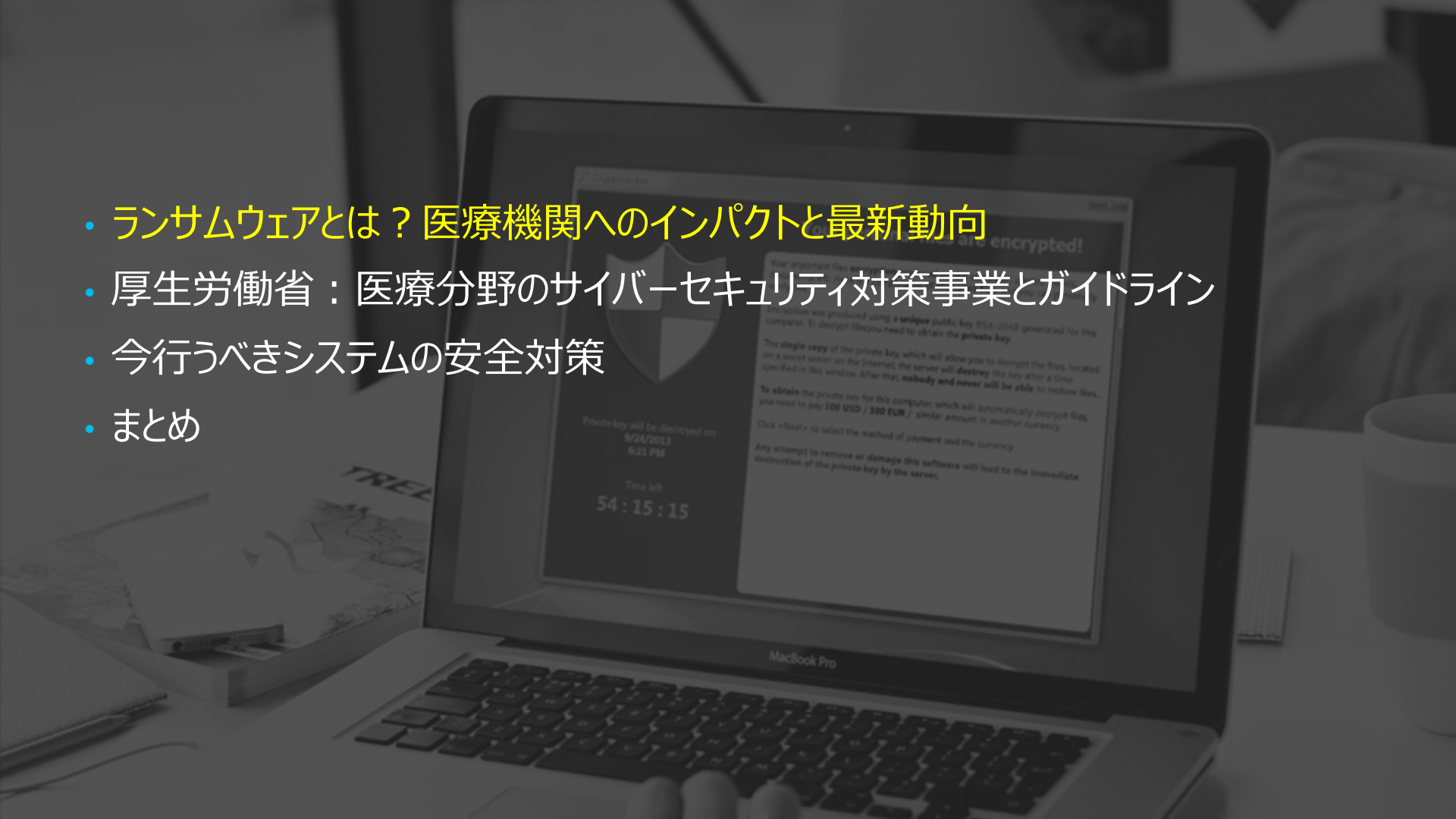
Cisco オンラインセミナー

医療機関向け『ランサムウェア対策』セミナー

医療機関向けランサムウェア動向と 今行うべき安全対策 総まとめ

シスコシステムズ合同会社　セキュリティ事業
アーキテクト / エバンジェリスト　木村滋

2022/02/15

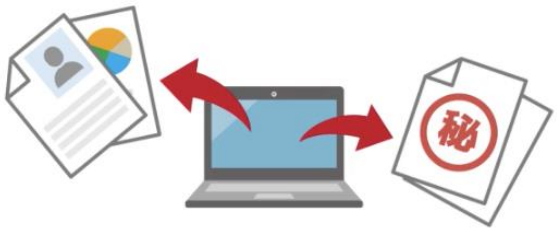


- ランサムウェアとは？医療機関へのインパクトと最新動向
- 厚生労働省：医療分野のサイバーセキュリティ対策事業とガイドライン
- 今行うべきシステムの安全対策
- まとめ

セキュリティの重要性

電子カルテ，診療予約システム等のITシステムの利用増加に伴い，
セキュリティリスクも増加，システムへの侵害で起こること

重要情報の漏洩



患者情報を保存した
USBメモリを紛失した

重要情報の改ざん

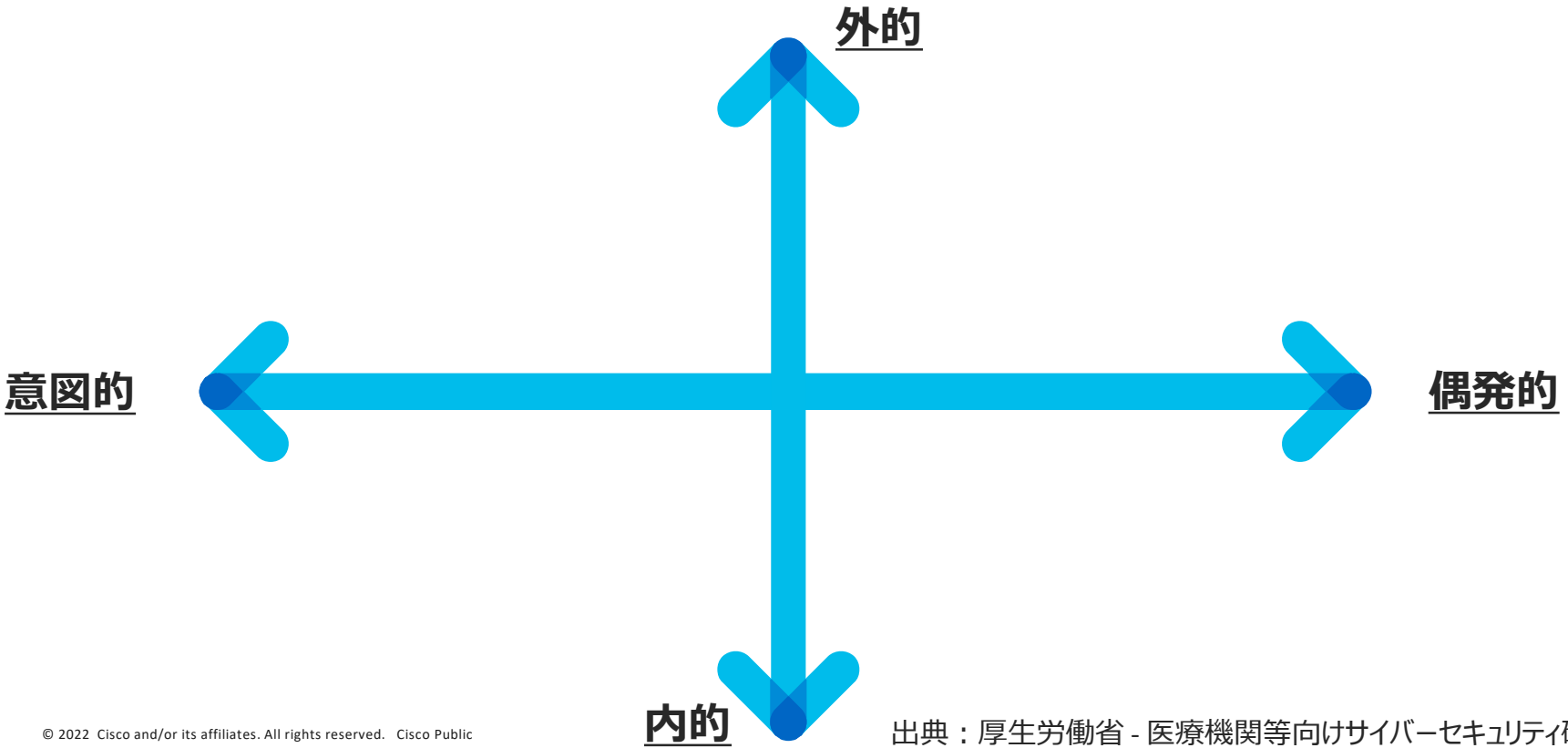
データベース上の患者
情報を改ざんされた

システムの停止

電子カルテのシステムが
急に使えなくなった

出典：厚生労働省 - 医療機関等向けサイバーセキュリティ研修
https://www.youtube.com/watch?v=I_udMT26DeE

セキュリティ事故はなぜ起こる？



出典：厚生労働省 - 医療機関等向けサイバーセキュリティ研修
https://www.youtube.com/watch?v=I_udMT26DeE

セキュリティ事故はなぜ起こる？

外的

外部からの攻撃

- **フィッシングメールによる感染・情報漏えい**
- **外部からのシステムへの脆弱性利用**
  - **リモートアクセスVPN**
  - **VDI**
  - **保守用サーバ**
  - **院内無線LAN**
- **物理アクセス, USBからの感染**
- **感染の拡大 (ラテラルムーブメント)**

外部から攻撃を許してしまう原因

- システムの脆弱性
- ネットワーク的アクセスコントロール
- 物理的アクセスコントロール
- ポリシーの明確化
- スタッフの責任範囲の明確化
- 行動規範の厳格化
- その他 …

