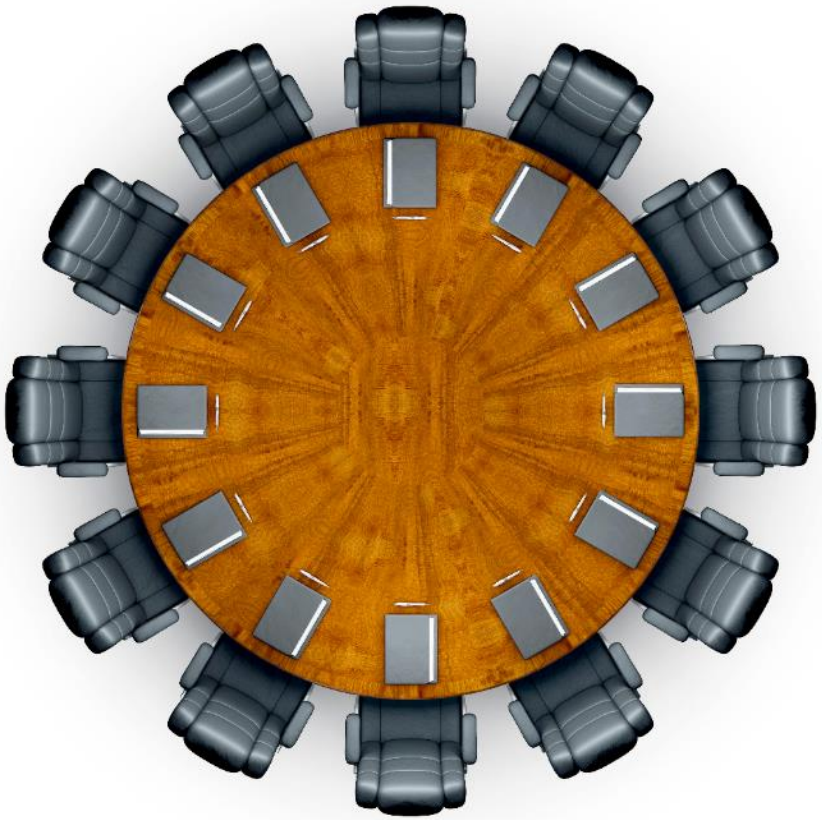


「情報セキュリティ研修教材（経営層向け）」

本日お伝えしたいこと

	特に重要なページ
1　正しく危機意識をもつこと（第1章）	2頁
2　サイバーセキュリティ対策について現状調査をすること（第2章）	3頁
3　サイバーセキュリティ対策のための予算確保と担当者・窓口の設置（第3章）	4頁
4　その他	5頁

第1章のまとめ

正しい危機意識を持つ ＝ 正しく理解すること

1　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重要な経営課題である

2　「外部事業者等によるミス・不正」・「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

3　サイバー攻撃によりシステムの稼働停止等の事実が発生している

4　外部事業者の管理、外部媒体の管理、ウイルス感染対策、EMOTET等の標的型攻撃への対策が重要である

第 2 章のまとめ

現状調査 ＝ セキュリティ対策の実施状況を把握し、どこまで自院で対応可能か検討すること

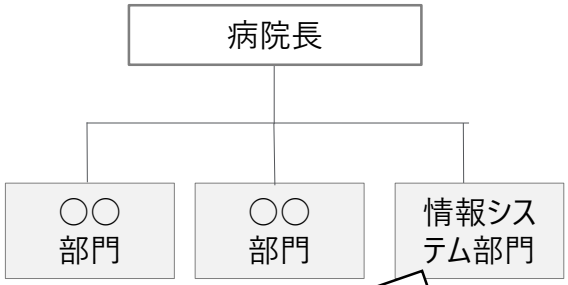
情報セキュリティ対策の実施状況

実施前 → **検討中** → **実施中**

「担当者」の設置

【ガバナンスの強化】

- 最初に講じる対策は、組織的対策となる「情報システム部門、又は、担当者の設置
- 組織の方針となるルールの整備
- セキュリティ対策を進めるための予算の確保



情報システム部門/担当の設置

院内で対応が難しい場合

【外部へ相談・依頼】

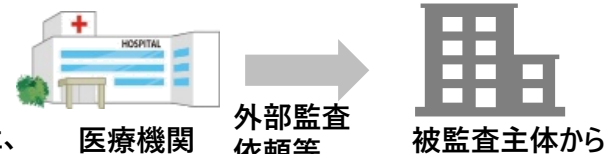
- 情報セキュリティは、専門領域であり組織的対策を病院内部で講じることが難しい場合、アウトソーシングサービスへの相談・委託を含めた対策の検討

組織体制、規定類の整備、インシデント対応フロチャートの構築支援を依頼

対策がある程度実施されている場合

【モニタリングの実施】

- 情報セキュリティ対策の実施ができている場合は、自己点検の実施に加えて、外部組織による情報システム監査を受審することで、継続的にセキュリティマネジメントを強化していく



マネジメント体制を強化するため、外部監査を依頼

第 3 章のまとめ

予算の確保と担当者の設置 ＝ セキュリティ対策の実効性を確保すること

予算の確保

予算科目

医業費用

- 給与費
  - 給料
  - 賞与
  - 法定福利費
  - ・・・
- 委託費
  - 保守委託費
  - その他委託費
  - 検査委託費
  - ・・・

