

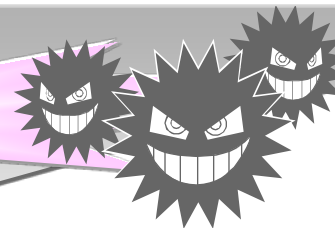
注) 弊社への保険お申込みについては、提案書完全版を必ずご覧ください

サイバーセキュリティ総合補償プランのご提案 (抜粋)

MS&AD 三井住友海上火災保険株式会社

企業にとってのサイバー攻撃の脅威

サイバー攻撃の発生



個人情報・企業情報の漏えい

取引先企業等の業務阻害

企業イメージ・信用の低下

自社業務の阻害

さまざまな対応や損害が発生

初動対応

- ・被害拡大防止
- ・原因・被害状況の調査
- ・証拠保全

等

事故対応（対被害者）

- ・通知（お詫び状送付等）
- ・コールセンター設置
- ・見舞金支払い
- ・損害賠償金支払い

等

事故対応（信用回復）

- ・謝罪広告・会見
- ・コンサルティング費用

等

自社業務の阻害

- ・システムダウン
- ・データ損壊・改ざん
- ・利益喪失
- ・営業継続費用

等

サイバーリスクに関するリスクマネジメントが急務

サイバーセキュリティ総合補償プランの特長

①	外部起因（サイバー攻撃、不正アクセス等）、内部起因（過失、使用人等の犯罪等）の事故を幅広くカバー	➡	サイバー攻撃・ハッキング等による不正アクセスのみならず、セキュリティ設定ミス等貴社の過失によるものや、一般に予防策が講じにくいとされる使用人等の犯罪リスクまで、幅広くカバーします。
②	情報漏えいはもちろん、他人の業務の休止・阻害、他人の電子情報の滅失・破損等、さまざまな事由が対象	➡	最も懸念される「情報漏えいまたはそのおそれ」のみならず、ネットワークの所有・使用・管理や電子情報の提供によって、他人の業務を休止・阻害したり他人の電子データに損害を与えた場合や、人格権・著作権を侵害した場合も補償対象となります。
③	不正アクセス等の際の対応費用を手厚く補償	➡	情報漏えいまたはその“おそれ”に加えて、ネットワークの所有・使用・管理や電子情報の提供によって他人の業務を休止・阻害した場合の広告宣伝活動費用、コンサルティング費用や事故対応費用等を補償します。
④	賠償事故については、海外で提起された損害賠償請求や、他人の身体障害や財物損壊も対象	➡	海外で事故が発生し、海外で損害賠償請求を受けた場合や現地で事故対応に必要な各種費用も補償対象となります。また、サイバー攻撃に起因する他人の身体障害・財物損壊による損害賠償責任も対象となります。
⑤	ネットワーク機器等の機能停止による、貴社の利益損失、営業継続費用も補償	➡	サイバー攻撃等不測かつ突発的な事由に起因して、貴社のネットワークを構成する日本国内の I T 機器等が機能停止することによって生じた、貴社の利益損失、営業継続費用も補償します。
⑥	充実した各種リスクマネジメントサービス、事故対応等のサービスを提供	➡	「標的型メール訓練サービス」や「情報セキュリティ診断サービス」等のリスクマネジメントサービスのほか、事故が発生した場合に経験豊富な専門事業者を紹介する「専門事業者紹介サービス」を提供します。

サイバーセキュリティ総合補償プランの概要

「サイバーセキュリティ総合補償プラン」は、サイバー事故等に起因して発生するさまざまな損害を総合的に補償するプランで、「サイバープロテクター」（専門事業者賠償責任保険）のプレミアムプランと「企業費用・利益総合保険」で構成されています。

