「情報セキュリティ研究開発戦略（改定版）（案）」の概要について

資料2

サイバーセキュリティ戦略（2013年6月策定） において示された
○ サイバー攻撃の検知・防御能力の向上
○ 制御システム、ICチップなど社会システム等を保護するためのセキュリティ技術の確立
○ ビッグデータ（パーソナルデータ等）利活用等の新サービスのための技術開発　等

を推進する観点から、**「情報セキュリティ研究開発戦略」を改定**

情報セキュリティ研究開発の推進方針

1. **サイバー攻撃の検知・防御能力の向上**
   - ・分散しているサイバー攻撃情報等の共有のための組織等の連携強化
   - ・研究者等へ政府の有するサイバー攻撃の検体等の提供等を検討
2. **社会システム等を防護するためのセキュリティ技術の強化**
   - ・制御システム等のセキュリティ技術の国際標準化・認証制度等を推進
3. **産業活性化につながる新サービス等におけるセキュリティ研究開発**
   - ・今後発展が期待されるIT利用分野で上流工程からセキュリティ品質の組込を推進
4. **情報セキュリティのコア技術の保持**
   - ・暗号等のコア技術の保持は、我が国の新規産業創出や安全保障等の観点から重要であり維持・強化
5. **国際連携による研究開発の強化**
   - ・各国が「強み」を有する技術を組合せ発展させるため、研究者受入等国際連携を推進

研究開発の効果・成果を高めるための方策等

1. 研究成果の社会還元の推進
2. 必要な研究開発リソースの確保と柔軟性確保
3. 情報セキュリティ技術と社会科学など他分野との融合

情報セキュリティ研究開発における重要分野

（※　左記の観点を踏まえ、重要分野を整理）

（1）情報通信システム全体のセキュリティの向上

サイバー攻撃の検知、認証、次世代ネットワーク　等

（2）ハード・ソフトウェアセキュリティの向上

制御システム、デバイス、ソフトウェアの安全性確保　等

（3）個人情報等の安全性の高い管理の実現

プライバシー保護、パーソナルデータ利活用　等

（4）研究開発の促進基盤の確立と理論の体系化

理論体系化、調査研究、標準化、評価、暗号技術　等

（5）発展分野でのセキュリティ研究開発

医療健康、農業、次世代インフラ、ビッグデータ、
自動車のネットワーク接続　等