ゼロトラスト環境におけるMITRE ATT&CK Cloud Matrixに基づく段階伝播型リスク評価モデルの提案と評価

Proposal and Evaluation of a Stepwise Propagated Risk Evaluation Model Based on the MITRE ATT&CK Cloud Matrix in a Zero Trust Environment

伊藤　吉也†　　加藤　孝史‡　佐々木　良一†　齊藤　泰一†
Yoshinari Ito†　　Takafumi Kato‡　Ryoichi Sasaki†　Taiichi Saito†

†東京電機大学
‡フォーティネットジャパン合同会社
† Tokyo Denki University
‡ Fortinet Japan G.K.

要旨

サイバー攻撃は年々その頻度と複雑性を増しており、組織に対するリスクが質量ともに拡大の一途をたどっている。自社内の情報システムのリスク分析を実施しその対策を実施することの重要性は広く認知されてきており業界標準のリスク分析ガイドブックの存在は重要である。そのひとつである IPA 制御システムのセキュリティリスク分析ガイドは、経済産業省の依頼により重要インフラ企業向けに開発されたものであるが、その手法の手順が明確化されているため、地方公共団体の情報セキュリティポリシーガイドライン検討会やデジタル庁など重要インフラ企業以外でも幅広く採用されている。一方で本ガイドにはいくつかの課題が潜在している。今回は、事業被害ベースのリスク分析の課題に焦点をあてる。標準でプリセットされている脅威・対策セットは非常に広義で、どのようにその脅威を発生させるかについて、具体的な手口を自社で策定していかなくてはならず分析コストが高くなる点、攻撃者視点から攻撃シナリオに基づいた攻撃ツリーを策定しなければならない点、段階毎にその対策の実施具合によって変化するリスク値を攻撃ツリー全体のリスク値に活かしきれていない点の３点について、解決手法を提案する。そこで本研究では、MITRE ATT&CK の STIX2.0 データを取り込み、Cloud Matrix に含まれる攻撃テクニック群より攻撃再現性スコアにより新たに再発する可能性の高い攻撃テクニックを選定する手法の提案、選定された攻撃テクニックを標的資産にマッピングし攻撃シナリオを実現するための攻撃ツリーの適正数を生成する手法を提案する。また、攻撃ツリーのステップ毎の残存リスク値に基づき、前段階の残存リスクが次段階の残存リスクに連鎖的に影響を与える段階伝播型リスク評価モデルを提案し、IPA 方式との比較を検証する。

キーワード

MITRE ATT&CK、シナリオ/事業被害ベース、リスクアセスメント、ゼロトラスト、Cloud Matrix

1. はじめに

近年、サイバー攻撃の手法は高度化・巧妙化が進み、組織の情報資産に深刻な影響を及ぼす脅威として広く認識されている。国家サイバー統括室（NCO）（旧・内閣官房サイバーセキュリティセンター（NISC））によれば、従来から多発しているランサムウェアや標的型メールに加え、近年ではクラウド環境を標的とした攻撃が急増している［1］。こうした動向を踏まえ、情報システムに対するリスク分析と対策の必要性が急速に高まっている。その中で、我が国のリスク分析実務において広く参照されているのが、独立行政法人情報処理推進機構（IPA）が提供する『制御システムのセキュリティ分析ガイド』（以下、IPA 方式）である［2］。本ガイドは経済産業省の要請を受けて策定されたもので、ICS（Industrial Control Systems：産業用制御システム）を想定したリスク評価手法が提示されている。その体系的な分析プロセスと脅威・対策のプリセットが明示されている点から、重要インフラ企業に限らず、一般企業や地方自治体でも採用が進んでいる。しかしながら、この IPA 方式の標準の脅威・対策のプリセットは非常に広義で粒度が粗い。IPA 方式のシナリオベースのリスク分析の際に策定する具体的な攻撃手口の手法を自社環境に合わせて考えて策定しなければならない。国は 2030 年を目標に、地方自治体におけるセキュリティモデルを「三層分離型」からゼロトラストへ転換する方針を示している。この政策の一環として、2025 年度よりデジタル庁主導でゼロトラストにおけるセキュリティ対策の実証事業が 7 団体で開始され［3］、他の全国 1800 の自治体も今後、ゼロトラストへの移行への対応を迫られていく［4］。このような強い社会的ニーズを背景として、本

研究では IPA 方式を活用する際の課題を解決し、ゼロトラスト環境に適したリスク評価手法を構築することを目的とする。具体的には、MITRE ATT&CK の Cloud Matrix［5］に基づく攻撃テクニックを用い、自治体の重要資産に対して現実的な攻撃シナリオを構成し、攻撃ステップが伝搬する際のリスクを評価する「段階伝播型リスク評価モデル（以降、SPRE 方式）」を提案する。本構成は、第 2 章で既存手法である IPA 方式を紹介し、その問題点を明確化する。第 3 章で提案手法を説明し先行研究との比較を行う。第 4 章で検証と評価を示し、第 5 章で結論と今後の課題を述べる。なお、付録には本研究で用いた Python コード（Google Colab 上で実行した Python の Version は 3.12.11）を掲載し、検証結果は GitHub にて公開する[31]。

2. IPA 方式のリスク評価手法と課題

2.1. IPA 方式の概要

IPA 方式のリスク分析は、表 1 にあるように資産ベースとシナリオベースによるリスク分析の双方を実施する詳細リスク分析を採用している。

表 1 詳細リスク分析と他の分析手法
（出典：IPA 方式をもとに著者が作成）

分析手法			工数	効果
ベースラインアプローチ			小	△
非形式的アプローチ			小	×？
詳細リスク分析	資産ベース		中	○
	シナリオベース	攻撃ツリー解析（ATA）	大	○
		イベントツリー解析（ETA）	大	○
組み合わせアプローチ			大	◎

・資産ベース：システムを構成する資産（サーバ、端末、通信機器等）に対して、その価値、想定される脅威、脆弱性を評価指標としてリスク分析を実施する。
・シナリオベース：業務に対する被害を重視し、最終的な事業被害を回避可能か否かに焦点を当て、攻撃シナリオを構築し、それに基づく攻撃ツリーを策定する。攻撃ステップ群の中から成熟度の高い対策レベルが採択され、事業被害レベル、脅威レベルと脆弱性レベルによりリスク値が算出される。
本研究では、IPA 方式のうちシナリオベースのリスク分析手法に着目し、以下の課題を抽出・考察する。

2.2. 課題１：IPA 方式の脅威・対策セットから具体的な攻撃ストーリが作りにくい点

IPA 方式では、資産ベースの分析に対応するため、あらかじめ表２のように脅威・対策のプリセットが用意されている。
IPA 方式は産業用制御システム（ICS）を前提としているが、リスク分析手法や IPA 方式に標準添付の脅威・対策のプリセットが汎用的な内容であるため、一般企業や地方自治体にも適用されてきた。

表２ IPA 方式資産ベースの脅威・対策一覧より抜粋
※IPA 方式[2]：105 ページより引用

脅威（攻撃手法）	対策					
	防御				検知/影響把握	事業継続
	侵入/拡散抑制		目的遂行抑制			
不正アクセス	ファイアウォール				IPS/IDS	
	通信相手の認証	○			ログ収集・分析	
	IPS/IDS				統合ログ管理システム	
	パッチ適用					
	脆弱性回避					
不正侵作	操作者認証	○				
誤失侵作	URLフィルタリング/Webレピュテーション					
	メールフィルタリング					
不正端末・機器接続	デバイス接続・利用制限		デバイス接続・利用制限		デバイス接続・利用制限	
					ログ収集・分析	
					統合ログ管理システム	
プロセス不正実行	検疫管理	○	検疫管理	○		
	アクセス制御		アクセス制御		機器異常検知	
	ホワイトリストによるプロセスの起動制限	○	ホワイトリストによるプロセスの起動制限	○	機器死活監視	
	重要操作の承認		重要操作の承認		ログ収集・分析	
マルウェア感染	アンチウィルス				機器異常検知	
	ホワイトリストによるプロセスの起動制限	○			機器死活監視	
	パッチ適用				ログ収集・分析	
	脆弱性回避				統合ログ管理システム	
	データ署名					
情報窃取	検疫管理	○	検疫管理	○	ログ収集・分析	
	アクセス制御		アクセス制御		統合ログ管理システム	
	データ暗号化		データ暗号化			
	DLP		DLP			

IPA 方式が提供する脅威と対策群は、非常に広義で粒度が荒い。例えば、「不正アクセス」という IPA 方式の脅威の定義はその候補を具体的にあげていくと多種多様な攻撃手口が存在する。例えば脆弱性を悪用しての不正アクセス、フィッシングメールを送付してからの不正アクセス、デフォルトのルートのアカウントを搾取してからのものなど。IPA 方式のシナリオベースのリスク分析ではその攻撃シナリオを実現していく攻撃手口をいわゆるどのようにの「HOW」の部分までを、自組織で独自に具体的に策定していかなくてはならない。このコストは高くなる傾向がある。

2.3. 課題２：攻撃ツリーの策定数が膨大となりやすい

IPA 方式におけるシナリオベース分析では、分析対象に応じた脅威・対策セットの策定に加え、図２のような複数の攻撃経路を想定した攻撃ツリーの作成が求められる。

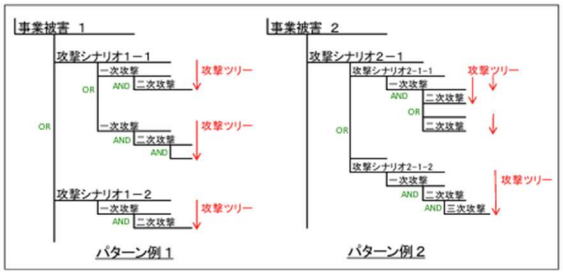


図１ 事業被害・攻撃シナリオ・攻撃ツリー

しかしながら、対象資産が多岐にわたり、攻撃者視点での経路探索も含めると、攻撃パスの組み合わせ数の爆発が発生する。
これにより、リスク分析者の作業負荷が大きくなり、また攻撃手法やそれに対する適切な対策の選定が属人的になり、妥当性判断の困難さを引き起こす可能性がある。

2.4. 課題３：伝播するリスク構造が反映されていない

IPA 方式は、各攻撃ステップにおける脅威と脆弱性の組み合わせにより、表３にあるような最終的な事業被害レベルを評価する「定値結合型リスク評価モデル（Fixed-Value Compositional Risk Model）を採用している。IPA 方式の事業被害レベルは「脅威 × 脆弱性（対策と逆相関の関係。具体的には、対策レベル 3 の十分な対策実施では脆弱性レベルは 1 となり、対策レベル 2 の中程度の対策実施では脆弱性レベルは 2 として評価する。）の乗算によりリスク値を算出する。攻撃ステップ１や２の対策が未実施の場合でも攻撃ステップ３が対策の成熟度が高ければ、その成熟度が攻撃ツリー全体の対策レベルとして採用されてしまう。本来はこのようなケースでは前段階の脆弱性が残存していることから、攻撃ツリー全体のリスク値は危険であるというシグナルを発すべきである。この点については IPA 方式と SPRE 方式の比較の際に具体事例をもとに第４章で検証結果を詳述する。本研究では、これらの構造的な限界を解消するため、段階ごとのリスク伝播を考慮した SPRE 方式を提案する。

表３　シナリオベースのリスク値算定表
(IPA 方式[2]：250 ページより引用)

評価指標と評価値			リスク値	判定条件
脅威レベル	脆弱性レベル	事業被害レベル		
3	3	3	A	事業被害＝3 6≦脅威×脆弱性≦9
3	2	3		
2	3	3		
2	2	3	B	事業被害＝3 3≦脅威×脆弱性＜6
3	1	3		
1	3	3		
3	3	2		事業被害＝2 6≦脅威×脆弱性≦9
3	2	2		
2	3	2		
2	1	3	C	事業被害＝3 1≦脅威×脆弱性＜3
1	2	3		
1	1	3		
2	2	2		事業被害＝2 3≦脅威×脆弱性＜6
3	1	2		
1	3	2		
3	3	1		事業被害＝1 6＜脅威×脆弱性≦9
2	1	2	D	事業被害＝2 1≦脅威×脆弱性＜3
1	2	2		
1	1	2		
3	2	1		事業被害＝1 3＜脅威×脆弱性≦6
2	3	1		
2	2	1		
3	1	1	E	事業被害＝1 1≦脅威×脆弱性≦3
1	3	1		
2	1	1		
1	2	1		
1	1	1		

