サイバー攻撃の脅威から社会インフラを守るリスクアセスメントコンサルティング手法

Risk Assessment Consulting Method to Protect Social Infrastructure from Threat of Cyberattacks

山口　貴詩

あらまし

昨今のサイバー攻撃の増加により，企業は多様かつ広範なセキュリティ対策を余儀なくされている。特に，電力，通信，交通，金融などの社会インフラサービスが万一停止した場合，社会への影響は極めて大きくなる。したがって，社会インフラ事業者は，自社の重要なセキュリティリスクに対して優先度を判断しながら確実に対策を講じていくことが必要になる。この課題に対して，富士通総研では効率的かつ効果的にリスク対応するためのリスクアセスメントコンサルティング手法を開発した。本手法は，まず重要な事業やサービスを特定し，対象となる情報システムや制御システムといった情報資産に関わるサイバー攻撃などの脅威やセキュリティの脆弱性を踏まえた独自のリスク分析を行う。その分析結果に基づいて企業内の重要課題を明確にした上で，セキュリティ対策を順位付けして対応することによって，投資の合理性を確保できる。

本稿では，主に社会インフラサービスを担う事業者を対象とした，本手法の考え方やアプローチについて述べる。

Abstract

The recent increase in cyberattacks is compelling companies to take diverse and extensive security measures. In particular, if social infrastructure services such as power, communication, transportation, and finance are interrupted, society will be greatly affected. Accordingly, social infrastructure operators are required to implement reliable measures while making decisions on the priorities of their critical security risks. In order to deal with this issue, Fujitsu Research Institute has developed a risk assessment consulting method for addressing risks efficiently and effectively. This method first identifies important businesses and services and conducts unique risk analyses based on an understanding of cyberattacks and other threats and security vulnerabilities relating to information assets, including relevant information systems and control systems. Then, the results of these analyses can be used as a basis to clarify important issues facing a company, and security measures can be prioritized for implementation. This in turn leads to ensured rationality in investment. This paper describes the concept and approach of this method, mainly intended for operators responsible for social infrastructure services.

1. まえがき

昨今，急増しているサイバー攻撃の手法は高度化の一途をたどっており，企業はかつてないほどのリスクにさらされている。そのターゲットは広がりを見せており，ネットワークに接続されデータを取得するIoT機器なども狙われている。また，工場や発電所といったプラントやインフラの制御システムが狙われ始めており，設備そのものや，サービスを提供し安全を維持するシステムへの攻撃が懸念されている。[(1)] このように，より多様で広範な領域でセキュリティ対策が求められるようになっている。

政府のサイバーセキュリティ戦略本部は，2017年4月「重要インフラの情報セキュリティ対策に係る第4次行動計画」を公表した。[(2)] 同計画では，情報通信や金融などの13分野を重要インフラ分野として特定している。そして，国民生活や社会経済活動の維持に不可欠な重要インフラサービスにおけるセキュリティ対策の必要性と，有効な対策の考え方や実施に向けた取り組みの進め方が述べられている。

しかし，これらの社会インフラサービスを提供する事業者（以下，インフラ事業者）は，必ずしもサイバーセキュリティに対する意識が高いわけではなく，十分な対策を講じていない状況も見受けられる。

このような状況を踏まえて，富士通総研はインフラ事業者が抱えるセキュリティ対策に関わる問題への解決アプローチを盛り込んだリスクアセスメントコンサルティング手法を開発した。本手法を適用することにより，インフラ事業者はセキュリティ対策の優先順位を明確化でき，経営的な視点からセキュリティ投資の合理性を確保できる。

本稿では，社会インフラのセキュリティ対策の現状とインフラ事業者の抱える問題を述べ，本手法の活用手順と有効性を説明する。

2. インフラ事業者におけるセキュリティ対策の問題点と解決のアプローチ

本章では，インフラ事業者におけるセキュリティ対策の問題点を挙げ，解決策を提言する。

2.1 インフラ事業者の抱える問題

インフラ事業者はそのほとんどが大企業であり，企業内の事業・サービス関連部門が様々なシステムやデータなど（情報資産）を保有している。通常，インフラ事業者では情報システム部門が企業内のセキュリティ対策を担当するケースが多いが，以下のように情報資産の管理に問題があることから対策が立ち遅れている状況も見受けられる。

