厚生労働行政推進調査事業（地域医療基盤開発推進研究事業）
研究報告書

病院サイバーセキュリティ調査の管理方式

研究分担者　長谷川高志
特定非営利活動法人日本遠隔医療協会

研究要旨
各施設サイバーセキュリティ調査では、調査項目・調査水準・秘密保持や質管理などのために、文書や手順の共通化、監督企業の設置など、管理方式を構築した。　構築に時間を要したが、構築後は調査が効率的かつ均質に進み、短期間に調査作業が進んだ。

A．研究目的

病院のサイバーセキュリティ調査は、調査内容と別に対象先病院の募集と選定、調査実施に至るまでの調整業務があった。また調査担当各社の実施項目の準備、実施時の監督や調査の質のすりあわせ等、様々な運営の努力を集結して、管理方式を構築した。

管理方式には以下の質保証や手順の効率化の利点がある。

1，同時に複数の病院･企業で共通の手順で作業を進め、業務の質を安定できる。
2，各施設･各社同じ手順を進めるので、組織内部の説明や意思決定が円滑になる。
3，秘密保持等の誓約が均質に管理できる。
4，調査の質を安定できる。

B．研究方法

1．手順、秘密保持契約、工数管理などのドキュメントを共通化した。
2．担当組織を一本化した。

C．研究結果

1．共通ドキュメント
① 病院向け調査手順
② 日本遠隔医療協会から病院への依頼状
③ 病院・協会間秘密保持誓約書
④ 調査担当企業向け調査手順
⑤ 調査担当企業・協会間秘密保持契約
⑥ 調査工数確認票
【資料1～6】

2．手順
① 企業募集
② 企業・研究班会議
③ 企業向け書式（資料①～⑥）提供
④ 病院募集
⑤ 応募病院への依頼（意向確認）
⑥ 誓約等手続
⑦ （各社調査）
⑧ 各社に途中の工数確認およびドキュメントチェック

3．監督企業の設置

セコム山陰株式会社を監督企業とした。監督企業と調査各社はシステム開発の工程管理システムで工程、ドキュメントの提出等を管理した。また調査内容の確認を随時行った。

3．考察

（1）業務の質と効率

手順構築の時間を要したが、調査開始以降は効率的に作業が進んだ。そのため調査が2023年1月～3月に集中したが、調査は短期間で終了し、複数調査が同時並行して進行した。

（2）調査内容のレベル統一

サイバーセキュリティは、皆の意識がバラバラだが、調査手順書の作成･配布および監督企業の業務により、調査レベルの平準化が進んだ。

（3）総論として

ネットワーク接続図などの重要情報を調査対象とした。各社で秘匿レベルの意識差があり、当初、曖昧な情報に留めたケースと詳細なケースが混在した。しかし曖昧な情報では、問題点を絞れないので、監督企業として詳細調査を指導できた。

サイバーセキュリティは、まだしばらく、意識差が大きいと考えられるが、質をコン

トロールした調査が可能であることを実証
した。

D．健康危険情報
なし

厚生労働行政推進調査事業

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

【資料１　病院向け説明書】

病院に対するサイバーセキュリティに関する調査・報告書作成業務

各病院調査等手順

特定非営利活動法人日本遠隔医療協会

第 1.1 版　2022 年 11 月 21 日

【調査の基本構想】

日本国内の複数の医療機関で、サイバー犯罪者による破壊行為の被害（ランサムウェアの攻撃）が多発している。被害（アクシデント）に至らずとも、インシデントも多数発生していると考えられる。その対策が急務であるが、サイバー犯罪自体が急速に進化していること、元々の日本の医療機関の情報化の弱さや要員不足から、この事態への対応が進んでいない。そこで厚生労働省の調査研究（厚生労働行政推進調査事業）により、医療機関のサイバーセキュリティに関する調査を進めている。

本研究班は、日本の医療分野のサイバーセキュリティの専門家を結集して（参考資料　研究班体制）、複数の病院に訪問調査を実施している。

セキュリティインシデント発生時の対応として CSIRT の組織化が医療機関に求められているが、CSIRT の対応ができる人材は日本では限られている現状がある。CSIRT の対応には米国の NIST の SP－800 が参考にされており、日本では IPA, JPSIRT での議論資料があり、これらをフォローしている必要がある。しかし、日本の電子カルテベンダー等医療情報システム関連の大企業の医療部隊で、これらをフォローされていたとは言えない状況である。一方、攻撃は組織化しており迅速な対応が要求されているにも関わらず、これを医療機関側に求めることはかなり厳しい状況と言える。全国的に委託業者の育成が必要と判断する。

具体的には CSIRT の対応は 3 つのステップからなる。

① 事前にネットワーク全体像、外部接続全体像、内部の通信全体像の把握が各医療機関に求められる。

② この資料に応じて脆弱性が明確になった場合に迅速に対応することが必要である。

③ 何らかの異常を察知した場合に対応する。

このうち、**①事前調査**について、日本の医療機関ではシステムの構築に多数のベンダーがネットワークとサーバ、端末を導入し接続しており、全体像が掴み難い現状がある。これは電子カルテベンダーが全体を入札していても部門については部門システムに任せていることが多く、全体像は十分把握されているとは言えない。ネットワークとサーバ等のハードウェアを一括管理し、その上に幾つかのソフトウェアを載せる方法が管理上理想であり、その方向を進める必要はあるが、現状では全体把握は難しい状況である。2022 年 3 月に行った先行調査（A 病院調査）でも調査結果に現れたが、コロナ禍で現地保守がいつの間にか、オンライン保守になり、外部接続がされている状況もあり、病院は病院資産でない機器（ベンダー資産の保守用機器）の管理状況を把握する必要がある。CT など検査機器は院内の管理も情報担当ではなく、遠隔読影、地域連携なども存在する。中小病院ではこれらの把握に人材もおらず、専門業者に委託する必要がある。**②脆弱性への対応**のステップは既にネットワーク管理事業者等では各施設の機器のリストを保持し、脆弱性が発表されるとシステム上で対応すべき医療機関等を検索し、担当部署に連絡する体制を作っている事例がある。中小病院ではこれらの部分も委託が望ましいと言える。**③異常検知時の対応**のステップは、事前調査がされていると容易であり、これらの委託事業者の負荷も抑えられる。

