To Be a Good Company

サイバーセキュリティ・リスクへの対処について

2021年7月26日
東京海上日動火災保険株式会社
企業商品業務部　九州グループ

【ご注意】
本資料では、保険の補償内容につき、概要のみを記載しています。保険の内容の詳細につきましては、代理店または東京海上日動までお問い合せください。

TOKIO MARINE NICHIDO
東京海上日動

本日の流れ

1 サイバーリスクを取り巻く環境

2 保険による備え

3 自社のリスクを認識する

1. サイバーリスクを取り巻く環境

直近のサイバー関連ニュース

2021年	（新聞記事の見出しより一部編集して抜粋）
5月28日	市立病院で新型コロナ感染者21名の検査情報を誤送信
5月24日	フリマアプリのソースコードから顧客情報など約2万8千件流出か
5月24日	お見合いアプリが不正アクセス被害、免許証データなど約171万件流出
5月21日	国内大手電機メーカーのグループ会社、欧州子会社がサイバー攻撃被害
5月21日	着物クリーニング会社が運営するサイトにシステム脆弱性、565名のカード情報流出か
5月20日	オンラインショップを運営する会社にて、リスト型攻撃で41件のアカウントに不正ログイン
5月20日	スマホゲーム「ブルーアーカイブ」にDDoS攻撃、臨時メンテへ

出典：Cyber Security.com（https://cybersecurity-jp.com/leakage-of-personal-information#news）

日々サイバーインシデントが発生し、報道されています！

情報セキュリティに関する事故の動向

アンケート調査によると、企業の約３社に１社は情報セキュリティに関する事件・事故を過去１年以内に経験しており、サイバー攻撃はいまや身近な犯罪といえます。

Q. 過去1年間で発生した情報セキュリティに関する事件・事故はありますか？

1 位	2 位	3 位	4 位	5 位
電子メールなどの誤送信	**標的型メール攻撃**	**ランサムウェアによる金銭等の要求**	**マルウェア感染**	情報機器等の紛失・置き忘れ
				
35.6 %	*34.1 %*	*32.5 %*	*31.0 %*	*28.9 %*
ヒューマンエラー	サイバー攻撃	サイバー攻撃	サイバー攻撃	ヒューマンエラー

1 年間で約2倍！

出典：NRIセキュアテクノロジーズ『企業における情報セキュリティ実態調査2017』

豆知識

サイバー攻撃等による情報セキュリティ事故の発生率は、自動車事故よりも高いと言われています。

情報セキュリティ事故の発生率

16%

＞

自動車事故の発生率

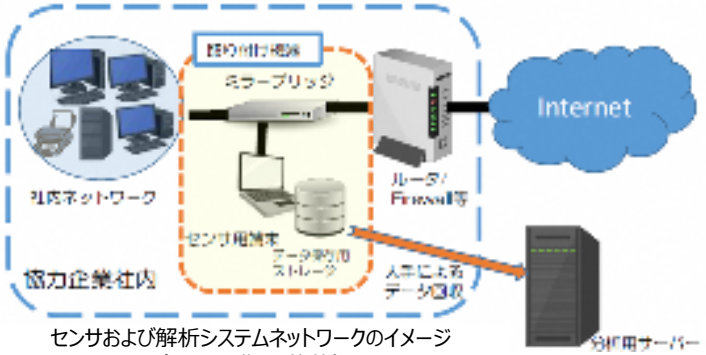
12%

出典：IPA『中小企業の情報セキュリティ対策ガイドライン』

中小企業も標的に

平成30年度 中小企業に対するサイバー攻撃実情調査（2019年7月3日）

大阪商工会議所と神戸大学、東京海上日動火災は、2018年9月から約4カ月間にわたり、製造業や小売業など30社に専用の機器を設置し、中小企業を狙ったサイバー攻撃の実態を調査した。



センサおよび解析システムネットワークのイメージ
（下記出典より抜粋）

調査の中間報告では、**機器を設置した30社すべてが、外部の第三者からのサイバー攻撃を受けている**ことが発覚した。

さらに、**そのうちの複数社では、悪意のあるサイトとの間で、データのやりとりが繰り返し行われており**、知らぬ間に、中小企業が抱える内部の情報が流出したおそれがあることがわかった。

