地域医療連携・地域包括ケア
分科会報告書

（分科会報告・提言書案）

平成 29 年 1 月 20 日

地域医療連携・地域包括ケア分科会

Ⅰ.はじめに：地域医療連携・地域包括ケアシステムの現状と課題

メディカル IT セキュリティフォーラム代表理事
愛知医科大学医療情報部
深津　博

地域医療連携は開業医・かかりつけ医から一般病院（急性期病院）への患者紹介を前提とする前方連携と、急性期病院から退院する患者を亜急性期もしくは療養型病院に定員させる後方連携の機能に大別される。

関与する職種としては前者では医師、地域医療連携室の担当事務職、後者では医師、看護師に加え社会福祉士（MSW）等の役割が大きい。

両者に共通するのは、異なる医療施設・法人の複数の異なる職種間で、一人の患者に関する情報を共有してその患者に関する医療的な連携がスムーズに進むように配慮することが重要である点である。

地域医療連携の重要性は電子カルテ等の IT システムが導入される以前から指摘されており、国による診療報酬付与等の政策誘導も加わって 2000 年代前半に比較的急速に普及した。

その後一般病院における電子カルテの普及に伴い、地域連携機能のシステム化の流れが始まった。しかしながら国による補助金による試験事業としてのスタートアップが多かったためもあり、補助金の期限が切れた後維持ができなくなった事例等が散見され、必ずしも順調に推移しているとは言えない。

また多くのシステムが開業医からは急性期病院のカルテを閲覧できるのに対して、急性期病院からは開業医のカルテの閲覧が一般的にはできない、といった一方通行性の問題もあり、システムの機能や運用、将来性についても、必ずしも楽観的とは言えない現状である。

セキュリティ上の観点から言えば、情報共有を行うネットワーク全体としてのセキュリティについて、責任の所在や分界点が明確でない点、運用上の対策について一定の基準がなく、ネットワークの構成員に任されておりレビューされていない現状も問題として指摘できる。

さらに大きな問題点は、自施設がいくらセキュリティ対策に力を入れていても、低レベルのセキュリティ対策しか採っていない施設と連携した瞬間に、そのレベルに落ちてしまうという厳然たる原則である。裏返せば、現状で接続していて大丈夫なのか、新たな施設を参加させて大丈夫なのか、という本来は本質的かつ基本的な問題が省みられることなく放任された状態で、ネットワークの運用や拡大が日々行われているという点が指摘されるべきであろう。

また 2012 年から導入が推進されている地域包括ケアについても、そのシステム化における問題点、さらにセキュリティ上のリスクについて、現在まで十分に検討されているとは言えない状況が存在する。

メディカル IT セキュリティフォーラムでは地域医療連携システムの上記問題点に加え、システム上のセキュリティに関する問題点を指摘し、セミナー等で報告してきたが、

今回は分科会として、地域医療連携に加え、介護連携も含めた地域包括ケアのセキュリティ上の課題・問題点を抽出し、技術的観点と運用上の観点から考慮すべき対策等について提言することを志向した。

本報告・提言書においては、地域医療連携、地域包括ケアの各システムについて、運用面・技術面の問題点・課題、運用面・技術面での対策について、それぞれの分野の担当者により分担して記述を依頼した。

さらに第三者監査の観点から監査法人の担当者には、外部監査の適用や基準等についても記載を依頼した。

今後の地域医療連携・地域包括ケアシステムの発展の前提となるセキュリティの確保について、関係者の理解を深めていただく一助になることを切に願うものである。

Ⅱ.地域医療連携システム(ユーザの立場から)

独立行政法人 国立病院機構 名古屋医療センター 佐藤智太郎

1. 現状における課題と問題点

情報のデジタル化は医療連携を大きく変え、IT を使った地域連携システムは日本全国に広く拡大し、大学病院から診療所、訪問看護ステーションや薬局、さらに介護施設まで診療情報を共有できる体制が整ってきている。

