NSHC Threat Research Lab, ThreatRecon Team
Document No. TR-CTI2025121102

Evolution of Composite Cyber Threats: 2025 Analysis and 2026 Key Response Strategies

- twitter.com/nshcthreatrecon
- service@nshc.net

11 Dec 2025

Table of Contents

- Do not share — The content of this work is provided only to specific customers of information service. Therefore, sharing this content without permission is prohibited.
- Non-disclosure agreement — This work is provided under a non-disclosure agreement (NDA), and violation of this agreement may result in legal consequences.
- Caution — Other copyright-related matters, including actions permitted under this license, must be confirmed with the information service provider before use.

Executive Summary

2025 年のサイバー脅威環境は過去のどの年よりも急激な変化と技術的進化を示しました。特にサイバー攻撃の自動化、供給網エコシステムを狙った侵入方式の高度化、人工知能(AI)と大規模言語モデル(LLM)の積極的悪用、国家基盤ハッキンググループの知能化された作戦遂行など、様々な要素が複合的に結合し、組織のセキュリティパラダイム全般を再定義するレベルの脅威様相が現れました。攻撃者たちはもはや単一ベクトルや単一技法に依存せず、異なる技術と社会工学要素を組み合わせた複合型攻撃体系を構築し、高い成功率と隠密性を確保しています。これらの変化は単なるセキュリティ脅威の増加を超え、産業と国家安全保障にまで影響を及ぼす構造的危険要因へと発展しました。

最も顕著な特徴は、供給網攻撃の爆発的増加である。2025 年の 1 年間で、オープンソースパッケージマネージャー(npm, PyPI など)や Chrome 拡張プログラム、GitHub リポジトリ、ソフトウェアアップデートサーバーなど信頼に基づくエコシステムを悪用する攻撃が多数捕捉された。特に Ethereum 開発者を対象とした Hardhat 悪用事例、悪性 npm パッケージ挿入事例、OAuth 認証奪取を通じたアカウントハイジャックなどは、攻撃者が開発者環境自体を掌握し、入力段階から組織内部網まで伝播する方式を好んでいることを示している。供給網攻撃は、一度の侵害で数百～数千の組織に連鎖的な被害を引き起こすことができ、サイバー攻撃エコシステムで最も魅力的な戦術として位置づけられた。

一方、フィッシングおよび社会工学に基づく攻撃は、AI 技術の導入によりさらに現実的で検出が困難に進化しました。攻撃者は生成型 AI を活用して自然な文体と文脈を持つフィッシングメッセージを自動生成し、ディープフェイク音声・映像技術を組み合わせて高位幹部を詐称する高度な BEC(Business Email Compromise)攻撃を実行しました。また、PaaS(Phishing-as-a-Service)エコシステムが活性化される中、MFA 回避型フィッシングキット、OAuth トークン奪取ツール、クラウドアカウント奪取パネルなどが容易に取引されています。これにより、2025 年には組織内部の認証システムが何度も突破され、情報の窃取、アカウントの改ざん、サービスの中断などの被害が多数報告されました。

2025 年はまた、ランサムウェアとインフォスティラー系 Malware の結合が本格化した転換点だった。伝統的なデータ暗号化ベースのランサムウェア攻撃を超えて、攻撃者は重要データの窃取と破壊、暗号通貨ウォレットの窃取、マルチプラットフォーム暗号化ツールの活用、高度な難読化・アンチ分析技術の結合などを通じて攻撃成功率を最大化した。LockBit, RansomHub, HexaLocker V2 など主要組織は Python·Go·Rust ベースのマルチプラットフォーム暗号化ツールを導入し、Curve25519·ChaCha20 ベースのキー交換システムを活用して分析と復旧を困難にした。また、スティーラー型 Malware と連携して攻撃初期段階でアカウントと認証トークンを収集し、ネットワーク内部で側面移動(Lateral Movement)を自動で行った後、最終的にランサム暗号化を実行する「二重・三重搾取体系」が広範囲に広がった。

国家支援ハッキンググループの活動もさらに大胆で攻撃的でした。ロシア・中国・北朝鮮・イランなど主要国家基盤グループは、エネルギー、防衛、金融、通信など重要インフラを対象にスパイ活動だけでなく、実際の破壊的攻撃を行いました。特にロシア-北朝鮮連携組織の活動強化、中国のValleyRAT・Salt Typhoon 基盤インフラ侵入、北朝鮮の KimJongRAT と暗号通貨窃取キャンペーン拡大は、2025 年を地政学的サイバー衝突の分水嶺としました。サイバー作戦が物理的戦争と結合される'サイバー-キネティック融合'現象も強化されました。

最後に、デジタルトランスフォーメーションが加速した環境で、クラウド・IoT・OT インフラの攻撃表面が幾何級数的に拡大しました。誤ったクラウド構成、脆弱な API エンドポイント、認証キーの露出、エッジデバイスのハッキング、OT/ICS ネットワーク侵入など、様々な攻撃ベクターが利用され、IoT 基盤のボットネットの超大型化により、単一攻撃で数十 Tbps 規模の DDoS 攻撃が発生する事例も報告されました。モバイル基盤 Malware も C2 を Firebase、Telegram などに偽装しながら、リアルタイム情報の窃取およびアカウント乗っ取り攻撃が頻繁に観察されました。

結果として、2025 年のサイバー脅威は技術的進化と攻撃者エコシステムの産業化を基盤に前例のない拡大を見せた。2026 年にはこの流れがさらに加速すると予想され、組織は既存の境界ベースの防御モデルから脱却し、人工知能ベースの脅威検出、Zero Trust アーキテクチャ、サプライチェーンセキュリティの強化、脅威インテリジェンス中心の防御戦略など新しい対応体制に移行する必要性がこれまで以上に高まった。続く章では、これらの分析に基づいて 2025 年の主要脅威動向と 2026 年の展望を詳細に検討し、組織が取るべき対応戦略を提示する。

2025年主要サイバー脅威動向

1. サプライチェーン攻撃の大規模化

2025 年のサイバー脅威で最も顕著な特徴は、サプライチェーン（Supply Chain）攻撃の爆発的拡散と高度化である。サプライチェーン攻撃は、もはや単一企業やサービス提供者の問題にとどまらず、産業全体や国家レベルで連鎖的被害を誘発する「大規模伝播型攻撃ベクトル」として定着した。攻撃者はソフトウェアエコシステムの信頼構造を悪用し、開発環境、配布経路、更新体系、認証インフラなど複数の地点を同時に狙うことで、これまでよりもはるかに速く広範囲に影響が波及した。

2025 年のサプライチェーン攻撃の核心的な特徴は、オープンソースパッケージエコシステムを対象とした攻撃の急増である。今年初め、npm・PyPI・RubyGems などのパッケージレジストリで多数の悪性パッケージが発見され、特に npm では Ethereum 開発者を狙って Hardhat プラグインを模倣したり、悪性スクリプトを挿入したパッケージが 20 個以上発見されるキャンペーンが報告された。攻撃者はタイポスクワッティング(typosquatting)技法を利用して、開発者がよく使用するパッケージ名に似た悪性パッケージを投稿し、インストール過程でプライベートキー・ウォレット情報・

API キーを窃取したり、悪性 C2 サーバーと通信するように構成した。このような攻撃は開発段階で Malware が注入されるため、実際のサービス展開時にユーザーと組織全体が危険にさらされる構造的問題を引き起こす。

また、Chrome 拡張プログラムとブラウザ生態系を悪用したサプライチェーン攻撃も増加しました。2025 年に発見された事例では、開発者の Google Web Store アカウントを奪取し、正常な拡張プログラムに悪性機能を挿入した後、自動更新を通じて数十万のユーザーに Malware ペイロードが配布される事故が発生しました。特に広告ブロッカー、個人情報保護ツール、業務自動化プラグインなど高い信頼性を持つ拡張が攻撃者に奪取され、攻撃者はこれを活用して OAuth トークン奪取、セッションハイジャック、パスワード奪取攻撃を連続的に実行しました。ブラウザ拡張プログラムの自動更新メカニズムが被害範囲を劇的に拡大させる結果を招きました。

API および CI/CD パイプラインを狙った攻撃も目に見えて増加した。攻撃者たちは GitHub Actions・GitLab Runner など自動化ビルドシステムを侵入してビルド産出物にマルウェアを挿入したり、環境変数を奪取し、OAuth 基盤の開発者認証を回避して全体プロジェクトアクセス権限を獲得しようとする試みを繰り返した。実際に 2025 年上半期に発見されたあるキャンペーンでは、攻撃者がサードパーティ API キーを奪取してビルド過程でマルウェアスクリプトを自動追加するように操作し、その結果 1,000 人以上の開発者環境が同時に汚染された事例も報告された。このような攻撃は開発者アカウント・自動化サーバー・ビルドプロセスがすべて接続された現代的 DevOps 環境で特に致命的である。

