JAIPA Cloud Conference

医療機関のサイバーセキュリティ対策：2023

2023年9月21日

一般社団法人医療ISAC代表理事
愛知医科大学医療情報部長・教授
深津　博

©2023 Medical ISAC Japan All Rights Reserved

COI

本講演に関して、講演者および関連団体について開示すべき
COI関係にある企業・団体・個人は存在しません

©2023 Medical ISAC Japan All Rights Reserved

Agenda

- 医療ISACのご紹介
- 医療機関における被害事例の実態と学ぶべき教訓
- 厚生労働省「医療情報システムの安全管理ガイドライン第6.0版」および「医療法施行規則の一部改正」について
- 経済産業省・総務省ガイドラインの活用方法について
- 医療機関として検討すべき対策について

©2023 Medical ISAC Japan All Rights Reserved

Agenda

- **医療ISACのご紹介**
- 医療機関における被害事例の実態と学ぶべき教訓
- 厚生労働省「医療情報システムの安全管理ガイドライン第6.0版」および「医療法施行規則の一部改正」について
- 経済産業省・総務省ガイドラインの活用方法について
- 医療機関として検討すべき対策について

©2023 Medical ISAC Japan All Rights Reserved

医療ISAC活動実績

沿革

2014年	メディカルITセキュリティフォーラム設立 一般社団法人化
2019年	米国Health ISACと事業提携
2019年	・医療ISACと改称 ・Health ISAC Council Japan設立（日米合同事業の枠組み）
2021年	ISO27702-27799 WG-4 Editorとして参画
2023年	新体制移行（理事会・Steering Committee方式）

【活動実績（2022~2023年）】

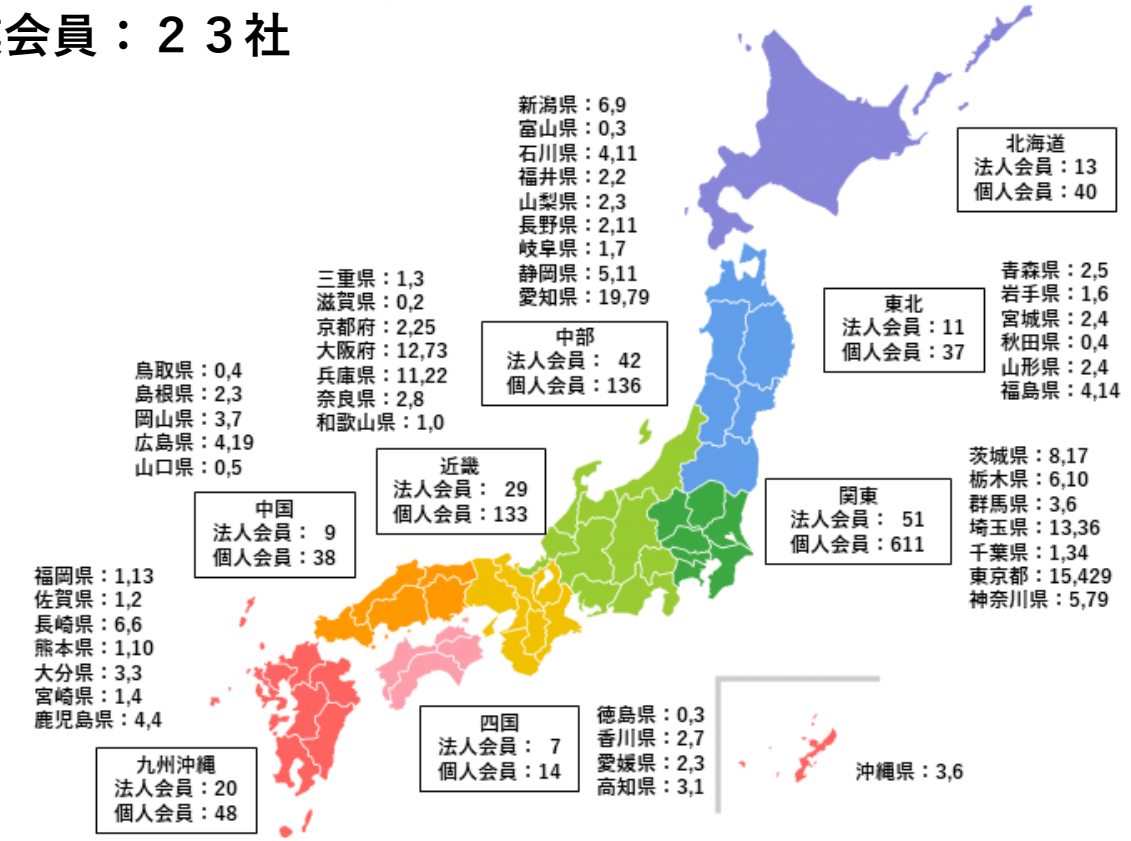
活動形態	項目	実施数
セキュリティニュース配信	デイリーセキュリティニュース、脆弱性情報、インシデント情報、分析情報	525回
セミナー・ワークショップ	「医療ISAC　Security Lecture2022/2023」・日米合同ワークショップ	18件
講演会	医療関連組織に対するセキュリティセミナー	46回
被害防止・最小化活動	①脅威インテリジェンス調査による通知（うち1件は厚労省関連ドメインの侵害に関する通知）	22件
	②Fortigate脆弱性に関する通知	23件
	③クラウドファンディングによるセキュリティ支援	3件
国内医療機関に対する無料相談	サイバーセキュリティに関する無料相談対応（1時間）	66施設
アンケート調査	四病院団体協議会加盟病院対象のアンケート調査により、医療機関のサイバーセキュリティ対策の実態と課題を明確化（調査対象：5596病院、回答：1144病院）、日本病院会に対するセキュリティ緊急調査、全国保険医団体連合会に対するセキュリティ緊急調査全国老人保健施設協会に対するセキュリティ調査、人間ドック学会にに対するセキュリティ調査、日本保険薬局協会に対するセキュリティ調査	6回

医療ISAC会員分布

医療ISAC会員分布　法人会員 193 組織／個人会員　1,123名

個人会員：医療機関576名、ITベンダー等547名
（入会金・年会費無料）
企業会員：２３社

2023年7月14日現在



都府県の数字：法人会員数,個人会員数

医療ISAC Daily Security News

Leading Story
ランサムウェア攻撃で日本最大の港が操業停止
名古屋港は、7月4日に発生したランサムウェア攻撃で名古屋港統合ターミナルシステム（NUTS）がオフラインになり、すべての荷役作業を中止せざるを得なくなりました。
名古屋港は日本最大の港であり、日本の年間貿易額の10%を占めています。
本稿執筆時点では、データ流出サイトに名古屋港をリストアップするなど攻撃を主張するランサムウェアグループは確認できていません。

訳者追記：名古屋港でシステム障害ロシアからサイバー攻撃か（時事通信）

Data Breaches & Data Leaks
データ流出、海外にいるスイス人に影響
Swiss Review誌を購読しているスイス国民が、5月中旬の攻撃でデータを盗まれたようです。
スイス政府は、同誌の発行元であるSwissCommunity社でさえアクセスできないほど機密性の高いデータとみなしています。
刑事告訴が提出され、捜査当局は回答を求めています。

Cyber Crimes & Incidents
攻撃の増加に伴い、FBIがスワッティング事件を追跡
「スワッティング」とは、地元警察からSWATの出動を要請するために、悪意を持って虚偽の通報する行為のことで、このような事件は、しばしば被害者の不当な死につながり、国内テロリズムに分類されます。
FBI は、このデータベースが増加傾向を追跡するために多数の警察署間での情報共有を促進することにより、増大する問題に対処できることを期待しています。
スワッティングは、セレブ・スワッティング、ゲーマー・スワッティング、党派スワッティング、ヘイト・スワッティングの4種類に分類され、この種の犯罪が増加しているため、組織はこの犯罪についてよく理解し、万が一スワッティング攻撃が発生した場合に警察に説明できるようにしておくことが推奨されます。

Vulnerabilities & Exploits
Ghostscriptのバグで不正なドキュメントがシステムコマンドを実行する可能性
Ghostscriptは、AdobeのPostScript文書合成システムと、広く使われているPDFファイルフォーマットの無料オープンソースです。
Ghostscriptの最新リリースであるバージョン10.01.2には、CVE-2023-36664として追跡されるバグがあり、不正なドキュメントがテキストやグラフィックページを作成するだけでなく、レンダリングエンジンにシステムコマンドを送信してユーザーを騙す可能性があります。
ユーザーは、最新バージョンのGhostscriptを実行していることを確認する必要があります。

Trends & Reports
2023年第2四半期のランサムウェア動向サマリー
Cyberintは2023年第2四半期に発生した1,386件のランサムウェアインシデントを分析し、Lockbit 3.0が最も悪質な加害者であることを特定し、米国が最も標的とされた国であることが確認しました。
また、ヘルスケアセクターは、57件のランサムウェアインシデントが発生し、6番目に標的とされたセクターでした。
2023 年の第 2 四半期には、ランサムウェア インシデントが大幅に増加し、ランサムウェアを目的として開発されたゼロデイ攻撃が大量に悪用されています。
この四半期は既存のランサムウェアグループにとっては大きな成功を収め、新規参入者にとっては知名度を素早くあげる方法を提供した期間となりました。

ランサムウェア被害多発の総括
（医療ISACのアプローチの実態と結果）

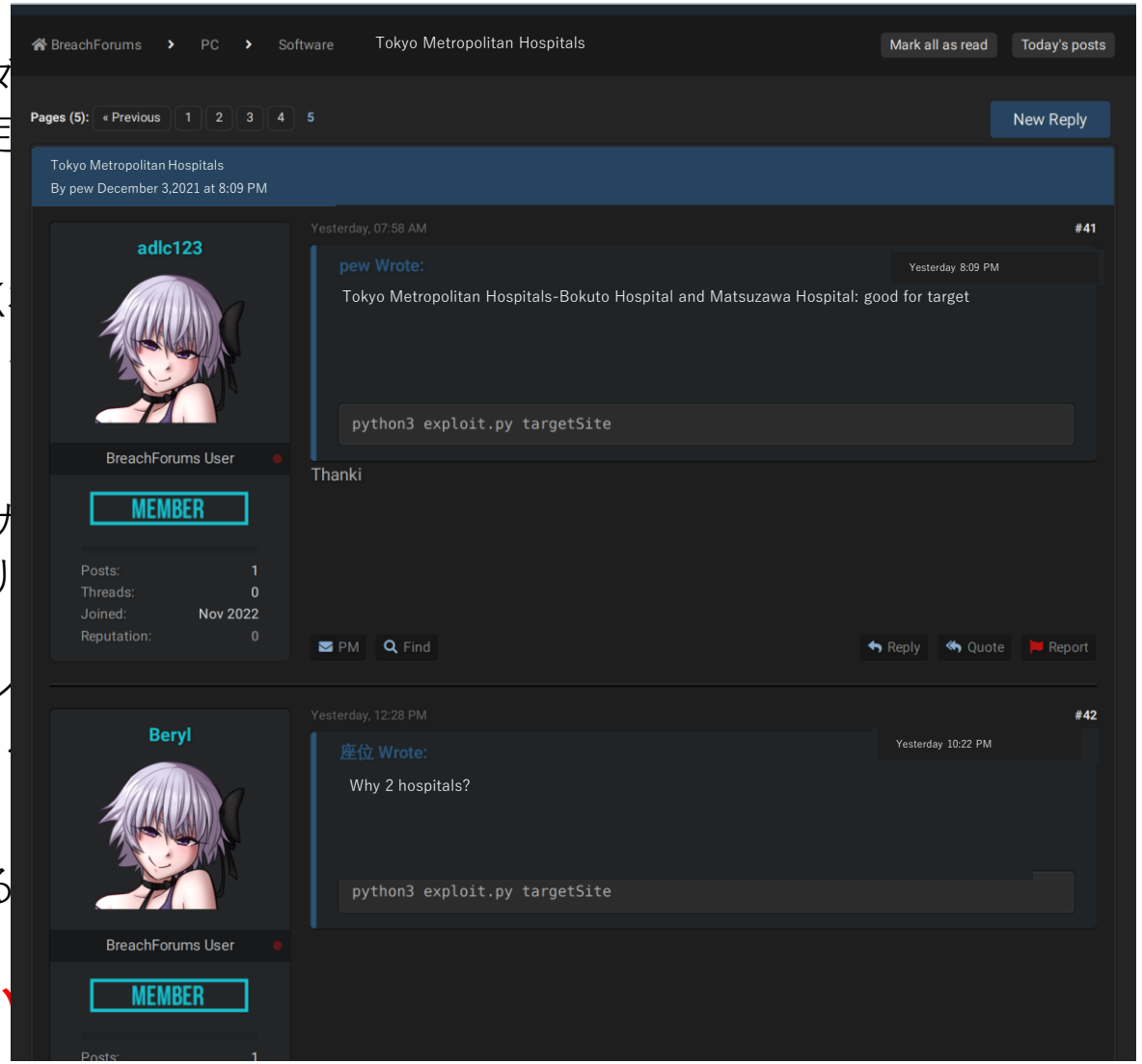
鳴門山上病院の被害事例(2022/6)から、電子カルテベンダ
が放置され、アカウント情報が漏洩している３病院を特定
→同社と３病院に注意喚起。**被害未然防止実現**

