Vol.2020-CSEC-91 No.6
Vol.2020-SPT-40 No.6
Vol.2020-EIP-90 No.6
2020/11/25

サイバーフィジカル空間におけるリスク連鎖を考慮した防御分析モデルの提案

大山慎雄[1] 金井敦[1] 谷本茂明[2] 畑島隆[3]

概要：組織における情報漏洩のリスクやその対策には，リスクの連鎖や複数リスクに効果を発揮する対策の存在など，複雑な関係性がある．このため，多くの機器が混在する環境では，インシデントの検出やインシデント対応のための管理・監視箇所の決定が困難であることから，リスクの把握や防御対策の最適化が経験的に行われていることが問題視されている．加えて，リスクの分析と評価はサイバー空間と物理空間を分離した形で行われることが多く，これらが絡み合った現実には必ずしも対応できていないことも課題とされている．本研究では，サイバー空間と物理空間を統合し，これらのリスク連鎖を状態遷移図で表現し，さらにリスク対策を実施した結果を可視化するモデルおよびその分析手法を提案する．これにより，現実に発生するリスクの状況変化への対応を可能とし，クリティカルパスの概念に基づき関連リスクに対する防御の最適化ならびに防御コスト最適化が可能となることについて言及する．

キーワード：リスク分析

A Proposal of Defensive Analysis Model Considering Risk Chains in Cyber-Physical Space

YOSHIO OYAMA[1] ATUSYI KANAI[1]
SYIGEAKI TANIMOTO[2] TAKASHI HATASIMA[3]

Abstract: There is a complex relationship between the risks of information leakage in an organization and its countermeasures, such as a chain of risks and the existence of countermeasures that are effective for multiple risks. In an environment with many devices, it is difficult to detect incidents and decide where to control and monitor for incident response, and therefore, the optimization of risk identification and defense measures is considered to be a problem. In addition, the analysis and assessment of risk is often done in a way that separates cyber and physical space, which does not always correspond to the intertwined reality. In this paper, we propose a model that integrates cyber and physical space, represents these risk chains as a state transition diagram, and visualizes the results of the risk countermeasures. This enables us to respond to the changes in the situation of the real risk and to optimize the defense against the related risk and defense cost based on the concept of the critical path.

Keywords: Risk Analysis

1. はじめに

会社などの組織において，情報漏洩は長らく問題となっている．近年では，内部不正による情報漏洩が情報セキュリティ 10 大脅威に入っている[1]．そのため組織では，情報漏洩リスクを下げるために対策を施す必要がある．しかし組織における情報漏洩リスクやその対策には，リスクの連鎖や複数リスクに効果を発揮する対策の存在など，複雑な関係性がある．またサイバー空間と物理空間でも対応が異なるため，リスクを正確に把握することや最適な防御対策が立てられずに経験的に行われていることが課題となっている．またサイバー空間と物理空間で対応部署が異なるために，それぞれの対策が独立してしまっている側面がある．

加藤らの研究[2]では，複雑なリスク連鎖の関係を体系的に分析する手法が提案されている．しかし先の研究ではサイバー空間に限定して分析を行っており，物理空間については分析が行われていない．

本研究では，サイバー空間と物理空間の２つの空間において分析を行い，状態遷移図で表現することにより複雑なリスク連鎖を表現し，最も脆弱でリスク値の大きい経路をクリティカルパスと定義を行う．その上で，クリティカルパスに対策を施すことで，各経路のリスク値を均等化するため，防御の最適化を防御コストを抑えながら達成できる点について考察を行った．

まず 2 章で既存手法とその問題点を述べる．3 章では分析を行う上での前提条件を定義し，モデル化を行う．4 章では前提条件に基づきリスク分析を行う．5 章で評価・考察を行う．最後に 6 章で今後の課題を述べ，7 章にてまとめを行う．

1 法政大学大学院応用情報工学研究科
Graduate School of information engineering, Hosei University
2 千葉工業大学
Chiba Institute of Technology
3 NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories

