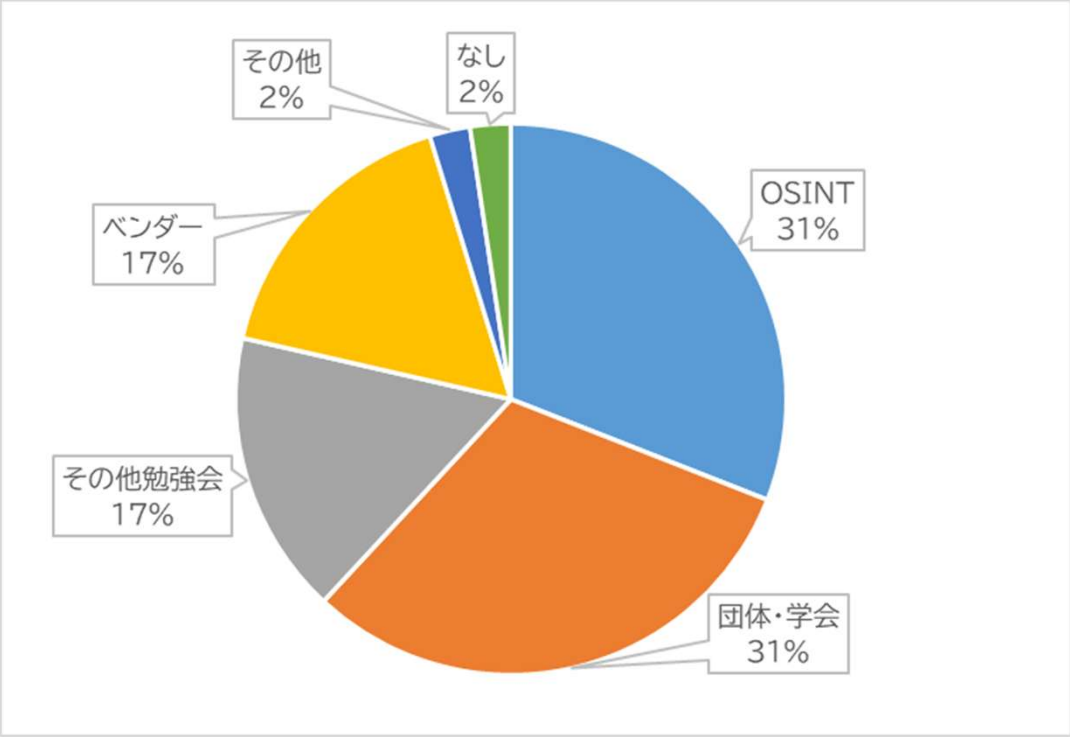
本日のみなさま

【情報源は？】

N＝42



・医療情報学会の名前を約３割の方が挙げてました
・一方で、IPA,JNSA等のIT系団体の名前はほぼ見当たらず
・なしと答えた方も・・・・

講師への質問コーナー

【テーマ　インシデントレスポンス（あの日、あの時・・・）】

★情シス担当者視点での実際のインシデント対応について教えてください
★インシデント後に**最低限ここはしておくべきだったと思ったこと**を教えてください。
★最初はパニックになったと思うが、**どの様に判断して動いたのか、**具体的な話を聞きたい
★被害を受けた時に、**何が最も大切だと感じる**か。
★ウィルス感染時の対応（主に初動）
★サイバー攻撃を受けている中で、**情報部からの発信が職員に正確に届くものでしょうか**？
　難しそうな印象を持っています。
★攻撃の流れ ・**かならず強化すべき箇所**（ADサーバーの管理者の操作履歴など）
★**やっても意味が無かった、意味はあったけど大変だったこと**はありましたか？

