普通論文

IP電話におけるスパム(SPIT)防止法

ユールゲン クイテク・サベーリオ ニッコリーニ
サンドラ タルタレルリ・リナン シュレゲル

要　旨

近い将来、IP電話におけるスパム(SPIT)が深刻な問題になると予想されています。しかも、SPITの場合、電話がかかってくるたびに受信者が煩わされるため、電子メールのスパムよりもさらに重大な問題となる可能性を秘めています。本稿では、効果的で、なおかつ通話参加者が容認可能な、新しいSPIT防止法について説明します。この防止法は、受信者にはまったく影響を及ぼさず、発信者との必要なやりとりも許容可能なほど最小限に留めています。

キーワード

●スパム　● VoIP　●インターネット電話　● SPIT

1. はじめに

スパムとは、勝手に送り付けられる大量の迷惑メールのことであり、インターネットにおけるこれまでの重大問題のひとつであると考えられます。そして、Voice over IP(VoIP)と呼ばれるインターネット電話ソリューションにおいても、導入が進むにつれて、同じような形式のスパムがこの分野にも影響を及ぼすのではないかという危惧が一般的になりつつあります。この脅威はSPIT(SPam over Internet Telephony)と呼ばれ、インターネット電話経由で、必要のない通話発信を勝手に行うことを意味します。

SPITによる生産性低下の可能性は、電子メールのスパムの場合よりもはるかに大きなものです。なぜなら、SPITによる通話発信があるたびに、時を選ばず電話がかかってしまうことになり、受信者が迷惑を被るからです。VoIPの普及を確実にするためには、効果的な予防措置を講じることがきわめて重要です。公衆ネットワークおよび公衆ネットワークと企業ネットワーク間のゲートウェイにおいては、なおさらです。

必要のない通話発信は、既存の公衆交換電話網(PSTN)にもすでに存在しており、そういった通話の大半はテレマーケター(電話を使って販売活動を行う人々)によるものです。しかし、電子メールやVoIP通信と比較してコストのかかるPSTN通話では、発信者側にとってこのような形の広告への魅力はあまりありません。これに対して、インターネット電話を用いたスパムは、発信者側のコストを大幅に削減することができます。最近の研究[1)]には、従来のPSTNを用いたテレマーケターによる通話よりも、SPITの方がおよそ3桁も安価に送信できるという報告があります。

残念なことに、SPITの性質は電子メールのスパムとは大分異なり、同じようなスパム防止策を用いても、SPITに対しては有効な手段とはなり得ません。受信者が着信音に煩わされる前に、SPITの内容を確認することはできないからです。

本稿では、典型的な音声通信パターンに基づいて、SPIT通話を識別する画期的な手法を提案します。しかし、電子メールのスパムと同様、単一の手法では、SPITの攻撃を完全に防止するには十分であるとは言えません。したがって、本稿では、様々なSPIT防止法を柔軟に統合できる、普遍的なSPIT防止システムのアーキテクチャを紹介します。これにより、SPIT防止システムによってもたらされる音声通話の発信者および受信者に対する不都合を最小限に留めつつ、必要な通話のみを受信者に到達させるという点では最大限の実効性を発揮します。

2. 従来のスパムとSPITの比較

常にユーザを煩わせるSPITは、電子メールのスパムよりも大きな脅威です。SPIT通話はただちに呼び出し音が鳴ることになり、受信者を煩わせます。電子メールのスパムは、受信するユーザの電子メール・プログラムによって順次蓄えられるため、ユーザが見るまでは煩わしい問題とはなりません。また、メールをチェックする際にも、ユーザは大量のメールを短時間で処理し、大した注意を払うことなく素早くスパムであることを識別することができます。SPIT通話による煩わしさは長時間にわたって繰り返されます。

インターネット電話のプロトコルおよびシステムには不十分なID管理機能しか備わっていないため(電子メール・システム

にも同様の技術的課題が存在します)、SPITを送信することは技術的には難しくありません。

SPITに関しては、さらに問題があります。それは、もっとも広く利用されている(電子メールのスパム防止法に由来する)技術が有効ではないという点です。その理由を以下に示します。

