暗号の安全性評価とCRYPTREC暗号リスト改定

ネットワークセキュリティ研究所 セキュリティ基盤研究室

CRYPTRECへの貢献

CRYPTRECとはCryptography Research and Evaluation Committeesの略であり、我が国の電子政府における調達のために参照すべき暗号のリスト（電子政府推奨暗号リスト）に掲載されている暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトです。CRYPTRECは、総務省及び経済産業省が共同で運営する暗号技術検討会と、NICT及び情報処理推進機構（IPA）が共同で運営する3つの下部委員会で構成されています。その中でセキュリティ基盤研究室はこれまで電子政府推奨暗号リストに掲載されている暗号を監視し、安全性の経年劣化に伴い必要な技術的助言を行うという役割を担ってきました。2003年に発表された電子政府推奨暗号リストが、近年の技術動向等を踏まえて改定され、2013年3月に総務省及び経済産業省からCRYPTREC暗号リストとして発表されました。セキュリティ基盤研究室は、この改定作業に暗号安全性評価及び事務局運営の面で貢献しました。

CRYPTREC暗号リスト改定

電子政府推奨暗号リストは、2003年に10年間安心して利用できるという観点で選定されましたが、（1）10年が経過したこと、（2）暗号解析技術・計算機の発展により安全性の低下が進んだこと、（3）暗号が利用されるシーンが広がったことから、2013年に新たに「電子政府推奨暗号リスト」を改定した「CRYPTREC暗号リスト」が作成されました*。CRYPTREC暗号リストは安全性だけではなく、調達容易性、国産暗号の普及促進といった様々な視点で検討され、「電子政府推奨暗号リスト」、「推奨候補暗号リスト」、「運用監視暗号リスト」から構成されています。電子政府推奨暗号リスト及び推奨候補暗号リストには安全性及び実装性能が確認された暗号技術が掲載されています。特に、電子政府推奨暗号リストには、CRYPTRECにて調達が容易である等と判断されたものが掲載されています（図1）。また、運用監視暗号リストにはハッシュ関数SHA-1など実際に解読されるリスクが高まるなど推奨すべき状態ではなくなった暗号技術が掲載されています。

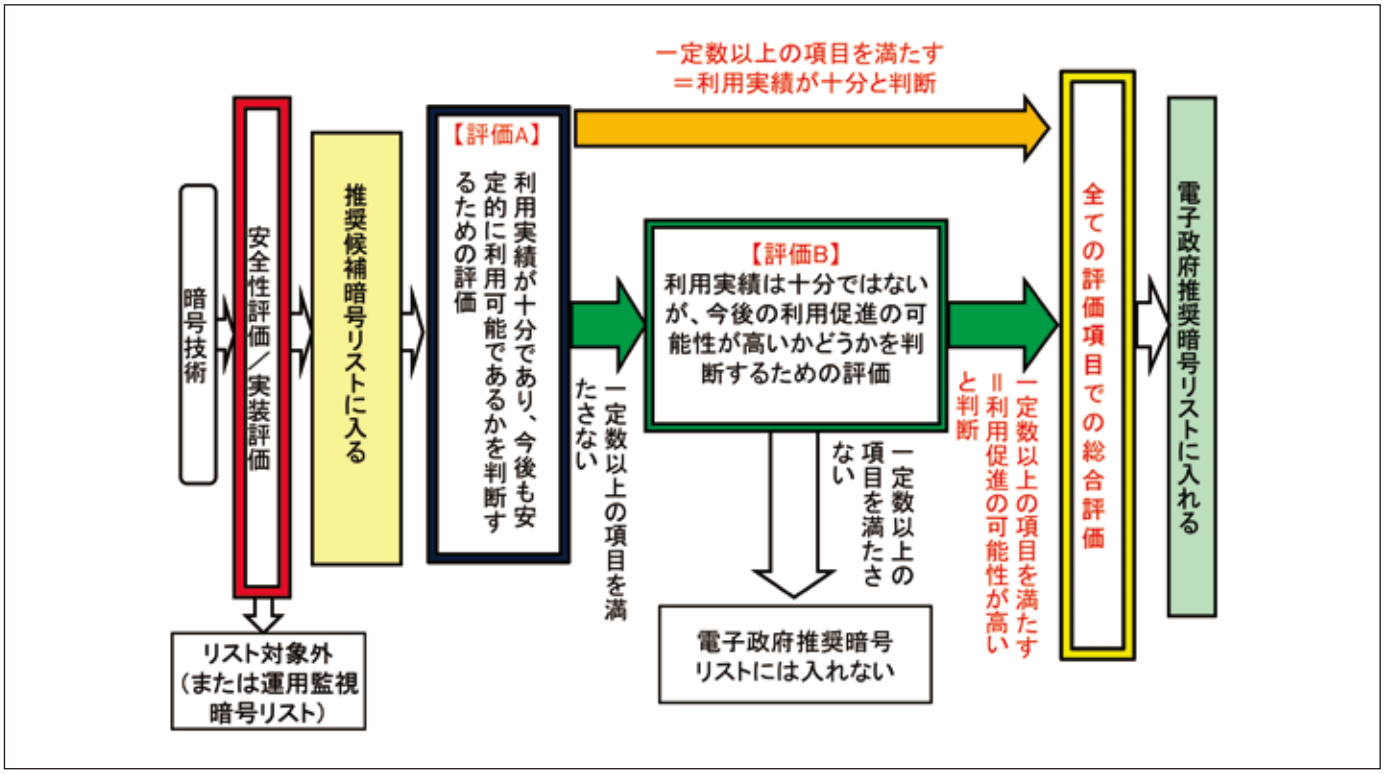

図1　リストの改訂プロセス

＊ 電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）
http://www.soumu.go.jp/main_content/000206523.pdf