補償	賠償損害に関する補償	費用損害に関する補償	利益損失に関する補償
保険商品	サイバープロテクター（プレミアムプラン） 専門事業者賠償責任保険普通保険約款 + サイバープロテクター特約・サイバープロテクター拡張補償特約 IT業務特約（オプション）		企業費用・利益総合保険 企業費用・利益総合保険普通保険約款 + サイバーセキュリティ補償特約
被保険者	<記名被保険者> 貴社 <被保険者> 貴社および貴社の役員（注1）（注2） （注1）貴社の役員として行うまたは行った行為に起因して損害を被る場合に限ります。 （注2）IT業務特約をセットした契約の場合、貴社のすべての販売業者または下請業者、およびそれらの者の役員（貴社のIT業務について販売業務または下請業務を行った場合に限る。）を含みます。		貴社
補償する損害	① 情報の漏えいまたはそのおそれ ② 情報システムの所有・使用または管理に起因する他人の業務阻害等 ③ サイバー攻撃に起因する他人の身体障害・財物損壊 ④ IT業務の遂行に起因する業務阻害等（IT業務特約セットの場合） に起因して、保険期間中に貴社に対して損害賠償請求がなされたことにより貴社が被る次の損害 ア. 法律上の損害賠償金 イ. 争訟費用 ウ. 権利保全行使費用 エ. 訴訟対応費用	① 情報の漏えいまたはそのおそれ ② 情報システムの所有・使用または管理に起因する他人の業務阻害等 ③ IT業務の遂行に起因する業務阻害等（IT業務特約セットの場合） ④ ①～③を引き起こすおそれのあるサイバー攻撃 ⑤ ①～④を除き、サイバー攻撃またはそのおそれが発生した場合（注1）に、一定期間内に貴社が措置を講じることによって被る損害（注2） （注1）別途定める「公表要件」のいずれかによって事故の発生が明らかになった場合に限ります。 （注2）対象となる費用等、詳細はP. 9～をご参照ください。	貴社のネットワークを構成する日本国内のIT機器等の機能停止によって、貴社がIT機器等を用いて日本国内で行う営業の遂行の全部または一部が休止・阻害されたために生じた次の損害 ①利益損失 （喪失利益、収益減少防止費用） ②営業継続費用

サイバープロテクターの概要

「サイバーセキュリティ総合補償プラン」のうち賠償損害および費用損害は、サイバープロテクターの3つのプラン（エコミー・スタンダード・プレミアム）のうち、プレミアムプランで補償します。

プレミアムプラン

サイバー攻撃を含めた幅広い補償の充実プラン

スタンダードプラン

エコミープラン

賠償損害

情報の漏えいに起因する賠償損害

賠償損害

情報システムの所有、使用または管理に起因する他人の業務阻害等

費用損害

■ 対象となる事故(情報セキュリティ事故) ■

■ 対象となる損害 ■

- ① 情報の漏えいまたはそのおそれ
- ② 情報システムの所有、使用または管理に起因する他人の業務阻害等
- ③ IT業務の遂行に起因する業務阻害等 (IT業務特約セットの場合)