供給網攻撃のもう一つの主要な傾向は、クラウドベースの SaaS・MSP（Managed Service Provider）を介した大規模な拡散です。攻撃者は、一つの MSP またはクラウドソリューション業者に侵入することで、その業者を利用する数十から数百の顧客を同時に感染させる戦略を好みました。例えば、2025 年初めにあるグローバル IT アウトソーシング業者が侵害された事例では、内部ソフトウェアアップデートサーバーが Malware パッケージを配布するように変更され、同じプラットフォームを使用する複数の公共機関・医療機関・金融機関にまで二次被害が拡散しました。これは、供給網エコシステムの最上位に位置する MSP が侵害された場合、国家基盤全体が危険にさらされる可能性があることを示しています。

2025 年にはブロックチェーン基盤 C2 インフラを活用した供給網感染体系も登場した。 일부캠페인では Ethereum スマートコントラクトを Malware 命令伝達経路として使用し、一般的なドメイン/IP ブロックでは攻撃を無力化できないように設計された。 MisakaNetwork ボットネットキャンペーンのようにスマートコントラクトを通じて C2 アドレスを暗号化・配布する方式は、伝統的供給網攻撃と結合する場合、分析・対応の難易度を極度に高める。

総合すると、2025 年のサプライチェーン攻撃は、開発者エコシステム → ブラウザエコシステム → クラウド・SaaS → ブロックチェーンインフラへと拡張される多層的な形態を持っています。すべての段階が相互に接続された現代のデジタルエコシステムの特性上、攻撃者は弱いリンク一つに侵入するだけで全体のチェーンを掌握する結果につながります。組織は単純な脆弱性パッチやファイアウォールルールの強化だけでは対応できず、SBOM ベースのコンポーネント追跡、コード署名検証

の強化、開発者アカウントの保護、CI/CD セキュリティのモジュール化など、サプライチェーン中心のセキュリティ体制を全面的に再構築する必要があります。

2. フィッシングおよび社会工学攻撃の高度化

2025 年、フィッシングおよび社会工学に基づく攻撃は、従来のメールベースの手法を超えて、AI・ディープフェイク・クラウドアカウントの奪取・モバイルメッセンジャーの悪用・OAuth ハイジャックなど、複数の要素が結合した複合型攻撃へと発展しました。攻撃者は人間の心理的脆弱性と信頼に基づく意思決定構造を巧妙に悪用し、自動化された攻撃エコシステムの成熟により、規模と速度の面でも過去と比較できないほど拡大しました。

最も顕著な変化は、AI
を基盤としたフィッシング自動化の本格化である。攻撃者は大規模言語モデル（LLM）を活用した生成型 AI
を用いて、自然で文脈的一貫性の高いフィッシングメールを大量に生成した。単なる文法改善の段階を超え、標的の SNS
活動、メール履歴、業務プロファイルなどに基づいてカスタマイズされた文体を作り出し、「通常の内部コミュニケーションと区別が困難なレベル」のメッセージを生成した。特に 2025
年には、攻撃者コミュニティにおいて、いわゆる悪意ある LLM
モデルが登場し、スピアフィッシング文面生成、ソーシャルエンジニアリングシナリオ作成、フィッシングページの自動構成など、特定目的に最適化された機能を提供することで、フィッシング攻撃の産業化を加速させた。

これと並行して、ディープフェイク音声・映像技術を活用した BEC（Business Email Compromise）攻撃の急増も観測された。攻撃者は経営層の音声を高精度で学習し、実際の通話とほとんど区別できないレベルのディープフェイク電話を用いて緊急送金を要求したり、ビデオ会議用のディープフェイク映像を使って本人になりすまし、機密文書の提出を求める手法まで使用した。このようなディープフェイク型の社会工学攻撃は、従来のメールフィルタリングやセキュリティ意識向上トレーニングだけでは対処が困難な領域へと拡大しており、複数のグローバル企業で実際に金銭的損害へと発展した。

2025 年には PaaS(Phishing-as-a-Service)生態系が本格的に大衆化され、攻撃技術の障壁が大幅に低くなった。今や初心者の攻撃者でも、Web ダッシュボード形式で提供される PaaS プラットフォームを利用して、MFA 回避型フィッシングページ、リアルタイムセッションハイジャックツール、OTP プロキシサーバーなどを簡単に活用できるようになった。代表的なものとして Rockstar2FA のようなプラットフォームは、クラウド資格情報の窃取のために WebSocket ベースのリアルタイム C2 通信を提供し、ユーザーが入力する OTP を攻撃者に即座に伝達して認証を回避できるように設計

されている。このような自動化されたフィッシング生態系は攻撃成功率を大幅に向上させ、クラウド・SaaS サービスアカウントの窃取事件が世界的に急増する結果をもたらした。

また、OAuth および SSO 基盤の認証システムを悪用した攻撃も頻繁に発生しました。攻撃者は合法的なサービスのログイン画面にリダイレクトされるフィッシングリンクを使用し、OAuth 承認トークンを傍受してアカウントアクセス権を獲得しました。これはパスワードが露出しなくてもアカウントが乗っ取られる可能性があるため、検出と対応が非常に難しい攻撃手法です。2025 年に報告された複数のキャンペーンでは、攻撃者は企業内部の従業員に GitHub、AWS、Google Workspace アカウントの再認証メールを偽装して送り、OAuth トークンを盗み、その後、内部コードリポジトリ・メール・クラウド資産に長期間アクセスするために利用しました。

2025 年フィッシング攻撃のもう一つの特徴は、メッセンジャー・SNS・モバイル環境中心の攻撃拡大である。攻撃者は WhatsApp・Telegram・Discord などを通じて偽のゲームテスト、偽のモバイルアプリ配布、偽の銀行カスタマーセンターメッセージなどを通じて APK や悪性リンクを伝達し、モバイルアカウント・銀行情報・USSD データなどをリアルタイムで窃取した。代表的に FireScam のような Android 基盤 Malware は、GitHub.io ページや Telegram チャンネルを通じて自然に流布され、インストール後にユーザーの通知メッセージ・クリップボード・認証トークンを即座に窃取し、C2 サーバーに送信した。モバイルメッセージ基盤フィッシングは、個人端末から企業アカウントに拡張される BYOD 環境と絡み合い、組織全体を危険に陥れる可能性のある深刻な問題として浮上した。

視覚的要素を通じた社会工学技法も着実に発展しました。攻撃者は PNG・SVG 画像内にフィッシングリンクやスクリプトを密かに挿入したり、invisible iframe・base64 エンコーディング技法を活用してシグネチャベースの検出を回避しました。ClickFix のようにユーザーに「セキュリティチェックのためにアップデートが必要です」と案内する画面を表示し、Windows の PowerShell コマンドを実行するよう誘導する技法も発見されました。これらの攻撃は視覚的に正常なセキュリティ通知のように見えるため、社会工学に基づく脅威の効果を最大化します。

総合的に見ると、2025 年のフィッシング・社会工学攻撃は、AI 基盤の自動化 + 多チャンネル伝播 + MFA 回避技術 + モバイル・クラウド認証窃取 + ディープフェイク基盤の BEC という複合的な様相を示しています。これはもはや「ユーザーがリンクをクリックしないように教育するレベル」で対応できる脅威ではありません。組織は、フィッシング検出モデルの高度化、Zero-Trust 基盤の認証体系強化、アカウントアクセス権限モニタリングの自動化、ディープフェイク検出プロセスの導入など、多層的な防御戦略を必須で準備する必要があり、人間のセキュリティが技術的セキュリティと同様に重要な要素として再び浮上しています。

3. ランサムウェアおよびインフォスティーラーの進化

2025 年はランサムウェアとインフォスティーラー（情報脱取 Malware）の境界が事実上消滅した年だと評価できる。従来はランサムウェアがデータ暗号化を通じた金銭搾取にのみ集中していたが、今では攻撃の初期段階からインフォスティーラーを配布し、アカウント情報・トークン・セッション・クラウド認証キーなどを脱取し、これを基にネットワーク内部の権限上昇と側面移動（Lateral Movement）を自動化する方式で攻撃が結合されている。このような変化はランサムウェアの成功率と破壊力を同時に上昇させ、一度侵害が発生すると組織全体が瞬く間に掌握される事例が数回観察された。
最初に注目すべき変化は、多重恐喝戦略（Multi-extortion）の高度化である。従来のランサムウェアは「データの暗号化 – 復号鍵の費用要求」という単一の構造で運営されることが多かったが、2025 年に活動した主要組織は次の段階を組み合わせることで圧力の強度を大幅に高めた。

① データ脱取 → 顧客情報・財務データ・機密文書など流出
② 暗号化 → サーバーとワークステーションファイルのロック
③ データ公開による脅迫 → 流出サイトにサンプルファイルを掲載
④ DDoS 攻撃の併用 → サービス可用性の停止による追加的な圧迫
⑤ 3rd Party 圧迫 → 被害企業のパートナー社・顧客社に追加脅迫

