補足資料3

有識者ヒアリングに基づく重点分野候補

有識者ヒアリングの対象者

研究カテゴリ	ヒアリング相手	観点
暗号基盤技術	横浜国立大学大学院　教授 松本勉先生	秘密計算、次世代ハッシュ、ペアリング暗号等の新技術の方向性と課題
アクセス制御技術	NTTコミュニケーションズ 山下達也氏	ネットワークサービスに対する不正アクセスの傾向、課題、優先分野。
バイオメトリクス技術	産業技術大学院大学　教授 瀬戸洋一先生	マルチモーダルバイオメトリクスなど今後の研究の方向性、課題
セキュアネットワーク構築技術	倉敷芸術科学大学　教授 小林和真先生	次世代インターネット移行に係わるリスクと対策、課題
ネットワーク観測防御技術	JPCERT/CC 理事　鈴木裕信氏	内部攻撃検知、攻撃予測などによる早期対応技術の現状、期待効果、課題。
無線セキュリティ技術	慶応義塾大学　教授　笹瀬巌先生	無線ネットワークの普及により脅威と研究課題の方向性
プライバシー保護技術	筑波大学　准教授　佐久間淳先生	プライバシー保護データマイニング等の新しい技術の課題、効果、方向性。
セキュアシステム構築技術	東京大学　教授　柴山悦哉先生	ソフトウェアライフサイクルにおける対策技術、高信頼システム開発技術の課題
コンテンツセキュリティ技術 （データセキュリティ技術）	奈良先端技術大学院大学　教授 山口英先生	DRM等によるコンテンツ保護技術の課題、効果、方向性。
セキュリティ評価・マネジメント	東京大学　准教授　松浦幹太先生	攻撃者インセンティブとリスクの影響度評価に関する課題と対策の方向性。

有識者ヒアリングに基づく重点分野候補(1/3)

研究カテゴリ	重点分野	達成目標 (社会ビジョン)	選定理由
暗号基盤技術	情報理論的安全性を備えた暗号技術	汎用コンピュータから組込み・重要インフラへと暗号基盤の拡大	計算理論的な暗号技術は、暗号危殆化の問題が付きまとう。情報理論的な暗号に基づく鍵管理により、長期に耐えられる暗号が実現される。また、情報理論的な暗号は、線形演算をベースとすることで計算が抑えられるため、計算資源の小さい組込みシステムなど幅広い分野への応用が期待される。
アクセス制御技術	ルータ等へのDDoS検知機能の組込み	広くインターネット全体の脅威検知基盤を確立することにより、脅威の低減を実現する。	現在、DDoS攻撃を利用者・運用者側からは即座に知る手段がないため、被害の拡大防止の仕組みが弱い。ルータ等にDDOS検知機能を組み込み、広く普及させることにより、脅威の発見と対策を早期に行うことで、被害を最小限に抑える効果が期待できる。特にネットワークの境界で、観測および対策を行うことで効果が期待できる。また、ルータの置換えなどに合わせてセキュリティ対策を実施することによりコストを抑えることができる。
	脅威観測ﾃﾞｰﾀの形式の統一化と共有方式の開発	脅威観測に関する国際レベルの協力体制と研究環境の構築により、脅威の低減を実現。	現在、マーケティングなどにおいて通信データの分析が積極的に行われているが、セキュリティの分野で十分に活用されていない。脅威分析を考慮した観測データの統一化とデータの共有方式を検討することにより、脅威検知等の技術の向上に寄与する。
バイオメトリック技術構築	ID管理に関するｼｽﾃﾑｱｰｷﾃｸﾁｬの全体像（ﾌﾚｰﾑﾜｰｸ）の構築	バイオメトリクスを要素とする情報システムのトータルなID管理基盤の確立。	バイオメトリクスの要素技術は性能面でも成熟している。今後は、ID管理、アプリケーション、バイオメトリクスを含むオープンなシステムアーキテクチャの構築が求められる。日本では、人材、企業、政府の取組みにおいて、システムアーキテクチャの検討が十分行われていないために、欧米のみならず、アジアにおいてもリーダーシップを確保することが困難な状況になっている。システムの全体像（フレームワーク）の構築は、国として取り組むべき優先課題であり、国際競争力の面でも、要素技術を開発する企業に対して高い効果が期待できる。
	ﾊﾞｲｵﾒﾄﾘｸｽの適合性評価ﾌﾚｰﾑﾜｰｸの確立	バイオメトリック製品の普及促進によるID管理環境の向上。	各国が認証の技術基盤を提供して適合性評価に向けた取り組みが始まっている。バイオメトリクスの要素技術に強みをもつ日本が、各国の技術基盤を活かした国際的な適合性評価フレームワークを構築するためのイニシアチブをとることが期待される。国際標準を含むこのようなフレームワークの構築において、国として取り組むことにより最小のコストで最大の効果を期待することができる。日本がイニシアチブをとることができれば、日本のバイオメトリックデバイス関連の産業にもプラスの効果を期待することができる。

