幡多ＩＴ署事件簿　Vol.1 - ゾンビ -

主な登場人物

ヨシオ：（私設）幡多ＩＴ署の署長兼捜査員。

Ａ社長：高校時代のヨシオの同級生。現在は建設会社の社長。

Ｂ君：Ａ社長の近所に住むフリーのＩＴ技術者

１．発端

2012 年 7 月 27 日金曜日の午後、突然ヨシオの携帯電話がけたたましく鳴り始めた。発信者はヨシオのアドレス帳には登録されていない番号だ。電話番号を見ると、その市外局番は県内の「とある都市」である。

「一体誰だ？」ヨシオがいぶかしながら電話を取ると、いきなり...

A「もしもしヨシオ君？ 高校の同級生のＡやけんど...覚えちょう？」

ヨシオ「えっ！？」（A...？ はて...？）

ヨシオが通っていた当時の高校で、ヨシオの学年は総勢約 300 人。しかも帰宅部だったヨシオは親しい友人も数えるほどしかいない。

A「ほら、２年の時に同じクラスやった...」

ヨシオ「..あぁ..ひょっとしてＡ君？」

A「そうそう！Ａ！ お久しぶり！」

ヨシオ「久しぶりやねぇ！元気にしようが？」

A「元気は元気ながやけんど、パソコンの事で今、様（ざま）に困っちょうがよ...」

ヨシオ「どうしたが？」

A「あのねぇ...Excel が動かんがよ！ ウイルスにやられちょうみたいながよ！」

A「うちの社員と近所の知っちょう人にも色々やってもろうたけんど、直らんがよ！」

ヨシオ「うん...わかった。自分、車が運転できんけん、
　　大変申し訳ないがやけんど、幡多ＩＴ署まで迎えにきてもろうて構んろうか？」

A「わかった。今すぐ行くけん！」

ヨシオ「えぇー...今からかえ！？」

A「すまん！どひたち急がないかんがよ！」

２．通報の経緯

それから程なく、シルバー塗装の高級車が幡多ＩＴ署に乗り付けてきた。車から降り立ったのは、恰幅の良さそうな社長さん風の出で立ちのA君である。彼は挨拶もそこそこに、「とにかく車に乗ってくれ。詳しい事は車の中で話す」との事。

彼は最近、お父さんが経営していた建設業を継いで社長となり、域内でも中堅の建設会社を奥さんと一緒に切り盛りしている。

この度、比較的規模の大きな土木工事を竣工（完成）させ、来週に発注者である行政機関の完成検査を受ける予定との事だ。

完成検査には必ず成果報告書が必要であり、それを提出しないと検査には合格できない。もし、成果報告書が間に合わなければ、定められた工期内に工事が完了したとはみなされず、契約違反の謗りは免れない。結果的には違約金を課せられたり、施工業者としての評価が下がるなど、会社の経営にとっても極めて深刻なダメージを及ぼす事にもなりかねない。

ところが...である。成果報告書の作成に、どうしても欠かせない Excel のファイルがコンピュータウイルスに感染し、計算しようと思ってもヌード写真を表示して、全く正しく機能しないという状況に直面したのである。

Ａ社長の会社の従業員がコンピュータウイルスを発見したのは３日前の火曜日の事。当初は「ウイルス対策ソフトで駆除すれば何とかなる」と、高をくくっていたようだ。従業員に指示して放っておいたのだが、木曜日になってその従業員から、どうしてもコンピュータウイルスを駆除できないという報告を受けた。それではという事で、Ａ社長の人脈を駆使して域内のパソコンに詳しい技術者を３人ほどかき集めて駆除を試みたのだったが、どうしても駆除できない。

ついには技術者たちも完全に匙を投げてしまった様子で、

「社長… 申し訳ないけんど、僕らの手に追えんですよ...」

その言葉には、さすがのＡ社長も血の気が引いた。

しばし、空虚な時間が過ぎ去った後、ふと、技術者の一人が...

