静岡県保険医協会セミナー

医療機関に対するサイバー攻撃の実態と、事例から見える教訓、直ちに行うべき対策について

2023年1月20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

Agenda

0．医療ISACの活動紹介

1．医療機関におけるランサムウェア感染の事例から導出される教訓
　：特にFortiOSおよびデータバックアップについて

2．システムおよび医療機器ベンダーとの付き合い方
　：「セキュリティはベンダーに丸投げ」で本当によいのか？

3．経済産業省・総務省ガイドラインの活用方法（事例紹介）

4．脅威インテリジェンス診断の有用性

5．医療ISACとして医療機関に対して支援できること

6．質疑応答

Agenda

0．医療ISACの活動紹介

1．医療機関におけるランサムウェア感染の事例から導出される教訓
：特にFortiOSおよびデータバックアップについて

2．システムおよび医療機器ベンダーとの付き合い方
：「セキュリティはベンダーに丸投げ」で本当によいのか？

3．経済産業省・総務省ガイドラインの活用方法（事例紹介）

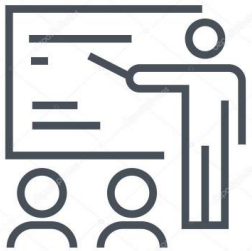
4．脅威インテリジェンス診断の有用性

5．医療ISACとして医療機関に対して支援できること

6．質疑応答

医療ISAC（英語表記：Medical ISAC Japan）

Seminars



22 seminars
& 3 workshops
2014~2022

Services

****MITSF Cloud Exit Security Service***
****Security “119” Service***
****H-ISAC Green Report Localization Service***
****Security Information Service***

WG s

10WGs
2014~2022

Consultation

****DMARC Consultation***
****Operation Management Regulation Consultation***

MITSF が H-ISAC との日本における事業提携を発表

*Medical IT Security Forum (MITSF)*は米国の *Health Information Sharing and Analysis Center (H-ISAC)*の日本における事業に関して事業提携を行いました。

2019 年 2 月 9 日、東京およびフロリダ州タイタスビル発–

日本における医療系のセキュリティ啓発団体である ***Medical IT Security Forum (MITSF:ミッツ)***と、米国の ***Health Information Sharing and Analysis Center (H-ISAC)***は、日本における事業に関して事業提携を締結しました。

H-ISAC は、医療機関および関連する業界に対し、サイバーおよび物理的なセキュリティ上の脅威の未然防御・検出・対応を取るための実用的な情報をタイムリーに提供することで、人命を救うという本来業務に専念できることを目的としたコミュニティです。

本提携は 2019 年 2 月 9 日に東京での記者会見で公表されました。

米国Health ISACとの事業提携
2019~

会員数：法人会員　134施設（医療・福祉事業者）
個人会員　807名、うち医療機関400名、ITベンダー等407名
協力企業　18社

医療ISACの活動概要 （~2022年）

【海外提携活動】

期日	内容
2019年02月	H-ISAC(※1)がMITSF(※2)と提携してH-ISAC Japan Councilを設立。これを医療ISACと共同運用(※3)することで合意
2019年10月	H-ISAC／医療ISAC合同ワークショップ(大手町)
2022年06月	H-ISAC Japan Council　日米合同ワークショップ2022(虎ノ門＆オンライン)

【国内活動（2022年）】

活動形態	項目	実施数
セミナー	「医療ISAC　Security Lecture2022」#001～#010	10件
講演会	医療関連組織に対するセキュリティセミナー (10月以降の5回は、ランサムウエアを含むサイバー攻撃の対策に特化)	21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)	7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）	40施設
アンケート調査(※4)	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	3回

(※1) H-ISAC：Health Information Sharing and Analysis Center(※2) MITSF：Medical IT Security Forum(※3) H-ISAC Japan Council 運営委員会：日本病院会、全日本病院協会、全国老人福祉施設協議会、人間ドック学会、徳洲会インフォメーションシステム、富士フィルムメディカル
(※4) https://www.hospital.or.jp/pdf/06_20220323_01.pdf

Agenda

0．医療ISACの活動紹介

1．医療機関におけるランサムウェア感染の事例から導出される教訓
：特にFortiOSおよびデータバックアップについて

2．システムおよび医療機器ベンダーとの付き合い方
：「セキュリティはベンダーに丸投げ」で本当によいのか？

3．経済産業省・総務省ガイドラインの活用方法（事例紹介）

4．脅威インテリジェンス診断の有用性

5．医療ISACとして医療機関に対して支援できること

6．質疑応答

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）

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（種別不詳）	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？
2022/12/3	金沢西病院	公表	電子カルテの一部閲覧不可	詳細不明	不明

NISC注意喚起（2021/4/30）

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）

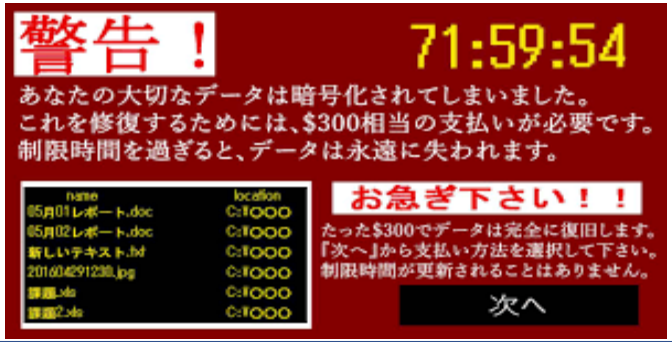
厚労省注意喚起（2022/11/10）

- 米国FortiNet社のVPN機器の脆弱性未対策が原因での侵入事例：11/17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：17/5件

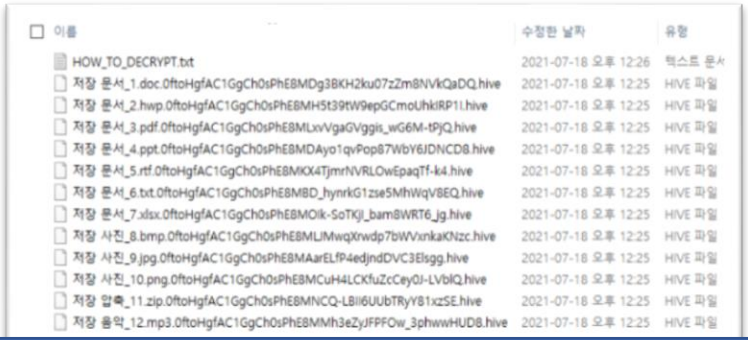
注意喚起の効果は残念ながら不十分！

ランサムウェア感染被害イメージ

■暗号化型ランサムウェアに感染した場合の脅迫画面のイメージ



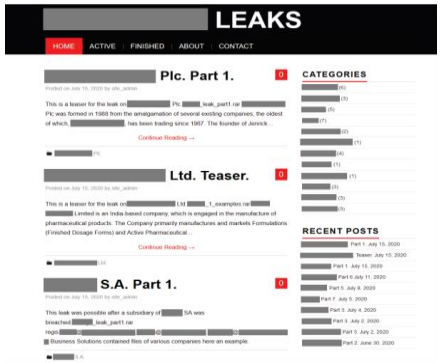
■ランサムウェアに暗号化され、利用不可となったファイル一覧（イメージ）



脅迫画面の表示や脅迫文ファイルがシステム内部に作成され、ファイルの拡張子が通常とは異なる内容へと置き換えられる（暗号化）

■二重脅迫型ランサムウェアに感染した場合の脅迫文イメージ
（暗号化解除、暴露防止のための身代金支払手順が記載）

■ダークウェブ上の窃取データの公開サイト（イメージ）



二重脅迫型の場合は、同様の被害にあった他社の窃取データを公開するダークウェブ上のサイト等へのURLが脅迫ファイルに含まれる場合もある。

ランサムウェア被害多発の総括
（厚生労働省のアプローチの実態と結果）

FortiGateの同一の脆弱性(CVE-2018-13379)により繰り返し侵入を許し、ランサムウェア被害を発生

- **３回の注意喚起のうち２回とガイドライン改訂では、FortiGate等の具体名を挙げてない**
- **いずれの注意喚起も医療機関向けに発出されている**

当該装置は事業者が調達し医療機関に設置・設定した場合が大半であり、医療機関は当該装置が設置されていることも、脆弱性対策が必要であったことも知らなかった場合がほとんどであった。

・上記脆弱性での被害が最初に確認された東大阪医療センターの事例において、厚労省担当者は、***”攻撃者に攻撃が成功したことを知らせることになり被害が続発する恐れがある”***との理由で**“ランサムウェア被害を公表しないよう“に指示**。病院は「システム障害として公表」したため、結局脅威情報が有効な形で共有されず、被害多発を誘発した可能性が高い。

「注意喚起の具体性の欠如」と「情報宛先の不適切性」であったことにより、**最初の被害から１年半以上経過しても同じ原因での被害を繰り返す事態**に立ち至った。
さらに情報共有の在り方も、被害未然防止や被害最小化といった明確な方針が感じられず、取り敢えずのアリバイ作りと言われても仕方ないレベルのものであった。
事実として半田病院の事例を含め、２例目以降は全て防止できたはずの被害であったことを明確に認識し方針自体を再検討しなければ、さらなる被害が続発する可能性が高く、最悪の場合患者の死亡にも繋がりかねない、と危惧される事態である。

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、電子カルテベンダーのWiseman社の持ち込んだFortiGateの脆弱性が放置され、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**

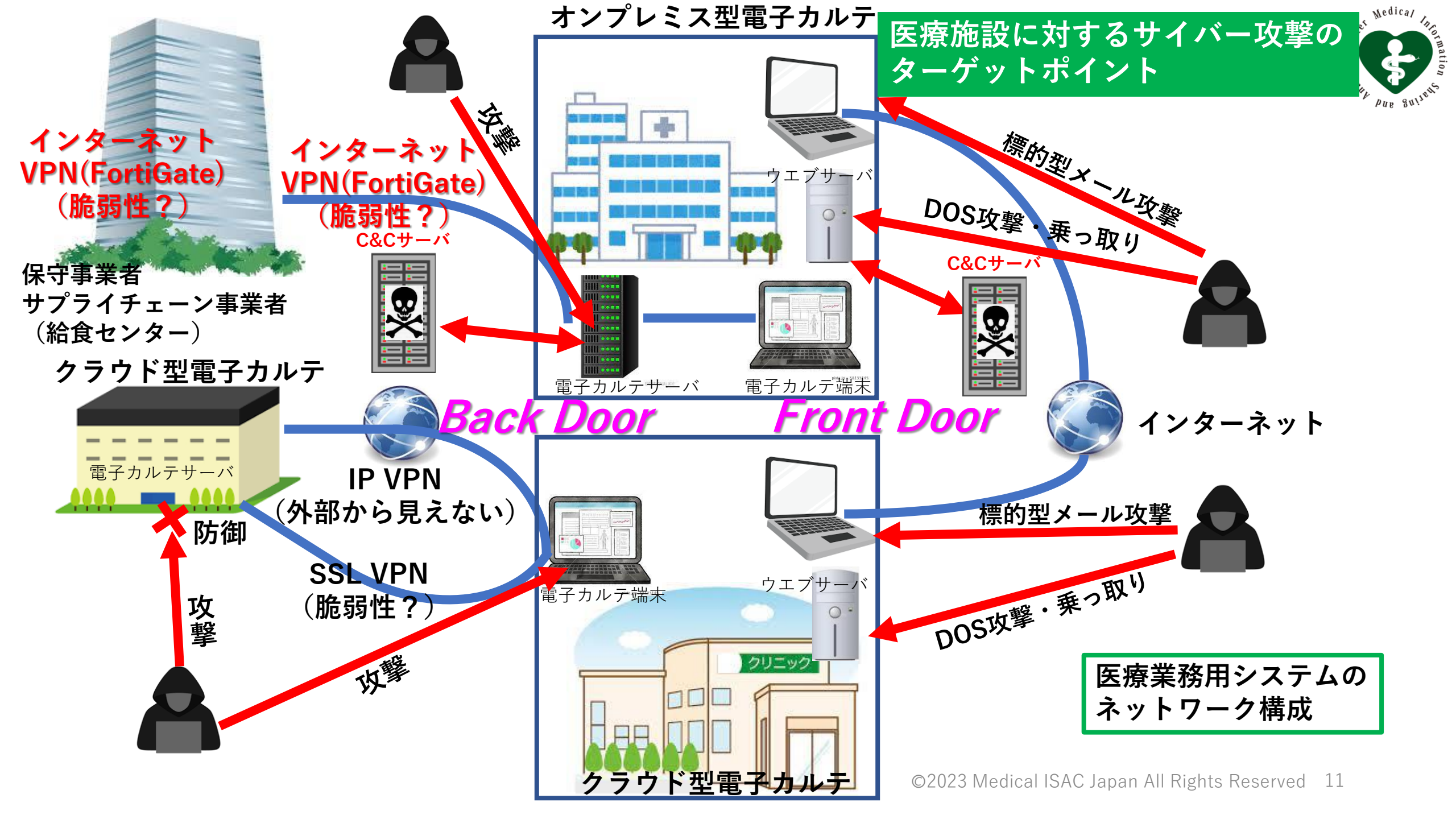
愛知県の産婦人科有床診療所の被害事例(2022/3)から、協立機電工業が持ち込んだFortiGateの脆弱性を特定、電子カルテベンダーのTAK社のアカウント情報が漏洩している１９病院を特定。
TAK社側での脆弱性対策を支援、対策完了確認。**被害未然防止実現**

東京都立の２病院に対する攻撃予兆（DarkWeb上のハッカーのチャット情報）検知(2021/12)。
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、**被害未然防止実現**

大阪市内の医療法人立病院(2022/9)の脅威インテリジェンス調査により、FortiGateの接続元IP制限がかかっていない状態であることを発見(Global IPをURL欄に入力することでログイン画面が表示）。IP制限設定・PW変更により、**被害未然防止実現**

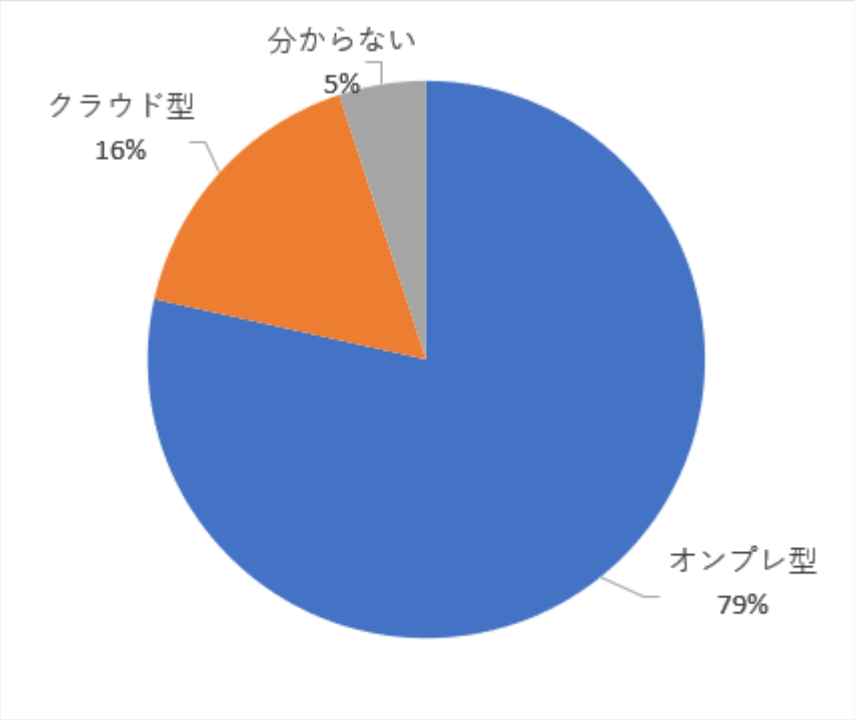
無料相談・被害事例関連情報等から、被害防止につながる調査を医療機関と共に行い、**事業者の協力**を得て被害防止・最小化活動を継続している
株式会社ヘンリー（電子カルテ事業者）、日本事務器、PHC他と協議中

医療施設に対するサイバー攻撃のターゲットポイント



医療業務用システムのネットワーク構成

診療所向け電子カルテ導入シェアランキング2021



グラフ1：導入している電子カルテのタイプ　(n=79)

日経メディカル開業サポート

順位	前回	企業名、代表的な製品名	形式	割合
1位	前回1位	PHC（旧パナソニックヘルスケア）「Medicomシリーズ」	オンプレ型 （クラウド利用可能）	22.8%
2位	前回6位	ユヤマ「BrainBoxシリーズ」	オンプレ型／クラウド型 2製品あり	12.7%
3位	前回5位	ダイナミクス「Dynamics」	オンプレ型	11.4%
同率4位	前回6位	エムスリーデジカル「M3 DigiKar」	クラウド型	5.1%
同率4位	NEW	シィ・エム・エス「Doctor's Desktop3」	オンプレ型	5.1%
同率4位	前回10位	富士フィルムヘルスケアシステムズ（旧日立ヘルスケアシステムズ）「Hi-SEEDシリーズ」	オンプレ型／クラウド型 2製品あり	5.1%
同率4位	前回2位	富士通Japan「HOPEシリーズ」	オンプレ型／クラウド型 2製品あり	5.1%
同率8位	前回9位	キャノンメディカルシステムズ（旧東芝）「TOSMECシリーズ」	オンプレ型	3.8%
同率8位	前回2位	ラボテック「SUPER CLINIC」	オンプレ型	3.8%
同率10位	前回2位	ピー・エム・エル「Medical Station」「Qualis」	オンプレ型	2.5%
同率10位	前回6位	島津メディカルシステムズ「SimCLINIC シリーズ」	オンプレ型	2.5%
同率10位	NEW	DONUTS「CLIUS」	クラウド型	2.5%
同率10位	NEW	MIU「Dopanet Doctors」	オンプレ型	2.5%

表1：電子カルテ導入シェアランキング　(n=79)

厚生労働省医療情報システムの安全管理ガイドライン5.2版(2022/3)

第６章ー５：技術的安全対策

不正ソフトウェアの対策としては、スキャン用ソフトウェアを導入するだけでなく、医療情報システム側の脆弱性を可能な 限り小さくしておくことが重要である。そのために実施すべき対策として、**セキュリ ティ・ホール（脆弱性）が報告されているソフトウェアへのパッチ適用、利用していな いサービスや通信ポートの非活性化、マクロ等の利用停止、メールやファイルの無害化** がある。また、**EDR（Endpoint Detection and Response）**や「振る舞い検知」などの方策も有効である。

