第1章 序論

企業が、情報技術の利便を享受するためには、ウイルスによる情報流出等の脅威から防御する手段を講じる必要がある。
企業では、企業内ネットワークとインターネットとの境界点にファイアウォール等の機器を設置し、内部のネットワークを外部ネットワークから隔離することで、情報セキュリティ上のリスクを軽減させる対策を行ってきた。
しかし、内部ネットワークに不正な PC を接続されると、情報セキュリティ上の重大な脅威となるが、対策は未だ一般的ではない。
当研究は、不正な機器が内部ネットワークに接続された場合に、検知することのできる装置を一般的なものとするため、ＰＩＣＮＩＣを用いて低価格に作成し、機能の評価を行った。

第2章 背景

第1節 情報セキュリティの確保

電子メールや発注システムの普及により、インターネットへの常時接続が不可欠になっている。同時にファイル共有ソフトの利用やOSを始めとする各種ソフトウェアの脆弱性等により、ウイルスや情報流出の被害が増えている。
情報流出を発生させると信用の失墜による損失は相当額に達するため、情報セキュリティの確保は重要となっている。
インターネットとの境界点からの情報流出やウイルス等の攻撃に対しては、ファイアウォール等の設置やウイルス対策ソフトウェアの導入により対策がされていることが一般的である。

第2節 内部統制の整備

企業の内部においては、個人の操作誤りや不正行為によって重大な損失を発生させることがないようにチェックする体制が整備されてきている。
チェックする体制は、財務や業務に関する事項に対するものから発展し、情報の管理及び情報技術の利用に関して、チェックする体制が整備されつつある。
内部ネットワークに機器を接続するには、規則等を定め、目視によりチェックしていることが多いが、不正なPCが接続された際に、システム的にチェックする製品も利用されている。

第3節 関連研究及び製品

内部ネットワークへの機器に対する情報セキュリティついては、次の研究がある。

第1項 関連研究

大林猛「小型・簡易なネットワーク侵入・攻撃検知システムの作成と考察」2005年信州大学大学院工学研究科修士論文

第2項 製品

日本電気株式会社「WebSAM SecureVisor」
米国 CISCO「NAC」
米国 Juniper Networks, Inc.「IDP」

第4節 導入の障害

情報セキュリティの確保への投資は、生産性向上に関連しないため、情報セキュリティ上のリスクへの対応として、リスク保有と判断されることが多い。
インターネットとの境界点における対策と比べ、内部ネットワークの保護については、目視での確認によっても補完できると考えられることが多く、高価格のシステムは導入されにくいと見られる。

第3章 目的

第1節 費用の最小化

導入を用意にするため、機器の購入費用は最小となるようにし、入手方法も容易にする必要がある。
ライセンス費用を最小にする必要がある。特に端末の台数により契約する費用については導入の障害となる。

第2節 省電力化

専用の機器を常時稼動させるためには、機器の消費電力は最小とする必要がある。
また、設定値を保存するためにバックアップ装置や無停電電源装置を要すると合計消費電力が多くなる。

第3節 導入の容易性

ネットワークに流れる不正な通信をすべて捕捉するためには、スイッチング HUB を導入する際に、すべての通信を傍受できるミラーポートの設定が可能な製品を選定する必要がある。
当研究においては、導入を容易にするため、ARP プロトコルでのブロードキャスト通信に限定して検知を行うことで、ミラーポートの設定は不要であり、一般のスイッチング HUB で利用可能である。
検知の対象は、ブロードキャストドメインとする。

第4節 検知機能

検知機能は、接続された PC を検知する必要最小限のものとし、接続禁止機能、ウイルスソフト検知機能等は導入しない簡易型とする。

第4章 機能の検討

第1節 検知機能

第1項 基礎技術

物理的に離れた場所にある２つの端末がネットワークを経由して通信が行うためには、物理的な通信経路が必要であり、見ず知らずの端末同士が通信を行うためには、両者の間に約束事が必要である。
現在のネットワークにおいては、物理的な通信経路及び通信の約束事が存在している。
通信上の経路制御や再送処理を行うかどうかで、通信を階層的にとらえ、モデル化されている。
そのモデルの一つは、国際標準化機構（ISO）が提唱した OSI（OpenSystemInterconnection）参照モデルと呼ばれる。
端末上のサービスが通信する際、次の各層を経由して通信しているとするモデルである。
アプリケーション層
プレゼンテーション層
セッション層
トランスポート層
ネットワーク層
データリンク層
物理層
各層ごとに上位の層に提供するサービスのインターフェイスが定められており、プロトコルと呼ばれる。
モデルのもう一つは、TCP/IP 参照モデルと呼ばれ、次の各層を経由して通信しているとするモデルである。
アプリケーション層
トランスポート層
インターネット層
ホストツーネットワーク層（物理＋データリンク層）
TCP/IP 参照モデルには、プレゼンテーション層及びセッション層は存在しない。
ネットワーク層又はインターネット層から下位のデータリンク層に通信をゆだねる際に、ネットワーク層又はインターネット層で利用する IP アドレスを、ハードウェアアドレスに変換する必要がある。

