

～AIエージェント時代の ガバナンスとセキュリティ～

そのAI、新入社員より 自由に働いていませんか？

奥村 光希

NRIセキュアテクノロジーズ株式会社

2026年10月10日



Agenda

本日の流れ

1

AIは、新しい従業員

2

導入だけで満足？

3

人は教育、AIは野放し

4

AIも教育する

5

そこでガイドライン

導入で終わらせず、AIも教育する

1. 何が変わったのか

AIは、新しい従業員



権限を持ち、自ら業務を実行する

守るものは「権限と行動」

2. 導入だけで満足していませんか 導入だけで、満足していませんか？

83.2%

生成AI利用率

2024年度 65.3%

→ 2025年度 83.2%



導入した



教育した？



権限を絞った？



監督している？

雇っただけで、育てていない

3. 人は教育する、AIは野放し 人を雇ったら、まず教育する



NRIセキュア研修

全社員

eラーニング

技術者

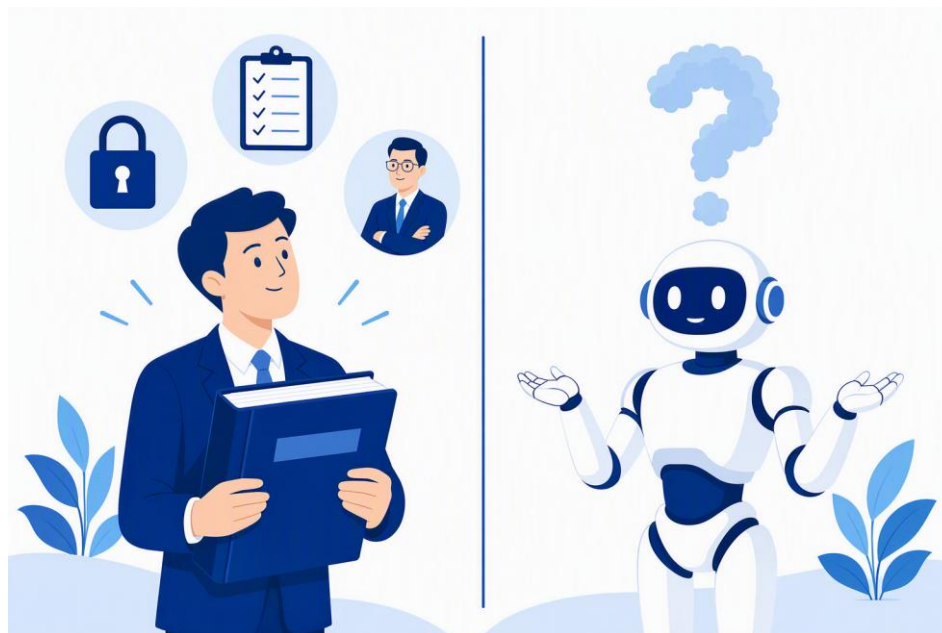
セキュアEggs

経営層

経営層向け研修

「使う人」は、教育している

3. 人は教育する、AIは野放し では、AIには？



ルールがある 何もない

AIには、何もしていない

3. 人は教育する、AIは野放し 野放しの結果、起きたこと



Replit
本番DBを削除

Amazon Kiro
13時間の障害

Antigravity
ドライブを全消去

「やるな」では、止まらない

4. AIを教育する AIも、教育する

採用



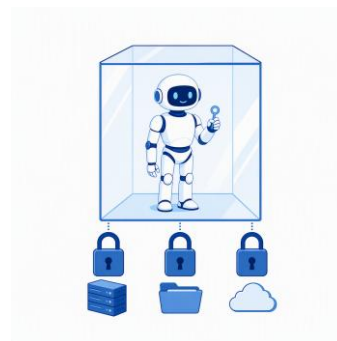
どのAIが
どこにいる

教育



できること
ダメなこと

権限



最小の権限
隔離で実行

監督



記録と承認
止められる

人の型は、AIにも使える

4. AIを教育する 自助だけでは、守り切れない

自助



自社で決めて
自社で守る

共助



業界で
知見を共有

公助



国の基準に
合わせる

自助から、共助・公助へ

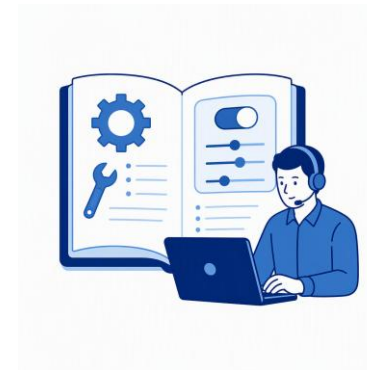
5. そこでガイドライン そこで、ガイドライン

リスク編



全社員向け
考え方とあるべき姿

ツール編



エンジニア向け
ツールごとの推奨設定

禁止リストではなく、設計図

5. そこでガイドライン 4ステップで、使われるものに



作って終わりにしない

まとめとご支援

AIを信頼するために、無条件には信頼しない



- ▶ 実態をつかむ
- ▶ 2種類で設計
- ▶ 人もAIも教育

NRIセキュアが
ご支援します

弊社ブースへ、ぜひお越してください！