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

超高精細度テレビジョン放送システムに関する中間報告（限定受信方式）

第１章　概要

超高精細度テレビジョン放送の限定受信方式について、情報通信審議会放送システム委員会（以下、情通審と記す。）による要求条件および関連して整理した要件を踏まえ、スクランブルサブシステムと関連情報サブシステムに関する技術検討を行った。

スクランブルサブシステムについては、情通審からの要求条件に基づいて、複数の暗号アルゴリズムから選択可能とする方式とし、多重化レベルで暗号アルゴリズムを指定する記述子などを導入することとした。具体的には、暗号アルゴリズムは、CRYPTREC で公表されている電子政府推奨暗号リストを参考に、鍵長 128 ビットの AES ブロック暗号および同鍵長の Camellia ブロック暗号から選択可能とした。また、スクランブル方式の暗号アルゴリズムを指定する記述子としてスクランブル方式記述子を導入するとともに、MMT･TLV 方式においては、通信利用を考慮してメッセージ認証方式記述子を採用した。

関連情報サブシステムについては、現行の方式と同等のサービス・機能が実現できることなどの要件が出されたことから、アクセス制御機能は現行の 3 重鍵方式を採用し、関連情報を構成する情報は共通情報として ECM、および個別情報として EMM とした。さらに、関連情報サブシステムに対する要求条件（安全性の維持・改善）のために、新たに、放送や通信を使って関連情報の処理に関わる受信機側のソフトウェアを更新する技術手段について整理し、その送出方式について検討した。

用語・略語

ECM	Entitlement Control Message
EMM	Entitlement Management Message
CBC	Cipher Block Chaining
OFB	Output FeedBack
CTR	Counter
DCM	Download Control Message
DMM	Download Management Message

第 2 章　限定受信方式の要件

2.1　情報通信審議会放送システム委員会で示された要求条件

（スクランブルサブシステム）

- 高度な秘匿性を有すること。
- 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可能な機能を有すること。

（関連情報サブシステム）

[アクセス制御機能に関する事項]

- 種々のサービス形態に対応するため、課金・収納方式などに自由度があり、弾力的な運用が可能であること。
- 関連情報は可能な限り共通の形式によること。
- 個々の受信者へ向けた情報の伝送・表示が可能であること。
- 関連情報の配布は、効率的で正確、確実なものであること。
- 各認定基幹放送事業者の運用の独立性が確保できること。

[安全性の維持・改善および拡張性に関する事項（その他）]

- 関連情報伝送や限定受信機能に関して十分な安全性を有し、その安全性を継続的に維持・改善できること。
- 新規関連情報サブシステムへの更新や拡張性を考慮すること。

2.2　広帯域伝送における限定受信方式の要件

2.1 に示す要求条件を踏まえ、広帯域伝送における限定受信方式の要件を下記のとおり検討・整理した。

（関連情報サブシステム）

[アクセス制御機能に関する事項]

- 現行の方式と同等のサービス・機能が実現できること。
- RMP として利用する際に、十分な安全性が確保されていること。
- 関連情報が放送波以外でも送信できるように考慮すること。
- 契約者／非契約者へのコミュニケーションツールが用意されていること（自動表示メッセージ）。
- 関連情報の暗号化においては、関連情報の内容を知り、又は改変することが容易でなく、かつ短期間で暗号化方式の変更が必要とならないこと。
- 複数事業者が、それぞれのサービスに適した（異なる）方式を他の事業者へ影響を与えることなく同時に運用できること。

[安全性の維持・改善および拡張性に関する事項（その他）]

- 関連情報伝送や限定受信機能において十分な安全性を有し、その安全性を継続的に維持・改善で

きること。

- 暗号化の安全性を継続的に維持・改善できること。
- 限定受信システムとして、安全性を継続的に維持・改善できること。
- 関連情報サブシステムは、セキュリティが破られた場合の対策手段を持ち、その対策手段は、技術的、経済的に容易に実現できること。
- 万が一セキュリティが破られた場合においても、その影響を限定できる工夫が施されていること。更に、セキュリティが破られた場合の対策手段が備えられており、その対策手段は、技術的かつ経済的に容易に実施できること。
- 次世代放送・新サービスへの対応（拡張性）を考慮すること。
- 関連情報サブシステムは、サービスの拡張や受信者への情報伝送機能の追加・変更が可能なこと。その手段は、技術的、経済的に容易に実施できること。
- 関連情報サブシステムの実装として、専用ハードウェアを前提としない方式であること。
- 受信機の保守、サービスモードの改ざんや大規模リコールなどで、セキュリティの低下や事業者の放送運用へ影響を与えないこと。

2.3　要求条件への適合

（スクランブルサブシステム）

<table>
<tr><th>要求条件（情報通信審議会）</th><th>限定受信方式の要件</th><th>検討結果</th><th>適合</th></tr>
<tr><td>高度な秘匿性を有すること。</td><td rowspan="2">情報通信審議会の要求条件に同じ。</td><td>AES（鍵長 128 ビット）ブロック暗号、Camellia（鍵長 128 ビット）ブロック暗号への移行することを提案する。</td><td rowspan="2">（情報通信審議会）
本報告書 3.1、3.2、3.3 に以下を記載する。
・AES、Camellia の各暗号アルゴリズム等と、選定にあたっての留意事項
・暗号アルゴリズムを指定できるスクランブルサブシステム（CAT/CA メッセージ、暗号ブロック図等を含む）</td></tr>
<tr><td>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可能な機能を有すること。</td><td>スクランブル方式記述子を規定し、暗号アルゴリズムを指定できる仕組みを導入する。</td></tr>
</table>

（関連情報サブシステム：[アクセス制御機能に関する事項]）

要求条件（情報通信審議会）	限定受信方式の要件	検討結果	適合
・関連情報は可能な限り共通の形式によること。 ・個々の受信者へ向けた情報の伝送・表示が可能であること。 ・関連情報の配布は、効率的で正確、確実なものであること。 ・各認定基幹放送事業者の運用の独立性が確保できること。 ・種々のサービス形態に対応するため、課金・収納方式などに自由度があり、弾力的な運用が可能であること。	・現行の方式と同等のサービス・機能が実現できること。 ・RMP として利用する際に、十分な安全性が確保されていること。 ・関連情報が放送波以外でも送信できるように考慮すること。 ・契約者／非契約者へのコミュニケーションツールが用意されていること（自動表示メッセージ）。 ・関連情報の暗号化においては、関連情報の内容を知り、又は改変することが容易でなく、かつ短期間で暗号化方式の変更が必要とならないこと。 ・複数事業者が、それぞれのサービスに適した（異なる）方式を他の事業者へ影響を与えることなく同時に運用できること。	・現行の 3 重鍵方式を提案する。 ・柔軟度が高い関連情報（ECM、EMM）のフォーマットを導入する。	（情報通信審議会） 本報告書 3.4.1 に以下を記載する。 ・現行の 3 重鍵方式の採用と、関連情報を構成する情報（ECM および EMM） （民間規格等） ECM および EMM の具体的な詳細については、今後民間規格等で策定する。

（関連情報サブシステム：[安全性の維持・改善および拡張性に関する事項（その他）]）

要求条件（情報通信審議会）	限定受信方式の要件	検討結果	適合
・関連情報伝送や限定受信機能に関して十分な安全性を有し、その安全性を継続的に維持・改善できること。 ・新規関連情報サブシステムへの更新や拡張性を考慮すること。	・関連情報伝送や限定受信機能において十分な安全性を有し、その安全性を継続的に維持・改善できること。 ・暗号化の安全性を継続的に維持・改善できること。 ・限定受信システムとして、安全性を継続的に維持・改善できること。 ・関連情報サブシステムは、セキュリティが破られた場合の対策手段を持ち、その対策手段は、技術的、経済的に容易に実現できること。 ・万が一セキュリティが破られた場合においても、その影響を限定できる工夫が施されていること。更に、セキュリティが破られた場合の対策手段が備えられており、その対策手段は、技術的かつ経済的に容易に実施できること。 ・次世代放送・新サービスへの対応（拡張性）を考慮すること。 ・関連情報サブシステムは、サービスの拡張や受信者への情報伝送機能の追加・変更が可能なこと。その手段は、技術的、経済的に容易に実施できること。	・安全性の維持改善の手段としては、①受信機側でハードウェアを更新する更新手段、②受信機側で記録媒体などを使ってソフトウェアを更新する更新手段、③放送や通信を使ってソフトウェアを更新する更新手段の3つに大別でき、このうち、放送や通信を使って安全にソフトウェアを更新する更新手段について提案する。	（情報通信審議会） 本報告書 3.4.2 に以下を記載する。 ・放送や通信を使って安全にソフトウェアを更新する送出側の技術手段 （民間規格等） 送出に係るテーブルの具体的な詳細、および受信機実装や運用に関する部分については、今後民間規格等や運用検討の場において検討する。

要求条件（情報通信審議会）	限定受信方式の要件	検討結果	適合
	・関連情報サブシステムの実装として、専用ハードウェアを前提としない方式であること。 ・受信機の保守、サービスモードの改ざんや大規模リコールなどで、セキュリティの低下や事業者の放送運用へ影響を与えないこと。	・上記提案と独立に検討が可能である。	（民間規格等） 受信機実装や運用に関する部分は、今後民間規格等や運用検討の場において検討する。

第 3 章　広帯域伝送における限定受信方式

3.1　拡張 MPEG-2 TS 方式におけるスクランブルサブシステム

拡張 MPEG-2 TS 方式のスクランブルサブシステムにおいて、スクランブルの範囲およびスクランブルの対象に関しては、現行方式との整合性を考慮して、デジタル放送の標準方式（平成 23 年総務省令第 87 号）第 8 条第 1 号、第 2 号に準拠するものとする。

スクランブル方式の暗号アルゴリズムに関しては、高度な秘匿性を確保するために、現行デジタル放送で採用されている MULTI2 ではなく、セキュリティ強度がより高い複数の暗号アルゴリズムから選択できることが適当である。

