医療機関向けサイバー攻撃
(情報窃取/ウェブ改ざん攻撃)
対応検討の手引き

～医療機関向けランサムウェア対応検討ガイダンスの追補として～

一般社団法人医療ISAC

2023年10月

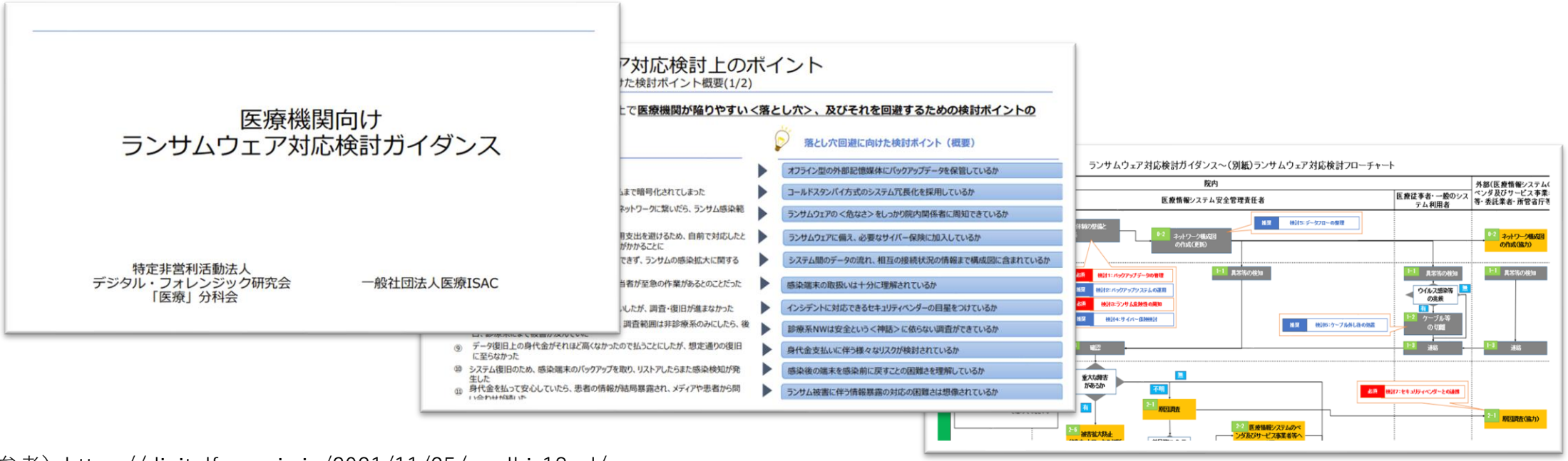
目次

１.本書の位置づけ

1．本資料の位置づけ(1/4)

一般社団法人医療ISACは、2021年11月に、特定非営利活動法人デジタル・フォレンジック研究会/医療」分科会による**「医療機関向けランサムウェア対応検討ガイダンス」**（以下、「医療ランサム対応ガイダンス」と略記）の公開のサポートを行っている。

このガイダンスは当時国内の医療機関を取り巻くランサムウェアの脅威を前に、医療機関の限られたリソース（ヒト・カネ・モノ）のなかで、実際にランサムウェア感染被害を受けた場合に、どのような対応を行うべきかについて、厚生労働省が2021年10月に公開した「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」（以下、「厚労省対応フローチャート」と略記）をもとにアクションプランを整備したものである。



（参考）https://digitalforensic.jp/2021/11/25/medhi-18-gl/

1．本資料の位置づけ(2/4)

医療機関を取り巻くランサムウェアの脅威は当時より増しており、医療ランサム対応ガイダンスは今も有効であると考える。

一方、当該ガイダンスが中心的に論じていないサイバー攻撃、つまり、インターネットと接続した情報系の業務端末に対するメール添付ファイル・サポート詐欺攻撃、またはウェブサイトの改ざんに伴う情報改ざん・マルウェア感染等の攻撃も未だ多く発生している。

医療ランサム対応ガイダンス のスコープ

ランサムウェア攻撃（暗号化/漏洩）

情報詐取を目的とするメール攻撃

インターネット利用時のサポート詐欺攻撃

ウェブサイトの改ざん、それに伴うアクセスユーザへの攻撃

未だに医療機関においても被害が多いサイバー攻撃例

1．本資料の位置づけ(3/4)

上記理由のもと、本資料では医療ランサム対応ガイダンスを追補する観点より、**特に医療ISACに直近で多く問い合わされる質問・相談事項を傾向分析し、特に、この種のサイバー被害の発生に伴い、国内の医療機関としてどのようなアプローチを取るべきか**について、直近に厚生労働省が開示するチェックリストとともに整理することとする。

具体的には、国内の医療機関を対象とした、情報詐取やサイト改ざんサイバー攻撃被害を受けた場合の復旧までのチェックポイントについて、医療ランサム対応ガイダンスでも取り込んでいる厚労省対応フローチャートに加え、厚生労働省が23年6月に医療法に基づく立入検査向けに公開した「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」の要件に紐づけながら、解説する。

情報窃取

- ✓ 情報窃取を目的とした不正ファイルをメールを介して送信
- ✓ インターネット利用時のサポート詐欺

など

サイト改ざん

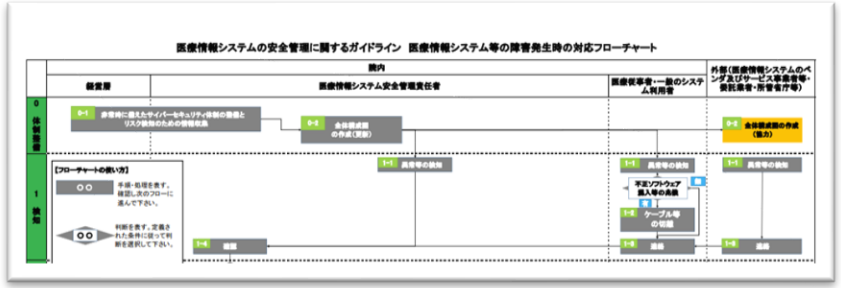
- ✓ 不適切な情報の発信
- ✓ アクセスユーザに対する不正プログラムの強制ダウンロード