第６章ー１０：サイバー攻撃を受けた際の対応

・**バックアップ**からの重要なファイルの復元（重要なファイルは数世代バックアッ プを複数の方式（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）で取得することが重要である）

同じランサムウェア(Lockbit 2.0)に感染した２病院の比較

つるぎ町立半田病院（バックアップまで暗号化）　復旧まで約２か月＋２億円

鳴門山上病院（オフラインバックアップ取得）　復旧まで４日＋数１０万円

バックアップ確保はランサムウェア被害最小化の最後の砦

ランサムウェア対応検討上のポイント
バックアップソリューション

(参考)

検討すべき課題
1．どのバックアップソリューションを採用するか？
2．どの範囲のデータをバックアップ対象とするか？
3．インシデント発生時の対応手順の検討・訓練実施

従来のオンラインバックアップ
←ランサムウエアに対しては無効

オフラインバックアップ：磁気テープ等
←ランサムウエアに対して有効
バックアップ自体にも復元にも時間がかかる

オフサイトバックアップ：クラウド上のデータセンター
←ランサムウエアに対して有効
バックアップ・復元も比較的高速

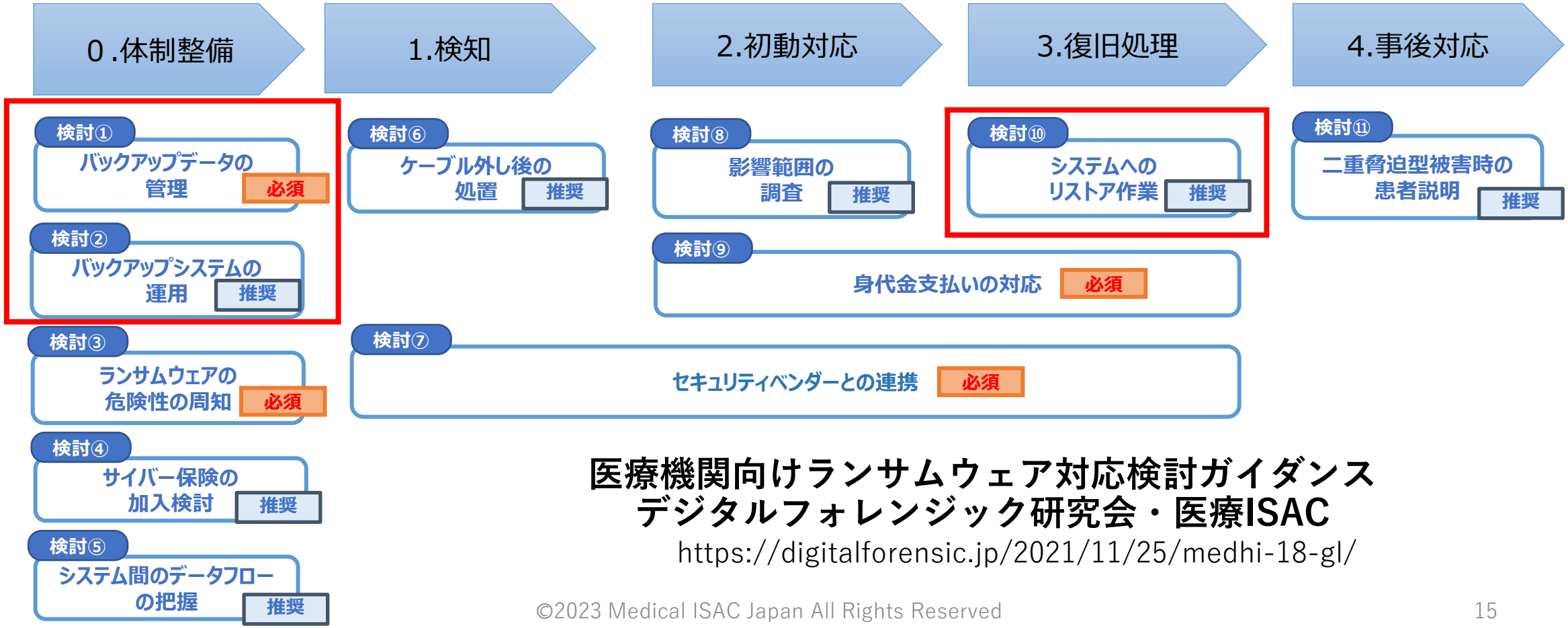
オンラインイミュータブルバックアップ：
ユーザー管理者の権限でも書換え・編集不可
←ランサムウエアに対して有効
バックアップ・***復元も非常に高速***

コスト・利便性

3．ランサムウェア対応検討上のポイント

～3-1：＜落とし穴＞回避に向けた検討ポイント概要(2/2)

＜落とし穴＞を回避するための**検討ポイントを必須/推奨の2つの観点より分類**し、厚生労働省「医療情報システム等の障害発生時の対応フローチャート」の**時間区分**に応じて以下の通り整理している。
各検討ポイントの詳細は次頁以降を参照。



医療機関向けランサムウェア対応検討ガイダンス
デジタルフォレンジック研究会・医療ISAC
https://digitalforensic.jp/2021/11/25/medhi-18-gl/

Agenda

0．医療ISACの活動紹介

1．医療機関におけるランサムウェア感染の事例から導出される教訓
：特にFortiOSおよびデータバックアップについて

2．システムおよび医療機器ベンダーとの付き合い方
：「セキュリティはベンダーに丸投げ」で本当によいのか？

3．経済産業省・総務省ガイドラインの活用方法（事例紹介）

4．脅威インテリジェンス診断の有用性

5．医療ISACとして医療機関に対して支援できること

6．質疑応答

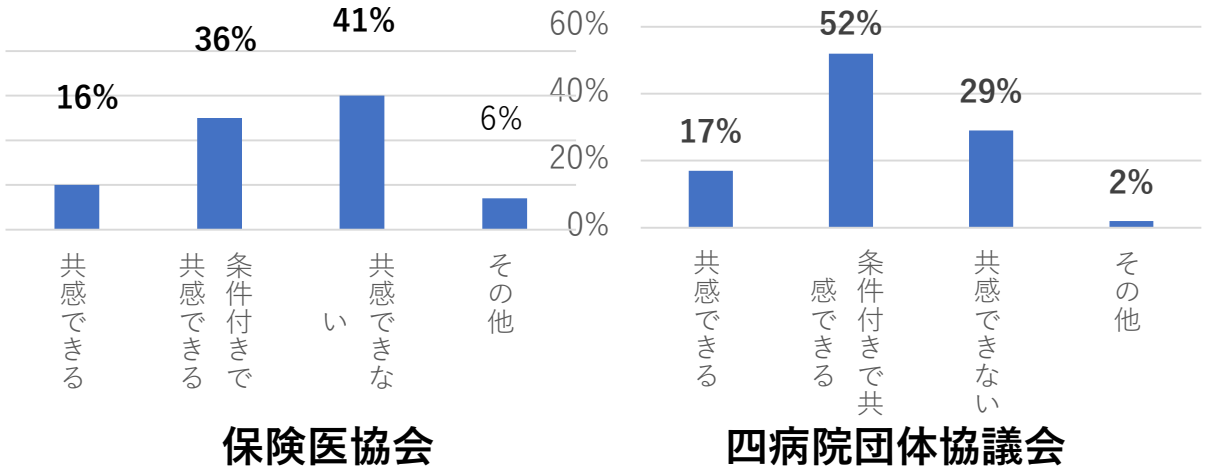
「セキュリティはベンダーに丸投げ」で本当に大丈夫ですか？

「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・・・・・」

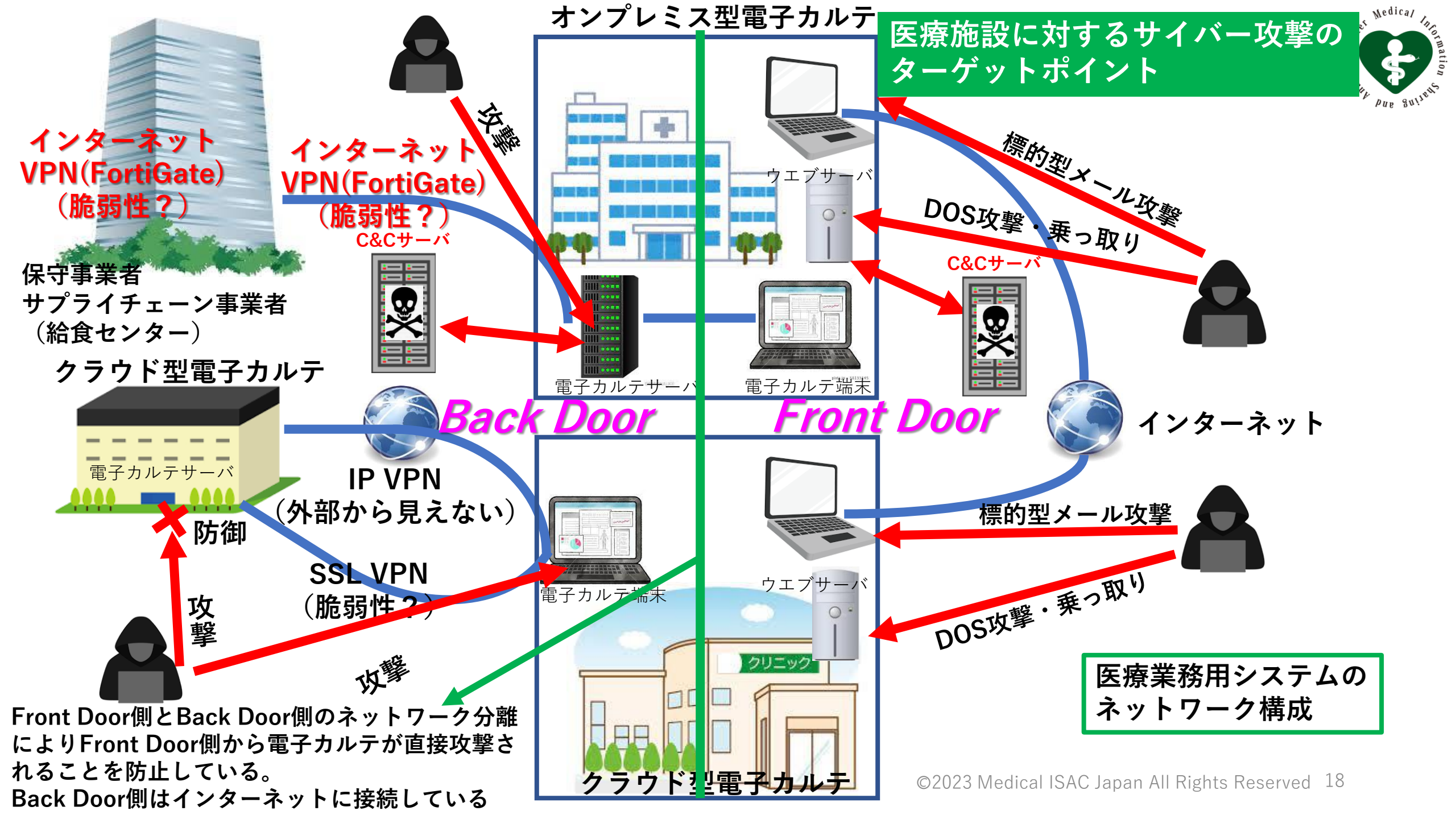
2022/1-2月医療ISACアンケート調査より

・「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＞



医療施設に対するサイバー攻撃のターゲットポイント



Front Door側とBack Door側のネットワーク分離によりFront Door側から電子カルテが直接攻撃されることを防止している。
Back Door側はインターネットに接続している

医療業務用システムのネットワーク構成

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

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

関連事業者の課題（半田病院の第三者委員会報告書 2022/6より）

１．電子カルテシステムの動作環境について
＊C 社は、クライアントのアンチウイルスソフトの稼働に関する不具合の報告はないとし、A 社はアンチウイルスソフトの担当外であるとしているが、古いActiveX pluginによるアニメーションの動作確保を優先し、アンチウイルスソフトを無効化していた。
＊C 社は Windows アップデートは最新バージョンの動作検証をし、必要に応じてユーザーに案内も 実施しているとされるが、**C 社は A 社に対し、Windows アップデートの無効を指示**している。 加えて C 社は**パーソナルファイアウォール**の稼働により、電子カルテに不具合が発生したケースは報告さ れていないとするも、**A 社に対し稼働させないと指示**を出している。
・上記は稼働後の運用保守支援サポート契約がないなかでのシステムの安定稼働を優先したものだが、ActiveX の利用や HTTPS への仕様変更予定がないことなど、セキュリティ意識が欠落していると言 わざるを得ない。また、A 社は動作環境に関して「責任」はないと認識しているため、セキュリティに関する進言の意識もなかったと思われる。

２．電子カルテシステムのリモートメンテナンスについて
C 社は、電子カルテシステムの**リモートメンテナンス業務の主体**であるにもかかわらず、**インフラ担当が A 社であることを理由にリモートメンテナンスに利用する VPN 装置の設定仕様書及び通信キャリア、サービ スプロバイダー名、経路上の暗号化等の仕様について把握していない**。
2010 年にC 社が設置した旧 VPN 装置の故障にともない、2019 年にA 社が VPN 装置のリプレ ースを実施したが、**10 年近く月日が経ちセキュリティ脅威が変化しているにも関わらず、VPN 装置の設定 は旧 VPN の内容を踏襲**している。踏襲して構わないと指示があったとしても、**セキュリティ意識が欠落して いるか、適切な設定を施す技術力が全く無かったと言わざるを得ない**。

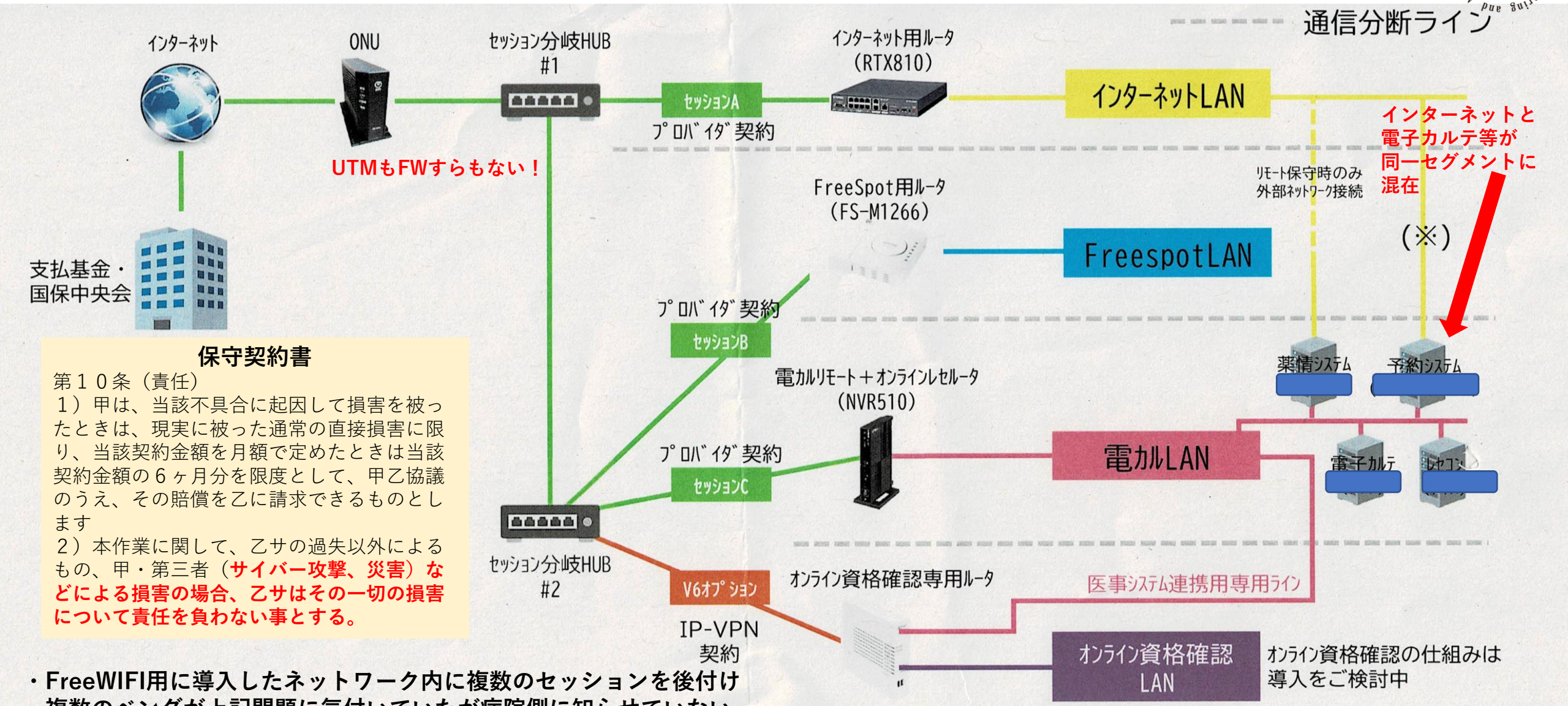
３．VPN 装置の脆弱性
C 社と A 社双方ともに、脆弱性情報(CVE-2018-13379)の存在は認識があったとしている。C 社は電子カ ルテシステムのアプリケーションが担当であり範疇外の意識、A 社は VPN 装置の担当であるが、ISO27001 に準ずる社内運用ルールに基づき管理運営していたとあり、**脆弱性情報に関するセキュリティ知識が全く無 かったと言わざるを得ない**。

- **アンチウイルス無効化**
- **Windowsアップデート無効化**
- **パーソナルファイアウォールの無効化**
- **不適切なVPN装置設定**
- **VPN装置の脆弱性未対策**