→ 【担当者の設置】
情報システム担当や
セキュリティ担当者等の
人件費に関する予算

→ 【外部業者との連携】
セキュリティを確保した
ネットワークの構築等、
外部業者からの協力に
関する予算

担当者の設置

組織名	医療法人○○会
部門	情報システム部 サイバーセキュリティ対策班
役職	係長
担当者名	○○　○○

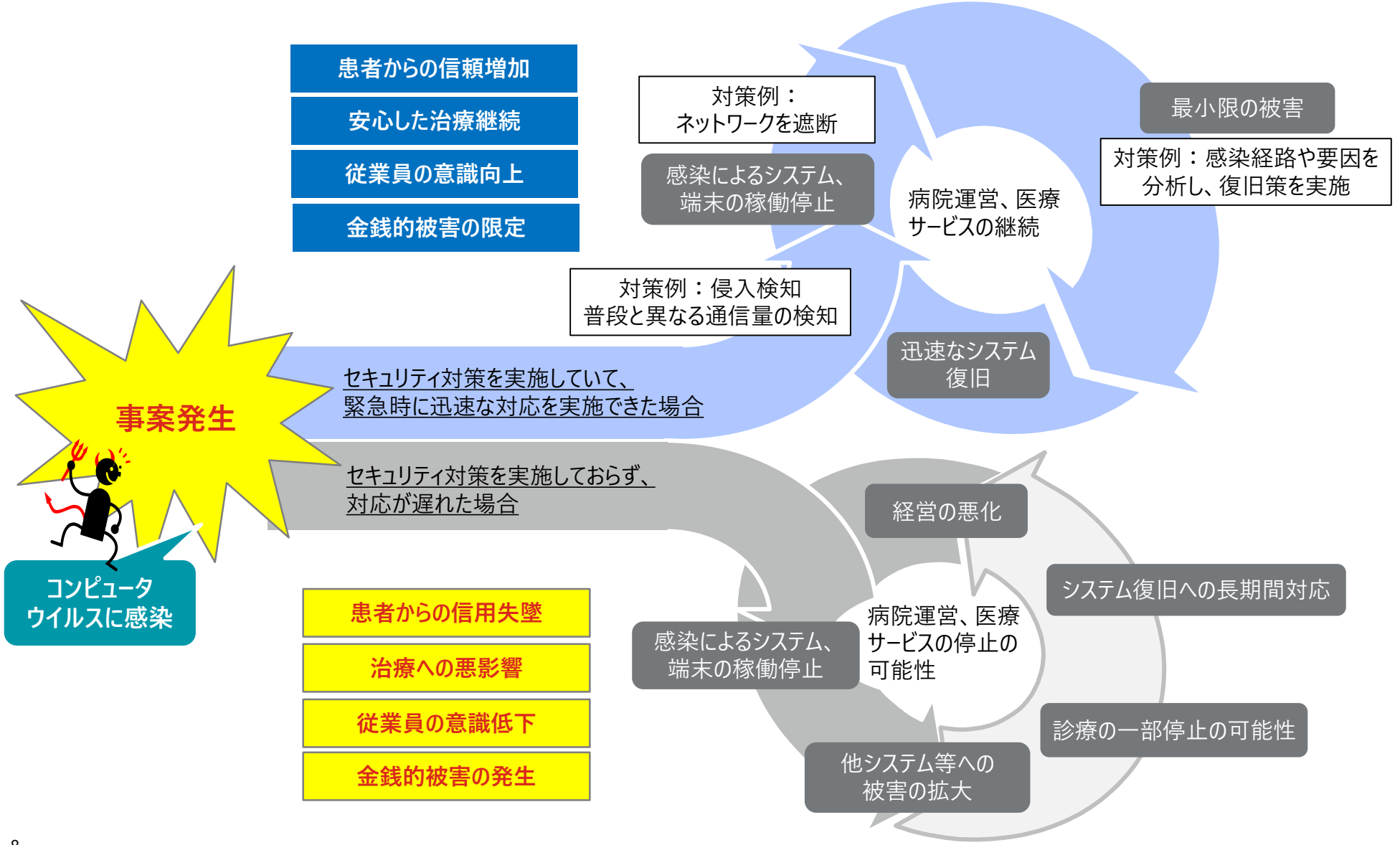
最後に・・・
サイバーセキュリティ担当者をほめてください

サイバーセキュリティ担当者の成長が
組織を守る要になります！！！

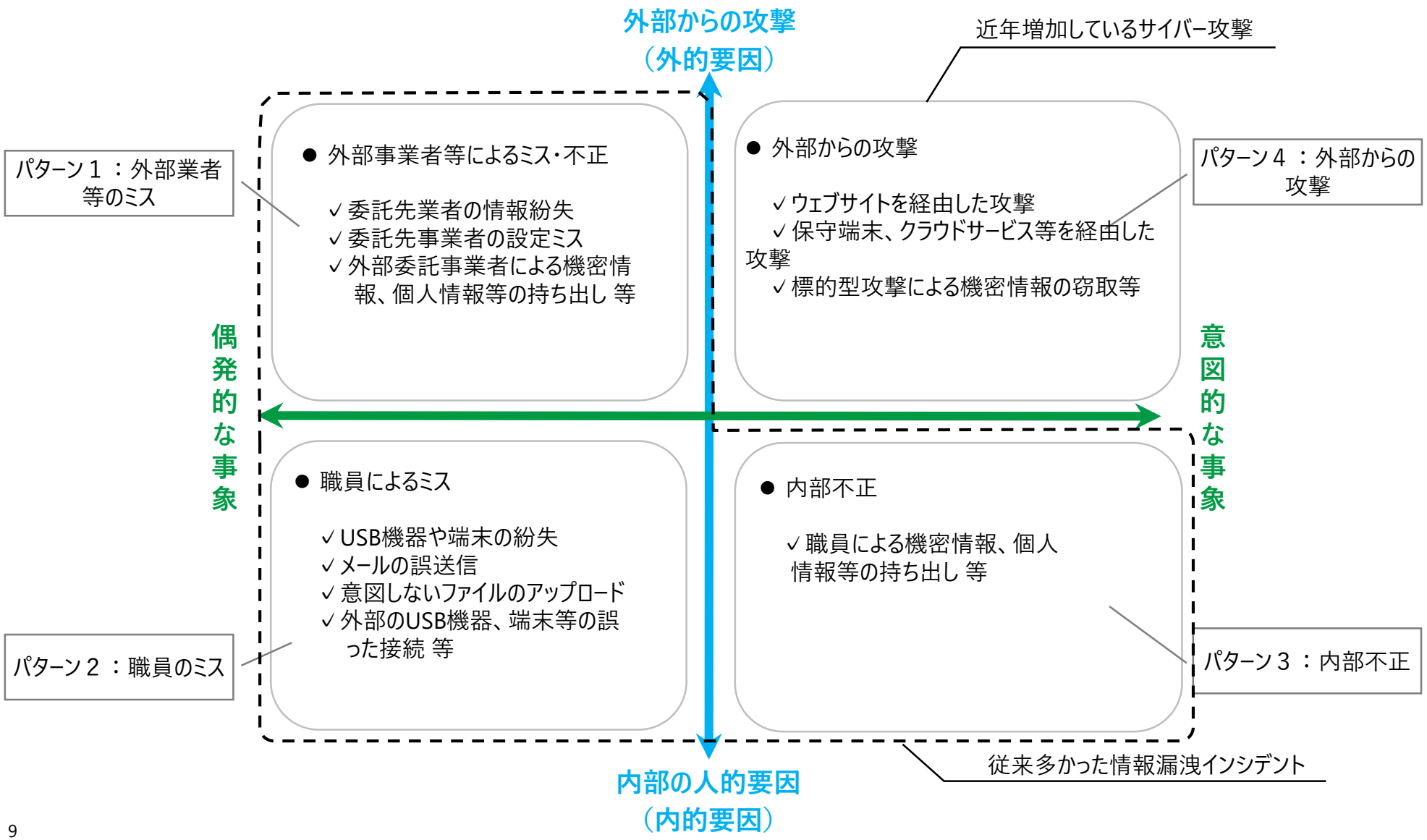
目次

第1章　正しい危機意識を持つ

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



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	情報セキュリティ対策の不足	ICT技術の進展に伴う院外との接続の増加	医療等分野の更なる情報化の進展（想定）
