2F-06

システム・シンキングを用いた バランスのとれたサイバーリスク管理のアプローチ

菊地正人[†1]　大久保隆夫[†2]
情報セキュリティ大学院大学[†1]　情報セキュリティ大学院大学[†2]

1. はじめに

今までのサイバーリスク管理は、ネガティブな側面のみ持つ純粋リスクとして、リスク抑制の側面を強調するという考え方が支配的である。大木らと共著の「経営者のための「企業価値に基づくサイバーセキュリティ・リスクモデル」の提案」[1]の中で定義されている「企業価値に基づくサイバーセキュリティ・リスクモデル」(以下「リスクモデル」と記載）では、サイバーリスクは企業活動がサイバー空間に依存することに起因するリスクとしている。本稿では、サイバー空間を企業活動に利用して、企業価値を向上させるために生まれるリスクをサイバーリスクととらえ、ネガティブな側面のみでなく、ポジティブな側面も含んだ将来に生み出す企業価値の不確実さの大きさを表すものとする。サイバー空間に依存する企業価値を残留サイバーリスクレベルとの関係で表した場合の分布は、正規分布になるとする。つまり、サイバー攻撃により企業価値が下振れするネガティブ・リスクの分布と、サイバー空間を企業活動のために利用して企業価値が上振れするポジティブ・リスクの分布は、正規分布の中で期待値であるサイバー空間を企業活動に利用しない場合の企業価値を中心に左右対称になっているとする。そのうえで、受容するサイバーリスクとサイバー空間に依存する企業価値の向上のバランスをとる仕組みを可視化できるサイバーガバナンスモデルを提言する。具体的には、攻めのガバナンスのチェックの指標となる目標とするサイバー空間に依存する企業価値、および、それとバランスのとれた、守りのガバンスのチェックの指標となるサイバーリスク選好をガバナンスが設定したうえ、マネジメントに提示する。マネジメントが目標とするサイバー空間に依存する企業価値に従って業務執行したうえ、サイバーリスク選好に従ってサイバーリスクに対応する。その結果、企業が受容するサイバーリスクとサイバー空間に依存する企業価値の向上のバランスをとることができる。この仕組みを可視化するために、複雑な構造の要素間が相互作用する動的な現象を俯瞰・分析することができるシステム･シンキングの理論を適用する。それにより、ガバナンスは、目標とするサイバー空間に依存する企業価値とサイバーリスク選好の値の最適なバランスを見出すことができるようになる。

2. サイバーガバナンスモデルの構築

2.1 モデルのステークホルダー

ステークホルダーは、企業と攻撃者とする。

2.2 モデルに含む変数

企業のサイバーリスクへの関心事項は、「リスクモデル」の構成要素として、以下のようにすでに明確になっているものとしたうえ、これらを変数とする。

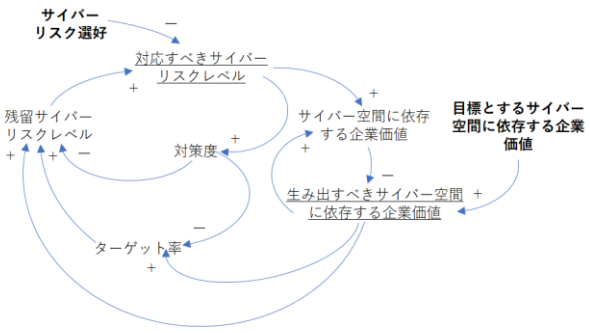
- サイバー空間に依存する企業価値（サイバー空間からアクセス可能な Asset と Process、及び Capability Value の和)
- ターゲット率(脅威源からサイバー攻撃を受ける可能性)
- 1 - 対策度(脅威源からのサイバー攻撃を受けた場合に、脆弱性を突かれて情報資産が影響を受ける確率を、対策の実装により低減する割合)
- 残留サイバーリスクレベル(上記３つの要素の積)

また、攻撃者のサイバーリスクへの関心事項は、Jos Corman と David Etue が定義している Adversary ROI の理論[2]ですでに明確になっているものとする。この理論では、脅威源である攻撃者らは攻撃の ROI を考慮して攻撃の対象を選んでいると示している。この場合、攻撃によって得られる利益はサイバー空間に依存する企業価値に、攻撃のコストは対策度に相当するものとする。

2.3 モデルに含む変数の因果関係

システム・シンキングの理論を適用して変数の因果関係を表した因果ループ図は以下になる。

図 1　因果ループ図 1



これを、サイバーガバナンスモデルと呼び、以降では、各因果関係の根拠について説明する。

Balanced Cyber Risk Management Approach by Application of System Thinking
†1 MASATO KIKUCHI, Institute of Information Security.
†2 TAKAO OKUBO, Institute of Information Security

2.3.1 対策度と残留サイバーリスクレベル

対策度を原因、残留サイバーリスクレベルを結果とする、負の因果リンクが存在する。脅威源からのサイバー攻撃を受けても、それを阻止できる割合が増加すると、残留サイバーリスクレベルはその分小さくなる。