(1) 情報資産のブラックボックス化

インフラサービスの提供で使われるシステム（制御システムなど）は，事業部門が独自に開発・運用しているケースが多い。このため，情報システム部門は事業部門の重要なシステムを十分に把握しておらず，セキュリティリスクを正しく評価できない場合がある。また，それらのシステムは全社的なセキュリティ統制の枠組みに含まれていないことも多い。

(2) 情報資産の多種多様化

事業・サービス関連部門では，多くの情報システムや制御システムが運用されている。更に，IoT機器やスマートデバイスも利活用され始めるなど，様々な情報資産が扱われている。そのような状況から，情報システム部門は，社内の情報資産のセキュリティ対策に対してどこから手を付けてよいか分からない状況に陥ることも多い。

2.2 問題解決のアプローチ

上述の問題を解決するための施策のポイントを以下に示す。

(1) 情報資産の可視化

まず，情報資産の棚卸を行い，可視化する。その際，企業の既存資料を活用するだけでなく，各部門へのヒアリングやアンケート調査を実施し，その結果を整理しながら可視化する。情報資産の可視化は，部門横断の全社的な活動となるため，経営層から実施部門までの連携が重要である。

(2) 優先順位を踏まえたセキュリティ対策の実施

次に，可視化した情報資産を評価しセキュリティ対策を実施する。実施に当たっては，事業やサービスの重要性などによって優先順位を明確にすると良い。

3. リスクアセスメントコンサルティング手法

本章では，前章で述べたアプローチを踏まえて開発した，リスクアセスメントコンサルティングの手法について述べる。

3.1 リスクアセスメントコンサルティング手法の特長

従来のリスクアセスメントは，対象とする情報資産をあらかじめ決定した上で，あるべき対策と現状対策との比較評価によって，課題を明確にする。今回，富士通総研が開発したリスクアセスメントコンサルティング手法の特長は，セキュリティ対策のリスクアセスメントを事業継続視点で捉え直した新たな方法論を構築している点にある。

本手法は，富士通総研が事業継続マネジメントコンサルティングの実践で培ってきたビジネス影響度分析のノウハウと，富士通のセキュリティのナレッジを融合して開発したものである。本手法を適用することにより，経営視点からセキュリティ対策にリソースを投下すべき重要な情報資産を絞り込むことができ，効果的かつ効率的にリスクを低減することが可能となる。

図-1に示すように，リスクアセスメントコンサルティングは，ビジネスリスク分析（ステップ1）とICTリスク分析（ステップ2）から構成される。各ステップの具体的な内容を以下に解説する。

3.2 ビジネスリスク分析（ステップ1）

ビジネスリスク分析は，事業やサービスの全体像を整理した上で重要性の高い業務を絞り込み，当該業務の実施に不可欠な情報資産を特定するプロセスである。つまり，目的に照らしてリスク管理対象とすべき重要資産を合理的に絞り込み，リスク対応に必要となる経営資源（ヒト，モノ，カネ）を重点的に投下するロジックを整理するための方法論である。

以下，ビジネスリスク分析を構成するフェーズについて述べる。

（1）事業・サービス重要度評価

まず，事業やサービスの単位で企業のビジネスの全体像を整理する必要がある。例えば，業務分掌の資料や業務主管部門へのヒアリング結果を基に，事業とサービスを構造化する。そして，サービスが中断した場合の影響の大きさを分析し，サービスの重要度を評価する。

