



2026年2月版

# 『医療機関用サイバー保険』の ご案内

2026年●●月●●日

損害保険ジャパン株式会社

代理店 有限会社ミック三重

拝啓 時下ますますご清栄のこととお慶び申し上げます。  
平素は、格別のご高配を賜り、ありがとうございます。

さて、昨今医療施設におけるインフラについてもインターネットによる外部環境と繋がることが一般化しており、医療施設のみなさまにおかれましても、安全かつ安定したシステム、ネットワークの管理および提供や情報セキュリティの確保が求められています。また、ウイルスやハッキングによるサイバー攻撃により電子データの損壊や情報漏えいに関する被害、システム・ネットワークの不具合による経済的被害は拡大しており、直近においては病院を中心として地域を問わず各地においてマルウェア被害などの報道事例が増えており、その対応に高額な費用を要する事態が判明しております。

このたび、医療施設の皆さまの情報システムおよびネットワークに関する有効なリスクマネジメントの1つとして、電子カルテなどの電子データの損壊、情報漏えいおよびネットワークの使用不能などのサイバーセキュリティ事故により第三者から損害賠償を請求された場合やその際の各種対応費用などに備える包括的な保険として、『医療機関用サイバー保険』をご案内いたします。

何卒ご高覧のうえ、ご採用賜りますようお願い申し上げます。  
末筆ながら、貴院の益々のご繁栄をお祈り申し上げます。

敬具

# 1. 医療施設におけるICT化とサイバーリスク

## 医療施設とサイバーリスク

- オンライン資格確認や電子カルテの普及など、医療業界のICT化が進む中、情報技術の進化とともに、医療施設におけるコンピュータシステムへの依存度は高まる一方であり、**システムの利用なくして医療施設の経営は成り立ち得ない環境にある**といえます。
- ネットワークの遮断やシステムの誤作動、または情報メディアのコンテンツ誤りや誤作動などが生じた場合の**第三者からの賠償リスク、個人情報や機密情報を漏えいしてしまうリスク、事業停止による利益喪失リスク**などは医療施設における重大な基幹リスクの一つです。

## サイバーリスクのキーワード

- 1 PC、インターネット、情報メディアの利用なくしては存続し得ない企業のオペレーション
- 2 ボードレスで繋がるネットワーク（被害または損失の際限ない拡散リスク）
- 3 システムの停止または誤作動による業務の停止や情報漏えいが招く巨額の損失リスク



厚生労働省の「**医療情報システムの安全管理に関するガイドライン**」においても、**医療情報の適切な取扱いなどの具体的な対策が求められています。**

リスクの  
発見および確認

リスクの  
分析および評価

リスク処理  
方法検討

リスクコントロールおよび  
リスクファイナンスング  
実施

## 2. サイバー・情報セキュリティに関連した事故①

### 情報セキュリティ10大脅威

- 近時のサイバー攻撃の手法として「標的型攻撃」「ランサムウェア」「ビジネスメール詐欺」などの手法が上位を占めています。
  - これらの攻撃は情報の窃取や直接的な金銭要求など、金銭目的の攻撃であり、あらゆる企業が標的となるリスクがあります。
- (注) これらの攻撃による被害や損失の全部または一部については、医療機関用サイバー保険では補償の対象とならないことがあります。

2025年順位	内容	10大脅威での取り扱い (2016年以降)
1位	ランサムウェアによる被害	10年連続10回目
2位	サブライチエーションや委託先を狙った攻撃	7年連続7回目
3位	システムの脆弱性を突いた攻撃	5年連続8回目
4位	内部不正による情報漏えい	10年連続10回目
5位	機密情報等を狙った標的型攻撃	10年連続10回目
6位	リモートワーク等の環境や仕組みを狙った攻撃	5年連続5回目
7位	地政学的リスクに起因するサイバー攻撃	初選出
8位	分散型サービス妨害攻撃 (DDoS攻撃)	5年ぶり6回目
9位	ビジネスメール詐欺	8年連続8回目
10位	不注意による情報漏えい等	7年連続8回目

