6W-05

自己消去プログラムによるデータ流出への対応

石川 達大† 小高 知宏† 黒岩 丈介† 白井 治彦‡ 諏訪 いずみ†
† 福井大学工学研究科 ‡ 福井大学工学部

1. はじめに

現在、インターネットの普及によりパソコンやスマートフォンをはじめとして情報システムが広く実装されるようになり生活に欠かせないほど深く浸透している。そのため、セキュリティが重要視され強化されているが情報漏洩がしばしば見受けられる。従来の情報漏洩防止システムでは、機密情報が外部に出る前に情報漏洩を防止している。従来の情報漏洩防止システムでは新しい攻撃やウイルスが生まれることにより、完全に情報漏洩を防ぐことが出来ない。そこで、機密情報が外部に出た後に情報漏洩を防止する方法を考えた。

先行研究として自己消去プログラムによる情報漏洩防止システムを開発した [1]。この研究では、外部に機密情報が出た場合、自分以外のパソコンで機密情報が開かれたら、自己消去プログラムが実行され機密情報自体を消去することによって情報漏洩を防止する研究である。この研究では、実行環境が制限されてしまう問題点があり java 言語を用い os に依存しない自己消去プログラムを作成した [2]。しかし、先行研究では機密情報をテキストファイルでしか編集することが出来ない。各企業や団体では、テキストファイルで機密情報を保存していることは考えにくく、バイナリファイルで保存されていることが想定される為、一般的に利用するには難しい。

そこで、本研究では機密情報がテキストファイルだけでなくバイナリファイルでも編集・表示可能な自己消去プログラムを作成し、動作確認を行う。

2. 自己消去プログラムによる情報漏洩防止システム

自己消去プログラムによる情報漏洩防止システム構成を図 1 に示す。

自己消去プログラムによる情報漏洩防止システムは、実行したらまず OS 名を取得する OS 名によってプログラムの処理が分かれる。OS 名 が Windows 又は Linux の場合 ip アドレスの取得に移る。 OS 名が Window 又は Linux 以外の OS の場合、機密情報自体を消去し

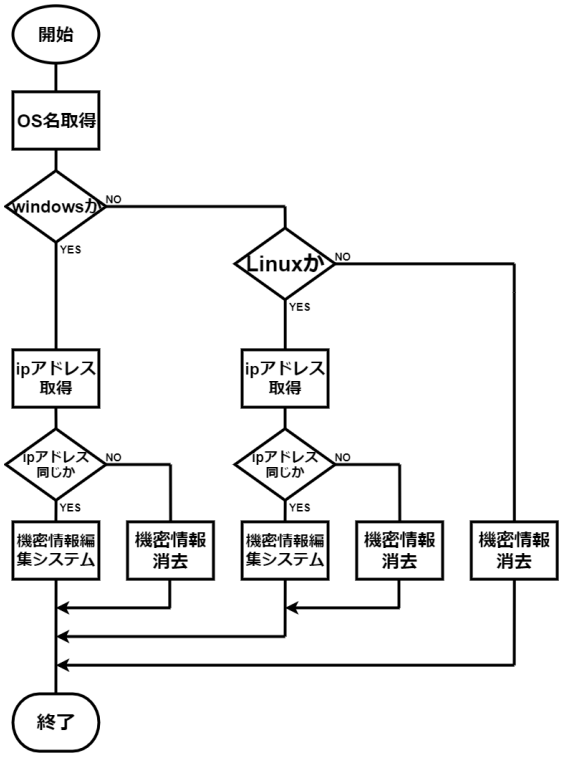

図 1: システム構成

情報漏洩を防止する。

ip アドレスを取得の処理の後 ip アドレスが同じか相違かで処理が分かれる。 ip アドレスが同じ場合、機密情報編集システムに移る。機密情報編集システムは、機密情報を編集・保存したファイルを消去することによって攻撃者に容易に機密情報を取られないシステムである。また、機密情報を保存したファイルを消去しても前回編集した機密情報の内容が 2 回目以降の実行の時に表示されるシステムである。 ip アドレスが相違の場合、機密情報自体を消去する。

自己消去プログラムによる情報漏洩システムは、上記のような流れのシステムである。実行環境を制限しないために OS 名で判断し、 ip アドレスを取得することによって自分又は自分以外のパソコンかを判断している。自分以外のパソコンの場合自己消去プログラムを実行し、機密情報自体を消去することによって情報漏洩を防止するシステムである。

