CSIRT（Computer Security Incident Response Team）
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

2025年、CSIRT（Computer Security Incident Response Team）は企業のサイバーセキュリティ戦略において中核的な役割を担っている。日本シーサート協議会への加盟チーム数は**563**チーム（2024年10月現在）に達し、2013年以降急速な成長を続けている。一方で、**78%**の組織がセキュリティ人材不足に直面しており、AI活用による自動化とアウトソーシングサービスの活用が重要な解決策として注目されている。

CSIRT構築運用支援サービス市場は2017年度時点で**72.3**億円（前年度比**18.7%**増）を記録し、継続的な成長を示している。特に中小企業における導入促進、AI技術を活用したインシデント対応の自動化、SOCとの連携強化が主要なトレンドとして浮上している。

1. CSIRT市場の現状と成長動向

1.1 日本における**CSIRT**設置状況

日本シーサート協議会（NCA）のデータによると、2024年10月現在、同協議会への加盟チーム数は累積で563チームに達している。2007年の協議会設立時の6組織から飛躍的な成長を遂げており、特に2013年以降、CSIRT設立と加盟が急速に進んでいる。

企業規模別の設置状況を見ると、従業員規模10,000人以上の大企業では約8割がCSIRTを導入済みであり、1,000人以上の中堅企業でも約4割がCSIRTを構築している。しかし、全体的な設置率は約20%程度にとどまり、中小企業における普及が課題となっている。

1.2 市場規模と成長予測

ITRの調査によると、国内CSIRT構築運用支援サービス市場の2017年度売上金額は72.3億円で、前年度比18.7%増と順調な成長を示した。この市場は2016年から2022年にかけて右肩上がりの成長を続けており、今後も拡大が予想される。

市場成長の背景には、サイバー攻撃の高度化・多様化、規制強化、企業のデジタル変革（DX）推進に伴うセキュリティリスクの増大が挙げられる。特に製造業、金融業、インフラ事業者における導入ニーズが高まっている。

2. 主要ビジネストレンド

2.1 人材不足とスキルギャップの深刻化

最も深刻な課題として、**78%**の組織がセキュリティ人材不足を感じている。特に以下の課題が顕著である:

- 専門性の高い人材確保の困難 - CSIRT要員に求められる技術的スキルと経験を持つ人材の絶対的不足
- 組織体制の未整備 - 63%の組織でSOC/CSIRTなどの専門組織が未設置
- 経営層の理解不足 - 60%の組織でCSO/CISO/サイバーセキュリティ専任者が不在
- 継続的な人材育成の課題 - インシデント対応スキルの維持・向上が困難

2.2 AI・機械学習技術の活用拡大

人材不足を補完する手段として、AI・機械学習技術を活用したインシデント対応の自動化が急速に進展している:

2.2.1 自動検知・分析機能

- 異常検知アルゴリズムによるセキュリティインシデントの早期発見
- 機械学習を用いた攻撃パターンの自動分析
- 生成AIによるインシデント報告書の自動作成

2.2.2 対応プロセスの自動化

- SOAR（Security Orchestration, Automation and Response）ツールの導入
- 定型的なインシデント対応手順の自動実行
- エスカレーション判定の自動化

2.3 SOCとの連携強化

SOC（Security Operation Center）とCSIRTの役割分担と連携が明確化され、効率的なセキュリティ運用体制の構築が進んでいる:

項目	**SOC**	**CSIRT**
主要機能	24時間365日の監視・検知	インシデント発生時の対応・復旧
運用体制	常時監視体制	インシデント発生時に起動
専門性	監視・分析技術	事後対応・フォレンジック
自動化度	高度な自動化	判断を要する手動作業中心

2.4 アウトソーシング市場の拡大

人材不足と専門性の課題に対応するため、CSIRT機能のアウトソーシングが急速に拡大している。主なサービス形態は以下の通り:

2.4.1 フルアウトソーシング型

- CSIRT機能全体を外部事業者に委託
- 24時間365日のインシデント対応体制
- 専門的なフォレンジック調査サービス

2.4.2 部分委託型

- 特定領域(マルウェア解析、法的対応等)のみ外部委託
- 社内CSIRTと外部専門家の連携体制
- 緊急時のオンデマンド支援サービス

2.4.3 コンサルティング・構築支援型

- CSIRT立ち上げ支援
- 運用プロセス整備・改善
- 人材育成・トレーニングサービス

3. 業界別動向と特徴

3.1 金融業界

金融庁の「金融分野におけるサイバーセキュリティ強化に向けた取組方針」により、CSIRT設置が事実上義務化されている。主な特徴：

- 規制対応の徹底 - 金融庁ガイドラインに基づく体制整備
- 高度なインシデント対応 - 脅威ベースペネトレーションテスト（TLPT）の実施
- 業界横断的な情報共有 - 金融ISAC等を通じた脅威情報の共有
- レジリエンス重視 - 事業継続性を重視したインシデント対応計画