など

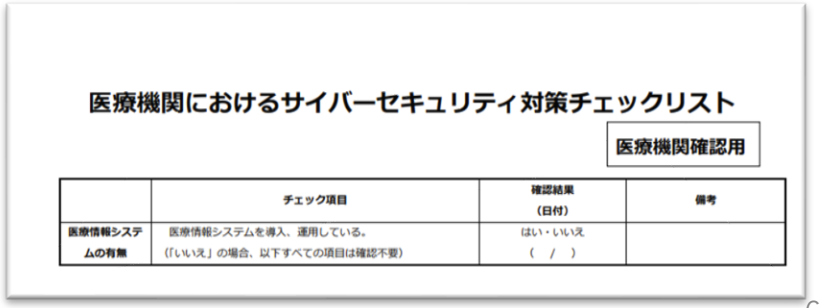
医療ISACへの問い合わせ傾向

被害に備える、または受けた場合の検討ポイント

＜対応フローチャート(21/10)＞



＜サイバーチェックリスト（23/6）＞



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

医療機関確認用

	チェック項目	確認結果（日付）	備考
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ （　/　）	

1．本資料の位置づけ(4/4)

医療ランサム対応ガイダンスの定義を援用し、本資料でも検討ポイントは必須/推奨の二つの観点で分類し、厚労省対応フローチャート上の対策番号と紐づけ、その対策の検討・対応主体も定義している。
なお、本資料では上記事項に加え、**各検討ポイントの対象範囲（情報窃取/ウェブ改ざん）の分類**とともに、23年6月時点の**「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(医療機関確認用）」の各チェック項目との紐づけ**も行っている。

必須・推奨の考え方

必須

攻撃を受けた場合に必ず検討すべき事項。
本事項の検討が十分でない場合、対応手続上、深刻なリスクを招く。

推奨

【必須】ほどではないが、攻撃を受けた場合に対応の際に、検討することが強く推奨される事項。

関連する対策番号

「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」で示される対策のどこで、該当する検討を行うべきかを示している

関係する検討主体

「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」で示される対策の検討・対応主体が誰かを示している

医療ランサム対応ガイダンスと同一の定義を援用

対象範囲の分類

例）情報窃取/サイト改ざん双方に関係する検討ポイント

情報窃取
サイト改ざん

例）情報窃取のみに関係する検討ポイント

情報窃取
サイト改ざん

関連するチェック項目

23年6月に公開された「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（医療機関確認用）」における、どのチェック項目と重点的に関連付けて検討を行うべきかを示している。

例）チェック項目番号の「2-(7)」「2-(9)」と関係のある検討ポイント

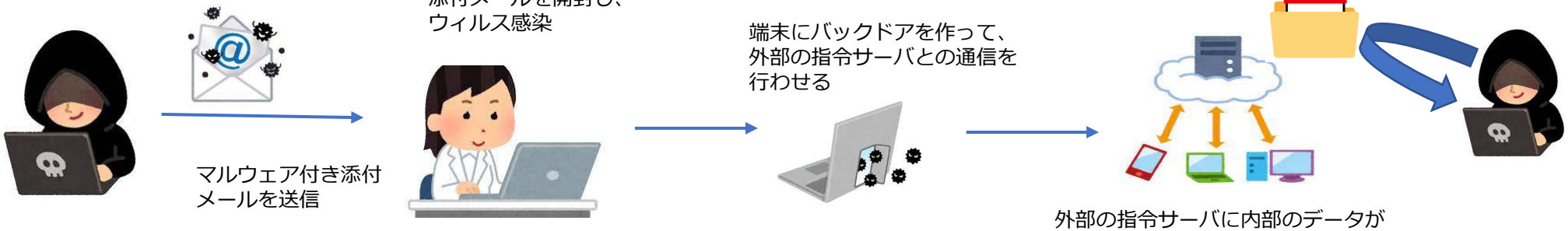
関連するチェック項目： 2-(7) 2-(9)

２.本書の対象範囲

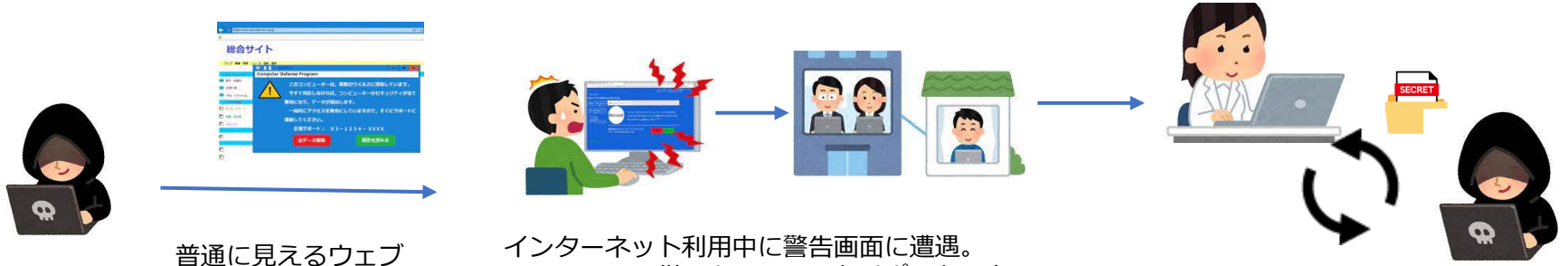
2．本書の範囲(1/2)～情報窃取型攻撃について

今回検討ポイントを追加的に解説する、情報窃取目的のサイバー攻撃のイメージは以下の通り。
何らかのツールを用いて、端末に裏口または正面いずれかから侵入を試みるものである。

