「セキュア・ジャパン２００７（案）」に対する
提出意見の概要及び御意見に対する考え方

情報セキュリティ政策会議
平成19年６月14日

意見提出者一覧（五十音順）

株式会社CSKシステムズ
NTTコミュニケーションズ株式会社
（社）日本経済団体連合会
日本ユニシス株式会社
株式会社日立製作所
マイクロソフト株式会社
北陸無線データ通信協議会

その他個人２件

第３章　対策実施４領域における情報セキュリティ対策の強化			
該当箇所		ご意見の概要	ご意見に対する考え方
第１節　ア　政府機関	①ウ）ｂ） 情報セキュリティマネジメントに関する評価等	企業においても自組織内でのPDCAサイクルの定着は重要であると考えるところ、PDCAサイクルの定着度合いを評価するための手法やその適用ノウハウは、企業においても十分に役に立つものと考えられる。そこで、公表においては、評価結果と合わせて、ここで確立される情報セキュリティマネジメントに関する客観的に比較可能な評価手法と、その政府内での適用ノウハウ等についても、可能な範囲で公開されることが望ましいと考える。 （株式会社日立製作所）	評価の結果については、情報セキュリティの維持・確保にも配慮しつつ公表することとしているが、その際、政府機関の情報セキュリティ対策のベストプラクティスについても、取りまとめ、公表する予定です。
	①オ） コンピュータウイルスなどに起因する情報流出への対応	デジタル情報は様々な方法で持ち出しが可能であり、技術の進展により、常に新たな流出経路が発生する可能性がある。このため、デジタル情報そのものを機密レベルに応じて暗号化し、当該情報が万一流出しても内容を流出させないといった、流出を前提としたデータレベルでの暗号化対策を講じるべきである。 この方法を用いた場合、利用する暗号化の手法によっては流出経路の遡及も可能となることから、流出元の特定を行う等の効果も期待できる。 （マイクロソフト株式会社）	御指摘の情報流出に係る対策については、政府機関統一基準において必要な対策事項を定めているところです。
	同上	情報の外部持ち出し及び私物パソコンの業務使用に関する管理は、ルールだけでは徹底できない面もあると考えられるので、システムにより自動的又は強制的に処置を行う対策も必要になると考える。そこで、「第３章 第１節 ア ③（イ） エ）警察における情報セキュリティ対策の強化」と同様に、情報の暗号化をする等のシステム的な処置が必要なのではないか。 （株式会社CSKシステムズ）	御指摘の情報流出に係る対策については、政府機関統一基準において必要な対策事項を定めているところです。
	①キ） 情報セキュリティに配慮したシステム選定・調達の支援	情報システムは設定によってセキュリティレベルが大きく変化するのであり、製品の選定基準と合わせてセキュリティ設定についても取りまとめて公開する必要があるものと考える。 そこで、米国において製品のセキュリティ設定が具体的なレベルで公開されているように、日本でも単に製品の選定にとどまらず、広く利用されている製品のセキュリティ設定についても情報提供すべきである。 （マイクロソフト株式会社）	製品のセキュリティ設定については重要と認識しておりますが、各製品に特有な情報も含まれ、情報提供においては、製造企業等の協力等も不可欠であると考えており、御指摘の内容については、今後の政策の推進に当たって参考とさせていただきます。
	③（ア）イ） 安全性・信頼性の高いＩＴ製品等の利用推進	政府系各種システムにおいても認証された製品を優先的に使うことは重要だが、政府統一基準から外れないように、また、過剰な投資にならないように推進していく必要があると考えることから、政府統一基準やそのガイドブック等において、これらの認証された製品を利用するべき個所について具体的に明示するべきと考える。 （NTTコミュニケーションズ株式会社）	御指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
	③（イ）イ） 高セキュリティ機能を実現する次世代ＯＳ環境の開発	現在広く普及しているOSやアプリケーションは、重要なIT資産であり、次世代OS環境の開発においてもこれら既存資産の動作が保証されることを明記し、本施策により不必要なIT再投資が発生することへの懸念を払拭すべきである。 そこで、次世代OS環境の開発について、「現在のＯＳやアプリケーション等の利用環境を維持しつつ、推進する」とあるが、既存のOSやアプリケーションの動作環境が保証されることを明記されたい。 （マイクロソフト株式会社）	本施策は、ＯＳ及びアプリケーション等からなる現在の利用者環境を活用可能な、次世代ＯＳ基盤環境の確立を目指すものであり、本施策により不必要なＩＴ再投資が発生するとの懸念には当たらないものと考えておりますが、御指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。

