March 19, 2021

To JICPA members

The Japanese Institute of Certified Public Accountants

Remote Work Series No.6

Audit Considerations in Relation to External Confirmation Using Electronic Mail

<<I. Introduction>>

In recent years, there has been an increase in the use of electronic media or electronic processes to confirm the balances of the receivables and payables when auditing financial statements. Also in Japan, even when a confirmation form is sent in paper form, in some cases electronic mail (“ email”) may be used to send the response, and in other cases the approach used for the confirmation procedure may involve the auditor sending the confirmation request by email, and obtaining the confirmation response data from the confirming party by email.

Furthermore, IT Committee Research Report No. 38 “Audit Considerations In Relation to External Confirmation Using Electronic Media or Processes” (May 18, 2010) (hereinafter “ICRR No.38”), provides a systematic research and exploration of electronic confirmation methods and associated risks, and will be of reference when using these “Considerations”.

In these “Considerations”, taking into account the further rise in the popularity of email use since ICRR No.38 was published, and the need for the remote work that has arisen to prevent the spread of COVID-19, we provide a list of audit considerations to bear in mind when using email for confirmation in this way, which we hope will be of reference to members in their practices.

Furthermore, we anticipate multiple methods being used for confirmation, and taking into consideration the likelihood that the risk associated with the use of an electronic response to a confirmation request will vary depending on the details of the method used, we suggest matters to keep in mind when designing and performing audit procedures. (II 3. Reference)

Moreover, in contrast to the confirmation procedures using electronic confirmation systems described in Remote Work Series No.1 “Audit Considerations In Relation to External Confirmation Using Electronic Media and Processes”, when using email to perform confirmations, there is a high risk that fraudulent behavior, such as inappropriate manipulation or falsification at the time of sending or receiving, may go undetected and compromise the integrity of information transmission. Accordingly, this approach may be investigated for

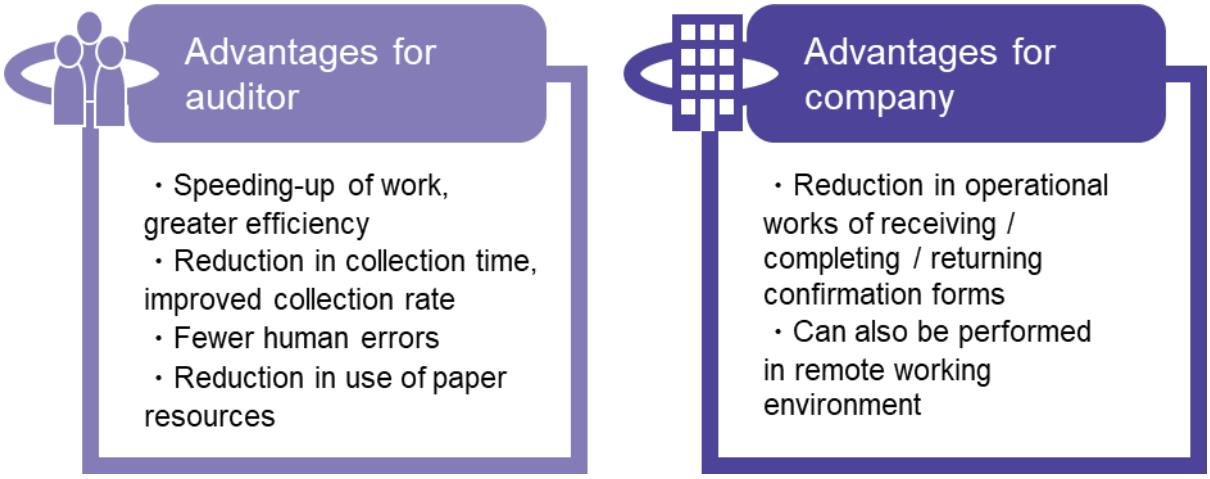
adoption in cases where, confirmation procedures using paper form or electronic confirming system appear difficult, but careful consideration is needed to manage risk, such as by combining multiple procedures. (III 2. Reference)

<<II Electronic confirmation>>

1. What is electronic confirmation?

"Electronic confirmation" refers to the use, in audit procedures performed by auditors, of requests for confirmation sent, or responses to such requests obtained, via electronic media or electronic processes.

