資料２－２

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５月２４日

一般社団法人保健医療福祉情報システム工業会
運営会議
議長　大原 通宏

サイバーセキュリティに対するJAHISの取り組み（アジェンダ）

1．セキュリティ関連のJAHIS標準類の発行

2．会員向け啓発活動や支援活動の実施

3．2023年のJAHISの活動内容

JAHIS標準類の例

- 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ガイドライン5.2版の内容を反映し、サイバーセキュリティ対策も具体化
- 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（MDS/SDS）
  - 安全管理ガイドライン対応状況を自ら説明するための開示書を規定
    ※ MDS：Manufacturer Disclosure Statement
    SDS：Servicer Disclosure Statement
  - 安全管理GL5.2版対応に向け改定作業のパブリックコメントを終了。最終原案作成中
- 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10月に安全管理GL5.2版との整合を確認したVer.3.1aを発行
- 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
  - 2023年3月にFHIR対応を意識し、OpenID Connect、OAuth2.0への対応を含めたVer.2.1を発行
- 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
- 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
  - 2023年2月にJIS X 6320 シリーズの廃止に伴う修正への対応等を含めたVer.3.0aを発行
- 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

【参考】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）を定めたもの。

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）

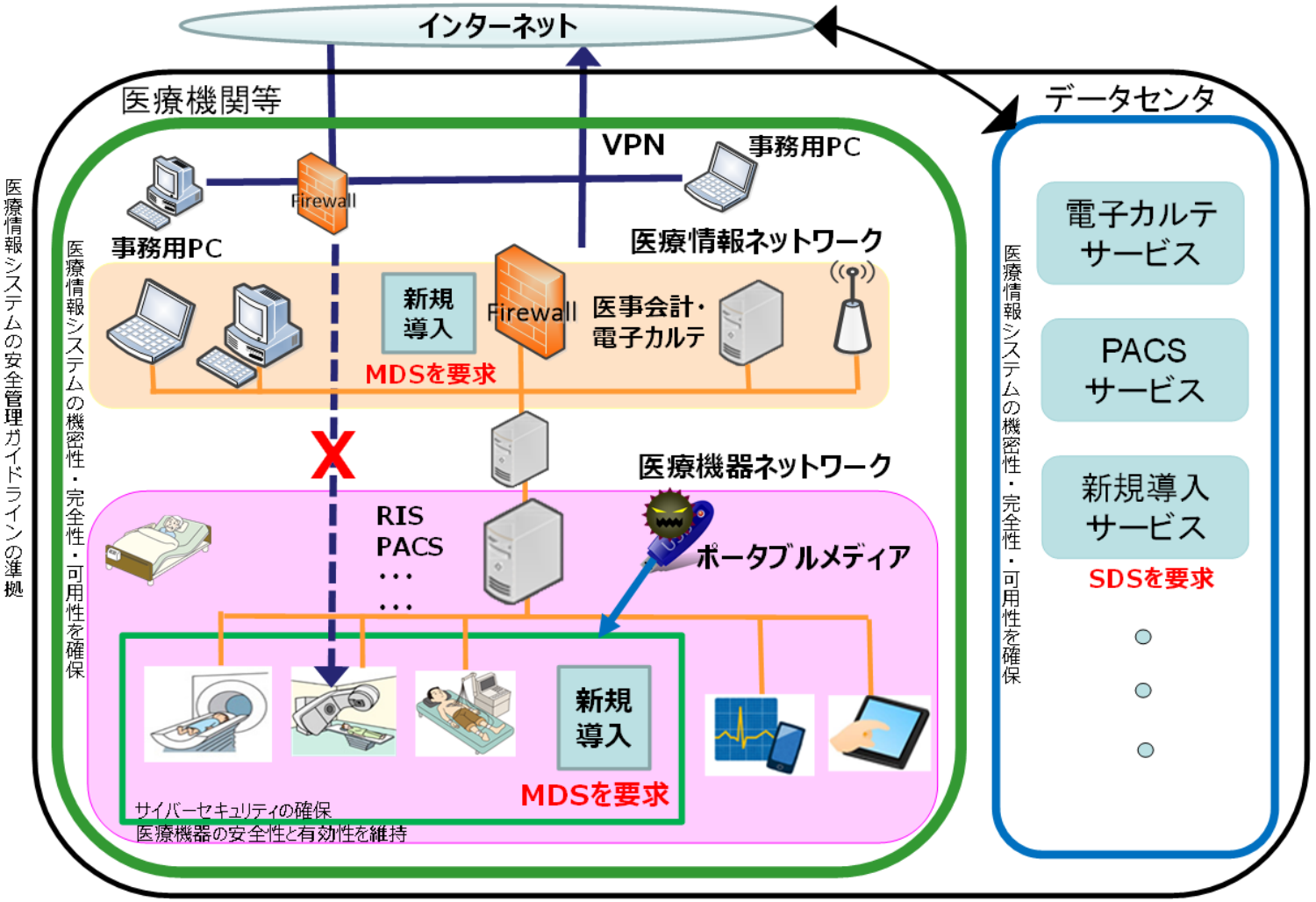
製造事業者向け（MDS）は、安全管理GLの各章の「C.最低限のガイドライン」の技術的対策項目について、サービス事業者向け（SDS）は、運用も含めた対策項目について、対応状況を記載する。

