ASIS INTERNATIONAL
Advancing Security Worldwide®
055 JAPAN

ASIS インターナショナル日本支部
広報担当理事　長瀬　泰郎

ASIS インターナショナル日本支部便り

7 月度セキュリティミーティング「サイバーテロの一側面」

7 月 15 日のセキュリティミーティングでは、前日本支部長で現在は、学術社団　日本安全保障・危機管理学会理事長の二見　宣氏による講演が行なわれました。以下はその要旨です。

地下鉄サリン事件と核攻撃

私の父は、大東亜戦争後にシベリアに抑留されていた。帰国すると小学生の私にそのときの話をよくしてくれた。その影響で私は防衛大学校に入り、陸上自衛隊で勤務した。現在は日本安全保障・危機管理学会を通じ、いろいろな危機管理に関する普及活動をやろうと思っている。

この学会を立ち上げる前にオウム真理教による地下鉄サリン事件などが起った。

病院に運ばれなかった乗客がそのまま一日仕事をして夕方になったら電気が暗いと言い出した。サリンガスは水にとけやすい。着ていた衣類に滲みていたサリンガスが汗腺や目・鼻・口の粘膜から体内に入り視神経などがやられてしまった。いまだに 5600 人に後遺症が残っている。事件直後に自衛隊が先頭に立って PR すれば、その被害者は1割(560)以下ですんでいただろう。霞が関駅を通過した人はみんな服を着替えてビニール袋に入れ、水を浴びるか、濡れタオルで体を拭けばよかった。日本社会は欧米と違い安全対策に触れず、その後も、「上祐がこう言った」、「松本千津男が牢屋で何を言った」、「誰が死刑判決を受けたか」ということばかりテレビで言って、再びサリン事件が起きたらどうすればいいかには触れていなかった。

同様なことが核兵器についても起きている。戦後反対政治運動はやっているが、もし核兵器が再び、日本に落ちたらどうすればいいかということはやらない。欧米はきちんとやっている。フィンランドやスイスは 90%の人がシェルターに入ることができる。アメリカも同様だ。30 年ほど前に米国アリゾナ州に留学したとき、生徒が教室からシェルターに退避する訓練を見学した。

核兵器で何が怖いかというと、熱と放射線が一瞬にして来ること。これは自分で防ぐことはできないが、大事なのはその数秒後の爆風で被害を受けないようにすることだ。(講演をしている)この部屋で言えば、窓ガラスが飛んでくる。速度は音速(秒速340m)。ガラスで目をやられないよう、目を覆いながら避難する。そんな訓練だった。

戦時中の私の田舎の防空壕は人があふれかえり、座っているのがやっとだったが、アメリカの学校のシェルターにはベッドがあり、ハンドボールコートがあって、3 か月いても退屈しないようにしてあった。欧米はこんな準備をしている。

フィンランドでは、窓が不要な音楽堂や劇場や駐車場を利用して、核兵器が落ちたときの収容施設にしている。

日本ではそんなことを一切していない。これはお金があっても 5 年や 10 年程度で完成するものでも

ない。そこで、自衛官なら誰でも知っている知識を一般に広げていきたいのだ。

■ サイバー戦争

サイバー戦争とは相手国の戦争能力を無力化するもので、典型的なのは湾岸戦争やイラク戦争だ。電子戦もやったし、変電所の上に鉄の鎖を落としてショートさせることもした。

現在米国と中国は、プレ・サイバー戦争状態にあるとも言われている。最近では「中国からのハッカー攻撃で機密資料が盗まれた」、「ネット攻撃で 1 秒間に百数十回アクセス」、「アメリカのエシュロン情報を翻訳した会社が中国政府の代理会社だった」など報道されている。また、中性子爆弾の機密情報を盗んだ疑惑などトラブルの種は尽きない。

■ サイバーテロ

サイバーテロとは、非戦闘員を対象とするもので、特定国の防衛・治安や外交・経済活動をはじめ重要インフラ機能をつかさどるコンピュータ・ネットワークと情報システムを機能不全にして自分の目的を達成しようとする行為である。形態としては「ネットワーク内」テロと「ネットワーク外」テロがある。

■ サイバー犯罪

サイバー犯罪には、コンピュータやインターネットなどの情報技術を悪用してサイバースペースで行われる犯罪と、ネットワーク外からの犯罪がある。よくあるのが銀行からお金を盗む話しや、パチンコ業の同業者潰し（ワゴン車に発信機を積んで、パチンコ屋の前で電波照射するとコンピュータが狂う）。

昨秋 16 歳の少年がオンラインゲーム会社の管理するコンピュータに不正アクセスし、ポイント購入画面を改ざんして、三日で 3600 万円だまし取ったという犯罪があった。また、不正入手した銀行キャッシュカードを使って携帯電話からインターネット銀行のコンピュータに不正アクセスし、110 万円引き出したという犯罪などが記憶に新しい。

■ サイバーいたずら

サイバー「いたずら」で有名な話では、イギリスの少年が米空軍の研究所に数か月不正侵入し、NAS など軍関係のネットワークにアクセスして多くの軍事秘密情報を持ち出した。「データスリム・カウボーイ事件」と呼ばれている。ファイアーウォールでちゃんとやっていてもこういうことが起こる。「起きる」という前提でものを考えているべきだ。今でもアメリカの国防総省などのコンピュータ・ネットワークに侵入したなどと自慢する人が存在している。

