Vol.2015-EMB-38 No.5
2015/8/28

遠隔診療におけるリスクアセスメント手法の提案

藤田健治[†1]　青木利晃[†1]

ICT の進展により，遠隔診療の展開可能性が高まっている．遠隔診療は地域のネットワーク回線を介した形態をとるため，自然災害等の外部環境からの影響を考慮する必要がある．しかしながら，これに適用可能なリスクアセスメント手法が存在していない．そのため，自然災害などの外部環境における事象がシステムに与える影響を分析する手法として，複合的因果関係分析手法（MCCA:Multiple Cause Consequence Analysis）を提案する．

A Risk Assessment Method for Telemedicine

KENJI FUJITA[†1]　TOSHIAKI AOKI[†1]

Nowadays, the possibility of telemedicine is becoming higher level according the progress of ICT. The telemedicine is a system which is dispersed over an area. It is necessary to consider the influence from the external environment, such as natural disasters; however a risk assessment method for such effects does not exist. In this report, we propose MCCA(Multiple Cause Consequence Analysis) . It can analyze the effects of external event.

1. はじめに

ヘルスケア関連機器，ウェアラブル機器の市場への登場により，遠隔診療の展開可能性はより高まっている．遠隔診療は地域に分散した形態をとるため，自然災害等環境からの影響を考慮することが望まれる. しかしながら, 現状，これに適したリスクアセスメント手法が存在していない．本研究では，環境からの影響を分析可能とするリスクアセスメント手法として，環境から影響を受けるメカニズムに着目した複合的因果関係分析手法（MCCA: Multiple Cause Consequence Analysis）を提案し，適用実験を行った．その結果，本手法により，環境による対象システムへの影響分析を行えると共に，故障の連鎖，多重故障の観点から対象システムへの影響分析を行えることを確認した．また，本手法を導入して分析を進める場合，確認パターン数は膨大なものとなるため，大規模なシステムに対してはツールによる支援が前提となることが明らかになった．

本論文の構成として，まず 1 章は研究の概要を述べる．2 章から 4 章にかけては MCCA の検討経緯を述べ，5 章では MCCA の説明を行い，6 章では適用実験，及び実験結果に対する考察について述べる．7 章では関連研究について紹介した後，最後に，8 章で研究内容のまとめと今後の課題について述べる．

2. 遠隔診療における安全設計

遠隔診療は，遠隔医療のうち，医師が遠隔地から在宅等で療養する患者の診察およびそれに続く一連の診療を行うことを意味する[1]．いわゆる医師-患者間の非対面診療である. 遠隔診療が特に展開する可能性がある地域としては，高齢化が進み在宅医療の需要が高まる地域，往診医師が不足する地域，高血圧，糖尿病，心疾患等，慢性疾患管理が必要で，管理のための通院や往診が困難な地域などが考えられる[2].

遠隔診療は，通信技術を活用して離れた二地点間で行われるという点において一般的な診療と異なる．しかしながら，遠隔診療においては，現状，患者安全に対する薬事規制，ガイドライン，安全関連規格の整備が十分でなく，患者安全についての明確的な設計方針は定められていない．そのため，過去の医療過誤と同様に事故が発生し，人身に傷害を与える可能性がある．そこで，遠隔診療システムを対象に，安全の国際規格である「電気・電子・プログラマブル電子系の機能安全（IEC61508）」等を参考に安全設計を実施し，リスク低減効果の確認を行った．リスク対策の効果については試作システムによる確認を行っている[3].

遠隔診療のリスクアセスメントにおいて，病院と患者宅の二地点間の通信回線を隔てて行われるため，患者安全を考える場合，自然現象やヒューマンエラー等外部事象による通信回線，及び遠隔診療への影響を網羅的に整理して分析すると共に，故障の連鎖，多重故障の観点からも網羅的な分析が必要である．しかしながら，現状，これに適した既存のリスクアセスメント手法が存在していなかった．

3. 既存のリスクアセスメント手法

3.1 既存のリスクアセスメント手法の適用可能性

リスクアセスメントは，安全を達成するためにリスクを許容可能なレベルまで低減するプロセスであり，様々な手法が存在する．遠隔診療の観点から，既存のリスクアセスメント手法について確認する．これにより，遠隔診療でのリスクアセスメント手法における要件を明確にする．

