6 情報漏えい補償制度
＜専門事業者賠償責任保険（サイバープロテクター）＞

～グループホームの情報漏えい等のリスクに備えて～

情報の漏えいまたはそのおそれ等により、損害賠償責任を負った場合の賠償金や費用を補償します。

主な事故例

- 業務中に利用者の介護保険証や個人情報が記載されたメモが入ったカバンを紛失した。

- 社用車に置いていた顧客の個人情報が入ったパソコンが盗難に遭った。

●支払限度額と保険料

補 償 内 容	A プ ラ ン	B プ ラ ン
賠償損害 （サイバープロテクター特約）	1請求・期間中　2,000万円	1請求・期間中 1,000万円
費用損害 （プロテクト費用補償特約）	1事故・期間中　1,000万円	1事故・期間中　500万円
免責金額	な　し	

保険料

保険料は売上高＊や告知内容により異なります。（＊新規開設の事業者様は1年間の事業計画値）

〈保険料例〉

年間売上高	Aプラン	Bプラン
3億円	約11.5万円	約8万円
2億円	約10.3万円	約7.1万円
1億円	約5.1万円	約3.6万円
5,000万円	約3万円	約3万円

お見積りをご希望される場合は9～10ページの見積りシートに必要事項をご記入のうえ取扱代理店宛にFAXをお送りください。
この保険契約では、ご加入時に「把握可能な最近の会計年度(1年間)の実績数値」に基づいて算出される、あらかじめ確定した保険料を払い込んでいただきます。

●この保険の対象となるお客さま

原則として情報を取り扱うすべての事業者が対象となります。（事業者単位でご加入いただく必要があり、事業の一部のみの引受けはできません。）ただし、次のいずれかに該当する事業者等は対象となりませんのでご注意ください。

○官公庁、地方公共団体、独立行政法人
○株式公開を行っていない消費者向貸金業者
○冠婚葬祭互助会
○把握可能な最近の会計年度の売上高が5,000億円を超える事業者　　等

なお、ご加入にあたっては、次の事項について記載いただいた引受保険会社所定の告知事項申告書(42ページ)をご提出いただきます。

①保険料算出の基礎	貴社の把握可能な最近の会計年度（1年間）における売上高 ■新規設立で最近の会計年度（1年間）の売上高等が把握できない場合は、事業計画書等に計画された1年間のすべての売上高の総額を記入してください。 ■保険料確定特約の規定に基づく確定保険料での引受となるため、保険料算出の基礎が確認できる資料を添付ください。
②過去の事故について （新規・更改問わず）	現時点から起算して過去3年間において、貴社のネットワーク関連業務（※）において他人から損害賠償請求を受けたことまたは損害賠償請求がなされるおそれの有無。 上記以外に、不正アクセス等を受けてその対応のために費用（原因調査、データ復旧等）を負担したことの有無。 （※）ネットワークの所有・使用または管理、ネットワーク上の電子情報の提供

保険金のお支払い等詳細についてはP19～P21および重要事項説明をご参照ください。

【送付先】FAX **03-6806-2155**　【取扱代理店】株式会社　ヤジマ　行

サイバープロテクター見積りシート(FAX専用)

見積りシートに必要事項をご記入の上、FAXをお送りください。

会員名(法人名)		会員番号			
事業所名 (グループホーム名等)					
担当者名		TEL		FAX	
お見積もりを 希望されるプラン	Aプラン　・　Bプラン　・　どちらも				

質問番号	ご質問事項	ご回答内容			質問番号
A★	貴社の把握可能な最近の会計年度（1年間）における売上高 ※新規設立で最近の会計年度（1年間）の売上高等が把握できない場合は、事業計画書等に計画された1年間のすべての売上高の総額を記入してください。	_____年_____月期(1年間) _____千円			A
B★	現時点から起算して過去3年間において、貴社のネットワーク関連業務（※）において他人から損害賠償請求を受けたことまたは損害賠償請求がなされるおそれがありますか？ 上記以外に、不正アクセス等を受けてその対応のために費用（原因調査、データ復旧等）を負担したことがありますか？ （※）ネットワークの所有・使用または管理、ネットワーク上の電子情報の提供	Yes		No	B
1	セキュリティポリシー、または情報セキュリティポリシーを策定している。	Yes		No	1
	上記が「YES」の場合、下記もご回答ください。				
	セキュリティ対策を所管する部門があり、監査体制も整っている。	Yes		No	
	セキュリティの社内教育・研修・訓練を定期的（年１回以上）に実施している。	Yes		No	
	パート、派遣社員等を含む使用人に、情報の取扱いに関する誓約書（情報保護の義務、そしてその義務違反時の損害賠償を定めたもの）の提出を要請している。 またはセキュリティ事故が発生した場合の、発生させた本人に対する罰則を定めた社内規定がある。	Yes		No	
2	社内ネットワーク(イントラネット)では、機密情報を区分･特定し、そのダウンロード、アクセスは特定の権限者に制限し、暗号化などで保護している。	Yes	制限のみ実施	No	2
	上記が「YES」、または「制限のみ実施」の場合、下記もご回答ください。				
	機密情報のダウンロード、アクセスについてログを一定期間保存している。	Yes		No	
3	クレジットカード（提携カードを含む）またはキャッシング機能を有するカードの発行を行っている。	Yes		No	3
4	社内ではIDカードなどの身分証明書の着用を義務づけている。	Yes	行っているが不完全	No	4
5	外来者との応対は、執務場所を通過しないようにし、かつ、応対場所はゾーニング（区分け）している。	Yes	一部実施	No	5
6	外部と接続するサーバー等には、ファイアウォールやIDSが最新の状態で導入されている。	Yes	最新ではないが導入	No	6
7	社内と社外間のネットワークへのアクセスおよび社内ネットワークから外部へのアクセスについて、最低3か月以上ログを保存し、定期的に分析・監視している。	Yes		No	7
8	パソコン、サーバーには、ウイルス対策ソフトおよびOSのセキュリティ上の脆弱性に対する修正プログラム（セキュリティパッチ）が最新の状態で導入されている。	Yes	最新ではないが導入	No	8
9	Eメールに関して、フィルタリングや暗号化を実施している。	Yes		No	9
10	ネットワーク上の通信は暗号化している。	Yes	一部実施	No	10
11	ISO/IEC15408の認証が付与されたOA機器またはシステムを導入使用している。	Yes		No	11
12	退職者のIDやパスワードを遅滞なく無効化・削除している。	Yes		No	12
13	情報セキュリティに関して外部業者による監査を定期的に(年1回以上)実施している。	Yes		No	13
14	災害や障害の発生時における業務の復旧、データのバックアップなど危機管理対策が策定されている。	Yes		No	14

