



吉浦 裕  
Hiroshi YOSHIURA

### 研究课题 媒体安全

#### 关键词

信息安全, 媒体安全, 互联网安全, 电子签名, 电子水印, 防火标识

所属专业	研究生院信息理工学研究科 综合信息学专业
研究成员	吉浦 裕 教授
所属学会	电子信息通信学会, 信息处理学会, 日本安全管理学会, IEEE, 系统控制信息学会

#### 研究概要

### 在信息化社会中保护自己

随着互联网的普及, 媒体正在迅速地数字化、复合化、个人化。比如在互联网、移动网络、数字广播中普及大容量的媒体, 随着存储信息的形态及制作方法的变化、发信人的多样化, 计算机上的图标操作直接关系到网络交易等, 媒体的意义正向着多样化发展。

互联网诈骗也日益增加。在这种背景下, 由于互联网用户的本质比较多样化, 全世界每年都会增加数亿人的用户, 伴随着用户的增加, 就比较难确认对方的身份, 信息及数据的可靠性也会变得比较难确认。

在这样的时代, 面对偷偷钻过数字媒体安全策略的违法魔手, 当务之急就是如何确立对策来保护自己及企业的重要信息。

作为保护用户的安全技术, 该研究室主要从事的研究为: 对应各种电子合同的高级化「电子签名」、检测存储信息非法外流的「电子水印」、「互联网[Web]的安全性」、「非法复制问题的风险管理」、「作品的二次利用·构思的具体化」、「个人隐私和个人信息的保护」。

### 电子签名的研究

吉浦教授在之前任职的日立制作所从事商品开发, 他活用已取得多个专利的丰富经验, 研究电子签名算法的「抗病毒数字签名验证方法」, 采用这种算法, 即使计算机感染病毒, 也不能将无效的签名判断为有效, 以及防伪数字签名的「抗病毒数字签名生成方法」。在这些领域中, 在考虑防止一般的非法入侵本身及防止泄漏生成签名的「密匙」时, 该研究室提出了安全性算法的方案, 即使被非法入侵也能继续维持其安全性。

### 电子水印的研究

该研究室在维持画质的同时, 还挑战通过提高检测性能来提取嵌入信息这种课题, 进一步确切防止存储信息的非法泄漏。

到目前为止, 他们把原图像分解为 3 个平面, 将一个平面中存储的信息嵌入到其中两个平面中, 这样就能提高检测性能, 而不会降低画质。此外他们还在设计即使公开算法也很安全的电子水印, 致力于这种尚未解决的「可公开算法的电子水印」的研究。

### 互联网(Web)安全性的研究

该研究室在思考防伪证书验证程序的同时, 使用电子水印, 成功地将签名信息嵌入到「防火标识」中, 以用户通俗易懂的方式显示出无法伪造的数字签名信息嵌入式防火标识。

### 非法复制问题的风险管理研究

该研究室与其他大学一起进行很多共同研究, 比如「产生对立风险时的系列管理系统」; 针对「促进作品的二次利用」, 研究复制技术的有效利用; 将作品的构思具体化, 以便能够实现维度较高的二次利用。

#### 优势

### 获得很多专利, 从基础研究到实用化, 能够进行全盘思考

该研究室活用丰富的产品开发经验, 以在企业积累的研究知识为基础, 从其他研究机构还未开展的着眼点开始推进相关的研究, 进行制造, 从「研究」和「实用」两个角度确信能够达到实用化水平。到现在为止取得的专利已经高达 60 项以上。

电子水印的研究成果在 2005 年获得信息处理学会颁发的论文奖, 因而备受关注。

「防火标识」于 2000 年以日本商工会议所为中心, 被众多企业采用, 2005 年获得系统控制信息学会颁发的产业技术奖。

#### 未来展望

### 以创造安全放心的媒体环境为目标

信息安全是能够从信息处理的角度来思考与人们生活紧密相关的安全方面的一门学问。生活处处能够发现新的问题点, 可以预测在丰富的研究课题的领域中, 今后研究的必要性还会有所增加。以创造安全放心的媒体环境为目标, 以目前已取得实绩的「电子签名」、「电子水印」为主, 该研究室还致力于作品流通管理的研究及风险管理系统的构建。



### 媒体安全的研究

- 与媒体数字化、复合化、个人化相关的安全
- 确保所提供的信息及提供人员的真实性, 保护内容的著作权
  - 对应各种电子合同的高级化电子签名
  - 检测内容非法流通的电子水印
  - 保护隐私及个人信息
  - 非法复制问题中的风险管理
  - 著作物的二次利用、构思的具体化

