日医総研リサーチレポート No.121

2021 年 11 月 24 日

医療分野におけるサイバー保険について

日本医師会総合政策研究機構

堤 信之

坂口一樹

【ポイント】

サイバー保険（付帯・関連サービス含む）が医療機関の実態とニーズに合致し、医療機関のサイバーセキュリティに役立つ方策となり得るかを把握・評価するため、損害保険主要 3 社について関連書類の分析に加え、インタビュー調査を実施した。結果は以下の通りであった。

◆サイバー保険および付帯・関連サービスは、医療機関のサイバーセキュリティ対策に関するニーズを一定程度満たす枠組みと評価できる。

◆これらを医療機関に対して周知し活用することは、有効なサイバーセキュリティ対策になる可能性がある。保険業界は医療界のニーズに応える機能の提供者として、今後とも有望な候補の一つと言える。

◆他方で同保険には以下のとおり改善すべき課題がある。

①厚生労働省「医療情報システムの安全管理ガイドライン（5.1 版）」を踏まえたサイバー保険（付帯・関連サービス含む）の組み立て。

②医療機関にとって魅力ある補償金額および保険料水準の保険設計の実現。

③緊急時対応窓口サービスの拡充。

④各種コンサルティングサービス等における医療機関の独自性を踏まえたノウハウの向上。

など。

目次

１．はじめに

近年、日本でも産業界が被るサイバー攻撃が注目され、攻撃による被害発生も報告されている[1]。そのリスクに備えるため、民間の損害保険会社がこぞって「サイバー保険」を各社独自に開発し、提供している[2]。しかしながら、2021 年 1 月に公益社団法人日本医師会と公益財団法人医療機器センターが共同で実施した「医療機関の情報システムの管理体制に関する実態調査」[3]（以下「2021 調査」）によれば直近の医療界における同保険の加入率は極めて低く、保険内容の理解度も高くないことが判明した[4]。その主な理由として、従来、医療機関の医療情報システムが外部ネットワークと接続しないのが一般的であったこともあり「サイバー事故」の発生が外部に報じられることが少なく、身近な脅威と感じられなかったことが考えられる。実際に 2021 調査では、サイバー保険の加入検討に至る以前のサイバーセキュリティ対策への基本的な取組からして立ち遅れているという医療界の実態が明らかになった[5]。

本来的には、医療機関で取り扱う医療情報には極めてセンシティブかつ高い価値を有するデータが含まれており、犯罪者にとって魅力的なものと考えられる。にもかかわらず、重大インシデントの発生があまり報じられてこなかったのは、筆者見解によれば、医療機関の医療情報システムが外部接続のない特殊なものとの印象がサイバー攻撃の犯罪者側に強くあり、医療界が積極的にはターゲットにされなかったという心理的な要因が大きいのではないかと考える。今後、患者・受診者にとっての利便性の向上や公共利益の追求を背景に、オンライン診療、オンライン資格確認といった外部ネットワークと接続する仕組みが拡大すると、上記前提条件が大きく変わる結果、急速にサイバーリスクが顕在化し、重大インシデント発生の可能性が高まることが懸念される。実際に、昨年来いくつ

---

[1] 独立行政法人情報処理推進機構 セキュリティセンター（2021）。

[2] サイバー保険とは ｜ サイバー保険 ｜ 日本損害保険協会（sonpo.or.jp）
「サイバー保険」とは、サイバー事故により企業に生じた第三者に対する損害賠償責任のほか、事故時に必要となる費用や自社の喪失利益を包括的に補償する保険と説明されている。保険会社により「サイバー保険」の他、「サイバーリスク保険」、「サイバーセキュリティ保険」等の商品名がつけられているが、本稿では総称して「サイバー保険」とする。

[3] 坂口・堤（2021）。

[4] 本稿 3 頁資料 1 参照のこと。2021 調査によれば、「保険に加入していない」90.1%、「保険に加入しており内容も知っている」3.6%、「保険に加入しているが内容はよく知らない」5.3%という結果であった。2021 調査では「サイバーセキュリティ保険」と称したが、本稿では「サイバー保険」に統一した。

