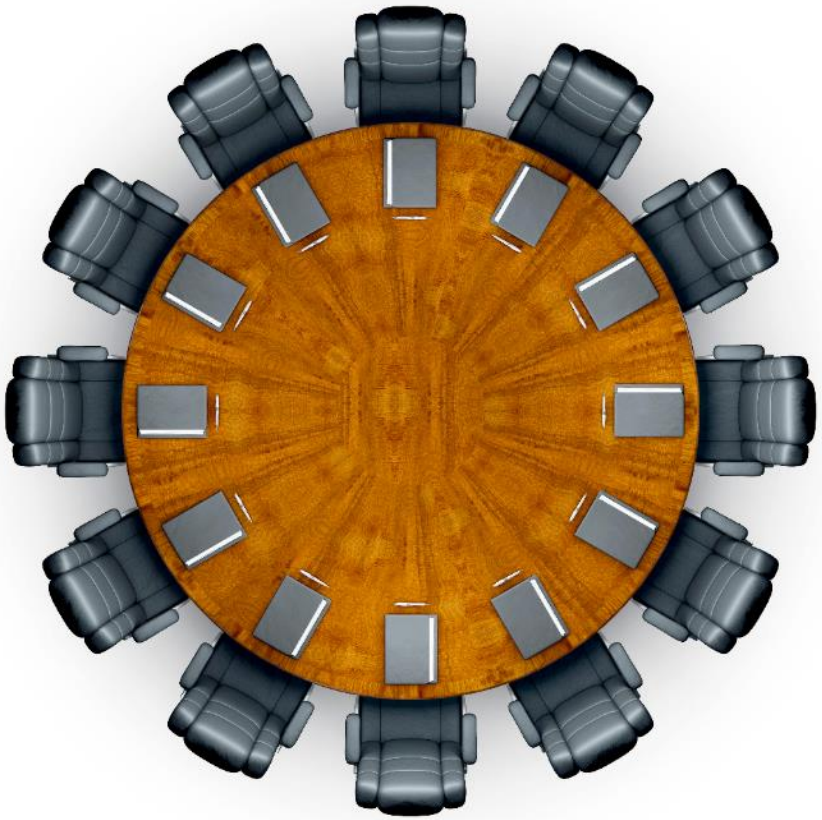
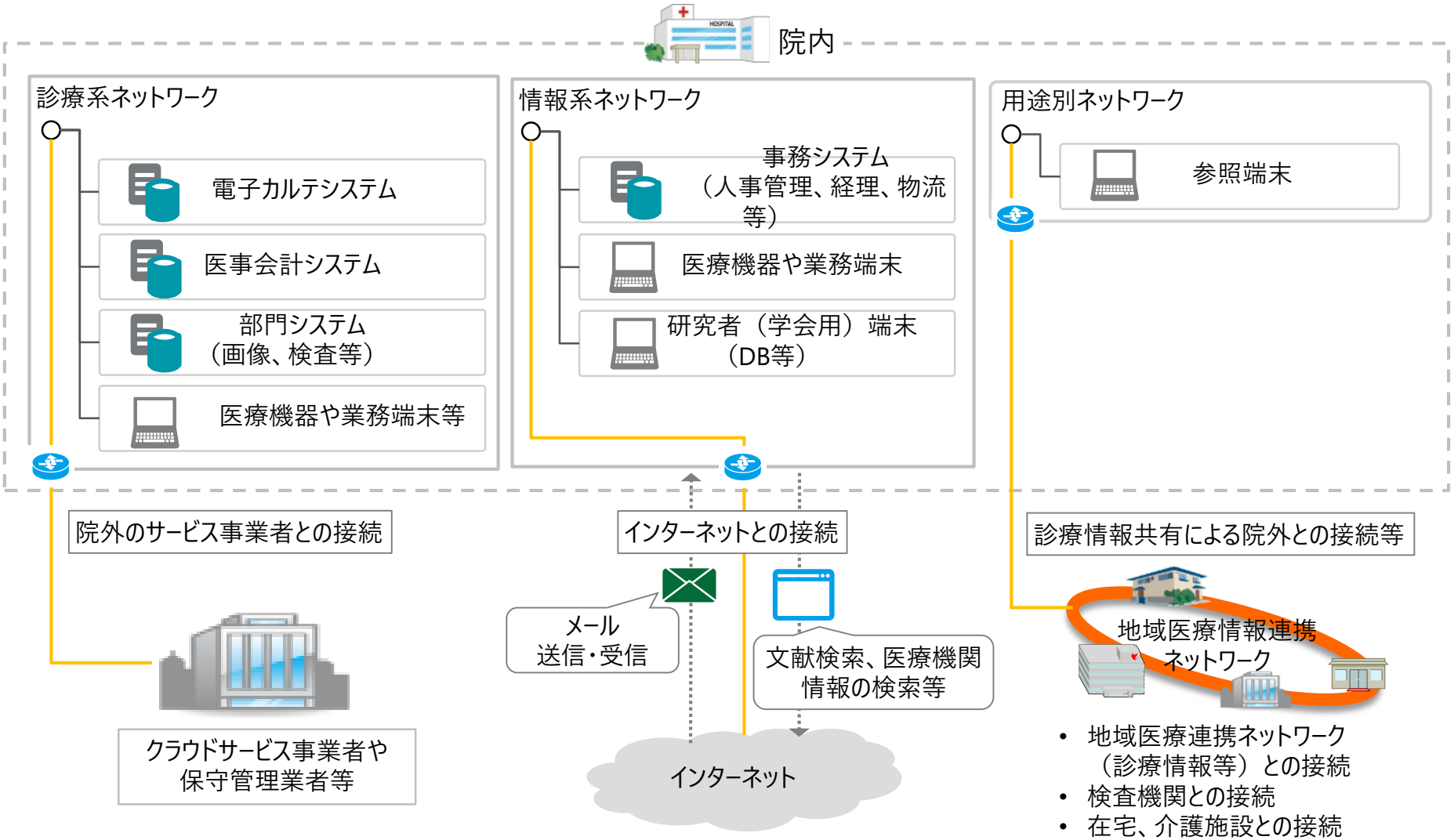


「情報セキュリティ研修教材（システム管理者向け）」

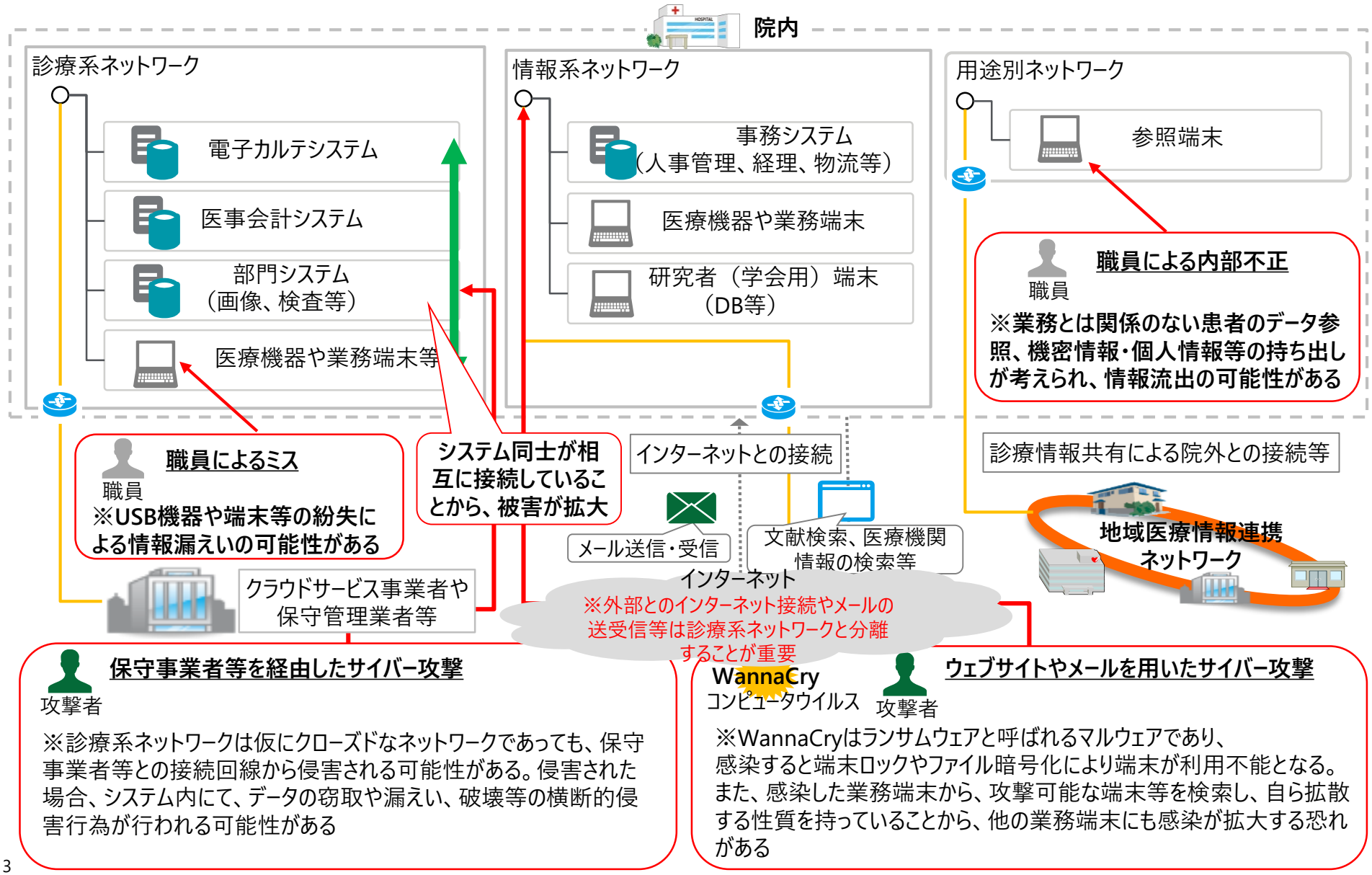
目次

第1章　医療機関におけるIT化について

院内の情報化の進展により、医療機関は様々な情報システムの導入や院外ネットワークとの接続を行っており、現場で複雑化している



医療機関の様々な現場で情報セキュリティインシデントリスクの脅威にさらされており、現場で異常を感じたら速やかに報告する体制づくりが重要である



第1章のまとめ

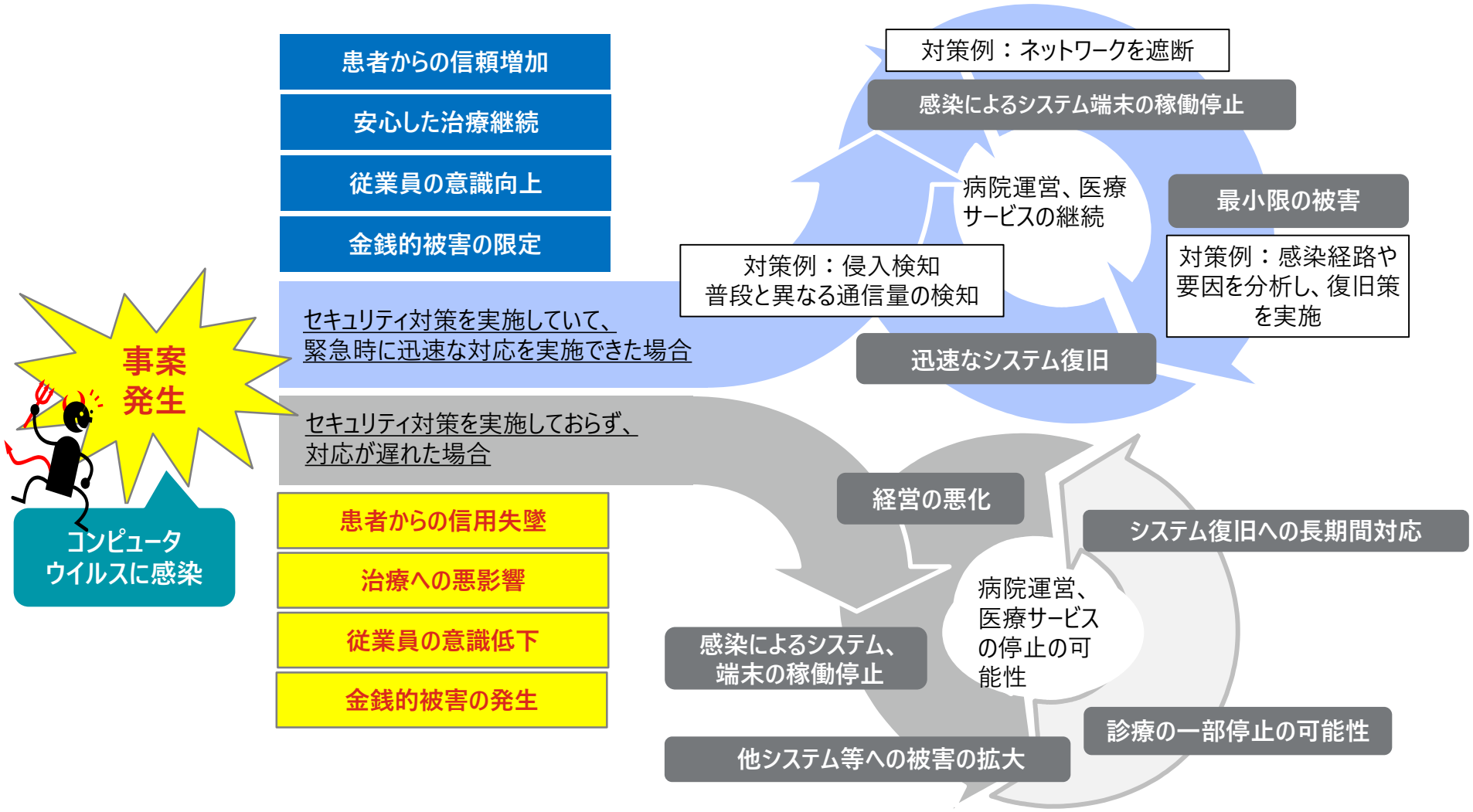
院内の情報化の進展により、医療機関は様々な情報システムの導入や院外ネットワークとの接続を行っており、現場で複雑化している

