○議長（井上勝彦君）次に、順番11、11番　土井君。

〔11番（土井裕美子君）登壇〕

○11番（土井裕美子君）それでは、ただ今議長のお許しをいただきましたので、通告に従いまして一般質問を始めさせていただきます。

今回の私の質問は１点でございます。橋本市における情報セキュリティについてでございます。

最近、企業や国の機関でもＩＴシステムに関する障害（サイバー攻撃などによるウイルス感染など）の問題が起こっているとの報道がございました。本市においても、ＩＴシステム障害による情報漏えいなどの問題は、人権侵害や犯罪にもつながるおそれがあるため、早急に対策を講じなければならない問題と考えております。そこで、本市の情報セキュリティについて何点かお伺いをさせていただきます。

１．①端末からのＵＳＢメモリなどを利用した情報の持ち出しはどのように制限されていますか。

②その制限がすべての端末に施行されているか確認されていますか。

③その施行確認の方法はどのようにされていますか。

２．①メール送信による情報漏えいについては、どのような制限をされていますか。

②課や室のメールアドレスの参照、送信はだれが行っていますか。

③課や室のメールアドレスを送信する場合のルールなどはありますか。

④送受信されたメールを一定期間保存することで漏えいを防ぐ仕組みがあると聞きましたが、本市にはありますか。

３．ウイルスなど不正プログラムの対策はすべてのコンピュータの中でどの程度なされていますか。

４．外部からの攻撃に対する対策はどのようにされていますか。

以上で私の１回目の質問を終わらせていただきます。明快な答弁をお願いいたしたいと思います。

○議長（井上勝彦君）11番　土井君の一般質問に対する答弁を求めます。

理事。

〔理事（吉田長司君）登壇〕

○理事（吉田長司君）最初に、コンピュータ端末からの情報の持ち出し制限についてお答えします。

まず、コンピュータ端末の分類をご説明します。外部ネットワークと接続をしていない住民登録、税など窓口業務に関する住民記録業務系ネットワークに接続するコンピュータ端末、２点目がインターネットサービスが利用可能である内部情報系ネットワークに接続するコンピュータ端末、そして、３点目に、各課室独自のコンピュータ端末があります。

内部情報系ネットワークに接続するコンピュータ端末については、コンピュータ端末からＵＳＢメモリなどを利用したファイル持ち出しを制限するシステムを導入しています。ファイルの持ち出しについては、許可された職員のみ持ち出しが可能となっており、持ち出した場合、いつだれがどんなファイルを持ち出したかがシステムに記録されています。

全コンピュータ端末610台中、平成20年度までに導入したウインドウズＸＰで動くコンピ

ュータ端末440台は、持ち出したファイルの実体も記録していますが、平成20年度以降購入した基本ソフトがウインドウズビスタやウインドウズ７で動くコンピュータ端末約170台については、現在、オプションソフトがあり、必要台数や導入時期等について導入業者と調査検討中です。

また、住民記録業務系ネットワーク系コンピュータ端末約65台のうち約40台は、パソコン機能のない端末であり、持ち出しが不可能です。残り25台はウインドウズ基本ソフトを利用していますが、このパソコン端末からは、情報推進室以外の職員に対して情報の持ち出し手順及びログインＩＤを通知していません。また、必要なファイルがホストコンピュータにどのように存在するかを認識していないため持ち出しについては不可能です。また、各課独自システムについては、おのおのの課において対策を実施しています。

次に、情報持ち出しの確認方法の質問についてですが、内部情報系ネットワーク系につながるコンピュータ端末での確認方法は、情報推進室よりリモートで１台１台確認することになります。情報持ち出し制限にかかわらず、ウイルス対策その他の脆弱性の確認等、稼働コンピュータ数の把握にも時間を要するため、現在、コンピュータ端末などの機器の管理に関してシステム導入の検討を行っています。このシステムにおいて、情報推進室が把握しているコンピュータがすべてであるか、他のネットワークに接続していないかという機能についても自動監視できるシステムを検討していきたいと考えています。

