IDC Security and Trust Forum 2026, Japan

Post-AI時代のビジネスを衛るKeyDriver

2026/4/15

NEC　Corporate Executive CISO
NECセキュリティ株式会社　取締役
淵上　真一, CISSP

淵上 真一 （ふちがみ しんいち）

CISSP(Certified Information Systems Security Professional)

NEC Corporate Executive CISO
兼　NECセキュリティ株式会社 取締役

- ベンチャー系システムインテグレータでのネットワークエンジニアを経て、専門学校グループを運営する学校法人に転職
- 教員経験を経て、セキュリティ担当の役員として経営に参画
- 社外では司法、防衛関連のセキュリティトレーニングを手掛ける
- 2018年よりNEC、NECグループ全社のセキュリティ統括を担当

- **総務省・最高情報セキュリティアドバイザー**
- **情報セキュリティ大学院大学アドバイザリーボード**
- **Hardening Project実行委員**
- **一般社団法人ITセキュリティセンター理事**
- **一般社団法人サイバー安全保障人材基盤協会（CSTIA）理事**
- **一般財団法人日本情報経済社会推進協会（JIPDEC）評議員**
- **ISC2認定主任講師**
- **情報処理安全確保支援士集合講習講師**
- **Cisco Networking Academy Instructor Trainer**
- **警察大学校 嘱託講師**
- **北海道大学情報基盤センター客員研究員**
- **琉球大学情報基盤統括センターセキュリティアドバイザー**

Post-AI時代の到来：AIは社会インフラへ

AIは“特別な魔法の杖”から“当たり前のインフラ”へ

電気やインターネットと同様、AIはもはや特別な技術ではなく、
ビジネスの基盤となる「社会インフラ」として定着。

競争力は「安全かつ迅速なAI統合」に依存

一部の業務効率化にとどまらず、AIが自律的に意思決定を行うビジネス
モデルへの転換が加速。組織の勝敗はAI統合のスピードと安全性で決まる。

従来の境界型・後追い型では防御が困難に

AIが自律的に外部APIを操作し、データを処理する環境下では、
人間による監視や境界防御だけのアプローチは破綻する。

ビジネスの成長を維持しながら
未知の脅威に対抗するため、
セキュリティ概念の
根本的なアップデートが
不可欠である

攻撃側の進化：ランサムウェアの自動化

攻撃プロセスの全自動化と高速化

スクリプト生成、テンプレート化、ペイロード展開、横展開、セキュリティ制御の無効化までの一連の作業をAIが代替。手動オペレーションからの脱却が進んでいる。

“手法”ではなく“実行時間”の革命

ランサムウェア自体は既知の脅威だが、AIによって実行速度が「機械のスピード（Machine Speed）」へと加速。防御側が対応する猶予時間は極小化している。

国内被害は依然として高水準で推移

令和7年（2025年）の被害報告数は226件。AIによる亜種量産等の影響により、いたちごっこが続いている。

Threat Multiplier（脅威の増幅器）

AIは攻撃者のリソース制約を克服し、
高度な攻撃を「誰でも・安価に・大規模に」実行可能なものへと変質させている

守るべき資産の拡張：モデル／プロンプト／意思決定

Traditional Security
静的なインフラ資産

- 物理サーバー／仮想マシン
- ネットワーク機器／境界FW
- エンドポイント端末（PC／Mobile）
- 構造化データベース（SQL）

主な防御策

- 境界防御
- アクセス制御
- マルウェア検知

Post-AI Security
動的・認知的資産

New Attack Surface

- AIモデルの**学習データ**（コーパス）
- **プロンプト／システム指示**
- 推論メモリ（Context Window）
- AIエージェントの**意思決定プロセス**

必要な防御策

- 入力フィルタ
- 出力検証
- 思考プロセスの監査

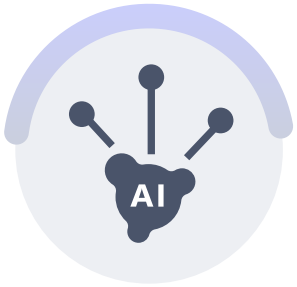
Impact Expansion（Blast Radius）

RAGや自律エージェントの導入により、AIが機密データへのアクセス権やシステム操作権限を持つため、**プロンプトひとつで「情報漏洩」や「不正操作」が完結してしまう**リスクが出現している。

