

課題番号:051302004

音情報の高信頼高品質ネットワーク通信技術の開発

研究代表者

鈴木陽一（東北大学電気通信研究所）

研究分担者

**牧野正三，伊藤彰則，鈴木基之，静谷啓樹，酒井正夫，
坂本修一（東北大学）**

研究協力者

西村竜一（分担者@東北大学→ATR/NICT）

阿留多伎明良（NEC→NEC通信システム）

岩田 淳（NEC）

研究背景と目的

■ 背景

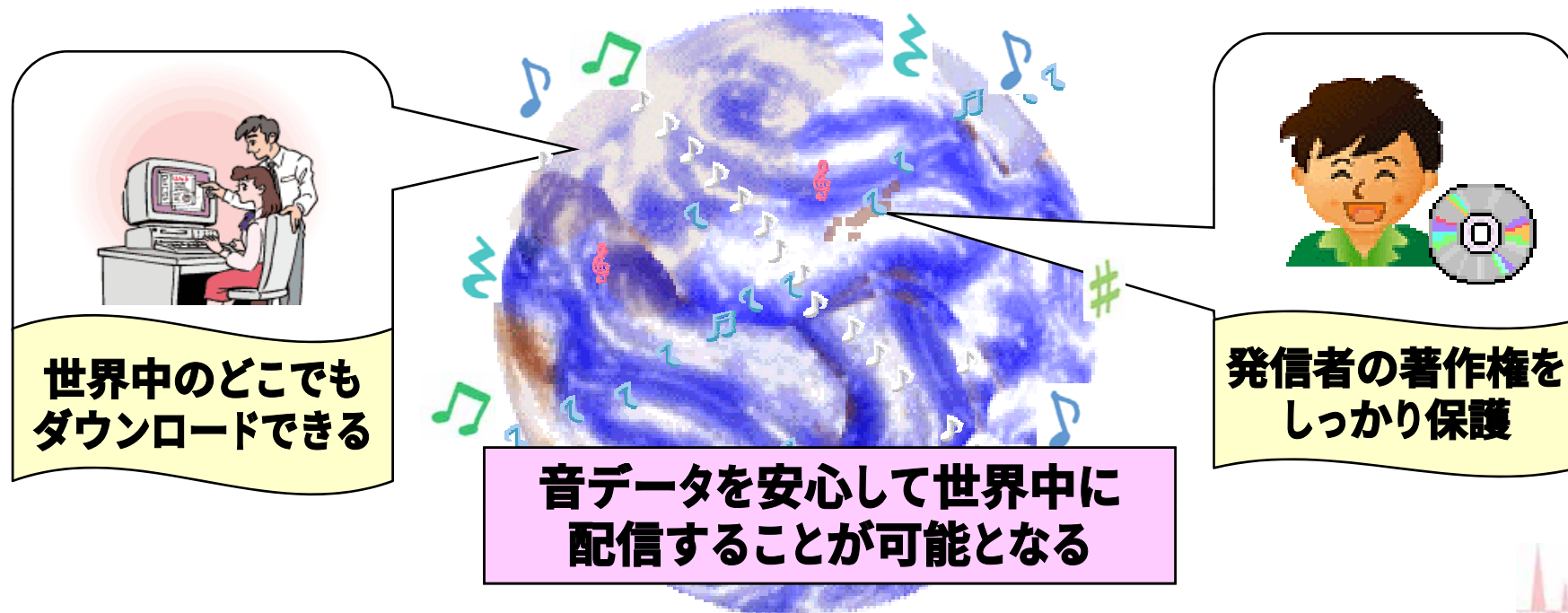
- インターネットのブロードバンド化と普及による新しい音・音声情報を扱うサービスの登場
- メリット (時間的空間的制約の解決など) の一方, デメリット (安全性や品質の保証がない) も

■ 研究目的

- ネットワーク環境における高信頼高品質音情報処理技術の開発
 - デジタルおよびアナログの両耐性を持つデジタル音信号電子透かしを開発
 - 高音質高圧縮音楽信号のストリーミング配信技術を開発
 - 高い秘話性を有するインターネット音声通話 (VoIP) 技術を開発

電子透かしの意味と意義

- 暗号: 復号化しないと使えないが, 復号後は原信号と同一
- 電子透かし: 埋め込み後もコンテンツのあるべき形は保存
 - アナログ耐性を持てば, カセットテープにダビングされてもラジオ放送に使われても著作権が保護できる



