情報処理学会論文誌 Vol.60 No.12 2184–2195 (Dec. 2019)

セキュリティ対策導入にかかる時間とサイバーリスクレベル変動の関係から探る，過剰なセキュリティ対策の問題とその対策

菊地 正人[1,a)] 大久保 隆夫[1]

受付日 2019年3月11日, 採録日 2019年9月11日

概要：セキュリティ対策の実施には時間がかかるものがあるが，それによりサイバーリスクのレベルが一時的に大きくなることがある．一時的に大きくなるサイバーリスクのレベルを通常のサイバーリスク選好と比較して対応してしまうと，過剰なセキュリティ対策を実施してしまう可能性があり，生産性やセキュリティ対策のユーザビリティにも悪影響を及ぼす．そこで，本論文では，セキュリティ対策の実施に時間がかかるとサイバーリスクのレベルが一時的に大きくなる現象の仕組みを可視化することにより，過剰なセキュリティ対策を実施してしまうという問題点とその対応策を提唱する．まず，サイバーリスクを作り出している要素として，サイバー空間に依存する企業価値，サイバー空間の攻撃者，そしてサイバーリスクを軽減するセキュリティ対策とそれらの関係に注目する．そして，定性分析モデルであるシステム・シンキングの理論を適用したうえ，それらが相互に影響を与えながら，サイバーリスクのレベルの変化を導くことを可視化する．また，実施に時間がかかるセキュリティ対策がサイバーリスクのレベルを一時的に大きくする現象を，定量分析モデルであるシステム・ダイナミックスの理論を適用してシミュレーションすることにより，その問題の性質と対応策を提示することができた．

キーワード：サイバーセキュリティ，リスク選好，リスクマネジメント，システム・シンキング

Issues and Remedies for Excessive Security Controls Explored by Relationships between the Time taken to Implement Security Controls and the Fluctuation of Cyber Risk Level

Masato Kikuchi[1,a)] Takao Okubo[1]

Received: March 11, 2019, Accepted: September 11, 2019

Abstract: Cyber risk level sometimes rises for a limited time due to delay of the implementation of security controls. If such a cyber risk level is compared with a normal cyber risk appetite, there are some possibilities that excessive security controls may be implemented, and productivities and usability of security controls may be undermined. This paper proposes the issues of the implementation of excessive security controls and their remedies by visualizing how cyber risk level rises for a limited time due to delay of the implementation of security controls. First, the elements that create cyber risk: cyber accessible corporate value, attackers in cyber space, and security controls that reduce cyber risk and their relationships are highlighted. And then, how they interact each other and change cyber risk level is visualized by application of system thinking that is a qualitative analysis model. The simulation on how cyber risk level rises for a limited time due to delay of the implementation of security controls was conducted by application of system dynamics that is a quantitative analysis model. It clarified the characters of issues and their remedies.

Keywords: cybersecurity, risk appetite, risk management, system thinking

1. はじめに

企業活動のサイバー空間への依存度が高まるなか，サイバー攻撃の脅威などのサイバーリスクの話題はつきないが，一方，そのようなリスクを管理するためのセキュリティ対策によるユーザビリティや従業員の生産性への好ましくない影響も話題にのぼっている．たとえば，Dell inc. による Dell End-User Security Survey 2017 [1] では，日本を含む 8 カ国のエンドユーザである回答者の 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．

本論文では，そのセキュリティ対策の従業員の生産性への好ましくない影響の原因と考えられるもののうち，セキュリティ対策の実施に時間がかかることが，一時的にサイバーリスクのレベルを大きくしてしまい，通常のサイバーリスク選好に基づいて対応する結果，過剰なセキュリティ対策を実施してしまうという問題の性質について検証する．そして，そのような過剰なセキュリティ対策を回避するために，大きくなりがちなサイバーリスクのレベルの変動を抑えるための方法を提唱する．これにより，セキュリティ対策によるユーザビリティや従業員の生産性への好ましくない影響を軽減することが期待できる．

まず，サイバーリスクを作り出す要素とその構造について，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」[2] で提示した，トップダウン型のサイバー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）を参照する．そして，「リスクモデル」に示されている，サイバーリスクを作り出している要素として，サイバー空間に依存する企業価値，サイバー空間の攻撃者（ターゲット率），そしてサイバーリスクを軽減するセキュリティ対策（対策度）とそれらの関係に注目する．「リスクモデル」は静的なモデルであるため，システム・シンキングの理論を適用することにより時間の概念を追加して拡張する．このようにして拡張した「リスクモデル」をダイナミック・サイバーリスク・モデル（DSRM）と呼ぶ．DSRM を構築することで，サイバーリスクを作り出している要素が時間の経過とともに相互に影響を与えながら，サイバーリスクのレベルの変化を導くことを可視化する．また，実施に時間がかかるセキュリティ対策がサイバーリスクのレベルを一時的に大きくする現象を，システム・シンキングの理論の定量分析版であるシステム・ダイナミックスの理論を適用してシミュレーションすることにより，その問題の性質と対応策を示唆する．システム・シンキング理論は，複雑な構造の要素間が相互作用して生まれるまとまった機能を俯瞰・分析することに特徴がある．

なお，「リスクモデル」の中では，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され，サイバー空間に依存する企業価値はサイバー空間からアクセス可能な Asset と Process，および Capability Value の和としている．

まず，2 章において，システム・シンキングの理論のサイバーリスク管理への応用研究例を検証する．3 章において，ISMS の概要を説明している国際規格である ISO/IEC 27000:2016 の中で提示されている，セキュリティ対策の実施に時間がかかることが，一時的に情報セキュリティリスクのレベルを大きくしてしまうという問題と，その対応策の検証を可能にする DSRM の要件を特定する．4 章において，DSRM のモデル化の考え方を述べ，5 章において，システムの振舞いを定性的に推測できるシステム・シンキングの理論を適用して DSRM を構築する．6 章において，DSRM に時間の経過とともに変化するシステムの振舞いを定量的に評価できるシステム・ダイナミックスの理論を適用して，3 章において特定された要件を満たすシミュレーションを行う．7 章ではシミュレーションの結果を基に考察を行い，8 章においてこの研究をまとめる．

2. 先行研究

システム・シンキングの理論をサイバーリスク管理に応用した既存研究はいくつかある．

TrČek による研究 [3] では，インターネットの普及とともに，無数のつながるコンピュータが出現し，それまでとは比較にならないほどの様々な要素とその相互作用がリスクを生み出しているとしている．このようなリスクに対応するには従来の手法には限界があるとし，包括的なリスク管理の姿とその構成要素の動的な関係をグラフィカルに表現できるシステム・シンキングを用いた手法を提案している．

