

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	20001	施策名		国際連携によるサイバー攻撃予知・即応技術の研究開発			
新規／継続	新規	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	サイバー攻撃に関する情報収集ネットワークを国際的に構築し、ISP、大学等と協力して、サイバー攻撃に対抗するための研究開発を実施し、日本におけるサイバー攻撃等のリスクを最小限に抑える。						
達成目標及び達成期限	平成27年度までに、サイバー攻撃に関する情報収集ネットワークを国際的に構築し、ISP、大学等と協力して、サイバー攻撃に対抗するための研究開発を実施し、日本におけるサイバー攻撃等のリスクを最小限に抑える。						
研究開発目標及び達成期限	平成27年度までに、情報セキュリティ脅威に対しての即応技術及びネットワーク脅威予報技術を確立する。						
23年度の研究開発目標	平成23年度末までに、新種マルウェア収集システム、マルウェア挙動観察システム、攻撃情報検知・分析システムの各基本枠組みを構築						
施策の重要性	近年、大規模なサイバー攻撃が世界各国で発生し、大きな問題となっている。2007年4月にはエストニア、2009年7月には米国及び韓国において大規模なサイバー攻撃が発生し、政府関係機関等の主要機関のウェブサイトのサービスが長期間に渡って停止する事態となり、国民生活や経済活動に甚大な影響を及ぼしたところである。我が国においても、大規模なサイバー攻撃を想定した対策が必要である。						
実施体制	研究開発主体は公募により決定。本研究開発では、海外を含む多数のISP、大学等と連携体制を構築予定。得られた成果は国内ISPやウイルスベンダー及び内閣情報セキュリティセンター等の関係機関に提供することで、国内のセキュリティ対策を強固にしていく。						
H22予算額(百万円)				H23概算要求額(百万円)			
-				700			
独立行政法人名(運営費交付金施策のみ)							
H23概算要求額の内訳	人件費:122 (部長等研究員2人 主任研究員7人 研究員16人) 機材費:441 【主な内訳】 ・機器リース費:441 ・機器購入費:0 その他:137						
期間	H23～H27			資金投入規模(億円)		35	
これまでの成果(継続のみ)							
社会情勢・技術の変化(継続のみ)	近年、大規模なサイバー攻撃が世界各国で発生し、問題となっている。2007年にはエストニア、2009年には米国及び韓国において大規模なサイバー攻撃が発生し、政府関係機関等の主要機関のウェブサイトのサービスが長期間に渡って停止する事態となり、国民生活や経済活動に甚大な影響を及ぼしたところである。 サイバー攻撃の対応が現状後手に回っている背景に、Gumblar等の新種マルウェアの発						

	生数の急増、サイバー攻撃手法の高度化・巧妙化等がある。さらに、国境を越えた広域事例が増加しており、各国の協力体制強化が課題となっている。		
昨年度優先度判定(継続のみ)	—	優先度判定時の指摘への対応(継続のみ)	
国民との科学・技術対話推進への対応(対象施策のみ)			