意図的

偶発的

委託先事業者
のミスオペ

組織内職員
の不正・内部犯行

組織内職員
のミスオペ

内的

ランサムウェア (Ransomware) とは？

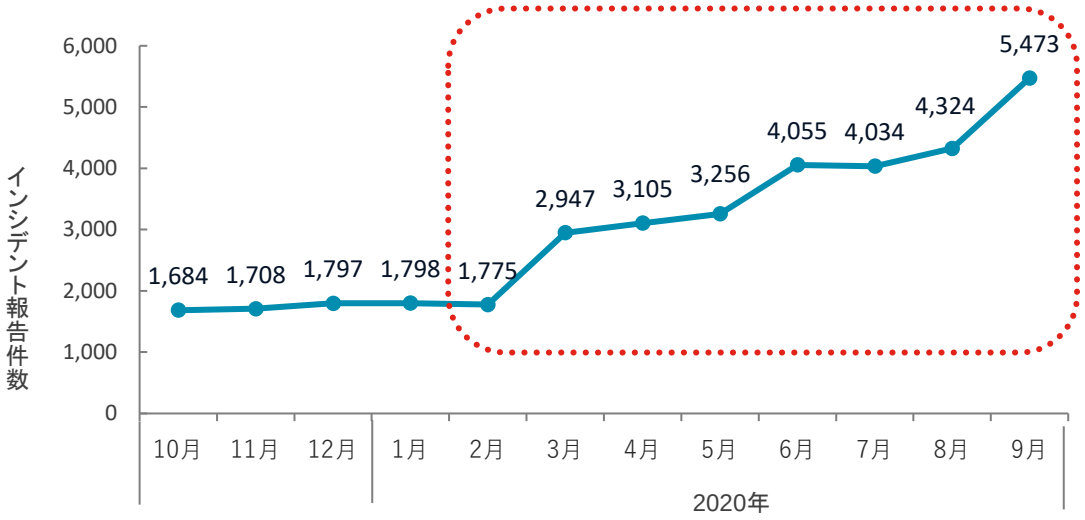
悪意のあるプログラムの総称：マルウェア

ウィルス	プログラムの一部を改ざんして、増殖するプログラムユーザーに害を与えるプログラムの総称
ワーム	自己増殖型であり自分自身を複製して、他へ感染動を行うプログラム
キーロガー	パソコンやキーボードの操作の内容を記録するプログラム
スパイウェア	ユーザーの個人情報や行動を収集し別の場所に送るプログラム
トロイの木馬	有用なプログラムに見せかけた悪意のあるプログラム（バックドア）で、兵士が中に入った木馬をトロイアの街に招き入れ壊滅した手口（ギリシャ神話）
ランサムウェア	データの利用制限（暗号化・使用不可）を行いその制限を解除するため、もしくは搾取された機密情報を公開しないために身代金（Ransom）を要求するマルウェア
クライムウェア	クライム（Crime：犯罪）ウェアは犯罪を目的として作られたプログラムの総称技術的な知識を持たない人でも使え、クライムウェアキットも流通している

WannaCry
ワーム型ランサムウェア

現状：ランサムウェアと脅威の拡大

コロナ影響 / テレワーク普及時期からセキュリティ事故が急増



出典：JPCERT/CC インシデント報告対応レポート[2020年7月1日～2020年9月30日]

急増するランサムウェア被害
Cisco Talos 最新四半期レポート

ランサムウェアの脅威観測が激拡大

- 観測脅威全体の **46%** がランサムウェア
- 攻撃対象：業種を問わない

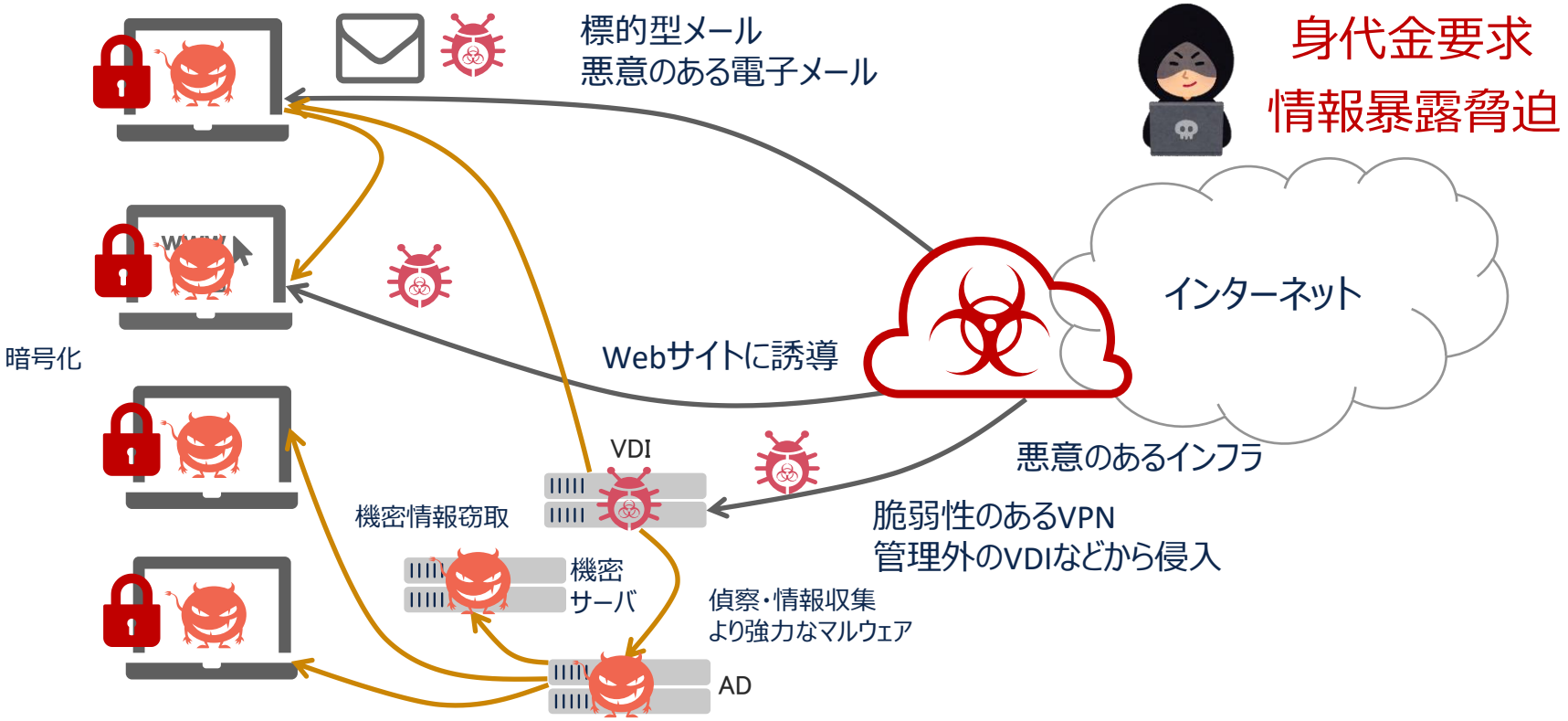
  運輸, 公益, **医療**, 政府, 通信, テクノロジー, 機械, 化学品流通, 製造, 教育, 不動産, 農業
- 攻撃対象：3四半期連続医療No1
- 医療系資産の注目度と価値上昇
- 新型コロナウィルスの影響による

ITセキュリティ/ランサムウェア対策が 医療業務 継続性 に重大なインパクトを与え得る

https://gblogs.cisco.com/jp/2021/11/talos-quarterly-report-incident-response-2/

ランサムウェア攻撃のプロセス

ラテラルムーブメントによってサイバー攻撃の被害が大きくなる



1.侵入開始・初期感染

2.偵察行動・感染拡大

3.実行・被害

最近のランサムウェア (Ransomware) の特徴

ランサム被害にあったら何が起こる？ :「二重脅迫 & 標的型ランサムウェア」

1. 内部の1端末の感染を手がかりに重要システムを奪取 (ドメインコントローラ等)
2. 感染システム全体の端末からファイルを盗み出す
3. 感染端末全体のファイルを暗号化
4. 利用できないシステムの復旧に対する身代金を要求
5. 復旧のための身代金を拒んだ場合、漏洩サイトで盗んだファイルの漏洩に対する身代金を再要求

※ 個々のユーザにランサムウェアファイルを感染させるでなく、標的型攻撃と同様な手法で組織全体を狙う

ランサムウェアを利用したビジネスが確立

- Ransomware as a Service : RaaS
- ランサムウェアアクターがランサムウェア利用者向けにインフラを開放し利用料を得る, テクニカルサポート, 標的型攻撃のガイド, トレーニング環境, 被害者とのコミュニケーションポータルを提供している

ランサムウェアは種別が存在, 常にアップデート

- 近年上位のランサムウェアファミリー : REvil, Conti, WastedLocker, Darkside, Zeppelin, Ryuk, Mount Locker, Avaddon
  - **最新Microsoft 脆弱性, 商用ソフトウェア脆弱性等を細かく機能としてアップデートを行っている**