ここでは、2016 年 10 月の時点で IT 利用の地域連携の主流となっている、「地域の基幹病院で電子化されて生成・保管されている、文書・画像などのデジタルデータを、何らかの回線で外部の医療機関に閲覧させる」というシステムの課題と問題について、実際に運用しているユーザの立場から以下の点について述べる。

① 基幹病院の病院情報システムの問題
② 基幹病院内の人的なセキュリティの課題
③ 利用する回線やデータ暗号化(SSL、IP-Sec など)の問題
④ 匿名化の問題
⑤ 閲覧する病院・診療所・訪問看護ステーションなどの側の課題
⑥ 単位地域連携システムのセキュリティ管理者の課題
⑦ 管理コストの低減化への提言

2. 技術的な対策として必要な要件、具体的な対策方法

① 現在主流となっている病院内あるいは外部データセンターにある電子カルテサーバーのデータを閲覧する方式自体には多くの脆弱性がある。

まず、閲覧にマイクロソフト社の Internet Explorer、画像閲覧にアドビ社の Flash player など、マルウェアの標的にされやすいソフトウェアを使用しているシステムが多いことである。いわゆる「定番」「使い慣れた」システムであるが、パッチを当て続けることができない管理体制である事業主体も少なくないところでは、情報流出が危惧される。HTML5 や Safari など他のブラウザへの対応も進める必要があると考える。

② 地域連携システムの整備に関するさまざまな補助金で構築されたシステムは運用にかかる費用を賄うのに苦労することが多く、本フォーラムで行ったアンケートでも、「活動を休止し、ハードウェアは各施設に寄付した。」と答えた事業体があった。この事業体のサーバーや端末が管理されずに放置されることは、セキュリティ上の大きな問題となり得る。病院側も管理する人員がおらず、アップデートも行なえないところもあり、複数の病院ネットワークをまとめる、いわゆるN対N形式の地域連携の事務局がコストの制約のため、連携サーバーを十分に管理できていない状況もある。これらに関しては、一律の補助金で整備する時代は終わり、診療報酬で担当者の公的 IT 関係資格を定めるなど、セキュリティレベルの担保をすることを提案したい。

③ SSL の脆弱性が指摘され、インターネット上に VPN を張って診療データをやり取りするリスクが

徐々に顕在化している。少なくとも、基幹病院間のやり取りは専用線ないしは閉域網に準じたセキュリティを確保すべきで、モバイル運用にあたっても、専用線に近いセキュリティを持つ SIM が開発されており、そちらを使用すべきであると考える。

④ 近年では、診療データを匿名化して大規模に収集してビッグデータとしてまとめ、人工知能の機械学習等に活用しようという方向性が打ち出されているが、病院側に匿名化に関する十分な知識がなく、特に臨床研究を普段行っていない施設では容易に匿名性がなくなる可能性が高い。匿名化にあたっては専門家に十分な検討を依頼する必要があることをガイドライン等で強調する必要があると考える。

3. 運用的な対策としての必要な要件、具体的な対策方法

⑤ 基幹病院等の診療データを閲覧する側のセキュリティレベルには、施設間で大きな差があり、問題のある場合も多い。基幹病院側が定期的に閲覧側施設を巡回し、問題点がなくてもマルウェア等の進化が速く、リスクを完全に排除できない。提案としては、閲覧側の休眠会員（ほとんど閲覧実績がない）は数カ月から 1 年程度で接続を打ち切り、セキュリティ条件を満たさない限り再開しないルールをガイドライン等で設定しておくとよいと思われる。

⑥ 数多くの地域連携システムが全国に存在するが、運用母体が資金潤沢な事例は少なく、事務職員等の兼任で中継サーバーの管理を行なっている事業体が多いと考えられる。中には事業継続をあきらめて、管理を放棄している場合もあると思われ、知らずに診療情報が流失している可能性もあり得る。解決法として、全国の統一的な中央管理システムに各病院が接続し、専任の担当者が中継サーバー（あるいはデータセンター）でトラフィックが正常かどうかを管理する必要があると思われる。

