事　務　連　絡
令和 5 年 8 月 25 日

地区歯科医師会　御中

公益社団法人東京都歯科医師会

医療機関におけるサイバーセキュリティ対策について
（厚生労働省委託オンライン研修のご案内）

時下、ますますご清栄のこととお喜び申し上げます。また、平素より本会会務運営にご理解ご協力を賜り厚く御礼申し上げます。

さて、標記につきまして、日本歯科医師会より別添の情報提供がありましたので、お知らせ致します。サイバーセキュリティに関しましては、本会からの事務連絡(R5.7.7 付)「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等について」にて、同名の日歯事務連絡(R5.6.14 付)を各地区歯科医師会へ転送・配信いたしました。

今般、厚生労働省の委託事業により、一般社団法人ソフトウェア協会が「『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』に基づいた立ち入り検査に備える研修」(オンライン形式、開催日①R5/9/13、②R5/9/27、研修名「導入研修－立入検査対策コース－」、申込受付中、無料)を開催しますので、ご活用をご検討の程よろしくお願い申し上げます。また、同協会では、これに関連する他の研修も予定されています。参考資料を追加添付いたしますので、併せてご高覧ください。

ご多忙のところ誠に恐縮ですが、貴会会員への周知方につきまして、ご協力の程よろしくお願い申し上げます。

(別添)
１．「医療機関におけるサイバーセキュリティ対策について」
日本歯科医師会　事務連絡・R5.8.18 付

(参考資料、都歯追加添付)
参考１．医療分野のサイバーセキュリティ対策について　厚生労働省 HP
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html
参考２．医療機関向けセキュリティ教育支援ポータルサイト　ソフトウェア協会 HP
https://mhlw-training.saj.or.jp/
参考３．研修内容　導入研修－立入検査対策コース－　他　ソフトウェア協会 HP
https://mhlw-training.saj.or.jp/training/#1
参考４．R4 年度サイバーセキュリティ研修資料「サイバーセキュリティは難しい？」
医療従事者初学者向け　ソフトウェア協会

※なお、ソフトウェア協会 HP「よくある質問 (FAQ)」によると、全オンライン研修終了後にアーカイブ配信を予定(Q3)、アーカイブ配信時に研修資料を掲載予定(Q8)とのことです。
https://mhlw-training.saj.or.jp/contact-us/

〔担当〕
公益社団法人東京都歯科医師会
事業部　医療管理・調査担当　鈴木・正岡
TEL：03-3262-1149（直通）　FAX：03-3262-4199

別添１

事　務　連　絡
令和５年８月18日
（情報管理課扱い／メール）

都道府県歯科医師会　御中

公益社団法人　日本歯科医師会

医療機関におけるサイバーセキュリティ対策について

平素は格別のご高配を賜り、厚く御礼申し上げます。

先般、厚労省が作成した「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」について情報提供（事務連絡・令和５年６月14日／情報管理課扱い）させていただいたところですが、以下、同省が開設している「医療機関向けセキュリティ教育支援ポータルサイト」において**医療機関向けのサイバーセキュリティ対策チェックリストに基づいた立ち入り検査に備える研修**が実施される予定となっておりますので、情報提供いたします。

引き続き、会員診療所が契約しているシステム事業者と連携の上、日頃よりサイバーセキュリティ対策を心掛けていただくよう、貴会会員への周知にご協力をお願いいたします。

【医療機関向け】セキュリティ教育支援ポータルサイト
https://mhlw-training.saj.or.jp/

○導入研修－立入検査対策コース－　※申込を開始しています
https://mhlw-training.saj.or.jp/info-20230810-2/
（提供内容）「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」に基づいた立ち入り検査に備える研修
（実施方法）オンライン開催
（受講料）無料
（受講対象）医療機関と保健所関係者
（実施時期）第１回：2023年９月13日（水）16時～18時
※９月７日（木）13時締切
第２回：2023年９月27日（水）16時～18時
※９月21日（木）13時締切
※第１回と第２回は、ほぼ同じ内容になります。

