な選択的別姓をやるべきだといいますか、構わないという声が四割、あるいは四七％になるわけですよ。女性を見れば、例えば二十代の女性は五三・三％がやるべきだと言っているわけですよね。その声を、何だか賛成も反対もあるみたいなことで、やってはならないという人だけの声を何か代弁するような姿勢というのは、これは法務大臣としていかがなものですかと厳しく申し上げなければならないと思います。

今日、銀行口座を作るについても、あるいは国民健康保険、あるいは健康保険に当たっても通称では作れないということも金融庁、厚労省に確認したいと思っておりましたけれども、時間がなくなりました。できないんですよ。通称使用には限界があるし、その二重の管理、通称と戸籍名の管理にはもう極めて膨大なコストが掛かる。

そうした実態をしっかり見て、実現のために全力を尽くしていただきたいと願って、今日は質問を終わります。

○田中茂君　日本を元気にする会・無所属会、無所属の田中茂です。

今日は、法務省のサイバー攻撃、ウイルス感染に対するセキュリティーについて質問をさせていただきます。

去る六月二十四日に法務省のネットワークシステムにつながれた端末で不正プログラムに感染し

た疑いがあるとの報道がありました。それに先立ち、国土交通省の局長がタブレット端末の置き引きに遭ったというニュースもありましたが、政府全体のセキュリティー体制はどうなっているのか、大変に不安に感じるところであります。そもそも、事務所を出て、飲酒等の立ち寄りにタブレット端末を持ち歩いていたとのことでありますが、網棚に荷物を載せるなどは、民間企業では厳禁であり、セキュリティー意識が低いのではないかと思わざるを得ません。

そこで、法務省のセキュリティー対策はどうしているのか、お聞きしたいと思います。

最初の質問ですが、今回の法務省の端末が不正プログラムに感染した疑いがある事案に関して、いつどこで誰がどのようにして発見したのか。法務省独自で見付けたのか、あるいは内閣サイバーセキュリティセンター、ＮＩＳＣからの情報なのか。具体的な経緯及び、現在調査中と聞いておりますが、現状について、ＮＩＳＣとの協力関係も含めてお聞かせいただけませんでしょうか。

○政府参考人（髙嶋智光君）　お答えいたします。

昨月、六月十七日に、法務省が保管している端末、使用している端末につきまして、不審な通信先への通信の試行があるということが当省職員によって確認されました。これは、当省が設置しておりますセキュリティーシステムに引っかかったと、こういうことでございます。

この不審な通信先への通信の試行は、当省のシステムセキュリティーによってブロックされておりまして、そこから情報が出たということはございません。セキュリティー機能によってその試行は成功しなかったということでございますが、念のためネットへのウエブ閲覧を全部遮断しました上、原因の調査を進めました。その結果、六月二十四日、当省の端末が不正プログラムに感染した可能性があるということが判明したものであります。

そこで、二十五日にこれを公表したものでありますが、ＮＩＳＣ、つまり内閣サイバーセキュリティセンターとの関係におきましては、まずこのアラートを発見しました六月十七日の翌日にすぐ、試行があったけれども、つまり不審な通信先への通信の試行が確認されたけれども、これはブロックされていますということはＮＩＳＣには報告しております。また、その後も随時調査の進捗状況等についてＮＩＳＣに報告しまして、六月二十四日には不正プログラムに感染した疑いがあるということが判明したものですから、これにつきましてもＮＩＳＣに報告しております。

ＮＩＳＣとの関係におきましては、随時いろいろ援助をいただきまして対応を講じているというところでございます。

以上でございます。

○田中茂君　それでは、現在において情報流出はないということでしょうか、まだ疑いがあるということでしょうか。

○政府参考人（髙嶋智光君）　六月十七日に検知されましたその試行によっては、これはブロックされておりますので、そこから情報が出たということはございませんが、念のためほかに出ていないかということを調査している、そういう状況でございます。

○田中茂君　ありがとうございます。

それで、今現在、法務省でデータベース化している重要情報としてどのようなものがあるのか。セキュリティーに関しては、特に技術的なものは公にするには限界があると、そう思っております。一般的なもので結構ですので、お聞かせいただければと思います。

また、法務省では、そのような秘匿性の高い情報の管理体制はどのようになっているのか、この点も、話せる範囲で結構ですので、お聞かせいただければと思います。

○政府参考人（髙嶋智光君）　法務省で管理しております、そういうセキュリティーの非常に高い情報がどのようなものであるかということにつきましては、その性質上、この場ではお答えするのは差し控えさせていただきたいと思っております

