多重リスクコミュニケータ MRC シリーズの 2025 年段階での開発状況と今後の展開

佐々木 良一 [1,*]　寺田 眞敏 [1,†]

概要：著者らは，IT リスク学の中核として長年にわたり開発を進めてきた多重リスクコミュニケータ（MRC）群を，2024 年に「MRC シリーズ」として体系化し，構成要素と相互関係を明確化した．基本となる手法「Basic-MRC」は，コストや使い勝手を制約条件とし，アタックツリーを用いて求めた残存リスクを最小化する対策案の組み合わせ求めることを繰り返しつつ関与者の合意形成を図るものである．さらに，多くの関与者の合意形成を支援するための「Social-MRC」や，多段にわたる攻撃に対応するためにイベントツリーとディフェンスツリー分析を融合したリスクアセスメント手法「MRC-EDC」など合計 9 つの手法に整理した．2025 年には，動的変化に対応するリスクコミュニケーション手法「MRC-Dynamics」を開発し，能動的サイバー防御政策への適用を試行したほか，社会共同体における施策決定議論を支援する AI システム「AI 応用 Social-MRC」も開発した．本稿では，これらの成果を整理するとともに今後の MRC シリーズの展開計画について述べる．

キーワード：IT リスク学，多重リスクコミュニケータ，リスクアセスメント，リスクコミュニケーション

Development Status and Future Prospects of the Multiple Risk Communicator MRC Series as of 2025

Ryoichi Sasaki[1,*]　Masato Terada[1,†]

Abstract: The authors have long pursued the development of the Multi-Risk Communicator (MRC) as the central system in IT risk studies. In 2024, we organized various models under the "MRC Series," clarifying its structural components and interrelationships. The basic method, "Basic-MRC," seeks to build consensus among participants while seeking combinations of countermeasures that minimize the residual risk calculated using attack trees, with cost and ease of use as constraints. In addition, the autors organized them into a total of nine methods, including "Social-MRC" to support consensus building among many involved parties and "MRC-EDC," a risk assessment method that combines event tree and defense tree analysis to deal with multistage attacks. In 2025, the authors developed a dynamic risk communication method, "MRC-Dynamics," which was applied to active cyber defense policy, and implemented an AI-supported decision-making system, "AI-Enhanced Social-MRC," to assist in policy discussions within social communities. This paper summarizes these results and describes future development plans for the MRC series.

Keywords: IT risk studies, multiple risk communicator, risk assessment, risk communication

1. はじめに

文献［1］にも記載したように，社会全体の IT システムへの依存の増大により，IT システムの重要性が増大してきている．これに伴い，IT システムの安全性は従来よりも広い統一的アプローチが必要になっていると考えられる．

すなわち，IT システムの安全性には次の 3 つが考えられる．

① IT システムが行うサービスの安全
② IT システムの扱う情報の安全
③ IT システムそのものの安全

従来のセキュリティはこのうち，②を中心に扱うものであった．今後は，①②③を統一的に扱うべきであると考えこれを「IT リスク学」[2][3]と名付け 2006 年頃より研究を開始し，下記のように研究を実施していった．

① 2008 年 5 月に日本セキュリティ・マネジメント学会の中に「ＩＴリスク学」研究会を立ち上げ
② IT リスク学の定義を決定
③ IT リスク学の全体像と構成要素を明確化
④ 構成要素の概要と研究課題の明確化
⑤ 研究課題の解決に向けての活動
⑥ 本「IT リスク学」の出版（2013 年 1 月）[3]
⑦ 活動の継続

1 東京電機大学
Tokyo Denki University
* r.sasaki@mail.dendai.ac.jp
† masato.terada@mail.dendai.ac.jp

ここで，IT リスク学の定義は，「不正によるものだけでなく，天災や故障ならびにヒューマンエラーによって生ずる IT システムのリスクならびに IT システムが扱う情報やサービスに関連して発生するリスクを，リスク対策の不確実性や，リスク対リスクの対立，関与者間の対立などを考慮しつつ学際的に対処していくための手段に関する学問」とした．また，IT リスク学の全体像と構成要素は，図 1 に示すように設定した．この図に示すように IT リスク学の中心となるのは，IT リスクマネジメント技術であり，特にその中で中心となるのが多重リスクコミュニケータ MRC（Multiple Risk Communicator）である．

