福県医発第2762号(地)
令和３年１月 26 日

各 医 師 会 長　殿

福 岡 県 医 師 会
会長　松　田　峻一良
（公　印　省　略）

厚生労働省委託事業「医療機関におけるサイバーセキュリティ研修」開催について

厚生労働省医政局研究開発振興課より、同省が実施している令和２年度厚生労働省委託事業「医療分野におけるサイバーセキュリティ対策調査一式」において、医療機関を中心とした医療分野のサイバーセキュリティ対策の強化を目的に、「医療機関におけるサイバーセキュリティ研修」の開催ならびに、掲示板などの情報共有ツールを用いた情報共有・相談体制の試行を行うため、参加者を募集している旨、日本医師会を通じて周知依頼がありました。

つきましては、貴会におかれましても本件についてご了知いただきますとともに、貴会会員への周知方につき、よろしくお願い申し上げます。

記

１.「医療機関におけるサイバーセキュリティ研修」
（資料１）厚生労働省からの周知依頼
（資料２）開催概要（詳細は別添をご覧ください）
（資料３）参考資料　「経営者向け」研修の資料案
■「システム管理者・セキュリティ管理者」向け研修（定員 50 名）
【 e-learning 】
・研修期間：令和３年２月１日（月）～ 令和３年３月 15 日（月）
・研修時間：60 分程度
【 Webinar （Web 上で行うセミナー） 】
・研修日程：令和３年２月 25 日（木）14:00～16:00

■「医療従事者」向け研修【 e-learning 】（定員 500 名）
・研修日程：令和３年２月１日（月）～ 令和３年３月 15 日（月）
・研修時間：60 分程度

小郡三井医師会より　　医療情報システム担当理事　柳　大三郎
会長　島田昇二郎

２．「医療分野におけるサイバーセキュリティに関する情報共有・相談体制の試行」
（資料４）厚生労働省からの周知依頼
（資料５）募集概要（注意事項等詳細は別添をご覧ください）
・概要：各医療機関で情報システム・サイバーセキュリティに関する業務に従事されている従業員の方を対象として、インターネット上の情報共有ツール（掲示板）にご登録いただき、医療分野におけるサイバーセキュリティに関する情報共有や質問・コメントをいただくことを想定。

・試行期間：2021 年１月中旬から３月末まで

・参加条件：以下の条件を満たす医療機関。
1. 国内にある医療機関であること。
2. 医療機関における情報システムやサイバーセキュリティに関する業務に従事する従業員を参加者として登録すること。
3. 別紙の利用規約に同意すること。

□申し込み方法
１．２．いずれも下記の URL もしくは QR コードのサイトから申込み可能です。
https://www.mhlw.go.jp/stf/cybertraining2020.html

※信頼性担保のため、上記の厚労省 HP 内に案内サイトから、それぞれの募集ページへのリンクを掲載しています。

（情シ 48）
令和 3 年 1 月 19 日

都道府県医師会
情報システム担当理事殿

日本医師会常任理事
長　島　公　之
（公印省略）

厚生労働省委託事業
「医療機関におけるサイバーセキュリティ研修」開催について　（周知）

拝啓　時下ますますご健勝のこととお慶び申し上げます。日頃より会務運営に対しましてご高配を賜り深く感謝申し上げます。

厚生労働省が実施しております、令和２年度厚生労働省委託事業「医療分野におけるサイバーセキュリティ対策調査一式」において、医療機関を中心とした医療分野のサイバーセキュリティ対策の強化を目的に、「医療機関におけるサイバーセキュリティ研修」の開催ならびに、掲示板などの情報共有ツールを用いた情報共有・相談体制の試行を行うため、参加者を募集しております。つきましては貴会会員に対し、別添案内の周知方お願い申し上げます。

敬具

１.「医療機関におけるサイバーセキュリティ研修」
（資料１）厚生労働省からの周知依頼
（資料２）開催概要（詳細は別添をご覧ください）
■「経営層」向け研修【 Webinar（Web 上で行うセミナー） 】（定員 50 名）
・研修日程：令和 3 年 1 月 25 日（月）　16:00～17:00

■「システム管理者・セキュリティ管理者」向け研修（定員 50 名）
【 e-learning 】
・研修期間：令和 3 年 2 月 1 日（月）～ 令和 3 年 3 月 15 日（月）
・研修時間：60 分程度
【 Webinar （Web 上で行うセミナー） 】
・研修日程：令和 3 年 2 月 25 日（木）　14:00～16:00

■「医療従事者」向け研修【 e-learning 】（定員 500 名）
・研修日程：令和 3 年 2 月 1 日（月）～ 令和 3 年 3 月 15 日（月）
・研修時間：60 分程度
（資料３）参考資料　「経営者向け」研修の資料案

２．「医療分野におけるサイバーセキュリティに関する情報共有・相談体制の試行」

（資料４）厚生労働省からの周知依頼

（資料５）募集概要（注意事項等詳細は別添をご覧ください）

・概要：各医療機関で情報システム・サイバーセキュリティに関する業務に従事されている従業員の方を対象として、インターネット上の情報共有ツール（掲示板）にご登録いただき、医療分野におけるサイバーセキュリティに関する情報共有や質問・コメントをいただくことを想定。

・試行期間：2021 年 1 月中旬から 3 月末まで

・参加条件：以下の条件を満たす医療機関。

1. 国内にある医療機関であること。
2. 医療機関における情報システムやサイバーセキュリティに関する業務に従事する従業員を参加者として登録すること。
3. 別紙の利用規約に同意すること。

□申し込み方法

１．２．いずれも下記の URL もしくは QR コードのサイトから申込み可能です。

https://www.mhlw.go.jp/stf/cybertraining2020.html

※信頼性担保のため、上記の厚労省 HP 内に案内サイトから、それぞれの募集ページへのリンクを掲載しています。

以上

資料１

事　務　連　絡
令和３年１月８日

公益社団法人日本医師会
　情報システム担当理事　殿

厚　生　労　働　省
医政局研究開発振興課
医療情報技術推進室長
（公　印　省　略）

医療機関におけるサイバーセキュリティ研修開催の周知について（協力依頼）

平素から、医療分野の情報化の推進にご理解とご協力を賜り厚くお礼申し上げます。

標記について、医療機関を中心とした医療分野のサイバーセキュリティ対策の強化を目的として、令和２年度厚生労働省委託事業「医療分野におけるサイバーセキュリティ対策調査一式」を実施しております。

本事業において、医療機関関係者の皆様を対象として、「医療機関におけるサイバーセキュリティ研修」を開催させて頂きます。つきましては貴会会員の皆様に対し、ご案内（別添１）の周知のほど何卒よろしくお願い申し上げます。

なお、別添２は、本研修のうち「経営者向け」研修の資料案となりますので、参考に添付させて頂きます。

資料２　別添１

令和３年１月８日

関係者各位

有限責任監査法人トーマツ
医療分野におけるサイバーセキュリティ対策調査業務
事務局

厚生労働省委託事業　令和２年度「医療分野におけるサイバーセキュリティ対策調査業務」
医療機関におけるサイバーセキュリティ研修開催のご案内

拝啓　時下ますますご清栄のこととお喜び申し上げます。

当法人では厚生労働省「医療分野におけるサイバーセキュリティ対策調査業務」の委託を受けまして、医療機関関係者の皆様を対象として、「医療機関におけるサイバーセキュリティ研修」を開催させて頂きます。つきましては下記の研修の背景、目的および次頁の研修概要をご確認頂きまして、研修参加をご検討頂きたく、何卒宜しくお願い申し上げます。

敬具

記

- **研修の背景**

平成 27 年 9 月 4 日閣議決定「サイバーセキュリティ戦略」において『機能が停止又は低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして官民が一丸となり重点的に防護していく必要がある。その際、民間は全てを政府に依存するのではなく、政府も民間だけに任せるのではない、緊密な官民連携が求められる』とされています。
重要インフラに該当する医療分野では、厚生労働省と医療機関等が連携し、実効性のある情報セキュリティ対策を講じていくことが求められました。

また、平成 30 年 7 月 27 日に閣議決定された現行の「サイバーセキュリティ戦略」では、従来の枠を超えた情報共有・連携体制の構築として、国は ISAC(Information Sharing and Analysis Center/情報共有分析組織)を含む情報共有における取組の推進を支援するとともに、新たな役割を果たしていくことが求められています。

その後に公開された年次計画「サイバーセキュリティ 2019」（令和元年 5 月 23 日にサイバーセキュリティ戦略本部決定）においても、厚生労働省は医療分野の ISAC 等の情報共有のあり方について引き続き検討することとしています。

- **研修の目的**

こうした中、今年度においては、医療分野におけるサイバーセキュリティ対策に関する情報共有体制の構築に向けた検討を進めるとともに、並行して医療従事者の情報セキュリティに関するリテラシー向上も図っていく必要があり、本研修はリテラシー向上の一環としての位置付けとなっています。

➢ **研修の概要**

医療機関関係者の皆様を対象として、医療分野のサイバーセキュリティに関するリテラシー向上を目的とした研修を開催します。研修は「経営層」、「システム管理者（含むセキュリティ管理者）」、「医療従事者（医師、コメディカル、事務職員（システム部門以外））」と対象を分けて開催します。

■ **「経営層」向け研修（定員 50 名様）**

【 Webinar（Web 上で行うセミナー） 】

- ✓ 研修日程：令和 3 年 1 月 25 日（月）
- ✓ 研修時間：16:00～17:00
- ✓ 研修概要：経営層としてサイバーセキュリティ事故を防ぐ為に認識すべき事項を学ぶ

■ **「システム管理者・セキュリティ管理者」向け研修（定員 50 名様）**

【 e-learning 】

- ✓ 研修期間：令和 3 年 2 月 1 日（月）～ 令和 3 年 3 月 15 日（月）
- ✓ 研修時間：60 分程度

【 Webinar （Web 上で行うセミナー） 】

- ✓ 研修日程：令和 3 年 2 月 25 日（木）
- ✓ 研修時間：14:00～16:00
- ✓ 研修概要：インシデント対応に関するロールプレイング
- ✓ 研修ツール：インシデント対応ボードゲーム

※Webinar 参加者は、参加前に e-learning での事前研修を受講頂くことが必須です。当日 13:00 より、研修会場にて e-learning を受講頂くことも可能です）