表４　IPA 方式　攻撃シナリオ全体のリスク値算出法

課題	事業被害	シナリオNo	攻撃シナリオ	資産	脆弱性レベル	リスク値	対策（直接ベースの結果を反映）	対策状況
1	情報漏洩	1-1	ガバメントクラウドのマイナンバー利用事務系システムから住民情報が漏洩する。					
攻撃Step1			ガバメントクラウドの運用管理端末に悪意の第三者が侵入する。	運用管理端末	3		1	MFAを実施していない。IAMで最小権限を行なっていない。
攻撃Step2			運用管理端末の運用アカウントで管理者権限を奪取し、業務アカウントになりすます。	マイナンバー利用事務系業務端末	3		1	MFAを実施していない。EDR導入済。Internetアクセス禁止。IAMで最小権限を付与していない。
攻撃Step3			マイナンバー利用事務系システムに業務アカウントで侵入し住民情報にアクセスする	マイナンバー利用事務系システム	1		3	クラウドファイアウォール機能を利用、運用管理VPCおよび各当該からの通信を必要最小限に制限。
攻撃Step4			住民情報を持ち出す。	マイナンバー利用事務系システム	1	C	3	アプリケーションの通信の不正通信の監視、転送、保存データの暗号化

3. 本研究の提案手法

３.１課題１：MITRE ATT&CK Cloud Matrix の攻撃テクニックを採用

リスク分析者は自ら攻撃の手口を検討しなければならない。それを解決するために本研究では MITRE ATT&CK[6]の攻撃テクニックを攻撃ツリー策定時に検討する攻撃手口として採用する。MITRE ATT&CK は米国の非営利研究機関の MITRE Corporation の攻撃者の行動（Tactics（戦術）、Techniques（技術）、Procedures（手順）：TTPs）に基づく実践的な知識ベースである。MITRE ATT&CK にはその攻撃手法が対象システム毎に Matrix としてまとめられており、Enterprise、Mobile、ICS に分かれている。リスク分析対象として MITRE ATT&CK はその攻撃対象のプラットフォーム毎にも Matrix を用意しており、Windows、MacOS、Linux、Cloud、Network Devices などがある。ゼロトラスト環境下に最も適した Cloud Matrix を採用した。Cloud Matrix はクラウドに特化した 135（重複排除で 111）の攻撃テクニックが存在する。

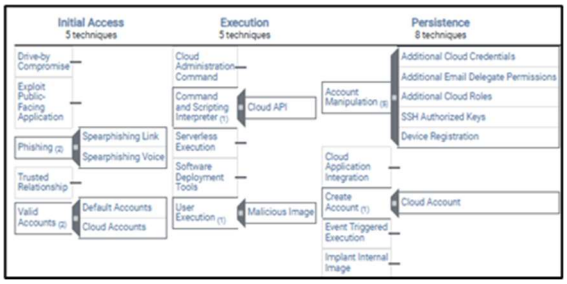


図２　MITRE ATT&CK Cloud Matrix 一部抜粋[12]

この 135 の攻撃テクニック群から以下の客観的指標に基づくスコアリングを実施し、攻撃再現性の高いテクニックを 16 選定する。

MITRE ATT&CK 自体でそれらの攻撃テクニックの脅威発生可能性や危険度などの定義は行っていないため、先行研究の以下の論文や記事を参照し、Cloud Matrix の攻撃テクニック群の中から MITRE ATT&CK 観測データを基に攻撃グループ等が過去に何回再現して利用したのかの頻度数を取得し、攻撃再現性スコアリングを行う。

スコアリングでは MITREATT&CK が提供する STIX2.0 形式の JSON ファイルを利用した。それを Python の Pandas 等を用いて構造化データを抽出・集計した。（詳細は参考文献[7]および Appendix1 を参照）

３.１.１：スコアリング策定のために参照した先行研究

・Hardik らは推論により MITRE 攻撃テクニックの最終攻撃目標である Impact をその攻撃が成功した場合に与える影響と悪用可能性を高、中、低でレベル分けし保護スコアを算出した。[8]

・Picus-RedReport-2025 は 2024 年中の 100 万以上のマルウェアサンプルを調査し、1,400 万以上の悪意のあるアクションと 1,100 万以上の MITRE ATT&CK テクニックをマッピングし最も頻繁に観測された MITRE 攻撃テクニックの Top10 を抽出した。[9]

・Jon Baker らは MITRE 攻撃テクニックを収集した実データからの実行可能性（頻度分析）、オープンソースの脅威レポートを分析し、チョークポイントになりえる MITRE 攻撃テクニックを抽出、攻撃テクニックにおける検出数と Mitigation の数が多いものを抽出しランサムウェア攻撃でもっとも利用される MITRE 攻撃テクニックの順位付けを行った。[10]

３.１.２：攻撃再現性スコアリングにおける評価パラメータの設定

スコア１

攻撃グループ、攻撃キャンペーン、攻撃に利用されるソフトウェアのそれぞれで過去に数多く使われた攻撃テクニック（本研究では「攻撃の再現性が高く、攻撃コストが低いテクニックほど脅威度が高い」と仮定し、この定義に基づきスコア１を危険度評価の基準とした。）

重み付け：50%

・具体的な算出手順

１）MITRE STIX2.0 より、Cloud Matrix 攻撃テクニック群の攻撃 G、キャンペーン、ソフトウェア（以降、３指標）の頻度回数を取得

２）３指標の頻度回数を５段階に分ける。（分位数による Bin 分割）

３）３指標の５段階レベルを求め、合計値を満点の１５で除算し、スコア１として 50%の重みづけでそれを攻撃再現性スコアリングとする。

・参照データ

実績ベース（観測頻度）の信頼性が高く、攻撃者も効果実証済みの手法を再利用する傾向があるため。特に APT グループは TTP（戦術・技術・手順）を固定化しやすい。観測頻度が高い＝再現性・汎用性が高い証拠になりえる。Red Canary[12]の年次脅威レポートでもこの視点が採用されている。

表５　CloudMatrix Initial Access 攻撃再現性スコアリング

MITRE ATT&CK TechniqueID	MITRE ATT&CK Technique Name	SPRE Threat Category	score1	score2	score3	score4	score5	Final score
T1190	Exploit Public-Facing Application	Initial Access	43.33%	20.00%	0	1	0.00%	63.33%
T1078.004	Valid Accounts: Cloud Accounts	Initial Access	23.33%	20.00%	0	1	0.00%	43.33%
T1566.002	Phishing: Spearphishing Link	Initial Access	43.33%	0.00%	0	1	0.00%	43.33%
T1189	Drive-by Compromise	Initial Access	36.67%	0.00%	0	1	0.00%	36.67%
T1078.001	Valid Accounts: Default Accounts	Initial Access	13.33%	20.00%	0	1	0.00%	33.33%
T1199	Trusted Relationship	Initial Access	13.33%	20.00%	0	1	0.00%	33.33%
T1566.004	Phishing: Spearphishing Voice	Initial Access	6.67%	0.00%	0	1	20%	26.67%

スコア２

利用者の構成ミスによっても同様に引き起こされる攻撃テクニック（MITRE には構成ミスの定義はないが、独自に調査を行い、スコアに反映した。Cloud Matrix の攻撃テクニック総数 135 のうち、56 存在した。

重み付け：20%

・具体的な算出手順

スコア２として利用者の構成ミスによっても同様に引き起こされる攻撃テクニックは、20%をスコア１に加算する。

・参照データ

クラウド環境では人的な設定ミスが最大のリスク源であると言われており Check Point Software Technologies Ltd.[12]の調査でもクラウド構成ミスによるクラウドインシデントを経験した企業は全体の 82%にのぼる）。にもかかわらず監視対象外となっていることが多く、顕在化しにくいが実は頻度が高いリスクと判断した。

スコア３

Mitigation が存在しないもの。（Mitigation/緩和策が存在しないものは、攻撃が成功する可能性が高く危険であるという定義にした。）

重み付け：10%

・具体的な算出手順

スコア３として当該攻撃テクニック MITRE の Mitigation がひとつも存在しないものは、10%としてスコア１+スコア２に加算する。

・参照データ

Rahman & Williams(2022)らは[13]、NIST SP800-53 の 298 のセキュリティコントロールが、MITRE ATT&CK に掲載されている 188 の攻撃テクニックのうち、53 技術には Mitigation がマッピングされておらず、実例で被害につながる高リスク技術であると述べられている。該当する攻撃テクニック数は Cloud Matrix の攻撃テクニック総数 135 のうち、14 存在しているため、10%のウェイトとした。

3 つのパラメータの重みづけを 1-0 間で計測し 3 つを加算した数値を比較し、数値の高い攻撃テクニックを再現率が高く、次回も再度、攻撃が発生する可能性が高いと判定した。

$$Score_{raw} = 0.5 \cdot F + 0.2 \cdot M + 0.1 \cdot N \quad (1)$$

ここで、F は MITRE ATT&CK における観測頻度（Normalized）、M は構成ミス関連のフラグ（0/1）、N は緩和策の不存在（0/1）を表す。

スコア４

Tactic が「Collection」「Discovery」「Persistence」に該当する場合、単体での攻撃影響が小さいことから、Score_raw を 1/2 に補正し、採用優先度を低下させた。

$$Score(adj) = 1/2 \times Score(raw) \quad (Tactic\text{が「}Collection\text{」「}Discovery\text{」「}Persistence\text{」の場合})$$
$$Score(raw) (\text{それ以外の場合}) \quad (2)$$

スコア５

さらに、頻度が 5 未満である新規攻撃に対しては、過小評価を防ぐため+0.2 の補正値を加算した（新興 TTP の検出困難性を加味）。一方でこの補正値を追加しない場合、過去の頻度数の多い境界防御型の攻撃テクニックが選定される懸念があるため、本補正値を採用している。
以下が、総合式になる。

$$Score\ final\ =$$
$$1/2\ \times\ (0.5\ \times\ F+0.2\ \times\ M+0.1\ \times\ N)+0.2$$
（Tactic 該当かつ $F<5$）
$$1/2\ \times\ (0.5\ \times\ F+0.2\ \times\ M+0.1\ \times\ N)$$
（Tactic 該当かつ $F\ \geqq\ 5$）
$$0.5\ \times\ F+0.2\ \times\ M+0.1\ \times\ N+0.2$$
（非該当かつ $F<5$）
$$0.5\ \times\ F+0.2\ \times\ M+0.1\ \times\ N$$
（非該当かつ $F\ \geqq\ 5$）

(3)

これらの重みは Red Canary（2023）[14] 等の TTP 出現頻度に基づき、観測頻度が危険度に最も強く影響することからスコア１を 50%を配分。スコア２の構成ミスはクラウドリスクの主要因であることから 20%、スコア３の緩和策なしは重大性を示すが限定的なため 10%と設定した。またスコア４（Tactic 補正）は、Collection・Discovery・Persistence といった攻撃準備段階の Tactic に対応する技術では、単独での重大インパクトが限定的である点を踏まえ、論理的に危険度を半減している。この認識は MITRE ATT&CK の公式説明においても示されている[15]。またスコア５については（頻度補正）は、過去 CTI 報告の分析において頻度の低い TTP が存在するにもかかわらずレビュー対象から除外されている傾向があるというデータも報告されている[16]。これにより、最新傾向もバランスよく反映した攻撃再現性の高いテクニックの選定となっている。なお、実際の頻度データの自動抽出には、MITRE ATT&CK Cloud Matrix の STIX データから各攻撃テクニックの出現回数をカウントする Python コードを用いた（Appendix 1 参照）。これにより、攻撃の再現性を客観的に評価できるデータ基盤を構築した。

３.１.３：IPA 方式の攻撃ステップに MITRE Tactics をマッピングし MITRE CloudMatrix から攻撃テクニックを選定する

図３、表６のように MITRE tactics を IPA 方式にマッピングさせるために 4 つの SPRE 方式攻撃ステップグループに分類し、名称を決めた。

この 4 分類は、MITRE ATT&CK の Tactic カテゴリの目的と攻撃フェーズ構造に基づき、初期アクセス～影響発現までの時間的連続性を反映するよう再整理したものである。

