重要インフラのGRC対応強化に向けた連鎖ダイアモンドモデルの提案

阪田 恒晟[1,2,a)]　藤井 翔太[1]　川口 信隆[1]　武本 敏[1]

概要：重要インフラを対象としたサイバー攻撃の高度化に伴い，ガバナンス・リスク・コンプライアンス（GRC）対応の強化が求められている．IT 分野では，既に各種フレームワークが整備され，体系的なリスク評価および規格準拠管理が進展している一方，重要インフラでは，現場の運用データや攻撃検知ログと連携した，実態に即したリスク・コンプライアンス評価の仕組みは未だ確立されていない．本研究では，実際の攻撃シナリオの連鎖性や環境変化を反映するため，攻撃者の行動・能力・インフラ・被害主体といった要素間の関係を記述するダイアモンドモデルを基盤に，ネットワークログや脅威インテリジェンスから自動的に「連鎖ダイアモンドモデル」を生成し，規格要件との対応関係を明示化する手法を提案する．提案手法は，各攻撃フェーズにおける検知情報をもとにダイアモンド同士を因果関係で連鎖させ，重要インフラ向けの国際標準である IEC 62443 における 7 つのカテゴリとのトレーサビリティを確立することで，動的かつ説明可能なリスク評価を実現する．評価実験では，産業制御システムに接続された侵入検知システム（IDS）の実運用ログに対して，規格要件に基づくクエリを適用し，連鎖ダイアモンドモデルを自動生成することで，要件との整合性を実証した．本手法により，重要インフラにおけるセキュリティ運用に対し，より実態に即した準拠性評価とリスク把握が可能となり，GRC 対応の高度化に資することが期待される．

キーワード：ガバナンス・リスク・コンプライアンス，重要インフラ，連鎖ダイアモンドモデル，侵入検知システム

Chained Diamond Model for Enhancing GRC Practices in Critical Infrastructure

Kousei Sakata[1,2,a)]　Shota Fujii[1]　Nobutaka Kawaguchi[1]　Satoshi Takemoto[1]

Abstract: As cyberattacks on critical infrastructure grow more sophisticated, there is a growing need to strengthen Governance, Risk, and Compliance (GRC) practices in operational technology (OT) environments. While the IT domain has established frameworks enabling structured risk assessment and standards compliance, OT systems still lack mechanisms that leverage operational data and detection logs for context-aware evaluation. This paper proposes a method for automatically generating chained Diamond Models from network logs and threat intelligence, capturing the causal relationships among adversary, capability, infrastructure, and victim across multiple attack phases. These models are aligned with the seven foundational requirement categories defined in IEC 62443—an international standard for OT security—through query-based mapping, establishing traceability between observed attack behaviors and regulatory requirements. The proposed method was validated using real-world industrial IDS logs, demonstrating its ability to consistently reflect compliance-relevant patterns and multi-stage attack flows. This approach enables dynamic and explainable risk assessments and supports more realistic and standards-aligned GRC management in critical infrastructure environments.

Keywords: Governance, Risk, and Compliance (GRC), Critical Infrastructure, Diamond Model, IDS

1. はじめに

サイバー攻撃の高度化・巧妙化により，産業，鉄道，電力といった重要インフラにおけるセキュリティリスクが深刻化している．2016 年のウクライナ電力網における大規模停電 [1] や，2021 年の米国石油パイプラインの供給停止 [2]，最近では 2022 年のデンマーク鉄道システムの停止事案 [3] など，重要インフラを標的としたサイバー攻撃は社会全体に甚大な影響を及ぼしてきた．

こうした背景のもと，組織のセキュリティ対応力を包括的に高めるための枠組みとして，ガバナンス・リスク・コンプライアンス（Governance, Risk, and Compliance, GRC）[4–6] が重要視されている．GRC とは，組織が目標を達成するために必要な組織運営の方針・監督（Governance），脅威や不確実性の評価と対応（Risk），および法令・規格の遵守（Compliance）を統合的に運用する枠組みである．

IT（Information Technology）領域では, NIST Risk Management Framework [7] や ISO/IEC 27001 [8] に代表される各種フレームワークを早期に整備・展開し，GRC 対応を推進してきた．その背景には，システム構成や運用環境が比較的均質かつ更新頻度が高いため，新たな脅威情報や規格要件を迅速に取り込み，運用プロセスに反映しやすいという IT 特有の性質がある．

これに対し OT（Operational Technology）領域では，IEC 62443 [9] に基づくコンプライアンス対応は進展している一方，長期稼働や更新困難な特性から，新たな脅威情報を運用に即応的に反映することが難しく，結果として静的なリスク評価に依存してきた [10,11]．言い換えれば，システムの運用ログや検知イベントを活用した動的リスク評価は十分に整備されていない．

さらに，リスク評価で得られた知見を IEC 62443 のセキュリティ要求（Security Requirement, SR）に体系的に対応付け，侵害要件への是正プロセスに反映する仕組みも確立されていない [12–15]．リスク管理とコンプライアンス要求が分断されたままでは，セキュリティ水準の実効的な向上や継続的な改善サイクルの確立は困難となる．

本研究はこれら二つの課題に対処するため，(i) 実運用データに基づく動的リスク評価の高度化手法，及び (ii) リスク評価結果とコンプライアンス要求を結びつける体系的手法の確立を目的とし，両者を同時に実現する枠組みを提案する．

第一に，制御システムに接続された侵入検知システム（Intrusion Detection System, IDS）から得られるアラートログを入力とし，IEC 62443 のセキュリティ要求や脅威知識ベースに基づくクエリを適用して分析対象となる攻撃イベントを抽出する．本研究では抽出したイベントを，MITRE ATT&CK® [16] と補完的に利用されるダイアモンドモデル [17] を用いて，その構成要素である Adversary（攻撃者），Capability（攻撃手段），Infrastructure（攻撃基盤），Victim（被害対象）の 4 要素にマッピングする．さらに，関連する SR および ATT&CK 戦術・技術 ID を付与することで「拡張ダイアモンドモデル」を構築する．これにより，IDS ログを単なる検知記録として扱うのではなく，規格要件や攻撃技術と結び付けた統一的な表現として整理し，動的リスク評価の基礎を与える．

