# 参考資料4　評価に係る実施者意見

評価委員会は、評価結果を確定するに当たり、あらかじめ当該実施者に対して評価結果を示し、事実関係から正確性を欠くなどの意見がある場合に、補足説明や反論などの意見を求めた。評価委員会では、意見があったものに対し、必要に応じて評価結果を修正の上、最終的な評価結果を確定した。

この過程を経て見解の相違が解消されなかったものについて、以下に評価に対する実施者意見及びそれに対する評価委員の見解を示す。

（2） 情報家電用マルチメディアセキュアチップ TRON-SMP の研究開発

実施者：東京大学、パーソナルメディア株式会社、株式会社ルネサステクノロジ

| 評価に対する実施者意見と評価委員の見解 |
| --- |
| 【評価委員会が提示した評価結果（案）】<br>マイクロペイメントを実現するために、暗号処理部と復号処理部を1チップに載せて課金と視聴を不可分に実装した耐タンパーなLSIと、このLSIを含むプラットフォームおよびサーバーシステムを同時に開発して、ひとつのソリューションとして完成した点は評価できる。指摘1一方、共通鍵方式と個別暗号システムの比較優位性を端末やサーバ上の負荷増減のトレードオフ関係等で実証する必要がある。暗号化の方式が今後の動向や市場要求にあっているか、耐タンパー性の定量的評価などが必要である。<br>DTV,IPTV 端末、携帯向けサービスなど今後の成長ポテンシャルが大きく発展が期待される領域での事業展開を考えている。先行している他のサービスに対する補完技術/付加価値として早急に普及できれば意味がある。IPTV など利用者サイドの利便性を考慮するとともに、既存のプラットフォーム、暗号サービスなどに組み込まれるためには、本技術の有意性を明確にすることを要する。コストダウンの検討を進めチップの実用化時期を明確化し、課金サービスなど早期にサービスプロバイダーを巻き込んだグローバル展開が必要である。 |
| 【実施者の意見（修正案）】<br>指摘1一方、現行のDVDで採用されている~~共通鍵~~方式と個別暗号システムにおいて、~~の比較優位性を端末や~~コンテンツ保護の強度とサーバ上の負荷増減との間のトレードオフがあるため、~~関係等で実証する必要がある。~~暗号方式などが可変である特長を生かし、暗号化の方式~~が~~を今後の動向や市場要求~~にあっているか、耐タンパー性の定量的評価などが必要である~~を考慮して選択し、実際のサービスを行っていくことが望ましい。<br>理由：<br>もともとの eTRON のコンセプトとして、暗号アルゴリズムは時代と共にトレンドが変化していくため、固定の暗号方式を定めるのではなく、暗号アルゴリズムを変更可能な形で API を定義しております。また、今回の個別暗号システムに関しても、コンテンツならびにユーザごとに個別の暗号鍵を生成する方式を開発しておりますが、同じ枠組みでコンテンツの種類で暗号鍵を変更し、ユーザごとでは暗号鍵を変えない方式を用いることも可能です。このようにすれば、サーバ上で動的に暗号処理を行う必要がなくなるため、サーバに負荷がかからず、さらに、現行の DVD のようにすべてのコンテンツで共通の鍵を使う方式ではないことから、DVD よりは強固なシステムとなります。また、DVD と同じように鍵を共通化させることも仕組みとしては可能です。<br>今回の研究開発の成果は、以上のように柔軟な方式であり、実サービスのときにはこの特長を生かして、市場にあった方式を採用していく予定です。 |

【評価委員会の見解】
受けいれない。
理由：
当該部分の記述は、技術的内容の優劣や包含関係を論じているのではなく、主に事業化の観点からの指摘である。すでにある共通鍵暗号方式と比べ、様々な観点からの市場における優位性が立証されることが、事業化の必要条件となることを指摘したものである。
ただし、実施者の意見も考慮して、「一方」を削除し、「また、柔軟性等の点で技術的優位性は認められるが」を挿入する。

【評価結果（確定）】
マイクロペイメントを実現するために、暗号処理部と復号処理部を１チップに載せて課金と視聴を不可分に実装した耐タンパーな LSI と、この LSI を含むプラットフォームおよびサーバーシステムを同時に開発して、ひとつのソリューションとして完成した点は評価できる。また、柔軟性等の点で技術的優位性は認められるが、共通鍵方式と個別暗号システムの比較優位性を端末やサーバ上の負荷増減のトレードオフ関係等で実証する必要がある。暗号化の方式が今後の動向や市場要求にあっているか、耐タンパー性の定量的評価などが必要である。
DTV,IPTV 端末、携帯向けサービスなど今後の成長ポテンシャルが大きく発展が期待される領域での事業展開を考えている。先行している他のサービスに対する補完技術/付加価値として早急に普及できれば意味がある。IPTV など利用者サイドの利便性を考慮するとともに、既存のプラットフォーム、暗号サービスなどに組み込まれるためには、本技術の有意性を明確にすることを要する。コストダウンの検討を進めチップの実用化時期を明確化し、課金サービスなど早期にサービスプロバイダーを巻き込んだグローバル展開が必要である。