セキュリティ診断（脆弱性診断・侵入テスト）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

セキュリティ診断市場は2025年に向けて急速な成長を遂げており、特に日本市場では2023年度に前年比33.3%増という驚異的な拡大を記録しました。AI技術の活用による診断自動化、クラウド・ゼロトラスト対応、TLPT（脅威ベースペネトレーションテスト）の普及、規制強化への対応が主要なトレンドとなっています。本レポートでは、市場動向、技術革新、企業事例を詳細に分析し、2025年に向けた戦略的示唆を提供します。

1. 市場規模と成長予測

1.1 日本市場の急速な拡大

日本セキュリティ診断市場規模（**JNSA**調査）

- 2023年度：719億円（前年比33.3%増）
- 2022年度：540億円（前年比4.2%増）
- 2024年度予測：755億円（前年比5.0%増）
- 2025年度予測：793億円（前年比5.0%増）

日本ネットワークセキュリティ協会（JNSA）の最新調査によると、2023年度のセキュリティ診断市場は前年比33.3%増の719億円に達し、情報セキュリティサービス市場全体（6,724億円）の24.9%を占める重要なセグメントとなっています。この急成長は、サイバー攻撃の高度化、クラウド移行の加速、ゼロトラストセキュリティの普及が主要な要因となっています。

1.2 グローバル市場の動向

グローバルペネトレーションテスト市場

- 2024年：42.5億米ドル
- 2029年予測：127.6億米ドル（年平均成長率24.59%）

- 2025年予測：27.4億米ドル（年平均成長率12.5%）
- 2032年予測：174.1億米ドル（年平均成長率17%）

複数の調査機関による予測では、グローバルペネトレーションテスト市場は2020年代を通じて年平均15-25%の高成長を維持すると予想されています。特にクラウドペネトレーションテストサービス市場は2025年に3.7億米ドル、2033年までに5.6億米ドルに達する見込みです。

2. 主要ビジネストレンド分析

2.1 AI・機械学習による診断自動化の革新

2.1.1 AI活用の現状と展望

2025年は「AI駆動セキュリティ診断元年」と位置づけられ、従来の手動診断からAI支援診断への根本的な転換が進んでいます。生成AI技術の活用により、これまで専門知識が必要だった脆弱性診断が大幅に自動化・効率化されています。

2.1.2 主要AI診断ツールの動向

- **AeyeScan**（エーアイスキャン）：生成AIを活用したSaaS型脆弱性診断ツール。Webサイトの重要度を自動で可視化し、脆弱性対策の優先順位付けを支援
- **VAddy**：継続的セキュリティテストを実現するクラウド型脆弱性診断ツール
- **AI脆弱性チェッカー**：AI技術によりWebサイト全体を自動スキャンし、短時間での脆弱性検出を実現

2.1.3 AI活用の効果

AI導入による効果

- 診断時間の大幅短縮（従来の1/10〜1/5に削減）
- 人的リソース不足の解消
- 診断精度の向上と標準化
- 継続的監視の実現
- 専門知識なしでの高品質診断の実現

2.2 クラウド・ゼロトラスト対応の高度化

2.2.1 新たな診断領域の拡大

JNSAの調査では、「クラウドシステムの安全性やゼロトラストシステムの安全性を診断するサービス」が高い伸びを示していると報告されています。従来のオンプレミス環境中心の診断から、クラウドネイティブ環境、ハイブリッドクラウド、マルチクラウド環境への対応が急務となっています。

2.2.2 主要クラウド診断サービス

- **AWS/Azure/Google Cloud**診断：クラウドプラットフォーム設計の不備を検出
- コンテナセキュリティ診断：Docker、Kubernetesの脆弱性評価
- マイクロサービス診断：分散アーキテクチャの総合的セキュリティ評価

2.3 TLPT・Red Team演習の標準化

2.3.1 TLPT（脅威ベースペネトレーションテスト）の普及

金融庁の「金融分野におけるサイバーセキュリティに関するガイドライン」改訂により、TLPTの実施が金融機関に実質的に義務化されました。これにより、従来の脆弱性診断から、より実践的な攻撃シミュレーションへとニーズがシフトしています。

TLPTの特徴

- 現実的な攻撃シナリオに基づく演習
- 攻撃側（Red Team）と防御側（Blue Team）の実戦型演習
- 組織全体のサイバーレジリエンス評価
- 継続的な改善サイクルの確立