第二に，複数の拡張ダイアモンドモデル間の共有要素の一致（攻撃主体・攻撃対象・基盤の同一性），及び戦術フェーズの論理的順序に基づいて因果関係を判定し，攻撃イベントを連鎖させた「連鎖ダイアモンドモデル」を生成する．これにより，単発の検知結果を超えて攻撃シナリオ全体を再構成し，各段階を IEC 62443 の 7 カテゴリに属する SR に明示的に対応付けて整理できる．その結果，実際の攻撃発生順序を反映しつつ，優先的に対処すべき侵害要件を抽出でき，リスク評価とコンプライアンス評価を結び付けた分析を実現する．

評価実験では，実際の FA（Factory Automation）システムを対象に，総当たり攻撃および中間者攻撃の 2 種類の攻撃シナリオを実施した．攻撃実施後の IDS ログに対し IEC 62443 の SR に基づく 14 件のクエリを適用した結果，6 件でアラートを検出し，7 個の拡張ダイアモンドモデルを生成した．さらに，共有ノードと戦術フェーズの順序を考慮して連鎖化した結果，28 ノードからなる連鎖ダイアモンドモデルが得られ，共有ノードは 7 個に集約された．

この結果，単発の検知イベントを拡張ダイアモンドとして整理することでリスクを構造的に高度化し，それらの連鎖化によって攻撃進行過程を IEC 62443 の規格要件と体系的に対応付けられることを確認した．

本研究の主な貢献は以下の通りである．

- OT 環境の実運用ログに基づき，攻撃イベントを拡張ダイアモンドモデルとして構築することで，従来未整備であった動的リスク評価の高度化手法を確立した．
- 複数の拡張ダイアモンドモデルを連鎖させ，各段階を IEC 62443 のセキュリティ要求（SR）に体系的に対応付けることで，リスク管理とコンプライアンス管理を統合的に結びつける方法論を確立した．
- 評価実験により，提案手法が攻撃進行過程と規格要件を体系的に紐づけられることを確認した．これにより，優先的に対処すべき侵害要件を抽出し，動的かつ説明可能な GRC 評価の実現可能性を示した．

[1] 株式会社 日立製作所
[2] 国立大学法人 東京科学大学 工学院 システム制御系
[a)] kosei.sakata.ky@hitachi.com

表 1　Risk/Compliance 観点に基づく既存研究の比較（✓=対応, 空欄=非対応）

	(i) Risk			(ii) Risk to Compliance		
研究	現場データの利用	リスクの同定	TTP 連携	攻撃連鎖性の復元	要件マッピング	是正プロセス反映
Ghaeini, H. R. et al. (2018) [10]	✓					
Ahmed, M. et al. (2022) [11]		✓	✓			
Hollerer, S. et al. (2022) [12]		✓	✓		✓	
Göttel, C et al. (2023) [13]					✓	
Zahid, S. et al. (2023) [14]		✓	✓		✓	
Da Silva, M. et al. (2025) [15]		✓	✓		✓	
本研究（提案）	✓	✓	✓	✓	✓	✓

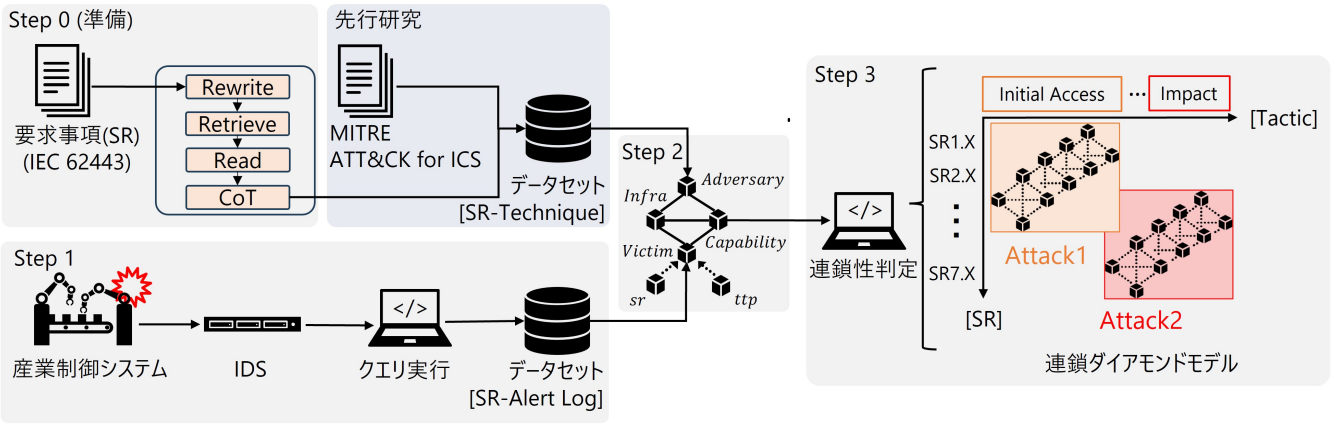

図 1　提案フレームワーク

2. 関連研究

本章では OT 領域における（i）リスク評価，および（ii）リスクとコンプライアンスの連携に関する先行研究を**表 1** に整理する．まずリスクに関する研究として，ネットワークやプロセス状態を活用した異常検知 [10] や，ATT&CK に基づく TTP（Tactics, Techniques, and Procedures）駆動の脅威同定手法 [11] が報告されている．しかし，これらの研究では運用ログを統一的な単位表現に整理してリスクを体系的に評価する仕組みは示されていない．次にリスクからコンプライアンスへの連携に関する研究としては，リスクと安全の相互依存性を整理し体系化を試みた研究 [12] や，IEC 62443 に基づくリスク評価の自動化に関する研究 [13, 15]，さらにセキュリティフレームワーク間の対応付けを行った研究 [14] が報告されている．これらはリスクの知見を規格や管理基準に接続する取り組みに位置づけられる．しかし，いずれも文書や脅威モデルを基盤とした静的な整合にとどまり，実運用ログに基づく攻撃過程を因果関係や時系列を保持したまま規格要求に動的にマッピングし，是正プロセスへと接続する枠組みは示されていない．

