ANDERSON MŌRI & TOMOTSUNE

### **AMT Newsletter**

December 2020

# Japanese Law Issues Relating to E-contracts and E-signatures – Admissibility of Evidence in Respect of E-contracts Executed between Companies

<u>Kenji Miyagawa</u> / <u>Yoshiyuki Nishi</u> / <u>Shogo Tsuji</u> / <u>Ryosuke Mochizuki</u> / Kenta Ichien

Despite strong demand for the use of e-signatures as a result of the COVID-19 pandemic, Japanese companies are still hesitant to use e-signatures due to the widespread practice of using physical seals in Japan. In order to resolve the uncertainties surrounding the use of e-signatures, certain solutions have been provided based on Q&As which have been published by the Japanese government in 2020. Furthermore, the switch from using seals to e-signatures has now been recognized as an important driver for the digital transformation (DX) of the Japanese economy, and both the public and private sectors in Japan now share the view that such DX must be completed as soon as possible. On the other hand, companies face various practical issues when switching from using seals to e-signatures. Accordingly, this newsletter will analyze (a) the admissibility of evidence in respect of e-contracts executed by e-signatures, (b) practical tips in respect of the execution of e-contracts between companies, and (c) certain outstanding issues in respect of converting paper contracts to e-contracts.

### 1. Admissibility of evidence in respect of e-contracts

Due to the COVID-19 pandemic in 2020, discussions have been accelerated in order to push for a switch from using paper contracts to using e-contracts instead. Such discussions are mainly driven by the Council for Regulatory Reform (the "Regulatory Reform Council") which was established in the Cabinet Office headed by the Prime Minister of Japan. Three main Q&As have been published by the relevant ministries in order to support the admissibility of evidence in respect of e-contracts, including the applicability of Article 3 of the Act on Electronic Signatures and Certification Business which came into effect on April 1, 2001 (the "E-signature Act"), which sets out certain presumptions in respect of the authenticity of e-contracts.

As can be seen in Section 2 below, there are various ways to prove the validity of contracts executed between companies, and one such way of executing a contract is by either affixing a seal on a paper contract or affixing an e-signature on an e-contract. However, based on the theory of the "two-stage presumption" (*nidan-no-suitei*) (as explained in (1)(a) below), contracts among Japanese companies are commonly executed by affixing the registered seal of each contract party to the contract. Through this method, each party is able to verify the due execution of such contract by checking (i) the seal impression of the other party which appears on the contract, and (ii) the seal impression which appears on the certificate of the other party's registered seal (*inkan-toroku-shomeisho*) which is issued by the Legal Affairs Bureau (*houmu-kyoku*).

In order to make the shift from paper contracts to e-contracts, it is ideal to have the same or similar level of admissibility of evidence in respect of e-contracts as compared to that of paper contracts that are executed by affixing seals. In this context, we set out our analysis regarding the admissibility of evidence in respect of e-contracts in this Section 1 based on the interpretations suggested in the three main Q&As issued by the relevant ministries.

- (1) Importance of discussions relating to admissibility of evidence in respect of e-contracts
- (a) What does "admissibility of evidence" mean?

  Admissibility of evidence under the Code of Civil Procedure is divided into two categories, i.e., (i) admissibility as to formality (*keishikiteki-shokoryoku*), and (ii) admissibility as to substance (*jisshitsuteki-shokoryoku*).
  - (i) Admissibility as to formality (keishikiteki-shokoryoku) means admissibility of evidence in respect of whether a document has been duly executed by its signatory. This issue is the first test which needs to be verified prior to the second test below in order for such document to be admissible as evidence under the Civil Procedure Code.
  - (ii) Admissibility as to substance (*jisshitsuteki-shokoryoku*) means admissibility of evidence in respect of whether and to what extent such document is admissible as evidence in order to prove certain facts (e.g., a contract has been duly executed by the parties). This issue is the second test which needs to be evaluated after the first test has been verified (e.g., whether or not the court decides that certain facts have been proven by the contents of the document if there are other evidences which are inconsistent with such document).
- (b) Two-stage presumption (*nidan-no-suitei*)
  - Article 228(4) of the Code of Civil Procedure provides that "a contract between private parties shall be presumed to be duly executed if there is a signature or a seal by the party (or its agent) on such contract". It is generally considered that such article sets out the rules in respect of admissibility as to formality (keishikiteki-shokoryoku) only.
  - The so-called theory of "two-stage presumption" (*nidan-no-suitei*) has been established under Article 228(4) of the Code of Civil Procedure and can be summarized as follows:
  - (i) the first-stage presumption: a seal is deemed to be affixed by a party if the seal impression (*in'ei*) of the seal of such party appears on a contract, which is a de-facto presumption that has