人材豊富な大病院では**①事前調査**、**②脆弱性への対応**のステップは可能かもしれないが、情報管理の人材の少ない中小病院では難しい。

本調査は、**①事前調査**に関する、調査手法開発の試みである。2022 年 3 月に一施設で先行調査を行い、様々な事柄がわかった。しかしながら、本研究班とコミュニケーションがある施設や企業で行ったもので、その調査結果が多くの施設に共通的普遍的と言えるか、調査手法をそのまま多くの施設に適用できるか、不明である。そこで 2022 年度に全国各地の複数の施設でトライアルを行うこととした。

1．　本文書について

本文書は調査に協力いただく病院向けの説明および手続の解説であり、以下事項が記載されている。

① 調査協力施設の役割、負担
② 調査事項と手順
③ 手続および工程（スケジュール観）
④ 書式類

2．　調査協力施設の役割、負担

① 責務

- 調査担当会社よりの要請に基づく、調査協力施設の関係者（病院長、職員、システム担当者）へのヒヤリングの日程調整
- 調査担当会社よりの要請に基づく、調査協力施設内の設備の調査（同行、案内）
- 調査担当会社よりの要請に基づく、調査協力施設内の設備業者との情報提供に関する仲介
- 調査担当会社よりの質問への対応

② 調査目的

まだ日本国内の病院のサイバーセキュリティの状況に関する実態情報が無く、日本国内の多くの病院がどのような状況にあり、国家レベルの対策として何を打ち出すべきか、厚生労働省に伝え政策立案の情報収集が本調査研究の目的である。

調査結果の詳細情報を秘密保持すべき厚生労働省に報告する。また統計的処理等を経て、対象施設との関係を全くたどれない情報を学術的に公開（論文投稿、学会等の講演、図書出版）することがある。

調査により、施設内のサイバーセキュリティ上の不足や不備が見いだされるかもしれないが、その責任追及や処罰のための報告などは研究目的ではない。不備や不足な状況も、受け止めるべき現実として明らかにしてゆく。調査結果を整理した段階で指摘できる問題点や対策について、報告書に記す。

③ 調査に関する秘密保持

調査担当企業は厚生労働行政推進調査事業研究班の受託機関（事務局）の特定非営利活動法人日本遠隔医療協会との契約に基づき、担当する。各企業は、調査対象病院に対して日本遠隔医療協会が誓約する秘密情報保持の諸条項を遵守して調査する。

④ 調査に関する負担

調査に係わる対象施設職員への謝金（日本遠隔医療協会規定に基づく）、調査に於いて対象施設が支払う必要がある費用を、日本遠隔医療協会は対象施設に支払う。支払については、日本遠隔医療協会研究事務局が調整する。

3．　調査事項と手順

3.1　概要

今回の調査は**①事前調査**のステップとして、病院担当者あるいは調査各社が効率的に実施できる手

法の開発を狙っている。ただし開発途上の手法なので、不明点や過不足は、調査途上で適宜修正しながら進める。

3.2　チェックリストによるヒヤリング

① 医療情報システムの安全管理のガイドラインにあるチェックリスト（経営層向け、システム管理者向け、利用者向け）を訪問調査で聞き取り、作成する。

② チェックリストは下記 URL よりダウンロードできる。

「医療機関のサイバーセキュリティ対策チェックリスト」　Excel 版
（経営層向け、システム管理者向け、利用者向けがこの Book 内に含まれる）
https://www.mhlw.go.jp/content/10808000/000936169.xlsx
https://www.mhlw.go.jp/content/10808000/000936167.pdf　（PDF 版）

③ 病院長、システム管理者、利用者（1、2 名）の 3−4 人に、訪問調査前に予め上記チェックリストをダウンロードいただき、内容を確認いただき、第一回訪問に備えていただきたい。そこで結果を調査員と付き合わせる。

- 分からないことは、何が分からないか、記載して頂き、○×を記載して頂く。
- 理解が困難であった部分は記録し、今後の検討材料にする。ヒヤリングは一人 30 分ほどで終える。**（病院長、利用者で最大で 1.5 時間×2）**

④ システム管理者にも同様に対面での調査を行う。**2 時間以上、半日程度の調査にする。**資料が病院にあってすぐに出ない場合は、その場では宿題として、一週間の期間に提出を求める。提出されなかった場合、出されなかったとして記録する。（提出が必須ではなく、1 週間掛けても提出できないことも、実態の情報となる）資料が保守業者にある場合には業者の担当者、連絡先を聞き、病院の了解の下、直接ベンダーに聞く。ベンダーに聞く場合も、1 週間以内に情報が出されない場合には、出せなかったとして記録する。