次に、メール送信による情報漏えいについては、メールアカウント利用者からインターネット用電子メールアカウント登録申請書とともに誓約書を提出していただき、総合行政ネットワーク基本要綱に定められたＬＧＷＡＮ利用者に電子メールアカウントを配布しています。その誓約書で情報漏えい等について誓約していただいているところです。

次に、課や室メールアドレスの参照、送信についてですが、「橋本市行政内部情報系ネットワーク系のためのセキュリティ実施基準」の中で「文書主任が責任を持って毎日確認してください。当メールでの送信は所属長が行うか、あるいは所属長決裁を得て行ってください」という文書によってルール化されています。

次に、送受信したメールの保存により漏えいを防ぐ仕組みについては、現在、橋本市にはありません。これはメールによる漏えい防止対策とセットで供給され、権限者による内容の監査も可能であり、削除したり、保存場所がわからないといった障害時にも有効に利用できるシステムと聞いており、今後の導入について調査研究してまいります。

次に、コンピュータ端末のウイルス対策についてですが、最新の対策ソフトを更新する必要があり、内部情報系ネットワークに接続する基本ソフトがウインドウズビスタやウインドウズ７のコンピュータ端末やサーバーについては、現在、端末及びサーバー更改の途中であり、更改を終えた段階で約610台中約240台が対策済みとなり、残り370台の基本ソフトがウインドウズＸＰ以前のコンピュータ端末については、対策を進めることを検討いたしましたが、コンピュータ端末の能力が不足し、著しく動きが遅くなるということがあり、最新ソフト更新できたコンピュータ端末は約80台となっております。残り290台が旧の対策ソフトによる対応となっています。

インターネットに接続していないコンピュータ端末、いわゆる住民情報系端末のウイルス対策は、ポータブルセキュリティを使用し、ＵＳＢメモリによりウイルスの検索・除去を

行います。これは１台１台のコンピュータ端末ごとに調査を行うこととなります。また、各課独自のシステムは、おのおのの担当課においてソフトを導入し対策を行っています。

次に、外部からの攻撃に対する対策ですが、ウエブやメールなどによる通信手段ごとに通過、拒否を設定し、必要最小限の通信のみ通過する機能を持ったファイアーウォールを設置しています。

ファイアーウォールにより通過を許可されたメールに関しては、ウイルスチェックを行い、スパムメール――いわゆる迷惑メールでございますが――を隔離、マーキングを行う機器を設置しています。また、ファイアーウォールによる通過を許可されたウエブ通信に関しまして、公序良俗に反するもの、いわゆる風俗・暴力・不正ＩＴ技術・ギャンブル・求人情報・オークション・株式金融等業務の障害になるものの閲覧を防止するため、アイフィルターと呼ばれる機器を設置しています。アイフィルターは、また、ウエブページを利用した情報のやりとりについても監視をしており、許可されたページにおいてだれが何をいつ行ったか記録を残しております。

今後検討すべき対策としては、侵入検知、防御システムがあります。一般に運用管理知識と手間がかかるため、今後、導入に向け調査研究を進めてまいりたいと考えております。ご理解のほど、よろしくお願いいたします。

○議長（井上勝彦君）11番　土井君、再質問ありますか。

11番　土井君。

○11番（土井裕美子君）それでは、まず、一番初めの質問といたしまして、ざっくりと情報セキュリティというくくりでくくらせていただきましたが、本市の行政として市のパソコンなどの中から、これは持ち出されては困るんだというような情報というのは、どのようなものがあるとお考えになっておられますか。これ、別にないんですというのであれば、情報セキュリティは全く要らないわけですから、持ち出されては困るなという情報、ざっくりとで結構でございますので、お答えいただけたらと思います。

○議長（井上勝彦君）11番　土井君の再質問に対する答弁を求めます。

理事。

○理事（吉田長司君）一番大事なのが個人情報でございます。内部情報系にしましても個人情報がたくさん入っていますので、個人情報が特に大事です。その次には公文書関係等がございます。主なところとしては、そういうところかというふうに認識しております。