質問番号	ご質問事項	ご回答内容			質問番号
15	情報の取扱いの全部または一部、または情報の廃棄処理を、外部に委託または外部から受託している。	Yes	時々ある	No	15
	上記が「YES」または「時々ある」の場合、下記もご回答ください。				
	契約書には、「秘密保持」「再委託禁止」「損害賠償」「委託終了時の返却方法」が規定されている。	Yes	一部規定	No	
16	個人情報など管理すべき情報の保管場所は、施錠管理がされており、入退室は許可者に限定され、かつ、入室者等は記録されている。	Yes	一部実施	No	16
17	情報の廃棄時には、再利用不可となるよう適切な処理を行い、その記録を保存している。 外部業者へ廃棄を委託する場合は、その外部業者から報告書を保管している。	Yes		No	17
18	ノートパソコンや、USBメモリ、DVD－R等の記録媒体に保存されたデータを社外に持ち出せないようにしている。 または、これらを持ち出す際には、第三者が容易に情報を読み取ることができないようデータの暗号化やパスワード設定するなどの対策を行っている。	Yes	一部実施	No	18
19	パソコン、サーバー上の情報について、USBメモリ、DVD－R等の記録媒体へのコピー制限、プリンタへの印刷制限、またはプリンタへの印刷時に印刷者の特定ができるソフト等を導入している。	Yes	一部実施	No	19
20	情報セキュリティ管理を委託している特定の情報セキュリティ業者がいる。	Yes		No	20
21	ウイルス情報、 不正アクセス情報、 インシデントがあった場合にIPAへの届出やJPCERTへの情報提供、その他民間企業等が推進している情報共有の仕組みへの情報提供を実施している。	Yes		No	21
22	貴社および貴社グループ企業以外の第三者が使用することを目的としたネットワーク・ECサイトは構築していない。	Yes		No	22
23	情報セキュリティに関する事故に対する、具体的な手順フローを定め、ネット遮断等を含めた対応につき、期限をもって責任者が判断する体制を構築している。	Yes		No	23
	上記が「YES」の場合、下記もご回答ください。				
	情報セキュリティに関する事故収束後の再発防止策の策定も含めて、定期的に対応訓練や演習を行っている。	Yes		No	
24	CISO（Chief Information Security Officer：最高情報セキュリティ責任者）を置いている。	Yes		No	24
25	CSIRT（Computer Security Incident Response Team）またはSOC（Security Operation Center）を構築している。	Yes		No	25
26	社内ネットワーク上にWindows－XP等、サポートが終了しているOSを使用している端末は存在しない。または存在する場合であっても、セキュリティベンダ等から提供されるアップデート・パッチ対応を遅滞なく行っている。	Yes		No	26
27	社員の私有端末の業務利用（BYOD：Bring your own device）を認めていない。 または、認めている場合であっても、顧客情報へのアクセス・保存の禁止およびその他のセキュリティ対策を十分に実施している。	Yes		No	27
28	取得している認証にチェックしてください。				28
	□ TRUSTeマーク…Webサイト・携帯サイトに関する個人情報保護の認証制度。認証付与機関は日本プライバシー認証機構。				
	□ プライバシーマーク制度…個人情報保護に関する認証制度。認証付与機関はJIPDEC（日本情報経済社会推進協会）				
	□ ISMS認証…情報セキュリティマネジメントシステムを適切に保持しているかどうかの認証制度（JIPDECが定める適合性評価制度）。				
	□ BS7799…英国規格協会による情報セキュリティマネジメントシステムに関する規格				
	SECURITY ACTION …独立行政法人情報処理推進機構が運営する情報セキュリティ対策に関する制度。				
	□ 一つ星ロゴマーク				
	□ 二つ星ロゴマーク				
29	導入しているソフトウェア・システムにチェックしてください。				29
	□ URL（WEB）フィルタリングソフト				
	□ IPS（Intrusion Prevention System）				
	□ WAF（Web Application Firewall）				
	□ C&Cサーバーとの通信を遮断する機能を有する機器・ソフトウェア				
	□ パターンファイル型のウイルス検知ソフト以外に振る舞い検知を行う機器・ソフトウェア				

A★～B★の事項は、専門事業者賠償責任保険普通保険約款に規定する「引受保険会社が保険申込書において定めた危険に関する重要な事項」であり、故意または重大な過失によって事実を告げなかった場合または事実と異なることを告げた場合は、ご契約を解除し、保険金をお支払いできないことがありますので、十分にご確認のうえご回答(記入)ください。