

次世代型超低消費電力デバイス開発プロジェクト

出口戦略

①次世代半導体微細加工評価基盤

半導体メーカー	デバイス: A社 他 半導体世界シェア20% 3D NANDフラッシュシェア2位	2016年からの実用化を目指す。
マスクメーカー	マスクブランク: B社 他 世界シェア85%	EUV対応マスクブランクの供給。 トップシェアを維持。
レジストメーカー	マスク: C社、D社、B社 参画企業3社の世界シェア45%	EUV対応マスクを2014～2015年から供給。
装置メーカー	レジスト: E社、F社、G社、H社 参画企業4社世界シェア77%	EUV対応レジストを2014～2015年から供給。
	マスクブランク検査装置: I社 同検査装置シェア100%	EUV対応装置の供給。 トップシェアを維持
	マスクパターン欠陥検査装置: J社 微細化(45nm)対応装置事業化	EUV対応の検査装置をマスクメーカー等へ供給

次世代EUVについては、マスク、レジスト材料などに特化しており、戦略として有効であると考えられる。但し、EUVリソグラフィシステムが世界の開発拠点あるいは半導体企業のいずれかででも実現することが大前提であるので、グローバルでの連携・協調をさらに進めて、EUVのトータルシステム実現に貢献いただきたい。

②革新的な次世代型低消費電力デバイス開発事業



● 各テーマのキーポイントについての助言、提案(続き)

次世代型超低消費電力デバイス開発プロジェクト

- 1) 0.4V駆動デバイス技術開発については、既出のアプリケーションが求める半導体デバイスの動作速度、集積規模、機能をその時期の最先端半導体デバイスとベンチマークする必要がある。トレードオフがあるならば、「何等かのExcuseについて許容できるか?」、あるいは「出口として機能を限定したアプリを追及できるか?」についての議論を、超低消費電力化指向の携帯機器メーカー等のアプリレイヤーの方々と一緒に議論を進めていけば、より良い体制になると考えれる。
- 2) 微細化の進展に伴う問題的(パラメータばらつきやリーク電流の増大)により、半導体デバイスの低電圧化は限界に達していることを解決する一手段として、新原理デバイスを活用する観点は重要。ただし、新原理利用に伴う新たなリスクも発生する。特に、「実用化」を推進するにあたり、デバイス性能はもちろん、インテグレーションし易さや材料コスト(レアメタル問題など)なども総合的に鑑みて、新原理デバイスを取捨選択していく体制を検討してはどうか。
- 3) 次世代EUVについては、マスク、レジスト材料などに特化しており、戦略として有効であると考えられる。但し、EUVリソグラフィシステムが世界の開発拠点あるいは半導体企業のいずれかでも実現することが大前提であるので、グローバルでの連携・協調をさらに進めて、EUVのトータルシステム実現に貢献いただきたい。

6. 【次・総04】サイバーセキュリティの強化

出口戦略

「サイバーセキュリティの強化」については、マルウェア解析技術、ネットワークモニタリング技術、データマイニング技術、ぜい弱性検証・セキュリティ評価技術等の研究開発を実施。これらの技術について、外部有識者による評価会等の意見を踏まえながら、主に以下の3つの方向性から効果的な成果の展開を図ることで、社会全体におけるサイバー攻撃等に対する対処能力を向上させる。

■ テレコム・アイザック推進会議※等の業界団体との連携を通じたサービス化・事業化

(例) 個人のインターネット利用者を対象としたマルウェア配布サイトへのアクセスを未然に防止する技術、サイバー攻撃の発生を予知し、即応を可能とする技術、サイバー攻撃に対する防御モデルについて、国内の主要インターネットサービスプロバイダ等から構成される団体等を通じて効果的な成果の共有を行う。

※ テレコム・アイザック推進会議: インターネット・サービス・プロバイダやウイルス対策ベンダ等の事業者間で情報セキュリティに関する情報を共有・分析し、サイバー脅威に対して適切な対策をとることを目的とする団体