[5] 脚注 3 に同じ。医療現場の医療情報システム関連の組織体制、サイバーセキュリティに関する行政の取組の認知度・活用度、サイバーリスクマネジメント体制の何れも問題含みであることが判明した。例えば、リスクマネジメントの基礎となるべき院内医療情報システムのネットワーク構成図ですら、約半数の医療機関が保有していない実態は、医療機関のリスクマネジメントに関する取組の立ち遅れを象徴する結果と考えられる。

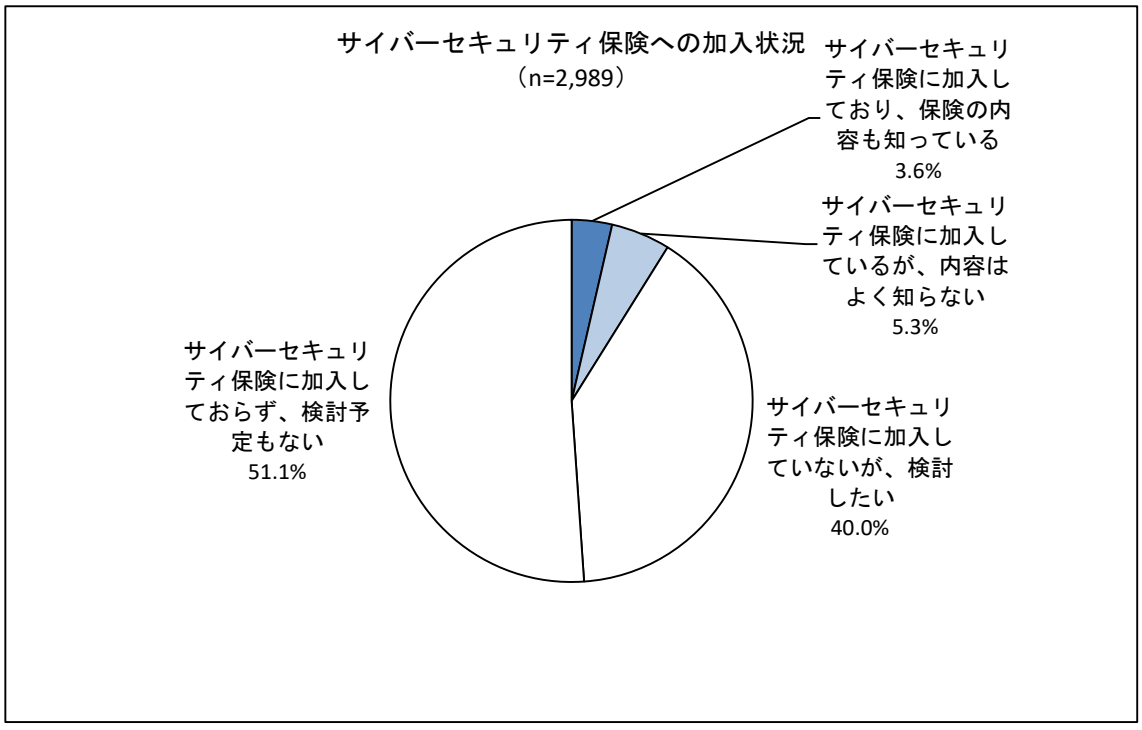
かの病院でのサイバー事故例がメディアでも報じられた[6]。このような事態への備えとして、サイバー保険の位置付けが重要になることが想定される。

他方では、保険業界としても、事故発生後の損害に対するサイバー保険による金銭的補償の及ぶ範囲もさることながら、リスク低減策、被害軽減策等の総合的なサービス（付帯サービスまたは関連サービス等。以下「付帯・関連サービス」）が、保険とセットで保険会社から提供されることを医療機関に十分周知できていないことが窺われ[7]、これも同保険の普及が果々しくない要因と思われる。

上記を総合すれば、サイバー保険の補償内容や付帯・関連サービスが、医療機関の実態やニーズ[8]に合致すると評価できるなら、医療機関のサイバーセキュリティ対策に関する取組の遅れを取り戻すための方策として、これらを医療機関に対して周知し活用することが考えられる。そこで本稿では、サイバー保険（付帯・関連サービス含む）が有効な対応策になり得るかを論じた。

