kyndryl

歴史的転換点を迎えた サイバーセキュリティ： デジタル時代の複合的脅威への対応

執筆：クリス・ラブジョイ（Kris Lovejoy）
キンドリル　グローバル・プラクティス・リーダー　セキュリティ & レジリエンシー

目次

はじめに：
複合的サイバーリスクの時代へ

サイバーセキュリティは今、歴史的な転換点を迎えています。 従来の「個別の脅威」、例えば、パスワードの盗難、マルウェア感染の封じ込めなどは、経済的および社会的影響を伴う複雑で構造的なリスクに収束しつつあります。 実際、サイバー犯罪による世界的な損失額は、2030 年までに数兆ドル規模に達すると予測されています。 この新しい時代に、現在の脅威を正確に把握し、対処するだけでは十分とは言えません。それらが今後どのように加速し、相互につながり合い、将来の課題を形成していくのかを予測する必要があります。

この次なるサイバーリスクの進化は、互いに密接に関連する 5 つの変革を通じて発生しています。その中で最も大きな変革を引き起こすものは、自律型 AI の台頭です。この自律型 AI の出現は、攻撃と防御の両面における戦術を根本から再構築しつつあります。 次に挙げられるのが、AI がもたらす人間の労働市場への大きな変化であり、それが経済にもたらす影響が新たなサイバー犯罪の動機を生み出しています。第 3 の変革は、地政学的な緊張の高まりです。この緊張はインターネットそのものを分断し、デジタルサプライチェーンを主戦場へと変えつつあります。 第 4 の変革は、量子コンピューティングの台頭によって引き起こされるものであり、量子時代に対応できる柔軟な暗号基盤の整備、暗号アジリティの確立が急務となっていることです。 そして最後に、私たちのデジタル基盤の新たな脆弱性が顕在化しており、その安定性を脅かす構造的なリスクが新たに発生しています。

ビジネスおよびテクノロジー分野のリーダーは、統合された実践可能な指針を理解することで、不確実な将来環境において真の企業レジリエンスの構築に必要な戦略的な計画と投資を行うことができるようになります。 この複雑な状況を乗り越えるには、これらの課題を 5 つの個別の問題として捉えるのではなく、単一かつ統合された現実の 5 つの側面として理解することが必要です。

自律的攻撃者：パラダイムシフトをけん引する自律型 AI

サイバーセキュリティにおける最も直接的かつ変革的な力は、AI が2つの用途で用いられていることです。AI は今、私たちにとって最強の防御手段であると同時に、最大の脅威ともなり得るものであり、次の10 年を規定する新たな軍拡競争を生み出しています。

AI 戦線：進化する脅威と防衛の最前線

現在、AI の影響には 2 つの側面があります。 この新たな戦場の一方で、攻撃者は生成 AI を活用して高度なソーシャルエンジニアリングを仕掛けたり、環境に適応するマルウェアを生成したりしています。香港のある事例では、攻撃者がディープフェイク技術を用いて企業のCFO になりすまし、ビデオカンファレンス上で従業員を騙すことにより、2,500 万ドルを詐取するという被害が発生しました。 これは、「ポストトゥルース」環境の到来を鋭く予告する象徴的な出来事であり、EUROPOL（欧州刑事警察機構）は、今後 AI によって合成されたオンラインコンテンツが急増すると予測しています。 同時に、AI を組み込んだマルウェアの実用化も進んでおり、これは自身の実行環境を解析し、セキュリティツールの存在を特定し、検出を回避するよう動的にコードを書き換える機能を持っています。

その一方で、防御側は AI を使って AI に対抗しています。防御アルゴリズムは、数兆件におよぶデータポイントをふるいにかけ、攻撃の兆候となる微細な異常を識別することで、セキュリティチームの姿勢を受動的から能動的へと転換させつつあります。 AI 駆動型の Security Orchestration, Automation, and Response（SOAR）プラットフォームは、一般的な脅威に対するトリアージと封じ込めのプロセスを自動化し、人間のアナリストが未知のインシデントへの対応に集中できるようにしています。

