ハイブリッドクラウドにおける ネットワークセキュリティのあり方 ーこれで安心クラウドセキュリティー ～守りし者達の道標～

アブストラクト

1. 研究の背景・課題・問題認識

近年、多くのパブリッククラウドサービスが提供されており、それらを利用する企業が増加しているものの、いまだにセキュリティの不安を考える企業は少なくない。そのためデータの重要性に応じて、オンプレミス環境とクラウド環境を併用する「ハイブリッドクラウド」の形態をとる企業が多い。

従来のネットワークセキュリティは、オンプレミス環境で情報資産を守るために考案されてきたものであり、クラウド環境にそのまま適用することができない。システム担当者がハイブリッドクラウド構成において、どのようにセキュリティ対策を実施すれば良いか、指針が無いことが課題となっている。

加えて、各省庁、団体から発行されているガイドラインの多くは、システム担当者にとって必要な、ネットワーク構成を設計するための情報が不足していることも課題である。

本分科会では、システム担当者に対して有用な、具体的なネットワーク構成例・装置・セキュリティ対策を明示したガイドラインを作成することを研究目標とした。

2. 研究のアプローチ・進め方

新しいガイドラインを作成するためには、リスクと対策を網羅的に洗い出す必要があると考え、複数のアプローチ（3 つのアプローチ）によるリスクと対策の抽出を行った。また、セキュリテガイドラインでは対策製品も明示する必要があると考えたため、上記アプローチと平行してセキュリティ対策製品の収集も行った。

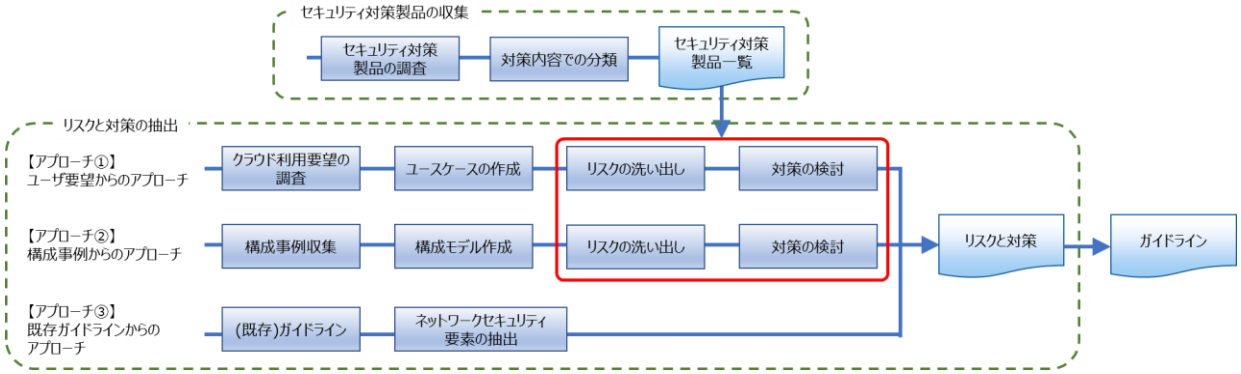

図 1 研究へのアプローチ

(1) セキュリティ対策製品の収集

ガイドラインで「具体的なネットワーク構成例・装置」を明示するため、市場で流通しているセキュリティ対策製品を調査する。

(2) リスクと対策の抽出

① 要望からのリスクと対策方法の抽出

利用者がどのようなサービスを使いたいのか、何を実現したいのかを要望・RFP からシステムの利用例（ユースケース）をまとめる。利用例からシステム構成例を作成し、システム構成例のどこにリスクが存在し、どのような対策が必要であるかを検討する。

② 構成事例からのリスクと対策方法の抽出
　ハイブリッドクラウド構成のシステム導入事例を文献・インターネットを活用して収集し、システム構成例を抽出する。①同様に構成例のどこにリスクが存在し、どのような対策が必要であるかを検討する。

③ 既存のガイドラインからのリスクと対策方法の抽出
　既存のガイドラインはシステム担当者が利用しやすい形ではないが、これらはリスクと対策方法について検討した結果がまとめられたものであり、網羅性という観点では優れたものであると考えられる。そのため、既存のガイドラインからリスクと対策方法を抽出する。

3. 研究内容と成果

網羅したリスクと対策を基に作成する新しいガイドラインは、システム担当者のクラウド導入時の判断材料や、上層部や経営層に対する的確な説明材料となることを目指した。

従来は「システム概要」から「対策製品」までの検討に時間を要し、かつ検討者により結果が左右されるものであった。本分科会の新ガイドラインは、「システム概要」→「対策製品」までの検討を自動化するツールを作成し、検討時間の削減と検討者による結果のばらつきを抑えることを目指した。

新ガイドラインでは、ユーザが質問票の問いに答える（選択式）だけで、システム概要、そこに存在するリスク一覧と対策方法までが自動で作成されるようになっている。また、現状のセキュリティ対策の実施状況を考慮できるように、既存環境の入力シートを追加した。さらにツールの利便性向上のために、ガイドライン質問票と現状対策を入力することで、ハイブリッドクラウドの基本構成図、および想定リスクとその対策を自動出力する機能を追加した。これらにより、担当者のスキルレベルに依存することなく、全ての想定リスクとその対策が検討できるガイドラインが完成した。

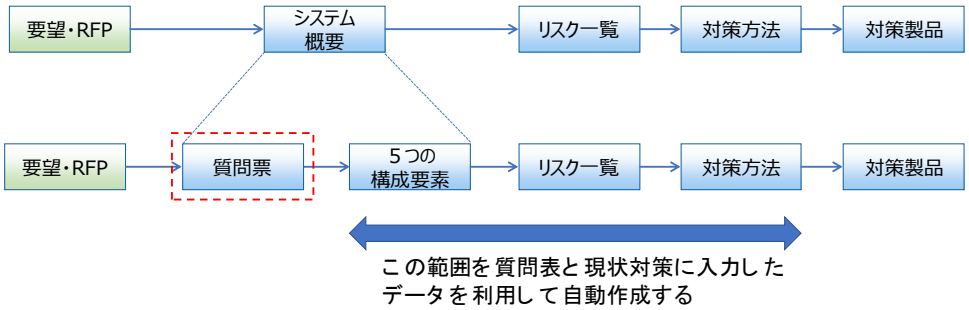

図 2 新ガイドラインの利用フロー

4. 考察

ガイドライン作成の目的である「リスク・対策・ネットワーク構成の明確化」が達成できているか、アンケートによる評価を行った。アンケートには、利用時に重要となる「利用のしやすさ」、「経営層への説明時の活用しやすさ」を含めることとした。アンケート結果から本分科会で作成したガイドラインは、クラウド利用時のネットワークにおけるリスクと対策を提示する機能を有するものであると言える。今回はクラウドサービスとのネットワークセキュリティに重点を置き評価したが、クラウドサービス自体の適切な評価と信頼感の醸成が必要と考えられる。

5. 研究の総括と提言

本分科会で作成したガイドラインを用いることで、ハイブリッドクラウド採用時のネットワークセキュリティリスク、対策方法、望ましいネットワーク構成をシステム担当者のスキルに依存せずに明確にすることが可能となった。

ハイブリッドクラウドを安全に利用するためには、事前にクラウドベンダー側で実施しているセキュリティ対策を確認したうえで、本ガイドラインを用いて明確になったセキュリティ対策を、各企業のセキュリティポリシーにしたがい、実施することが重要である。

本分科会で作成したガイドラインは、現場で活用されることで価値を発揮する。ガイドラインを活用し積極的にクラウドサービスの採用に取り組んでいただきたい。