以上の検討から，既存研究は（i），（ii）両観点に部分的な貢献を示しているものの，実運用ログを活用した動的リスク評価は依然として確立されておらず（以下，課題 1），さらにその結果を規格要求や是正プロセスに結び付ける枠組みも不足している（以下，課題 2）．

3. 提案手法

本章では，前述した二つの課題を解決することを目標に，**図 1** に示すフレームワークを提案する．

まず Step 0 では，IEC 62443 などの規格文書を機械可読化し，セキュリティ要件（SR）と ATT&CK の TTP を対応付けることで，規格要求とリスク知見を結び付ける基盤を整備する（課題 2 への対応）．Step 1 では，この対応関係に基づき，SR ごとのクエリで実運用ログから観測データを抽出し，動的リスク評価に資する（課題 1 への対応）．Step 2 では，抽出ログを拡張ダイアモンドに写像して統一的に表現し，異種ログ間の差異を吸収する（課題 1 への対応）．Step 3 では，戦術順序や共有属性から因果連鎖を構築し，各ノードに SR ラベルを保持させることで，攻撃過程の復元と規格要求とのトレーサビリティを同時に実現する（課題 1・2 への対応）．以下に，各ステップの内容を詳述する．

Step 0：IEC 62443 の機械可読化

本ステップでは，IEC 62443-3-3 の公式 PDF から SR コーパス（SR ID／本文／カテゴリ等のメタ情報）を自動抽出・正規化し，さらに SR に対応する ATT&CK Technique を著者らの先行研究 [18] のマッピング結果に基づき紐付ける．

PDF からの構造化抽出には，LLM（gpt-4o, gpt-4.1, gpt-4.1 mini の 3 種）と LangChain [19] を組み合わせ

表 2 LLM 構成ごとの抽出結果
抽出 SR/全 SR(誤抽出数) と消費 token 数の推移

モデル	手法（1）	手法（2）	手法（3）
GPT-4o	29/51（3） 71,735	12/51（1） 23,643	43/51（1） 30,462
GPT-4.1	27/51（3） 84,162	14/51（0） 29,003	40/51（0） 39,671
GPT-4.1mini	30/51（6） 79,154	35/51（2） 34,479	**50/51（1）** **35,257**

た複数のパイプラインを比較・評価する．具体的には，（1） LLM ＋ LangChain，（2） LLM ＋ LangChain ＋ Rewrite–Retrieve–Read [20]，（3） LLM ＋ LangChain ＋ Rewrite–Retrieve–Read ＋ Chain-of-Thought（CoT）[21] の 3 構成を全モデルで実装し，抽出件数・誤抽出率・トークン効率の観点で比較した．

本ステップでは，精度を最優先としつつも，実運用でのコスト抑制のためトークン消費を可能な限り抑えることを目的とした．**表 2** に示す通り，gpt-4.1 mini ＋ LangChain ＋ Rewrite–Retrieve–Read ＋ CoT の構成は，精度指標で最も高い値を示すと同時に，消費トークン数も他の高精度構成に比べ低く抑えられており，本ステップの目的に照らして最良のトレードオフと判断できる．

この結果は，手法（3）が構造化抽出の精度向上に有効であることを示す先行研究 [20] とも整合している．ここで自動抽出された SR 及び紐づけられた TTP は Step 1 の SR 準拠クエリ実行，Step 2 の拡張ダイアモンド化の基盤として用いる．

Step 1：SR 準拠クエリによる現場ログの抽出

Step 1 では Step 0 にて抽出した SR に対応したクエリを適用し，制御システムの運用ログを抽出する．本研究では，Nozomi 社のネットワーク型 IDS を用い，IEC 62443 Content Pack の SR 対応クエリ [22] を参照する．

クエリを適用する前段として，評価対象アセット集合 Ω（IP/MAC やゾーン・コンジットで選定）に基づくフィルタリングを実施し，観測期間 W の設定，および通信状態で絞り込む（例：status $\in \{\texttt{open}, \texttt{ack}\}$）．

ここで，セキュリティ要求 $sr \in \mathcal{SR}$ に対応する検知カテゴリ集合を T_{sr}，当該カテゴリから誘導されるクエリ（IDS ルール）集合を $R(sr)$，フィルタ後にクエリ適用で得られるアラート集合を $\mathcal{A}_{sr}$ とし，表 3 にそれらを整理した．T_{sr} 及び $R(sr)$ は Content Pack [22] から抽出したカテゴリ及びクエリ群である．形式的には $\mathcal{A}_{sr}$ を次式で定義する．

$$\mathcal{A}_{sr} = \{\, a \mid a.\text{rule\_id} \in R(sr),\ a.\text{asset} \in \Omega,\ a.\text{time} \in W, a.\text{severity} \geq \tau,\ a.\text{status} \in \{\text{open}, \text{ack}\} \,\}$$

全 SR に対するアラート集合は $\mathcal{A} = \bigcup_{\text{sr} \in \mathcal{SR}} \mathcal{A}_{\text{sr}}$ であり，処理での一貫性を確保するために正規化した上で，拡張ダイアモンドモデル生成および連鎖構造構築の入力とする．

