迷惑電話を撃退するSPIT対策システム

片山 勝（かたやま まさる）/吉田 順一（よしだ じゅんいち）
山崎 裕史（やまざき ひろふみ）/金子 斉（かねこ ひとし）
茶木 愼一郎（ちゃき しんいちろう）

NTTネットワークサービスシステム研究所

IP電話が普及し，今までの電話で起こっていたワンギリや電話番号スキャン，インターネットでのDoS攻撃などの脅威への対応が必要になってきました．本稿では，これらの脅威からSIPサーバを防御するSPIT対策システムについて紹介します．

IP電話のセキュリティ

電話網のIP化が進み，SIP（Session Initiation Protocol）を用いたIP電話へと移行が進んでいます．これに伴い，今までの電話網で起こっていたワンギリ（相手が電話をとる前に電話を切り，着信履歴を残し，かけ直してもらう）や電話番号スキャン（使われている電話番号を調べる）のようなものから，IP電話になることによって，新たにインターネットで起こっているDoS（Denial of Service）攻撃などの脅威への対応が要求されています．

IP電話の普及に伴い，2005年にはVoIPのセキュリティ確保を推進する団体VOIPSA（VoIP Security Alliance）[(1)]が設立され，ホワイトペーパーの公開やセキュリティツールの開発をはじめ，VoIPセキュリティの啓発を行っています．

IP電話のセキュリティは，大きく2つに分類されます．1つは，プロトコルや実装の脆弱性に関するものです．もう1つは，DoSに代表される大量のトラフィック，つまり大量のワンギリなどの迷惑電話（SPIT：SPam over IP Telephony）によるものです．脆弱性に関するものは，サーバや端末へのパッチの適用等の対策がなされますが，大量の迷惑電話によるものに関しては，正常な電話トラフィックを阻害してしまう場合があります．SPIT対策システム（**図1**）は，特に大量の迷惑電話トラフィックに関するIP電話のセキュリティに対して有効なシステムです．

大量トラフィックとハードウェア技術

DoS攻撃に代表される大量トラフィックによるネットワーク的な攻撃は，サーバ等が処理できない量のトラフィック

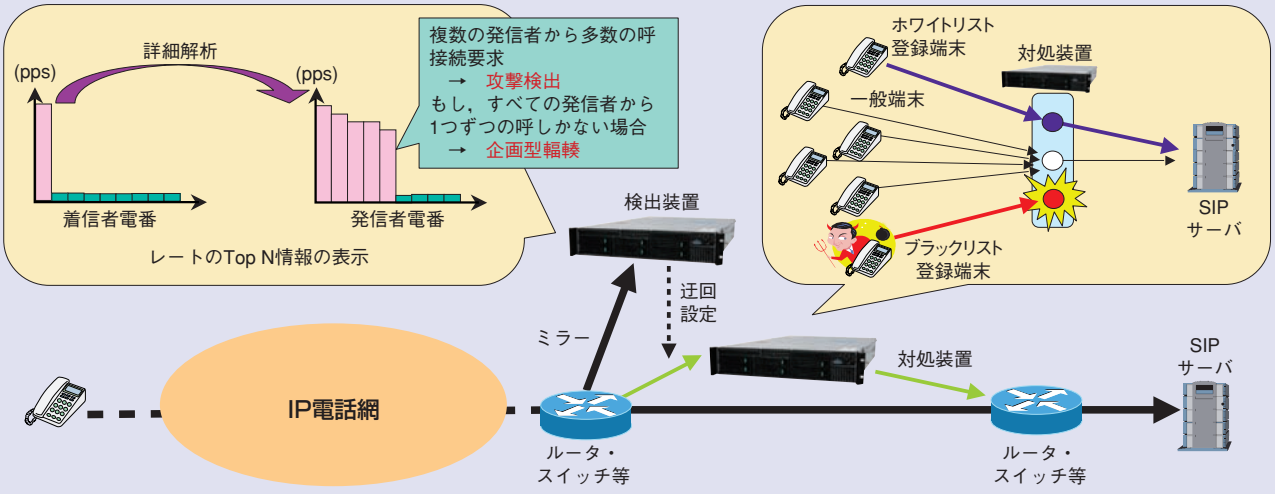

図1　SPIT対策システム概要

を送出します．そのため，ソフトウェアで大量のトラフィックの処理を行うと，攻撃がくればくるほど処理が重くなってしまい，正常な通信へも影響してしまいます．つまり，Denial of Serviceとなってしまいます．そのため，これらの攻撃からサーバを守るためには，ソフトウェアではなくハードウェアによる対策が必要になってきています．

