

2003（平成15）年9月24日

株式会社ナカヨ通信機

デュアル暗号方式でセキュアなIP電話を実現 盗聴防止 IP電話機の開発について

株式会社ナカヨ通信機（本社：東京都渋谷区、代表取締役社長：秋山進）は、この度、次世代の通信手順「SIP」に対応したIP（インターネット・プロトコル）電話機に暗号通話機能を搭載した盗聴防止IP電話機を開発いたしました。

近年、ADSL や FTTH を用いたインターネット常時接続サービスの利用拡大に伴い、無料通話・格安料金設定等、様々なメリットのあるIP電話サービスが爆発的なスピードで普及し始めています。しかし、IP電話はインターネットというオープンな通信環境を利用することから、第三者による不正な情報取得等の危険も同時に存在します。

そこで当社では、お客様に安心してIP通話をご利用していただくために、暗号通話機能を搭載した盗聴防止IP電話機を開発いたしました。

今回開発した盗聴防止IP電話機では、公開鍵方式の一つであるRSA暗号（1）を利用した手順で秘密鍵方式の一つ、DES（2）の暗号鍵を交換する、という二重の暗号方式をとっております。

当社の盗聴防止IP電話機ユーザ同士であれば、暗号モードで発信すると自動的に相手と暗号接続され、盗聴やなりすまし等の被害を防止することが可能となります。

また、当社のIP電話機（DATAGATE IP Phone）及び、その他のIP電話機との接続も可能です。（この場合、暗号はかかりません）

今後、商用化に向けて、AES暗号の採用によるセキュリティ強化、操作の簡略化等、更なる改良を重ね、技術開発を進めてまいります。

なお、盗聴防止IP電話機を本年10月7日～11日に幕張メッセにて開催される「CEATEC JAPAN2003」のナカヨ通信機ブースに出展する予定です。

- 1 RSA暗号...公開鍵方式の一つ。公開鍵方式とは、対になる2つの鍵を使ってデータの暗号化・復号化を行なう暗号方式のことで、このRSA暗号を解読するには巨大な整数を素因数分解する必要があり、効率の良い暗号解読の方法はまだ見つかっていない。
- 2 DES暗号...秘密鍵方式の一つ。暗号化と復号化に同じ鍵を用いる。このDES暗号は1977年にアメリカ政府標準技術局（NIST）によって連邦情報処理基準に採用された。
- 3 AES暗号...秘密鍵方式の一つ。DESに代わる米国政府の次世代の標準暗号化方式。

<主な特長>

1. デュアル暗号（RSA・DES）使用

音声データの暗号化にはセッション鍵としてDES暗号を使用、このセッション鍵の交換にはRSA暗号を使用しています。このデュアル暗号方式により、高度な暗号化を実現、盗聴・なりすまし等の危険から通話を守ります。なお、暗号はソフト・ライブラリの書き換えで様々な方式に対応予定です。

2. 認証サーバ等の設備が不要

当社の盗聴防止IP電話機同士であれば、認証サーバ等の設備を用意しなくても暗号通話を行なうことができます。

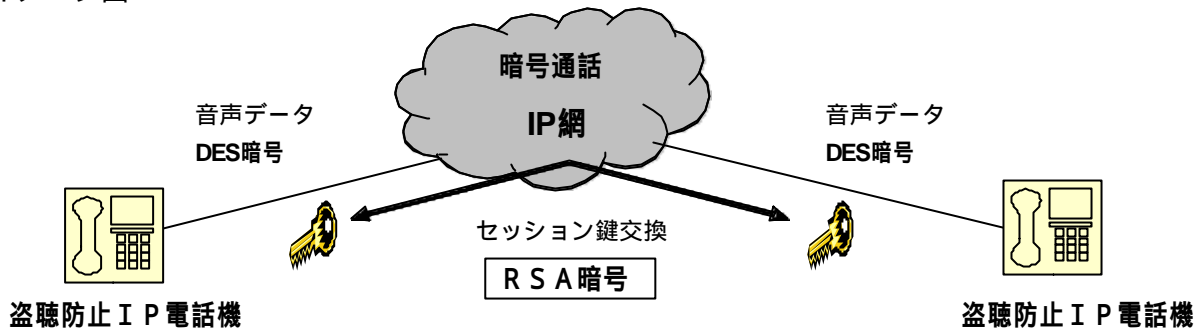
3. 自動暗号モード接続

暗号モードを選択すれば、発信するだけで自動的に相手と暗号通話が可能です。

4. 暗号・非暗号選択

暗号モード・非暗号モードを通話前に選択することができます。

イメージ図



仕様

項目	仕様概要
インタフェース	10Base-T/100Base-TX
呼制御プロトコル	SIP
暗号方式	RSA,DES,AES(エンハンス)
外形寸法	約 175(W) × 238(D) × 130(H)mm
質量	約 0.9kg(AC アダプタ除く)
電源	AC100V ± 10V (50/60Hz) 専用 AC アダプタによる

株式会社ナカヨ通信機 会社概要

名称 : 株式会社ナカヨ通信機
設立年月日 : 1944年5月30日
本社所在地 : 〒150-0031 東京都渋谷区桜丘町 24 - 4
社長 : 秋山 進
資本金 : 49 億円
従業員数 : 449 人 (2003 年 3 月末現在)

本ニュース・リリースに掲載されている情報は、発表日現在の情報です。発表日以降に仕様などの情報が変更される場合もありますので、あらかじめご了承ください。

この件に関するお問い合わせ先

株式会社ナカヨ通信機

<http://www.nyc.co.jp/>

開発統括本部 商品企画室 大戸・塚本

〒150-0031 東京都渋谷区桜丘町 24-4

TEL 03 - 3496 - 1149

FAX 03 - 3496 - 2089

E-mail www@nyc.co.jp