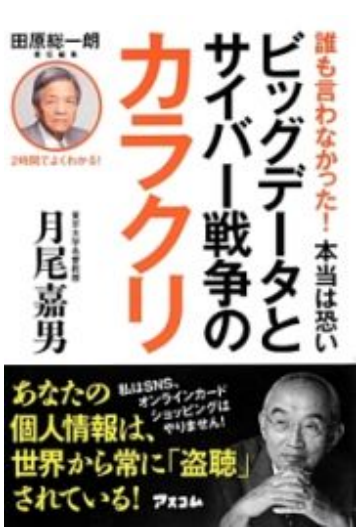


タイトル　誰も言わなかった！本当は恐い
ビッグデータとサイバー戦争のカラクリ

著　　者　月尾嘉男（つきお　よしお）
田原総一朗（たはら　そういちろう）責任編集

出 版 社　(株)アスコム

発 売 日　2013 年 12 月 6 日

ページ数　188 頁

「ビッグデータ」とは、膨大、多様で複雑なデータのことを指す。パソコンやスマートフォンなどを通して個人が発する情報や、コンビニの購買情報、カーナビの走行記録、医療機関のカルテなどなど、日々生成されるデータの集合を指し、これらは単に膨大なだけでなく、非定形でリアルタイムに増加・変化するという特徴を持ち合わせている。

人間が生み出す情報には限りがあるが、物と物、機械と機械は、高速で大量の情報通信を続けることが出来るようになってきたことがビッグデータの背景にある。

マイクロソフト、ヤフー、グーグル、フェイスブック、アップル、ツイッターなどビッグデータを生み出した張本人のはずの先進企業が、世界中の利用者から集めたデータをアメリカの諜報機関に密かに提供していたという。

アメリカの CIA（中央情報局）でコンピュータの保安技術者として勤務後、NSA（国家安全保障局）ハワイ事務所で 3 ヵ月間働いたという、エドワード・スノーデン容疑者が最近そう暴露した。

本書は月尾氏と田原氏の対談になっており、非常に判り易い。目次を見てみよう。

第1章　「ビッグデータ時代の到来」のカラクリ
第2章　「すべてが丸裸になるネット社会」のカラクリ
第3章　「ビッグデータ」のカラクリ
第4章　スノーデンが暴露した「サーバー戦争」のカラクリ
第5章　「サイバー戦争」最前線のカラクリ
第6章　誰も言わなかった、本当は恐いビッグデータ、その先にあるもの

著者は、ビッグデータに至る道筋を紹介しながら、クラウド（Cloud）時代を紹介する。

コンピュータが小型・高性能・低価格になると、一人一台になって会社には何百、何千というコンピュータが存在するようになった。最初は相互に関係なく使っていたが、次第に相互に通信し、データも共有するようになると、会社のサーバーと呼ばれる記憶装置に繋いで使うようになった。この時期はクライアント（端末）・サーバー時代といわれた。

そこにグーグルが新しい概念を持ち込んできた。グーグルは「会社で全員の端末を管理するサーバーは不要です。端末の記憶装置も最低限の容量があれば大丈夫です。グーグルのサーバーをお貸ししますから、そこへ情報を送って預けて下さい。何時でもどこでも利用できます」と提案した。これがクラウドサービスの始まりである。

グーグルのサーバーは全世界に膨大な数があるが、何処にあるかは意味がなく、利用者は無料で便利なサービスとしか考えていない。

グーグルは「ピカサ」という名前のサービスを始めた。これはデジカメ写真を数千枚でも無料で預かってくれる。必要な時は自宅のパソコンでも、外出先のノートパソコンやスマートフォンでも、インターネットに接続しさえすれば見ることが出来る。しかも、特定の写真を仲間だけで共有も出来るし、全世界に向けて公開も出来る。これがクラウドだ。

写真だけでなく、文書や映像などの情報も入っている。企業もクラウドに重要なデータを有料で預けて使っている。預けた文書に別の社員が別のパソコンからアクセスして文書を修正したり、共同で仕上げることが出来る。ネットワークに接続さえすればこのようなことが可能であり、便利だし、バックアップもできて安心である。

ところが、クラウドには大きな問題があった。多くの人が使っているグーグルの G メールはグーグルのクラウドを使ってメールを送受信するサービスだ。当初は 500 メガバイトという量のメールを保存できる容量を無料で提供していた。

