医療機関におけるサイバーセキュリティ対策セミナー

医療機器・情報システム導入時のセキュリティ

一般社団法人 日本画像医療システム工業会（JIRA)
医用画像システム部会　セキュリティ委員会

全体内容

- **医療機関等のサイバー攻撃被害の状況**
  - 医療機関を狙ったサイバー攻撃
  - 閉域網（VPN）への過信は禁物
- **工業会からの対策活動**
  - 安全管理ガイドラインについて
  - セキュリティ情報開示書（MDS/SDS）の活用
  - リモートサービスにおけるセキュリティについて
  - 医療機器のサイバーセキュリティの取り組み
- **被害を防ぐために実践すべきこと**
  - 院内ネットワークの現全体像の把握
  - 各科ローカル運用の確認
  - 管理責任の明確化

内容

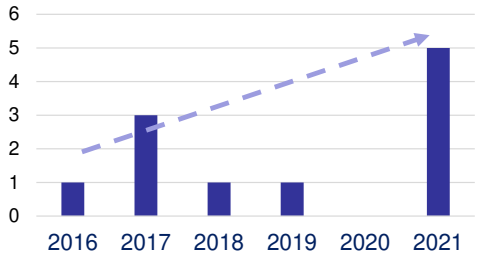
医療機関等のサイバー攻撃被害の状況

- 医療機関を狙ったサイバー攻撃
- 閉域網（VPN）への過信は禁物

医療機関を狙ったサイバー攻撃

年代	施設	発生内容
2018	宇陀市立病院	ランサムウェア攻撃で電子カルテが使用不可
2019	多摩北部医療センター	Emotet 亜種感染。結果的に患者情報の流出はなし
2020	福島県立医科大学附属病院	ウイルス感染でCTで胸部を撮影中に管理端末が再起動他
2021	つるぎ町立半田病院	ランサムウェア攻撃で電子カルテのデータ約85,000人分がバックアップを含め全て暗号化され、利用不可
2022	日本歯科大学附属病院	ウイルス感染(種別特定中)で4日間にわたり電子カルテが閲覧不可
2022	春日井リハビリテーション病院・付属クリニック	外部からの不正アクセスで電子カルテシステム医事会計システムに障害。すべてのサーバーを一時停止
2022	大阪急性期・総合医療センター	ランサムウェア攻撃で電子カルテシステム及び関連するネットワークが利用不可

＜参考＞ランサムウェア被害件数



出典：読売新聞オンライン（2021/12/29）

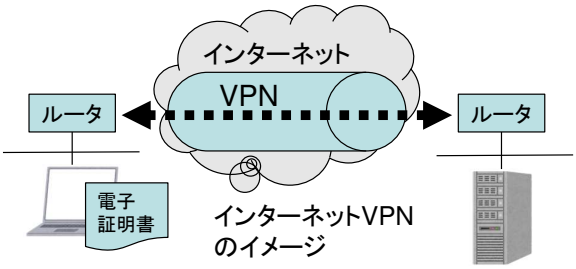
医療機関が集中的にターゲットにされている状況ではないが、被害が長期化する等、社会的影響性が大きい。

対策していないとサイバー攻撃の被害はいつでも起こり得る状況

閉域網（VPN）への過信は禁物

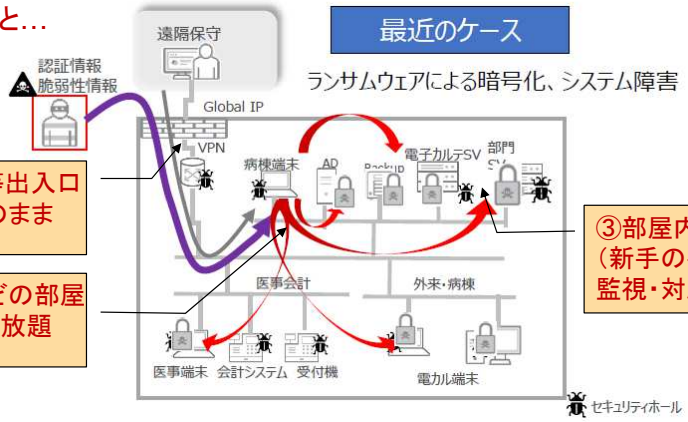
昨今、閉域網（VPN）へ侵入される被害が続出している

- インターネットVPNは管理者不在では危険
  - ① VPNルーターの脆弱性の放置、パスワード強度不足
  - ② ネットワーク内部でのアクセス制限がない
  - ③ セキュリティ対策ソフト（エンジン、ウイルスパターン等）、セキュリティ関連OSパッチが未更新