RansomHub、8Base、Hunters International といった組織は、こうした多重恐喝戦略を標準化しており、重要な OT（Operational Technology）環境や医療・製造・物流分野を集中的に標的とした。実際に 2025 年には、製造業や医療機関の手術システムが中断される事例も発生するなど、ランサムウェア攻撃による被害が国家基盤サービスへと拡大した様子が繰り返し報告された。
2025 年ランサムウェア生態系のもう一つの重要な変化は、多重プラットフォーム暗号化技術の高度化および自動化である。攻撃者たちは分析の難易度を高め、迅速に拡散するために Python、Go、Rust ベースのマルチプラットフォーム暗号化技術を積極的に導入した。代表的な例として、HexaLocker V2 は Windows・Linux・VM 環境で全て動作するように設計されており、Curve25519 ベースのキー交換アルゴリズムと ChaCha20・AES 複合暗号化を適用して分析および復旧を困難にした。また、仮想環境検出・サンドボックス回避・アンチデバッグ機能が基本的に内蔵されており、初期分析段階で Malware 行為が明らかにならないように高度化された。
これと共に情報窃取型 Malware (Infostealer) の活動も急激に増加した。Lumma、Raccoon、RedLine、MetaStealer など主要スティーラーファミリーは 2025 年内に活動量が大きく増加し、様々な攻撃キャンペーンに活用された。特に Lumma はバージョン 4.0 アップデートを通じて「自動トークンエクスポート機能」、「Cloudflare Turnstile 回避」、「ブラウザ内 credential DB リアルタイム窃取」機能を備え、攻撃者はこれを通じて Google、Microsoft 365、AWS、GitHub など様々なクラウドベースのアカウントを大規模に窃取した。これらのアカウント窃取はその後のランサムウェア攻撃実行に重要な足場として活用された。

2025 年の攻撃フローは、スティーラー → 初期権限の掌握 → C2 接続 → 横方向移動 → ランサム実行という「単一自動化プレイブック」形式で構成される場合が多かった。Nova Stealer、Ageo Stealer
を含む複数の新型スティーラーは社会工学に基づく配布戦略と結合され、攻撃の初期段階から高度な情報を窃取し、攻撃者はこれを内部ネットワーク拡張に即座に再利用した。いくつかのキャンペーンでは、スティーラーが注入された初期ペイロードがシステム情報、ネットワーク構造、インストール済みセキュリティソリューションの一覧などを C2 に送信し、C2
サーバーが当該システムに最適化されたランサムウェアビルドを自動生成して再送信する「カスタムランサムウェア自動化」手法も登場した。
また 2025 年にはランサムウェアグループ間の協力構造がさらに強化された。例えば、LockBit 解体後、分散された開発者・運営者たちが複数の RaaS 組織に散らばりプラットフォームを維持しながら、同一のコード基盤を共有する変種が大規模に登場した。これは全体の生態系の変異速度を大きく高め、セキュリティ業界でのシグネチャベースの検出モデルを迅速に無力化する結果につながった。
特に北朝鮮およびロシア基盤の APT 組織は、金銭的目的と国家レベルの意図を結合したハイブリッド攻撃モデルを積極的に使用しました。北朝鮮グループは KimJongRAT・Konni などを活用し、金融・仮想資産分野を集中的に攻撃し、大規模な暗号通貨の窃取を続けました。また、一部のキャンペーンでは情報窃取後に該当組織にカスタマイズされたランサムウェアを配布し、追加の収益を得る戦略も確認されました。ロシア基盤の組織は OT 分野を直接攻撃したり、ICS ネットワーク内部で即時中断効果を引き起こす破壊性 Malware（Destructive Malware）とランサムウェアを結合する攻撃を実行しました。
総合してみると、2025 年のランサムウェアとインフォスティーラーの脅威は、① 多重恐喝戦略、② マルチプラットフォーム自動化暗号化技術、③ スティーラー基盤のアカウント奪取、④ カスタマイズされたランサムウェア自動化、⑤ 国家基盤組織の積極的活用という 5 つの特徴で要約できる。このような傾向は今後 2026 年にもさらに強化されると見られ、単純なエンドポイントレベルの防御だけでは対応が不可能な複合型攻撃体系が標準となると予想される。

4. 国家支援ハッキングの高度化および地政学的緊張に基づく攻撃

2025 年は国家支援ハッキンググループの活動がこれまで以上に攻撃的で戦略的に進化した年だった。地政学的な対立が高まる国際情勢の中で、サイバースペースはもはや単なる情報収集の舞台ではなく、軍事・外交・経済的目的のために活用される実質的な戦場として位置づけられた。特にロシア・中国・北朝鮮・イランなどの主要国家基盤グループは、既存の長期潜伏型スパイ活動を超えて、社会基盤施設破壊・金融混乱誘発・暗号通貨脱取・サプライチェーン侵入など多様な目的を持つ攻撃を大規模に実行した。

最も攻撃的な活動を見せた国はロシア拠点のハッキンググループだった。ロシアグループはウクライナ戦争の長期化状況の中で、エネルギー・物流・交通・政府機関などウクライナの重要インフラを対象に破壊的攻撃を継続した。多数のロシア拠点ハッキンググループは、Wiper 系 Malware を活用して電力供給システム・食料輸送ライン・通信網などを麻痺させる作戦を繰り返し遂行した。特に SectorC08 グループは 2025 年基準で最も多くの攻撃キャンペーンを展開したウクライナターゲットグループとして記録されており、彼らは低価格のスピアフィッシングと迅速な配布速度を活用して持続的な内部ネットワーク侵入を試みた。このようなロシア拠点ハッキンググループはウクライナ外部国家、特に NATO・EU 加盟国政府機関と国防関連企業を対象にスパイ活動を拡大するなど、サイバー戦場の範囲を国際的に拡張した。

中国拠点のハッキンググループも 2025 年にグローバル規模の攻撃を実行した。多数の中国拠点ハッキンググループは、アメリカ本土の電力網・海軍通信網・防衛軍ネットワークなどの核心インフラに長期間潜入し、情報収集と非常時の撹乱攻撃を同時に準備した。SectorB108 グループは特定のアメリカ州の防衛軍ネットワークにほぼ 1 年近く潜伏し、ネットワーク移動経路・応答体系・セキュリティポリシーなどを収集し、SectorB73 グループは IoT ルーターとエッジ機器の脆弱性を悪用してアメリカ電力網内部の構造を把握する作戦に集中した。中国拠点のハッキンググループはまた、アジア・ヨーロッパ・南米まで攻撃範囲を拡大し、民間衛星・通信事業者・航空物流会社などを狙う攻撃を実行するなど、全世界的な作戦能力を誇示した。

2025 年最も急速に成長した脅威の一つは、北朝鮮ベースのハッキンググループによる金融中心の攻撃戦略です。北朝鮮は暗号通貨の窃取を国家経済戦略の一部としており、2024 年に約 13 億ドル以上の暗号通貨を窃取した後、2025 年にも Bybit 事件のような超大型ハッキングを通じて世界中の仮想資産市場に深刻な衝撃を与えました。Kimsuky・Lazarus・Andariel などの北朝鮮組織は、仮想通貨取引所・フィンテック企業・国際金融機関などを対象にスピアフィッシング・ソーシャルエンジニアリング・トロイの木馬ベースの侵入を行い、KimJongRAT・Konni・ValleyRAT などの高級 Malware を活用してアカウント・資金フロー・ウォレット情報を窃取しました。また、一部のキャンペーンでは内部者になりすました偽装就職を試み、長期的に内部運営情報を収集する戦略も確認されました。

イランを拠点とするハッキンググループも、中東地域における地政学的緊張の高まりの中で攻撃活動を強化した。イランの複数のハッキンググループは、イスラエルおよびサウジアラビアの政府機関、エネルギー施設、輸送インフラなどを対象に、ワイパー系マルウェアとランサムウェアを組み合わせた攻撃を展開した。彼らはサイバーと心理戦を結合した戦略を用い、偽情報の流布、ウェブサイトの改ざん、メディアプラットフォームの侵害などを通じて社会的混乱を誘発する手法も使用した。

2025 年国家基盤ハッキンググループの攻撃の技術的特徴は大きく四つに要約できる。

第一に、攻撃者たちは供給網エコシステムへの侵入を戦略的に活用しました。中国とロシアのグループは、ソフトウェア更新サーバー・開発者アカウント・API 認証トークンなどを奪取し、多数の機関と企業が使用するソリューションを汚染する方法で攻撃範囲を拡大しました。第二に、C2 インフラの隠蔽技術が極度に発展しました。ブロックチェーン基盤の命令送信、VPN・プロキシチェーン・合

法的 SaaS の悪用、偽の Tor ブリッジ運営など多様な技法を使用して検出の難易度を高めました。第三に、マルチプラットフォーム攻撃能力が強化されました。Windows・Linux・macOS だけでなく、ルーター・NAS・VoIP 機器・ファイアウォール機器などエッジデバイスを積極的に狙う傾向が拡大し、OT/ICS 機器の脆弱性基盤侵入も繰り返し報告されました。第四に、国家基盤組織が金銭目的および破壊目的を同時に追求する事例が増加しました。北朝鮮は金融奪取を一次目標としていますが、特定の時期には妨害作戦や情報収集を併行し、ロシアは戦略的目標達成のためにサイバー攻撃と物理的作戦を混合して使用する様相を見せました。