- 分からないことの説明、帳票など具体的なものがあるのかなど、詳細を質問し完成させる。
- この調査は第一回訪問だけでは終わらない。二回目訪問などが必要である。

3.3　院内設備の巡回調査

① 外部接続、サーバ、ネットワーク機器等は調査会社、システム管理者、病院からの委託事業者が直接院内巡回して機種等を確認する。

- システム管理者と委託事業者担当者の技術的な詳細確認は 1 時間を 2 回ほど必要

② 必要な場合、調査施設の了解の下、ベンダーに問合せていただく。

③ 外部接続の状況調査（管理者の知らない接続なども洗い出す）の対象は以下の通り。

[1] 各システム
[2] ネットワーク保守
[3] ＣＴ、ＭＲＩ等ネットワーク接続検査等の機器の保守
[4] マイナカード関係接続
[5] 地域医療連携接続
[6] 遠隔読影サービス接続
[7] 研究ネットワーク接続
[8] 各種遠隔サービス接続など

3.4　追加ヒヤリング等

① 本調査開始後も、サイバー犯罪状況は刻々と変化している。調査項目や内容を追加する場合がある。

② 脆弱な機器からの侵入だけでなく、サプライチェーン経由の侵入が発生しており、それに関する質問などを検討中である。まとまり次第、各社に連絡する。

3.5　作成する図面、表、図書

以下のドキュメントを作成、提出いただく。

① チェックリストによる調査結果（経営層向け）
② チェックリストによる調査結果（システム管理者向け）
③ チェックリストによる調査結果（利用者向け）
④ 病院情報システムのバックアップ状況（表）
⑤ 外部接続先一覧　および　外部接続先調査履歴
⑥ ネットワーク概要図
⑦ 情報システム管理体制図

3.6　調査対象病院への報告

① 現状の詳細資料（前項①～⑦）を提出し、脆弱性、管理上の必要性など指摘する。

② 既存のファイアウォール,VPN の脆弱性が公開された時に、自院に同様の状況がないか判断するためにも、事前に作成すべき資料である。

③ サーバーセキュリティ対策、事故発生時に 各病院が保持し、更新していくことが重要である。

④ ここで作成された資料は、脆弱性が公開された場合に自院に同様の脆弱性がないか確認し、脆弱性がある場合の対応を可能にする。脆弱性情報は日本国内では IPA、JPSIRT 等で公開されるので、今後その部分の委託が可能になると期待する。

⑤ これら資料（詳細情報）は、厚生労働省担当室（特定医薬品開発支援・医療情報担当参事官室）に提出する。ただし、厚生労働省からの公開（政策検討の会議資料、各種規則や指針）および当研究班での公開（学会等への報告）では、個別施設名を示す事や特定のセキュリティ上の弱点を晒すこと（サイバー犯罪者に資する情報の公開）はせず、統計的情報などに限定する。調査担当各社も日本遠隔医療協会との秘密保持協定で、本項の遵守が義務づけられる。

4．調査手順

① 日本遠隔医療協会からの意向確認
- 調査に協力いただけるか、研究班事務局（日本遠隔医療協会）が確認する。
- 日本遠隔医療協会から秘密保持に関する誓約書を提出する。
- 確認次第、調査担当社が引き継ぐ。

② 意向確認後、一ヶ月以内
- 調査担当社から連絡
- 訪問調査日程等の調整

③ 調査

- チェックリストヒヤリング　1～2 回（一回半日程度）
- 施設内巡回調査　　1～2 回訪問（一回半日程度）

④ 調査報告提出

- 調査後一ヶ月以降、2023 年 5 月末日までにお送りする。

5．誓約書

① 調査対象施設（病院）と研究班（日本遠隔医療協会）で情報に関する取決を行う。

② 情報管理に関する誓約書を日本遠隔医療協会から各施設に提出する。

③ 研究班と調査各社は誓約書に沿った秘密保持契約を締結してから、調査に入る。

【資料２　病院向け依頼状】

令和５年１月＊日

貴院名
院長先生名　御侍史

厚生労働行政推進調査事業
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
研究代表者　近藤博史

サイバーセキュリティに関する病院調査への協力のお願い

日頃より厚生労働行政推進調査事業でお世話になっております。一般社団法人日本病院会様より、サイバーセキュリティに関するご意向調査を行いましたところ、貴院よりご協力をお申し出いただき、深く感謝申し上げます。研究班で検討の結果、貴院にて調査を進めたく、ご依頼いたします。以下は日本病院会殿よりの意向調査の説明の繰り返しですが、趣旨と今後の手順をお示しいたします。

1. 背景と目的

ランサムウェア等の被害で、複数の病院が狙われ、医療情報システムを破壊され、診療に支障を来す事態が発生しております。厚生労働省では、その対策を立案すべく、厚生労働行政推進調査事業で複数の病院について、サイバーセキュリティの現状に関する調査を進めております。

サイバーセキュリティに関する各病院の技術水準を高めることや、人材を揃えることはたいへん困難です。一方でサイバーセキュリティ上のリスクは高く、今後さらに高まります。今後の政策立案に活かすため、日本病院会様の会員施設から選ばれた約 10 施設で詳細に調べ、リスクと管理状況を明らかにすることが調査目的です。そこで各施設の医療情報システムの管理状況を後述の手法で調査します。ご協力いただいた施設には、サイバーセキュリティ上の防衛に欠かせない情報設備の管理状況データ（資産管理台帳に相当）をご報告します。今後、このような資産管理台帳は各施設で導入が進むので、パイロットスタディとして、いち早くセキュリティ対策に着手でき、台帳も少ない負担で入手できます。そのような背景をご理解の上で、ご協力いただけますよう、よろしくお願い申し上げます。

2. 調査手法

(1) 厚生労働省の「医療情報システムの安全管理ガイドライン 5.2 版」に基づく調査
以下がホームページの URL です。　参考となる情報が多々掲載されています。このような調査は、今後各施設で必要となります。いち早く手法を習得できる機会となります。

https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html
ガイドライン本体は以下の URL です。
https://www.mhlw.go.jp/content/10808000/000936160.pdf