（参考）厚生労働省 医療分野のサイバーセキュリティ対策
医療分野のサイバーセキュリティ対策について｜厚生労働省（mhlw.go.jp）

参考１

医療分野のサイバーセキュリティ対策について

医療機関等がサイバー攻撃を受けた際の厚生労働省連絡先　規程等　研修等

過去事業

医療機関等がサイバー攻撃を受けた際の厚生労働省連絡先

「医療情報システムの安全管理に関するガイドライン」では、医療機関等がサイバー攻撃を受けた（疑い含む）場合等の際には、厚生労働省等の所管省庁への連絡等、必要な対応を行うほか、そのための体制を整備する必要があることを示しています。

医療機関等がサイバー攻撃を受けた場合の厚生労働省連絡先

医政局特定医薬品開発支援・医療情報担当参事官室
TEL:　03-6812-7837
MAIL:　igishitsu×mhlw.go.jp
※迷惑メール防止のため、メールアドレスの一部を変えています。
「×」を「@」に置き換えてください。

規程等

医療法施行規則の一部を改正する省令について（令和５年３月10日）

令和５年３月10日に、医療法施行規則の一部を改正する省令（令和５年厚生労働省令第20号。）が公布され、令和５年４月１日施行されました。 医療法施行規則の一部を改正する省令について［148KB］

医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）（令和４年11月10日）

医療機関のサイバーセキュリティ対策について、自治体を通じて医療機関等へ注意喚起しております。

1．サプライチェーンリスク全体の確認
2．リスク低減のための措置
3．インシデントの早期検知
4．インシデント発生時の適切な対処・回復
5．金銭の支払いに対する対応
6．ランサムウェア特設ページ

医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）（令和４年11月10日）［4.5 MB］

医療情報システムの安全管理に関するガイドライン

個人情報保護に資する情報システムの運用管理とe-文書法への適切な対応を行うためのガイドラインです。
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（令和5年5月）　関係資料一式
「医療情報システムの安全管理に関するガイドライン」とは

関連ガイドライン
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

研修等

医療機関向けサイバーセキュリティ対策研修等について

厚生労働省は、「医療機関向けセキュリティ教育支援ポータルサイト」（MIST：**M**edical **I**nformation **S**ecurity **T**raining）を開設し、医療機関の更なるサイバーセキュリティ対策の強化を図ることを目的に、

・医療機関の経営層や医療従事者など階層別のサイバーセキュリティ対策研修の実施
・医療機関内でのサイバーセキュリティ教育に活用できるコンテンツ集の掲載
・サイバーセキュリティインシデント発生時の相談・初動対応依頼窓口の設置

をしています。

研修のお申し込み、研修内容やスケジュール等については、以下リンク先よりご覧下さい
https://mhlw-training.saj.or.jp/

本ページに関するお問い合わせ先

医政局特定医薬品開発支援・医療情報担当参事官室

TEL:03-6812-7837

参考２

医療機関向け セキュリティ教育支援ポータルサイト

Medical Information Security Training (MIST)

厚生労働省
厚生労働省委託事業

お知らせ

2023年8月14日
よくある質問（FAQ）について

2023年8月10日
導入研修－立入検査対策コース－申込開始

2023年8月10日
令和5年度のオンライン研修について

2023年5月11日
令和5年度医療情報セキュリティ研修について

本サイトの使い方

本サイトは医療機関の方がサイバーセキュリティに関する研修情報を収集または受講申し込みなどができるサイトです。またインシデント発生時の通報などにもご利用いただけます。

サイバーセキュリティ研修

医療機関に向けたサイバーセキュリティに関するオンライン教育教材をご提供しています。
経営者向け、システム・セキュリティ管理者向け、初学者（職員）向けのオンライン研修やe-learningを用いたカリキュラムをご用意しています。これらの教材は期間中何度でもご受講いただくことができます。

