暗号化ラッパプログラムの開発

松澤 英之

宮崎大学 情報基盤センター

matuzawa@cc.miyazaki-u.ac.jp

Development of Wrapper Program for Encryption

Hideyuki Matsuzawa

Information Technology Center, University of Miyazaki.

概要

昨今情報漏えい対策は重要である。宮崎大学でも個人情報の漏えい対策として、個人情報が書き込まれているファイル・フォルダをパスワード付 ZIP で圧縮する、すなわちファイル・フォルダを暗号化する事を推奨している。本研究では、ユーザが常に暗号化されているパスワード付 ZIP ファイルを簡単に参照・編集できるラッパプログラムを開発した。

1 はじめに

独立行政法人 情報処理推進機構(IPA)が作成した情報セキュリティ啓発のための対策のしおり「初めての情報セキュリティ対策のしおり(第 1 版)」[1]では、新入社員に対する最初のセキュリティ対策として個人情報及び企業情報の漏洩対策を挙げている。また NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループが作成した 2015 年情報セキュリティインシデントに関する調査報告書【速報版】Ver. 1.0[2]から、 2006 年度の個人情報漏えいの原因の約半数は紛失・置き忘れ、盗難であることがわかる。IPA が作成した「暗号化による<情報漏えい>対策のしおり(第 1 版)」[3]では、紛失・置き忘れ、盗難の対策の例として情報の暗号化を挙げている。

宮崎大学でも「教員の個人情報ファイルの取り扱い方針」で個人情報を含むファイル・フォルダに対してパスワードで保護する事を推奨している。ファイル・フォルダ自体にパスワードを付ける機能はない。そこで宮崎大学ではファイル・フォルダをパスワード付 ZIP で圧縮する方法を推奨している。パスワード付 ZIP ファイル作成時には暗号化も行われるので、宮崎大学の方針によれば個人情報を含むファイル・フォルダは常に暗号化する事が推奨されていることになる。通常暗号化されているファイル・フォルダをユーザが参照・編集する時には、どのような工程を経る必要があるだろうか。

1. 暗号化されたファイル・フォルダを暗号化ソフトを用いて復号化する。
2. 復号化されたファイルを参照・編集する。
3. 復号化したファイル・フォルダを暗号化ソフトで再度暗号化する。暗号化の際に暗号化ソフトが暗号化前のファイル・フォルダを削除しないものもある。この場合秘密保持のため、暗号化前のファイル・フォルダを暗号化したのち手動で削除する必要がある。

暗号化ソフトには自動でこれら 3 つの工程を行うものもある[4][5]。

しかし宮崎大学ではパスワード付 ZIP ファイルを自動的に復号・暗号化する便利な暗号化ソフトは導入されていない。またデフォルトの Windows クライアント OS にはパスワード付 ZIP ファイルを作成する機能はない。自動的に復号化して参照・編集できる暗号化ソフトを導入している人以外は、ファイルを参照・編集するたびに上記 3 工程を手作業で行わなければならない。暗号化したファイルを参照・編集するたびに行われるこれらの作業は、パソコンユーザにとっては非常に面倒な作業である。2015 年に発生した年金機構における不正アクセスによる情報流出事案の検証報告書[6]では、原則として厳格なルールを定めていてもルールが遵守されなければ情報が漏洩する事に言及している。同様にこのファイル・フォルダの暗号化に関しても、ユーザが個々のファイル・フォルダを暗号化して運用する事が面倒な作業であると認識すればそれを回避する方向、即ちファイルを暗号化しないで保存するようになることが考えられる。

そこで、この面倒な 3 工程をなるべく簡単にし、パソコンユーザに個人情報を含んだファイル・フォルダをパスワード付 ZIP で保存・利用してもらうためにパスワード付 ZIP ファイルに対する Windows 向け暗号化ラッパプログラムを開発した。

2 暗号化方法

ラッパプログラムの暗号化方法としてパスワード付 ZIP を用いた。パスワード付 ZIP ファイルを暗号化方法として採用する利点は、

1. 最近の Windows クライアント OS ではデフォルトでパスワード付 ZIP の復号化が行える
2. IPA「電子メール利用時の危険対策のしおり(第 4 版)」[7]で、電子メールにファイルを添付する際にはファイルをパスワード付 ZIP で暗号化してから添付する事を紹介している
3. Mac OS X ではデフォルトでパスワード付 ZIP ファイルの暗号化が行える
4. 宮崎大学の方針では個人情報を含むファイル・フォルダにパスワードをつける事を推奨している。またファイル・フォルダにパスワードを付ける方法としてファイル・フォルダをパスワード付 ZIP で圧縮(暗号化)する事を推奨している