近い将来に起こること：自律型 AI サイバー戦

現在のバランスの取れた対立構造は、やがて自律型 AI 戦争という新たなパラダイムへと劇的に進化していくでしょう。 今日の AI 支援型攻撃は、やがて AI エージェントの協調的な群れへと成熟し、脆弱性を自律的に発見し、一連の攻撃全体を実行できるものになります。 同時に、敵対者は「敵対的 AI」、つまり、私たち防御側の防御 AI モデルを欺き、悪用することに特化して設計されたテクニックを巧みに操るようになるでしょう。 2026 年までに、リアルタイムでのディープフェイク技術が完全に商品化され、その結果として、「デジタルトラスト（デジタル上の信頼）」という概念自体が根本から脅かされるでしょう。

予測

2027 年までに、完全自律型 AI を活用したサイバー攻撃が、実際に企業に対して成功裏に実行され、人間による直接の指令なしに最初の侵入からデータ流出までの目標が達成されるでしょう。 この出来事は、従来型のヒューマン・イン・ループ（人間中心的な）インシデント対応タイムラインを時代遅れなものとし、マシン・スピード・ディフェンス（機械速度による防御）こそが、今後取り得る唯一の道であることを証明するでしょう。

推奨アクション

AI を使って AI に対抗

脅威ハンティング、異常検知、対応自動化のための、次世代 AI 駆動型防御プラットフォームへの投資を優先してください。

デジタルトラストの再定義と防衛

FIDO2 準拠のハードウェアキーなど、なりすまし耐性を備えた次世代の多要素認証（MFA）技術を導入および投資してください。

ネットワークだけでなく AI も保護

内部 AI の安全な開発と展開に向けたガバナンスプログラムを確立してください。これには、データソーシング、モデルトレーニング、継続的な監視のためのセキュリティー基準の策定が含まれます。

人間的要素：変容する労働市場と進化する脅威

AI がテクノロジーの世界を大きく変える一方で、その技術的変革が引き起こす経済的影響と同じぐらい深刻な人間ドラマが展開されています。 この混乱は、キャリアパスの変更だけでなく、高度な金融犯罪を生み出す新たな、そして強力な動機や土壌をも生み出しています。

テクノロジーキャリアの分岐

AI は、テクノロジー職の構造に明確な分断を生み出しつつあります。 たとえば、レベル 1 の IT サポートや定型コードの作成などの反復的業務は自動化される一方で、開発、設計、データサイエンスといった高度な職種は AI によって拡張され、これらの専門家たちは戦略やイノベーションといった高次の作業に集中できるようになっています。 その結果として、AI/ML エンジニア、プロンプトエンジニア、AI 倫理担当（AI エシシスト）といった全く新しい職種が登場し、クリティカルシンキング、戦略的思考、コミュニケーションといった人間固有のスキルの重要性がかつてないほど重視されています。

サイバーセキュリティの分野は、こうした変化の小宇宙（マイクロコスモス）であり、そのリスクはさらに重大です。 従来型のセキュリティ・オペレーション・センター（SOC）は変革の真っ只中にあり、脅威の検知は AI によって自動化され、人間アナリストは真の「調査官」へと進化しつつあります。 侵入テスターの役割は、AI モデルそのものの脆弱性を検証する敵対的 AI テスターの役割へと進化しています。 ガバナンス、リスク、コンプライアンス（GRC）は、チェックリスト中心の運用から脱却し、アルゴリズムに起因するリスクをビジネス用語に翻訳する AI リスクストラテジストを必要とする時代へと移行しています。

この流れの最終進化形では、ソフトウェアの主要な筆者は AI となるでしょう。 サイバーセキュリティ実務者は、もはや「人間が書いたコードの欠陥を見つけるデジタル整備士」ではなく、AI セキュリティアーキテクト、ガバナー（統制責任者）、オーケストレーター（統合実行者）として、開発者の意図の妥当性を検証すること、AI サプライチェーンのセキュリティを確保すること、AI によって生成されたコードに対して防御用 AI を展開し脆弱性を探知することといった責務を担うことになります。