3.1.1　スクランブル方式の暗号アルゴリズム

スクランブル方式で使用する暗号アルゴリズムの評価にあたっては、CRYPTREC（Cryptography Research and Evaluation Committees：電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト）で公表されている電子政府推奨暗号リスト ※1 を参考にした。この電子政府推奨暗号リストは、最新・最先端の暗号解析結果を基にして、専門家により安全性評価、実装評価および利用実績の評価が行われ、推奨暗号としてまとめられたもので、暗号アルゴリズムの選定にあたっては大きな指標となる。

この CRYPTREC では、64 ビットブロック暗号から 128 ビットブロック暗号への移行が推奨されており、現行のデジタルテレビジョン放送で採用されている暗号方式 MULTI2（64 ビットブロック暗号）は、除外した。また、現行のデジタルテレビジョン放送では、ブロック暗号が採用されており、これまでのシステム運用のノウハウなどを有効活用できる観点から、現行方式と同様にブロック暗号を前提とした。

以上を踏まえ、スクランブル方式で使用する暗号アルゴリズムは、CRYPTREC の電子政府推奨暗号リストから次の 2 つのブロック暗号を選択可能とすることが適当である。

※1：http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2013.pdf　電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）

(1)　AES 128 ビットブロック暗号　（米国政府標準暗号）

- 安全性 ※2：
  電子政府推奨暗号リストにも採用されており、新たな暗号解析手法が発見されない限り、数十年に亘り十分商用に耐えると考えられる。なお、現段階で、関連鍵攻撃や中間一致攻撃などの暗号解析手法に関する研究報告があるものの、現実的な脅威ではなく、実用上問題ないと考えられる。
- 性能評価 ※3※4：
  処理速度に関して、4K および 8K のストリームを十分に処理できるレベルにあると考えられる。
- 国際標準化 ※5：
  ISO/IEC 18033-3、NESSIE、IETF （TLS、IPsec、S/MIME、PGP、Kerberos）、IEEE などで広く採用されている。
- 利用実績 ※5：

利用実績が十分であり、今後も安定的に利用可能である。

(2) Camellia 128 ビットブロック暗号 （国産暗号）

・ 安全性 ※2：
電子政府推奨暗号リストにも採用されており、新たな暗号解析手法が発見されない限り、数十年に亘り十分商用に耐えると考えられる。なお、現時点では、安全性の問題に関する報告は無い。

・ 性能評価 ※3※4：
処理速度に関して、4K および 8K のストリームを十分に処理できるレベルにあると考えられる。

・ 国際標準化 ※5：
ISO/IEC 18033-3、NESSIE、IETF (TLS、IPsec、S/MIME、PGP、Kerberos)などで広く採用されている。

・ 利用実績 ※5：
利用実績が十分ではないが、今後の利用促進の可能性が高いと考えられる。

※2：http://www.cryptrec.go.jp/report/c12_sch_web.pdf　CRYPTREC Report 2012「暗号方式委員会報告」 P.32（要約）

※3：http://www.cryptrec.go.jp/report/c02.pdf　暗号技術評価報告書(2002 年度版）CRYPTREC Report 2002　P.143

※4：https://www.ipa.go.jp/files/000024409.pdf　「電子政府推奨暗号の実装」評価報告書　P.5

※5：http://www.cryptrec.go.jp/report/c12_opr_web.pdf　CRYPTREC Report 2012「暗号運用委員会報告」

【スクランブル方式の暗号アルゴリズムの選定にあたっての留意事項】

スクランブル方式の暗号アルゴリズムの選定にあたっては、以下の各項に留意することが望ましい。

・ スクランブル方式は、暗号アルゴリズム自身の安全性だけではなく、受信機における実装面、コスト面、および実用化スケジュール、ならびに、長期にわたってセキュリティリスクを抑える送出運用などに考慮して、民間規格や運用検討の場において、放送事業者や受信機製造メーカなどの関係者で最終的に選定する必要がある。

・ 長期視点で見ると、より効率的な暗号解析手法が見つかる可能性も否定できない。CRYPTREC の電子政府推奨暗号リストの改定など、暗号アルゴリズムの最新動向に今後留意する必要があり、民間規格や運用検討の場において、必要に応じて、議論・検討する必要がある。

3.1.2　スクランブル手順

スクランブル手順に関して、現行規定と同様に暗号利用モードは CBC+OFB モードとする。

3.1.2.1　AES 暗号を用いたスクランブル手順

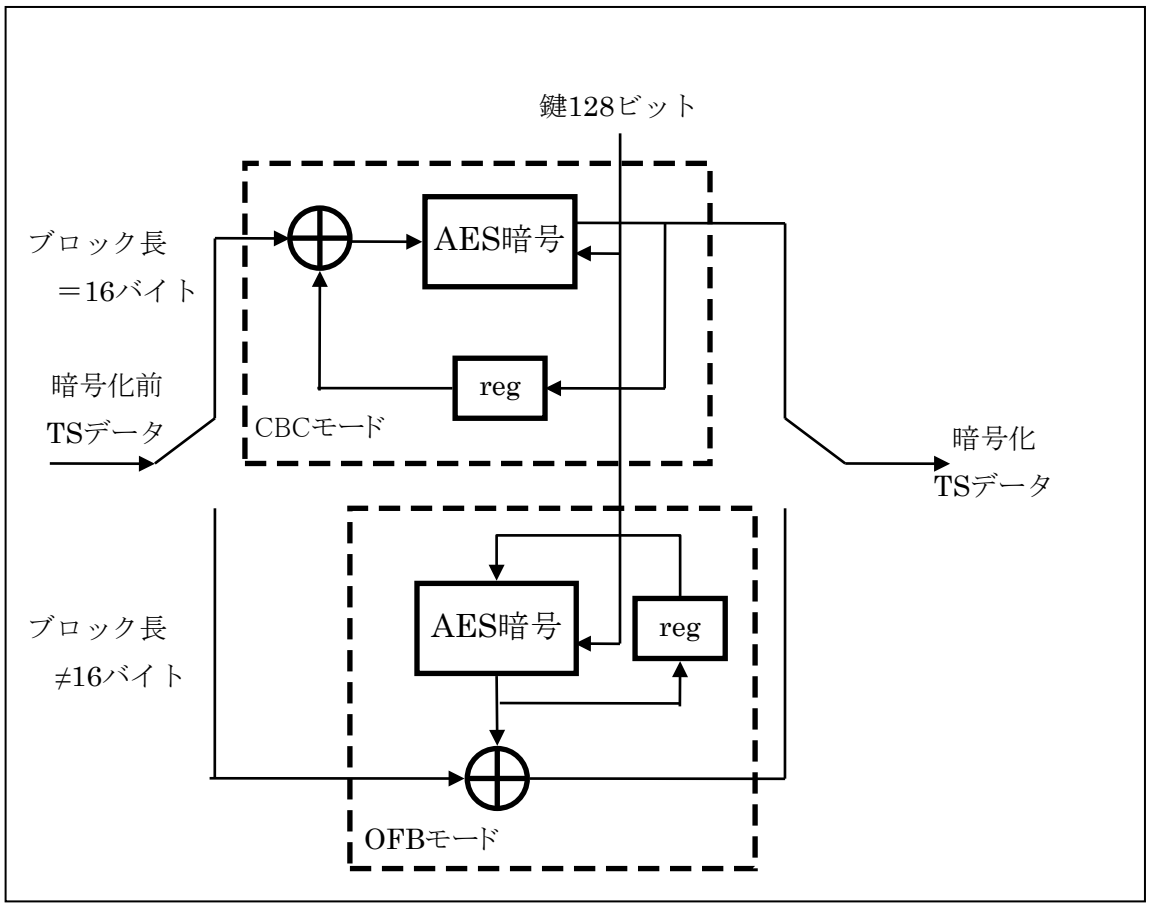


図 1

3.1.2.2　Camellia 暗号を用いたスクランブル手順

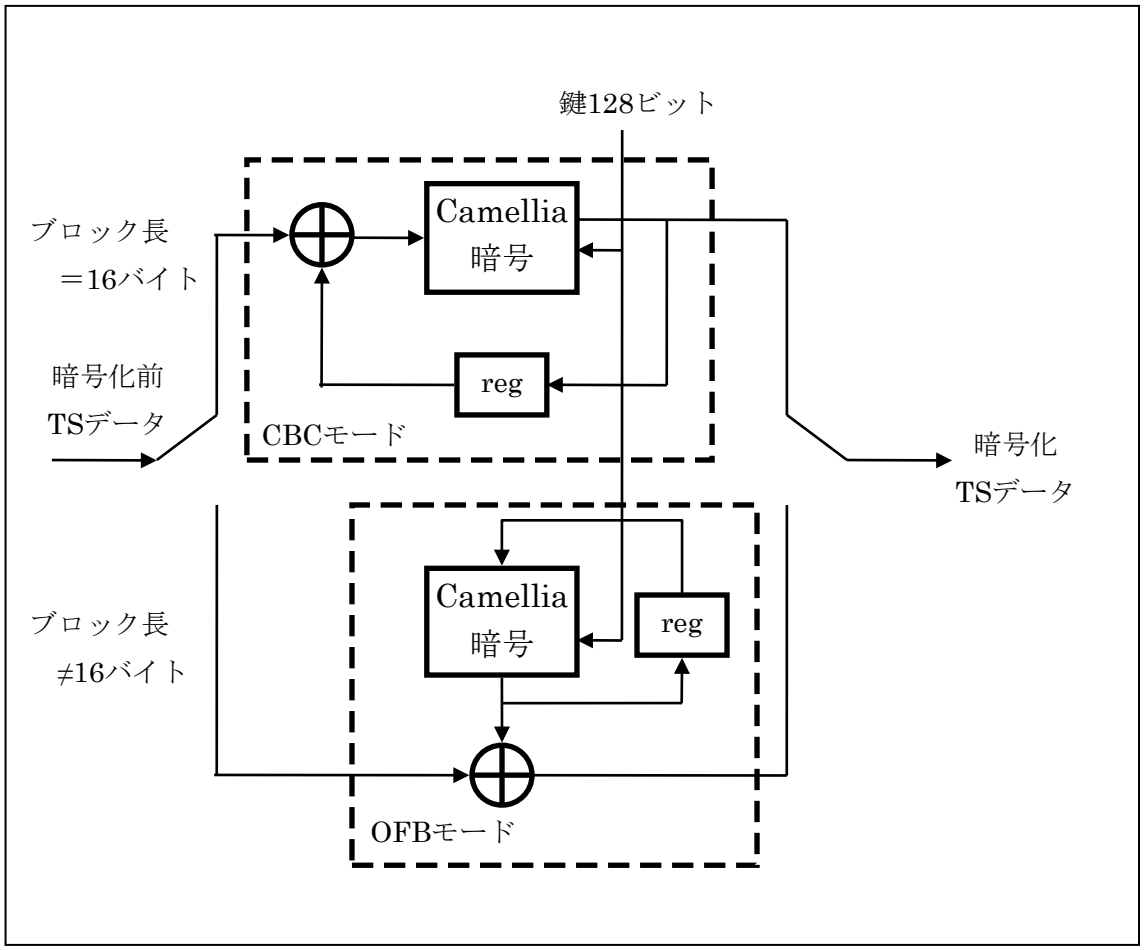


図 2

3.1.3　スクランブルの範囲

スクランブルの範囲は、TS パケット（伝送制御信号、及び、関連情報を送るためのものを除く）のペイロード部分とする。

3.1.4　スクランブル方式に係る伝送制御信号

スクランブル方式に脆弱性が発見された場合において対応可能とするために、スクランブル方式の暗号アルゴリズムを指定する記述子（以下、スクランブル方式記述子という。）を新たに規定する。スクランブル方式記述子は、平成 23 年総務省告示第 299 号別表第 20 号で規定の伝送制御信号に配置可能な記述子とする。