Vol.2020-CSEC-91 No.6
Vol.2020-SPT-40 No.6
Vol.2020-EIP-90 No.6
2020/11/25

2. 既存研究とその問題点

2.1. 木構造分析によるリスク分析

一般的なセキュリティリスク分析手法として挙げられるのが FTA(Fault Tree Analysis)である．リスク発生確率を算出するための FTA は頂上事象に発生確率が好ましくないリスクを置き，対策実施の有無によってリスクが発生する確率が変化すると捉え，対策を基本事象とする．またアタックツリー分析では脅威となる攻撃を引き起こす他の攻撃や操作を分析し可視化するために利用されている．これにより構造的に可視化されるため，特定の攻撃が具体的にどのような条件を満たすと可能となるか確認を行うことが可能である．

しかし上記の分析手法は，分析の対象や条件による FTA 図が肥大化することが課題である．さらに，ある FT の一部が別の FT に含まれる FT 重複の問題がある[1]．FT 重複の問題は分析の労力や対策決定のための計算量の点で問題となる．

2.2. イベントツリーとディフェンスツリーを併用したリスク分析における共通事象を考慮したリスク計算法

EDC(Event tree and Defense tree Combined method)手法では，イベントツリーとディフェンスツリー分析を併用して職種や規模，脅威となる攻撃を定めて分析を行い，分析結果と制約条件から最適な対策を算出することができる．相原ら[5]の研究では，1 つの攻撃が複数事象に影響を与える共通事象問題を考慮した提案を行っている．しかし木構造による分析であるため，分岐が膨大になる問題は解決できていない．

2.3. 状態遷移リスクモデル

加藤ら[1]の研究では，リスクが顕在化する流れやサービス利用の流れを状態遷移図で表現し，対策と合わせてネットワークモデルへ配置することで，リスク，利便性，対策の関係を視覚的に把握することができるモデルを提案した．しかし，物理環境については扱っていない．

3. サイバーフィジカル空間のモデル化，制約条件

本章では，リスク分析を行う上の対象や条件を明確にする．

3.1 ネットワーク環境のモデル化，制約条件

まずネットワーク環境についてモデル化と条件定義を行う．一般的に，組織や企業のネットワークは DMZ，イントラネットなどの領域に分けられるとする．また Web サーバ，メールサーバ，ファイルサーバを運用していると想定する．部署ごとにイントラネットを分けられることも考えられるが，本論文では簡単のため行わない．分析を行うネットワーク構成について図 1 について示す．

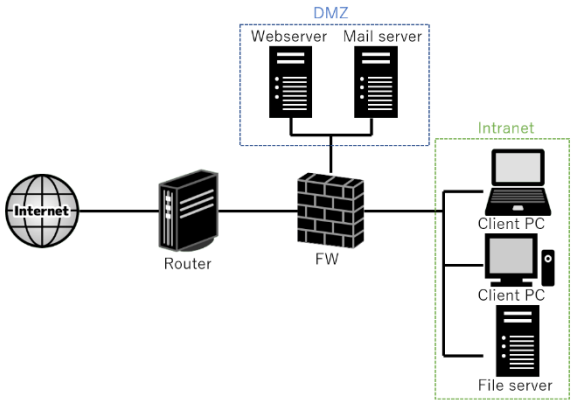

図 1 想定するネットワーク構成

3.2 物理環境のモデル化

次に物理環境についてモデル化と条件定義を行う．一般的に企業において，①企業内部，②一般社員エリア，③重要室が存在すると仮定する．また重要室には個人情報等の情報資産を保有すると仮定する．また，②の一般社員エリアでは覗き見や聞き耳などの脅威が存在すると想定する．①の企業内部への侵入には受付が必要であると仮定する．図２に示すように，脅威に対して物理的侵入によって試みられる脅威に対して，重要室に設置された個人情報漏洩の脅威レベルは相対的に①>②>③となると考えられる．