A社：現地SIer
C社：電子カルテ販社

・こんなベンダーに丸投げして大丈夫なわけがない！
・複数ベンダが関与する場合の責任分界の不明確さ

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

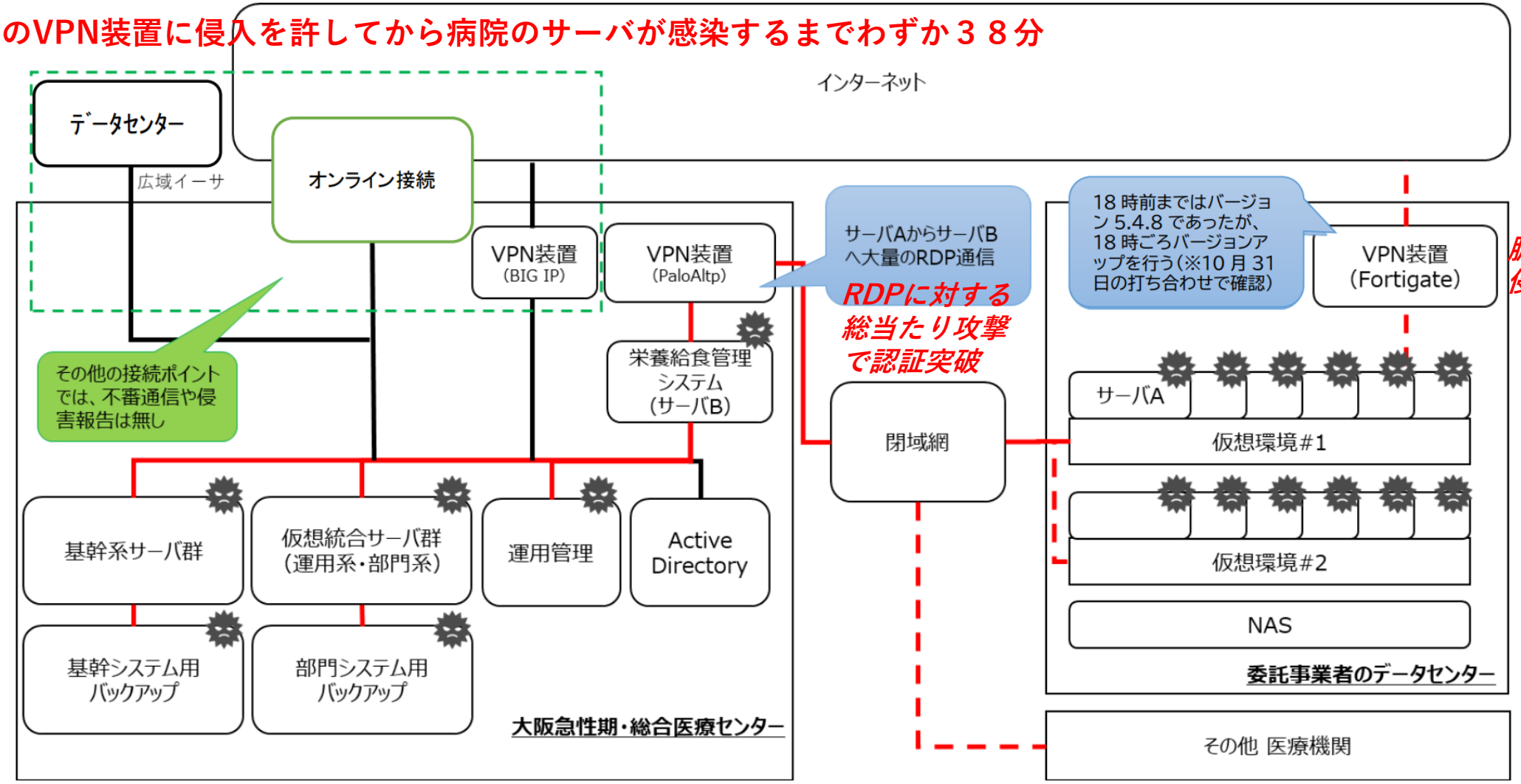
２）本作業に関して、乙サの過失以外によるもの、甲・第三者（**サイバー攻撃、災害）などによる損害の場合、乙サはその一切の損害について責任を負わない事とする。**

- **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。

大阪急性期医療センターのランサムウエア被害の実態

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＞　2022 年 11 月 7 日報道公表資料より

Agenda

0．医療ISACの活動紹介

1．医療機関におけるランサムウェア感染の事例から導出される教訓
：特にFortiOSおよびデータバックアップについて

2．システムおよび医療機器ベンダーとの付き合い方
：「セキュリティはベンダーに丸投げ」で本当によいのか？

3．経済産業省・総務省ガイドラインの活用方法（事例紹介）

4．脅威インテリジェンス診断の有用性

5．医療ISACとして医療機関に対して支援できること

6．質疑応答

医療機関が遵守すべきGL

３省２ガイドラインの相互関連性

事業者が遵守すべきGL

「医療情報システムの安全管理に関するガイドライン 5.2版」
(厚生労働省 2022/3)

4.2.1. 委託における責任分界

万一、何らかの不都合な事態が生じた場合にも同様に、受託する事業者と連携しながら 「説明責任」及び「善後策を講ずる責任」を果たす必要があるため、受託する事業者との契約において、受託する事業者の義務を明記すべきである。 また受託する事業者の責任によって不都合な事態が生じた場合に、
受託する事業者との 間で「善後策を講ずる責任」をどのように分担するかについても、受託する事業者との契約 で明記すべきである。 そのため**「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」**に示す「サービス仕様適合開示書」、「サービスレベルアグリーメント」に

医療機関が守るべきガイドライン

相互連携

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 」

「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2020/8)

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20を取得すること。

事業者が守るべきガイドライン

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

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

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

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

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）

改正民法における契約不適合責任：ユーザが当然期待すると思われる性能を満たしていない場合、契約不適合に該当し、ユーザはその不具合が発覚した時点から１年以内にベンダに通知した場合、１０年間は損害賠償を請求できる

繰り返し注意喚起をされている脆弱性を放置した場合
悪意もしくは重過失が存在すると認定されれば、契約無効を主張できる可能性はある

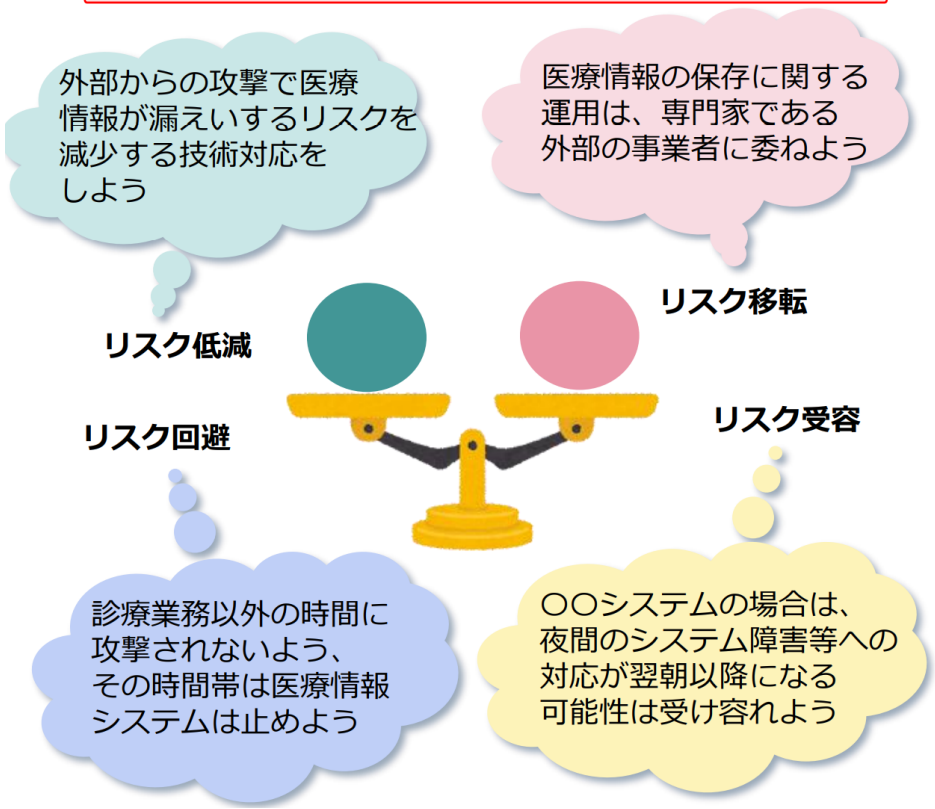
民法における私人間の契約の自由の原則（公序良俗に反するしない限り契約内容が優先）

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 概要

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



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。

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

事業者の対応状況の見定め方法

事業者の安全管理体制の第三者的評価指標
・ISMS(ISO/IEC 27001, JIS Q27001)ないしPマーク(JIS Q15001)取得状況を確認

経産省総務省ガイドラインへの対応状況確認
・HP上やパンフレットの記載事項
「弊社システムは３省３ガイドラインに準拠し・・・・」
「システムの安全管理やプライバシー保護については、関係法令やガイドラインに基づき適切に対処します」
・リスクコミュニケーションを要請した際の対応
「リスクアセスメントの内容については社外秘となっておりますので、開示できません」
「院内の環境及びセキュリティポリシーに対応し、セキュリティを担保するようネットワークを構築いただく必要がございます。必要に応じて、ネットワークベンダー様と協議のうえご対応いただけますようお願いいたします。」
・契約書上の文言の確認
「サイバー攻撃やハッキング、コンピュータウイルス等による被害については、弊社補償の範囲外」
「不具合が発生してから３ヶ月以内にユーザから通知がなかった場合は、補償の対象外」
「システムの不具合が発生した際の補償額は保守契約の月額費用の３か月分を上限とする」

医療分野のサイバーセキュリティの目指すべき方向性

ユーザ医療機関

・セキュリティについては“ベンダーに丸投げ”
（例：「当院は〇〇社にまかせているから大丈夫」）
・電子カルテはインターネットに接続していないから安全**「クローズドネットワークの安全神話」**：**崩壊**

・ベンダーに経産省・総務省GLに基づく対応状況の情報提供を行うことを求める
・ベンダーの支援のもとでユーザとしてなすべきセキュリティ対策を考える

ベンダー

・医療機関のIT・セキュリティ無理解への考慮不足
・契約に定めのないことは求められていない（やるべきでない）という、従来ベンダーとしての当たり前の姿勢

・ユーザ医療機関のIT・セキュリティ無理解を考慮し、互いが成すべきセキュリティ上の責任範囲を明確に定義する能動的なリスクコミュニケーション
・医療機関の安全管理措置の履行における補助的役割（経産総務GLがベンダーに求める役割）を遂行する

・自院内のシステム・ネットワークを中心としたセキュリティ対策

・ベンダーが持ち込んだ機器（VPN装置等）や在宅医療・オンライン診療等で用いるリモートアクセス環境を含めた、セキュリティ対策
・自施設の状況の具体的な把握とその状況に応じた最適化・合理化された対策

＊侵入・攻撃されることを前提とした

脅威インテリジェンス診断

ユーザ・ベンダー共同のセキュリティ対策

レジリエント（復旧力のある）なサイバーセキュリティ対策
Resilient Cyber Security

Agenda

0．医療ISACの活動紹介

1．医療機関におけるランサムウェア感染の事例から導出される教訓
：特にFortiOSおよびデータバックアップについて

2．システムおよび医療機器ベンダーとの付き合い方
：「セキュリティはベンダーに丸投げ」で本当によいのか？

3．経済産業省・総務省ガイドラインの活用方法（事例紹介）

4．脅威インテリジェンス診断の有用性

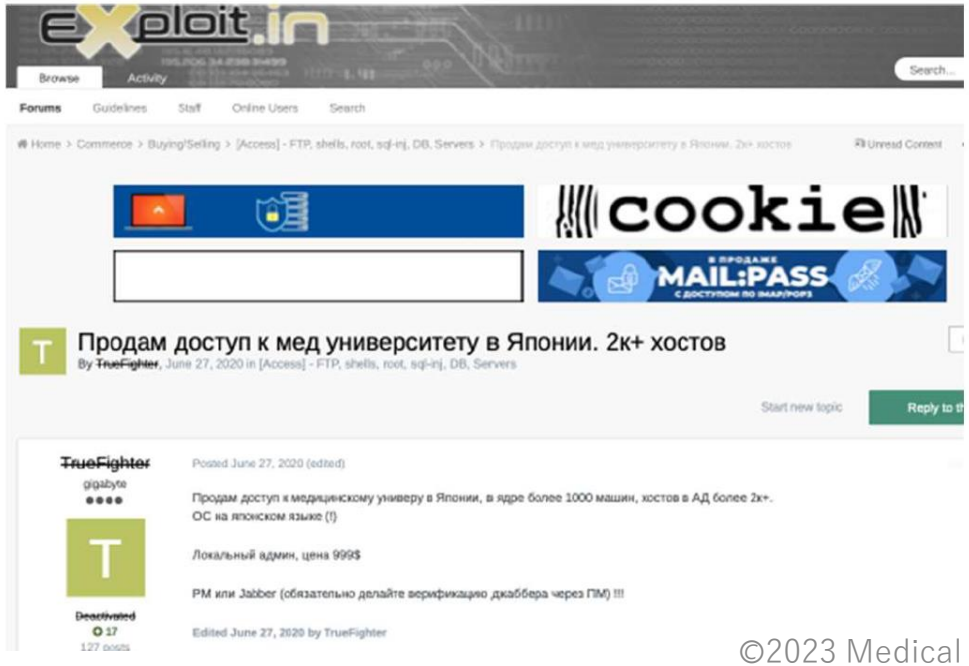
5．医療ISACとして医療機関に対して支援できること

6．質疑応答

Initial Network Access Sales on Black Market

組織への侵入を狙うアクターたちの活動

- 企業のネットワークへの侵入を可能とするアクセス情報の販売
  - ✓ 主にVPN機器のログイン情報、RDPのアクセス情報などが闇マーケットで販売されており、購入した攻撃者はランサムウェア攻撃や大規模なデータ窃取のために用いる。

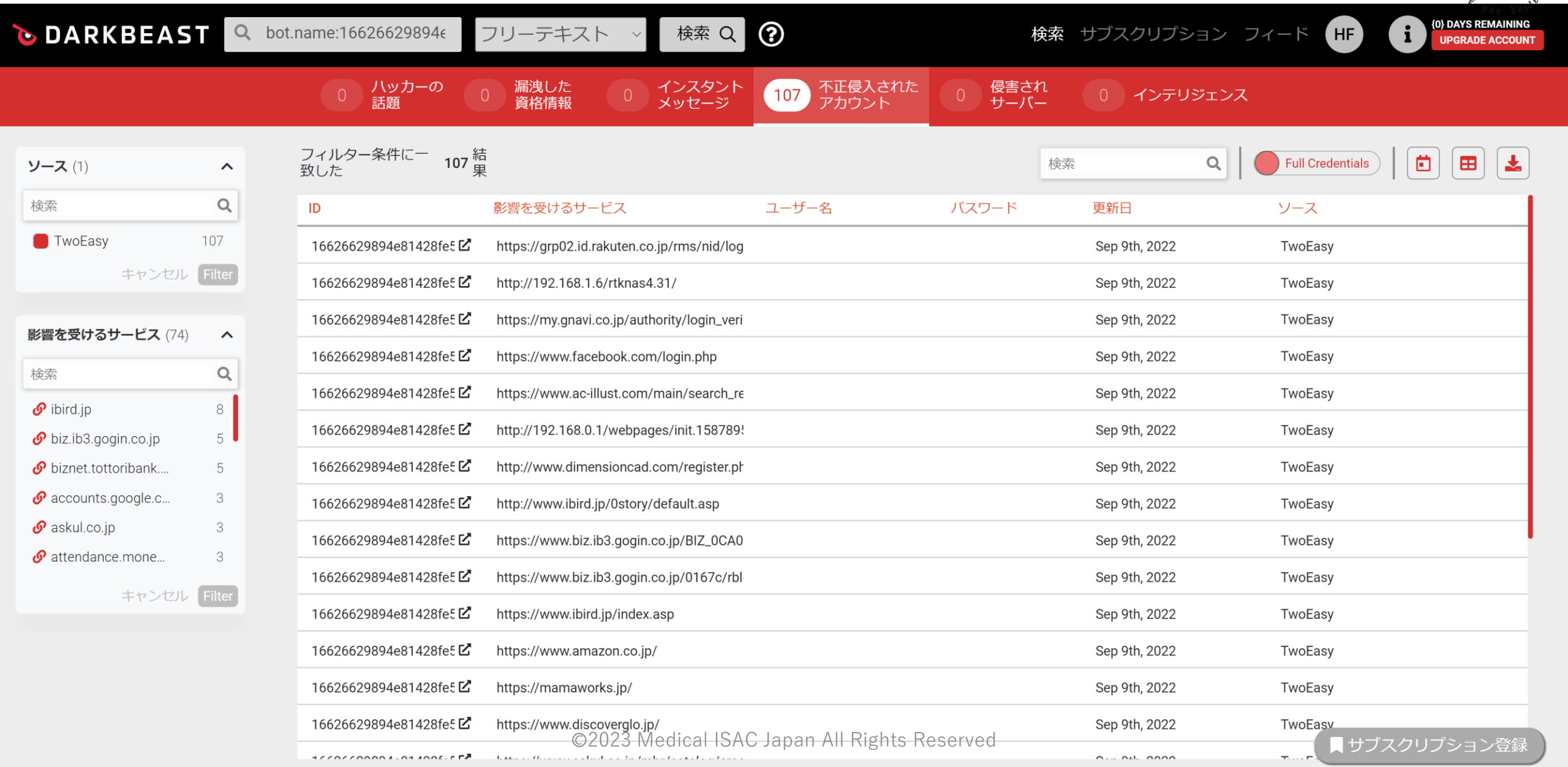


左図は日本国内組織へのアクセス件を$999で販売すると主張するアクターによる闇フォーラム（Exploitin）への投稿

販売される金額は、アクターの信用度合いのほか、被害組織の規模、業種（どれだけ身代金を取れるそうか、高価なデータが期待できるか）といった要素で異なる

その他にもRedlineやVidarのような情報窃取型マルウェアに感染したPCからのログイン情報販売マーケットで、大学ポータルやVPNログイン情報が売られていることもある。

不正侵入されたアカウント＝BOTNETのアカウント情報



サブスクリプション登録

不正侵入されたアカウント＝BOTNETのアカウント情報

DARKBEAST | mhlw.go.jp | ドメイン | 検索 | 検索 サブスクリプション フィード HF | {0} DAYS REMAINING UPGRADE ACCOUNT

109 ハッカーの話題 | 298 漏洩した資格情報 | 1 インスタントメッセージ | 103 不正侵入されたアカウント | 0 侵害されサーバー | 0 インテリジェンス

ソース (3)

検索

- RussianMarket 63
- TwoEasy 32
- Genesis 8

キャンセル Filter

影響を受けるサービス (

検索

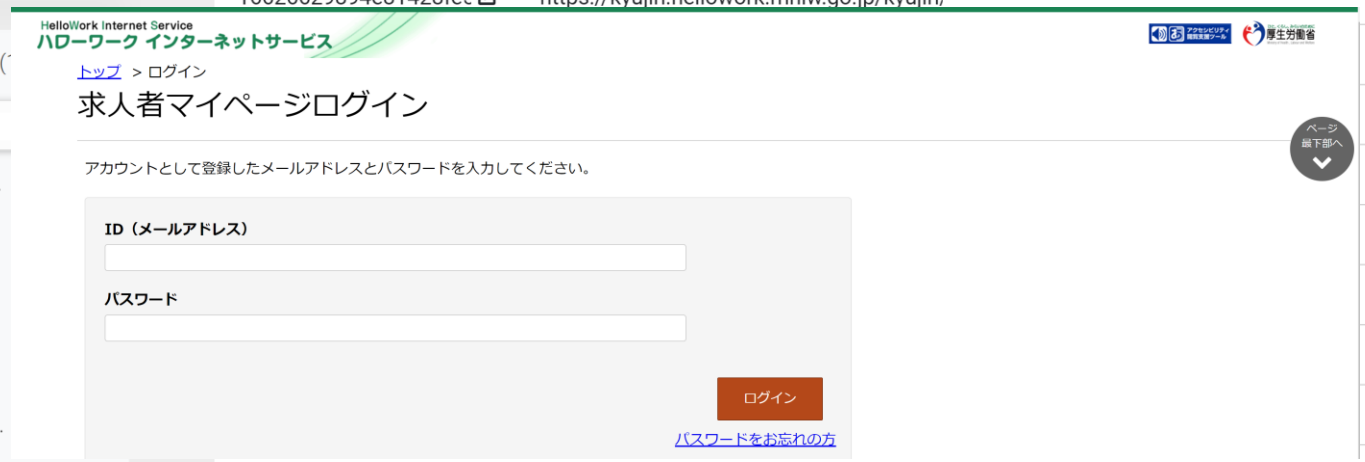
- kyushoku.hellowo...
- kyujin.hellowork....
- knwguest.kyuugy...
- careerconsultant....
- teikyo.hellowork....
- kaigokensaku.mhl...