第３章　対策実施４領域における情報セキュリティ対策の強化			
該当箇所		ご意見の概要	ご意見に対する考え方
第１節　ア　政府機関	③（イ）イ） 高セキュリティ機能を実現する次世代ＯＳ環境の開発	OSに依存しない形で情報セキュリティ機能を集約的に提供できる方法として仮想機械（VM：Virtual Machine）の記述があるが、「仮想機械」が指し示す機能や具体的実装が不明瞭である。 　コンピュータ自体にセキュリティ監視機能を持たせ、安全性を高める「フルボリューム暗号化機能」や「TPM (Trusted Platform Module)」など、主要な既存OSにおけるセキュリティ機能向上のためのフレームワークや機能拡張の内容を具体的に記述すべき。 （マイクロソフト株式会社）	御指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
	③（イ）ウ） 情報アクセス権限を統合し集中管理する機構を導入した革新的な仮想化技術の開発	「革新的な仮想化技術(セキュア・プラットフォーム)」と、第３章第１節 ア ③ （イ）イ）高セキュリティ機能を実現する次世代OS環境の開発で説明されている「次世代OS環境(セキュアVM)」との２つの違いがわかりにくいので、これらの関係が明らかになるような説明を加えたら、より理解しやすくなると思われる。 （株式会社CSKシステムズ）	御指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
	③（イ）オ） 電子政府に用いられるOSのセキュリティ品質の評価尺度の確立	情報システムは設定によってセキュリティレベルが大きく変化するのであり、製品の選定基準と合わせてセキュリティ設定についても取りまとめて公開する必要があるものと考える。 　そこで、米国において製品のセキュリティ設定が具体的なレベルで公開されているように、日本でも単に製品の選定にとどまらず、広く利用されている製品のセキュリティ設定についても情報提供すべきである。 （マイクロソフト株式会社）	御指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
	同上	電子政府に用いられるOSのセキュリティ品質の評価尺度の確立においては、コモン・クライテリアなど既に世界的に普及している国際標準との整合性を充分考慮することが、WTO-TBT協定の観点からも必要である。 （マイクロソフト株式会社）	御指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
	③（ウ）イ） 政府機関から発信する電子メール及び政府機関のホームページからダウンロードされる電子文書に係る成りすまし及び改ざんの防止	「電子署名」の意味するところについて、一般国民等に何らかの形でわかりやすく説明をされることが、結果的に全領域における情報セキュリティ対策の底上げにつながると考える。そこで、政府機関に係る電子文書に電子署名を付加する施策と合わせて、電子署名等の情報セキュリティに関する技術をわかりやすい形で一般国民等に啓発する取組みがより望ましいと考える。 （株式会社日立製作所）	御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。
	③（イ）ク） 中長期的な視点での電子政府における個人認証の発展方向の検討	「諸外国の政府における個人認証の制度及びシステムの実態等を調査する」とあるが、平成18年度にも政府や関連団体で認証制度に関連した様々な先進事例等の調査が実施されているので、これらの調査結果を総合的に踏まえた上で、更に不足部分について調査するべきと考える。 （NTTコミュニケーションズ株式会社）	御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。
	同上	IT新改革戦略の2006年度評価において、個人認証基盤のあり方が課題とされている（http://www.kantei.go.jp/jp/singi/it2/dai40/40gijisidai.html　資料４参照）。 　今後の政策として標榜されている各種電子政府システムなどについても、現有システムの有効活用と共有化等を検討の土台とし、利用者視点に立った政策を推進するべきと考える。 （NTTコミュニケーションズ株式会社）	御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。