サブテーマ1における成果

- **新しい電子透かしの開発**
 - LDPC符号を用いた電子透かしを開発
 - データマイニング技術に基づく新しい電子透かしを開発
 - 既存の電子透かしの埋め込み／検出技術と併用し、その秘匿性と攻撃耐性を向上させる「乱択法」を開発
- **我々が先に提案したエコー拡散法の最適化により、アナログ耐性向上を実現**
 - 埋め込みビットレート16 bpsで100%、32 bpsでも約90%の検出率を達成

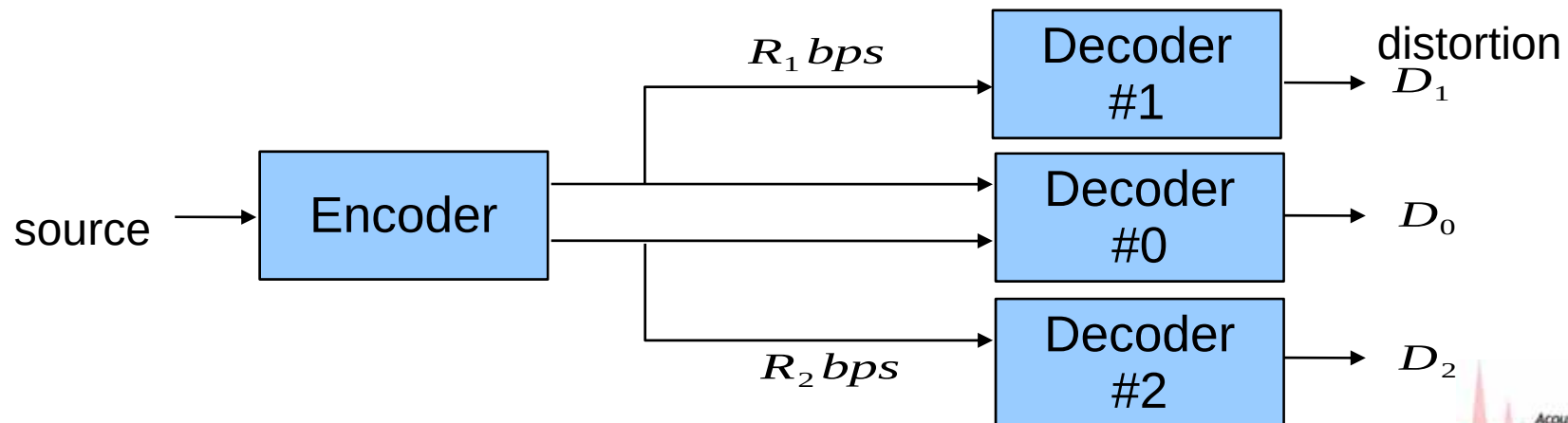
**当初の目標 (16bpsで検出率90%)
を超える成果を実現**

サブテーマ2の目標

- IPネットワーク上の高性能オーディオ (音楽) 伝送法を開発
 - 高信頼: パケット欠落に強い
 - 送信側インターリーブ + 受信側ロス補償
 - 高音質, 低ビットレート
- 採用する方法論
 - 複数記述符号法 (Multiple Description Coding) を, 圧縮音楽信号 (今回はMP3) に適応

