Innovation for Wellbeing
SOMPOリスクマネジメント

NEWS RELEASE

2019年12月5日

「BCMコンサルティング」の拡充

BCMとサイバーセキュリティ技術の専門コンサルタントによる合同チームを結成し サイバー攻撃を想定したBCM体制構築を支援

ＳＯＭＰＯリスクマネジメント株式会社（本社：東京都新宿区、代表取締役社長：布施 康、以下「ＳＯＭＰＯリスク」）は、従来から提供している「BCMコンサルティング」について、新たにサイバー攻撃を想定したコンサルティングサービス（以下「本サービス」）を追加し、12月5日から、本サービスの提供を開始します。

1. 背景

日本国内・海外で頻発しているサイバー攻撃への意識を高めるために、経済産業省等によって「サイバーセキュリティ経営ガイドライン」(*1)が公開され、民間企業や公的機関でのサイバーセキュリティへの取組みは活発化しています。しかし、サイバー攻撃よる事故は後を絶ちません。

民間企業等のなかには、サイバーセキュリティ対策について、侵入防止の技術的対策だけを重視したりサイバー攻撃が組織のシステム部門で対処すべき取組みであると認識することが多くサイバー攻撃を受けた後の全社的な危機対応・事業継続の観点を十分に考慮できていないケースもあり、ＳＯＭＰＯリスクはお客さまからこうした状態を改善したいとのご相談を多く受けています。

ＳＯＭＰＯリスクは、自然災害などの危機時の事業継続を目的としたコンサルティングを行ってまいりましたが、このような背景を踏まえて、このたび、新たにBCMとサイバーセキュリティ技術の専門コンサルタントからなる合同チームを結成し、本サービスの提供を開始することとしました。

*1 経済産業省と独立行政法人情報処理推進機構が、経営者のリーダーシップの下で企業のサイバーセキュリティ対策を推進するために定めたもので、平成29年11月にVer2.0が発行されています。

2. 本サービスの内容

ＳＯＭＰＯリスクの専門コンサルタントが、お客さまのサイバーセキュリティ態勢のアセスメントを実施し、そこで確認された問題点や脆弱性の解決に向けた改善策を総合的に提案し、支援します（各メニューの概要は＜別紙＞をご参照ください）。

（主なメニュー）

①サイバーセキュリティ態勢アセスメント
②サイバー攻撃想定BCP（事業継続計画）策定
③サイバー攻撃想定対応演習

（1）特長

①BCMとセキュリティ技術の専門コンサルタントからなる合同チームがプロジェクトを進行し、全社的な危機対応・事業継続およびサイバーセキュリティに関する技術の両面から実効性の高いBCP等の成果物を策定します。

SOMPOリスクマネジメント株式会社
総務部　160-0023　東京都新宿区西新宿　1-24-1　Tel:03-3349-4330　http://www.sompo-rc.co.jp

②サイバーセキュリティ態勢アセスメントを先行して行うため、BCP 策定、演習のコンサルティングだけではなく、防御策等のソリューションの提案も可能です。

(2) 費用・期間(*2)

【1】費用
500 万円（税抜）～

【2】期間
6 か月～12 か月

*2 メニュー①、②、③全てを実施した場合を想定した費用です。

3. 受注目標

年間 10 件、5,000 万円の受注を目指します。

4. 今後の展開

ＳＯＭＰＯリスクは引き続きサービスレベルの向上、サービス内容の拡充に取り組み、日々高度化・巧妙化するサイバー攻撃から企業をお守りすべく、お客さまの安心・安全・健康に資する最高品質のサービスを提供してまいります。

ＳＯＭＰＯリスクマネジメントについて

ＳＯＭＰＯリスクマネジメント株式会社は、損害保険ジャパン日本興亜株式会社を中核とするＳＯＭＰＯホールディングスのグループ会社です。「リスクマネジメント事業」「サイバーセキュリティ事業」を展開し、全社的リスクマネジメント（ERM）、事業継続（BCM・BCP）、サイバー攻撃対策などのソリューション・サービスを提供しています。

サービス内容に関するお問い合わせ先

ＳＯＭＰＯリスクマネジメント株式会社
リスクマネジメント事業本部 事業開発部［担当：末岡］
サイバーセキュリティ事業本部 サービス推進部［担当：西出・木村］
〒160-0023 東京都新宿区西新宿 1-24-1 エステック情報ビル
TEL：03-3349-4226（直通）

報道機関の方からのお問い合わせ先

ＳＯＭＰＯリスクマネジメント株式会社
総務部［担当：田所］
〒160-0023 東京都新宿区西新宿 1-24-1 エステック情報ビル
TEL：03-3349-4330

以上

＜別紙＞本サービスの各メニューの概要

メニュー	内容
① サイバーセキュリティ態勢アセスメント	・サイバーセキュリティで整備すべき対策（防御策、CSIRT(*3)、ガバナンス）についてヒアリングします。 ・ヒアリングで CSIRT、ガバナンスに関する問題点が確認された場合、以下の②もしくは③のメニューを継続して提供します。 ・防御策等のソリューションについては必要に応じて別途提案します。
② サイバー攻撃想定 BCP（事業継続計画）策定	・①のアセスメント結果を参考に、お客さまのシステムおよびネットワーク環境がサイバー攻撃を受けた場合の最悪のシナリオを設定します。 ・このシナリオにおいても会社として継続すべき重要業務を抽出し、これらを実行するための体制や行動手順を BCP として整理していきます。
③ サイバー攻撃想定対応演習	・②で設定したシナリオを前提とし、BCP に定めた行動手順が実際に機能するか関係者が集まり机上で検証します。

*3 Computer Security Incident Response Team の略で、コンピュータセキュリティに係るインシデントに対処するための組織の総称（機能）です。具体的には、平時においては、インシデント関連情報、脆弱性情報および攻撃予兆情報を収集して対応方針や手順の策定等の活動を実施し、有事においては、インシデント発生時に迅速かつ適切な判断を行います。