○二十八番　神﨑　聡

サイバー空間における情報セキュリティ対策について

皆さん、こんにちは。食と緑を守る緑友会福岡県議団の神崎聡です。通告に従いまして、一般質問を致します。

小川知事は、年頭の挨拶の中で、「元気を西からという思いで、今年は、福岡県をますます元気にする、「元気躍進の年」にしたい」と述べられました。政治も経済も、社会そのものが不安定で激動の時代にあって、リーダー特にトップは、難局に臨んで動じず、これを好機として、飛躍を成し遂げる、組織の長として明るくて、しかも強くなければなりません。

私は、会社の社長時代、トップとしてお客様や取引先、社員の前でいつも明るく元気にエネルギシュに活動していました。ただ、株主や親会社からは、危機意識を忘れるな！コンプライアンスをしっかり守れ！リスク管理を怠るな！と、口を酸っぱく言われていました。

チェック機関というのは、いつの時代も、どこの世界でも、目を光らせ、厳しい指摘をするものです。

でも、そのお陰で、外に向かっては、明るく元気に、夢やビジョンを発信し、内の中にあっては、程度大切・油断大敵を心がけ、常に危機感を持ち、不測の事態に備えなければならないことを学びました。そして、一度、危機に直面した時には、何よりもスピード感を持って対処しなければならないこと。そのためには、平時における備えこそ、大切だという事を学んできました。

急速なＩＴ化の進展に伴い、情報の危機管理が求められている時代になってきました。最近では、サイバー攻撃によって、国の安全保障や個人の財産にまで影響を及ぼす大きな問題となってきています。情報化社会には、光と影があり、利便性と危険性が常に背中合わせであります。特に、様々な情報が集まっている行政関連機関は、利便性とともに機密性が要求されますから、情報管理には細心の注意を払う責務があると思います。従って、サイバー空間の脅威に対する対処能力は、喫緊の課題となっており、最善の防御策・対抗措置を早急に講じなければならないんじゃないでしょうか。

毎年２月は情報セキュリティ月間であります。先日、２７日には、九州経済産業局・総務省九州総合通信局による情報セキュリティセミナーが福岡合同庁舎で開催され、私も参加してきましたが、受講人数の多さに、情報セキュリティの関心の高さが伺われました。

サイバー攻撃における国防対策と言えば、とても遠くの話のように思われ、コンピュータ内部におけるセキュリティ・チェックと言えば、組織内におけるオペレーションの一つに捉われがちになりますが、国民・県民の安心・安全を図るためには、とても大きなテーマであり、かつ重要な政策課題だと思います。着眼大局・着手小局の視点で、このサイバー空間の脅威に対して、本県として、どのような情報セキュリティ対策を講じているのか、質問をしたいと思います。

本県においても、昨年１１月９日午後に、職員採用試験などの申し込み手続きができる電子申請システムが一時利用できなくなったという事態になりました。システムのサーバーにサイバー攻撃を受けたのが原因ということでした。また今年に入り、民間企業でも、福岡市の化粧品製造販売の通販サイトがサイバー攻撃を受け、顧客１４９３人分の氏名やクレジットカード番号等、個人情報が外部に流出し、カード情報の不正使用も確認されております。

そこで知事に質問致します。現在、本県では県が保有する情報資産を様々な脅威から保護するため、平成１４年３月、福岡県情報セキュリティ基本方針を定めております。この基本方針に基づいた物理的対策や技術対策、あるいは職員への研修など人的対策に、現在どのように取り組んでおられるのか、実施状況についてお尋ねします。

標的型攻撃メール等の対応では、インターネットから内部ネットワークに接続する入り口の部分で、全ての電子メールについてセキュリティ・チェックを行っていると思います。新たなサイバー攻撃は、市販されているウィルス対策ソフトでは検知できない“未知のウィルス”を使って、パソコンやサーバーを乗っ取り、機密情報等を外部に送り出します。

これまでは、外部からの攻撃をガードする入り口を中心としたセキュリティ対策を取ってきましたが、今後は外部への通信を監視し、情報漏えいを防御する出口対策、また、監視ログを取ったり、どういうルートで誰が持ち出したのか、追跡調査ができる対策が必要になってきます。現在どのような対策を取っていますでしょうか。また今後、どのような対策が必要だと認識されていますでしょうか。お尋ね致します。

職員を対象とした情報セキュリティ研修において、標的型攻撃メール等への対応はどのように図っていますでしょうか。職員全員を対象とした抜き打ち調査等を実施する事も必要かと思います。どのような研修になっているのかお伺いします。また、今後、強化すべき対策があればお聞かせ下さい。

基本方針の対策の実効性をしっかり確保するためには、セキュリティ監査が必要不可欠になってまいります。監査体制はどのようになっていますでしょうか。お伺い致します。

医療関連機関の情報セキュリティについても同様にお伺いしたいと思いますが、医療機関は、患者さんの情報など多くの機密情報を持っていて、日々、情報漏えいの危機にさらされています。医療機関の多くはオフラインで運用されているため、一般的に直接的なサイバー攻撃を受けにくいと思われていますが、実は人を介して、ＵＳＢメモリー等からの感染で情報流出するケースがあり、情報漏えい防止に向けた教育・研修がとても重要になってきます。

