情報セキュリティ研究開発戦略に関する各省取組詳細

※研究開発戦略策定時のヒアリングより

分類	重要テーマ名	概要	推進内容	各省・独法の取組	大学・有識者等（※）
情報通信システム全体のニュー・ディペンダビリティの確保					
①	実世界とコンピュータ内のモデル世界が融合した次世代ネットワークにおける情報セキュリティ基盤技術	リアルとバーチャルが融合した社会システムにおいては、様々なセンサーが家庭や職場に設置され、エネルギー効率の高い社会が実現されると考えられているが、同時に災害発生時の状況把握にも威力を発揮し、安全・安心な社会の実現に寄与することが期待できる。一方、個人が持つスマートフォン等の発信者情報やセンサーからの身体健康情報の漏えいが懸念されるため、それらを保護する仕組みの構築が求められる。 また、このようなセンサーネットワークにおいては、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が見込まれるが、無線通信特有の物理レイヤの部分の情報セキュリティ技術は未だ確立されておらず、利便性と安全性のバランスを考慮した情報セキュリティ基盤の確立が必要である。 このため具体的には、(a)センサーネットワークの情報セキュリティ基盤技術、(b)アドホックネットワークにおける利便性と安全性のバランスを考慮した情報セキュリティ基盤技術等の研究開発を推進する。 なお、スマートフォンに係る情報セキュリティ課題は、端末からのプライバシー情報の漏えい以外にも、端末識別子のなりすましによるスマートフォン用のウェブサイトへの不正アクセスなども想定されるため、スマートフォンの情報セキュリティ基盤の開発を早期に行う必要がある。	(a)センサーネットワークの情報セキュリティ基盤技術の研究開発	「IT活用による生活安全技術を目指し、暗号などのセキュリティ基盤技術やネットでの認証技術の研究等を行う。（産総研）」 「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム（JST）」	慶応義塾大学　笹瀬巌教授 ・アドホックネットワーク（特に無線センサネットワーク）における省電力技術、高電力効率伝送技術、メディアアクセス制御技術、ルーチング・マルチキャスト技術、セキュリティ・プライバシ技術 ・アドホックネットワークに適したPKI、安全な通信の保証・監査
			(b)アドホックネットワークにおける利便性と安全性のバランスを考慮した情報セキュリティ基盤技術等の研究開発		
			(c)スマートフォンの情報セキュリティ基盤の開発		
②	システムのセキュリティ設定を上位から下位まで自動保証する技術	システムのコンポーネント化が進む中、システムの上位層から下位層まで、情報セキュリティの整合性を系統的に保証する情報システムの構築技術が求められている。このため、システムのアーキテクチャに基づいて、情報セキュリティ・ポリシーやコンフィグレーションを管理するフレームワークを開発する。さらに、このフレームワークに基づいて、ポリシーやコンフィグレーションが守られていることを保証するために、形式手法等の技術を活用した自動検証技術の研究開発を推進する。自動検証技術については、米国の情報セキュリティ・オートメーション等の研究動向を踏まえ、海外の成果を活用して研究を進めることが求められる。 また、IPv6への移行に伴う情報セキュリティ面の懸念は、ネットワーク層の問題だけではなく、上位アプリ層まで含めたトータルの整合性を取ることが必要であり、情報セキュリティ・ポリシーやコンフィグレーションを管理するフレームワークの一環として研究開発を推進する。	(a)情報セキュリティ・ポリシーやコンフィグレーションを管理するフレームワーク開発	「適材適所にセキュリティ技術を自動選択し、セキュアなネットワークを最適に構成するためのセキュリティアーキテクチャの研究開発（NICT）」	