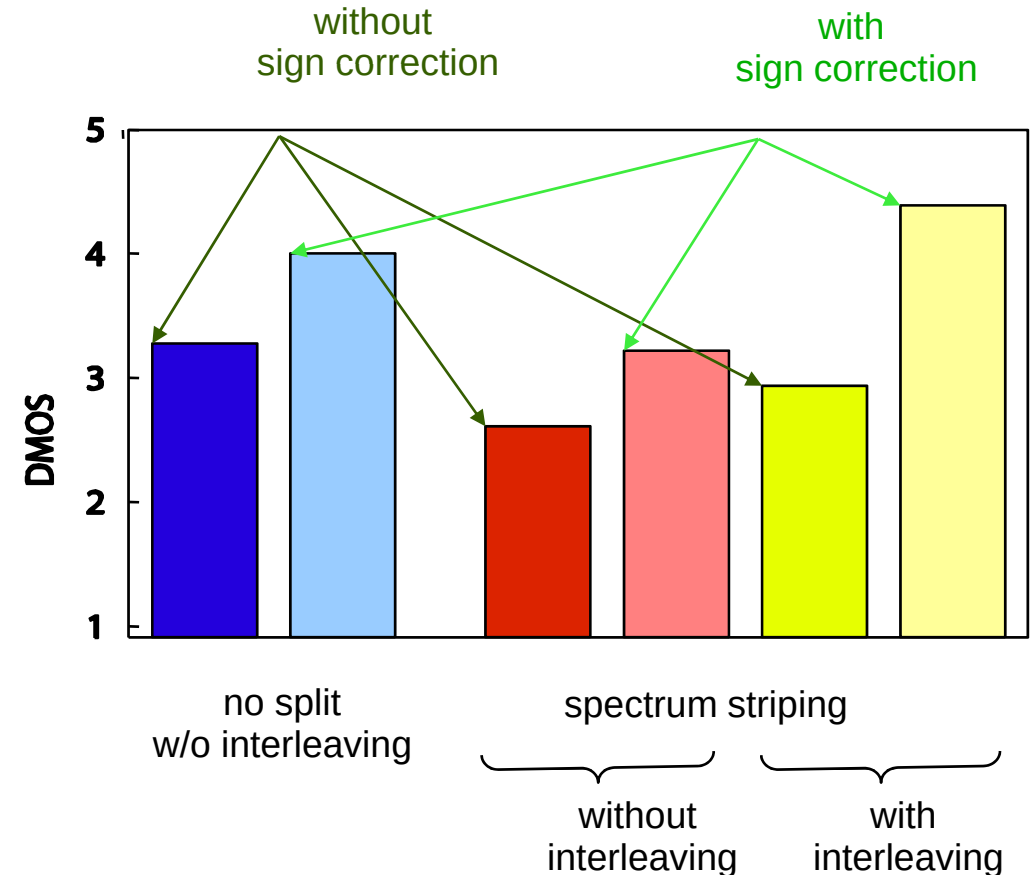
複数記述(Multiple Description)符号化

- 1組のデータを2つ以上のストリームに分割
- ストリームがすべて受信できれば
 - (ほぼ) 元のデータが復元可能
- 1つ以上のストリームが欠けた場合には
 - 他のストリーム受信できれば, 誤差はあるが元のデータに近いデータが復元可能



MP3音楽信号に対するMD型通信方式の開発

- 周波数ストライプ分割
 - パケットデータを周波数領域で2分割してMD化
- MD化のための情報付加
 - MP3符号のMDCT係数の正負符号情報 (約7.8 kbit/s)
- 上記に, 冗長符号情報とインターリーブングも併用
- 10%パケットロス時, 5段階主観評価値で4以上の高い品質を実現



音質のDMOS評価値
(パケットロス10%時)

当初の目標 (パケットロス10%で
音質劣化が気にならない) を達成

サブテーマ3の背景と目標

- **インターネット音声通信 (VoIP)の普及**
 - メリット: 時間的空間的制約の解決, 低コスト
- **懸念**
 - オープンネットワーク経由のため, 秘密性の高い内容の通話には躊躇がある
- **盗聴への対策 ⇒ 暗号化技術**
 - 暗号化通信は解読される可能性がある
 - 実際に, DVDの暗号は解読された
- **暗号と併用可能なセキュア化技法が求められている**
 - 秘密分散共有法に着目

秘密分散法 (Secret Sharing Scheme)