・時間的尺度がまったく異なっている(電子メールはリアルタイムではないが、インターネット電話による通話はリアルタイムの通信である)

・もっとも有効な防止法の1つ(具体的には、コンテンツ・フィルタリング)を適用することができない。つまり、コンテンツを受信するには電話に応答する必要がある。また、音声認識に基づく自動方式は、現在のところ、VoIP通話に実装するには複雑すぎ、言語に対する依存性も高い。

上記の簡単な考察は、SPITによる潜在的な脅威の概要を示しているにすぎませんが、将来的には、SPITが本格化するおそれがあります。その理由は、PSTNに代わり、インターネット電話を利用することによって発生する、SPIT発信者のコストの削減です。PSTN、および公衆インターネットを使用した場合に発生する通話コストの差を示す簡単なコスト分析があります。PSTNのスパムとインターネット電話のスパムにかかるコストの差を予測するには、以下に示すように3つの要素があります。

・ソフトウェアに関するシステムのコスト

・ハードウェアに関するシステムのコスト

・スパム通話一件ごとにかかるコスト

ソフトウェアに関するシステムのコストについては、基本的に、2つの音声スパムに違いはありません(ソフトウェアは基本的には同一であり、ネットワークに接続するために必要なハードウェアのみが異なります)。ハードウェアに関するシステムのコストについては、明らかにPSTNのスパム発信者が不利です(PSTN用カードはネットワーク・インタフェース・カードに比べはるかに高価です)。スパム通話一件ごとのコストに関しては、PSTN接続の方がコストが高く、PSTNを用いてスパムを送信するシステムが不利です。大まかな分析によると、SPITシステムにかかるコストの方が3桁低くなっています。

表1　音声通話スパム・システムのコスト比較の概要

コスト	PSTN のスパム	SPIT	追加事項
ソフトウェア・コスト	X	X	X はシグナリング・プロトコルに依存する。
ハードウェア・コスト	10Y - 100Y	Y	Y はシグナリング・プロトコルに依存しない。
一通話あたりのコスト	約 1000Z	Z	Z はシグナリング・プロトコルに依存しない。

表1はコスト比較の概要であり、SPITシステムが、テレマーケターにコスト削減をもたらすことが明確に表れています。

3. 普遍的なSPIT防止システム・アーキテクチャ

SPIT防止システムが有効であるとされるためには、以下に示す基本的な必要条件をいくつか満足させる必要があります。

・正規の通話を遮断してしまう可能性を最小限に抑える

・SPIT通話を遮断する確率を最大限に引き上げる

・通話がSPITであるか否かを受信者に判断させるための作業を最小限に抑える

・正規の通話を行う発信者の不便さを抑える

・様々な環境(オフィス、家庭等)、文化、言語などに適用できるほどの普遍性を備えている

SPIT通話を防止するための手法はいくつか提案されています。しかし、上記の必要条件をすべて満足させるものはありません。もっとも効果的なSPIT防止法は、発信者とのやりとりを必要とする、非常に「イントルーシブ(邪魔)」なものです。しかし、発信者が通話を控える可能性はありますが、受信者が重要な通話を逃してしまう可能性もあります。さらに他の手法では、受信者からのフィードバックが不可欠となっているものもあります。したがって、効果的なSPIT防止システムとは、その構成要素となる様々な防止法の能力を組み合わせた結果として、発信者および受信者とのやりとりを必要最小限に抑えつつ、効果的にSPIT通話を遮断できるシステムなのです。

また、行動を起こす側である発信者は、受信者と比較した場合、システムの不便さへの寛容の度合いが高いものと考えられます。そのため、我々は、受信者からのフィードバックを求める方式よりも、発信者の関与を必要とする方式の方が、途中に入るシステムによる介在を少なくすることができると考えています。

