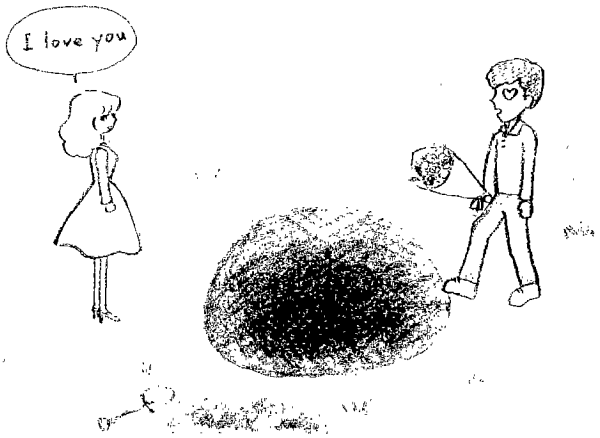
SEの知恵袋

第4回　I love you に大きな落とし穴

新貝 哲昌　日綱商事（株）
妹尾 稔　名古屋商科大学



最近新聞をにぎわせたのは「I love you」なるウィルスである．それ以前には「セキュリティ」とか「ハッカー」についての記述が多かった．卑近な例では「電子政府にハッカーの脅威」と記載されたのが平成12年1月27日（日経新聞・朝刊）である．これによれば科学技術庁，総務庁など政府のホームページが相次いで悪質なハッカーの侵入を受けたとのことである．政府ホームページの書き換え事件は日本政府がハッカー対策を決めたばかりなのに，日本政府に対するハッカー諸氏の挑戦といえるのではないだろうか．このような事態が頻繁に起きるのはなぜなのだろうか．空き巣が入りやすいのだろうか．ネットワーク社会の到来とともに，我々のコンピュータが世界中のどこのコンピュータにも常時接続されているのはもちろんであるが，適切な防護処置が施されておれば，そう安々と侵入され，被害に遭うことはないはずである．家の戸締まりと同じように，ネットワークの戸締まりという基本的なことについて考え直してみてはどうだろうか．IDとかパスワードの入手が攻撃の第一歩だそうだ．

SE諸君，我々の電子メールの通信文が誰かに解読される脅威について考えたことがあるだろうか？　あるいは自分のパソコンに見ず知らずの人（ハッカー）が侵入してくることを考えたことがあるだろうか？　パスワードはチャント管理してあるし，ウィルス検出ソフトも入れてあるので大丈夫だと安心していないだろうか．

まず，パスワードや暗号解読の初歩的なことから始めると，通信文のうち誰でもが読める文を平文（Planetext），何らかの変換規則（アルゴリズム）を用いて暗号文に変換することを暗号化（Encipherment），そして何らかの変換規則をもとに規則性を与えるものを鍵（key）といっている．暗号化された暗号文を平文に翻訳することを解読（Decipherment）というのは，もうご承知の通りである．歴史的に有名な暗号は「シーザ暗号」でローマの英雄ジュリアス・シーザーが始めたといわれている．

暗号解読について古い話で恐縮であるが，昭和の初期，我が国と当時の仮想敵国との国境で暗号解読・暗号研究に携わった方から直接聞いた話であるが，その地域を警戒中の日本兵を東から西に移動させるという．するとこの行動を相手方は暗号に組み立てて電報を発信する．その内容は多分「日本兵が東から西に移動した」とでもいうのだろう．西から東に移動させるとまた暗号電報が発信される．ここで東とか西の暗号が解読され，兵隊の人数を変えるなどすると数字が判明する．そのうちにこのアルゴリズムは有名な文章からだとか，キーは×××とかが判明してきたという．これは暗号解読をどのようにしたか，手探りで解読した初歩的な一例で

ある．今日，ハッカーも何らかの手法でこれに類する解読作業をしているのであろうが，パソコンを使用してさらにその処理速度も向上したため，難解なキーも解読の時間も短縮されている．

