改訂案	備考
サイバーセキュリティ研究開発戦略 （改訂案） 令和３~~平成29~~年○~~7~~月○~~13~~日 サイバーセキュリティ戦略本部	資料２－２

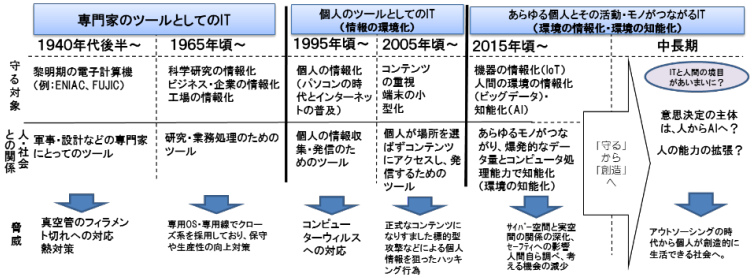
改訂案	備考

目次

※目次のページ数や項目名変更は後に反映予定。

改訂案	備考
③ サイバーセキュリティの考え方の再定義 ..... 25 （３）想定できない変化に対応するための全体設計（デザイン） ..... 26 ４．研究・産学官連携の推進方策と産学官エコシステムの構築 ５~~４~~．まとめ ..... 29 （参考）各府省の研究開発の例 31	

改訂案	備考
# １．はじめに **（１）サイバーセキュリティ研究開発戦略策定までの経緯** 我が国のサイバーセキュリティに係る研究開発戦略については、「サイバーセキュリティ戦略」（平成 25 年６月 10 日　情報セキュリティ政策会議決定）に基づき、３年程度を見据えた研究開発に係る基本的方針を示した「情報セキュリティ研究開発戦略（改訂版）」（平成 26 年７月 10 日　情報セキュリティ政策会議決定）を策定した。また、サイバー空間の重要性と、サイバー攻撃の脅威が増大する中、サイバーセキュリティ基本法（平成 26 年 11 月 12 日　成立）に基づき、３年程度の基本的な施策の方向性を示した「サイバーセキュリティ戦略」（平成 3027 年 7 9 月 27 4 日　閣議決定）を策定し、~~（参考１）及び（参考２）に示すように、~~政府や公的研究機関等で研究開発を推進して~~いる~~~~きた~~。	時点修正
本戦略は、これまでのサイバーセキュリティに係る研究開発の進捗と、IT の利活用の広がりやサイバー攻撃の脅威の深刻化といった環境の変化を踏まえ、将来的なサイバーセキュリティの研究開発を検討・推進するためのビジョンとして、研究開発戦略専門調査会における議論を通じて策定し（平成 29 年７月 13 日）、研究・産学官連携の振興について具体化を行った第４章を追記する改訂を行ったものである。~~たものである。~~	時点修正
（２）本研究開発戦略の趣旨、位置づけ **①　これまでの情報通信技術（IT）に関わる進化** 情報通信技術（IT）の進歩は極めて急速であり、将来の方向性を予測することは難しい。このため、長い人類の歴史を見据えた上で現在を位置付け、未来に向けたサイバーセキュリティの研究開発を考えていくことが必要である。これまでの人類の知的活動に関する歴史を振り返ると、「知の継承」（文字と紙の発明）、「知の流通」（活版印刷の発明）、さらに、「場所や時間の制約に囚われない知の共有・活用」（コンピュータとインターネットの発明）が進められてきた。知の共有・活用については、当初は、軍事や設計・研究のために使われる専門家のツールとしての情報通信技術（IT）から、パソコンやスマートフォンが普及し、個人、企業、大学、政府等が利用し、情報収集・発信やイノベーションのためのツールとしての IT へと発展した。そして、近年では、IoT（モノのインターネット）に代表されるように、あらゆる個人とその活動・モノがつながる情報通信技術（IT）へと進化を遂げている（図１）。こうした進化は、人間と情報の関わり方について、①情報の環境化（インターネットの普及により、多くの情報が身の回りにあふれること）、②環境の情報化（IoT により、情報通信技術（IT）が実世界と結びつき、センサーが実世界から収集したデータを基に実世界を変えることができる時代）、さらには、③環境の知能化（実世界から収集したデータがビッグデータとして蓄積され、そこから有用な情報を取り出すために人工知能が活用されること）、を促してきている。	



（図１）これまでの情報通信技術（IT）の進化

② サイバーセキュリティ研究開発の目的

上述した通り、情報通信技術（IT）が進化し、人間と情報の関わり方が変化していることを念頭におきつつ、我が国としては、以下の目的を持ってサイバーセキュリティに関連する研究開発を推進することが重要である。

a. 多様な価値観を持つ人間の思いが実現でき、人間が安心して暮らすことのできる社会システムを創造していくことを前提として、
b. 研究開発を通じて国際競争力を強化すること
c. 研究開発で得られた知見により経済成長につながる新産業を創出すること
d. 我が国として必要な技術力を獲得・保持すること

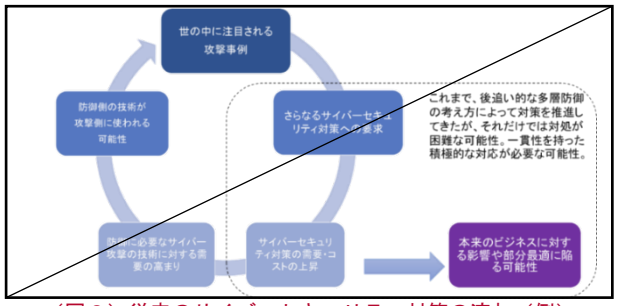
③ 本研究開発戦略の位置付けと構成

情報通信技術（IT）の進化の方向性を予測することは難しいため、本戦略では、個々のサイバーセキュリティ技術に関する技術的課題を深掘りすることはしないものとする。本戦略においては、情報通信技術（IT）の進化や、人間と情報の関わり方が変化していることを意識しつつ、将来的なサイバーセキュリティ研究開発の方向性についてビジョンを示すものとする。その際、「近い将来」だけでなく、「中長期的」な社会・経済の変化と情報通信技術（IT）の利活用の進化を視野に入れるものとする。