2.3.2 Red Team演習サービスの拡充

金融業界を中心にRed　Team演習の需要が急速に拡大しており、専門事業者の参入が相次いでいます。従来の技術的な脆弱性発見に加え、組織的な対応力の評価・訓練が重視されています。

3. 技術革新と診断手法の進化

3.1 次世代診断技術の動向

3.1.1 統合診断プラットフォーム

従来の個別ツールによる診断から、SIEM、SOAR、XDRと連携した統合診断プラットフォームへの移行が進んでいます。これにより、診断から対策実施までの一気通貫したセキュリティ運用が可能となっています。

3.1.2 継続的セキュリティテスト（CST）

DevSecOpsの普及により、開発プロセスに組み込まれた継続的セキュリティテストが標準化されています。CI/CDパイプラインと統合されたセキュリティ診断により、リアルタイムでの脆弱性検出・修正が実現されています。

3.2 診断対象の拡大

3.2.1 IoT・OT環境診断

- 産業制御システム（ICS/SCADA）の脆弱性診断
- IoTデバイスのセキュリティ評価
- IT/OT統合環境の総合診断

3.2.2 モバイルアプリケーション診断

- iOSアプリの静的・動的解析
- Androidアプリの総合セキュリティ評価
- モバイルAPI診断

4. 業界別導入事例分析

4.1 金融業界の先進事例

事例**1**：大和ネクスト銀行の**Red Team Lite**導入

概要：顧客の資産形成を支える金融サービスを提供する大和ネクスト銀行は、サイバーレジリエンスの強化を目指し、セキュアワークスのRed Team Liteを導入。

実施内容：TLPT（脅威ベースペネトレーションテスト）を実施し、これまでの対策の有効性を実証。現実的な攻撃シナリオに基づく演習により、組織全体の対応力を評価。

成果：既存のセキュリティ対策の有効性確認と、更なる強化ポイントの特定。インシデント対応体制の実戦力向上。

4.2 IT業界の革新事例

事例**2**：**Sansan**株式会社のレッドチーム演習

概要：名刺管理サービスを提供するSansan株式会社は、組織全体のセキュリティリスク可視化とブルーチームの評価・トレーニングを目的としてレッドチーム演習を実施。

実施内容：GMOサイバーセキュリティ　byイエラエによるレッドチーム演習。現実的な攻撃シナリオによる侵入テスト。

成果：セキュリティチームの実戦対応力向上、組織横断的なセキュリティ意識の醸成、継続的改善プロセスの確立。

事例**3**：**freee**株式会社の本番環境レッドチーム演習

概要：クラウド会計ソフトを提供するfreee株式会社は、全サービスの本番環境に対してレッドチーム演習を実施。

実施内容：本番環境での実戦的ペネトレーションテスト。丁寧な事前ケアにより業務影響を最小化。

成果：本番環境での実際の脅威検証、リアルタイムでのセキュリティ対応力評価。

4.3 中小企業向けソリューション

4.3.1 中小企業の課題と対策

中小企業では専門人材やリソースの制約により、大企業レベルのセキュリティ診断実施が困難な場合が多いです。しかし、AI活用ツールやクラウド型診断サービスの普及により、中小企業でも高品質な診断が可能となっています。

中小企業向けソリューション特徴

- 月額制のSaaS型診断ツール
- 専門知識不要の自動診断
- 段階的導入による負担軽減
- 大企業レベルのセキュリティ運用をアウトソーシング

5. 規制強化とコンプライアンス対応

5.1 金融庁ガイドラインの影響

5.1.1 主要要求事項

2024年10月改訂の「金融分野におけるサイバーセキュリティに関するガイドライン」では、以下の診断実施が求められています：

- 脆弱性診断およびペネトレーションテストの定期実施
- インターネット非接続のVPN網、内部環境も対象とした診断
- 定期的な脅威ベースペネトレーションテスト（TLPT）の実施
- 脅威インテリジェンスを活用した実践的演習

5.1.2 業界への波及効果

金融業界での規制強化は他業界にも波及しており、製造業、エネルギー、通信など重要インフラ事業者でも同様の診断実施が検討されています。

5.2 国際規格・標準への対応

5.2.1 主要規格・標準

- ISO/IEC 27001：情報セキュリティマネジメントシステム
- NIST Cybersecurity Framework：サイバーセキュリティフレームワーク
- OWASP Testing Guide：Webアプリケーションセキュリティテストガイド
- PTES（Penetration Testing Execution Standard）：ペネトレーションテスト実行標準

