盗聴に強い安全なインターネット音声通信が可能に

～東北大学の音声信号秘密分散共有技術とＮＥＣのマルチパスルーティング技術を融合～

平成 19 年 1 月 26 日

東北大学電気通信研究所
日本電気株式会社

■ ポイント ■

- あるデータを理論的に推定不可能な複数のサブデータの組み合わせで表現し直す「秘密分散共有理論」（注１）に基づくディジタル音声信号秘話化と，インターネット上の２地点間を複数のルートでデータ転送を行う「マルチパスルーティング技術」（注２）との融合により，従来とは全く原理の異なるネットワーク音声秘話化通信を実現
- データ表現の工夫により，音声信号の秘密分散共有によるデータ量の増加を大幅に削減
- 第 3 者によるネットワーク上の盗聴が困難となり，VoIP(Voice over IP)等，ネットワーク上の音声通信のセキュリティが向上

■ 概　要 ■

東北大学【総長 井上明久】電気通信研究所【所長 伊藤弘昌】の鈴木陽一教授，工学研究科【研究科長 内田　龍男】の牧野正三教授，伊藤彰則助教授らの研究グループ(以下「東北大」という)は，日本電気株式会社【社長 矢野薫】システムプラットフォーム研究所【所長 加納敏行】（以下「NEC」という）の岩田淳部長らと共同で，ディジタル音声信号の秘密分散共有技術とマルチパスルーティング技術とを融合させた，音声の新しい秘話通信技術の開発研究を進めてきた。今回，システム実装を完了し，実証実験を行い，その有効性を確認した。今後，早期の実用化を目指す。

■ 新技術開発の背景 ■

VoIP（IP 電話）の普及により，インターネット上を音声データが行き来する時代となった。しかしながら，本来的にオープンなネットワークであるインターネットを用いて通話するにあたり，現在の盗聴対策をさらに強固にした，より一層の盗聴対策を求める声も多い。

また，盗聴に対して暗号は一つの有力な対応策ではあるものの，解読された場合に無力化することや，暗号化と解読処理のコストが無視できないなどの問題点も指摘されている。

インターネットを用いながら手軽に安全な音声通信が可能となれば，これまでより経済性やユビキタス性に優れる VoIP 通信を，様々な場面で利用することが可能になると期待される。

■ 新技術の特徴 ■

新技術の特徴は以下のとおりである。

○ 秘密分散共有理論に基づく音声秘話化により，高い秘話性を確保
○ 近年技術開発が進むマルチパスルーティングを用いることにより，高い安全性を確保

東北大学で開発した秘密分散共有理論に基づくディジタル音声信号秘話化技術と，元来は負

荷分散や信頼性向上を目的として NEC が開発したマルチパスルーティング技術とを融合することにより，従来とは全く原理の異なるネットワーク音声秘話化通信を実現した。

通常，インターネット上の 2 地点間での通信は，1 セッション中は全て同じルートでデータが転送されるが，マルチパスルーティングでは複数のルートでデータの転送が行われる。一方，秘密分散共有とは，あるデータを，各サブデータからはオリジナルのデータに関する情報が理論的に推定不可能な複数のサブデータの組み合わせで表現し直す手法である。

今回のシステムでは，音声データに対して秘密分散共有を行い，各サブデータをマルチパスルーティングにより別々のルートで転送する。秘密分散共有理論により，サブデータを盗聴しただけでは音声は原理的に復元不可能なため，盗聴するためには，物理的に異なる複数のパスでハッキングを行うという実質的に不可能な行為を行わなければならない。つまり，このたび開発した技術を活用することにより，第 3 者による盗聴が困難となり，安全性が向上される。

ただし，単純にこの手続きを実現したのでは，データ量が大幅に増加するため，今回，CELP 符号化（注３）された音声データの表現を工夫することにより，ほぼ完全な秘話性を確保したまま，データの増加量を約 50%に抑えることができる新しい技術の開発も行った。

この新技術は，オープンなネットワーク環境においても，安全な音声信号伝送を可能とする基盤技術として，VoIP(Voice over IP，IP 電話)通信でのセキュリティ向上への応用が期待される。

今後，更に秘話性を高めるとともに，実用性の向上を図るための研究を更に推進する予定である。

■ 開発システムの概要■

図 1 に，今回開発したシステムの構成を示す。送信側クライアントにおいて，(a)の秘密分散共有による秘話符号化を行い，入力された音声を複数のフローに分割する。そのうえで，(b)により構築した複数のマルチパス経路に，(c)の拡張ソケットを通じ，分割したフローをそれぞれ送出する。これにより，高い秘話性をもった音声通信を実現している。