事故対応費用

事故原因・被害範囲調査費用

広告宣伝活動費用

法律相談費用

コンサルティング費用

見舞金・見舞品購入費用

適用地域は日本国内

賠償損害

サイバー攻撃に起因する他人の身体障害・財物損壊

上記①～③の情報セキュリティ事故



④上記①～③を引き起こすおそれのあるサイバー攻撃

⑤上記①～④を除き、サイバー攻撃またはそのおそれ

クレジット情報モニタリング費用

公的調査対応費用

情報システム等復旧費用

被害拡大防止費用

再発防止費用

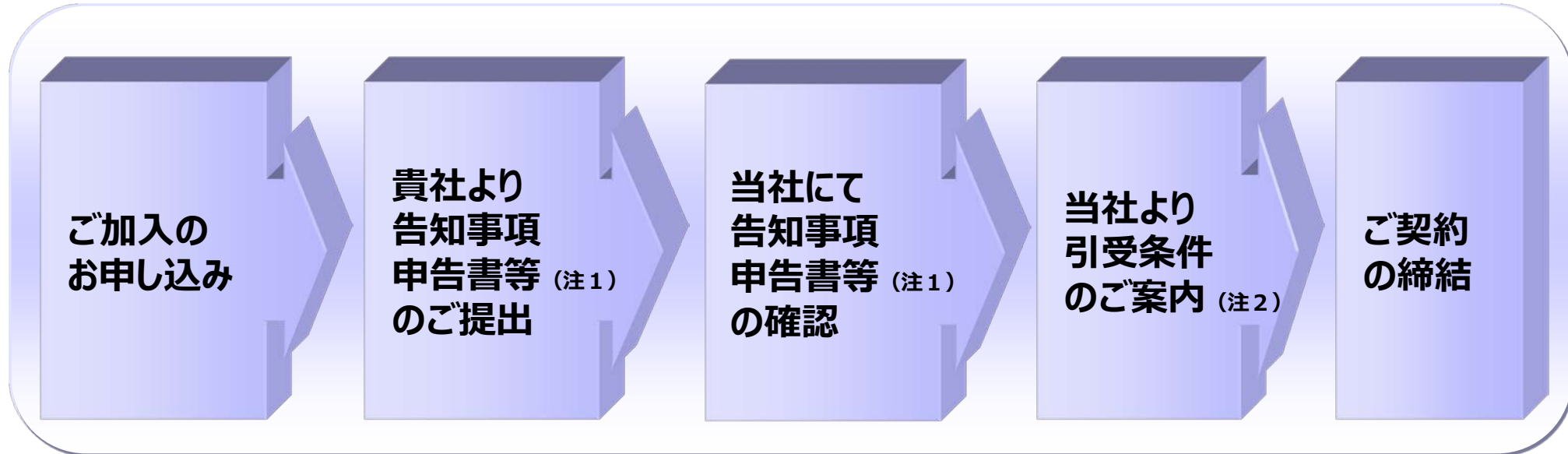
サイバー攻撃調査費用

適用地域は全世界※

(※) IT業務の遂行に起因する事故については、保険適用地域は日本国内となります。

ご契約までの流れ

保険設計・保険料のお見積りにあたってご教示いただきたい情報等と、ご契約までの流れは以下のとおりです。



(注1) 告知事項申告書等

<サイバープロテクター>

・「告知事項申告書」では、「保険料算出の基礎」、「過去の事故について」等を告知いただきます。

<サイバープロテクター、企業費用・利益総合保険共通>

・「サイバーセキュリティ総合補償プラン ヒアリングシート」をご提出いただきます。このシートの質問事項にご回答いただくことにより、情報管理体制の診断を行い、ご回答内容に応じた割引が適用可能です。

(注2) ご申告内容等によっては、引受をお断りすることがございますので、あらかじめご了承ください。

インターリスク総研による各種リスクマネジメントサービス

※株式会社インターリスク総研は、MS&ADインシュアランスグループでリスクマネジメント事業を担っているリスクコンサルティング専門の会社です。

(1) 中小企業向け・情報セキュリティ診断サービス

この診断サービスでは、情報セキュリティに関する対策の実施状況について、チェックリストを用いて、『人的対策』『組織的対策』『物理的対策』『技術的対策』の4つの対策分野にわたる設問にご回答いただいた後、インターリスク総研の訪問によるヒアリングを実施したうえで、その診断結果を、報告書にまとめてご提供します。

<サービスの概要>

実施内容	
事前アンケート	▼チェックリストをご提供し、貴社に記入いただきます。
ご訪問 所要時間（目安） ：1.5時間	▼記入いただいたチェックリストに沿って、対策取組に関するヒアリングを行います。
（約2～3週間）	* チェックリスト結果をもとに貴社の取組レベルを診断し報告書を作成
訪問後	▼報告書を送付

