ANDERSON MŌRI & TOMOTSUNE

AMT NEWSLETTER

June 2020

Japanese Law Issues Relating to E-contracts and E-signatures – Increased Use of E-signatures Due to Rise in Working from Home

Kenji Miyagawa / Ryosuke Mochizuki

Demand for the use of electronic contracts ("e-contracts") and electronic signatures ("e-signatures") has been increasing as a result of the implementation of telecommuting and work from home policies by many businesses in Japan due to the COVID-19 pandemic. On the other hand, it has been pointed out that the legal nature of e-signatures under Japanese law is not clear due to the widespread practice of using physical seals in Japan. This newsletter will analyze the current status of e-signatures under Japanese law and the issues that need to be clarified in order for e-signatures to become more widely used in business-to-business transactions in Japan.

1. General Considerations Regarding E-contracts and E-signatures under Japanese law

As a general legal principle, contracts are valid under Japanese law as long as the parties reach an agreement, regardless of whether such agreement is reached verbally, electronically, or by way of writing in a physical document (e.g. written on paper). Under such principle, contracts executed by e-signatures are generally valid under the Civil Code unless there is a specific requirement that the contract be in a certain form[1]. In that sense, a contract can be validly executed in the form of an e-contract or by way of an e-signature under the general provisions of the Civil Code.

[1] There are certain contracts which need to be "executed and delivered in writing" in order to be valid under Japanese law, such as a guarantee (*hosho*) (although please note that an e-contract is also acceptable in respect of a guarantee), a fixed term land lease agreement (*teiki-shakuchi-keiyaku*) and a fixed term building lease agreement (*teiki-tatemonochintaishaku-keiyaku*).

However, in the event that there is a dispute between the parties as to whether or not a contract has been duly executed and the matter is brought before the courts, the party asserting that the contract was duly executed will have the burden of proving that the contract was duly executed.

In this regard, Article 228, Paragraph 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*". In respect of Article 228, Paragraph 4 of the Code of Civil Procedure, the so-called theory of "two-stage presumption" (*nidanno-suitei*) has been established and companies typically execute contracts confirming that the other party has duly executed the contract based on such theory.

For example, in respect of contracts between companies that are executed by using physical seals, the theory of "two-stage presumption" involves the following:

(i) 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 (the "first-stage presumption", which is a de-facto presumption that has been established by court precedents); and

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

Based on the above theory, contracts among Japanese companies are commonly executed by affixing the registered seal of each company to the contract, after which each party checks the seal impression of the other party by reviewing the certified copy of the other party's registered seal (*inkan-shomeisho*). We discuss below how the above practice applies to a case where an e-contract is executed by way of affixing e-signatures.

2. Major Japanese Acts Relating to E-signatures

The development of Japanese legislation relating to e-signatures commenced in 2000 when the use of the internet and e-commerce became more widespread. The major Japanese legislation relating to e-signatures are as follows:

(i) The Act on Electronic Signatures and Certification Business which came into effect on April 1, 2001 (the "E-signatures Act").

(ii) The Act on the Promotion of the Use of Electronic Powers of Attorney which came into effect on January 1, 2018 (the "E-POA Act").

(iii) The E-signatures and Certification of E-signatures System under the Company Registration System, which was established under the amended Company Registration Act which came into effect on October 1, 2000 (the "2000 Amended Company Registration Act").

There are actually other Acts in addition to the ones mentioned above which deal with the use of e-signatures in certain business sectors in Japan (such as the Act Concerning Construction Business and

the Act Concerning Prevention of Delay of Payments related to Sub Construction Contracts)[2]. However, for the purposes of this newsletter, we have chosen to focus on the three major Acts set out above since this newsletter is intended to discuss the general issues relating to e-signatures that apply to all business sectors in Japan.

(1) **E-signatures Act**

The E-signatures Act provides, among other things, (a) the definition of "E-signature", (b) the presumption of due execution related to the use of E-signatures and (c) the detailed requirements relating to the E-signature verification business.