ランサムウェア (Ransomware) の影響

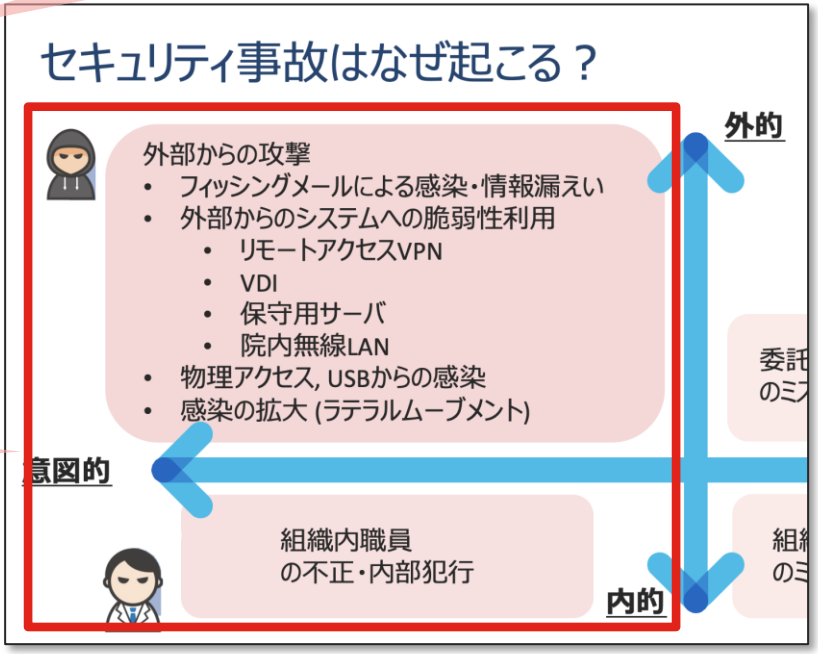
セキュリティの重要性

電子カルテ, 診療予約システム等のITシステムの利用増加に伴い,
セキュリティリスクも増加, システムへの侵害で起こること

重要情報の漏洩	重要情報の改ざん	システムの停止
		
患者情報を保存した USBメモリを紛失した	データベース上の患者 情報を改ざんされた	電子カルテのシステムが 急に使えなくなった

ランサムウェア被害の結果,漏洩, 改ざん,
システム停止, のすべてが起こる

セキュリティ事故はなぜ起こる？



意図的な攻撃の動機, 個々の攻撃
の手法のすべてはランサムウェアの感染
活動に関連している

「診療系ネットワークの完全分離」

なぜ電子カルテを利用するのか？

- 医療関連多職種間で情報を共有
- 物理場所，アクセス時間を短縮し業務実行

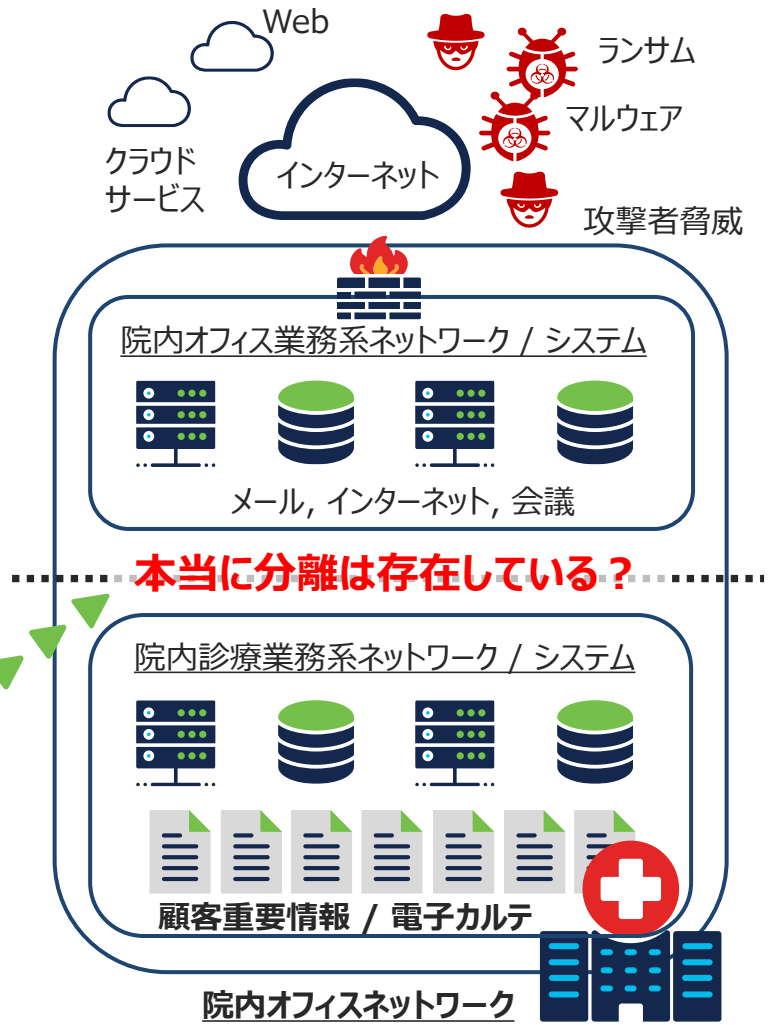
なぜ診療予約システムを利用するのか？

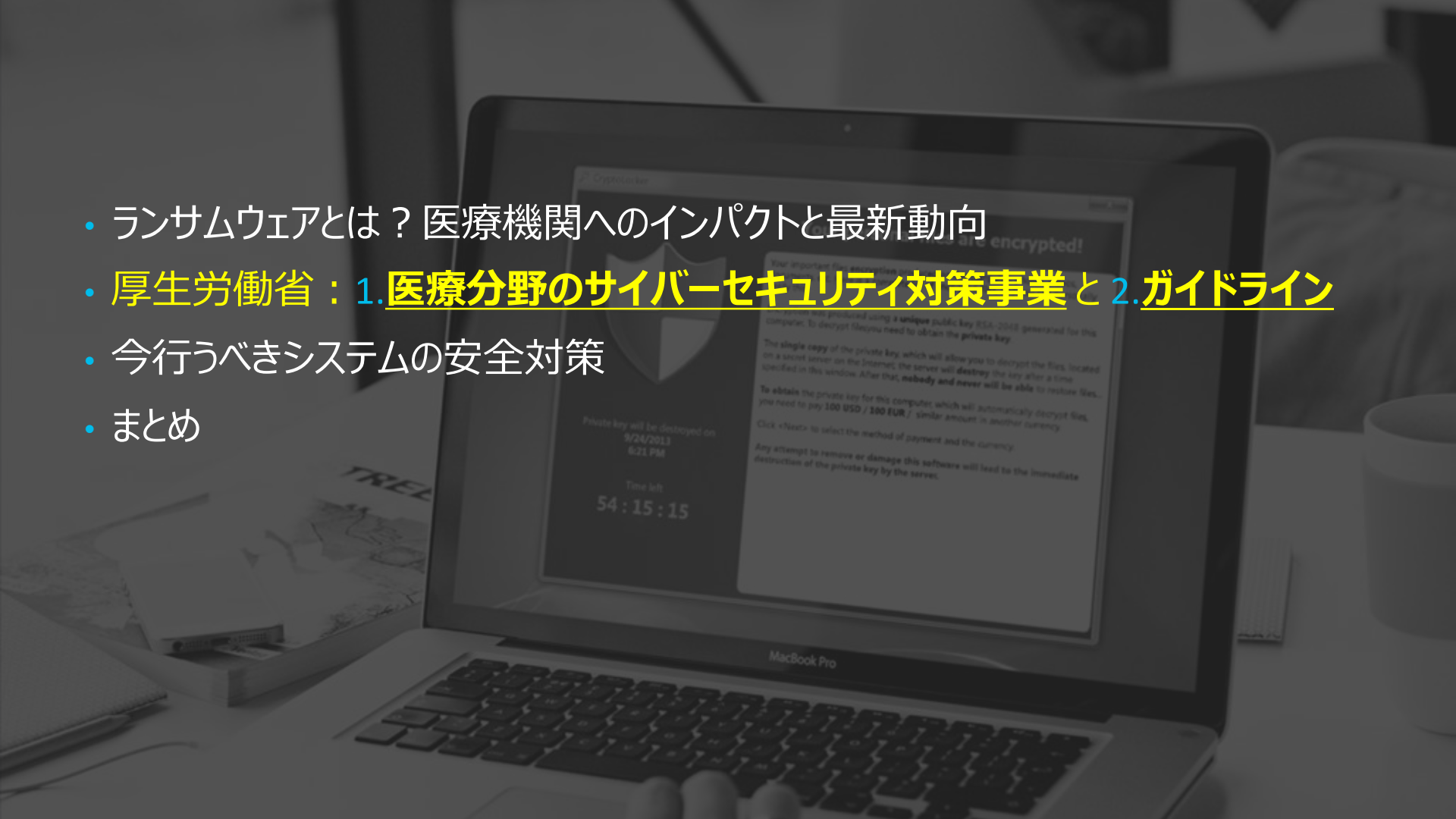
- 医療関係者、患者とも簡単な操作で時間を有効活用

今後さらなるオープン化が進む

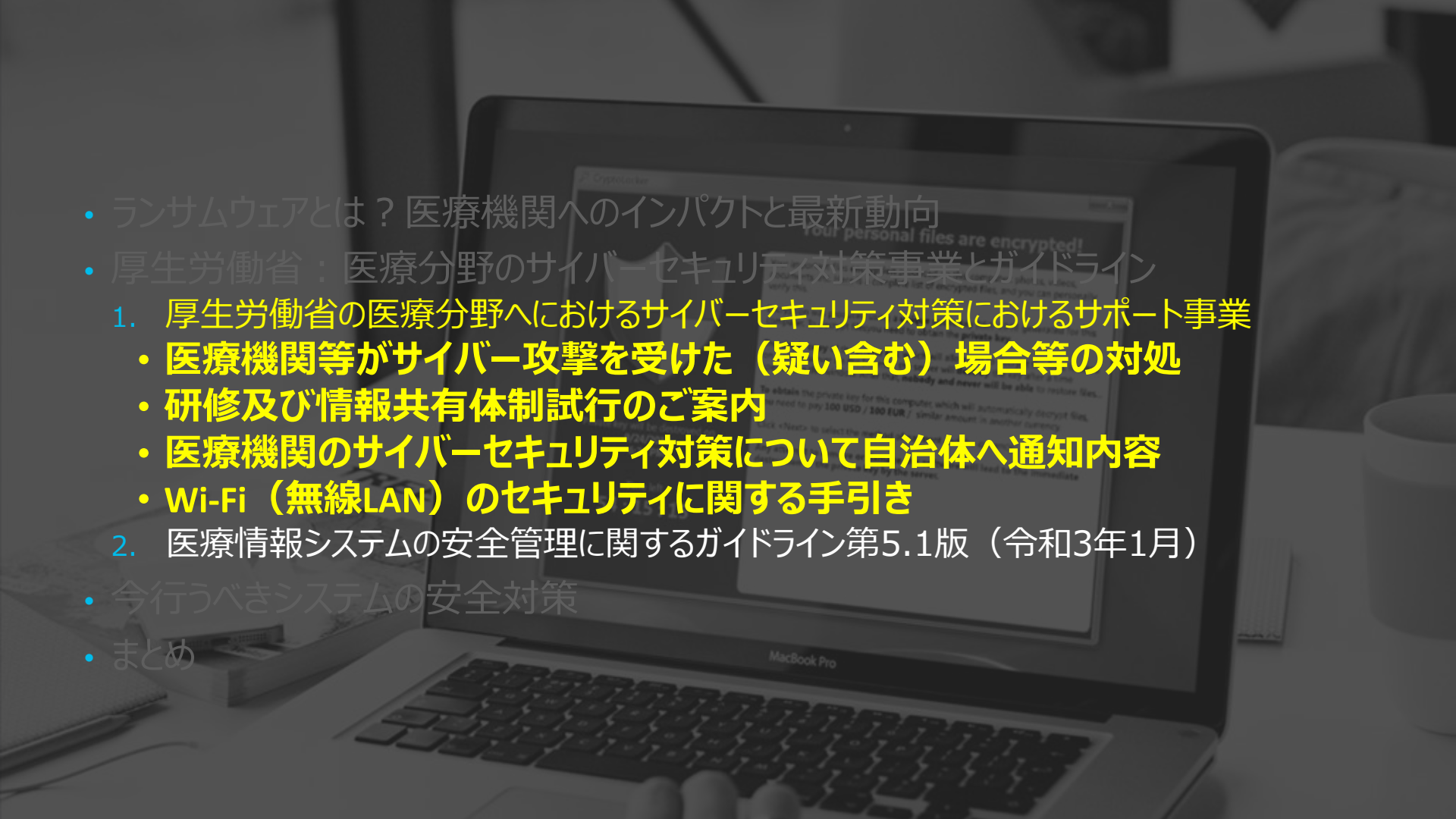
システム運用におけるIT有効活用の現実は

- オフィス業務VDIから診療系情報へのアクセスできる
- 保守用物理アクセスネットワークが存在する
- 保守用リモートアクセスVPN / VDIが存在する
- 過去のアクセス手段，撤去予定設備が残存する





- ランサムウェアとは？医療機関へのインパクトと最新動向
- 厚生労働省：1.**医療分野のサイバーセキュリティ対策事業**と2.**ガイドライン**
- 今行うべきシステムの安全対策
- まとめ



- ランサムウェアとは？医療機関へのインパクトと最新動向
- 厚生労働省：医療分野のサイバーセキュリティ対策事業とガイドライン
  1. 厚生労働省の医療分野へにおけるサイバーセキュリティ対策におけるサポート事業
     - **医療機関等がサイバー攻撃を受けた（疑い含む）場合等の対処**
     - **研修及び情報共有体制試行のご案内**
     - **医療機関のサイバーセキュリティ対策について自治体へ通知内容**
     - **Wi-Fi（無線LAN）のセキュリティに関する手引き**
  2. 医療情報システムの安全管理に関するガイドライン第5.1版（令和3年1月）
- 今行うべきシステムの安全対策
- まとめ