調査に用いるチェックリストの URL は以下です。
（Excel 版）　https://www.mhlw.go.jp/content/10808000/000936169.xlsx

（PDF 版）　https://www.mhlw.go.jp/content/10808000/000936167.pdf

参考資料として、以下が医療情報システム等の障害発生時の対応フローチャートです。
（Excel 版）　https://www.mhlw.go.jp/content/10808000/000936170.xlsx
（PDF 版）　https://www.mhlw.go.jp/content/10808000/000936168.pdf

調査員（研究班が委託する企業社員）が訪問して、病院長様、システム管理者様、利用者様（職員１、２名）の 3～4 人にヒヤリングいたします。上記チェックリストを用いて、チェックしていただきます。分からないことは、何が分からないか、記載して頂き、○×を記載して頂きます。　所要時間は各 15 分ほどです。

(2) 貴院の情報システムに関する委託事業者に 1 時間程度の面談調査
調査員が訪問して、帳票など具体的な管理文書の有無など、詳細を質問して情報を整理します。

(3) 貴院システム管理者様および貴院委託事業者担当者様の技術的な詳細確認
1 時間ほどの調査を 2 回ほど行い、以下の情報をまとめます。

① 外部接続の状況調査（管理者の知らない接続なども洗い出します。）
- 各システム、ネットワーク保守
- ＣＴ、ＭＲＩ等ネットワーク接続検査等の機器の保守
- マイナカード関係接続
- 地域医療連携接続
- 遠隔読影サービス接続
- 研究ネットワーク接続
- 各種遠隔サービス接続など

② 内部の全体ネットワーク図
- システム名称、DB の名称とサーバと端末、バックアップ等の配置など
- 場合により、病院様の了解の下、委託事業者からベンダーに調査いたします。

③ システム管理台帳

④ 院内各システムのデータバックアップ状況

⑤ 管理体制図

(4) 個人情報について
職員や患者の個人情報は収集しません。

3. 調査結果について
(1) 複数施設を調査するので、それらをまとめて厚生省の政策立案もしくは、学術的な場での公表（論

文、書籍、学会発表）に用います。個別の施設に関する情報やシステム上の詳しい情報を外部に公開することはありません。これについて、後日　日本遠隔医療協会より情報保護に関する誓約書を提出いたします。

(2) ご協力いただいた施設には、調査結果（詳細報告資料）を提出し、管理上の課題など指摘します。

- これまでに攻撃を受けた施設事例のように既存のファイアウォールや VPN の脆弱性が公開された時に、自院に同様の状況がないか判断するためにも、事前に作成すべき資料です。
- ここで作成された資料は、脆弱性が公開された場合に自院に同様の脆弱性がないか、確認し、あった場合の対応することを可能にします。脆弱性の公開については日本国内では独立行政法人情報処理推進機構(IPA), Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) 等に発表されます。今後その部分は委託することも可能になると思います。
- これらの資料は、サーバーセキュリティ対策、事故発生時に 各病院が保持し、更新していくことが重要です。

5. 調査の進め方

今後の調査の窓口を、貴院よりのご協力申出で記されました、以下のご担当者様にお願いしたく存じます。

＜部署名＞　＜役職名＞　＜お名前＞ 様

6. 謝礼について

ヒヤリング等に要した時間ついて、本研究班の規定により謝金をお支払いいたします。また各施設から委託している会社等への調査費用が発生する場合、ご相談の上、お支払いいたします。

7. お問い合わせについて

調査の詳細なご連絡は調査員（研究班が委託する企業社員）が務めます。それ以外の事柄について、下記の研究事務局がご連絡や調整を担当いたします。

特定非営利活動法人日本遠隔医療協会
厚生労働行政推進調査事業、研究運営担当（研究分担者　長谷川高志）
telemedicine-research@j-telemed-s.jp

日本遠隔医療協会事務局
〒370-0033　群馬県高崎市中大類町 37-1
高崎健康福祉大学健康福祉学部 医療情報学科内
http://http://j-telemed-s.jp/

以上

【資料３　病院向け誓約書】

【調査対象施設・日本遠隔医療協会間の秘密保持誓約書（ひな形)】

＊＊病院　殿

この度、特定非営利活動法人日本遠隔医療協会(以下、協会)は、＊＊病院殿(以下、貴院)の第1条に定める本件業務を遂行するにあたり、情報の取扱いに関し以下のとおり誓約する。

第1条(本件業務)

1 本誓約は、貴院のサイバーセキュリティに関する調査に際し、調査で収集する情報について、その秘密保持に関する取扱いを定めることを目的とする。

2 調査により収集する情報は、調査研究の委託者である厚生労働省に、秘密情報(非公開対象)として提出する。

3 調査により収集する情報について、統計的処理等を施して、貴院との関係性を消失したものを、学術的に公開(論文、講演、書籍執筆)することは本件業務の一部に含まれる。

第2条(秘密情報)

1 本誓約において秘密情報とは、文書、口頭、物品および電子媒体等形態を問わず、本件業務の実施に伴い収集する情報のうち、次の各号に定める情報をいう。

　1 秘密である旨が明記された文書、図面、写真またはその他有体物(電子的手段による場合を含む。)として開示された情報。

　2 貴院の施設運営に関する情報で、調査の際に収集された聞き取り結果、文書、図面、写真またはその他有体物(電子的手段による場合を含む。)。

2 前項の規定にかかわらず、次の各号に該当することを協会が証明し得るものは秘密情報には含まれないものとする。

　① 貴院より開示を受ける前に、既に所有または取得していたもの

　② 貴院より開示を受ける前に、既に公知公用となっているもの

　③ 貴院より開示を受けた後に、協会が本契約の規定に違反することなく公知公用となったもの

　④ 開示の権限を有する第三者から、秘密保持の義務を負うことなく、適法に知得したもの

第3条(秘密保持)