※Webinar 終了後は e-learning 研修のみ受講できます。

■ **「医療従事者」向け研修（定員 500 名様）**

【 e-learning 】

- ✓ 研修日程：令和 3 年 2 月 1 日（月）～ 令和 3 年 3 月 15 日（月）
- ✓ 研修時間：60 分程度
- ✓ 研修概要：サイバーセキュリティ事故を防ぐ為に医療従事者に求められる役割を学ぶ

➢ **お申込み方法**

下記の URL もしくは QR コードを読込んで頂き、お申込みサイトからお申込みいただけます。
令和 2 年 12 月 23 日（水）から受付開始いたします。

URL：

https://www.mhlw.go.jp/stf/cybertraining2020.html

QR コード：

なお、本件に対するお問い合わせは以下のアドレスまでメールでお願い致します。

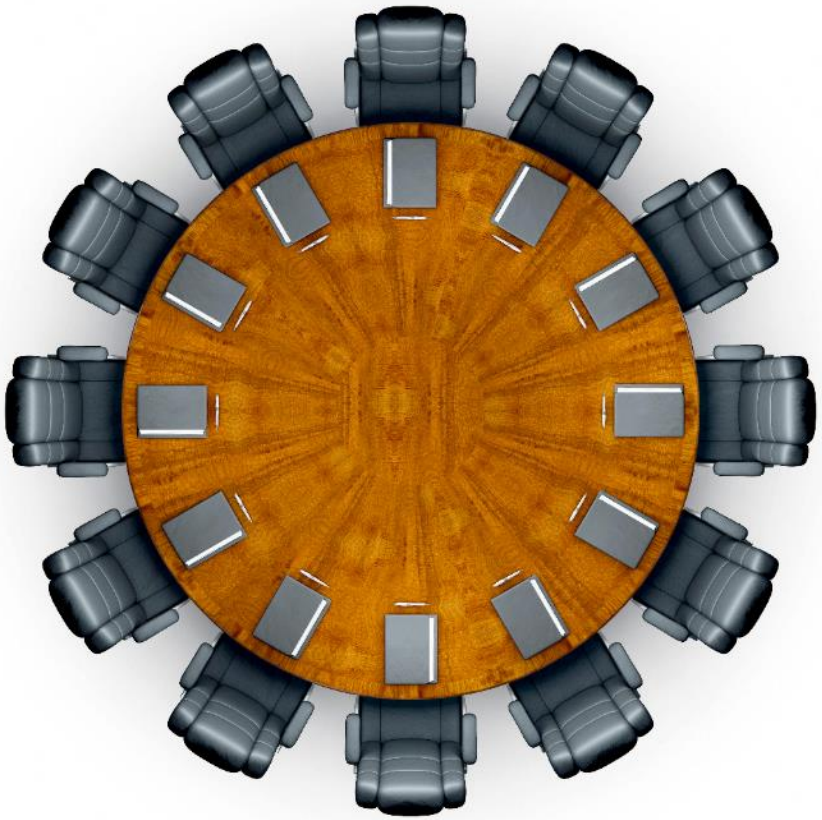
MAIL：cybersecurity_contact@tohmatsu.co.jp

