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に対するJAHISの取り組み

２０２３年２月１５日

一般社団法人保健医療福祉情報システム工業会
戦略企画部
部長　並川寛和

JAHISの概要

一般社団法人保健医療福祉情報システム工業会
(Japanese Association of Healthcare Information Systems industory)

略称：JAHIS　「ジェイヒス」

◆**設立目的**：
1．**標準化の推進、技術の向上、品質及び安全性確保**
2．産業界の**健全な発展**と**国民の保健・医療・福祉**に寄与

◆**事業内容**：
1．**標準化の推進**とその普及のための活動
2．政策・制度等に関する**意見具申**
3．研究会、講演会、展示会開催を通じた**知識の交流と普及**
4．**海外**との交流、国際協調の推進
5．工業統計の整備
6．**政府の政策への協力**（委託事業、補助事業等）

◆**会員数**：**３８３社**（２０２３年２月１日 現在）

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ではセキュリティ委員会を中心に関係機関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標準類を多数発行

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ベンダーの技術的対策を規定
（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）
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メッセージを規定
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：安全管理GL対応状況を自ら説明するための開示書を規定
（安全管理GL5.2版対応に向け改定作業を実施中）
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）
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
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の手続きを規定
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
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：シングルサインオンの要求事項とリスクアセスメントの考え方を記載
セキュアトークン実装ガイド・機器認証編：医療機関内おける無線接続機器の機器認証のための考慮事項を記載
セキュアトークン実装ガイド・ノード認証編：医療機関内、施設間などにおけるノード認証のための考慮事項を記載

会員向け啓発活動や支援活動

リモートサービスセキュリティガイドライン対応「ISMS準拠リスクアセスメントテンプレート」の公開し、サンプルSLA、サンプルSDSを発行予定
MDS・SDS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セキュリティ関連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
審査支払基金に対するオンライン資格確認等のセキュリティ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検討への協力

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標準化指針に採択

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リモート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）

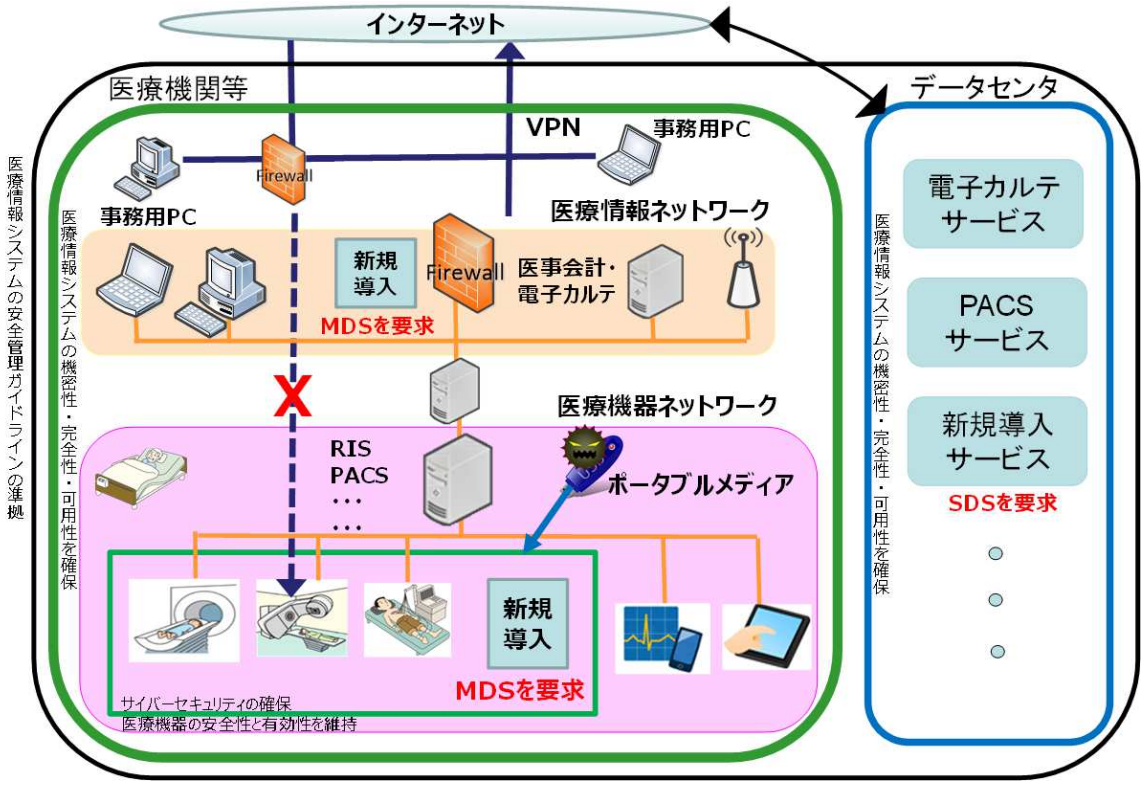
製造事業者向けMDS(Manufacturer Disclosure Statement)は、安全管理GLの各章の「C. 最低限のガイドライン」の技術的対策項目について、サービス事業者向けSDS:(Servicer Disclosure Statement）は、運用も含めた対策項目について、対応状況を記載する。

