NISC National center of Incident readiness and Strategy for Cybersecurity

資料4

今後の取組の方向性について

平成28年10月31日

サイバーセキュリティ戦略本部 研究開発戦略専門調査会

内閣サイバーセキュリティセンター（NISC）

１．方針

- 平成26年7月に、今後3年程度を見据えた基本的な研究開発の方針として、「情報セキュリティ研究開発戦略（改定版）」を策定。今後、「サイバーセキュリティ基本法」及び「サイバーセキュリティ戦略」（平成27年9月策定）を踏まえ、「サイバーセキュリティ研究開発戦略」を本資料７ページのスケジュールに従い、来年６月を目途に策定することとしたい。その際、以下の方針の下で策定することとしてはどうか。

- 「サイバーセキュリティ戦略」においては、サイバーセキュリティの研究開発は、サイバーセキュリティの「共通基盤的な取組」であり、「成果が出るまでに長い時間を要することに加え、多岐にわたる取組が必要となることから、横断的、中長期的な視点で取り組むことが必要」としている。このため、**近い将来と中長期の双方の視点で研究開発を推進することが必要**ではないか。

- 具体的には、今後、**近い将来**を視野に入れ、社会・経済やITの利活用の進化と深刻化するサイバー攻撃の脅威に対応するため、幅広い分野でのITの利活用（組織内の生産性向上を目的とした情報システムの活用に留まらないITの利活用）について、技術的なアプローチだけでなく、社会科学的なアプローチを含めたサイバーセキュリティに関する研究開発を推進することが必要ではないか。

- さらに、**中長期的な社会・経済の進化（メガトレンド）**を見据え、ITの利活用の方向性に関わらず、本質的に必要なセキュリティの研究開発を推進していくことも必要ではないか。

２．次期サイバーセキュリティ研究開発戦略について

１．研究開発の目的

次期サイバーセキュリティ研究開発戦略における研究開発の目的については、サイバーセキュリティ戦略等を踏まえ、現行の「情報セキュリティ研究開発戦略（改定版）」と同様、以下の考え方としてはどうか。

(1) 研究開発を通じて国際競争力を強化すること
(2) 研究開発で得られた知見により経済成長につながる新産業を創出すること
(3) 我が国として必要な技術力を獲得・保持すること

２．論点の時間軸

以下の２つの時間軸で、検討をしてはどうか。また、その際、「近い将来」と「中長期的な」とは具体的にどの程度の時間を想定すれば良いか。

(1) 近い将来の社会・経済とITの利活用の進化と、深刻化するサイバー攻撃の脅威への対応
(2) 中長期的な社会・経済とITの利活用の進化（メガトレンド）を踏まえた対応

３．論点の対象範囲

政府や公的研究機関等のみならず、大学、企業等の取組についても視野に入れた議論が必要ではないか。

また、個々の技術的な課題を深掘りするのではなく、将来的なセキュリティの概念を踏まえた研究開発の方向性について、ビジョンを示すものとしてはどうか。

2．次期サイバーセキュリティ研究開発戦略について

4．論点の項目

（1）ー①：近い将来のITの利活用をとりまく社会・経済の変化はどのようなものか。

【社会におけるITの変化（例）】
・社会における情報通信技術への依存の高まり
・データが新たな価値を創出
・すべての人が常につながる状況へ

【ITの技術的な変化（例）】
・通信量の増大
・クラウドサービスの普及
・センサの低価格化、増加
・データ解析技術の向上

新たな社会への
アプリケーション

【アプリケーションの例】

保険医療：
　生涯にわたる健康情報を自分で管理でき、自分の判断のもとで病院などに健康情報を提供することで安全で効果的な健康や医療、介護に関わるサービスを利活用できる

生活空間：
　人の状態や行動に合わせて、家庭やオフィスや公共空間のさまざまな機械やディスプレイが協調して、情報提示やものの運搬、移動の支援をする

環境対策：
　家庭内から地球規模にいたるマルチスケールでエネルギーや資源の産出、利用、消費の情報が可視化され、「人と地球との調和」に向けて活用される。環境や人間活動のセンシングデータに基づき、利用者ニーズに適した形で情報やサービスが提供される

