

# アクセス予測に基づいた 広域冗長型安否システムの提案と基礎評価

永田正樹<sup>†1†2</sup> 阿部祐輔<sup>†2</sup> 金原一聖<sup>†2</sup> 福井美彩都<sup>†2</sup> 峰野博史<sup>†1</sup>

本論文では、WEB システムを構成するサーバ群を世界規模で冗長化し、アクセス数を事前予測して適切なサーバ数で負荷分散を行う広域冗長型安否システムを提案する。既存の安否システムには、災害時の確実な稼働とアクセス状況に応じた適切なサーバ数算出が困難という課題がある。そこで提案システムでは、日本、シンガポール、カリフォルニア、など多地点および地理的に離れた広域拠点にシステムを分散配置し可用性を向上する広域冗長化機構と、災害規模に応じたアクセス数を事前予測し適切なサーバ数にて負荷分散を行うアクセス予測に基づくオートスケーリング機構を実装した。過去災害データを基にしたシミュレーション評価の結果、多地点での広域冗長化稼働とアクセス予測に基づくオートスケーリング機構を用いて年間費用約 64%削減の見込みを得ることで、提案システムの有効性を確認した。

## A Proposal and Evaluation of a Global Redundant Safety Information System Based on Access Prediction Model

MASAKI NAGATA<sup>†1†2</sup> YUSUKE ABE<sup>†2</sup> ISSEI KINPARA<sup>†2</sup> MISATO FUKUI<sup>†2</sup>  
HIROSHI MINENO<sup>†1</sup>

In this paper, we propose global redundant web safety information system which implemented global redundant on the world area and load balancing by the access prediction model. Conventional web safety information system has a problems, which are certain operation at the disaster and adjustment of the number of servers in conformity with access. So we have developed global redundant and auto scaling based on access prediction model to settle a problems. Global redundant arranges a system separately in the distant area and multiple locations (e.g. Japan, California and Singapore). Auto scaling based on access prediction model predicts the access amount according to the disaster scale before access concentration. And load balancing executes. A result of the simulation experiment expected a cost reduction about 64% by global redundant and auto scaling based on access prediction model, and the validity of the proposal system was confirmed.

### 1. はじめに

安否システムとは災害（本論文では地震とする）時に、システム対象ユーザの安否情報を収集・公開する WEB システムである。災害時の被災状況や被災者の安否情報を公開する安否システムは、家族・組織間での安否確認や災害後の復旧活動の迅速化など、災害情報を多数の関係者に公開する仕組みとして WEB システムでの実装が適している[1][2]。安否システムへの要件として災害時の持続稼働が挙げられる。東日本大震災のような深刻な被害を出した災害では早期の被災者安否の収集・公開が多数の人命救助につながるため[3]、安否情報を公開する WEB システムの停止は避けなければならない災害時に途絶することなくシステムを稼働し続けることが重要である[4]。一般的な安否システムの動作仕様は、災害発生時システムからユーザへ安否情報報告を促すメールが送信され、ユーザは受信したメール

に対しリアクションして自己の安否情報を登録・公開し利用者間で安否情報を共有するものである。昨今の安否システムはクラウドコンピューティングを利用した実装が主流であり、スケーラブルな基盤上での冗長化や負荷分散技術を用いて持続可能なサービス提供を実現している。運用面では、サーバ、スイッチなどのハードウェアを資産として保持せずクラウドへアウトソースすることにより、経営資源、人件費などの費用削減を可能とし収益性向上に寄与する。しかし安否システムを既存のクラウド環境上で運用する場合、2つの課題がある。

1 つ目の課題は、広域拠点での冗長化である。安否システムは災害時においてユーザの安否情報収集・公開を目的とするため、災害時は確実に稼働し続けなければならない。東日本大震災のような大規模災害では災害地域周辺のデータセンター施設群が倒壊する恐れがあり、災害地域のデータセンターにて安否システムを稼働している場合、システム停止が懸念される。つまり一地域・一大陸内での冗長化対策では大規模災害時のシステム停止リスクを回避できない。

†1 静岡大学 創造科学技術大学院  
Graduate School of Science and Technology, Shizuoka University  
†2 株式会社アバンセシステム  
AvanceSystem Corporation

2 つ目の課題は、アクセス状況に応じた適切なサーバ数算出である。安否システムは災害時にユーザからの安否情報報告や安否情報公開リクエストが集中するため、平常時と比較するとアクセス処理に必要なサーバ数に開きがある。仮に災害発生に備え災害時のアクセスに対処可能なサーバ数で常時運用する場合、アクセスが少ない平時では過剰リソースとなり安否システムのように常時稼働を求められるサービスでは費用対効果の面から困難な運用を強いられる。

本研究では上記 2 つの課題を解決するため、WEB システムを構成するサーバ群を世界規模で冗長化し、災害時のアクセス数を事前予測し適切なサーバ数にて負荷分散を行う広域冗長型安否システムを試作開発し評価結果から有効性を示す。

2 章では従来研究と課題、3 章では提案システム構成、4 章ではアクセス予測モデル、5 章では実装と評価、6 章では考察、7 章でまとめとする。

## 2. 従来研究と課題

### 2.1 安否システム

安否システムの関連研究には、図 1 に示すように、情報収集、WEB システム、通信など様々な分野の研究が関係するが、本研究では冗長化、負荷分散といった WEB システム基盤を対象とする。通信関連の研究では、ワンセグや無線等[5][6]を用いて災害時のネットワーク輻輳に対して輻輳回避や回線確保のためのアルゴリズムを用い確実な通信手段を実現し有効性を示している。情報収集関連の研究では、DTN を用いたすれ違い通信にて安否情報を中継し最終的に SNS へ登録する提案[7]や、QR コードを用いた安否情報の収集[8]では、収集後の情報管理までを含んだ情報マネジメントシステムの構築を行い利便性の高い安否情報管理を実現している。これら通信及び情報収集関連の研究においても情報管理には一般的に WEB システムが用いられているため、災害時の総合的な安否情報管理には WEB システム基盤の持続稼働が重要となる。

WEB システム基盤関連の研究では[9][10]、災害時にシステムのロバストネス向上を目的とし、複数サーバを用いたミラーリングでの冗長化や、DNS ラウンドロビンやリダイレクトでのアクセス先振り分けを用いた複数サーバでの負荷分散の提案がある。しかし冗長化は国内での実装評価に留まっており東日本大震災規模の災害ではシステム持続稼働が課題となる。負荷分散は複数サーバを用いている点は本研究においても同じ立場を取るが、平常時・災害時を問わず常時複数サーバでの構成のため平常時でのサーバ費用や余剰リソースが課題となる。