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

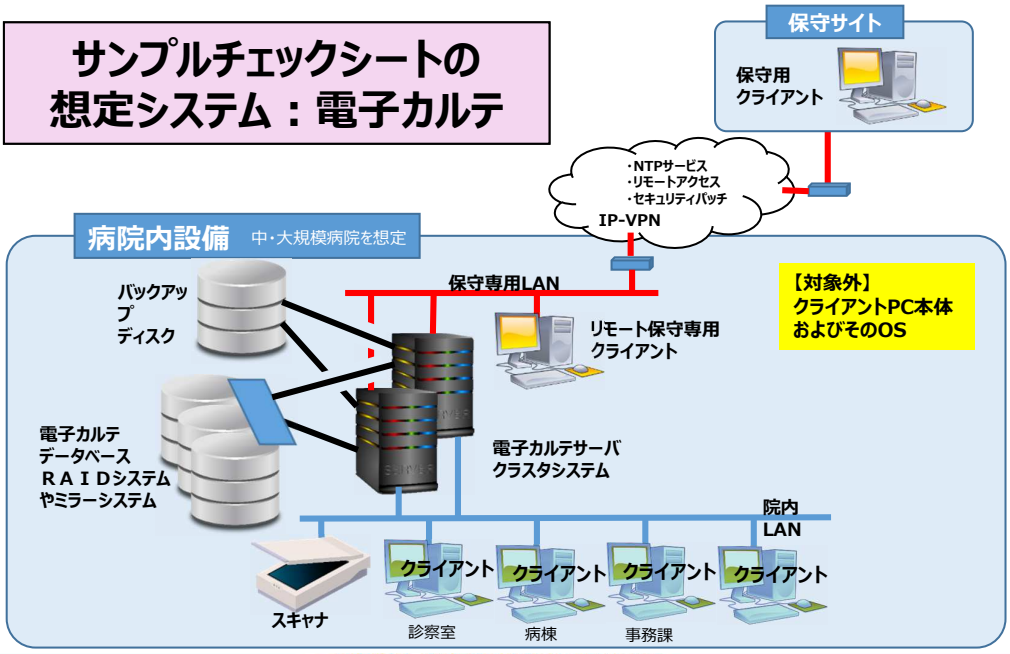
医療機関等が新規システムやサービスを導入する際に安全管理GL準拠のために必要な事項をMDS（製造業者向け）、SDS（サービス事業者向け）を用いて確認する。



MDS作成支援のため、一般的な構成と考えられるサンプルシステムを構成し、それに対応したサンプルMDSを作成している。JAHISのWebページに公開するとともに啓発セミナー等でサンプルの解説を行い、会員各社の自社製品のMDS作成作業が円滑に行えるよう支援している。