<チェックリストと報告書（イメージ）>

情報セキュリティチェックリスト

設問	選択	結果	確認事項
01.01 従業員が電子メールの送付先を誤って送信し、重要な情報が漏洩するおそれがあるかどうか	○	○	
01.02 個人情報、業務上の重要な情報、機密情報、営業秘密、知的財産権等の重要な情報が、誤って送信された場合に、速に発見し、適切な対応がとれるかどうか	○	○	
01.03 重要な情報、機密情報、営業秘密、知的財産権等の重要な情報が、誤って送信された場合に、速に発見し、適切な対応がとれるかどうか	○	○	
01.04 重要な情報、機密情報、営業秘密、知的財産権等の重要な情報が、誤って送信された場合に、速に発見し、適切な対応がとれるかどうか	○	○	
01.05 重要な情報、機密情報、営業秘密、知的財産権等の重要な情報が、誤って送信された場合に、速に発見し、適切な対応がとれるかどうか	○	○	
01.06 重要な情報、機密情報、営業秘密、知的財産権等の重要な情報が、誤って送信された場合に、速に発見し、適切な対応がとれるかどうか	○	○	
01.07 重要な情報、機密情報、営業秘密、知的財産権等の重要な情報が、誤って送信された場合に、速に発見し、適切な対応がとれるかどうか	○	○	
01.08 重要な情報、機密情報、営業秘密、知的財産権等の重要な情報が、誤って送信された場合に、速に発見し、適切な対応がとれるかどうか	○	○	
01.09 重要な情報、機密情報、営業秘密、知的財産権等の重要な情報が、誤って送信された場合に、速に発見し、適切な対応がとれるかどうか	○	○	
01.10 重要な情報、機密情報、営業秘密、知的財産権等の重要な情報が、誤って送信された場合に、速に発見し、適切な対応がとれるかどうか	○	○	

〇〇株式会社 御中

情報セキュリティ診断 報告書

三井住友海上火災保険株式会社
株式会社インターリスク総研

ご挨拶

このたびは弊社提供サービス「セキュリティ診断サービス」をご利用いただき誠にありがとうございます。ご回答いただきました結果をもとに、弊社による診断結果をご報告させていただきます。

情報セキュリティ対策の不備による情報漏えいインシデントは、損害賠償などの直接的損失のみでなく、信用の失墜やブランドイメージの毀損など間接的な被害も計り知れないものがあります。

総合評価

総合リスク対策 **C**

ご回答いただきましたチェックリストをもとに評価した、貴社の情報セキュリティ対策状況は右図のとおりです。

情報セキュリティ対策においては、「人的対策」「組織的対策」「物理的対策」「技術的対策」をバランスよく実施していくことが重要となります。

本報告書の結果を参考に、現状の取組が十分な点、不十分な点を確認のうえ、さらなる対策の拡充・高度化につなげられることをお勧めいたします。

総評

チェックリストをもとにした診断結果は、情報セキュリティ対策は総合的に〇〇点という結果となりました。このため、総合的なセキュリティ対策評価は「A・B・C・D」（出来ている・改善が必要である・不十分である・できていない）と判定しました。（A) 門レベルの情報セキュリティ対策で満足していると考えられます。・総合的な対策において対策の不十分点が多く見受けられます。・各対策分野別の詳細結果、および別添の診断結果をご参照いただき、早急に対策を講じていただきます。

※このサービスは株式会社インターリスク総研との提携サービスです。お客さまの費用負担はありません。

インターリスク総研による各種リスクマネジメントサービス

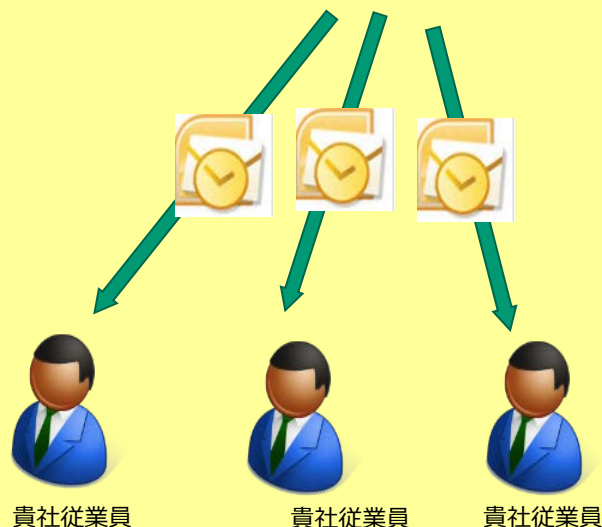
(2) 標的型メール訓練サービス

- ・貴社従業員（100名まで）に、標的型メールを模した訓練メールを送信し、メール本文に記載されているURLのクリック状況等を報告します。
- ・貴社従業員のURLクリック状況をふまえて、株式会社インターリスク総研から簡易レポートを作成・提出します。
（レポートは、主にクリック割合および今後のアドバイスに関する簡易的な内容となります。）
- ・サービスのご利用については、所定の条件がありますので、株式会社インターリスク総研までお問い合わせください。

