社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DPS－125（6）
2005－ EIP － 29（6）
2005／11／14

パーソナルIDSを用いたモバイルネットワークにおけるセキュリティ情報提供サービス

東 雄介* 川口 信隆* 小畑 直裕* 塩澤 秀和‡ 重野 寛† 岡田 謙一†

本稿ではパーソナル IDS を用いたモバイルネットワークにおけるセキュリティ情報提供サービスを提案する．ホットスポットのようなモバイルネットワークサービスでは, セキュリティ上の脅威をもたらす悪意あるユーザも含めて, 多数の匿名のユーザが存在する．そのようなモバイルネットワークにおいてユーザが接続先のセキュリティ情報を取得することは安全に接続するために大変有益なことである. しかし, 現状ではユーザは十分なセキュリティ情報を取得することは困難である．そこで本稿ではパーソナル IDS を用いたセキュリティ情報提供サービスを提案する．本提案は各地のネットワークに接続している個人端末の IDS（パーソナル IDS）から収集した IDS ログを用いてネットワークの状況を分析, セキュリティ情報を算出し, 管理体制によらないセキュリティ情報の提供を実現する．

Security Information Provider Service of Mobile Networks using Personal IDS

Yusuke AZUMA * Nobutaka KAWAGUCHI*
Naohiro OBATA* Hidekazu SHIOZAWA‡ Hiroshi SHIGENO† Kenichi OKADA†

In this paper, Security Information Provider Service of Mobile Networks using Personal IDS is proposed. In mobile network services such as hot spot services,many anonymous users including malicious ones share a network and it may cause security threats. The serutiry information of the mobile networks is the inportant factor to find the networks the users can access to safely.However most networks do not provide such information to the users. Therefore in this paper, we propose a security information provier service using personal IDS. Our service provides security information by collecting and analyzing logs from Personal IDS connected to the networks. As a result our service enables to find the safe networks without relying on official information from the networks.

1　はじめに

ノート PC，PDA などの携帯端末や無線 LAN の普及に伴い，ホットスポットなどのモバイルネットワークサービスの増加・多様化が進んでいる．これらモバイルネットワークサービスは, ユーザの匿名性が高く，悪意あるユーザが比較的容易にネットワークに入り込めてしまうなどセキュリティ面での不安を抱えている．

このような現状からユーザがモバイルネットワークに安全に接続するためにはネットワークのセキュリティ情報を事前に入手してなんらかの対策を立てる必要がある．しかしながら，モバイルネットワークサービスのセキュリティ対策レベルや管理体制は不明確で信頼性が低く，セキュリティ情報が公開されることは少なく情報の信頼性も高いとはいえない．

その一方で個人のセキュリティに対する意識は高まってきており，個人の端末にもパーソナルファイアウォールや IDS が搭載されるようになってきている．

そこで本稿では，個人端末の IDS（パーソナル IDS）を用いたモバイルネットワークにおけるセキュリティ情報提供サービスを提案する．本提案は，各地のモバイルネットワークに接続しているパーソナル

* 慶應義塾大学 大学院 理工学研究科
Graduate School of Science and Technology, Keio University

† 慶應義塾大学 理工学部
Faculty of Science and Technology, Keio University

‡ 玉川大学工学部
Faculty of Technology, Tamagawa University

IDS からセキュリティログを取得し，ネットワーク状況を分析し安全性を評価することで，ネットワークの管理体制に依存しないセキュリティ情報の提供サービスを実現する．本稿では，プロトタイプの実装を通じて評価指標の妥当性を示した．またパーソナル IDS における検知に関する考察をシミュレーションを通じて行った．

本稿では，まず 2 章で既存の関連研究について触れ，3 章でセキュリティ情報提供サービスの基本モデルを提案する．4 章では本提案の基本モデルの有効性を実装実験を通じて示し，5 章ではパーソナル IDS における検知に関する考察とシミュレーションを行う．6 章を本稿のまとめとする．