Groš による研究 [4] では，情報システムはそれを構成するリソースが複雑に相互作用してビジネスプロセスを支援するものであり，それは複雑系のシステムであり，また，その情報システムのリスク管理も複雑系のシステムに該当するとした．セキュリティインシデントは，1 つのリソースで発生するものではなく，複数のリソースを巻き込んで発生するものであるため，物事を分解した要素を独立して考える従来の手法の限界を唱え，それらの要素の相互作用を重視して考えるシステム・シンキングを用いた手法を提案している．

Branagan らの研究 [5] では，重要 IT 基盤は複雑系のシステムとしたうえ，脅威源から異常現象へつながる因果連鎖に基づいたシミュレータを利用して，重要 IT 基盤の異

[1] 情報セキュリティ大学院大学
Institute of Information Security, Yokohama, Kanagawa 221–0835, Japan
[a)] dgs188101@iisec.ac.jp

常現象を検証することを提案している．そしてその異常現象は，その表面上の現象のみの観察では将来の現象を予想することは困難であり，重要 IT 基盤が依存している様々な構成要素の相互作用を理解する必要があるとしている．インターネットの出現により，多くのシステムの相互依存が高まり，それが重要 IT 基盤の複雑性を高めており，対策が追いつかないインターネットを経由したウィルス感染の急激な拡大などのサイバーリスクの特徴を形作っているとしている．

Saunders の研究 [6] では，従来の IT セキュリティリスク分析の静的な手法の限界を唱え，定性分析を行うシステム・シンキングの定量分析版であるシステム・ダイナミクスを用いた動的な手法を提案している．ここでは，システム・ダイナミクスを用いた具体的な IT セキュリティリスク分析モデルが描かれている．

これらの研究から，システム・シンキングをサイバーリスク管理に応用する道筋を示すことができているが，情報セキュリティの目標である情報の機密性，完全性，および可用性の保護を追求したうえ，サイバーリスクを抑制する側面のみを強調していることが分かった．本論文では，システム・シンキングが表現できる時間の概念の特徴をより生かして，セキュリティ対策の時間の遅れのサイバーリスクへの影響まで含めた全体像をモデル化する．

3. ダイナミック・サイバーリスク・モデル（DSRM）の要件

ISO/IEC 27000:2016 [7] の中で，セキュリティ対策の実施には時間がかかるものがあるが，それにより通常のリスク受容基準よりもリスクのレベルが一時的に大きくなることがあり，そのような性質を持ったリスクを許容するようにリスク受容基準は考慮すべきという記述がある．これを企業のサイバーリスクのレベルにあてはめると，一時的に大きくなるサイバーリスクのレベルを通常のサイバーリスク選好と比較して対応してしまうと，過剰なセキュリティ対策を実施してしまう可能性があり，生産性やセキュリティ対策のユーザビリティにも悪影響を及ぼすことを示唆している．この課題とその対応方法を実際のデータを用いて検証するのは困難がともなうと思われるため，筆者らは，シミュレーションを用いて検証する．そのシミュレーションを行う DSRM の要件を次の 3 点とした．

- 様々な要素が相互に影響を与えながらサイバーリスクのレベルの変化を導くことを可視化できる．
- セキュリティ対策の実施に時間がかかる場合に，サイバーリスクのレベルの変動が大きくなるという現象をシミュレーションしたうえ，その性質を可視化できる．
- セキュリティ対策の実施に時間がかかる場合に，サイバーリスクのレベルの変動を抑える方法を示唆できる．

4. ダイナミック・サイバーリスク・モデル（DSRM）のモデル化の考え方

4.1 モデル化の要件

互いに影響を与えながらサイバーリスクを形作っている要素はつねに不確実性を含んでいる．DSRM のシミュレーションは過去の固定したデータから推測できるものだけでなく，将来変化するであろう要素の影響を考慮したものである必要がある．

また，様々な要素がサイバーリスクに影響を及ぼしている現象が線形とは限らず非線形であることや，影響を及ぼした原因である要素が，今度は逆に結果である要素から影響を受けるフィードバックという現象も考えられ，これらを数式に表すことは難しい．これらの現象を DSRM は可視化できる必要がある．

これらの要件を満たすモデリング手法として，システム・シンキングが考えられる．

4.2 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 [8]．

システム・シンキングは，従来のロジカル・シンキングを用いて分解した構成要素に時間の概念を加えて，それらの要素の変化が別の要素に対してどのような影響を与えるか，全体としてどのようなフィードバックが作用するかを可視的に把握することができる．

構成要素間の関係は，因果リンクと呼ばれるダイアグラムを用いて表現される．この因果リンク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** に因果リンクの例を示す．

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リンクがあり，それをフィードバックと呼ぶ．**図 2** にフィードバックループの例を示す．

フィードバックループのうち目標追求型のバランス型

図 1 因果リンク例
Fig. 1 An example of causal link.

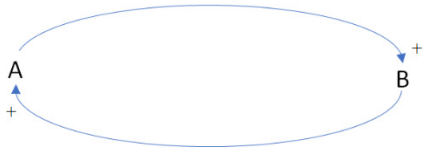


図 2 フィードバックループの例
Fig. 2 An example of feedback loop.

ループは，動的な均衡状態に接近したり，その状態を保持したりする．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作り出す [9]．

4.3 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舞いを生み出し，システムの振舞いがシステムの結果を生み出すと考える [8]．DSRM をシステムととらえて，この考え方をあてはめると，システムの結果がサイバーリスクになり，システムの構造が，サイバーリスクを生み出す要素の関係となる．システムの振舞いは，サイバーリスクを生み出す要素の相互作用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 [8]．

1. 時間軸分析
2. ステークホルダ分析
3. 変数摘出
4. 因果分析
5. 仮説構築

ステークホルダ分析を行うことにより，ステークホルダ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．

5. ダイナミック・サイバーリスク・モデル（DSRM）の構築

セキュリティ対策の実施に時間がかかることが，一時的にサイバーリスクのレベルを大きくしてしまい，過剰なセキュリティ対策を実施してしまうという問題の解決のために，4.3 節に説明されているプロセスに従いシステム・シンキングを適用して，DSRM を構築する．

5.1 時間軸分析

DSRM は，サイバーリスクを生み出す要素とそれらの関係に注目したうえ，その相互作用が生み出すサイバーリスクの変化を可視化する必要がある．本論文では，企業全体的にとらえた大きなサイバーリスクにひととおり対応するのにかかると予測される 3 年を 1 サイクルと考え，それが 4 回経過する 12 年の間に残留サイバーリスクレベルが，対策の遅れの影響の中でどのように推移するかをシミュレーションすることとする．

5.2 ステークホルダ分析

サイバーリスクと，それを生み出す要素に利害関係を有するステークホルダは，企業とする．他にも，株主，顧客，サプライヤなどが考えられるが，本論文のスコープには含まないこととする．

