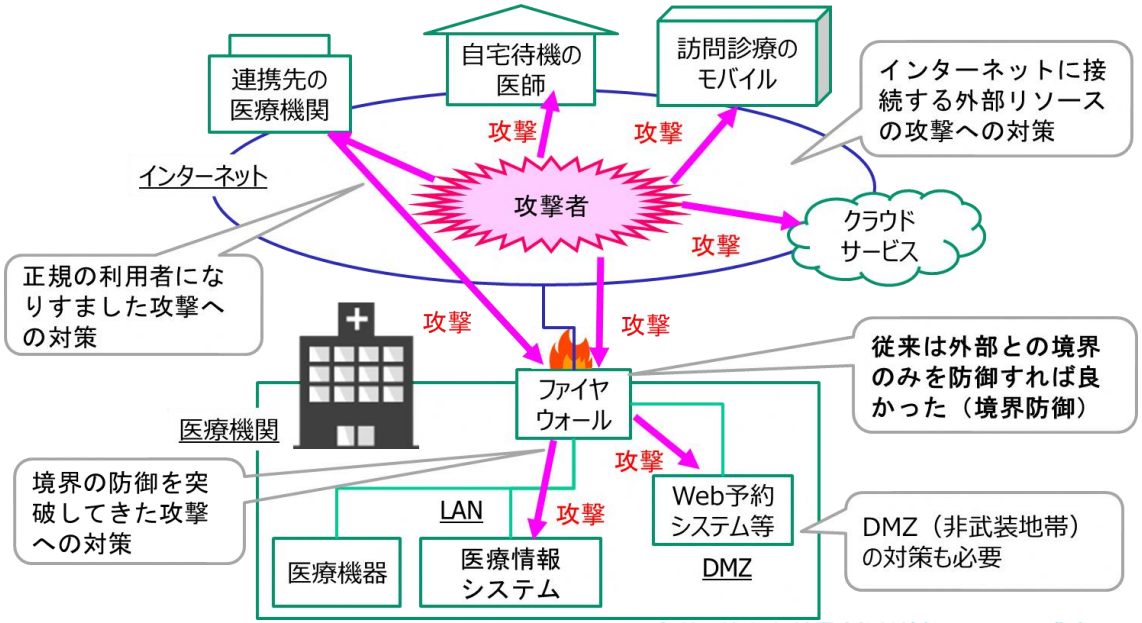
利活用例：
・医療情報システムベンダー各社のリモート保守のリスクアセスメントに活用
・オンライン資格確認のリスクアセスメントのベースに本ガイドラインを活用
・電子処方箋のリスクアセスメントのベースに本ガイドラインを活用
・ISO/TS11633-1：2019、ISO/TR11633-2:2021として2分冊されてISO規格化

会員各社へのサイバーセキュリティ啓発ポイント

- サイバー攻撃は引き金事象でそれによって起こるのは医療情報システムの異常である
- 医療情報システムの異常＝医療事故ではない
- 通常の情報セキュリティ対策で対処可能であればインシデントとして事態は収束する
- 異常が生じたシステムを起因とする医療安全問題が発生した場合にアクシデントとなる

医療情報システムの異常に対する対策と引き金事象の予防の両方の対策が必要

引き金事象の予防はサイバーセキュリティを意識した対策が必要
（セキュリティに100%はない→予防は発生確率を下げることが目的）
事象が起きた後は、やることは従来と一緒でサイバー攻撃に特化したものはない
（例：電子カルテデータの破壊はハードウェアの故障、従業員によるミスや悪意による削除でも発生する）



行うべき対策はサイバーセキュリティに特化したものではなく、常日頃から様々なセキュリティのリスクを踏まえた対応が必要

会員各社への依頼事項

・自社が提供するシステム・サービスに対する脆弱性の把握と可及的速やかな対応
・医療機関等からの問い合わせや相談に対する適切な対応と情報開示
・昨今の情報セキュリティ事故を踏まえた適切なシステム・サービス設計

健康で豊かな国民生活を保健医療福祉情報システムが支えます

ご清聴ありがとうございました