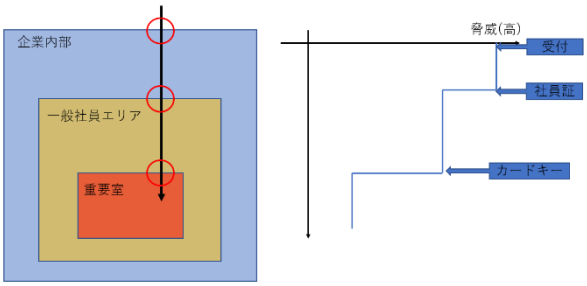

図 2 想定する物理環境モデル

4. リスク分析

本章では，３章で示した制約条件を元に防御分析を行う．

4.1 FTA 分析

本研究では，最初に全体の事象を把握するために，FTA を表 1 の全要因に対して行った．まず，組織の保有する情報資産についての FTA 分析を行う．しかし，FTA 分析を網羅的に行うことは容易ではない．そのため，米田ら[6]の RBS 手法に基づく場のセキュリティにおけるリスク要因抽出結果を参考に，情報漏洩に関する項目を抽出することでこれを解決した．例えば，「放火」などは例え社屋が全焼しても情報が流出するということはない．また，「DoS 攻撃」についても Web サービスが停止することがあっても情報

Vol.2020-CSEC-91 No.6
Vol.2020-SPT-40 No.6
Vol.2020-EIP-90 No.6
2020/11/25

が流出するということが考えにくい. 以下に示す表 1 では，物理セキュリティと情報，ネットワークセキュリティに関するリスク要因をまとめている.

表 1　RBS 手法に基づく情報漏洩に関するリスク要因

分類	リスク要因
1.物理セキュリティ	1.侵入
	2.盗難
	3.聞き出し
	4.覗き見
	5.聞き耳
	6.紛失
	7.内部犯行
	8.書置き
2.情報セキュリティ	2.1 ウイルス感染
	2.2 不正アクセス
	2.3 なりすまし
	2.4 フィッシング
	2.5 誤操作

次に，作成した表を元に，分析した FT 図の一部を図 3 に示す.

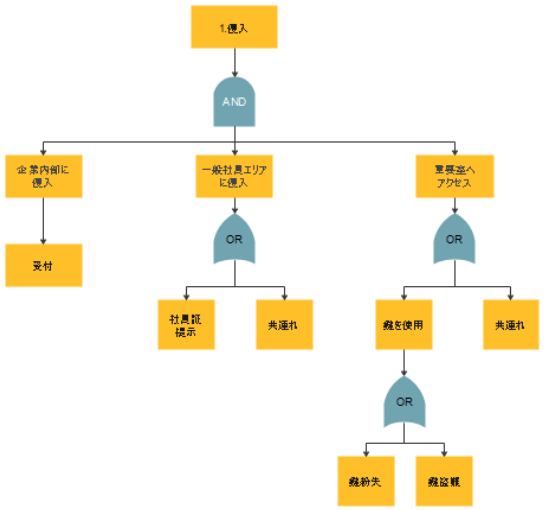

図 3 侵入のフォルトツリーの一部

AND 端子で結んでいる事象「企業内部に侵入」,「一般社員エリアに侵入」,「重要室にアクセス」すべてが達成されたとき，「侵入」事象が発生する．また「一般社員エリア」事象下にて OR 端子で結んでいる「社員証提示」事象や「共連れ」事象は片方が起こった時に「一般社員エリアに侵入」事象が達成されることを意味している．そして「侵入」事象は「情報漏洩」事象下にて OR 端子で結ばれており，表 1 の事象のいずれかが起こった時に情報漏洩が発生すると仮定する.

次に，不正アクセスのフォルトツリーを図 4 に示す．図 4 では，物理空間で起こる事象をオレンジ色で表現し，ネットワーク空間で起こる事象を青色で表現している．以降この表現は統一する．図 4 を参照すると，物理空間とネットワーク空間が入り混じった状態であることが分かる．また，同じ FT 事象が現れており，図 3 で用いた「侵入事象」が図 4 にも現れていることが分かる．この冗長性によって FT 図は膨大になってしまう.