出典：独立行政法人情報処理推進機構「技術本部セキュリティセンター 情報セキュリティ10大脅威2025」



#### 近時のサイバー攻撃の目的および手法

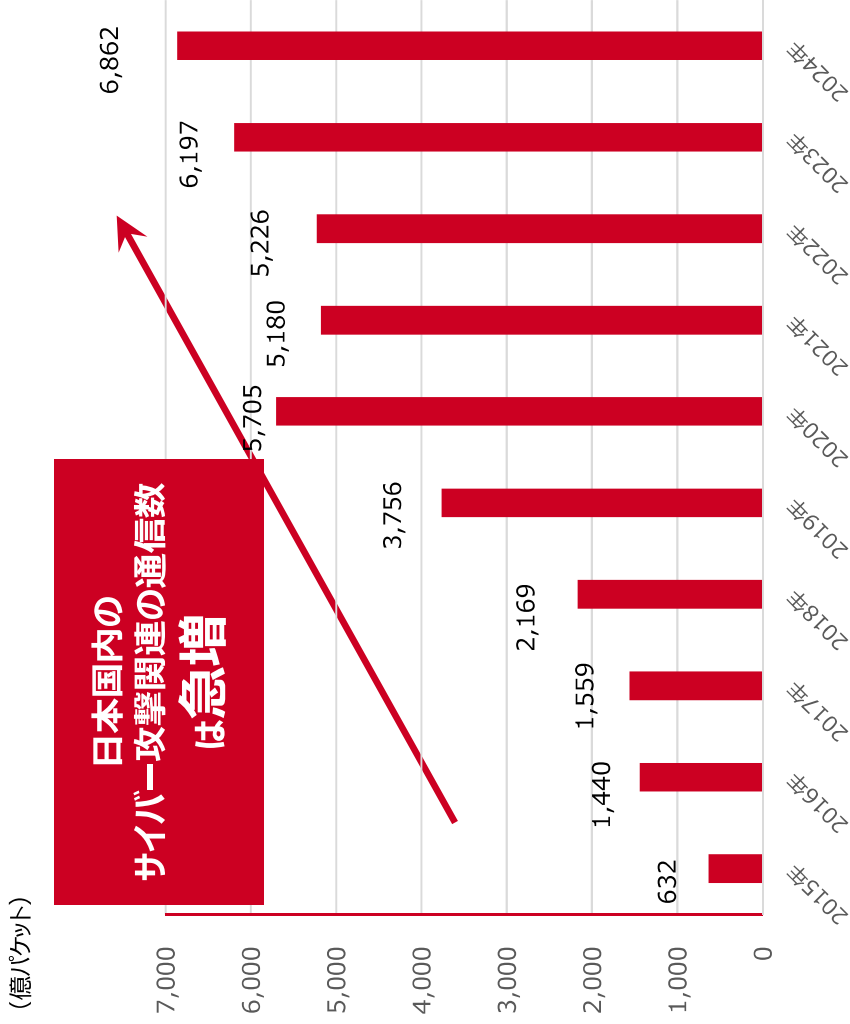
- サイバー攻撃の目的は従来型の「嫌がらせ」や「いたづら」を目的としたものから、「金銭目的」へとシフトしていると言われています。
- 攻撃手法も高度化しており、「ウイルス対策ソフトでは検知できない」「組織内のメールに偽装する」などの手法が横行し、より目立たない手法で、悪質な攻撃を仕掛けるものが主流となっています。
- サブライチエーションの弱点を悪用した攻撃が増えており、企業における情報セキュリティ対策の重要性はより高まっています。

## 2. サイバー・情報セキュリティに関連した事故②

### サイバー攻撃による被害動向

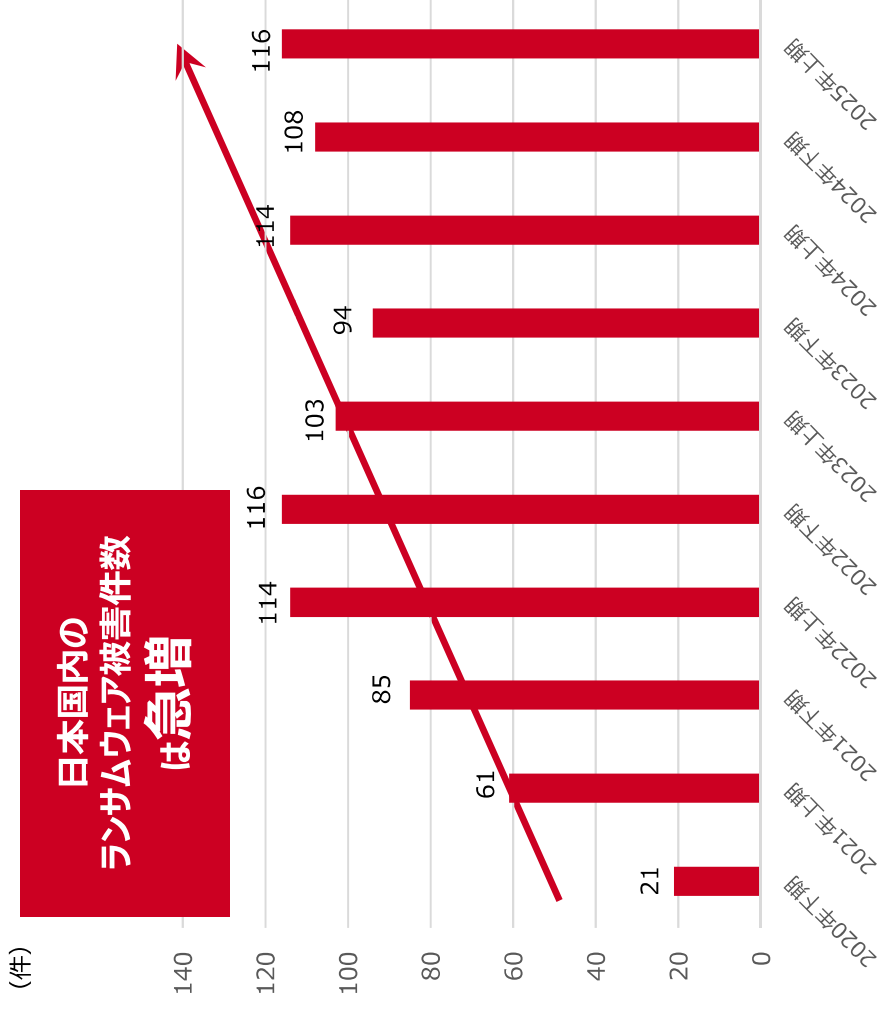
- 近年のDXなどの推進に伴い、日系企業がサイバー攻撃の標的になる危険性は高まっています。
- 近年では、IoT機器を標的とするサイバー攻撃も著しく活発化しており、情報社会の進展に伴うサイバー攻撃の件数は増加の一途をたどっています。また、社会の情報システム依存度の高まりに比例するかのよう、近年の被害件数は急激に増加しています。