出典：大阪商工会議所『平成30年度 中小企業に対するサイバー攻撃実情調査（報告）』および記者発表資料をもとに作成

サイバー攻撃は、中小企業にとっても他人事ではありません。
これらに備えるため、保険によるリスクヘッジをご検討ください。

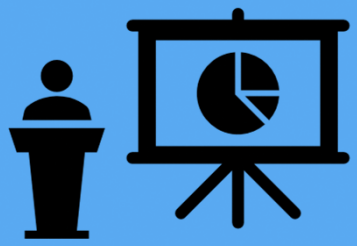
出典　Tokio Cyber Port：
https://tokiocyberport.tokiomarine-nichido.co.jp/cybersecurity/s/CyberAttacks

（ご参考）サイバーリスクチェックシート

中小企業でも、以下に１つでも該当する場合は**要注意**です！

チェック項目	業種の例
☑ 自社ホームページを持っている	その他サービス業 飲　食　業 小　売　業
☑ 取引先とメールでやりとりすることがある	製　造　業 建　設　業 運　送　業
☑ 取引先の機密情報を取り扱っている	デザイン・広告業 製　造　業 設計事務所
☑ ネット通販等でクレジットカード決済を導入している	食品製造業 小　売　業
☑ お客様・従業員のセンシティブ情報やマイナンバーを扱っている	全　業　種