医療機関向けサイバーセキュリティ研修はこちら

インシデントが発生した際の初動対応支援

ランサムウェアに感染してシステムに影響が出た、Webサイトが改ざんされたなどのインシデントが発生した際、初動対応をご支援できる窓口をご用意しています。また、インシデントによってはオンラインまたは現地訪問を行ってご支援する体制をご用意しています。

インシデント発生時のご連絡はこちら

一般社団法人 ソフトウェア協会

厚生労働省委託事業
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

事業について　お問い合わせ　プライバシーポリシー

- Medical Information Security Training -

参考３

医療機関向け

セキュリティ教育支援ポータルサイト

Medical Information Security Training (MIST)

厚生労働省
厚生労働省委託事業

研修内容

導入研修 経営者向け システム・セキュリティ管理者向け 初学者・医療従事者向け

導入研修－立入検査対策コース－

提供内容	「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」に基づいた立ち入り検査に備える研修です。
実施方法	オンライン開催 ※研修資料の事前配布はございません。
実施時期	【第1回】2023年9月13日（水）16時～18時　9月07日（木）13時締切 【第2回】2023年9月27日（水）16時～18時　9月21日（木）13時締切 ※第1回と第2回は、ほぼ同じ内容になります。
受講料	無料
受講対象	医療機関と保健所関係者

※研修の内容は予告なく変更する場合があります。
※受講申し込みは、1名ずつ申し込みとなります。
※1組織あたりの受講回数に制限はございません。

第1回　9/13(水) 研修申し込み

第2回　9/27(水) 研修申し込み

経営者向け研修

提供内容	つるぎ町立半田病院、大阪府立病院機構、大阪急性期・総合医療センター等のインシデント事例を基に経営者として必要なサイバーセキュリティの意識と知識について学習します。
実施方法	オンライン開催 ※研修資料の事前配布はございません。
実施時期	8月下旬から9月に申し込みを開始いたします。 ※各回共通の内容ですので、いずれかの回にご参加ください。 【第1回】2023年10月10日（火）16時～17時 【第2回】2023年11月14日（火）16時～17時 【第3回】2023年12月20日（水）17時～18時 【第4回】2024年01月16日（火）16時～17時 【第5回】2023年02月06日（火）16時～17時
受講料	無料
受講対象	医療機関等の経営に携わる方

※研修の内容は予告なく変更する場合があります。
※受講申し込みは、1名ずつ申し込みとなります。
※1組織あたりの受講回数に制限はございません。

システム・セキュリティ管理者向け研修

提供内容	現在あるIT資産を活用したセキュリティ対策について学習します。 （Active Directory(AD)入門、認証・許可や特権管理の重要など。）
実施方法	オンライン
実施時期	8月下旬から9月に申し込み開始いたします。 ※本研修は、計7回で構成されております。各回の内容が異なります。 できる限りすべての回にご参加いただき、技術的な点を学習します。 【第1回】2023年10月19日（木）16時～17時　「IT環境における組織の管理」 【第2回】2023年10月26日（木）16時～17時　「資産へのアクセス制御」 【第3回】2023年11月02日（木）16時～17時　「攻撃に強い環境構築」 【第4回】2023年11月16日（木）16時～17時　「セキュリティの自動化」 【第5回】2023年11月30日（木）16時～17時（予定）　「Group Policyの設定解説」 【第6回】2023年12月07日（木）16時～17時（予定）　「脆弱な医療機器の保護方法」 【第7回】2023年12月21日（木）16時～17時（予定）　「インシデントに備えた体制確立」 一部参加が難しい場合は、アーカイブ配信を予定しておりますので、後日ご視聴ください。
受講料	無料
受講対象	医療機関等のシステム・セキュリティ管理する方

