情報処理学会論文誌 Vol.56 No.10 2022–2032 (Oct. 2015)

インターネットレジリエンス感知のための スパム送信サーバの行動変容観測

山口 翔生[1,a)] 中平 勝子[1] 北島 宗雄[1]

受付日 2015年1月9日, 採録日 2015年7月1日

概要：本稿は，インターネットを安心・安全に利活用するレジリエンス感知を行うためのスパム送信サーバ行動変容観測手法を構築する．現代社会におけるインターネット利活用は通信インフラとして確固たる地位のもと，世界中に利用者（構成員）が存在する．こうしたインフラの共有原則・基準・規則・意思決定手順・進化および使用のための綱領はドメインおよびそれを管理する団体によって階層構造により管理運用されているが，実際には利用者の潜在的な価値観に基づく利用となるため必ずしも原則・規則が遵守されるわけではない．この小さな綻びを大きな綻びにしないための新たな安心・安全への仕掛けとしてインターネットにおけるレジリエンスの導入が考えられる．そこで，インターネット利活用状態の安心・安全度をスパム送信サーバの行動という形でとらえ，それを定量的に測定するための手法である総合 ED 値，およびスパム送信サーバの生態である行動変容を特徴づける最大送信能力，継続性，再起性を定義する．これらの量を用い，地域や TLD ごとのレジリエンス特性の抽出可能性について考察した．

キーワード：スパム，レジリエンス，インターネットガバナンス

Observation of Behavioral Changes of Spam Mail Servers to Detect Resilience in the Internet

Kakeru Yamaguchi[1,a)] Katsuko, T. Nakahira[1] Muneo Kitajima[1]

Received: January 9, 2015, Accepted: July 1, 2015

Abstract: Resilience in the Internet is critical for maintaining sound and safe use of the Internet. This paper addresses the issue of detection of resilience in the Internet by developing a method for observing behavioral changes of spam mail servers. Currently the infrastructure that enables people in the world to make use of the Internet has been established. There exist hierarchically organized fundamental principles for its use, sharing, development, decision-making procedures, etc. These principles are managed and operated by a variety of administration committees. However, they are not necessarily obeyed strictly due to their diverse understandings. This paper suggests that resilience force would be effective for maintaining e-mail servers in their safe and secured conditions by avoiding small problems from turning into critical ones. On the assumption that the working of resilience force of an e-mail server should be reflected in its observable behavior, this paper proposes a method for quantitatively measuring the degree of server's safety and security conditions, called "Evolution Diagram," and for deriving the degree of resilience by means of maximum transmission potential, the degree of continuity and reproducibility defined by using Evolution Diagram. Regional and TLD resilience is examined by using these features.

Keywords: spam, resilience, Internet governance

1. はじめに

本稿は，スマート社会を実現する重要な基盤であるインターネットの継続的な安心・安全な利活用が実現されているかを，“インターネットレジリエンス” という観点から

[1] 長岡技術科学大学
Nagaoka University of Technology, Nagaoka, Niigata 940–2188, Japan
[a)] yukidaruma1232@yahoo.co.jp

感知するためのスパム送信サーバ行動変容観測手法を構築する．インターネットを通じて情報交換を行う社会において，その機構の中枢であるサーバや通信インフラには様々な問題が起こりうる [3]．それらの問題が発生する大多数の原因はセキュリティ技術だけでなく，そのサーバや通信インフラを取り巻くサーバ管理者の活動，ユーザのモラル，法規制やその実現のための意思決定手順，インフラ普及およびその発展計画などが複雑に絡み合って存在する．こうした問題解決の一手法にレジリエンスの考え方を導入することができる [7]．ネットワークにおけるレジリエンスは，Smith ら [6] によって，“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能力” であるとされている．

本稿では，インターネット社会のレジリエンスは，セキュリティ技術だけでなくインターネット社会を構成する種々の要素とあわせて存在しうると考える．すなわち，安心・安全なネットワーク利活用の推進には，セキュリティ技術を含めた不正行為防御や堅牢な設備を構築するためのハード/ソフトウェア技術開発のほか，そこに介在する人や環境を内包する社会システムとしての設計や管理運用綱領が必要となる．こうした社会システムにおいて，現状維持，現状への復興という堅牢なシステム構築だけでなく，“許容できるレベル” でのサービス提供という柔軟な発想によって安心・安全を提供するという考え方がインターネットレジリエンスであるとした．

例として取り上げるスパム送信行為はサーバを技術的に安全/安定運用しようとする人，ユーザとして通常メールを送受信する人，スパムを意図的に送信する人で構成される．こうした人の営みは，運用を担う人は管理運用綱領という規範に，ユーザはインターネット利用に対するモラルの有無に，あるいは経済活動の一環として正規/不正なインターネット活動を行わざるをえない環境，といった様々な社会環境との相互作用の結果，生じる．したがって，スマート社会のように人–情報–基盤が互いに共存しあう社会において安心・安全にそれらを推進するうえで各々の社会に見合った適切な管理運用綱領の存在は，ユーザのモラル向上や健全な経済活動に資するという意味で重要である．

本稿では，インターネット利活用において実際にさらされる現象に立脚したセンサに基づいたインターネット利用状況の実態把握を行うことで，レジリエントな安心・安全に配慮したインターネット利活用を行うための情報提供を行う手法を提案する．その第 1 段階として，インターネットレジリエンスを感知するための指標を作成する．そのために，ネットワーク上に存在するサーバに着目し，時間軸にそってサーバから発信される典型的な違法行為であるスパム送信パターンを観測する．この際のスパム送信は，サーバ管理者を含めたサーバ利用者によるものだけではなく，サーバに不正に侵入したスパム送信や bot によるものも含まれる．その送信パターンの変化をスパム送信行動変容としてとらえることでスパム送信サーバの行動変容を捕捉できるようにする．本稿では，そのために，スパム送信サーバの特性を解析するための指標として ED 値を積分した総合 ED 値を提案する．次に，総合 ED 値から得られる ED 推移図を導入し，スパム送信サーバの生態を特徴づける量として最大送信能力，継続性，再起性を導出し，これら 3 つのパラメータの組合せによりサーバごとのインターネットレジリエンスを記述する．サーバは全世界に分散して存在することから，サーバを地域ごとにグループ化，地域内に存在するサーバのインターネットレジリエンスやそこから派生するインターネットレジリエンスの地域特性の有無，その抽出可能性について考察する．

2. スパム送信サーバ行動とレジリエンス

スパム送信サーバを扱ううえで重要なことは，その行動変容を引き起こす周辺要素を取り上げ，それらを接続する “レジリエンス” との関係を可能な限り記述することである．スパム送信サーバのレジリエンス強度とは，スパム送信を停止，あるいは防止し，健全な状態へ回帰する力によって決まり，複数の要素によって求められる．