⑦ 各地域で多くの地域連携システムが林立した結果、多数の中継サーバーが重複設置されており、運用開始から数年後のサーバー更新時に費用が払えず、運用停止となる事業体が多いと考えられる。小規模な連携では、コストを掛けた割に良いアウトカムが得られたとの分析結果も得られず、結果としてモチベーションが低下することになる。このコストとパフォーマンスの解決策としては、北欧で行われているような、クラウドコンピューティングを利用した全国統一のカルテ閲覧連携システムが良いと考える。

参考：ICTを活用した「次世代型保健医療システム」の構築に向けて－データを「つくる」・「つなげる」・「ひらく」－、平成28年10月19日、保健医療分野におけるICT活用推進懇談会提言
http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000140306.pdf#search='%E5%8E%9A%E5%8A%B4%E7%9C%81+0000140306'

Ⅲ.地域包括ケアシステム（ユーザの立場から）

大妻女子大学　平野貴大

1. 現状における課題と問題点

地域包括ケアでは、地域に居住する要介護高齢者に適切なサービスをシームレスに提供することが求められる。そのためには、それぞれのサービス提供対象となる要介護高齢者に関するタイムリーな情報がサービス提供において肝要である。

ケアプランや訪問看護計画、訪問介護計画などに記述された内容もサービス提供の場面の情報として重要であるが、利用者の変化について把握しなくては、状況に応じた適切なサービス提供、特に予防的なアプローチは困難となる。同時にサービス提供の状況等に関する情報についても、他のサービス提供事業者との共有が求められる。また、従来の施設型のサービスとは異なり、一人の介護サービス利用者に対して地域内に存在している、複数の医療関係者、介護事業者が関わることを視野に入れる必要がある。

その中で、現在、地域包括ケア実践での情報共有においては、以下の問題が考えられる。

A)　介護分野の情報化（IT 化）の遅れ

B)　介護サービス利用者に関わる情報の偏在と情報の冗長化

C)　事業所ごとの個人情報管理と運用の差異の存在

それぞれの内容については以下の通りである。

A)　介護分野の情報化（IT 化）の遅れ

介護、または福祉分野における情報化は 1970 年代から各地で散見されているが、現在、医療分野における情報化からは大きく遅れをとっている。

この原因として、介護に限らず福祉業界全般で言えることとして、情報化などの検討を行う時間、または資金的な部分での余裕がないため、開発、または継続的な運用できていないことが挙げられる。

また、介護従事者の年齢が比較的高く、IT リテラシーが低いことなどにより、情報システムの導入を行えない、または行わない選択を取っている事業所も存在している。情報共有に電子メールではなく、ファクシミリなどの利用が行われている場合もある。また、記録などもアナログで行われおり、電子化がされていない事業所も存在している。

実際、厚生労働省主導でペーパーレス化などの実証実験を行っている状況で、連携などの検討ではなく、電子化もしくは OA 化の段階で推移している。そのため、現状では医療の情報連携の技術的課題よりは、実作業における運用で対応をしている部分が多くなっている。

このことは地域医療連携システムのセキュリティに関するポリシーのアンケートにおいて、介護関連の参加事業所が少ないことの一因と考えられる。

B)　介護サービス利用者のサービス提供に関わる情報の偏在と冗長化

介護サービスの提供、特に在宅における介護サービスの場合、介護サービス利用者のニーズに

合わせて複数の事業所が関わる。また、同一の利用者に対してのサービス提供頻度はケアプラン等によって事業所ごとに異なってくる。

そのため、介護サービス利用者のケアプラン、訪問介護計画などサービス提供に関する情報は各サービス提供事業者で共有がされるが、サービス提供後の状況等に関する情報量はサービス提供事業者によって異なる。加えて、先に述べたように情報化などの遅れにより情報共有が進まない事態も発生している。結果的に、介護サービス提供事業所によって持っている情報の量や質が異なり、介護サービス利用者にシームレスなサービス提供ができなくなっている場合がある。

