参考資料２

情報セキュリティ研究開発戦略の重要分野の具体化（案）

「情報セキュリティ研究開発戦略」に掲げられる重要分野の各分野について、問題認識、期待効果、要素課題について以下のように具体化する。

- 問題認識
  重要分野に係る現状や環境に関する問題認識や解決すべき課題などを示し、重要分野の重要性や必要性を明確にする。
- 期待効果
  重要分野の研究開発への取組みにより問題や課題が解決されることにより期待される効果を示す。
- 要素課題
  重要分野の課題を達成するために求められる要素課題を具体化する。

重要分野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

■問題認識

近年、自動車の電子制御化、家電のネットワーク化、ビルや都市環境のセンサー情報に基づく制御管理など実世界の様々なシステムと情報システムの融合が急速に進んでいる。このような物理システムと情報システムが融合した将来社会のシステムにおいては、実世界からのセンサーデータなどが情報システムにより処理され、実世界の物理システムの動作に直接影響を与えるため、ネットワーク上でやり取りされるデータの完全性や通信の信頼性が失われると、最悪、人命や身体に深刻な影響を与える危険性がある。

一方、センサーによる身体健康データや、スマートフォン、SNS などで扱われる個人情報などがネットワークを介したアプリケーションにおいて利活用が進むなど、扱われる情報の内容も多様化している。セキュリティ対策技術が確立されていないセンサーネットワークや無線アドホックネットワークを用いて、身体健康情報や位置情報などの機微情報が送受信されると、それらが漏洩した場合の影響が深刻となるリスクをはらんでいる。

■期待効果

物理システムと情報システムが融合した社会システムにおいて利用される制御情報やセンサーデータの機密性や完全性が確保されれば、このような社会システムを、安心して利用することができるようになる。

また、身体健康データやライフログなど機微情報を含む通信のセキュリティを確保することができれば、健康や生活の質向上につながるシステムやサービスを安心して利用することが可能となる。

■要素課題

要素課題	内容と達成目標	達成時期
(1) 仮想化技術を用いたシステム及びネットワークによるセキュリティ基盤の確立	仮想化技術を用いた、柔軟で、独立性の高いシームレスなシステム及びネットワークにおいて必要なセキュリティ機能を実現し、制御データ、身体健康データなどの情報の完全性、機密性等に対する要求水準を満たす。	既存の仮想化ネットワーク技術を対象として 2015 年までに基本機能を実現し、その後、センサーネットワークや無線ネットワークを含めた新世代ネットワーク向けの機能を 2020 年頃までに実現する。
(2) センサーネットワークの情報セキュリティ基盤の確立	小型センサーなどリソースの限られたセンサーネットワークにおいて必要なセキュリティ機能を適切なレベルで確保するための基盤を確立することで、社会システムにおけるセンサーネットワークのセキュリティを確保する。	2015 年までに、基本技術を確立し、その後 2020 年までに実用化技術を確立する。
(3) アドホックネットワークの情報セキュリティ基盤の確立	Bluetooth、車車間・車内通信、無線アドホックネットワークなど動的に構成される局所ネットワークの利便性を享受しつつ、必要なセキュリティ要件を確保するための基盤を確立する。	移動体通信等の既存技術に関するセキュリティ基盤を 2015 年までに実現し、2020 年までに異なるアドホックネットワークを統合した新世代ネットワークにおけるセキュリティ基盤を実現する。
(4) スマートフォンの情報セキュリティ基盤の開発	個人情報、位置情報、センサー情報など様々な情報を用いたスマートフォンのアプリケーションやサービスにおいて必要なセキュリティ機能を実現する基盤を開発する。具体的には、スマートフォンのアプリやネットワーク通信に係るセキュリティを確保するための共通基盤を開発する。	2013 年までに、現在実用化されているスマートフォンに適用可能なセキュリティ技術を確立する。2017 年までに、次世代のスマートフォンにおける統合的なセキュリティ基盤を実現する。

重要分野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

■問題認識

複雑化するシステムや、構成が進化するシステムにおいては、ユーザの計算資源へのアクセス権限やシステムの脆弱性に対する更新管理などがシステム全体に渡って矛盾なく適用されていることを、人手による管理に頼ることは現実的ではなく、システマティックに管理の効率化を行うことが求められる。

一方、多様なユーザにより多くの計算資源（サーバ、ネットワーク、ストレージ等）を共通して利用するシステム環境が増加している。そのような環境において計算資源へのアクセスを制御するOS、ネットワークなどのセキュリティの統合管理が重要となる。そのためには、従来のセキュアOSにおける計算資源のアクセス制御や特権管理を強化したセキュリティポリシーの設定と管理に係わるアーキテクチャを構築し、セキュリティポリシーが適切に設定され、システム全体に渡って確実に反映されていることを保証するための統合管理の仕組みが求められる。

■期待効果

複雑化するシステムや進化するシステムにおいて、システム全体に渡ってセキュリティポリシーが矛盾なく適用されることを、人手に頼ることなく一定レベルで自動検証することが可能となれば、オペレータの負荷を低減できるとともに、システマティックな管理による信頼性の向上が期待できる。

