

サプライチェーンセキュリティ(SCS)に関する ダブルループ・フレームワークの提案

神橋 基博†

概要：近年、サプライチェーン攻撃の増加に加え、フロンティア AI の発展によってサイバー攻撃の速度と規模が拡大している。また、認証情報の漏えいによるアカウント乗っ取りが常態化し、正当な権限を持つアクターによる不正行為への対応が重要な課題となっている。さらに、Society 5.0 や Cyber-Physical Systems (CPS) の進展により、企業、サービス、IoT 機器、API などが複雑に接続されたサプライチェーン全体の安全性確保が求められている。本稿は、こうした課題に対応するため、サプライチェーンセキュリティ (SCS) に関する「ダブルループ・フレームワーク」を提案する。提案モデルは、個々のアクターが検知・制御を行う「マイクロループ」と、サプライチェーン全体で脅威情報を共有し、不正アクターの排除と信頼維持を行う「マクロループ」から構成される。さらに、SCS 標準メッセージ、ゼロトラストに基づく動的アクセス認可、SCS ビザンチン耐性を主要概念として提示し、事例を通じて有効性を考察した。併せて、技術・組織、経済、制度の各側面から今後の研究課題を整理した。本研究は、従来の事前審査中心の静的な SCS を拡張し、サプライチェーン全体のサイバーレジリエンスを向上するための枠組みを提示するものである。

キーワード：サプライチェーン、サイバーレジリエンス、NIST SP 800-18

A Double-Loop Framework for Supply Chain Security (SCS)

MOTOHIRO KAMBASHI†

Abstract: Recent advances in frontier AI have accelerated the speed and scale of cyberattacks, while credential theft and account hijacking have become increasingly common. At the same time, the emergence of Society 5.0 and Cyber-Physical Systems (CPS) has created highly interconnected supply chain ecosystems consisting of enterprises, services, IoT devices, and APIs, requiring security governance beyond organizational boundaries.

This paper proposes a Double-Loop Framework for Supply Chain Security (SCS). The framework consists of a Micro Loop, which enables individual actors to continuously monitor and control suspicious activities, and a Macro Loop, which shares threat information across the supply chain to identify malicious actors and maintain collective trust.

The framework consists of three key concepts: SCS Standard Messages, Zero Trust-based Dynamic Access Authorization, and SCS Byzantine Fault Tolerance. In addition, this paper outlines future research issues from technological, organizational, economic, and institutional perspectives. This study extends conventional static SCS approaches and provides a framework for enhancing cyber resilience across the entire supply chain.

Keywords: Supply Chain, Cyber Resilience, NIST SP 800-18

1. はじめに

1.1 研究の背景

近年、サイバー攻撃の手法は高度化・巧妙化の一途を辿っており、単一の企業や組織の境界防御のみで自社の情報資産や事業継続性を保護することは極めて困難となっている。特に、セキュリティ対策が相対的に手薄な関連企業、委託先、クラウドサービス、あるいはソフトウェアサプライチェーンを経由して標的組織へ侵入する「サプライチェーン攻撃」が増加しており、サプライチェーン全体を通じたサイバーセキュリティ (SCS: Supply Chain Security) の確保が重要な課題となっている。

さらに近年は、大規模言語モデル (LLM) を中心とするフロンティア AI の発展により、攻撃者側の能力も大きく向上し、従来よりも短時間かつ大規模な攻撃が実行可能となる。この結果、防御側がインシデントを認識し対応するま

での時間的猶予は急速に縮小している。

加えて、認証情報 (ID・パスワード) の流出とアカウント乗っ取りも常態化している。攻撃者は流出した認証情報を利用して正規の利用者になりすますことができるため、従来のアクセス権限管理や境界防御のみでは検知・遮断が困難である。

したがって、現代の SCS においては、従来の対策に加えて、正規の権限が悪用されていることを前提とし、利用者の挙動そのものを継続的に監視・評価する新たなセキュリティの枠組みが必要である。

