

世界先端IT国家の具体像

昨年11月11日に開催された日装連理事・全国組合理事長会で、自民党IT戦略特命委員長・衆議院議員の平井たくや氏が、「世界最先端IT国家の具体像」と題して講演した。その詳細を紹介する。

第3次産業革命の真っ只中

今日の講演のテーマは「世界先端IT国家の具体像」ですが、では今はどんな時代なのか。

1760年代は蒸気機関の産業革命、1850年代は電気と石油、そして今はまさにコンピュータとネットワークの産業革命の時代の只中にあります。産業革命というのは、半世紀かかると私は思っています。

50年、60年かけて新しいものが生活の中に溶け込んで、世の中が変わってくる。第2次産業革命では電気と石油が台頭し、馬車や帆船などの産業が衰退しましたが、新しく自動車産業や航空産業が興りました。したがって、産業革命では淘汰、進化、創出を繰り返します。

今はちょうど第3次産業革命の真ん中にあります。

どうしてそう思うかというと、ここ10年の世の中の変化は本当に大きいのです。2001年の通信速度と今の通信速度を比べると850倍、赤ん坊が這う速度からジャンボジェット機の速度に変わっています。

皆さんが使っておられる 아이폰 や アンドロイド は、1997年にチェスの世界チャンピオンに勝ったIBMチェス用スパコン「ディープ・ブルー」よりも高性能になっています。

スマートフォンはスーパーコンピュータよりも上、それを無防備にネットワークにつないで持ち歩いているのです。そういう時代になっている。

こうなってくると、デジタルデータは商売になります。

日経が今後の日本を担うと期待される企業を選んだ上位中堅50社中、ICT関連企業で、データを活用することを生業にする企業が15社あります。

考えてみると、グーグルやアップル、アマゾンにしても全部そうです。結局、第3次産業革命の波に乗れた企業が大儲けしています。この動きは止まらないし、日本でもそうです。そして、私が委員長を務めている自民党IT戦略特命委員会です。いろいろなことに取り組んでいます。内容については、皆さんにまたお話しする機会があらうかと思えます。

我々が提言をつくるに当たっては、多くの民間企業等からヒアリングの機会をいただいております。

さて先週、国会で通ったサイバーセキュリティ基本法はどういうものか、お話しします。

私はずっとIT戦略特命委員長を務めていて、世の中が想定外の事態になっていると感じるようになりました。

これだけスマホが普及し、みんながコンピュータを持ち歩いて、ネットワークでつながる時代になった。

日に日にそのセキュリティの必要性を感じるようになりました。

2011年、私は野党の委員長だったのですが、民主党に早く法律をつくって国や地方自治体の危機を防がないと、大変な事態になると主張してきました。それを煮詰めたのが、サイバーセキュリティ基本法です。

なぜそういう準備をしなければならないか。2020年東京五輪でICTを使ったおもてなしは現時点では、すべて実現できることばかりです。

医療や酷暑克服、エネルギー、管路インフラなど、こういうものは全部、ICTで対応できると考えています。

東京五輪でのおもてなしということでは、自動翻訳機、これも英語、韓国語、中国語、韓国語から日本語へ、英語から韓国語へ、ほとんどストレスがない状態の音声の同時通訳というものを無料で提供できる水準になっています。

あまり進み過ぎて語学を学ぶ人が少なくなる懸念がありますが(笑)。

これはクラウドコンピューティングを利用しています。コンピュータによる処理やデータの格納をネットワーク経由でサービスとして利用する。スマホの中に通訳機能が入っているのです。辞書といいますか、音声認識のデータベースをどんどん大きくすると、大きくすればするほど、皆さんが使いやすいものになっていきます。