上記の前提に基づき、本稿では、5つのステージで構成され、ステージが高まるほどシステムによる介在が増大するSPIT防止法の分類体系を含む、SPIT防止システムのための普遍的なアーキテクチャを提案します。**図1**をご覧ください。

第1ステージでは、発信者も、受信者も、防止システムが動作していることに気付きません。第2ステージでは、防止システムが、発信者と、あるいは少なくとも発信者の端末と交信します。第3ステージでは、通話が成立する前に受信者からのフィードバックが必要となります。第4ステージでは、通話が行われている間に、これらの手法を適用し、通話の検査を実行します。最後の第5ステージでは、通話終了後に受信者から

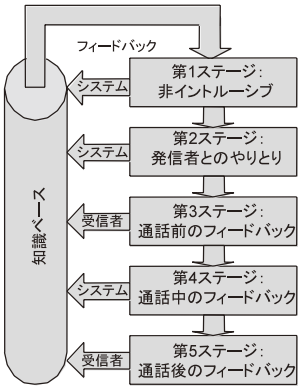

図1　普遍的なSPIT防止システムのアーキテクチャ

フィードバックが行われ、そのフィードバックが以降のSPIT遮断のために活用されます。

すべてのステージにおいて、各ステージ固有の自動化されたメカニズム、あるいは受信者がSPIT防止システムにフィードバックを行うようになっています。必要とする知識は、第1ステージの項目のいくつかに入力を行うといった程度のものです。

なお、かかってきたすべての通話が全ステージを通過するわけではありません。たとえば、第1ステージで、正規の通話であることがすでに確認された通話は、それ以上は管理下に置く必要がないので、直ちに通話が成立し、第4ステージへと進みます。一般的に、通話がたどる経路は各実装における固有の要素、たとえば、システムが許容するイントルーシブ性、つまり「システムの介在」のレベルなどによって左右されます。

次章では、各ステージで用いられる手法を説明しますが、一般的に、上位のステージになるほど、有効性は高まり、本質的には「システムの介在」の度合いも増大するという事実が示されています。我々が想定している、きわめて優れたSPIT防止システムとは、イントルーシブ性と有効性のバランスに優れ、複数の方式によって構成された、すべてのステージを対象とするシステムです。

4. SPIT防止システムの構成要素

SPIT防止システムの構成要素の候補としては、いくつかの手法が検討の段階にあります。詳細については、1) および、その参考文献をご参照ください。本章では、既知の手法について概要を説明します。

本章では、各手法を、図1の、それぞれ適用可能なステージに対してマッピングします。各手法については、概略に加えて、当該モジュールに対する前提条件(例:インフラストラクチャ、標準化の動き等)がすでに存在しているか否か、近い将来に達成することが現実的であるか否か、といったコメントを添えています。また、各モジュールを実装するにあたっての難易度に関しても、大まかな評価を提供しています。

4.1 第1ステージ:発信者・受信者との通信

この手法は、発信者との通信を必要とせず、発信者はその存在をまったく認識できません。**表2**に詳細を説明します。

4.2 第2ステージ:発信者とのやりとり

この手法は、発信者の端末(Computational Puzzles、Sender Checksの場合)、あるいは発信者(Turing Testの場合)との通信が必要です。**表3**に詳細を説明します。