■ 研究開発の受託事業者における実用化・製品化

(例) 利用者の行動特性に応じてサイバー攻撃を早期に検知し動的な防御を実現する技術について、システムベンダ等の受託事業者において、技術の商品化・製品化を行う。

インフラを制御するシステムのセキュリティ評価・認証技術について、制御システムを運用する企業などにおいて活用を図る。

■ 独立行政法人・大学等の研究機関等の公的機関を通じた社会への還元

(例) マルウェア感染の早期検知技術で開発した一部の技術(DAEDALUS)について、地方公共団体向けに展開することで、成果の展開を図る。

課題

- 「サイバーセキュリティの強化」の推進において、主に以下の課題を認識している。
- サイバー攻撃については常に攻撃手法が最新化され、高度化・複雑化により、研究開発する技術が陳腐化する可能性がある。
 - サイバーセキュリティの分野においては、サイバー攻撃に対する防御を前提とするため定量的な評価が困難である。

本質的な見直しが必要に思える

- 出口戦略

1. 国家として守るべき拠点に対し、研究成果を実システムに適用し、戦略的に防御(=実装)していく。
2. 東京オリンピックへの実装
例えば、「世界一安全な都市(東京)・国(日本)」。
3. 新たな領域への展開
例えば、
 - a. スマートグリッドや交通など重要社会インフラを担う制御系システム
 - b. 災害現場などでの活用が期待される自動化・自律化ロボットなど
4. ファクトに基づいた(国内外の)政策立案を支援
 - a. 諸外国との法制度の相互運用性、国際的連携体制
 - b. 国内業界団体との連携によるファクトの情報共有

- 課題

1. IT機器の利用者や運用者との協働
2. グローバル空間での国際的連携体制(含政策)
3. 新たな領域の出現

- 施策・研究内容に関するコメント

1. 実際に、国家として防御すべき拠点への実装・運用が示されていない。
2. IDおよび本人確認に関する研究が、不足している。
3. セキュリティー専門家のみでの活動になっているように見える。
 - a. 他分野との連携を促すべき。
 - b. 競争的研究費を増やすべき。
4. グローバルな空間での諸外国との連携に関する具体的な施策が提示されていない。
5. 関連する業界団体が、縦割りにになっていないか？
6. 情勢判断及び意思決定の支援に関する研究が欠けている。
7. ソフトウェアの脆弱性に偏っていないか？ SW、HW以外にもプロトコル、設定、運用の脆弱性が認識されている。

「サイバーセキュリティの強化」については、総務省・NICT・経済産業省の連携のもと、以下の取組を実施しているところ。

- ・国際連携によるサイバー攻撃予知・即応技術の研究開発（総務省）
- ・サイバー攻撃解析・防御モデル実践演習の実証実験（総務省）
- ・サイバー攻撃の解析・検知に関する研究開発（総務省）
- ・高度化・巧妙化するマルウェアを検知・除去し、感染を防止するためのフレームワークに関する実証実験（総務省）
- ・マルウェア感染の早期検知技術の研究開発（NICT）
- ・ネットワーク構成要素における適切な情報セキュリティ設定導出に関する研究開発（NICT）
- ・東北復興再生に資する重要インフラIT安全性検証・普及啓発拠点整備・促進事業（経済産業省）

国際連携によるサイバー攻撃予知・即応技術の研究開発

2

プロジェクト略称: **PRACTICE**, Proactive Response Against Cyber-attacks Through International Collaborative Exchange