■要素課題

要素課題	内容と達成目標	達成時期
(1) システム構成の変化に対応したセキュリティポリシーの管理フレームワークの構築	階層化、コンポーネント化が進むシステムや、構成の動的な変化に対応して、計算資源とユーザに関するアクセス制御や特権管理を行うための管理フレームワークを開発する。既存のセキュアOSのアクセス制御、特権管理を拡張し、大規模で、動的に変化するシステム構成にも対応できるようにする。	2015年までに各構成において統括的にポリシーを管理する技術を確立する。
(2) システム全体のセキュリティポリシーを自動検証する機構の開発	上記の管理フレームワークに基づくセキュリティポリシーに対して、システム全体がポリシーを満たしていることを自動検証するための仕組みを開発する。そのための方法として、形式手法などの技術を活用して、ポリシーの記述言語と論理検証の処理系を実現する。	(1)の成果を活用し、2014年頃から5年程度で実現する。
(3) 脆弱性データベース等を用いて脆弱性対策情報を入手し、ソフトウェアの更新を効率化する仕様の開発	製品開発者等が提供する脆弱性対策情報等を提供する脆弱性データベース等を活用し、OSのみならず、コンパイラ、ミドルウェア、サービスプロセス等のシステムソフトウェアの脆弱性の対策を効率よく自動処理するための仕様やインタフェースを開発する。	2015年頃までに実現する。

重要分野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

■問題認識

クラウドサービスの普及に伴い、従来の情報システムとは異なる種類のリスクへの対応

が求められるようになっている。クラウドサービスは、マルチテナントを前提としており、共通のリソース（通信機器、電源装置、ミドルウェア、OS 等）を、多数のユーザにより共有することが一般的である。そのような環境においては、仮想化ソフトの多数の複製利用や、共通管理部のハイパーバイザー機能の脆弱性に係るインシデントは、多くのユーザを抱えるサービス全体に波及する。また、共有リソース（通信機器、電源装置、ストレージ等）の障害も、サービス全体に拡大し被害の甚大化を引き起こしている。

一方で、災害、機器の故障、攻撃など様々な事象の発生時に、通信機能が完全に失われることで生命や経済面で深刻な損害にいたることがある。TCP/IP レイヤにおいては、機器の障害等に対する障害回避機能が設計に組込まれているため、一定の範囲で通信機能の喪失を回避することができているが、通信機器、電源、サーバなど様々な階層における自動回復性、障害回避性が実装されていなければ、システム全体としての高度な可用性を実現することはできない。実際、近年、頻繁に発生している携帯電話における通信障害は、このような様々な階層における障害回避性が実現されていれば回避できたものが多い。

■期待効果

通信に係る様々なレイヤにおける多様性、冗長性を持たせ、障害の回避性・復元性を備えた通信アーキテクチャを実現することにより、通信機能の完全な停止を回避し、通信性能は低下しつつも、通信機能を維持することが可能となれば、被害の深刻化を抑えるとともに、利用者に直接影響を及ぼす障害の発生頻度を大幅に低減することが可能となる。

■要素課題

要素課題	内容と達成目標	達成時期
(1) ネットワーク仮想化と計測技術の基盤確立	ネットワークの耐障害性、回復性を実現するために、ネットワーク仮想化技術を用いたネットワーク資源の多様化・冗長化を図る通信方式を開発する。また、仮想化ネットワークやクラウド環境が急速に普及する中、これらに対応したトラフィック計測手法及び障害発生箇所や障害原因を検出する技術を開発する。	現在基礎研究が進められているオーバーレイネットワークや仮想化サーバをベースとして、2015 年までに基本技術を確立し、2020 年頃までに実用化技術を確立する。
(2) 多重化・冗長化ネットワークを活用した自動回復機能の実現	(1)により実現される多様化・冗長化されたネットワーク資源を管理し、障害の原因及び障害箇所に関する情報に基づき、多重化・冗長化されたネットワークを活用した自動回復技術を開発する。また、仮想システム間でプロセス移転を安全かつ迅速に行い、サービス断絶時間を最小化する技術の開発が必要である。	(1)の成果も反映するため 2014 年頃から 5 年程度で達成する。
(3) プログラマブルネットワークの基盤構築	環境の変化や用途の変化に動的に対応したインテリジェントな機能をフレキシブルに組込むためのプログラム可能なネットワーク基盤を構築する。	2015 年までに基本的な方向性を検討し、2020 年までに実用化技術を確立する。

重要分野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

■問題認識

様々なサービスや業務システムの利用において、ID／パスワードによる認証や生体認証等様々なメカニズムが適用されている。様々なシステム間で ID 情報を統合し利用可能とすることにより利用者の利便性が飛躍的に向上することが期待できる。ただし、各認証方式には、それぞれメリット・デメリットが存在し、特に ID／パスワードは、利用者の管理に依存しており漏洩リスクが高いこと、生体認証は、一度、生体情報が漏洩すると変更ができない等の問題がある。このようなことから、様々な認証方式を利用するサービスやシステムを統合する上で、利用者の利便性や管理・運用の効率化のため、それらの一元管理と統合的なセキュリティ管理の実現が重要である。

■期待効果

バイオメトリクスを用いた認証を行い、多数のシステムやサービスにおいて、認証と ID 管理を一元管理することができれば、利用者個人の ID／パスワード管理に依存したアクセス制御に係わるリスクを抑えることができ、また、複数の業務システムやサービスを利用する際のユーザビリティと利用効率の向上が実現される。