○議長（井上勝彦君）11番　土井君。

○11番（土井裕美子君）やはり漏れては困るような情報はあるということですね。それでは、質問が始められるわけですね。ないのであれば別に細かく質問をする必要はないので、あるということで。

それでは、１番の①から質問をさせていただきます。

大変詳しくご説明をいただきまして、本当にありがたいなと思っております。１番の①に関しては三つあったんですかね。住民記録業務系のネットワークと内部情報系のネットワークの端末と、そして各課・室独自の端末、ちょっとこの辺の部分がわからないので、各課・室独自の端末とは一体どんなものか。そして、また、その各課において対策をしておりますということでございましたが、どのような対策をされているのか、わかる範囲で結構でございますので、お答えください。

○議長（井上勝彦君）理事。

○理事（吉田長司君）各課独自の端末におきましては、１点として閉鎖しているネットワークがございます。そういうものにつきまし

ては、例えば防災行政無線システムとか地籍支援システム、それから土木積算システムということで、これにつきましては、ネット上に流出するということはございませんけれども、情報の持ち出しということで管理していかなければならないと考えております。

それと、各課独自のシステムの中で、インターネットにつながっている独自のシステムがございます。例えば保育園・幼稚園関係につきましては､これはイントラ系ではなしに、独自の家庭用のインターネットのような形でしております。そういうことで、インターネットに流出しないためにも、また外から入ってこないためにも対策というのが必要かというふうに考えてございます。例を言いましたら､インターネット系では図書館のシステム、それから企業誘致のほうでも独自のシステムで動いてございます。それと幼稚園・保育園関係という認識をしてございます。

○議長（井上勝彦君）11番　土井君。

○11番（土井裕美子君）ちょっと細かいことになるので、持ち出しをできないようにする対策というのは具体的に言えませんか。

○議長（井上勝彦君）理事。

○理事（吉田長司君）最初の答弁で言わせてもらいましたとおり、内部情報系、要するにイントラネットについては強制的に持ち出しできないように、ＵＳＢにつなぎましてもコピーできないような形になってございます。独自の許可された人でないと、そのコンピュータでないといけないという形になってございます。

それと住民系につきましては、言いましたように、これは持ち出しするにはかなり知識とＩＤ､パスワード関係が必要ということで、普通の職員については持ち出しできません。持ち出しするときについては、文書をいただいて許可を与えて管理のもとでやっていくというような形になってございます。

それと、自由に持ち出しできるとかいうことになりましたら独自の分になろうかと思いますけれども、これについては、システム上で持ち出しできないような形はとりづらいところがございますので、そのセキュリティポリシーに基づいて管理をやっていくと。個人の認識を最大限活用しなければならないような形で持ち出し禁止をしております。

○議長（井上勝彦君）11番　土井君。

○11番（土井裕美子君）わかりました。

それでは、②③のほうに入らせていただきます。

答弁がなかなか、専門的な用語もいっぱいあって難しかったんですが、情報持ち出し制限の端末に対する、施行してあるかどうかの確認の方法ですが、情報推進室より１台ずつリモートで確認をするということでございましたね。パソコンの数の把握にも時間を要するためにシステムの検討をしているということでございました。ネットワークにつながっている端末で、情報持ち出し制限ができているかできていないか把握している端末があるのか、ないのか。これ、わからないということなんですかね、今の時点では。数とかはいいので、新しいものについては、まだわからないとかということがあれば言っていただいたらと思います。

○議長（井上勝彦君）理事。

○理事（吉田長司君）メールのやりとり、それからインターネットの中身の検索なんかについてはすべて記録できるようになってございますけれども、後から調べてわかるというような形がとれるシステムになってございます。