「…ヨシオさん...幡多の...」

他の２人も、はっとしたかのように、思わず首を縦に振った。

Ａ社長「幡多のヨシオさん言うてどんな人？　頼めるがかえ？」

しばらくの間、ヨシオに関する情報が技術者達から社長に伝えられた。

Ａ社長「ひょっとして... ヨシオさん言うて...同級生のヨシオ君か？！」

“多分そうそう”と頷く技術者たちの相槌を確認するが早いか、Ａ社長は技術者の一人からヨシオの連絡先を聞き取り、速攻で電話をかけたのだった。

３．現場到着

18 時 30 分、ヨシオはＡ社長のスピード違反まがいの運転によって、早々に事件現場であるＡ社長が経営する建設会社の本社に到着した。

10 台ほどのパソコンが並ぶ設計室には､先程の技術者の一人であるＢ君が待機していた。ヨシオはＢ君から詳しい状況を聞き、その上で適宜な対応を取っていく事とした。

まずは、コンピュータウイルスに感染しているパソコンの特定だ。どうやら２台のパソコンが感染しているらしい。すぐさま２台のパソコンのＬＡＮケーブルを引き抜いてネットワークから隔離。その上で、全てのパソコンのウイルスチェックを開始した。

「多分、コンピュータウイルスとしては検出されないだろう…」（ヨシオ）

さて、いよいよ問題の Excel ファイルだ。Ｂ君の報告によると、このファイルの中に幾つかのマクロ（プログラム）が埋め込まれていて、その中にコンピュータウイルスらしきものが混ざっているとの事。

ヨシオが特殊な方法でこれらのマクロを自動的に実行できないようにした上で Excel ファイルを開いてみると、果たしてその中には６個のマクロが登録されていた。マクロの中を覗いてみると、その中の一つに明らかに疑わしい部分を特定する事がでた。

この疑わしい部分が、具体的にどのような働きをしているのかの詳細については割愛するが、おおよそ以下のようなものである。

(1) 悪さをする（今回の場合はヌード写真を表示して、本来の機能を妨害する。ヌード写真そのものはインターネット上にあってパソコン本体にはない）
(2) 自分自身が削除されそうになると「共犯者」に通知する
(3) 少なくとも通常のコンピュータウイルスのようなアプリケーションソフトの脆弱性（弱点）を突いた造りはしていない（合法ドラッグならぬ、合法コンピュータウイルスの可能性がある）

どうやら自分自身が削除されそうになると、その直前に共犯者の手を借りて、一時的に他の場所（予め用意された隠れ家）に身を潜め、一定時間（それが数日かも知れないし、すぐかもしれない）が経過すると再びマクロとして自動登録しているようだ。

普通ならば「なんだ！このマクロを削除すればいいじゃないか！」と思って処置するのだろうが、こいつの場合、ゾンビのように数秒から数時間後には甦っているという、何とも技術屋泣かせの「嫉こいコンピュータウイルス」である可能性が高い。

「駆除完了です！」と言って技術者が帰った後、再び開いてみると全く治っていないという事で、技術者の信頼を失墜させる。まさに「技術屋殺し」のコンピュータウイルスだ。

４．現場検証

こう言った、ある意味「嫉こいコンピュータウイルス」は、最近はその数こそ減ってきたものの、運悪く遭遇してしまう可能性は否定できない。この手のコンピュータウイルスを駆除するためには、基本ソフトやアプリケーションソフトの動作の仕組みをかなり詳細に把握した技術者でなければ対処できない。また長年培った経験と勘も必要だ。敏腕刑事と同じく、過去の犯行の手口を知り尽くし、折々の社会情勢や流行なども考慮しながら、その手口を絞り込んでいく必要がある。それと、その犯罪がどのような条件下で起こったか、例えば基本ソフトは Windows XP or 7、とか、Office は 2003 or 2007 or 2010 などの諸々の条件を把握しておく事も大切だ。（実際 Office2007 と 2010 は見かけも違うが、それ以上に内部構造が大きく違う）

２１時頃、Ｂ君の報告や実際の動作検証によって、手口に関しては一つの推論にたどり着いた。

まず状況証拠。（詳細を書くともっと複雑な事になる）

(1) 感染した Excel ファイルを開くと「隠れ家」が必ずできる
(2) 「隠れ家」はハードディスクの中の“ある特殊な場所”にひっそりと作られる
(3) 「共犯者」は Excel ファイルの外部に存在していて、Windows が起動されると同時に隠れたプログラムとして動いている可能性が極めて高い

つまり、(3)の「共犯者」である隠れたプログラムこそが主犯だという事になる。しかし、もしもこの推論が外れていれば、以後の対策は全くの水泡に帰する。しかし完成検査を間近に控えたこの段階に至っては、もはや一種のバクチを打つしか手がないような状況である事も、また事実である。

そして手口の特定。（これも詳細を書こうと思えばもの凄く大変だ）

(1) まず主犯は Windows の動きを絶えず監視している。 Excel から Windows を経由して、主犯に「Excel のマクロのうち問題のあるやつを削除する命令が出ましたよ」というような「お知らせ」が届く。
（このような「Windows からのお知らせ」は、言わば「Windows 国の公報」のようなもので、原則として動作中の全てのプログラムに速やかに届けられるという事が Windows 国の法律に明記されている）

