資料１０

NISC National Information Security Center

情報セキュリティの研究開発における政府関与のあり方に関する検討【概要版】

2010年3月9日

内閣官房情報セキュリティセンター（NISC）

http://www.nisc.go.jp/

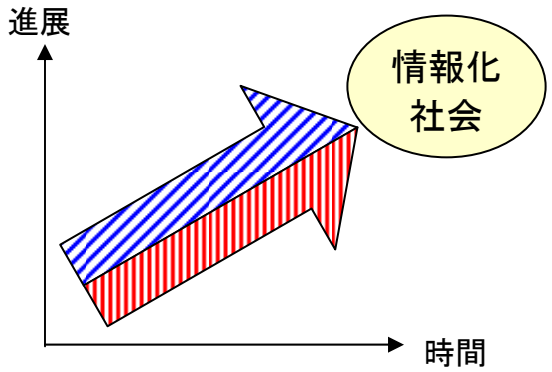
情報セキュリティの研究開発における政府関与のあり方に関する検討（概要1）

●政府関与の必要性

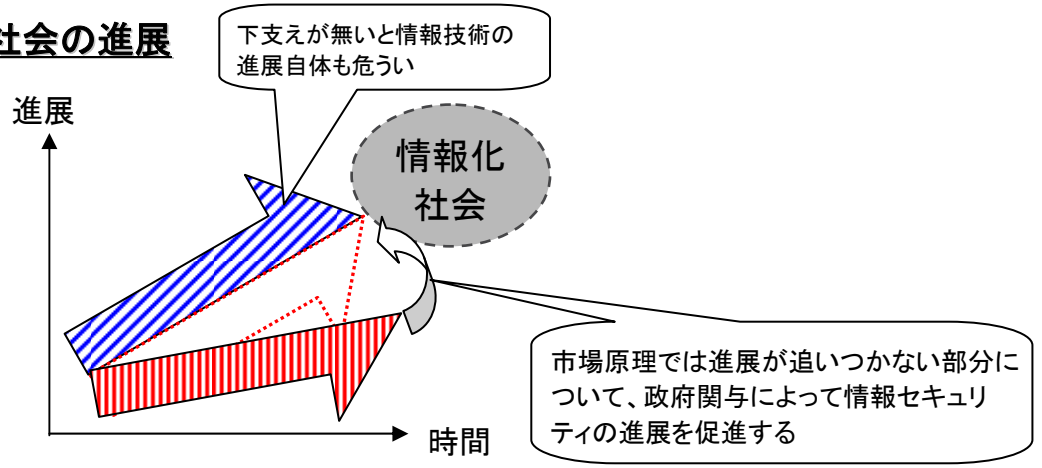
（なぜ、情報セキュリティの研究開発に政府が関与する必要があるのか）

- ITを安心して利用できる環境を提供することは、IT基本法においても明記されている政府の使命であり、情報セキュリティの研究開発は、安心・安全を確保したIT社会の基盤を支えるもの。
- 「情報技術に内在する人為的ミスや信頼性」に係わる情報セキュリティ技術は、情報技術との相関が高いので同期して進展していくべきだが、市場原理に任せておくと過小投資になる傾向がある。
- 情報セキュリティ技術は、第三者への二次被害を防ぐためにも、積極的に普及させていく必要性があり、公共性が高いという特性（広範で一様な適用が必要）を持つ。

健全な情報化社会の進展



情報セキュリティは、情報技術を下支えしながら健全な情報化社会の形成に寄与している



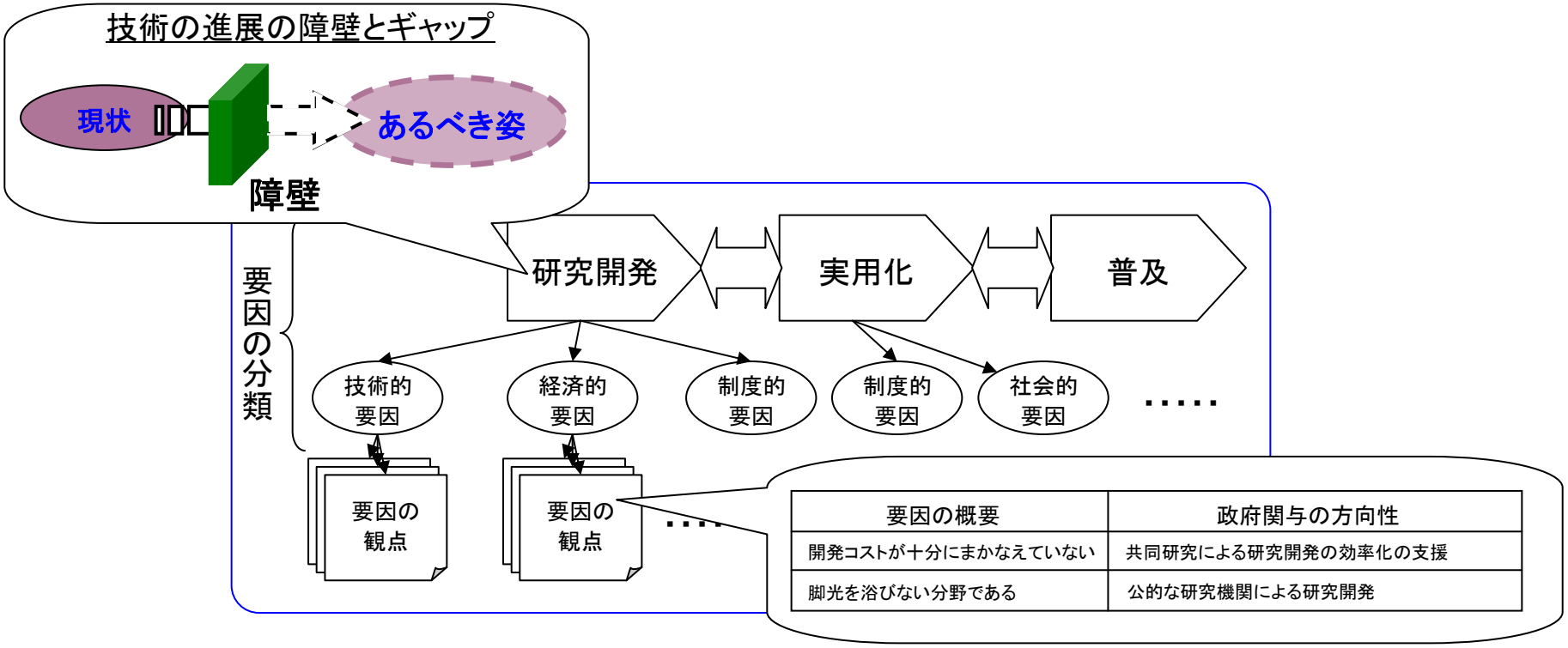
情報セキュリティの進展度が情報技術に追いつかなくなるとリスクが顕在化しやすくなるため、健全な情報化社会を形成できなくなる

情報技術の更なる進展を目指すためには、民間の市場原理と役割分担を行いながら、政府関与によって情報セキュリティの進展を促進するべき。

●政府関与の方向性

（国の規制など非技術的課題によって普及が制約されることもある。資金拠出のみならず様々な観点で政府関与が必要である。）

- 技術開発のサイクル（研究開発→実用化→普及）の段階毎に異なる課題。
- 各段階における障壁は、技術的要因、経済的要因、制度的要因、社会的要因に分類。
- 障害の要因毎に、異なる「政府関与のあり方」が必要。



