Risk Assessment of "Ostrich ZIP"

Michihiro Nakayama and Akira Kanaoka(✉)

Toho University, Miyama 2-2-1, Funabashi Chiba 274–8510, Japan
akira.kanaoka@is.sci.toho-u.ac.jp

Abstract. When sending highly confidential information by e-mail, there is a method of attaching a ZIP file encrypted with a password to the e-mail, and then sending the password for decryption separately by e-mail, which is the same channel. We named this method "Ostrich ZIP". While Ostrich ZIP method is used to protect information through encryption and to prevent misdirection, its meaning is sometimes questioned. However, it is difficult to say that these discussions have been organized. In this paper, the advantages, disadvantages, and threats of Ostrich ZIP are summarized based on these discussions, and the current situation is clarified by surveying the environment related to Ostrich ZIP. In addition, we construct an information leakage event model for file sharing when sending and receiving e-mails, and evaluate and discuss the information leakage risk of ostrich ZIP and alternative measures based on the model. Finally, the background of the use of the ostrich ZIP is discussed from institutional and other perspectives, adding another perspective along with the information leakage risk results. This paper will be provided as a comprehensive risk assessment of the ostrich ZIP.

Keywords: Encrypted ZIP · Passwords

1 Introduction

Information sharing has become an indispensable part of social activities using PCs, smartphones, and the Internet. In sharing information, we do not need to discuss the importance of delivering information to the right person and disclosing information only to the right person.

E-mail has been used as a channel for information sharing for a long time. It is achieved by attaching electronic files saved or created on a PC or smartphone to the e-mail. Since the SMTP used to send and receive e-mails does not have its data protection mechanism, the contents can be viewed by a third party. A protection mechanism must be applied to the data being sent and received separately to protect the information.

One way to protect email attachments is to use ZIP, an archive format that combines multiple files into a single file. ZIP is widely used because it supports compression and encryption of archived contents. Various operating systems support archive decompression as a standard feature, making it convenient to use without installing special applications.

A. Moallem (Ed.): HCII 2021, LNCS 12788, pp. 76–90, 2021.
https://doi.org/10.1007/978-3-030-77392-2_6

When protecting data in file sharing via e-mail, a ZIP file encrypted using this encryption function is sometimes used. Such a ZIP file will be referred to as an encrypted ZIP file in this paper. This file is encrypted, so a key is required to decrypt it. It is common for ZIP files to be encrypted with a password as the key. When an encrypted ZIP file is attached to an e-mail, the key to decrypt it must be shared somehow. The password, which is the key for its decryption, is often sent separately in plain text in another email on the same channel. While this method of sending an encrypted ZIP file as an attachment to an e-mail and sending the decryption password in a separate e-mail is widely used, many doubts about its data protection have been raised.

In this method, passwords are sent through the same channel, and passwords are sent separately near the e-mail with the encrypted ZIP attached. It is imagined that the level of data protection by encryption is lower than what is expected because the key protection is not sufficient. Many of the users of this method are aware of this low level of data protection. Still, they use it because of their organization's rules, the requirements of the recipient organization, and social requirements. We believe that they are operating under the Ostrich Policy, which means escape from reality or self-deception. We call this method the "Ostrich ZIP".

While Ostrich ZIP's advantages and disadvantages have been discussed from various viewpoints, it is difficult to say that there is any literature that organizes them. Therefore, in this paper, we first organize these discussions and clarify the advantages, disadvantages, and threats. Then, Ostrich ZIP's current status is surveyed for typical OSs, software, and Web services. Then, we propose an information leakage event model for file sharing when sending and receiving e-mails, evaluate the information leakage risk of ostrich ZIP and alternative measures based on the proposed model, and compare and discuss the results.

2 Organizing the Ostrich ZIP Discussion

There are already many criticisms of the Ostrich ZIP [1–4]. On the other hand, these criticisms cover multiple viewpoints and are not the same criticism. Therefore, it has not been sufficiently organized, including risk assessment. In this study, we will first conduct a literature review, including academic literature, a survey of discussions on the Web to organize the ostrich ZIP debate, and then organize the advantages and disadvantages, threats, and background to its use, alternative methods, and risk assessment listed therein.

