Mehr Licht!
More Photonics for Intelligence

#C20

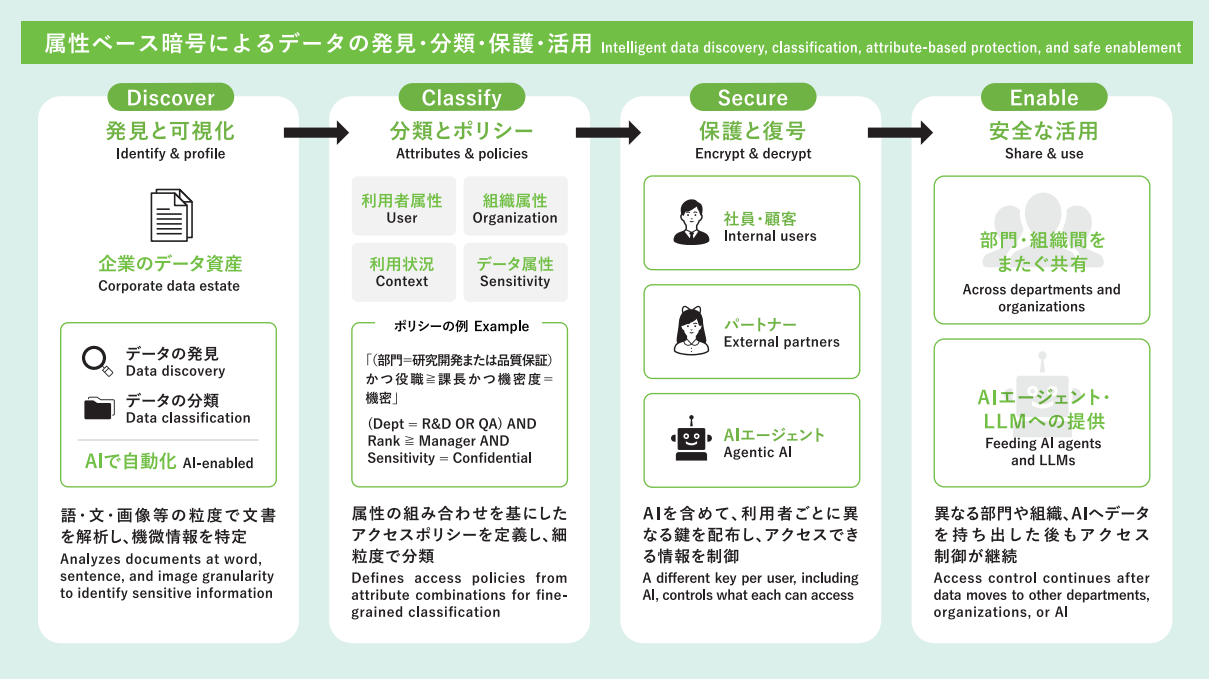
#Cybersecurity#Digital & AI Transformation#Responsible AI

Zero-Trust Data Security for the AI Era

Embedded policies enable fine-grained access control at the data level

Technical Challenges & Goals

Cyberattacks and AI keep expanding the data to protect. Perimeter defenses fail once breached, and data-layer control is all-or-nothing. Attribute-based encryption embeds access conditions in the ciphertext, so only matching attribute keys decrypt. Governing AI agents by the same policies accelerates safe adoption.



Key Technologies

Core Technologies

- Access policies embedded in ciphertext; decryption only by keys whose attributes satisfy them
- Multi-authority scheme where each organization issues its own attributes and manages keys

Key Differentiators

- One ciphertext serves N recipients instead of N; scope decided by attributes, not key possession
- Industry-first zero-trust data security product built on attribute-based encryption: PQC-ready

Use Cases

Financial Services

Banks and insurers share screening files internally and with auditors. AI agents decrypt only permitted fields; unapproved data are never read or learned.

Exhibitors

NTT Research, Inc.

Related Links

https://ntt-research.com/scale-academy/
https://ntt-research.com/ntt-research-launches-scale-academy-and-new-quantum-safe-security-platform/

CONTACT：NTT Research, Inc.