Response to data leakage by self-erase program
†Tatsuhiro Ishikawa †Tomohiro Odaka †Josuke Kuroiwa
‡Haruhiko Shirai †Izumi Suwa
†Graduate School of Engineering, University of Fukui
‡Faculty of Engineering, University of Fukui

3. 方法

現在の自己消去プログラムによる情報漏洩防止システムでは、テキストファイルで機密情報編集・表示を行えるがそれ以外のファイルでは実行することが出来ない。そこで、本研究ではバイナリデータを用いることによってバイナリファイルでも自己消去プログラムによる情報漏洩防止システムを実行する方法を考えた。

現在の自己消去プログラムによる情報漏洩防止システムでは、テキストファイルの中身の文字列を配列に格納し編集・表示を行っている。そのため、ファイル自体ではなく中身のみ扱っている。本研究では、バイナリデータを用いる。バイナリデータはファイルの中身だけでなくファイル自体のデータも含まれている為、バイナリデータを配列に格納することが出来れば、機密情報が書かれているファイル自体の自己消去プログラムを作成出来る。

本研究では、自己消去プログラムによる情報漏洩防止システムの機密情報編集システムを変更し、バイナリファイルでも編集・表示可能な自己消去プログラムの作成を考える。機密情報として読み込んでくるデータをテキストデータではなく、バイナリデータを読み込むことによってすべてのファイルで自己消去プログラムを実行することが出来ると考えた。

3. 動作実験

動作実験として、以下の 2 つの実験を行う。

動作実験 1 として、自分のパソコン上で機密情報を埋め込んだ自己消去プログラムを実行し、機密情報が表示されるのか・編集できるのかの実験を行う。機密情報を 2 回以上開き前回編集・保存した機密情報が表示されるのかの確認を行う。テキストファイルのみでなくバイナリファイルで自己消去プログラムを実行しても、機密情報を編集することができ表示されるのかの確認を行う。

動作実験 2 として、自分以外のパソコン上で機密情報を埋め込んだ自己消去プログラムを実行し、機密情報自体が消去されるのかの実験を行う。バイナリファイルで実験を行い、自己消去プログラムを実行し、機密情報自体が消去されるのかの実験を行う。

4. 考察

テキストデータではなくバイナリデータを用いることによってテキストファイルのみではなく、バイナリファイルで自己消去プログラムを実行することができるのかの確認を行った。テキストファイルでのみの自己消去プログラムの実行だと、メモ帳などで機密情報を保存するため実用的でない。本研究で、バイナリファイルで自己消去プログラムを実行することができた場合、各企業や団体で自己消去プログラムを実用することができる。バイナリファイルで自己消去プログラムを実行することができる場合、OS に関係なく自己消去プログラムを実装することができ、容易に自己消去プログラムを実装することができる為、実用的であると考える。また、自己消去プログラムによる情報漏洩防止システムは、従来の情報漏洩防止システムと併用することが出来るため、更に情報漏洩を防止することが出来ると考える。

現在では、バイナリファイルで自己消去プログラムを作成したが、ファイルが 1 つの場合を想定して自己消去プログラムを作成した。今後の課題として、各企業や団体では機密情報をファイル 1 つのみで保存している場合は少ないと考えられるため、ファイル 1 つのみではなく機密情報が入ったフォルダごと自己消去プログラムを実行する方法を考える。フォルダごと自己消去プログラムを実行するためには容量が大きいためエラーが出ると考えられる。そこで zip ファイルなどの圧縮ファイルを用いてフォルダごとの自己消去プログラムを作成したいと考える。

また、現在は自己消去プログラムは実行ファイルを開く又は実行すると自己消去プログラムが実行される。実行ファイルを開く又は実行するのではなく自分のパソコンから出た瞬間に自己消去プログラムを実行する方法を考える。

5. まとめ

自己消去プログラムによる情報漏洩防止システムではテキストファイルのみを扱っていたがバイナリファイルを扱う自己消去プログラムの作成を行った。バイナリファイルでの自己消去プログラムを作成することで、実用性があがり各企業や団体で実装することができると考えた。今後はフォルダごとの自己消去プログラムの作成と新たな自己消去プログラムの実行方法を考えることが課題である。

参考文献

[1] 石川　達大, 小高 知宏, 黒岩 丈介, 諏訪 いずみ, 白井 治彦. 自己消去プログラムによる情報漏洩防止システム. 平成 28 年度電気関係北陸支部連合大会 2016.

[2] 石川　達大, 小高 知宏, 黒岩 丈介, 諏訪 いずみ, 白井 治彦. 実行環境への依存性を低減した自己消去プログラムの構成方法. 平成 28 年度電気関係北陸支部連合大会 2017.