Vol.2018-SPT-31 No.14
Vol.2018-EIP-82 No.14
2018/11/2

資源ベースの企業価値向上を目指すサイバーリスク管理の考え方

菊地正人[†1]

概要：企業価値を向上させるうえで、サイバー空間を活用することは、もはや企業にとって副次的なものではなく、企業全体のビジネス戦略に不可欠なものとなりつつある。そのために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（サイバーリスク）を適切なレベル受け入れることは必然である。本稿では、サイバー空間に依存した企業価値向上の側面に「資源ベースの経営戦略論」、サイバーリスク管理の側面に「企業価値に基づくサイバーセキュリティ・リスクモデル」を取り入れ、事業とそれに付き物であるリスクの全体的な構造の理解をより深め、サイバー空間を活用した企業価値の向上のために望ましいレベルのサイバーリスクを企業が受け入れ、リスク抑制とリスク受け入れの双方向のバランスをとる望ましいアプローチを提言する。

キーワード：サイバーリスク、資源ベース理論、リスクマネジメント、ガバナンス、システムシンキング

Consideration of a Resource-Based Corporate Value Oriented Cyber Risk Management

MASATO KIKUCHI[†1]

Abstract: It is becoming essential for corporate strategy to utilize cyberspace to increase corporate value. Therefore, it is certain to take appropriate amount of cyber risk that arises from corporate activities rely on cyberspace. This paper promotes an understanding of entire stricture of business and it risk by considering a resource-based approach for corporate value creation and corporate value oriented cyber security risk model for cyber risk management and proposes the desirable approach that the companies take appropriate amount of cyber risk to increase corporate value and then balance risk reduction with risk taking.

Keywords: Cyber Risk, A Resource-Based Approach, Risk Management, Governance, System Thinking .

1. はじめに

企業価値を向上させるうえで、サイバー空間を活用することは、もはや企業にとって副次的なものではなく、企業全体のビジネス戦略に不可欠なものとなりつつある。従来のサイバーセキュリティリスク管理は、企業価値の保護のためにリスク抑制の一方向で捉えがちである。そこで、本稿では、企業価値の向上のために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（サイバーリスク）を望ましいレベル受け入れ、リスク抑制とリスク受け入れの双方向のバランスをとることができる新しいフレームワークを提言する。

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]では、包括的なサイバーリスク認識が可能なトップダウン型のリスク管理モデルである「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）の考え方を提示した。

また、「システム・シンキングを用いたサイバーセキュリティリスクに対する考え方」[2]、および「ガバナンスの視点によるシステム・シンキングを用いたサイバーセキュリティリスク管理」[3]では、「リスクモデル」にシステム・シンキングを応用した結果生み出された「サイバーセキュリティリスク・エコシステム」により、サイバーリスクと、それを生み出す要素の相互関係に経営者が注目することができることを示した。さらに、ガバナンスの考え方が、サイバーリスクレベルを最小に抑えながら、企業価値を最大化するために果たしている役割を、「サイバーセキュリティリスク・エコシステム」の中で可視化することができた。

本稿では、サイバーリスクの側面だけではなく、サイバー空間を利用して企業価値を向上させる側面を、「資源ベースの経営戦略論」[4]と照らし合わせながらさらに掘り進め、企業がサイバーリスクリスクとサイバー空間に依存した企業価値を生み出す全体的な構造の理解をより深め、リスク抑制とリスク受け入れの双方向のバランスをとることができる新しいフレームワークを追求する。

まず、2 章において「リスクモデル」、3 章において、「リスクモデル」にシステム・シンキングを応用したうえ、「資源ベースの経営戦略論」[4]の考え方を反映した「サイバーリスク・エコシステム」について紹介する。4 章で「サイバーリスク・エコシステム」についての考察をしたうえ、5 章でこの章に述べられている本稿の目的を達成できたことを

†1 情報セキュリティ大学院大学
Institute of Information Security.

Vol.2018-SPT-31 No.14
Vol.2018-EIP-82 No.14
2018/11/2

まとめる。

2. 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」の構成要素

「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]において提示されている「リスクモデル」では、サイバーリスクレベルの算出において、以下の要素の積を求める。

- 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)

なお、上記の要素のうち、対策度については,「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]では、実際にはどれくらいの対策を実装しているか（対策度）に加えて、その対策をどの程度精緻に運用しているかも考慮する指標として保護率という名称を利用している。本稿では、リスクマネジメントで一般的に利用されている用語との整合性も考慮したうえ、そのような指標の判りやすい名称として、対策度の名称を利用している。また、サイバー空間に依存する企業価値は、企業価値とその企業価値がどのくらいサイバー空間からアクセス可能かの割合を示すサイバー依存度の要素に依存している。