（参考資料）2021 調査より

〇資料１：サイバーセキュリティ保険への加入状況

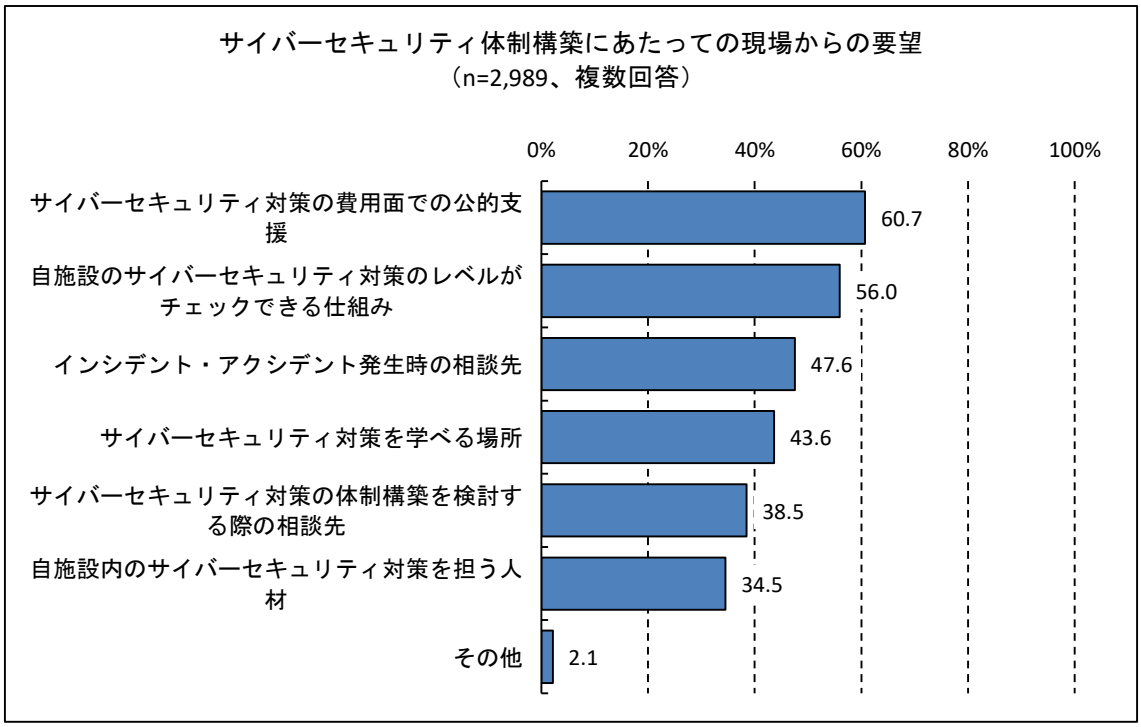


[6] 福島県立医科大付属病院事件（2020 年 12 月 3 日日本経済新聞朝刊）、徳島県つるぎ町立半田病院事件（2021 年 11 月 12 日日本経済新聞夕刊）など。

[7] 脚注 4 に同じ。本頁資料 1 参照のこと。

[8] 本稿次頁資料 2 参照のこと。本稿では、「費用面での公的支援」を除く選択肢（医療機関のニーズ）への対応を評価する。

○資料２：サイバーセキュリティ対策に関する医療機関の主なニーズ



（「サイバーセキュリティ体制構築にあたっての現場からの要望」（複数回答）について要望の多かった順に記載。）

サイバーセキュリティ体制構築にあたって最も優先度が高い要望

		全体	自施設のサイバーセキュリティ対策のレベルがチェックできる仕組み	インシデント・アクシデント発生時の相談先	サイバーセキュリティ対策の体制構築を検討する際の相談先	サイバーセキュリティ対策を学べる場所	自施設内のサイバーセキュリティ対策を担う人材	サイバーセキュリティ対策の費用面での公的支援	その他
全体		2,989	27.4	14.2	9.9	9.4	15.2	22.3	1.7
病床規模	診療所	1,400	28.9	21.0	12.5	10.6	7.7	16.6	2.6
	病院　20～199床	979	25.7	9.8	8.1	9.7	21.3	24.6	0.7
	病院　200～499床	463	26.6	6.0	6.5	6.9	21.6	30.9	1.5
	病院　500床以上	147	25.9	4.1	7.5	2.7	25.9	33.3	0.7

２．本稿の目的

本稿では、損害保険会社が提供している「サイバー保険」（付帯・関連サービス含む）が医療機関の実態とニーズ[9]に合致し、医療機関のサイバーセキュリティに役立つ方策となり得るかを把握した。その結果を踏まえ、同保険（付帯・関連サービス含む）の評価について考察した。加えて、医療機関の立場で、保険商品（付帯・関連サービス含む）について改善すべき課題を提示することを目的とした。