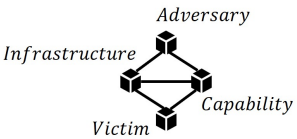

図 2 ダイアモンドモデル

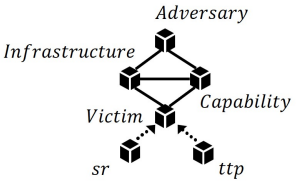

図 3 拡張ダイアモンドモデル

Step 2：拡張ダイアモンドモデルへの変換

Step2 では，Step1 で得られた $\mathcal{A} = \bigcup_{\text{sr} \in \mathcal{SR}} \mathcal{A}_{\text{sr}}$ を入力とし，各アラート $a \in \mathcal{A}_{\text{sr}}$ を拡張ダイアモンドモデルへ変換する．

ダイアモンドモデルは, 攻撃者の侵入解析に用いられ [17], **図 2** に示すように 4 タプル (A, C, I, V) で表現される．ここで A（Adversary）は攻撃者，C（Capability）は攻撃手段，I（Infrastructure）は攻撃基盤，V（Victim）は被害対象を表す．本研究では，このダイアモンドモデルに対し，**図 3** に示すように IEC 62443 3-3 のセキュリティ要件 $sr \in \mathcal{SR}$ と ATT&CK for ICS の技術 $ttp \in \mathcal{TTP}$ の 2 要素を追加し，6 タプルで表す拡張ダイアモンドモデル $d = (A, C, I, V, sr, ttp)$ を定義する．

このダイアモンドモデルのメタ要素拡張により，「攻撃主体」「使用された攻撃手段」「攻撃対象」に加え，「関連するセキュリティ要件」「該当する攻撃フェーズ」を各ノードで一意に表現可能となる．

上記で拡張したダイアモンドモデルに対し，Step1 で得られたアラートの属性を，各要素に以下のように具体的に対応付ける：$A(a), V(a) \in (\mathcal{IP} \times \mathcal{MAC}) \cup \mathcal{H}$，　$C(a) \in \mathcal{CAP}$，　$I(a) \in \mathcal{INF}$，　$sr(a) \in \mathcal{SR}$，　$ttp(a) \in \mathcal{TTP}$.

ここで，$\mathcal{IP}$ は IP アドレス集合，$\mathcal{MAC}$ は MAC アドレス集合，$\mathcal{H}$ は機器ラベル／ホスト名集合，$\mathcal{INF}$ はインフラ種別集合（例：SMB, Modbus），$\mathcal{CAP}$ は攻撃能力集合（例：Brute-force Attempts, MITM）である．また，戦術順序を表す写像 $\pi : \mathcal{TTP} \to \{1, \ldots, K\}$ を定義し，$\pi(ttp)$ を当該 TTP の戦術（フェーズ）番号とする．

これらを用いて，アラートから拡張ダイアモンドモデルへの写像 α を次のように定義する:

$$\alpha : \mathcal{A} \to \mathcal{D},\quad \alpha(a) = (A(a), C(a), I(a), V(a), sr(a), ttp(a)).$$

Step2 の出力は $\mathcal{D} = \{\alpha(a) \mid a \in \mathcal{A}\}$ であり，Step3 での連鎖構造構築のノード集合となる．

Step 3：連鎖条件の定式化と構築アルゴリズム

Step3 では，Step2 で得られた拡張ダイアモンドモデル集合 $\mathcal{D} = \{\alpha(a) \mid a \in \mathcal{A}\}$ を入力として，攻撃イベント間の因果的関係を有向辺として付与し，攻撃の進行を可視化する連鎖ダイアモンドモデル $G = (\mathcal{D}, \mathcal{E})$ を構築する．

攻撃の各イベントをつなげて時系列的な「連鎖」として表すには，まず ATT&CK for ICS の戦術フェーズ順序を用いて前後関係を決める必要がある．しかし，順序だけでは単なる時間的並びであり，実際に同じ攻撃の一部かどう