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	-

【参考】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

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。



２．会員向け啓発活動や支援活動の実施

- MDS・SDSの普及促進
  - MDS・SDS書き方セミナーの開催
    - 会員へのセキュリティ意識の啓発とMDS・SDSの書き方の支援を実施
  - 医療機関等向けユーザーズガイドも作成し、Q＆Aを掲載する等、開示書を参照する医療機関向けのドキュメントも用意
  - サンプルMDSを公開し、書き方の支援を実施（初めての方でも取り組みやすいように）

- リモートサービスセキュリティガイドラインの普及促進
  - 「ISMS準拠リスクアセスメントテンプレート」を公開
  - 標準的なサービスモデルに基づくサンプルSLAならびに当該SLAに基づくSDSテンプレートを作成し、各社のリモート保守サービス設計を支援する活動を実施
    ※SLA：Service Level Agreement
  - 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SLA・SDSテンプレートを2023年4月に公開

【参考】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。

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**

3．2023年のJAHISの活動内容

会員各社へのサイバーセキュリティ啓発ポイント

医療情報システムの引き金事象の予防と異常に対する対策の両方の対策が必要

- セキュリティに100%はないが、予防し発生確率を下げることが重要
- サイバーセキュリティ事故発生時にやるべきことは、通常のシステム障害との共通点も多い
  - 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、常日頃から様々なシステム運用のリスクを踏まえた対応も必要

会員各社への呼びかけ

・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

直近のJAHISの対応内容のご紹介

会員各社への呼びかけ

・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

2022年12月26日に
全メンバー向けに
NISC等の通知を
一斉配信

JAHIS会員各位

運営会議議長　大原 通宏

「【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を会員の全員メールにて配信しました」

昨今の医療機関に向けたサイバー攻撃の増加に伴い、厚生労働大臣・厚生労働省からJAHISに向けて周知徹底の依頼が来ております。
つきましては、下記の関連通知を熟読の上、社内で周知し適切な対応をお願いいたします。
また、本内容に関しましては、JAHISに加盟していない販社や部門ベンダー等へも周知下さい。

【関連通知】
（お知らせ）【ＮＩＳＣからの情報提供Ｔ７００」】
Fortinet製品の深刻な脆弱性について (注意喚起)
https://www2.jahis.jp/shien/jhssnpwztlt.asp?cd=1788&ck=22399

