NEC Cyber Day’26夏

ポストAI時代のサイバーセキュリティ
～「ビヨンドゼロトラスト」で切り拓く新戦略～

2026/7/14

NEC
NECセキュリティ株式会社

本日のプログラム

13:00～	はじめに（ご連絡など）
13:00-13:45 （45分）	【講演】 「ビヨンドゼロトラスト」という次の一手 いまの組織を衛るために採るべき経営戦略  淵上 真一
13:45-13:50	休憩
13:50-14:50 （60分）	【対談】 現場責任者が語る、 「ビヨンドゼロトラスト」の実践と、 ポストAI時代の組織の衛り方  青木 聡 ｜ 田上 岳夫 ｜ 奥 隆行
～14:55	おわりに（ISC2認定資格 CPEクレジット申請、視聴アンケートなど）

NEC Cyber Day’26夏
ポストAI時代のサイバーセキュリティ ～「ビヨンドゼロトラスト」で切り拓く新戦略～

「ビヨンドゼロトラスト」という次の一手――
いまの組織を衛るために採るべき経営戦略

2026/7/14

NEC　Corporate Executive CISO
　兼 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

フロンティアAI時代のサイバー脅威動向

AIは支援ツールからサイバー攻撃・防御の実行主体へと進化
攻撃側・防御側の双方でAI活用を前提とする環境変化を踏まえた備えが必須

Claude Mythosなどの登場
Anthropic Claude MythosやOpenAI GPT-5.5-Cyberなどの登場により、生成AIはコードレビューなどにとどまらず未知の脆弱性を発見できるレベルに

攻撃の自動化
ターゲットの探索、脆弱性の発見、悪用、攻撃経路へ組み込みなどの攻撃サイクルがAIエージェント化

ゼロデイ、Nデイ攻撃のリスク増加
AIによるゼロデイ脆弱性の発見、攻撃高速化によるNデイ攻撃のリスクが増加

防御側でのAI活用の必要性
高速化・スケール化する攻撃に対して、監視、資産管理、パッチ管理、インシデント対応など防御側もAIを活用した対応が必要になる

AIを用いた攻撃ライフサイクル

攻撃側AI
- 自律的な探索
- 脆弱性の検証
- 高速・大量の実行

防御側AI
- 継続的な監視・検知
- リスクの優先順位付け
- 修正・緩和の支援

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

AIによる攻撃と防御の構造変化

AI高度化により、攻撃は高速化し大量実行が可能になる
そのため防御側にもAIを用いた高速化、広範囲化が求められる

項目		Before	After
攻撃	標的偵察	人手によるスキャンやOSINT	AIによる自動大規模スキャン
	侵入手法	詐取された認証情報、設定ミス、放置された既知脆弱性の悪用	既存の侵入手法がAIにより自動化・高速化される フロンティアAIによる未知脆弱性の悪用
	脆弱性発見	高度人材、診断企業、バグバウンティ	AIが探索 発見量が大きく増える
	悪用可能性検証	熟練者が検証	AIがPoC化、攻撃経路化へ組み込み
防御	経営判断	IT、セキュリティ部門の課題	事業継続に関わる課題として考える サプライチェーンまで含めた責任が生じる
	システムの確認	人手による確認・診断	フロンティアAIによるチェック AI利用による情報コントロールが課題
	SOC運用	人手検知、チケットによる管理	AI検知、分析、自動封じ込めなどの継続的な適用が必要
	パッチ猶予	数week~数month	数hour~数day リスクの大きな資産に対して素早く適用する必要がある

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。

顕在化するサイバーセキュリティの課題

大量に発見される脆弱性と高速化/スケール化するサイバー攻撃に対する処理能力が不足
技術対策だけでなく、資産管理、意思決定、運用体制を含めた見直しが必要

資産の把握・管理不足

外部公開資産、クラウド、SaaS、API、OSSなど、攻撃の起点となりうる資産を把握し、サプライチェーンまで含めて管理する必要がある。

そのうえで、重要資産や影響の大きい資産を明確にし、攻撃時の影響やリスクの大きさを判断できる状態を整える必要がある。

脆弱性修正のリソース不足

大量かつ継続的に発見される脆弱性に対し、すべてを迅速に修正することは難しくなる。

そのため、リスクに応じて優先順位を付け、継続的に是正を進められる対応力が必要になる。

従来型防御の有効性低下

攻撃の自動化・高速試行が進み、攻撃を難しくするだけの防御は効果が下がりつつある。

そのため、侵入を防ぐ防御に加えて、侵入後も素早く検知・対応できる体制が必要になる。

意思決定の遅延

高速化する攻撃に対して迅速に対応するには、リスク抽出、影響分析、事業判断、責任の所在を事前に定義した意思決定フローの整備が不可欠になる。

Project YATA-Shield ～日本政府のフロンティアAI対策パッケージ～

2026/5/29時点

AI性能の高度化に伴うサイバー脅威の増大に備え、日本のサイバーセキュリティを確保するために策定された政府全体としての対策パッケージ

目的

攻撃の高度化への対応

- AIにより脆弱性発見や攻撃コード生成が加速し、サイバーリスクが増大
- リスクベースで優先順位を付けた迅速なパッチ適用を推進

攻撃時間の短縮への対応

- 脆弱性発見から攻撃までの期間短縮に対応
- 経営主導で資産管理・脆弱性対策を機動化

重要インフラの保護

- 重要インフラのサイバーレジリエンスを強化
- システム停止などの事態に備える

実施内容

重要インフラ事業者等・政府機関等への対応

- 注意喚起の実施
- 金融分野での先行的な取組と他分野への展開
- 人材育成支援
- 政府システムの対応強化

脆弱性の発見・修正等への対応

- 外国政府機関やビッグテック（AnthropicのProject GlasswingやOpenAIのGPT-5.5-Cyber等）との連携
- ソフトウェア・ベンダへの注意喚起
- AISI（AI安全性評価機関）による技術支援

技術・能力の強化

- 技術開発の推進
- 防御側における高性能AIを活用したサイバー対処能力の強化

国家サイバー統括室(NCO)「AI性能の高度化を踏まえたサイバーセキュリティ対策の強化について ～Project YATA-Shield～ 」(2026/5/18) https://www.cyber.go.jp/pdf/press/20260518_AI_CS_kankeishouchoukaigi.pdf

攻撃の高速化・スケール化に備える対策の基本方針

対策をいかに “速く・継続的に・経営主導で” 実施できるかが重要

❶ 経営層のリーダーシップのもと推進されること

投資判断　リスクの許容　クラウドリフト・シフト

❷ 攻撃者より先にリスクを把握しておくこと

資産管理　ASM　脅威インテリジェンス　サプライチェーン

❸ 侵入後に素早く止められること

ゼロトラスト　AIを活用した検知　バックアップ

❹ リソースを重大リスクに集中させること

優先順位付け　ネットワーク設計　パッチ　CI/CD

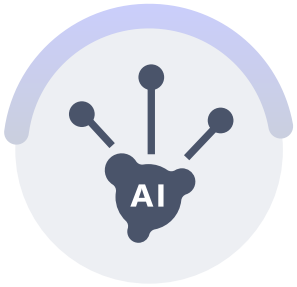
重要な考え方

- 基本の対策は今後も有効
- これまでとの大きな違いは “速度”と“規模”
- 自動化され継続的に実施される必要がある
- 素早い経営判断ができる体制
- AIによる実行と人間の承認と統制

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”

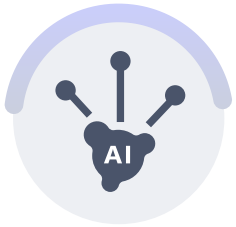
安全なAI統合が**ビジネスの成長を加速**させる

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。

\Orchestrating a brighter world

NEC Cyber Day’26夏
ポストAI時代のサイバーセキュリティ ～「ビヨンドゼロトラスト」で切り拓く新戦略～

現場責任者が語る、「ビヨンドゼロトラスト」の実践と、ポストAI時代の組織の衛り方

NEC　Corporate Executive CISO
　兼 NECセキュリティ株式会社　取締役　淵上 真一, CISSP ＜モデレータ＞
NEC　サイバーセキュリティ技術統括部長　青木 聡,CISSP
NEC　サイバーセキュリティ戦略統括部長　兼 CISOオフィス長　田上 岳夫,CISSP
NECセキュリティ株式会社　取締役執行役員副社長
　兼 NEC　サイバーディフェンス事業開発統括部　上席プロフェショナル　奥 隆行,CISSP