総合的に 2025 年国家支援ハッキンググループは軍事的・政治的・経済的目的が混合された戦略的攻撃モデルに発展しており、地政学的衝突が深化するほど国家はサイバー空間でより大胆で攻撃的な行為を試みる可能性が大きくなっている。このような流れはグローバルセキュリティ秩序を大きく揺るがしており、2026 年にも国家基盤ハッキング組織の高度化された活動は持続することが予想される。

5. クラウド・IoT・モバイル攻撃の拡大

2025 年はクラウド、IoT、エッジ(Edge)、モバイル環境が企業・公共機関の核心 IT インフラとして完全に定着した中で、これらの領域を狙った攻撃が幾何級数的に増加し、技術的にも高度化した時期だった。攻撃者たちはクラウド構成エラー、認証キー流出、API 脆弱性、IoT 機器のデフォルトアカウント、モバイルメッセンジャー基盤の社会工学など異なる要素を組み合わせて複合的な侵入シナリオを構築した。その結果、クラウドおよびエッジコンピューティングを中心とする現代 ICT インフラが直ちに攻撃者の戦略的標的となり、これは既存のオンプレミス基盤防御体系だけでは対応不可能な新しいリスク環境を生み出した。

まず、2025 年のクラウドセキュリティ脅威の核心は、誤った設定(Misconfiguration)と認証資格情報の窃取が全体のインシデントの中心にあったという点です。多くの AWS S3 バケット、Azure Blob Storage、Google Cloud Storage インスタンスがパブリックに露出した状態で発見され、API キー・サービスアカウント JSON ファイル・Access Token などがコードリポジトリ(GitHub, GitLab)に誤ってアップロードされる事故が頻繁に発生しました。攻撃者は GitHub の高度な検索または自動クロールツールを使用して露出した API 資格情報を見つけ出し、クラウド内部リソースを掌握し、データベース抽出・仮想マシン暗号化・リソース窃取(Cryptojacking)などを迅速に実行しました。特に Cryptojacking は低コスト・低リスクの攻撃であるにもかかわらず、利用可能なリソースを大量に消耗させ、企業のクラウドコストを急増させることで間接的な被害を引き起こしました。

また、クラウドネイティブ環境（Kubernetes, Docker など）を狙った攻撃も急増しました。 一部の攻撃者は、Kubernetes の露出された API ポートを通じてクラスター制御権限を獲得したり、誤って設定された RBAC (Role-Based Access Control) を悪用して Pod を生成し、悪性コンテナイ

メージを配布しました。攻撃者が内部でコンテナイメージを変更して悪性スクリプトを挿入し、自動更新機能を通じて複数のマイクロサービスに伝播させる事例も発見されました。これは事実上、コンテナベースのサプライチェーン攻撃と同じ構造を持ち、クラウド環境が持つ簡便なデプロイ特性が攻撃拡散を加速する要素として作用しました。MSA (Microservice Architecture) 構造では、一つのサービス侵害が他のサービスに伝播しやすく、攻撃者が単一のエントリーポイントを確保するだけで全体システムを掌握する事例が多数報告されました。

2025 年、IoT 分野ではボットネットの規模が既存と比較できないほど巨大化した。代表的に発見された'Aisuru'ボットネットは、全世界の数十万台の IoT 機器（監視カメラ、家庭用ルーター、NAS、スマートプラグなど）を感染させ、29.7Tbps 規模の DDoS 攻撃トラフィックを生成するのに使用された。これはインターネット歴史上最も大きな規模の攻撃の一つとして記録され、5G・ブロードバンドインターネット環境の拡散により、IoT 端末が大容量トラフィック攻撃インフラに変わる危険性を鮮明に示した。IoT 機器の大部分は、デフォルトパスワード、脆弱なファームウェア、自動アップデート非対応などの構造的脆弱性を持っており、攻撃者は Shodan・Censys のようなスキャニングツールを活用して脆弱な機器をリアルタイムで識別し、全世界的に迅速に感染を拡散させた。

産業用 IoT、すなわち OT（Operational Technology）および ICS（Industrial Control System）環境を狙った攻撃も増加した。攻撃者は産業用ゲートウェイ、PLC、SCADA 機器のプロトコル脆弱性を悪用し、遠隔操作・設定変更・センサー値の改ざんなどを試みた。特にロシアおよびイランを拠点とするハッキンググループは、エネルギー分野や発電所の制御網を対象に撹乱型攻撃を実施しており、特定の ICS 機器を悪用して物理的障害を誘発しようとする試みも報告された。これは、サイバー攻撃が単なる情報窃取を超え、実際の物理的被害を引き起こす「サイバー・フィジカル融合脅威」が本格化したことを示している。

モバイル環境も攻撃の主要な標的となりました。FireScam・Flubot・Xenomorph のようなモバイル基盤の Malware は Telegram・Discord などのメッセンジャーを通じて拡散され、Android Accessibility API を悪用して通知メッセージ・OTP・クリップボード・銀行アプリのデータをリアルタイムで窃取しました。攻撃者は GitHub Pages、Telegram チャンネル、偽のモバイルアプリ更新サイトなどを通じて正常なアプリケーションに偽装した悪性 APK を配布し、多くの被害者が発生しました。また、iOS 環境でもウェブ基盤のフィッシングとモバイルプロファイルインストール誘導手法を通じてデバイスを部分的に制御する攻撃が登場しました。BYOD(Bring Your Own Device)環境が拡散した組織では、これらのモバイル基盤攻撃が内部業務アカウントの窃取に直結する事例が多くありました。

2025 年クラウド・IoT・モバイル攻撃の総合的特徴は ① 攻撃表面の拡大、② 認証情報の窃取中心攻撃体系、③ 自動化された IoT 感染、④ コンテナベースのサプライチェーン攻撃、⑤ モバイル-クラウドアカウント連携窃取で要約される。攻撃者たちは既存のネットワーク境界が事実上解体された現代インフラの特性を正確に把握し、人が直接アクセスするレイヤーよりも API・メタデータ・自動化アカウントなどを優先的に攻撃した。このような変化は企業が既存のオンプレミス中心のセキュリ

ティ戦略を維持する場合、即座にリスクにさらされる環境を意味し、クラウドおよび IoT 中心の新しいセキュリティパラダイムの構築が切実に求められる。

2026年5大サイバー脅威展望

1. AI を基盤とした高度化攻撃の拡散

2026 年のサイバー脅威環境で最も核心的で影響力のある変化は、AI 基盤の攻撃の本格的な大衆化と自動化された攻撃生態系の拡散である。2025 年の一年間にわたり、悪性 LLM、AI 基盤のフィッシング自動化、ディープフェイク基盤の社会工学、AI 補助型 Malware など多様な事例が登場したが、2026 年にはこれらの技術が初期実験段階を超えて完全な攻撃体系に統合されると予想される。これはサイバー攻撃の速度・正確性・規模を過去と比較できないほど引き上げるものであり、自動化された大規模攻撃の時代が本格的に始まることを意味する。

最初に注目すべき変化は、「自律攻撃システム(Autonomous Attack System)」の登場可能性です。現在まで攻撃者は、LLM を利用してフィッシング文を自動生成したり、脆弱性分析を補助するレベルで AI を活用していました。しかし、2026 年には攻撃者が AI を基盤とした統合攻撃フレームワークを構築し、初期侵入から情報収集、権限昇格、側面移動、データ脱取、最終ペイロード実行まで全過程を自動化する攻撃体系が登場する可能性が高いです。これらのシステムは、状況に基づく意思決定機能を備え、自ら攻撃経路を選択し、内部ネットワーク探索結果に応じて最適な攻撃モジュールを呼び出す形で進化することができます。これは、セキュリティチームが侵害を検知し対応するための時間的余裕を劇的に減少させます。

また、2026 年に最も広く拡散するとみられる脅威の一つが、AI を基盤としたポリモーフィック（Polymorphic）およびメタモーフィック（Metamorphic）マルウェアの爆発的増加です。AI モデルがコード変形をリアルタイムで実行できるようになることで、シグネチャベースの検知体系は事実上無力化されると予測されます。攻撃者は同一の機能を持つマルウェアを数百～数千の変形版として自動生成でき、各亜種は構造的・言語的特徴が異なるため、分析および検知の難度が大幅に上昇します。LLM ベースのマルウェア生成器は API 形式でダークウェブ上で販売される可能性があり、「入力された目標環境に最適化されたマルウェア」を自動生成する形へと進化する可能性があります。

2026 年には AI が脆弱性分析およびエクスプロイト開発プロセスにも直接関与することが予想される。最近の研究では、AI がセキュリティアドバイザリやパッチ情報を基に数時間以内にエクスプロイトコードを生成できることが確認されており、これは脆弱性公開後の攻撃までの時間を劇的に短縮するだろう。攻撃者は AI に特定のソフトウェアバージョンの脆弱性情報を分析させ、自動で PoC を生成した後、内部テストを経て実際の攻撃用エクスプロイトを迅速に完成させることができる。これ

