# 医療機関におけるサイバーセキュリティ確保事業について

**令和５年度第一次補正予算額　36億円**

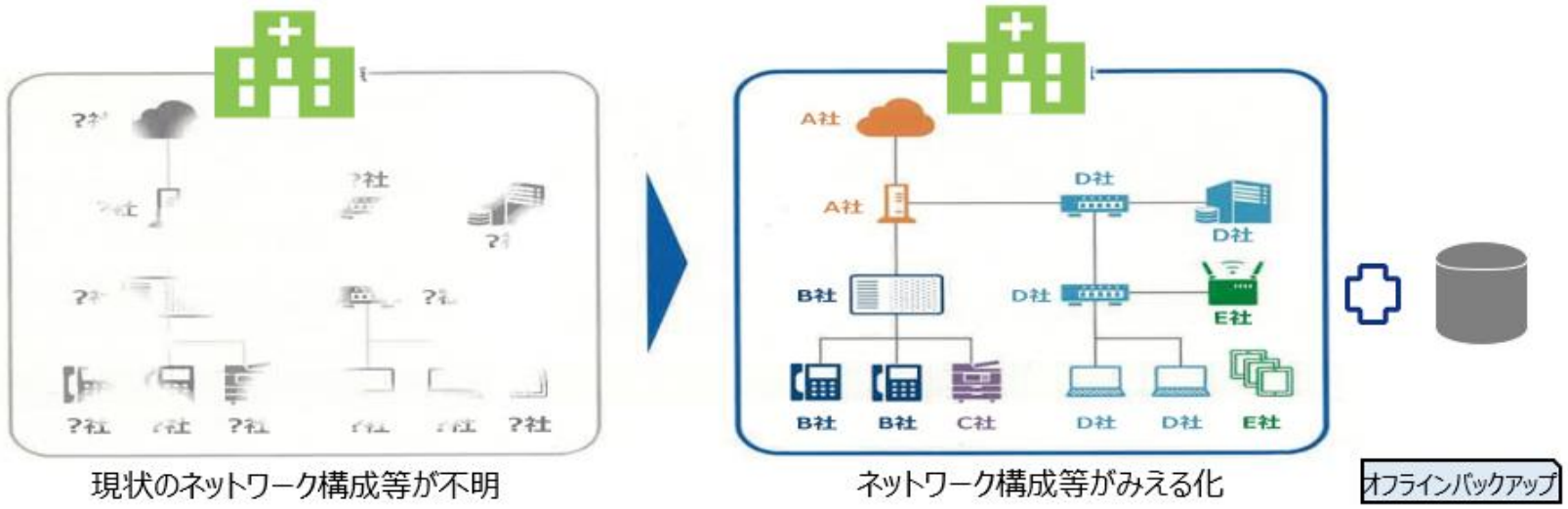
## ①　施策の目的

- 医療機関の医療情報システムがランサムウェアに感染すると、診療の一部を長時間休止せざるを得なくなることから、医療機関等におけるサイバーセキュリティ対策の充実は喫緊の課題となっている。
- そのため、医療機関におけるサイバーセキュリティの更なる確保を行う。

## ②　施策の概要

- 厚生労働省では、全ての外部ネットワーク接続点を確認することを求めているが、中・大規模病院は多数の部門システムで構成されているため、各システムを提供する事業者と個別に連携しても、全てのネットワーク接続を俯瞰的に把握することは困難である可能性がある。
- また、ランサムウェア対策にはオフライン・バックアップが有効であることを踏まえ、厚生労働省ではオフライン・バックアップ整備を求めている。
- 医療機関におけるサイバーセキュリティの更なる確保のため、外部ネットワークとの接続の安全性の検証・検査や、オフライン・バックアップ体制の整備を支援する。

## ④　施策のスキーム図

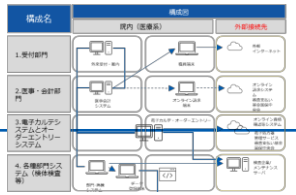


# ①　外部ネットワークとの接続の安全性の検証・検査（作業イメージＰ）

**①各種資料ご提出**

- 自組織の医療情報システム一覧・ネットワーク構成図等のご提出
- 事前質問票へのご回答

事前質問票



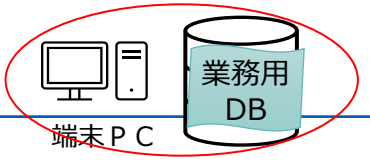
ネットワーク構成図

**②ヒアリング**

- 医療機関情報システム担当者等へのヒアリング（病院内の外部接続点を洗い出す（特に病院内の部門が独自に外部サービスを導入しているケースもあることから、その把握を重点的に行うこと）