サイバー攻撃関連の通信数の推移（年間件数）



出典：「情報通信研究機構『NICTER観測レポート2024』

ランサムウェア被害報告件数（半期件数）



## 2. サイバー・情報セキュリティに関連した事故③

### 病院におけるサイバー被害の事例

- 外部からの不正アクセスやマルウェア感染などにより、Webサイトや制御システムが停止したり、大量の顧客情報が流出するなどの被害も発生しています。
- 2021年から2022年にかけて医療施設におけるサイバー被害の事例が急激に増えていきます。またそれに伴い、システム復旧の費用が高額化することが判明しています。

時期	医療施設	概要	影響
2021年	病院	ランサムウェアにより、病院内のシステムが使えなくなり、約2か月間通常診療が行えなくなった。	新システムへ替えに相当額のコストを要したほか、システム復旧期間の診療報酬請求に大きな影響が出た。
2021年	病院	病院に勤務する医師がクラウドサービスのアカウントのパスワードを窃取され、不正アクセスを受けた。	医師のPCには患者さんの個人情報が入力されているため、個人情報が流出したおそれがある。
2022年	病院	職員がランサムウェアに感染している状態を発見した。	院内のPCが使用不可になり、診療に影響が発生した。また、新システムに入れ替えるため、約7000万円の費用を要した。
2022年	病院	外部からの不正アクセス被害により、院内の電子カルテが一時使用できなくなり、患者さんおよび職員の個人情報が流出した可能性が発生した。	患者さんおよび職員の個人情報の個人情報が約11万件流出したおそれがある。
2024年	病院	ランサムウェアにより、電子カルテを含む総合情報システムに障害が発生した。	患者さんの個人情報約4万件と会議の議事録等が流出したおそれがある。

(注)上記事例は報道内容をもとに記載しています。また、影響の内容によっては、医療機関用サイバー保険では補償の対象とならない場合があります。

### 3. 『医療機関用サイバー保険』の特長

#### 緊急時の対応を総合的にサポートする保険

『医療機関用サイバー保険』の特長は次のとおりです。

- サイバーリスクに起因する事故によって生じる賠償責任および事故発生時の各種対応費用および自院の利益損失を包括して補償可能
- ご契約に自動セットのサービスを通じて緊急時における総合的なサポートによる大きな安心を提供

#### 賠償責任、事故発生時の各種対応費用および自社の利益損害を包括的に補償

- サイバー攻撃や情報セキュリティなどに起因する事故が発生した場合における「賠償責任」「事故対応に要する諸費用」「自院の逸失利益や営業継続に要する費用（オプション補償）」を総合的に補償する保険です。

#### 事故の初動から再発防止までに要する費用をトータルで補償

- サイバー攻撃や情報セキュリティなどに起因する事故が発生した場合における「初動対応→原因調査→被害抑制→事態収拾→再発防止」までの対応に要する費用をトータルで補償します。

#### 事故発生のおそれに対応する費用も補償

- サイバー攻撃のおそれが発生した場合において、これらの発生の有無を調査するために要した費用も補償します。（外部からの通報などによりサイバー攻撃のおそれが見られた場合に限りです。）

#### 緊急時の対応サポートを自動セットのサービスでご提供




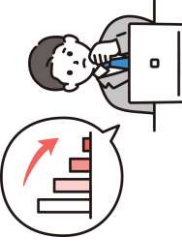
- 医療機関用サイバー保険には、情報漏えいや不正アクセスなどのサイバーセキュリティ事故の発生に伴う各種の緊急対応を総合的にサポートするサービスが自動でセットされています。

# 4. 『医療機関用サイバー保険』の概要①

## (1) 商品構成

- 医療機関用サイバー保険では、次のそれぞれの事由に対して3つの損害を包括して補償します。
- サイバー攻撃や情報セキュリティなどに起因する事故はボードレスのため、**全世界で発生した事故**や損害賠償請求が補償対象です。

### サイバー保険の構成

サイバー保険の構成	
<b>賠償責任</b> 下表記載の対象事由①～④の発生に起因して他人に損害を与えた場合の賠償責任および争訟費用の補償 	<b>事故発生時の各種対応費用</b> 下表記載の対象事由①～④の発生に起因して生じる「事故の調査」から「解決/再発防止」までの諸費用の補償 
<b>他人の損害</b> 	<b>利益・営業継続費用 オプション</b> 下表記載の対象事由③または④に起因したネットワークの中断などによる喪失利益や営業継続のための費用の補償 

### 対象事由

### 概要

①情報漏えいおよびそのおそれ※	貴院（被保険者）の業務における情報漏えいおよびそのおそれ
②デジタルコンテンツ不当事由※	デジタルコンテンツの使用の結果生じた名誉棄損、プライバシー侵害、著作権、商標権または意匠権の侵害など
③サイバー攻撃	貴院（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や処理、操作、犯罪行為など
④①～③以外のその他の業務	上記①～③以外の貴院（被保険者）の業務の一環としてのシステムの所有、使用または管理などに起因する偶然な事由

# 4. 『医療機関用サイバー保険』の概要②

## (2) 事故発生時の各種対応費用の詳細

### 事故対応特別費用

原因調査から事態収拾まで、サイバー事故の対応にあたり必要となる諸費用を幅広く補償

調査/対応/事態収拾/復旧/再発防止

#### 【対応例】

- 調査：事故原因調査および影響調査
- 事態収拾：会見、マスコミ対応およびコールセンター設置
- 復旧：データ復旧および情報機器復旧
- 再発防止：コンサルティング

