分散システム／インターネット運用技術 20－8
（2000. 12. 1）

ネットワークAPIの再考と機能拡張

緒方 健一† 長田 智和† 谷口 祐治‡ 玉城 史朗†

†琉球大学理工学研究科 ‡琉球大学総合情報処理センター

概要

近年のインターネットの普及，パーソナルコンピュータの高性能化や携帯端末の普及により，様々な通信端末がネットワークを介して接続されるようになった．ネットワークの利用形態も多様化し，現在，ネットワークは社会システムの一つとなっている．

しかし，それに伴って不正アクセスの件数も増加している．現在では個人での常時接続も可能になるなど，ネットワークが身近なものになっており，セキュリティ対策の必要性が増している．様々なセキュリティ技術が導入されているが，外部ネットワークに対する技術が多く，ネットワーク内部からの不正アクセスに弱いといえる．

本研究では，この問題に対応するため，ネットワークAPIの機能拡張を行う．また，不正アクセスを受けた教訓を踏まえ，LAN環境におけるセキュリティについて提案および実装を行う．

Reconsideration and functionality expansion of Network API

Kenichi OGATA† Tomokazu NAGATA† Yuji TANIGUCHI‡ Shiro TAMAKI†

†Graduate School of Science and Engeneering, University of the Ryukyus
‡Center for Integrated information processing, University of the Ryukyus

Abstract

Various communications terminal were connected through network by the spread of Internet of late years, high performance of personal computer and the spread of mobile terminal. Configuration of network diversified and became one of social system. However, the number of unjust access increased. An individual continuous connection is possible currently. Necessity of security mechanism is increased.

Various security technology were developed, but the most are things for attack from outside network, and there are weak in unjust access from the network inside.

Corresponding to this problem, in this study we suggest improvement of network API. In addition, we suggest about security in LAN environment and implement.

1 はじめに

インターネットの普及により，多種多様な通信端末がネットワークを介して接続されるようになった．WWW，FTP など自組織内外からのアクセスを許可するサービスも行われており，広域に世界中の端末からアクセス可能な状況である．WWW や電子メールなど，様々なインターネットアプリケーションサーバ群がネットワークに接続されることで，コンピュータの利便性は向上し，幅広い分野や用途で利用されるようになった．しかし，ネットワークを介してのアクセスにより，第三者からの不正なアクセスを受ける可能性も高まっている．現実に，近年ネットワークを利用した不正アクセス件数が増加している．[1]

一般に，外部ネットワークからの不正アクセスに対する対応は組織単位で行われ，それぞれの AUP が異なることで，組織全体のネットワークで導入するセキュリティ対策に差が生じるため，問題も多い．また，仮に侵入を受けたとしても気付かない場合もある．さらに，組織内のセキュリティホールにより，他のホストが不正アクセスを受ける可能性も高くなる．不正アクセスの手法も多種に及び，その全てに対応するのには相応の負担が必要となる．

そこで本研究では，ネットワーク API の機能拡張という側面から，ネットワークを介した不正アクセスに対するセキュリティ強化に関して提案を行う．

2 不正アクセス

本稿では，不正アクセスの定義を「システムを利用する者が，その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと」とする．

2.1 不正アクセス技術

不正アクセスを行うための技術が数多く存在する．ここでは，そのうち典型的ないくつかの手法について述べる．

(1) ネットワークスキャン
ping コマンドを用いた応答確認や，traceroute コマンドによる経路確認，ポートスキャンなどがある．ポートスキャンにより，ホストで稼動しているサービスを知ることが可能である．これはホストへの侵入の足がかりとなる技術であり，未然に防ぐことが望ましいが技術的に困難とされている．

(2) パケットスニファリング
ネットワーク内を流れるデータを取り出す手法であり，データの内容を知ることが可能である．tcpdump ではコンピュータの接続しているネットワーク内のパケットを取り出すことができるため，ネットワーク解析の手法としても用いられているが，これを不正に利用することで，認証情報の取得などが可能になる．実際に作成したプログラムでは，パケット内のデータからパスワードそのものを閲覧することが可能であった．

(3) データ改ざん
通信データの内容を不当に書き換える行為である．ネットワーク上の全ての回線は同一組織のものではなく，公衆回線を経由してデータ通信が行われている．経路上で中継を行うルータやゲートウェイ上でデータの改ざんが行われる危険性がある．

(4) 無権限利用
権限を与えられていないユーザが，権限を奪取し，プログラムの実行やファイル操作を行うことをいう．組織内部にアクセス権を持つ正規ユーザへのなりすましなどは，不正アクセスとの区別が困難である．

2.2 不正アクセスの例

今年夏，情報工学科内の Linux/WindowsNT ホストが，不正アクセスの被害を受けた．この時の攻撃の対象となったのは Linux システムで，異常終了後の調査の結果次のことが行われていたことが分かった．

