セキュリティインシデント対応のためのユーザ特定支援システムの実装

上原 雄貴† 水谷 正慶‡ 武田 圭史‡ 村井 純††

†慶應義塾大学 総合政策学部 ‡慶應義塾大学大学院 政策・メディア研究科 ††慶應義塾大学 環境情報学部

1 はじめに

ネットワーク上でセキュリティインシデントが発生した場合，ネットワーク管理者は即時に対応して被害を最小限に抑制する必要がある．特に，ホスト利用者の裁量により構成が変化するネットワーク環境下では速やかに当該ホストの所有者または管理者を特定し，その者に対して通知し，事態の収拾と被害の拡大防止につとめなければならない．

本稿では，ホスト利用者の裁量により構成が変化するネットワーク環境下において，インシデント発生時の対応を支援するためのユーザ情報管理システムを実装した．このシステムを利用し，インシデントに関連するホスト利用者の特定と，迅速なインシデント対応が可能となる．

2 問題点

ネットワーク上のホスト利用者を特定するの既存手法として，該当ホストの IP アドレス，MAC アドレスや DHCP から得られた情報から，ホスト利用者を特定する手法や，802.1x などの認証技術を利用する手法が挙げられる．しかし，これらの既存手法は管理者の負担が大きく，手法を導入するコストも高いという問題点がある．

DHCP から得られた情報でホスト利用者を特定する手法は，即時に該当ホストと利用者を対応付けすることは困難である．特に，前述するネットワーク環境下では，多数のホスト利用者から IP アドレスや，MAC アドレス，ホスト名の情報からは該当ホストのホスト利用者を特定することは難しい．DHCP から得た情報で該当ホストの MAC アドレスを取得しても，その MAC アドレスで常にホスト利用者を特定できるわけではない．

また，802.1x などの認証技術や IDlogger[1] を導入する手法は，導入のコストやホスト情報の継続的な管理負担が高い．802.1x の認証技術は，ネットワークに導入する際に，認証サーバ，サプリカント，認証装置を設置しなければならない．そして，ホスト利用者が増える度に管理者はホストを登録しなければならない．これらの手法はネットワーク規模に比例して管理者のマネジメントコストは増加する．そして，IDlogger など，クライアントにアプリケーションを導入して管理する手法は，新規利用者の度にアプリケーションをインストールする必要やネットワーク上のサーバと通信する必要がある．また，一つのホストを複数人が利用していた場合，対象ホストの利用者を識別できないという問題点がある．

3 アプローチ

第 2 節の問題を解決するアプローチとして，通信データからホスト利用者の特徴を抽出し，ホスト利用者のプロファイルを作成する手法を提案する．ホスト利用者はネットワークのサービスを利用する際に，各利用者毎に特徴のある情報を出力している．本手法はこれらの情報を定常的に収集し，ホスト利用者と結びつけたプロファイル作成する．このプロファイルを利用してネットワークに接続しているホストの利用者が特定可能となり，インシデント発生時に該当ホスト利用者に関する情報を迅速に特定できる．

本手法で扱う利用者毎に特徴ある情報とは，通信データから得られるあらゆる情報を対象としている．本手法はネットワークの中継地点に設置したサーバによって通信データを監視することで，宛先 IP アドレスや利用しているサービス，使用時間帯，使用頻度，ペイロードに含まれる ID 情報などが利用できる．これらの情報は組み合わせることによってプロファイル結果の精度を高められる．また，ネットワークの運用ガイドランや利用者の合意に基づき，使用できる情報が制限される場合が考えられるため，少ない情報や曖昧な情報でもプロファイルが作成できる必要がある．そのため，本手法はプロファイルに利用する情報を容易に追加できる拡張性を考慮した実装とし，複数の情報を状況に応じた対応が可能である．

本手法は 802.1x や専用のアプリケーションを各ホストにインストールする手法と比較し管理者のマネジメントコストが軽微であるという特徴がある．本手法は新規にネットワークに接続してくるホストの情報をネットワーク管理者が管理・追加する必要はなく，ネットワーク通信を監視することで自動的に情報を収集する．厳密な認証をしていないため，プロファイル情報を詐称される可能性は考えられるが，マネジメントコストが大幅に少ないと言う点で，本手法の意義は大きいと考える．

4 実装

本手法を実現するのアプローチの一つとして，前提ホスト利用者毎の情報としてアプリケーションで利用されているユーザ ID に着目し，通信データから監視，収集する実装について述べる．ユーザ ID の収集には，プライバシ情報や倫理的な問題があるため，ユーザの同意を得ており，合法な行為であることを前提とする．また，想定するネットワークは 10 から 500 人程度のユーザが利用するネットワーク環境である．

対象とするアプリケーションの ID は Google アカウ

Implementation of User Identification Support System for SecurityIncident Response

Yuki Uehara†, Masayoshi MIZUTANI‡, Keiji TAKEDA‡and Jun MURAI††

†Faculty of Policy Management, Keio University
252-8520, Kanagawa, Japan

‡Graduate School of Media and Governance, Keio University
252-8520, Kanagawa, Japan

††Faculty of Environment and Information Studies, Keio University
252-8520, Kanagawa, Japan