ビジネスを守る 3つのKeyDriver

Post-AI時代のセキュリティアーキテクチャを再構築するための視点

1 Beyond-Zero Trust
ビヨンドゼロトラスト



AIを単なるツールではなく、意思決定を行う**「自律アクター」**として定義

人間と同様にアイデンティティを管理し、最小特権の原則と継続的な検証（Continuous Verification）を徹底

2 Autonomous SOC
自律型SOC

AIによる攻撃スピードに対抗するため、防御側もAIをフル活用

検知・分析・封じ込め・復旧のサイクルを**「機械のスピード（Machine Speed）」**で回し、人間の負荷を低減

3 Agile Governance
アジャイル・ガバナンス

技術の進化に追従できる柔軟なルール形成

セキュリティを経営課題（Agenda）として位置づけ、法務・技術・事業部門が連携する**「人間中心」**の統制モデルを構築

KeyDriver 1：AIを組み込んだビヨンドゼロトラスト

New Identity Paradigm

AIエージェントはもはや単なる「ツール」ではなく、環境内で意思決定を行う「アクター」として、人間の従業員と同等以上の厳格なアイデンティティ管理下に置く必要がある。

NIST SP 800-207/207A への準拠

「決して信頼せず、常に検証する（Never trust, always verify）」原則を徹底。
境界防御への依存を排除し、アイデンティティとコンテキストに基づく動的アクセス制御へ移行する。

AIにも「最小特権」と「継続的検証」を適用

AIエージェントを特権ユーザーとして放置せず、タスク実行に必要な権限のみを厳格に付与（Scope Attenuation）。
セッションごとにアイデンティティと振る舞いを継続的に検証する。

AIは24/7の自律アクター：静的信頼を排除

24時間超高速で稼働し、自律的に外部と通信するAIに対し、一度のログインで長期間のアクセスを許す静的な信頼モデルは破綻する。M2M通信の複雑性を前提とした制御が不可欠。

KeyDriver 1：AIエージェントのアイデンティティ管理

Architecture Shift: From "User Login" to "Agent Authorization"

AIエージェントをIAM（Identity and Access Management）の「ファーストクラス・シチズン」として扱い、OAuth 2.0/2.1のトークンエクスチェンジ標準などを活用して、エージェント間の権限委譲を検証可能にする必要がある。

Current Challenges

アイデンティティの断片化

- **追跡不能な「再帰的委譲」**
  AIが別のAIやAPIを呼び出す際、
  元の依頼者（人間）のIDコンテキストが失われる。
- **過剰な権限付与（Impersonation）**
  「なりすまし」として全権限をAIに渡してしまい、
  AIの暴走時に被害が拡大する。
- **監査ログの分断**
  「誰が」その指示を出したのか、システム間でログが紐づかない。

Recommended

Solutions & Standards

委譲された権限管理

- **委譲された権限 Delegated Authority**
  AIを「代理人」として定義し、
  本人とは区別可能な一時的権限を付与する。
- **スコープ減衰 Scope Attenuation**
  タスクに必要な最小限の範囲に、AIが持つトークンの権限を動的に縮小させる。
- **標準プロトコルの導入**
  OAuth Token ExchangeやMCP（Model Context Protocol）で安全に接続。

KeyDriver 2：AIにはAIを「自律型セキュリティOps」

Combat AI with AI

「AIによる攻撃」には「AIによる防御」で対抗する。人間の役割は、AIが提示した対応策の「承認」と、戦略的な「監督（Human in the loop）」へとシフトする。

人手のトリアージでは“機械スピード”に追いつかない

攻撃者がAIを用いて機械的な速度で攻撃を展開する中、手動でのログ分析やチケット起票といった
旧来のプロセスでは物理的に対応が間に合わない時代となっている。

予防・検知・対応・復旧にAIを深く統合

SOC（Security Operation Center）のあらゆるフェーズにAIを組み込み、
脅威の検知から封じ込めまでを自動化する「自律型SOC」へ移行する。

Dwell Time / Breakout Time の短縮をKPI化

脅威がシステム内に滞留する時間（Dwell Time）や、侵入から横展開完了までの時間（Breakout Time）を
極小化することを新たな重要指標として設定する。