である。

一方、パスワード付 ZIP ファイルに対しては暗号化の解読のためのフリーソフトが出回っているなどセキュリティ強度の点で問題がある。今回は開発したラッパプログラムを宮崎大学でたくさんのユーザに使ってもらうため、セキュリティ強度の問題は目をつぶってパスワード付 ZIP を用いた。

3 暗号化ソフト

Windows にはデフォルトでパスワード ZIP を作成する機能はない。Windows 用の GUI 暗号化ソフト(実際は書庫ソフト)は広く普及してので、最初にファイル・フォルダを暗号化するプロセスは一般に利用されている GUI タイプの暗号化ソフトで行う事とする。ラッパプログラムで復号・暗号化、或いはファイルの参照・編集を行う際は、ラッパプログラムから復号・暗号化用の、或いはファイル参照・編集用の外部プログラムをそれぞれ起動して行う。これは以下の利点がある。

1. 車輪の再発明を防ぐ。
2. ユーザがファイルを参照・編集する時、暗号化されていないファイルを扱う時と同様に操作できる。
3. ラッパプログラムからファイルの参照・編集を行う外部プログラムを起動する場合、Windows のファイルの拡張子とフソフトウェアの関連付けを利用して起動するので、Windows パソコンで利用できる様々な形式のファイルを参照・編集する事が出来る。また、ラッパプログラム導入後もラッパプログラムが扱えるファイルの種類を増やすことが出来る。
4. ラッパプログラムで手動或いは自動的に暗号化ソフトを選択できるようにすれば、ラッパプログラムが将来的に様々な暗号化形式に対応できる。