各要素の算出方法やその根拠については、「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]にまとめられている。

3. サイバーセキュリティリスク・エコシステムとその発展形

「システム・シンキングを用いたサイバーセキュリティリスクに対する考え方」[2]において、システム・シンキングを「リスクモデル」に適用して「サイバーセキュリティリスク・エコシステム」が生まれた。ここでは、そのシステム・シンキングを「リスクモデル」に適用する過程を顧みながら、サイバー空間を利用して企業価値を向上させる側面を「資源ベースの経営戦略論」と照らし合わせて発展させ、「サイバーリスク・エコシステム」と名付ける。

3.1 システム・シンキングの考え方

システム・シンキングとは、対象をシステムととらえて分析する思考技法である。システムとは、「複数の構成要素が相互作用しながら全体としてまとまった機能を果たすもの」と定義される[6]。

構成要素間の関係は、因果ループ図と呼ばれるダイアグラムを用いて表現される。この因果ループ図には時間の概念が存在しており、ある要素の変化が他の要素にどのように影響を与えるかが表現される。

図 1　因果ループ例

図 1 の例では、要素 A の変化と同じ方向の変化が要素 B に起きているため、ループの矢印の近くにプラスマークが示されているが、反対方向の変化が要素 B に起きていると、マイナスマークが示される。

また、ある要素の変化が他の要素に影響を与えた結果、元の要素にもまた影響を及ぼすことを表す因果ループがあり、それをフィードバックと呼ぶ。

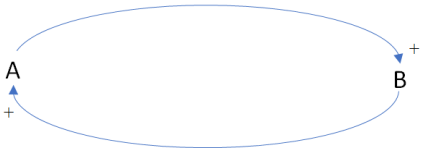

図 2　フィードバックループ例

フィードバックループのうち目標追求型のバランス型ループは、動的な均衡状態に接近したり、その状態を保持する。一方、自己強化型ループは、幾何級数的な成長を生み出す。この両者が相互につながり成長、衰退、均衡状態を生み、それが直線ではない非線形の原因と結果の関係をつくりだす[7]。

3.2 問題解決アプローチ

システム・シンキングでは、システムの構造がシステムの振る舞いを生み出し、システムの振る舞いがシステムの結果を生み出すと考える[6]。「サイバーリスク・エコシステム」をシステムととらえて、この考え方を当てはめると、システムの結果がサイバー空間に依存する企業価値とサイバーリスクレベルになり、システムの構造が、「サイバーリスク・エコシステム」の構成要素の関係となる。システムの振る舞いは、「サイバーリスク・エコシステム」の構成要素のつながりが生み出したフィードバックループで表現される。

また、システム・シンキングを問題解決に適用するには、以下のプロセスに従うことが勧められている[6]。

(1) **時間軸分析**
(2) **ステークホルダー分析**
(3) **変数摘出**
(4) **因果分析**
(5) **仮説構築**

3.3 時間軸分析

「サイバーリスク・エコシステム」は、ガバナンスがサ

Vol.2018-SPT-31 No.14
Vol.2018-EIP-82 No.14
2018/11/2

イバー空間に依存した企業価値向上を求めるとともに、サイバーリスクの抑制と受け入れの双方向のバランスをとる意思決定の判断材料に有用なものを目指している。そのため、経営者が 2 - 3 年の間にサイバー空間に依存した企業価値とサイバーリスクレベルがどのような動きで変化するかを見ていると想定する。

3.4 ステークホルダー分析、及び変数摘出

ステークホルダー分析を行うことにより、ステークホルダーの関心事項を特定することができ、それらを基に、問題に関連する変数も特定することができる。

本稿では、サイバーリスク対応への意思決定に利害関係を有するステークホルダーの関心事項、つまり問題に関する変数を、「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ている、

- サイバーに依存する企業価値
- ターゲット率
- 1 - 対策度
- サイバーリスクレベル(上記 3 つの要素の積)

また、サイバー空間への攻撃者の関心事項は、Jos Corman と David Etue が定義している Adversary ROI の理論[10]の中で、サイバー空間に依存する企業価値に利害関係を有するステークホルダーの関心事項は「資源ベースの経営戦略論」[4]の中で、そしてガバナンスの関心事項は、COSO ERM (COSO 全社的リスクマネジメント-戦略およびパフォーマンスとの統合[5]) および、情報セキュリティガバナンスの国際規格である ISO/IEC27014 Governance of information security[12]中で、それぞれ明確になっているものとする。