2.1 Literature Review

The literature review was conducted using the free word search function of CiNii[1]. We selected "misdirection," "encrypted e-mail," and "information leak prevention e-mail" as keywords for the search. A total of 136 documents were obtained from the search using each search keyword, but there were no academic discussions about this study.

[1] https://ci.nii.ac.jp/.

2.2 Web Survey

In the survey using Web search, we used Google search. We selected "encrypted ZIP file separate mail," "encrypted ZIP sending later," and "ZIP file business with password" as keywords and searched. The keywords were set to Japanese, and only Japanese web pages were used for the survey. As a result of the search, many results were obtained, of which the contents were carefully examined. The contents of 11 articles, in particular, were organized.

2.3 Advantages of Ostrich ZIP

The advantages of Ostrich ZIP obtained as a result of the survey include "countermeasures against erroneous transmissions (10 cases)," "reduction of the risk of information leaks by password protection (3 cases)," "use of only e-mail and ZIP files and no need to introduce new technology (1 case)," "reduction of the risk of route eavesdropping by separate delivery (1 case)," and "support for AES encryption of ZIP specifications (1 case)". Based on the above, we identified the following advantages of the ostrich ZIP. The merits of the effect are not discussed here.

- Countermeasures against missending: Opportunity to notice missending when sending passwords separately
- Eavesdropping prevention: Data protection with encrypted ZIP makes sense for eavesdropping prevention
- Environment-independent: Extraction of encrypted ZIP files is less dependent on the environment

2.4 Disadvantages of Ostrich ZIP

As the disadvantages of ostrich ZIP obtained from the survey, the following were cited: "the anti-tapping effect is weak due to the use of the same channel (4 cases)," "the anti-missending effect of the automatic ostrich ZIP file support is weak (2 cases)," "vulnerability of the ZIP specification (2 cases)," "encryption makes security scanning on the mail server impossible (2 cases)," and "eavesdropping by the server (1 case)". Based on these, we put the advantages of Ostrich ZIP as follows. As with the advantages, the merits of the effect are not discussed here.

- The Dangers of Email Eavesdropping
- Decrease in the significance of using the same channel to prevent miscommunication
- Low strength of encrypted ZIP files

The point that security scan becomes impossible is not a disadvantage of Ostrich ZIP because it covers not only Ostrich ZIP but also multiple methods such as encrypted ZIP files, mail encryption by PGP or S/MIME, and the use of file sharing services such as online storage services. E-mail eavesdropping by the server was likewise determined not to be an inherent disadvantage of Ostrich ZIP.

2.5 The Ostrich ZIP Threats

Two threats to the ostrich ZIP were identified as a result of the survey.

- Eavesdropping by a malicious third party
- Missending of e-mail

2.6 Background of Ostrich ZIP Usage

7 of the 11 Web articles mentioned "meeting the PrivacyMark[2] and ISMS certification" as the background of using the Ostrich ZIP obtained as a result of the survey.

2.7 Alternative Methods for Ostrich ZIP

As the alternative methods of ostrich ZIP obtained from the survey, "PGP or S/MIME (3 cases)", "Online storage service (3 cases)", "Automation of ostrich ZIP (1 case)", "Tell the password by phone (1 case)", "Mail the password (1 case)", "Give the password in person (1 case)" were listed. Based on these results, we put the alternative methods to ostrich ZIP as follows. The merits of the effect are not discussed here.

- PGP and S/MIME
- Sending passwords through a different route
- File sharing services, online storage services
- Automatic ostrich ZIP

The method that automatically encrypts ZIP processing of the attached file and sends the password is called automatic ostrich ZIP.

3 Survey on the Current Status of the Ostrich ZIP

In this section, we investigated the surrounding environment related to the ostrich ZIP as a material to explore the background of the ostrich ZIP. In this section, a survey of the surrounding environment related to the Ostrich ZIP is conducted as a material to explore the background of the ostrich zip's use.