			(b)形式手法等の技術を活用した自動検証技術の研究開発	「情報基盤における安全性や信頼性の確立を目指し、形式手法を利用した基幹ソフトウェアのセキュリティ評価技術等の研究開発を行う。（産総研）」	
③	障害に対する自動回復可能なコンピュータネットワーク構築技術	緊急に対応が必要な局面において指示系統を構成する通信基盤が失われると壊滅的な状況が生じることになる。一方、想定を超える災害、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であり、ネットワークの障害をゼロにすることはできないという前提に立ちつつ、ネットワークサービスを止めないようにする為の仕組み（自己治癒型ネットワークの構築技術）を開発する必要がある。 具体的には、ネットワークの仮想化技術などを用いて、ネットワーク通信方式の多様性や冗長性を高めることで、サイバー攻撃などによる障害への耐性を高めたダイバーシティ・ネットワーク・アーキテクチャの研究開発を推進する。 また、ネットワークの多様性や冗長性を活用して、障害が発生した場合の自己治癒機能の研究開発を推進する。この研究には、他の重要テーマである「大規模ネットワークにおける広域観測技術とマルウェアの挙動分析技術の統合」の成果も活用し、攻撃に対しても即応できる治癒機能を開発する。	(a)ダイバーシティ・ネットワーク・アーキテクチャの研究開発	「新世代ネットワークのセキュリティアーキテクチャの実現（NICT）」	倉敷芸術科学大学　小林和真教授 ・トラヒック分散技術（CDN：Contents Delivery Service/CDS：Contents Distribution Network） ・仮想化ネットワーク運用技術 ・ダイバーシティ・ネットワーク
			(b)自己治癒型ネットワークの構築技術		
④	生体情報をコンピュータで管理するためのID管理と生体情報を統合するシステム設計構築技術	リアルとバーチャルが融合した社会システムにおいて、リアルの人間をコンピュータ内に取り込む場合、バイオメトリクス情報とID管理の統合が必要になる。バイオメトリクス分野の要素技術は性能面で成熟しており、これからの研究開発テーマとしては、バイオメトリクスを含むオープンなID管理システム・アーキテクチャの設計及び、当該システム・アーキテクチャの標準化、SAML（Security Assertion Markup Language）等による認証システムとの統合技術が求められている。これは、例えば入国審査システム等にも適用されうるものである。 また、日本はバイオメトリクスの要素技術に強みを持っており、この強みを維持するためにも、統合システムの部品となるバイオメトリクス認証技術の適合性評価を行う国際的なフレームワークにおいて、イニシアチブを取ることが望ましい。 具体的には、OpenID をベースとしたミドルウェア・アーキテクチャの開発、SAML等を活用してバイオメトリック・デバイスとのインタフェースやプロトコルを開発する必要がある。また、統合システムの部品となるバイオメトリクス認証技術の適合性評価を行う国際的なフレームワークを構築する。さらに、ISOの国際標準化を想定し、事前に国内の関係者などとの調整及び新作業項目（NP: New Work Item Proposal）の提案取りまとめを行う。	(a)OpenID をベースとしたミドルウェア・アーキテクチャの開発	「ITによる生活安全技術：安全な社会生活の実現をIT技術で支援するため、消費者情報保護のための情報セキュリティ技術の開発を行う。（産総研）」	産業技術大学院大学　瀬戸洋一教授 ・個人認証における安全性強化技術 ・プライバシー影響評価手法 ・国際標準と産業力強化に関する政策
			(b)SAML等を活用してバイオメトリック・デバイスとのインタフェースやプロトコルを開発		
			(c)バイオメトリクス認証技術の適合性評価を行う国際的なフレームワークの構築		