- been established by court precedents; and
- (ii) the second-stage presumption: a contract shall be presumed to be duly executed if there is a seal affixed by the party on such contract, which is a presumption provided by Article 228(4) of the Code of Civil Procedure.

### (c) E-contracts

The analysis in (1)(a) above essentially applies to e-contracts as well. In other words, e-contracts cannot be admissible as evidence if the admissibility as to formality is denied (even before the court can examine the admissibility as to substance). In addition, e-contracts may not be admissible as evidence in order to prove certain facts if there are other evidences which are inconsistent with such e-contracts (i.e., the lack of admissibility as to substance). As such, it is important for e-contracts to meet the criteria for both admissibility as to formality and admissibility as to substance. Article 3 of the E-signature Act sets out the rules in respect of admissibility as to formality (*keishikiteki-shokoryoku*) which is equivalent to Article 228(4) of the Code of Civil Procedure. Therefore, it would be ideal that Article 3 of the E-signature Act apply to e-contracts in order to secure the admissibility as to formality of such e-contracts.

- (d) Types of e-signatures under Japanese law
  - There are various types of e-signatures which are currently used in Japan. Although there are no statutory definitions for each type, such e-signatures can be categorized as follows:
  - (i) E-signatures managed by users themselves locally ("Local/Contract Party Type E-signatures"): These are e-signatures whereby secret keys (himitsukagi), etc. in respect of e-signatures encrypted by public key infrastructure (PKI) technology are held in integrated circuit cards or users' computers, and the e-signatures are attached to the e-contracts by the users themselves locally by using such secret keys. There e-signatures are encrypted by using secret keys assigned to the users of such e-signatures (i.e., the contract party).
  - (ii) E-signatures managed remotely ("Remote/Contract Party Type E-signatures"): These are e-signatures which are managed by e-signature service providers on cloud computing servers (i.e., managed remotely by users). There are e-signatures which are encrypted by using secret keys assigned to the users of such e-signatures (i.e., the contract party).
  - (iii) Third Party Type E-signatures (*jigyoshagata-denshishomei*): These are e-signatures which are encrypted by using secret keys assigned to the Other E-signature Service Provider in accordance with the instructions given by the contract party. The Article 2 Q&A and Article 3 Q&A (as explained in (3) and (4) below) both set out analyses of the admissibility of evidence in respect of these Third Party Type E-signatures.

Based on the above, we have analyzed the admissibility of evidence in respect of e-signatures by reviewing the three major Q&As published by the relevant government ministries in 2020.

#### (2) Q&A related to affixing seals

On June 19, 2020, the Ministry of Justice and other ministries published the Q&A related to affixing seals ("Seal Q&A"). The Seal Q&A can be summarized into two major points below.

(a) The legal effect of affixing seals is limited. In other words, it was believed that the burden of proof

- was lightened based on the "two-stage presumption" (as set out in (1)(b) above) if a seal was affixed to a paper contract. However, the Seal Q&A explains that the burden of proof may not necessarily be substantially lightened simply by affixing seals to paper contracts.
- (b) There are many ways to prove the due execution of contracts which are executed in the form of either paper contracts or e-contracts. In other words, the due execution of contracts can be proven through a combination of various ways, including by reviewing the know your customer ("KYC") information of the other contract party prior to the execution of the contracts, the e-mail correspondence in respect of the contract negotiations between the contract parties and/or the use of e-signatures when the contracts were executed in an electronic form.