従来，種々の MRC を個別に開発し，体系化なども行わないできた．しかし，それでは，目的に応じて使い分けたり，開発すべきものを明確にできたりせず，まずいと考えた．そして，2024 年に体系化を図り，MRC 群として開発した種々のシステムの位置づけを明確にし，名称の見直しを行い，シリーズ化して紹介した［1］．

本稿では 2025 年に開発したものを追加して位置づけるとともに，今後の開発計画を展望する．

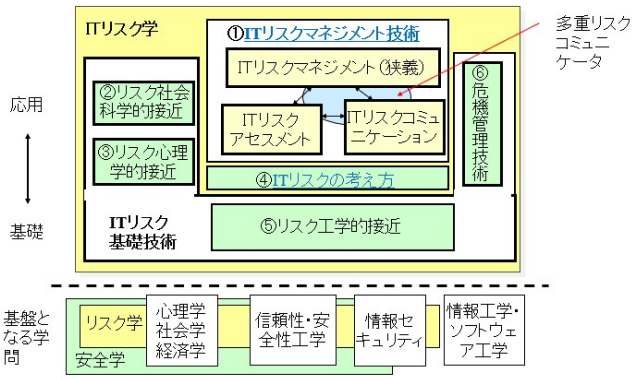

図１　ＩＴリスク学の構成
Figure 1 Structure of IT Risk Studies

2. 既開発の MRC シリーズ

2.1 MRC シリーズの全体像

多重リスクコミュニケータシリーズ MRC の全体像は，図２に示すとおりである．このうち最初に開発し，基本となるのが Basic-MRC であり，従来 MRC と呼んでいたものである．また，リスクコミュニケーションを充実するために，1000 人以上の多人数の関与者がいる場合にも対応を可能としたものが Social-MRC である．そして，リスクアセスメントの充実のために，多段にわたるサイバー攻撃に適用できるようイベントツリーとディフェンスツリーを組み合わせて用いるよう改良したものが，MRC-EDC 法(Event Tree and Defense Tree Combined Method)である．その他いろいろな目的で改良した既開発の方式が 6 種類あり，以下，それぞれについて説明を追加する．

図２　多重リスクコミュニケータシリーズの全体像
Figure 2 Overall view of the Multiple Risk Communicator Series

2.2 基本となる MRC である Basic- MRC の概要

文献［1］にも記述したように基本となる多重リスクコミュニケータである Basic-MRC は，図 3 に示すように，関与者の合意を取りながら個人情報漏洩対策などの最適な対策の組み合わせを求めるものである[4][5]．この Basic-MRC を開発した背景は以下のとおりである．

背景１．多くのリスク（セキュリティリスク，プライバシーリスク，使い勝手など）が存在する．したがってリスク間の対立を回避する手段が必要である．

背景２．ひとつの対策だけでは目的の達成が困難である．したがって，対策の最適な組み合わせを求めるシステムが必要である．

背景３．多くの関与者（経営者・顧客・従業員など）が存在する．したがって，多くの関与者間の合意が得られるコミュニケーション手段が必要である．

背景１と２に対応するため，コストや使い勝手などを制約条件とし残存リスクなどを最小化する組み合わせ最適化問題として定式化する．背景３に対応するため，対策案の組み合わせに関する関与者の合意が得られるまでパラメータの値や制約条件値を変えつつ最適化エンジンを用いて求解する．

例えば，対策案がｎ個あり，図 3 に示すように定式化されているとする．Basic-MRC を用いることにより最初に，対策案①と③の組み合わせが良いということになったとしても，リスクコミュニケーションによって関与者から例えば対策コストを３０％増加してもよいではないかという意見が出たらその条件下で最適に組み合わせを求める．また，対策案③は使い勝手に問題があるのでこの対策を外した場合の最適な対策案の組み合わせを知りたいという声があれば，その解を求める．そして対策案の組み合わせに関する関与者間の合意が成立するまでこの過程を繰り返す．

図 4 に個人情報漏洩問題を対象とした定式化結果の一例を示す[4]．ここでは利便性負担度を金額で表すようにしているが，何段階に分けて準定量的に表すことも可能である．また，情報漏洩確率などは，アタックツリーをベースに 0－1 変数 Xi を導入することにより対策の採用不採用を同時

