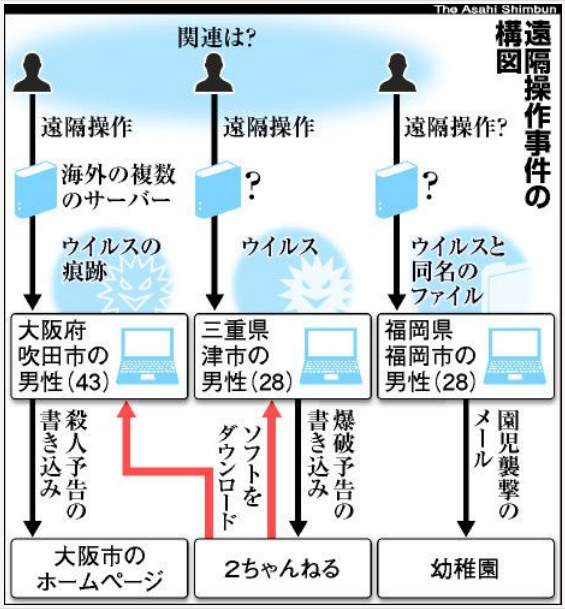
朝日新聞
THE ASAHI SHIMBUN DIGITAL

2012年10月11日03時00分

3人のPCに同名ファイル　遠隔操作の感染源か



遠隔操作事件の構図

ウイルスに感染していた大阪と三重の男性のパソコン（ＰＣ）からネット上に犯罪予告が書き込まれた事件で、大阪の男性のＰＣからは、遠隔操作でウイルスや書き込み履歴などが消されていた疑いがある一方、三重の男性のＰＣにはいずれも残ったままだったことがわかった。

２人のＰＣからは、同じウイルスが仕込まれた同名のファイルやその痕跡が見つかっているが、遠隔操作の仕方が異なるため、警察当局はウイルスの発信元が異なる場合も視野に捜査する方針。

捜査関係者によると、大阪府警に逮捕され、その後釈放された大阪府吹田市のアニメ演出家北村真咲（まさき）さん（４３）は、ネット掲示板「２ちゃんねる」を経由して無料ソフトをダウンロードした際にウイルスに感染。何者かが遠隔操作で大阪市のホームページ（ＨＰ）に殺人予告を書き込んだ可能性がある。

しかし、府警が北村さんのＰＣを解析したところ、無料ソフトをダウンロードした記録や大阪市のＨＰへの接続履歴が消えており、ウイルスのファイル自体も消去されていた。府警は復元作業からこれらの痕跡を見つけたが、ウイルスの発信者が証拠隠滅を図ろうと、北村さんのＰＣ内の履歴を遠隔操作で消した疑いがあるとみている。

一方、三重県警に逮捕された津市の男性（２８）＝釈放＝も、２ちゃんねる経由で無料ソフトをダウンロードし、ウイルス感染したとみられる点は大阪のケースと同じだ。しかし、ファイルそのものやいずれの履歴もパソコンに残されていたという。

また、北村さんのＰＣには、海外の複数のサーバーを経由して遠隔操作された痕跡が残っていた。捜査から逃れるために複雑なルートを使っていた疑いもあるという。しかし、津の男性のケースでは、三重県警は海外サーバーが経由された可能性は低いとみている。

お茶の水女子大付属幼稚園（東京都文京区）に脅迫メールを送ったとして逮捕

された福岡市の男性（２８）＝処分保留で釈放＝のＰＣからも、同じ名前のファイルが見つかった。しかし、実際にウイルスに感染していたかどうかは不明という。

◇

■海外経由なら究明難題

【須藤龍也】海外の複数のサーバーを経由して遠隔操作する手口は、これまでのサイバー攻撃などでもたびたび使われてきた。海外を経由することで発信元をたどることが極めて困難になるためだ。