4.3 第3ステージ:受信者とのやりとり

この手法は、若干ですが、SPIT通話の着信に際して受信者の対応を必要とします。**表4**に詳細を説明します。

表2　第1ステージ・モジュールの詳細

第1ステージ・モジュール	詳細
Lists（リスト）	発信者のIDを、蓄積している一連のIDと比較して、着信を受諾するか拒否するかを決定する。リストとしては、ホワイトとブラックの2種類が考えられる。ホワイト・リストには通話を許されたIDを、ブラック・リストには通話を拒否するIDを記載する。このような方法論に関しては、関連技術が発達しており、実装も容易なため、実装に伴う障害はない。
Circles of trust（信頼の輪）	対象となる受信者に通話を転送する前に、ドメイン間通信の信頼性を確認する。各ドメインが、自身のユーザの管理を行い、SPITやスパムを相互に送信しないことを承諾することが理論的根拠となる。このような方法論に関しては、関連技術が発達しており、現在標準化作業の対象となっているため、実装自体の複雑さについては中程度である。
Pattern/Anomaly detection（パターン／変則性検出）	この手法では、SPIT通話を識別するために、トラフィック内の不審なパターンの検出を試みる。不審なパターンの定義は、決定論的な規則、あるいは統計的な規則を用いて行われる。関連技術は発達しているが、音声通話への適用例がないため、実装自体の複雑さについては中程度である。
Greylisting（グレイリスト作成）	PMG（Progressive Multi Grey-leveling）と呼ばれるこの手法は、通話を監視し、各通話に対してグレイ・レベルに関する属性を与える。発信側が特定範囲の時間内に発信を繰り返すと、グレイ・レベルは増大し、発信側が発信を中止すればグレイ・レベルは徐々に低下する。このような方法論に関しては、他の研究機関[3]がすでに実装を行っており、実装自体の複雑性については中程度である。

表3　第2ステージ・モジュールの詳細

第2ステージ・モジュール	詳細
Computational Puzzle（コンピュータ・パズル）	この手法では、通話を成立する前に、発信者の端末にリソースを浪費するタスクを実行させる。Computational puzzleは、SIPと共に、IETFの手により現在標準化作業が進められており、実装の複雑さは中程度である。
Sender Check（送信者照合）	この手法の背後にあるアイデアは、発信者が、通話を発信したドメインの正当な発信者であるか否かを照合するというものである。このような方法論に関しては、関連技術が成熟したとしても、発信者の照合に時間がかかるため、SPIT防止などのリアルタイム通信への適用が容易ではない。
Turing Test（チューリング・テスト）	Turing Testは、人間とコンピュータを区別する手法である。このようなテストは、CAPTCHA（Completely Automated Public Turing Test to Tell Computers and Humans Apart： コンピュータと人間とを区別する完全に自動化された公開チューリング・テスト）とも呼ばれている。音声によるCAPTCHAに関しては、誤りが発生しやすい傾向があるものの、SPIT防止には非常に適している。実装自体の複雑さについては中程度である。

表4　第3ステージ・モジュールの詳細

第3ステージ・モジュール	詳細
Consent-based Communication（同意に基づく通信）	このソリューションでは、ユーザBがユーザAに対して最初に通話を試みる際に、ユーザAによるユーザBに対する認証が必要となる。同意に基づく通信とリストとを組み合わせたこの枠組みは、現在、IETFの手によってSIPプロトコル向けに標準化作業が進められている。実装自体の複雑さについては中程度である。

4.4 第4ステージ:受信者が電話を受ける

この手法は、電話を取った受信者が通話中に操作を行うことを必要とします。最新の文献によれば、このカテゴリーに当てはまるのはコンテンツ・フィルタリング法のみです。これは、以下で説明するように、この手法がSPITには適していないためですが、将来的には、このカテゴリーに適した別の手法が提案される可能性もあります。したがって、この手法も、我々の提案するアーキテクチャのステージを割り当て、考慮する価値があると判断しました。**表5**に詳細を説明します。

表5　第4ステージ・モジュールの詳細

第4ステージ・モジュール	詳細
Content Filtering（コンテンツ・フィルタリング）	SPITのコンテンツは電子メール（ASCIIテキストと符号化された音声）とは大きく異なるため、コンテンツ分析をSPIT防止に適用することはできない。また、音声認識は未だ不完全な技術であるうえ、コンピュータ・リソースを大幅に消費する。しかも、検査を実施すべき時に、コンテンツを利用することができないという問題もある（SPITのコンテンツは、着信音に煩わされる受信者が、かかってきた電話に応答した後に、オンラインで送信される）。

