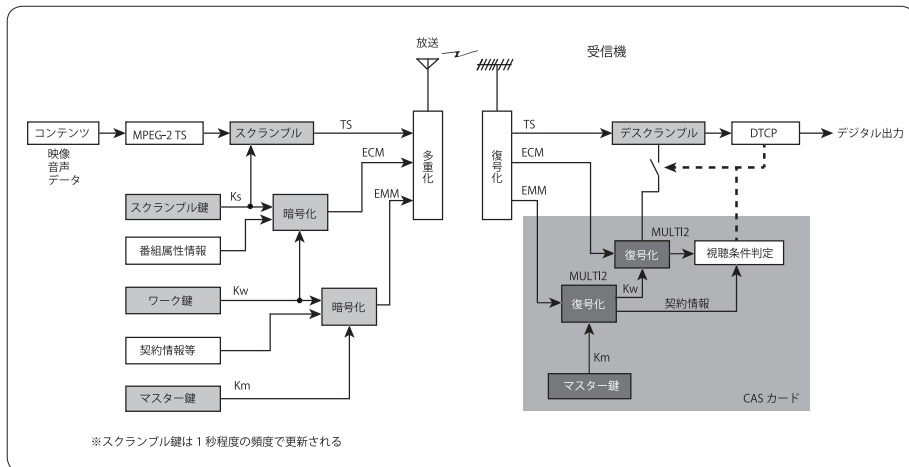


▼デジタル放送での限定受信システム



これらの暗号化には日立製作所が開発した、MULTI2が用いられている。ブロック長は64ビットと少なく、既に過去の暗号と言えるかもしれない。

■受信側にはB-CASカードが必要となる

- ① B-CASカードに書き込まれているマスター鍵(カード固有)を使用しEMMの復号化をおこない、ワーク鍵(Kw)と契約情報等を取り出す。
- ② 取り出したワーク鍵を使い、ECMからスクランブル鍵(Ks)と番組の属性情報を取り出す。
- ③ スクリンブル鍵と契約情報、番組属性情報によりトランスポート・ストリームのスクランブル解除をおこなう。(無料放送であっても暗号化されて放送がおこなわれている。)

このほかEMMは特定のB-CASカードIDに記録された、契約情報を書き換えることができる。

以上はアクセスコントロールだが、コンテンツ保護機能としてコピーワンス²が採用されていた。しかし1回のコピーのみでは失敗した場合など、心もとないということで緩和され、無料の放送にはダビング10³が採用された。

2012年5月、B-CASカードのデータを書き換えて、デジタル放送の視聴制限を解除するソフトウェアがネットに拡散された。受信契約なしに有料放送の視聴が可能