そういうことで、検討しておりますのは逐次わかるような形。どこの課がどことつながっているよということがわかるような。一々

調べて、ここはこことつながってたんだなということがわかるような形じゃなしに、逐次自動でコンピュータの状態がわかるような形のものの導入を検討していきたいということでございます。

○議長（井上勝彦君）11番　土井君。

○11番（土井裕美子君）１台１台調べる必要性があるということで、調べなくても全部わかるようなシステムをこれから検討して導入に向けるということでございますよね。そのように解釈をいたしました。

それでは、１と２も重なっている部分があるんですけれども、２に入らせていただきます。

メール送信による情報漏えいの制限についてですが、ＬＧＷＡＮ利用者については誓約書で誓約を書いていただいているということでございましたが、送信する容量の制限というのはあるんですか、ないんですか。

○議長（井上勝彦君）理事。

○理事（吉田長司君）容量についても制限があります。ただ、写真とかそういうことで容量が必要な場合については、情報推進室と協議するようになってございます。

○議長（井上勝彦君）11番　土井君。

○11番（土井裕美子君）それでは、②と③のほうに移らせていただきます。

メールの参照、送信のルールについては、文書主任が責任を持って行い、送信は所属長が行う、もしくはその決裁を得て行う、毎日の確認をするということですが､それは毎日、文書主任がおのおのの職員のメールの確認をやっていらっしゃるのかなというのが一つの疑問点と、誓約書で誓約をしていらっしゃるということでございましたが、そういう倫理的なものに関しての職員への研修というのはされているんですかね。その２点だけお願いいたします。

○議長（井上勝彦君）理事。

○理事（吉田長司君）メールについては、これは必要なツールでございますので、機械的に誓約するというのは非常に難しゅうございます。そういうことで、メール内容につきましては、これは公文書でございます。ということで、それについては、特にＬＧＷＡＮ関係の官庁関係のメールが多いんですけども、ほかのメールも含めまして、すべて原課の課長なりが確認するということになってございます。

ただ、どこまでできているか、できていないかというところまで把握してございませんけども、判を押した公文書という位置づけでしてくださいよということはしております。

それと、研修ですけども、統一した研修というのは、以前、３年か４年前に行いましたけれども、行っていない現状です。

それと、ちょっと前後しますけれども、メールのアカウントを配布するときにつきましては、過去については正職員だけということであったわけでございますけども､嘱託職員、それから臨時職員につきましても、必要なメールを送らなければならない部署の職員につきましては、一人ひとり協議を行って許可していくような形をとっております。

○議長（井上勝彦君）11番　土井君。

○11番（土井裕美子君）ルールを決めているので、それを守れているか、守れていないかはまだ把握していないということでございましたが、やはり情報の漏えいということも大変な問題がございますので、やっぱりそれはまず把握をする責任があるのではないかなというふうに考えます。その辺のところのこれから徹底していただくということに対してのご答弁と、それから、今までにそのルールが守られなかったということが発覚したような事件というか事象はございませんでしたか。

○議長（井上勝彦君）理事。

○理事（吉田長司君）それについては認識しておりません。あったということは聞いておりません。

○議長（井上勝彦君）11番　土井君。

○11番（土井裕美子君）答弁もれだったんですが、もう一点は文書主任が責任を持って行い、確認しているかどうかは把握していないということでは問題があるのではないですかということの質問です。

○議長（井上勝彦君）理事。

○理事（吉田長司君）失礼しました。確認できていないということがございますので、これについては、セキュリティポリシーの勉強も含めまして、再度そういうことで確認もしていきたいなと、その辺が重要かなというふうに考えてございます。

○議長（井上勝彦君）11番　土井君。

○11番（土井裕美子君）ありがとうございます。そのご答弁をいただくことによって安心感が生まれてくるということでございますので。

２の④でございます。送受信のメールの保存システムがあるということで、行政によってはこういうシステムを導入して、ＵＳＢでの持ち出しとか、それからメールを保存しておくことによって漏えいの抑止力になるということを聞いてございます。人権問題等にもかかわることであり、個人情報の漏えい等については、やはり行政として責任を持って対処していくということが重要でございますので、送受信のメール保存のシステムの導入に向けての調査研究ということだと思うんですが、具体的な検討の、このぐらいには入れたいよという、そのようなお考えはございませんか。

