損害保険ジャパン日本興亜株式会社

2017年4月以降保険始期契約用
Ver.1.10

質問書
（サイバーLite用）

被保険者名	

1. 組織的安全管理

No.	確認内容	ご回答	
1	派遣を含む全従業員に対して、採用、退職の際に本人または派遣会社等と守秘義務に関する書面を取り交わすことで、情報セキュリティに関する就業上の義務を明確にしている。	はい	いいえ
2	すべての従業員に最新の業務手順や情報セキュリティなどを認識させるための計画的な教育や指導を定期的に実施している。	はい	いいえ
3	サイバーセキュリティリスクを経営リスクの一つとして認識し、組織全体での対応方針（セキュリティポリシー）を策定している。	はい	いいえ
4	サイバーセキュリティ対策を行うため、経営者とセキュリティ担当者をつなぐ仲介者としてのCISO等からなる適切なサイバーセキュリティリスクの管理体制を構築し、各関係者の責任が明確になっている。	はい	いいえ
5	サイバーセキュリティリスクへの対策を実施するための予算の確保、またはサイバーセキュリティ人材の育成や専門事業者の活用を行なっている。	はい	いいえ
6	サイバーセキュリティリスクに関する情報の積極的な取得および外部への情報提供を行なっており、取得した情報を自社のサイバーセキュリティ対策に活かしている。	はい	いいえ
7	事故発生時に、迅速に影響範囲や損害を特定するために、初動対応マニュアルの策定や組織内のCSIRT構築など体制整備を行なっている。	はい	いいえ
8	事故発生時に、外部に対して迅速な対応を行うために、被害の通知先や開示が必要な情報を予め把握している。また、情報開示の際、経営者が組織の内外へ説明ができる体制を整備している。	はい	いいえ

2. 契約・監督

No.	確認内容	ご回答	
1	業務や情報システムの開発・運用管理を提供する時の契約書・仕様書には、ITサービスの品質や情報セキュリティ上の観点からSLAや機密保持などを記載している。	はい	いいえ
2	委託先から提供されるサービスまたは委託元へ提供するサービスが、契約に基づいた内容となっているか監視やレビューなどによって適切な管理が行なわれている。	はい	いいえ
3	パフォーマンスやサポート時間・方法などSLAや開発仕様書などサービスの内容が適切に実現されているか、報告会または報告による見直しが定期的に行なわれている。	はい 対象外	いいえ
4	改訂版や更新版を含めて第三者にパッケージソフトや情報システムなどのサービス提供を実施する場合には、仕様書が確実に実現されているかテストを行い、脆弱性や瑕疵を発見した場合には必ず修正している。	はい 対象外	いいえ
5	系列企業やサプライチェーンのビジネスパートナーにおいてサイバーセキュリティ対策が適切に行われていることを把握し、契約書等で合意を得ている。	はい	いいえ

3. 通信・システム

No.	確認内容	ご回答	
1	不正アクセス、改ざんを検知するために、運用環境や運用データに対して定期的にログを点検するなどの対策を実施している。	はい	いいえ
2	情報システムやネットワーク機器に対して、ウィルス対策ソフトの導入、バージョンアップまたはパッチの適用など適切な対策を実施している。	はい	いいえ
3	インターネットを介してやり取りする重要なデータには、VPNの利用や専用線を構築するなど適切な保護対策を実施している。	はい	いいえ
4	サーバーやネットワークの障害などが発生した場合に、SLAや契約書を遵守するために必要な保護対策を実施している。	はい	いいえ

4. 開発・保守、アクセス制御管理措置

No.	確認内容	ご回答	
1	業務システムの開発・運用において、重要なデータの保護機能や入力データの妥当性などセキュリティ要件を定め、その要件を適切に実施している。	はい	いいえ
2	重要なデータや情報システムへのアクセスには、ログイン認証やアクセス制御など適切な対策が実施されている。	はい	いいえ
3	退職した従業員のアカウントが存在することがないなど、アカウント（ID、パスワードなど）とそのアクセス制限が定期的に見直されている。	はい	いいえ
4	情報セキュリティ上の側面から、ソフトウェアの選定や購入、情報システムの開発や保守におけるプロセスごとに点検を実施するなど、適切な運用の確認を実施している。	はい	いいえ

5. 技術的安全管理措置

No.	確認内容	ご回答	
1	社内からのすべてのインターネット接続およびDMZと内部ネットワーク境界との間に、ファイアウォールなどを設置し、適切な設定をしている。	はい	いいえ
2	リモートアクセスを行なう場合、ユーザ認証システムを使用している。	はい / 対象外	いいえ
3	外部からの攻撃を検出・防御するためにIDS/IPSなどの侵入検知システムを導入し、最新版のパターンファイルに更新している。	はい	いいえ
4	インターネット上で商品の売買および決済を行うなど重要な情報をやり取りする場合、SSLによる暗号化が行われている。	はい	いいえ
5	Web・パッケージソフトなどアプリケーションにSQLインジェクションやクロスサイトスクリプティングなどに対する適切なセキュリティ対策を実施している。	はい	いいえ
6	サイバー攻撃を受けた場合に被害の拡大を防止するために、攻撃元のIPアドレスの特定と遮断、DDoS攻撃に対して自動的にアクセスを分散させる措置またはバックアップによるデータの復元などを講じる体制を整えている。	はい	いいえ
7	インターネット等の通信手段を利用した非対面の取引を行う場合に、以下のいずれかのセキュリティの確保を講じている。講じている場合は、その個数を選んでください。 ①可変式パスワードや電子証明書など、固定式のID・パスワードのみに頼らない認証方式 ②取引に利用しているPCとは別の携帯電話等の機器を用いるなど複数経路による取引認証 ③ハードウェアトークン等でトランザクション署名を行うトランザクション認証 ④電子証明書をICカード等、取引に利用しているPCとは別の媒体・機器へ格納する方式 ⑤不正なログイン・異常な取引等を検知し、速やかに利用者に連絡する体制の整備	なし / 2 / 4	1 / 3 / 5