皆様のご参加をお待ちしております。何卒宜しくお願い申し上げます。

以上

資料３

別添2



「情報セキュリティ研修教材（経営層向け）」（案）

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

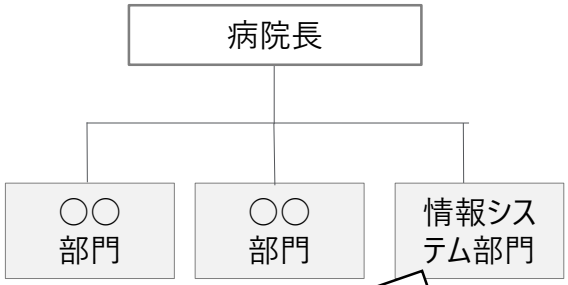
情報セキュリティ対策の実施状況

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

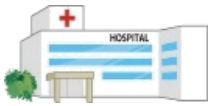
医療機関 → 依頼 → コンサルティング会社、システムベンダー等

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



医療機関 → 外部監査依頼等 → 被監査主体から独立した組織等

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	○○　○○

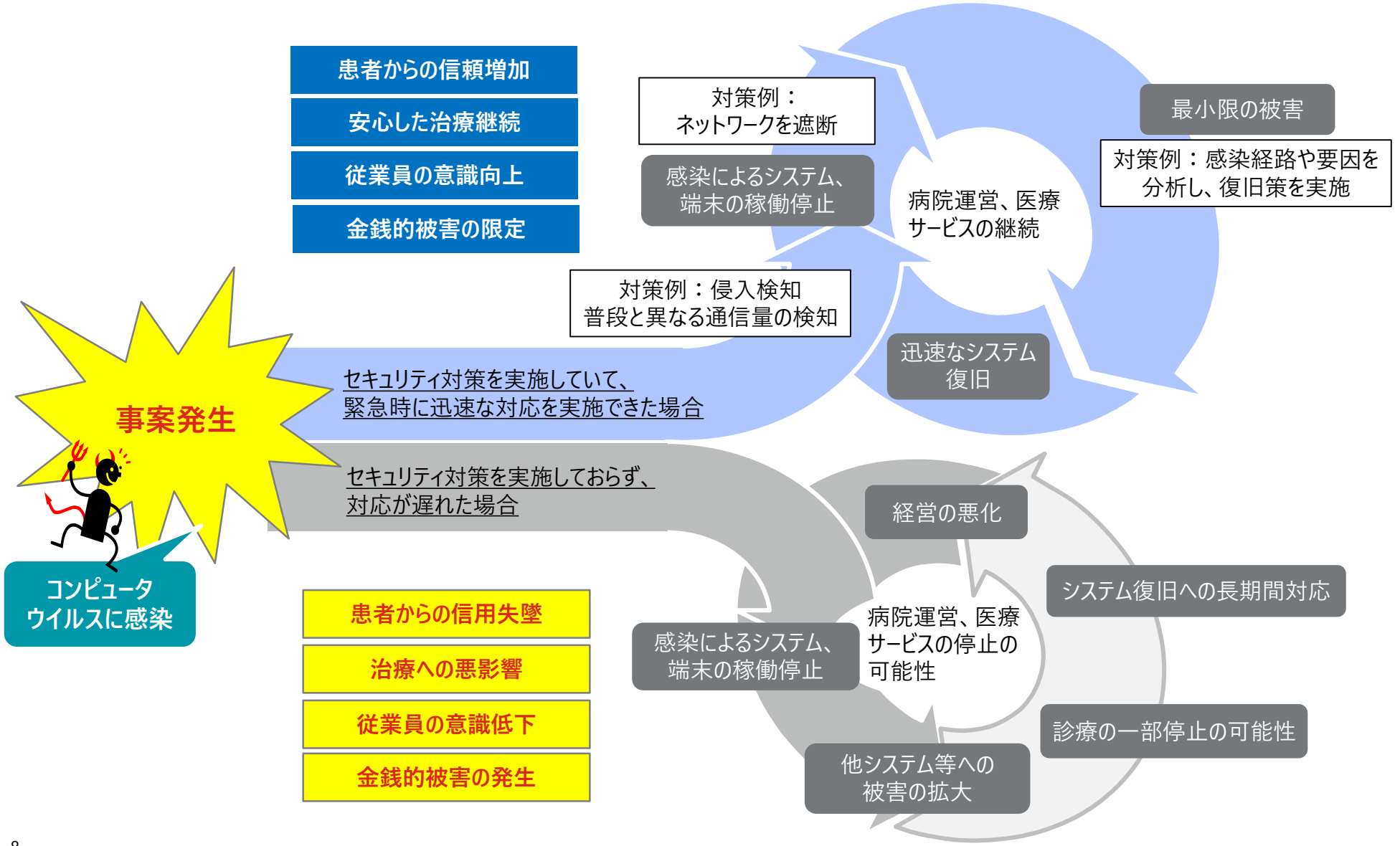
最後に・・・
サイバーセキュリティ担当者をほめてください

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！！！

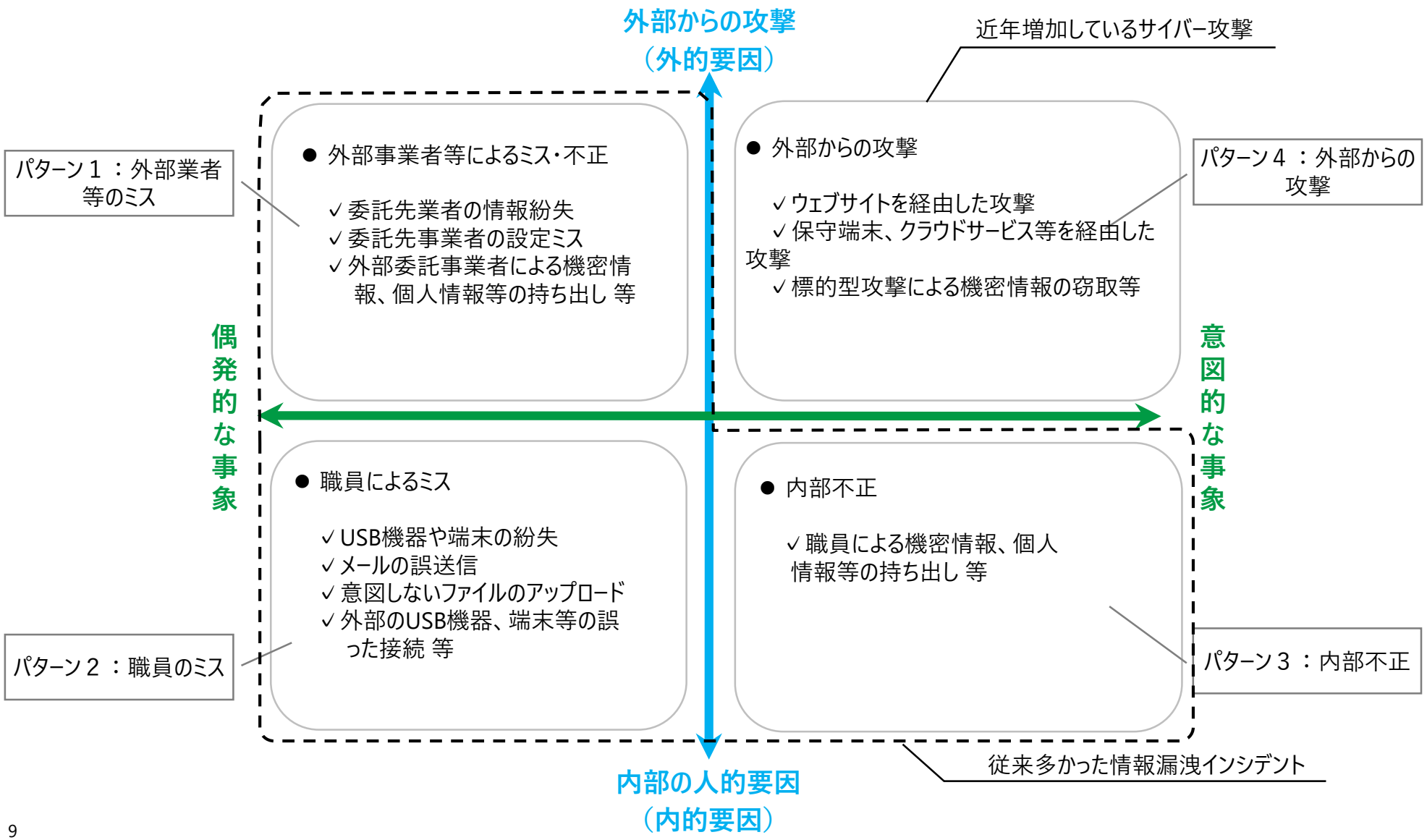
目次

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

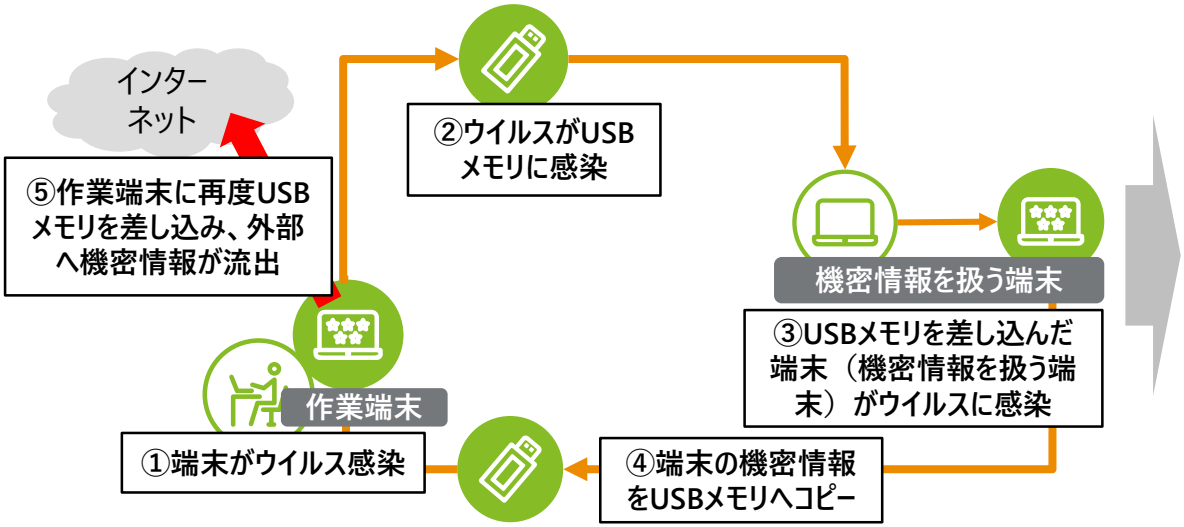
明示の例

- ■ 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

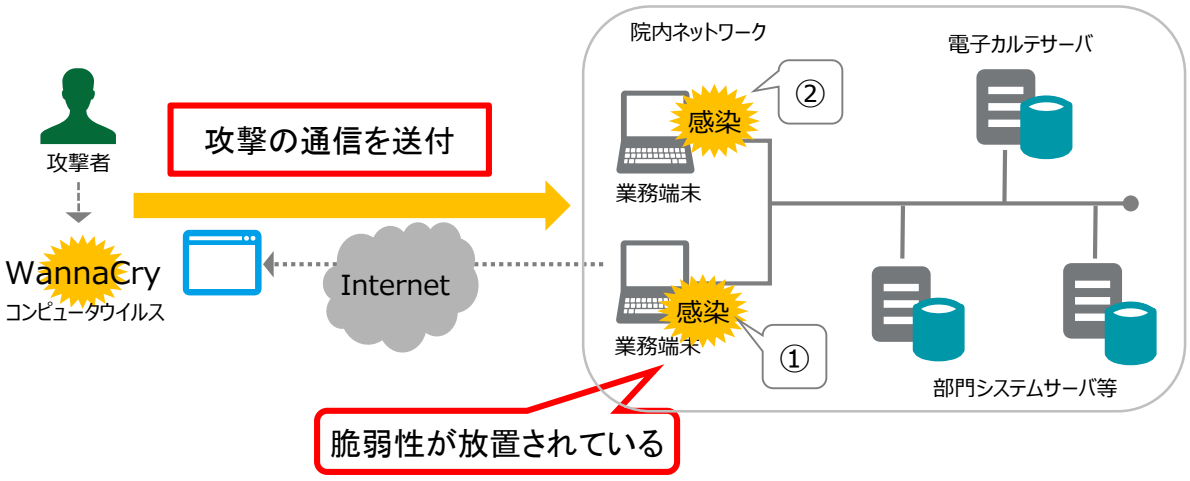
③相互点検の実施
担当者間、部門間等で相互に運用状況の点検を実施し、相互牽制を働かせる

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

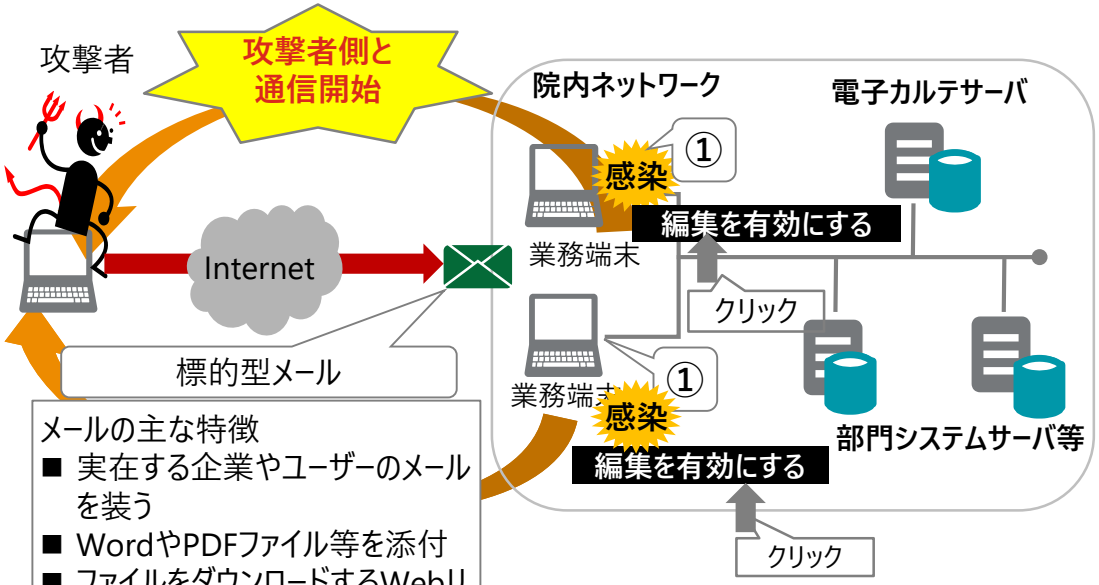
要因

- **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）



メールの主な特徴
- 実在する企業やユーザーのメールを装う
- WordやPDFファイル等を添付
- ファイルをダウンロードするWebリンク先を記載

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

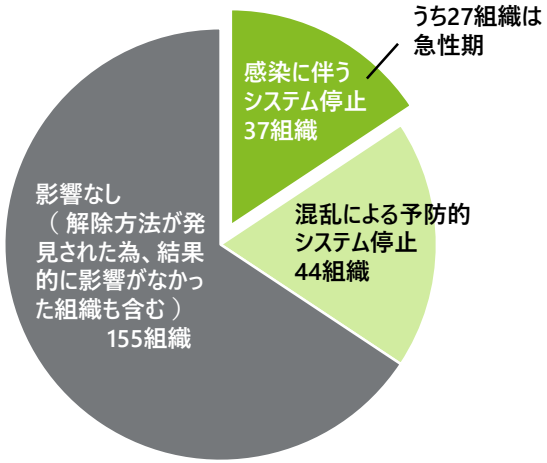
要因

- 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



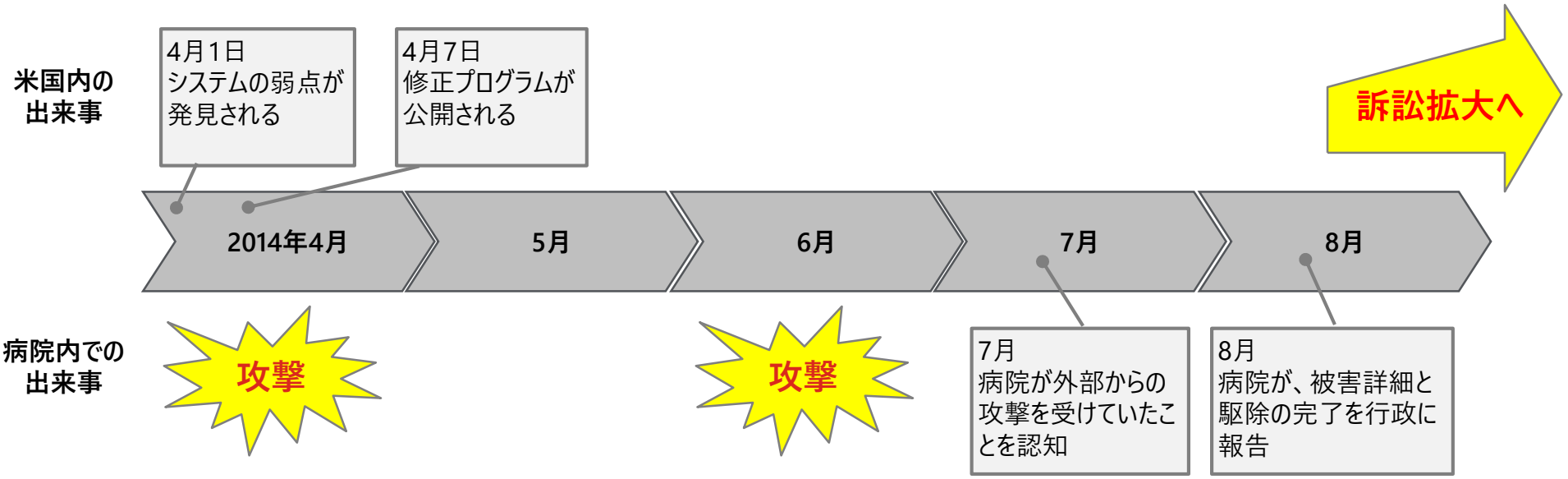
（出典）Investigation: WannaCry cyber attack and the NHS, National Audit Officeなどに基づき作成