出典：新世代ネットワーク推進フォーラム　アセスメントWG活動報告

2．次期サイバーセキュリティ研究開発戦略について

（１）－②：近い将来のITの利活用技術の進化とセキュリティ研究開発における課題をどのように認識すべきか。

【イメージ】

	①サイバー空間と物理空間の融合（IoT）	②AIの高度化・BD（ビッグデータ）の活用	③ネットワーク技術の高度化
想定されるIT利活用技術の進化	（例） ✓ 自動走行技術の実現 ✓ スマートハウス・ロボット普及 ✓ 物理セキュリティ（警備など）のIT化	（例） ✓ 職業代替 ✓ 個人情報の自動収集・BD化 ✓ サイバー攻撃のAI化	（例） ✓ SDN等によるネットワーク仮想化技術の高度化 ✓ 分散処理(ｴｯｼﾞｺﾝﾋﾟｭｰﾃｨﾝｸﾞ・ﾌｫｸﾞｺﾝﾋﾟｭｰﾃｨﾝｸﾞ) ✓ ブロックチェーン
セキュリティ研究開発の課題例	• セキュリティの範囲が広がるため、セキュリティ技術のみならず、幅広い技術の知見を統合した研究開発。 • これまで物理空間特有の問題であった安全管理を視野に入れたセキュリティの研究開発。	• ビッグデータの信頼性を確保して活用する技術やプライバシー保護の技術開発。 • AIの脆弱性に対する攻撃対応。 • サイバー攻撃のAI化への対応（防御のAI化）。	• 新しいネットワーク技術におけるセキュリティ・バイ・デザインが必要。 • 暗号の高速化・高度化が必要。（例：暗号化したまま高速に検索ができる技術の確立など）

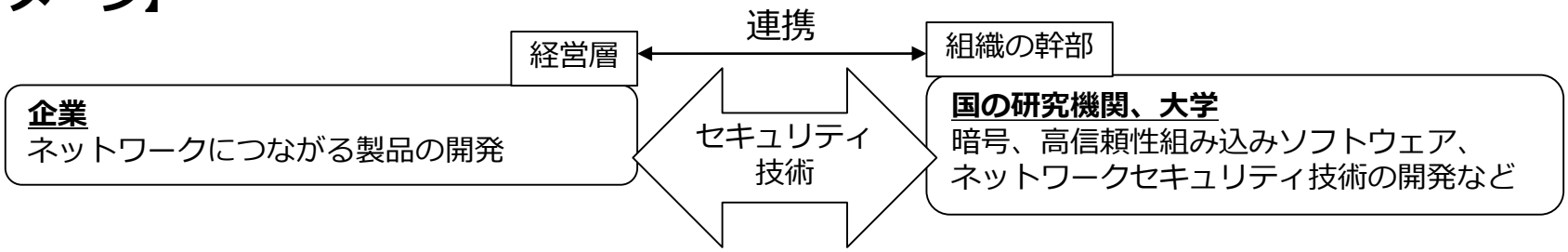
2．次期サイバーセキュリティ研究開発戦略について

（1）－③：こうした変化に対応するため、セキュリティの研究開発ではどのような方法論が必要か。

【方法論の例】

○産学官連携と企業経営層のリーダーシップ

【イメージ】



○攻撃の実データを活かした実践的な研究開発

【研究機関に求められるアクションの例】

- 多様な主体と連携し、積極的にサイバー空間で起こっていること（攻撃動向や攻撃データ）を収集
- アクティブディフェンス（積極的に攻撃を受けながら守る）

○サイバーセキュリティの研究に係る法令、基準等の検討

2．次期サイバーセキュリティ研究開発戦略について

（2）中長期的な社会・経済（メガトレンド）はどのように想定されるか。その上で、どのような方向にITの利活用が進化したとしても、中長期的な視点に立った場合、共通して必要となる本質的なセキュリティの研究開発は何か？