重要度は，以下のビジネスリスクシナリオの観点などから，事業・サービス重要度評価表を用いて総合的に評価する（**表-1**）。

・売上，利益，マーケットシェアへの影響
・顧客の事業継続や社会機能維持への影響
・事業やサービスの停止に伴う社会的信用への影響

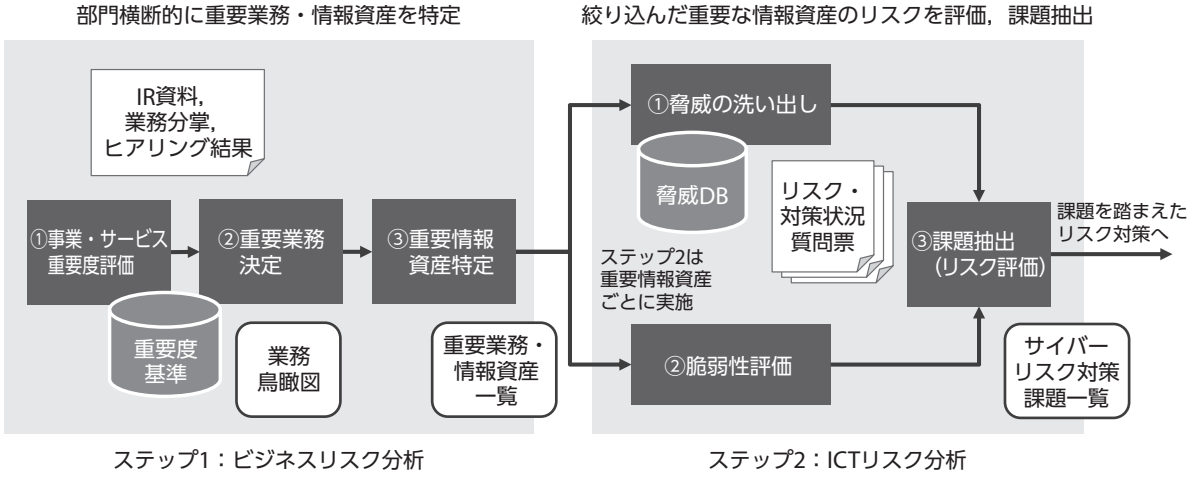

図-1　リスクアセスメントコンサルティングのプロセス

表-1　事業・サービス重要度評価表

対象		重要度基準による評価					業務継続に必要なサービスレベル	目標復旧時間
事業	サービス	売上・利益	顧客の事業継続	社会的信用	重要なイベント	総合		
A事業	aサービス	◎	◎	○	○	◎	平常時の50%	24時間
	bサービス	◎	○	◎	○	◎	平常時の40%	24時間
	cサービス	○	◎	△	○	○	−	−
B事業	dサービス	◎	○	△	○	○	−	−
	eサービス	△	○	△	△	△	−	−
C事業	fサービス	△	○	○	○	○	−	−

◎：当該サービスの重要度が高い
○：当該サービスの重要度は中程度
△：当該サービスの重要度が低い

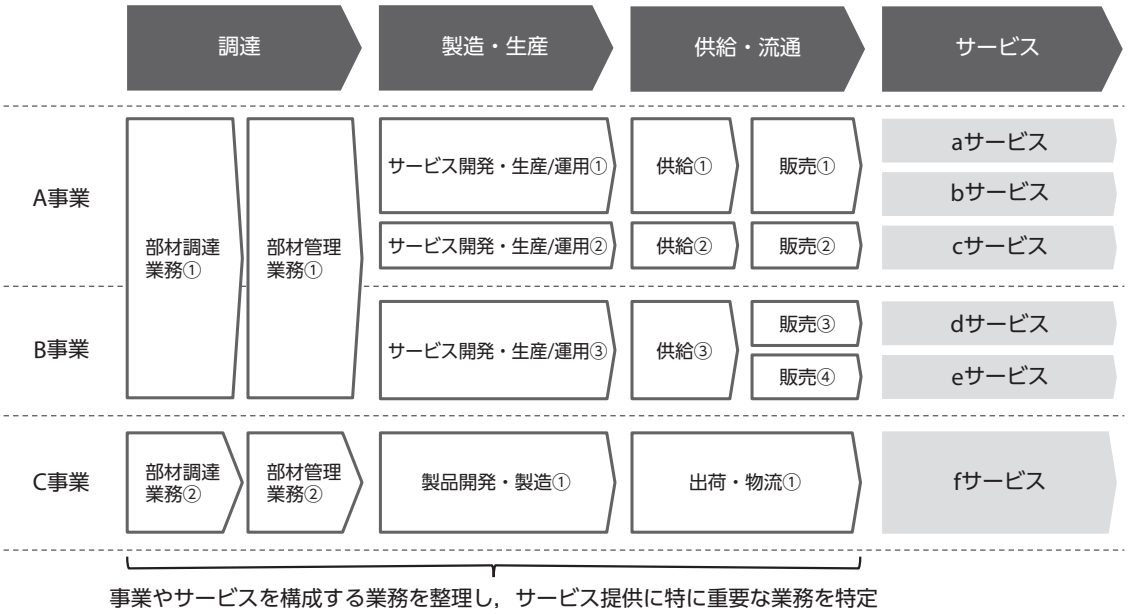

図-2　業務鳥瞰図

・企業が主催もしくは参加する重要なイベントへの影響

(2) 重要業務決定

次に，バリューチェーンの観点で顧客サービス提供までに至る業務を，図-2に示すように業務鳥瞰図として整理する。

上述の分析で明らかにした必要不可欠な重要業務を特定する。重要業務は，間接業務や代替可能業務などは対象外とする。

(3) 重要情報資産特定

最後に，重要業務の情報資産を特定する。重要業務の主管部門へのヒアリングやアンケート調査を基に，業務で使われている情報システムの構成や他システムとの連係，データの種類・内容を把握する。

