りますけれども、二期工事に入ることなく基地の建設の中止、撤去を、最後強く求めまして、質問は終わります。

○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。

早速質問させていただきます。

内外からのサイバー攻撃、サイバーテロに備える上で、現状の政府の管理体制をお伺いしたいと思います。

現時点において、政府機関、各省庁で使用している情報関連ハードウエア、パソコン等のハードウエアですが、及びソフトウエア、メールソフト、オフィス、セキュリティーソフトは各省庁の裁量に任されていますが、これはいかなる理由でそうなっているのでしょうか。また、それに関するメリット、デメリットがあると思いますが、それをお聞かせください。

一見すると、政府官庁、国立大学や国立研究開発法人においては、サイバー対処としては統一規格のハード、ソフトを使用した方が管理の上で効率的なのではと思うんですが、いかがでしょうか。お聞かせください。

○政府参考人（高野修一君）　お答えを申し上げます。

政府における情報システムの調達でございますが、これはやはり公金を使って調達をするものでございますので、公正、透明な調達手続、またその予算を効果的、効率的に使うという観点から、会計法令、あるいは国際的にはＷＴＯの政府調達協定などに従って適切に行う必要があるということになります。

政府における情報システムの調達に当たりましては、例えばＷＴＯの国際的な協定に基づきますと、特定の型式あるいは生産者又は供給者を要件としてはならないといったことが定められてございます。

仮にということでございますが、政府における情報システムの調達において何らかの統一化を図ったと、こういうふうにした場合に、ハードウエア、ソフトウエア等を単一の種類に限定してしまいますと、特定の事業者からしか調達ができないと。調達先の囲い込みのようなベンダーロックインと言われるようなことが起こりまして、調達コストが高騰したり、また、市場において多様な技術進展の見られる分野でございますので、多様な技術又は製品の採用ができず、情報システムの多様性、柔軟性の確保が困難になるといったことも場合によって考えられるというふうに思います。

ただ、委員御指摘の事柄とは全く同じではございませんけれども、政府全体として、例えば政府共通プラットフォームといった大きなクラウドのシステムの中になるべく乗っていっていただいて運用コストを下げていこうということもやってございますが、そういった中におきまして、一つの大きな目標、目的といたしまして、政府情報システムのセキュリティー強化というのを統一のプラットフォームに持っていくときには、より一段と高いセキュリティーレベルを確保するというような努力も一方でいたしてございます。

ただし、最初から申し上げましたとおり、政府全体としまして、特定のベンダーあるいは製品といったものに統一化を図るということには必ずしもならないというふうに考えてございます。

○田中茂君　確かに、システムが多様な方が強靱性というのは高いと思っておりますので、統一にしない部分もあるのはいいのかもしれませんが、もう一つ、安全面ということであれば、一つはインターネットにつながるネットワークと外部に接続しない閉じたネットワークの二重ネットワークがあると思うんですが、その点はいかが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（高野修一君）　例えば専用回線等を通じて特定のクローズドのネットワークをつくるとか、そういうことのお尋ねかなと思いますけれども、必要に応じまして、一般的な回線を使ってやる場合、あるいは非常に秘匿性の高いような情報を扱うので、その性質に応じて専用回線ある

いは特別のセキュリティーレベルを設定するといったようなことは、それぞれの事柄、情報システムが扱う情報の内容といったものに応じて適切に判断する必要があると、このように考えてございます。

○田中茂君　その二重ネットワークというのは、全省庁に整備されているんでしょうか、一部だけなんでしょうか。

○政府参考人（高野修一君）　二重ネットワークという意味合いがちょっと私分かりかねておりますが、先ほどお答え申し上げた趣旨は、一般の回線を使う場合、それでも様々な技術、手段によりましてセキュリティーを高めることは当然やっておりますし、可能でございますし、やっておりますが、それ以外に専用回線を引いてネットワークを構築する必要があるものについては、政府全体としても適切に判断をしてシステム構築あるいはネットワークの整備を行っていると、このように考えてございます。

○田中茂君　外部と接続する直接のやつと、外部と接触しない二重のネットワーク、多分それは各省庁によってちょっと違う部分があるかと思うんですが、これは全体をそういう二重のネットワークにした方がよろしいかと私は思っておりますので、予算の都合があるかと思いますが、その点、最大な考慮をしていただきたいと、そう思っております。

