

# **Business E-mail Compromise Survey Report**

**JPCERT Coordination Center  
March 25, 2020**

## Table of Contents

1. Introduction .....	4
1.1. Overview .....	4
1.2. Target audience.....	4
1.3. Aim of this report .....	4
2. What Is Business E-mail Compromise? .....	5
3. Business E-mail Compromise Survey .....	6
3.1. Survey overview.....	6
3.2. Survey results .....	7
3.2.1. Relevant countries and languages used .....	7
3.2.2. Categorization .....	8
3.2.3. Methods .....	10
3.2.3.1. Forgery of invoices .....	10
3.2.3.2. Timing of misrepresentation .....	11
3.2.3.3. Impersonation.....	11
3.2.3.4. Account hijacking .....	12
3.2.3.5. Possible involvement of parties familiar with internal affairs.....	12
3.3. Losses incurred.....	13
3.4. Lessons learned from the survey results.....	14
3.4.1. Increasingly complicated structure .....	14
3.4.2. Existence of related incidents.....	16
3.4.3. Difference of position.....	16
3.5. Countermeasures.....	17
3.5.1. Operational approach.....	17
3.5.1.1. System .....	17
3.5.1.2. Training .....	18
3.5.1.3. Review of payment process .....	18
3.5.2. Technological approach.....	18
3.5.2.1. Detection function.....	18
3.5.2.2. Monitoring for lookalike domains .....	19
4. Business E-mail Compromise Abroad .....	19
4.1. International efforts.....	19
4.2. Efforts made by financial institutions .....	20
4.3. Cases of arrest.....	20
5. Countermeasures and Responses .....	22
5.1. Pre-incident measures (countermeasures) .....	23
5.1.1. Establishment of internal system.....	23
5.1.2. Anti-phishing measures .....	23
5.1.3. Measures against unauthorized access .....	23

5.1.4. Anti-malware measures .....	23
5.1.5. Measures against internal fraud .....	24
5.1.6. Detection mechanisms .....	24
5.1.7. Clarifying the money transfer process .....	27
5.1.8. Training .....	27
5.1.9. Proper log retention.....	28
5.2. Reactive measures (responses).....	29
5.2.1. Getting the big picture .....	29
5.2.2. Investigation and handling of prior incidents .....	30
5.2.3. Canceling money transfers made in response to BEC .....	30
5.2.4. Information disclosure when impersonated in a BEC scheme .....	30
6. Conclusion .....	31
7. Acknowledgment .....	33

## **1. Introduction**

### **1.1. Overview**

This report summarizes the findings of a survey carried out by the JPCERT Coordination Center (JPCERT/CC) to clarify the losses caused by Business E-mail Compromise (BEC), and what organizations should do to protect themselves against this type of scam.

### **1.2. Target audience**

This report targets the following readers.

- Information system department (IT department) staff
- Information security department (CSIRT) staff
- Management members (mainly those in charge of system, accounting, risk, or legal department), etc.

### **1.3. Aim of this report**

BEC has become widely known since the Federal Bureau of Investigation (FBI) released information about it in 2015, but losses linked to BEC scams continue to grow. According to the data on incidents reported to the FBI's Internet Crime Complaint Center (IC3), the combined number of victims inside and outside the US was 22,143 with losses amounting to approximately 3.1 billion US dollars (\$3,086,250,090) from October 2013 to May 2016, but the corresponding figures for the period from June 2016 to July 2019 surged to 166,349 and 26.2 billion US dollars (\$26,201,775,589), respectively.

In Japan, organizations such as Information-technology Promotion Agency, Japan (IPA), the National Police Agency, and Trend Micro started releasing information about BEC to alert the public in 2017. Around the end of 2017, losses incurred by Japanese organizations due to BEC scams were widely publicized, and in 2018 businesses started receiving scam e-mails in Japanese, highlighting the need to be increasingly vigilant against the BEC threat in Japan.

In light of these circumstances, JPCERT/CC decided to conduct a survey and interviews on BEC, thinking it was necessary to clarify the actual nature of the threat and, based on its findings, disseminate information about measures and responses that organizations in Japan should take in order to minimize losses related to BEC.

This report provides information about specific actions that will be effective against BEC, considering how this threat has developed and transitioned based on the survey results along with information publicly available.

## 2. What Is Business E-mail Compromise?

Various organizations have provided information about BEC. While definitions vary, they all agree on its general description: "a scam intended to trick businesses into making money transfers by sending spoof e-mails impersonating suppliers or business partners."

IC3 started releasing alerts on BEC from around early 2015, and in January 2015, it described BEC as "a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments."<sup>1</sup> Other types of e-mail scam include "romance scams" in which scammers try to lure victims into a fake relationship and then later ask for money, and "lottery scams" in which scammers ask the recipients to send them money saying they will notify lottery numbers in advance. It is also known that criminal organizations that perpetrate BEC scams against businesses also commit romance and lottery scams mainly targeting individual victims.<sup>2</sup> Although BEC is sometimes put in the same category of scam as romance and other types of e-mail scam, this report will focus on BEC as it differs from other e-mail scams in targets and methods used. In fact, statistics released by the FBI's IC3 tally the victims and losses for BEC and romance scams separately.<sup>3</sup>

In this report, BEC refers to scams intended to trick businesses into making money transfers by sending spoof e-mails impersonating suppliers or business partners. (The type of fraud known as phishing is not included.)

---

<sup>1</sup> Business E-mail Compromise  
<https://www.ic3.gov/media/2015/150122.aspx>

<sup>2</sup> 281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes  
<https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds>

<sup>3</sup> 2018 Internet Crime Report  
[https://pdf.ic3.gov/2018\\_IC3Report.pdf](https://pdf.ic3.gov/2018_IC3Report.pdf)

### 3. Business E-mail Compromise Survey

#### 3.1. Survey overview

This survey was conducted in the form of a questionnaire prepared by JPCERT/CC to gather details concerning individual cases of BEC, including failed attempts. The survey was carried out with the help of 12 organizations that supported the aim of the survey, including Japan Foreign Trade Council ISAC and the Japan Petrochemical Industry Association, and compiles the information submitted by 117 respondents. In addition, JPCERT/CC visited six of the organizations that agreed to take the questionnaire and interviewed key personnel to obtain further information about BEC incidents and measures currently in place to counter BEC.

Survey Period	July 8, 2019 to November 22, 2019
Survey Target	Japan Foreign Trade Council ISAC (supporting organization) Japan Petrochemical Industry Association (supporting organization) etc.
Method	Questionnaire and face-to-face interviews
Survey Name	Business E-mail Compromise (BEC) Survey
Survey Overview	Survey of BEC incidents observed and actions taken at each organization, etc.
No. of Responding Organizations	Questionnaire: 12; Interviews: 6

### 3.2. Survey results

#### 3.2.1. Relevant countries and languages used

[Table 1] lists relevant countries (countries where organizations involved in BEC incidents are located) and languages used.

While relevant countries may depend on the business model of the organization being surveyed, many cases involved transactions with a location or business partner in Asia.

English was by far the language most frequently used, and Japanese was used in some cases.

[Table 1: Relevant countries and languages used]

Relevant country	Cases	Language used	Cases
Japan	41	English	108
China	19	Japanese	8
United States	18	Chinese	2
India	11	Indonesian	1
Singapore	10	French	1
South Korea	7	Portuguese	1
Thailand	6		

\* Cases involving multiple locations and languages are counted multiple times.

<Other relevant countries/region>

Indonesia, United Kingdom, Germany, Brazil, Vietnam, Malaysia, Australia, Sri Lanka, Belgium, Mauritius, Turkey, the Philippines, Taiwan, UAE, Uzbekistan, Egypt, Qatar, Sweden, Spain, Tunisia, Dubai, Haiti, Pakistan, Panama, Belarus, Myanmar, Mexico, Laos, and Russia

### 3.2.2. Categorization

BEC incidents can be categorized using various approaches, but this report adopts an approach that follows the "five types of Business E-mail Compromise"<sup>4</sup> defined by IPA.