ICRR No.38 discusses various methods to perform electronic confirmation, such as the use of paper documents to perform a confirmation request, with the responses obtained either in electronic format or using electronic processes. The use of electronic confirmation has the advantages for both auditors and companies, as shown in the following diagram.



2. Electronic confirmations covered by these "Considerations"

In these "Considerations", we cover methods in which an auditor performing an audit procedure obtains confirmation response data sent using email by a confirming party (confirmation using email).

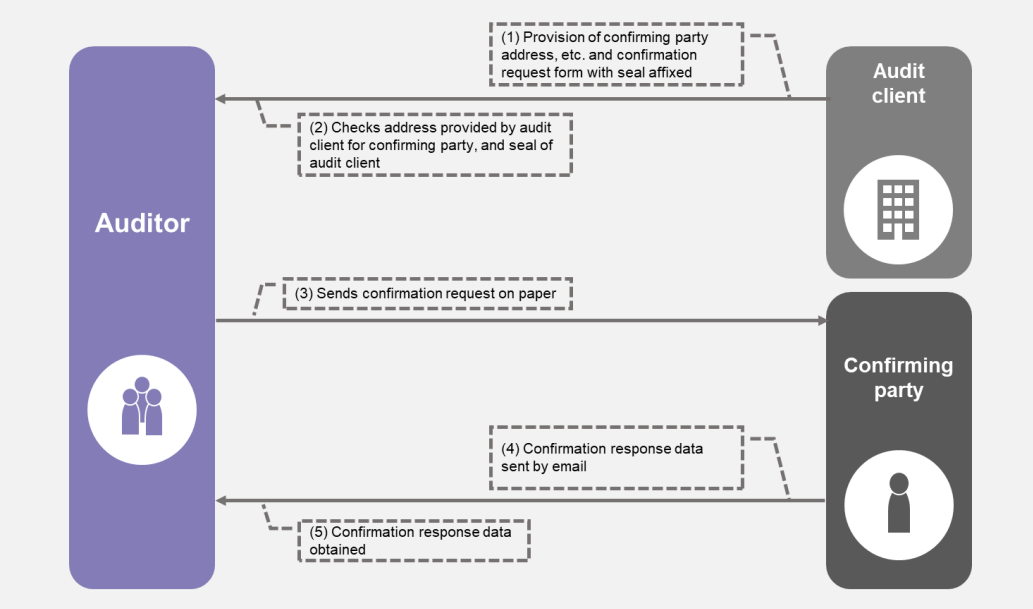
Refer to Remote Work Series No.1 for the use, in audit procedures performed by auditors, of electronic confirmation systems based on websites implemented and operated by auditors, in which both requests for confirmation and responses obtained are implemented via electronic media or electronic processes (confirmation using an auditor website).

3. What is external confirmation using email?

"Confirmation using email" refers to methods in which an auditor performing an audit procedure obtains confirmation response data sent using email by a confirming party.

Based on the organization used in ICRR No.38, the following methods may be used for confirmation using email.

[Method 1] Cases in which the confirmation request is sent in paper form and the confirmation response is obtained by email



(1) The auditor obtains a confirmation request form from the audit client, with the address, etc. of the confirming party and the seal of the audit client affixed.