• 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 等	• 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 等	• • •

- 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

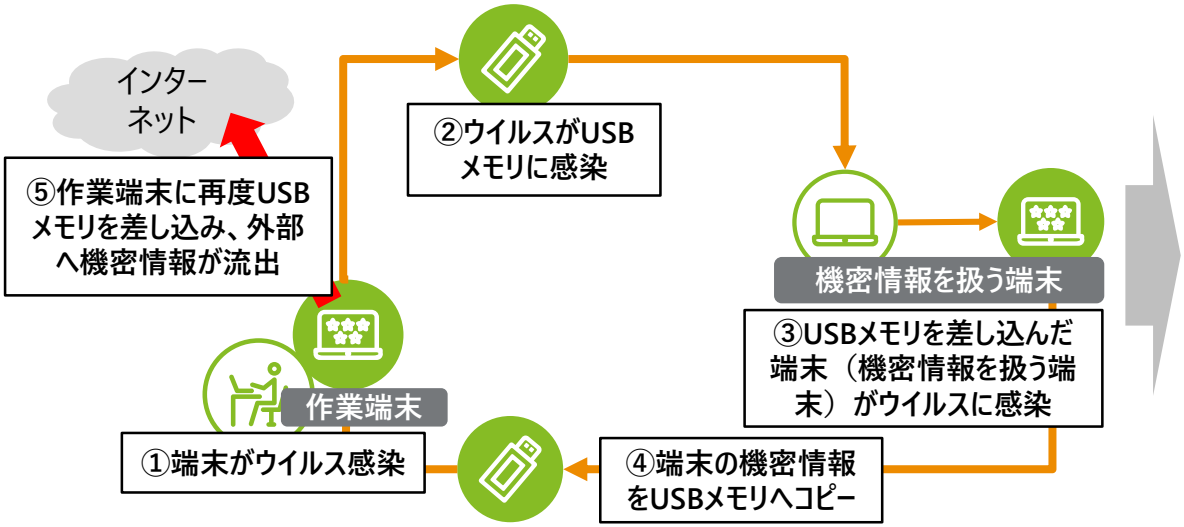
明示の例

- ■ 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

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

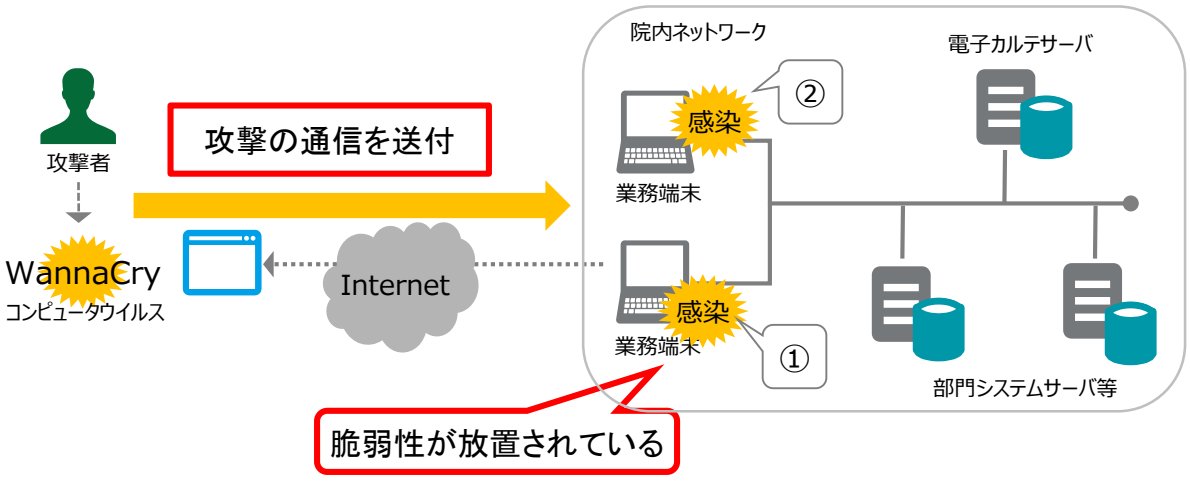
③相互点検の実施
担当者間、部門間等で相互に運用状況の点検を実施し、相互牽制を働かせる