1.2 サプライチェーンセキュリティ (SCS) の範囲拡大

Society 5.0 や Cyber-Physical Systems (CPS) で提唱されているように、現代では、多様かつ多数の組織、サービス、IoT/OT 機器、API などが物理空間とサイバー空間を跨いで

† 学校法人岩崎学園 情報セキュリティ大学院大学 客員講師

相互に動的に接続し続けるエコシステムを形成している。後藤（2024）が指摘するように、現代社会のサプライチェーンはそれ自体が複数のシステム・組織にまたがる巨大なCPSを形成しており、デジタルネットワークを通じた高度な連携が進む一方で、サプライチェーン固有のリスクとして、保守時の不正機能混入やOSSの脆弱性といった一箇所が発生したリスクが正当な流通・更新機構を介してサプライチェーン全体へ拡散する「汚染」、サプライチェーン内の事業者における事業継続性の喪失が取引関係を通じて川上・川下へ連鎖的な事業停止を波及させる「寸断」が指摘されている。[1]

また、石島（2021）が指摘するように、Society 5.0におけるCPSの拡大はサイバー攻撃の機会と防衛範囲の急激な拡大をもたらしており、サプライチェーン全体の連携と継続性に注目し、防衛技術面を含めた認証制度を構築し、運用するとともに、リアルタイムな監視・対応体制を構築することが必要である。[2]

本稿では「アクター (Actor)」を、物理空間とサイバー空間が融合したCPS環境下において、ネットワークを介して相互に接続し、作用し合う全ての主体を指す総称として定義する。具体的には、製品・サービスのライフサイクル全般に関わる事業体、各事業体のシステム間を連携・結合させるAPIやプラットフォームなどのサービス、およびそれらにアクセス権を持って介在する従業員や外部ベンダーなどの利用者を内包する。

また、本稿における「サプライチェーン」とは、多種多様なアクターが、製品・サービスのライフサイクル全般でデジタルネットワークを通じて相互接続し、最終顧客にサービスを提供し続けるCPSを意味する。

1.3 本稿の目的と構成

本稿は、SCSを取り巻く課題に対し、「ダブルループ・フレームワーク」を提案する。

本フレームワークは、図1に示すようにサプライチェーンに属する個々の組織内でゼロトラストに基づく動的アクセス制御と即時回復を担う「マイクロループ」と、エコシステム全体で異常情報を共有し不正アクターの排除と信頼維持を担う「マクロループ」から構成される。本稿ではその基本構造と主要コンセプトを示すとともに、実現に向けた課題を整理する。

第2章では従来型SCSの限界、第3章では提案するフレームワークの概要、第4章では中核となる概念、第5章では事例分析、第6章では今後の研究課題を述べる。

2. 従来のSCSとその限界

2.1 従来のアプローチ (Static SCS)

従来のサプライチェーンセキュリティ (以下、「Static SCS」

と呼ぶ)におけるリスク管理は、主にシステムや製品の調達時、開発時、または定期的な監査時といった特定時点における状態を検証するアプローチが中心となっていた。

具体的には、ソフトウェア構成要素の可視化と脆弱性管理を目的としたSBOM (Software Bill of Materials) の導入、開発パイプラインにおける安全性を担保するCI/CD (Continuous Integration / Continuous Delivery) の管理、ならびに政府や業界団体が定める各種セキュリティガイドライン (ISMAP、NIST SP 800-171/161 等) に基づく基準適合性審査や事前評価制度 (チェックリスト型の自己評価や第三者認証) が挙げられる。

これらのアプローチは、製品や組織が満たすべきセキュリティ要件を規格化・標準化し、調達や契約、開発のプロセスにおいて一定の客観的な基準を提供するという点において、セキュリティ水準向上に貢献してきた。