医療機関等がサイバー攻撃を受けた場合の対処

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

医療機関等がサイバー攻撃を受けた（疑い含む）場合等の対処

- 所管省庁への連絡
- そのための体制を整備する
- 「医療情報システムの安全管理に関するガイドライン第5.1版」に基づく対応

コンピュータウイルスの感染などによるサイバー攻撃を受けた状況とは

- 障害が発生
- 個人情報の漏洩
- 医療提供体制に支障が生じる（恐れがある）事案
- サイバー攻撃でなく医療情報システムに障害が発生した場合も含まれる

医療機関等がサイバー攻撃を受けた場合等の厚生労働省連絡先
医政局研究開発振興課医療情報技術推進室
TEL: 03-3595-2430
MAIL: igishitsu@mhlw.go.jp

研修及び情報共有体制試行のご案内

https://www.mhlw.go.jp/stf/cybertraining2021.html
https://www.mhlw.go.jp/content/10808000/000885625.pdf

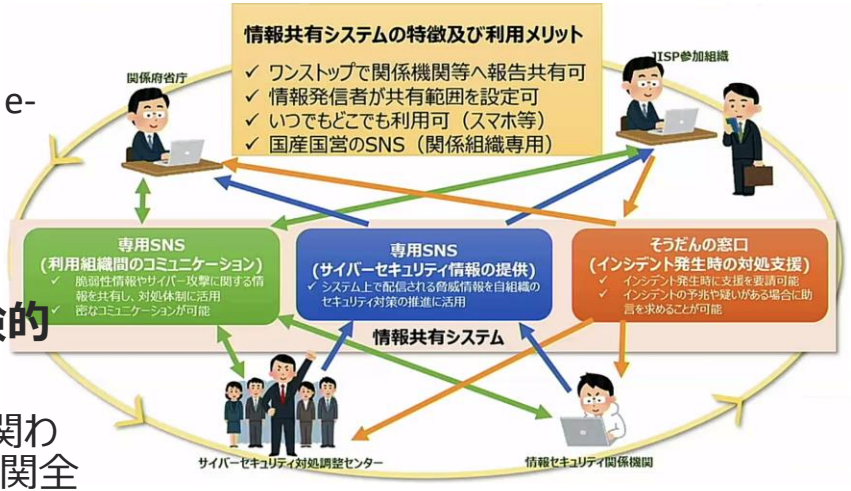
医療従事者向けのサイバーセキュリティ研修の実施提供

- 「経営層（大規模医療機関）」向け研修 (30分)
- 「経営層（中小規模医療機関）」向け研修 (30分)
- 「システム管理者・セキュリティ管理者」向け研修 (60分：e-learningのみ / 90分：Webinar＋e-learning)
- 研修日程：令和4年1月31日～令和4年3月11日
  - 申し込み期限 3 月 4 日

情報共有システム (JISP) を利用した情報共有の試験的導入を開始

- ある医療機関にてサイバー攻撃を受けた際、その攻撃に関わる情報を他の医療機関に共有し、同様の攻撃を医療機関全体として防ぐことができる
- 情報共有の仕組みを検討する際のプロトタイプとする
- 情報共有ツールを用いた情報共有・相談体制の試行

JISP



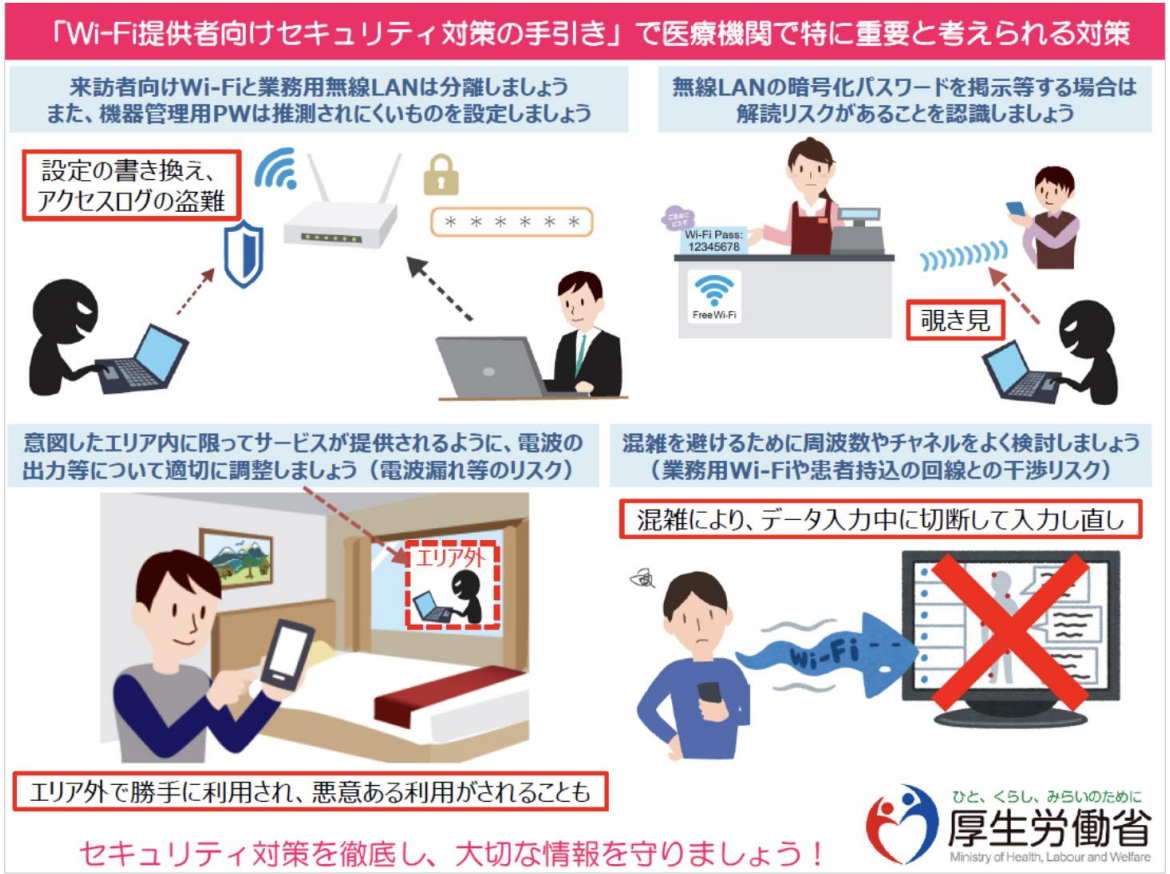
医療機関のサイバーセキュリティ 自治体 へ通知内容

https://www.mhlw.go.jp/content/10800000/000646143.pdf

1. 「医療情報システムの安全管理に関するガイドライン」の周知徹底について
   - ガイドラインの徹底
   - 事故発生時の連絡「医療技術情報推進室」
2. 情報セキュリティインシデントが発生した医療機関等に対する調査及び指導について
   - **被害状況、対応状況、復旧状況、再発防止策等に係る調査及び指導を行ってください**
   - **医療技術情報推進室に報告してください**
   - **指導の際、医療法に基づき医療機関への立ち入りが可能**
3. 医療分野におけるサイバーセキュリティの取り組み（医療セプター）との連携について

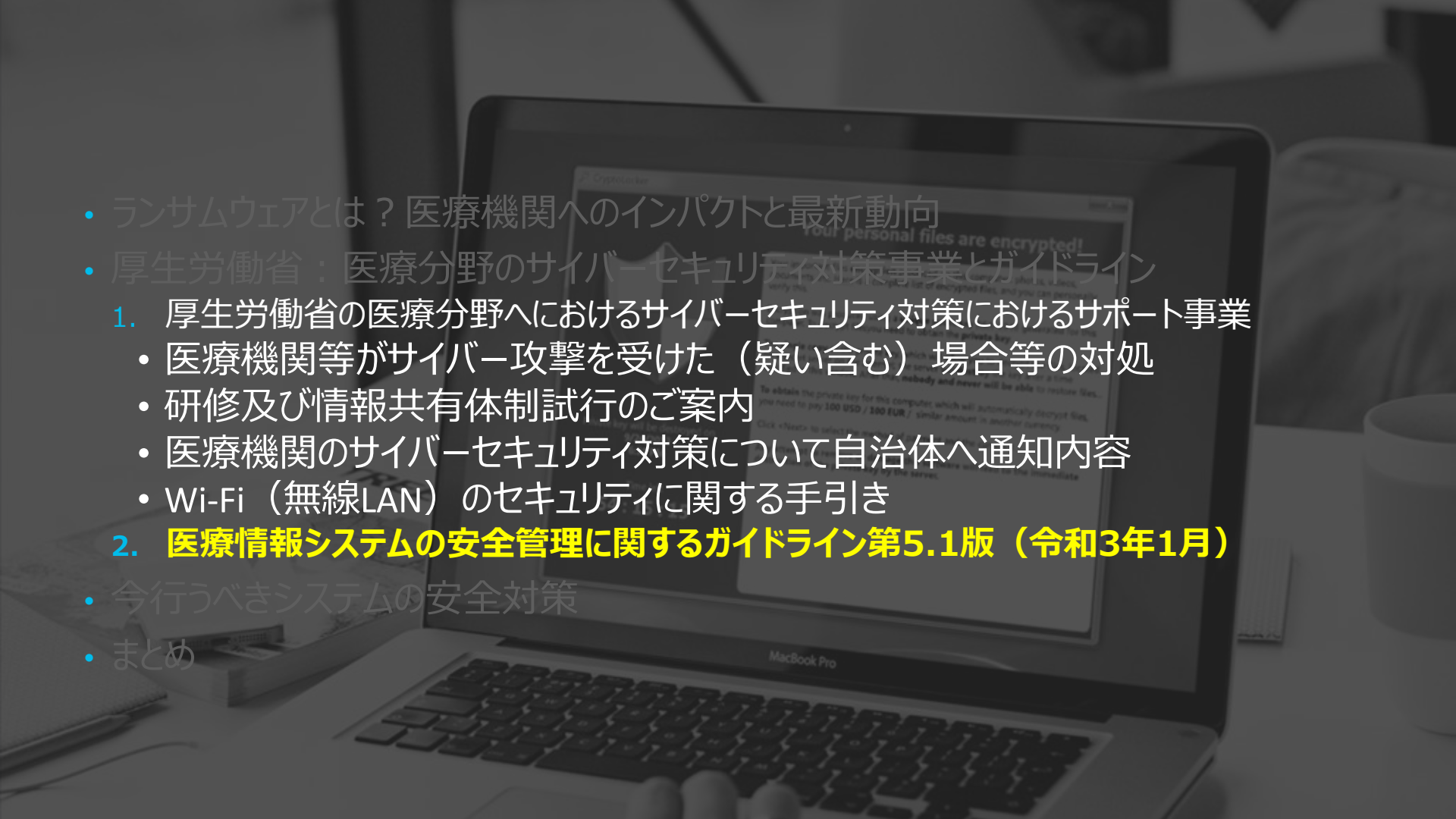
Wi-Fi（無線LAN）のセキュリティに関する手引き

https://www.mhlw.go.jp/content/10800000/000637312.pdf
https://www.mhlw.go.jp/content/10800000/000637123.pdf