要因の概要	政府関与の方向性
開発コストが十分にまかなえていない	共同研究による研究開発の効率化の支援
脚光を浴びない分野である	公的な研究機関による研究開発

●サイバーセキュリティ促進パッケージ

（我が国でも統合的なパッケージを作ることが必要）

- 政府は、ステークホルダーが共通の方向に向かう為にビジョンを示すことも必要。
  （例）世界で一番、安全・安心なネット社会を実現

技術マップから抽出された「情報セキュリティ研究・技術開発の重点課題」

- **攻撃への対抗手段の開発に資する研究・技術開発**
  例） 攻撃者をトレースバックする技術　等
- **IT利用者の対応力向上に資する研究・技術開発**
  例） 心理学を利用したフィッシング詐欺対策の研究　等
- **IT技術の発展・普及に伴う情報セキュリティの確保に資する研究・技術開発**
  例） IPv6、クラウド対応のセキュリティ技術開発　等
- **課題の根本解決に資する研究・技術開発**
  例） 情報漏えいの原因を特定する技術開発　等
- **セキュリティを高めたITの実現に資する研究・技術開発**
  例） 開発環境や要件定義の研究　等

米国ではサイバーセキュリティ促進法案により財政支出を強化する動き。

・3カ年の情報セキュリティR&D戦略を政府が策定

・サイバーセキュリティ関係研究開発予算として、5年間で9．6億ドル（約860億円）の資金を確保
（人材育成のための奨学金含む）

NISC National Information Security Center

情報セキュリティの研究開発における政府関与のあり方に関する検討

2010年3月9日

内閣官房情報セキュリティセンター（NISC）

http://www.nisc.go.jp/

政府関与の方向性
【総論】

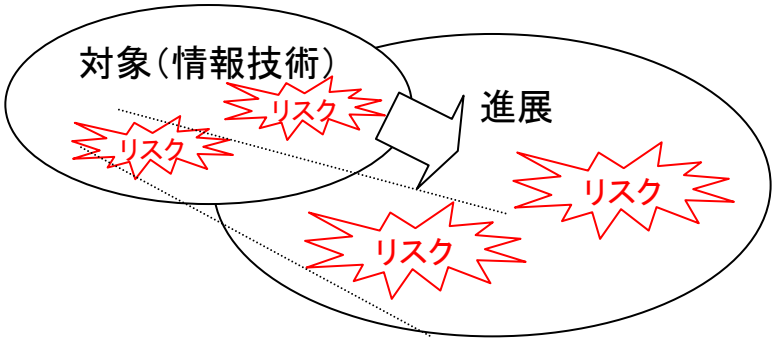
なぜ、情報セキュリティの研究開発に政府が関与する必要があるのか

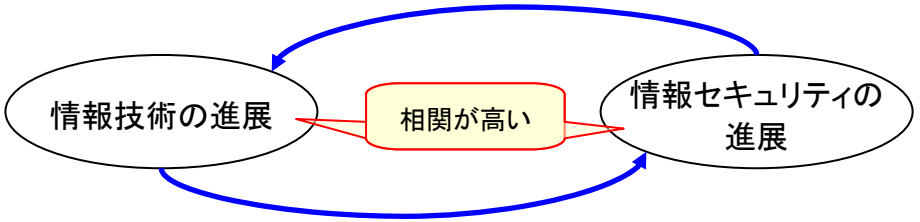
情報セキュリティの特性　～情報セキュリティと情報技術の相関

- 「情報技術に内在する人為的ミスや信頼性」に係わる情報セキュリティ技術は、情報技術との相関が高いので同期して進展していくべき。

情報セキュリティ

情報セキュリティ上のリスクは情報技術に内在するため、適切な対策を行わなければ情報技術の進展（例えば、処理速度の高速化）と供にリスクも増大する



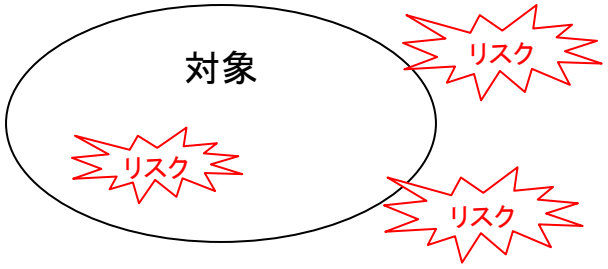


情報セキュリティ上のリスクは情報技術に内在するため、情報技術の進展に同期して情報セキュリティ技術も進展していかなければならない。

対象の安心・安全と高めることと、対象の進展の相関が高い

情報セキュリティ以外（航空機のセキュリティなど）

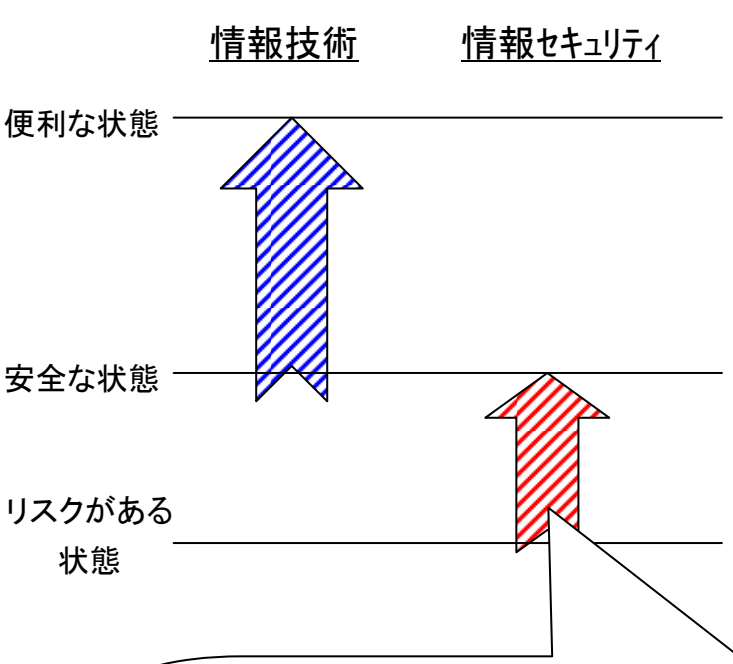
リスクは、対象に内在するもの以外にも多数存在する



例えば、航空機のセキュリティ（安心・安全）は、航空機自体の安全性（材料工学や航空工学が関係）にも依存するが、空港の警備（爆発物検知装置や警備員の配置）等の影響も大きいから、セキュリティ向上のための施策にはバリエーションがある。したがって、対象自体の進展（例えば、高速化）と、対象の安心・安全との相関は比較的小さい。

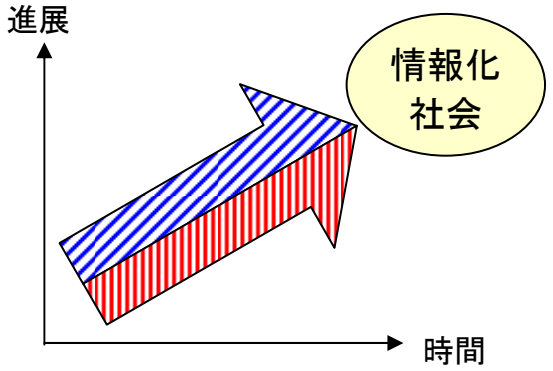
情報セキュリティの特性　～動機的な理由による進展のスピードの違い

- 一般的な情報技術は、利用することによって「便利」「楽しい」「効率的」など特長を持っており、技術開発や普及において進展のインセンティブが働く。
- 情報セキュリティはリスクを軽減するための技術であり、動機的な観点からは情報技術と同じスピードで進展することは困難である。