2 関連研究

ネットワークの様々な地点で IDS を設置し, 広範囲にわたってネットワークを監視することは, ネットワーク間での攻撃比較ができたり, 攻撃予兆の早期発見によって被害を抑制できるなど有益な点が多い．Stainford らが Cyber”Center for Disease Control” [1] という広域監視システムの有効性・必要性について言及しているように今後重要な役割を占めるようになると考えられる．

2.1 ログの統合分析

広範囲にわたるネットワークを監視するには複数の IDS をまとめて運用する必要があるが, 冗長なログが多量に出力され出現頻度の低いログを見落としがちになり, 新たな異常を見逃してしまうなどの問題がある．

竹森らが提案する IDS ログ分析支援システム [2] [3] では, 長期間のログ出力特性に対する短期間のログ出力特性の異常率, 他ネットワークのログ出力特性に対する注自ネットワークのログ出力特性の異常率を算出する．そして, その異常率を用いて検証不要な攻撃ログの示唆による冗長なログの排除, 効率的な異常ログの抽出を実現している．

2.2 IDS 情報の共有

IDS 情報を共有することで，より効率よく攻撃を検知し被害を抑えることができる．

Janakiraman らが提案する Indra [4] では，P2P ネットワークを用いて情報を共有する．ネットワーク内のあるユーザが攻撃を受けた時，攻撃先の IP アドレスを調べ，その IP アドレスをネットワーク内の他のユーザに教えることでそれ以上その攻撃先からの被害を受けないようにしている．

Yegneswaran らが提案する DOMINO [5] は，ネットワークのドメイン間でログの共有をするシステムであり，大規模な攻撃の検知がフォレンジックコンピューティングに利用可能である．

3 セキュリティ情報提供サービスの提案

3.1 コンセプト

本章ではパーソナル IDS から IDS ログを収集・分析することでセキュリティ情報を提供するサービスを提案する．

セキュリティ情報をユーザに提供しているモバイルネットワークは少なく，ユーザは実際に接続するまで接続先ネットワークが安全かどうかを知ることは困難である．本提案では，各ネットワークに接続している個人端末の IDS モジュール（パーソナル IDS）からのログを収集し分析することでこの問題を解決する．近年，個人の端末にも IDS モジュールをもつものが増加しており，本提案では管理体制に依存しない情報をこのパーソナル IDS から取得する．

本提案では, 次の 2 つのセキュリティ情報を提供する．

- ユーザの現在地から近くに存在するモバイルネットワークの安全性評価指標
- ネットワークに安全に接続するために必要なホストのセキュリティ設定

本サービスでは，それぞれのネットワークの安全性として異常指標を用いる．この指標が高い数値を示すほど，そのネットワークの安全性は低い．また, それぞれのネットワークに存在している攻撃の中にユーザホストの脆弱性をつくものがあるかどうかをチェックし，安全に接続するための方法を脆弱性マッチング情報として提示する．

異常指標と脆弱性マッチング情報については, 後のセクションで詳しく述べる．

3.2 サービスプロトコル

本サービスの手順を図 1 に示し, 以下に説明する．各構成要素は次のようになっている．

- **パーソナル IDS** 各ネットワークに接続している個人端末の IDS モジュール．
- **ログ収集サーバ** IDS クライアントから IDS ログを分析するサーバ
- **情報提供サーバ** 脆弱性マッチングを行い，ユーザにセキュリティ情報を提供するサーバ
- **サービスクライアント（ユーザ）** 本サービスを利用するユーザ

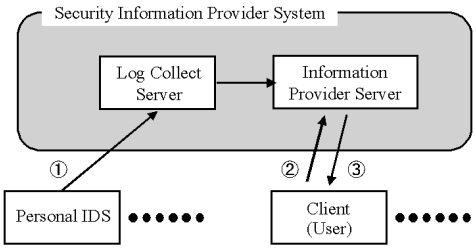

図 1: サービスの流れ

以下, サービスの流れを説明する.