The two points above will enhance the approach set out in Section 2 below where the contract parties are encouraged to prepare for the possibility of having to prove the due execution of contracts by keeping various evidences relating to the facts during three stages, namely the pre-contract, upon-contract and post-contract stages.

(3) Q&A related to Article 2 of the E-signature Act

Under Article 2(1) of the E-signature Act, an "E-signature" is defined as "an e-signature affixed on electronic data (i.e., data or information which are recorded in an electronic form) which satisfies the two requirements as set out below":

- (i) the e-signature is affixed on certain electronic data (e.g., an e-contract) (the "E-data") in order to express that the E-data was made by the person who has affixed such e-signature; and
- (ii) it can be verified that the contents of the E-data have not been modified after such e-signature was affixed.

It is generally considered that the scope of e-signatures to which Article 2 of the E-signature Act applies ("Article 2 E-signatures") are wider than the scope of e-signatures to which Article 3 of the E-signature Act applies ("Article 3 E-signatures"). On the other hand, it was previously unclear whether Article 2 of the E-signature Act would apply to Third Party Type E-signatures.

In this regard, on July 17, 2020, the Ministry of Justice and other ministries published the Q&A related to Article 2 of the E-signature Act ("Article 2 Q&A") to resolve the above issue. The Article 2 Q&A can be summarized into two major points below.

- (a) In respect of Third Party Type E-signatures, e-signatures are encrypted by using the secret keys of the e-signature service provider (which is not the party to the contract) rather than the secret keys of the party to the contract. As such, the question arose as to whether the contract party would fall under the scope of "the person who has affixed such e-signature" as set out in Article 2(1)(i) of the E-signature Act. In this regard, the Article 2 Q&A explains that the contract party can be deemed to be "the person who has affixed such e-signature" if the e-signature service provider has attached the e-signatures by using their secret keys where such e-signatures are automatically attached to the e-contracts in accordance with the instructions of the contract party without the discretion of the e-signature service provider.
- (b) The procedure for attaching e-signatures in respect of Third Party Type E-signatures can be divided into two stages, i.e., (i) the first stage where the contract party gives the instruction to the e-signature

service provider and (ii) the second stage where the e-signature service provider executes the e-contract by affixing the e-signature using the secret keys of such e-signature service provider in accordance with the instruction given by the contract party. The above two-stage processes can be considered as a single process of affixing an e-signature of the contract party where the intention of the contract party can be verified by information ancillary to the executed e-contracts (including information relating to the instruction which was actually made by the contract party).

Based on the above, it is now clear that Article 2 of the E-signature Act applies to Third Party Type E-signatures in cases where (i) any modification of the executed version of the e-contract is prohibited by encrypting it by using the secret keys of the e-signature service provider and (ii) the e-signature is affixed to the e-contract solely in accordance with the intention of the contract party without being affected by the intention or discretion of the e-signature service provider.

It should be noted that Article 2 E-signatures are actually referred to in other statutory provisions in Japan. For example, copies of board minutes need to be attached to applications for amendments to a company's commercial registration, and such board minutes can be submitted to the Legal Affairs Bureau in an electronic form if such board minutes are executed by the relevant directors by attaching certain e-signatures which are designated by the Minister of Justice. As such, it is now clear that Third Party Type E-signatures designated by the Minister of Justice can be used to execute board minutes which are to be used as attachments to commercial registration applications.

However, it was still unclear whether or not the second stage presumption (i.e., the presumption of due execution under Article 3 of the E-signature Act) would apply to Third Party Type E-signatures. Therefore, the Article 3 Q&A (as defined below) was published in order to resolve the aforesaid issue.

- (4) Q&A related to Article 3 of the E-signature Act
- (a) Overview

On September 4, 2020, the Ministry of Justice and other related ministries published the Q&A related to Article 3 of the E-signature Act ("Article 3 Q&A"). The summary of the Article 3 Q&A is as set out below.

