JNSA ワーキンググループ紹介

暗号モジュール評価基準 WG

暗号モジュール評価基準WGリーダー　　執筆者
株式会社シーフォーテクノロジー　小川　博久　　萩原 雄一

■ はじめに

ネットワークが身近になった現在では、安全な通信が必須となり、あらゆる場面で暗号が利用されています。しかしながら、暗号は実装を誤ると安全性を向上することになりません。

本WGでは、これらの暗号の実装に伴う評価や基準について議論、検討し、ベンダーが正しく理解することを目標とし発足しました。また、セキュアなネットワークの実現には、暗号の正しい評価や、実装が必要であり、利用者や、設計開発者など、暗号製品に関わる現場の担当者の知識を深めることも目的としています。

■ 活動目的

本WGでは「正しく」暗号を使用することに注目し、現存する規格・制度の他に今まさに日本で制定されようとしている規格・制度について議論し、提言を行うことを目的の一つとしています。

- 現存する規格・制度とは現在米国およびカナダで採用されている暗号モジュールのセキュリティ要件であるFIPS 140-2およびその評価制度CMVPを指します。本WGでは、この規格や制度について議論し、理解を深めることを目的にしています。必要があれば、積極的に提言などを行うことも視野に入れ活動します。
- 国際的な動向としてはFIPS 140-2ベースのISO 19790が2005年中に制定されることが予想されています。本WGでは、これらの国際的な動向を把握し、利用者や設計開発者が知識を深めることを目的としています。
- 日本でもCRYPTRECにて電子政府での使用が推奨される暗号が制定され、現在どの様にそれらの暗号を実装すればよいかが議論されています。最近では、独立行政法人 情報処理推進機構から、暗号モジュール評価制度に対する移行措置の提案も行われました。本WGでは、これらの日本の検討についても動向を把握し、ベンダーとしての取組み方を議論することを目的としています。

■ 今後の予定

昨年の11月に発足し、暗号実装と正しさと、評価や基準の重要性の理解を促す活動として、アットマーク・アイティ社に『暗号モジュール評価の基礎知識』を執筆しました。

また、昨年12月14日に、『暗号モジュール評価基準カンファレンス』を行い、国内外の暗号モジュールを取巻く動向について議論し、公開WGを開催しました。

今後、本WGでは、さらにCC（ISO / IEC 15408）とFIPS 140-2の関連性についても議論します。メンバー加入は随時受付けていますので、ご興味ある方は、是非、ご連絡ください。

■ WGメンバー

リーダー：小川　博久　（シーフォーテクノロジー）
オブザーバー：Travis Spann（InfoGard Laboratories）
メンバー：佐藤　能行　（みずほ情報総研）
　　杉本　浩一　（セコムトラストネット）
　　武部　達明　（横河電機）
　　中川路　哲男（三菱電機）
　　萩原　雄一　（シーフォーテクノロジー）

2004年12月14日『暗号モジュール評価基準カンファレンス』風景