

- NICTがネット広告と暗号化技術をリンクさせた新システムを開発  
ー凸版印刷(株)へ技術移転し、暗号化無料ソフトウェアが実現ー
- 平成18年11月16日

独立行政法人情報通信研究機構(以下、NICT。理事長:長尾 真)は、暗号化された電子文書等を復号化\*1する際にネット広告を表示させる新しい暗号化ソフトウェアを開発し、凸版印刷株式会社(以下、凸版印刷。代表取締役社長:足立 直樹)に技術移転を行いました。

このネット広告機能付き暗号化技術は、凸版印刷のフリーDVDマガジン「codeNEO」(配布数:25万部)に、無償ソフトウェア「CIPHERON NEO」\*2の名称で組み込まれ、11月20日から都内コンビニエンスストア等の店頭に並びます。

## <背景>

近年、情報記憶媒体の盗難やインターネットを通じた情報漏えい\*3事件が多発しており、その安全管理が強く求められています。その対策として、データ等の暗号化が有効な手段とされていますが、データの送り手と受け手の双方が同一の暗号ソフトウェアを購入する必要があるなど、必ずしも利用促進が図られていない状況が続いています。

## <成果>

NICTは、暗号化ソフトウェア「CIPHERON Initiative」\*4をベースに、ユーザーが暗号情報の復号化を行う際、“広告ページ”を自動的に表示する技術を開発しました。これにより“広告主”が、広告料としてソフトウェアの購入代金をユーザーに代わって負担することで、暗号ソフトウェアをユーザーに無償で提供できるようになります。ソフトウェアの無償化によって一般への暗号化技術普及が進むことにより、ネット上でやりとりされる情報や、記録媒体に保存されるデータの暗号化が促進され、社会問題となっている情報漏えい被害防止に役立つことが期待できます。

さらに、復号化の際、ユーザーが確実に広告に接触する仕組みが出来ることにより、新たなネット広告ビジネスモデル創出の可能性も秘めています。

## <問合せ先>

独立行政法人情報通信研究機構  
総合企画部広報室  
栗原則幸、大野由樹子  
TEL:042-327-6923、FAX:042-327-7587

## <本件に関する問合せ先>

情報通信研究機構 研究推進部門 知財推進グループ  
澤田 史武  
Tel: 042-327-7464、Fax: 042-327-6659

凸版印刷株式会社 文化事業推進本部  
情報ビジネス開発部  
Tel:03-5840-2455

## 【用語説明】

## \* 1. 復号化

データを第三者に見られても解読できない様にする暗号化と対をなす概念であり、暗号化されたデータを元データに復元する操作をいいます。

## \* 2. CIPHERON NEO

CIPHERON NEOは、暗号化復号化を可能とするソフトウェアで、USBメモリー等のデバイスに、暗号の“鍵”を入れ、それを抜き差しすることで自動的に暗号化復号化する無償暗号化ソフト「CIPHERON Initiative」をベースとしています。また、復号化時に広告を入れるために、「CIPHERON Initiative」の自己暗号化対象ファイルの容量制限40Mバイトを撤廃しています。さらに暗号化の宛先指定に必要な公開鍵をカメラ付き携帯電話で読み取り可能な2次元バーコードとして出力する機能も付け、将来のユビキタス公開鍵インフラストラクチャーを実現する機能も付加しています。NICTは、セキュリティのビジネスモデルを一新させる可能性を持つ本広告機能付き暗号化復号化ソフトウェアのコンセプトを特許出願するとともに、今回、凸版印刷に技術移転しました。

<http://www.cipheron.net/> (ユビキタス公開鍵インフラストラクチャーについて)

## \* 3. 情報漏えい

インターネット上やノートPCの紛失により、特定の第三者、あるいは不特定多数の第三者に、秘密とすべき情報が流出することを指します。最近では、ファイル共有ソフトWinny(ウニー)やShare等の利用により、個人・民間企業・地方自治体等からも情報漏えいが多数発覚して問題となっています。このような情報漏えい問題は、対象ファイルを暗号化し、さらに、復号化期限を設けることにより、第三者が仮にデータを手入しても、暗号化されているため復号化をすることができず、加えて、正当な権限を有しない第三者が復号化しようとしても、データを消滅させる設定ができるため、情報漏えいの2次拡大の防止や、本質的な意味での機密情報の漏えいを防止することができます。

## \* 4. CIPHERON Initiative

NICT発ベンチャー企業(株)カオスウェアが、2005年10月にリリースした暗号化復号化ソフトウェア。USBメモリー等に“鍵”を入れることで、直接的な操作で暗号化復号化が実現できます。さらに、厳密な復号化期限も設定可能で、復号化期限以降復号化する際、自動的にファイルをランダムに上書きした後、消去するという電子シュレッダー機能もついています。

<http://www2.nict.go.jp/pub/whatsnew/press/h17/051018/051018.html>

## ＜ネット広告機能付き暗号化ソフトとその配布スキーム＞