Article 3 of the E-signature Act sets out that "e-contracts are presumed to be duly executed if an e-signature is affixed on such e-contract by the intention of the signatory (provided that, such e-signature is limited to those which can be affixed only by the signatory by proper management of required encryption and devices)". In respect of the phrase "which can be affixed only by the signatory", the Article 3 Q&A requires that the requirements of "uniqueness (koyu-sei)" must be satisfied in addition to the requirements set out in Article 2 of the E-signature Act.

The requirements of "uniqueness (*koyu-sei*)" mean that "any third party is unable to make an encryption which is identical to that used by a signatory when such signatory affixes an e-signature".

Furthermore, the requirements of "uniqueness (*koyu-sei*)" must be satisfied in respect of each of the following two processes:

- (i) the process between the e-signature user and the e-signature service provider; and
- (ii) the e-signature service provider's internal process.

There are currently no court precedents that set out the requirements of "uniqueness (*koyu-sei*)". However, generally speaking, the requirements of "uniqueness (*koyu-sei*)" can be satisfied if the following elements are present:

- (i) the signatory is verified by two-factor authentication (*nihoso-ninsho*) (e.g., authentication by (a) a registered e-mail address and log-in password and (b) a one-time password which is circulated to the signatory by a mobile phone SMS or a token); and
- (ii) the e-signature service provider affixes the e-signature of the signatory only if the e-signature service provider receives the instruction from such signatory (whose authentication is verified by step (i) above.

### (b) Confirmation on the identity of the signatory

The Article 3 Q&A explains the details of the uniqueness requirements in Q1, Q2 and Q3, and the importance of conducting "background checks (*mimoto-kakunin*)" in Q4. According to the "report concerning person identification procedures in respect of online services" published by the Ministry of Economy, Trade and Industry on April 17, 2020, confirmation on the identity of the signatory can be divided into (a) background checks (*mimoto-kakunin*) and (b) authentication (*tonin-ninsho*), each of which means as follows:

- Background check (mimoto-kakunin) means "to verify that the name, address and date of birth of a person (which are registered) are accurate."
- Authentication (tonin-ninsho) means "to verify that a certain person is actually the one acting by checking any or all three of the following factors: (i) biometrics (e.g., face or finger print), (ii) possession (e.g., possessing certain types of ID such as My Number Card¹) and/or (iii) knowledge (e.g., password which is created by the signatory and known to the signatory only).

In respect of the authentication (*tonin-ninsho*) above, it can be verified by two-factor authentication (*nihoso-ninsho*) as mentioned above. In addition, as mentioned above, whether a "background check (*mimoto-kakunin*)" is required in addition to such authentication has been subject to discussions among practitioners. Although Q4 of the Article 3 Q&A refers to the importance of "background checks (*mimoto-kakunin*)" in the context of the choice of an appropriate e-signature service provider, Q1 and Q2 of the Article 3 Q&A do not refer to "background checks (*mimoto-kakunin*)" in the discussions relating to the requirements of "uniqueness (*koyu-sei*)". Therefore, it is reasonable to consider that the Article 3 Q&A does not require the conduct of a "background check (*mimoto-kakunin*)" as one of the conditions to enjoy the benefit of Article 3 of the E-signature Act. This interpretation is confirmed by the confirmation paper which was issued by the Ministry of Justice and the other relevant ministries and provided to the meeting of the "Digital Government Working Group" (which is one of the working groups formed by the Regulatory Reform Council) held on 17 November 2020.

The above discussion relates to the recent discussions on how to take actions against cyber security

<sup>&</sup>lt;sup>1</sup> A "My Number Card" is a card with a 12-digit identification number that is issued by the Japanese government to citizens and residents of Japan

incidents. Please refer to Section 3(1) below for further details on the same.

### (5) Two-stage presumption and admissibility of evidence in respect of e-contracts

Based on the discussions above, the two-stage presumption can be applied to e-contracts as well. Please refer to the table below which compares the applicability of the two-stage presumption in respect of paper based contracts and e-contracts.