2020年五輪時には通訳は要らないということになります。

我々はこれらについて、実験し完璧に使えることを確かめました。ただし、ネットワークにつながっていなければならない。Wi-fiにつながっている必要があります。

第3次産業革命の観点からは、知らない間に皆さんが全部ネットワークに乗ってしまっていることになります。

皆さんは全くネットを使わずには仕事はなりたない。紙と音声だけでは駄目で、建設業でも入札からはじまってすべてのことがそうです。

サイバーセキュリティ戦略

インターネット前提の社会になったのは実は、この13年の間なのです。

2001年にIT基本法をつくった時、何もかもがここまでいくとは誰も思っていなかった。

아이폰にしても日本に上陸してまだ6、7年ですよ。それなのにこれだけの人が使っています。

第3次産業革命の変化のスピードは今までの産業革命とは違うと思って下さい。

そういうことになりますと、何が起きるか。悪いことをする人が増大してきます。2001年、IT基本法をつくった時はサイバーセキュリティの概念はありませんでした。

ですから、インフラをどんどん整備し、いつでもどこでもつながったら、それでみんな幸せになれると思っていたら、政府や金融機関、いろいろなものが攻撃対象になっています。事実、韓国やエストニアはサイバー攻撃によって、政府の機能がおかしくなりました。

今、日本政府がどのくらいサイバー攻撃にさらされているか。6秒に1回、霞が関が攻撃されています。電力会社などの重要インフラも攻撃されています。インターネットでなくても、電源がいつサイバー攻撃でダメになるかわからない。このような事態を看過できないところまできたので、ギリギリのタイミングでサイバーセキュリティ基本法が成立したというわけです。

自動運転の車がすでにハッキングされて、右に曲がろうとしたところ、左に曲がった。

怖いことですが、自動運転ですと車の保険料が安くならなければならなくなる。ところが、サイバーバックのリスクがあるので、保険料はもしかすると上がってしまうかもしれません。つまり、サイバー攻撃に対する保険概念が今は成立していますが、非常に危ういものです。

2012年のロンドンオリンピックでは2億件のハッカーによるアクセスがあった。

1秒間に1.1万DDOS攻撃(踏み台と呼ばれる多数のコンピュータが標的のサーバーなどを攻撃すること)を受けました。信じられません。

2020年東京五輪もターゲットになっていてこのレベルではないといわれています。

ロンドンオリンピックを開催したイギリスの場合は、開会式の電力制御をコンピュータで行っていました。開会式を停電させるぞ、という脅し、開会式が狙われるという情報があつて前日になって全部手動に切り替えました。

イギリスの信用を落とすには、開会式を停電させて全世界に中継すればいい。

その時、悪い人たちは株の空売りなどとセットで攻撃してくる。日本の東京五輪の開会式を守るためのチーム作りをそろそろスタートさせなければならないということになっています。このような中で、我々がつくった法律の概念があります。サイバーセキュリティ本部、国家安全保障会議などありますが、各省、民間企業要するに狙われないところはなくなった。それで国民にある程度自分のことは自分で守る、後は国や地方自治体の責任にして、その攻撃が国家安全保障に関わるケース、ただの愉快犯のケース、いろいろありますが、起きた事案に対応し、それぞれが機能的に働くための法律を私はつくりました。

攻撃を受ける側は情報共有を

野球でいうと、ヒットは打たれるだろう、だけどできるだけポテンヒットの数を少なくしよう、球がここに飛んだらここに取りに行くことを事前に決めておく。それでもヒットは打たれます。そうなので、盗塁を未然に防ぐ、本塁は何としても守って点はとられないようにする、というのがサイバーセキュリティ。ですから、100%守れることはありません。

東京五輪で一番リスクになっているのは、停電です。東京電力がスマートメーターというものを2020年までに各世帯に装備する。それによって柔軟な料金体系になり、自分の電力がどのように使われているかがデータで分かります。

しかし、それは通信回線につながる。ですから100%狙われます。あの工場を停電させる、あの家庭を停電させるのは料金のところをちょっと触れば簡単にできてしまうようになります。

もちろん、暗号などは使えますが、それでも必ず破られます。

スマートメーターは電力の自由化の流れの中で必要でしょうが、しかし、大きなリスクを抱えることになります。

100%は防げないので、やられたらすぐ気が付くようにする、停電される場合はできるだけ狭いエリアで終わるようなネットワークのあり方にしよう、復旧をできるだけ早くしよう、というようなことになっております。ですから世の中が進歩すればするほど、余分な心配が増えます。