愛知県の産婦人科有床診療所の被害事例(2022/3)から、K
電子カルテベンダーのT社のアカウント情報が漏洩してい
T社側での脆弱性対策完了確認。**被害未然防止実現**

東京都立の２病院に対する攻撃予兆（DarkWeb上のハッカ
東京都病院経営本部に注意喚起を行い、認証強化等により

大阪市内の医療法人立病院(2022/9)の脅威インテリジェン
いない状態であることを発見(Global IPをURL欄に入力す
変更により、**被害未然防止実現**

無料相談・被害事例関連情報等から、被害防止につながる
被害防止・最小化活動を継続している
大半の事例で、脆弱性対策が必要な機器が持ち込まれてい

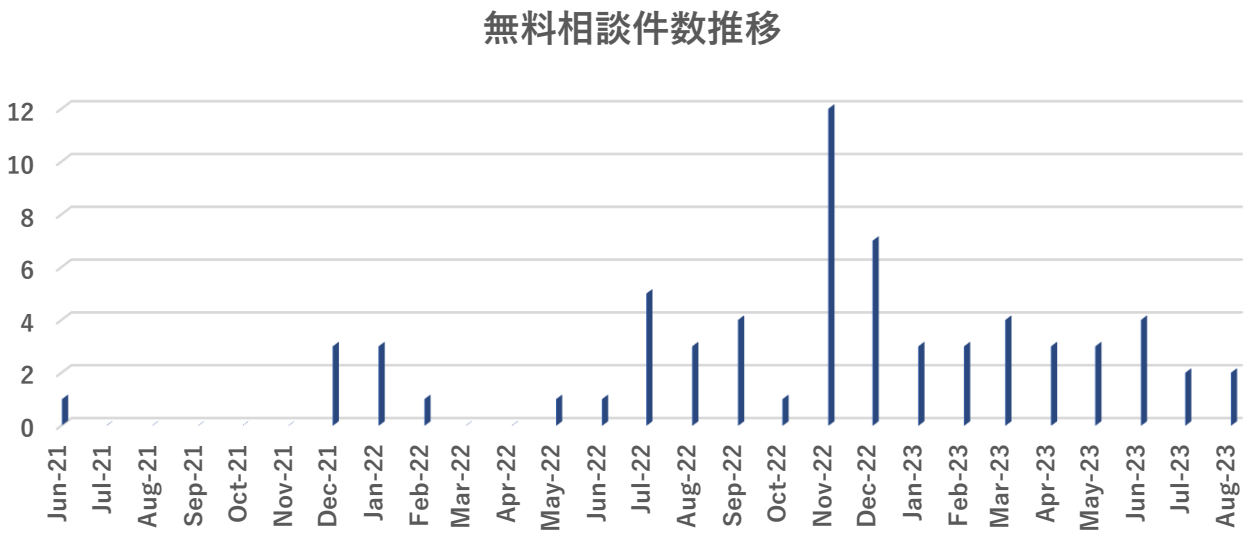


©2023 Medical ISAC Japan All Rights Reserved

医療ISACのサイバーセキュリティ無料相談

相談事業者数(2021-2023)：69
- 病院　：34
- 診療所　：14
- 薬局　：15
- その他　：6

相談内容
- 一般的なセキュリティ対策　：40
- 脅威インテリジェンス診断関連　：21
- 被害発生後の相談　：4
- 総合的な相談（コンサルテーション依頼）：4



相談者様からの声

医療ISAC御中
昨日は貴重なお時間を頂戴いたしまして誠にありがとうございました。
大変参考になり、具体的にメディコム様にアプローチできる内容も
ご教授いただきましたので、早速取り掛かって参ります。
また、ガイドラインのアドレスもありがとうございました。
早速確認させていただきます。
EDRなど、またご相談させていただく場合は改めてご連絡させていただきますので
今後ともよろしくお願い申し上げます。

○○クリニック　○○○○

愛知医科大学理事長○○○○殿

昨今医療機関に対するサイバー攻撃による被害が多発している中、弊院でもその対策知識の取得や職員の啓発を目的として、去る10月18日に、貴大学の医療情報部長の深津　博先生に、ご講演をお願い致しました。

深津先生におかれましてはご多忙中にも関わらず、詳細かつ最新の情報を、現場の目線と知識のない一般職員でも理解しやすいご講演をいただき、職員一同多いに啓発されたところであります。

弊院でのセキュリティ対策の甘さを痛感し、深津先生にご相談申し上げたところ、数々の有用なアドバイスをいただいたのみではなく、電子カルテ等の関与する複数の事業者の指導や、交渉の支援もお引き受けいただき、統合的なリスクアセスメント、緊急性の高いセキュリティ対策の導入、事業者との保守契約書の見直し、など抜本的な対策が開始することができました。

このような有効な措置を早期に開始することができましたのは、深津先生の指導力に依拠するところが大であり、そのような人材が貴大学および名古屋地区に存在することは、真に幸甚であったと実感しております。

弊院のようにセキュリティ対策に危機意識を持ちながら、具体的に何からどのように手をつけてよいかわからない医療機関は、名古屋地区に限らず他にも数多く存在すると思われるため、深津先生のご活動をさらに広めるお手伝いができればとも考えております。

弊院としては、深津先生のご活動を地域の指導的立場にある貴学の地域への貢献として受け止め、まずは書面にて篤くお礼申し上げます。

医療法人○○○○会理事長　○○○○

©2023 Medical ISAC Japan All Rights Reserved

Agenda

・医療ISACのご紹介

・**医療機関における被害事例の実態と学ぶべき教訓**

・厚生労働省「医療情報システムの安全管理ガイドライン第6.0版」
および「医療法施行規則の一部改正」について

・経済産業省・総務省ガイドラインの活用方法について

・医療機関として検討すべき対策について

©2023 Medical ISAC Japan All Rights Reserved

2021-2022の医療機関のランサムウエア被害一覧と課題（疑い例・未公表例含む）

NISC注意喚起（2021/4/30）

2021/4/6-5	香川県坂出市・回生病院	部分的に公表	電子カルテ閲覧できず	病院関係者がランサムウェアが原因と示唆	クラウドバックアップから復旧か？
2021/5/31～	市立東大阪医療センター	システム障害として公表	画像ファイル数万枚暗号化。２日間外来予約診療１部休診	Revil, Avadn	Fortinet社のVPN機器の脆弱性未対策、オンラインバックアップも暗号化
2021/9/10	名豊病院（元：豊田新成病院・愛知県）	非公表	電子カルテ閲覧できず、システム復旧後11月に事業譲渡	ランサムウエア（種別不詳）	身代金支払いか？
2021/10/1～2022/2/22	富士病院（静岡県）	システム障害として公表	電子カルテ閲覧できず。２カ月以上紙カルテ。	病院長がランサムウェアが原因と認める	バックアップも暗号化？
2021/10/31～2022/1/4	つるぎ町立半田病院（徳島県）	公表	８万５千人分のカルテ閲覧できず。	LockBit2.0	二重脅迫型、Fortinet社のVPN機器の脆弱性未対策、オンラインバックアップも暗号化、仲介事業者を介して身代金支払い？
2022/1/14~1/18	日本歯科大学病院	システム障害として公表	電子カルテ閲覧できず	ランサムウエア（種別不詳）	バックアップデータから復旧？
2022/1/12~	春日井リハビリテーション病院	システム障害として公表	電子カルテ・画像システム閲覧できず	ランサムウエア（種別不詳）	バックアップも暗号化？ Fortinet社のVPN機器の脆弱性経由
2022/1～	東北地方眼科有床診療所	未公表	電子カルテ閲覧できず	ランサムウエア：Win32 SHADOWCRYPT.A	Fortinet社のVPN機器経由疑い
2022/2～	九州地方胃腸科外科診療所	未公表	電子カルテ閲覧できず	ランサムウエア：acuna	Fortinet社のVPN機器経由疑い
2022/2～	田関東地方歯科診療所	未公表	電子カルテ閲覧できず	ランサムウエア：Makop	Fortinet社のVPN機器経由疑い
2022/3/29~4上旬	愛知県産婦人科有床診療所	未公表	電子カルテ・予約システム・検査システム閲覧できず	LockBit2.0	Fortinet社のVPN機器経由疑い
2022/4～	青山病院（大阪府）	公表	電子カルテ閲覧できず	LockBit2.0	ランサムウエア（種別不詳）、Fortinet社のVPN機器経由疑い、仲介事業者を介して身代金支払い？
2022/6/19	鳴門山上病院	公表	電子カルテ閲覧できず	LockBit2.0	*オフラインバックアップから復旧、Fortinet社のVPN機器経由疑い
2022/10/27	田沢医院（沼津市）	公表	電子カルテ閲覧できず	ランサムウエア:Makop	Fortinet社のVPN機器経由疑い、オンラインバックアップも暗号化
2022/10/31	大阪府急性期医療センター	公表	電子カルテ閲覧できず	Phobos亜種	給食センターのFortinet社のVPN機器経由疑い
2022/10/31	東邦大学医療センター大橋病院	未公表	会計システム使用できず	ランサムウエア（種別不詳）	身代金支払い？
2022/11	山陰地方無床診療所	未公表	電子カルテ閲覧不可	詳細不明	不詳
2022/12/3	金沢西病院	公表	電子カルテ閲覧不可	ランサムウエア（種別不詳）	Fortinet社のVPN機器経由疑い
2022/12	東北地方有床診療所	未公表	電子カルテ閲覧不可	詳細不明	不詳

厚労省注意喚起（2021/6/28）

厚労省注意喚起（2021/11/26）

厚労省GL5.2版（2022/3/30）

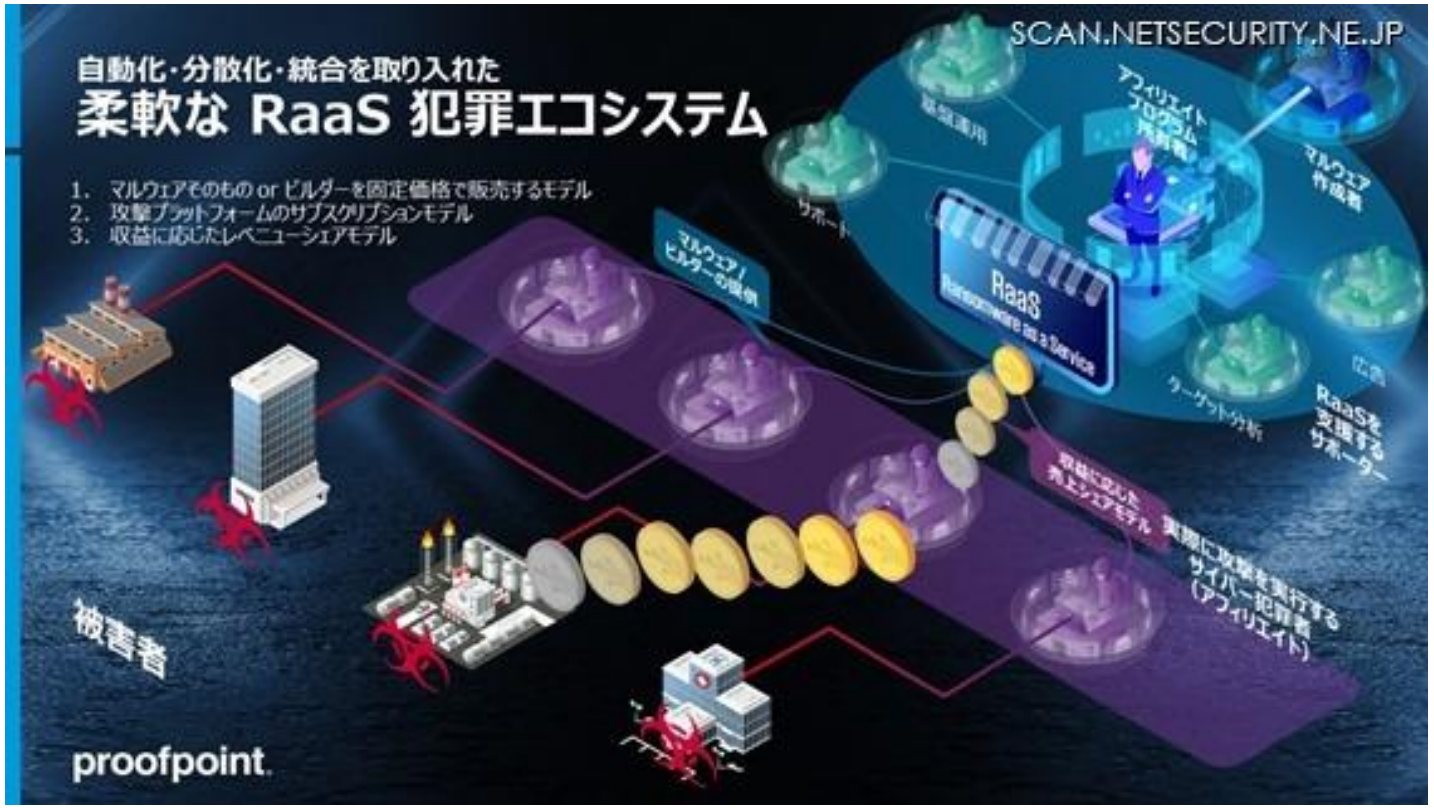
厚労省注意喚起（2022/11/10）

- 米国Fortinet社のVPN機器の脆弱性未対策が原因での侵入事例：12/19件
- バックアップデータまで暗号化され復旧が困難になった事例：5/19件
- VPN装置の大半が事業者が調達・設置・設定したもの（医療機関はそれを十分認識していない）

注意喚起の効果は残念ながら不十分！

©2023 Medical ISAC Japan All Rights Reserved

Ransomware as a Service: RaaS



被害施設の責任者のメッセージ：
今までランサムウェアの危険性は聞いていましたが、やはり被害者にならないとわからない対応であったり、精神的な辛さなども経験することができました。

気持ち的には院内が焼け野原になったような気がして、何も信用できない、些細なことでもまた再感染するのではないかという恐怖感などもあります。私自身も認識が甘かったり、どこか他人事であったりしたのかと痛切に反省しております。

日本の医療機関が狙われている？

Are you here?