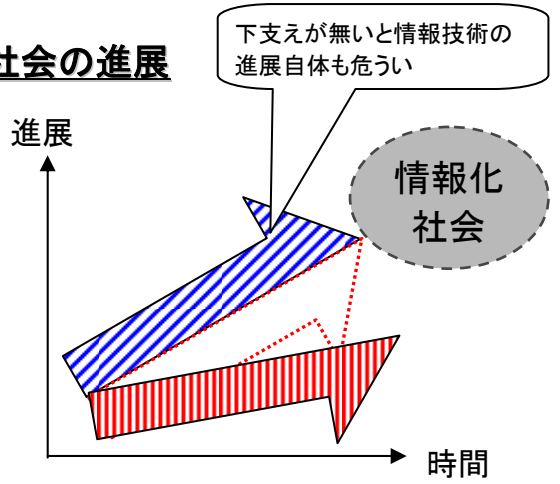


自分自身への被害が顕在化していない段階でコストを負担することや、社会に被害を拡大しないようにするためにコストを負担することに対して、心理的あるいは社会的合意を形成する上での障壁がある。

健全な情報化社会の進展



情報セキュリティは、情報技術を下支えしながら健全な情報化社会の形成に寄与している

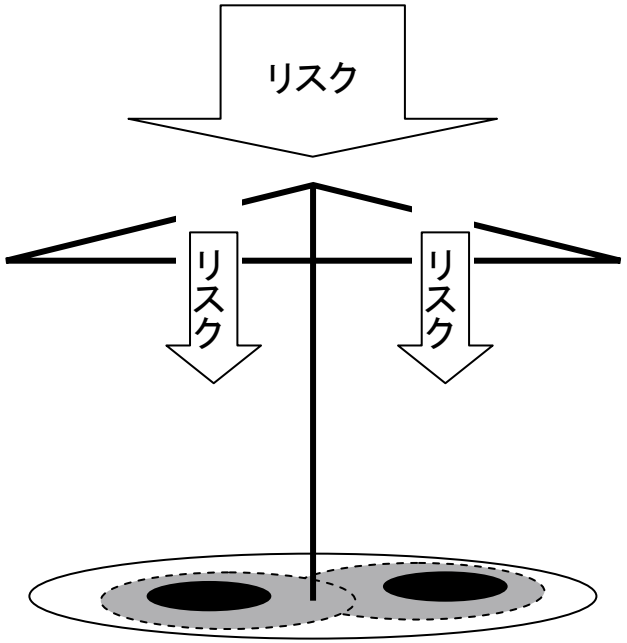


情報セキュリティの進展度が情報技術に追いつかなくなるとリスクが顕在化しやすくなるため、健全な情報化社会を形成できなくなる

情報セキュリティの特性 ～広範で一様な適用が必要

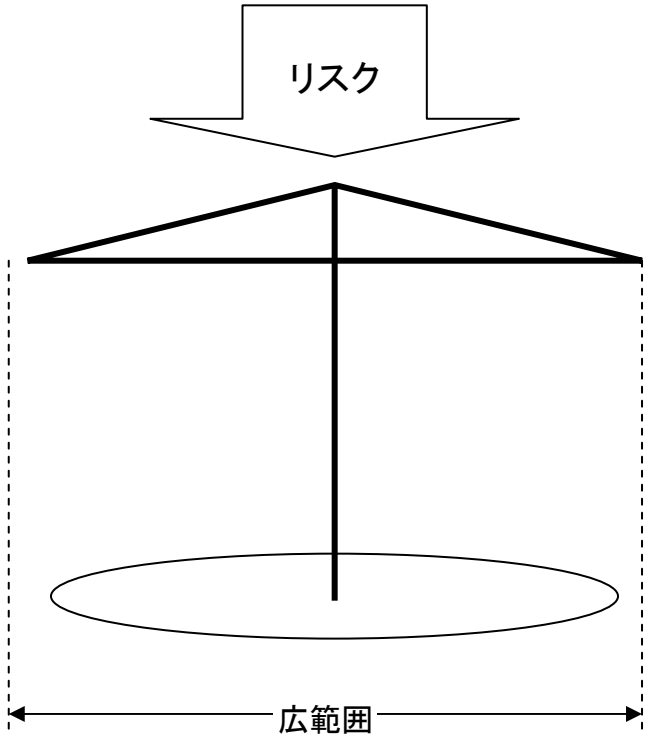
●情報セキュリティは、情報技術に内在する様々なリスクに対応する必要があるため、広範囲にわたって一様に（漏れがないように）適用する必要がある。