3.1 Specification

The ZIP specification is provided by PKWARE and has been standardized as ISO/IEC 21320-1:2015. The encryption is based on the symmetric key cryptographic algorithm Traditional PKWARE Encryption (TPE), which was later modified to allow other cryptographic algorithms such as AES.

TPEs are already known to be vulnerable, and it has been reported that they can be easily decrypted in a commercial environment by running the open-source software Hashcat on a GPU-equipped computer [5].

[2] The PrivacyMark is a reputable privacy-centric certification in Japan. https://privacymark.org/.

Table 1. Results of survey on the actual status of ZIP files encrypted by OS

OS	Generation	Default algorithm	Expansion	OS Details
Windows	✓	–	Only TPE	Windows10 pro
macOS		TPE	Only TPE	macOS Mojave 10.14.6
Raspbian OS		TPE	Only TPE	Linux4.14.98-v7, Raspbian OS: 9.8

3.2 Encrypted ZIP Support in Typical Environments

One of the advantages of Ostrich ZIP was its environment-independence. Here, the results of a survey on how encrypted ZIPs are supported in typical environments are reported.

Support by OS. Windows 10, Mac OS X, and Raspbian OS were selected as the target operating systems, and encrypted ZIP creation, decompression, and the default encryption algorithm at the time of creation were investigated. In the case of generation, it was investigated whether it was possible to generate encrypted ZIPs without installing any special software after installation. The cryptographic algorithm information used in the generated encrypted ZIP was obtained from the ZIP file's binary data. For decompression, two types of encrypted ZIP files (encrypted with TPE and encrypted with AES) were prepared in advance, and it was investigated whether decompression was possible for each. Since the Raspbian OS usually has zip software installed at the time of installation, the generation and decompression were investigated using this software.

The results are shown in Table 1. It can be seen that in both OS environments, only TPE is deployed.

A survey was also conducted on iOS and Android OS, which are the leading operating systems used in mobile devices. For the mobile OS, it was investigated whether it was possible to generate encrypted ZIPs. It was confirmed that it was not possible to generate encrypted ZIPs in both the Android 7.0 environment and iOS 13.2.

Typical Software Support. It was investigated whether it is possible to create encrypted ZIPs for four typical e-mail software (Microsoft Outlook 2016 16.0.4266.1001, Mozilla Thunderbird 68.2.2, Apple Mail 12.4, and Becky! Internet Mail 2.74.03). As a result, it was confirmed that none of the software had the function to generate encrypted ZIPs.

Support by Typical Webmail Services. E-mail is increasingly being used by Web services via browsers. Therefore, it was investigated whether it is possible

to create encrypted ZIPs for the representative web services, Google's Gmail and Yahoo! The survey was conducted on November 13, 2019. As a result, it was confirmed that there is no function to generate encrypted ZIPs for either service.

3.3 Automatic Ostrich ZIP

The ostrich ZIP requires both the sender and receiver to perform the encryption and decryption process, which is more burdensome than sending and receiving plaintext e-mail. A mechanism can reduce the burden on the sender by automatically encrypting and decrypting the attached file and sending the password. We call it automatic ostrich ZIP.

There are several services and solutions for automatic ostrich ZIP. Depending on the type of automation, there are three main types of automated ostrich ZIPs: gateway ostrich ZIPs, client ostrich ZIPs, and mail server ostrich ZIPs.

Gateway-type automatic ostrich ZIP is a device or service dedicated to encrypted ZIP between the mail server and the sender. Client-based automatic ostrich ZIP automatically performs encrypted ZIP by installing it in the sender's environment. A mail server type automatic ostrich ZIP includes a function to perform automatic ostrich ZIP.

In our research, we found 10 automatic ostrich ZIP solutions. 6 of them were gateway type, 2 were client type, and 2 were mail server type. Besides, 4 of the 10 solutions claimed to support cryptographic algorithm changes.

We also investigated the encryption algorithms of 10 types of e-mails that the authors had received, which were supposed to have been sent by automatic ostrich ZIP. The encrypted ZIP files sent by the same sender were counted as one type. The results showed that all of them were encrypted by TPE.