- ある情報を分解して複数の媒体に運搬させ、それらの媒体全てを集めた者だけが、もとの情報を得ることができる
 - 古典的な宝島の地図の分け持ちにたとえられる

宝島の地図

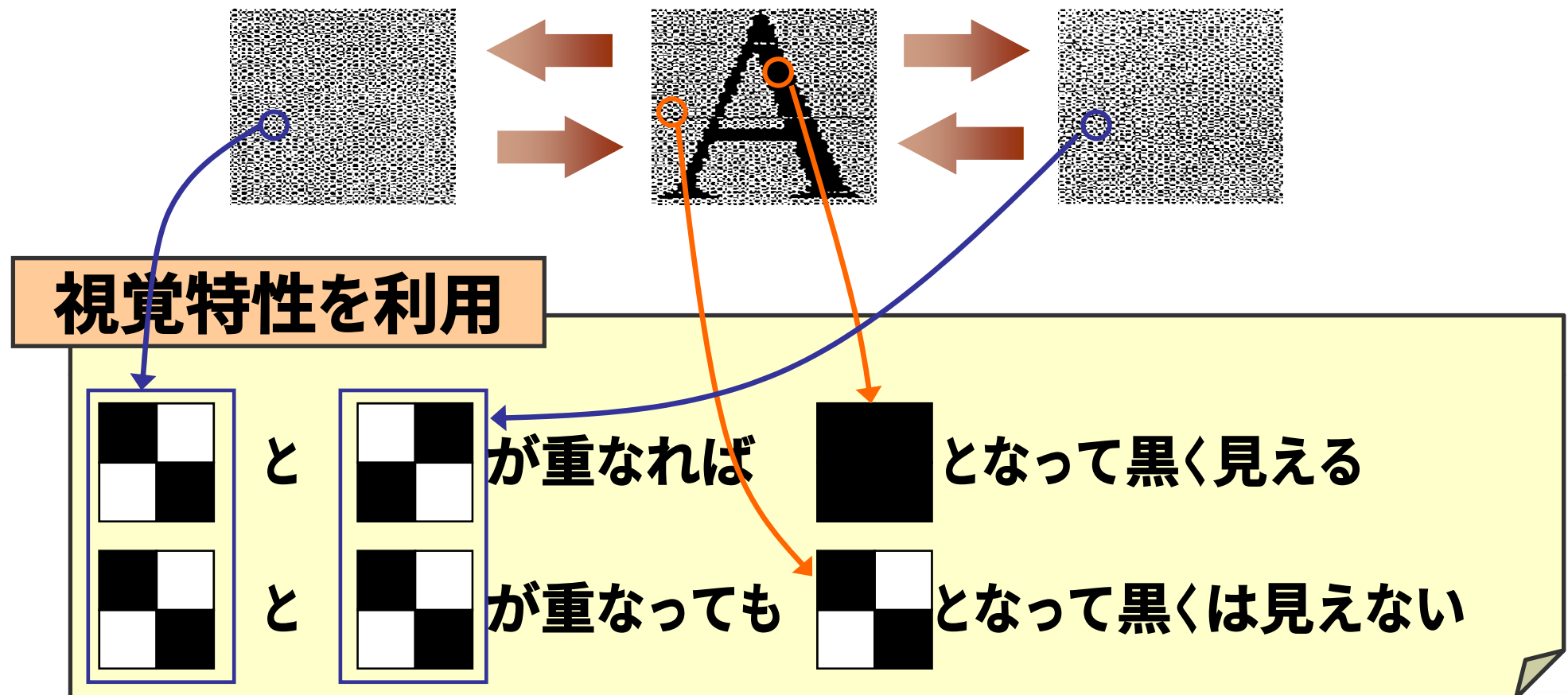


秘密分散法の利用例: ストレージ情報の保秘



画像の 2 out of 2 秘密分散 (Naor, 1994)

- 二つの画像に分散し, 再び重ねる



音声信号への秘密分散法の適用

■ 秘密分散による情報の秘匿

■ k out of n 秘密分散

■ 原情報を n 個の分散情報に分解する

- 任意の $k-1$ 個までの分散情報からでは, 原情報の一部の情報すら得られない
- 任意の k ($\leq n$) 個の分散情報を集めることで復号化が可能