2. 保険による備え

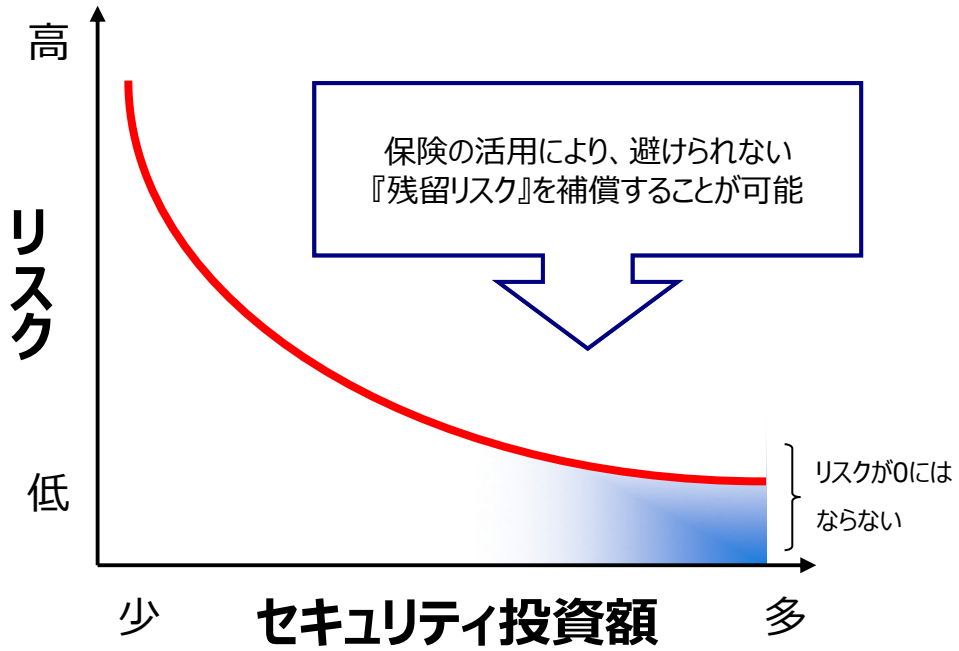


超ビジ・サイバー補償／サイバーリスク保険の意義

Part 2

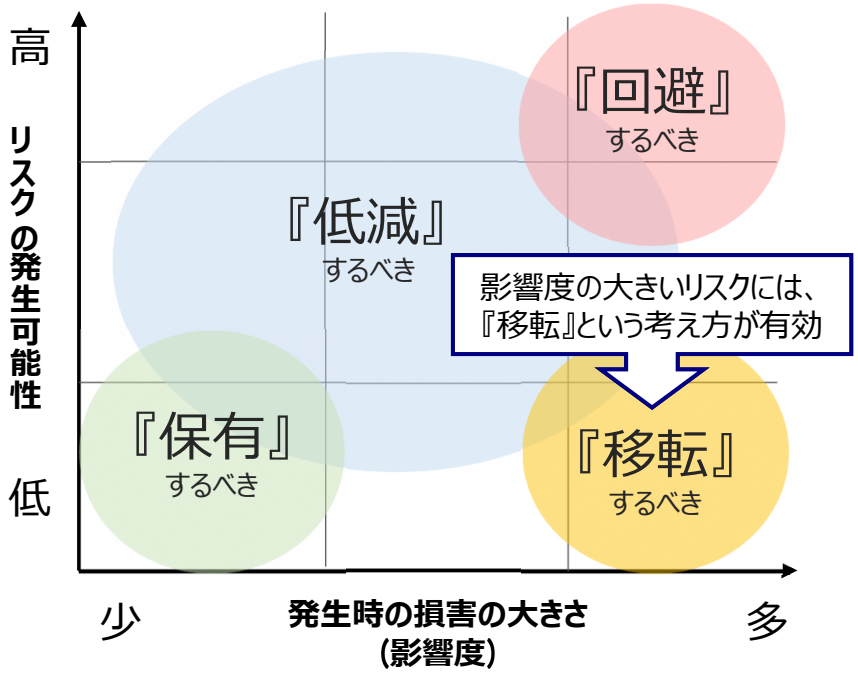
リスクマネジメントの選択肢の１つとして、保険の活用は有効な手段です。

＜リスクとセキュリティ投資額の関係＞



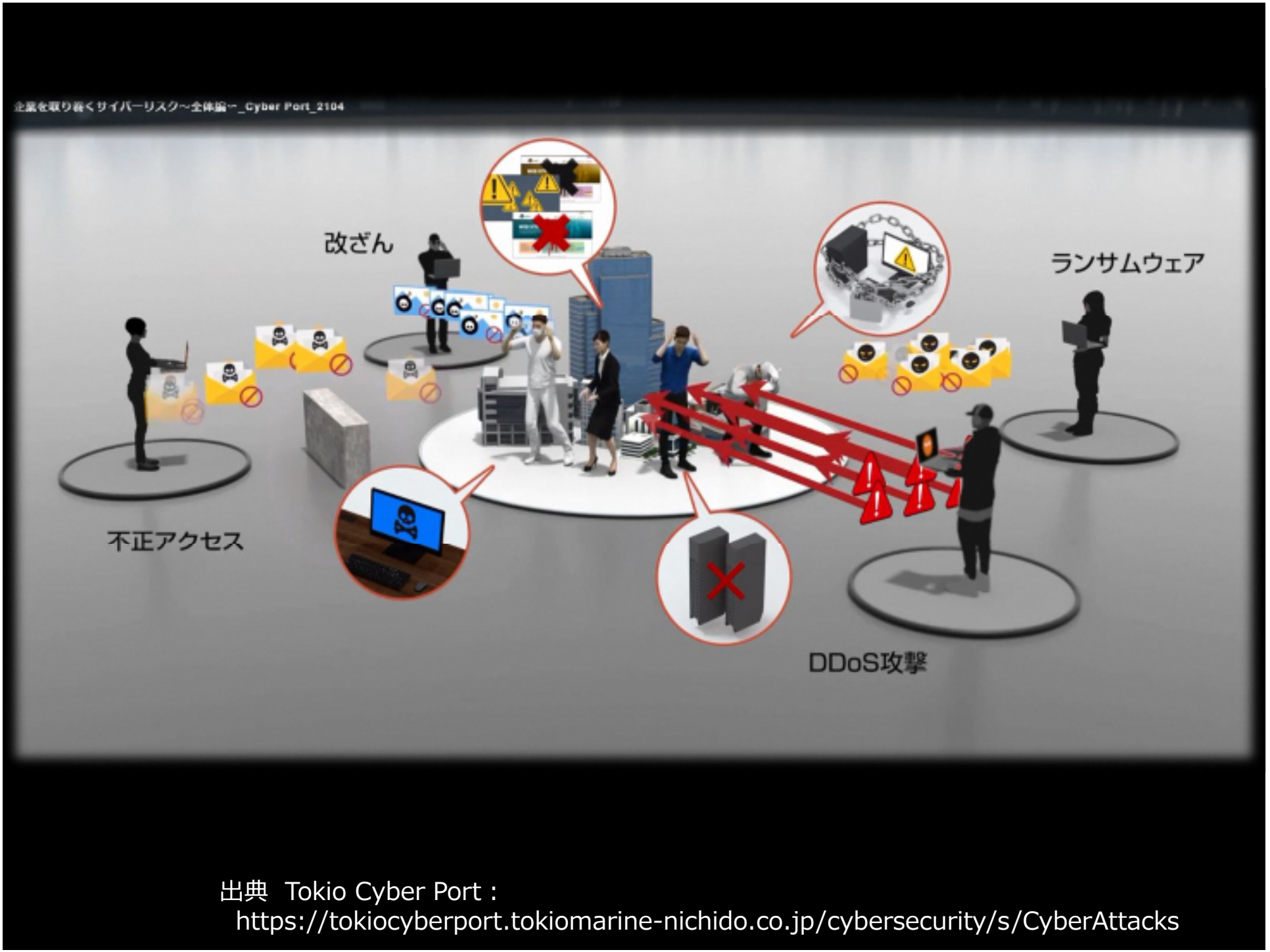
✓ どれだけセキュリティ対策に投資をしても、サイバーリスクをゼロにすることはできないといわれています。