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

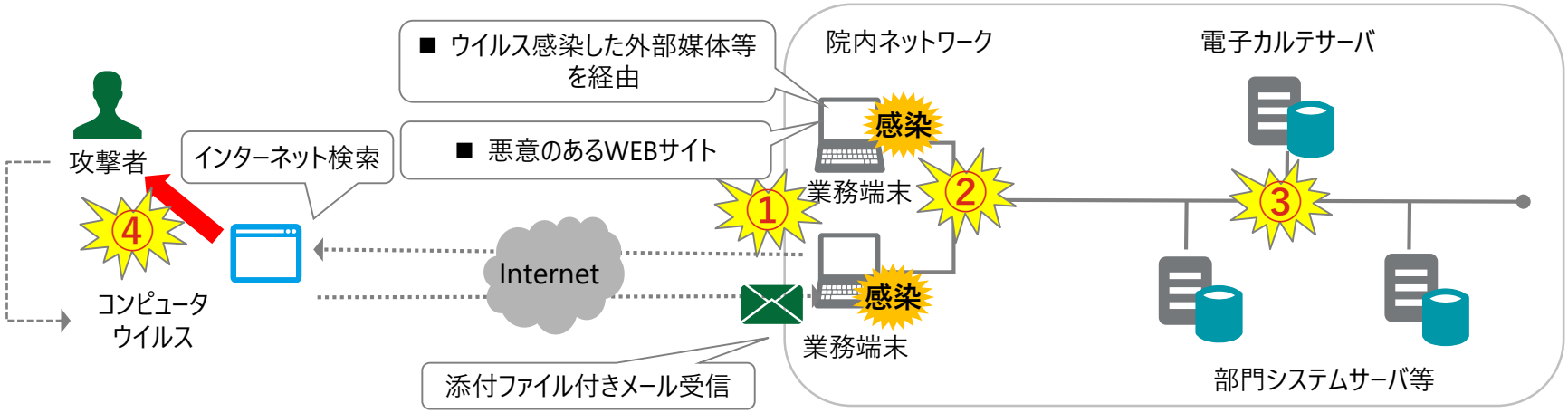
- 2014年8月、米国内29州で206施設を運営する大手民間病院グループが、外部からのサイバー攻撃により、患者約450万人分の個人情報が流出した可能性があることを外部公表した
- 原因は、発見されたばかりの暗号通信技術の弱点を利用されたものであった
- 英国の事例とは異なり、明確に当該グループのシステムを狙った高度な攻撃だったと考えられている
- 全米規模で発生した集団訴訟は2018年3月以降も係争中であり、病院に大きな影響を与えている



（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

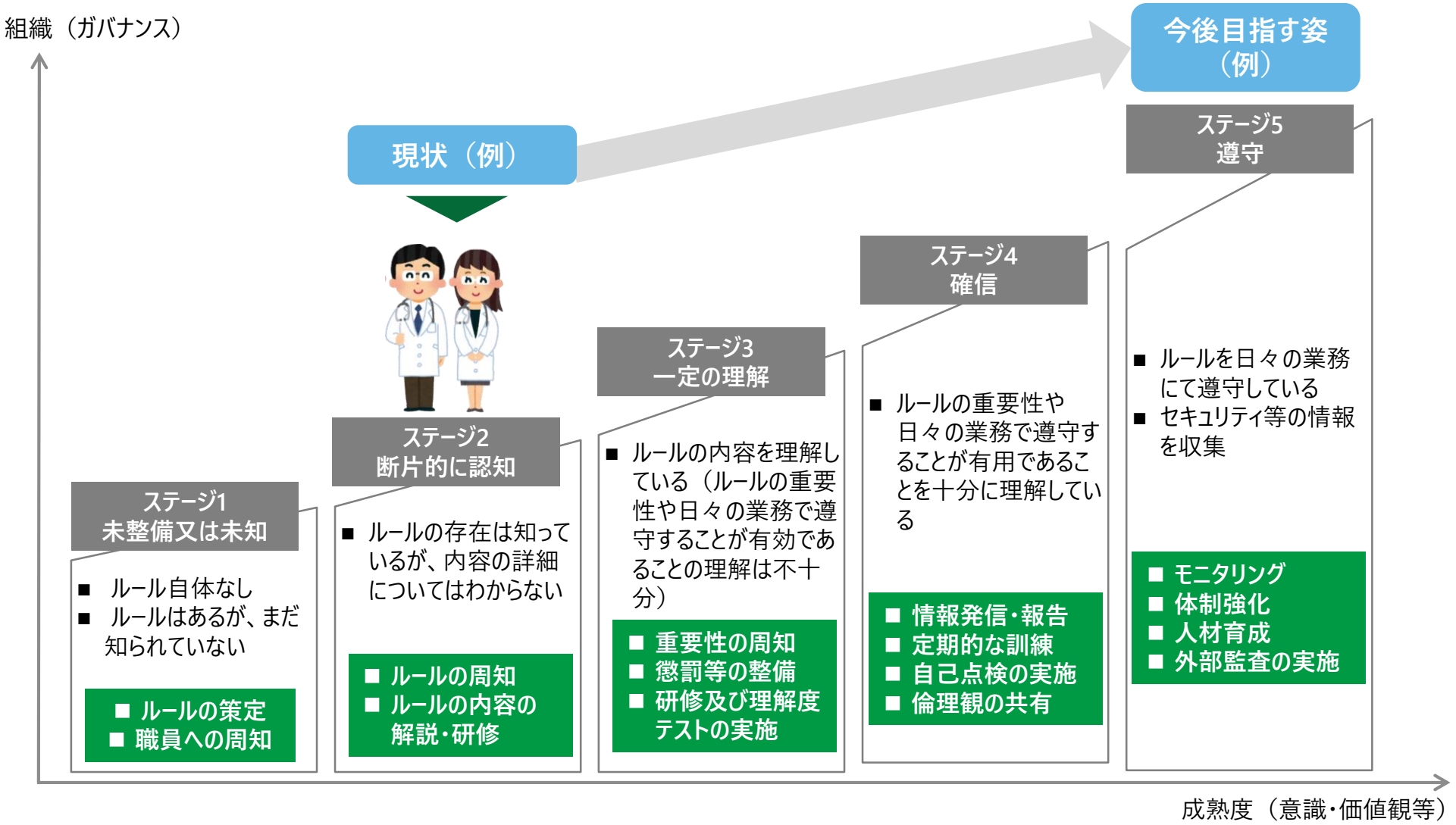


	攻撃の説明	対策例（多層防御の考え方）
① 初期侵入	悪意あるWEBサイトや添付ファイル付きメール等を経由してマルウェアが組織内部に侵入する	■ ユーザーである職員への教育を適切に実施し、不自然なメールの開封やダウンロード等を防止する ■ ファイアーウォール ■ 最新のウイルス対策、アップデート ■ 脆弱性診断 ■ 侵入検知、ログ分析 ■ 負荷監視　　等
② 攻撃基盤構築	攻撃指令に基づき、攻撃基盤を構築する（バックドアの構築等）、組織内部の調査	
③ 内部侵入・調査	他のPCやサーバー等へ侵入する	
④ 目的遂行	機密データの外部送信 データの破壊、業務妨害、バックドアを通じた再侵入等	