また、本戦略が想定する対象者については、我が国のサイバーセキュリティ技術の研究開発に関わる政府機関や公的研究機関だけではなく、直接的であれ、間接的であれ、情報通信技術（IT）に関わる研究開発を行っている大学や企業等を含め、経営者から研究開発の戦略企画を行う担当者、研究者まで、幅広い層を想定している。

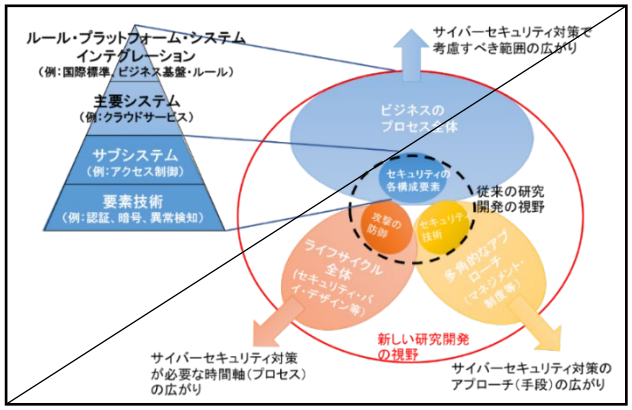
第２章においては、近い将来の情報通信技術（IT）の利活用に必要なサイバーセキュリティに関する研究開発を推進するため、その基本的な考え方を示すとともに、サイバー空間と物理空間の融合、AI の高度化・ビッグデータの活用、ネットワーク技術の高度化といった

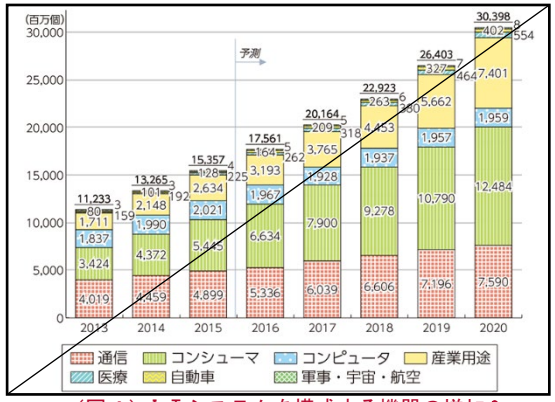
改訂案	備考
情報通信技術（IT）の利活用の進化の具体例も含め、近い将来の研究開発の今後の課題を提示する。主に、組織における研究開発に携わる管理職～担当者が、今後の自組織における研究開発の戦略や具体的なプロジェクトの企画・立案を行う際に、この内容を踏まえて取り組むことを想定している。 　また、将来の社会像や、サイバー空間とそれを支える技術の進化を踏まえれば、サイバー空間を介して人間の能力が拡張し、これまでの生活や労働を情報通信技術（IT）が代替するにとどまらず、新しい価値を創造し、より良い社会や人々の思いの実現につながっていく可能性がある。第３章においては、こうした変化の中で、改めて人間を中心としたサイバーセキュリティ研究の広がりを示し~~にサイバーセキュリティの考え方を見直し~~、中長期的な研究開発を検討する際の考え方~~切り口~~を提示している。 　さらに、第４章においては、研究及び産学官連携の振興に係る検討の具体化として、研究開発の国際競争力を躍進させる産学官エコシステムの構築を目指した推進方策を示した。 　本研究開発戦略は、主に、情報通信技術（IT）やサイバーセキュリティの研究者のみならず、経営者や組織の中長期的な経営課題について考えるべき立場にある者、さらには、人文社会科学系の研究に従事している立場にある者を含め、自組織の中長期的な戦略を議論する際に活用されることを期待している。	第３章の表現の見直しに伴うもの 第４章の追記に伴うもの

改訂案	備考
## ２．近い将来の情報通信技術（IT）の利活用を想定した研究開発戦略 ### （１）基本的な考え方 ~~これまで~~従前、サイバーセキュリティ対策については、攻撃に応じて、有効な対策を立てて防御していくということに注力をしてきた。その際、攻撃者側が日々、攻撃を進化させてきていることや、守るべき情報資産の分類に対応するため、~~いわゆる多層防御と言われる考え方で、~~様々な手段を使って守りを固める考えが一般的に浸透している。具体的には、~~多層防御においては、~~攻撃者のシステムへの侵入等の行為が行われないよう、攻撃を受ける側で過去の攻撃情報の共有を行い、それに基づいて後追い的に技術的な手法を中心として対策が講じられてきた。こうした仕組みの下では、脆弱性対策をはじめとしたシステム等のメンテナンスや更新の管理が肥大化・複雑化する可能性がある。ビジネス全体を見据えた広い視野がなければ、攻撃が進化すればするほど、サイバーセキュリティ対策に対するコストは上昇し続け、そのコストは、本来のビジネスに対する影響を及ぼす可能性があり、増大するコストは、経営層の正しい認識なしには承認を得られないことが生じ得る。また、後追い的なセキュリティ対策では、インシデント対応のコストが増加する可能性があり、失われた情報や評判の回復にリソースを費やすことにもなりかねない。さらに、このような対策の下では、結果としてサイバーセキュリティの側面だけの部分最適になっている可能性もあり、このような流れに依存するだけでは、問題解決が困難になる可能性がある。社会的・経済的要因を考慮に入れながら、安全・安心なサイバー空間を発展させ、本来のビジネス等を促すために一貫性を持つ形で、セキュリティの問題を合理的かつ積極的に達成可能なものとしていく視点が必要である。そのためには、業務、製品・サービス等のデジタル化、さらには変革を伴うデジタル・トランスフォーメーション（DX）を含め、IT の利活用の発展を踏まえつつ、視野を広げてサイバーセキュリティ対策を捉えていくことが期待される。こうした方向に資するようなサイバーセキュリティ対策におけるアプローチを検討した上で、研究開発を進めることが期待されるため、以下に基本的な考え方を提示することとする。個別の研究開発の企画・立案に当たっては、こうした考え方を念頭に置きつつ、検討が行われることが重要である。  ~~（図２）従来のサイバーセキュリティ対策の流れ（例）~~	時点修正 表現の見直し 表現の見直し 時点修正 簡略化：図の削除

