

非PC系デジタル機器のIPv6最小仕様 Low Cost Network Applianceの課題

インターネットノード株式会社
岡部宣夫

nov@tahi.org

<http://www.i-node.co.jp/>

アウトライン

- セキュリティ的課題
- 標準化を通して学んだこと
- 3GとLCNAの取り組み方の違い
- 今後の進め方
- IPv6市場の状況

セキュリティ的課題

- **そもそもの動機**
 - たとえ非力なシステムであっても、ネットワークセキュリティは必要。
 - しかし、IPsecは実用的か？
 - 重くて動かないのでは？
 - 機能が限定されていると、IPsecは不要ではないか？
- **なら、そうドラフトに書いてみよう。**
 - IPsec仕様を軽くし、かつ必須機能としない。
- **IPv6 WG (53rd IETF @ Minneapolis)での反応は**
 - 非難ごうごう

セキュリティ的課題

■ IETF IPv6 WG

- IPsecは、これからのインターネットセキュリティの基盤技術である。
- 今々の技術を理由に「必須ではない」とはできない。
- IPsecに関しては、IPsec WGが決める。

■ IETF IPsec WG

- 議論の進展が遅い。
- 実は、IPv4 VPNのことが議論の中心。
- 下位互換性を重視するので、古い仕様のMUSTがそのまま継承される。
 - 例えば、DESはMUST。
- 鍵管理プロトコルの検討が振り出しに戻った。

セキュリティ的課題

■ 個人的な考え

- 一般的な議論では、理想 / 現実のトレードオフは導き出せない。
 - LCNAの目指す具体的なターゲットを設定し、
 - 必要なモデルとデータを提示、
 - 利用モデル、ネットワークモデル、セキュリティモデル
 - コードサイズ、処理性能と負荷
 - これに基づいた仕様の議論が必要。

セキュリティ的課題

■ 個人的な考え(続き)

- チープなシステムでも、IPsecだけなら動くかもしれない。
 - 試みる価値あり。
 - 暗号アルゴリズムの選択には、注意が必要。
- 問題は、鍵管理だろう。
 - IKEは振り出しに戻った。
 - IKEは、LCNAにとっては複雑すぎるし、重すぎる。
 - 軽い鍵管理プロトコルが必要かもしれない。
 - しかも、組込み用途にあった使い勝手
 - それは何か？
 - 組込みの用途は幅広い
 - また別のモデル問題
- IPv6普及の過程では、IPv4/IPv6変換の存在が、IPsecにとっては悩ましい。

標準化を通して学んだこと

- 標準化と実装の立場を区別して考える。
 - 標準化は、一般的な視点が求められる。
 - 「資源が貧しいから」、「非力だから」など特定要件に囚われると、相手と議論が噛み合わない。
 - 時には、「仕様と実装は別」との割り切りも必要。
- 用語に気をつける
 - 「最小仕様」、「最小要求」などは誤解を招く
 - せっかく作った仕様を、勝手な都合で改変するのか？
 - 目指していたことは：
 - 組み込み系ホストのためのIPv6/IPsec仕様
 - プロファイルとIPv6/IPsec機能のマップ
 - 結果として、マップされない機能は実装不要

3GとLCNAの取り組み方の違い

- 体制が違う：
 - 3G: IETFと3Gのリエゾン
 - LCNA: ボランティア (ボランティアがIETFの標準)
- LCNAにとってはラッキーだった：
 - IETFとしては、3Gに注目している。
 - 偶然に3GとLCNAが同様の活動(IPv6ホスト仕様)を行っていたので、LCNAも注目された。
- まだまだこれから：
 - LCNAは、3Gのようにマーケットと規模が見えないので、存在感は希薄。

今後の進め方

- LCNAの活動をFootprintとして残すこと。
 - 独自のIDは書く。
 - 本文は建前に合わせ、appendixにcurrent practiceを記録する。
- 議論を噛み合わせるために、具体的なデータなどを提示する。
 - 想定するターゲット
 - 利用モデル、ネットワークモデル、セキュリティモデル
 - IPsec実現性のバックデータ
- 我々単独では非力なので、国内の他の活動と連携する。
 - IPv6高度化利用推進協議会のセキュリティWGやテレコンWG

IPv6市場の状況

- そもそも、LCNAの意義は：
 - インターネット技術を新しい分野(産業、家庭、医療、etc)に普及させる(=ビジネスとして成立させる)こと。
- 実際の状況は？
 - B2C(例えば情報家電)は、課題(特に非技術)が明らかになってきた。
 - B2B(例えば遠隔監視)は、IPv6への要望がでつつある。

IPv6市場の動向

■ B2Cにおける課題

- 一般消費者の財布の紐は固い。
- ビジネスモデルが見つからない。
 - 結構コストがかかる
 - ユーザ宅での機器設置、サポート
 - サービスの運用
 - 機器自体のコスト
 - コストを凌駕するサービスを見つけられない。
- 誰も、Risk Takerになれない
 - 百万台普及後の価値は誰でも理解できるが、問題は百万台へ至るための筋書き。

IPv6市場の動向

- B2Cにおける課題(続き)
 - 社内的なデッドロック
 - 全ての技術とサービスは自社で賄え。
 - 今までの経緯と既得権。
 - メーカーはサービスが不得意。
 - 家庭ネットワーク環境のばらつき
 - 様々なアクセス形態
 - ユーザ側の知識の差

IPv6市場の動向

- B2Cにおける課題(続き)
 - セキュリティ
 - 妥当な技術の確立
 - コスト(製品、サービス)に転嫁できるか？
 - 制度、政策
 - ユーザのプライバシーを守る制度。
 - 想定外のネットワーク攻撃に対するベンダーの免責。

IPv6市場の動向

- B2BにおけるIPv6への期待
 - 遠隔監視など、エンド・エンド通信を必要とするビジネス要求が実際に出てきた。
 - 医療、工場など
 - 監視する側、される側ともIPv4プライベートアドレスが普及しているため、アドレスが重複する。
 - アドホックで複雑なアドレス変換や割り当て調整を行うぐらいなら、IPv6を導入したい。