＜リスクコントロールの考え方＞



✓ リスクの発生可能性を下げたとしても、発生した場合の影響が大きいリスクに対しては、**リスクの『移転』**が有効です。

✓ 超ビジ・サイバー補償／サイバーリスク保険は、リスクの『移転』に効果的な手段です。



出典　Tokio Cyber Port：
https://tokiocyberport.tokiomarine-nichido.co.jp/cybersecurity/s/CyberAttacks

（ご参考）各種費用の相場

サイバー攻撃の被害状況によっては、
費用だけで数百万円にのぼる可能性があります。

費用	相場
フォレンジック費用 ※ネットワーク機器やサーバのアクセスログ、あるいはコンピュータ上にあるファイルから不正アクセスの有無、影響箇所・範囲の特定を行い、原因、被害調査等の対応を行うことを指します。	約100万円/台
ウェブサイト新規作成費用 （ウェブサイトがウィルス感染し、新規で作成し直す費用）	約80万円
セキュリティ強化費用 （セキュリティ対策ソフト導入費用）	約7,000円/台
不正プログラム除去費用	約１万円/台

※上記金額は一例であり、実際の金額は被害状況等により異なります。

（ご参考）各種費用の相場

パソコンのフォレンジック調査費例

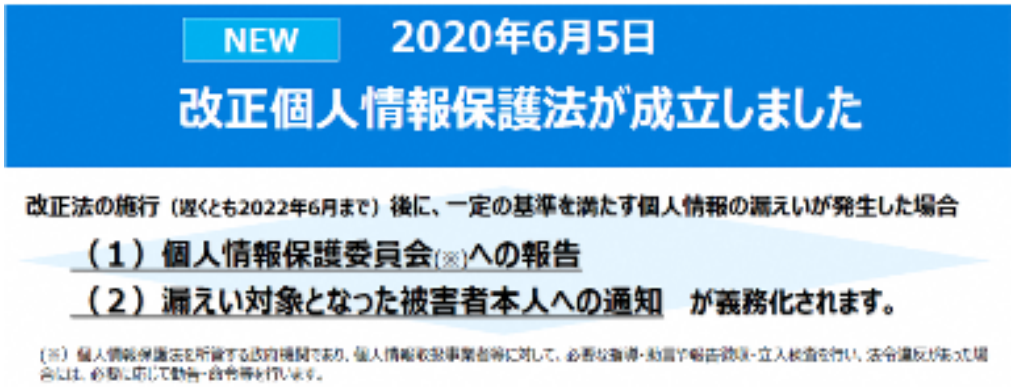
1.保全準備費			
	正常なHDD、SSD	**40,000**	（1個当たり）
	RAID構成	**30,000**	（×媒体数）
	故障、破損したHDD、SSDの検査	**40,000**	（1個当たり）
2.基本技術料			
	パソコン （HDD、SSDなど）	**150,000**	（1台当たり）
	サーバー （ファイル、メール、グループウェアなど）	**300,000**	（1台当たり）
	外部記憶媒体 （USBメモリ、デジカメなど）	**50,000**	（1個当たり）
	故障、破損したHDD、SSDや外部記憶媒体	別途見積	
3.各種調査費			
データ解析	Officeデータ	**50,000**	
	画像データ	**50,000**	
	動画データ	**50,000**	
	メール	**50,000**	
	その他	**50,000**	
特定ログ解析	ユーザー利用履歴	**50,000**	
	デバイス利用履歴	**50,000**	
	WEB閲覧履歴	**50,000**	
	メモリ解析	**50,000**	
	その他	**50,000**	
4.特殊調査費			
	1～3では対応できないもの	**200,000**	

＊ 調査の個別性が高いため、多くの調査会社では個別相談のうえでお見積り作成という流れを取っているようです。

出典 株式会社くまなんピーシーネット Webサイト（https://www.kumanan-pcnet.co.jp/forensic/service/forensic-pc.php）

（ご参考）法規制の強化

【個人情報保護法の改正スケジュール】
◆2020年6月5日：改正個人情報保護法が成立
◆**2022年4月1日：施行期日**
※個人情報保護委員会HPより（一部施行済み）