記述子タグ	記述子長	スクランブル方式識別子	データ
8	8	8	8×N

注 1）記述子タグの値は、スクランブル方式記述子を示す 0xXX とする。

注 2）記述子長は、これより後に続くデータバイト数を書き込む領域とする。

注 3）スクランブル方式識別子は、スクランブル時の暗号アルゴリズムの種別を示す。

注 4）本記述子は、CAT の記述子領域又は PMT の記述子 1 若しくは記述子 2 の領域で伝送するものとする。

図 3：スクランブル方式記述子の構成

表 1：スクランブル方式識別子の値の割当て

値（2 進数）	割当て
00000000	未定義
00000001	AES、鍵長 128 ビット
00000010	Camellia、鍵長 128 ビット
00000011 - 11111111	未定義

3.2　MMT・TLV 方式におけるスクランブルサブシステム

MMT・TLV 方式では、コンテンツ伝送のために MMT パケットおよび IP パケットを用いる。そのため、スクランブルサブシステムにおいては、MMT パケットおよび IP パケット双方のスクランブル方式について規定する。MMT パケットに関しては、MMT パケット（制御メッセージを除く）のペイロード部とする。IP パケットに関しては、IP パケットのペイロード部とする。

スクランブル方式の暗号アルゴリズムに関しては、高度な秘匿性を確保するために、現行デジタル放送で採用されている MULTI2 ではなく、セキュリティ強度がより高い複数の暗号アルゴリズムから選択できることが適当である。

3.2.1　スクランブル方式の暗号アルゴリズム

3.1.1 に同じ。

3.2.2　スクランブル手順

スクランブル手順に関しては、MMT パケットおよび IP パケットが可変長パケットであり、また、パケットサイズが比較的大きいこと考慮して、暗号利用モードを CTR モードとする。

3.2.2.1　AES 暗号を用いたスクランブル手順

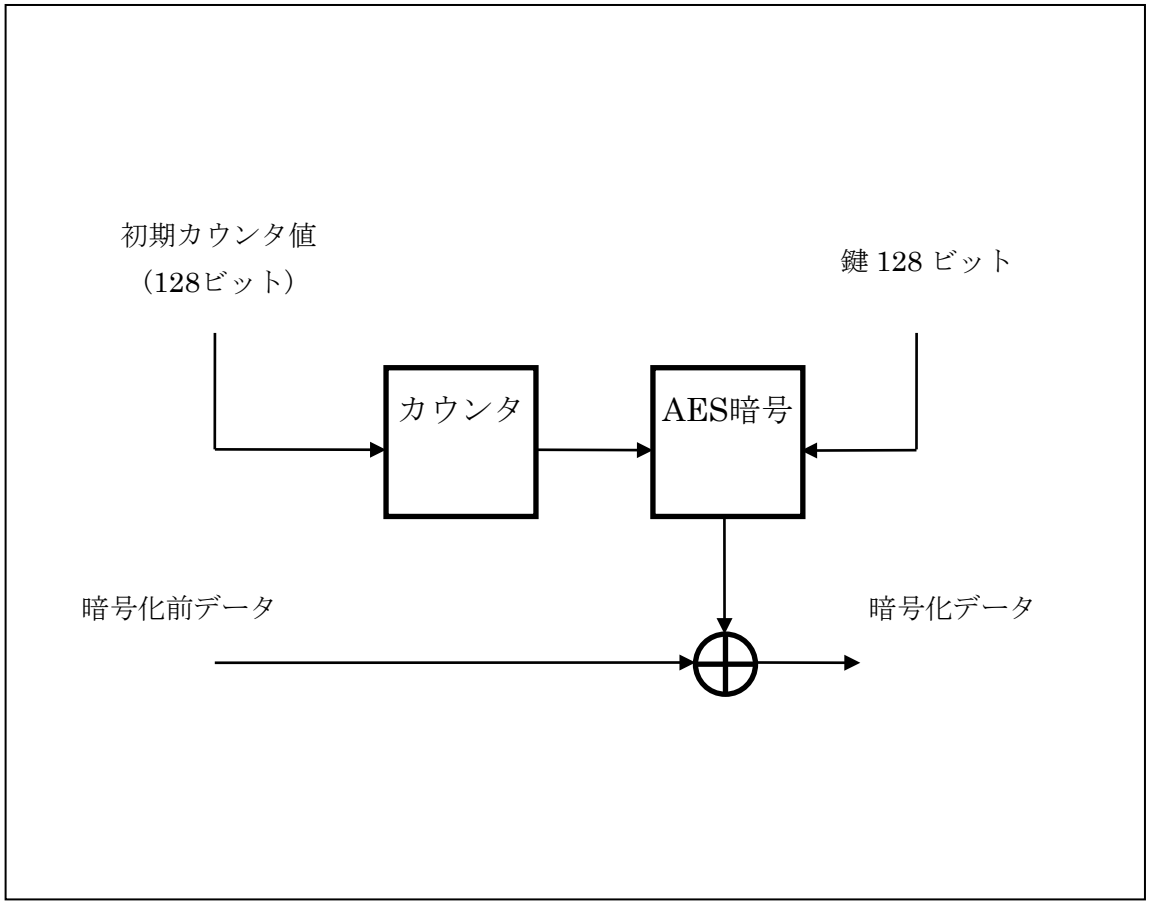


図 4

3.2.2.2　Camellia 暗号を用いたスクランブル手順

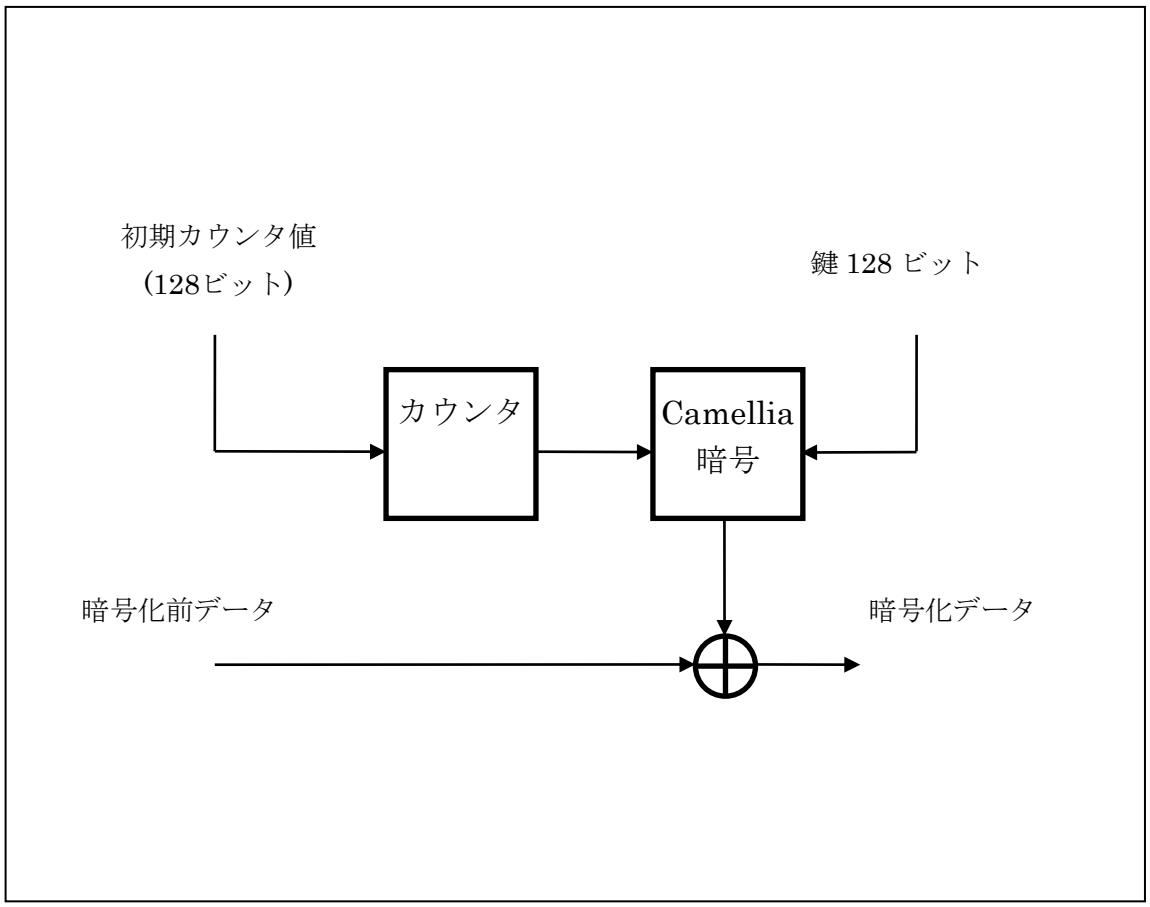


図 5

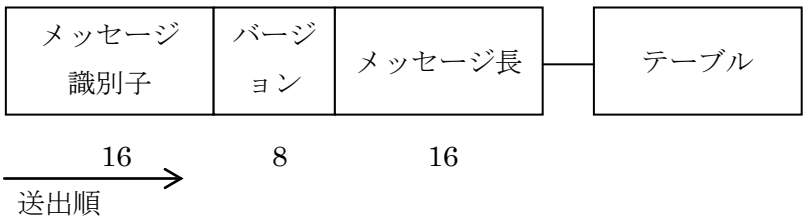
3.2.3　スクランブルの範囲

スクランブルの範囲は、MMT パケット（制御メッセージを除く）のペイロード部および IP パケットのペイロード部とする。

3.2.4　スクランブル方式に係る伝送制御信号

限定受信方式の識別のために、図 6(a)に示す伝送制御信号（CA メッセージ）に配置される CA テーブル（図 6(b)）に配置可能な記述子として、アクセス制御記述子（図 7）を導入する。また、スクランブルサブシステムの識別のために、伝送制御信号に配置可能な記述子として、スクランブル方式記述子（図 8）を導入する。

