

リスクアセスメントサービス

サイバーセキュリティリスクから守るべき情報資産を明確化したうえで、現状の脅威と脆弱性を評価し、効果的かつ効率的な対策の推進を支援

リスクアセスメントから始めるサイバーセキュリティ

昨今、サイバー攻撃は急増、高度化の一途を辿っており、企業や組織はかつてないほどのリスクにさらされています。また、あらゆるものがネットワークに接続される社会になったことで、IoT機器をはじめ、従来はサイバーセキュリティ対策がそれほど意識されてこなかった制御システム等を含めた、より多様で広範な領域におけるサイバーリスク対応が必要になっています。そのような状況においてサイバーリスク対応を効果的かつ効率的に行うためには、企業や組織のなかで最もクリティカルな業務や情報資産を特定したうえで、それらに対して最新の脅威を踏まえた詳細なリスク分析を行い、現状対策の課題を抽出するリスクアセスメントアプローチが不可欠です。富士通総研は、当該アプローチによるリスクアセスメントサービスにより、企業や組織のクリティカルなサイバーセキュリティリスクの把握、及び、それらのリスクへの予防（防御）と有事への備え（検知・対応）の最適化を実現します。

富士通総研は、サイバーセキュリティ分野の専門的知見と多くの企業・組織へのコンサルティングで培ったナレッジをもとに構築した独自のアセスメントフレームワークを活用し、貴社／貴組織におけるサイバーセキュリティリスクの可視化・評価を支援します

リスクアセスメントサービスの内容

リスクアセスメントサービスでは、大きくは下記の2つのSTEPにより、組織のサイバーセキュリティリスクを明らかにします。STEP1では、自組織のビジネス状況を俯瞰的に整理したうえで業務観点でのリスク特定を行います。STEP2では、重要な情報資産のリスクを詳細分析し、端末／サーバー／ネットワーク等の領域、技術的／非技術的対策など、多面的な視点から、サイバーセキュリティ上の現状課題を明らかにします。

STEP 1 : ビジネスリスク分析

STEP 2 : ICTリスク分析

	STEP 1 : ビジネスリスク分析	STEP 2 : ICTリスク分析
インプット	<ul style="list-style-type: none"> 社内組織図及び職務分掌資料等 サービス・業務プロセス関連資料等 	<ul style="list-style-type: none"> STEP1アウトプット及び関連資料等 システム概要、ネットワーク概念図、リスクアセスメント調査票 ※裏面参照
作業概要	<p>組織の事業・サービスがどの業務で構成され、どのシステムが利用されているかを棚卸し。具体的には、バリューチェーン観点でサービス提供までの構成要素を鳥瞰図として整理し、クリティカルな業務・情報システムを仕分けする。</p>	<p>重要なシステムを明らかにした後は、対象システムがそれぞれどんな脅威に曝される可能性があるのか、脅威に対する脆弱性、すなわち、リスク対策状況を分析する。</p>
アウトプット	<ul style="list-style-type: none"> 業務鳥瞰図（バリューチェーン視点で整理）※裏面参照 重業業務・情報資産一覧、等 	<ul style="list-style-type: none"> 情報資産ごとのリスク評価結果及び課題一覧、等

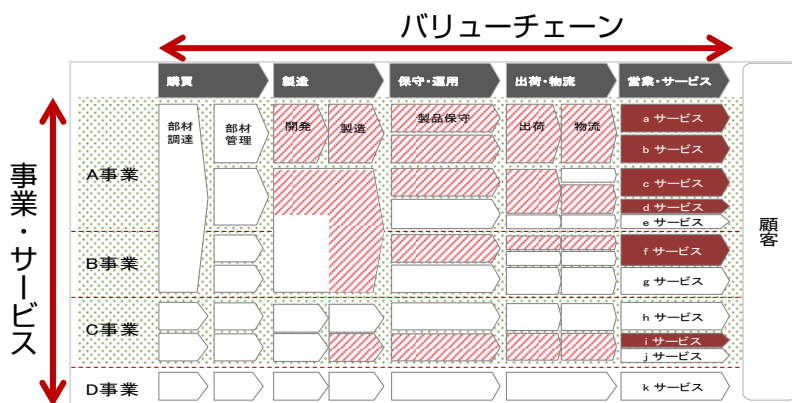
リスクアセスメントサービスの進め方（一部）

■ ビジネスリスク分析：バリューチェーン視点での業務鳥瞰図

バリューチェーン分析（事業活動を構成する機能の連鎖を整理し、どの機能で大きな付加価値が生まれているのか等について分析）を応用した業務分析手法により、今まで見えていなかった業務や情報システムの存在を俯瞰的に把握し、顧客提供価値の視点から重要な情報システムを特定します。

富士通総研独自のノウハウをもとに構築した業務分析フレームワークを用いて、企業や組織における顧客への製品・サービス提供までの構成要素（業務）を鳥瞰図で整理・可視化し、事業経営やリスクアセスメントの目的の観点から重要なサービス・業務、及び、当該業務の遂行に必要な情報資産（システムやデータ）の把握・仕分けを行います。ここ（STEP 1）で明確化した重要な情報資産に対して、STEP 2でICTリスク分析を行います。

＜バリューチェーン視点での業務鳥瞰図による整理（イメージ）＞

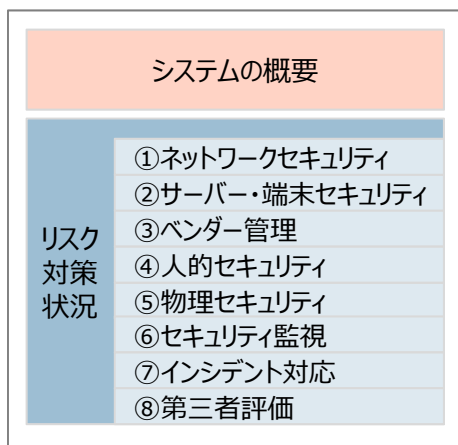


■ ICTリスク分析：リスクアセスメントフレームワーク（調査票）

富士通総研が有するサイバーセキュリティ分野の専門的知見と、IPA等各機関のセキュリティガイドライン等の要求事項を体系的に集約したアセスメントフレームワーク（調査票）を活用。調査票の項目に沿ったインタビューにより、情報システムのリスク・対策状況を可視化・評価し、課題を明確化します。

昨今、サイバーセキュリティ対策の必要性が注目されている制御システムへの適用を図るため、情報処理推進機構（IPA）発行「制御システムのセキュリティリスク分析ガイド」をはじめ、各種セキュリティ関連ガイドライン等をもとに、リスク・対策状況を把握するための質問項目を8カテゴリに構成し、チェックリスト化しています。

＜調査票の構成＞



IPA「制御システムのセキュリティリスク分析ガイド」や各種ガイドライン等をもとに、セキュリティ対策の主要な項目を網羅

リスクアセスメントサービス ご提供価格・実施期間

メニュー	価格（税別）	実施期間（目安）
リスクアセスメントサービス	600万円～	約3ヶ月～

このカタログに掲載されている内容については、予告なしに変更することがありますのでご了承ください。

2018年5月

お問い合わせ先

株式会社 富士通総研

コンサルティング本部 ビジネスレジリエンスグループ
〒105-0022 東京都港区海岸1-16-1 ニューピア竹芝サウスタワー
Tel: 03-5401-8432 Email: fri-bcm-dm@cs.jp.fujitsu.com