ウイルス添付型メール攻撃のイメージ（悪意あるツールで裏口から侵入する手法）

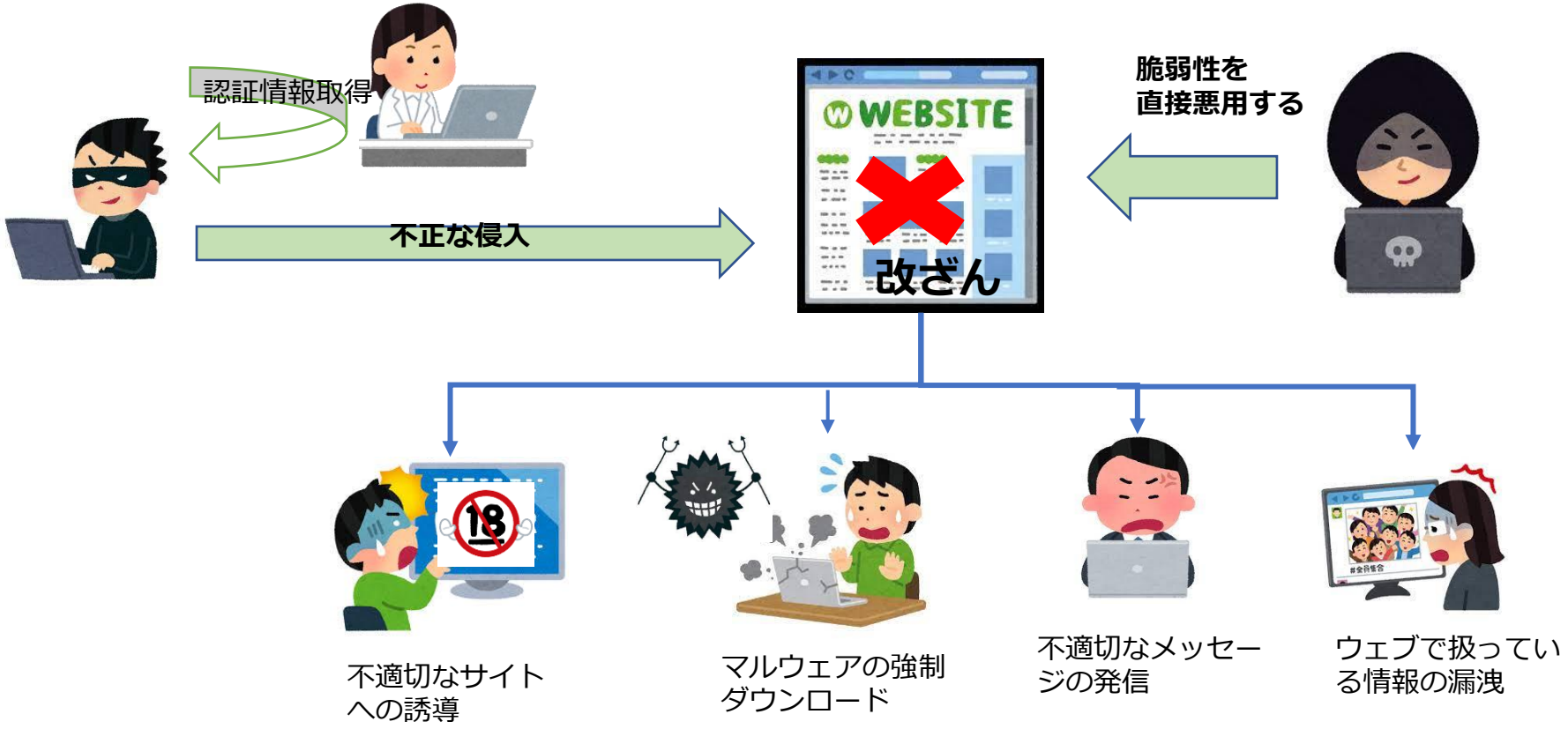


サポート詐欺型の攻撃イメージ（正規のツールで、正面から侵入する手法）



2．本書の範囲(2/2)～ウェブサイト改ざん攻撃について

追加検討対象とするウェブサイトの攻撃の一般的な内容は以下の通り。
おおむね、ウェブサイト本体の技術的な脆弱性を突いた攻撃、またはウェブサイトの管理端末（コンテンツマネジメントシステム：CMS含む）を介した不正侵入を介した、様々な被害がもたらされる。



３.検討ポイント概要

3．<落とし穴>回避に向けた検討ポイント概要(1/2)

情報窃取/サイト改ざん被害対応に際して国内の医療機関が陥りやすい<落とし穴>、及びそれを回避するための検討ポイントの概要は以下の通り。各ポイントは情報窃取/改ざん/双方共通の三つの区分で分類している。
なお、**⑥～⑧は医療ランサム検討対応ガイダンスの各検討ポイントの内容を、今回の攻撃種別に応じた観点を踏まえた対応を行うこと**。

