1H-2

検疫ネットワークシステム対応サイジング手法の検討

安田　晃久†　　北上　眞二†　　加藤　太‡　　大森　敬介‡　　黛　潤一‡

三菱電機株式会社　情報技術総合研究所†

三菱電機情報ネットワーク株式会社　ネットワークサービス事業部‡

1. はじめに

近年，社内ネットワークがウィルスに脅かされる事例が多く，企業のセキュリティ問題が深刻化している．このような状況に対処すべく，個々の接続端末のセキュリティレベルを確保する事によってネットワーク全体をセキュアに保つ検疫ネットワークシステムが提唱されている．

各企業では社内ネットワークの規模や構成が様々であるため，検疫ネットワークシステム適用の際には企業毎にサイジング見積もりを実施し，最適なシステム構成を取る必要がある．しかし，そのような検疫ネットワークシステムに対応したサイジングは一般的でなく，また指針となる考え方も存在していない．

本稿では検疫ネットワークシステムに対応したサイジングについて検討し，得られた知見について報告する．

2. 検疫ネットワークシステム

検疫ネットワークシステムでは，一般的にはネットワーク全体を社内ネットワーク（ファイルサーバ等）と検疫ネットワークに切り分け，どちらのネットワークに接続すべきかを判定する機能を持った，認証・検疫のためのポリシーサーバ，及び隔離デバイスを持つ（図 1 参照）．

ポリシーサーバは任意のセキュリティポリシーを持ち，社内ネットワークへの接続を許可する端末の条件が事前に設定されている．当該ポリシーによって，社内ネットワークへは一定の条件を満たしたセキュアな端末のみ接続可能となる．また，ポリシーサーバは定期的に接続端末をチェックし，不適応の場合は隔離デバイスを利用して接続先を検疫ネットワークへと変更する．こうしたセキュリティポリシーに則った

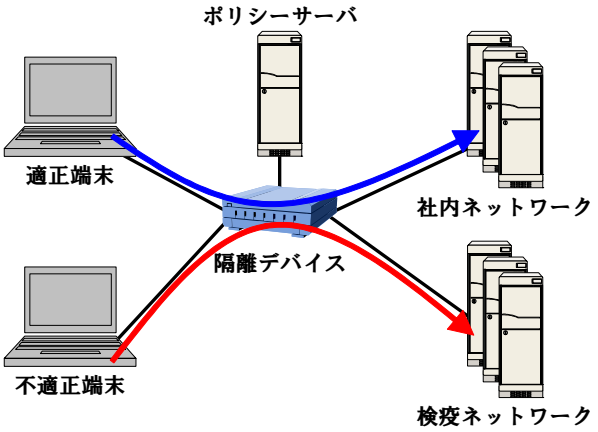

図 1　検疫ネットワークシステム構成図

接続端末選別方式により，検疫ネットワークシステムは企業内ネットワークのセキュリティを確保する事が出来る．

上記検疫ネットワークシステムにおいては，負荷の掛かる点はネットワーク内のトラヒック量よりも認証・検疫における処理性能であると考えられ[1]，ポリシーサーバの処理性能を適切に見積もるためのサイジングが必要となる．

ポリシーサーバのサイジングには検疫ネットワークシステム特有の挙動をモデリングする必要があるが，システムに対する端末アクセスパターンは無数にあるため特定は困難である．従って，正規分布に分散したアクセス数に対するポリシーサーバへの負荷を見積もり，実データ採取による結果と比較してその検証を行う事とした．

3. サイジング手法の検討

3.1. モデル設定と検証方法

対象モデルの企業規模を 1000 人とし，出社した社員の端末起動と同時に検疫ネットワークシステムが社内ネットワークに接続するのを認証し，更に定期的に（本モデルでは 15 分毎と仮定）接続端末の状態を検証して認証処理するモデルを設定した．

従って，ポリシーサーバには以下のトランザ

APPROACH OF HOW TO SIZING THE NETWORK ACCESS CONTROL SYSTEM

†Akihisa Yasuda，Shinji Kitagami
Mitsubishi Electric Corporation
‡Futoshi Kato，Keisuke Ohmori，Junichi Mayuzumi
Mitsubishi Electric Information Network Corporation