青木 聡（あおき さとし）

CISSP(Certified Information Systems Security Professional)

NEC サイバーセキュリティ技術統括部長

これまでにセキュリティ研究開発、脆弱性診断サービスや上流コンサル、NECグループ内のセキュリティ人材育成を担当

NECグループの製品・システム・サービスに対してセキュリティを確保するためのセキュア開発・運用を推進

推進リーダーとして、セキュア開発・運用ルール策定や展開、脆弱性マネジメント、セキュリティインシデント発生時のハンドリングに従事

- CISSP(Certified Information Systems Security Professional)
- CISA（Certified Information Systems Auditor）
- 経産省 産業サイバーセキュリティ研究会WG1「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース」委員
- IPA 情報処理安全確保支援士
- IPA ネットワークスペシャリスト

田上 岳夫（たがみ たけお）

CISSP(Certified Information Systems Security Professional)

NEC サイバーセキュリティ戦略統括部長 兼 CISOオフィス長

NEC入社後、ネットワークセキュリティ技術に関する研究開発、技術支援、コンサルティング等を経て、現在、サイバーセキュリティ部門にて、NECグループのサイバーセキュリティ戦略、国内外の社内セキュリティ対策を統括

- ガートナー　セキュリティ＆リスク・マネジメント サミット 講演
- 大阪大学　社会人教育講座セキュア・ネットワークセミナー　講演
- マイクロソフト　Microsoft Digital Trust Summit　講演
- 情報セキュリティ大学院大学　ISSスクエア水平ワークショップ 講演
- PwC Digital Trust Forum 講演
- ITmedia Security Week 講演
- Splunk .conf Go Tokyo 講演
- ビジネス＋IT 製造DX時代のOTセキュリティセミナー 講演
- Tanium Converge US　講演 等

社外活動
保有資格

- JQA(日本品質保証機構)技術専門委員
- CISSP
- ISMS主任審査員
- 情報処理技術者
  システムアナリスト、システム監査技術者
  テクニカルエンジニア(ネットワーク、システム管理)等
- G検定

奥 隆行（おく たかゆき）

CISSP(Certified Information Systems Security Professional)

NECセキュリティ株式会社　取締役執行役員副社長
兼 NEC サイバーディフェンス事業開発統括部
上席プロフェッショナル

警察においてサイバー犯罪捜査やデジタルフォレンジック業務を20年以上経験。その間、インターポールをはじめとする海外法執行機関や国際機関との共同オペレーション等に多数参画

2024年5月よりNECのサイバーセキュリティ事業の企画立案、Cyber Intelligence & Operation Centerプロジェクトの責任者
2026年4月より、NECセキュリティの取締役執行役員副社長に着任

- CISSP(Certified Information Systems Security Professional)
- ISC2/アジア太平洋情報セキュリティリーダーシッププログラム(ISLA)獲得

NEC Cyber Day’26夏
ポストAI時代のサイバーセキュリティ ～「ビヨンドゼロトラスト」で切り拓く新戦略～

現場責任者が語る、「ビヨンドゼロトラスト」の実践と、ポストAI時代の組織の衛り方

NEC　Corporate Executive CISO
　兼 NECセキュリティ株式会社　取締役　淵上 真一, CISSP ＜モデレータ＞
NEC　サイバーセキュリティ技術統括部長　青木 聡,CISSP
NEC　サイバーセキュリティ戦略統括部長　兼 CISOオフィス長　田上 岳夫,CISSP
NECセキュリティ株式会社　取締役執行役員副社長
　兼 NEC　サイバーディフェンス事業開発統括部　上席プロフェショナル　奥 隆行,CISSP

セキュア開発・運用のルール体系

サイバーセキュリティ管理規程、実施基準、サイバーセキュリティチェックリスト、
マニュアル／ガイドは国際的な規格類とNECグループでの独自の知見から作成

① 各種情報の集約と体系化

各種外部規格やガイドから必要な要素を
取り込み集約、統一的な枠組みとして体系化

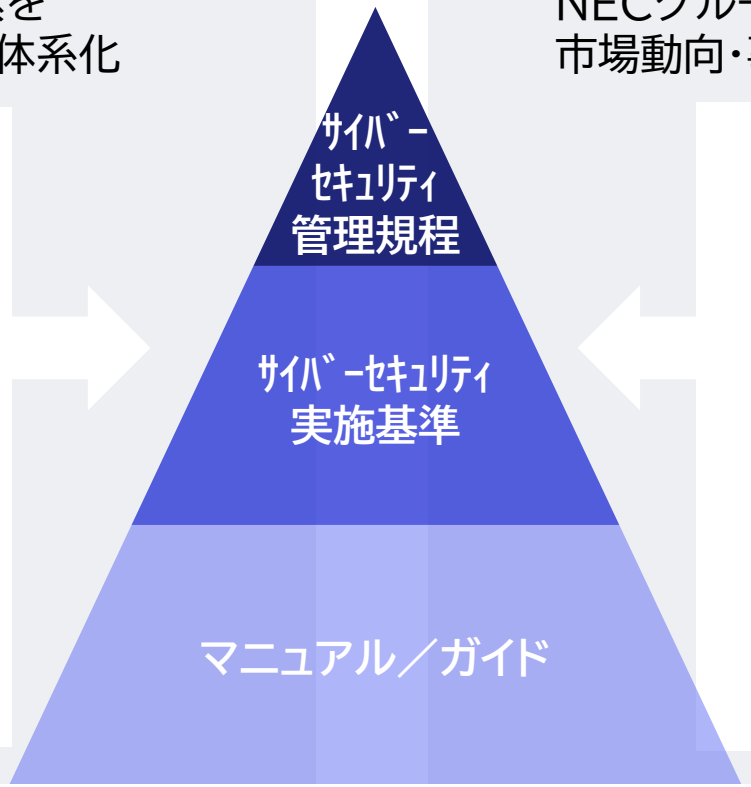
外部規格・ガイド

国際標準規格

ISO/IEC 15408, Common Criteria	PCI DSS
	IEC62443

国内の基準・ガイド	業界団体のガイド
内閣 サイバーセキュリティセンター	IPA
総務省	JPCERT/CC
経済産業省	業界/分野別

海外のガイド：NIST SP800-53



② NECグループでの実践と積み重ね

NECグループ内での長年にわたる活用の中で、
市場動向・事故事例の取り込み等により強化

市場の動向

- 新たな脆弱性、サイバー攻撃の対策
- セキュリティ事故の再発防止策

NECにおけるセキュア開発・運用プロセス

NECでは、20年以上にわたりSecurity By Designの取り組みを実施
システム開発・運用の全工程にて、その経験と実績を活かしたセキュア開発プロセスを実践

事業部門でセキュリティ実装を徹底する仕組みづくり

体制

事業部門にセキュリティ責任者を配置

プロセス

サイバーセキュリティ管理規程
全社員対象に全社規程として厳格化

約400項目のチェックリスト
ISO／IEC15408、NIST SP800-171など
国際標準や業界ガイドライン、最新技術動向を参照

システム化

脆弱性管理システム
システム構成製品の脆弱性情報をタイムリーに配信

セキュア開発点検システム
セキュリティ実装状況の定期点検、是正指示

サイバーセキュリティ実施基準によるセキュア開発実践

開発に必要なセキュリティ対策を定義し、フェーズごとに確認すべきタスクをチェックリストとして用意

セキュリティ対策分類

リスクアセスメント	ネットワーク保護	可用性対策
脆弱性診断	データ保護	運用管理
脆弱性情報の収集・対処	認証	保守管理
ネットワーク監視・検知	アクセス制御	開発環境セキュリティ確保
ログ管理	マルウェア対策	委託先管理