【イメージ】

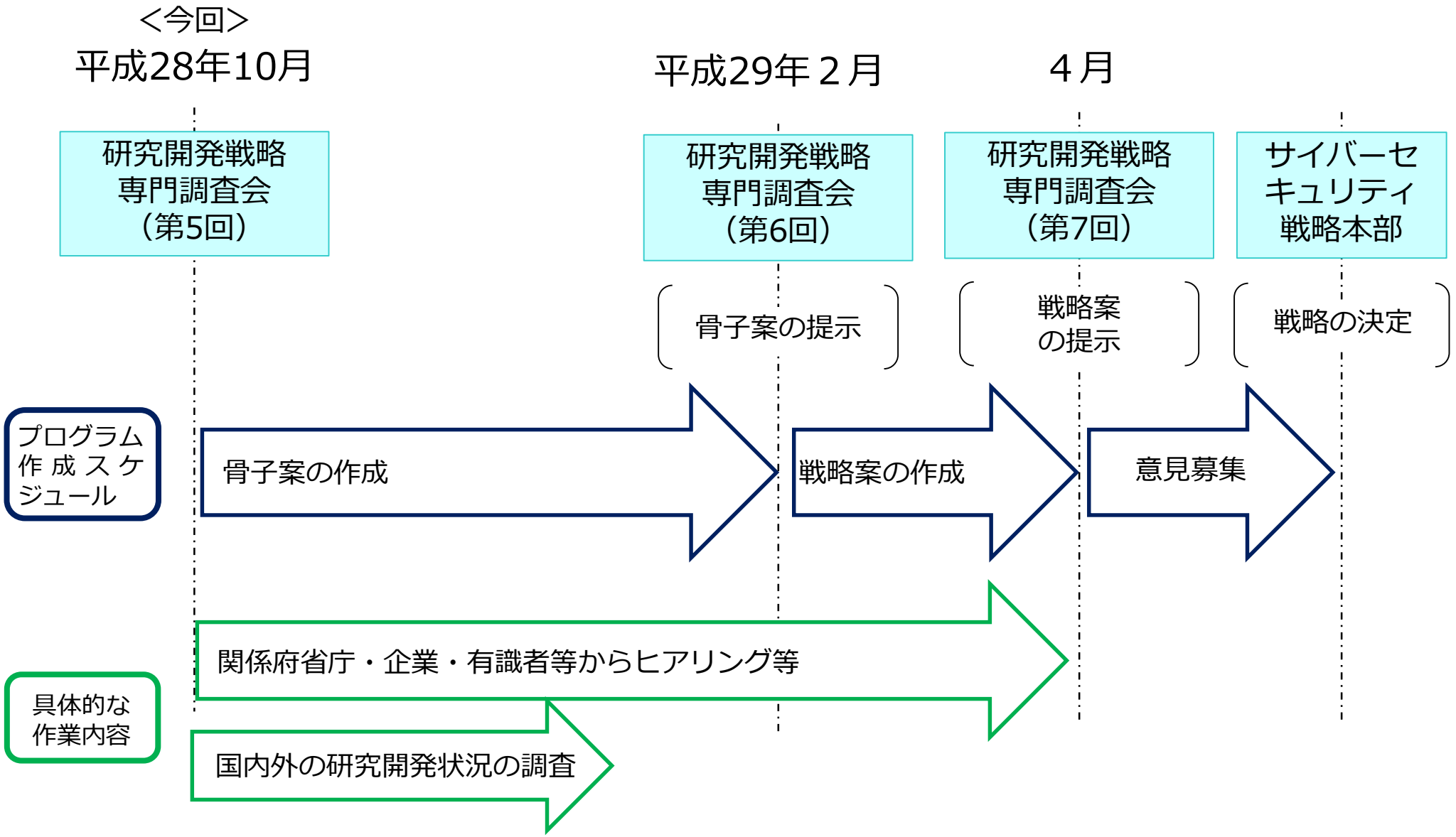
人間を取り巻く体制の変化（集中から分散へ）
- ブロックチェーンにより、各国の通貨の在り方が変わり、あらたな政策協調が求められる可能性。
- IoTは非対称な個人・組織にも、社会の基盤に影響を及ぼしうる能力を与える可能性。

価値の変化（モノ文化からサービス文化へ）
- 新たな製造技術や自動化技術の登場によって、大半のモノは容易に一定の品質の下でカスタマイズされ、サービスが競争力の源泉になる可能性。
- サービス品質は人から収集したデータが支配する可能性。

主体の変化（人・組織からプログラムへ）
- プログラムの品質が社会を左右する可能性。
- 判断の主体の変化によって、責任分界点が変化するとともに、それに併せた規制の在り方が求められる可能性。

【ITの利活用の方向性に関わらず必要な本質的なセキュリティの研究開発とは？】
- サイバー空間と人・物理空間が接する部分のセキュリティ研究（安全とサイバーセキュリティの分野など）？
- 新しいサービスのモデル・プラットフォームのセキュリティに関わる研究やデータの信頼性・トレーサビリティに関わる研究？
- プログラムの脆弱性に関する研究？

3．研究開発戦略改定のスケジュール（イメージ）



（参考）「情報セキュリティ研究開発戦略（改定版）」（平成26年７月）の概要

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

（参考）これまでの政府における研究開発の取組状況

関係省庁	各省庁の研究開発の例
総務省	・標的型攻撃研究の基盤となる組織内ネットワークのリアルタイム分析環境および大規模蓄積環境を整備（NICT） ・サイバー攻撃観測技術を高度化するための能動的観測システムの開発及び実証実験を実施（NICT） ・暗号化したままセキュリティレベルの更新と加算と乗算が可能な技術を開発（NICT）
経済産業省	・システムの挙動を解析し、サイバー攻撃を検知する技術開発や、ホワイトリスト技術に関する研究を実施（CSSC） ・ソフトウェア工学について、大規模ソフトウェアの解析ツールを開発し、自動車等組込みシステムを題材に有効性を検証（AIST） ・暗号技術において、暗号化したままデータ処理や認証・認可を実現する高機能暗号技術について、高速処理を可能とする新方式や暗号文サイズが世界最小値となる技術を開発（AIST）
総務省・経済産業省	・暗号技術評価委員会及び暗号技術活用委員会を開催し、暗号技術の安全性に係る監視及び評価、新世代暗号に係る調査、暗号技術の安全な利用方法に関する調査、暗号の普及促進、セキュリティ産業の競争力強化に係る検討、暗号政策の中長期的視点からの取組の検討等を実施（NICT・IPA）
文部科学省	・M2Mを含めたサイバー攻撃に関する通信データ等を収集し、共有する体制の構築を開始（NII） ・ビッグデータやAI（人工知能）等、社会・技術の変化を先取りした研究開発について検討
内閣府	・戦略的イノベーション創造プログラム（SIP）に「重要インフラ等におけるサイバーセキュリティの確保」を新規課題として追加し、府省庁の枠や旧来の分野の枠を超えた研究開発を推進