1. ログ収集サーバが様々なモバイルネットワークのパーソナル IDS(Snort [6] など) からのログを定期的に収集し，必要な要素を抽出して分析, 異常指標を出す.
2. 情報提供サーバは, ユーザの近くにあるモバイルネットワークの異常指標を提供する．また合わせてユーザホストの脆弱性マッチングを行い, ユーザの脆弱性をつく攻撃の有無, その攻撃への対策法を提供する.
3. ユーザは, 取得したセキュリティ情報から安全なネットワークに接続，もしくは安全となるようセキュリティレベルの変更を行う.

3.3 異常指標

ログ収集サーバでそれぞれのネットワークの異常指標を算出する．異常指標にはネットワーク軸異常指標と時間軸異常指標の 2 つがある.

ネットワーク軸異常指標

ネットワーク軸異常指標は，他のネットワークと比べて分析するネットワークのログがどの程度異常であるかを示す.

E_{mk} はネットワーク m で検出された攻撃 k の数, N_{mk} はネットワーク m で攻撃 k のログを送信した IDS 数， そして l_k は攻撃 k の危険度を示す．ネットワーク m の危険度 L_{net_m} は,

$$L_{net_m} = \sum_k \left(\frac{E_{mk}}{N_{mk}} \times l_k \right) \tag{1}$$

となる.

そして，ネットワーク m のネットワーク軸異常指標 W_m は,

$$W_m = \frac{L_{net_m}}{\left(\sum_l^n L_{net_l}\right)/n} \tag{2}$$

となる.

ここで n は分析対象のネットワーク m を除くすべてのネットワークの数を表す.

時間軸異常指標

時間軸異常指標は，最近収集されたログが過去に収集されたログと比べてどの程度異常であるかを示す.

ネットワーク m は分析対象のネットワークである．t_{short} は分析対象のタイムインターバル，そして t_{long} 比較対象となる過去長期間のタイムインターバルを示す．E_{tmk} はタイムインターバル t で検知された攻撃 k の数，N_{tmk} は攻撃 k のログを送信した IDS 数，l_k は攻撃 k の危険度を示す．分析対象タイムインターバル t_{short} の危険度 L_{t_m} は,

$$L_{tm} = \sum_k \left(\frac{E_{tmk}}{N_{tmk}} \times l_k \right) \tag{3}$$

となる.

そして，時間軸異常指標 $T_{t_{short}m}$ は,

$$T_{t_{short}m} = \frac{L_{t_{short}m}}{\left(L_{t_{long}m}\right) / \left(\frac{t_{long}-t_{short}}{t_{short}}\right)} \tag{4}$$

となる.

3.4 脆弱性マッチング情報

情報提供サーバは，それぞれのネットワークに存在する攻撃とクライアントの OS のバージョン情報やアップデート情報をマッチングする．そして，脆弱性をつく攻撃が存在するかどうかをチェックした結果およびそのネットワークに安全に接続する対策（必要なアップデートなど）を提示する.

4 評価

本章では提案の基本モデルの評価をプロトタイプの実装実験を通じて行う.

4.1 実験環境

提案サービスのプロトタイプシステムを実装し，実験を行った．図 2 に示すようにそれぞれ 2 つのホストを持つ 3 つのネットワーク（NW1〜3）を作成した．ネットワークは 100MbpsLAN，OS は Windows2000 および XP を用いて行った．また IDS モジュールとして Snort2.0 を用いてログの収集を行い，攻撃ツールとして nmap3.75 [7] を用いてポートスキャンを行った.

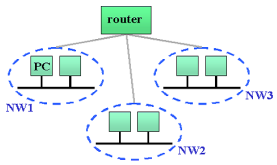

図 2: 実験ネットワーク構成

4.2 指標の変化

ポートスキャンツール nmap を用いて TCP ステルススキャン，UDP スキャンを行い, それに対する各指標の変化を調べた.