4 Model of Information Leakage Events in File Sharing During E-Mail Sending and Receiving

To evaluate Ostrich ZIP's risk, an information leakage event model for file sharing during e-mail sending and receiving is proposed, which enables evaluation, including alternative methods. In proposing the model, the threats are limited to information leakage during e-mail transmission and reception, based on the advantages and disadvantages of ostrich ZIP that have been discussed.

First, the events related to information leakage via e-mail are listed and named. Second, the probability of information leakage in various e-mail usage situations, including Ostrich ZIP and alternatives, is represented using combinations of events. Finally, the probability models are simplified, and the probability of information leakage for each method is compared by entering actual values.

4.1 Events Related to Information Leakage via E-Mail

Table 2 shows the events related to information leakage by e-mail. Each event is based on "missending" and "eavesdropping," which were raised as threats of

the Ostrich ZIP. Authors examined and listed the events where missending and eavesdropping could occur between sending and receiving e-mail. Each event was assigned an event ID from a to i.

Table 2. Information leakage events by e-mail including ostrich ZIP

Event ID	Information leakage event by e-mail
a	Missending
b	Eavesdropping on mail server
c	Eavesdropping on communication channels
d	Eavesdropping from outside the mail server or communication channel
e	Be aware of missending when sending passwords separately
f	Decryption of encrypted ZIP files by malicious third parties
g	Missending e-mail and sending the password to the erroneous recipient through a different channel
h	Incorrectly selecting a publickey, and its owner is the same as the user to whom the mail was sent in error
i	Incorrectly selecting a user who is allowed to access cloud storage, and that user is the same as the user to whom the mail was sent in error

4.2 Situation of E-Mail Use and Incidents of Information Leakage

Table 3 shows the situations of e-mail use and the events of information leakage under these situations, evaluated as a combination of events.

For the e-mail usage situation, the authors listed in advance factors such as the presence or absence of attachment protection, file sharing methods The presence or absence of communication channel encryption, and the usage situation was subdivided according to each difference. For each usage situation, the events that cause information leakage were represented by the combination of events from a to i listed in Table 2.

4.3 Event Model and Simplified Probability of Leakage Occurrence for Each Leakage Case

Next, the probability of each leakage case defined in Table 3 is examined. Each of the events listed in Table 2 cannot be considered to occur independently It is difficult to calculate the probability of occurrence of each leakage case. However, we believe that even a simplified model has a particular significance, so the simplified probability is obtained by assuming that each event's occurrence is independent. The equations for each leak occurrence case and probability are shown in Table 4.

Table 3. Status of e-mail use and cases of information leakage

Case ID	E-mail usage	Event
1	Send attachments without encryption + without SSL/TLS	$a \cup b \cup c \cup d$
2	Send attachments without encryption + SSL/TLS	$a \cup b \cup d$
3	Send as ostrich zip + no SSL/TLS	$(e^- \cap (a \cup b \cup c \cup d)) \cup (e \cap f \cap (b \cup c \cup d))$
4	Send as ostrich zip + with SSL/TLS	$(e^- \cap (a \cup b \cup d)) \cup (e \cap f \cap (b \cup d))$
5	Send with auto ostrich zip + no SSL/TLS	$a \cup b \cup c \cup d$
6	Send as auto-ostrich ZIP + SSL/TLS available	$a \cup b \cup d$
7	Send encrypted ZIP passwords via alternative channels (SMS, mail, phone) + SSL/TLS available	$(a \cap g) \cup (f \cap (b \cup d))$
8	Sending encrypted mails by PGP and S/MIME + SSL/TLS available	$a \cap h$
9	Send shared URL and password for link protection in a single email + SSL/TLS	$a \cup b \cup d$
10	Send the shared URL and password for link protection in separate emails + SSL/TLS	$e^- \cap (a \cup b \cup d)$
11	Send shared URLs and passwords for link protection via a separate route from email + SSL/TLS	$a \cap g$
12	Send shared URL and password (link protected + encrypted ZIP) in a single email + SSL/TLS	$a \cup b \cup d$
13	Send shared URL and password (link protected + encrypted ZIP) via email + SSL/TLS respectively	$e^- \cap (a \cup b \cup d)$
14	Send shared URL (without link protection) and encrypted ZIP password in a single email + SSL/TLS	$a \cup b \cup d$
15	Send shared URL (without link protection) and encrypted ZIP password respectively by email + SSL/TLS	$e^- \cap (a \cup b \cup d) \cup (e \cap f \cap (b \cup d))$
16	Send shared URLs (without link protection) and encrypted ZIP passwords via a separate route from email + SSL/TLS	$(a \cap h) \cup (f \cap (b \cup d))$
17	Send shared URLs (without link protection) in a single email + SSL/TLS	$a \cup b \cup d$
18	Online storage with access control + encrypted ZIP password sent by email + SSL/TLS	$a \cap i$

