「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3

サイバーセキュリティ戦略（H25年6月策定） において示された、「活力ある」サイバー空間の構築」（産業活性化、研究開発）を目指し
- ○ 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**
   研究開発における実際のサイバー攻撃情報等の重要性に鑑み、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、可能な範囲・方法・条件で研究者等へ政府の有する標的型攻撃等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**
   社会システム等を構成する制御システム等のセキュリティ技術の研究開発にあたっては成果の早期実用化が重要であることに鑑み、国際標準化・認証制度につながるよう推進。
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**
   産業活性化・国際競争力の強化の観点から、今後発展が期待されるICT利用分野で企画・研究開発・設計段階等上流工程からセキュリティ品質を組み込み等の取組みを促進。
4. **情報セキュリティのコア技術の保持**
   暗号等の基礎研究をはじめ情報セキュリティ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、大学・公的研究機関等の役割も含めて維持・強化。
5. **国際連携による研究開発の強化**
   サイバーセキュリティに係る高度な技術の研究開発に向け、各国が「強み」を有する技術を組み合わせ発展させるなどのため、研究者受け入れを含め国際連携を推進。

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** ： 事業化等に向けて研究者等を支援するための環境整備
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、経営学など他分野との融合** ： 技術のみならず安全保障・危機管理、経済学、経営学、心理学等の研究者とも連携した取り組みを促進

情報セキュリティ研究開発における16の重要分野

（※ 上記の観点を踏まえ、従来の重要分野を見直し）

（1）情報通信システム全体のセキュリティの向上	
①	サイバー攻撃の検知／防御
②	ID連携／認証／アクセス制御
③	ITサービスのセキュリティ（スマートフォン／クラウド等）
④	次世代ネットワークセキュリティ
（2）ハード・ソフトウェアセキュリティの向上	
⑤	制御システムセキュリティ
⑥	セキュリティデバイス
⑦	ソフトウェアの安全性確保
（3）個人情報等の安全性の高い管理の実現	
⑧	プライバシー保護／パーソナルデータ利活用のための技術
⑨	フォレンジック等を支援するためのデータ管理・追跡技術
（4）研究開発の促進基盤の確立とセキュリティ理論の体系化	
⑩	セキュリティ理論体系化／調査研究
⑪	標準化／評価／制度／基盤整備
⑫	暗号技術
（5）発展が期待される応用分野でのセキュリティ研究開発	
⑬	医療健康分野での情報流通変革に伴い必要となるセキュリティ技術
⑭	次世代インフラで必要となるセキュリティ技術
⑮	ビッグデータにおける情報の秘匿化、暗号化等のセキュリティ技術
⑯	家電、自動車のネットワーク接続で必要となるセキュリティ技術