南谷清司　令和４年３月議会一般質問　３月１１日（金）午後３人目

【標題１】成人年齢の引き下げについて
（１）市民の理解促進に向けた取り組みについて　（健康福祉部長）
【標題２】市民病院へのサイバー攻撃について
（１）サイバー攻撃の脅威について　（市民病院事務局長）
（２）被害防止と復旧対策について　（市民病院事務局長）

皆様こんにちは。
議長より許可をいただきましたので、通告に従いまして「成人年齢の引き下げについて」と、「市民病院へのサイバー攻撃について」の、２標題についてお尋ねします。

最初に、成人年齢の引き下げについてお尋ねします。

この４月から、成人になる年齢が２０歳から１８歳へ引き下げられます。１８歳になれば、たとえ高校生であっても、法律上は、私達と同じ成人として扱われることになります。羽島市では、２０歳を対象に成人の日の式典を実施してきましたが、様々な理由から、今後も現行どおり２０歳を対象に、「二十歳（はたち）のつどい」として開催することになっています。そのことに何も疑問はありませんが、馴染み深い式典が２０歳で実施されようとも、１８歳で、法律上は成人として扱われることに変わりはありません。

そして、１８歳になって成人となった本人だけでなく、その周りの大人も、この４月から、１８歳の若者を取り巻く環境が大きく変化することを理解し、その内包する危険性について十分に認識することが必要です。

高校生は、主に家庭科の授業で、自立した消費者の育成や、若年者の消費者被害防止と救済を目指した、消費者教育の内容を学習します。しかし、その保護者や周りの大人には、そのような学習の機会はあまりありません。ややもすると、自分たちの若い頃と同じだと思い込み、１８歳になったばかりの若者に対して、法律上は成人であることを意識せず、今までと同じように対応してしまう可能性もあります。

そのようなことがないよう、成人年齢が１８歳に引き下げられることの影響を周りの大人が理解し、成人となったばかりの若者に適切に接することができるよう、行政は支援しなければなりません。

そこでお尋ねします。

成人年齢が１８歳へ引き下げられることの影響を、周りの大人に理解し認識していただくための、市の取り組みについてご説明ください。

【健幸福祉部長の答弁】

現在の民法においては、未成年者による契約には保護者の同意が必要であり、同意を得ずに結んだ契約、例えば、携帯電話、クレジットカード、自動車ローンなどにかる契約は、取り消すことができるとされています。

この４月から施行される改正民法では、成年齢が２０歳から１８歳に引き下げられることから、今まで取り消すことができた１８歳、１９歳の高校生、大学生が保護者の同意なく行ったそうした契約は、成年が行った行為であることから取り消すことができなくなります。

当市では、新成人のみならず、保護者の方々に向けても、広報はしま、回覧板、市ホームページ、SNS、デジタルサイネージなどを用いて、そうした危険性を周知し、 トラブル防止の啓発に取り組んでいます。

併せて、トラブル発生等でお困りの際には、当市の消費生活相談窓口や岐阜県の相談窓口、消費者庁の消費者ホットラインなどを活用していただくよう、周知に努めています。

次は２つ目の標題「市民病院へのサイバー攻撃について」お尋ねします。

最近､医療機関を狙ったサイバー攻撃による被害が発生しているようです。例えば、報道によると、１２０床１３診療科を持つ、ある公立の中核総合病院では、昨年１０月末、サーバのデータを暗号化し、暗号化解除と引き換えに身代金を要求するコンピューターウイルス､「ランサムウエア」に感染し、約８万５０００人分の電子カルテが閲覧できなくなったようです。

電子カルテが使えなくなり紙カルテも残っていないため、産科と小児科を除いて、新規患者や救急搬送の受け入れを中止し、従来からの患者に対しては、一人一人に過去の症状や治療内容、薬の種類を聞き出しながら、紙カルテを作成し直したそうです。

病院は身代金の支払いを拒否して、２ヶ月間に渡ってカルテなどの復旧作業を行い、今年１月４日に通常診療を再開したようです。システムの再稼働のためにかかった費用は、非公表のようですが、報道では２億円とも伝えられています。

そこでお尋ねします。
羽島市民病院へのランサムウエアによるサイバー攻撃などについて、攻撃や被害の有無など、その脅威についてご説明ください。

【市民病院事務局長の答弁】
私からは、サイバー攻撃について、お答えします。
まず、電子カルテシステムにつきましては、これまでランサムウェアによるサイバー攻撃や、それらによる被害が発生していません。
サイバー攻撃により被害を受けると、日々診療時に用いている電子カルテシステムが使用できなくなる恐れがございます。そうした場合には、紙カルテで診療を行う必要が生じ、診療自体に影響を及ぼす脅威であると考えています。
それ以外にも、「個人情報」の漏洩、「システム復旧に要する費用」などが脅威であると考えています。

