サイバーセキュリティにおけるリスクアセスメントサービスのトレンドと事例に関するレポート

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

2024年は、サイバーセキュリティ分野において転換点となる年となった。日本国内におけるランサムウェア被害の公表件数が過去最大の84件に達し、新興ランサムウェアグループの台頭により脅威の複雑化が進展している。本レポートでは、こうした脅威環境の変化を背景に、リスクアセスメントサービスの重要性の高まりと市場トレンドを分析する。

主要な知見として、日本企業のパッチ適用期間（MTTP：Mean Time To Patch）が平均36.4日と世界平均の1.2倍に達しており、脆弱性対応の迅速化が急務となっている。また、サイバーセキュリティ市場規模は2024年に180億米ドルに成長し、継続的脅威曝露管理（CTEM）アプローチの採用が急速に拡大している。

企業の経営層においても、SECの新規則やEUのNIS2指令により、サイバーセキュリティへの関与とリスク評価への責任が明確化されており、今後はより戦略的なアプローチが求められる。

1. 2024年のサイバーセキュリティ情勢概観

1.1 脅威ランドスケープの変化

2024年のサイバー脅威環境は、国家を背景とするグループからの攻撃をはじめとするサイバー攻撃の洗練化・巧妙化が一層進展した年として特徴づけられる。特に、ランサムウェア攻撃の手法が多様化し、従来のデータ暗号化に加えて、データ窃取後の恐喝を目的とした攻撃が新たに30件確認されている。

2024年の主要サイバー脅威統計

- 日本国内ランサムウェア被害公表件数: 84件（過去最大）
- 国内セキュリティインシデント総数: 1,319件（前年度比10.4%増）
- 不正アクセス事案: 372件（最多）
- マルウェア感染: 315件
- 紛失・盗難: 213件

1.2 新興ランサムウェアグループの台頭

2024年下半期に急速に拡大した新興ランサムウェアグループが、上位10グループによるリーク数の90%を占める状況となっている。RansomHub、8base、Hunters International、BlackSuit、Undergroundなどの新興グループが日本企業を標的とした攻撃を展開している。

グループ名	活動開始時期	特徴
RansomHub	2024年2月頃	2024年下半期最も活発。アンチEDR技術を駆使
8base	2022年3月頃	中小企業（従業員数1-200名）を主要標的
Hunters International	2023年第3四半期	解体されたHIVEグループとの関連性指摘
BlackSuit	2023年5月頃	ContiやRoyalとの関係性指摘
Underground	2023年7月頃	拡張子変更せずファイル暗号化が特徴

2. リスクアセスメントサービスの主要トレンド

2.1 継続的監視への移行

従来の年1回のポイントインタイム監査から、継続的監視（Continuous Monitoring）への移行が加速している。IBMの報告によると、2023年のデータ侵害の世界平均コストは445万ドルで、3年間で15%増加しており、早期検知の重要性が高まっている。

2.2 CTEMアプローチの採用拡大

Gartnerが2022年に提唱した継続的脅威曝露管理（CTEM：Continuous Threat Exposure Management）アプローチの採用が急速に拡大している。CTEMは以下の5つのステップで構成される：

1. 既存のサイバーセキュリティ露出のスコープ定義
2. 隠れた脆弱性の発見プロセス開発
3. 悪用可能性に基づく脅威の優先順位付け
4. 様々な攻撃シナリオの検証・評価
5. 組織全レベルでの従業員動員

2.3 サイバーリスク定量化（CRQ）の普及

財務的観点からのサイバーリスク定量化（Cyber Risk Quantification：CRQ）が注目を集めている。CRQにより、技術的なリスクを金銭的影響と発生確率で表現することで、経営層との意思疎通が改善され、より効果的な予算配分が可能となっている。

3. 国際的なフレームワークとベストプラクティス

3.1 NIST Cybersecurity Framework 2.0

2024年に更新されたNIST CSF 2.0は、従来の5つの機能（識別、保護、検知、対応、復旧）に「統治（Govern）」機能を追加し、より包括的なサイバーセキュリティ管理を実現している。組織のリスク管理戦略とcybersecurityの統合がより明確化された。

3.2 ISO/IEC 27001:2022

情報セキュリティマネジメントシステム（ISMS）の国際標準であるISO 27001の2022年版では、クラウドセキュリティ、プライバシー保護、サプライチェーンセキュリティに関する管理策が強化されている。

フレームワーク統合事例

多くの組織がNIST CSFの戦略的フレームワークとISO 27001の運用管理を組み合わせたハイブリッドアプローチを採用している。NIST CSFがリスク管理の方向性を示し、ISO 27001が具体的な管理策の実装を支援する相補的関係を構築している。

3.3 規制要件の強化

米国SECの2023年サイバーセキュリティ規則やEUのNIS2指令により、取締役会レベルでのサイバーセキュリティ責任が明確化されている。経営層は単なる予算承認者から、積極的なリスク管理参加者へと役割が変化している。