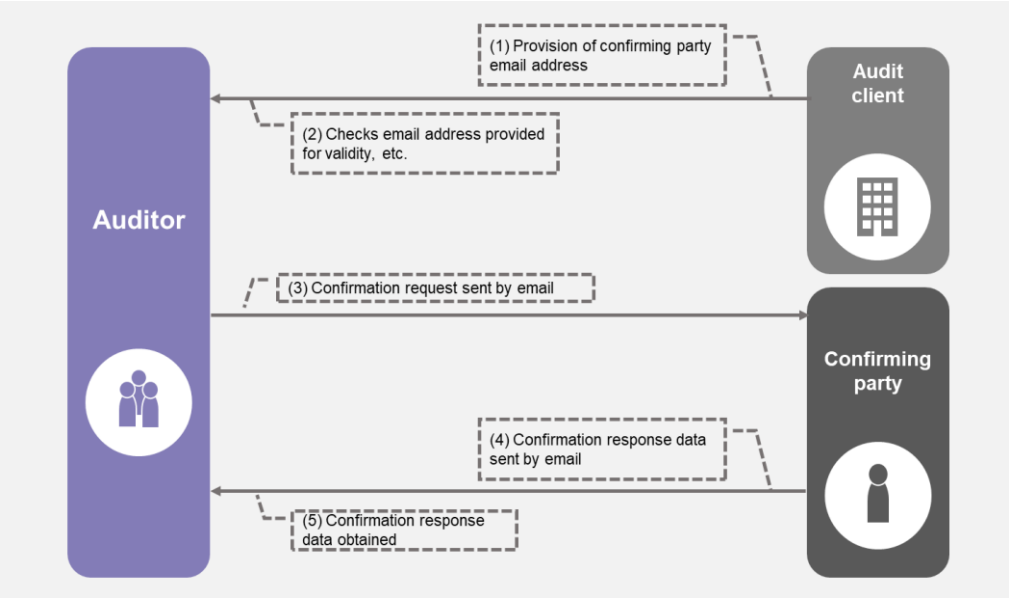
(2) The auditor checks the address provided by the audit client for the confirming party, and the seal of the audit client.

(3) The auditor sends the confirmation request in paper form to the confirming party. (The auditor includes their email address.)

(4) The confirming party responds to the items to be confirmed in the request ("confirmation response data") by sending an email to the auditor.

(5) The auditor obtains the confirmation response data in the form of an electronic file.

[Method 2] Cases in which the both request and the response are sent by email



(1) The auditor receives the email address of the confirming party from the audit client.
(2) The auditor checks the email address received from the audit client for validity, etc.
(3) The auditor sends a confirmation request to the confirming party by email.
(4) The confirming party responds to the items to be confirmed in the request ("confirmation response data") by sending an email to the auditor.
(5) The auditor obtains the confirmation response data in the form of an electronic file.

In addition, in the case of both Method 1 and Method 2, the auditor needs to consider using the telephone or other means to confirm directly with the confirming party that they have actually sent the response by email.

When performing external confirmation using email, it is assumed that the confirming party has agreed to provide a response by email, but such agreement may not be obtained from confirming parties at some financial institutions.

Normally the confirming party uses the presence of the seal (hanko) and typed name on the paper confirmation sent to them as grounds to deem that the agreement of the audit client has been obtained in relation to responding to a confirmation request from the auditor. However, in cases where the confirmation request is sent by email as in the above-mentioned Method 2, no response may be received if the confirming party is unable to conclude that the agreement of the audit client has been obtained. For that reason, when sending a confirmation request by email, the audit client may add their electronic signature to a confirmation request that has been created in email format, or notify the confirming

party beforehand to the effect that the audit firm will perform confirmations, and cc the auditor in the email. This approach enables the confirming party to recognize that the confirmation request from the auditor is made with the agreement of the audit client. (Refer to ICRR No.38, II 7.(1)(i), (ii))

In addition, as impersonation of email senders and other phishing techniques are becoming increasingly sophisticated, in order to provide an opportunity for the confirming party to verify the validity of email from the auditor, the auditor is advised to use an email address from the domain that has been registered by the audit firm to send emails.

As well as this, from the perspective of managing the risk that arises as a result of confirmation by email, the auditor may consider that the confirmation request sent by the auditor and the confirmation response data sent by the confirming party are not be presented in the body of the email, but might instead be attached to the email as an encrypted PDF file. (Refer to III 3. Example 7)

<<III. Considerations>>

1. External confirmation using electronic methods based on ASCS 505

Paragraph 10 of Auditing Standards Committee Statement 505, “External Confirmations” (hereinafter, “ASCS 505”), states that “if the auditor identifies factors that give rise to doubts about the reliability of the response to a confirmation request, the auditor shall obtain further audit evidence to resolve those doubts.” Furthermore, Paragraph A11 states that “All responses carry some risk of interception, alteration or fraud. Such risk exists regardless of whether a response is obtained in paper form, or by electronic or other medium.”