３．調査概要

（１）対象と方法

民間の損害保険会社のうち主要な 3 社（A 社、B 社、C 社）のサイバー保険商品（付帯サービス、関連サービス等含む）について、関連書類の分析に加え、3 社へのインタビュー調査を実施した。

（２）調査内容

サイバー攻撃に関して医療現場で想定される事象を、以下の通り、時系列（①～⑪）で整理したうえで、それぞれのフェーズにおけるサイバー保険商品（付帯・関連サービス含む）による対応状況を調査、分析した。

①（平時）予防措置検討
②不正アクセス等のおそれの発生
③不正アクセス等の確定作業
④不正アクセス等の確定に伴う被害発生前の防止作業

---

[9] 脚注 8 に同じ。具体的には次のとおり。
・自施設のサイバーセキュリティ対策のレベルがチェックできる仕組み
・インシデント・アクシデント発生時の相談先
・サイバーセキュリティ対策を学べる場所
・サイバーセキュリティ対策の体制構築を検討する際の相談先
・自施設のサイバーセキュリティ対策を担う人材

⑤不正アクセス等の確定に伴う除去作業
⑥院内医療情報システムへの影響発生等に伴う内部被害の軽減措置
⑦院内医療情報システムへの影響発生等に伴う内部被害の復旧作業
⑧外部への被害拡大（情報漏洩等）に伴う軽減措置
⑨外部への被害拡大（情報漏洩等）に伴う復旧作業
⑩外部での被害発生に伴う賠償関連
⑪事後の再発防止策等
上記に付随して発生する事象
□業務継続
□身代金要求への対応

４．調査結果と分析

保険会社 3 社のサイバー保険の補償内容と付帯・関連サービスについて調査結果を分析し、それぞれの「概要と注目点」および「留意すべき点」を整理した。

3 社が提供するサイバー保険および付帯・関連サービスには、外形的に大きな違いは確認されなかったため、一つにまとめて記載した。全体像は、本稿 12 頁掲載の別表「サイバー保険（付帯・関連サービス含む）のサイバーリスクに係る補償内容」をご覧いただきたい。なお、本稿では保険料水準には触れていない。

（１）サイバー保険の仕組み

サイバー保険では、従来の賠償責任保険で補償される損害に追加して、次の賠償損害や費用損害を補償することができる。

【従来の賠償責任保険（契約）で補償される損害】

院内医療情報システムの所有・使用・管理等に起因する事由により、法律上の損害賠償責任を負担することで被る賠償損害および医療機関に発生する費用損害が補償される。

ただし他人の身体の障害、財物の損壊、紛失等または盗難等に起因する損害は対象外である。サイバー攻撃による場合も対象外であるが、医療機関が使用・管理する磁気ディスク等の紛失・窃取等に起因して発生した他人の情報の漏えいまたはそのおそれについては例外的に補償される。

【サイバー保険（契約）による追加補償】

サイバー攻撃（注１）に起因する他人の身体障害・財物損壊について、医療機関が法律上の損害賠償責任を負担することで被る賠償損害および医療機関に発生する費用損害が、追加補償される。

◆上記比較の概要

原因（事由）と発生した損害の区分		従来の賠償責任保険（契約）	サイバー保険（契約）
院内医療情報システムの所有・使用・管理等に起因する事由	賠償損害	○*	○
	費用損害	○	○
サイバー攻撃による他人の身体の障害、財物の損壊・紛失または盗難等	賠償損害	×*	○
	費用損害	×	○

＊○補償対象、×補償対象外

（注１）「サイバー攻撃」とは
（A 社保険約款「サイバーセキュリティ特約」より）
コンピュータシステムへのアクセスまたはコンピュータシステムの処理、使用もしくは操作に関連する不正な行為または犯罪行為を指し、以下のものを含みます。
①正当な使用権限を有さないものによる、不正アクセス
②コンピュータシステムの権限の停止、阻害、破壊または誤作動を意図的に引き起こす行為
③マルウェア[10]などの不正なソフトウェアの送付または第三者にインストールさせる行為
④コンピュータシステムで管理される電子データの改ざんまたは不正に情報を入手する行為