キャンセル Filter

フィルター条件に一致した 103 結果

検索 | Full Credentials

ID	影響を受けるサービス	ユーザー名	パスワード	更新日	ソース
5042890	kyushoku.hellowork.mhlw.go.jp			Sep 20th, 2022	RussianMarket
5006313	r4syudanshidou-e-learning.mhlw.go.jp			Sep 17th, 2022	RussianMarket
16626629894e81428fe5	https://kyujin.hellowork.mhlw.go.jp/kyujin/			Sep 9th, 2022	TwoEasy
16626629894e81428fe5	https://kyujin.hellowork.mhlw.go.jp/kyujin/			Sep 9th, 2022	TwoEasy
				Sep 8th, 2022	RussianMarket
				Sep 8th, 2022	RussianMarket
				Aug 29th, 2022	TwoEasy
				Aug 26th, 2022	RussianMarket
				Aug 20th, 2022	RussianMarket
				Aug 14th, 2022	RussianMarket
				Aug 10th, 2022	TwoEasy
4449001	kyushoku.hellowork.mhlw.go.jp			Aug 7th, 2022	RussianMarket
4449001	kyujin.hellowork.mhlw.go.jp			Aug 7th, 2022	RussianMarket
1659093096c872111d6	https://knwguest.kyuugyoushienkin.mhlw.			Jul 29th, 2022	TwoEasy



サブスクリプション登録

脅威インテリジェンス診断で何がわかるか？

＊外部攻撃対象領域 (External Attack Surface)分析

・インターネット側から見えるIT資産一覧
・それらに存在する脆弱性とその重要性分類
・開放されているポート
・使用されているOSやアプリケーション、Version
・デジタル証明書の有効期限切れ
・etc

Passive survey

Shodan等のOSINT情報活用
ドメインオーナーの許可不要

最新の脅威には必ずしも対応できない

Active survey

専用のツールによるScanning
当該ドメインオーナーの許可が望ましい
最新の情報にも対応可能

＊ダークウエブ(Dark Web)監視

・ブラックマーケットで販売されているe-mail アカウント情報
・ドメイン関連に関与するBOT NET情報
・VPN装置等へのログインアカウント情報
・ハッカーのフォーラム上のチャット情報
・インスタントメッセージ(Telegram等）上の情報
・etc

＊得られる情報の重要性や有効性について個別評価が必要

脅威インテリジェンス診断による外部攻撃対象領域：EAS(External Attack Surface)評価

外部から見たシステムの状況

対象ドメイン	aichi-med-u.ac.jp

EXTERNAL ATTACK SURFACE

<攻撃対象となり得る外部公開システムの状態>

	aichi-med-u.ac.jp hamawaki.or.jp
確認できた外部公開資産数	43
① 上記のうち、脆弱性が存在する可能性のある資産	2
② 上記のうち、不要なポートが空いている可能性のある資産	3

番号	サブドメイン	IPアドレス	公開されている利用ソフトウェア	ポート
①	hp-web2.aichi-med-u.ac.jp	192.218.116.35	IIS8.5	80,443
①	www.aichi-med-u.ac.jp	192.218.116.35	IIS8.5	80,443
②	amugw22.aichi-med-u.ac.jp	192.218.116.33		25,53
②	amugw32.aichi-med-u.ac.jp	192.218.116.33		25,53
②	amugw35.aichi-med-u.ac.jp	192.218.116.85		53

※ベンダー持込の機器に関して、グローバルIPアドレスが把握できれば、そちらも対象に調査は可能です。

CERTIFICATE WEAKNESS

<証明書の脆弱性>

	aichi-med-u.ac.jp hamawaki.or.jp
脆弱な証明書を利用している可能性のある資産	0

EMAIL/CREDENTIAL LEAKS

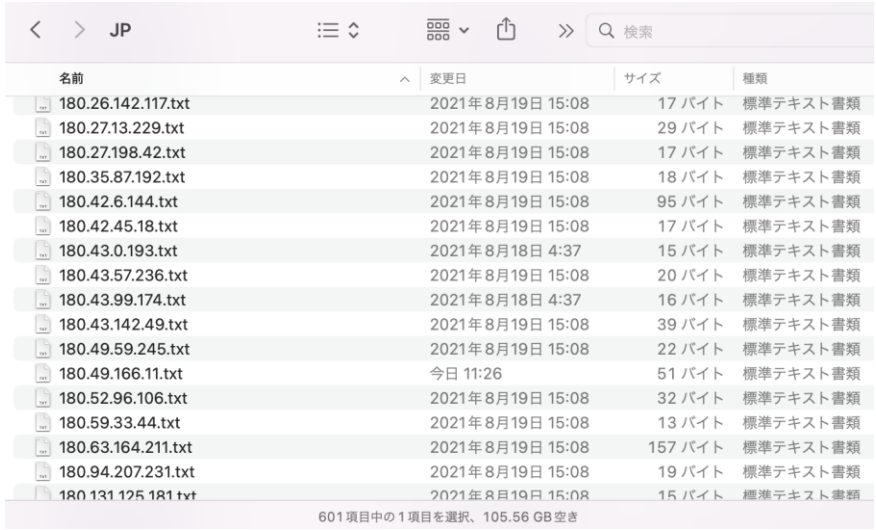
<漏洩しているメールアドレスとパスワード> aichi-med-u.ac.jp

	hamawaki.or.jp
確認できた漏洩しているメールアドレスとパスワード数	673

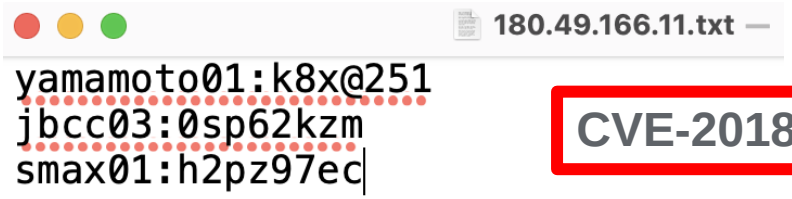
※重複有

2021/11調査結果（既に対策済み）

脅威インテリジェンス・ダークウエブ監視による*差し迫った脅威情報*



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）



CVE-2018-13379

同リスト内における徳島半田病院のVPN装置に該当すると
思われるID/PW情報のブラックマーケットでの公開（販売）

鳴門山上病院の被害事例から同じ電子カルテユーザで
米FortiNet社製のVPN機器を利用していると思われるの脆弱性情報の
リストに含まれる他の医療機関情報

医療法人[redacted]病院
153.142.107.251
[redacted]01:0663886666
[redacted]05:0663886666
[redacted]03:0663886666
wiseman01:wisemanP@ss01

医療法人[redacted]病院
118.243.20.167
wiseman01:wisemanP@ss01
[redacted]ofujiP@ss
cim01:cimP@ss01

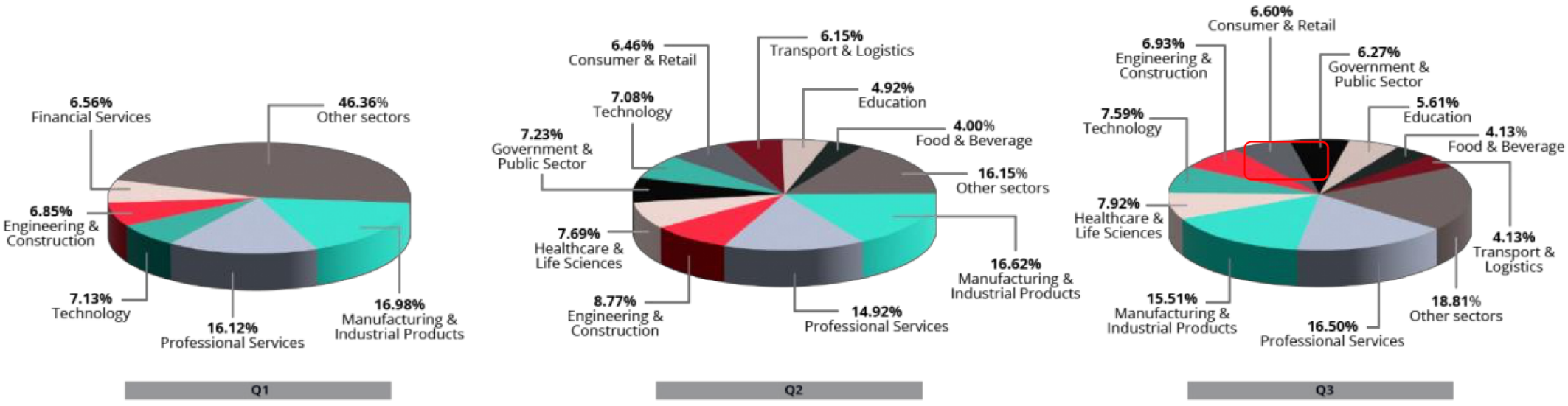
特定医療法人[redacted]病院
118.243.16.2
[redacted]02
wiseman:wisemanP@ss01
[redacted]03

医療ISACから
各病院および
電子カルテベンダー
のワイズマン社
に注意喚起を行い
対策を講じた

ハッカーはどのようにして攻撃対象を選んでいるのか？

業種にかかわらず、ランサムウェア攻撃は起きる

- 確認されているアクターはまちまちで、攻撃者は日和見的。偵察活動は無差別に行い、攻撃サーフェイスが見つかった後に標的として吟味し、攻撃を行うのが一般的。



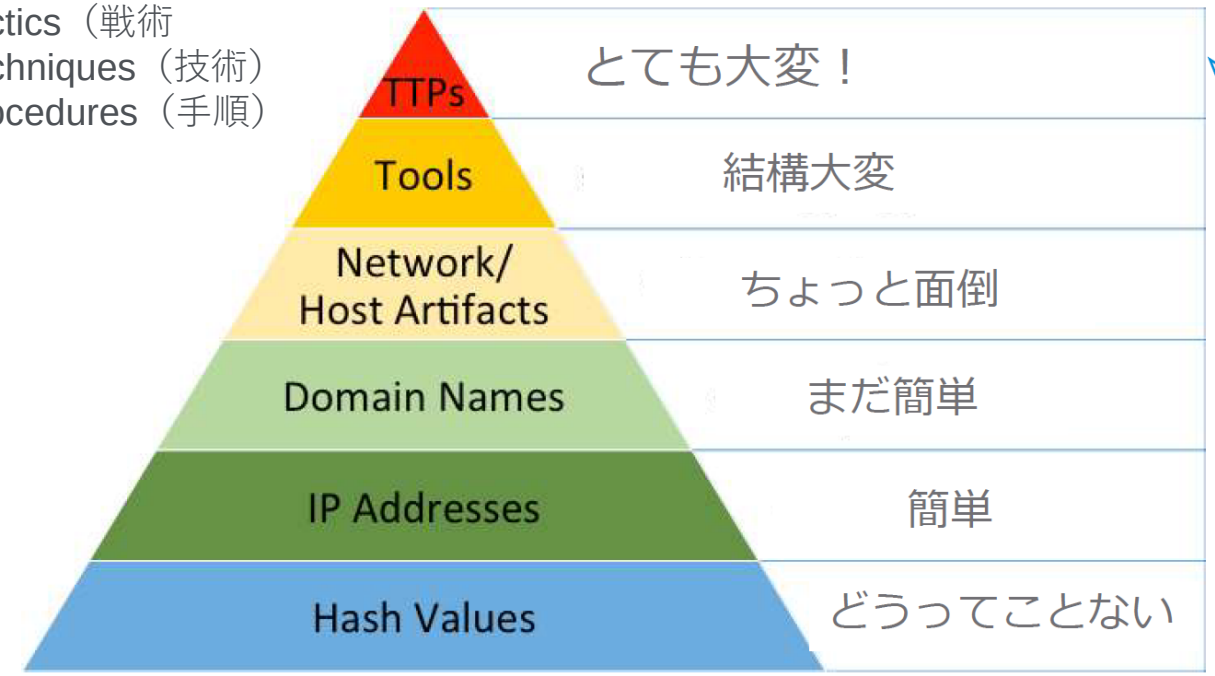
出典／KELAレポート： 2022 年第 3 四半期のランサムウエア被害組織とネットワークアクセスの販売状況

ハッカーの視点から見る：Pain of Pyramid

効果的な脅威インテリジェンス活用のためには

攻撃者の視点で攻撃の継続の容易さを考えてみる

Tactics（戦術
Techniques（技術）
Procedures（手順）



✓ 高度な対策であるほど、攻撃者にとってや攻撃の継続が困難に

- 攻撃者が用いる手法（戦術、技術、手続）を無力化されるような対策を考える
- アタックサーフェースを減らす
  - 脆弱性を狙う攻撃であれば穴を塞ぐ
  - 漏洩した認証情報が悪用されないよう、ダークウェブでの流出を監視
  - 自組織ポータルサイトへのアクセス情報がボットネットマーケットで販売されていないか

EAS可視化＋脆弱性診断

[redacted]医科大学様　ULTRA RED*- 調査結果報告書 2022/8/15

ULTRA RED は脅威アクターの TTP を追跡し、潜在的な攻撃者側の視点から企業の全体像を把握することで、実際の攻撃方法を自動的にエミュレートし、企業が防御策を講じてネットワークセキュリティを確保できるようにしている。

1. **OpenAM における RCE（CVE-2021-35464）** - 5/5 CRITICAL（重大）

   http://amo1.noc[redacted]ac.jp

   説明：

   古い ForgeRock OpenAM サーバーにリモートコマンド実行攻撃に対する脆弱性がある。サーバー内の危険な Java デシリアライゼーションによってこの脆弱性が発生している。攻撃者はエンコーディングされた OS コマンドを含む GET リクエストを作成し、リクエストがサーバーに送信されると同時にこのコマンドを実行することができる。

   PoC：

   - http://amo1.noc.[redacted]ac.jp/openam/oauth2/..;/ccversion/Version?jato.pageSession=<serialized_object>

   対処法：

   ForgeRock OpenAM を最新バージョンにアップグレードする。

   参考資料：

   ForgeRock OpenAM 内の事前認証済み RCE（CVE-2021-35464）

私立大学付属病院

株式会社〇〇様　ULTRA RED-調査結果報告書2022/9/05

1. **SQL Injection** - 5/5

- www.jm-10.mediwel.net

Description:

SQLインジェクションはセキュリティ脆弱性の一種で、攻撃者によるデータベースクエリの妨害を可能にする。一般に攻撃者は通常であればアクセスできないデータの閲覧や操作が可能になる。これにはパスワード、クレジットカードの詳細、個人のユーザー情報など、機密情報も含まれる。多くの場合、攻撃者がこのデータを変更または削除することによりアプリケーションの内容や挙動が永続的に変更されてしまう。

場合によっては攻撃者がSQLインジェクション攻撃をエスカレーションし、基礎になっているサーバーやその他のバックエンドインフラストラクチャに侵入してRCE機能の実行に至る場合もある。

基本的にはメタ文字\sをデータ入力として配置し、コントロールプレーンでSQLコマンドを誤ってトリガーさせることで攻撃が行われる。この不具合はコントロールプレーンとデータプレーンを正しく分離できないSQLの操作モードに起因している。

The site has also enabled debug mode in Symfony, exposing sensitive exception information, and specifically the following credentials to the API gateway:

- username: apigwmediwel

- password: FryHFfRpiy

大手調剤薬局チェーン

社会医療法人〇〇会様　DETECT-調査結果報告書 2022/9/11

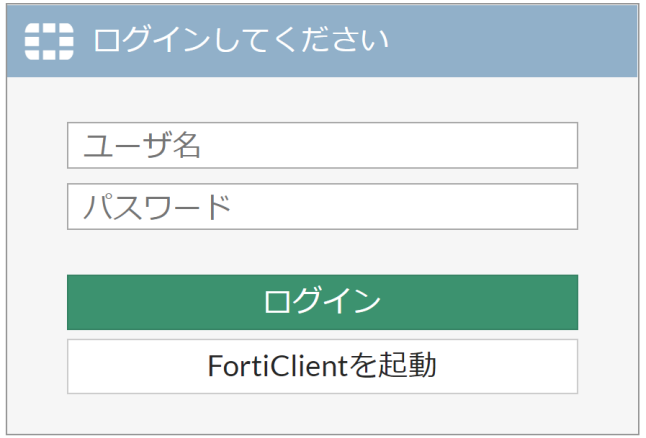
Fortinetが稼働しており、証明書エラー等の表示なくログイン画面を表示可能です。
パッチの適用状況、アクセス権をご確認ください。また、クライアント証明書などの2要素認証またはやIPアドレス制限などの実施をご検討ください。

[redacted]

https://210.131.254.42:10443/remote/login?lang=x-sjis

[redacted]

IP:210.131.254.42
Open port: 10443
S



医療法人立病院

私立大学病院よりの中間報告(2022/10/29)

