A Japanese Perspective on the International Energy Landscape (819) November 12, 2026

Rapidly Increasing Cyberattacks: Perspectives from Geopolitical Risk and Energy Security

Ken Koyama, PhD
Senior Advisor
The Institute of Energy Economics, Japan

The growing frequency of cyberattacks and the escalating scale of the damage they inflict have become subjects of major global concern. Since October in particular, reports of cyber incidents have become a near-daily feature of headline news in Japan. The country has witnessed an unprecedented surge in cyberattacks, resulting in large-scale information leaks and substantial economic and social damages.

According to media reports, the number of publicly disclosed cyberattack incidents in Japan reached 233 cases in October, representing a 2.4-fold increase over the previous record of 96 cases reported in September 2024. Equally noteworthy is not only the increase in the number of incidents but also the extraordinary scale of information breaches. Publicly reported cases of personal data leakage reportedly reached 185.44 million records in October alone, more than double the figure recorded in the preceding month. Cumulative personal data breaches through the end of October 2026 amounted to 376.21 million records, already far exceeding the previous annual record of 49.53 million records set in 2025.

Another striking characteristic is the growing size of individual data breach incidents. In 2026, ten separate cyber incidents each resulted in the leakage of more than 10 million records, six of which occurred in October alone. Between 2012 and 2025, only three such incidents had been recorded. The developments observed in 2026, and particularly in October, therefore represent a highly unusual situation. Large-scale information leaks have affected several major and widely recognized corporations, transforming cybersecurity from a corporate concern into a significant social and economic issue for Japan as a whole.

The intensification of cyber threats is by no means limited to Japan. Across the globe, cyberattacks have emerged as a major concern. In Asia, several financial institutions in South Korea, including major banks, have reportedly suffered cyber intrusions resulting in the leakage of substantial amounts of personal information. In Taiwan, cyberattacks against financial institutions have reportedly led to customer losses through unauthorized fund transfers and related fraudulent activities. In Europe, incidents in France, Belgium, Sweden, the Netherlands, Germany, and other countries have attracted considerable attention after cyberattacks reportedly caused malfunctions in refrigeration systems at supermarkets, resulting in temperature increases and large-scale food spoilage. In France, cyber

incidents targeting refrigeration facilities at blood banks have also been reported.

While numerous factors have been cited to explain the rapid increase in cyberattacks and associated damages, one of the most significant recent developments is the emergence of cyberattacks utilizing generative artificial intelligence (AI). AI-assisted attacks appear to have substantially enhanced the sophistication, speed, and frequency of malicious operations, potentially enabling levels of efficiency previously unattainable. As electrification, digital transformation (DX), and internet connectivity continue to expand throughout modern society and economic activity, existing cybersecurity vulnerabilities have become more consequential. In this sense, the advancement of digitization itself can be viewed as a growing source of cybersecurity risk.

It has long been recognized that many cyberattacks are motivated by economic gain. Cybercriminals may demand payments in exchange for refraining from disclosing stolen customer information or for restoring access to critical data and systems disabled through ransomware attacks. Stolen personal information may also be traded or publicly exposed on so-called dark web marketplaces. In some cases, however, the principal objective is simply to inflict extensive damage upon the targeted organization or institution.

Cyberattacks, however, possess another dimension that extends beyond criminal profit-seeking. They can serve as instruments of military strategy and geopolitical competition. Conducted alongside or prior to conventional military operations, cyberattacks may be intended to disrupt economic activity, weaken social stability, create confusion, and undermine an adversary's capacity to sustain military operations.

The Russian invasion of Ukraine, which began in February 2022, provides a notable example. Prior to the invasion, cyberattacks targeting Ukrainian government agencies, media organizations, critical infrastructure facilities, and information technology systems reportedly increased significantly. Energy infrastructure, including electricity systems, constitutes a particularly important component of national resilience. Should cyberattacks impair or disable such systems, the consequences could be severe. Indeed, in December 2015, Ukraine experienced a large-scale power outage widely attributed to a cyberattack believed to have originated from Russia. Although cyber operations against Ukraine appear to have continued throughout the conflict, attacks against energy infrastructure increasingly shifted toward direct military strikes involving missiles and drones. Nevertheless, the Ukrainian experience demonstrates that critical energy infrastructure can become a target of both conventional military attacks and cyber operations during armed conflict.

Cyber activities may also have played a role in the conflicts that occurred in the Middle East during 2026. While direct military attacks involving missiles and drones generally cause more visible and

immediate destruction, the effects of cyberattacks are often less apparent and therefore more difficult to assess. Since the summer of 2026, allegations have emerged suggesting that Iran may have been involved in cyber incidents, or suspected cyber incidents, occurring in the United States and the United Kingdom. In another notable case, the French government publicly attributed cyberattacks against refrigeration facilities to Iran, an accusation that Tehran subsequently denied.

These developments illustrate the close relationship that frequently exists between geopolitical tensions, military confrontations, and cyber operations. Given the range of geopolitical uncertainties surrounding East Asia and Japan in particular, policymakers and stakeholders must remain vigilant regarding a broad spectrum of risks and threats, including cyberattacks. Ensuring social and economic stability will require preparedness based on objective risk assessment rather than preconceived assumptions.

As societies become increasingly electrified and interconnected through digital networks, maintaining a stable electricity supply is becoming an even more critical component of energy security. Simultaneously, the large-scale expansion of renewable energy deployment is creating new challenges for power system management and resilience. In this context, cybersecurity is emerging as an essential dimension of electricity security. To conclude this discussion, it is useful to cite excerpts from the executive summary of *Security Challenges Associated with the Expansion of Renewable Power Generation* (Yu Nagatomi, October 2026), one of the key analyses included in the "IEEJ Outlook 2027", which examines the intersection of power system security and cybersecurity under evolving energy conditions.

"As electrification progresses and electricity accounts for an increasing share of final energy consumption, addressing cyber threats to electricity-related equipment will become increasingly important. In particular, cybersecurity risks associated with small-scale distributed energy resources (DERs), such as rooftop solar PV systems and battery storage, represent an emerging challenge. Cybersecurity measures must therefore extend beyond individual power plants to encompass the entire power system, including distributed energy resources."

"Power conditioning systems (PCSs) used in solar PV installations, as well as inverters widely deployed in battery storage systems and household appliances, may be vulnerable to unauthorised access and remote manipulation through communication functions and cloud connectivity. Furthermore, as with solar PV modules and battery cells, global inverter manufacturing capacity is concentrated in a limited number of countries. This concentration could expose power systems to overlapping risks arising from supply chain dependence and cybersecurity vulnerabilities."