医療機関の様々な現場で情報セキュリティインシデントリスクの脅威にさらされており、現場で異常を感じたら速やかに報告する体制づくりが重要である

システム管理者は、現場の職員からの報告を受けたら、迅速に異常の原因調査や被害拡大の防止に向けて取組することが必要となる

第2章　情報セキュリティの重要性について

医療機関のIT化が進んだ現在では、情報セキュリティ事故は、医療機関の事業継続や存続に影響する経営課題であり、経営者のリーダーシップで対策を進める必要がある



情報セキュリティ対策は、国や各種団体が発信している様々な情報を収集することが基本である

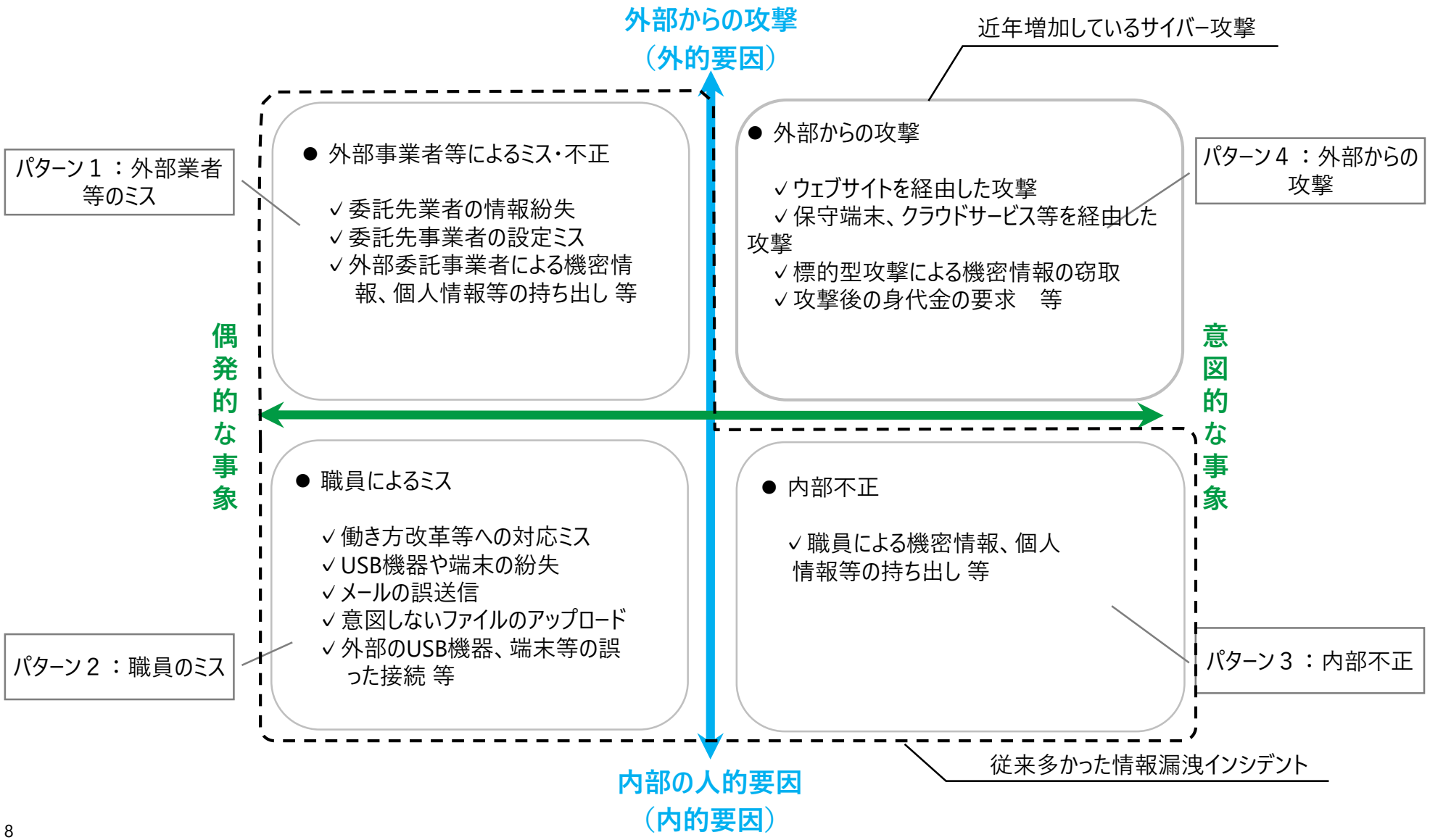
例1　各種ガイドライン等

名称	提供元
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版）※1 ※1　第5.1版への改訂素案が検討されている	厚生労働省
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	経済産業省・総務省
医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス	厚生労働省
情報セキュリティハンドブック	内閣サイバーセキュリティセンター
サイバーセキュリティ経営ガイドライン（Ver2.0） 等	経済産業省

例2　独立行政法人情報処理推進機構（IPA）が公表している「情報セキュリティ10大脅威2020」

順位	個人	組織
1位	スマホ決済の不正利用	標的型攻撃による機密情報の窃取
2位	フィッシングによる個人情報の詐取	内部不正による情報漏えい
3位	クレジットカード情報の不正利用	ビジネスメール詐欺による金銭被害
4位	インターネットバンキングの不正利用	サプライチェーンの弱点を悪用した攻撃
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	ランサムウェアによる被害
6位	不正アプリによるスマートフォン利用者への被害	予期せぬIT基盤の障害に伴う業務停止
7位	ネット上の誹謗・中傷・デマ	不注意による情報漏えい（規則は遵守）
8位	インターネット上のサービスへの不正ログイン	インターネット上のサービスからの個人情報の窃取
9位	偽警告によるインターネット詐欺	IoT機器の不正利用
10位	インターネット上のサービスからの個人情報の窃取	サービス妨害攻撃によるサービスの停止

従来は、「職員のミス」「内部不正」に加えて、近年は外部からの攻撃である「サイバー攻撃」も増加している



医療機関の情報化に伴う業務環境の変化に対して十分な対策がとれていないことや、攻撃者の手法の進歩により、情報セキュリティインシデントは増加傾向にある

医療機関における情報化の動向

院内の情報化に伴う業務環境の変化
- 医療情報システムの導入に伴う業務環境の変化（業務端末の増加、情報システム規定類・マニュアル等の整備等）

情報セキュリティ対策の不足
- 情報システム管理部門、担当者の不足
- 情報セキュリティ対策の不足
- 職員に対する教育訓練の不足

ICT技術の進展に伴う院外との接続の増加
- 外部との診療情報の共有
- インターネットの利用
- グループウェアサービス（メール、共有フォルダ）の利用
- オンライン診療の増加
- 認められていないツールの導入等

医療等分野の更なる情報化の進展（想定）

・・・

外部事業者の管理不足による「**パターン１：外部事業者等のミス**」の発生

職員に対する教育訓練不足による「**パターン２：職員によるミス**」の発生

システムや業務端末の管理不足による「**パターン３：内部不正**」の発生

攻撃者

攻撃手法の進歩

「**パターン４：外部からの攻撃（サイバー攻撃）**」の発生

情報セキュリティインシデントの増加

外部事業者に任せきりにすることはリスクであり、外部事業者に任せきりでなく、外部事業者を管理することが重要である

事例	発生国	被害組織	内容
委託先業者の情報紛失・設定ミス	日本	S病院	• 設定ミスにより、患者70人分の個人情報が含まれたファイルがインターネットを経由しアクセス可能な状態となり、個人情報が漏えいする恐れがあった
	オーストラリア	オーストラリア政府（My Health Record）	• 外部委託業者によるシステム設定不備により、システムの管理者用ID、パスワードなどが公開された状態であり、個人の健康記録が漏えいする恐れがあった

外部委託先との責任範囲の明確化

ポイント　外部委託先と責任範囲や実施すべき情報セキュリティ対策を明示する

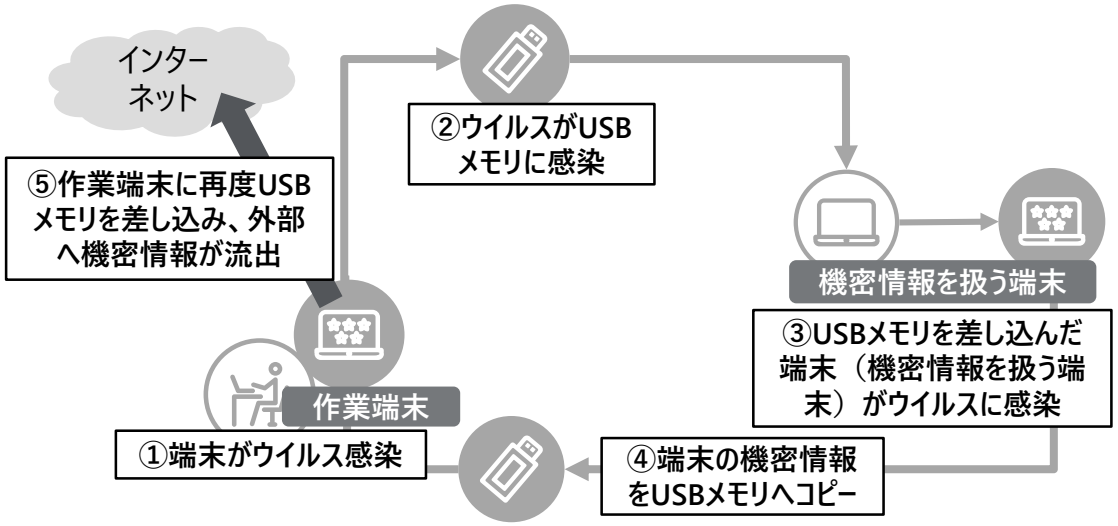
明示の例

- ■ 機密情報の利用、保管、持ち出し、消去、破棄における取り扱い
- ■ 情報へのアクセス者の限定
- ■ 定期的なバックアップの実施とバックアップ媒体の機密区分に応じた管理
- ■ 情報セキュリティ対策に係る内部点検の実施と結果の報告
- ■ 再委託の事前承認の徹底
- ■ 私用PCの業務利用の禁止
- ■ 機密情報を保管および扱う場所の入退室管理と施錠管理
- ■ 業務に不要なWEBサイトへのアクセス禁止
- ■ 定期的なウイルス検査の実施
- ■ 脆弱性の解消（アップデート等の実施）
- ■ ID・パスワード管理
- ■ 情報漏えいの発生時の迅速な報告義務や再発防止策の提示等

同等かそれ以上のセキュリティ対策を
外部委託先に求めることが基本

外部媒体は情報持出のリスクだけでなく、外部媒体を介したウイルス感染も留意が必要である

事例	発生国	被害組織	内容
USB機器や端末の紛失	日本	A医学部付属病院	• 総合内科・総合診療科で患者約1万3千人分の個人情報を記録したUSBメモリを紛失した • 持ち運びできる媒体への情報保存はマニュアルで禁止されていたが、医師はマニュアルの存在を知らなかった
		B市立病院	• 医師が、患者約330人分の手術記録を保存したUSBメモリーを紛失した • 病院は個人情報の外部への持ち出しは禁止しているが、無断で自宅に持ち帰っていた • 情報の流出や悪用は確認されていないが、警察に遺失物届を提出した
		C医科大学病院	• 薬剤師が、糖尿病・内分泌・代謝内科を受診した患者3,835人の氏名や生年月日などの個人情報が入ったUSBメモリーを紛失した • 情報の流出は確認されていないが、同病院は患者に文書で謝罪し、警察に遺失物届を提出した