You might be here!

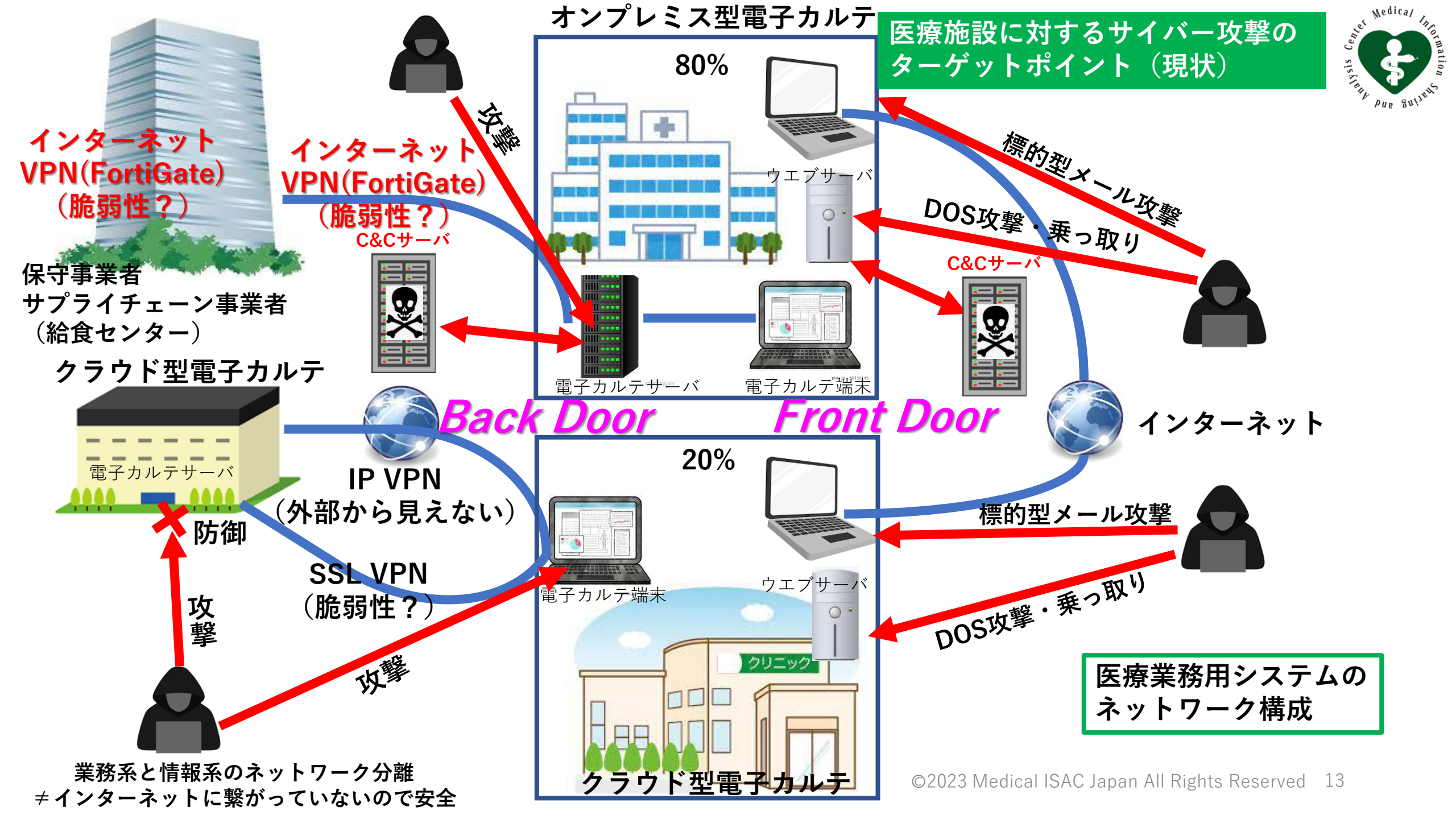
侵入できる対象をリストアップ → 侵入して内部探索 → “日本”の“医療機関”であることを確認 → 身代金要求

複数の日本の医療機関が身代金を支払ったことから日本の医療機関が狙われやすい状況となっている可能性がある

漢字が読める日本人や中国人を利用

©2023 Medical ISAC Japan All Rights Reserved

医療施設に対するサイバー攻撃のターゲットポイント（現状）



医療業務用システムのネットワーク構成

©2023 Medical ISAC Japan All Rights Reserved

被害事例から学ぶべき教訓

・遠隔保守用のVPN装置等のベンダが持ち込んだ機器の脆弱性対策を確実に行う
FortiGateのみが*悪目立ち*しているが、他のVPNルータ等も同様の対策必要

・ランサムウェア対応のバックアップシステムの導入は急務（最後の砦）
＃バックアップ導入に当たっては、復旧（システム・データ）の方法についても検討を行った上で実施することが重要
＃二重脅迫対策としてバックアップデータの独自の暗号化も必要

・電子カルテベンダ等との協力体制の確立が重要

・サプライチェーン攻撃への対応も求められる（大阪府急性期医療センターの事例）

・サイバー保険は？

・マイナ保険証・オンライン診療・オンライン予約等の導入のリスクは？

・

具体的に何をすればよいか？

©2023 Medical ISAC Japan All Rights Reserved

予算不足、人材不足による医療機関のサイバーセキュリティの厳しい現状

2022/1-2月医療ISACアンケート調査より

約**90**%の医療機関が
サイバーリスクの脅威
を感じている

約**50**%の医療機関が
サイバーセキュリティの
予算が不足

平均**3**名弱で
セキュリティ業務を兼務
IT人材が不足

約**50**%以下の医療機関が
BCP対策を
策定していない

約**30**%の医療機関が
脆弱性のあるVPN
を使用している

約**30**%以上の医療機関が
ランサムウェア対応の
バックアップをしていない

約**70**%の医療機関が
サイバー保険に未加入

予算がない

人材がない

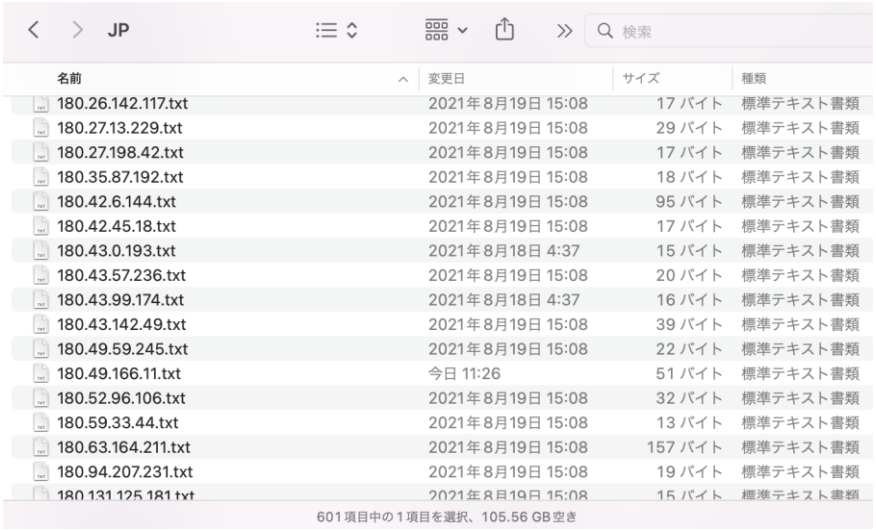
知識がない

これは病院・クリニック等の病床規模、医科/歯科等の区分を問わず、
公定価格に基づく保険診療を制度的な前提とした国内医療機関全般の共通的な課題である

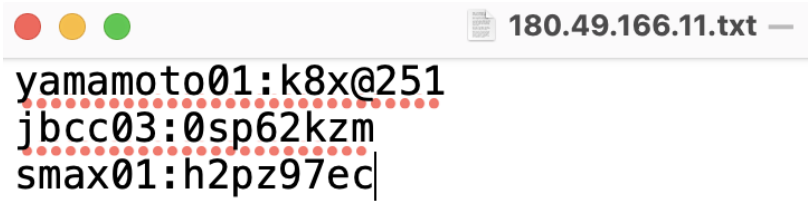
©2023 Medical ISAC Japan All Rights Reserved