＞1. OpenAM における RCE
回避策を実施中、ソフトウェアが古い状態のため、
年度内を目標にリプレース予定で検討中。

＞2. パスワードリセットにおけるホストヘッダー
インジェクション該当部署と調整中です。

＞3. オープエンドポイントによる機密情報の開示
以下はサーバーの管理者に連絡して対策済みです。

済　https://renke[redacted].ac.jp/web.config
済　https://[redacted].ac.jp/web.config
済　https://lms.shs.[redacted].ac.jp/test.php
済　https://redcap.[redacted].ac.jp/info.php
済　http://nurse[redacted].ac.jp/wp-content/degub.log

＞4. 複数のウェブサイトに古いテクノロジーが利用。
以下はサーバーの管理者に連絡して対策済みです。

済　https://assembly.[redacted].ac.jp/
済　https://syllabus.[redacted].ac.jp/
済　https://renkei[redacted].ac.jp/
済　https://nurse[redacted].ac.jp

以下は年内に非公開化、将来的にサーバー廃止の方向性。

[redacted]
未　https://sns.fujita-hu.ac.jp/

以下はサーバーの管理者に連絡し、当該プライグインの廃止で対応予定。

[redacted]
済　https://spm.med.fujita-hu.ac.jp/

FortiOSの脆弱性について：対策すべき複数の課題

＜脆弱性CVE-2018-13379＞　多数のランサムウエア被害
(2019/5公表、2020/9アカウント情報公開)
■不正アクセスによる侵入を許す脆弱性
■対象バージョン・機器、推奨対策
FortiGateSSL-VPN機器
　FortiOS 6.0.0 ～ 6.0.4 → 6.0.13にアップグレード
　FortiOS 5.6.3 ～ 5.6.7 → 5.6.14にアップグレード
　FortiOS 5.4.6 ～ 5.4.12→ 5.4.13にアップグレード

＜脆弱性CVE-2022-40684＞
(2022/10/10公表、10/14攻撃手法公開)
■ID/PW無しでログインを許す脆弱性
■対象バージョン・機器、推奨対策
FortiGateSSL-VPN機器
　FortiOS 7.2.0 ～ 7.2.1 → FortiOS 7.2.2にアップグレード
　FortiOS 7.0.0 ～ 7.0.6 → 7.0.7にアップグレード

＜脆弱性CVE-2022-29055＞(2022/10/19公表)
■SSL-VPNのサービス拒否
対象バージョン・機器、推奨対策
■ FortiGateSSL-VPN機器
　FortiOS7.2.0 → 7.2.2にアップグレード
　FortiOS7.0.0 ～ 7.0.5 → 7.0.7にアップグレード
　FortiOS6.4.0 ～ 6.4.9 → 6.4.10にアップグレード
　FortiOS6.2.0 ～ 6.2.10 → 6.2.11にアップグレード
　FortiOSバージョン6.0系 → 6.0.15にアップグレード

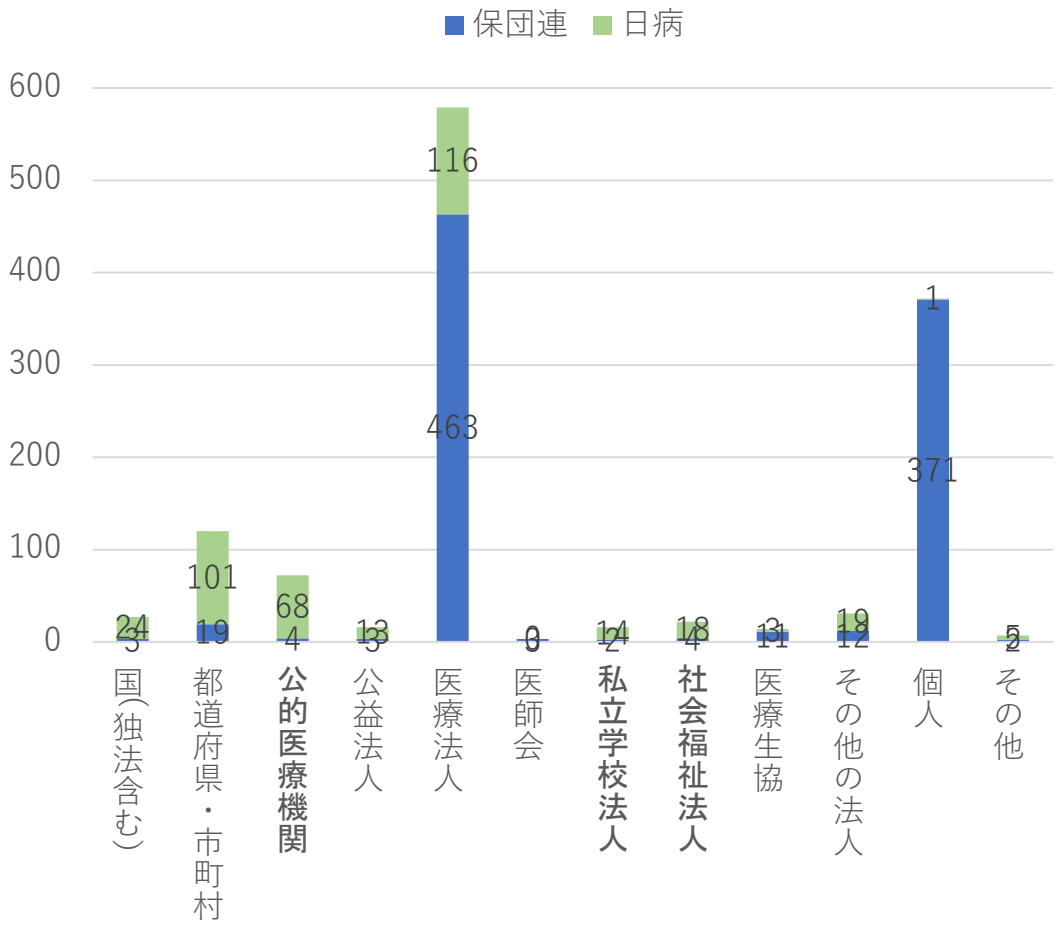
＜脆弱性 CVE-2022-42475＞(2022/12/14公表)
FortiGate SSL-VPNのヒープ・オーバーフローの脆弱性
■不正プログラムの実行を許す脆弱性
■対象バージョン・機器、推奨対策
FortiGateSSL-VPN機器
　FortiOS 7.0.0 から 7.0.8 → 7.0.9以降にアップグレード
　FortiOS 7.2.0 から 7.2.2 → 7.2.3以降にアップグレード
　FortiOS 6.4.0 から 6.4.10→ 6.4.11以降にアップグレード
　FortiOS 6.2.0 から 6.2.11→ 6.2.12以降にアップグレード
　FortiOS 6.0.0 から 6.0.14→ 6.0.15以降にアップグレード

全て重大な被害を生じる可能性があり早急な対策が必要（修正パッチ適用、アクセス元IP制限、PW変更etc.）
＊インターネットVPN装置として非常に高いシェア→狙われる機会が多い（延々と脆弱性対策を行い続ける宿命）

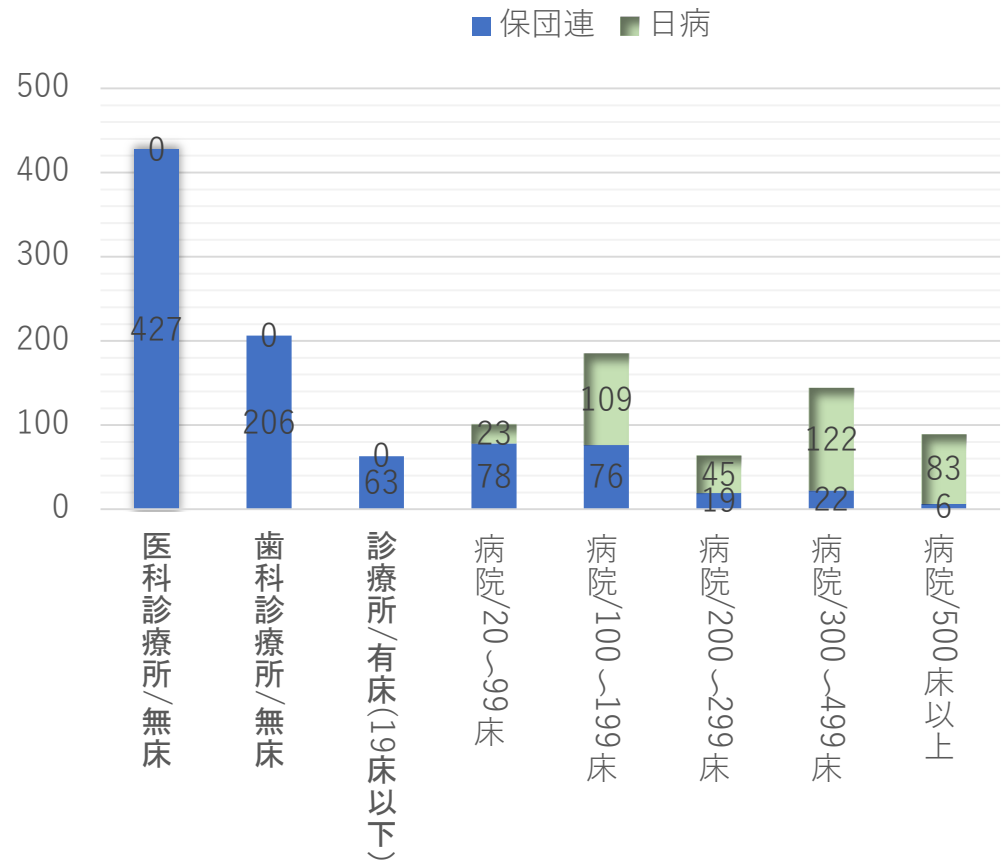
サイバーセキュリティアンケート調査

- **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）**

＜開設者別内訳＞



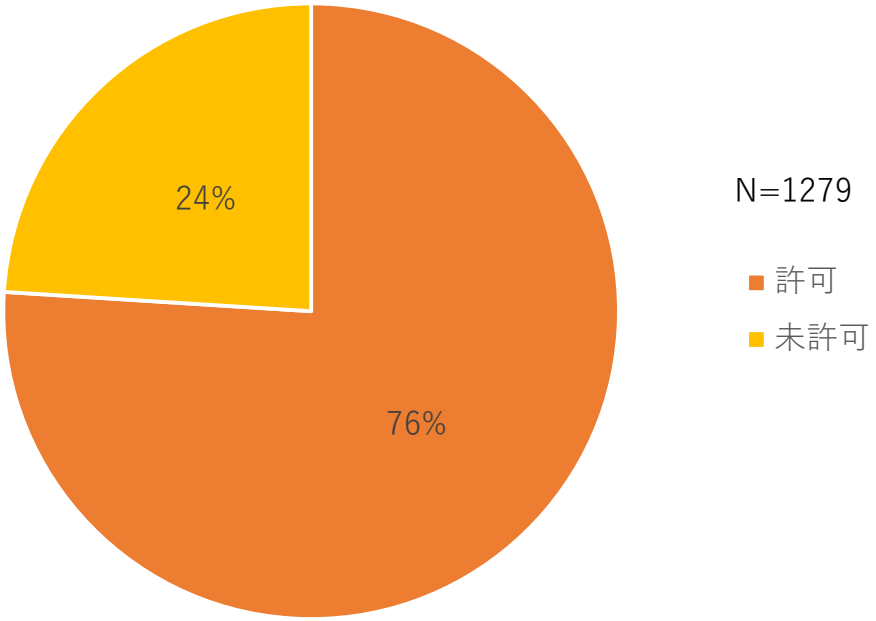
＜病床規模別内訳＞



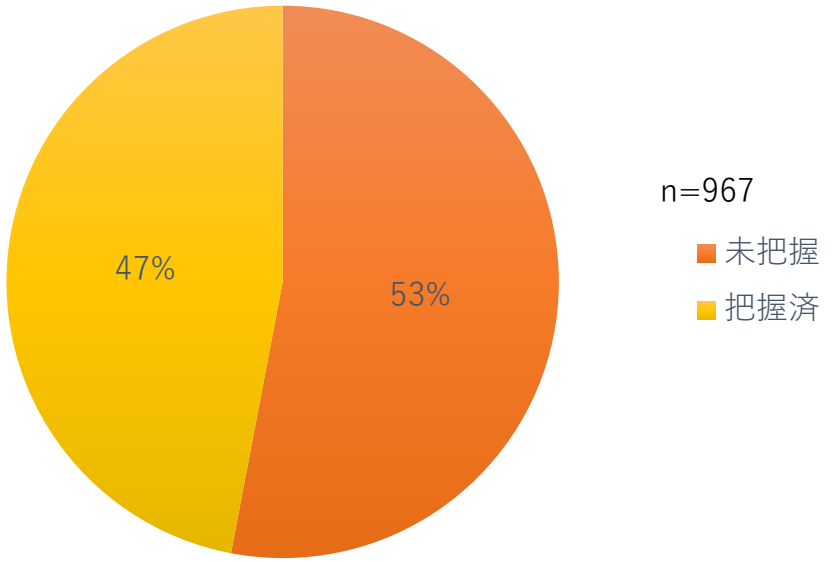
＜アンケート調査結果_全体結果(1/4)＞

【①：リモートメンテナンス用製品の利用・把握状況】

＜Q1：リモートメンテナンスを許可していると回答した組織割合＞



＜Q2. リモートメンテナンス機器情報を把握していると回答した組織割合＞

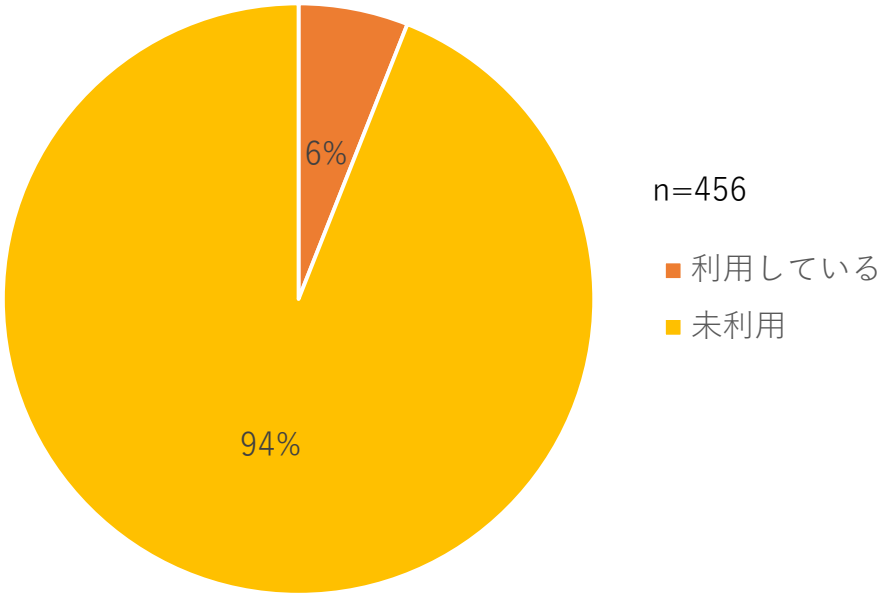


リモートメンテナンスを許可していると回答した組織は全体の７６%、そのうち**リモートメンテナンスに利用している機器・製品のバージョン情報等を把握している組織は４７%であった**。

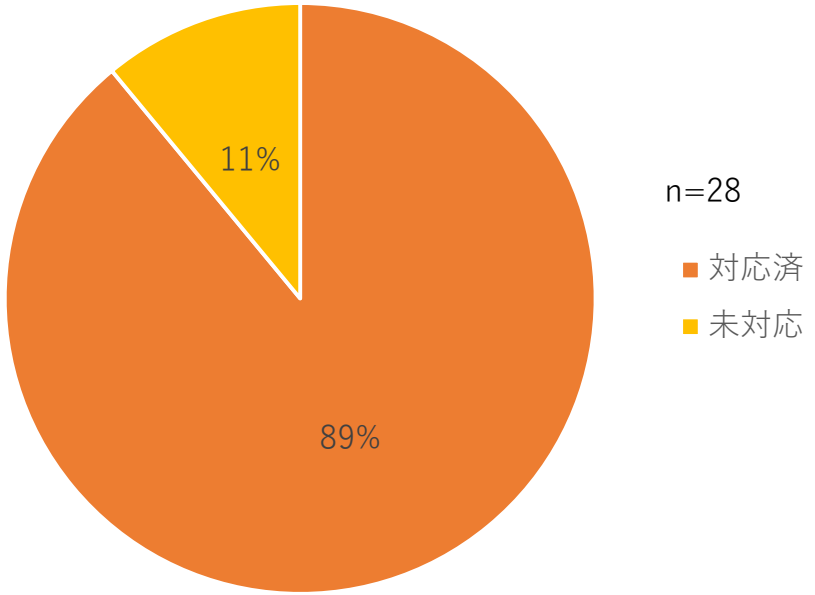
＜アンケート調査結果_全体結果(2/4)＞

【②-A：Fortinet社リモートメンテナンス用製品の利用・脆弱性対応状況】

＜Q3：22年10月に脆弱性報告されたFortinet製品を利用していると回答した組織の割合



＜Q4：脆弱性へのベンダ対応が完了していると回答した組織の割合＞

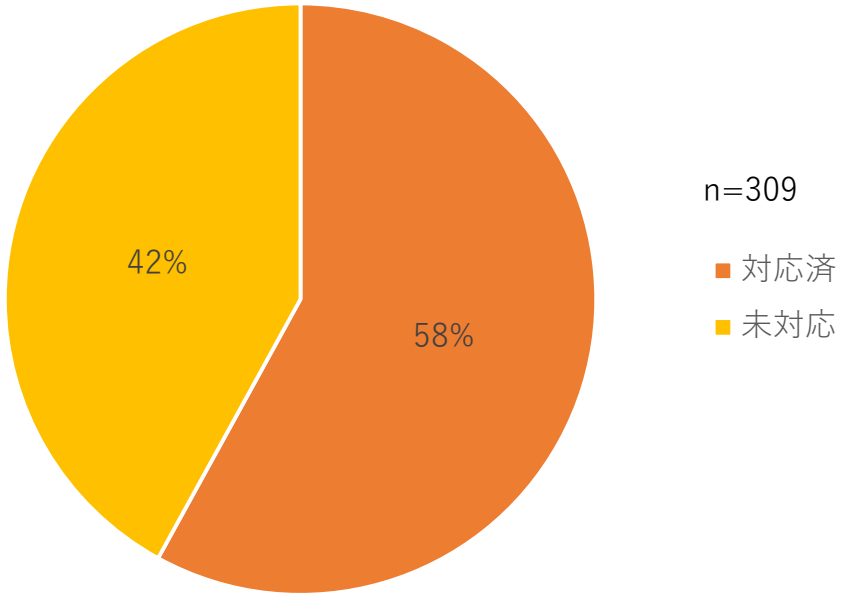


リモートメンテナンス機器・製品のバージョン情報を把握している組織の中で、２２年１０月に深刻な脆弱性が発生したForitnet社製品を利用している組織は6%、そのうち**脆弱性対応が未了の組織は1割程度**であり、ほとんどの組織で対応が完了している。

