平成２３年度決算特別委員会速記録（第３号）

平成２４年９月２５日（火）　午後１時０２分開会

場　　所　　第３・４委員会室

……

○委員長（樋渡紀和子君）　　これより審議に入ります。前日に引き続き、歳出第２款総務費の質疑を行います。

初めに、錦織委員。

○委員（錦織淳二君）　　情報システムのセキュリティ対策について質問させていただきます。

港区情報安全対策指針運用経費の当初予算額は1,476万円で、決算額は1,475万9,010円になっています。平成24年７月27日の総務常任委員会における「区民の声への対応の充実・強化に向けた新たな取り組みについて」の中で、その背景及び現状として、「昭和46年４月から始まった広聴制度は40年余りが経過し、社会経済状況の変化やインターネットに代表されるＩＴ化の影響により変遷を遂げてきたが、現在の広聴制度は、この変遷に対応しきれていない。区民ニーズの多様化や近年の人口増、区役所・支所改革などにより、時代の要請に即応できる広聴制度を見直す時期に直面していると言える。区民に信頼される広聴制度とするために、より迅速で的確な対応を全庁的に展開する必要がある」旨の報告がありました。

また、情報提供の方法としては、区民に対してはホームページを利用し、職員向けには庁内ＬＡＮを活用して公表し、平成25年度中には広聴データベースの導入を検討されていますが、サイバー攻撃対策、情報漏えい対策はどのようにされているのか、お聞きいたします。まず、区の情報システムはサイバー攻撃を受けたことがあるかどうか、お尋ねいたします。

○区政情報課長（佐々木貴浩君）　　インターネット等を通じて情報システムに不正に侵入し、データを改ざんするなど、いわゆるサイバー攻撃についてでございますが、現在までのところ、区の情報システムが被害を受けたことはございません。

○委員（錦織淳二君）　　では、他区または他府県でサイバー攻撃を受けたという事例はありますでしょうか。また今後、港区がサイバー攻撃を受ける可能性があるとお考えでしょうか、ないとお考えでしょうか。

○区政情報課長（佐々木貴浩君）　　まず、他自治体での事例についてでございますけれども、現在のところ、特別区においてサイバー攻撃で被害を受けたという報道はありません。他府県の事例につきましては、幾つかの県で県のメールシステムに対しまして大量のメールが送付され、

システムダウンのおそれ、システムの遅延が発生したとの報道がなされております。

なお、政府機関におきましては、昨年から標的型攻撃メールと呼ばれる実在の差出人を装ってメールを送信し、添付ファイルにウイルス等を仕込み、システムを破壊しようとする攻撃を受けている事例が報道されております。

次に、区がサイバー攻撃を受ける可能性についてですが、セキュリティ対策は十分に実施しておりますけれども、今後、港区においても攻撃を受ける可能性はないとは言えない状況でございます。継続的な対策を行う必要があると考えてございます。

○委員（錦織淳二君）　日本では企業や自治体、どこでも同じですが、特に行政機関は情報漏えいが懸念されるような事件はひた隠しにする習慣があるので、実際にはかなりあるのではないかと想像することができます。シマンテック社が2011年に防いだサイバー攻撃は、日本を含め全世界で55億件を超え、前年比で８割増えていると発表しています。今回の尖閣諸島の問題に関すると見られるサイバー攻撃だけでも、行政機関や民間企業など19のウェブサイトで確認されたと警視庁が今月19日に発表しており、対象となった組織のうち、総務省統計局や防衛省、電力会社など11のウェブサイトで一時閲覧ができなくなり、一部は大量データを送りつけてパンクさせるＤＤｏｓ攻撃と見られ、また裁判所など８つのウェブサイトが不正に侵入され、中国国旗の画像と尖閣諸島は中国のものという趣旨の文章が勝手に表示されるなどの改ざんを受けています。

また、東京都のホームページには、16日から17日にかけて１億5,000万件以上の不正アクセスがあり、閲覧に通常の10倍程度の時間がかかる障害が出ていることもわかっています。

