

報道関係各位

住商情報システム株式会社

住商情報システムは、米 eEye Digital Security 製  
無償 Winny 検出・通信遮断ツール(日本語版)を  
提供いたします。

検出ツールはリモートから Winny 稼動ホストを高速に検出  
通信遮断ツールは簡単な設置で Winny トラフィックを遮断

住商情報システム株式会社 (略称:SCS 本社:東京都中央区 代表取締役社長:阿部康行)は、eEye Digital Security 社 (略称:eEye 本社:米国 カリフォルニア州 CEO: Firas Bushnaq) が開発した日本語版 Winny 検出・通信遮断ツールを住商情報システムの Web サイト <<http://www.scs.co.jp/eeeye/>> にて無償提供することを、以下の通りお知らせいたします。

尚、2006年5月12日に住商情報システムが主催する eEye Security Forum / Spring 2006 にて eEye 鵜飼裕司氏による講演「Inside Winny ~ Winny の解析とそのセキュリティ脅威分析~」、「Ring “-1” Rootkit ~ 周辺機器などシステムの「外」で動作する新たな Rootkit や BOT の脅威とその対策」を予定しています。

<[http://www.scs.co.jp/event/2006/0512\\_eeeye/index.html](http://www.scs.co.jp/event/2006/0512_eeeye/index.html)>

記

## 1. フリーツール無償配布の背景:

P2P アプリケーション Winny のネットワークを介して感染する多くのマルウェア\*1により、数多くの企業及び政府機関より重要情報の流出が相次いでいます。Winny ネットワークの性質上、一度流出してしまったファイルを回収することは現時点では不可能です。

eEye ではこの問題をユーザーアプリケーションが企業ネットワークを攻撃する際の脆弱点として用いられている世界的な流行の一部と考えています。安全な企業ネットワーク維持の援助を目的として、eEye 社のネットワーク脆弱性検査ツール「Retina」の技術を生かした「eEye Winny Scanner」日本語版及び「eEye Winny Monitor」日本語版を無償配布することとなりました。

## 2. フリーツール概要:

### (1) 「eEye Winny Scanner」日本語版

「eEye Winny Scanner」は、リモートから Winny が動作しているホストを検出するためのネットワークスキャナです。IP アドレス範囲を指定してスキャンをかける事により、組織内で Winny が動作しているホストがあった場合、それらを簡単に列挙する事ができます。

プロトコル検出(暗号化された Winny2 パケットを解読して初期鍵送信パケット\*2を検出)に基づいたスキャンを実現していますので、ネットワークにかかる負荷が少なく、ファイルスキャンによる検出を行うツールと比較して大幅に高速なチェックが可能です。スキャン対象ホストのアクセス権(クレデンシャル)も不要です。

### (2) 「eEye Winny Monitor」日本語版

「eEye Winny Monitor」は、ネットワーク内に流れる暗号化された Winny2 パケットをリアルタイムに解読し、初期鍵送信パケットを検出します。初期鍵送信パケットが検出されると、その接続元、接続先の IP アドレスを表示します。

また、検出された初期鍵送信パケットにより Winny ノードを特定し、TCP 接続をリセットする事ができます。このため、管理対象のネットワーク内に流れる Winny トラフィックを強制的に遮断する事ができます。導入はミラーポート\*3に接続するだけで、非常に簡単です。

## 3. 提供開始日:

2006年4月11日(火)より提供開始いたします

## 4. eEye Digital Security概要:

米国セキュリティ業界で著名な Marc Maiffret 氏が中心となって 1998 年に設立。

過去 3 年間で最も多くのハイリスクな脆弱性を発見している、世界有数の脆弱性リサーチチーム eEye Research Team を編成し、セキュリティホール発見、OS、ソフトウェア、ハードウェアの脆弱性に関する研究を行い、各国の政府機関やベンダーに報告を行っています。

主力製品である高速、高精度なネットワークスキャナ Retina は世界 80 カ国 8000 社以上の導入実績があります。

## 5. 用語解説:

### \*1 マルウェア:

「悪意のこもった」ソフトウェアのこと。「mal-」という接頭辞には「悪の」という意味があり、これとソフトウェアを組み合わせた造語である。主にコンピュータウイルス、ワーム、スパイウェアなどのことを指す。

### \*2 初期鍵送信パケット:

ファイル転送用 TCP ポートに接続確立後、最初に送受信される 11 バイトのパケット。以降やりとりされるパケットの暗号化に利用する 4 バイトの RC4 キーを含む。

### \*3 ミラーポート:

主としてスイッチに搭載されている特殊なポートで、ネットワーク監視などのために利用される。ミラーポートは、そのスイッチの通常のポートを通過する全てのデータを複製して通過させるため、そこにネットワーク監視のための機器を接続することで、スイッチを通過する全データを監視することができる。

## 6 . 本件に関するお問い合わせ先 :

### 【製品に関するお問い合わせ先】

住商情報システム株式会社 IT 基盤ソリューション事業部  
セキュリティソリューション第 1 部  
担当：富田、脇  
TEL：03-5166-1764  
E-Mail：eeye-info@ml.scs.co.jp

### 【本資料に関する報道機関からのお問い合わせ先】

住商情報システム株式会社 広報・IR 部  
担当：片山  
TEL：03-5166-1150

\*掲載の社名、商品名は、各社の商標、または登録商標です。

以 上