サイバーセキュリティ インシデント/トレンドレポート

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年は日本のサイバーセキュリティにとって転換点となった年であった。国内法人組織で公表されたサイバー攻撃被害は**587**件に達し、前年の383件から53.3%増加した。これは**1**日平均**1.7**件のペースで被害が発生していることを意味し、サイバー脅威が日常的なリスクとなったことを示している。

特に注目すべきは、サプライチェーン攻撃による二次被害の急増である。2024年の二次被害報告は213件に上り、全体の36.3%を占めた。これは委託先企業が攻撃を受けることで、委託元企業にも連鎖的に被害が拡大する新たな脅威パターンの定着を示している。

1. 国内サイバーセキュリティインシデント概況

1.1 インシデント発生件数の推移

2024年主要統計

- 総インシデント件数:**587**件(前年比+53.3%)
- 1日平均発生件数:**1.7**件
- ランサムウェア被害:**84**件(過去最大)
- 個人情報漏洩件数:**2,164**万件
- 二次被害件数:**213**件(全体の36.3%)

2024年のサイバーセキュリティインシデント発生状況は、前年と比較して大幅な増加を記録した。特に下半期における二次被害の急増が全体の件数押し上げに寄与している。2022年のEMOTETによる集中的な被害(140件)とは異なり、2024年は多種多様な攻撃手法による被害が分散して発生している点が特徴的である。

1.2 業種別被害状況

業種	インシデント件数	構成比	個人情報漏洩件数
製造業	30件	24.8%	840万件
卸・小売業	18件	14.9%	848万件
サービス業	14件	11.6%	-
教育・学習支援	14件	11.5%	-
情報通信業	13件	10.8%	145万件

製造業が最も多くのインシデントに見舞われた背景には、IoTデバイスの普及とデジタル化の進展による攻撃面の拡大がある。また、製造業のサプライチェーンの複雑性が、攻撃者にとって魅力的なターゲットとなっている。

1.3 攻撃手法別分析

1.3.1 ランサムウェア攻撃の深刻化

2024年のランサムウェア被害は84件と過去最大を記録し、被害は年々増加傾向にある。警察庁のデータによると、ランサムウェア被害報告は222件に達している。攻撃者はRaaS（Ransomware as a Service）モデルを活用し、攻撃の裾野を拡大している。

ランサムウェア攻撃の主要原因

1. **VPN**等ネットワーク機器の脆弱性：50%以上
2. 設定ミス：主にVPN機器の設定不備
3. アカウント侵害：認証情報の不正利用

1.3.2 不正アクセスによる被害

2024年のインシデントの61.1%が不正アクセスに起因している。特にクラウドサービスへの不正ログインが増加しており、多要素認証の導入不備が主要な要因となっている。

1.4 サプライチェーン攻撃と二次被害

2024年最大の特徴は、サプライチェーン攻撃による二次被害の激増である。株式会社イセトーの事例では、同社のランサムウェア被害が伊予銀行、東海信金ビジネス等の金融機関に連鎖的な影響を与えた。また、東京ガスエンジニアリングソリューションズの不正アクセス被害、ライクキッズのランサムウェア被害なども、多数の委託元企業に二次被害をもたらした。

2. グローバルサイバーセキュリティトレンド

2.1 AI技術を悪用したサイバー攻撃

2024年は人工知能（AI）を悪用したサイバー攻撃が本格化した年である。Center for Security and Emerging Technology（CSET）の調査によると、AI技術を活用したサイバー攻撃は50%増加すると予測されており、実際に以下のような攻撃が確認されている。

- **AI**生成フィッシングメール：60%の成功率を記録
- ディープフェイク技術：音声・画像偽造による詐欺
- 自動化された脆弱性探索：効率的な攻撃対象の特定
- マルウェア生成：生成AIによる不正プログラム作成

2.2 ゼロデイ脆弱性の動向

Google Threat Intelligence Teamの2024年年次レポートによると、2024年に確認されたゼロデイ脆弱性の悪用は75件で、前年の98件から減少した。しかし、エンタープライズプラットフォームを標的とした攻撃は44%に増加（前年37%）しており、企業を狙った攻撃の高度化が進んでいる。