[Table 2: IPA's "five types of Business E-mail Compromise" and types of incident identified]

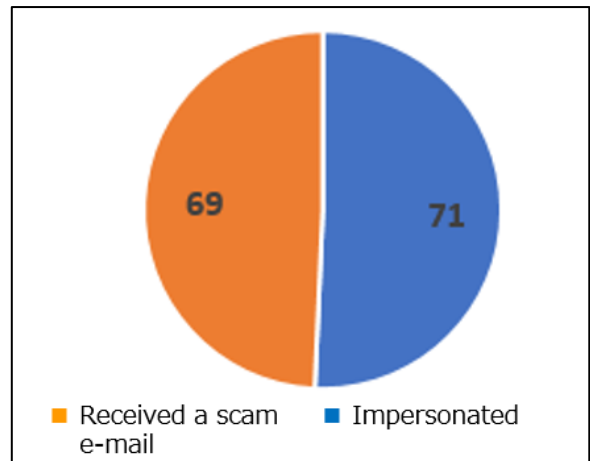
IPA's "five types of Business E-mail Compromise"	Categorization Result
[Type 1] Forgery of an invoice from a business partner E.g., Scammer sends a fake invoice (account for wiring money into) during the course of exchanging e-mails on a business transaction	Identified
[Type 2] Impersonation of a business manager, etc. E.g., Scammer impersonates a business manager and gets the victim to transfer money into a fake bank account	Identified
[Type 3] Fraudulent use of a compromised e-mail account E.g., Scammer hijacks an e-mail account and commits fraud on a business partner	Identified
[Type 4] Impersonation of an external third party with authority E.g., Scammer pretends to be a lawyer acting on the instructions of the president or other such person and requests money to be transferred	Not identified
[Type 5] Acquisition of information by fraudulent means, apparently in preparation for a scam E.g., Scammer impersonates an executive or HR department staff and obtains employee information to be used for committing fraud	Identified

Of the five types defined by IPA, incidents falling under four types excluding type 4 ("Impersonation of an external third party with authority") were identified. The most common type was type 1 ("Forgery of an invoice from a business partner"), making up approximately 75% of the total. The next most common type was type 2 ("Impersonation of a business manager, etc."), with impersonated positions including CEO and CFO. There were also some cases combining multiple types, such as a fraudster gaining access to the e-mail account of an officer and using it to have money transferred into a fake bank account.

<sup>4</sup>Cases of Business E-mail Compromise (BEC) and Security Alert (Follow-up Report) (Japanese)  
<https://www.ipa.go.jp/files/000068781.pdf>



It is also important to mention about the existence of impersonated organizations. Reports and articles currently published on BEC often focus on organizations whose money has been stolen (or nearly been stolen). However, it must be noted that while there are organizations that have received scam e-mails, there are also organizations that have been impersonated. As shown in [Figure 1], this trend is clearly visible among the cases identified in the survey as well, and there were nearly as many organizations that received a scam e-mail as those that were impersonated. the difference in position with respect to BEC will be key to considering countermeasures and responses.

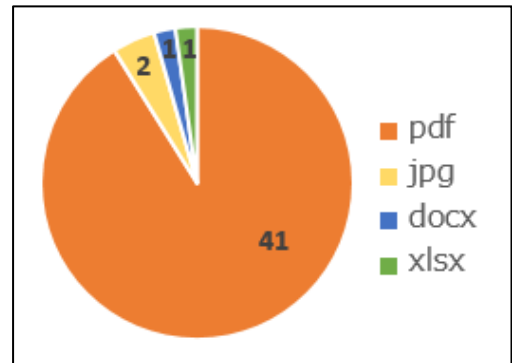


[Figure 1: Difference in position with respect to BEC]

**3.2.3. Methods**

**3.2.3.1. Forgery of invoices**

Of the "five types of Business E-mail Compromise," the most common type was type 1 ("Forgery of an invoice from a business partner"). There were also many cases in which invoices used in actual transactions were falsified and used to perpetrate BEC scams. The survey asked if there was an attachment in each case, and if there was, what file format was used and the date and time the file was created. The results showed that PDF files were used in 90% of the cases, and that many of the files were created using free conversion software or conversion websites. Also, in some cases the date and time created recorded in the document properties are in a different time zone from the relevant country, so this information can also be used to spot BEC.



[Figure 2: Attachment file types]

[Table 3: Examples of software and websites used to convert attachment files to PDF]

PDF Conversion Software	PDF Conversion Websites
3-Heights™ Document Converter	Convert-JPG-to-PDF.net
Adobe Acrobat	Zamzar
Excel for Office 365	Online PDF-Converter
GPL Ghostscript	pdf-tools.com
Microsoft Word	Sejda SDK
Quartz PDF Context	
PDFfill FREE PDF Tools	
PDFlib	
RAD PDF management tool	
SAMBox	
Skia/PDF	

Some of the falsified invoices contained signs of forgery, such as something odd in the billing details and indications that text boxes were simply copied and pasted. If examined carefully, these signs could have been identified and losses prevented.

E-mails asking to have money wired into a different account by replacing a legitimate invoice with a forged one, for example, often have a reason attached for the change. The table to the right lists the reasons given for why the account

[Table 4: Reasons given for account change]

<Reasons for account change>	
✓	Account cannot be used due to an annual audit
✓	Main account is under inspection due to a tax issue
✓	Financial records are being created for the main account to issue a check
✓	Foreign exchange rates are being adjusted due to system reform
✓	Bank merger, etc.

needs to be changed in the cases identified in the survey. Although they all look legitimate, it must be noted that these were reasons given in actual cases of BEC. Many of the cases reported in this survey used "annual audit" as a reason that the normal account could not be used.

**3.2.3.2. Timing of misrepresentation**

Attackers tend to give instructions to change the account during the process between issuing an invoice and making a payment by sending a forged invoice and other means. BEC has occurred during the course of concluding a new business contract as well. Some respondents have claimed that such cases are difficult to spot since, unlike with existing business transactions, they offer no opportunity for noticing any irregularity through comparison with an existing account and so on.

[Table 5: Timing of misrepresentation]

Timing of Misrepresentation		
Before issuing an invoice		
	Misrepresentation during the process before issuing an invoice	13
When issuing an invoice		
	Misrepresentation during the process of issuing an invoice	33
Before transferring money		
	Misrepresentation during the process between issuing an invoice and transferring money	29
After transferring money		
	Misrepresentation after transferring money	3
Other		
	Misrepresentation that occurred regardless of the payment process	28

**3.2.3.3. Impersonation**

Of the "five types of Business E-mail Compromise," the next most common type was type 2 ("Impersonation of a business manager, etc."). As discussed in 3.2.2. Categorization, the survey found cases in which CEO and CFO were impersonated, but there was also a case using a new approach in which the attacker impersonated a business manager and a secretary. In this case, a person identifying him/herself as a

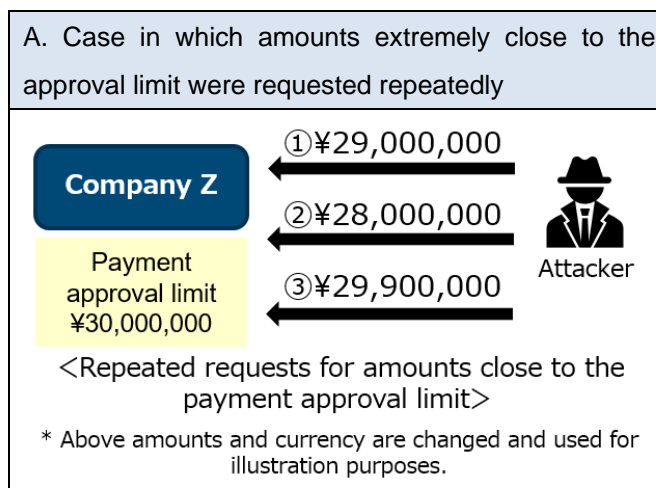
secretary first sent an e-mail saying the CEO will give instructions on a business transaction the next day, and that he/she (the secretary) will be absent that day. The next day, someone impersonating the CEO gave instructions to send money. As businesses have become increasingly concerned about and wary of BEC, it is assumed that the attacker impersonated multiple actors to gain the confidence of the victim. Impersonation is not limited to type 2 ("Impersonation of a business manager, etc."). There were also many type 1 ("Forgery of an invoice from a business partner") cases in which scammers impersonated an officer or employee of the same organization as the victim. Attackers employ the same impersonation methods used to date, such as using lookalike domains with a different top-level domain (TLD) or altered character strings.