に表すことのできるようにしている．

本手法は，地方自治体からの個人情報漏洩問題[4][5]，内部統制問題[6]などに適用し，関与者の数が 5-6 人以内なら適用可能であるということを確認している．

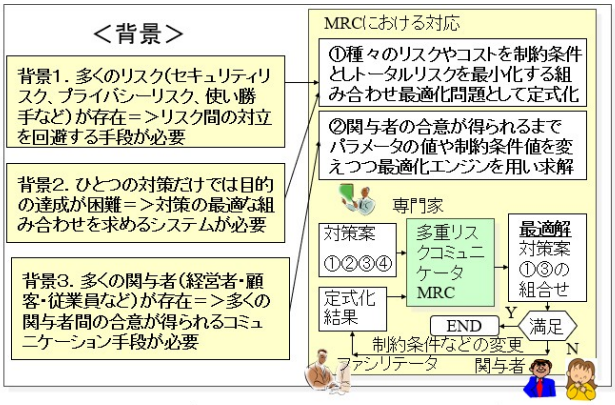

図３基本となる多重リスクコミュニケータの概要
Figure 3　Overview of the Basic Multiple Risk Communicator

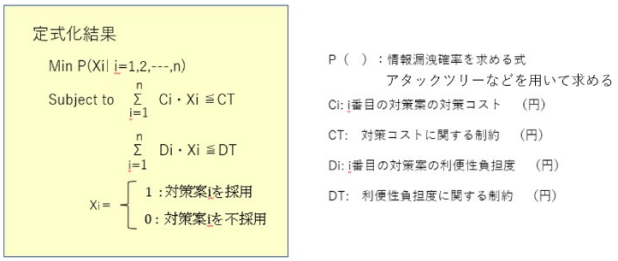

図４定式化の一例
Figure 4 Example of Formulation

2.3　Social-MRC の概要

文献［1］にも記述したように，社会的合意を形成するためには，より多くの人が合意形成に参加できるようにするとともに，できるだけその人たちの意見が反映できるようにすることが必要である．したがって，数千人以上が直接 Basic-MRC を使えるようにすることが望ましいが，非常に困難である．そこでここでは，現実の政治と同様に間接民主主義的な方法をとることとした．すなわち，対象とする問題に関し，オピニオンリーダに意見を戦わせてもらい，それを見て一般関与者が意見を言ったり，誰を支持するかを言ってもらったりしようというものである．このようにすることによって，次のような長所が生じる．

（１）一般関与者の意見の動向をリアルタイムに知ることにより，それぞれのオピニオンリーダが自分の意見に固執していつまでたっても合意が形成できないという問題を回避しやすくなる．

（２）一般関与者の中のすぐれた意見を意思決定に反映し，もともとの各オピニオンリーダの意見による解よりもよいものが得られやすくなる．

上記の目的を達成するため，オピニオンリーダ間のコミュニケーションと一般関与者参加型のコミュニケーションの２階層のリスクコミュニケーションを統合的に支援する Social-MRC システムを開発した[7]-[9]．

この概要は図 6 に示すとおりである．

（１）オピニオンリーダ間のコミュニケーション支援および一般関与者との間のコミュニケーション支援の２階層アプローチをとる．

（２）オピニオンリーダ間の合意形成に多重リスクコミュニケータ関連技術を使用する．

（３）オピニオンリーダと一般関与者間のコミュニケーション支援に，（ａ）USTREAM などのインターネット利用画像配信システム，（ｂ）Twitter などのインターネット利用意見収集システム，（ｃ）対策案最適組合せ演算機能などを利用する．

（４）Twitter などの短いコンテンツのから，有効な意見を（半）自動的に抽出できるようにするために機械学習を導入する[10][11]．

このシステムを開発し，図 6 に示すように「青少年に対する情報フィルタリング」に適用し，その有効性を認識することができた[7]-[11]．

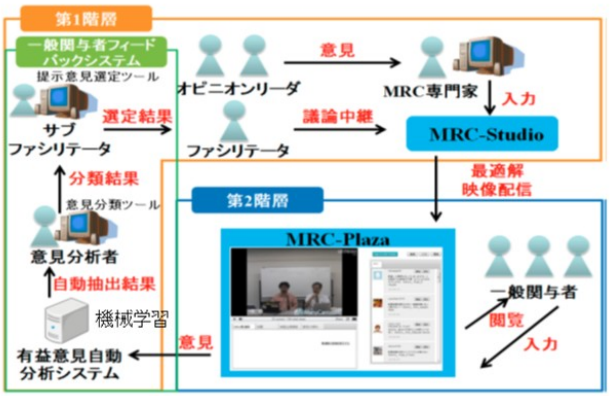

図5　Social-MRCの概要
Figure 5 Overview of Social-MRC

図6　Social-MRCの出力画面の一例
Figure 6 Example of Social-MRC output screen

2.4　多段の攻撃に対応可能な MRC-EDC の概要

MRC-EDC 法とは，多段にわたる複雑な攻撃に対応できるようにするため，Basic-MRC で用いていたアタックツリー分析の代わりにイベントツリー分析（図 7 参照）とディフェンスツリー 分析（図 8 参照）を併用したリスク分析法