次に、サイバー防護の一元的管理、先ほどもちょっとお話がありましたが、現在、我が国のサイバー政策は、サイバーセキュリティ戦略本部と内閣サイバーセキュリティセンター、ＮＩＳＣが総括を行い、その指示に基づいて防衛省・自衛隊、あと外務省、警察庁など、各機関がそれぞれ独自のサイバーセキュリティーを管轄していると説明されております。ただし、これはマネジメント上の一元化が行われているだけであり、実際のサイバー防護は各省庁の諸機関に任されていると聞いております。

例えば、防衛省・自衛隊には、二〇一四年に電子防護を扱う専門部隊として組織されたサイバー防衛隊がありますが、同部隊の管轄範囲は防衛省・自衛隊の自己防護だけであり、その外にある重要インフラを防護する役割を負ってはいません。これは、自衛隊が我が国全国民の安全を確保する義務を有しているのと対照的であります。

大規模サイバー攻撃やサイバーテロに際しては、政府機関や各官庁はもとより、電気通信会社などの重要民間インフラも同時に防護するシステムがなければ意味が全くないと思っております。

このような問題に対して政府はどのように対処する考えを持っておられるのか、重要インフラの一義的責任を負っている大臣、官庁はどこにあるのか、そこには実動部隊があるのか等を含めてお聞かせください。

○政府参考人（藤山雄治君）　まず最初に、御指摘のありました重要インフラに対して大規模なサイバー攻撃があった場合の政府の対応ということで申し上げますと、これは、そういった緊急事態ということになりますと、官邸において官邸対策室というものを立ち上げるということになると思います。その場において、防衛省あるいは今委員御指摘になりましたような様々な関係省庁という方から担当者を集めまして、緊急参集チームということで対応するということによって政府一元化の対応がなされるということになろうかと思います。

一方、御指摘のありました各省庁における様々な重要インフラに対する取組というのは、それぞれを所管する関係省庁においても様々な取組をやっているということによって、もちろんその元立ちとしてはＮＩＳＣが、失礼しました、サイバーセキュリティ戦略あるいはそれを受けました行動計画なども作りまして全体の取りまとめをやっているという状況にございます。

○田中茂君　欧米の対応が全ていいとは思いませんが、一応、欧米の対処方法としては、個別対処の限界から、全て情報の共有、一元化対処センターを設置したと聞いておりますが、多分、日本の

方もそういうセンターをつくった方がよろしいかと思うので、その点は是非とも検討をしていただきたいと、そう思っております。

次に、官庁における情報機材の入札についてお聞かせください。

さきに政府機関、各官庁における情報関連機材の管理状況について質問をいたしましたが、現在、防衛省では、調達に係る入札公告によって、どのような部署でどのような機材が使われているのか、その仕様が明確に分かるようになっております。

例えば、昨年の入札公告における仕様書の中には、情報システム関連の業務用機材として、国内某所のパソコンが採用されていること、パーソナルコンピューターのスペック、処理能力、ルーター、外付けＨＤＤなど周辺機械の構成、ウイルス対策ソフト、セキュリティーソフトの種類などが全てオープンになっております。

これらの機材の構成が分かれば、当然ながら、悪意のある外部者は、同様のシステムを仮組みし、そこに通用するサイバー攻撃の手法を物理的にシミュレーションできるわけであります。言い換えれば、実際にサイバー攻撃を行う際の予行演習ができてしまうと、そう考えております。このような現状は、情報保全の観点からして明らかに問題であると思っています。

調達に際して、入札の公平性を期するためとの事情は理解できますが、こうした分野については公開入札の例外として特定秘密に準ずるものとして非公開にすべきだと、そう思っておりますが、いかがでしょうか。

○政府参考人（高野修一君）　情報システムの調達におけます情報の開示ということについてのお尋ねでございますが、先ほどもお答え申し上げましたとおり、政府における情報システムの調達も公的な調達でございますので、原則として一般競争入札によるということになりますので、その限りにおいては仕様書等を公開して行うということになります。

ただし、一般競争入札を行う場合でありましても、仕様書の中に、例えば、セキュリティー上の観点から機密性、秘匿性の高い情報が含まれるような場合には、該当部分について公開はせずに、誓約書を出していただき、職員による監視の下、希望する事業者のみに閲覧を限定するなどの対応が可能になっておりますし、現に行われているものと考えてございます。

