NAGASHIMA OHNO & TSUNEMATSU
長島·大野·常松 法律事務所

NO&T Japan Legal Update

March, 2024 No.44

This issue covers the following topics:

International Arbitration / International Mediation

Recent Reform of Japan's Arbitration Act

- Enforcement of the Order for Interim Measure and the Settlement Agreement through Mediation -

I. Introduction

April 21, 2023 saw the enactment of three laws arbitration- and mediation-related laws: the Law Partially Amending the Arbitration Act (Act No. 15 of 2023) (the "Amended Arbitration Act"), the Law Concerning the Implementation of the United Nations Convention on International Settlement Agreements resulting from Mediation (Act No. 16 of 2023) (the "Act Implementing Singapore Convention"), and the Law Partially Amending the Act on Promotion of Use of Alternative Dispute Resolution (Act No. 17 of 2023) (the "ADR Act"). These laws were promulgated on April 28, 2023, and are scheduled to go into effect on April 1, 2024.

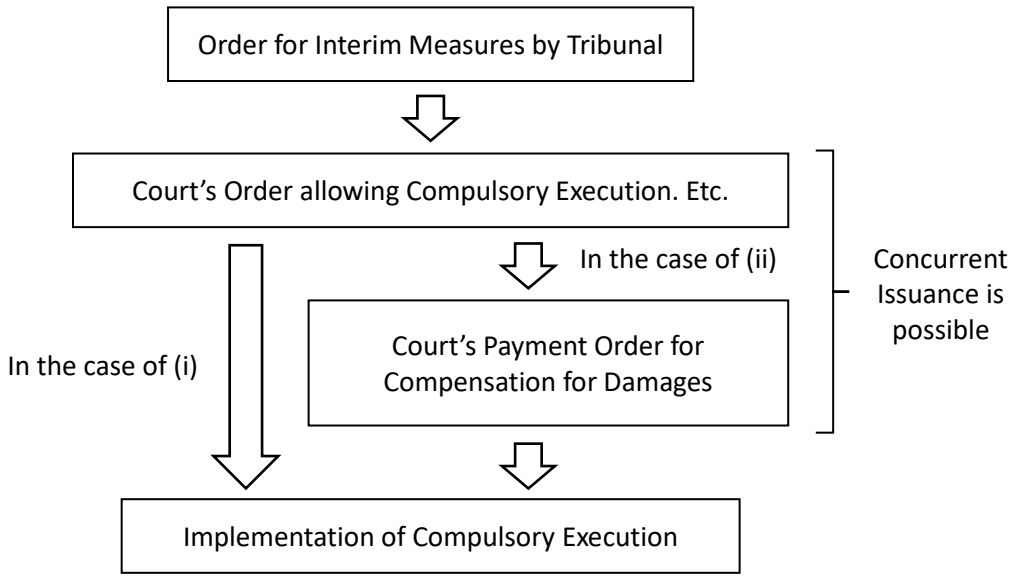
These three laws are aimed at integrally strengthening dispute resolution procedures administered by private dispute resolution organizations, including international arbitration and mediation, by making the order for interim measures issued by the arbitral tribunal and the settlement agreement through mediation enforceable. A summary of the laws is as follows.

II. Amendment Enabling Enforcement of an Order for Interim Measures

Japan's current Arbitration Act (Act No. 138 of 2003) was enacted in 2003 based on the UNCITRAL Model Law (the original 1985 version) but has not reflected the latest UNCITRAL Model Law (amended in 2006). This has been an obstacle to Japan's being selected as a seat of arbitration. In addition, under Japan's current Arbitration Act, there is no means to enforce an order for interim measures issued by the tribunal until an arbitral award is issued, and there was a risk that property dispositions, etc. would be made before the arbitral award is issued, hampering the effectiveness of the order for interim measures.

