Vol.2020-SPT-36 No.40
2020/3/2

オストリッチZIPの総合的リスクアセスメント

中山 道裕[1,a)]　金岡 晃[1,b)]

概要：機密性の高い情報を電子メールで送る場合に、パスワードによる暗号化を施したZIPファイルを電子メールに添付し、その後復号のためのパスワードを同じチャネルである電子メールで別送する方式がある。我々はその方式を「オストリッチZIP」と名付けた。オストリッチZIP方式は暗号化による情報保護や誤送信の対策として利用されている一方で、その意味に疑義が呈されることもある。しかしそれらの議論は整理されてきたとは言い難い。本稿ではそれらの議論を踏まえてオストリッチZIPの利点や欠点、脅威等を整理し、オストリッチZIPにかかわる環境を調査して現況を明らかにする。さらに電子メール送受信時のファイル共有における情報漏洩事象モデルを構築し、モデルに基づいてオストリッチZIPと代替策の情報漏洩リスクを評価し議論する。最後に情報漏洩リスク結果と合わせて別の視点を加えてオストリッチZIPが利用される背景を制度面などから考察し、本稿を総合的なオストリッチZIPのリスクアセスメントとして提供する。

1. はじめに

PCやスマートフォン、そしてインターネットを利用した社会活動において、情報の共有は欠かせないものとなっている。情報の共有に際して適切な相手に情報を配送し、適切な相手にのみ情報が開示されることの重要性は、ことさら論ずるまでもない。

情報共有に用いられるチャネルとして電子メールは長らく利用されており、そこでの情報共有は電子メール本文に加えPCやスマートフォンにおいて保存ないし作成された電子ファイルを電子メールに添付することで実現がされている。電子メールの送受信に用いられるSMTPはプロトコル自身ではデータの保護機構を持たないため、第3者により内容を閲覧される可能性は存在する。情報を保護するためには別途送受信されるデータに保護の機構を適用しなければならない。

電子メールの添付ファイルを保護するための方法として、複数ファイルを1つのファイルにまとめるアーカイブフォーマットであるZIPを用いる方法がある。ZIPはアーカイブされた内容の圧縮機能や暗号化をサポートしていることに加え、各種OSがアーカイブの展開に標準で対応し特別なアプリケーションを導入することなく利用可能な利便性があることから、広く利用されている。

電子メールによるファイル共有においてデータ保護を行う際に、このZIPの暗号化機能を用いて暗号化したZIPファイル（以後暗号化ZIPファイルと呼ぶ）を用いることがある。暗号化が施されているために復号時には鍵が必要になるが、ZIPの暗号化はパスワードを鍵として行われることが一般的である。電子メールで暗号化ZIPファイルを添付した場合、その復号のための鍵を何らかの形で共有しなければならない。その復号の鍵であるパスワードを同じチャネルである電子メールで別送し、かつその情報が保護しない平文のまま送られる。この「電子メールの添付ファイルは暗号化ZIPファイルにして送信し、別送する電子メールでその復号パスワードを送る」方式は広く使われている一方で、そのデータ保護への疑義は多く指摘されてきた。

この方式は、パスワードを同じチャネルで送ることや、パスワードの別送が暗号化ZIPを添付した電子メールの直近で行われるために、鍵の保護が十分ではなく暗号化によるデータ保護のレベルは期待されるものよりも低いことが想像される。この方式の利用者の多くは、こういったデータ保護レベルの低さを認識しつつも所属する組織のルールや受信側組織の要求、社会的な要求があるために利用していることが想像される。我々はそれを現実逃避や自己欺瞞を意味するオストリッチポリシー（Ostrich Policy）で運用されていると考え、この方式をオストリッチZIP（Ostrich ZIP）と呼ぶことにした。

オストリッチZIP方式については、さまざまな視点で利点や欠点が語られている一方で、それらが整理された文献が存在しているとは言い難い。そこで本稿では、まずそれ

[1] 東邦大学
Toho University, Funabashi, Chiba 274–8510, Japan
[a)] 5516077n@nc.toho-u.ac.jp
[b)] akira.kanaoka@is.sci.toho-u.ac.jp

らの議論を整理し利点や欠点、脅威等を明らかにする。そして代表的な OS やソフトウェア、Web サービスなどを対象にしてオストリッチ ZIP の現状を調査する。続いて電子メール送受信時のファイル共有における情報漏洩事象モデルを提案し、提案モデルに基づいてオストリッチ ZIP や代替策の情報漏洩リスクを評価し、比較と議論を行う。