{nakajima, mizutani, keiji, jun}@sfc.wide.ad.jp

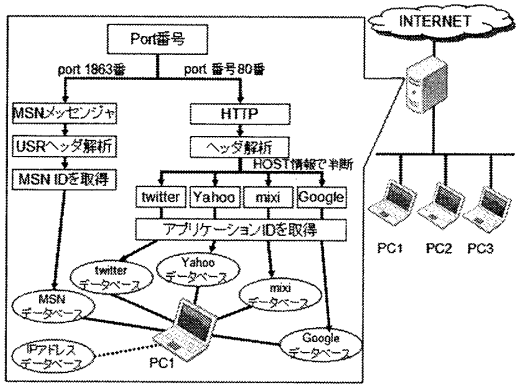

図 1: 動作概要

ント，Yahoo アカウント，MSN メッセンジャーで使用するアカウント情報 (メールアドレス)，mixi アカウント ID，twitterID の 5 つとした．本稿ではこれら 5 つをアプリケーションユーザ ID と呼ぶ．

監視するネットワークでのトラフィックが流れる中継点に監視サーバを設置する．取得したトラフィックから，TCP/UDP のポート番号が MSN メッセンジャー (1863)，HTTP(80) のパケットのみを取得する．ポート番号が 80 番の場合，ペイロードを解析してアプリケーション ID を取得する．

ID を中心に各々のテーブルを結びつけて増設を容易するため，複数のデータベースを作成する．図 1 で示すように，取得したアプリケーション ID をデータベースで格納し，プロファイルを作成する．

次に，このプロファイルの手法の特徴を述べる．ホスト利用者が別の IP アドレスで再接続した場合でも，特定が可能となる．その際に，　同じ IP アドレスから別のサービスを利用した場合，以前に作成した情報と結びつける．異なる IP アドレスで接続した場合でも，一度テーブルに登録されたアプリケーションユーザ ID が一致したら，同一人物とする．一つのサービスで ID を複数持つホスト利用者も，この手法で特定できる．

別のホスト利用者が同じ IP アドレスを使用している場合でも，識別することができるように，IP アドレス有効期限を設置した．有効期限の設置により，一つのホストを複数のホスト利用者が利用した場合でも個別に判別できる．

インシデント発生時，前述の手法によって情報を収集することで，インシデントに関連すると考えられる IP アドレスからホスト利用者を特定できる．また，アプリケーションユーザ ID を取得した際のアプリケーションを利用し，ホスト利用者を特定できる．

5　評価

本手法では，通信データを監視するため，想定する環境で運用した場合，プライバシ情報などの問題が発生する可能性がある．そのため，

筆者が所属する研究室の 50 名程度が利用するネットワーク環境下で，本手法によって ID 情報が収集可能となる範囲を示した．

前述したネットワーク環境下において，取得できる IP アドレスをプロファイルできるの範囲を検証し，本手法の有効性を評価した．取得したパケットヘッダの宛先 IP アドレスが，対象アプリケーションサーバに関連するのいずれかであった場合，その IP アドレスはプロファイルできたものとする．対象アプリケーションサーバは，ヘッダのみでログインできたと推測か容易である twitter,mixi,MSN メッセンジャを評価対象とした．

プロファイルできた IP アドレス数を取得した IP アドレス総数で割ることによって導き出す．
2009 年 1 月 13 日 15 時 57 分から 1 月 14 日 15 時 56 分までの間，パケットを観測し，結果は表 1 のようになった．取得した IP アドレスが 72 に対し，プロファイルできた IP アドレス数は 3 である．本結果、全体の約 4%のプロファイルが取得できた．

表 1: プロファイル範囲の評価

総数	プロファイル数	成功率
72	3	4%

この割合はインシデント発生時のホスト利用者の特定に際して十分な割合ではない．しかし，本手法の評価方法では，トラフィックを取得した期間のネットワーク利用状況やホスト利用者の振る舞いによって，評価結果にかなりの差異が発生してしまう．そのため，一日だけの評価期間では十分とは言えない．

6　本手法においての課題

6.1　プライバシを考慮したシステムの検討

本手法においては，ホスト利用者の同意を得ていることを前提で，実装した．しかし，ペイロードを監視するため，プライバシに関する倫理的な問題がある．そのため，プライバシーの保護とトラッキングの可能性を両立するシステムを検討する．例えば，アプリケーションユーザ ID をハッシュ値とすることによって，特定の条件でのみしかアプリケーション ID を閲覧できないといった方法や，ガイドラインを作成するといった方法が挙げられる。

6.2　共通アカウントの対応

本稿では，実装で述べたように，複数のホスト利用者が一つの共通アカウントを利用することを考慮していない．同ネットワーク上でホスト利用者が共通アカウントを利用した場合，共通アカウントを使用したすべてのホスト利用者が同一であると見なされるされるため，改善する必要がある．

6.3　評価期間の検討

本手法の評価により，4%程度の評価結果しか得ることができなかった．これは，ホスト利用者が対象アプリケーションを利用しない場合など，ホスト利用者の振る舞いによって評価結果の差異が発生する．そのため，長期間で評価を行う必要がある．

7　まとめ

インシデント発生時，ユーザの裁量により構成が変化するネットワーク環境下では，即時にユーザに連絡する必要がある．そこで、動的にユーザ情報を取得・管理することにより，インシデント発生時の対応を支援するシステムを実装した．また，評価実験により，4%カバーしかしておらず，本手法が有効どうかを継続的に観測する必要がある．

参考文献

[1] OAK INFORMATION SYSTEM COROORATION . *IP* アドレスからログオンユーザ名を特定できるアプライアンスサーバ「*IDLogger*」. http://www.oakis.co.jp/idlogger/index.html