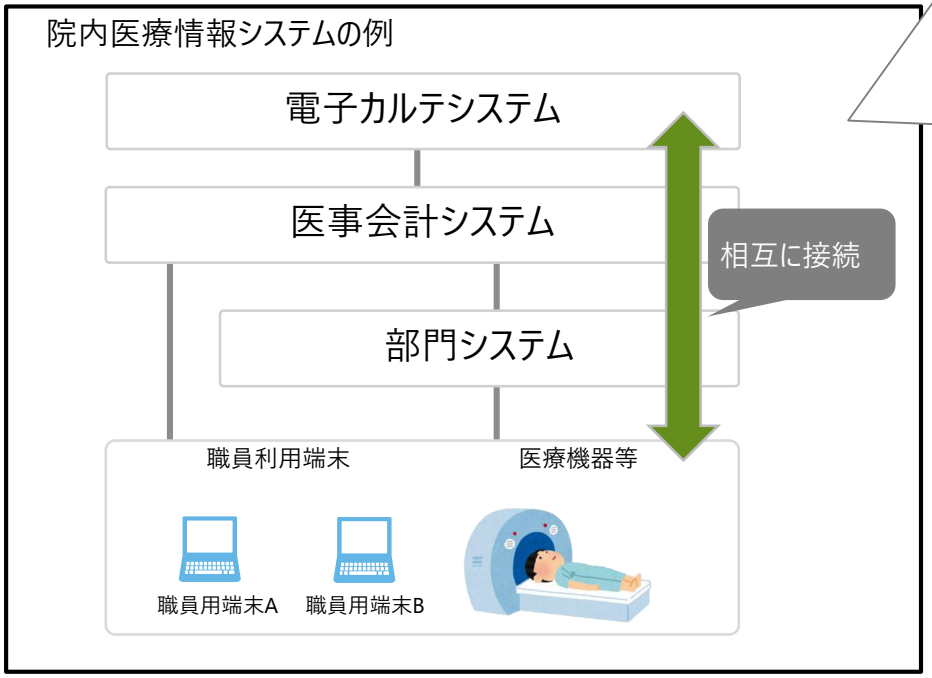
防御策の例

- ■ 従業員個人のUSBメモリ等の外部媒体の使用を禁止する
- ■ 業務上、外部媒体の使用が必要な場合は事前申請とし、法人管理の外部媒体を使用する
- ■ 法人の外部媒体は、ウイルスチェック機能やパスワードロック機能、生体認証等のセキュリティ対策機能がある媒体を使用する
- ■ 外部媒体の外部持出は原則禁止とし、外部媒体は予め定められた場所で保管する　　等

OS等のアップデートは、セキュリティ対策に欠かせません。ただし、医療機関では様々なシステムが連携していますので、現場で勝手にアップデート等をしないように適宜指示をすることが重要です

【アップデートとは】

- ソフトウェアを最新の状態に更新することを「アップデート」といいます。アップデートを行うと不具合（バグ）を直したり若干の機能向上などが行われます。
- パソコンやサーバのOSのアップデートは、情報セキュリティの面から重要な意味を持ちます。OSなどには、「セキュリティホール」と呼ばれる不具合（バグ）が発見されることがあります。「セキュリティホール」はソフトウェアの設計ミスによって発生するセキュリティ上の欠陥のことを指します。このセキュリティ上の弱点ともいえる「セキュリティホール」を修復するためのプログラムを更新します。アップデートすることで、セキュリティホールが修復し安全な状態になります。



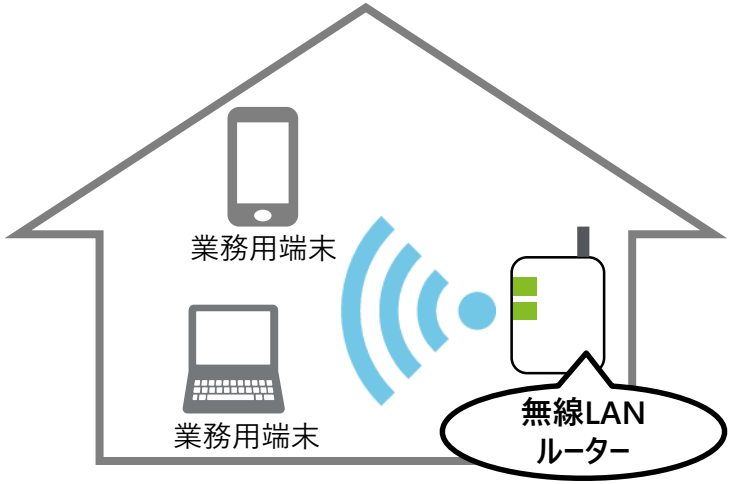
【医療情報システムの特徴】
- ■ 電子カルテシステムや医事会計システム、部門システムなどのシステム同士が相互に接続
- ■ 部門システムと医療機器が相互に接続
- ■ 職員利用端末からは、電子カルテシステムや部門システムなど様々なシステムにアクセス

【アップデートを行う際の留意点】
- ■ 医療機関では様々なシステムが連携しているため、OS等のアップデートを行うことで、一部のシステムを正常に利用できなくなる可能性がある
- ■ セキュリティの面から重要なアップデートが必要な場合は、正常な動作確認の観点から外部委託業者の協力を得て進める必要があるため、システム調達時にあらかじめ契約書等で定めておくことが望ましい

対応策の例

業務用パソコンやスマートフォンなどでアップデートの通知が届いた場合は以下の対応を実施する
- ■ 院内の情報システム部門または担当者に確認する
- ■ 事前に情報システム部門より、対応方法の連絡がある場合は指示に従う

無線LANアクセスポイントにおいて、ユーザー名やパスワードを設定し、かつ通信の暗号化を設定することが重要です。システム管理者は、医療従事者へ無線LANの運用について適時に指示をしてください



- ノート型パソコンやスマートフォン、タブレット端末などの普及を背景に、インターネットに接続する手段として、無線LANの利用が拡大している
- 情報セキュリティ対策を施していない無線LANは危険性が高く、通信内容を盗み見られる等の危険がある

【無線LANの危険性の例】
■ 個人情報、機密情報の漏洩
勝手に接続した第三者の端末から、パソコンの共有フォルダなどが見られてしまう
■ ID/パスワードの漏洩
セキュリティ対策をしていない無線LANから第三者が侵入し、内部で解析後、ID/PWが盗まれる（さらに悪用された場合、医療情報システムへの不正アクセスや迷惑メールの送信元にされる場合もある）

対応策の例

ユーザ名、パスワードの設定	■ 無線LANアクセスポイントには、ユーザ名（SSID：Service Set Identifier）とパスワードの設定を行う。パスワードを掲示等を擦る場合は解読リスクがあることを認識する）
暗号化方式の設定	■ 通信の防御策として暗号化設定が有効である ■ WPA2による暗号化や端末から接続先までを暗号化する「HTTPS」、「VPN」の活用
無線LANルーターの定期的な買い替え及び設定（ファームウェア）の更新	■ 無線LANルーターを最新のファームウェア（ハードウェアを制御するためのソフトウェア）に更新することで、不具合の修正や機能向上が追加されるため、ファームウェアは常に最新版に更新する、または老朽化しないよう定期的な買い替えを行う

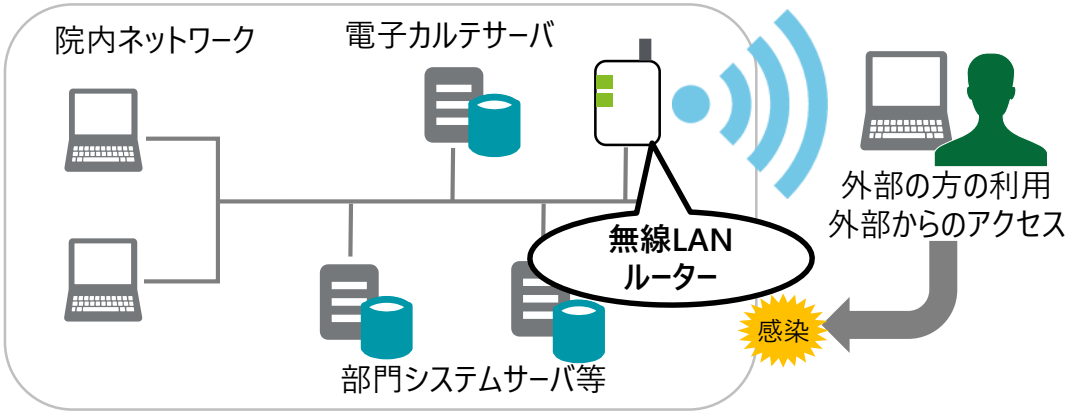
暗号化方式の種類

■ 主に端末とルーター間を暗号化する「WPA」、「WPA2」と端末からルーターを介した接続先までの通信を暗号化する「HTTPS」、「VPN」がある※1

暗号化方式	特徴
WPA	暗号化方式を変更し、WEPを拡張して策定
WPA2	暗号化アルゴリズムや改ざん検知の方式により強固とした方式。現時点では最も強固な暗号化形式
HTTPS（SSL/TLS）	暗号化を用いたセキュアな通信
VPN	暗号化された疑似的なトンネルを用いた通信

※1　その他新しいセキュリティ方式としてWPA3やWi-Fi CERTIFIED Enhanced Openが登場している。

無線LANは気軽に外部からの接続を行うとウイルスやマルウェアが入り込む可能性があります。訪問者用のアクセスポイントを設定し院内ネットワークと分離しておくことが重要です



■ 外部の方が持ち込んだノートPCやタブレットをインターネットに接続したいと要望された場合、院内ネットワークの無線LANを知らせれば接続できるが、訪問者の端末からウイルスやマルウェアが入り込む可能性もある。

【ケースの例】

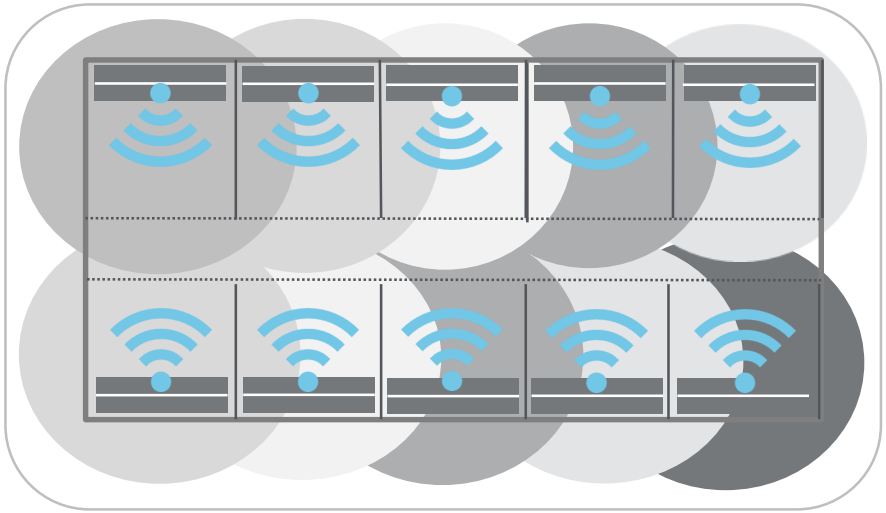
- 講演会の開催にあたり、演者の方が自身のPCを接続したい
- 外部業者が打ち合わせのため訪問した際に、業者のタブレットを接続したい

対応策の例

訪問者用にゲスト用のネットワークの設定	■ 無線LANのゲストポートを有効にして、訪問者用の無線LANアクセスポイントを作成し、外部の方が持ち込んだノートPC等の接続に利用する ⇒これだけの設定では、無線LANのユーザ名とパスワードを入手した訪問者が、訪問後も勝手にゲスト用無線LANに接続できてしまうため、定期的な暗号化キーの変更を行う等の手段を行うことが望ましい
利用者情報の確認アクセスログの記録	■ 誰がいつ無線LANを使用しているのか確認できるように利用者認証を実施したり、事後的な追跡調査が可能になるようにアクセスログを記録する
利用時間の制限や電波出力の調整	■ 接続1回あたりの利用時間の制限等やアクセスポイントが発する電波の出力を調整し、施設内からの利用に限定する等の対応を実施する