C) 事業所ごとの個人情報管理と運用の差異の存在

地域包括ケアの実践では複数の事業所が関わっているが、それらの事業所内での個人情報などを含む情報管理については、共通のセキュリティポリシーなどは存在していない。医療分野と異なり、個人情報保護等に関するガイドラインは高齢、介護分野だけではなく、障害、児童、地域などの全ての福祉分野を対象としたものであり、介護分野に特化したガイドラインは策定されていない。現状では個人情報保護法と厚生労働省による「福祉分野における個人情報保護に関するガイドライン」に基づいて事業所レベルで運用方針を決めているのが実態である。

そのため、利用者の情報の共有においても、記録の中で本名の記載を行うかイニシャル表記にするか運用レベルでの差異が発生している場合もある。また、事業所内での情報共有手段として、事業所の端末ではなく、個人所有のスマートフォンなどを含む情報端末で情報共有を行っている事業所も存在し、セキュリティについては大きなリスクを抱えた状態になっている。

以上が、現状での課題と考えられる部分である。

2. 技術的な対策として必要な要件、具体的な対策方法

上記のような状況にあるため、まず、技術的な対策等として考えられるのは、現在、地域医療連携で行われている各種システムを発展させた形で、医療、介護事業者が介護サービス提供に関する情報を共有可能とするプラットフォームの開発と介護事業者へのシステム導入の推進が考えられる。

技術的な要件としては、多くの介護従事者が比較的高齢であることや IT リテラシーの面で不安を抱えていることを踏まえ、システムの導入においての作業手間等がかからないこと、アナログデータと電子データのシームレスな連携を具体化すること、加えてソフトウェアの操作性を高めることが求められる。あわせて、情報共有に対して負担感を持たないシステムにすることが求められるだろう。その対応策として、あじさいネットにおける運用講習会のような取り組みは他の地域連携ネットワークの展開の中で求められていくことが考えられる。

また、介護業界の財政面の課題などを勘案した場合、管理端末の貸与などを行うことにより、導入とその後の運用において資金面での負担が発生しない形も視野に入れておく必要があると考えられる。

3. 運用的な対策としての必要な要件、具体的な対策方法

幸い、地域医療連携システムのセキュリティに関するポリシーのアンケート内では個人情報の流出等の問題事例は発生していないが、セキュリティの担保については、介護事業所内でアナログデータを取り扱うっている現状を勘案した場合、技術面よりも運用面による対策が有効と考えられる。将来的には情報システムの活用を踏まえたソフトウェア、ハードウェア両面からのセキリュティの対策が必要だが、現状では、アナログデータ、特に紙媒体を用いる事業所が一定数存在することを視野に入れた運用方法の明示を行うことが優先されるだろう。

当然、データの入出力時における、ウィルス対策や通信技術などによるセキュリティの確保も必要であるが、同時に、紙への出力などを行う場合の運用について、システム運用の段階で明確なルール作りをすることと併せて、行政、都道府県、市町村のいずれかのレベルでそのルールを策定することも必要であると考えられる。

このためには、各種事業者による連絡協議会や作業部会などの場を設けることにより電子化ではなく紙媒体を含んだ情報の共有方法の検討を行った上で、電子化後も継続して運用できる情報共有のあり方を模索する必要がある。また、介護サービス利用者によって、利用している介護サービス事業者が異なるため、共有範囲が従来の行政区、または介護保険制度の中学校区基準の範囲を超えての共有が求められる場合も考えられる。

そのため、平成25年3月に厚生労働省より出されている、福祉分野における個人情報保護に関するガイドラインに基づき、市町村、または都道府県単位での詳細な取扱規定やセキュリティポリシーの策定が求められるだろう。

加えて、地域包括ケアの展開に対応することを視野に入れ、医療情報と同等のセキュリティ等のレベルを維持した形での運用にすべきかを含め、個人情報の取扱については、実態に即して検討をする必要がある。

＜参考＞

福祉分野における個人情報保護に関するガイドライン　厚生労働省　平成 25 年 3 月
http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/250329fukusi.pdf

Ⅳ. 地域連携システム（技術的観点）

株式会社 UNI　白水重明
愛知医科大学　深津　博

地域連携システムにおけるセキュリティ対策の考え方として、技術的な対策と運用的な対策をそれぞれ考慮する必要がある。特に、従来型の不正操作を検知して対応するフィルター型の対策にとらわれず、ユーザと操作を限定したホワイトリスト型の採用を可能な限り採用することが有効な対策となる。