2.3.2 サイバー空間に依存する企業価値と残留サイバーリスクレベル

サイバー空間に依存する企業価値を原因、残留サイバーリスクレベルを結果とする、正の因果リンクが存在する。サイバー空間に依存する企業価値が高まると、攻撃を受けた場合の影響度が高くなり、残留サイバーリスクレベルも高まる。

2.3.3 ターゲット率と残留サイバーリスクレベル

ターゲット率を原因、残留サイバーリスクレベルを結果とする、正の因果リンクが存在する。ターゲット率が高まると、残留サイバーリスクレベルも高まる。

2.3.4 残留サイバーリスクレベル、対策度、サイバーリスク選好、および対応すべきサイバーリスクレベル

残留サイバーリスクレベルを原因、対策度を結果とする、正の因果リンクが存在する。残留サイバーリスクレベルがサイバーリスク選好よりも上回る場合、残留サイバーリスクレベルが増加すれば、対策を行う選択肢を実施する。しかしながら、残留サイバーリスクレベルがサイバーリスク選好を下回る場合、対策を行うことはない。そのため、サイバーリスク選好よりも上回る分の残留サイバーリスクレベルの値を対応すべきサイバーリスクレベルという変数として追加したうえ、残留サイバーリスクレベルと対策度の因果関係の間に置いた。

2.3.5 対策度とターゲット率

対策度を原因、ターゲット率を結果とする、負の因果リンクが存在する。Adversary ROI の理論[2]により、攻撃のコスト（対策度）が大きくなれば、攻撃の ROI は小さくなるため、ターゲット率は低くなると言える。

2.3.6 サイバー空間に依存する企業価値、目標とするサイバー空間に依存する企業価値、および生み出すべきサイバー空間に依存する企業価値

目標に不足しているサイバー空間に依存する企業価値を生み出すべきサイバー空間に依存する企業価値という変数として追加したうえ、サイバー空間に依存する企業価値と残留サイバーリスクレベルの因果関係の間に置いた。サイバー空間に依存する企業価値の増加は、生み出すべきサイバー空間に依存する企業価値が減少する原因になるが、一方、目標とするサイバー空間に依存する企業価値の増加は、生み出すべきサイバー空間に依存する企業価値を増加させる原因にもなるとする。そして、生み出すべきサイバー空間に依存する企業価値の増加が、サイバー空間に依存する企業価値の増加につながる。

2.3.7 生み出すべきサイバー空間に依存する企業価値とターゲット率

生み出すべきサイバー空間に依存する企業価値を原因、ターゲット率を結果とする、正の因果リンクが存在する。Adversary ROI の理論[2]により、攻撃により得られる利益（企業価値）が大きくなれば、攻撃の ROI は大きくなるため、ターゲット率は増加すると言える。

2.3.8 対応すべきサイバーリスクレベルとサイバー空間に依存する企業価値

対応すべきサイバーリスクレベルを原因、サイバー空間に依存する企業価値を結果とする、正の因果リンクが存在する。内閣府による平成 20 年度年次経済財政報告[3]では、総資産利益率(ROA)のばらつき（標準偏差）が大きいリスクテイクしている企業の方が、ROA の平均値が高いとしている。つまり、目標とするサイバー空間に依存する企業価値が高くなり、それに伴い対応すべきサイバーリスクレベルも増加すると、1 章のサイバー空間に依存する企業価値を残留サイバーリスクレベルとの関係で表したものが正規分布になるという前提から、サイバー空間に依存する企業価値のばらつきが増加して、その平均値も増加する。

3. サイバーガバナンスモデルの振舞いと制御

目標とするサイバー空間に依存する企業価値の設定により増加するサイバー空間に依存する企業価値とともに、影響されたターゲット率の上昇が残留サイバーリスクレベルを増加させる。サイバーリスク選好を超えた残留サイバーリスクレベルは対策度を上げることで減少できるが、サイバー空間に依存する企業価値を増加させる。このような振る舞いを制御するには、生み出すべきサイバー空間に依存する企業価値のトレンドが大きい場合は、リスクを回避しすぎているため、ガバナンスがサイバーリスク選好を上げて、継続的なサイバー空間に依存する企業価値の成長を促す。対応すべきサイバーリスクレベルのトレンドが大きい場合は、リスクを取りすぎているため、ガバナンスが目標とするサイバー空間に依存する企業価値を下げ、継続的な対応すべきサイバーリスクレベルの低下を促す。

4. おわりに

サイバーガバナンスモデルにより、ガバナンスの設定したサイバーリスク選好が受容するサイバーリスクとサイバー空間に依存する企業価値の向上のバランスをとる仕組みを可視化できた。

参考文献

[1] 大木榮二郎、田村仁一、清水惠子、杉浦昌、菊地正人、堀越繁明、那須浩修、常川直樹、冨士浩一、「経営者のための「企業価値に基づくサイバーセキュリティ・リスクモデル」の提案」、日本セキュリティ・マネジメント学会誌、査読論文、Vol.32、No.1、pp.16-32、2018 年.

[2] Jos Corman, David Etue, Adversary ROI: Evauating Security from the Threat Actor’s Perspective, RSA Conference Europe 2012、2012 年.

[3] 内閣府、「平成 20 年度 年次経済財政報告」、2008 年.