cognizant

AI時代のテクノロジー モダナイゼーション：
AI時代におけるセキュリティ

はじめに

エンタープライズスケールの AI は、強力な「盾」であると同時に、新たな「矛」ともなり得るため、サイバーセキュリティにとって根源的な挑戦を突きつけています。多くのセキュリティリーダーが、この変化によって既存のサイバー戦略は時間と共に陳腐化すると確信しています。本稿では、AI のポテンシャルを解き放ち、新たなサイバーセキュリティ・パラダイムに備える旅路の中で、組織がいかにしてこの「二面性」という新たな現実と対峙すべきかを概説します。

企業は、AI がいかにして高度な脅威検知を自動化し、過負荷状態にあるチームを増強（Augment）するのかを学ばなくてはなりません。同時に、AI を悪用した新たな脅威のリスクを管理するため、新しい標準とプロセスを確立する必要もあります。正しいアプローチを取れば、セキュリティはもはやイノベーションの「ブロッカー」ではなく、組織全体の迅速かつ効果的なイノベーションを可能にする「イネーブラー」へと昇華するのです。

業界全体の最新動向については、こちらの完全ガイドもあわせてご覧ください。

AI の統合・運用モデルの進化に対応するセキュリティ

脅威が増大し続ける現代において、自社のリスク許容度（リスクアペタイト）に合致した適切なセキュリティレベルを確保することは、持続的なビジネスの成功を実現するための鍵です。

サイバーセキュリティは、活発化する脅威への防御はもちろん、コンプライアンスとイノベーションに不可欠な「信頼」を醸成する上でも極めて重要です。私たちがセキュリティ態勢の強化を絶え間なく続ける一方で、攻撃者（Adversary）もまた、人、プロセス、テクノロジーの脆弱な環（Weak Link）を突き、私たちの防御を突破しようと、急速なペースで進化を続けています。

AI は、サイバーセキュリティに「機会」と「リスク」という二つの側面をもたらします。AI は、膨大なデータ分析の自動化、パターン特定、そして潜在的脅威の予測を、より高い精度と速度で実現し、脅威検知・対応能力を強化します。しかしその一方で、攻撃者もまた AI を悪用し、AI 強化型フィッシングやディープフェイク詐欺といった、より洗練された攻撃手法を開発しているのです。

今後 6 ～ 12 か月で、貴社が優先的に取り組むべき懸念領域トップ 3 は何でしょうか。

日本企業の **40%** が、「サイバーセキュリティとデータ保護」を組織における最重要課題の一つとして挙げています。

Everest Group Enterprise Digital Transformation Trends Japan 2025

サイバーセキュリティとデータ保護を管理するためのアプローチ

AI がゲームのルールを変えつつある今、適切なリスクバランスの実現が不可欠です。過剰な制約はセキュリティを業務の「ブロッカー」とし、現場チームがその制約を迂回しようとすることで、かえって統制やプラクティスの質を低下させます。適切な「態勢（Posture）」を整えることで初めて、組織は AI のポテンシャルをセキュリティ強化に最大限活用し、同時にその悪用を防ぐことができるのです。

Only 24% of organisations feel fully or mostly prepared

Source: ADAPT Security Edge Survey in Apr 2025. Sample size: 111 Australian CISOs

AI という好機が事業計画に組み込まれ、それに伴う新たなリスクが出現したとしても、セキュリティ環境を管理するための最も重要なアプローチは、我々の「基礎（Fundamentals）」を正しく確立することにあります。この一点に、揺るぎはありません。

AI 時代におけるレジリエンスを構築するため、私たちは、新たに出現する脅威と企業の複雑性に応じて進化し続ける「多層防御戦略」を推奨します。

1. 人間中心のセキュリティ意識向上

基礎的な訓練から、脅威の進化に適応する「AI 強化型」の教育へと移行すべきです。ユーザー一人ひとりが、ディープフェイク、ソーシャルエンジニアリング、そして生成 AI による詐欺を自らの力で見抜けるよう、能力を付与（Empower）します。

2. AI 拡張による脅威監視と AI セキュリティ態勢管理（SPM）

行動ベースの分析と文脈的インテリジェンス（Contextual Intelligence）を活用し、誤検知（False Positive）を減らし、インシデント対応を加速させます。リアルタイムの可視性は、もはや選択肢ではなく「土台」です。業界をリードする適切な SPM を導入することで、組織は脅威を管理・軽減し、コンプライアンスを遵守し続けることが可能になります。

3. AI を念頭に置いた「セキュア・バイ・デザイン」

システムアーキテクチャの根底からセキュリティを組み込みます。特に、エージェント型 AI、コード自動生成、AI アプリのセキュリティ&ペネトレーションテスト、データ暗号化、セキュアアクセス、動的データフローといった、AI 特有の要素を考慮することが不可欠です。これからの設計フレームワークは、AI による自律的な意思決定や、進化し続けるアクセスパターンを予見しなくてはなりません。

セキュリティのための AI

AI は、セキュリティ支援システムとして、計り知れない機会を提供します。既存のセキュリティシステムを改善してリスクを低減し、あらゆる状況への対応能力を強化するのです。

