2W-5

コミュニティセキュリティにおける共通プラットフォームに関する研究

渡邊利晃† 井手口哲夫† 村田嘉利††

†愛知県立大学 ††NTTドコモ東海

1．はじめに

現在、日常生活における安全性に関する問題が顕著になっており、日本ではホーム単位を対象とした様々なセキュリティ問題対策が施されている。本研究では、地域を対象としたコミュニティセキュリティシステムを提案する。セキュリティとして求められる機能は幾つか考えられるが、それらの実現及び拡張生の向上の為には共通プラットフォームを用意する必要性がある。そこで、共通プラットフォームとして MPB(Mobile Police Box)システムを提案する。システムを構築する上で、コミュニティの実現法とノード間の通信メカニズムの設計が重要となる。これらおいて要求されるアーキテクチャを提案し、比較、考察する。

2．コミュニティセキュリティの概要

本研究における提案の対象となるコミュニティセキュリティについて述べる。

(1) コミュニティの構成要素

コミュニティは公的所有物と私的所有物により構成されている。公的所有物は公園・公道・その他公的な建築物を指し、私的所有物は主に家や私有地を指す。それぞれに人・物・情報が存在している。

(2) セキュリティとして考えられる機能

前述したコミュニティにおけるセキュリティとしてどのような機能が挙げられるかを考える。

安全を侵す“脅威”の事象を、時系列的にとらえると、その事象が発生するまでの時間 T1、事象が発生してから検知するまでの時間 T2、それ以後の時間 T3 の 3 つに分けることができる。

T1 においては、いかにして事象が起こるのを防ぐか、または事象を起こりにくくするか、どうしても事象が起こってしまう場合、被害を最小限に食い止めるための対策を立てることが課題となる。T2 は、事象が発生後、いかに早く、正確に事象が発生したことを伝えるかが重要である。T3 は事象を分析することによって、なぜ事象が起こってしまったのか、どうすれば同じ事象の再発を防ぐことができるのかを考えることが重要となる。

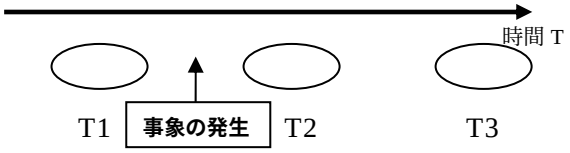

図１：時系列における脅威の事象

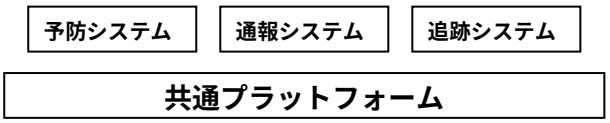

図２：実現方式のモデル

A Research on the common platform in community security
Toshiaki Watanabe†,Tetsuo Ideguchi†and Yoshitoshi Murata‡
†Aichi Prefectural University, ‡NTT DoCoMo Tokai

3．共通プラットフォーム

3．1 共通プラットフォームの提案

前章で述べたセキュリティ機能を実現するための共通プラットフォームを導入する。その上に各機能をアプリケーションとして実現させることにより、機能の追加や拡張が容易となる。実現方式を図 2 に示す。

3．2 MPB(Mobile Police Box)システム

3．1節で述べた共通プラットフォームを実現するにあたって、MPB(Mobile Police Box)システムを定義し、検討する。

(1) ＭＰＢシステムの構成要素

・コミュニティ(開空間ネットワーク)
・MPB(Mobile Police Box)：移動ノード
・VPS(Virtual Police Station)：固定ノード
・LR(Local Residence)：固定ノード
・MS (Monitoring Station):固定ノード

MPB はコミュニティ内の事象に対するセキュリティ対策を行う。VPS は複数のコミュニティの状態をまとめて管理するノードである。LR は事象の通報者で、コミュニティ内に存在する。MS は監視を行いながら事象に関する映像を通報として送信するノードで、コミュニティ内に設置する。

(2) MPB システムの定義

・MPB は各コミュニティにつき１つ設置
・複数のコミュニティを管理するステーションを設置
・セキュリティ機能を実現させるための共通プラットフォームを持つ

(a) 予防機能：コミュニティ内での MOB の移動による巡視
(b) 通知機能：VPS や LR、MS、及び隣接コミュニティの MPB との通信
(c) 追跡機能：事象発生場所への移動、事象移動の際の追跡

(3) システムを実現するにあたっての課題

ＭＰＢシステムを実現させるために重要な点として1つ目に実開空間をどのように表現させるかということである。今回、その方式の 1 つとして仮想閉空間とのマッピングを検討する(図３参照)。もう 1 つの課題として、システムの構成要素として必要となるノード間の通信プロトコルが挙げられる。

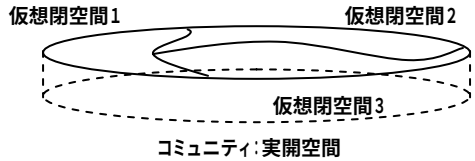

図３：仮想閉空間と実閉空間のマッピング

4．通信プロトコル

4．1 ネットワーク層

LR からの MPB に対する通報において、迅速に処理が進むよう、LR は予め MPB のアドレスを認識しておく必要がある。このため、MPB にはアドレスの一意性求められる。つまり、MPB がどこに移

動しても同じノードとして認識できる、移動透過性が必要であるといえる。移動ノードを扱う通信プロトコルを紹介し、MPB システムに適切なプロトコルを検討する。

４．１．１　関連研究

(1)Mobile IP／Mobile IPv6[2][3]