	Paper contracts executed by affixing a seal (in cases where Article 228(4) of the Code of Civil Procedure applies)	E-contracts executed by affixing e-signatures (in cases where a Third Party Type e-signature is affixed and Article 3 of the E-signature Act applies)
The first- stage presumption	A seal is deemed to be affixed by a party if the seal impression (in'ei) of the seal of such party appears on a contract, which is a de-facto presumption that has been established by court precedents.	Subject to the judgement of the court in any future court cases, an e-signature can be deemed to be affixed by the signatory of such e-signature if such e-signature appears on an e-contract and such e-signature can be affixed by the signatory only after verification by two-factor authentication.
The second- stage presumption	A contract shall be presumed to be duly executed if there is a seal affixed by the party on such contract, which is a presumption provided by Article 228(4) of the Code of Civil Procedure.	An e-contract shall be presumed to be duly executed if there is an e-signature affixed by the party on such contract, which is a presumption provided by Article 3 of the E-signature Act.

The discussions relating to admissibility as to formality (*keishikiteki-shokoryoku*) have become clearer due to the Article 3 Q&A and the discussions between practitioners as mentioned above. However, there are other issues that should be discussed in order to ensure the validity of e-contracts executed between companies. We have analyzed such issues in Section 2 below.

# 2. Practical issues in respect of e-contracts executed between companies

As suggested by the Seal Q&A, affixing a seal or an e-signature is one of various ways to ensure that an e-contract has been duly executed. It would be practical to mitigate risks of future disputes by conducting due diligence and/or maintaining proper evidences in respect of various facts prior to and/or after execution of an e-contract.

Generally speaking, the representative director of a company is authorized to execute a contract on behalf of the company, subject to certain restrictions. Typically, the company would also register the official seal of the representative director (the "Registered Seal") with the Legal Affairs Bureau (houmu-kyoku) (which is a governmental body), the authentication of which can be verified by reviewing the certificate of the Registered Seal which is issued by the Legal Affairs Bureau. Hence, Japanese companies tend to execute certain important contracts by affixing their Registered Seals to such contracts.

On the other hand, it is burdensome for each of the contracts to be executed by affixing the Registered Seal. As such, the representative director of the company typically delegates his/her authority to certain authorized signatories of the company (e.g., the head of the legal division, the heads of certain business divisions) and such authorized signatories create certain unofficial seals (*mitome-in*) ("Unofficial Seals") which are not registered with the Legal Affairs Bureau. Hence, Japanese companies tend to execute certain less important contracts by affixing an Unofficial Seal to such contracts.

However, it is understood that Article 3 of the E-signature Act does not provide a presumption in respect of the proper authorization of the representative director and/or the authorized signatories. Hence, checks should be conducted to ensure that the representative director and/or the authorized signatories have been properly authorized, in addition to the other issues related to Article 3 of the E-signature Act.

Envisioning a scenario where Companies X and Y (both of which are Japanese companies) execute an e-contract (governed by Japanese law), we have set out below our analysis on certain practical issues in respect of the execution of e-contracts between companies. Please note, however, that it is not necessary to verify each of the points below in respect of various types of contracts (e.g., some of the points can be omitted in respect of certain contracts where legal risks are not high).

- (1) Practical issues prior to execution of E-Contracts
- There are various types of e-signatures provided by various e-signature service providers. Hence, Company X needs to decide which type of e-signatures would be suitable for the e-contract it wishes to execute. In this regard, Company X needs to review the contracts executed by Company X in the past (including whether such contracts were executed by affixing the registered seal of the representative director or the seals of certain authorized signatories who are not the representative director) and categorize such contracts into a few categories depending on the legal risks relating to such contracts.
- Company X needs to check whether (a) as a general matter, Company Y can execute e-contracts by using e-signatures and (b) Company Y can execute e-contracts by using e-signatures provided by the e-signature service provider chosen by Company X. Company X then needs to decide on who will be the authorized signatories of Company Y in respect of Company Y's e-signatures. There are various choices in respect of such authorized signatories, such as (i) the representative director of Company Y, (ii) the persons from the legal/compliance divisions of Company Y who are also authorized to affix the Registered Seal of Company Y (the "Authorized Signatories (Legal/Compliance)"), or (iii) the persons from the relevant business divisions of Company Y who are also authorized to affix the UnofficialSeal of Company Y (the "Authorized Signatories (Business"). In this regard, a question that has been discussed among practitioners is whether an

e-signature can be affixed by the persons who are acting on behalf of the person who holds such e-signature account, but there is currently no official confirmation from the courts or the Japanese government regarding this. Company Y also needs to amend its internal rules on the execution of contracts so that e-contracts can be executed by any of its signatories in (i), (ii) or (iii) above.