※研究開発戦略策定時のヒアリングより

分類	重要テーマ名	概要	推進内容	各省・独法の取組	大学・有識者等（※）
攻撃者の行動分析に基づくゼロデイ・ディフェンス					
⑤	攻撃者の行動分析等による予防基盤技術	現在のインターネット環境は攻撃者に有利な状況であり、攻撃に対する後追い対策では、対策コストの増大を抑えることができない。このため、米国においては、攻撃者に有利な状況を打開するための研究開発を緊急の課題として進めており、我が国においても早急に取り組むことが期待されている。 具体的には、情報漏えいを起こす内部攻撃者やネットワークを介した外部攻撃者の行動観測によるプロファイリング、インセンティブやゲーム理論に基づく行動モデルの分析により、攻撃の公算や影響を予測し、対策の最適化を行う技術の研究開発を推進する。	(a)情報漏えいを起こす内部攻撃者やネットワークを介した外部攻撃者の行動観測によるプロファイリング	「実践的サイバーセキュリティ技術の確立（NICT）」	
			(b)攻撃者の行動モデル分析により、攻撃の公算や影響を予測し、対策の最適化を行う技術の研究開発	「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）」	
⑥	大規模ネットワークにおける広域観測技術とマルウェアの挙動分析技術の統合	スマートフォンの爆発的な普及やスマートフォンを狙ったウイルスの登場、更にはWebやSNS等を用いた新たなサイバー攻撃の増加によって、パンデミックなネットワーク障害のリスクが高まっている。このため、従来行われてきた「人」による監視と対応には限界がくるため、Web等の観測・分析技術、マルウェアの自動検知技術及び自動対処技術（トラフィックの制御など）が必要不可欠になってくる。これには、IPv6に対応した広大なアドレス空間を効率的に観測する技術の研究開発が必要である。 また、異常を検知した際に、自動的にトラフィックを制御する技術の開発も必要となる。 なお、近年のサイバー攻撃は、防護システムを回避するように巧みに設計されたものとなっているため、マルウェアの挙動分析においては、攻撃者から観測ネットワークの存在を察知されないシステムの開発も必要となる。	(a)広大なアドレス空間を効率的に観測する技術の研究開発	「広域の攻撃観測とマルウェアの解析、さらにそれらを統合するサイバーセキュリティ技術の研究開発（NICT）」	JPCERT/CC 鈴木博信様
			(b)マルウェアの自動検知技術及び自動対処技術（トラフィックの制御など）	「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）」	
			分類不可	「実践的サイバーセキュリティ技術の確立（NICT）」：Web等の観測・分析技術	

※研究開発戦略策定時のヒアリングより

分類	重要テーマ名	概要	推進内容	各省・独法の取組	大学・有識者等（※）
個人情報等の柔軟管理の実現					
⑦	個人情報等の利活用を促進する自己情報の統制技術	現在は、プライバシー情報を提供するか、提供しないかという二者択一であるため、プライバシー情報を有効活用することが難しい。プライバシー情報を適切にコントロールすることができれば、情報の有効活用によるメリットを享受することが可能になる。 例えば、位置情報やライフログなどのプライバシー情報を適切に利用するためには、利用者ごとにプライバシー保護レベルやポリシーを柔軟に設定するシステムの開発、プライバシーを保護したまま有用なデータを計算するための秘密計算、プライバシー保護データマイニング等の基礎的研究を行う必要がある。 また、医療情報など特に機微な情報の活用については、社会環境に即した法制度の検討、業界における合意の形成や、医療情報システムと連携したデータ活用の技術開発を進める必要がある。 なお、新しいビジネスモデルとして注目を集めているクラウドにおいてもプライバシー情報の漏えいが情報セキュリティ上の大きな課題であり、クラウドに係わる他の情報セキュリティ課題についても研究開発を推進する。	