サイバー犯罪を加速させる経済的プレッシャー

この技術的変革は、同時に、別の側面でさらに陰湿なリスクを生み出しています。 2023 年から 2024 年にかけて広範に発生したテクノロジー分野での人員削減により、米国だけでも、高度なスキルを持ちつつ、経済的に追い詰められた 50 万人を超える人々が新たに出現しています。 この状況は、旧ソビエト圏東欧におけるポスト冷戦期の経済的混乱と人材の過剰供給が、世界的なサイバー犯罪の急増を招いた構造と類似しています。

これは、以下の 3 要素が重なり合う「不正のトライアングル」で説明がつきます。

1. 動機：集中的な経済的プレッシャー
2. 機会：インターネットの匿名性とアクセス容易性
3. 正当性：自分を見捨てたと感じる社会制度に対する憤り

経済の低迷により、技術に熟練した人々にとってこれら 3 要素のすべてが増幅され、サイバー犯罪行為へのバリアが低くなります。

予測

2026 年末までに、少なくとも 1 つの主要な Ransomware-as-a-Service（RaaS）グループが、信頼され、広く認知された主流テクノロジー企業の元従業員によって設立されるか、もしくはその中心メンバーとして構成される可能性があります。 これにより、最上位層の犯罪シンジケートにおいて、オペレーションの高度化、コードの品質向上、およびビジネス的な巧妙さがさらに著しく高まることが予想されます。

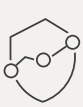
推奨アクション

「Cyber Workforce 2030」イニシアチブの立ち上げ

サイバーセキュリティ人材のスキル強化およびリスキリングを目的とした正式な育成プログラムを策定・予算化し、最も重要な防御資産である人材へ投資してください。

コーディング担当者だけでなく、AI ガバナンス人材も育成

セキュア・プロンプト・エンジニアリング、AI モデルの監査、AI レッドチーミング（対 AI 攻撃シミュレーション）といったスキルに重点を置いた育成を行ってください。



内部脅威対策プログラムの強化

経済的プレッシャーに直面する従業員からのリスクの増加に対処するために、技術的な対策や従業員向けの認識プログラムを見直し、強化してください。

地政学的リスク：分裂されゆくデジタル世界

世界経済をつなぐ同じデジタルプラットフォームが、いまや新たな地政学的対立の戦場にもなりつつあります。「単一でオープンなグローバルインターネット」という概念は崩れつつあり、データが戦略的資産であると同時に「武器」となる分断された現実へと変貌しつつあります。

「スプリンターネット（Splinternet）」の台頭とデジタル主権

テクノナショナリズムの高まりにより、インターネットはデータプライバシー、ローカライゼーション、アクセスに関する規則がそれぞれに異なる複数のブロックへと分断されつつあります。OECD の報告によれば、2023 年初頭の時点で、40 カ国において 100 件を超えるデータローカライゼーションに関する制限措置がすでに導入されています。 この分断により、世界規模で活動するあらゆる組織は直接影響を受けることになります。その一方で、国家主導の組織や過激派組織が、AI による偽情報を武器として用い、個人の過激化、制度への信頼の失墜、そして対立の扇動を引き起こしており、サイバー活動やテロリズムの温床を作り出しています。

サード・パーティー・リスクの連鎖：リスクが外部にある場合

この地政学的な分断により、すでに重大化した脆弱性であるサード・パーティー・エコシステムは悪化していくでしょう。組織のリスクサーフェスは、自社の境界内だけで定義されるものではなく、デジタル・サプライ・チェーン全体によって規定されるようになっています。 ベライゾン（Verizon）の 2025 Data Breach Investigations Report（2025 年度データ漏えい / 侵害調査報告書）によれば、すべてのデータ侵害のうち 30% がサード・パーティー・ベンダーに関連しており、この割合は前年の 2 倍に達しています。さらに、2021 年以降、サプライチェーン攻撃は 400% 以上の急増を見せています。 この外部リスクは現在、多面的な様相を呈しており、少数の主要なクラウドプロバイダーに依存することによる集中リスク、ベンダー製ソフトウェアに組み込まれた AI モデルに起因する不透明さによるリスク、さらにベンダーがデジタル国境の対立軸に巻き込まれることによる地政学的リスクが含まれます。

