FAX：03-3268-8832　　有限会社 東京福祉企画　行

# サイバーリスク保険（情報漏えい補償）保険料見積依頼シート

●保険期間：　令和　　年　　月　　日　～　　令和 5 年　4 月　1 日

＜ご注意＞
・サイバーリスク保険（情報漏えい補償）の保険料算出にあたり、本ご質問書にご回答ください。
・ご回答内容は、保険料の決定に関して使用させていただきますので、正確にご記入いただきますようお願いいたします。

**1. 貴社会福祉協議会の把握可能な最近の会計年度（1年間）の総売上高（事業活動計算書のサービス活動収益計と補助金等の合計額）をご申告ください。**

| | |
|---|---|
| 千円未満を四捨五入し、千円単位で申告してください。 | 千円 |

**2. 以下のご質問事項にお答えください。**

| | ご質問事項 | ご回答 | |
|---|---|---|---|
| a | 過去3年間において、下記に該当する事故が発生したことがありますか。ある場合は、末尾の欄に詳細（事故の概要、損害額、復旧状況・再発防止策等）をご記入ください。<br>①不正アクセス等による自社ホームページの改ざん・データ破損<br>②不正アクセス等による情報（個人情報に限定しません。）の漏えい<br>③大量データの受領による事業停止・システムダウン（ＤｏS攻撃・ＤＤｏS攻撃） | あり | なし |
| b | **【IT業務**を行っている場合】<br>過去3年間において、IT業務の遂行に起因して第三者から損害賠償請求を受けたことがありますか。<br>ある場合は、末尾の欄に詳細（事故の概要、損害額、再発防止策等）をご記入ください。<br>＊**IT業務**を行っていない場合または、**IT業務**を補償対象としない場合は、本質問事項へのご回答は不要です。 | あり / なし<br>対象外（IT業務を行っていない/補償対象としない） | |
| c | **【IT業務**を行っている場合】<br>**電子認証業務**を現在行っていますか。または、今後1年以内に行う予定はありますか。<br>＊**IT業務**を行っていない場合または**IT業務**を補償対象としない場合は、本質問事項へのご回答は不要です。 | あり / なし<br>対象外（IT業務を行っていない/補償対象としない） | |
| d | **暗号資産交換業務**を現在行っていますか。または、今後1年以内に行う予定はありますか。 | はい | いいえ |