※研修の内容は、予告なく変更する場合があります。
※受講申し込みは、1名ずつ申し込みとなります。
※1組織あたりの受講回数に制限はございません。

初学者・医療従事者向け研修

提供内容	サイバーセキュリティインシデントが身近であることを認識いただくとともに、システムや端末を使うにあたって、自分達で今すぐできる備えなどについて学習します。
実施方法	オンライン ※研修資料の事前配布はございません。
実施時期	8月下旬から9月に申し込みを開始いたします。 ※各回共通の内容ですので、いずれかの回にご参加ください。 【第1回】2023年10月11日（水）16時～17時 【第2回】2023年10月25日（水）16時～17時 【第3回】2023年11月08日（水）16時～17時 【第4回】調整中　2023年11月下旬実施予定 【第5回】2023年12月06日（水）16時～17時 【第6回】2023年12月12日（火）17時～18時 【第7回】2024年01月23日（火）16時～17時 【第8回】2024年01月30日（火）16時～17時
受講料	無料
受講対象	サイバーセキュリティの基礎知識を習得したい方

※研修の内容は、予告なく変更する場合があります。
※受講申し込みは、1名ずつ申し込みとなります。
※1組織あたりの受講回数に制限はございません。

一般社団法人 ソフトウェア協会
厚生労働省委託事業
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

サイバーセキュリティは難しい？

～自分たちでできる対策と組織を守るための意識～

令和４年度厚生労働省セキュリティ研修事業

