4X-07

行動変容過程の解明のためのスパム送信サーバ観測

Classification of spam mail transmission patterns based on their servers' severity levels

山口 翔生 † 中平 勝子 † 北島 宗雄 †
Kakeru Yamaguchi Katsuko T. Nakahira Muneo Kitajima

1 はじめに

本稿ではスパム送信サーバの情報送信を観測し, その収集データより各サーバの情報送信行動を解析する. 先行研究 [1] ではイベント発生のパターンを定量的に測る手法である Evolution Diagram を使用し, サーバのスパム送信行動変容の特徴として最大送信能力, 継続性, 再起性を定義した. 本稿では, これらのサーバの行動変容過程から, サーバの健全性を回復し保つ力である復元力 [4][5] について議論する. 復元力とは Zolli らの"システムなどが基本的な目的と健全性を維持する能力"という定義を利用し, 本研究ではネットワーク上に存在する様々な障害や課題の存在下でサービスを許容できるレベルに維持する力として扱っている. サーバのスパム送信行動変容は復元力によって, 変容過程を分析する事で復元力の強弱を考察する事ができる. 復元力の強弱は単純なスパム送信量だけではなく, スパム送信密度, 期間, スパム送信再発率といった, サーバ管理者側が如何に早急にサーバのスパム送信に気がつき, サーバに対して適切な処理を行いスパム送信を停止させ, その後も安定したサービスを提供し続けているか, といった点が重要となる. これは復元力の強弱がセキュリテリシステムだけではなく, サーバ管理者の活動, ユーザのモラル, 法律, インフラなどのサーバの環境に影響されることを示している. これら環境は各地域, TLD ごとの管理運用ポリシーによって変化, スパム送信の行動変容を観測する事で, 環境の実態を分析できると考える. 本稿では復元力を指標としたサーバ分類を行い, 地域ごとのスパム送信特性について考察を行った. それによりスパム送信サーバ生態の実態を調査する手法を確立する.

2 Evolution Diagram

先行研究 [1] ではスパムの情報送信量特性を表す Evolution Diagram (以下, ED) を定義した. ED はメール送信を観測する時間間隔を変化させ, 各時間間隔ごとのスパム送信頻度を求めることによってスパムの情報送信量特性を表す手法である. そしてこの手法から得られたスパムの悪質さを表す総 ED 値が得られる. そしてこの総 ED 値より, スパム送信特性である最大送信能力, 継続性, 再起性を定義した. 総 ED 値を観測期間 $T = 1year$ で求めた場合, 1 年間でのスパム送信に対するおおよその悪質さを示すことがわかっている. スパム送信の観測区間を $T = 1week$ とし, 区間ごとの総 ED 値の変化を観測しスパム送信特性を解析した. 先行研究 [1] において, 最大送信能力, 継続性, 再起性は次の様に定義された. 最大送信能力は全期間中, 最もスパム送信が激しかった (総 ED 値の高かった) 連続する数区間を抜き出すことで導出され, そのサーバの潜在的なスパム送信能力を表す. 継続性は全期間中のスパム送信区間数と, 各区間の取る総 ED 値によって導出され, そのサーバのスパム継続送信能力を表す. 再起性は一定の非スパム送信区間を挟んで出現したスパム送信区間数によって導出され, スパム送信の再開率を表す. 復元力に関わるスパム送信特性の強弱は再起性 > 継続性 > 最大送信能力と定義する. 再起性が 0 ということは, スパムが常に送信されているのでなければ, スパムが再発しなかったということであり, それはサーバに起こっている問題を根本的に解決できたという事でもある. 継続性は問題解決にかかった時間を表している. 短時間での問題解決が好ましいことは自明であるが, どの程度でその問題を発見 · 解決できるかはサーバの環境次第である. 最大送信能力はそのサーバの能力や環境などに大きく依存すると考えられる. 復元力の観点からいうなら, 再起性や継続性の値が小さければ最大送信能力はどれほど大きくても問題ない.

3 スパム送信サーバ分類

本章では最大送信能力, 継続性, 再起性の 3 つのサーバ特性の組み合わせよりサーバ分類を行う. 各特性値の規格を合わせるために, 特性値の出現確率からウォード法によるクラスタリングを行った. 表 1 は分類された各クラスのパラメータを表している. この表より A~G の各クラスの考察と, 対応するクラスが多かった地域の復元力についての考察を行う.

観測データは, 筆者の大学のメールフィルタリングソフト (spam assasin) によってスパムと認定されたものを収集した. 観測期間は 2013 年 3 月 1 日から 2014 年 2 月 28 日までであり, 全体で 21,332,168 通のスパムと 1,733,929 ドメインを確認した. 本研究では 1,733,929 ドメインの中からランダムに 10,000 ドメインを抽出し, これをスパム送信サーバの代表例として扱った.

A **クラス**: 最大送信能力, 継続性双方の平均値で他のクラスを大きく引き離す値を持っていることから, 大量のスパムを長期的に送信するサーバである. およそ半年から 1 年間にかけて毎日スパム送信を行っているサーバが多く属している. このクラスの送信スパムメール数は, 全クラスのスパムメール総数の 37 % に及ぶ. 全体の 2.5 % のサーバが 37 % のスパムを送信しているというのは, スパム送信の大部分が少数のサーバから行われている事を示している. このクラスは 1 年のほとんどの期間を取り締まられずに常にスパム送信を行うことが可能な環境にいるため最も危険なサーバ群である.