つるぎ町立半田病院のランサムウエア被害の実態

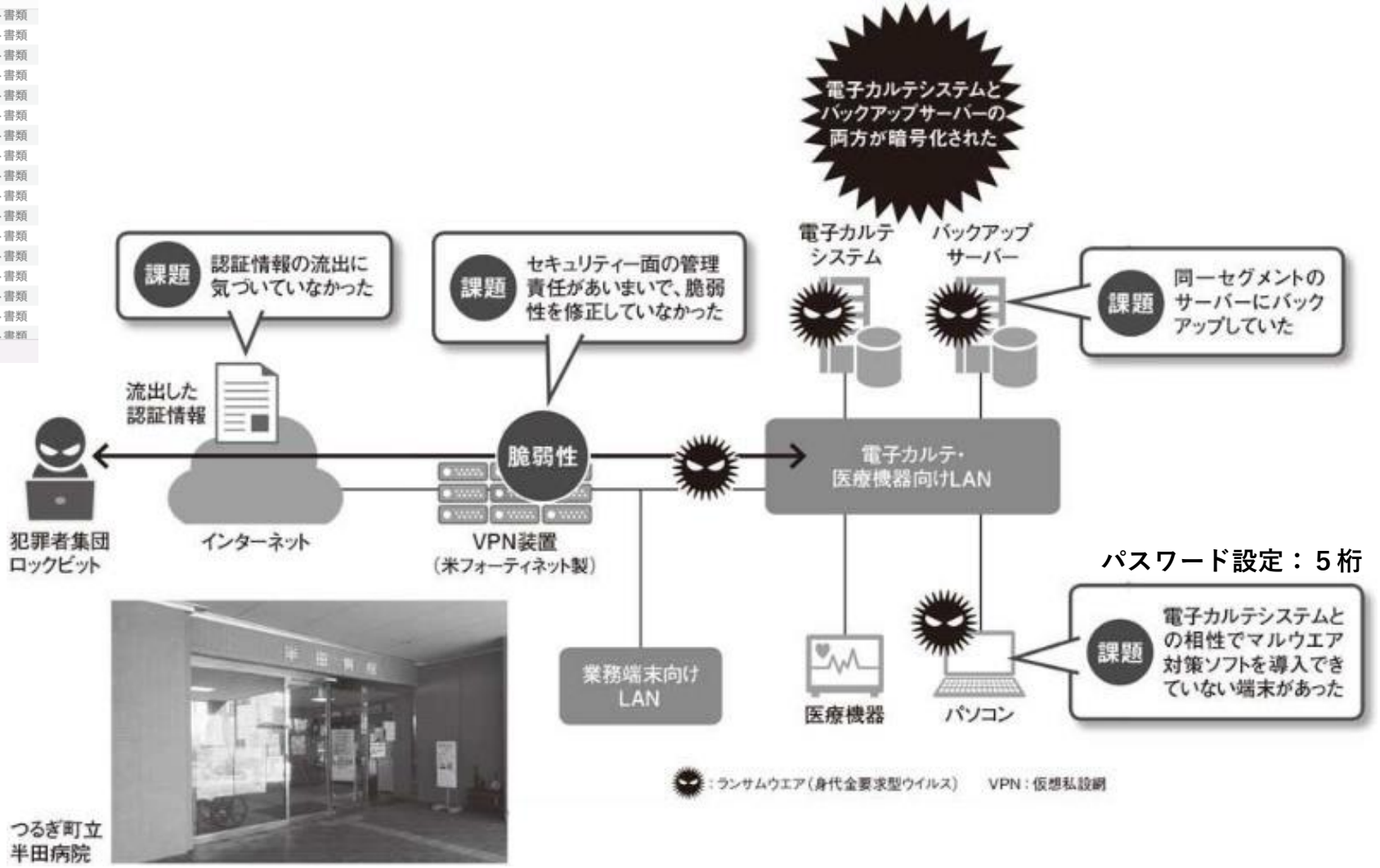
2021/10/31



2021/9にダークウエブ上で公開（販売）された
米FortiNet社製のVPN機器の脆弱性情報のリスト
（約8.5万件のリストの一部）



半田病院に設置されたVPN装置へのログイン
情報（漏洩）

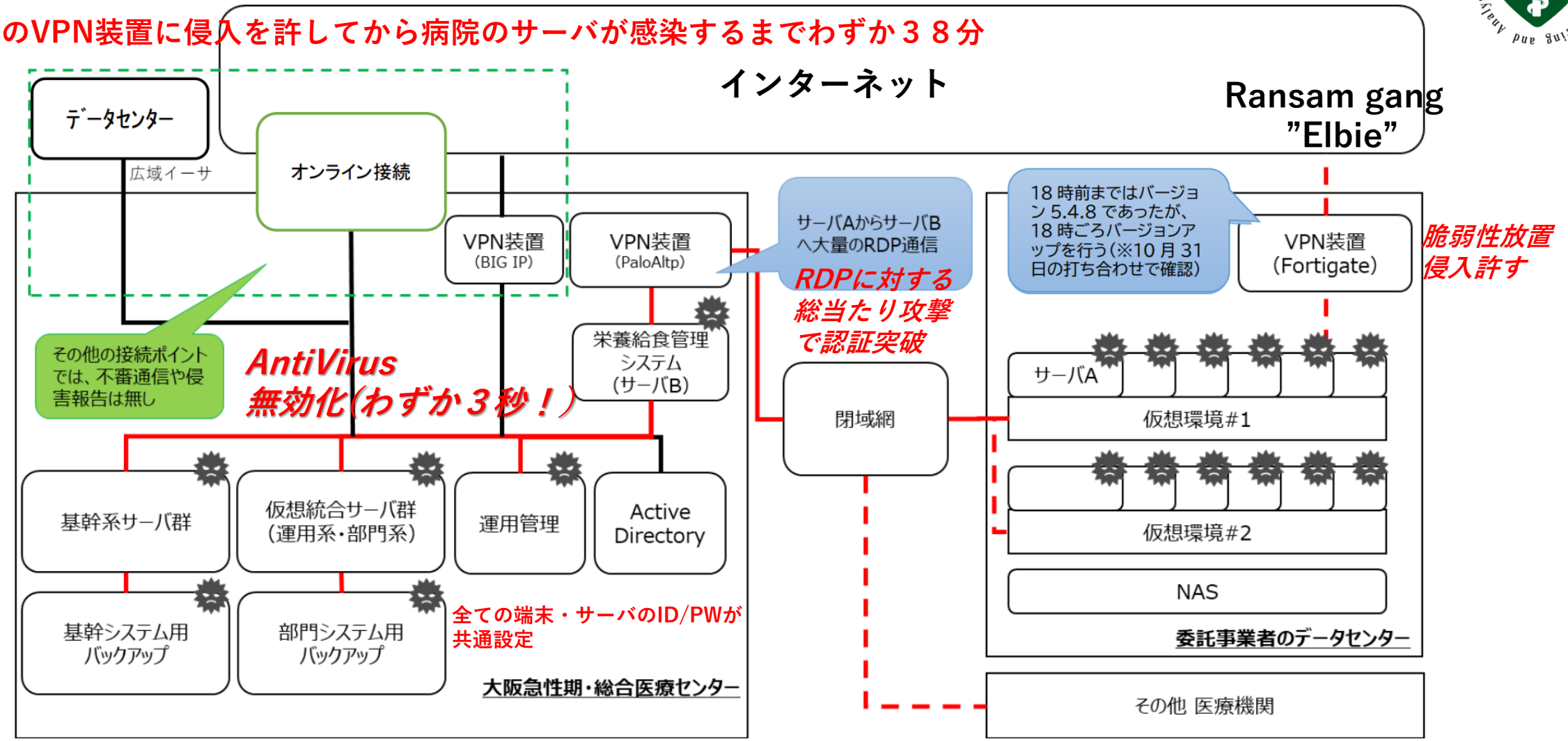


©2023 Medical ISAC Japan All Rights Reserved

大阪急性期医療センターのランサムウエア被害の実態

2022/10/31

委託業者のVPN装置に侵入を許してから病院のサーバが感染するまでわずか３８分



＜関連システムのネットワーク構成図と感染状況＞

医療分野ではおそらく初のサプライチェーン攻撃→厚労省通知2022/11/10

2022 年 11 月 7 日報道公表資料より

関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき、脆弱性対策を実施する。

©2023 Medical ISAC Japan All Rights Reserved

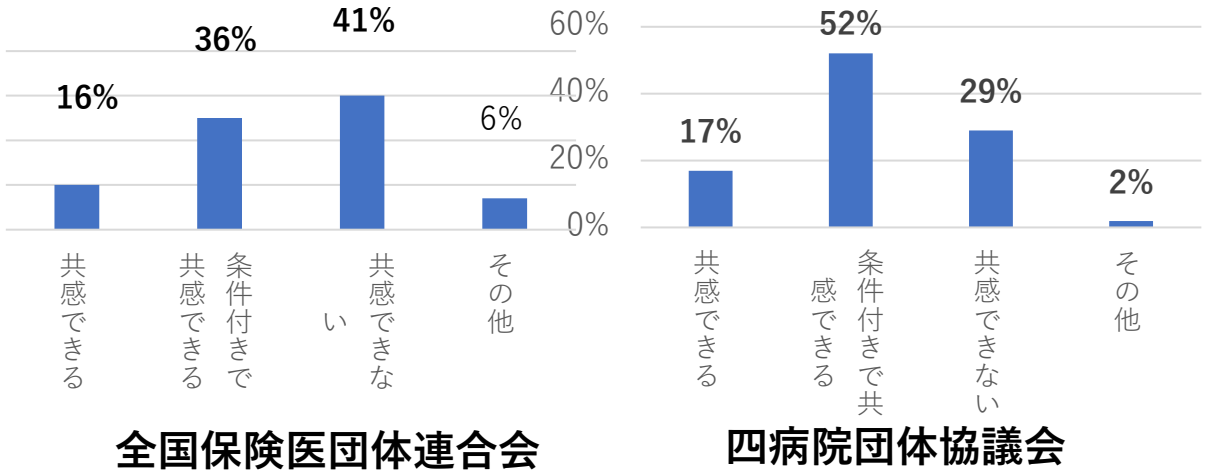
「セキュリティはベンダーに丸投げ」で本当に大丈夫ですか？

「当院は○○社に任せているからちゃんとやってくれているはず」
「セキュリティのことは専門職員もいないし、何してよいのかもわからないから、実際にはほとんど何もしていない」
「セキュリティ対策をしても診療報酬では全く手当されないから自発的に予算確保するのは難しい」
「当院のような地方の小規模病院が狙われるはずがない」
「電子カルテなどの医療用の業務システムはインターネットに接続していないから、サイバー攻撃を受けないはず・・・・・」

2022/1-2月医療ISACアンケート調査より

・ **「診療系ネットワークは外部ネットワークと遮断されているため安全である」**という考えに何らかの形で**共感すると回答した病院の割合は7割弱**、**保険医協会では５割強**と両者の認識に若干の差異がみられた。これはクラウド型電子カルテの導入事例が増加している診療所ではそもそも外部との接続が前提であるための可能性がある。
・病院では**診療系ネットワークの安全神話**（狭小な境界防御）に依存した**“時代遅れ”なセキュリティリテラシー**が色濃く残る環境において、サイバー保険に加入するという選択自体、院内で十分な合意を得ることが困難であることが推測される。

＜「診療系ネットワークは安全であるという考え」“クローズドネットワークの安全神話”への共感度＞



全国保険医団体連合会　　四病院団体協議会

©2023 Medical ISAC Japan All Rights Reserved

電子カルテベンダ等の事業者とシステム・機器の導入および保守契約を締結する際の留意点

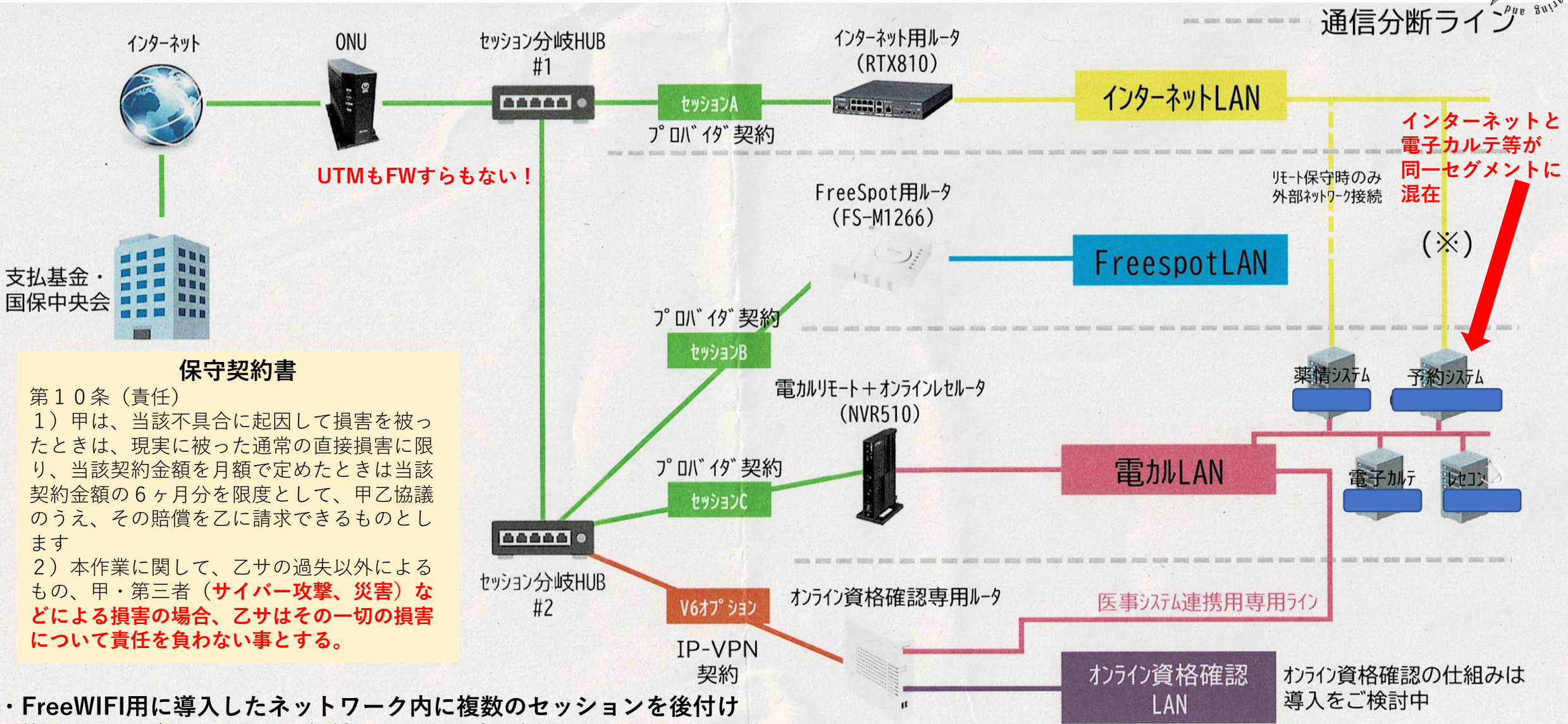
- **医療機関にとって一方的に不利な契約を締結させられている可能性**があることを認識
- 少なくともサインする前に契約書を熟読し、契約内容や責任範囲、免責事項等について確認すること
- わからない場合は弁護士等に相談することも必要
- 本来は改正民法(2020)により、契約不適合責任（契約に特に定めなくとも当然の性能として要求できる仕様を満たしていない場合に、販売後発覚した問題も含め、損害賠償を請求できる）

