

# サイバー保険のご案内

(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)

## サイバー攻撃、情報漏えいなどに対する備えは万全ですか？

### 日本におけるサイバー攻撃の脅威の高まり

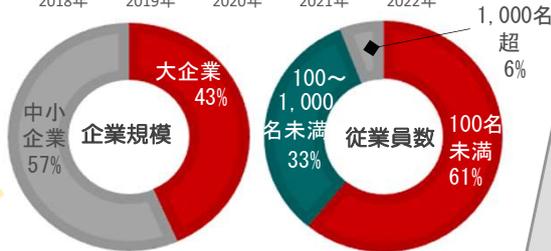
◆2022年に検知した日本国内の不正アクセス件数は、2018年と比較して約2.8倍に増加

出典：警察庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について」  
(警察のセンサーに対する1日あたりのアクセス件数)



◆サイバー攻撃の対象は企業規模に関係なく発生

出典：一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査2020」  
(サイバー被害を受けたことがあると回答した企業の企業規模および従業員数別割合)



すべての企業がサイバー攻撃をいつ受けてもおかしくない状況であり、「自社には関係ない」と他人事ではすまされません。

### 情報漏えい事故はあとを絶たず、法規制も強化

◆2022年における上場企業の情報漏えい・紛失事故は過去最多の165件、前年の1.2倍に増加  
→「ウイルス感染・不正アクセスによる漏えい事故」が5割超を占めています

出典：株式会社東京商工リサーチ「2022年「上場企業の個人情報漏えい・紛失事故」調査」

◆1件でも個人情報を取り扱う企業は個人情報保護法の対象

→改正個人情報保護法（2022年4月施行）では漏えい報告および本人への通知が義務化へ  
法令違反に対する罰則が強化され、罰金刑の最高額が1億円と大幅に引上げ

※法令違反などによる罰金については、サイバー保険の保険金の支払対象外となります。



企業活動のIT化や法規制を踏まえた情報漏えい対策の強化が必要になっています。

### 業務のIT化によるシステム関連リスクの増加

◆企業のクラウド活用やネットワークセキュリティの再設計/構築への取り組み割合は高い一方、社内のIT人材の不足やセキュリティ対策への取り組みが課題

◆生産性対策として、既存のシステムだけではなく、AIやRPAなどのデジタルテクノロジーの重要性が向上

出典：一般社団法人日本情報システム・ユーザー協会「企業IT動向調査2019(2018年度調査)」



IT化に対する企業の取り組みや新しいテクノロジーの採用が重要な環境下において、企業のシステム関連リスクは急速に高まっています。

サイバー攻撃や情報漏えいなどのセキュリティ事故は、企業活動に直接的に影響する経営リスクそのものです。



企業活動の中断・事業継続の阻害

取引先・顧客などへの損害、信用の失墜・顧客喪失

損害を与えた被害者への謝罪・損害賠償

再発防止・信頼回復などに関する対応

一連の対応コストの発生、自社利益の減少

すでに対策を取られているとは思いますが、企業を取り巻く環境は常に変化しており、セキュリティ事故に遭遇する可能性は日々高まっています。

万が一の際の被害を抑え、迅速に事故に対応するためにサイバー保険の活用をおすすめいたします。

# サイバー保険の概要

サイバー攻撃や情報漏えい、自社ネットワークの管理誤りなど貴社システムに関連して発生するセキュリティ事故に起因した第三者への賠償責任や事故対応に要する貴社の諸費用を包括的に補償する保険です。

## 補償の構成

### 基本補償

#### A 第三者への賠償責任

サイバー攻撃、情報漏えい、システム管理などに起因して他人に経済的損害を与えた場合の賠償責任・争訟費用の補償

損害賠償金  
争訟費用 etc



#### B 事故対応に要する貴社の費用

サイバー攻撃、情報漏えいなどの発生に起因して生じる『事故調査』から『解決/再発防止』までの諸費用の補償

原因調査費用 再発防止費用  
データ復旧費用 etc



### オプション

#### C 喪失利益・営業継続費用

システムの中断・停止に起因して発生した喪失利益や営業継続のための費用の補償

喪失利益 収益減少防止費用  
営業継続費用



## 事件事例

①業務用のパソコンにウィルスが感染し、社内のデータベースに保存されている顧客データのクレジットカード情報などが流出した。

⇒ A：顧客データを漏えいしたことによる損害賠償金  
B：顧客への見舞費用、ウィルス感染原因の調査・影響範囲特定費用、個人情報流出に関する謝罪会見・公告費用など

