

## 口座狙うウイルス「スパイアイ」か ネット銀行の偽画面



「スパイアイ」ウイルスの手口

【須藤龍也】インターネットバンキングで偽の画面が表示され、不正に送金された事件で、金融機関を標的にした「Spy Eye（スパイアイ）」と呼ばれるウイルスの一種が使われた疑いの強いことが、複数のウイルス対策会社の分析でわかった。こうしたウイルスは海外で猛威をふるい、昨年ごろから国内でも目立っており、専門家は注意を呼びかけている。

複数のウイルス対策会社の分析によると、今回使われたウイルスは、感染したパソコン（PC）のネット閲覧を「傍受」し、データを改ざんしたり抜き取ったりする機能がある。

事件では、ネットバンキングの利用者がPCでアクセスすると、ログイン画面に本来求められない暗証番号や契約者情報を入力する項目を追加したり、偽の画面を表示させたりしていた。振込先を、利用者が指定したのとは別の口座に置き換え、送金手続きする機能もあるという。

金融機関やクレジットカード会社を狙うスパイアイは2010年2月ごろ、欧米で見つかった。情報セキュリティー会社「ラック」（東京）の西本逸郎専務理事によると、その約1年半後の昨年夏に日本の金融機関が初めて標的にされたという。

利用者は普段通りの手順でアクセスするため、異変に気づきにくい。ウイルス対策各社はスパイアイを駆除する対策を施してきているが、スパイアイは次々と亜種を作り出す機能があり、いたちごっこの状態だ。

ウイルス感染をどう防ぐか。対策各社は「不審なメールや添付ファイルを開かない。知らないサイトからソフトをダウンロードしない」などと呼びかけている。

#### ■ 「日本語の防壁」弱まる

海外で大規模に感染したウイルスが日本で広がらなかったのは「日本語の壁」があったからだ、と専門家は指摘する。スパイアイのケースでも、日本語で書かれた金融機関のホームページをウイルス作成者が理解できず、ウイルス上陸の抑

止力となっていたとされる。それが乗り越えられつつある。

日本語の分かる人物がウイルス作成者と結びついた、と複数の専門家は指摘する。「日本在住の中国人がネットバンキングの不正送金に絡み次々逮捕されている。偶然の一致とは思えない」。今回の事件でも中国人の影が見え隠れする。

別のセキュリティー専門家は、最近解析したウイルスが表示するメッセージや感染を誘発するメールの文言が、すんなり読める日本語で書かれていることに驚く。「つまり」「ところで」などの接続詞の使い方で引っかかる程度。「以前は機械による自動翻訳のようにギクシャクしていた。日本語が使える人物がかかわっているのは間違いない」

事情はサイバー攻撃でも同じだ。今年6月、財務省や最高裁のホームページなどを閲覧停止に追い込んだ国際的ハッカー集団アノニマスは「我々は必要とあらば言語の壁を越えて行動する」とツイッターで宣言した。

「日本語がわからず、情報がなかった。ずっと日本人とコンタクトしたいと思っていた」。6月、アノニマスたちが情報交換するサイトでは、日本語を解する人物の参加を歓迎するこうした書き込みが相次いだ。

ネットを通じ取材に応じたアノニマスのメンバーは、「政府と言えば財務省」「今の政権は民主党」など日本人とみられるメンバーの助言で攻撃対象を決めた、と証言した。

攻撃はやまない。7月27日には東京電力が新たな攻撃対象に加わった。「原発問題への対応で批判が集中していることを知った。攻撃対象を募ったネットの情報も参考にした」。アノニマスのメンバーは話す。

---

朝日新聞デジタルに掲載の記事・写真の無断転載を禁じます。すべての内容は日本の著作権法並びに国際条約により保護されています。

Copyright ©2012 The Asahi Shimbun Company. All rights reserved. No reproduction or republication without written permission.