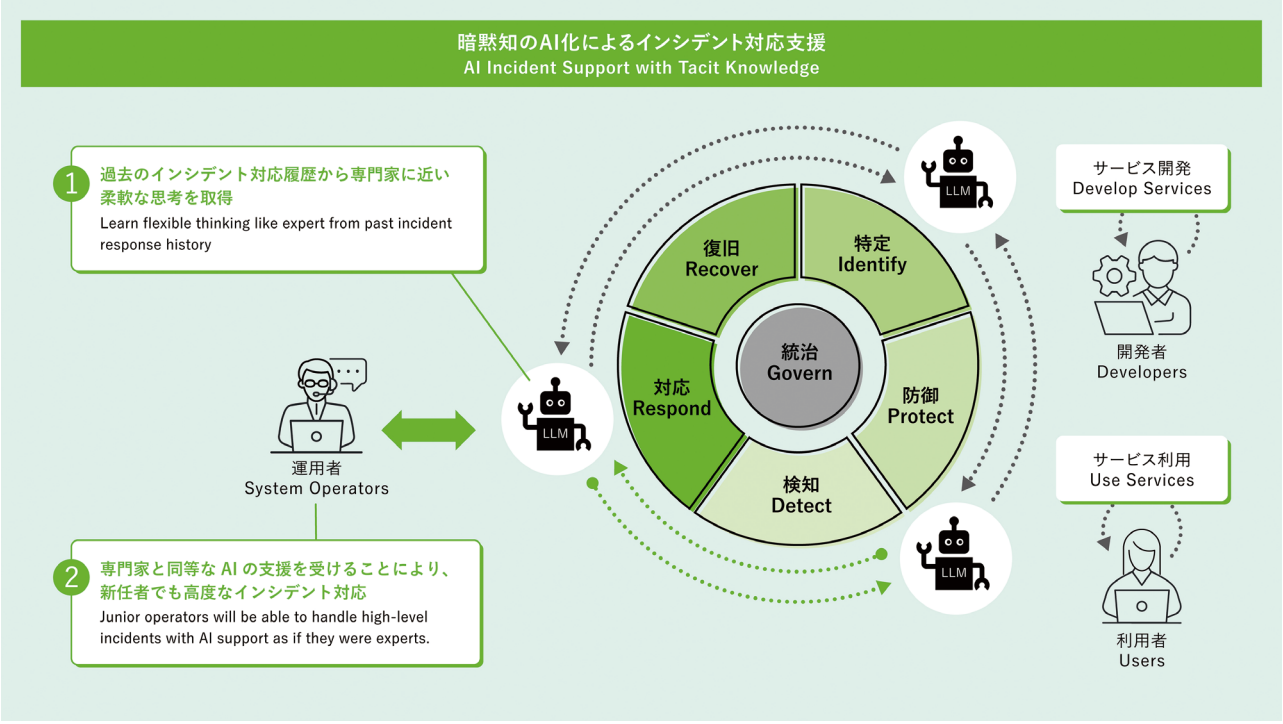
#Cybersecurity #Operational Efficiency

AI leverages tacit knowledge of security experts and supports non-experts in incident response

Incident support that uses AI based on tacit knowledge

Background and Technical Challenges

While cyber attacks become more sophisticated, there is a shortage of security personnel, and operations depend on expert experience. We need AI that inherits such experience, but current AI-generated response plans are generic and hard for non-experts to execute.



R&D Goals and Outcomes

AI supports end-to-end incident response in knowledge-intensive cybersecurity, raising enterprise security levels and business continuity.

Key Technologies

01 Core Technologies

This is achieved by having AI, which leverages the tacit knowledge of security experts, generate incident response procedures based on user environment information and publicly available data.

02 Key Differentiators

By having AI incorporate various knowledge, such as incident experienced by others, into response procedures, appropriate responses can be created even for incidents that the organization has not experienced.

Use Cases	Information Technology(IT)	**R&D phase**	Development
Technology Schedule	FY25-26	**Commercialization Schedule**	TBD

【Exhibitors】
NTT Social Informatics Laboratories

【Co-exhibitors】
-

【Contact】
Social Innovation Research Project

【Related Links】
-