マニュアル／ガイド

セキュリティ対策提案・見積マニュアル	セキュリティ機能設計ガイド	スマートデバイスセキュリティ対策ガイド
脆弱性対策マニュアル	セキュリティログ技術ガイド	データベースセキュリティ対策ガイド
暗号化マニュアル	ファイル暗号化技術ガイド	セキュリティテストガイド
可用性対策マニュアル	Webアプリケーションセキュリティ対策ガイド	セキュア運用・保守ガイド
脅威分析ガイド	クラウドセキュリティ対策ガイド	開発環境セキュリティ対策ガイド

実施すべきタスクをチェックリスト化

サイバーセキュリティチェックリスト フェーズごとにチェック項目を用意（約400項目）

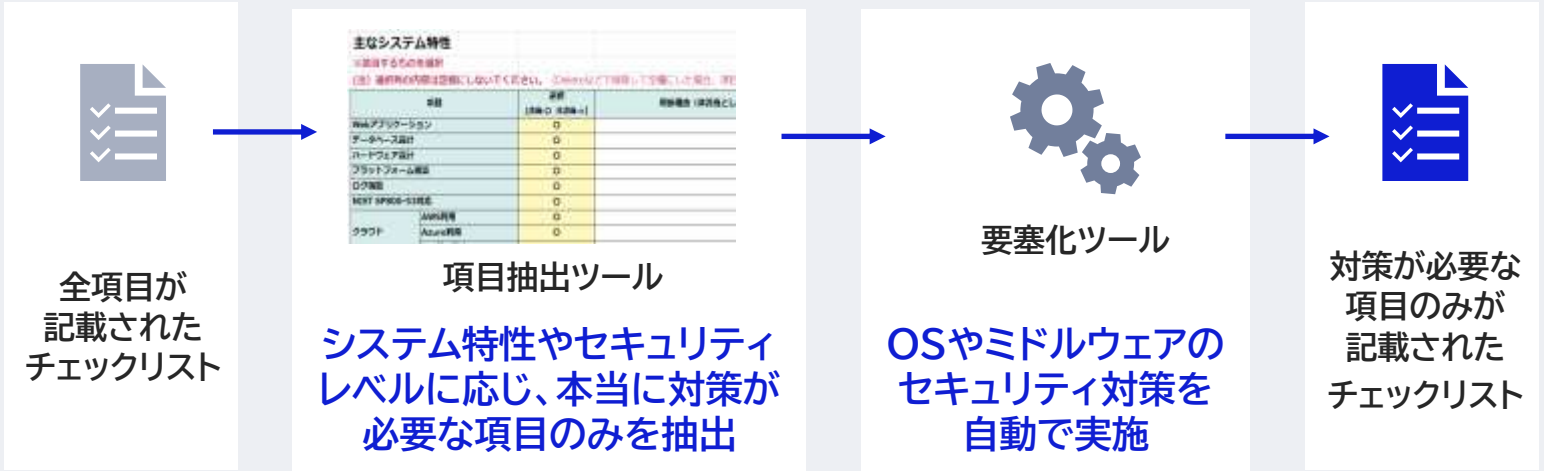
企画 提案 → 要件定義 → 設計 → 実装 → テスト → 出荷 → 運用 / 保守

チェックリストの省力化・可視化による開発の効率化

省力化

チェックリスト実施項目削減

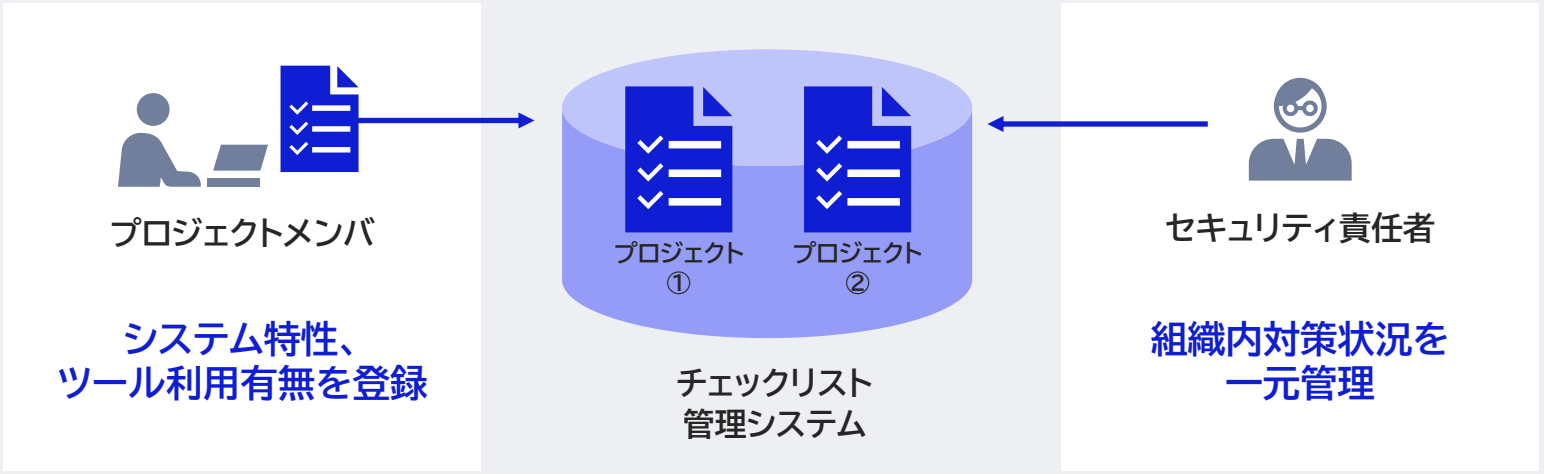
「項目抽出ツール」と「要塞化ツール」を
活用することで、チェックリストの
実施項目数を約30%～45%削減



省力化 **可視化**

チェックリストのWebシステム化

- システム上でシステム特性や
  ツール利用有無を登録可能
- セキュリティ責任者が組織内の
  対策状況を横断で確認可能



セキュリティ対策の危殆化への対応

過去構築したシステムやサービスに実装されていたセキュリティ対策が時間の経過とともに、その有効性が弱体化

セキュリティの危殆化
- 脆弱になった暗号アルゴリズム(3DES, MD5, ・・・)
- 認証に関わる情報(パスワード長,署名鍵長, ・・・)
- **セキュリティアーキテクチャ**

10年以上前に開発・構築された外部公開システムにおいて、
単一認証(ID/PWのみ)はよく使われていた
現在、外部公開システムでは、多要素認証(MFA)が主流化

長期間利用されたことで、セキュリティ対策が危殆化した
サービス、システムが動き続かないように、定期的な点検の
実施のルール化

\Orchestrating a brighter world

NEC Cyber Day’26夏
ポストAI時代のサイバーセキュリティ ～「ビヨンドゼロトラスト」で切り拓く新戦略～

現場責任者が語る、「ビヨンドゼロトラスト」の実践と、ポストAI時代の組織の衛り方

NEC　Corporate Executive CISO
　兼 NECセキュリティ株式会社　取締役　淵上 真一, CISSP ＜モデレータ＞
NEC　サイバーセキュリティ技術統括部長　青木 聡,CISSP
NEC　サイバーセキュリティ戦略統括部長　兼 CISOオフィス長　田上 岳夫,CISSP
NECセキュリティ株式会社　取締役執行役員副社長
　兼 NEC　サイバーディフェンス事業開発統括部　上席プロフェショナル　奥 隆行,CISSP