インターネットVPNのイメージ

建屋で例えると…



最近のケース

ランサムウェアによる暗号化、システム障害

①玄関、裏口等出入口のカギが旧式のまま

②建物内ではどの部屋へも自由に入り放題

③部屋内での不穏な動き（新手の手口での犯行等）を監視・対応する人がいない

内容

工業会での対策活動

- 安全管理ガイドライン
- セキュリティ情報開示書（MDS/SDS）の活用
- リモートサービスにおけるセキュリティについて
- 医療機器のサイバーセキュリティの取り組み

安全管理ガイドライン

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5.2版**」が発行（2022年3月）

- 2023年にはガイドライン6.0版が発行される予定
- JIRAは第５版まで実際の記述作業に参加（現在はオブザーバとして参加）

- **ガイドライン5.2版で詳細化された内容**
  - ランサムウェアによる攻撃への対応としてのバックアップ
    - ✓ 重要なファイルは数世代バックアップ
    - ✓ 追記可能な設定がなされた媒体と追記不能設定がなされた媒体の組み合わせ
    - ✓ 端末及びサーバ装置やネットワークから切り離したバックアップデータの保管等
  - ネットワーク構成図、システム構成図、及びシステム責任者一覧（設置事業者等含む）の整備
  - 外部アプリケーションとの連携における利用者の認証・認可
    - ✓ 二要素認証の追加実装
  - 電子署名を含む文書全体にタイムスタンプを付与

安全管理ガイドラインへの対応にセキュリティ情報開示書（MDS/SDS）を活用

セキュリティ情報開示書（MDS/SDS）の活用

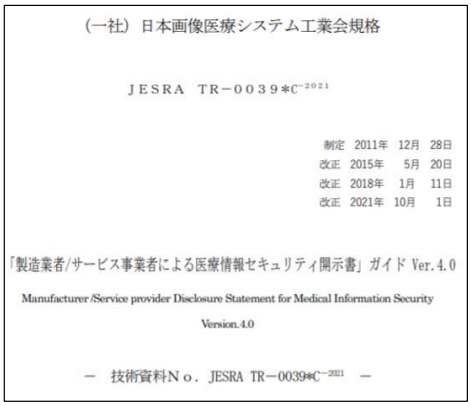
MDS：製造業者による医療情報セキュリティ開示書

SDS：サービス事業者による医療情報セキュリティ開示書

- 「安全管理ガイドライン」への医療情報システムに関する対応状況を示すチェックリスト
- 医療機関はこれらを確認することで、採用予定、もしくは既に採用しているシステムシステムのセキュリティの状況を理解し、サイバー攻撃に対する安全対策についての見直し等を行うことができる。

MDS/SDS活用促進に向けてのJIRA活動

- 医療情報セキュリティ開示書ガイドの発行
  - 「安全管理ガイドライン5.1版」へ対応した開示書ガイド（Ver.4.0）[公開]
  - 「安全管理ガイドライン5.2版」対応に向け改正作業中［最終確認中］
    - ➢ 医療情報セキュリティ開示書ガイド Ver4.1原案作成完了(2023年1月)
- MDS/SDS書き方セミナー（JAHIS/JIRA合同）
  - 2022年10月13日実施（前回実施は1月28日）
  - 製造/サービス事業者に向けたMDS/SDSチェックシートの書き方の解説
  - 具体的にチェックシートを表示して記入事項を説明


