# インターネットには何台の不正ホストがいるのか？

菊池　浩明† 田中 貴之† 福野 直弥† 杉山 太一‡ 菊地 大輔‡
寺田 真敏†† 土居 範久¶

† 東海大学電子情報学部情報メディア学科
259-1292 平塚市北金目 1117
kikn@tokai.ac.jp

‡ 中央大学理工学部情報工学科
112-8551 東京都文京区春日 1-13-27

¶中央大学研究開発機構
112-8551 東京都文京区春日 1-13-27

†† 日立製作所 Hitachi Incident Response Team (HIRT)
212-8567 神奈川県川崎市幸区鹿島田 890　日立システムプラザ新川崎

**あらまし**　複数の観測点からの不正アクセスデータを基にして，インターネット全体で何台の不正ホストが存在するのか推定を試みる．不正ホスト数は，観測期間の長さと観測点数の二つの変数の関数としてモデル化する．

# How Many Scanners in the Internet?

Hiroaki Kikuchi† Takayuki Tanaka† Naoya Fukuno† Taichi Sugiyama‡
Daisuke Kikuchi‡ Masato Terada†† Norihisa Doi¶

†Dept. of Info. Media Technology, School of Info. Technology and Electronics, Tokai University
1117 Kitakaname, Hiratsuka, Kanagawa 259-1292

‡Dept. of Info. and System Engineering, Faculty of Scienece and Engineering, Chuo University
1-13-27 Kasuga, Bunkyo, Tokyo 112-8551

¶Research and Developement Initiative, Chuo University

**Abstract** Given independent multiple access-logs, we try to identify how many malicious hosts in the Internet. Our model of number of malicious hosts is a formalized as a function taking two inputs, a period of sensing and a number of sensors.

## 1　はじめに

インターネットには何台の不正なホストがいるのだろうか？

彼らは定常的にポートスキャンを実行して，脆弱性のあるホストを探しては攻撃を繰り返す．[2] によると，ワームの代表例である Sasser は，52%の割合で攻撃対象のアドレスを完全にランダムに，25%で上位 2 オクテット以外をランダムに，23%で 1 オクテット以外をランダムに生成しては，TCP コネクションの確立を試みるという．この振る舞いを実行する不正なホストはどのぐらいの割合で存在しているのだろうか．もしも，その値がわかれば，ネットワーク管理者にとってはセキュリティ対策のコスト評価を行うことが可能となり，無駄のない効率的な安全対策が期待される．

この問題を解く鍵は，ネットワーク中に独立に設置された定点センサの情報である．現在，

多くの組織でポートスキャンやハニーポットなどの観測 [1] が行われているが，それらを統合することで，単体のセンサではわからなかった情報が得られる．本論文は，攻撃アルゴリズムを単純化するいくつかの仮定を行い，スキャナで観測できるスキャンの数に対する理論式を導く．実際に行った観測データを下に，インターネットに潜在するスキャナの総数を明らかにする．

## 2 潜在スキャナ数の同定問題

### 2.1 モデル

スキャナとは，ウィルスやネットワークワームなどにより他のホストへの攻撃（ポートスキャン）を仕掛ける不正ホストである．センサとは，スキャナからの攻撃を観測する正規ホストであり，決して感染しないものとする．スキャナもセンサも静的なグローバルアドレスを割り当てられており，常時インターネットへのアクセスを行なう．また，有効な全グローバルアドレスの数を $n_0$，不正スキャナの数を $n$ とする．$x$ 台の独立したスキャナで期間 $[0,t]$ で観測できるセンサの数をユニークホスト数と呼び，$h(x,t)$ で表す．同一のホストから繰返しポートスキャンが試行されても，ユニークホスト数は変わらないことに注意せよ．