■要素課題

要素課題	内容と達成目標	達成時期
(1) ID 統合のための共通仕様の開発	様々なサービスごとに独自に設定される ID を共通化して、個人 ID を統合的に管理できる仕様を開発することで、ID 管理の効率性、セキュリティの向上を達成する。（OpenID などをベースとすることなどが考えられる。） また、個人の認証に加え、機器認証の統合化を実現する。	2015 年頃まで実施する。
(2) 生体情報と ID 管理の統合化のための共通仕様の開発	(1)において共通化した ID 管理のための仕様に対して、その属性情報として生体情報を統合化し管理運用するための共通仕様を開発することで、利用者の利便性と管理・運用者の効率性、セキュリティの向上を達成する。ID 管理の標準としては、生体情報漏洩に対応するためのキャンセラブルバイオメトリクス技術を実用化する。	(1)の成果を反映し 3 年程度で実施する。
(3) 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	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。バイオメトリクスのデータの接続、性能・精度の標準化は進んでいるが、バイオメトリクス認証のセキュリティ評価については十分ではないため、ISO 等の国際標準化を想定し事前に国内の関係者等との調整及び新作業項目の提案取りまとめを行う。	ISO の標準化プロセスに従い 3～4 年程度で実施する。

重要分野⑤ 攻撃者の行動分析等による予防基盤技術

■問題認識

一般に、攻撃者はシステムの脆弱性を 1 つでも見つければ攻撃に成功するが、防御側は、そのような脆弱性をすべてふさがなければセキュリティを確保することができないというサイバー攻撃の非対称性があるため、攻撃者に有利な状況にある。この非対称性は、情報システム・ネットワークに対する社会の依存性が高まるについて顕著になっている。

セキュリティリスクは、防御側のシステムの特性だけではなく、攻撃などの脅威とシステムの関係によって決まるものであり、防御側の技術だけでなく、攻撃側に対する対策技術を組み合わせることが有効である。したがって、情報システムの利便性を追求しつつ、経済的にセキュリティを確保するためには、システム側の防御の強化とともに、脅威の低減についても研究し、双方のバランスから効率的にセキュリティを確保することが重要である。そのために、攻撃者の行動や攻撃手法、インセンティブについて理解を深め、それに応じた防御について考えることが重要である。

■期待効果

攻撃者の行動分析や攻撃の研究により、脅威を予測した防御策の効率的な開発や、攻撃のコストを上げることで攻撃のインセンティブを下げ、脅威を低減するなどの対策が可能となり、経済的にセキュリティを高めることが可能となる。

■要素課題

要素課題	内容と達成目標	達成時期
(1) 攻撃者の行動と攻撃手法の研究	内部犯行、外部からの攻撃等における攻撃者のプロファイリングに基づき、攻撃者の行動モデルと攻撃手法の推定を行い、予測される攻撃に対する防御技術を開発する。	ネットワークプロファイリングをベースとし、予測とその防御策について 2017 年頃までに実現する。
(2) 攻撃者のインセンティブと脅威の低減に関する研究	攻撃の影響度とその防御のコストの関係や、攻撃のインセンティブを低下させるためのコストなどを考慮して、情報セキュリティ経済学等の観点から、適切な防御策の選択を行う手法を開発する。攻撃の採算性を下げる等により、攻撃者のインセンティブを低下させ、セキュリティリスク全体をコントロールする。例えば、防御側のシステムの構成が頻繁に変化し有効な攻撃法の特定コストを増大させる等。	2015 年までに攻撃者のインセンティブ等のモデル理論を確立し、2018 年までにセキュリティリスク全体をコントロールする技術を実現する。

重要分野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

■問題認識

スマートフォン、ネットワークＴＶ、ゲーム機などインターネット接続を前提とした様々な機器が爆発的に普及し、それに伴い、これらの機器を狙った新たなウイルス・攻撃等による大規模被害のリスクが高まっている。特に、従来インターネット接続を想定しない組込みシステム産業ではセキュリティ対策に関する認識や技術が不足し、その結果、これらの新たな組込み機器のセキュリティ対策は極めて不十分である。また、ユーザ層が急速に一般層に拡大したため、ユーザのセキュリティ知識や設定に依存した対策は期待できず、その結果、脆弱性が放置されることにより、インターネット空間の脅威の拡大が緊急の課題となっている。一方で、IPv6 化によるアドレス空間の拡大、モバイル端末による動的 IP 割当、情報システム資源の仮想化・クラウド化により、従来の限定的なアドレス空間における攻撃観測・分析技術では、十分な観測、分析ができず、さらなる脅威増加に直面する状況にある。したがって、これらの新しい ICT 環境のための実効的な脅威検知が必要となり、高精度、かつ迅速な広域攻撃観測・分析技術、及びマルウェア収集挙動分析技術の研究開発が重要となる。

■期待効果

上記にある新たな ICT 環境への変化に適切・迅速に対応するための研究開発（広域攻撃観測・分析技術、及びマルウェア収集挙動分析技術）を実施することにより、上記に掲げた様々な脅威、具体的には、新たな情報機器への攻撃、新機器における脆弱性の放置、新環境における新たな攻撃などの脅威に対向し、これらの攻撃を早期に検知し、高度な分析、及び適切・迅速な対応を実施することが可能となる。さらに、これらの研究開発の成果を実用化することにより、新たな ICT 環境の普及促進を活性化させ、社会生活や産業の幅広い分野における ICT 利活用のメリットが享受できるようになる。

