サイバーリスク保険
ご質問書

東京海上日動火災保険株式会社　行

●証券番号：

●保険期間：　　年　　月　　日　　～　　年　　月　　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。
・「個人情報保護に関する規制等対応特約条項」については、ご回答内容によっては、付帯いただけない場合がございます。
・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．以下の質問事項にご回答ください。

番号	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（個人情報に限りません。）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、破壊または改ざん等 （※）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業務を補償対象としますか。 （IT業務担保特約条項を付帯しますか。）	○ はい ○ いいえ
3	【**IT業務**を補償対象とする場合（IT業務担保特約条項を付帯する場合）のみご回答ください】 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。	○ はい ○ いいえ
4	【**IT業務**を補償対象とする場合（IT業務担保特約条項を付帯する場合）のみご回答ください】 **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。	○ はい ○ いいえ
5	**暗号資産交換業務**を行っていますか。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

2．貴社記名被保険者の情報セキュリティ対策について、以下のご質問事項にご回答ください。

番号	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	サイバー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。	○ ルールが存在し、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、定期的な見直しを行う決まりは無い。 ○ 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）へ実施しているサイバー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。	○ サイバー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・演習（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。 ○ サイバー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・演習は行っていない。 ○ サイバー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（例：顧客データ・知的財産等の情報、基幹情報システム・制御システム等のデジタル環境、利用または提供しているクラウドサービス等のサービス）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、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	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、文書化されていますか。	○ 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、必要な資源（予算・人材等）を確保していますか。	○ はい ○ いいえ
8	社内にCISO等のサイバーセキュリティ関連業務を統括する役職を置き、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	サイバー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３年以内に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、（外部委託している場合）ITシステム管理の委託先が、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則り、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、**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が存在し、そのルールが実行されていることを定期的に確認している。 ○ インストールを行うルールが存在しているが、そのルールが実行されていることまでは定期的に確認できていない、または把握していない。 ○ 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。	○ 更新を行うルールが存在し、そのルールが実行されていることを定期的に確認している。 ○ 更新を行うルールが存在しているが、そのルールが実行されていることまでは定期的に確認できていない、または把握していない。 ○ 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。	○ 更新を行うルールが存在し、そのルールが実行されていることを定期的に確認している。 ○ 更新を行うルールが存在しているが、そのルールが実行されていることまでは定期的に確認できていない、または把握していない。 ○ 特に更新に関するルールは存在しない。
20	従業員が業務に利用している端末やクラウドサービスはシステム管理者または管理部門が指定する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（個人情報や機密情報等）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（個人情報や機密情報を使用・格納している場所等）について、最も当てはまるものを選択してください。	○ 他の執務室エリアとの隔離を行った上で、入退室を全て記録している。 ○ 他の執務室エリアとの隔離を行っている。 ○ 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、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

3．【任意回答】記名被保険者の情報セキュリティ対策について、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。

○	**追加質問に回答する。**
○	**回答しない。**

番号	ご質問事項	ご回答
1	サイバー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（例：顧客データ・知的財産等の情報、基幹情報システム・制御システム等のデジタル環境、利用または提供しているクラウドサービス等のサービス）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（例：顧客データ・知的財産等の情報、基幹情報システム・制御システム等のデジタル環境、利用または提供しているクラウドサービス等のサービス）とその場所について、リスト化を行ない、責任者による承認を得ていますか。	○ はい ○ いいえ
4	サイバー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	自社のサイバーセキュリティリスクや対策状況に関する、社外のステークホルダー（投資家、取引先、サプライチェーン関係者等）とのコミュニケーションについて、最も当てはまるものを選択してください。	○ 情報公開（自社ホームページ等での公開）を行い、ステークホルダーと双方向のコミュニケーション（公開した情報を基にステークホルダーから質問を受け回答する等）をしている。 ○ 情報公開を行っているが、ステークホルダーとの双方向のコミュニケーションは行っていない。 ○ 上記に当てはまるものは無い。
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、自社の事業に与える影響が大きいものについて優先的に対応していますか。	○ 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。 □ サプライチェーン全体（製造業における部品調達や、データ管理の業務委託のような関係のみならず、クラウドサービスなど外部のデジタルサービスの利用などデジタル環境を通じた繋がりを含む。）を考慮して対策を実施している。 □ 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。 □ サプライチェーン全体（製造業における部品調達や、データ管理の業務委託のような関係のみならず、クラウドサービスなど外部のデジタルサービスの利用などデジタル環境を通じた繋がりを含む。）を考慮して対策を実施している。 □ 上記に当てはまるものは無い。

４．「個人情報保護に関する規制等対応費用担保特約条項」の付帯をご希望される場合は、以下の質問にご回答ください。

○	**特約付帯を希望する。**
○	**希望しない。**

個人情報保護に関する規制等への対応について貴社で行っているセキュリティ対策をお答えください。
番号１から９のご回答に１つでも「いいえ」がある場合は、「個人情報保護に関する規制等対応費用担保特約条項」を付帯いただけません。

番号	ご質問事項	ご回答
1	貴社およびグループ企業内で収集、処理、保存されているEU居住者の個人データ*を把握できていますか。 *顧客情報だけでなく、EU域内の従業員や取引先担当者等の情報も含まれます。	○ はい ○ いいえ
2	EU居住者の個人データを取得する際の同意取得に係るルール・手順を定め、実施していますか。	○ はい ○ いいえ
3	EU居住者の個人データのEU域外への移転を行っていますか。	○ はい ○ いいえ

4	３．が「はい」の場合にご回答ください。 ３．が「いいえ」の場合は、「いいえ」を選択してください。 データの移転を行っている場合、移転先の国・地域で個人データの十分な保護措置を確保していますか。	○ はい ○ いいえ
5	GDPR（第37条）に従い、データ保護オフィサー（DPO：Data Protection Officer）*の設置が義務付けられている事業者に該当しますか。 *社内の法令遵守状況をモニタリングし、データ主体や監督当局との対応を統括する役職です。	○ はい ○ いいえ
6	5．が「はい」の場合にご回答ください。 5．が「いいえ」の場合は、「いいえ」を選択してください。 DPOを設置し、その役割・責任を定めていますか。	○ はい ○ いいえ
7	EU居住者の個人データ漏洩などの事故が発生した場合、事故を認識してから72時間以内に監督機関に報告できるよう、報告基準、報告者等のレポートライン等の具体的な報告手順を定めていますか。	○ はい ○ いいえ
8	EU居住者の個人データの取り扱いルールを社内規定等として文書化し、従業員に周知・徹底していますか。	○ はい ○ いいえ
9	貴社およびグループ企業は、GDPRに違反する、あるいは違反のおそれがあるとして、監督当局から過去に１度も指摘を受けていないですか。	○ はい（１度も受けていない） ○ いいえ（過去に指摘を受けたことがある）

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、他の保険会社等と共同して利用すること

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