**3. 貴社のセキュリティ対策等について、以下のご質問事項にご回答ください。**
不明な場合は、「×」を選択してください。また、ご質問事項内の太字につきましては、末尾の「用語集」に用語の意味を記載しておりますので、ご参照ください。

| | ご質問事項 | ご回答 | | |
|---|---|---|---|---|
| | **（1）セキュリティ全般**「サイバーセキュリティ経営ガイドライン」（経済産業省・独立行政法人情報処理推進機構）関連＞ | | | |
| 1 | サイバー攻撃等のサイバーセキュリティリスクを経営リスクの1つとして認識し、サイバーセキュリティリスクに対する対応方針を組織外に宣言していますか。　＜「サイバーセキュリティ経営ガイドライン」３．１．（１）関連＞ | ○ | | × |
| 2 | 情報セキュリティに関するルール（個人情報保護および業務上の機密情報の取扱いを含むルール）はありますか。また、そのルールは適宜見直されていますか。<br>＊「ルールはあるが、個人情報保護または業務上の機密情報の取扱いが含まれてない」あるいは「ルールはあるが、見直しは行っていない」場合は、△を選択してください。　＜「サイバーセキュリティ経営ガイドライン」３．１．指示１関連＞ | ○ | △ | × |
| 3 | 従業員(社員・派遣社員・協力会社社員等)に情報セキュリティに関するルールを周知し、定期的な教育を行っていますか。<br>＊「情報セキュリティのルールを設けて従業員に周知しているが、定期的な教育は行っていない」場合は、△を選択してください。　＜「サイバーセキュリティ経営ガイドライン」３．１．指示１関連＞ | ○ | △ | × |
| 4 | 社外から最新のサイバー攻撃情報を入手することで、情報セキュリティに関するルールを定期的に確認し、必要に応じて見直されていますか。<br>＊質問2が×の場合は×、「定期的に内容を確認しているが、サイバー攻撃のトレンドに対応するための見直しは行っていない」場合は△を選択してください。　＜「サイバーセキュリティ経営ガイドライン」３．２．（４）、３．３．（８）関連＞ | ○ | △ | × |
| 5 | 組織内に**SOC、CSIRT**を設置する等、情報セキュリティインシデントの発生時に迅速に対応できる体制が構築されていますか。<br>＜「サイバーセキュリティ経営ガイドライン」３．１．（２）、３．４．（９）（１０）関連＞ | ○ | | × |
| 6 | 情報セキュリティについて、従業員（社員・派遣社員・協力会社社員等）の教育（e-learning、集合研修、標的型メールなどに対する訓練等）を行っていますか?<br>＊「教育を行ってはいるものの不十分と感じている」場合は、△を選択してください。<br>＜「サイバーセキュリティ経営ガイドライン」３．１．（２）、３．４．（９）関連＞ | ○ | △ | × |
| 7 | 社内にCISO（Chief Information Security Officer:最高情報セキュリティ責任者）等の情報セキュリティ関連業務を統括する役職を置き、定期的にセキュリティ対策状況が報告される等、組織としてセキュリティ状況を把握できる管理体制が構築されていますか。　＜「サイバーセキュリティ経営ガイドライン」３．１．（２）関連＞ | ○ | | × |
| 8 | 情報セキュリティに関する監査(**ペネトレーションテストを含む**)を定期的に実施していますか。<br>＊「過去実施したことはあるが、定期的に実施していない」場合は、×を選択してください。<br>＜「サイバーセキュリティ経営ガイドライン」３．２．指示６関連＞ | ○ | | × |
| 9 | 系列企業、ビジネスパートナー、ITシステム管理の委託先(外部委託している場合)のセキュリティ対策状況を把握していますか。<br>＜「サイバーセキュリティ経営ガイドライン」３．２．（５）、３．３．（７）関連＞ | ○ | | × |

（2）ネットワーク・セキュリティ

| | | | | |
|---|---|---|---|---|
| 10 | 「システムを新規公開または更新する場合はシステムに対して**ペネトレーションテスト**を実施する」「作業の証跡（操作記録）を取得する」等、システムを新規公開または更新する際の手順が定められていますか。<br>＊「手順は定められているものの、ペネトレーションテストは実施していない」場合は、△を選択してください。 | ○ | △ | × |
| 11 | システムは定められた接続手順にのっとりリリースされていますか。<br>＊質問10が×の場合または定められた接続手順にのっとっているケースが50%未満と見込まれる場合は×、50%以上80%未満の場合は△、80%以上の場合は○を選択してください。 | ○ | △ | × |
| 12 | ユーザ認証を必要とする**ファイアウォール**を導入し、システムへの接続経路を制限する等、システムに対する接続時のセキュリティ対策を実施していますか。<br>＊「セキュリティ対策を実施しているものの、定期的な見直しを行っていない」場合は、△を選択してください。 | ○ | △ | × |
| 13 | **IDS/IPSやWAF等を導入する等、社外から社内へ、社内から社外への通信を定期的に確認していますか？** | ○ | | × |
| 14 | インターネットまたは無線ネットワーク上の通信を暗号化していますか。 | ○ | | × |
| 15 | 社外から社内のサーバにリモートアクセス（外部接続）する際に認証処理を行っていますか。<br>＊「社外から社内のサーバにリモートアクセスを行わない」場合は、○を選択してください。 | ○ | | × |

