L-014

# 位置情報を用いた自己消去プログラム

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、 ip アドレスを用いて機密情報が外部に出たかどうかを判断している。 ip アドレスはネットワーク上での住所であるが、変更可能なため実際にネットワーク上で外部に機密情報が出たかどうかを判断するには不確定な部分が大きい。そこで、本研究ではネットワーク上の住所である ip アドレスだけではなく物理的な位置情報を用いて機密情報が外部に出たかどうかを判断する自己消去プログラムを作成し、動作確認を行う。 ip アドレスを用いることによってネットワーク上の情報を取得し、それに加えて物理的な位置情報を取得する。2 つの判断基準を用いることによってより外部に出たかどうかの判断を正確にすることによって実用的な自己消去プログラムの作成する。

## 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 ip アドレスを取得する。 ip アドレス取得後 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、位置情報取得の処理に入る。ip アドレスが相違の場合、機密情報自体を消去する。

位置情報取得後、位置情報が自分がパソコンを使用する範囲の場合 os 名取得の処理に入る。位置情報が使用する範囲外の場合、パソコンごと持ち去られたり機密情報を抜き取られ別の場所で機密情報が漏洩する可能性が高いため機密情報自体を消去する。

OS 名を取得後 OS 名によってプログラムの処理が分かれる。現在自己消去プログラムによる情報漏洩防止システムは OS 名 が Windows 又は Linux の場合のみ実行することが出来る。その為 OS 名が Windows 又は Linux の場合は機密情報編集システムの処理に入る。OS 名が Window 又は Linux 以外の OS の場合、機密情報自体を消去し情報漏洩を防止する。

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。

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。 ip アドレスを取得することによってネットワーク上の情報を取得し、位置情報を用いることによって物理的な位置情報を取得し外部に出たかどうかを 2 つの判断基準で判断している。また実行環境を制限しないために OS 名で判断している。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。

## 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、機密情報が外部に出たかどうか判断する方法として ip アドレスを用いて判断している。 ip アドレスは変更することが出来るため、 ip アドレスのみで機密情報が外部に出たかどうか判断した場合、間違っている可能性もある。そこで、本研究では物理的な位置情報も用いることによって判断基準を 2 つにし、機密情報が外部に出たかどうかの正確性を高める方法を考えた。

---

Self-erase program using location information program
†Tatsuhiro Ishikawa †Tomohiro Odaka †Josuke Kuroiwa ‡Haruhiko Shirai †Izumi Suwa
†Graduate School of Engineering, University of Fukui
‡Faculty of Engineering, University of Fukui

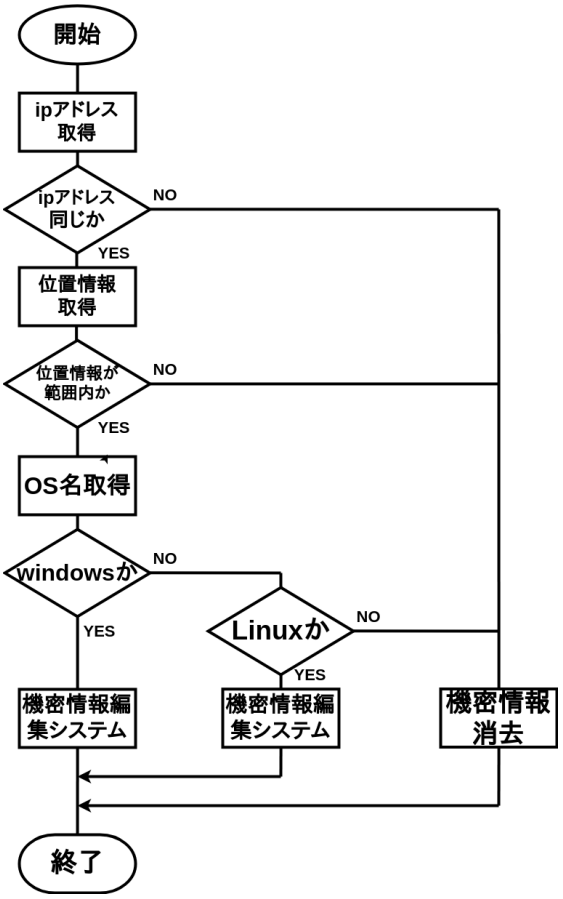


図 1: システム構成

位置情報は Geolocation API を用いることによって取得する。 Geolocation API では、無線 LAN・WiFi・携帯電話基地局・ GPS ・ IP アドレスなどから位置情報を取得する。端末によって色々あった位置情報取得の仕組みを標準化したものである。GPS だけではなく多様な要因から位置情報を取得することが出来る。この Geolocation API を用いることによって物理的な位置情報を取得することが出来る自己消去プログラムの作成を考える。

## 4. 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

本研究では、機密情報が外部に出たかどうかを変更される可能性が高い ip アドレスだけではなく物理的な位置情報を用いることによってより正確性が高く判断することが出来る自己消去プログラムの実装、動作実験を行った。 ip アドレスだけでなく物理的な位置情報を用いることによって機密情報が外部に出たかどうかの判断基準を 2 つにすることができ、正確性が高くなったと考える。

ip アドレスや MAC アドレスは変更することができるが GPS 等の物理的な位置情報を書き換えることは難しい為、機密情報が外部に出たかどうかの判断には最適で実用的であると考える。

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、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、 ip アドレスのみを用いて機密情報が外部に出たかどうかを判断していたが物理的な位置情報も併用して機密情報が外部に出たかどうかを判断する自己消去プログラムの作成を行った。2 つの判断基準で判断することによってより正確に判断することが出来ると考える。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.