昨日も文化庁がウェブサイト、国指定文化財等データベースのトップページが改ざんされ、尖閣諸島・魚釣島の写真に大きな中国国旗の画像が取りつけられたと発表しており、19日ごろから中国の多数のアクセスが確認されているので、中国からのサイバー攻撃と見られています。

また、ことしの２月28日の朝、市役所に出勤した前橋市情報政策課の男性職員がいつものようにパソコンをチェックすると、見なれぬタイトルのメールが入っており、送信元は自治体の情報システムを管理する総務省の外郭団体、地方自治情報センターでした。メールを開くと、市が運営する前橋競輪のホームページの改ざんのお知らせで、メールには改ざん推定日時や不正ファイルが検知された日時など、関連情報９項目が箇条書きで記されていました。ユーザーがホームページにアクセスすると、強制的にオーストラリアのコーヒー関連サイトに飛ばされるように仕組まれていたのですが、このサイトも踏み台にすぎず、そこから段階的に２種類のウイルスに感染するように指定され、それが完了すると、偽りのウイルス対策ソフトがダウンロードされているかのような画面が突如あらわれ、一切操作は不能となる仕組みでした。

職員は当惑して前橋競輪の事務所に通報し、競輪職員がホームページ運用を委託している会社に閉鎖を要請すると、午後１時ごろには全面停止されました。その後の調査で、改ざんはフラン

スのコンピューターから操作されたことまで判明しましたが、実際の攻撃相手はさらに複数のサーバーを経由していると見られ、たどり着くのは到底無理だと前橋市では言っています。今回は、アドレス対策ソフトが整備されているパソコンでは感染がロックされていたため、実際にユーザーからの被害の届け出は１件にとどまりましたが、市職員は市関連のホームページでも必ずしも安全でないと気づかされたと衝撃を受けたようです。

群馬県内では、別の市でも昨年の８月下旬の朝、半日ほどメールのやりとりがストップしています。原因は外部から大量にメールが送りつけられたことによるコンピューターの処理能力オーバーでした。前日の夜から朝にかけて行われたと見られ、朝、職員が出勤すると、メールの送受信ができず、差出人は特定できません。草津町でも平成21年４月、町の携帯ホームページがサーバーに異常を起こして、侵入するＳＱＬインジェクションと見られるサイバー攻撃に遭い、ホームページにアクセスすると、別のページに自動的に転送される状態に陥りましたが、誰が攻撃を行ったのかいまだにわからないままです。

これらは群馬県におけるほんの一例ですが、公的機関は膨大な個人情報を扱うことからサイバー攻撃には常に危機意識を持っていなければなりません。港区ではサイバー攻撃に関して、どのような対策をとられているのでしょうか。

○区政情報課長（佐々木貴浩君）　区では、平成15年に情報安全対策指針を策定し、さまざまな情報セキュリティ対策を講じています。物理的な対策としまして、インターネットとその他のネットワークの分離など物理的な対策を実施しております。人的な対策といたしましては、職員への情報セキュリティ教育を実施しております。今年度は職員等を対象としたセキュリティセミナーで標的型攻撃メールについての内容、対応方法などについての周知も実施いたしました。技術的な対策として、ウイルス対策ソフトの導入、インターネット接続におけるホームページ閲覧の制限など、さまざまなセキュリティ対策を講じております。

○委員（錦織淳二君）　ウイルス対策ソフトでセキュリティ対策をされているようですが、最近のサイバー攻撃は標的型メール攻撃で、例えば、昨年11月の衆議院のサイバーテロは、議員に貸与しているパソコンでメールの添付ファイルを開き、ウイルス感染したのが原因で、三菱重工業など防衛関連企業に対する攻撃もこの標的型メールでした。メールには添付ファイルがついており、コンピューターウイルスが仕込まれています。件名にはセキュリティ調査報告、次回会議のお知らせ、出張報告などと書かれたメールが届きます。送信者は実在の企業名や官公庁名で、会議場所の地図を添付しましたのでご確認くださいとか、報告書に最近のサイバーテロの事例を記載しておりますので参考にしてくださいと、思わず開きたくなるような内容が書かれており、添付ファイルはワードやＰＤＦになっています。また、就活シーズンになると、内定通知書という件名で○○株式会社採用担当という担当者からメールが送られてきます。就活中の学生なら、