Under Article 2, Paragraph 1 of the E-signatures Act, "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.

The first requirement in (i) above means that an e-signature shall be affixed by a person on the E-data in order for such person to express that the E-data was made by them.
The second requirement in (ii) above means that an e-signature service provider needs to show that its service provides certain functions by which it can prove that the contents of the E-data have not been modified after such e-signature was affixed. Please note, however, that the E-Signatures Act does not provide details on the encryption requirements in order to allow for flexibility in terms of technological developments.

Article 3 of the E-signatures Act provides that "*Electronic data created by a particular private person shall be presumed to be duly executed by such person if the e-signature of such person is affixed by such person on such electromagnetic record*". In order for the e-signature of a person to be recognized as having been affixed by them, Article 3 of the E-signatures Act requires that "*such e-signature can be performed [only] by the signatory through appropriate management of codes and properties necessary to [affix the e-signature]* ".

As can be seen from the above, Article 3 of the E-signatures Act sets out a presumption which is similar to the second-stage presumption provided in Article 228, Paragraph 4 of the Code of Civil Procedure in respect of the "two-stage presumption" theory explained above. Having said that, Article 3 of the E-signatures Act is different from Article 228, Paragraph 4 of the Code of Civil Procedure in some aspects. Three major points are set out below.

---

[2] For example, the use of e-contracts is permitted under Article 19, Paragraph 3 of the Act Concerning Construction Business (*kenchiku-gyoho*) and Article 3, Paragraph 2 of the Act Concerning Prevention of Delay of Payments related to Sub Construction Contracts (*shitaukedaikin-shiharai-chiento-boushiho*).

(i) Authorized E-signature Service Providers and Other E-signature Service Providers

Articles 4 to 16 of the E-signatures Act provide for detailed regulations concerning e-signature service providers that are authorized by the Ministry of Justice[3] ("Authorized E-signature Service Providers").

However, in order to allow new service providers to enter the Japanese market, the above authorization is "optional" in the sense that the e-signatures provided by each of Authorized E-signature Service Providers or E-signature Service Providers other than Authorized E-signature Service Providers ("Other E-signature Service Providers") would be able to enjoy the benefit of the presumption in Article 3 of the E-signatures Act so long as the conditions specified under such Article 3 have been satisfied. Having said that, for cases where the validity of e-signatures are disputed in court, it is expected that it would be easier to satisfy the conditions specified under such Article 3 in a case where the parties had used e-signatures provided by an Authorized E-signature Service Provider (as compared to a case where the parties had used e-signatures provided by an Other E-signature Service Provider) since the detailed systems of creation and maintenance of e-signatures provided by an Authorized E-Signature Service Provider have already been authorized by the Ministry of Justice.

(ii) Relationship between Article 3 of the E-signatures Act and the two-stage presumption

As mentioned above, Article 3 of the E-signatures Act provides a presumption which is similar to the second-stage presumption provided by Article 228, Paragraph 4 of the Code of Civil Procedure. However, the first-stage presumption has not been established yet in respect of e-signatures. Accordingly, in a case where a party is arguing that a contract had been duly executed by way of e-signatures, such party has the burden of proving the first-stage presumption, i.e., that the relevant e-signature had actually been affixed by the party that is purported to have affixed the said e-signature on the contract. Please refer to the table below which summarizes the major differences between (a) execution by way of affixing a physical seal, and (b) execution by way of affixing an e-signature (please note that, in order to avoid confusion, in the table below we have excluded cases where e-signatures are affixed but where Article 3 of the E-signatures Act does not apply).

