資料 2－2

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

第19回　健康・医療・介護情報利活用検討会

医療等情報利活用ワーキンググループ

2023（令和５）年11月６日

サイバーセキュリティお助け隊サービスとの連携について

医政局 特定医薬品開発支援・医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

医療機関におけるサイバーセキュリティ対策に関する調査研究結果１

本調査研究*において得られた知見は以下の通り

*厚生労働科学研究費補助金「医療分野の情報化の推進に伴う医療機関等におけるサイバーセキュリティ対策のあり方に関する調査研究（令和3-4年度, 研究代表者：近藤博史）」

主な調査	調査内容	主な結果・課題
医療機関のサイバーセキュリティ確保に関する現地調査	医療機関におけるネットワーク構成図等の情報資産やバックアップ整備状況に関する現地調査 ※実施期間：令和４年１月～３月 ※調査対象：11医療機関 ※各医療機関の病床規模 ~199床：3、200～399床：2、400床～：６	・ 情報資産台帳等で把握されていない情報機器及び外部接続部が存在。 ・ ①外部接続部が数カ所に集約化されているケースと、 ②検査機器毎の保守回線等、外部接続部が多数あるケースがあり、 医療機関ごとの状況は様々である。 （一医療機関当たり外部接続部：７～47カ所）
医療機関のサイバーセキュリティに関する意識調査	サイバーセキュリティ対策の実施状況や施設内の運用規程の有無、インシデント発生時の対応方法等に関するアンケート調査 ※実施期間：令和４年9月～11月 ※調査対象：日本病院会会員2489会員 （回答数581会員、回答率23%）	・ 多くの院内ネットワークが異なったベンダーにより形成されており全体図を俯瞰的に把握できていない。 ・ バックアップ接続時の設定が適切になされていない。 ・ネットワークセキュリティのための必要最低限の設定がなされていない。 ・ インシデント発生時に対応できる人材の不足。

医療機関におけるサイバーセキュリティ対策に関する調査研究結果２

本調査研究を踏まえて必要な対応策を以下に示す

医療機関への調査の結果、自施設だけでなく、サプライチェーンリスクを念頭に置いたサイバーセキュリティ対策として、ネットワークの俯瞰的把握やインシデント発生に備えたバックアップ作成支援等の下記の５点が挙げられた。

- NDR等ネットワーク監視機器を効果的に配置するための、外部接続等を含むネットワーク構成の俯瞰的把握の支援
- ネットワークへの機器追加時の適切な接続に関する支援
- ネットワークへの機器追加後のフォローアップ支援
- バックアップ作成時の初期設定等の支援
- インシデント発生時の対応に関するコンサルテーション（初動対応支援）

上記のうち、サイバーセキュリティお助け隊のサービスとの連携候補として、以下のサービスが挙げられる。

１．バックアップ作成時の初期設定等の支援
２．インシデント発生時のコンサルテーション（初動対応支援）
３．外部接続等を含むネットワーク構成の俯瞰的把握の支援等

調査研究結果を踏まえて１
バックアップ作成時の初期設定等の支援内容

ＩＰＡ（独立行政法人　情報処理推進機構）がサイバーセキュリティお助け隊サービス（以下「お助け隊サービス」という。）提供事業者にサービス内容に関するアンケートを実施

アンケート方法等

・　お助け隊サービスへの追加候補である、
　１．バックアップ作成時の初期設定等の支援
　２．インシデント発生時のコンサルテーション（初動対応支援）
　３．外部接続等を含むネットワーク構成の俯瞰的把握の支援
　に関し、アンケート調査を実施。
・　実施時期・実施主体：令和５年９月、ＩＰＡ
・　調査対象：お助け隊サービス事業者35社（回答事業者 30社,回答率 86%）