電波干渉により医療機器の作動に影響を及ぼす可能性があり、運用の際には無線LANネットワーク事業者と連携して電波環境調査の実施や定期的な保守点検が重要である

例：配慮を欠いた過密なアクセスポイントの設置



- 患者や外部の人間が持ち込む端末や無線通信機能付携帯ゲーム機、管理外の無線LANアクセスポイント等により、電波干渉を起こし、通信障害が発生する可能性がある
- 病院職員がシステム管理者に無断で執務室や手術室等に無線LANのアクセスポイントを設置し、管理されている無線LANアクセスポイントへ電波干渉を与えてしまう事例も報告されている

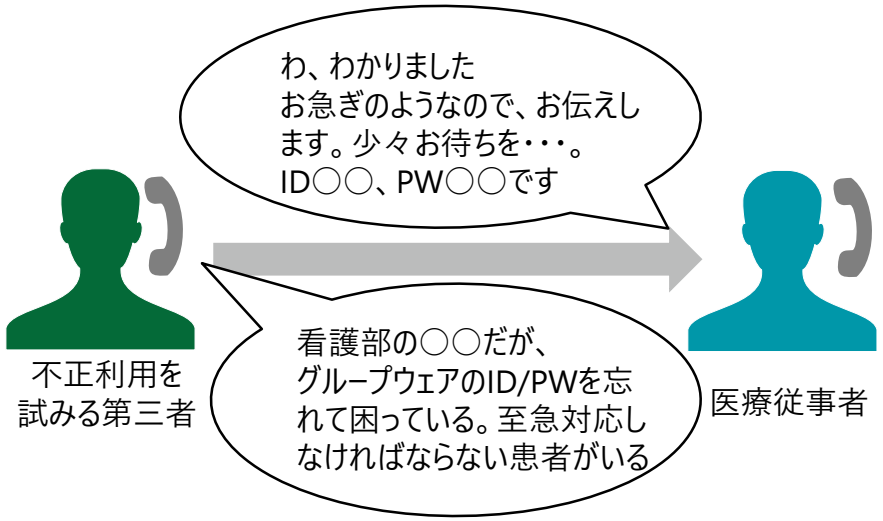
- **医療情報システムの端末装置で通信障害が発生し、機器の稼働が停止する可能性がある**

運用の際の取組例

①電波環境調査のために管理表を作成	■ 無線LANネットワーク事業者から提供された無線LANアクセスポイントの位置と、それぞれの無線チャンネル等の情報が記載された管理表を作成し、保管する
②電波環境調査の実施	■ 管理表に基づいて、チャンネル設定、受信強度、受信状態等に変化がないか確認する ■ 変化がある場合は、設定の変更、建物の増改築、病院内外からの無線LANへ影響を与える機器等の導入等が生じていないか確認し、管理表を更新する
③トラブル内容の記録や原因の特定・対策の実施	■ トラブル内容について、いつ、どこで、どのように発生したか管理表に記録する ■ トラブルの原因が特定される場合は、対策を実施する。原因が不明あるいは対策が困難な場合は、無線LANネットワーク事業者や機器を設置する業者と連携し対応する
④定期的な保守点検の実施	■ 定期的に電波環境調査を実施する ■ 医療機関の施設増築や無線LANのメンテナンス等、機器設定に変更が出る場合には、適切に利用できるように無線LANネットワーク事業者へ予め指示をする

出典：電波環境協議会「医療機関において安心・安全に電波を利用するための手引き（平成28年4月）」

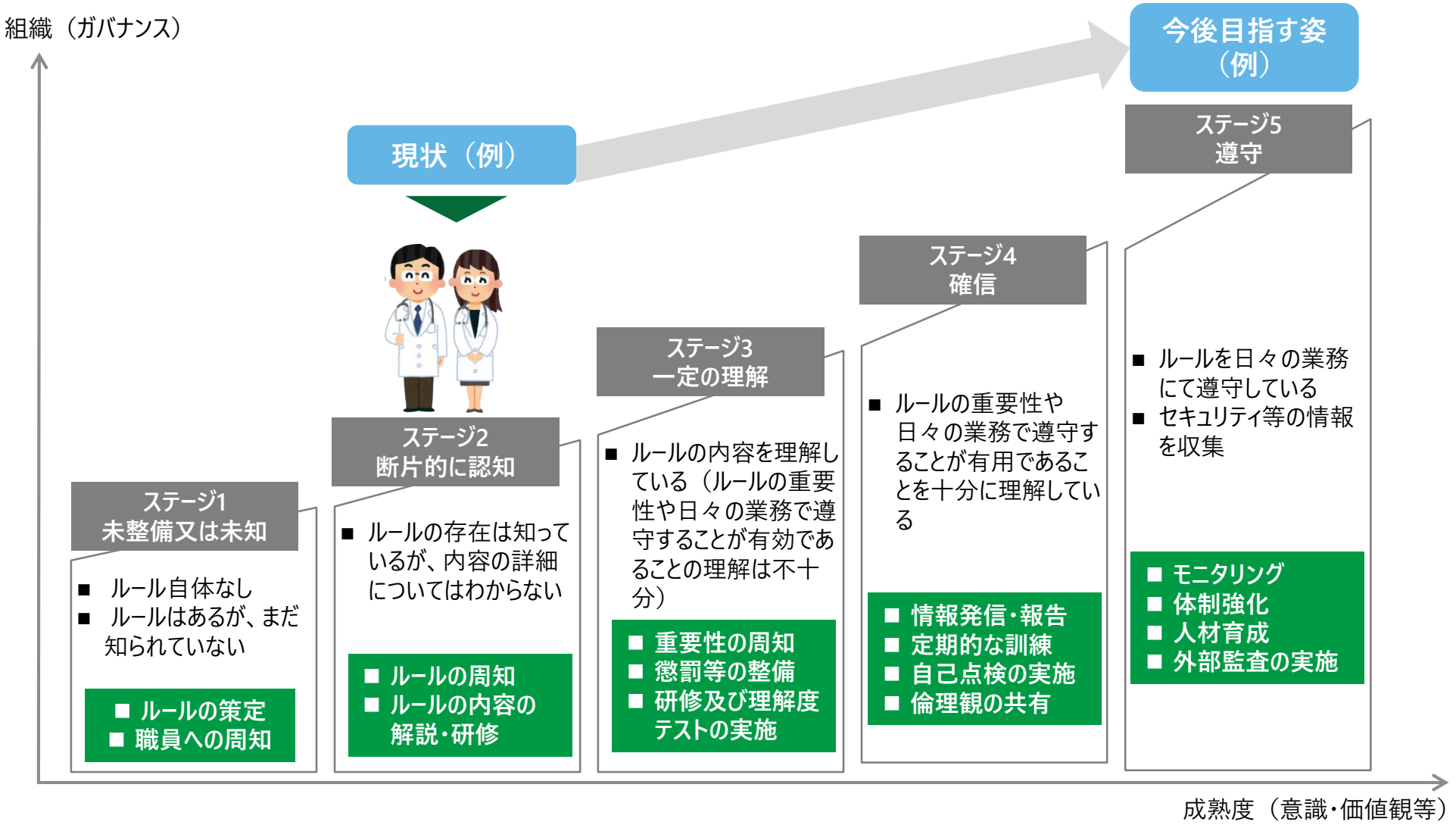
攻撃者は、電話やメールを用いて職員などを装い、心理的に答えざるを得ない状況を作り聞き出そうとするが、即時に対応せず本人確認を行う等の対応方針や規程を準備しておくことが重要です。



- ソーシャルエンジニアリングとは、コンピュータやネットワークに侵入するために必要となるパスワードなどの重要な情報を、人の心理的・社会的な弱点や盲点をついて入手する手法である。
- 電話やメールで、職員や関係者を名乗り、ID やパスワードを詐取する「なりすまし」や、廃棄物から情報を詐取する「トラッシング（ゴミ箱を漁る方法）」などが代表的である。
- 近年、特定の企業等に対して社内の関係者を装ったウイルス付きメールを送信するなどの手口が増加している。

	手口の例	対策の例
電話によるなりすまし	■ 職員になりすまし 職員を装い電話をかけ「ID、パスワードを忘れてしまったので教えてほしい」等といって聞き出す ■ 職員の中でも役員や管理職等になりすまし 標的となる役員や管理職を事前に調べ、その者になりすまし電話をかけ「ログインできない。急いでいる！」等、高圧的な態度を迫り、答えざるを得ない雰囲気を作り聞き出す	➢ 折り返し連絡をし、本人確認を行ったうえで回答する ➢ 電話番号などから本人が特定できない問い合わせには答えない ➢ 上記のほか、病院の情報セキュリティポリシーを整理し、「ID、パスワードの再発行は、本人が直接システム担当部署に出向いて手続きを行う」などの規定を策定しているケースもある
メールによるなりすまし	■ フィッシング詐欺 事業者等になりすまし、メールを送信し偽装したサイトに誘導し、パスワードやクレジット番号などを盗み取る詐欺行為 ■ クリック詐欺 なりすましメール内にあるリンクをクリックさせて、架空請求先のページに誘導する詐欺行為	➢ 差出人のメールアドレスを確認する ➢ リンク先のURLがある場合、公式のものか確認する ➢ 見知らぬ電子メールは注意する（安易にクリックしない等） ➢ 二段階認証を設定し、ID/パスワードが詐取された場合でも簡単にアクセスできない仕組みにする

職員のセキュリティに対する意識の現状を把握し、現状に合わせた対応策を取る必要がある
高度なセキュリティ人材を育成することではなく、一般的なセキュリティ意識を持ち、仕事を進めることが出来る人材を育成していくことが重要である



国内でも内部不正による情報漏えい事例が確認されているが、公表されていない、または、気づかないケースが多く発生している

事例	発生国	被害組織	内容
職員による機密情報、個人情報等の持ち出し	日本	J記念病院	• 元職員が、在職中に患者の個人情報を持ち出し、新しく開設する介護事業所の案内状送付に利用していた

不正のトライアングル

不正の対策例

①権限の縮小と分離
アクセス権限について分類して一人の職員でデータの閲覧から出力等を実施できないようにする

②アクセス時間の制限
機密情報へのアクセスについては、予めアクセス予定時間を申請して承認を取る運用にする

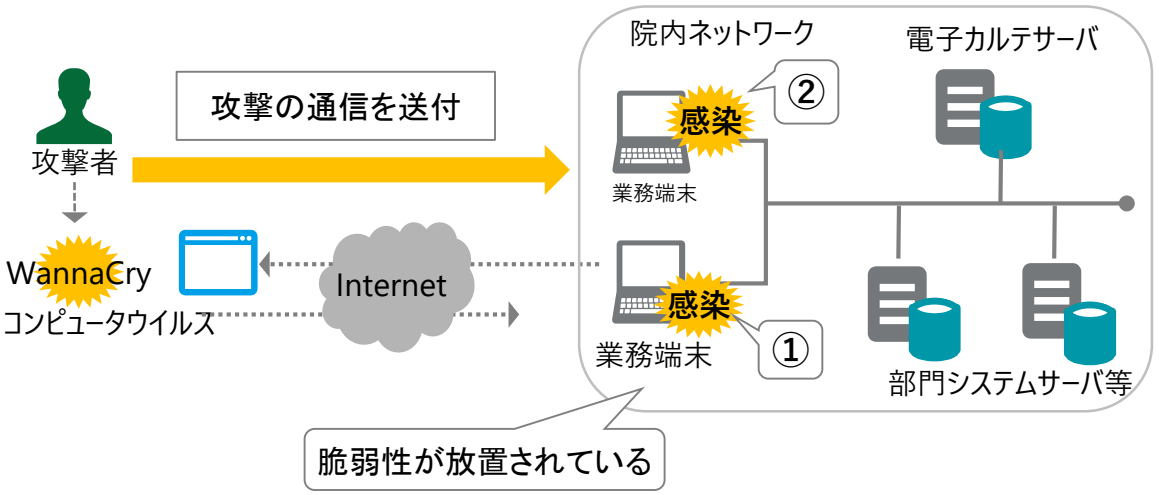
③相互点検の実施
担当者間、部門間等で相互に運用状況の点検を実施し、相互牽制を働かせる