■ n out of n 秘密分散なら

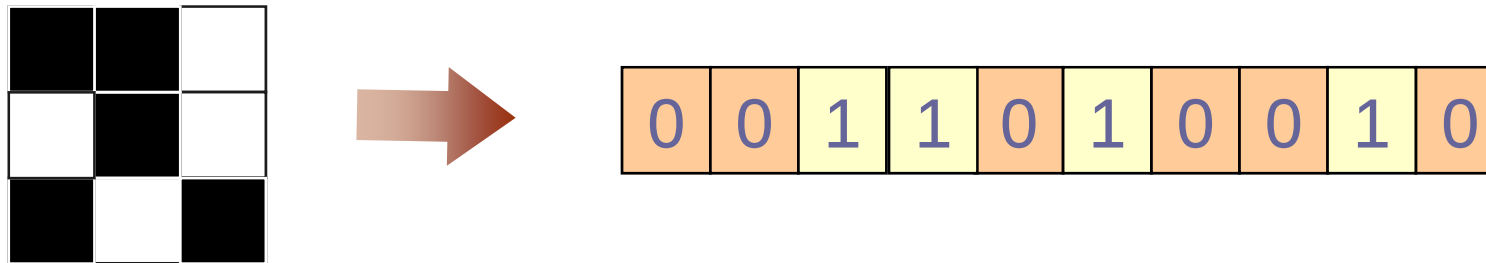
■ 全情報を集めた者のみが復号可能

■ 秘密分散法を用いた音声信号の秘話化

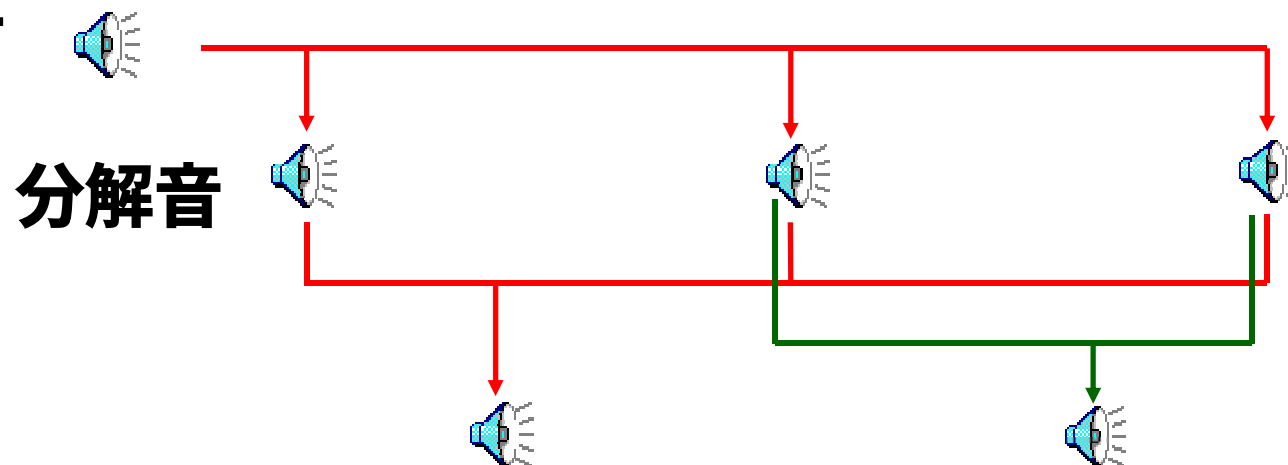
- ある音声信号を幾つもの音声信号データに分割
- それぞれを聞いても, どんな音なのかが不明
- 全てのデータを集めると元の音声信号が聞ける