有識者ヒアリングに基づく重点分野候補(2/3)

研究カテゴリ	重点分野	達成目標 (社会ビジョン)	選定理由
ｾｷｭｱﾈｯﾄﾜｰｸ構築技術	障害時に自動的にﾘｶﾊﾞﾘｰ可能なﾈｯﾄﾜｰｸｱｰｷﾃｸﾁｬの構築技術	一般の利用者が意識しなくても一定のセキュリティが確保される仕組みの実現。	自己治癒(self-configuration, self-healing, self-repairment)型ﾈｯﾄﾜｰｸの構築技術とも捉えられる。 様々な脅威や障害からﾈｯﾄﾜｰｸを完全に守るために必要なｺｽﾄは膨大になる．そこで、ﾈｯﾄﾜｰｸの障害は必ず発生するという前提に立ち、ﾈｯﾄﾜｰｸｻｰﾋﾞｽを止めないようにする為の技術を開発する必要がある。 これには、ﾈｯﾄﾜｰｸに多様性と冗長性を持たせることが必要であり、IPv4とIPv6が共存するﾀﾞｲﾊﾞｰｼﾃｲﾈｯﾄﾜｰｸやﾈｯﾄﾜｰｸの仮想化技術の研究を進める必要がある。
ﾈｯﾄﾜｰｸ観測防御技術	大規模ﾈｯﾄﾜｰｸにおけるﾏﾙｳｪｱ収集挙動分析と広域攻撃観測の統合	ユビキタス環境における安全基盤の向上	ｹﾞｰﾑ機やｽﾏｰﾄﾌｫﾝなどの情報家電のネット接続、IPv6化によりﾈｯﾄﾜｰｸの複雑化や大規模化が進んでいる。 従来は「人」がｵﾍﾟﾚｰｼｮﾝを行うための可視化技術が注目されていたが、「人」による対応には限界がくるため、自動検知技術が必要不可欠になる。 また、異常検知の結果を攻撃対応に活用するためには、自動的にﾄﾗﾌｨｯｸを制御する技術が必要となる。 「悪意の利用者のゲーム理論の研究」【技戦】を含む。
無線セキュリティ技術	ｱﾄﾞﾎｯｸﾈｯﾄﾜｰｸのｾｷｭﾘﾃｨ設定の管理技術	日常用途の無線ネットワークの安全性向上により、ローカル通信サービスの充実。	バックボーンを介さないアドホックネットワークの利活用の拡大が見込まれる中、有線系のセキュリティ技術に対して、特に無線LAN等の物理レイヤー以下の階層の無線セキュリティ技術が十分確立されていない。利便性と安全性のバランスを考慮したセキュリティレベル設定手法を含む、無線セキュリティの基盤確立が市場拡大に伴い求められる。 「無線ブロードバンド環境におけるセキュリティ技術」【技戦】を含む。
	ｾﾝｻｰﾈｯﾄﾜｰｸにおけるﾌﾟﾗｲﾊﾞｼｰ保護	センサーネットワーク普及社会におけるセキュリティ基盤の確保	携帯端末の無線の発信情報の漏洩、センサーネットワークを利用した身体健康情報の送受信などプライバシーに関わる無線通信の拡大に伴い、それらを保護する仕組みの構築が求められる。
ﾌﾟﾗｲﾊﾞｼｰ保護技術	自己情報ｺﾝﾄﾛｰﾙ権を管理する技術	自己情報をコントロールすることで、プライバシー情報を安全に積極活用する基盤の実現。	現在、プライバシ情報の提供するかしないかというように選択肢が限られているために、情報が有効に活用されていない。医療情報や個人情報を適切にコントロールすることにより、一定のプライバシを保護したまま、情報の有効活用によるメリットを同時に享受することが可能になる。情報を守るだけという発想から、情報の安全な活用という発送で、新たな産業創出の社会基盤として重要な技術である。 「クラウド化・大規模化に伴うセキュリティ技術」、「高度に重要な情報の管理技術」【技戦】を含む。