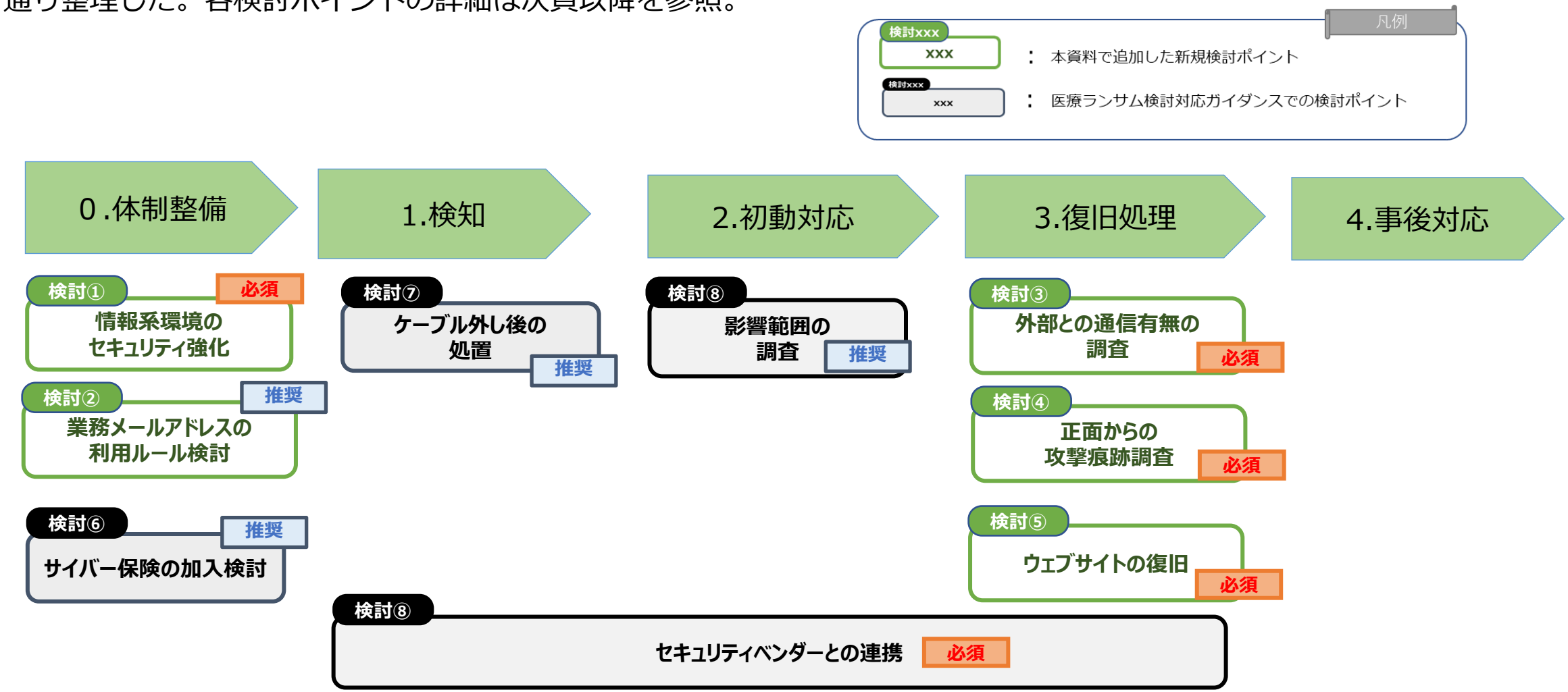
陥りやすい<落とし穴>

落とし穴回避に向けた検討ポイント（概要）

	陥りやすい<落とし穴>	落とし穴回避に向けた検討ポイント（概要）		
①	患者データを取り扱わない情報系端末のため、セキュリティを特に意識していなかった	インターネットとの接続点を持つ情報系環境に適したセキュリティ対策を考えていたか		情報窃取 サイト改ざん
②	院内の業務メールアドレスを外部のニュースサイトやECサイトに登録していたら、そこから情報漏洩が発生した	業務用メアドを個人目的で利用することに伴う漏洩リスクを考えているか		情報窃取 サイト改ざん
③	被害端末はクリーンインストールして初期状態にもどしたので、もう大丈夫	外部との不審な通信がないかまで確認したか		情報窃取 サイト改ざん
④	最新のパターンファイルでウィルススキャンして異常がなかったので、職員には注意するよう指示して、そのまま端末を利用した	用途不明なツール・機能が急に有効になっていたりしないか		情報窃取 サイト改ざん
⑤	ウェブサイトが改ざんされたが、プログラムやファイルをウイルススキャンしたが問題なかったため、そのまま再利用した	ウェブサイト内のファイルやプログラムは改ざんされていないか		情報窃取 サイト改ざん
⑥	情報漏洩被害の復旧コストが想定より高額に	*復旧費用の補填も行うサイバー保険は検討したか*	*ランサムガイダンス 検討④参照*	情報窃取 サイト改ざん
⑦	感染した端末は急いでケーブルを抜いて、シャットダウンした	*被害端末の取り扱いは十分か*	*ランサムガイダンス 検討⑥参照*	情報窃取 サイト改ざん
⑧	どの業者に被害対応のお願いをすればよいかわからないので、とりあえず自院の電カルを担当する業者に連絡した	*正しい影響範囲を精査できるセキュリティ専門ベンダーの目星はついているか*	*ランサムガイダンス 検討⑦・⑧参照*	情報窃取 サイト改ざん

3．<落とし穴> 回避に向けた検討ポイント概要(2/2)

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た。各検討ポイントの詳細は次頁以降を参照。



４.各検討ポイント詳細

４．検討ポイント詳細

～その①：情報系環境のセキュリティ強化(1/2)

情報窃取

サイト改ざん

経営層

管理責任者

一般利用者

関連する対策番号：0-1

関連するチェック項目：2-(7)

国内の医療機関は診療系/情報系（非診療系）の環境をネットワーク分離し、患者診療に直結する前者の環境のセキュリティを重視する。ただ、現行のサイバー脅威を考えれば、外部と直接的に接続する情報系の環境（メール問い合わせ環境、ウェブサーバ等）のほうが、**外との接点を広く持つという意味で本質的にセキュリティリスクは高い。**

そのため、インターネット接続度の高いメール端末には、**診療系端末以上に徹底したセキュリティ対策**を講じることが必要である。

①：陥りやすい落とし穴

患者データを取り扱わない情報系端末のため、セキュリティを特に意識していなかった

診療系ネットワーク上の端末は、やはり患者さんの情報を取り扱うから、ちゃんとセキュリティやらないと！！

インターネット経由のメール問い合わせ窓口の情報系端末のセキュリティはそれほど気に留めていなかった・・・
その結果、感染！！！

必須 検討すべきポイント

常にインターネットという外部と接する、情報系の端末には診療系以上のセキュリティ対策を実施すること

■考え方

インターネットと常時接続を前提とする情報系環境におけるシステム・端末のセキュリティは、診療系以上に、しっかりとした対策を講じること

４．検討ポイント詳細
～その①：情報系環境のセキュリティ強化(2/2)

サイバーセキュリティとは、**IT環境の衛生管理（ハイジーン）**であり、別に難しい概念ではない。医療面の衛生管理（安全管理）の文脈で考えれば、**むしろ医療関係者のほうがその概念の本質を正確に理解できるポジションにある**。

新型コロナ環境下で、我々は未知のウイルスに備えて、マスク着用、手洗い・うがい、免疫力向上に向けた運動等、様々なウイルス対策を講じた。

同じことをIT環境に当てはめて考えれば、なぜ常にインターネットという＜外＞に触れている情報系環境のセキュリティが、＜外＞と切り離された空間（診療系）よりも、感染リスクが高いのかは自ずと分かるはずであり、そうした意識で自院のセキュリティも向かうべき。

医療面の衛生管理対策（例）

サイバー対策に置き換えると・・・

手を洗おう → 
ウイルスに感染しないように、常時チェックできる仕組みを入れよう！

マスクをしよう → 
感染や攻撃につながる不調ポイント（脆弱性）をなくそう！

うちで過ごそう → 
喫緊の必要なく、インターネットに繋がない（外出しない）ようにしよう！

４.検討ポイント詳細

～その②：業務メールアドレスの利用ルール(1/2)

情報窃取　サイト改ざん

経営層　管理責任者　一般利用者

関連する対策番号：0-1

関連するチェック：項目 1-(1)

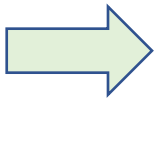
業務目的で院内の職員に付与したメールアドレスが、職員個人の目的で、専門職サイトや情報系サイト等の外部サイトにIDとして登録され、利用されることは多くある。

一方で、**外部サイトが攻撃被害を受け、登録した認証情報が漏洩するリスク**を考慮した場合、「院内メールアドレスを外部サイトでログインIDとして登録しない」「院内ログインIDのパスワードと同一のパスワードを外部サイトで利用しない」「ウェブサイトにログインする管理用IDは院内メールアドレス・パスワードを転用しない」等、**院内メールアドレス自体の利用ルールを病院全体として策定し、職員へ周知徹底することが必要**である。