④懲罰規程の整備と周知
内部不正に関して毅然として対応することを従業員に周知する

日本においてサイバー攻撃の事例が報告されており、最悪の場合、システムの稼働停止などによる診療停止の可能性がある

事例	被害組織	内容
外部からの標的型攻撃と想定（未特定）	D大学医歯科学総合病院	• ランサムウェア（コンピュータウイルス）の感染により、治験に関する個人情報が保存されていた端末が暗号化され、使用できない状態であったが、情報漏えいは確認されていない • また、ウェブサイトの改ざんも発覚し、調査を行うとともに暫定ウェブサイトを準備し復旧に向けた対応を行った
外部からのランダム攻撃と想定（未特定）	E大学病院	• ログ解析用ソフトにより業務端末を解析したところ、病院内の業務端末 2 台がマルウェア（コンピュータウイルス）に感染し、外部と不正な通信を行っていたことが判明した • 業務端末の中には、患者の個人情報（計2名分）が保存されており、情報漏えいは確認されていないが、外部に流出した可能性があった • 同大学は、学長による謝罪文を公表し、情報セキュリティ対策の強化を実施した

ランサムウェア（WannaCry）の特徴（参考）



事象

①攻撃者がWindowsの「脆弱（ぜいじゃく）性」を利用し、ランダムな通信先に対して攻撃の通信を送りつけ、WannaCry感染させた。端末ロックやファイル暗号化により端末が利用不能となった

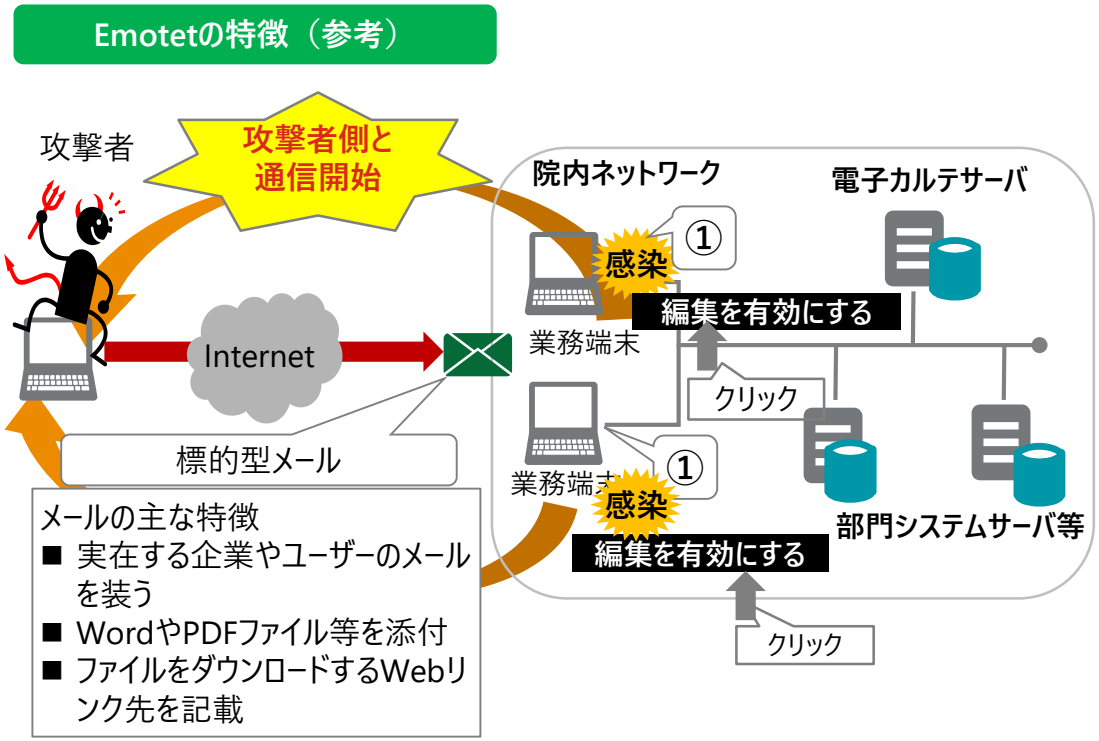
② WannaCryは、感染した業務端末から、攻撃可能な端末等を検索し、自ら拡散する性質を持っていることから、他の業務端末等にも感染が拡大した

要因

- 更新プログラムの適用、ウイルス定義ファイルのアップデートの不徹底（技術的対策の不足）
- 院内ネットワークとインターネットを利用する通信ネットワークとの分離の未実施（技術的対策の不足）
- 情報セキュリティ対策に関する職員への教育訓練の未実施（人的対策の不足）
- 職員への教育訓練を実施する情報システム部門や担当者の未設置（組織的対策の不足）　等

Emotetは、感染した端末のメールの情報を窃取し、それを悪用してメール経由で感染を拡大するマルウエアである。特にURLをクリックさせたり、実在の組織や人物になりすましたメールにWordファイルを添付する手口で、感染を拡大させている

事例	被害組織	内容
外部からの標的型攻撃と想定（未特定）	A法人B病院	• 病院の事務処理用パソコン1台が不審メールを受信し、マルウエア「Emotet」の感染を確認。グループの他関係機関において、A法人B病院をかたる不審メールが送付されていることを確認した。 感染した事務処理用パソコンから漏洩した可能性のある情報の把握が困難な状況となっている。（個人情報の外部への漏洩は確認していない）



事象

① 受信したメールの添付URLのクリックや添付ファイルを開封、ダウンロードし、マクロを有効化するとマルウェアに感染し、攻撃者と通信を始める

※URLのリンクの添付については、ウイルス検知が無効になるケースが多く、感染のリスクが高い。

② メールアカウントやパスワード、アドレス等の情報を窃取

③ 外部にデータを暗号化して送信を実施

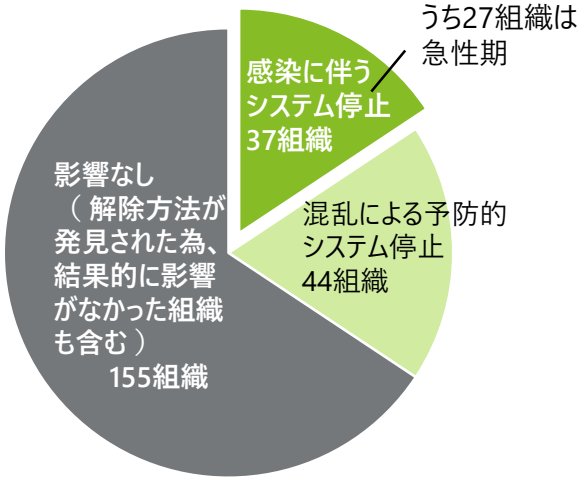
要因

- 更新プログラムの適用、ウイルス定義ファイルのアップデートの不徹底（技術的対策の不足）
- 院内ネットワークとインターネットを利用する通信ネットワークとの分離の未実施（技術的対策の不足）
- 情報セキュリティ対策に関する職員への教育訓練の未実施（人的対策の不足）
- 職員への教育訓練を実施する情報システム部門や担当者の未設置（組織的対策の不足） 等

海外ではサイバー攻撃により、大規模な情報漏洩や診療停止の事例が発生している状況である

事例	発生国	被害組織	内容
外部からの攻撃	米国	医療保険者（Anthem）	• 外部からの攻撃により、「名前、誕生日、医療ID、社会保障番号、住所、メールアドレス、雇用情報、収入データ」等の8,000万件の個人情報が漏えいした
		医療機関（Community Health Systems）	• サーバの脆弱性を利用した外部からの攻撃により、「名前、住所、誕生日、電話番号、社会保障番号」等の450万件の個人情報が漏えいした
		医療機関（Advocate Medical Group）	• 外部からの攻撃により、「名前、住所、生年月日、社会保障番号、診断、電子カルテ番号、医療サービスコード、医療保険情報」等の403万件の個人情報が漏えいした
	英国	国立病院組織（NHSイングランド）	• ランサムウェア（コンピュータウイルス）の感染により、救急部門を含む診療業務の停止、検査結果の受領不能などが発生した
	オーストラリア	大学病院（ロイヤルメルボルン大学）	• ウイルス感染による病理部門システムに障害が発生し、一部の診療業務の手動にて対応した • また、外部向けウェブサイトが停止した

英国公立病院組織における
コンピュータウイルスの感染状況



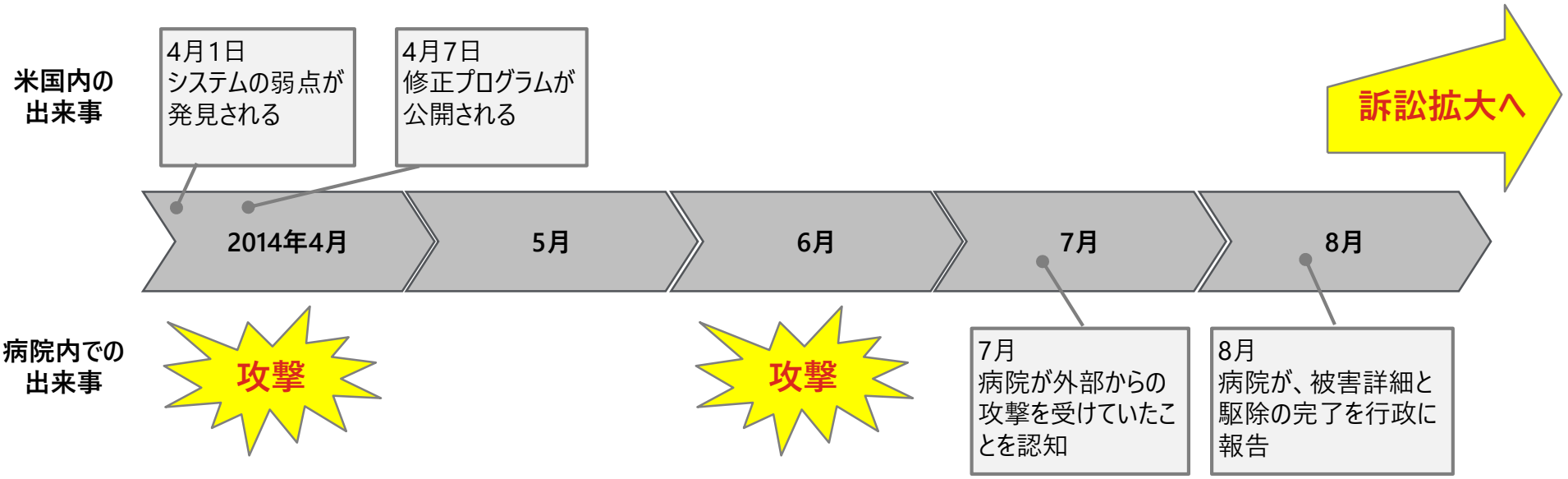
（出典）Investigation: WannaCry cyber attack and the NHS, National Audit Officeなどに基づき作成

2017年5月、英国の複数の病院でシステムが利用不可に。原因は、WindowsOSの弱点を利用してシステムに感染したコンピュータウイルスであった
国内に236ある公立の病院運営組織のうち、少なくとも81組織に影響した

- 27の急性期病院で感染し、ロンドン有数の総合病院をはじめ、5病院で救急車の受け入れを停止
- 推定で約19,000件超の予約がキャンセル
- 1,220台（全体の1%）の医療機器が感染して利用不可になりましたまた感染防止に機器とシステムが分断されたことで混乱が生じた
- 603のプライマリケア施設が感染
- 感染していない施設でも、予防的システムの停止やシステムを停止した施設とシステムが共有されていたために検査結果の参照が不能になるなど、混乱が生じた
- 感染発生から終結まで約1週間の期間を要した

米国では、サイバー攻撃により大手病院グループが標的にされ、450万人分の患者情報が流出

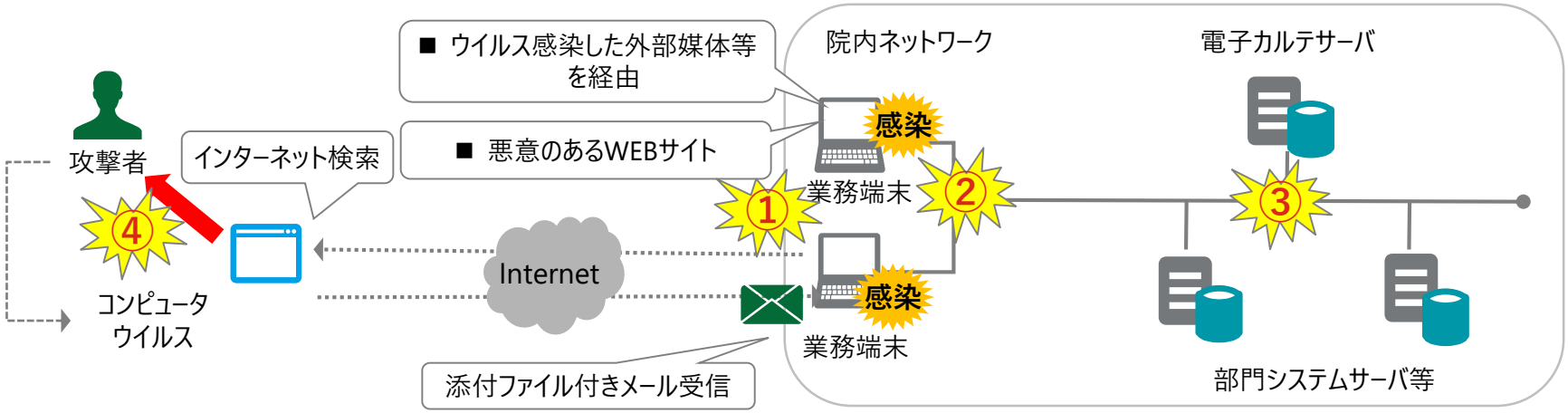
- 2014年8月、米国内29州で206施設を運営する大手民間病院グループが、外部からのサイバー攻撃により、患者約450万人分の個人情報が流出した可能性があることを外部公表した
- 原因は、発見されたばかりの暗号通信技術の弱点を利用されたものであった
- 英国の事例とは異なり、明確に当該グループのシステムを狙った高度な攻撃だったと考えられている
- 全米規模で発生した集団訴訟は2018年3月現在も係争中であり、病院に大きな影響を与えている