＜アンケート調査結果_全体結果(3/4)＞

【②-B：それ以外のリモートメンテナンス用製品の利用・脆弱性対応状況】

＜Q５：Q3以外のリモートメンテ機器を把握しているが、特に脆弱性対応を行っていないと回答した組織の割合＞

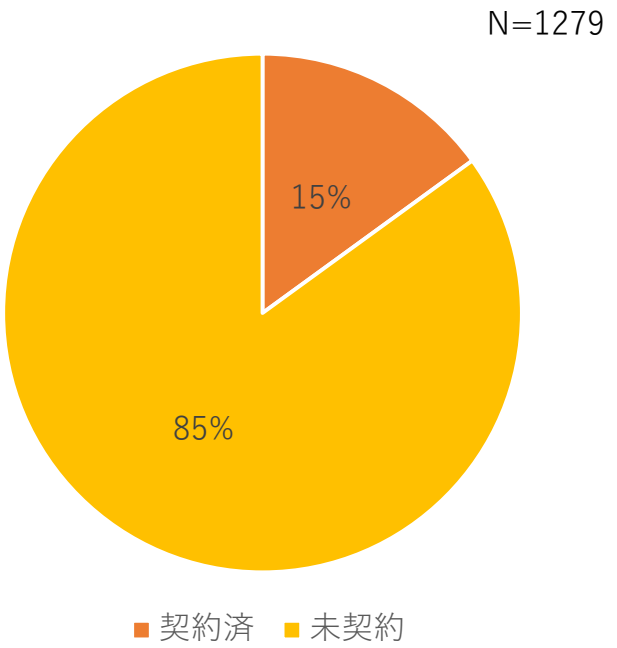


２２年１０月に深刻な脆弱性が発生したForitnet社製品以外のリモートメンテナンス機器・製品を利用している組織のうち、該当機器・製品へのセキュリティ上の脆弱性対応を行っている組織の割合は58%であり、**４割強は特段対応を実施していない**。

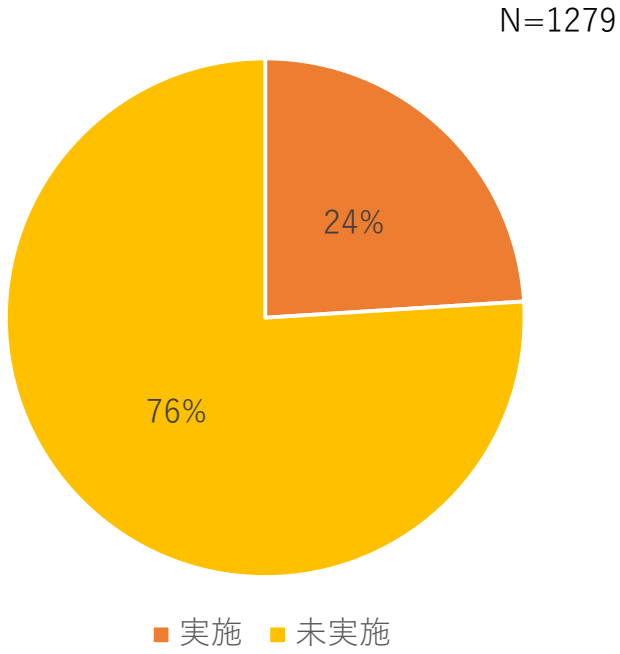
＜アンケート調査結果_全体結果(4/4)＞

【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】

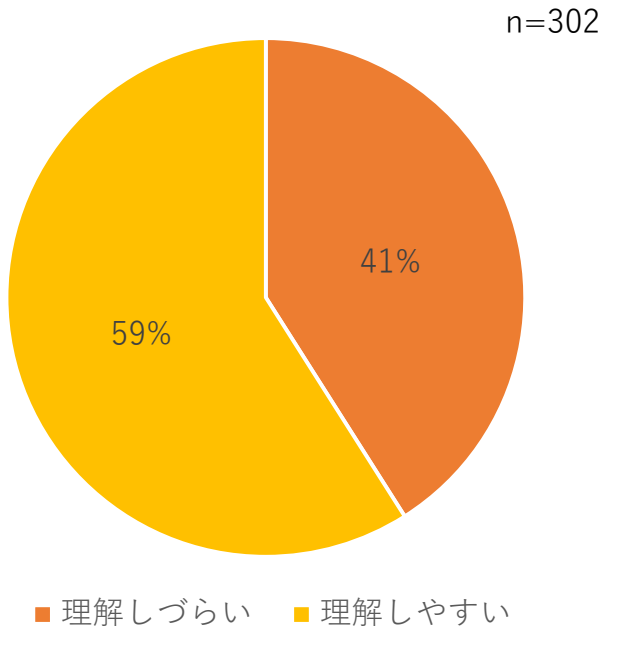
＜Q6：契約書・SLAにおけるセキュリティ責任分界を定めていないと回答した組織の割合＞



＜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＞

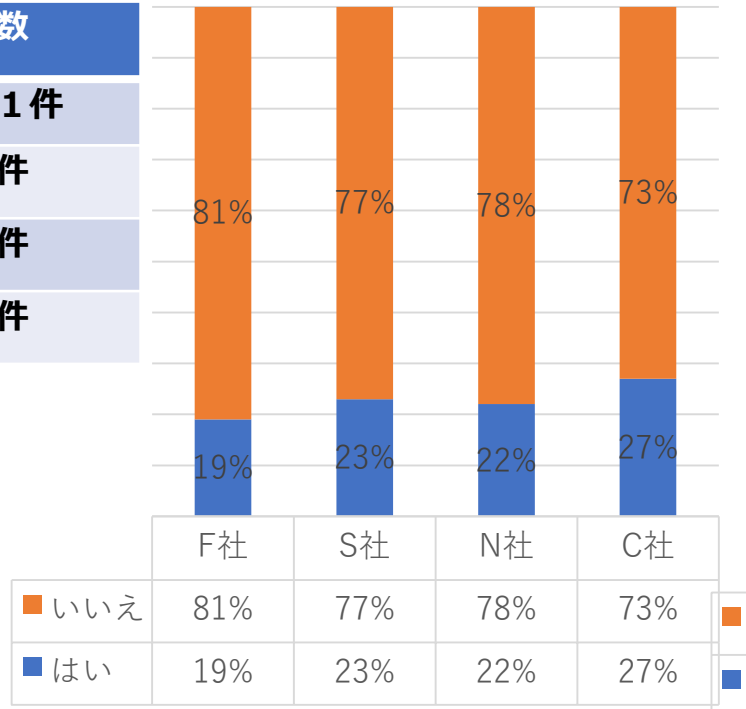


ベンダと契約等でセキュリティの役割・責任を定めている組織の割合は**15%**、さらにベンダからセキュリティ等も含めた報告を行わせている組織は**24%にしか満たない**。
報告を受けている組織においてもその内容は理解しづらく、セキュリティ向上に資さないと回答した割合は**41%**に及んだ。

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）

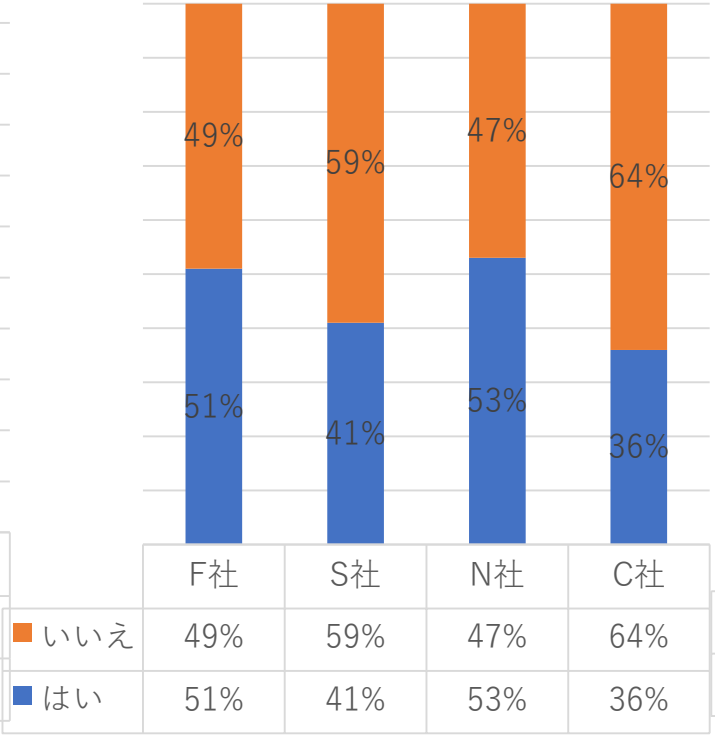
電カルベンダ	導入数
F社（富士通）	１４１件
S社（SSI）	６４件
N社（NEC）	６０件
C社（CSI）	２２件

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



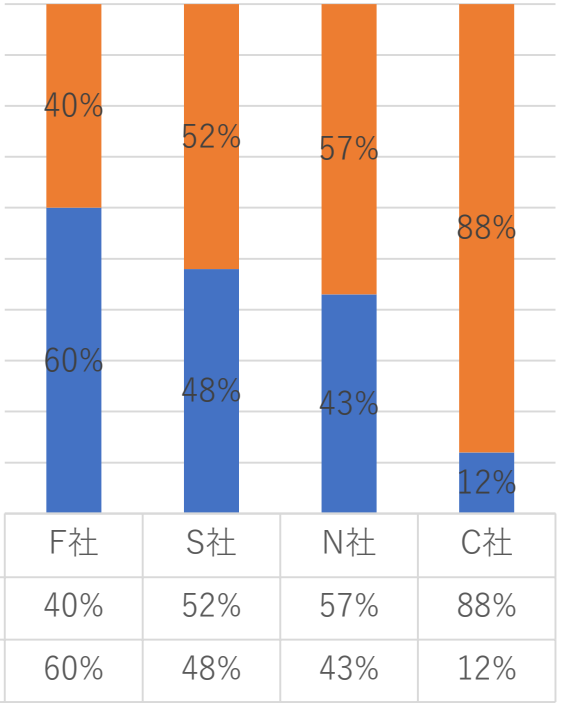
	F社	S社	N社	C社
いいえ	81%	77%	78%	73%
はい	19%	23%	22%	27%

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。

＜アンケート調査結果_全体総評＞

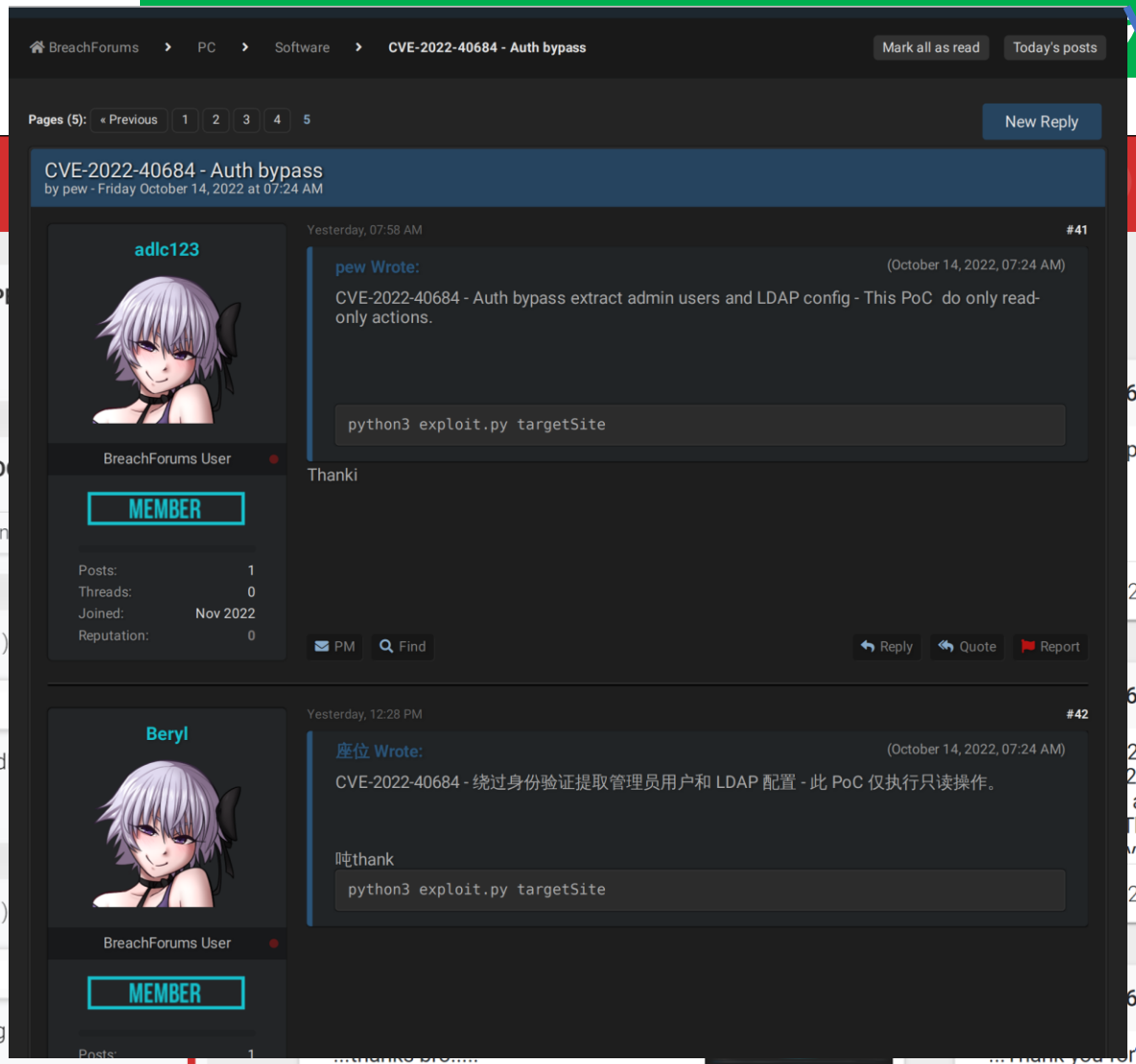
- 今回のアンケート回答組織のうち、８割は院内システムへのベンダによるリモートメンテナンスを行わせているものの、**そのうち５割弱はメンテナンス用の機器・製品の種別・バージョン情報を把握していない状況**である。

- 22年10月に深刻な脆弱性が報告されたFortinet社のリモートメンテナンス製品・機器の利用率は1割弱と少なく、かつ、該当組織において脆弱性対応が既に完了していると回答した組織は全体の9割程度に及んでおり、**Fortinet社製品の脆弱性へのリスク認識が高く、それゆえ適切な対応が図られている状況**が見受けられる。

- 一方で、**Fortinet社製品以外のリモートメンテナンス機器・製品**については、種別・バージョン情報等を把握しているものの、**4割強の組織が特段脆弱性対応を実施していない**状況である。そのため、**Fortinet社以外の機器の脆弱性を悪用したサイバー攻撃が発生するリスクはまだ根強く残存している**ことが把握できる。

- ベンダとの間で医療機関としてセキュリティ上の役割・責任分担を定め、**契約等で合意形成している組織は全体の1割強**にしか満たず、さらにセキュリティ等の情報提供も含めた**報告を定期的に行わせている組織は2割強程度**にしか満たない。
- さらにベンダの報告内容が医療機関の職員にとって理解しやすい水準で整理され、提供されていると回答した組織は6割弱だが、**4割程度はその内容は理解しづらく、満足していない状況**であった。
- 経済産業省・総務省安全管理ガイドラインではベンダは医療機関がセキュリティ上の安全管理措置を講じるうえで、適切な情報提供を行うことが求められている。**ベンダは医療機関におけるITリテラシー水準を考慮したうえで、コミュニケーションの工夫を行い、医療機関はベンダと共同でITリテラシーを高める取組等を促進することが不可欠**であるといえる。

ダークウエブで話題沸騰！　CVE-2022-40684(2022/10/10公表)に関する
...ムの現状



Compromised Accounts 0 Breached Servers 0 Finished Intelligence

SOURCE TYPE
Forum
SOURCE GEO
Internation
CRAWLER (1)
Search
Breached
AUTHOR (51)
Search
BX1xrang
Beryl 1
Corvo 1
CutDCrap 1
DarkShadow21 1
Evolved 1

Search
Posted date

CVE-2022-40684 - Auth bypass
...Thanks for share mate....
Nov 15th, 2022 Breac... rchunt... #29460...

CVE-2022-40684 - Auth bypass
...(October 14, 2022, 07:24 AM)pew Wrote: CVE-2022-40684 - Auth bypass extract admin users and LDAP config - This PoC do only read-only actions, python3 exploit.py
Nov 11th, 2022 Breac... _6n #29444...

CVE-2022-40684 - Auth bypass
...(October 14, 2022, 07:24 AM)pew Wrote: CVE-2022-40684 - Auth bypass extract admin users and LDAP config - This PoC do only read-only actions, python3 exploit.py
Nov 11th, 2022 Breac... BX1xr... #29444...