サンプルMDSにおける想定システム（電子カルテ）の構成例

サンプルチェックシートの想定システム：電子カルテ



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。

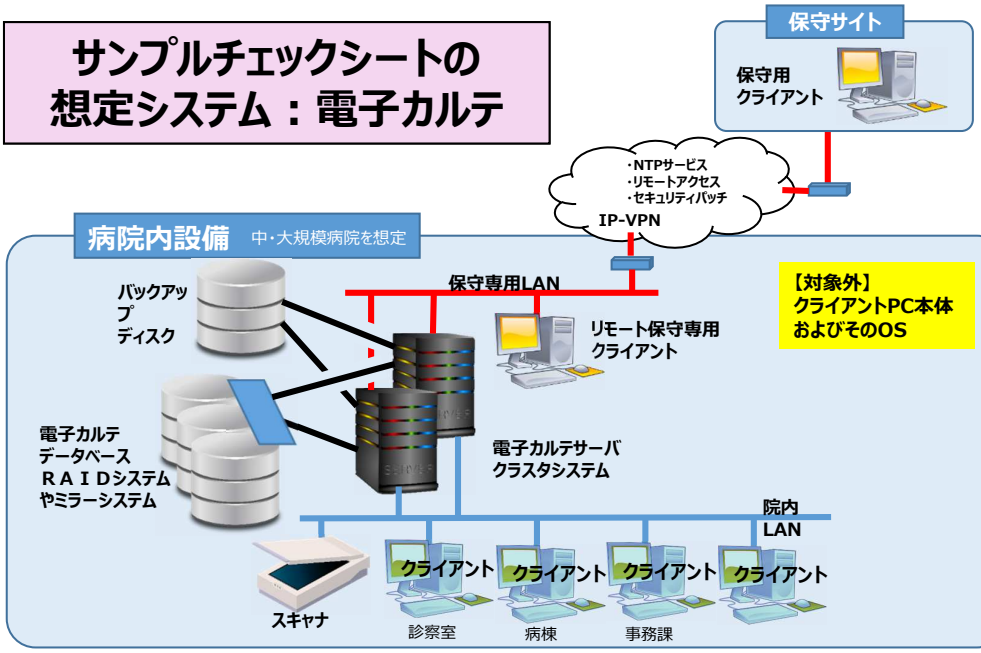
ポイント：
・標準的なリモート保守モデルを定義（予防保守、ソフトウェア改定、故障対応、監視）
・JISQ27001：2014ならびにJISQ27002：2014に対応したリスクアセスメントを実施
・汎用的なリモートサービスのリスクアセスメントに利用可能なテンプレートを作成

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

サンプルモデルに対応したSLA例とSDS例の作成

リモート保守サービスの適正化に向けたリモート保守サービサ支援活動として、
標準的なサービスモデルに基づくSLA例ならびに当該SLAに基づくSDS例を作成し、
各社のリモート保守サービス設計を支援する活動を行う。（近日公開予定）
（ SLA: Service Level Agreement SDS: Servicer Disclosure Statement ）

サンプルチェックシートの想定システム：電子カルテ



リモート保守のサンプルモデルでは、MDSで用いられた電子カルテシステムに対するリモート保守を行うサービスを前提にSLAとSDSが作成されており、MDSと整合を取ることで会員各社の理解を促進するようにしている。

リモート保守サンプルモデルに対応したSLA

リモート保守サービスのサンプルSLA作成に当たっては業界において比較的一般的と考えられるサービス条件を設定し、その条件を踏まえたうえで、総務省・経済産業省の「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」別紙１のSLA参考例をベースとして作成している。