一般的に，メール発信可能なサーバは，サーバの下に多くのユーザが存在し，スパム送信の原因となる状況として，以下の場合が想定される：

(1) 管理者自身が違法プログラムをサーバに実装した場合．
(2) サーバを利用しているユーザが，故意に，あるいはウィルスなどに汚染されたクライアントを使用し続けることによりスパム送信が行われる場合．
(3) サーバが第三者によってクラッキングされてスパム送信が行われる場合．

スパム送信を防ぐことを考える場合，インターネット社会に多く存在するユーザが自身のクライアントにおいて違法行為を行わないための措置をとることで違法行為を防ごうと考えるのが主流である．しかし，サーバ管理者はサーバが他者に迷惑をかけるような行為を極力防ぐという役割を担っているため，スパム送信行為が放置されている状態は，サーバ管理者の技術力不足，あるいは管理に対する意識不足，またはモラルの低さからくる防御放棄が起こっていると見なされる．また，サーバを利用しているユーザにむけた違法行為を防ぐための啓蒙活動もサーバ管理者の役割の 1 つである．このことから，本稿ではスパム送信サーバの行動変容は近似的に管理者に依存するインターネットレジリエンスと関係すると見なす．

ネットワークにおけるレジリエンスは Smith ら [6] によって規定されているが，ここではスパム送信サーバおよびそこに連なる人や環境を 1 つの巨大なシステムに見立てるため，より広範なレジリエンスの定義として Zolli らによって紹介されているものを想定する．Zolli ら [8] によれ

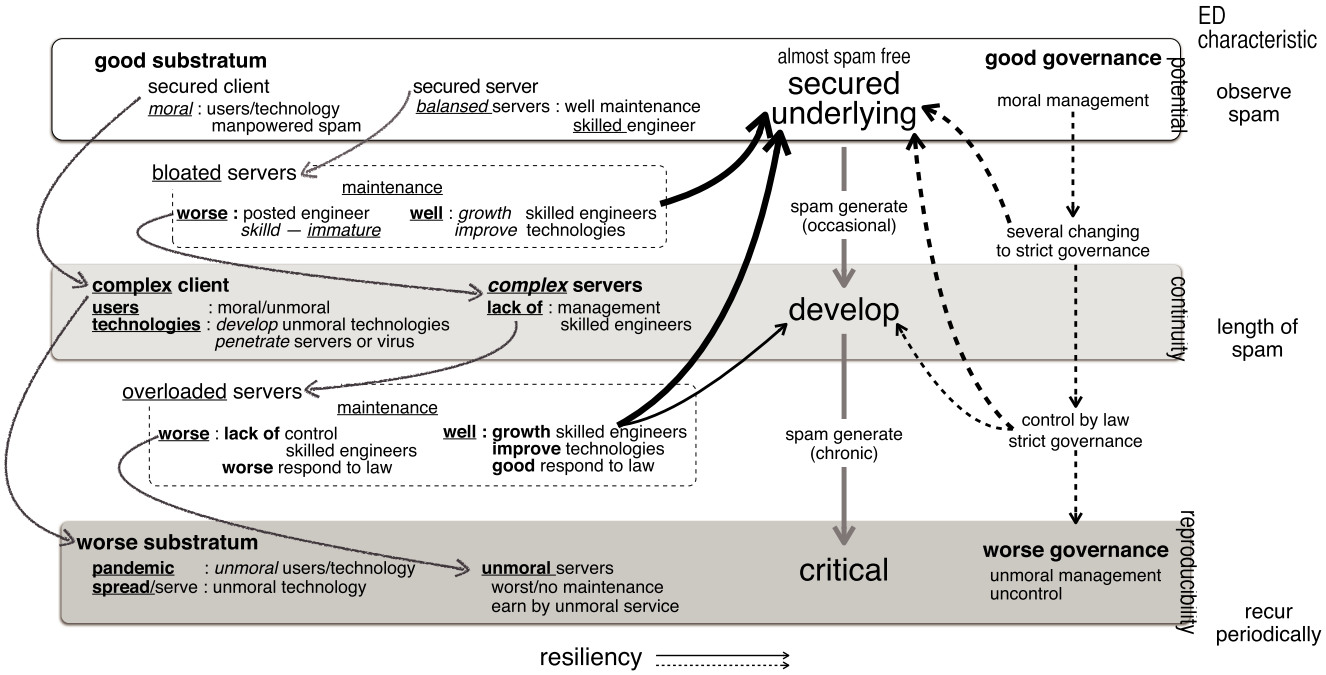


図 1 スパム送信サーバ行動変容プロセスの微細構造

Fig. 1 Microstructure of behavioral change processes of spam mail servers.

ば，レジリエンスとは

“システム，企業，個人が極度の状況変化に直面したとき，基本的な目的と健全性を維持する能力”

と定義される．本稿では，これに対応させ，インターネットレジリエンスを支える技術的/文化的/人的な要素が極端な改悪へと状態変化がおきたとしても，インターネット社会全体，各地域/団体，個人が，インターネットの円滑な利活用を維持するための改善が行われる，すなわち健全性維持能力をインターネットレジリエンスとして扱う．

図 1 に，スパム送信サーバ行動変容プロセスの微細構造を示す．スパム送信サーバは，利用者，ハードウェアなどの基盤，ソフトウェア，管理者，インフラ，文化など様々なものが相互作用することでその生態系を形成しており，これらはスパム送信行為の是非判断にも影響している．一連の相互作用は Nakahira ら [5] によって e-Network として提案されており，本稿でもその枠組みに従ってスパム送信サーバの行動変容を記述する．e-Network の枠組みによれば，インターネットにおける様々な社会現象は人的要素，基盤要素，生成物，環境の 4 要素に，要素間接続するメディアを加える形で記述可能であるとしている．人的要素にはメール利用者や管理者（サーバや ISP），基盤要素にはメール送信サーバやインターネット通信網およびこれらの通信を可能とする種々の技術，生成物にはスパムメール，環境には法規制やインターネット管理運用綱領をあてはめる．これらは，図中の各レイヤにおいて，左側 2 列に人的要素とそこから派生する基盤要素を，レイヤ間に人的要素と基盤の関係を，右側に環境要素をそれぞれ記述し，各要素もしくは条件の状態遷移を下向き矢印で，レジリエンスによる状態復元を上向き矢印で示している．各レイヤは，観測対象とするサーバの状態を “secure underlying（準安定状態）”，“developing（スパム送信拡散初期）”，“critical（スパム送信慢性発生期）” の 3 状態で記述する．