さらに次の例として，第二次世界大戦時の日米暗号戦争は有名である．1941年（昭和16年）5月5日のこと，駐米大使野村吉三郎氏は，東京の松岡洋右外相から次のような電報を受領した．「相当信頼すべき筋から入手した情報によればアメリカ政府は貴殿が発する日本からの暗号電報を解読しつつあるものの如くである」と．日本の暗号をアメリカは「Purple：紫」と呼んでいたが，これが解読されていたのである[1]．また，1943年（昭和18年4月18日），山本五十六連合艦隊司令長官機が南太平洋の海上で撃墜されている．ガダルカナルのヘンダーソン飛行場を発進した「双胴の悪魔」と呼ばれた米軍のP38戦闘機18機の待ち伏せ攻撃を受けた．これもアメリカ側に暗号が解読されていたことが原因である．この松岡外相の政府公電やミッドウェー海戦の敗戦原因を子細に検討して，然るべき対策を講じておけば未然に防ぐことができたことであろうに[2]．マージャンでいえば，自分の手の内を相手にさらけ出して勝負しているのと同じ理屈である．これではいかなるプロでも勝てない．国家存亡の大事な時にかけがえのないリーダを失ってしまった．

第1話の教訓は類推が容易なアルゴリズムとキーを使い続けるのは避けるべきことを示しているし，第2の話はこれが解読されているのと違うかとの疑問を持ち，新しい暗号に，今日的にいえばパスワードを頻繁に変更するということが基本で，この「基本の中の基本を守る」ということであり，ネットワーク社会の被害を最小限に食い止める基本ではないか．

SE諸君，我々はパスワードをいろいろなところで使用している．「パスワードの変更は頻繁に」[3]と筆者らオールドSEの知恵袋が記述しているが，この内容は，銀行や郵便局のキャッシュカードの暗証番号は他人に決して漏らさないように自分自身が十分に注意して管理してほしいこと．個人の財産に関することなので，他人に渡ると自分自身に直接大きな被害を蒙るのである．あまりにも秘密保持が徹底していて，夫婦の間で別々の預金通帳を持ち，暗証番号をお互いに秘密にしていて突然事故が起こり，言語障害に陥り，銀行預金が使えないという笑えない事実があったが，これは秘密保持が行き過ぎたのかもしれない．でも今日のようにインターネットやLANが発達して，同一ネットワーク上に多くのパソコンが接続され，サーバには各人の名前でデータが登録され，データの管理責任が大きく問われるようになった．顧客データが流失したとか，名簿が競争企業に売り渡されたとか．．．データの管理責任を確実にすることや社員の倫理の問題でもある．自社データを競合他社にいかほどかの金銭授受で漏らすとは言語道断である．オフィスで聞かれる会話の1つに，「このデータ・サーバは君が管理しろ．極秘のデータだから他人には絶対に漏らすな！」「ハイ，分かりました」「パスワードは他人に知られないようにしておけ」と厳しく通達をしておきながら，たまたまその担当者が突然会社を休むことになったならば，この厳しいお告げもたちまちご破算となる．上司から，担当の日満（ひみつ）君に，「人事のデータが今すぐ欲しいのだが，すぐ出してくれ」，「日満君は今日お休みですよ」「なに，じゃ，すぐ電話で聞け！」このような光景は普段よく見かける．担当者からパスワードを教えてもらえばたちまちにして，データ・サーバにアクセスできる．日満君は次の日に出勤したら何をさておいてもパスワードの変更をしておかねば大変なことが起きると思わねばならぬ．他人に知られたパスワードはパスワードではない，というのが記述の大要である．

最近のパスワードは使用のつど変更されるものも出回り，よりセキュリティの保持が確実になってきた．いわゆるワンタイム・パスワードの使用である．それから，外部からの不正な侵入を防ぐものにファイアウォール（Firewall）もある．これなどは企業の組織として，ハッカーから情報システムと企業資産を防衛する情報システム部門のSEとして十分に心にとめおく必要がある．

パスワードの解読ができれば，引き続き盗聴，なりすまし，データの盗難，さらには金融機関の預金口座への不正アクセスなど犯罪の種は尽きない．SE諸君，我々は頭の中では理解できるが，現実の問題としては実行が伴わない．パスワードの頻繁な変更，それから暗証番号は自分や家族の生年月日，電話番号など安易なものは避けるべきである．簡単で基本的な事柄を守ることで大きな事故を未然に防ぐことが可能になるのである．今後はネットワーク・ビジネスがますます盛んになる時代で，いわゆるB to Bと呼ばれる企業間取引の時代に「皆さんのセキュリテイ対策は万全か」という質問を投げかけ，いささか，オールドSEの説教になってしまい恐縮であるが古くて新しい基本について述べてみた．

参考文献
1）吉田一彦：暗号戦争，p.16，小学館．
2）吉田一彦：暗号戦争，p.63，小学館．
3）妹尾，新貝等：新時代を生き抜くSEの知恵袋，p.172，共立出版．

（平成12年5月16日受付）