†1 北陸先端科学技術大学院大学
Japan Advanced Institute of Science and Technology

表 1 既存のリスクアセスメント手法

○は適用可能，または対応可能

#	手法名	発生原因特定	影響分析	外部事象への対応	故障連鎖多重故障	備考
1	HAZOP		○			パラメータの設計意図からのズレの原因と影響を評価
2	STPA		○			制御構造図における振る舞いを分析
3	FMEA		○			構成要素の故障モードとその上位項目への影響を確認
4	FTA	○			○	特定故障から発生原因を特定
5	CCA		○	○		起因現象がシステムに与える影響を分析

3.2 分析

(1) HAZOP

HAZOP（Hazard And Operability Study）は，電圧や温度のようなプラントのパラメータの設計意図からのズレの原因と影響を評価することで，製品に潜在する事故シナリオを摘出し，その軽減策を検討する方法である[4]．HAZOP は，設計意図からのズレの原因と影響という特定の観点からの評価に限定される．外部事象による影響の分析，故障の連鎖，多重故障の観点から評価するものではない．

(2) STPA

STPA（STAMP‐Based Process Analysis）は，制御構造図における不適切な制御の振る舞いによりハザードシナリオを識別する手法である[5]．発生事象からのシステムへの影響を分析する手法ではあるが，パラメータの変動による特定の観点からの分析に限定される．外部事象による影響の分析，故障の連鎖，多重故障の観点から評価するものではない．

(3) FMEA

FMEA（Fault Mode and Effect Analysis）は，設計上の潜在的な欠点を見出すために構成要素の故障モードとその上位項目への影響を確認する手法である[4]．外部事象による影響には向いておらず，発生事象がシステムへ与える影響を分析する手法ではない．

(4) FTA

FTA（Fault Tree Analysis）は，システムの特定故障を想定して，その発生原因を上位レベルから下位レベルまで論理的に展開し，最下位レベルのシステムの機能の故障発生率からシステムの特定故障の発生原因や発生確率を求める方法である[4]．FTA は対象とするシステムにおいて，望ましくない事象をトップイベントとして設定し，トップイベントの発生原因を機器・部品レベルまで展開し，その原因・結果を論理記号で結びつけてツリー状に表現したものである．そのため，外部事象による影響の分析には適していない．また，FTA は故障の連鎖，多重故障を取り扱うことは可能であるが，遠隔診療のような複雑なシステムの場合，対象のケースが多岐にわたるため網羅的に分析するには適していない．

(5) CCA

CCA（Cause-Consequence Analysis）は，起因現象，及びそれに影響を及ぼす要因と展開結果をダイアグラムに表わすものである[6]．CCA を実行すれば，すべてのリスクを特定することが可能である[7]．CCA は，外部事象による影響を分析することは可能であるが，個々のケースに対して分析を実施する手法である．対象システムの規模があまり大きくなく簡単な場合によく用いられる．遠隔診療ではシステムの規模が大きくなると共に複雑となるため，遠隔診療におけるリスクアセスメントへの適用に適していない．

3.3 遠隔診療でのリスクアセスメント手法に対する要件

遠隔診療でのリスクアセスメントの観点から既存のリスクアセスメント手法を分析すると，表 1 に示す通り，既存のリスクアセスメント手法は発生故障から原因を特定する手法と，発生事象がシステムへ与える影響を分析する手法に分類され，遠隔診療でのリスクアセスメントにおいては後者の手法が求められることがわかった．また，外部事象による通信回線，及び遠隔診療への影響を網羅的に整理して分析でき，かつ故障の連鎖，多重故障の観点から網羅的に分析ができる既存リスクアセスメント手法がないことがわかった．よって，遠隔診療でのリスクアセスメント手法に対する要件としては，自然現象やヒューマンエラー等外部事象が通信回線，及び遠隔診療に与える影響を網羅的に整理して分析できること，故障の連鎖，多重故障の観点からも発生事象がシステムに与える影響を網羅的に分析できることに加えて，大規模なシステムや複雑なシステムに適用可能であることが挙げられる．

