

日本の暗号研究と政府推奨暗号の 今後について

モデレータ
東京電機大学未来科学部
情報セキュリティ研究室
佐々木良一
sasaki@im.dendai.ac.jp





モデレータ

佐々木良一(東京電機大学)

パネリスト

岩下直行(日本銀行)

辻井重男(情報セキュリティ大学院大学)

苗村憲司(SC27/WG2コンビーナ)

松本勉(横浜国立大学)

伊藤毅志(内閣官房情報セキュリティセンター)

目的

日本の暗号研究や電子政府推奨暗号の今後のあり方などに関する討議

パネルの進め方案(1)

1. 個別発言(5-10分)

(1) 松本先生

セキュアな暗号アルゴリズムを確保し管理する立場から、活動の成果の概要と残された問題点に言及

(2) 苗村先生

国際標準の動向の紹介と政府推奨暗号との関連付けについての考え方を述べる。

(3) 岩下さん

ユーザの立場から専門家が何を行いユーザが何をすべきかと言う立場で考えを述べる。

パネルの進め方案(2)

(4) 辻井先生

松本先生などの発言に対し、大局的見地からコメント

(5) 伊藤さん

リストのユーザとしての意見、移行の進め方についての考えなど

2. 全体討議

(1) 個別発言の中で出てきたものの討議

(2) 個別発言の中で議題にならなかったものに関する討議

(a) CRYPTRECと政府専門組織の関係

(b) 暗号危殆化に関する危機管理など