今回は、GUI、CUI で利用可能でパスワード付 ZIP ファイルを作成できる 7-Zip[8]を暗号化ソフトとして利用した。

4 ラッパプログラムのプロセス

ラッパプログラムの基本コンセプトは

1. 暗号化ファイルを参照・編集する 3 工程は外部プログラムに任せる。
2. ラッパプログラムは外部プログラム同士が円滑に働くように補助する。

ラッパプログラムの具体的なプロセスは以下のとおりである。

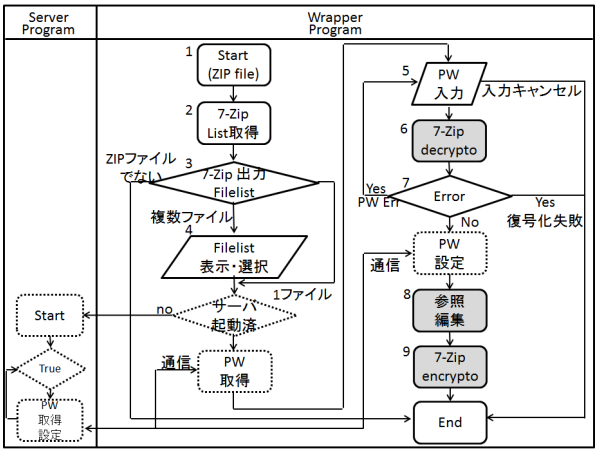

図 1

1. 復号化したいパスワード付 ZIP ファイル名を引数としてラッパプログラムを起動する。
2. ラッパプログラムは外部暗号化ソフトにパス

ワード付 ZIP ファイル名を引数として渡し、戻り値としてパスワード付 ZIP ファイルに含まれるファイル・フォルダのリストを取得する。

3. ラッパプログラムは外部暗号化ソフトからの戻り値であるファイル・フォルダのリストについて判断する。ラッパプログラム起動時に引数で指定したファイルが ZIP で暗号化されていない場合、ラッパプログラムは終了する。パスワード付 ZIP ファイルに含まれるファイルが一つの場合は、パスワード入力画面(プロセス 5)に進む。それ以外はプロセス 4 に進む。
4. ラッパプログラムは取得したファイルリスト(フォルダは除く)を表示し、ユーザに参照・編集するファイルを選択させる。
5. パスワード付 ZIP ファイルを復号化するためのパスワード入力画面を表示する。入力されたパスワードは伏字で表示される。パスワードの入力がキャンセルされた場合は、ラッパプログラムを終了する。ユーザが入力する以外の方法でパスワードを取得する方法については改めて言及する。
6. ラッパプログラムはユーザが入力したパスワード、パスワード付 ZIP ファイル名を引数として外部暗号化ソフトに渡し、外部暗号化ソフトで復号化を行う。ラッパプログラムは復号化した際に外部暗号化ソフトが表示するメッセージを取得する。
7. 外部暗号化ソフトから取得したメッセージで外部暗号化ソフトが正常に終了したか判断する。パスワードが間違っていた場合は、パスワード入力画面(プロセス 5)に戻る。復号化に失敗した場合は、ラッパプログラムを終了する。
8. プロセス 4 で選択したファイルに対応した参照・編集するソフトウェアを起動する。Windows ではコマンドプロンプトでファイル名を入力するだけで、GUI でファイルアイコンをダブルクリックした場合と同じようにファイル形式に対応したソフトウェアを起動する事ができるので、ラッパプログラムは Windows のシェル(コマンドプロンプト)に 'start "画面表示名" 選択されたファイル名'を渡す。ここで"start"コマンドは現在利用しているコマンドプロンプトとは別のコマンドプロンプトを起動するためのコマンドである。参照・編集するソフトウェアの起動に失敗した場合でも、既に復号化されているファイル・フォルダを再度暗号化する必要があるのでラッパプログラムのプロセスは続行する。
9. 外部暗号化ソフトに引数としてパスワード、ZIP ファイル名、暗号化するファイル・フォルダ一覧を渡してファイル・フォルダの暗号化を行う。暗号化ソフトとして使用した 7-Zip は暗号化時に、暗号化前のファイル・フォルダを削除する機能があるので、この削除機能を利用して復号化したファイル・フォルダを削除する。

5 パスワード一時保存サーバ

5.1 パスワード一時保存サーバ

上で記述したプロセスでは、このラッパプログラムを起動するたびに、ユーザはファイルを復号・暗号化するためのパスワードを入力する必要がある。ファイル・フォルダを参照・編集するたびにユーザがパスワードを入力するのは大変なので、パスワードを一時保存するサーバを作成した。ラッパプログラムがこのサーバと通信する事でパソコン起動後最初にラッパプログラムを利用する時または、前に入力したパスワードと異なる場合を除いてパスワードの入力を省略できる。

パスワードを共有する方法として、サーバではなく一時ファイルにパスワードを保存・共有する方法も検討した。しかしファイルにパスワードを保存した場合、パソコンが異常終了した時でもパスワードを保存したファイルを完全に削除する方法を思いつけなかった。つまりパソコンが異常終了した場合は、パソコン内にパスワードを保存したファイルが残されてしまう恐れがある。しかしサーバプログラムの場合は、メモリー上にパスワードが保存されるので、パソコンが異常終了した場合でもパスワードが残されることはないと判断した。

サーバプログラムはユーザが起動する複数のラッパプログラムからアクセスされるので、ラッパプログラムとサーバ間の通信には TCP/IP を用いた。このサーバは重要なファイルを復号化するパスワードを保存しているので、特にセキュリティには気を付ける必要がある。そこでパスワードを保持しているサーバが起動している時間を短くするように努めた。そのため、パソコンが起動し

ている間は常にプログラムが働く Windows サービスとしては登録せずに、ラッパプログラムと同じように起動しているときはコマンドプロンプトが表示されるコンソールプログラムとした。コンソールプログラムの場合、サーバプログラムが動いているコマンドプロンプト画面を閉じることで簡単にサーバプログラムを終了できる。

5.2 プロセス

サーバを起動する場合は、ラッパプログラムのプロセス 4 終了後に行う。まずパソコンでサーバプログラムが起動しているかどうかラッパプログラムが確認する。サーバが起動していない場合は、ラッパプログラムから外部プログラムとしてサーバプログラムを起動する。サーバプログラムが既に起動していた場合は、ラッパプログラムはサーバと通信して保存されているパスワードを取得、プロセス 5 でパスワード入力画面に伏字でパスワードを表示する。ラッパプログラムはプロセス 7 でパスワードが正しいと確定した後にサーバへパスワードの保存を行う。