1.　技術的な対策：さらにインフラによるセキュリティ対策とアプリケーションによるセキュリティ対策に分類される。

インフラによるセキュリティ対策としては、VPN、SSL、アクセス制御が、アプリケーションによるセキュリティ対策として、端末に資料データを保持しない設計、カルテ情報の参照権限、アプリケーションによる脆弱性対策、ウイルスチェックが挙げられる。

VPN および SSL は接続を行なうことにより、盗聴やなりすましの防止、暗号化によるセキュリティ手法であり、厚生労働省のガイドラインでも推奨されている手法である。但し VPN 自体は物理層における盗聴に対しては脆弱であること、ルータを設置する必要があること、等問題点も存在することを認識する必要がある。

アクセス制御は、センタ機能を介さずに情報公開施設同士や情報公開施設-参照施設が直接やりとりするような通信が発生した場合にはこのファイヤーウォールにて通信を遮断する機能を使う。また、これにより、他施設のコンピュータへの不正アクセスを防止している。コンピュータへの不正アクセスを防止する必要がある。また、センタ機能においては各施設からのアクセスは WEB サーバのみに行われるように制御しており、外部から接続の必要がない DB サーバへは通信が行われないように制御すべきである。

アプリケーションによるセキュリティ対策として、地域連携システムの中継サーバには診療データを保持しない設計にすべきである。これにより診療データの外部保管先を分散することを防ぎ、流出のチャンスを低減することが可能となる。

参照権限の設定と制御は重要であり、カルテ情報の開示については、誰が（診療科・利用者）、何を（データ種別・診療科・データの対象期間）、いつ（期間）といったように項目を細かく設定しアクセス許可を受けたもののみが参照できる形とすべきである。特に患者本人の同意がある場合にのみ閲覧可能とすることにより、改正個人情報保護法の要請にも対応可能となる。

インフラによるセキュリティ対策の各機能をまとめると以下の表1のようになる。

表1. セキュリティリスクに対する対策方法とその対象

リスク	回避方法	技術	情報提供機関	情報参照機関
①ウィルス・ワーム侵入	・ウィルスチェック ・必要以外の通信遮断	・各サーバのウィルスチェエク導入 ・ウィルスチェエクゲートウェイ ・ファイヤーウォール	○	―
②不正侵入	・必要以外の通信遮断 ・認証	・ファイヤーウォール、NATルータ ・SSLによる証明書認証	○	―
③サービス不能攻撃	・Dos攻撃の検知、ブロック	・ファイヤーウォール（IPS機能）	○	―
④なりすまし	・認証	・証明書による認証 ・PKIによる本人確認（認証）	○	○
⑤盗聴、改ざん	・通信暗号化	・SSL暗号化	○	○
⑥情報漏えい	・院内からインターネットへの通信遮断	・ファイヤーウォール	○	―

アプリケーションによる脆弱性対策としては、クロスサイトスクリプティング対策、サードパーティ製品／Webアプリケーションに対する脆弱性対策、不正なリクエストまたは入力データに対する脆弱性対策、HTMLドキュメント内に存在する脆弱性対策、出力コンテンツの脆弱性対策、セッション管理の脆弱性対策、アクセス制御の脆弱性対策、ユーザー認証の脆弱性対策、利用環境の脆弱性対策、その他に分けて、それぞれ対策を施すことが必要と考えられる。（表2）