通常，ネットワーク上の状態変化，特にネットワークの安全な利用を阻害する要因を取り除くという意味ではセキュリティの堅牢性やシステム構成の冗長性という観点から研究されている（たとえば，文献 [3], [11], [12], [13], [14]）．本稿では管理者/運用者/利用者の思考を変える，あるいは社会規範を変えることで利用者が安心してネットワークを継続的に利用できるための，観測事実に基づいた管理運用綱領を提案するための方策を提案する．そのため，現状をどのように最適化しているかという点が重要になる．サーバ行動の最適化とは，そのサーバが目的としているサービスを問題なく行えるような環境を構築することを指す．したがって，スパム送信行為を行ってしまったサーバが，スパム送信やサーバ乗っ取りなどの問題に対し，ユーザの利便性，そのサーバが提供する機能を維持できるならばレジリエンスは高いと考える．

スパム送信状態の変容は次のように考える．

secure underlying：サービスを行うには最も良い状態で，サーバ提供サービス開始時はよほどのことがない限りこの状態である．最新 OS や最新技術を備え，モラルの高いユーザが大部分を占めており，またサービスの規模もサーバ管理者が管理しやすい規模で構成される．しかし時間がたつにつれ，サービスの拡大，ユーザの増加，システムの陳腐化，ユーザモラルの悪化など様々な環境変化が起こると予想される．高いレジリエンスを保持していれば，

これらの悪化は深くはならず，安心してインターネットを利活用できる．その意味において，良いサービスを維持でき “secure underlying” にとどまることができるが，レジリエンスが弱ければ悪意を持つユーザの増加や，サービスへの妨害が増加し “Developing” の段階へ移行する．この場合，レジリエンスを決めるのは，主としてサーバ管理者の管理技術，基盤技術，モラルである．

Developing：“secure underlying” の状態に戻すために様々な戦略を構想するべき段階であるとともに，悪意を持つユーザが増加している段階でもある．この状態を放置すると，より悪い状態へと変容することが考えられるため，可能な限りスパム送信を抑制する手段を講じる必要がある．その際のアクタはネットワーク利用者/管理者/運用者，技術開発，および法による緩やかな規制となる．これらがうまく相互作用できた場合にはレジリエンスがうまく働き，secure underlying の状態に戻ることができるが，そうでなければ “critical” 状態へと変容するだろう．

critical：まったくレジリエンスが期待されない段階である．スパム送信は続き，サーバ管理者は管理を放棄し，法律も止めようとしない．この状態に置かれたサーバにはそのサーバ本来の役割は期待できず，安心なインターネット利活用という観点では末期の状態といえる．

こうした事実の観測/分析は，(1) インターネット上のある特定サーバだけに対して，(2) インターネット上のある特定地域に対して，(3) インターネット社会全体に対して，行うことができる．一連の観測/分析結果を研究機関や管理運用策定機関間で共有することにより，(1) については，個のサーバあるいは ISP に対する管理運用綱領の即時見直しに，(2) については，地域内全体の，(3) については，インターネット社会全体の，管理運用綱領の見直しやより良い改訂に寄与することが可能である．

3. サーバごとのスパム送信行動変容観測

スパム送信サーバの行動変容は，個々のサーバがスパムを送信するパターンの変化としてとらえるため，次の手順で指標化する．

(1) ある観測幅 δt において記述される ED 値の提示
(2) δt を変化させた ED 値を k 種類について算出
(3) k 個の ED 値を合計した総合 ED 値を算出
(4) 総合 ED 値の時間変化を ED 推移図として記述
(5) 記述された ED 推移図から 3 つの特徴量を提示

本章では，その中でも最も重要な値である総合 ED 値の算出法について述べる．

ED 値とは，特定イベント発生の時間遷移パターンを定量的に示したものである．ここでいう特定のイベントとはスパム送信である．スパム送信やスパム送信を行うサーバには様々なタイプがあることは先行研究により分かっている [13], [14]．本稿では時系列パターンの特徴によるタイプ分けに着目した．類似手法として，Reference Interval Free 連続 DP（RIFCDP）や，それらの応用手法がある [15]．これらの手法は，音声データなどの複雑な信号から類似する任意区間を検出し，データを特徴づけるパターンを得る．本稿では，それらとは違って，類似した区間を検出するのではなく，時系列順に連続する各区間でスパム送信の特性がどのように遷移していくかに注目する．

ED 値はイベント発生の時間遷移に関係する量として規定される．これにより，観測期間，観測幅を変化させることでスパム送信密度の変容を観測でき，スパム送信サーバの行動変容をとらえるのに適していると考えられる．

この密度変化を効果的にとらえるために，いくつかの区間幅（1 年，半年，3 カ月，$\cdots$）を用意し，特定の区間幅の観測期間の中でイベント発生がどのように起こっているかを記述する．その際，イベント発生の様子は配列として記録される．配列の各要素は時間軸に沿った区間で並べられ，イベントが起こっていればその区間に対応する要素には 1 が割り当てられ，起こっていなければ 0 が割り当てられる．最小計測単位時間を τ とする．なお，本稿では $\tau = 1$ 秒である．このとき，計測を行う全配列数は T/τ になり，観測結果に基づいて各要素に 1 または 0 が割り当てられる．この観測基本配列を，

$$\vec{a} = (a_1, \cdots, a_{T/\tau})$$

と表現する．次に任意の区間幅でのイベント発生をみるために，分割区間幅 $\delta t = j \times \tau,\ j = 1, 2, \cdots, T/\tau$ とし，その分割区間数を以下のように定義する．

$$L(\delta t) = \frac{T}{\delta t} \tag{1}$$

任意の分割区間数 $L(\delta t)$ でのイベント発生配列を $\vec{b}(\delta t) = (b_1, \cdots, b_{L(\delta t)})$ とする．この配列 $\vec{b}(\delta t)$ も $\vec{a}$ 同様に要素のとる値は 0 または 1 である．ED 値 $I(\delta t)$ は以下の式を適用して $\vec{b}(\delta t)$ から導出される．

$$I(\delta t) = \sum_{i=1}^{L(\delta t)} \frac{b_i}{L(\delta t)} \tag{2}$$

ED 値は $0 \leq I(\delta t) \leq 1$ であり，j が T/τ に近づくにつれて 1 に近づいていく．仮に対象のサーバがスパムを全期間で 1 通のみ送信した場合，ED 値が 1 になるのは $j = T/\tau$ のときである．

総合 ED 値 $ED_{\mathrm{total}}(k)$ は $I(\delta t)$ の値を k 種類の分割区間数に対して求めたものを合計することで算出する．

$$ED_{\mathrm{total}}(k) = \sum_{i=1}^{k} I(\delta t_k) \tag{3}$$

総合 ED 値の特徴を理解するため，総合 ED 値を形成する要素であるスパム数，スパム発生間隔を変化させ，総合 ED 値の変化を追跡する．**表 1** は，スパム送信の観測期間

表 1 $T = 2^{24}$ 秒の場合の総合 ED 値．括弧内の数字は全スパム数
Table 1 Total ED value in the case of $T = 2^{24}$ sec. The numbers of spam mails in parentheses.