(2) すると主犯は、Windows に対して「ちょっと待って！消してもええけんど、消す前に、ちょっとやっちょかなぁいかん事があるけん、ちょっと待っちょってよ。作業が終わったら直（じき）に連絡するけんね！」と申し立てを行う。（これを「割り込み処理」とか「トラップ（罠)」とか言う）
(3) 性善説に立つ善良なお役人の Windows さんは、直ちに主犯からの申し立てを認めて犯行が完遂されるまで素直にじっと待ち続ける。
(4) かくして、主犯はマクロが削除される前に、そのマクロの複製と、一定時間後に再びマクロを元の Excel ファイルに戻すプログラムを秘密の隠れ家に書き込んだ上で、「すまんねぇ！終わったけん！」と Windows に対して律儀にも直ちに連絡する。「…しめしめ！」（主犯）

５．捜査方針

さて、いよいよ犯人捜しだ。どうするか？

(1) Windowsに標準装備されている「現在動作中のプログラムの各種の情報を提供する」ソフト（タスクマネージャ）を開いて、すべてのプログラムの動作を監視する。
(2) 各々のプログラムからどんな命令が出されているのかを監視し、Excel のマクロを削除するという「お知らせ」が出された時に、どのプログラムがそれを受け取って活動しているのかを特定するための”簡単なソフト”を急ごしらえで製作して監視する。

要するに、(1)は「今どんな人が動いているのか？」であり、(2)は「その中で誰が犯行を行ったのか？」という事である。そこで、(1)と(2)のプログラムが連携しながら「張り込み」を行う体勢を作り上げるのだ。その上で、囮捜査を仕掛けて犯人が網にかかるのをじっと待つと言う戦法である。

本来ならば「デバッグツール」と呼ばれる自動監視ツールがあるのだが、それを導入できるような時間的な余裕は、もはや残されていない。結果として、手間はかかるが“昔ながらのマニュアル的な捜査手法”を使って、犯人を丹念に追い込んで行こうとヨシオは判断したのだった。

６．張り込み開始

日付が変わって午前１時。急ごしらえのソフトが完成。ついに「張り込み」を行う体勢が整った。

テレビではロンドンオリンピックの開催を告げる華やかなテーマソングが繰り返し流されている。Ａ社長から「もう帰ってもいいよ」と言われていたＢ君だが、帰る事なくヨシオの作業を後ろから一心に見つめている。Ａ社長も余程申し訳ないと思ったのか、彼の奥さんに電話して３人分の夜食の差し入れを運んできた。しばし休憩だ。

午前２時。いよいよ張り込み開始。

実は張り込みを開始すれば、犯人をすぐに特定できるというものではない。Windows では一見何もしていなくても、場合によっては１００本近いプログラムがその陰で動き続けている。いわゆる「常駐ソフト」と呼ばれるソフトをインストールすれば、その数は更に膨れ上がる。被疑者が１００人近くもいて、犯行の瞬間にそれぞれの被疑者がどのような動きをしたのかを、今回は高々２名の人間が目視で監視するのである。被疑者の絞込みには相当な困難が予想された。

何回も何回も感染した Excel ファイルを開いては、感染したマクロを削除し、その瞬間に不審な挙動を示したプログラムを絞り込んでいくと言う、いつ終わるかも分からない果てしない作業が延々と続く。

また、いい加減な特定をしてしまうと、それは「誤認逮捕」にも繋がりかねない。「無実のプログラム」を即決裁判で処刑した場合、そのプログラムが Windows やアプリケーションソフトにとって重要な役割を担っていたともなれば、最悪の場合 Windows 自体を起動する事が出来なくなる可能性もあるのだ。「誤認逮捕は絶対に許されない！」というプレッシャーが、ヨシオ達に大きくのしかかってくる。

幸い、Ｂ君が「汚染マクロの削除役」を買って出てくれる事となり、感染したパソコンに２台目の液晶ディスプレイを接続して二人一組で作業する事となった。１台目の画面でＢ君が汚染されたマクロを削除する（これが囮のアクション）、そして２台目の画面ではヨシオが「マクロが削除された瞬間」の被疑者たちの挙動を監視するという体勢だ。デュアルディスプレイにする事で、張り込み捜査は大いに捗った。しかし、それでも膨大な作業量になるかもしれないと言う事は容易に想像がつく。