表2. 脆弱性診断項目

項番		脆弱性分類		診断内容
1		クロスサイトスクリプティング（XSS）		フォームの入力項目にスクリプトを埋め込み、Webサーバを参照したユーザーに対する攻撃が行われる脆弱性の確認
2	A	サードパーティ製品／Webアプリケーションに対する脆弱性	サードパーティ製品の設定	診断対象システムを構成するWebサーバの環境設定に起因する脆弱性の確認
	B		既知のセキュリティホール	Webサーバに既知の脆弱性が存在するかの確認
	C		バックドアとデバックオプション	Webサーバに対してバックドアの設置が可能な脆弱性、およびサーバアプリケーションに対してテスト時に使用するデバックモードが存在していないかの確認
	D		バッファオーバーフロー	Webサーバへ不正なリクエストデータを送ることにより、アプリケーションの誤動作を狙う脆弱性の確認
3	A	不正なリクエストまたは入力データに対する脆弱性	入力データチェック	端末とWebサーバ間を流れるデータが安全に送受信されているかの確認
	B		強制ブラウジング	Webサーバに存在するディレクトリに適切なアクセス権限が設定されているかの確認
	C		パラメーターの改ざん	Webサーバへ送信されるリクエストデータに含まれるパラメー

				ターを改ざんし、不正なリクエストデータがサーバアプリケーションに受け入れられる脆弱性の確認
	D		コマンド・インジェクション	フォームの入力項目にシステムコマンドを埋め込むことでWebサーバが不正なシステムコマンドを実行する脆弱性が無いかの確認
	E		SQLインジェクション	フォーム入力項目にSQの制御文字を埋め込むことでWebサーバが不正にデータベースへのアクセスを実行する脆弱性が無いかの確認
4	A	HTMLドキュメント内に存在する脆弱性	Hiddenフィールドの不正操作	フォーム等で使用されているHiddenフィールドの受け渡しに起因する脆弱性が無いかの確認
	B		疑いのあるコンテンツ	Webサーバ内のコンテンツ（主にHTMLファイル）にコメントとして未公開のURLやファイル名が記述されていないかの確認
5		出力コンテンツの脆弱性		Webサーバから送信されたコンテンツ（HTMLファイル内のScript）にサーバ内部で使用しているパラメーターの情報が記述されていないかの確認
6	A	セッション管理の脆弱性	Cookieの悪用	Cookie情報を改ざんし、不正なCookieがWebアプリケーションに受け入れられる脆弱性を確認
	B		ライフサイクルの確認	セッション情報を再利用し、Webアプリケーションがセッション情報の異常を検知できるかの確認
	C		セッションIDの構成ルールの確認	セッションIDの構成（文字種、長さ）ルールに問題がないかの確認
7		アクセス制御の脆弱性		Webサーバ内のコンテンツにアクセス制御が実施されているかの確認
8		ユーザ認証の脆弱性		ユーザ認証で使用しているアカウントやパスワードのルールが適切であるかの確認
9		利用環境の脆弱性		クライアント側にブラウザの設定変更を要求する部分が無いことの確認
10		その他		Webアプリの画面設計などが適切であるかの確認

ウイルスチェックについては、SaaS 型の場合はアプリケーションレベルでのウイルスチェックの実施が、外部連携拠点設置型の場合は、サーバ機上にウィルス対策ソフトウェアを導入することでウイルスチェックを実施が望まれる。さらに利用者の端末におけるウイルスチェックも必要である。

運用的な対策としては、地域連携運営委員会の設置、運用管理規定の作成、ネットワーク監視が挙げられる。

拠点病院および参加診療所の双方が参加する委員会の設置は重要であり、これにより定期的な情

報交換、運用の見直し、セキュリティ啓蒙活動、責任の所在の明確化等を適宜行い、組織としての継続的なセキュリティ確保の活動につなげていく必要がある。
運用管理規定の作成は、入会（証明書配布）／退会の運用規定、パスワード漏洩防止／証明書コピー防止のための運用規定、ウィルス対策／Winny対策のための運用規定等を定めることが求められる。上記の地域連携運営委員会により決定し、維持されることが想定される。

ネットワーク監視は、ウィルス定義の最新化、Windows Updateの実施、ネットワーク、アプリケーションログ監視などを継続的に行うもので、地域連携運営委員会が主体となって実施することが求められる。

重要な点は、ベンダーに技術的な対策を依頼したのみで安心して、運用面からの対策をとらなければ本当の意味で強固なセキュリティは確保されない点であり、地域連携運営委員会は拠点病院および参加診療所の双方に対して、その点を継続的に啓発することが求められる。