(1) 各種設定ファイルの変更
(2) ログの消去
(3) ユーザ作成
(4) コマンドの置換
(5) 他組織への不正アクセス

[1] http://www.jpcert.or.jp/

この不正アクセスは，その時期などから，gpm もしくは Canna のセキュリティホールを狙って行われたものと推測される．また，これらの不正アクセスの内容は，ヒストリの一部が残されていたことにより判明したものがほとんどである．

これにより，ルータの処理能力を超えるトラヒックが約 40 時間近く流され，ネットワーク上の他のホストが通信不能に陥るなど，著しい通信遅延を招いた．(実際には，ルータよりも上位の経路に対しては，データが流れなかったため，学科ネットワークだけの被害で済んでいる.)

この時，tcpdump によるトラヒックの状況把握も行ったが，学内に対して異常なトラヒックを送信しているホストを割り出すまでにはいたらなかった．これは tcpdump によって捕獲できるパケットに限界があるためである．全てのネットワークコンセントで tcpdump を利用すれば解決できるが，アプリケーションの実装状況などから判断しても不可能であった．

このように被害が発生するまで，不正アクセスを受けても気付かない場合がある．ネットワークを介した不正アクセスに対して，どのような対策を施せば検知できるか，また，攻撃を未然に防ぐためにはどうしたらよいか，というのがこの攻撃での教訓である．

しかし，この例のように，不正アクセスには一連の行為があると考えられる．システムのセキュリティホールに対して攻撃を行い，ユーザ権限や root 権限を奪取しファイルの置換を行い，さらに他の組織への中継に使うことがそれにあたる．これから分かることは，ファイルの置換に関しては，タイムスタンプを比較しながら状況変化を監視するシステムの必要性，攻撃の対象となるホスト自身にセキュリティ上の実装を施すことがより良い，ということである．また，これまでのような，設定ファイルを元にして，アクセス制限を行う手法から，TCP/IP の通信自体に特化した動的セキュリティ対策の必要性がある．

ネットワークやシステム規模の拡大に伴い，運用上や設定上のミスが起きることは十分考えられることから，ホスト自身のセキュリティ対策はより重要になる．

3 実験ネットワーク

本研究では，実験ネットワークとして，琉球大学総合情報処理センター内にある実験ネットワーク"OSN"[2]および，同ネットワークのサブネットワークを用いた．また，サブネットワークにある 2 台のホストを中心として実装を行った．
予備実験として，一般的なセキュリティ技術により強化したネットワークを構築し，本実験に際して，新たにセキュリティ実装用のネットワークを構築した．

3.1 予備実験

実際にネットワーク内部から，不正アクセス技術を使った模擬攻撃を行い，内部からのネットワーク経由による不正アクセスについて検証を行ったほか，セキュリティに関する実装を行い，ホスト自身のセキュリティ強化を図った．

また，先行的に構築していた，既存のセキュリティ技術により構築されたネットワークと比較することで，問題点をより明確にすることができた．

先行的に構築したネットワークでは，一般的な不正アクセスへの対策として、図 1 に示す対策を施している．

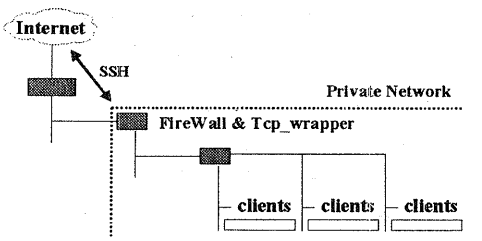

図 1: ネットワーク構築例

(1) ファイアウォール

主にインターネットと自組織ネットワークとの接点において用いられるセキュリティ機能．特定ポートや特定データのみの通信を許可し，他のデータについては拒否するといったアクセス制御を行う．これにより，外部からの侵入対策を行っている．このネットワークでは対

[2]Open Space Network

外的にWWWの公開も行っているため，SSH以外のアクセスについては，ポートフォワーディングにより解決を図っている．一般に，組織ごとに異なるセキュリティポリシが存在するため，全ての組織にファイアウォールが導入されているわけではなく，この差によって，セキュリティ対策にも違いが生じる．

(2) SSH

Secure Shell．ネットワーク経由でリモート端末に接続し，コマンドの実行を行ったり，端末間でファイルを移動する場合などに用いられる．独自の認証システムと暗号通信をサポートするため，より安全なネットワーク通信が可能となる．このネットワークでは，外部からのアクセスは，SSHのみ許可している．