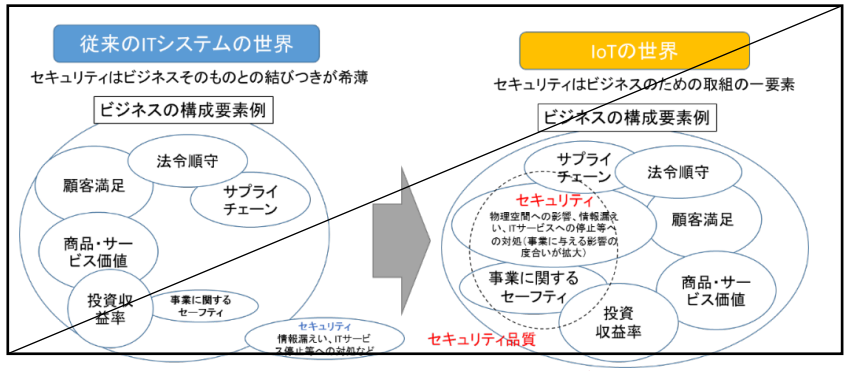
改訂案	備考
① ビジネスのプロセス全体を視野に入れることが重要 ~~これまで~~従前、我が国の企業における情報通信技術（IT）の利活用は、業務効率化を目的として、基幹系システム（生産・販売、会計、人事、給与、資産等の管理に関する企業内のシステム）や情報系システム（メールや文書作成、スケジュール管理等に関する企業内のシステム）を活用することが中心であった。近年は、IoT、ビッグデータ、AIなど、情報通信技術（IT）の利活用によって、新しい価値を創造するような、いわばビジネスにおけるイノベーションを目的とした情報通信技術（IT）の利活用が増加する傾向にある。 特に、IoT システムの急速な普及は目覚ましく、これによって、サイバー空間と実空間の融合が高度に深化することになる。こうした中で、市場における個人・企業が IoT システムを通じたサービスに期待する品質の要素としての安全やセキュリティ、すなわちより高いレベルの「セキュリティ品質」[1]を目指し、企業価値や国際競争力の源泉としていくことが必要である。その際、これまでの「セキュリティ」品質は、情報システムの信頼性が極めて重要な要素であったが、IoT システムをはじめとする新しい情報通信技術（IT）の利活用においては、それが提供するサービスを安全かつ持続的に提供すること（機能保証）が求められる。それは、セキュリティを含めたシステムの個々の構成要素の組み合わせ（システムインテグレーション）によって実現されるものであり、その組み合わせ方を決めるものが「ルール」である。このため、セキュリティ技術やその要素技術はあくまでビジネスのプロセスを実現する一つの手段と考え、「ルール」を含めた情報システムを取り巻くビジネスのプロセス全体を考慮に入れたセキュリティの研究開発が実施されるべきである。同時に、上述の通り、ビジネスのプロセス全体を考慮に入れ、ビジネスにおける機能保証とセキュリティ品質の向上を目指す場合、機能レベルを含めた脅威やセキュリティの問題点の可視化や評価技術の確立など経営層が認識を深めるための取り組みや、対外的なセキュリティ品質等に関する情報発信を含めて取り組んでいくことが重要である。 **② システム運用時に必要なサイバー攻撃の検知・防御だけでなく、ライフサイクル全体で捉えることが必要** 先述の通り、情報通信技術（IT）の利活用によって、新たな価値を創造する中で、企業価値や国際競争力の源泉となる高いレベルでの「セキュリティ品質」を実現していくことは重要な課題である。しかし、セキュリティをシステムの運用が始まった後に、後付けで導入しても、システムは本質的に安全になるものではなく、むしろ単にコストの大幅な増加の要因となる。また、欧米においては、インダストリー4.0 やインダストリアルインターネットに代表される企業間連携や、製品にセキュリティ対策が行われていることを前提とした標準化の動きがあり、サイバーセキュリティ対策は、サイバー攻撃の検知・防御だけでは不十分となりつつある国際的な動向も踏まえた対応が必要である。この際、連携される既存のシス 1 「セキュリティ品質」：市場における個人・企業が当該サービスに期待する品質の要素としての安全やセキュリティ（平成 27 年９月　サイバーセキュリティ戦略） 5	時点修正