このように，大量なトラフィックによる攻撃にはハードウェアによる処理が必要です．しかし，ハードウェアはソフトウェアのような柔軟性，拡張性がありません．特にセキュリティに関しては，日々の攻撃の進化に対応して，機能変更，機能追加が必要となり，ソフトウェアのような柔軟性が必要です．大量トラフィックを処理するためには，高速性と柔軟性の両立が重要となります．

NTTネットワークサービスシステム研究所では，次世代のプロセッサである「リコンフィギャラブルプロセッサ」と呼ばれる技術を用いて高速性と柔軟性の両立を行い，IP電話のセキュリティに適用しています．

SPIT対策システムの概要

SPIT対策システムは，1 Gbit/s回線上のSIPトラフィックをワイヤレートで解析できる処理能力を持っています．SPIT対策システムは2つの機能から構成され，SIPサーバの手前のネットワークに導入します．第1の機能は検出機能，第2は対処機能です．

検出機能の特徴は，定常的なIP電話のトラフィック監視と，異常トラフィック（迷惑電話）の監視・検出です．異常トラフィックを検出するために，さまざまな分析機能を有しています．ここでは，ワンギリを検出する方法を例に紹介します．

ワンギリの特徴は，ランダムの電話番号に対して，電話をかけ，相手が電話を取る前に切ります．そこで相手の電話に着信履歴を残し，かけ直してもらいます．つまり，かけ直してもらうために，発信者の電話番号が同じになります．この特徴を利用し，ワンギリを検出します．

では実際のSPIT対策システムの検出動作を見てみます．最初に定常的なトラフィックの場合を**図2**に示します．これはSIPトラフィックをメソッドと呼ばれる，電話をかける，電話を呼び出す，電話を切る，などの動作を規定したもので分類し，それぞれのトラフィック量をリアルタイムで表示しています．

この状態でワンギリが行われると，**図3**に示したように，Initial-INVITEと呼ばれる電話をかける動作のトラフィックが急激に多くなり，グラフが赤く変わります．この段階で，何らかの異常が起こったことが分かります．

次に，このInitial-INVITEの分析を行います．**図4**は発信電話番号ごとに1秒間に何回電話をかけているかを示しています．表示はトラフィックの

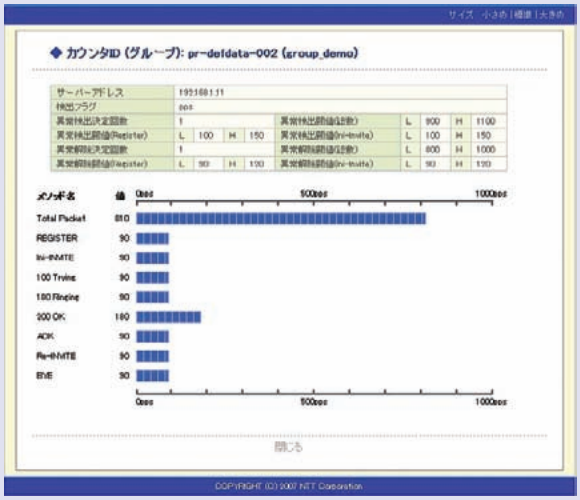

図2　定常状態のトラフィック

図3　ワンギリによるInitial-INVITEの増加

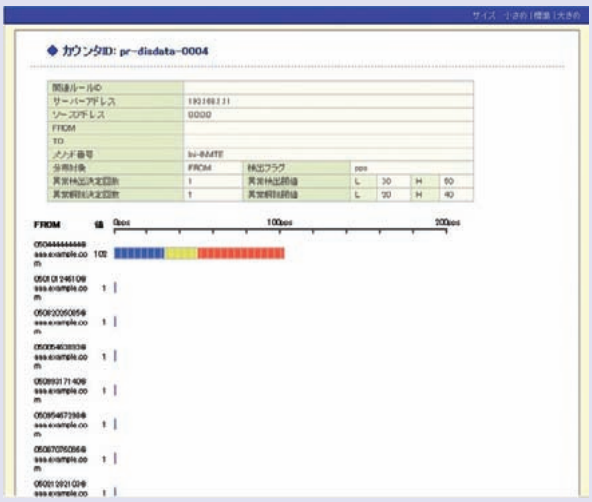

図4　発信者電話番号ごとのトラフィック量

多い順に表示しています．ここで，ある1つの電話番号から大量に電話がかかってきていることが分かります．通常は電話のリダイヤル機能を使っても，1秒間に数回しかかけられませんから，機械的に電話をかけていることが分かります．