### 2.2 課題 1: 広域冗長化

災害時の確実な稼働を要求される安否システムは一地域内でなく多地域での冗長化運用が有効である。AWS (Amazon Web Services) [11]や Azure[12]に代表されるクラ

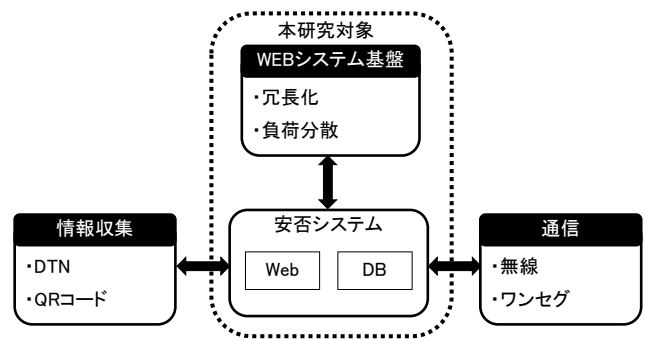


図 1 安否システム関連研究

Fig. 1 Related study of Safety Information System.

ウドベンダーは、世界各地にデータセンターを有しており広域冗長化を実現するシステム基盤として適している。しかし現状の各サービスは主に同一の地域(以下、「リージョン」)内での提供が主流であり、システムを複数地域に跨ぐ構成にする場合は課題がある。負荷分散を行うロードバランシングサービスではロードバランサーが稼働しているリージョン内のサーバに対してのみ通信可能で他リージョンのサーバへ通信できない。冗長化では、リージョン内の同ネットワークセグメントのサーバに対してルーティングテーブルを変更し参照先サーバを切り替えることでフェイルオーバーが可能だが、ルーティングテーブルへは他リージョンのネットワークセグメントを指定できないため、やはりリージョン内での冗長化になる。つまり 1 リージョン全域が大災害等で被災しリージョン内の全てのサービスが停止した場合、複数リージョン間での広域冗長化が必要になるためクラウドベンダーの標準サービスに追加した機能実装が必要となる。

### 2.3 課題 2: 状況に応じたサーバ数

平常時と災害時でシステムへのアクセス数に開きがある安否システムは、アクセス状況に応じたサーバ数で運用することで費用削減が可能である。アクセス集中に対するシステムのリソース管理として最も安直な施策は、状況に依らず予め多数のサーバで常時稼働しておくことである。しかし常時多数サーバでの運用は、アクセスが少ない平時のサーバリソースは余剰リソースとなり、そのまま余分費用に直結する。広域冗長化は災害の発生予測が困難なため常時敷設でなければ意味を為さないが、アクセス状況に応じたサーバ数をその都度確保する仕組みがあればアクセスの少ない平時の余剰リソースを削減でき、安否システムのリソース管理としては理想的である。またアクセス集中後のサーバ追加では、システムが高負荷となった状態での事後対応となりレスポンス低下などユーザの利便性を損ねるため、アクセス集中前に適切なサーバ数算出および追加が望まれる。アクセス状況に応じた最適なサーバ数を算出するためには、災害発生からその後のアクセス分布の予測が必要である。

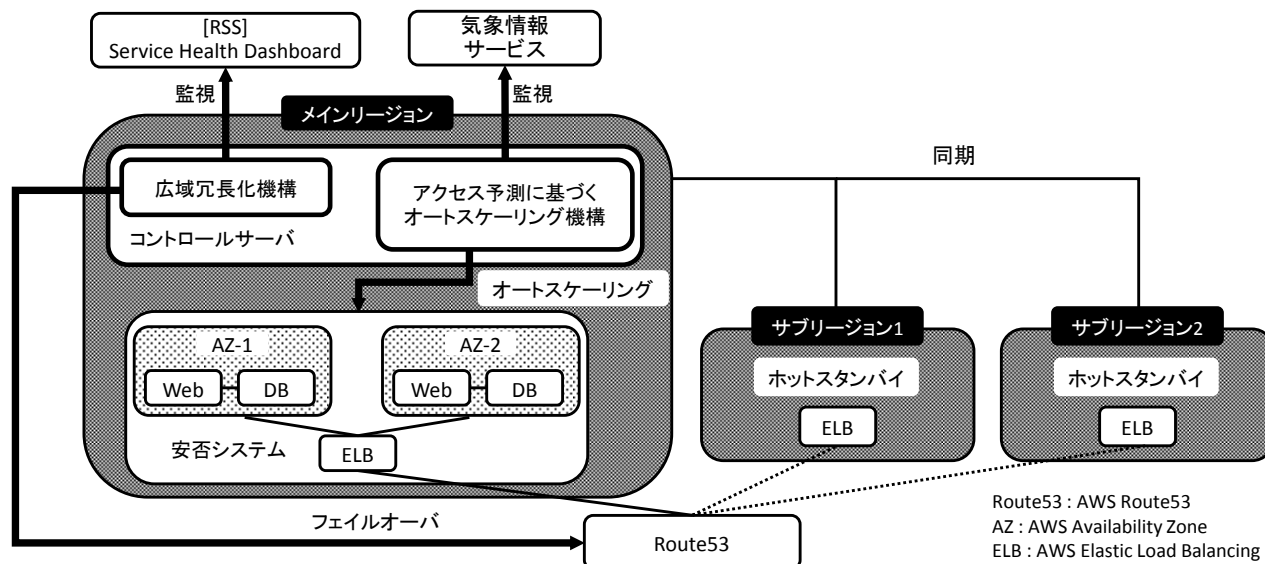


図 2 広域分散 WEB 安否情報システム

Fig. 2 Architecture of Global Distributed Web Safety Information System.