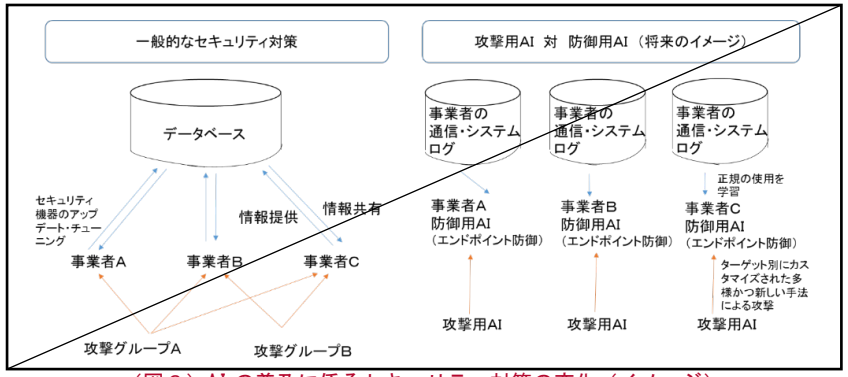
改訂案	備考
テムを含めて、システム全体の企画・設計段階から、セキュリティの確保を盛り込むセキュリティ・バイ・デザイン（Security By Design）の考え方を推進する。 　また、IoT システムや AI 等を活用した新たなビジネスを創出する際、コスト抑制の観点から、安価な機器の調達・導入が選択される可能性があることや、企画・設計から廃棄までのライフサイクルが長いこと、機器の演算処理能力に制限があることなど、IoT システムにおいては、従来の情報通信機器とは異なるセキュリティに関わる構成要素の特徴が存在する。このため、セキュリティの研究開発においては、こうしたシステムの特徴を踏まえつつ、ライフサイクルの各段階において必要な技術の検討を行うことが重要である。特に、IoT システムの製造に関わるサプライチェーンシステムの複雑性を踏まえ、製品に組み込まれる IC チップを含むハードウェアの真正性の検証技術等は重要である。 **③ セキュリティ技術だけでなく、多角的なアプローチが重要** 　情報通信技術（IT）の利活用に関する技術の進歩により、サイバー空間が実空間と融合し、現実社会への影響も大きくなっている。一方で、サイバー攻撃の手段も日々進化している。こうした中、単に情報システムに対するサイバー攻撃の脅威だけに注目し、その検知・防御等のためのセキュリティ技術による後追い的な対策だけでは、脅威に対抗し、システム全体を守ることは困難になりつつある。言い換えれば、攻撃の検知や防御には限界がある可能性を前提とした取り組みが重要である。このため、従来から行われてきた検知技術、暗号、認証技術、ネットワークアクセス制御など検知・防御を中心としたセキュリティ技術に関する研究のみならず、攻撃を受けた場合のシステムの抵抗力や回復力（レジリエンス）の確保や被害を最小化するためのシステム運用技術・ノウハウ、マネジメントやリスクコミュニケーション、さらには法律や経済・経営、国際関係、安全保障、心理等の社会科学的視点も含め、様々な領域の研究との連携、融合領域の研究に取り組むなど、社会・技術の変化を先取りし、多角的なアプローチ（手段）によるセキュリティに関連した研究開発を進めていくことが重要である。例えば、サイバーセキュリティは、経営層が自ら理解し、必要な判断が求められているため、企業としての「挑戦」と、それに付随する「責任」として、サイバーセキュリティに取り組むための経営に関する研究や、経済や社会との関係において企業に求められるサイバーセキュリティの対応に関する研究などが挙げられる。	状況の反映

改訂案	備考
 ~~（図３）研究開発の視野の広がり~~	簡略化
（２）近い将来の情報通信技術（IT）の利活用 近年の情報通信技術（IT）の進化の流れ（トレンド）については、サイバー空間と物理空間の融合（IoT）に代表されるように、様々なモノが①つながること、そして、つながるだけでなく、AI の高度化やビッグデータの活用によって、モノが②知能化すること、さらに、そういったものがネットワーク効果（つながるモノが増えれば増えるほど、ネットワークの価値が高まり、モノがより良くなっていくこと）によって、③広がること、が進展していると言える。また、④量子技術の進展も起きている。こうした変化の流れ（トレンド）を捉えつつ、サイバーセキュリティの研究開発に係る課題を見いだし、取り組んでいくことが必要である。	状況の反映
①~~つながる~~ーサイバー空間と物理空間の融合（IoT）ー~~つながる~~ー IoT システムの普及により、サイバー空間と実空間の融合が高度に深化する。今後、企業は、こうした IoT システムを活用した新たなビジネスの創出や既存ビジネスの高度化を図る方向に向かうと見込まれる。このため、我が国企業がこうしたビジネスチャンスを確実に捉えることは、我が国の経済社会の活力の向上及び持続的発展にとって極めて重要である。 その際、IoT システムのサイバーセキュリティを確保することは重要であるが、IoT システムの特徴を意識しつつ、ビジネス自体の目的や戦略に沿った形で、重点的に取り組むべき事項等の検討が行われることが重要であり、それに資するような研究開発が行われるべきである。 具体的には、IoT システムについては、先述の通り、特に産業用システムの場合、それを構成する機器のライフサイクルが長いことや、安全性や長時間の安定稼働、さらには、家電	表現の見直し

改訂案	備考
などの小型システムの場合に低い演算処理能力の下でのセキュリティ対策が求められる。そして、業種・ビジネスモデルによって、システム全体を構成する要求項目が広がる可能性があるとともに、個々の要求項目に対する水準も大きく変わることなど、これまでのコンピュータやサーバーがネットワークにつながった主に業務効率化を目的とした従来型の情報システムとは大きく異なる。 一方で、こうしたIoTシステムを構成する機器が爆発的に増加し、様々な機器が入り混じる形でつながることから、~~いちいち~~一つ一つの機器を管理し、同じレベルで整合的に技術的な対策を講じることには限界がある可能性がある。このため、これまで、事業との関係が希薄であった情報システムにおける機密性・完全性・可用性を目指したセキュリティコントロール、例えば、通信の暗号化、アップデートによる脆弱性対策、ウィルス対策等による予防措置、個々の通信監視による検知や冗長化による復旧を、IoT システムに従来と同様に適用することは適切ではない可能性があるとの認識を持つことが必要である。むしろ、IoT システムのセキュリティを単独で企画・設計等を検討するのではなく、IoT システムにより、新しい価値を生み出すビジネスの創出が促進できるよう、それ以外の強み・弱みを捉え、想定されるビジネス自体の目的や戦略に照らして、ビジネスの品質を決定する一要素としてIoTシステムのセキュリティの考え方を整理することが期待されている。このため、こうした考え方を踏まえた、必要な技術の研究が進められるべきである。~~なお、その際、内閣サイバーセキュリティセンターが平成28年8月に策定した「安全なIoTシステムの創出に向けたセキュリティに関する一般的枠組」を、ビジネスの目的や戦略に必要なIoTシステムのセキュリティの検討を行う上で活用することが期待される。~~	表現の見直し 簡略化及び状況の反映
 ~~（図4）IoTシステムを構成する機器の増加[2]~~	簡略化

