デ高作17－２－６

地上デジタル放送方式高度化の限定受信方式に関する中間報告

概要

2022年10月11日

一般社団法人 電波産業会
デジタル放送システム開発部会
権利保護作業班／アクセス制御方式作業班

中間報告の内容／検討状況

- 限定受信方式検討の前提となる基本方針（検討済）

- スクランブルサブシステム（検討中）
  1. 暗号アルゴリズム
  2. スクランブル手順
  3. スクランブルの範囲
  4. スクランブル方式に係る伝送制御信号

基本方針

- 権利保護作業班／アクセス制御方式作業班で策定した、限定受信方式の技術的条件を検討する際の基本方針

① 地上デジタルテレビジョン放送方式高度化におけるサービス要件が現時点で決まっていないため、関連情報サブシステムについては議論せず、スクランブルサブシステムのみを検討する。

② 新4K8K衛星放送で採用されているスクランブル方式をベースに検討するが、諸外国の標準化動向を踏まえ、通信で用いられているスクランブル方式の採用可否についても検討する。

③ 暗号方式については、現時点での安全性だけでなく将来を見据えた安全性を考慮する。

④ 受信機コストや現行放送システムとの互換性確保などの実現可能性についても考慮する。

検討方式の概要

- スクランブルサブシステム

項目	検討方式
暗号アルゴリズム	検討中 ・法令や民間規格ではAESとCamelliaの両方を規定（運用で1方式に絞る） ・鍵長の変更（現行の128ビットにするか、192ビットまたは256ビットにするか）
スクランブル手順	検討中 ・CTRモード※1とCBCモード※2の両方を規定
スクランブルの範囲	検討中 ・MMTPパケットのMMTPペイロードのデータ部またはCMAF※3
スクランブル方式に係る伝送制御信号	検討中 ・スクランブル方式記述子 ・メッセージ認証方式記述子

※1 CTR (Counter)モード: 「カウンタ」と呼ばれる値を暗号化することで鍵ストリームブロックを生成し、平文ブロックとXOR演算することにより暗号化する方式

※2 CBC (Cipher Block Chaining)モード: 平文の各ブロックを前の暗号文とXOR演算することにより暗号化する方式

※3 CMAF (Common Media Application Format): 低遅延で HTTP ストリーミングを実現するフォーマット

検討方式の特徴と選定理由

- スクランブルサブシステム
  1. 暗号アルゴリズム：AESとCamelliaいずれかを選択または切替
     - CRYPTRECの電子政府推奨暗号リストから選定（基本方針②）
     - 鍵長の変更も検討中（量子計算機による暗号技術の危殆化対策）（基本方針③）
  2. スクランブル手順：CTRモードとCBCモードの両方を規定
     - 放送・通信両方に対応（共用受信機を想定）（基本方針②）
  3. スクランブルの範囲： MMTPパケットのMMTPペイロードのデータ部またはCMAF
     - 多重化方式が「MMT・TLV方式」「CMAF・MMT・TLV方式」いずれの場合でも対応可能となるように、詳細を検討中（基本方針②）
  4. スクランブル方式に係る伝送制御信号：スクランブル方式記述子、メッセージ認証方式記述子
     - 暗号アルゴリズムの切り替え、パケットの改ざん検知について、必要性も含めて検討中（基本方針②）

要求条件への適合性

- スクランブルサブシステム

要求条件	検討方式による適合性
高度な秘匿性を有すること	CRYPTRECの電子政府推奨暗号リストからAESとCamelliaを暗号アルゴリズムとして選定（検討中）
不正受信に対して十分な安全性を有し、脆弱性が発見された場合等に対応できる機能を有すること	スクランブル方式に脆弱性が発見された場合に対応可能とするため、送信側でスクランブル方式の暗号アルゴリズムを指定できる仕組みを導入（検討中）

まとめと今後の作業

- 基本方針
  - 限定受信方式の技術的条件を検討する際の基本方針を策定
- スクランブルサブシステム
  - 技術検討の結果を報告

- 今後の作業
  - 技術的条件の詳細検討
    - 中間報告ではスクランブルサブシステムに限定して議論しており、その他の要求条件（サイバーセキュリティなど）に関する検討は最終報告までの課題とする

参考資料

- スクランブル方式の動向
  - 世界的にISO BMFF※4対応が進んでいる
  - 通信で標準的なスクランブル方式CENC※5が一部の放送システムで採用されている

諸外国の方式	ATSC3.0（米国）	ATSC3.0（韓国）	DVB	Google（Widevine CAS）
スクランブル対象	ISO BMFF	ISO BMFF	MPEG2-TS／PES	MPEG2-TS、ISO BMFF
スクランブル方式（暗号方式）	CENC (AES)	CENC (AES)	DVB-CSA (AES等)	各放送方式にカスタマイズ対応

日本方式	地上（B-CAS方式）	地上（TRMP方式）	新4K8K衛星放送
スクランブル対象	MPEG2-TS		MMTPパケット
スクランブル方式（暗号方式）	告示 (MULTI-2)		告示 (AES／Camellia)

※4 ISO BMFF (ISO Base Media File Format): MPEG-4 Part12で定義されているメディアファイルのコンテナフォーマット
※5 CENC (MPEG Common Encryption): 複数のDRMで暗号化コンテンツを共通化することが可能なスクランブル方式

参考資料

- スクランブル方式の動向
  - 通信のストリーミングでは、暗号利用モードの対応がDRM※6毎に分かれており、CTRモードだけでなくCBCモードの採用も進んでいる

DRM	AES-CTRモード	AES-CBCモード
Widevine (Google)	○	○
FairPlay (Apple)	×	○
PlayReady (Microsoft) V4.0以降	○	○
PlayReady (Microsoft) V1.0～3.3	○	×
WisePlay (Huawei)	○	○

    - CTRモードの特徴
      - 暗号化・復号ともに並列処理可能なため、多量のデータを高速に暗号化・復号できる
    - CBCモードの特徴
      - 復号のみ並列処理可能

※6 DRM (Digital Rights Management): コンテンツの著作権を保護し、その利用や複製を制限する技術

参考資料

- 量子計算機による暗号技術の危殆化
  - 将来大規模な量子計算機が出現すると、既存の暗号方式が危殆化（安全でなくなる）
    - AESやCamelliaなどの共通鍵暗号方式は、量子計算機を用いると鍵の全数探索を高速に実行可能なアルゴリズムが知られている
    - 長期的に保護したいデータには、鍵長128ビットの暗号方式ではなく、192ビットや256ビットの暗号技術を使用するのが賢明である※7

※7 https://www.cryptrec.go.jp/exreport/cryptrec-ex-2901-2019.pdf
CRYPTREC 外部評価報告書（2019年度）「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」エグゼクティブサマリー