経営者に必要な
サイバーセキュリティの2つの視点と8項目

2023年2月

事業名：医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初期対応支援・調査事業

委託事業者：一般社団法人ソフトウェア協会

【本日ご理解頂きたいこと】
経営者としての心構え

**たくさんの説明・用語が出てきます
まずはここから。
細かいところは今後の担当者や
ベンダーとのコミュニケーションに
ご活用ください。**

思考停止しない（困ったら相談する）

- サイバーセキュリティは継続的な課題。費用捻出の検討＋費用が無くてもできることを考える。

知らないではすまされない

- どのようなシステムや機器が入っているのか、全くわからないでは済まされない。相談役を持つ。任せる。

現場を混乱させず、決断は早く

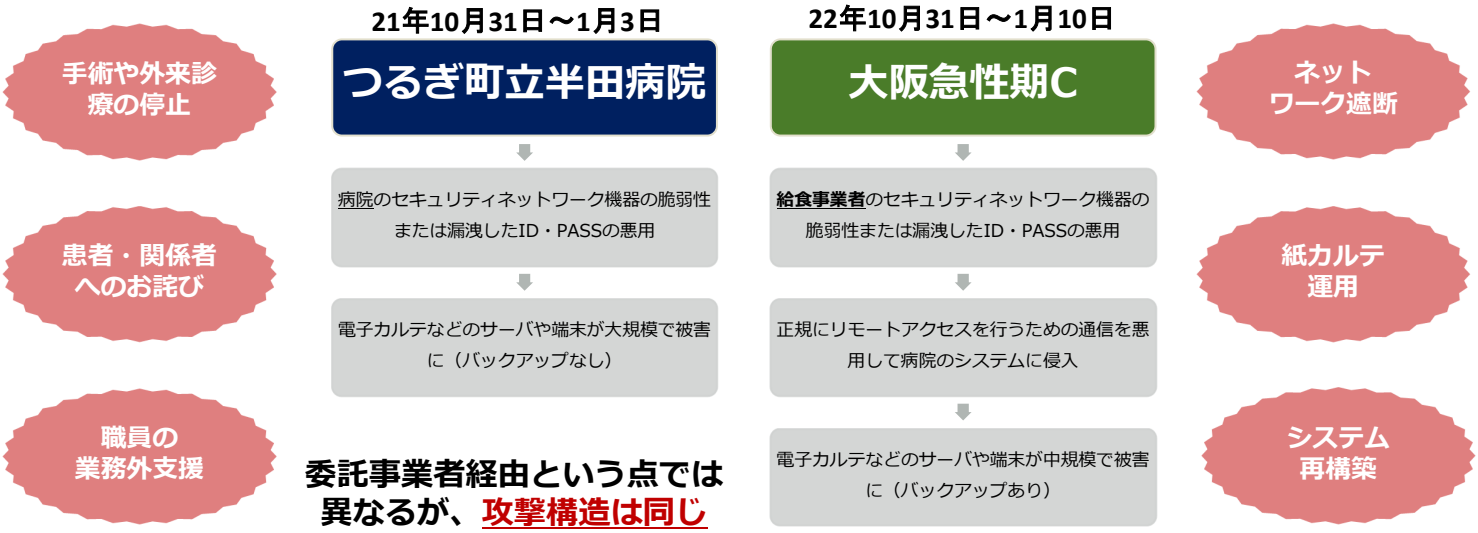
- 自分の発言によって現場の動き方も、作業も、患者の皆様の理解も変わることを理解する。決断を変えない。

システムやネットワークの責任もある

- いざというときに謝るの自分、説明責任は自分にある。

何が起きたのか？

直近で起きたインシデントの概要



委託事業者経由という点では異なるが、攻撃構造は同じ

サイバーセキュリティと病院の経営会計

病院の経営・会計

収入	支出
• 診療報酬（保険・自由） • その他（駐車場、学生実習協力費など）	• 人件費 • 医薬品診療材料費 • 設備費 • その他

病院の経営・会計（インシデントが起きると…）

収入	支出
~~診療報酬（保険・自由）~~ • ペナルティによる減額 ~~その他（駐車場、学生実習協力費など）~~	• 人件費 • 医薬品診療材料費 • 設備費（**追加設備**） • **対応・復旧費** • その他

給与支払いができない…？

２億円
つるぎ町立半田病院の新システム対応

意識の転換

- サイバーセキュリティインシデントは起きる
- 閉域網は存在しない
- 機器やシステムはネットワーク接続が前提
- オンラインバックアップは使えない可能性
- バックアップがあってもすぐには戻せない可能性
- 医療機器および周辺機器のソフトウェア更新は可能
- オンプレよりもクラウドの方が安全