また、そもそも会計法におきましては、外交防衛の活動など国の行為を秘密にする必要があるときには、仕様書を公表せず、随意契約を締結することも可能になっている仕組みがございますので、様々な事案に応じまして適切に調達の形態が選ばれているものというふうに考えてございます。

○田中茂君　ありがとうございます。

次は、情報収集が複雑化しサイバー犯罪が巧妙になっておりますが、優秀な若手研究スタッフの養成が必要であると、そのように思っております。経済産業省や情報処理推進機構主導でこのような人材育成に取り組んでいることも承知しておりますが、省庁の枠を超えて情報収集や外交防衛にもこうしたホワイトハッカーの力を活用すべきではないかと考えております。既に、政府は二〇一五年度から、いわゆるホワイトハッカーのような人材を民間から数人公募で採用するということで選考作業に入っていると聞いております。

米国と比較しても無意味かもしれませんが、米国はホワイトハッカーの育成に大規模に取り組んでおり、昨年、当時のヘーゲル国防長官がサイバー部隊を約六千人に計画する発表をしております。この一部を国家任務部隊として、安全保障上で決定的に重要である発電所等の電源網や、そのほかインフラ関連施設などを守る任務を二〇一八年までに増強することとなっております。

日本でも人材強化を図ることは良い方向だと思っております。ただし、公募で採用して五年間の有期雇用ということでありますが、この点に関して問題はないのでしょうか。というのは、有期雇用であればセキュリティー面、雇用期間終了後の処遇等での安全性が確保できるとは限りません。

有能な人材を確保するだけでなく、そのような採用形態、身元確認の対策について万全を期していらっしゃるのか、お聞かせください。よろしくお願いします。

○政府参考人（谷脇康彦君）　お答え申し上げます。

本年一月にサイバーセキュリティ基本法が全面施行されまして、この法律に基づきまして内閣にサイバーセキュリティ戦略本部を設置するとともに、その事務局として内閣官房に内閣サイバーセキュリティセンター、ＮＩＳＣを発足をさせまして、サイバーセキュリティー確保のための政府の司令塔機能の強化を図ったところでございます。

こうした体制強化の一環といたしまして、ＮＩＳＣの人員の増強に努めているところでございます。具体的には、本年一月及び三月から四月にかけまして、諸外国のサイバー政策、サイバー攻撃をめぐる情勢分析等を行ういわゆる任期付職員の募集を行ったところでございます。

委員御懸念のこの職員が任期を終了した後という点でございますけれども、任期付職員につきましては、国家公務員法第百条に基づきまして、任期中はもとより退職後におきましても、職務中に知り得た情報を漏らしてはならないこととされております。こうした規定を踏まえながら、職員の任期中及び退職後の情報の保秘に関しても職員教育を徹底してまいりたいと考えております。

○田中茂君　今、規定上はそういうふうに規定としてあると思いますが、誰も守るとは思っておりませんので、その辺はどういうふうにフォローしていくのか。辞めた後の、そこで五年間なり二年間、最大で五年間研修ということですが、その後のフォローというのはかなり難しいと思います。だけど、これをどうにかしないことには何らかの形で漏れる可能性もあるし、もう一つは、彼らの中にも、五年間というのであればかなりの能力が付いていくと思います。その段階で辞めさせるということはちょっと問題もあるんではないかと思っております。何らかの形でキャリアパスという道は開けないのでしょうか。その辺をお伺いできませんでしょうか。

○政府参考人（谷脇康彦君）　委員御指摘の点でございますけれども、五年なり任期付職員として勤務した後、キャリアパスという問題が確かにございます。これは、民間企業におきましてもセキュリティー人材が不足しておりまして、必ずしも明確なキャリアパスが描けていないというのが現状でございます。

そういった意味で、私ども、人材育成、官民の壁を越えてどのように人を育て、そしてキャリアパスを実現していくのかという点について、産学官民の連携の下で引き続き人材育成について考えてまいりたいというふうに考えております。

○田中茂君　その点、是非とも早期にやっていただきたいと、そう思っております。

次に、質問させていただきます。

日米首脳会談についてなんですが、隣国との歴史問題が米国の懸念を呼び起こす外的問題であるとすれば、沖縄問題は米国の懸念を惹起する内的問題であると思っております。この沖縄問題については、ホワイトハウス、さらには米上下両院議会からも問われることと思いますが、この間の新聞報道によりますと、日米首脳会談で発表予定の共同声明で、普天間飛行場の辺野古移設を再確認する文言を盛り込むことで進めていると、そのような報道がありました。