（3）クライアント・セキュリティ

| | | | | |
|---|---|---|---|---|
| 16 | システム管理者がシステム操作を行うための**特権アカウント**を設定していますか。 | ○ | | × |
| 17 | **特権アカウント**の利用を管理していますか。<br>＊質問16が×の場合は×、「管理システムによる運用を行っておらず、異常検知をする仕組みが存在しない」場合は△を選択してください。 | ○ | △ | × |
| 18 | PC等の社員用端末に**アンチウィルスソフト**や**マルウェア**対策ソフトをインストールしていますか。<br>＊ アンチウィルスソフトやマルウェア対策ソフトをインストールしている社員用端末が50%未満と見込まれる場合は×、50%以上80%未満の場合は△、80%以上の場合は○を選択してください。 | ○ | △ | × |
| 19 | 社員用端末にインストールされた**アンチウィルスソフト**や**マルウェア**対策ソフトの**パターンファイル**や**更新プログラム**を定期的に更新していますか。<br>＊ 質問18が×の場合または定期的に更新している社員用端末が50%未満と見込まれる場合は×、50%以上80%未満の場合は△、80%以上の場合は○を選択してください。 | ○ | △ | × |
| 20 | 社員用端末にインストールされたOSや**ミドルウェア**の**更新プログラム**を定期的にインストールしていますか。<br>＊ 質問18が×の場合または定期的にインストールしている社員用端末が50%未満と見込まれる場合は×、50%以上80%未満の場合は△、80%以上の場合は○を選択してください。 | ○ | △ | × |
| 21 | 社員用端末に接続する外部媒体（USBメモリ、DVDディスク等）は会社指定のものを使用していますか。<br>＊ 会社指定の外部媒体を使用しているケースが50%未満と見込まれる場合は×、50%以上80%未満の場合は△、80%以上の場合は○を選択してください。 | ○ | △ | × |
| 22 | 機密性の高い情報を印刷またはコピーする際に出力制限をするまたは実行者を特定するソフトを導入していますか。<br>＊ 導入している端末が50%未満と見込まれる場合は×、50%以上80%未満の場合は△、80%以上の場合は○を選択してください。 | ○ | △ | × |

（4）サーバー・セキュリティ

| | | | |
|---|---|---|---|
| 23 | サーバの重要度に応じて、アクセス制限（機密情報へのアクセスは特定の権限者のみ許可する等）を行っていますか。 | ○ | × |
| 24 | アクセス状況を確認するために、ログなどを定期的にチェックしていますか。 | ○ | × |
| 25 | サーバへアクセスするためのアカウント（ID等）は個人毎に設定されていますか。 | ○ | × |
| 26 | サーバに**アンチウィルスソフト**や**マルウェア**対策ソフトをインストールしていますか。<br>＊自社で所有・管理するサーバが存在しない場合は、○を選択してください。 | ○ | × |
| 27 | サーバにインストールされた**アンチウィルスソフト**や**マルウェア**対策ソフトの**パターンファイル**や**更新プログラム**を定期的に更新していますか。<br>＊自社で所有・管理するサーバが存在しない場合は、○を選択してください。 | ○ | × |
| 28 | インストールされたOSや**ミドルウェア**の更新プログラムを定期的にインストールしていますか。 | ○ | × |
| 29 | サーバに接続する外部媒体（USBメモリ、DVDディスク等）は会社指定のものを使用してますか。<br>＊自社で所有・管理するサーバが存在しない場合は、○を選択してください。 | ○ | × |

（5）セキュアな環境・施設・オフィス

| | | | | |
|---|---|---|---|---|
| 30 | 重要情報が格納されたサーバ類は施錠されたラック(サーバを収納する専用の棚)内に設置されていますか。 | ○ | | × |
| 31 | 従業員（社員、派遣社員、協力社員等）の入社時・退職時のルールには、入社・退職に伴うIDの発行・削除処理に関する内容が含まれていますか。 | ○ | | × |
| 32 | 入社時・退職時のルールに基づいて手続きが行われていますか。<br>＊ 質問31が×の場合またはルールに基づいた手続きが50%未満と見込まれる場合は×、50%以上80%未満の場合は△、80%以上の場合は○を選択してください。 | ○ | △ | × |
| 33 | 入室時に施錠、カード(IDカードや入館証等)認証などを行い、許可された者のみが入室できる仕組みを導入している等、外部の業者などがオフィス内の重要なエリアに立ち入れないように入室制限を行っていますか。また、入退室の記録をとっていますか。<br>＊入室制限または入退室の記録のいずれか一方のみを行っている場合は、△を選択してください。 | ○ | △ | × |
| 34 | 重要システム（個人情報や機密情報を保持・使用するシステム等）のログを収集していますか。 | ○ | | × |
| 35 | 収集したログを分析する等セキュリティインシデントを特定するためのプロセス・仕組みが存在していますか。 | ○ | | × |