○議長（井上勝彦君）理事。

○理事（吉田長司君）担当課のほうからそういうシステムがあるということは聞いてございます。そういうことで、答弁で申しましたように、検討して、導入がどれぐらいかということも含めまして、効果等を含めまして、これから協議させていただきたいなということで、それ以上の答弁はできないような状態でございます。

○議長（井上勝彦君）11番　土井君。

○11番（土井裕美子君）それでは３番のウイルス対策と４番の外部からの攻撃対策について。これは大分関連している部分もございますので、あわせて質問をしたいと思います。

ファイアーウォールというものを設置して通過を拒否したりとか、メールに関してはウイルスチェックを行われているということなんですが、ファイアーウォールを通り抜けておのおののパソコンに入ってくるようなウイルスがまだあるということで、再度二重の防御の意味を込めて、多分、おのおののコンピュータにウイルス対策を施しているということだと思うんですね。

今お聞きしますと、機種がどんどん変わっていきますので、対応は難しいということは重々理解をしておりまして、お金も大分かかるんだろうなということは理解しておりますけれども、一つ、住民記録系のネットワークのほうで、外部には接続していないけれどもウイルスがどこかから入ってくると、住民記録のほうが情報が消されたりですとか、なくなって紛失したりですとか、そういうことも考えられます。今は、ご答弁の中ではＵＳＢメモリによる１台ずつの調査をしているということでございましたが、その対処はたしか検索と除去というお答えだったと思うんですが､検索と除去をするだけでは効果がなくて、イタチごっこだと思うんですね。それに対処するためにはやっぱり防御をするというシステムが大事だと思うんですけれども、その必

要性というのはどのようにお考えになっておられますか。

○議長（井上勝彦君）理事。

○理事（吉田長司君）住民情報系については、そういうことで何というんですか、その都度おかしくなったときにというような形になろうかと思いますけども、ＵＳＢのそこにソフトが入っていまして、検索するような形になってございます。それについても二、三個だったと思います。そういうことで、これ、非常に弱いシステムだなというふうに考えてございますけども、インターネットとつながっていませんので、入ってくるのが恐らくＵＳＢ関係かなと思います。

そういうことで､ちょっとこれについては、１回目の答弁では何も申しませんでしたけど、研究してまいりたいというふうに考えてございます。

○議長（井上勝彦君）11番　土井君。

○11番（土井裕美子君）これも重要であると思いますので、ぜひともご検討いただいて、前向きに。前向きにというのは行政用語では何もしないとよく言われるんですが、ぜひとも導入に向けて、金額もございますが、取り組んでいっていただきたいと思います。

４番の外部からの攻撃対策で、今後の検討すべき対策として、侵入検知防御システムの導入が検討されているというご指摘でございました。運用管理知識と手間がかかるので調査研究中。

確かに、私もこの問題をいろいろ調べさせていただきましたが、本当にすごく専門的な知識が必要であるということがよくわかりました。どんどん新しい用語が出てまいりまして、その用語を、これは何という意味なんだろうと調べるだけでもとても時間がかかり、本当に難しいなというのは再認識させていただいたんですが、やはり昨日も同僚議員のご質問の中に、専門職、プロフェッショナル的な職員を育成していく必要性があるのではないかというようなご質問がございました。まさにここの部署に関しましても、その必要性は十分にあるというふうに認識をいたしました。

知識の習得に年月を必要とすることで、昨日のご答弁の中では、新任であれば３年で交代、ほかの方でも３年から５年で交代ということでしたが、やはりこういう専門の知識を必要とするところであれば、もう少しスパンを長くして、せっかく一人前にわかってきた頃にまた配置転換というふうになると、やっぱりいろんな問題も生じてくるかなと思います。その辺の配慮をこれからなされるのかどうかという点と、そして、内部の研修だけではどんどん情報関係のものは進んでいきますので、ここの職員に対する外部への研修というのも大変重要な問題となってまいりますが、その辺の市職員の外部研修の強化というのをどのようにお考えかという点の２点についてお答えいただきたいと思います。