(a)利用者ごとにプライバシー保護レベルやポリシーを柔軟に設定するシステムの開発	「災害に備えたクラウド移行促進セキュリティ技術の研究開発（旧：クラウド対応型セキュリティ技術の研究開発）（総務省）」 「適材適所にセキュリティ技術を自動選択し、セキュアなネットワークを最適に構成するためのセキュリティアーキテクチャの研究開発（NICT）」 「ITによる生活安全技術：消費者の情報や権利を保護するための情報セキュリティ対策技術（産総研）」	筑波大学　佐久間淳准教授 個人情報の保護と活用を両立させるためのプライバシー保護データマイニング技術の研究、時空間情報・ネットワークマイニング技術の研究
			(b)プライバシーを保護したまま有用なデータを計算するための秘密計算	「災害に備えたクラウド移行促進セキュリティ技術の研究開発（旧：クラウド対応型セキュリティ技術の研究開発）（総務省）」	
			(c)プライバシー保護データマイニング等の基礎的研究		
			(d)クラウドに係わる情報セキュリティ課題の研究開発	「災害に備えたクラウド移行促進セキュリティ技術の研究開発（旧：クラウド対応型セキュリティ技術の研究開発）（総務省）」	
			分類不可	「新世代情報セキュリティ研究開発事業（アクセス制御、クラウド）（経産省：H24終了予定）」	
⑧	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	個人にとってプライバシー情報の漏えいが大きな問題であると同じように、政府にとっては、国家機密の情報漏えいや知的財産の国外流出が発生することは大きな問題であり、これらを防止するために早急な技術開発が求められている。ネットワークを介した情報漏えい事件が増加傾向にあることから、漏えい先を突き止めるためのネットワーク・トレースバックや、情報の改ざんや情報漏えいに関与したものを特定するための証拠データの収集技術が必要とされている。 具体的には、(a)リアルタイムの証拠データの保全・調査、(b)ネットワーク・フォレンジック(c)証拠データの信頼性評価などの研究課題がある。ネットワーク・フォレンジックで扱うデータ量は極めて大きくなるため、データの収集・解析を効率的に行うための研究が必要となる。	(a)リアルタイムの証拠データの保全・調査技術	「適材適所にセキュリティ技術を自動選択し、セキュアなネットワークを最適に構成するためのセキュリティアーキテクチャの研究開発（NICT）」	
			(b)ネットワーク・フォレンジック（大容量データの収集・解析を効率的に行うための研究）		
			(c)証拠データの信頼性評価などの研究		
⑨	ITリスクに関する理論から実務までの体系化	大きな災害が発生すると、リスクに対する社会のとらえ方が変化する（例えば、平常時にプライバシー情報がネットに公開されると問題であるが、災害時には安否確認が優先される）。さらに、災害復興に向かう過程では、多様な価値観が混在するため、許容されるリスクを調整するリスク・コミュニケーションの仕組み等が重要となる。 また、社会基盤を支える重要インフラシステムの中核にはリスク・マネジメントが不可欠であるが、リスクは益々複雑化しており、1つのリスク対策が別のリスクを生む原因になることがある。 このため具体的には、(a)リスク対リスクを回避するための手段の研究、(b)複数の関係者間で合意を得るためのコミュニケーション手段の研究、(c)対策の最適な組み合わせを求めるシステムを開発する必要がある。	(a)リスク対リスクを回避するための手段の研究		東京電機大学　佐々木良一教授 (a)リスク対リスクを回避するための手段の研究 (b)複数の関係者間で合意を得るためのコミュニケーション手段の研究 (c)対策の最適な組み合わせを求めるシステムの開発 を推進
			(b)複数の関係者間で合意を得るためのコミュニケーション手段の研究		
			(c)対策の最適な組み合わせを求めるシステムを開発する		