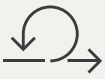
予測

2028 年までに、G20 諸国のいずれかが、データローカライゼーションおよびデータ主権に関する法制度を主要な貿易紛争における攻撃的な手段として正式に行使し、外国企業のデータの押収またはサービス停止を命じる事態が発生すると予測されます。 同時に、サプライチェーンの信頼性および安全の確保は、ネットワークへの直接的な侵入対策を上回り、C レベルの経営層にとって最優先のセキュリティ懸念事項となる見込みです。

推奨アクション

地政学に関するインテリジェンス情報を活用しスプリンターネットをナビゲート

IT アーキテクチャー、データ保存戦略、ベンダー選定における意思決定を支援するため、地政学的リスクに関するインテリジェンス提供サービスおよび専門知見への投資を強化してください。



継続的なアシュアランスでサプライチェーン全体を掌握する

サード・パーティー・リスク管理（TPRM）を、定型的なアンケートや契約上の義務に依存する従来型の手法から、ベンダーのセキュリティ態勢を継続的にスキャン可能なツールへの投資により、動的かつ実効性のある管理アプローチへと進化させる必要があります。

徹底的な透明性の確保を義務化

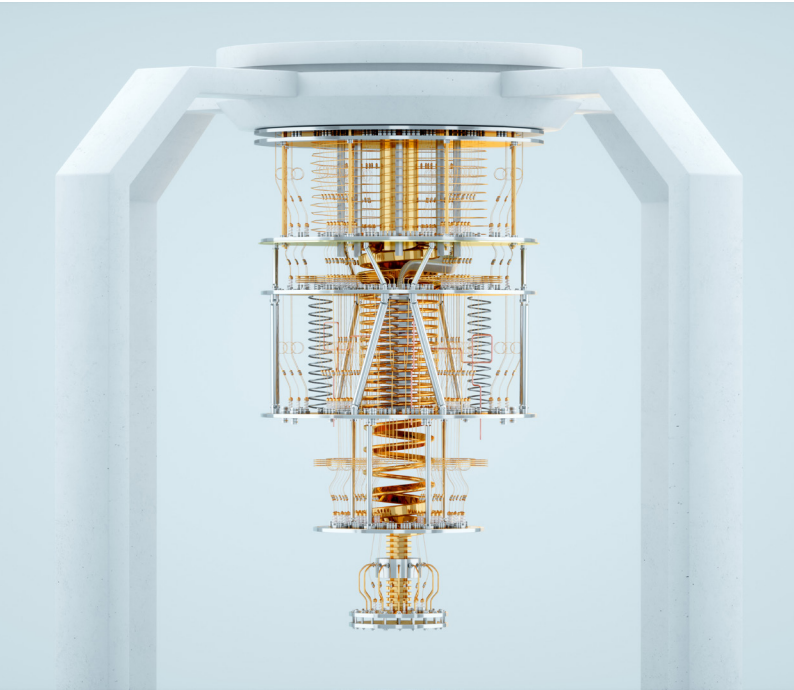
透明性の確保を義務化 し、すべての新規ソフトウェアベンダーに対して、ソフトウェア部品表の提出を契約要件として義務付けるとともに、AI 部品表（ABOM）の提出を求めるための標準策定を推進してください。

量子の脅威：暗号が破られるとき

世界で即時的な紛争が進行する一方で、より深く本質的なリスクが出現しつつあります。それは、デジタル世界の物理的前提そのものを脅かす「暗号危機」です。 量子コンピューティングの到来により生じるこのリスクは、特定の企業やネットワークを標的とするものではなく、すべてのデジタルコミュニケーションの根幹にある「信頼」を揺るがす存在です。 この脅威は進行の速度こそ緩やかですが、すでに始まっており、その対策に猶予はありません。

暗号解読に用いる量子コンピューターの開発競争は、新たな、水面下で進行する巧妙データ窃取を引き起こしています。 国家レベルの攻撃者が、将来の解読を見越してデータを収集する「Harvest Now, Decrypt Later：HNDL」という攻撃を積極的に実行していると考えられます。 彼らは現在、膨大な量の暗号化データ、つまり長期にわたり保護されるべき政府機密、機微な知的財産、財務記録、個人の医療情報などを吸い上げており、これらのデータが現時点では安全であっても、将来的に量子コンピューターによって解読可能になることを十分に理解しています。 事実上、ほぼすべてのデジタル取引および通信を保護している公開鍵暗号は、明確な時期は不明ですが、将来的に破られることが前提となっています。

