

# サイバーインシデント発生時の頼れる味方「緊急サポート総合サービス」の詳細 とサイバーインシデント実務フローの解説

---

2026年1月

本店企業保険金サービス部 法人保険金サービス課

# 本日のテーマ

01 インシデントサポート（緊急時サポート総合サービス \*サイバー保険加入者が利用可能）

02 事故が発生したお客さまの事故対応詳細イメージ（ランサムウェア）

03 保険対応における事故対応上の確認ポイント

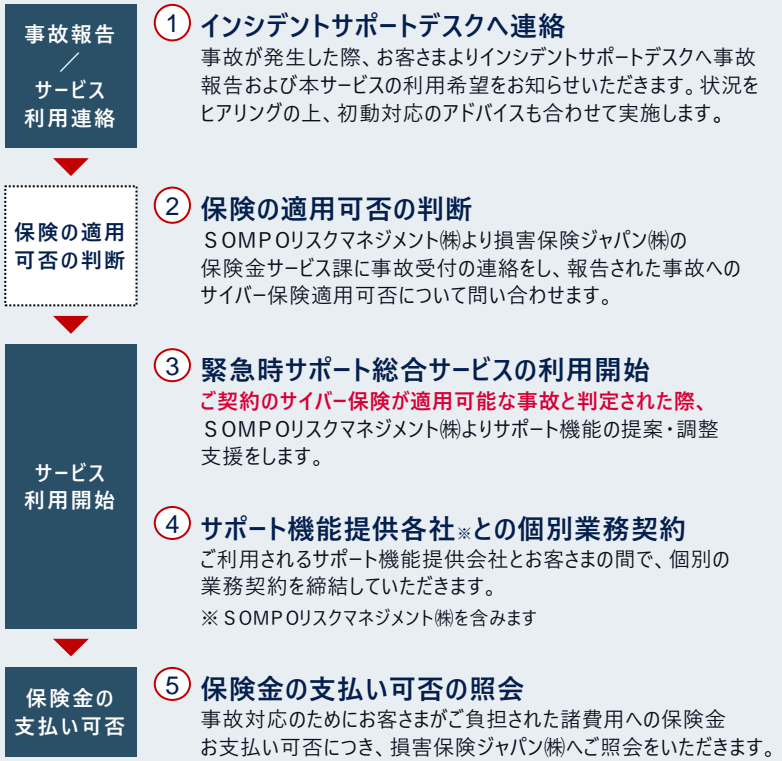
04 補足 主な必要書類

05 部工会団体サイバー保険の特徴

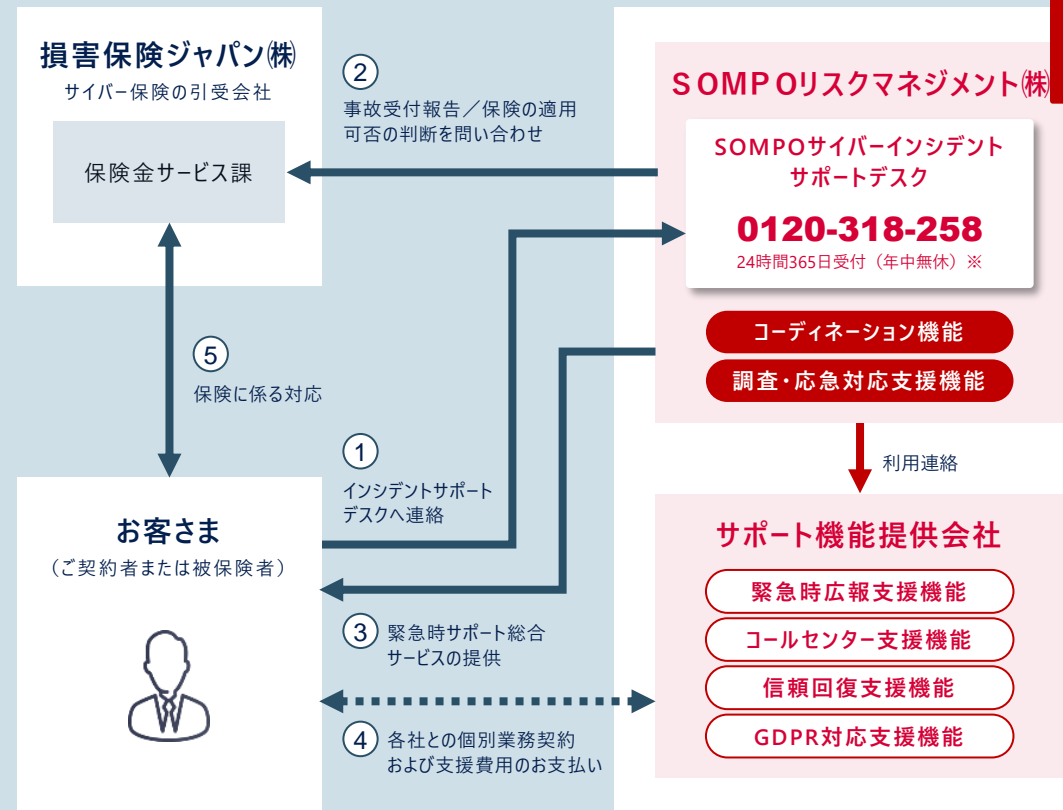