※本稿において「サイバー攻撃」は、以下「不正アクセス等」（注２）と称する。

（２）サイバー保険で追加補償される内容について

a. 概要と注目点

①自院ネットワークの所有･使用･管理に起因して負担する法律上の損害賠償責任によって被る損害（訴訟対応費用含む）に加え、不正アクセス等(注 2)のおそれが発生した以降の各局面において発生することが想定される次の費用が補償される（12 頁別表参照のこと）。
・不正アクセス等の確定に伴うネットワーク遮断、代替措置手配や原因・被害範囲調査、原因除去にかかる費用
・院内医療情報システムへの影響が発生した場合の内部･外部被害の軽減措置および復旧作業に伴うネットワーク遮断、代替措置、データ復元・サイト復旧、各種システム対応等にかかる費用、見舞金支払いや風評被害拡大防止にかかる費用
・事後の再発防止策にかかる費用
等。

[10] コンピュータウイルスやスパイウェアなど、PC などの端末に不利益をもたらす悪意のあるプログラムやソフトウェアの総称。

(注 2)「不正アクセス等」とは
（B 社保険約款「サイバーセキュリティ事故対応費用担保特約条項」より）
①他者の ID・パスワード等を使用して他者になりすまし、または権限者が設定したファイアウオールを通過することにより、不正にアクセスする行為
②大量のデータを送りつける DoS 攻撃
③不正なプログラムの送付またはインストール
④ネットワーク上で管理されるデータベースに SQL 文を注入し、データベースを改ざんまたは不正に情報を入手する SQL インジェクション
⑤その他①から④までに類似の行為

②不正アクセス等のおそれが発生した段階で行われる「不正アクセス等の確定作業」にかかる費用が補償される。また一定の条件下(注 3)では、確定作業の結果、不正アクセス等がなかったことが判明した場合でも同費用は補償される。

(注 3)確定作業の結果、不正アクセス等が無かったことが判明した場合でも同作業に要した費用が担保される「一定の条件」とは
（C 社保険約款「サイバー保険特約条項」より）
①「*公的機関からの通報」又は「*公的機関への届出」
*公的機関；サイバーインシデント(注 4)に関する被害の届出および情報の受付等を行っている独立行政法人または一般社団法人を含みます。
②被保険者のコンピュータシステムのセキュリティ運用管理を委託している会社等からの「通報」又は「報告」

※保険会社によっては上記枠内①②について、「通報」に限定し、「届出」や「報告」を除外している。

(注 4)「サイバーインシデント」とは
①被保険者のコンピュータシステム上の電子データまたはソフトウェアの盗難、改ざんまたは破壊
②被保険者のコンピュータシステムに対する不正なアクセスおよび使用等
③被保険者のコンピュータシステムに対する Dos 攻撃またはそのアクセスの制限もしくは禁止
④第三者のコンピュータシステムに対する Dos 攻撃への被保険者のコンピュータシステムの参加
⑤被保険者のコンピュータシステムへの、または被保険者のコンピュータシステムから第三者のコンピュータシステムへの悪意のあるコードの送信
⑥その他①から⑤に類似する行為

③業務継続費用を補償対象とすることが可能である。

b. 留意すべき点

①不正アクセス等のおそれが発生し「不正アクセス等の確定作業」を行ったが、結果として不正アクセス等が無かったことが判明したケースでは、確定作業に要した費用が補償される場合が限定されている。

②サイバーセキュリティ対策に関し、保険申込時の告知内容に基づき一定のリスク評価を行い、その結果に連動して保険料を一定の幅で割り引く仕組みはあるが、医療機関専用に用意された告知内容やリスク評価方法ではない。

③ランサムウェア[11]感染等も同保険にいう「不正アクセス等」に該当するので、これに起因して発生する賠償損害や費用損害は同保険で補償されるが、身代金の要求に応じて支払った場合に、医療機関に発生する身代金相当の費用損害については、補償対象外とされている。

（３）付帯・関連サービスについて

a. 概要と注目点

①サイバー保険契約者専用の緊急時対応窓口があり、不正アクセス等のおそれやネット接続不具合などのトラブルが発生した時点で無償利用できるサービスがある。

②サイバーリスク評価サービスや標的型攻撃メール訓練サービスといった平時からリスクに備えるためのコンサルティングサービス（前者は原則として無償、後者は原則として有償）がある。