潜在スキャナ数の同定とは，複数の分散スキャナで観測されたユニークホスト数 $h(x,t)$ を与えて，全スキャナ数 $n$ を同定する問題である．センサは複数箇所に分散して設置しているが，不正スキャナはその場所を知らない．有限時間内に観測できるスキャナの数は限られているが，分散観測された複数の攻撃履歴を統合することが許されている．

この問題を，次を仮定する簡単化されたモデルで考えよう．

仮定 1 スキャナは静的なアドレスを持つ (DHCP などによる動的なアドレス割り当ては行なわない）．IP アドレスの詐称は行なわない．

仮定 2 スキャン先はランダムに決定し，有効なアドレス空間を一様分布する．ポートの区別は行なわない．

仮定 3 スキャンはステートレスに行なう．すなわち，スキャナは過去のスキャン先の記憶は行なわず，毎回ランダムにスキャン先を決める．

仮定 4 単位時間当たり $c$ 回のスキャンを実行する．スキャンの割合は時刻にもスキャナにも依らず一定とする．

このモデルの上では，あるセンサが攻撃対象に選ばれる確率は $1/n_0$ であり，実際には $n$ 台のスキャナがあるので単位時間にスキャンを受ける確率は $n/n_0$ といえる．仮定 4 により，単位時間にセンサが観測する平均ユニークホスト数 $a$ は，

$$a = c\frac{n}{n_0} \tag{1}$$

で与えられる．

今，センサが 2 台あるとする．仮定 2 より観測できるユニークホスト数は変わらないが，同一スキャナから攻撃を受ける可能性があるので，

$$h(2,t) \leq 2h(1,t)$$

であることが予想される．また，同様に，期間を倍にして長く観測する時も，

$$h(x,2) \leq 2h(x,1)$$

である．従って，センサ数 $x$ や観測期間 $t$ を増やしても，ユニークホスト数はそれらに対して線形ではなく，やや鈍い増加を示すはずである．このゆがみは，不正スキャナの総数 $n$ に依存して大きくなり，それゆえ，このゆがみを正確に測定できればそこから $n$ が求められるだろう．

ここで，$n$ の上限は $2^{32}$ の全 IP アドレス空間であるが，実際には未割り当てや外部へ公開していないプライベートなアドレスブロックがある．[1] によると，一カ月の観測結果より，$n_0 = 89 \cdot 2^{24} = 1,493,172,224$ が示されている．

### 2.2 観測期間についてのユニークホスト数

仮定より，$h(1,1) = a$ であり，次の単位時刻には更に $a$ 台のスキャナが観測できる．ただし，

そのうち，既に観測済である確率は $h(1,1)/n = a/n$ なので，平均 $a^2/n$ 台が重複する．よって，

$$h(1,2) = h(1,1) + a - ah(1,1)/n = 2a - a2/n$$

ここでは，センサ数 $x = 1$ とおいて，$h(t) = h(1,t)$ と置き換え，一般化すると，

$$h(t+1) = h(t)(1 - a/n) + a$$

が得られる．差分 $h(t+1) - h(t)$ から極限を取り，ユニークホスト数に対する微分方程式

$$\frac{dh}{dt} = -\frac{a}{n}h(t) + a \qquad (2)$$

が得られる．

一階線形微分方程式の一般解を式 (2) に適用すると，

$$\begin{aligned} h(t) &= C \cdot e^{-\frac{a}{n}t} + e^{-\frac{a}{n}t} \int e^{\frac{a}{n}t} \cdot a dt \\ &= C e^{-\frac{a}{n}t} + n \end{aligned}$$

ここで，初期条件 $h(0) = C e^0 + n = 0$ より，$C = -n$．よって，

$$h(t) = n(1 - e^{-\frac{a}{n}t}) \qquad (3)$$

を得る．ここで，$n$ が潜在的なスキャナの数，$a$ が単位時間にセンサが観測する平均ユニークホスト数である．

### 2.3 センサ数についてのユニークホスト数

全節では，$h(1,t) = h(t)$ と置いたが，$t$ を $x$ と置き換えても全く同様な議論が成立する．すなわち，センサ数 $x$ についてのユニークホスト数もまた式 (3) で定式化できる．従って，観測期間を変えてのユニークホスト数から導く不正スキャナ数と観測センサ数についてのユニークホスト数から推定する不正スキャナ数とが一致することが期待できる．