5.3 変数摘出

企業の関心事項，つまり問題に関する主な変数を，「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する．

- サイバー空間に依存する企業価値
- 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）

各構成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」[2] にまとめられている．たとえば，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が，具体的には，サイバー空間からアクセス可能な Asset Value，Process Value，および Capability Value の和になる．Asset Value は企業が保有している資産の価値であり，Process Value は企業の売上高であり，また，Capability Value は企業の将来の収益を生み出す価値になり，サイバー空間からアクセス可能な各 Value の例を以下に示す．

- サイバー空間からアクセス可能な Asset Value：例）貸借対照表に現れる資産のうち，論理的な価値がデジタル情報としてコンピュータ管理されている非物理資産として，ソフトウェア，特許権，預金，そして有価証券などの価値の和
- サイバー空間からアクセス可能な Process Value：例）損益計算書の売上高をそれに寄与している主要プロセスごとに分けたものに，その主要プロセスのサイバー空間依存度を乗じたものの和
- サイバー空間からアクセス可能な Capability Value：例）知的財産権や情報資産のそれぞれの損益計算書の売上高への影響分の和

そして，サイバー空間に依存する企業価値を補足する要素として，以下の変数がある．

- 目標とするサイバー空間に依存する企業価値：例）年に 10%の成長を目標にしている企業では，現在のサイ

バー空間に依存する企業価値が 1,000 億円だとすると，1 年後の目標とするサイバー空間に依存する企業価値は 1,100 億円

- 新たに作り出すサイバー空間に依存する企業価値：例）現在のサイバー空間に依存する企業価値が 1,000 億円，目標とするサイバー空間に依存する企業価値は 1,100 億円だとすると，企業活動によって，新たに作り出すサイバー空間に依存する企業価値はその不足分の 100 億円

なお，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」[2] 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．本論文では，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，そのような指標の分かりやすい名称として，対策度の名称を利用している．

5.4 因果分析

サイバーリスクを生み出す重要な要素である，サイバー空間に依存する企業価値とそれを補足する変数の因果関係は，以下のものが考えられる．

1. 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，および新たに作り出すサイバー空間に依存する企業価値

また，サイバー空間に依存する企業価値を補足する変数の 1 つである，新たに作り出すサイバー空間に依存する企業価値は，新たに生じるサイバーリスクレベルを生み出す．その新たに生じるサイバーリスクレベルに関連して，「リスクモデル」の構成要素とその関係から導かれる変数間の因果関係は，以下のものが考えられる．

2. 新たに作り出すサイバー空間に依存する企業価値と新たに生じるサイバーリスクレベル
3. ターゲット率と新たに生じるサイバーリスクレベル
4. 対策度と新たに生じるサイバーリスクレベル

そして，新たに生じるサイバーリスクレベルが蓄積していく残留サイバーリスクレベルと，それを補足する変数の因果関係は，以下のものが考えられる．

5. 残留サイバーリスクレベル，新たに生じるサイバーリスクレベル，サイバーリスク選好，低減させるべきサイバーリスクレベル，低減中のサイバーリスクレベル，および低減済みのサイバーリスクレベル

これらの変数の因果関係を統合した DSRM 因果ループ図を**図 3** に示す．

以降では，各因果関係の根拠について説明する．

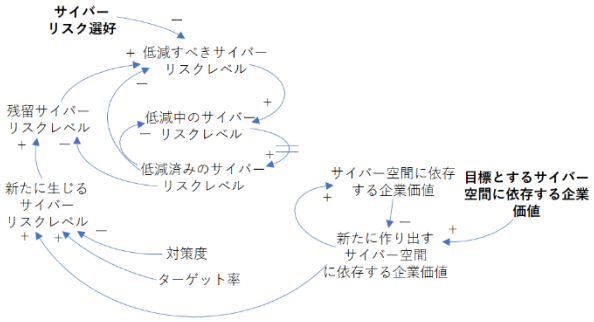


図 3 DSRM 因果ループ図
Fig. 3 DSRM causal link diagram.

5.4.1 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，および新たに作り出すサイバー空間に依存する企業価値

「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」[2] では，企業経営者のミッションとして企業価値の向上をあげている．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，その不足分（新たに作り出すサイバー空間に依存する企業価値）を満たすために企業活動が行われる．サイバー空間に依存する企業価値の増加は，新たに作り出す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．つまり，現在のサイバー空間に依存する企業価値が増加すると，目標とするサイバー空間に依存する企業価値との差が縮まるため，その差を埋めるための新たに作り出すサイバー空間に依存する企業価値が減少する．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，新たに作り出す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．つまり，目標とするサイバー空間に依存する企業価値が増加すると，現在のサイバー空間に依存する企業価値との差がひらくため，その差を埋めるための新たに作り出すサイバー空間に依存する企業価値が増加する．そして，新たに作り出す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．以上の根拠により，これらの因果関係は妥当であると見なせる．

たとえば，現在のサイバー空間に依存する企業価値が 1,000 億円，目標とするサイバー空間に依存する企業価値は 1,100 億円だとすると，企業活動によって，新たに作り出すサイバー空間に依存する企業価値はその不足分の 100 億円になる．もし，現在のサイバー空間に依存する企業価値が増加して 1,100 億円になると，目標とするサイバー空間に依存する企業価値との差がなくなり，企業活動によって，新たに作り出すサイバー空間に依存する企業価値は減少してゼロになる．一方，目標とするサイバー空間に依存する企業価値が増加して 1,200 億円になると，現在のサイバー空間に依存する企業価値との差が開き，企業活動によって，新たに作り出すサイバー空間に依存する企業価値

は増加して 200 億円になる．

5.4.2 新たに作り出すサイバー空間に依存する企業価値と新たに生じるサイバーリスクレベル

新たに作り出すサイバー空間に依存する企業価値を原因，新たに生じる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，新たに作り出すサイバー空間に依存する企業価値が増加した場合は，新たに生じるサイバーリスクレベルが増加する関係がある．ISO/IEC 27000:2016 [7] の中で，リスクの 1 つの定義は，イベントの影響度とその発生確率の組合せとなっている．新たに作り出すサイバー空間に依存する企業価値が高まると，サイバー攻撃のイベントの影響度が高くなるため，新たに生じるサイバーリスクレベルも高まる一因となる．以上の根拠により，この因果関係は妥当であると見なせる．

たとえば，ISO/IEC 27000:2016 [7] の中のリスクの定義に照らし合わせると，サイバー攻撃のイベントの発生確率が 20%，新たに作り出すサイバー空間に依存する企業価値が 100 億円のためそれに対するサイバー攻撃の影響度が 100 億円の場合は，新たに生じるサイバーリスクレベルは 20 億円となる．また，新たに作り出すサイバー空間に依存する企業価値が 200 億円に増加した場合はそれに対するサイバー攻撃の影響度が 200 億円になるため，新たに生じるサイバーリスクレベルも増加して 40 億円となる．