背後のテレビに映し出されるロンドンの華やかな実況中継とは全くかけ離れた雰囲気の中で、Ａ社長が祈るように２人の囮捜査を見守り続けている。

７．被疑者特定

午前４時過ぎ。

「ん！...これ...か？」（ヨシオ）

「Ｂ君！もう一遍削除して！」（ヨシオ）

「はいっ！」（Ｂ君）

「うーーん…多分…今の所…多分だけど…」（ヨシオ）

傍らで舟の櫓を漕いでいたＡ社長が思わず身を乗り出してくる。

結局１０回以上、このプログラムに狙いを定めて検証作業を繰り返し、居合わせた３人全員が「これだ！」という確証を得た頃、既にオリンピックの開会式は始まっていた。

８．被疑者の素顔

「それにしても...何でこんな名前のプロセスが...」（ヨシオ）

ここで「プロセス」という用語について説明しよう。プロセスとは「プログラムが実際にパソコンの中で動いているときの仮の名前」の事だ。ちなみに、それぞれのプログラムには皆さんご存知の「ファイル名」と言う名前がついている。ところがパソコンの中では場合によっては、同一のプログラムが同時に何個か動く場合がある。そこで A というプログラムが同時に何個か動いた場合、パソコンはそれぞれ A1, A2, A3, …と言うように個々にプロセス名（仮の名前）をつけて管理しているのだ。時には、プログラムの名前（ファイル名）とプロセスの名前は全く異なる場合だってあり得る。

ヨシオは“重要参考人”として特定されたこのプロセスの名前が、巧妙に偽装されている可能性がある事に気付いた。ここでそのプロセスの名前について具体的に記術する事は割愛するが、そのプロセスがまるで Microsoft Office の一部であるかのような、言い換えれば“Microsoft の身内”であるかのような名前が付けられていた。

人間社会に例えれば、「まるで AKB48 に所属するアイドルのような、一見、出所身上も明らかで、虫も殺さぬような１８歳のかわいい女の子が、実はその裏で密かにゾンビの飼育に手を染め、A社長をはじめとする多くの善良無垢な市民を恐怖のどん底に陥れている」といった具合だろうか。
（もしこれが発覚すれば、週刊誌やスポーツ紙の１面トップを大きく飾る事は確実である）

かくして、被疑者は一人に絞り込まれた。しかし、まだ問題がある。それは、

(1) この被疑者が AKB48(Office)に属していると言うのは真っ赤なウソで、チャットやオレオレ詐欺で言う所の「成りすまし」のような存在なのか？ それとも…
(2) 本当に AKB48 に所属しているかわいい女の子（正真正銘の Office からの生成プロセス）にもかかわらず、実際にその娘が犯罪に手を染めているのか？
（アイドルの麻薬摘発のような感じ？）

という問題だ。

(1)の場合、パソコンの世界では即逮捕・即裁判・即処刑で何ら問題はない。

ところが(2)の場合、処刑してしまうと「AKB48 の機能」の一部が失われる事になり、芸能界(パソコン) 全体に少なからぬ影響を与えかねない。この場合、被疑者を裁判で懲役刑とし、しかるべく速やかに矯正教育（コンピュータウイルス部分の除去）を行わなければならない。

さて、彼女が(1)なのか、それとも(2)なのか... この解決策はある意味簡単だ。

AKB48 の事務所に連絡して、実際にその被疑者の娘が所属しているのか、そして彼女が当の本人なのかを事務所のスタッフに確認してもらえばいい。

実際には Microsoft は自社に所属しているタレント... じゃなかった、「Office から生成されるプロセス」については原則として公開していない。しかし大丈夫、ちゃんと Office の内部構造と動作原理を解析して、公開してくれている Microsoft の追っかけサイトが幾つもあるので、そこで探してみる事にした。

そして、地道で綿密な捜査の結果、彼女は AKB48 には所属しておらず、(1)である事がついに判明したのだ。

９．身柄確保

午前５時前。主犯格の女の逮捕状（電子計算機損壊等業務妨害罪の容疑）が裁判所に請求された。逮捕状の到着を待って、いよいよ女の身柄の確保にかかる。（実際のパソコンの世界では、逮捕状も裁判所も存在しない）

プロセスの名前から、ファイル名を特定する事はいとも簡単な話だ。案の定、女の居場所はすぐに特定できた。しかし、これで安心してはいけない。彼女はその見かけによらず、ゾンビを無尽蔵に生み出す事が出来るほどの「猛者」である。羊の皮を被った「狼」ではなく「Ninja」なのだ。ひょっとしたら、分身の術（自己複製）を使うかもしれない。また偽名（ファイル名変更）を使っていたり、変装によって年齢（ファイルの生成日時）や性別（ファイルの拡張子）を誤魔化したりしているかもしれない。