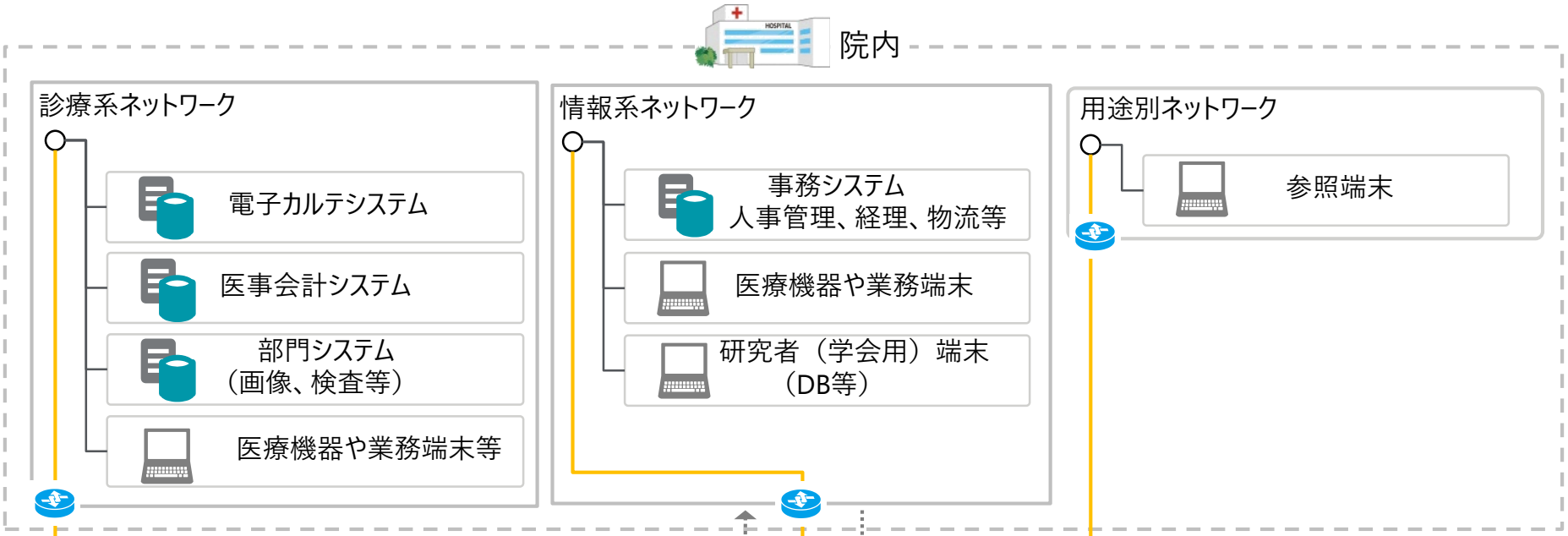
第2章　セキュリティ対策について現状調査をする

2-1 職員へのルールの周知や遵守について

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



院外のサービス事業者との接続

クラウドサービス事業者や
保守管理業者等

インターネットとの接続

メール
送信・受信

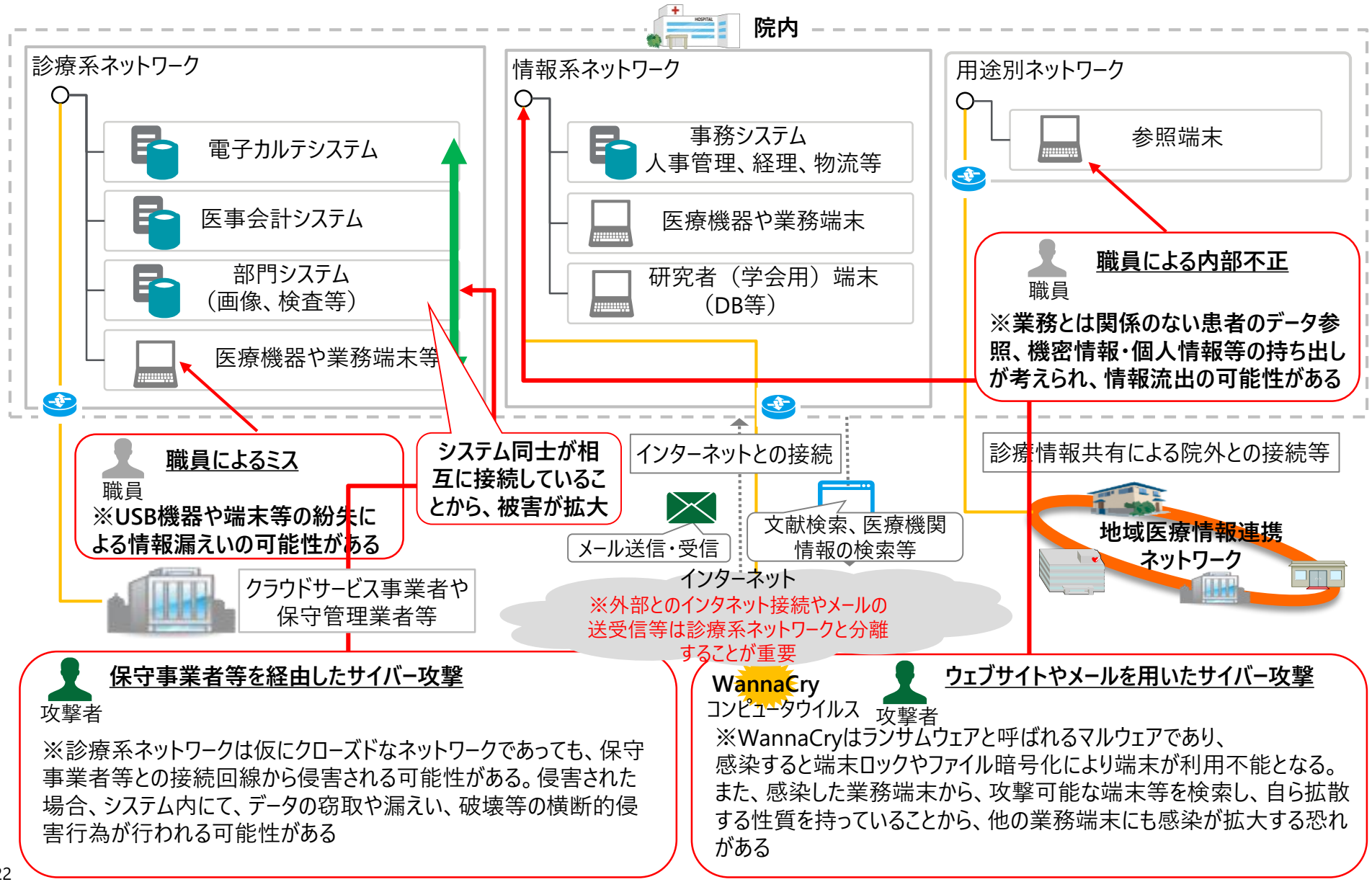
文献検索、医療機関
情報の検索等

インターネット

診療情報共有による院外との接続等

- 地域医療連携ネットワーク（診療情報等）との接続
- 検査機関との接続
- 在宅、介護施設との接続
- 遠隔医療等

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
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

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

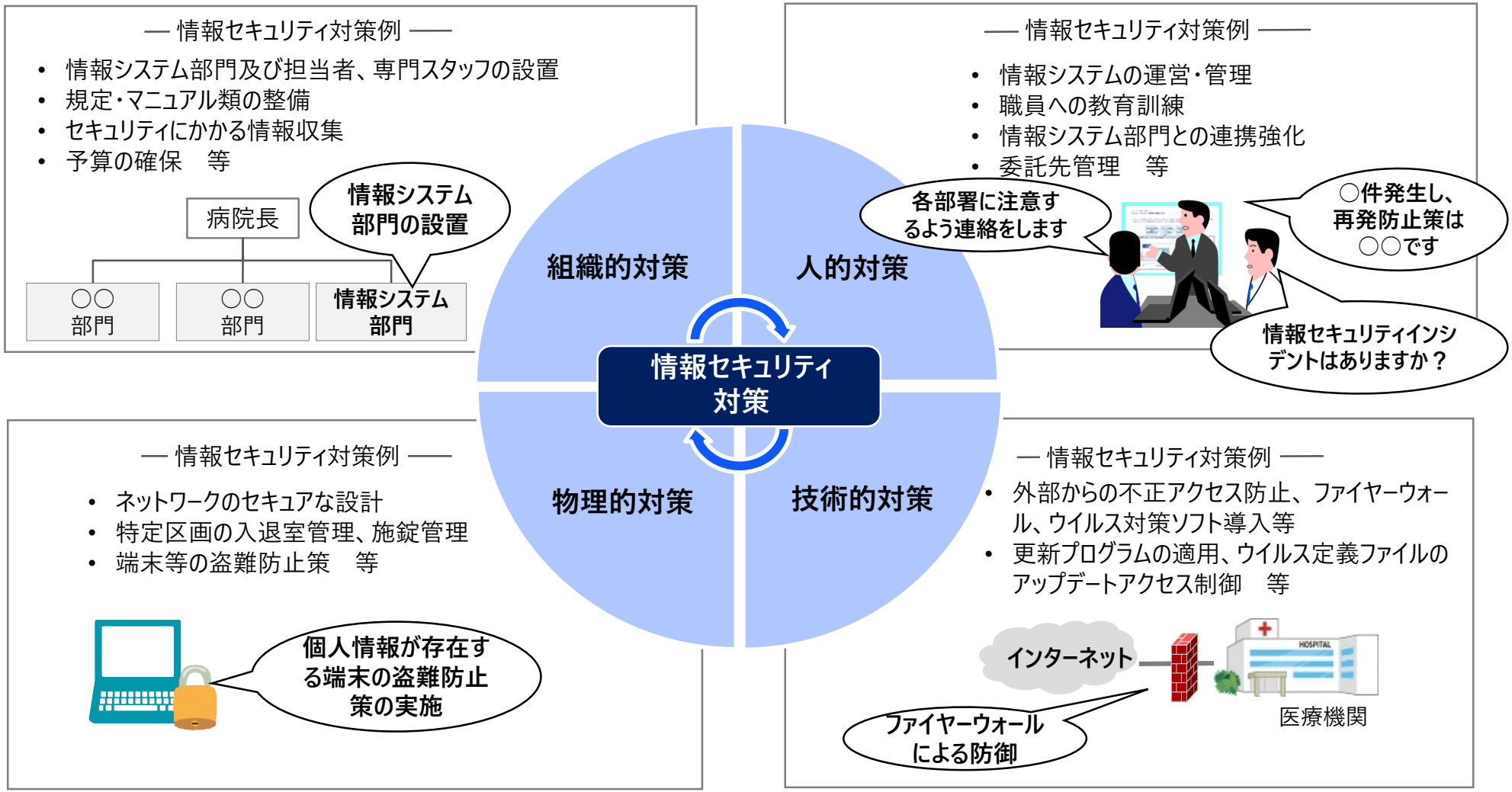
— 医療安全管理での対策例 —

- 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技術情報推進室へ連絡する。
- 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

資料４

事　務　連　絡
令和３年１月14日

公益社団法人日本医師会
　情報システム担当理事　殿

厚　生　労　働　省
医政局研究開発振興課
医療情報技術推進室長
（公　印　省　略）

医療分野におけるサイバーセキュリティに関する情報共有・相談体制の試行の
周知について（協力依頼）

平素から、医療分野の情報化の推進にご理解とご協力を賜り厚くお礼申し上げます。

標記について、医療機関を中心とした医療分野のサイバーセキュリティ対策の強化を目的として、令和２年度厚生労働省委託事業「医療分野におけるサイバーセキュリティ対策調査一式」を実施しております。

本事業において、医療分野におけるサイバーセキュリティに関す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ことを目的として、医療関係者のご協力を賜りつつ、掲示板などの情報共有ツールを用いた情報共有・相談体制の試行を行います。つきましては貴会会員の皆様に対し、ご案内（別添）の周知のほど何卒よろしくお願い申し上げます。

資料５

令和３年１月 14 日

関係者各位

有限責任監査法人トーマツ
医療分野におけるサイバーセキュリティ対策調査
事務局

厚生労働省委託事業　令和２年度「医療分野におけるサイバーセキュリティ対策調査」
医療分野におけるサイバーセキュリティに関する情報共有・相談体制の試行へのご協力のお願い

拝啓　時下ますますご清栄のこととお喜び申し上げます。

当法人では厚生労働省「医療分野におけるサイバーセキュリティ対策調査」の委託を受けまして、「医療分野におけるサイバーセキュリティに関する情報共有・相談体制の試行」にご協力いただける医療機関を募集したく、下記のとおりご案内させていただきます。何卒宜しくお願い申し上げます。

