平成23年度個別施策ヒアリング資料(優先度判定)【総務省】

施策番号	20114	施策名		ネットワークセキュリティ基盤技術の推進			
新規／継続	継続	領域	共通基盤	国際的位置付け	世界最先端	AP施策	
競争的資金		e-Rad		社会還元			
施策の目的及び概要	我が国の国民生活・社会経済活動において情報通信技術への依存度が高まってきている今日、様々な種類の脅威に対するネットワークセキュリティに関する基盤技術の研究開発を推進することにより、継続的にネットワークセキュリティ対策の高度化を図り、我が国の高度情報通信ネットワークの安全性及び信頼性を確保する。						
達成目標及び達成期限	平成27年度までに、理論と実践を高度に融合させたネットワークセキュリティ基盤技術を確立し、我が国の高度情報通信ネットワークの安全性及び信頼性を確保することを目標とする。						
研究開発目標及び達成期限	NICTの次期中期計画期間の最終年度である平成27年度までに、世界最先端のサイバー攻撃観測・分析・対策・予防技術、セキュアネットワークの設計・評価と最適構成技術、次世代暗号基盤技術等、理論と実践を高度に融合させたネットワークセキュリティ技術の研究開発を行う。						
23年度の研究開発目標	<p>本施策により、平成23年度中に、能動的サイバー攻撃観測技術および、サイバー攻撃分析・予防基盤技術の基礎検討を完了するとともに、モバイル機器・クラウド向けセキュリティ要素技術の理論的モデルの確立や、現代暗号と量子通信技術の融合による量子セキュリティの基礎理論を構築。また、IPv6ネットワークのセキュリティ検証を実施しガイドライン化するとともに、セキュリティ情報利活用のためのサイバーセキュリティ研究基盤構築の基礎技術を確立。</p> <p>さらに、マルウェアの駆除ツールを自動生成し、感染に該当するユーザーに対して迅速(10分程度)に提供する技術を開発するとともに、ルーター等に実装されているカスタマイズ等されたプロトコルに対する評価フレームワーク、評価プロトコルを開発。</p>						
施策の重要性	情報通信ネットワークの飛躍的な発展・普及に伴い、セキュリティ上のリスクも急速に多様化・高度化・複雑化するなか、リスク発生の根本的な解決策として、ネットワークセキュリティに関する先端のかつ実践的な研究開発を実施し、国民が常に安心・安全なコミュニケーションを享受できる環境基盤の構築・実現を図ることが重要。						
実施体制	NICTの自ら研究として研究開発を推進するとともに、一部研究開発については、公募により決定した民間側(受託者)が中心となって研究開発を推進。						
H22予算額(百万円)				H23概算要求額(百万円)			
1,478				1,489			
独立行政法人名(運営費交付金施策のみ)				NICT			
H23概算要求額の内訳	0 0						
期間	H23～H27			資金投入規模(億円)			
これまでの成果(継続のみ)	<ul style="list-style-type: none"> リアルタイム攻撃トラフィック観測・分析、マルウェア自動分析、相関分析等の技術を確立し、それらを統合したインシデント分析センターnicterを構築。 サイバー攻撃発信元追跡、攻撃手法を分析・検証する再現ネットワーク、攻撃下での性能劣化を抑制するセキュア・オーバーレイ等の技術を確立。 プライバシー保護プロトコル、セキュリティ確保プロトコル及びその評価手法等を確立。 <p>・攻撃の全域性および地域性、攻撃の原因、攻撃への対策を明らかにできるインシデント分析の広域化・高速化技術を確立。</p>						

	<ul style="list-style-type: none"> ・ユーザのパソコンに負荷をかけない方法で怪しい実行コードを探索・収集する機能、怪しい実行コードがマルウェアかどうかを解析・判断する機能、マルウェアを駆除するツールを短時間で生成する機能を確立。 ・通信機器に実装された通信プロトコルが、規格上、想定されない動作を行っていないかを判定する技術を確立。 		
社会情勢・技術の変化(継続のみ)	<p>サイバー犯罪は、平成21年度の検挙件数が5年前の2倍に達するなど、年々増加しており、ネットワークセキュリティ対策の強化が望まれている状況にある。また、IPv6やクラウドなど、新たなネットワーク基盤やサービス基盤が普及しつつあり、そのセキュリティ検討が喫緊の課題となっている。さらに、暗号解読技術や、計算機の処理能力の向上による暗号アルゴリズムの危殆化が問題視されるようになり、運用を含めた現代暗号技術および次世代暗号技術の高度化が重要となっている。</p>		
昨年度優先度判定(継続のみ)	着実	優先度判定時の指摘への対応(継続のみ)	<ul style="list-style-type: none"> ・インシデントの対策では、攻撃の地域性に対処するため、その拠点を地域性を網羅する形で広域化し、全国民が安心してネットワークを利用できるよう研究基盤を強化する。 ・マルウェア対策では、国民のPCに負荷をかけない方法で脅威を発見し、より短時間に対策を供給できるよう迅速な安全対処を実現する。
国民との科学・技術対話推進への対応(対象施策のみ)	—		