＊当然の性能：ITシステム等の場合は、サイバーセキュリティが確保されていること
⇔民法上の契約の自由

サイバー事故が発生した際のベンダの言い分
・脆弱性対策については契約書に明記されていないため当社には責任がない
・サイバー事故に関しては自然災害と同様不可抗力であるため、免責となる
・不具合が発生した際にユーザ側から３か月以内に通知しなかった場合、不具合対応の費用はユーザ側負担となる
＊セキュリティ対策は一般にベンダにとってコスト
＊システムベンダのスキルとセキュリティのスキルは全く別物
＊現地営業のいい加減な安請け合いを鵜呑みにすると痛い目に遭うことも（春日井リハビリテーション病院）

©2023 Medical ISAC Japan All Rights Reserved

医療法人○○○○会ネットワーク構成図(2022/10)



保守契約書

第１０条（責任）

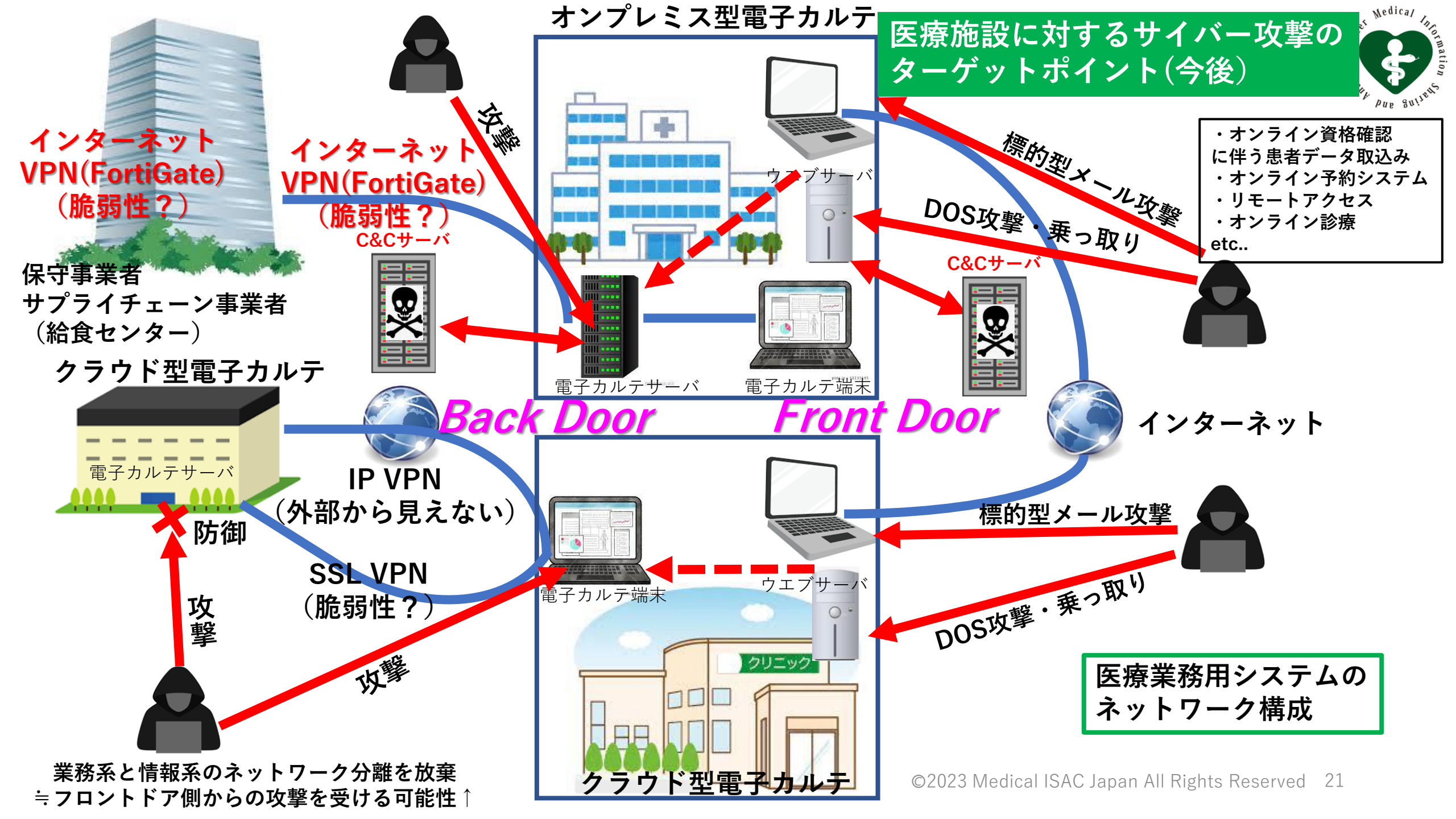
１）甲は、当該不具合に起因して損害を被ったときは、現実に被った通常の直接損害に限り、当該契約金額を月額で定めたときは当該契約金額の６ヶ月分を限度として、甲乙協議のうえ、その賠償を乙に請求できるものとします

２）本作業に関して、乙サの過失以外によるもの、甲・第三者（**サイバー攻撃、災害）などによる損害の場合、乙サはその一切の損害について責任を負わない事とする。**

- **FreeWIFI用に導入したネットワーク内に複数のセッションを後付け**
- **複数のベンダが上記問題に気付いていたが病院側に知らせていない**

※■詳細な接続を把握できておりませんが、外部通信があるため何らかの形で外部に出ていると思われます。

医療施設に対するサイバー攻撃のターゲットポイント(今後)



医療業務用システムのネットワーク構成

©2023 Medical ISAC Japan All Rights Reserved

Agenda

・医療ISACのご紹介

・医療機関における被害事例の実態と学ぶべき教訓

・厚生労働省「医療情報システムの安全管理ガイドライン第6.0版」および「医療法施行規則の一部改正」について

・経済産業省・総務省ガイドラインの活用方法について

・医療機関として検討すべき対策について

©2023 Medical ISAC Japan All Rights Reserved

医療情報システムの安全管理に関するガイドライン 第5.2版（令和4年3月）

ルールベースの記載（To Do List形式）
一律で
「C.　最低限のガイドライン」と
「D.　推奨されるガイドライン」
を提示する。

採用しているシステムの態様や、医療機関の運用等により場合分けが発生するため（オンプレミス型かクラウド型か等）、場合分けの記載が必要となり、ページ数が増加して、読む側としてわかりにくい。

6.4.　物理的安全対策

B.　考え方

物理的安全対策とは、医療情報システムにおいて個人情報が入力、参照又は格納される端末や情報媒体等を物理的な方法によって保護することである。具体的には情報の種別、重要性と利用形態に応じていくつかのセキュリティ区画を定義した上で、以下の事項を考慮して、適切に管理する必要がある。

- 入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理）
- 盗難、覗き見等の防止
- 機器、装置、情報媒体等の盗難や紛失防止も含めた物理的な保護及び措置

また、医療情報システムを格納するデータセンター等の場所については、6.2.3 章のリスク分析を踏まえて、適切に選定することが重要である。

なお、情報及び情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、6.9 章に記載しているので参照すること。

C.　最低限のガイドライン

1. 個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。
2. 個人情報を入力・参照できる端末が設置されている区画は、業務時間帯以外は施錠するなど、運用管理規程等に基づき許可された者以外の者が立ち入ることができないようにするための対策を実施すること。ただし、上記の対策と同等レベルの他の対策がある場合はこの限りではない。
3. 個人情報が保存されている機器が設置されている区画への入退管理を実施すること。例えば、次に掲げる対策を実施すること。
   - 入退者に名札等の着用を義務付ける。
   - 台帳等によって入退者を記録する。
   - 入退者の記録を定期的にチェックし、妥当性を確認する。
4. 個人情報が保存されている機器等の重要な機器に盗難防止用チェーン等を設置すること。
5. 個人情報が入力・参照できる端末の覗き見防止対策を実施すること。

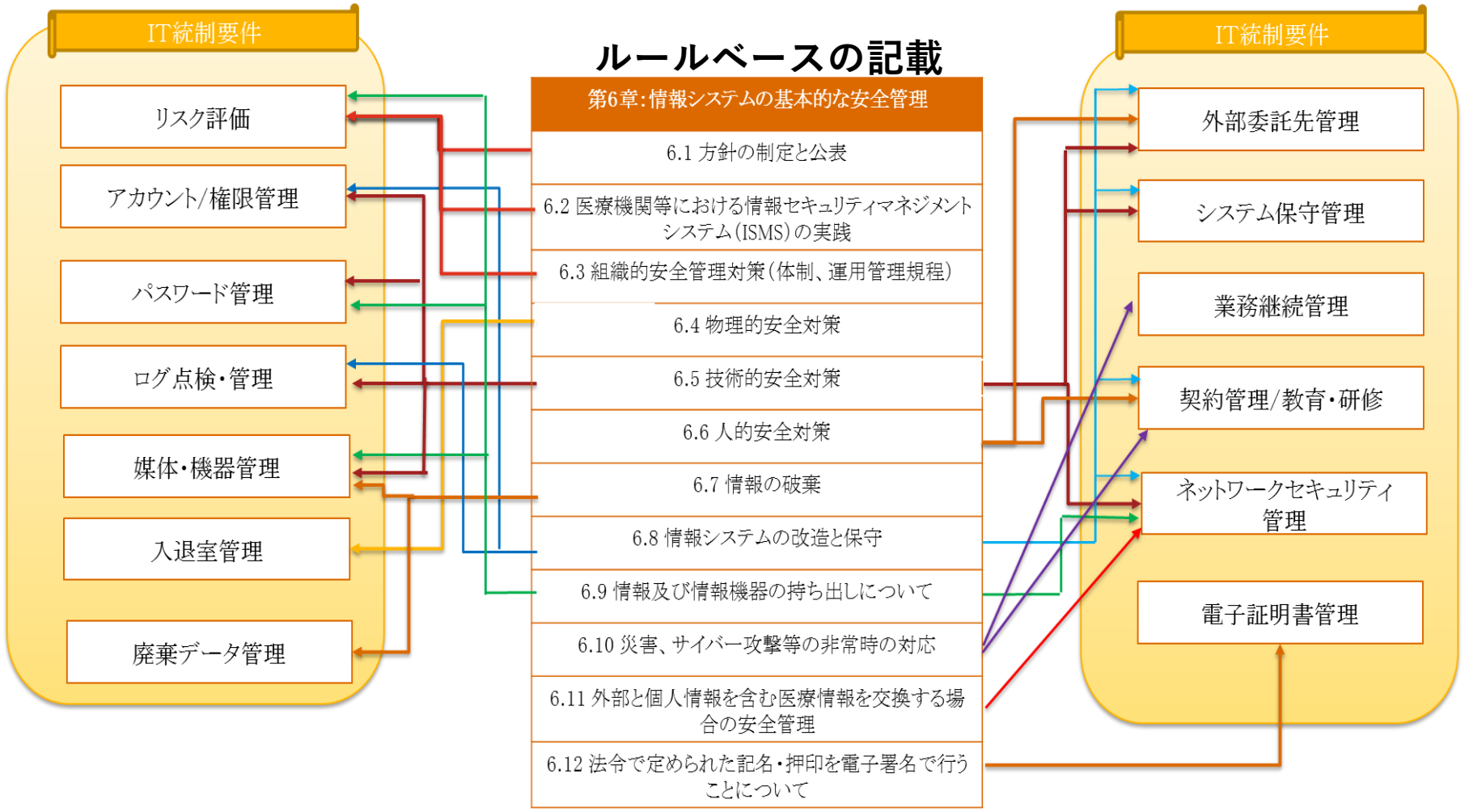
D.　推奨されるガイドライン

1. 情報管理上重要な区画に防犯カメラ、自動侵入監視装置等を設置すること。

©2023 Medical ISAC Japan All Rights Reserved

ルールベースとリスクベースのアプローチ

厚生労働省の医療情報システムの安全管理に関するガイドラインと
会計監査で求められるIT内部統制要件の関連性イメージ図



リスクベースの記載の利点

1．管理統制側の視点から
　何をすべきかわかりやすい
（IT統制要件）
2．大幅なページ数削減
3．自施設に当てはまらない
　項目はスキップ可能

リスクベースの記載の課題
1．ユーザ側が自らのシステムを把握し、リスク評価ができることが前提となる

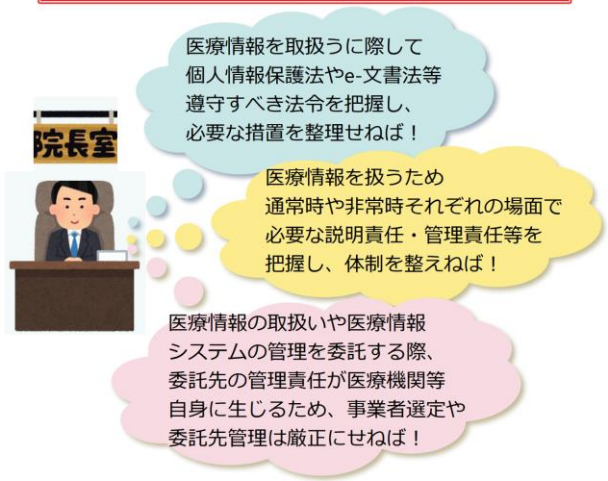
MITSF：「厚生労働省「医療情報システムの安全管理に関するガイドライン4.2版」のガイダンス 1.0版」より