なお、本稿では、サイバー空間の観点からの脅威は、故意の攻撃と位置づけている。

3.5 因果分析（１）

「リスクモデル」の構成要素、及びサイバーリスクレベルの算出のロジックから導かれる変数間の因果関係については、以下のものが考えられる。

(1) 対策度とサイバーリスクレベル

(2) サイバー空間に依存する企業価値とサイバーリスクレベル

(3) ターゲット率とサイバーリスクレベル

これらの変数の因果関係を因果ループ図で表したものは以下になる。

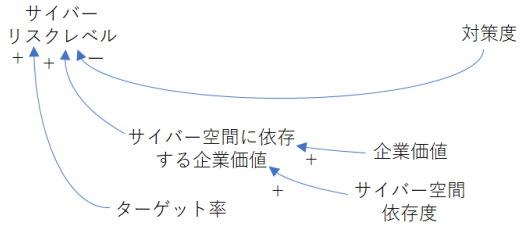

図 3　因果ループ図 1

3.5.1 対策度とサイバーリスクレベル

対策度を原因、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。つまり、対策度が増加した場合はサイバーリスクレベルが減少する関係がある。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、サイバーリスクレベルはその分小さくなる。

3.5.2 サイバー空間に依存する企業価値と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、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。つまり、サイバー空間に依存する企業価値が増加した場合はサイバーリスクレベルも増加する関係がある。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、サイバーリスクレベルも高まる。

3.5.3 ターゲット率とサイバーリスクレベル

ターゲット率を原因、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。つまり、ターゲット率が増加した場合はサイバーリスクレベルも増加する関係がある。ターゲット率が高まると、脅威源から攻撃を受ける可能性が高くなり、サイバーリスクレベルも高まる。

3.6 因果分析（２）

サイバーリスクレベルの算出のロジックには直接含まれていない変数間の因果関係も、以下のものが考えられる。

(1) サイバーリスクレベルと対策度

(2) 対策度とサイバー空間に依存する企業価値

(3) 対策度とターゲット率

(4) サイバー空間に依存する企業価値とターゲット率

これらの変数の因果関係を、因果ループ図 1 に追加したものは以下になる。

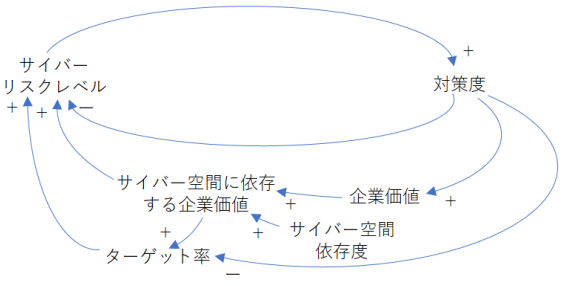

図 4　因果ループ図 2

3.6.1 サイバーリスクレベルと対策

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。サイバーリスクレベルが増加した場合は対策度も増加する関係がある。

マネジメントは、サイバーリスクレベルがサイバーリスク選好よりも下回らない限り、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。そのため、サイ

バーリスクレベルが増加すると、対策度が増加すると言える。

3.6.2 対策度とサイバー空間に依存する企業価値

対策度を原因、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。つまり、対策度が増加した場合はサイバー空間に依存する企業価値も増加する関係がある。

藤原による調査レポート[8]では、高い情報セキュリティを維持することが、直接企業価値を高めることを示している。また、田中、松浦による研究調査報告書[9]では、企業の情報セキュリティ投資が企業価値に与えるポジティブな影響を実証的に示している。

情報セキュリティへの投資は、情報セキュリティ対策を行うことであるため、つまり対策度が増加することである。このことから、対策度が増加した場合は、経営者には明瞭ではないかもしれないが、時間の遅れを伴いサイバーに依存する企業価値も増加する関係があると言える。

3.6.3 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。つまり、対策度が増加した場合はターゲット率が減少する関係がある。

Jos Corman と David Etue が定義している Adversary ROI の理論[10]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。攻撃のコストが大きくなれば、攻撃の ROI は小さくなるため、攻撃の対象になる確率、つまりターゲット率は低くなると言える。

このことから、対策度を増加することにより攻撃のコストの増加につながり、攻撃者らの攻撃対象を他に変えさせることができるため、その結果、ターゲット率が減少すると言える。

3.6.4 サイバー空間に依存する企業価値とターゲット率

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。つまり、サイバー空間に依存する企業価値が増加した場合はターゲット率も増加する関係がある。

Adversary ROI の理論[10]に従うと、攻撃により得られる利益が大きくなれば、攻撃の ROI は大きくなるため、攻撃の対象になる確率、つまりターゲット率は増加すると言える。

このことから、サイバー空間に依存する企業価値が増加すると、攻撃者らにとって攻撃により得られる利益が大きくなり、ROI も大きくなるため、ターゲット率は増加すると言える。