（出典）Data Breach Notification, Community Health Systems （http://www.chs.net/media-notice/）ほか公表資料に基づき作成

ユーザーである職員への注意喚起やソーシャルエンジニアリングの理解、入口と出口対策、日常時における監視等、多層防御での取組が重要である

※1　標的型攻撃は、マルウェアを含む添付ファイル付の標的型メールをターゲット組織に送り、PCやサーバをマルウェアに感染させ、遠隔操作などを行いシステム破壊や機密情報の詐取を行う攻撃をいう



	攻撃の説明	対策例（多層防御の考え方）
① 初期侵入	悪意あるWEBサイトや添付ファイル付きメール等を経由してマルウェアが組織内部に侵入する	■ ユーザーである職員への教育を適切に実施し、不自然なメールの開封やダウンロード等を防止する ■ ソーシャルエンジニアリングについて理解する ■ ファイアーウォール ■ 最新のウイルス対策、アップデート ■ 脆弱性診断 ■ 侵入検知、ログ分析 ■ 負荷監視　　等
② 攻撃基盤構築	攻撃指令に基づき、攻撃基盤を構築する（バックドアの構築等）、組織内部の調査	
③ 内部侵入・調査	他のPCやサーバー等へ侵入する	
④ 目的遂行	機密データの外部送信 データの破壊、業務妨害、バックドアを通じた再侵入等	

第2章のまとめ

情報セキュリティ対策は医療機関の経営に関わる重要な問題であり、医療安全管理と同様に日々の業務で取り組んでいく必要がある

【外部委託先管理】
外部委託先と責任範囲や実施すべき情報セキュリティ対策を明示する

【アップデート処理】
医療従事者が勝手にアップデート処理をしないように、注意喚起やアップデート処理の指示を実施する

【外部媒体の管理】
USB等の記憶媒体は、ウイルス感染や情報漏えいのリスクがあるため、個人保有の記憶媒体は使用せずに、医療機関で管理する必要がある

【マルウェアへの感染防止】
見知らぬ添付ファイル付きの電子メールは注意する（受信メールの信頼性を確認する、添付ファイルを開かない、安易にクリックしない等）

【無線LANの貸与】
無線LANは気軽に外部からの接続を行うとウイルスやマルウェアが入り込む可能性があるため、訪問者用のアクセスポイントを設定し院内ネットワークと分離する

【電波環境調査】
電波干渉により医療機器の作動に影響を及ぼす可能性があり、運用の際には無線LANネットワーク事業者と連携して電波環境調査の実施や定期的な保守点検が重要である

【なりすましの防止】
折り返し連絡をし、本人確認を行ったうえで回答したり、電話番号などから相手が特定できない問い合わせには答えない

【内部不正防止】
機会・動機・正当性の3要素を満たさないように、アクセス権限分離や担当者間の相互牽制、懲罰規程等の周知等が有効である

第3章　3省2ガイドラインについて

従来の3省3ガイドラインから3省2ガイドラインへ統合されました。今後は委託先と一緒になってリスクマネジメントを進めていくことが求められます

医療情報システムの安全管理に関するガイドライン（第5版）	
内容	電子的な医療情報の取り扱いに関して、運用管理上の観点から対策を示している。病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者における情報システム責任者を主に対象としている。
第1章	ガイドラインの位置づけや改訂概要
第2章	ガイドラインの読み方
第3章	ガイドラインの対象システム及び対象情報
第4章	電子的な医療情報を扱う際の責任のあり方
第5章	情報の相互運用性と標準化
第6章	情報システムの基本的な安全管理
第7章	電子保存の要求事項
第8章	診療録及び診療諸記録を外部に保存する際の基準
第9章	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
第10章	運用管理について

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	
内容	従来の経済産業省のガイドライン（情報処理事業者向け）と総務省のガイドライン（クラウド事業者向け）のガイドラインを統合している。内容の明瞭化とリスクベースアプローチ（※1）を採用したことが特徴となる。
第1章	本ガイドラインの基本方針
第2章	本ガイドラインの対象
第3章	医療情報の安全管理に関する義務・責任
第4章	対象事業者と医療機関等の合意形成
第5章	安全管理のためのリスクマネジメントプロセス
第6章	制度上の要求事項

※1　リスクベースアプローチとは?

リスクに応じて、医療機関とコミュニケーションを取りながら合意形成し、リスクマネジメントをしていくことを要求している。医療機関は、ベンダー等のサービス提供事業者に対して、安全管理のためのリスク情報の開示を受け、外部事業者がどのようにリスク軽減をしていくのか説明をうけて管理する手法である。

第3章のまとめ

医療機関で遵守すべきセキュリティに関するガイドラインとしては、土台として主に２つのガイドラインがあります

	医療情報システムの安全管理に関するガイドライン（第5版）	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
内容	電子的な医療情報の取り扱いに関して、運用管理上の観点から対策を示している。病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者における情報システム責任者を主に対象としている。	従来の経済産業省のガイドライン（情報処理事業者向け）と総務省のガイドライン（クラウド事業者向け）のガイドラインを統合している。内容の明瞭化とリスクベースアプローチを採用したことが特徴となる。

今後は委託先と一緒になってリスクマネジメントを進めてセキュリティ水準を向上していくことが求められます

第4章　情報セキュリティ対策について

情報セキュリティ対策における構成は、「組織的対策」「人的対策」「技術的対策」「物理的対策」であり、患者への医療サービスの品質向上（医療安全対策）においても、同様の構成である

病院の医療安全対策の例示

— 医療安全管理での対策例 —

- 医療安全管理に関する規定等の策定
- 専門スタッフの配置
- 医療スタッフの雇用・育成

— 医療安全管理での対策例 —

- 医療安全の管理・改善業務
- 職員への教育訓練
- 医療安全管理のルールの遵守

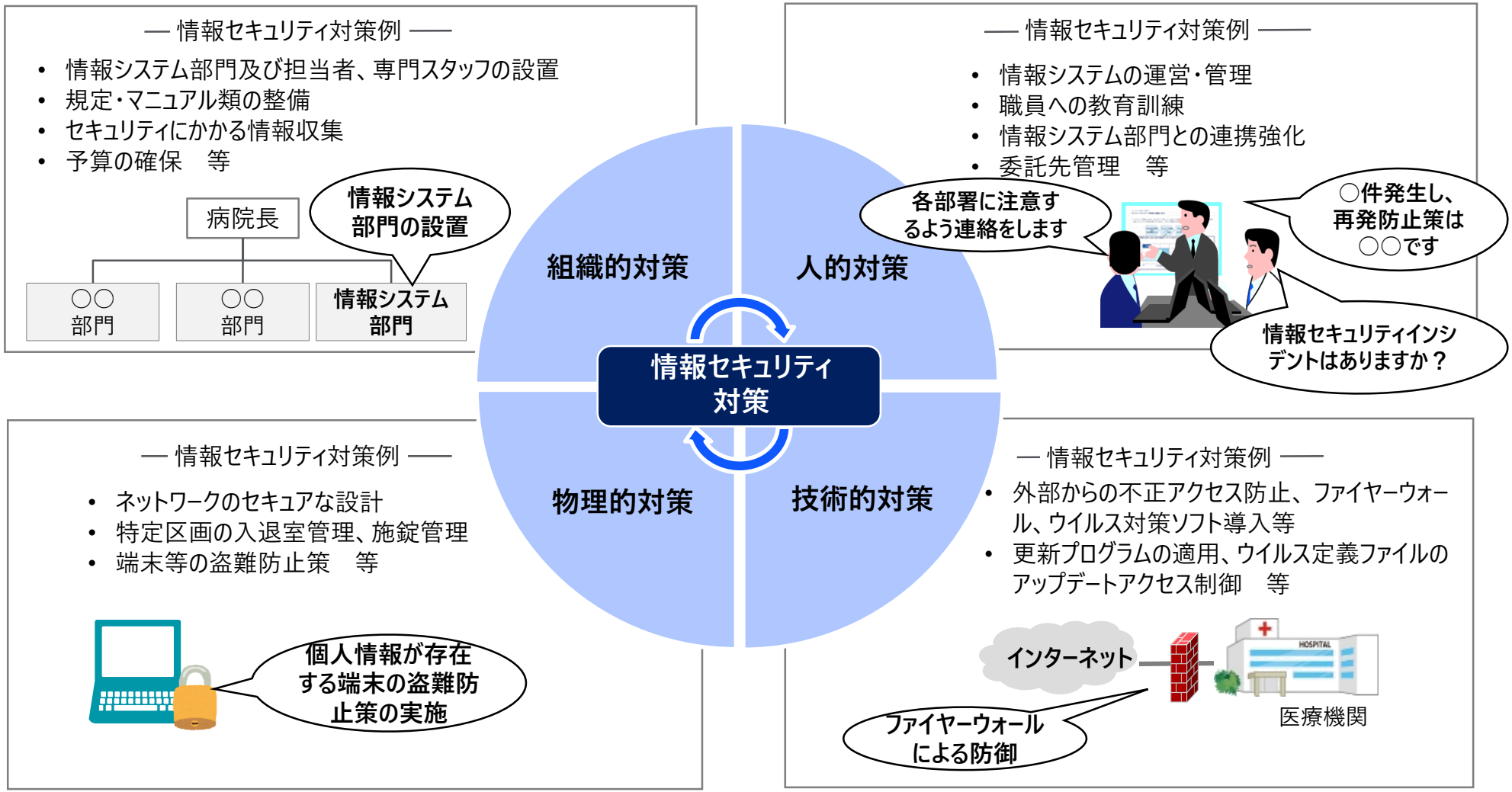
— 医療安全管理での対策例 —

- 院内における感染対策を踏まえた導線の整備
- 麻薬や劇薬の保管管理方法　等

— 医療安全管理での対策例 —

- 医療安全に配慮した機器の導入
- 転倒・転落防止策の実施
- 診療記録
- インシデント記録の分析

情報セキュリティ対策は、患者への医療サービスの品質向上（医療安全）と同様に、各職種で対応する必要があり、「組織的対策」「人的対策」「技術的対策」「物理的対策」のうち、いずれかの対策が欠けても、全体の有効性は欠けた部分と同じく、最も低い水準となる



セキュリティ対策で言われる４つの分類を医療機関の現実に即した具体的な9領域に分解してチェックリストとして整理しました

情報セキュリティ対策の４つの分類

イメージ

人
・従業員一人ひとりの規則遵守の意識（コンプライアンス）
・教育訓練
・判断、目配り気配り、運用と管理
⇒ ①②③⑦

技術
・ウイルス対策ソフトやファイアウォールなどの正しい配置と運用による防御、ならびに常時監視、
・定期チェックによる検知・発見
⇒ ④⑤⑥

4領域

物理
・特定区画への入退室・施錠管理、PCなど情報機器やUSBメモリ・ 紙などの記録媒体の盗難対策等の管理（移動・輸送・廃棄も含め）
⇒ ④⑤⑦⑧

組織
・部門や担当者等の配置
・ルール作り、ルールを守る取り組み、ルールが守れるPDCAサイクルの実施
・情報収集
⇒ ⑦⑧⑨

情報セキュリティ対策で言われる４つの分類について、医療機関が実際に対応できているかどうか、主体の観点（人的・システム的・組織的）とコントロール方法の観点（予防・発見・是正）で分類してチェックリストとして整理しています