敬具

記

１．試行の背景

平成 27 年９月４日閣議決定「サイバーセキュリティ戦略」では、『機能が停止又は低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして官民が一丸となり重点的に防護していく必要がある。その際、民間は全てを政府に依存するのではなく、政府も民間だけに任せるのではない、緊密な官民連携が求められる』とされ、重要インフラに該当する医療分野においても、厚生労働省と医療機関等が連携し、実効性のある情報セキュリティ対策を講じていくことが求められています。また、平成 30 年７月 27 日に閣議決定された現行の「サイバーセキュリティ戦略」では、従来の枠を超えた情報共有・連携体制の構築として、ISAC（Information Sharing and Analysis Center/情報共有分析組織）を含む情報共有における取り組みを推進していくことが示されています。

２．目的

本委託事業では、今年度、医療分野におけるサイバーセキュリティに関す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ことを目的として、医療関係者のご協力を賜りつつ、掲示板などの情報共有ツールを用いた情報共有・相談体制の試行を行います。

３．概要

このたび、本委託事業での試行にご協力いただける医療機関を募集いたします。

なお、本試行では、各医療機関で情報システム・サイバーセキュリティに関する業務に従事されている従業員の方を対象として、インターネット上の情報共有ツール（掲示板）にご登録いただき、医療分野におけるサイバーセキュリティに関する情報共有や質問・コメントをいただくことを想定しております。

サイバーセキュリティに関する情報共有の意義

- 医療機関という共通の立場にある関係者が、医療機関に特有なサイバーセキュリティに関する課題や、最新の知見を相互に共有・相談することで、より具体的・実効的な対策を共有しつつ、担当者のリテラシーを向上させることができる。
- ある医療機関が特定の医療機器に関する脆弱性情報を入手したり、外部からの攻撃を検知した場合に、これを他の医療機関とも共有することで、他の医療機関も早期に対策を実施できる。

共有・相談する内容の例

Q. 院内システムに対するサイバーセキュリティ対策の予算申請に関して、他の医療機関の担当者はどのような点に留意しているのか？

Q. 医療情報システムの管理やサイバーセキュリティ対策について、他の医療機関ではどのような規程を整備・運用しているのか？

Q. 医療機関におけるシステム停止や情報漏えいに関する報道があった場合に、自組織としては具体的にどのように対応・対策をすべきか？

Q. 不正アクセスを検知した場合に、情報システム業者への指示や業者に報告させるべき事項について、他の医療機関の担当者はどのような点に留意しているのか？

Q. 自組織に対するサイバー攻撃を検知した際、二次被害を防止するため、インディケータ情報（サイバー攻撃を受けていることを検知するための方法・手がかりとなる情報）を共有したい。

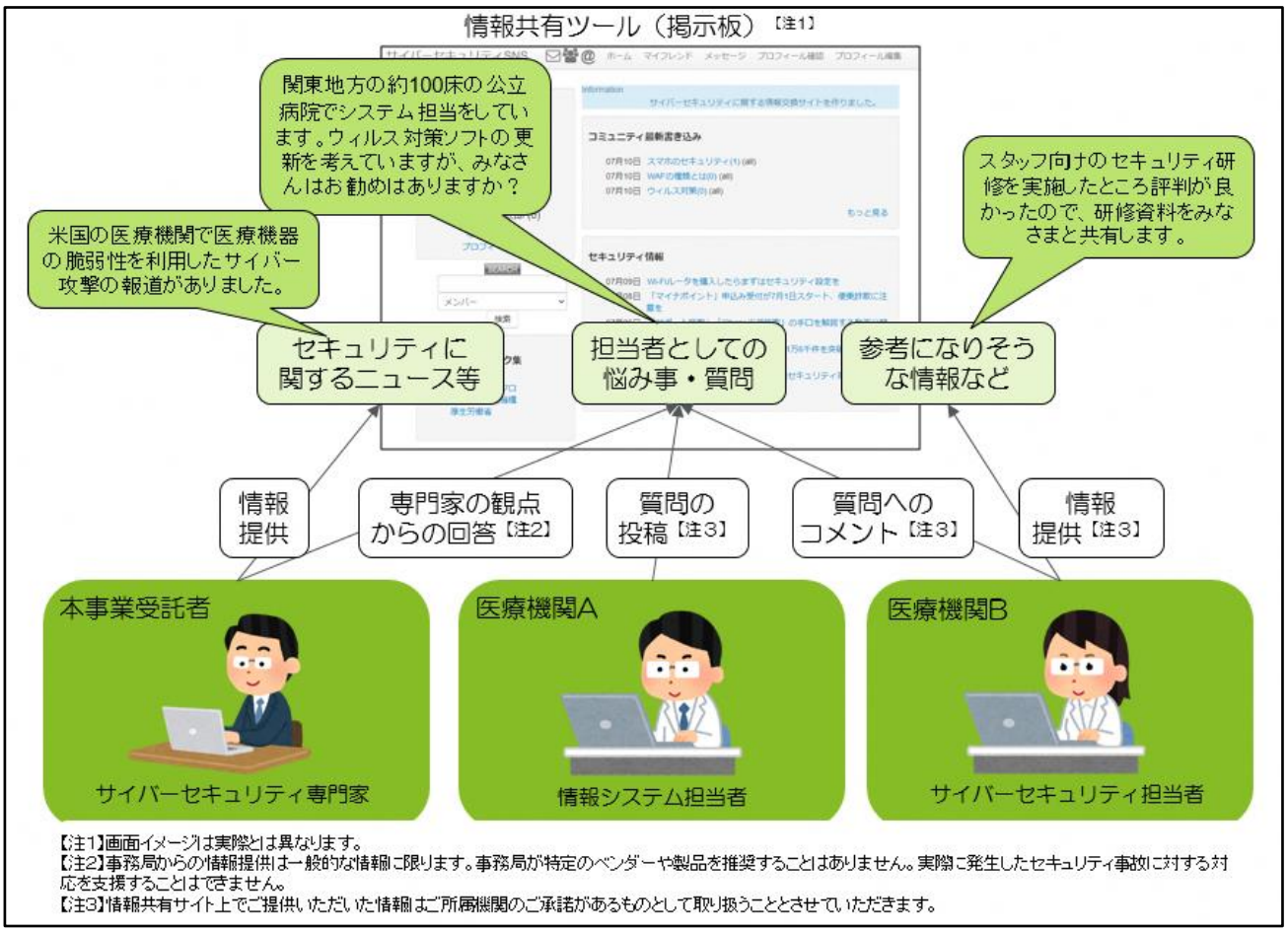


図 1 情報共有のイメージ

試　行　期　間：2021 年 1 月中旬から 3 月末まで

情報共有サイト：一般社団法人 JPCERT コーディネーションセンターが提供する SIGNAL を利用

参　加　条　件：本試行では、以下の条件を満たす医療機関を募集しております。

1. 国内にある医療機関であること。
2. 医療機関における情報システムやサイバーセキュリティに関する業務に従事する従業員を参加者として登録いただけること。
3. 別紙の利用規約に同意いただけること。

注　意　事　項：1. 情報共有サイト上でご提供いただいた情報はご所属機関のご承諾があるものとして取り扱うこととさせていただきます。
2. 情報共有サイトに接続するための通信機器・通信回線に要する費用は各医療機関にてご負担ください。
3. 各参加者が利用される OS やブラウザの種類・バージョンに情報共有サイトが対応していない場合や、医療機関において上記情報共有サイトへのアクセスが許可されていない場合などは、お申込みいただいてもご利用いただけない場合があります。

４．お申込みの方法

ご協力いただける医療機関におかれましては、連絡担当者を 1 名ご指定いただき、以下の申込フォームにて必要事項をご記入の上、お申込みください。

■申込フォーム URL

https://www.mhlw.go.jp/stf/cybertraining2020.html

■QR コード

注 1．申込フォームよりご提供いただいた個人情報は本試行の運営の目的および厚生労働省からの来年度以降の情報提供の目的で利用いたします。個人情報の取扱いについては別紙利用規約をご覧ください。

注 2．同一医療機関では連絡担当者を含め最大 5 名までの登録とさせていただきます。

注 3．ご登録いただくメールアドレスは、原則として医療機関のドメインであるもののみとさせていただきます。フリーメールアドレス以外に登録アドレスがない場合は、下記事務局にご相談ください。ご登録内容がご本人様からのものであることが確認できない場合は、申請をお断わりする場合があります。

５．お問合せ先

本試行へのご応募その他本件に関するお問合せは下記事務局までお問合せください。

事務局：有限責任監査法人トーマツ

メールアドレス：hccyber2021@tohmatsu.co.jp

メールタイトルに「情報共有の試行に関する問合せ」とご記入ください。

以上

別紙
厚生労働省令和２年度事業「医療分野におけるサイバーセキュリティ対策調査」に係る「医療分野におけるサイバーセキュリティに関する情報共有・相談体制の試行」における情報共有サービス利用規約

初版発行：2021 年 1 月 11 日

第１章 総則

第１条　目的

本利用規約は、有限責任監査法人トーマツが厚生労働省から受託した令和２年度事業「医療分野におけるサイバーセキュリティ対策調査」（以下、本事業という）に係る「医療分野におけるサイバーセキュリティに関する情報共有・相談体制の試行」（以下、本業務という）の一環として、医療分野におけるサイバーセキュリティに関する情報共有サービスをインターネット上で提供するにあたり、当該サービスの利用条件について定めることを目的とする。

第２条　用語定義

本利用規約において使用する用語を以下のように定める。

① 本サービスとは、本業務に関連してサービス提供者が提供するインターネット上の情報共有サービスをいう。
② サービス提供者とは、有限責任監査法人トーマツをいう。
③ サービス申込者とは、本サービスを利用することを申し込む法人、機関等をいう。
④ サービス利用者とは、サービス申込者のうち、サービス提供者によって本サービスを利用することを認められた法人、機関等をいう。
⑤ ユーザーとは、サービス利用者が承認し、本サービスを利用する者をいう。
⑥ 利用契約とは、本利用規約に基づきサービス提供者とサービス利用者との間に締結される本サービスの提供に関する契約をいう。
⑦ 提供情報とは、サービス利用者が本サービスを利用して他のサービス利用者に提供する情報をいう。
⑧ サービス利用者側システムとは、サービス利用者が本サービスを利用するにあたって必要となる情報システム等（パソコン等の端末機器、ソフトウェア、電気通信回線を含むが、これらに限らない）をいう。