Risks associated with responses to confirmation procedures, such as reliability, falsification and fraud, exist irrespective of whether the confirmation procedure is performed in paper form using mail or by electronic methods. However, when performing confirmations by email it needs to be kept in mind that the nature and the assessment of these risks varies depending on whether the confirmation is performed using an electronic confirmation system or in paper form and the auditor needs to evaluate whether these risks have been reduced to an acceptable low level.

2. Risks associated with external confirmation using email

Risks associated with confirmation using email basically consist of risks such as impersonation of the confirming party and denial after replying a confirmation, as described in ICRR No.38, and are composed of the following four risks.

(1) Risk that the response is not obtained from appropriate source of information
(2) Risk that the confirming party does not have the authority to respond
(3) Risk that the integrity of the information transmission has been compromised

(4) Risk that the confirming party denies details of the response

Of these, "(4) Risk that the confirming party denies details of the response" refers to the risk that, in the event that the confirming party subsequently denies their involvement or the details of the response, the auditor cannot present any evidences to disprove them.

For confirmation using email, it is assumed that either Method 1 or Method 2 will be applied, and in Method 1 the use of mail makes it possible to check whether the confirmation request has been delivered to the address at which the auditor expected the confirming party to be found. By contrast, under Method 2 a similar result cannot be achieved by a confirmation request sent by email, which could raise the risk of the confirming party being impersonated by somebody else.

For that reason, when designing and performing confirmation procedures that use Method 2, the auditors needs to bear in mind that (1) the risk that the response is not obtained from an appropriate source of information, and (2) the risk that the confirming party does not have the authority to respond, and (4) the risk that the confirming party denies the details of the response are relatively high.

In addition, when using an auditor website for confirmations, in order to manage the above-mentioned (3) risk that the integrity of the information transmission has been compromised, the administrator may continuously assess whether the design of the internal controls built into the electronic confirmation system of the auditor website is suitable for the circumstances, and take steps to rectify the situation in cases where there is a deviation from predetermined processing, or use a service auditor's report from an independent third party in relation to internal controls for outsourced operations.

However, for confirmations using email, the same approach cannot be used. For that reason, when compared to confirmation using an auditor website, it is not possible to fully manage the above-mentioned (3) risk that the integrity of the information transmission has been compromised. In order to check that the content of the response has not been falsified, the auditor may assess whether there are any physical or human vulnerabilities in the security of the email system being used, and whether the email was properly encrypted, as well as carefully considering the need for designing and performing additional procedures.

In addition, we advise auditors performing a confirmation using email to take into account the following matters, which are assumed to be guaranteed under an electronic confirmation system. These are not directly related to the reliability of an electronic response but can be thought of as requirements for guaranteeing the reliability of an electronic response, either indirectly or in a supplementary way. (Refer to ICRR No.38, II 4.(5))

(1) Confidentiality

Auditors shall pay attention to the possibility of the information being intercepted through the route to obtain the electronic response and maintaining the confidentiality of

information after it has been obtained.

(2) Processability

In order to use the information in an electronic response to perform comparisons of the amounts and volumes for items that have been confirmed and to reconcile exceptions, the auditor considers ensuring that the original data is not modified when processing the non-numerical information in the electronic response.

(3) Readability

Generally speaking, in order for the auditor to read an electronic response, personal computer hardware and specific software is required, and it is assumed that these are similar for the issuer and the user of the electronic response. Accordingly, when the auditor is building a system for using electronic responses, they consider what hardware and software are required.

3. Examples of responses to the risks associated with external confirmation using email

Methods assumed to mitigate the above-mentioned risks associated with confirmation using email may include those listed in the examples below. Also, it should be understood that the following methods are only examples and are not limited to those presented below.