注意しなくてはならないのは，実際に観測するユニークホスト数はセンサの位置するアドレスブロックの場所やパケットフィルタリングの影響を受けて，必ずしも一定にはならないことである．可能なすべての組合せについて平均を取るなどの前処理が必要になる．

## 3 実験

以上の原理の正当性を検証し，ユニークホスト数からの不正スキャナ推定するために次の実験を行った．

### 3.1 実験環境

本実験でセンサを設置した環境と条件を表 1 に示す．センサには，Windows XP 上で動作するパーソナルファイアウォール Zone Alarm を用い，全てのポートを遮断してログに履歴を記録した．センサ $S_1, S_2$ の環境では，インターネットとのゲートウェイにおいていくつかのポートがフィルタリングされており，観測されるスキャン数が少ない．一方，$S_3$ はインターネットに直接接続されている．いずれのセンサも常時接続しているが，停電や障害により数日単位の欠損が生じている．

表 1: センサ実験環境

| | $S_1$ | $S_2$ | $S_3$ |
|---|---|---|---|
| 観測期間 | 2005 年 5 月 29 日〜8 月 31 日 | | |
| クラス | B | B | C |
| 帯域 [bps] | 100M | 100M | 8M |
| ネットワーク | 大学 1 | 大学 2 | 商用 ISP |

### 3.2 実験結果

観測されたユニークホスト数を表 2, 3, 4, 5 に示す．

表 2 は週ごとの平均と標準偏差であり，前節の平均ユニークホスト数 $a$ を示している．ただし，センサ $S_3$ に限っては，他のセンサと条件をそろえるために TCP ポート 111(SUN RPC), 135 (MS RPC), 139 (NetBIOS), 445 (SMB) を除外している．単位時間を月，週にするかによって，$a$ は大きく変わる．

表 3, 4, 5 は月間，週間，センサ数についての累積ユニークホスト数である．ただし，センサ数についての累積は全ての組み合わせの平均値を取っている．例えば，$x = 2$ の時は，$(S_1, S_2)$, $(S_1, S_3)$, $(S_2, S_3)$ の 3 組の平均値である．

表 4: 週別累積ユニークホスト数

| $t$ [week] | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $S_1$ | 104 | 245 | 353 | 474 | 583 | 706 | 817 | 893 | 989 | 1054 | 1091 | 1198 | 1326 |
| $S_2$ | 339 | 676 | 1016 | 1309 | 1671 | 2015 | 2319 | 2579 | 2889 | 3155 | 3437 | 3644 | 3938 |
| $S_3$ | 440 | 827 | 1177 | 1560 | 1960 | 2391 | 2839 | 3225 | 3621 | 3850 | 4063 | 4384 | 4754 |

表 2: 平均ユニークホスト数 $a$

| センサ | 週平均 | 標準偏差 | 日平均 |
|---|---|---|---|
| $S_1$ | 129.00 | 18.22 | 18.43 |
| $S_2$ | 346.89 | 28.18 | 49.56 |
| $S_3$ | 452.89 | 31.93 | 64.70 |

表 3: 月別累積ユニークホスト数

| $t$ [ヶ月] | 1 (6 月) | 2 (6-7 月) | 3 (6-8 月) |
|---|---|---|---|
| $S_1$ | 517 | 975 | 1389 |
| $S_2$ | 1495 | 2828 | 4040 |
| $S_3$ | 1665 | 3128 | 4579 |