\Orchestrating a brighter world NEC

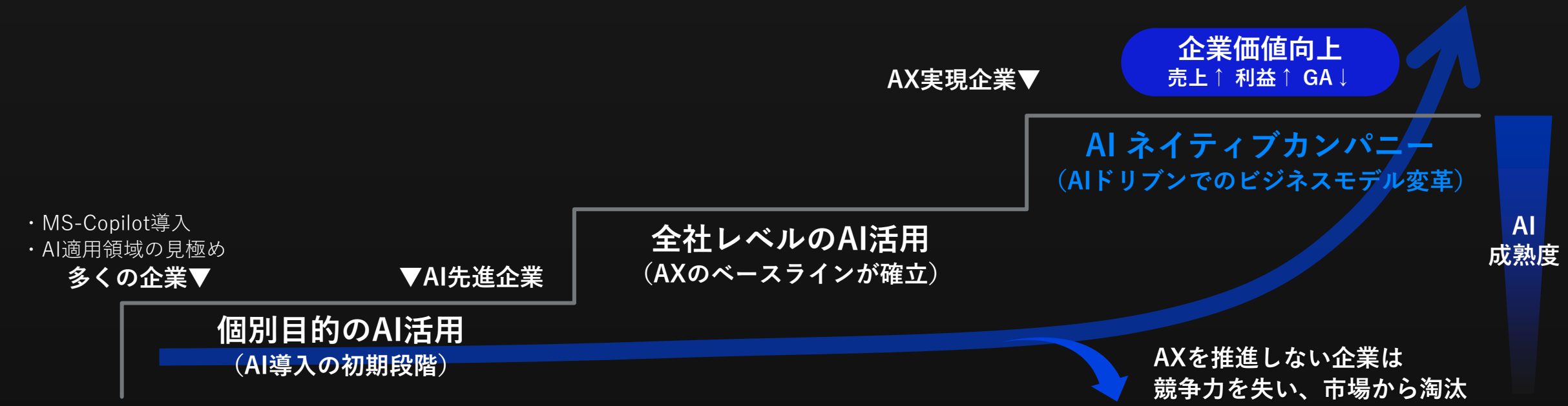
Security for AI の取り組み

2026年7月14日

日本電気株式会社

AXがもたらす経営インパクト

AIは新たな産業革命。AIを駆使して人・組織の生産性を上げ、時間の使い方を変え、新たな企業価値を創造することが競争力の源泉。AXを推進しない企業は企業存続にかかわるリスクに直面



考え方	実務で“使える” ユースケースの創出	AIと人の価値の組込み	AIファーストでの Enterprise Re-design
企業	デジタル化を超える インパクトの予兆	包括的自動化とWork Re-design 劇的な効率化･高度化	ビジネスモデル変革を高速化し 圧倒的競争力を獲得
人	AIエクスペリエンスの実感	人だから価値の出せる業務へシフト スピード、RoTを追求	AIによる能力拡張 本質を捉えた問い立てと価値に集中

AI ガバナンス

NECでは、AIの利活用によって生じうるリスクを予防・解決するためのポリシーを制定し、基本規定、ガイドライン、マニュアルを整備

AIと人権ポリシー

「NECグループAIと人権に関するポリシー」の基本規定・ガイドライン・マニュアル

項目	分類	内容	参照ガイドライン
基本規定	-	AIリスクマネジメントシステムの策定・実施・運用についての体制や社員が遵守すべき基本的事項を定めたもの	「人間中心のAI社会原則」（内閣府） 「ビジネスと人権に関する指導原則」（国連人権理事会） 「AI原則実践のためのガバナンス・ガイドライン」（経済産業省） 等
ガイドライン	-	AIのガバナンス体制を確立・実施・維持・改善するための基本的事項を定めるもの	
マニュアル	運用	AIガバナンス体制の構築・運用・改善に係る詳細を定めたもの	
	リスク管理	AIガバナンスの運用の詳細を定めたもの	
	事象発生・予兆検知時	AI事業における危機への対応を定めたもの	

参照すべきAI 外部ガイドライン

海外でのビジネスも視野に置きつつ、日本国内でのAIビジネス・利用には、複数のガイドラインを併用

AI事業者ガイドライン（総務省／経産省）

AI開発・提供する事業者やサービス運営者を対象とし、利用者や社会全体の安全・信頼性を守るため、AIの安全・信頼性を確保しつつ、リスクに応じた適切に管理し、健全な利活用を促進することを目的とする

キーワード
#人間中心の原則 #リスクベース #プライバシー保護
#安全性確保（生命・身体・財産） #公平性・バイアス対策
#透明性 #セキュリティ確保 #マルチステークホルダー
#トレーサビリティ #アカウンタビリティ
#継続的モニタリング

日本国内で事実上のデファクトスタンダードとなるガイドラインであり、最重要

NIST AI RMF（AI 100-1）

AIのリスクを体系的に管理し、信頼できるAIの設計・運用を促進するための枠組みとして、AIを開発・提供・利用するすべての組織や関係者を対象とし、AIの安全性・公平性・透明性を確保することを目的とする

キーワード
#GOVERN #MAP（リスクの把握・文脈化） #MEASURE
#MANAGE #リスク許容度
#信頼できるAIの特性 #透明性・説明責任
#継続的モニタリング #インベントリ管理

リスクZマネジメントの体制やプロセスを確立するフレームワークとして事実上のグローバル標準

EU AI Act（EU AI規制法）

EU域内でAIシステムやAIモデルを提供・導入・輸入・流通する事業者（EU外企業も含む）を対象とし、EU域内で安全かつ信頼できるAIの普及を促進し、健康・安全・基本的権利を保護しながら、イノベーションを支援することを目的とする

キーワード
#リスクベース分類 #高リスクAIの要件 #適合宣言
#適合評価 #提供者・導入者の義務
#一般目的AI／基盤モデル要求事項
#不履行の制裁・罰則 #コンプライアンスチェックリスト

EU域内でビジネスをする際に要求される法律であり、罰則もある

NIST AI RMFをフレームワークとし、遵守項目をAI事業者ガイドラインを取り込みつつ、EU AI Actとも対応付ける

AIアセットに対する脅威とセキュリティアプローチ

AIアセットの拡大に伴い顕在化・高度化するリスクに対し、ガバナンス・マネジメント・基盤の観点から体系的な対策を講じる必要あり

AIアセット（管理対象）

デジタル空間

- AIシステム/サービス
- モデル
- LLM
- 学習データ、RAG
- AIエージェント
- A2A
- MCP
- 既存システム

現実空間

- センサー
- 機械・装置

×

脅威（リスク）

現時点のリスク

- プロンプトインジェクション（直接/間接）
- 不適切な出力処理
- 機密情報漏えい
- システムプロンプト漏えい
- サプライチェーン汚染
- RAGに起因する情報漏えいや出力操作
- リソース無制限消費
- データ/モデルポイズニング
- ユーザリテラシー

今後のリスク

- 過剰な自律性
- AIモデル侵害
- AIエージェント暴走
- マルチAIエージェント競合
- AIサプライチェーン攻撃の高度化
- AIの透明性喪失
- リソース無制限消費
- データ/モデルポイズニング
- AIバイアス・スパイラル
- シャドウAI

×

対策（アプローチ）

ガバナンス

- 方針・ルール
- ガイドライン
- リテラシー向上

マネジメント

- 遵守状況把握（点検）
- 遵守状況可視化
- 体制

基盤（技術）

- AIアセット検出
- シャドウAI
- AI脆弱性診断
- AIガードレール

AI Native時代における経営リスク

ルール＋ITの仕組みの組み合わせでAIに関するリスクを低減

AIに関する経営リスク

透明性（ブラックボックス）	• 複数の関係者やサービスが関わるため責任の所在や説明責任が明確にできない • 透明性確保が難しく、結果を分析できない
安全性（性能）	• 誤認識を引き起こす「AIが騙される」リスク • ディープフェイクなどAIの性能の高さゆえに「人間が騙される」リスク
プライバシー	• 推察不正確、不適切なデータや偏りが誤った判断や予測、時に差別的・個人特定に至る判断を引き起こす
公正性（法令・コンプラ違反）	• 法規制や基準の変更も多く、追随できないと不正利用による情報漏洩や法令違反、信用失墜につながる