この脅威も、もはや理論上の懸念ではなく、現実の問題となっています。 米国政府は、国家安全保障覚書第 10 号（NSM-10）により、この課題を研究段階から国家安全保障政策の領域へと引き上げ、連邦機関に対して 2035 年までに量子耐性暗号規格への移行を完了することを厳格に求めています。 これにより、「Y2Q Years to Quantum」と呼ばれるグローバルな取り組みが始動し、基幹的な暗号基盤の刷新が進められています。 米国国立標準技術研究所（NIST）などの機関の主導のもと、新たなアルゴリズムの標準化が進められています。しかし、その移行規模は極めて大きく、Y2K 対応をはるかに上回るものとなっています。なぜなら、この取り組みには、企業全体にわたって、レガシーなソフトウェア、ハードウェア、デジタル証明書の内部に深く埋め込まれた暗号プロトコルの特定と置き換えが求められるためです。



予測

2029 年までに、国家支援を受けた情報機関が、戦略的価値を有する直近の暗号化データセットを秘密裏に解読可能であることを実証する見通しです。 このブレークスルーの情報が漏えいすると、世界規模で市場が混乱し、ポスト量子暗号（Post-Quantum Cryptography：PQC）の導入に向けた、慌ただしく受動的な対応が引き起こされます。その結果、事前に備えていなかった組織が可視化され、データセキュリティの分野において「備えている組織」と「備えていない組織」という新たな格差が、瞬時に形成されることになります。

推奨アクション

暗号アルゴリズムの機動的な移行に対応できる体制を整備する

これは交渉の余地なき必須要件です。 直ちに実施すべきは、経営層のスポンサーシップのもと、ポスト量子対応タスクフォースを設置し、この数年規模の取り組みを主導することです。

今すぐ「暗号インベントリ」を実施

タスクフォースの最初の使命は、企業全体にわたる公開鍵暗号の全面的な棚卸しを行うことです。 このインベントリは、すべての移行計画の重要な基盤となるもので、優先的に予算措置を講じましょう。

移行の計画と予算

暗号インベントリに基づき、NIST 承認のポスト量子暗号（PQC）アルゴリズムへの移行に向けて、優先順位付けされたロードマップを策定してください。 この移行は、通常の IT アップグレードとは区別されるべきものであり、将来のテクノロジーおよびセキュリティ予算において、正式かつ予算化された独立項目として明確に位置付ける必要があります。

電力リスクが揺るがすデジタル社会の基盤

将来の脅威からデータを保護するための競争が進む一方で、そのデータを保存・処理するインフラを支える電力供給そのものが、深刻な脆弱性となりつつあります。 デジタル経済全体は、電力が常時かつ安定的に供給されるという前提の上に成り立っています。 かつては自明とされていたこの前提は、指数関数的に高まる需要と拡大する脅威環境の圧力により揺らぎ始めており、エネルギーは運用上の課題からサイバーセキュリティの中核的リスクへと変貌しつつあります。

デジタルパワーのトリレンマ

現在、私たちのエネルギーインフラは、危機的なトリレンマに捉えられています。

1. 需要の急増：前述のとおり、AI 革命が主要な原動力です。 国際エネルギー機関（International Energy Agency：IEA）は、データセンターの電力需要が2030 年までに 2 倍以上に増加し、現在の日本全体の消費量に匹敵すると予測しています。 この爆発的な需要は、地方および広域の電力グリッドにこれまでにない負荷をかることになります。

2. 老朽化したインフラ：世界中の電力網の多くは数十年前に構築されたものであり、現在の高度に集中したデジタル経済の需要に対応するよう設計されておらず、最新のセキュリティ対策も備えていないのが現状です。

3. 拡大する攻撃対象領域：電力網のモダナイゼーション（スマートグリッド）とエネルギー管理分野における IoT 機器の急増は、効率性を高める一方で、攻撃者にとって数百万単位の新たなデジタル侵入経路を生み出しています。 この脆弱性はすでに積極的に悪用されており、最近の Sophos 社のレポートによると、エネルギーおよび公益事業関連企業の 67% が、ランサムウェア攻撃を受けたと報告されています。