そこで、現在複雑化している辺野古の工期、およそ九年間と聞いております。代替施設の工事に九年間掛かるにもかかわらず、沖縄県の要請である、現在使用している普天間基地、五年以内に運用を停止するということは、海兵隊の部隊はその間の四年間を別の地域で活動せねばならないということになります。この整合性はどのようになっているのか。そもそも普天間基地の五年以内の運用停止と辺野古代替施設の工期九年間はリンクしているとは思えませんが、その間のずれをどのように対応されるのか、アメリカ訪問前に是非ともその点は聞かせていただきたいと思います。

○政府参考人（鈴木敦夫君）　お答え申し上げます。

住宅や学校等に囲まれまして市街地の真ん中に位置しております普天間飛行場の固定化、これは絶対に避けなければなりません。これが大前提でございますし、かつ政府と地元の皆様との共通認識であると思っております。このような認識の下、辺野古への移設が普天間飛行場の継続的な使用を回避する唯一の解決策であることを日米間で再確認しております。

その上で、普天間飛行場の危険性の除去を少しでも早く実現する観点から、普天間飛行場の五年以内運用の停止についても、仲井眞前知事からの強い要請を受け、政府として全力で取り組んできているところでございます。既に、昨年八月、普天間飛行場に所在する固定翼機の大部分を占めますＫＣ１３０十五機全機を岩国飛行場に移駐しました。

政府といたしましては、引き続き、沖縄を始めまして全国の自治体の御協力を得る努力をしながら、オスプレイの沖縄県外における訓練等を始め、できることは全て行うという姿勢で取り組んでいきたいというふうに考えてございます。

○田中茂君　先ほど委員からもお話がありましたが、毎日新聞の世論調査、非常に危機的な話では僕はないかと、そう思っております。

そういう中で、普天間飛行場以外の地区の返還状況について、若干関連性があるのでお聞きしたいと思っております。

先日、菅官房長官や翁長知事の出席の下で、西普天間住宅地区の返還が実現しました。他方、嘉手納以南におけるこれ以外の地域の返還について、従来は、県内で機能移設後、もう一つは海兵隊移設後、三番目が普天間代替施設完成後に行われるとされていましたが、その後、日米政府間で、普天間の辺野古移設と嘉手納以南の返還を切り離すことで合意されております。ただ、政府と沖縄の対立が、先ほど来からかなり話がありましたが、深刻化し、辺野古代替施設の建設が遅れ、普天間の返還もめどが立たなくなると、もうその間に沖縄県民の不満はますます増大する可能性が高いと思っております。

そこで、政府は積極的にほかの地区の区域の返還や振興事業の進展を図るべきだと思っておりますが、現在行われている嘉手納以南の土地返還計画についての具体的状況をお聞かせいただけませんでしょうか。

○国務大臣（中谷元君）　一昨年四月に公表した沖縄の施設・区域の統合計画は、人口が密集する沖縄本島の中南部において、嘉手納以南に所在する米軍施設・区域のうち約千四十八ヘクタールを超える土地の返還を進めるものであります。これまでに、牧港補給地区の北側の進入路が返還され、また本年三月にはキャンプ瑞慶覧の西普天間住宅地区が返還をされました。今回の西普天間住宅地区の返還は、その跡地利用を通じて沖縄全体の発展のために輝かしい可能性が秘められており、目に見える形で沖縄の負担軽減につながるものと期待をいたしております。

また、返還に向けたこれまでの取組として、牧港補給地区の移設先であるトリイ通信施設のマスタープラン及び嘉手納弾薬庫地区の知花地区のマスタープランについて日米間で合意したところでありまして、防衛省としましては、この統合計画を着実に実施をいたしまして、沖縄の負担軽減を目に見えるものとするために引き続き努力をしてまいりたいと思っております。

○田中茂君　先ほどの世論調査の結果を見ても明らかなんですが、日本国民になるべくならそういう説得できるような材料を与えるのが賢明だと私は思っておりますので、この提言を最後に私の質問とさせていただきます。

ありがとうございました。

○中西健治君　無所属クラブの中西健治です。お疲れさまでございます。

まず、外務大臣にアジアインフラ投資銀行についてお伺いしたいと思います。

中国からの回答についてなんですが、日本は、