をベースに，対策案の最適な組合せを求める方法であり，従来EDC法(Event Tree and Deffense Tree Combined Method)と呼んでいたものである． MRC-EDC 法について詳しくは文献［1］[12]-[14]などを参照願いたい．

この方法は，複雑なサイバー攻撃のリスク分析にも適用可能であり，大学の次期ネットワークシステム向けセキュリティ対策[12]や，自治体のセキュリティ対策の検討[13]-[16]のために広く用いられてきた．

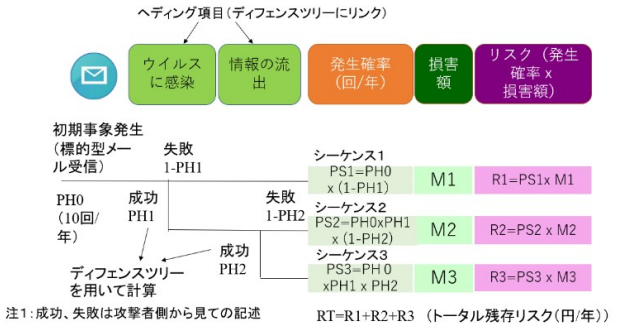

図7　説明用イベントツリー分析
Figure 7 Explanatory Event Tree Analysis

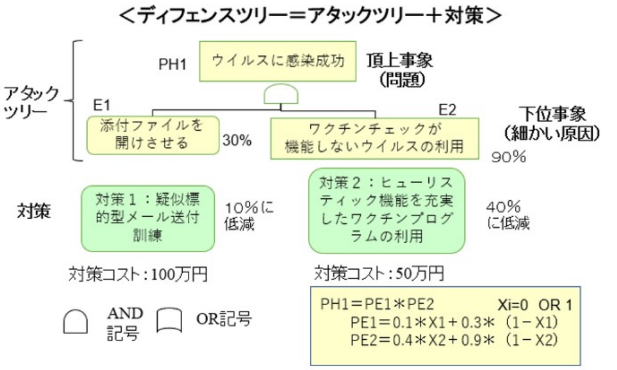

図8　説明用ディフェンスツリー
Figure 8 Defense Tree for Explanation

2.5 その他の MRC シリーズ

2.5.1 パラメータ値の不確実性へ対応する MRC-CCP 法

Basic-MRC 法や Social-MRC 法, MRC-EDC 法で発生確率やコストなどのパラメータの値に不確実性があり，一点ではなく分布として与えたい場合に関する方式（MRC-CCP 法と名付ける）の開発も実施している[17]．これは発生確率やコストが指定の制約を守れる確率を目標値以上にするよう Chance Constrained Programing 問題として定式化し，高速で求解する方法である．詳しくは文献[17]を参照願いたい．

2.5.2 インシデント発生対策と回復対策の両方の対策案の組み合わせを求めることのできる MRC-DRP 法

MRC-EDC 法などでは，インシデントの発生確率を減少するための種々の対策は検討してきたが，修復時間を短縮するための対策は検討してこなかった．ここでは，MRC-EDC 法をベースとし，インシデントの発生確率を減少するための種々の対策だけでなく，修復時間を短縮するための種々の対策を導入する．そして対策の組み合わせによって実現できる回復時間を, PERT(Program Evaluation and Review Technique)を用いて計算できるようにしたものである[18]．これにより，システムダウンを低減する対策と復旧を早める対策の両方が同時に扱えるようになり，より現実的な分析が可能となった. この方式を MRC-DRP（Disaster Recovery Plan）法と名付ける．

2.5.3 対策としてリモートメンテナンスを伴うシステムのためのリスク分析 MRC-RM 法

IoT(Internet of Things)や CPS(Cyber Physical System)の普及により，様々な機器がネットワークと接続されるようになってきている．これにより，リモートメンテナンスを伴うシステムが増加してきている．平均修復時間を小さくするというメリットがある一方, それを利用した攻撃により，平均故障間隔が小さくなるというディメリットもある．そこでリモートメンテナンスを考慮したリスク分析を可能とする MRC を開発し今回 MRC-RM と名付けた．併せてこれを敷布型マルチバイタル IoT モニタに適用し，その有効性を確認した[19][20].