### 3.2.3.4. Account hijacking

The questionnaire also asked about the e-mail services used by the perpetrators of BEC scams to send e-mails. While there were some cases in which an account created with a free e-mail service was used to carry out attacks, a number of cases involved fraudulent use of hijacked e-mail accounts as defined in type 3 ("Fraudulent use of a compromised e-mail account") of the "five types of Business E-mail Compromise." In the survey, none of the cases involved a breach of an account set up with an e-mail service administered by the organization in question. However, there were breaches of accounts using free e-mail services, as well as cloud-based e-mail services introduced independently by overseas office. Interview respondents listed brute force attacks and the use of credentials stolen by means of phishing or malware as reasons for the breaches of accounts.

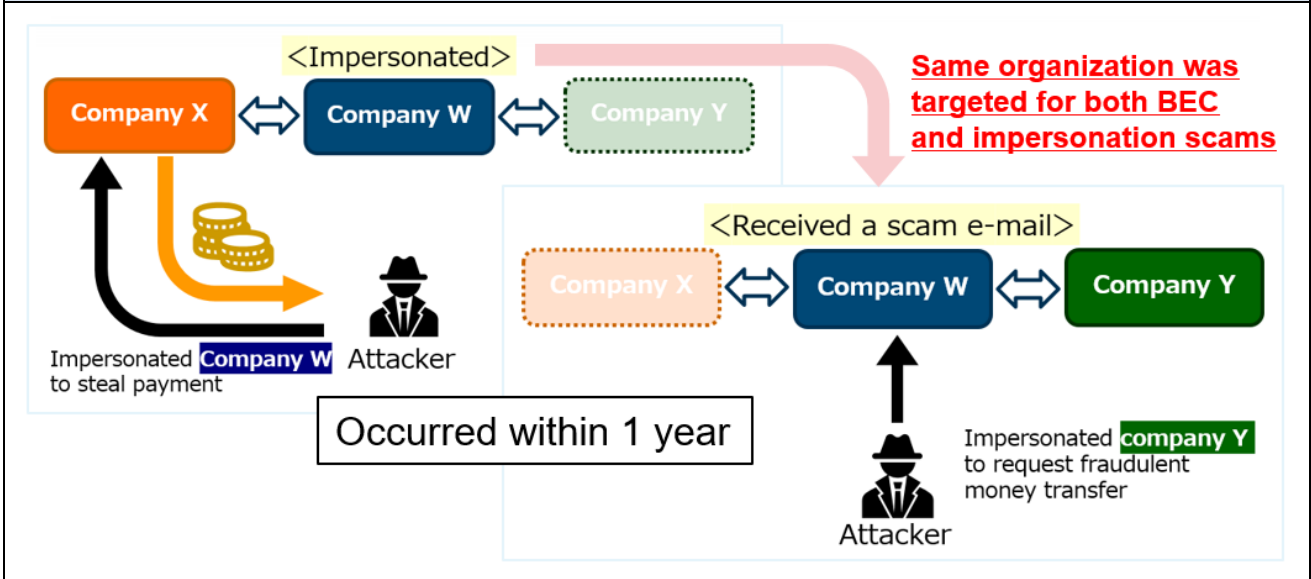
### 3.2.3.5. Possible involvement of parties familiar with internal affairs

Some of the cases attempted BEC scams using information that only related parties can know. Examples include "A. Case in which amounts extremely close to the approval limit were requested repeatedly" and "B. Case in which the same organization was targeted for BEC (received a scam e-mail) after suffering losses in an impersonation scam" (see the figure below). In some cases, attackers do collect preliminary information before perpetrating BEC scams. However, given that some BEC scams are carried out using information



external parties cannot possibly know, such as the approval limit of payment amounts and details of multiple transactions, the possibility of involvement of parties familiar with internal affairs cannot be denied.

B. Case in which the same organization was targeted for BEC (received a scam e-mail) after suffering losses in an impersonation scam



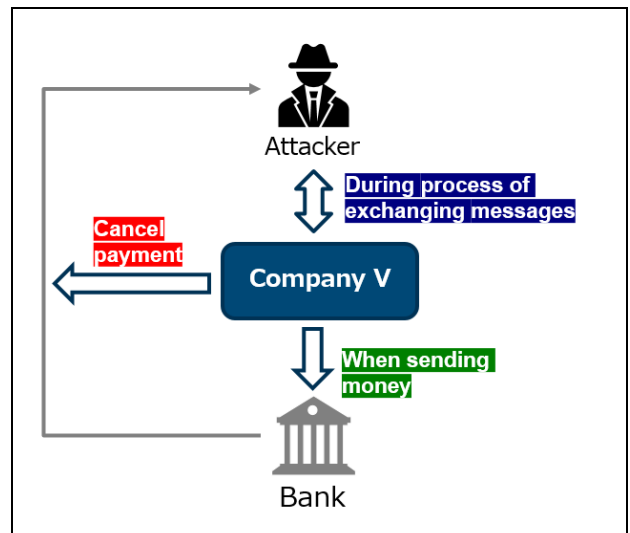
[Figure 3: Cases in which parties familiar with internal affairs could be involved]

### 3.3. Losses incurred

In the cases surveyed, scammers basically requested money transfers denominated in a foreign currency, but a majority of the cases were identified as BEC scams before incurring any actual losses.

How these cases were identified and the reasons losses were avoided are described below.

- (1) The person who was exchanging e-mails noticed that it was a BEC scam
- (2) Money could not be transferred because the specified account was frozen or for some other reason
- (3) The person involved noticed that it was a scam after receiving a reminder from the business partner and was able to cancel the money transfer



[Figure 4: Timing in which losses were avoided]

In most cases, persons involved notice the scam during the course of exchanging e-mails, and as soon as they feel anything suspicious, they check with the counterparty using a means of communication other than e-mail (phone, messaging app, etc.) and avoid losses.

Examples of clues drawn from the survey results are listed in the table to the right. Unnatural local language is a level of language that local staff feel unnatural and may be difficult for people like overseas representatives to notice.

[Table 6: Examples of clues that helped detect scams during the course of exchanging e-mails]

<Examples of clues>	
✓	Request for payment already made, invoice that looks unnatural
✓	Request for money transfer to an unfamiliar region
✓	Frozen bank account
✓	Unnatural local language, etc.

While losses were avoided in many cases, there were also cases in which losses amounting to millions or even tens of millions of yen were incurred. Amounts of losses vary because the amounts requested differ depending on the details of transaction. This suggests that attackers who perpetrate BEC scams fully understand the transaction details.

In some cases, the account where money was sent was later frozen, and a portion of the losses was returned according to the balance of the account. There were also some cases in which losses could be recovered by filing a crime insurance claim. However, there are issues as well. One is complicated procedures for recovering losses. To prove losses in a BEC scam, many documents need to be submitted to banks, insurance companies, and so on. In addition, when an overseas financial institution is involved, the necessary procedures often must be handled in the local language and may entail other complexities, adding considerably to the burden. Another issue is the timing of reversal. If losses are returned in the next accounting period, the returned amount will be treated as proceeds on the books. There appears to be cases in which losses cannot be recovered for this reason.

The total amount (converted into yen) requested in the BEC scams reported in this survey, regardless of whether losses were incurred, was approximately 2.4 billion yen.