The following include some methods that may not mitigate risks sufficiently when used independently. Depending on the situation, careful assessment may be required to ascertain whether it is necessary to use a number of different methods in combination, or to consider that it may not be possible to obtain an appropriate response when the confirming party is an individual person. In addition, depending on the level of inherent risks, audit risk may not be able to be reduced to an acceptable low level even when combinations of these methods are used. The responses performed more efficiently at the audit firm level are included rather than at the level of individual audit teams.

When obtaining a confirmation response using email, the provision of evidence in relation to the risks shown in 2 above should not be limited to the response itself, because other relevant procedures may result in evidence, such as the electronic signature add to the email, the history of sending and receiving (including email header information), the body of the email message, and communications conducted separately by telephone. The auditor needs to bear in mind the necessity of including these in appropriate documentation.

It also needs to be kept in mind that in examples 1, 5, 6 and others, it is important to obtain the cooperation of the audit client and the confirming party.

	Possible Responses	Risks associated with confirmation using an auditor website (refer to 2.)			
		(1) Risk that the response is not obtained from appropriate source of information	(2) Risk that the confirming party does not have the authority to respond	(3) Risk that the integrity of the information transmission has been compromised (Note)	(4) Risk that the confirming party repudiates the details of the response
(Example 1)	Involvement of multiple persons in the confirmation response	◎	◎		
(Example 2)	Using the telephone to confirm with the confirming party	◎	◎		
(Example 3)	Additional procedures related to the confirming party	◎	◎		
(Example 4)	Investigating the appropriateness of the domain	◎	◎		
(Example 5)	Using electronic signatures	◎	◎	◎	◎
(Example 6)	Using the Ministry of Justice's electronic certification system based on commercial registration	◎	◎		
(Example 7)	Procedures for discovering inappropriate manipulation and falsification of emails at the time of sending or receiving			◎	
(Example 8)	Obtaining pledges, etc. from confirming parties		◎		◎

*The ◎ symbol denotes the main risks that may need to be managed in each possible response.
*(Note) Compared to the method using an auditor website, careful consideration may be required.

(Example 1) Involvement of multiple persons in the confirmation response

In order to manage the risk that the response is not obtained from an appropriate source of information, or the risk that the confirming party does not have the authority to respond, when sending an email confirmation request form, or when the confirming party sends the response by email to the auditor, it may be effective to include the superior of the confirming party or the person at the confirming party who is responsible for accounting in the CC field.

After a confirmation response has been obtained from the confirming party, sending an email to their superior, with a message that confirmation has been obtained, may also be an effective way of managing the above-mentioned risks.

The involvement of multiple persons in the response to a confirmation request may be an important factor in restricting the confirming party to an appropriate response.

When a confirmation responses has been received by email, it is usually impracticable to determine by inspecting the body of the email whether the response has been approved in the appropriate manner by the confirming party's superior, etc. For that reason, as a means of demonstrating that the superior, etc. is involved, it is appropriate to make this clear in advance, in the confirmation request form. For example, when the confirming party responds to the auditor they could include their superior in the CC field, or after the response from the confirming party, the superior could declare to the auditor, by responding to the email, that the approval has been given to the confirmation response.

(Example 2) Using the telephone to confirm with the confirming party

In order to manage the risk that the response is not obtained from an appropriate source of information, or the risk that the confirming party does not have the authority to respond, when sending a confirmation request the auditor is expected to check that the confirming party actually exists, and that they have the appropriate authority to respond, determining whether requests are properly addressed by telephoning the confirming party to test the validity of some or all the addresses before sending out the confirmation requests (Paragraph A6, ASCS 505). In addition, where possible, the auditor usually does not make a telephone call directly to the confirming party whose details have been obtained from the audit client, but instead telephone the main switchboard of the organization to which they belong, and ask to be put through to the responding party in question. In this way the auditor is able to confirm that the responding party actually exists in the organization (company, department) communicated to the auditor by the audit client.