このようにワンギリを検出でき，迷惑電話をかけている電話番号が特定できます．

続いて，対処機能の特徴を説明します．対処機能は，メソッドごと，電話番号ごとにトラフィック量を制御可能です．制御機能としては，ブラックリストによる特定トラフィックの全廃棄機能，レート制限機能，ホワイトリストによる特定トラフィックの優先機能があります．先ほどのワンギリの例では，特定された発信者電話番号に対して，制御をかけることで対処が可能となります．

SPIT対策システムを支えるハードウェア技術

SPIT対策システムは，1 Gbit/sのワイヤレートでSIPパケットの中を解析し，さまざまな処理を行う必要があります．加えて，ソフトウェアと同じようにプログラムにより機能変更の自由度が必要です．そのキーとなるのが**図5**のGbit-RNPというPCのPCIスロットに搭載可能なギガビットイーサのインタフェースを2個搭載したリコンフィギャラブルプロセッサボードです．

リコンフィギャラブルプロセッサ[(2)]は，**図6**に示したように，1個のチップに376個の演算機能（PE: Processing Element）を並列に搭載しており，これらの並列処理により高速な動作が保

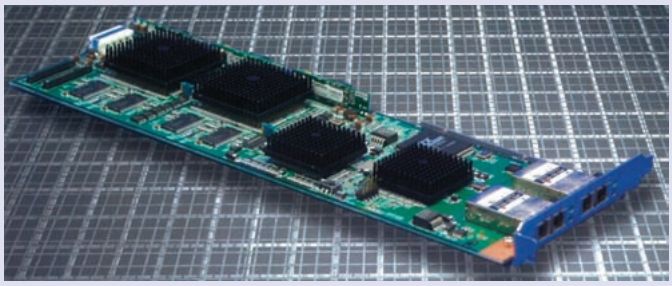

図5　リコンフィギャラブルプロセッサボード（Gbit-RNP）

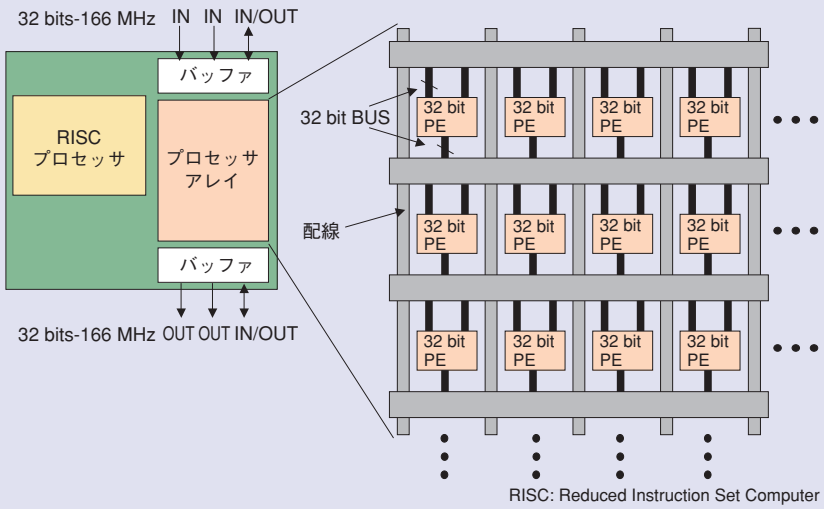

図6　リコンフィギャラブルプロセッサアーキテクチャの概要

証されます．このGbit-RNPには2個のリコンフィギャラブルプロセッサが搭載されており，合計752個の演算機能で並列処理およびパイプライン処理を行っています．演算機能の中には32個の独立したメモリを内蔵しており，並列にデータ検索が可能です．また，動作中でもパケットロスなく機能変更が可能な構成になっており，本装置を動作させたまま，機能追加，機能変更が可能になっています．

今後の予定

今後，IP電話に対する攻撃が予想されるため，新しい攻撃に対応する検出アルゴリズムの高度化を行いながら，継続的に本システムの研究開発を推進していきます．また，安心・安全なネットワークを実現するために，SIPサーバばかりではなく，さまざまなサーバ防御への適用を検討していく予定です．

■参考文献

⑴　http://voipsa.org/
⑵　http://www.ipflex.com/

（後列左から）茶木　慎一郎/ 山崎　裕史/
金子　斉
（前列左から）片山　勝/ 吉田　順一

私たちは，安心・安全なネットワークを目指して，日々高度化するセキュリティ技術に追従可能な柔軟性のあるハードウェアを用いて，ワイヤレートで高位レイヤ処理を実現する研究開発に取り組んでいます．

◆問い合わせ先

NTTネットワークサービスシステム研究所
第一推進プロジェクト　IPサービスネットワーク推進DP
TEL　0422-59-4354
FAX　0422-59-4549
E-mail　katayama.masaru@lab.ntt.co.jp