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 6 年　4 月　1 日

＜ご注意＞
・弊社のサイバーリスク保険契約をお申し込みいただくにあたり、本ご質問書にご回答ください。
・ご回答内容は、保険料およびご契約条件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。
・ご質問事項内の太字につきましては、別紙「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。

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	
1	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、別紙に詳細をご記入ください。 ①サイバー攻撃による情報（個人情報に限定しない）の漏えい（※） ②サイバー攻撃により生じた24時間以上の事業またはコンピュータシステムの一部または全部の停止 ③サイバー攻撃によるデータの消失、破壊もしくは改ざん等 （※）個人情報保護法およびそれに類する法令に基づき規制当局への通知または報告を要する、個人情報の漏えいのおそれを含みます。 ＜別紙への記載項目＞ 事故概要、原因および被害範囲の特定状況、復旧状況、再発防止策、事故対応に要した費用額（概算見込額）	はい	いいえ
2	【**IT業務**を行っている場合】 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。 ある場合は、別紙に詳細をご記入ください。 ＊**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、「いいえ」を選択してください。	はい	
		いいえ （IT業務を行っていない/補償対象としない）	
3	【**IT業務**を行っている場合】 **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。 ＊**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、「いいえ」を選択してください。	はい	
		いいえ （IT業務を行っていない/補償対象としない）	
4	**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。**

	ご質問事項	ご回答	
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。	はい	いいえ
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）について、当てはまるものを選択してください。	ルールは存在し、定期的な見直しにより変更している。	
		ルールは存在するが、見直しのためのルールは無い。	
		ルールは存在しない。	
3	従業員（派遣社員・協力会社社員を含む）へ実施している情報セキュリティ教育について、最も当てはまるものを選択してください。	情報セキュリティに関するルールを従業員に周知したうえで、定期的に教育（e-learning、集合研修、標的型メール等に対する訓練等）を行っている。	
		情報セキュリティに関するルールを従業員に周知しているが、特に定期的な教育は行っていない。	
		情報セキュリティに関するルールを従業員に周知していない、あるいはルールが存在しない。	
4	経営戦略に基づき、守るべき情報資産とその場所を特定していますか。	はい	いいえ
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。	はい	いいえ
6	情報セキュリティインシデントによる被害からの復旧に向けた体制が構築され、明確になっていますか。	はい	いいえ
7	必要なサイバーセキュリティ対策を明確にし、その対策の適切性を評価の上で、必要な予算を確保していますか。	はい	いいえ
8	社内にCISO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。	はい	いいえ
9	情報セキュリティに関する監査について、最も当てはまるものを選択してください。	定期的に実施している。	
		過去実施したことがあるが、定期的に実施しているわけではない。	
		実施したことは無い。	

