セキュリティオペレーションセンター（SOC）
ビジネストレンド・事例レポート

Librus株式会社
コンサルティングサービス事業部

エグゼクティブサマリー

セキュリティオペレーションセンター（SOC）は、AI技術の急速な進歩と統合セキュリティプラットフォームの普及により、根本的な変革期を迎えている。2025年は「AI-powered SOC」が本格的な成長を遂げる転換点として位置づけられ、従来の人的リソース中心の運用から自動化・自律化されたインテリジェントな脅威対応への進化が加速している。

市場規模においては、SOC as a Service市場が2024年の74.5億ドルから2032年には204億ドルへと年平均成長率13.4%で急拡大すると予測されており、企業のセキュリティ運用のアウトソーシング需要が顕著に高まっている。

1. SOC市場の現状と成長予測

1.1 グローバル市場規模の動向

セキュリティオペレーションセンター市場は急速な拡大を続けており、特にSOC as a Service（SOCaaS）セグメントが牽引役となっている。複数の市場調査機関の報告によると:

- **SOC as a Service**市場：2024年74.5億ドル → 2032年204億ドル（CAGR 13.4%）
- セキュリティオペレーションソフトウェア市場：2024年268億ドル → 2033年5,168億ドル（CAGR 7.5%）
- マネージドセキュリティサービス市場：2025年190.4億ドル → 2032年4,148億ドル（CAGR 11.40%）

1.2 日本市場の特徴

日本ネットワークセキュリティ協会（JNSA）の2024年調査によると、国内情報セキュリティ市場は2023年度に1兆4,628億円（前年比9.8%増）に達した。この成長の背景には以下の要因がある:

- 国際的紛争の影響によるサイバー攻撃の増加
- ランサムウェア攻撃とフィッシング詐欺の多様化
- 個人情報保護法改正等の法規制対応需要

- ハイブリッドワーク環境でのセキュリティ強化
- ゼロトラスト概念の普及とエンドポイントセキュリティ重視

1.3 成長促進要因

SOC市場の急成長を支える主要な促進要因として、以下が挙げられる:

1. サイバー脅威の高度化:攻撃者のAI活用による攻撃手法の巧妙化
2. 人材不足の深刻化:専門的なセキュリティアナリストの慢性的不足
3. **24**時間**365**日監視需要:グローバル事業展開企業の増加
4. 規制・コンプライアンス要求:業界固有のセキュリティガイドライン強化
5. クラウド移行加速:マルチクラウド環境でのセキュリティ複雑化

2. 技術革新による次世代**SOC**の台頭

2.1 AI-Powered SOCの実現

2025年は「AI-powered SOC」が本格的な普及段階に入る転換点として位置づけられている。Palo Alto Networksの分析によると、AI活用により以下の変革が実現されている:

- アラート処理の自動化:100%アラートカバレッジの実現
- アナリスト業務の高度化:トリアージ業務から脅威ハンティング・攻撃シミュレーションへのシフト(70%の時間配分変更)
- リアルタイム脅威検知:機械学習による異常検知精度の向上
- 自動修復機能:同一アラートの再発防止による継続的セキュリティ向上

2.2 統合セキュリティプラットフォームの進化

2.2.1 次世代**SIEM・XDR・SOAR**の統合

従来の個別ツール運用から統合プラットフォームへの移行が加速している。主要な統合トレンドは以下の通り:

技術要素	従来の課題	統合後の効果
SIEM	サイロ化された情報管理	統一された脅威可視化
SOAR	手動インシデント対応	オーケストレーション自動化

XDR	エンドポイント限定検知	マルチレイヤー統合検知
NDR	ネットワーク単体分析	コンテキスト統合分析

2.2.2 クラウドネイティブ**SOC**の台頭

クラウドファーストの企業戦略に対応し、クラウドネイティブなSOCソリューションが主流となっている。主な特徴：

- マルチクラウド環境での統一監視
- スケーラブルなログ処理能力
- API連携による拡張性
- DevSecOps統合

2.3 生成**AI**活用による変革

生成AIの企業導入が進む中で、SOC運用における活用も急速に拡大している：

- インシデント分析の自動化：自然言語でのレポート生成
- 脅威インテリジェンス強化：パターン認識精度の向上
- プレイブック自動生成：対応手順の動的最適化
- アナリスト支援：専門知識のリアルタイム提供