• Generally speaking, it would be difficult for Company Y to deny the validity/due execution of a contract if the authorized persons have duly negotiated the terms of such contract with Company X. As such, it is advisable for Company X to keep records of all major correspondence (e.g., e-mails or meeting minutes) with Company Y in order to be prepared for any future litigation that may occur in respect of the validity/due execution of such contract.

### (2) Practical issues upon execution of e-contracts

- E-contracts must be executed by Company X only after (i) the execution of such contract has been duly authorized by the relevant bodies of Company Y (e.g., via a board resolution) and (ii) the authentication/authorization of the authorized person of Company Y has been duly confirmed.
- It would be useful for Company X to procure the relevant representations and warranties/covenants of Company Y in respect of Company Y's ability to duly execute contracts by way of using esignatures in an E-Contract. Since the practices in relation to E-Contracts are currently still evolving, it may be practical to execute a paper contract with Company Y first and to procure such representations and warranties/covenants of Company in such paper contract.
- Based on the Article 3 Q&A, Company X must make sure that the decision making mechanism as well as the instructions by Company Y to the e-signature service provider can be evidenced.

### (3) Practical issues after execution of e-contracts

- Company X needs to decide on how the e-contracts will be kept after they are executed (e.g., (i) whether e-contracts will be recorted in the server of the e-signature service provider and/or the server of Company X and (ii) whether certain important contracts that have been executed as e-contracts will also be kept in paper form).
- Generally speaking, it would be difficult for Company Y to deny the validity/due execution of a
  contract if Company Y has performed its obligations under such contract (e.g., post-signing/postclosing obligations, payment obligations). As such, it is advisable to keep evidence which shows
  Company Y's performance of its obligations.

# 3. Remaining issues to complete DX (including transformation from seals to e-signatures)

### (1) Issues concerning cyber security risks

Cyber security risks are currently a focus of concern due to various cyber security incidents that have occurred in Japan (e.g., fraudulent use of access IDs/passwords in respect of online payment services). As mentioned in 1(4)(b) above, a reasonable interpretation is that "background checks (*mimoto-kakunin*)" would not be required as one of the requirements under Article 3 of the E-signature Act.

However, from the view point of compliance with anti-money laundering regulations and/or regulations concerning anti-social forces, in our example scenario in 2 above, the background check issue would need to be discussed separately from the issue relating to Article 3 of the E-signature Act depending on the details of the businesses to be conducted by Company X. Generally speaking, companies need to perform their KYC procedures depending on their services and such KYC procedures can be conducted online ("e-KYC"). Also, the details of the e-signature account of the counterparties of Company X need to be carefully reviewed since the level of cyber security risks would vary depending on the cyber security measures of each of Company X's counterparties. In practice, it is advisable for Company X to start using e-signatures only with certain reliable counterparties with whom Company X has had long-term relationships.

- (2) Issues concerning e-contracts
- (a) Scope of Article 3 of the E-signature Act

Although the Article 3 Q&A has been published, the detailed requirements of Article 3 of the E-signature Act are not yet crystal clear since this issue is subject to determination by the court in the future. In the meantime, the scope of Article 3 of the E-signature Act is expected to become clearer based on discussions among practitioners and governmental agencies (e.g., which type of Third Party Type E-signatures will be allowed to be used in E-Government procedures (see (4) below)).