表 3 各 SR に対応する検知カテゴリ集合 T_{sr} とアラート集合 $\mathcal{A}_{sr}$

SR	Definition	Formal detection condition
SR 1.1 SR 1.5	Human user identification Authenticator management	$T_{\mathrm{sr}} = \{\texttt{WeakPassword}, \texttt{CleartextPassword}, \texttt{WeakAuthProtocol}\}$ $\mathcal{A}_{\mathrm{sr}} = \{\, a \in \mid a.\mathrm{asset} \in \Omega_{\mathrm{IPMAC}},\ a.\mathrm{status} \in \{\texttt{open}, \texttt{ack}\},\ a.\mathrm{type} \in T_{\mathrm{sr}} \,\}$
SR 1.8 SR 1.9	Public key infrastructure certificates Strength of public key authentication	$T_{\mathrm{sr}} = \{\texttt{WeakPassword}, \texttt{CleartextPassword}, \texttt{WeakAuthProtocol}\}$ $\mathcal{A}_{\mathrm{sr}} = \{\, a \in \mid a.\mathrm{asset} \in \Omega_{\mathrm{IPMAC}},\ a.\mathrm{status} \in \{\texttt{open}, \texttt{ack}\},\ a.\mathrm{type} \in T_{\mathrm{sr}},\ \mathrm{days\_ago}(a.\mathrm{time}) \leq 30 \,\}$
SR 1.11	Unsuccessful login attempts	$T_{\mathrm{sr}} = \{\texttt{MultipleAccessDenied}, \texttt{MultipleUnsuccessfulLogins}, \texttt{BruteForceAttack}\}$ $\mathcal{A}_{\mathrm{sr}} = \{\, a \in \mid a.\mathrm{asset} \in \Omega_{\mathrm{IPMAC}},\ a.\mathrm{status} \in \{\texttt{open}, \texttt{ack}\},\ a.\mathrm{type} \in T_{\mathrm{sr}} \,\}$
SR 2.8	Auditable events	Aggregation: group $\{\, a \in \mid a.\mathrm{asset} \in \Omega_{\mathrm{IP}} \,\}$ by a.name and sort by count desc
SR 3.1 SR 3.2	Communication integrity Malicious code protection	$T_{\mathrm{sr}} = \{\texttt{MalwareDetected}, \texttt{MaliciousURL}, \texttt{MaliciousIP}, \texttt{MaliciousProtocol}, \texttt{MaliciousDomain}, \texttt{MalformedTraffic}, \texttt{NewNodeMaliciousIP}, \texttt{MaliciousFile}, \texttt{SuspiciousActivity}\}$ $\mathcal{A}_{\mathrm{sr}} = \{\, a \in \mid a.\mathrm{asset} \in \Omega_{\mathrm{IPMAC}},\ a.\mathrm{status} \in \{\texttt{open}, \texttt{ack}\},\ a.\mathrm{type} \in T_{\mathrm{sr}} \,\}$
SR 4.1	Information confidentiality	$T_{\mathrm{sr}} = \{\texttt{CleartextPassword}, \texttt{WeakEncryption}\}$ $\mathcal{A}_{\mathrm{sr}} = \{\, a \in \mid a.\mathrm{asset} \in \Omega_{\mathrm{IPMAC}},\ a.\mathrm{status} \in \{\texttt{open}, \texttt{ack}\},\ a.\mathrm{type} \in T_{\mathrm{sr}} \,\}$
SR 7.1	Denial of service protection	$T_{\mathrm{sr}} = \{\texttt{DDoS}, \texttt{MITM}\}$ $\mathcal{A}_{\mathrm{sr}} = \{\, a \in \mid a.\mathrm{status} \in \{\texttt{open}, \texttt{ack}\},\ a.\mathrm{type} \in T_{\mathrm{sr}} \,\}$
SR 7.2	Resource management	$T_{\mathrm{sr}} = \{\texttt{NetworkScan}, \texttt{MACFlood}, \texttt{ProtocolFlood}, \texttt{TCPFlood}, \texttt{UDPFlood}, \texttt{PortScan}\}$ $\mathcal{A}_{\mathrm{sr}} = \{\, a \in \mid a.\mathrm{asset} \in \Omega_{\mathrm{IP}},\ a.\mathrm{status} \in \{\texttt{open}, \texttt{ack}\},\ a.\mathrm{type} \in T_{\mathrm{sr}} \,\}$
SR 7.8	Network & security configuration settings	$T_{\mathrm{sr}} = \{\texttt{ConfigurationChange}\}$ $\mathcal{A}_{\mathrm{sr}} = \{\, a \in \mid a.\mathrm{asset} \in \Omega_{\mathrm{IP}},\ a.\mathrm{status} \in \{\texttt{open}, \texttt{ack}\},\ a.\mathrm{type} \in T_{\mathrm{sr}} \,\}$

かは分からない．そこで，本研究では，順序条件に加えて，両イベントが同じ主体・能力・インフラ・被害対象のいずれかを共有している場合にのみ，因果的なつながりがあると判定する．この判定を数式で表したものが，以下の共有属性判定関数 Φ である．

$$\Phi(d_i, d_j) \iff (A_i = A_j) \vee (C_i = C_j) \vee (I_i = I_j) \vee (V_i = V_j)$$

これは，攻撃者（A），攻撃能力（C），攻撃基盤（I），被害対象（V）のいずれかが一致すれば，両イベントは同一の攻撃シナリオ内に存在する可能性が高いとみなすものである．したがって，有向辺 (d_i, d_j) を付与する条件は

$$\pi(ttp_i) < \pi(ttp_j) \quad \wedge \quad \Phi(d_i, d_j) = \mathrm{true}$$

である．すなわち，d_i がより前の戦術に属し，かつ属性のいずれかを共有する場合に，d_i から d_j への有向辺を生成する．

アルゴリズム 1 は，この条件に基づき全てのノード対 (d_i, d_j) を走査し，連鎖条件を満たす場合に有向辺を追加する．手順は以下の通りである．まず，Step2 で構築した拡張ダイアモンドモデルのノード集合 $\mathcal{D}$ を入力とし，空の辺集合 $\mathcal{E}$ を初期化する．次に，$\mathcal{D}$ 内の全てのノード対 (d_i, d_j) について走査を行い，d_i が d_j より前の戦術フェーズに属するか（$\pi(ttp_i) < \pi(ttp_j)$）を判定する．続いて，共有属性判定関数 Φ により両ノード間に因果関係があるとみなせるかを確認する．これらの条件をともに満たした場合に限り，辺 (d_i, d_j) を $\mathcal{E}$ に追加する．以上の処理を全てのノード対に適用することで，攻撃フェーズの進行と因果的つながりの双方を満たす関係のみを有向辺として持つ連鎖ダイアモンドモデル $G = (\mathcal{D}, \mathcal{E})$ が構築される．

Algorithm 1 連鎖ダイアモンドモデル構築

Require: アラート集合 $\mathcal{A}$（Step1 の出力）
Ensure: 連鎖ダイアモンドモデル $G = (\mathcal{D}, \mathcal{E})$

```
D ← {α(a) | a ∈ A}                ▷ Step2 の拡張ダイアモンド集合
E ← ∅
for all d_i ∈ D do
    for all d_j ∈ D do
        if π(ttp_i) < π(ttp_j) and Φ(d_i, d_j) then
            E ← E ∪ {(d_i, d_j)}
        end if
    end for
end for
return G = (D, E)
```

この方法は全ノード対を走査するため計算量は $O(|\mathcal{D}|^2)$ であるが，ICS のアラート数は一般的に中規模であるため，実用的な処理時間で構築可能である．得られた G は，攻撃フェーズに沿った時系列的な攻撃シナリオの可視化に加え，規格要件（$\mathcal{SR}$）および TTP の双方に基づく防御策評価に活用できる．

4. 評価実験

本章の目的は，序章で掲げた二つの目的，動的リスク評価の高度化手法の確立，及びリスク評価結果とコンプライアンス要求を結びつける体系的手法の確立が，図 1 に示す提案フレームワークで達成できるかを検証することにある．