Table 4. Event model and simplified probability of leakage for each leakage case

Case ID	Event	Probability of an event occurring
1	$a \cup b \cup c \cup d$	$P(a) + P(b) + P(c) + P(d)$
2	$a \cup b \cup d$	$P(a) + P(b) + P(d)$
3	$(e^- \cap (a \cup b \cup c \cup d)) \cup (e \cap f \cap (b \cup c \cup d))$	$P(e^-)(P(a) + P(b) + P(c) + P(d)) + P(e)P(f)(P(b) + P(c) + P(d))$
4	$(e^- \cap (a \cup b \cup d) \cup (e \cap f \cap (b \cup d))$	$P(e^-)(P(a) + P(b) + P(d)) + P(e)P(f)(P(b) + P(d))$
5	$a \cup b \cup c \cup d$	$P(a) + P(b) + P(c) + P(d)$
6	$a \cup b \cup d$	$P(a) + P(b) + P(d)$
7	$(a \cap g) \cup (f \cap (b \cup d))$	$P(a)P(g) + P(f)(P(b) + P(d))$
8	$a \cap h$	$P(a)P(h)$
9	$a \cup b \cup d$	$P(a) + P(b) + P(d)$
10	$e^- \cap (a \cup b \cup d)$	$P(e^-)(P(a) + P(b) + P(d))$
11	$a \cap g$	$P(a)P(g)$
12	$a \cup b \cup d$	$P(a) + P(b) + P(d)$
13	$e^- \cap (a \cup b \cup d)$	$P(e^-)(P(a) + P(b) + P(d))$
14	$a \cup b \cup d$	$P(a) + P(b) + P(d)$
15	$e^- \cap (a \cup b \cup d) \cup (e \cap f \cap (b \cup d))$	$P(e^-)(P(a) + P(b) + P(d)) + P(e)P(f)(P(b) + P(d))$
16	$(a \cap h) \cup (f \cap (b \cup d))$	$P(a)P(h) + P(f)(P(b) + P(d))$
17	$a \cup b \cup d$	$P(a) + P(b) + P(d)$
18	$a \cap i$	$P(a)P(i)$

5 Leakage Risk Assessment Using Event Models

In this section, the risks of Ostrich ZIP and its alternatives are evaluated by defining specific numerical values for the occurrence probability of each event and obtaining the occurrence probability of each case for the simplified probability formula obtained in Table 4.

It is difficult to obtain the true value of the occurrence probability of each event, and it is also difficult to obtain an approximate or guess value that can serve as an indicator. Therefore, the authors decided to set the values based on their considerations. However, the values set by the authors could not eliminate bias. Therefore, the set of probability values prepared by the authors is used as a baseline, and a set of probability values that consider situations where the attacker has an advantage compared to the baseline, and a set of probability values that show a strong effect of Ostrich ZIP are prepared, and by comparing

them, the risks of the ostrich ZIP and alternatives are compared. The three sets of probability values are shown in Table 5.

Table 6 shows the three sets of probability values. In situations where the attacker has an advantage, the probability values of events c "Eavesdropping on communication channels" and f "Decryption of encrypted ZIP files by malicious third parties" were increased. On the other hand, in the situation where Ostrich ZIP is effective, the probability of event e "Be aware of missending when sending passwords separately" is increased and the probability of event f "Decryption of encrypted ZIP files by malicious third parties" is decreased. Table 6 shows the probability of occurrence of each leakage case obtained by these values.

