

サイバー・情報漏えいリスクに鉄壁の守りを

1

従業員が取引先から戻る際、書類が入ったバッグを電車内に置き忘れ、顧客情報が漏えいした。

*DDoS攻撃とは (distributed denial of service attack)

複数のコンピュータから標的のサーバーやネットワークに意図的に大量のアクセスを集中させることで負荷を与え、サービスを妨害するサイバー攻撃の一種です。

5

社内のパソコンが乗っ取られ、DDoS攻撃*に加担させられて、取引先のWEBサイトが機能停止。セキュリティの脆弱性を放置していたと取引先から収益減少分について損害賠償請求を受けた。



ホームページに掲載している写真が、著作権を侵害しているとして、無断使用による掲載期間分の使用料と事後承諾料を請求された。

6

4

業務委託先に提供していた個人情報漏えいし、委託先に対する監督が不十分であったと顧客から損害賠償請求を受けた。

9

閲覧したウェブサイトに掲載されたファイルを開きマルウェア*に感染し、顧客情報が漏えいした。原因・被害範囲の調査費用、データの復旧費用、不正なプログラムの除去費用および再発防止のためのコンサルティング費用を支出した。

◆マルウェアとは

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です。遠隔地のコンピュータに侵入したり攻撃したりするソフトウェアや、ウイルスのようにコンピュータに侵入して他のコンピュータへの感染活動や破壊活動を行ったり、情報を外部に漏えいさせたりする有害なソフトウェアを指します。メールでの攻撃、ウェブサイトでの攻撃を受けることによりマルウェアに感染します。

ネットワークセキュリティ運用管理会社から、不正アクセス*の可能性があると通報を受けた。不正アクセスの有無の調査を外部に依頼したところ、不正アクセスは無かったと判明したが、パソコン1台につき100万円の調査費用が発生した。

調査費請求
100万円

8

★不正アクセスとは

本来アクセス権限を持たない者がサーバーや情報システム内部へ侵入することです。インターネットは世界中とつながっているため、世界中のどこからでも行われる可能性があり、不正アクセスへの対策は必須です。不正アクセスの結果として、サーバーや情報システムの停止・重要な情報の漏えいなど、企業・組織の業務のみならずブランドイメージにもダメージを及ぼします。

3

社員のプライベートパソコンがウイルスに感染していたが、気付かずにUSBを使用して、会社のパソコンにデータを移行、社内パソコンがウイルスに感染し、顧客情報が盗み取られた。

7

カフェで仕事していた社員のパソコンを背後の席から盗み見られ、ネット上で情報が流出。顧客のセンシティブ情報が漏えいした。

2





サイバー攻撃のリスクは、発見前から始まっています!

〈サイバー・情報漏えい事故補償特約〉の特長

- 特長1** 情報漏えい等の事故が実際に発覚する前の、調査段階から費用を補償します!
 - 特長2** 万が一、情報漏えいや取引先の営業妨害が発生した場合でも、原因調査→訴訟対応→損害賠償→再発防止の費用まで、トータルで補償します!
- 日々進化するサイバー攻撃に対して、迅速な初動対応が可能となり、ウイルス感染等による取引先の営業妨害や、個人情報の漏えい等の事故や被害の拡大を防止できます!
- 万全なセキュリティ対策でも、日々進化するサイバーリスクをゼロにすることはできません。

サイバー・情報漏えい事故補償特約の概要

例

セキュリティ監視サービスにより、不正アクセスのおそれを検知したため、外部業者に調査を依頼。サイバー攻撃があったことが判明し、顧客情報2,000件が流出していたため、インターネット上で当該事実を公表した。



ご注意

上記の事例の場合に保険金をお支払いできる補償概要を掲載しています。ケースによりお支払いする金額等は変わりますので、詳しくはピサポパンフレットをご参照いただくか、取扱代理店または弊社へお問い合わせください。