3.2 製造業

サプライチェーン攻撃への対策として、製造業でのCSIRT導入が加速している：

- **OT**（運用技術）セキュリティ - 工場システムを含む包括的な対応
- サプライヤー管理 - 関連会社を含むインシデント対応体制
- 事業影響最小化 - 生産停止リスクを考慮した優先順位付け

3.3 中小企業

リソース制約の中で効率的なCSIRT運用を目指す動きが活発化：

- 共助型**CSIRT** - 複数企業による共同運用モデル
- クラウド型サービス - 初期投資を抑えたSaaS型CSIRT
- 段階的導入 - 最小限の機能から段階的に拡張

4. 企業導入事例

4.1 大企業事例：**freee**株式会社

概要：クラウド会計ソフト大手のfreee株式会社は、GMOサイバーセキュリティ　byイエラエと連携し、レッドチーム演習を実施。

特徴：

- 本番環境に対する実戦的なペネトレーションテスト
- 組織全体のセキュリティリスク可視化
- ブルーチーム（防御側）の評価・トレーニング
- 継続的なセキュリティ体制改善

成果：実際の攻撃シナリオに基づく演習により、従来の診断では発見できない組織的課題を特定し、CSIRT体制の強化を実現。

4.2 金融機関事例：大和ネクスト銀行

概要：セキュアワークスのRed Team Liteサービスを活用し、脅威ベースペネトレーションテスト（TLPT）を実施。

導入背景：

- 金融庁ガイドラインへの対応
- サイバーレジリエンス強化の必要性
- 既存セキュリティ対策の有効性検証

実施内容：

- 実際の攻撃者手法に基づくシミュレーション
- 防御体制の総合的な評価
- インシデント対応プロセスの検証

4.3 中小企業向けサービス事例：網屋「セキュサポ」

概要：専門知識が必要なCSIRT構築を3ヶ月で実現するクラウドCSIRTサービス。

サービス特徴：

- 月額定額制のクラウドサービス
- 専門コンサルタントによる24時間365日サポート
- インシデント対応手順書の提供
- 定期的な訓練・研修プログラム

導入効果：

- 初期投資コストの大幅削減
- 専門人材確保の課題解決
- 段階的な体制構築が可能

4.4 技術企業事例：サイボウズ株式会社

概要：自動脆弱性診断ツールの導入により、CSIRT業務の効率化を実現。

取り組み内容：

- 手動診断と自動診断の役割分担最適化
- パターン化可能な診断項目の自動化
- 専門性を要する項目への人的リソース集中

成果：

- 診断工数の大幅削減
- 診断品質の標準化
- 継続的なモニタリング体制の構築

5. 技術革新と自動化動向

5.1 AI活用によるインシデント対応自動化

生成AIをはじめとする最新AI技術がCSIRT業務に本格導入されている:

5.1.1 インシデント分析の自動化

- **NTT-AT「AIサイバーインシデント分析」** - CyCraftのAI技術を活用したセキュリティ運用負荷軽減
- 機械学習による異常検知 - 正常な挙動を学習し、異常パターンを自動識別
- 攻撃手法の自動分類 - MITRE ATT&CKフレームワークに基づく脅威分析

5.1.2 レポート生成の自動化

- 生成AIによるインシデント報告書の自動作成
- 技術的詳細の経営層向け要約生成
- 対応履歴の自動記録・分析

5.2 SOAR（Security Orchestration, Automation and Response）の普及

定型的なインシデント対応手順の自動化により、CSIRT要員の負荷軽減と対応速度向上を実現:

- **Splunk SOAR** - 脅威判定・一次対処・影響範囲調査の自動化
- トリアージの自動化 - 優先度判定とエスカレーション判断
- 証跡収集の自動化 - フォレンジック調査に必要なデータの自動収集

5.3 統合プラットフォームの進化

SIEM、SOAR、脆弱性管理を統合したプラットフォームが普及し、CSIRT業務の効率化が進んでいる:

- 単一画面での状況把握 - 散在する情報の一元管理
- ワークフロー管理 - インシデント対応手順の標準化・可視化
- 知識ベース統合 - 過去事例とベストプラクティスの活用

6. 規制・コンプライアンス動向

6.1 金融分野の規制強化

金融庁による「金融分野におけるサイバーセキュリティ強化に向けた取組方針」が改訂され、より具体的な要件が示されている:

- **TLPT**（脅威ベースペネトレーションテスト）の定期実施
- サイバーレジリエンス強化 - 事業継続性を重視した対応体制
- グループ会社を含む統合的な管理
- 第三者によるセキュリティ評価

6.2 重要インフラ分野の対応強化

NISC（内閣サイバーセキュリティセンター）による重要インフラ防護対策の強化：

- 重要インフラ14分野でのCSIRT設置推進
- 政府機関との情報共有体制強化
- 国際的なサイバー演習への参加促進

6.3 製造業向けガイドラインの策定

経済産業省による「サイバーセキュリティ経営ガイドライン」の改訂により、製造業でのCSIRT設置が推奨されている：

- OT（運用技術）セキュリティの強化
- サプライチェーン全体でのセキュリティ管理
- インシデント発生時の迅速な情報共有

7. 課題と解決策

7.1 人材不足問題への対応

7.1.1 課題の詳細

- 絶対的な人材不足 - 日本全体で約17万人のセキュリティ人材が不足
- スキル要件の高度化 - AI、クラウド、IoTなど新技術への対応
- 経験者の偏在 - 大企業への人材集中
- 継続的な学習負荷 - 常に進化する脅威への対応