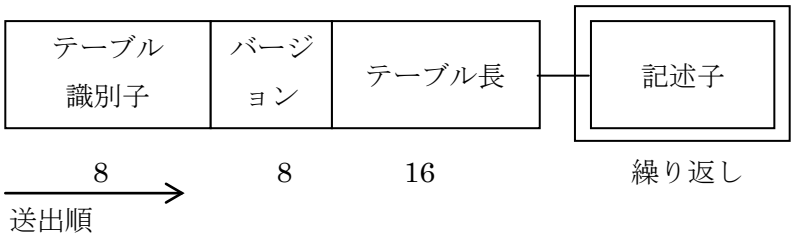
MMT・TLV 方式においては、放送と通信を組み合わせたコンテンツ配信を行うことから、パケットの改ざんを防止できるメッセージ認証方式（改ざん検出のために、パケット単位にメッセージ認証コードを付与する仕組み）を導入する。そのメッセージ認証方式を識別するメッセージ認証方式記述子（図 9）を規定する。ただし、メッセージ認証方式記述子が配置されない場合は、メッセージ認証を行わない（メッセージ認証コードが付加されない）ことを示す。なお、放送で映像音声のコンポーネントを配信し、通信で字幕データ等のコンポーネントを配信するケースも想定されるが、通信で配信されるコンポーネントに関しては、コンテンツ保護のために、各種 DRM などを適用することも想定される。この場合、必要に応じて、各記述子の拡張領域に各種 DRM に関するセキュリティ情報を記述することも想定されるが、その詳細は、事業者任意規格とする。



注 1）メッセージ識別子の値は、CA メッセージを示す 0xXXXX とする。

注 2）テーブル領域には、CA テーブルが配置される。

図 6(a)：CA メッセージの構成



注 1）テーブル識別子の値は、CA テーブルを示す 0xXX とする。

図 6(b)：CA テーブルの構成

記述子タグ	記述子長	限定受信 方式識別子	MMT_general_location_info	データ
16	8	16		8×N

注 1）記述子タグの値は、アクセス制御記述子を示す 0xXXXX とする。

注 2）記述子長は、これより後に続くデータバイト数を書き込む領域とする。

注 3）限定受信方式識別子は、限定受信方式の種別を示す。

注 4）MMT_general_location_info は、MMT で定義されるロケーション情報である。アクセス制御記述子にある MMT_general_location_info は、関連情報を含む MMT パケットのロケーションを示す。

注 5）本記述子は、CA メッセージの CA テーブルの記述子領域又は MP テーブルの MPT ディスクリプタ領域若しくは MP テーブルのアセットディスクリプタ領域で伝送するものとする。

図 7：アクセス制御記述子の構成

記述子タグ	記述子長	対象レイヤ ー識別子	“111111”	スクランブル 方式識別子	データ
16	8	2	6	8	8×N

注 1）記述子タグの値は、スクランブル方式記述子を示す 0xXXXX とする。

注 2）記述子長は、これより後に続くデータバイト数を書き込む領域とする。

注 3）対象レイヤー識別子は、スクランブル時の暗号化対象（IP パケット、MMT パケット）を示す。

注 4）スクランブル方式識別子は、スクランブル時の暗号アルゴリズムの種別を示す。

注 5）本記述子は、CA メッセージの CA テーブルの記述子領域又は MP テーブルの MPT ディスクリプタ領域若しくは MP テーブルのアセットディスクリプタ領域で伝送するものとする。

図 8：スクランブル方式記述子の構成

記述子タグ	記述子長	対象レイヤー識別子	“111111”	メッセージ認証方式識別子	データ
16	8	2	6	8	8×N

注 1）記述子タグの値は、メッセージ認証方式記述子を示す 0xXXXX とする。

注 2）記述子長は、これより後に続くデータバイト数を書き込む領域とする。

注 3）対象レイヤー識別子は、MMT パケットまたは IP パケットの改ざん検出を行うメッセージ認証の対象（IP パケット、MMT パケット）を示す。

注 4）メッセージ認証方式識別子は、MMT パケットまたは IP パケットの改ざん検出を行うメッセージ認証方式の種別を示す。

注 5）本記述子は、CA メッセージの CA テーブルの記述子領域又は MP テーブルの MPT ディスクリプタ領域若しくは MP テーブルのアセットディスクリプタ領域で伝送するものとする。

図 9：メッセージ認証方式記述子の構成

表 2：スクランブル方式識別子の値の割当て

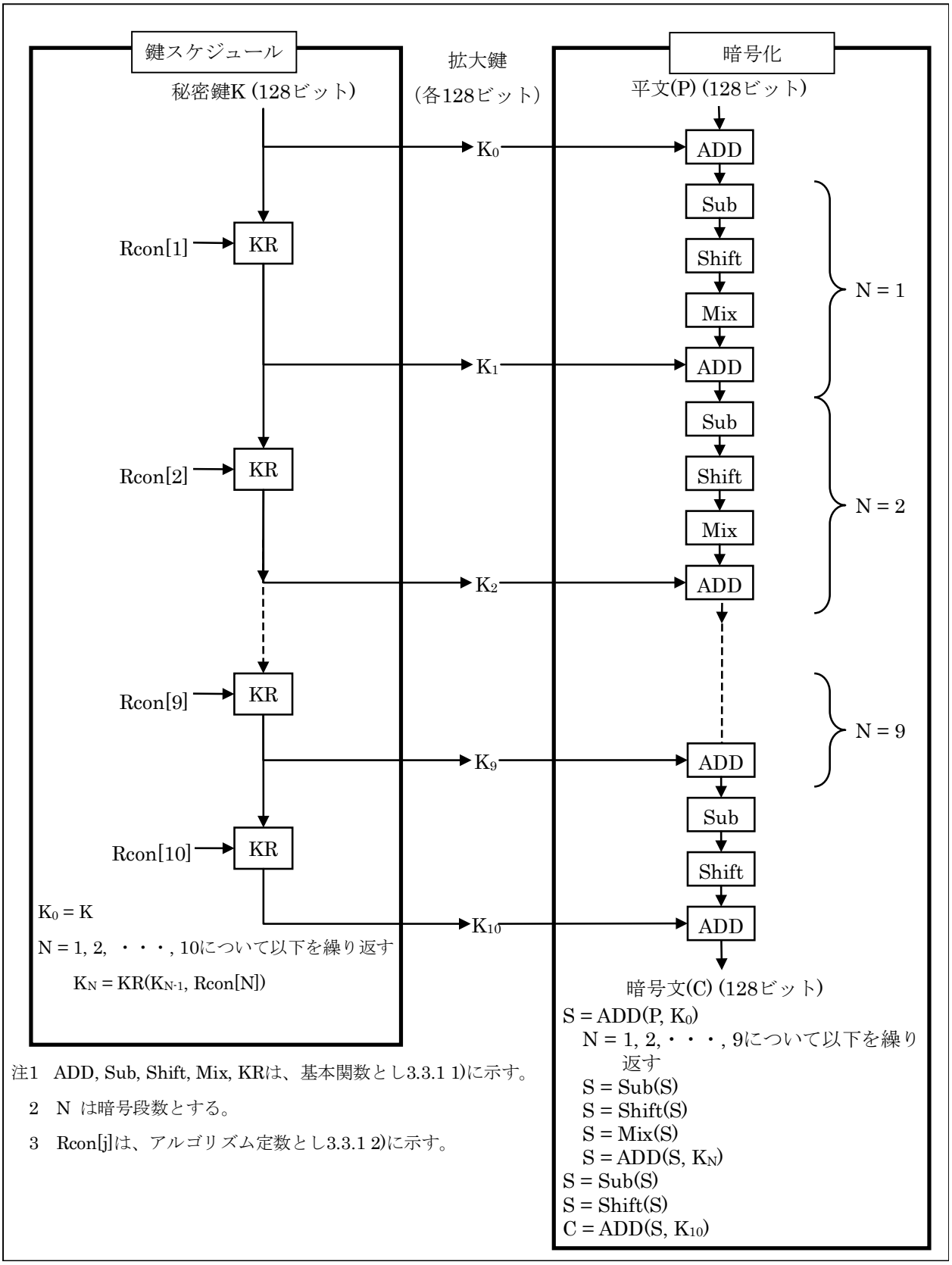
値（2 進数）	割当て
00000000	未定義
00000001	AES、鍵長 128 ビット
00000010	Camellia、鍵長 128 ビット
00000011 - 11111111	未定義