そこで、鑑識（バイナリエディタ）の助けを借りて、現場に残された彼女固有の DNA（プログラムの中のそのプログラムにしかない特徴的な部分）を特定し、パソコンに接続された全てのハードディスクの中の、全てのファイル（要するに全国民）に対して、彼女固有の DNA で検索をかけるという、空前絶後の大捜査網（全国民に対する完全な人定捜査）を展開する事となった。ちなみにこの作業、完了するまでに実に３時間を要した。
（たまたまハードディスク内の情報量が少なかった事が不幸中の幸いであった。ちなみに、ヨシオの使っているパソコンでこの捜査を行えば、単純計算で軽く３日はかかる）

その結果...いました！いました！まるでゴキブリの如くである。合計２０個を超える彼女の分身がハードディスク内の至る所に隠れ潜んでいたのだ。ちなみにその殆どが偽名。また、性別や年齢を大幅に誤魔化している者も多い。ゾンビを生み出す彼女そのものが、まさにゾンビだったのだ！

もはや、事件は「広域重要指定事件」に発展した。場合によっては「破壊活動防止法」の適用も視野に入る。遂に、幡多ＩＴ署の総力を挙げて、国内全てのアジトの一斉捜索と被疑者全員の緊急逮捕が決行された。（実際には１個のコマンドを打ち込むに過ぎない）

並行して海外の関連国（健全であると思われるパソコン８台）でも捜索が決行された。
（幸いな事に海外逃亡はしていなかった）

１０．事件終結へ

午前８時前、遂に全ての職務の執行（コンピュータウイルス除去作業）が完了した。

テレビからは、ポール・マッカートニーの「ヘイ・ジュード」の最後のフレーズが何度も繰り返され、オリンピックスタジアムの中の数多くの観衆と選手たちの朗らかな表情が、打ち上げられた花火をバックに次々と映し出されていく。開会式のフィナーレに呼応するかのように、ヨシオ達の戦いも次第にフィナーレに近づきつつある。

もうこの頃には従業員たちがぼちぼちと出社して来ていて、ヨシオたち３人の只ならぬ雰囲気を察してか、皆が立ったまま３人を遠巻きにして眺めている。Ａ社長の奥さんは従業員たちに事の経緯を説明して廻っている。当然の事ながら、いつもの朝礼は中止である。

いよいよ、最後の仕上げの時が来た。

「さぁ、マクロのけますよ！」（ヨシオ）

「うん！」（Ａ社長）

遠巻きだった従業員たちは、“その瞬間”をこの目で見ようと、自然とその輪が小さくなっていく。

「のけました。社長、開いて実行してみて！」（ヨシオ）

「よしっ！」（Ａ社長）

Ａ社長の声が震えている。彼はおもむろに Excel ファイルのアイコンをダブルクリックした後、深々と深呼吸してから、画面上に展開されたマクロの「実行」ボタンをクリックした。

一瞬沈黙...

「う・ご・い・た...！」（しっかりと瞑った両目の片方を薄く開きながら...Ｂ君）

「...動いたね！」（ヨシオ）

「...うん...」（もはや放心状態のＡ社長）

「うぉー！...」（居合わせた全員）

従業員も含めて、誰からともなく拍手と歓声が巻き起こり、思わず万歳をする者まで出る仕儀となった。

ヨシオはこれまでＩＴに関連する深刻な問題が劇的に克服されるその「歓喜の瞬間」に、捜査員（技術要員）として過去何度となく立ち会ってきた。ヨシオは、この瞬間を提供出来る職業に就いた事を、実のところ密かに誇りに思っている。

１１．その後

感染した２台のパソコンだが、完成検査が終わった後に幡多ＩＴ署付属病院に入院させ、精密検査の上、必要な治療を施す事となった。

ついに一件落着である。ヨシオはＡ社長の運転で、幡多ＩＴ署に帰る事となった。有難い事に、全従業員とＡ社長の奥さん、そしてＢ君が玄関まで出て、手を振りながらヨシオを見送ってくれた。

奇しき因縁で、実に３２年ぶりの再会となった同級生の２人。

シルバー塗装の高級車は、彼らがその死闘の上に勝ち取った“達成感”と言う名の香りに包まれながら、一路、幡多ＩＴ署へと向かって疾走して行った。

幡多ＩＴ署事件簿　Vol1. - ゾンビ -　おわり