### 情報漏えい対応費用

情報漏えいまたはそのおそれ起因して貴院（被保険者）が支出した諸費用を補償

見舞金・見舞品/モニタリング

#### 【対応例】

- 上記の事故対応特別費用
- 被害者への見舞金または見舞品
- 情報漏えいのモニタリング

### サイバー攻撃対応費用

サイバー攻撃またはそのおそれ起因して貴院（被保険者）が支出した諸費用を補償

初動/早期発見・早期復旧

#### 【対応例】

- サイバー攻撃発生の有無の確認のための外部委託費用
- ネットワークの遮断のための外部委託費用
- 弁護士などの外部の専門家への相談費用

### 法令等対応費用

情報漏えいまたはサイバー攻撃によって、公的機関の調査が行われた場合に、貴院（被保険者）が支出した諸費用を補償

相談・調査

#### 【対応例】

- 弁護士またはコンサルタントなどの専門家への相談費用
- 報告書などの文書作成費用、公的機関への報告にかかる費用
- 証拠収集費用および翻訳費用

欧州GDPRおよび改正個人情報保護法に対応!



### サイバー保険の緊急時対応機能

- 情報漏えい、ネットワークの中断、データまたはプログラムの損壊による事故発生の場合、事故の早期発見および早期対応が極めて重要であり、対応の遅れは被害の拡大を招きます。
- 事故発生時には「緊急時サポート総合サービス」を活用することで、損保ジャパンを通じて必要な業者を手配することが可能です。お客さまの有事における負担の軽減を図ることができます。

## 4. 『医療機関用サイバー保険』の概要③

サイバー攻撃や情報セキュリティなどに起因する事故が発生した場合には、各種対応のためにさまざまな費用が発生します。加えて損害賠償金の支出や喪失利益が発生する可能性があります。医療機関用サイバー保険では、これらの損害を包括的に補償します。

### 【事故例】 電子カルテのサーバに外部から不正アクセスの可能性があることが判明した場合

主な対応事項	主な対応内容	損害額（例）
原因究明	外部の調査専門会社（セキュリティベンダー）に発生原因の究明と漏えいの可能性があるデータ範囲の特定を依頼するために、サーバ3台の調査を委託した。セキュリティベンダーの調査の結果、約3万人の患者さんの個人情報に対し、外部から不正にアクセスされた可能性があることが判明した。	約300万円
謝罪 および 広報対応	弁護士と相談のうえで、被害者への謝罪と報告文書送付、関係機関への報告、社外公表文書（WEB公表）などを作成した。 セキュリティベンダーによる調査結果から判断した外部に漏えいまたはそのおそれの可能性がある約3万人に、漏えいの経緯の説明を兼ねたお詫び状を郵送した。	約50万円
コールセンターの 設置	その後、お詫びの品を発送した（1人500円の商品券＋郵送料）。	約1,800万円
コンサルタント委託	外部に公表した時点で、既存の問い合わせ窓口では対応できなくなると想定し、新たに専用の問い合わせ窓口を設置した。 （10ブース・2週間程度、5ブース・2週間程度） 危機管理コンサルタント（外部）の支援を受けながら、現状把握および今後の対応方針の検討などを行う対策会議（3回）を実施した。	約500万円
		約200万円

（注）上記費用はすべて医療機関用サイバー保険の「事故発生時の各種対応費用」の補償で保険金のお支払対象になります。



損害賠償	医療施設が保有する個人情報にはセンシティブな情報や金融情報などが含まれる可能性があるため、損害賠償額が高額になる可能性があります。
喪失利益・営業継続費用 （オプションセットの場合）	システム停止の原因となった感染したウイルス次第では復旧までに時間を要することとなり、その間営業を停止せざるを得なくなる可能性があります。また、営業を継続させるための緊急対応に追加費用が発生することもあります。

（注）上記費用は医療機関用サイバー保険の「賠償責任」、「利益・営業継続費用」の補償で保険金のお支払対象になります。

## 4. 『医療機関用サイバー保険』の概要④

### 利益・営業継続費用オプション

- 本オプションのセットにより、サイバー攻撃などにより、自院システムが中断または停止し、業務が中断したことに伴う利益減少、自院の利益減少を抑えるための費用、営業を継続するための費用を補償します。

#### 喪失利益

サイバー攻撃などに起因するシステム停止によって営業が休止または阻害されて生じた損失のうち、営業の休止または阻害がなければ得ることができた営業利益および経常費を補償。

#### 収益減少防止費用

営業収益の減少を防止または軽減するために必要かつ有益な費用のうち通常要する費用を超える次の費用を補償。  
(サイバー攻撃などの実行者に支払う身代金は含みません。)

- 収益減少防止費用
- サイバー攻撃などによる影響が消滅し回復するまでの期間に支出した費用  
(費用の支出によって減少することを免れた営業収益に利益率を乗じた額が限度)
- 営業継続費用  
システムの機能が復旧するまでの期間に支出した費用  
(期間内に支出を免れた費用や収益減少防止費用の額を控除します)

#### 営業継続費用



- サイバー保険の利益補償条項・営業継続費用補償条項で補償の対象となるのは、ネットワーク中断が発生した場合に限ります。
- 情報漏えいや情報メディアの提供に起因して生じた事故による利益喪失・営業継続費用損失は補償の対象にはなりません。
- また、ネットワーク中断を伴わないランサムウェアなどの脅迫行為に起因して発生した利益損失についても補償の対象には含まれません。
- ネットワークの中断は工場での製造の中断や取引先および顧客からの受発注の阻害などによる利益喪失を招くリスクであり、被害の拡散や中断時間の長期化が発生すると、巨額の損失を招く可能性があります。オプションのセットをオススメいたします。