表6　第5ステージ・モジュールの詳細

第5ステージ・モジュール	詳細
Reputation System（評判システム）	Reputation Systemは、各通話に対して、通話者の行為の良し悪しを示す評価スコアを付けることによって機能する。この評価スコアは、ユーザのフィードバックに基づいており、もっとも効果的な評価を行うことができるが、他の基礎的要素と関連付けることもできる。このような方法論に関しては、技術が成熟しているため、実装に伴う障害はないが、フィードバックの枠組の標準化が必要である。実装自体の複雑さについては中程度である。
Limited-Use Addresses（限定使用アドレス）	Limited-Use Addressesは、スパム・メッセージが到着すると速やかにアドレスを変更することによって、スパム撃退を試みるメカニズムである。このような方法論に関しては、技術が発達しているため、実装に伴う障害はないが、最初のSPIT通話の受信後すぐにアドレスを変更する必要があるため、実装の複雑さは高い。
Payments At Risk（リスクのある支払い）	Payments at riskでは、初めての通話に対して料金が課される。ただし、その通話がSPITでなければその料金は返還され、その発信者はホワイト・リストに追加される。この手法には、通話がSPITであったか否かを知らせるフィードバックの仕組みに加えて、少額決済のインフラストラクチャが必要である。この2つめの必要条件が存在するため、この方法論はきわめて非現実的であり、実装の複雑さも高くなると考えられる。
Legal Action（法的措置）	Legal Actionは、すべての国々に対して、VoIPでのスパムの流通を禁止する法律の立法を提起するものである。実行することは比較的容易であると思われるが、世界的な立法の枠組みがないため、この方法論はきわめて非現実的である。
First-Contact Feedback（ファースト・コンタクト・フィードバック）	First-Contact Feedbackは、受信者がフィードバックを提供するメカニズムに依存する。この手法では、身元不明のIDを持つ発信者が、一度だけ受信者と通話することを許可される。受信者は、通話後、この通話に関するフィードバックを行う必要がある。このような方法論に関しては、技術が成熟しているため、実装に伴う障害はないが、フィードバックの枠組の標準化が必要である。実装自体の複雑さについては中程度である。

4.5 第5ステージ:受信者による通話後のフィードバック

この手法は、受信者が、応対した電話に関するフィードバックを行うことを必要とします。**表6**に詳細を説明します。

5. 第2ステージにおけるSPIT防止

本章では、人間の通信パターンの分析に基づく、新しいSPIT防止法について説明します。このSPIT防止法の設計とSPIT防止システムへの統合については、第3章の考察に基づいて行われています。

SPIT防止システムの主要な目的は、受信者が、正規の通話を逃すことがないように保証しつつ,SPIT通話に煩わされないように防御することです。さらに、発信者の心証を害さない方法で実現できれば理想的です。しかし、第1ステージに適した手法、つまり、発信者にも受信者にもその存在が意識され

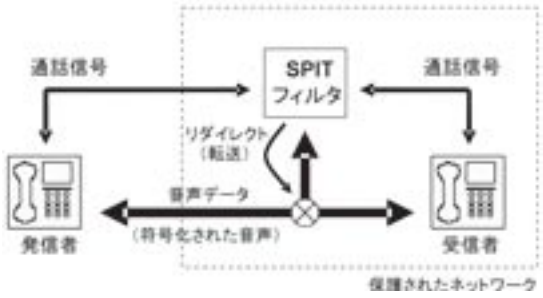

図2　第2ステージのSPITフィルタ

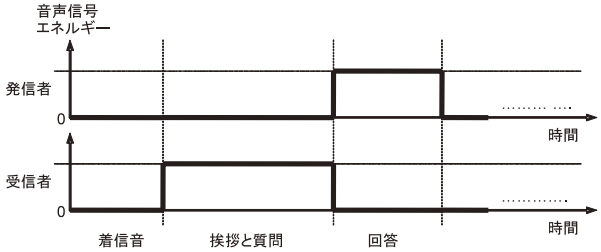

図3　通信開始時における、発信者から受信者（上）および、受信者から発信者（下）の基本的な音声信号エネルギーのパターン

ない手法は、多くの場合、十分な効果を発揮することができません。したがって、ある程度のレベルのイントルーシブ性、つまり「システムの介在」を考慮に入れる必要があります。