3.7 因果分析（３）

「リスクモデル」の構成要素である変数間の因果関係をより論理的に補足説明するために、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それぞれに影響を与える変数も隠れて存在していると思われる。なお、サイバー空間に依存する企業価値を生み出している変数の把握については、「資源ベースの経営戦略論」[4]の考え方を応用している。それらは、以下が考えられる。

(1) **サイバーリスク選好、および対応すべきサイバーリスクの大きさ**
(2) **サイバー空間に依存する企業資源**
(3) **目標とするサイバー空間に依存する企業価値、不足するサイバー空間に依存する企業価値、および投資**
(4) **サイバー空間に依存する無形資産、および評判**
(5) **サイバー空間に依存するケイパビリティ、および生産性**

これらの変数とそれに関連する因果関係を因果ループ図２に追加したものは以下になるが、これを「サイバーリスク・エコシステム」と呼ぶこととする。

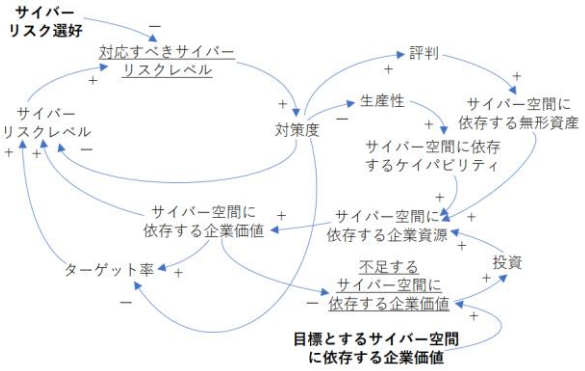

図 5　サイバーリスク・エコシステム

3.7.1 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

マネジメントは、サイバーリスク対応の意思決定を行う時は、リスク分析の結果、サイバーリスクレベルとサイバーリスク選好を比較したうえ、目標とするサイバーに依存する企業価値の向上を考慮するうえで、サイバーリスクレベルが許容可能か、もしくはそうではないか決定を行う。

サイバーリスクレベルが大きくなっても、それがリスク選好を下回るものであれば、対策を行う意思決定は行われないため、対策度も変わることはない。そのため、サイバーリスク選好よりも上回る分のサイバーリスクレベルの値を対応すべきサイバーセキュリティレベルという変数として追加したうえ、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。サイバーリスクレベルの増加は、対応すべきサイバーリスクを増加する原因になるが、一方、サイバーリスク選好の増加は、対応すべきサイバーリスクレベルを減少させる原因にもなるとする。

3.7.2 サイバー空間に依存する企業資源

「資源ベースの経営戦略」[4]では、企業資源は企業価値を創造するための究極の源泉であるとしている。そのため、サイバー空間に依存する企業資源という変数を追加したうえ、その増加は、サイバー空間に依存する企業価値の増加の原因になるとする。なお、企業資源は、有形資産、無形

資産、そして組織のケイパビリティの三つの大きなカテゴリーに分類される。

3.7.3 目標とするサイバー空間に依存する企業価値、不足するサイバー空間に依存する企業価値、および投資

サイバー空間に依存する企業価値が目標とするレベルに達していない場合は、その不足する企業価値を満たすために投資が行われ、それによってサイバー空間に依存する企業資源が増加する。そのため、目標とするサイバー空間に依存する企業価値、不足するサイバー空間に依存する企業価値、および投資という変数とそれらの因果関係も追加する。

3.7.4 サイバー空間に依存する無形資産、評判

藤原による調査レポート[8]では、情報セキュリティへの投資は、企業にとって重要な無形資産である「信用」や「信頼」を維持するために必要不可欠な継続的企業活動のひとつであり、高い情報セキュリティを維持することが、直接企業価値を高めることを示している。

情報セキュリティへの投資、つまり対策度が増加した場合に、時間の遅れを伴い企業価値が増加するとは、つまり、対策の実施が企業の「信用」や「信頼」を高め、同時に企業の評判を高めることでもあるため、評判という変数を追加する。また、評判は無形資産に含まれる要素の一つ[4]のため、サイバー空間に依存する無形資産という変数も追加する。対策度の増加はまず、評判の増加になり、それがサイバー空間に依存する無形資産の増加につながり、結果的にサイバー空間に依存する企業価値の増加になる関係に置き換えるとする。