Comparing the probability of a leak occurring in Case 3 "Sending with ostrich ZIP + no SSL/TLS" and Case 4 "Sending with ostrich ZIP + SSL/TLS", there is no significant difference between the baseline value set of 0.0109 and 0.0100. It is assumed that the application of SSL/TLS to the communication channel prevents the occurrence of event c, but it is shown that the effect is not strong.

For the valid set of numbers, the results are 0.0056 and 0.0111, and if we assume that the ostrich ZIP is valid, the difference in probability itself is small, but it is almost double the value, which can be said to be an obvious result.

There is a difference in automating the generation and sending of passwords between Case 4 "Sending by ostrich ZIP + with SSL/TLS" and Case 6 "Sending by automatic ostrich ZIP + with SSL/TLS". It can be seen that there is no significant difference in the probability of a leak, 0.0100 and 0.0111 in the baseline set of values. Also, the probability of information leakage in case 6, "Sending with automatic ostrich ZIP + SSL/TLS", is the same as that in case 6, "Sending attachments without encryption + SSL/TLS". In the proposed model, there is no change in the risk of information leakage, indicating that auto-ostrich ZIP is not effective against information leakage in e-mail sending and receiving.

Compared to Case 4, "Sending encrypted ZIP + SSL/TLS", there is a difference between Case 7, "Sending encrypted ZIP + SSL/TLS", which uses encrypted ZIP, and Case 4, "Sending encrypted ZIP + SSL/TLS", in that the password for decryption is sent through a different route. Looking at the probability of leakage, we can see that there is a difference of 0.0001 and 0.0100 in the baseline set of values. This value is about 1/100, indicating that sending passwords through a different route is highly effective. In the same way, we can see that the probability of a leak occurring in case 11, "Sending a shared URL and password for link protection via a separate route from e-mail + SSL/TLS," and case 16, "Sending a shared URL (without link protection) and encrypted ZIP password via a separate route from e-mail + SSL/TLS," in which passwords, etc. are sent via a separate route, are smaller than the other cases. The probability of occurrence is small compared to other cases, indicating that sending the password through a separate route is highly effective.

There is a difference between the case 8 "Sending encrypted mails with PGP and S/MIME + SSL/TLS" and the case 4 "Sending encrypted mails with ostrich ZIP + SSL/TLS" in that a different method is used for encryption. Looking at the probability of leakage, we can see that there is a difference between 0.001

Table 5. Probability of occurrence for each event

Event ID	Baseline	Attacker advantage	Ostrich ZIP advantage
a	0.01	0.01	0.01
b	0.0001	0.0001	0.0001
c	0.001	0.01	0.001
d	0.001	0.001	0.001
e	0.1	0.1	0.5
f	0.01	1.0	0.001
g	0.01	0.01	0.01
h	0.1	0.1	0.1
i	0.1	0.1	0.1

Table 6. Probability of occurrence of each leakage case

Case ID	Baseline	Attacker advantage	Ostrich ZIP advantage
1	0.0121	0.0211	0.0121
2	0.0111	0.0111	0.0111
3	0.0109	0.0201	0.0061
4	0.0100	0.0101	0.0056
5	0.0121	0.0211	0.0121
6	0.0111	0.0111	0.0111
7	0.0001	0.0012	0.0001
8	0.001	0.0010	0.001
9	0.0111	0.0111	0.0111
10	0.0100	0.0100	0.0056
11	0.0001	0.0001	0.0001
12	0.0111	0.0111	0.0111
13	0.0100	0.0100	0.0056
14	0.0111	0.0111	0.0111
15	0.0100	0.0101	0.0056
16	0.0010	0.0021	0.0010
17	0.0111	0.0111	0.0111
18	0.001	0.0010	0.001

and 0.0100 in the baseline set of values. The value is about 1/10, indicating that adopting a different method for encryption is highly effective.