<イメージ>



標的型メール訓練システム



【ご利用上のご注意】

- 本サービスは、貴社専用のID・パスワードを発行し、貴社ご自身で、ID・パスワードを使って専用システムにアクセスしていただき、メール送信先等を設定していただくサービスです。
（貴社におかれましても一定の作業が発生します。）
- 訓練メールの送信は1回のみ、送信先は100名までです。
- 実施時期については、お申込みをいただいてから、お時間をいただくことがあります。
- 訓練メールを送信した従業員個人のURLクリック有無（誰が訓練メール記載のURLをクリックしたか等）のフィードバックは実施しておりませんので、予めご了承ください。
（個人情報保護の観点から、本サービスの専用システムでは、訓練メール送信後に、ユーザーIDのみが保存され、名前、メールアドレスは削除されます。）
- 貴社メールシステム上、本サービスによる訓練メールが迷惑メールフィルタ等で遮断される場合、個別のシステム対応（ホワイトリスト機能等がある場合には予め訓練メールアドレスを追加等）をお願いするケースがあります。（貴社メールシステムによっては、本サービスによる訓練が実施できないことがありますので、あらかじめご了承ください。）



※このサービスは株式会社インターリスク総研との提携サービスです。お客さまの費用負担はありません。

※株式会社インターリスク総研は、MS&ADインシュアランスグループでリスクマネジメント事業を担っているリスクコンサルティング専門の会社です。

インターリスク総研による各種リスクマネジメントサービス

(3) <<管理職層向け>>標的型メール攻撃対策研修

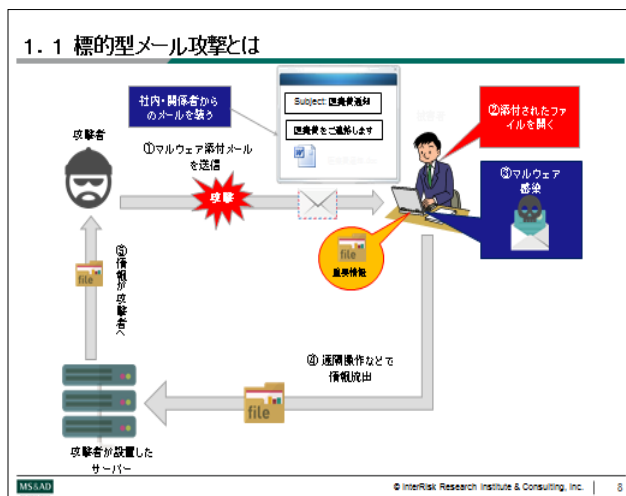
企業が有する個人情報や重要な技術情報等を狙うサイバー攻撃は年々増加の傾向にあります。また特定の組織を狙う標的型攻撃を中心としてその手口や攻撃手法が高度化・巧妙化されてきており、組織は攻撃を受けたことに気付かず、攻撃の発覚経緯の約70%は外部からの指摘によるものと言われています。

この研修によって、標的型メール攻撃のトレンドを知り、不審なメール等によるサイバー攻撃への防衛力アップと情報セキュリティ意識の向上を期待することができます。

※この研修では技術的な対策には触れません。

この研修では次のような内容についての研修を企画・実施いたします。

- 標的型メール攻撃とは
- 標的型攻撃の特徴
- 標的型メール攻撃への対策
- インシデント発生時の緊急対応



<<参考>>組織内の業務連絡メールを加工して使用した事例

	攻撃者	管理部門	幹部職員
①	官公庁や公的機関を詐称してウイルス添付メールを送信		不審なメールと判断、添付ファイルを開かなかった
②		添付ファイルを調査、ウイルスと判明	管理部門に報告
③		標的型メールに関する注意喚起メールを送信	
(約2時間後)			
④	③の注意喚起メールを加工したウイルス添付メールを送信		開封、感染