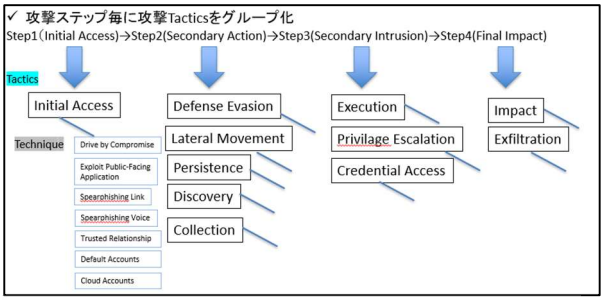


図３ IPA 方式の攻撃ツリーにマッピングされた MITRE 攻撃テクニック

表６　MITRE tactics、Technique と SPRE 攻撃ステップグループ

Step order No	TACTICS ID	TACTICS Name	Step Group(J)	Step Group(E)	リスクラベル
1	TA0001	Initial Access	初期侵入	Initial Access	高
2	TA0003	Persistence	二次アクション	Secondary Action	低
2	TA0005	Defense Evasion	二次アクション	Secondary Action	中
2	TA0007	Discovery	二次アクション	Secondary Action	低
2	TA0008	Lateral Movement	二次アクション	Secondary Action	中
2	TA0009	Collection	二次アクション	Secondary Action	低
3	TA0002	Execution	二次侵害行為	Secondary Intrusion	高
3	TA0004	Privilege Escalation	二次侵害行為	Secondary Intrusion	高
3	TA0006	Credential Access	二次侵害行為	Secondary Intrusion	高
4	TA0011	Command and Control	最終侵害行為	Final Impact	最も高い
4	TA0010	Exfiltration	最終侵害行為	Final Impact	最も高い
4	TA0040	Impact	最終侵害行為	Final Impact	最も高い

1. 攻撃ステップ４グループに対応した MITRE 攻撃テクニックのベスト４を選出した。この時点ではひとまずベスト４としたが、３.２の攻撃経路の最適化の際に改めてベスト４が最適なのかを検証する。
2. 図４の通り、MITRE Cloud Matrix の１３５の攻撃テクニックから攻撃再現性の高い１６の攻撃テクニックを選定した。

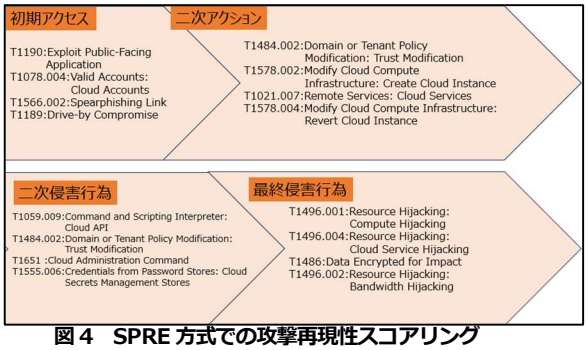


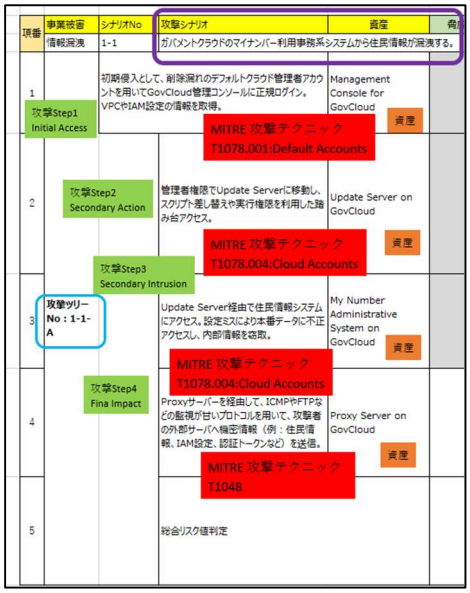
図４　SPRE 方式での攻撃再現性スコアリングにより選定された攻撃テクニック 16

3.

３.１.４：MITRE CloudMatrix の攻撃テクニックを標的となる資産と組み合わせる

最終的には表７のように IPA 方式の攻撃ツリーの攻撃ステップ毎に MITRE 攻撃テクニックをマッピングしていく。

表７　IPA 方式の攻撃ツリーを構成する攻撃ステップそれぞれに MITRE 攻撃テクニックとその標的になる資産をマッピングする



IPA 方式では攻撃テクニックがどの資産を標的として実施されるかを特定する必要がある。MITRE ATT&CK では資産という定義はないが、Platform という定義があり、それは Containers, ESXi, IaaS, Identity Provider, Linux, Network Devices, Office Suite, SaaS, Windows, macOS などが攻撃テクニックの標的になりうる Platform という定義がされている。これらを参考に IPA 方式の資産粒度に合わせて以下の資産名との組み合わせを策定した。

表８　MITRE Platform と IPA 方式資産

No	IPA方式_資産	MITRE Platform	No	IPA方式_資産	MITRE Platform	No	IPA方式_資産	MITRE Platform
1	Business Workstation	Windows	5	Wireless Access Point (LGWAN Network)	Network devices	9	GovCloud-Connected Firewall	Network devices
2	Management Console for GovCloud	Windows	6	Wireless Access Point (LGWAN Network)	Network devices	10	My Number Administrative System on Govcloud	IaaS
3	VDI Server	Vittualization	7	Internet-Connected Firewall	Network devices	11	Proxy Server on Govcloud	IaaS
4	VDI Auth server	Identity Provider,Network Devices	8	Internal LGWAN & Internet Network Intermediary Firewall	Network devices	12	Proxy Server on Govcloud	IaaS

３.２課題２：最適化攻撃ツリーの生成手法

3.1 で攻撃テクニック数のすべての組み合わせを頻度分析に基づく攻撃再現性スコアリングにより絞り込んだが、新たに攻撃テクニックの標的になる資産を取り決め、その組み合わせを策定した。その結果、絞り込んだ攻撃テクニックは資産との組み合わせにより改めて構成されるため攻撃ツリーは再度倍増することになる。

どの程度まで攻撃経路数を策定しリスクアセスメントを実施すべきなのか。これもリスク分析者を悩ませる課題である。攻撃ステップ数を絞れれば、攻撃経路数が減少する。しかしシステム構成や環境によっても攻撃経路は変わってくる。ここではもっとも事業被害レベルが高い重要資産に対する脅威を想定し指数関数的な組み合わせの爆発を抑制しながら最適化された攻撃ツリーを生成する手順を提案する。

３.２.１初期アクセス攻撃手口のなりすまし限定化

今回のリスク分析対象は自治体のゼロトラスト環境である。

ゼロトラスト環境下でもっとも恐れる脅威は何か？ゼロトラスト・アーキテクチャでは、ID ベースの認証や MFA、リスクベース認証等によりセッションの信頼性を確保しているが、Impersonation-as-a-Service（IMPaaS）の台頭により、正規ユーザになりすますことでゼロトラストの前提を根底から破壊する攻撃が実現可能となっている。Campobasso らの研究[17]では、IMPaaS によりリスクベース認証を含む高度な認証も回避可能であることが示されており、ゼロトラストの最大の弱点のひとつに、なりすましへの脆弱性が含まれることは確かである。

本研究ではゼロトラスト環境におけるなりすまし攻撃を前提とする。このことにより、潜在するリスクをあぶりだし、本来対処すべき対策を導出することが可能になる。

もうひとつのメリットとしては、対象となる資産を絞り込むことができる点だ。

このことにより当初、表８にあった標的資産のうち、ネットワークデバイスに相当するファイアウォール・無線 AP・ネットワークスイッチ等の経路上の標的資産を表９のように除外できた。

以下を前提に攻撃ルートを絞り込んでいく。

表９　なりすましを想定した資産の選定

No	IPA方式_資産	MITRE Platform	No	IPA方式_資産	MITRE Platform	No	IPA方式_資産	MITRE Platform
1	Business Workstation	Windows	5	~~Wireless Access Point (LGWAN Network)~~	~~Network devices~~	~~9~~	~~GovCloud-Connected Firewall~~	~~Network devices~~
2	Management Console for GovCloud	Windows	6	~~Wireless Access Point (LGWAN Network)~~	~~Network devices~~	5	My Number Administrative System on Govcloud	IaaS
3	VDI Server	Vittualization	~~7~~	~~Internet-Connected Firewall~~	~~Network devices~~	6	Proxy Server on Govcloud	IaaS
4	VDI Auth server	Identity Provider,Network Devices	~~8~~	~~Internal LGWAN & Internet Network Intermediary Firewall~~	~~Network devices~~	7	Proxy Server on Govcloud	IaaS

３.２２攻撃ステップ数の策定方法

攻撃ステップ数や攻撃テクニック数を絞れれば、攻撃経路数が減少する。しかしシステム構成や環境によっても攻撃経路は変わってくる。様々な文献や脅威レポートを調査した中では、ORCA Security の 2022 年の脅威レポート[18]で典型的なクラウド攻撃では、攻撃者がクリティカル資産に到達するまでに必要なステップ数は平均で 3 ステップ程度という実証データや実在する攻撃者グループの手口を用いて各種セキュリティ製品の検知能力を第三者機関（MITRE

Corporation）が評価する国際的なベンチマークプログラムである MITRE ATT&CK Evaluation[19]によると Enterprise2024 の攻撃グループ Lock Bit は 19 のセキュリティベンダーにより検知された攻撃ステップ数は 8 ステップであるという結果が出されていた。一意に攻撃ステップ数を決めることは困難なため、著者らは攻撃ステップ数については、IPA 方式が推奨している 20～100 の範囲に収まる数から逆算して最適な攻撃ステップ数を算定した。前提条件としては、IPA 方式で推奨している正規ユーザにおいて通信が確立しているものを優先して攻撃ルート数（＝攻撃ツリー数）を算出した。([2]p204)

任意の資産が侵害されると通常時通信が確立していない経路が新たに追加発生する可能性があるがその場合は攻撃コストが高くなるため、今回はそのケースは除外して試算を行った。

３．２．２．１ 攻撃ステップ数が 4 段階の場合における検討

正規ユーザが通信を確立している攻撃ルートに限定することで一つのシナリオについて 64 の攻撃ツリー数になった。
攻撃ステップ 1：攻撃テクニック数 1
攻撃ステップ 2：攻撃テクニック数 4
攻撃ステップ 3：攻撃テクニック数 4
攻撃ステップ 4：攻撃テクニック数 4
1×4×4×4＝64

３．２．２．２ 攻撃ステップ数が５段階の場合における検討

正規ユーザが通信を確立している攻撃ルートに限定したとしても、一つのシナリオについて 256 の攻撃ツリー数になり、IPA 方式が推奨している 20～100 の範囲を超えた攻撃ツリー数になった。
攻撃ステップ 1：攻撃テクニック数 1
攻撃ステップ 2：攻撃テクニック数 4
攻撃ステップ 3：攻撃テクニック数 4
攻撃ステップ 4：攻撃テクニック数 4
攻撃ステップ 5：攻撃テクニック数 4
1×4×4×4×4＝256

攻撃テクニック数、攻撃ステップ数含めた、上記シミュレーションの結果、今回は IPA が推奨する範囲内になる攻撃ステップ数 4、攻撃テクニック数 4 が最適と判断を行った。

３.２.３攻撃シナリオの策定方法

もっとも機密度の高い資産であるガバメントクラウド上のマイナンバー利用事務系システムと位置づけ、「ガバメントクラウドのマイナンバー利用事務系システムが侵害される。」と定義を行い、１）で取り決めたなりすましの攻撃テクニックを策定していく。

以下、攻撃テクニックになりすましを前提として標的になりうる資産を選定していく。

・シナリオ A での初手の攻撃テクニックと標的資産：T1078.004-Valid Accounts: Cloud Accounts
（ガバメントクラウド管理者アカウントの漏洩）

・シナリオ B での初手の攻撃テクニックと標的資産：T1190-Exploit Public-Facing Application
（業務端末から VDI 認証装置を介した認証バイパスによる既知の脆弱性攻撃）

・シナリオ C での初手の攻撃テクニックと標的資産：T1189- Drive-by Compromise（業務関連情報を取得・更新する際、標的管理者がアクセスする Web サイト/ポータルが改ざんされており、閲覧/ダウンロードしただけでマルウェアに感染。）

・シナリオ D での初手の攻撃テクニックと標的資産：T1566.002-Phishing:Spearphishing Link
（業務端末から phishing link にアクセス）