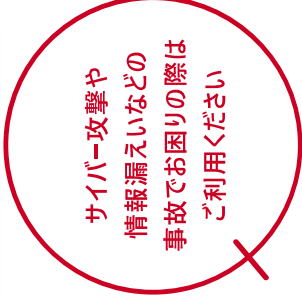
### 自主的停止による利益担保オプション

- 本オプションのセットにより、利益・営業継続費用オプションでは補償対象外となる、被害拡大防止のための調査や早期復旧などのために自院システムを自主的に停止したことに伴う、自院の喪失利益と収益減少防止費用および営業継続費用を補償します。

# 4. 『医療機関用サイバー保険』の概要⑤

## (3) 緊急時サポート総合サービスの仕組み

サイバー攻撃や情報漏えいなどによって、当該事故の原因調査や事故の公表、被害者への謝罪等の対応をしなければならぬ緊急時に、一連の対応をワンストップかつ総合的に支援するサービスです。サイバー保険に加入すると、情報漏えいまたはそのおそれが生じた場合に、必要な各種機能を備えた本サービスをご利用いただけます。



**特長**

# 1

### 緊急時の対応をワンストップで支援

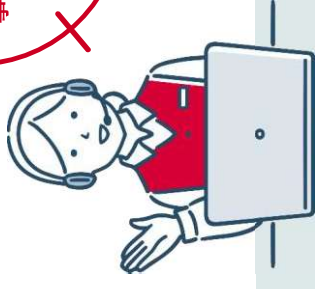
サイバーセキュリティ事業を行うSOMPOLリスクマネジメント㈱が緊急時対応をコーディネート

**特長**

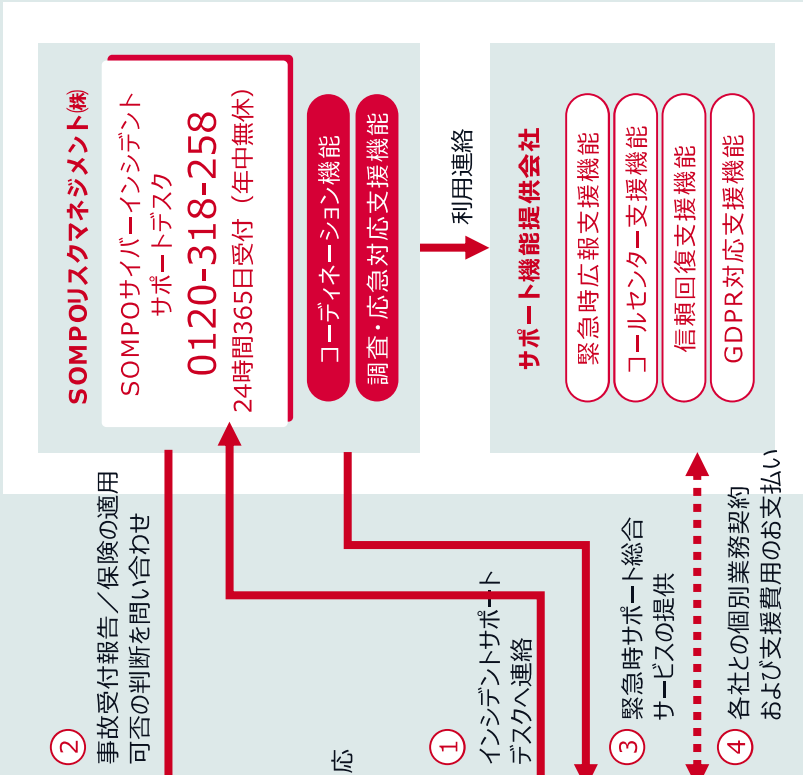
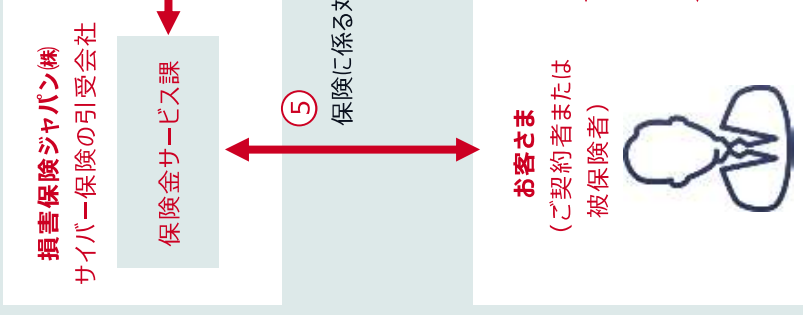
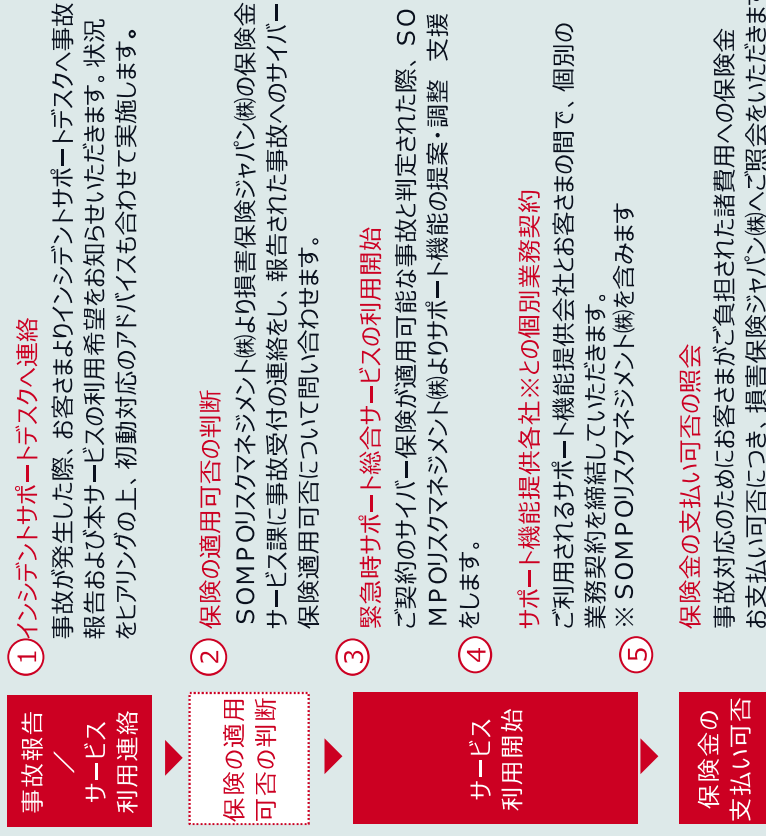
# 2