そういう風に考えますと、不思議で仕方がないのですが、我々は攻撃を受けて対処する側、攻撃する側は情報共有ができています。我々守っている方はどこかで攻撃されても攻撃されたことを知られたくないので、抱え込むのです。だからいつまでたっても攻撃された側は情報共有ができません。そういうことを、この法律で、可能なかぎりなくそうというわけです。

攻撃できる人と守っている人が同じタイプの人という問題があります。もともとコンピュータが好きでハッカーの能力がある人、そういう人たちをいかに国にひきつけていくか、が大事です。最近、ハッカーに会う機会があつたのですが、彼らは普通のサラリーマンとか組織人とちょっと違う。

大学は東大、京大とかは出ていない。地方の大学か専門学校を出ていて、腕一つでコンピュータに関わっている。

我々に貢献してくれる200人のハッカーに前職を聞いたら、普通の会社に入れなかった、引きこもりです。

これらの方々に協力を得て今、守る側に立ってもらっています。

攻撃側につくか、守り側につくかは紙一重のところなので、周りにコンピュータが好きな引きこもり少年がいたら、こっちの世界へ連れてこなくてはなりません。

現実がそうなので、我々は危うい世界にいる、そういう現状を皆さんに知っていただきたかったし、これは全産業、全世界が足をすくわれる可能性がある。そこで最後になりますが、誰がこんな世の中を望んでいたのかと、ふと思うことがあります。私は2000年に当選してからずっとITをやってきました。

よく考えたらサイバーセキュリティはマッチポンプみたいなものです。守る側、個々の産業はどんどん大きくなってきて、いつのまにかロッキードマーティンとかボーイングなどはもう飛行機会社ではなく、サイバーセキュリティ産業として大きな研究所を持つようになりました。

人間性見失わず、ハイテク推進

こんな時代にしてしまった時にふと気づくことは何かというと、第3次産業革命の結末はどうなるか。

我々はこのまま調子に乗って行って幸せになれるのかどうかを考えなければなりません。

私は国で一番ITを進める立場にあります。ですからサイバーセキュリティ基本法、IT法案もつくってきました。日本みたいに少子化・高齢化で地方創生といった時に、やっぱりITを使わないと生産性は上がらないし、成長ができません。そういう立場にある私がふと考えるのは、このままだって大丈夫か、やっぱり手紙は手書きだな、万年筆もいいだろうということです。

バルト三国のエストニアはサイバーセキュリティがある、ただしこの国はWi-fiの密度が世界No.1、インターネットによって国民を幸せにして国を発展させる、ということを閣議決定しています。ですからIT一本槍の国です。

一方、キューバはアメリカと国交がないし、基本的にインターネットはつながりません。キューバに着いた日はメールが届かないのでイライラするのですが、2日目になるとこちらがいいなあと思うようになっています。要するにつながらない快感というのがでてくる。キューバみたいなのをデジタルデトックスといいます。インターネット依存症の人がそういうものから離れるというわけです。

電車に乗っている皆さん、スマホばかりやっているでしょう。これは病気ですよ。そういうのを治すにはつながらないところにいくのがいい。だから世界でつながらないところを何力所かつくっておかないといけません。

日本でも一時、携帯がつながらないといけないということで、山の中に鉄塔立てて、今はどこへいったって通じるでしょう。でも今考えてみたら、豊かな自然があるところでは通じない方がいいですね、そこはそこで切り替えたらいいと思います。

そんなことを考えた時に、ハイテクが進むとハイタッチ、人間同士の付き合いが大事になってきます。メールのやりとりよりは居酒屋で一杯飲んで話をつけた方が仕事も早いし、実際、我々は理屈を超えたところでやっています。つまり第3次産業革命の結末はわからないということ、それに振り回されて我々が人間性を失ってはいけないと考えます。そのことはすべてに当てはまりますし、日装連さんにおきましては西浦理事長をはじめ、その人間性を失うパターンにならないと思います。もう少しハイテクも使いながら、業界の発展に「いい」加減に取り組んでいただきたいと思います。ご静聴ありがとうございました。