３.２.４攻撃テクニックと資産の組み合わせ数の策定

攻撃ステップの１は以下の攻撃テクニックと資産の組み合わせになる。

表 10:Step1:初期アクセス

攻撃テクニック ID	割当資産
T1078.004	Management Console for Govcloud
T1190	VDI Auth Server
T1189	Management Console for Govcloud
T1566.002	Business Workstation

Step1 における攻撃テクニックと資産の組み合わせについて
Step1 の組み合わせ総数は 4 ペアである。
※初手の攻撃テクニックのみ、標的資産を限定した。そのため攻撃テクニックと資産の組み合わせが固定化され、組み合わせ数は 4 となる。

攻撃ステップ２は以下の組み合わせになる。

表 11:Step 2: 二次アクション

攻撃テクニック ID	割当資産
T1484.002、T1578.002, T1021.007, T1578.004	VDI Server,,VDI Auth Server,Business Workstation,Management Console for Govcloud,My Number Administrative System on Govcloud,Update Server on Govcloud ,Proxy Server on Govcloud

Step2 における攻撃テクニックと資産の組み合わせについて
Step2 の組み合わせ総数は 28 ペアである。

表 12:Step 3: 二次侵害行為

攻撃テクニック ID	割当資産
T1059.009, T1484.002, T1651, T1555.006	VDI Server,VDI Auth Server,Business Workstation,Management Console for Govcloud,My Number Administrative System on Govcloud,Update Server on Govcloud ,Proxy Server on Govcloud

Step3 における攻撃テクニックと資産の組み合わせについて
Step3 の組み合わせ総数は 28 ペアである。

表 13:Step 4: 最終侵害行為

攻撃テクニック ID	割当資産
T1496.001, T1496.004, T1486, T1496.002	My Number Administrative System on Govcloud, Proxy Server on Govcloud

Step4 における攻撃テクニックと資産の組み合わせについて
Step4 の組み合わせ総数は 8 ペアである。

ゆえに、総組合せ数は以下で表される。

組み合わせ総数= 4 ×28 ×28 ×8 = 25,088

これは、ネットワーク理論における有向非巡回グラフ（DAG: Directed Acyclic Graph）[20]上でのパス列挙問題と同等であり、現実的には通信経路や資産制約によって成立し得ないルートも多数含まれる。

３.２.５通信確立ルートへの限定と攻撃パスの最適化

本研究では、通常時に通信が確立された攻撃コストの少ない攻撃ルートを対象とする。これは IPA 方式が推奨している攻撃コストが低い正規のデータフローが存在するルートをまずは選定すべきであるという主張によるものである。([2]p204)

通信整合性の判定には、stepwise_techniques_assets.xlsx および通信ルート定義 CSV を用い、各ステップの資産ノードが実際に双方向通信関係を持つ場合のみ有効なルートと判定した。
このような通信ルートの前提条件を導入することで、攻撃ツリーの通過可能なパス集合 P’ は、全組合せ P の部分集合として以下のように再定義される。

$$|P| = 4 \times 4 \times 4 \times 4 = 256 \qquad (4)$$

ここで、元々の 25,088 通りの組合せは、今回のリスク分析対象の自治体のゼロトラスト環境において、危険性の高い経路 256 通りにフィルタされ、さらに通信確立済の経路は 1 シナリオにつき、4 ステップの 64 通りに絞り込まれる。これにより、4 つの異なるシナリオ（例：T1078.004, T1566.002 等による初期侵入）それぞれに 64 通りずつの通信確立攻撃パスを構成し、網羅的かつ現実的な攻撃シナリオ分析が可能となった。
なお、本研究で最終的に抽出された 4 ステップ 64 通りの攻撃パスは、IPA 方式における 1 シナリオあたりの想定パス数（おおむね 20〜100 通り）とも整合する範囲内にあり、実運用上の評価粒度としても妥当性が確認された。結果として、本手法は理論的な攻撃グラフ構築と実務的な適用可能性の両立を実現している。通常通信が確立された正規経路上に限定して攻撃パスを抽出するための具体的な処理例については、Appendix 2 に本研究で用いた Python コードを付録した。NetworkX ライブラリを活用し攻撃グラフを有向グラフとして実装することで、実データに基づき、効率的に高リスクな攻撃経路を抽出した。今後のリスク分析の再現性と実装容易性に活用できる。

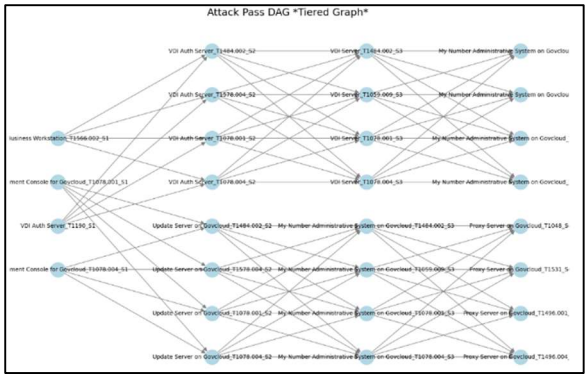


図 5 DAG による 256 攻撃パスのグラフ化

３.３攻撃ステップ毎の攻撃再現率および対策有効率を反映しリスク算定する段階伝搬型リスク評価モデル

現状の IPA 方式に基づくシナリオベースのリスク評価は、攻撃シナリオの各ステップにおける脅威・脆弱性/対策の効果を、事業被害レベルに応じて定数的に結合したリスク値として一括して評価する「定値結合型」モデルである[表３]。この手法では、たとえばあるステップが十分な対策が講じられていなかったとしても、複数あるうちの他のステップで高度な対策が講じられていればその対策が当該シナリオ全体の対策として採用され、その結果、全体とし…攻撃ステップごとのリスク値をシナリオ全体としてのリスク値に反映できていない IPA 方式のリスク値算出法がその理由と考える。これを解決するため本研究では、「段階伝播型リスク評価モデル（Stepwise Propagated Risk Evaluation Model）」を提案する。IPA 方式の攻撃ツリーは攻撃シナリオに基づいて、第三者からの攻撃を

攻撃ステップを踏んで最終標的資産を攻略していくために策定する。SPRE 方式は各ステップのリスク値を個別に算出する。各ステップのリスク値は、攻撃再現率（Prevalence 以降 P）、対策有効率（Mitigation Effectiveness 以降 M）、および直前の攻撃ステップの残存リスク値により算定される。攻撃ステップのリスクは逐次的に進行するものであり、後続ステップのリスクは前段階の攻撃の残存リスク値によって変化する。この構造により、リスクはステップ間で逐次的に伝播され、現実の攻撃連鎖を反映する形で評価が可能となる。各ステップのリスク値を連続的に乗算することで、攻撃ツリー全体の残存リスク値を算出する。この構造は、履歴全体ではなく直前の攻撃ステップの残存リスク値に依存して評価されるという性質を持ち、攻撃連鎖における構造的依存性を反映するモデルとなっている。

３.３.１評価モデル構成要素

段階伝播型リスク評価モデルは各攻撃ステップにおけるリスク値 (R_i)を以下の式で定義する：

各ステップのリスクは、その直前のステップの残存リスクに 1 を加えた形で乗算される。

これにより、前段階のリスクが高いほど、次段階のリスクが指数的に増加する構造を持つ。

この数式の考え方は Muñoz ら[21]が用いた Loopy Belief Propagation（LBP）モデルと類似する「依存型伝播構造」に基づいている。

$$[R_1 = P_1 \cdot M_1]$$
$$[R_2 = P_2 \cdot M_2 \cdot (1 + R_1)]$$
$$[R_3 = P_3 \cdot M_3 \cdot (1 + R_2)]$$
$$[R_4 = P_4 \cdot M_4 \cdot (1 + R_3)]$$
$$[R_{total} = R_4] \quad (5)$$

(P_i)：攻撃再現率（Prevalence）
（攻撃テクニックに対する再現性スコア）

(M_i)：対策有効率（Mitigation Effectiveness）

(R_i)：各攻撃ステップの残存リスク

この構造は、前段階のリスク値を次段階の係数として乗算するものであり、攻撃の連鎖性と影響の伝播性を数学的に表現する。

本稿におけるP_iは、MITRE ATT&CK Cloud Matrix におけるテクニックの観測頻度を基に、攻撃再現性を定量化したスコアであり、厳密な意味での発生確率とは異なる。ただし、過去の採用実績が高いテクニックは、攻撃者にとって再利用しやすく、将来的にも採用される可能性が高いという実務的仮定に基づき、本研究では攻撃成功確率の代替指標として適用した。

３.３.２ステップ毎のリスク値

・攻撃再現率（Prevalence）

３.１.２で Cloud Matrix から攻撃再現性の高い攻撃テクニックを選定する際に活用した攻撃再現性スコアリングをここでも活用する。

MITRE ATT&CK Cloud Matrix に含まれる 135 の攻撃テクニックを対象にスコア１～５を採用

$$Pi = \begin{cases} 1/2 \times (0.5 \times F + 0.2 \times M + 0.1 \times N) + 0.2 & \text{（Tactic 該当かつ } F < 5\text{）} \\ 1/2 \times (0.5 \times F + 0.2 \times M + 0.1 \times N) & \text{（Tactic 該当かつ } F \geqq 5\text{）} \\ 0.5 \times F + 0.2 \times M + 0.1 \times N + 0.2 & \text{（非該当かつ } F < 5\text{）} \\ 0.5 \times F + 0.2 \times M + 0.1 \times N & \text{（非該当かつ } F \geqq 5\text{）} \end{cases} \quad (6)$$

・対策有効率（Mitigation Effectiveness）

$$Mi = 1 - (\text{"5 段階評価"} \times 0.2) \quad (7)$$

上記規定類の推奨項目は対策として実施している前提に基づき、対策有効率を 5 段階で評価する。

本研究では、

- 総務省地方公共団体における情報セキュリティポリシーに関するガイドライン（令和 7 年 3 月版）[22]
- デジタル庁ガバメントクラウド利用システムにおけるセキュリティ対策（共通）2023/03/27 公開[23]
- 総務省クラウドの設定ミス対策ガイドブック 2024 年 4 月[24]

に記載された対策要件を遵守している仮想の自治体を想定し、対策レベルを評価した。

本研究では、自然言語処理モデルである Sentence-BERT（SBERT[25]）を活用し MITRE ATT&CK テクニックの説明文と、総務省・デジタル庁の PDF ガイドラインに記載された対策文書との文脈的な意味類似度を評価し、その類似度に応じて対策成熟度（M）を定量化する試みも行った。

たとえば、クラウドアカウントの乗っ取り（T1078.004）に対して、総務省ガイドライン中に「多要素認証の強制適用」や「アカウント使用履歴のモニタリング」が明記されている場合、SBERT により高い類似度（0.85 以上）が得られ、M=5（最大対策）と判定された。

センテンスのマッチング精度の悪い場面には、人為的にドキュメントを読み込み、修正を行った。

クラウドアカウントの乗っ取り（T1078.004）に対して、総務省ガイドライン中に「多要素認証の強制適用」や「アカウント使用履歴のモニタリング」が明記されている場合、SBERT により高い類似度（0.85 以上）が得られ、M=5（最大対策）と判定される。

センテンスのマッチング精度の悪い場面には、人為的にドキュメントを読み込み、修正を行った。（Appendix3 参照）

３.３.３SPRE 方式の数学的基盤と先行研究との比較

本研究で提案する SPRE（Stepwise Propagated Risk Evaluation）方式は、「各攻撃段階のリスク値が前段階のリスク値を係数として段階的・連鎖的に伝播する」という伝播型リスク評価構造に基づいている。このアプローチは、情報セキュリティの枠を超え、他分野の伝統的数理モデルとも強い構造的類似性が認められる。

相原らの EDC 法におけるイベントツリー分析の乗算・最終加算の構造を図 6 に示す[26]。

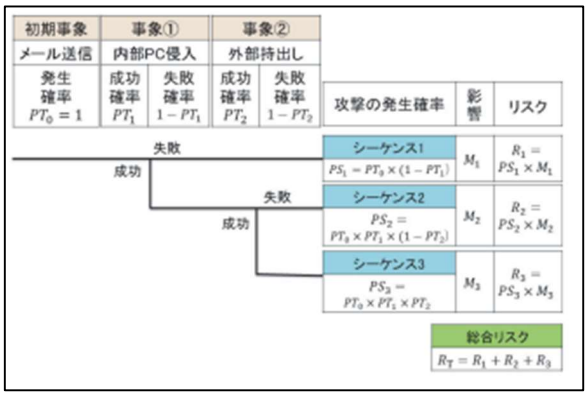


図 6 EDC 法におけるイベントツリー分析のシーケンス[26]より引用。

イベントツリー分析では、各攻撃ステップにおいてイベントの成功率・失敗率を乗算で逐次的に計算し、ステップごとにリスク額を個別に算出する。最終的なトータルリスク（残存コスト）は、各シーケンスでの「発生確率×損害額」を加算して求められる（例：R1+R2+R3）。