SLA参考例項目と考え方	SLA参考例記載	RSS SLA sample 記載案	解説
6．6 サポート			
【本項を定める上での考え方】 ・本項では、サポート内容を明示する。 ・対象事業者は、一般に利用者からの問合せに対する問合せ受付を用意する。その際、どの範囲の内容を受け付けるのかをあらかじめ合意する必要がある。 ・クラウドサービスの利用では、その前提として利用者側のOSやネットワークに関する設定、Webブラウザ等の設定等が正しくなされていることが求められる。一方で利用者によっては、OSやブラウザの利用方法自体に精通していない場合も多く想定される。 ・サポートセンターの受付内容として、利用者の幅広い問い合わせを受け付ける場合には、一般的にはそのための人員や受付時間のための負担が多くなり、サービスコストの上昇が余儀なくされる。そのため、受付内容の範囲を明確にし、利用者の利便性とサービスコストとのバランスを図ることが求められる。 ・本例で示した報告項目は、あくまでも例示であり、対象事業者において上記観点から必要とされる項目については、追記することが想定される。また受付方法や応答時間との関係で、受付内容の範囲を区分することも想定される（急を要しない内容については受付内容の範囲を広くする等）。	(1) 利用者に対するサポート ① サポート内容 本サービスの利用に関し、乙は、甲から下記の問い合わせを受け付け、サポート対応をする。 ・本サービスで提供するアプリケーションの使用方法等に関する内容 ・本サービスの利用環境及びその設定に関する確認（OS、Webブラウザ等。ただし、以下は含まない。本サービスで提供するアプリケーション以外のアプリケーション等の使用方法等、乙が管理しないパソコンの機器の使用方法等に関する内容） ・本サービスの利用上の障害に関する内容 ・本サービスの利用に起因する甲のシステムの障害に関する内容	(1) 利用者に対するサポート ① サポート内容 本サービスの利用に関し、乙は、甲から下記の問い合わせを受け付け、サポート対応をする。 1．医療機関が障害等の一次切り分けの支援を実施する際に、リモート保守ベンダに対しSaaSサービスの状況等これに必要な情報を提供する 2．本サービスの利用上の障害に関する内容 3．本サービスの利用に起因する甲のシステムの障害に関する内容	1．医療機関の一次切り分け支援 2．リモート保守サービス自体の障害 3．リモート保守サービスに起因する保守対象機器の障害（マルウェア感染等）に対するサポート を指します。
【本項を定める上での考え方】 ・本項では、サポート対応時間等を明示する。なお、「Ⅰ.参考例編（サービス仕様適合開示書）」では、問合せ対応について（2）③で示している。 ・サポート対応時間は、通常電話によるものが想定されるが、例えば、時間外や、急を要しない報告内容等は、メールによる受付を行う対象事業者もある。このような場合には、本項で問合せ用のWebページ等を併せて明示する。	② サポート対応時間 本サービス提供に関し、乙は、甲からの問い合わせを受けるため、下記において受付対応を行う。 【乙サポートセンター】 連絡先 （受付対応時間、曜日）	② サポート対応時間 本サービス提供に関し、乙は、甲からの問い合わせを受けるため、下記において受付対応を行う。 【連絡先】（連絡先を記入） 【平日】 9:00～17:00 【土曜日・日曜・祝日】 提供なし	

SLA参考例の項目と考え方、SLA参考例の具体的記載内容、
リモート保守のSLAサンプルを並べて記載。必要に応じて解説の追記を
実施し、会員各社のサービスにカスタマイズしやすいように配慮している。

リモート保守サンプルモデルに対応したSDS

リモート保守サービスのサンプルSLAに基づきそれと合致するサンプルSDSを提供することで会員各社のSDS作成をより円滑に行えるよう支援している。

サービス事業者による医療情報セキュリティ開示書（医療情報システムの安全管理に関するガイドライン第5.1版対応）						回答欄	
作 成 日	2023年2月8日					2023/2/8	
サービス事業者	リモートメンテナンス株式会社（仮称）					リモートメンテナンス株式会社（仮称）	
サービス名称	電子カルテシステムリモート保守サービス					電子カルテシステムリモート保守サービス	
バージョン	1.0					1.0	
※本開示書の適合性をJAHIS/JIRAが証明するものではありません。						プルダウン選択(はい/いいえ/対象外)	備考番号の入力(数字)(なし="-")
診療録及び診療諸記録を外部に保存する際の基準(8.)							
1 診療録及び診療諸記録の外部保存を受託するか？(8.1.2)	はい	**いいえ**	対象外	備考	-	2. いいえ	-
本質問の回答が「はい」の場合は、従属質問のいずれかを「はい」としてください。保存場所が複数「はい」の場合は、それぞれ個別のチェックリストを作成してください。							
1．1 保存場所が「病院、診療所、医療法人等が適切に管理する場所」の場合、安全管理ガイドラインで示された選定基準と情報の取扱い要件を満たすか？(8.1.2.C1(1)～(5))	はい	いいえ	対象外	備考	-		-
1．2 保存場所が「医療機関等が外部の事業者との契約に基づいて確保した安全な場所」の場合、安全管理ガイドラインで示された選定基準と情報の取扱い要件を満たすか？(8.1.2.C2(1)～(9))」	はい	いいえ	対象外	備考	-		-
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(6.2)							
2 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	-	1. はい	-
組織的安全管理対策（体制、運用管理規程）(6.3)							
3 医療情報システムを運用する際に医療情報システム安全管理責任者を設置しているか？(6.3.C1)	**はい**	いいえ	対象外	備考	-	1. はい	-
4 医療情報システムを運用する際に、運用担当者を限定しているか？(6.3.C1)	**はい**	いいえ	対象外	備考	-	1. はい	-
5 個人情報が参照可能な場所においては、入退管理を定めているか？(6.3.C2)	**はい**	いいえ	対象外	備考	-	1. はい	-
6 情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成しているか？(6.3.C3)	**はい**	いいえ	対象外	備考	-	1. はい	-
7 医療機関等との契約に安全管理に関する条項を含めているか？(6.3.C4)	**はい**	いいえ	対象外	備考	-	1. はい	-