NECの考え

基本方針

「AI と人権に関するポリシー」
「企業秘密管理規程」
「情報セキュリティ基本規程」
を遵守し、入力する情報に応じて生成 AI を適切に利用する

＋

ITの仕組み

- 法・制度準拠
- クローズド環境
- ガードレール
- 不正検知
- 安全性チェック　・・・

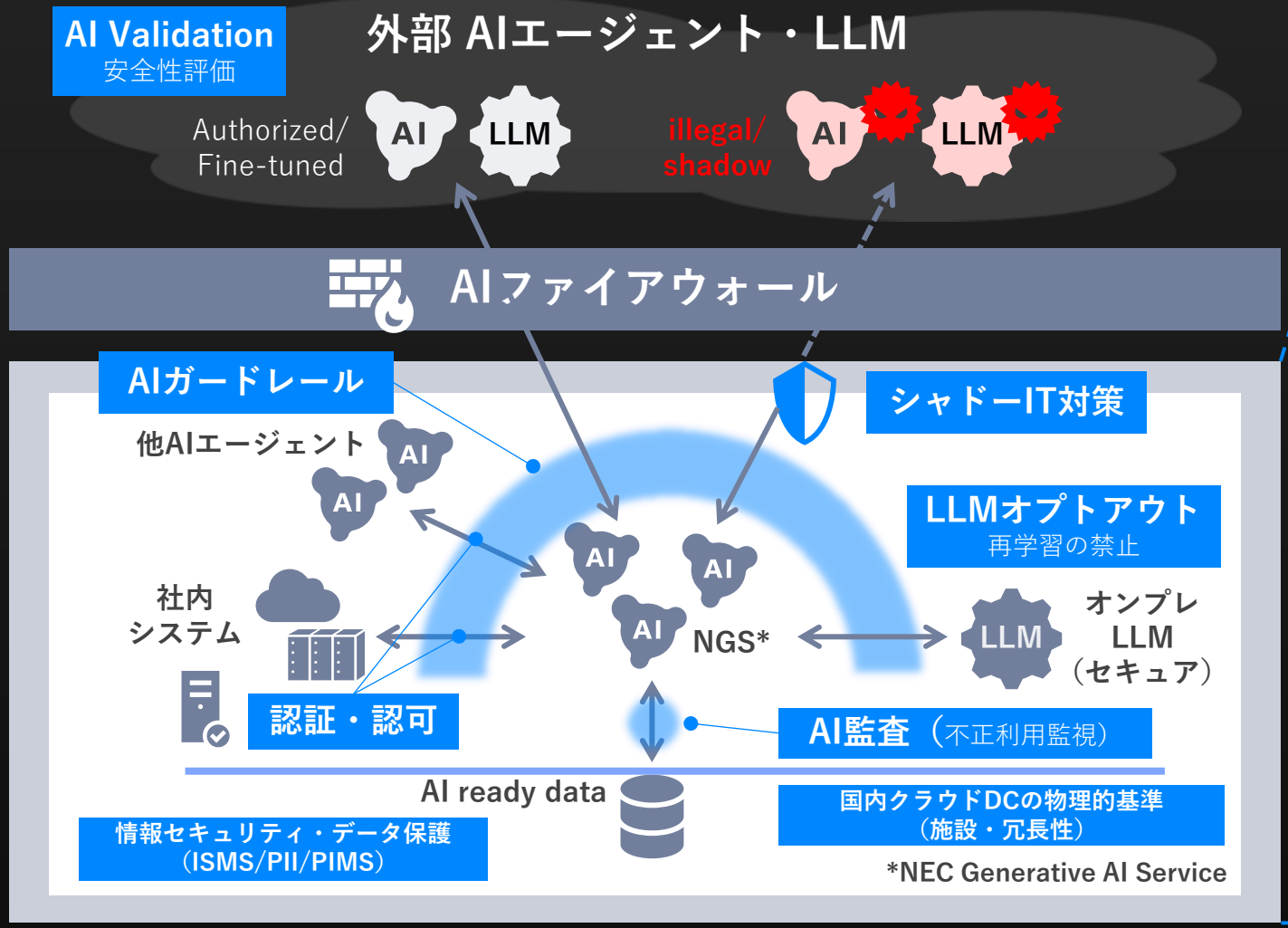
AI-Readyなデータの拡張要件

- 従来のデータの要件に加え、AI-Readyならではの要件への対応が必要
- AI-Readyなデータの整備が、今後のAI活用の成否に関わる重要な取り組みとなり試行錯誤で進めている

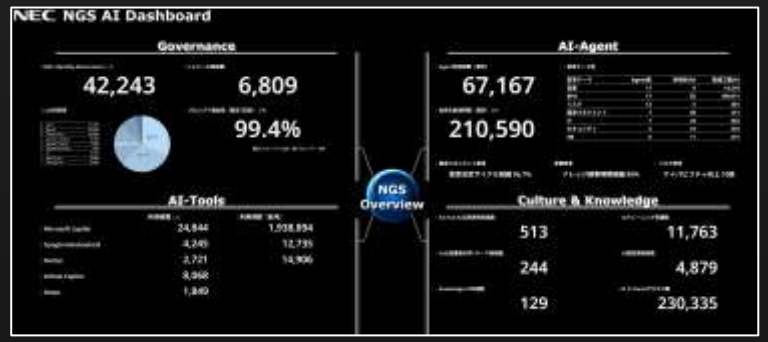
分類	これからの要件	
	従来の要件	＋ AI-Readyデータ実現に向けた拡張要件
データの整合性	データソースの特定と連携	＋ ① 非構造化データへのアクセス 学習や推論に必要な情報は、構造化だけでなく、非構造化データにも存在
	データの前処理（標準化）	＋ ② 特徴量エンジニアリング 機械学習モデルの予測精度を上げるためには入力データの加工が必要
	メタデータ管理	＋ ③ アノテーション（ラベリング） データに意味や属性を付与し、AIが理解できるように整備
データガバナンス	プライバシー	＋ ④ 倫理的、法的、社会的な対応 AIによる差別や偏見、社会的信頼を下げるようなデータを排除するルール策定
	データセキュリティ	＋ ⑤ 公平性、透明性、説明責任の担保 AIがどのデータを入力し、何の業務に使っているか担保
	データ品質管理	＋ ⑥ 信頼性の高いデータ AIの安定運用の為には、データ品質基準を策定し、データ品質を可視化・改善
継続的な適格性	一貫性	＋ ⑦ 可観測性 AIで使用されるデータを観測し、データ品質やパフォーマンスを最適化

AIガバナンス 全体図

AIエージェント・社内IT・LLM間を中心にガードレールを設定し、外部利用のエージェント、
LLM自体の安全性も評価。また不正利用防止でログ管理機能を設け、利用状況を可視化