スパム数/1 カ月		1 通	5 通	10 通	30 通
1 カ月		2.00(1)	2.25(5)	2.34(10)	2.48(30)
連続	2 カ月	2.3(2)	2.99(10)	3.17(20)	3.45(60)
	3 カ月	2.63(3)	3.41(15)	3.70(30)	4.10(60)
	4 カ月	2.88(4)	3.72(20)	4.06(40)	5.57(120)
等間隔	6 カ月	3.00(2)	3.99(10)	4.16(20)	4.42(60)
	4 カ月	3.50(3)	4.37(15)	4.64(30)	5.06(90)
	3 カ月	4.00(4)	4.99(20)	5.57(40)	6.34(120)

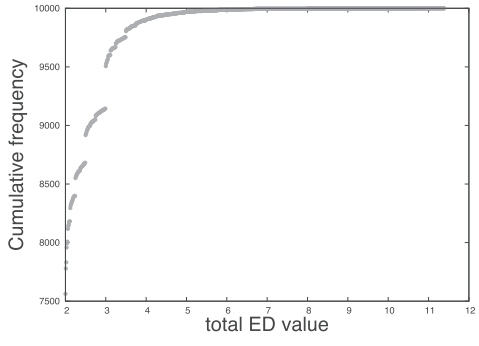


図 2 総合 ED 値発生頻度
Fig. 2 Frequency of total ED value occurrences.

を 1 年，期間の最大分割区間幅を 2^N（$N = 24$）とした際に，表に記された条件下における総合 ED 値を表している．分割区間数を $j = (1, 2, 4, \cdots, 2^N)$ として，それに合わせた区間幅 $L(\delta t)$ を決める．表の列は 1 カ月に送信されるスパム数を表し，スパムはその月の中で等間隔に送信されるとして計算を行った．たとえば，5 通の場合，その月の中で等間隔になるように約 6 日おきに送信されるとした．表の行はスパムが送信される月のパターンを表す．これは等間隔送信と連続送信に分けられる．等間隔送信では表に示した間隔でスパム送信が行われる月が出現する．一方，連続送信ではスパムを送信する月が表に示した期間，連続で現れる．カッコ内は 1 年を通した総メール送信数を表している．表から分かるように，総合 ED 値は必ずしも総スパム数と比例しない．スパム数が同じであったとき，より広範囲にスパムを送信するサーバをより危険だと判定している．また，たとえスパムの送信量が少なくても長期的にスパム送信を行うサーバは健全な状態へ戻るレジリエンスが弱いといえる，期間全体での総合 ED 値は，これらの特徴を有しているので大まかなサーバの健全度を示しているといえる．

実際のスパム送信サーバがどのような総合 ED 値をとりうるのかを確認するために，実測を行った．その結果を**図 2** に示す．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（SpamAssassin）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 7 月 31 日までであり，21,332,168 通のスパムと 1,733,929 サーバを確認した．本稿では 2013 年 3 月 1 日から 2013 年 12 月 31 日の間で 1 通以上スパム送信を行ったサーバの中から，ランダムに 10,000 サーバを抽出し，これをスパム送信サーバの代表例として扱った．図 2 に，標本として抽出した 10,000 サーバにおける ED 値分布を示す．これが母集団と同等の振舞いをすると考える．図から分かるように 7,562 サーバは総合 ED 値 ≈ 2 である．これは，ほとんどが 1 年を通してスパムが 1 通もしくは同時刻に複数のスパムを送信し，それ以降の送信がなかった場合である．これは，式 (3) を導く $\vec{a}$ において，1 要素のみが 1，それ以外が 0 であったため，$\vec{b}(\delta t)$ も 1 要素のみが 1 でそれ以外が 0 となり，式 (3) の右辺が以下のように 2 に近づくことによる．

$$\sum_{n=0}^{N} \frac{1}{2^n} \approx 2 \tag{4}$$

総合 ED 値が 2.5 以上のサーバは 1,318 サーバであり，全体の 13%程度を占める．表 1 から分かるように，1 カ月間毎日 1 通ずつスパムを送信するようなサーバであっても総合 ED 値は 2.5 未満に収まっている．そして 1 カ月以上，複数のスパムを送信するようになって総合 ED 値は 2.5 以上となることが見て取れる．このことから “総合 ED 値が 2.5 以上の値となる” ということは，スパム送信の悪質さを示すうえでの 1 つの区切りの基準であると考えられる．

4. ED 推移図とスパム送信特性

4.1 ED 推移図

前章において，ある時点までのスパム送信サーバの状態を示す指標として総合 ED 値を導入し，その特性を調べた．しかし，スパム送信サーバの行動は時間とともに変化するため，時間経過にともなって変化する行動変容をさらに評価する必要がある．そのために，本章では，“ED 推移図” を導入し，スパム送信特性に関係する 3 つの量を指標として導くことで，スパム送信サーバの行動変容をとらえる．ここでは，観測期間 T を 6.048×10^5 秒（約 1 週間）として，全 N_w 週にわたる期間の総合 ED 値の変動を観測する．

ED 推移図は，連続する 2 週間の総合 ED 値を用いて定義される N_w 個の xy 平面上の点，

$$(x_{n-1}, y_{n-1}) = (ED_{\text{total}}(t_{w_{n-1}}), ED_{\text{total}}(t_{w_n}))$$
$$n = 1, \cdots, N_w$$

を結んで構成される多角形（軌跡）によって作成される．ここで，観測する週を t_{w_n} と表現している．時間経過とともにある一定の軌跡を描くが，その軌跡が早い段階で原点もしくは x 軸，あるいは y 軸へ近づけば近づくほど，スパム送信数が 0 に近づく，すなわちよい変容を起こしていると見なせる．

図 3 は ED 推移図の極端な 2 つの例を示したものであ

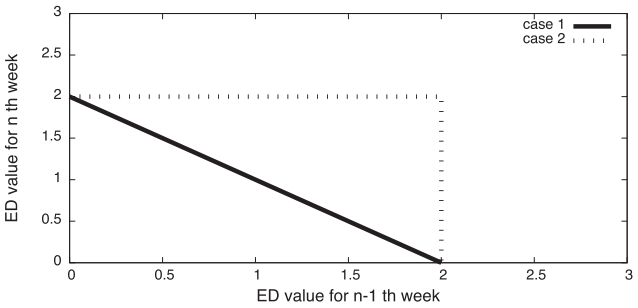


図 3 ED 推移図の例
Fig. 3 Examples of ED transition diagram.