②自社のサーバーがサイバー攻撃を受け自社データが消失すると共に、取引先企業へのサイバー攻撃へ利用され、取引先企業の業務阻害が発生した。

⇒ A：業務阻害によって発生した取引先企業の損害に対する損害賠償金、B：データ復旧費用、再発防止策策定のためのコンサルティング費用など

③自社のホームページ上に記載している文章や掲載している画像などが人格権侵害や著作権侵害をしていた。

⇒ A：権利侵害された被害者に対する損害賠償金

④自社システムのバージョンアップ中に不具合が発生し、1か月近くシステム利用ができず、業務中断が発生した。

⇒ A：業務中断によって取引先などに発生した損害に対する損害賠償金、C：業務中断期間中の喪失利益、営業継続のための代替手段の費用

## サイバー保険の特長

内部のシステム  
起因の事故も  
包括的に補償

外部からの攻撃だけではなく、内部のシステムオペレーションミス、システムの管理不備などの過失に起因する事故も対象です。使用人の犯罪行為に起因する事故も補償対象となります。

サイバー攻撃の  
おそれの調査  
費用なども補償

サイバー攻撃を受けた可能性を検知した場合、実際の攻撃の有無を調査する費用、万が一に備えシステムやネットワークを遮断する費用も補償します。

紙媒体による  
情報漏えいも  
対象

電子データによる情報漏えいに限らず、書類の誤廃棄や鞆の置き忘れなど、システムに関係のない情報漏えいまたはそのおそれの事故も補償します。

データ復旧や  
機器修理費用も  
お支払い

事故の原因調査や見舞費用、再発防止策費用などのほか事故によって損壊したデータや情報機器の復旧・修理費用も事故対応費用に含まれています。

海外での事故・  
損害賠償請求も  
対象

情報セキュリティ・システムに関する事故は国内だけで発生するとはかぎりません。サイバー保険では海外で発生した事故および海外で提起された損害賠償請求も補償します。

オプションで  
IT事業リスクも  
カバー可能

他人にソフトウェアの開発やクラウドサービスの提供などを行うIT事業の遂行に起因した賠償責任もオプションによって補償対象となります。

緊急時の対応を  
サポートする  
サービスも  
提供

サイバー保険には、情報漏えいなどのセキュリティ事故が発生した際に原因調査や事故の公表、被害者からの問い合わせ窓口の設置などの緊急対応を支援する「緊急時サポート総合サービス」が自動でセットされます。

調査・緊急対応支援機能	原因・影響範囲特定、被害拡大防止アドバイス
緊急時広報支援機能	報道発表・社告支援、WEBモニタリング支援など
コールセンター支援機能	コールセンター立ち上げ、運営支援
信頼回復支援機能	再発防止策の評価に関する証明書発行など
GDPR対応支援機能	規制当局への対応支援、協力弁護士紹介など

※緊急時サポート総合サービスは、SOMPOリスクマネジメント㈱がコーディネーション役を担い、各サービスの提供委託先との総合調整を行います。  
※緊急時サポート総合サービスは、保険金がお支払いできる場合にかぎり、ご利用いただけます。  
※サービス利用料金は、契約の範囲内でサイバー保険の事故対応に関する費用保険金から充当されます。

●このちらしは概要を説明したものです。詳しい内容につきまして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。

【引受保険会社】

損害保険ジャパン株式会社

〒160-8338 東京都新宿区西新宿1-26-1  
<連絡先> <https://www.sompo-japan.co.jp/contact/>

【お問い合わせ先】

株式会社ヒューマン&アソシエイツ  
& ASSOCIATES, INC. 琉球本部 沖縄支店 那覇市銘苅1-2-15  
TEL:098-988-9900 FAX:098-988-9902