Subscribe

脅威インテリジェンス診断とダークウエブ監視
東京都立病院への攻撃予兆検知

- 2021/12/7 イスラエルの脅威インテリジェンス事業者から医療ISACの理事の一人に

「東京都立墨東病院と松沢病院を含む都立病院の公式メールのアドレスやパスワードが大量に漏洩していること

ハッカーらのダークウエブ上のチャットにて、上記２病院を標的対象としていること」

の情報がもたらされた。

・同日両病院、東京都病院経営本部、都知事に注意喚起を行い、経営本部から、標的型メール攻撃対策、システムアクセスの二要素認証化、VPNの脆弱性対策等の指示を全１４病院に対して行ったことの報告と、感謝の意を伝えられた。

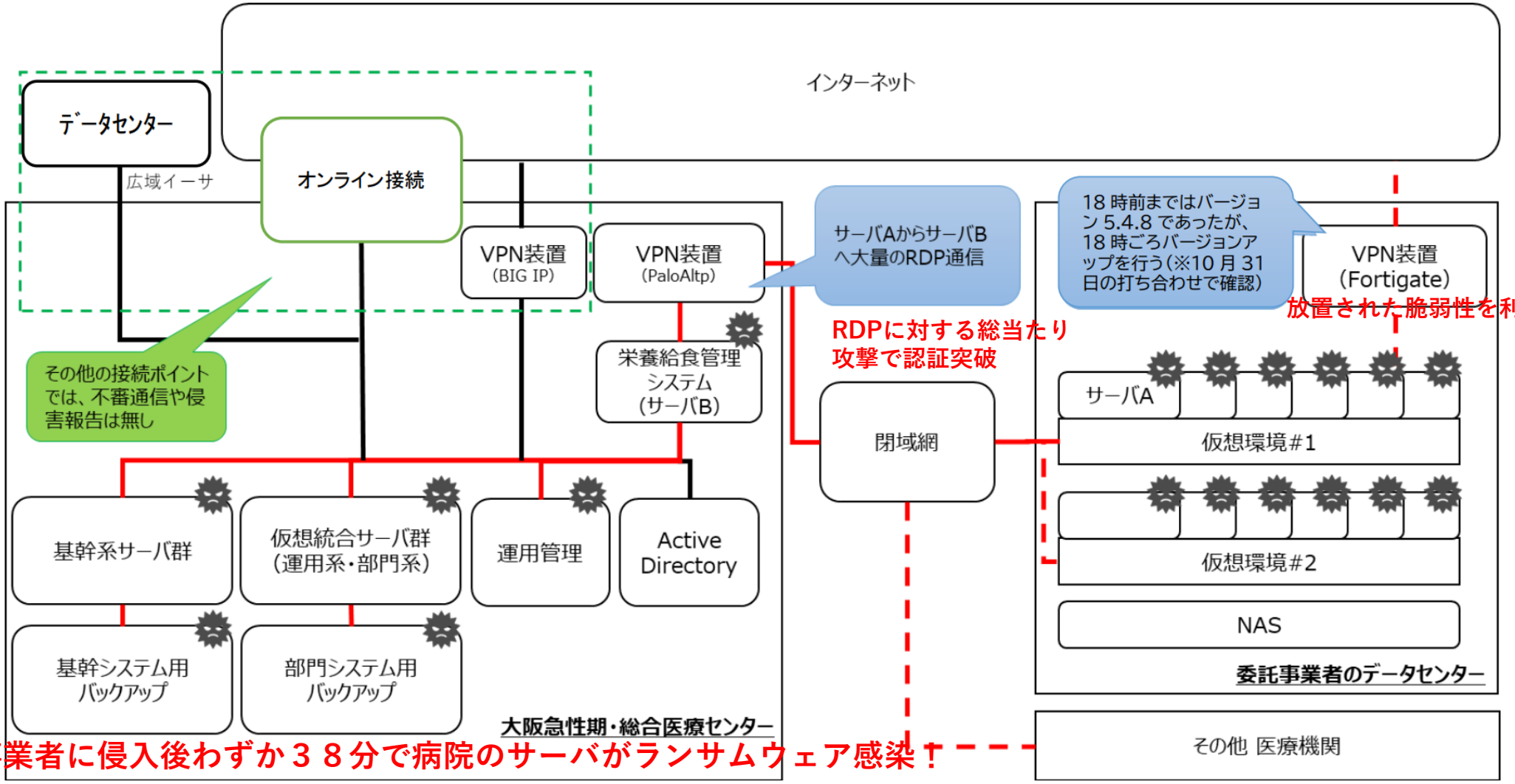
ダークウエブ情報の活用による被害に未然防止

読売新聞2021/12/30朝刊

都立2病院 ハッカー標的
サイバー攻撃準備 都が注意喚起

箱根「第１回参加章」
大阪で発見 1920年開催

大阪急性期医療センターのランサムウエア被害の実態



委託事業者に侵入後わずか３８分で病院のサーバがランサムウェア感染！

＜関連システムのネットワーク構成図と感染状況＞

2022 年 11 月 7 日報道公表資料より

厚生労働省注意喚起(2022/11/10)：サプライチェーン攻撃への対処
～脅威インテリジェンス診断の活用提案～

厚生労働省注意喚起(2022/11/10)
「～自組織のみならずサプライチェーン全体を俯瞰し、発生が予見される リスクを医療機関等自身でコントロールできるようにする必要があることから、関係事業者のセキュリティ管理体制を確認した上で、**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。**」

- **自施設のリスクの客観的な把握・評価**
- **ベンダーと協力したセキュリティ対策**
- **医療機関としての診療継続確保(BCP対策)**
- **医療機関としての患者情報の安全管理確保**

医療機関として具体的に何をすればよいのか？

自施設がハッカーからどう見えているか？を具体的に把握

外部攻撃対象領域(External Attack Surface : EAS)の可視化

自施設およびサプライチェーン内の管理対象事業者のドメイン・サブドメイン・IPの脆弱性の存在有無と脆弱性の特定、重要性・対策方法の特定

脅威インテリジェンス調査

施設毎の優先順位・予算等に応じた最適化された対策実施

自施設自身およびベンダー依頼による脆弱性対策実施

常に変化するサイバーリスクに対する継続的な調査・対応

脅威インテリジェンス調査

月１回定期的
新規脆弱性公表・新規脅威発生
システム更新・入替え、新規医療機器・システム導入

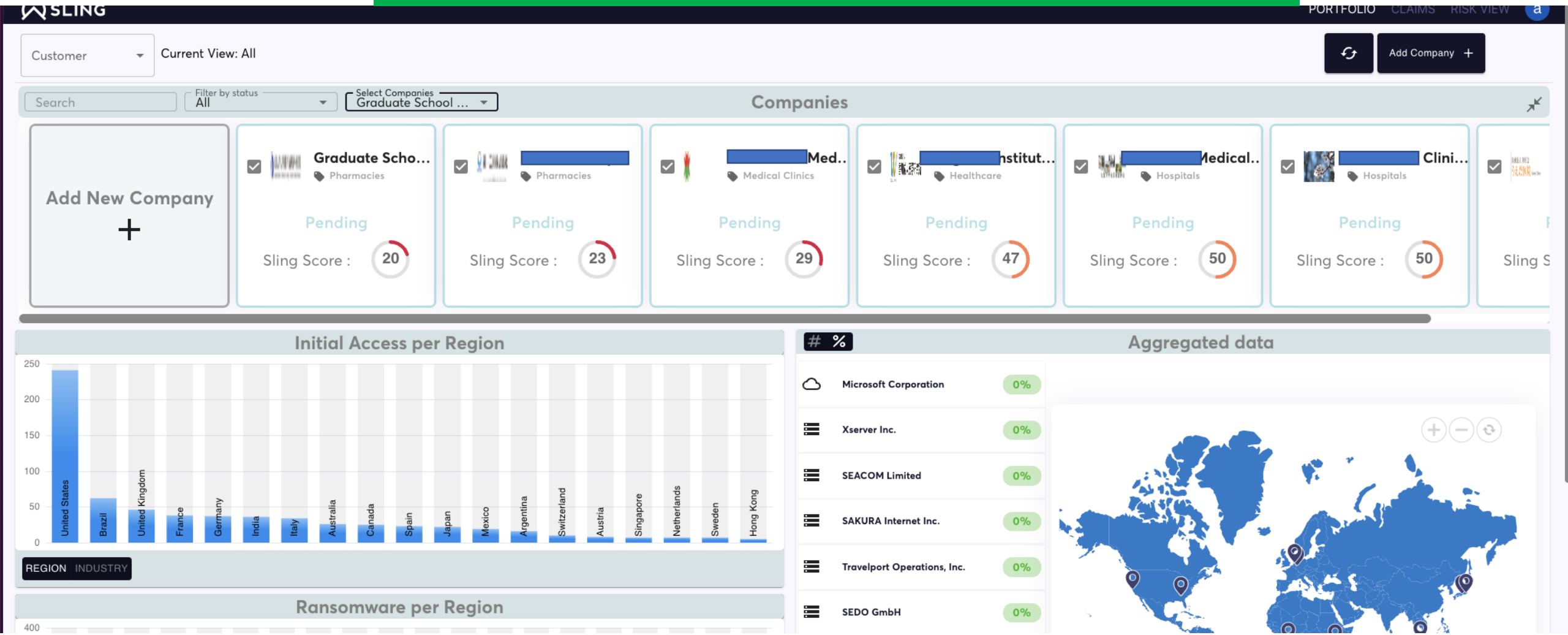
医療ISACが、脅威インテリジェンス診断（MITIS）・分析・説明・対策提案・対策導入まで全て継続的に支援します

医療ISACが提案する脅威インテリジェンスの新たなソリューション “SLING”

- リスクスコア表示（スコアの経時的変化可視化）
- ベンチマーク比較
- EAS診断とダークウエブ監視の併用
- サプライチェーンリスクも同時に評価可能
- 比較的安価で容易な導入

SLING: Vendor Monitoring Japan - Sling Cyber Insurance

医療ISACが提案する脅威インテリジェンスの新たなソリューション “SLING”



ベンチマーク比較

サイバーキルチェーンの各段階と対策

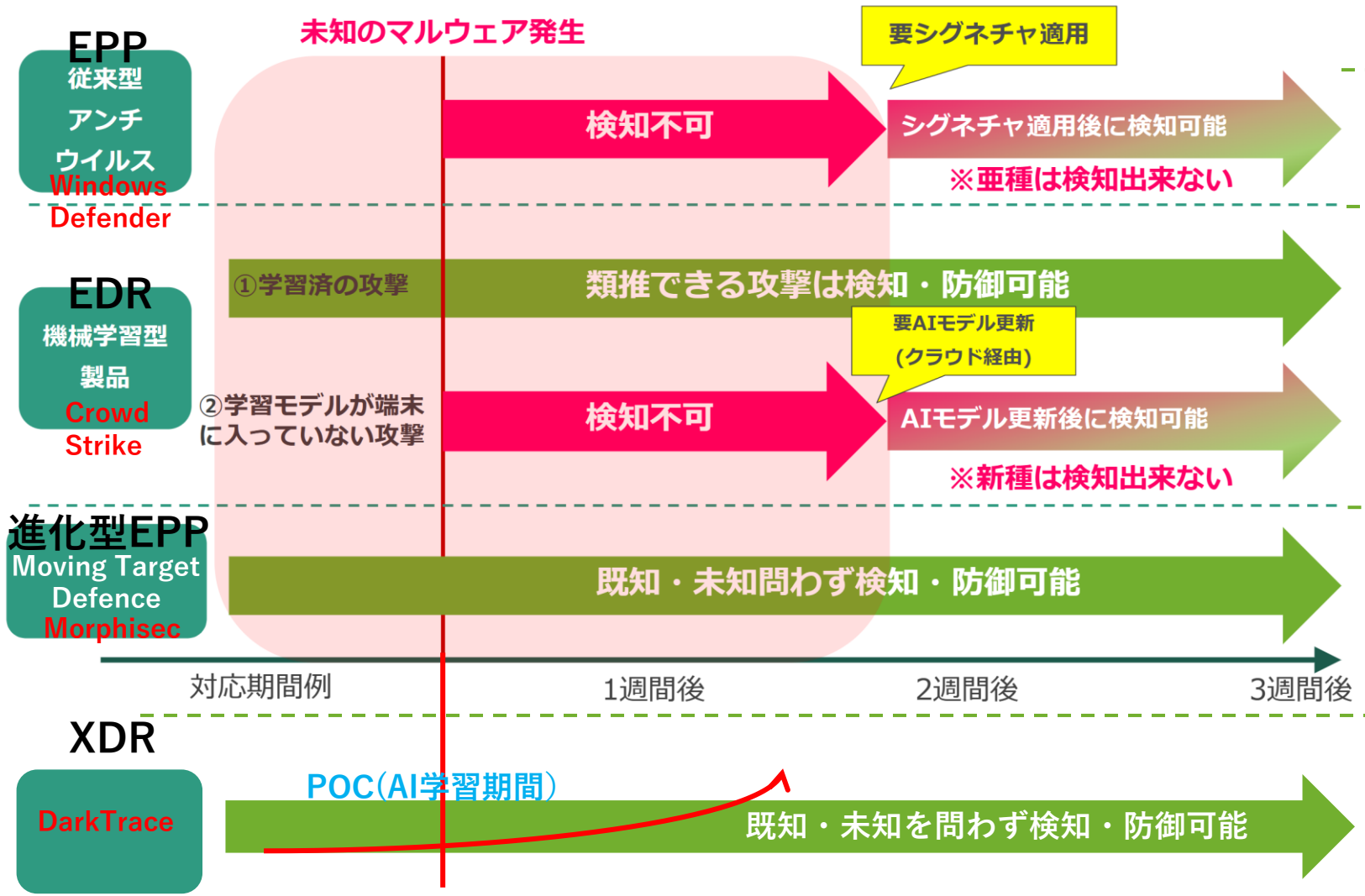
0.事前準備	1.開始	2.足掛かりの確立とビーコニング（C2）	3.水平移動	4.データ抜き出し	5.ファイル暗号化	6.身代金 - $	7.クリーンアップと復旧 - $$$	8.サイクルの繰り返し
・情報収集 ・**脅威インテリジェンス** ・BCP策定 ・サイバー保険加入 ・マニュアル・規定類整備 ・サイバー訓練 ・従業員教育	・Eメールセキュリティ ・FW・UTM ・エンドポイントアンチウイルス ・IDS/IPS ・EDR/XDR	・FW ・IDS/IPS ・EDR/XDR/MDR ・EPP	・FW & NAC ・IDS/IPS ・EDR/XDR ・AD保護	・FW&Proxy ・DLP ・EDR/XDR	・FW & NAC ・IDS/IPS ・エンドポイント ・アンチウイルス ・EDR/XDR	・サイバー訓練 ・経営者の覚悟	・IR ・Backup対策 ・サイバー保険 ・サイバー訓練	

Proactive ← → **Reactive**

侵入・感染させない対策

侵入・マルウエア感染することを前提とした対策

EPP(EndPoint Protection)/EDR(Endpoint Detection and Response)/ XDR(Extended Detection & Response)



	目的	Internet 接続	Smart phone Tablet 対応	導入 方法	規模感	価格	検知後 対応
EPP	防御	要	可	端末 install	小~大	安価	要
EDR	被害 検知 最小化	要	製品 によっ て可	端末 install	小~大	中程度	要
進化型EPP	防御	不要	不可	端末 install	小~大	中程度	不要
XDR	被害 検知 最小化	不要	可	Network 上に Agent 設置	中~大	高価	要

データの復旧と身代金支払いに関して
半田病院調査報告書より

25	11 月 3 日	1 時 30 分	一部の環境でローカルネットワークを構築。
26		15 時 00 分	FortiGate（Fortinet 社）の VPN のファームウェアのアップデートを実施。 → VPN のログ確認や保全、保存などは未確認。
27		16 時 00 分	A 社紹介の修復会社（以下、B 社という。）との調査と復旧に関する打ち合わせをオンライン会議にて実施。以下の方針を確認。 サーバー系統（約 15 台）、部門システムサーバー（台数不明）をＢ社（東京）に郵送し、調査復旧を試みる。 クライアント端末（200 台）は、ネットワークに接続し、ウイルススキャンを行い、駆除対応を行う。
64	11 月 19 日		一部の端末でファストフォレンジックを再実施。 Ｂ社より暗号化されていたデータの一部が復元されたサンプルデータが送付される。（復元できる状況になったことの確認。） 電子カルテの再開目標をサーバーの返却目処や電カルのサーバー調整や導入などを鑑みて、22 年 1 月 4 日に設定。 産婦人科において新規の妊産婦の受け入れを再開。
65	11 月 22 日		一部の端末でファストフォレンジックを再実施。 身代金要求が行われていないが、支払わない方針を正式決定。 C 社、A 社と Web 協議（クラウドシステムは利用せずに仮復旧を行う旨の打ち合わせを実施。C 社に提案や対応の遅れに対するクレームを入れる。）

A社：スタンシステム社（徳島）
B社：デジタルデータソリューションズ社
C社：JBCC社

3.4.3.5 データの復旧

多数の PC やサーバーが Lockbit2.0 によって暗号化されてしまったため、院内のシステムに あるデータが利用できない状況になってしまった。想定される復旧としては大きく二点である。

2018 年まで にオフラインで保管していたバックアップデータについては Lockbit2.0 の影響を受けなかったため、復旧す ることができた。

もう一点は、**Ｂ社による復旧で今回のデータ復元に必要な手段を入手し、対応した可能性** である。特に後者の復旧においては、最終的な復旧方法はＢ社独自の調査のため詳細は把握できなかったが、半田病院側との会議の中で「適合が困難で復旧に時間がかかっている」「修復プログラムを組んでい る」といったようなやり取りがあったこと、さらには、データを復元できていることから、**何かしらの方法で修復に必要な手段を入手し、データの復元を行った可能性**がある。なお、楕円曲線暗号などの暗号技術そ のものを解決しなければデータ復旧を行うことができないため、Ｂ社の回答はセキュリティの初心者である ユーザーへの説明不備であり、**修復プログラムではなくデータ復元に必要な手段を入手したと考えるのが復旧の流れとしては考えるのが妥当**である。しかしながら、攻撃者によるデータ暗号に関する脅迫文は最初の プリンタによる出力のみであり、データが攻撃者によって公開された事実などが確認できなかったこと、それ以降の身代金要求の事実も確認できなかったことなどから、**Ｂ社の折衝は定かではない**。なお、当然ながら***半田病院は身代金を支払わない方針を決めており、身代金を支払った事実もない***。

