

CyberCrime Control Project

平成28年第1号

広島県警察本部
サイバー犯罪対策課
082-228-0110

～ 実在する企業を騙った **ウイルス付き** メールに注意 ～



狙いは国内ネットバンキング!!

■ ばらまき型攻撃の手口

ばらまき型攻撃は、機関・企業の機密情報や個人情報盗み出すことを目的として、ウイルス付きメールを不特定多数の標的に対して送信する攻撃です。

県内においても、ネットバンキングの不正送金に使用される「**Rovnix(ロヴニクス)**」と呼ばれるウイルスを添付ファイルに仕込んだメールが多数確認されています。

このウイルスに感染した状態でネットバンキングサイトへアクセスすると、偽のログイン画面を表示するなどの方法で、預貯金を第三者の口座に不正送金されてしまいます。

■ ばらまき型メールの実例(県内)

差出人を「日本郵政」と装い、「委託運送状」と称する添付ファイルを開かせようとする。送信元のメールには**ロシアのフリーメールアドレス**が使用されていました。

※実際に被害者宛に送られてきたメールです。

ファイル メッセージ

2016/

郵便局 - 日本郵政 <[redacted]@rambler.ru>

宛先 [redacted]@[redacted].jp

メッセージ 日本郵政_お問い合わせ番号_9050922019215100通.zip (1 KB)

拝啓
配達員が注文番号 447231584780 の商品を配達するため電話で連絡を差し上げたのですが、つながりませんでした。従ってご注文の品はターミナルに返送されました。ご注文登録時に入力していただいた電話番号に誤りがあったことが分かりました。このメールに添付されている委託運送状を印刷して、最寄りの日本郵政取り扱い郵便局までお問い合わせください。
敬具
日本郵政ジャパンの宛先：
〒108-3353
東京都港区芝浦
[redacted]ビル 13F
日本郵政
[redacted] 2016 05:45:41

差出人を偽装!!

Check! Check! Check!

不審なメールアドレスに注意!!

添付ファイルに注意!!



■ 被害防止対策

- 見覚えの無いメールの添付ファイルは、開かずに差出人に確認!
- ウイルス対策ソフトを導入し常に最新の状態に!
- 通常業務に使用する端末と機密情報やネットバンキングを扱う端末を分ける!
- 端末利用者に対する教養・訓練を実施する!