G メールが始まる時、多くの人が「それは危険だ。管理者のグーグルに全ての情報が筒抜けではないか」と警告した。ところがグーグルは「社員が勝手にメールを見ることは絶対しません」と言っていた。ところが最近、スノーデン容疑者が「グーグルのクラウドに預けた情報は盗視されている」と暴露してしまった。つまり、クラウドは「自分の情報管理を放棄する」ということでもあったわけである。

無料だから多くの人が喜んで使っていたが、グーグルに預けた写真も映像も G メールも文書も、グーグルに筒抜けで、スノーデン容疑者によれば、裏側で NSA や CIA につながっていたというわけだ。

最近では、政府などの内部文書を公開する民間サイトの「ウィキリークス」や、先ほどのスノーデン容疑者の例もあり、情報の公開どころか、情報の暴露が当然という世の中になってきた。

中国の検索大手「Baidu（百度）」製の日本語入力ソフト「Baidu IME」が文字情報を同社のサーバーへ無断で送信していた問題で、同社が設定を改め、情報の外部送信を停止していたことが分った。変更について Baidu 日本法人は「担当者が不在のため回答出来ない」

としている。また、Baidu は、スマートフォン用の日本語入力ソフト「Simeji(シメジ)」については、27 日未明、「情報を送信しないように初期設定を修正したと発表。同ソフトでは、クラウド変換を利用しない設定に変更しても、入力した文字列が送信されていたが、これについては「プログラムの欠陥だった」と説明している。読売新聞 2013. 12. 28

インテリジェンスの世界では「だまされる奴がバカ」と言われている。この記事、上記グーグルの話を知った上で皆さんどう思われますか？

あの「幸福の王国」ブータンが、情報のために今変わりつつある。「情報」はあればあるほど良いというものではなく、時として様々な問題を引き起こす火種になるという。

ブータンは貧しい国だが、前国王が GNH（国民総幸福量）という概念を提唱し、GNP（国民総生産）や GDP（国内総生産）より、GNH のほうが大切だと宣言した。そのためブータンは「幸福の国」と言われてきた。

そのブータンが情報によって姿を変えつつあるという。ブータンでは 1999 年、国王がテレビとインターネットを解禁した。いまは首都（ティンプー：人口 9 万 9 千人）にインターネット・カフェがある。

4 年後の 2003 年には携帯電話が解禁され、すでに 63%の国民が携帯電話を持っている。これは 5 年前の日本と同じくらいの普及率だという。

その結果、何が起こったか。知ることで、国民は幸福になれたのだろうか？・・・・・。

2012 年 5 月に、「フレーム」という新種のコンピュータ・ウィルスが見つかった。これは、イランの核施設攻撃に使われた「スタクスネット」と非常に良く似た部分がかなり含まれていることが判った。「スタクスネット」と同じということは、アメリカとイスラエルの共同チームが作ったものだろうと推定されている。

今度の「フレーム」はプログラムの容量が「スタクスネット」の 1 メガバイトに対して 20 メガバイトで、コンピュータが「スタクスネット」に感染すると、ウィルスはそのコンピュータに潜伏するとともに、通信回線でつながった別のコンピュータに感染し、ある時感染したコンピュータの中で工作を始める。

「フレーム」は、コンピュータからコンピュータに感染していくところは「スタクスネット」と同じだが、感染したコンピュータから周囲の携帯電話や別のコンピュータに無線でどんどん指令を飛ばして、すべてをコントロールしてしまうという。

例えば、アイフォンなどのスマートフォンにはカメラがついている。そのスマートフォンが、「フレーム」に感染したパソコンのそばに置いてあると、「写真をどこそこに送れ」という指令によって、撮った写真を全部抜き取られるという。

最近では、そんな恐ろしいウィルスが登場している。これは、兵器が視野にあり、軍隊は、より早く、より遠く、より正確に、より効果的に敵をやっつけるものをつくりたいという本性があるからだと著者はいう。

さて、各国のサイバー戦争要員の現状は、どうだろうか？

圧倒的に進んでいるのはアメリカで、すでに 1990 年代初めから戦争情報センターという組織を作り、国防大学にサイバー戦争指揮官養成コースを設置している。現在、アメリカのサイバー戦争要員は 10 万人規模と言われている。アメリカのサイバー部隊の要員は、陸軍・海軍・空軍・海兵隊の 4 軍で、海軍には船を一隻も持たない第 10 艦隊、空軍には飛行機を 1 機も持たない第 24 空軍など・・・で構成されている。