2.5.4 対策効果にフィーバックのあるシステムへの対応が可能な MRC-SS 法

IoT(Internet of Things)の普及により, 対策効果にフィードバックを伴い，またその影響が人命や環境に危険をもたらすものがある．したがって，これらのシステムでは，従来別の領域で扱われてきたセキュリティ上のリスクとセーフティ上のリスクを統合的に分析する必要がある．しかし，従来のリスク分析手法では統合的な分析が困難であると同時に，フィードバックを含む複雑なシステムを分析するのに不適切である．

そこで, 本稿では STPA(System-Theoretic Process Analysis)と呼ばれる安全解析手法をベースにセキュリティとセーフティの両方に対応可能なリスク分析手法を提案するとともにリスクに対して費用対効果の高い対策を選定する手法も提案し，今回 MRC-SS（Safety and Security）法と名付けることにした[21]-[23]．また，適用例として，糖尿病向け医療機器であるインスリンポンプに対して分析を行った結果を示している．

2.5.5 Attack by AI 向け準定量化 MRC-EDC 法

生成 AI の誕生が AI とセキュリティの関係にどのような影響を及ぼすかを検討した結果, Attack by AI への影響が大きく,しかも世の中の検討が進んでいないため研究の必要性が高いことを明確にした[24]．一方，対策案の最適な組

み合わせを求めるためには，MRC-EDC 法は一般的には望ましい方法であるが，本対象のように対策コストやリスク低減効果の厳密な推定が非常に困難なものには向かないと判断した．そしてコストや効果を準定量化するアプローチを含む準定量化 MRC-EDC 法を開発し,Attack by AI 問題に試適用した [25].その結果，図 9 に示すようにコスト・効果の良い 5 つの対策を示すとともに方式が適用可能であることを確認することができた．

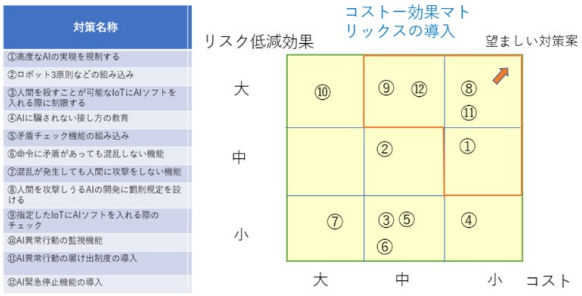

図9　Attack by AIへの準定量MRC-EDC法の適用結果
Figure 9　Results of applying the quasi-quantitative MRC-EDC method to Attack by AI

2.5.6　メタバース向けモデリング法 MRC-SVR 法

近年，ゲームやビジネスにおいて利用が増加しつつあるメタバースには種々のメリットがある反面，セキュリティ問題などのリスクも憂慮されており，メタバースに関する適切なリスクアセスメントが必要とされている．メタバース利用ゲームに対するリスクアセスメントについては MRC-EDC 法などを適用することでリスクアセスメントが可能であることが確認できた[26].

しかしより高い安全性が要求されるメタバースビジネスアプリケーションにこの方法を適用した場合，リスク要因抽出の網羅性･効率性の面で問題があることが分かった．そこで従来どおりシステムの構成図に対する処理やデータの流れを可視化するだけでなく，バーチャル空間の状態および現実世界の周辺環境を図として可視化し，それぞれに対し並行してリスク要因をプロットする SVR (**S**ystem - **V**irtual - **R**eal) リスク要因抽出法と名付けた方式の開発を行った．そして，メタバース上で VR ヘッドセットを介して行う VR ショッピングを対象とし従来手法と提案手法を用いて第三者によるリスクアセスメント実験を実施した結果，VR 特有のリスク要因の抽出において SVR リスク要因抽出法(MRC-SVR 法と名付けた)が優位であることが確認できた[27][28].

3.　MRC-Dynamics の開発

海外からのサイバー攻撃の激化に伴い，攻撃を行っている相手国のサーバに対し，日本としてアクセスを行い相手国の攻撃を無効化する能動的サイバー防御を導入すべきであるという意見が高まっており法制化がすすめられてきた．一方,能動的サイバー防御の効果は少ないにもかかわらず，相手側の反発を招き，かえって日本の被害が増えるのではないかという見方もある．相手の対応の変化に伴うリスクの変化を動的に評価することで，どのようにすれば相手国の反発があっても能動的サイバー防御が望ましい対応になるのかを検証しておく必要がある．そのために，従来から著者らが開発してきた多重リスクコミュニケータ MRC シリーズを動的評価が実施できるように改良を行った[29].