自分が受けた企業じゃなくても、思わずあけたくなるようなタイトルになっています。

さらに、メール送信者は簡単に偽装できるので、各プロバイダーは、その対応のため25番ポートブロック対応を行っていますが、送る側も添付ファイルを開けさせる確率を高めるため、あの手この手を使ってきており、組織内のパソコンをウイルス感染させ、メールの本文などを盗み出すという、いかにもそれらしいメール送信を行うことができるようになっています。

衆議院の攻撃で使われたメールの差出人は、「週刊焦点」安栗弘子という記者名で、件名は「お願い事」。内容は、「最新号の週刊誌にあなたの顔写真を掲載することになりますが、よろしいですか」という確認を求める内容で、「Photo zip」というファイルが添付されており、添付ファイルを開くとパソコンがウイルス感染しますが、表面上は何の被害もないため、ウイルス感染したことに気がつきませんし、不特定多数に送られるウイルスメールと違い、特定個人に送られるメールなのでウイルス対策ソフトでは検知されないことが多く、ほとんどがすり抜けてしまいます。

もう一つ多いのがフィッシングメールです。これは特定の組織を狙う標的型攻撃メールとは異なり、不特定多数の人々を狙った悪質なメールです。銀行やクレジットカード会社などの金融機関からのメールを装い、情報確認のためなどと称してメール受信者に偽りのウェブサイトにアクセスするように仕向け、偽りのウェブサイトで口座番号やクレジットカードの番号、パスワードなどを入力させ、個人の金融情報を不正入手しようとします。偽りのウェブサイトは本物のウェブサイトに見せかけてつくられており、利用者がだまされやすくなっています。

特に、東日本大震災及び原発事故以降、放射性物質など原発事故に関する人々の関心が高まっている中、それらのキーワードを件名に表示したメールを送りつけ、義援金募集等の偽りのウェブサイトに誘導し、住所や氏名、電話番号、クレジットカード情報などを入力させる事例が多く報告されています。区では、これらの標的型攻撃メールやフィッシングメールのセキュリティ対策はどのようにされていますでしょうか。

○区政情報課長（佐々木貴浩君）　標的型攻撃メールやフィッシングメールにつきましても、職員等を対象としたセキュリティセミナーにて攻撃内容や対応方法などについて説明を実施するなど周知啓発に努めております。今後は、職員等に対し、標的型不審メールへの対応訓練等を実施し、さらに職員への意識啓発や周知徹底を図り、攻撃等への対応力強化に努めてまいります。

○委員（錦織淳二君）　ＩＴ化が進んだ今日では、職場だけではなく、学校や日常生活においてもパソコンやインターネットは欠かすことのできないものになっています。一般の企業でも、行政機関でも今では１人１台のパソコンを持ち、書類やデータの作成も管理も全てパソコンを使って行い、業務上の連絡や資料の送付などもインターネットを通じて、自分のパソコンからメールで行うのが当たり前になっています。職場では情報セキュリティの規則を守って仕事をしてい

たとしても、家庭に帰れば、つい気が緩んでしまうのも至極当たり前な話ですが、危険から身を守るのは常に自分自身の危機意識を持った判断、行動でしかありません。また、できる限りの対策をしていても、常にこちらが用意するセキュリティを上回るものを向こうは必ずつくってきます。それに対抗するためには、今できる対策を常に怠らず、必死に努力するしかありません。情報社会は非常に便利な社会です。それは危険との裏腹です。決して軽んじることなく、ぜひ十分な費用と労力をかけて区民の安全と安心を守ってください。

次に、サイバー攻撃以外の情報セキュリティの実態についてお伺いします。

港区において、過去３年ぐらいの間で情報漏えい、盗難、紛失等の事実があれば、幾つか教えていただきたいのですが、いかがでしょうか。また、この種の事件は、どこの行政においてもひた隠しにするのが通例なので、表に出てくるのは氷山の一角かもしれませんが、港区以外で表に出た事件があれば、お教えください。