~~2 総務省　平成28年版　情報通信白書（原出典　HIS Technology）~~

改訂案	備考
 ~~（図５）IoT システムの利活用によるセキュリティの位置づけの変化（イメージ）~~	簡略化
② ~~知能化する＝~~AI の高度化・ビッグデータの活用－知能化する－ ａ．人工知能の活用におけるセキュリティ 人工知能に関する研究は、これまで、数学の定理を証明することやチェスを指す人工知能といったコンピュータによる探査・推論によって特定の問題に対して解を提示するもの、コンピュータに知識を与えることで人工知能が実用可能な水準に達し、専門家のように振る舞うことができるもの、そして、近年では、ビッグデータを用いて、人工知能自体が知識を獲得するディープラーニング（多層構造のニューラルネットワークを用いた機械学習）が実用化されている。こうした人工知能は、産業、教育、行政など幅広い領域で人間社会に深く浸透することで、人々の生活が豊かになることが期待される一方で、悪用されることにより、公共の利益を損なう可能性も否定できない。こうした観点から、人工知能の活用~~研究開発~~におけるセキュリティに関し、どのような具体的な課題があるのかという社会全体での議論が期待される。我が国においては、Society 5.0 の実現を通じて世界規模の課題の解決に貢献するとともに、我が国自身の社会課題も克服するために、今後の AI の利活用の環境整備・方策を示した「AI 戦略 2019」（令和元年６月 11 日　統合イノベーション戦略推進会議決定）が策定されたが、~~具体的な取り組みとしては AI ネットワーク社会推進会議において、「AI 開発ガイドライン」の策定に向けた検討や国立研究開発法人科学技術振興機構社会技術研究開発センターの研究開発領域「人と情報のエコシステム」における活動、人工知能学会倫理委員会において、今後の人工知能学会と社会との対話に向けた方針として「人工知能学会倫理指針」の策定などが行われている。~~こうした取組の内容を踏まえつつ、AI に関するセキュリティを実現するための研究開発を行うことが期待される。また、AI の高度化と併せて、~~ビッグデータの活用がますます進むことから、~~プライバシーの確保や AI そのものを守るセキュリティに関しても、研究開発の検討においては重要な要素である。	表現の見直し 表現の適正化 時点修正 状況の反映
ｂ．サイバーセキュリティ分野における AI の活用 近年、サイバーセキュリティに関する業務において AI を活用することが注目されている。これまで、サイバー攻撃に対する検知は、ルールベース（不正が疑われるプログラムの動作を解析し、「ルール」と合致する動作を行うものを判定する方法）やシグネチャーベース（過	

改訂案	備考
去に行われた攻撃に関する通信をデータベース化し、通信の内容が一致するものを判定する方法）の防御システムを導入し、そのシステムの設定を調整（チューニング）することで行われてきた。こうした手法では、情報共有・収集等による過去の攻撃に関する一元的なデータベースの構築を前提としており、攻撃者側のスピードに追い付くことができず、全く新しい手法による高度な攻撃に対応することはできない。このため、特に侵入検知の領域において既に AI の活用が進んでおり、エンドポイント（ネットワークに接続されたサーバー、パソコン等）の振舞いを検知しログを取るエンドポイント分析、ユーザーの行動（メールのやりとりや、システムの操作）の分析、ネットワークトラフィックのビッグデータの分析、これらを総合的に組み合わせた、異常な動きや振舞いの分析に関するさらなる研究開発や実用化が期待されている。さらに、~~近年では、~~攻撃者側によるが~~-~~AI のを活用が考えられ~~し~~、~~個々の被攻撃者（ターゲット）に対してカスタマイズされた多様かつ新しい攻撃を行うようになってくることが想定されており、~~こうした動きへの対応も必要である。加えて、このように AI がサイバー空間上で攻撃・防御を人間に代わって行うような状況においては、これまでのサイバーセキュリティ対策の常識に囚われず、攻撃者の持つ技術の異次元の高度化に対応した適切なアプローチの在り方に関する研究開発についての検討も必要である。	状況の反映
 ~~（図６）AI の普及に係るセキュリティ対策の変化（イメージ）~~	簡略化
③ ~~広がる－~~ネットワーク関連技術の高度化－広がる－ 様々なモノがネットワークにつながるようになり、5G によってネットワークの拡大と併せて通信容量は大幅に増大するとともに、クラウドサービスをはじめ新しいサービスが登場している。また、IT の利活用による新しい価値を生み出すビジネスのモデルが時々刻々と変化を遂げる中、ネットワークが提供するサービスのライフサイクルが短くなっている。こうした中では、通信に求められる品質に応じて通信毎のネットワークの分離を図ることにより、通信の	表現の見直し 状況の反映