注：現行のサンプルSDSは5.1版対応となっているが、ＪＡＨＩＳ標準の改定に合わせて最新版に対応するようアップデートしていく予定である。

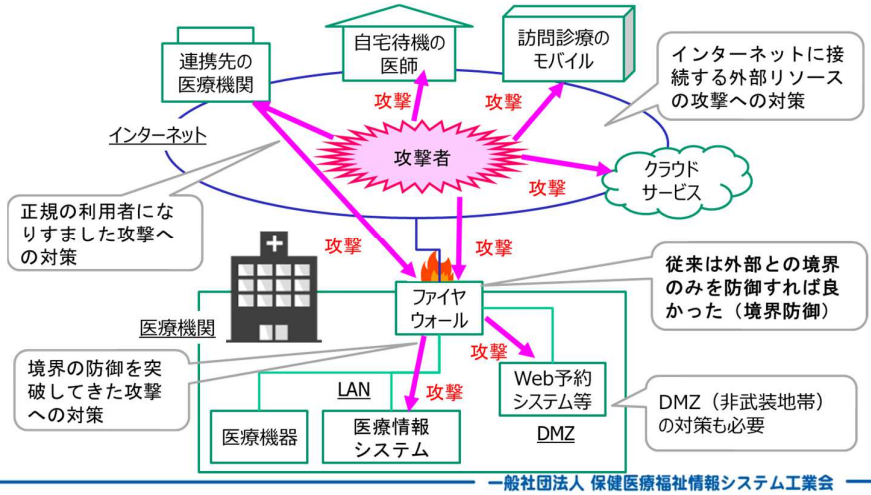
会員各社へのサイバーセキュリティ啓発ポイント

- 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だけではなく、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

JAHISから会員各社への発信

- 厚生労働省、内閣官房内閣サイバーセキュリティセンター（NISC)等からのセキュリティに関する通知を会員各社へ随時発信
- 2023/1/17にJAHIS会員各社へ全員メールを発信
  - 医療機関の現場での声掛け、目視確認を呼びかけ