具体的には示すように，従来の MRC シリーズの持つリスクコミュニケーション機能に System Dynamics の機能を追加した MRC-Dynamics を開発した（図 10 参照）．これを能動的サイバー防御対策に適用した結果，「①現状に比べ，能動的サイバー防御を導入した方が短期的には日本への攻撃成功数が小さくなるが数年で逆転する．②逆転までの期間を大きくするためにはインテリジェンスの強化と能動的サイバー防御の導入を組み合わせることが望ましい.」などを明らかにした．この結果 MRC-Dynamics は，対応を行うことにより相手側が動的に反応する対象のモデル化が容易であり，関与者の意見を反映して再シミュレーションを実施しやすく，今回のような対象への適用に適したものであることが明らかになった．

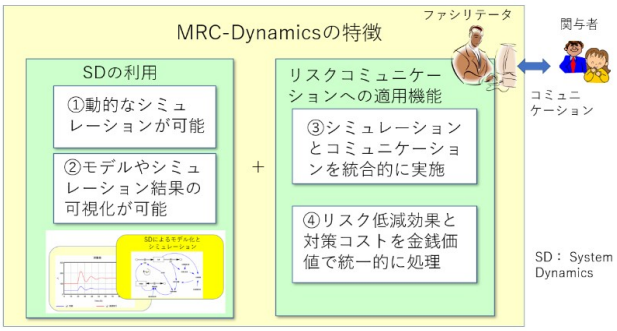

図10　システムダイナミックスとMRC-Dynamicsの関係
Figure 10 Relationship between System Dynamics and MRC-Dynamics

4.　AI 応用 Social-MRC の開発

Social-MRC[8]においては，AI を用いて有用な意見を抽出しオピニオンリーダたちに自動的に表示する機能を一部持たせていた[10]．しかしこの方法では，一般関与者の意見が多すぎるとオピニオンリーダが意見を十分把握できない問題や，逆に意見が少なすぎる場合に議論が深まらない問題があった．

そこで本研究では，図 11 に示すように生成 AI の 1 つである大規模言語モデル（LLM）を活用し，議論予測，意見抽出，意見補完機能を持つ議論支援 AI システム「AI 応用 Social-MRC」を開発した[30].

この開発において LLM を使用するにあたっては，意見の抽出や補足といった 複雑なタスクを一度の処理で行わせることは,思考の飛躍 や誤りを招くリスクがあると筆者らは考えた．そこで本研究では，これらを段階的に処理す

るため，まず「議論の予測」 をさせるという中間タスクを設定した． この段階的なアプローチは，近年の大規模言語モデル研究で提案されている Chain-of-Thought（CoT）プロンプティング[31]の考え方を参考にしている．

実験では，青少年のインターネット利用制限に関する議論に適用した結果，AI 応用 Social-MRC の有効性を確認することができた．

なお，文献[30]では「AI 応用 Social-MRC」のことを「新 Social-MRC」と呼んでいたが「AI 応用 Social-MRC」に名前を変更することにした．

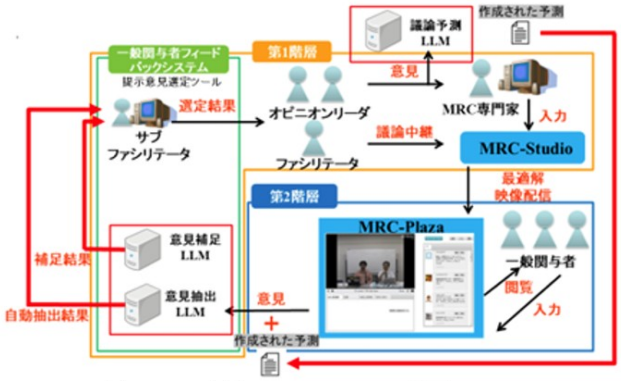

図11　AI応用Social-MRC の概要
Figure 11 Overview of AI-applied Social-MRC

5. 今後の展開計画

今後，MRC に関連し，次のようなことを実施することを計画中である．

（１）既開発手法の適用範囲の拡大

佐々木らが中心になり，対象ごとにいろいろな方法を開発し，適用してきたが，佐々木ら以外の適用数は限定的である．Baisc-MRC や Social-MRC，MRC-Dynamics などはほかの人でも適用可能であると考えられる．ドキュメントやツールを整備するとともに，日本セキュリティ・マネジメント学会ＩＴリスク学研究会などで，適用訓練をする機会を設けていきたい．