表 3：対象レイヤー識別子の値の割当て

値（2 進数）	割当て
00	未定義
01	MMT パケットを対象
10	IP パケットを対象
11	未定義

3.3　スクランブルサブシステムにおける暗号アルゴリズムの詳細

3.3.1　AES 暗号



注1　ADD, Sub, Shift, Mix, KRは、基本関数とし3.3.1 1)に示す。

2　N は暗号段数とする。

3　Rcon[j]は、アルゴリズム定数とし3.3.1 2)に示す。

図 10

1）基本関数

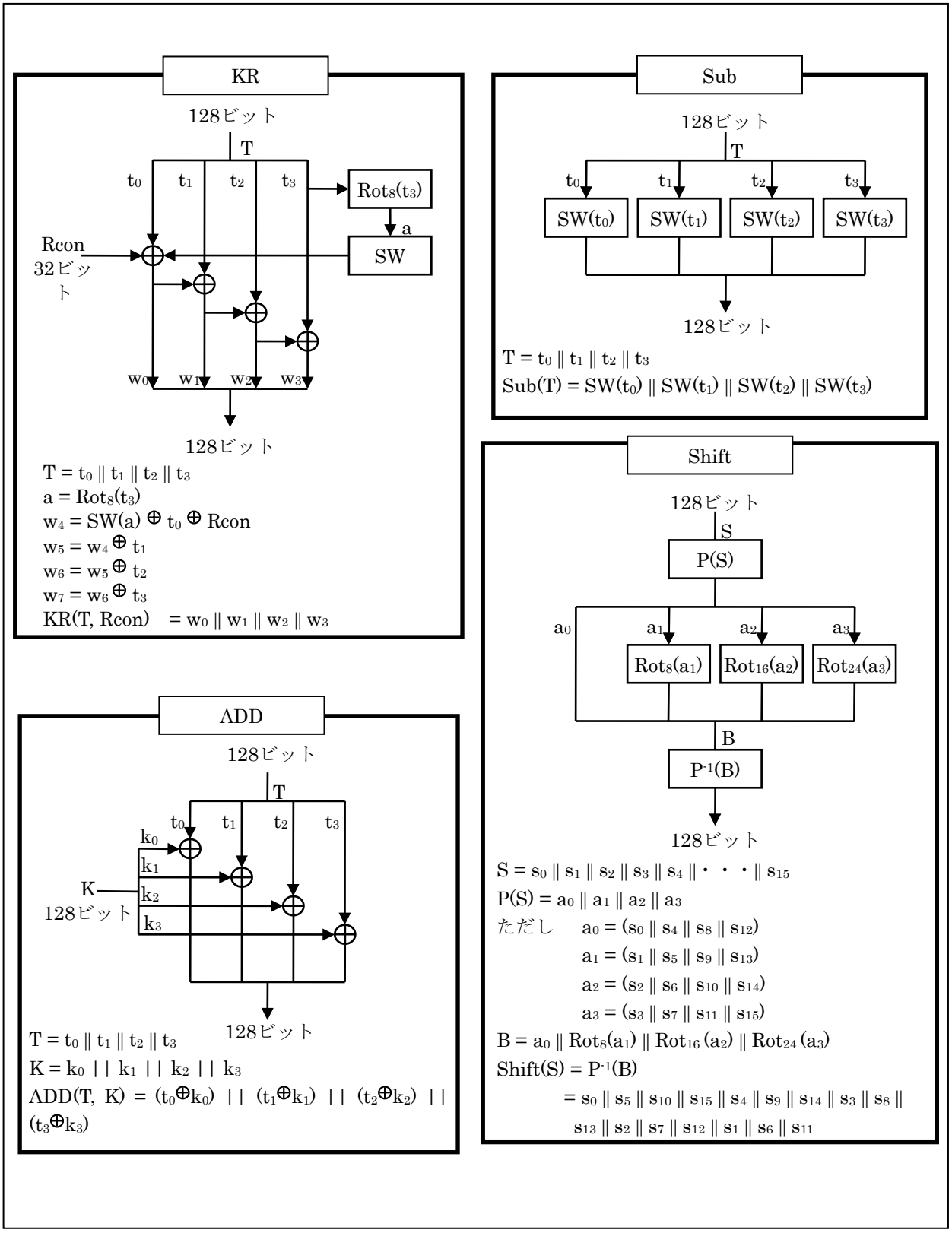
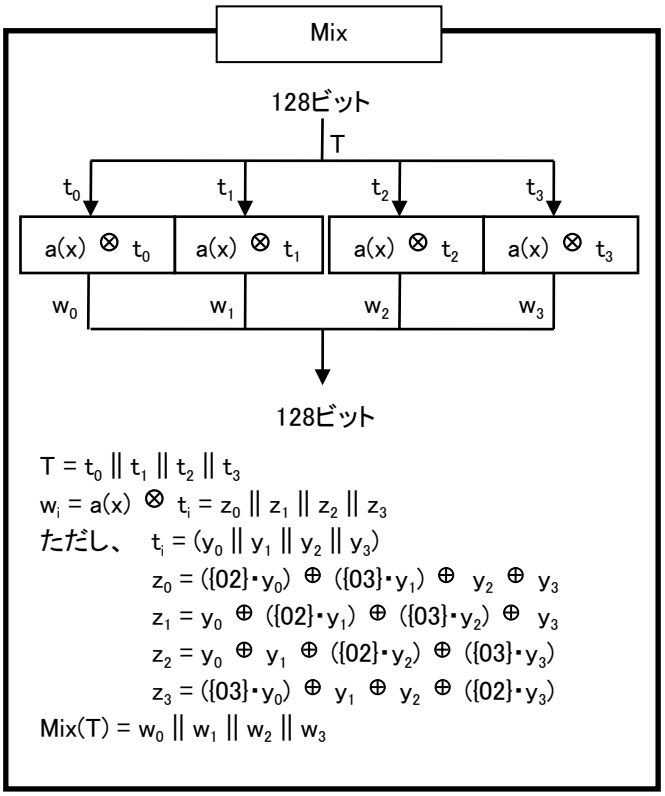

KR
128ビット
T
t0 t1 t2 t3
Rot8(t3)
a
SW
Rcon
32ビット
w0 w1 w2 w3
128ビット
T = t0 || t1 || t2 || t3
a = Rot8(t3)
w4 = SW(a) ⊕ t0 ⊕ Rcon
w5 = w4 ⊕ t1
w6 = w5 ⊕ t2
w7 = w6 ⊕ t3
KR(T, Rcon) = w0 || w1 || w2 || w3
Sub
128ビット
T
t0 t1 t2 t3
SW(t0) SW(t1) SW(t2) SW(t3)
128ビット
T = t0 || t1 || t2 || t3
Sub(T) = SW(t0) || SW(t1) || SW(t2) || SW(t3)
Shift
128ビット
S
P(S)
a0 a1 a2 a3
Rot8(a1) Rot16(a2) Rot24(a3)
B
P-1(B)
128ビット
S = s0 || s1 || s2 || s3 || s4 || ・・・|| s15
P(S) = a0 || a1 || a2 || a3
ただし a0 = (s0 || s4 || s8 || s12)
a1 = (s1 || s5 || s9 || s13)
a2 = (s2 || s6 || s10 || s14)
a3 = (s3 || s7 || s11 || s15)
B = a0 || Rot8(a1) || Rot16 (a2) || Rot24 (a3)
Shift(S) = P-1(B)
= s0 || s5 || s10 || s15 || s4 || s9 || s14 || s3 || s8 ||
s13 || s2 || s7 || s12 || s1 || s6 || s11
ADD
128ビット
T
t0 t1 t2 t3
k0 k1 k2 k3
K
128ビット
128ビット
T = t0 || t1 || t2 || t3
K = k0 || k1 || k2 || k3
ADD(T, K) = (t0⊕k0) || (t1⊕k1) || (t2⊕k2) || (t3⊕k3)

図 11

注1　Tは、基本関数への入力とする。
2　⊕は、ビット毎の排他的論理和とする。
3　‖ は、ブロックの結合とする。
4　SWは、補助関数とし3.3.1 2)に示す。
5　Rot_n は、左巡回nビットシフトとする。
6　・は、GF(2^8)上の乗算を表す。
既約多項式は、
$x^8 + x^4 + x^3 + x + 1$とする。



$T = t_0 \| t_1 \| t_2 \| t_3$
$w_i = a(x) \otimes t_i = z_0 \| z_1 \| z_2 \| z_3$
ただし、 $t_i = (y_0 \| y_1 \| y_2 \| y_3)$
$z_0 = (\{02\}\cdot y_0) \oplus (\{03\}\cdot y_1) \oplus y_2 \oplus y_3$
$z_1 = y_0 \oplus (\{02\}\cdot y_1) \oplus (\{03\}\cdot y_2) \oplus y_3$
$z_2 = y_0 \oplus y_1 \oplus (\{02\}\cdot y_2) \oplus (\{03\}\cdot y_3)$
$z_3 = (\{03\}\cdot y_0) \oplus y_1 \oplus y_2 \oplus (\{02\}\cdot y_3)$
$Mix(T) = w_0 \| w_1 \| w_2 \| w_3$

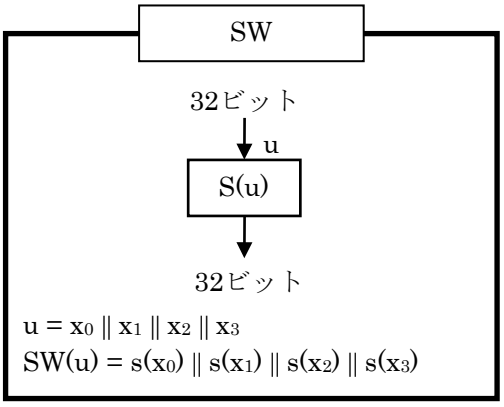
図 12

2）アルゴリズム定数と補助関数

アルゴリズム定数

Rcon[1] = 01000000
Rcon[2] = 02000000
Rcon[3] = 04000000
Rcon[4] = 08000000
Rcon[5] = 10000000
Rcon[6] = 20000000
Rcon[7] = 40000000
Rcon[8] = 80000000
Rcon[9] = 1b000000
Rcon[10] = 36000000
注　数値は16進表記とする。