7.1.2 解決策

- アウトソーシングの活用 - 専門事業者への部分委託
- **AI**・自動化技術の導入 - 定型業務の自動化による効率化
- 人材育成プログラム - TRANSITS Workshopなどの専門研修
- 共助型モデル - 複数企業での人材・知見共有

7.2 中小企業における導入課題

7.2.1 課題の詳細

- コスト制約 - 専門人材の確保・維持コスト
- 経営層の理解不足 - セキュリティ投資の優先度
- 技術的知見の不足 - 適切な対策選択の困難
- 運用継続の困難 - 日常業務との両立

7.2.2 解決策

- クラウド型サービス - 初期投資を抑えたSaaS型CSIRT
- 段階的導入 - 最小限機能から徐々に拡張
- 業界団体の活用 - 同業他社との情報共有・共同対策
- 政府支援制度 - 中小企業向け補助金・税制優遇の活用

8. 将来展望

8.1 技術トレンド予測

8.1.1 AI技術の更なる進化

- 自律型**AI CSIRT** - 人間の判断を要さない自動対応の実現
- 予測型セキュリティ - 攻撃発生前の予兆検知・予防
- 自然言語処理の活用 - 経営層向けリスクコミュニケーションの自動化

8.1.2 量子コンピューティング時代への対応

- 量子暗号技術への対応準備
- 既存暗号方式の移行計画策定
- ポスト量子暗号の実装準備

8.2 組織・体制の進化

8.2.1 統合セキュリティ運用センター

- SOC、CSIRT、脆弱性管理の統合運用
- グローバル規模でのFollow the Sun運用
- クラウドネイティブなセキュリティ運用

8.2.2 エコシステム型協力体制

- 業界横断的な脅威情報共有基盤
- 官民連携によるサイバー演習
- 国際的なCSIRT連携ネットワーク

8.3 市場予測

CSIRT関連市場は今後も堅調な成長が予想される:

- 市場規模 - 年率15-20%の成長継続（2025-2030年）
- サービス多様化 - 業界特化型、機能特化型サービスの拡大
- 国際展開 - 日本企業の海外展開に伴うグローバルCSIRTサービス
- 新興技術対応 - IoT、5G、エッジコンピューティング対応の専門サービス

9. 推奨事項

9.1 企業向け推奨事項

9.1.1 大企業

- **AI**活用の本格導入 - SOAR、機械学習による自動化推進
- グループ横断的な統合 - 子会社・関連会社を含む統合CSIRT
- 継続的な演習実施 - レッドチーム演習、TLPT等の定期実施
- 人材育成投資 - 社内セキュリティ人材の計画的育成

9.1.2 中小企業

- 段階的な導入 - 最小限機能からの段階的拡張
- アウトソーシング活用 - 専門事業者との戦略的パートナーシップ
- 業界団体参加 - 同業他社との情報共有・共同対策
- クラウドサービス活用 - 初期投資を抑えたSaaS型サービス

9.2 政策・制度面での推奨事項

- 人材育成支援の強化 - 公的機関による研修・資格制度の充実
- 中小企業支援制度 - CSIRT導入に対する財政支援・税制優遇
- 情報共有基盤整備 - 官民連携による脅威情報共有プラットフォーム
- 国際協力の推進 - アジア太平洋地域でのCSIRT連携強化

9.3 サービス事業者向け推奨事項

- **AI**技術の積極的導入 - 次世代CSIRT支援サービスの開発
- 業界特化サービス - 金融、製造業等の業界ニーズに特化
- グローバル展開 - 日本企業の海外事業支援サービス
- 人材育成支援 - 顧客企業の内製化支援サービス

結論

2025年、CSIRTは企業のサイバーセキュリティ戦略において不可欠な要素となっている。人材不足という構造的課題に直面しながらも、AI技術の活用、アウトソーシングサービスの進化、SOCとの連携強化により、効率的で実効性の高いインシデント対応体制の構築が可能になっている。

特に注目すべきは、従来の大企業中心から中小企業への展開、技術志向から事業継続性重視への転換、国内完結型からグローバル連携型への進化である。今後は、量子コンピューティング、6G、メタバースなど新興技術に対応したCSIRT機能の拡張が求められる。

成功の鍵は、技術的な対策だけでなく、組織文化の変革、継続的な人材育成、ステークホルダーとの協力関係構築にある。CSIRTを単なるインシデント対応組織から、企業の競争力を支える戦略的機能へと発展させることが、デジタル時代を生き抜く企業の必須要件となっている。

参考資料：

- 日本シーサート協議会（NCA）公開資料
- ITR「CSIRT構築運用支援サービス市場規模推移および予測」
- NISC「サイバーセキュリティ2025」
- 金融庁「金融分野におけるサイバーセキュリティ強化に向けた取組方針」
- 各種企業事例・プレスリリース

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