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

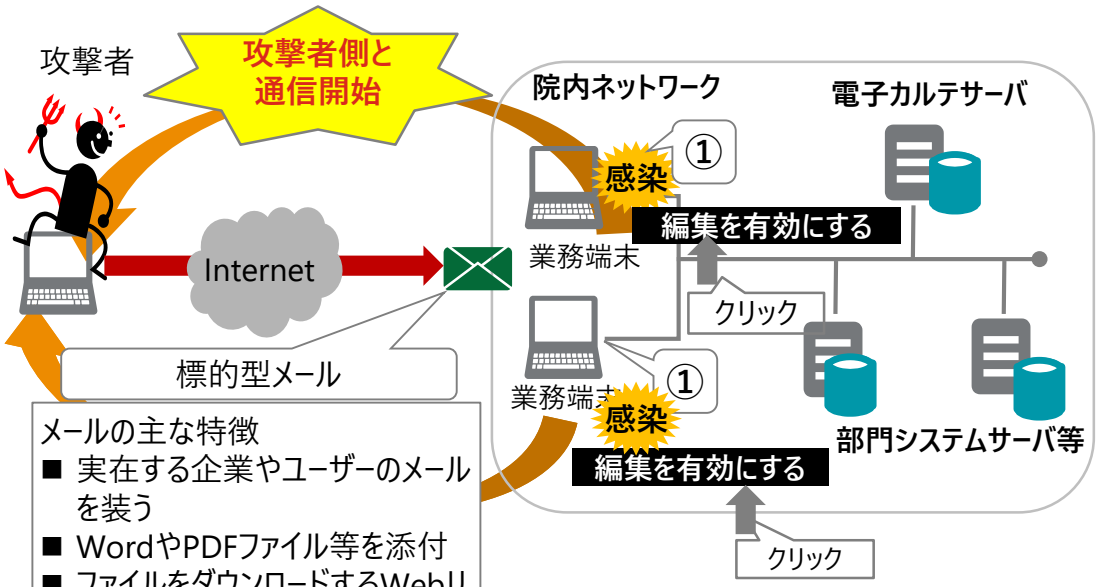
要因

- **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。特に実在の組織や人物になりすましたメールに、URLのリンク先の添付や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）

Emotetの特徴（参考）



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

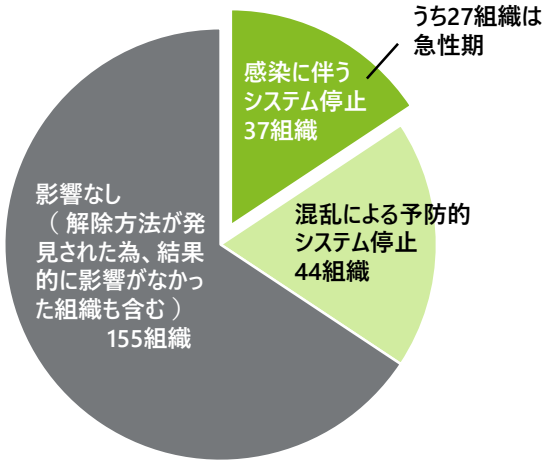
要因

- 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



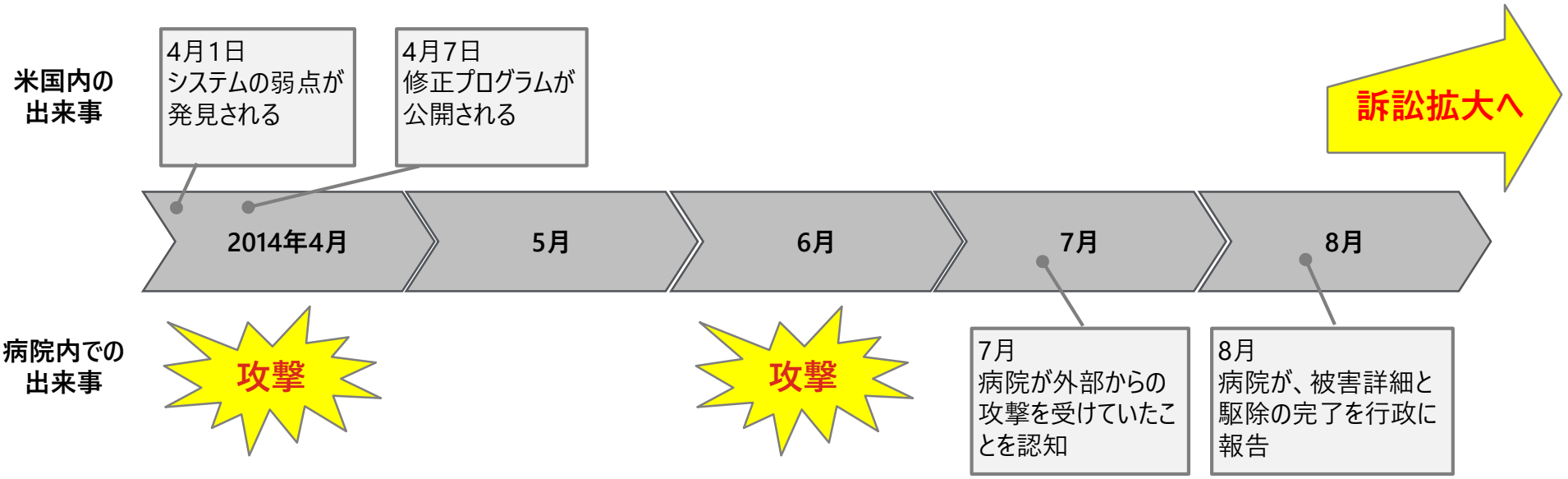
（出典）Investigation: WannaCry cyber attack and the NHS, National Audit Officeなどに基づき作成