今後、医療を取り巻く環境は、病々診連携、医療・福祉・介護の地域における連携が、推進・拡大されてきます。ネットワークシステムとしては、効率性・利便性・運用面からもクラウド化への流れが医療・福祉・介護全般に普及していくことが予想されます。そのため、これまで以上の個人情報・医療情報等を安全性の高い情報セキュリティとして担保していかなくてはならないと思います。

そこで知事に質問致します。このような医療・福祉・介護分野全般にわたって、どのように情報セキュリティを担保し連携していくのか、システム間の連携、ネットワーク構築の基本的考え方をお伺い致します。関連機関への周知についても伺いたいと存じます。

サイバー攻撃の視点から、ＴＰＰによって懸念される医療情報・個人情報について、私は日本の公的保険でまかなわれています医療が市場開放されると、国内で保有している個人情報及び医療情報が、他国から開示を求められる事態になるんじゃないかと心配しています。先月２２日、米通商代表部がＴＰＰへの参加交渉や事前協議で、保険適用の診療と適用外の自由診療を併用する「混合診療」の全面解禁を対象外とする方針を日本政府に非公式に伝えていたこと報道されました。

全面解禁が国民皆保険制度の崩壊につながるとの日本国内の懸念に配慮しての譲歩だということですが、米国側は医薬品規制の見直し、保険事業の優遇措置撤廃などは譲歩しない構えで、

混合診療の全面解禁は、ＴＰＰとは別の枠組みで日本に要求する可能性もあるという事です。ＴＰＰに限らず市場自由化の中で、農業分野と共に医療分野、特に混合診療や営利目的の医療参入については、今後とも注視していかなくてはならないと思います。と申しますのは、混合診療の全面解禁をめぐっては、米保険業界が参入を狙っていることは、承知の通りです。

現在は、個人情報及び医療機関情報は、基本的にオフラインで運用し、国内で管理されていますが、米保険業界が公的保険に参入してくると、国民皆保険制度が崩壊すると共に、この個人情報・医療機関の情報等の膨大なデータが、米保険会社に集まります。ここをハッカーたちが標的として、サイバー攻撃を受けるという事になりますと大変な事態になってきます。

ご存知の通り、サイバー攻撃を受けた米国企業は、パトリオット法によりアメリカ大統領から直接開示を求められます。パトリオット法とは、米国内外のテロリズムと戦うことを目的とした米国の法律です。２００１年に米国で発生した同時多発テロ事件後に、捜査機関の権限を拡大する法律として成立しました。

情報通信の分野についての主な点は、電話回線の傍受に加えて、ＩＳＰ（インタネット・サービス・プロバイダー）における通信傍受も可能となり、捜査令状により電子メールやボイスメールを入手でき、またテロ活動の防止を目的としていれば捜査機関が金融機関やネットサービス企業に対してプライバシー情報の提出を求めることも可能になった点などです。

今後、パトリオット法に対抗できる日本版パトリオット法等の法整備も急務だとも言われていますが、本来、国でしっかりとした対策をとらなければいけない大きな問題だと思います。ＴＰＰ等によって、日本国内に参入してきた外国企業がサイバー攻撃を受け、それが私たちの手の届かないところで、日本国民の情報が開示されることにとても不安を感じます。サイバー攻撃によって危惧される個人情報・医療情報ついて、是非、国も地方も十分な議論を深めて頂くことを要望致します。

次に警察本部長にお尋ね致します。このように政府関係や関連企業のコンピュータやネットワークを狙ったサイバー攻撃は、これはもう犯罪ではなく、国の安全保障を脅かす、新たな脅威となっています。国家の重要機関や施設の機能を破壊したり麻痺させたりするサイバー攻撃は、国際的にサイバーテロとも呼ばれ、新たな“戦争”の形態と位置づけられつつあります。

警察庁ではサイバーテロ対策推進室を設置し、都道府県警察に対してサイバーテロ対策に関する指導・調整のほか、都道府県警察の職員に対する教育訓練を行うなど、総合的なサイバーテロ対策を推進しているということです。本県ではどのような体制で、諸対策に取り組んでいますでしょうか、お尋ね致します。

サイバーテロ対策の技術的基盤として、各管区警察局等に、サイバーフォースと呼ばれる技術部隊が設置されておられます。サイバーフォースは、全国の警察職員から選抜された高度かつ専門的な知識及び技術を有する者で構成されており、都道府県警察に対する技術支援を実施していると聞きました。そこで質問致します。機密事項があると思いますので、答えられる範囲で結構です。被害状況の把握、被害拡大の防止、証拠保全等の緊急対処活動を行うにあたり、十分な技術支援が受けられているんでしょうか。お聞かせ下さい。サイバーテロ対策を行うに当たっては、サイバー攻撃の手法や情報セキュリティに関する知識及び技術が必要であることから、対策に従事する職員を対象として、どのような教育訓練を実施しているのかも併せお聞かせ下さい。