# 01. インシデントサポート概要（緊急時サポート総合サービス \*サイバー保険加入者が利用可能）

- サイバーインシデント対応をワンストップでご支援
- セキュリティベンダーが初動まで24時間365日対応実施により、迅速かつ的確なサポートを提供(2026年2月以降)
- 保険加入していると、フォレンジック等の外注についても迅速な判断の一助となる。

## ■ ご利用の流れ



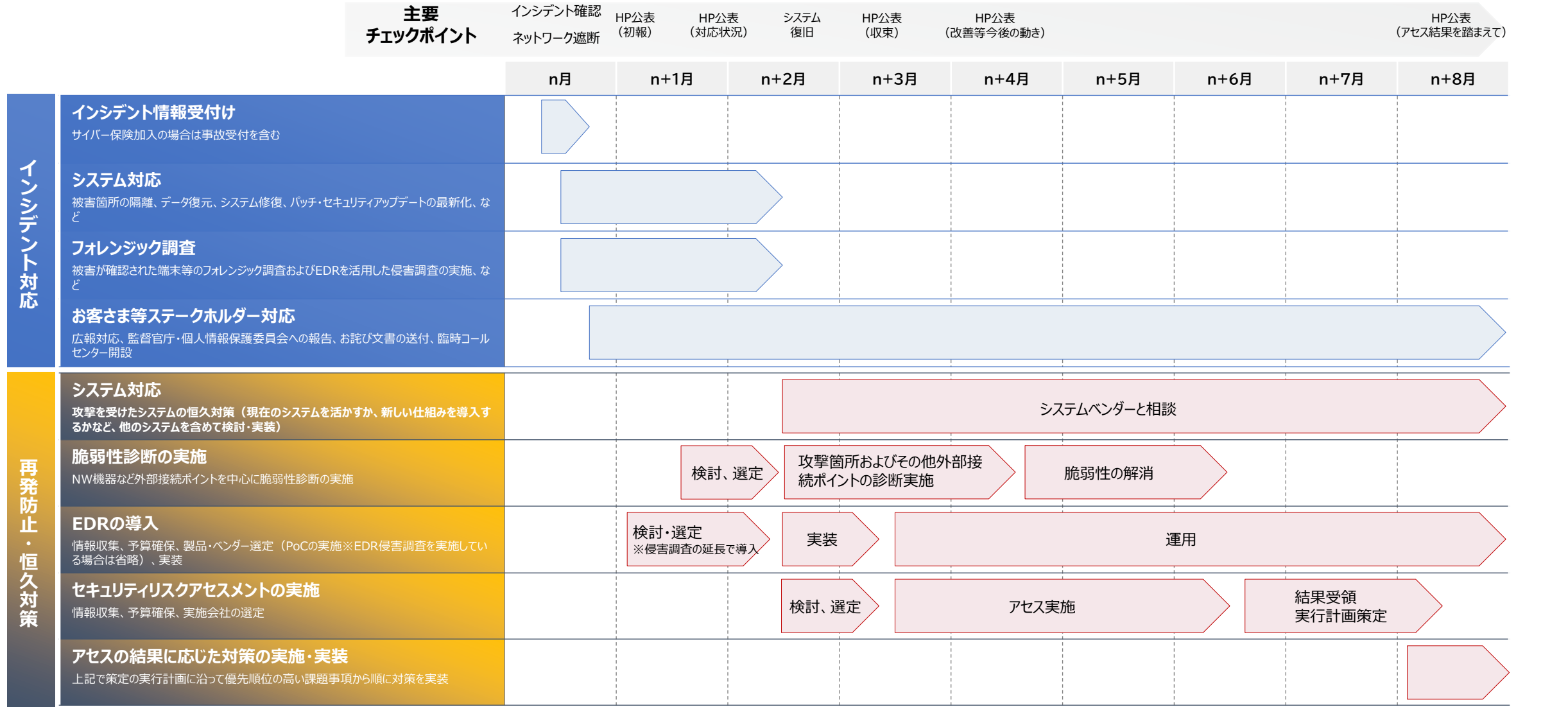
本サービスでのご提供サービスにつきましては保険金の支払対象外となる場合があります。  
支払い可否については担当保険金サービス課へご確認ください。