②：陥りやすい落とし穴

院内の業務メールアドレスを外部のニュースサイトやECサイトに登録していたら、そこから情報漏洩が発生した

病院の業務メアドをもらったので、そのメアドで自己研鑽のため、医療系外部サイトに登録。PWは忘れないように院内IDと同様のPWを利用！！



セキュリティが甘い外部サイトから情報漏洩。メールアドレスとして使ったIDとパスワードがまるまる漏洩・・・

推奨　検討すべきポイント

院内メールアドレスを外部サイトで利用する場合のセキュリティルールをしっかり決め、職員に周知すること

■考え方

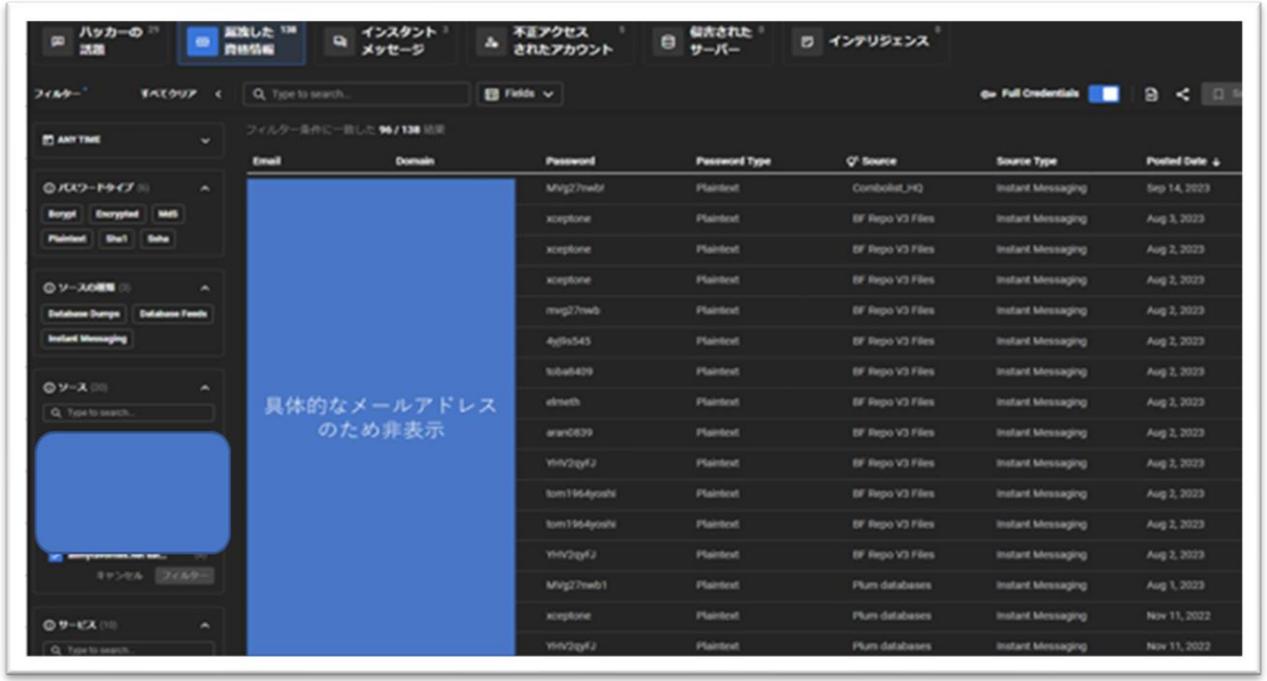
院内のセキュリティをどれほど徹底していても、同一の認証情報が院外の外部サイト等で利用されていると、そこが攻撃を受け、情報漏洩すれば、即座にセキュリティホールになってしまう。

院内業務メールアドレスの外部サイト利用、病院サイトの管理用IDとして利用等のケースを想定して、OK/NGルールを明確化すべき

４.検討ポイント詳細
～その②：業務メールアドレスの利用ルール(2/2)

　ダークウェブではこうしたセキュリティが脆弱な外部サイト、あるいはウェブサイトを管理するツール（コンテンツマネジメントシステム）の脆弱性を起点として漏洩した認証情報が日々やり取りされている。
　例えば、院内業務メールアドレスを用いて、医学系のニュースサイトや関連団体（学会、書籍・雑誌、認定団体等）に登録、あるいはコンテンツマネジメントシステムのログインIDとして利用している場合、**<u>そのアドレス(ID)/パスワードが漏洩すれば、もちろんサイバー攻撃者にとっては病院本体への攻撃を考える上での格好のネタになる。</u>**

＜医療ISAC会員企業(KELA)が提供するサービスで把握した、
ダークウェブ上で取り交わされるメールアドレス/パスワード情報のイメージ図＞



【外部サイトからの漏洩事例】
- ✓ 特定専門職認定団体サイト
- ✓ 医学系専門情報共有サイト
- ✓ 医学専門系書籍サイト
- ✓ 看護情報系サイト
- ✓ コメディカル系情報共有サイト

等

４.検討ポイント詳細

～その③：外部との不審通信有無確認

情報窃取

サイト改ざん

経営層

管理責任者

一般利用者

関連する対策番号：3-1/3-4

関連するチェック項目：2-(8) 2-(9)

標的型メール攻撃により、外部の指令サーバと通信を確立され、データを窃取される攻撃被害を受けた場合、直接的な被害端末を対象にOSベースでクリーンインストールしても、**当該端末とネットワーク接続している他の端末も感染被害を受けていれば、実は適切な修復ができていない**というケースに陥りがちである。

平常時への修復という観点では、感染端末のクリーンインストールのみでなく、**当該端末も含めた周辺の他端末が外部ネットワークと許可していない通信を行っていないかについても調査することが不可欠**である。

③：陥りやすい落とし穴

被害端末はクリーンインストールして初期状態にもどしたので、もう大丈夫

外部通信のリスクが検知されるのであれば、復旧は未完全

必須 検討すべきポイント

被害を受けた本体以外の周辺端末が、本来許可していない外部ネットワークとの通信を行っていないか

■考え方

感染端末のクリーンインストールに加え、**関連する周辺端末が、許可していない外部と勝手にデータ通信をしていないかも確認すること（復旧業者にその点の調査もしっかり依頼すること）**

４.検討ポイント詳細

～その④：正面からの攻撃痕跡調査(1/2)

情報窃取
サイト改ざん

経営層
管理責任者
一般利用者

関連する対策番号：3-1/3-4

関連するチェック項目：2-(5) 2-(9)

悪意ある外部者の攻撃は、標的型メール攻撃を介した裏口侵入でなく、正面からの侵入を狙うものもある。たとえば、その典型が**サポート詐欺**である。インターネットを利用していると、「セキュリティ上の問題あり」等の警告メッセージ・復旧のための連絡先等がブラウザに表示され、そのメッセージに従い、相手（攻撃者）にコンタクトをすると、**攻撃者は業務端末にリモート操作用の正規のツール・機能をインストールさせようとする。**

こうした詐欺の実害を受けた場合、未許可な正規のツール・機能が知らぬ間にオンになっていないかという観点より、端末の状況（もちろんその端末とネットワーク接続している他端末を含めて）を確認する必要がある。