情報セキュリティが一様に適用されていない場合



一様に情報セキュリティが適用されないと、リスクが顕在化してしまうことに加えて、その脅威が伝搬して全体のセキュリティの低下が懸念される場面が多い

情報セキュリティが一様に適用されている場合



個人のレベルを超えて、国内全部または世界全体での適用が必要な場面もある

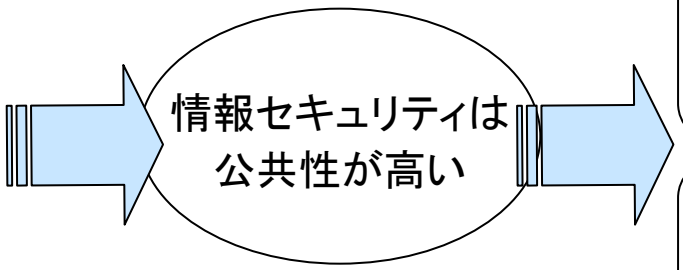
政府関与の総論

ITを安心して利用できる環境を提供することは、IT基本法においても明記されている政府の使命

「情報技術に内在する人為的ミスや信頼性」に係わる情報セキュリティ技術は、情報技術との相関が高いので同期して進展していくべき

主にモチベーションを原因として
情報セキュリティの研究開発に対する
過少投資が発生しやすい

情報セキュリティは、穴が残ってはいけないため、誰でも使えるようにすることが必要　→　対価を伴わない利用を許容する必要性



発展や普及を民間の市場原理のみに委ねるわけにはいかない

利害関係や権利・自由の制約が生じる場合があり、民間では調整が困難な側面がある

リスクをコントロールしながら情報技術の更なる進展を目指すためには、市場と役割分担を行いながら、政府関与によって情報セキュリティの進展を促進するべき

政府関与の方向性
【各論】

具体的にどのような関与が必要なのか

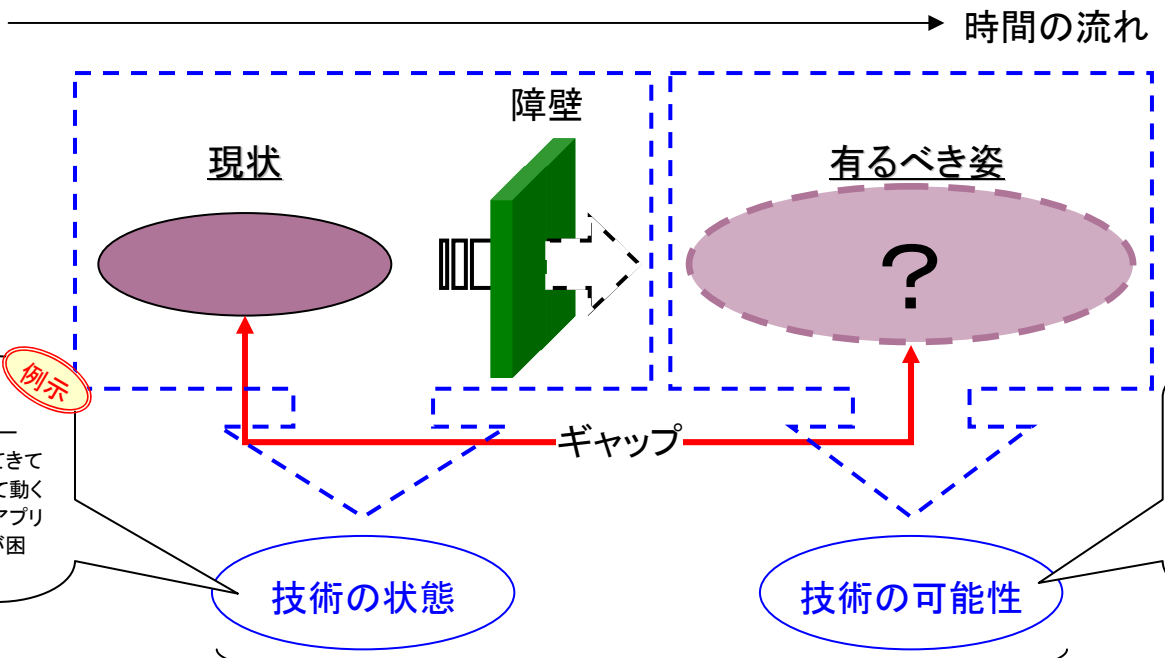
政府関与の必要性の判断ポイント　～技術の進展の障壁

技術の期待値と現状とのギャップを障壁の解消が政府関与であると捉え、ナレーティブに技術に関する情報を整理した後、障壁の捉え方を検討する

●技術の現状と将来的に目指したい状況の2つの観点で技術の有るべき姿と現状とのギャップを把握する

技術の進展の障壁とギャップ

技術は有るべき姿に近づいていくが、障壁によって有るべき姿と現状にギャップが生じる



現在の達成状況と課題等

例示

＜パッチの自動作成＞

単純なOSや古くからある形態のアプリケーション等に対しては自動化が可能になってきているが、ネットーワークを経由して連携して動くアプリーションや処理が複雑な業務用のアプリケーション等はパッチ作成のパターン化が困難であり、対応が進んでいない

技術の実現により達成されること

例示

＜パッチの自動作成＞

製品・サービスの信頼性の維持向上によって、これらの利用促進につながるほか、これまでパッチの作成・配布に投じられていたコスト・リソースを製品・サービスの高度化等に利用することが可能になる