3.7.5 サイバー空間に依存するケイパビリティ、および生産性

Dell inc.による Dell End-User Security Survey 2017 [11]では、日本を含む８か国のエンドユーザーである回答者の76%が、セキュリティ優先のため従業員の生産性が犠牲になっていると回答している。このことからも分かるように、対策を行うことは、企業活動の生産性を下げる影響もあるため、生産性という変数を追加する。また、組織がインプットをアウトプットへと変換するために用いる資産、人材、プロセスの複雑な組み合わせ方を意味するケイパビリティ[4]に含まれる要素の一つが生産性であるため、サイバー空間に依存するケイパビリティという変数も追加する。対策度の増加はまず、生産性の減少になり、それがサイバー空間に依存するケイパビリティの減少につながり、結果的に企業価値の減少になる関係も追加する。

3.8 因果分析（４）

ガバナンスの要素をカバーした全社的なリスク管理のフレームワークである COSO ERM (COSO 全社的リスクマネジメント-戦略およびパフォーマンスとの統合[5]) と、情報セキュリティガバナンスの国際規格である ISO/IEC 27014 Governance of information security[12]に、サイバーセキュリティ管理に関連するガバナンスの要件が示されている。その中で、特にガバナンスによる執行機関、つまりマネジメントの監督とリスク選好についての要件は、以下の変数とその新たな因果関係に表されると考えられる。

(1) 不足するサイバー空間に依存する企業価値のトレンドと目標とするサイバー空間に依存する企業価値

(2) 不足するサイバー空間に依存する企業価値のトレンドとサイバーリスク選好

(3) 対応すべきサイバーリスクレベルのトレンドと目標とするサイバー空間に依存する企業価値

本稿では、これらの因果関係を順番に、企業価値追求ループ、リスク選好制御ループ、そして企業価値制御ループと呼び、まとめて制御ループと呼ぶ。

サイバーリスク選好が一定になっているという仮定のもと、企業価値追求ループを以下のように「サイバーリスク・エコシステム」に反映した。

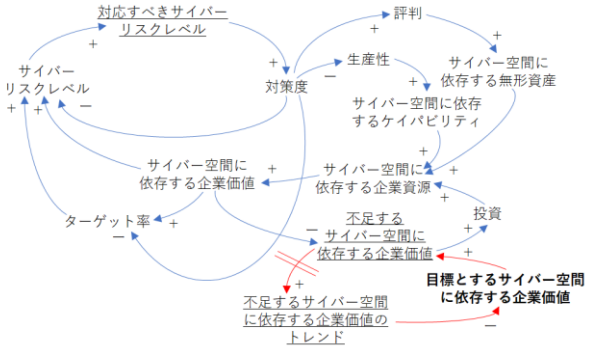

図 6　ガバナンス要件を反映させたサイバーリスク・エコシステム(シーン 1)

目標とするサイバー空間に依存する企業価値が一定になっているという仮定のもと、リスク選好制御ループを以下のように「サイバーリスク・エコシステム」に反映した。

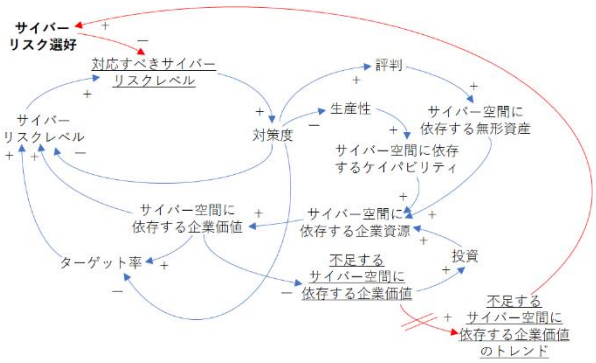

図 7　ガバナンス要件を反映させたサイバーリスク・エコシステム(シーン 2)

サイバーリスク選好が一定になっているという仮定のもと、企業価値制御ループを以下のように「サイバーリスク・エコシステム」に反映した。

Vol.2018-SPT-31 No.14
Vol.2018-EIP-82 No.14
2018/11/2

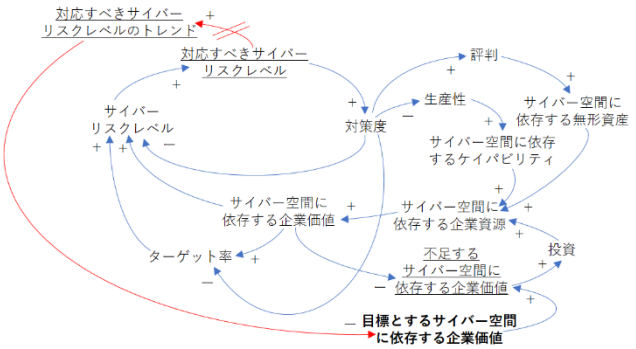

図 8　ガバナンス要件を反映させたサイバーリスク・エコシステム(シーン 3)