受信者がSPIT通話によって煩わされることがないように、我々は､SPIT防止のための画期的なチューリング・テスト(第2ステージの手法)への取り組みに焦点を絞り込みました。第2ステージでは､受信者に代わってSPIT防止システムが着信を受け、検査を実行します。その結果に応じて、通話が受信者に転送されるのか､切断されるのかを決定します。**図2**をご覧ください。

我々は、SPIT通話が人間の発信者ではなくコンピュータによって実行されていることを前提とし、機械と人間とを区別する強力な手法を追及しました。それにふさわしいチューリング・テストは以下の7つの必要条件を満足させる必要があります。

1) 発信者の感情を害することのない礼儀正しさ
2) 発信者に過度の忍耐を強いることのない迅速性
3) 様々な知識を持つ発信者への的確な対応
4) 様々な発音の仕方をする発信者への的確な対応
5) 様々な方言や言語を話す発信者への的確な対応
6) 受信者側の比較的安価な機器に実装できる程度の簡素さ
7) 人間を装う機械に対抗する、複雑かつリソース集約的なタスクの作成

我々は、これらの必要条件を満たす、人間の通信パターンの検証に基づいたチューリング・テストを開発しました。このテストは、受信者に対して高度な防御を提供するとともに、発信者の不便さのレベルをきわめて限定的なものに抑え、かつ調整可能としています。

5.1 通信パターンの検査

我々のチューリング・テストは、人間の会話は特定の活動パターンに従って進むという前提に基づいています。このような通信パターンが識別可能であることを実証する研究はいくつかあり、2) もそのうちのひとつです。ひとりの発信者が他の人間に電話をかける場合、両者が共に従うある種の慣習があります。受信者が電話を受けた後、最初に話すのは受信者の方です。また､通話中は､片方が話している間は､もう片方は黙っているのが普通です。我々が提案するチューリング・テストでは、発信者がこれらの慣習に従うか否かの検査が行われます。

図3は､発信者から受信者(上)そして､受信者から発信者(下)という2つの音声通信による音声信号エネルギーが示す通信パターンの例です。電話が鳴っている間は、両者の音声通信エネルギーは低いか、ゼロになっています。

このパターンは、音声信号エネルギーのみに関係するものです。つまり、音声信号の内容とは無関係であるため、実装が容易であり、ほんのわずかなリソースで実現することができます。

5.2 SPIT検知の仕組み

SPIT防止システムが通話を受けると、あらかじめ録音された挨拶のメッセージが、発信者に対して送信されます。このメッセージは、発信者が受け入れ可能であると思われる「システムの介在」のレベルに対応させることができます。

発信者がメッセージを遮った場合、その発信者は、不躾にも通常の通信パターンに従わない人間、あるいは間髪を入れずにSPITメッセージの再生を開始する機械であるということになります。いずれの場合も､SPIT防止システムは、その通話をSPITであると分類し、通話を切断します。切断する前に、あらかじめ録音された、その旨を伝えるメッセージを送信するというオプションを利用することもできます。

SPIT防止システムが着信音を送信するのではなく、電話を受けることによって、この手法の「システムの介在」は最小

限に留められています。人間の発信者であれば、未だに通話は成立していないと思うはずです。しかし、発信者がSPITエンジンである場合、接続が成立した信号は発せられているため、挨拶メッセージの分析は行わず、SPITメッセージの送信を開始できるものと思い込みます。

「システムの介在」がさらに厳重になるにもかかわらず、良好に受け入れられると思われるのは、通話は現在転送中であり、すぐに通話が成立する旨を伝える挨拶メッセージだからです。