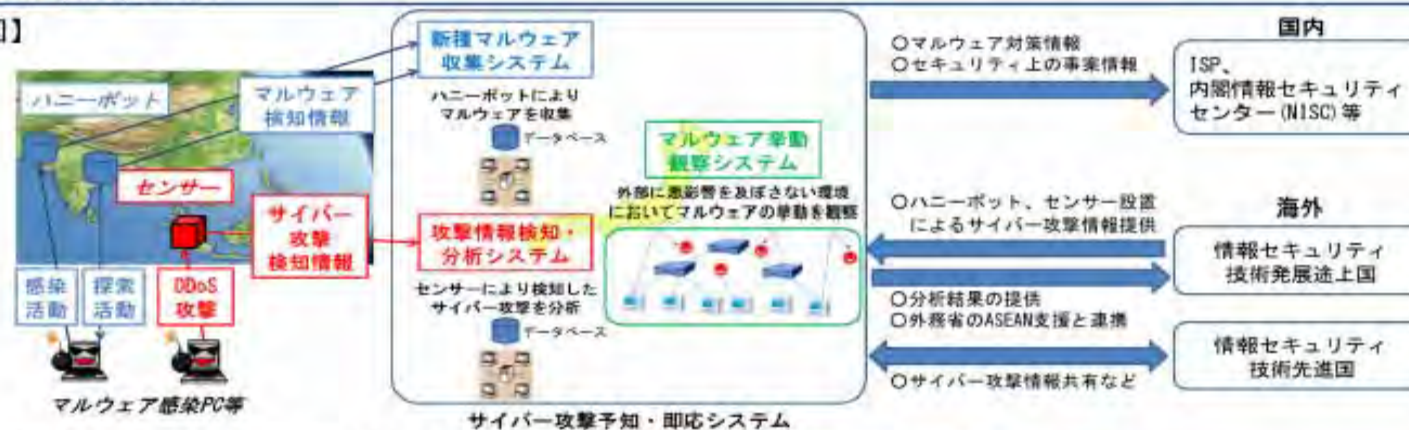
○目的:

近年、被害が拡大しているサイバー攻撃(分散型サービス妨害攻撃、マルウェアの感染活動等)に対処し、我が国におけるサイバー攻撃のリスクを軽減。

○概要:

国内外のインターネットサービスプロバイダ(ISP)、大学等との協力によりサイバー攻撃、マルウェア等に関する情報を収集するネットワークを国際的に構築し、諸外国と連携してサイバー攻撃の発生を予知し即応を可能とする技術について、その研究開発及び実証実験を実施。

【イメージ図】



○マルウェア: コンピュータウイルスのような有害なソフトウェアの総称。

○DDoS(Distributed Denial of Service)攻撃: 分散型サービス妨害攻撃。多数のPCから一斉に大量のデータを特定宛先に送りつけることにより、当該宛先のネットワークやサーバを動作不能にする攻撃。

○ハニーポット: 故意に外部からの侵入を容易にした図のネットワーク機器。マルウェアの感染活動等の検知を目的にネットワーク上に設置。

【実施期間】 H23~H27

【実施機関】 総務省

国際連携の状況

- 平成23年11月、「第4回日・ASEAN情報セキュリティ政策会議」において、ASEAN各国に連携を呼びかけ。
- 平成24年3月には、サイバー攻撃の予知のための研究開発の協力について、米国と合意。6月に研究者中心の日米会合を実施。
- そのほか、平成24年3月にインドネシア、4月にモルディブ、平成25年2月にタイ、3月にマレーシアとの間で合意。
- 現在、欧州諸国、シンガポール等と連携に向けて協議中。