ルールベースやシグネチャベースの監視から、「行動ベース」のセキュリティ管理へと移行する今日、AI は従来型ツールの有効性を劇的に向上させます。この「適応型アプローチ」は、組織全体のデータから悪意ある活動の最も微細な兆候をも検知し、攻撃を特定・緩和します。このプロアクティブな能力は、人手による介入と比較して、問題解決までの時間を大幅に短縮するのです。

私たちは現在、SOUL ツールを展開し、セキュリティのプレイブックを、エンドツーエンドの監査証跡を含む「AI オーケストレーションによる自動化」へと転換させています。この自動化を通じて、脅威の検知から実対応に至る典型的なサイクルが、従来の 8 〜 16 時間から、わずか 15 〜 30 分へと劇的に短縮される事例を、私たちは目の当たりにしてきました。

誤検知の管理

セキュリティダッシュボードに流入する数千ものアラート、その誤検知率が一般的に 60 〜 70% に達する状況では、「アラートはエラーである」という認識が常態化し、真のインシデントが人間のチームの目からすり抜けてしまうのは必然です。しかし、脅威インテリジェンスとネットワークのリアルタイム評価から得られる洞察によってアラートを「文脈化」することで、私たちは今、誤検知を 10% 未満にまで低減させ、真に対応を要する問題へと焦点を絞ることが可能になっています。

AI ダッシュボードとアナリティクス

一般的な企業環境には、多種多様なツールやサービスに、数十ものセキュリティ統制が散在しています。セキュリティ態勢の全体像を把握するには、無数のレポートとシステム連携が不可欠です。コグニザントの革新的な「Neuro ™ Cybersecurity」プラットフォームは、これらの多様なセキュリティツールを統合・連携（オーケストレーション）させ、CISO、CIO、リスク管理、脆弱性管理、そしてセキュリティアナリストといった、あらゆる関係者に統一されたユーザー体験を提供します。お客様が選択した AI モデルを活用し、リスク・コンプライアンス管理、脅威・脆弱性管理、インフラ・ネットワークポリシーの適用、そしてアプリやアカウントのオンボーディングにおける ID・アクセス管理（IAM）まで、極めて広範なユースケースを実現。これにより、組織はリスクを効果的に軽減し、全体的なセキュリティ態勢を抜本的に強化できるのです。

セキュリティスキルの不足

サイバーセキュリティ人材が慢性的に不足する中、専門的な知見へのアクセスは、多くの組織にとって依然として主要な懸案事項です。AI は、定型業務を自動化し、実用的な洞察（Actionable Insights）を提供することで、人間への作業負荷への依存を軽減する助けとなります。

ユーザー意識向上トレーニングの強化

今日、高度なスキルを持たない攻撃者でさえ、ディープフェイクをいとも簡単に作成し、ビジネスユーザーを極めて標的型の手法で攻撃するツールを手にしています。しかし、私たちもまた AI を活用し、ユーザー教育の方法を改善し、彼らのセキュリティリテラシーへの関与を深めることができます。よりスマートで、より魅力的な参加型トレーニングによって、全てのユーザーが、ビジネス環境に潜む最も一般的なリスクを回避するための、最善のマインドセットを維持するのです。

AI に求められるセキュリティ

AI がビジネス IT システム全体に「新たな常識」として組み込まれようとしている今、私たちは AI がもたらす新たなリスクを、既存のセキュリティフレームワークに統合しなくてはなりません。これは、AI システムにデータを流し込むのであれば、新たなプライバシーとコンプライアンスの規範に対応すべく、データガバナンスを更新することが必須である、ということを意味します。

AI に対応するためのセキュリティポリシーを更新する際、私たちは以下の主要な論点を検討することを推奨します。

- どの AI の利用を許可するのか？
- AI の所有権は誰にあるのか？
- データの所有権は誰にあるのか？
- どのデータタイプが許容されるのか？

前述の通り、より優れたデータガバナンスモデルとペルソナの必要性は論をまちません。そして今、堅牢なデータ分類と並行して、ペルソナ設計に「AI」の観点を取り入れることが、かつてなく重要になっています。これにより、ビジネス上の様々な用途や、異なる AI サービス・プラットフォームに応じて、データセキュリティ制御の階層を定義することが可能になります。例えば、個人識別情報（PII）は、ナレッジベースや一般文書とは全く異なる、格段に厳格な扱いが要求されなければなりません。

AI ガバナンスは、CIO、CISO、そしてデータプライバシー責任者による「共同意思決定」の領域となりつつあり、未来のセキュリティ、システム統合、そしてより広範なビジネスガバナンスそのものを基礎づけています。この「集合的リーダーシップ」は、AI による高速化の追求が、ビジネス要件のみならず、セキュリティ要件への配慮を常に維持することを保証しなければなりません。

自動生成されたコードが、マルウェア注入攻撃を受けて社内に展開される。あるいは、カスタム LLM がデータ攻撃によって「汚染」される。こうしたリスクは、もはや現実の脅威です。この脅威を軽減するため、自動スキャンと検証を継続的に維持することの重要性が、ますます高まっています。