補助関数

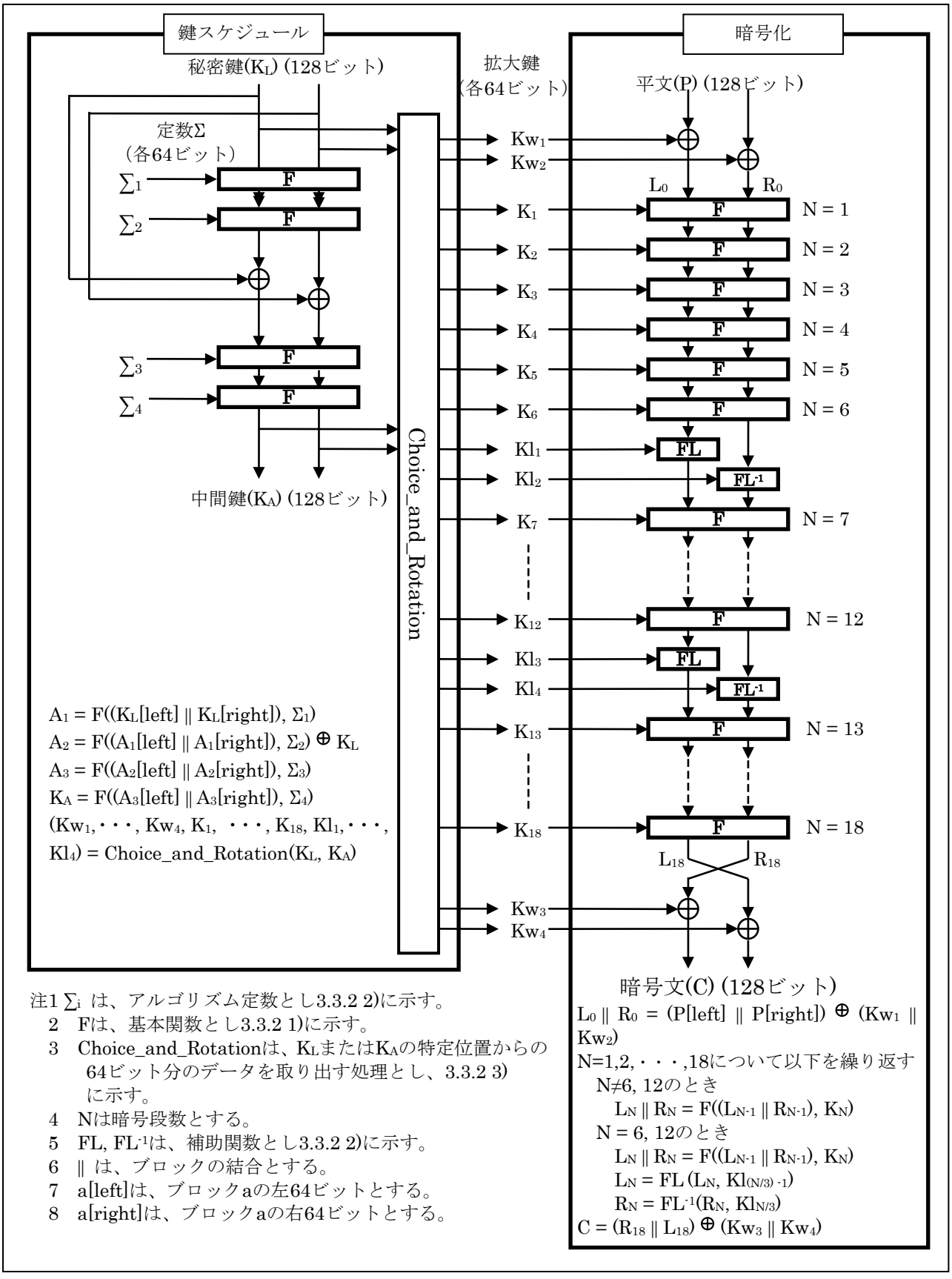


$u = x_0 \| x_1 \| x_2 \| x_3$
$SW(u) = s(x_0) \| s(x_1) \| s(x_2) \| s(x_3)$

注1　u は、補助関数への入力とする。
2　‖ は、ブロックの結合とする。
3　s は、8ビットの置換表とし、詳細はISO/IEC 18033-3 に従うものとする。

図 13

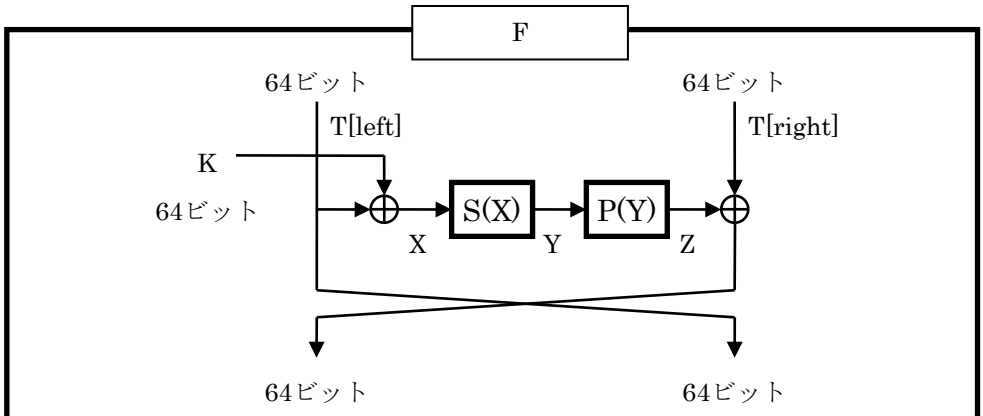
3.3.2 Camellia 暗号



注1 $\sum_i$ は、アルゴリズム定数とし3.3.2 2)に示す。
2 Fは、基本関数とし3.3.2 1)に示す。
3 Choice_and_Rotationは、K_LまたはK_Aの特定位置からの64ビット分のデータを取り出す処理とし、3.3.2 3)に示す。
4 Nは暗号段数とする。
5 FL, FL^{-1}は、補助関数とし3.3.2 2)に示す。
6 || は、ブロックの結合とする。
7 a[left]は、ブロックaの左64ビットとする。
8 a[right]は、ブロックaの右64ビットとする。

図 14

1）基本関数



$X = T[left] \oplus K = (x_8 \| x_7 \| x_6 \| x_5 \| x_4 \| x_3 \| x_2 \| x_1)$

$Y = S(X) = (s_1(x_8) \| s_4(x_7) \| s_3(x_6) \| s_2(x_5) \| s_4(x_4) \| s_3(x_3) \| s_2(x_2) \| s_1(x_1))$

$= (y_8 \| y_7 \| y_6 \| y_5 \| y_4 \| y_3 \| y_2 \| y_1)$

$Z = P(Y) = (z_8 \| z_7 \| z_6 \| z_5 \| z_4 \| z_3 \| z_2 \| z_1)$

ただし

$z_1 = y_1 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7 \oplus y_8$

$z_2 = y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_7 \oplus y_8$

$z_3 = y_1 \oplus y_2 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_8$

$z_4 = y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7$

$z_5 = y_1 \oplus y_2 \oplus y_6 \oplus y_7 \oplus y_8$

$z_6 = y_2 \oplus y_3 \oplus y_5 \oplus y_7 \oplus y_8$

$z_7 = y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_8$

$z_8 = y_1 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7$

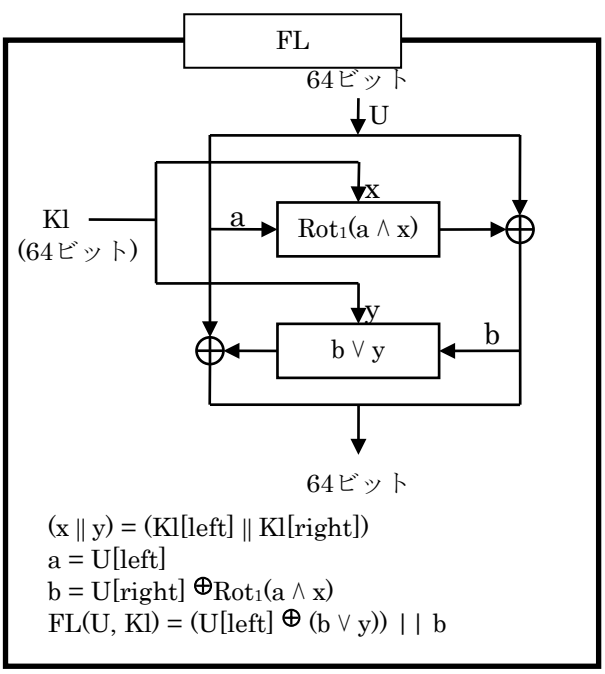
$F(T, K) = (T[right] \oplus Z) \| T[left]$

注1　Tは、基本関数への入力とする。
2　T[left]は、ブロックTの左64ビットとする。
3　T[right]は、ブロックTの右64ビットとする。
4　‖ は、ブロックの結合とする。
5　s_i は、8ビットの置換表とし、詳細はISO/IEC18033-3:2005(E) 5.2.3.4節に従うこととする。

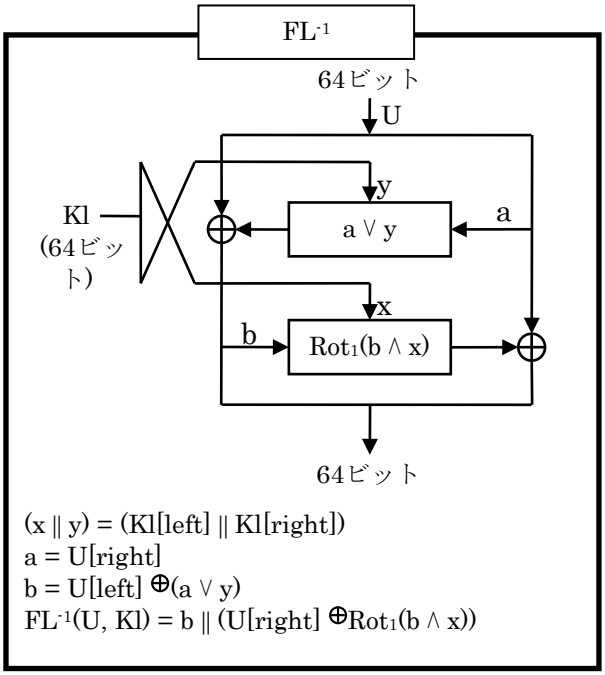
図 15

2）補助関数とアルゴリズム定数

補助関数



(x ‖ y) = (Kl[left] ‖ Kl[right])
a = U[left]
b = U[right] ⊕Rot_1(a ∧ x)
FL(U, Kl) = (U[left] ⊕ (b ∨ y)) ‖ b



(x ‖ y) = (Kl[left] ‖ Kl[right])
a = U[right]
b = U[left] ⊕(a ∨ y)
FL^{-1}(U, Kl) = b ‖ (U[right] ⊕Rot_1(b ∧ x))