は既存の攻撃開発サイクルを根本的に短縮し、ゼロデイ開発能力を持つ国家基盤攻撃者だけでなく、一般のサイバー犯罪者まで高度な攻撃を実行させる危険要素である。

AI 기반社会工学攻撃も 2026 年にさらに拡大されるだろう。ディープフェイク技術の発展により、リアルタイム音声合成・リアルタイム映像生成が可能になり、BEC・CEO なりすまし攻撃は実際のビデオ会議参加レベルまで精巧になる可能性が高い。攻撃者は対象者の音声と顔を完璧に模倣してビデオ会議中に送金要求をしたり、セキュリティプロセスを回避するよう指示することができ、これは既存の人的検証方式では識別が事実上不可能な新しいリスク環境を引き起こす。ここに AI チャットボットを通じたリアルタイム対話ベースのフィッシングまで結合されると、攻撃者はマルチチャネル・マルチステージ社会工学攻撃を自動化されたシステムで実行することができる。

また、2026 年には AI がセキュリティソリューションを回避する機能まで学習する可能性がある。AI モデルがサンドボックス検出、メモリ分析回避、API 呼び出しパターン攪乱など Malware 分析回避技術を自ら学習し最適化する方式で動作することができる。つまり、攻撃者は「この環境で検出されない方式で動作するようにしろ」という形で AI に指示を出し、AI は自動で検出を回避するペイロードを生成する方式である。このような攻撃パターンは既存 EDR/XDR モデルの検出ロジックを迅速に無力化することができ、攻撃者と防御者間の技術軍備競争が AI 中心に激しく展開されるだろう。

AI
を利用した攻撃の拡大は、サイバー犯罪エコシステムの産業化とも密接に関連している。ダークウェブでは、AI ベースの攻撃自動化ツール、悪性 LLM
API、フィッシング自動生成システム、詐欺メッセンジャーボットなど、Crimeware-as-a-Service 型のサービスが大量に出現する可能性が高い。攻撃経験のない初級攻撃者であっても、AI
サービスを利用することで高度なフィッシング、マルウェア開発、ネットワーク侵入を実行できるようになり、これにより攻撃エコシステム全体が爆発的に拡大する結果を招くと考えられる。

総合すると、2026 年は AI が攻撃者の核心的な武器として位置づけられ、サイバー攻撃の範囲・速度・知能が飛躍的に拡大する転換点となると見られる。既存の防御体系ではこれらの変化に対応できず、セキュリティ業界は AI 基盤の防御技術、AI 動作分析、モデル無欠性検証、AI 行動プロファイリングなど新しい形態の防御戦略を用意する必要がある。AI が攻撃の加速器となるだけに、AI 基盤のセキュリティ体系なしでは 2026 年以降のサイバー脅威環境での生存が難しくなるだろう。

2. ゼロデイに基づくサプライチェーン攻撃の拡散

2026 年に最も深刻に懸念される変化の一つは、供給網攻撃が既存の単純なアップデート汚染やパッケージ改ざんのレベルを超え、ゼロデイ脆弱性を基盤とした構造的侵入方式で本格的に拡散する可能性が高いという点です。2025 年にもいくつかの供給網関連事故が発生しましたが、これらは主に攻撃者が既存のパッチされていない脆弱性、開発者アカウントの奪取、悪性ライブラリの挿入などを利用したものでした。しかし、2026 年には攻撃者があらかじめ供給網構成要素自体でゼロデイを先制

的に発掘し悪用する戦略に転換することが予想されます。これは大規模な拡散性と検出回避力という供給網攻撃の固有の特徴とゼロデイの隠密性が結合することにより、過去よりもはるかに脅威的で対応が難しい形態の攻撃生態系を生み出すでしょう。

最も懸念される点は、オープンソース生態系の脆弱性がさらに深刻化することです。npm、PyPI、Maven Central のようなパッケージレジストリは、世界中の数百万の開発者にリアルタイムで使用されており、主要なライブラリは数万のプロジェクトで核心コンポーネントとして機能しています。これらの生態系は透明性と開放性を利点としていますが、同時に攻撃者が特定のライブラリ内部でゼロデイを発見し、悪性ロジックを注入した場合、その影響範囲が想像を超えるほど拡大する可能性があることを意味します。攻撃者が外部依存性の単一の脆弱性を悪用して、数千のプロジェクトに Malware が伝播することは、もはや理論的な可能性ではなく現実的な脅威となっています。

クラウドと SaaS 環境が拡大するにつれて、供給網攻撃のリスクはさらに増幅された。2026 年には、単一の SaaS または MSP(Managed Service Provider)のゼロデイが国家単位のセキュリティ事故につながる可能性も高い。例えば、Azure AD、AWS IAM、Google Identity のようなグローバル認証プラットフォームでゼロデイが発見された場合、単一の脆弱性が全世界の数十万の組織のアカウント・トークン・環境変数を同時に露出させる結果につながる可能性がある。このようなタイプの攻撃は、被害組織が直接攻撃者にならなかったにもかかわらず、第三者の脆弱性によって連鎖的に被害を受けるという点で、供給網攻撃の本質的特性と正確に一致する。

さらに、開発者環境と CI/CD パイプラインは 2026 年にサプライチェーン攻撃の新たな主要戦場となるだろう。開発者が使用する IDE、ビルドツール、パッケージマネージャー、Git クライアントなどはソフトウェアサプライチェーンの最上部に位置しているため、これらのツールでゼロデイが発見された場合、攻撃範囲は幾何級数的に拡大する。攻撃者は開発者のセッションをハイジャックしてリポジトリを操作したり、ビルド過程に悪性スクリプトを注入して後に配布される正式ソフトウェアに悪性要素が含まれるようにすることができる。この過程は正常なビルドプロセスをそのまま維持したまま内部的にのみ改ざんが行われるため、既存のコードレビュー・テストプロセスでは検出がほとんど不可能である。

これと共にゼロデイ取引市場も 2026 年にさらに活性化されると見られる。ダーク웹では既に高価なゼロデイが取引されているが、サプライチェーン攻撃に特化したゼロデイは高い収益性と攻撃成功率のため、さらに高い価値を持つことになるだろう。特に国家基盤組織が攻撃者集団に資金を提供したり、直接ゼロデイを購入する可能性が高いため、サプライチェーン関連のゼロデイが戦略的に悪用される可能性も大きく増加している。一部では‘Zeroday-as-a-Service’形態のサービスが登場し、特定のパッケージエコシステムや SaaS プラットフォームを狙ったカスタマイズされたゼロデイを提供する市場が作られる可能性があるという展望も提起されている。

ランサムウェア生態系との結合も見過ごせない。供給網侵害を通じて攻撃者が多数の組織に同時に初期アクセス権限を得ることができれば、この中から価値が高い組織を選別してカスタマイズされたランサムウェアを投入する戦略が 2026 年にはさらに標準化されるだろう。すでにスティーラー基盤の

アカウント奪取と RaaS 運営方式が結合し、多層的攻撃構造が一般化しており、ここに供給網基盤の初期侵入経路が結合される場合、その波及力は過去と比較できないほどに拡大するだろう。
このように、2026 年は供給網攻撃が単純なソフトウェア変造の段階を超え、ゼロデイの戦略的悪用と結合した超大型サイバー攻撃の時代になる可能性が非常に高い。組織はもはや直接保有するシステムだけを防御するだけでは十分ではなく、自身が使用するすべてのライブラリ・サービス・SaaS・クラウドインフラ全般に対するセキュリティレベルを持続的に検証する体制が必須である。SBOM 基盤の構成要素追跡、コード署名検証強化、開発者アカウント防御、CI/CD パイプラインセキュリティ強化などは、これらの脅威環境で必ず要求される核心的な対応戦略となるだろう。

3. 多重プラットフォーム・AI融合ランサムウェアの深化

2026 年に Ransomware は既存の単純なファイル暗号化攻撃を超え、AI 基盤分析・多重プラットフォーム拡散・情報脱取型 Malware との結合を特徴とする複合的形態に進化することが予想される。
2025 年までに Ransomware は既に RaaS モデルを中心に産業化され、供給網攻撃・情報脱取・Deepfake 基盤脅迫など多様な形態と結合する傾向を見せていたが、2026 年にはここに AI 自動化エンジンが加わり、攻撃の全過程が人間の介入なしに体系的に遂行される水準に達するだろう。これは Ransomware が「単一目的ツール」から脱し、自律的意思決定を遂行する攻撃システムとして位置づけられる変化を意味する。
まず最も重要な変化は、2026 年にランサムウェアが AI 基盤の自己最適化(Self-Optimization)機能を備える可能性が非常に高いという点です。攻撃者はもはや事前に定義されたスクリプトや固定された攻撃経路を使用する必要がなくなり、Malware は感染したシステム内部の環境を分析して最も効果的な攻撃戦略を自ら選択できるようになります。例えば、AI がシステムにインストールされたアンチウイルス・EDR・バックアップソリューションの種類を把握して回避可能な経路を選択したり、内部ネットワーク構造をスキャンして価値の高いサーバー・データストアを優先的に攻撃する方法です。このような自律攻撃方式は、攻撃の速度だけでなく破壊力を劇的に増加させ、検知対応時間を大幅に短縮し、既存のセキュリティ体制が攻撃の開始を認識する前にシステムを完全に掌握する形に発展する可能性があります。
このとともに、ランサムウェアは Multi-Platform 環境を狙った汎用攻撃ツールへと進化している。過去には Windows 基盤エンドポイントを重点的に狙っていたが、徐々に Linux サーバー・コンテナ・仮想化ハイパーバイザー・NAS 及び SAN 機器・ルーター・IoT 機器まで攻撃対象が拡張された。特にクラウド環境が急激に増加するに伴い、Kubernetes・Docker・VMware ESXi など運用インフラの中心を成すプラットフォームが攻撃の主要標的となっている。このような拡張は単にランサムウェアの攻撃対象を増やすことを意味しない。攻撃者は AI 分析機能を基に各プラットフォームの脆弱性・権限構造・サービス形態を把握し、各環境に最適化された暗号化ツールを自動生成できるように