### 3. 提案システム

#### 3.1 システム概要

広域冗長型安否システム（以下、「提案システム」）は、システム基盤に AWS を用い、図 2 に示すようにメインリージョンとサブリージョンを有し、各リージョン内に安否システムとコントロールサーバで構成する。メインリージョンは主たるユーザから最も近接したリージョンであり、サブリージョンはメインリージョンから近接している順にサブリージョン 1, 2 となる。AWS がサービス展開している 11 リージョンのうち、メインリージョンを中心として位置的に離れているリージョンをサブリージョンに選択することで、近接地域に偏ることなく広域な冗長化が可能となる。サブリージョンは数が多いほどシステムの可用性が向上するが、本研究では広域冗長化の基礎評価のため 2 つのサブリージョンを用いた。システムが正常稼働中は、常にメインリージョンにアクセスが向けられ、サブリージョンはアクセスされずメインリージョンのバックアップサイトとしてホットスタンバイする。各リージョンには異なる地点に配置されているアベイラビリティゾーン（以下、「AZ」）があり、AZ は一般的なデータセンターと同意である。安否システムはリージョン内の 2 つの AZ に WEB・DB サーバ 1 台ずつ合計 WEB・DB サーバ 2 台ずつでシステムを構成し、リージョン内単体においても閉域冗長構成を敷く。

提案システムは、コントロールサーバ上に広域冗長化機構とアクセス予測に基づくオートスケーリング機構を有する。広域冗長化機構は障害等でシステム稼働が停止した際バックアップサイトにてシステム稼働を継続する。アクセス予測に基づくオートスケーリング機構は災害時のアクセス集中に対して適切なサーバ数にて負荷分散を行う。

#### 3.2 広域冗長化機構

広域冗長化機構は、メインリージョンが停止した場合、サブリージョンを新たなメインリージョンとしてフェイルオーバーを行う。フェイルオーバーは、AWS の障害状況サイト「Service Health Dashboard[13]」の監視から障害発生を起点に実行し、アクセス先をメインリージョンからサブリージョンに変更して実現する（図 3）。アクセス先リージョンの変更は AWS の DNS サービスである Route53[14]で行う。メインリージョンに障害が発生した場合は、Route53 を用いてアクセス先の重み付けを変更しサブリージョンにアクセスを向ける。新たにアクセスを受けるサブリージョンはメインリージョンに昇格し元のメインリージョンが復旧するまでその役目を果たす。サブリージョンの選択基準はアクセス地域から次に近接しているサブリージョンであるためメインリージョンは常にユーザから最近接のリージョンとなりアクセス速度向上も同時に実現する。

メインリージョンとサブリージョンのデータ同期は、DB サーバのレプリケーション機能を用いて行う。通常はメインリージョンにアクセスが向けられるため、メインリージョン AZ-1 の DB サーバがマスターとなり AZ-2 がスレーブとなる。同様にサブリージョンの DB サーバはメインリージョンのスレーブとなり広域間でデータを冗長保持する。

#### 3.3 アクセス予測に基づくオートスケーリング機構

アクセス予測に基づくオートスケーリング機構は、災害発生時、対象ユーザ数を基にアクセス数を予測し適切なサーバ数をスケールアウトし負荷分散を行う。サーバ数の増加をスケールアウト、削減をスケールインと呼ぶ。災害発生は、気象情報を電文形式で公開するサービス（例えば [15]）から検知する。負荷分散は、AWS のロードランシングサービスである ELB[16]内に、各 AZ の WEB サーバが同

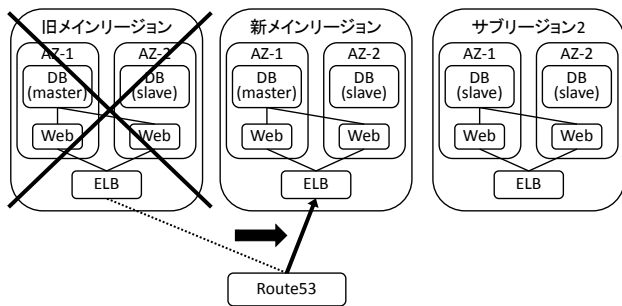


図 3 フェイルオーバー  
 Fig. 3 Failover.

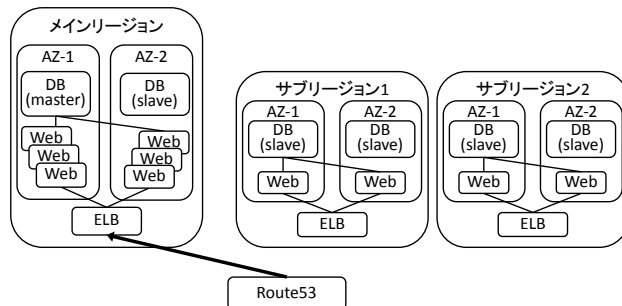


図 4 負荷分散  
 Fig. 4 Load Balancing.

表 1 スケールアウトのタイミング

Table 1 Scale out Timing.

	常時 配置	事後 追加	事前追加 (予測なし)	事前追加 (予測あり)
利便性	○	×	△	○
費用	×	○	○	○

数となるようスケールアウトし均等に実行する (図 4)。

WEB サーバをスケールアウトするタイミングは表 1 に示すように、サーバを平時から常に複数台配置する常時配置、アクセス集中後に追加する事後追加、アクセス集中前に追加する事前追加がある。常時配置はアクセスが少ない平常時では余剰リソースとなり高費用となる。アクセス集中後の事後追加は、システムが高負荷となった状態での対応のためレスポンス低下によるユーザ利便性を損ねる。アクセス予測なしの事前追加では、サーバ数算出に明確な根拠が無い場合リソース余剰もしくは不足の懸念がある。提案システムで用いるアクセス予測ありの事前追加では、アクセス予測を用いて必要サーバ数を算出するため、適切なリソース管理が可能である。また、提案システムで用いるサーバ AWS EC2[17]は、起動時間にて費用が積算されるため使用時のみのサーバ起動で費用削減が可能となる。つまり提案システムは、アクセス集中前の適切なサーバ数でのスケールアウトにより、利便性だけでなく費用面においても高い効果を期待できる。

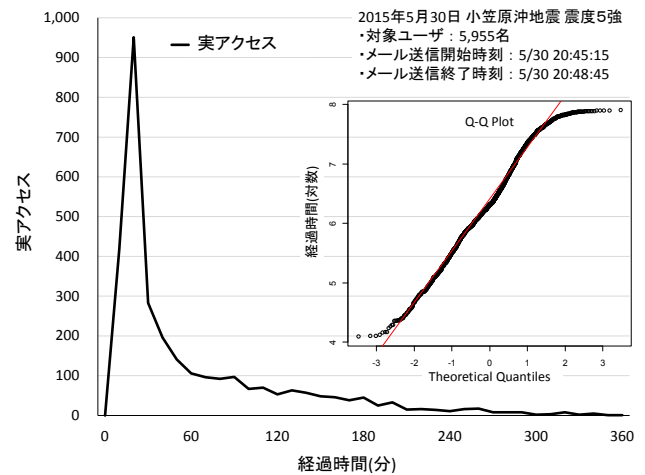


図 5 災害時のアクセス分布  
 Fig. 5 The access distribution of the disaster.