2.2 制度的・技術的な課題

しかしながら、こうした特定時点の評価に基づくStatic SCSには、以下3点の困難が生じている。

第一に、継続的監視の欠如である。事前の評価や定期審査は、あくまで評価を実施した時点あるいは期間の適合性を保証するものに過ぎない。製品出荷後やシステム運用開始後に新しく発見される未知・既知の脆弱性、あるいは運用中の設定ミスや不正な設定変更といったインシデントを未然防止することは不可能であり、NISC(2025)が指摘するように、セキュリティ対策は導入して終わりではなく、常に対策を継続することが重要である。[3]

また、NIST(2026)が公開したガイド(NIST SP 800-12r2)では、サイバーサプライチェーンリスク管理(C-SCRM)をシステムライフサイクルで統合的に管理し、継続的モニタリング(Continuous Monitoring)を確立することを求めている。[4]

第二に、自己評価・第三者評価におけるインセンティブの歪みである。調達基準への適合が契約継続や受注の条件となる場合、受注者側にはセキュリティ上の問題やインシデント、基準未達を隠蔽・矮小化して報告するインセンティブが働く。さらに実務においては、厳格な第三者評価が中堅・中小の受注者に多大な負担を強いるというトレードオフが存在する。このように、複雑なサプライチェーンでは、受注企業への過度な負担と、発注企業における実効性の不透明さを生み出しており、結果としてサプライチェーン全体のレジリエンスを阻害する構造的要因となっている。

(NISC, 2025)

第三に、組織間連携の欠如である。従来の制度は主に1対1の委託・受託関係を前提として構築されており、サプライチェーン内の特定の1社で異常が検知された場合、そのリスク情報をサプライチェーン全体で共有し防御する仕組みが整っていない。

2.3 「正当な権限の悪用」への対応の困難さ

第1章で述べた通り、Static SCS は正規の権限を悪用するアクターへの対処が困難である。Static SCS は、事前の適合審査や認証に対する全面的な信頼に依拠しており、正規のAPI や権限を行使したデータの改ざん（データ汚染）や踏み台攻撃を実行する場合、そのシステムアクセス自体は正当な手続として処理される。そのため、いくら審査や認証を厳格にしても、運用中にアクターが正規の権限を悪用して行う不正な挙動（Behavior）をリアルタイムに検知し、即座に制御することは原理的に不可能である。

以上の理由から、特定時点の状態を評価・事前審査する既存の Static SCS に加えて、運用中のアクターの挙動と証拠に基づき継続的かつ動的にアクセス制御・ガバナンスを行うためのフレームワークが必要となる。

3. サプライチェーンセキュリティ（SCS）フレームワークの提案

3.1 フレームワークの全体像（ダブルループ構造）

前章で論じた通り、現代のサプライチェーンにおいては、特定時点の状態評価（Static SCS）のみでは、正規の権限が悪用される脅威に対処できない。この課題を解決するため、本研究ではサプライチェーンセキュリティ（SCS）に対する「ダブルループ・フレームワーク」を提案する。

本フレームワークは、図1に示す通り、個々の組織が動的かつリアルタイムに防御を行う「マイクロループ（Micro Loop）」と、サプライチェーン全体におけるレジリエンス向上を目指す「マクロループ（Macro Loop）」の2つの相互作用ループによって構成される。

マイクロループでは、各企業やシステムの現場レベルにおいて、アクセスしてくるアクターの挙動をリアルタイムに評価・制御するループである。

マクロループでは、マイクロループで発生した検知情報や証

拠を集約し、サプライチェーン全体としての信頼スコアを更新し、リスクの高いアクターを排除するループである。この2つのループが連携することで、現場での局所的・即時的なリスクコントロールと、サプライチェーン全体でのサイバーレジリエンス向上を目指す。

3.2 ミクロループ：個別企業による自律的・動的防御

マイクロループの主たる目的は、自社のシステム境界内において「正規の認証情報を有するアクターであっても完全には信頼しない」というゼロトラスト原則に基づき、動的なアクセス制御と即時的な機能回復を実現することである。マイクロループは、以下の4つの連続するステップによって構成される。

