企業経営者の皆さまへ

2024年1月1日以降始期契約用

強固なセキュリティを構築しても、
サイバーリスクを完全に排除するのは困難。
起きたセキュリティ事故の損害賠償。
十分に対応できる備えがありますか。

1契約で包括的に補償「**サイバーリスク保険**」のご案内

To Be a ***Good Company***

サイバー攻撃への備えは大丈夫ですか?

サイバー攻撃による主な被害

マルウェア感染

●標的型メール攻撃

正当な業務や依頼を装ったメールの添付ファイルに不正プログラムを仕掛けておき、添付ファイルを開いたり、リンク先に遷移したりすることでマルウェアに感染させる方法です。

ウェブサイトの改ざん

●不正アクセス

企業のネットワークを守る情報セキュリティを通過したり、ソフトウェア等の開発時の欠陥を悪用したりすることで、外部から不正にネットワークへ侵入する行為です。一度ネットワークに侵入されてしまうと、権限を有しない第三者にウェブサイトを書き換えられてしまうおそれがあるほか、不正プログラムを埋め込まれてしまうおそれがあります。

個人情報・法人情報の窃盗

●なりすまし

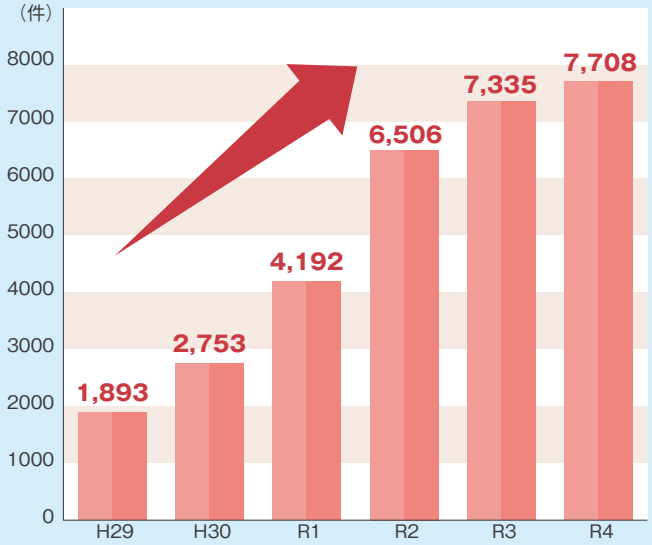
他者のIDやパスワードを使用して他者になりすまし、企業が所有する様々な情報を盗み出すもの。企業の社員になりすますことで、本人以外の情報や取引先の企業に関する情報まで盗まれてしまうケースもあります。

業務妨害

●DoS攻撃

企業や組織が運営するサービスやシステムに大量のデータを送り込み、過剰な負担をかけ利用不能にする攻撃です。自社が攻撃を受け、そのサービスやシステムが利用不能になるだけでなく、それらを利用する他人の事業が阻害されるケースもあります。

警察のセンサー(*)に対する不正アクセス件数(1日あたり)



出典)警視庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について」
(*)警視庁が24時間体制で運用しているリアルタイム検知ネットワークシステムにおいて、インターネットとの接続点に設置しているセンサーをいいます。

たとえばこんな事故が…

事故例

情報通信事業者であるA社の業務用パソコン数台が**不正なプログラム(マルウェア)に感染していることが判明**した。感染したパソコンからは、同社の顧客情報が漏えいしている可能性があり、A社は、自社のホームページ上で、情報漏えいのおそれがあることについて外部に公表した。同時にA社は、その原因や影響等について調査を実施するために、専門業者へ相談を開始した。
調査の結果、**約10万人分の個人情報が外部に漏えい**していることが判明した。同社は企業イメージ損失の拡大を防止するために、外部機関に緊急対応のコンサルティングを依頼し、被害者へのお詫び状の送付等の対応を行ったが、情報が漏えいした一部の顧客から、**プライバシーの侵害を理由に損害賠償請求訴訟を提起**された。

支出

●被害状況の把握	100万円
●原因調査・証拠保全の実施	1,100万円
●謝罪、会見等の実施コンサルティング	200万円
●見舞金支払い(1名500円)	5,000万円
●謝罪広告費用	500万円
●損害賠償金	1億円
●争訟費用	300万円

合計 1億7,200万円

東京海上日動の「サイバーリスク保険」なら“まとめて”補償できます!

- **損害賠償責任リスク**(損害賠償金、争訟費用等)
- **危機管理対応リスク**(サイバー攻撃対応費用、コンピュータシステム復旧費用、再発防止費用等)
- **情報漏えいリスク**(見舞費用、コールセンターの設置費用等)
- **事業中断リスク**(オプション)(喪失利益、営業継続費用等)

補償を一本化!

このご案内書は、サイバーリスク保険の概要をご紹介したもので、サイバーリスク保険に関するすべての事項を記載しているものではありません。保険の内容は企画書等をご請求の上、ご確認ください。詳細は、保険約款およびセットされる特約条項によりますが、ご不明な点がありましたら、ご遠慮なく代理店または東京海上日動までお問い合わせください。ご契約に際しましては必ず保険約款および重要事項説明書をご確認ください。

【取扱代理店】

【引受保険会社】
東京海上日動火災保険株式会社

【担当課支社】

1760-ER04-14027-202310