ただ、情報セキュリティー会社・ネットエージェントの杉浦隆幸社長は書き込みの内容などから「遠隔操作をする第三者は国内にいる」とみる。

世界中に点在するレンタルサーバーを複数利用すれば、警察当局が通信記録をたどる手間を増やし、時間稼ぎができる。借りたサーバーの契約を解除すれば通信記録も消せる。

過去にも、警視庁などの国際テロ情報に関する文書が流出した事件では、ルクセンブルクのレンタルサーバーを経由して、ファイル共有ソフトで拡散した。日本の警察は海外のサーバーを直接捜査できず、流出元を特定できていない。

海外サーバーを経由した遠隔操作は高度な技術に見えるが、米セキュリティー対策大手マカフィーの本橋裕次サイバー戦略室長は「遠隔操作の仕組みを売る地下業者がいて、知識がなくてもサイバー攻撃ができる」と明かす。

同社によると、遠隔操作のウイルスに感染したパソコンやサーバーは「ボット」と呼ばれ、サイバー攻撃などのために有料で貸し出す地下業者もいる。その価格はたとえば「銀行口座への攻撃は５００回あたり５千ドル」などと細かく設定されているという。

本橋室長は「今回の事件は氷山の一角。国内でもボットからの送信は１万５千近く確認されている。次の指示をじっと待っている状態だ」と語った。

◇

■ファイル名「アイシス」ウイルス感染

３人のＰＣから見つかったファイルは、いずれも「ｉｅｓｙｓ（アイシス）．ｅｘｅ」と呼ばれる名前だった。遠隔操作ウイルスが仕込まれた疑いがあり、警察当局が解析を進めている。

一方、ウイルス対策大手のトレンドマイクロは１０日、このウイルスを検知で

きるソフトを開発したと明らかにした。ウイルスを解析したところ、企業などを狙ったサイバー攻撃に利用されてきた遠隔操作タイプの一種だった。

感染先のＰＣの画面情報やパスワードを読み取ったり、感染ＰＣにファイルを送ったり無断で取り出したりする機能がある。ウイルスの発信者はネット上の掲示板を通じて感染ＰＣに指令を送り、感染ＰＣは掲示板に指令を受け取りに行って作動する仕組みという。

このウイルスを検知し、感染を防げるよう、ホームページからの対策ソフトの有料ダウンロードや、同社の既存ソフトの自動更新を始めた。

◇

■不審メール開かないで　無料ソフトは危険

ウイルス感染からパソコンを守るには、どうすればいいのか。

独立行政法人・情報処理推進機構（東京）のセキュリティー担当によると、まずはウイルスの感染を防ぐ「ウイルス対策ソフト」を導入することが基本だ。次々に生まれる新手のウイルスを防ぐため、対策ソフトは常に最新版に更新する必要がある。しかし、新手のウイルスには効かないこともある。

メールの添付ファイルで感染することもあり、不審なメールは開かずに削除する。他人になりすまして届くメールもあり、開く前に本当に本人からのものか確認した方が無難だ。

特に危険なのは、今回の事件のように無料ソフトをダウンロードする行為だ。見知らぬサイトからのダウンロードはもちろん、大手の無料ソフト提供サイトでも安心できない。大手サイトで配布されていた無料ソフトに、ウイルスが忍び込んでいたケースもあるためだ。担当者は「むやみにダウンロードしないことが最善の防衛手段。パソコンをそこそこ使い慣れた人が一番危ない」と注意を促している。

◇

■ウイルス感染が疑われる兆候

（１）システムやアプリケーションが頻繁に固まる。システムが起動しない。

（２）ファイルが無くなる。見知らぬファイルが作成されている。

（３）タスクバーなどに妙なアイコンができる。

（４）いきなりインターネットに接続しようとする。

（５）意図しないメール送信をする。

（６）ハードディスクの音が気になったり、動作が重かったりするなど、直感的にいつもと違うと感じる。

〈独立行政法人・情報処理推進機構による〉

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.