■要素課題

要素課題	内容と達成目標	達成時期
(1) 広域攻撃観測技術（マクロ的分析技術）	IPv6 によるアドレス空間の拡大やモバイル端末による動的 IP 割当など、従来の物理センサーでは対処できなくなりつつあるネットワーク環境に対応するための広域攻撃観測技術を確立する。具体的には、動的な観測対象の変更技術、観測対象の広域化技術、実時間の観測分析技術などを達成する必要があり、例えば、仮想化技術を用いた観測環境を構築し、マクロ的視野で広域かつ動的な観測環境を構築する方法を実現する。	2012 年から 3 年程度で実現する。
(2) マルウェア収集挙動分析技術（ミクロ的分析技術）	脆弱性探索のためのスキャン、権限奪取のためのシェル混入などの挙動の観測・分析だけではなく、その後に混入されるマルウェアに対向するため、マルウェア収集挙動分析技術を確立する。具体的には、ステレス型（収集システムとは気付かれない）の高度マルウェア収集技術、及び迅速なマルウェア挙動解析技術などを達成する必要があり、例えば、動的 IP を用いた環境変動型の収集システム、マルウェア静的解析、短期・長期動的解析、及び解析結果による駆除ツール自動生成などの技術を確立し、攻撃をミクロ的にみた総合分析を実施する。	2012 年から 3 年程度で実現する。
(3) 広域攻撃観測とマルウェア収集挙動分析を用いた統合解析技術	広域攻撃観測及びマルウェア収集挙動分析等を統合することにより、広域なインターネット環境における攻撃状況とマルウェアの関係の実時間分析を可能とする統合解析技術を確立する。具体的には、現状の攻撃増加と関連するマルウェアの把握、攻撃側（ボットハーダー等）が保有している感染端末のクラスタリング、新たなマルウェアにつながる予兆攻撃の導出など、広域攻撃観測とマルウェア収集挙動分析を有機的に組み合わせ、高精度な攻撃状況把握、近未来の予兆攻撃の導出、及び防御対策の自動化などに関わる研究開発を実施する。	(1),(2)の成果も反映するため 2017 年に達成する。

重要分野⑦ 個人情報等の利活用を促進する自己情報の統制技術

■問題認識

プライバシー情報の保護や利活用に対する考え方は個人により異なり、一律に決めることができない。モバイル端末による位置情報活用やライフログの共有など、様々なサービスを利用する中で、情報を適切にコントロールし、有効に活用することで、新たなサービスや価値が創出される。

医療情報や市民アンケート情報などの統計情報には有益な情報が含まれていても、プライバシー保護の制約があるために、情報が有効活用されないものが多数存在している。

また、個人レベルでも普及が進むクラウドサービスにおいて、プライバシー保護に対する不安が高まっている。

■期待効果

プライバシー保護レベルを柔軟に設定・管理することができれば、情報を有効に活用した新たなサービスや価値を創出することができる。また、近年のプライバシー保護データマイニング技術の進展により、プライバシーを保護したまま、統計情報から有用な傾向を抽出することが可能になりつつある。

■要素課題

要素課題	内容と達成目標	達成時期
(1) プライバシー保護に関する多様な要求レベルを柔軟に管理する手法の確立	サービスごとに異なるプライバシー保護レベルやポリシーを体系化し、設定管理の容易性や柔軟性を向上させる基盤を開発する。	プライバシー保護の基盤となるため重点的に取組み 2015 年で目星をつける。
(2) プライバシーを保護したまま有用情報を抽出する技術の開発	秘密計算及びプライバシー保護データマイニングの性能や用途に関する制約を解消し、実用的で、幅広い用途に適用可能な技術を開発する。特に、医療分野において有用な医学知見を抽出するために、症例情報の抽出に応用することが期待される。	基礎理論の研究が必要であり 2017 年頃までに達成する。
(3) クラウド環境に係わる情報セキュリティ課題の研究開発	(1)(2)の成果に加え、サーバにおけるプロセス間の情報漏洩等を防止する技術を開発し、クラウド環境のアーキテクチャを考慮して技術を適用する。	実践のための設計であり、2015 年頃までに実現する。

重要分野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

■問題認識

企業活動において情報システムの利用が浸透するに伴い、コンピュータやネットワークに係わる犯罪や事故が増加している。米国においては 2006 年に連邦民事訴訟規則が改正され、e ディスカバリ（電子的証拠の開示）が正式な法手続きとして認められ、電子的に保存されている情報を、適切な場所・適切な方法・適切な手順で管理・保管する体制を築かなければ、法的紛争において不利を強いられる状況が生じつつある。企業活動の国際化に伴い、自己防衛としてのフォレンジック技術を構築する必要がある。近年の国家機密、防衛関連情報の漏洩事故などに際して、事故原因の究明や訴訟防衛のニーズが高まっている。

従来のデータ・フォレンジックではメモリー上に直接展開されるマルウェアに対する証拠保全等ができないため、ネットワーク・フォレンジックの必要性が高まっている。また、近年、企業におけるスマートフォン、タブレット端末等の業務利用の増加に伴い、これらの機器に対するネットワーク・フォレンジックに対するニーズも高まっている。

