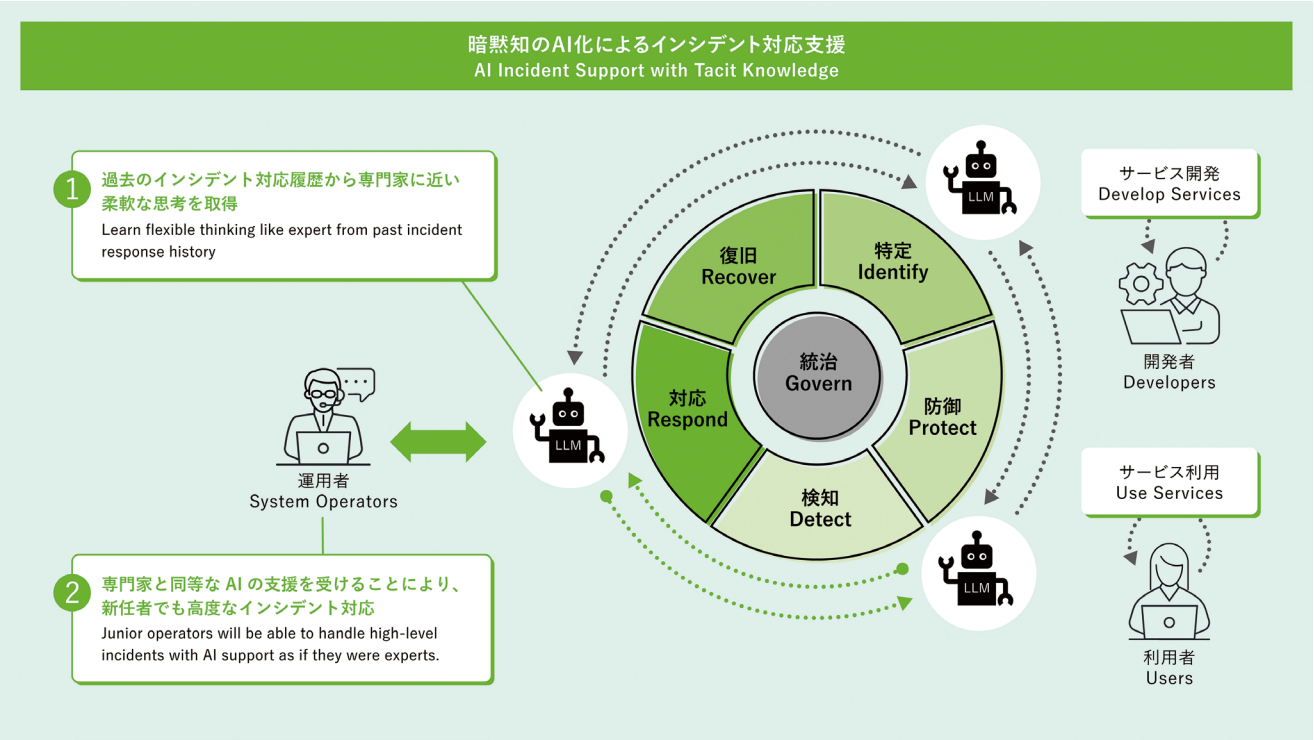
AIがセキュリティ専門家の暗黙知を活用し、非専門家によるインシデント対応を伴走します

暗黙知を用いたインシデント対応支援技術

背 景 – 技術課題

サイバー攻撃の高度化に対し、インシデント対応を担う人材は不足し、専門家のノウハウに依存しています。ノウハウを継承したAIによる支援が求められますが、既存AIの提案手順は抽象度が高く、また攻撃状況や社内環境は考慮されていないため、非専門家は実行できません。



研 究 目 標 – 成果

多くの専門知識と経験が必要なサイバーセキュリティ運用において、セキュリティ事故の一連の対応をAIが支援することにより、企業のセキュリティ水準と事業継続性の向上に貢献します。

技 術 ポ イ ン ト

01 要素技術

セキュリティ事故対応における専門家の暗黙知を含む公開情報やユーザ環境情報をもとにインシデント対応手順をAIに自動生成させることで、ユーザ環境を踏まえつつ専門性の高いAI伴走型の支援技術

02 市中技術差異点

他の組織が経験したインシデント対応に関する公開情報などの多様な知識をAIが具体的な対応手順に落し込んだ上で支援を行うことで、自組織が未体験のインシデントに対しても適切な対応が実現可能

利用シーン	情報技術	**R&Dフェーズ**	開発
技術確立予定時期	FY25-26	**ビジネス化予定時期**	未定

【出展企業】
NTT株式会社 社会情報研究所

【問い合わせ先】
社会イノベーション研究プロジェクト

【共同出展社/社外連携先】
–

【関連Link】
–