### 3.4. Lessons learned from the survey results

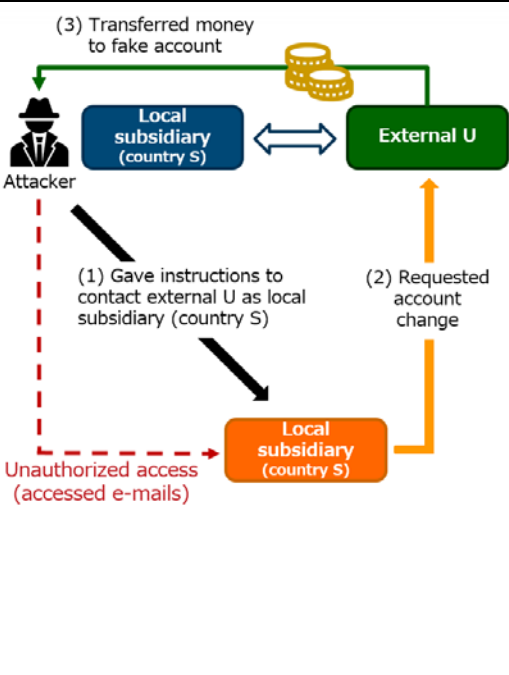
The following lessons were learned through this survey.

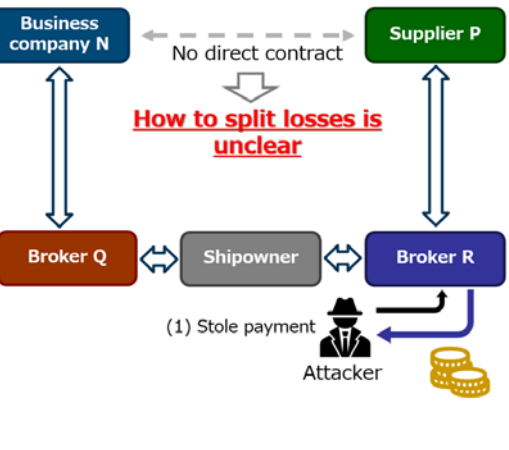
- BEC scams do not always take place only between the attacker and the affected organization; there are also cases involving multiple organizations and/or persons
- Some BEC incidents occur in connection with a preceding incident
- Measures against BEC must address the risk of being impersonated as well as being tricked

#### 3.4.1. Increasingly complicated structure

Many of the reports and articles currently published on BEC discuss cases occurring on a one-to-one basis, such as between two different companies or between an officer and employee.

While many of the cases reported in this survey were on a one-to-one basis, there were also cases that involved multiple persons and/or organizations on one side or both sides. Here are some examples.

C. Case involving another group organization		
Overview	<ul style="list-style-type: none"> <li>■ Occurred during a transaction process between a local subsidiary (country S) and an external U</li> <li>■ Payment from the external U to the local subsidiary (country S) was stolen</li> </ul>	 <p>(3) Transferred money to fake account</p> <p>Local subsidiary (country S) ↔ External U</p> <p>Attacker</p> <p>(1) Gave instructions to contact external U as local subsidiary (country S)</p> <p>(2) Requested account change</p> <p>Unauthorized access (accessed e-mails)</p>
Method	<ul style="list-style-type: none"> <li>■ The attacker impersonated the local subsidiary (country S) and instructed another local subsidiary (country T) to request the external U to change the account</li> <li>■ The local subsidiary (country T) requested the external U to change the account</li> <li>■ The external U sent a payment to a fake account</li> </ul>	
Key points	<ul style="list-style-type: none"> <li>■ Communication between the local subsidiary (country T) and external U was legitimate</li> <li>■ Confidence was gained using another group organization</li> </ul>	

D. Case handled through brokers		
Overview	<ul style="list-style-type: none"> <li>■ Occurred during a transaction process between business company N and supplier P</li> <li>■ Payment is made through brokers</li> <li>■ Payment from broker R to a shipowner was stolen</li> </ul>	 <p>Business company N ↔ Supplier P</p> <p>No direct contract</p> <p><b>How to split losses is unclear</b></p> <p>Broker Q ↔ Shipowner ↔ Broker R</p> <p>(1) Stole payment</p> <p>Attacker</p>
Method	<ul style="list-style-type: none"> <li>■ The attacker impersonated the shipowner and set up a fake payment account</li> <li>■ Broker R sent a payment to the fake account</li> </ul>	
Key points	<ul style="list-style-type: none"> <li>■ No direct contract between business company N and supplier P</li> <li>■ Multiple organizations are involved without any direct contract, so how to split the losses is at issue</li> </ul>	

[Figure 5: Examples of cases in which multiple persons and/or organizations were involved]

These were cases in which multiple persons and/or organizations were involved, with third parties intervening in the transaction process and, as a result, BEC occurring between organizations with no direct contractual relationships.

Such structural relationships may make it difficult to identify causes and require considerable effort to

resolve legal issues like the proportion of losses to be borne. In any case, when thinking about BEC, it is necessary to keep in mind that multiple actors and organizations may be involved, instead of thinking in terms of a simple structure of a perpetrator and victim.

### **3.4.2. Existence of related incidents**

As a rule, it is difficult for anyone other than the persons in charge or other related parties to obtain the details of a transaction between organizations. However, there were many cases in which the attacker appeared to have known the transaction details in advance, as suggested, for example, by the broad range of payment amounts requested from tens of thousands of yen to hundreds of millions of yen, or the fact that a forged invoice was received immediately after a legitimate invoice was sent.

One organization found in an internal survey that a user had accessed a phishing site and entered the credentials of the e-mail service immediately before the BEC scam came to light, which it believed led to the leakage of transaction details. Another organization found in an internal investigation conducted later that it had been infected with malware.

In both cases, the acts in question took place before the BEC scam was uncovered. When faced with an incident, a victim tends to focus on the event unfolding before their eyes, and be oblivious of why the attacker has the transaction details or how they came by the e-mail account information. However, it is important to be aware of the possibility that information obtained in a prior security incident may have been exploited to perpetrate a BEC scam.

If a security incident such as a breach of account or information leakage occurs at your own organization or at a related party, it is recommended that appropriate steps be taken to urge vigilance against BEC by issuing a security alert within the organization, in view of the possibility that the leaked information may be used in a BEC scam.

### **3.4.3. Difference of position**

Another point that should be kept in mind is that while you could become a victim, one could also be helping the perpetrator. In cyber security incidents, infrastructure of one's own organization could be used as a springboard for carrying out cyber attacks. Likewise, any organization can unwittingly become an accomplice in BEC scams as well. At the same time, this is a problem that is easy to be overlooked as organizations tend to prioritize their own defenses and fail to implement countermeasures in a timely manner.

As stated in 3.2.2 Categorization, in this survey there were nearly as many organizations that received scam e-mails as those that were impersonated. Given that BEC is a type of scam connected with business transactions, the organization that incurred financial losses (defrauded organization) might file a civil action against the impersonated organization and seek compensation for damages. In considering measures against BEC, it is necessary to address not just the risk of incurring losses by paying money to fraudsters, but also the risk of being impersonated in view of a possible claim for damages from the affected



organization, and to be prepared in case such a claim is made.