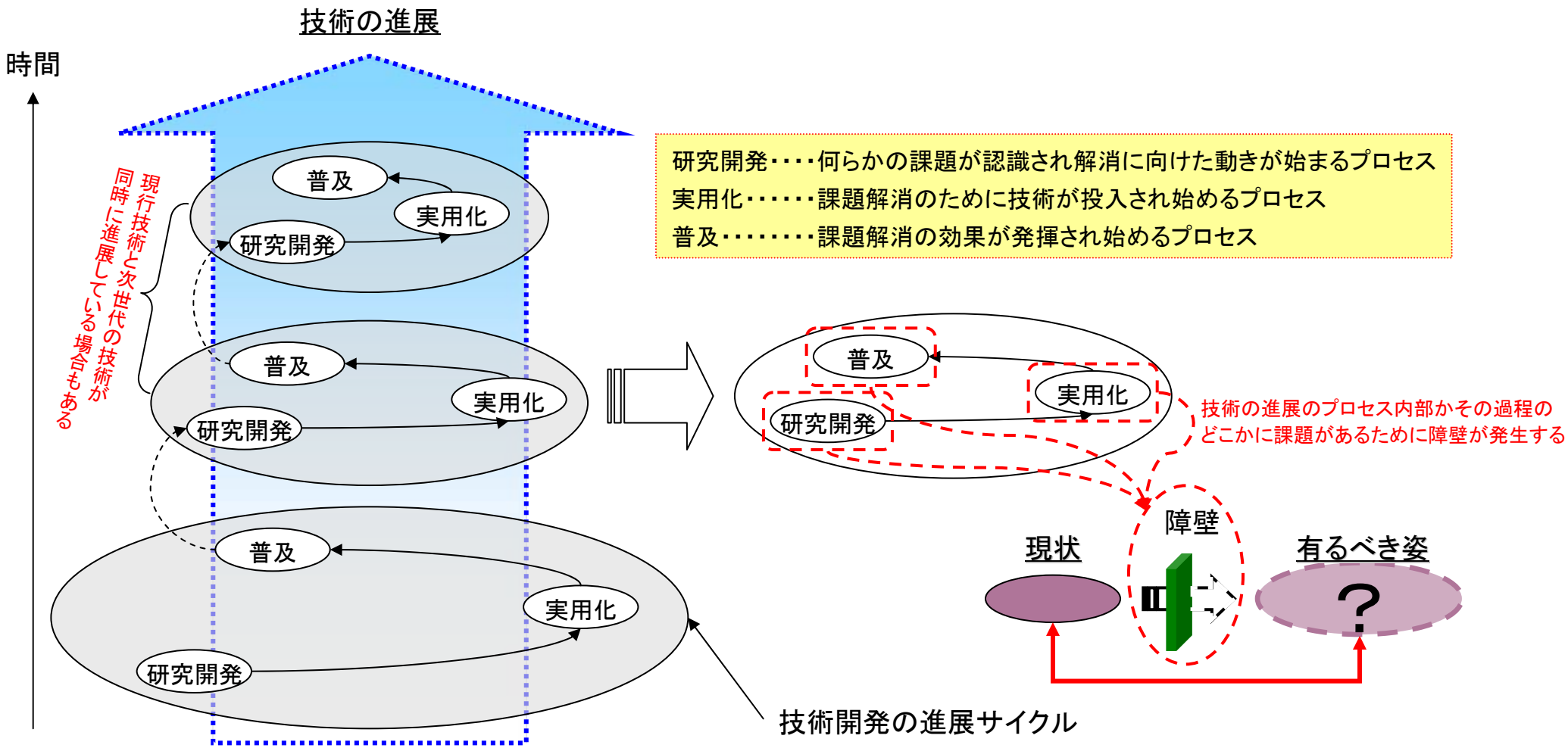
文章で表現する（ナレーティブな記述）

政府関与の必要性の判断ポイントの検討(2/2) ～技術の進展のプロセス

関与すべき課題が技術開発のサイクルのどこにあるかを検討しておく

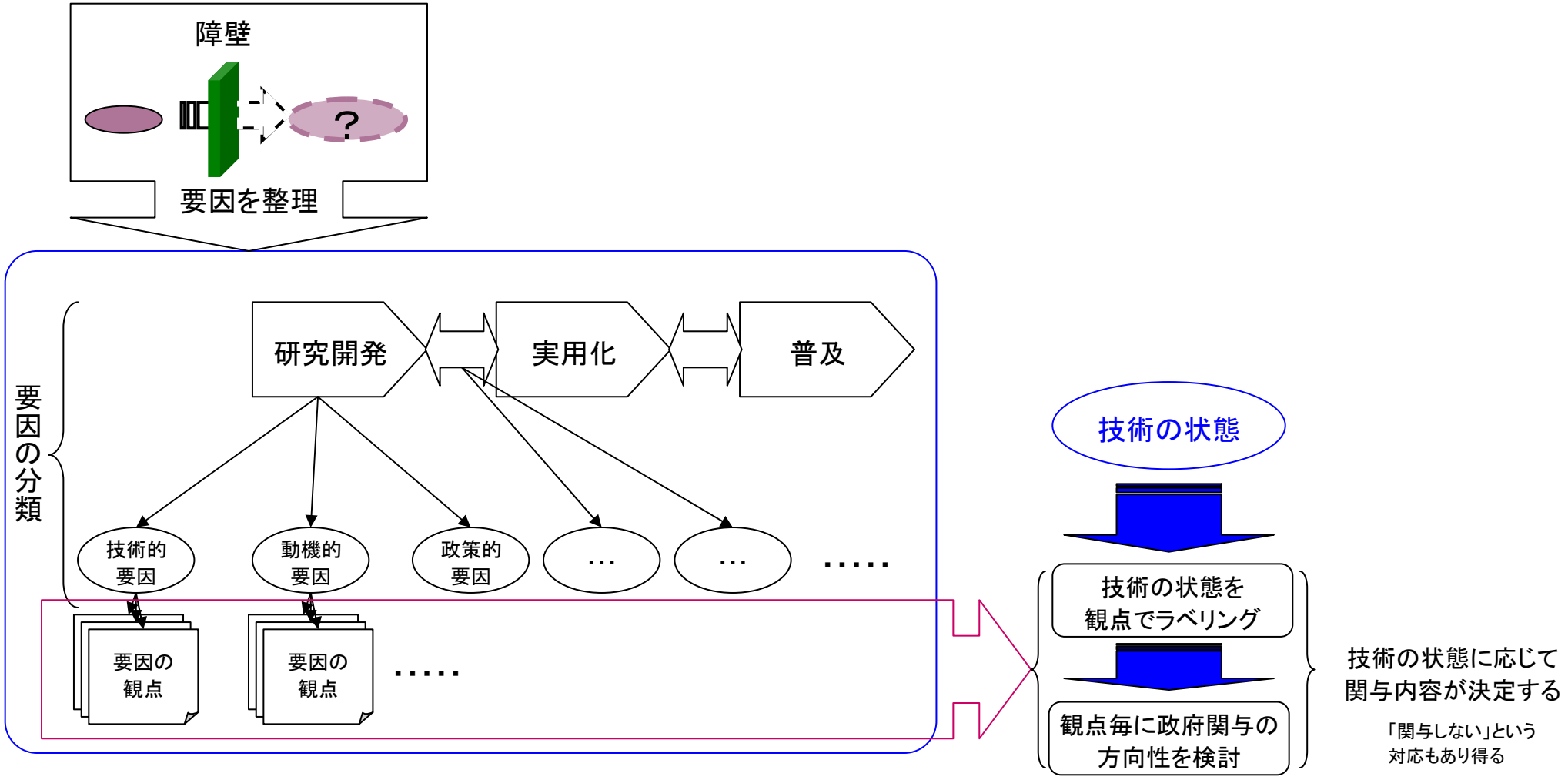
技術は、研究開発→実用化→普及のプロセスを繰り返しながら進展していく

ある技術が普及すると裏側で、同じ課題に対して次世代ないしは、別のパラダイムの技術が進展し始める



情報セキュリティ技術の選定基準の検討概要

技術の状態における障壁の要因の観点で整理した後、観点に沿った政府関与の方向性を設定することで情報セキュリティ技術の選定基準を検討する



情報セキュリティ技術の選定基準の検討(1/4) ～基準検討の観点の整理

障壁や溝を生む要因の有無を基準検討の観点とする（要因の有無や多少によって、関与するかしないかの判断や優先順位を議論する）

段階	要因の分類	要因概要（観点の例示）
研究開発段階	**技術的要因**	●セキュリティ課題の解消のための技術の具体的な実現方法が見つかっていない ●技術の課題解決能力が利用者にとって技術が目指す問題解消に十分でない
	経済的要因	●課題の認識が研究者になされずに研究開発の必要性が想起されない ●開発コストが十分にまかなえていない ●経済状況の影響を受けて研究開発への投資が進まない
	政策的要因	●技術の研究開発に関して規制等があるため開発が進まない
	社会的要因	●脚光を浴びない分野であるため研究開発のモチベーションを研究者が持ちにくい ●課題解消に適用される技術が社会的なコンセンサスが得られていない
実用化段階	**技術的要因**	●実用化のために必要な周辺技術のパフォーマンスが十分ではない ●実用化のために必要な周辺技術は存在するが十分なパフォーマンスを得るために必要なコストがかかり過ぎる
	経済的要因	●実用化に参加する企業が少ない ●需要が明確化ではないため投資がなされていない ●他の要因によって実用化に向けた研究開発のリスクが民間にとって高い ●経済状況の影響を受けて技術の必要性が薄れている
	政策的要因	●実用化のための政策的後押しや調整が進んでいない(外交的な課題解消や実用化を阻む社会的コンセンサスの解消等) ●技術の実用化を阻む規制等がある
	社会的要因	●技術の進展のスピードよりも社会から求められる要求が高くなるスピードの方が速い ●技術を実用化する社会的な要請が無い
普及段階	**技術的要因**	●不完全ではあるが平易な代替手段があるため技術を利用するメリットが少ない ●技術が持つソリューション能力の満足度が利用者にとって低い
	経済的要因	●普及の見通しの悪さから過少投資に陥っている ●技術を利用するためのコストが利用者にとって大きすぎる ●経済状況の影響を受けて技術の利用が進まない
	政策的要因	●普及のための政策的後押しや調整が進んでいない(公的な研究開発の商用化や技術開発の市場化等の課題) ●法律等により適用・利用が困難である
	社会的要因	●技術の進展のスピードよりも社会から求められる要求が高くなるスピードの方が速い ●技術の使用が社会的に受け入れられていない

情報セキュリティ技術の選定基準の検討(2/4) ～政府関与の方向性の議論（各論）

技術の状態に応じて、政府関与の方向性を議論しておく

段階	要因の分類	要因概要（観点の例示）	政府関与の方向性（事務局案）
研究開発段階	**技術的要因**	●技術の課題解決能力が利用者にとって技術が目指す問題解消に十分でない	✓課題解決能力向上ための技術の研究開発の立ち上げ ✓課題解決能力向上のための技術の研究開発への資金投入
		●セキュリティ課題の解消のための技術の具体的な実現方法が見つかっていない	✓研究開発促進のためのコンソーシアム／研究会等の立ち上げ
	経済的要因	●課題の認識が研究者になされずに研究開発の必要性が想起されない	✓公的研究機関による直接的な研究開発の立ち上げ ✓関係者への勉強会や研究会の立ち上げ
		●開発コストが十分にまかなえていない	✓研究開発への直接的な資金投入 ✓共同研究による研究開発の効率化の支援
		●経済状況の影響を受けて研究開発への投資が進まない	✓研究開発への直接的な資金投入 ✓景気対策目的の関連研究開発の立ち上げ
	政策的要因	●技術の研究開発に関して法規制等があるため開発が進まない	✓規制等の改正 ✓研究特区等の研究開発促進のための特別な許可
	社会的要因	●脚光を浴びない分野であるため研究開発のモチベーションを研究者が持ちにくい	✓技術開発のコンテスト化等によるモチベーション向上施策の実施 ✓公的な研究機関による研究開発
		●課題解消に適用される技術が社会的なコンセンサスが得られていない	✓技術の受容性を高めるための法制度の策定 ✓政府主導によるキャンペーンの実施