WEB システムへのリソース管理において、先行研究[18]はサーバ単体のベンチマーク結果からシステム全体のリソース管理のモデル化を試みている。本研究では先行研究を参考に、サーバ 1 台のアクセス許容量を把握し、予測で得られたアクセス数に対し 1 台の許容量から必要台数を見積もる。本研究で対象とする安否システムへの災害時の安否報告アクセスは、主に WEB サーバの CPU リソースを消費する。従ってサーバ 1 台の許容量はアクセス数に対して CPU 使用率の関係から算出する。本研究では EC2 タイプの t2 シリーズの内、t2.small を採用する。t2 シリーズは、CPU 使用率のベースラインが定められており CPU 使用率がベースラインを超えた場合バースト状態となる。t2 シリーズにおけるバーストとは一時的に CPU 性能が向上する状態であり、AWS の CPU クレジットを消費して継続可能となる。バースト状態ではベースラインを超えた CPU 使用が可能だが徐々に CPU クレジットを消費していきクレジットが尽きた場合、ベースライン以上の CPU 性能が発揮されない特性がある。本研究ではバースト状態でのアクセス許容量は考慮せず、t2.small のベースラインとして定められている CPU 使用率 20%までのアクセス許容量を 1 台のアクセス許容量とする。また、安否システムへの災害発生後のアクセス数は分単位で増減が見られるため、本研究ではアクセス予測を 10 分単位で行うことを想定し、アクセス許容量を 10 分単位で算出した。t2.small の CPU 使用率 20%時点でのアクセス許容量は約 200/10 分間であり、この値を基に必要台数を算出する。

## 4. アクセス予測モデル

### 4.1 安否システムのアクセス分布特性

アクセス予測モデルは、過去災害データの分析からアクセス傾向をモデル化し災害発生後、システムに対してのアクセス分布を予測する。アクセス分布の予測には過去災害

表 2 過去災害・訓練データ

Table 2 Data of the past disaster and training.

区分	対象組織, 災害	TU	M	E	AN <sub>max</sub>	D (E-M)	PR (AN <sub>max</sub> /TU)
訓練	教育機関 A	1,311	20	45	503	25	0.3836
訓練	教育機関 B	371	10	45	78	35	0.2102
訓練	教育機関 C	15,308	20	115	1,425	95	0.0930
訓練	企業 A	229	10	25	98	15	0.4279
訓練	企業 B	794	10	60	199	50	0.2506
訓練	企業 C	229	10	35	83	25	0.3624
訓練	企業 D	129	20	40	26	20	0.2015
災害	宮城県沖 (サーバ 1)	717	10	50	160	40	0.2231
災害	奄美大島近海 (サーバ 1)	565	10	30	149	20	0.2637
災害	奄美大島近海 (サーバ 2)	584	10	40	121	30	0.2071
災害	埼玉県北部 (サーバ 1)	510	20	40	70	20	0.1372
災害	埼玉県北部 (サーバ 2)	752	10	35	176	25	0.2340
災害	小笠原諸島 (サーバ 1)	1,740	20	50	303	30	0.1741
災害	小笠原諸島 (サーバ 2)	5,955	20	60	951	40	0.1596

時のアクセス分布特性の把握が必要である。図 5 は災害発生時の安否報告アクセス分布である。アクセス分布は WEB サーバに用いている Apache のログファイルから抽出した。図 5 からアクセス分布はシステムからのメール送信を起点 (0 分時) とし, しばらくしてピークを迎え時間経過とともに減衰する。ある動作を起点としたシステムへのアクセス分布に対し先行研究[19]では正規分布を仮定している。また[20]ではネットワークのトラフィック分布に対し対数正規分布を用いて解析を試みている。本研究では図 5 の形状からメール送信を起点とした安否システムへのアクセス分布は対数正規分布に従うと仮定した。アクセス時間の対数を取った値で Q-Q プロットしたものが図 5 の Q-Q Plot である。アクセス分布は集計時間単位が短いほど対数正規分布の傾向がより顕著なため, ここでは 1 秒単位で集計した。Q-Q Plot から経過時間における安否報告アクセス分布の大部分が対数正規分布に従っている。先行研究[21]では, HTTP におけるサービス時間分布に対して対数正規分布を用いたモデル化や, [22]ではサーバへの実アクセス分布に対数正規分布を用いており, 本研究においても安否システムへのアクセス分布予測に対数正規分布を用いた。

#### 4.2 対数正規分布を用いたアクセス予測モデルの構築

安否報告アクセスの分布を予測するため, 対数正規分布の確率密度関数に必要なパラメータ決定について明らかにする。対数正規分布の定義式は, 確率密度関数  $f(x)$  は式(1), 最頻値  $M$  は式(2), 平均値  $E$  は式(3)となる。  $\mu$  は正規分布の平均値,  $\sigma$  は正規分布の標準偏差である。式(1)の確率密度関数に対してパラメータ  $\mu$ ,  $\sigma$  を与え確率変数  $x$  (分) の関数としてアクセス分布の確率を求める。  $\mu$ ,  $\sigma$  は, 式(2), 式(3)を連立して解くと式(4), 式(5)となる。式(4), 式(5)へ最頻値  $M$  と平均値  $E$  を与えることで  $\mu$ ,  $\sigma$  が決定で

$$f(x) = \frac{1}{x\sqrt{2\pi}\sigma} \exp\left(-\frac{(\ln x - \mu)^2}{2\sigma^2}\right) \quad (1)$$

$$M = \exp(\mu - \sigma^2) \quad (2)$$

$$E = \exp\left(\mu + \frac{\sigma^2}{2}\right) \quad (3)$$

$$\mu = \frac{(\ln(M) + 2 * \ln(E))}{3} \quad (4)$$

$$\sigma^2 = \frac{2 * (\ln(E) - \ln(M))}{3} \quad (5)$$

$$E = M + 4.6039 * TU^{0.2802} \quad (6)$$

$$AN = A * f(x) \quad (7)$$

きる。次に災害発生時その災害に対しての最頻値  $M$  と平均値  $E$  の算出方法を示す。

最頻値  $M$  はアクセスが最も多い時間であり, 平均値  $E$  は平均アクセス数の時間となる。最頻値  $M$  と平均値  $E$  は過去災害の対象ユーザ数 ( $TU$ ) と災害発生後のアクセス分布を分析し算出する。表 2 は過去の災害・訓練時のアクセスデータを 10 分間隔で集計したものであり, 各パラメータを求めるための分析対象データである。最頻値  $M$  は表 2 から災害及び訓練の対象ユーザ数  $TU$  によらず 20 分以下でピークを迎えている。従って今回構築するモデルでは最頻値  $M$  を固定値 20 とする。平均値  $E$  は, アクセスが開始された時間からアクセス数が 1 桁台になる時間までのアクセス数