### 3.5. Countermeasures

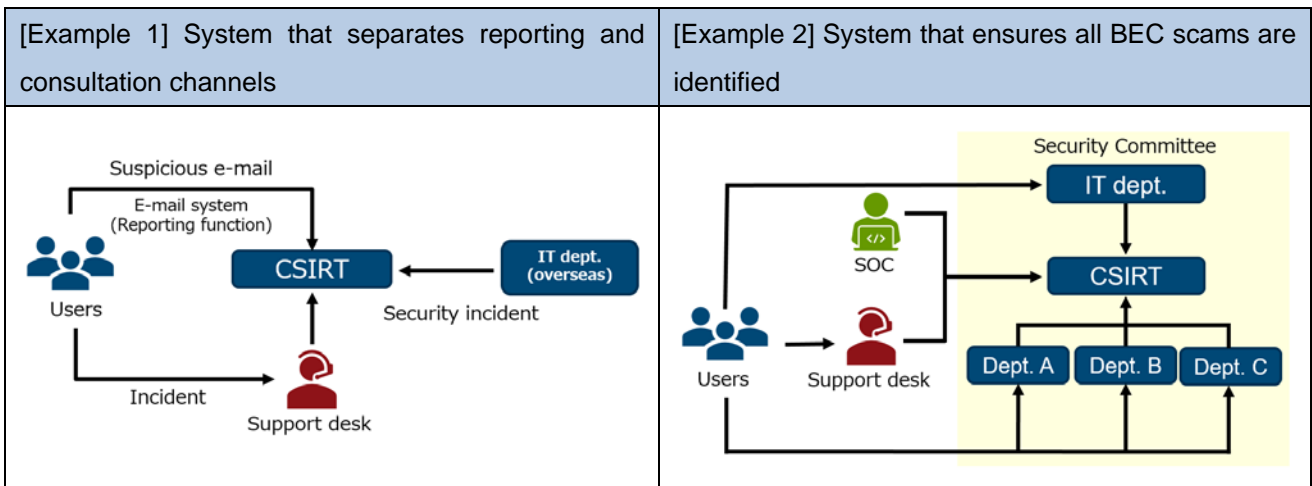
So far, the specific methods used, characteristics, and losses incurred that came to light through the survey have been discussed. The interviews also asked about measures taken against BEC, and roughly two types of approach have been found: operational and technological. This section will discuss measures implemented by organizations from these perspectives.

#### 3.5.1. Operational approach

##### 3.5.1.1. System

To prevent losses from BEC, it is necessary to detect the scam. In many cases, a company's IT support desk or other department responsible for IT troubles is in charge of handling reports and consultations related to BEC incidents since they stem from e-mail. When there is no specified contact point, these reports and consultations are directed to the sales department, accounting department, or elsewhere as determined by the user. There is a concern that these BEC cases could be buried among other matters and go unnoticed.

Organizations that handle BEC effectively often have separate contact points for reports and consultations concerning IT troubles and e-mails, and regularly share information about BEC with general affairs, legal, accounting, sales, and other related departments so that relevant information is channeled into departments responsible for handling BEC.



[Figure 6: Systems of organizations that handle BEC effectively (examples)]

### **3.5.1.2. Training**

The survey revealed that many organizations provide training described in reports currently published on BEC.

Every organization that provides training includes it in the training on suspicious e-mails with an eye on targeted attacks and cyber attacks.

Some organizations provide company-wide training through e-learning while regularly sharing with users information that requires their attention, such as insights gained through BEC scam e-mails received by the organization. There are also organizations where legal, financial, and IT departments jointly conduct group training targeting managers with authority to approve payments, and provide knowledge about IT and information from multiple perspectives such as laws and regulations of foreign countries, payment flow, and clues for spotting scams.

Responses on the effects of these initiatives differ for each organization. Organizations that provide group training have seen some effects, so they are planning to make it available to the entire company in the form of video content. On the other hand, some organizations, while showing understanding for the necessity of training, also claimed that initiatives that rely on users are not sufficient, and are focusing on creating a system that ensures information about incidents is quickly reported.

### **3.5.1.3. Review of payment process**

Review of payment process has been discussed as a common countermeasure by various public institutions and security vendors, and some organizations have actually reviewed their processes. Specifically, they added checks by the accounting department in addition to the sales department to enhance the payment process.

## **3.5.2. Technological approach**

### **3.5.2.1. Detection function**

As mentioned in the discussion on the operational approach, BEC scams need to be detected in order to be prevented. To this end, establishing a system to help recipients identify scams and a simple reporting scheme will be effective. One organization uses a pop-up function to alert recipients when they have received an e-mail from a domain that they have not received an e-mail from in the past three months.

Another organization provides a button in the inbox of its e-mail system that enables recipients of suspicious e-mails to report them with a simple push of a button, making the reporting process hassle-free.

### 3.5.2.2. Monitoring for lookalike domains

BEC scams often use a domain that closely resembles a legitimate domain ("lookalike domain") for the e-mail sender address. The use of lookalike domains is not a problem unique to BEC, but one organization uses a paid service as a countermeasure to monitor the registration status of domains that closely resemble its own and, when a lookalike domain is identified, send an alert across the company and applying filters on the e-mail system. According to this organization, a lookalike domain is created in about two days on average after a legitimate domain is created, and the sheer number of lookalike domains generated each day makes the effort to counter them endless. As mentioned in 3.2.3.3 Impersonation, there is a wide variety of patterns for creating lookalike domains, such as using a different TLD or modifying character strings, so it is understandable that this countermeasure is unlikely to be highly effective.

## 4. Business E-mail Compromise Abroad

This section discusses the situation surrounding the BEC threat outside Japan and efforts made to combat it. Various communities have been formed among many organizations and countries in an ongoing effort to reduce losses linked to BEC. This effort is mainly popular in the United States, where losses from BEC are growing each year. In a number of publicized cases, individuals suspected of involvement in BEC schemes have been prosecuted and arrested thanks to cooperation between financial institutions and law enforcement agencies.

### 4.1. International efforts

In December 2015, an e-mail group called "The Business Email Compromise List" was founded to fight the BEC threat.<sup>5</sup> The e-mail group was originally launched with the aim of sharing information about the BEC threat and analyzing its methods. Later, as the membership grew, it also started engaging in activities to protect victims.<sup>6</sup> In October 2018, Ronnie Tokazowski, founder and administrator of The BEC List, received the M3AAWG JD Falk Award in recognition of the group's achievements.<sup>7</sup>

Members use the information obtained from the e-mail group to help prevent BEC at their own organizations, and these include law enforcement agencies, e-mail service providers that have the ability to suspend e-mail accounts, and financial institutions involved in transferring money. The list of cooperating members includes security vendors as well, since there are also reported cases of BEC incidents in which the attacker used malware or other means to steal information from the target organization before requesting fraudulent money transfers. As it is difficult for a single organization, industry, or even country to combat the threat of BEC alone, it would be desirable to further promote various forms of cooperation between countries and

---

<sup>5</sup> How Do You Fight a \$12B Fraud Problem? One Scammer at a Time  
<https://krebsonsecurity.com/tag/bec-mailing-list/>

<sup>6</sup> "Under the Radar" Industry Group Fighting BEC Phishing Receives 2018 M3AAWG JD Falk Award  
<https://www.m3aawg.org/Rel-FalkAward-2018>

<sup>7</sup> SilverTerrier: 2018 Nigerian Business Email Compromise Update  
<https://unit42.paloaltonetworks.com/silverterrier-2018-nigerian-business-email-compromise/>

organizations.

#### 4.2. Efforts made by financial institutions

In the US, financial institutions are required to report suspicious transactions that may be associated with criminal activities to the Department of the Treasury through a system called Suspicious Activity Reporting (SAR), which is used to collect information about suspicious transactions.<sup>8</sup> Reported information is forwarded to the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and used by FinCEN and law enforcement agencies to conduct criminal investigations. These efforts enable FinCEN and law enforcement agencies to cooperate and, in some cases, recover funds. In particular, funds are often successfully recovered if reported within 24 hours of payment. FinCEN requests US-based financial institutions to report the following information about BEC schemes to facilitate investigation.