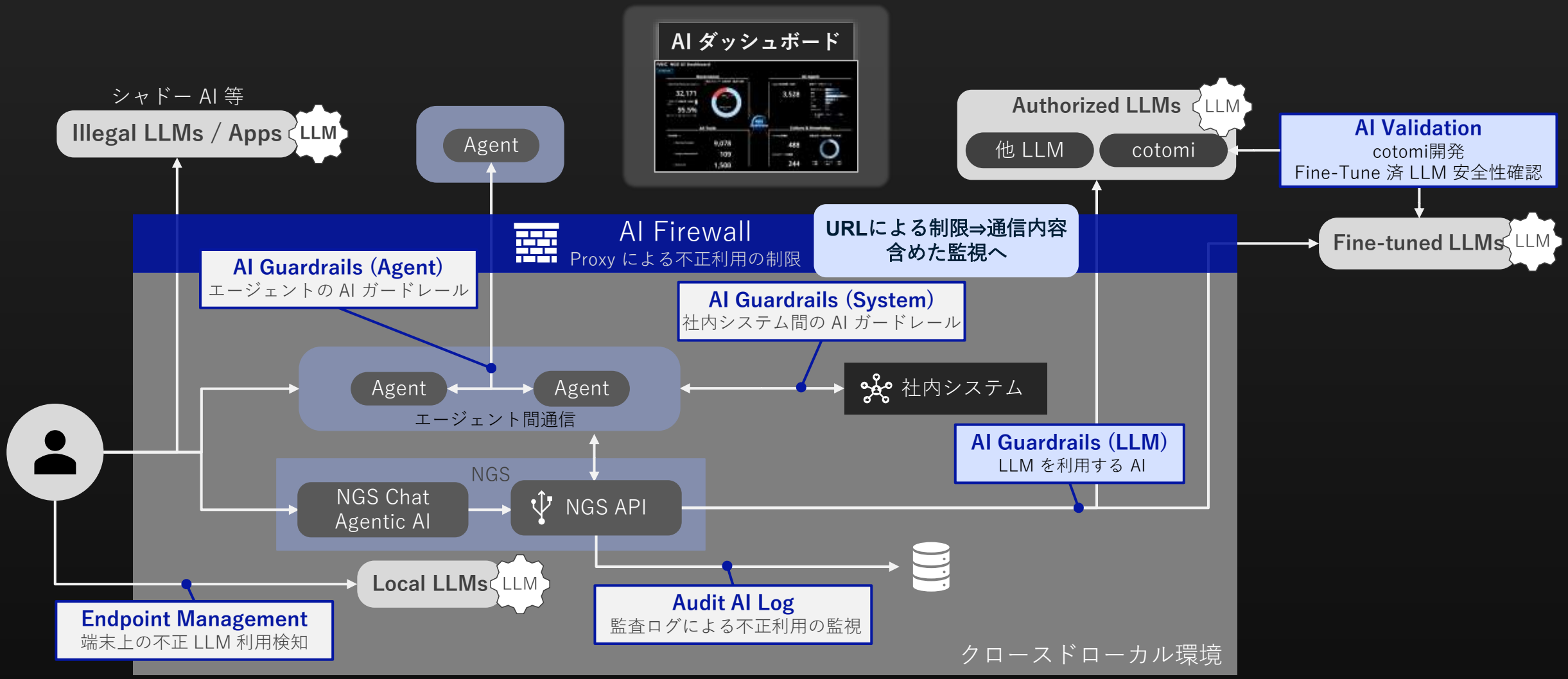


AIコックピット（可視化）



価値が出ているか？　　**セーフティか？**

NEC における AI ガバナンス機能全体図



AIエージェント サイバーセキュリティ対策 全体像

AIエージェントに対するゼロトラスト、アイデンティティ管理、脆弱性管理、監視、可視化を実施

NIST CSFにおける分類	事前対策		運用		
	特定	防御	検知	対応	復旧
	資産・リスク・脆弱性を特定	対策を講じて、脅威から資産を防御	攻撃の可能性を検知・分析	インシデントに対する対応	影響を受けた資産・業務を復旧

❶ 悪意ある/脆弱な外部コンポーネントの混在

❷ インターフェースの脆弱性を突いた攻撃

❸ エージェントの乗っ取り

アセット管理・リスクアセスメント

インベントリ自動化
(AI-BOM*1作成)
サプライチェーン管理

*1 Bill Of Materials

Agent ID 管理・認証

エージェント管理
ポリシーに基づく
動的アクセス制御

Agent 通信制御

入出力制御
(ガードレール)
ネットワーク分離

Agentic AIに対応したセキュリティオペレーション

脆弱性・リスク管理

脆弱性・攻撃手法のデータベース化
シャドーAI *2対策

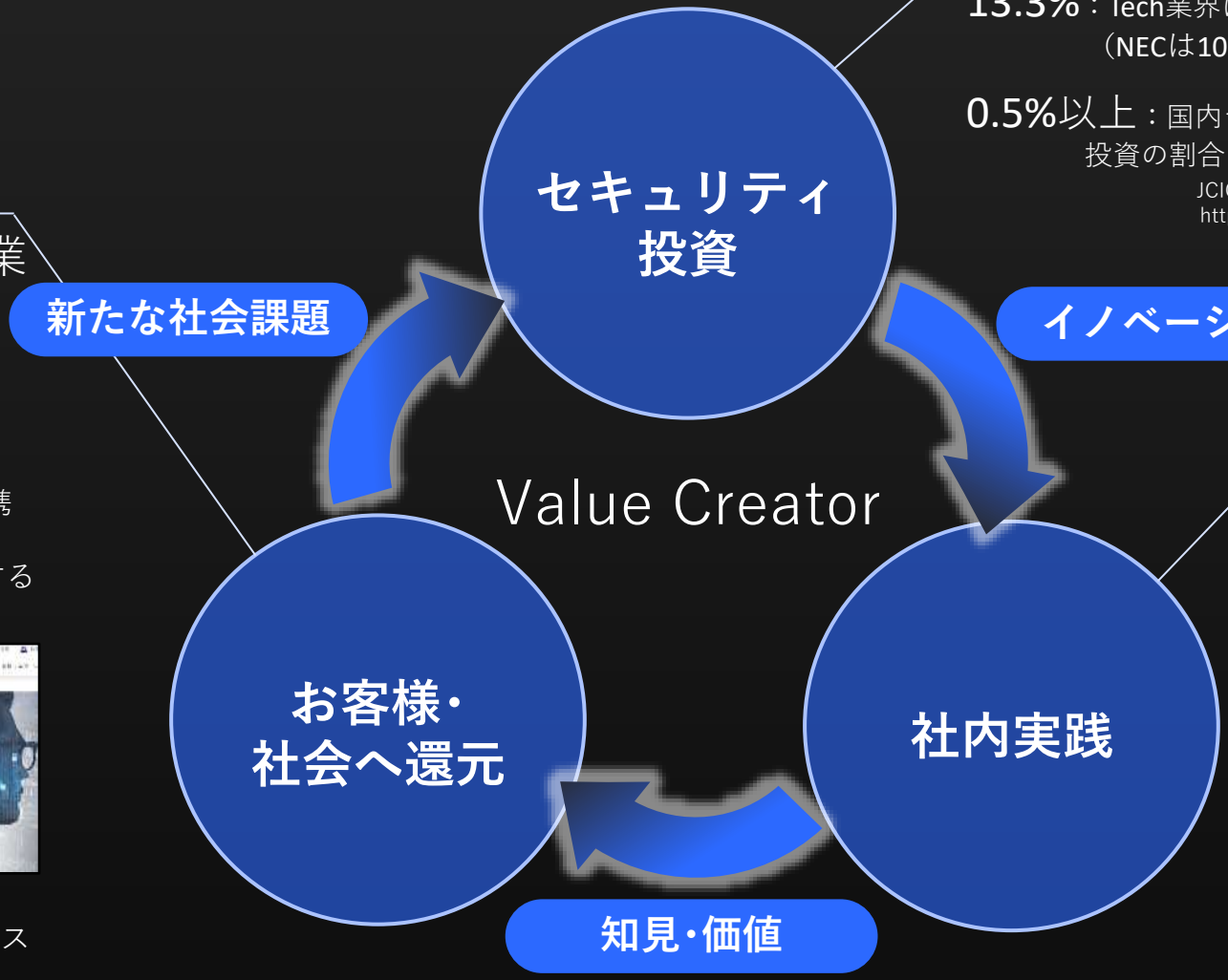
攻撃・異常監視(Agentic AI SOC*3)

脅威インテリジェンス・運用手法の確立

*2 組織が把握・管理していないAI
*3 Security Operation Center

最後に

社会の安心・安全のため、NECは「Value Creator」として
社会やお客様の課題に対し、常に全力で取り組んでまいります



13.3%：Tech業界におけるIT支出に占めるセキュリティ予算の割合（平均）
（NECは10%）
IANS & ARTICO「2022 Security Budget Benchmark Report」
https://cdn.iansresearch.com/Files/Marketing/IANSResearch-2022SecurityBudgetBenchmarkSummaryReport.pdf