2.3 サプライチェーン攻撃の国際的動向

2021年から2023年にかけて、サプライチェーン攻撃は431%の急増を記録し、2024年も継続的な増加傾向にある。主要な攻撃事例には以下が含まれる：

1. **Discord Bot Platform**攻撃（2024年3月）：悪意のあるコードがソースコードに直接注入
2. **npm** パッケージ攻撃（2024年1月）：GitHubに悪意のあるパッケージがアップロード
3. **CrowdStrike**障害（2024年7月）：世界規模のITサービス停止

2.4 クラウドセキュリティインシデント

2024年のクラウド関連セキュリティインシデントでは、60%以上の組織がパブリッククラウド利用に関連するセキュリティ事案を経験した。主要な脅威は以下の通りである：

- **Snowflake**攻撃：複数の顧客データベースが侵害
- 設定ミス：33%がクラウドデータ漏洩の原因
- 環境侵入攻撃：27%を占める

- クリプトマイニング：23％の攻撃が仮想通貨採掘目的

2.5 IoTデバイス攻撃の増加

SonicWallの「2025年サイバー脅威レポート」によると、IoT攻撃は2024年に124％増加した。特に以下の脆弱性が悪用されている：

脆弱性タイプ	構成比	主な影響
バッファオーバーフロー	28.25％	システム制御の乗っ取り
サービス拒否攻撃	27.20％	サービス停止
古いファームウェア	-	既知脆弱性の悪用

3. 注目すべき特定事例分析

3.1 国内主要インシデント

3.1.1 大手メディアグループへのランサムウェア攻撃

2024年6月、大手メディアグループがデータセンター内サーバーへの大規模なサイバー攻撃を受けた。この攻撃により255,241人分の個人情報が外部漏洩し、動画サイトの一時的なサービス停止や売上・利益の下方修正を余儀なくされた。

3.1.2 大手鉄道グループモバイルシステム障害

2024年5月、大手鉄道グループがサイバー攻撃を受け、関連モバイルサービスが一時的に使用不可となった。交通インフラへの攻撃として社会的影響が大きな事例となった。

3.1.3 国内大手インフラグループ顧客情報漏洩

大手インフラ子会社のネットワークへの不正アクセスにより、416万人分の顧客情報が漏洩した2024年最大規模の個人情報流出事案。連鎖的に京葉ガスも81万人分の顧客情報漏洩を公表した。

3.2 国際的な重大インシデント

3.2.1 Change Healthcare ランサムウェア攻撃

米国最大級の医療決済処理業者であるChange Healthcareが攻撃を受け、米国の医療システム全体に深刻な影響を与えた。約3分の1の米国人の個人健康情報が影響を受けたとされる。

3.2.2 CrowdStrike障害によるグローバルIT障害

2024年7月19日、CrowdStrikeのセキュリティソフトウェアアップデートの不具合により、世界中で大規模なシステム障害が発生。航空、金融、医療、放送などの重要インフラが影響を受けた。

4. 新興脅威と技術トレンド

4.1 生成AI悪用の脅威

2024年は生成AIの悪用が本格化した年である。以下のような新たな脅威が確認されている：

- 自動化されたフィッシング攻撃：大規模かつ個人化されたフィッシングメールの生成
- ディープフェイク詐欺：音声・映像偽造による振り込め詐欺の高度化
- マルウェア自動生成：専門知識なしでの不正プログラム作成
- 偽情報の大量生成：災害時等における偽の救助情報の拡散

4.2 フィッシング攻撃の進化

フィッシング対策協議会のデータによると、2024年のフィッシング報告件数は171万8,036件に達し、前年比約52万件（44%）増加した。特に注目すべき進化として以下が挙げられる：

1. リアルタイム型フィッシング：被害者の入力情報をリアルタイムで正規サイトに中継
2. AI生成コンテンツ：より自然で説得力のあるフィッシングメール
3. ボイスフィッシング（Vishing）：AI音声合成技術を活用した電話詐欺

4.3 暗号資産を悪用した犯罪の高度化

2024年は暗号資産を利用したマネーローンダリングが一層高度化した。特に匿名性の高い暗号資産「モネロ」への交換による資金洗浄が増加している。北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」による暗号資産関連事業者からの窃取も確認されている。