[Table 7: Information about BEC schemes that FinCEN requests US-based financial institutions to report]

Transaction Details		Scheme details	
(1)	Dates and amounts of suspicious transactions	(1)	Relevant e-mail addresses and associated IP addresses with their respective timestamps
(2)	Sender's identifying information, account number, and financial institution	(2)	Description and timing of suspicious e-mail communications and involved parties
(3)	Beneficiary's identifying information, account number, and financial institution	(3)	Description of related cyber-events
(4)	Correspondent and intermediary financial institutions' information, if applicable	(a)	E-mail autoforwarding
		(b)	Inbox sweep rules or sorting rules
		(c)	A malware attack
		(d)	Authentication protocol that was compromised

#### 4.3. Cases of arrest

In 2018, the FBI cooperated with the law enforcement agencies and private organizations in a number of countries in a large-scale effort to dismantle international BEC schemes. This operation—named Operation WireWire—was carried out over a period of six months and resulted in 74 arrests in the US, Nigeria, Canada, Mauritius, Poland, and other countries.<sup>9</sup> In Operation reWired, undertaken a year later in 2019, a total of 281 arrests were made, including in Japan. In a different case reported the same year, the Tokyo

<sup>8</sup> Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes  
[https://www.fincen.gov/sites/default/files/advisory/2019-07-16/Updated BEC Advisory FINAL 508.pdf#page=9](https://www.fincen.gov/sites/default/files/advisory/2019-07-16/Updated%20BEC%20Advisory%20FINAL%20508.pdf#page=9)

<sup>9</sup> International Business E-Mail Compromise Takedown  
<https://www.fbi.gov/news/stories/international-bec-takedown-061118>

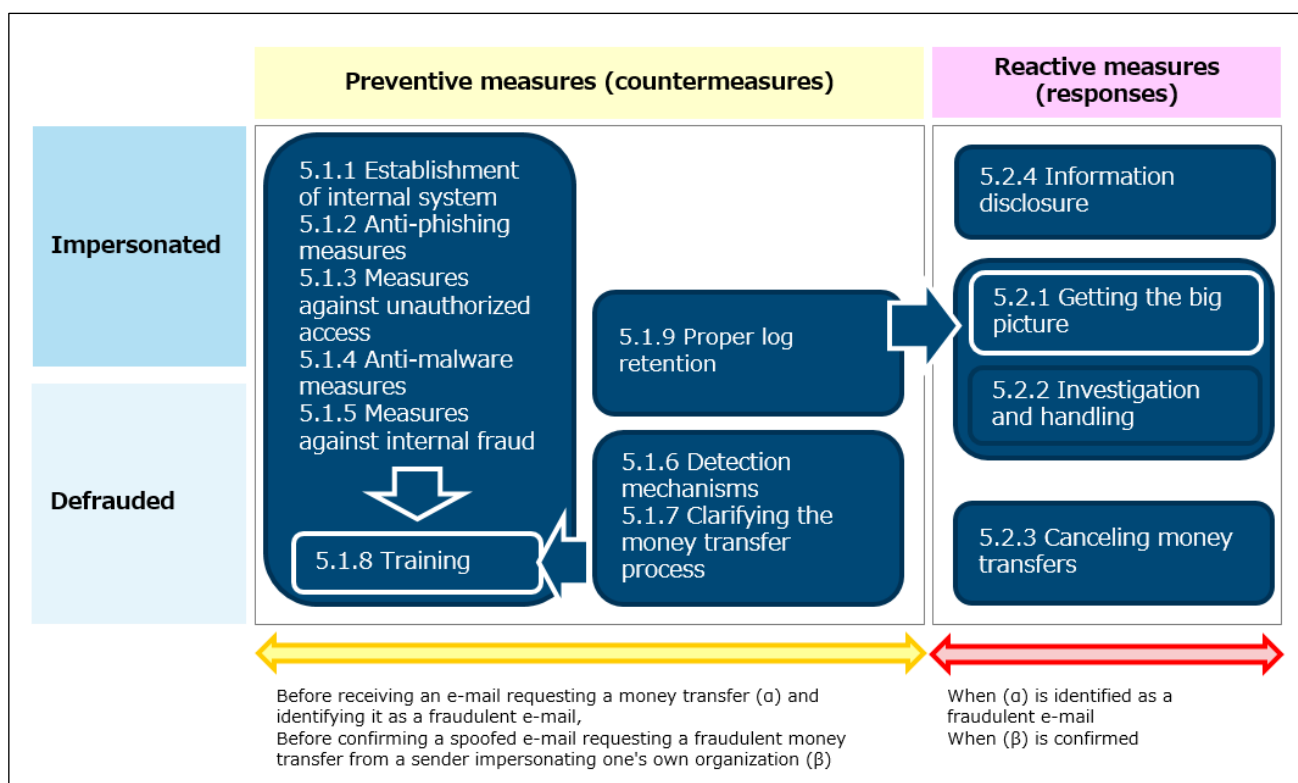
Metropolitan Police Department cooperated with the FBI in an investigation that resulted in the arrest of Japanese nationals suspected of helping an international criminal organization perpetrate a BEC scam. Cooperation with law enforcement agencies is essential to exposing cases of fraud like these. With respect to the threat of BEC as well, it is hoped that further cooperation between law enforcement agencies and private organizations will lead to more arrests and deterrence of criminal activities through announcement of arrests.

## 5. Countermeasures and Responses

BEC scams are difficult to prevent only with countermeasures implemented by the IT department. The accounting department which is responsible for transferring money must identify suspicious payment requests and ask the requesting party for confirmation. If a business partner incurs losses due to a BEC scheme in which the name of a department or individual of one's own company was used, the IT department may be able to prove the absence of negligence on the part of the company by analyzing logs and other data. In this manner, BEC must be handled as an issue for the entire organization by combining the technical knowledge and skills provided by the IT department with actions taken by relevant departments according to their functions.

This chapter discusses measures against BEC in terms of preventive measures (countermeasures) and reactive measures (responses).

While each organization has a different definition for incidents, this report categorizes preventive and reactive measures according to their timing, that is, whether they are taken before or after receiving an e-mail requesting a money transfer and identifying it as a fraudulent e-mail, or before or after confirming a spoofed e-mail requesting a fraudulent money transfer from a sender impersonating one's own organization.



[Figure 7: BEC countermeasures and responses]

## **5.1. Pre-incident measures (countermeasures)**

### **5.1.1. Establishment of internal system**

If the internal system and escalation rules for responding to confirmed or suspected cases of BEC are established, the organization can respond rapidly. With a shared awareness of the possibility of a BEC attack, organizations should establish a system that facilitates collaboration between the accounting department which requests financial institutions to make money transfers, IT department which is responsible for e-mail and system operation, legal department which responds when a case involves legal issues, and sales department which undertakes negotiations with outside business partners. As the survey results show, most BEC schemes occur outside Japan, so organizations should also have a communication system set up and tested with overseas locations.

### **5.1.2. Anti-phishing measures**

Organizations using Office 365 or other web-based e-mail services are at risk for having credentials stolen through phishing. When credentials are stolen and e-mail accounts are hijacked, attackers will be able to obtain full knowledge of communication with business partners based on past e-mail exchanges, and send e-mails masquerading as the account holder. Users should be trained and educated on how to identify phishing and prevent credentials from getting stolen.<sup>10</sup>

### **5.1.3. Measures against unauthorized access**

Authentication of e-mail accounts may be breached by a brute force attack or other means. To prevent e-mail accounts from getting hijacked, measures to enhance authentication such as the use of strong passwords, prohibition of reusing passwords, and introduction of multi-factor authentication are recommended for e-mail services.

### **5.1.4. Anti-malware measures**

There were some cases in which attackers used malware with a function for collecting information to steal relevant information from the target organization as a preparatory step for making a fraudulent money transfer request. For this reason, organizations must have measures in place to prevent malware infections and, in case of an infection, to detect malware communications with external servers.

---

<sup>10</sup> Anti-phishing Guidelines (Japanese)  
[https://www.antiphishing.jp/report/pdf/antiphishing\\_guide.pdf](https://www.antiphishing.jp/report/pdf/antiphishing_guide.pdf)

### 5.1.5. Measures against internal fraud

As discussed in "3.2.3.5 Possible involvement of parties familiar with internal affairs," the possibility of involvement of parties familiar with internal affairs cannot be denied in BEC scams in which attackers make repeated requests to different targets for varying amounts of payment. Parties familiar with internal affairs include officers, employees, former officers/employees, and business partners. When devising countermeasures, organizations should consider cases of both unintentional involvement and involvement as the main culprit or an accomplice.

Measures against cases of unintentional involvement include ensuring employees are fully aware that they must not leak internal information to outside parties, and restricting access rights so that only users who need to access or work with necessary information may do so. As for involvement in BEC schemes as the main culprit or an accomplice, it is not realistic to expect individuals who engage in such practices to act on their conscience. Therefore, organizations should show their stance toward internal fraud through penal provisions and so on, make it difficult to conduct criminal acts by restricting employees from bringing their own devices and storage media or by monitoring access logs, and reduce the reward that can be gained by engaging in criminal acts.