1 協会は、貴院の事前の書面(電磁的措置を含。)による承諾なしに、秘密情報を本件業務以外の目的のためには一切使用しない。

2 協会は、本件業務の遂行上知る必要のある自己の従業者および本件業務の一部を委託する他団体の従業者(以下「関係者」という)に対してのみ、秘密情報を開示および共有することとし、合理的かつ善良と認められる注意をもって管理するものとする。

3 協会は、秘密情報を関係者および本件業務で定義した開示先以外の第三者に開示しない。

第4条(秘密情報の管理)

協会は、本件業務を遂行するために合理的に必要な範囲内で、秘密情報を複写および複製することができるものとし、その範囲を超えて複写・複製してはならない。また、秘密情報の複写物および複製物も秘密情報とみなすものとする。

第5条(秘密情報の返還)

協会は、貴院の要請があり次第、速やかに秘密情報(複写物、複製物を含む)を返還し、返還が不可能な場合には、貴院の指示に従って、当該資料を消去または廃棄するものとする。

第6条（秘密情報の権利）

1　秘密情報に関する一切の権利は、貴院に帰属するものとする。また、当事者間で別途合意した場合を除き、秘密情報の開示は、協会に対していかなる権利も付与しないものとして解釈する。

第 7 条（損害賠償）

貴院は、協会が本誓約の規定に違反した場合、当該違反を是正するために必要な措置をとることを求めることができるとともに、当該違反によって被った損害の賠償を請求することができる。

第 8 条（有効期間）

本誓約の有効期間は、202＊年＊月＊日から2023年 3 月 31 日までとする。ただし、第3条、第4条および第5条、第6条、第 7 条はそれぞれの対象事項が存続する限り、本誓約の有効期間終了後も有効に存続する。

2022 年　　＊月　　＊日

群馬県高崎市新後閑町 4-2
特定非営利活動法人　日本遠隔医療協会
理事長　酒巻　哲夫　（押印）

【資料４　調査担当企業向け説明書】

調査担当企業向け資料

調査に当たる企業ご担当者向けの調査業務概説

1．　本文書について

本文書は調査に従事する企業向けの説明文書および手続の解説であり、以下の事項が列記されている。

① 調査企業の責務と役割
② 調査事項と手順
③ 調査事例
④ 手続および工程（スケジュール観）
⑤ 書式類

2．　調査企業の責務と役割

① 調査企業の条件

医療 ICT に関する事業実績が有り、病院内の情報システムに詳しい企業に調査を委託する。厚生労働省発行の医療情報システムの安全管理のためのガイドラインを読み込んでいれば、後述の手順の難度は高くない。調査対象施設でのシステム構築や運用に携わっている企業であれば、円滑な調査の遂行を期待できる。

② 調査企業への支援

研究代表者と協力して、A 病院の調査を担当し、調査手順を開発したセコム山陰株式会社が、手順実施の支援や質問対応、レポートの確認、情報共有支援、工数モニタリングなどの調査支援を担当する。その指導や支援に沿って調査されたい。

③ 調査目的

まだ日本国内の病院のサイバーセキュリティの状況に関する実態情報が無く、日本国内の多くの病院がどのような状況にあり、国家レベルの対策として何を打ち出すべきか、厚生労働省に伝え政策立案の情報収集が本調査研究の目的である。個別施設の課題解決は重要だが、大方針が立たないうちに個別課題に没入することは全ての病院に取り、好ましい状況ではない。そこで調査対象施設のサイバーセキュリティに関する能力向上、問題点の詳細調査や指導、監査は範囲外である。調査を担当する各社は、現状調査に徹していただきたい。

調査により、サイバーセキュリティ上の不足や不備が見いだされるかもしれないが、その責任追及や処罰のための報告なども研究目的ではない。不備や不足な状況も、受け止めるべき現実として明らかにしてゆく。監査や改正に要する研究予算も有していない。

後述の調査結果を整理した段階で指摘できる問題点や対策について、報告書に記す。

④ 調査に関する契約

調査各社との契約者は各病院でなく、厚生労働行政推進調査事業研究班の受託機関（事務局）の特定非営利活動法人日本遠隔医療協会である。各企業は日本遠隔医療協会との間で、見積・発注・秘密保持等の契約を結ぶ。秘密保持契約の対象には、調査各社と日本遠隔医療協会の知財だけでなく、調査対象病院から得た調査結果情報が含まれる。知財と言えない情報でも、調査各社で許可なく利用や公開することは認められない。

3．　調査事項と手順

3.1　概要

今回の調査は**①事前調査**のステップとして、病院担当者あるいは調査各社が効率的に実施できる手法の開発を狙っている。ただし開発途上の手法なので、不明点や過不足は、調査途上で適宜修正しながら進める。調査手順に関する不明点、過不足について、調査各社はセコム山陰株式会社に報告、相談しながら、調査を進められたい。

3.2　チェックリストによるヒヤリング

① 医療情報システムの安全管理のガイドラインにあるチェックリスト（経営層向け、システム管理者向け、利用者向け）を訪問調査で聞き取り、作成する。

② チェックリストは下記 URL よりダウンロードできる。

「医療機関のサイバーセキュリティ対策チェックリスト」　Excel 版
（経営層向け、システム管理者向け、利用者向けがこの Book 内に含まれる）
https://www.mhlw.go.jp/content/10808000/000936169.xlsx
https://www.mhlw.go.jp/content/10808000/000936167.pdf　（PDF 版）