情報セキュリティ技術の選定基準の検討(3/4) ～政府関与の方向性の議論（各論）

段階	要因の分類	要因概要（観点の例示）	政府関与の方向性（事務局案）
実用化段階	**技術的要因**	●実用化のために必要な周辺技術のパフォーマンスが十分ではない	✓パフォーマンス向上ための技術の研究開発の立ち上げ ✓パフォーマンス向上のための技術の研究開発への資金投入
		●実用化のために必要な周辺技術は存在するが十分なパフォーマンスを得るために必要なコストがかかり過ぎる	✓コスト削減のための研究開発への資金投入 ✓現状の技術を用いた実装に際して資金投入
	経済的要因	●実用化に参加する企業が少ない	✓コンソーシアムの立ち上げ ✓資金提供による活性化 ✓政府による実用化事業のインキュベーション
		●需要が明確化ではないため投資がなされていない	✓政府調達における積極的な活用の明示 ✓市場創造を後押しする法制の制定
		●他の要因によって実用化に向けた研究開発のリスクが民間にとって高い	✓実用化に向けた取り組みへの直接的な資金投入 ✓公的な研究機関による研究開発と民間への還元
		●経済状況の影響を受けて技術の必要性が薄れている	✓＜関与しない＞
	政策的要因	●実用化のための政策的後押しや調整が進んでいない	✓外交や情報セキュリティの適用にあたってのステークホルダ間の調整等、政府が担うべき役割を発揮
		●技術の実用化を阻む規制等がある	✓実用化を阻む法規制等の改正
	社会的要因	●技術の進展のスピードよりも社会から求められる要求が高くなるスピードの方が速い	✓＜関与しない＞
		●技術を実用化する社会的な要請が無い	✓問題を提起する研究会・コンソーシアムの立ち上げ ✓意識改革のためキャンペーンの実施

情報セキュリティ技術の選定基準の検討(4/4) ～政府関与の方向性の議論（各論）

段階	要因の分類	要因概要（観点の例示）	政府関与の方向性（事務局案）
普及段階	技術的要因	●不完全ではあるが平易な代替手段があるため技術を利用するメリットが少ない	✓＜関与しない＞
		●技術が持つソリューション能力の満足度が利用者にとって低い	✓満足度を下げる要因に関する研究会の立ち上げ ✓満足度を下げる要因解消に向けた法制度の整備
	経済的要因	●普及の見通しの悪さから過少投資に陥っている	✓直接的な資金投入 ✓政府調達における積極的な活用
		●技術を利用するためのコストが利用者にとって大きすぎる	✓コストダウンを図るための技術開発
		●経済状況の影響を受けて技術の利用が進まない	✓政府調達における積極採用による需要の維持
	政策的要因	●普及のための政策的後押しや調整が進んでいない	✓商業化に際しての優遇税制等、普及に向けた政策的後押しの実施 ✓公益性が高い対策の公的な機関による実施
		●法律等により適用・利用が困難である	✓適用を阻害する法制度の改正
	社会的要因	●技術の進展のスピードよりも社会から求められる要求が高くなるスピードの方が速い	✓＜関与しない＞
		●技術の使用が社会的に受け入れられていない	✓技術の受容性を向上させるための法制度整備

グランドチャレンジに関する検討

我が国でも統合的なパッケージ

（cyber security enhancement act）を作ることが必要

米国の研究開発プログラムと情報セキュリティ政策

（1）サイバーセキュリティ促進法案（Cyber Security Enhancement Act）

・サイバーセキュリティに係るR&D戦略策定、R&Dおよび人材育成にかかる財政支出を認めることが主たる内容。

・議会予算局（Congress Budget Office）の見積もりでは、FY2010～2014の間に6億3900万ドル、それ以降3億2000万ドル必要。

・サイバーセキュリティ研究開発3カ年戦略を１年以内に策定・・・連邦政府のサイバーセキュリティを保障するために必要なR&D戦略を議会に提出（3年毎に改訂）

（2）連邦政府による研究開発プログラム

・米国は軍用・民生用両面において情報セキュリティの技術開発を積極的に支援。

・政府のR&D戦略には、情報セキュリティに係る高度人材育成の側面も存在。

・CSIA（Cyber Security and Information Assurance）※1に約２．８億ドルの莫大な研究予算。

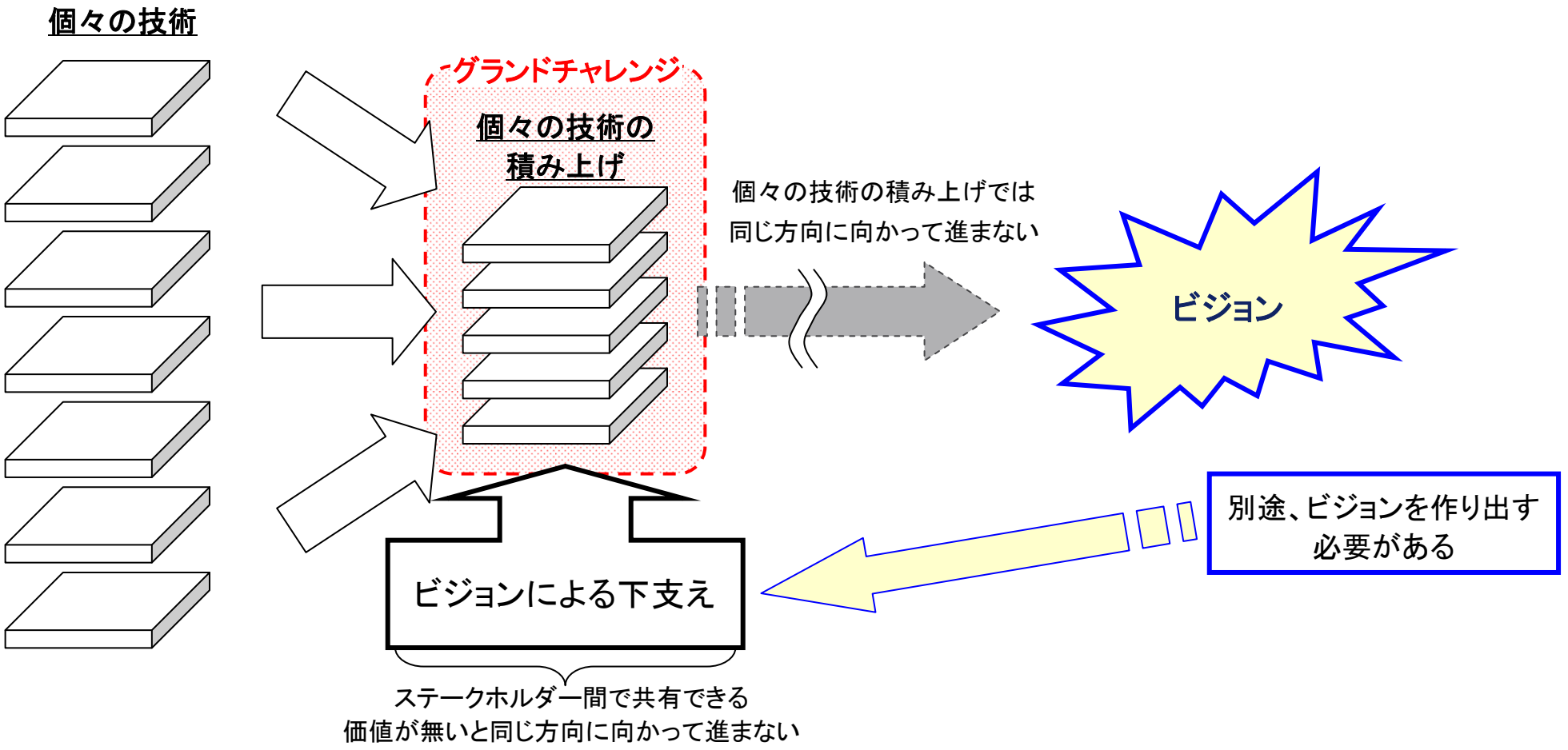
・中小企業や大学研究者の起業を支援するSBIR(Small Business Innovation Research)やSTTR(Small Business Technology Transfer)等の支援制度も充実。

※1：NITRD(Networking Information Technology Research and Development)における情報セキュリティの研究開発。