KeyDriver 3：人間中心のアジャイル・ガバナンス

経営アジェンダとしての運用

「ルールを決めて終わり」ではなく、環境変化やインシデントに合わせてルール自体を継続的に見直し、更新し続けるプロセス（アジャイル）こそが最強の防御となる。

AIガバナンスの4つの指針

変化の速いAI技術に対応するため、固定的なルールではなく柔軟な運用を重視。

スモールスタート	リスクベース
マルチステークホルダー	アジャイル

NIST CSF 2.0の中核機能「GOVERN（統治）」

セキュリティ戦略を経営目標と整合させ、組織全体のリスク管理体制を確立する機能が新設。
技術偏重から経営主導への転換を促す。

組織横断的な役割分担と協奏

法務・コンプライアンス、セキュリティ、事業部門がサイロ化せず連携する体制へ。

経営層	法務
セキュリティ	事業

KeyDriver 3： GOVERN機能で整える“守りの地ならし”

CSF 2.0で新設された「GOVERN（統治）」は、他の5つの機能（特定、防御、検知、対応、復旧）を支える基盤。技術的な対策の前に、組織としての意思決定プロセスを確立する。

Step 1

コンテキスト理解

組織のミッション、ステークホルダー、法的要件を整理。**AI活用におけるリスク許容度**を経営層と合意形成する。

Step 2

戦略策定

ビジネス目標と整合したサイバーセキュリティ戦略を策定。 AIモデルの保護、プロンプトの安全性確保を戦略に組み込む。

Step 3

ポリシー & 役割

AI利用規定、データ取り扱いポリシーを整備。 CISO、法務、事業部門の**役割と責任**を明確化する。

Step 4

サプライチェーン管理

外部AIモデルプロバイダーやAPI提供者のリスク評価。 契約による保証と継続的なモニタリングプロセスを確立。

適用範囲の拡大

Identity	Data	App	Infrastructure	Supply Chain

AIシステムを含む全てのデジタル資産に対してガバナンスを効かせる

フレームワーク連携

ゼロトラスト（NIST SP 800-207）や
AI RMF（AIリスク管理フレームワーク）と相互に参照し、
実装の詳細を補完する。

セキュリティは“ブレーキ”ではなく“イネーブラー”

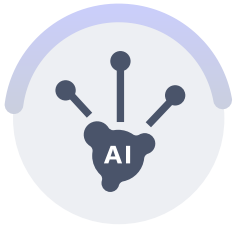
安全なAI統合が**ビジネスの成長を加速**させる

Post-AI時代において、セキュリティはリスクを止めるだけの存在ではない。
AIのポテンシャルを最大限に引き出し、競争優位性を確立するためのエンジン。

Integrated Strategy

KeyDriver 1

ビヨンド ゼロトラスト



KeyDriver 2

自律型SOC

KeyDriver 3

アジャイル・ガバナンス

Immediate Actions

社内合意と資産の棚卸し

経営層に対し「セキュリティ＝必要経費」のコンセンサスを形成。現状のAI利用状況（シャドーIT含む）とデータ資産を可視化する。

PoCの展開

特定の業務領域（例：カスタマーサポート、社内FAQ）で、RAGやAIエージェントの安全な導入実証を行う。MCP等の標準プロトコルを検証。

段階的スケールと自動化

PoCの成功モデルを全社展開。同時にSOCの自動化を進め、増大するログとアラートに対応できる体制を構築する。

継続的な監査と改善

レッドチーミングによる定期的な攻撃演習（プロンプトインジェクション等）を実施し、ガバナンスをアジャイルに更新し続ける。

参加者様限定

“次世代”サイバーセキュリティーサービスで、Post-AI時代のビジネスを衛る

1.「NEC展示卓」に、お立ち寄りください

インテリジェンス駆動型次世代サイバーセキュリティサービス「CyIOC」とAIセキュリティ

NEC独自のインテリジェンスとAI技術を融合した最新ソリューションをぜひご体感ください。

2. 簡単なアンケートに回答して、特典資料・情報をGet！

1	【限定公開】 本日の講演資料	Post-AI時代のビジネスを衛るKeyDriver NEC Corporate Executive CISO 淵上 真一, CISSP
2	【特典資料】 本日の展示に関する資料	本日の振り返りや、セキュリティ業務の生成AI活用のヒントに

NEC アンケートフォーム

※My NEC会員登録(無料)が必要

https://jpn.nec.com/cybersecurity/event/IDCSecurityForum2026/material.html

お問い合わせ：NEC サイバーセキュリティ戦略統括部 イベント事務局 cyber@mlsig.jp.nec.com

\Orchestrating a brighter world