Special Bulletin

A Japanese Perspective on the International Energy Landscape (532) May 12, 2021

Cyberattacks and Energy Security

Ken Koyama, PhD
Chief Economist, Managing Director
The Institute of Energy Economics, Japan

On May 7, the largest oil pipeline system in the United States shut down all operations in response to a cyberattack. The Colonial Pipeline system extends 8,859 kilometers from a refinery base on the Gulf of Mexico coast in Texas to huge northeastern oil consumption markets including New York, transporting 2.5 million barrels per day in gasoline, diesel and jet fuel, covering 45% of oil consumption on the East Coast, known as the U.S. oil consumption center. It is one of the major arteries for transporting petroleum products in the United States.

Colonial Pipeline Co. fully halted its pipeline operations after finding the ransomware cyberattack using malware that encrypts key data in a computer system to restrict users from accessing those data until they pay a ransom. The company resumed partial pipeline operations on May 9 and announced on May 10 that it would try to effectively restart full operations by the next weekend. At present, however, no optimism can be warranted about future developments

The shutdown of the major artery tightened U.S. fuel supply. In response to the shutdown, efforts are being made to switch to other means including tankers for transporting petroleum products from domestic refineries, to secure petroleum product imports and to gather market inventories to make up for any supply shortfall. Gasoline futures prices temporarily reacted to the cyberattack and crude oil futures rose gradually until May 11. However, their reaction to the shutdown has so far been limited, leaving the market to remain relatively stable. If the restoration of the pipeline is delayed, with the supply disruption prolonged, however, the overall U.S. petroleum product supply-demand balance could tighten. This is because demand for gasoline and other petroleum products is increasing amid a recovery from the COVID-19 catastrophe toward the driving season.

In fact, the shutdown caused concerns about gasoline shortages, long lines at gas stations and gasoline outages at many gas stations in states that depend heavily on the pipeline. Concerns about supply shortages usually lead to panic buying and hoarding that add to shortages, causing a vicious circle. While consumers are required to coolly react to the pipeline shutdown, the early restoration of the pipeline will hold the key to future developments.

On May 10, the Federal Bureau of Investigation attributed the cyberattack to DarkSide, a Russia-linked hacking group, which has frequently hacked networks to make money. DarkSide has issued a statement claiming that it is not political and that they only want to make money. As the attack has been attributed to DarkSide, however, Russian authorities' potential involvement in the attack has attracted attention. President Joseph Biden said that although there was no evidence of the Russian government's involvement in the attack, a Russian hacking group evidently implemented the cyberattack from Russia. He thus indicated that Russia was responsible to some extent for the attack. While the Russian government has denied any involvement in the attack, the incident could further affect U.S.-Russia relations that have already been soured.

Attracting attention in the future will be the restart of the pipeline, the U.S. petroleum product supply-demand balance, oil price trends and the impact on U.S.-Russian relations of investigations and arguments on the cyberattack. Anyway, the oil supply disruption caused by the cyberattack has impressed the world anew with the fact that cyberattacks are a grave risk factor for energy security. Cyberattacks on energy infrastructure were seen earlier, bringing about huge damage and impacts. They included a cyberattack on Ukraine's power system, causing massive blackouts. In April this year, an alleged Israeli cyberattack hit a power supply system for Iran's nuclear facility. However, the latest attack took place in the United States, becoming a remarkable incident causing a large-scale, serious energy supply disruption in a big energy-consuming industrial economy. As a matter of fact, cyberattacks on energy systems and infrastructure were seen earlier in Japan, Europe and the United States. However, the pipeline attack inflicted the largest damage in an industrial economy, attracting global attention. It is also significant that the attacker was from Russia that has deepened confrontation with the United States in international politics or geopolitics.

Energy security is defined as securing sufficient energy for normal economic activities and civic life stably at reasonable or affordable prices. There are various risk factors threatening energy security. Among them are emergent or accidental risk factors that come suddenly and unpredictably. They include accidents and troubles in some parts of an overall energy supply chain covering from the upstream sector for energy development and production to the international and domestic transportation sector, the conversion sector producing final energy from primary energy, and the downstream sector including distribution and consumption. Accidents or troubles are caused by cyberattacks as well as political incidents such as wars and revolutions, natural disasters and abnormal weather conditions. Interests in the significance of cyberattacks have grown in recent years.

The global energy system represents a large, complex supply chain consisting of the upstream, midstream and downstream sectors. Its stable management secures energy security. The stable, efficient management of the giant system depends on advanced information and communications technologies. Energy security is based on the use of advanced information and communications technologies. For this reason, cyberattacks become a grave risk factor that threatens energy security by taking advantage of potential vulnerabilities in today's advanced energy systems to trigger malfunctions.

Given that energy is an indispensable good for civic life, economic management and national management, and a strategically important material, threatening energy supply or energy security with cyberattacks can be considered identical to doing so with direct military or terrorist attacks. Therefore, cyberattacks inflicting serious damage on energy security are significant for international politics or geopolitics. As noted above, earlier cyberattacks in Japan, the United States and Europe had triggered few large-scale energy supply shortages. However, the Colonial pipeline attack and shutdown have led countries in the world to recognize that this kind of problem could come at any place or time.

This year saw power supply crises caused by abnormal weather in Japan and the United States early this year before the cyberattack disrupted oil supply, indicating that how to enhance energy security policies to address various new risk factors would become important in future policy discussions.

Contact: report@tky.ieej.or.jp
The back issues are available at the following URL
http://eneken.ieej.or.jp/en/special_bulletin.html