R&Dフェーズ｜研究　**実用化時期**｜FY27-

Mehr Licht!
More Photonics for Intelligence

#C13

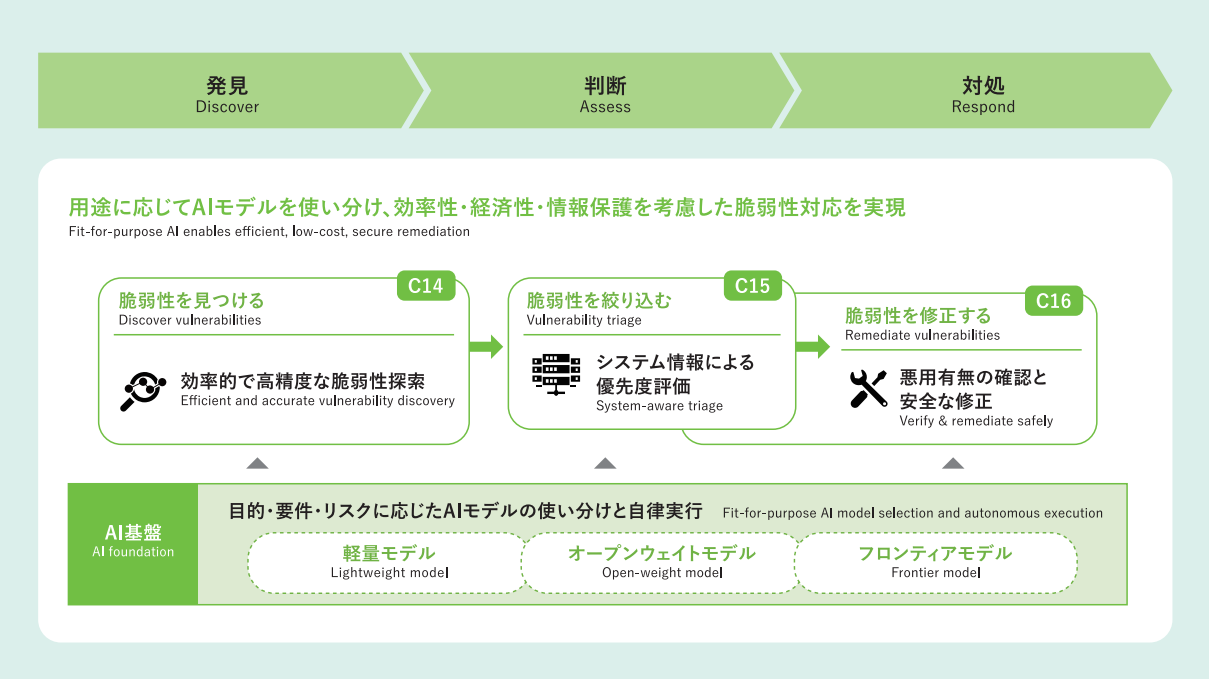
#サイバーセキュリティ#リスクマネジメント#安心・安全

自律実行型AIによる脆弱性リスク対応技術

用途に応じてAIモデルを使い分け、効率性・経済性・情報保護を考慮した脆弱性対応を実現します

技術課題・ゴール

ソフトウェアの複雑化やAIによる開発スピードの加速、攻撃の激化により、対応すべき脆弱性は増加しています。本技術は、脆弱性の発見・影響調査・優先度付け・対処をAIが自律的に実行し、脆弱性対応の迅速化・省力化を実現します。さらに、目的やリスクに応じたAIモデルの使い分けにより、経済性と情報保護も両立します。



技術ポイント

要素技術

・顧客要件に応じたAIモデル選択と、AIと専門的な解析技術の組合せによる安全・低コスト・高精度な脆弱性発見
・システム特性を踏まえた脆弱性の自動優先度判定による迅速な対処と、副作用を抑えた安全な修正技術

市中技術差異点

・AIモデルの性能のみに依存せずに効率的で厳密な脆弱性探索を実現
・脆弱性対応が必要なシステム特定とその特性に応じた対応優先度判定、および長年のセキュリティ運用で培った暗黙知のAI化を駆使した脆弱性修正が可能

適用ビジネス/ユースケース

情報技術

システム開発・運用現場の脆弱性対応において、顧客要件に応じたAIモデルを活用し、脆弱性の発見・影響調査・優先度付け・対処を自動化します。コストを抑えつつ、機密性の高いソースコードや閉域環境にも対応します。

出展組織

NTT株式会社 社会情報研究所