2. オストリッチ ZIP 議論の整理

オストリッチ ZIP へはすでに多くの批判が存在する [1], [2], [3], [4]。一方でこれらの批判は複数の視点に及び同一の批判とはなっていない。そのため、リスク評価を含めて十分に整理がされているとは言い難い。本研究ではまずオストリッチ ZIP 議論の整理を目的として学術文献をはじめとした文献調査と Web 検索による Web 上の議論の調査を行い、そこで挙げられている利点と欠点、脅威、利用される背景、代替手法、リスク評価を整理する。

2.1 文献調査

文献調査は CiNii[*1]のフリーワード検索機能を用いて行った。キーワードとして「誤送信」「暗号化 メール」「情報漏洩対策 メール」を選択し検索した。それぞれの検索キーワードによる検索では、延べ 136 件の文献が結果として得られたが、本研究に関連する学術議論を行っている文献は存在しなかった。

2.2 Web 調査

Web 検索を用いた調査では、Google の検索を用いて行った。キーワードとして「暗号化 ZIP ファイル　別メール」「暗号化 ZIP 後送」「パスワード付き ZIP ファイル ビジネス」を選択し検索した。検索の結果、多くの結果が得られたがそのうち内容を精査し、特に 11 件の記事等の内容を整理した。

2.3 オストリッチ ZIP の利点

調査の結果得られたオストリッチ ZIP の利点として「誤送信対策（10 件）」「パスワード保護による情報漏洩のリスク軽減（3 件）」「電子メールと ZIP ファイルだけの利用であり新たな技術導入を要しない（1 件）」「別送による経路盗聴リスク軽減（1 件）」「ZIP 仕様の AES 暗号化対応（1 件）」が挙げられた。これらを踏まえ、我々はオストリッチ ZIP の利点を以下と置いた。その効果の大小はここでは論じない。

- 誤送信対策：パスワードを別送する際に誤送信に気づく機会がある
- 盗聴対策：暗号化 ZIP によるデータ保護による盗聴対策の意義がある
- 環境非依存性：暗号化 ZIP ファイルの展開は環境依存が少ない

2.4 オストリッチ ZIP の欠点

調査の結果得られたオストリッチ ZIP の利点として「同チャネル利用のため盗聴対策効果が薄い（4 件）」「自動的なオストリッチ ZIP ファイル対応の誤送信対策効果は薄い（2 件）」「ZIP 仕様の脆弱性（2 件）」「暗号化によりメールサーバ上のセキュリティスキャンが不可能になる（2 件）」「サーバによる電子メール盗聴（1 件）」が挙げられた。これらを踏まえ、我々はオストリッチ ZIP の利点を以下と置いた。利点と同様に、その効果の大小はここでは論じない。

- 電子メール盗聴の危険性
- 同チャネル利用による誤送信対策の意義減少
- 暗号化 ZIP ファイルの強度の低さ

セキュリティスキャンが不可能になるという論点は、オストリッチ ZIP だけではなく暗号化 ZIP ファイルや S/MIME、PGP 等によるメール暗号化、オンラインストレージサービスといったファイル共有サービス利用など複数の手法にまたがるためにオストリッチ ZIP 固有の欠点ではないと判断した。サーバによる電子メール盗聴も同様にオストリッチ ZIP 固有の欠点ではないと判断した。

2.5 オストリッチ ZIP の脅威

調査の結果得られたオストリッチ ZIP の脅威は 2 点挙げられた。

- 悪意のある第 3 者による盗聴
- 電子メールの誤送信

2.6 オストリッチ ZIP 利用の背景

調査の結果得られたオストリッチ ZIP 利用の背景として「プライバシーマークや ISMS 認証を満たす」ことが 11 件の Web 記事中の 7 件に記載があった。

2.7 オストリッチ ZIP の代替手法

調査の結果得られたオストリッチ ZIP の代替手法として「PGP や S/MIME（3 件）」「オンラインストレージサービス（3 件）」「オストリッチ ZIP の自動化（1 件）」「パスワードを電話で伝える（1 件）」「パスワードを郵送する（1 件）」「パスワードを直接会って渡す（1 件）」が挙げられた。これらを踏まえ、我々はオストリッチ ZIP の代替手法を以下と置いた。その効果の大小はここでは論じない。なお、添付ファイルの自動的な暗号化 ZIP 処理とパスワード送付を行うものを自動オストリッチ ZIP と呼んだ。