<Application of Two-stage Presumption in Cases Where Physical Seals and E-signatures are Used>

	Cases where physical seals are affixed to contracts (i.e., cases where Article 228, Paragraph 4 of the Code of Civil Procedure applies)	**Cases where e-signatures are affixed to e-contracts (i.e., cases where Article 3 of the E-signatures Act applies)**

[3] There were 10 Authorized E-signature Service Providers as of November 10, 2018 according to the list of Authorized E-signature Service Providers Service published at the Ministry of Justice's website below:
http://www.moj.go.jp/MINJI/minji32.html

The First-Stage Presumption	A seal is deemed to be affixed by one party if the seal impression (*in'ei*) of the seal of such party appears on the contract (a de-facto presumption established by court precedents).	It is understood that a de-facto presumption would generally not apply to e-signatures. Hence, if one of the parties to a contract denies that it had duly executed the e-contract by way of e-signature (the "defendant") and the case is brought to court by the disputing party (the "plaintiff"), the plaintiff would need to prove that the e-signature purported to have been affixed to the e-contact by the defendant had actually been affixed to the e-contract by providing various types of evidence, such as an e-certificate relating to the e-signature and records of transaction logs which show the access and approval logs of the defendant.
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 (a presumption provided by Article 228, Paragraph 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 e-contract (a presumption provided by Article 3 of the E-signatures Act).

(iii) Proving Due Execution of E-Contracts under the Principle of Free Evaluation of Evidence

Even if Article 3 of the E-signatures Act does not apply to certain e-signatures, it does not mean that the e-contracts on which such e-signatures are affixed would be invalid and unenforceable. Under the Code of Civil Procedure, the court has a wide discretion to determine the authenticity of certain contracts (i.e., the Principle of Free Evaluation of Evidence (*jiyu-shinsho-shugi*)). The party arguing due execution of a particular contract would be able to prove that the e-contract had actually been duly executed by the authorized representative of the other party who affixed the e-signature (i.e. the signatory) by arguing/proving various facts, such as by providing a record of access times showing when the signatory actually accessed the e-contract, correspondence with the signatory in respect of such contract, how the e-signature service provider confirmed that the person accessing the e-contract was actually the signatory, and any technical details as to how the e-signature service was designed to prevent any misuse of such e-signature, although the court has the discretion to decide whether or not it accepts the party's argument based on such evidence provided.

In addition to the above three points, it should be noted that Authorized E-signature Service Providers are able to issue an e-signature certificate certifying that a particular e-signature is actually the e-signature of that particular person, but Authorized E-signature Service Providers are unable to certify in an e-signature certificate the authority or the position of such person (e.g., that the person is a member of the Legal Department of Company X). Please refer to Section 3 for further details.

(2) **E-POA Act**

The E-POA Act provides, among other things, the definition of "E-POA" and the optional registration system under which certain E-POA Service Providers may be registered with the Ministry of Justice (which is similar to the system of Authorized E-signature Service Providers under the E-signatures Act).

As explained above, although Authorized E-signature Service Providers are entitled to certify that a particular e-signature is the e-signature of a particular person, they are not entitled to certify that such person is authorized by the representative director of the company. However, by issuing an E-POA under the E-POA Act, it is possible to prove in an electric form only that such person is duly authorized by the representative director of the company.

The E-POA Act provides for different forms of an E-POA. Among others, in respect of an E-POA which is in the form of an electronic certificate ("e-certificate"), it is possible to describe "the title and authority of the person who affixes the e-signature for and on behalf of the company" in the e-certificate so that the e-certificate can certify the authorization of such person in respect of the execution of a particular e-contract. Although there is no specific provision in the E-POA Act which provides for a presumption similar to those under Article 3 of the E-signatures Act, the authenticity of the E-POAs issued by Authorized E-POA Service Providers is secure since Authorized E-POA Service Providers are obliged to verify that a particular E-POA has actually been issued by the representative director of that particular company and such E-POA has not been modified after it has been issued.

(3) **E-signatures under the 2000 Amended Company Registration Act**

Under the 2000 Amended Company Registration Act, the legal affairs bureau is expected to be able to (a) verify the authenticity of a particular e-signature (a "LAB e-signature") that is registered with the legal affairs bureau as an e-signature of the representative director of a particular company, and (b) issue an e-certificate in which the legal affairs bureau certifies the existence of that company, the authority of that representative director of that company, and the authenticity of the LAB e-signature of that representative director.