④：陥りやすい落とし穴

最新のパターンファイルでウィルススキャンして異常がなかったので、職員には注意するよう指示して、そのまま端末を利用した

職員がインターネットを利用していたところ、サポート詐欺の被害を受けてしまった

サポート被害の端末はウイルスチェックしても問題なかったので、そのまま利用していた

必須 検討すべきポイント

知らぬ間に、サポート詐欺が利活用するリモートアクセス用のツール･機能が有効になっていないか

■考え方

有効にしていないOSの機能、導入許可していないリモートメンテナンス用のソフトウェアがインストールされていないかを確認することが重要

OS機能やリモートソフトを活用したログイン施行

４.検討ポイント詳細
～その④：正面からの攻撃痕跡調査(2/2)

警視庁もサポート詳細の注意喚起の情報を公開しているため、あわせて確認することが望ましい。

特徴

- 偽のセキュリティ警告画面はウイルス感染の有無に関わらず表示される
- 偽のセキュリティ警告画面には、警告内容を信じさせるために、実在の企業ロゴ等が使われる場合がある
- 警告音を鳴らしたり、警告メッセージを音声で流したり、偽のセキュリティ警告画面を閉じられないようにして不安を煽る
- **偽のセキュリティ警告画面画面に記載されたサポート窓口に電話をかけると、セキュリティソフトを装って遠隔操作ソフト等のダウンロード・インストールへ誘導される**
- 偽のセキュリティ警告画面画面に記載されたサポート窓口に電話をかけると、サポートの必要性があるといい、有料のサポート契約を勧められる
- 支払い方法はクレジットカード決済や各種ギフトカード、コンビニ決済、電子マネー等が使われる

＜警視庁サポート詐欺対策サイト＞

https://www.npa.go.jp/bureau/cyber/countermeasures/support-fraud.html

４.検討ポイント詳細

～その⑤：ウェブサーバの復旧

情報窃取

サイト改ざん

経営層

管理責任者

一般利用者

関連する対策番号：3-1 3-3

関連するチェック項目：2-(9)

　ウェブサーバが改ざん被害を受ければ、当該サーバを構成するファイルやプログラムも知らぬ間に攻撃者により書き換えられている可能性が非常に高い。

　直接的な被害範囲のみを復旧しても、**例えば特定の条件を満たすことで不正なプログラム動作を行うようにソースコード等が潜在的に書き換えられている可能性が非常に高い**ため、**基本的にウェブサイトの復旧に際しては全てのプログラム・ファイル等をゼロベースで入れなおし、再構築する（クリーンインストール）ことが重要**である。

⑤：陥りやすい落とし穴

ウェブサイトが改ざんされたが、プログラムやファイルをウイルススキャンしたが問題なかったため、そのまま再利用した

自院が運営するウェブサイトが改ざんされた！

とりあえず応急処置は終わったので、ウェブサーバ（またはCMSで管理しているファイル類）をウイルススキャンしたが、異常なし。一から再構築するのは面倒なので、そのままファイルは使おう！

またウェブサイトが改ざん！

必須　検討すべきポイント

一度改ざんされたウェブサイトに関するファイルやプログラムはすべて入れなおし、サイトの再構築を行うこと

■考え方

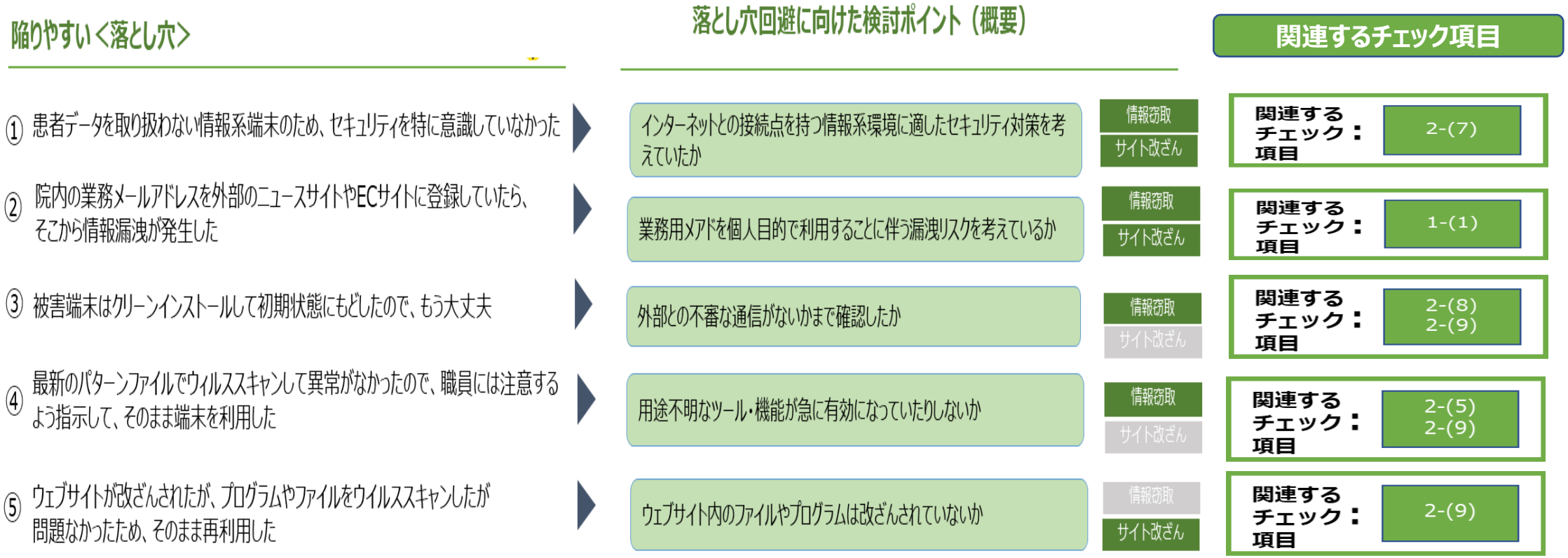
一度汚れた服はすべて洗いなおすように、一度改ざんされたウェブサイトはゼロから洗いなおす

手間暇惜しんで洗い直しをしないと、もっと手ひどい事態になるリスクがたかい・・・
（早期発見・早期治療の精神）

5.「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」(23/6)の観点を踏まえた、各検討ポイントの補足説明

チェック項目を考慮した検討ポイントの考え方

本書で新規追加した5つの検討ポイントは、23年6月に厚生労働省から公開された「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(医療機関確認用）」 のチェック項目と関連付けて考えられる立て付けとしている。
各検討ポイントとチェック項目をどのように関連付けて考えるかについて、「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マニュアル」（以下、「マニュアル」）の解説を踏まえた観点より、補足する。