サイバーセキュリティにおける AI 活用

コグニザントは、独自の「Neuro ™ Cybersecurity」プラットフォームにより、直感的なユーザーインターフェースを通じて、エンタープライズ規模でのリアルタイム・リスク軽減を実現します。複数のセキュリティプラットフォームを「統合」することで、サイロ化したオペレーションを克服し、リスクエクスポージャーを低減させ、脅威の検知・対応能力を強化します。さらに、本プラットフォームは機密データの分類と保護を支援して機密性とデータ完全性を向上させるだけでなく、ID・アクセス管理（IAM）を改善し、重要システムの統制に対する「確信」を高めるのです。

Cognizant Neuro® Cybersecurity Platform は、包括的で柔軟性と拡張性を備えたソリューションです。企業のサイバー耐性強化とリスク管理の高度化を支援します。

Cognizant Neuro® Cybersecurity Platform

AI 主導の自動化の強化

- AI への投資によりセキュリティ業務を効率化し、手作業の削減と対応スピードの向上を支援

高度な脅威検知と対応

- 脅威インテリジェンスとインシデント対応を高度化
- 効果的な脅威軽減を支援

OEM AI ソリューションとの統合

- 各種 OEM AI ソリューションとの連携を拡張
- インシデント対応の効率化と防御力の強化

統合セキュリティ管理

- 複数のセキュリティシステムの出力を一元化
- 脅威・脆弱性・リスクを包括的に可視化

スケーラビリティと柔軟性

- 組織の成長に応じてシームレスに拡張・適応
- 増加するデータ量や高度化するセキュリティ要件に対応

顧客要件に応じた導入とデータ管理

- 個別ニーズに対応した導入モデルとデータ管理

エージェント型 AI 時代におけるセキュア・バイ・デザイン

企業における「セキュア・バイ・デザイン」アプローチでは、責任はセキュリティチームだけに限定されるものではなく、組織全体で共有されます。この考え方は最新のエンジニアリングフレームワークやテンプレートにも反映されており、認証、認可、アクセス制御、データ制御を含め、システム設計の初期段階からセキュリティ要件を織り込んでいます。

とくに、AI によるコード生成が増え、エージェント型 AI が技術環境に導入される中では、必要最小限のアクセスをデフォルトにすることが極めて重要になります。エージェント型 AI は、アプリケーション、データ、意思決定システム間のシームレスな連携を前提とするため、アプリケーションやデータプラットフォームへの新たなアクセス形態が求められます。その結果、一見セキュリティリスクのように見えるエージェントの動きを許容できるセキュリティ制御も必要になります。

各レイヤーにおいては、エージェント型 AI が何を行い、その結果の責任を誰が持つのか、を明確にしておくことが重要です。エージェント型 AI が各システムとどのように連携するかを把握すること自体が、セキュア・バイ・デザインを支えるセキュリティ制御やフレームワークの一部となります。そして、シャドー IT がセキュリティリスクを生むのと同様に、シャドー AI もまた、人間のデジタルシステム利用を模倣するエージェント型 AI へと進化していく中で、新たなリスク要因となっていくでしょう。

AI によるセキュリティ強化を、現実のものに

AI 時代に備えるための、あらゆるセキュリティチームとテクノロジーに通用する万能薬は存在しません。AI の利点を享受するために既存システムをいかに進化させ、そしてその挑戦にいかに備えるか。この問いを見極めることこそ、個々の企業にとって正しいセキュリティアプローチを見出すための鍵となります。コグニザントは、企業のセキュリティの現状（Status Quo）をどこから調査し、眼前に広がる好機と課題に対する準備状況（Readiness）をいかにして特定すべきか、その知見を有しています。

私たちは、Cognizant Neuro ™ AI プラットフォームを通じ、CIO をはじめとするお客様のリーダーと、あるべき未来の姿（the art of the possible）をリアルタイムで探求し、その実現への道筋を具体化します。お客様のセキュリティ環境に AI をどう適用すれば、サイバーセキュリティ運用へのプレッシャーを和らげ、検知・分析能力を向上させられるのか。その姿を、私たちは実証（demonstrate）することができます。

私たちの戦略的支援は、第三者としての客観的な信頼性をご提供するだけではありません。お客様をいかなる継続的コミットメントにも縛ることなく、理想のセキュリティ態勢（Posture）の実現を可能にします。さらに、お客様のビジネス成果に連動する、リスクゼロの商用モデルをご提案することも可能です。

To learn more how Cognizant can help you strengthen security design in the era of AI:

Email: contact_au@cognizant.com

www.cognizant.com/au/en/cmp/technology-modernisation-security-in-the-era-of-ai

World Headquarters
300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters
280 Bishopsgate
London
EC2M 4RB
Phone: +44 207 297 7600

India Operations Headquarters
5/535, Okkiam Thoraipakkam,
Old Mahabalipuram Road,
Chennai 600 096
Tel: 1-800-208-6999
Fax: +91 (01) 44 4209 6060

APAC Headquarters
1 Fusionopolis Link, Level 5
NEXUS@One-North, North Tower
Singapore 138542
Phone: +65 6812 4000

WF 3696162