3.8.1 不足するサイバー空間に依存する企業価値のトレンド、目標とするサイバー空間に依存する企業価値

「不足するサイバー空間に依存する企業価値」のトレンドは時間をかけて形成されるため、この変数は他の変数と比較して時間の遅れを伴い変化するものとする。

「サイバーリスク・エコシステム」では、価値追求ということは、「不足するサイバー空間に依存する企業価値」のトレンドが低くなり、「目標とするサイバー空間に依存する企業価値」に到達しようとすると、さらに高い「目標とするサイバー空間に依存する企業価値」を掲げる。

3.8.2 不足するサイバー空間に依存する企業価値のトレンド、サイバーリスク選好

「不足するサイバー空間に依存する企業価値」のトレンドは時間をかけて形成されるため、この変数は他の変数と比較して時間の遅れを伴い変化するものとする。

「不足するサイバー空間に依存する企業価値」のトレンドが増加すれば過少のリスクしか受容しないことになるため、企業価値向上のためよりリスクテイクするために「サイバーリスク選好」を増加させる。反対の場合は、過剰なリスクを受容していることになるため、リスク回避するため「サイバーリスク選好」を減少させる。

3.8.3 対応すべきサイバーリスクレベルのトレンド、目標とする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」のトレンドは時間をかけて形成されるため、この変数は他の変数と比較して時間の遅れを伴い変化するものとする。

「対応すべきサイバーリスクレベル」のトレンドが高いと、「目標とするサイバー空間に依存する企業価値」の設定が高すぎ、必要以上にリスクテイクしているため、「目標とするサイバー空間に依存する企業価値」を低く調整する。

3.9　仮説構築

ガバナンスの要件を反映させた「サイバーリスク・エコシステム」は、大きく分けて、3.8 章において解説した制御ループと、以下の３つのフィードバックループで構成されている。

(1) **主要リスク増強ループ**
(2) **副次的リスク増強ループ**
(3) **リスクバランスループ**

3.9.1 主要リスク増強ループ

「サイバーリスク・エコシステム」から、主要リスク増強ループを摘出したものは以下になる。

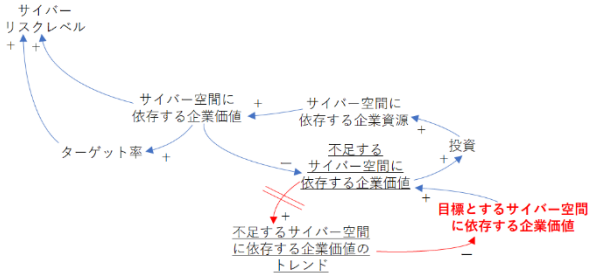

図 9　主要リスク増強ループ図

目標とするサイバー空間に依存する企業価値を生み出すために、サイバー空間に依存する企業資源を投資により適切に調整する、バランス型ループがある。しかしながら、目標とするサイバー空間に依存する企業価値に近づく状態が長く続く（不足するサイバー空間に依存する企業価値のトレンドが減少する）と、さらに高い目標とするサイバー空間に依存する企業価値を設定する企業価値追求ループであるもう一つのバランス型ループが存在する。この二つのループの組み合わせた働きは、サイバー空間に依存する企業価値、そしてサイバーリスクレベルを同じ方向に作用させるサイバー空間に依存する企業資源が反復的に増加するものであり、自己強化型となる。

サイバーリスクのレベルが上がると、そのレベルをさらに上げようとする(2)副次的リスク増強ループと、そのレベルのバランスをとろうとする(3)リスクバランスループが始まる

3.9.2 副次的リスク増強ループ

「サイバーリスク・エコシステム」から、副次的リスク増強ループを摘出したものは以下になる。

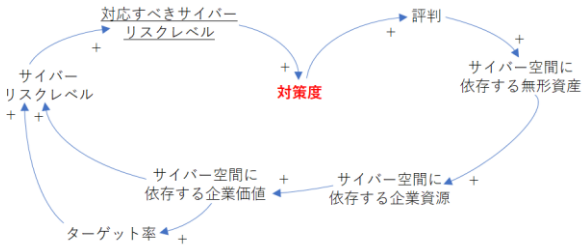

図 10　副次的リスク増強ループ図

サイバーリスクのレベルが上昇し、それがサイバーリスク選好を超えていれば、対策を行うために対策度が上昇す

Vol.2018-SPT-31 No.14
Vol.2018-EIP-82 No.14
2018/11/2

る。対策度が上昇後は、評判効果により時間の遅れを伴いサイバー空間に依存する企業価値を上げ、それにより、サイバーリスクのレベルが上昇する。このように、ループ内の変数の変化が、一回りしてさらに強化される自己強化型ループがある。