第３章　対策実施４領域における情報セキュリティ対策の強化			
該当箇所		ご意見の概要	ご意見に対する考え方
第１節　ア　政府機関	③（エ）イ） 政府機関における安全な暗号利用の推進体制等の検討 ③（エ）ウ） ハッシュ関数SHA-1の安全性低下への対応	電子政府推奨暗号については、現時点で安全とされるリストを出すだけでなく、将来に渡って、いつ頃どういうレベルのセキュリティを持つ暗号に乗り換えていくべきか等の長期的な視点に立った見通しと戦略を、マイルストーンの形で時期とともに提示していただきたい。 そうすれば、暗号関連製品の開発ベンダや利用するサービスプロバイダがこれに計画的に対応することが見込まれるので、非常に有益なものになると考えられる。 （NTTコミュニケーションズ株式会社）	御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。
	同上	これまで、学術的観点からCRYPTRECにおいて暗号アルゴリズムの安全性についてまとめているが、一方で暗号を利用した製品の調達については、とりまとめを行う機関が政府に存在しないように思われる。 今後、暗号危殆化への対応を政府全体で取り組んでいくため、暗号の技術的な観点だけでなく、電子政府に関わる様々なシステム、利用者視点等の観点を含めて検討し指針を示すことができる仕組みを、政府内に作っていくべきと考える。 そうすれば、ベンダは製品開発方針等が立てやすくなり、早期に対応製品を出すことが可能になるため、早期の製品調達が可能になると考えられる。 （NTTコミュニケーションズ株式会社）	御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。
	③（エ）オ） ファイル（電磁的記録）のセキュリティ対策の推進	デジタル情報は様々な方法で持ち出しが可能であり、技術の進展により、常に新たな流出経路が発生する可能性がある。このため、デジタル情報そのものを機密レベルに応じて暗号化し、当該情報が万一流出しても内容を流出させないといった、流出を前提としたデータレベルでの暗号化対策を講じるべきである。 この方法を用いた場合、利用する暗号化の手法によっては流出経路の遡及も可能となることから、流出元の特定を行う等の効果も期待できる。 （マイクロソフト株式会社）	御指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
	④イ）c) サイバー攻撃等に係る分析・対処及び研究の推進	「サイバー防護用分析器材」とはどのようなものかが、わかりにくい。 「サイバー防護用分析器材」ではなく、「サイバー攻撃防護用分析器材」とするほうが、意味がわかりやすいのではないかと思う。 （株式会社CSKシステムズ）	本器材は、ネットワークインフラとしてのサイバー空間を防護するために必要な分析装置であることから、「サイバー防護用分析器材」としました。
第２節　重要インフラ	② 情報共有体制の強化	官民における情報セキュリティ対策の底上げのためには、官民の各主体間における情報共有体制を強化していくことが不可欠である。重要インフラ連絡協議会(CEPTOAR-Council)（仮称）の創設促進が施策として挙げられているが、官民連携の重要モデル施策と位置づけ、確実に推進すべきである。 （（社）日本経済団体連合会）	御指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
第３節　企業	①エ） 中小企業における情報セキュリティ対策の推進	「第１章第３節２（ａ）（ウ）企業」の説明の中で、企業規模の違いによる情報セキュリティ対策の格差が課題としてあがっているが、特に情報流出への対策の推進を行うことは緊急の課題であると考える。 そこで、本項目で説明されている「中小企業における情報セキュリティ対策の推進」については、2007年度中に検討を開始するのみでなく、もう少し早急で具体的な進め方が必要になるのではないか。 （株式会社CSKシステムズ）	御指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。