■ 戦争、テロ、犯罪、悪戯、事故

下表は、戦争、テロ、犯罪、悪戯および事故についての差異をまとめたものである。戦争とは国益と国益の衝突、テロは一般的には政治目的、サイバー犯罪は経済目的、サイバー悪戯は自己満足、サイバー事故は無意思といえる。

戦争、テロ、犯罪、悪戯、事故

	国益	政治	経済	自己満足	無意思
サイバー戦争	◎	○	○		
サイバーテロ	△	◎	○		
サイバー犯罪 インシデント		△	◎	○	
サイバー悪戯			△	◎	△
サイバー事故				△	◎

■ ネットワーク内でのサイバーテロ

ネットワーク内でのサイバーテロについて説明を略したい。これは、情報インフラに電子的に進入し、情報窃取、破壊、改ざんなどを行うもの。

一つの方法はコンピュータウィルスを大量発生させるもので日本-中国、日本-韓国間のテロが有名。

もう一つは大規模なハッキング。韓国で、中国軍所属の外国語学院を発信源として、韓国の情報機関などがハッキングされたことがあった。

■ ネットワーク外からのサイバーテロ

まずは EMP 攻撃。これは強い電磁パルスを発生・放射させることにより、電子機器を破壊ないし誤動作させる方法で、原理的には雷と同じ。発生方法として一番大きいのは核爆発。あとはミサイルや電子砲・爆弾などがある。爆発するとその付近の電子機器が壊れる。

■ テンペストによる情報搾取

次はテンペストによる情報搾取。アンテナを使い、コンピュータが発する微弱電波から情報を盗視する方法。盗まれるほうは全然気付かない。秘匿性が高いので、各国の情報機関でよく使われている。ひとつの機械でひとつしか情報収集できないので、重要人物のコンピュータに限られる。

テンペストによる情報収集は、気が付かないうちに取れるということで活用されている。大きな会社は注意しないと、隣のビルから新製品の情報を盗まれているかもしれない。

これに対抗して最近日本のあるメーカーが出したのが、電源に微弱な電波を発するパーツを一つはめ込んで漏洩電磁波を隠すという製品。少し前まではシールドルームくらいしかなかった。

■ 電磁波照射による対人殺傷テロ攻撃

次は電磁波による対人殺傷テロ攻撃方法。ミリ波やレーザー光線などを使い、殺傷するレベルではなく、目を見えなくさせる程度の機材が多い。

次は情報インフラの窃盗・破壊である。サイバーテロの中で一番簡単明瞭な手段。会社で火事やコンピュータがこわされたり、盗まれたりした場合はこれを疑ってください。なお、衛星破壊もこの類。

M 社のコンピュータが休みの日に盗まれた。中に入っていたのは戦闘機のフライングデータ。ドアーの鍵をこじあけの形跡がないため、外国人研修員の内部犯罪ではないかということになった。

天王洲アイルの大手コンピュータ会社で大量のコンピュータが盗まれたことがある。これは転売目的の窃盗ではないかといわれている。

事件直後はコンピュータを鎖でつないで持って行けないようにした。その後防衛各社は出入管理を厳格化し、かつ社員はコンピュータ端末を使用するだけ、ということをやるようになった。

■ サイバーテロにどう備えるか

サイバーテロにどう備えたらよいか。一般的には最近重要視されている BCP などの危機管理の考え方で対応すればいい。自社がサイバーテロに遭わないためには、人材の育成と敵に勝る技術の開発が一番大切。暗号はいつか解読されてしまうのでいつまでも暗号だと思わないほうがいい。セキュリティホールの除去やシールドルームは常識。

被害の未然防止については、長期的には、平時から情報収集や新技術の研究・開発を継続する。短期的には、不用不急なパソコンなどはスタンドアロンで使う、怪しいメールは開かない、重要な通信ネットワークはインターネットと分離またはクローズドネットワークにするなどの対策をする。

被害の拡大防止では、特定地域・分野のアクセスを遮断するほか、予想対象に逆にサイバー攻撃をする。なお、訓練と演習を継続するのはよいが、その都度改善しなければ効果がない。続けることによって進歩していく。そして関係機関と連携する。国レベルでは、国際法を制定する、そしてサイバー攻撃のための部隊を育成する。

最後に、安全保障で私が見出した法則を紹介する。「東から西に攻めれば、戦争は負けない」である。このため、東から攻撃されないように、警戒し、施策をしなければならない。

■ ASIS インターナショナル日本支部の月次ｾｷｭﾘﾃｨﾐｰﾃｨﾝｸﾞへのお誘い

ASIS インターナショナル日本支部は、月次セキュリティミーティング*を開いています。産業セキュリティに興味がある方ならどなたでも参加できます。お申し込みはホームページから！

■ 開催日　：　毎月第三火曜日午後 6 時半

■ 場所　：　国際文化会館（六本木）
東京都港区六本木 5-11-16
TEL: 03-3470-4611

■ 参加費　：　2,000 円

このコーナーへのお問い合わせや入会お申込みは
ASIS ｲﾝﾀｰﾅｼｮﾅﾙ日本支部　事務局まで
〒101-0021　東京都千代田区外神田 2-2-17
日本保安人事株式会社内
TEL　03-3255-3468　　FAX　03-3258-7630
E-Mail info@asis-japan.org/
www.asis-japan.org