6. 市場構造と競合分析

6.1 市場セグメント別分析

セグメント	**2023**年度市場規模	成長率	主要プレイヤー
コンサルティング	1,393億円	20.7%	大手コンサル、SI事業者
診断サービス	719億円	33.3%	専門診断事業者、セキュリティベンダー
監査・評価	406億円	0.1%	監査法人、認証機関
規格認証	368億円	13.1%	認証機関、コンサル

6.2 主要事業者の動向

6.2.1 大手システムインテグレータ

NTTデータ、NEC、富士通等の大手SIerは、既存顧客基盤を活用しながらセキュリティ診断サービスを強化。特にクラウド移行支援と組み合わせたセキュリティ診断の提供が増加。

6.2.2 専門セキュリティ事業者

ラック、NRIセキュア、GMOサイバーセキュリティ、GSX等の専門事業者は、高度な技術力を武器にTLPT、Red Team演習等の付加価値の高いサービスを展開。

6.2.3 新興**AI**診断事業者

エーアイセキュリティラボ、Secure　SkyTechnology等、AI技術を活用した診断自動化に特化した新興事業者が急成長。従来の人的診断の常識を覆すソリューションを提供。

7. 2025年に向けた展望と戦略的示唆

7.1 市場成長予測

2025年市場予測

- 日本セキュリティ診断市場：793億円（2023年比10.3%増）
- グローバルペネトレーションテスト市場：127.6億米ドル
- AI活用診断ツール市場：急速拡大継続
- TLPT/Red Team演習市場：金融以外への拡大

7.2 技術トレンド予測

7.2.1 AI技術の更なる進化

- 生成AIによる攻撃シナリオ自動生成
- 機械学習による脆弱性パターン予測
- 自然言語処理による診断レポート自動作成
- AIアシスタントによる診断業務支援

7.2.2 プラットフォーム統合の加速

- 診断・監視・対応の統合プラットフォーム
- クラウドネイティブ診断ソリューション
- DevSecOpsパイプライン統合
- ゼロトラストアーキテクチャ対応

7.3 事業者への戦略的推奨事項

7.3.1 診断サービス事業者向け

1. **AI**技術への投資強化：診断自動化ツールの開発・導入により競争優位性を確保
2. クラウド・ゼロトラスト対応：新たな診断領域への専門性構築
3. **TLPT/Red Team**能力構築：高付加価値サービスによる差別化
4. 継続的サービス化：一回限りの診断から継続的監視サービスへの転換

7.3.2 ユーザー企業向け

1. 診断の定期化・継続化：年1回の診断から継続的監視への移行
2. **AI**診断ツールの活用：内製化による効率性向上とコスト削減
3. 実践的演習の導入：TLPT、Red Team演習による実戦力強化
4. クラウド環境対応：従来診断に加えクラウドセキュリティ診断の実施

8. 結論

セキュリティ診断市場は2025年に向けて構造的な変化の中にあります。AI技術の活用による診断自動化、クラウド・ゼロトラスト環境への対応、TLPT/Red　Team演習の普及、規制強化への対応という4つの大きなトレンドが市場を牽引しています。

特に日本市場では2023年度に33.3%という驚異的な成長を記録し、今後も継続的な拡大が予想されます。この成長の背景には、サイバー攻撃の高度化、デジタル変革の加速、規制要求の強化があり、企業のセキュリティ診断に対するニーズは質・量ともに高度化しています。

成功する事業者は、AI技術の活用、新たな診断領域への対応、高付加価値サービスの提供という3つの要素を統合したソリューションを提供する企業となるでしょう。一方、ユーザー企業は従来の年次診断から継続的セキュリティテストへの転換、内製化とアウトソーシングの適切な組み合わせ、実践的演習による組織力強化が重要になります。

2025年はセキュリティ診断業界にとって「AI活用元年」かつ「実戦演習標準化元年」として記憶される年になると予想されます。この変化に適応できる事業者・ユーザーが、次世代のサイバーセキュリティ環境で競争優位を確立できるでしょう。

03-6772-8015
お問い合わせフォーム
https://librus.co.jp/contact