4. 本研究のアプローチ

現状，遠隔診療に適したリスクアセスメント手法が存在していない．そのため，過去の医療過誤と同様に事故が発生し，人身に傷害を与える可能性がある．遠隔診療は病院と患者宅の二地点間の通信回線を隔てて行われるため，患者安全を考える場合，自然現象やヒューマンエラー等外部事象による通信回線，及び遠隔診療への影響を網羅的に整理して分析すると共に，故障の連鎖，多重故障の観点からも網羅的に分析する必要がある．そのため，遠隔診療でのリスクアセスメント手法に対する要件を満たす新たなリス

クアセスメント手法を提案し，評価を実施する．

遠隔診療の場合，地域に分散した形態をとるため，自然災害等環境からの影響も考慮する必要がある．システム外部において地震等の事象が発生した場合,その外部事象は，停電による電源供給障害発生など最終的に何らかの内部事象に伝播される．例を図 1 に示す．地震が発生した結果，機器故障が発生するケース，停電が発生し電源障害が発生するケースなどがあげられる．このようにシステム内における事象の展開規則を与えることにより，システムの外部事象をシステムの内部事象へ置き換えることが可能である．

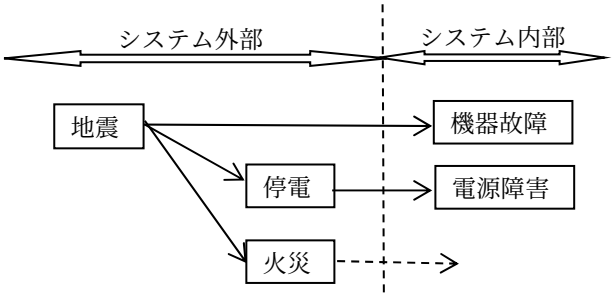

図 1　地震における事象展開例

システムの外部事象から内部事象への展開規則を定め，その事象の伝播をモデル化することにより，外部事象がシステムに及ぼす影響を分析することが可能になる．また，複数の事象を連続的に発生させることで故障の連鎖や多重故障によるシステムの挙動を分析することも可能になる．この考え方に基づいて検討したリスクアセスメント手法が複合的因果関係分析手法 MCCA(Multiple Cause Consequence Analysis)である．

5. リスクアセスメント手法 MCCA

5.1 MCCA の概要

複合的因果関係分析手法 MCCA は，リスクアセスメントにおいて，システムの外部事象からシステムの内部事象への展開規則を与えることによりシステムの外部事象がシステムへ及ぼす影響の分析を可能とする．また，複数の事象を連続的に発生させることで故障の連鎖や多重故障によるシステムの挙動の分析も可能とする．

MCCA の処理概要を図 2 に示す．MCCA では，事象の生成，事象展開，システムの状態遷移といった処理を一つのサイクルとし，このサイクルを繰り返し実施し，結果を評価することでリスクアセスメントを実施する．生成事象がシステムの外部事象であった場合は，システムの外部事象からシステムの内部事象への展開規則に基づいて事象展開を実施する．導き出された最終的な事象に基づいてシステムにおける状態の遷移を実施する．サイクル開始時は，状態は初期状態を設定しておくものとする．

事象生成　　事象展開

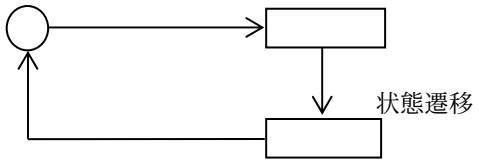

図 2 MCCA の処理概要

以降では，例として電灯を対象に分析した場合の例を用いて説明する．電灯を図 3 に示す．

図 3 電灯

5.2 用語の定義

(1) 事象

他の現象と区別できる単一の観察可能な現象

(2) 生成事象

MCCA によって生成される事象

(3) シナリオ

事象の発生履歴

(4) 展開規則

システムの外部事象をシステムの内部事象へ展開する際の規則

(5) 制約条件

システム構成要素のある状態と，その状態に対しては発生し得ない事象の組み合わせ

5.3 テーブル

5.3.1 概要

MCCA におけるテーブル構成を表 2 に示す．MCCA では，事象を生成し，それがシステムに与える影響を評価するために，ID を定義するための 3 つのテーブルと，事象と状態を対応づけるための 3 つのテーブルを利用する．