（２）新しい対象に関するＭＲＣシリーズの開発

今のままの手法では適用が困難な対象も多い．例えば，MRC-EDC 法などでは，Event Tree の各ヘッディング項目の発生を独立事象と仮定している．多くの場合これで問題ないが，ある各ヘッディング項目が別の各ヘッディング項目に対し従属性が高い場合もあり，このような場合には，独立を仮定すると計算精度が落ちる．このような対象に関する容易な計算手法を確立する必要があると考えている．

（３）MRC-Dynamics の核となる System Dynamics を用いた動的モデリングと，AI 応用 Social-MRC で実績のある LLM の活用を統合し，生成 AI を活用した新たな動的リスクコミュニケータを開発する．例えば，**①生成 AI の活用** MRC-Dynamics の基盤である System Dynamics モデルの構築および改善プロセスにおいて，生成 AI を導入し，モデル化の精度と効率を向上させる．②また，関与者がいうべきでありながら言ってないことを，生成 AI を用いて抽出できるようにする．

6. おわりに

著者らが長年にわたっての確立を図ってきた IT リスク学において，その中核をなすシステムが多重リスクコミュニケータ MRC であり，適切なセキュリティ対策の合意形成を支援するためのものである．MRC に関連して 2025 年時点での構成要素とその相互関連について紹介した．

MRC シリーズのようなものは今後ますます重要性を増すと考えており，今後の開発計画，普及計画についても紹介した．

参考文献

[1] 佐々木良一，「多重リスクコミュニケータ MRC シリーズの体系化と最近の展開」情報処理学会 CSS2024

[2] 佐々木良一，「IT リスクの考え方」岩波書店, 2008

[3] 佐々木良一監修「IT リスク学」共立出版, 2013

[4] 佐々木良一, 日高　悠, 守谷　隆史, 谷山　充洋, 矢島　敬士, 八重樫清美，川島　泰正，吉浦　裕「多重リスクコミュニケータの開発と適用」情報処理学会論文誌第 49 号第９号 pp3180-3190 2008

[5] Ryoichi Sasaki,” Consideration on Risk Communication for IT Systems and Development of Support Systems （Invited Paper）” Journal of Information Processing Vo.20（2012）-4, pp814-822

[6] Ryoichi Sasaki, “Trial Application of the Multiple Risk Communicator to Internal Control Problems” International Journal of Information Processing and Management(IJIPM) Volume4, Number6, pp40-49, September 2013

[7] Ryoichi Sasaki, Shoko Sugimoto, Hiroshi Yajima, Hidetaka Masuda, Hiroshi Yoshiura, Masaki Samejima,” Proposal for Social-MRC: Social Consensus Formation Support System Concerning IT Risk Countermeasures” International Journal of Information Processing and Management Vol.2,No.2 pp48-58　2011

[8] 佐々木良一，杉本尚子，矢島敬士，増田英孝，吉浦　裕，鮫島正樹，船橋誠壽「ＩＴリスク対策に関する社会的合意形成支援システムＳｏｃial-MRC の開発構想」情報処理学会論文誌 VOL.52,No.9，pp 2562-2574，2011

[9] 大河原優，高草木一成，矢島敬士，増田英孝，小林哲郎，佐々木良一「IT リスク対策に関する社会的合意形成支援システム Social-MRC の情報フィルタリング問題への試摘用と考察」日本セキュリティ・マネジメント学会誌 26 巻第 1 号 2012 年 5 月 pp3-14

[10] Hayaki Ando,Yuusuke Inose, Hidetaka Masuda, Ryoichi Sasaki,” Proposal and Evaluation of Method for Automatically Extracting Useful Opinions Relating to Risk Communication in Micro-blogs” International Journal of Information Processing and Management, Vol.5,No.2, May, 2014, pp1-13