さらに、企業にとっては、内部犯行や内部統制における手段としてもデジタル・フォレンジック技術に対するニーズが高まっている。

■期待効果

デジタル・フォレンジックの技術整備により、国内外における情報システムに係わる事故や犯罪において、法的紛争に関する不利益、損害を回避することが可能になる。また、内部犯行の抑止、内部統制の手段として、効果が期待できる。

■要素課題

要素課題	内容と達成目標	達成時期
(1) リアルタイム証拠データ保全・分析	スマートフォン、モバイル端末等のデータ及びネットワークを流れるデータについて、一定のタイミングで変更や改竄を防止し、証拠データをリアルタイムで保全する技術を実現する。	2015 年頃までに実現する。
(2) ネットワーク・フォレンジックの実用化	サーバ対象のデータ・フォレンジックでは対応できないインシデントに対応するため、ネットワーク・フォレンジックを開発する。特に、スマートフォン、モバイル端末を含むネットワークトラフィックの記録、攻撃の記録等の機能を実現する。	応用技術の機能実装が中心であり 2015 年頃までに実現する。
(3) 証拠データ全体の信頼性向上・評価技術	内部者を含む複数のログ間の整合性や相関の分析などにより、主張したい事象や証拠データ全体の信憑性の向上や、信頼性の評価を行う技術を実現する。	ネットワーク・フォレンジック技術を反映し、2017 年頃までに実現する。

重要分野⑨ ITリスクに関する理論から実務までの体系化

■問題認識

一般にITサービスの提供企業と利用者など立場の異なるステークホルダーにとってリスクの対立が存在する。これはインターネットの普及やサービスの国際化等、IT サービスが社会に与える影響やリスクが複雑化することにより問題が顕在化する傾向にある。例えば、GoogleMap サービスにおけるプライバシー侵害の問題など、異なるステークホルダー間の対立が増加している。

一方、震災等が発生すると人々の価値観が変化し、リスクの捉え方が変化するなど動的に変化するリスクが存在する。生命や健康に係わるリスク、経済的損失リスク等に関する対立リスクや動的リスクなどリスクは益々複雑化しており、IT リスクを体系的に評価し、リスクを事前に調整することができれば、不必要な紛争に伴うコストの発生を抑えることができると考えられる。

■期待効果

社会の対立リスクや動的リスクに関するリスクコミュニケーションによる調整や合意形成が可能になれば、法的紛争などのコストの発生を回避することができる。

■要素課題

要素課題	内容と達成目標	達成時期
(1) IT リスクの体系化	安全性、信頼性、ユーザビリティ、プライバシーなども含むITリスク全体を体系化し、ステークホルダー間の対立リスク、動的リスクの関係についての理論を確立する。IT リスクの体系化は、米国のリスク評価メトリクスの調査結果なども踏まえて実施する。	継続的に研究が行われ、2013 年に完成見込み。
(2) 動的及び複合リスクの評価・対策モデル	震災等による人々の価値観の変化、アノニマス事件における被害者の反応に応じて変化するリスクなど動的リスクや複合リスクの評価・対策モデルを確立する。このモデルは、リスク評価の専門家が利用するものである。	震災やアノニマス事件など新たな事象に対する実証を経て2017 年に実現する。
(3) 合意形成のためのリスクコミュニケーション手法	対立リスク、動的リスク等の様々なリスクについてコミュニケーションによるリスクの調整、最適化を行う手法を開発する。ISMS 等のセキュリティマネジメントにおいて、対立リスクを考慮した拡張に活用可能である。	(2)の成果を反映し2018 年に実現する。

重要分野⑩ 情報セキュリティ研究の基盤体系化

■問題認識

情報セキュリティの研究開発は、攻撃者や攻撃者が作成したツール等の脅威などに対応する技術を対象とするため、理論モデルの構築が困難な場合が多い。その結果、脅威に対する対処療法的な方法が中心となり、開発された手法の効果測定や研究成果の評価が十分に行われておらず、研究推進の効率性や効果に関する根拠が十分ではなかった。

暗号研究やその他の科学研究分野における理論的なアプローチの導入を推進するとともに、実証データをデータベース化し、研究成果を客観的なデータに基づき評価するための基盤を整備することが求められている。

■期待効果

情報セキュリティの研究開発において、科学的なアプローチを導入することにより、効果の評価を適切に行い、合理的な研究開発の推進につなげることができる。

■要素課題

要素課題	内容と達成目標	達成時期
(1) サイバーセキュリティ研究における科学的アプローチの導入	米国セキュリティサイエンスに関する議論の動向を踏まえ、サイバーセキュリティ研究において、比較検証可能な問題や対象モデルの定義、共通概念の形成、科学的な評価手法の導入方法などについて検討する。	2015 年までに概念モデルを確立し試行する。2019 年頃までに実用レベルでの適用を確立する。
(2) 技術評価のための実証データベースの整備	実証評価が必要な研究の効率化と成果の比較検証の促進のため、マルウェア検体や攻撃ログデータ等と運用レベルに有効な研究に必要なデータ項目等の洗い出しを行い、その上で各データ構成の設計と標準化を行い、データベースのインタフェースやシステム仕様を開発する。	2015 年頃までに基本的な研究データの共有を実現し、2020 年までに汎用的な枠組みに拡張する。