○議長（井上勝彦君）理事。

○理事（吉田長司君）そういうことで専門性がありますので、あとの答弁からですけど、研修についてはかなり言って行かせております。

それと、情報推進室のあり方でございますけれども、この住民系を導入したときから、旧の橋本市においてはキーパンチャー的な考え方の中で専門職という形で雇用してきた経過がございます。そういうことで住民系については橋本市用にカスタマイズされたところがございます。

ということで、専門職を置かなければわかりにくいということがあったわけでございますけども、この住民系につきましては、将来は市にシステムを置くのではなしに、クラウ

ドコンピュータ的な考え方の中で今後は進めていきたいなとういふうに考えてございます。

それと、内部情報系につきまして、今システム運用係というのがあるわけでございますけども、システム運用につきましては、外部のほうへ発注するのが望ましいんじゃないかなというふうに考えてございます。

ただ、情報政策につきましては、これは職員が考えていかなければいけないということがございますので、このことについては専門的な知識を要する者を育成していく必要があろうかなというふうに考えてございます。これはまだどうするという組織決定をしたわけではございせんけども、私の考え方の中でそういう考えでございます。

○議長（井上勝彦君）11番　土井君。

○11番（土井裕美子君）ありがとうございました。この問題に関しましては、皆さまもご承知のように、壇上でも申し上げましたが、国会、衆議院や参議院、また大企業でさえ情報の漏えい、多分、橋本市行政よりは数倍の対策を施しているにもかかわらず、攻撃をしようと思えば、パソコンの中に侵入して、そこからの情報を入手できるというような、本当に恐ろしいような事態になっているのが事実でございます。

アメリカでは陸海空、宇宙に続く第５の戦場というふうに言われているようなサイバー空間でございますけれども、だからといって何もしないということは大きな問題でございます。私もそれを認識した上で質問をさせていただきました。

部長もご答弁を真摯にお答えをいただきまして、大変ありがたかったと思います。本来であるならば、あまり詳しいことを言うこと自体が情報の漏えいになってしまいますので、私も大分考えたんですが、できる限りの範囲で今の現状をご報告いただいて、そして、その重要性についても再認識をしていただくことができたかなというふうに考えております。

本当にこの問題に関してはずっとお金をかけ続けなければいけませんし、また、その人材も必要となってまいります。本当に大きな問題で、優先順位のどこに入るかというと、なかなかこれは答えられない部分もあるかなと思います。

今後ともこの重要性をしっかりと認識していただくということが大切でございますので、その辺のところを、行政の中でトップの方がこの問題に関しては今後どのような方向性をもって取り組んでいただけるのかということを最後にお答えいただきたいと思います。よろしくお願いします。

○議長（井上勝彦君）副市長。

○副市長（清原雅代君）私は情報セキュリティの関係の最高情報統括責任者ということになっております。ただ今土井議員からご指摘いただきました、情報システムをさまざまな脅威から守っていくというのは、市民の財産、プライバシーを保護していくということはもちろんですが、事務の安定的な運営のためにも本当に必要不可欠なことと思っております。

ご指摘の情報セキュリティの対策の重要性というのは十分認識いたしておりますので、今後、職員の研修も含めまして対策にはできる限りのことをしていきたいというふうに考えております。

○議長（井上勝彦君）11番　土井君。

○11番（土井裕美子君）ありがとうございました。そのお言葉をいただいたら、今後期待をしておりますので、どうぞよろしくお願いをしたいと思います。

これで私の一般質問を終わらせていただきます。

○議長（井上勝彦君）これをもって、11番　土井君の一般質問は終わりました。

この際、午後１時まで休憩いたします。

（午前11時50分　休憩）