第2項 ARP プロトコル

ARP プロトコルは、３２ビットの IP アドレスから４８ビットの MAC アドレスに変換するプロトコルであり、OSI 参照モデルではデータリンク層に位置し、RFC826 に規定されている。
ネットワークに接続した機器がゲートウェイ装置を含む他の機器と通信を行うためには、IP アドレスをハードウェアアドレスである MAC アドレスに変換する必要がある。
IP アドレスと MAC アドレスの変換は端末間のピア・ツー・ピア型で行い、主にブロードキャスト通信により解決する。
ARP プロトコルによりやりとりされるフレームの構造は次のとおりである。

Ethernet あて先アドレス	Ethernet 送信元アドレス	プロトコルタイプ	ハードウェアタイプ	上位プロトコルの Ether タイプ	ハードウェアアドレス長	プロトコルアドレス長

オペレーションコード	発信ハードウェアアドレス	発信プロトコルアドレス	目的ハードウェアアドレス	目的プロトコルアドレス

ARP 要求メッセージでは、変換したい IP アドレスを、「目的プロトコルアドレス」に入れ、「発信ハードウェアアドレス」に自分の MAC アドレスが入り、Ethernet プロトコルアドレスを FFFFFFFF とし、ブロードキャストする。

ARP 要求メッセージを受け取った端末は、「目的プロトコルアドレス」が自分の IP アドレスと合致した場合、「発信プロトコルアドレス」あてに ARP 返答メッセージを返信する。

ARP 返答メッセージを受け取った機器は、変換テーブルにキャッシュする。

キャッシュの有効期間は数分間のため、経過後に再度 ARP 要求メッセージを送信し、変換テーブルを更新する。

第3項 検知の流れ

ネットワークに接続した機器は次のとおり検知される。
① 機器がネットワークに接続される
② ①が他の機器への通信を開始する
③ ①ARP 要求メッセージをブロードキャスト
④ 当システムがブロードキャストパケットを把握
⑤ 検知

第2節 通知機能

第1項 リスト化

検知をした端末の MAC アドレスをリスト表示し、端末の使用を容認する場合は承認処理を行う。
承認された端末の MAC アドレスは EEPROM に保存され、次回検知された際に表示されないようにする。
リストを更新するためには、リストに掲載された MAC アドレスを一括し消去し再度承認処理をすることができる。

第2項 通知方法

検知した際は、LED の表示、LCD の表示、web 画面の表示を行う。動作モードが「警告モード」の場合は、合わせてブザーの鳴動を行う。

第3節 通信許可機能

未承認の機器に対しての通信妨害機能については、当研究では対象外とする。

第5章 実装

第1節 機器の選択

価格安価であること及び入手が容易なことから､有限会社トライステート社から発売されている「PICNIC　ver.2」を選択することとした。
イーサネットのネットワークカードを実装した I/O ユニットであり、Microchip 社の CPU16F877 を搭載している。

第2節 周辺機器の選択

次の機器を接続した。
①モード切替用及び承認用のスイッチ
②警告モードにおける検知時のブザー

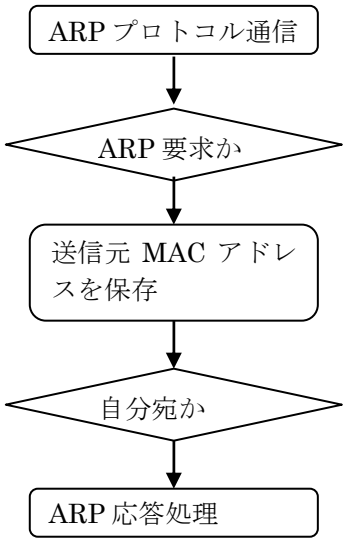
第3節 プログラム言語

ファームウェアで利用されているアセンブリ言語を利用し、機能を追加した。
開発の元にするファームウェアのバージョンは、SUGSI の IT 技術演習で利用する 1.2.0.4 とした。