Ⅴ. 第三者監査の視点の重要性

PwC あらた有限責任監査法人　江原悠介

日本における医療機関、介護事業体における個人情報管理あるいは情報セキュリティ管理上の遵守要件を取りまとめた「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ドライン」、及び「医療情報システムの安全管理に関するガイドライン」はその制定より複数回の改定を両書とも重ね、内容面の充実化が図られてきた。

特に後者においては、無線 LAN やモバイル端末の医療現場への導入等の組織内部的な動向に加え、外部サービスの台頭、サイバーリスクの高まり等の外部の技術変化も踏まえた観点より更新が行われており、医療機関等が自機関の情報セキュリティを検討する上で大変有益な準拠枠となっている。一方、当該ガイドラインは多様な論点を網羅し、複雑な構成であることから、その内容を正しく理解し合理的に展開するためには、読み手に一定以上のセキュリティリテラシーを求めるものとなっている。その結果、安全管理ガイドラインの内容を過剰に解釈し、全ての対策を一律同水準で適用する等、費用対効果の面からも実効性が乏しい対策を講じ、対策の形骸化を招いている医療機関も少なくない。

このような状況を解決するためには、二つの観点が必要であると考えられる。一つめの観点は『リスクベースアプローチ』である。監査法人には様々な監査上のメソトロジーが存在するが、この考え方は最も一般的であるとともに、非常に重要な要素となる。様々な解釈があるため、エッセンスのみを抽出して簡単に言えば、リスクが高い範囲にこそ重点的に管理資源（監査資源）を配分するという合目的的な考え方であり、安全管理ガイドラインにも記載されているリスク評価の結果に基づく合理的な管理資源の配分を可能とする基礎である。リスクベースな考えに立ち、自機関が求められる情報セキュリティ上の管理要件のうち、管理資源を重点的に配分するリスクの高い範囲を識別し、強弱ある対策を展開する合理的な管理態勢のもとでこそ、一定の情報セキュリティ水準を継続的に維持することが可能となる。

しかしながら、リスクベースな考え方に基づき、情報セキュリティ管理態勢の整備を行うためには、相応のセキュリティリテラシーが自機関の要員に求められることも事実である。そこで、もう一つの観点として求められるものが『第三者による助言型監査』である。第三者による外部監査の必要性は内部監査（自己評価）の妥当性を検証すべく安全管理ガイドラインにおいても求められるものであるが、ここで言う助言型監査は、自機関の取組是非を外部者として裁断するのでなく、本来あるべきリスクベースな改善の方向性を含め提言することで、自機関の管理水準の円滑な改善・維持に向けた取組を協働的に推進する取組を指す。助言型監査自体は経済産業省「情報セキュリティ監査基準 / 実施基準ガイドライン」に定めがあるが、ここではその定義をさらに拡大解釈し、情報セキュリティ管理態勢を外部の専門家の知見を利活用し、継続的に維持可能な合理的な水準へ是正することで、管理責任力の向上を図る内部的な取組と位置付ける。なお、外部の中立的な第三者機関によるこのような取組自体は、（一社）医療情報安全管理監査人協会(i-MISCA)、（一社）保健医療福祉情報安全管理適合性評価協会（HISPRO）においても行われている。しかし、各団体

が開示する一般情報を閲覧するかぎりでは、経済産業省ガイドラインに照合すると、審査・認証等の保証型監査という性格が強く、気軽に相談したい医療機関や診療所等にとっては「監査」という言葉の生硬さに物怖じしてしまうのではないかとの懸念がある。言うまでもなく、助言型であろうが保証型であろうが、外部監査による態勢の高度化に向けた取組自体は有益であることは論を待たない。しかし、今後、直近に控えた改正個人情報保護法の施行を見るまでもなく、地域医療連携において複数の医療機関、介護事業体、診療所等のステークホルダーが患者情報を共有しあうネットワークの普及に伴い、一定の情報セキュリティ水準の維持が加入機関に求められることはほぼ確実であると思われる。そのような状況下で、今まで情報セキュリティとは縁のなかった機関にとって、ネットワーク加入に向けて自助努力で整備した管理水準の妥当性を、本格的な「監査」というアプローチではなく、リスクベースの観点に立ち、合理的な助言を行うことで、継続的に維持可能なセキュリティ管理に向けた道筋を指し示してくれる、そのような助言型監査を担える外部組織体のニーズは、地域医療連携という社会インフラシステムの普及促進という今後の動向からも確実に高まっていくと考えられる。