（一社）日本画像医療システム工業会規格

JESRA TR−0039*C−2021

制定 2011年 12月 28日
改正 2015年 5月 20日
改正 2018年 1月 11日
改正 2021年 10月 1日

「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 Ver.4.0

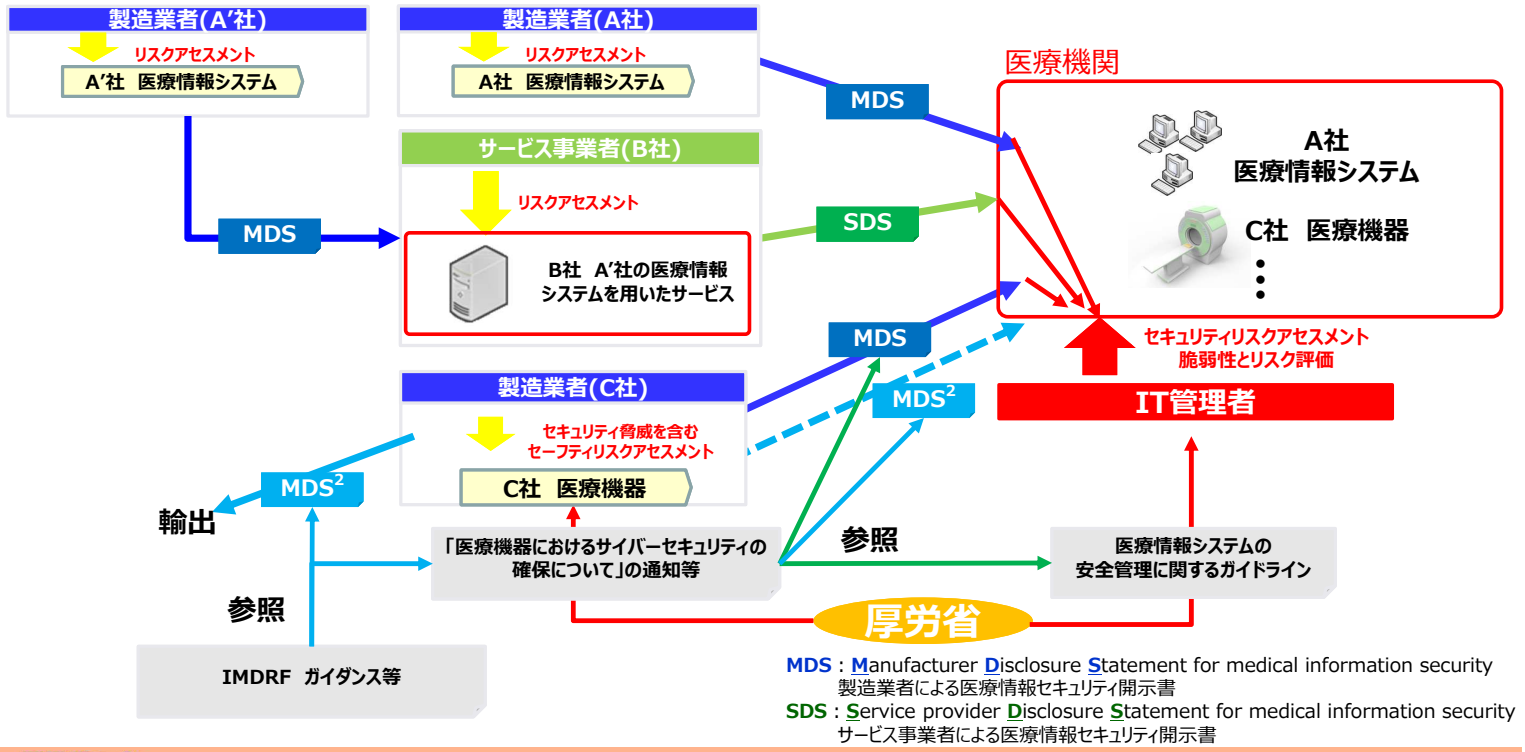
Manufacturer /Service provider Disclosure Statement for Medical Information Security

Version.4.0

− 技術資料No. JESRA TR−0039*C−2021 −

TR-0039 JESRA_MDSSDS_Ver.4.0 （jira-net.or.jp)

<参考>MDS/SDSの位置付け



MDS：Manufacturer Disclosure Statement for medical information security
製造業者による医療情報セキュリティ開示書
SDS：Service provider Disclosure Statement for medical information security
サービス事業者による医療情報セキュリティ開示書