御答弁ありがとうございます。
２つ目の標題の２回目の質問をさせていただきます。

医療機関へのサイバー攻撃は、地域の医療体制に大きな影響を与える一方、その対策については、明確で有効な方針が確立しているわけではないようです。

全国の被害状況は、厚生労働省が公表していないため分かりませんが、１月に実態調査をしているようなので、厚生労働省としても危機感を持って対応しているようです。また、報道によると、今年度中には、医療機関向けの新たな情報セキュリティー指針を策定するようです。
しかし、一旦被害に遭うと、その影響は市民の命を守ることに影響が及ぶので、国や県の動きを待つことなく、新型コロナウイルス感染症の対応で大変な中ですが、そのような中だからこそ、サイバー攻撃によって病院機能をストップすることがないよう、対策を後回しにするわけにはいきません。
サイバー攻撃は、メールに記載されたURLや、添付されたファイルを利用してというのがよく知られていますが、システム保守業者が、遠隔保守用に病院内のシステムと接続する機器の、脆弱性を利用したものもあるようです。

しかし、サイバー攻撃への対策と言っても、予算措置や専門的知識、技術が必要ですので、直ぐに完璧な対応ができるわけではありません。まずやらなければならないことは、現状分析、対応策の計画立案、対応策の着実な実

施、だと思います。
　例えば、バックアップ用機器は、バックアップするときだけネットワークに接続し、それ以外はネットワークから物理的に切り離しておく、電源も落としておくという対策も、システム保守業者は避けたがるかもしれませんが、バックアップデータはネットワークから切り離すという原則に忠実な方法という点で、とても有効です。先ほどの被害に遭った公立病院は、この方法を取っていれば、カルテ消失という最悪の事態は防ぐことができたはずです。
　危機管理対応は、単純な方法ほど費用が少なくて効果は大きいということは、よくあることです。また、メールを経由したコンピュータウイルスの侵入に対しては、抜き打ちで怪しいメールを送り、ＵＲＬや添付ファイルを開かないよう訓練するという方法もあります。

　ところで、メールのセキュリティ対策にＰＰＡＰというものがあります。添付ファイルをメール送信する場合に、パスワード保護したＺＩＰファイルを送信後、その解凍パスワードを後から別にメールで送るという、お馴染みの方法です。しかし、この方法は、パスワード付きＺＩＰファイルである添付ファイルが、セキュリティーチェックをくぐり抜ける可能性があるため、ＺＩＰファイルに仕込まれたウイルスにコンピュータが感染する場合があるそうです。実際、文部科学省では、昨年１２月１日付けでこのＰＰＡＰ方式を廃止しているようです。今後、内閣府など他省庁でも廃止が進むと思われます。

**　そこでお尋ねします。**
**　羽島市民病院へのランサムウエアなどのサイバー攻撃について、感染防止や、万が一感染した場合のＢＣＰなどについて、現在取っていらっしゃる対策や今後に向けて検討されている対策についてご説明ください。**

【市民病院事務局長の答弁】
**　現在、当院の電子カルテシステムのデータにつきましては、院内にバックアップデータを含む記憶装置を保有しております。電子メールについては、電子カルテシステムのネットワークとは独立したネットワークを構築して運用しており、当該システム内では使用できない環境となつております。**
**　また、有事の際に備えて、今年度紙カルテを使用した診療の運用を試験的に実施し、対策を行つているところです。**
**　しかしながら、情報セキュリティの問題については、日々巧妙に進化し、システムの脆弱性を攻撃されるという性質があることから、適宜見**

直しを行い、万が一に備えていく必要があると考えております。
**　このため、今後策定される国の指針を踏まえて、引き続き、検討を行い、計画的に対策を講じてまいりたいと考えております。**

先程、電子メールと電子カルテとは独立のシステムとなっているという説明がありました。システムを独立させることが、有効な対策の一つであることは確かです。

しかし､独立した別システムになっていると業者から説明を受けていても、実はVLANを切って論理的に分離させているだけで、物理的には２つのシステムは繋がっている場合があります。この場合には、結果的に全部のシステムがインターネット空間に接続していることになります。また、質問でもお話ししましたが、システム保守業者が、病院内のサーバーをVPN等を利用して遠隔管理している場合もあります。この場合も、物理的にはサーバーはインターネット空間に接続していることになります。そして、物理的にインターネット空間に接続していれば、電子メール等の人的操作とは関係なく、接続等に使用されている情報機器の脆弱性に、直接アタックしてくるサイバー攻撃もあります。

なお、これらは例え話で、羽島市民病院が実際にどうなっているかは、私は承知していません。

危機管理は最悪の場合を想定してと言いますが、ありとあらゆる危険性を想定した対策を実施することは、専門的知識と予算確保など、課題は多く、困難な作業だと思います。そのような状況は理解していますが、厚生労働省が近く示すであろう医療機関向けの情報セキュリティー指針を参考に、羽島市民の命と安心を守るためにより一層の御努力をよろしくお願いします。

今回は、コロナ対策で質問時間が短いため、議論や提案というより、現状を説明していただくだけの質問としましたが、いつかの機会に、サイバー攻撃だけでなく、地震や水害、大規模で長時間にわたる停電、火災などの災害を想定した、羽島市民病院のBCP、事業継続計画を中心に議論させていただきたいと思います。

その時にはよろしくお願いします。

以上で私の質問を終わります。ありがとうございました。