※夜間（17時以降）および休日・祝日の受付事業については、SOMPOリスクマネジメント(株)における対応およびサービス提供が翌営業日（平日9時以降）になる場合があります。

## 02. 事故が発生したお客さまの事故対応詳細イメージ（ランサムウェア）

- サイバーインシデント発生時には、システム対応、フォレンジック調査、ステークホルダー対応、再発防止策定等、多岐にわたり長期間の対応を求められる



## 02. 事故が発生したお客さまの事故対応詳細イメージ（ランサムウェア）

- サイバーインシデントで動揺している中、初動での的確かつ迅速なアドバイスを実施
- 早々にWeb打ち合わせおよび現地調査を実施(自社および提携会社にて対応する為、迅速に対応が可能)
- サイバーインシデント発生後、約1週間程度で、速報の調査報告会を実施および、その後約1か月程度で最終報告会を実施。

### 初動およびフォレンジック調査・システム対応支援の詳細タイムラインイメージ

事故日：N月1日 AM9:00  
事故報告：N月1日AM12:00

	N月				N+1月	
対応フェーズ	受付	初回ミーティング	現地訪問	速報会	経過報告会	最終報告会
日時	N月1日 AM12:00	N月1日 PM5:00	N月2日～3日	N月7日	適宜	N+1月 7日
打合せ事項	<ul style="list-style-type: none"><li>・現在発生している状況とお客様の対応状況を確認</li><li>・被害範囲拡大防止の観点で、ネットワーク隔離や遮断などのアドバイスを実施</li><li>・リスク社より折り返し、状況ヒアリング実施</li><li>同日PM5:00に打ち合わせ決定</li></ul>	<ul style="list-style-type: none"><li>・初回実施打ち合わせ（約1時間～1.5時間）</li><li>・状況の把握とSRMサービスの紹介、今後の流れ等を説明</li><li>・翌日もしくは翌々日あたりに現地を訪問し、「オンサイトハンドリングサービス・証拠保全」のサービスを提供。</li><li>・見積は当日もしくは翌日までには見積もりを提示し、メールの内諾ベースで作業着手を行う</li><li>・システム対応についてはベンダー様と対応いただくよう依頼。</li></ul>	<ul style="list-style-type: none"><li>・現地訪問とともに追加ヒアリング実施</li><li>・およそ5営業日程度で調査速報を実施。</li><li>・日々の連絡・確認はメールや電話で行う。</li><li>・さらなる攻撃を防ぎつつ、業務復旧に向けた対応をお客様に行っていただく。</li></ul>	<ul style="list-style-type: none"><li>・速報報告会実施</li><li>・追加ヒアリング</li><li>・システム復旧タイミング等を適宜アドバイス</li></ul>	<ul style="list-style-type: none"><li>・最終報告会までの間、適宜、メールおよび電話等でやりとりを実施。</li></ul>	<ul style="list-style-type: none"><li>・調査最終報告会実施</li><li>・調査完了後、お客様や取引先対応が終わるまでには3か月程度を要する。</li><li>・業務の完全な復旧については約1か月～6か月程度要することが多い。</li></ul>