5.4.3 ターゲット率と新たに生じるサイバーリスクレベル

ターゲット率を原因，新たに生じる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．ISO/IEC 27000:2016 [7] の中で，リスクの 1 つの定義は，イベントの影響度とその発生確率の組合せとなっている．ターゲット率が増加するというのは，サイバー攻撃のイベントの発生確率が増加することであるため，新たに生じるサイバーリスクレベルも増加する一因となる．以上の根拠により，この因果関係は妥当であると見なせる．

たとえば，ISO/IEC 27000:2016 [7] の中のリスクの定義に照らし合わせると，影響度が 1 億円，サイバー攻撃を受ける可能性であるターゲット率が 20%のため発生確率が 20%の場合，サイバーリスクレベルは 2,000 万円となる．また，サイバー攻撃を受ける可能性であるターゲット率が 40%に増加した場合は発生確率が 40%になるため，サイバーリスクレベルも増加して 4,000 万円となる．

5.4.4 対策度と新たに生じるサイバーリスクレベル

対策度を原因，新たに生じる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．ISO/IEC 27000:2016 [7] の中で，対策（Control）の定義は，リスクを変更する処置となっている．サイバーリスクの対策は通常，サイバーリスクを低減させる処置であるため，対策度が増加した場合は，新たに生じるサイバーリスクを減少させる一因となる．以上の根拠により，この因果関係は妥当であると見なせる．

たとえば，ISO/IEC 27000:2016 [7] の中のリスクの定義に照らし合わせると，影響度が 1 億円，サイバー攻撃を受ける可能性であるターゲット率が 20%のため発生確率が 20%の場合，サイバーリスクレベルは 2,000 万円になる．ISO/IEC 27000:2016 [7] の中の対策（Control）の定義に照らし合わせると，対策度が 20%の場合，サイバーリスクレベルは 20%減少して 1,600 万円となる．また，対策度が 40%に増加した場合は，サイバーリスクレベルは 40%減少して 1,200 万円となる．

5.4.5 残留サイバーリスクレベル，新たに生じるサイバーリスクレベル，サイバーリスク選好，低減させるべきサイバーリスクレベル，低減中のサイバーリスクレベル，および低減済みのサイバーリスクレベル

企業は，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下回らない限り，残留サイバーリスクレベルが増加すれば，それを低減させることを選択する．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低減させるべきサイバーリスクレベルという変数として追加した．ISO/IEC 27000:2016 [7] の中で，リスク評価の定義は，リスク分析の結果をリスク基準と比較して，リスクを受容するか判断するとなっている．残留サイバーリスクレベルの増加は，リスク基準を上回り低減させるべきサイバーリスクレベルを増加させる一因になるが，一方，サイバーリスク選好の増加は，残留サイバーリスクレベルがリスク基準を下回り低減させるべきサイバーリスクレベルを減少させる一因にもなる．以上の根拠により，これらの因果関係は妥当であると見なせる．

たとえば，ISO/IEC 27000:2016 [7] の中のリスク評価の定義に照らし合わせると，サイバーリスク選好が 10 億円のためリスク基準が 10 億円の場合，残留サイバーリスクレベルが 10 億円であると低減させるべきサイバーリスクレベルはゼロになるが，残留サイバーリスクレベルが 12 億円に増加すると，低減させるべきサイバーリスクレベルも増加して 2 億円になる．また，残留サイバーリスクレベルが 10 億円の場合，サイバーリスク選好が 8 億円のためリスク基準が 8 億円であると，低減させるべきサイバーリスクレベルは 2 億円になるが，サイバーリスク選好が 10 億円に増加したためリスク基準が 10 億円になると，低減させるべきサイバーリスクレベルはゼロに減少する．

また，セキュリティ対策を実施してサイバーリスクレベルを低減させるには一般的に時間がかかるため，低減させるべきサイバーリスクレベルについてその進捗状況ごとに，セキュリティ対策の導入が開始された低減中のサイバーリスクレベル，セキュリティ対策の導入が完了した低減済みのサイバーリスクレベルという変数も追加した．低減させるべきサイバーリスクレベルの増加は，低減中のサイバーリスクレベルの増加の原因になり，また，低減中のサイバーリスクレベルの増加は，セキュリティ対策の効果

の遅れをともない，低減済みのサイバーリスクレベルの増加の原因になるとする．そして，低減済みのサイバーリスクレベルの増加は，低減中のサイバーリスクレベル，低減させるべきサイバーリスクレベル，そして残留サイバーリスクレベルの減少の原因になるとする．

たとえば，低減させるべきサイバーリスクレベルが 2 億円の場合，そのリスクへのセキュリティ対策の導入が開始されると，低減中のサイバーリスクレベルが 2 億円になり，セキュリティ対策の導入が完了すると，低減済みのサイバーリスクレベルが 2 億円になる．低減させるべきサイバーリスクレベルが 4 億円に増加すれば，そのリスクへのセキュリティ対策の導入が開始されると，低減中のサイバーリスクレベルも増加して 4 億円になり，セキュリティ対策の導入が完了すると，低減済みのサイバーリスクレベルも増加して 4 億円になる．そして，前者では，低減済みのサイバーリスクレベルが 2 億円になった時点で，低減させるべきサイバーリスクレベル，低減中のサイバーリスクレベル，および残留サイバーリスクレベルが 2 億円減るが，後者では，低減済みのサイバーリスクレベルの増加幅が広がり 4 億円になった時点で，低減させるべきサイバーリスクレベル，低減中のサイバーリスクレベル，および残留サイバーリスクレベルの減少幅が広がり 4 億円減る．

6. ダイナミック・サイバーリスク・モデル（DSRM）のシミュレーション

5 章において，システムの振舞いを定性的に推測できるシステム・シンキングの理論を適用して，DSRM 因果ループ図を構築した．そのモデルに，時間の経過とともに変化するシステムの振舞いを定量的に評価できるシステム・ダイナミックスの理論を適用して DSRM ストック・フロー図を構築したうえ，シミュレーションを行う．

6.1 定性分析モデルから定量分析モデルへの変換

6.1.1 システム・ダイナミックスの考え方

システム・ダイナミックスでは，時間の経過とともに変化するシステムの振舞いを定量的に評価するために，ストック・フロー図というモデル表現法を用いている [8]．ストック・フロー図では，ストック，フロー，バルブ，クラウドと呼ばれる 4 つの要素を用いてシステムの構造を表現する．

ストックとはシステム内における物質などの蓄積を再現する要素で，長方形を用いて表す．フローはシステム内の物質などの流れを再現する要素で，先端に矢印のついたパイプ形状で表現する．フローには，ストックへの物質などの流入を再現するインフロー，ストックからの物質などの流失を再現するアウトフロー，そしてインフローとアウトフローの両方を再現するバイフローの 3 種類がある．バルブは，フローの流れをコントロールする役目を果たし，水道の蛇口の形状で表す．クラウドはシステムの境界を定義する要素で，雲形の形状で表す．フローの始点に接続されたクラウドをとくにソースと呼び，これによりシステム外からシステム内への資源投入を再現できる．逆に，フローの終点に接続されたクラウドをとくにシンクと呼び，システム内からシステム外への資源流出を再現できる．

図 4 フィードバックループにおける表現例
Fig. 4 An example of feedback loop.