医療従事者・初学者向けコンテンツ

（作成：一般社団法人ソフトウェア協会）

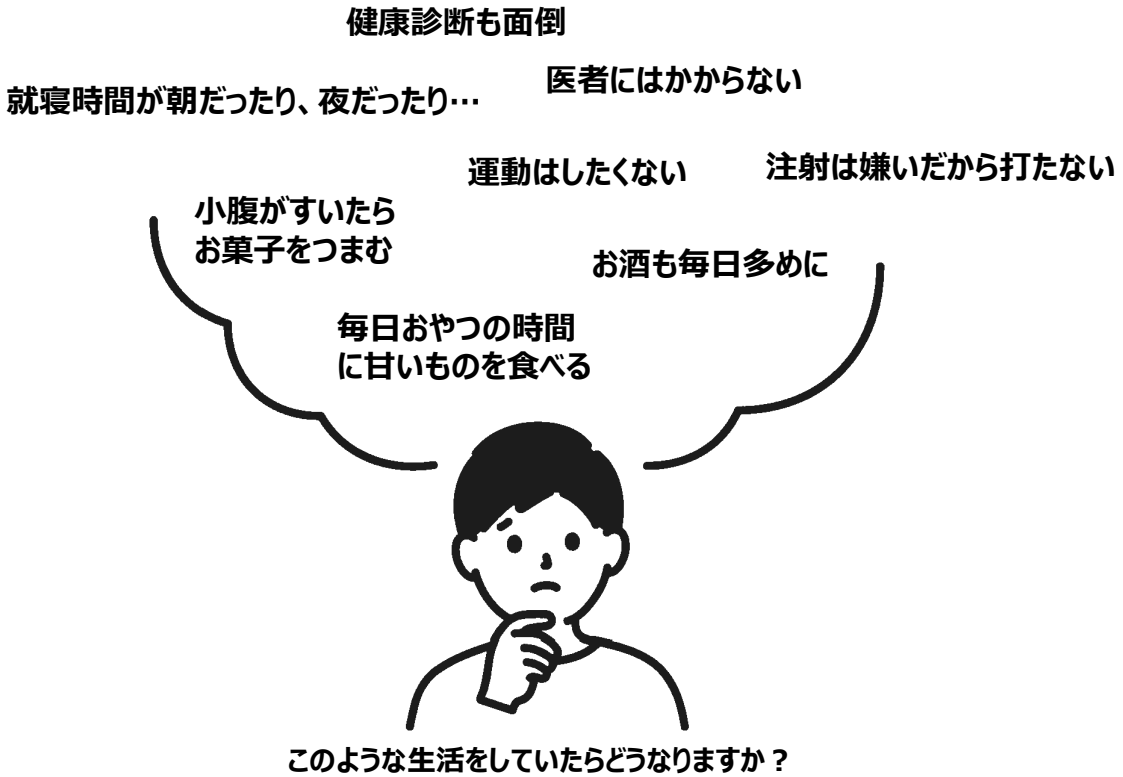
1

議題

- ✓サイバーセキュリティは難しいの？
- ✓サイバー攻撃の現状
- ✓サイバー攻撃への対策
- ✓医療業界独自の課題？
- ✓全体で意識改革！
- ✓さいごに

2

サイバーセキュリティは難しいの？



このような生活をしていたらどうなりますか？

アプリケーション入れたい放題

どこのWi-Fiでも使ってインターネットを使う

便利なツールはたくさん使う

どのようなサイトでも閲覧できる

USBは差し放題

セキュリティ対策は導入しない

ソフトウェアは更新しない

このような使い方をしていたらどうなりますか？

日々のメンテナンスが大切

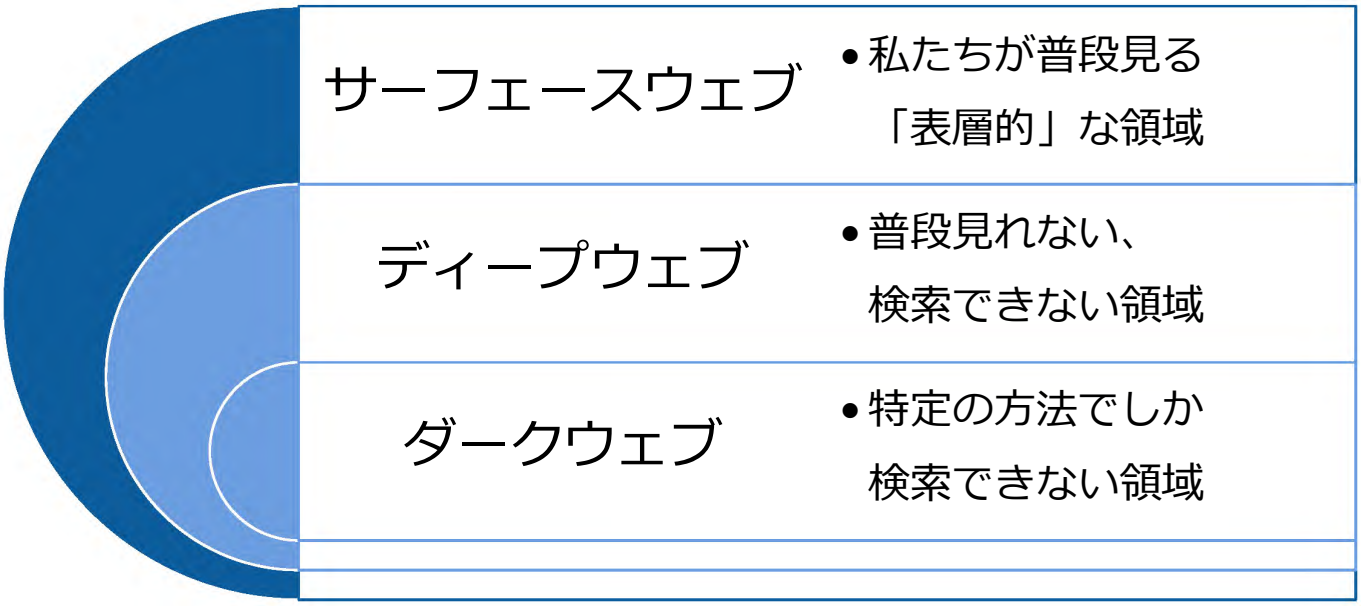
何気なく使っている
インターネットやスマートフォンなどの世界

ネットワーク？インターネット？

ネットワーク

インターネット

普段使うインターネットの世界



サイバー攻撃の現状

サイバー攻撃の目的は・・・

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」

用語を知る。脆弱性とは何か？

まずは、ハードウェアとソフトウェアとは？

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ションシステム（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。