### 最適なサポート機能を提案

事故の状況やお客さまのニーズに合わせて、最適なサポート機能を提案し、確実な緊急対応を実現



## ご利用の流れ



本サービスのご提供サービスにつきましては保険金の支払対象外となる場合があります。支払い可否については担当保険金サービス課へご確認ください。

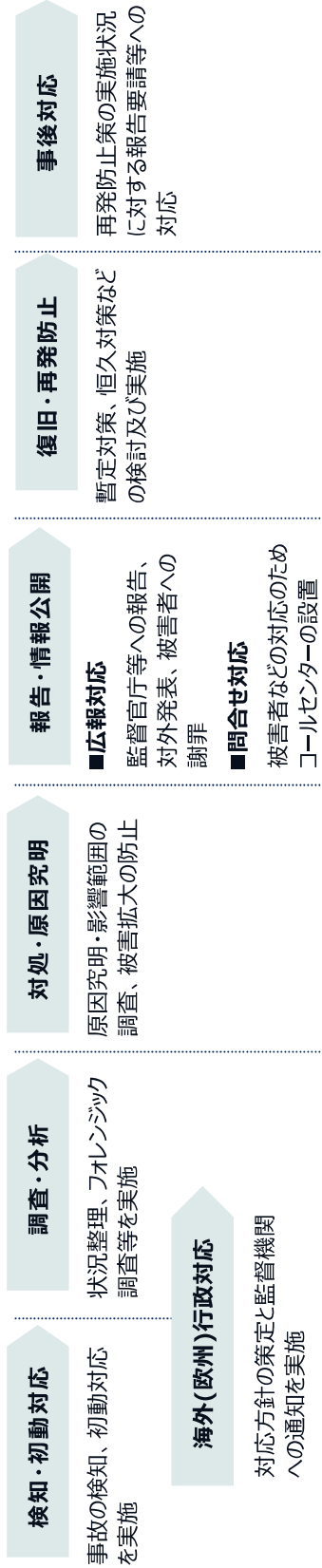
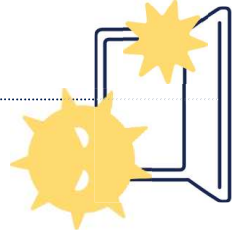
# 4. 『医療機関用サイバー保険』の概要⑤

## ■ サービスの概要

SOMPOリスクマネジメント(株)が事故対応に関する必要なサポート機能をコーディネートし、提携する専門事業者のサービスを通じて、緊急時におけるお客さまの被害拡散防止・早期復旧等を支援します。(サービスの適用地域は、日本国内に限られます)

### サイバー事故等による情報漏えいが発生した場合の対応〔例〕

サイバー攻撃の発生  
(情報漏えいのおそれ)



このような緊急時に、お客さまのニーズに合った以下サポート機能をご利用いただけます

主なサポート機能	概要	サポート機能提供会社
■ コーディネーション機能	● 必要となる各種サポート機能の調整 ● 事故対応窓口との連携・アドバイス etc	SOMPOリスクマネジメント(株)
■ 調査・応急対応支援機能	● 事故内容の精査 ● 原因究明・影響範囲調査支援 ● 被害拡大防止アドバイス etc	SOMPOリスクマネジメント(株) / (株)ラック
■ 緊急時広報支援機能	● 記者会見実施支援 ● 報道発表資料のチェックや助言 ● 新聞社告支援 etc	プラップコンサルティング(株)
■ コールセンター支援機能	● 事故に関し信用を毀損するSNS投稿等への対応支援 ● WEBモニタリング・緊急通知 etc	(株)エルテス
■ 信頼回復支援機能	● コールセンター立上げ ● コールセンター運用 ● コールセンターのグローピング支援 etc	(株)ベルシステム24
■ GDPR対応支援機能	● 再発防止策の実施状況等について報告書を発行 etc	(一財) 日本品質保証機構 / BSIグループジャパン(株)
	● GDPR対応に要する対応方針決定支援 ● 監督機関への通知支援 ● 協力弁護士事務所との紹介 etc (株)インターネットイニシアティブ	