- PGP や S/MIME
- 別経路でのパスワード送付
- ファイル共有サービス、オンラインストレージサービス

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

- 自動オストリッチ ZIP

3. オストリッチ ZIP の現状調査

本章では、オストリッチ ZIP が利用される背景を探るための材料としてオストリッチ ZIP に関連する周辺環境の調査を行った。

3.1 ZIP 仕様

ZIP の仕様は PKWARE 社により提供され、ISO/IEC 21320-1:2015 として標準化されている。暗号化は共通鍵暗号アルゴリズム Traditional PKWARE Encryption (TPE) が採用され、その後 AES など他の暗号アルゴリズムも適用できるように仕様が変更された。TPE は Zipcrypto と呼ばれることもある。

TPE は脆弱であることがすでにわかっており、オープンソースソフトウェアの Hashcat を GPU 搭載コンピュータで実行すれば市販の環境でも容易に解読が可能であることが報告されている [5], [6]。

3.2 代表的な環境での暗号化 ZIP 対応状況

オストリッチ ZIP の利点の 1 つとして、環境非依存性を挙げた。ここでは代表的な環境において、暗号化 ZIP がどのように対応されているかを調査した結果を報告する。

3.2.1 OS による対応

対象の OS として、Windows 10、Mac OS X、Raspbian OS を選択し、暗号化 ZIP 作成と展開、作成時のデフォルト暗号アルゴリズムを調査した。生成では、インストール後の状態で専用ソフトウェア等を別途導入することなく暗号化 ZIP が生成可能かを調査した。生成された暗号化 ZIP に用いられる暗号アルゴリズム情報は ZIP ファイルのバイナリデータより得た。展開では、あらかじめ用意した暗号化 ZIP ファイル 2 種類（TPE による暗号化と AES による暗号化）を用意し、それぞれ展開が可能かを調査した。Raspbian OS では通常インストール時に zip のソフトウェアがインストールされていたため、それを用いることで生成と展開を調査した。

その結果を表 1 に示す。いずれの OS 環境においても、展開が TPE のみとなっていることがわかる。

モバイル端末に主に用いられる OS である iOS と Android OS に対しても調査を行った。モバイル用 OS に対しては、暗号化 ZIP の生成が可能かを調査した。Android 7.0 環境と iOS 13.2 においていずれも暗号化 ZIP の生成が不可能であることが確認された。

3.2.2 代表的ソフトウェアによる対応

電子メールの代表的なソフトウェア 4 種（Microsoft Outlook 2016 16.0.4266.1001、Mozilla Thunderbird 68.2.2、Apple Mail 12.4、Becky! Internet Mail 2.74.03）に対し、暗号化 ZIP の作成が可能かを調査した。その結果、いずれのソフトウェアにおいても暗号化 ZIP の生成を行う機能はないことが確認された。

3.2.3 代表的 Web メールサービスによる対応

電子メールの送受信はブラウザを介した Web サービスで行うことも多くなってきている。そこで代表的な Web サービスである Google 社の Gmail と Yahoo!社の Yahoo! メールに対し、暗号化 ZIP の作成が可能かを調査した。調査は 2019 年 11 月 13 日に行った。その結果、いずれのサービスにおいても暗号化 ZIP の生成を行う機能はないことが確認された。

3.3 自動オストリッチ ZIP

オストリッチ ZIP は送信者と受信者の双方に暗号化や復号の処理を行わせる必要があるため、通常の電子メール送受信よりも負担が生じる。そういった送信者の負担を減らすことが可能な、添付ファイルの自動的な暗号化 ZIP 化とパスワードの送信を行ってくれる機構が存在する。我々はそれを自動オストリッチ ZIP と呼んでいる。

自動オストリッチ ZIP は複数のサービスやソリューションが存在している。自動化を行う主体により、「ゲートウェイ型自動オストリッチ ZIP」「クライアント型自動オストリッチ ZIP」「メールサーバ型自動オストリッチ ZIP」に大別できる。

ゲートウェイ型自動オストリッチ ZIP はメールサーバと送信者の間に位置する暗号化 ZIP 化専用の機器またはサービスである、クライアント型自動オストリッチ ZIP は送信者の環境にインストールすることで暗号化 IZP 化を自動的に行うソフトウェアである。メールサーバ型自動オストリッチ ZIP は、メールサーバ機能として自動オストリッチ ZIP を行う機能を含んだものを指す。