表 2 MCCA におけるテーブル構成

#	テーブル名	内容
1	要素 ID	システムの構成要素
2	事象 ID	システム事象
3	状態 ID	システムの構成要素が持つ状態
4	事象展開	外部事象から内部事象への展開内容
5	制約条件	特定状態において発生しない事象
6	状態遷移	発生事象に対する状態遷移

5.3.2 ID 関連テーブル

(1) 要素 ID テーブル

システムの構成要素を識別するための ID を定義する．要素 ID テーブルは以下のように構成される．

要素 ID	要素名

- 要素 ID：システムの構成要素の識別 ID
- 要素名:要素 ID に対応するシステムの構成要素の名称

要素 ID テーブルの例を表 3 に示す．電灯に対しては，要素 ID として EL01，要素名として電灯を定義する．

表 3 要素 ID テーブルの例

要素 ID	要素名
EL01	電灯

(2) 事象 ID テーブル

事象を識別するための ID を定義する．事象 ID テーブルは以下のように構成される．このテーブルにおいて，外部事象，内部事象であるかは問わない．

事象 ID	事象名

- 事象 ID：事象の識別 ID
- 事象名：事象 ID に対応する事象の名称

事象 ID テーブルの例を表 4 に示す．例えば，電灯障害発生に対しては，事象 ID として EV0101，事象名として電灯障害発生を定義する．

表 4 事象 ID テーブルの例

事象 ID	事象内容
EV0101	電灯障害発生
EV0102	電灯障害回復
EV0901	地震
EV0902	津波
EV0903	火災
EV0904	停電

(3) 状態 ID テーブル

システムの構成要素が持つ状態を識別するための ID を定義する．状態 ID テーブルは以下のように構成される．

状態 ID	状態名

- 状態 ID：状態の識別 ID
- 状態名：状態 ID に対応する状態の名称

状態 ID テーブルの例を表 5 に示す．電灯点灯中に対しては，状態 ID として ST0101，状態名として電灯点灯中を定義する．

表 5 状態 ID テーブルの例

状態 ID	状態名
ST0101	電灯点灯中
ST0102	電灯障害中

5.3.3 処理関連テーブル

(1) 事象展開テーブル

発生した外部事象に対して次に発生し得る事象を定義する．事象展開テーブルは以下のように構成される．次に発生し得る事象は複数を定義することが可能である．

発生事象 ID	次発生事象 ID

- 発生事象 ID：発生事象の事象 ID
- 次発生事象 ID：発生事象から派生して発生する事象の事象 ID

事象展開テーブルの例を表 6 に示す．例えば，地震に対して津波が発生した場合，発生事象 ID として，地震の事象 ID である EV0901，次発生事象 ID として EV0903 を定義する．

表 6 事象展開テーブルの例

発生事象 ID	次発生事象 ID	備考
EV0901	EV0902	地震→津波
	EV0903	地震→火災
	EV0904	地震→停電
	EV0101	地震→電灯障害発生
EV0902	EV0903	津波→火災
	EV0904	津波→停電
	EV0101	津波→電灯障害発生
EV0903	EV0904	火災→停電
EV0904	EV0201	停電→電灯障害発生

(2) 制約条件テーブル

特定状態において，発生しない事象を定義する．制約条件テーブルは以下のように構成される．

状態 ID	非発生事象 ID

- 状態 ID：状態 ID
- 非発生事象 ID：状態 ID に対応する状態にて発生しない事象の事象 ID

制約条件テーブルの例を表 7 に示す．例を挙げると，電灯点灯中に電灯障害回復が発生することはない．これに対応した制約条件として，電灯点灯中の状態 ID である ST0101 に対して，非発生事象 ID として電灯障害回復の事象 ID である EV0102 を定義する．

表 7 制約条件テーブルの例

状態 ID	非発生事象 ID	備考
ST0101	EV0102	電灯点灯中の電灯障害回復
ST0102	EV0101	電灯障害中の電灯障害発生

(3) 状態遷移テーブル

特定状態において発生した事象に対する状態遷移後の

状態を定義する．

状態 ID	発生事象 ID	次状態 ID

- 状態 ID：状態 ID
- 発生事象 ID：発生事象の事象 ID
- 次状態 ID：発生事象に対する状態遷移後の状態 ID

状態遷移テーブルの例を表 8 に示す．例えば，電灯点灯中に電灯障害が発生した場合は，電灯は電灯障害中へ状態遷移する場合，状態 ID は，電灯点灯中の状態 ID である ST0101，発生事象 ID は，電灯障害発生の事象 ID である EV0101，次状態 ID として，電灯障害の状態 ID である ST0102 を定義する．