講師への質問コーナー

【テーマ　インシデントレスポンス（あの日、あの時・・・）】

★インシデント後に**最低限ここはしておくべきだったと思ったこと**を教えてください。
★**意味はあったけど大変だったこと**はありましたか？
アンチウィルスソフトの確実な導入、Syslogの利用
★最初はパニックになったと思うが、**どの様に判断して動いたのか、**具体的な話を聞きたい
偶然、「暗号化される」途中の端末に気づいた
プリンタの紙は最初文字化けかと思ったが後にLockBitのランサムノートだと判明した
★被害を受けた時に、**何が最も大切だと感じる**か。
組織内の報告ルート、最終的な意思決定をだれが行うか確実にしておくことが、迅速な対応には必須です（座長より）。
★サイバー攻撃を受けている中で、**情報部からの発信が職員に正確に届くものでしょうか**？
難しそうな印象を持っています。
元々設けていた災害対応時の連絡体制が上手く機能したが、実際は最低限必要な初動（抜線等）は、都度、
病棟、部署のリーダーに対して共有しておく必要はある
★攻撃の流れ ・**かならず強化すべき箇所**（ADサーバーの管理者の操作履歴など）
それぞれの接続点（外部ー内部、内部のネットワーク同士）の監視とセキュリティ強化
接続点を明確にし、把握漏れがないようにするのは重要で、それにより万一の場合の被害想定の精度が上がる
（座長より）

講師への質問コーナー

【テーマ　経営層の理解】

★サイバーセキュリティ対策に対する**予算計上を病院幹部に納得させるためにできること**について。

・一度被害に遭ったことで、院内での納得感のレベルは変化。必要なものと認識できた。

・病院によっては、訓練シナリオの作成を複数年でのプロジェクトにすることで、参加者の範囲を広げ、院内にセキュリティ対策の重要性の浸透を図る例もある（座長より）

【テーマ　ベンダーマネジメント】

★インシデント対応時の**電子カルテベンダーとのやりとり**

★**セキュリティについてベンダーとの契約書に入れるべき必須項目**。

メンテナンス契約があっても保守契約を結んでいなかったことで、アップデート等に対応できてなかった点がある、日常から良好な関係性を維持するのも必要

アンケートQAコーナー

【テーマ　セキュリティマネジメント】

★情報セキュリティ対策の**順番、重要度などの順位付け**

★セキュリティ領域に対する**安全管理の一環で、演者様が有効だったと考えられている施策**はどのようなものでしょうか？

バックアップとデータ参照用仮システムの有効性は他の事例でも取り上げられており、有効だと思います。
また、重複しますが、内外、ネットワーク同士の接点の管理とログ監査も有効です（座長より）

★ISMSは有効と思いますか

ISMSの制度そのものはある時点での評価であることから肯定的でない意見もありますが、準備段階でセキュリティ関連の情報が整理できる点は効果的だと思います。ただし、ＩＳＭＳをゴールとせず、標準的に維持できるべきレベルと考えるのが重要です（座長より）。

★セキュリティ対策の**部署はあの事件以降増えていますか**？ また、セキュリティ対策は**他社依存メーカに依頼）なのか内製なのか**割合など知りたいです。

セキュリティチームの加盟する日本シーサート協議会に加入している医療機関はほとんどありませんが、厚労省のトレーニングが開発されたり、兼任でも担当者を置こうという例は増えているのでは（座長より）

【テーマ　IT-BCP】

★**IT-BCPの観点から平常時からの準備、対策、有用なツール**などがあれば知りたいです

他の項目と重複しますが、バックアップを挙げます。（座長より）。また、職員相互の連絡手段が、システムと連動している場合は、他の事例でも、別の連絡手段も確保している（電話回線増設、災害用安否確認ツールの利用）ので、災害用BCP以外での利用場面も想定できると良いと思います（座長より）

アンケートQAコーナー

【テーマ　人材・教育・研修】

★**医療機関のシステム管理者に必要だと思う素養、基礎知識に**ついて

色々な業務に対応できること

★コンピューターの専門知識を持っていないが、セキュリティ担当になった場合の勉強方法、**そもそも何から勉強を始めると良いか**、

厚生労働省の提供している医療機関向けサイバーセキュリティ研修の動画をお勧めします。

またはIPAのセキュリティ啓発動画もあり、いずれも無料です。（座長より）

★もはや侵入される前提である時に、被害を最小限にとどめるという命題に多層防御や訓練などは当たり前として、**担当職員の質として何が重要**だと考えますか？

被害を最小限にとどめるには、案外に人の要素が重要になります。適切に報告ができること、何より動揺してパニックにならないこと、記録を残せること。簡単なようで案外難しいのが記録ではないかと思います。（座長より）