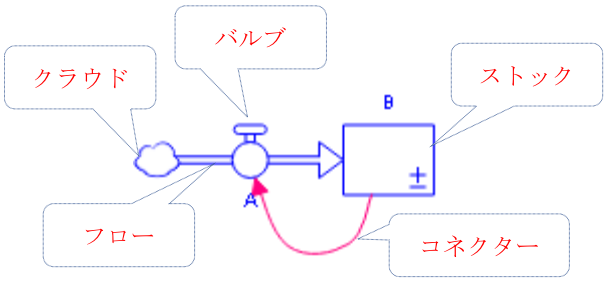


図 5 ストック・フロー図における表現例
Fig. 5 An example of stock and flow diagram.

また，ストックとフロー以外の要素を表すコンバータがある．コンバータは円形を用いて表され，補助変数や定数を定義するために用いられる．フローとコンバータの違いは，フローは必ずストックの増減を直接的にもたらすのに対して，コンバータはストックの増減を直接的にもたらすことはないという点である．これらの要素間の情報の流れを記述するためにコネクタを用いることもある．コネクタは，矢印で表される．

4.2 節で表現した因果ループのフィードバックループ例を**図 4**，それをストック・フロー図に変換したものを**図 5** として示した．

6.1.2 システム・ダイナミックスを適用したモデルの構築

5 章において構築した DSRM 因果ループ図にシステム・ダイナミックスの理論を適用するために，以下のように，DSRM 因果ループ図の変数を，ストック・フロー図の要素に割り当てる．

（ストック）

DSRM 因果ループ図の変数の中で，ストックに該当するものは，以下とする．

- 残留サイバーリスクレベル
- 低減中の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

なお，サイバーリスクの大きさを表現するために使われるユニットについては，様々なものがあるが，「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」[2] で提示した「リスクモデル」の中では，サイバーリスクの大きさを金額で表している．DSRM では，その「リスクモデル」から変数を導いているため，サイバーリスクの大きさを表す変数の値はすべて金額で表している．

（フロー）

DSRM 因果ループ図の変数の中で，フローに該当するものは，ストックである低減中のサイバーリスクレベルへのフローとして以下とする．

- 低減させるべきサイバーリスクレベル
- 低減済みのサイバーリスクレベル

（コンバータ）

DSRM 因果ループ図の変数の中で，コンバータに該当するものは，以下とする．

- サイバーリスク選好
- 目標とするサイバー空間に依存する企業価値
- 新たに作り出すサイバー空間に依存する企業価値
- 対策度
- ターゲット率

また，低減済みのサイバーリスクレベルのパラメータとして，それぞれ以下をコンバータとして追加する．

- 対応の遅れ
- 対応率

対応の遅れは，低減中のサイバーリスクレベルが，セキュリティ対策の導入が完了して，低減済みのサイバーリスクレベルになるまでにかかる時間を表すものとする．また，対応率は，その低減中のサイバーリスクレベルが，セキュリティ対策の導入が完了して，低減済みのサイバーリスクレベルになる割合を表すものとする．つまり，セキュリティ対策がサイバーリスクレベルを低減する割合を表す．

そして，サイバーリスク選好は，目標とするサイバー空間に依存する企業価値にサイバーリスク選好係数をかけたもの，目標とするサイバー空間に依存する企業価値は，サイバー空間に依存する企業価値に目標企業価値係数をかけたものとし，それぞれの係数も以下のようにコンバータに該当するものとする．

- サイバーリスク選好係数
- 目標企業価値係数

上記でストック・フロー図の要素に割り当てられた変数に，DSRM 因果ループ図に表現されている因果関係を反映させて構築した DSRM ストック・フロー図を**図 6** に示す．

6.2 定量分析モデルを利用したシミュレーション

6.2.1 シミュレーションの仮定

DSRM ストック・フロー図を利用してシミュレーションするために，**表 1** に示した性格を持つ企業を仮定する．

独立行政法人情報処理推進機構の 2014 年度情報セキュリティ事象被害状況調査報告書 [10] によると，サイバー

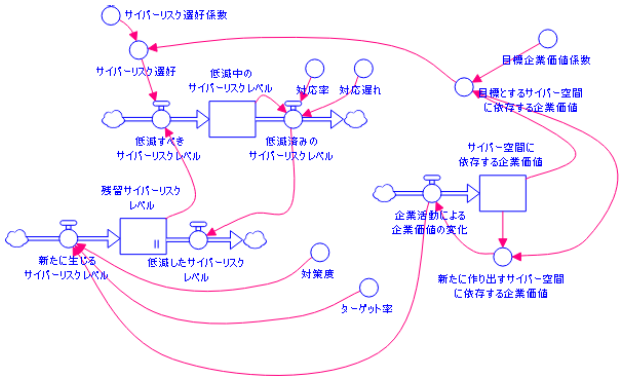


図 6 DSRM ストック・フロー図
Fig. 6 DSRM stock and flow diagram.

表 1 想定企業例
Table 1 An example of an assumed company.

変数	値
目標企業価値係数	1.1 (110%)
サイバー空間に依存する企業価値	1000 億円
サイバーリスク選好係数	0.01 (1%)
ターゲット率	0.2 (20%)
対策度	0.6 (60%)
対応率	1 (100%)
残留サイバーリスクレベル	20 億円
低減中のサイバーリスク	0 円