が、今回のネットワークシステムのインシデントの関係で申し上げれば、今回この試行が検知された法務省のネットワークシステムというのは、法務省独自、法務省の一般事務を扱っている、そういうネットワークシステムでありまして、他の外庁とはまた別のシステムになっております。そこの間にはファイアウオールがしっかりつくられておりまして、法務省本省の一般事務の中だけのそういう問題が発見されたと、こういうことでございます。

○田中茂君　公安調査の情報についてはどのようになっているんでしょうか、お聞かせいただければと思います。

○政府参考人（髙嶋智光君）　委員御指摘の公安調査庁の情報といいますのは非常に保秘性が高いものでございまして、そういう観点からの御質問かと承知しますが、公安調査庁が扱っている治安情報、ふだんから収集しています治安情報等につきましては、これは、今回ウイルスが発見された、不正プログラムが発見されたネットワークシステムとはまた別のネットワークシステムでございます。現場で情報収集している、その際につくっているネットワークは先ほど申し上げましたとおり別のシステムでありまして、そこにはしっかりとしたファイアウオールがございます。

○田中茂君　ありがとうございます。

次に、最高裁においてもデータベース化している重要情報、どのようなものなのか、管理体制はいかになっているのか、お聞かせいただけませんでしょうか。

○最高裁判所長官代理者（中村愼君）　お答えいたします。

裁判所におきましても、事件情報の管理や司法行政に関する情報の管理を目的としてデータベースを構築して活用しているところでございます。その中に含まれている重要情報ということを具体的に申し上げますのは、先ほど法務省の答弁もございましたとおり差し控えさせていただきますが、裁判所としては、そのような、含まれている重要な情報について情報漏えいというようなことがないように管理体制を構築しているところでございます。

データベースの保護の技術的な対策の具体的な内容は、事柄の性質上、答弁を差し控えさせていただきますが、現在政府において置かれているＣＳＩＲＴというんでしょうか、そういうのと同様に、最高裁の事務総局情報政策課に情報セキュリティー対策の専門の係を設けまして、同様の体制で管理等を行っているということでございます。

○田中茂君　ＣＳＩＲＴについては先にお答えいただいたんですが、今からちょっと質問いたしますが、どちらにしろ、どういう秘匿性の高いものがあるかというのは大体想像は付くんですが、かなり重要なものがたくさん含まれていると思いますので、その辺十分注意をしていただきたいと、そう思っております。

そこで、サイバー攻撃は日常化しつつあるわけでありまして、ウイルスには必ず感染するという前提で処理すべきであると、そう思っております。問題は感染後の緊急事態への対応の仕方だと、そう思います。そういう意味での危機管理が重要ではないかと。そういう意味で、今さっきおっしゃったＣＳＩＲＴ、これは緊急対応組織ということで期待されて、二〇一三年までに全省庁にＣＳＩＲＴが設置されていると、そう聞いております。

法務省において、ＣＳＩＲＴの構成及び専門家の有無、レポートラインといいますか、指揮命令系統はどのようになっているのか、チェック体制を含めてお聞かせください。まずは法務省の方から、それじゃお願いいたします。

○政府参考人（髙嶋智光君）　お答えいたします。

法務省内におきましては、情報セキュリティーが害され又は害されるおそれがある事象が発生した場合につきましては、今委員御指摘のＣＳＩＲＴ、そのためにＣＳＩＲＴという組織を整備してございます。

これは、最高情報セキュリティ責任者、ＣＩＳＯと呼んでおりますが、この最高情報セキュリテ

ィ責任者であります官房長をヘッドとしまして、運用面、技術面等のスタッフによって構成される法務省の独自のものでございまして、この法務省ＣＳＩＲＴは、情報セキュリティーインシデントが発生した際、その発生した事案を正確に把握し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とする、そういうものでございます。

ちなみに、このＣＳＩＲＴの中にはＣＩＯ補佐官という技術的な専門官が入っておりまして、このＣＩＯ補佐官、実際に法務省の中で勤務していただいているのですが、このＣＩＯ補佐官は内閣官房における非常勤の国家公務員として任用された上で当省に派遣いただいている、当省の職員としても併任されているんですけれども、そういう方でして、国家公務員という立場で守秘義務を持って働いていただいていると、こういうことでございます。