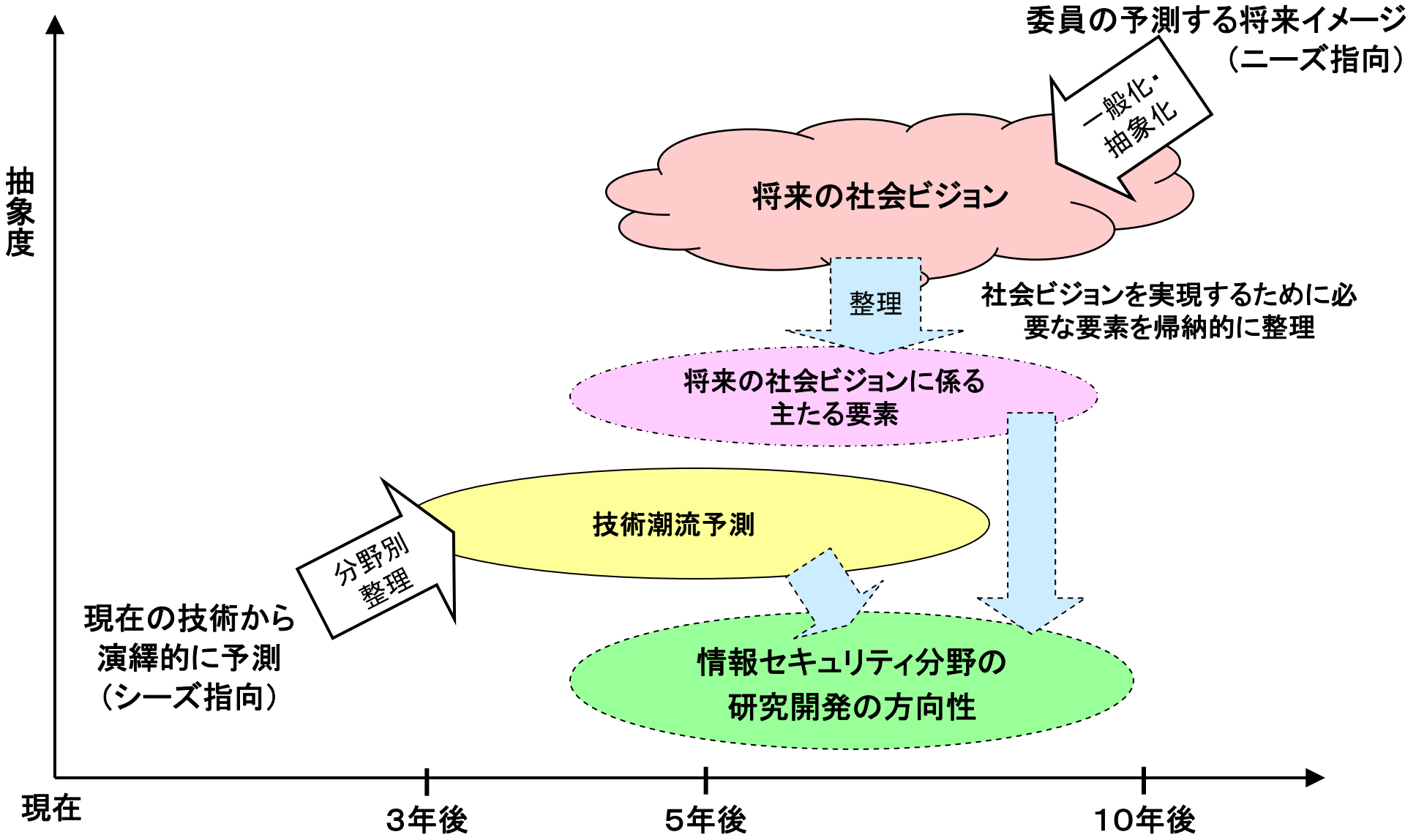
グランド・チャレンジ・ビジョンの必要性

●政府関与によって、個々の技術における進展の障壁を取り除くことも重要。

●一方で、個々の技術の積み上げでは、共通の方向に向かって技術が進展しないと考えられるため、情報セキュリティに関するビジョンを別途検討しておく必要がある。

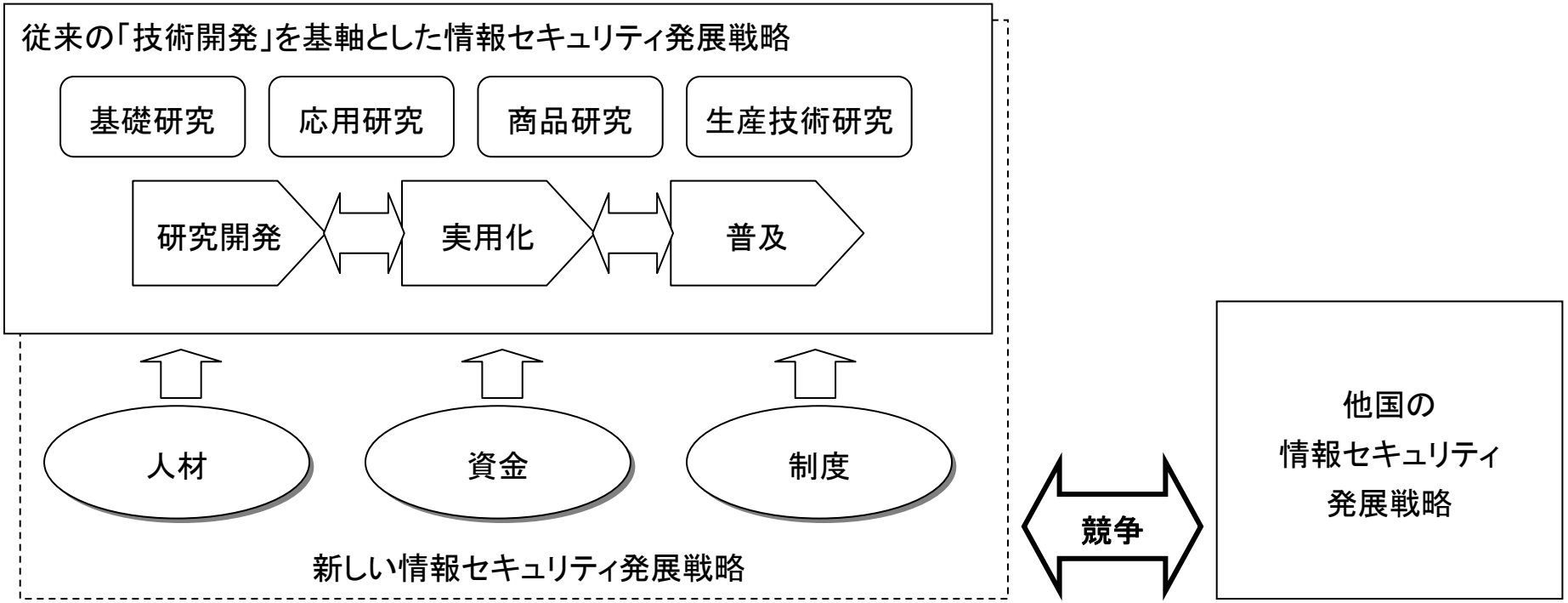


グランドチャレンジのテーマ検討のアプローチ（過去のアプローチ）



新しい情報セキュリティ発展戦略

従来のままの「技術開発」を基軸とした情報セキュリティ発展の戦略を踏襲するのではなく、「人材」、「資金」、「制度」を総合した情報セキュリティの発展戦略として見直しをする必要がある。