表 8 状態遷移テーブルの例

状態 ID	発生事象 ID	次状態 ID	状態	発生事象	次状態
ST0101	EV0101	ST0102	電灯 点灯中	電灯 障害発生	電灯 障害中
ST0102	EV0102	ST0101	電灯 障害中	電灯 障害回復	電灯 点灯中

5.4 手順

MCCA は，事前分析，事象展開，評価の 3 つの手順で評価を行う．表 9 に MCCA の手順を示す． 手順１の事前分析では，システム構成要素，及びその状態，事象，事象の展開規則，発生事象の制約条件を識別し，全てのテーブルを作成する．手順２の事象展開では，事象を生成，生成事象が外部事象の場合は展開規則に基づいて内部事象へ事象展開し，システム構成要素の状態遷移を行う．手順３の評価では，MCCA で生成される事象に対するシステムの動作を分析し，リスクを洗い出す．以降，各手順の詳細を説明する．

表 9 MCCA の手順

#	手順名	内容	出力物
1	事前準備	テーブル作成	・要素 ID テーブル ・事象 ID テーブル ・状態 ID テーブル ・事象展開テーブル ・制約条件テーブル ・状態遷移テーブル
2	事象展開	事象生成	・発生事象の履歴 ・状態遷移内容
3	評価	アセスメント	・特定したリスク

5.4.1 事前分析

事前分析では，システム構成要素，及びその状態，事象，事象の展開規則，発生事象の制約条件を識別し，表 2 に示すテーブルを作成する．

5.4.2 事象展開

事象を生成，生成事象が外部事象の場合は展開規則に基づいて内部事象へ事象展開し，システム構成要素の状態遷移を行う．事象生成は，事象発生プロセス，事象展開プロセス，状態遷移プロセスの 3 つのプロセスに分かれる．事象の展開イメージを図 4 に示す．これらの 3 つのプロセスを一つのサイクルとし，繰り返し実施する．

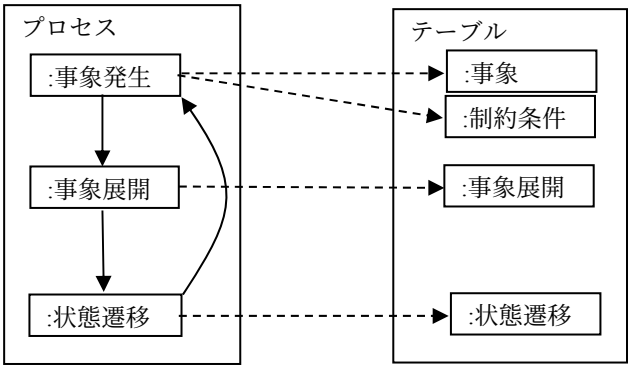

図 4 事象の展開イメージ

(1) 事象発生プロセス

事象発生プロセスでは，事象テーブル，制約条件テーブルと各システム構成要素の状態を参照し，事象を生成する．各システム構成要素と制約条件テーブルを参照し，制約条件を満たす事象を生成するようにする．一例を挙げると，電灯の状態が電灯点灯中の場合には，表 7 の制約条件テーブルにより，電灯障害回復は発生し得ない．この場合は制約条件を満たす事象として地震を選択し，発生させる．

(2) 事象展開プロセス

事象展開プロセスでは事象展開テーブルを参照し，事象発生プロセスで生成された事象を展開する．一例を挙げると，表 6 を参照し，地震から津波，津波から停電，停電から電灯障害発生と事象展開プロセスを展開させる．

(3) 状態遷移プロセス

最後の状態遷移プロセスでは事象展開プロセスで確定した内部事象に基づいて状態遷移テーブルを参照し，状態遷移を行う．一つの事象の事象展開，システム構成要素の状態遷移が終了したら，事象発生プロセスに戻る．一例を挙げると，電灯の状態が電灯点灯中の場合に，最終的な内部事象として電灯障害発生が生じた場合は，電灯の状態を電灯障害中にする．

