イスラエルにおけるセキュリティ関連動向調査　報告書概要

報告者：イスラエル　Globalconn **社**

テーマ：量子暗号通信システムの研究開発動向調査

1　調査項目

量子暗号通信システムを構成する主要デバイスの研究開発動向と、システムの研究開発動向の両面の調査を行う。調査項目としては、主要デバイスの研究開発拠点、その進捗状況及び（目標）性能、製品販売状況並びに輸出規制状況を調査する。又、量子暗号通信システムに関しては、研究開発拠点及びそこでの開発状況、製品化状況、使用実績等を調査する。

2　報告書の概要

(1) **量子暗号の概要**

○ **盗聴に対して協力で、安全。通信チャンネル上のノイズを計ることで、盗聴者による妨害を追跡可能。（盗聴を防ぐことはできず、検出することは可能。）**

○ **通信可能距離は、約** 100km **で実証済み（**2006 **年、**2003 **年では約** 25km **であった）。又、低空軌道衛星を利用した通信に成功している。**

(2) **量子暗号製品市場**

○ **イスラエルにおける量子暗号は、未だ研究開発段階にある。量子暗号システムとしては、まだ理想的なパフォーマンスを提供するに至っていない。**

(3) **取引規制**

○ **法律**

イスラエルにおける暗号製品の取引は、1957 **年制定の「**Laws Governing the Control of Commodities and Services**」により規制。この法律は、イスラエル国家のセキュリティを守るために制定されたもの。**

○ **輸入**

・1999 **年、暗号製品の管理及び許可は国防省に移管され、新たに「**Commercial Encryption Items Controls Policy**」を制定。商用暗号製品の購入又は** Internet **からダウンロードする際に許可が必要。**

・**認証機関については、電子署名用の暗号に限り、許可を得る前に購入等が可能。但し、使用開始前に、国防省への届け出が必要。（追って許可を取る必要あり）**

○ **販売**

暗号製品の販売に関しては、製品の技術リビューの後、許可が与えられる。

○ **輸出**

・**商用暗号製品に関しては、許可を得ることにより、鍵長に制限なく、世界中の（政府を除く）ユーザに輸出することができる。（国によっては政府機関へも可能）**

・国防省への届け出が必要。許可は毎年更新する必要あり。

(4) 調査研究動向

○ Single Photon Source

単一光子源を使用して、量子暗号のセキュリティを高められるかどうかを実験。Photon Number Splitting Attack を防止するための対策として、有効かどうかを検証。セキュリティを高めるためには、Spontaneous Parametric Down Conversion の光子対を利用すべきであることが判明。

○ Effect of turbulence on a QKD scheme Based on Transformation from the Polarization to the Time Domain

移動体間での QKD では、偏光が時間領域での揺らぎに変換されるが、温度環境等で、この揺らぎが与える影響を実験的に評価した。

○ BB84 プロトコルの実装

従来の BB84 プロトコルの実装では、4 つの光子検出器を必要とする。しかし、偏光を検出するためのビームスプリッター等の影響で、4 方向の偏光（0°, +90°, +45°, -45°）を符号化/光子検出するときに遅延が生じるので、この遅延を利用して 1 個の光子検出器のみで、4 方向の偏光検出できる実装を研究。

○ B92 プロトコルの実装

BB84 は、4 つの非直交状態を用いるのに対し、B92 プロトコルでは、2 つの非直交状態を用いている。このため、符号化/光子検出が単純化されるメリットがある。しかし、BB84 とことなり、通過経路による時間差がないため、光検出器が 2 つ必要となる。そこで、遅延素子を積極的に挿入することで、通過経路による遅延を発生させ、光検出器を減少させる実装を研究している。

○Turbulence

自由空間を利用した QKD システムに対して、温度環境の変化が与える影響に関する研究が実施されている。

［調査研究動向に対するセキュリティセンターの分析］

イスラエルでの QKD システムの研究開発は、「小型・軽量化」と「自由空間」がキーワードとなっているように見える。添付された参考文献の多くが、将来の衛星・航空機での運用を研究の背景としてあげていることからも裏付けられる。