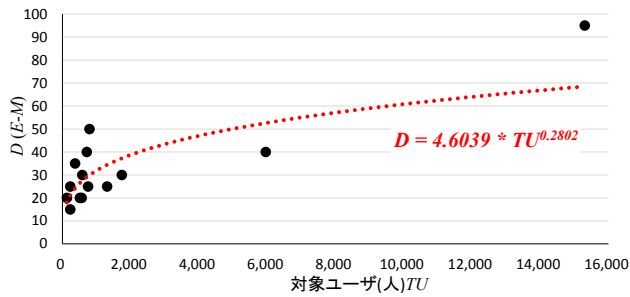


図 6 TU と D (E-M) の関係

Fig. 6 Relationship between TU and D(E-M).

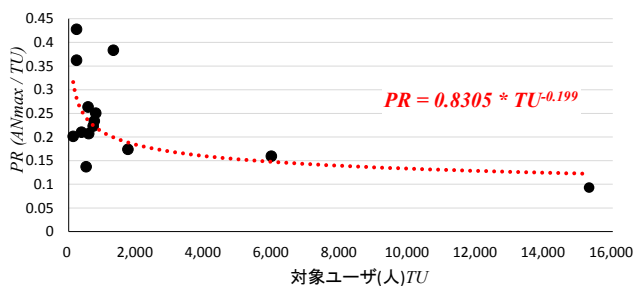


図 7 TU と PR (ANmax/TU) の関係

Fig. 7 Relationship between TU and PR(ANmax/TU).

の平均値を取り、その平均値のアクセスがあった時間とする。表 2 から平均値  $E$  は、対象ユーザ数  $TU$  に影響を受けない最頻値  $M$  に対して、対象ユーザ数  $TU$  に応じて値に開きがある。図 6 は対象ユーザ数  $TU$  と平均値  $E$  から最頻値  $M$  を引いた差 ( $D$ ) の関係であり図 6 の近似式を用いて対象ユーザ数  $TU$  から  $D$  を求める。 $D$  は平均値  $E$  から最頻値  $M$  を引いた差なので平均値  $E$  は式(6)で求める。これまでで、災害発生時その災害の対象ユーザ数  $TU$  を基に最頻値  $M$  と平均値  $E$  を推定できる。また求めた最頻値  $M$  と平均値  $E$  を式(4)、式(5)に代入すると  $\mu$  と  $\sigma$  が決定し、同時に式(1)の確率密度関数のパラメータが決まる。

次に対数正規分布のグラフ形状を決定するために式(1)に付与する係数  $A$  を算出する。 $A$  は式(1)を対象ユーザ数  $TU$  に応じたピークアクセス数に合わせるための係数であり、式(7)が  $x$  分時のアクセス数  $AN$  を予測するアクセス予測モデルとなる。係数  $A$  は式(7)の  $x$  に最頻値  $M$  を代入し、 $AN$  がピークアクセス数 ( $AN_{max}$ ) となるよう求める。表 2 からピークアクセス数  $AN_{max}$  は対象ユーザ数  $TU$  が増加するほど対象ユーザ数  $TU$  に対する割合が減少 ( $PR$ ) していく傾向にあり図 7 の関係となる。図 7 の近似式にて対象ユーザ数  $TU$  からピークアクセス数  $AN_{max}$  を求める。例として、アクセス予測モデル式(7)を用いて対象ユーザ数 20,000 人でのアクセス分布を予測すると図 8 の各パラメータおよびアクセス分布曲線となる。各時間の予測アクセス分布に対して許容可能なサーバ数を割当ててことでアクセス数に応じた負荷分散を行う。

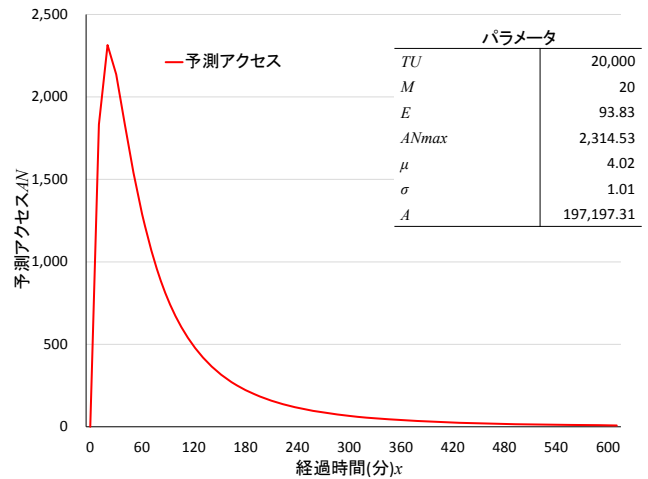


図 8 ユーザ数 20,000 名でのアクセス分布予測

Fig. 8 The access distribution prediction of the 20,000 Users.

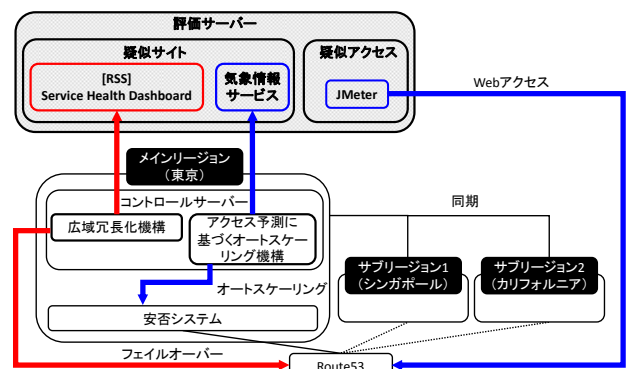


図 9 評価構成

Fig. 9 Evaluation Constitution.