我々の調査で、10 件の自動オストリッチ ZIP ソリューションが見つかった。そのうち 6 件はゲートウェイ型であり、クライアント型は 2 件、メールサーバ型は 2 件であった。また、暗号アルゴリズムの変更に対応していると謳っているソリューションは 10 件のうち 4 件であった。

さらに、著者らがこれまでに受信した電子メールにおいて自動オストリッチ ZIP により送信されたと思われる電子メール 10 種類に対し、その暗号化アルゴリズムの調査を行った。なお、同一送信者から送られた暗号化 ZIP ファイルは 1 種類と数えた。

その結果、いずれも TPE による暗号化であったことが判明した。

4. 電子メール送受信時のファイル共有における情報漏洩事象モデル

オストリッチ ZIP のリスクを評価するために、代替策を含めた評価を可能にする電子メール送受信時のファイル共有における情報漏洩事象モデルを提案する。モデル提案に

表 1　OS による暗号化 ZIP ファイルの実態調査結果

OS	生成	デフォルトアルゴリズム	展開	OS 詳細
Windows	×	-	TPE のみ	Windows10 pro
macOS	○	TPE	TPE のみ	macOS Mojave 10.14.6
Raspbian OS	○	TPE	TPE のみ	Linux : 4.14.98-v7, Raspbian OS: 9.8

表 2　オストリッチ ZIP を含めた電子メールによる情報漏洩事象

事象 ID	電子メールによる情報漏洩事象
a	誤送信をする
b	メールサーバを盗聴される
c	通信路を盗聴される
d	メールサーバーや通信路以外から盗聴される
e	パスワードを別送する時、誤送信に気付く
f	悪意のある第三者が暗号化 ZIP ファイルを解く
g	メール誤送信し、かつ、その誤送信相手に別経路でパスワードを送る
h	公開鍵の持ち主を誤り、かつ、その宛先がメール誤送信者と一緒になる
i	クラウドストレージのアクセス制御する相手を誤り、かつ、その宛先がメール誤送信相手と一緒になる

あたり、これまで議論してきたオストリッチ ZIP の利点や欠点などを踏まえ、脅威を電子メール送受信時の情報漏洩に限定した。

最初に、電子メールによる情報漏洩関連事象をリストアップし、それぞれに名称を付ける。次に、オストリッチ ZIP や代替策を含むさまざまな電子メール利用の状況における情報漏洩の発生確率を事象の組み合わせを用いて表現する。最後にそれらの発生確率モデルの簡略化を行い、実際に数値を入力してそれぞれの手法の情報漏洩発生確率の値を比べる。

4.1　電子メールによる情報漏洩関連事象

電子メールによる情報漏洩関連事象を表 2 に示す。それぞれの事象は、オストリッチ ZIP の脅威として挙がった「誤送信」と「盗聴」を基本とし、電子メール送信から受信までの間で誤送信と盗聴が起きうる事象を著者らで検討してリストアップした。それぞれの事象に a から i までの事象 ID を割り当てた。

4.2　電子メール利用の状況と情報漏洩発生事象

電子メール利用の状況と、その状況下における情報漏洩の発生事象を事象の組み合わせとして評価したものを表 3 に示す。

電子メール利用の状況は、添付ファイルの保護の有無、ファイル共有の手法、通信路暗号の有無などの要素をあらかじめ著者らがリストアップし、それぞれの違いにより利用状況を細分化した。またそれぞれの利用状況に対し、情報漏洩が発生する事象を表 2 に挙げた a から i の事象の組み合わせで表した。

4.3　事象モデルと各漏洩発生ケースでの簡略化した漏洩発生確率

次に表 3 で定義した各漏洩発生ケースに対し、その発生確率を検討する。表 2 で挙げられた各事象は独立に発生するとは考えられず、それぞれの漏洩発生ケースの発生確率は単純に求めることは難しい。しかし、簡略化したモデルであっても一定の意義があると考え、各事象の発生を独立と置いて簡略化した確率を求める。各漏洩発生ケースと確率の式を表 4 に示す。

5.　事象モデルを用いた漏洩リスク評価

本章では表 4 で求めた簡略化した確率式に対し、各事象の発生確率に具体的な数値を定義して各ケースの発生確率を求めることでオストリッチ ZIP やその代替策のリスクを評価する。