### 3.3 不正スキャナ総数

以上の実測データを基にして，式 (3) の理論値への当てはめを行う．最少二乗法を適用して，未知パラメータ $n$, $a$ を同定した．例えば，表 3 の $S_3$ の 3 点から，

$$h(3) = 14828.5(1 - e^{-x/8.25})$$

が算出できる．ここで，$n = 14828.5$ が推定される潜在スキャナ数, 時定数 $n/a = 8.25$ である．である．同様にして，他の全ての測定データについてあてはめを行った結果を表 6 に示し，図 3.3, 2, 3 にそれぞれ図示する．

表 6 における誤差は最少二乗法による近似誤差の大きさを示しており，図からも明らかなように近似精度は悪くはない．しかし，潜在スキャナ数を表す $n$ には，同定に用いたデータに応じて 4857 から 95709 までの 20 倍近くの差が生じている．それでも，センサの数は高々10 万台で押さえられることが予想される．これは，$n_0$ の母集団に対して極端に小さく，$n/n_0 = 6.409 \cdot 10^{-5} = 0.0064[\%]$ である．すなわち，**1 万 5 千台に 1 台存在する**程度である．

表 5: センサ台数別累積ユニークホスト数

| $x$ | 1 | 2 | 3 |
|---|---|---|---|
| 6 月 | 1226 | 2394 | 3533 |
| 7 月 | 1147 | 2228 | 3280 |
| 8 月 | 1068 | 2042 | 3097 |

最も多くのデータに基づいて推定が行われた図 2 のグラフを観察すると，ユニークホスト数の増加が線形よりもわずかに小さくなっていることがわかる．この測定期間の範囲内では極端にデータが変わる事件も起きておらず，増加率も安定している．週間累積でも月間累積でも，$S_3 > S_2 > S_1$ の順でユニークホスト数に違いがあり，それが最終的な潜在スキャナ数 $n$ にも影響している．

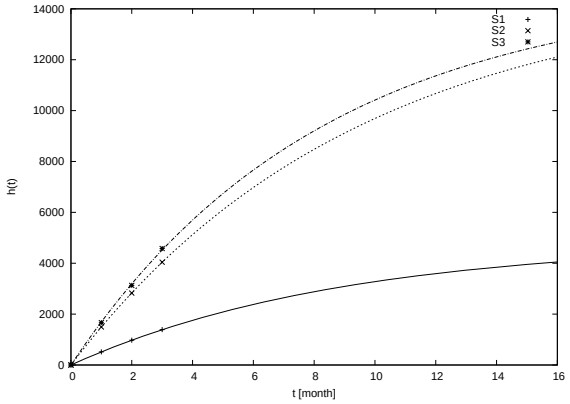


図 1: 月間累積ユニークホスト数

本実験結果について，累積ユニークホスト数の他にも，スキャン先の時系列分布 (表 4) とセンサ間の相関 (表 5) を解析した．スキャン先分布は，全センサにスキャンを行ったあるホストに着目して，時刻についてのスキャン先 ($S_1, S_2, S_3$ に対応する 1,2,3) をプロットしている．偏りはあるが，スキャン先が周期的に変化してきていることが観察できる．対象としたスキャナは，全センサに攻撃してきた全 60 台のスキャナの中から平均的なものを選んでおり，他のスキャナも同様の振る舞いをしている．

表 6: 推定パラメータ

| 推定手段 | $n$ | 誤差 | $n/a$ | 誤差 |
|---|---|---|---|---|
| $S_1$ 月間累積 | 4857.88 | 106.3 | 8.91224 | 0.2255 |
| $S_2$ 月間累積 | 14828.5 | 335.3 | 9.43599 | 0.2447 |
| $S_3$ 月間累積 | 14828.5 | 3951 | 8.25209 | 2.571 |
| $S_1$ 週間累積 | 6001.53 | 1705 | 48.6973 | 14.89 |
| $S_2$ 週間累積 | 17293.2 | 3236 | 48.8514 | 9.837 |
| $S_3$ 週間累積 | 32446.5 | 1107 | 31.5434 | 1.205 |
| 6 月センサ累積 | 33212.5 | 2653 | 26.6853 | 2.239 |
| 7 月センサ累積 | 26266.7 | 2502 | 22.5051 | 2.272 |
| 8 月センサ累積 | 95709.6 | 204800 | 91.4829 | 198.8 |