## 5. 実装と評価

### 5.1 実装

本研究では実装した提案システムに対して疑似ユーザアクセスを行う評価サーバを用いて挙動を評価した。構築した提案システムと評価サーバの構成を図 9、システム環境を表 3 に示す。図 9 から提案システムには 3 つのリージョンを用い日本をメインリージョン、シンガポールをサブリージョン 1、カリフォルニアをサブリージョン 2 とした。フェイルオーバーやオートスケーリングは表 4 の AWS API を用いて実装し、アクセス予測モデルの計算は PHP の Math 関数にて実装した。評価サーバには、Service Health Dashboard の RSS と気象情報サービスの疑似サイトおよび、負荷分散評価のために JMeter を用いた疑似アクセス環境を実装した。JMeter とは WEB サーバに対し複数のリクエストを送信し負荷を掛けることができるツールである。

### 5.2 広域冗長化機構に関する評価

広域冗長化機構の評価では、評価サイトにメインリージョンである日本に障害が発生した情報を配信し、フェイルオーバーの動作を確認した。本研究ではアクセス予測に基づ



表 3 システム環境

Table 3 System Environment.

	Hardware	Software
WEB	EC2 t2.small	CentOS 6.4 Apache 2.2.15
DB	EC2 c3.2xlarge	CentOS 6.4 PostgreSQL 8.4.12
コントロールサーバ	EC2 t2.micro	CentOS 6.4 PHP 5.3.3
評価サーバ	EC2 m3.medium	Windows Server 2008 JMeter 2.13

表 4 AWS API

Table 4 AWS API

EC2 操作	ec2-api-tools 1.6.7
スケールアウト・イン	AutoScaling CLI 1.0.61
DNS 操作	Route 53 Authentication Tool for Curl(dnscurl.pl)

くオートスケーリング機構のアクセス予測モデルに焦点を絞っているため、広域冗長化機構の実験詳細や考察は省略し結果のみ述べる。フェイルオーバーの動作確認として、評価サイトに障害発生情報発信後、Route53にてメインリージョンの重みを0としサブリージョン1の重みを1に設定し、約70秒後にアクセス先が新たなメインリージョンであるシンガポールになることを確認した。また、フェイルオーバー時、リージョン間のデータ同期も問題なく実施されていることを確認した。

### 5.3 アクセス予測に基づくオートスケーリング機構に関する評価

#### 5.3.1 アクセス予測モデルでのサーバ数算出

実災害のアクセス分布に対してアクセス予測モデルを用いてサーバ数を算出した。図10は2015年5月13日に発生した宮城県沖地震の実際のアクセス分布と、対象ユーザ数4,828名に対してアクセス予測モデルを用いて算出した10分単位の予測アクセス分布である。EC2は1時間単位で課金されるため1時間単位のアクセス数に対して適切なサーバ数を求める。図10の0~60分の間では最高741/10分間アクセスが予測される。t2.smallは200/10分間のアクセス許容能力があるため、t2.smallを各AZに2台ずつ合計4台で負荷分散を行う。ここで0~60分の間で実アクセスとモデルにわずかに差があるが、t2.smallの単体の許容能力内もしくは負荷分散に用いる合計台数の許容能力内でこの差を吸収可能なため、モデルの精度としては妥当だと考える。次の60~120分間では最高358アクセスが予測されるため、各AZに1台ずつ合計2台で負荷分散を行う。以上のように1時間単位の予測アクセス分布に対してサーバの許容量

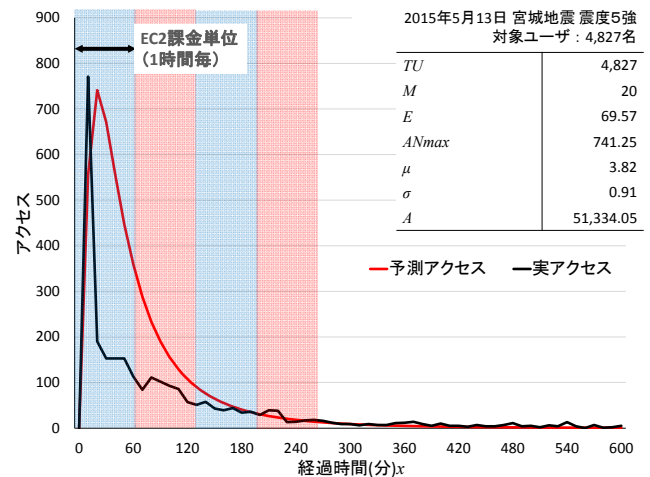


図 10 実災害とアクセス予測モデルの分布

Fig. 10 Distribution of Disaster and Access Prediction Model.

を基にサーバ数を算出する。また予期せぬ事態の発生で実アクセスが予測を上回った事態を考慮し、t2.smallのCPU使用率が20%超となった場合は、アクセス予測モデルとは別にサーバを追加し負荷分散を実施する。

#### 5.3.2 シミュレーション評価

実災害のアクセスに対して負荷分散のシミュレーション評価をした。評価内容は、図10の実災害アクセスを基にJMeterにてテストシナリオを作成し、評価サーバから提案システムへ実行した。図10では発生から1時間単位の最高アクセスは、0~60分間で771/10分間アクセス、60~120分間で111/10分間アクセス、120~180分間で58アクセスとなっており、テストシナリオは各時間帯の最高アクセスを1時間継続するよう作成する。このテストシナリオは各時間帯で実災害と同数の最高アクセスを継続する疑似アクセスとなるため、実災害アクセスのシミュレーション評価が可能となる。図10のパラメータをアクセス予測モデルに与えテストシナリオを実行した結果、対象ユーザ4,827名の実災害に対して、0~60分間ではt2.smallを2台スケールアウトし合計4台、60~120分間では2台スケールインし合計2台、120~180分間では標準構成の合計2台で負荷分散を確認した。負荷分散中の各サーバのCPU使用率は、t2.smallの許容値である20%以下を推移し、想定通りのCPU使用率で負荷分散実行を確認した。

次に、筆者が所属する企業でサービス提供している安否システムの顧客20,000名に対して、シミュレーション評価をした(図11)。図11から対象ユーザ20,000名では、0~60分間ではt2.small12台、60~120分間では8台、120~180分間では4台と、図10の対象ユーザ4,827名と比較しより大規模なスケールアウト・インとなる。つまり対象ユーザ数が増加するほどオートスケーリングの規模が大きくなるため、対象ユーザ数増加に伴い費用対効果向上が期待できる。

