2019年12月9日

国際仲裁・調停におけるサイバーセキュリティ

髙取　芳宏　弁護士（日本・米国ニューヨーク州）
日本仲裁人協会常務理事
英国仲裁人協会上級仲裁人（ F.C.I.Arb. ）

一色　和郎　弁護士（日本）

国際仲裁・調停におけるサイバーセキュリティの必要性・重要性・トレンド

- 近年のサイバーセキュリティに対する意識の高まりを受けて、国際仲裁・調停におけるサイバーセキュリティが議論されている。
- 特に国際仲裁・調停においては、センシティブな情報を含むデータがオンラインにてやり取りされることも多く、これらデータをサイバーアタック等から保護することは、経済的な損失を免れるという観点のみならず、仲裁・調停への信頼確保の観点からも重要であると考えられてきた。
- 日本においても、日本国際紛争解決センター（Japan International Dispute Resolution Center（JIDRC））や京都国際調停センター（Japan International Mediation Center in Kyoto（JIMC-Kyoto））、東京国際知的財産仲裁センター（IACT）の設立に示されるように、国際仲裁・調停の重要性が高まっており、これら手続におけるサイバーセキュリティ対策は重要な課題である。

国際仲裁・調停におけるサイバーセキュリティの必要性・重要性・トレンド（続）

- ICSIDの依頼により、2018年9月にパリの世界銀行にて、以下のトピックを含む「Cybersecurity in International ADR – Considering new trends in Japan and Cross-Asia」についてセミナーを行った：

1. Situation and Trends in Japan, and Cross-Asia
   - JIDRCやJIMC-Kyotoの設立に示される日本での国際仲裁・調停の高まり等。
2. Cybersecurity situation in Japan and Cross-Asia
   - 日本政府によるサイバーセキュリティに関するガイドライン等。
3. Technology and Legal Aspect, including Cross-Asia issues
   - 国際仲裁・調停関係者に生じ得る様々な責任等。

国際仲裁・調停におけるサイバーセキュリティの必要性・重要性・トレンド（続）

- International Council for Commercial Arbitration（ICCA）、New York City Bar Association及びInternational Institute for Conflict Prevention & Resolution（CPR）がWorking Groupを設立し、国際仲裁におけるサイバーセキュリティ対策を協議してきた。
- 2019年11月21日、Working Groupは「ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration (2020 Edition)」（Protocol）を公表。https://www.arbitration-icca.org/projects/Cybersecurity-in-International-Arbitration.html
- 同Protocolは、国際仲裁の当事者、代理人、仲裁人及び仲裁機関に対して、適切なサイバーセキュリティに関するガイダンスを示すことを目的とする。

2020 Cybersecurity Protocolの構成

- Protocolは、Principle 1-14の全14条、Schedule A-Fにて構成される。
- Principle 1-4は、Protocolのスコープ・適用について規定。
- Principle 5は、個別の案件における情報セキュリティにつき、合理的な措置が採用されるべき旨を規定。
- Principle 6-8は、個別の案件における情報セキュリティ措置に関する考慮要素を規定。
- Principle 9-13は、情報セキュリティに関するイシューにつき、推奨される手続的ステップを規定。
- Principle 14は、Protocolが何らかの責任を生じさせる根拠となるものでない旨を規定。

Principle 1

- *The Cybersecurity Protocol provides a recommended framework to guide tribunals, parties, and administering institutions in their consideration of what information security measures are reasonable to apply to a particular arbitration matter.*

Principle 2

- *As a threshold matter, each party, arbitrator, and administering institution should consider the baseline information security practices that are addressed in Schedule A and the impact of their own information security practices on the arbitration. Effective information security in a particular arbitration requires all custodians of arbitration-related information to adopt reasonable information security practices.*
- 当事者、仲裁人及び仲裁機関がそれぞれSchedule Aに定めるbaseline information security practicesを採用すべき旨を規定。
- Schedule AにてBaseline Security Measures Checklistが定められている。

Schedule A（Baseline Security Measures Checklist）

- 以下に一部を列挙：
- Knowledge and Education
  - Keep abreast of security threats and solutions
  - Consider professional obligations relating to cybersecurity
  - Consider industry standards and governmental regulations
- Asset Management
  - Know assets and infrastructure
  - Identify sensitive data and take steps to minimize and protect it
  - Avoid unnecessary multiple copies of documents
  - Establish document retention and destruction practices
  - Enable remote location tracking and data wiping functions
  - Minimize access to sensitive data while traveling
  - Back-up data