③ 病院長、システム管理者、利用者（1、2 名）の 3−4 人に、訪問調査前に予め上記チェックリストをダウンロードいただき、内容を確認いただき、第一回訪問に備えていただきたい。そこで結果を調査員と付き合わせる。

- 分からないことは、何が分からないか、記載して頂き、○×を記載して頂く。
- 理解が困難であった部分は記録し、今後の検討材料にする。ヒヤリングは一人 30 分ほどで終える。**（病院長、利用者で最大で 1.5 時間×2）**

④ システム管理者にも同様に対面での調査を行う。**2 時間以上、半日程度の調査にする。**資料が病院にあってすぐに出ない場合は、その場では宿題として、一週間の期間に提出を求める。提出されなかった場合、出されなかったとして記録する。（提出が必須ではなく、1 週間掛けても提出できないことも、実態の情報となる）資料が保守業者にある場合には業者の担当者、連絡先を聞き、病院の了解の下、直接ベンダーに聞く。ベンダーに聞く場合も、1 週間以内に情報が出されない場合には、出せなかったとして記録する。

- 分からないことの説明、帳票など具体的なものがあるのかなど、詳細を質問し完成させる。
- この調査は第一回訪問だけでは終わらない。二回目訪問などが必要である。

3.3　院内設備の巡回調査

① 外部接続、サーバ、ネットワーク機器等は調査会社、システム管理者、病院からの委託事業者が直接院内巡回して機種等を確認する。

- システム管理者と委託事業者担当者の技術的な詳細確認は 1 時間を 2 回ほど必要

② 必要な場合、調査施設の了解の下、ベンダーに問合せていただく。

③ 外部接続の状況調査（管理者の知らない接続なども洗い出す）の対象は以下の通り。

[1] 各システム
[2] ネットワーク保守
[3] ＣＴ、ＭＲＩ等ネットワーク接続検査等の機器の保守
[4] マイナカード関係接続
[5] 地域医療連携接続

[6] 遠隔読影サービス接続
[7] 研究ネットワーク接続
[8] 各種遠隔サービス接続など

3.4 追加ヒヤリング等

① 本調査開始後も、サイバー犯罪状況は刻々と変化している。調査項目や内容を追加する場合がある。
② 脆弱な機器からの侵入だけでなく、サプライチェーン経由の侵入が発生しており、それに関する質問などを検討中である。まとまり次第、各社に連絡する。

3.5 作成する図面、表、図書

以下のドキュメントを作成、提出いただく。

① チェックリストによる調査結果（経営層向け）
② チェックリストによる調査結果（システム管理者向け）
③ チェックリストによる調査結果（利用者向け）
④ 病院情報システムのバックアップ状況（表）
⑤ 外部接続先一覧　および　外部接続先調査履歴
⑥ ネットワーク概要図
⑦ 情報システム管理体制図

3.6 調査対象病院への報告

① 現状の詳細資料（前項①～⑦）を提出し、必要に応じて、脆弱性、管理上の必要性など指摘する。
② 既存のファイアウォール,VPN の脆弱性が公開された時に、自院に同様の状況がないか判断するためにも、事前に作成すべき資料である。
③ サイバーセキュリティ対策、事故発生時に 各病院が保持し、更新していくことが重要である。
④ ここで作成された資料は、脆弱性が公開された場合に自院に同様の脆弱性がないか確認し、脆弱性がある場合の対応を可能にする。脆弱性情報は日本国内では IPA、JPCERT 等で公開されるので、今後その部分の委託が可能になると期待する。
⑤ これら資料（詳細情報）は、厚生労働省担当室（特定医薬品開発支援・医療情報担当参事官室）に提出する。ただし、厚生労働省からの公開（政策検討の会議資料、各種規則や指針）および当研究班での公開（学会等への報告）では、個別施設名を示す事や特定のセキュリティ上の弱点を晒すこと（サイバー犯罪者に資する情報の公開）はせず、統計的情報などに限定する。調査担当各社も日本遠隔医療協会との秘密保持協定で、本項の遵守が義務づけられる。
⑥ 病院への報告書は日本遠隔医療協会を通じて提出する。

4．調査の作業量の目安

① 2022 年 3 月に実施した A 病院で要した作業概要を以下に示す。
- 詳細工数内訳を参考資料 1 に示す。

② 総工数としては約 300 時間（参考資料 1　参照）

- A 病院は、研究代表者（近藤博史）と人間関係がある施設である。
- セコム山陰と同院技術担当者とコミュニケーションがとり易い状況だった
- 初めてコンタクトする病院の場合は、調整などで工数が増える可能性がある。
- 訪問人数　2 名又は 3 名で訪問。　1 名で訪問の場合、工数削減可能。

③ 工数変動要因

- 病床数、情報系担当の人的体制（スキル)、ベンダーに対する保守の委託内容など
- 移動に関わる交通費・工数、宿泊費が追加になる

④ 今後の打合せ

- 全体キックオフ
- 各社スタート時の小キックオフ（各社、セコム山陰、日本遠隔運動療法協会）を行う。

5．調査対象病院

① 日本病院会会員の候補施設

- 長谷川から、意向確認して、その後、担当社との手順に入っていただく。
- その病院に出入りのシステム会社を紹介してもらう施設がいくつかあるので、日本遠隔医療協会から会社にも連絡を入れて、「本当に調査を担当するか？」を確認する。

② おしどりネット内の対象候補病院（研究代表者から各施設に依頼する）

③ 各病院への訪問の連絡は、担当各社より実施する。

- その際に病院向け説明書（本書前部、別途独立版あり）を各社より渡して説明する。
- 訪問に関する諸業務は各社で調整の上で実施する。
- 後述の情報共有システムで、訪問日程などを報告する。
- 各病院と日本遠隔医療協会（研究事務局）での調整すべき事項は、必要時に研究事務局まで連絡する。