4. 日本市場の動向と特徴

4.1 市場規模と成長予測

日本サイバーセキュリティ市場規模

- 2024年市場規模: 180億米ドル
- 2033年予測市場規模: 433億米ドル
- 年平均成長率（CAGR）: 10.3%
- 2032年予測（別統計）: 263億米ドル

4.2 日本特有の課題

日本企業が直面する特有の課題として、パッチ適用の遅延問題が深刻化している。トレンドマイクロの調査によると、日本組織の平均パッチ適用期間（MTTP）は36.4日で、これは世界平均の1.2倍に相当する。

4.3 委託先からの情報漏洩問題

2024年には、印刷業や配送業などデータ集積型業種のランサムウェア被害により、委託元の個人情報漏洩が深刻化した。株式会社イセトーの事例では約150万件の個人情報漏洩が発生し、「データサプライチェーン」問題の深刻さが浮き彫りとなった。

委託先経由の情報漏洩件数推移
2024年下期には委託先から漏洩した情報件数が300万件を超過。組織は委託先のサイバーリスク評価の見直しが急務となっている。

5. 技術革新とAIの活用

5.1 AI・機械学習によるリスク評価の高度化

人工知能（AI）と機械学習（ML）技術の活用により、膨大なデータを迅速に分析し、従来よりも効率的にセキュリティリスクを特定することが可能になっている。米国国勢調査局の予測では、2024年前半にAIを活用する企業が劇的に増加するとされている。

AI活用の主要分野:

- SIEM（Security Information and Event Management）での偽陽性の除去
- ファイアウォールとマルウェア対策の自動化
- 異常検知とパターン認識の高精度化
- 脆弱性スキャンの効率化

5.2 リアルタイム脅威検知

従来の定期的なリスクアセスメントから、リアルタイムでの脅威検知・評価への移行が進んでいる。Continuous Threat Exposure Management (CTEM) の普及により、動的なリスク環境に対応した評価手法が確立されつつある。

5.3 Attack Surface Management (ASM) の導入

攻撃対象領域管理（ASM）ツールの導入により、組織のデジタル資産とその脆弱性を継続的に監視・評価することが可能となっている。これにより、早期の脆弱性発見とリスク管理の精度向上が実現されている。

6. 将来予測と推奨事項

6.1 市場予測

日本のサイバーセキュリティ市場は、2025年から2034年の期間で年平均成長率14.6%の継続的成長が予測されている。特に、リスクアセスメント分野では以下のトレンドが予想される：

- CRQ（サイバーリスク定量化）ツールの普及拡大
- ツール統合によるオールインワンプラットフォームの採用増加
- 経営層レベルでのサイバーリスク関与の法制化
- サイバー保険との連携強化

6.2 組織への推奨事項

6.2.1 リスクの可視化

組織は「サイバーリスクの可視化」を最優先課題として取り組むべきである。リスク指標を用いた統計データから、ランサムウェアに感染した組織が非感染組織よりも高いリスク指標を記録していることが示されており、継続的なリスク監視が重要である。

6.2.2 Security by Contract の推進

委託先のセキュリティ対策として、「Security by Contract」アプローチを推奨する。これは、契約段階でセキュリティ要件を明確化し、"Same Data, Same Management"原則に基づく管理体制を構築することである。

6.2.3 多要素認証（MFA）の徹底

認証情報の漏洩リスクに対する最も効果的な対策として、多要素認証（MFA）の全面的な導入を強く推奨する。また、定期的なパスワード変更と権限管理の厳格化も重要である。

6.3 政策・制度面での展望

能動的サイバー防御に関する法案が2025年5月に成立予定であり、経済安全保障推進法における基幹インフラ事業者を中心としたサプライチェーンセキュリティ強化が進展する見込みである。これに伴い、インシデント対応体制のより一層の強化が必要となる。

7. 結論

2024年のサイバーセキュリティ環境は、脅威の高度化・複雑化と市場の急速な成長により、リスクアセスメントサービスの重要性が飛躍的に高まった年となった。日本企業が直面する課題は多岐にわたるが、適切なフレームワークの採用と継続的な改善により、効果的なリスク管理が実現可能である。

特に重要なのは、従来の年1回の評価から継続的監視への移行、経営層の積極的関与、そして技術革新を活用したリスク可視化である。また、委託先を含むサプライチェーン全体のセキュリティ強化は、今後の重要な課題として位置づけられる。

組織は、NIST CSF 2.0やISO 27001等の国際標準を基盤としつつ、自社の事業特性に応じたカスタマイズされたリスクアセスメント体制を構築することが求められる。同時に、AIや機械学習等の新技術を積極的に活用し、より効率的で精度の高いリスク評価を実現することが、持続的な競争優位性の確保につながるであろう。

今後の展望として、サイバーセキュリティは単なるIT部門の課題から、組織全体の戦略的経営課題へと位置づけが変化していく。この変化に適応し、プロアクティブなリスク管理体制を構築した組織が、デジタル社会における持続的成長を実現できると考えられる。

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