5.4.3 評価

発生事象に対する各状態の遷移内容からシステムの動作を評価する．作成例においては，電灯の状態が電灯点灯中の場合に地震が発生し，地震→津波→停電→電灯障害発生という流れで電灯障害が発生し，電灯の状態が電灯障害中になったことなどに対する評価を実施する．

6. 提案手法の適用実験

6.1 目的

提案手法を評価するために，適用実験を行った．主な評価内容は，提案手法の有効性である．

6.2 対象システム

提案手法の有効性を評価するために，単純化しやすいルーター運用のケースを対象とした．

(1) システム構成

システム構成を図 5 に示す．システム構成要素は次の通りとする．この場合，通信が可能となるのはルーター，回線が共に稼働状態にある場合である．また，電源，UPS が共に障害中となった場合は,ルーターが稼働できないため，通信不可となる．

- ルーター
- 電源
- UPS
- 回線

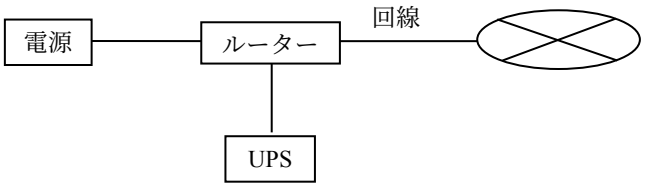

図 5 システム構成

(2) 前提条件

前提条件として，外部事象は簡素化し，地震，火災，停電のみ発生するものとする．表 10 に事象に関する前提条件を示す．地震からの展開事象として，火災，停電，各システム構成要素の故障が発生し，火災からの展開事象として停電，各システム構成要素の故障，停電からの展開事象として,電源供給障害,回線障害が発生し得るものとする．

表 10 事象に関する前提条件

発生事象	次発生事象
地震	・火災 ・停電 ・各システム構成要素の故障
火災	・停電 ・各システム構成要素の故障
停電	・電源供給障害 ・回線障害

6.1 外部事象の展開

6.1.1 事象展開テーブル

この場合の事象展開テーブルは，表 11 に示す 13 通りとなった．事象展開の一例を挙げると，表 11 の#1 の地震から火災，表 11 の#7 の火災から停電，表 11 の#12 の停電から電源供給障害発生という展開が挙げられる．いずれの事象も最終的には内部事象に展開されることがわかった．

表 11 事象展開テーブル

#	発生事象	次発生事象	備考
1	地震	火災	外部事象
2		停電	外部事象
3		電源供給障害発生	内部事象
4		ルーター障害発生	内部事象
5		UPS 障害発生	内部事象
6		回線障害発生	内部事象
7	火災	停電	外部事象
8		電源供給障害発生	内部事象
9		ルーター障害発生	内部事象
10		UPS 障害発生	内部事象
11		回線障害発生	内部事象
12	停電	電源供給障害発生	内部事象
13		回線障害発生	内部事象

6.1.2 外部事象の展開パターン

表 11 に従い，外部事象を展開した場合のパターン数は表 12 に示す 16 通りとなった．UPS については，バッテリー切れ，バッテリー回復の事象発生も想定されるが，外部事象に起因して発生する事象ではないため，事象展開の対象外とする．

表 12 事象展開パターン

#	事象展開パターン
1	地震→火災→停電→電源供給障害発生
2	地震→火災→停電→回線障害発生
3	地震→停電→電源供給障害発生
4	地震→停電→回線障害発生
5	地震→電源供給障害発生
6	地震→ルーター障害発生
7	地震→UPS 障害発生
8	地震→回線障害発生
9	火災→停電→電源供給障害発生
10	火災→停電→回線障害発生
11	火災→電源供給障害発生
12	火災→ルーター障害発生
13	火災→UPS 障害発生
14	火災→回線障害発生
15	停電→電源供給障害発生
16	停電→回線障害発生

6.1.3 システム全体の事象発生パターン

単一で発生した場合の事象は，電源供給障害発生，電源供給障害復旧，ルーター障害発生，ルーター障害復旧，UPS 障害発生，UPS 障害復旧，UPS バッテリー切れ，UPS バッテリー回復，回線障害発生，回線障害復旧の 10 個となる．システム全体の事象発生パターンは表 12 に示す外事事象の展開パターン数 16 通りにシステムの内部事象が単一で発生した場合の事象 10 通りを加えた 26 通りとなった．これを表 13 に示す．これにより，事象展開テーブルを用いて，システム全体の事象発生パターンを網羅的に生成し，評価可能であることがわかった．