各事象の発生確率の真の値を得ることは困難であり、指標となる近似値や推測値を得ることも難しい。そこで、著者らが考察をもとに値を設定することとした。しかし著者らの設定した数値では偏りが起こることが容易に考えられるために、著者らが用意した確率の値のセットをベースラインとし、ベースラインと比較してより攻撃者が有利な状況を考えた確率の値のセットと、オストリッチ ZIP の効果が強くでるような確率の値のセットを用意し、それらを比較することでオストリッチ ZIP のリスクや代替策との比較を行うこととした。3 種類の確率の値のセットを表 5 に示す。

攻撃者が有利な状況では、事象 c「通信路を盗聴される」と事象 f「悪意のある第三者が暗号化 ZIP ファイルを解く」の確率の値を上げた。一方オストリッチ ZIP が有効な状況では、事象 e「パスワードを別送するとき、誤送信に気付く」の確率の値を上げ事象 f「悪意のある第三者が暗号化 ZIP ファイルを解く」の確率の値を下げた。これらの値により得られた各漏洩発生ケースの発生確率を表 6 に示す。

漏洩発生ケース 3「オストリッチ ZIP で送る＋ SSL/TLS なし」と漏洩発生ケース 4「オストリッチ ZIP で送る＋ SSL/TLS あり」における漏洩発生確率を比較すると、ベースラインの数値セットにおいて 0.0109 と 0.0100 と大きな差は見られない。SSL/TLS を通信路に適用することで事象 c の発生が起きないとしているが、その効果は強いとは言えないことが示されている。

表 3 電子メール利用の状況と情報漏洩発生ケース

ケース ID	電子メールの利用状況	事象
1	暗号化なしで添付ファイルを送る+SSL/TLS なし	$a \cup b \cup c \cup d$
2	暗号化なしで添付ファイルを送る+SSL/TLS あり	$a \cup b \cup d$
3	オストリッチ ZIP で送る+SSL/TLS なし	$(e^- \cap (a \cup b \cup c \cup d)) \cup (e \cap f \cap (b \cup c \cup d))$
4	オストリッチ ZIP で送る+SSL/TLS あり	$(e^- \cap (a \cup b \cup d)) \cup (e \cap f \cap (b \cup d))$
5	自動オストリッチ ZIP で送る+SSL/TLS なし	$a \cup b \cup c \cup d$
6	自動オストリッチ ZIP で送る+SSL/TLS あり	$a \cup b \cup d$
7	別経路 (SMS や郵送や電話) で暗号化 ZIP パスワードを送る+SSL/TLS あり	$(a \cap g) \cup (f \cap (b \cup d))$
8	PGP、S/MIME で暗号化メールを送る+SSL/TLS あり	$a \cap h$
9	共有 URL とリンク保護のためのパスワードを一つのメールで送る+SSL/TLS	$a \cup b \cup d$
10	共有 URL とリンク保護のためのパスワードをそれぞれ別メールで送る+SSL/TLS	$e^- \cap (a \cup b \cup d)$
11	共有 URL とリンク保護のためのパスワードをメールと別経路で送る+SSL/TLS	$a \cap g$
12	共有 URL とパスワード (リンク保護+暗号化 ZIP) を一つのメールで送る+SSL/TLS	$a \cup b \cup d$
13	共有 URL とパスワード (リンク保護+暗号化 ZIP) をそれぞれメールで送る+SSL/TLS	$e^- \cap (a \cup b \cup d)$
14	共有 URL(リンク保護なし) と暗号化 ZIP パスワードを一つのメールで送る+SSL/TLS	$a \cup b \cup d$
15	共有 URL(リンク保護なし) と暗号化 ZIP パスワードをそれぞれメールで送る+SSL/TLS	$e^- \cap (a \cup b \cup d) \cup (e \cap f \cap (b \cup d))$
16	共有 URL(リンク保護なし) と暗号化 ZIP パスワードをメールと別経路で送る+SSL/TLS	$(a \cap h) \cup (f \cap (b \cup d))$
17	共有 URL(リンク保護なし) を一つのメールで送る+SSL/TLS	$a \cup b \cup d$
18	オンラインストレージでアクセス制御あり+暗号化 ZIP のパスワードをメールで送る+SSL/TLS	$a \cap i$