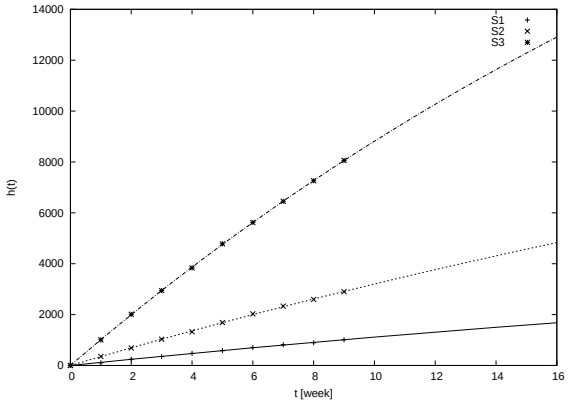


図 2: 週間累積ユニークホスト数

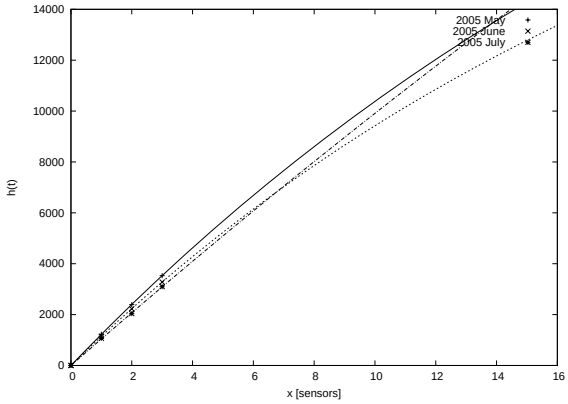


図 3: センサ数累積ユニークホスト数

図 5 では，上記の 3 つのセンサに加えて，$S_2$ に近いサブネット（第 2 オクテットまで同一）に設置したセンサ $S_4, S_5, S_6$ の 6 台のセンサの間で，一週間の間で共通に観測できたスキャナの数を示している．図より，$S_2, S_4, S_5, S_6$ の間の相関が高く，ほぼ対角線と同一のユニークホスト数を有していることがわかる．重複の割合は，0.4 から 0.8 に分布しており，このセンサ群については仮定 2 が成立しない．

### 3.4 単位時間当たりの平均スキャン数

実験結果から得られるもう一つの知見は，一つのスキャナが単位時間あたりに実行するポートスキャンの数 $c$ の推定である．

仮定 2 の元で，ユニークホスト数は確率 $c/n_0$ で試行する二項分布になる．二項分布の平均値より，式 (1) が得られる．一方，表 6 の時定数 $n/a$ が与えられているので，

$$c = \frac{a\, n_0}{t_w n}$$

が得られる．ここで，$t_w$ はその単位時間の大きさ，$c$ は一秒あたりのスキャン数に置き換えている．例えば，表 4 の週間累積の $S_3$ の $n = 32446.5, n/a = 31.5434$ から求めると，$t_w = 60 \cdot 60 \cdot 24 \cdot 7$, $c = 78.27$ [回/秒] が得られる．この値は明らかに手作業で行う回数を越えており，ウィルスや攻撃用のスクリプトによる実行であることを示唆している．

### 3.5 考察

実験結果の誤差について考える．センサ数と測定期間という異なった条件から算出したにもかかわらず，表 6 の与える $n$ のオーダー ($10^4$) は一致していた．また，測定結果のグラフから