5. 脅威対策と推奨事項

5.1 組織に求められる優先対策

5.1.1 アカウントセキュリティの強化

- 多要素認証の導入：特にクラウドサービスアカウント
- アカウント監視：異常なログイン試行の検知
- 定期的なアクセス権見直し：最小権限の原則の徹底

5.1.2 VPNセキュリティの徹底

- ファームウェア最新化：定期的なセキュリティアップデート
- 設定の見直し：不要なアカウント・サービスの削除
- 多要素認証導入：VPNアクセスの二要素認証

5.1.3 サプライチェーンリスク管理

- 委託先セキュリティ監査：定期的なリスク評価
- 最小権限アクセス：委託先への情報提供の最小化
- 契約条項の強化：セキュリティ要件の明確化
- 代替委託先の確保：リスク分散とBCP策定

5.2 業種別対策指針

5.2.1 製造業

- IoTデバイスのセキュリティ強化
- OT（Operational Technology）システムの分離
- サプライチェーン全体のセキュリティ標準化

5.2.2 金融業

- リアルタイム不正検知システムの導入
- 顧客情報の暗号化強化
- ボイスフィッシング対策の徹底

5.2.3 自治体・教育機関

- 職員のセキュリティ教育強化
- レガシーシステムの刷新
- バックアップシステムの冗長化

5.3 新興脅威への対応

5.3.1 AI脅威対策

- AI検知システムの導入：ディープフェイク検出技術
- 従業員教育の強化：AI悪用手口の認識向上
- 多層防御の構築：技術的対策と人的対策の組み合わせ

5.3.2 ゼロトラスト原則の採用

- 継続的認証：アクセス毎の身元確認
- ネットワーク分離：マイクロセグメンテーション
- 行動分析：異常な行動パターンの検出

6. 今後の展望と課題

6.1 2025年以降の脅威予測

2025年に向けて、以下の脅威の拡大が予想される:

1. **AI**技術の悪用拡大:より高度で自動化された攻撃
2. 量子コンピューティング脅威:暗号化技術への挑戦
3. **6G**通信への移行リスク:新技術導入に伴う脆弱性
4. メタバース空間の脅威:仮想空間における新たなリスク

6.2 日本のサイバーセキュリティ政策

2024年5月、日本は「アクティブサイバー防衛法」を成立させ、より積極的なサイバー防衛への転換を図っている。また、警察庁はサイバー特別捜査部を設置し、国際共同捜査体制を強化している。

6.3 国際協力の重要性

サイバー犯罪の国境を越えた性質を踏まえ、国際的な協力体制の構築が不可欠である。ランサムウェアグループ「Phobos」の摘発では、日本、米国、EUROPOLの連携が成果を上げた。

7. 結論

2024年のサイバーセキュリティ環境は、従来の防御中心のアプローチでは対応困難な複雑性を増している。特にサプライチェーン攻撃による二次被害の拡大は、組織間の相互依存性が生み出す新たなリスクを浮き彫りにしている。

今後求められるのは、技術的対策の高度化だけでなく、組織文化の変革、人材育成の強化、そして業界を越えた協力体制の構築である。AI技術の発達は攻撃者と防御者の双方に新たな可能性をもたらしており、この技術革新の波を適切に活用できるかが、組織のサイバーレジリエンス向上の鍵となる。

サイバーセキュリティは、もはや技術部門だけの課題ではなく、経営戦略の中核に位置づけられるべき重要な要素である。2025年以降、この認識を共有し、継続的な投資と改善を行う組織のみが、激化するサイバー脅威に対抗し得るであろう。

参考資料:
• 警察庁「令和6年におけるサイバー空間をめぐる脅威の情勢等について」
• トレンドマイクロ「2024年年間セキュリティインシデントを振り返る」
• 東京商工リサーチ「2024年上場企業の個人情報漏えい・紛失事故調査」
• サイバーセキュリティクラウド「企業のセキュリティインシデントに関する調査レポート2024」
• フィッシング対策協議会「フィッシングレポート2024」
• Google Threat Intelligence「2024年ゼロデイレポート」

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コンサルティング合同会社に転籍。金融機関に対するコンサルティング業務に従事。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