★**職員への教育方法、社内のセキュリティ意識醸成・向上**

・小規模な訓練を行うこと、一斉停電を利用してのシステム停止時の対応の訓練の実施

・新入職研修からの繰り返し、組織内ポータルサイトでの啓発等を行っています（座長）

アンケートQAコーナー

【テーマ　訓練】

★**IT一BCP訓練の具体的方法**が知りたい

厚生労働省が2025年度に、「講師養成講習」やシステム管理者向けトレーニング
として訓練を提供していますので、そのような企画への参加も一案ではないでしょうか。
また、大学のセキュリティ専門のリカレント教育でも訓練を行っている例、都道府県
によっては警察や保健局主導で訓練を行った例もあります。（座長より）

★**スモールスタートでできる訓練方法**がございましたらご教授ください。

仮想のシナリオを用いて、意思決定に関わるメンバーだけを集めて行う訓練方式が
あります。それであれば、数人からのスタートが可能です（座長より）

★**他社・他部署・多職種横断型の訓練**

・とある施設では、複数年をかけて徐々に参加部署を増やして実施した例があります
最初から多職種連携は勤務調整も必要なので、多職種横断をゴールにして、シナリオ
のブラッシュアップの過程で参加者を拡大してはどうでしょうか（座長より）

講師への質問コーナー

【テーマ　日常業務のコツ＆病院情シスの生態とは？】

★**参照用データをバックアップとは別に確保する**仕組みについて
別途資料あり
★**毎日ここは見ろ！**というポイントを教えてもらいたい
内部ー外部の、NW同士の接続点
★カルテや部門を含めた**統一した二要素認証とID管理**の方法。
電子カルテの中には、Teamsと連動させられるものがあり、その場合はＭＳアカウントを使えます。個々の端末はWindowsHelloを利用する例もあり
業務上多要素認証が難しい箇所（手術室等）は、入退室を厳密な管理と顔認証の併用（参加者より）
★何から**情報収集を行っているのか。普段から意識している事**は何か。
・ベンダーからの情報提供は重要です
・医療情報学会やCISSMED（医療機関のセキュリティ関係者の任意団体）等での情報収集のほか、IPAや日本ネットワークセキュリティ協会等も様々な情報を提供していますのでご参考ください（座長より）

講師への質問コーナー

【テーマ　立ち入り検査どうなの？参加者の皆様も教えて！ 】

★これまでの立ち入り検査と、**2021年以降の立ち入り検査**との違い

★立入検査対策（**規程類の整備等**）

【テーマ　こうなればいいけど・・・・ 】

★医療機関のセキュリティ対策に対し、**国に対して言いたい事**は何ですか？

★病院のセキュリティ対策(それ以前に医療情報化も)はあまりにも**インセンティブ設計**が出来ておらず，おざなりになるのも止むなしと感じるのですが，どのようなインセンティブ設計（たとえば保険点数への反映，義務化…）が医療機関をセキュリティ向上活動に向かわせることができるとお考えでしょうか.

医療機関と
サイバー問題をめぐる現在地

国内のサイバー攻撃被害

国内でのランサムウェア攻撃（2025年上半期）

116件（上半期としては最多）二重脅迫型が多くを占める

復旧までの費用　復旧に長期間を要した組織ほど高額に
ただし、1週間未満であっても14%は
1,000万円超を要している

サイバー空間をめぐる脅威の情勢等（警察庁　2025年上半期）より

流れ弾の被弾から
明確な標的に

医療機関をターゲットとする攻撃グループ

BlackCat（別名ALPHV、Linuxでも実行可）、LockBit 4.0

医療機関のランサムウェア攻撃（2025年1月～10月）

病床規模	被害件数	被害割合	平均身代金要求額
20床未満（診療所）	15	17.60%	5,000万円
20-99床	28	32.90%	1.5億円
100-199床	17	20.00%	2.5億円
200-299床	12	14.10%	3億円
300-499床	8	9.40%	4億円
500床以上	5	5.90%	5億円