（お知らせ）【ＮＩＳＣからの情報提供Ｔ７００－２」】
2022年12月13日に注意喚起を行ったFortinet製品の深刻な脆弱性について、
Fortinetが対象ソフトウェアの追加と回避策を公開したことを踏まえ、注意喚起するもの。
https://www2.jahis.jp/shien/jhssnpwztlt.asp?cd=1789&ck=45800

【情報提供】ＦｏｒｔｉＯＳ　に関する脆弱性情報への対応について（注意喚起）
https://www2.jahis.jp/shien/jhssnpwztlt.asp?cd=1791&ck=84450

（お知らせ）【ＮＩＳＣからの情報提供Ｔ７０３」】の送付
年末年始休暇において実施いただきたい対策について（注意喚起）
https://www.nisc.go.jp/news/notice/20221220.html

直近のJAHISの対応内容のご紹介

2023年1月17日に全メンバー向けにセキュリティ調査の呼びかけを実施

「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	[illegible]	
5	[illegible] 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	[illegible]	
7	[illegible]	
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

直近のJAHISの対応内容のご紹介

2023年3月31日に
全メンバー向けに
「更なる取り組み」につ
いての一斉配信を実施
（詳細は次スライド）

2023年3月31日

JAHIS会員各位

運営会議議長　大原 通宏

2023年度 省令改正に対応したサイバーセキュリティの更なる取り組みについて

昨今の医療機関に向けたサイバー攻撃の増加に伴い、JAHISではサイバーセキュリティ対策に関する情報提供、およびセキュリティ調査実施の呼びかけをしてきました。
一方、3月10日には、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るため、医療法施行規則の一部を改正する厚生労働省の省令が公布され、4月1日から施行されます。

JAHISでは、この省令に対応し、更なる対策を進めるため、2023年度は以下の施策の実施を予定しています。会員各位におかれましては、是非、積極的な取り組みをしていただき、業界全体のセキュリティ意識の醸成およびセキュリティレベルの向上にご協力をお願いいたします。

①セキュリティ調査を継続実施します
1月17日に発信したセキュリティチェックを継続します。
「【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」
3月30日には、アンケートの集計シートを全会員向けに発信しました。
後日、集計結果のサマリーをJAHISホームページで公開します。
（本集計については公正取引委員会からの承認を得ております）

②セキュリティセミナーのコンテンツを充実させ、無償化します
セキュリティ意識の向上及びより多くの方にセキュリティ知識を習得いただくため、
JAHIS開催のセキュリティ関連セミナーの受講料の無償化を実施します。
また、JAHIS作成のコンテンツに加え、外部有識者を招聘する等、セミナーのコンテンツを充実させます。
少しでも多くの方に受講いただくため、オンデマンド配信も検討します。

③戦略企画部配下にサイバーセキュリティを担当するタスクフォースを設置します
サイバーセキュリティに関する情報提供、および、Q&A対応等による会員向けサービスを提供します。
Q＆Aは会員間で共有するとともに、頂いたご意見はJAHISの事業計画立案のインプットとしても活用します。