攻撃の遭遇率は 19.3%となっているため，ターゲット率は 20%とした．サイバー攻撃に遭遇したケースのうち，目に見える形で被害にあったケースは 22%であったが，実際には被害がすぐに見える形ではなくてもサイバー攻撃が情報資産に影響を及ぼしているケースがもっとあり 40%ほどであろうという推定のもと，対策度は 60%とした．企業価値の評価額が 10 億ドル以上の未上場のテクノロジ企業はユニコーン企業と呼ばれ注目されている [11] が，これらの企業の価値はほとんどサイバー空間に依存するものと思われるため，サイバー空間を積極的に利用している典型的な企業のサイバー空間に依存する企業価値を 1,000 億円とした．日経平均株価の 2009 年から 2018 年までの 10 年間の CAGR（年平均成長率）は 10.02%になるため，目標企業価値係数を 1.1 とし，毎年，サイバー空間に依存する企業価値を 10%増加させることを目標とした．日本情報システム・ユーザー協会の第 23 回企業 IT 動向調査 2017 企業 [12] によると，企業では売上高のほぼ 1%を IT に投資している．IT には全般的に何らかのサイバーリスクへの対策の要素が含まれていることと，通常，リスクへの対策はリスクの大きさと対策のコストを比較して行うことを考慮すると，企業は許容できるサイバーリスクの大きさに比例してセキュリティ対策を含んだ IT への投資を行っているととらえることができる．これらのことから，サイバーリスク

選好は，現実的と思われる値である企業価値の 1%とした．セキュリティ対策がサイバーリスクレベルを低減させる割合である対応率は 100%とする．

なお，シミュレーションを開始する時点で，残留サイバーリスクレベルはサイバーリスク選好を上回る 20 億円，低減中のサイバーリスクレベルはなしとする．また，ターゲット率と対策度はシミュレーションの中で変化しないものとする．

6.2.2 問題を可視化するためのシミュレーションとその結果

セキュリティ対策の実施に時間がかかる場合に生まれる残留サイバーリスクレベルの大きな変動の性質を可視化するために，この企業において，DSRM ストック・フロー図の中の変数である対応の遅れを以下のように異なる値に変化させたうえ，今後 12 年間のシミュレーションをそれぞれ行った．サイバーリスクに関連しない要素はすべて変動しないと仮定する．

Run 1: 0.0（0 年）
Run 2: 0.2（0.2 年）
Run 3: 0.4（0.4 年）
Run 4: 0.7（0.7 年）
Run 5: 1.0（1 年）

シミュレーションでは，変数の計算に実際のサイバーリスクレベルの変動をより正確に反映させるという面（計算頻度が高い方が計算の正確度が高くなる）と，変数の計算のシミュレーションソフトへの負荷を抑えるという面（計算頻度が低い方がシミュレーションソフトへの負荷が低くなる）を考慮したうえ，各変数の計算の最適な頻度を四半期とした．最初の計算の時点で，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が低減させるべきサイバーリスクレベルに代入される．そして，次の計算の時点で，セキュリティ対策の導入を開始したものとして，低減させるべきサイバーリスクレベルは低減中のサイバーリスクレベルに加算されリセットされる．そして，対応の遅れが 0 に設定されている場合は，次の計算の時点で，セキュリティ対策の導入が完了したものとして，低減中のサイバーリスクレベルが低減済みのサイバーリスクレベルに代入され，その代入された分は低減中のサイバーリスクレベルから減算されるが，同時に新たに低減させるべきサイバーリスクレベルが加算される．対応の遅れが 0 以上に設定されている場合は，低減中のサイバーリスクレベルは，低減済みのサイバーリスクレベルに，対応の遅れで指定された時間間隔で平均化して加算され，その加算された分は同様に平均化して低減中のサイバーリスクレベルから減算される．これは，実際にはセキュリティ対策の導入開始によりサイバーリスクレベルは時間比率で少しずつ低減されることを考慮したものである．

低減中のサイバーリスクレベルは任意の時点で計算されるが，その単位ごとのサイバーリスクレベルをゼロにするためのセキュリティ対策が開始される．任意の時点で計算された低減中のサイバーリスクレベルは，セキュリティ対策の導入が開始され，それが対応の遅れに指定されたセキュリティ対策にかかる時間が経過して完了するとゼロになる．これは，任意の間隔でまとめてセキュリティ対策が必要なサイバーリスクレベルを把握したうえ，一括してそれへのセキュリティ対策を行うというリスク管理プロセスが前提になっている．

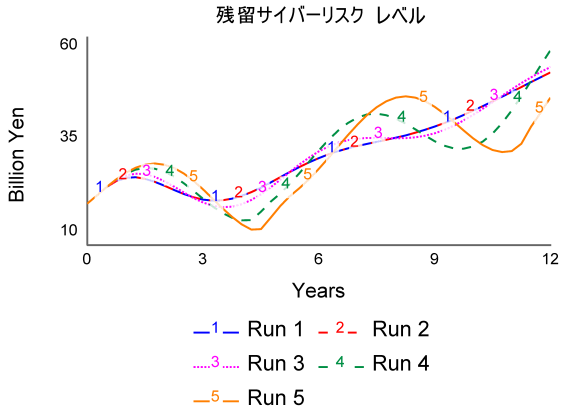


図 7 残留サイバーリスクレベル（対応の遅れの影響の比較）
Fig. 7 Residual cyber risk level (comparison of impacts of delay of control implementation).

なお，実際は個々のサイバーリスクへのセキュリティ対策は様々であり，その実施にかかる時間も様々であるが，このシミュレーションでは，セキュリティ対策にかかる時間の影響をより明確に把握するため，任意の間隔で把握したサイバーリスクレベルへ一括して行うセキュリティ対策にかかる時間は，一様に対応の遅れに指定された時間であるという仮定を用いた．実際に，個々のサイバーリスクに対するセキュリティ対策の導入開始から完了にかかる時間が異なる場合は，残留サイバーリスクレベルの変動への影響はより小さくなると思われる．

それぞれのシミュレーションの結果，残留サイバーリスクレベルの推移の様子は**図 7** のようになった．セキュリティ対策の実施にかかる時間である対応の遅れが長いと，残留サイバーリスクレベルの変動が大きくなる．たとえば，対応の遅れがないシミュレーションである Run 1 は，残留サイバーリスクレベルの推移が直線に近いが，対応の遅れが 1 年のシミュレーションである Run 5 は，残留サイバーリスクレベルの推移がいくつかの山を描いている．

6.2.3 対応策を可視化するためのシミュレーションとその結果

セキュリティ対策の実施に時間がかかる場合に，サイバーリスクのレベルの変動を抑える方法を検証するために，DSRM ストック・フロー図の中の変数である対応の遅れを 1 年に固定したまま，対応率を以下のように異なる値

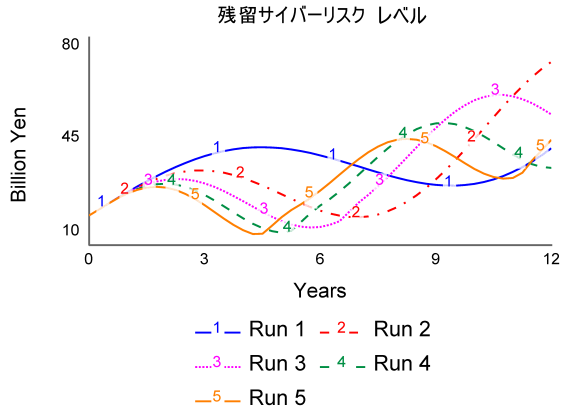


図 8 残留サイバーリスクレベル（対応率の影響の比較）
Fig. 8 Residual cyber risk level (comparison of impacts of risk reduction rate of control).