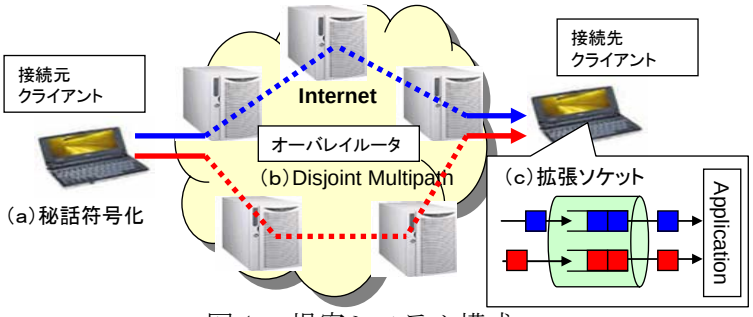

図 1　提案システム構成

(a)秘密分散共有による秘話符号化：音声の符号化時に，原情報を n 個の分散情報に分散させて（複数のフローに分割して）暗号化を行う。復号化時は任意の k(n≧k)個以上の分散情報を用いれば復号可能だが，それに満たない k 個未満の分散情報だけでは元情報は理論的に全く復元が不可能である。この特性を音声の秘話に応用し，(b) により構築した複数経路（マルチパス）に，分割したフローをそれぞれ送出すること，たとえ 1 フローのデータをすべて傍受された場合でも，通信内容を判別できない。今回は，n=k=2 として，システムの実現を行っている。

(b)ディスジョイント・マルチパス転送：図に示すように，インターネット等のネットワーク内に複数のオーバレイルータ（注４）を配置し，オーバレイネットワーク（注５）を構築する。接続元クライアントはオーバレイルータと連携し，接続先クライアントとの間で，重なりのない経路（ディスジョイントになる経路）を複数設定して接続する。

本システムでは，(a)の秘密分散共有に加え，クライアントとオーバレイルータ間や，オーバレイルータ間の通信を IPsec（注６）または SSL（注７）により暗号化することで，単一フローに IPsec や SSL を単純適用した場合よりも，盗聴に対する秘話強度を強固にできる。
(c)拡張ソケット: アプリケーションシステムからの接続要求を受け，オーバレイネットワーク上で，ディスジョイント経路を生成する。ネットワークからのパケット到着時は，バッファで到着タイミングのずれを吸収し，各パスからのパケットを同期させてアプリケーションシステムに転送する。

【用語の説明】

注１　秘密分散共有
あるデータを，各サブデータからはオリジナルのデータに関する情報が理論的に推定不可能なような複数のサブデータの組み合わせで表現し直す手法。宝の地図を切り分けて複数人が分けて持ち，全員の地図が合わさらないと宝物には行き着けない，という秘密保持法にたとえることができる。

注２　マルチパスルーティング
通常，インターネット上の 2 地点間での通信は，1 セッション中は全て同じルートでデータが転送されるのに対し，複数のルートでデータ転送を行う通信技術。これまでは，複数経路伝送による負荷分散技術や広帯域化技術として，あるいはネットワーク障害が生じたときにネットワーク通信を断絶させないための高信頼技術として着目され，研究開発が行われてきた。

注３　ＣＥＬＰ符号化
人の発声機構を電気的にモデル化し，音声の情報量を圧縮する符号化方式。人間の音声は，声帯の振動を声道で共振させることで生成されるが，この生成過程に基づき，「音源」と「共振による音の変化」の二つの要素に分けて符号化を行い，高い圧縮率を実現する。

注４　オーバレイルータ
第 4 層（TCP 等のトランスポート層）以上のプロトコル処理機能を有する経路制御装置。通常のルータは第 3 層(IP 等のネットワーク層)により経路制御を行うが，第 4 層以上の情報により経路制御を行うことで，マルチパスルーティング等の複雑な経路構築を実現できる。

注５　オーバレイネットワーク
オーバレイルータにより構成されたネットワーク。インターネット上での VoIP 通話ソフトウェアや，ファイル交換ソフトウェア等に利用されている。

注６　ＩＰｓｅｃ
インターネットで暗号通信を行うための規格。データの盗聴を防止できる。多地点間通信にも対応できるため，企業の拠点間通信の暗号化等に利用されている。

注７　ＳＳＬ

インターネットで暗号通信を行うための規格。データの盗聴のみならず，改ざんやなりすましも防止できる。暗号強度が高いため，インターネット上での個人情報の送受信などに利用されている。

〈本件に関する問い合わせ先〉

東北大学電気通信研究所
教授　鈴木　陽一
〒980－8577 仙台市青葉区片平 2-1-1
東北大学電気通信研究所
tel: 022-217-5460　fax: 022-217-5535
E-mail：suzuki@ais.riec.tohoku.ac.jp