③不正アクセス等発生時の緊急対応や事後の再発防止、信頼回復等を支援する各種コンサルティング業者に繋ぐサービスがある。専門業者との提携による有償サービスとなるが、同費用はサイバー保険の補償範囲で補填される。

---

11 「ランサム（Ransom＝身代金）」と「ウェア（Software）」を繋げた造語で、ソフトウェアを悪用し、データの身代金を要求するマルウェア（コンピュータに悪事を働くソフトやコードの総称）のこと。

b. 留意すべき点

①緊急時対応窓口は音声応答のみで、画像通信ができない。また利用できる日時に各社それぞれ制限がある。

②各種対応サービスやコンサルティングサービスにおいて、医療機関に特化したノウハウが蓄積されていない可能性がある。

③専門業者との提携による各種コンサルティングサービス（有償）を利用する場合、一旦、医療機関がサービス費用を支払った後、サイバー保険の保険金を請求し、補償される範囲の保険金を受け取る手続きとなる。サイバー保険の契約内容によっては、サービス費用の全額を保険金で受け取れるとは限らないので、サービス利用に当たり補償範囲を確認することが望ましい。

別表「サイバー保険（付帯・関連サービス含む）のサイバーリスクに係る補償内容」

	事象	保険の補償対象	付帯・関連サービス	備考
①	(平時) 予防措置検討	―	■サイバーリスク診断 ■標的型攻撃メール訓練	
②	不正アクセス等のおそれの発生	―	■緊急時窓口対応（不正アクセス等の有無にかかわらず無償で利用可）	■音声対応のみで画像通信なし。利用できる日時に各社制限あり。
③	不正アクセス等の確定作業	○（不正アクセス等確定作業）	■緊急時窓口対応による初期アドバイス	○確定作業の結果、不正アクセス等が無かった場合でも、一定条件では作業に要した費用が補償される。
④	不正アクセス等の確定に伴う被害発生前の防止作業	○（ネットワーク遮断、代替措置）	■緊急時窓口対応によるセキュリティ診断等	
⑤	不正アクセス等の確定に伴う除去作業	○（原因・被害範囲調査、原因除去）	■緊急時窓口対応によるウイルス駆除等	
⑥	院内システムへの影響発生等に伴う内部被害の軽減措置	○（ネットワーク遮断、代替措置）	■左記 6～11 支援コンサルティングサービス（有償）	保険会社と提携する外部専門業者により提供される。
⑦	院内システムへの影響発生等に伴う内部被害の復旧作業	○（データ復元・サイト復旧）		
⑧	外部への被害拡大（情報漏洩等）に伴う軽減措置	○（各種システム対応等）		
⑨	外部への被害拡大（情報漏洩等）に伴う復旧作業	○（見舞金支払いや、風評被害拡大防止含む）		
⑩	外部での被害発生に伴う賠償関連	◎（自院ネットワークの所有･使用･管理に起因して負担する法律上の損害賠償責任によって被る損害）＋ ○（訴訟対応費用）	■争訟対応	
⑪	事後の再発防止策等	○		
□	業務継続	○（継続費用）		
□	身代金要求への対応	×（身代金支払い費用）		ランサムウェアに起因し発生する左記以外の損害は補償対象である。

○・・・費用損害を補償　◎・・・賠償損害を補償　×・・・保険補償対象外
■・・・具体的な付帯・関連サービス

５．考察

保険会社が提供するサイバー保険および付帯・関連サービスは、以下（１）（２）の通り、医療機関のニーズ[12]を一定程度満たす枠組みであると評価できる。

医療機関のサイバーセキュリティ対策に関する取組の遅れを取り戻すための方策として、これらを医療機関に対して周知し活用することが、有望な選択肢となる可能性があると考える。医療界のニーズに応えるため、医療機器・システムベンダーやIT業界、その他の産業界を挙げての協力が求められる中で、保険業界はその機能の提供者として、今後とも有望な候補の一つと言えるのではなかろうか。

他方で、その前提として同保険には改善すべき課題がある。例えば、各保険会社のサイバー保険の説明書や案内書には、厚生労働省が策定した「医療情報システムの安全管理ガイドライン（5.1版）」[13]への言及が見られない。同ガイドラインは医療機関が医療情報システムの管理等を行うに際して最優先で参考にするものであり、保険会社にも同ガイドラインを踏まえた組み立てが望まれる。また現行の保険内容（付帯・関連サービス含む）にも、医療界のニーズを踏まえた一層のカスタマイズが期待される。具体的に改善の検討が望まれる点を、以下（３）に提示する。