## 02. 事故が発生したお客さまの事故対応詳細イメージ（ランサムウェア）

- 個人情報保護委員会への報告や自社HPへのリリース、顧客へのおわび状、コールセンターの設置等、お客様ステークホルダーの対応すべき事項は多岐にわたる。
- 初回ミーティングにて、今後の対応事項の整理および、個人情報保護委員会への報告や自社HPへのリリースのサポートを開始。
- 必要に応じて、顧客へのおわび状やコールセンターの設置サポート等を実施。

### お客様等ステークホルダーのタイムラインイメージ

事故日：N月1日 AM9:00

事故報告：N月1日AM12:00

	N月							N+1月		N+2月
対応フェーズ	受付	初回ミーティング (フォレンジック調査等のミーティングと同タイミング)	関連機関への報告準備	関連機関への報告（速報）	HP等への第二報掲載・ 被害顧客への対応方法検討	顧客へのおわび状送付準備・ コールセンター対応準備	顧客へのおわび状送付対応準備	コールセンター稼働	関連機関への報告（最終報）	コールセンタークローズ
日時	N月1日 AM 12:00	N月1日 PM5:00	N月2日～3日	N月3日～5日	N月5日以降	N月20日前後	N+1月頃	N+1月 7日	N+1月中～下旬	N+2月 中旬
打合せ事項	・現在発生している状況とお客様の対応状況を確認 ・被害範囲拡大防止の観点で、ネットワーク隔離 や遮断などのアドバイスを実施 ・リスク社より折り返し、状況ヒアリング実施 同日PM5:00に打ち合わせ決定	・初回実施打ち合わせ（約1時間～1.5時間） ・今後の対応の流れを整理 ・広報支援業務の見積を提示し、メールの内諾ベースで作業着手を行う ・個人情報委員会への報告準備サポート。（3日～5日以内） ・自社HPへの告知準備サポート。	・個人情報保護委員会への報告 および自社HPでの告知対応の資料作成および社内調整対応サポート。 ・メールや電話等で質問事項に対応していく。	・個人情報保護委員会への報告をサポート ・自社HPでの告知をサポート	・フォレンジック調査の速報報告後HP等への第二報掲載をサポート ・情報漏洩等の被害者への対応方法を検討（DM発送、コールセンター設置等）	・DM文書ドラフト作成・送付準備をサポート ・コールセンター立ち上げに当たり、質問マニュアル等の作成をサポート	・フォレンジック最終報告実施後、おわび状の送付やコールセンター設置対応等をサポート。	・顧客へのお詫び状の送付に合わせ、コールセンターの稼働をサポート。	・フォレンジック最終報告をベースとし、個人情報保護委員会等への最終報告をサポート	約1か月～2か月程度でコールセンターをクローズ