チェックの観点	組織的（経営層）	システム的（システム管理者）	人的（一般職員・医療従事者）
是正的コントロール	1 インシデント発生後の組織としての原因究明・改善対応の仕組みが整備できているか	4 バックアップや復旧時の縮退運用の仕組みが有効になっているか	7 不具合発生期間時の現場対応方法が周知できているか
発見的コントロール	2 院外も含めた初動通報体制の確認と通報基準が整理・共有できているか	5 外部からの侵入を検知する仕組みが構築できているか	8 不具合発見時の連絡方法が周知徹底ができているか
予防的コントロール	3 委員会やシステム管理組織・運用管理ルールの整備ができているか	6 エンドポイントのウィルス対策・セキュリティパッチの適用ができているか	9 職員のセキュリティ意識向上の取り組みが行えているか

チェックリストを活用し、実際にどの分類の対策が不足しているのか把握し、不足している領域に対して優先的に資源投入をすることが重要である

確認項目と対策例

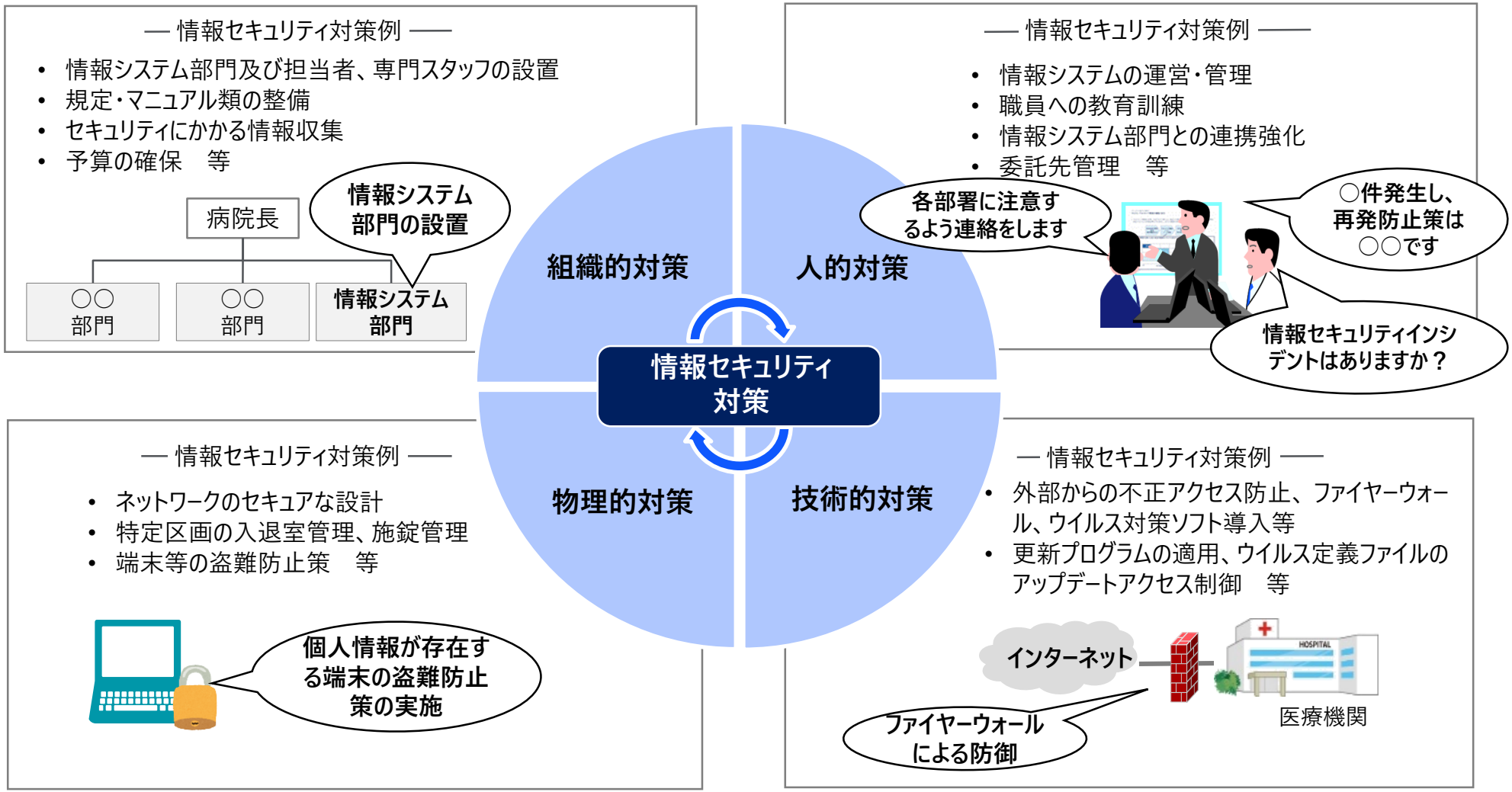
規模に関わらず、定期的な自己点検において確認すべきと考えられる項目と、点検によって不備が見つかった場合の対策例を記載します。

	組織的（Structure）		システム的（System）		人的（Staff）	
	経営層あるいは、病院組織全体として、十分に理解・対応できているか		システム管理者層・システム管理組織が十分に理解・対応できているかどうか		従業員一人ひとりの規則遵守の意識（コンプライアンス）	
	確認項目	対策例	確認項目	対策例	確認項目	対策例
是正的コントロール	証拠保全のためのルールと運用状況の記録は十分か	証拠保全と運用状況の記録ルールの見直し	情報のバックアップ・縮退運転などの対策は十分に行われているか	障害時復旧の手段が有効かの再確認	インシデント発生時の運用が考慮されているか	トラブル発生時の診療実施ルールの周知
発見的コントロール	国や県といった外部機関との連携は十分か	発見時の連絡体制・ルールの整理見直し	外部からの侵入に早期に気づける仕組みがあるか	水際対策・IDSなどの整備ができているかの確認	異常を感じた時の相談窓口・通報ルールが周知されているか	相談窓口・通報ルールの再教育
予防的コントロール	システムを管理するルール・組織が機能しているか	情報システム運用管理規定や委員会等の役割・運用の見直し	最新リスクの把握がされているか	最新リスクへの対策 セキュリティパッチの適用	各種規定書、指示書、取扱説明書等が周知されているか	各種規定書、指示書、取扱説明書の周知状況の整理・再周知
	システムの状態把握を委託業者にまかせっきりになっていないか	委託業者管理・報告ルールの見直し	外部からの侵入を防ぐことができる技術的対策がされているか	システム上の対策の強化 IPSやFWの導入や設定見直し	ヒューマンエラー（規定違反）が起こる可能性が考慮されているか	ヒューマンエラー防止のための教育・訓練の実施

より詳細なチェックについては、別紙「セキュリティチェックシート」を活用して実施してください。

第4章のまとめ

情報セキュリティ対策は、患者への医療サービスの品質向上（医療安全）と同様に、「組織的対策」「人的対策」「技術的対策」「物理的対策」をバランスよく対応することが重要である



第5章　情報セキュリティ事故発生時の対応

事故発生時は、迅速な復旧（医療の提供）と原因調査や再発防止の取り組みを同時に進める必要がある

情報漏洩等インシデント発生

復旧

- 情報漏洩によって発生した被害の拡大の防止と復旧のための措置を行う。
- 専用の相談窓口を設置し被害が発生した場合にはその動向を素早く察知し対応する。
- 医療の提供が再開できるように関連する部門システムへの影響も踏まえて調査復旧を実施する。

検知・初動対応

- 情報漏えいに関する兆候や具体的な事実を確認した場合は、責任者に報告し速やかに情報漏えい対応のための体制をとる。
- 情報が外部からアクセスできる状態にあったり、被害が広がる可能性がある場合には、これらを遮断する措置をとる。（情報の隔離、ネットワークの遮断、サービスの停止等）
- 不正アクセスや不正プログラムなど情報システムからの情報漏えいの可能性がある場合は、不用意な操作をせず、システム上に残された証拠を消さないようにする。

報告・体制構築

- 個人情報の漏えい、滅失又は毀損等のおそれがある場合は個人情報保護委員会へ速やかに報告を実施する。
- サイバー攻撃で医療サービス提供体制に支障が発生する場合は、厚生労働省医政局研究開発振興課医療情報技術推進室へ連絡する。
- 対策本部を設置し当面の対応方針を決定し、情報漏えいによる被害の拡大、二次被害の防止のために必要な応急処置を行う。

原因調査 被害特定

- 適切な対応についての判断を行うために５Ｗ１Ｈの観点で情報を整理する。
- 事実関係を裏付ける情報や証拠を確保する。
- 原因調査の結果を経営層へ報告する

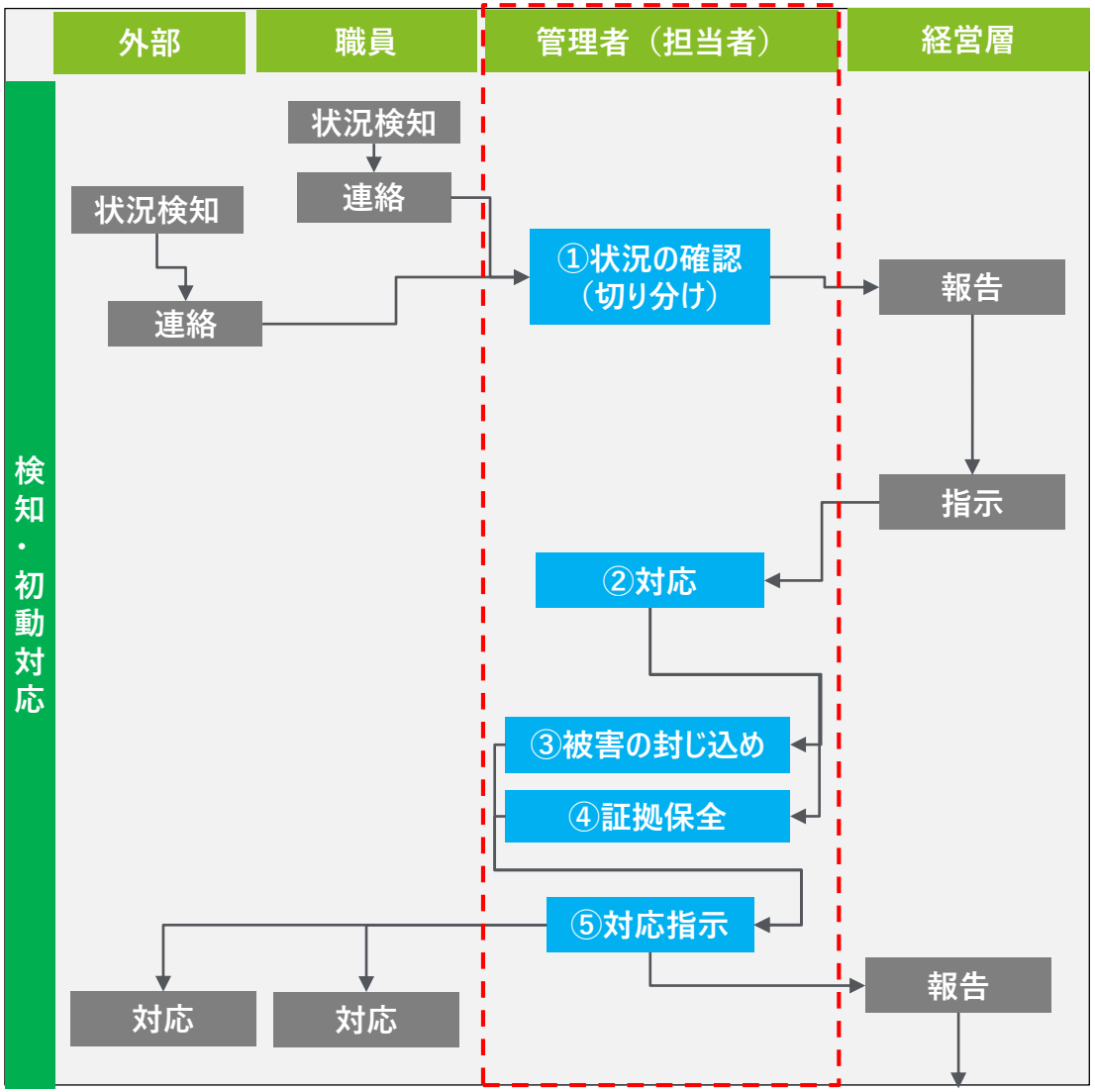
公表・届出

- 漏洩した個人情報の本人、取引先などへの通知、監督官庁、警察、IPAなどへの届出、ホームページ等による公表を検討する。
- 漏洩した個人情報の本人については特別な理由がない限り通知する。
- 紛失・盗難のほか不正アクセス、内部犯行、脅迫等不正な金銭の要求など犯罪性がある場合は警察へ届出する。