Under the 2000 Amended Company Registration Act, the existence of a particular company and the authority of the representative director of that company can be verified by the following process:

(i) The company (or its representative director) registers the LAB e-signature as well as the information required to read such e-signature with the legal affairs bureau.

(ii) The company executes a particular e-contract by affixing a LAB e-signature.

(iii) The company requests the legal affairs bureau to issue an e-certificate which contains the information required to read the LAB e-signature and the company delivers such e-certificate to the counterparty of the e-contract.

(iv) The counterparty confirms with the legal affairs bureau that the e-contract has actually been executed by way of the company's registered LAB e-signature.

The 2000 Amended Company Registration Act is designed to provide a registered LAB e-signature and an e-certificate of such registered LAB e-signature which are equivalent to a registered seal and the certificate for that registered seal. As such, if LAB e-signatures become widely used by Japanese companies, it can be said that the current practice of relying on a registered seal and a certificate of registered seal may be replaced by using LAB e-signatures/e-certificates. Please note, however, that LAB e-signatures/e-certificates can be issued in the name of the representative director or the manager (*shihai-nin*) of the company only (hence, it cannot be issued in the name of any other employees of the company).

(4) **Contents of e-certificate under the relevant laws**

As discussed above, since Article 3 of the E-signatures Act requires that "the *e-signature of [a particular] person is affixed by such person*", using an e-certificate to prove such fact is generally considered to be effective.

(i) E-certificate issued by the legal affairs bureau under the 2000 Amended Company Registration Act

An e-certificate issued under the 2000 Amended Company Registration Act certifies certain facts, including (a) the existence of the company, (b) the authority of the representative director of the company, and (c) the authenticity of the e-signature of the representative director of the company.

(ii) E-certificate issued by an Authorized E-signature Service Provider

An e-certificate issued by an Authorized E-signature Service Provider certifies that the e-signature of a particular person has actually been affixed on an e-contract by such person. However, if a person affixes an e-signature to an e-contract for and on behalf of a company, such e-certificate does not certify the existence of the company or the authority of the aforesaid person to affix the e-signature for and on behalf of the company. Such additional facts can instead be proved by obtaining an E-POA from an Authorized E-POA Service Provider.

(iii) E-certificate issued by Other E-signature Service Providers

An e-certificate can be issued by Other E-signature Service Providers. An e-certificate issued by Other E-signature Service Providers can also be used in order to prove that "*the e-signature of [a particular] person is affixed by such person*" subject to discussions as set out in Section 3 below.

3. How to Effectively Use E-signatures in Respect of Contracts Between Companies

Based on the current status under the relevant Japanese laws, there are multiple options to effectively use e-signatures in respect of contracts between companies, which include the examples set out below.

(i) Use of LAB e-signatures under the 2000 Amended Company Registration Act

Companies can use LAB e-signatures. The authenticity of LAB e-signatures can be verified by checking such LAB e-signatures against the e-certificates issued by the legal affairs bureau.

(ii) Use of e-signatures provided by Authorized E-signature Service Providers

Companies can use e-signatures provided by Authorized E-signature Service Providers.

An E-certificate issued by Authorized E-signature Service Providers certifies that the e-signature of a particular person has actually been affixed on an e-contract by such person. In addition to that, the existence of the company and the authority of the person who affixes the e-signature for and on behalf of the company can be proved by obtaining an E-POA from an Authorized E-POA Service Provider.

(iii) Use of e-signatures provided by Other E-signature Service Providers

Companies can use e-signatures provided by Other E-signature Service Providers (collectively, "Other E-signatures"). Companies can enjoy the benefit of the presumption provided under Article 3 of the E-signatures Act if the conditions specified under Article 3 of the E-signatures Act are satisfied in respect of such Other E-signatures. Please note that there are three major points which need to be carefully examined in respect of Other E-signatures as set out below.

