SONY

VIDEO COMMUNICATION SYSTEM-TECHNICAL DOCUMENTATION

暗号化機能について

PCS-G60	All
PCS-XA55	All
PCS-XA80	All
PCS-XG55/XG55S	All
PCS-XG80/XG80S	All
PCS-XL55	All

IPELA™

はじめに

ソニーのビジュアルコミュニケーションシステム（以下、PCSという[*1]）はセキュアな通信を実現するために音声データ、映像データなどに暗号化処理を施した上で通信する機能を有しています。この機能を利用すると、特にIPネットワーク上で起こりうるかも知れない第三者による通信されるデータの盗み見や改ざんを防ぐことが出来ます。
ソニーのビジュアルコミュニケーションシステムはITU-T国際標準方式に準拠した方式を標準機能として提供しており、同じ標準方式に従った製品であれば、他社製品とも暗号化通信を行うことが可能となります。

*1 対象機種は、表紙を参照してください。

暗号化方式

暗号化アルゴリズム

暗号化アルゴリズムとしてAES(Advanced Encryption Standard)を採用しています。AESは米国のNIST(National Institute of Standards and Technology)がそれまでに使用されていた標準暗号化方式DES(Data Encryption Standard) に代わる次世代暗号化方式として世界中から公募し、最終的に選択されたベルギーの数学者Joan DaemenとVincent Rijmenにより開発された秘密鍵暗号化アルゴリズムRijndaelに基づく標準暗号化方式です。当然DESより信頼性の高い暗号化方式となっています。

AESは暗号化と復号化に共通の鍵を用います。送信側で情報は128ビットずつにブロック化され、鍵で暗号化されます。受信側では同じ鍵を使って復号化し、ブロックを元の情報に戻します。

AESは鍵長として128ビット、192ビット、256ビットの3つから選択できます。もし128ビットの鍵を使うと、情報の盗聴者は正しい鍵を求めるために2の128乗回の総当り攻撃をする必要があります。これは現在の計算機の性能からすると十分な強度といわれています。

鍵交換方式

AESがいくら優れているとは言え、暗号化に使用する鍵が安全に通信相手と共有できないと暗号化の意味がなくなります。

ITU-T国際標準方式の鍵の交換方法はDiffie-Hellman鍵交換方式を採用しています。

Diffie-Hellman鍵交換方式はWhitfield DiffieとMartin E. Hellmanによって考案された方式で、鍵そのものではなく、鍵から生成した情報と乱数を送受信することで、その通信内容が盗聴されても直ちに鍵が知られないという数学的難解性を利用します。これにより相手と自分とで共通の値を安全に共有します。またこの方法では、鍵を管理する手間が省けます。利用者は明示的にパスワードなどを入力しないでも、自動生成された乱数を用いて確実に安全に相手と鍵を共有できます。

PCSが提供する暗号化方式

ITU-T国際標準方式

ITU-T(International Telecommunication Union - Telecommunication Standardization Sector)では暗号化通信方式を勧告H.233 H.234 H.235として定めています。H.233及びH.234はISDN上のH.320通信システムが従うべき暗号化通信方式を規定するもので、前者ではメディアの暗号化方法、後者では鍵交換も含めた暗号化通信に必要なシグナリング方法を記述しています。H.235はIPネットワーク上のH.323通信システムが従うべき暗号化通信方式を規定するもので、AESはH.235 Version 3でサポートされています。PCSは、これらのH.233、H.234およびH.235 Version 3に準拠しています。またAESの鍵長は、128ビットを使用しています。

暗号化対象メディアは下記の通りです。
ご使用のPCS端末がサポートしているメディアはすべて暗号化されます。

- 音声データ、映像データ
- 相手カメラ制御データ
- PCプレゼンテーションデータ*2
- ビデオカメラを2台使用した時の2ndビデオストリーム*2
- ペンタブレットから入力される描画データ*2

対向接続時の他、多地点接続時も暗号化通信は可能です。特に多地点接続時はH.320接続とH.323接続とが混在していても暗号化通信をすることができます。ただし、一部のモデルがサポートしているソニー製ネットワークカメラとの接続時は、暗号化通信をすることができません。

*2 これらのデータの取り扱われかたは、モデルによって異なります。

接続形態と暗号化サポートの関係

（表 .1）対向接続時

	IP	ISDN	SIP
PCSの暗号化方式	●	●	×

（表 .2）多地点接続時

	IP のみ	ISDN のみ	SIP のみ	IP&SIP	IP&ISDN	SIP&ISDN	IP&ISDN&SIP
PCSの暗号化方式	●	●	×	×	●	×	×

SONY