評価対象は産業用のロボットアームとコンベアから構成される模擬 FA システムである．本システムには IDS が接続されており，制御中の通信データがログとして蓄積される．ここで，総当たり攻撃，及び中間者攻撃の 2 種類の攻撃シナリオを実施することで得られた通信ログに対して

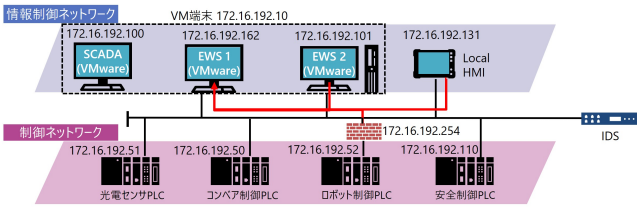

図 4　シナリオ 1: 総当たり攻撃

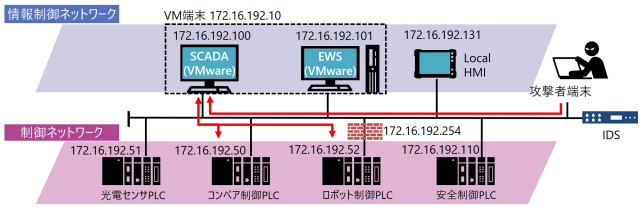

図 5　シナリオ 2: 中間者攻撃

表 3 に示す 14 件のクエリを適用する．これにより第一に，アラートが拡張ダイアモンドモデルを介して各要件に動的に対応付けられるかを確認する．第二に，得られた拡張ダイアモンドモデルが共通ノードを共有し連鎖ダイアモンドモデルを生成，及び実際の攻撃進行と SR の関係性を明確化可能かを評価する．

4.1　評価シナリオ

シナリオ 1: 総当たり攻撃（Brute-force Attempts）

図 4 に示す通り，制御ネットワーク上の EWS（Engineering Work Station）端末を標的とし，既知の IP アドレスおよび MAC アドレスを利用して不正ログインを試行する．試行は異なるユーザ ID とパスワードの組合せを総当たりで異なるデバイスから送信することで実施し，成功後は制御コマンドの送信を試みる．本シナリオは，IDS で作成可能なアラートクエリの内，IEC 62443-3-3 の `SR 1.11`（ログインの試行），`SR 2.8`（監査イベント），及び `SR 3.1`，`SR 3.2`（通信の完全性）に関連する検出能力を評価するために選定した．

シナリオ 2: 中間者攻撃（MITM）

図 5 に示す通り，攻撃者は制御ネットワーク上で中間者攻撃（Man in the Middle, MITM）を行い，SCADA と PLC（Programmable Logic Controller）間の通信経路を掌握する．これにより，Modbus/TCP パケットの改ざんやコマンドの遅延・挿入を実施する．本シナリオは，IDS で作成可能なアラートクエリの内，IEC 62443-3-3 の `SR 7.1`（DoS 攻撃防護），`SR 7.2`（リソースマネジメント）を含む可用性要件に関連する検出能力を評価するために選定した．

4.2　評価結果

本節では，これらのシナリオを実行して得られた IDS ログに対し，Step1–3 の手順を適用して得られた結果について説明する．

結果 1：動的リスク評価の高度化

攻撃実施後の IDS ログに対し，14 件のクエリを適用した結果，**表 4** に示す 6 件の SR でアラートを検出し，計 7 個の拡張ダイアモンドを生成した．シナリオ 1 では 4 個の拡張ダイアモンドが得られ，`SR 1.11`（*Brute Force, T0806*），`SR 2.8`（*Alarm Suppression, T0878*），`SR 3.1`（*Spoofed Command/Reporting, T0856*），`SR 3.2`（*Automated Collection, T0851*）にそれぞれ対応した．各ダイアモンドの A, V はログ中の同一主体／対象を反映し，能力 C と基盤 I も当該イベントの属性に即して付与されている．

シナリオ 2 では，3 個のダイアモンドが得られ，`SR 7.2`（*Network Scan, T0840*）が 1 件，`SR 7.1`（*Denial of Control, T0813*）が異なる Victim に対して 2 件検出された．同一の Adversary（MAC）が複数資産に作用した事実が，A と V の組で明示されている．

以上より，各イベントは運用ログの内容を $\{A, C, I, V, \mathrm{sr}, \mathrm{ttp}\}$ に動的に写像でき，規格要求単位の統一化表現として拡張ダイアモンドを個別に生成できることを確認した（課題 1）．

結果 2：リスクとコンプライアンス連携の体系化

結果 1 で得られた 7 個の拡張ダイアモンド $\mathcal{D}$ をノードとして，戦術順序条件 π と共有属性条件 Φ を満たす対のみに辺を付与したところ，**図 6** に示す 28 ノードからなる連鎖ダイアモンドモデルが生成され，共有ノードは 7 個に集約された．各ノードは sr ラベルを保持するため，連鎖全体を IEC 62443 の 7 つのカテゴリに属する要件単位で追跡できる．

シナリオ 1 では，`SR 1.11`→`SR 2.8`→`SR 3.1`→`SR 3.2` の線形連鎖が復元され，それぞれ *T0806*（*Credential Access*）→ *T0878(Defense Evasion)* → *T0856*（*Initial Access*）→ *T0851*（*Collection*）に対応した SR/TTP の動的マッピングが確認できた．実際，表 4 では同一 `Victim`（例：`172.16.192.162`）や継続する `Adversary`（例：`172.16.192.131`）が複数の SR に跨って観測され，単一シナリオ内の連続活動として自然に解釈できる．

シナリオ 2 は，`SR 7.2`（*T0840; Discovery*）から，同一 Adversary を共有する `SR 7.1`（*T0813; Impact*）の二分岐が形成され，単一攻撃能力の他資産への波及が SR ラベル付きで可視化された．これにより，可用性要件群（7.x）の中で Impact 側を優先是正として抽出できる．以上より，結果 1 で得た個々の拡張ダイアモンドを $\pi \cdot \Phi$ に基づき連鎖化しつつ SR ラベルを維持することで，実運用ログから因果・時系列を保ったリスクの SR へのマッピングが可能であることを示した（課題 2）．