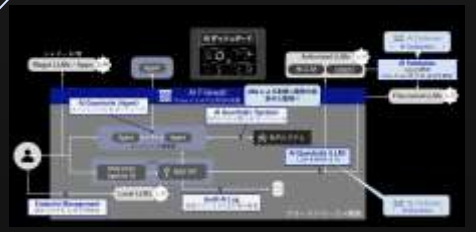
0.5%以上：国内シンクタンクが推奨する連結売上高に占めるセキュリティ投資の割合
JCICシンクタンクレポート　社内のセキュリティリソースは「0.5%以上」を確保せよ
https://www.j-cic.com/pdf/report/Security-Resources-Report.pdf

産官学連携/戦略協業

- インターポールとサイバーセキュリティ対策で提携
- 情報通信のサプライチェーンセキュリティ技術を開発
- 国立高専機構とNECによるセキュリティ分野の包括連携協定締結
- （ISC）2との人材育成に関する戦略的提携

データドリブン
サイバーセキュリティサービス

クライアントゼロ



AIガバナンス

サイバーセキュリティ経営報告書2026
https://jpn.nec.com/sustainability/ja/security

Orchestrating a brighter world

NEC Cyber Day’26夏
ポストAI時代のサイバーセキュリティ ～「ビヨンドゼロトラスト」で切り拓く新戦略～

現場責任者が語る、「ビヨンドゼロトラスト」の実践と、ポストAI時代の組織の衛り方

NEC　Corporate Executive CISO
　兼 NECセキュリティ株式会社　取締役　淵上 真一, CISSP ＜モデレータ＞
NEC　サイバーセキュリティ技術統括部長　青木 聡,CISSP
NEC　サイバーセキュリティ戦略統括部長　兼 CISOオフィス長　田上 岳夫,CISSP
NECセキュリティ株式会社　取締役執行役員副社長
　兼 NEC　サイバーディフェンス事業開発統括部　上席プロフェショナル　奥 隆行,CISSP

CyIOC事業のチャレンジ

BluStellar

2026
CyIOCのコアビジネス展開
- コアビジネス・サービス展開
- グローバルPF/Hubの確立

2027
グローバル機能拡張
- Follow-the-Sunの確立
- グローバルJOC市場へのアプローチ

2028~
ビジネス・サービス拡張
- グローバルビジネスモデル拡張
- グローバル競合可能な機能獲得

サービスの最適化

事業基盤の確立

能力及び機能の獲得・強化

JP-HQ　EU　APAC　US

コアビジネス強化　フォローザ・サン　サービス拡張

ナレッジ　人的基盤　機能拡張　コミュニティ形成　事業連携

グローバルデータ・ツール　官民連携　ACD能力強化

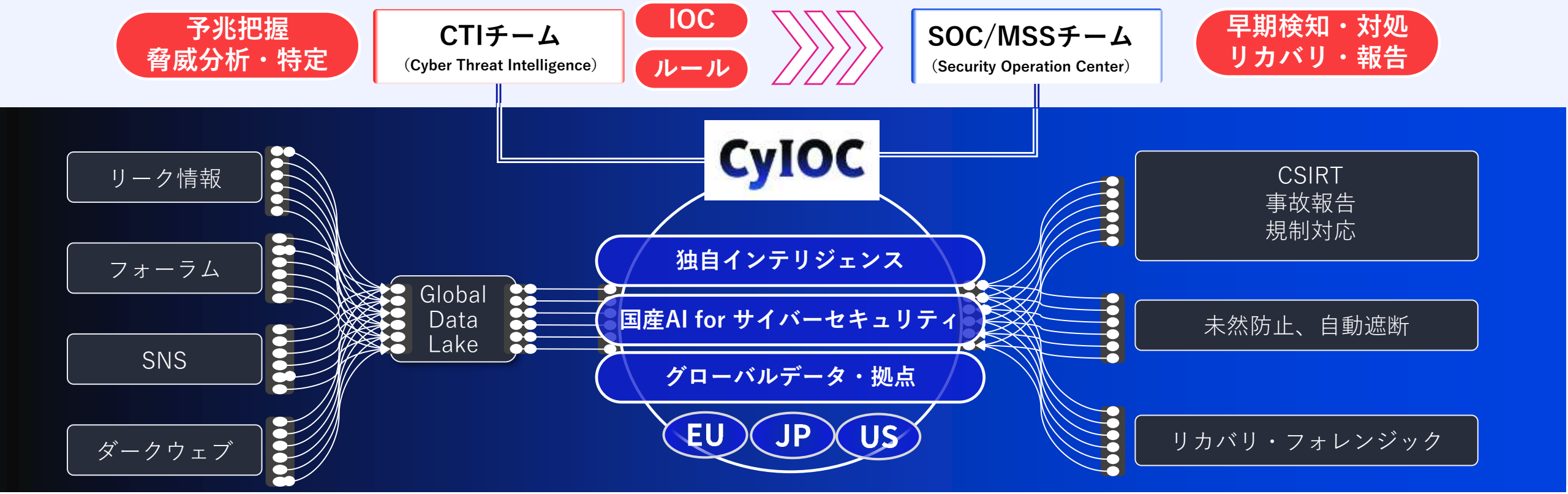
AI for Cybersecurity（AIエージェント）

サイバーセキュリティサィービス AI+インテリジェンス+ SOC/MSS

BluStellar

Cyber Intelligence & Operation Center

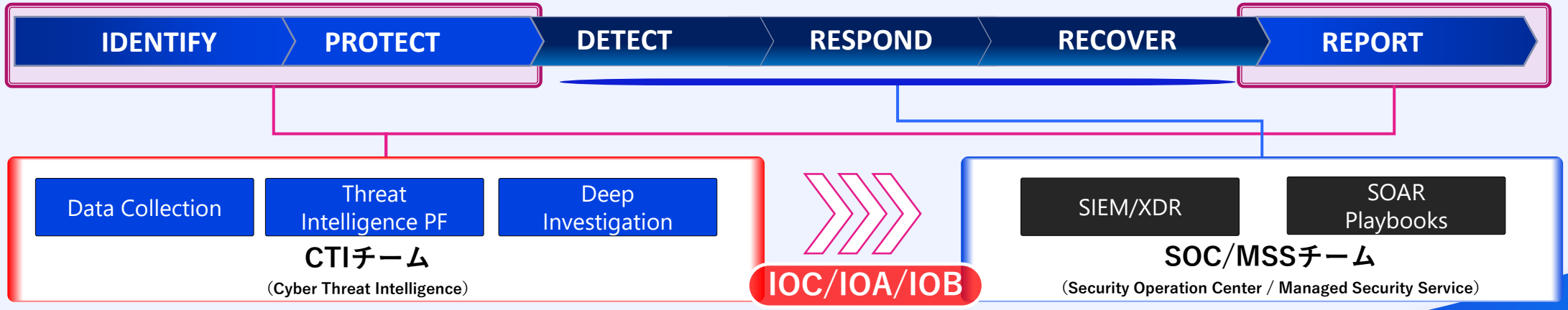
- インテリジェンス分析プラットフォームとSOC検知プラットフォームのシームレスな融合
- 国産AI（Cotomi）を活用した自律型AIエージェントの導入
- グローバルデータ集約・オペレーション拠点の拡張