【技戦】技術戦略専門委員会の委員意見

有識者ヒアリングに基づく重点分野候補(3/3)

研究カテゴリ	重点分野	達成目標 （社会ビジョン）	選定理由
セキュアシステム構築技術	上位レイヤのコンフィグレーションを下位レイヤまで自動的に保証する技術	ソフトウェアのセキュリティを上位層から下位層までトータルに確保する仕組みの確立	システムの上位から下位に渡るトータルのセキュリティを確保できなければ意味が無い。本技術は、トータルのセキュリティ確保の基盤として幅広く利用されることが想定されるため、その波及効果が大きい。 「ディペンダブル情報システムの構築」、「組み込みデバイスのセキュリティパッチ適用スキーム」、「組み込みシステムにおけるセキュリティ」【技戦】を含む。
	アイソレーションとアクセスコントロールを保証する技術	障害を前提として、被害を最小限に食い止めるための仕組みの確立。	従来の延長線上にあるアイソレーションとそれに基づくシステマティックなアクセスコントロールにより、セキュリティ対策のコストパフォーマンスを高めることで、ソフトウェア全体の基盤を確立する。 「BCMにおける情報セキュリティ対応策の策定」【技戦】を含む。
セキュリティ評価・マネジメント	サイバーセキュリティサイエンスの確立	サイバーセキュリティ技術を評価できる体系を確立することで、セキュリティ分野の技術発展の基盤を確立	サイバーセキュリティをサイエンスとして評価できるような体系にしなければ、セキュリティ分野の進展は期待できない。ノウハウ集ではなく研究として評価するためのサイエンスとすることにより、セキュリティの他の分野全般に対して、良い研究と悪い研究を選別することや、適切な普及方法を明らかにすることが可能になる。新たな技術研究の成果を迅速に普及させ、一般に使われているITシステムを少数のスキルの高い攻撃者に対抗できるだけの安全性レベルとするためにも、サイエンスとしての体系化が必要。 「新しい社会システムにおける情報セキュリティのあり方」「ROSIの可視化の研究」」【技戦】を含む。
	サイバーセキュリティ研究のためのデータ基盤の確立	サイバーセキュリティの研究を活性化するために実証研究に使えるデータの基盤を確立する。	理論研究は進展しても、問題となるのは実証研究のためのデータが必要になること。データがなければ研究すらできないテーマもある。実証研究のための基盤づくりは国でなければできないこと。そのために、データを継続的に観測する仕組みが必要になる。例えば、情報処理実態調査におけるセキュリティ評価やマネジメントに関する調査項目の修正や追加をより適切なものとするために、学術研究成果の知見を活用することが考えられる。 「トレースバックのための国際観測拠点の設置とデータ解析」【技戦】を含む。
	セキュリティ部品が正しく実装されていることを保証する製品評価技術	システム設計におけるセキュリティ対策の費用対効果を改善する仕組みの確立。	標準化された評価認証により、システムの部品であるセキュリティ製品を適切に普及させることができる。製品認証は、システム設計の費用対効果を改善する上でも有用である。また、認証制度とそのための基盤を世界に先駆けて具体化することで、我が国の産業競争力の向上につながる。例えば、バイオメトリクスなどがその候補である。

【技戦】技術戦略専門委員会の委員意見