音声信号への適用

- 2値画像秘密分散アルゴリズムの白と黒を1ビットオーディオ信号の0と1に対応させる

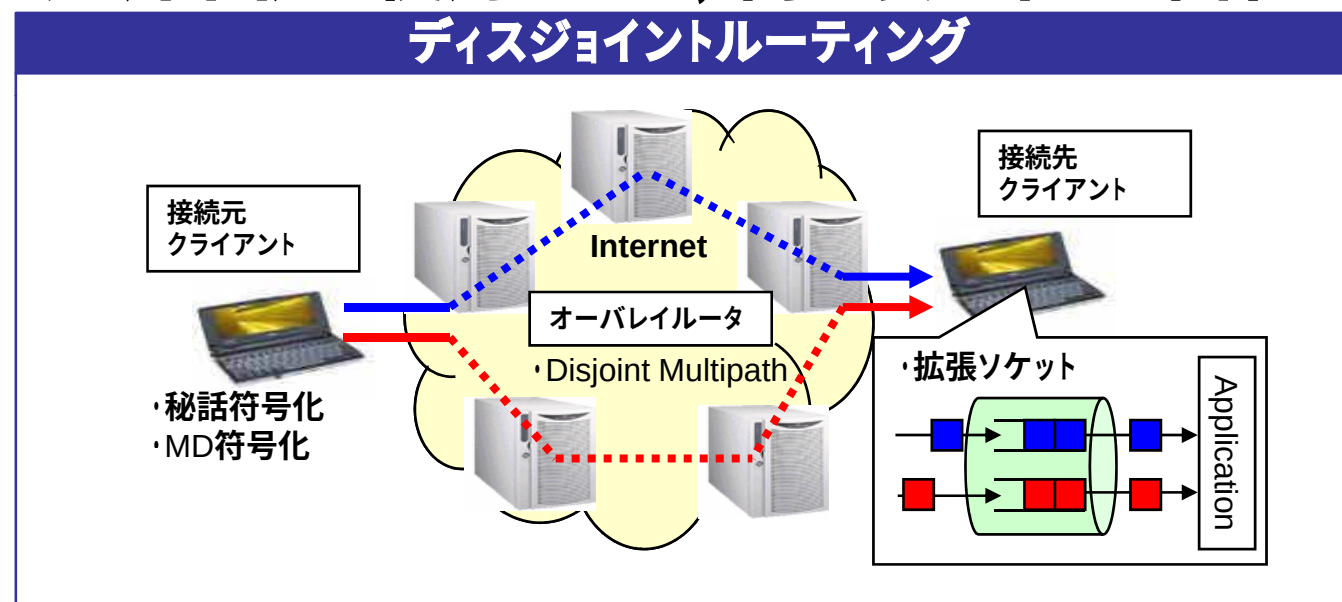


- 1ビットオーディオ信号の3 out of 3 秘密分散
原音



秘密分散通信の提案

- マルチパスルーティングと秘密分散法を併用した通信システムが構成可能
 - n 個の分散情報を, それぞれ n 個の通信路で送信
 - 暗号解読のためには複数回線で同期した盗聴が必須
 - 各経路で異なる鍵による暗号化行えば, より高い秘匿性も実現可能
 - 完全に経路を分離したディスジョイント型マルチパスルーティング (下図) の使用により, 高い安全性を確保

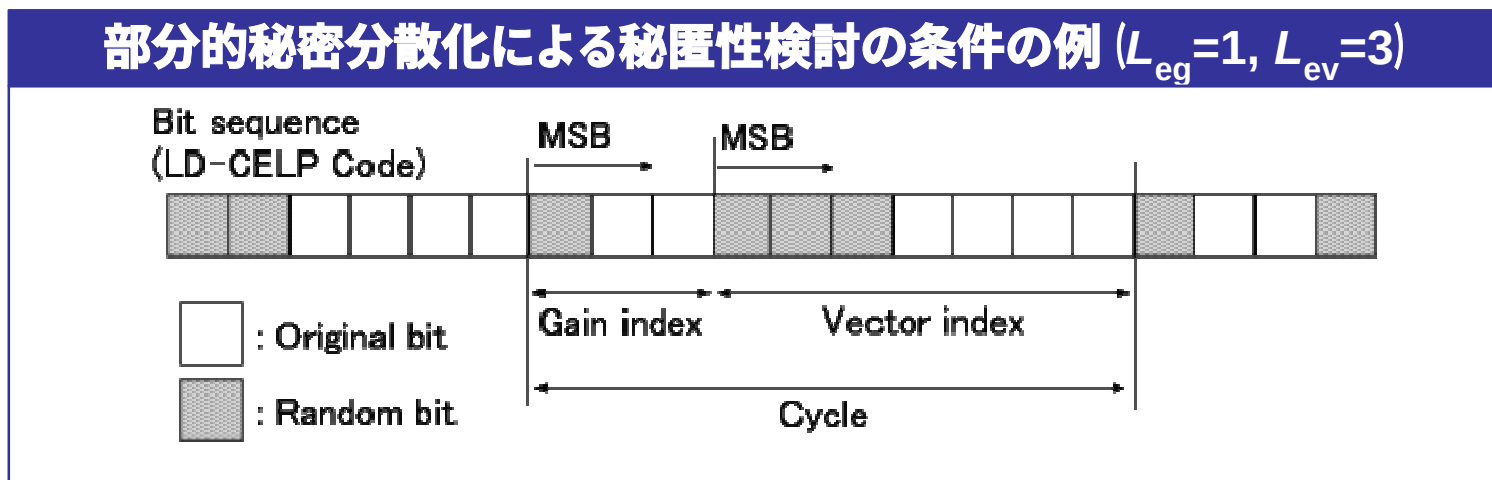


秘密分散による情報量増大への対処

- **秘密分散通信のデメリット**
 - 情報量(ネットワークリソース)の増大
 - Shamirらの提案した秘密分散法で n 倍に伝送量が増大
- **伝送量増大を低減した秘密分散通信方式が必要**
 - 「部分的秘密分散」の提案
 - 波形の一部が漏えいしたとしても、音声の内容が漏洩しないように、音声符号の一部に対して秘密分散を施す
 - 残る符号は平文のまま通信を行う
 - 本プロジェクトで検討した符号
 - CS-ACELP(8 kbps) VoIPで良く用いられている
 - LD-CELP(16 kbps) 符号の構造が単純
 - ADPCM (32kbps) PHSで広くもちいられている