※研究開発戦略策定時のヒアリングより

分類	重要テーマ名	概要	推進内容	各省・独法の取組	大学・有識者等（※）
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	情報セキュリティ研究の基盤体系化	情報セキュリティの研究開発を対策の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必要がある。また、理論研究が正しいことを確認するためには、実証研究のためのデータが必要となり、データを継続的に観測する仕組みも必要になる。 サイバーセキュリティ研究の活性化の基盤として、(a)サイバーセキュリティ研究の科学的な評価フレームワークの確立、(b)実証研究のためのデータ基盤の整備が必要になる。(a)については、脅威やリスクの評価手法、技術の効果の評価手法、科学的に評価体系を研究開発する必要がある。(b)については、データ整備が必要なものの洗い出し、各データ構成の設計、データ提供システムの研究開発が必要になる。	(a)サイバーセキュリティ研究の科学的な評価フレームワークの確立	「情報基盤における安全性や信頼性の確立（産総研）」	東京大学　松浦幹太准教授 ソーシャルクリプト（社会と情報通信システムの相互作用に関わる情報セキュリティ技術およびその設計・運用態様やそのあり方、それらの実効性に影響する施策設計手法のための総合科学）の研究
			(b)実証研究のためのデータ基盤の整備	「マルウェア検体や攻撃トラフィック等のセキュリティ情報を安全に研究利用するためのサイバーセキュリティ研究基盤（NONSTOP）の研究開発（NICT）」	
⑪	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認証技術	ソフトウェアの品質評価手法、及びソフトウェア品質の属性（セキュリティ、安全性、信頼性等）に与える影響に基づいた欠陥の特性解析が必要である。情報システムの構成要素であるセキュリティ部品の品質評価の基準が標準化されていれば、セキュリティの要求に合った適切なセキュリティ製品を使ってシステムを構成することが可能になる。これは、セキュリティ対策の費用対効果を改善する上でも有用である。また、品質評価に基づく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は、我が国の産業競争力の向上にもつながる。 具体的には、(a)セキュリティ製品のセキュリティレベルを評価するための基準設計、(b)セキュリティ製品の組み合わせ方の正当性を評価する手法、(c)評価プロセスの標準化などが必要になる。	(a)セキュリティ製品のセキュリティレベルを評価するための基準設計	「適材適所にセキュリティ技術を自動選択する技術の一環として、セキュリティ技術の組み合わせ方の正当性を評価する手法の研究開発及びプロセスのISOにおける標準化（NICT）」	
			(b)セキュリティ製品の組み合わせ方の正当性を評価する手法の開発	「情報基盤における安全性や信頼性の確立（産総研）」	
			(c)評価プロセスの標準化	「アーキテクチャ安全性評価技術の確立（NICT）」	
			分類不可	「高度大規模半導体集積回路セキュリティ評価技術開発事業(経産省)」	
⑫	情報理論的安全性を備えた暗号技術	情報理論的に安全な暗号技術は、従来主流の計算量的暗号技術に対比される技術である。近年、重要インフラの制御システムを狙ったマルウェアが登場しており、制御システムのセキュリティ対策の必要性が高まっている。DES,RSAなどの計算量的な暗号技術の場合、計算機の処理速度の向上に伴う危殆化の問題が付きまとう為、制御システムの稼働期間（十数年の長期）に渡って、安全性を保障することはできない。 また、センサー機能を持った組込み機器が家庭やオフィスに配置され、ネットワークに接続されるようになってきており、組込み機器のセキュリティ対策が求められている。情報理論的な暗号は、線形演算で構成でき高速処理が可能となるため、計算資源の小さい組み込みシステムへの適用が可能と考えられる。 情報理論的に安全な暗号技術を実用化するためには、組込みシステムへの導入に関する研究も重要となる。車載コンピュータ、制御系コンピュータ、電力システムなど、システムごとにリソースやリアルタイム性の制約を考慮した方式の研究開発が必要である。 また、情報理論的に安全な暗号技術の1つである量子暗号技術では、大きな秘密鍵を事前に共有する仕組みが重要となり、その手段として量子通信等が有望とされている。特定環境における量子通信の実現は、10～20年程度の研究課題とされており、国際的な成果も活用して推進することが効率的である。	(a)情報理論的に安全な暗号技術の研究	「現代暗号と量子ICTを組み合わせて新たな秘匿通信システムを実現する量子セキュリティ技術の研究開発（NICT）」	横浜国立大学　松本勉教授 情報ハイディング（通信していること自体を隠すステガノグラフィ技術、データや装置に追跡性を付与するフィンガープリンティング技術における、理論的に優れ実用性もある方式や解析手法）の研究
			(b)リソースやリアルタイム性の制約を考慮した方式の研究開発		

※研究開発戦略策定時のヒアリングより

分類	重要テーマ名	概要	推進内容	各省・独法の取組	大学・有識者等（※）
震災からの復旧・復興、新たな成長に寄与する研究開発					
⑬	耐災害性の高い情報通信システムの構築	情報連絡・共有の困難化、サプライチェーン崩壊等が問題となった。耐災害性の高いシステムの再構築、バックアップや分散化等に対応した事業継続計画（BCP）の見直しが不可欠。	耐災害性の高いシステムの再構築、バックアップや分散化等に対応した事業継続計画（BCP）の見直しに係る研究開発	②、③の研究に関連することを想定	
⑭	リスク・マネジメント等	災害発生時には、最適な対応を行うための「ダイナミック・リスク対応」の観点が必要。また、リスク・コミュニケーションの観点から情報の伝達、情報のコントロールを検討しておく必要がある。	災害発生時における情報の伝達、情報のコントロールに係る研究	⑨の研究に関連することを想定	
⑮	個人情報等の柔軟管理	一度インターネットに流出した情報の回収における困難性を鑑み、平時から災害時に備え、個人情報等を適切にコントロールする研究開発を進めておくことが望ましい。	個人情報等を適切にコントロールする研究開発	⑦の研究に関連することを想定	
⑯	ニュー・ディペンダビリティ	社会の情報システムへの依存度が増す中、ダイバーシティ・ネットワークや、上位から下位までセキュリティの整合性を保証するシステム構築技術が求められている。	ダイバーシティ・ネットワークや、上位から下位までセキュリティの整合性を保証するシステム構築技術の研究開発	②、③の研究に関連することを想定	