以上です。

○田中茂君　今、ＣＩＳＯということで、黒川さんですか、がなっていらっしゃるんですか。多分官房長というと多忙を極めていらっしゃると思うので、あと、官房長が果たしてセキュリティーにそんなに精通していらっしゃるのかどうかは微妙なところなんですが、そういう意味でその今おっしゃったＣＩＯ補佐官というのがいらっしゃるとは思います。

この件についてはまたちょっと後で質問したいと思うんですが、最高裁の方でも同様な、ＣＳＩＲＴとは言わないと思うんですが、多分別の言い方、これは行政府の方での言い方だと思うので、最高裁においても同じように、その構成及び専門家の有無、先ほどＣＩＯとおっしゃいましたが、その有無、あとレポートライン等チェック体制がどのようになっているのか、お聞かせいただきたいと思います。

○最高裁判所長官代理者（中村愼君）　先ほど、少し先に答弁してしまいまして申し訳ございませんでした。

最高裁におきまして、ＣＳＩＲＴという名前は付けてはいないんですが、政府等のＣＳＩＲＴと同様に、まず責任者ということで最高裁の情報政策課長を置いております。インシデント管理責任者ということで情報政策課の参事官を置き、その下にインシデント担当者、窓口ということで事務総局情報政策課の専門官ほかの係員で構成しております。さらに、それらの情報を、インシデントアドバイザーということでＣＩＯ補佐官等の助言を受けつつ、迅速に分析、検討し、適切な対策の立案、指示するための体制を整えているところでございます。

それによりまして、情報漏えい等、仮に緊急事態が発生した場合におきましては、速やかにその係に所要の情報が集約され、内外の関係部署と的確に情報共有ができるというふうな形を取っているところでございますし、また、仮に事故が起こったような場合には復旧支援等を迅速に行えるような体制を整えているということでございます。

○田中茂君　ありがとうございます。

先ほどもちょっとお話ししましたが、ＣＩＳＯ、そんなに専門ではないので、ＣＩＯの方がどんなに大事かというのが分かるわけでありますが、その専門家について、民間会社からの採用になると思うんですが、その場合に、セキュリティー面というか、雇用期間終了後の安全性の確保が極めて重要だと思っております。

そこで、その会社との採用形態といいますか、具体的にはどのようにしているのか。任期終了後の秘密保持などの契約、交わしていらっしゃるとは思うんですが、どのようにしているのか、具体的にちょっとお聞かせいただければと思います。

○政府参考人（髙嶋智光君）　先ほども若干御説明させていただいたんですが、このＣＩＯ補佐官は国家公務員としての身分を有しております。したがいまして、国家公務員法第百条に基づく守秘義務というのを負っておりまして、これは職員がその職を退いた後といえども守秘義務は課せられる、そういう規定になってございます。

○最高裁判所長官代理者（中村愼君）　裁判所におきましては、ＣＩＯ補佐官、補助者について競争入札を実施いたしまして、落札業者との間で委託契約を結んで、最高裁の定める資格要件を満たす者をＣＩＯ補佐官及び補助者として充てることになっております。

契約におきましては、その受託者に対して資格要件という、情報セキュリティマネジメントシステム適合性評価制度の認証でありますとか、ＩＴストラテジスト等の公的資格を持っている等、いろんな要件を課しているところでございます。

さらに、機密保持の点でございますが、これは受託者の契約におきまして、業務の全期間及び委託期間の終了後におきましても業務上の秘密等を第三者に開示しないということで契約を定めておりまして、適切な管理がなされているものと認識しております。

○田中茂君　ありがとうございます。

雇用形態、そういうことで、問題は、とにかく終わった後その方が常に秘密保持をしていただけるのか、もしそれができなかった場合の罰則がどうなのか、その辺は厳重な契約ということで、あと国家公務員という立場でその後も続くということですので、その辺はしっかりとしておいていただきたいと思います。

次に、最後に、昨年、サイバーセキュリティ基本法が成立しまして、政府ではサイバーセキュリティーを高めるとしていますが、これまでの状況を考えれば、果たして全体としてのセキュリティー意識が高いか疑問を持たざるを得ないわけであります。

この点について、法務省ではいかなる取組を現在で行っているのか。今の体制は分かるんですが、標的型メール攻撃への訓練とか教育、その辺を含めて具体的にお聞かせいただけませんでしょうか。