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

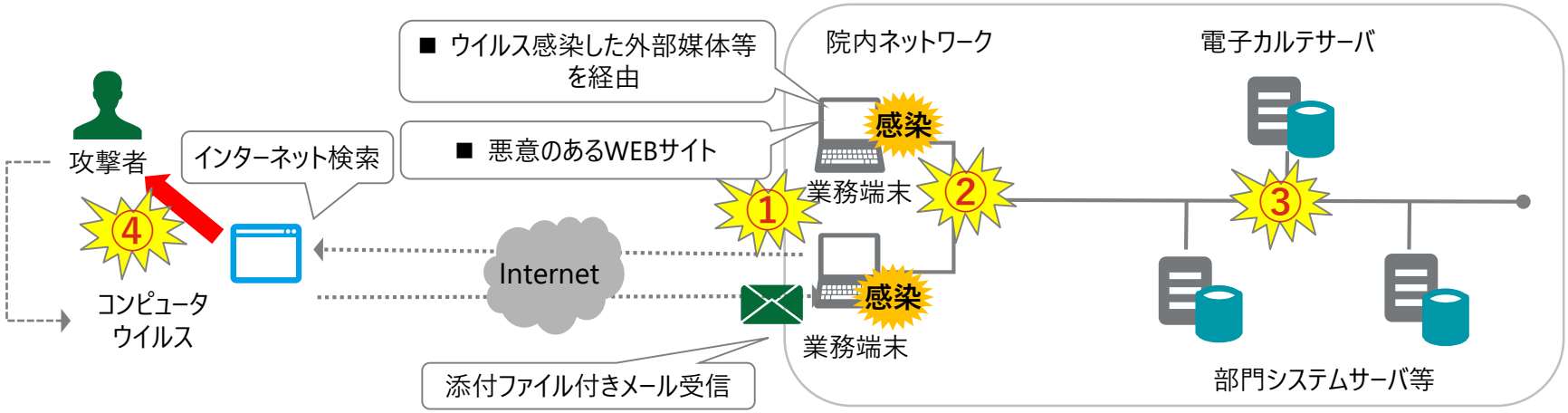
- 2014年8月、米国内29州で206施設を運営する大手民間病院グループが、外部からのサイバー攻撃により、患者約450万人分の個人情報が流出した可能性があることを外部公表した
- 原因は、発見されたばかりの暗号通信技術の弱点を利用されたものであった
- 英国の事例とは異なり、明確に当該グループのシステムを狙った高度な攻撃だったと考えられている
- 全米規模で発生した集団訴訟は2018年3月以降も係争中であり、病院に大きな影響を与えている