Principle 3

- *Parties, arbitrators, and administering institutions should ensure that all persons directly or indirectly involved in an arbitration on their behalf are aware of, and follow, any information security measures adopted in a proceeding, as well as the potential impact of any security incidents.*
- 仲裁手続に関わる全当事者が情報セキュリティ措置を採用する重要性を規定。

Principle 4

- *The Protocol does not supersede applicable law, arbitration rules, professional or ethical obligations, or other binding obligations.*

Principle 5

- *Subject to Principle 4, the information security measures adopted for the arbitration shall be those that are reasonable in the circumstances of the case as considered in Principles 6-8.*
- 個別の案件における情報セキュリティにつき、Principles 6-8を踏まえ合理的な措置が採用されるべき旨を規定。

Principle 6

- *In determining which specific information security measures are reasonable for a particular arbitration, the parties and the tribunal should consider:*
  - *a) the risk profile of the arbitration, taking into account the factors set forth in Schedule B;*
  - *b) the existing information security practices, infrastructure, and capabilities of the parties, arbitrators, and any administering institution, and the extent to which those practices address the categories of information security measures referenced in Principle 7;*
  - *c) the burden, costs, and the relative resources of the parties, arbitrators, and any administering institution;*
  - *d) proportionality relative to the size, value, and risk profile of the dispute; and*
  - *e) the efficiency of the arbitral process.*

Schedule B（Arbitral Information Security Risk Factors）

- Schedule Bは以下を含むArbitral Information Security Risk Factorsを規定。
  I. Nature of the Information Risks Relating to the Subject Matter of the Arbitration or the Identity of Parties, Key Witnesses, Other Participants (Including Arbitral Institution and Experts)
  II. Other Factors Impacting the Cybersecurity Risk Profile of an Arbitration
  III. Consequences of a Potential Breach

Principle 7

- *In considering the specific information security measures to be applied in an arbitration, consideration should be given to the following categories:*

  (a) asset management;

  (b) access controls;

  (c) encryption;

  (d) communications security;

  (e) physical and environmental security;

  (f) operations security; and

  (g) information security incident management.

- Schedule Cにて情報セキュリティ措置が例示

Principle 8

- *In some cases, it may be reasonable to tailor the information security measures applied to the arbitration to the risks present in different aspects of the arbitration, which may include:*

(a) information exchanges and transmission of arbitration-related information;

(b) storage of arbitration-related information;

(c) travel;

(d) hearings and conferences; and/or

(e) post-arbitration retention and destruction policies.

- 場面に応じた情報セキュリティ措置に関する規定。

Principle 9

- *Taking into consideration the factors outlined in Principles 6-8 as appropriate, the parties should attempt in the first instance to agree on reasonable information security measures.*
- 情報セキュリティに関しても、まずは当事者自治が重要である旨を規定。

Principle 10

- *Information security should be raised as early as practicable in the arbitration, which ordinarily will not be later than the first case management conference.*
- Schedule Dにて、仲裁条項においてセキュリティ措置を採用する際の文言等が提示されている：
  - *The Parties shall take reasonable measures to protect the security of the information processed in relation to the arbitration, taking into consideration, as appropriate, the ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration.*

Principle 11

- *Taking into consideration Principles 4-9 as appropriate, the arbitral tribunal has the authority to determine the information security measures applicable to the arbitration.*
- 当事者自治（Principle 9）を踏まえ、最終的には仲裁廷が情報セキュリティ措置について決定権を有する旨を規定。
- 例えば、第三者の利益を保護するために必要がある場合等においては、仲裁廷は当事者が合意した情報セキュリティ措置に拘束されない。
- 一般的には、仲裁廷は情報セキュリティ措置に関する決定をProcedural Orderにて示すことが期待される。Procedural Orderにて採用され得る文言はSchedule Dにて例示されている。

Principle 12

- *The arbitral tribunal may modify the measures previously established for the arbitration, at the request of any party or on the tribunal's own initiative, in light of the evolving circumstances of the case.*

Principle 13

- *In the event of a breach of the information security measures adopted for an arbitration proceeding or the occurrence of an information security incident, the arbitral tribunal may, in its discretion: (a) allocate related costs among the parties; and/or (b) impose sanctions on the parties.*

Principle 14

- *The Protocol does not establish any liability or any liability standard for any purpose, including, but not limited to, legal or regulatory purposes, liability in contract, professional malpractice, or negligence.*

今後の展望

- 国際仲裁・調停におけるサイバーセキュリティ対策の必要性・重要性は今後も高まることが予想される。
- JAAとしても、仲裁人のトレーニングにおける項目に追加するなど、積極的な対応が望まれる。
- また、国際仲裁・調停の実務家としても、Transactional Lawyerとの連携を含め、国際仲裁・調停におけるProtocolの採用等を広めたい。