In cases where the address from which the confirming party sends email is a group email address, there may not be one individual specified as the confirming party. Because this suggests a higher risk that the response is not obtained from an appropriate source of information, or that the confirming party does not have the authority to respond, in addition to identifying the confirming party who used the group email address, the auditor needs to consider whether they have appropriate authority within the organization to respond to confirmation requests. However, similarly to the way a company that is a confirming party may formally notify the audit client of a dedicated address for responding to electronic confirmation requests, it may be more reliable to use a group address for registering a confirming party rather than the address of an individual. In addition, the auditor may in some cases telephone the confirming party to verify that it was actually them who sent the response (Paragraph A14, ASCS 505).

In cases where a confirming party whose identity was checked by telephone in previous years is being asked for another confirmation response, or in cases where the auditor determines that the risk that the response is not obtained from an appropriate source of

information, or the risk that the confirming party does not have the authority to respond has been reduced to an acceptable low level, it may be possible to omit telephone confirmations, investigations into the appropriateness of the domain (discussed below).

(Example 3) Additional procedures related to the confirming party

In order to manage the risk that the response is not obtained from an appropriate source of information, or the risk that the confirming party does not have the authority to respond, the auditor may take actions such as the following to confirm that the confirming party exists, that they are an appropriate confirming party, and that their email is valid.

- Inspecting the history of communication between the relevant person in charge at the audit client and the confirming party (including inspecting the business card of the confirming party obtained by the audit client)
- Investigating whether the name of the confirming party is included in documents. obtained by the audit client from the confirming party in relation to transactions.

Also, in the event that doubts arise about the reliability of the information after confirmation has been obtained, the auditor may consider sending a request for additional responses in relation to the amount confirmed, such as documents providing a breakdown to support the details of the initial response.

(Example 4) Investigating the appropriateness of the domain

In order to manage the risk that the response is not obtained from an appropriate source of information, or the risk that the confirming party does not have the authority to respond, the appropriateness of the domain in the confirming party's electronic email address may be investigated.

In terms of investigating the appropriateness of the domain, in cases where the email address for inquiries is available in the confirming party's official website, the auditor may check for consistency of the domain of the email address.

An alternative method would be to verify the registration status of the electronic domain used in the confirming party's email address.

For checking the registration status of an email address domain, the so-called Whois (https://whois.jprs.jp/) search service can be used to confirm whether an email address has been recorded in the registry, as well as the organization name, and information related to the domain administrator. In particular, "co.jp" domains cannot be obtained without having some form of corporate status in Japan, and only one such domain can be obtained by each individual company or organization, with the presentation of company registration information being required at domain registration, so registered corporations should actually exist, and users of the domain are likely to belong to the corporation.

For that reason, it may be informative to check whether the confirming party's email address domain is appropriate, using the actual email address used to provide the response. Be aware that for domains other than "co.jp" domains, it is not necessarily the case that the registry confirms the actual existence of the organization before registering a domain name.

In some cases, as a result of a domain search it is found that the domain is registered by the registry, but it seems likely that the risk that the response is not obtained from an appropriate source of information, or the risk that the confirming party does not have the authority to respond has not been reduced to an acceptable low level. In such circumstances the auditor may consider, in addition to the domain search, making inquiries by means of a telephone call to the confirming party, or sending an email to the domain administrator registered with the domain administering organization for the domain of the confirming party.

(Example 5) Using electronic signatures

In order to manage the risk that the response is not obtained from an appropriate source of information, the risk that the confirming party does not have the authority to respond, or the risk that the confirming party will denies the details of the response, the auditor may request the confirming party to add an electronic signature to the response, so as to prove that the organization to which the confirming party belongs actually exists.

By "electronic signature" we mean an encryption device, as prescribed in Articles 2 and 3 of the Act on Electronic Signatures and Certification Business (hereinafter, "the Electronic Signatures Act") related to electronic signatures and authentication services, used to identify the creator of electrical information, and that if someone made edit, users of the electrical data enable to figure out changes made to the electrical data. In cases where it is confirmed that the electronic signature attached to the response from the confirming party satisfies the requirements of the Electronic Signatures Act, it is possible and effective for the auditor to confirm that the response from the confirming party was intentionally performed by the respondent, and that the electronic document to which the electronic signature is attached has not been falsified. For example, even in cases where the email was subject to inappropriate manipulation at the time of sending or receiving, it can be confirmed that the confirmation response data was not falsified, which helps maintain the integrity of information transmission.