Mobile IP は移動ノード(MN)に対しての通信を行う際、MN の本来属するネットワークにあるホームエージェント(HA)にまず送信する。HA は現在 MN が存在するネットワークにあるフォーリンエージェント(FA)にカプセル化して転送し、FA はカプセル化を解き MN に転送する。Mobile IPv6 では移動ノード自身でアドレスを構築できるため FA の概念がなく、一度通信したらそれ以降は直接通信が行える。

(2)DDNS(Dynamic Domain Name System)[4]

CN は MN のホストネームを DNS サーバーに問い合わせ、MN の IP アドレスを取得し、通信を開始する。DDNS は動的に DNS をノードの名前に対応する IP アドレスに動的に更新する。これより、ノードは常に同じ名前で通信することができる。

(3)MAT[5]

MN は 2 つのアドレスを持つ。ホームアドレス（MN のノード識別子として使われるグローバル IP アドレス）とモバイルアドレス（移動ノードの位置指示子として使われる IP アドレス）という。MAT では、この 2 つのアドレスをマッピングする IMS（IP Address Mapping Server）を導入する。

ノードは IMT(IP Address Mapping Table)を保持している。通信する際、CN は MN のホームアドレスを用いてマッピング情報を IMS から取得し、IMT に登録し、通信を開始する。MN が移動した場合、位置指示子のモバイルアドレスを IMS に通知する。CN は IMS からの情報により IMT を書き換える。

４．１．２　検討

提案する MPB システムにおいては移動時間が極めて少ない場合は稀と考えられるため、移動時間を無視することができない。DDNS は DNS サーバーからの応答を一定時間キャッシュする機能があるので、頻繁な移動には対応しきれない場合がある。
MAT は実際の移動時間を考えない場合、理論的にはノードが移動してもコネクションの継続が可能である。しかし、IMS の参照に時間を要する。Mobile IP は経路冗長問題や障害問題、送信元アドレスが HA となる問題(IPv6 は障害問題以外は解決)があるが、移動透過性は保証されている移動時間の観点からも、まず Mobile IP を使用することを検討する。

４．２　トランスポート層

TCP と UDP があるが、MPB システムの通信は通報によるものと構成要素の操作に使われるものから成るので、処理を迅速に進めるために UDP を選択する。なお、UDP では受信確認などの信頼性が欠けるが次節に示すプロトコルをアプリケーション層に置くことで解決する。

４．３　アプリケーション層でのプロトコルの検討

先述したプロトコルを用いた上で、各構成要素のやり取りを定める必要がある。具体的には MPB の状態切り替えや通報の処理の手順の仕組みを定める。また、UDP では行うことの出来ない受信確認機能も付加する。これを MPB プロトコルとして定義する。MPB システムにおける構成要素の通信は MPB 同士、LR と MPB、MS と MPB、LR と PS、MS と PS、そして PS と MPB の計 6 種類がある。この種類別にやり取りを決める際、検討するべき課題があり、これらを解決するプロトコルが求められる。以下に種類毎の課題と解決案を述べる。

(1)MPB 同士(事象が他のコミュニティに移動した場合に行う)

[a]相手先の MPB のアドレスを知る方法

・PS に問い合わせる

・通報相手のコミュニティは隣接コミュニティに限定されるので MPB 自身に記憶させる場所を設ける

[b] 隣接コミュニティのうち逃走先のコミュニティの特定方法

・位置情報システムの導入

・MS を閉空間の境界に設置し、その通報から特定する

[c] 通報者に処理終了を知らせる方法

・事象移動先の MPB に通報者のアドレスを渡しておく

・通報者のいるコミュニティの MPB 経由で知らせる

(2) LR と MPB、MS と MPB

[a] 通報者の位置の特定方法

・位置情報サービスを利用

・その他、特定できる機構を利用

[b] 通報が多いときの抑制方法

・MPB に処理可能タスク数を設け、それを超す場合は非受理通知

・タスク数を設けるが、通知だけは受理してキューにいれる

・タスク数を設けず FIFO で処理する

(3) LR と PS、MS と PS

[a]PS に来た通報のＭＰＢへの通知方法

・PS に MPB の HA リストを用意し、それを参照する

・その他

[b] LR への受理・処理確認方法

・PS から行う

・MPB に行わせる

(4)その他

[a]通報者の IP アドレスから該当ネットワークを割り出し方法

・ネットワーク識別番号を別途用意し、付加して通報させる

・IP アドレスだけでネットワークが識別されるように割り振る

５．まとめと今後の課題

コミュニティセキュリティの重要性を述べ、実現に向けアプリケーションの下に共通プラットフォームとして MPB システムを提案し、システムで使用するプロトコルについて述べた。今後は MPB プロトコル作成における種々の問題点を検討し、提案プロトコルをシミュレーションにより評価を行う。

参考文献

[1] 平手正博,井手口哲夫:コミュニティセキュリティとそのシステム構成の一考察,情報処理学会,FIT2003

[2] Perkins,C.: IP Mobility Support, IETF (1996). RFC 2002

[3] Hohnson, D.B. and Perkins, C.: Mobility Support in IPv6 IETF(2001)Draft-ietf-mobileip-ipv6-14.txt,Internet-draft (Work in progress)

[4]楯岡孝道：DNS による IP 移動透過性の実現,情報処理学会誌,Vol.44,No.06,PP.656-657(2003)

[5]相原玲二他,アドレス変換方式による移動透過インターネットアーキテクチャ,情報処理学会論文誌,Vol.43,No.12,PP3889-3897(2002)