©2023 Medical ISAC Japan All Rights Reserved

厚生労働省
ガイドライン第6.0版
経営管理編概要

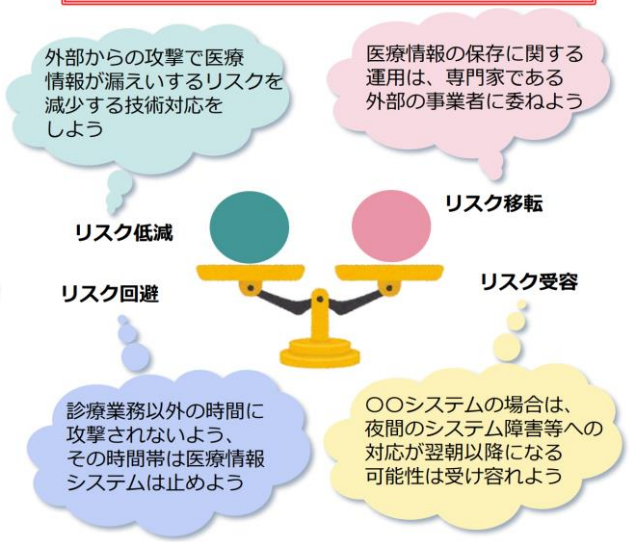
1．医療機関等における情報や情報システムの安全管理に関する責任・責務

◆医療機関等で取扱う医療情報や医療情報システムに関する法令を遵守
◆医療機関等が負う安全管理に関する責任（説明責任、管理責任など）の内容を理解した上で対応



2．リスク評価を踏まえた管理

◆医療機関等で取扱う医療情報や医療情報システムを取り巻くリスクを理解
◆リスク評価結果への対応判断を行い、適切なセキュリティ対策を実施



3．安全管理全般（統制、設計、管理等）

◆医療機関等において組織として体系的に医療情報システムの安全管理を実施
◆安全管理に必要な統制（規程、体制）や設計（セキュリティ対策、教育・訓練）、管理（自己点検、内部/外部監査）を実施

4．安全管理に必要な対策項目

◆医療機関等の特性や医療情報システムの構成を踏まえて、安全管理に必要なセキュリティ対策の概要を把握し、管理されていることを確認

5．情報システム・サービス事業者との協働

◆委託する情報システム・サービス事業者との間で、責任分界、役割分担を明確化
◆委託する事業者との協働を前提とした適切な安全管理の体制を構築

厚労省ガイドライン
で初めて「リスク評価」
の文言が登場

遵守事項

5．1　事業者選定

本ガイドライン、法令等が求める要件を満たす事業者を選定する。
JIS Q 15001またはJIS Q 27001（これと同等の規格含む）の認証を受けていることを確認する。

©2023 Medical ISAC Japan All Rights Reserved

サイバーセキュリティの確認のためのチェックリスト（案）

ガイドラインを遵守することを前提に、特に重要な項目のチェックリストを提示する

【医療機関において確認する項目】

大項目	項番	チェック項目
1 体制構築	1－1	医療機関に医療情報システム安全管理責任者を配置している。
2 情報システムの管理	2－1	医療機関において、以下について把握している。
		①　医療機関で用いる端末の一覧
		②　医療機関で用いるネットワーク機器の一覧
		③　医療機関で用いる記録媒体の一覧
		④　医療機関で用いるサーバーの一覧
	2－2	職員の私物や事業者所有の機器等について、診療に関する業務で使用する場合の許可や管理体制が明確になっている。
	2－3	医療機関は、既に報告されている脆弱性について、事業者から最新の安全性に関する確認結果の報告を受けている。
3 情報システムの運用	3－1	退職者のアカウント等、不要なアカウントを削除する管理体制ができている。
	3－2	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。
	3－3	ネットワーク機器（※）にセキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。 （※）VPN機器を含むインターネットとの接続を制御するルータ。
	3－4	サーバーでアクセス記録（アクセスログ）の管理をしている。
	3－5	ネットワーク機器にアクセス制限を実施している。
4 インシデント発生時の対応	4－1	サイバー攻撃を受ける等システムに重大な障害が発生したことを想定した事業継続計画（BCP）を策定済み、又は、令和５年度中に策定予定である。
	4－2	インシデント発生時に備えて、組織内連絡体制と外部関係機関（事業者、厚生労働省及び警察等）への連絡体制を整えている。
	4－3	医療機関において、診療継続のために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。

【事業者において確認する項目】

大項目	項番	チェック項目
1 体制構築	1－1	事業者内に、医療情報システムの管理責任者がいる。
2 情報システムの管理	2－1	事業者は、提供するソフトウェア・機器等の脆弱性に関して、医療機関への導入時、以降適時、求められる安全性に関する状況（初期PWの変更、脆弱性の更新状況）を確認し、医療機関にその結果を報告し、対応している。
3 情報システムの運用	3－1	ネットワーク機器（※）にセキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。 （※）VPN機器を含むインターネットとの接続を制御するルータ。
	3－2	サーバーでアクセス記録（アクセスログ）の管理をしている。
	3－3	ネットワーク機器にアクセス制限を実施している。
4 インシデント発生時の対応	4－1	事業者は、インシデント発生時、事前に明確化している責任分界点に応じて対応できる体制を整えている。
	4－2	事業者は、バックアップについての保管及び取り扱いについて、医療機関に取り扱い説明書等の文書として提供している。

©2023 Medical ISAC Japan All Rights Reserved

「医療法施行規則の一部改正」

改正概要・対応の方向性

- ○　医療法施行規則第14条第２項を新設し、病院、診療所又は助産所の管理者が遵守すべき事項として、サイバーセキュリティの確保について必要な措置を講じることを追加する。
- ○　令和５年３月10日公布、４月１日施行
- ○　「必要な措置」としては、最新の「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」という。）を参照の上、サイバー攻撃に対する対策を含めセキュリティ対策全般について適切な対応を行うこととする。
- ○　安全管理ガイドラインに記載されている内容のうち、優先的に取り組むべき事項については、厚生労働省においてチェックリストを作成し、各医療機関で確認できる仕組みとする。
- ○　また、医療法第25条第１項に規定に基づく立入検査要綱の項目に、サイバーセキュリティ確保のための取組状況を位置づける。

省令

○厚生労働省令第二十号

医療法（昭和二十三年法律第二百五号）第十七条の規定に基づき、医療法施行規則の一部を改正する省令を次のように定める。

令和五年三月十日

厚生労働大臣　加藤　勝信

医療法施行規則の一部を改正する省令

医療法施行規則（昭和二十三年厚生省令第五十号）の一部を次の表のように改正する。

（傍線部分は改正部分）

改正後	改正前
第十四条　病院又は診療所の管理者は、その病院又は診療所に存する医薬品、医療機器及び再生医療等製品につき医薬品医療機器等法の規定に違反しないよう必要な注意をしなければならない。	**第十四条**　病院又は診療所の管理者はその病院又は診療所に存する医薬品、再生医療等製品及び用具につき医薬品医療機器等法の規定に違反しないよう必要な注意をしなければならない。
2　病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を確保するために必要な措置を講じなければならない。	（新設）

附　則

この省令は、令和五年四月一日から施行する。

医療法２５条に基づく立入り検査において、サイバーセキュリティ対策についても検査対象となる

©2023 Medical ISAC Japan All Rights Reserved

令和５年度立入検査要綱

医療法第25条第１項の規定に基づく立入検査要綱の項目に、サイバーセキュリティ確保のための取組状況を位置づけた（令和５年６月）。

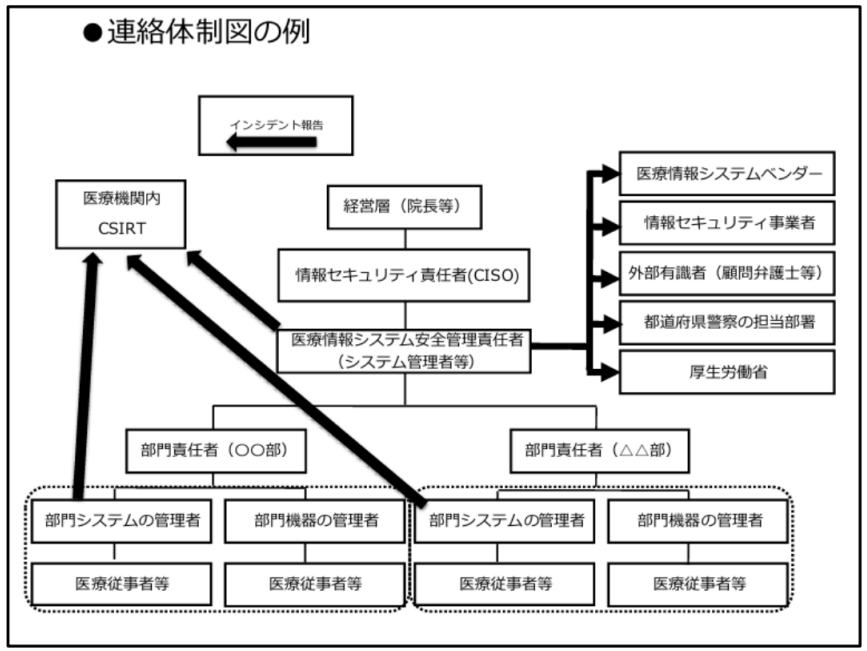
（改正内容）

●新規項目を設け（2-19）、備考欄に以下の内容を記載。

2-19 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ているか

- 必要な措置については、「医療情報システムの安全管理に関するガイドライン第6.0版」を参照。
- 医療機関において優先的に取り組むべき事項として、「医療機関におけるサイバーセキュリティ対策チェックリスト」及び「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」におけるチェックリストに必要な事項が記入されているかを確認。
- 上記チェックリストにおいて医療機関に求める項目のうち、インシデント発生時の連絡体制図については、連絡体制図の提示を求めることにより、その有無を確認。

●連絡体制図の例



©2023 Medical ISAC Japan All Rights Reserved

立入検査対策(2023/7~実施予定)

医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

	チェック項目	確認結果（日付）
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ （ / ）

○ 令和５年度中

*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*２（２）及び２（３）については、事業者と契約していない場合には、記入不要です。
*1 回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付） 1回目	目標日	2回目
1 体制構築	（1） 医療情報システム安全管理責任者を設置している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**			
	（1） サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（2） リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（3） 事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	サーバについて、以下を実施している。			
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（6） アクセスログを管理している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	ネットワーク機器について、以下を実施している。			
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（8） 接続元制限を実施している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
3 インシデント発生に備えた対応	（1） インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ（ / ）		

● 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。
● 立入検査の際は、チェックリストに必要な事項が記入されているかを確認します。

医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

○ 参考項目（令和６年度中）

*以下項目について、令和６年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

	チェック項目	確認結果（日付） 1回目	目標日	2回目
2 医療情報システムの管理・運用	**サーバについて、以下を実施している。**			
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	端末 PC について、以下を実施している。			
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
3 インシデント発生に備えた対応	（2） インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（3） サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和６年度中に策定予定である。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）

● 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。

医療機関におけるサイバーセキュリティ対策チェックリスト

事業者確認用

○ 令和５年度中

*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1 回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付） 1回目	目標日	2回目
1 体制構築	（1） 事業者内に、医療情報システム等の提供に係る管理責任者を設置している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**			
	（2） リモートメンテナンス（保守）している機器の有無を確認した。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（3） 医療機関に製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出した。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	サーバについて、以下を実施している。			
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（6） アクセスログを管理している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	ネットワーク機器について、以下を実施している。			
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（8） 接続元制限を実施している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）

事業者名：

● 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。

医療機関におけるサイバーセキュリティ対策チェックリスト

事業者確認用

参考項目（令和６年度中）

*以下項目について、令和６年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

	チェック項目	確認結果（日付） 1回目	目標日	2回目
2 医療情報システムの管理・運用	**サーバについて、以下を実施している。**			
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	端末 PC について、以下を実施している。			
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）

各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。

001107854.pdf (mhlw.go.jp)

©2023 Medical ISAC Japan All Rights Reserved

パブコメ結果の総括

パブコメ対応結果は、パブコメ対象ガイドラインを取り巻く内外の環境変化を踏まえた観点より、ガイドラインドラフトで強化すべき範囲、あるいは他GLとの平仄観点より整合させるべき範囲を中心に反映が行われることが多い。
その観点で見た場合、厚労省安全管理GLは旧版から主に以下のポイントが集中的にフォーカス＝強調されていると言える。