MDS：製造業者による医療情報セキュリティ開示書

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	3
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	-
・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
・上記のうちの二要素を組み合わせた認証（具体的な組み合わせを備考に記入してください）	**はい**	いいえ	対象外	備考	5
4．1．1 パスワードを利用者認証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.C13(1)～(5))	**はい**	いいえ	対象外	備考	-
4．1．2 セキュリティ・デバイスを用いる場合に破損等で本人の識別情報が利用できない際の代替機能があるか？(6.5.C3)	はい	いいえ	**対象外**	備考	-
4．2 利用者の職種・担当業務別の情報区分ごとのアクセス管理機能があるか？(6.5.C6)	**はい**	いいえ	対象外	備考	6
4．3 アクセス記録（アクセスログ）機能があるか？(6.5.C7)	**はい**	いいえ	対象外	備考	-
4．3．1 アクセスログを利用者が確認する機能があるか？(6.5.C7)	**はい**	いいえ	対象外	備考	-
4．3．2 アクセスログへのアクセス制限機能があるか？(6.5.C8)	**はい**	いいえ	対象外	備考	-
5 時刻情報の正確性を担保する機能があるか？(6.5.C9)	**はい**	いいえ	対象外	備考	7
6 不正ソフトウェア対策を行っているか？(6.5.C10)	**はい**	いいえ	対象外	備考	8
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.C14)	はい	いいえ	**対象外**	備考	9

- 所定のチェック項目に対して、「はい」「いいえ」「対象外」で記述
- 説明が必要となる項目には備考番号を入れ、備考欄に内容を記述
  - 例）備考４：クライアント証明書でアクセス元の正当性を担保している等
- 電子カルテ等、保存義務のある文書を取り扱うシステムでは、以下の情報を記述
  - 法定の電子署名について
  - 真正性の確保について
  - 見読性の確保について
  - 保存性の確保について

※ 上記は、安全管理ガイドラインのC項（実施が必須）中の“**技術的安全対策**”への対応を示す。MDSにはこれ以外に、“物理的安全対策”、“情報及び情報機器の持ち出しについて”、“災害、サイバー攻撃等の非常時の対応”、“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”等多くのチェック項目を含む。

医療機関は導入される機器、医療情報システムがどのような安全対策が取られているかを、共通の形式で確認可能

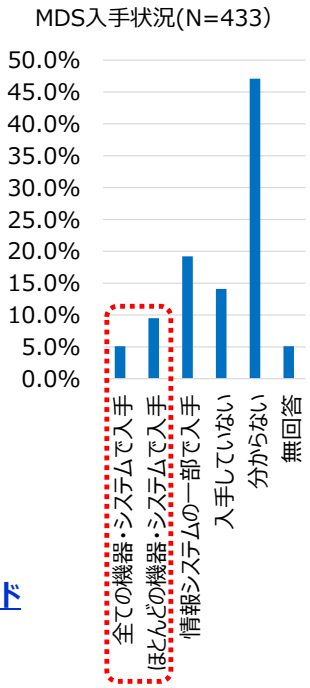
＜参考＞医療機関によるMDSの入手状況

まだMDS/SDSの知名度は高くない状況

- 全て及び、ほとんどの機器・システムで入手を足して15%程度

	全ての機器・システムで入手	ほとんどの機器・システムで入手	情報システムの一部で入手	入手していない	分からない	無回答
国（24）	16.7%	0.0%	12.5%	16.7%	54.2%	0.0%
大学（56）	8.9%	21.4%	17.9%	7.1%	42.9%	1.8%
公的機関（125）	7.2%	10.4%	28.0%	11.2%	40.8%	2.4%
社会保険（14）	14.3%	7.1%	21.4%	14.3%	35.7%	7.1%
医療法人（158）	1.3%	6.3%	14.6%	20.9%	48.7%	8.2%
個人（7）	0.0%	14.3%	0.0%	14.3%	57.1%	14.3%
その他（45）	0.0%	8.9%	17.8%	4.4%	64.4%	4.4%

出典：JIRA　第19回（2021年度）　画像医療システム等の導入状況と安全確保状況に関する調査報告書（資料編）



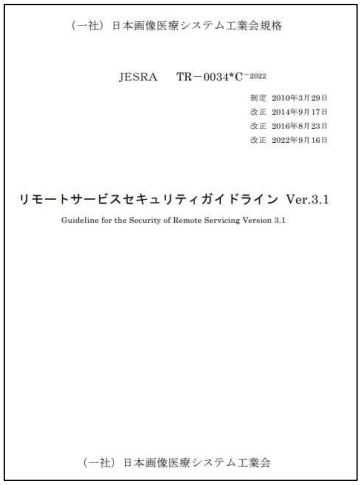
MDSは医療情報標準化推進協議会（HELICS）にて2022年9月に指針採択されたこともあり、活用推奨を進めます