（事故の概要、損害額、復旧状況・再発防止策等をご記入ください。）

上記内容は、事実に相違ありません。
（加入申込をされる際には、記名･捺印ください。見積り依頼時には不要です。）

ご記入日：　　年　　月　　日　　ご契約者名

㊞

フルネームで自署（法人の場合は、記名・捺印）をお願いします。

## 情報の取扱いに関するご案内

弊社および東京海上グループ各社は、本質問書において取得するお客様の情報を、保険引受の判断、本契約の管理･履行、付帯サービスの提供、他の保険･金融商品等の各種商品･サービスの案内･提供のために利用する他、下記①から④の利用･提供を行うことがあります。
①本質問書において取得するお客様の情報の利用目的の達成に必要な範囲内で、業務委託先（保険代理店を含みます。）、保険仲立人等に対して提供すること
②契約締結等の判断をするうえでの参考とするために、他の保険会社等と協働して利用すること
③弊社と東京海上グループ各社または弊社の提携先企業等との間で商品･サービス等の提供･案内のために、共同して利用すること
④再保険契約の締結、更新･管理、再保険金支払等に利用するために、再保険引受会社等に提供すること

（ご参考）用語集

| 質問No. | 用語 | 意味 |
|---|---|---|
| b,c | IT業務 | 以下ア～クのいずれかの業務をいいます。<br>ア．ソフトウェア開発・プログラム作成業務<br>イ．情報処理サービス業務<br>ウ．情報提供サービス業務<br>エ．ポータルサイト・サーバ運営業務<br>オ．アプリケーション・サービス・コンテンツ・プロバイダ業務<br>カ．インターネット利用サポート業務<br>キ．電気通信事業法が規定する電気通信業務<br>ク．その他アからキまでに準ずる業務 |
| c | 電子認証業務 | 電子署名の本人証明等の認証を行う業務をいいます。 |
| d | 暗号資産交換業務 | 暗号資産（仮想通貨）に関する次の業務をいいます。<br>ア．暗号資産の売買・他の暗号資産との交換<br>イ．アの行為の媒介・取次ぎ・代理<br>ウ．ア、イの行為に関する利用者の金銭の管理<br>エ．他人のための暗号資産の管理 |
| 5 | SOC<br>（ソック） | Security Operation Centerの略。<br>セキュリティインシデントの監視、分析、報告を行う組織やサービスのことをいいます。 |
| 5 | CSIRT<br>（シーサート） | Computer Security Incident Response Teamの略。<br>企業や行政機関などに設置される組織の一種で、コンピュータシステムやネットワークに保安上の問題に繋がる事象が発生した際に対応する組織のことをいいます。 |
| 8、10 | ペネトレーション<br>テスト | コンピュータやネットワークのセキュリティ対策の弱点を発見するため、実際にシステムを攻撃して侵入を試みるテスト手法のことをいいます。 |
| 12 | ファイアウォール | あるコンピュータやネットワークと外部ネットワークの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システムなどのことをいいます。 |
| 13 | IDS<br>（アイディーエス） | Intrusion Detection Systemの略。<br>ネットワークを監視し、サイバー攻撃の侵入や兆候を検知する機能を有するシステムのことをいいます。 |
| 13 | IPS<br>（アイピーエス） | Intrusion Prevention Systemの略。<br>IDSの検知機能に加えて、サイバー攻撃を防御する機能を有するシステムのことをいいます。 |
| 13 | WAF<br>（ワフ） | Web Application Firewallの略。<br>サイバー攻撃の中でも特にWebアプリケーションへの攻撃を検知防御する機能を有するシステムのことをいいます。 |
| 16、17 | 特権アカウント | アクセスしたコンピュータに対してどんな操作も行うことが可能となる強力な権限をもつアカウントのことをいいます。 |
| 18、19、26、27 | アンチウイルス<br>ソフト | コンピュータウイルスに感染したコンピュータからコンピュータウイルスを駆除し、感染前の状態に修復するソフトウエアのことをいいます。 |
| 18、19、26、27 | マルウェア | コンピュータウイルス、ワーム、スパイウェアなどの「悪意のこもった」ソフトウェアのことをいいます。 |
| 19、27 | パターンファイル | コンピュータウイルスを検知するための、コンピュータウイルスの特徴を定義したファイルのことをいいます。 |
| 19、20、27 | 更新プログラム | ソフトウエアのバグ（システム仕様上の欠陥）や脆弱性（コンピュータセキュリティ上の欠陥）を修正するプログラムのことをいいます。 |
| 20、28 | ミドルウェア | OSとアプリケーションの間で中間的な処理を行うソフトウェアの一種をいいます。 |