（１）サイバー保険で追加補償される事由の評価

各社とも同保険では、同様に以下の項目（12頁別表③～⑪）等に係る各種費用を幅広く補償することが可能な点を評価できる[14]。

・不正アクセス等のおそれの発生に伴う同確定作業
・不正アクセス等の確定に伴う被害発生前の防止作業および除去作業
・院内医療情報システムへの影響の発生等に伴う内部被害の軽減措置および復旧作業
・外部への被害拡大（情報漏洩等）に伴う軽減措置および復旧作業
・外部での被害発生に伴う賠償関連
・事後の再発防止策
等

---

[12] 本稿4頁資料2および脚注8参照。
[13] 厚生労働省（2020）。
[14] ランサムウェア感染等で身代金を要求され支払ったことにより、医療機関に発生した身代金相当の費用損害については、補償対象外とされている。本稿10頁(2)ｂ③参照のこと。

（２）サイバー保険の付帯・関連サービスへの評価

医療機関は、サイバーリスクに備える体制をどうしたらよいか分からないながらも、何かしら対策が必要でないかという漠然とした不安を抱え、これを解消したいというニーズがある。

一方で保険会社が提供する付帯・関連サービスは、「リスクマネジメントに立脚し、リスク度合いの評価、これを踏まえたリスクの事前（平時）の低減策、インシデントにより発生する内外の被害軽減策提示までを、自社あるいはそれぞれの局面に応じたコンサルティングノウハウを有する専門業者に繋ぐことで担う」ものである。インシデント・アクシデント発生時の対応策やサイバーセキュリティ体制構築を検討する際の相談先としての機能の提供に加え、サイバーセキュリティ対策を学べる場所の提供や人材育成にも資することで、医療機関のニーズを満たすことが期待されると評価する。

例えば、医療機関の院内医療情報システムでも何らかの不具合は日常的に発生しており、2021 調査結果からも窺われたように、当不具合がサイバー事故によるものかどうかも分からない初期段階から相談先に対するニーズが極めて高い。筆者見解によれば、従前は多くの場合、当該医療機器やシステムのベンダーがこれに対応し解決する機能を果たしてきた。しかしながら今後、院内医療情報システムが相互接続するようになると、原因箇所の特定が困難となり、今まで果たしてきたベンダー個社での対応も困難となることが予測される。医療界は極めて危うい環境に置かれていると言える。

そこで、各保険会社がそれぞれ提供する院内医療情報システム相談窓口サービスは、不正アクセス等のおそれやネット接続不具合などのトラブルまで対応できるため、特に診療所や中小規模の病院でシステム部門や専任担当者のいない医療機関においては、このような事態への受け皿となることが期待される。

（３）改善が望まれる点

(3)-1. 補償について

①厚生労働省「セルフチェックシート」の活用

保険料を当該医療機関のサイバーリスクの度合いに連動させる仕組みが各保険会社で採用されているが、各社が独自に作成したチェックシートで評価を行っ

ている現状にある。

これを、公的なチェックシートを活用して評価する方式に統一することが望ましい。具体的には、医療機関が自らリスク判定する目的で厚生労働省が策定した「セルフチェックシート」[15]の活用が考えられる。

②不正アクセス等調査費用の補償条件の緩和

不正アクセス等のおそれを発見し、その確定作業を実施した結果、不正アクセス等が生じていなかった場合、当作業費用が補償されるためには一定の条件を満たす必要があるとされている。

これを、なるべく当条件が限定されないように緩和することが望ましい。条件の厳しさによっては、初期段階での対応に逡巡し事態の悪化を招きかねないと考えられる。

③魅力ある補償金額・保険料水準の実現

前述の通り、本稿では保険料水準には触れないが、具体的な保険設計においては、医療機関にとって魅力ある補償金額および保険料水準に設定することにも配慮が必要である。

一旦事故が発生してから必要となる各種費用は相当の金額となることが想定される。同保険の補償事由そのものは①のとおり手厚いとしても、当該費用が十分に賄える補償金額で、かつ現実的な保険料水準でなければ医療機関にとって魅力に乏しく、加入に至ることは難しいと思われる。