以　上

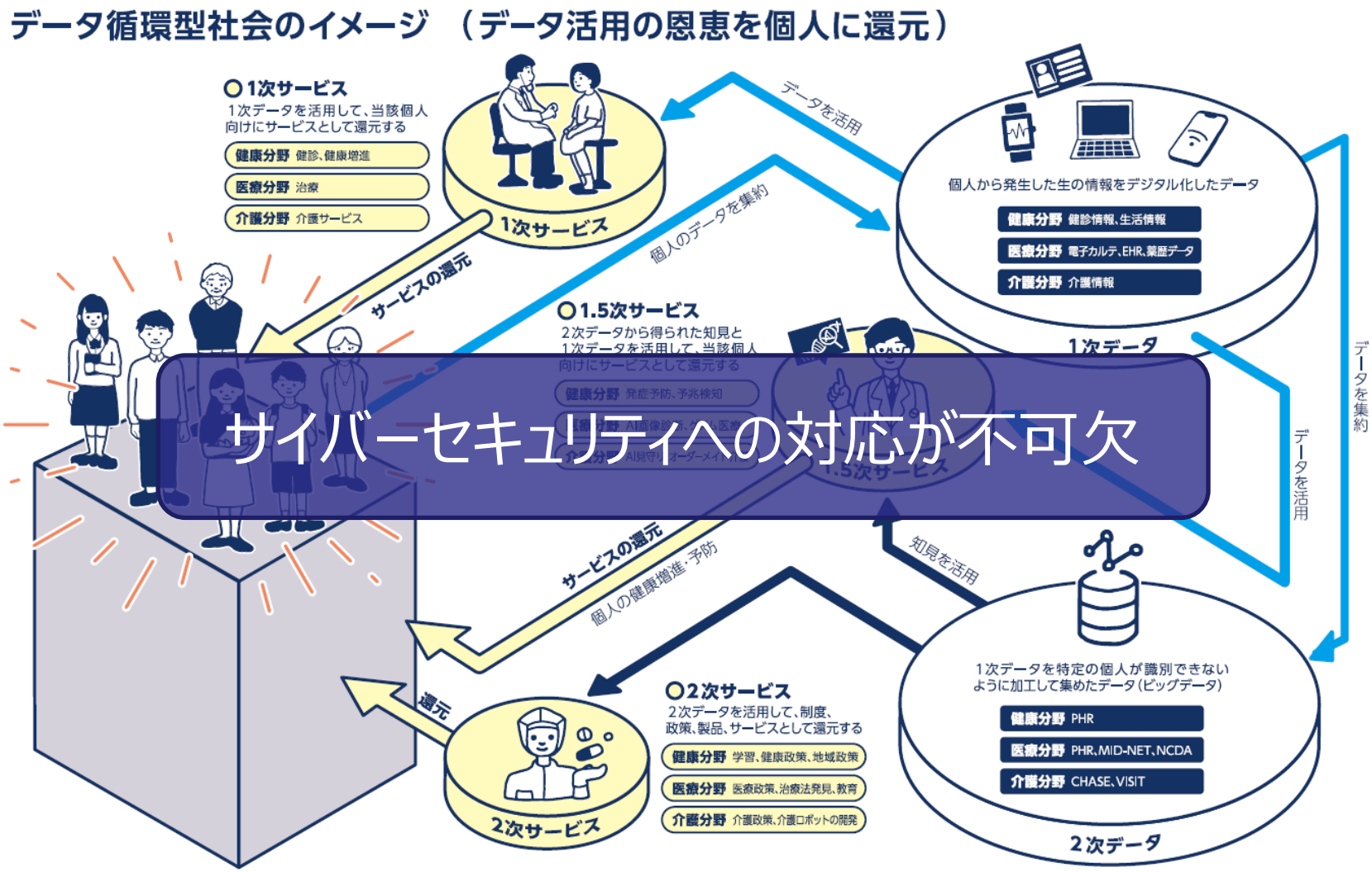
直近のJAHISの対応内容のご紹介

- セキュリティ調査の実施
  - 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ことを踏まえ、医療機関の現場での声掛け、目視確認を呼びかけを実施
    - 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
  - 確認結果をJAHISで集計し公表

- セキュリティ関連セミナーの無償化
  - 2023年度のセキュリティ関連のセミナーを無償化
    - 第一回を7月3日に予定
  - JAHIS作成の従来のコンテンツに加え、外部有識者を招聘しコンテンツを充実
  - 教育コンテンツのオンデマンド配信を行う等、受講機会増加を目指す

- サイバーセキュリティを担当するTFを設置
  - 会員のサイバーセキュリティに対する意識啓発
  - セミナー、教育、情報提供、Q&A対応による会員向けサービスの提供（駆け込み寺）

JAHIS 2030ビジョン（データ循環型社会）



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

ご清聴ありがとうございました