それに対して SPRE 方式は連鎖乗算による累積方式を採用している[表 14]。

表 14 SPRE 方式が採用している連鎖乗算式

シナリオ B/攻撃ステップ	攻撃手口	標的資産	想定 MITRE Technique ID	実施対策、緩和度およびデジタルガイドライン適守レベル	攻撃再現性 (Pi)	実施対策/5段階評価 (Mi)	残存リスク(Ri)	リスク値/5段階評価（以下は設定）
1	外出先の職員端末の認証ゲイトウェイの脆弱性を悪用して認証バイパスし庁内ネットワークに初期侵入する。	VDI Auth Server	T1190	脆弱性管理、EDR,SASE,WAF,ZTNA導入済	P1	M1	R1=P1*M1	1:極めて低い
2	クラウド認証で使用されるIAMトークンやAPIを盗み、正規ユーザとして再ログイン	VDI Auth Server	T1584.004	MFA,Role-base AccessControl,Cloud Trail導入済	P2	M2	R2=P2*M2*(1+R1)	2:かなり低い
3	クラウドAPIを悪用し、スクリプトでクラウド環境へ不正指令を送信	VDI Server	T1059.009	CloudTrail, CSPM,SIEMを利用した常時監視	P3	M3	R3=P3*M3*(1+R2)	2:かなり低い
4	マイナンバー利用事務系にマルウェアを侵入させ業務データを暗号化し、利用不能状態を強制	My Number System	T1486.004	IAM最小権限、API監査、CSPM導入済	P4	M2	R4=P4*M4*(1+R3)	1:極めて低い

SPRE 方式では「攻撃再現率 P」と「対策有効率 M」をその都度乗算し、各ステップの残存リスクを導出する。さらに SPRE では、前の攻撃ステップの残存リスク（1 にリスク減少分を加味した値）を掛け合わせることで、一連の攻撃フロー全体のリスク連鎖を再現している。この枠組みはイベントツリー分析の「パスごとの乗算的リスク累積」と本質的に同様の思想に基づくものであり、違いは加算か乗算かという計算構造の差にある。

SPRE 方式では、攻撃フローの各段階でリスクが減少・蓄積される様子を逐次的かつ定量的に評価できるのが特徴であり、最終的な残存コスト集計では各経路ごとではなく、全体フローの掛け算を通じて包括的なリスク評価が可能となる。

先行研究との比較においては、Muñoz-González ら[21]の Loopy Belief Propagation（LBP）を用いたベイジアン攻撃グラフでは、各ノードのリスク（あるいは成立確率）は「直前ノードの条件付き確率」に依存して動的に伝播・更新される構造となる。これにより攻撃パスの連鎖的成立や累積的危険度が可視化される。この「前段階値に依存した積み上げ構造」は、SPRE モデルで定義する

$$R\,n+1 \;=\; R\,n \;\times \text{各段階のスコア} \tag{8}$$

という乗算的伝播形式と本質的に近似している。

Kermack‐McKendrick の SIR 疫学モデル[27]や Acemoglu ら[28]の経済ネットワーク・ショック伝播モデルや CVSS v4.0[29]もまた、伝播型数式でモデル化している。

表 15 SPRE モデルと LBP モデル、疫学モデル数式の比較

モデル名	数式構造例	伝播構造	説明
LBP (Muñoz)	$\mu i \to j = f(\mu k \to i)\mu_{i\to j} = f(\mu_{k\to i})$	ベルマン型伝播	前ノードの信頼度・確率が次ノードへ反映
疫学 SIR モデル	$It+1 = It + \beta \cdot St \cdot It I_{t+1} = I_t + \beta \cdot S_t \cdot I_t$	感染者 × 感受性 × 接触頻度	前段階が強く次に影響
経済ネットワーク	$S_{n+1} = S_n \times$ 伝播係数	「前段階 × 伝播係数」という積型構造	サプライチェーン等ネットワーク上のショック伝播
Ahmed et al.	Risk = LO × MoI × EoE	条件付き伝播（機会・環境・前進達成値）	前段階の成立度や目的達成度が次段の攻撃伝播を決定、MITRE TTP と資産依存の累積型
SPRE モデル（本論）	$Ri = Pi \cdot Mi \cdot (1 + Ri - 1)R_i = P_i \cdot M_i \cdot (1 + R_{i-1})$	段階的な残存リスク乗算的伝播	前段階リスクが次に影響する新規構造

SPRE 方式の独自性は、理論的な確率モデル（LBP や Ahmed 方式）の枠組みを応用しつつも、現場で実運用可能な多軸リスクスコア（攻撃再現性・頻度・検知困難性・対策有効性など）を統合できる柔軟性と、攻撃段階ごとに粒度細かくリスク値を評価・可視化できる点にある。このことにより、説明責任やパラメータ調整・再評価のしやすさ、実務での意思決定支援力において従来モデルよりも高い適用性・合理

性を実現可能にした。上記の共通項としてはいずれも段階伝播型（積み上げ型）の数理構造である点であるが、SPRE 方式の新規性・有用性は、従来の確率論モデルや数理伝播モデルの枠組みを活かしつつも、「再現性・頻度・検知困難性・対策実効性」等、現場で真に意味のある多軸リスク評価要素を柔軟に導入している点である。

以上により、SPRE 方式は他分野の伝播理論とも親和性を持ちつつ、“情報セキュリティ現場のために進化・最適化された次世代型リスク伝播モデル”であり、学術的基盤と実務応用性との両立を実現する。

4.検証と評価

4.1課題1

IPA 方式の脅威セットは非常に広義の定義になっており、その脅威をどのような攻撃手口で実行していくかを検討していかなくてはならない。今回採用した MITRE ATT&CK の攻撃テクニックはその攻撃手口が粒度が細かく、より具体的で実践的な事例が豊富なため、IPA 方式のシナリオベースのリスク分析の際のサイバーキルチェーンモデルをイメージしやすいため非常に攻撃の組み立てがしやすい。特に今回のゼロトラスト環境に最適な Cloud Matrix から攻撃テクニックを採用しているため攻撃者目線での攻撃攻略戦略を立てやすい。そのため、MITRE の攻撃テクニックをそのまま各ステップに組み合わせるだけで、攻撃ツリーがそのまま完成可能である。IPA 方式と比較して攻撃ツリーの策定に時間を要することは少なかった。そのためリスク分析者はかなりの工数が削減できる。

そのためリスク分析者はかなりの工数が削減できる。

表 16 IPA 方式と MITRE の脅威の粒度の比較

観点	IPA方式（脅威セット例）	MITRE ATT&CK方式（テクニック例）
粒度	粗い・包括的	細かい・ピンポイント
脅威名	不正アクセス※今回のCloud Matrix135の攻撃手口のうち、50以上がこの不正アクセスに該当した。	T1190 Exploit Public-facing Application T1078 Valid Accounts 等
内容	脆弱性悪用、アカウント漏洩、公開サーバ侵害、脆弱認証設定、etc.	各攻撃手口ごとに詳細に定義されているため、そのままIPA方式の攻撃ステップ毎の攻撃内容に記載可能。（例：公開アプリ脆弱性攻撃、デフォルトアカウント利用など）
利用時の具体性	複数の攻撃手法を一括でカバーし抽象度が高い	そのまま攻撃シナリオやキルチェーンの攻撃ステップに利用できる
攻撃の組み立て	個別の手口を分解し自分で“攻撃経路”を想定する必要あり	公式技術名で“どの手口か”明確、ストーリーが組みやすい
分析負荷	不正アクセスを「どのような攻撃手口で？」を検討しなければならない。→具体化の工数が高い	具体的な例えばどのような攻撃手口がありなどと具体事例が豊富なため、攻撃をイメージしやすく、そのまま攻撃ステップ毎の攻撃ストーリを組み立て安い。

4.2課題2

攻撃ツリーの組み合わせの爆発を抑制し、経路組合せ生成と通信制約によるフィルタを実装し、リスク分析者へ攻撃ツリー策定の最適解を実現した。これにより、分析者の主観やスキル差に依存せずに、効率的に攻撃パスを可視化することが可能となった。実施した Python コードは Appendix2 に添付している。

4.3課題3

IPA 方式と SPRE 方式とのリスク算定結果を表 17 に示す。

表 17　IPA 方式と SPRE 方式リスク値算定結果

ステップ毎リスク値		低← IPAリスク →高			低← SPREリスク →高				
		A	B	C	Level1	Level2	Level3	Level4	Level5
シナリオA	Step1			100%	100%				
	Step2			100%	100%				
	Step3			100%	75%	25%			
	Step4			100%	100%				
シナリオB	Step1		100%		100%				
	Step2		100%		75%	25%			
	Step3		100%		50%	50%			
	Step4		100%		100%				
シナリオC	Step1			100%	100%				
	Step2			100%	50%	25%	25%		
	Step3			100%	18%	44%	38%		
	Step4			100%	36%	63%	1%		
シナリオD	Step1			100%	100%				
	Step2			100%	25%	75%			
	Step3			100%	50%	50%			
	Step4			100%	100%				

IPA 方式では攻撃ツリー全体のリスク値のみの算定になり、その攻撃ツリーに内在しているリスクが可視化できない。一方で SPRE 方式ではリスク値が攻撃ステップ毎に可視化可能であり、攻撃ステップ毎の検証も可能である。

IPA 方式は、攻撃ツリー内の複数の攻撃ステップの脅威に対する対策が最も成熟度の高いレベルが選択されるため、シナリオ A,B,C,D すべての攻撃ツリーの対策は 3 となり、脆弱性は 1 となった。事業被害レベルは 3、脅威は 3 となり、結果リスク値はシナリオ B 以外は C になった。シナリオ B は T1190-Exploit Public-Facing Application（業務端末から VDI 認証装置を介した認証バイパスによる既知の脆弱性攻撃）の脆弱性関連のため、運用面の課題も懸念としてあり、脅威レベルが一段上がり 3 になったため、リスク値は B という結果になった。

攻撃ステップによっては対策要レベルの 1 も散在されたが、IPA 方式ではそれが水面下に見えなくなってしまうのが大きな欠点といえる。

SPRE 方式は、5 段階評価になっており、その数字の分布は以下、表 18 の通りである。

表 18　SPRE 方式リスク値分布

SPRE方式	
リスクスコア範囲	5段階評価
0.00～0.19	Level1：極めて低い
0.2～0.39	Level2：かなり低い
0.40～0.59	Level3：中程度
0.6～0.79	Level4：やや高い
0.8～1.00	Level5：高い

SPRE 方式のリスク値算定結果は、表 16 の通りであるが、シナリオ A では、Step3 において、5 段階のリスク値のレベル 2 を 16 件が該当した。攻撃テクニック ID は T1059.009 であり、対象資産は My Number Administrative System on GovCloud であった。この攻撃は Cloud API 経由でスクリプトを実行しバッチ改ざんや設定変更を行うもので、API は攻撃者と正規ユーザの見分けが難しい。AWS でいう、CloudTrail,などで API 利用のログを監視し、UEBA や SIEM、SOAR などで相関分析を行うことも重要になる。

シナリオ B では Step2 においてリスク値レベル２で T1578.004（クラウド認証で使用される IAM トークンや API キーを盗み出し、正規ユーザになりすまし再ログインする攻撃）が資産対象 VDI Auth Server で 16 件該当した。この攻撃の対策は EDR の振る舞い検知では完全に検知は困難で GPO 改変については即時検知はほぼ困難なため最小権限を管理徹底したうえで早期検知、対処が重要になる。

また Step3 において T1059.009 が、資産対象 VDI Server で 16 件該当し、同時に T1484.002（クラウドテナントまたは AD ドメインのグループポリシーを変更し、ログ記録停止・ツール使用許可など攻撃者に有利な構成変更を実施する攻撃）も資産対象 VDI Server 16 件該当した。