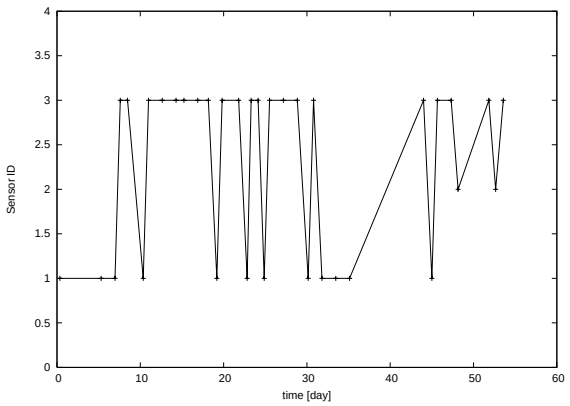


図 4: スキャン先の推移

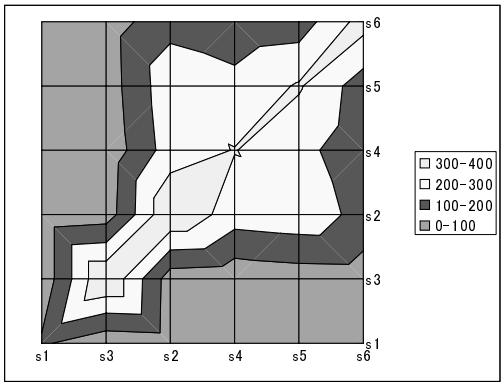


図 5: センサ間の相関（重複ユニークホスト数）

理論どおりの振る舞いが生じていることも観察できた．それゆえ，本提案の推定方式は妥当であると結論付ける．

誤差の生じる原因としては，次が考えられる．

- センサ数 3，測定期間 13 週間という観測データが小さすぎる．
- センサの独立性．アドレス空間が近いなどの理由で，攻撃の相関の高いセンサを用いていると一様性の仮定 2 に反する．しかし，図 5 に示されたように，ユニークホスト数を見る限り 3 つのセンサは十分に独立していると考える．
- センサ先の一様性．攻撃者が特定のネットワークを対象にしているとすると，推定スキャナ数に大きな誤差が生じる．スキャン先の時系列分布の図 4 より，スキャンは十分にランダムに分布していると考えられる．
- スキャナの攻撃パターンの違い．実際のスキャンはポート番号や脆弱性の種類によって大きく異なる [2]．しかし，今回はポート番号の区別をせず，全て共通のスキャンアルゴリズムに従うことを仮定した．この仮定 4 が強すぎる可能性がある．
- センサの設置箇所の環境の違い．フィルタリングだけではなく，アクセス制御やトラフィック制御などが実行されていると観測数に大きなゆがみが生じる．あるいは，ファイアウォール内からの攻撃が生じて，測定値に影響を与えている可能性もある．

## 4 おわりに

ポートスキャンの振る舞いに単純な確率モデルを導入し，観測できるユニークホスト数の理論式を導出した．この結果に基づいて，3 台の独立したセンサのポートスキャンの履歴データを分析し，インターネット全体における不正な潜在的スキャナの数は 4,900 から 96,000 台の間であることを推定した．これは，インターネット全域において，約 1 万 5 千台に 1 台の不正なホストが存在することを意味している．また，スキャン先を一様に選んでいるという仮定の下で，不正ホストは平均して毎秒 78 回のポートスキャンを実行していることを示した．

## 参考文献

[1] 杉山，他，アクセスログを用いた不正ホスト総数の推定に関する検討，情報処理学会, FIT 2005, 2005.

[2] 寺田，高田，土居，ネットワークワーム動作検証システムの提案，情報処理学会論文誌，Vol. 46, No. 8, pp. 2014-2024, 2005.

[3] J. Jung, V. Paxson, A. W. Berger, and H. Balakrishnan, “Fast Portscan Detection Usig Sequential Hypothesis Testing”, proc. of the 2004 IEEE Symposium on Security and Privacy (S&P’04), 2004.