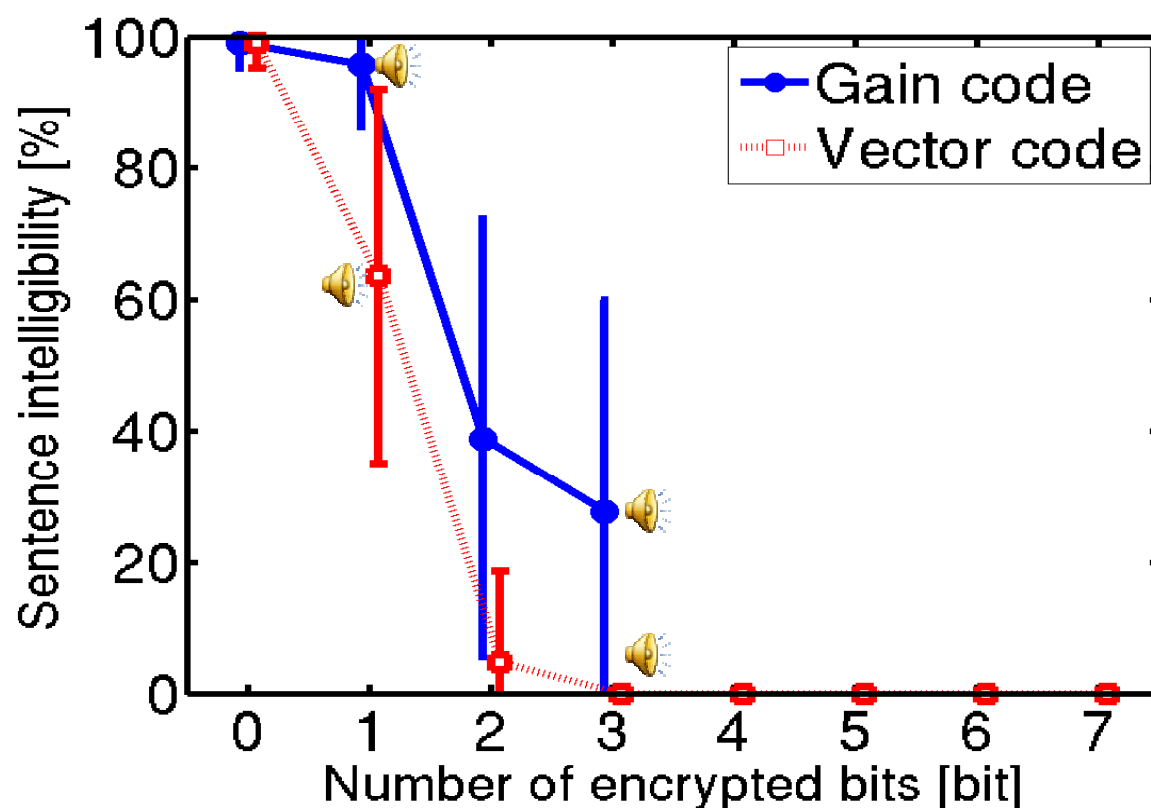
分散秘匿化対象符号の検討(LD-CELPの場合)

- 符号の構造が単純だが、圧縮率は低い (16 kbps)
 - 5 サンプル波形ベクトルをコードブックにより符号化
 - 基底ベクトルコードブック: 7 bit
 - 基底励振ゲイン: 3 bit
 - $10 \text{ bit} \times 8 \text{ kHz} / 5 \text{ サンプル} = 16 \text{ kbps}$
- 符号のどの部分を分散対象とすれば良いか
 - 秘匿性の変化を聴取実験により調べる
 - ベクトルコードの上位何bitか (L_{ev}) とゲインの上位何bitか (L_{eg})