4.2.1 ネットワーク軸指標の変化

NW1〜3 のすべてに TCP ステルススキャンを行った際のネットワーク軸指標を図 3 に，NW1 について TCP ステルススキャンと UDP スキャンの両方を行い，NW2，3 について TCP ステルススキャンを行った際のネットワーク軸指標を図 4 に示す.

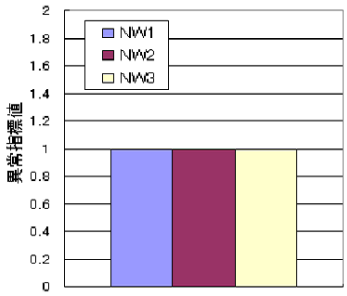

図 3: ネットワーク軸指標 (1),NW1〜3:TCP

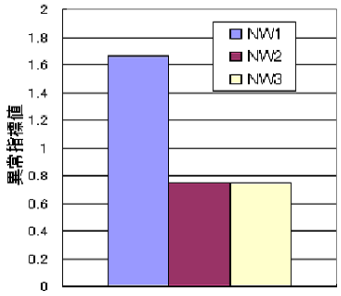

図 4: ネットワーク軸指標 (2),NW1:TCP+UDP, NW2,3:TCP

図 3 を見てわかるように各ネットワークに対し均等に攻撃が行われている場合，ネットワーク軸指標は等しくなる. また，図 4 を見てわかるように他のネットワークよりも攻撃が多く行われている NW1 ではネットワーク軸指標は大きくなっている.

4.2.2 時間軸指標の変化

タイムインターバル $t_{short} = 10t$, 比較タイムインターバルを $t_{long} = 60t$ として実験を行った．１０ t 毎に TCP ステルススキャンのみ，TCP ステルススキャンと UDP スキャン両方の２通りの攻撃を交互に行った際の NW1 の時間軸指標の変化を図 5 に示す.

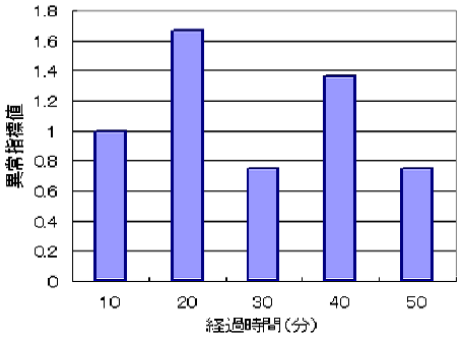

図 5: 経過時間と時間軸指標の関係

図 5 からわかるように攻撃の増減に伴い時間軸指標は増減している．また過去の傾向によってその増減の幅は変化している.

以上から, 攻撃の増減に伴いそれぞれの指標は適切に変化していることを示すことができた.

4.3 レスポンスタイム

サービスクライアントが要求を出してからセキュリティ情報を取得するまでのレスポンスタイムを調べた．処理ログ量に対するレスポンスタイムを図 6 に示す.

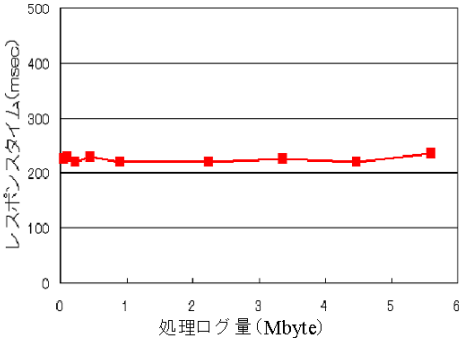

図 6: 処理ログ量とレスポンスタイムの関係

図6からわかるようにレスポンスタイムは220msec程度におさえることができた．これは異常指標の算出は常にログ収集サーバでバックグラウンドで行い，情報提供サーバには脆弱性マッチングによる負荷だけがかかるようにしているためである．

5 パーソナルIDSにおける検知に関する考察

本章では，まずパーソナルIDSの検知性能の制限について述べ，次に空間軸における制限を低くするためのARPを用いたアドレススキャンの検知手法について考察する．

5.1 パーソナルIDSの検知性能における制限

提案するサービスでは，個々のホストのパーソナルIDSから寄せられるセキュリティログを元にネットワークの安全性を評価する．ここで組織ネットワークなどのネットワークIDSと比較して，パーソナルIDSは以下の3つの制限がある．