(注1)本サービスは、サイバー保険で保険金がお支払いできる場合にご利用いただけるサービスです。

(注2)各サポート機能提供会社にお支払いいただく諸費用は、サイバー保険でご契約している保険金額を上限に保険会社から保険金として貴社へ支払われます。

なお、諸費用は保険金の支払い対象外となる場合があります。支払い可否については担当保険金サービス課へご確認ください。

(注3)本サービスは、ご利用を希望する規模や期間等により、対応ができない場合があります。

サイバー保険の付帯サービスに関する不透明点・質問は、損害保険ジャパン株式会社の各営業店舗または取扱代理店へお問合せください

## 4. 『医療機関用サイバー保険』の概要⑥

### 医療機関用サイバー保険の引受プラン

- 医療機関用サイバー保険ではサイバーセキュリティに関するすべてのリスクを補償する【オールリスクプラン】と、情報漏えいに関するリスクのみを補償する【情報漏えい限定プラン】の2プランを用意しております。

#### オールリスクプラン

対象事由	概要
① 情報漏えいおよびそのおそれ	貴院（被保険者）の業務における情報漏えいおよびそのおそれ
② デジタルコンテンツ不当事由	デジタルコンテンツの使用の結果生じた名誉棄損や、プライバシー侵害、著作権、商標権または意匠権の侵害など
③ サイバー攻撃	貴院（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や処理、操作、犯罪行為など
④ ①～③以外のその他の業務	上記①～③以外の貴院（被保険者）の業務の一環としてのシステムの所有、使用または管理などに起因する偶発的な事由

#### 情報漏えい限定プラン

対象事由	概要
① 情報漏えいおよびそのおそれ	貴院（被保険者）の業務における情報漏えいおよびそのおそれ

# 4. 『医療機関用サイバー保険』の概要⑦

## 医療機関用サイバー保険の補償内容

### (1) お支払限度額（オールリスクプランの場合）

保険金のお支払限度額は下表のパターンをご用意しております。

【オールリスクプラン】

型コード	S 1	S 2	S 3	S 4	S 5	S 6	S 7
お支払限度額	①賠償責任	1,000	3,000	5,000	10,000	20,000	20,000
	②事故発生時の各種対応費用	100	300	500	1,000	2,000	3,000

単位：万円

【オールリスクプラン】

型コード	T 1	T 2	T 3	T 4	T 5	T 6	T 7
お支払限度額	①賠償責任	1,000	3,000	5,000	10,000	20,000	20,000
	②事故発生時の各種対応費用	100	300	500	1,000	2,000	3,000
	③喪失利益 収益減少防止費用	500	1,500	2,500	5,000	10,000	10,000
	④営業継続費用	500	1,500	2,500	5,000	10,000	10,000

単位：万円

(注1)お支払限度額とは、賠償責任の場合「1 損害賠償請求保険金額」および「総保険金額」を、費用損害の場合「1 事故保険金額」および「総保険金額」を、喪失利益および営業継続費用の場合「総保険金額」を指します。

(注2)総保険金額とは、ご契約いただいた保険契約により、①から④までのすべての補償において損保ジャパンがお支払いする保険金の合計の限度額を指します。

(注3)縮小支払割合は100%とします。

(注4)上表以外のパターンをご希望の場合は、損保ジャパンまでお問い合わせください。

## 4. 『医療機関用サイバー保険』の概要⑧

### 医療機関用サイバー保険の補償内容

#### (1) お支払限度額（情報漏えい限定プランの場合）

お支払限度額は下表のパターンをご用意しております。

【情報漏えい限定プラン】

型コード	P1	P2	P3	P4	P5
お支払限度額	①賠償責任	1,000	3,000	5,000	10,000
	②事故発生時の各種対応費用	100	300	500	1,000

単位：万円

単位：万円

型コード	Q1	Q2	Q3	Q4	Q5
お支払限度額	①賠償責任	1,000	3,000	5,000	10,000
	②事故発生時の各種対応費用	50	150	250	500

R1	R2
10,000	20,000
3,000	3,000

(注1)お支払限度額とは、賠償責任の場合「1 損害賠償請求保険金額」および「総保険金額」を、費用損害の場合「1 事故保険金額」および「総保険金額」を指します。

(注2)総保険金額とは、ご契約いただいた保険契約により、①および②の補償において損保ジャパンがお支払いする保険金の合計の限度額を指します。

(注3)縮小支払割合は100%とします。

(注4)上表以外のパターンをご希望の場合は、損保ジャパンまでお問い合わせください。

#### (2) 自己負担額（免責金額）

賠償責任および事故発生時の各種対応費用：なし

喪失利益および営業継続費用（オールスクプランでセットいただいた場合）：30万円

(注)上記以外のパターンをご希望の場合は、損保ジャパンまでお問い合わせください。

## 4. 『医療機関用サイバー保険』の概要⑨

### 医療機関用サイバー保険のご契約条件

#### 加入の対象となる事業者

- 医療施設の開設者

(注)ご申告内容によってお引き受けできないケースがありますので、詳細は取扱代理店または損保ジャパンまでお問い合わせください。

#### 補償の対象となる方（被保険者）

- 貴院

(注)なお、賠償責任に関するリスクについては、貴院の業務に関するかぎりにおいて、貴院の役員や従業員の方も被保険者となります。

#### ご契約期間（保険期間）

- 1年間

(注1)保険責任は保険期間の初日の午後4時（保険契約申込書またはセットされる特約などにこれと異なる時刻が記載されている場合はその時刻）に始まり、末日の午後4時に終わります。