医療機関の皆様は、MDS/SDSについては
「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」医療機関等向けユーザーズガイド
MDS-SDS-Ver4_usersguide.pdf (jira-net.or.jp)
を是非ご活用ください

リモートサービスにおけるセキュリティ

- **リモートサービスにおける注意喚起とさらなる対策支援**
  - リモートサービス経路を狙ったランサムウェア攻撃が多発

- **リモートサービスセキュリティにおけるJIRA活動**
  - 「厚生労働省からの緊急の医療施設への調査依頼」に関する会員企業への協力依頼と注意喚起［2022年1月］
  - リモートサービスセキュリティガイドライン改訂（Ver3.1）
    （JESRA TR-0034C(最新 2022/9/16)）
    - 安全管理ガイドライン5.2版が対象とする内容
      - **リモートサービスの必要性とリスクを解説**
      - **リモートサービスの運用モデルを事例をあげて解説**
      - **リスク分析方法の手法を解説**
  - リモートサービスに対するSDSの記載例作成［2022年度活動として実施］
    - 総務省・経産省の統合ガイドラインのService Level Agreement (SLA)サンプルを参考にサンプルSLAを作成（2022年12月）
    - SLAを踏まえたSDS記載例を作成（2023年3月予定）


（一社）日本画像医療システム工業会規格

JESRA　TR−0034*C−2022

制定 2010年3月29日
改正 2014年9月17日
改正 2016年8月23日
改正 2022年9月16日

リモートサービスセキュリティガイドライン Ver.3.1

Guideline for the Security of Remote Servicing Version 3.1

（一社）日本画像医療システム工業会

JESRA_TR-0034C_r1_2022.pdf (jira-net.or.jp)

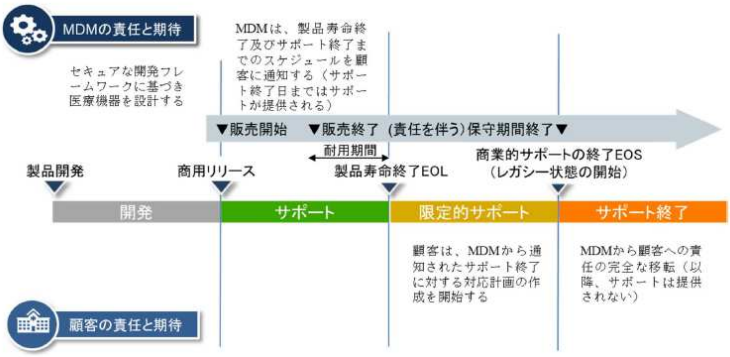
医療機器のサイバーセキュリティの取り組み

「医療機器のサイバーセキュリティ導入に関する手引書」の作成

- 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作成 **※医機連サイバーセキュリティTF**
  - 医療機関向け手引書。パブコメ終了、2023年3月に発行予定
- 医療機器のサイバーセキュリティ導入に関する手引書（改訂）案作成 **※※医機連サイバーセキュリティWG**
  - 製造業者向け手引書。パブコメ終了、2023年3月に手引書（改訂版）発行予定