第３章　対策実施４領域における情報セキュリティ対策の強化			
該当箇所		ご意見の概要	ご意見に対する考え方
第４節　個人	①イ）ａ） 全国的な情報セキュリティ教育の推進	「インターネット安全教室」には文部科学省も加わるべきである。初等・中等教育に携わる教職員には受講を義務化するなどの強力なメッセージが欲しい。 （北陸無線データ通信協議会）	御指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
	②ア）ｄ） 電波利用秩序の維持のための周知啓発活動の強化	最も情報セキュリティの認識に身近な無線LANだけの「技術基準適合マーク」の啓発活動が必要である。 （北陸無線データ通信協議会）	「技術基準適合マーク」を確認することについて、平成１８年度から周知啓発を強化しているところです。 ご指摘の内容については、今後の周知啓発活動の推進に当たっての参考の一つとさせていただきます。
	③ 個人が負担感なく情報関連製品・サービスを利用できる環境整備	企業には「税制優遇措置」を行っているが、個人に対しても優遇措置を実施することで、個人における金銭的な負担軽減を促するべきと考える。 （NTTコミュニケーションズ株式会社）	御指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
	③ウ） 「無線ＬＡＮのセキュリティ対策」	現行の「安心して無線LANを利用するために」は2004年4月発表であり、現行の技術水準では明らかに時代遅れであると考えるので、以下のように変更していただきたい。 「2007年度において、無線LANのセキュリティに関するガイドライン「安心して無線LANを利用するために」を現行の技術水準に合う内容に改訂し、更なる普及を図るとともに、…。」 （北陸無線データ通信協議会）	今後の政策運営に適切に反映することを検討させていただきます。
	同上	以下のように変更していただきたい。 「2007年度において、…、一般利用者向けの普及啓発施策である「インターネット安全教室」の冊子等においても、無線LANの安全な使い方に関するコンテンツの充実を図り、公務員・団体職員・学校教職員に確実に行き渡る様努力する。」 （北陸無線データ通信協議会）	御指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。

第４章　横断的な情報セキュリティ基盤の形成			
該当箇所		ご意見の概要	ご意見に対する考え方
第２節　情報セキュリティ人材の育成・確保	②情報セキュリティに関する資格制度の体系化	具体的施策が記載されていないため、記載していただきたい。 （日本ユニシス株式会社）	情報セキュリティに関する資格制度の体系化については、昨年、情報セキュリティ政策会議の下に「人材育成・資格制度体系化専門委員会」を設置して検討を行い、その成果を「人材育成・資格制度体系化専門委員会報告書」に取りまとめたことにより、基本計画に掲げた目的を達成したと考えております。
	②情報セキュリティに関する資格制度の体系化	具体的施策が記載されていないので、 （１）②ごと削除 （２）「【具体的施策】」を削除 （３）具体的施策を書く （無ければ無いで「なし」と書く） のどれかにした方が良いのではないか。ここの項目だけ具体的施策が無いので違和感がある。 （個人）	御指摘を踏まえ、「【具体的施策】」を削除いたします。

第５章　政策の推進体制と持続的改善の構造			
該当箇所		ご意見の概要	ご意見に対する考え方
第３節　持続的改善構造の構築	（３）ア）情報セキュリティ対策に関する評価指標の確立	無線LANの実態調査を行い、国としての無線LANセキュリティガイドラインの再構成と指標を確立する必要があると考えるので、無線LANセキュリティ問題についても評価指標を確立されたい。 （北陸無線データ通信協議会）	御指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。