- 来訪者及び患者向けにWi-Fiアクセスサービスは十分なセキュリティ対策がとられていないと踏み台に悪用される
- 総務省資料参照を推奨

出展：https://www.mhlw.go.jp/content/10800000/000637123.pdf



- ランサムウェアとは？医療機関へのインパクトと最新動向
- 厚生労働省：医療分野のサイバーセキュリティ対策事業とガイドライン
  1. 厚生労働省の医療分野へにおけるサイバーセキュリティ対策におけるサポート事業
     - 医療機関等がサイバー攻撃を受けた（疑い含む）場合等の対処
     - 研修及び情報共有体制試行のご案内
     - 医療機関のサイバーセキュリティ対策について自治体へ通知内容
     - Wi-Fi（無線LAN）のセキュリティに関する手引き
  2. **医療情報システムの安全管理に関するガイドライン第5.1版（令和3年1月）**
- 今行うべきシステムの安全対策
- まとめ

医療情報システムの安全管理に関するガイドライン第5.1版

https://www.mhlw.go.jp/stf/shingi/0000516275.html

- **厚生労働省**が策定した**医療分野の情報システムにおけるガイドライン**
  - 個人情報保護に扱う情報システム定義，選定，導入，運用管理、の適切な対応

ガイドライン文書と全体構成とポイント

1. 位置づけ、改訂履歴
2. ガイドラインの読み方
3. ガイドラインの対象システム
4. 電子的な医療情報を取り扱う際の責任のあり方
5. 情報の相互運用性と標準化について
6. **医療情報システムの基本的な安全管理**
7. 電子保存の要求事項について
8. 診療録及び診療諸記録を外部に保存する際の基準
9. 診療録等をスキャナ等により電子化して保存する場合について
10. 運用管理

4章：医療機関が扱う医療情報利用、運用に伴う**責任性の分界点、明確化、対処、契約**等

5章：医療情報の電子化に伴う、**国際的標準的規格、国内標準規格による相互運用**

6章：医療情報システムの技術的・システム的対策、医療情報システムの組織的、人的、運用対策

医療情報システムの安全管理に関するガイドライン第5.1版

https://www.mhlw.go.jp/stf/shingi/0000516275.html

- **6. 医療情報システムの基本的な安全管理**
  - **医療情報システムセキュリティに関するシステム対策**
  - 医療情報システムセキュリティに携わる組織・管理・運用体制の実践

6.1. 方針の制定と公表 (※)
6.2. 医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践
6.3. 組織的安全管理対策 (体制、運用管理規程) (※)
6.4. 物理的安全対策 (※)
6.5. 技術的安全対策 (※)
6.6. 人的安全対策 (※)
6.7. 情報の破棄 (※)
6.8. 医療情報システムの改造と保守 (※)
6.9. 情報及び情報機器の持ち出しについて (※)
6.10. 災害、サイバー攻撃等の非常時の対応 (※)

体制と管理システム，そのマネージメント

6.5 システムアプローチ

(※)「最低限のガイドライン」に従う対策を行う必要がある
制度上の要求事項（法律、厚生労働省通知、他の指導の要求事項）を満たすために必ず実施しなければならない
(2章 :本ガイドラインの読み方)

医療情報システムの安全管理に関するガイドライン第5.1版

https://www.mhlw.go.jp/stf/shingi/0000516275.html

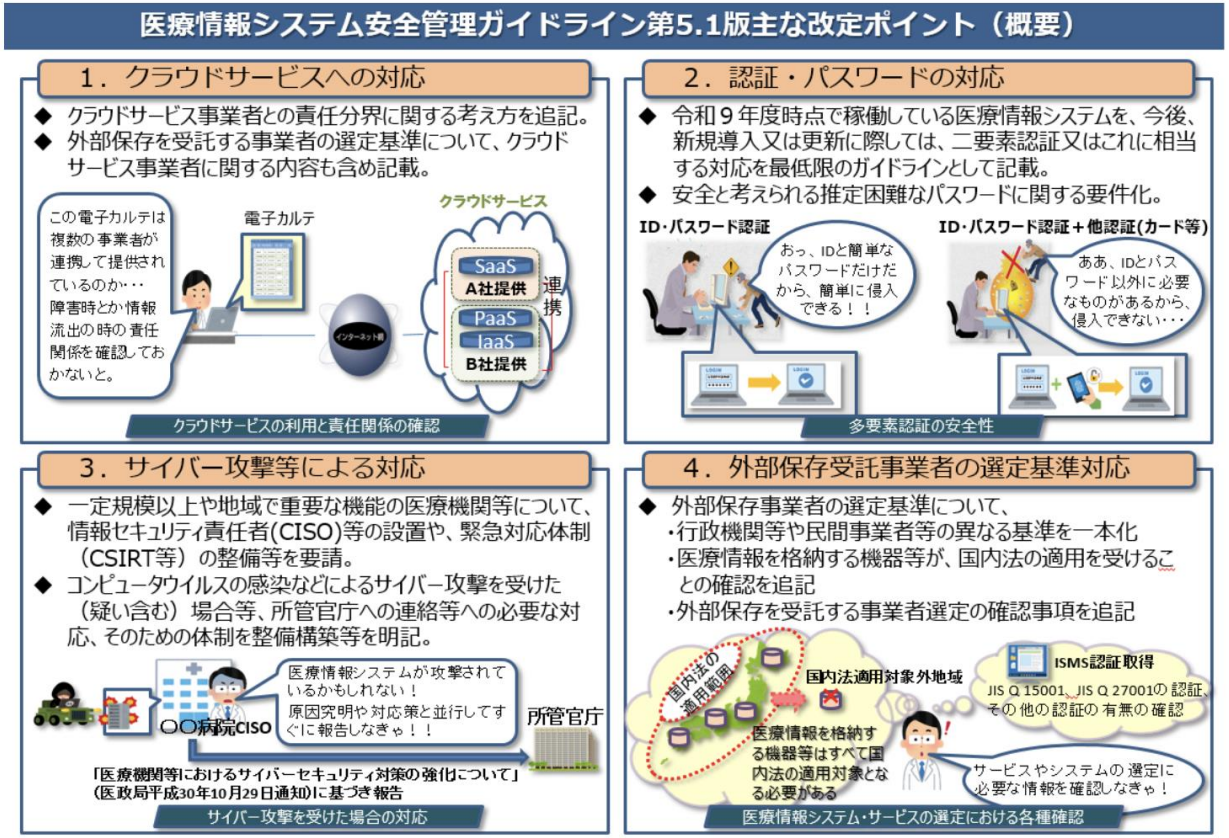
- **6.5 技術的安全対策**
  - **医療情報システムセキュリティにおけるIT/システム的対策**
  - 技術的な対策のみで全ての脅威に対応できるわけではない、運用管理と併用する
  - それでも、技術的対策は強力な安全管理の手段

(1) 利用の識別・認証
(2) 情報の区分管理とアクセス権限の管理
(3) アクセスの記録 (アクセスログ)
(4) 不正ソフトウェア対策
(5) ネットワーク上からの不正アクセス
(6) 医療等分における IoT 機器の利用

6.5 システムアプローチ

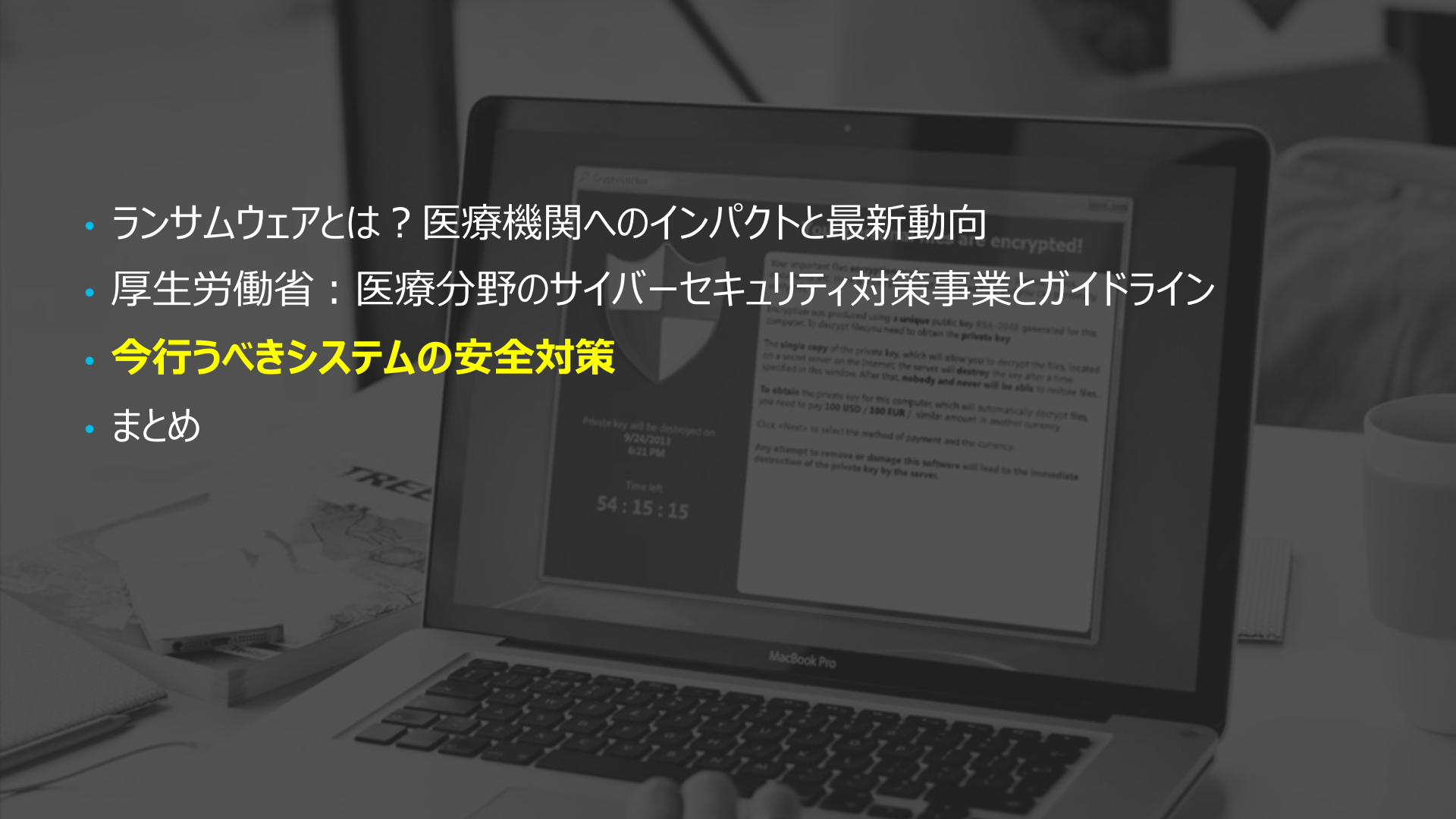
医療情報システムの安全管理に関するガイドライン第5.1版

https://www.mhlw.go.jp/stf/shingi/0000516275.html



1. **クラウドサービスへの対応**
2. **認証・パスワードの対応**
3. **サイバー攻撃等による対応**
4. **外部保存受託事業者の選定基準対応**