表 4 事象モデルと各漏洩発生ケースでの簡略化した漏洩発生確率

ケース ID	事象	事象発生確率
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	$a \cap i$	$P(a)P(i)$

漏洩発生ケース 4「オストリッチ ZIP で送る＋ SSL/TLS あり」と漏洩発生ケース 2「暗号化なしで添付ファイルを送る＋ SSL/TLS あり」を比較すると、暗号化によりデータが保護されているとはいえその漏洩発生確率がベースラインの数値セットにおいて 0.0100 と 0.0111 とこちらも大差がないことがわかる。しかしオストリッチ ZIP がより有

表 5　各事象の発生確率仮定

事象 ID	ベースライン	攻撃者有利	オストリッチ ZIP 有効
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

表 6　各事象の発生確率仮定をもとにした各漏洩発生ケースの発生確率

ケース ID	ベースライン	攻撃者有利	オストリッチ ZIP 有利
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

効な数値セットにおいては 0.0056 と 0.0111 となり、オストリッチ ZIP が有効であるという仮定を置けば確率の差自体は小さいがほぼ 2 倍の値となるという、自明ともいえる結果が示された。

漏洩発生ケース 4「オストリッチ ZIP で送る＋ SSL/TLS あり」と漏洩発生ケース 6「自動オストリッチ ZIP で送る＋ SSL/TLS あり」では、パスワードの生成と送付を自動化する差異がある。漏洩発生確率はベースラインの数値セットにおいて 0.0100 と 0.0111 と大きな差がないことがわかる。また漏洩発生ケース 6「自動オストリッチ ZIP で送る＋ SSL/TLS あり」は、漏洩発生ケース「暗号化なしで添付ファイルを送る＋ SSL/TLS あり」と同じ発生確率となっている。本提案モデルにおいては情報漏洩発生リスクに変わりがなく、自動オストリッチ ZIP は電子メール送受信における情報漏洩には効果があるとは言えないことが示されている。

漏洩発生ケース 7「別経路 (SMS や郵送や電話) で暗号化 ZIP パスワードを送る+SSL/TLS あり」は、発生ケース 4「オストリッチ ZIP で送る＋ SSL/TLS あり」と比べると、暗号化 ZIP を採用しているもののその復号のパスワードは別経路で送るという差がある。漏洩発生確率を見るとベースラインの数値セットにおいて 0.0001 と 0.0100 と差が出ていることがわかる。その値がおよそ 1/100 になっており、別経路でパスワードを送付することの効果が高いことが示されている。同様にパスワード等を別経路で送付する漏洩発生ケース 11「共有 URL とリンク保護のためのパスワードをメールと別経路で送る+SSL/TLS」、漏洩発生ケース 16「共有 URL(リンク保護なし) と暗号化 ZIP パスワードをメールと別経路で送る+SSL/TLS」が他のケースと比較すると小さな発生確率となっており、別経路で送付することの効果が高いことがわかる。

漏洩発生ケース 8「PGP、S/MIME で暗号化メールを送る+SSL/TLS あり」は発生ケース 4「オストリッチ ZIP で送る＋ SSL/TLS あり」と比べると、暗号化に別手法を採用している差がある。漏洩発生確率を見るとベースラインの数値セットにおいて 0.001 と 0.0100 と差が出ていることがわかる。その値がおよそ 1/10 になっており、暗号化に別手法を採用することの効果が高いことが示されている。

漏洩発生ケース 10「共有 URL とリンク保護のためのパスワードをそれぞれ別メールで送る+SSL/TLS」は発生ケース 4「オストリッチ ZIP で送る＋ SSL/TLS あり」と比べると、ファイル共有にオンラインストレージ等の別手法を採用している差があるが、ファイル共有自体の情報とその保護パスワード送付を電子メールで送っていることは同様である。漏洩発生確率を見るとベースラインの数値セットにおいて 0.010 と 0.0100 とほぼ差がないことがわかる。発生ケース 10 と類似の共有手法を持つ発生ケース 11「共有 URL とリンク保護のためのパスワードをメールと別経路で送る+SSL/TLS」は、パスワードの共有を別経路で行う違いがあるが、その漏洩発生確率の差は 0.100 と 0.0001 と大きな差になっている。ここでも別経路でのパスワード共有が大きな意味を持つことが示され、同時にオンラインストレージ等の URL によるファイル共有は電子メール送受信時の情報漏洩対策としては大きな効果を持つものではないことが示されている。