○政府参考人（髙嶋智光君）　お答えいたします。

法務省におきましては、この基本法が施行される以前から、相当前からネットワークシステムの情勢を踏まえました適正な教育を行っているところであります。全職員に対して情報の適正な取扱いやサイバー攻撃に関する訓練を行ってきております。

また、施行後は、情勢を踏まえた標的型メール等のサイバー攻撃に関する訓練、これは実際職員にメールを送り付けまして、ちゃんと開かないようにできるかどうかと、こういう訓練をやったりしております。また、情報セキュリティ責任者を対象にした訓練、研修、それから一般職員を対象としました一般的な研修、こういう中におきましても情報セキュリティーに関する講義などを行いまして、その一層の意識の向上というのを図っているところでございます。

○田中茂君　お答えできる範囲で結構なんですけど、今までの訓練で、おとりメール、おとり添付ファイル、何人か引っかかった方はいらっしゃるんですか。

○政府参考人（髙嶋智光君）　私自身は引っかかりませんでしたけれども、その結果については私も聞いておりませんので、ちょっとお答えができません。申し訳ございません。

○田中茂君　先ほども言いましたように、法務省、最高裁には秘匿性の高い情報がありますので、サイバー攻撃が今、日常茶飯事になっております。今後も様々なウイルス、サイバー攻撃が出てくると想定されます。そこで、もちろん感染に対する事前防止も大事でありますが、感染後への迅速な対応には十分な危機意識を持って臨んでいただきたいと、そう思っております。

最後に、時間がもうありませんが、質問させていただきます。

先ほど真山先生からも質問がありまして、最後なものですから重なる部分があって恐縮なんですが、例の神戸児童連続殺傷事件、先ほどもお話がありましたように、この件に関しては、私自身実際に本は読んでおりません、メディアからの情報のみでありますが、元少年が書くことが唯一の自己救済の方法であったと、非常に違和感を私は覚えたわけであります。被害者遺族にも自己救済の

方法などないのは明らかであります。万が一その少年がそうであったとしても、それを公表して商業的な方法で出版することに関しては、通常の感覚ではあり得ないと思うわけであります。犯罪心理学的見地などから知りたいという意見は理解できなくはありませんが、もしそうであれば、ネットで限定公開するなど商業的ではない方法などもあったのではと、そう思っております。

　このような、先ほど言いましたサムの息子法、アメリカでもあるようでありますが、犯罪者が自らの事件を商業的に利用して金銭を得ることには歯止めを掛けるべきではないかとも私自身は考えておりますが、先ほど大臣はお答えになりましたが、非常にこの件は社会的にも大きなインパクトを与えておりますので、上川大臣のこの件について御意見をお聞かせいただければと思います。

○委員長（魚住裕一郎君）　上川法務大臣、時間ですので、簡潔にお願いいたします。

○国務大臣（上川陽子君）　はい。

　御指摘のとおり様々な意見がございまして、出版に対しての規制、抑制ということになりますと、当然のことながら表現の自由等の観点ということがございますので、慎重な検討が必要である案件というふうに考えているところでございます。

　被害者の皆さんの、また御遺族の皆さんの本当に思いを考えますと、大変、二次被害、三次被害で苦しめ続けるという状態は本当にあってはならないというふうに思うところでございます。基本法の理念にのっとって尊厳を守りつつ、また、犯罪を受けたところから本当に平穏な生活に戻っていただくところまで切れ目ない施策の支援ということについては、これはこれからもしっかりと取り組んでいくべきことであるというふうに思っております。

○委員長（魚住裕一郎君）　田中君、時間です。

○田中茂君　時間ですので簡潔に締めをしたいと思うんですが、本がなかなか売れないこの御時世に初版分が十万部を刷り、また増刷もしていると。出版社の意図があからさまであるわけであります。

　そこで、この事件、少年法が改正されるほどの事件であったわけでありますが、それほど社会全体に大きな衝撃と影響を与えたわけであります。司法制度改革の骨子が市民感覚を反映させた司法を目指しているのであれば、市民感覚を必要とするのは裁判員裁判だけではないと思っております。被害者や遺族が二重三重に苦しむことにより、もっと被害者遺族の立場に立った施策を是非とも検討していただきたいと、そのように思って、私の質問を終わりにいたします。

　どうもありがとうございました。

○委員長（魚住裕一郎君）　本日の調査はこの程度にとどめ、これにて散会いたします。

午前十一時四十九分散会