（1） 空間軸における情報量の制限

ネットワーク全体の情報（パケットログなど）を参照可能なネットワークIDSとは異なり，個々のパーソナルIDSが得られる情報は，ホストが受信する，もしくはホストが送信するパケット等に限られる．このため，アドレススキャンのように，攻撃対象が複数のホストに跨る攻撃を検知するのは容易ではない．

（2） 時間軸における情報量の制限

個々のパーソナルIDSは，ホストがネットワークに滞在している間のみ検知を行う．ここで，個々のホストがモバイルネットワークに滞在する時間は比較的短いと考えられるため，スロースキャンなど，検知に長期間のネットワーク情報が必要な攻撃をパーソナルIDSが検知するのは容易ではない．

（3） セキュリティログへの信頼性の制限

悪意があるユーザがパーソナルIDSのセキュリティログを改竄して意図的にネットワークの安全度を低くみせかけようとしたり，反対にセキュリティログをログ収集サーバに送信せずネットワークの安全度を高くみせかけようとする，という攻撃が考えられる．このため，サービス側では1つホストから受信したセキュリティログを完全に信頼することは難しく，他のホストから受信したログと対応づけることで，このような攻撃を検知する必要がある．

5.2 ARPを用いたアドレススキャンの検知に関する考察

通常，アドレススキャンの検知は，同一ホストから送信される無効なIPアドレス宛のパケットを検知することにより行われる．しかし，宛先ホスト以外の通常ホストがこのパケットを取得することはできない．よってパーソナルIDSがこの手法を用いて検知することは難しい．そこで我々はARPリクエストを利用した検知手法を用いる．

5.2.1 検知手法

ホストが同一ethernet内のホストにIPパケットを送信しようとする場合，まずARPリクエストをブロードキャストし，これに対応するARPリプライを受信することで，送信先IPアドレスに対応するMACアドレスを解決する必要である．ここで，送信先IPアドレスを持つホストが存在しない場合やスイッチ内などでロスが起きた場合，ARPリプライを受信することは出来ない．この場合，ARP送信ホストは短時間に連続して数回ARPリクエストを再送し，それでもARPリプライが受信できない場合，MACアドレスの解決をあきらめる．よって，悪意あるホストやワームがアドレススキャンを行う場合，同一ホストあての連続したARPリクエストが大量に送信される．そして，ARPリクエストはブロードキャストされるため，モバイルIDSも取得することが可能である．

我々は以下の簡易な検知アルゴリズムを用いる．

送信元ホストごとの，有効ARPリクエスト数をN_v，無効ARPリクエスト数をN_Iとする．有効ARPリクエストは対象ホストが存在し，IPアドレスの解決が可能なリクエスト，無効ARPリクエストは対象ホストが存在せず，解決できないリクエスト数を示す．そして，スキャン指数Sを

$S = N_V - N_I$

と定義する．そしてSが閾値を超えた場合，当該ホストはスキャンが行っていると判定する．

5.2.2 シミュレーション

提案アルゴリズムの有効性を確認するためのシミュレーションを行った．なお，シミュレーション上での単位時間を$1TU$（タイムユニット）とする．シミュレーション環境を以下に示す．

ネットワーク環境

Cクラスのアドレス空間を持つモバイルネットワークを想定する．各ホストの到着間隔時間は平均$25TU$の指数分布に従い，平均滞在時間時間は一様分布に従うものとする．またDHCPによりアドレスをx.x.x.2からx.x.x.254まで連続に割り当てるものとする．

アドレススキャン

攻撃者はシミュレーション開始後$6000TU$にネットワークに加入しアドレススキャンを行う．アドレ

ススキャンは，DHCP によるアドレスの割り当て同様，x.x.x.2 から x.x.x.254 まで連続して行われる．スキャン速度は 5 アドレス /1TU とする．また検知アルゴリズムのスキャン指数の閾値は 10 とする．