6. 考察

6.1 情報漏洩リスクとユーザビリティ

情報漏洩リスクに対しては別経路でパスワードを送付することの効果が高いことが本モデルを用いた試算により示されたが、別経路で送付することは送信者と受信者の双方に負担となる。あらかじめ別の経路としてどの経路を使うかを合意しなければならないことは、各組織ごとの運用ポリシによりソフトウェアやサービス利用に制限がかかることを考慮すると、簡単ではない。

PGP や S/MIME といった ZIP とは別の暗号化手法を用

いることの効果も高くでているが、これらの手法は環境への依存度が高く、利用不可能なユーザはまだ多くいることが予想される。たとえば Gmail や Yahoo!メールでは PGP や S/MIME の対応は行われていない。

仮に PGP や S/MIME の採用が各種ソフトウェアやサービスに行われ、送受信者ともに利用可能な状態になったといえども、適切な暗号化の難しさは残る。ユーザブルセキュリティ分野ではエンドユーザによる適切な暗号化の困難さは古くからの課題であり [7]、さまざまなアプローチが研究されているが根本解決には至っていない。

公開鍵暗号を利用した暗号化の場合は、送信者による受信者公開鍵の適切な選択などが主要な問題となるが、仮にこれがメールアドレスと紐づけられて自動的に選択するようにサービスやソフトウェアが対応した場合、誤ったメールアドレスを選択した時点でその誤ったメールアドレスのユーザ公開鍵が自動選択され、誤って送信されたユーザは情報が復号できてしまい、誤送信対策にはなりえないものとなる。

手法の環境非依存性はユーザビリティの視点で重要であり、こちらも簡単ではないと言えよう。

6.2 TPE の利用廃止と各種環境での AES 対応の効果

我々の調査で、各種 OS は追加のソフトウェアを導入することなく暗号化 ZIP を展開可能ではあるものの対応する暗号化アルゴリズムが TPE のみであることが示された。

漏洩発生確率の比較では、PGP や S/MIME 等の他の暗号手法を用いることで発生確率に差が出ることが示されていたが、確率の値のセットは TPE が利用されていることが前提で設定されており、AES が利用されていることや TPE が撤廃されていることを前提と置くならば、事象 f「悪意のある第三者が暗号化 ZIP ファイルを解く」の発生確率は大きく下げることができ、関連する発生ケースの情報漏洩発生確率が下がる。しかし事象 f の発生確率が下がったとしても、誤送信に送信者が気づくかどうかの事象 e の発生確率がパスワードをメールで送付する場合の情報漏洩発生に強くかかわっていることから、大きな差が生まれない。

6.3 情報のコントロール

オンラインストレージサービスといった共有 URL によるファイル共有は、情報漏洩の発生リスクにおいてはオストリッチ ZIP と大きな差がないことが示された。しかしオンラインストレージサービスには他の利点がある。ファイル共有を設定した送信者は、ファイル共有情報を送信した後もファイル共有設定の変更などのコントロール権を持っている。情報漏洩の発生リスクと、情報漏洩の拡大リスクを別のものと考えると、共有 URL によるファイル共有は後者を抑える効果がある。またブラウザ利用による共有は環境非依存性も高く、ユーザビリティ上の問題も起きにくいと考えられる。

本稿の主眼は情報漏洩の発生リスクに置いたが、別の視点を合わせて考えると、共有 URL はオストリッチ ZIP と比較して良い大体策になると考えられる。

6.4 オストリッチ ZIP の採用理由と現状

オストリッチ ZIP 利用の背景にプライバシーマークや ISMS 認証の取得が挙げられていた。JIS Q 15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン [8] では、「個人情報の移送・通信時の対策」の望ましい手法で「電子メールの添付ファイルで送受信する場合、暗号化やパスワードロック等の秘匿化の措置を講じている。」と記載されているなど、背景として存在している事実はうかがえる。

しかし JIS Q 15001 は 2017 年に改訂が行われており、改訂された標準への対策ガイドブック [9] を見ると、同様の記述は見られない。採用理由としてのプライバシーマークや ISMS 認証の取得には、現在では強い根拠はなくなったと考えられる。