Like the latest UNCITRAL Model Law, the Amended Arbitration Act allows for enforcement of an order for certain types of interim measures issued by the tribunal to preserve rights and evidence pending an arbitral

award (an "Order for Interim Measures"). While there are a variety of types of orders for interim measures that are issued by the tribunal, the Amended Arbitration Act specifically provides two types of Order for Interim Measures that are enforceable: (i) measures necessary to avoid significant damage or imminent danger to the property or rights subject to dispute, or to restore the property to its original condition, and (ii) prohibition of the disposal of property, etc.[1]. After the Order for Interim Measures is issued, the petitioner may request the court to issue a compulsory execution[2]. The court will examine whether or not there are grounds for refusing compulsory execution, and if there are none, the court will issue an order allowing compulsory execution, etc.[3]. If the court's order allowing compulsory execution, etc. is issued, compulsory execution is implemented based on the Order for Interim Measures as a title of obligation in the case of "(i)", above, or, in the case of "(ii)," as a payment order for compensation for damages as a result of violation (which is to be issued by the court where there is a violation or threat of violation of the Order for Interim Measures as a title of obligation).



Prepared by the author based on the website of the Ministry of Justice (https://www.moj.go.jp/content/001395270.pdf)

In addition, in connection with this amendment, the following revisions have been made:

- In procedures where a petitioner is seeking a compulsory execution based on the arbitral award, the court may, if it deems it appropriate, not require a Japanese translation of the arbitral award[4]; and
- the petition for a compulsory execution based on the arbitral award may also be filed at the Tokyo District Court and the Osaka District Court as additional concurrent jurisdictions[5].

These amendments would make the Order for Interim Measures more effective and simplify the procedures for the enforcement of arbitral awards in Japan.

[1] Article 24(1) of the Amended Arbitration Act
[2] Article 47(1) of the Amended Arbitration Act
[3] Article 47(7) of the Amended Arbitration Act
[4] Proviso to Articles 46(2) and Proviso to Article 47(2) of the Amended Arbitration Act
[5] Article 46(4) of the Amended Arbitration Act

III. Establishment of a System for Enforcement of Settlement Agreements Reached Through Mediation

(i) Compulsory Execution of Settlement Agreement Reached Through International Mediation

Under the current legal system, there was no framework to enforce the settlement agreement even if a settlement agreement was reached in international mediation. In addition, in September 2020, the United Nations Convention on International Settlement Agreements resulting from Mediation (the "Singapore Convention on Mediation") came into effect, and Japan acceded it in October 2023. In response to this trend, a system was established to allow courts to issue enforcement decisions based on settlements reached in international mediations[6]. In order for an enforcement decision to be issued, (i) the agreement must be an international settlement agreement[7], (ii) the agreement must be a settlement agreement pertaining to a commercial dispute (not applicable to disputes in which individuals are parties, individual labor disputes, or disputes concerning personal status or family matters)[8], and (iii) the parties must have agreed on enforceability of the international settlement agreement based on the Singapore Convention on Mediation or the Act Implementing Singapore Convention (an "opt-in reservation")[9], and (iv) there must be no grounds for refusal of execution[10].

(ii) Compulsory Execution of Settlement Agreement Reached Through Domestic Mediation

Under the current system, even if a settlement was reached through mediation in Japan, there was no mechanism for enforcement based on the settlement. The ADR Act establishes a new system which allows the court to issue an enforcement decision based on settlements reached in domestic mediations (Article 27-2 of the ADR Act). In order for an enforcement decision to be issued, (i) the settlement must be achieved via certified (accredited) dispute resolution procedures conducted by certified dispute resolution business operators, (ii) the settlement agreement must pertain to a commercial dispute (not applicable to contract disputes between a legal entity and a consumer, individual labor disputes, and disputes concerning personal status or family matters) (Article 27-3 of the ADR Act), (iii) the parties must have agreed in the certified mediation procedures on enforceability of the settlement agreement through domestic mediation (*Opt-in Reservation*) (Article 27-3 of the ADR Act) (Article 2, Paragraph 5 of the ADR Act) and (iv) there must be no grounds for refusal of execution (Article 27-2, Paragraph 11 of the ADR Act).