「サイバーセキュリティ対策アンケート」シート

医療機関名		病床数		回答日		回答者	

※本取り組みに伴う作業においては、競争法、下請法等に抵触しないように留意してください。

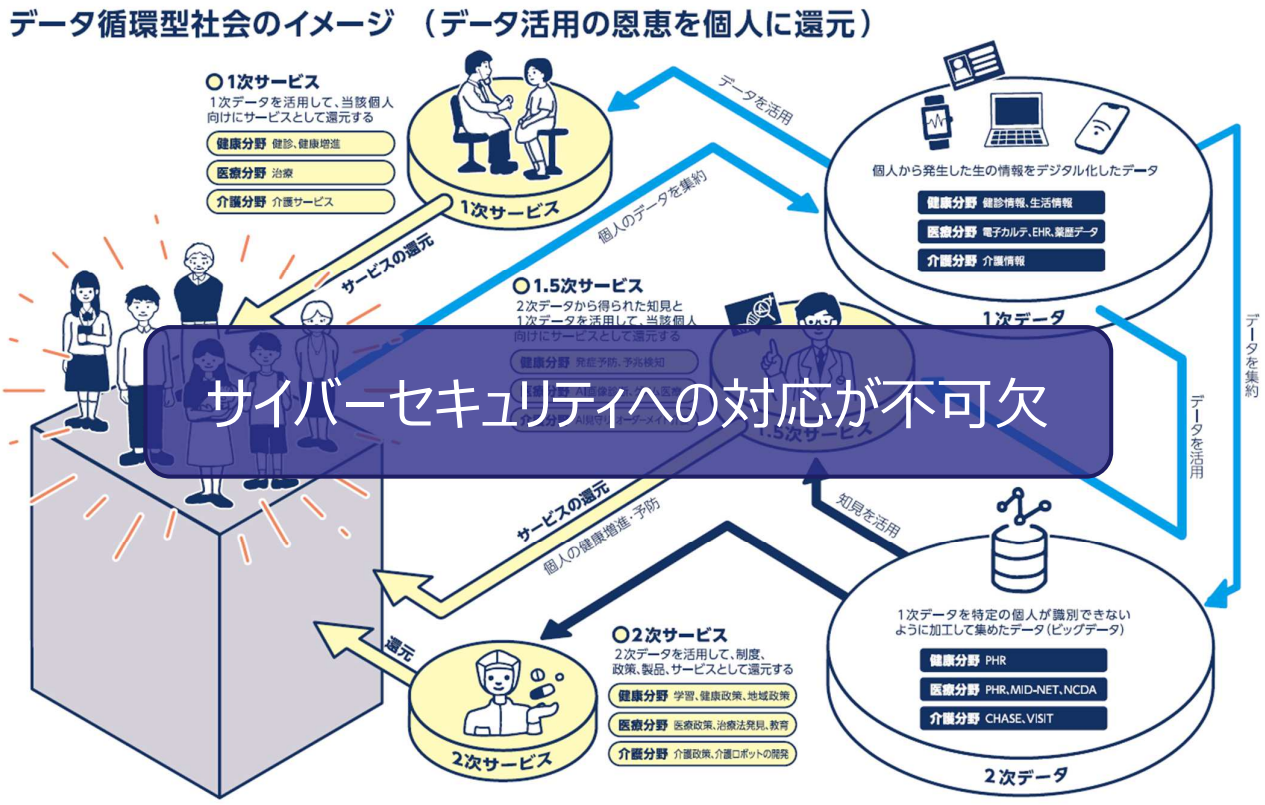
No.	質問	回答
1	2022/12/26にJAHISより送信された以下のメールの内容を確認しましたか？ または、同等の情報を入手済みでしたか？ [ZENIN:1094]【緊急重要連絡・依頼】サイバーセキュリティに対する周知徹底依頼の件	
2	No.1のメールの内容について、具体的なアクションをとりましたか？	
3	No.1のメールの内容について、自社が直接納入した範囲だけではなく、部門ベンダー等も含めて確認をしたり、確認する旨を医療機関に促したりしましたか？	
4	[redacted]	
5	[redacted] お客様へのヒアリングだけではなく、サーバー室やONUの設置場所付近を実際に探索しましたか？　あるいは、その旨を医療機関に促しましたか？	
6	[redacted]	
7	[redacted]	
8	No.6が「はい」の場合、ご回答ください。 セキュリティパッチの適用を行っていますか？ 他社導入機器に関しても、パッチ適用の旨を医療機関に促しましたか？	

医療機関はすべてのVPN装置を把握していないことが多い

会員各社への依頼事項
- サーバー室やONU近辺の目視確認
- 自社導入製品だけではなく、他社導入製品に関しても声がけ

医療機関、ベンダーが一体となり、サイバーセキュリティ対策に立ち向かう流れへ

JAHIS 2030ビジョン（データ循環型社会）



サイバーセキュリティへの対応が不可欠

https://www.jahis.jp/about/contents_type=13

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

一歩踏み出し、一言出しゃばり
医療機関、ベンダーが共になって
サイバーセキュリティに対する風土の醸成を！！

ご清聴ありがとうございました