なる。その結果、一つの感染イベントで組織内の多様なプラットフォームと環境が同時に麻痺する最悪のシナリオが現実化する可能性が高い。

2026 年にはランサムウェアが情報脱取型インフォスティーラーと完全に結合した形態に進化することも重要な特徴である。2025 年までにすでに Lumma Stealer、RedLine、MetaStealer など情報脱取 Malware がランサムウェアと結合する事例が捕捉されていたが、2026 年にはこの結合が標準攻撃フローになる可能性が高い。攻撃はまずインフォスティーラーが組織内部のアカウント・セッション・クッキー・OAuth トークン・クラウド API キーなどを脱取し、AI エンジンがこのデータを分析して組織の重要資産・権限構造・バックアップパスなどを自動で把握する。その後、この情報を基にカスタマイズされたランサムウェアが投入され、暗号化戦略を最適化する。このような方法は攻撃者の成功率を飛躍的に増加させ、暗号化自体が始まる前からすでに被害範囲が確定する構造を作る。

また、2026 年には AI を活用したカスタマイズされたランサムウェアビルドの自動生成が大衆化される可能性が高い。攻撃者は単純に「対象環境情報」だけを提供すれば、AI がその環境に適した Malware を自動で生成してくれる。例えば、特定組織のサーバー構造・EDR パターン・バックアップ方式を分析し、それらの要素を回避または破壊する方法でカスタマイズされた攻撃コードが自動ビルドされる形態だ。これは既存の画一的なランサムウェア攻撃とは異なり、被害者ごとに固有の弱点を正確に狙う精密攻撃につながる。

最後に、RaaS 生態系への AI 統合は、攻撃をより体系化・自動化された産業へと進化させる上で大きな役割を果たすと考えられる。一部の組織はすでに、被害者の財務状況・保険加入状況・企業規模に基づいて身代金を自動算出するシステムを運用しており、2026 年には AI ベースの交渉ボット、脅迫メッセージ自動生成器、データ公開スケジューリングシステムなどが組み合わされ、攻撃の全工程が「サービス化」される可能性が高い。これはランサムウェア攻撃の参入障壁をさらに低下させ、攻撃生態系を爆発的に拡大させる結果につながるとみられる。

総合すると、2026 年のランサムウェアは単なる金銭強奪用 Malware の範疇を超え、AI によって駆動される複合攻撃エンジンであり、マルチプラットフォームインフラを同時に麻痺させる戦略兵器として位置づけられることになるだろう。供給網攻撃・情報脱取・仮想化環境拡散・AI 自動化が結合し、組織は単一攻撃イベントだけでも致命的な被害を受けるリスクにさらされることになり、既存の対応戦略はこのような変化を防御するには全く不十分である。2026 年以降のランサムウェアは「より複雑でより速く、より精密な攻撃モデル」へと進化し、これに対する備えは組織の生存の核心要素となるだろう。

4. 地政学的緊張に基づくサイバー戦の深化

2026 年には国家基盤ハッキンググループの活動が以前どの時期よりも攻撃的で戦略的に展開されると展望される。これは単純にサイバー攻撃の頻度が高まるという意味を超え、サイバー空間が国際紛争と国家戦略の核心戦場として位置づけられる変化が本格化するという点で重要な含意を持つ。特に

ロシア・中国・北朝鮮・イランをはじめとする主要国家は、既存の情報収集中心作戦から脱却し、実際の物理的基盤施設を無力化したり社会的混乱を引き起こす攻撃を積極的に試み、影響力を拡張している。このような変化は、サイバー戦がもはや局地的な技術紛争ではなく、地政学的競争の必須要素となったという事実を示している。

まずロシアの場合、ウクライナとの長期的な武力衝突の中で、サイバー戦はすでに主要作戦手段の一つとして定着しました。ロシアのハッキンググループは単純なスパイ活動を超えて、電力・ガス・物流・通信網を麻痺させるワイパー基盤の攻撃を継続的に行ってきました。これらの組織は短期間の攪乱ではなく、長期的な心理戦・物理的圧迫・政策的混乱を引き起こすための複合的な作戦を展開する傾向を示しており、2026 年にはこれらの攻撃範囲がウクライナ支援国や西ヨーロッパの主要インフラにまで拡大する可能性が高いです。特にロシア基盤のハッキンググループは IoT・エッジデバイス・VPN 機器・産業用コントロールシステムを積極的に利用して攻撃経路を多様化し、サプライチェーン侵害を通じて連鎖的に拡散する攻撃を好む特徴を示しています。

中国のハッキンググループは、より長期的で体系的なアプローチを取ると予想される。2025 年に注目された SectorB73 グループと SectorB108 グループの事例は、中国がアメリカ本土の電力網と軍事通信網に数年単位の潜伏作戦を実行していることを示している。これらは単に脆弱性を悪用するレベルを超え、IoT ルーター・通信機器・エッジゲートウェイなど国家基盤デジタルインフラの末端要素を掌握し、内部構造を広範囲に収集する偵察作戦を遂行する。2026 年には、これらの長期潜伏型攻撃がさらに精巧になる可能性が高く、有事の際に物理的障害や通信攪乱に即座に転換できる準備された攻撃体系を整えると予想される。これは伝統的な軍事的脅威とサイバー脅威が完全に結合する様相として解釈できる。

一方、北朝鮮は経済的圧迫と制裁環境の中で金銭的利益を得るためのサイバー作戦を強度高く遂行することが予想される。2024~2025 年の間に大規模な暗号通貨脱取事件を主導した北朝鮮は、2026 年にも仮想資産プラットフォーム・フィンテック企業・国際金融機関を主要ターゲットにして精巧な攻撃を持続する可能性が大きい。しかし、最近数年間、北朝鮮は金銭的目的だけでなく軍事・政治的目的を結合した複合的攻撃も試みてきた。例えば、特定期間には軍事情報脱取と社会混乱誘発を同時に狙うキャンペーンを遂行し、他の時期には経済的目的の攻撃を併行する方式で目標を多層化する傾向が現れる。2026 年には北朝鮮がハッキンググループを通じたサイバー-物理攻撃能力まで拡大する可能性も提起されている。

イランはまた、地政学的緊張が高まる中東地域でサイバー攻撃を積極的に活用している。イランのハッキンググループは、政府機関・エネルギー施設・航空および輸送インフラを対象にワイパー基盤の破壊攻撃を継続しており、特定の時期には心理戦と情報操作を組み合わせて社会的不安定を高める戦略を使用した。イランのサイバー戦はしばしばテロ団体や非国家行為者と結合した形で現れることもあり、これは検出を困難にし、対応をさらに複雑にする要因として作用している。

2026 年国家基盤ハッキンググループ脅威の特徴の一つは、金銭・政治・軍事目的が混在したハイブリッド攻撃モデルが拡大するという点である。攻撃者たちは単一の目的を追求する代わりに、一つのキャンペーンで同時に複数の目的を達成する方式で戦術を変化させている。例えば、特定産業を狙っ

た攻撃でまず金融情報を脱取し、その後サプライチェーン侵害を通じて産業インフラを攪乱し、最後に政治的メッセージを拡散させる形態の攻撃が登場する可能性がある。このような多層的攻撃は、被害範囲を予測するのが難しいだけでなく、攻撃の出発点と目的を把握するのに多くの時間と分析資源が必要であるという点で、防御の側面での負担が大きく増加する。

また、国家基盤のハッキンググループ間の連合型攻撃や間接支援体制もますます強化されています。最近数年間、ロシアと北朝鮮間の協力の可能性が継続的に提起されており、他の国家も非正規組織・サイバー傭兵・犯罪グループを非公式に活用する事例が増えています。このような流れは攻撃の匿名性と拡散力を大幅に高め、国際社会の責任追及を困難にする要因として作用します。

総合的に見ると、2026 年の地政学的緊張に基づくハッキンググループの脅威は、攻撃範囲・目的・技術・戦術がすべて多層的に拡大する方向で深化するものと見られる。サイバー空間はもはや物理的衝突の補助的な戦場ではなく、独立した戦略兵器であり、国家間競争の核心領域であり、今後もその重要性は増し続けるだろう。このような環境では、組織は従来のセキュリティ体制では国家基盤のハッキンググループの脅威に対応するのが難しく、サプライチェーンセキュリティの強化・AI 基盤の検出体制の導入・産業インフラセキュリティの強化など、中長期的な戦略に基づく全社的な対応が必須である。