マルウェア感染の拡大とステージ（独自）

ステージ	がん	マルウェア
ステージ０	がん細胞が上皮細胞内に留まる。	セキュリティ対策ソフトによる注意の通知。（右下に出るポップアップ）
ステージⅠ	がん細胞は筋肉層で留まる。	セキュリティ対策ソフトによる検出（隔離や駆除）が行われている。
ステージⅡ	がん細胞が筋肉層を越え、リンパ節への転移の可能性も。	普段と違う挙動があり、セキュリティ対策ソフトでも検出されていない。他端末への感染可能性。
ステージⅢ	がん細胞が浸潤。リンパ節の転移もある。	マルウェアが一部環境で感染している。（データのバックアップは存在する。）
ステージⅣ	原発巣を越えて、他の臓器への転移。	マルウェアが端末やサーバなど広域に感染している。（データのバックアップが存在しない。）

直近で起きたインシデントの概要

つるぎ町立半田病院

病院のセキュリティネットワーク機器の脆弱性または漏洩したID・PASSの悪用

電子カルテなどのサーバや端末が大規模で被害に（バックアップなし）

ステージⅣ

大阪急性期C

給食事業者のセキュリティネットワーク機器の脆弱性または漏洩したID・PASSの悪用

正規にリモートアクセスを行うための通信を悪用して病院のシステムに侵入

電子カルテなどのサーバや端末が中規模で被害に（バックアップあり）

ステージⅢ

委託事業者経由という点では異なるが、攻撃構造は同じ

対策につながる共通点

- 脆弱性があると攻撃される可能性が高まる
- 漏洩した情報は悪用される
- 他の端末につながらないようにする
- ランサムウェアに感染したデータは返ってこない
- オフラインのデータバックアップが必要

サイバー攻撃への対策

皆さんの身の回りの安全管理策は？

鍵をかける	金庫などの厳重保管	マスクをする
体温を測る	予防接種	絆創膏

皆さんの身の回りの安全管理策と同じ？

実施してほしい対策①

パスフレーズ

- パスワードは複雑性でも、変更回数ではなく、いかに長くするか。（パスフレーズ）
- 安易なパスワードにしない　＋　漏洩していないパスワード

バックアップ

- USBなどの外部記憶媒体を使ってデータを保存する。
- クラウド（インターネット上で）のデータを保存する。

実施してほしい対策②

フィルタリング

- URL（Web）フィルタリングを使って、怪しいサイトには近づかないようにする。
- 迷惑メールフィルタリング機能などを使って、余計なメールは開封しないようにする。

検出状況の確認

- セキュリティ対策ソフトのログを見てみる。
- （設定を確認してみましょう。できる限り強い設定にする。）

実施してほしい対策③

セキュリティ対策のアップデート

- 製品のバージョン、検索エンジン、パターン（定義）ファイルが更新できているか確認する。

パッチを適用する

- 使っている全てのソフトウェアのバージョンを確認して、更新プログラム、パッチを適用する。

サイバー攻撃の侵入経路を考える

メール

ネットワーク
（Web）

外部記録媒体
（USB・スマホ）

脆弱性

使用上の注意点

メール	インターネット
• 添付ファイルや文章内のリンクは安易に開かない。 • 差出人の情報、メールアドレスなども正しいか確認する。 • 変な文章や書体になっていないかメールを確認する。 • （どうしても気になる場合）メール記載の連絡先ではなく、名刺やWeb検索するなど、他の方法連絡先を確認して連絡する	• 関係ないサイトには近づかない • 業務などでよく使うサイトは登録しておく。（ブックマークする。） • WebサイトのURLを確認する • ログインするサービスの場合、特にパスフレーズを使いできる限り長く設定する。

使用上の注意点

外部記憶媒体	脆弱性
• むやみに持ち込まない、差さない。 • やむを得ず使用しなければならない場合は、セキュリティ対策つきのUSBを使う。 • 接続前に最新の製品や検索エンジン、パターンファイルのバージョンで、セキュリティ対策ソフトでの検索を行う。 • USB以外にも読み込める外部記憶媒体に注意。（DVD、スマートフォンなど）	• サポートされているソフトウェアを利用する。 • 最新のバージョンの製品を利用する。 • 公開されているパッチを適用する。 • 出来る限り情報収集する。