表 2 種々の状況下における最大送信能力の値
Table 2 Maximum transmission potential values under a variety of circumstances.

スパム総数		1 通	5 通	10 通	30 通
送信間隔	送信パターン				
半月	等間隔	1.00	4.98	7.18	12.69
	ランダム	1.00	2.48	3.23	4.02
1 カ月	等間隔	1.00	2.60	3.90	8.81
	ランダム	1.00	2.23	2.85	3.82
2 カ月	等間隔	1.00	1.81	2.18	4.60
	ランダム	1.00	2.00	2.66	3.57

る．ケース 1 は観測期間全体（$T = 2^{24}$ 秒）のうちでスパムが 1 通のみ送信された場合を示している．表 1 が示しているように，区間全体でスパムが 1 通のみ送信された場合は $ED_{\text{total}} = 2$ となる．このケースでは，スパムが送信された区間は 1 通のみのため $ED_{\text{total}} = 2$ となり，それ以外の区間ではスパムが送信されていないため $ED_{\text{total}} = 0$ となる．よってこのケースの座標は $(0,0) \Rightarrow (0,2) \Rightarrow (2,0) \Rightarrow (0,0)$ と推移する．ケース 2 は 1 週間の間をおいて 2 通のスパムが送信された場合であり，スパム数の区間ごとのパターンとしては $(0,1,1,0,\cdots)$ であったケースである．この場合の座標は $(0,0) \Rightarrow (0,2) \Rightarrow (2,2) \Rightarrow (2,0) \Rightarrow (0,0)$ と推移する．ケース 1，2 の座標推移を見た場合，ケース 1 の方がサーバが早めに健全に戻るという点でレジリエンスは高いと推定できる．以下の節では，この ED 推移図から，本稿で提案するサーバのレジリエンス指標である，スパム送信サーバの最大送信能力，継続性，再起性を導入し，それらの指標の値を求め，サーバのレジリエンスについて考察する．

4.2 最大送信能力

最大送信能力は短期間でのスパム送信の集中度という特性を表すことができ，期間全体のスパム送信密度ではなく，そのサーバが最も活発だった期間の危険度，潜在的なサーバの危険度を測る指標である．本稿ではスパム送信パターンを送信密度と期間により分類しており，最大送信能力は前者を定量的に求める．

最大送信能力は，ED 推移図の外縁で囲まれる面積から求める．図 3 を例とすると，ケース 1 は三角形の面積，ケース 2 は四角形の面積となる．複数の多角形が交わっている，あるいは重なっている場合は，図の外縁をなぞり 1 つの多角形を構成した後に計算する．これはサーバの潜在的なスパム送信量を示し，スパム送信の短期間（1〜4 週間程度）でのスパム送信密度が高いほど瞬間的に大量のスパム送信を行う力が高いことを示している．

表 2 は設定した状況下での最大送信能力を計算したものである．状況は 1 カ月，半月の期間中に等間隔，ランダムの間隔で設定した量のスパムが送信された場合を想定している．ランダムな送信パターンは同じ状況下で 1,000 回試行した結果の平均をとった．観測期間中に 1 通のみスパム送信した場合を基準値 1 とし，他の値を正規化している．表から分かるようにスパム送信密度が高いほど最大送信能力が高くなる．また，スパム送信間隔が長い場合はランダムな送信間隔の方が高い値を持つと考えられる．さらに，スパム送信密度が同じであるなら，スパム送信期間が長い方が値が高くなり，基本的には等間隔な送信間隔より，ランダムな送信間隔の方が値が小さい．しかし，期間 2 カ月の状況では 5 および 10 通のときにその関係は逆転している．これは等間隔の場合ではスパム送信期間が長く，スパム総数が少ない状況では個々の区間に入るスパム数がごく少数になり，区間ごとの総合 ED 値が固定化され，ED 推移図に現れる図形が一定の形から変化しないためである．逆にランダムな送信間隔の場合は，いずれかの区間にスパム送信が偏る場合が多く，その結果，隣接区間との ED 値の変化が激しくなり ED 推移図に現れる図形が複雑な形をとるからである．

図 4 左は，図 2 と同一データから得られた最大送信能力の出現頻度である．0.1%が 25 以上，0.5%が 8 以上，1%が 6 以上，10%が 2 以上の値をとることが観測されている．表 2 のランダムな送信間隔の値を基準とするなら，10%以上のサーバが短期間ではあっても，数日に 1 度はスパムを送信していることが推定できる．逆に全観測期間（$T = 2^{24}$ 秒）で 1 通のみスパムを送信するサーバは全体の 48%であることが分かっている．また 70.03%が “最大送信能力 = 1” であるから，およそ 22%ほどが 1 度の送信で 2 通以上のスパムを送信しているといえる．

4.3 継続性

継続性は ED 推移図内の隣接点間の距離を合計することによって算出される．この値はスパム送信期間が長いほど高い値を持ち，対象となるサーバの送信継続能力を表す値である．**表 3** は設定された状況下での継続性を計算したものである（条件，観測データは表 2 と同様）．スパム送信が同一送信間隔である場合，スパム送信数に対してある特定の状況を除いてはさほど感度がない．それに対し，スパ