## 03. 保険対応における事故対応上の確認ポイント

分類	ヒアリング項目	確認内容
共通	インシデントの発見日と発見経緯	<ul style="list-style-type: none"><li>・ 事故日を特定する</li><li>・ 公的機関やセキュリティ運用管理の委託先など、外部からの通報によるものか確認する</li></ul>
共通	被保険者の商流（※）、業務フロー、システムフロー ※取引の流れ	<ul style="list-style-type: none"><li>・ 被保険者の業種はITサービス業務か（ITユーザー業務か）確認する</li></ul>
共通	被害状況	<ul style="list-style-type: none"><li>・ 被害状況、影響等を確認する</li><li>・ 「情報漏えいまたはそのおそれ」の事故の場合、どのような情報が漏えい（のおそれ）か</li></ul>
共通	応急処置対応の有無	<ul style="list-style-type: none"><li>・ 応急処置の内容を確認</li><li>・ 応急処置を指示した人の有無</li></ul>
共通	事故発生からの対応経緯	<ul style="list-style-type: none"><li>・ 社内報告書やセキュリティ委託先会社の対応レポートの有無</li></ul>
共通	ネットワーク構成図の有無	<ul style="list-style-type: none"><li>・ 被害状況、範囲の確認</li></ul>
共通	インシデント対応希望の有無	<ul style="list-style-type: none"><li>・ SOMPOサイバーインシデントサポートデスクTEL（0120-318-258）を案内する</li></ul>
費用	公的機関への報告の有無	<ul style="list-style-type: none"><li>・ 報告ありの場合：報告先機関はどこか</li><li>・ 報告なしの場合：今後の報告予定の有無</li></ul>
費用	情報漏えいのおそれにおける対応	<ul style="list-style-type: none"><li>・ 被保険者のHP上の掲載、謝罪文の送付、記者会見などによる外部への公表の有無</li></ul>
賠償	賠償請求の有無	<ul style="list-style-type: none"><li>・ 賠償請求が発生する場合は、項目名、金額、書面などを確認する</li></ul>

# 04. 補足 主な必要書類

サイバー保険の事故対応に必要な書類について、以下の条件、事故を想定とした例を掲載します。サイバー保険においてはインシデントにより必要な書類が異なります。

前提条件	当社サイバー保険の記名被保険者であること／緊急時サポート総合サービスを利用し、各種インシデント対応を行うこと
想定事故	記名被保険者の所有するサーバに外部から不正アクセスがあり、サーバ内の個人情報that漏えいした可能性が生じた。 (サイバー保険特約条項 第1条(1)①、サイバー保険特約条項 第1条(1)②イ)

## 保険金請求に必要な書類（通常の賠償責任保険と同様）

必要書類
保険金請求書
示談書 or 示談書不添付に関する確認書
負担立証資料【例：領収書や振込明細等】

## 事故内容の検討に必要な書類（例）

必要書類	確認趣旨
本件事故の概要や対応の経過が分かる資料【例：社内報告書等】	サイバーインシデント発見の経緯（“だれが、いつ、どのように”）や、その後の対応、現時点の判明事項等を時系列で把握
漏えいの可能性がある情報の概要（人数・種類等）が分かる資料【例：個人情報管理台帳等】	漏えいした個人情報の種類や件数等の把握
本件事故で影響を受けた範囲が分かる資料【例：被害システムのネットワーク構成図等】	不正アクセスを受けたシステムについて、そのシステムとその他関連し得るシステムの概要等の把握
(相手方と何らかの契約関係にある場合) その契約関係や賠償に関する取り決め等が分かる資料【例：業務委託契約書】	記名被保険者と相手方の関係性ならびに法律上の賠償責任が発生するか否かの確認
(下記、実施している場合) ・新聞、雑誌、テレビ、ラジオまたはこれらに準じる媒体による会見、発表、広告等の文書 ・被害にあった本人またはその家族へ送付した謝罪文書 ・公的機関に届け出した資料	個人情報の漏えいまたはそのおそれに基づき費用保険金を支払う場合に充足すべき第2条（保険金を支払う場合－費用）(3)に規定する情報漏えい対応費用のトリガーを満たすことの確認