6．全工程のスケジュール観

このスケジュール観を目安とするが、遅れ気味なので早めるよう努力する。早く調査が進む施設は以下のスケジュールに囚われず、早々に報告書作成まで終える。

① ～11 月中旬

- ターゲット病院の決定
- 並行して作業内容、工数、費用などの算定

② ～11 月下旬

- 契約
- 日本遠隔医療協会から各調査会社への発注

③ 12 月初

- 訪問・メール・電話等での調査開始
- 途中調査会社～セコム山陰との間で調整、フォローを実施

④ ～1 月中旬　調査会社は途中経過をセコム山陰に報告し、レビューを受ける。
追加で必要な調査を実施頂く（深掘りして欲しい部分）

⑤ ～2 月上旬　調査会社～セコム山陰の間で報告書、ドキュメントの調整
この段階のとりまとめ前報告書も、研究班で参照し、まとめ方を改良する。

⑥　～2 月下旬　　調査会社から日本遠隔医療協会に報告書提出と検収

7．調査各社間の情報共有体制

セコム山陰により、各社・研究班間の効率的な情報共有システムを準備するので、各社もこれを用いてデータ共有や報告など行う。詳細説明および ID,パスワード等は別途、セコム山陰より連絡する。

8．契約関連事項

① 見積予算。

- 人件費で300万円を上限として､見積いただく｡出張回数見通しも見積に含めていただく。見積は概算でかまわない。実績時に調整する。

② セコム山陰による「調査会社に対する調査・報告書作成業務の支援、監修」

- 別途　研究班とセコム山陰で、調査各社への支援に際しての秘密保持契約を結ぶ。
  - 両者の知財保護だけでなく、「調査時に調査対象施設で得た情報を秘密保持対象とすること、秘密保持期間は無期限」との条項を盛り込む。
- 複数施設調査への支援業務として契約を協議して内容を決定して、終了時に精算する。
- 作業途中で、セコム山陰が工数モニタリングして、日本遠隔医療協会に報告する。

③ 個別病院と研究班の秘密保持（各施設～日本遠隔医療協会）

- 調査対象施設（病院）と研究班（日本遠隔医療協会）で情報に関する取決を行う。
  - 情報管理に関する誓約書を日本遠隔医療協会から各施設に提出する。
  - 研究班と調査各社は発注契約と秘密保持契約を結ぶ。(対象病院別の締結)
- 調査病院のリスクを“調査した内容が外部に漏洩すること”として、防衛する。
- 研究班の秘密保持の誓約の元で、委託する調査会社に対しても同様に遵守させる

④ 調査各社の病院別調査契約（各社～日本遠隔医療協会）

- 日本遠隔医療協会と各社で締結する。
- 各社は日本遠隔医療協会に見積書を提出する。
- 日本遠隔医療協会は各社に発注書を渡す。これを契約とする。
- 秘密保持契約を別に締結する。
  - 両者の知財保護だけでなく、「調査時に調査対象施設で得た情報を秘密保持対象とすること、秘密保持期間は無期限」との条項を盛り込む。
  - 秘密保持契約のサンプルは日本遠隔医療協会から提供する。
- 調査担当各社には､秘密保持を前提として､A 病院調査報告書をサンプルとして開示する。この報告書も秘密保持対象とする。

⑤ 見積と契約の手続について

- 以下の条件で見積書を作成して、研究事務局（takahasegawa@j-telemed-s.jp）に PDF で提出する。
  - 本資料に定める調査を行う。
  - 人件費 300 万円に収まる範囲での作業を計画する。
  - 工数（調査、図書作成)、出張旅費、必要経費（消耗品等）を示す。

- 週一回、工数実績を報告いただく（セコム山陰でモニタリング、集計する）
- 担当窓口を定めて、日本遠隔医療協会およびセコム山陰との連絡を一本化する。
- 終了時に工数等実績を見て、必要な調整を行う。

● セコム山陰のアシスト下で調査、報告を作成する。

- セコム山陰の情報共有システムを用いて、情報共有、データ共有を行う。
- 前述の工数報告は、同システムを用いて行う。

⑥

付属資料

参考資料１　２０２２年２月～２０２２年５月に於いてＡ病院に対して行った調査業務での工数内訳

【研究班情報】

1. 研究代表者　近藤博史
   ① 鳥取大学名誉教授（元鳥取大学医学部附属病院医療情報部　部長・教授）
   ② 協立温泉病院　院長
   ③ 特定非営利活動法人日本遠隔医療協会　特任主席研究員

2. 研究分担者　山本隆一
   ① 一般社団法人医療情報システム開発センター　理事長

3. 研究分担者　美代賢吾
   ① 国立研究開発法人　国立国際医療研究センター　医療情報基盤センター　センター長

4. 研究分担者　星本弘之
   ① 国立研究開発法人　国立国際医療研究センター　医療情報基盤センター

5. 研究分担者　長谷川高志
   ① 特定非営利活動法人日本遠隔医療協会　特任上席研究員
   ② 本調査の事務局

6. 調査事務局

特定非営利活動法人日本遠隔医療協会
厚生労働行政推進調査事業、研究運営担当（研究分担者　長谷川高志）
telemedicine-research@j-telemed-s.jp

日本遠隔医療協会事務局
〒370-0033　群馬県高崎市中大類町 37-1
高崎健康福祉大学健康福祉学部 医療情報学科内
http://http://j-telemed-s.jp/