- (b) Use of e-signatures provided by different e-signature service providers

  There are many e-signature service providers which currently provide different forms of esignatures (e.g., Remote/Contract Party Type, Third-Party Type). It is possible that Company X may
  wish to use the e-signature service provider A and Company Y may wish to use the e-signature
  service provider B. In such a case, it would be ideal if Company X/Company Y are able to use their
  respective e-signature service providers even in respect of the same contract (i.e., Company X will
  execute the contract by using the e-signature service provider A and Company Y will execute the
- (c) Use of e-signatures in respect of an e-contract to be executed by companies located in different jurisdictions

same contract by using the e-signature service provider B to the extent possible).

A cross-border contract is typically executed by the exchange of the signature pages in PDF format. However, if the parties would like to execute a cross-border contract by using e-signatures, the validity and due execution of such e-contract would need to be carefully reviewed from a conflict of laws perspective.

- (d) Possible amendment to statutory requirements for contracts to be in "paper form"

  For example, a joint guarantee (*rentai-hosho*) must be executed "in writing", but it can be executed "in electronic form". Although there are still certain categories of contacts which must be executed "in writing" and "in paper form", such statutory requirements may need to be reviewed/amended in order to achieve complete DX.
- (3) Issues concerning DX in respect of other back office services
- (a) DX concerning invoices, etc.

A company that deals with documents which are not contracts (e.g., invoices, receipts) may have to deal with a much bigger number of such documents than the number of contracts executed by the

company. As some companies issue such invoices / receipts by affixing an Unofficial Seal of the company to them, it would be useful if companies could shift from using seals to e-signatures or e-seals in respect of such invoices / receipts.

(b) DX concerning internal corporate procedures

Another category of paperwork for a company is the preparation of various company minutes (e.g., board resolutions, shareholders' resolutions). It would be ideal if each company could prepare any and all of its internal corporate documents by using only one type of e-signature (e.g., a Third Party Type E-signature) provided by a single e-signature service provider.

- (4) Issues concerning DX in respect of the procedures with the governmental agencies / the courts
- (a) Use of e-signatures in E-Government

The Japanese government has set-up a platform called "E-Government" where various governmental procedures can be processed via online, but such E-Government is not commonly used by private sector companies due to various reasons.

The current Japanese government has been trying to complete DX both in respect of governmental procedures and contracts between private companies. The Regulatory Reform Council has been actively discussing on how to promote the use of E-Government. It would be ideal if each company could use E-Government by using only one type of e-signature (e.g., a Third Party Type E-signature) provided by a single e-signature service provider.

- (b) Use of e-signatures in various registration procedures
  - Corporate registration and real estate registration procedures are some governmental procedures which are frequently used by companies in Japan. Again, it would be ideal if each company could complete such corporate registration / real estate registration procedures by using only one type of e-signature (e.g., a Third Party Type E-signature) provided by a single e-signature service provider.
- (c) DX of civil court procedures

Under the current plan, it takes time to achieve compete DX of civil court procedures. However, it is currently possible for the companies to submit e-contracts executed by e-signatures to the court as evidence. Therefore, a delay in DX of the civil court procedures would not be an excuse of delay of achieving DX in contracts.

### 4. Final remarks

As can be seen from above, there are various practical issues in respect of the use of e-signatures in Japan. It is understandable that companies may be hesitant to convert from using seals to e-signatures in respect of important contracts/documents. If a company wishes to implement DX, we recommend that it first begins by converting from using seals to e-signatures in respect of certain categories of contracts that are subject to a lower level of legal risks, e.g., contracts with counterparties with which the company has a long-term relationship, or where the contract amount is low.

■ This newsletter is published as a general service to clients and friends and does not constitute legal advice. Should you wish to receive further information or advice, please contact the authors below.

#### Authors:

Kenji Miyagawa (kenji.miyagawa@amt-law.com)

Yoshiyuki Nishi (yoshiyuki.nishi@amt-law.com)

Shogo Tsuji (shogo.tsuji@amt-law.com)

Ryosuke Mochizuki (ryosuke.mochizuki@amt-law.com)

Kenta Ichien (kenta.ichien@amt-law.com)

- If you wish to unsubscribe from future publications, kindly contact us at General Inquiry.
- Previous issues of our newsletters are available <u>here</u>.