There is a difference between the case 10 “Sending the shared URL and the password for link protection in separate e-mails + SSL/TLS” and the case 4 “Sending the file in ostrich ZIP + SSL/TLS” in that a different method such

as online storage is used for file sharing. However, the fact that the file sharing information and its protection password are sent by e-mail is similar. Looking at the probability of a leak, we can see that there is almost no difference between the baseline value set of 0.010 and 0.0100. Incident Case 11, "Sending the shared URL and password for link protection through a separate route from e-mail + SSL/TLS," which has a similar sharing method to Incident Case 10, has a difference in that the password is shared through a separate route, but the difference in the probability of leakage is large, 0.100 and 0.0001. At the same time, file sharing via URLs, such as online storage, is not very effective as an information leakage countermeasure when sending and receiving e-mail.

6 Discussion

6.1 Information Leakage Risk and Usability

The model shows that sending passwords through a separate channel is highly effective against the risk of information leakage. However, sending passwords through a different channel is burdensome for both the sender and the receiver. It is not easy to agree in advance on which channel to use as a separate one, considering that the operational policies of each organization may restrict the use of software and services.

The use of encryption methods other than ZIP, such as PGP and S/MIME, has been highly effective, but these methods are highly dependent on the environment, and it is expected that there will still be many users who cannot use them. For example, Gmail and Yahoo! Mail do not support PGP or S/MIME.

Even if PGP and S/MIME are adopted in various software and services and made available to both senders and receivers, the difficulty of appropriate encryption will remain. In the field of usable security, the difficulty of appropriate encryption by end users has been an issue for a long time, and various approaches have been studied but have not yet reached a fundamental solution.

In the case of encryption using public key cryptography, the main problem is the appropriate selection of the recipient's public key by the sender. If the service or software supports the automatic selection of the recipient's public key linked to the e-mail address, the user's public key for the wrong e-mail address will be automatically selected when the wrong e-mail address is selected, and the erroneously sent user will be able to decrypt the information.

The environment-independence of the method is important from the viewpoint of usability, and it is not easy either.

6.2 Discontinuation of the Use of TPE and the Effect of AES Support in Various Environments

Our survey showed that although various operating systems can deploy encrypted ZIPs without installing additional software, the only supported encryption algorithm is TPE.

In the comparison of the probability of leakage, it was shown that the use of other cryptographic methods such as PGP and S/MIME made a difference in the probability of leakage, but the set of probability values was set on the assumption that TPE was used. However, the set of probability values was set on the assumption that TPE is used. If we assume that AES is used and TPE is abolished, the probability of event f "Decryption of encrypted ZIP files by malicious third parties" can be greatly reduced, and the probability of information leakage in the related occurrence cases can be reduced. However, even if the probability of occurrence of event f is reduced, the probability of occurrence of event e, whether the sender notices the erroneous transmission or not, is strongly related to the occurrence of information leakage in the case of sending passwords by e-mail, and thus does not make a significant difference.

6.3 Control of Information

File sharing through shared URLs, such as online storage services, was shown to be not significantly different from ostrich ZIP in terms of the risk of information leakage. However, online storage services have other advantages. The sender who set up the file sharing has the right to control the file sharing settings even after the file sharing information is sent. If we consider the risk of information leaks occurring and the risk of information leaks spreading as two different things, file sharing via shared URLs has the effect of suppressing the latter. In addition, file sharing through the use of a browser is highly environment-independent and is unlikely to cause usability problems.

Although the main focus of this paper is on the risk of information leakage, when considered from a different point of view, shared URLs can be a good general measure compared to ostrich ZIP.

6.4 Reasons for Adopting Ostrich ZIP and Current Status

The acquisition of Privacy Mark and ISMS certification was cited as the reason behind the use of Ostrich ZIP. In the Guidelines for the Implementation of Personal Information Protection Management Systems based on JIS Q 15001:2006 [6], it is stated that

> When sending and receiving personal information in the form of e-mail attachments, measures are taken to ensure confidentiality, such as encryption and password locks.

is a desirable method for "countermeasures during the transfer and communication of personal information". The fact that this exists as a background can be seen.