The above amendments will also ensure the effectiveness of settlements reached through mediation, and are expected to expand opportunities for the use of mediation in Japan as a dispute resolution tool.

---

[6] Article 5 of the Act Implementing Singapore Convention

[7] Article 2 of the Act Implementing Singapore Convention. As used herein, "international settlement agreement" means an agreement entered into by parties (i) whose head office, or parent company's office, is located outside Japan, (ii) whose addresses, business offices, etc. are in different countries, or (iii) whose domicile, place of business, etc., as well as the place of performance of obligations under the settlement agreement, are in different countries.

[8] Article 4 of the Act Implementing Singapore Convention

[9] Article 3 of the Act Implementing Singapore Convention

[10] Article 5, Paragraph 12 of the Act Implementing Singapore Convention

[Author]

Kaori Sugimoto, Partner
kaori_sugimoto@noandt.com

Kaori Sugimoto focuses on international construction & infrastructure project (including ODA project and PPP project) and international dispute resolution including international arbitration. She has extensive experience in negotiation or drafting of contracts for international construction and infrastructure projects, particularly those involving Japanese companies in Southeast Asia, the Middle East, and Europe. She is proficient in international arbitration, with a focus on resolving construction-related disputes, in which she frequently serves as legal counsel. She is currently a member of ENAA (Engineering Advancement Association of Japan) and ECFA (Engineering and Consulting Firms Association).

Cyber Security

Recent Legal Developments in Japan for Fortifying Essential Infrastructure Services' Resilience Against Cyber Threats

I. Introduction

In light of the escalating cyber threats in Japan during the year 2023, the Japanese National Police Agency ("**JNPA**") has underscored the persistent prevalence of ransomware attacks, with a noteworthy increase in incidents related to a new form of ransomware known as "No-ware ransom"[11]. This variant involves the theft of data from victims' companies without encryption of the stolen information, thereby causing substantial harm. Additionally, the Information-Technology Promotion Agency publicly reported "10 Major Security Threats 2024"[12]. In this article, which concerns threats to enterprises, attacks exploiting vulnerabilities embedded in the supply chain are ranked as the second-highest threat, while damage caused by ransomware attacks is ranked first.

Given the concerning trend in cyberattacks, the Japanese national government, together with pertinent government agencies, has proactively established a system (the "**System**") under the Economic Security Promotion Act ("**ESPA**") to ensure provision of essential infrastructure services ("**EIS**") and enhance the supply chain risk management, including ensuring cybersecurity in EIS. This System is aimed at fortifying EIS resilience against cyber threats and ensuring a comprehensive response to emerging challenges.

The subsequent sections provide a comprehensive outline of the System, especially focusing on the supply chain risk management implemented to safeguard EIS.

II. Outline of the System for Ensuring Provision of Essential Infrastructure Services Under the Economic Security Promotion Act

The System is established pursuant to the ESPA, which was enacted in 2022 in response to escalating cybersecurity threats in Japan. Operational from May 2024, the System aims to mitigate risks such as the embedding of malware during equipment installation or software updates and the exposure of vulnerable information by third parties outside Japan. Starting from 2023, competent authorities have created and updated guidelines in preparation for effective implementation of the System beginning in May 2024[13].

(i) Outline of the System for Ensuring Provision of EIS

- **Purpose:** The primary objective of the System is to prevent critical facilities of the EIS ("**CF**") from being exploited from outside Japan as a means of disrupting stable provision of EIS. Competent authorities conduct a prior screening process and issue recommendations or orders concerning the installation or entrustment of maintenance, etc. (as defined below), of the CF.