10	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）が、貴社の定める情報セキュリティ要件を満たしていることを確認していますか。	はい	いいえ
11	システムを新規公開または更新する際の手順について、最も当てはまるものを選択してください。	全てのケースにおいて予め定められた手順にのっとり、新規公開または更新を行っている。	
		予め定められた手順は存在するが、全てのケースで適用しているかは分からない。	
		上記以外	
12	システムに対する接続時のセキュリティ対策について、最も当てはまるものを選択してください。	**ファイアウォール**や**UTM**等を導入してシステムへの接続経路を制限しており、定期的に見直しや設定基準の確認を行っている。	
		ファイアウォールや**UTM**等を導入してシステムへの接続経路を制限しているが、特に定期的な見直しは行っていない。	
		特に対策は行っていない。	
13	すべての重要なサーバの通信を、**IDS/IPS**や**WAF**の導入等により、監視および制限していますか。	はい	いいえ
14	すべての重要なサーバの通信を、安全性が認められた推奨手法を用いて暗号化していますか。	はい	いいえ
15	社外から社内のサーバへのリモートアクセスについて、最も当てはまるものを選択してください。	全てのリモートアクセスについて、**2段階認証（多要素認証）**を導入している。	
		全てのリモートアクセスについて、認証処理を行っている。	
		社外から社内のサーバにリモートアクセスを行うケースは存在しない。	
		上記以外、または、特に認証処理は行っていない。	
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**について、最も当てはまるものを選択してください。	**特権アカウント**のログ管理や異常検知を行う管理システムを運用し、特権アカウントの利用状況を管理している。	
		特権アカウントを特定のユーザのみに付与しているが、利用状況の管理は行っていない。	
		上記以外	
17	社員用端末やサーバの**アンチウィルスソフト**や**マルウェア**対策ソフトのインストール状況について、最も当てはまるものを選択してください。	インストールを行うルール（インストールが出来ない場合は個別管理を行うことを含む）が存在し、そのルールが必ず実行されていることを確認している。	
		インストールを行うルール（インストールが出来ない場合は個別管理を行うことを含む）は存在するが、そのルールが必ず実行されているかどうかは、分からない。	
		特にインストールに関するルールは存在しない。	
18	社員用端末や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**対策ソフトの更新状況について、最も当てはまるものを選択してください。	更新を行うルール（更新が出来ない場合は個別管理を行うことを含む）が存在し、そのルールが必ず実行されていることを確認している。	
		更新を行うルール（更新が出来ない場合は個別管理を行うことを含む）が存在するが、そのルールが実行されているかどうかは、分からない。	
		特に更新に関するルールは存在しない。	
19	社員用端末やサーバにインストールされたOSや**ミドルウェア**の更新状況について、最も当てはまるものを選択してください。	更新を行うルール（更新が出来ない場合は個別管理を行うことを含む）が存在し、そのルールが必ず実行されていることを確認している。	
		更新を行うルール（更新が出来ない場合は個別管理を行うことを含む）が存在するが、そのルールが実行されているかどうかは、分からない。	
		特に更新に関するルールは存在しない。	
20	社員用端末やサーバに接続する外部媒体(USBメモリ等)は会社指定のものを使用していますか。	はい	いいえ

21	機密性の高いデータの出力ルールとその運用について、最も当てはまるものを選択してください。	データの出力ルールが存在し、その徹底や監査が可能な仕組み（※）を導入している。 （※）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の導入等。	
		データの出力ルールは存在するが、特に徹底や監査を可能とする仕組みは導入していない。	
		特にデータの出力ルールは存在しない。	
22	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。	はい	いいえ
23	アクセス状況を確認するために、サーバのログを収集・管理する仕組みを構築していますか。	はい	いいえ
24	重要情報が格納されたサーバ類は施錠されたラック内に設置されていますか。	はい	いいえ
25	従業員の入社時・退職時のルールについて、最も適当なものを選択してください。	入社・退職に伴うIDの発行・削除処理を、予め定めたルールに基づき、必ず実施している。	
		入社・退職に伴うIDの発行・削除処理に関するルールは存在するが、実施を確認しているわけでは無い。	
		特に入社・退職に伴うIDの発行・削除処理に関するルールは存在しない。	
26	施設内の重要なエリアについて、当てはまるものを**全て**選択してください。（複数選択可、最低1つ選択）	施錠や認証システム等により、入室制限を行っている。	
		入退室の記録を行っている。	
		上記に当てはまるものは無い。	
27	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・管理する仕組みを構築していますか。	はい	いいえ
28	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。	はい	いいえ