最近の脅威は

情報セキュリティ10大脅威 2022（組織編）

1位：ランサムウェアによる被害

2位：標的型攻撃による機密情報の窃取

3位：サプライチェーンの弱点を悪用した攻撃

4位：テレワーク等のニューノーマルな働き方を狙った攻撃

5位：内部不正による情報漏洩

6位：脆弱性対策情報の公開に伴う悪用増加

7位：修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

8位：ビジネスメール詐欺による金銭被害

9位：予期せぬIT基盤の障害に伴う業務停止

10位：不注意による情報漏えい等の被害

（出典元：（独）情報処理推進機構）

ランサムウェア（感染・攻撃）とは
端末や端末の情報などを攻撃者によって暗号化（施錠）し、端末やデータを人質に金銭を要求する攻撃

- **データは基本的に元に戻すことはできない**
- **攻撃者との交渉は原則行わない**
- **感染しないための対策とデータのバックアップを取得**

大切なモノは「情報資産」

情報資産（医療に関わる情報を医療機関等の資産）とは

- 組織の価値あるまたは必要な情報
  - 例：患者情報、研究情報
- それらを記録している媒体
  - 例：パソコン、サーバ
- 情報を取り扱うその他の機器や設備など
  - 例：ネットワークプリンタ

用語を知る。脆弱性とは何か？

ハードウェア

- 私たちの体（骨や筋肉など）そのもの。
- 鍛えれば増強も可能だが、構造そのものを大きく変えるのは難しい。

ソフトウェア

- 私たちの脳、神経、思考、意識など、ハードウェアを動かすための機能。（代表的なソフトウェアとして、ソフトウェアを動作させる基本となるオペレーティングシステム（OS）がある。）
- 自分の考え方や興味などによって変化する。

脆弱性（ぜいじゃくせい）

- セキュリティホールやバグとも呼ばれる、ソフトウェアの不具合や設計ミスなどに起因して生じるソフトウェアの弱点。

マルウェア

- コンピュータウイルスとも呼ばれ、利用者の意図しない（不正かつ有害に）動作させるプログラムの総称。Malicious（悪意のある）＋Software（ソフトウェア）のが組み合わさった造語。

サイバーセキュリティは難しいのか？

人かシステムか？
医療よりも
難しくはない！？

医療		システム
医師の職業倫理		システム・セキュリティのポリシー
診察	（経過観察）	運用（ログなどを元に確認）
精密検査		専用の機器やツールを使った詳細調査
指導	手洗い・うがい・歯磨き	システム・ソフトウェアなどの脆弱性を無くす
	生活習慣改善	システム・ソフトウェアなどの使い方を見直す
	処方	セキュリティ対策ソフトの活用や追加 （新しいソフトウェア・パターンファイルへの更新、オプションやプラグインの利用）