図 7 に，ネットワーク内で最も早くスキャンを検知したホストが検知するまでに，攻撃ホストが送信する有効 ARP リクエスト数と，スキャン開始時の滞在ホスト数を示す．

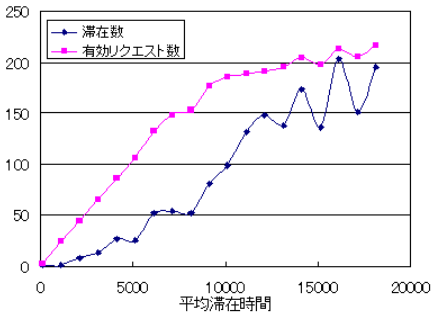

図 7: 有効 ARP リクエスト数と平均滞在時間の関係

図 7 より，平均滞在時間が長くなるほど，滞在ホスト数が増えるため，検知までの有効 ARP リクエスト数は増加する傾向にある．また，有効 ARP リクエスト数と滞在ホスト数の比率は平均して 51.1%になる．

5.3 考察

5.2.2 のシミュレーションより，滞在ホスト数の 51%にリクエストが送信される前に，スキャンを検知することが可能になる．しかし，スキャンが長期間によって行われた場合，時間軸における制限により，スキャンの検知に時間がかかる，もしくは不可能になる可能性がある．さらに，サービス側としては，個々のホストのセキュリティログに高い信頼性をおけないため，複数のホストからのログを対応付け改竄されたログを発見する必要がある．アドレススキャンの場合，ネットワーク内の一定割合のホストが検知することが可能と考えられるため，短時間に同一攻撃を指すセキュリティログが一定数送られてくるはずである．このため，ネットワークにある程度のホストが存在するにもかかわらず，1 台のホストのみがアドレススキャンに関するログを送信した場合などは，不正な送信とみなすことができると言える．このように今後は，空間軸，信頼性における限界を考慮した検知手法を検討していく予定である．

6 まとめ

本稿ではパーソナル IDS を用いたモバイルネットワークにおけるセキュリティ情報提供サービスを提案した．本提案によりネットワークの管理体制に依存しないセキュリティ情報の提供を実現した．プロトタイプの実装実験を通じて，セキュリティ情報として提供する提案指標の妥当性を示すことができた．またシミュレーションによりパーソナル IDS における検知に関する考察を行った．

今後の課題としては，より詳細に様々な状況を想定して指標の妥当性を検討する必要がある．また，5.3 で示したようにパーソナル IDS の検知の限界を考慮した検知手法を検討していく必要がある．

謝辞

本研究は，ＡＳＦ（応用セキュリティフォーラム）の支援のもとで行われた．

参考文献

[1] Stuart Staniford, Vern Paxon, Nicholas Weaver: ”How to Own the Internet in Your Spare Time”, *Proceedings of the 11th USENIX Security Symposium*. 2002.

[2] 竹森 敬祐, 三宅 優, 中尾 康二: ”IDS ログ分析支援システムの提案”, 情処技法, CSEC. 2003 年 5 月.

[3] 竹森 敬祐, 三宅 優, 中尾 康二, 菅谷 文昭, 笹瀬 巌: ”セキュリティデバイスログ分析支援システムの広域監視への適用”, コンピュータセキュリティシンポジウム２００３. 2003 年 10 月.

[4] Ranaoradhu Janakiraman, Marcel Waldvogel, Qi Xhang: ”Indra: A peer-to-peer approach to network intrusion detection and prevention”, *Proceedings of IEEE WETICE 2003 Workshop on Enterprise Security*. 2003.

[5] Vinod Yegneswaran, Paul Barford, Somesh Jha: ”Global Intrusion Detection in the DOMINO Overlay System”, *Proceedings of NDSS*. 2004.

[6] ”Snort”. http://www.snort.org/

[7] ”nmap”. http://www.insecure.org/nmap/