一方で、組織において過去に規定したルールを変更することは簡単ではなく、その労力は無視できないことも考慮した検討が必要となるだろう。

6.5 海外動向

オストリッチ ZIP は、日本国内だけで利用がされており海外では一般的ではないということが言われている [10]。

我々の調査でも、オストリッチ ZIP が海外で利用されている例は発見されなかった。一方で、暗号化 ZIP がメールで利用されているケースが存在することが見つかった。Matthew Green の Twitter でのツイート [11] では、米国上院議員の Ron Wyden が NIST に安全なファイル送受信の標準技術を設定するように求めた [12] ことが紹介されており、それが暗号化 ZIP を用いた電子メール上のファイル共有を置き換えることの期待が述べられていた。当該ツイートには賛意を表するツイートも続いており、オストリッチ ZIP とは言い切れないものの、海外においても暗号化 ZIP により電子メールでのファイル共有が行われていることがうかがえた。

7. まとめ

本研究では、「電子メールの添付ファイルは暗号化 ZIP ファイルにして送信し、別送する電子メールでその復号パスワードを送る」方式をオストリッチ ZIP と名付け、その総合的なリスクアセスメントとして利点と欠点や、脅威、利用の背景、代替手法などの整理を行った。こういった整理はこれまで十分な整理がされておらず、本稿により現状が俯瞰できるようになったと考える。

さらに、電子メールの送受信時における情報漏洩に焦点を当て情報漏洩の事象発生のモデルを構築した。構築したモデルを用いて情報漏洩発生のケースを洗い出し、それらのケースについての発生確率の試算とケース間の情報漏洩発生のリスク比較を行った。その結果、オストリッチ ZIP 自体の情報漏洩発生にかかわるリスクは他のケースと比べて特筆すべき効果はなく、他の暗号化手法を用いることや、パスワード等の秘密情報を別経路で送ることの効果の高さが示された。

情報漏洩リスクを明確にしたことで、さらなる議論が可能になった。そのため、ユーザビリティや社会的背景、海外動向を踏まえた考察を加え、オストリッチ ZIP の有用性は高くないことと、情報漏洩リスクとしてオストリッチ ZIP と大差のないオンラインストレージサービスに代表される共有 URL の利用は情報コントロールの面で利点があることが示された。

オストリッチ ZIP はすでに多くの組織でルール化されて広く使われており、過去に規定したルールを変更することは簡単ではない。本稿により示されたオストリッチ ZIP の技術的優位点の少なさと社会的要求の減少がルール変更の一助になると幸いである。

参考文献

[1] 木村, “組織間の安全なファイル送受信を考える～暗号化 ZIP は何のため～”, Internet Week 2016, https://www.nic.ad.jp/ja/materials/iw/2016/proceedings/t17/t17-kimura.pdf, 2016
[2] 乃村, “そのメール, ホントに暗号化が必要ですか?”, 岡山情報通信技術研究会, https://www.slideshare.net/nomlab/ss-85329306, 2017
[3] 沢渡, “仕事ごっこ その“あたりまえ”、いまどき必要ですか?”, 技術評論社, 2019
[4] 上原, “私たちはなぜパスワード付きｚｉｐファイルをメール添付するのか”, 第 595 号コラム, デジタル・フォレンジック研究会, https://digitalforensic.jp/2019/12/23/column595/, 2019
[5] @lumin, ”GPU で ZIP パスワードを解析する”, https://qiita.com/lumin/items/cf1e10cccfe5727f8180, 2019
[6] @hashcat, https://twitter.com/hashcat/status/1129441728761610242, 2019
[7] Whitten, Alma, and J. Doug Tygar. ”Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0.” USENIX Security Symposium. Vol. 348. 1999.
[8] 日本情報処理開発協会プライバシーマーク推進センター (編集) “JIS Q 15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン”, 日本規格協会出版, 2010
[9] 打川和男. JIS Q 15001:2017 対応 個人情報保護マネジメントシステム導入・実践ガイドブック. 日本規格協会出版, 2018.
[10] 小川, “続けてパスワード送付」欧米でまったく使われないワケ”, ITmedia エンタープライズ, https://www.itmedia.co.jp/enterprise/articles/1509/18/news016.html, 2015
[11] @matthew_d_green, https://twitter.com/matthew_d_green/status/1141430884459044864
[12] Ron Wyden, https://www.wyden.senate.gov/imo/media/doc/061919\%20Wyden\%20Sensitive\%20Data\%20Transmission\%20Best\%20Practices\%20Letter\%20to\%20NIST.pdf