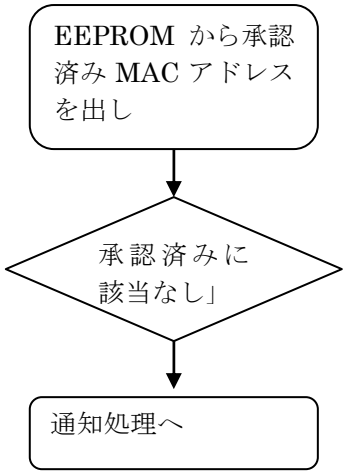
第4節 流れ図

第1項 検知機能

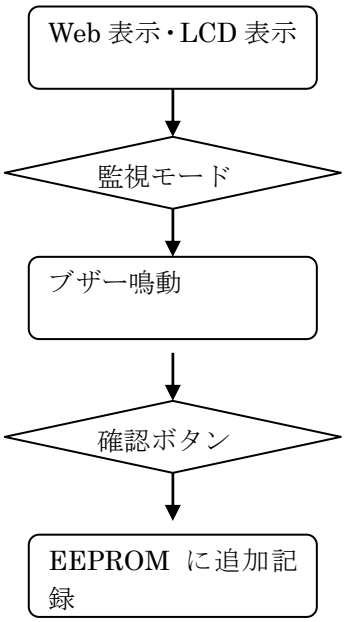
（1） パケット受信処理



（2） 検知処理



第2項 通知機能



第6章 評価

第1節 費用

PICNIC 本体は 7,300 円である。（2008 年 1 月現在）

第2節 機能

第1項 検知機能

Web 画面を表示しておく。
他の機器が接続され、ネットワーク上の他の機器に対して通信を発生させた。
Web 画面等に当該機器の MAC アドレスが表示された。

第2項 通知機能

EEPROM にエントリーがない MAC アドレスの場合、次のとおりの動作した。
Web 画面等に MAC アドレスが表示された後、確認ボタンにより、表示が消去。
再度接続すると、表示されなくなった。

第7章 考察

第1節 必要な機能

一般に不正な PC の接続を監視する機能に付随する機能については、次のとおりの機能がある。
(1) 未承認機器の通信遮断機能（arp poinsoning による方法）
(2) 未承認機器の通信遮断機能（認証スイッチによる方法）
(3) PC にインストールされた認証サプリカントによる認証機能
(4) 検知ログ記録機能
(5) 検知メール送信機能

当研究においては、簡易型のため、未承認機器への通信遮断機能は実装しなかったが、導入することにより、より厳密な監視と管理が可能である。
しかし、web 画面からの操作を行う PC を接続可能としなければならず、PICNIC の電源投入後 1 分間は接続可とするなどの対応が必要であろう。
検知し、通知をした際に管理者が不在であった場合、ログを残す必要があると思われるが、当研究においては、簡易型のため、実装していない。
ログの実装にあたっては、時間を記録するための NTP モジュールが必要になる。
発売されている製品においては、ウイルス対策ソフトの有無や、ソフトウェアの修正プログラム適用状況を検査し、ネットワークへの接続を制限するものがあるが、導入及び運用の難易度は高い。
当研究の目的は、低価格で導入が容易なシステムとすることであるため、実装していない。

第2節 費用と導入

情報セキュリティにとって、費用に対して短期的な収益に結びつく成果が想定できないため、投資に消極的にならざるをえない。
ウイルス対策ソフトウェアによる対策は、一般的になっている。
情報漏えい事件の発生時に、導入をしていなければ、不作為による職務不履行と見られるため、費用をかけることが問題とならない。
内部ネットワークへの攻撃を防ぐ対策については、未だ一般的でないため、導入に消極的となっている。
当研究では、PC 接続の検知を簡易的に実装した。
しかし、簡易型であっても安価な装置を導入することで、企業等においては、安易な PC の接続に対する牽制効果が期待でき、価格以上の効果が見込まれる。

謝辞

信州大学大学院工学研究科 Pauline Naomi Kawamoto 先生には、学習及び論文についてご指導いただいた。
その他 SUGSI の設立及び運営に関わっている先生方・事務局職員の方には、学習及び研究の貴重な機会をいただいた。
これらの方にお礼を申し上げる。

参考文献

アンドリュー・S・タネンバウム　著，　水野忠則　他訳,『コンピュータネットワーク第４版』,日経 BP 社，2003 年

笠野英松　監修，マルチメディア通信研究会　編集,『ポイント図解式インターネット RFC 事典』，株式会社アスキー，1998 年

トランジスタ技術編集部　編集,『LAN によるハードウェア制御』，CQ 出版社株式会社，2005 年

神崎康宏　著,『作りながら学ぶ PIC マイコン入門』，CQ 出版社株式会社，2005 年