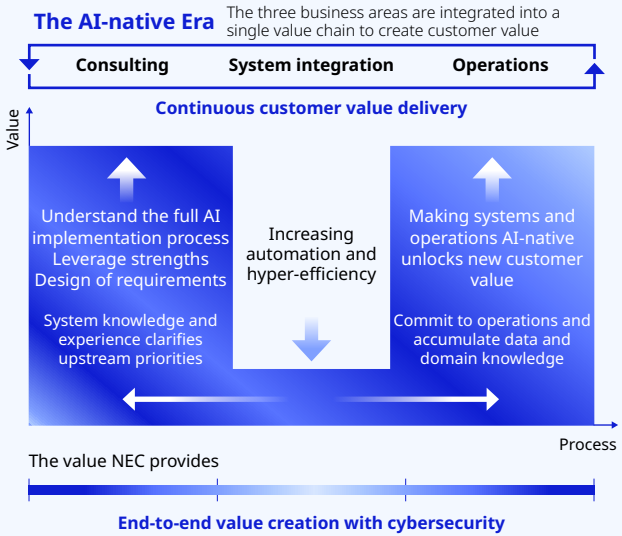
Business Environment

Innovations in AI and shifts in the security environment are fundamentally transforming the global order, creating both threats and opportunities

Structural Changes in the IT Services Market Driven by the Evolution of AI

As the AI industrial revolution gains momentum, new applications, platforms, and ultimately new forms of society and industry built around AI are expected to emerge, creating a global market exceeding ¥45 trillion in scale. Amid such profound changes in the market environment, competitive polarization among companies is expected to accelerate.

In the IT services market, structural changes are anticipated, including the automation and greater efficiency of system development, the expansion of in-house development, lower vendor switching costs, and increased risks stemming from the growing adoption of AI and the resulting ambiguity in operational accountability. The market has traditionally been divided into three distinct domains, namely consulting, system integration, and operations, each of which evolved as a separate market. In the AI-native era, however, companies that can seamlessly connect these domains and deliver end-to-end value, from requirements definition grounded in a deep understanding of the entire AI implementation life cycle to the creation of customer value (outcomes) will enhance their competitive position.



Broadening the Security Landscape Driven by Persistent Geopolitical Tensions and Innovations in AI

As strains on international cooperation and the malicious use of technology increasingly threaten everyday life, the distinction between peacetime and contingencies becomes increasingly blurred. Against this backdrop, civilian and defense technologies and markets are converging, and the importance of digital infrastructure continues to grow, broadening the scope of security. This expansion extends beyond growing defense budgets and the broader application of defense technologies for civilian use. It also reflects expanding business opportunities across the broader security domain, including economic security and cybersecurity. The need to ensure the safety and reliability of critical digital infrastructure is becoming increasingly important. At the same time, as cyberattacks become more sophisticated, the value of strengthening cybersecurity to protect social systems will continue to grow.

What It Takes to Win amid Structural Change

To emerge as a winner amid the profound changes reshaping industrial structures and social systems, companies must be able to make outcomes tangible by combining three essential elements: domain knowledge that enables decision-making and sustained value delivery, a system architecture designed to deliver customer outcomes, and foundational capabilities that create value in the AI-native era. How NEC acquires and strengthens these capabilities is a key focus of Mid-term Management Plan 2030.

Domain Knowledge
Drives decision-making and sustained value delivery

- Industrial knowledge
- Cross-industry knowledge

System Architecture
Designed to deliver customer outcomes

- AI governance
- AI platform
- AI-ready data preparation
- Cloud IT infrastructure with security

Foundational Capabilities
Create value in the AI-native era

- Cutting-edge AI technology
- Dual-use technology* development
- AI-native processes and culture
- Partnerships

* Dual-use technology: Technology that may be used for both civilian and security purposes