シナリオ C については Step2 においてレベル２で T1482.002 が資産対象 Update Server on GovCloud で 16 件、T1578.004（仮想マシンを過去の脆弱なバージョンに戻す攻撃で資産対象 Update Server on GovCloud で 16 件該当した。Step3 において、レベル２で T1059.009 が 16 件、T1484.002 が 16 件該当した。

シナリオ D については Step2 において、T1484.002（攻撃者は VDI 認証環境のクラウド ID 基盤（資産対象:VDI Auth Server）に対し、信頼設定や条件付きアクセスルールを不正に変更）が 16 件、同様の資産対象で T1578.004 が 16 件が該当した。Step3 において T1059.009 が資産対象 VDI Server で 16 件。T1484.002 が 12 件、レベル２に該当した。さらにレベル３（リスク中程度で本リスク分析対象攻撃ステップのうちもっとも高いリスク値）の該当が発覚した。攻撃手口は資産対象 VDI Server で上述の T1484.002 であるが残存リスク値としては 42%を計測した。このリスク値が高まった理由は、管理者権限奪取後のポリシー改変はログ改ざんが伴えば特定困難な点にある。すでに対策として実施されていることは GPO 変更検知／管理者操作ログ記録とアラート設定、クラウド ID 基盤の権限管理、設定変更検知、MFA 導入 EDR、メールセキュリティ、標的型攻撃訓練などであるが、さらなる追加対策としてはリアルタイム遮断、改ざん耐性ログ、Just-In-Time 権限/Dual Control、自動復旧、証跡保全等の実施があげられ、それらの追加対策を検討することになる。

SPRE 方式では攻撃ツリー全体のリスク値のみならず、それぞれのステップ毎のリスク値も可視化できるため、早めに危険の兆候になりえるシグナルに気づき、中長期的な視点からの対策を検討することが可能になる。

また、本研究で設定した攻撃再現性スコアの各重み（観測頻度・構成ミス・緩和策有無等）について、パラメータを±5%の範囲で感度分析を実施したが、最終的に選定される攻撃テクニックの組み合わせおよびリスク値への影響はごくわずかであり、実務上問題となるレベルの変動はなかった。

本研究では、IPA 方式のシナリオベースのリスク分析に内在する３つの課題に着目し、第 1 の課題である「攻撃者視点での攻撃テクニックの選定」については MITRE ATT&CK の知識ベースである STIX2.0 データを活用して頻度分析により攻撃再現性の高い攻撃テクニックの選定がリスク分析者が迷うことなく行える。次に攻撃ツリーの組み合わせの爆発を抑制し、ネットワークグラフ理論を応用してリスク分析者へ攻撃ツリー策定の最適解を実現した。これにより、分析者の主観やスキル差に依存せず、網羅的かつ効率的に攻撃パスを可視化することが可能となった。

第３の課題である「動的伝搬リスクを算定し連鎖するリスクをいかに次ステップや最終リスク値に反映させるかに対しては、攻撃再現性確率と対策有効率の掛け算によるステップ毎のリスク値にステップ間の遷移に際して、前段階のリスク値が次段階の攻撃再現性を高める要因を導出する手法を構築した。IPA 方式では見えてこない攻撃ステップ毎のリスクが可視化されるため、速やかに対策の検討を開始できる。

５おわりに

本稿では、地方公共団体が 2030 年に向けて取り組んでいるゼロトラスト環境に移行する際のリスクを、シナリオベースで可視化・定量化する手法として、ゼロトラスト環境における MITRE ATT&CK Cloud Matrix に基づく段階伝播型リスク評価モデルを提案した。

IPA 方式のシナリオベースのリスク分析では、実務においてリスク分析者が攻撃手口を検討する必要がある点や攻撃ツリー策定時の工数発生による負荷の増加、サイバー攻撃特有の段階を踏んで伝搬するリスク値が適正に測れないといった課題を抱える中で、本研究の提案手法は、攻撃再現性スコアリングやネットワークグラフ理論を活用して攻撃ツリーの爆発を抑制してその適正数を生成する手法や、攻撃ステップ毎に前の攻撃が成功した場合に次の攻撃の危険性が高まる伝搬型リスクを測定可能なリスク算定法を提案し、実務適用に耐えうる改善点を組み込んでいる。

今回は攻撃経路を絞ることを行い、IPA 方式の人為的にも可能な範囲での可視化を行い、専門知識がなくとも誰でもリスク分析ができるというポリシーを踏襲したが、今後はプログラム等を利用して多くの脅威データを最適化せずにそのまま採用して、将来の脅威の予測や AI を活用した自動化による各種パラメータ値を算定することなどの研究も実施していく。さらにはリスク診断エンジンへの応用、ガバメントクラウド運用監視の一助となるゼロトラストの弱みである“なりすまし”時の脅威の仕組みの研究とそれに対峙可能な高度な対策の検証、さらには全国自治体への実装・展開可能な全体最適型サイバーセキュリティ評価フレームワークの確立に役立てる研究を目指していく。

謝辞
今回の研究にあたり、IPA 方式の考え方などについて詳細なアドバイスを INJANET（株）の福原聡氏、木下仁氏に頂戴した。謹んで感謝の意を表する。

参考文献

[1] NISC サイバーセキュリティ 2025（2024 年度年次報告・2025 年度年次計画）
https://www.nisc.go.jp/pdf/policy/kihon-s/250627cs2025.pdf
2025 年 7 月 12 日アクセス

[2] IPA 制御システムのセキュリティリスク分析ガイド 第 2 版
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html#section10
2025 年 6 月 5 日アクセス

[3] 令和 7 年度 国・地方ネットワークの将来像の実現に向けた検証事業の採択案件について
https://www.digital.go.jp/news/705bfd57-6780-48fe-983e-616e1da90a3c
2025 年 6 月 26 日アクセス

[4] 「国・地方ネットワークの将来像及び実現シナリオに関する検討会」
https://www.digital.go.jp/councils/local-goverments-network
2025 年 6 月 26 日アクセス

[5] MITRE ATT&CK Cloud Matrix
https://attack.mitre.org/matrices/enterprise/cloud/
2025 年 6 月 21 日アクセス

[6] MITRE ATT&CK
https://attack.mitre.org/
2025 年 6 月 21 日アクセス

[7] MITRE ATT&CK “enterprise-attack_V17.1.json”
https://github.com/mitre/cti/tree/master/enterprise-attack
2025 年 6 月 21 日アクセス

[8] Hardik Monocha, , Akash Srivastava, Chetan Verma, Ratan Gupta, Bhavya Bansal,Security Assessment Rating Framework for Enterprises using MITRE ATT&CK Matrix
https://arxiv.org/abs/2108.06559
2025 年 6 月 21 日アクセス

[9] PICUS RedReport2025 The Top 10 Most Prevalent MITRE ATT&CK Techniques
https://www.picussecurity.com/resource/report/ed-report-2025
2025 年 6 月 21 日参照

[10] Jon Baker,Where to begin?Prioritizing ATT&CK Techniques
https://medium.com/p/c535b50983f4
2025 年 6 月 21 日アクセス

[11] 2025 Threat Detection Report,Red Canary
https://redcanary.com/resources/guides/threat-detection-report-exec-summary/
2025 年 6 月 21 日アクセス

[12] 2024 Cloud Security Report,Check Point
https://www.checkpoint.com/resources/items/cloud-security-report-2024
2025 年 6 月 21 日アクセス

[13] Md Rayhanur Rahman, Laurie Williams, An investigation of security controls and MITRE ATT&CK techniques
https://arxiv.org/abs/2211.06500
2025 年 6 月 21 日アクセス

[14] 2024/2023 Red Canary Threat Detection Report
https://www.youtube.com/watch?v=ObL8ocWRtHQ
https://www.youtube.com/watch?v=ntMFrCh4XzQ
2025 年 7 月 21 日アクセス

[15] MITRE ATT&CK Collection ,Discovery, Persistence
https://attack.mitre.org/tactics/TA0009/
https://attack.mitre.org/tactics/TA0007/
https://attack.mitre.org/tactics/TA0003/
2025 年 6 月 21 日アクセス

[16] Zhenyuan Li, Jun Zeng, Yan Chen, Zhenkai Liang,AttacKG: Constructing Technique Knowledge Graph from Cyber Threat Intelligence Reports
https://arxiv.org/abs/2111.07093
2025 年 6 月 21 日アクセス

[17] Michele Campobasso, Luca Allodi, Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale
https://arxiv.org/pdf/2009.04344
2025 年 7 月 27 日アクセス

[18] 2022 State of Public Cloud Security Report
https://orca.security/wp-content/uploads/2022/09/2022-State-of-Public-Cloud-Security-Report.pdf
2025 年 6 月 21 日アクセス

[19] MITRE ATT&CK Evaluations
https://attackevals.mitre.org/results/enterprise?view=cohort&evaluation=er6&result_type=DETECTION&scenarios=1,2,3
2025 年 6 月 21 日アクセス

[20] Jean C Digitale , Jeffrey N Martin , M Maria Glymour ,Tutorial on directed acyclic Graphs
https://pmc.ncbi.nlm.nih.gov/articles/PMC8821727/
2025 年 6 月 21 日アクセス

[21] Luis Muñoz-González, Daniele Sgandurra, Andrea Paudice, Emil C. LupuAuthors Info & Claims,"Efficient Attack Graph Analysis through Approximate Inference", 2016 https://dl.acm.org/doi/abs/10.1145/3105760 2025 年 6 月 26 日アクセス
[22] 総務省 地方公共団体における情報セキュリティポリシーに関するガイドライン（令和 7 年 3 月版） https://www.soumu.go.jp/main_content/001001336.pdf 2025 年 7 月 1 日アクセス
[23] デジタル庁 ガバメントクラウド利用システムにおけるセキュリティ対策（共通）2023/03/27 公開 https://guide.gcas.cloud.go.jp/general/security-tech 2025 年 7 月 1 日アクセス
[24] 総務省クラウドの設定ミス対策ガイドブック 2024 年 4 月 https://www.soumu.go.jp/main_content/000944467.pdf
[25] SBERT.net https://www.sbert.net/ 2025 年 7 月 1 日アクセス
[26] 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,Vol59 No3 1082-1094(Mar,2018)
[27] W O Kermack , A G McKendrick,Contributions to the mathematical theory of epidemics--I. 1927 https://pubmed.ncbi.nlm.nih.gov/2059741/ 2025 年 7 月 1 日アクセス
[28] Daron Acemoglu, Vasco M. Carvalho, Asuman Ozdaglar and Alireza Tahbaz-Salehi ,The Network Origins of Aggregate Fluctuations, https://www.jstor.org/stable/23271439 2025 年 7 月 1 日アクセス
[29] CVSS, Common Vulnerability Scoring System version4.0 Specification Document https://www.first.org/cvss/v4-0/specification-document https://www.first.org/cvss/v4-0/specification-document 2025 年 7 月 1 日アクセス
[30] Mohamed Ahmed, Sakshyam Panda, Christos Xenakis, Emmanouil PanaousisAuthors Info & Claims,MITRE ATT&CK-driven Cyber Risk Assessment https://dl.acm.org/doi/abs/10.1145/3538969.3544420 2025 年 7 月 1 日アクセス
[31] my _paper_materials_SPRE posted on github, yIto8047/my_paper_materials_SPRE: This document is a repository for documents related to the comparison and verification of the SPRE method and the IPA method.