システム利用の
基本はおさえる！

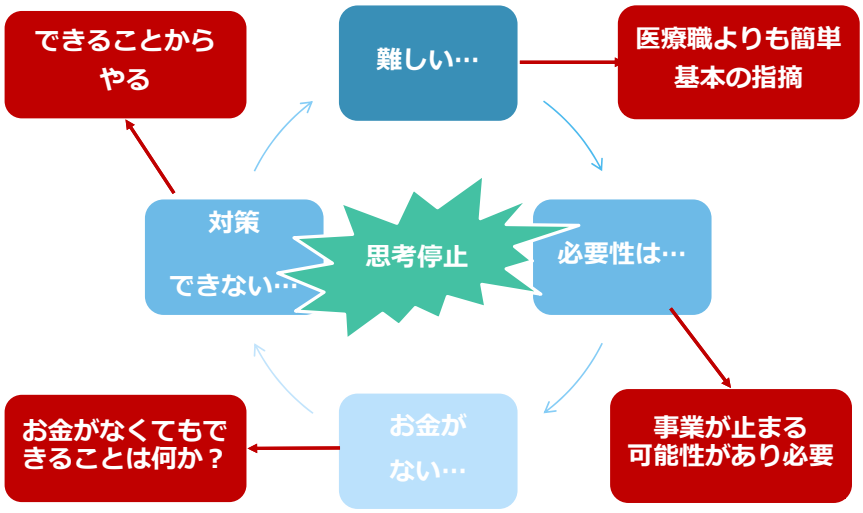
サイバーセキュリティは難しいのか？（参考）

医療		システム	経営者からのヒント・言葉
医師の職業倫理		システム・セキュリティのポリシー	現状はどうなっているのか教えてほしい。半田や急性期のようなことが起きない、起きても対応できる内容なのか？職員はこれを理解しているのか？
診察	（経過観察）	運用（ログなどを元に確認）	定期的に報告会をもとう。そこでは資産の状況について報告してほしい。事故の予兆とかは無いのか？
精密検査		専用の機器やツールを使った詳細調査	（調査対象があった場合）どのような調査を行う必要があるのか？費用はどれくらいかかるのか？
指導	手洗い・うがい・歯磨き	システム・ソフトウェアなどの脆弱性を無くす	今、院内のシステムや機器に脆弱性は無いのか？新しい脆弱性は見つかっていないのか？受容しないといけないリスクはあるのか？
	生活習慣改善	システム・ソフトウェアなどの使い方を見直す	今、使っている製品で更新したり、設定変更したりすることは無いのか？
	処方	セキュリティ対策ソフトの活用や追加 （新しいソフトウェア・パターンファイルへの更新、オプションやプラグインの利用）	資産は最大限利用しているのか？（最新のバージョンにして新しい機能をちゃんと使っているのか？）

経営者の思考と
サイバーセキュリティ

サイバーセキュリティの思考

繰り返される進まないループ（医療機関に限らず…）



お金がないから対策できないで済まされるか？

善管注意義務

- 行為者の階層、地位、職業に応じて要求される、社会通念上、客観的・一般的に要求される注意を払う義務

説明責任を果たす

- 半田病院や急性期Cのインシデントが発生したとして、自ら（患者、職員、他の医療機関、取引・委託先企業、業界団体、公的機関など）説明ができるか？

サイバーセキュリティを考えるための２つの視点

Emergency Readiness

（緊急事態への備え）

Incident Response

（事故対応）

緊急事態への備え

そもそもインシデントを起こさない組織にするために。

ないものはない。あるものはある。

直近で捻出するお金はないかもしれない…

「保守・運用」

保守・運用は何を指しているのか？

病院のシステムで使っているソフトウェアが古く、脆弱性もある…

サイバー攻撃によって、病院のシステムが使えなくなった…

これは健全に保守・運用されている状態と言えるのか？

ポイント１：現在の契約を見返し、確認、見直し

この「運用」という言葉にはセキュリティ運用も含まれているのだからちゃんとやって！！

→ ベンダーとの緊張関係をもたらし、警戒されかねない…

- システムを運用するためには、ソフトウェアの更新は必要だと思うが、どう思うか？
- 脆弱性を放置しておくことは安全なシステムと言えるのか？
- 今、ランサムウェア感染したら、当院はどうなるのか？
- 皆さんにとってのインシデントとは何ですか？

ポイント２：情報資産を把握する

院内の情報資産（機器・システム・ネットワーク・データ）を把握する。

- 電カル、部門、医療機器、全ての情報資産
- 委託先とのネットワーク接続や管理体制
- システムやデータの優先順位付けを行う

ポイント３：脆弱性のない環境を作る

皆さんは傷口を放置しません。では、システムの傷口（脆弱性）は？

OSのバージョン等の追加・変更・削除は機器の変更には当たらない

人の脆弱性（権限、甘いパスワード設定など）

システムや機器を入れているベンダーと他の病院と連携する

ポイント４：アクセスコントロール

組織内外の機器、システム、ネットワーク、データへの「アクセス」を制御する。

端末制限	接続制限	権限	セグメントの細分化
• ソフトウェアや設定変更を自由にできる権限を全員に持たせない	• 組織内外のネットワーク接続を制限する	• システム運用は管理者権限ではなく、ユーザ権限で	• セグメント（同じような属性を持つ固まり）をできる限り分けておく