表 13 システム全体の事象発生パターン

#	事象展開パターン
1	地震→火災→停電→電源供給障害発生
2	地震→火災→停電→回線障害発生
3	地震→停電→電源供給障害発生
4	地震→停電→回線障害発生
5	地震→電源供給障害発生
6	地震→ルーター障害発生
7	地震→UPS 障害発生
8	地震→回線障害発生
9	火災→停電→電源供給障害発生
10	火災→停電→回線障害発生
11	火災→電源供給障害発生
12	火災→ルーター障害発生
13	火災→UPS 障害発生
14	火災→回線障害発生
15	停電→電源供給障害発生
16	停電→回線障害発生
17	電源供給障害発生
18	電源供給障害復旧
19	ルーター障害発生
20	ルーター障害復旧
21	UPS 障害発生
22	UPS 障害復旧
23	UPS バッテリー切れ
24	UPS バッテリー回復
25	回線障害発生
26	回線障害復旧

6.2 システムへの影響分析

システムへの影響分析例として，外部事象がシステムに与える影響の分析，故障の連鎖や多重故障によるシステムへの影響分析を行った．

(1) 外部事象がシステムに与える影響の分析

外部事象がシステムに与える影響の分析として，ルーターが運用中の状況において地震が発生した場合に，停電，電源供給障害発生という事象展開を経た結果，ルーターが電源供給障害中へ遷移することが確認できた．事象展開，状態遷移の流れを表 14 に示す. 表 11 に示す事象展開テーブルに示されている通り，地震による表 11 の#2 の停電が発生した場合は, 表 11 の#12 により内部事象として電源供給障害が発生する．その結果，ルーターは電源供給障害中に状態遷移するため，外部事象がシステムへ与える影響を分析することが可能であることがわかる．

表 14 外部事象がシステムに与える影響の分析

#	発生事象	要素	ルーターの次状態
1	地震		
2	停電		
3	電源供給障害発生	ルーター	電源供給障害中

(2) 故障の連鎖や多重故障による状態遷移

故障の連鎖による状態遷移として，UPS バッテリー切れ中に UPS 障害発生による状態遷移を確認した．事象展開，状態遷移の流れを表 15 に示す．UPS バッテリー切れ中に UPS 障害が発生した場合，UPS バッテリー回復するまで UPS 障害を検出できないリスクがある．このリスクが許容されない場合は対策を行う必要があることがわかる．

表 15 故障の連鎖がシステムに与える影響の分析

#	発生事象	要素	UPS の次状態
1	UPS バッテリー切れ	UPS	UPS バッテリー切れ
2	UPS 障害発生	UPS	UPS 障害中
3	UPS バッテリー回復	UPS	UPS 障害中

6.3 評価・考察

適用実験を実施した結果，提案手法について次のことを確認した．提案手法では事象展開により，いずれの外部事象も最終的には内部事象に置き換わる．これにより，遠隔診療にリスクアセスメント手法を適用する場合の一つ目の要件である外部事象がシステムに与える影響を網羅的に整理しての分析が可能であることを確認した．また，事象を連続的に生成することで，故障の連鎖や多重故障による状態遷移の分析が可能であることを確認した．これにより二つ目の要件である故障の連鎖や多重故障の観点による網羅的な分析が可能であることを確認した．

また，事象組み合わせの網羅に必要な事象発生パターン数は，x^n（x:事象発生パターン数，n:組み合わせのレベル）となる．そのため，事象発生パターン数が大きくなるような大規模システムや複雑な事例についてはツールによる支援が必要である．

7. 関連研究

(1) EPC

EPC（Event-Process Chain）は，システムを，イベントと機能との間を有効線分で結んだ別個のプロセスチェーンに分割する手法であり，Mock が EPC を用いたリスクアセスメントを行っている[8]．外部事象からの事象展開，故障の連鎖や多重故障を取り扱うことが可能であるが，事象の展開規則は持っておらず，事象発生パターンについては個々のパターンを羅列する必要がある．

(2) SMHA

SMHA（State Machine Hazard Analysis）は，状態遷移図を対象に，初期状態から遷移可能な全てのパスを網羅的に探索し，リスクが潜在するパスを摘出する[9]．状態遷移図を用いるため，扱える事象は単一の事象のみであり，事象展開は行えない．

(3) ESIM

ESIM（Embedded Systems Improving Method）は，理論的なモデルから簡略化した状態遷移表である非正常系分析マトリクスを適用した障害シナリオ抽出手法である[10]．これは，ガイドワードを用いて特定の観点から非正常系の分析を行うものである．局所的な分析に向いた手法であり，全体的な視野での分析が難しい．.