検知	初動対応	対応	事態收拾 争訟対応(弁護士費用等) 損害賠償	再発防止	損害賠償責任に関する補償	支払限度額 ^(※1) (1請求・保険期間中)
	影響調査・初動対応	原因・被害調査			被保険者が法律上の損害賠償責任を負担することによる損害を補償します。	3億円
		データ復元・サイト復旧			各種費用に関する補償^(※3) ①不正アクセス等対応費用 不正アクセス等の有無の確認費用、不正アクセス等確定後のネットワークの遮断費用を補償します。 ②原因・被害範囲調査費用 事故の原因・被害範囲の調査費用等を補償します。 ③相談費用 弁護士費用、コンサルティング費用を補償します。 ④データ等復旧費用 消失したデータの復元費用、改ざんされたウェブサイトの復旧費用を補償します。	3,000万円
			コールセンターの設置、記者会見、見舞金支払い		⑤その他事故対応費用 コールセンターの設置、記者会見、見舞金支払い等、事態の收拾に係る費用を補償します。	3,000万円 うち、見舞金費用 被害者が個人の場合:500円(1名) 被害者が法人の場合:5万円(1法人)
				再発防止策の計画・実行	⑥再発防止費用・不正プログラム除去費用 事故の再発防止に係る費用を補償します。(外部機関による認証取得のための費用等)	10万円
			訴訟対応		⑦訴訟対応費用 損害賠償請求訴訟に対応するために必要な費用(意見書・鑑定書の作成費用等)を補償します。	3,000万円

(※1) 保険契約においてお支払いする保険金の額は、すべての保険金を合算して、損害賠償責任に関する補償で設定された保険期間中支払限度額または3億円のいずれか低い額が限度となります。
(※2) 各種費用の支払限度額は、費用全体での支払限度額(最大3,000万円)の内枠で適用されます。
(※3) 各種費用については、弊社の同意を得て支出したものに限りま。

サイバー緊急連絡先 (専門事業者のご紹介)

万が一不正アクセス等のおそれがあった場合に、被害範囲の確認や原因調査について、専門事業者が対応します。

事業者	サービス名称	緊急連絡先	ホームページ
株式会社ラック	緊急対応サービス「サイバー119」	0120-362-119	https://www.lac.co.jp/
株式会社サイバーディフェンス研究所	フォレンジック調査/インシデント対応サービス	03-5843-9015	https://www.cyberdefense.jp/
セコムトラストシステムズ株式会社	セコムプロフェッショナルサポート	0120-39-0756	https://www.secomtrust.net/

専門事業者により、一部サービスをご提供できない場合があります。サービスの詳細については専門事業者のホームページをご確認ください。なお、サービスの内容は予告なく変更・中止となる場合があります。

※左記は専門事業者のご紹介であり、ご契約者様ご自身で記載されていない専門事業者をご選定いただくことに問題はありません。

支払限度額に関するご注意

- 調査の結果、不正アクセスがなかった場合は、外部からの通報により調査を開始した場合のみ、お支払いの対象となりますが、縮小支払割合90%が適用され、かつ、支払限度額は200万円となります。
 - 調査の結果、不正アクセスがあった場合で、不正アクセス等についての事実の公表を行わないときは、縮小支払割合90%が適用され、かつ支払限度額は200万円となります。
- ※ネットワークのセキュリティ運用会社や公的機関をいいます。

※このチラシはピサポ(統合賠償責任保険)にセットされるサイバー・情報漏えい事故補償特約のごく簡単な説明を記載したものです。保険金の支払条件その他この特約の詳細につきましては、約款をご覧ください。また、実際の契約内容は申込書等をご確認ください。特にご注意いただきたい事項を、重要事項説明書に記載しておりますので、ご契約前に必ずご確認ください。
※保険金をお支払いできない場合やお支払いする保険金の制限額があります。詳細につきましては、取扱代理店または弊社にご照会いただくかご契約の約款をご参照ください。

日新火災海上保険株式会社

本店/〒101-8329 東京都千代田区神田駿河台2-3 TEL03(3292)8000(大代表)
お客さま相談窓口 フリーダイヤル 0120-17-2424 [9:00~17:00(土日祝除く)]
ホームページアドレス https://www.nisshinfire.co.jp/

万一事故にあわれたら サービス24時間・365日 フリーダイヤル 0120-25-7474

代理店・営業担当
●安心のトータルライフプランをお手伝い。お気軽にご用命ください。

※1 このサービスは、お客さまと専門事業者との間で締結される委託契約に基づき有償で提供されるものです。保険の付帯サービスではありません。
※2 サイバー・情報漏えい事故補償特約をセットされている場合のみ。保険金のお支払対象となる費用については、取扱代理店または弊社までお問い合わせください。