（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

近年は標的型攻撃（※1）のリスクが非常に高くなっている

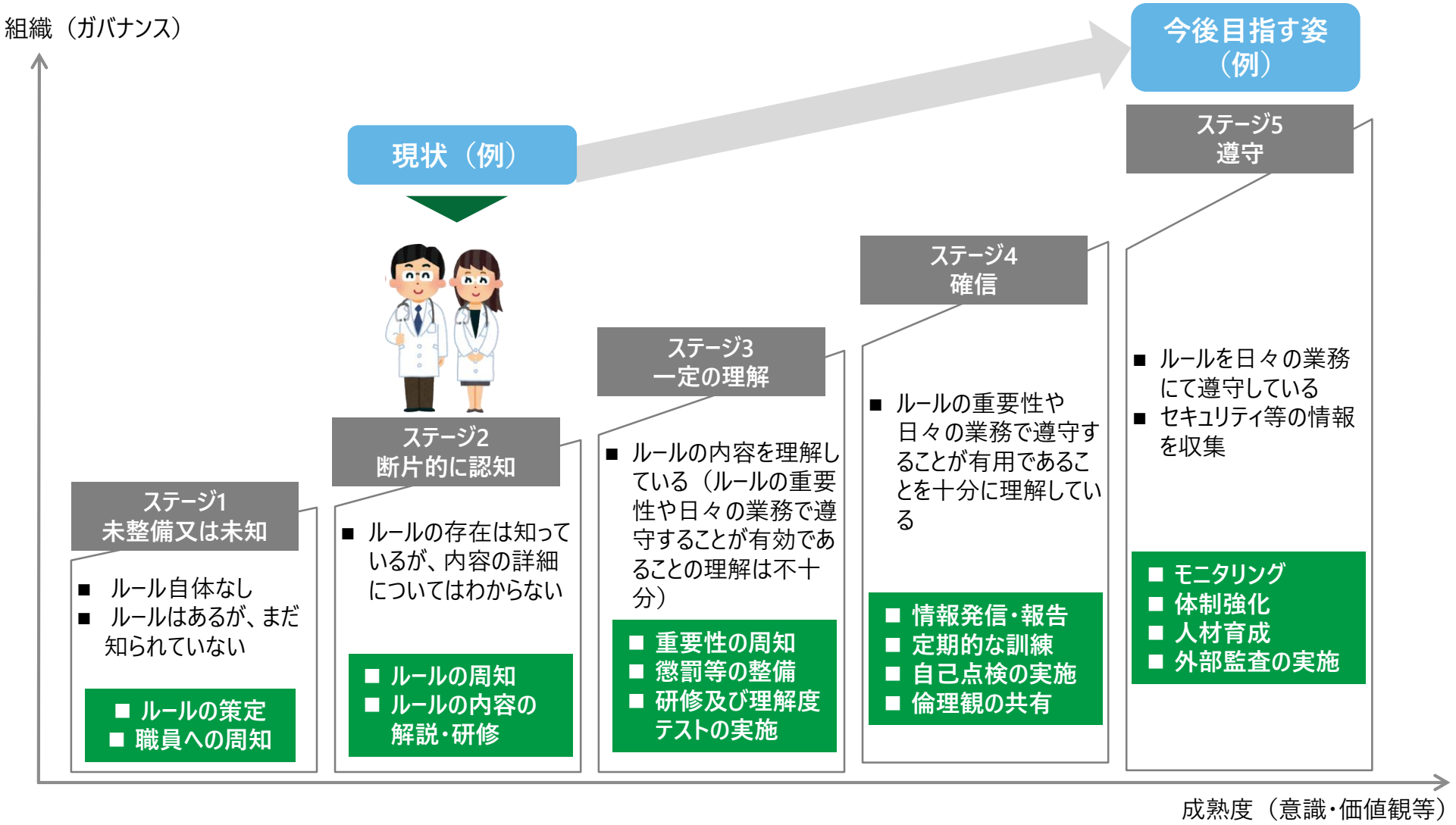
※1　標的型攻撃は、マルウェアを含む添付ファイル付の標的型メールをターゲット組織に送り、PCやサーバをマルウェアに感染させ、遠隔操作などを行いシステム破壊や機密情報の詐取を行う攻撃をいう



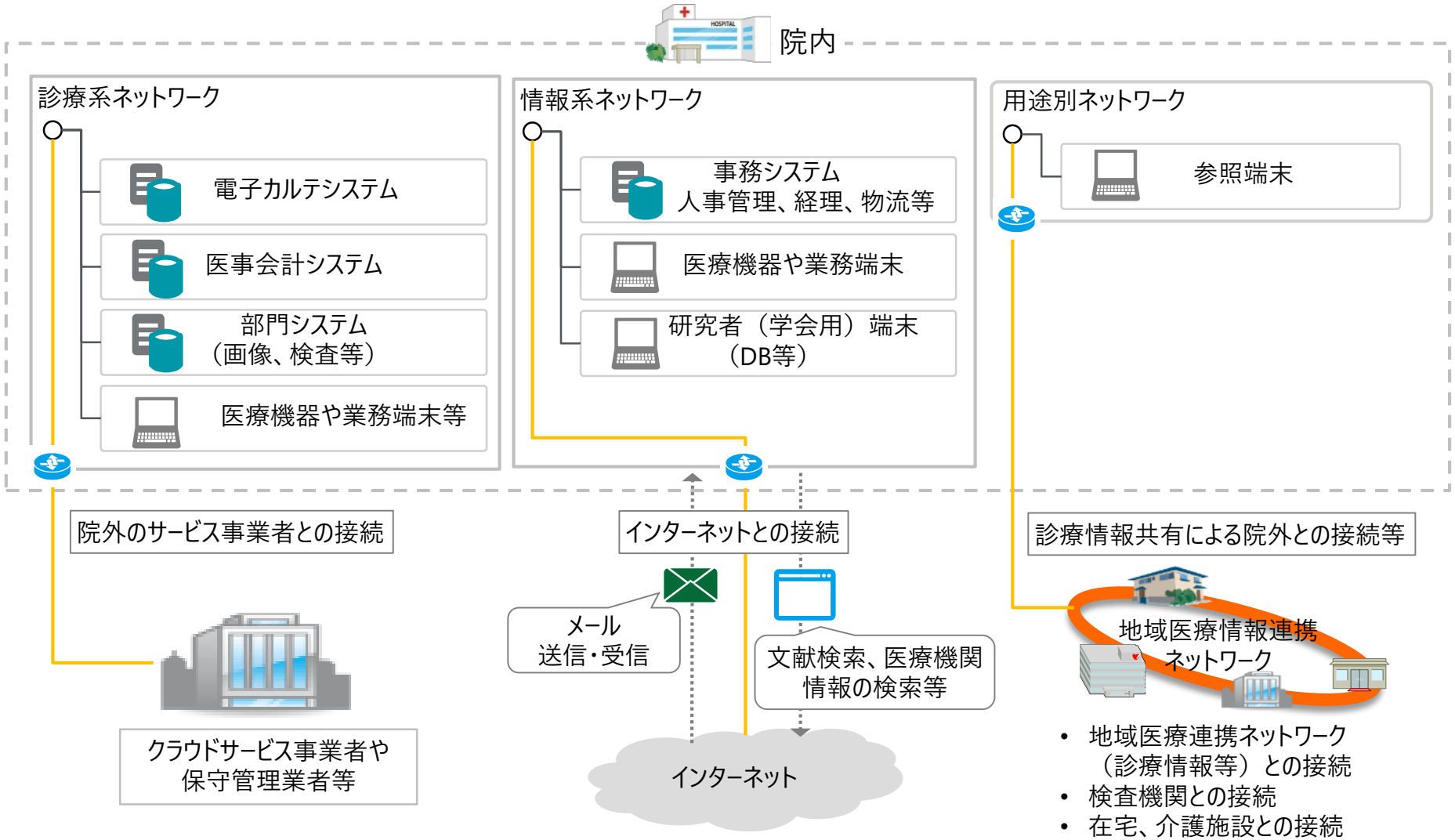
	攻撃の説明	対策例（多層防御の考え方）
① 初期侵入	悪意あるWEBサイトや添付ファイル付きメール等を経由してマルウェアが組織内部に侵入する	■ ユーザーである職員への教育を適切に実施し、不自然なメールの開封やダウンロード等を防止する ■ ファイアーウォール ■ 最新のウイルス対策、アップデート ■ 脆弱性診断 ■ 侵入検知、ログ分析 ■ 負荷監視　　等
② 攻撃基盤構築	攻撃指令に基づき、攻撃基盤を構築する（バックドアの構築等）、組織内部の調査	
③ 内部侵入・調査	他のPCやサーバー等へ侵入する	
④ 目的遂行	機密データの外部送信 データの破壊、業務妨害、バックドアを通じた再侵入等	