検査をより強固なものにするために、挨拶のあとに、電話をかけている相手先の名前、など簡単な質問を追加することも可能です。この場合、質問は、高い確率で簡単な答えが得られるようなものにすべきです。SPIT防止システムは、まず、質問のすぐ後に発信者が話し始めたか否かを確認し、会話を中断します。そして、質問に対する回答があった後も、ほんのわずかな間だけ沈黙状態を保ちます。なお、この検査は、両方とも音声認識を必要としません。「低」から「高」へ、そして、再び「低」へという音声エネルギーのレベル変化を検知するだけで十分なのです。このようなエネルギーのパターンが観察されない場合、SPITフィルタは、その発信者が機械であると判断し、通話を切断します。

5.3 評価およびプロトタイプシステム

この方法は、前述の7つの必要条件をすべて満たしています。礼儀正しさ、迅速性に関しては十分な能力を備えており、発信者の背景的知識や発音にも依存しません。さらに、(通話が設定された際に、発信者が音声を発した場合)発信者の言語にも対応することができます。音声エネルギー分析は、コンピュータ的には簡単ですが、SPITエンジン側にとっては、この検査を通過するためには、きわめて大きな労力が必要となります。また、受信者の好みに応じて、「システムの介在」のレベルを選択することも可能です。プロトタイプの実装により、音声信号エネルギー検知が、「完全な静寂」と「ある程度の音声エネルギー」とを区別できないことが分かりました。これは、発信者が、雑音の生じる環境(バスの車内、鉄道の駅など)にいるためと考えられます。そのため、この検知システムには、実験で確認された「低」と「高」音声エネルギーのしきい値レベルを使用する必要があります。また、発信者の環境で発生した信号エネルギーの短いピークに対してはフィルタリングを行い、「高」音声信号レベルとして感知されないようにする必要があります。

この手法を用いるSPIT防止システムには、第1ステージの手法、とりわけ、ホワイト・リストとブラック・リストも利用すべきです。ホワイト・リストは、既知の発信者が検査の対象となることを避けるのに役立ちます。また、チューリング・テストの結果を、ホワイト・リストとブラック・リストにフィードバックすることもできます。つまり、あらかじめ設定した回数、連続してチューリング・テストに拒絶された発信者はブラック・リストに追加し、テストに1回または複数回合格した発信者は最終的にホワイト・リストに追加するわけです。

6. おわりに

本稿では、典型的な音声通信パターンに基づく、SPIT通話を識別するための新たな手法を提案しました。さらに、他のSPIT防止手法との統合を図るために、普遍的なSPIT防止システムのアーキテクチャの提案もしました。このシステムは、様々なSPIT防止手法の柔軟な統合を可能とし、発信者と受信者にもたらされる不都合を最小限に抑えるものであり、発信者および受信者とのやりとりのレベルが異なるいくつかのステージに分類されています。このステージ・モデルは、すでに知られている一連のSPIT防止法を分類するために使用されています。我々は、このような推奨システムを実現するための必要条件を詳しく提示するとともに、SPIT防止システムの設計に関しても言及しました。また、すべての必要条件に適合したこの設計の革新的な構成要素として、人間の発信者とSPITエンジンを区別する、第2ステージのチューリング・テストを開発しました。

参考文献

1) J. Rosenberg、ほか「The Session Initiation Protocol (SIP) and Spam」、draft-ietf-sipping-spam-01.txt、2005年7月、加筆中

2) F. Hammer、ほか「Elements of Interactivity in Telephone Conversations」、Proc.、
8th International Conference on Spoken Language Processing (ICSLP/INTERSPEECH 2004)、Vol. 3, pp. 1741-1744、韓国済州島、2004年10月

3) D. Shin、C. Shim「Voice Spam Control with Gray Leveling」、Proc. of 2nd VoIP Security Workshop、ワシントンDC、2005年6月1～2日

執筆者プロフィール

ユールゲン クイテク
Senior Manager,
Network Laboratories,
NEC Europe Ltd.

サンドラ タルタレルリ
Senior Research Staff,
Network Laboratories,
NEC Europe Ltd.

サベーリオ ニッコリーニ
Research Staff,
Network Laboratories,
NEC Europe Ltd.

リナン シュレゲル
Swiss Federal Institute of Technology