サーバを利用するかどうかは設定ファイルで指定できるようになっている。デフォルトはサーバを利用できない。この設定については後程議論する。

5.3 プロトコル

サーバの送受信プロトコルは HTTP プロトコルを参照した。サーバのプロトコルは HTTP プロトコルと同じステートレスである。サーバはクライアントからのアクセス要求を受け、パスワードが保存されている場合は保存してあるパスワードを、パスワードが保存されていない場合は空文字をクライアントに送信してクライアントの接続を終了する。

クライアントからの送信データは"GET:"と"POST:パスワード"の 2 種類がある。送信データが"POST:パスワード"の場合は、まずサーバに保存されているパスワードを送られたパスワードで更新する。そのあとどちらの場合もサーバに保存されているパスワードをラッパプログラムに送信する。

5.4 セキュリティ

ラッパプログラムからサーバプログラムへのアクセスは同一パソコン内に限定している。TCP/IP で通信しているので、サーバはパソコンに登録されている全ユーザからアクセス可能である。一般にアクセス制御等を行うサーバの設定はサーバが起動しているコンピュータに保存されている。サーバとクライアントが別のパソコンで動いている場合は、アクセス制御のためのパスワード等サーバの設定をクライアントから見る或いは変更することはできない。しかしサーバとクライアントが同一のパソコンで動いている場合、管理者権限等を用いてサーバの設定を見ることができる。つまりパソコンに管理者権限を持つ複数のユーザが登録されている場合、パスワード付 ZIP ファイルのパスワードを他の管理者権限を持っているユーザから完全に防御する方法を見つけ出せなかった。そこでパスワードを保護するために管理者権限を所有しているユーザが一人だけの場合にサーバプログラムを起動できるように、ラッパプログラムの設定でサーバプログラムの起動を選択できるようにした。デフォルトの設定ではサーバプログラムは起動しない。

6 ラッパプログラムの起動

Windows のデフォルト設定では ZIP ファイルをダブルクリックするとエクスプローラーが起動する。Windows での ZIP ファイルをダブルクリックした場合のデフォルトの振る舞いを変えることができなかったので、ファイルを右クリックしたときに表示されるメニューに"CryptoWrapper"の項目を設け、ラッパプログラムを起動する事にした。

7 今後

現在、今回開発したラッパプログラムの実証実験を行っている。その結果を待って更に改良を行う予定である。

それ以外にいくつか改良を予定している。今回開発したプログラムは Windows 向けである。パソコンユーザには Mac ユーザも多数いるので、Mac 版も作成する予定である。

また、今回は暗号化方式としてセキュリティ強度の高くないパスワード付 ZIP を選んだ。これ以外にも暗号化方式を活用出来るようにする予定である。

参考文献

[1] 独立行政法人 情報処理推進機構(IPA)、初めての情報セキュリティ対策のしおり(第 1 版)、1-5 ページ、2012 年、http://www.ipa.go.jp/security/antivirus/documents/09_hazimete.pdf

[2] NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ、2015 年情報セキュリティインシデントに関する調査報告書【速報版】Ver. 1.0 、4 ページ、2016 年 、http://www.jnsa.org/result/incident/data/2015incident_survey_sokuhou.pdf
[3] 独立行政法人 情報処理推進機構(IPA)、暗号化による<情報漏えい>対策のしおり(第 1 版)、7-8 ページ、2014 年、https://www.ipa.go.jp/security/antivirus/documents/12_crypt.pdf
[4] Dekart Private Disk 、http://www.dekart.com/products/encryption/private_disk/
[5] セキュリティ・ウェアハウス、http://www.ost-net.com/swh/
[6] 日本年金機構における不正アクセスによる情報流出事案検証委員会、検証報告書、12 ページ、2015 年、http://www.mhlw.go.jp/kinkyu/dl/houdouhappyou_150821-02.pdf
[7] 独立行政法人 情報処理推進機構(IPA)、電子メール利用時の危険対策のしおり(第 4 版)、11 ページ、2012 年、http://www.ipa.go.jp/security/antivirus/documents/07_mail.pdf
[8] 7-Zip、http://www.7-zip.org/