**③現地調査**

- 調査員による医療情報機器及びネットワーク機器等の調査設置場所及び機器情報（設定情報を含む）に関する確認


**④調査結果報告書ご確認**

- 調査結果報告書のご確認


調査結果報告書

◆（想定）作業時間　※ 1日8時間　調査員は２または３人（１病院あたり）

・小規模病院（20~199床）②ヒアリング・③現地調査あわせて　1.6 ～2.5 日

・中規模病院（200~399床）②ヒアリング・③現地調査あわせて　3.3 ～ 5 日

・大規模病院（400床以上）②ヒアリング・③現地調査あわせて　6.6 ～ 10 日

# ② オフライン・バックアップ体制の整備（作業イメージＰ）

**①打ち合わせ**

作業時間（想定）

５～８時間

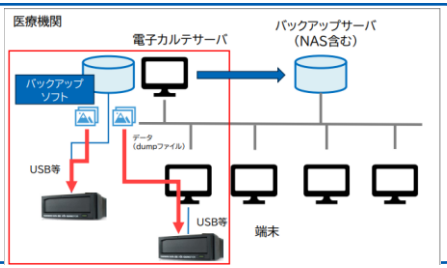
- 医療機関情報システム担当者等と作業内容の確認

**②現地作業**

作業時間（想定）

５～８時間

- 医療機関でのオフラインバックアップの実施
  ※バックアップ媒体（クラウドサービスを含む）
  ソフトウェア等は事前に医療機関で準備




**③実施報告書**

ご確認

- 実施報告書のご確認


実施結果報告書

※ 保守管理、データ復旧作業は作業対象外

# 医療機関におけるサイバーセキュリティ確保事業の概要について

第19回健康・医療・介護情報利活用検討会
医療等情報利活用ＷＧ　資料2-2
一部改変

予防

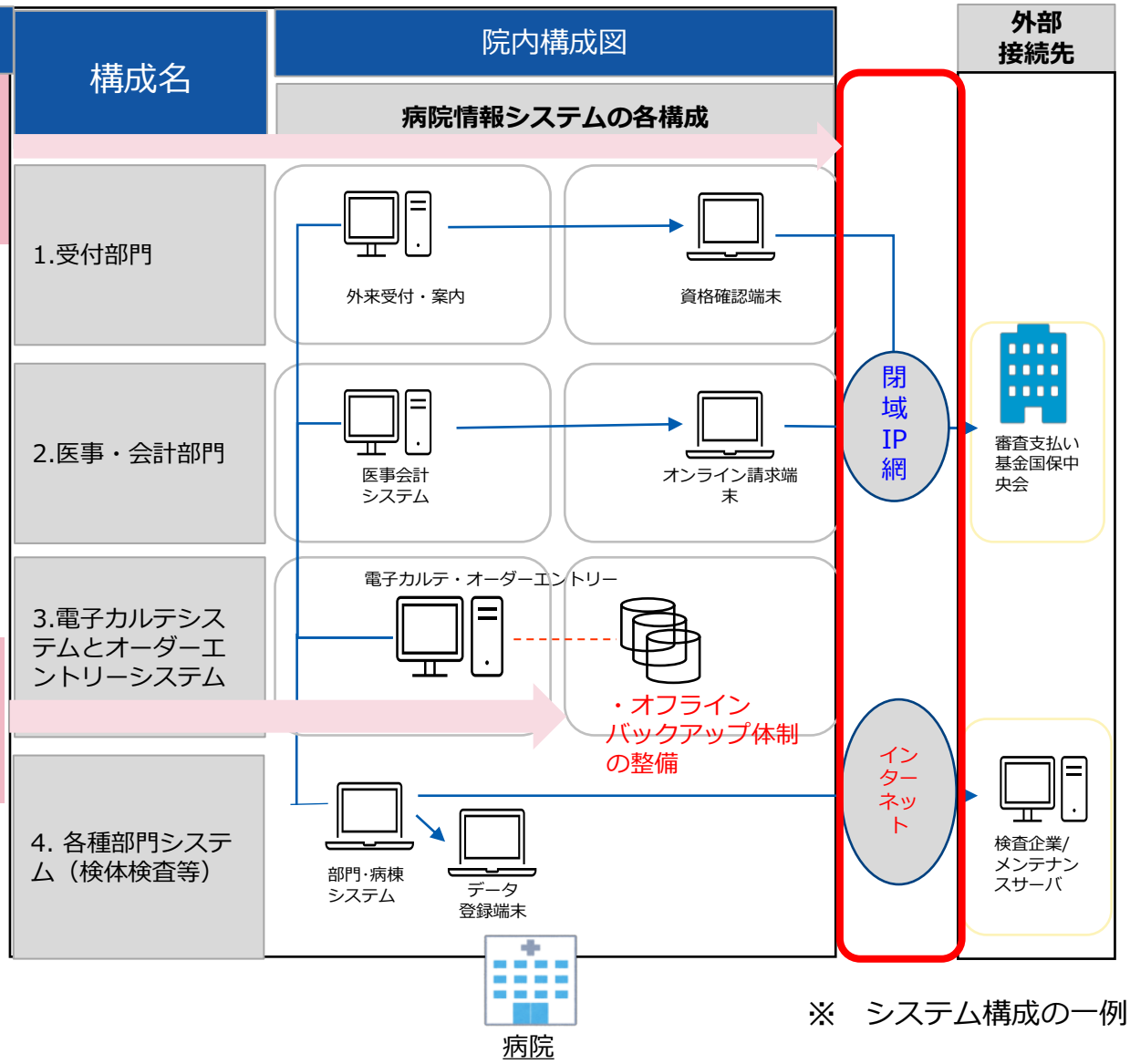
初動

復旧

**事業概要と主な利点**

**①外部NWとの接続の安全性の検証・検査（外部接続点等を把握することで、効果的な機器の設置等が可能になる）**

**②オフラインバックアップ体制の整備（ランサムウェア等による被害を最小限に抑えることができる）**




※　システム構成の一例

# 事業概要の詳細①　※入札仕様書（案）の抜粋

## ①病院の外部ネットワーク接続の俯瞰的把握、安全性の検証・調査

　病院の医療情報システムに接続する外部ネットワーク接続点を俯瞰的に把握した上、そのネットワークに係るセキュリティ対策状況を調査する。