第３条　本利用規約の適用

1　サービス提供者は、利用契約の内容に従って本サービスの提供を行い、サービス利用者は、利用契約及びサービス提供者が定める条件にてこれを利用するものとする。
2　本利用規約は、サービス提供者とサービス利用者との間における本サービスに係る一切の関係について適用される。

第４条　本利用規約の変更

1　サービス提供者は、サービス利用者の事前の承諾を得ることなく、本利用規約を随時変更することができるものとし、本利用規約が変更された後のサービス提供条件は、変更後の新利用規約に従うものとする。
2　サービス提供者は、前項の変更を行う場合は、事前に変更後の新利用規約の内容をサービス利用者に通知又は本サービス上に表示するものとする。但し、変更内容が軽微なものであってサービス利用者に特に不利益にならないとサービス提供者が判断した場合は、かかる通知又は表示を省略することがある。
3　サービス利用者が変更後の利用規約に同意できない場合は、利用規約の変更が有効になる前にサービス提供者に通知することによって、利用契約を解除できるものとする。

第２章　利用契約

第５条　サービス利用の申込

1　サービス申込者は、予め本利用規約に同意の上、サービス提供者が指定する方法により、本サービスの利用の申込を行う。
2　利用契約は、サービス提供者が第７条に基づきサービス利用者にユーザーＩＤ等を通知することもって成立するものとし、本利用規約は利用契約の一部を構成する。

第６条　サービス申込者の条件

1　サービス申込者は、本サービスの利用申込にあたり、次の各号に掲げる条件をすべて満たさなければならない。
　① 日本国内に実在する医療機関であること。
　② 自己の情報システム又はサイバーセキュリティに関する業務に関与する従業者をユーザーとすること。
2　サービス提供者は、サービス申込者が次の各号に掲げる場合のいずれかに該当するときは、サービス申込者による申込を承諾しない、あるいは承諾を留保することができる。
　① 前項の条件を満たさない場合。
　② 提供を受けたサービス申込者及びユーザーに関する情報に不備があるとき、又は真実でない場合。
　③ 本サービスの利用目的が、本来の目的（医療分野におけるサイバーセキュリティに関する情報共有）とは異なるものであると疑われる場合。
　④ 第２８条第１項又は第２項の確約に違反している、あるいは違反するおそれがあるとサービス提供者が判断した場合。
　⑤ その他、申込を承諾することが本業務の遂行上、不適当とサービス提供者が判断した場合。
3　サービス提供者は、本サービスの設備や技術上の課題によって、サービス申込者に本サービスを提供することが困難な場合（サービス利用者が多数になることによって、本サービスの提供が困難となる、あるいは、本サービスの改修が必要となる場合を含む）は、申込を承諾しない、あるいは承諾を留保することができる。

第７条　サービス申込者への通知

サービス提供者は、サービス申込者をサービス利用者として承諾した場合は、本サービスの利用に必要なユーザーＩＤ及びパスワード（以下、ユーザーＩＤ等という）を発行し、サービス申込者に電子メールで通知する。

第８条　ユーザーID 等の追加・削除

サービス利用者は、サービス提供者が定める方法によってユーザーＩＤを追加又は減少させることができる。この場合における申込手続等については、第５条及び第６条を準用する。

第３章　本サービスの内容

第９条　本サービスの範囲

1　サービス提供者は、サービス提供者指定の条件下で、サービス利用者が管理するパソコン等の端末機器から電気通信回線を経由してサービス提供者の指定サーバーに接続することにより、本サービスを利用することのできる環境を提供する。
2　サービス提供者は、本サービスを構成するソフトウェアにバグ等の瑕疵がないこと、本サービスがサービス利用者の特定の利用目的に合致すること、本サービスの性能や品質がサービス利用者の期待や要求に応える水準にあることなどを保証するものではない。
3　サービス提供者は、提供情報が正確であること、最新であること、有用であること、その他提供情報に関する一切の事項について、いかなる保証もしないものとする。
4　本サービスに重要な瑕疵が認められた場合におけるサービス提供者の責任は、本業務の目的に照らして合理的に必要な範囲において、本サービスの修正ないし瑕疵の除去の努力をすることに限られるものとする。

第１０条　本サービスの提供期間及び利用時間

1　本サービスの提供期間は、サービス提供者が本サービスの提供を開始した日から、令和３年３月３１日までとする。
2　サービス提供者による本サービスの提供時間は、原則として２４時間３６５日とする。但し、サービス提供者は、本サービスの保守管理のために、サービス利用者に予告なく一時的にシステムを停止することができる。
3　サービス利用者による本サービスに関する問合せについては、原則として平日１０時から１７時までの間に対応する。

第１１条　本サービスの停止又は利用制限

1　サービス提供者は、定時に又は必要に応じて、保守管理作業のために、サービス利用者に事前の通知を行うことなく、本サービスを一時的に停止できるものとする。

2　サービス提供者は、サービス利用者が次の各号に掲げる場合のいずれかに該当すると判断した場合、サービス利用者による本サービスの利用を停止又は制限することができる。

①　第６条第１項に規定するサービス申込者の条件を欠いていることが判明した場合、また、同条第２項に掲げる事項に該当することが判明した場合。

②　第１５条各号に規定する利用目的以外の目的で提供情報を利用した場合。

③　第１６条に規定する提供情報に係る利用及び共有の条件に従わなかった場合。

④　第１８条に規定する禁止行為を行った場合。

⑤　その他、本利用規約の違反等により、本サービスの利用を継続させることが不適当とサービス提供者が判断した場合。

3　サービス提供者は、次の各号に掲げる場合、本サービスを停止又は利用を制限することができる。

①　災害その他の非常の事態が発生し、若しくは発生する恐れがあるとき。

②　サイバーテロ、情報システムの故障等、本サービスの保守管理上やむをえないとき。

③　その他本サービスの適切な運営及び保守管理をすることが困難なとき。

4　サービス提供者は、本条に基づいてなされた本サービスの停止又は利用制限によってサービス利用者又は第三者に損害が生じた場合であっても、当該損害に対する賠償責任その他の責任を負わないものとする。

5　サービス提供者は、第２項により本サービスを停止又は利用を制限することが合理的に予測できる場合は、電子メールを通じてサービス利用者に通知するよう努めるものとする。但し、緊急のためやむを得ない場合はこの限りではない。

第１２条　本サービスの中止

1　サービス提供者は、サービス提供者の都合により、本サービスの全部又は一部の提供を中止することができる。但し、サービス提供者は、本サービスの中止を決定した場合は、緊急のためやむを得ない場合を除き、速やかにサービス利用者に通知するものとする。

2　前項の場合において、サービス利用者又は第三者に損害が生じた場合であっても、サービス提供者は当該損害に対する賠償責任その他の責任を負わないものとする。

第４章　サービス利用者の責務等

第１３条　本サービスの利用方法

1　サービス利用者による本サービスの利用は、サービス利用者が管理するパソコン等の端末機器からサービス提供者指定のＵＲＬへ接続することにより行われるものとする。

2　サービス利用者は、本サービスを構成するソフトフェア自体のダウンロードやコピー等の方法により本サービスを構成するソフトウェアを入手する、あるいは入手しようと試みてはならない。

3　サービス利用者は、如何なる場合であっても、他のサービス利用者のユーザーからのコメントに対し、応答する義務を負うものではない。

第１４条　ユーザーの管理

1　サービス利用者は、自己の情報システム又はサイバーセキュリティに関する業務に関与する従業者のみをユーザーとして承認の上、本サービスを利用させることができ、その他の第三者に対して本サービスを利用させることはできない。

2　サービス利用者は、ユーザーによる本サービスの利用について責任を持ち、本利用規約に定める条件をユーザーに周知するとともに、これに従わせるものとする。

第１５条　提供情報の利用目的の遵守

サービス利用者は、本サービスを利用して取得した他のサービス利用者の提供情報を、次の各号に掲げる利用目的にのみ利用し、これらの目的以外の目的（有償・無償の別を問わず、商業目的を含む）には利用してはならない。

①　サービス利用者自身のサイバーセキュリティに関する知見の向上。

②　サービス利用者自身のサイバーセキュリティ対策の強化。

③　社会全体のサイバーセキュリティ対策の強化。

④　前各号に資する、サービス利用者どうしの意見交換又は連携強化。

第１６条　提供情報の利用及び管理

1　サービス利用者は、本サービスをとおして取得した提供情報を他のサービス利用者を除く第三者に開示してはならない。但し、法令により開示が求められる場合及び当該提供情報を開示したサービス利用者の許諾がある場合を除く。

2　サービス利用者は、提供情報に対してその利用及び共有について条件が付されている場合は、当該条件に従わなければならない。

3　サービス利用者は、提供情報の漏えい等の防止のため、サービス利用者側システムに対し、必要な安全管理措置を講じなければならない。

4　サービス利用者は、本サービスをとおして提供又は取得した必要な情報については、自己の責任において保全するものとし、かかる情報が本サービス上の障害、誤操作、設備の故障等により滅失した場合でも、情報の復元等をサービス提供者に求めることはできない。

第１７条　ユーザーＩＤ等の管理

1　サービス利用者は、ユーザーＩＤ等の使用及び管理について一切の責任を負うものとする。

2　サービス利用者は、申込の内容に変更が生じた場合又は本サービスの利用の中止を希望する場合は、直ちにその旨をサービス提供者に通知するものとする。

3　サービス利用者は、ユーザーＩＤ等をサービス利用者以外に利用させ、又は漏洩してはならず、自己のユーザーＩＤ等の不正利用に係る責任を負担する。

4　ユーザーＩＤ等の認証を行った後に行われた本サービスの利用行為については、すべてサービス利用者による行為とみなすものとし、サービス利用者はかかる取扱いに対して異議を述べないものとする。