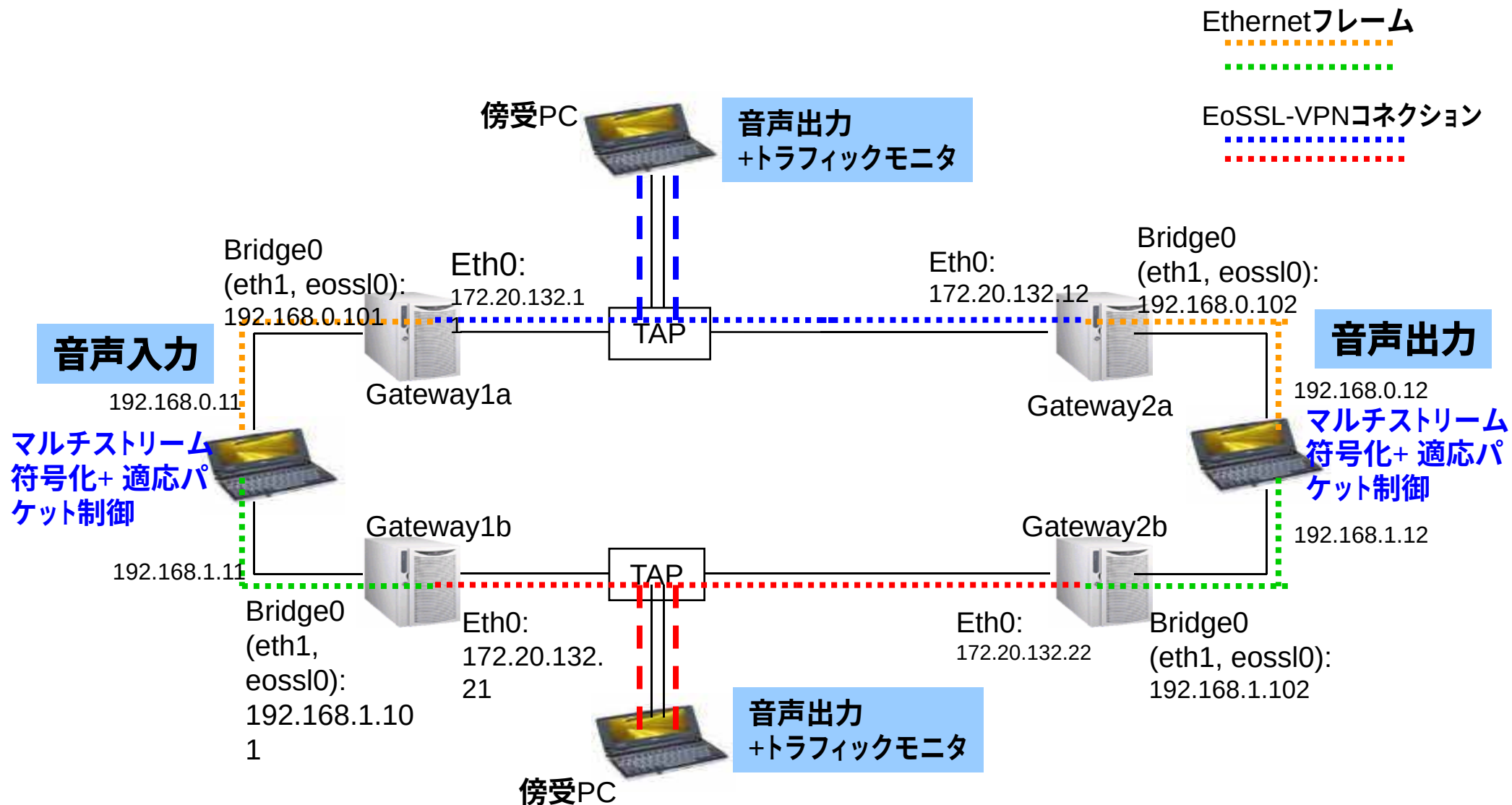
実験結果(LD-CELP符号の場合)

- 盗聴者が聞き取れる音声内容を定量的に評価
 - 各文章中のキーワードの正答率 (文章理解度) で評価
 - ベクトルコード符号 (10 bitsのうち3 bits) のみを部分的秘密分散の対象とすることによって, 高い秘匿性が実現可能



当初の目標 (理解度10%以下) を超える成果を達成

方式実証デモシステムの構成



まとめ

- **高信頼性と高性能，頑健性を有する，音声・音楽信号のネットワーク通信技術を開発。目標を超える成果を得た。**
 - **誰もが安心して利用できる通信技術の実現に一步貢献**
- **実績のまとめ**
 - **査読付き論文誌論文： 5編**
 - **国際学会議事録論文： 11編**
 - **学会口頭発表： 32件**
 - **受賞： 1件 (IIH-MSP2007 Best Paper Award)**
 - **特許： 学内申請3件，出願2件**
 - **報道発表2件 (いずれも日経新聞の科学技術欄に掲載)**
 - **秘密共有分散に基づくCELP音声秘話通信システム (H19年1月24日)**
 - **IPネットワークリアルタイム音楽ストリーミング方式 (H19年3月23日)**