第2章　セキュリティ対策について現状調査をする

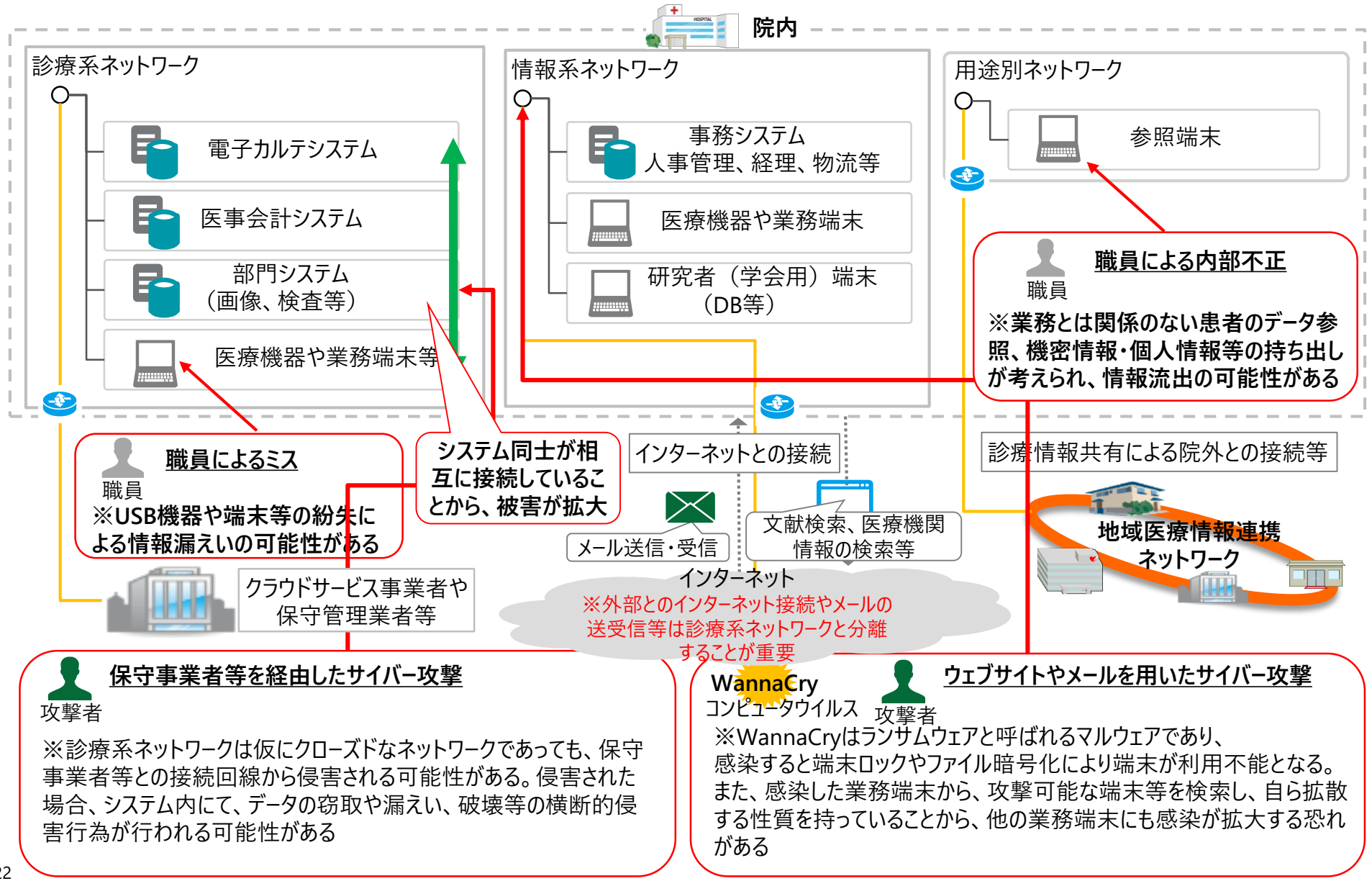
職員のセキュリティに対する意識の現状を把握し、現状に合わせた対応策を取る必要がある
高度なセキュリティ人材を育成することではなく、一般的なセキュリティ意識を持ち、仕事を進めることが出来る人材を育成していくことが重要である



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、複雑化している



院内における情報セキュリティ対策が不十分である場合、様々な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いる可能性がある