3.9.3 リスクバランスループ

「サイバーリスク・エコシステム」から、リスクバランスループを摘出したものは以下になる。

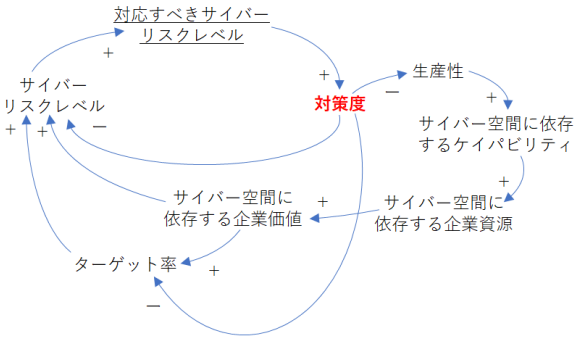

図 11　リスクバランスループ図

対応すべきサイバーリスクレベルが上がると、以下の２パターンの作用が起きる。

- 対策度が上がり、ターゲット率が下がり、また脆弱性も減るため、サイバーリスクレベルが下がる。
- 対策度が上がり、それがサイバー空間に依存する企業活動の生産性を下げたうえ、サイバー空間に依存する企業価値も下げるため、サイバーリスクレベルが下がる。

このように、ループ内の変数の変化が、一回りして、最初の変化の方向と反対の方向に働く二つのバランス型ループがある。

4. 考察

「サイバーリスク・エコシステム」についての考察を以下に述べる。

4.1 振る舞いの性質

「サイバーリスク・エコシステム」の様々な要素は、サイバー空間に依存する企業資源の増加をきっかけとして、自ら互いに影響を及ぼしあいながら、攻撃者らの振る舞いも含めた「サイバーリスク・エコシステム」の振る舞いを独自に生み出していると解釈できる。

具体的には、目標とするサイバー空間に依存する企業価値が設定されると、主要リスク増強ループの作用による反復的なサイバー空間に依存する企業資源の増加と、それによるサイバー空間に依存する企業価値の増加により、サイバーリスクレベルが上昇する。

サイバーリスク選好を超えるサイバーリスクレベルの上昇をきっかけとする対策度の増加は、バランス型のリスクバランスループの作用でサイバーリスクレベルをサイバーリスク選好のレベルに近づけようとするが、一方、自己強化型の副次的リスク増強ループの作用により、時間の遅れを伴いサイバーリスクレベルを上げる効果もある。

4.2 振る舞いの制御

サイバーリスク選好の値、もしくは目標とするサイバー空間に依存する企業価値の値を調整することによって、4.1章において説明された振る舞いを制御することができる。

4.2.1 サイバーリスク選好による制御

不足する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、よりリスクを取るようにしたうえ、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。図 7 のガバナンスの要件を反映させた「サイバーリスク・エコシステム(シーン 2)」参照。

4.2.2 目標とするサイバー空間に依存する企業価値による制御

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。図 8 のガバナンスの要件を反映させた「サイバーセキュリティリスク・エコシステム(シーン 3)」参照。

4.3 ガバナンス

企業の目標もリスク管理の目標も、サイバーリスクレベルを最小に抑えながら、サイバー空間に依存する企業価値を最大化することであり、そのような振る舞いを「サイバーリスク・エコシステム」が生み出すように、目標とするサイバー空間に依存する企業価値の値とサイバーリスク選好の値を適切に設定することが、ガバナンスの最大の使命と言えよう。

マネジメントは、目標とするサイバー空間に依存する企業価値を生み出すために、投資により準備されたサイバー空間に依存する企業資源を活用することと、サイバーリスク選好により促されるサイバーリスク管理活動を行うことで業務執行していることになる。ガバナンスの要件を反映させた「サイバーリスク・エコシステム」から、このマネジメントが関わるループを摘出したものは以下になり、これをマネジメントループと呼ぶ。

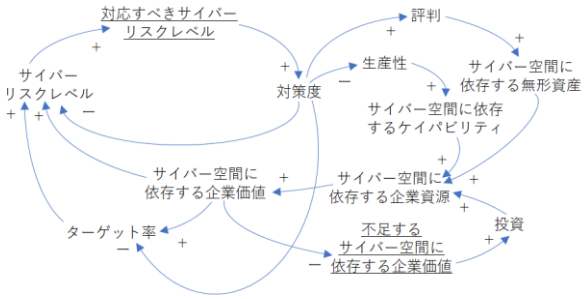

図 12　マネジメントループ図

Vol.2018-SPT-31 No.14
Vol.2018-EIP-82 No.14
2018/11/2

ガバナンスは、対応すべきサイバーリスクレベルのトレンドをモニタリング(MONITOR)しながら、目標とするサイバー空間に依存する企業価値を定める(DIRECT)。また、不足するサイバー空間に依存する企業価値のトレンドをモニタリング(MONITOR)しながら、サイバーリスク選好を定め(DIRECT)、また、目標とするサイバーに依存する企業価値を設定しなおす(DIRECT)。このことにより、ガバナンスは適切にサイバーリスクを管理しながら、サイバー空間に依存する企業価値の最大化を達成するための業務執行(マネジメントループ)を監督していることになる。ガバナンスの要件を反映させた「サイバーリスク・エコシステム」から、このガバナンスが関わるループを摘出したものは以下になり、これをガバナンスループと呼ぶ。