(1) 監視（Monitor）：

アクターによるアクセス試行、API 呼び出し、データ転送量等の挙動をリアルタイムかつ継続的に監視・集積する。

(2) 検知（Detect）：

集積されたデータに基づき、アクターの通常時の振る舞いからの逸脱や異常なアクセスといった兆候を検知する。

(3) 制限（Restrict）：

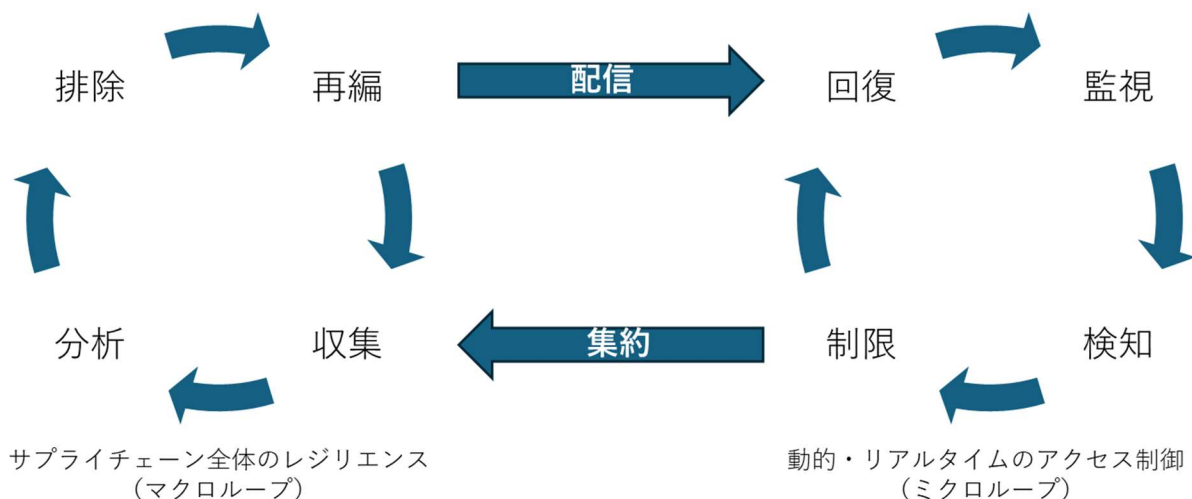
兆候が検知された場合、事前に設定されたリスクレベルに応じてアクセス権限の縮小、追加認証の要求、あるいはセッションの即時遮断といったアクターへの制御を自動的に実行し、影響の極小化を図る。

(4) 回復（Recover）：

制御されたアクターに対し、現実の利用者や企業への照会、アクセスログの詳細分析等から検証する。問題無いことが判明すればアクターへの制御を解除する。

マイクロループの最大の特徴は、認証情報や第三者報告書といった事前に評価されたアクターの属性に依存せず、運用中の実際の挙動に基づいてリアルタイムにアクセス制御を更新する点にある。

図1：ダブルループフレームワークの全体像



3.3 マクロループ：エコシステム全体のガバナンス

ミクロループが個別企業での即時防御を担うのに対し、マクロループはサプライチェーン全体のベースラインを維持する。単一の組織で検知された局所的な異常をサプライチェーン全体で共有・分析し、潜在的な脅威や不誠実なアクターを排除することで、サプライチェーン全体の信頼性を継続的に保証する。

マクロループは、以下の4つの連続するステップによって構成される。

(1) 収集 (Collect) :

各企業のミクロループで検知された兆候および検証可能な証拠(アクセスログ等)を、標準化されたメッセージプロトコル(第4章参照)を介して集約する。

(2) 分析 (Analyze) :

集約された兆候および証拠を相関的に分析し、それが広域的な攻撃の予兆か、あるいは特定アクターの乗っ取りや悪意を持った行動(虚偽報告等)かを判定する。

(3) 排除 (Exclude) :