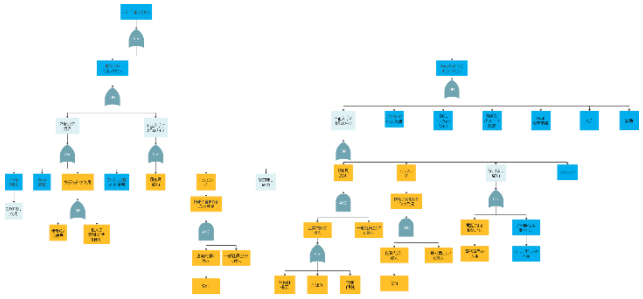

図 4　不正アクセスのフォルトツリーの一部

4.2 状態遷移図リスクモデル作成

4.1 節で作成した FTA 分析に基づき，それぞれの FTA シナリオを対応させるように状態遷移図シナリオを作成する.

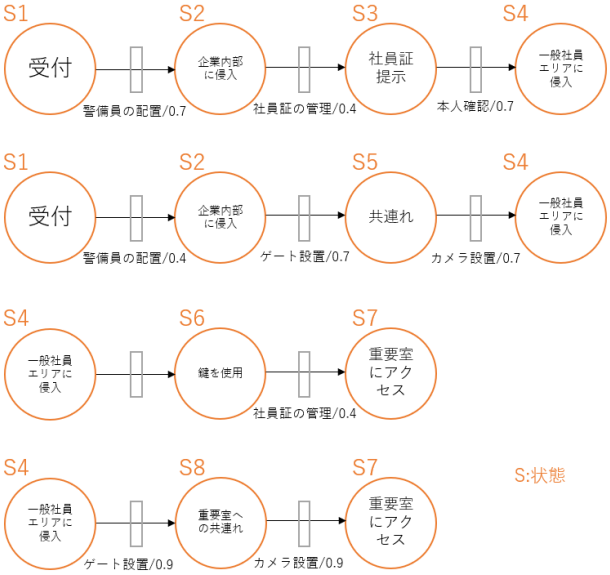

図 5 状態遷移によるリスク表記

Vol.2020-CSEC-91 No.6
Vol.2020-SPT-40 No.6
Vol.2020-EIP-90 No.6
2020/11/25

図 5 は，表 1 の「侵入」事象シナリオを状態遷移図によって表記したものである．各事象を状態として表記し，遷移時に対策を記載することで次の状態に遷移する確率を表現することができる．また，図 5 では S1 の「受付」状態や S4 の「一般社員エリアに侵入」, S7 の「重要室にアクセス」事象が複数回使用されていることが確認できる．

4.3 状態遷移図の結合

次に 4.2 節で示したような複数回現れる事象を重ね合わせて結合する．この際，状態遷移モデルと FT は対応関係があるため, FT 図下位原因事象が頂上事象に向かって遷移するように，状態遷移の向きに注意する．先ほど作成した状態遷移図を元に結合を行う．結合時に注意しなければならないのが，個々の状態遷移が前後の状態と無関係， そ