第６章　２００８年度の重点施策の方向性		
該当箇所	ご意見の概要	ご意見に対する考え方
第１節　情報セキュリティ人材の育成・確保に向けた集中的な取組み	わが国では、情報セキュリティ人材のみならず、社会のニーズを踏まえた高度情報通信人材の供給が質量ともに大幅に不足している。少子化に伴い益々人材確保が困難になる中、人材育成は短期間で成し得るものではないことも踏まえ、高度情報通信人材供給の全体のパイを増やす計画的な産学官プログラム推進が必要であり、その中で情報セキュリティ人材の育成を直実に推進することが望ましい。 （（社）日本経済団体連合会）	御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。
	優秀な人材を確保するためには、単に人材育成施策のみならず、育成した技術者のキャリアのモデルケース（政府機関におけるCIOへのキャリア・パス、企業におけるCISO等のキャリア・パス）を示し、人材育成のモチベーションを高める施策も並行して進めるべきである。 （（社）日本経済団体連合会）	御指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。
第２節 情報セキュリティ政策の国際展開に向けた集中的な取組み	従来の施策は、まず国内の守りを着実にする情報セキュリティ対策が中心であったが、インターネットが今やビジネス・インフラとなりつつある状況で、一国のみではその目的を達成できない。2007年度において戦略的に国際協調・貢献にと取組む基本方針及び具体策の検討、また、2008年度においてその本格化・加速化が盛り込まれている点を評価し、その実現を期待する。 （（社）日本経済団体連合会）	御指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
	米国、EU等の情報セキュリティ対策の先進国とは、官民連携のあり方やベストプラクティスについての情報共有に向け、双方の官民が参加する継続的な対話の場を設けるべきである。 （（社）日本経済団体連合会）	御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。
	途上国等に対しては、情報セキュリティ対策の整備、人材育成、文化醸成に向けて、日本の経験やノウハウを積極的に移転し、情報セキュリティ対策向上のための具体的な支援プロジェクト等を立ち上げるべきである。具体的には、日本と関係の深いアジア諸国の中で、今後、経済成長が期待されている国をモデルとし、政府のODAや民間のノウハウも活用した官民連携の下、CSIRT等の体制整備・強化等の支援プログラムを実施し、他国へも展開していくべきである。日本企業の立場から言えば、ビジネスパートナーとなる途上国・地域の企業等には、事業のアウトソース等の商行為一般において十分な情報セキュリティレベルが実装されていることが望ましく、このような企業等の情報セキュリティに関する取組みを支援する観点からも、途上国・地域におけるCSIRT基盤の確立に向けたプロジェクトを強力に推進するべきである。 （（社）日本経済団体連合会）	御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。
	国連（IGF等）、OECD、APEC等のマルチな場での情報セキュリティ検討の場にも、日本として積極的に対応し、日本のベストプラクティスの発信や情報セキュリティに関する標準化等への日本の立場・関心の反映に努めるべきである。 （（社）日本経済団体連合会）	御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。

第６章　２００８年度の重点施策の方向性		
該当箇所	ご意見の概要	ご意見に対する考え方
第３節 電子政府等の情報セキュリティ強化のための総合的な取組み	電子行政に関しては、NISCが情報セキュリティ分野で取組んでいるように、政府全体の統一ビジョンの下で、各府省庁横断的な取り組みが求められるが、現状においては利用者の視点に立った利便性・透明性の高い電子行政は実現していない。また、電子行政を推進する上で、利用者のシステムへの信頼を高め、その利用を促進する観点からも、総合的な電子政府の情報セキュリティ対策は不可欠である。 まずは、情報セキュリティにおける電子行政の全体最適を確保する観点からも、施策として述べられている電子政府の情報セキュリティを企画・設計段階から確保するための方策を、確実に実施し、強化していくべきである。 （（社）日本経済団体連合会）	御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。
その他	官民の各主体間における情報共有体制の強化については、本年だけでなく中期的に取り組むべき課題であり、第6章の2008年度の重点施策においても、重要な施策として明記しておくべきである。 （（社）日本経済団体連合会）	第６章は、１）取組みの開始から実際に効果が現れるまでに時間をかける必要がある分野、２）対策の取組みを開始したもののその取組みはまだ入り口の段階に過ぎず、今後取組みを加速化するべき分野、３）時宜に合った喫緊の課題として迅速な対応が必要となる分野について、特に問題意識を持ち注意喚起したものですが、これ以外についても、第１次情報セキュリティ基本計画の目標を達成するのに重要であり、中期的に取り組むべきものがあると考えております。 御指摘の施策についても重要であると認識しており、御意見の趣旨については、今後の政策運営に適切に反映してまいります。