4. **【任意回答】 追加質問（全14問）にご回答いただくと、保険料の割引率が拡大する可能性がございます。**

ご質問事項		ご回答	
1	情報セキュリティ管理体制において、各関係者の役割と責任を明確にしていますか。	はい	いいえ
2	守るべき情報資産について、リスクを洗い出したうえで、優先順位付けを行っていますか。	はい	いいえ
3	守るべき情報資産とその場所の特定について、最も当てはまるものを選択してください。	リスト化を行い、責任者による承認を得ている。	
		担当者によるリスト化を行っている。	
		特定していない、あるいはリスト化は行っていない。	
4	情報セキュリティリスクが事業に与える影響（ビジネスインパクト）を分析していますか。	はい	いいえ
5	**脆弱性スキャン**と**ペネトレーションテスト**を定期的に（少なくとも1年に1回）実施し、結果に応じて必要な対策を講じていますか。	はい	いいえ
6	自社の情報セキュリティリスクや対策状況を、自社ホームページ等で外部に公開していますか。	はい	いいえ
7	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**について、一般アカウントよりもセキュリティレベルの高い手順（例：**多要素認証**）を必須要件としていますか。	はい	いいえ
8	重要なデータについて、バックアップを定期的に取っていますか（オンライン、オフライン、クラウド上を問いません）。	はい	いいえ

9	バックアップデータからの復元テストを定期的に実施していますか。	はい	いいえ
10	OSや**ミドルウェア**の**更新プログラム**の適用について、明確な基準を定めたうえで、優先度をつけて対応していますか。	はい	いいえ
11	**パターンマッチング**では検知できない**マルウェア**への対策ツール（例：EDR）を導入していますか。	はい	いいえ
12	インシデントを24時間/365日監視する体制を自社または外部委託により構築していますか。	はい	いいえ
13	インシデント発生時の緊急対応計画について、当てはまるものを全て選択してください。（複数選択可、最低1つ選択）	初期対応マニュアルを作成している。	
		定期的に対応訓練や演習を行い、必要に応じて見直しを行っている。	
		対応プロセスには、それぞれ責任が定義・付与されている。	
		経営者が組織の内外へ説明できる体制（報告ルート、公表する内容やタイミング等）を整備している。	
		上記に当てはまるものは無い。	
14	インシデントによる被害に備えた復旧体制について、当てはまるものを全て選択してください。（複数選択可、最低1つ選択）	被害が発生した場合に備えた業務の復旧計画を策定している。	
		復旧作業の課題を踏まえて、復旧計画を見直している。	
		組織の内外における緊急連絡先・伝達ルートを整備している。	
		定期的に復旧対応訓練や演習を行っている。	
		上記に当てはまるものは無い。	

上記内容は、事実に相違ありません。

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、国内外の再保険引受会社等に提供すること

（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。）

（別紙）用語集

用語	意味
IT業務	以下ア～クのいずれかの業務をいいます。 ア．システム設計・ソフトウェア開発業務 イ．情報処理・提供サービス業務 ウ．ポータルサイト・サーバ運営業務 エ．アプリケーション・サービス・コンテンツ・プロバイダ業務 。ただし、アを除きます。 オ．インターネット利用サポート業務 カ．システム保守・運用業務。ただし、アを除きます。 キ．電気通信事業法が規定する電気通信業務 ク．その他アからキまでに準ずる業務
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。
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。 ア．暗号資産の売買・他の暗号資産との交換 イ．アの行為の媒介・取次ぎ・代理 ウ．ア、イの行為に関する利用者の金銭の管理 エ．他人のための暗号資産の管理
SOC （ソック）	Security Operation Centerの略。 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。
CSIRT （シーサート）	Computer Security Incident Response Teamの略。 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。
脆弱性スキャン	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、網羅的に検査するテスト手法のことをいいます。
ペネトレーションテスト	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。
2段階認証（多要素認証）	２つの（あるいは複数の）認証方法を組み合わせて本人確認を行う仕組みをいいます。
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。
UTM （ユーティーエム）	Unified Threat Managementの略。 複数の異なるセキュリティ機能をハードウェア製品に統合させることで、効率的かつ包括的にコンピュータやネットワークを管理するシステムのことをいいます。
IDS （アイディーエス）	Intrusion Detection Systemの略。 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。
IPS （アイピーエス）	Intrusion Prevention Systemの略。 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。
WAF （ワフ）	Web Application Firewallの略。 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。
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。
アンチウイルスソフト	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。
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。
パターンマッチング	コンピュータウイルスを検出する際に、既存のウイルスの特徴や型（パターン）のデータベースと照合する手法のことをいいます。
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。
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。