検討ポイント①について

陥りやすい〈落とし穴〉	落とし穴回避に向けた検討ポイント（概要）		関連するチェック項目
① 患者データを取り扱わない情報系端末のため、セキュリティを特に意識していなかった	インターネットとの接続点を持つ情報系環境に適したセキュリティ対策を考えていたか	情報窃取 サイト改ざん	関連するチェック項目：2-(7)

<チェック項目の内容>

2.医療情報システムの管理と運用-（７）：
「セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。（医療情報システム全般）」

<マニュアルにおける解説>

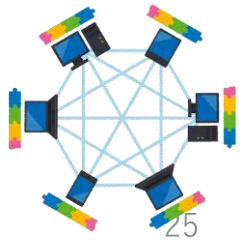
不正ソフトウェアは、電子メール、ネットワーク、可搬媒体等を通して医療情報システム内に侵入する可能性があります。対策としては不正ソフトウェアのスキャ ン用ソフトウェアの導入が効果的であると考えられ、このソフトウェアを医療情報 システム内の端末、サーバ、ネットワーク機器等に常駐させることにより、不正ソフトウェアの検出と除去が期待できます。しかし、不正ソフトウェア対策のスキャン用ソフトウェアを導入し、適切に運用 したとしても、全ての不正ソフトウェアが検出できるわけではありません。このため、**システム運用担当者がまず実施すべき対策として、スキャン用ソフトウェアの導入に加えて、パターンファイルの更新を含め、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セキュリティパッチを適用することが挙げられます**（…）

■検討ポイントとの関連性の補足

左記マニュアルの解説内容は、患者診療に直結する医療情報を取り扱う診療系環境のみでなく、その環境から分離した情報系環境～メール端末やウェブサーバ、予約管理・受付システム等～にも適用される

チェック項目自体は、厚生労働省「医療情報システムの安全管理に関するガイドライン」という、診療系環境を対象とした観点から構成されるため、このような記載であるが、**インターネットと接点のある情報系環境のほうが、ウイルス感染のリスクが高いことは自明**である

よって、**「医療情報システム全般」でなく、「医療機関で取り扱う情報システム全般」という観点に立ち、左記内容を検討する必要がある**



検討ポイント②について

陥りやすい<落とし穴>	落とし穴回避に向けた検討ポイント（概要）		関連するチェック項目
② 院内の業務メールアドレスを外部のニュースサイトやECサイトに登録していたら、そこから情報漏洩が発生した	業務用メアドを個人目的で利用することに伴う漏洩リスクを考えているか	情報窃取 サイト改ざん	関連するチェック項目：1-(1)

<チェック項目の内容>

1.体制構築 -（1）：
「医療情報システム安全管理責任者を設置している」

<マニュアルにおける解説>

医療機関等において、医療機関の経営層は安全管理を直接実行する医療情報システム安全管理責任者を設置する必要があります。
医療情報システム安全管理責任者としての職務は、**情報セキュリティ方針の策定及び教育・訓練を含む情報セキュリティ対策を推進すること**です。
（…）

■検討ポイントとの関連性の補足

院内メールアドレスの利用ルールはセキュリティに無関係に思えるが、**攻撃者はこうした＜まさか！＞という着眼点**から、組織内部へ侵入する手法を開発する

院内メールアドレスを外部サイトで利用する場合のOK/NGルールは安全管理責任者が策定し、職員に周知する責務を負う。
そうしたルールを策定し、入所時、または定期的なセキュリティ研修で教育することで、外部攻撃者による侵入リスクを低下させる必要がある

検討ポイント③について

陥りやすい<落とし穴>	落とし穴回避に向けた検討ポイント（概要）		関連するチェック項目
③ 被害端末はクリーンインストールして初期状態にもどしたので、もう大丈夫	外部との不審な通信がないかまで確認したか	情報窃取 サイト改ざん	関連するチェック項目：2-(8) 2-(9)

<チェック項目の内容>

2. (8)： 「 接続元制限を実施している。（ネットワーク）」	（…）システム運用担当者は、例えば、ネットワーク機器に接続出来る MAC アドレスが限定すること等、**不正アクセス対策を実施してください**。
2. (9)： バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。（サーバ、端末 PC）」	（…）システム側の脆弱性を低減するため、まずは利用していないサービスや通信ポートを非活性化させることが重要です。**システム運用担当者はプログラム一覧やタスクマネージャー等で不要なソフトウェアやサービスが作動していないかを確認し、不要なものがある場合は企画管理者に相談の上、対策を講じてください**。（…）

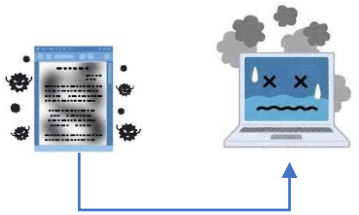
検討ポイントとの関連性の補足

通信先制限によるデータ漏洩防止

通信元制限による感染防止

情報窃取型への攻撃に感染したリスクシナリオにおいては、接続元の制限のみでなく、**外部への不審なデータ通信を行うプログラムの制限（ネットワークレベルでは通信先制限）が必須**

クリーンインストールした端末で動作するプログラムはすべて許可されているものである必要がある。**未許可のプログラム（怪しいプログラム）はすべて停止すべき。**



不正プログラムのバックグラウンド動作

検討ポイント④について

陥りやすい〈落とし穴〉	落とし穴回避に向けた検討ポイント（概要）		関連するチェック項目
④ 最新のパターンファイルでウィルススキャンして異常がなかったので、職員には注意するよう指示して、そのまま端末を利用した	用途不明なツール・機能が急に有効になっていたりしないか	情報窃取 サイト改ざん	関連するチェック項目：2-(5)、2-(9)

<チェック項目の内容>

2. (5):
「退職者や使用していないアカウント等、不要なアカウントを削除している。（サーバ、端末 PC）」

2. (9)：
バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。（サーバ、端末 PC）」

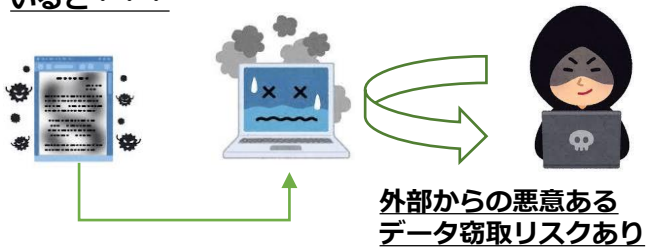
<マニュアルにおける解説>

企画管理者は２（４）で整理した情報を元に、退職者や使用していない ID 等が含まれていないかを確認してください。**長期間使用されていない等の不要な ID は不正アクセスに利用されるリスクがありますので、速やかに削除してください**。（…）