SBOM、レガシー医療機器ガイダンス案の作成 ※※※IMDRF サイバーセキュリティWG

- 製品ライフサイクル全体に渡って安全性が受容可能なレベルに保たれているかの情報提供を行う
  - パブコメ終了、最終審議を経て2023年3月に文書発行



製品ライフサイクル

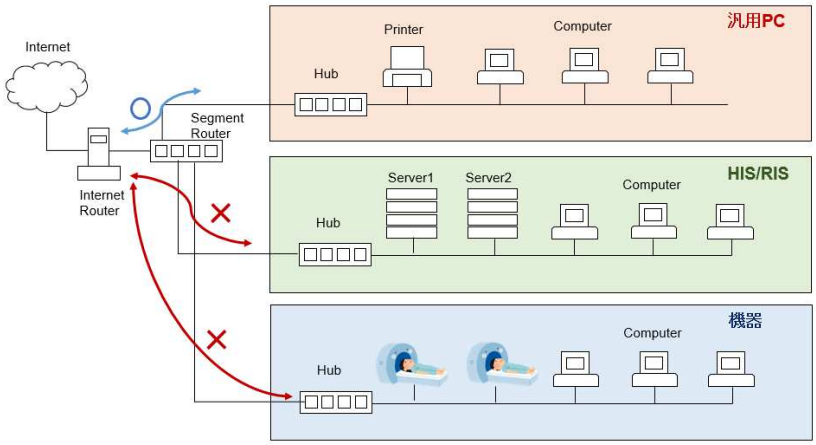
内容

被害を防ぐために実践すべきこと

- ネットワーク構成の把握
- 日常での運用点検・確認
- 管理責任の明確化

ネットワーク構成の把握

- **普段使用している機器のネットワーク構成を把握する**
  - 例）放射線科の場合、関連機器、システムのコンピュータ、端末及び、ネットワーク機器の構成図を把握する
  - 中央情報部門からのHIS端末分も含め、IPアドレス表が最新のものに整理されているかを把握する。

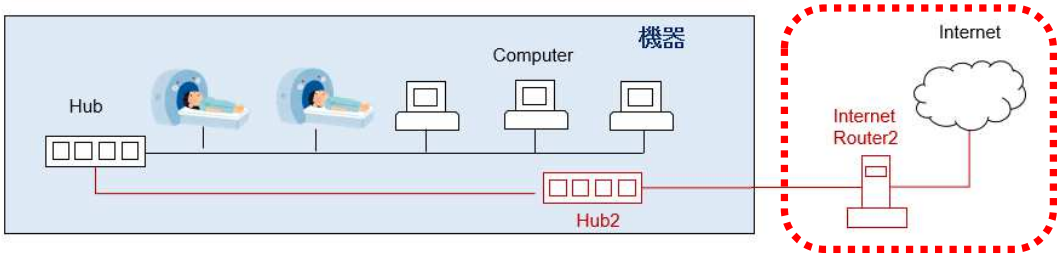


ホスト名	IPアドレス	備考
PC-01	11.200.31.1	汎用PC1
PC-02	11.200.31.2	汎用PC2
. . .		
RIS-01	10.102.31.1	RIS端末1
RIS-02	10.102.31.2	RIS端末2
HIS-51	10.100.10.51	HIS端末51
HIS-51	10.100.10.52	HIS端末52
. . .		
CT-01	10.102.41.1	CTコンソール1
CT-02	10.102.41.1	CTコンソール2
. . .		
Router	10.100.254.1	インターネットルーター

日常での運用点検・確認

日頃から機器、ネットワークの状態点検を継続的に行うこと

- **把握されていないネットワークが追加されていないか確認する**
  - 例）リモート保守等で別途インターネットに抜けるラインが追加されていないか？
  - 例）pingコマンド等にネットワーク構成図にないものが反応していないか？
    - ✓ C:¥>arp –a　「arp –a」コマンドで同一ネットワーク接続機器の一覧を表示
- **各機器のウイルス対策ソフトの状態を確認する**
  - 例）ウイルス対策ソフトのエンジンがエラー等で更新されないままになっていないか？
  - 例）ウイルスパターンの更新が止まったままになっていないか？
  - 例）ネットワーク業者からのルータ機器のファームウェア更新通知を放置していないか等？



別ルートでインターネットに抜ける経路がないか？

管理責任の明確化

管理部署・管理者の明文化を行い、サイバー攻撃に対応出来る体制を整えること

- **ネットワーク構成を把握し、日常での運用点検を行うには、具体的にこれらを行う管理部署、管理者を決め、実践していく必要がある。**
  - 部門内でのネットワーク機器の管理、責任範囲の明確化
  - ネットワーク構成上のベンダー、医療機関の責任分界点の明確化
    - ✓ 例）院内に設置された、どのルータ機器の管理までがベンダー責となっているか等
- **有事の際には、状況をいち早く察知し、被害を最小限に止めることが重要**
  - サイバー攻撃を受けていないセグメントの切り離し等

サイバー攻撃には、製造業者、サービス事業者、医療機関、セキュリティ監視機関、国や自治体など、関係者が協調して対応する必要があります。

終わりに

JIRAはこれからもセキュリティ対策に積極的に取り組んでいきます。

御清聴 ありがとうございました。