実務における影響
…「報告」や「通知」を実施しようとすると…？

- フォレンジック（原因調査）費用がかかる！
- 通知費用がかかる！

改正法を踏まえた業務フローの見直しと、
個人情報漏えい時への備えをご検討ください！

（1）個人情報保護委員会への報告	（2）漏えい対象となった被害者本人への通知
• 社内外の関係者と連携し、情報漏えいの事実関係の確認、影響範囲を特定 • フォレンジック調査による情報漏えいの原因調査 （例：サーバー1台あたり 約500～1,000万円の費用） • 個人情報保護委員会への報告書の作成　等	• 情報漏えいの被害者の特定および連絡先（住所、メールアドレス等）の確認 • 通知内容および通知方法の検討 • 郵送またはメール等による通知の実施

３．自社のリスクを認識する

Tokio Cyber Portについて

ニュース・コラム

最新ニュース

国内の様々なメディアが発信するニュース記事の中から、サイバーに関連する最新ニュースをAIによって自動的に収集し、デイリーで掲載しています。

記事コラム

サイバーセキュリティに関する役立つ情報を様々なテーマで定期的に更新しています。専門家による事例紹介などをご提供しています。

無料セキュリティサービス

標的型攻撃メール訓練*

ウイルス対策だけでは完全に防ぐ事が難しい「標的型攻撃メール」の訓練を最大10名まで実施することができます。

サイバーセキュリティ・外部診断*

会員登録時に登録いただいたメールアドレスのドメインを対象に、外部視点から企業・組織のサイバーセキュリティリスクを10のリスクファクターごとに5段階で評価・スコアリングします。

予想損失額シミュレーション*

設問項目に入力いただいた内容と、弊社作成のシナリオに基づき、サイバー攻撃による被害が生じた場合の「予想損失額」を算出します。

トラブル発生時の電話相談*

期間限定

期間限定でウイルス感染やネット接続不具合等のトラブルに対して、初期アドバイスやリモートサポートを行います。

お役立ち情報

事故対応マニュアル*

Cyber Risk Journal*

従業員実践テキスト*

用語集

※最新ニュース、記事コラム、用語集は会員登録なしで利用できます。

「Tokio Cyber Port」無料セキュリティサービス

簡単な会員登録をすることで、無料で各種診断・訓練サービスを受けることが可能です！

【ご用意しているコンテンツ】

① サイバーセキュリティ・外部診断
② 標的型攻撃メール訓練
③ 予想損失額シミュレーション

サイバーセキュリティ・外部診断*

会員登録時に登録いただいたメールアドレスのドメインを対象に、外部視点から企業・組織のサイバーセキュリティリスクを10のリスクファクターごとに5段階で評価・スコアリングします。

標的型攻撃メール訓練*

ウイルス対策だけでは完全に防ぐ事が難しい「標的型攻撃メール」の訓練を最大10名まで実施することができます。

予想損失額シミュレーション*

設問項目に入力いただいた内容と、弊社作成のシナリオに基づき、サイバー攻撃による被害が生じた場合の「予想損失額」を算出します。

「Tokio Cyber Port」その他のコンテンツ

会員登録をすると多彩なサービスを受けることが可能です。

緊急時ホットライン
サービスと同内容です！

【トラブル発生時の電話相談】
サイバーリスクに関するトラブルのご連絡・ご相談を日本全国どこからでも受け付けるサービス。サイバーリスク保険の加入者に提供しているサービスで、登録から期間限定（10カ月間）で提供。

トラブル発生時の電話相談*

期間限定

期間限定でウイルス感染やネット接続不具合等のトラブルに対して、初期アドバイスやリモートサポートを行います。

Cyber Risk Journal*

サイバーリスクの最新動向や企業が取り組むべき対策等を紹介する情報誌「Cyber Risk Journal」をダウンロードいただけます。

従業員実践テキスト*

サイバー攻撃に対する知識を習得し、サイバーリスクを低減するための従業員の実践内容を紹介したテキストをダウンロードいただけます。

事故対応マニュアル*

情報漏えい等の事故が発生した場合の対応について、誰が何をするべきか、フェーズごとのポイントをまとめたマニュアルをダウンロードいただけます。

用語集

サイバー攻撃やサイバーセキュリティに関する用語を分かりやすく解説しています。

※用語集の利用は会員登録不要です。

最後に

情報セキュリティに関する事故は規模・業種を問わず発生していることを認識しましょう。

万が一の際は多額の費用が発生します。備えをご検討ください。

Tokio Cyber Portを活用し、自社のリスクを正しく認識することから始めてみましょう！

ご清聴ありがとうございました。

東京海上日動火災保険株式会社