病院に医療情報システムを提供している業者は、Pマーク or ISMSを取得してないと原則NG

現場へのセキュリティ投資（カネ）の確保には、病院長がコミットすべき。

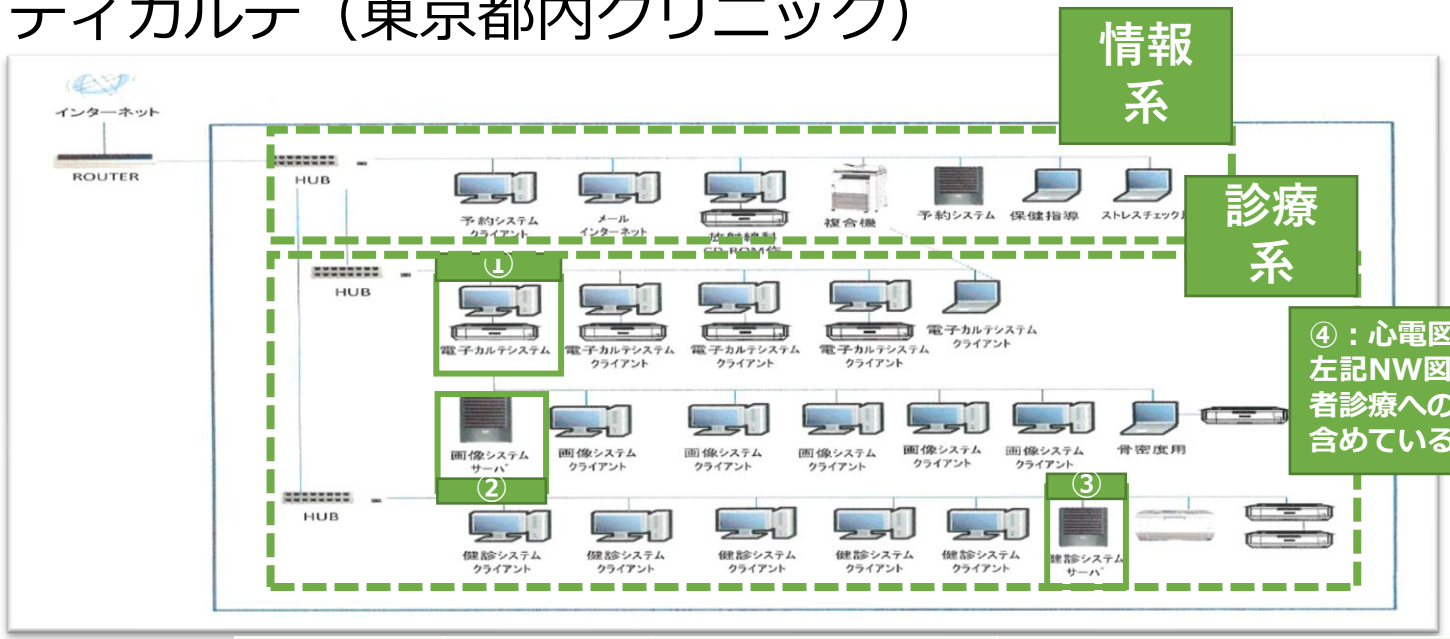
医療IoT等、医療機器/医療情報システムのどっちかよく分からないモノにはIMDRFによるカバーも業者に求めるべし。

サイバーセキュリティ対策はもう医療法施行規則の一部で、医療安全管理の一部です

©2023 Medical ISAC Japan All Rights Reserved

医療ISACの情報セキュリティカルテ（東京都内クリニック）

調査対象
①：電子カルテシステム
②：画像システムサーバ
③：健診システムサーバ
④：心電図・眼底検査等システム



④：心電図・眼底検査等システムは左記NW図上には記載がないが、患者診療への影響が大きいため対象に含めている

調査項目１：事業者向けGL- 4.4第三者認証等の取得に係る要件

貴社ではプライバシーマーク認定またはISMS 認証を取得していますか？

調査項目２：事業者向けGL-「4.1. 医療機関等へ情報提供すべき項目」

『医療機関等との共通理解を 形成するため に情報提供す べき項目』として定義される情報が確認できる資料をご提供ください。

事業者	提供システム	調査項目①		調査項目②		補足（対応の真摯度）
		回答内容	調査結果	情報提供状況	調査結果	
A社	電子カルテシステム	回答無し	NG	情報提供なし	NG（情報提供自体がないため判断不可）	リモート用のVPN機器を利用しているが、当該機器の脆弱性対応有無の回答も含め、一切リプライなし
B社	PACS	ISMS/Pマークともに未取得	NG	情報提供なし	NG（情報提供自体がないため判断不可）	メールでのリプライのみ
C社	健診システム	・Pマーク取得 ・ISMS未取得	OK	情報提供なし	NG（情報提供自体がないため判断不可）	メールでのリプライのみ
D社	心電図・眼底検査等システム	ISMS/Pマークともに未取得	NG	情報提供なし	NG（医療機関向け安全管理GLに未対応との回答）	4社のうち唯一、紙面での回答提出あり

Agenda

- 医療ISACのご紹介
- 医療機関における被害事例の実態と学ぶべき教訓
- 厚生労働省「医療情報システムの安全管理ガイドライン第6.0版」および「医療法施行規則の一部改正」について

- **経済産業省・総務省ガイドラインの活用方法について**
- 医療機関として検討すべき対策について

©2023 Medical ISAC Japan All Rights Reserved

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

経済産業省・総務省

令和 2 年 8 月

https://www.meti.go.jp/press/2020/08/20200821002/20200821002-3.pdf

4. 対象事業者と医療機関等の合意形成

本章では、対象事業者が医療機関等と適切な合意形成を行うにあたり、医療機関等へ情報提供すべき項目、医療機関等との役割分担の明確化、医療情報システム等の安全管理に係る評価及び、第三者認証等の取得に係る要件について示す。

4.1. 医療機関等へ情報提供すべき項目

対象事業者と医療機関等の合意形成においては、対象事業者から医療機関等への適切な情報提供が必要である。合意形成のために提供すべき情報とは何であるかを表 4-1 に示す[14]。対象事業者は、これら項目に係る情報提供にあたっては、医療機関等が容易に理解可能となるよう努め、適切に共通理解を得ること。

4.2. 医療機関等との役割分担の明確化

医療情報システム等の安全管理には、対象事業者と医療機関等の双方における適切な運用管理を行うこと。例えば、医療情報システム等が堅牢なアクセス制御機能を持っていたとしても、医療機関側の利用者がパスワードを利用端末に貼っていたり、アカウントを複数で共有していたりすれば、医療情報を守ることはできない。

したがって、対象事業者は、合意形成にあたり、医療機関等における運用管理も踏まえた形で、役割分担を定めること。具体的には、4.1 で示した医療機関等の運用管理規程に定める必要がある事項として、医療機関等へ対応を求める内容を含めること。

リスクアセスメント→リスクコミュニケーション

©2023 Medical ISAC Japan All Rights Reserved

表 4-1 医療機関等へ情報提供すべき項目

目的		情報提供すべき項目
医療機関等が医療情報安全管理ガイドラインに基づき「外部保存を受託する事業者の選定基準」として少なくとも確認する必要がある項目		医療情報等の安全管理に係る基本方針・取扱規程等の整備状況
		医療情報等の安全管理に係る実施体制の整備状況
		実績等に基づく個人データ安全管理に関する信用度
		財務諸表等に基づく経営の健全性
医療機関等との共通理解を形成するために情報提供すべき項目	医療機関等との役割分担の明確化（4.2 参照）	医療機関等の運用管理規程に定める必要がある事項
	医療情報システム等の安全管理に係る評価（4.3 参照）	医療情報システム等の安全管理に係る評価の結果
	リスクアセスメントの成果物（5.1.1、5.2.1 参照）	医療情報システム等の全体構成図
	リスク対応の成果物（5.1.5、5.2.2 参照）	リスク対応一覧
	運用管理規程に含める事項（5.1.6 参照）	医療情報システム等の安全管理に係る基本方針
		医療情報システム等の提供に係る体制
		契約書・マニュアル等の文書の管理方法
		機器等を用いる場合の機器等の管理方法
		リスク対応策の運用方法
		事故発生時の対応方法及び医療機関等への報告方法
		医療情報を格納する記憶媒体の管理方法
		医療情報の外部保存に係る患者等への説明方法
		医療情報システム等に対する監査の実施方針
		医療機関等の管理者からの問い合わせ窓口
	制度上の要求事項への対応の成果物（第 6 章参照）	制度上の要求事項への対応

医療機関等からこれらの情報を業者に求めることが重要

＊リスク特定

不正な閲覧・操作、ネットワーク上の盗聴なりすまし、高度サイバー攻撃、情報の摂取・漏洩、情報の改竄・破壊、医療情報システムの停止、技術的脆弱性の混入、機器・記憶媒体の持出し時の紛失・盗難、施設への物理的侵入、災害等

＊リスク評価

表 5-2 リスクレベルの分類例

影響度			顕在化率 きわめて低い（ほとんど起こらない） 1	低い（まず起こらない） 2	中程度（起こる可能性がある） 3	高い（起こる可能性が高い） 4	きわめて高い（頻繁に起こる） 5
	きわめて小さい	1	1	2	3	4	5
	小さい	2	2	4	6	8	10
	中程度	3	3	6	9	12	15
	大きい	4	4	8	12	16	20
	きわめて大きい	5	5	10	15	20	25

リスクレベル（ランク）	影響度×顕在化率
S	20～25
A	10～16
B	5～9
C	2～4
D	1

＊リスク対応

表 5-3 リスク対応の選択肢

選択肢	概要
リスク低減	リスクへの対策を行うことで、リスクレベル（顕在化率及び影響度）を低減させる。
リスク回避	リスクを生じさせる情報流を廃止したり、別の情報流に変更する。
リスク移転（リスク共有ともいう）	保険への加入により金銭面での損失に備えたり、医療情報システム等の運用を外部に委託することで専門的な業者の管理下に置いたりする。
リスク保有（リスク受容ともいう）	意思決定に基づき、残存するリスクの顕在化により生じ得る被害や金銭面での損失を受容する。

＊リスクコミュニケーション

©2023 Medical ISAC Japan All Rights Reserved

３省２ガイドラインの相互関連性

医療機関が遵守すべきGL

「医療情報システムの安全管理に関するガイドライン 第6.0版」（厚生労働省 2023/5） **経営管理編**

5.1 事業者選定

遵守事項①： ② 委託する事業者を選定する場合には、**JIS Q 15001（プライバシーマーク）、JIS Q 27001（ISMS）**又はこれと同等の規格の認証 を受けているシステム関連事業者を選定するよう指示すること。

5.2.2 体制管理

① 委託するシステム関連事業者に対して、業務実行体制を明確にし、医療情報の取扱い及び医療 情報システムの管理に関して再委託を行う場合には、**事前に医療機関等に情報を提供し、協議・ 合意形成を経た上で承認を得る**こと等を契約の内容に含めるよう、企画管理者に指示すること。

5.3 委託における責任分界

遵守事項①：システム関連事業者に委託を行う際の責任分界の管理に関する重要性を認識し、医療機関と委 託先事業者との間での責任分界を明確にし、認識の齟齬等が生じないよう、書面等により可視化 し、適切に管理することを、企画管理者やシステム運用担当者に指示すること。

相互連携

事業者が遵守すべきGL

「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v.1.1」
（経済産業省・総務省2023/6）

4.対象事業者と医療機関等の合意形成

4.1. 医療機関等へ情報提供すべき項目

対象事業者と医療機関等の合意形成においては、対象事業者から医療機関等への適切な 情報提供が必要である。対象事業者は、これら項目に係る情報提供にあたっては、医療機関等が容易に理解可能となるよう努め、適切に共通理解を得ること。

4.2. 医療機関等との役割分担の明確化

対象事業者と医療機関等の双方における適切な運用管理を行うこと。対象事業者は、合意形成にあたり、医療機関等における運用管理も踏まえた形で、役割分担を定めること。

4.3. 医療情報システム等の安全管理に係る評価

医療情報システム等の安全管理に係る評価を行い、評価結果を医療 機関等へ情報提供すること。対象事業者内部の独立した監査部門や第三者機関が評価を行うことが望ましい。

4.4. 第三者認証等の取得に係る要件

情報セキュリティに係る公的な第三者認証として、**プライバシーマーク認定または ISMS 認証**を取得すること。

医療機関の負う３つの責任

①患者に対する 「説明責任」
②事業者に対する「管理責任」
事業者に任せきりにしているだけでは、これを果たしたことにはならない
・定期的報告、・責任の所在の明確化、・事業者の監督
③「定期的に見直し必要に応じて改善を行う責任 」