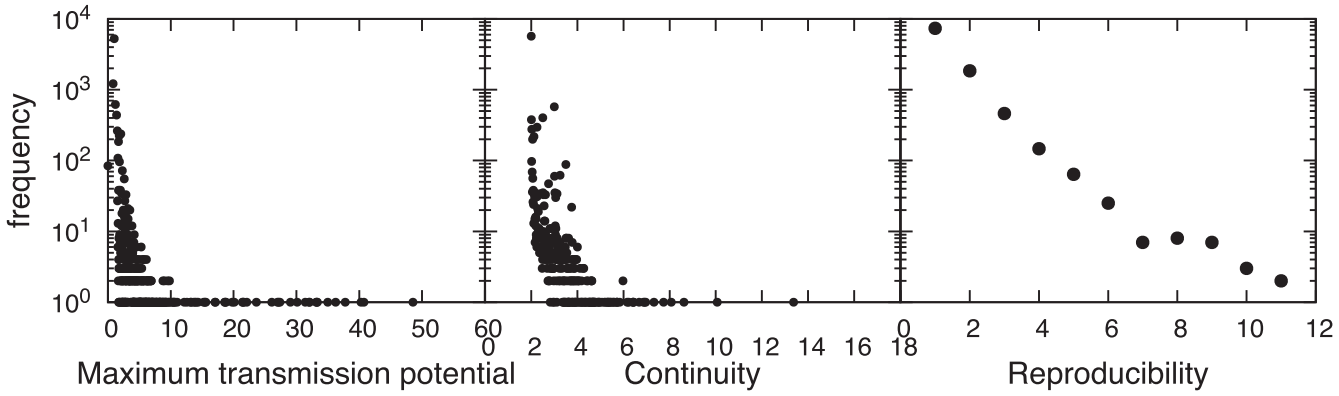


図 4 各パラメータの出現頻度．左：最大送信能力，中：継続性，右：再起性
Fig. 4 The frequency of each parameter. Left: Maximum transmission potential, Center: Continuity, Right: Reproducibility.

表 3 種々の状況下における継続性の値
Table 3 Continuity values under a variety of circumstances.

スパム総数		1 通	5 通	10 通	30 通
送信間隔	送信パターン				
半月	等間隔	1.00	1.20	1.57	1.63
	ランダム	1.00	1.10	1.18	1.31
1 カ月	等間隔	1.00	1.63	1.83	2.54
	ランダム	1.00	1.57	1.47	1.57
2 カ月	等間隔	1.00	3.36	1.37	1.75
	ランダム	1.00	2.57	2.72	2.20

ム送信数が同一である場合には，スパム送信期間に対して高い感度を示す．これは，スパム送信密度が高くなることで総合 ED 値の変動が少なくなることによる．また，スパムごとの送信間隔が広く，かつ複数のスパム送信が行われる場合には，表中の期間 2 カ月/等間隔/スパム総数 5 通のときに見られるように，継続性は高い値を示す．つまり，継続性は，長い送信期間，まばらにスパム送信を行うサーバを特に危険だと判断する．継続性が高い値をとるということは長期的なスパム送信をしているということであり，サーバ管理者がスパム送信を認知していない，もしくは対策していないということを表している．図 4 中央は図 2 と同じデータから得られた継続性の出現頻度である．0.1%が 12.5 以上，0.5%が 6.4 以上，1%が 5.1 以上，10%が 1.9 以上の値をとることが観測されている．

4.4 再起性

再起性は，スパム送信に対して自発的に，あるいはなにがしかの対策がなされていったんスパム送信を停止したサーバがスパム送信を再開した回数として定義する．スパム送信の再開は，スパム送信が最後にあった区間から n_m 区間以上離れてスパム送信が再開した場合カウントする．本稿では n_m を 1 カ月に相当する 4 とする．表 3 から分かるように，継続性は連続した期間のスパム送信密度によってスパム送信の危険度を示す．再起性は，継続性と違いスパム送信密度には影響されにくく，長スパンで断続的にスパムを送信するサーバに対して評価が低くなる．図 4 右は図 2 と同じデータから得られた再起性の出現頻度である．図から分かるように，スパム送信サーバのうち，スパム送信が再開するサーバの割合はおよそ 15%である．

4.5 スパム送信特性

以上の過程から得られたサーバ特性値である．最大送信能力，継続性，再起性を用い，実際に観測されたスパム送信サーバを特性値の出現頻度からウォード法によるクラスタリングによってクラス分けを行う．各特性値の規格を合わせるために図 4 より各特性値の出現確率を用いてウォード法によるクラスタリングを行った．その結果，以下に示す 7 クラスタを得た．

A，*B* クラス：最大送信能力，継続性の両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．*A* クラスと *B* クラスの違いは再起性の高さの違いである．*A* クラスはおよそ半年から 1 年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．再起性は全クラスの中で 3 番目であるが，これはスパム送信に切れ目がなく絶えず行っているため，1 カ月以上スパムを送信しないサーバが少ないからだと考えられる．送信スパム数は，全クラスのスパム総数の 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，スパム送信サーバの生態がスケール性に基づいているともいえる．*A* クラスは 1 年のほとんどの期間を取り締まられずにつねにスパム送信を行うため最も危険なサーバ群である．*B* クラスは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．

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%ほどであるが，その大多数が *C* クラスに集まっている．最大送信能力が低いことから，1 カ月に 1，2 通のみのスパム送信であることが分かる．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．このサーバ群はきわめて少数のスパム送信を数カ月おきに行うサーバ群だといえる．

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，最大送信能力が高い割には，継続性は高くないことが分かる．およそ1カ月程度の期間，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である．

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，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．しかし，短期間とはいえなかには数百通のスパム送信を行ったサーバも含まれている．100通を超えるスパム送信を行っているサーバの割合はサーバ全体で1.1%であり，その中にクラスGのサーバが13%含まれている．これは結果的にスパムを大量送信するサーバが，必ずしも継続的に送信しているわけではないことを示している．*G* クラスではスパム送信量の多寡に差はあるが，ごく短期間でスパム送信が停止した，という点において共通している．

4.6 スパム送信特性とレジリエンス

以上の議論をふまえ，各サーバにおけるレジリエンス強度について議論する．レジリエンス強度とは，個のサーバの健全性を維持するための力の強さであり，スパム送信が行われた後，どれだけ早急にスパム送信を停止できたか，また再発を防げたかによって決まる．この際のスパム送信にはbotによるものも含まれる．その場合は，サーバ管理者がスパム送信botの存在をどの程度の期間で認知できたか，対処を行ったか否か，という点がスパム送信特性に表れ，レジリエンスとして評価することができる．なかでも，再起性は最も影響力のある特性である．再起性が0ということはスパム送信が再発しなかったということであり，つねにスパム送信を行っている場合を除き，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ことでもある．この問題の根本的な解決というのはレジリエンスにおいて最も重要な要素であり，e-Networkにおいてサーバ管理者，利用ユーザ，法律などが有効に作用し，“secure underlying” にサーバの状態を戻した証拠といえる．

次に，継続性について考察する．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管理者の職能やサーバモニタリング技術導入など様々な要素が関わるため，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．レジリエンスの観点からいえば，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．また，最大送信能力が高いということは，大量のスパムを一瞬にして送信している状態を指すため，サーバの管理者が異変に気が付きやすいとも考えられる．もしこの値が大きいまま，継続性，再起性が上昇するのであれば，それはサーバ管理者や法律などがサーバの健全性を維持しようとしないと考えられ，e-Networkにおける “Development” から “critical” へと状態が遷移する．