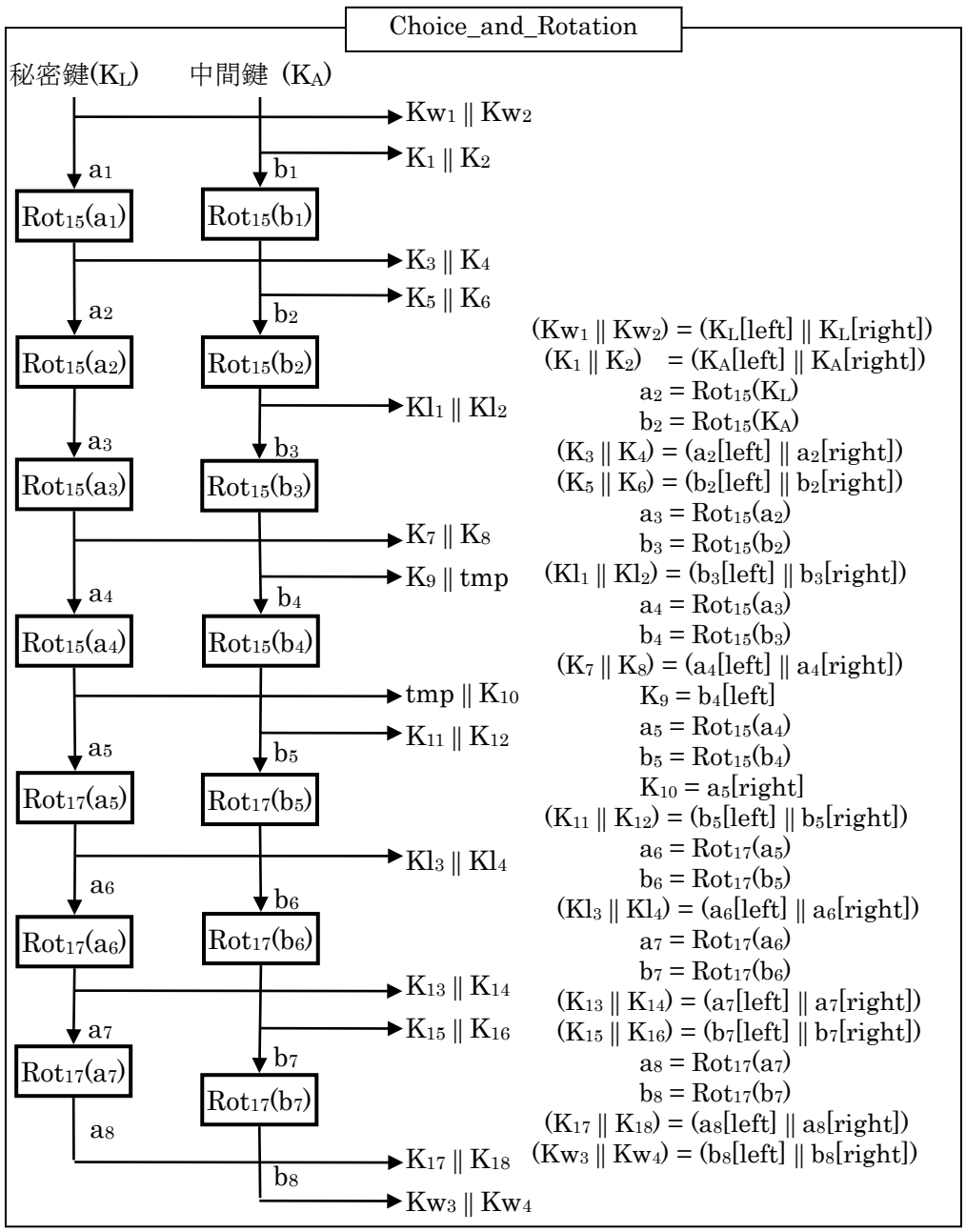
注1　Uは、補助関数への入力とする。
2　‖ は、ブロックの結合とする。
3　Rot_1 は、左巡回1ビットシフトとする。
4　∧ は、ビット毎の論理積とする。
5　∨ は、ビット毎の論理和とする。
6　U[left]は、ブロックUの左32ビットとする。
7　U[right]は、ブロックUの右32ビットとする。

アルゴリズム定数

Σ_1 = a09e667f3bcc908b
Σ_2 = b67ae8584caa73b2
Σ_3 = c6ef372fe94f82be
Σ_4 = 54ff53a5f1d36f1c
注　数値は16進表記とする。

図 16

3）Choice_and_Rotation



注1　U[left]は、ブロックUの左64ビットとする。
　2　U[right]は、ブロックUの右64ビットとする。
　3　 || は、ブロックの結合とする。
　4　Rot_n は、左巡回nビットシフトとする。

図 17

3.4　関連情報サブシステム

3.4.1　アクセス制御機能

関連情報サブシステムのうち、アクセス制御に関わる情報等について、以下の 2 つの方針で検討を行った。

【方針 1】現行の 3 重鍵方式を採用し、関連情報を構成する情報を ECM および EMM とする。

（理由）当作業班で要件を整理した結果、「現行の方式と同等のサービス・機能を実現できること」をはじめとして、関連情報サブシステムの基本的な方式は、現行デジタルテレビジョン放送の限定受信方式で採用されている 3 重鍵方式の枠組みで実現できると考えられる。3 重鍵方式は、現行のデジタル放送で長期間の運用実績があり、方式としてセキュリティ上の問題は特に発見されていない。よって、超高精細度テレビジョン放送においても、3 重鍵方式を採用する。

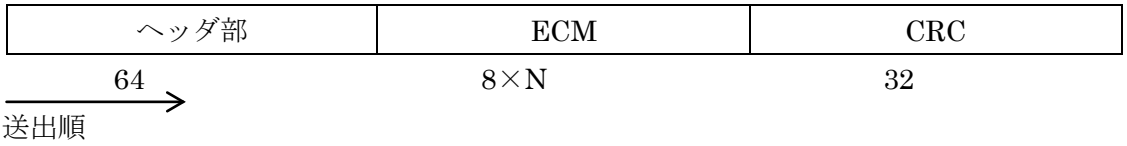
また、現行のデジタル放送では、関連情報を構成する情報として ECM および EMM が規定されており、これについてもそのまま踏襲する。

【方針 2】柔軟度が高い関連情報（ECM、EMM）のフォーマットを規定する。

（理由）当作業班で要件を整理した結果、課金方式の自由度や弾力的な運用に関する要件や、サービスの拡張性に関する要件が出てきた。これらの要件を鑑みると、関連情報サブシステム自体の弾力性や柔軟性を担保するために、ECM および EMM の詳細については、事業者任意仕様とすることが適当と考えられる。

3.4.1.1　ECM の構成及び送出手順

超高精細度テレビジョン放送における関連情報（ECM）の構成及び送出手順を下記に示す。



注 1）単位の指定のない数字は、その領域のビット数を示すものとする。

注 2）各領域は、最上位ビットから最下位ビットの順に伝送するものとする。以下同じ。

注 3）ECM の伝送は、セクション形式のうち拡張形式によるものとする。

注 4）ヘッダ部内の「テーブル識別子」の値は ECM を示す 0xXX または 0xYY とする。

注 5）ECM は、次表に示すものを含む情報により構成されるものとする。なお、暗号鍵識別以外の情報は、暗号鍵識別により識別される暗号鍵を用いて暗号化することができる。

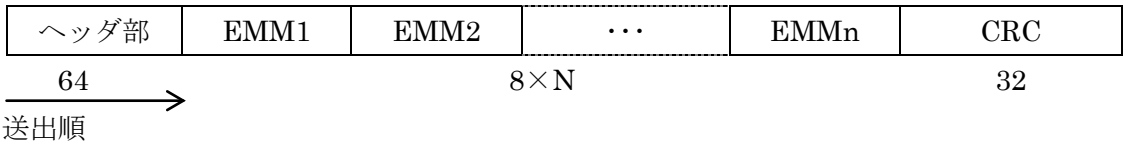
図 18：ECM の構成

表 4

項目
暗号鍵識別
スクランブルの解除に用いる鍵

3.4.1.2　EMM の構成及び送出手順

超高精細度テレビジョン放送における関連情報（EMM）の構成及び送出手順を下記に示す。なお、EMM は、ECM の暗号を解くための鍵情報だけでなく、受信機へメッセージ情報を伝送するための情報（以下「EMM メッセージ」という。）を伝送することも可能とする。EMM メッセージが EMM に含まれる場合の識別については、事業者任意規格とする。



注 1）単位の指定のない数字は、その領域のビット数を示すものとする。

注 2) EMM の伝送は、セクション形式のうち拡張形式によるものとし、その範囲内で、EMM は複数多重できるものとする。

注 3）　ヘッダ部内の「テーブル識別子」の値は EMM を示す 0xXX または 0xYY とする。

注 4）EMM は、次表に示すものを含む情報により構成されるものとする。なお、識別番号以外の情報は、暗号化することができるものとする。

図 19：EMM の構成

表 5

項目
識別番号

3.4.1.3　関連情報の送出方法

ECM および EMM の送出方法に関しては、多重化方式が拡張 MPEG-2 TS 方式の場合は、セクション形式の拡張形式として送出する。MMT・TLV 方式の場合は、前記セクション形式の拡張形式を保ったまま、M2 セクションメッセージとして送出する。

3.4.2　安全性の維持・改善

2.1 および 2.2 のそれぞれ[安全性の維持･改善および拡張性に関する事項（その他）]に示される“安全性の維持・改善”を直接実現する手段は、大別して、受信機側で（ソフトウェアを含む）ハードウェアを更新する更新手段、受信機側で記録媒体などを使ってソフトウェアを更新する更新手段、および放送や通信を使ってソフトウェアを更新する更新手段が考えられる。

これらの更新手段のうち、放送や通信を使って関連情報を処理するソフトウェアを安全に更新する更新手段に関して、放送を用いて事業者が主体的に実施するものであることから、その技術的な詳細を検討した。

3.4.2.1　前提となる想定システム

受信機内で限定受信方式に関わる関連情報を直接処理する機能を CAS プログラムと呼び、CAS プログラム本体はソフトウェアの形態で実装されていることを想定する。CAS プログラムは受信機内に 1 つ以上存在することを想定し、いずれかの CAS プログラムを放送および通信を使って安全に更新する技術方式と関連する方式（以下、総称してダウンローダブル CAS 方式という。）とする。スクランブルサブシステムを提案方式で更新することは想定しない。