(3) tcp_wrapper

アクセス制御機構の一つである．既存のネットワークサービスに変更を加えることなくセキュリティを強化することが可能である．tcp_wrapperは，あらかじめ決められたアクセス制御リストにより，接続拒否するホストと接続許可するホストを判断する．このため，ネットワークのセキュリティポリシに応じてサービスの是非を決める必要がある．このネットワークでは，SSH以外の全てのサービスについてtcp_wrapperにより制限している．

(4) ルータによるアクセス制限

データの通過するルータ上でアクセス制御を行う．ルータによってパケットのフィルタリングを行うことにより，パケットを選択して配送することが可能となる．セキュリティを強化する場合，相応の設定が必要になる．

3.2 実験結果

実際に，組織内のホストにてセキュリティに関する攻撃を行ったところ（図2），次のような結果を得られた．

(1) ポートスキャン

可能な範囲においてポートスキャンプログラムを実行したところ，図3のようにサービス名とポートの一覧を得られた．

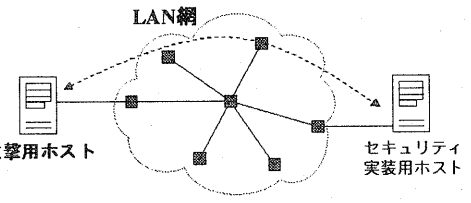

図2: 実験ネットワーク

```
ftp     service (port 21) is available.
ssh     service (port 22) is available.
telnet  service (port 23) is available.
smtp    service (port 25) is available.
```

図3: ポートスキャン実行結果

(2) ネットワークモニタプログラムによるパスワード取得

パケット捕獲ライブラリを用いて作成したプログラムを実行すると，図4のように組織内のユーザのパスワードを取得することが可能である．

```
TCP 133.13.49.xxx ( 2165) > 133.13.48.xxx ( 110): USER *******
TCP 133.13.49.xxx ( 2165) > 133.13.48.xxx ( 110): PASS *******
TCP 133.13.49.xxx ( 2165) > 133.13.48.xxx ( 110): STAT
TCP 133.13.49.xxx ( 2165) > 133.13.48.xxx ( 110): LIST
```

図4: ネットワークモニタ実行結果

(3) Sendmail システムへの DoS 攻撃

sendmailシステムに対するDoS攻撃を行った．用いたプログラムは，sendmailのヘッダー解析コードのバグを利用するものであったが，システムはほとんど影響を受けなかった．

(4) Nmap を用いたリモート OS 識別

OSの識別は，セキュリティに対する攻撃方法を決定する上で重要になる．Nmapとは，様々なネットワークスキャナ機能を取り込んだ包括的なポートスキャナである．Nmapでは，TCP/IPスタックフィンガープリンティングの手法を用いてリモートOSの識別が可能となる．

TCP/IPスタックフィンガープリンティングとは，RFCの解釈の違いに着目してOSを識

別する手法のことである．例えば，サービスを公開しているポートに対しFINパケットを送信した場合，OSによってはRSTパケットを送り返すように設定されているものがあり，これらの手法を組み合わせることでOSの識別が可能となる．実際に次のような結果が得られた．

```
-Linux-
TCP Sequence Prediction: Class=random positive increments
                Difficulty=194891 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.2.14

-Windows2000-
TCP Sequence Prediction: Class=random positive increments
                Difficulty=8508 (Worthy challenge)
Remote operating system guess: Windows 2000 RC1 through final release
```

図 5: リモートからのOS識別

3.3 考察

これらのセキュリティ機構を複合的に管理，利用することでネットワークの強化を図っている．しかし，これらの対策は基本的に外部ネットワークからの不正アクセスに関するものがほとんどである．外部からのアクセス制限を行う意味では非常に有効であるが，ネットワークやシステム規模の拡大に伴い，運用上や設定上のミスが起きることも十分考えられる．また，セキュリティ技術によって強固なシステムを構築しても，内部にアクセス権限をもつユーザからの攻撃に対しては防ぐことは不可能であり，内部に対するセキュリティ対策としては十分でない．

4 提案手法

このようなセキュリティ攻撃と実際に行った先行実験から，問題点などがより明確になってきた．アプリケーションについては，こまめにバージョンアップを行うことで，既存の攻撃手法に対しての影響を少なくことができる．しかし，ポートスキャンやパケット捕獲によるデータの閲覧では，アプリケーションの動かせる範囲にあれば，どこでも実行可能である．そこで本研究では，ネットワーク経由での攻撃に対して，ホスト自身のセキュリティ強化という側面からセキュリティ対策について提案を行う．

(1) ポートスキャン対策

ポートスキャン対策として必要なものは，ポートスキャンの検知とその処理方法である．その場合，サービスを利用するための正規の接続とポートスキャンとの区別をどのように行うかが重要である．正規の手続きを踏んで行われる接続であるから防ぐことはできないという考えが一部にはあるが，ポートスキャンのように攻撃の仕方が定型化しているものであれば対策も可能である．基本的にポートスキャンを防ぐにはサービスの停止をしてポートを塞ぐしかないが，それでは正規のサービスにも影響を与えてしまう．