次に教育機関の情報漏えい対策及び情報セキュリティ教育について教育長に質問致します。学校での個人情報漏えいについても後が立ちません。昨年一年間、報道されただけで９件の個人情報漏えいがありました。紛失・置き忘れ３件、盗難４件、誤操作・誤送信１件、そして今年１月には不正アクセスによるサイバー攻撃によって個人情報が流出しました。

先程から申し上げていますように、急速なＩＴ化の進展に伴い、情報セキュリティへのニーズが高まってきますと、国民のセキュリティリテラシーの向上施策を講じなければならないと思います。私は、義務教育段階から、セキュリティリテラシーに関する内容を学習カリキュラムに組み込み、子供たちがネット社会の一員となるための基礎的素養としてセキュリティ意識を身につけられるよう、検討を進めなければならないと思います。そのためには、教員に対して、セキュリティ意識を身につける研修が必要だと思います。どのように進められていますでしょうか。お尋ね致します。

また、県立学校ではどのような情報漏えい対策をおこなっているのか、併せてお伺いします。学校の特殊性に配慮した実効性のある、学校情報セキュリティポリシーの策定・改善・周知はどのようになっていますでしょうか。お聞かせ下さい。

情報漏えい事故等、発生時の対応としての対応マニュアル等はどのようになっているのでしょうか。また、現場に対しては、過去の情報漏えい事故等を受けて、どのような改善を図ってきたのか、情報漏えい事故に対する対応と改善について質問致します。監査の実施も必要と思われます。実施状況を評価し，具体的改善策を提案する内部監査・外部監査の実施も必要と思いますので、ご指摘させて頂きます。今後はクラウドコンピューティング技術の活用によって、情報セキュリティを担保し、加えて、教員が子供たちと向き合う時間を増加させ、先生方の校務の負担軽減を図り、教育の質の向上と学校経営の改善に資するためにもクラウドの活用が必要になってくると思います。教育現場においてクラウドを利用することによるメリットは、個人情報を私物パソコンやＵＳＢ等に保存して持ち出すことよる情報漏えいを、ローカル環境にデータを保存、複写できないようにすることで防止ができます。昨年６月定例会一般質問でも申しましたが、地域情報プラットホームの整備や福岡県の自治体クラウド化を推進する一環として、県立学校もこのクラウド化を進めなければならないと思います。教育長の見解をお伺い致します。是非とも、教育の情報化を加速度的に推進し、生きる力を持ったたくましい子供の育成と、子供たちの真の学力向上を目指し、併せて情報セキュリティを担保できるシステムを構築して頂きたいと存じます。

最後になりますが、アメリカではサイバー攻撃対抗するため、違法なサイバー攻撃に関わっていない優秀なハッカー、これをホワイトハットと呼ぶんでいるそうです。このホワイトハットの力を積極的に取り入れる企業が次々と現れています。

アメリカ政府も、ホワイトハットたちが集まるイベントで採用活動を始めているそうです。毎年夏にラスベガスで開かれる世界最大のセキュリティカンファレンスと「ハッカーの祭典」と呼ばれているデフコンです。２０１０年には、日本の大学生が優勝しています。また、昨年には３００チームが参加した予選で、デフコンに参戦できる１２チームの中に日本人チームも入りました。

実は日本でも、ハッカー日本一を目指し、コンピュータへの不正アクセスを防ぐ知識や技術を競うコンテスト、キャプチャー・ザ・フラッグが、先月１８日１９日に飯塚市の九州工業大学情報工学部で国内で初めて開催されました。県内外から７チーム計３１人が参加し、暗号解読などに挑戦しています。ＣＴＦ大会実行委員会では、日本国内で上位者が競う全国大会を２年以内に

開催する予定だそうですが、是非とも福岡県・飯塚の地で全国大会が開催され、本県としても、情報セキュリティ技術者の育成に力を注いで頂きたいと思います。

知事、今後の新たなＩＴ戦略のキーワードは、クラウドコンピューティングとこのネットワーク情報セキュリティだと思います。情報セキュリティ技術者の育成に力を注ぐことで、本県は、セキュリティ先進県として、情報・人材、データーセンター等のネットワーク企業や研究機関の投資や集積が期待されてきます。

インターネットの爆発的普及、クラウドコンピューティングの浸透、スマートフォンなどのデバイス多様化等、ＩＴのメリットを生かして企業価値や行政サービスの維持向上を図る上でも、情報セキュリティ戦略の遂行が極めて重要になっています。産学官連携や人材育成等により、ＩＴのクラスター化を図り、差別化されたＩＴ立県を目指し、情報産業を強力に推進して頂けますように要望致しまして、私の一般質問を終わります。ご清聴ありがとうございました。