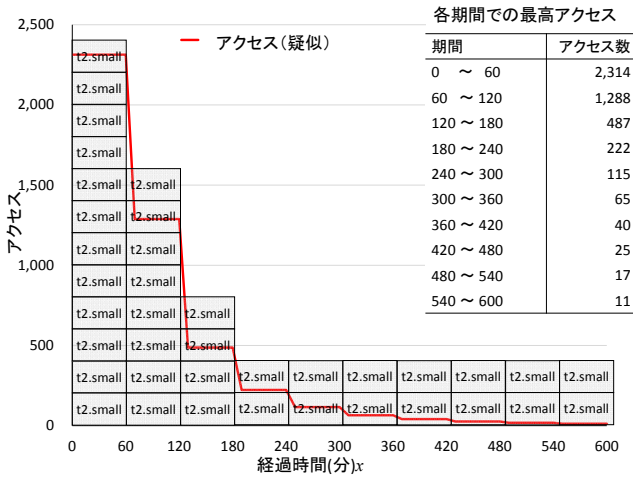


図 11 20,000 名ユーザでのオートスケーリング  
 Fig. 11 AutoScaling of the 20,000 Users.

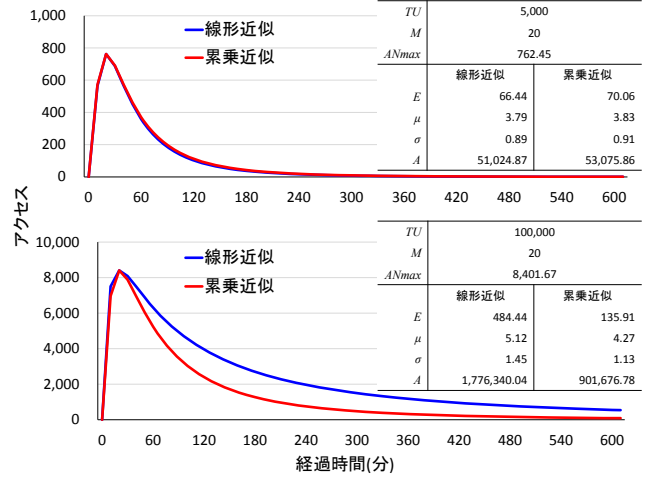


図 12 線形近似と累乗近似  
 Fig. 12 Linear approximation and Power approximation.

## 6. 考察

### 6.1 対数正規分布の仮定

災害発生後の安否システムへのアクセス分布は図 5 から対数正規分布に従うと仮定した。対数正規分布への仮定の背景は、図 5 のアクセス分布が Q-Q プロットにおいてほぼ直線に乗るためであるが、シャピロ-ウィルクでの正規性検定では P 値は 0.05 以下となり正規性があるとは言えない。ここで図 5 の Q-Q プロットが直線から外れるのは 7.6 付近からとなる。7.6 はアクセス時間の対数を取った値なので  $Exp(7.6) \approx 2,000$  (秒) となり災害発生後約 30 分後となる。図 5 の災害では発生から 30 分後ではアクセスが少なくなっており、アクセス予測モデルでのオートスケーリングを行うことなく標準構成のサーバ数でアクセスを許容可能である。つまり災害発生後、システムへのアクセス分布は最繁忙期間において対数正規分布に従っており、この期間において適切にアクセス予測ができれば安否システムにおける災害時の負荷分散は問題ないと考える。以上が厳密な正規性ではないものの対数正規分布を基にアクセス予測モデルを構築した理由である。また現状の調査では対象ユーザ数が多いほどアクセス分布が Q-Q プロットにおいて直線になる傾向があり、例えば数万名規模であれば正規性が認められる可能性がある。対象ユーザ数が多いほど対数正規分布に近づけばアクセス予測モデルの精度を向上でき、さらに適切なサーバ数算出が期待できる。

### 6.2 平均値 E の決定

アクセス予測モデル構築過程において平均値 E は、対象ユーザ数 TU と D (平均値 E と最頻値 M の差) の関係 (図 6) から近似式にて決定した。ここで採用した近似式は累乗近似である。一方、対象ユーザ数 TU と D が線形的な関係であれば線形近似も考えられる。図 6 の両者の相関係数は  $R=0.77$  となり高い相関があった。図 12 は対象ユーザ数 5,000 名と 100,000 名で、累乗近似および線形近似を用いて

平均値 E を算出した場合の予測アクセス分布である。5,000 名では累乗近似と線形近似に目立った差はないが、100,000 名では線形近似のほうがピークからの減衰が緩やかであり、対象ユーザ数が多いほどこの傾向は顕著になる。この結果だけ考えれば対象ユーザ数に閾値を設定し累乗近似もしくは線形近似を選択することは可能だが、現状のデータ量では両者の挙動差に対する根拠に乏しいため現時点での断定は避けたい。またサーバ数算出であれば線形近似のほうが台数削減は緩やかになりシステムリソースに余裕が生まれ安定性が向上するが、過剰な余裕は費用向上にも繋がるため安定性と費用面を考慮した上で線形近似もしくは累乗近似を選択しなければならない。両者の挙動を明らかにするために今後のデータ収集及び分析が必要である。

### 6.3 運用費用

現在サービス提供中の 20,000 名ユーザに対して現システムと提案システムでの 1 年間の稼働費用比較を行った。使用する EC2 タイプ、費用は表 5 に示すように現システムでは過去災害のアクセス結果から余裕のある c3.2xlarge を採用しており、費用は t2.small の 10 倍以上となる。提案システムを用いることにより表 6 に示すように適切なサーバ数運用が可能となり、表 7 が表 6 の構成での年間費用となる。表 7 から現システムと比較し提案システムでは、合計年間費用の 32.22%削減、WEB サーバのみの場合は 64.44%の削減が見込める。20,000 名ユーザの地震 1 回に対するオートスケーリングでの対処費用は、図 11 から 0~180 分間の 3 時間で t2.small を標準構成 2 台に 18 台追加した費用であり、\$1.83 (18 台\*\$0.034\*3 時間) となる。仮に年間 10 回災害が発生した場合、\$18.3 の費用で対処可能となり、提案システムの運用費用に加算しても現システムと比較し大幅に費用を削減できる。また今回は採用 EC2 タイプを t2.small に限定したが、各タイプの性能特性や費用を考慮すれば、さらに精度の高い負荷分散や費用効果が期待できる。



表 5 c3.2xlarge と t2.small の稼働費用

Table 5 c3.2xlarge,t2.small Cost

タイプ	1時間 (\$)	月間 (\$)	年間 (\$)
c3.2xlarge	0.478	355.63	4,267.58
t2.small	0.034	25.29	303.55

表 6 現システムと提案システムのサーバ構成

Table 6 Present System, Proposal System Server Composition

	現システム	提案システム
メイン	WEB:c3.2xlarge 2台 DB:c3.2xlarge 2台	WEB:t2.small 2台 DB:c3.2xlarge 2台
サブ1	—	WEB:t2.small 2台 DB:t2.small 2台
サブ2	—	WEB:t2.small 2台 DB:t2.small 2台

表 7 現システムと提案システムの年間稼働費用

Table 7 Present System, Proposal System, 1 year cost.