この攻撃以前に少なくとも1名以上の職員のメールが窃取され、標的型メール攻撃の被害に遭っていた？！

※典: IPAデジタルフォレンジック調査チーム「標的型攻撃メールの分析に関するレポート」(国立行政法人情報処理推進機構)

MS&AD © InterRisk Research Institute & Consulting, Inc. | 15

3.1 標的型メール攻撃への技術的対策

入口 組織に入れないための対策	<ul style="list-style-type: none"> ・マルウェア対策ソフトやOSなどのソフトウェアを、最新の状態でしておく ・振る舞い検知型アンチウイルスソフトの導入 ・IPS(侵入防止システム)の導入
潜伏中 活動させない/早期発見のための対策	<ul style="list-style-type: none"> ・パソコン、サーバのセキュリティパッチを最新の状態でしておく ・マルウェア検索を行う ・アクセスログの監視
出口 活動されても外に出さない/被害を出さない	<ul style="list-style-type: none"> ・通信の監視 ・迅速な連絡・対応体制の構築 ・アクセスログの迅速な分析

何年も前から言われ続けている対策
これだけで標的型メール攻撃を防御できるのか？！

MS&AD © InterRisk Research Institute & Consulting, Inc. | 21

株式会社インターリスク総研では、この他にも、様々なコンサルティングサービスをご用意しています。詳しくは、弊社までお問い合わせください。

サイバー攻撃時の損害額簡易算出サービス

- ・所定の質問（全9問）にご回答いただくだけで、貴社がサイバー攻撃を受けた場合の損害額を簡易算出し、その結果を報告書として、無償でご提供します。
- ・ご回答に基づいて、外部からのサイバー攻撃による次の4つの被害シナリオにおける、「賠償損害」、「費用損害」、「利益損害」の各損害額を簡易算出します。
 - ① 個人情報の漏えい
 - ② 企業情報（営業秘密）の漏えい
 - ③ 情報漏えい（上記シナリオ①②）以外の、第三者に対する損害賠償
 - ④ ネットワークを構成するIT機器等（日本国内。クラウドを除きます。）の機能停止
- ・サイバー攻撃を受けた場合の具体的な損害額をイメージいただくことで、サイバーセキュリティ対策や保険による備えの必要性を認識することができます。

3. 算出結果サマリー

シナリオ		算出結果	想定損害額(単位: 万円)			
			賠償損害	費用損害	利益損害	合計額
シナリオ ①	個人情報の漏えい	算出済	約33,900万円	約17,040万円	算出対象外	約50,940万円
シナリオ ②	企業情報(営業秘密)の漏えい	算出済	算出対象外	約1,530万円	算出対象外	約1,530万円
シナリオ ③	情報漏えい(上記シナリオ①②)以外の第三者に対する損害賠償	算出済	算出対象外	約1,230万円	算出対象外	約1,230万円
シナリオ ④	ネットワークを構成するIT機器等(日本国内。クラウドを除く)の機能停止	算出済	算出対象外	約1,530万円	約417万円	約1,947万円



【ご利用上のご注意】

- ・このサービスは、種々の仮定・前提に基づく簡易的な算出であり、損害額を保証するものではありません。
- ・このサービスで算出した項目以外にも損害が発生する可能性があります。
- ・このサービスは、保険の引受を確約するものではありません。
- ・所定のヒアリング項目に回答がない場合、損害額の算出ができません。

サイバー事故発生時の、専門事業者紹介サービス

- ・貴社のご意向に基づき、サイバー事故発生時の被害範囲の確認や原因調査または事故対応方法の策定について、経験豊富な専門事業者をご紹介するサービスです。
- ・このサービスは、貴社と当社がご紹介する専門事業者との間でご締結される委託契約に基づき、有償でご提供するものですが、プロテクト費用保険金の対象となる費用^(注)については、当社から貴社に保険金としてお支払いします。

(注) あらかじめ当社の承認を得て支出した費用に限ります。