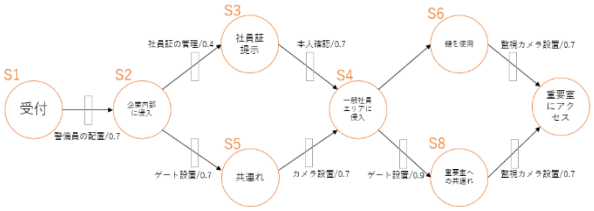

図 6　状態遷移図の結合の一部

の状態に遷移した原因やその後に続く遷移を検討せずに対策を割り当てるために，状態を細分化して定義することが望ましいということである．

しかし，すべての状態遷移が独立となるように分析を行うことは容易ではない．そのため，個々のリスクの分析と結合による不整合の確認を繰り返す中で，妥当なリスク分

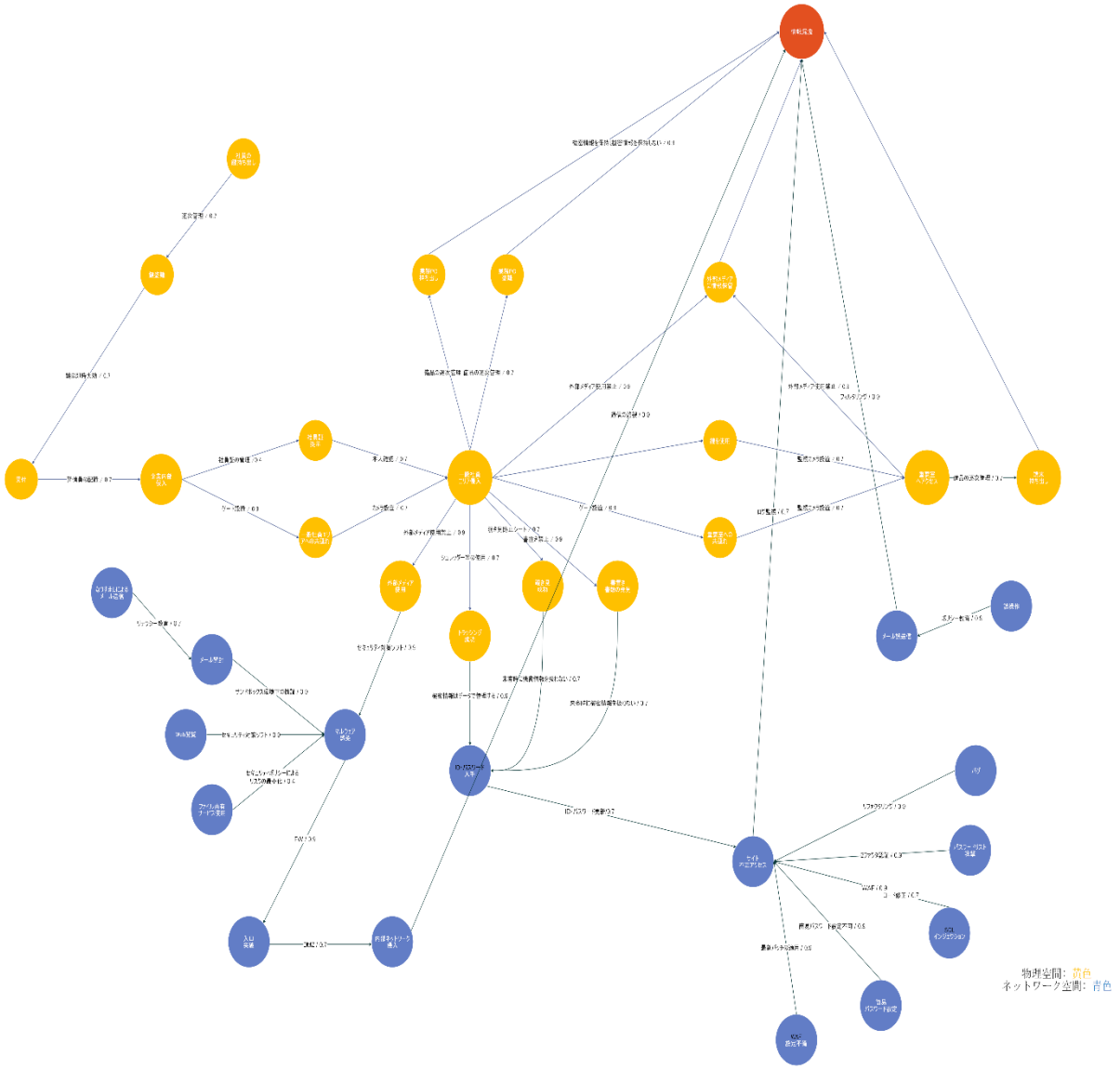

図 7 サイバーフィジカル空間における情報漏洩リスク分析状態遷移図モデル

Vol.2020-CSEC-91 No.6
Vol.2020-SPT-40 No.6
Vol.2020-EIP-90 No.6
2020/11/25

結果を得る必要がある．

4.1 節 FTA 解析，4.2 節状態遷移図リスクモデル作成，4.3 節状態遷移図の結合の手順により，図 7 のようなサイバーフィジカル空間の情報漏洩リスクモデルが作成された．なお，図が煩雑になるため，状態名や対策名は簡易表記としている．また，対策の低減確率を 0，0.4，0.7，0.9 と設定しているが，これは暫定的に設定している．そして頂上事象である「情報漏洩」事象を赤で表現している．また，モデルに設定した対策を表 4 に示す．表 4 の対策はより優れた対策に置き換えることが可能である．そのため対策者は表を確認し，常に時代に合った最新の対策を適用することが望ましい．

5. 評価

4 章で作成したモデルを元に，リスク値を算出する．

5.1 事故発生確率，リスク値の算出

図 7 のように作成されたモデルから，情報漏洩リスクを算出する．まず，始点と終点の２つの状態を選択する．次に，始点から終点へたどり着くパスを抽出する．これには式(1)を用いて，パス n のリスクP_nを算出する．ここで，パス n に含まれるイベント e とその集合E_n，イベント e の遷移確率や対策による低減確率P_e，対策の実施の有無$x_i \in E\{0,1\}$，対策 i を実施した時のイベント e に対するリスク低減効果を$\Delta P_{e,i}$とする．

$$P_n = \prod_{e \epsilon E_n} P_e \prod_i \left(1 - \Delta P_{e,i} x_i\right) \dots (1)$$