5. 新技術脆弱性及び暗号体系脅威の拡大

2026 年には、クラウドネイティブ環境、ブロックチェーン、IoT・OT インフラ、サーバーレスアーキテクチャ、人工知能モデルなど最新技術エコシステム全般でセキュリティ脆弱性が本格的に悪用され、サイバー脅威の地形が大きく変化すると予想される。これらの新技術はビジネスの拡張性と敏捷性を提供するが、同時に従来のセキュリティモデルが考慮できなかった新しい攻撃面を無限に拡張している。技術の進展速度がセキュリティ体制の整備速度を上回る状況で、攻撃者は構造的な弱点を迅速に検出し、悪用することで、過去にない方法で企業と社会基盤施設を脅かすことになる。

まず注目すべき点は、量子コンピューティングの実質的な登場により、既存の暗号体系が根本的な脅威に直面しているということである。2025 年までは量子技術は主に研究段階にとどまっていたが、2026 年には限定的ながら実用レベルに到達した量子システムが登場し、「量子脅威」はもはや遠い未来の話ではなくなった。RSA・ECC を含む従来の公開鍵暗号は、ショアのアルゴリズムに基づく量子計算に脆弱であることが既に繰り返し立証されており、攻撃者は既存の暗号化トラフィックを長期間保存しておき、後に量子技術を用いて解読する“Harvest Now, Decrypt Later（HNDL）”戦略を本格的に使用する可能性が高い。これは、現在安全だと信じられている通信やデータが将来の攻撃によっていつでも露出し得ることを意味し、長期的なセキュリティ要件が重視される政府・軍事・医療・金融分野が特に大きなリスクに直面することになる。

これと並行して、量子耐性暗号（PQC）への移行過程で発生し得る過渡的脆弱性も重要な脅威要因となる。PQC アルゴリズムそのものは量子攻撃に耐性を持つよう設計されているが、実際の運用環境

に適用する際には、実装エラー、鍵管理上の問題、性能ボトルネックなど、新たな脆弱性が生じる可能性が高い。特に既存システムとの互換性を維持する過程で「ハイブリッド暗号化構造」が広く導入されることになり、こうした混合環境は攻撃者に中間層を狙った迂回攻撃や認証偽造を可能にする新たな攻撃の入口を提供する恐れがある。

ブロックチェーンとスマートコントラクト生態系の拡張も脅威を増幅させる重要な要因である。2026 年には DeFi サービス・L2 拡張ソリューション・Cross-chain ブリッジなどが爆発的に拡散し、セキュリティ脆弱性の種類と規模も増加すると予想される。スマートコントラクトは自動化された金融ロジックを実行する特性上、単一の脆弱性が発見された場合、数億ドル規模の被害に直結する事例が繰り返し発生する可能性がある。また、攻撃者はブロックチェーンを Malware の C2 インフラとして活用し、検出をさらに困難にしており、ユーザーのウォレット拡張プログラムや開発者ツールに悪性パッケージを注入する方法でサプライチェーンベースの攻撃を行う可能性も高い。これは、ブロックチェーン生態系が単なる金融サービスではなく、攻撃者の隠匿・伝播インフラとして活用され得ることを意味する。

クラウドネイティブ技術も 2026 年の主要攻撃対象になると見られる。Kubernetes、Docker、Serverless 環境は利便性と拡張性を提供する一方で、構成エラー・過剰な権限設定・API 攻撃面の拡大など構造的脆弱性を内包している。Kubernetes API サーバーが外部に露出したり RBAC 設定が不適切な場合、攻撃者は全体のクラスター制御権を容易に獲得でき、Serverless 関数のイベントトリガーを操作して Malware を自動実行させる攻撃も登場する可能性がある。API Gateway とサービスメッシュ環境では、認証回避、内部トラフィックの傍受、メタデータ URL アクセスなど新しいタイプの攻撃が増加する見込みである。クラウド環境は速度と拡張性を前提としているため、小さな設定ミスが組織全体に影響を及ぼすシャドウリスクに拡大しやすく、攻撃者はこれらの隙を迅速に悪用する。

IoT と OT・ICS 環境の拡大もまた深刻な危険につながる可能性が高い。家庭用 IoT 機器だけでなく、産業用センサー・PLC・発電所制御システム・自動化設備などは、基本パスワードの使用、パッチ不可能な構造、認証のないプロトコルなど長期間にわたって蓄積された構造的脆弱性を持っている。2025 年にはすでに数十 Tbps 規模の IoT ベースの大規模 DDoS 攻撃が登場しており、2026 年にはその規模がさらに大きくなり、グローバルインターネットバックボーンにも影響を与えるレベルに拡大する可能性がある。特に OT・ICS システムがクラウド・IoT と徐々に統合されているため、攻撃者が IT ネットワークを侵害した後、OT に拡張して物理的事故—停電、生産停止、設備破壊—を引き起こすシナリオは現実的な脅威となっている。

最後に、AI 技術そのものを標的とする攻撃も、2026 年には重要な脅威として位置づけられるだろう。データポイズニング（Data Poisoning）、モデル窃取（Model Stealing）、プロンプトインジェクション、モデル完全性への攻撃など、AI モデルの信頼性を根本から揺るがす手法が拡散する可能性が高い。セキュリティソリューションが AI ベースの検出モデルに徐々に依存するようになるにつれ、攻撃者が AI モデルを直接攪乱したり誤認させたりする攻撃は、防御体系全体を迂回する効果をもたらす恐れがある。

総合的に見ると、2026 年の新技術に基づく脅威は、技術導入の速度に比べてセキュリティガバナンスが十分に追いついていない構造的な問題から生じており、単一の脆弱性が全体のエコシステムに拡散する連鎖的な脅威を引き起こす可能性が非常に高い。組織は新しい技術の導入と同時にそれに適したセキュリティ戦略を確立し、技術中心の拡張速度にセキュリティ体制が遅れを取らないように、持続的なリスク管理体制を構築する必要がある。

示唆点および対応戦略

2025 年のサイバー脅威の様相と 2026 年に予想される未来の脅威を総合してみると、組織が既存の防御体系をそのまま維持したまま未来の攻撃環境に耐えることは事実上不可能に近い。攻撃者たちはすでに AI を活用して精巧さと自動化を備えた攻撃体系を構築しており、サプライチェーン全体にわたる脆弱性を戦略的に活用して単一経路のみ確保しても数十から数百の組織に攻撃を拡散させる能力を持っている。ランサムウェアはすべてのプラットフォームとデバイスを対象に拡張され、情報スティーラーと結合して内部資格情報・セッション・クラウドトークンを自動で窃取した後、組織の核心資産に対する攻撃をさらに迅速に展開する。ここに国家基盤ハッキンググループは地政学的緊張と結合し、単純な情報収集を超えて、サイバー-物理融合攻撃を実行するレベルに高度化されている。このような環境では既存のネットワーク中心境界セキュリティ、ユーザー中心の断片的なセキュリティ教育、イベント発生後の対応に集中する SOC 運用方式だけでは攻撃の速度と規模に対処できない。

これらの変化は、セキュリティ戦略の根本的な転換を要求する。最も優先的に導入すべきアプローチは、Zero Trust セキュリティモデルである。Zero Trust は内部・外部ネットワークを区別せず、いかなるアクセス要求も信頼せずに継続的な検証を要求する方式である。過去には外部からの侵入を防ぐための境界セキュリティ中心の戦略が効果的であったかもしれないが、今では内部アカウントの乗っ取り・クラウドトークンの流出・開発者キーの露出などが攻撃の出発点となる場合がはるかに一般的になった。したがって、すべてのシステム・ユーザー・サービス間の通信に対して、細分化された権限管理、継続的な認証、行動基盤のアクセス制御が必要である。特に組織は MFA を超えて、セッション単位のリアルタイムポリシー適用、異常アクセス検知、ネットワークマイクロセグメンテーションなどを活用する必要がある。

2 番目に重要な対応戦略は、供給網セキュリティ体制の全面的な強化である。組織は使用するすべてのソフトウェア構成要素を明確に識別し、SBOM(Software Bill of Materials)を通じてライブラリ・パッケージ・外部モジュールの変更履歴を追跡可能な構造に転換する必要がある。開発者環境は供給網攻撃の最上段露出ポイントであるため、アカウント保護、MFA・FIDO2 基盤の強化認証、Git 署名検証、IDE プラグイン検証などが必須である。また、CI/CD パイプラインに対するセキュリティ検証手続きを強化し、ビルド成果物に対するコード署名・無欠性検証を自動化する必要が

ある。ソフトウェア更新過程に対する攻撃が徐々に拡大しているため、組織はサードパーティ供給者に対するセキュリティ評価体制を構築し、契約時にセキュリティ要件を明文化することが必須である。