重要分野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

■問題認識

身の回りの様々な機器システムへのソフトウェアの浸透が進むにつれて、ソフトウェアの不具合、セキュリティの脆弱性に係わる事故や被害が増えている。このような状況から、ソフトウェアの品質に関する客観的な評価手法を確立し、品質に対する説明力の向上が強く求められるようになっている。IT 製品、部品などからセキュリティを含むソフトウェア品質を特定し、それらに対して要求される品質が、正しく実装されていることを客観的に示すための基準や手法が明確になっていないため、既存の IT 部品や製品を用いて構築されたシステム全体の正しさやセキュリティを保証できないことが問題となっている。

■期待効果

IT 製品や部品に関するソフトウェア品質やセキュリティ要求を特定し、それらに対する客観的な評価手法を確立し、国際標準として認証制度を構築することにより、認証済みの既存の IT 部品等を用いて構築されるシステム全体の品質やセキュリティを説明することが可能になる。これにより、品質やセキュリティに対する高い保証を確保しつつ、経済的にシステムを構築することが可能になる。

■要素課題

要素課題	内容と達成目標	達成時期
(1) ソフトウェア／ハードウェアのセキュリティ品質を客観的に評価する手法の確立	ソフトウェア及びハードウェアのセキュリティ品質を客観的に評価する枠組み及び手法を確立し、利用者に対して品質に関する説明力を高める。	2015 年頃までに実現する
(2) セキュリティ部品を正しく組み上げる方法の開発	認証されたセキュリティ部品を組み合わせてシステム全体として、セキュリティ要求を満たすように、安全な組み上げ方法を開発する。具体的にはインタフェースの定義方法、入出力の制約条件、部品の組み合わせに関する制約条件等に関する定義方法、検証方法を開発する。開発した手法は普及のため標準化を図る。	2017 年頃までに実現する。

重要分野⑫ 情報理論的安全性を備えた暗号技術

■問題認識

現在広く利用されている AES、RSA などの暗号技術は、計算量的な安全性に基づいている。これらの計算量的暗号技術は、攻撃手法の進歩と計算機性能の向上に伴う危殆化の脅威から逃れられない。よって、これらを利用した、制御系システムをはじめとする多くの長期運用を前提とする組込みシステムは、常に暗号危殆化への対策が必要となる。この課題を抜本的に解決するアプローチとして、情報理論的安全性を備えた実用的な暗号技術の開発が挙げられる。具体的には、守秘や認証などのセキュリティ機能を情報理論的安全性の枠組みにおいて達成する暗号技術の研究開発と、そのような暗号技術を支える量子暗号技術等を用いた鍵管理技術の研究開発と、大量の乱数を効率よく得る技術の研究開発など、チャレンジングな課題の解決が必要である。さらに、情報理論的安全性を備えた暗号技術を使いやすい形で整理し、実用方式を標準化していくことも重要である。

一方、リアルタイム性や過酷な環境における高信頼性や長寿命性への要求が厳しく、計算資源の面での制限も強い機器においては、従来の計算量的安全性に基づく暗号技術が適用できず、その結果、情報セキュリティへのニーズがあるにも関わらず暗号技術の適用が見送られてきた場合が数多く存在する。計算量的安全性の枠組みの中で実装コストの低い方式を開発する努力を継続するとともに、実装コストの点で一般的に有利となりえる情報理論的安全性を備えた暗号技術の実用方式を整備していくことが重要である。

■期待効果

情報理論的に安全でかつ実用的な暗号技術により、暗号危殆化への対策が不要で長期運用が可能な暗号技術が広く使えるようになる。また、情報理論的な暗号技術は、線形演算等で構成でき高速処理が可能となるため、リアルタイム性や過酷な環境における高信頼性や長寿命性への要求が厳しく計算資源の面での制限も強い組込みシステムにおいても、暗号技術を適用することができるようになる。

■要素課題

要素課題	内容と達成目標	達成時期
(1) 情報理論的に安全な暗号技術	守秘や認証などのセキュリティ機能を情報理論的安全性の枠組みにおいて達成する暗号技術の研究開発と、そのような暗号技術を支える鍵管理技術の研究開発と、大量の乱数を効率よく得る技術の研究開発などが必要である。鍵管理については、安全なメモリー保管技術や、通信路の特性を活用した鍵共有技術、量子鍵配送技術などの研究開発が含まれる。さらに、情報理論的安全性を備えた暗号技術を使いやすい形で整理した実用方式の標準化が必要である。	2020 年をめどに、特定用途向けに量子鍵配送を用いた暗号通信の実用化を実現する。その他の情報理論的安全性を備えた暗号技術は基礎研究と位置付け 2020 年に実用可能な暗号方式を実現する。
(2) リソースやリアルタイム性の制約に対応したシステムの開発	センサーや小型組込み機器などの計算資源の限られた機器において線形演算等をベースとした高速処理によりリアルタイム性を確保したシステムを開発する。また、車載コンピュータ、制御系コンピュータなどシステムごとのリソースやリアルタイム性の要件に対応したシステムを開発する。	(1)の実現を前提とするが、それと並行して実装技術を 2020 年頃までに実現する。