第１８条　禁止行為

サービス利用者は、本サービスを利用するにあたり、以下の行為を行わないものとする。

①　法令に違反する行為又はそのおそれがある行為。

②　公序良俗に反する行為。

③　サービス提供者による本サービスの提供又は他のサービス利用者による本サービスの利用を妨害する行為又はそのおそれがある行為。

④　他のサービス利用者のユーザーＩＤ等を使用する行為又はその入手を試みる行為。

⑤　他のサービス利用者又はユーザーを特定するために探索する行為。

⑥　他のサービス利用者から取得した提供情報を第 15 条に定める利用目的以外の目的のために第三者に口外する行為。

⑦　虚偽の内容を含む投稿、あるいは、他のサービス利用者に対して故意に誤解を与える内容の投稿を行う行為。

⑧　他者の誹謗中傷等、他のサービス利用者に不利益又は不快感を与えるおそれのある内容の投稿を行う行為。

⑨　本サービスの目的と明らかに無関係な内容の投稿を行う行為。

⑩　前各号のいずれかに該当する行為を援助又は助長する行為。

⑪　その他、サービス提供者が不適当と判断する行為。

第１９条　サービス利用者の責任

1　サービス利用者は、本サービスの利用及び本サービス内におけるすべての行為（情報の登録、投稿、閲覧、削除、送信等）及びその結果について、一切の責任を負う。

2　サービス利用者は、自己の本サービスの利用により、サービス提供者若しくは他のサービス利用者又は第三者に損害を与えた場合、また、他のサービス利用者若しくは第三者からクレーム等の請求がなされた場合、自己の責任と費用をもって処理、解決しなければならない。

第２０条　利用料金

1　本サービスの利用は無料とする。

2　サービス利用者側システムは、サービス利用者の責任と負担

で、これを整備及び維持する。

第５章　その他の事項

第２１条　通知及び連絡

サービス提供者は、サービス利用者が本サービスを利用するにあたり必要な事項については、本サービスに関するＷｅｂサイトへの掲載、サービス利用者が利用申込時に指定したメールアドレスへの電子メールの送付その他の方法により通知、連絡等する。

第２２条　投稿データの削除

1　サービス提供者は、本サービスの目的ないし本利用規約の規定に反していると認められる投稿等について、サービス利用者の同意を得ることなく、そのデータを削除することができる。

2　サービス提供者は、サービス利用者の投稿データを削除し、または保存しなかったことについて一切責任を追わず、またその理由を説明する義務も負わない。

第２３条　免責

サービス提供者は、本サービスを利用したことに起因してサービス利用者に損害が発生した場合（以下の各号に定める損害を含むが、これらに限らない）であっても、当該損害に対していかなる責任も負わないものとする。但し、当該損害の発生がサービス提供者の故意又は重過失による場合を除く。

①　本サービスを利用できなかったことにより生じた損害。
②　提供情報が正確、最新、あるいは有用でなかったことなど、提供情報の内容に由来する理由により生じた損害。
③　サービス利用者間でのトラブルに起因して生じた損害。

第２４条　個人情報の取扱い

1　サービス提供者は、本サービスの提供にあたりサービス利用者（サービス申込者を含む。）から提供を受けた個人情報について、「個人情報の保護に関する法律」（平成１５年法律第５７号）に従い、適切に取得、利用、提供、管理等を行うものとする。

2　サービス提供者は、別添「個人情報の取扱いに関する基本方針」に従い、個人情報を取り扱うものとする。

第２５条　サービス提供者による情報の管理・利用

1　サービス提供者は、本サービスをとおして知得した情報（提供情報及びサービス利用者による本サービスの利用状況等に係る情報を含む。以下、本件情報という）について、善良な管理者による注意をもって機密保持とその管理に努めるものとする。

2　サービス提供者は、以下に掲げる事項のために必要な範囲において、本件情報を利用契約の終了後も利用できるものとする。但し、かかる利用を行う場合、サービス提供者は、サービス利用者及びユーザーの匿名性の維持に配慮する（必要に応じて加工する）ものとする。

①　本サービスの改良及び維持管理。
②　本業務の一環として行う厚生労働省への本サービスの運用状況及び利用状況等に係る報告。
③　本事業に関連してサービス提供者が行う提言・統計・調査等及び公的機関等の諮問に応じるなどの社会貢献活動。
④　その他、本サービスの目的に資する事項。

3　サービス提供者は、以下に掲げる場合、本件情報を開示できるものとする。

①　裁判所、その他の法的な権限のある官公庁の命令等により本件情報の開示ないし提出を求められた場合。
②　デロイト トウシュ トーマツ リミテッド(英国の法令に基づく保証有限責任会社。以下、ＤＴＴＬという）及びＤＴＴＬに加盟するサービス提供者以外のネットワーク・ファーム（ＤＴＴＬ及び当該ネットワーク・ファームを以下総称して、ＤＴＴＬ等という)に対し、独立性・利益相反の確認、品質管理レビュー等の品質管理目的並びに管理業務のために必要な範囲で開示する場合。なお、サービス提供者は、ＤＴＴＬ等による本件情報の守秘について、一切の責任を負う。

第２６条　委託

サービス提供者は、本サービスの提供に関する業務の全部又は一部をサービス利用者の承諾を得ることなく第三者（一般社団法人ＪＰＣＥＲＴコーディネーションセンターを含むが、これに限られない）に委託することができる。但し、その場合、サービス提供者は責任をもって委託先を管理する。

第２７条　知的財産権

本サービスを構成する有形・無形の構成物（ソフトウェアプログラム、データベース、アイコン、画像、文章、マニュアル等の関連ドキュメント等を含む）に関する著作権を含む一切の知的財産権、その他の権利は、サービス提供者又はサービス提供者に許諾した第三者に帰属する。

第２８条　反社会的勢力の排除

1　サービス提供者及びサービス利用者は、相手方に対し、自らが、暴力団、暴力団員、暴力団員でなくなった時から５年を経過しない者、暴力団準構成員、暴力団関係企業、総会屋等、社会運動等標ぼうゴロ又は特殊知能暴力集団等、その他これらに準ずる者（以下総称して「暴力団員等」という）に該当しないこと、及び次の各号のいずれにも該当しないことを表明し、かつ利用契約が有効である期間にわたって該当しないことを確約する。

①　暴力団員等が経営を支配していると認められる関係を有すること。
②　暴力団員等が経営に実質的に関与していると認められる関係を有すること。
③　自己若しくは第三者の不正の利益を図る目的又は第三者に損害を加える目的をもってするなど、不当に暴力団員等を利用していると認められる関係を有すること。
④　暴力団員等に対して資金等を提供し、又は便宜を供与するなどの関与をしていると認められる関係を有すること。
⑤　役員又は経営に実質的に関与している者が暴力団員等と社会的に非難されるべき関係を有すること。

2　サービス提供者及びサービス利用者は、自ら又は第三者を利用して次のいずれかに該当する行為も行わないことを確約する。

①　暴力的な要求行為。
②　法的な責任を超えた不当な要求行為。
③　取引に関して、脅迫的な言動をし、又は暴力を用いる行為。
④　風説を流布し、偽計を用い又は威力を用いて相手方の信用を毀損し、又は相手方の業務を妨害する行為。
⑤　その他前各号に準ずる行為。

3　サービス提供者又はサービス利用者は、相手方が、前二項の表明又は確約に違反した場合、何らの催告をすることなく、利用契約を直ちに解除することができる。この場合、当該解除をした者は、相手方に対して損害を賠償することは要さない。また、当該解除をされた者は、かかる解除により相手方に損害を生じさせたときは、相手方に対して全ての損害を賠償する。

4　サービス提供者及びサービス利用者は、利用契約に基づく取引に関し、暴力団員等から不当な介入を受けたときは、直ちにその旨を相手方に報告する。

第２９条　権利義務譲渡の禁止

サービス利用者は、利用契約の契約上の地位を第三者に承継させ、又は利用契約に基づく権利義務の全部又は一部を第三者に譲渡し、承継させ、又は担保に供してはならないものとする。

第３０条　協議

本利用規約の解釈について両当事者間に異議、疑義等が生じた場合、又は本利用規約に定めのない事項が生じた場合、誠実に協議し、円満にその解決を図るものとする。

第３１条　準拠法

利用契約の成立、効力発生及び解釈にあたっては、日本法を準拠法とする。

第３２条　合意管轄裁判所

利用契約に関してサービス提供者とサービス利用者との間で生じた紛争については、東京地方裁判所を第一審の専属

的合意管轄裁判所とする。

別添 個人情報の取扱いに関する基本方針

サービス提供者は、本サービスの提供に際してサービス利用者（ユーザーを含む。以下同じ）から提供を受けた個人情報について、以下の基本方針に基づき、これを取扱うものとする。

１　サービス提供者が取得する個人情報等

サービス提供者は、サービス利用者の個人に関する情報であって、直接的に若しくは間接的に個人を特定できる情報（以下、個人情報等という）として、以下の情報を取得する。

① サービス利用者の氏名、所属する医療機関の名称及び部門名称、メールアドレスその他連絡先に関する情報。
② サービス利用者が利用する端末機器のＩＰアドレス、オペレーティングシステム及びブラウザに関する情報。

２　個人情報等の利用目的

サービス提供者は、個人情報等を以下の目的のために利用する。

① 本サービスの提供のため。
② 本サービスに係る情報セキュリティの確保、システムメンテナンス等の連絡及びサービス利用者による問合せの対応のため。

３　個人情報等の取扱いの委託について

サービス提供者は、本サービスの提供のために必要な範囲において、個人情報等の取扱いに関する業務の一部を一般社団法人ＪＰＣＥＲＴコーディネーションセンターその他の第三者に委託することがある。この場合、サービス提供者は、委託した個人情報等の安全管理が図られるよう、委託先の必要かつ適切な監督を行うものとする。

４　個人情報等の共同利用について

サービス提供者は、厚生労働省からの委託を受けて本サービスを提供しており、以下の範囲において個人情報等を共同利用することがある。

① 共同利用することのある項目　：「１　サービス提供者が取得する個人情報等」に同じ
② 共同利用する者　：厚生労働省
③ 共同利用の目的　：「２　個人情報等の利用目的」に同じ
④ 共同利用管理責任者　：有限責任監査法人トーマツ

５　個人情報等の取扱い

サービス提供者は、個人情報等を以下の Web サイトに提示したとおりに取り扱う。

Web サイトのアドレス

https://www2.deloitte.com/jp/ja/footerlinks1/privacy.html

６　個人情報の取扱いに関する問合せ先

本サービスに係る個人情報の取扱いに関する問合せ先は、以下のとおりとする。

問合せ先

厚生労働省令和２年度事業「医療分野におけるサイバーセキュリティ対策調査」事務局
受託者　有限責任監査法人トーマツ
所在地：東京都千代田区丸の内 3-2-3　丸の内二重橋ビルディング
電話番号：03-6213-1000
メールアドレス：hccyber2021@tohmatsu.co.jp
担当部署：リスクアドバイザリー事業本部ヘルスケア

以上