ポイント５：オフラインバックアップ

直ぐに戻せる、バックアップを活かせる環境づくり。

オフラインでのバックアップ

電カル・部門システムのバックアップ

（優先的に取得させるシステムやデータの議論の必要性）

参照できる環境づくり・戻す練習

ポイント６：まずは目の前のことをやる。その先に…

ガイドラインに準拠するために…

どれくらいの資源が必要か？

どのくらいの時間を要するか？

どうやっても実現できないことは？

組織の対象外となる項目は？

何ができて、何ができないのか？

「医療情報システムの安全管理に関するガイドライン」

やるべきことから始める

（インシデントからの学び：VPN、バックアップ、サプライチェーン）

（どうしても難しい場合は他の医療機関などに相談してみる？）

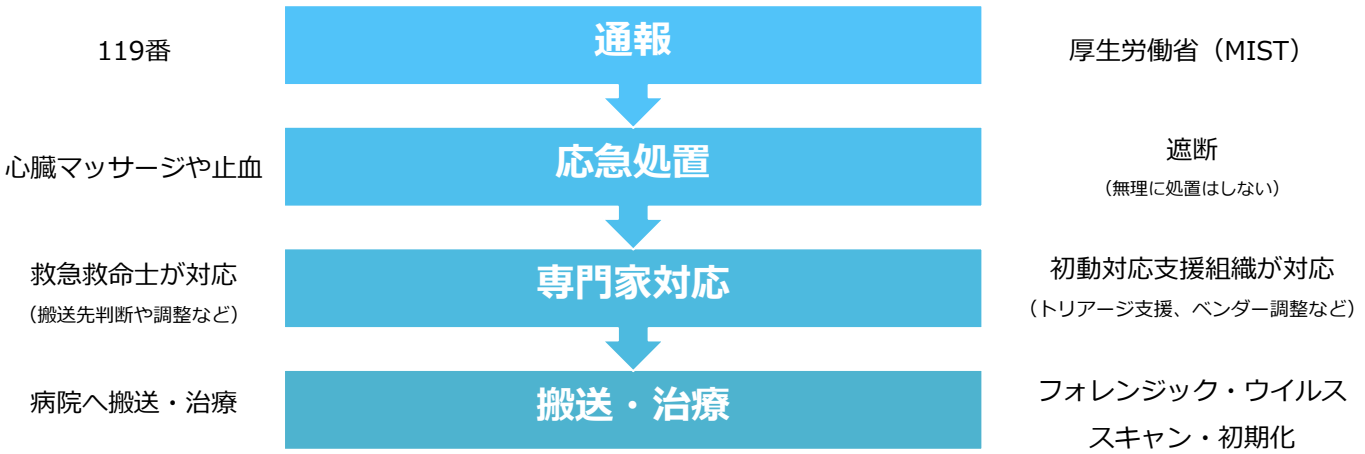
ポイント７：共有し合う。（→助け合いになる。）

- 対策状況
- 対応可否・難易度
- インシデント情報
- ベンダー情報
- 製品情報

インシデント対応

インシデントが起きても焦らない組織にするために。

インシデントが起きたらどうするのか？



厚生労働省に相談しましょう！

ポイント８：サイバーの「119番」

厚生労働省または「インシデントかも？」に即時通報

- 報告すると社会的なインパクトが大きくなる？
- 情報が勝手に公開され、必ず記者会見？
- インシデントを根掘り葉掘り調査される？
- 規模が小さいから関係ない？

https://mhlw-training.saj.or.jp/

２つの視点と８項目

【緊急事態への備え】

既存の契約を見直し、運用を見直す	情報資産の把握	脆弱性のない環境を作る	アクセスコントロール
オフラインバックアップ	まずは目の前のことをやる。その先に…	共有し合う	サイバーの119番を把握し、万が一は即通報

【事故対応】

プラスα

意識を変えないと同じ事が繰り返される

意識の転換

サイバーセキュリティインシデントは起きる

閉域網は存在しない

機器やシステムはネットワーク接続が前提

オンラインバックアップは使えない可能性

バックアップがあってもすぐには戻せない可能性

医療機器および周辺機器のソフトウェア更新は可能

オンプレよりもクラウドの方が安全

意識の転換

緊急連絡網や窓口の設置

限定的なオープンネットワークを作る

外部接続を把握、管理（申請制）

オフラインバックアップ

導入時に演習・シミュレーション

医療機器および周辺機器のソフトウェア更新を促進

管理しないオンプレか、管理されているクラウドか

（クラウドにも管理は必要）

残念ながら、明日インシデントが起きるかもしれません…

セキュリティの意識を持って頂き、継続して考えていきましょう！

（参考）ベンダーの言い訳に負けないために…

仕様です！

●サポートされたOSやネットワーク機器など、きちんと検証を行ってください。

薬機法の観点からソフトウェアの更新が行えません！

•薬生機審発１０２０第１号（平成 29 年１０月２０日）「医療機器プログラムの一部変更に伴う軽微変更手続き等の取扱いについて」
https://www.jaame.or.jp/mdsi/pdf/other/291020kiki102001.pdf?fbclid=IwAR081ytXZLMOWsQB4y_6PmxBa5vKGTonkiv0aBd7vHR7INOA5E_4WU96JFs

•一部変更承認申請及び軽微変更届のいずれの手続きも要さない事例
（①動作環境である OS バージョン等の追加・変更・削除。②動作環境として用いるデータベース等のバージョンの追加・変更）

検証するためには費用が必要です！

•当院だけの話でしょうか。ベンダーとしての姿勢は？

接続先（ベンダーのデータセンター等）の情報は開示できません！

•秘密保持契約があるにもかかわらず（なければ結んでも）開示できないのはなぜか。信頼できない接続であれば、病院としての統制が取れないため、他社製品の検討も？

契約にありません！

•現状の契約を確認します。貴社の運用というのはどの範囲を差しているのか。もし、別の契約が必要であればベンダーの説明責任を果たして、提案してほしい。

脅威が増加しているから、新しいセキュリティ製品を入れませしょう！

•まず、今の導入している製品で出来ないことは無いのか？まずは運用の範囲でそちらを提案してほしい。