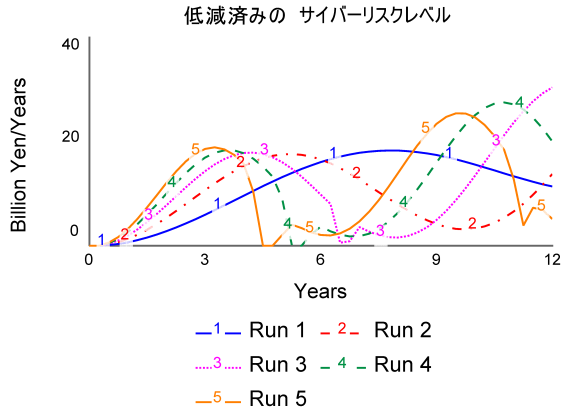


図 9 低減済みのサイバーリスクレベル（対応率の影響の比較）
Fig. 9 Reduced cyber risk level (comparison of impacts of risk reduction rate of control).

に変化させたうえ，今後 12 年間のシミュレーションをそれぞれ行った．

Run 1: 0.2（20%）
Run 2: 0.4（40%）
Run 3: 0.6（60%）
Run 4: 0.8（80%）
Run 5: 1.0（100%）

それぞれのシミュレーションの結果，残留サイバーリスクレベルの推移の様子は図 8 のようになった．

セキュリティ対策がサイバーリスクレベルを低減させる割合である対応率が低い方が，残留サイバーリスクレベルの変動が小さくなる．たとえば，対応率が 100%のシミュレーションである Run 5 は，残留サイバーリスクレベルの推移がいくつかの山を描いているが，対応率が 20%のシミュレーションである Run 1 は，描いている山がよりなだらかになっている．つまり，12 年間の間に，Run 1 の残留サイバーリスクレベルの最低レベルは，対応率がより高いどのシミュレーションの残留サイバーリスクレベルの最低レベルよりも高いが，最高レベルは，対応率がより高いどのシミュレーションの残留サイバーリスクレベルの最高レベルよりも低く収まっている．

また，それぞれのシミュレーションの結果，低減済みのサイバーリスクレベルの推移の様子は図 9 のようになった．

セキュリティ対策がサイバーリスクレベルを低減させる割合である対応率が高いと，低減するサイバーリスクレベルの変化が作る山が険しいが，対応率が低いと緩やかになる．

7. 考察

7.1 問題を可視化するためのシミュレーションの考察

問題を可視化するためのシミュレーションと図 7 に示されるその結果により，3 章で定義された以下の要件を満たすことができた．

- 様々な要素が相互に影響を与えながらサイバーリスクのレベルの変化を導くことを可視化できる．
- セキュリティ対策の実施に時間がかかる場合に，サイバーリスクのレベルの変動が大きくなる現象をシミュレーションしたうえ，その性質を可視化できる．

図 7 に示されるシミュレーションの結果は，ISO/IEC 27000:2016 [7] の中で記述されている，セキュリティ対策の実施には時間がかかるものがあり，それにより通常のリスク受容基準よりもリスクのレベルが一時的に大きくなるという現象と一致している．シミュレーションでは，セキュリティ対策の実施にかかる時間を長くすると，残留サイバーリスクレベルの変動が大きくなり，セキュリティ対策の実施にかかる時間が短い場合と比較して，一時的に残留サイバーリスクレベルが大きくなっている．これは，ある時点で同じリスクレベルの環境においても，そのセキュリティ対策の実施にかかる時間が異なると，その後の任意の時点ではリスクレベルが異なることを意味していて，通常のリスク受容基準よりもリスクのレベルが一時的に大きくなるという現象につながる．以上の根拠により，DSRM，および対応の遅れを異なる値に変更させて，時間の経過とともに変化する DSRM の振舞いを定量的に評価したこのシミュレーションは，妥当であると見なせる．

セキュリティ対策の実施に時間がかかる場合に生まれる残留サイバーリスクレベルの大きな変動は，以下の要素のサイクルの繰返しによるものといえる．

1. サイバー空間に依存する企業価値が増加すると，残留サイバーリスクレベルが増加していく．そして，増加した残留サイバーリスクレベルとサイバーリスク選好を比較して，そのギャプの分を低減させようとセキュリティ対策の実施を決める．
2. セキュリティ対策の実施を決めてから，実際に残留サイバーリスクレベルが低減するまで時間の差が生まれる．そのため，引き続き残留サイバーリスクレベルが増加していく．

3. 一時的に増加した残留サイバーリスクレベルとサイバーリスク選好を比較して，そのギャプの分を低減させようと過剰なセキュリティ対策を実施する結果，今度は，時間の遅れをともない急激に残留サイバーリスクレベルが減少していく．
4. サイバーリスク選好と比較してセキュリティ対策を抑制するようになる．

7.2 対応策を可視化するためのシミュレーションの考察

対応策を可視化するためのシミュレーションと図 8，および図 9 に示されるその結果により，3 章で定義された以下の要件を満たすことができた．

- セキュリティ対策の実施に時間がかかる場合に，サイバーリスクのレベルの変動を抑える方法を示唆できる．

セキュリティ対策の実施に時間がかかる場合に，サイバーリスクのレベルの変動を抑える方法として，セキュリティ対策がサイバーリスクレベルを低減させる割合である対応率を低くすることを示唆している．

図 8 に示されるシミュレーションの結果は，ISO/IEC 27000:2016 [7] の中で記述されている，セキュリティ対策の実施に時間がかかることにより，一時的に大きくなったリスクのレベルを許容するようにリスク受容基準は考慮すべきという考え方と一致している．セキュリティ対策がサイバーリスクレベルを低減させる割合である対応率を下げるということは，リスクレベルを単純にリスク受容基準まで低減するまでセキュリティ対策を行うということではなく，リスク受容基準を超えるリスクレベルもある程度許容するレベルまでセキュリティ対策を行うということになる．以上の根拠により，DSRM，および対応率を異なる値に変更させて，時間の経過とともに変化する DSRM の振舞いを定量的に評価したこのシミュレーションは，妥当であると見なせる．

セキュリティ対策がサイバーリスクレベルを低減させる割合である対応率を下げると，対応率が高い場合と比較して，残留サイバーリスクレベルはゆるやかに低減していく．しかし，その残留サイバーリスクレベルの低減効果は長い時間軸で見ると，対応率が高いときに起こる特定の時間に現れる偏りがやわらぎより均等になるため，残留サイバーリスクレベルの変動をやわらげることができる．