　その方法については、最低限以下の項目をあげるが、受託事業者は自身の専門的見地から有効と考えられる方法については、以下の項目以外についても積極的に提案すること。最終的な実施方法と調査対象については、当室と相談の上決定すること。また調査対象の業務に支障を来すことのない範囲の調査とすること。

ア　事前に病院に提出してもらう医療情報システムに関する資料（ネットワーク構成図・システム構図）や実施してもらう作業（病院の各部門への周知文書の作成等）に関する調査

イ　アの調査結果をもとに病院が保有する医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図）等情報の収集した上で、医療情報システム担当者やシステムベンダーのヒアリングを行い、病院内の外部接続点を洗い出す。特に病院内の部門が独自に外部サービスを導入しているケースもあることから、その把握を重点的に行うこと。

ウ　病院外との接続部分及び病院内の外部接続端末について、ネットワーク　上からの不正アクセスへの対策状況等セキュリティ対策状況調査を行う。

エ　イ及びウの結果をとりまとめ、ネットワーク接続点の管理方法や脆弱性　対策の提案等を含めた調査報告書を作成し、調査対象医療機関に報告する。当室へは、業務報告書等内にて報告すること。

# 事業概要の詳細②　※入札仕様書（案）の抜粋

## ②病院のオフラインバックアップ体制の整備支援

　病院の医療情報システムを対象としたオフラインバックアップ実施に係る支援を行う。その方法については、最低限以下の項目をあげるが、受託事業者は自身の専門的見地から有効と考えられる方法については、以下の項目以外についても積極的に提案すること。

　最終的な実施方法と支援対象については、当室と相談の上決定すること。オフラインバックアップ実施に向け、支援対象が準備すべき物品、病院負担部分を明確にして提案すること。

　また、オフラインバックアップ計画については、本事業終了以降も病院が継続して有効なオフラインバックアップ体制維持が可能な内容とすること。

1　オフラインバックアップ計画書の策定

2　オフラインバックアップの実施

3　１、２の結果をとりまとめ、実施報告書を策定し、支援対象医療機関に報告すること。当室へは、業務報告書等内にて報告すること。

※バックアップ媒体（クラウドサービスを含む）・ソフトウェアの購入、保守管理、データ復旧作業については、本事業支援の対象外とする。