改訂案	備考
効率化のための制御を実現することや、ビジネスのニーズに対応したネットワークの変更等、ネットワークに高い柔軟性が求められることになる。さらに、ネットワークが拡大していく中で、つながるモノや人の信頼性（トラスト）の確保が重要となる。集中化された信頼の起点に頼る形で多くのネットワークへの参加者のアクセス権を制御することは、単一起点がボトルネックになることや、それ自体の脆弱性が大きな悪影響につながることなど、ネットワーク全体の信頼性の観点からは、分散化、例えばネットワークの参加者相互のコンセンサスによる信頼の確保が有効な可能性がある。このように、IoT 時代において、ネットワークが大幅に拡大していく中で、ネットワークの「効率性」、「柔軟性」、「参加者の相互信頼」を高めることが重要になってくると考えられる。 　こうした中、ネットワーク技術の高度化が急速に進展しつつある。例えば、昨今、ネットワーク機器の操作・制御の自動化を進め、オペレーションの効率化を進める観点から、幅広い範囲のネットワーク機器を、ソフトウェアによって集中的に制御する、いわゆる SDN（Software Defined Networking）に対応した製品の導入が進められており、データセンター内ネットワーク、データセンター間ネットワーク、クラウド基盤、インターネット・エクスチェンジの運用・管理や地上デジタル放送の中継回線の制御など、一部の大規模ネットワークの運用・管理に導入が進んで~~始まって~~いる。[2]また、機能の定まった個々の機器の制御にとどまらず、ソフトウェアによる「ネットワークの機能の仮想化」(NFV: Network Function Virtualization)により、ネットワークを構成する機器の機能は「所与」のものでなく、機能分担を自由に決定、変更することも可能となってきた。これらの技術を活用すれば、ネットワークの構築に携わる者自身が、汎用的なハードウェアの上に、ネットワークの構成要素を自由に設計・制作することが可能となる。さらに、セキュリティに関しては、ネットワーク全体のコントローラの保護を前提として、サイバー攻撃等により問題が生じたネットワークに関して、攻撃された部分を分離し、バーチャルに冗長化された代替のネットワークに切り替えることによって、ネットワークの機能を損なわずに、攻撃された部分の修復を行なうような柔軟な対応が可能となる。 　また、シェアリング・エコノミー[3]が広がっていく中で、その要素の一つとして活用が期待されるビットコイン等の価値記録の取引に使用されているブロックチェーン技術は、「取引履歴を暗号技術によって過去から１本の鎖のようにつなげ、ある取引について改ざんを行うためには、それより新しい取引について全て改ざんしていく必要がある仕組みとすることで、正確な取引履歴を維持しようとする技術」である。その構造上、従来の集中管理型のシステムに比べ、①改ざんが極めて困難であり、②実質ゼロ・ダウンタイムなシステムを、③安価に構築可能、という特性を持つものであり、IoT ~~(Internet of Things)~~ を含む幅広	時点修正 省略

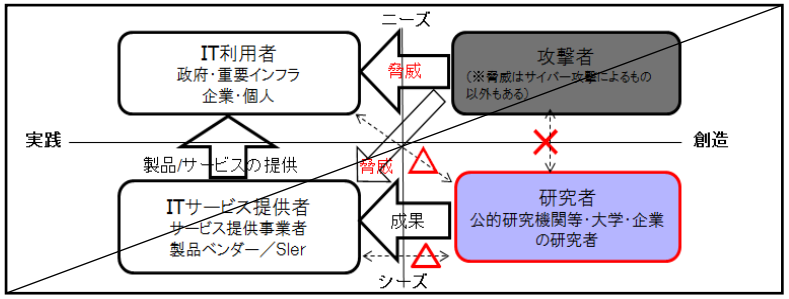
2 IoT/ビッグデータ時代に向けた新たな情報通信政策の在り方について第三次中間答申（平成 29 年 1 月 27 日　情報通信審議会）

3 「シェアリング・エコノミー」とは、典型的には個人が保有する遊休資産（スキルのような無形のものも含む）の貸出しを仲介するサービス（総務省　平成 27 年版　情報通信白書）

改訂案	備考
い分野への応用が期待されている。これまで、サイバー空間においては、経済活動の基盤となる取引相手の信頼性を担保する手段として、様々な制度や仕組みを構築してきたが、ブロックチェーン技術は、これらの仕組みを代替し、従来の社会システムを大きく変容させる可能性がある。例えば、参加者同士が対等の関係で相互に協力・監視することで、これまで社会システムを維持するために多大なコストを払って構築してきた中央集権的な第三者機関（中央機関）を不要とする可能性がある。 　このように、~~「効率性」、「柔軟性」、「相互信頼」の向上が今後の方向性として期待される中で、新しい考え方によるネットワーク技術の登場が期待されるが、~~こうしたネットワーク技術の発展の方向を見定めつつ、それに関わるセキュリティの問題の研究を適時に実施していくことが望まれる。~~併せて、既存の仕組みを根本的に変えてしまうような技術の発展の影響に関する人文社会科学的な研究も必要である。~~	状況の反映 第３章と重複するため簡略化
④量子技術の進展 　量子コンピュータの急速な進展により、現代のインターネットにおけるセキュリティを支える公開鍵暗号技術が将来的に解読される可能性が生じ、国際的に耐量子計算機暗号に関する検討が進められている。一方、耐量子計算機暗号においても危殆化のリスクがあるため、安全保障にも関わる重大脅威との認識の下、原理的に安全性が確保される量子通信・暗号に関する研究開発が進められている。 　我が国としても、国及び国民の安全・安心の確保、産業競争力の強化等の観点から、重要な情報を安全に保管する手段として、機密性・完全性等を有し、かつ市場化を見据えて国際競争力の高い、量子通信・暗号に関する研究開発や、その事業化・標準化等に、国をあげて取り組むことが極めて重要である。	状況の反映（量子技術イノベーション戦略（最終報告）（令和２年１月 21 日、統合イノベーション戦略推進会議）及び研究開発戦略専門調査会第 15 回会合（令和２年 11 月 25 日）資料 1-5）