6. その他

No.	確認内容	ご回答	
1	損害が発生した場合、復旧や代替品の手配に1か月以上を要するコンピュータやユーティリティ設備がない。	はい	いいえ
2	自社で使用するコンピュータについて、メーカー（保守業者含む）とメンテナンス契約（保守契約）を締結している。	はい	いいえ
3	クレジットカード情報を保存、処理、または伝送する場合、PCI DSS（Payment Card Industry Data Security Standards）に準拠した対策を採っている。	はい	いいえ
		クレジット情報の扱いがない	
4	情報セキュリティに関連する認証を取得している。 ※ISMS、ISO27000シリーズ、ISO15408、プライバシーマーク等 （「はい」の場合は、取得されている認証を別紙にご記入ください。）	はい	いいえ
5	独立行政法人情報処理推進機構（IPA）が提供している「自社診断シート※」の診断を行っている場合は、その点数を記入してください。 ※IPAのホームページからダウンロードしてください。 （本項目を記入した場合は、現物のコピーを添付してください。）	点	

別紙
認証名： 認証交付機関： 認証番号： 認証有効期間：

用語の解説（五十音・アルファベット順）

用語	告知書No	解説
ＤＭＺ	６－１	Demilitarized Zone（非武装地帯）。 インターネットに接続されたネットワークにおいて、組織の内部ネットワークと危険の多い外部ネットワークの間に設置されている隔離されたネットワーク領域のこと。
ＩＤＳ	６－３	Intrusion Detection System（侵入検知システム）。ネットワーク等への不正なアクセスの兆候を検知し、ネットワーク管理者に通報する機能を持つソフトウェアまたはハードウェア。
ＩＰＳ	６－３	Intrusion Prevention System（侵入防止システム）。コンピュータネットワークにおいて、特定のネットワークおよびコンピュータへ不正に侵入されるのを防御するシステム。
ＰＣＩ ＤＳＳ	７－４	Payment Card Industry Data Security Standards。加盟店やサービスプロバイダにおいて、クレジットカード会員データを安全に取り扱うことを目的として策定された、クレジットカード業界のセキュリティ基準のこと。国際カードブランド5社(American Express、Discover、JCB、MasterCard、VISA)が共同で設立したPCI SSC(Payment Card Industry Security Standards Council)によって運用、管理されている。
ＳＬＡ	３－１ ３－３ ４－４	Service Level Agreement（サービス品質保証）。サービスを提供する事業者が契約者に対し、どの程度の品質を保証するかを明示したもの。混雑時の通信速度や処理性能の最低限度や、障害やメンテナンス等による利用不能時間の年間上限など、サービス品質の保証項目を定め、それらを実現できなかった場合の料金の減額などの補償規定を利用契約に含める。
ＳＳＬ	６－４	Secure Socket Layer。インターネット上で個人情報等を送受信する際に、暗号化して行う仕組みのこと。
ＳＱＬインジェクション	６－５	Structured Query Language Injection。アプリケーションのセキュリティ上の不備を意図的に利用し、アプリケーションが想定しないSQL文を実行させることにより、データベースシステムを不正に操作する攻撃方法のこと。
ＶＰＮ	４－３	Virtual Private Network（仮想専用ネットワーク）。通信事業者の公衆回線を経由して構築された仮想的な組織内ネットワークまたはそのようなネットワークを構築できる通信サービス。企業内ネットワークの拠点間接続などに使われ、あたかも自社ネットワーク内部の通信のように遠隔地の拠点との通信が行える。
クロスサイトスクリプティング	６－５	Cross Site Scripting。ウェブページをユーザからの入力をそのままエコーバックすることによって生成しているアプリケーションのセキュリティ上の不備を利用して、サイト間を横断して悪意のあるスクリプトを注入する攻撃のこと。
パッチ	４－２	コンピュータにおいてプログラムの一部分を更新してバグ修正や機能変更を行なうためのデータのこと
プライバシーマーク	７－５	個人情報保護に関して一定の要件を満たした事業者に対し、個人情報保護団体である日本情報経済社会推進協会(JIPDEC) により使用を認められる登録商標のこと。
保守契約	７－３	ハードウェアやソフトウェアのメンテナンス、障害対応などのサービスを提供する契約のこと。
ユーザ認証システム	６－２	ユーザを認証して特定し、ネットワークシステムのセキュリティレベルを高めるために使用されるシステムのこと。ユーザIDやパスワードなどの組み合わせにより、ログインしたユーザが、ネットワークの利用可能ユーザであるかどうかを識別する。