分析の結果に基づき、問題のあるアクターをサプライチェーンから信頼スコアの引下げやブラックリスト化によって、論理的に切り離し、リスクの顕在化を防止する。

(4) 再編 (Reconfigure) :

問題のあるアクターの排除に伴い、影響を受けるビジネスプロセスや代替の調達ルート・サービスに切り替え、サプライチェーン全体を最適化する。

3.4 ミクロ・マクロループの相互作用

本フレームワークの価値は、ミクロループとマクロループがデータを循環させる相互作用にある。

個々の企業のミクロループで検知された脅威情報はマクロループに集約される。マクロループにおける分析結果は、信頼スコアの更新や警戒レベルの変更として、サプライチェーンを構成するすべてのアクターのミクロループに配信される。これにより、ある一社が遭遇した未知の脅威やインシデントに関する情報が、他社における事前防御のために活用されることで、サプライチェーン全体のサイバーレジリエンスの強靱化を可能にする。

4. フレームワークを支えるキーコンセプト

異種多様な企業やシステムが連携するサプライチェーンにおいて、前章で提案したSCSダブルループ・フレームワークを機能させるためには、フレームワークを支える技術的・概念的な基盤が不可欠である。本章では、本フレームワークの核となる3つのキーコンセプトについて詳述する。

4.1 SCS メッセージ標準化と自動防御連鎖

サプライチェーン全体のマクロループによる迅速な集団防御を実現する上での最大の課題は、各企業が導入しているセキュリティ製品(EDR、IDS/IPS、WAF、SIEM等)や管理システムのアラート形式およびログ構造が統一されていないことにある。このために、従来は人手を介した定型連絡や手作業での影響評価に頼らざるを得ず、被害拡大のスピードに対処できていなかった。本フレームワークでは、一社で検知された障害やインシデントの予兆をサプライチェーン全体で即時に共有・自動処理を可能とするため、「SCS 標準メッセージ (SCS Standard Message)」のプロトコルおよびデータフォーマットを検討する。

SCS 標準メッセージは、主に以下の4点で構成される。

(1) アクター識別子

異常な挙動や攻撃の送信元として特定されたアクターをサプライチェーン内で識別するための情報

(2) イベント類型

検知された異常・予兆の分類(寸断、データ汚染・改ざん、不正利用など)

(3) 証拠データ

検知されたイベントの根拠となるログ、あるいは通信データを特定可能な情報(電子署名、ハッシュ値など)

(4) 推奨アクション

検知されたイベントに対して推奨される対処(即時遮断、追加認証、監視強化、要照会など)

本メッセージ構造の導入により、サプライチェーン内のあるアクターで異常・予兆が検知された際に、その情報をサプライチェーン内の他のアクターへ共有するとともに、メッセージを受信した各社では、人間による判断を介さず、後述する動的認可メカニズムを用いて、自動的にアクセス制限や遮断を実行する。これにより、サプライチェーン全体での迅速な脅威の共有と対処を可能とする。

4.2 ゼロトラストに基づく動的アクセス認可

従来のアクセス制御は、認証成功時に固定的なアクセス権限を付与し、セッション終了までその権限を保持し続ける静的な許可が主流であった。しかし、不正利用や内部不正に対処するには、セッション継続中であってもアクターの挙動に応じてリアルタイムに権限を制限・変更するメカニズムが必要となる。本フレームワークにおけるミクロループでは、ゼロトラスト原則に基づく動的アクセス認可(Dynamic Access Authorization)を導入する。これにより、ビジネスの継続性への影響を抑えつつ、リスクレベルに応じた権限制御を可能とする。具体的には、ミクロループでの検知結果およびマクロループから配信される信頼スコアに基づき、アクターのリスク評価を行い、以下の4段階のアクセス制御ポリシーを適用する。