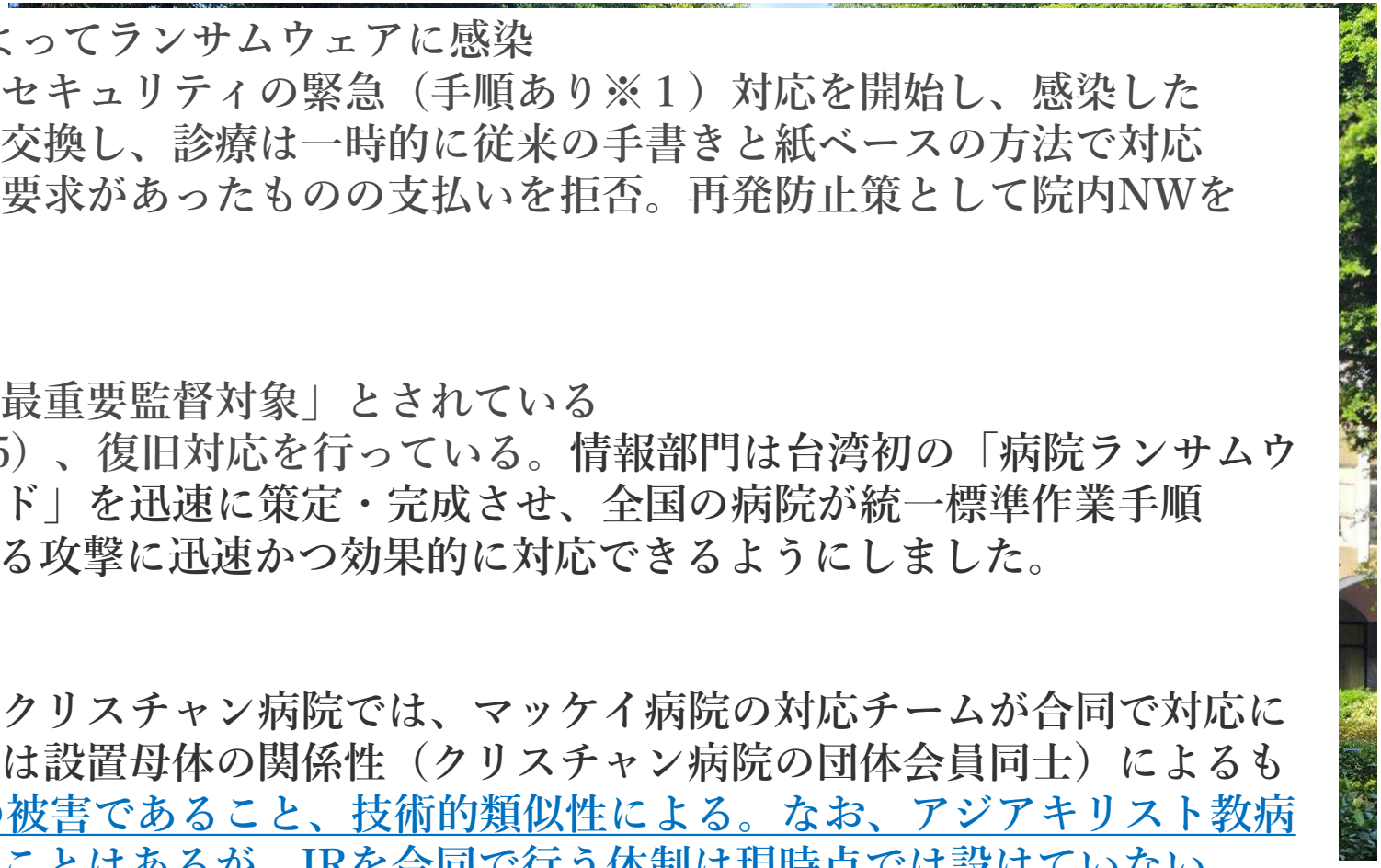
20～199床の施設が半数

病床数の分布もヴォリュームゾーン

医療機関を狙うランサムウェア最新事情2025より　https://00m.in/OGnnd

馬偕記念病院事件

カナダ・プロテスタント系私立病院。１８８０年
G.マッケイ宣教師によって設立



2025年2月　CrazyHunterによってランサムウェアに感染
即座にサイバーセキュリティの緊急（手順あり※１）対応を開始し、感染したすべての端末を交換し、診療は一時的に従来の手書きと紙ベースの方法で対応
高額な身代金の要求があったものの支払いを拒否。再発防止策として院内NWを分割

【補足】
現在、台湾では医療機関は「最重要監督対象」とされている
情報保安局が調査（中身はT5）、復旧対応を行っている。情報部門は台湾初の「病院ランサムウェア対応訓練および戦闘コード」を迅速に策定・完成させ、全国の病院が統一標準作業手順(SOP)のもとで将来起こりうる攻撃に迅速かつ効果的に対応できるようにしました。
※SOP＝標準作業流程