以上のことから，レジリエンスに関わるスパム送信特性の強弱は，再起性 > 継続性 > 最大送信能力の順にその深刻さを判定できる．このことから，分類した7つのクラスのレジリエンスの強弱を $G > F > E > D > C > B > A$ であるとした．

G クラスを最もレジリエンスが高いとした理由は，すべてのパラメータの低さである．前述したように *E* クラスには数秒のうちに100通以上のスパムを送信するサーバも含まれている．しかし，その後の送信がないということは，おそらくサーバ管理者や周りの環境がスパム送信を止めたのだと推定できる．そして再発性もないことから，その後の維持管理もしっかりとしており，レジリエンスはきわめて高いクラスだと考えられる．

D，*E*，*F* クラスは一定期間のスパム送信は許すが，その後はスパムに対して対処できたサーバ群である．これらのクラスも一時的にサービスに不備がでたが，その後 “secure underlying” に戻ったレジリエンスが強い部類だといえる．

C クラスは再発性の高さからレジリエンスが弱い部類に入る．最大送信能力，継続性は低いが，それはこちらのサーバに送信してきたスパムが少ないだけで，別のサーバには大量のスパム送信を行っているかもしれない．また1度サーバからスパム行為者を追い出したとしても，何度も再び侵入されているようでは管理能力が高いとはいえず，レジリエンスは低いと考えられる．

A，*B* クラスはおそらくサーバ管理者がサーバ管理にいっさいかかわっていない状況だと考えられる．そして周りの法律，文化などもスパム送信を止める要因にはなりえない環境であると推定できる．毎日，大量のスパム送信を行っていても問題ない環境に置かれたサーバは最も弱いレジリエンス下で存在すると考えられる．

5. 地域群ごとのサーバ生態

最後に，個のスパムサーバ送信変容の地域特性を見ることで，インターネットレジリエンスをとらえることの可能性について述べる．スマート社会において人，基盤，情報は密接につながっているものであり，その中で行われるスパム送信行為も同じく，これらの要素が原因となっていると考えられる．特に，人が介在するということは，スパムサーバ送信変容にはなにがしかの地域特性，あるいは基盤

表 4 スパム送信サーバの行動特定結果の地域分布
Table 4 Regional distribution of the results of behavior assessment of spam servers.

項目名		サーバ数	平均スパム数	サーバ重篤度タイプの割合 (%)							ネット普及率 (%)
				A	B	C	D	E	F	G	
観測対象サーバ		10,000	12.33	2.58	3.74	5.28	7.27	11.37	5.04	63.72	
高ネット普及率		601	22.00	4.33	4.83	2.00	15.64	7.32	7.15	58.74	74.7
低ネット普及率		2,809	16.78	4.38	4.95	3.42	7.33	8.44	4.20	67.28	15.0
地域	アジア	1,994	23.84	4.46	5.87	3.51	9.38	10.68	4.91	61.1	36.4
	アメリカ大陸	624	16.78	3.21	4.65	1.60	11.38	8.01	5.77	65.5	44.2
	中東，南アジア	1,640	17.97	0.55	1.10	2.99	4.21	10.18	4.33	76.6	13.9
	西ヨーロッパ	389	11.10	2.83	2.31	2.83	8.74	8.71	5.40	69.2	60.1
	東ヨーロッパ	3,357	5.85	2.65	4.05	8.76	6.49	13.50	5.09	59.4	28.9

状態に関係する特性が見られても不思議ではない．そこで，特定地域，特定条件に存在する個のスパムサーバ送信の状態とレジリエンスのクラス分布から地域特性が見られるか，地域のインターネットレジリエンスの相違を見ることができるか，といった可能性について述べる．

表 4 に，筆者の所属する大学のデータから観測されたスパム送信サーバの行動特定分布を示す．まず，全体的なスパム送信サーバのクラスの内訳について考察する．レジリエンスが高いと考えられる E，F，G クラスは全体の約 80%を占めている．これらのサーバはおよそ 1 週間程度の期間スパムを送信し，停止するサーバ群である．この停止した理由は，サーバ管理者などが人為的に停止させた場合と，単に観測しているサーバがスパムを送らなくなった場合の 2 通りが考えられるが，本稿ではメールアドレスの再利用性や実在性の観点から前者が大多数だと仮定している．全体的に見れば，世界の多くのサーバはスパム送信を行っても 1 週間程度で気づき対応できることが分かる．また基本的には悪質なスパム送信を行っているサーバほど少なく，レジリエンスが高いサーバの割合が多い．

高/低ネット普及率については ITU 統計 [9] の順位から，20 通を超えるスパム送信を行っているサーバを上下から 10 カ国抽出した．地域別は各地域からスパム送信が多い順に 5 カ国選び出し，その地域の代表とした．表最右列，各項目に対するネット普及率は ITU の統計をもとにし，国ごとのスパム送信サーバ数の割合より，その分類での平均を求めた．項目別のクラス分類の偏りよりサーバ生態について考察する．

ネット普及率が高い地域：この地域の特徴は，D クラスの割合が高い点，平均スパム数が多い点である．D クラスのサーバは，1 カ月程度の間に 20 通程度のスパムを送信する．このクラスがネット普及率の高い地域に多いということは，高密度なスパム送信を行うには，相応の環境が必要であることを示唆している．インターネット普及率が高ければ，その地域の回線は速くなり，それにともないサーバなどの基盤性能の上昇が考えられる．つまり，スパム送信サーバの性能が上昇するということであり，複数のスパムを多方面に送信することができるのではないかと考えられる．また再発性の高い C クラスは，この地域には少ない．ネット普及率の上昇は同じく IT 技術の向上，法整備の充実にも影響し，長期的なスパム送信やスパム送信の再発を妨げる役割を担っていることが考えられる．

ネット普及率が低い地域：この地域には，スパム送信サーバ数が多い．ネット普及率の高い地域と比較して，同じ 10 カ国であるのに対して 5 倍近いスパム送信サーバが観測されている．これはスパム送信の大部分はネット環境の整っていない地域，IT 技術が未発達の地域から行われていることを示している．

地域特性：本稿では，アジア，アメリカ大陸，中東/南アジア，西ヨーロッパ，東ヨーロッパに分けてその特性抽出を試みた．アジア諸国は，基本的に A，B クラスの割合が平均の倍近く存在する．スパム総数も特定 5 カ国だけでアジア全体の 38%に及ぶ．

国籍別スパム送信割合を報告したシマンテックインテリジェンスレポート 2013 年 1 月 [8] では本稿ほどの偏りが見受けられないことから，インターネットレジリエンス観測地域との距離が大きく影響することが見て取れる．西ヨーロッパは再起性が高い A，B，C，E クラスの比率が低く，特に，ネット普及率の高い地域と比較して B クラスの割合が低いことから，1 つの可能性として長期的なスパム送信と再発防止に努力を払っていることが示唆される．