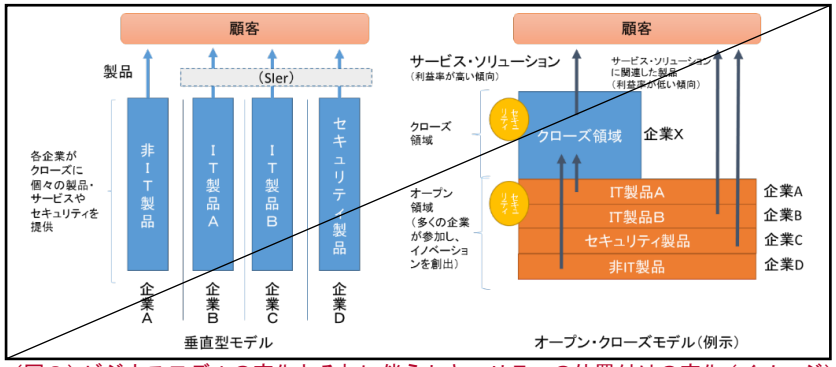
改訂案	備考
（表１）　サイバー空間に関わる技術の変化とその対応 変化：つながる 現象例：サイバー空間と物理空間の融合（IoT） 現象に関する変化：IoT の利活用により新しい価値を生み出すビジネスモデルの要素としてセキュリティが位置付けられる 変化への対応：ビジネス全体の強み・弱みを捉え、ビジネスの目的や戦略から必要と想定されるセキュリティ技術の研究開発に取り組む 変化：知能化する 現象例：AI の高度化・ビッグデータの活用 現象に関する変化：AI の普及により、その悪用が公共利益の損失につながる可能性 変化への対応：AI 利活用のガイドライン・指針に対する認識を高め、AI や、AI に関するセキュリティの研究開発に取り組む 現象に関する変化：AI が検知・防御の担い手になる。一方で、AI によるターゲット別にカスタマイズされた多様かつ新しい手法による攻撃への対処が必要 変化への対応：データベースの構築を前提としたこれまでのセキュリティだけでなく、エンドポイントの AI による防御も視野に入れるなど、これまでの常識に囚われず、攻撃者の持つ技術の異次元の高まりに対応した研究開発に取り組む 変化：広がる 現象例：ネットワーク技術の高度化（SDN、ブロックチェーン等） 現象に関する変化：IoT の利活用による新しい価値を生み出すビジネスが求められる中、ネットワークの効率性、柔軟性、参加者相互の信頼を高めつつ、セキュリティを確保することが必要 変化への対応：SDN やブロックチェーンといった新しいネットワーク関連技術の発展の方向を見定めつつ、それに関わるセキュリティに関わる研究開発をタイムリーに実施していく。併せて、既存の仕組みを根本的に変えてしまうような技術の発展の影響に関する人文社会科学的な研究に取り組む	簡略化

改訂案	備考
（３）セキュリティ研究開発における課題に対応した方法論 **① 国内外における産学官の連携と企業経営層のリーダーシップによる研究開発** これまで、サイバーセキュリティに関する技術の研究開発を行ったとしても、事業化して、その技術そのものが普及するためには、大きな壁があるとされてきた。これはサイバーセキュリティの分野に限らず、いわゆる「死の谷」の問題として研究開発で指摘されてきた問題である。こうした問題に陥らないようにするため、顧客にとって魅力的で品質の安定した製品・サービスが、現実的な価格で提供できることを想定した研究開発が必要である。ところが、こうした顧客の視点や製品・サービスの品質に関わる事項については、研究者の科学的知識と能力だけで研究開発に反映できるものではなく、ビジネス戦略上の判断や顧客目線を持った上での研究開発のアプローチが不可欠となる。例えば、他の異なる企業が持つ技術と組み合わせることや、自組織が持つ技術の改良なのか、新規技術の研究が必要なのかといった判断、技術に期待される品質のプライオリティ、などである。このような観点で研究開発を行うためには、研究を実施する主体だけが独立して研究を実施するのではなく、国内外の産学官の連携や、企業経営層を巻き込んだ研究開発の推進（例えば、研究機関の幹部と産業界の幹部の連携枠組に基づく、個別の研究の推進）が必要である。なお、こうした連携を実現するためには、研究の実施機関においても、単に実用化に極めて近い技術だけを追求するのではなく、産学官連携の中で貢献できるような魅力的な基盤技術を高めていくことも重要である。 **② 脅威に関する情報やユーザー等のニーズを踏まえた実践的な研究開発** IoT システムが普及し、世界とのつながりが拡大する中、サイバーセキュリティの研究開発は社会的なニーズや世界のトレンドを踏まえ実用化されることが重要であり、研究成果の社会還元の推進が重要である。このため、情報通信技術（IT）の利用者が受けているサイバー攻撃の実態や脅威、~~情報通信技術（~~IT~~）~~の利用者のニーズ・リテラシーを十分に把握した上で、研究が行われなければ、社会還元を図ることは難しい。~~（図７）は、「情報セキュリティ研究開発戦略（改訂版）」（平成 26 年７月 10 日　情報セキュリティ政策会議決定）において示した図を一部修正したものであり、例えば、~~研究者とサイバーセキュリティの実践側（IT の利用者や IT サービスの提供者）との連携が重要であり、~~行われていない場合や、~~研究者が攻撃者の動向を把握することも重要である。~~できていない可能性、さらには、そもそもサイバーセキュリティの実践側がサイバー攻撃やニーズについて不明確な状況を指摘したものでがある~~。研究開発をより実践的なものとし、効果・成果をあげるために、具体的な事象などの脅威に関する情報やユーザー等のニーズに関する情報共有などを促していくことが重要である。	簡略化 表現の見直し

改訂案	備考
 ~~×：一般的には情報共有・理解がほとんどないと思われる~~ ~~△：一般的には情報共有・理解が十分でないと思われる~~ ~~（図７）サイバーセキュリティ対策の関係者を取り巻く課題~~	簡略化
③ サイバーセキュリティの研究開発に係る制度等の検討 先端のサイバーセキュリティの研究開発を推進していくため、必要な制度の見直しを柔軟に検討していくことが重要である。~~このため、~~例えば平成 30 年度に、~~著作権法における~~セキュリティ目的のリバースエンジニアリングに関する適法性の明確化を含む~~や、所要の制度の見直しについて検討を行う~~著作権法改正が行われた。関連して、サイバーセキュリティ対策の実施において参照すべき法制度に関する整理が行われている（「サイバーセキュリティ関係法令 Q&A ハンドブック」（令和元年度））。 また、サイバーセキュリティに関連する技術の発展に伴い、社会との接点で生じる様々な倫理的・法的・社会的課題（ELSI）[4]に対する適切な配慮が必要である。	時点修正 状況の反映
④ オープン・クローズ戦略の推進 **ａ．オープン・クローズ戦略に関わるセキュリティ** 我が国は、これまで現場の「カイゼン」によって、匠の技を磨き、品質が高く、生産性の高い「もの」づくりを実現してきた。しかし、~~「ものづくり白書」[6]でも指摘をされているように、~~付加価値が「もの」そのものから、「サービス」「ソリューション」に移っており、3D プリンターなどのデジタルファブリケーションの登場等により、単に良い「もの」をつくるだけでは企業が生き残れない時代に入っている~~可能性がある~~。さらに、サイバー空間が、「サービス」「ソリューション」における価値の形成において、大きな役割を担うようになってきている。こうした中、ビジネスモデルについては、近年、オープン・クローズ戦略が重要になっている。これは、国際連携によって、様々なプレーヤーが自由に参加し、切磋琢磨しながらイノベーションを生み、その恩恵を参加者が得て、市場全体を広げる領域（オープン領域）と、外部のプレーヤーには参加を許さず、技術や仕組みそのものを独自の取り組みに	簡略化及び状況の反映