事後対応 再発防止

- 再発防止策を検討し実施する。
- 再発防止策を含めて経営層へ報告し、被害者に対する損害の補償等について必要な措置を行う。
- 内部職員の責任等について必要な処分手続きを行い、必要に応じて情報を開示する。

迅速な検討のためには、システムやネットワークの普段の状況を把握しておくことが必要である。また記録（証拠）を消去しないように定期的にシステム復旧のテストをしておくことが重要である



① 状況の確認

■ 職員や外部委託先等からシステム異常等について連絡を受けたら、各システムやネットワークの状況を確認して経営層へ報告する。（通常時の稼働状況や高負荷時等のシステム特性を把握しておくことで障害を迅速に検知できる可能性が高くなる。）

② 対応

■ システムの障害状況等も踏まえて、経営層から指示を受け復旧対応を進める。職員や外部委託先等に対してシステムの復旧まで利用ができないことを伝達する。

③ 被害の封じ込め

■ 不正アクセスや改ざん等の場合は、ネットワークからの遮断や不正アクセスに使用されているログインIDの無効化、パスワード変更、機器の隔離等の被害拡大防止の対策を実施する。

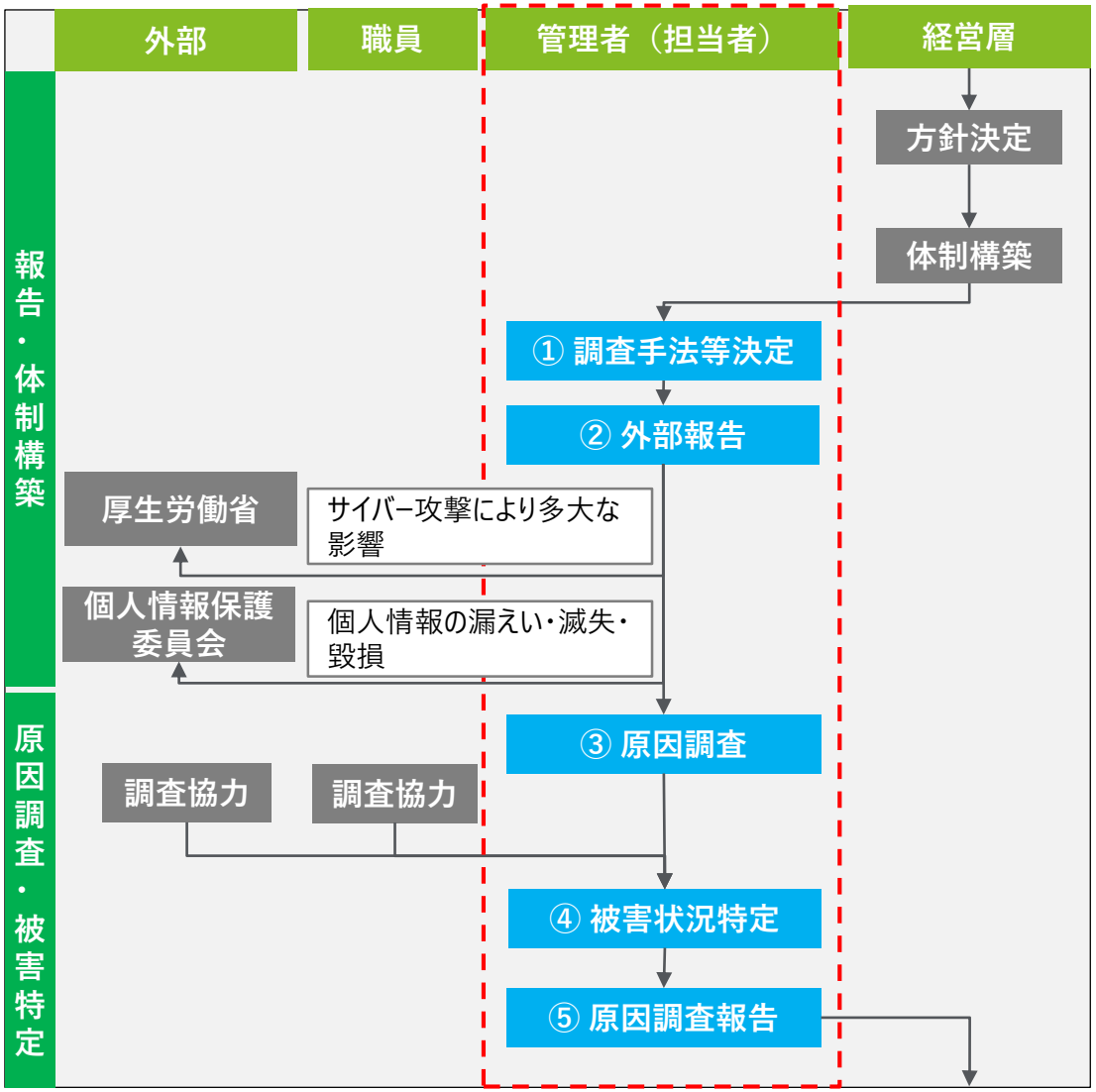
④ 証拠保全

■ 不正アクセスや不正プログラムなど情報システムからの情報漏えいの可能性がある場合は、証拠保全のために、システム上に残された証拠を消さないようにする。（システム復旧処理時に記録を消去しないように留意する。）

⑤ 対応指示

■ 経営層へ適宜状況報告をする。管理者側で証拠保全が難しい場合は、外部委託先に証拠保全の指示を実施する。原因調査に向けて職員への協力依頼を実施する。

個人情報の漏えい、滅失又は毀損等のおそれがある場合は個人情報保護委員会へ速やかに報告を実施する。サイバー攻撃で医療サービス提供体制に支障が発生する場合は、厚生労働省医政局研究開発振興課医療情報技術推進室へ連絡する



① 調査手法等決定

■ 経営層で決定した体制を踏まえて、原因調査及び被害状況の特定のための調査手法等を決定する。必要に応じて外部業者の協力依頼を検討する。

② 外部報告

■ 個人情報の漏えい、滅失又は毀損等のおそれがある場合は個人情報保護委員会へ速やかに報告を実施する。
■ サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、非常時と判断した上で、厚生労働省医政局研究開発振興課医療情報技術推進室へ連絡する。

③ 原因調査

■ 事故発生の原因について5W1H（誰が、何を、いつ、どのような理由で、どうやって）実施したのか情報を整理する。ログの解析や復元等の技術が必要な場合は、外部委託先等に調査への協力を実施する。

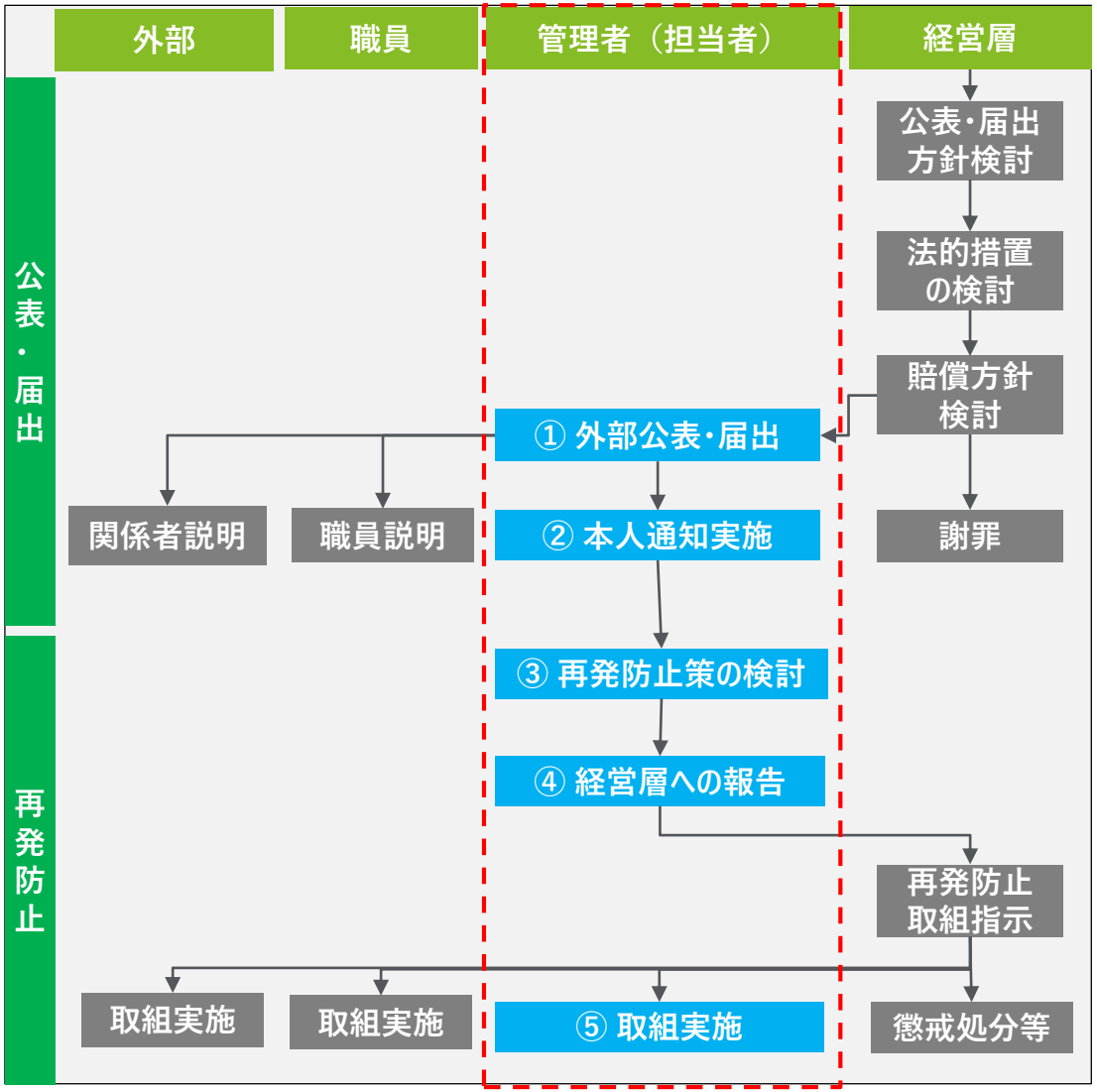
④ 被害状況特定

■ 被害状況について、漏えいした個人情報の範囲（数、データの内容、漏えい手段、原因等）を特定する。意図的な犯行等の可能性がある場合は、関連する証拠（ログ等）を保全し、必要に応じて顧問弁護士等へ相談する。

⑤ 調査結果報告

■ 原因調査の結果に加えて、外部公表や届出、法的措置等の必要性について情報を整理して経営層へ報告する。

再発防止の取組が各部門の業務に反映されているかどうか、外部委託業者の業務に反映されているか、定期的にモニタリングすることが重要である



① 外部公表・届出

■ 取引先などへの通知、監督官庁、警察等への届出、ホームページ等による公表を実施する。

② 本人通知実施

■ 経営層による賠償方針を踏まえて、漏洩した個人情報の本人へ謝罪も含めて通知を実施する。本人や取引先、監督官庁等からの問合せ等に対しては、問合せ窓口を設置して対応する。

③ 再発防止策の検討

■ 原因調査結果を踏まえて、再発防止策を検討する。再発防止策を実施にあたり、関係部門の責任者等を踏まえて日常業務への反映を検討する。必要に応じて現行ルールの改正を検討する。

④ 経営層への報告

■ 再発防止策及び日常業務への影響を経営層へ報告する。（新たな設備投資等が必要な場合は、必要コストや効果について説明する）

⑤ 取組実施

■ 経営層からの取組指示に基づいて、再発防止の取組を実施する。職員及び外部委託先へ指示を実施し、取組状況のモニタリングを定期的に実施して確認する。

第5章のまとめ

情報セキュリティ事故発生時点の対応のポイント

検知・初動対応

迅速な検討のためには、システムやネットワークの普段の状況を把握しておくことが必要である。また記録（証拠）を消去しないように定期的にシステム復旧のテストをしておくことが重要である

報告・公表・届出

個人情報の漏えい、滅失又は毀損等のおそれがある場合は個人情報保護委員会へ速やかに報告を実施する。サイバー攻撃で医療サービス提供体制に支障が発生する場合は、厚生労働省医政局研究開発振興課医療情報技術推進室へ連絡する

原因調査・再発防止

再発防止の取組が各部門の業務に反映されているかどうか、外部委託業者の業務に反映されているか、定期的にモニタリングすることが重要である

ご受講ありがとうございました