For witness-type electronic signatures, the email address of the creator of the information may be included in the properties of the electronic signature or in the agreement concluded between the creator and the certification business operator.

In such cases, it is possible to check whether the response was obtained from the

appropriate source of information expected at the time the request was made by comparing this email address to the email address of the confirming party used in a confirmation request performed via an electronic process.

Furthermore, in cases where a confirmation response converted to PDF format is provided together with an electronic signature that does not satisfy the requirements of Articles 2 and 3 of the Electronic Signatures Act, it is likely that risks associated with identification and non-falsification will be greater than with an electronic signature attached that satisfies the requirements of the Electronic Signatures Act. Accordingly, depending on the details of the electronic functions, in order to carefully examine whether the response was obtained from an appropriate source of information, and whether there is a high probability that it was modified after it was created, the auditor needs to consider designing and performing audit procedures such as questioning the creator themselves by telephone or by email, investigating the sender's address of the email to which the confirmation response was attached, and scrutinizing the timestamp in cases where one has been used.

(Example 6) Using the Ministry of Justice's electronic certification system based on commercial registration

In order to manage the risk that the response is not obtained from an appropriate source of information, or the risk that the confirming party does not have the authority to respond, the auditor may request the confirming party to attach the electronic certificate issued by the registry for the company or corporation (http://www.moj.go.jp/MINJI/minji06_00028.html) to the response, so as to prove that the organization to which the responding party is affiliated actually exists.

Unlike the electronic signature system, which aims to confirm the identity of the creator of information, this certification system is a method for proving that commercial registration has been conducted using an electronic medium instead of a paper-based seal-registration certificate. Its use is currently limited to online applications and notifications for governmental and local governmental agencies, but in theory it could be applied to electronic transactions between companies. However, it needs to be kept in mind that certain measures must be taken beforehand, when used for an application the user (confirming party) must perform the initial procedure at the registry, and the auditor must install special software to read the electronic certificate.

(Example 7) Procedures for discovering inappropriate manipulation and falsification of emails at the time of sending or receiving

When connected to the Internet, the risk of intrusion from an external source is high,

and it is not easy to detect modifications to a confirmation response performed by email. There is a risk that fraudulent behavior such as inappropriate manipulation, interception, or falsification at the time of sending or receiving may go undetected, compromising the integrity of the information transmission. As to whether or not this risk can be mitigated to the required level, the auditor must take measures that are appropriate to the circumstances. In such cases, a combination of multiple procedures may be used to deal with this risk.

For example, in cases where a response is received by email from a confirming party whose identity was confirmed on the telephone before sending the confirmation request (Example 2, above), by contacting the confirming party using the telephone to confirm the receipt, it may be possible to detect manipulation by persons other than the expected confirming party.

Checking the information in the properties of a confirmation response sent in electronic format, or checking whether the images of the signature and seal in the confirmation response are the same as those from the previous year are also methods that may enable detection of signs of inappropriate manipulation or falsification.

Moreover, in cases where the response received is a file with an electronic signature attached, it may be possible to use the electronic signature's mechanisms (for example, timestamps) to check for the existence of modifications after the electronic signature was attached. (Refer to Example 5)

In addition, care needs to be taken to encrypt the confirmation items in the confirmation request before it is sent. Sending the document by attaching it to the email in the form of a PDF file, etc. rather than including it in the body of the email and requesting the confirming party to use the same method when sending the response helps prevent leaks of confidential information.

(Example 8) Obtaining pledges etc. from confirming parties

It is not easy to determine whether a confirming party has the proper authority to provide a response, and there is a risk that if the confirming party subsequently denies the details of the response, the auditor cannot present any evidences to disprove them. In order to mitigate such risks by a certain level, statements could be incorporated into the confirmation response form created in PDF or some other format, to the effect that the confirming party has the necessary authority in the confirming organization, that the response is accurate, and that the response takes precedence over other responses based in paper form. Such statements could also be included in the body of the responded email sent by the confirming party, rather than in the confirmation response itself.