○区政情報課長（佐々木貴浩君）　区の情報漏えい、盗難、紛失等の事例についてですが、平成22年10月に職員による園児・保護者の名簿の紛失、平成23年３月には委託事業者によるシステムテスト帳票の紛失、今年度におきましては、個人情報が記載されました調査票の紛失が発生しております。

なお、港区以外で表に出た事件でございますけれども、他区ではイベント参加者へメールを送信する際に、誤って参加者全員のメールアドレスが見られる状態で配信し、個人情報が流出したことが報道されております。

○委員（錦織淳二君）　そもそも情報漏えい、盗難、紛失等、何であれ、住民の大切な個人情報を流出させないのが当たり前の話ですが、港区でもこの３年間に、システムのテスト帳票の紛失や名簿の紛失事件などがあったということは、区民の安全と安心が守られていない重大な問題ではないでしょうか。このような事件に対する対処、処罰はどのようにされたのでしょうか。今後の対策も含めてお伺いいたします。

○区政情報課長（佐々木貴浩君）　受託事業者における紛失に関しての対処といたしましては、受託事業者の責任者に対し厳重に注意するとともに、再発防止策の策定とルールの再徹底を指示いたしました。また、関与した社員に対しましても厳重に注意をいたしました。今後も、職員はもとより、委託事業者、指定管理者に対しましても、このような事故が起きないよう、研修等を通じまして継続的に意識啓発を行ってまいります。

○人事課長（浦田幹男君）　区職員が起こした名簿紛失の事故については、関係者から事情聴取を行い、地方公務員法第29条、これは職員の懲戒についての規定でございますが、この規定に基づき、港区職員懲戒分限審査委員会で審査の上、厳正に処分を行いました。

○委員（錦織淳二君）　幾らマニュアルをつくったり、職員の研修をしても、結局は個人の危

機意識でしかありません。引き続き何度も繰り返して、職員の情報社会におけるセキュリティ研修をしっかり行っていただくのと、そのためにも個人だけではなく、連帯責任も含めた処罰を厳しくしていかない限り、事件の重大さとのバランスがとれないと思います。処罰を厳しくすることについて、どのようにお考えでしょうか。

○人事課長（浦田幹男君）　懲戒処分の量定については、懲戒処分を厳正かつ公正に行うため、量定の標準例を港区職員の懲戒処分に関する指針に定めています。区はこれまで、この指針に基づき、事故を起こした職員はもとより、管理監督者についても厳正に処分等を行ってまいりました。今後とも、具体的な量定の決定については、故意または過失の度合いや社会に与える影響、個人情報の質及び量などを総合的に考慮の上、厳正に対応してまいります。

○委員（錦織淳二君）　私の知る限りでは、我が国は世界中で安全と安心が守られる唯一の国です。女性の方が一人で深夜、現金を持ってコンビニに行くことに何も危険を感じない国は日本だけです。どこのまちを歩いているときでもトイレの心配をせず、安全、清潔、快適、ただで用を済ますことができるのも日本だけです。のどが渇けば、北海道から沖縄まで全国の水道の蛇口から、危ないなどと心配せずに水を思いっきり飲めるのも日本だけです。電車やバスや公園のベンチで隣同士になったり、エレベーターで２人きりになった場合でも、互いに黙っていても危険を感じないで済むのは日本だけです。そうです。日本は唯一安全と安心が保てる国なので、リスク社会といえども国民自体の危機意識が低く、お人好しになっているのではないでしょうか。ゆえに過去にイージス艦の機密情報のコピーを外国に渡した自衛官が出てきたり、産業スパイ天国だと言われているのもうなずけます。

2008年に来日した伝説のハッカーであるケビン・ミトニック氏が「良心と信頼の文化を持つ日本は、最もだまされやすい国だ」と警告しています。私はそれを逆に言えば、良心と信頼の文化を持つ国は日本だけということになるので、大変すばらしいことであると誇らしく思っております。ただし、その分、セキュリティ対策に万全を期すという覚悟が必要であることは言うまでもありません。情報システムのセキュリティ対策については以上で終わります。

……