そして，始点から終点にたどり着く総合的なリスク値P_{total}は，すべてのパスのうち少なくとも 1 つのパスが成立する確率となるため，式(2)により表される．P_{total}の取りうる範囲は 0~1 である．

$$P_{total} = 1 - \prod_{n \in N} (1 - P_n) \dots (2)$$

式(1)，(2)より求まったリスク値を表 2，表 3 に示す．

表 2 情報漏洩リスク値

情報流出パス	最大リスク	最小リスク
業務 PC 持ち出し	0.00162	0.00027
業務 PC 盗難	0.00162	0.00027
重要端末持ち出し	0.000486	0.000243
外部メディアによる外部持ち出し	0.0054	0.0027
内部 NW 侵入	0.0012	0.000009
サイト不正アクセス	0.07	0.009

表 3 総合リスク

最大総合リスク	0.0796
最小総合リスク	0.0125

表 4　モデル設定対策案

状態名	対策	低減効果
受付	—	0
企業内部侵入	警備員の配置	0.7
社員証提示	社員証の管理	0.4
一般社員エリアへの共連れ	ゲート設置	0.9
一般社員エリアへの侵入	本人確認 / 監視カメラ設置	0.7 / 0.7
外部メディアに情報保管	外部メディア使用禁止	0.9
鍵を使用	—	0
重要室への共連れ	ゲート設置	0.9
重要室へアクセス	監視カメラ設置	0.7
端末持ち出し	備品の逐次管理	0.7
業務 PC 持ち出し	備品の逐次管理	0.7
業務 PC 盗難	備品の逐次管理	0.7
社員の鍵持ち出し	—	0
鍵盗難	備品の逐次管理	0.7
なりすましによるメール送信	—	0
メール開封	サンドボックス環境下の検証	0.9
Web 閲覧	—	0
ファイル共有サービス使用	セキュリティポリシーによるリスク最小化	0.9
マルウェア感染	セキュリティ対策ソフト	0.9
ID・パスワード入手	ID・パスワードの更新	0.9
入口突破	FW アクセス制御	0.9
内部 NW 侵入	FW アクセス制御	0.9
サイト不正アクセス	FW アクセス制御	0.9
WAF 設定不備	最新パッチの適用	0.9
簡易パスワード設定	簡易パスワード禁止	0.91
SQL インジェクション	WAF 設定 / コード修正	0.9 / 0.7
パスワードリスト攻撃	2 段階認証追加	0.9
トラッシング成功	シュレッダー等の使用	0.7
覗き見成功	覗き見防止シートの活用	0.7