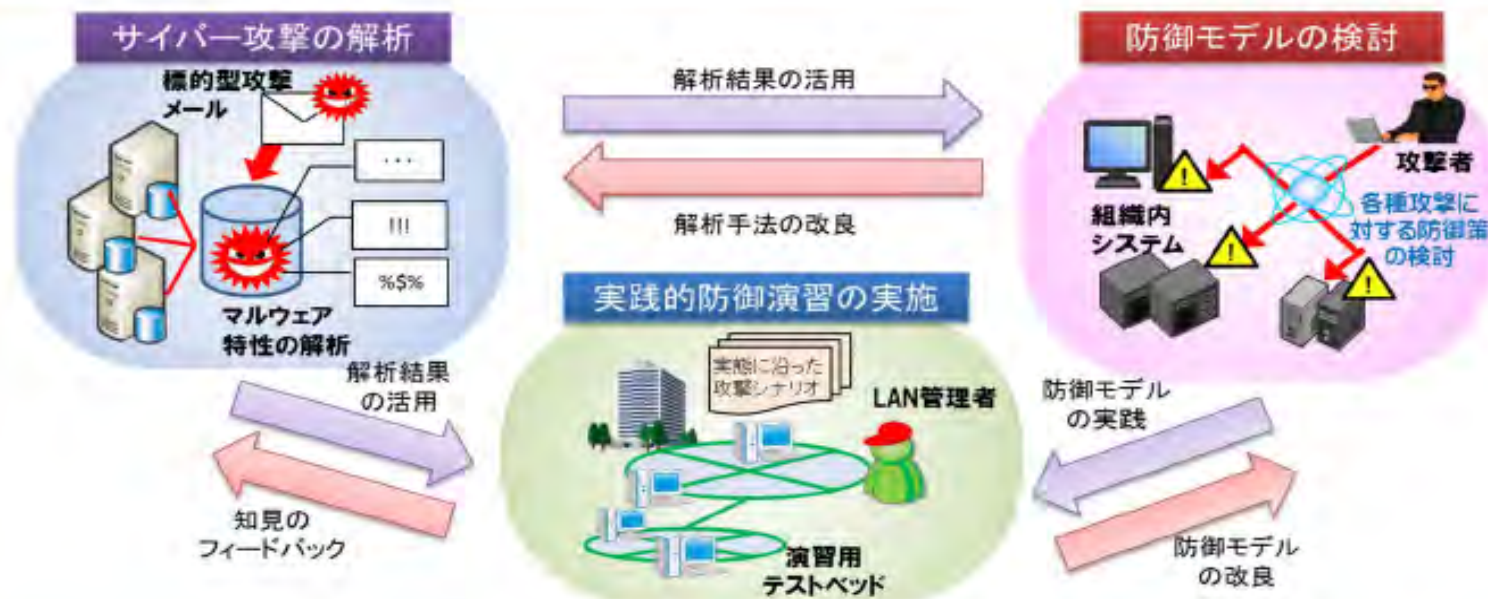
- ➔ 1. 具体的な施策に進展させるべき。
2. 実ビジネスの主体との連携を実現すべき

サイバー攻撃解析・防御モデル実践演習の実証実験

3

新たなサイバー攻撃に対応可能な環境を実現するため、攻撃の解析及び防御モデルの検討を行い、官民参加型のサイバー攻撃に対する実践的な防御演習を実施する。

標的型攻撃：特定の組織や個人を標的に複数の攻撃手法を組み合わせ、執拗かつ継続的に行われる攻撃。



【実施期間】 H24～H29

【実施機関】 総務省

- ➔ 1. 「サイバー攻撃の解析」の具体的な協力先と体制を構築すべき。
- 2. 「実習の実施」が人材育成のみでは、不十分である。
- 3. 実証実験の次を提案して頂きたい。

サイバー攻撃の解析・検知に関する研究開発

4

目的 利用者の行動特性や環境特性等に基づいて不正な意図を検知し、侵入や感染の可能性、被害の程度、被害に至った経緯を明らかにするための技術を確認するとともに、被害拡大の防止と業務継続を両立させる組織内ネットワークを自動的に構成する技術などを開発する。

研究開発概要

検知・解析 (Observe)

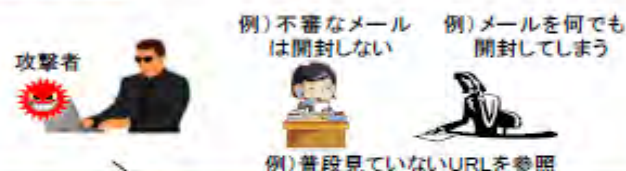
情勢判断 (Orient)

意思決定 (Decide)

行動 (Act)

I. 行動特性

・利用者の行動特性の研究 (騙され易い人、難しい人の差 等)



II. 環境特性

・端末情報の効果的な収集方法の研究開発
・ネットワーク状況の効率的なスキャン方法の研究開発 等



進行状況
進入経路
の把握

III. 攻撃阻止と業務継続

・行動特性に応じたセキュリティレベルを適応的に設定する技術の研究開発
・進行状況や進入経路を適切に把握する技術の研究開発
・被害を拡大させずかつ業務を継続させる組織内ネットワーク構成技術の研究開発 等



【実施期間】 H25～H29
【実施機関】 総務省

- ➔ 1. 重要な課題である。
2. 具体的な、行動と環境を決め、実際に、適用・運用することを、目指すべき。