## 支払保険金の検討に必要な書類（例）



必要書類	
損害賠償金：	
	・相手方からの請求内容および請求金額が分かる資料
	・請求明細（内訳を含む）とそれぞれの請求根拠が分かる資料
費用保険金／原因調査やデータ復旧、各種コンサル等の外注費用：	
	・作業概要が分かる資料【例：提案書、仕様書等】
	・作業結果が分かる資料【例：調査報告書、各種成果物等】
	・最終支払額が分かる資料【例：請求書等】
費用保険金／被害者への謝罪文や見舞品の送付等に係る費用：	
	・漏えいした個人情報の件数等が分かる資料【例：個人情報管理台帳等】
	・購入した見舞品の概要（対象人数、個数等）が分かる資料【例：請求書等】
	・発送費用が分かる資料【例：請求書、領収書等】
費用保険金／弁護士相談費用：	
	・相談内容の概要や作成依頼書類の概要、対応時間が分かる資料
	・最終支払額が分かる資料【例：請求書等】
費用保険金／使用人の事故現場派遣に係る費用：	
	・使用人を事故現場へ派遣した経緯および派遣した際の作業概要が分かる資料
	・支払の妥当性や最終支払額が分かる資料【例：社内決裁書類、請求書等】
費用保険金／事故対応に係る使用人の超過勤務手当：	
	・残業手当に関する規定【例：給与規程・賃金規程】
	・対象者が実施した作業内容が分かる資料【例：作業日報等】
	・対象者の勤務時間が分かる資料【例：勤務時間管理表（日毎）等】
	・対象者の給与単価が分かる資料【例：給与明細、給与階級表（職務グレード）等】
	・最終支払額が分かる資料【例：請求書等】
	・（派遣社員の場合）派遣会社との契約、費用、および事故対応のために要した時間が分かる資料【例：派遣契約書、請求書・請求明細等】
	・（臨時雇用者の場合）雇用契約等、事故対応のための臨時雇用であることが分かる資料【例：雇用契約書、請求書、請求明細等】

# 05. 部工会団体サイバー保険の特徴

特徴	概要
保険料水準	■ 団体制度ならではの <b>スケールメリットを生かした割安な保険料水準</b> となっております。
保険期間	■ 2025年4月1日（午後4時） ～ 2026年4月1日（午後4時） ■ 中途加入も可能でございます。 ■ 中途加入の場合、毎月20日締切で翌月1日（午後4時）～2026年4月1日（午後4時）でご加入が可能です。
損保ジャパン サイバー保険のメリット	■ 充実した付帯サービス： <b>緊急時サポート総合サービス(無料)</b> ■ 費用保険金の補償範囲：サイバー事故時の費用保険金の内容が充実

# 05. 部工会団体サイバー保険の保険料イメージ

- 企業の規模、補償内容、告知内容によって異なりますが、月々数万円程度からご検討いただけるケースもございます。
- 利益補償を追加されますと保険料は数倍に程度になりますが、ランサムウェア被害の場合、事業停止リスクを考慮すると、利益補償のご検討も併せてお勧めいたします。

## 売上毎の保険料イメージ

NO	売上高	保険金額				年間保険料(円)	月額参考保険料(円)
		賠償	費用	利益	利益 てん補期間		
1	10億円	5億円	5千万円	-	-	133,810	11,150
2				1億円	1か月	324,810	27,070
3	100億円			-	-	377,790	31,480
4				1億円	1か月	1,266,790	105,570
5	500億円			-	-	807,090	67,260
6				1億円	1か月	1,696,090	141,340

\*告知内容に関して、約7割をご対応いただいている想定です。  
によっては、上記保険料と異なることもございますので、ご参考程度としていただけますと幸いです。  
利益付保のケースは、利益+経常費が売上の20%の想定です。  
本契約は年払になるため、月額保険料はご参考用となります。

END

ご清聴ありがとうございました。



© JAPAN-DA