事業者が守るべきGL

リスクコミュニケーション

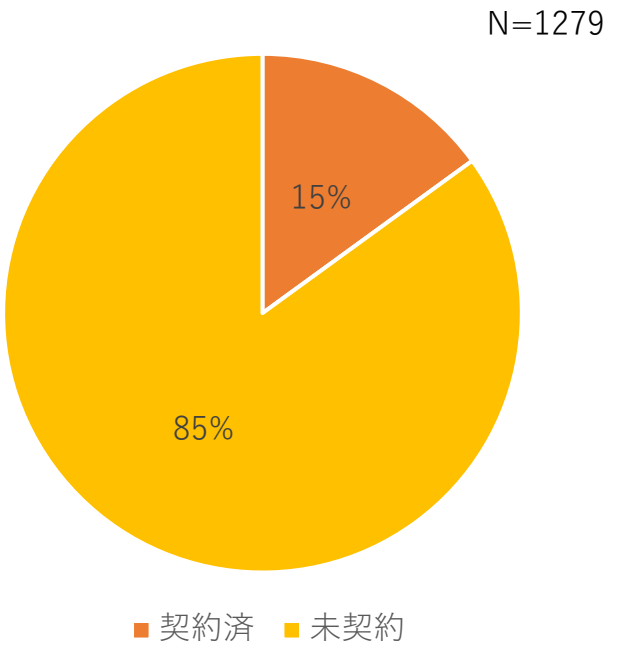
©2023 Medical ISAC Japan All Rights Reserved

＜アンケート調査結果_全体結果＞

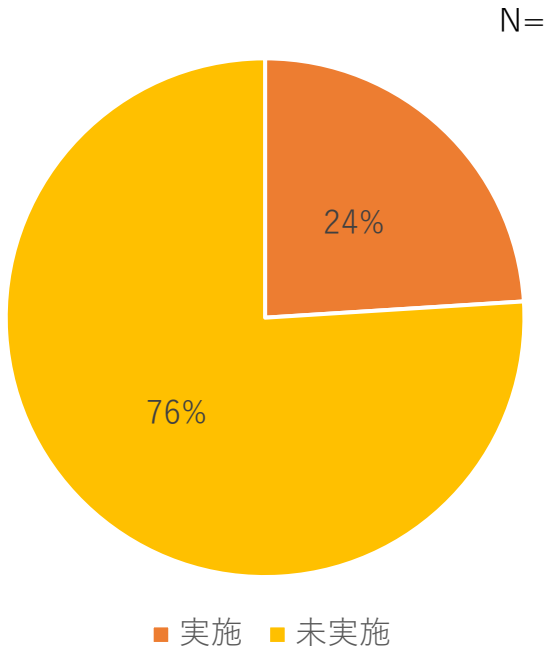
- **実施期間：2022年11月～12月**
- **対象組織合計数：1279件（全国保険医団体連合会897件、日本病院会382件）**

【③：医療機関/ベンダーとのリスクコミュニケーション状況】

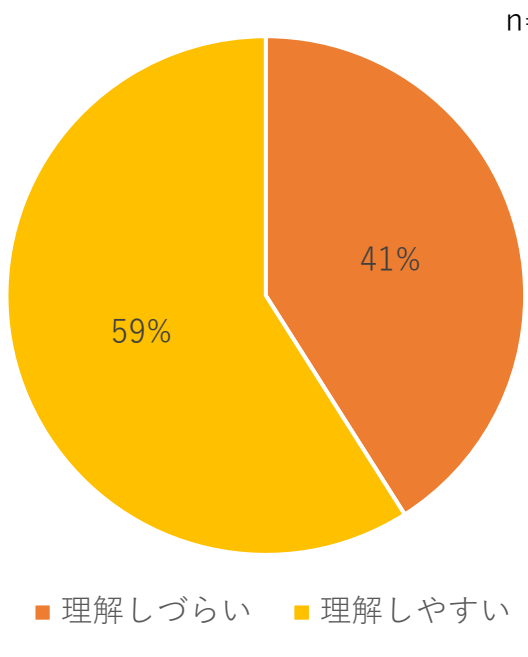
＜Q6：契約書・SLAにおけるセキュリティ責任分界を定めていないと回答した組織の割合＞



＜Q7：ベンダからの運用報告等の内容確認を行っていると回答した組織の割合＞



＜Q８：ベンダ報告は理解しづらく、院内セキュリティ向上にプラスになっていないと回答した組織の割合＞



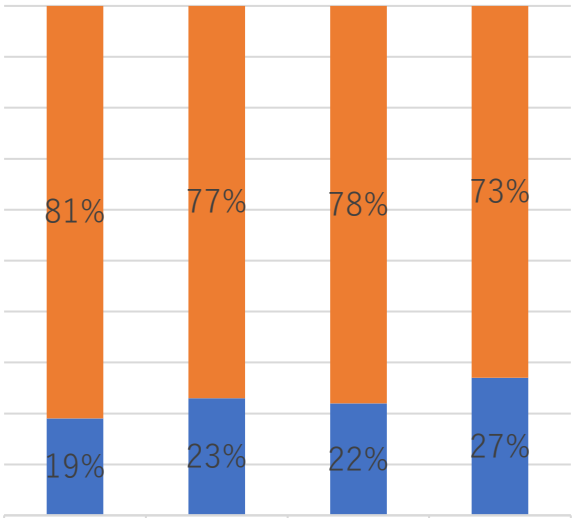
ベンダと契約等でセキュリティの役割・責任を定めている組織の割合は**15%**、さらにベンダからセキュリティ等も含めた報告を行わせている組織は**24%にしか満たない**。
報告を受けている組織においてもその内容は理解しづらく、セキュリティ向上に資さないと回答した割合は**41%**に及んだ。

©2023 Medical ISAC Japan All Rights Reserved

電子カルテベンダによるリスクコミュニケーションへの取組姿勢（参考）

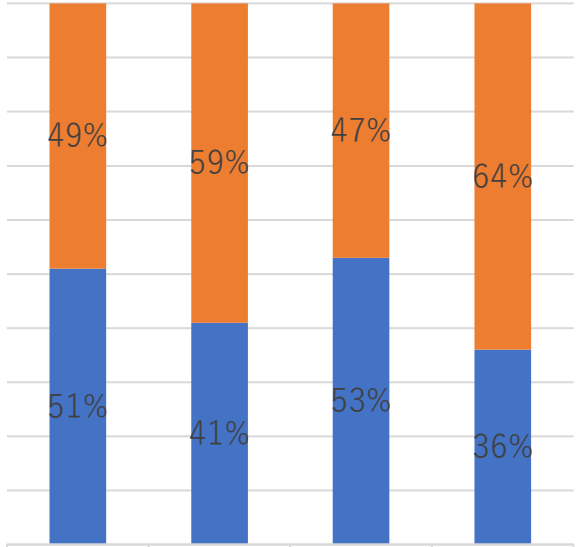
電カルベンダ	導入数
F社（富士通）	１４１件
S社（SSI）	６４件
N社（NEC）	６０件
C社（CSI）	２２件

①：契約書・SLAにおけるセキュリティ責任分界の定義・締結を電カルベンダと行っているか



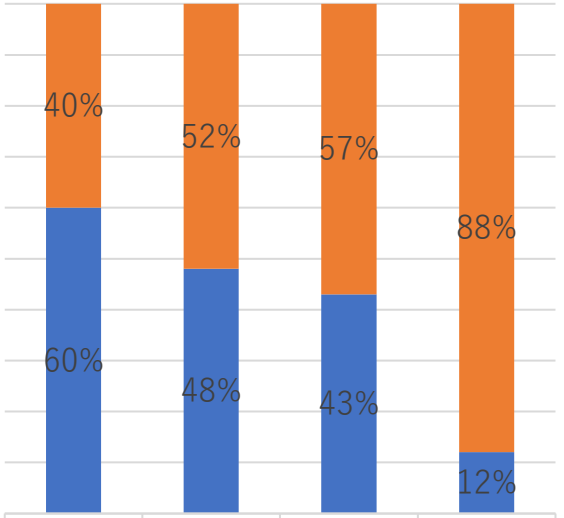
	F社	S社	N社	C社
いいえ	81%	77%	78%	73%
はい	19%	23%	22%	27%

②：電カルベンダからの運用報告等の内容確認を行っているか



	F社	S社	N社	C社
いいえ	49%	59%	47%	64%
はい	51%	41%	53%	36%

③：②が「はいの場合」、電カルベンダからの報告・情報提供内容は、理解しづらく、院内セキュリティ向上に役立たないものか？



	F社	S社	N社	C社
いいえ	40%	52%	57%	88%
はい	60%	48%	43%	12%

※すべての質問ともに、「いいえ」は「わからない」も含む

電カルベンダとの間で**セキュリティに係る契約締結は全体の2割程度**しか行われていない。
電カルベンダからの運用報告の確認は**医療機関の半数程度が行っているが、その内容の分かりやすさ・セキュリティ上の有用性にはベンダごとに差がある**ことがわかる。

©2023 Medical ISAC Japan All Rights Reserved

Agenda

・医療ISACのご紹介

・医療機関における被害事例の実態と学ぶべき教訓

・厚生労働省「医療情報システムの安全管理ガイドライン第6.0版」
および「医療法施行規則の一部改正」ついて

・経済産業省・総務省ガイドラインの活用方法について

・医療機関として検討すべき対策について

©2023 Medical ISAC Japan All Rights Reserved

厚労省ガイドライン6.0版に基づく対応モデル

組織体制見直し

システム管理責任者
サイバーセキュリティ担当者

委員会組織

文書類
- システム運用管理規程
- 障害時マニュアル（IR）
- BCPマニュアル（訓練方針含む）
- システム事業者との契約書類
- 委員会規程
- 委員会議事録
- 従業員研修方針
- 委託先管理方針
- 他

IT資産棚卸し

システム構成図
ネットワーク構成図

リスクアセスメント

リスク評価に基づく
対応方針の決定

リスク低減：技術的対策、運用的対策

リスク回避：情報流変更

リスク移転：損害保険加入

リスク受容・敢えて何もしない

リスクコミュニケーション

保守契約書
SLA

対策実行 → PDCA

©2023 Medical ISAC Japan All Rights Reserved

医療機関として検討すべき対策について

検討すべき課題	ソリューション例
• 情報収集	医療ISACセキュリティニュース
• 体制整備（責任者、会議体、規程類）	Shared CISO Service
• 自施設およびサプライチェーンのリスクアセスメント	脅威インテリジェンス診断活用
• ランサムウエア対応のバックアップ導入	
• Emailセキュリティ	DMARC
• Webセキュリティ	Cloud FLARE
• 従業員教育	
• BCP策定と図上訓練（Incident Response訓練含む）	Shared CISO Service
• 端末保護(EPP/EDR/XDR)	
• サイバー保険加入	
•	
•	
•	
•	
•	

©2023 Medical ISAC Japan All Rights Reserved

医療ISAC会員（一般会員）になるメリット

1．日本語のサイバーセキュリティ関連のニュース配信（医療ISACセキュリティニュース他）をほぼ毎日無料で受信できます
2．月一回の医療ISACセミナー（オンライン）および年１回の日米合同ワークショップ（ハイブリッド形式）に無料参加できます（過去のセミナーのトピックス例は以下）。
   - 厚労省ガイドライン改訂の解説
   - 医療法施行規則の一部改正に伴う立ち入り検査対策
   - 最新セキュリティトピックス
   - 会員医療機関の成功事例紹介
   - 個人情報保護法改正への対応
3．医療ISAC会員により構成される種々のワーキンググループに無料で参加できます。
4．自施設のサイバーセキュリティに関して約１時間のオンライン無料相談を受けられます
5．自施設のドメインに関するダークウエブ上の情報（ハッカーらのフォーラム、e-mail等の資格情報、BOT net情報、サーバへの侵入情報等）のチェックを受けられます（無料）
6．医療ISACが提供する以下の有償のサイバーセキュリティサービスを受けられます
   1）医療ISAC規定認証
   2）医療ISAC脅威インテリジェンス診断（Attack Surface診断、サプライチェーンリスク診断等）
7．医療ISACの会員で構成される”信頼できるコミュニティ”の一員として、当事者ならではの最新で具体的な情報、他施設での取組状況や課題、被害施設における実態等の情報を無料で得ることができます
8．医療ISACの会員になることにより、自施設がサイバーセキュリティに対して積極的に取り組んでいることを対外的に明示できます

サイバーセキュリティ対策は医療機関の社会的責任

- 医療機関は患者の機微な個人情報を預かって医療という事業を行っています。
- 従って**患者に対する説明責任**と、電子カルテ等の**委託事業者に対する管理責任**が発生します。
- 一昨年来の医療機関のサイバー被害の多発により、今年度より医療機関に対するサイバーセキュリティ対策について**法的要請**が具体的に課せられます。
- 知らなかった、予算がない、人がいない、は言い訳になりません。
- **自分事**として捉えましょう

是非医療ISACにご登録ください（無料です）

https://www.m-isac.jp/

オンライン無料相談をお待ちしております

©2023 Medical ISAC Japan All Rights Reserved