(4) SASTD/SAHSTD

SASTD（Safety Analysis method based on State Transition Diagram）は，状態遷移図を対象に，状態遷移図の各状態において満たされるべき条件が満たされていないという逸脱と，状態が遷移する際に実行されるべき処理が実行されていないという逸脱を HAZOP のガイドワードを用いてより網羅的に列挙するための手法である[11]．一方，SAHSTD（Safety analysis method based on hierarchical state transition diagram）は，SASTD に対してさらに状態遷移を階層化させた手法である．いずれも，ガイドワードを用いて，システムの正常な動作からの逸脱を分析するものであり，全体的な視野での分析が難しい．

8. まとめと今後の課題

現状，遠隔診療に適したリスクアセスメント手法が存在していない．本研究では，自然災害等の外部事象がシステムに与える影響について網羅的に分析することが可能で，故障連鎖や多重故障に対する影響も網羅的に分析を可能とする MCCA を提案した．また，提案手法に従ってルーター運用への適用実験を行った．適用実験の結果，提案手法により自然災害等環境からの影響が網羅的に分析可能であるとともに，事象展開パターンが網羅的に作成され故障連鎖や多重故障に対する影響を網羅的に分析可能であることを確認した．

今後の課題として，提案手法では，複雑なシステムの場合，組み合わせの網羅に必要な確認パターン数は，膨大なものとなるため，ツールによる支援が前提となることが明らかになった．支援ツールの検討が今後の課題である．また，今後は，MCCA 以外にも自然災害等の外部事象がシステムに与える影響を理論的に分析する手法の研究が進み，それらの研究をベースにして，複雑化したシステムに対するリスクアセスメントの質が向上することが期待される．

参考文献

1) 日本遠隔医療学会:遠隔診療指針, 日本遠隔医療学会, 2011.
2) 米澤麻子, 長谷川高志:総務省地域 ICT 利活用モデル構築事業, 遠隔医療モデルプロジェクト総括報告, 日本遠隔医療学会雑誌, 第 6 巻, 第 1 号, pp.55-58,(2010).
3) 藤田健治:遠隔医療システムの安全設計－リスク低減プロセスに基づいた遠隔医療システムにおける安全設計－, 第 8 巻, 第 1 号, pp.11-18(2012).
4) 社団法人組込みシステム技術協会 安全性向上委員会製品安全ワーキンググループ:組込み系技術者のための安全設計入門, 電波新聞社, 2010.
5) Nancy G. Leveson, Engineering a Safer World, The MIT Press, pp.211-249,(2012)
6) 松岡俊介:プラントの安全性評価 第 4 回 システムの安全性分析, 日本防災システム協会, 第 30 巻 3 号, pp.l8-19,(2008).
7) Nancy Leveson:Safeware : system safety and computers, Addison-Wesley Publishing Company, pp.332-335,(1995).
8) Moc, R., Risk analysis of information systems by event process chains, International Journal of Critical Infrastructures, vol. 1, issue 2-3, pp. 247-257,(2005)
9) Nancy Leveson:Safeware : system safety and computers, Addison-Wesley Publishing Company, pp.346-350,(1995).
10) 三瀬敏朗, 新屋敷泰史, 橋本正明, 中谷多哉子, 片峯恵一, 鵜林尚靖, 吉田隆一:非正常系分析マトリクスによるソフトウェア組込み製品の障害シナリオ抽出手法,電子情報通信学会論文誌, volume J95-D, number 11, pages 1897-1908,(2012)
11) 金周慧, 松原豊, 高田広章: 組込みシステムにおける階層型状態遷移図に基づく安全分析手法, 電子情報通信学会論文誌 A, Vol.J96-A, No.1, pp.34-48, (2013).