表 4　IDS アラートログに基づく IEC 62443 SR 別拡張ダイアモンドモデル・マッピング結果

SR	Adversary	Infrastructure	Capability	Victim	ATT&CK	Phase
SR 1.11	IP:172.16.192.101 MAC:00:0c:29:32:01:eb	SMB	Brute-force Attempts	IP:172.16.192.161 MAC:00:50:56:8b:d4:5e	Brute Force（T0806）	Credential Access
SR 2.8	IP:172.16.192.254 MAC:00:0c:29:62:ba:c4	SMB	New Link Group	IP:172.16.192.162 MAC:00:50:56:8b:6d:7b	Alarm Suppression（T0878）	Defense Evasion
SR 3.1	IP:172.16.192.131 MAC:00:50:56:8b:0a:58	Other	Spoofed Command	IP:172.16.192.162 MAC:00:50:56:8b:6d:7b	Spoof Reporting（T0856）	Initial Access
SR 3.2	IP:172.16.192.131 MAC:00:50:56:8b:0a:58	Other	Data Exfiltration	IP:172.16.192.162 MAC:00:50:56:8b:6d:7b	Automated Collection（T0851）	Collection
SR 7.1	IP: N/A MAC: 00:50:56:8b:2d:03	N/A	MITM Attack	IP: 172.16.192.52 MAC: N/A	Denial of Control（T0813）	Impact
		N/A	MITM Attack	IP: 172.16.192.100 MAC: N/A	Denial of Control（T0813）	Impact
SR 7.2	IP:172.16.192.101 MAC:00:0c:29:32:81:eb	N/A	Network Scan	IP: N/A MAC: N/A	Network Sniffing（T0840）	Discovery

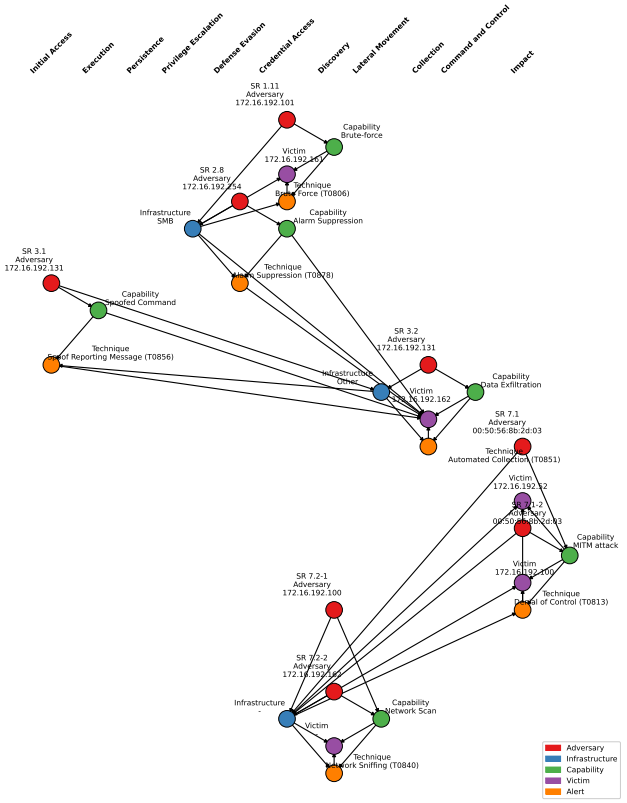

図 6　連鎖ダイアモンドモデル

5. 議論

5.1 連鎖再構成に基づく是正要件

シナリオ 1 の連鎖は攻撃者と被害対象が固定されたまま線形的に進行するため，波及や分岐は見られない．このような場合，侵入の初期段階を抑止することが最も効果的である．従って，優先是正は上流の SR 1.11（認証強化）および SR 2.8（監査イベント）で，当該要件を抑えることで後段の発生確率を下げられる可能性がある．

シナリオ 2 の連鎖は扇状の波及を示し，同一 Adversary ノードを中心に複数 Victim に広がる．末端は Impact に対応する SR 7.1 ノード群であり，ここが被害顕在化点である．優先是正は中心／分岐点の抑制と，プロトコル面の強化により，Impact 手前で波及を止められる可能性がある．

以上のように，提案手法では $\pi + \Phi$ により誤連結を抑えつつ「線形か波及か」と「中心ノード」が明確化されるため，どこを重点的に是正すべきか（シナリオ 1 では SR 1.11/2.8，シナリオ 2 では SR 7.1 近傍と分岐点）が図 6 から直観的に読み取れる．

5.2 実環境への適用

今回の評価では，精度面で課題 1 や課題 2 を解決しうることを確認した．他方で，実環境への適用に際しては，処理時間が実利用の範囲に収まっているか否かも重要な要素である．提案手法は，観測窓 W やしきい値 τ の設定に結果が感度を持ち，計算量は $O(|\mathcal{D}|^2)$ で増加するため，中規模を超える環境では，計算量並びに処理時間が長大化する可能性も考えられる．ただし，ブロッキングやインデクシング等を用いて高速化することによって，実利用の範囲に収めることが可能であると推察される．

5.3 制限事項

提案手法はネットワーク型 IDS のアラートを基盤としており，観測範囲は通信経路に限定される．そのためホスト内部のログや設定差分，物理プロセスの異常値は直接扱えないが，これらを統合することで精度やカバレッジの向上が期待できる．また，ある SR に対応するアラートが得られない場合（$\mathcal{A}_{sr} = \emptyset$）は N/A として扱うが，これは不可観測事象の排除ではなく，観測可能な範囲でのトレーサビリティを確立する意図である．本手法がカバーするのは IDS で検知可能な要件に限られ，構成管理や物理的防護などは現状対象外である．さらに，$R(sr)$ はベンダ提供ルー