国際的なルールに沿いながらも
不利とならないように見直し

既存のグランドチャレンジの方向性からの変更点

2008年度の検討において示されたグランドチャレンジの方向性

- 「安全・安心な生活、社会経済活動」や「グローバル・ユビキタス」を実現するべく、日常の生活、社会経済活動に浸透したIT機器の情報セキュリティ確保に係る技術
- 「当然化」を実現するべく、一定の情報セキュリティ水準が確保されたプロダクトを設計開発する手法および技術
- 「適切性」を実現するべく、利用シーンに応じて動的に情報セキュリティ水準を最適化するような技術・システム
- 「マネージャビリティ（可管理性）」を実現するべく、人間がリスクをコントロールできることで安心して情報を管理できるような技術

技術戦略専門委員会報告書2008(情報セキュリティ政策会議 技術戦略専門委員会),2009/4/16
P35－36 「2．3 情報セキュリティ技術のグランドチャレンジ型研究分野の方向性」

情報セキュリティの研究開発・実用化・普及に必要な「人材」「資金」のリソースを効率よく集中させ、障壁となる「制度」の見直しを行うことにより、国内の情報セキュリティを向上させることをグランドチャレンジの方向性に持たせる

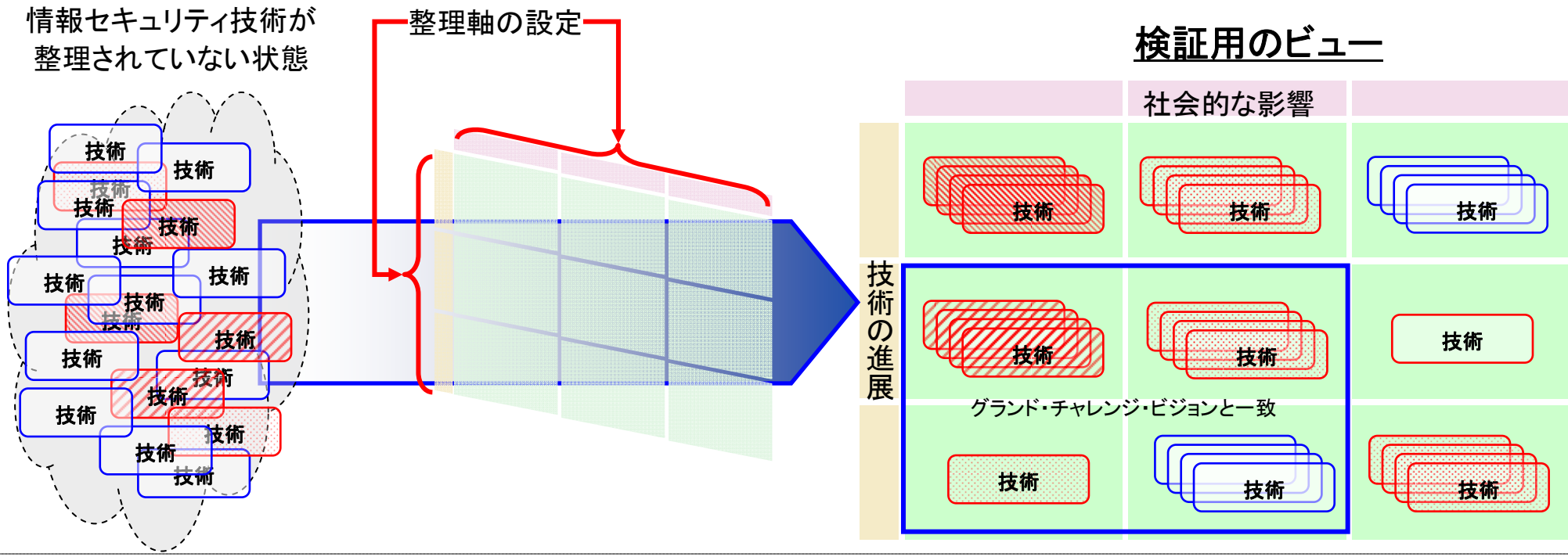
修正されたグランドチャレンジの方向性

- 広く適用されるべき情報セキュリティの効率的な適用を目指して、日本国における「安全・安心な生活、社会経済活動」や「ユビキタス」を実現するべく情報セキュリティ確保に係る技術
- 「当然化」を実現するべく、一定の情報セキュリティ水準が確保されたプロダクトを設計開発する手法および技術
- 「適切性」を実現するべく、利用シーンに応じて動的に情報セキュリティ水準を最適化するような技術・システム
- 「マネージャビリティ（可管理性）」を実現するべく、人間がリスクをコントロールできることで安心して情報を管理できるような技術

「情報セキュリティ研究開発プログラム」における重点研究開発課題の選定方法について

情報セキュリティ研究開発リストに関連する研究開発課題のうち、
検討会において整理された、①政府関与を必要とする何らかの理由があり、
②グランド・チャレンジ・ビジョンに合致する研究開発課題であって、
③今後4年～10年程度のうちに取り組むべき緊急性が高い課題

を、5～10個程度選定する。

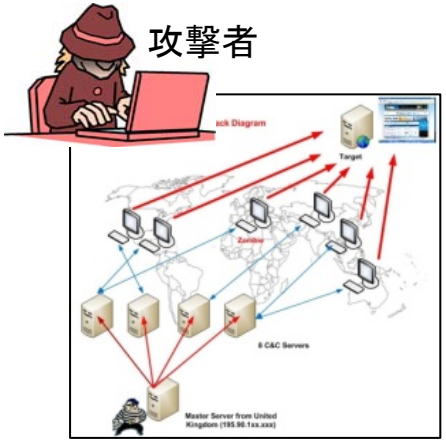


技術マップから抽出された研究開発課題

技術マップから研究段階のテーマを抽出

・情報漏洩検出技術（量子情報通信技術）
・個人情報の安全な利用を可能とする情報管理技術
・システムの相互影響評価・リスク分析技術

情報セキュリティ課題の根本的解決



IT利用者の対応力向上

・ユーザによる個人情報の制御
・ユーザの意図に沿った操作支援技術
・社会心理学に基づく情報セキュリティ対策技術
・セキュリティ投資対効果の評価技術

IT技術の発展・普及に伴う情報セキュリティ

・分散環境におけるプライバシー保護技術
・クラウドサービスを想定した脅威分析・検出技術
・仮想環境上の情報セキュリティ確保技術
・セキュア・ネットワーク・プロトコル技術

脅威の全体像の把握スキーム

・データマイニングによる異常検知技術
・大容量トラフィック監視技術
・サイバー攻撃のトレースバック技術
・未知プロトコル・不正コンテンツ検出技術

セキュリティを高めたITの実現

・社会的な安全性・信頼性の確保技術
・情報セキュリティの自動検証技術
・IT障害の自動復旧技術
・情報セキュリティ対策の定量評価技術
・HW/OS/SWの信頼性確保技術
・セキュア・ソフトウェア構築技術

情報セキュリティ研究・技術開発の重点課題

研究・技術開発テーマ

- 攻撃への対抗手段の開発に資する研究・技術開発
  例） 攻撃者をトレースバックする技術　等
- IT利用者の対応力向上に資する研究・技術開発
  例） 心理学を利用したフィッシング詐欺対策の研究　等
- IT技術の発展・普及に伴う情報セキュリティの確保に資する研究・技術開発
  例） IPv6、クラウド対応のセキュリティ技術開発　等
- 課題の根本的解決に資する研究・技術開発
  例） 情報漏えいの原因を特定する技術開発　等
- セキュリティを高めたITの実現に資する研究・技術開発
  例） 開発環境や要件定義の研究　等

体制の整備

- マルウェア等の研究環境の整備 （検体の捕捉等）
- 国際連携の推進 （国際共同研究開発等）