よって、本格的な監査も勿論従来通り必要ではあるが、リスクベースの助言型監査アプローチこそが今後の第三者監査に求められる重要な視点となるであろう。このような考えは筆者が所属する組織による意見表明でなく、あくまで筆者の私見に基づくものでしかないが、利害関係者に対する監査責任の遂行のみでなく、監査対象組織、ひいては社会全体の成長・発展について日々の監査業務を通して願う監査法人一般の職員にとってもご賛同を頂ける内容であると個人的に考えている。

Ⅵ.まとめ

メディカル IT セキュリティフォーラム代表理事
愛知医科大学医療情報部
深津　博

地域医療連携・地域包括ケアは、国の方針として本格導入が 2017 年度から開始され、その後の医療等 ID の導入等を経て、二次医療圏およびそれを超えた範囲での包括的な情報連携が想定されている。
情報連携・情報共有は、検査や処方の重複、情報不足による無駄な医療資源の投入の回避、より個別性の高い情報の事前把握による誤診や不適切な治療の回避などに有効性が期待されており、これらによる医療費の縮減効果も考えられるものである。
しかしながら注意すべきは、機微な個人情報を扱う地域医療連携・地域包括ケアにおいては、情報漏洩やサイバー攻撃によるシステム障害、内部不正による情報窃取や不正閲覧等があった場合に、刑事・民事賠償や、信用低下による患者減少等の経営上のインパクトは甚大である点である。
多くの医療機関職員、特に医師はセキュリティに関するリテラシーが低く、またそれを自覚していないために、繰り返し同じリスクを犯しがちである。
さらに 2017 年 4 月に施行予定の改正個人情報保護法では、病歴情報は要配慮個人情報として取得時・第三者提供時に個別同意（オプトイン）が必須とされる。さらに第三者から病歴情報の提供を受けた際には、提供元に対してオプトインを取得して得た情報かどうかを確認する義務も課せられることになる。この規程は不正な情報流通が行われた際にもトレーサビリティを確保して事後に追跡調査ができるような体制を構築するためのものであり、医療等分野以外でも広範囲に適用されるが、特に医療等分野においてはオプトインが原則となるため、要求される要件が自ずと高度となっている。
改正個人情報保護法対応は直接的にはセキュリティ確保と別問題ではあるが、医療機関や介護・福祉機関における個人情報の取扱いは、より厳重にせざるを得ない状況が差し迫っていると言える。
以上の検討を踏まえ、メディカル IT セキュリティフォーラムとして以下を提言する：

1. 地域医療連携・地域包括ケアシステムを利用する際には、それぞれの参加機関がシステム概要やセキュリティ対策について把握し、ベンダーの協力を得て、普段からセキュリティ対策を継続して行うべきである。
2. 地域包括ケアに特化した問題として、そもそも IT 化が遅れている点、運用面でのセキュリティ対策を優先すべき点、セキュリティ対策を統一的な基準で行うための全国的なルール作りが必要な点が挙げられる。
3. 技術的な観点からは
4. 外部監査の視点からは、今後スクベースの助言型監査アプローチこそが今後の第三者監査

に求められる重要な視点となると考えられる。

5. 2017 年に迫った改正個人情報保護法への対応として、オプトイン管理と、トレーサビリティ確保に向けての取組が急務である。

参考：

1) 個人情報保護法ガイドライン（通則編）（案）
http://www.ppc.go.jp/files/pdf/guidelines01.pdf

2) 個人情報保護法ガイドライン（確認記録義務編）（案）
http://www.ppc.go.jp/files/pdf/guidelines03.pdf