- **Scope of EIS:** EIS encompasses services in electricity, gas, oil, water, railways, truck transport, international maritime cargo, aviation, airports, telecommunications, broadcasting, postal services, financial services, and credit cards. Designated as EIS are services that are either (i) crucial for national livelihoods or economic activities and the lack of which may lead to widespread or large-scale social turmoil or (ii) essential for citizen survival with limited substitution possibilities. Competent authorities in the respective EIS fields designate the specific services falling under this purview. Please be informed that, in response to a ransom-ware attack on the Nagoya United Terminal system operated in Nagoya port facilities in July 2023, as a result of which certain port-facility operations were suspended for more than two days, the Japanese

[11] https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf
[12] https://www.ipa.go.jp/security/10threats/10threats2024.html
[13] For example, Cabinet Office of the Japanese government publicly discloses its guideline in the following website. https://www.cao.go.jp/keizai_anzen_hosho/doc/infra_kaisetsu.pdf

government decided to amend the relevant regulations in order to add "port transport" to EIS in January, 2024.

- **Scope of the CF:** Equipment or programs that may be exploited for interference with the stable provision of EIS, such as through cyber-attacks or physical interception measures, are designated as CF. Competent authorities in the respective EIS fields identify and designate such CF[14].

- **Scope of EIS Operators:** EIS operators are designated based on the unique circumstances of each EIS, considering factors such as the scale of operation or substitutability. Competent authorities in the respective EIS fields identify and designate EIS operators[15].

- **Duty of EIS Operators:** Upon the installation of CF for business use or the commencement of entrustment of maintenance, etc., of CF to other business operators, EIS operators are generally required to submit a notification plan in advance and undergo a screening process conducted by the competent authorities. This measure ensures a proactive approach to cybersecurity, aligning with the overarching goals of ESPA.

- **Definition of "maintenance, etc.":** Any maintenance, management, or operation that is critical for maintaining functions of CF or for the stable provision of EIS concerning CF in a stable manner, and that is likely to be used as a means of sabotage.

The outlined System under ESPA establishes a comprehensive framework to fortify the cybersecurity posture of CF, safeguarding against external threats and disruptions to EIS.

(ii) Outline of the Prior Screening Process in the System for Ensuring Provision of Essential Infrastructure Services Under the Economic Security Promotion Act

Please see below a brief outline of the prior screening process mentioned above:

- **Prior Notification Plan:**

  - **Installation:**
    - The Prior Notification Plan must include a summary of critical facilities, including content, timing of installation, suppliers, components, etc.; and
    - Measures which will be implemented for managing risks related to installation.

  - **Entrustment of Maintenance, etc.:**
    - In addition, it must set forth a summary of critical facilities, including content, timing of entrustment, contractors, subcontractors, etc.; and
    - Measures which will be implemented for managing risks related to the entrustment of maintenance, etc.

- **Measures for Risk Management:**

  - The EIS operator is required to report the measures taken to prevent interference with CF in both types of notifications.
  - Specific examples of measures are outlined in the System's guidance.

[14] For example, the Japanese Financial Services Agency has publicly disclosed its guidance relating to the CF in the following website.
https://www.fsa.go.jp/news/r5/economicsecurity/infra_kaisetsu_financesector.pdf

[15] For example, the Japanese Financial Services Agency has publicly disclosed the designation of the EIS operators in the financial services in the following website.
https://www.fsa.go.jp/news/r5/economicsecurity/tokuteishakaikiban.pdf

- **Examples of Detailed Measures for Risk Management:**

Among other things, detailed measures for the supply chain risk management against cyber threats include the following:

  - **For Installation:**
    - Implementing necessary controls to prevent unauthorized changes to the CF and their components during manufacturing by suppliers. A contract should stipulate the EIS operator's right to verify these controls.
    - Adoption of a system to identify signs of unauthorized disruption of the CF and their components, as a result of which the provision of EIS can be maintained.

  - **For Entrustment of Maintenance, etc.:**
    - Implementation of necessary controls to prevent unauthorized changes to the CF by the entrusted party (including the re-entrusted party). A contract should allow the EIS operator to verify such controls.
    - In the case of re-entrustment, a contract should stipulate the provision of information for cybersecurity checks and approval by the EIS operator.