【資料５　調査担当企業・日本遠隔医療協会間秘密保持契約】

【日本遠隔医療協会・調査担当企業間の秘密保持契約書（ひな形)】

秘密保持契約書

特定非営利活動法人日本遠隔医療協会（以下「甲」という）と＊＊＊＊＊＊＊＊＊株式会社（以下「乙」という）は、甲乙間で第１条に定める本件業務の遂行するにあたり、互いに開示又は提供する情報の秘密保持に関して、以下のとおり秘密保持契約（以下「本契約」という）を締結する。

第1条（本件業務）

1 本契約は、調査対象病院のサイバーセキュリティに関する調査に際し、調査で収集する情報について、その秘密保持に関する取扱いを定めることを目的とする。

2 調査により収集する情報は、調査研究の委託者である厚生労働省に、秘密情報（非公開対象）として提出する。

3 調査により収集する情報について、統計的処理等を施して、調査対象病院との関係性を消失したものを、学術的に公開（論文、講演、書籍執筆）することは本件業務の一部に含まれる。

第2条（秘密情報）

1 本契約において秘密情報とは、文書、口頭、物品および電子媒体等形態を問わず、本件業務の実施に伴い収集する情報のうち、次の各号に定める情報をいう。

　1　秘密である旨が明記された文書、図面、写真またはその他有体物（電子的手段による場合を含む。）として開示された情報。

　2　調査対象病院の施設運営に関する情報で、調査の際に収集された聞き取り結果、文書、図面、写真またはその他有体物（電子的手段による場合を含む。）。

2 前項の規定にかかわらず、次の各号に該当することを乙が証明し得るものは秘密情報には含まれないものとする。

　① 調査対象病院より開示を受ける前に、既に所有または取得していたもの

　② 調査対象病院より開示を受ける前に、既に公知公用となっているもの

　③ 調査対象病院より開示を受けた後に、乙が本契約の規定に違反することなく公知公用となったもの

　④ 開示の権限を有する第三者から、秘密保持の義務を負うことなく、適法に知得したもの

第3条（秘密保持）

1 乙は、甲の事前の書面（電磁的措置を含む。）による承諾なしに、秘密情報を本件業務以外の目的のためには一切使用しない。

2 乙は、本件業務の遂行上知る必要のある自己の従業者および本件業務の一部を委託する他団体の従業者（以下「関係者」という）に対してのみ、秘密情報を開示および共有することとし、合理的かつ善良と認められる注意をもって管理するものとする。

3 乙は、秘密情報を関係者および本件業務で定義した開示先以外の第三者に開示しない。

第4条（秘密情報の管理）

乙は、本件業務を遂行するために合理的に必要な範囲内で、秘密情報を複写および複製することができるものとし、その範囲を超えて複写・複製してはならない。また、秘密情報の複写物および複製物も秘密情報とみなすものとする。

第5条（秘密情報の返還）

乙は、甲の要請があり次第、速やかに秘密情報（複写物、複製物を含む）を返還し、返還が不可能な場合には、甲の指示に従って、当該資料を消去または廃棄するものとする。

第6条（秘密情報の権利）

1　秘密情報に関する一切の権利は、調査対象病院に帰属するものとする。また、当事者間で別途合意した場合を除き、秘密情報の開示は、乙に対していかなる権利も付与しないものとして解釈する。

第7条（損害賠償）

甲は、乙が本契約の規定に違反した場合、当該違反を是正するために必要な措置をとることを求めることができるとともに、当該違反によって被った損害の賠償を請求することができる。

第8条（有効期間）

本契約の有効期間は、202＊年＊月＊日から2023年 3 月 31 日までとする。ただし、第3条、第4条、第5条、第6条および第7条はそれぞれの対象事項が存続する限り、本契約の有効期間終了後も有効に存続する。

第9条（協議事項）

甲及び乙は、本契約に定めのない事項及び本契約の履行又は解釈にあたって生じた疑義について、信義誠実の原則に従い、その都度協議により定めるものとする。

本契約締結の証として、本書２通を作成し、甲及び乙は記名押印のうえ、各自その１通を保有する。

２０２＊年　＊＊月　＊＊日

甲：群馬県高崎市新後閑町4-2
特定非営利活動法人日本遠隔医療協会
理事長　　酒巻　哲夫　（押印）

乙：

【資料６　調査担当企業工数確認票】

病院に対するサイバーセキュリティに関する調査・報告書作成業務

対象病院	
調査企業	

	項目		予定工数（時間）	実績工数（時間）
1	①チェックリストによるヒアリング（経営層向け）	調査	16.00	
2	①チェックリストによる調査結果（経営層向け）	図書作成	16.00	
3	②チェックリストによるヒアリング（システム管理者向け）	調査	16.00	
4	②チェックリストによる調査結果（システム管理者向け）	図書作成	16.00	
5	③チェックリストによるヒアリング（医療従事者・一般のシステム利用者向け）	調査	16.00	
6	③チェックリストによる調査結果（医療従事者・一般のシステム利用者向け）	図書作成	16.00	
7	④病院情報システムのバックアップ状況（表）	調査	4.00	
8	④病院情報システムのバックアップ状況（表）	図書作成	16.00	
9	⑤外部接続先一覧　および　外部接続先調査履歴	調査	4.00	
10	⑤外部接続先一覧　および　外部接続先調査履歴	図書作成	16.00	
11	⑥ネットワーク概要図	調査	4.00	
12	⑥ネットワーク概要図	図書作成	16.00	
13	⑦情報システム管理体制図	調査	4.00	
14	⑦情報システム管理体制図	図書作成	16.00	
15	移動			
16	打合せ			
17	その他（事前調査、進捗報告など）		24.00	
		合計	200.00	

（調査会社）　→　セコム山陰（取り纏め）　→　日本遠隔医療協会