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）	経済産業省
等	

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

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

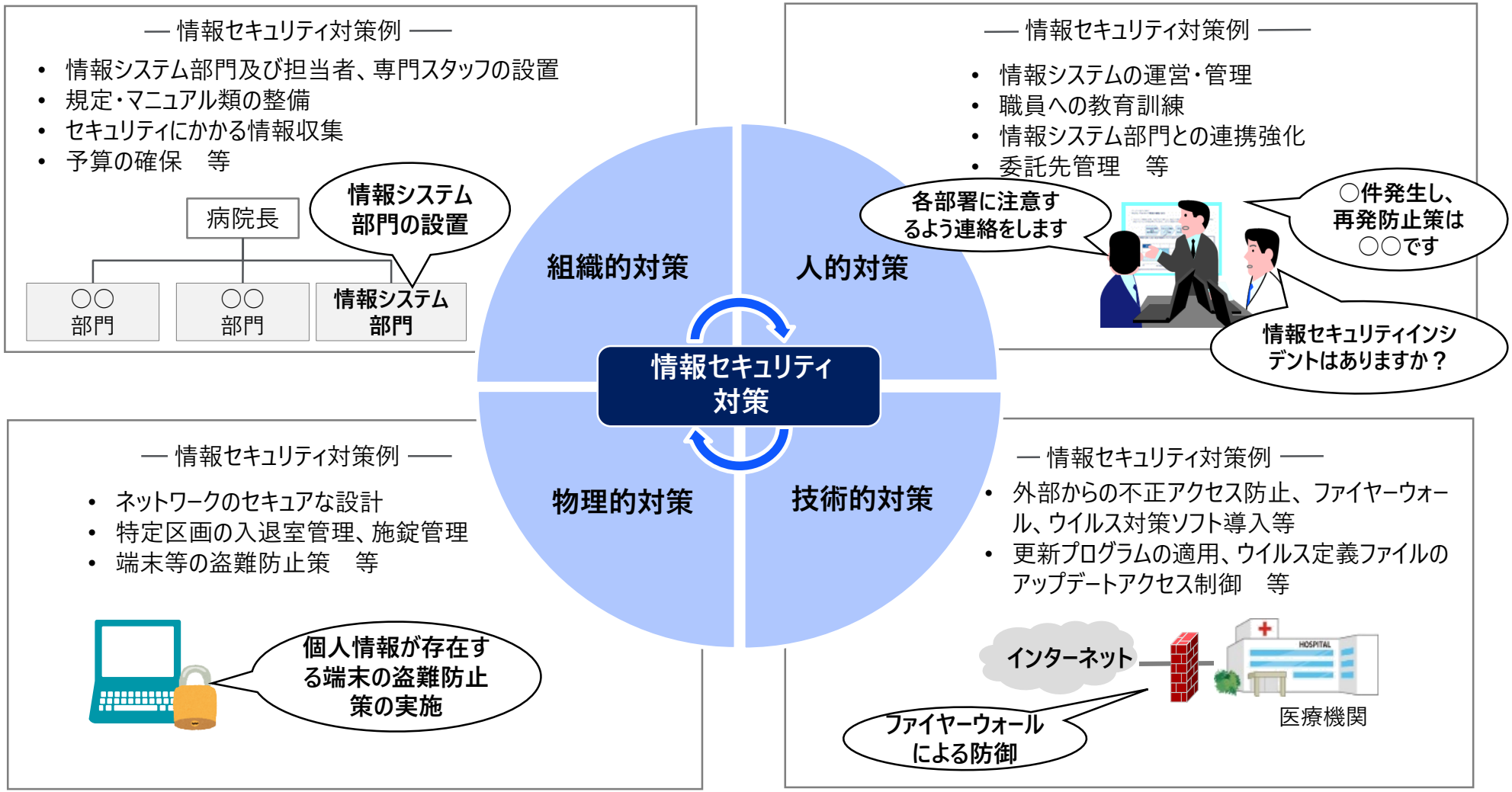
— 医療安全管理での対策例 —

- 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



第3章　サイバーセキュリティ対策のための予算確保と担当者・窓口の設置

情報セキュリティ対策は経営者が主体となって進めることが重要である

基本原則と主な取組について

①情報セキュリティ対策は経営者のリーダーシップで進める	現場の職員は安心して業務に従事できる環境を求める一方で、利便性が低下し、面倒な作業を伴う対策には抵抗感を示しがちです。そのため、情報セキュリティ対策は経営者が自ら判断して意思決定し、主導することが求められます。
②外部委託先の情報セキュリティ対策まで考慮する	委託先に提供した情報が漏えいしたり、改ざんされたとき、それが委託先の不備だったとしても事故を受ける者から委託先としての管理責任を問われることなります。そのため、外部委託先に対して、同等かそれ以上の情報セキュリティ対策を求めることが必要です。
③関係者とは常に情報セキュリティにかかるコミュニケーションを取る	情報セキュリティに関する取組方針を常日頃より関係者に伝えておくことで、サイバー攻撃に関するウイルス感染や情報漏えい等が発生した際にも説明責任を果たすことができ、必要以上の負担を与えることがなく、信頼関係を維持することができます。

取組1
情報セキュリティ対策に関する適宜の見直しを指示する

取組2
緊急時の対応や復旧時の体制について整備する

取組3
委託の場合はセキュリティに関する責任を明確にする

取組4
情報セキュリティにかかる最新動向を収集する

取組5
情報セキュリティ対策にかかる組織全体の対応方針を決める

取組6
情報セキュリティ対策のための予算や人材を確保する

取組7
必要とされる対策を検討させて、実行を指示する

※出所　IPA「中小企業の情報セキュリティ対策ガイドライン」より

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。

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。

ご受講ありがとうございました