1.1.1. 研究開発ロードマップ

前節において検討した「重要分野の具体化」に基づき、重要分野ごとの研究開発ロードマップを図１～３に示す。

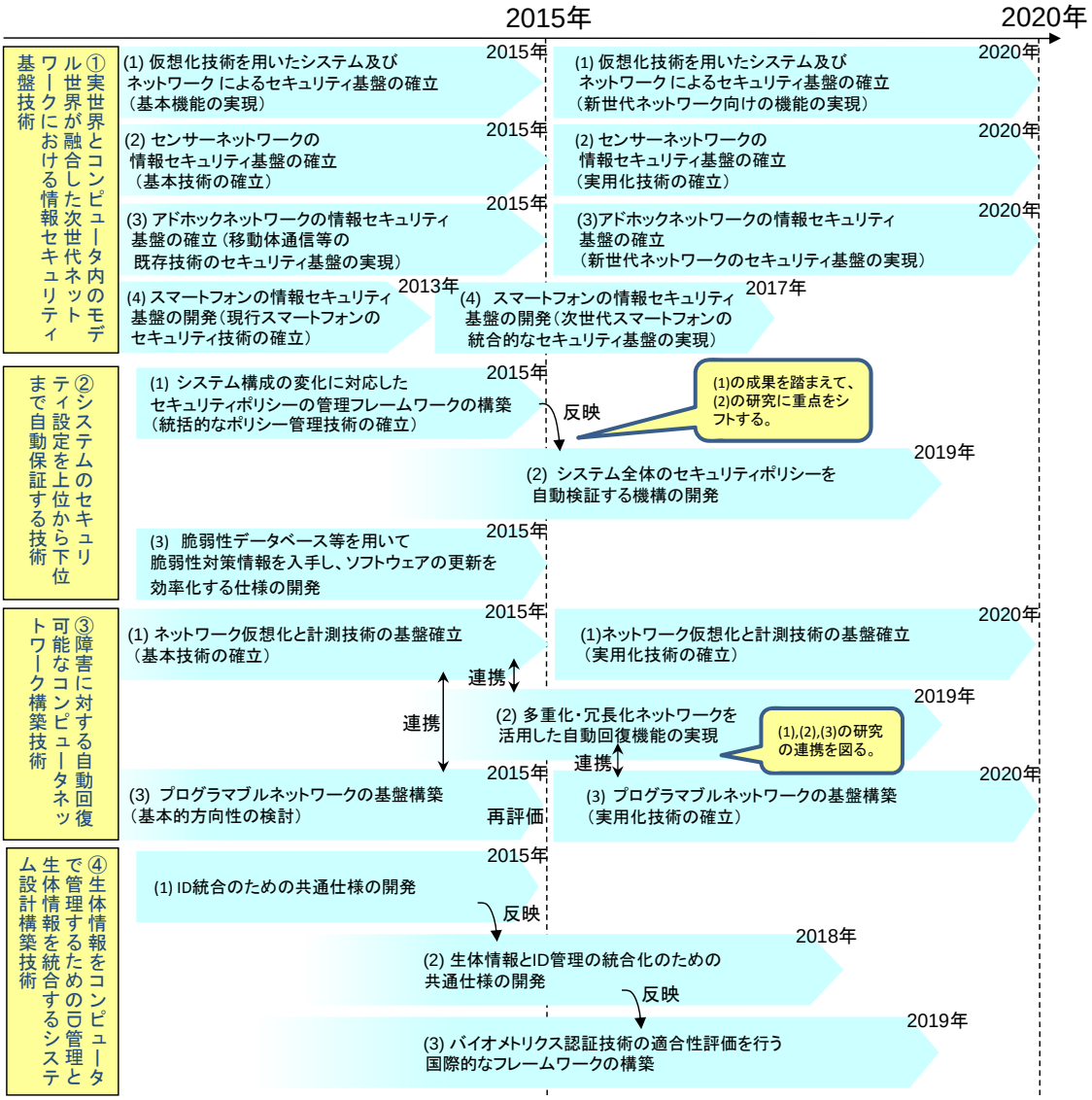

図1 研究開発ロードマップ（1/3）

（ニューディペンダビリティの確保）