用途	現システム (\$)	提案システム (\$)
WEB	8,535	3,035
DB	8,535	8,535
合計	17,070	11,570

## 7. まとめ

本研究では WEB システムを構成するサーバ群を世界規模で冗長化し、災害時のアクセス数を事前予測し適切なサーバ数にて負荷分散を行う広域冗長型安否システムを提案し評価結果から有効性を示した。過去災害のアクセスデータに対して対数正規分布を仮定したアクセス予測モデルでは、過去災害データに厳密な正規性は見られないもののアクセス減衰期までは対数正規分布に従っており、実運用時のサーバ数算出において期待した効果を得られた。

今後の課題として、アクセス予測モデルの精度向上が挙げられる。本研究ではアクセス予測モデル構築の概念と基礎評価に対して一定の効果が認められたが、モデル構築の際に分析した実災害データが乏しいためモデル妥当性の根拠も同様に乏しい。今後はより多くの実災害データを収集しモデル精度向上および修正を行う予定である。また今回は対象ユーザ数のみのアクセス予測を行ったが災害時のその他の要素（発生時刻、対象組織の特性など）がアクセス分布に及ぼす影響を調査する予定である。

## 参考文献

- 1) 長谷川孝博, 井上春樹, 八巻直一: 低コスト運用でユーザフレンドリな安否情報システムの開発, 学術情報処理研究誌, No.13, pp.91-98 (2009).
- 2) 梶田将司, 太田芳博, 若松進, 林能成, 間瀬健二: 高等教育機

- 3) 白井真人, 畑山満則, 福山薫: 地域コミュニティでの情報システムを用いた安否確認に関する研究, 地域安全学会論文集, No.16, pp.11-20 (2012).
- 4) 白鳥則郎, 稲葉勉, 中村直毅, 菅沼拓夫: 災害に強いグリーン指向ネバーダイ・ネットワーク, 情報処理学会論文誌, Vol.53, No.7, pp.1821-1831 (2012).
- 5) 西谷薫, 杉浦彰彦: ワンセグ用データ放送を用いた災害時安否情報配信, 情報処理学会論文誌, Vol.50, No.2, pp.839-845 (2009).
- 6) 大瀧龍, 重安哲也, 浦上美佐子, 松野浩嗣: 自律的無線ネットワークを用いた被災情報提供システム—被災地域の地形を考慮した無線ノード置局アルゴリズムの提案, 情報処理学会論文誌, Vol.52, No.1, pp.308-318 (2011).
- 7) 小山由, 水本旭洋, 今津眞也, 安本慶一: 大規模災害時の安否確認システムと広域無線網利用可能エリアへの DTN に基づいたメッセージ中継法, 情報処理学会研究報告, 2012-MBL-62, No.29, pp.1-7 (2012).
- 8) 東田光裕, 林春男, 松下靖, 三宅康一: 社会サービスとしての被災者対応の質を向上させる情報マネージメントシステムの構築—QR コードを利用した安否情報収集システムの開発, 地域安全学会論文集, No.9, pp.147-156 (2007).
- 9) 越後博之, 湯瀬裕昭, 干川剛史, 沢野伸浩, 高畑一夫, 柴田義孝: 大規模分散環境におけるロバストネスを考慮した広域災害情報共有システム, 情報処理学会論文誌, Vol.48, No.7, pp.2340-2350 (2007).
- 10) 太田芳博, 梶田将司, 林能成, 若松進: 名古屋大学安否確認システムの構築と運用, 電子情報通信学会技術研究報告, IA Vol.108, No.409, pp.77-82 (2009).
- 11) Amazon Web Services(online), from <http://aws.amazon.com/> (accessed 2015-8-30)
- 12) Microsoft Azure(online), from <http://azure.microsoft.com/> (accessed 2015-8-30)
- 13) Service Health Dashboard(online), from <http://status.aws.amazon.com/> (accessed 2015-8-30)
- 14) Route53, Amazon Web Services(online), from <http://aws.amazon.com/route53/> (accessed 2015-8-30)
- 15) 一般財団法人 気象業務支援センター, from <http://www.jmbc.or.jp/> (accessed 2015-8-30)
- 16) Elastic Load Balancing, Amazon Web Services(online), from <http://aws.amazon.com/elasticloadbalancing/> (accessed 2015-8-30)
- 17) EC2, Amazon Web Services(online), from <http://aws.amazon.com/ec2/> (accessed 2015-8-30)
- 18) 藤田靖征, 村田正幸, 宮原秀夫: Web サーバシステムのモデル化と性能評価, 電子情報通信学会論文誌 B, Vol.J82-B, No.3, pp.347-357 (1999).
- 19) 石原進, 岡田稔, 岩田晃, 櫻井佳一: イベント駆動方式による LAN 通信量解析モデル, 電子情報通信学会論文誌 A, Vol.J78-1, No.8, pp.961-964 (1995).
- 20) Antoniou, I., Ivanov, V.V., Ivanov, V.V., Zrellov, P.V.: On the log-normal distribution of network traffic, Physica D: Nonlinear Phenomena, Vol.167(1), pp.72-85 (2002).
- 21) Murta, C.D., Dutra, G.N.: Modeling HTTP service times, In Global Telecommunications Conference, GLOBECOM'04, IEEE Vol.2, pp.972-976 (2004).
- 22) 稗圃泰彦, 上村郷志, 小頭秀行, 中村元: 一斉報知を用いた遅延発呼制御方式におけるサーバ同時接続数の安定化に関する一考察, 電子情報通信学会論文誌 B, Vol.J95-B, No.3, pp.414-424 (2012).