これらの要因が重なることは、エネルギー供給事業者における脆弱性が、その事業者に依存するすべてのデータセンター、企業、およびデジタルサービスにとって直接的な脆弱性となることを意味します。 サイバー攻撃は現在、遠隔地にある変電所への攻撃のようなインフラに対する物理的な攻撃と組み合わさることで、長期的かつ広範にわたる停電を引き起こす可能性があります。

予測

2030 年までに、サイバー攻撃によって電力網が標的とされ、それにより特定の特定の大手クラウドプロバイダー のデータセンターを意図的に機能停止させることを目的として行われる、初の「コンバージド・インフラストラクチャー・クライシス（converged infrastructure crisis）」が発生することになるでしょう。 このイベントは、デジタルサービスと物理的サービスの両方に同時に影響を及ぼす、多面的な地域一帯の大規模障害を引き起こす可能性があり、デジタルインフラおよび物理的インフラが過度に集中していることによるシステミックリスク（構造的なリスク）を浮き彫りにすることになります。

推奨アクション

物理的リスクとサイバーリスクの統合的なガバナンス体制を構築する

CISO とファシリティオペレーション（施設オペレーション）部門の責任者による、正式な連携体制を構築する必要があります。 具体的なアクションとしては、電力系統の安定性、燃料供給、および物理セキュリティをサイバーセキュリティの直接的な関心事として扱う、共同のリスクレジスターおよびガバナンスコミッティを設置することが含まれます。

サイト選定およびレジリエンスプランニングにエネルギー要因を組み込む

新たなデータセンターや重要な業務拠点への投資判断においては、地域の電力網の安定性、セキュリティ、およびレジリエンスを主要な選定基準として重視する必要があります。

停電対応計画の策定とテスト

広範囲かつ長期にわたる大規模な停電に備え、限られたバックアップ電源のもとで、セキュリティ監視、中核事業運営、インシデント対応をどのように継続するかを詳述した対応計画を策定し、定期的に検証するための措置を講じる必要があります。

まとめ

サイバーセキュリティをファイアウォールで解決すべき技術的問題として捉える時代は、もはや完全に終わりました。自律型AI、地政学的分断、そして基盤インフラのリスクの統合は、新たな運用の現実を明るみにしています。防御の多層化（defense-in-depth）から、戦略的に先を見通し、抜本的なレジリエンスを考えるよう思考転換が求められています。 従来のセキュリティプレイブックは、もはや通用しません。

リーダーシップに求められる新たなミッションは、この変革を推進することです。 これは、「システムは侵害される可能性がある」、「コアサービスは不安定になるかもしれない」という前提を受け入れ、対策の焦点を予防だけでなく迅速なリカバリーへとシフトすることを意味します。 それは、人手による対応だけでなく、AI に対して AI で立ち向かうことを意味します。 それは、量子コンピューティングによる脅威が本格化する前に、クリプトグラフィックアジリティー（cryptographic agility）を確立することも不可欠です。 また、サプライチェーンの深部までを可視化し、ベンダーに対して徹底した透明性を義務づけることで、デジタルエコシステム全体を的確に掌握する力が求められます。それは、物理的リスクとサイバーリスクを統合し、電力系統の安定性がネットワークの安全性と同様に重要であることを認識する必要があります。

本資料で示された戦略的優先課題は、単一かつ統合された戦略を構成する要素です。それは、防御されているだけでなく、本質的にレジリエントで、適応力がありかつインテリジェントな組織を構築することを目的としています。 リーダーシップに求められるタスクは、単発的な防御への投資から継続的な信頼性の確保へ、個別のテクニカルスキルから広範なストラテジックフォアサイトへ、そしてサイロ化されたリスクマネジメントから、複雑かつ変動の激しいデジタル世界を統合的に理解する姿勢へと、シフトさせることです。

kyndryl

キンドリルジャパン株式会社
〒106-6143　東京都港区六本木 6 丁目 10 – 1 六本木ヒルズ森タワー 43 階
kyndryl.com/jp/ja