- 昨今のトレンドを反映
  - 近年のサイバー攻撃の手法の多様化・巧妙化
  - 情報セキュリティに関するガイドラインの整備
  - 地域医療連携や医療介護連携等の推進、クラウドサービス等の普及
  - 医療機関等を対象とするセキュリティリスクが顕在化



- ランサムウェアとは？医療機関へのインパクトと最新動向
- 厚生労働省：医療分野のサイバーセキュリティ対策事業とガイドライン
- **今行うべきシステムの安全対策**
- まとめ

ガイドラインに準拠 ： 医療機関向け次世代システム

『医療情報安全管理に関するガイドライン』に基づくゼロトラストセキュリティの実現

クラウドサービスへの対応

電子カルテ端末でのインターネット利用や、Web会議など、クラウドを前提としたセキュリティを構築する必要がある。

認証・パスワードの対応

モバイルデバイスなど多くのデバイスが接続される環境においては、ネットワークおよびデバイス認証（二要素認証など）による、強固な認証の仕組みが必要。
※令和9年時点で稼働しているシステムには２要素認証が必須

サイバー攻撃等による対応

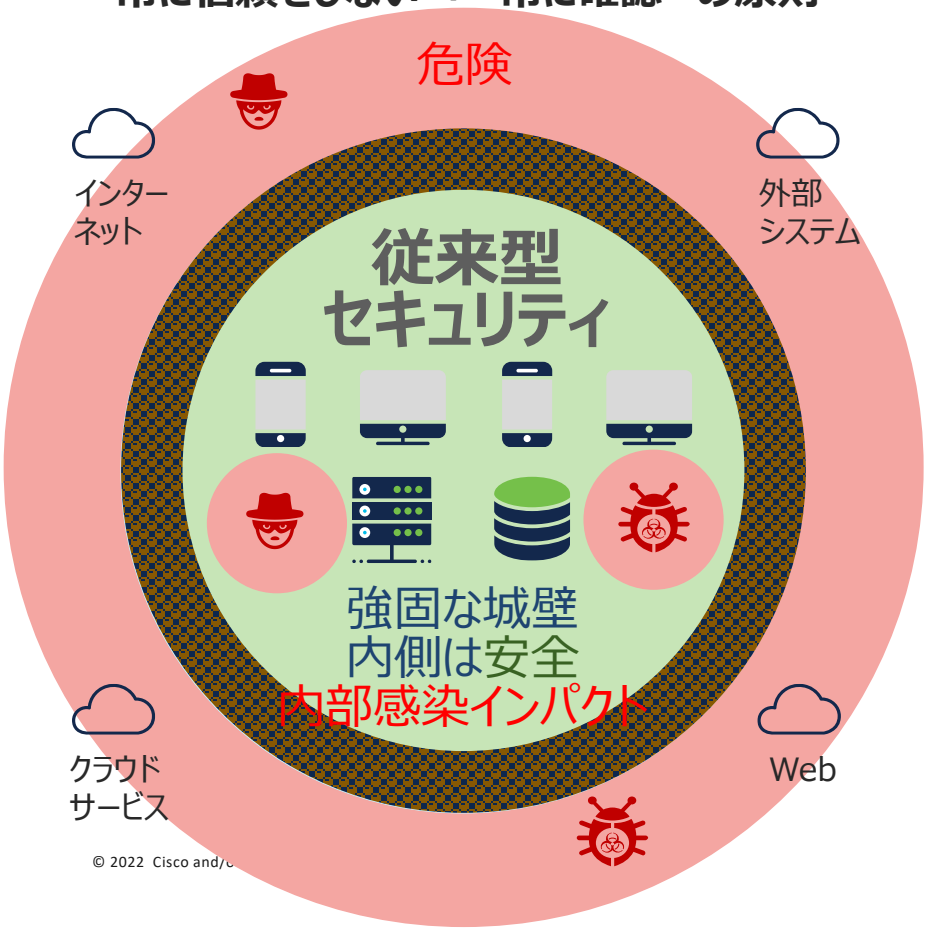
医療情報ネットワークをサイバー攻撃から守るためのファイアウォールやアンチウイルスはもちろん、内部のふるまい検知などにより、ゼロトラストなセキュリティを構築することが必要。

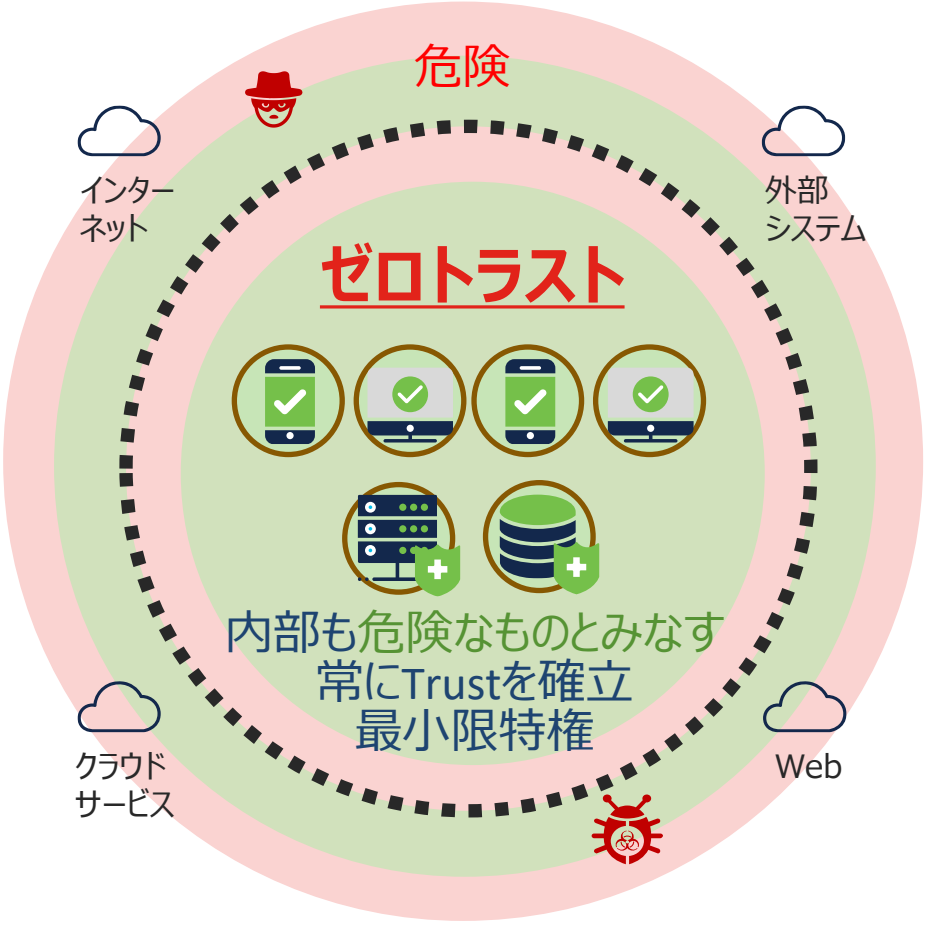
外部メンテナンス業者等の外部からのアクセスの対応

VPN等で外部からアクセスするユーザの本人確認の強化やアクセス先の限定など院内にアクセスするユーザによる脅威の軽減が必要。

ゼロトラスト – アクセスへの適用のプロセスを再考

“常に信頼をしない”+ ”常に確認” の原則





ガイドライン「6.5 技術的安全対策」の解釈のポイント

https://www.mhlw.go.jp/stf/shingi/0000516275.html

技術的安全対策の項目	項目番号	ガイドラインのポイント	該当対策カテゴリ
(1) 利用者の識別及び認証	6.5B (1)	• 必須機能 • 医療情報システムは利用の識別・認証を行う機能を持たなければならない • 医療情報システムへのアクセスを行う全ての職員及び関係者が対象 • 認証機能例：D・パスワード、IC カード、 電子証明書、生体 証等、本人の識別・認証に用いる手段 • 令和9 年度時点で稼働システムでは原則として二要素認証を採用されていること • 認証強度の考え方、二要素認証の説明が多くなってきている	NAC (Network Access Control) MFA (Multi Factor Authentication) IDaaS

ガイドライン「6.5 技術的安全対策」の解釈のポイント

https://www.mhlw.go.jp/stf/shingi/0000516275.html

技術的安全対策の項目	項目番号	考えられる対策例	該当対策カテゴリ
(2) 情報の区分管理とアクセス権限の管理	6.5B (2)	• 情報の種別、重要性と利用形態に応じて情報の区分管理を行う、情報区分ごと、組織における利用 や利用 グループ 業務単位等ごとに利用権限を規程 • アプリケーション、ネットワーク、システム利用における細分化 • クラウドサービス利用の場合、特性に注意して十分に考慮、対策を建てる • ネットワーク、クラウドに対する抽象的な説明、広い対象範囲での解釈が必要	NAC (Network Access Control) Firewall / UTM / NGFW SDN (Software Defined Network) マイクロセグメンテーション, Zero Trust Solution
(3) アクセスの記録(アクセスログ)	6.5B (3)	• 個人情報を含む資源については、全てのアクセスの 録 アクセスログを収集 • ログの保護が必要、削除、改ざん、追加から防止	医療システム、アプリ、ネットワークの正しいログ管理, SIEM

ガイドライン「6.5 技術的安全対策」の解釈のポイント

https://www.mhlw.go.jp/stf/shingi/0000516275.html

技術的安全対策の項目	項目番号	考えられる対策例	該当対策カテゴリ
(4) 不正ソフトウェア対策	6.5B (4)	• コンピュータウイルス、マルウェア、ワーム等様々な形態・呼称を持つ不正ソフト対策 • 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 • ランサムウェアを含めた不正ソフトウェア全般における、多様、多層な対策手法の検討	Anti Virus EDR (Endpoint Detection Response) SASE / SIG (Secure Internet Gateway IPS / IDS
(5) ネットワーク上からの不正アクセス	6.5B (5)	• 「Firewall」,「IPS/IDS」はカテゴリとして導入推奨の明記がされている • コンピュータウイルス等が侵入した場合を想定した内部脅威監視などのモニタリングが必要	Firewall / UTM / NGFW IPS / IDS NDR (Network Detection Response)
(6) 医療等分 におけるIoT 機器の利用	6.5B (6)	• セキュリティの観点から、これまで想定されなかったリスクが顕在化する恐れに対応 • 「IoT セキュリティガイドライン ver1.0」参照推奨 • 正しくIoTデバイスが利用されているかを可視化	Medigate (医療機器可視化)