・ **Level 1 (通常運用)**

正常と判定されたアクターに対し、認可されているサービスやデータへのアクセスを通常通り許可する。

・ **Level 2 (注意・追加認証)**

挙動への不審点や通常と異なるパターンが検知された場合、データの更新操作や重要領域へのアクセス時に多要素認証やステップアップ認証といった認証を要求する。

・ **Level 3 (警戒・隔離)**

高いリスクが懸念される挙動を示した場合、アクターのアクセスを即座に隔離環境 (サンドボックス) へ誘導し、ダミーデータを返却することで被害を防止しつつ攻撃者の挙動を観察・記録する。

・ **Level 4 (危険・即時遮断) :**

乗っ取りや明確な攻撃行動が確定した場合、アクティブな接続を即時破棄しアクターからのアクセスを遮断する。

この段階的な制御により、過剰な一律遮断による業務停止リスクを回避しつつ、高リスクなアクターを迅速に封じ込めることが可能とする。

4.3 SCS ビザンチン耐性

多種多様なアクターによって構成されるサプライチェーンでは、全てのアクターが常に正しい情報を誠実に報告するとは限らない。自社への攻撃や被害を隠蔽しようとする非協力的なアクター、あるいは自身の受注維持や競合排除を目的に虚偽のアラートや偽装情報を送信する悪意あるアクターが存在する可能性がある。不完全かつ不誠実な情報源が混在する環境下において、サプライチェーン全体として正当な合意に到達する課題は、計算機科学における「ビザンチン将軍問題 (Byzantine Generals Problem)」に帰着できる。本フレームワークでは、この問題に対処するため、ブロックチェーン等で用いられるビザンチン障害耐性 (BFT: Byzantine Fault Tolerance) の概念をサプライチェーンに応用した「SCS ビザンチン耐性メカニズム」を提案する。本メカニズムは、以下の3要素によって構成される。

(1) **多角的検証**

単一のアクターからの報告のみに依存せず、複数の独立したアクターから出力される通信ログや、外部の観測ポイントから収集したデータを統合し、相関分析を行う。

(2) **重み付け合意形成**

各アクターからの情報を集約する際に、アクター毎の過去の協力実績や証拠提供度に基づき、情報の重み付けを行う。

(3) **非協力へのペナルティ**

多角的検証により実態と異なる報告が判明したアクターに対しては、重み付け合意形成における情報の重み付け (信頼スコア) を低下させる。信頼スコアが一定以下となった場合、サプライチェーンからの隔離や取引停止といった明確なペナルティを課す。

これらのビザンチン耐性メカニズムの導入により、サプライチェーンに対して、不誠実な報告を行うインセンティブを経済的・システムの排除し、一部に乗っ取られたアクターが含まれる環境下であっても、サプライチェーン全体の合意形成と信頼性を維持することを可能とする。

5. 事例研究からの示唆

本章では、前章までに提案した SCS ダブルループ・フレームワークの社会実装における実現可能性を検討するため、すでに類似の運用が行われている2つの事例を取り上げ、そのメカニズムと本提案への示唆を分析・考察する。

5.1 SWIFT-CSP におけるセキュリティ評価の一元管理

5.1.1 事例の概要

国際金融取引の基盤である SWIFT (国際銀行間通信協会) は、加盟金融機関を標的としたサイバー攻撃の急増に対応するため、セキュリティプログラム (SWIFT-CSP: Customer Security Programme) を展開している。SWIFT-CSP では、すべての加盟金融機関に対して必須のセキュリティ管理策 (CSCF: Customer Security Controls Framework) への準拠を義務付けており、さらに年に一度、独立した第三者による評価結果の報告を求めている。

SWIFT-CSP の最大の特徴は、SWIFT というプラットフォーム提供者が全加盟金融機関の評価結果を一元的に管理されたプラットフォームに集約し、他の金融機関や各国の監督官庁・中央銀行が閲覧可能にしている点にある。