クション負荷が発生すると考えられる．

① 初期認証

② 再認証

また，上記①と②を重ね合わせた処理を

③ 全体認証

と定義する．

初期認証のタイミングは社員が出社する状況に依存し，当該状況については企業毎に多様である．また，全体認証数は初期認証のタイミングと再認証の間隔に依存する．そこで，まずは正規分布のような一般的な確率分布から初期認証数の論理モデルを構築した．

3.2. 論理モデルのサイジング

まず，出社時刻によって端末の初期認証数が正規分布の偏りに沿って推移する場合を考える．ここで，確率変数を分刻みの出社時間とし，その割合が 30 分程度の間に収まっている状況を仮定して分散を設定した．

左記初期認証モデルに対し，再認証の間隔を 15 分と仮定した場合の全体認証数の変移を図 2 に示す．

図 2 より認証数の最大値は 150 と判明したが，認証数の確率分布については分単位での分散値を取っているため，更に秒単位での認証数を見積もる必要がある．そこで，1 分当たりの確率分布が更に正規分布に従うと仮定した結果，平均を m，分散を σ^2 とすると 1 秒間の最大確率変数 $P(X)$は

$$P(X)=\int_{29.5}^{30.5}\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{(x-m)^2}{2\sigma^2}\right)dx\cong 0.045$$

となる．従って，全体認証数の最大値は

$$150\cdot 0.045=6.75$$

となる．

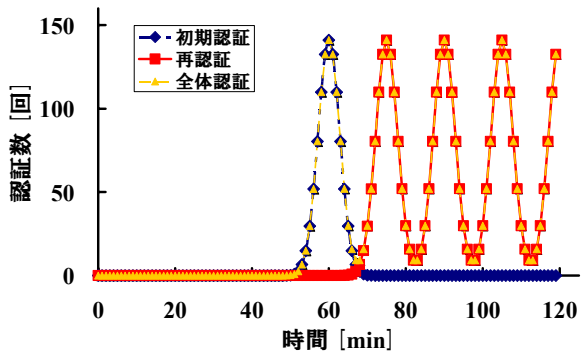

図 2　論理モデルの認証数の推移

3.3. 実データによるサイジング

1000 人規模の企業 2 つをサンプルデータとして抽出し，各企業の社員出社時刻（分単位のデータ）を基に初期認証数を見積もった．また，再認証間隔を 5～60 の範囲で変更した場合の全体認証数の最大値の変移を調べた結果，15 分の再認証間隔では 3.4～5.2 となり，**3.2**で得られたサイジング値と大きな相違が無い事を確認した（図 3）．ここでも**3.2**と同様に 1 分間の認証数の確率分布が正規分布に従うと仮定した．

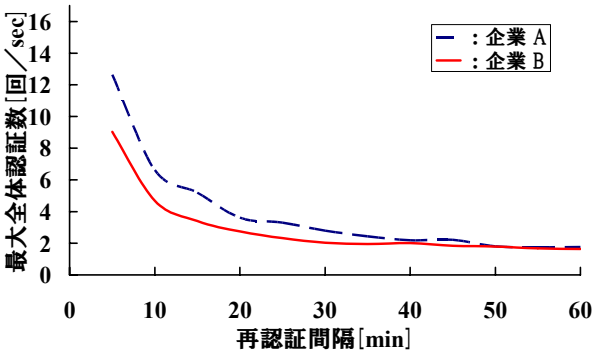

図 3　全体認証数の 1 秒当たりの最大値

また図 3 の 2 つのサンプル結果の相関を調べるため X を企業 A の全体認証数，Y を企業 B の全体認証数としてピアソンの相関係数 r を求めると，

$$r=\frac{\frac{1}{n-1}\sum_{i=1}^{n}(X_i-\bar{X})(Y_i-\bar{Y})}{\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(X_i-\bar{X})^2}\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(Y_i-\bar{Y})^2}}=0.995$$

となり，両者の間には極めて強い相関がある事を確認した．よって，2 つのサンプルから得られた結果には大きな隔たりが無いと言える．

4. 結論

- 正規分布に則した確率モデルから検疫ネットワークシステムに対応したサイジング値を導出する手法を示した．
- 論理モデルとサンプルデータを比較した結果，サイジング値に大きな相違が無い事を確認した．但しサンプル数が少ないため，更なる検討調査が必要である．

参考文献

[i] Andrew Ward, How to Size A Server, PC Network Advisor. 116, 3-6（2000）.