アメリカに次いでサイバー部隊の数が多いのは中国で、数万人規模と言われている。中心になっているのが上海に拠点を置く通称「61398 部隊」で、アメリカの政府機関や企業などにサイバー攻撃を仕掛けているという。北朝鮮のサイバー部隊は数千人規模、韓国も後を追っていて 1000 人規模だそうである。

さて、我が国は残念ながら各国に出遅れて、小規模なものが作られる予定だという。各国は、サイバー部隊を創設して能力を高める一方、サイバー戦争の交戦規定も作っているという。

日本がサイバー戦争の取り組みで遅れている一番大きな理由は、憲法 9 条が国の交戦権を認めていないから、他国に対してサイバー攻撃が出来ないからだという。

実際、サイバー防衛だけでは効果がない。攻撃手段を研究しなければ、効果的な防御法は判らないからである。

日本の役所などが外国のハッカーに侵入され、書き換えられたりする。日本は慌てて防御策を講じるが、普通はどのように侵入してきたかを逆探知で調べるが、日本ではこれが政治的な問題になる。すなわち、逆探知によって外国の国内通信を探るのは、攻撃にあたるというのである。

日本はサイバー攻撃の能力も十分ではないけれども、それ以前に法的に出来ないわけだ。安倍政権は現状を変えるべく、鋭意検討を始めている。現状では、日本はサイバー攻撃が出来ない状態なので、中国は安心して仕掛けているようだ。

憲法 9 条のいう「武力攻撃」がサイバー攻撃を想定していないことは確かだから、なんとしても憲法改正は必要である。

いまや各国はサイバー空間を戦争空間と認める方向で、サイバー空間も国土と同じであることを考えれば、我々も本気で守る覚悟を待たなくてはならない。

政治家はフェイスブックを使わない方が良いと著者はいう。というのも、フェイスブックに載せた情報は本来、公開されるものだから問題はない。ところが、安倍首相がフェイスブックで発言した時、新聞の首相動静欄などと照合していけば、「彼に影響を与えた出来事は何か」、「裏でどのようなことがあったか」、「誰が情報を提供したのか」が推定されてしまう。「どういう経緯で何を考えたかが分る」から、「次にどのような政策を出してくるかという行動まで推定されてしまう」と著者は危惧する。

オバマ大統領は、一番セキュリティが厳重とされ欧米ビジネスマンに人気のスマートフ

ォン「ブラックベリー」を使おうとした時、「電子メールから機密情報が流出する恐れがあるから使うな」と言われたそうである。フランスでは、アメリカに盗聴される恐れがあるということで、閣僚はブラックベリーが使用禁止になっているという。

NSA が「プリズム計画」によってネットから世界中の個人情報をかすめ取って蓄積・分析しているというスノーデン容疑者の暴露に対して 2013 年 6 月、NSA 長官のキースは、「情報収集は実際にテロ阻止に役立っている」と米議会の公聴会で発言している。つまり、NSA の盗聴内容の一部は、アメリカを守るための対テロ防衛作戦にも利用されているというわけである。

サイバー攻撃は、コンピュータ・システムやインターネットなどを利用して目標のコンピュータやネットワークに侵入し、データを盗んだり、改ざんしたり、破壊したり、攪乱したりする。そして、敵のシステムを機能不全に陥らせる。

ここで重要なのは、成功したサイバー攻撃は全く表沙汰にならないという。サイバー攻撃でバレるのは「愉快犯レベル」で、プロのサイバー攻撃はバレないという。

最近の情報ではサイバー攻撃の目的が上記のような「情報搾取」から「インフラ破壊」へと大きく変化している。

さて、ノルウェーの元閣僚が、今年のノーベル平和賞候補にスノーデン容疑者を推薦したというニュースが入ってきた。推薦理由は、スノーデン容疑者が「機密文書を暴露したことで、世界がより安全な場所に変わった」と指摘。また、暴露によって、「国家が自国民をどの程度監視しているかについて、市民の理解が深まった」としている。

数年前からノーベル平和賞も質が落ちたなと感じていたが・・・・・。

ネット上に続々と登場してくる新しいサービスに飛びつく前に、それがどんなことをもたらすか、立ち止まって熟考しなければならない時代が到来した。

すなわち、プライバシーの問題はどうなっているか？ ビッグデータは良いことずくめなのか？ サイバー戦争の現状はどこまで進んでいるか？ などに興味や疑問を持っている人には特にお薦めの一冊である。

2014.1.26