ルに依存するため，他環境へ適用する際にはルール移植が前提となり，連鎖判定も戦術順序 π と共有属性 Φ に基づくため，NAT やアドレス再利用環境では誤結合や結合漏れが生じ得る．ただし，本研究ではブルートフォース攻撃と中間者攻撃という代表的なシナリオを通じて有効性を確認しており，今後は異種データや多様な攻撃事例を取り込むことで，更に実運用に即した評価基盤へ発展可能であると考えられる．

6. おわりに

本研究では，重要インフラにおける GRC 対応の高度化を目的に，(i) 実運用ログに基づく動的リスク評価，及び (ii) リスクと規格規格要件との体系的な連携を同時に実現する枠組みを提案した．具体的には，IEC 62443 に準拠したクエリによるログ抽出，拡張ダイアモンドモデルの構築，戦術順序と共有属性に基づく連鎖モデルの生成という 3 ステップからなるフレームワークを定式化し，実際の攻撃シナリオを用いてその有効性を検証した．評価実験では，総当たり攻撃と中間者攻撃の 2 シナリオにおいて，IDS ログから得られたアラートを拡張ダイアモンドモデルに動的に変換し，攻撃の進行過程を IEC 62443 の SR と ATT&CK の TTP に対応付けて可視化することで，(i) リスクの評価の高度化，及び (ii) リスクと規格要件の体系的な連携手法を実現した．これにより，実際の侵害順序に基づく優先是正要件の抽出が可能となり，GRC 対応の実効性を向上させる手法としての有用性が示された．今後は，IDS 以外のデータソースとの統合，多様な攻撃事例への適用を通じてより実運用に即した GRC 評価基盤の構築をめざす．

参考文献

[1] Bindra, A.: Securing the Power Grid: Protecting Smart Grids and Connected Power Systems from Cyberattacks, *IEEE Power Electronics Magazine*, Vol. 4, No. 3, pp. 20–27 (2017).

[2] Beerman, J. et al.: A Review of Colonial Pipeline Ransomware Attack, *Proc. of the IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, pp. 8–15 (2023).

[3] Simone, S., Masti, D. and Lun, Y. Z.: Railway Cyber-Security in the Era of Interconnected Systems: A Survey, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 24, No. 7, pp. 6764–6779 (2023).

[4] Wiesche, M. et al.: Patterns for Understanding Control Requirements for Information Systems for Governance, Risk Management, and Compliance (GRC IS), *Advanced Information Systems Engineering Workshops*, pp. 208–217 (2011).

[5] Racz, N. et al.: IT Governance, Risk & Compliance (GRC) Status Quo and Integration: An Explorative Industry Case Study, *Proc. of the 2011 IEEE World Congress on Services*, pp. 429–436 (2011).

[6] Racz, N. et al.: A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC), *Proc. of the IFIP Advances in Information and Communication Technology*, Vol. 330, Springer, pp. 106–117 (2010).

[7] Force, J. T.: Risk management framework for information systems and organizations, *NIST Special Publication*, Vol. 800, p. 37 (2018).

[8] Hsu, C. et al.: The Impact of ISO 27001 Certification on Firm Performance, *Proc. of the 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 4842–4848 (2016).

[9] Björn, L., Čaušević, A. and Hansson, H.: Applicability of the IEC 62443 Standard in Industry 4.0/IIoT, *Proc. of the 14th International Conference on Availability, Reliability and Security (ARES)*, pp. 1–8 (2019).

[10] Ghaeini, H. R. et al.: State-Aware Anomaly Detection for Industrial Control Systems, *Proc. of the Security Track at the ACM Symposium on Applied Computing (SAC)*, p. 1620–1628 (2018).

[11] Ahmed, M. et al.: MITRE ATT&CK-driven Cyber Risk Assessment, *Proc. of the 17th International Conference on Availability, Reliability and Security (ARES)*, pp. 1–10 (2022).

[12] Hollerer, S. et al.: Risk Assessments Considering Safety, Security, and Their Interdependencies in OT Environments, *Proc. of the 17th International Conference on Availability, Reliability and Security (ARES)*, pp. 1–8 (2022).

[13] Göttel, C. et al.: Qualitative Analysis for Validating IEC 62443-4-2, *Proc.2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA)*, pp. 1–8 (2023).

[14] Zahid, S. et al.: Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls, *Internet of Things*, Vol. 22, p. 100766 (2023).

[15] Da Silva, M. et al.: Safety-security convergence: Automation of IEC 62443-3-2, *Computers & Security*, Vol. 156, p. 104477 (2025).

[16] Alexander, O. et al.: MITRE ATT&CK for industrial control systems: Design and philosophy, *The MITRE Corporation: Bedford, MA, USA*, Vol. 29, pp. 21–85 (2020).

[17] Caltagirone, S. et al.: The Diamond Model of Intrusion Analysis, Technical Report TR-2013-01, Center for Cyber Intelligence Analysis and Threat Research (2013).

[18] Kousei, S. et al.: Designing a Security Support System for Industrial Control Systems Powered by Generative AI, *Proc. of the 2025 Symposium on Cryptography and Information Security (SCIS)* (2025). 4G1-3 (in Japanese).

[19] LangChain Contributors: `https://github.com/langchain-ai/langchain` (2025). Accessed: August 18, 2025.

[20] Ma, X. et al.: Query Rewriting in Retrieval-Augmented Large Language Models, *Proc. of the 2023 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pp. 5303–5315 (2023).

[21] Wei, J. et al.: Chain-of-Thought Prompting Elicits Reasoning in Large Language Models, *Proc. of the 36th International Conference on Neural Information Processing Systems(NIPS)*, Vol. 35, pp. 24824–24837 (2022).

[22] NozomiNetworks: ISA/IEC 62443 Content Pack, `https://ja.nozominetworks.com/blog/new-release-isa-iec-62443-content-pack` (2023). Accessed: 2025-08-22.