(3)-2. 付帯・関連サービスについて

① 緊急時対応窓口サービスの拡充

緊急時対応窓口サービスへのニーズは極めて高いと考えられ、音声応答に加え画像通信による対応や、利用できる日時の拡大等による利便性の向上が望まれる。

②医療機関向けノウハウのさらなる蓄積

以下のサービス機能に関し、医療機関の独自性を踏まえたノウハウがどの程度蓄積されているか定かでない。保険業界および提携する専門業界の知見をさら

[15] 「医療機関のサイバーセキュリティ対策チェックリスト」：厚生労働省（2020）の別添資料。2021 調査において、サイバーセキュリティ体制構築にあたって最も優先度が高い要望」に挙げられた「自院のサイバーセキュリティ対策のレベルがチェックできる仕組み」に応えるものとして活用が期待される。

に高めることが望まれる。

・平時の予防措置を兼ねて、当該医療機関のシステムのサイバーリスクの度合いを個別かつ適正に評価する機能。前掲の「セルフチェックシート」[16]の活用も課題として挙げられる。
・院内医療情報システムの不具合発生時の相談窓口サービス、不正アクセス等（そのおそれを含む）発生時に緊急対応を実施するに当たってのコンサルティング機能、再発防止策を講じるに当たってのコンサルティング機能等。一連の対応について、厚生労働省が策定した障害発生時の対応フローチャート[17]を踏まえた仕組みづくりが課題として挙げられる。
・特にランサムウェアへの対応コンサルティング機能。身代金を支払わずに被害を最小限に抑えるための高度なコンサルティングが期待される。

③行政届出への関与

保険あるいは付帯・関連サービスの一環として、不正アクセス等を検知した場合の行政への届出[18]に保険会社が関与し、支援する仕組みが望まれる。行政への速やかな届出を後押しする効果も期待できる。

④ＩＰＡとの連携

各種コンサルティング業者との提携と並行して、「独立行政法人情報処理推進機構（ＩＰＡ）情報セキュリティ安心相談窓口」[19]との連携も検討課題である。

⑤コンサルティング費用の保険会社からの直接払い

有償サービスについて、コンサルティング業者に支払う費用は、一旦医療機関が立て替え、後追いで保険金として補填される仕組みとされているのを、保険会社からコンサルティング業者への直接払いとすることが望まれる。

---

16 脚注 15 に同じ。
17 「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」：厚生労働省（2020）の別添資料。
18 厚生労働省 医政局 研究開発推進課 医療情報技術推進室が行政窓口。厚生労働省（2020）参照。
19 厚生労働省（2020）でマルウェアや不正アクセスに関する技術的な相談窓口として紹介されている。

【参考文献・資料】

●一般社団法人 日本損害保険協会「サイバー保険とは ｜ サイバー保険 ｜ 日本損害保険協会（sonpo.or.jp）」
https://www.sonpo.or.jp/cyber-hoken/about/

●厚生労働省（2020）「医療情報システムの安全管理ガイドライン（5.1 版）：医政局 研究開発振興課 医療情報技術推進室」（2021 年 1 月）
https://www.mhlw.go.jp/stf/shingi2/0000166275.html

●同上・別添資料「医療機関のサイバーセキュリティ対策チェックリスト」（2021 年 10 月 20 日）
https://www.ajha.or.jp/mail_tmp/211021/211021_4.pdf

●同上・別添資料「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」（2021 年 10 月 20 日）
https://www.mhlw.go.jp/content/10808000/000844700.xlsx

●坂口・堤（2021）日医総研ワーキングペーパーNo.453「病院・診療所のサイバーセキュリティ：医療機関の情報システムの管理体制に関する実態調査から」（2021 年 4 月 27 日）
https://www.jmari.med.or.jp/research/research/wr_734.html

●独立行政法人情報処理推進機構 セキュリティセンター（2021）「コンピュータウイルス・ 不正アクセスの届出事例［2021 年上半期（1 月～6 月）］」（2021 年 8 月 23 日）
https://www.ipa.go.jp/files/000093083.pdf

【巻末資料１】医療機関のサイバーセキュリティ対策チェックリスト
（厚生労働省「医療情報システムの安全管理ガイドライン 5.1 版」別添資料）

【巻末資料２】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
（厚生労働省「医療情報システムの安全管理ガイドライン 5.1 版」別添資料）