(注2)実際にご契約いただく際の貴院の保険期間につきましては、保険契約申込書にてご確認ください。

#### 対象業務

- 医療施設の医療業務、介護業務または付帯業務

#### 保険適用地域

- 全世界

## 4. 『医療機関用サイバー保険』の概要⑩

### (5) 保険金をお支払いできない主な場合

保険金をお支払いできない主な場合は次のとおりです。なお、詳細についてはご契約に適用される約款の「保険金を支払わない場合」をご確認ください。

#### 【共通】

- ① 保険契約者または被保険者の故意
- ② 被保険者が行ったまたは加担もしくは共謀した窃盗、強盗、詐欺、横領または背任行為
- ③ 被保険者が、その行為が法令に違反していることまたは他人に損害を与えることを認識しながら行った行為
- ④ 他人の身体の障害、他人の財物の滅失、損傷、汚損もしくは紛失または盗取もしくは詐欺  
ただし、他人の紙または記録媒体が紛失、盗取または詐取されたことにより発生した情報の漏えいまたはそのおそれを除きます。
- ⑤ 記名被保険者の業務の履行不能または履行遅滞。ただし、次のアまたはイに掲げる原因による場合を除きます。
  - ア. 火災、破裂または爆発
  - イ. サイバー攻撃またはITユーザー業務の偶然的な事由による被保険者システムの損壊または機能の停止
- ⑥ 知的財産権の侵害。ただし、著作権、商標権および意匠権の侵害に起因する損害賠償請求を除きます。
- ⑦ 被保険者の業務の対価の見積もりまたは返還
- ⑧ 被保険者によって、または被保険者のために被保険者以外の者によって行われた不正競争等の不当な広告宣伝活動、放送活動または出版活動による他人の営業権の侵害
- ⑨ 差押え、徴発、没収、破壊等の国または公共団体の公権力の行使
- ⑩ 暗号資産の換金、売買、決済その他の取引または消失
- ⑪ 戦争等（次のアからウに掲げるものをいいます。）に起因する損害
  - ア. 戦争、外国の武力行使、革命、政権奪取、内乱、武装反乱その他これらに類似の事変または暴動
  - イ. アの過程または直接的な準備として行われる国家関与型サイバー攻撃
  - ウ. 安全保障または防衛に重大な影響を与えるもの

(注)①から③までについては、それらの行為を行った被保険者が被る損害のみ補償対象外です。

など

## 4. 『医療機関用サイバー保険』の概要①①

### (5) 保険金をお支払いできない主な場合（つづき）

#### 【事故に関する各種対応費用部分】

- ① 記名被保険者が偽りその他不正な手段により取得した情報の取扱いに起因する情報の漏えいまたはそのおそれ
- ② 記名被保険者の役員に関する個人情報に関する個人情報の漏えいまたはそのおそれ
- ③ 電気、ガス、水道、通信もしくはインターネット接続サービスの中断、停止または障害が発生したことにより、記名被保険者に対してそれらが提供されなかったことに起因して発生した費用

など

#### 【利益損害・営業継続費用部分】

- ① 保険契約者または被保険者の故意もしくは重大な過失または法令違反
- ② 電気、ガス、水道、通信もしくはインターネット接続サービスの中断、停止、または障害が発生し、被保険者に対して、それらが提供されないこと
- ③ 労働争議
- ④ 政変、国交断絶、経済恐慌、物価騰貴、外国為替市場の混乱または通貨不安
- ⑤ 被保険者システムの操作者または監督者等の不在
- ⑥ 政治的、社会的、宗教的もしくは思想的な主義もしくは主張を有する団体もしくは個人またはこれと連帯する者が、その主義もしくは主張に関して行う暴力的行為もしくは破壊行為
- ⑦ 衛星通信の機能の停止
- ⑧ 被保険者が新たなソフトウェアを使用した場合または改定したソフトウェアを使用した場合において、次のアまたはイに掲げる対象事故  
ア. 通常要するテストを実施していないソフトウェアの瑕疵によって生じた対象事故  
イ. ソフトウェアの瑕疵によって、そのソフトウェアのテスト期間内、試用期間内、または正式使用後10日以内に生じた対象事故

など

(注1) 保険期間が始まった後であっても、取扱代理店または損保ジャパンが保険料を領収する前に生じた事故や損害賠償請求による損害については保険金をお支払いできません。

(注2) この保険では、損保ジャパンが被保険者に代わって損害賠償請求権者の示談交渉を行う「示談交渉サービス」はありません。

## 6. お問い合わせ先

### ■ 取扱代理店

有限会社ミック三重

〒514-0003 三重県津市桜橋2丁目191番4 三重県医師会館2階

電話番号 059-246-0010

<受付時間>

平日：午前9時から午後5時まで

(土・日・休日・年末年始は、お休みとさせていただきます。)

### ■ 引受保険会社

・損害保険ジャパン株式会社

三重支店法人支社

〒514-0004 三重県津市栄町3-115

<受付時間>

平日：午前9時から午後5時まで

(土・日・休日・年末年始は、お休みとさせていただきます。)

この案内は 業務過誤賠償責任保険普通保険約款 サイバー保険特約条項、医療機関用追加条項 の概要を説明したものです。

詳しくは、「普通保険約款、特約条項、追加条項等」、「重要事項等説明書」をご確認ください。

またご不明な点がございましたら、取扱代理店または引受保険会社（損害保険ジャパン株式会社）までお問い合わせください。