その他		
該当箇所	ご意見の概要	ご意見に対する考え方
全般	「情報セキュリティ対策の底上げ」という文言について。 対策(＝手段)を講じた結果として水準(＝状態)が上がることを目指すことが目的なので、表紙の副題、および本文で使われている「情報セキュリティ対策の底上げ」という文言は、「情報セキュリティ水準の底上げ」としたほうがよいのではないか。 （株式会社CSKシステムズ）	御指摘の文言については、昨年決定された「セキュア・ジャパン2006」で用いられていた文言をそのまま用いたものであるため、原案のままとさせていただきます。
全般	文書全体の中でところどころ「ICT」という用語がでてくるが、「IT」との用語の違いを明確にするべき。 「ICT」と「IT」とで、それぞれの用語が違う意味合いで使われているのであれば、用語の説明を脚注などで記すとわかりすいのではないか。 なお、特に「ICT」と「IT」との区別をしていないのであれば、どちらかに用語を統一すべきと考える。 （株式会社CSKシステムズ）	御指摘につきましては、情報通信技術を表す「IT」という文言が全てを包含しているとの考えに基づき、原則として「IT」という文言を使用しておりますが、各省庁の個別施策に関する記述につきましては、各省庁における説明と平仄を合わせております。 なお、御指摘がありましたことについては、今後の政策の推進に当たっての参考の一つとさせていただきます。
全般	教育によるセキュリティ知識の向上や、PDCAサイクルを通じたセキュリティ向上等の比較的時間を必要とする施策に加え、既に直面しているセキュリティ課題に即応する対策の積極的な紹介、利用促進を含めるべき。 既に直面しているセキュリティ課題に対応するためには、OSやアプリケーションなどが提供している既存の機能活用による多層的な防御手段の構築や、セキュリティ関連企業などが提供する外部のセキュリティサービスの活用等が重要であるが、これらすぐに利用できる既存のセキュリティ技術・サービスの活用は、利用者の利便性や迅速な対応促進の観点から有益であり、利用促進を図るべきである。 （マイクロソフト株式会社）	御指摘の内容については、今後の政策の推進に当たっての参考の一つとさせていただきます。

その他		
該当箇所	ご意見の概要	ご意見に対する考え方
全般	情報漏えいが各府省で断続的に起きていることは事実。 しかしながら、防衛庁・自衛隊におけるイージス艦情報漏えい、警察官のwinny感染による捜査情報など、深刻化、顕在化した情報漏えい事案は、組織が大きく末端職員が多数存在し、業務用端末が一人１台用意できなかったような組織に集中している。 こういった、現状分析を適切に行い、まさにPDCAをまわして、深刻な情報漏えい事案の発生していない府省については、高い評価を与え、NISCの多様な調査、自己点検の対象からはずすような、インセンティブや効率的な手法を明示すべき。 現状は、NISCの仕事作り、組織維持、予算要求玉作りのみが先行し、多様な施策を打ち出している印象。 NISCは各府省から気軽に情報セキュリティ対策の相談等が寄せられるような雰囲気作りをして、たとえばスパムメールが大量に寄せられている現状に鑑み、海外のIPアドレスを特定して、国際的な手配をするなどの機能強化に特化すべき。こういったNISCのあり方について事務レベルで各府省情報セキュリティ担当者と十分な議論をしてはどうか。 学者や民間人に乗せられて、施策を作るのではなく、あくまで行政の一環として、官側でグリップしていただきたい。 法律によって罰則規定のある守秘義務を課せられている国家公務員は、もともと情報漏えいリスクが極めて低い。ましてや霞ヶ関で勤務する職員は遵法精神が高く、意識の高い職員ばかりで構成されている前提があるはず、こういった前提を真っ向から否定するようなNISCの仕事のやり方はステークホルダーである各府省から支持されないのではないか。 （個人）	御指摘の内容の一部については、今後の政策の推進にあたっての参考の一つとさせていただきます。