BluStellar

CyIOC機能の高度化

- CTIを用いたSOC/MSSの高度化・効率化の実現
- グローバルベンダーとの競合、競争性優位性確保に向けた活動



（ニア）ゼロデイ対策

脅威特定の高速化

CTIを活用することにより、新たな脅威の発生を特定するスピードが平均で**65%向上**

検知・分析能力の向上

分析効率の向上

CTIからのIOCルールの提供によりSIEM/EDRの検知効率を**40%向上**、レスポンスタイムを**30%短縮**

分析効率の向上

CTIによりシニアアナリスト業務を**週50時間短縮**、より高度な判断、プロセス改善へ**リソースをシフト**

対処能力の向上

リカバリ作業の短縮

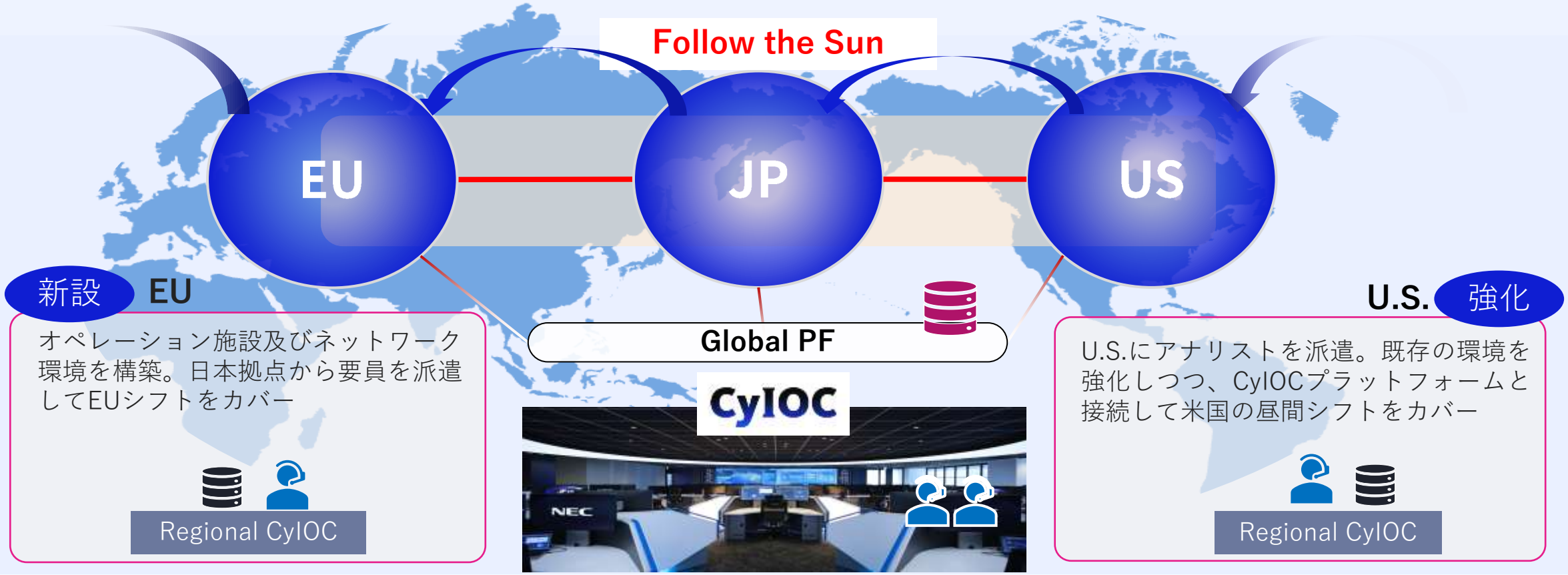
AI＋CTI自動化を活用することで、攻撃被害の封じ込めまでの期間を**約100日短縮**

https://www.recordedfuture.com/blog/improving-cybersecurity-productivity-threat-intelligence-recorded-future-drives-roi
https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec

BluStellar

CyIOCグローバル展開

■ EUにCyIOCのグローバル拠点を新設予定。セキュアな施設及びグローバルPFを共有
■ 日本と各拠点との間でグローバルデータ及びインテリジェンスを共有、サービス品質の向上



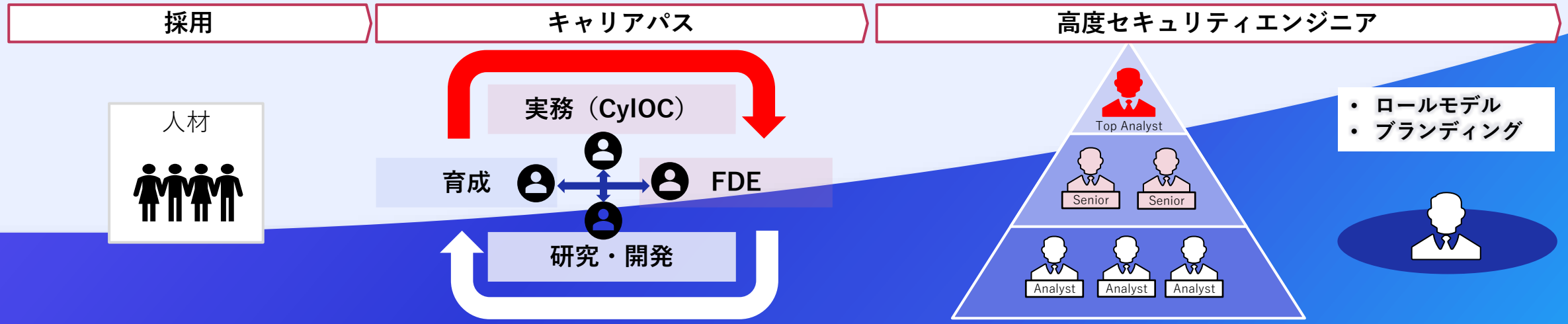
人的基盤の確立

■ CyIOCの高度かつ持続的なオペレーションを可能とする人的リソースの育成・確保
■ セキュリティエンジニアのキャリアパスの設定、モチベーションの向上

積極的採用による人材の確保
CSO部門・NSECにおけるポテンシャル人材の発掘・採用、中核チームの確立

人材のローテーションの構成
育成、実務、研究・開発、Forward Deployed Engineer（FDE）のローテ

キャリアパスとの最適なマッチング
人事システムとの統合、グループ企業との**人事交流**、**ナレッジトランファー**



\Orchestrating a brighter world

サイバーセキュリティ経営報告書2026

NECグループの情報セキュリティに関する最新の取り組みを紹介

NECでは「.JP（日本のサイバー空間）」を守るをスローガンに掲げ、経済産業省の「サイバーセキュリティ経営ガイドラインVer3.0」やNISTの「Cyber Security Framework（2.0版）」に基づき、深刻化するサイバー攻撃に対するインテリジェンス（事前防御）やレジリエンス（攻撃からの回復能力）を強化、実行する体制を構築しています

① 「.JP（日本のサイバー空間）」を守る

■NECの情報セキュリティレポート

② サイバーセキュリティ・ガバナンス
③ 情報セキュリティマネジメント
④ 情報セキュリティ基盤－AIセキュリティ（Security for AI）
⑤ 情報セキュリティ人材
⑥ サイバー攻撃対策
⑦ お取引先と連携した情報セキュリティ
⑧ セキュアな製品・システム・サービスの提供

■NECの情報セキュリティ最前線

⑨ NECのサイバーセキュリティ戦略
⑩ NECがご支援できること
⑪ 「.JP（日本のサイバー空間）」を守るためのグローバルな研究・事業開発
⑫ 第三者評価・認証
⑬ NECグループの概要

https://jpn.nec.com/sustainability/ja/security/

NEC Cyber Day’26夏
ポストAI時代のサイバーセキュリティ ～「ビヨンドゼロトラスト」で切り拓く新戦略～

セミナー事務局からのお知らせ

セミナー事務局からのお知らせ

ご視聴ありがとうございました。
次回、お会いできることを楽しみにしております。

1.アーカイブ配信

2026.7.16(木)～9.30(水)の間、My NECサイトから視聴いただけます。
新規申し込みによる視聴もできます。チームや同僚などへご案内ください。

My NECサイト
https://auth.nec.com/login

2. アンケートのお願い
投影資料Get、ISC2認定資格CPEクレジット申請

1 【回答特典】
本日の投影資料

今日の振り返りはもちろん、セキュリティ対策強化を検討される際の参考になれば幸いです。

2 【ISC2認定資格保持者様向け】
CPEクレジット付与申請

アンケートの最後に必要情報を記入ください。
CPEクレジット(2.0ポイント)を付与
期限： 明日（2026.7.15(水)）23:59 回答分まで

※期限後は、ご自身でISC2のサイトから登録をお願いします。

NEC Cyber Day'26夏
アンケート記入、
ISC2のCPEクレジット申請

https://forms.office.com/r/bu73cBE8w5

お問い合わせ：NEC Cyber Day セミナー事務局 cyber@mlsig.jp.nec.com

\Orchestrating a brighter world