7.3 シミュレーションの結論

問題を可視化するためのシミュレーションにより，セキュリティ対策の実施に時間がかかることが，過剰なセキュリティ対策につながる残留サイバーリスクレベルの大きな変動を生み出す現象を，可視化することができた．また，対応策を可視化するためのシミュレーションにより，残留サイバーリスクレベルが大きく変動することを抑制する方法として，セキュリティ対策がサイバーリスクレベルを低減させる割合（対応率）を低くすることを示唆できた．残留サイバーリスクレベルの大きな変動を抑制することにより，ユーザビリティや従業員の生産性へ好ましくない影響を与える過剰なセキュリティ対策を軽減することが期待できる．

なお，今回のシミュレーションでは，特定の性格を持つ企業のみを仮定しているため，今後の研究では様々な性格を持つ企業を仮定としたシミュレーションも検証する必要がある．また，実際の企業ではビジネス環境はつねに変化しているため，ビジネス環境を変数として組み込んだシミュレーションや，実際のデータを用いたシミュレーションの結果の有効性の検証を検討している．

8. まとめ

セキュリティ対策の実施に時間がかかることが，残留サイバーリスクレベルの変動を大きくしてしまい，一時的に残留サイバーリスクのレベルが大きくなったときも通常のサイバーリスク選好に基づいて対応する結果，過剰なセキュリティ対策を実施してしまうという問題について検証したうえ，その対応策を示唆することができた．

具体的には，「リスクモデル」に示されているサイバーリスクを作り出している要素として，サイバー空間に依存する企業価値，サイバー空間の攻撃者（ターゲット率），そしてサイバーリスクを軽減するセキュリティ対策（対策度）とそれらの関係に注目した．「リスクモデル」は静的なモデルであるため，システム・シンキングの理論の適用により時間の概念を追加して，そのような要素が相互に影響を与えながら，サイバーリスクのレベルの変化を導くことを可視化した DSRM を構築した．DSRM に，時間の経過とともに変化するシステムの振舞いを定量的に評価できるシステム・ダイナミックスの理論を適用して，セキュリティ対策にかかる時間の変化が，残留サイバーリスクレベルの変動にどのように影響を与えるかをシミュレーションした．そして，セキュリティ対策の実施に時間がかかることが，残留サイバーリスクレベルの変動を大きくする現象を確認したうえ，その現象を抑制する方法として，セキュリティ対策がサイバーリスクレベルを低減させる割合（対応率）を低くすることが示唆できた．

企業にとっては，生産性の犠牲を最小限にした適切なレベルのセキュリティ対策を導入するには様々な課題が存在するが，本論文で提案した DSRM とそのシミュレーションを応用することにより，将来的には，そのような課題の本質的な原因と解決策の把握に貢献することが考えられる．とくに，サイバーリスクに対応するための過剰なセキュリティ対策による介入は，生産性を下げるばかりか，サイバーリスクをかえって増幅させる効果も場合によってはあるため，企業は DSRM とそのシミュレーションが可視化するそのような反応の仕組みを参考にして，過剰ではない

必要十分なセキュリティ対策を実施する方法を見出すことができる．たとえば，導入に時間がかかるセキュリティ対策を用いる場合は，通常のサイバーリスク選好に従ってセキュリティ対策を行っているとサイバーリスク変動が大きくなり，必要以上の過剰なセキュリティ対策を行い，ユーザビリティや従業員の生産性を損なうことになる．そこで，サイバーリスク選好よりもサイバーリスクレベルが大きくなっても，短期的にはそのサイバーリスクレベルを受け入れ，サイバーリスクをさらに下げるためのセキュリティ対策を控える．それにより，サイバーリスクレベルの変動を抑えられ，必要以上の過剰なセキュリティ対策を行うことを避けられ，ユーザビリティや従業員の生産性を損なうことを回避できる．

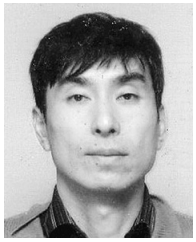
DSRMの構成要素やその関係は，それぞれ適切な根拠のもとに定義されており，DSRMのシミュレーションが提供する情報に，一定度の正確性が推測されるが，研究の次のステップとして，実際のデータを用いたその有効性の検証を検討している．

参考文献

[1] Dell Inc.: Dell End-User Security Survey 2017, available from ⟨http://dellsecurity.dell.com/dell-end-user-security-survey/⟩ (accessed 2017-06-28).
[2] 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).
[3] Trček, D.: Using System Dynamics for Managing Risks in Information Systems, *WSEAS Trans. Information Science & Applications*, Vol.5, No.2, pp.175–180 (2008).
[4] Groš, S.: Complex systems and risk management, *MIPRO* (2011).
[5] Branagan, M., Dawson, R. and Longley, D.: SECURITY RISK ANALYSIS FOR COMPLEX SYSTEMS, *ISSA* (2006).
[6] Saunders, J.H.: A Dynamic Risk Model for Information Technology Security in a Critical Infrastructure Environment, *10th United Engineering Foundation Conference* (2002).
[7] ISO/IEC 27000:2016 Information technology – Security techniques – Information security management systems – Overview and vocabulary
[8] 湊 宣明：[実践] システム・シンキング，講談社 (Mar. 2016).
[9] ドネラ・H・メドウズ：世界はシステムで動く，英治出版 (Dec. 2015).
[10] 独立行政法人情報処理推進機構：2014 年度情報セキュリティ事象被害状況調査報告書 (Jan. 2015).
[11] ウィキペディア，ユニコーン企業，入手先 ⟨https://ja.m.wikipedia.org/wiki/ユニコーン企業_(ファイナンス)⟩（参照 2019-06-28）.
[12] 日本情報システム・ユーザー協会：第 23 回 企業 IT 動向調査 2017（16 年度調査）(May 2017).

菊地 正人 （正会員）

情報セキュリティ大学院大学．1995 年 University of Manchester，Master of Science in Computation．ISO/IEC SC27 WG1 エキスパート．Fellow of the British Computer Society．2007 年より日本オラクル所属．



大久保 隆夫 （正会員）

情報セキュリティ大学院大学．1991 年東京工業大学大学院物理情報工学専攻修了．同年株式会社富士通研究所入社．2006 年情報セキュリティ大学院大学入学，2009 年同修了．博士（情報学）．2013 年より情報セキュリティ大学院大学准教授．2014 年より同教授．情報処理学会コンピュータセキュリティ研究会専門委員．電子情報通信学会会員，日本ソフトウェア科学会会員，IEEE CS 会員，Aviation Security 研究会幹事，脅威分析研究会幹事．専門はシステムセキュリティ，セキュリティ・バイ・デザイン．