5.1.2 本フレームワークへの示唆

従来の静的ガイドラインに基づくセキュリティフレームワークでは、誰が評価結果の信頼性を担保し、サプライチェーン内で管理・共有するのかという運用・ガバナンス主体の議論が十分でなかった。

SWIFT-CSP の事例は、サプライチェーン全体を統括するプラットフォーム事業者が、各アクターのセキュリティ評価結果を集約し、各国の金融規制当局と共有することで、信頼性を確保する。これは、本フレームワークにおけるマクロループ運用主体の具体的な設計に対して示唆を与えるものである。

5.2 クレジットカード決済における事前審査と事後評価

5.2.1 事例の概要

クレジットカード決済では、リアルタイムに近い事前審査と事後の不正排除が組み合わされた不正利用対策のメカニズムが確立されている。

(1) オーソリ (Authorization)

クレジットカード加盟店は、決済処理が発生すると専用端末からクレジット会社に照会する。クレジット会社は過去の取引履歴などから、一定時間内にその要求を承認するか

を判定し、回答する。

(2) チャージバック (Chargeback)

事前照会を通過して取引が完了した後であっても、クレジットカード会社による事後検証で不正利用や不備が発覚した場合、決済を遡及して取り消し、悪質な場合には不正利用者の口座凍結や加盟店契約の解除を実行する。

5.2.2 本フレームワークへの示唆

クレジットカード決済におけるオーソリとチャージバックは、本フレームワークのマイクロループとマクロループの相互作用を表している。

すなわち、オーソリは正規の利用者であっても不正利用の兆候や疑いがあれば利用を制限するというマイクロループの実装モデルであり、チャージバックは事前検証を切り抜けた不正利用を事後的に捕捉し、ペナルティを科すというマクロループの実装モデルに対応する。

この事例は、静的なホワイトリスト（事前認可）に依存せず、利用時の判定（マイクロ）と結果責任に基づく事後的排除（マクロ）を組み合わせることが、ビジネスの速度を落とすことなくサプライチェーン全体の信頼性を維持するために不可欠かつ有効であることを示唆している。

5.3 事例からの考察とフレームワークの独自性

以上の事例より、本稿で提案するダブルループ・フレームワークは、金融・決済領域において既に実現されているメカニズムと整合性を有することが確認できる。

しかしながら、一般的なサプライチェーンは、金融・決済領域と異なり単一の強力なプラットフォーム事業者（SWIFT 等）が存在しない、データや API 接続の形態が極めて多種多様であるという構造的な違いが存在する。

したがって、提案フレームワークを一般的なサプライチェーンへ適用するためには、前章で述べた SCS メッセージの標準化、動的アクセス認可、SCS ビザンチン耐性といったキーコンセプトを組み込むことが必要であり、この点に本研究の学術的独自性がある。

6. 今後の研究課題

本論文で提案した SCS ダブルループ・フレームワークは、従来の一時点・静的な評価制度（Static SCS）に、動的なサイバーレジリエンスを追加するものである。しかしながら、本フレームワークを多様なアクターが複雑に交錯する実際のサプライチェーンに実装するためには、解決すべき学術的・実務的な課題が残されている。本章では、これらの課題を技術、経済、制度の3つの側面から検討し、今後の研究課題として提示する。

6.1 技術・組織的課題

(1) 動的アクセス制御アルゴリズムと過検知の抑制

第4章で述べた動的アクセス認可を実装する上では、アクターの通常の挙動と異常な挙動を判別する精度が重要となる。特に、業務プロセスの急な変更や繁忙期のトラフィック増大を乗っ取りやデータ汚染と誤検知した場合、正当な業務が自動遮断され、事業継続に直接的な支障をきたすリスクがある。