アメリカ大陸は C クラスが少なく，D クラスが多い．これは大陸内における世界有数のネット大国を含むことが大きく影響すると思われる．突出した特徴を持つ地域を含む場合，1 カ国の影響がその地域のインターネットレジリエンスの判定に大きな影響を与えることを示している．

中東/南アジアは，G クラスの割合の高さ，A，B クラスの割合の低さが特徴である．しかし，サーバ数そのものの多さ，スパム送信数の多さが認められることから，1 つの可能性として，個々のスパムサーバは長時間スパムサーバとして振る舞うことはないが，サーバ行為者がサーバに侵入後，世界中にスパムをばらまきすぐに別のサーバに移るという行為を繰り返していることがあげられる．すなわ

ち，不正に侵入しやすいサーバが多い可能性は考えられ，地域全体のインターネットレジリエンスが高いとは即座にいい難い．

東ヨーロッパは，全スパムサーバの 3 割以上がこの地域に集中していることから，先のアメリカ大陸の例でも見られるとおり，全体平均に大きな影響を及ぼしていると読み取れる．そのため，ほぼ，平均的に近い様相を示す．E クラスの割合が高いことから，特に少ない量のスパム送信を長期的に行うケースが多く，再起性も高い．すなわち，スパム送信に対する管理はほぼ行われていないことになり，インターネットレジリエンスの弱い地域といえる．

6. まとめ

本稿ではレジリエンスを指標としたサーバ行動変容観測手法を提案した．そして，レジリエンス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た．その結果，地域，TLD ごとのスパム送信行動特性を分析し，それは，個々の地域のレジリエンスの違い，管理運用綱領の違いを示唆していることを明らかにした．本稿の結果は，筆者の所属する大学から観測されたものであり，全世界のスパム送信の特性，レジリエンスを必ずしも正確に表すものではない．しかし，スマート社会は，様々な情報が共有され，相互に補助しあう社会である．その共有される情報に，各々の視点からのスパム送信サーバの生態を含めることで，スパム送信サーバの実態をより深く解明でき，インターネット利活用に適したレジリエントな管理運用綱領に寄与することができると考える．本稿で提案した手法を，より多数の観測地点から得られたスパム送信データに適応し，スパム送信サーバのより正確な行動変容を観測することが，今後の目標である．

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：メール送信サーバ情報送信量特性，FIT2013（第 12 回情報科学技術フォーラム）講演論文集，第 4 分冊，pp.271–274 (2013).

[2] Goodman, J., Cormack, G.V., Heckerman, D.: Spam and the Ongoing Battle for the Inbox, *Comm. ACM*, Vol.50, No.2, pp.24–33 (2007).

[3] Xu, Z., Hu, Q. and Zhang, C.: Why computer talents become computer hackers, *Comm. ACM*, Vol.56, No.4, pp.64–74 (2013).

[4] 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，情報処理学会全国大会講演論文集，Vol.2011, No.1, pp.499–501 (2011).

[5] Nakahira, K.T.: A Framework for Understanding Human e-Network Interactions among Language, Governance, and more, *III Symposium International sur le Multilinguisme dans le Cyberespace*, available from ⟨http://www.maayajo.org/IMG/SIMC/paris-v2.pdf⟩ (2012).

[6] Smith, P., Hutchison, D., Sterbenz, J.P.G., Schöller, M., Fessi, A., Karaliopoulos, M., Lac, C. and Plattner, B.: Network resilience: A systematic approach, *IEEE Communications Magazine*, Vol.49, No.7, pp.88–97 (2011).

[7] European Network and Information Security Agency: Measurement Frameworks and Metrics for Resilient Networks and Services: Technical Report (2011).

[8] Symantec：シマンテックインテリジェンスレポート：2013 年 1 月，入手先 ⟨http://www.symantec.com/content/ja/jp/enterprise/white_papers/sr_wp_spam_report_1301.pdf⟩.

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

[10] 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).

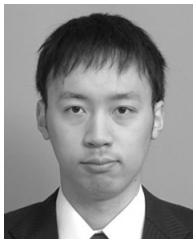
[11] 佐藤一道，脇田 建：大規模スパムフィルタと実験環境の構築手法の提案，情報科学技術フォーラム一般講演論文集，Vol.6, No.4, pp.457–460 (2007).

[12] 山中 純，安達直世，冬木正彦：経路間の距離測度に基づいたスパムメールフィルタリング方式の提案，電子情報通信学会技術研究報告，Vol.107, No.528, pp.33–38 (2008).

[13] 澤谷雪子：メッセージ本文受信前でのスパムメール探知方式の制度向上に関する一検討，信学技報 ICSS2009-57, pp.19–24 (2009).

[14] 鳴海健太，西田京介，山内康一郎：統計的手法と事例ベース手法を併用したスパムフィルタリング，電子情報通信学会論文誌 D，Vol.91, No.11, pp.2569–2578 (2008).

[15] 伊藤慶明：時系列パターンの任意部分区間の高速マッチング手法 ShiftCDP 法，電子情報通信学会論文誌 D-II, Vol.86, No.9, pp.1267–1277 (2003).



山口 翔生

2013 年長岡技術科学大学経営情報システム工学課程卒業．2015 年同大学大学院修士課程経営情報システム工学専攻修了．在学中，スパム送信サーバの研究に従事．現在，株式会社富士通北陸システムズ所属．

中平 勝子 （正会員）

1994 年奈良教育大学大学院教育学研究科修了．2000 年大阪大学大学院理学研究科単位取得満期退学．2001 年早稲田大学教育学部助手を経て，2003 年長岡技術科学大学 e ラーニング研究実践センタ助手，2007 年同経営情報系助教を経て，2015 年同情報・経営システム工学専攻助教，現在に至る．ICT と教育の連携について，技能教育，言語の多様性の観点からの研究に従事．教育工学会，教育システム情報学会，電子情報通信学会，その他各正会員．修士（教育学）．

北島 宗雄

1980年東京工業大学大学院理学研究科修士課程修了．同年4月通商産業省工業技術院製品科学研究所入所．2008年独立行政法人産業技術総合研究所サービス工学研究センター主幹研究員．2011年長岡技術科学大学経営情報系教授．2015年同情報・経営システム工学専攻教授，現在に至る．人間の行動選択過程の認知アーキテクチャ構築の研究に従事．日本人間工学会，Biologically Inspired Cognitive Architectures, Cognitive Science Society, ACMほか各会員．