Vol.2020-CSEC-91 No.6
Vol.2020-SPT-40 No.6
Vol.2020-EIP-90 No.6
2020/11/25

5.2 クリティカルパスの算出

一般的に「クリティカルパス」はプロジェクト上最長の経路を表す．しかし本研究では，最大リスクパスをクリティカルパスと定義することとする．表 2 より,「サイト不正アクセス」による情報漏洩パスが 0.07 と最もリスク値が高いことが分かる．つまり「サイト不正アクセス」情報漏洩パスがクリティカルパスである．総合リスクもこれに比例してしまっている．つまりこの経路における対策を行うことで，総合リスクを下げることが可能となる．図 7 を確認すると,情報漏洩に至るまでの状態が少ないことが分かる．そのため状態を増やすことで，状態遷移時に対策を設定する機会を増やすことができるため，多層防御の概念に基づき情報漏洩リスクを下げることが可能である．

6. 今後の検討

6.1 ペリメータラインの設定

分析モデルに物理面の非サイバー空間の要素を加え，セキュリティ防御ライン(ペリメータライン)を効率良く連動させる多層防御の考えを取り入れてモデルを配置することで安心安全な IT ガバナンスに寄与することが出来ないか検討を行う．

6.2 疲労度を考慮した対策設定

本研究では，リスク値のみ着目して分析を行ったが，利用するユーザの疲労度や可用性も考慮した対策を行うことが業務効率化の観点でも望ましい．そのため対策の低減確率だけでなく，ユーザの疲労度調査に基づいた疲労度も合わせて定量的な分析を行うことで可用性も考慮した対策を選択できないか検討を行う．

6.3 最適な対策値設定

本研究では，表 4 の通り暫定的に対策の低減確率を定めている．今後の研究では，状態遷移モデルをベイジアンネットワークとして扱い，ベイズ更新を行うことで低減確率を常に最適な対策値に定めることができないか検討を行う．

7. おわりに

本研究では，サイバー空間と物理空間を統合し，これらのリスク連鎖を状態遷移図で表現し，さらにリスク対策を実施した結果を可視化するモデルおよびその分析手法を提案し，リスク値を算出した．これにより現実に発生するリスクの状況変化への対応が可能であることを示し，クリティカルパスの概念に基づいて最適な防御が行うことが可能であることが確認できた．

参考文献

[1] IPA：情報セキュリティ 10 大脅威 2020，IPA（オンライン），入手先〈https://www.ipa.go.jp/security/vuln/10threats2020.html〉（参照 2020-10-29）．
[2] 加藤 弘一，勅使河原可海：事象連鎖と原因推測が可能なリスク・利便性・対策表示モデルの提案．情報処理学会論文誌．Vol50，No.9，pp.2243~2256（2009）．
[3] 加藤 弘一，勅使河原可海：利便性とセキュリティの動的移行によるユーザ要求の自動交渉方式の検討．情報処理学会研究報告コンピュータセキュリティ（CSEC），Vol.16，No.16（2007-CSEC-036），pp.219-224（2007）．
[4] IPA：制御システムのセキュリティ分析ガイド 第 2 版，IPA（オンライン），入手先〈https://www.ipa.go.jp/files/000080712.pdf〉（参照 2020-10-29）．
[5] 相原遼，佐々木良一：イベントツリーとディフェンスツリーを併用したリスク分析における共通事象を考慮したリスク計算法の提案．マルチメディア，分散，協調とモバイル(DICOMO2016)シンポジウム，Vol.2016，No.1，pp.1062-1067（2016）．
[6] 米田翔一，谷本茂明，佐藤周行，金井敦：オフィス空間における場のセキュリティを考慮したリスクアセスメント，情報科学技術フォーラム講演論文集 （FIT），Vol.13，No.4，pp.55-58（2014）．