また、CAS プログラムは、受信機ソフトウェアとは独立に放送事業者が運用することを前提に、受信機ソフトウェアのダウンロードとは独立に管理・更新が行われるものとする。なお、CAS プログラム本体がどのような機能を有するのかなど、CAS プログラムの仕様については、3.4.1 に示す機能を含むものとし、その詳細については、今後民間規格等で定めるものとする。

3.4.2.2　システム構成

ダウンローダブル CAS 方式のうち、送出側については、主として以下の方式（技術）から構成される。

① CAS プログラム本体の暗号化と電子署名による認証
② 3 重鍵方式によるスクランブル
③ スクランブルを復号するための鍵関連情報のパケット識別子やダウンロード経路（放送経由／通信経由）を指定するなどのダウンロードの告知に関する情報（テーブル）
④ 受信機内に複数ある CAS プログラムから放送事業者が運用する CAS プログラムを指定する記述子

①については、CAS プログラム製作後から受信機内に格納されるまで伝送路（ダウンロード経路）にかかわらず一気通貫で実施されるものである。そのための暗号方式や認証方式については、事業者任意仕様とする。

②については、セキュリティ維持の観点から不正受信機への放送ダウンロードを排除する目的で、送出レベルで提案する。図 20 にその構成を示す。スクランブルの復号に必要な鍵関連情報として、DCM（Download Control Message）と DMM（Download Management Message）を規定する。本項でいうスクランブルは、3.1～3.3 で示されるものとする。

③については、ARIB 標準規格（望ましい仕様）「デジタル放送用受信装置」（ARIB STD-B21）に

規定される SDTT（Software Download Trigger Table）をベースにして機能拡張することを想定するが、その詳細については、今後民間規格等で定めるものとする。

④については､使用する CAS プログラムの ID とバージョン番号を指定する新たな記述子を規定し、CAT（多重化方式が拡張 MPEG-2 TS 方式の場合）または CA メッセージ（多重化方式が TLV・MMT 方式の場合）に記載することを想定するが、その詳細については、今後民間規格等で定めるものとする。

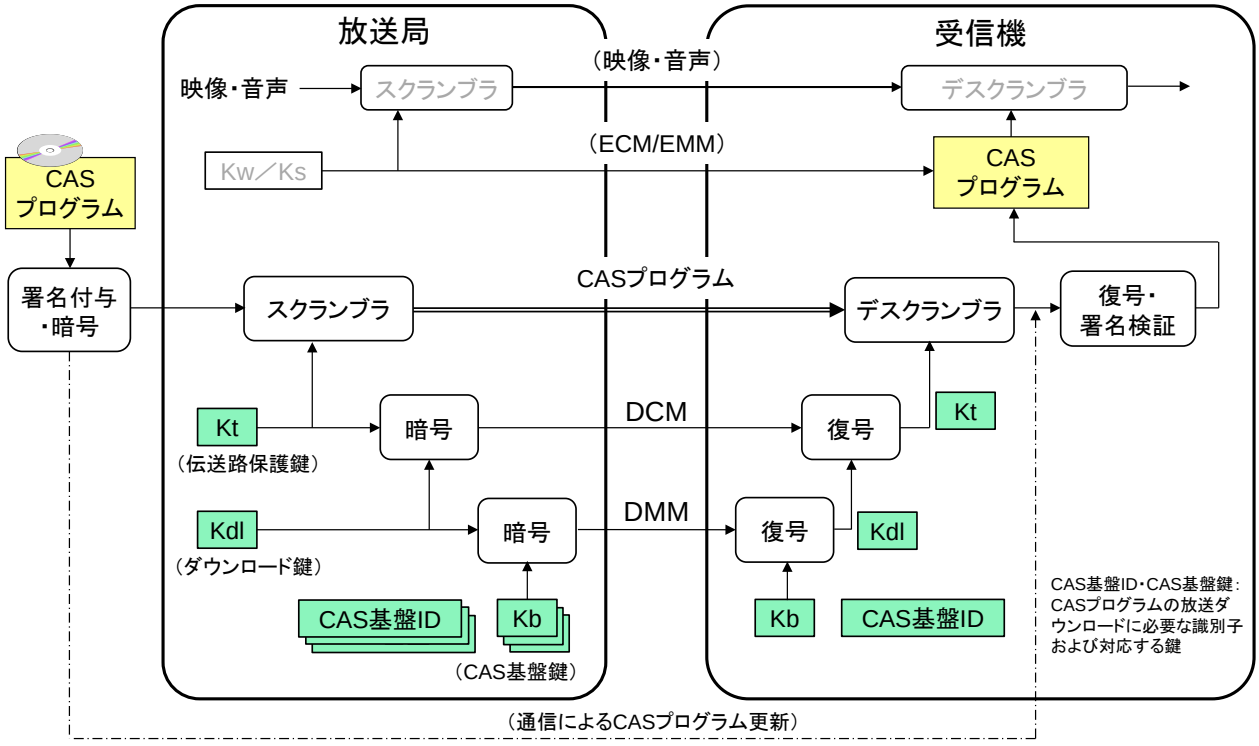


図 20：3 重鍵方式による放送ダウンロードの保護

3.4.2.3　CAS プログラムのスクランブル

CAS プログラムのスクランブルについては、3.1～3.3 で示されるものとする。なお、運用の詳細については、今後民間規格等で定めるものとする。

3.4.2.4　CAS プログラムの放送ダウンロードに関わる鍵関連情報

CAS プログラムの放送ダウンロードに関わる鍵関連情報は、DCM（Download Control Message）と DMM（Download Management Message）から構成される。

関連情報を伝送するパケットは、PMT（多重化方式が拡張 MPEG-2 TS 方式の場合)、MP テーブル（多重化方式が TLV・MMT 方式の場合）および SDTT を想定するが、その詳細については、今後民間規格等で定めるものとする。

3.4.2.4(1)　DCM

DCM は、伝送路暗号を復号するための鍵（伝送路保護鍵：Kt）、日時、改ざん検出などを伝送することを目的とする。ヘッダ部および CRC は、セクション形式の拡張形式と同様とする。

DCM は、多重化方式が拡張 MPEG-2 TS 方式の場合はそのまま MPEG-2 TS の形式で、多重化方式が TLV・MMT 方式の場合は、M2 セクションメッセージの形式でそれぞれ送出する。

DCM の一部の領域は、ダウンロード鍵（Kdl）によって暗号化することができる。暗号化の暗号アルゴリズムは、128 ビットブロック暗号方式とするが、具体的な暗号アルゴリズム、暗号利用モードおよび初期値など詳細は事業者任意仕様とする。

なお、DCM に関しては、放送番組を受信するために必須な情報ではないことから、民間規格として定めることが適当である。

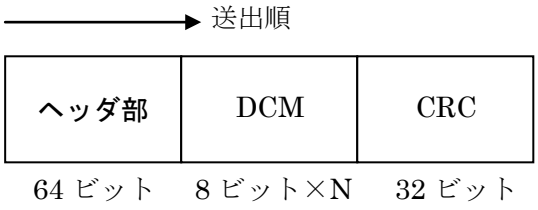


図 21：DCM の構成

3.4.2.4(2)　DMM

DMM は、ダウンロード鍵（Kdl）、有効期限、改ざん検出などを伝送することを目的とする。ヘッダ部および CRC は、セクション形式の拡張形式と同様とする。また、セクション形式の拡張形式の範囲で、DMM は複数多重することができる。

DMM は、多重化方式が拡張 MPEG-2 TS 方式の場合はそのまま MPEG-2 TS の形式で、多重化方式が TLV・MMT 方式の場合は、M2 セクションメッセージの形式でそれぞれ送出する。

DMM の一部の領域は、CAS 基盤鍵（Kb）によって暗号化することができる。暗号化の暗号アルゴリズムは、128 ビットブロック暗号方式とするが、具体的な暗号アルゴリズム、暗号利用モードおよび初期値など詳細は事業者任意仕様とする。

なお、DMM に関しては、放送番組を受信するために必須な情報ではないことから、民間規格として定めることが適当である。

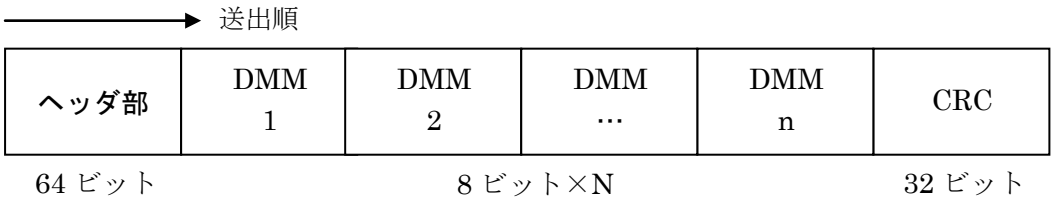


図 22：DMM の構成

3.4.2.5　通信利用、受信機実装など

CAS プログラムの通信仕様については、今後民間規格等として定めることが適当である。同様に、放送は単方向であるなどの特性を鑑みて、より安全・確実な運用のために通信を併用することなどが考えられるが、運用事項であるため、今後事業者任意規格等として策定することが望ましい。

ダウンローダブル CAS 方式に対応する受信機側の実装については、実装の難易度、安全性の維持管理、課金機能やコピー制御機能などへのエンフォースメントの行使、および適切なコストなどを考慮して、今後事業者任意規格等として策定することが望ましい。

(今後の課題)

今回、スクランブル方式やダウンローダブル CAS 方式に関して、超高精細度テレビジョン放送への適用について検討したが、今後は、それらのメディア横断的な利用や、現行放送との共用受信機を想定した利用などを含めて、民間で幅広い検討を行うことが重要である。

第 4 章　狭帯域伝送における限定受信方式

27MHz 帯域幅を使用する超高精細度テレビジョン放送の限定受信方式は、狭帯域伝送における限定受信方式の要件に基づき、更に 2014 年のサービス開始予定も考慮し、現行の高度狭帯域 CS デジタル放送で採用されている限定受信方式と同一のものとすることが適当と考える。