主　論　文　要　旨

No.1

報告番号	甲　乙　第　　号	氏　名	西嶋　克哉

主 論 文 題 目 :
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

（内容の要旨）

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めざしている．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．

本研究では，分散 SOC の有効性を，以下の三つの実証で示し，いずれも組織間の密な情報共有がセキュリティ向上に寄与したことが確認された．

1 つ目の実証として，複数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した．学術機関と電力会社が観測したデータを比較し，組織内外でのデータ解析結果を評価した実験結果から，データ共有がより多くの疑わしいホストを検出し，攻撃ターゲットが特定の組織に集中する傾向があることが明らかになった．この結果から，複数組織間でデータを共有することにより，スキャン活動や攻撃の観測範囲が広がり，セキュリティ対応の強化が期待できることが示された．

分散 SOC の 2 つ目の実証として，悪性 Web サイトへの接続防止を目的に分散型異常検知 AED（Autonomous Evolution of Defense）を提案し，評価を行った．従来の方法では未知の Web サイトの判定が難しいが，接続傾向の乖離度に基づき不審度を算出し，接続可否を判断する手法を提案. また, 他組織の接続ログを活用し誤検知を削減し, AUC（Area Under the Curve）の向上を確認した．さらに，ユーザ評価実験により，制御処理の 93.6%が 3 秒以内に完了し，実運用への適用可能性を示した.

分散 SOC の 3 つ目の実証として，複数組織間でのインシデント対応記録共有の有用性とシステム化の課題を明らかにした．大規模言語モデル（LLM）を活用して情報整理を自動化し，情報共有の効率化を図った．実証結果として，インシデント対応記録が他組織にとって有用であり，LLM を用いた情報整理の有効性と限界を明確にした.

さらに, 本論文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た．インフラ部分を統合しつつ，異なる分析を柔軟に適用できるアーキテクチャを構築することで，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とした.

加えて, インシデント対応記録の共有手法についても検討を行った. 本手法では,「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，共有相手や状況に応じた動的なアクセス制御が可能となる.

本研究は，セキュリティ情報共有の有効性を定量的に示し，提案モデルの実現可能性を技術的および運用的に検証した．これにより，情報共有の活性化とサイバーセキュリティ対策の向上に貢献し，政府のサイバー安全保障強化方針に沿って官民連携によるインシデント対応の向上に寄与することが期待される．分散型 SOC を活用することで，重要インフラ事業者間の情報共有の分断を解消し，迅速かつ協調的な対応が可能となることが期待できる.

キーワード : 情報共有, インシデント対応効率化, 異常検知