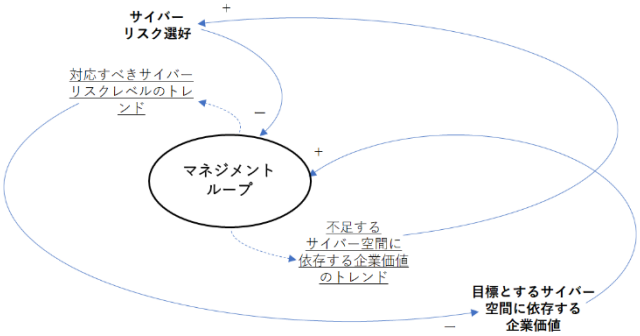

図 13　ガバナンスループ図

5. まとめ

「資源ベースの経営戦略論」[4]の考え方をサイバー空間に依存する企業価値向上の側面に、「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]の考え方をサイバーリスク管理の側面に取り入れ、さらにガバナンスの要素を追加した「サイバーリスク・エコシステム」により、１章に述べられている本稿の目的達成に道筋をつけた。

具体的には、まず、ガバナンスがサイバーリスクのレベルとサイバー空間に依存する企業価値を高めるという目標の達成度を長い時間軸でモニタリングして定めた、目標とするサイバー空間に依存する企業価値やサイバーリスク選好の値が、サイバー空間に依存する企業価値の向上とサイバーリスクの適正な管理との均衡を保つための、調整弁の役割を果たしていることを可視化できた。これにより、サイバー空間を活用した企業価値向上のために望ましいレベルのサイバーリスクを受け入れ、リスク抑制とリスク受け入れの双方向のバランスをとることができる。

また、ガバナンスとマネジメントの役割の違いを明確に可視化することで、ガバナンスの要件の１つである業務執行とその監督の役割を切り分けるシステムが、サイバーリスクレベルを最小に抑えながら、サイバー空間に依存する企業価値を最大化するための重要な役割を持っていることも可視化できた。具体的には、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やサイバーリスク選好などの目標値を設定し（What to Do）、投資やリスク対応などの目標値の実行（How to Do）はマネジメントに任すことにより、表面的な出来事に注意を奪われることなく、長い時間軸による本当の意味の企業価値向上を計ることができる。

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] 菊地正人、「システム・シンキングを用いたサイバーセキュリティリスクに対する考え方」、日本セキュリティ・マネジメント 第 31 回全国大会研究報告書、2017 年
[3] 菊地正人、「ガバナンスの視点によるシステム・シンキングを用いたサイバーセキュリティリスク管理」、日本セキュリティ・マネジメント 第 32 回全国大会研究報告書、2018 年
[4] デビッド・J・コリス、シンシア・A・モンゴメリー、「資源ベースの経営戦略」、東洋経済新報社、1998 年
[5] 一般社団法人日本内部監査協会　監訳、「COSO 全社的リスクマネジメント-戦略およびパフォーマンスとの統合」、同文舘、2018 年 4 月
[6] 湊宣明、 「[実践]システム・シンキング」 、講談社、2016 年 3 月
[7] ドネラ・H・メドウズ、 「世界はシステムで動く」、英治出版、2015 年 12 月
[8] 藤原 正弘、 「情報セキュリティ投資に対する 企業の意志決定について」、KDDI 総研調査レポート R&A、2006 年 .
[9] 田中 秀幸，松浦 幹太、「情報セキュリティ投資の経済的動機付けに関する企業レベルの実証研究」、電気通信普及財団研究調査報告書 第 21 号、 pp.9-15、2006 年.
[10] Jos Corman, David Etue, Adversary ROI: Evauating Security from the Threat Actor’s Perspective, RSA Conference Europe 2012、2012 年.
[11] Dell Inc.、Dell End-User Security Survey 2017、<http://dellsecurity.dell.com/dell-end-user-security-survey/>、2017 年 6 月 28 日アクセス.
[12] ISO/IEC 27014:2013 Information technology – Security techniques – Governance of information security