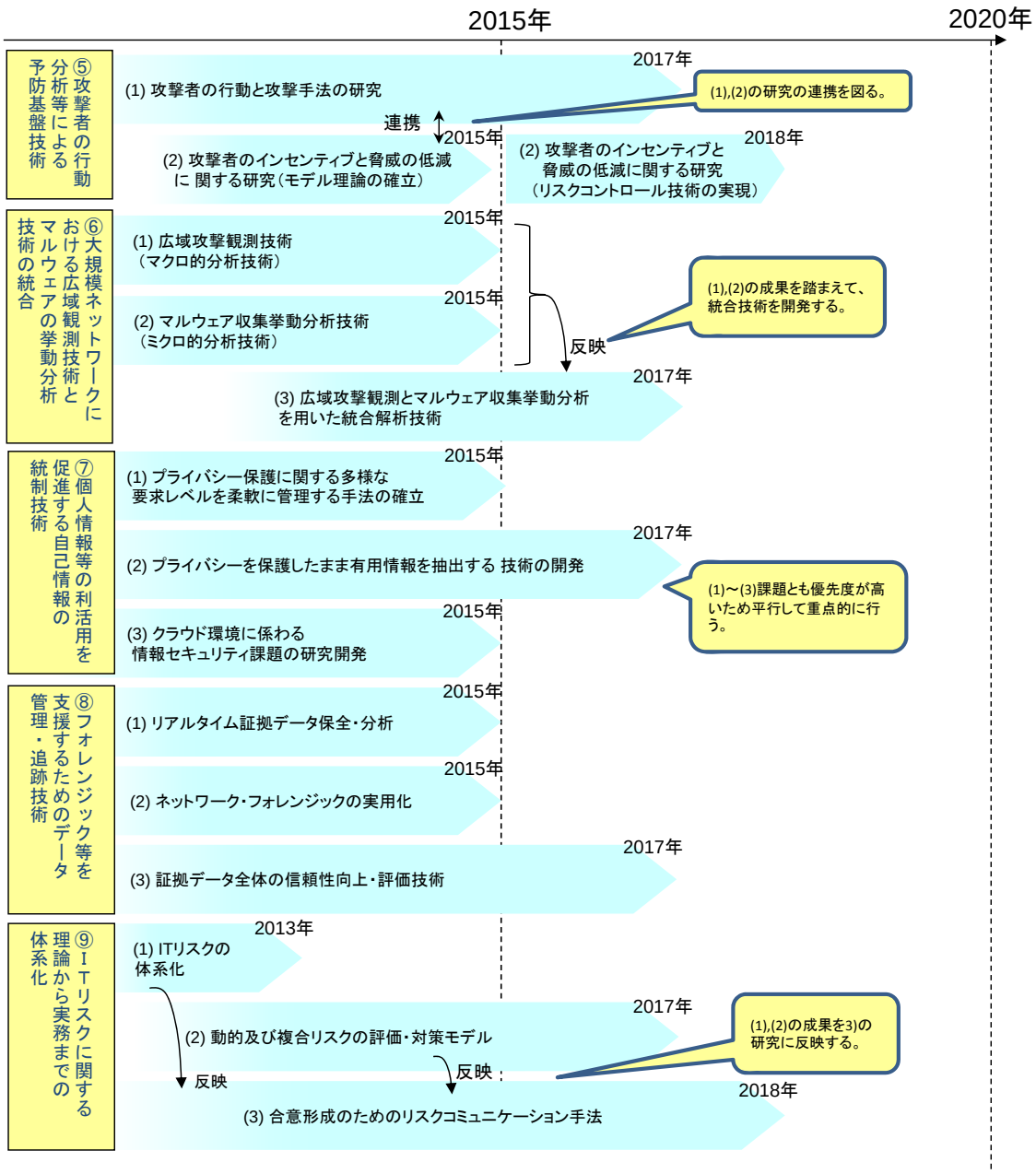

図2　研究開発ロードマップ（2/3）

（ゼロデイ・ディフェンス、柔軟管理の実現）

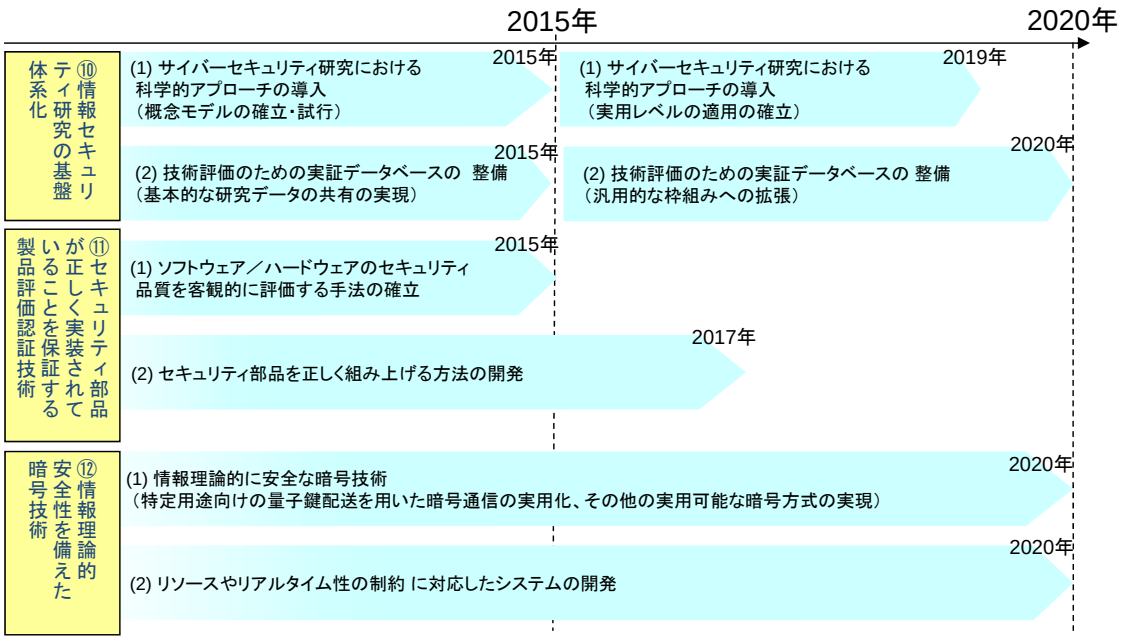

図3 研究開発ロードマップ（3/3）

（研究の促進基盤の確立）