[11] 安藤駿, 猪瀬裕介，増田英孝，佐々木良一「マイクロブログ中のリスクコミュニケーションに関する有益な意見を自動的に抽出する手法の提案と評価」情報処理学会論文誌, Vol.55,No.9,pp2149-2158　2014
[12] 相原遼，石井亮平，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標的型攻撃に対するリスク分析手法の提案と適用」情報処理学会論文誌 Vol. ５９，No.3，pp1082-1094 2018
[13] Ryoichi Sasaki, “Application of Risk Assessment Method to Local Government Security Models ” CFSE2021 in IEEE QRS2021
[14]佐々木良一,千葉寛之,甲斐賢,木下翔太郎「自治体セキュリティモデルのためのリスクアセスメント手法の提案と適用」情報処理学会誌, Vol63,No.3, pp899-907, 2022
[15] 竹原 直実,伊藤 吉也,佐々木 良一「地方公共団体のセキュリティ対策のための準定量的リスクアセスメントと EDC 手法による定量的リスクアセスメントの組み合わせの提案と適用」電子情報通信学会　SCIS2024
[16] 伊藤 吉也，加藤 孝史，竹原 直実，佐々木 良一，齊藤 泰一「教育情報システムに対する IPA 方式と EDC 方式によるリスク分析とそのセキュリティ対策」日本セキュリティ・マネジメント学会 2024 年度全国大会
[17] Masaki Samejima, Ryoichi Sasaki,” Chance-Constrained Programming Method of IT Risk Countermeasures for Social Consensus Making” IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, VOL. 45, NO. 5, MAY 2015 pp725-733 Vol.2,No.2 pp48-58 2011
[18] Ichiro Matsunaga, Ryoichi Sasaki “Development and Evaluation of a Continuity Operation Plan Support System for an Information Technology System” International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(2): 327-338, 2015 (ISSN: 2305-0012)
[19] Ryoichi Sasaki “A Risk Assessment Method for IoT Systems Using Maintainability, Safety, and Security Matrixes” ICISA2019 International Conference on Information Science and Applications 2019
[20] 佐々木良一「メンテナビリティ・セーフティ・セキュリティを考慮した IoT システム向けリスク評価手法の開発」情報処理学会論文誌, Vol.61, No.5, pp.1096-1103 (2020-05-15)
[21] Ryoichi Sasaki “Risk Assessment Method for Balancing Safety, Security, and Privacy in Medical IoT Systems with Remote Maintenance Function” IEEE, CFSE2020
[22] Takuo Hayakawa, Ryoichi Sasaki, Hiroshi Hayashi, Yuji Takahashi, Tomoko Kaneko, and Takao Okubo “Proposal and application of security/safety evaluation method for medical device system that includes IoT” ICNCC '18: Proceedings of the 2018 VII International Conference on Network, Communication and Computing, December 2018
[23] 佐々木良一　金子朋子　高橋雄志　福澤寧子「リモートメンテナンスを伴いフィードバックを有する医療用 IoT システムのリスクアセスメント手法」日本セキュリティ・マネジメント学会 2022 年 1 月号 pp3-17
[24] Ryoichi Sasaki “AI and Security - What changes with generative AI-” IEEE QRS2023
[25] Ryoichi Sasaki, Kenta Onishi, Yoshihiro Mitsui, Masato Terada,” Development and Trial Application of an Improved MRC-EDC Method for Risk Assessment of Attacks on Humans by Generative AI” Journal of Information Processing Vol.32 1057–1065 (Dec. 2024)
[26] Ryoichi Sasaki “Trial application of risk assessment method for metaverse” CFSE2022　in IEEE QRS2022
[27] Toshiya Seyama, Ryoichi Sasaki “Trial of Risk Assessment for Business Application of Metaverse” IEEE MetaCom 2023
[28] 瀬山稔哉，藤本一男，千葉尭，佐々木良一「メタバースのビジネス応用のためのリスクアセスメント法の評価」情報処理学会論文誌 Vol.65, No.9, pp 1423-1430, 2024 年 9 月号
[29] 佐々木良一，会田和弘，工藤竜也，寺田真敏「動的特性に対応可能なリスクコミュニケーション手法 MRC -Dynamics の開発と能動的サイバー防御政策への適用」日本セキュリティ・マネジメント学会第 38 回全国大会研究報告書，2025 年 8 月
[30] 大前俊暁，山田剛一，増田英孝，佐々木良一「社会共同体における対リスク施策決定議論を支援する AI システム」情報処理学会論文誌 2025 年 9 月号（掲載決定）
[31] Wei, J., Wang, X., Schuurmans, D., Bosma, M., Ichter, B., Xia, F., Chi, E., Le, Q., & Zhou, D., "Chain-of-Thought Prompting Elicits Reasoning in Large Language Models," Advances in Neural Information Processing Systems, Vol.35, pp.24827-24837 (2022).