The "Guidelines for the Prevention of Internal Improprieties in Organizations"<sup>11</sup> published by IPA sets forth basic policies as well as specific measures including technological management, securing evidence, and follow-up measures. Please read it through when devising countermeasures.

As for former officers and employees, who rarely stay in touch with the organization once they have retired, it is desirable to take measures as much as possible while the individuals are employed. In addition to having them sign a written pledge and quickly deleting unnecessary IDs, more in-depth measures such as checking the operation logs of retiring employees for any improper removal of information are effective. Since the handling at the time of retirement may be more uncertain overseas than in Japan due to difference of customs, organizations should maintain active involvement with regard to overseas locations, for example, by requesting submittal of evidence indicating implementation of countermeasures targeting retirees.

### 5.1.6. Detection mechanisms

Although it would be possible to prevent losses from BEC scams if e-mails requesting fraudulent money transfers could be blocked and kept from reaching their intended recipients, most of them do not have any malware attached or contain any fraudulent URL and therefore cannot be mechanically removed or blocked using anti-virus software or other such means. Moreover, many scam e-mails are extremely sophisticated and made to look like legitimate business e-mails, making them difficult to filter as spam.

To detect BEC scam e-mails that reach an organization and prevent losses, it might help recipients

---

<sup>11</sup> Guidelines for the Prevention of Internal Improprieties in Organizations  
<https://www.ipa.go.jp/files/000045873.pdf>



recognize e-mails requesting fraudulent money transfers by visually alerting them using system functions, such as attaching a warning to e-mails sent from a free e-mail address, or displaying a message when an e-mail is received from a domain not used in recent transactions.

In addition to technological measures, an approach from the aspect of operational processes would also be effective. In light of the fact that BEC scams take place in the course of a business process, having relevant personnel compare the process with the proper business process might facilitate identification of suspicious details. Specifically, it would be effective to create a check sheet that lists the details of a past transaction and the transaction instructed in an e-mail, and check for any differences. From the perspective of detecting BEC at an early stage, it is important for check sheets to be created and verified by recipients of billing e-mails and secondary reviewers.

[Table 8: Check items for detecting BEC]

	Existing Transaction (Normal)	E-mail Subject to Investigation	Anomaly
<b>(1) Requesting party</b>			
Sender's organization	XXX Co., Ltd.	XXX Co., Ltd.	□
Sender's name	Mr./Ms. ABC	Mr./Ms. ABC	□
Sender's phone number	(xx) xxxx-xxxx	(xx) xxxx-xxxx	□
Recipient's e-mail address	tantou@△△△cert.or.jp	tantou@△△△cert.or.jp	□
Sender's e-mail address * Taken from the e-mail header due to possibility of forgery	abc@□□□tech.com	abc@□□□tach.com	■
<b>(2) Payment and account information</b>			
Payment amount	7,800,000 yen (incl. tax)	7,800,000 yen (incl. tax)	□
Financial institution	XXX Bank	YYY Bank	■
Payment recipient account information (location)	AAA Branch (Country A)	BBB Branch (Country B)	■
Account number	xxx-xxxxxxxx	yyy-yyyyyyy	■
<b>(3) Related information</b>			
■ Time zone			
Date/time e-mail was sent	+0900 UTC	+0100 UTC	■
Date/time attachment was created	+0900 UTC	+0100 UTC	■
<b>(4) Notes and findings</b>			
<ul style="list-style-type: none"> <li>● The payment recipient's financial institution, account information, and sender's e-mail address are different from those used in the existing transaction.</li> <li>● The information security department has confirmed that the dates and times the e-mail was sent and the attachment file was created are in a different time zone from the existing transaction.</li> <li>● It appears that a third party is impersonating XXX Co., Ltd. and requesting the recipient to make a money transfer.</li> <li>● Since the third party is impersonating Mr./Ms. ABC of XXX Co., Ltd. and requesting payment of the same amount of money as before (7,800,000 yen, including tax), there is a possibility that the third party has obtained information about the existing transaction.</li> <li>● Both e-mail addresses need to be checked for a possible breach. <ul style="list-style-type: none"> <li>➢ tantou@△△△cert.or.jp</li> <li>➢ abc@□□□tech.com</li> </ul> </li> </ul>			

**5.1.7. Clarifying the money transfer process**

E-mails requesting fraudulent money transfers use various techniques to "trick" the recipient. The text is often written in a way that unsettles the recipient, for example, by claiming that payment is needed urgently to rush the recipient, or impersonating a superior or executive to pressure the recipient. To prevent being tricked into sending money by such tactics, it is necessary to incorporate a system that enables secondary review from an objective standpoint into the company's money transfer process. It goes without saying that money transfers should always be processed well ahead of the schedule.

**5.1.8. Training**

Generally, security measures do not achieve sufficient results due to a lack of awareness on the part of the users, lack of understanding of specific steps for implementing the measures, and so on. To put users on the alert, and have them learn the way to address the threat, repeated training is needed.

As for measures against BEC, it is important to alert the users of the possibility of getting involved in a scam, and have them understand the key points that they should look out for to avoid being tricked by highlighting some of the typical methods used.

The table below lists some telltale signs that help identify BEC scam e-mails according to findings from this survey.

[Table 9: Telltale signs that help identify e-mails and messages related to BEC]

<input type="checkbox"/>	Routine e-mail sent from an e-mail address different from the one used before
<input type="checkbox"/>	Routine e-mail sent during different hours or with different text (wording, expressions, etc.) from previous messages
<input type="checkbox"/>	E-mail is received near the end of business hours or right before the weekend, and requests an irregular handling at a rush
<input type="checkbox"/>	First e-mail received from a company with no past dealings
<input type="checkbox"/>	E-mail received from a superior or executive giving instructions, with no prior contact by a means other than e-mail
<input type="checkbox"/>	Money transfer is being requested to an account never used before

By highlighting telltale signs like these along with actual case examples, it is possible to cultivate skills for identifying BEC. Moreover, by requiring the use of the check sheet discussed in "5.1.6 Detection mechanisms" when the personnel who receive e-mails from outside the company requesting money transfers request the responsible department to send money, it is possible to raise the detection rate of BEC.

Even e-mails like those shown in Table 9 could be legitimate business e-mails unrelated to BEC, it is desirable to suspect BEC then check with the other party using a means other than e-mail (e.g., by phone

or in person). While such measures may take time and effort, the other party will most likely show understanding as rational precaution. It must also be ensured through training that, when checking by phone, the relevant personnel use a phone number obtained by exchanging name cards or other means, not the contact number given in the e-mail requesting a money transfer.

### 5.1.9. Proper log retention

During the course of incident handling, operation logs and other records are checked to understand the situation or as part of the investigation. BEC is no exception. If e-mail and system logs are not properly retained, it may not be possible to identify the cause or understand the situation. In one case, for example, the audit logs of e-mail accounts were not properly recorded, so only recent login history was available, and the evidence of an account breach by an attacker could not be confirmed. In another case, the recipient deleted a suspicious e-mail, making subsequent investigation difficult.<sup>12</sup>

In impersonated cases, retention of e-mail and system logs are important from the perspective of dealing with external parties as well. When the defrauded organization claims compensation for damages, it is up to the impersonated organization to prepare evidence to counter the claim.

If one's own organization was tricked into transferring money and wishes to request cancellation of the money transfer, the financial institution may request grounds for cancellation (e.g., data proving that the transaction in question was made in connection with a BEC scam). Accordingly, data such as e-mail and system logs might later be necessary to understand the situation or negotiate with external parties, so it is desirable to establish rules for retention and properly retain relevant data.

Specifically, e-mail logs and e-mail account audit logs including login history should be obtained, given that BEC takes place via e-mail. It is also recommended that communication logs of proxy servers, firewalls, and so on and operation logs such as Active Directory be obtained, assuming that other incidents may be related.

