第２８話（マルウェア解析について）

リバースエンジニアリング

タヌキ、今回はマルウェア解析だ。
開始する前に少し話しておくことがある。
マルウェア解析とは、言い換えるとリバースエンジニアリング
を行うということだ。

キツネ、マルウェアって何だ？

種々のコンピュータウィルスの総称がマルウェアだ。
広い意味でのコンピュータウィルスを指している。

リバースエンジニアリングって、初めて聞く用語だ
けれども何を意味しているんだ？

リバースエンジニアリングを簡単に表現すると、逆アセ
ンブルすることだ。

第３話のＣＰＵの説明でアセンブラ言語がチョッ
ト出てきたが、逆アセンブルって、あれか？

そうだ、あれだ。
アセンブラ言語で記述されたプログラムを機械（マシン）語に変換することをアセンブルというのは第３話で話したよな。逆アセンブルとは、１６進数や２進数で表現されている機械語をアセンブラ言語に戻すことだ。

その逆アセンブル（リバースエンジニアリング）とマルウェア解析とどういう関係があるのだ？

マルウエアつまり、コンピュータウィルスはプログラムだということは知っているよな。
このウィルスをソースファイルの形式で送りこんでくるようなアホなハッカーはいないよな。当然実行形式で送りこんでくるか、既存のファイルに組み込むよな。
実行形式というのは、機械語を意味する。機械語は１６進数や２進数で記述されている。１６進数や２進数で記述されているプログラムを解析することは無理だ。それで、逆アセンブルし、解析し易いアセンブラ言語に戻す、というわけだ。

アセンブラ言語に戻しても、オイラ、チンプンカンプンなんだけど。キツネはわかるのか？

オイラも、アセンブラ言語を読むのは苦手だ。時間もかかるし、疲れるし、ＯＳによって言語仕様（アーキテクチャ）も異なるし。でも一番コンピュータ（機械語）に近い言語なので、やるしかない。
４０年ほど前、まだ８ビットパソコンしかない時代、コンピュータ資源の少ないロシア（当時ソ連）やウクライナでは、プログラムの処理速度を上げる為にアセンブラ言語を手足のように使っていたので、今も優秀なコンピュータ技術者が多いのさ。

何事も、裕福になりすぎると人間は工夫をしなくなる、という典型だね。今は、コンピュータ資源が豊富にあるから、アセンブラ言語を使わなくても高級言語やＷｅｂ用のスクリプトで処理速度をそこそこ稼ぐことができるものね。
オイラもアセンブラ言語って知らなかったもの。

オイラ、日本の情報教育で情報に関する優秀な人材は育たないと思っているのだ。そりゃ、ワードやエクセル、スマホのアプリ操作の達人は育つと思うよ。でも、ＡＩのディープラーニングの基になるプログラムやハッキングの矛や盾になるプログラミングができる人材は育たないと思う。
なぜなら、情報の人材育成で小学校からいきなり、スクラッチでプログラミングさせるなんてことをやっているからさ。
スクラッチもプログラミング言語の一つだが、スクリプト自体を図形の中に隠してしまっている。理由は、情報嫌いを無くす為に、楽しく学ばせるということのようだ。
スクラッチに慣らされた生徒がアセンブラやC言語、Java 言語を学ぶようになるだろうか。面倒くせえ、となるのが目にみえてくる。当然、何人かの優秀な生徒がスクラッチの限界を知り、コンピュータの基本を学び、アセンブラの重要性に気が付き、自分で学び始めることを始めるでしょう。でも、それは何人かです。

キツネの言いたいことは解る。つまり、情報科学は、５大装置をコンピュータ内のデータの流れで把握することが基本である。その後に、アセンブラ言語→C 言語→Java 言語の順で学習することによってリバースエンジニアリングができる人材になる、ということだな。いきなりスクラッチで年少者をアホにしてはいけない、ということだな。
でも、日本の為政者が情報科学のことを学んでいないアホなのだから仕方がないよな。それよりも、マルウェア解析を教えてくれ。
オイラは乗り越えるぞ！