アンケート結果（１．バックアップ作成時の初期設定等の支援）

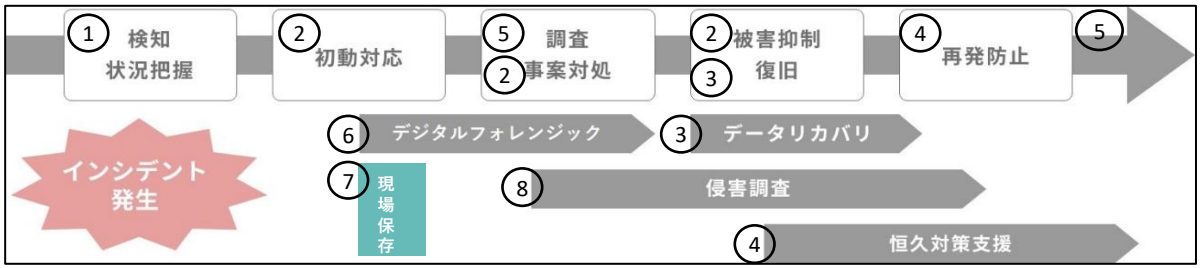
	お助け隊サービスとしての提供事業者数 ※（　）はオプションとして提供している事業者数	お助け隊サービスでない自社サービスとしての提供事業者数
バックアップ作成の初期設定を支援するサービス	3(1)	18
現状のバックアップ構成の評価（リスク調査等）サービス	4(3)	15
バックアップをオンプレミスのサーバ等へ作成・保存するサービス	4(3)	17
バックアップをクラウドへ作成・保存（アップロード）するサービス	4(4)	18

調査研究結果を踏まえて２
インシデント発生時の初動対応支援の範囲について

アンケート結果（２．インシデント発生時のコンサルテーション（初動対応支援）

		お助け隊サービスとしての提供事業者数 ※（　）はオプションとして提供している事業者数
①	インシデント発生時（疑い含む）の相談	29(0)
②	インシデント発生時の初動対応　※オンライン含む （事案対処、被害拡大防止、保全に関する一次アドバイスなど）	30(1)
③	データ復旧の支援	18(11)
④	再発防止・恒久対策支援	19(11)
⑤	インシデント調査と報告 （インシデントの原因調査および調査結果報告書の提出）	23(13)
⑥	デジタルフォレンジック調査	16(14)
⑦	事故状態の保全（現場保存）の支援	16(9)
⑧	情報漏洩・侵害被害の調査	16(12)

※インシデント発生の各フェーズにおける対応（支援）項目のイメージ



調査研究結果を踏まえて３

ネットワーク構成の俯瞰的把握の支援に関するサービスの提供状況について

アンケート結果（３．外部接続等を含むネットワーク構成の俯瞰的把握の支援）

	お助け隊サービスとしての提供事業者数 ※（　）はオプションとして提供している事業者数	お助け隊サービスでない自社サービスとしての提供事業者数
現状のネットワーク構成の評価（リスク調査等）サービス	5(4)	17
ネットワーク構成の可視化サービス （現地ヒアリング・ドキュメント作成・自動可視化ツールの導入等）	5(3)	16
ネットワーク構成の可視化サービス＋特定の情報資産に対する管理サービス	4(3)	16
ネットワーク構成の可視化＋監視サービス	4(2)	16

今後の方針

○　医療機関のニーズを踏まえたお助け隊サービスとの連携について、関連省庁等と連携しサービス事業者に働きかけていく。

○　対象となる医療機関にお助け隊サービスの認知を広めるため、関係団体等と連携し、進めていく。

調査研究結果を踏まえて 4
医療機関でのお助け隊サービスのユースケース（中小規模医療機関・ネットワーク監視型利用）

本サービスとの連携を検討するサービス

予防

NWの俯瞰的な把握

外部接続点等を把握することで、効果的な機器の設置が可能になる

初動

オフラインバックアップ作成支援

復旧

サイバーセキュリティお助け隊

相談窓口機能

監視装置の設置

対応機能

初動対応

ランサムウェア等による被害を最小限に

復旧支援（データ復旧等）

簡易サイバー保険

本サービス※
※ NW監視機器1台の場合
・初期費用50万まで
月額費用1万まで

※　システム構成の一例