- **Flexibility in Implementation:**

  - The Japanese government acknowledges that measures should be determined based on the nature and degree of risk associated with the business.
  - EIS operators are not obliged to implement all listed measures; they can choose substantially equivalent measures and select relevant items accordingly.
  - The focus is on achieving the intended cybersecurity goals, allowing flexibility in implementation based on individual circumstances.

- **Screening Period:**

  - The relevant competent authority will review the content of the prior notification.
  - As a general rule, the screening period is within 30 days from the receipt of the plan by the competent authority. This period could be extended to 4 months at most, depending on the plan-dependent degree necessary scrutiny.

- **Recommendations/Orders:**

Following review, the competent authority will take one of the following actions:

  - **High Risk Determination:**
    - If the relevant authority determines that the CF poses a high risk of its being misused to disrupt the stable provision of EIS, a recommendation will be made for necessary measures to prevent actions disruptive to the EIS operator. If the relevant authority determines that there is not a high risk of such misuse, no recommendation will be issued.

  - **EIS Operator's Response:**
    - The EIS operator is required to respond to the relevant authority within 10 days from the receipt of the recommendation, indicating whether or not it will accept the proposed measures.

  - **Orders in the Absence of Response or Rejection:**
    - If there is no response from the EIS operator within the specified period, or if the EIS operator explicitly notifies the relevant authority that it does not accept the

recommendation (unless there are legitimate grounds for such refusal), the competent authority may proceed to issue orders for the implementation of the recommended measures.

This outlined process ensures that EIS operators actively engage in risk management and cybersecurity measures, fostering a collaborative effort with competent authorities to protect the CF from external threats.

In addition, this structured process may have an effect on the suppliers and vendors of EIS operators, since there is a possibility that they would not be able to carry out transactions with EIS operators due to the recommendation by the relevant authorities. Therefore, under the System, while EIS operators are generally required to ensure to the supply chain risk management against cyber threats and make an appropriate prior notification to the competent authorities, the suppliers and vendors of the EIS operators are effectively obligated to cooperate with EIS operators in order to timely complete the screening process. The System therefore also has an indirect impact on both domestic and foreign EIS operator vendors and suppliers.

[Author]

Yasushi Kudo, Partner
yasushi_kudo@noandt.com
Yasushi Kudo is a partner at Nagashima Ohno & Tsunematsu. He mainly focuses on crisis management, including dealings with domestic and international authorities, regulatory compliance, cybersecurity/data privacy and advice on compliance systems and corporate governance, leveraging his expertise and experience gained from his secondment to the Financial Services Agency and the Securities and Exchange Surveillance Commission.
Recently, he has focused on legal issues raised by cybersecurity incidents such as ransomware attack, data compromise and business e-mail compromise (BEC) and the development of internal control system in response to cybersecurity risks such as the supply chain risk management.

NAGASHIMA OHNO & TSUNEMATSU

www.noandt.com

JP Tower, 2-7-2 Marunouchi, Chiyoda-ku, Tokyo 100-7036, Japan
Tel: +81-3-6889-7000 (general) Fax: +81-3-6889-8000 (general) Email: info@noandt.com

Nagashima Ohno & Tsunematsu, based in Tokyo, Japan, is widely recognized as a leading law firm and one of the foremost providers of international and commercial legal services. The firm's overseas network includes locations in New York, Singapore, Bangkok, Ho Chi Minh City, Hanoi, Jakarta* and Shanghai. The firm also maintains collaborative relationships with prominent local law firms. The approximately 600 lawyers of the firm, including about 50 experienced lawyers from various jurisdictions outside Japan, work together in customized teams to provide clients with the expertise and experience specifically required for each client matter. (*Associate office)

If you would like to receive future editions of the NO&T Japan Legal Update by email directly to your Inbox, please fill out our newsletter subscription form at the following link: https://www.noandt.com/en/newsletters/nl_japan_legal_update/
Should you have any questions about this newsletter, please contact us at <japan-legal-update@noandt.com>.
Please note that other information related to our firm may be also sent to the email address provided by you when subscribing to the NO&T Japan Legal Update.