ガイドラインの解釈の注意点

https://www.mhlw.go.jp/stf/shingi/0000516275.html

- **ガイドライン解釈の注意点**
  - **ガイドラインは、医療情報システムセキュリティにおける最低ラインの対策のみ言及**
  - ランサムウェア、洗練される攻撃、未知の攻撃（ゼロデイ）に対する**＋αな対処**が必要
    - 企業ITシステムに求められるセキュリティ対策としてはやや不足
    - ガイドラインの内容としてやや古い解釈がある

(4) 不正ソフトウェア対策

ただし、これらのコンピュータウイルス等も常に変化しているため、検出するためのパターンファイルや検索エンジンを常に最新のものに更新しておくことが必須である。

(5) ネットワーク上からの不正アクセス

ファイアウォールは、「パケットフィルタリング」、「アプリケーションゲートウェイ」、「ステートフルインスペクション」等の各種方式がある。また、その設定によっても動

ガイドラインに準拠 : 医療機関向け次世代システム

『医療情報安全管理に関するガイドライン』に基づくゼロトラストセキュリティの実現

優先度の高いセキュリティソリューションカテゴリ : MFA, EDR, SASE, SIG, NDR

2要素 +α 他要素認証ソリューション

MFA

MFA (Multi Factor Authentication, Zero Trust)

次世代エンドポイント EDR + EPP

EDR

EDR (Endpoint Detection & Response)

統合クラウド・セキュリティ / DNSセキュリティ / Proxy

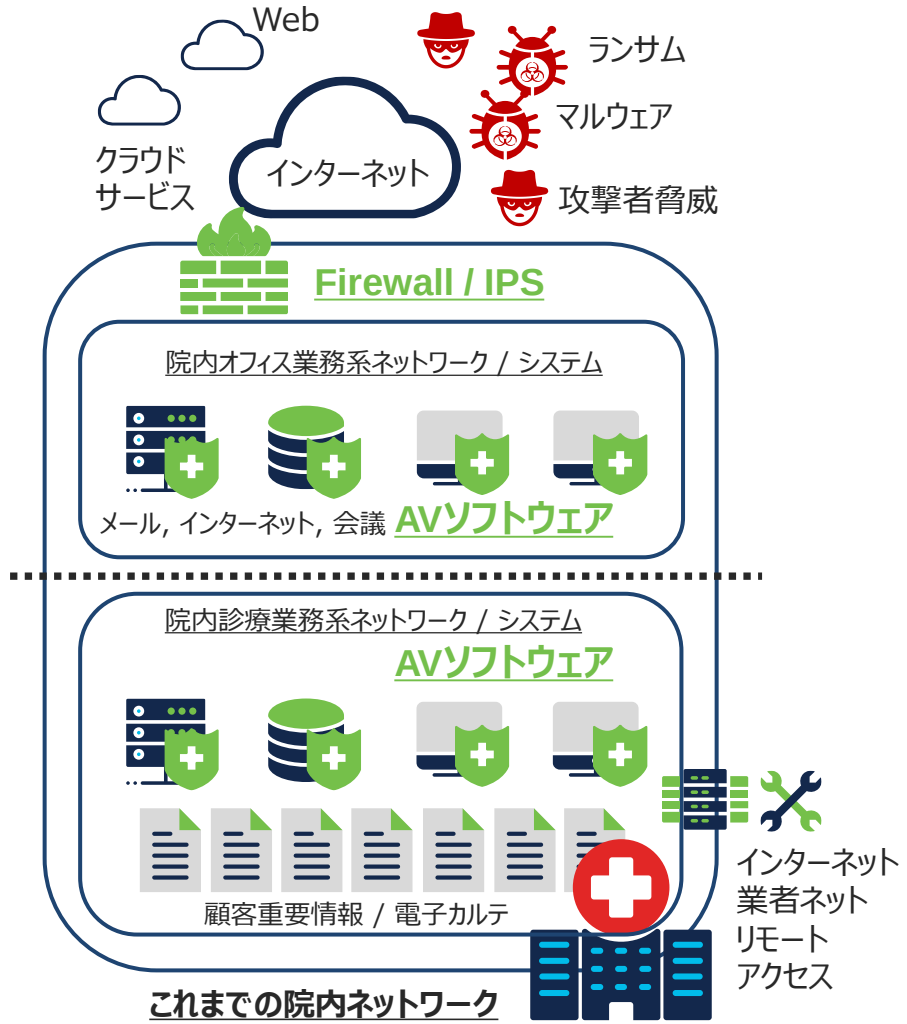
SASE / SIG

SASE (Secure Access Service Edge) / SIG (Secure Gateway)

NDR

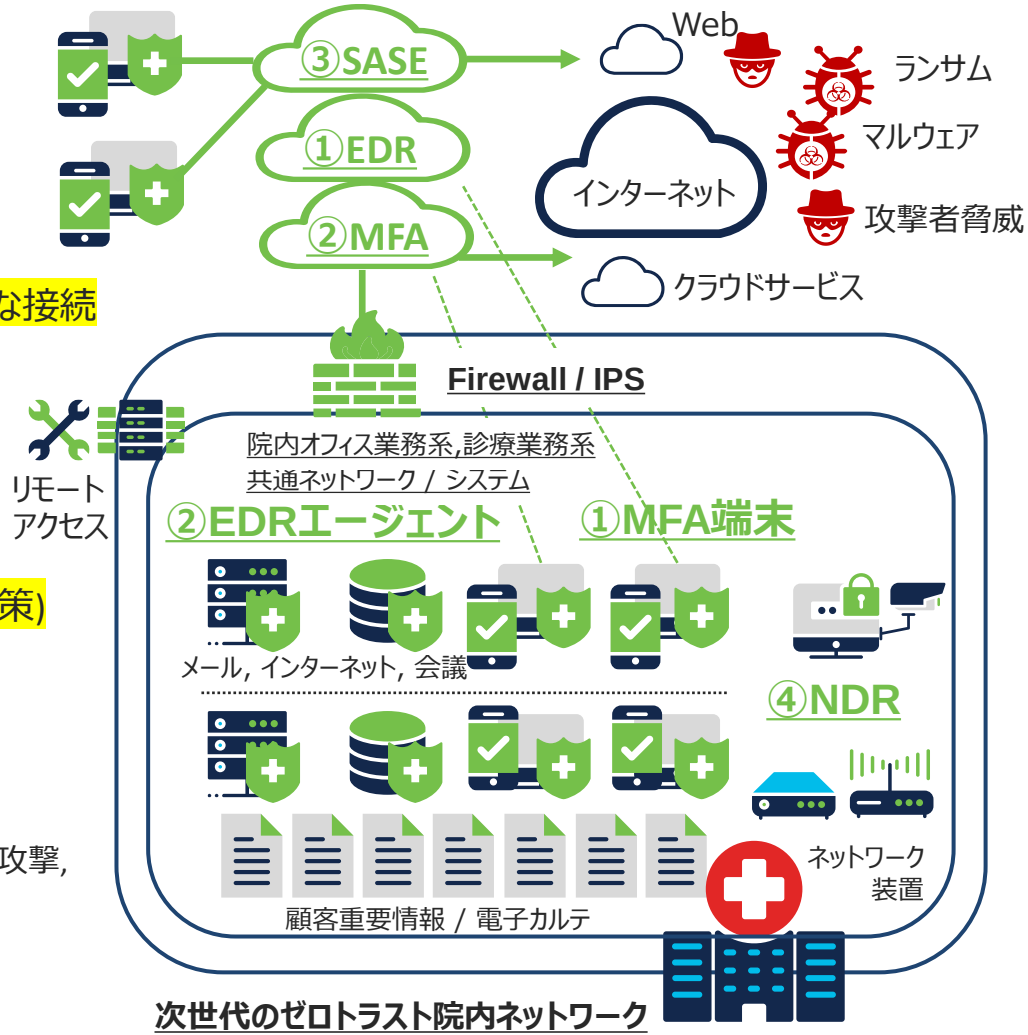
これまでのシステム

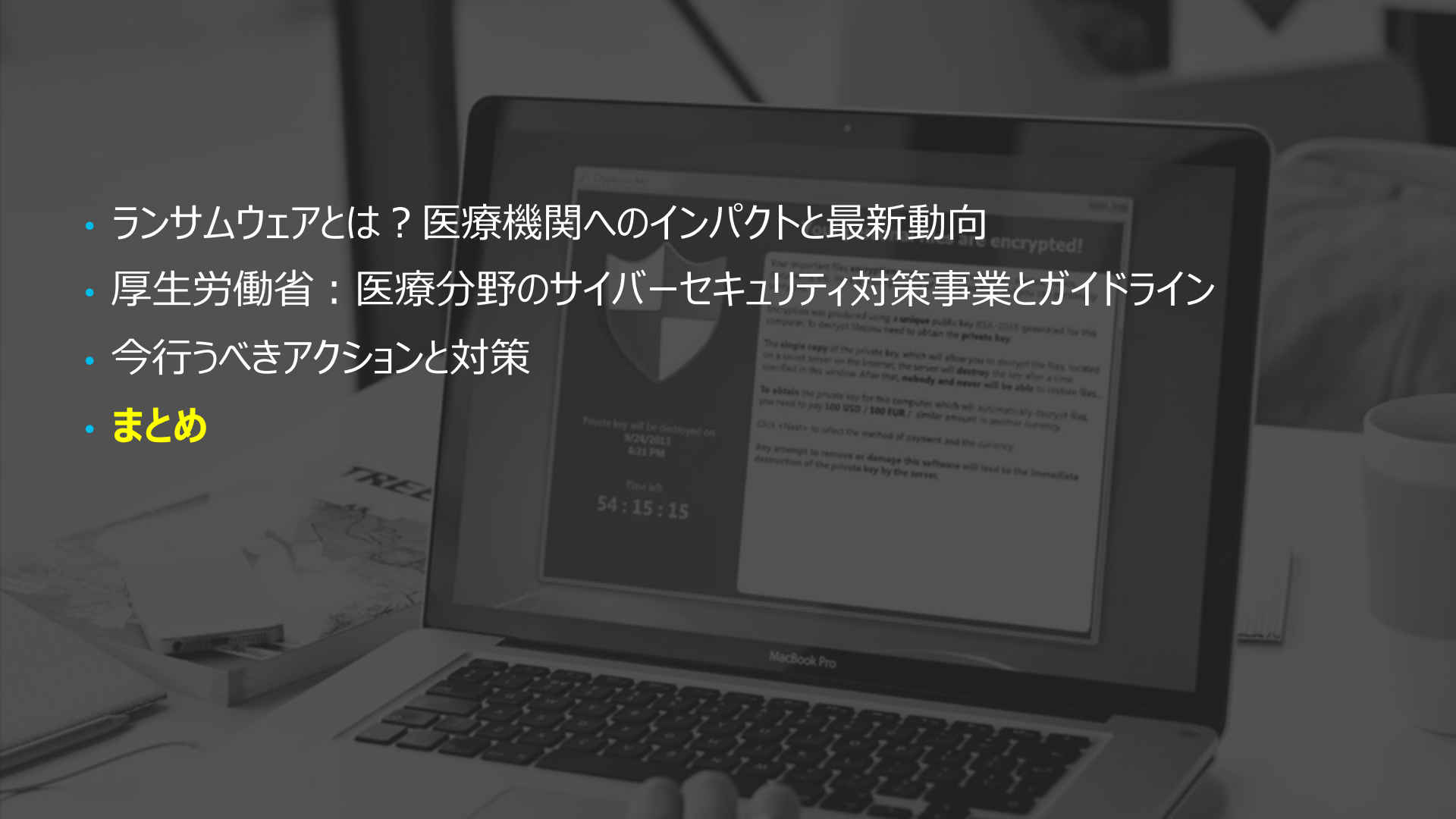
- **境界型セキュリティ対策**
  - Firewall, IPS / IDS の利用
- **端末セキュリティ対策**
  - アンチウィルス / EPP ソフトウェアの利用
- **診療業務系ネットワークの分割**
  - 完全分離, クローズド運用になっていない
  - セキュリティ技術の有効活用の阻害
    - AVアップデートサーバのオンプレミス運用
    - リアルタイムアップデート
    - インテリジェンスへの到達性 (タイムリーな客観的洞察が得られない)