著者略歴
伊藤 吉也（いとう・よしなり）
2022 年よりフォーティネットジャパン合同会社において地方自治体ビジネスを統括、同時にリスク分析の重要性の提言をデジタル省、総務省、文科省に行っている。
東京電機大学 先端科学技術研究科博士課程後期 2023 年 9 月より在学中
同年～現在，日本セキュリティ・マネジメント学会 IT リスク学研究会所属
令和 7 年より,総務省 地域情報化アドバイザー
令和 6 年より,文部科学省 学校 DX 戦略アドバイザー、ISC2 CISSP

加藤孝史（かとう・たかふみ）
大手 SIer にて 8 年間、ネットワークセキュリティ案件における提案および技術サポートに従事。数多くのプロジェクトを経験し、顧客のセキュリティ強化に貢献。2022 年よりフォーティネットジャパン合同会社にて、地方公共団体および教育委員会を担当するセールスエンジニアとして、ネットワークセキュリティソリューションの提案を担当。
ISC2 CISSP

佐々木 良一（ささき・りょういち）
1971 年 3 月東京大学卒業、同年 4 月日立製作所入社、システム開発研究所にてシステム高信頼化技
技術、セキュリティ技術、ネットワーク管理システム等の研究開発に従事。2001 年より東京電機大学教授、工学博士（東京大学）2002 年情報処理学会論文賞受賞。2007 年および 2017 年に総務大臣表彰等。日本セキュリティ・マネジメント学会名誉会長。

齊藤 泰一（さいとう・たいいち）
東京電機大学 博士 (工学) 工学部教授、
1989 年早稲田大学卒業、1991 年早稲田大学大学院修了、2001 年中央大学大学院修了 博士（工学）取得、専門分野 暗号理論・情報セキュリティ サイバーセキュリティ、近年、情報通信分野で重要度を増しているサイバーセキュリティ分野における脆弱性・攻撃法・防御法についての研究に従事

Appendix 1

3.1_MITRE-ATT&CK-Cloud-Matrix から攻撃再現性のための頻度カウントを抽出する Python コード
概要：
·MITRE ATT&CK の Cloud Matrix に基づき、攻撃テクニックの再現性（過去利用頻度）を自動集計する Python スクリプト一式。
·STIX 2.0 形式でエクスポートした MITRE ATT&CK データを入力し、攻撃グループ（intrusion-set）、キャンペーン、マルウェア／ツールごとに各テクニックの使用回数をカウントし集計。
·集計結果をテクニック ID・テクニック名とともに CSV ファイルへ自動出力。以降のリスク評価やデータ分析の基礎資料として汎用利用が可能。
·クラウド環境の攻撃分析や再現性スコアリングの自動化を実現し、オープンな MITRE データと Python 標準ライブラリや pandas、stix2 ライブラリのみで構築され、検証の再現性が高いプログラム例。
·本論文の「攻撃再現性スコアリング」手法で必要となる実利用頻度データの収集実装例として、研究や実務で幅広く応用可
Google Colab 用 Python コード（MITRE ATT&CK STIX 2.0 読み込み・Cloud Matrix スコアリング自動集計・CSV 出力対応）

```
# 必要なライブラリのインストール（初回のみ）
!pip install -q stix2

import json
import pandas as pd
from stix2 import parse

from google.colab import files
uploaded = files.upload()
stix_file_name = list(uploaded.keys())[0]

with open(stix_file_name, "r", encoding="utf-8") as f:
    stix_data = json.load(f)

stix_objects = stix_data.get("objects", [])

# Technique 情報を抽出（Cloud Matrix 限定）
techniques = {}
for obj in stix_objects:
    if obj.get("type") == "attack-pattern":
        platforms = obj.get("x_mitre_platforms", [])
        if "Cloud" in platforms:
            technique_id = None
            for ext_ref in obj.get("external_references", []):
                if ext_ref.get("source_name") == "mitre-attack" and "attack-pattern" in
ext_ref.get("external_id", ""):
                    technique_id = ext_ref.get("external_id")
            if technique_id:
                techniques[obj["id"]] = {
                    "technique_id": technique_id,
                    "name": obj.get("name", ""),
                    "group_usage": 0,
                    "campaign_usage": 0,
```

```
                "software_usage": 0
            }

# Relationship を走査して使用回数をカウント
for obj in stix_objects:
    if obj.get("type") == "relationship":
        target_ref = obj.get("target_ref")
        if target_ref in techniques:
            source_ref = obj.get("source_ref", "")
            if source_ref.startswith("intrusion-set--"):
                techniques[target_ref]["group_usage"] += 1
            elif source_ref.startswith("campaign--"):
                techniques[target_ref]["campaign_usage"] += 1
            elif source_ref.startswith("malware--") or source_ref.startswith("tool--"):
                techniques[target_ref]["software_usage"] += 1

df = pd.DataFrame([
    {
        "Technique ID": data["technique_id"],
        "Technique Name": data["name"],
        "Group_Usage_Count": data["group_usage"],
        "Campaign_Usage_Count": data["campaign_usage"],
        "Software_Usage_Count": data["software_usage"]
    }
    for data in techniques.values()
])

output_csv = "cloud_matrix_technique_usage_stats.csv"
df.to_csv(output_csv, index=False)
files.download(output_csv)
```

Appendix 2

3.2.4-3.2.5_攻撃パスを通常通信ルートに限定して抽出
概要：
・組織内システムの「通常時に確立されている通信ルート」を基準として、その正規通信経路上の資産間のみから成立する攻撃パスを自動抽出する手法の実装例。
・Excel や CSV 形式の資産ー通信経路データを解析し、MITRE ATT&CK Cloud Matrix の各攻撃テクニックを「実際に現場でありうる（＝閉じられた通信網で成立する）最小限の経路」に絞って抽出。
・IPA 方式で推奨される「攻撃コストが低い正規通信ルート上のみを優先」する方針を実現し、想定外の通信・横展開リスクの現実的な可視化に寄与。
・研究や実務においてシナリオ分析や攻撃グラフ抽出の自動化の基盤となり、特にクラウド・ゼロトラスト環境のリスクモデル運用に直結する処理例を示す。
・各種ファイル形式の前処理・パラメータ指定も柔軟で、実際の運用現場データで容易に検証・応用可能。

Google Colab 用 Python コード（NetworkX による正規通信路限定攻撃パス抽出・Excel/CSV ファイル入力自動化）

１：「資産と MITRE の攻撃テクニックの組み合わせリストを作成し、それらの全組み合わせの攻撃パスを自動生成する。」

```
# 必要ライブラリインストール

!pip install -q pandas openpyxl networkx matplotlib

from google.colab import files
import pandas as pd
import itertools
import networkx as nx
import matplotlib.pyplot as plt

# 1. ノードファイルのアップロード

print("nodes_assets_techniques_20250802.xlsx をアップロードしてください")

uploaded = files.upload()
nodes_file = list(uploaded.keys())[0]
xls = pd.ExcelFile(nodes_file)


# 各ステップのノードリスト(node_id, asset_name, technique_id)

steps = {}
for sheet in xls.sheet_names:
    df = xls.parse(sheet)
    df = df[["node_id", "asset_name", "technique_id"]]
    steps[sheet] = df


# 2. エッジファイルのアップロード（今回はパス列挙・可視化用途のみなら未使用でも OK）

print("edge_assets_techniques_20250802.xlsx をアップロードしてください")

uploaded = files.upload()
edges_file = list(uploaded.keys())[0]
```

```
# 3. 各 step のノードリストを列挙

step1 = steps["step1"].itertuples(index=False)
step2 = steps["step2"].itertuples(index=False)
step3 = steps["step3"].itertuples(index=False)
step4 = steps["step4"].itertuples(index=False)


# 4. 全組合せ列挙（25088 通り）

combis = itertools.product(step1, step2, step3, step4)


# 5. アタックパスを構造化

attack_paths = []
for a, b, c, d in combis:
    attack_paths.append({
        "step1_node_id": a.node_id,
        "step1_asset": a.asset_name,
        "step1_tech": a.technique_id,
        "step2_node_id": b.node_id,
        "step2_asset": b.asset_name,
        "step2_tech": b.technique_id,
        "step3_node_id": c.node_id,
        "step3_asset": c.asset_name,
        "step3_tech": c.technique_id,
        "step4_node_id": d.node_id,
        "step4_asset": d.asset_name,
        "step4_tech": d.technique_id,
    })


# 6. DataFrame 化して CSV 保存＆ダウンロード

attack_paths_df = pd.DataFrame(attack_paths)
attack_paths_df.to_csv("all_attack_paths_25088.csv", index=False, encoding="utf-8-
sig")
files.download("all_attack_paths_25088.csv")

print("all_attack_paths_25088.csv をダウンロード可能")


# 7. サンプル可視化（step1→step2→step3→step4 でグラフ化、最初の数個のみ描画）

def draw_attack_graph(paths_df, num_paths=10):
    G = nx.DiGraph()
    for i, row in paths_df.head(num_paths).iterrows():
        G.add_edge(row["step1_node_id"], row["step2_node_id"])
        G.add_edge(row["step2_node_id"], row["step3_node_id"])
        G.add_edge(row["step3_node_id"], row["step4_node_id"])
    plt.figure(figsize=(12, 8))
    pos = nx.spring_layout(G, seed=42)
    nx.draw(G, pos, with_labels=True, node_size=700, font_size=8, font_weight='bold',
arrows=True)
    plt.title(f"Sample Attack Paths (First {num_paths} Paths)")
    plt.show()
```

```
draw_attack_graph(attack_paths_df, num_paths=6)
```

２：「25,088 の攻撃パスを通信経路を特定して最適化された攻撃パス数を抽出する。」

```
#必要なパッケージのインストール
import pandas as pd
import networkx as nx
import matplotlib.pyplot as plt

from google.colab import files
# ノードファイルを手動でアップロード

uploaded_nodes = files.upload()  # ここで 1 ファイルだけ選べます

# 例: nodes.xlsx もしくは nodes.csv

import pandas as pd


# 拡張子に応じて読み込み

if list(uploaded_nodes.keys())[0].endswith('.xlsx'):
    nodes = pd.read_excel(list(uploaded_nodes.keys())[0])
else:
    nodes = pd.read_csv(list(uploaded_nodes.keys())[0])
print(nodes.head())


# エッジファイルを手動でアップロード

uploaded_edges = files.upload()  # ここで 1 ファイルだけ選べます

# 例: edges.xlsx もしくは edges.csv


if list(uploaded_edges.keys())[0].endswith('.xlsx'):

    # シートごとに読み込む場合

    sheet_names = pd.ExcelFile(list(uploaded_edges.keys())[0]).sheet_names

    # 例：複数シート合体

    edge_df_list = []
    for sn in sheet_names:
        edge_df_list.append(pd.read_excel(list(uploaded_edges.keys())[0],
sheet_name=sn))
    edges = pd.concat(edge_df_list, ignore_index=True)
else:
    edges = pd.read_csv(list(uploaded_edges.keys())[0])

print(edges.head())
```

```
# edges.csv, nodes.csv をアップロード後、データの読み込み

edges_all = edges  # 複数シートマージ想定

print(edges_all.head())

#通常時通信ルートのみ抽出する（communication_allowed＝１）

edges = edges_all[edges_all['communication_allowed'] == 1]

#有向グラフを作成

G = nx.DiGraph()
for _, row in edges.iterrows():
    G.add_edge(row['source_node_id'], row['target_node_id'],
step_from=row['step_from'], step_to=row['step_to'])

＃step ごとに開始・終了ノードリストを作成

step1_nodes = set(edges[edges['step_from']==1]['source_node_id'])
step4_nodes = set(edges[edges['step_to']==4]['target_node_id'])

#全 step1→step4 の Full4 step pass のみを抽出

paths = []
for start in step1_nodes:
    for end in step4_nodes:
        # 全４ステップパスだけ（longest path でフィルタ）
        for path in nx.all_simple_paths(G, source=start, target=end, cutoff=3):
            # path は [step1, step2, step3, step4] の長さ４
            if len(path) == 4:
                # 途中ノード移動も step 系列に沿うものだけ
                valid = True
                for i in range(3):
                    e = G.edges[path[i], path[i+1]]
                    if e['step_from'] != i+1 or e['step_to'] != i+2:
                        valid = False
                        break
                if valid:
                    paths.append(path)

＃DataFrame 化して保存

import pandas as pd
result = pd.DataFrame(paths, columns=["step1", "step2", "step3", "step4"])
result.to_csv("attack_paths_step4only.csv", index=False)

＃経路グラフを NetworkX で可視化（取り急ぎ１パス分のみのグラフ描画）

if len(paths) > 0:
```

```
    subG = nx.DiGraph()
    for i in range(3):
        subG.add_edge(paths[0][i], paths[0][i+1])
    nx.draw(subG, with_labels=True, node_color='lightblue', arrows=True)
    plt.show()
```

＃保存された csv ファイルをＤＬする

```
from google.colab import files
files.download('attack_paths_step4only.csv')
```

Appendix3

3.3.2 ：S-BERT（Sentence-BERT）を使って、MITRE ATT&CK の攻撃テクニックの説明文と総務省・デジタル庁のガイドライン PDF から抽出した文との意味的類似度をスコア化する Google Colab 対応の Python コードです。