However, JIS Q 15001 was revised in 2017, and the revised Guidebook on Countermeasures to Standards [7] does not contain the same description. It is believed that there is no longer a strong rationale for obtaining Privacy Mark or ISMS certification as a reason for adoption.

6.5 Overseas Trends

It has been said that Ostrich ZIP is only used in Japan and is not commonly used overseas [8].

In our survey, we did not find any examples of Ostrich ZIP being used overseas. On the other hand, we did find that there are cases where encrypted ZIPs are being used in e-mails. Matthew Green's tweet on Twitter [9] reported that U.S. Senator Ron Wyden had asked NIST to set up a standard technology for sending and receiving secure files [10], which would replace file-sharing over e-mail using encrypted ZIP. The tweet expressed hope that it would replace file-sharing over email with encrypted ZIPs. The tweets were followed by tweets of approval, suggesting that encrypted ZIPs are being used to share files via e-mail overseas.

7 Conclusion

In this paper, we named the method of "sending an encrypted ZIP file as an attachment to an e-mail, and sending the decryption password in a separate e-mail" as Ostrich ZIP, and organized its advantages and disadvantages, threats, background of use, and alternative methods as a comprehensive risk assessment. This paper gives us a bird's eye view of the current situation, because this kind of organization has not been sufficiently organized.

In addition, a model of information leakage event occurrence was proposed focusing on information leakage during e-mail sending and receiving. Using the proposed model, cases of information leakage were identified, and the probability of occurrence of each case was estimated and the risk of information leakage was compared among the cases. The results show that the risk of information leakage of Ostrich ZIP itself is not significant compared to other cases, and that using other encryption methods and sending secret information such as passwords through other channels are more effective.

The clarification of the risk of information leakage allowed for further discussion. Therefore, we added considerations based on usability, social background, and overseas trends. These showed that the usefulness of Ostrich ZIP is not high, and that the use of shared URLs represented by online storage services, which are not much different from Ostrich ZIP in terms of information leakage risk, has advantages in terms of information control.

Ostrich ZIP is already widely used in many organizations, and it is not easy to change the rules defined in the past. It is hoped that the small technical advantages and reduced social demands of the ostrich ZIP shown in this paper will help to change the rules.

References

1. KImura, T.: Thinking about secure file sending and receiving between organizations - what is the purpose of encrypted ZIP? Internet Week 2016. https://www.nic.ad.jp/ja/materials/iw/2016/proceedings/t17/t17-kimura.pdf (2016). (Japanese)

2. Nomura, Y.: Do you really need encryption on that email? Okayama Information and Communication Technology Study Group. https://www.slideshare.net/nomlab/ss-85329306 (2017). (Japanese)
3. Sawatari, A.: Work Game - Is that "natural" necessary nowadays? Gijutsu-Hyohron (2019). (Japanese)
4. Uehara, T.: Why do we attach zip files with passwords to emails? Column No. 595, Institute of Digital Forensics (2019). https://digitalforensic.jp/2019/12/23/column595/ (Japanese)
5. @hashcat (2019). https://twitter.com/hashcat/status/1129441728761610242
6. JIPDEC PrivacyMark Promotion Center: Guidelines for the implementation of personal information protection management systems based on JIS Q 15001:2006. JSA Press (2010). (Japanese)
7. Uchikawa, K.: Guidebook for Implementing and Implementing a Personal Information Protection Management System for JIS Q 15001:2017. JSA Press (2018). (Japanese)
8. Ogawa, D.: I'll send you the password after that. Why it's not used at all in the U.S. and Europe, ITmedia Enterprise (2015). https://www.itmedia.co.jp/enterprise/articles/1509/18/news016.html
9. @matthew_d_green. https://twitter.com/matthew_d_green/status/1141430884459044864
10. Wyden, R.: https://www.wyden.senate.gov/imo/media/doc/061919%20Wyden%20Sensitive%20Data%20Transmission%20Best%20Practices%20Letter%20to%20NIST.pdf