ゼロトラストへのマイグレーション

- **院内ネットワークの共通化**
  - 段階的な共通化移行とインターネットへの積極的な接続
    - 医療業務効率化, DX化, 本格テレワーク
    - 次世代対策によりゼロトラストの機能を利用
    - 効果的なセキュリティ技術の利用
- **端末セキュリティ対策強化**
  - EDR へのマイグレーションによる端末強化
  - MFA の導入による認証強化 (令和9年システム対策)
  - SASE / MFA 導入による安全な医療テレワーク
- **ネットワーク・セキュリティ強化**
  - Firewall, IPS / IDS の利用
  - SASE の追加セキュリティ機能 (DNSセキュリティ, Proxy等)
  - NDR / ネットワーク装置連携による内部犯行対策, 未知の攻撃, 高度なランサムウェア活動の識別





- ランサムウェアとは？医療機関へのインパクトと最新動向
- 厚生労働省：医療分野のサイバーセキュリティ対策事業とガイドライン
- 今行うべきアクションと対策
- **まとめ**

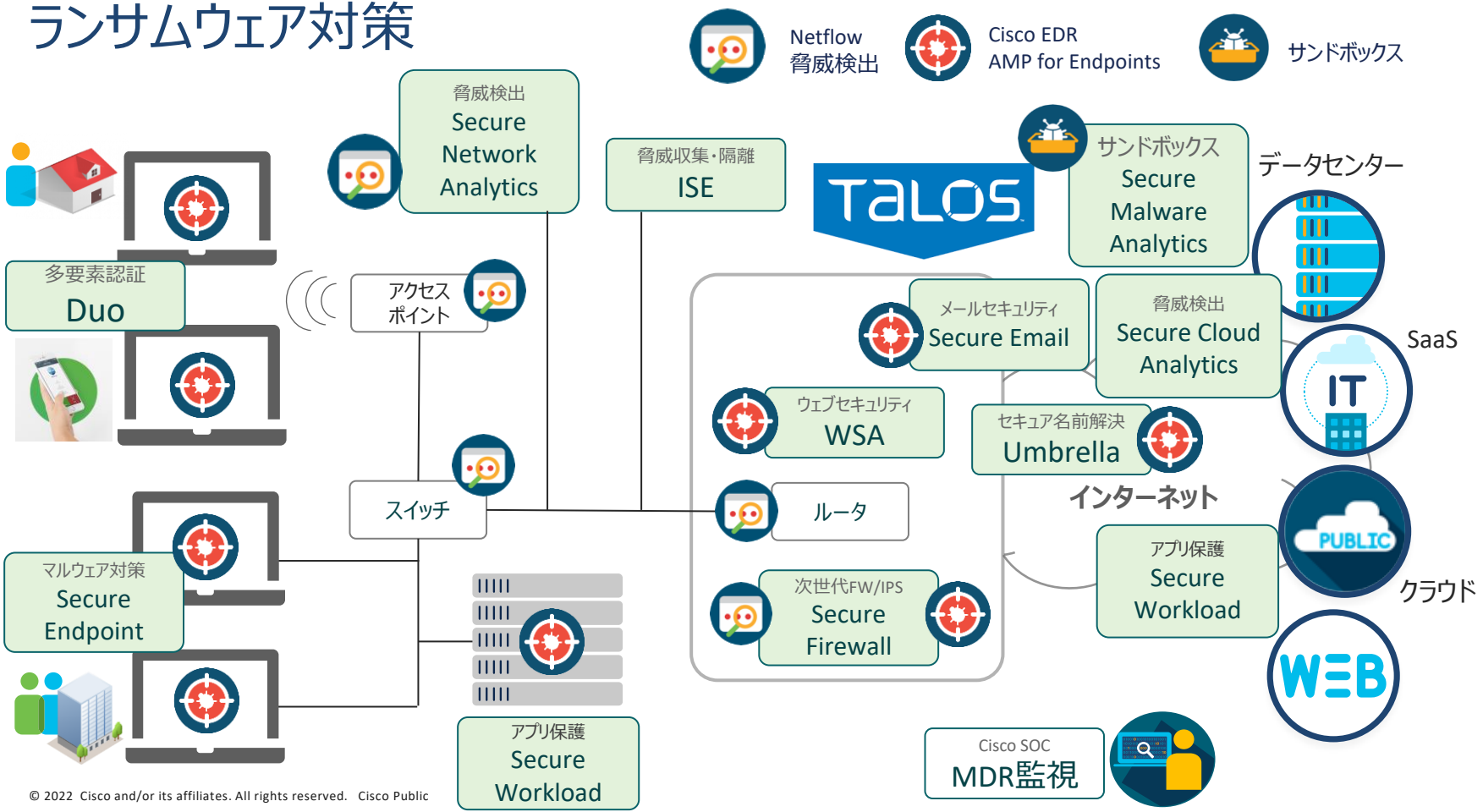
まとめ： 医療機関向け『ランサムウェア対策』セミナー

- 医療システムにおけるセキュリティの重要性と事故のポイント
- ランサムウェアの最新動向
- ランサムウェアと医療システムとの関連性と現実
- 厚生労働省の医療機関へのサポート事業 (通知, 指導, 研修, ガイドライン)
- 「医療情報システムの安全管理に関するガイドライン第5.1版」ポイント
- 次世代医療情報システム向けゼロトラストアプローチ
- 次世代医療情報システム向けクラウドソリューションの選択
  - 1.MFA, 2.EDR, 3.SASE

ランサムウェア対策

	侵入・初期感染	偵察・感染拡大	実行・被害	原因特定・対応
多要素認証 Duo	多要素認証で侵入を防御 端末の健全性を確認			
メールセキュリティ Secure Email	標的型メールを破棄 マルウェアファイルを破棄			
ウェブセキュリティ WSA	不正サイトアクセス防止 マルウェアファイルを破棄		C2通信の検出と遮断	
セキュア名前解決 Umbrella	不正サイトアクセス防止 マルウェアファイルを破棄		C2通信の検出と遮断	不正サイトアクセス継続監視 C2通信収束確認
次世代FW/IPS Secure Firewall	不正アクセスを防止 マルウェアファイルを破棄		C2通信の検出と遮断	
マルウェア対策 Secure EP (AMP)	マルウェア感染の防止・脅威の継続監視 侵入経路・拡散範囲の把握			脅威の継続監視 侵入経路・拡散範囲の把握
脅威検出 Secure N/CA		感染拡大を検出・継続的な監視 ラテラルムーブメント対策	C2通信の検出	脅威の継続監視 C2通信収束確認
脅威収集・隔離 ISE		脅威情報を集約、認証・認可 脅威の隔離・通信制御指示	脅威の隔離	
アプリ保護 Secure WR		感染拡大を検出・継続的な監視 ラテラルムーブメント対策	C2通信の検出と遮断	

ランサムウェア対策



厚生労働省：
医療分野のサイバーセキュリティ対策事業とガイドラインリンク

医療分野のサイバーセキュリティ対策について

- https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

研修及び情報共有体制試行のご案内

- https://www.mhlw.go.jp/stf/cybertraining2021.html
- https://www.mhlw.go.jp/content/10808000/000885625.pdf

医療機関のサイバーセキュリティ対策について自治体へ通知内容

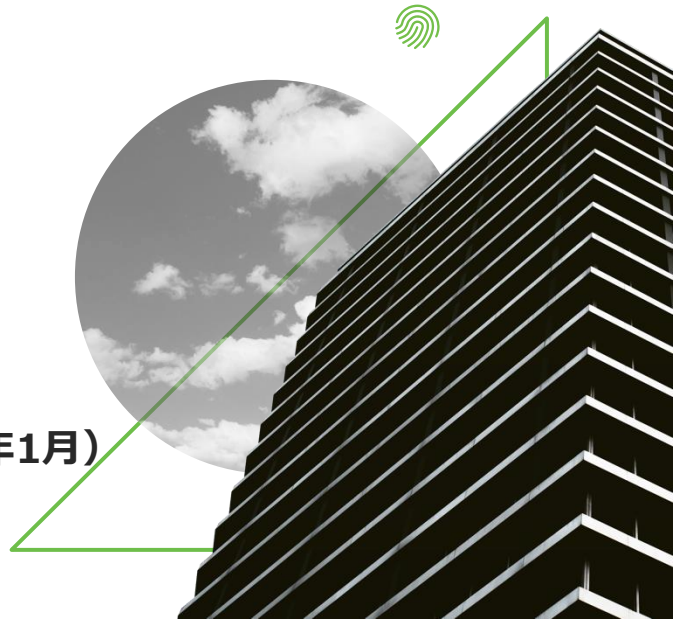
- https://www.mhlw.go.jp/content/10800000/000646143.pdf

Wi-Fi（無線LAN）のセキュリティに関する手引き（総務省）

- https://www.mhlw.go.jp/content/10800000/000637312.pdf
- https://www.mhlw.go.jp/content/10800000/000637123.pdf

医療情報システムの安全管理に関するガイドライン第5.1版（令和3年1月）

- https://www.mhlw.go.jp/stf/shingi/0000516275.html



Thank you

Possibilities