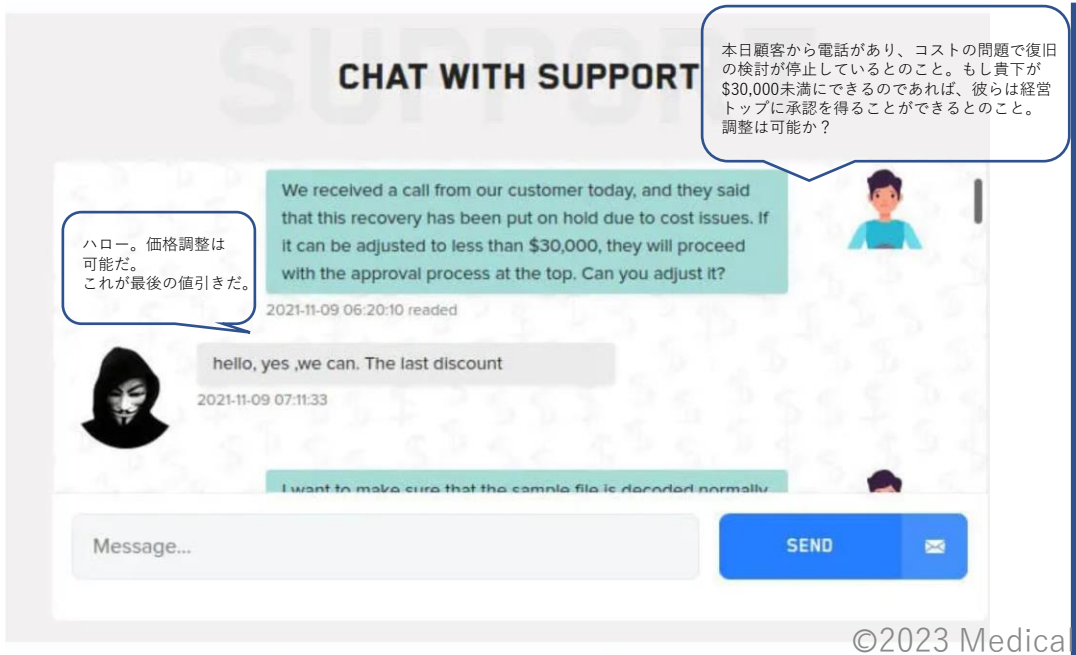
Lockbit2.0の楕円関数を用いた暗号は自力での復号は現実的には不可能
（現在のコンピュータでは約160万年かかる）

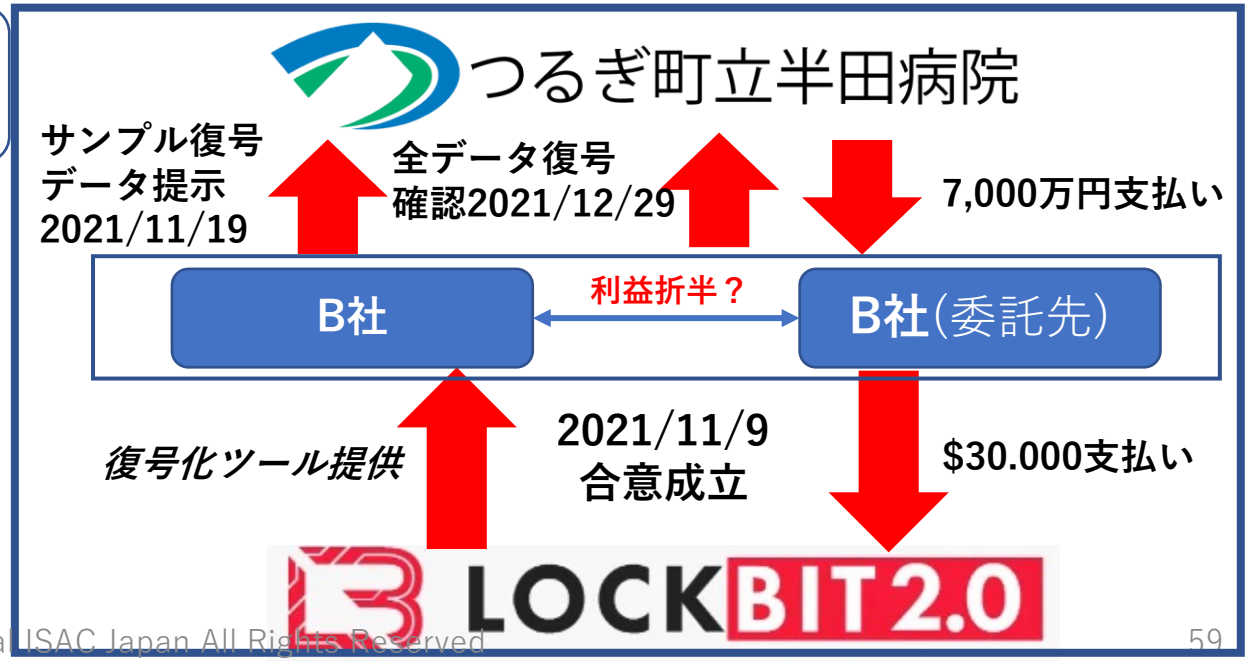
犯罪集団に3万ドル支払いか　ロシア拠点ハッカーが主張

共同通信社2022/10/26

昨年10月に身代金要求型コンピューターウイルス「ランサムウエア」によるサイバー攻撃を受け、一部診療停止に陥った徳島県つるぎ町立半田病院を巡り、ロシア拠点のハッカー犯罪集団が「データの『身代金』として3万ドル（約450万円）を受け取った」と主張していることが26日、分かった。警察庁などは身代金を払うべきでないとしており、つるぎ町も払わないと表明していたが、復元を依頼されたIT業者の関係者が交渉した可能性がある。

　ハッカー集団は電子カルテなどのデータを暗号化し、復元と引き換えに半田病院に金銭を要求。取材に対し「取引は成立し、復元プログラムを提供」と説明した。





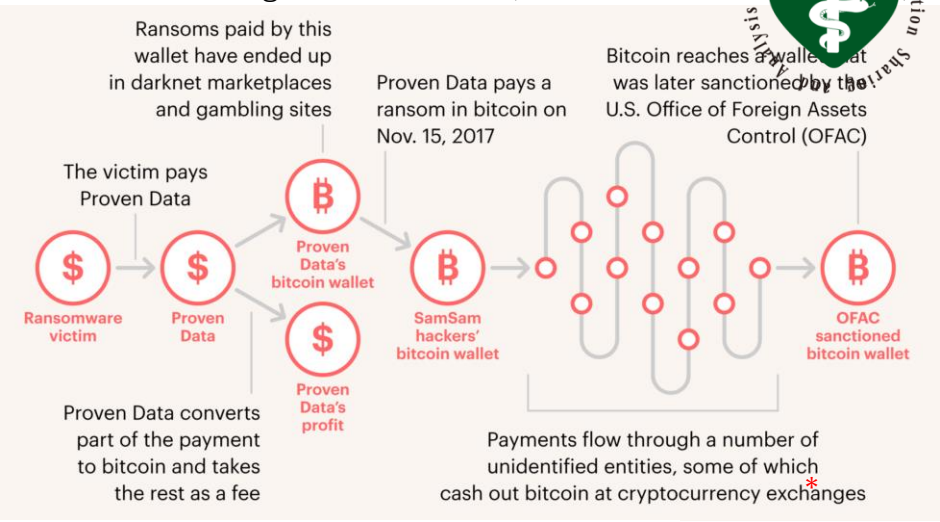
徳島県つるぎ町立半田病院の代理人とハッカー犯罪集団のやりとりとされる闇サイトの画面

ランサムウェアの攻撃者と被害企業とを仲介する「ビジネス」（疑い事例も含める）

＊Proven Data(New York, USA)←確定
＊MonsterCloud(South Florida, USA)？
＊Red Mosquito(Scotland, UK) ←ほぼ確定
＊ランサムウエアセンター（Saitama, JPN)?
＊デジタルデータソリューション(Tokyo, JPN)？
　サービス名：デジタルデータリカバリー

こうした企業はデータリカバリーの専門業者のようにも見えるが、実際には**被害企業に代わって身代金をランサムウェアの攻撃者に支払い、攻撃者から暗号化されたデータを復元するキーを入手してデータを復旧**している可能性がある
→**ランサムウェアの攻撃者と事実上結託**

Proven Data社における身代金窃取仲介の流れ(FBIにより解明)
*OFAC: Office of Foreign Asset Control(米国財務省外国資



S&Eシステムズ株式会社
We'll bring IT revolution to your company.

新聞社の取材に対して、lockbit側から復号化ツールを提供され身代金を代行して支払い、復号化を請負っていることを認めている。

デジタルデータソリューションズ社
半田病院
青山病院
においてデータ復旧を請負いか？
（独自技術による復元と主張)

ランサムウェア感染時のデータ復旧方法の選択肢

NO MORE RANSOM

優先順位

有効なバックアップデータから復元

↓

No More Ransomから復号キーを入手して復元

↓

警察庁に依頼して復元（現状ではLockbitのみ）

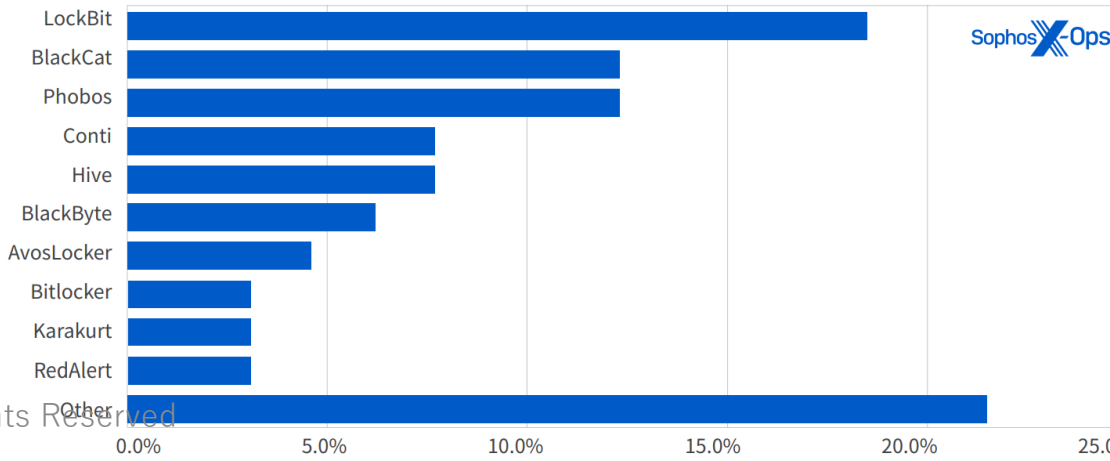
↓

仲介事業者に委託し復号キーを入手して復元

Lockbitによる暗号化されたデータの復元に成功

警察庁

- データ復元は警察庁のサイバー警察局、サイバー特別捜査隊が担当。暗号化されたデータからマルウェアを解析し、暗号化の復元を行うシステムを開発した。2022年4月以降、Lockbitの被害に遭った3社において捜査の過程でデータの復元に成功した。*1
- 復元成功に至った組織の一社はNITTANで、2022年9月13日早朝に暗号化によるシステム障害発生が発生し、2022年10月14日には警察、各システム会社及びサイバーセキュリティ専門会社の協力をうけシステム等の復旧作業を開始している。取材に対しては同社は復旧費などの損失を回避できたとコメント。*2
- 警察庁から欧州の複数の国の捜査機関に対して、今回の復元方法の情報を提供が行われている。
- 取材に対して警察庁は被害回復の事例が複数あることを認めているが、具体的内容については差し控えると回答している。*3



ソフォス脅威レポート 2023 年版 (sophos.com)

Agenda

0．医療ISACの活動紹介

1．医療機関におけるランサムウェア感染の事例から導出される教訓
：特にFortiOSおよびデータバックアップについて

2．システムおよび医療機器ベンダーとの付き合い方
：「セキュリティはベンダーに丸投げ」で本当によいのか？

3．経済産業省・総務省ガイドラインの活用方法（事例紹介）

4．脅威インテリジェンス診断の有用性

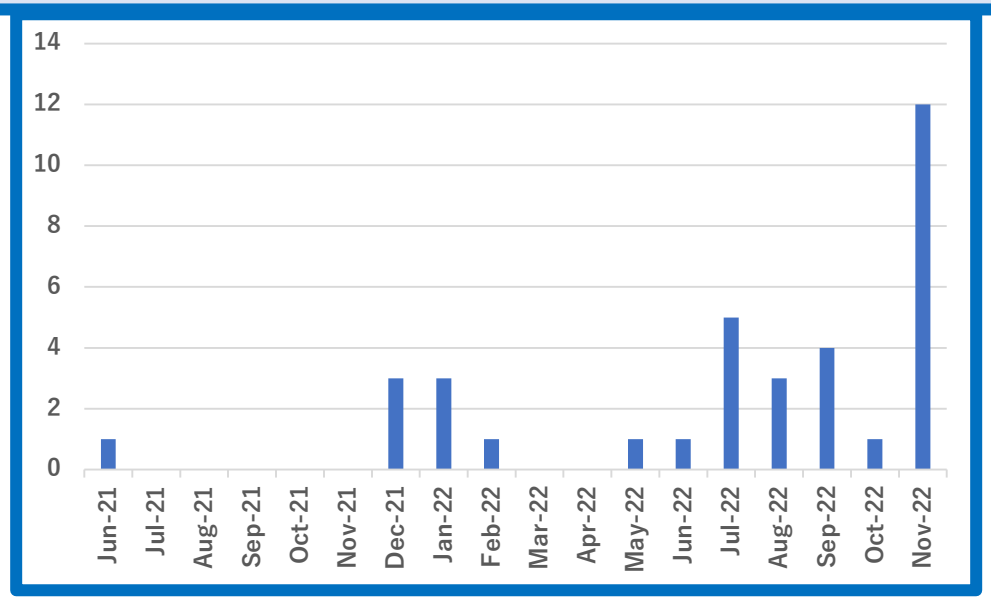
5．医療ISACとして医療機関に対して支援できること

6．質疑応答

医療ISACのサイバーセキュリティ無料相談

相談事業者数(2021-2022)：44
- 病院　：19
- 診療所　：8
- 薬局　：10
- その他　：7

相談内容（のべ43件）
- 一般的なセキュリティ対策　：25
- 脅威インテリジェンス診断関連　：11
- 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）：3



相談件数の月次推移

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　○○○○

医療ISACのCS²(Cyber Security Cordinater Service)

医療機関と各ベンダーの間に入る「情報システム管理人」をイメージ

医療ISACオンライン無料相談（１時間程度）

・e-mail security診断
・脅威インテリジェンス診断
　外部攻撃対象領域可視化（自施設がハッカーからどのように見えているかを可視化）
　脆弱性診断（ベンダが遠隔保守目的等で持ち込んだVPN装置：FortiGate等の脆弱性診断を含む）

・診断結果に基づいたコンサルティング
　優先順位・予算感等に基づいたセキュリティ対策提案・導入支援
　ベンダーとの交渉代行（脆弱性対策の確実な実行）
　医療機関にとって一方的に不利な保守契約書の改訂交渉代行
　技術的なセキュリティ対策の最適化・導入支援
＊ランサムウェア被害等発生時
　IR：インシデントレスポンス
　データ復旧支援
　費用補償（保険付帯）

※インシデント発生時の緊急コール先（Tell番号）を確認（提携緊急対応事業者など）
※インシデント発生時は直接↑にcallして対応を依頼
※IR・データ復旧費用を上限500万円まで補償（エビデンス＝IR対応ベンダーの報告書）

医療ISACセキュリティニュース配信

Jan.4th 2023
TLP: GREEN
TLP: GREENに該当する情報は、コミュニティ内の組織と共有できますが、公的に開示してはいけません。
医療ISACにおけるTLPの定義

Leading Story
ポーランド、ロシア系ハッキンググループGhostwriterによる攻撃を警告

Summary
ポーランドは、ロシア国家が支援する脅威アクターであるGhostWriterなどによるサイバー攻撃の脅威が増大していることについて警告しています。

Analysis & Action
ポーランド政府は、ロシア由来のサイバー攻撃が増加していると公式サイトで警告しており、ロシアがスポンサーとなっている脅威アクターGhostWriterの活動が確認されています。
サイバー攻撃は、さまざまな公共ドメイン、重要インフラ、兵器プロバイダーを標的にしていると評価されており、サイバー攻撃の中には、ロシアのハイブリッド戦争戦略の一環であるDDos攻撃やフィッシングが確認されています。
また、ロシアによる軍事活動に有利な偽情報の拡散や、ジャーナリストになりすまして反NATOの記事を広めることも攻撃の焦点になっているようです。
ロシアのウクライナ侵攻が継続されている中、戦争後もロシアへの経済制裁や周辺国化が続くため、NATOの同盟国やウクライナ支援国に対するサイバー攻撃は続くと予想されます。

MICSS
Medical ISAC Japan Cyber Security Service

無料相談
医療ISAC

①脅威インテリジェンス診断

MITIS
医療ISAC

外部攻撃対象領域を含む
リスクアセスメント

②ネットワークセキュリティ

AIによるサイバー脅威の検知・調査・遮断

電子カルテから
セキュアなインターネットアクセス

危険なサイトへのアクセスや
C&Cサーバへの通信をブロック

RevoWorks
ジェイズ・コミュニケーション

Darktrace
ダークトレース・ジャパン

MGSP
三井物産セキュアディレクション

MGSPは、ジェイズ・コミュニケーションが
RevoWorksProxyサービスとしてご提供します

侵入防止および早期検知

③エンドポイントセキュリティ

サーバーとPCのマルウェア感染を防止

端末防御

診療系NW
（電子カルテ等）

MORPHISEC
ワイ・イー・シー

情報系NW
（e-mail, Web）

④バックアップソリューション

ランサムウェアに対応したクラウドバックアップと確実な復元

TDaP
ティエスイー

ランサムウェア被害の最小化

医療機関様向けにMICSSソリューション群を
４つのスキームに分けて６つの製品をご提案

MICSS
Medical ISAC Japan Cyber Security Service

MICSSソリューション群の製品（MITISを除く）を年間契約していただくと万が一のサイバーインシデントに対する復旧作業の費用が補償されます

サイバー攻撃などによるランサムウェア等によるインシデントが発生した場合は、迷わずサイバーレスキュー専門業者をコールしてください。専門業者による以下のインシデントレスポンスに関する作業費用を、MICSSに付帯する保険で補償いたします。（年間500万円まで補償）

初動対応（戦略立案）	調査	復旧	報告
• 専門窓口への初期相談及び状況調査 • 対応方針決定等の初動支援 • フォレンジック調査対象策定 • 証拠保全（解析対象とするデータの保全と収集を実施。） • 復旧希望有無の確認	• HDD/SSD内の各種ログの調査・解析 • インシデント発生の原因調査 • マルウェア感染の影響範囲調査 • 影響範囲調査 • 情報漏洩有無の調査	• 削除データの復元 • システム修復支援 • 修復に向けた推奨事項 • システムの修復 • データの修復	• 調査内容報告会を開催 • 推奨事項のアドバイス • 調査報告書（納品物）

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

Agenda

0．医療ISACの活動紹介

1．医療機関におけるランサムウェア感染の事例から導出される教訓
：特にFortiOSおよびデータバックアップについて

2．システムおよび医療機器ベンダーとの付き合い方
：「セキュリティはベンダーに丸投げ」で本当によいのか？

3．経済産業省・総務省ガイドラインの活用方法（事例紹介）

4．脅威インテリジェンス診断の有用性

5．医療ISACとして医療機関に対して支援できること

6．質疑応答　　mail to hiroshi.fukatsu@m-isac.jp