したがって、過検知による業務影響を最小化しつつ高度な脅威を検知する、過酷な環境に耐えうるアルゴリズムおよび適応型学習モデルの開発が必要となる。

(2) サプライチェーン共同 SOC の設計と運用

マクロループを機能させるためには、個別の企業を超えて脅威情報や証拠を集約・分析するサプライチェーン共同 SOC（Security Operations Center）、あるいは分散型の集約・分析基盤が必要となる。

しかし、異種多様な組織間でのデータ統合運用においては、リアルタイムでデータ集約するための技術的課題に加えて、運用コストの分担、高度なセキュリティ人材の確保といった組織的な課題が存在する。AI 技術の活用を含め、実効性のある技術・組織モデルに研究が求められる。

6.2 経済的課題

(1) 誠実な情報共有のためのインセンティブ設計

マクロループにおけるサイバーレジリエンスは、各アクターがマイクロループで検知したインシデントや異常の兆候を遅滞なくサプライチェーン全体へ共有することによって成り立つ。しかし、現実のビジネス環境においては、自社で発生したインシデントの公表や不都合な情報の共有は、レピュテーションリスクの低下や取引停止、法的責任の発生といった不利益を招くため、企業が報告を躊躇・隠蔽するディスインセンティブが働く恐れがある。

この課題に対し、第4章で提案した SCS ビザンチン耐性に基づくペナルティに加え、誠実な情報共有を行った企業に対する経済的インセンティブを組み合わせるメカニズムに関する研究が必要となる。

(2) サプライチェーン全体におけるリスク分散

大企業と比較して資金的・人材のリソースが限られる中小企業にとって、高度なマイクロループを導入・維持することは経済的負担が大きい。サプライチェーン全体としてのセキュリティ水準を担保するためには、全てのアクターでリスクとコストを相扶共済的に分散するための共済制度や共通プラットフォームの提供など、持続可能な経済構造に関する研究が必要となる。

6.3 制度的課題

(1) 異常検知時における即時遮断の法的正当性

マイクロループまたはマクロループでの判断に基づき、特定

のアクターのアクセスを即時遮断する行為は、契約上・業務上の供給義務違反や損害賠償請求のリスクを伴う。とりわけ、誤検知によって正当なアクターを過剰に排除してしまった場合（いわゆる「冤罪」）、当該遮断行為の法的な正当性や損害の帰属・免責範囲が争点となると考えられる。したがって、事前契約（SLA）における即時遮断条項の標準化や、安全配慮義務・自衛権の観点からの法制度面での整理・ガイドラインの策定が必要となる。

(2) 不服申立ておよび救済手続きの確立

マクロループにおいて信頼スコアが低下し、サプライチェーンから排除されたアクターが、自らの潔白やセキュリティのリカバリー（復旧・是正）を客観的に証明し、再びサプライチェーンに再参加するためには、透明性の高い不服申立て・救済手続きの制度設計が必要となる。この手続きが確立されない場合、不当な排除や不可逆的な取引停止による訴訟の頻発など、サプライチェーン全体の健全性が損なわれる恐れがある。

謝辞

本稿の執筆にあたり、情報セキュリティ大学院大学 セキュアシステム研究所 (SSL) の重要産業のサプライチェーンリスクにおけるアジャイルガバナンス プロジェクトメンバー各位には貴重なご助言をいただきました。心より感謝いたします。

参考文献

- [1] 後藤厚宏. サプライチェーンのサイバーレジリエンス. 日本セキュリティ・マネジメント学会誌, 38(2), 3-12. (2024).
- [2] 石島隆. サプライチェーンのリスクに対応したサイバーフィジカルシステムの情報品質の確保策. 第 81 回大会予稿集. (2021).
- [3] 内閣サイバーセキュリティセンター. サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ. (2025). <https://www.nisc.go.jp/>
- [4] National Institute of Standards and Technology. Developing security, privacy, and C-SCRM plans for systems (NIST Special Publication 800-18, Revision 2). U.S. Department of Commerce. (2026). <https://doi.org/10.6028/NIST.SP.800-18r2>.