論文審査の要旨及び担当者

No.1

報告番号	甲　乙　第　　号	氏　名	西嶋　克哉

論文審査担当者	主　査	政策・メディア研究科委員　兼環境情報学部教授	中村　修
	副　査	政策・メディア研究科委員　兼環境情報学部教授	植原　啓介
	副　査	政策・メディア研究科委員　兼環境情報学部教授	楠本　博之
	副　査	慶應義塾大学　名誉教授	村井　純
学力確認担当者：			

(論文審査の要旨)

西嶋克哉君提出の学位請求論文は「インシデントレスポンス迅速化に向けた組織間連携支援のための分散型セキュリティオペレーション基盤の実証」と題し、全 8 章から構成される。

近年、サイバー攻撃の増加と巧妙化が進み、単独組織での対策には限界が生じている。高度な技術力を持つ攻撃者による脅威が拡大し、防御側は迅速な検知・対応を求められている。しかし、多くの組織では、攻撃への対処に必要な能力、情報、人材が不足しており、効果的な防御を実現できていない。このような課題に対処するためには、組織間での情報共有が不可欠である。政府機関や専門組織が主導する情報共有の枠組みが既に存在し、これらは参加組織間での脅威情報の迅速な共有を促進する役割を果たしている。

一方で、現行の仕組みは正確性を重視し、一定の信頼性を確保しているが、網羅性や迅速性の観点で課題がある。情報共有において、機密情報漏えいの懸念やコストの問題からすべての情報が共有されるわけではなく、特に IOC（Indicator of Compromise）に偏重し、攻撃者の戦術や対応策などの知見が十分に共有されていない。また、人手を介する共有や定例会合中心の枠組みにより、最新の攻撃情報が即時に伝わらず、迅速な対応が難しい。

本研究では、これら既存の情報共有の枠組みを踏まえ、それらを補完する情報共有モデルである分散型セキュリティオペレーション基盤（分散 SOC）を提案する。分散 SOC では、各組織の SOC が緊密に連携し、従来の枠組みを超えた情報共有と協調的防御を実現することを目指している。分散 SOC の特徴は、「多様な生データの、機微機密情報を保護した能動的な活用」と「システム化によるリアルタイム性の向上」を組み合わせることで、より高度な脅威検知・分析を可能にする点にある。

第 1 章の序論では、既存の情報共有の課題と、その解決手法である分散 SOC について述べている。

第 2 章では、分散 SOC における情報共有モデルを提案し、情報共有における課題を解決することを目的としている。具体的には、機微な生データの開示リスクや、大量データ共有にかかるコストが情報共有を妨げる要因であることを指摘し、これらの問題を解消するために、データそのものを共有せず、分析機能を提供するシステムを設計した。提案システムにより、必要最小限の情報のみを共有し、情報利用者が分析に必要な情報を選別できるようになり、より安全かつ効率的な情報共有が可能となる。

論文審査の要旨及び担当者

第 3 章では、1 つ目の実証について述べている。複数の組織間でのダークネット観測データを分析し、情報共有の効果を評価することを目的とする。特に、異なる組織が観測したデータを比較することで、ダークネット監視の効果を定量的に示している。具体的には、学術機関と電力会社の 2 つの組織が観測したダークネットデータを比較し、組織内と組織間でのデータ解析結果の違いを評価した。実験結果から、組織間でのデータ共有が、より多くの疑わしいホストの検出に寄与し、特定のポートやプロトコルに関する攻撃が特定の組織を標的にする傾向があることを明らかにした。

以上の結果から、複数組織のダークネット観測データを共有することにより、スキャン活動や攻撃をより広範に観測でき、セキュリティ対応を強化できる可能性があることが明らかとなった。

第 4 章では、分散 SOC の 2 つ目の実証について述べている。サイバー攻撃の高度化に伴い、悪性 Web サイトへの接続を防ぐ手法として、分散型異常検知 AED（AED：Autonomous Evolution of Defense）を提案し、評価を行った。従来のブラックリストやホワイトリストを用いた手法では、未知の Web サイトの良し悪しを判定できない課題がある。これを解決するため、Web サイトへの接続傾向の乖離度を基に未知サイトの不審度を算出し、接続の可否を判断する方法を提案した。さらに、他組織の接続ログを活用することで誤検知を削減するアプローチを導入し、実証実験で AUC（Area Under the Curve）の向上を確認した。また、ユーザ評価実験の結果、制御処理の 93.6%が 3 秒以内に完了することを確認し、実運用への適用可能性を示した。

第 5 章では、分散 SOC の 3 つ目の実証について述べている。本実証では、標的型攻撃をはじめとする高度化するサイバー攻撃に対抗するため、複数組織間でインシデント対応記録を共有し、その有用性を検証するとともに、システム化の課題を明らかにした。特に、大規模言語モデル（LLM）を活用して不要情報の削除・整形を自動化し、情報共有の効率化を図った。

本実証の成果として、インシデント対応記録が他組織にとって有用な情報を含むことを示すとともに、LLM を用いた情報整理の有効性とその限界を明らかにした。

第 6 章では、提案したシステムを検証するため行われた 3 つの実証実験を元に、本提案システムを分散 SOC のアーキテクチャとして総括している。3 つの実証実験を基に、共通する要件を洗い出し、インフラ部分を統合しつつ、異なる分析ロジックを柔軟に適用できるアーキテクチャを構築した。これにより、新たな分析要件が発生した際に効率的に対応できる柔軟なシステム設計が可能となる。

第 7 章では、インシデント対応記録の共有手法について述べている。本手法は、「攻撃を受けた組織が類似するほど、より有用なフィードバックが得られる」という仮定に基づき、秘密計算を用いた動的アクセス制御を実現するものである。これにより、共有相手、状況に応じた動的なアクセス制御の実現が可能となる。

第 8 章では、本研究の総括を行うとともに、今後の研究課題について詳細に指摘している。

論文審査の要旨及び担当者

著者は、2018 年からサイバーセキュリティの研究開発に従事し、分散 SOC という新しい概念を提案してきた。本博士論文は、既存の情報共有の取組における改良点に着目し、研究成果として「インシデントレスポンス迅速化に向けた組織間連携支援のための分散型セキュリティオペレーション基盤の実証」と題した博士論文としてまとめた。この成果は、著者が情報セキュリティ分野において広範な知識と高度な技術力を有していることを示すものである。

本論文は、著者が研究者として実社会の研究課題を発見・分析する能力を有し、先端的な研究を遂行するために必要な高度な研究能力と学識を備えていることを示したものである。

よって、本論文の著者は、博士（政策・メディア）の学位を受ける資格があると認める。