B **クラス**: A クラスに次ぐ, 最大送信能力と継続性の平均値を

† 長岡技術科学大学

表1　クラスタリング結果のパラメータ

	A	B	C	D	E	F	G
データ数	258	374	528	727	1137	504	6372
平均継続性	4.42	3.38	2.14	1.68	1.22	1.22	1
平均最大送信能力	5.04	3.03	1.09	2.64	1.17	1.59	1.02
平均メール数	178	83.1	3.14	20.7	6.9	8.07	2.75
再起性	37.9%	63.1%	87.5%	8.11%	6.08%	0%	0%

持ち合わせている．そして再起性の高さから, 大量のスパム送信を断続的に 1 年を通して行うサーバが多いことがわかる．

C **クラス**：特徴は再起性の高さにある．再起性の全サーバでの平均値は 15 % ほどなので, C クラスは再起性の高さによってクラスタリングされたと言える．最大送信能力が低いことから, 1 ヵ月に 1,2 通のみのスパム送信である．また継続性は再起性とある程度連動するため値が大きくなっているが, 最大送信能力の低さから, 1つ1つのスパム送信区間は連続していないと考えられる．このサーバ群は極少数のスパム送信を数か月置きに行うサーバ群だと言える．このクラスは東ヨーロッパの地域での割合が高い．アジアと違い, 地理的にも遠いはずなのに長期な送信を行うということは, この地域のサーバが全世界に長期的な周期でスパム送信を行っている可能性を示している．

D **クラス**：特徴は最大送信能力の高さにある．また B クラスと比べて最大送信能力ほど, 継続性は高くない事がわかる．およそ 1 ヵ月程度の期間, まとまった量 (20 通程度) のスパムをまばらに送信するサーバ群だといえる．このクラスは高いインターネット普及率の地位 (西ヨーロッパ, アメリカ大陸) での割合が高い．つまり十分にインフラが整備されたサーバから送信されるスパムは, 大量のスパムを送信する傾向があると言える．また短期的な送信で停止する場合が多いことから, インターネット普及率の高さは復元力の高さともつながっていると考える．

E, F **クラス**：2 つのクラスの特徴は似ている．1, 2 週間程度の期間に少数のスパムを送信するサーバである．E クラスの方が若干, 継続性, 再起性が高いサーバ群であり, F クラスは最大送信能力が高いサーバ群である．

G **クラス**：多くの場合は極短い期間 (数秒間) のみスパム送信を行うサーバである．スパム送信を行うサーバの半分以上がこのクラスに属する．このクラスは全ての地域で最も高い割合を示すが, 中でも中東地域はその割合が特に高い．ただ中東地域は一度のスパム送信数, スパム送信サーバ数がアジアに次いで高いため, 復元力が高いためにこのクラスが多いわけではなく, スパム行為者が転々とサーバを移動するために G クラスが多い可能性がある．

全体的な特徴としては低いインターネット普及率の TLD に属するスパム送信サーバが全サーバの大部分を占めていた．これは低いインターネット普及率がサーバ管理技術水準の低さ, 法整備の低さにつながり, スパム行為者の利用しやすい環境になっているからだと考える．また E, F, G クラスの様に非常に短期間 (1 週間程度) にスパムを送信し停止するサーバが全体の 80% 程度を閉める事は, スパム送信サーバは基本的には流動的にサーバからサーバへ渡り歩いている事を示している．

4　まとめ

本稿では復元力を指標としたサーバ行動変容観測手法を考案した．そして復元力によりサーバを分類し, 地域, TLD ごとに分類結果の比率を考察し, その結果, 各地域, TLD ごとのスパム送信行動特性を分析し, それは各地域の復元力の違い, 管理運用ポリシーの違いを示唆した．本稿の結果は本大学から観測されたものであり, 必ずしも全世界の正確なスパム送信の特性, 復元力を表すものではない．しかし, 現代は様々な情報を共有しあい, 相互に補助し合う社会である．その中で各組織, 地域の視点からのスパム生態を共有する事で, より鮮明なスパム送信サーバの生態を考察できると考える．

謝辞：本研究の一部は学術研究助成基金助成金 24500308 の助成を受けたものである

参考文献

[1] 山口 翔生, 中平 勝子, 北島 宗雄: スパム送信サーバの重篤度によるスパム送信パターン分類, FIT 2014 L-023, 2014

[2] Joshua Goodman, Gordon V. Cormack, David Heckerman; Spam and the Ongoing Battle for the Inbox, COMMUNICATIONS OF THE ACM, Vol.50, No.2, 25, 2007.

[3] 竹下 峰弘, 中平 勝子, 三上 喜貴: スパムメール発信源分析によるサーバ・ドメイン管理実態の推定, 一般社団法人情報処理学会 全国大会講演論文集, 2011(1), 499-501, 2011.

[4] Smith, P. Hutchison, D., Sterbenz, J.P.G., Sch ller, M., Fessi, A., Karaliopoulos, M., Lac, C., and Plattner, B: Network resilience: a systematic approach. Communications Magazine, IEEE, Vol. 49, No. 7, 88-97, 2011.

[5] アンドリュー・ゾッリ, アン・マリー・ヒーリー：レジリエンス 復活力–あらゆるシステムの破綻と回復を分けるものは何か, ダイヤモンド社, 2013

[6] Katsuko T. Nakahira, Kakeru Yamaguchi, Muneo Kitajima, Ecology of Spam Server Under Resilience Force in the e-Network Framework

[7] Internet indicators: Hosts, Users and Number of PCs ,http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[8] Katsuko T. Nakahira : A Framework for Understanding Human e-Network - Interactions among Language, Governance, and more. presented in "——— Symposium international sur le multilinguisme dans le cyberespace", http://www.maayajo.org/IMG/SIMC/paris-v2.pdf,2012