3. SOC as a Service（SOCaaS）の急成長

3.1 アウトソーシング需要の背景

企業のSOC運用外部委託が急速に拡大している背景には、以下の構造的要因がある：

1. 専門人材確保の困難：セキュリティアナリストの慢性的不足
2. **24**時間体制のコスト負担：内製SOCの運用コスト高騰
3. 技術的複雑性の増大：マルチベンダー環境の統合運用困難
4. 規制対応の専門性：業界固有要件への対応負荷

3.2 サービス提供モデルの多様化

3.2.1 Co-managed SOC

企業の内製SOCチームとサービスプロバイダーが協働する hybrid model が注目を集めている。

3.2.2 Industry-specific SOC

金融、製造業、ヘルスケア等の業界特化型SOCサービスが成長している。

3.2.3 SMB向け SOC

中小企業向けの簡易SOCサービスが市場拡大を牽引している。

3.3 主要SOCサービスプロバイダーの動向

企業カテゴリ	特徴	成長戦略
大手システムインテグレータ	既存顧客基盤活用	SI案件でのSOC併売
専業セキュリティサービス	高度専門性	AI技術投資による差別化
クラウドベンダー	プラットフォーム統合	クラウドネイティブ機能強化
グローバルMSSP	24時間グローバル体制	地域展開と現地パートナーシップ

4. 業界別SOC導入事例と成功要因

4.1 金融業界

4.1.1 導入背景

金融業界では、規制要求の厳格化とサイバー攻撃の標的化により、最も積極的なSOC投資が行われている。

4.1.2 特徴的な要件

- リアルタイム不正検知
- 金融庁ガイドライン準拠
- 低レイテンシー要求
- 厳格なデータ保護

4.1.3 成功事例

大手銀行では、AI-powered SOCの導入により不正取引検知精度を40%向上させ、偽陽性率を60%削減する成果を達成している。

4.2 製造業界

4.2.1 OT（運用技術）セキュリティの統合

製造業では、IT環境とOT環境の統合監視が重要な課題となっている。2025年のOTサイバーセキュリティトレンドとして以下が挙げられる：

- IT/OT統合セキュリティ監視
- 産業制御システム（ICS）保護
- サプライチェーンセキュリティ
- ハイブリッドワークフォース対応

4.2.2 成功要因

製造業のSOC成功事例では、以下の要因が重要視されている：

- 生産ラインへの影響を最小化する段階的導入
- OTスペシャリストとITセキュリティチームの連携
- ベンダー中立的なプラットフォーム選択

4.3 中小企業における SOC 活用

4.3.1 導入課題の解決

中小企業では、リソース制約を克服するため、以下のアプローチが効果的とされている：

1. クラウド型**SOC**サービス：初期投資の最小化
2. 業界特化型パッケージ：標準化による導入コスト削減
3. 段階的機能拡張：成長に応じたスケールアップ

4.3.2 効果測定

中小企業A社の事例では、SOCサービス導入により以下の効果を実現：

- インシデント対応時間：72時間 → 4時間（95%短縮）
- セキュリティ運用コスト：40%削減
- コンプライアンス対応工数：60%削減

5. 主要ベンダーの戦略動向

5.1 統合プラットフォーム戦略

5.1.1 Palo Alto Networks

Cortex XSIAMプラットフォームを中核とした統合戦略を推進。IBM QRadar SaaS資産の買収（2024年9月完了）により、SIEM市場でのポジション強化を図っている。

5.1.2 次世代SIEM競争の激化

従来のSIEMベンダーと新興XDRベンダーの競争が激化している。主要な差別化要因：

- AI/ML機能の実装度
- クラウドネイティブ対応
- 統合プラットフォーム提供能力
- 自動化・オーケストレーション機能

5.2 日本市場での競争環境

日本のSOC市場では、以下の競争軸が重要となっている：

競争軸	重要度	トレンド
日本語対応	高	AI翻訳技術による多言語対応向上
法規制対応	高	業界固有ガイドラインへの特化
オンプレミス対応	中	ハイブリッド環境への移行
価格競争力	中	TCO重視の評価基準