（…）システム側の脆弱性を低減するため、まずは利用していないサービスや通信ポートを非活性化させることが重要です。**システム運用担当者はプログラム一覧やタスクマネージャー等で不要なソフトウェアやサービスが作動していないかを確認し、不要なものがある場合は企画管理者に相談の上、対策を講じてください**。(…)

検討ポイントとの関連性の補足

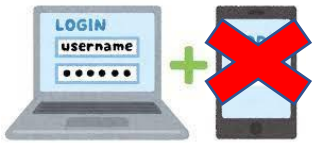
ウイルス感染＝よくわからないプログラム・タスクが動作していると・・・



外部からの悪意あるデータ窃取リスクあり

ウイルスは端末に不適切なソフト・サービスとしてバックグラウンドで稼働し、外にデータを送信しようとする

本来想定外のログインアカウントが登録されている場合、攻撃目的で登録された可能性がある。そのため、本来登録しているアカウントをちゃんと把握し、不審なアカウントの有無をチェックできるようにする必要がある



検討ポイント⑤について

陥りやすい<落とし穴>	落とし穴回避に向けた検討ポイント（概要）		関連するチェック項目
⑤ ウェブサイトが改ざんされたが、プログラムやファイルをウイルススキャンしたが問題なかったため、そのまま再利用した	ウェブサイト内のファイルやプログラムは改ざんされていないか	情報窃取 サイト改ざん	関連するチェック項目：2-(9)

<チェック項目の内容>

2. (9)：
バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。（サーバ、端末 PC）」

<マニュアルにおける解説>

（…）システム側の脆弱性を低減するため、まずは利用していないサービスや通信ポートを非活性化させることが重要です。**システム運用担当者はプログラム一覧やタスクマネージャー等で不要なソフトウェアやサービスが作動していないかを確認し、不要なものがある場合は企画管理者に相談の上、対策を講じてください**。（…）

■検討ポイントとの関連性の補足

ウイルス対策ソフトでスキャンしても検出できない、正規のツールで外部との通信経路が確保されているパターンが最近は多い。
そのため、本来必要のない未許可のソフトウェアやサービスは停止することが重要。

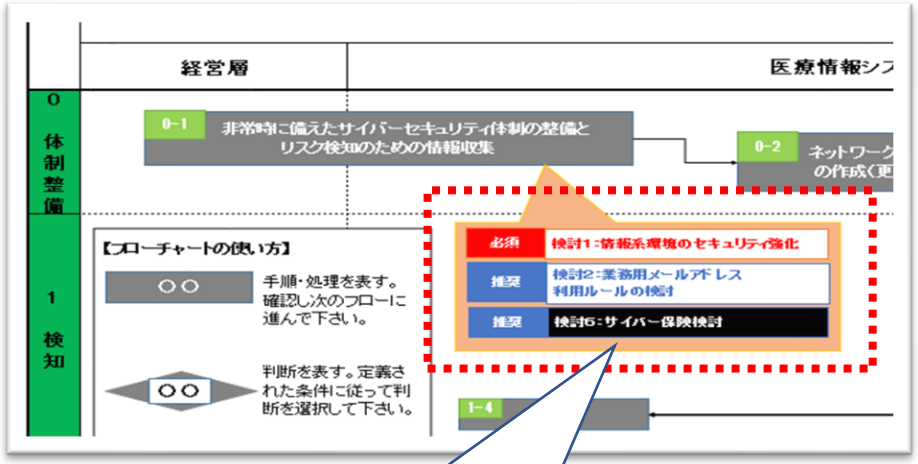
ウェブサイトのバックアップは、周辺サーバや管理端末内部で保存される傾向が多い。
こうしたバックアップも、未許可のサービス等を介した攻撃による感染被害を受ければ、ウイルスの卵を植え付けられているリスクがあることには留意が必要

(別添）情報窃取/サイト改ざん対応検討フローチャート

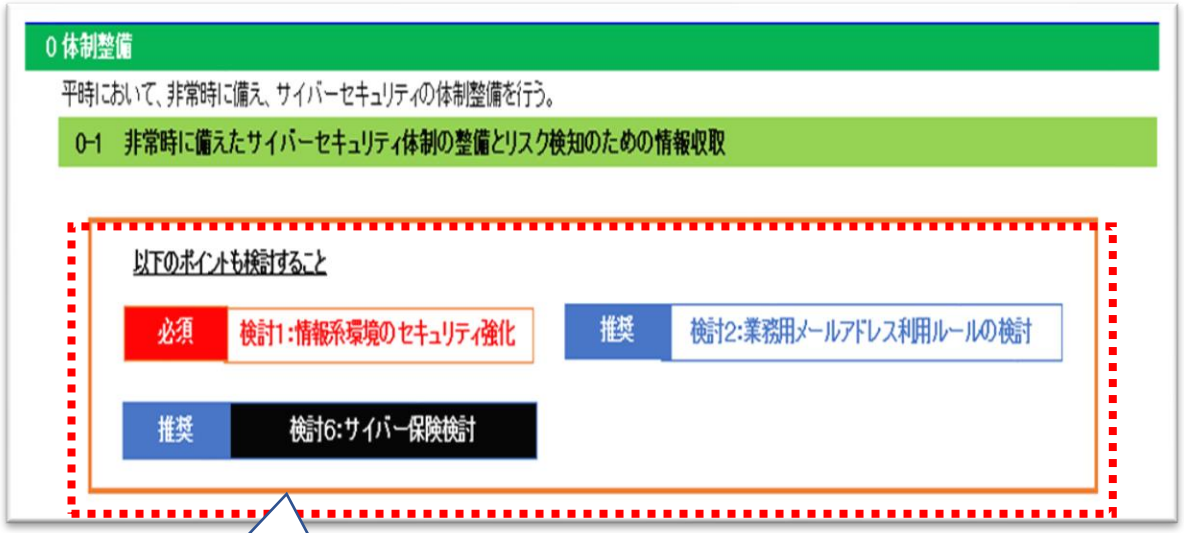
医療ランサム対応ガイダンス同様、本資料で解説した情報窃取/ウェブサイト改ざんに備えた検討ポイントを厚労省対応フローチャートに埋め込み、対応検討ポイントを把握できる**別添資料**も整理している。

当該別紙も利活用し、情報窃取やウェブサイト改ざんの未然防止、あるいは被害発生時の復旧対応を検討することが推奨される。

■（別添）情報窃取/サイト改ざん対応検討フローチャート



「フローチャート」シート上の
各手順に関連する検討ポイントの表示



「対応記述」シート上に、
関連する検討ポイントを表記