その後、被害が発生した彰化クリスチャン病院では、マッケイ病院の対応チームが合同で対応にあたっている。ただし、これは設置母体の関係性（クリスチャン病院の団体会員同士）によるものではなく、Crazy Hunterの被害であること、技術的類似性による。なお、アジアキリスト教病院協会は、合同で啓発を行うことはあるが、IRを合同で行う体制は現時点では設けていない。

長慎病院（慢性期病院）：システム停止、サイバー攻撃の疑い

2025年4月14日に駭客（ハッカー）から病院宛に「金を払わなければ8万件の病歴データを公開する」と脅迫メールが届き、同院のネットワーク予約・初診受付・処方箋発行などの機能が停止した。

対応状況
•長慎医院はハッカーからの連絡を受けた直後、桃園市衛生局に通報し、院内外のネットワークを遮断。
•衛福部（台湾の厚労省に相当）のガイドラインに従い、システムメーカーと共に全サーバのスキャンを実施。
•アンチウイルスソフトと医療情報システムを再インストール。個人情報の流出範囲は調査中。

警察の動き
•2025年4月15日に病院が警察へ届け出。
•中壢分局によると、メールは「国際ハッカー」を名乗っており、国外組織の可能性もあるとして捜査を進めている

現場の運用への影響
•システム停止により、病院は手作業で受付・呼び出し・処方箋作成を実施。
•報道取材について病院側は回答を拒否している。

政府の見解
•衛福部は被害を確認し、過去に被害があった馬偕病院や彰化基督教病院と同様の対応プロセスに基づき処理する方針。

医療機関59施設にみる、復旧優先度の考え方

N＝59

最優先で復旧	回答数	選択理由の例
電子カルテシステム	30	・診療の核となる ・電子カルテ参照システムがない ・システム構成上参照システムが無事な可能性を考慮 ・ミスの発生しやすい手書きを減らすため
電子カルテ参照システム	28	・診療に最低限必要な情報がある ・復旧所用時間が短い、できるだけ早期に診療水準を戻すため ・被災直前の患者情報を迅速に収集するため ・被災直後は紙運用のため、参照システムのほうが有効
医事会計システム	1	平時の業務負荷に基づく判断（中規模病院）

その他意見として「院内の情報共有用のWEBサーバ」とのコメントがあったが、ポータル用のWindows系サーバであった。（WEBサーバがLINUX系であればBlackCat、LockBit5.0以降は感染リスクあり）

基幹インフラ事業者への医療機関の追加について

高度な医療（救命・災害医療等を含む。）を提供する能力等を有する医療機関については、地域の医療の安定的な提供の確保に重要な役割を果たしている医療機関として基幹インフラ制度の対象サイバー攻撃等への対応強化を図ることとする

・事業規模（病床数等）
・代替可能性（地域医療において果たす役割や医療提供能力等）
・地域性
・救急医療や災害拠点としての役割

指定する側の条件？

改正法施行時	改正法施行から３年度目までに
１地方（北海道、東北、関東、中部、近畿、中国、四国、九州・沖縄）**につき少なくとも１病院を指定**。	**各都道府県につき１病院指定**。ただし、地域性も考慮し、必要に応じて、複数病院を指定。

基幹インフラ事業者指定により想定される状況

国は、届け出られた計画書に係る特定重要設備が、我が国の外部から行われる妨害行為の手段として使用されるおそれが大きいと認めるときは、当該計画書を届け出た者に対し、妨害行為を防止するため必要な措置を講じた上で重要設備の導入等を行うこと等を勧告（命令）できる。

現時点で命令権者は事業所管大臣（厚生労働大臣）とされ、「必要な措置」がガイドラインではなく、行政機関からの「命令」として発出される可能性がある

電子カルテ情報共有サービス
全国の医療機関・薬局をつなぐオンライン資格確認等システムのネットワークを活用し、医療機関や薬局等との間で電子カルテ情報を共有する仕組み。

電子処方箋管理サービス
電子的に処方箋の運用を可能とする仕組み。この仕組みにより、薬の処方・調剤の際に、患者が直近で処方・調剤された内容の閲覧や、当該データを活用した重複投薬等チェックの結果確認が可能となる。

オンライン資格確認等システム
マイナンバーカードのICチップ等により、オンラインで資格情報の確認ができるシステム

侵害時の切断基準、再接続までのプロセスがさらに厳格化される可能性あり
⇒ただし、「確たる情報が出てこない」ことが厄介さを増す