6. 2025年の重要予測と戦略的示唆

6.1 Palo Alto Networks による2025年予測

6.1.1 統合セキュリティプラットフォームの標準化

統合SOC・クラウドセキュリティプラットフォームが企業全体の攻撃阻止の標準となる。従来の個別ツール運用では、クラウド環境での迅速な脅威対応が困難となっている。

6.1.2 SOCの役割拡大：エクスポージャー管理

従来のアラート対応中心から、AI駆動によるエクスポージャー管理への役割拡大が進む。リアルタイムでの脅威識別・評価・修復の自動化が実現される。

6.1.3 AI革命によるアナリスト役割の再定義

AIによる日常的オペレーション自動化により、人間アナリストの役割が戦略的分析・意思決定にシフトする。

6.2 市場展望と投資動向

6.2.1 投資優先領域

1. **AI/ML**技術：自動化・自律化機能の高度化
2. クラウドネイティブ基盤：スケーラビリティとアジリティの向上
3. 統合プラットフォーム：運用効率化とTCO削減
4. 業界特化機能：垂直市場でのポジション確立

6.2.2 新興技術トレンド

- 量子暗号技術の実用化準備
- エッジコンピューティング環境でのセキュリティ
- IoT/OTデバイス統合監視
- ゼロトラストアーキテクチャとの融合

7. 実践的推奨事項

7.1 企業規模別アプローチ

7.1.1 大企業

- 統合プラットフォーム戦略の策定
- AI-powered SOC への段階的移行
- グローバル統一SOC体制の構築
- DevSecOps統合による開発プロセス組み込み

7.1.2 中堅企業

- Co-managed SOC モデルの検討
- 業界特化型SOCサービスの活用
- クラウドファーストによるコスト最適化
- 段階的機能拡張による投資効率化

7.1.3 中小企業

- SOC as a Service の積極活用
- 業界団体による共同SOCの検討
- 基本機能からの段階的導入
- マネージドサービスによる専門性確保

7.2 技術選定の要点

評価基準の優先順位:

1. AI/自動化機能の実装度
2. 統合プラットフォーム対応
3. クラウドネイティブ対応
4. 業界固有要件への適合性
5. スケーラビリティ・拡張性
6. ベンダーの技術投資継続性

7.3 組織・人材戦略

- 役割の再定義:自動化により余剰となる定型業務から戦略的分析へのシフト
- スキル開発:AI/ML技術理解とビジネスコンテキストの理解
- 外部パートナーシップ:専門性補完のための戦略的アライアンス
- 継続的学習:急速な技術進歩に対応する学習体制整備

8. 結論

セキュリティオペレーションセンター(SOC)は、AI技術の急速な進歩と統合プラットフォームの普及により、従来の概念を大きく超越した進化を遂げている。2025年は、この変革が本格的に実装され、企業のセキュリティ運用における競争優位性を決定づける重要な転換点となる。

市場データが示すように、SOC as a Service市場の急成長(CAGR 13.4%)は、企業のアウトソーシング需要の高まりを反映している。同時に、AI-powered SOCの実現により、人的リソースの制約を克服し、より効果的で効率的なセキュリティ運用が可能となっている。

成功する組織は、単純な技術導入を超えて、統合プラットフォーム戦略、AI活用による運用変革、そして人材の役割再定義を包括的に実装している。特に、従来のアラート対応中心の運用から、プロアクティブなエクスポージャー管理への転換が重要な差別化要因となっている。

今後、企業は自社の規模・業界特性・技術成熟度に応じた最適なSOC戦略を策定し、継続的な技術投資と組織能力向上を通じて、進化するサイバー脅威に対する強靭な防御体制を構築する必要がある。

監修者:
鎌田光一郎:青山学院大学法学部卒業。SMBC日興証券株式会社にて証券営業、経営管理業務に従事したのちPwCコンサルティンク゛合同会社に転籍。金融機関に対するコンサルティンク゛業務に従事。その後、Librus株式会社を設立、代表取締役に就任。

お問い合わせ先
Librus株式会社(代表取締役 鎌田光一郎)
105-0004東京都港区新橋6丁目13-12 VORT新橋Ⅱ 4F
03-6772-8015
お問い合わせフォーム
https://librus.co.jp/contact