第三に、AI ベースの攻撃の拡散に対処するため、組織は AI 統合型のセキュリティ運用体制（SOC）へと進化させる必要がある。攻撃者が自動化された攻撃エンジンを使用するのであれば、防御側も異常行動検知、イベント自動分類、対応自動化（SOAR）などを AI モデルに基づいて運用し、「機械速度（Machine Speed）」で対応できる体制を整備しなければならない。単純なログ分析型の検知モデルだけではもはや十分ではなく、ユーザー行動分析（UEBA）、ネットワーク異常検知（NDR）、エンドポイントの行動ベース検知（Behavioral EDR）などを組み合わせた XDR ベースの統合防御モデルの導入が求められる。また、AI ベースの防御モデルを運用する際には、データポイズニング（Data Poisoning）、モデル汚染（Model Corruption）、プロンプトインジェクションなどの新種攻撃にも備える必要があるため、AI セキュリティに関するガバナンスおよび検証体制の構築も不可欠となる。

4 番目に、クラウド・IoT・OT 基盤攻撃の拡大に備えて、プラットフォーム特化セキュリティ制御が必須である。クラウド環境では CSPM (Cloud Security Posture Management) を活用して設定エラーを継続的に検出し、CWPP (Cloud Workload Protection Platform) 基盤でクラウドワークロードの実行単位を保護する必要がある。IAM (Role & Identity 基盤権限管理) はクラウドセキュリティの核心であるため、最小権限原則・権限継承防止・未使用アカウント (Unused Credential) 廃棄ポリシーを必ず導入しなければならない。IoT・OT 環境ではネットワーク分離、プロトコル整合性検査、ICS 専用 IDS 導入、製造者デフォルト設定強制変更など、運用技術環境に特化したセキュリティ制御を適用する必要がある。ますます複雑化する IoT デバイスエコシステムでは、連動するエッジ・ルーター・ゲートウェイデバイスまでをも包括する詳細なセキュリティ構造が必要である。

最後に、組織は脅威インテリジェンスに基づく能動的防御(Proactive Defense)セキュリティ体制に移行する必要があります。攻撃者は既にインターネット上の露出資産を自動でスキャンし、攻撃可能性を探索するために AI を活用しており、脅威キャンペーンとスティーラー型 Malware の亜種生成速度は人的分析では追いつけないほど急速に増加しています。したがって、組織は最新の攻撃者 TTPs、Malware 亜種、グローバルサプライチェーン脅威、ゼロデイ情報などを継続的に収集し、それを防御戦略に即座に反映する体制を持つ必要があります。内部モニタリングだけでは不十分であるため、ISAC など産業別脅威情報共有体制に積極的に参加することが重要であり、国家・民間間の協調体制も必要です。

結論として、2026 年のセキュリティ環境は、断片的な防御ソリューションや伝統的な境界セキュリティでは対応できない複合的な脅威環境です。AI 基盤の攻撃自動化、供給網侵入、多重プラットフォーム Malware、サイバー-物理融合攻撃が現実化しており、これを防御するためには技術・

プロセス・人に基づく全社的なセキュリティガバナンスが必要です。組織は全体のセキュリティ体系を再設計し、これを通じて攻撃者の速度と知能に対抗できる持続可能なセキュリティ環境を構築しなければなりません。

結論

2025 年のサイバー脅威動向と 2026 年展望を総合的に見ると、グローバルサイバーセキュリティ環境が単に複雑になったレベルを超え、質的に完全に異なる段階に転換していることが明らかに示されている。過去のサイバー攻撃は特定技術脆弱性に対する単一 Exploit や社会工学に基づく個別的侵入に近い形が多かったが、今や攻撃者は AI・サプライチェーン・クラウド・暗号体系・地政学など多様な要素を同時に結合し、一つの攻撃キャンペーンで複数の目的と技術を統合的に実行する複合型攻撃モデルを標準のように使用している。このような攻撃は既存のセキュリティ体系を前提から崩し、組織がセキュリティ戦略全般を根本的に再設計しない限り、攻撃の拡散速度と破壊力を防御側が耐え難い状況に繋がっている。

2025 年の脅威の流れを振り返ると、供給網攻撃の大規模化、AI 基盤のフィッシングおよび社会工学攻撃の現実化、情報スティーラーとランサムウェアの結合、国家基盤 APT の攻撃的戦略変化、クラウド・IoT・モバイルインフラの攻撃拡大など、様々な領域で前例のないレベルの高度化が現れた。これは単に技術発展に伴う自然な結果ではなく、攻撃エコシステムが既に「完全な産業構造」を備えた形に変質したことを意味する。攻撃者たちは特定の攻撃ツールを開発した後、普及させるだけでなく、これを自動化されたサービス形態で提供し、収益を最大化している。攻撃のためのツール・知識・自動化システムが容易に確保可能な環境は、全体の攻撃者層を爆発的に拡大させ、結果として攻撃の頻度・精巧さ・波及力がすべて過去と比較できないほど強化された。

2026 年には、これらの動向がさらに加速すると予測される。特に AI ベースの攻撃自動化は、従来手作業に依存していた攻撃工程を排除し、自ら攻撃計画を立案し、環境に応じて最適化されたマルウェアを生成する段階へと進化する可能性が高い。サプライチェーン攻撃は、単一のオープンソースパッケージや SaaS の脆弱性を起点として数千以上の組織に同時侵入できる強力な戦術として定着し、ゼロデイ脆弱性の確保と活用は、特定国家やカルテル型犯罪組織間の競争要素となるだろう。また、国家ベースの APT は、地政学的危機の局面でサイバー・フィジカル融合型攻撃を積極的に活用し、IT システム侵害にとどまらず、発電所・通信網・航空・海運など実際の物理的環境にまで直接的影響を及ぼす段階へ進む可能性がある。

クラウド・仮想化・MSA 環境の拡散は便利さと拡張性を提供しますが、同時に既存には存在しなかった構造的脆弱性を大量に露出させています。IoT および OT/ICS 環境のリスクは、すでに新興脅威レベルを超えて国家的リスク要素として位置づけられており、大型 IoT ボットネットがグロー

バルネットワークを実際に中断させる可能性も排除できません。スマートコントラクト・ブロックチェーン・L2 エコシステムもまた、急速な拡張速度に比べてセキュリティ検証体制が十分でないため、大規模な事故が繰り返される可能性が高いです。ここに量子コンピューティング時代が本格的に到来すれば、既存の暗号体系が無力化されるリスクが高まり、その過程で発生する転換期のセキュリティ空白も新たな脆弱性として位置づけられる可能性があります。

攻撃環境がこのように複雑かつ急速に変化しているにもかかわらず、多くの組織は依然として既存の防御体制を維持したまま新たな脅威へ対処しようとする傾向を示している。しかし、2026 年以降のサイバー脅威環境においては、従来の境界型セキュリティ、イベントベースの検知、受動的な運用方式だけでは、攻撃者の速度に追いつくことはもはや不可能である。攻撃者は攻撃自動化、スティーラーを用いたアカウント窃取、マルチプラットフォーム型マルウェア、サプライチェーン侵入などを組み合わせ、加速された攻撃サイクルを構築しており、防御側が攻撃を認識する前に既に相当な被害が発生する状況が繰り返されるだろう。

したがって、今後組織が生き残るために取るべきセキュリティ戦略は、単なるセキュリティ製品の導入ではなく、全社的な観点からセキュリティの役割を再定義する構造的転換でなければならない。ゼロトラストを基盤とした継続的検証プロセス、サプライチェーン全体の透明性確保、AI 基盤の SOC 運用、クラウドネイティブセキュリティ統制の強化、人材セキュリティに対する体系的教育、脅威インテリジェンス中心の先制対応体制など、すべてが有機的に結び付けられる必要がある。これは技術的要素だけでなく、組織文化、経営戦略、人材運用など、組織全体の変革が求められることを意味している。

結論、2026 年以降のサイバー空間は、攻撃者と防御者の双方が AI・自動化・データ中心の戦略を積極的に活用する高度な知能型の戦場へと移行すると考えられる。攻撃者はこれまで以上に迅速かつ精巧な攻撃を展開し、防御者はより大量のデータとより強力な AI を基盤として対処する必要がある。このような変化の中で、組織が持続的な成長を続けるためには、セキュリティを単なる IT 管理領域ではなく、企業の生存戦略を支える核心的な要素として位置付ける認識が何より重要である。サイバー脅威は今後も進化し続けるが、適切なセキュリティ戦略と体系を備えた組織だけが、こうした急速な変化の中で対応力を維持し、安定的なビジネス運営を継続することができるだろう。この報告書が提示した動向と展望、対応戦略は、2026 年とその後の脅威環境に備えるための重要な参考資料となるでしょう。これを基に、各組織が自らのセキュリティレベルを点検し、未来の攻撃に先制的かつ戦略的に対応することを期待します。

LEGAL DISCLAIMER

NSHC (NSHC Pte. Ltd.) takes no responsibility for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuations. NSHC Research services are limited publications containing valuable market information provided to a selected group of customers. Our customers acknowledge, when ordering or downloading our publications

NSHC Research Services are for customers' internal use and not for general publication or disclosure to third parties. No part of this Research Service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

For information regarding permission, contact us. **service@nshc.net**

This document contains information that is the intellectual property of NSHC Inc. and Red Alert team only. This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of NSHC. Nothing in this document constitutes a guaranty, warranty, or license, expressed or implied.

NSHC.

NSHC disclaims all liability for all such guaranties, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non-infringement of intellectual property or other rights of any third party or of NSHC.