このように，ビジネスリスク分析によって，情報資産のうち重要性の高い事業やサービスに必要不可欠なシステムが経営視点から明確になる。

3.3 ICTリスク分析（ステップ2）

ICTリスク分析は，ビジネスリスク分析によって特定された重要な情報資産に対して，想定される脅威と脆弱性の観点からサイバーセキュリティリスクを評価するプロセスである。

以下，ICTリスク分析を構成するフェーズについて述べる。

(1) サイバー攻撃などの脅威の洗い出し

ここでは，対象となる情報資産の可用性，完全性，機密性が損なわれ，重要業務の阻害につながる脅威（例えば，サイバー攻撃など）を洗い出す。

脅威は，情報技術の発展によって変遷するため，既知情報に加えて，アセスメント時点の最新情報を含めて，網羅的に対応を検討することが望ましい。例えば，一般社団法人JPCERTコーディネーションセンターや，業種ごとの情報共有分析センターなどのISAC（Information Sharing and Analysis Center）団体から提供される情報を基に作成したデータベースの活用が有効である。

(2) セキュリティの脆弱性の整理と評価

情報資産のリスクの大きさは，サイバー攻撃などの脅威のみによって決まるのではない。以下のような自社内での要因の掛け合わせによって決まる。

・システムの不正アクセスやマルウェアの侵入の原因となるハードウェアやソフトウェア
・監視するシステムの運用管理の不備
・セキュリティ担当者への教育・訓練不足

このように想定される脆弱性を整理し，漏れなく評価することが重要である。

(3) 情報資産のリスク評価

最後に現状のセキュリティ対策の実施状況を踏まえて，対象となる情報資産がどれだけのリスクにさらされているのかを評価するとともに，課題を明確にする。リスク評価は，情報資産の運用・管理部門に対するシステム運用やセキュリティ対策状況のヒアリングや，アンケート調査などによって必要な情報を収集して実施する。

富士通総研では，セキュリティ対策状況を把握し，リスク評価を行うためのツールとして，以下の8カテゴリをベースにした質問票形式のアセスメントフレームワークを用意している。

・ネットワークセキュリティ
・サーバ・端末セキュリティ
・ベンダー管理
・人的セキュリティ
・物理セキュリティ
・セキュリティ監視
・インシデント対応
・第三者評価

このアセスメントフレームワークは，独立行政法人情報処理推進機構が公表している「制御システムのセキュリティリスク分析ガイド」[(3)]など，セキュリティ対策の主要な項目を包含し，構成されている。

4. むすび

本稿では，効率的かつ効果的なセキュリティ対策を実現するためのリスクアセスメントコンサルティング手法を紹介した。

現在，富士通総研では，本手法を用いたコンサルティングサービスを金融・交通などインフラ事業者のお客様に提供し，セキュリティリスクの可視化と対策の推進を支援している。今後，様々なインフラ事業者のお客様へのコンサルサービスの提供を通じて，リスクアセスメントコンサルティングの方法論やツール類（分析用テンプレートなど）の改善を図っていく。また，最新のサイバー攻撃などの脅威情報を取り入れて，ICTリスク分析の精度を向上させて本手法のアップデートを図り，今後，社会インフラのサイバーセキュリティ向上に，より一層貢献できるよう取り組んでいく。

参考文献

(1) 独立行政法人情報処理推進機構：制御システムのセキュリティ.
https://www.ipa.go.jp/security/controlsystem/index.html
(2) 内閣官房内閣サイバーセキュリティセンター：重要インフラの情報セキュリティ対策に係る第4次行動計画.
https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf
(3) 独立行政法人情報処理推進機構：制御システムのセキュリティリスク分析ガイド.
https://www.ipa.go.jp/files/000061925.pdf

著者紹介

山口　貴詩（やまぐち　たかし）
（株）富士通総研
コンサルティング本部
リスクマネジメントや事業継続マネジメント，サイバーセキュリティに関するコンサルティングに従事。