(a) Whether or not Article 3 of the E-signatures Act applies to E-signatures (Contract Party Type)

With regard to Other E-signatures, there are generally two types of e-signatures, namely (i) e-signatures which represent the e-signatures of each party to an e-contract ("E-signatures (Contract Party Type)"), and (ii) e-signatures which represent the e-signature of Other E-signature Service Providers as a witness (*tachiainin*) ("E-signatures (Witness Type)").

Among the conditions set out in Article 3 of the E-signatures Act, it would be easier for an E-signature (Contract Party Type) to satisfy the condition of "*e-signature to be affixed by the signatory*" since it is expected that an E-signature (Contract Party Type) would have the same appearance as either the written signature or the physical seal of a person who is an employee, officer or director of the party to the e-contract, just that it is in digital form. However, there is another condition under Article 3 of the E-signatures Act which requires that "*such e-signature can be performed only by the signatory through appropriate management of* ***codes and properties*** *necessary to [affix the e-signature]" (emphasis added). When the E-signatures Act was enacted in*

2001, it seems that the word "properties" was intended to refer to e-signatures in respect of which the private keys (*himitsu-kagi*) necessary for encrypting the e-signatures are saved in physical properties such as integrated circuit cards. On that basis, there has been a strong argument that "Article 3 of the E-signatures Act may not apply to e-signatures managed remotely by a cloud system (which includes both E-signatures (Contract Party Type) and E-signatures (Witness Type))". There have been discussions in respect of whether or not Article 3 of the E-signatures Act would need to be amended in order to make it clear that Article 3 would apply to both E-signatures (Contract Party Type) and E-signatures (Witness Type) even if such E-signatures are managed remotely by a cloud system. Given such ambiguity, the market players are expecting that certain guidelines will be issued by the relevant ministries and/or Article 3 of the E-signatures Act would be amended in the future.

(b) Whether or not Article 3 of the E-signature Act applies to E-signatures (Witness Type)
E-signatures (Witness Type) refer to e-signatures which are affixed in the name of an Other E-signature Service Provider acting as a neutral witness who certifies the fact that an e-contract has been executed by each of the parties. It is contemplated that Article 3 of the E-signatures Act may not apply to E-signatures (Witness Type) since E-signatures (Witness Type) are e-signatures in the name of Other E-signature Service Providers (rather than e-signatures in the name of a party to the contract) which are affixed to verify that the contents of the e-contract have been confirmed by the Other E-signature Service Provider who is acting as a neutral witness. However, in a case where a party is arguing due execution by the other party to an e-contract, it is possible to prove such due execution by the other party based on the general principle under the Code of Civil Procedure (see 1. above).

(c) How companies manage and affix their e-signatures
Article 3 of the E-signatures Act expects that each signatory to an e-contract shall affix its e-signature on such e-contract. However, in the case where a registered seal is used, a company typically affixes its registered seal through its employee who is acting in accordance with the instructions and the authorization given by the representative director of such company. In respect of e-signatures, we should keep a careful eye on how the e-signature of each company is actually affixed on e-contracts and how Article 3 of the E-signatures Act would apply to cases where an employee of the company affixes the e-signature of the representative director or other employees of the company.

4. Conclusion and Remaining Issues

As can be seen from the above, there are multiple ways of affixing e-signatures to e-contracts under Japanese law. As far as we are aware, there is no single established practice of affixing e-signatures in respect of e-contracts to be executed between companies. The demand for the use of e-contracts and e-signatures is expected to increase due to the various COVID-19 policies implemented by businesses

in Japan that have led to changes in working environments such as the rise in working from home, particularly as such changes are likely to remain even after the COVID-19 pandemic is over.

Based on the current practice of relying on the use of companies' registered seals and certificates of registered seals to execute contracts, it would be ideal to establish a single practice in respect of the execution of e-contracts between companies. It is therefore important for us to keep a close eye on how the practice of using e-signatures in the Japanese market develops, in order to determine which of the methods elaborated above can be consistently and effectively used in respect of all types of corporate transactions, including contracts among Japanese companies and non-Japanese companies.

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

- If you wish to unsubscribe from future publications, kindly contact us at General Inquiry.

- Previous issues of our newsletters are available here.