機能概要

- s-BERT モデルで埋め込み（sentence embedding）を生成
- cosine 類似度でスコア化（0〜1）
- PDF からテキストを抽出（PyMuPDF 使用）
- MITRE 説明文とガイドライン文書の組で最も高いスコアを記録
- 類似度が閾値を超えたら「実装済」と判定
- 出力は CSV でダウンロード可能

Google Colab 用 Python コード（s-BERT + PDF 対応 + 類似度スコア + CSV 出力）

```
# 1. 必要なライブラリのインストール
!pip install -q sentence-transformers PyMuPDF pandas scikit-learn

# 2. ライブラリのインポート
import pandas as pd
import fitz  # PyMuPDF
from sentence_transformers import SentenceTransformer, util

# 3. s-BERT モデルをロード
model = SentenceTransformer('all-MiniLM-L6-v2')

# 4. PDF からテキストを抽出する関数
def extract_text_from_pdf(pdf_path):
    doc = fitz.open(pdf_path)
    texts = []
    for page in doc:
        text = page.get_text().strip()
        if text:
            texts.append(text)
    doc.close()
    return texts

# 5. 類似度スコア計算関数
def compute_max_similarity(mitre_text, guideline_sentences):
    mitre_emb = model.encode([mitre_text], convert_to_tensor=True)
    guideline_embs = model.encode(guideline_sentences, convert_to_tensor=True)
    scores = util.cos_sim(mitre_emb, guideline_embs)[0]
    max_idx = scores.argmax()
    return float(scores[max_idx]), guideline_sentences[max_idx]

# 6. MITRE 説明 CSV アップロード
from google.colab import files
uploaded = files.upload()
mitre_df = pd.read_csv(next(iter(uploaded)))

# 7. ガイドライン PDF アップロード
```

```
uploaded_pdf = files.upload()
pdf_path = next(iter(uploaded_pdf))
guideline_sentences = extract_text_from_pdf(pdf_path)

# 8. スコア計算＆マッチ文記録
similarities = []
matched_texts = []
implementation = []

for i, row in mitre_df.iterrows():
    desc = row["Description"]
    score, matched = compute_max_similarity(desc, guideline_sentences)
    similarities.append(round(score, 3))
    matched_texts.append(matched)
    implementation.append("実装済" if score >= 0.7 else "要検討")

mitre_df["Similarity"] = similarities
mitre_df["Matched_Text"] = matched_texts
mitre_df["Implementation_Status"] = implementation

# 9. CSV 出力＆ダウンロード
output_path = "/content/mitre_similarity_result.csv"
mitre_df.to_csv(output_path, index=False)
files.download(output_path)
```

Appendix 4

MITRE ATT &CK STI2.0 JSON よりクラウド攻撃テクニックのうち危険な２つのオブジェクトを掲載

#T1484.002: Domain or Tenant Policy Modification: Trust Modification


```
  {
    "type": "attack-pattern",
    "id": "attack-pattern--24769ab5-14bd-4f4e-a752-cfb185da53ee",
    "created": "2020-12-28T21:59:02.181Z",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "revoked": false,
    "external_references": [
      {
        "source_name": "mitre-attack",
        "url": "https://attack.mitre.org/techniques/T1484/002",
        "external_id": "T1484.002"
      },
      {
        "source_name": "AWS RE:Inforce Threat Detection 2024",
        "description": "Ben Fletcher and Steve de Vera. (2024, June). New tactics
and techniques for proactive threat detection. Retrieved September 25, 2024.",
        "url":
"https://reinforce.awsevents.com/content/dam/reinforce/2024/slides/TDR432_New-
tactics-and-techniques-for-proactive-threat-detection.pdf"
      },
      {
        "source_name": "CISA SolarWinds Cloud Detection",
        "description": "CISA. (2021, January 8). Detecting Post-Compromise Threat
Activity in Microsoft Cloud Environments. Retrieved January 8, 2021.",
        "url": "https://us-cert.cisa.gov/ncas/alerts/aa21-008a"
      },
      {
        "source_name": "AADInternals zure AD Federated Domain",
        "description": "Dr. Nestori Syynimaa. (2017, November 16). Security
vulnerability in Azure AD & Office 365 identity federation. Retrieved September
28, 2022.",
        "url": "https://o365blog.com/post/federation-vulnerability/"
      },
      {
        "source_name": "Microsoft - Azure AD Federation",
        "description": "Microsoft. (2018, November 28). What is federation with
Azure AD?. Retrieved December 30, 2020.",
        "url": "https://docs.microsoft.com/en-us/azure/active-
directory/hybrid/whatis-fed"
      },
      {
        "source_name": "Microsoft - Azure Sentinel ADFSDomainTrustMods",
        "description": "Microsoft. (2020, December). Azure Sentinel Detections.
Retrieved December 30, 2020.",
        "url": "https://github.com/Azure/Azure-
Sentinel/blob/master/Detections/AuditLogs/ADFSDomainTrustMods.yaml"
      },
```

```
      {
        "source_name": "Microsoft - Update or Repair Federated domain",
        "description": "Microsoft. (2020, September 14). Update or repair the
settings of a federated domain in Office 365, Azure, or Intune. Retrieved
December 30, 2020.",
        "url": "https://docs.microsoft.com/en-us/office365/troubleshoot/active-
directory/update-federated-domain-office-365"
      },
      {
        "source_name": "Okta Cross-Tenant Impersonation 2023",
        "description": "Okta Defensive Cyber Operations. (2023, August 31). Cross-
Tenant Impersonation: Prevention and Detection. Retrieved February 15, 2024.",
        "url": "https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-
prevention-and-detection"
      },
      {
        "source_name": "Sygnia Golden SAML",
        "description": "Sygnia. (2020, December). Detection and Hunting of Golden
SAML Attack. Retrieved November 17, 2024.",
        "url": "https://www.sygnia.co/threat-reports-and-advisories/golden-saml-
attack/"
      }
    ],
    "object_marking_refs": [
      "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
    ],
    "modified": "2025-04-15T19:58:14.422Z",
    "name": "Trust Modification",
    "description": "Adversaries may add new domain trusts, modify the properties
of existing domain trusts, or otherwise change the configuration of trust
relationships between domains and tenants to evade defenses and/or elevate
privileges.Trust details, such as whether or not user identities are federated,
allow authentication and authorization properties to apply between domains or
tenants for the purpose of accessing shared resources.(Citation: Microsoft -
Azure AD Federation) These trust objects may include accounts, credentials, and
other authentication material applied to servers, tokens, and
domains.¥n¥nManipulating these trusts may allow an adversary to escalate
privileges and/or evade defenses by modifying settings to add objects which they
control. For example, in Microsoft Active Directory (AD) environments, this may
be used to forge [SAML Tokens](https://attack.mitre.org/techniques/T1606/002)
without the need to compromise the signing certificate to forge new credentials.
Instead, an adversary can manipulate domain trusts to add their own signing
certificate. An adversary may also convert an AD domain to a federated domain
using Active Directory Federation Services (AD FS), which may enable malicious
trust modifications such as altering the claim issuance rules to log in any valid
set of credentials as a specified user.(Citation: AADInternals zure AD Federated
Domain) ¥n¥nAn adversary may also add a new federated identity provider to an
identity tenant such as Okta or AWS IAM Identity Center, which may enable the
adversary to authenticate as any user of the tenant.(Citation: Okta Cross-Tenant
Impersonation 2023) This may enable the threat actor to gain broad access into a
variety of cloud-based services that leverage the identity tenant. For example,
in AWS environments, an adversary that creates a new identity provider for an AWS
Organization will be able to federate into all of the AWS Organization member
```

```
accounts without creating identities for each of the member accounts.(Citation:
AWS RE:Inforce Threat Detection 2024)",
    "kill_chain_phases": [
      {
        "kill_chain_name": "mitre-attack",
        "phase_name": "defense-evasion"
      },
      {
        "kill_chain_name": "mitre-attack",
        "phase_name": "privilege-escalation"
      }
    ],
    "x_mitre_attack_spec_version": "3.2.0",
    "x_mitre_contributors": [
      "Blake Strom, Microsoft 365 Defender",
      "Praetorian",
      "Obsidian Security"
    ],
    "x_mitre_deprecated": false,
    "x_mitre_detection": "Monitor for modifications to domain trust settings,
such as when a user or application modifies the federation settings on the domain
or updates domain authentication from Managed to Federated via ActionTypes
<code>Set federation settings on domain</code> and <code>Set domain
authentication</code>.(Citation: Microsoft - Azure Sentinel ADFSDomainTrustMods)
This may also include monitoring for Event ID 307 which can be correlated to
relevant Event ID 510 with the same Instance ID for change details.(Citation:
Sygnia Golden SAML)(Citation: CISA SolarWinds Cloud Detection)¥n¥nMonitor for
PowerShell commands such as: <code>Update-MSOLFederatedDomain –DomainName:
¥"Federated Domain Name¥"</code>, or <code>Update-MSOLFederatedDomain –
DomainName: ¥"Federated Domain Name¥" –supportmultipledomain</code>.(Citation:
Microsoft - Update or Repair Federated domain)",
    "x_mitre_domains": [
      "enterprise-attack"
    ],
    "x_mitre_is_subtechnique": true,
    "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "x_mitre_platforms": [
      "Windows",
      "Identity Provider"
    ],
    "x_mitre_version": "2.2",
    "x_mitre_data_sources": [
      "Command: Command Execution",
      "Application Log: Application Log Content",
      "Active Directory: Active Directory Object Modification",
      "Active Directory: Active Directory Object Creation"
    ]
  },
```

#T1059.009: Command and Scripting Interpreter: Cloud API


```
  {
    "type": "attack-pattern",
    "id": "attack-pattern--55bb4471-ff1f-43b4-88c1-c9384ec47abf",
    "created": "2022-03-17T13:28:24.989Z",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "revoked": false,
    "external_references": [
      {
        "source_name": "mitre-attack",
        "url": "https://attack.mitre.org/techniques/T1059/009",
        "external_id": "T1059.009"
      },
      {
        "source_name": "Microsoft - Azure PowerShell",
        "description": "Microsoft. (2014, December 12). Azure/azure-powershell.
Retrieved March 24, 2023.",
        "url": "https://github.com/Azure/azure-powershell"
      }
    ],
    "object_marking_refs": [
      "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
    ],
    "modified": "2025-04-15T19:58:32.612Z",
    "name": "Cloud API",
    "description": "Adversaries may abuse cloud APIs to execute malicious
commands. APIs available in cloud environments provide various functionalities
and are a feature-rich method for programmatic access to nearly all aspects of a
tenant. These APIs may be utilized through various methods such as command line
interpreters (CLIs), in-browser Cloud Shells,
[PowerShell](https://attack.mitre.org/techniques/T1059/001) modules like Azure
for PowerShell(Citation: Microsoft - Azure PowerShell), or software developer
kits (SDKs) available for languages such as
[Python](https://attack.mitre.org/techniques/T1059/006).  ¥n¥nCloud API
functionality may allow for administrative access across all major services in a
tenant such as compute, storage, identity and access management (IAM),
networking, and security policies.¥n¥nWith proper permissions (often via use of
credentials such as [Application Access
Token](https://attack.mitre.org/techniques/T1550/001) and [Web Session
Cookie](https://attack.mitre.org/techniques/T1550/004)), adversaries may abuse
cloud APIs to invoke various functions that execute malicious actions. For
example, CLI and PowerShell functionality may be accessed through binaries
installed on cloud-hosted or on-premises hosts or accessed through a browser-
based cloud shell offered by many cloud platforms (such as AWS, Azure, and GCP).
These cloud shells are often a packaged unified environment to use CLI and/or
scripting modules hosted as a container in the cloud environment.  ",
    "kill_chain_phases": [
      {
        "kill_chain_name": "mitre-attack",
        "phase_name": "execution"
      }
    ],
```

```
  "x_mitre_attack_spec_version": "3.2.0",
  "x_mitre_contributors": [
    "Ozan Olali",
    "Nichols Jasper",
    "Jason Sevilla",
    "Marcus Weeks",
    "Caio Silva"
  ],
  "x_mitre_deprecated": false,
  "x_mitre_detection": "",
  "x_mitre_domains": [
    "enterprise-attack"
  ],
  "x_mitre_is_subtechnique": true,
  "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
  "x_mitre_platforms": [
    "IaaS",
    "SaaS",
    "Office Suite",
    "Identity Provider"
  ],
  "x_mitre_version": "1.2",
  "x_mitre_data_sources": [
    "Command: Command Execution"
  ]
},
```