ポートスキャンにもいくつかの種類があるが，ここでは一般的なTCPスキャンについて考えることとする．一般的なTCPによる接続の確立は次のような処理を経ている．ここで

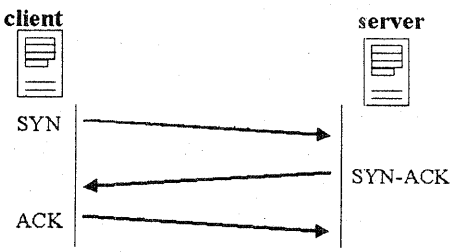

図 6: TCP接続の確立する課程

はTCPの3ウェイハンドシェイクに着目し，セキュリティ実装を行う．TCPのコネクション確立までに，ポートスキャンに対してトラップをしかけ，仮に，ポートスキャンを受けた場合，初期段階で停止できれば，サービスの有無を知られずに済む．

(2) パケット捕獲対策

tcpdumpのようなネットワークモニタによるパケットの捕獲・解析は内部ネットワークからの攻撃では脅威となる．特定のユーザ，パスワードの捕獲も可能である．今回作成したプログラムやtcpdumpといったアプリケーションは，実行に際してroot権限を要求されるこ

とから，このroot権限でのプログラム実行については，少なくとも2台以上のホスト同士の相互認証によるプログラム実行を行う方法が提案できる．

(3) その他の対策
その他の対策として，アプリケーションおよびサーバプログラムの自動アップデートシステムなどが考えられる．今回用いているネットワークでは，基幹サーバにLinuxシステムを搭載していることから，管理ホストを中心としてLAN内のアプリケーションの自動更新ができれば有効な手法になる．特に大規模分散システムの場合，アプリケーションのバージョンに関するデータベースとの整合性を元にホスト間での情報共有を行い，アップデートを行うことができれば，セキュリティ対策にもなる．

5 今後の課題

今回の提案手法では，ホストそのものへのセキュリティ対策として，TCPの接続方法に着目し提案を行った．ポートスキャン対策としては，コネクションの確立が行われるTCPスキャンにおいて実装を行ったが，ポートスキャンにも，TCP SYNスキャンやステルススキャン，UDPスキャンなどがあり，単純なTCP/IPのコネクションによる検知や対応だけでは万全でないこともわかっている．そのため，今回行った実装についても，それらに対応するシステムへと拡張していく必要がある． 組織内のネットワークからのroot権限によるプログラム実行においては，組織内ネットワークに存在するホスト同士による相互認証機能の導入という点から拡張を図る．

6 まとめ

本研究では，ポートスキャンやネットワークモニタ用のプログラムを作成し，組織内からの攻撃に対しての検証を行った．実際に，ネットワークモニタプログラムでは，パスワードの取得も可能で，組織内でのデータ通信に対してのセキュリティ上の問題点を知ることができた． セキュリティ対策は，外部ネットワークに対して行われることが多いが，内部からの攻撃に対して弱いといえることも確認できた．ネットワーク全体で強固なセキュリティ対策を行うためには，全体構成でのセキュリティのバランスに着目する必要があるが，大規模かつ管理方法の異なるネットワークでは，管理面から困難になる可能性が高い．

外部ネットワークからの攻撃に対してのセキュリティ対策にに今回提案する手法を組み合わせることで，総合的なセキュリティの向上が可能になる．

大規模ネットワークにおけるセキュリティ管理も今後重要になってくることから，ネットワーク管理技術との組み合わせについても視野に入れ，拡張していく．

参考文献

[1] 原田慎介，浅香緑：痕跡を用いた侵入検出手法への正規手続きデータベースを利用した侵入判定の適用，情報処理学会論文誌，Vol41，No.8，pp.2208-2215(2000).

[2] 高田哲司，小池英樹：ログ情報視覚化システムを用いた集団監視による不正侵入対策手法の提案，情報処理学会論文誌，Vol41，No.8，pp.2216-2227(2000).

[3] JPCERT/CC(コンピュータ緊急対応センター)：http://www.jpcert.or.jp/

[4] IPA (情報処理振興事業協会)：http://www.ipa.go.jp/

[5] 武田圭史，磯崎宏：ネットワーク侵入検知，ソフトバンク パブリッシング株式会社，2000.

[6] 寺田真敏，萱島信：基礎からわかるTCP/IPセキュリティ実験，株式会社 オーム社，2000.

[7] 澤川渡，綱島明浩：TCP/IP解析とソケットプログラミング，株式会社 オーム社，2000.