「情報セキュリティセミナー」のご案内

-- セキュリティの根幹を成す暗号技術、不正解読手法とその対策 --

岡山県工業技術センターと岡山大学では、今年度より総務省戦略的情報通信研究開発推進制度において「暗号機器のサイドチャネル攻撃に対する安全設計に関する研究開発」が採択され、研究開発を進めております。今回は、このプロジェクトの一貫として、地元の企業の方を対象としたセミナーを開催します。

近年、インターネット等の普及により、より広範囲なデータにアクセスする機会が増え、また、個人情報も広範囲に存在するようになりました。このデータの安全性を保つためにセキュリティに対する関心も高まっています。特に、情報通信の分野においては、インターネット上で通信されるデータは誰でも盗み見ることが可能との前提に立った暗号化が主流となっています。一方、この暗号化されたデータを復元して解読する試みも広く検討されており、今回は、この中でも最近注目されてきている「サイドチャネル攻撃」という技術を中心に講演を行なって頂きます。このサイドチャネル攻撃は、暗号の生成・復号の際に生じる副次的な電磁ノイズから情報を取り出す技術です。その対策設計として、電磁ノイズを出さないことが重要となります。従ってサイドチャネル攻撃の対策設計は EMC 課題の一つであると言えます。

貴社の製品に対してセキュリティについて関心の高い方および電磁ノイズに対しての関心が高い方にとって有益なセミナーであると思いますので、是非ご参加頂きたくご案内致します。

記

日　時　：　平成２４年１１月１４日（水）　１３：３０～１７：００

会　場　：　岡山県工業技術センター　１F　技術交流室

定　員　：　４０名

参加費　：　無料

内　容　：　講演会

１．　「最近の暗号技術とその実装手法」
　　岡山大学　大学院　自然科学研究科　准教授　野上 保之 氏

２．　「電磁波を用いたサイドチャネル攻撃と対策手法」
　　東北大学　電気通信研究所　研究員　林 優一 氏

３．　「サイドチャネル攻撃対策の現状および規格化動向」
　　産業技術総合研究所 セキュアシステム研究部門 研究員　堀 洋平 氏

４．　「プリント基板／製品レベルでの暗号漏洩対策設計技術」
　　岡山大学　大学院　自然科学研究科　助教　五百旗頭 健吾 氏

主　催　：　岡山県工業技術センター、岡山大学

連絡先　：　岡山県工業技術センター　研究開発部　計測制御グループ　渡辺哲史

(参加申込)　〒701-1296 岡山市北区芳賀 5301, e-mail: watanabe@okakogi.jp

Tel: 086-286-9600,　Fax: 086-286-9630

情報セキュリティセミナー(11/14)　参加申込み

* 企業・機関名 ：
* 所属 ：
* 参加者氏名 ：
* 連絡先メールアドレス ：
* 連絡先 TEL：

申込締切： 11/9(金)

申込先　岡山県工業技術センター　渡辺哲史
e-mail: watanabe@okakogi.jp,　Fax:086-286-9630