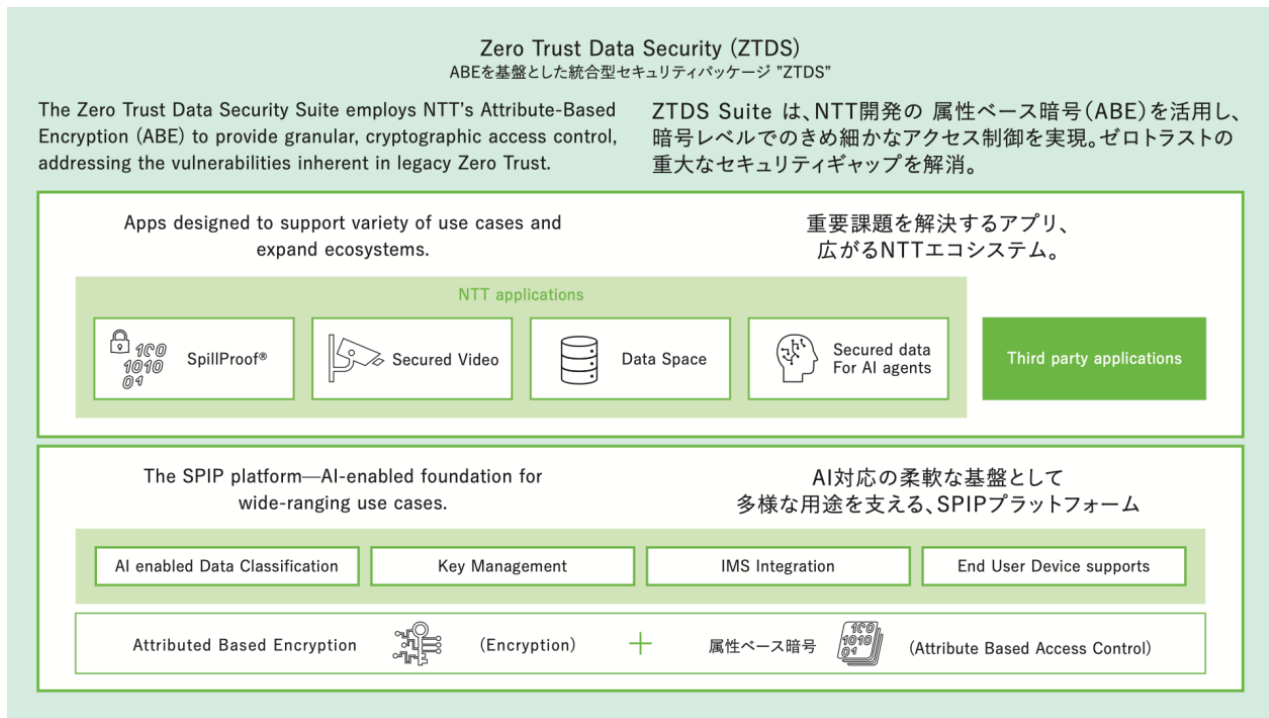AI-enabled data protection powered by ABE: addressing the gaps in current zero-trust implementations

Zero Trust Data Security (ZTDS)

Background and Technical Challenges

- Traditional encryption operates on a "all or nothing" basis, posing challenges in enforcing fine-grained access control and preserving confidentiality.
- Manual data identification and classification introduce significant burdens, hindering effective scalability.

R&D Goals and Outcomes

As data protection gains increasing significance, existing technologies encounter challenges in accommodating the rapid advancement of artificial intelligence and the implementation of stricter regulations.

Key Technologies

01 Core Technologies

Integrates ABE and AI-powered classification to effectively safeguard and disclose data.

02 Key Differentiators

In contrast to legacy access control, ABE integrates policies directly into data, thereby ensuring consistent protection throughout the entire data lifecycle, irrespective of where data is moved.

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