医療業界独自の課題？

古いOSの端末

●古いOSのまま端末を
利用しているのですが、
問題ないですか？

製品	販売日（日本語版）	メインサポート終了	延長サポート終了
Windows 2000	1999/12/24	2005/06/30	2010/07/13
Windows XP	2001/09/06	2009/04/14	2014/04/08
Windows Vista	2006/11/30	2012/04/10	2017/04/11
Windows 7	2009/09/01	2015/01/13	2020/01/14
Windows 8 Windows 8.1	2012/08/16 2013/08/27	2018/01/09	2023/01/10
Windows 2000 Server	2000/02/18	2005/06/30	2010/07/13
Windows Server 2003 Windows Server 2003 R2	2003/06/25 2006/02/03	2010/07/13	2015/07/14
Windows Server 2008 Windows Server 2008 R2	2008/02/05 2009/09/01	2015/01/13	2020/01/14
Windows Server 2012 Windows Server 2012 R2	2012/09/05 2013/10/17	2018/10/9	2023/10/10
Windows Server 2016	2016/10/01	2022/01/11	2027/01/12

変化の必要性

皆さんはそれぞれの年
何をしていましたか？

半田病院の事例で言うと…

Windows7の利用 → 2009年９月１日に一般リリース

電カルのために必要な「Internet Explorer７」との互換性 → 2006年10月18日（日本版は11月2日）に公開

ActiveX使用前提のアプリ → ActiveXは1996年にリリースされたインターネットの関連技術。
悪用が顕著になったのは2000年代前半位から・・・

端末やUSBは持ち込める？

●外から違う端末やUSBなどが持ち込まれたら、嫌ではないですか？

権限がある人が自由？

全体で意識改革！

発想を変える必要性

- サイバーセキュリティインシデントは起きてしまう
- コンピュータ機器を使うこと＝開かれた世界で機器や仕組みを使っている（閉域網はない）
- インターネット接続前提の機器・ソフトウェア構造
- 繋がっているとバックアップにならない・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（自分達で保有する）よりもレンタルサーバやクラウドの方が安全

さいごに

サイバーセキュリティは難しいのか？

セキュリティは本当はシンプルです。技術用語に惑わされない。

手洗いうがい（日常生活での注意）

- 最新（またはサポート内）のソフトウェア（OSやアプリなど）を使用し、脆弱性（ぜいじゃくせい）が無い状態を作る。
- セキュリティ対策製品を導入する。
- パスワード（パスフレーズ）は類推されにくく、出来る限り長いものを使う。

予防接種を受ける

- セキュリティ対策ソフトのパターン（定義）ファイルを更新する。

健康診断

- セキュリティ対策ソフトでフルスキャン（全ファイルのスキャン）を行う。

病院へ行く

- 駆け付けの病院・連絡先を確認しておく。

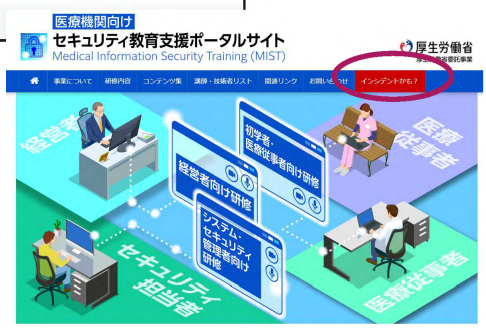
薬をもらう

- セキュリティ製品の更新や新たな設定や新しい技術の利用。

何かあったら・・・

まずはサイバーの「119番」に通報しよう！

- 職員の方は情報システム担当者や責任者に連絡
- 情報システム責任者や担当者の方は、厚生労働省に連絡、または「インシデントかも？」に即時通報



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

Fin.

本事業に関するお問い合わせ：厚生労働省医政局 特定医薬品開発支援・医療情報担当参事官室

ポータルサイトやコンテンツに関するお問い合わせ：HTTPS://MHLW-TRAINING.SAJ.OR.JP/