IPA　暗号フォーラム　2008・大川賞受賞記念シンポジウム

「暗号技術の今後」

日時：2008 年 11 月 21 日（金）13:00-18:00

場所：東京大学生産技術研究所 An 棟コンベンションホール

（東京大学駒場リサーチキャンパス）

http://www.iis.u-tokyo.ac.jp/access/access.html

独立行政法人　情報処理推進機構（IPA）

財団法人　大川情報通信基金

主催　独立行政法人　産業技術総合研究所（AIST）

情報セキュリティ研究センター（RCIS）

ジャパンデータコム株式会社

後援　東京大学生産技術研究所

プログラム（同時通訳付き　12:30 開場）

開会挨拶	財団法人　大川情報通信基金 奥島　孝康　理事長 （早稲田大学　学事顧問　前総長）
大川賞の趣旨・受賞者の紹介	相磯秀夫　大川賞審査委員長 （東京工科大学 理事　前学長）
来賓挨拶	平本　俊郎　教授 東京大学生産技術研究所
講演（Ⅰ）暗号と情報セキュリティ	中央大学　今井秀樹　教授 （産業技術総合研究所 情報セキュリティ研究センター 研究センター長）
講演（Ⅱ）我が国の暗号政策の動向	経済産業省　三角　育生氏 （情報セキュリティ政策室長）
講演（Ⅲ）RSA 暗号の現在・過去・未来	イスラエル・ワイツマン研究所 Adi Shamir 教授
講演（Ⅳ）ハードウェアセキュリティ技術の動向	産業技術総合研究所　佐藤　証氏 （情報セキュリティ研究センター ハードウェアセキュリティ研究チーム 研究チーム長）
閉会挨拶	情報処理推進機構　理事長 西垣　浩司

会場手配の都合がございますので、11 月 13 日（木）までに、電子メールあるいはファクシミリにて、別紙の参加申込書をお送りください。

［問い合わせ先］　（独）情報処理推進機構　セキュリティセンター　暗号グループ（isec-crypto@ipa.go.jp）

［参加申し込み］　IPA 暗号フォーラム事務局 E-mail:forum2008reg@ipa.go.jp FAX:03-5978-7518

2008 年 10 月吉日

IPA 暗号フォーラム 2008、大川賞[1]受賞記念シンポジウム
～ 暗号技術の今後 ～
開　催　案　内

独立行政法人　情報処理推進機構
財団法人　大川情報通信基金

拝啓、
仲秋の候、皆様にはますますご清祥の段、お慶び申し上げます。また、日頃当機構の事業に格別のご理解・ご高配を賜り、厚くお礼申し上げます。

さて、現代暗号技術は、電子商取引、携帯電話、インターネット、行政システム、交通システム等に用いられることにより、社会を支える重要な技術となっています。そこで、独立行政法人　情報処理推進機構（IPA）では、2004 年から現代暗号技術の普及・啓発の一環として、情報セキュリティや暗号技術の最新動向や最近のトピックスの紹介のために、IPA 暗号フォーラムを開催してまいりました。
現代暗号を利用するシステムにおいては、現在利用している暗号技術の多くが 1970 年代の後半に開発された技術であり、計算機技術の進歩等の影響を受け、世代交代の時期を迎えております。例えば、共通鍵暗号では、1976 年に米国連邦標準として制定された DES 暗号は、解読技術の進歩により、Triple-DES、AES と 2 度の世代交代を経験しようとしております。

一方、公開鍵暗号技術は、現代暗号技術の最大の成果であり、中でも RSA 暗号はインターネット社会の安全性を担保する為に、世界中で様々な場面で広く利用されています。しかし、この暗号の世代交代は、公開鍵暗号（RSA 暗号）を中核技術として構築された公開鍵暗号基盤（PKI[2]）にとっては、初めての経験といっても過言ではありません。

そこで、暗号の世代交代という状況をふまえ、また大川賞受賞を記念して RSA 暗号の開発者の一人である Adi Shamir 教授（イスラエル・ワイツマン研究所）と基礎研究から応用技術の開発に至る幅広い分野において、我が国の暗号研究をリードしてこられた今井秀樹教授（中央大学、東京大学名誉教授）のお二方をメインゲストにお招きし、「暗号技術の今後」と題して、IPA 暗号フォーラムを、11 月 21 日（金）東京大学駒場コンベンションホールにて開催することと致しました。

また、Adi Shamir 教授[3]と今井秀樹教授[4]は、2008 年度大川賞を受賞されるため、このたびの IPA 暗号フォーラムは、財団法人　大川情報通信基金、独立行政法人 産業技術総合研究所　情報セキュリティ研究センター、ジャパンデータコム株式会社と共同で開催することとしました。ご多忙のことと存じますが、多数の皆様のご参加を賜りたくお願い申し上げます。

---

[1] 大川賞は、財団法人　大川情報通信基金が行う表彰で、(株)CSK ホールディングスの創業者である故・大川 功氏が創立し、情報・通信分野における研究、技術開発および事業において顕著な社会的貢献をされた方の労に報い、その功績を表彰するとともに、情報・通信分野のさらなる発展と啓発に寄与することを目的とした国際的な賞（http://www.okawa-foundation.or.jp/oka/index.html）です。
[2] Public Key Infrastructure
[3] 受賞理由：「RSA 暗号の創案ならびに暗号技術の進展に関する多大な貢献」
[4] 受賞理由：「符号理論と暗号理論ならびにその応用に関する研究への多大な貢献」