Note that it might be necessary to configure settings to output logs, and it is also necessary to secure a place for storing logs. Retention period is another issue that must be considered along with the storage location. Given that losses from BEC come to light when an outstanding payment is pointed out, the investigation covers a relatively short time period. However, when investigation of related incidents is taken into account, logs must be examined for a considerable period of time.

JPCERT/CC recommends that logs be retained for at least one year taking advanced cyber attacks (APT attacks) into account, based on its experience supporting incident response. A similar retention period would be appropriate for BEC as well.<sup>13</sup>

---

<sup>12</sup> Incident Response Casefile – A successful BEC leveraging lookalike domains  
<https://research.checkpoint.com/2019/incident-response-casefile-a-successful-bec-leveraging-lookalike-domains/>

<sup>13</sup> How to Use and Analyze Logs in Dealing with Advanced Cyber Attacks (Japanese)  
<https://www.jpCERT.or.jp/research/apt-loganalysis.html>  
Preparing for Advanced Persistent Threats (APT): A Process Guide for Companies and Organizations (Japanese)  
<https://www.jpCERT.or.jp/research/apt-guide.html>

## 5.2. Reactive measures (responses)

### 5.2.1. Getting the big picture

When an e-mail requesting a fraudulent money transfer is identified, or when a spoofed e-mail requesting a fraudulent money transfer from a sender impersonating one's own organization is confirmed, the following matters must be sorted out with the aim of obtaining an accurate understanding of the situation and clarifying actions to be taken.

#### 1) Big picture

As recent cases of BEC sometimes involve multiple persons and/or organizations on one side or both sides, get the big picture of the incident by identifying all the actors and clarifying how they relate to each other. Using a relationship diagram to visualize the relationships will not only make it easier to understand the situation, but it will also help prevent misunderstanding between personnel.

#### 2) Organization's position

After grasping the big picture, determine whether one's own organization received a BEC scam e-mail or was impersonated. In the former case, check if any money transfer was made. If yes, immediately take steps to cancel the money transfer linked to BEC as described later in 5.2.3. In the latter case as well, check if any money transfer was made by the defrauded party. If yes, immediately instruct the party to cancel the money transfer to the financial institution. The impersonated organization should check the sending domain of the spoofed e-mail regardless of whether the business partner made any money transfer, and see if it is the domain the organization uses for business operations. It should also make preparations for information disclosure (see "5.2.4 Information disclosure when impersonated in a BEC scheme"). If an e-mail requesting a fraudulent money transfer was sent from an e-mail address with the domain used for business operations, it is highly likely that an e-mail account of the organization had been breached, so the steps described in "5.2.2 Investigation and handling of prior incidents" should be initiated.

#### 3) Existence of internal information

Check if information used for carrying out a BEC scam includes information that only a business partner or internal staff can know. If such information is included, there is a possibility that the attacker may have viewed e-mails, or information may have leaked due to other incidents, so the steps described in "5.2.2 Investigation and handling of prior incidents" should be initiated.

These steps should be undertaken by checking e-mail logs and the content of the e-mail requesting a money transfer, and by interviewing the e-mail recipient. If the check sheet discussed in "5.1.6 Detection

mechanisms" is used regularly, it can be used to understand the situation with efficiency as relevant information is already compiled.

### **5.2.2. Investigation and handling of prior incidents**

Once the situation is understood, take necessary steps such as changing the passwords of relevant e-mail accounts assuming they are compromised. In particular, if the e-mail contains details concerning internal information unique to the organization such as internal rules, there is a possibility that the attacker has already obtained information about the organization. In that case, the attacker may have viewed past e-mail exchanges, so the accounts of relevant persons at the organization and business partner need to be checked for a possible breach of account. If e-mail accounts have been compromised, account settings need to be reviewed in addition to changing passwords as e-mail forwarding, removal of received e-mails, and other such settings may have been added. Incident response such as identifying the cause of account breach and information leakage (e.g., phishing, unauthorized access, and malware infection) should be undertaken.

### **5.2.3. Canceling money transfers made in response to BEC**

It might be possible to cancel money transfers by making a request to the relevant financial institution. If a money transfer was requested to a financial institution unaware that it was a BEC scam, it is recommended that the financial institution be contacted immediately. To cancel the money transfer, the financial institution might request submittal of information proving the existence of a BEC scheme, investigation results as well as retained e-mails and logs should be prepared.

### **5.2.4. Information disclosure when impersonated in a BEC scheme**

When it is revealed through external notification or inquiry that one's own organization has been impersonated in a BEC attempt, it is vital to disclose relevant facts as quickly as possible to prevent the spread of damages assuming the possibility that similar attempts are being made against a wide range of organizations. The information to be disclosed should include specific details such as the sender's e-mail address (extracted from the e-mail log considering the possibility of forgery) and payment recipient's account information (bank name, branch name, account number, account holder's name), so that organizations that received the information may use it to conduct investigation and alert their employees. Information may be disclosed, for example, by sending individual notifications to business partners by e-mail or other means, or issuing an alert on the website.

## 6. Conclusion

This survey helped clarify the losses incurred in connection with BEC, countermeasures implemented, and three points that should be noted with regard to BEC, namely, that multiple actors and/or organizations may be involved, that there may be a prior related incident, and that a victim may also be a perpetrator. To prevent losses from BEC, organizations should act with these points in mind.

Countermeasures must address the risk of being impersonated as well as being tricked. One of the organizations that participated in this survey monitors the registration status of domains that resemble its domain as a measure against spoofing. This approach entails considerable operation costs, and its effectiveness including feasibility depends on the organization's resources. Protecting accounts from attackers by means of common security measures against phishing, unauthorized access, and malware is also an effective way to address the risk of being impersonated. In addition, organizations are advised to retain e-mail and system logs in a proper manner in case they become victims of a BEC scam. E-mail and system logs not only serve as evidence in case an organization is impersonated, but they also can be used in internal investigation and negotiations with external parties when defrauded.

As BEC scam e-mails do not always contain elements that can be filtered by a system, it is difficult to block them before they reach the organization. To prevent being tricked under these circumstances, it would be effective to create a mechanism for detecting e-mails that are not expected to be received. As discussed in this report, possible detection methods include displaying a warning when an e-mail is received from a free e-mail address and other system-based support. However, it is also important to approach this risk with operational measures, such as having personnel familiar with the transaction details or personnel responsible for processing payments perform a secondary check. This means that BEC is a problem to be addressed not just by the IT department alone but by the organization as a whole. Perhaps, one may even go further and say that BEC, which causes damage to an organization through financial losses, is a management issue that requires management's active involvement.

This report was prepared with the aim of helping reduce losses linked to BEC, which is affecting an increasing number of Japanese organizations. The report focuses on specific measures that organizations should take when engaging in a business transaction. We hope that this report will be used by organizations planning to implement measures against BEC and address its threat by ensuring the abovementioned points are covered. As for organizations that already have countermeasures in place, it might offer hints for improvements through comparison with existing measures.

Given the nature of BEC, which is a criminal act and fraud committed with the aim of stealing money, and its sophisticated techniques, efforts on the part of target organizations alone are not sufficient to reduce it. To prevent BEC-related losses, law enforcement agencies, e-mail providers, and financial institutions will also need to cooperate by inhibiting criminal acts through crackdowns on attackers and other efforts,

suspending fraudulent e-mail accounts used to carry out BEC scams, and freezing bank accounts. We hope that public institutions and private organizations in Japan will join hands and set up an environment for combating BEC, like The Business Email Compromise List overseas. Once we have set up such an environment, we would like to ask our readers to share information and make active use of it.



**7. Acknowledgment**

In closing, we would like to thank the organizations and their representatives who offered valuable input by taking part in the survey questionnaire and interviews. We also offer thanks to Mr. Motohiko Sato of Itochu Corporation, who serves on JPCERT/CC's expert committee, Mr. Nozomi Matsuzaka and Ms. Tomoko Takeuchi of IPA, and Mr. Kenzo Masamoto of Macnica Networks for their invaluable help in writing and editing this report.