4 ELSI: Ethical, Legal, and Social Implications

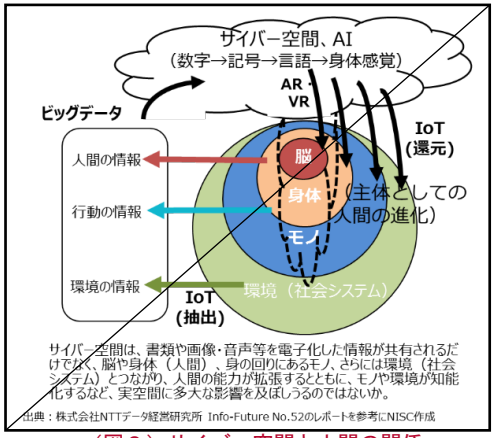
~~6 「ものづくり白書」（ものづくり基盤技術進行基本法第８条に基づく年次報告）2017 年版~~

改訂案	備考
よってブラックボックス化する領域（クローズ領域）を明確にすることである。セキュリティの問題についても、これまでは各企業がクローズに個々の製品や IT サービスと並んで、セキュリティ製品・サービスも提供してきた。しかし、これからの付加価値の力点が「サービス」「ソリューション」に移ると、例えば、利益率の低い傾向にあるオープン領域の製品に関する研究開発でしのぎを削るのか、利益率の高い傾向にあるサービス・ソリューションにおいてクローズ領域を設定し、全体のビジネスモデルを描く立場になるのかといった検討が必要になってくる。また、IoT システムの場合には、サイバー空間（例：ソフトウェアやデータ）と物理空間（例：ハードウェアやモノづくり）をクローズ領域にし、これらの空間をつなぐ領域は標準化を推進し、オープン領域に位置付け、市場の拡大を図りながら利益を得ていく、といった戦略の検討も必要である。そして、これらのオープン領域・クローズ領域それぞれにおいて、必要なセキュリティの研究開発をどのように位置付けて行うのかを考えることが重要である。この際、標準化されたオープン領域とクローズ領域が決まっているプラットフォーム以外でビジネスをしようとするとコストが非常に高くなり、プラットフォームのルールに従わざるを得ない状況となる。このため、このプラットフォームそのものを自社の競争優位にはたらくよう設計していく中での一要素としてサイバーセキュリティを位置づけ、どのようにその研究開発に取り組み、セキュリティ品質を高めていくのか、検討が必要である。  ~~（図８）ビジネスモデルの変化とそれに伴うセキュリティの位置付けの変化（イメージ）~~ **b．セキュリティ技術のオープン・クローズ戦略** サイバー攻撃は国境を越えて行われることから、高度化・巧妙化するサイバー脅威に対処するための技術的な取り組みに当たっては、国際的に連携して対応することが求められる。そのためには、各国が「強み」を有する技術を有機的に組み合わせ、発展させることが有効	簡略化

改訂案	備考
である。このため、研究の内容や我が国の安全保障上の問題にも留意しつつ、我が国の取り組みを積極的に海外に対して発信し、国際連携による研究開発を積極的に行っていくことが必要である。同時に、様々な国際標準化の取り組みが行われている中で、セキュリティ技術を中心とした様々な国際標準の策定・普及についても推進することが必要である。 　こうしたオープン領域に係る戦略と併せて、我が国の安全保障や競争力の観点から、外部にはオープンにしない独自の研究開発（クローズ領域）も重要である。こうしたクローズ領域の研究開発を行うためは、コンピュータやシステム等の原理・仕組みなどの理解と、それを自ら考え開発するために必要なコア技術が必要となる。これらの基盤技術自体は、直ちにビジネスにつながらないものであっても、クローズ領域の取り組みを図る上では必要となる可能性があるため、そうした技術を特定し、研究開発を推進することが重要である。いずれにしても、このように、国際連携によってオープンに研究開発を行うべき技術と、クローズ領域において必要な技術について、ポジショニングを行い、戦略的にセキュリティ技術の研究開発を進めていくことが必要である。 **⑤ イノベーションの「シーズ」としての研究開発の推進** 　ビジネスにおけるイノベーションからの「ニーズ」に応じて行うサイバーセキュリティの研究だけでなく、ビジネスのイノベーションにつながるような革新的なサイバーセキュリティ技術を生み出すための研究開発、換言すれば、ビジネスイノベーションに対する「シーズ」となるサイバーセキュリティ技術の研究開発についても、研究開発の検討においては考慮すべきである。例えば、公開鍵暗号方式（相手には公開鍵を伝え暗号化して送信をしてもらい、対となる秘密鍵で復号する方式。）の発明により、正規の受信者のみ安全に情報を得ることができる仕組みが実現し、電子商取引の発展などに大いに貢献したとされている。 	

改訂案	備考
## ３．中長期を見据えた考え方研究開発戦略 我が国が超高齢化社会と人口減少社会といった課題に直面する中、サイバー空間においては、IoT や AI、AR・VR により、実空間とサイバー空間の融合が高度に深化していく。それによって、人間の能力は拡張し、これまでの生活や労働を代替するにとどまらず、新たな価値を創造していくと考えられる。そして、より良い社会や人々の思いの実現につながっていく可能性がある。一方で、このように実空間とサイバー空間の融合が高度に深化していく中で、顕在化している目下の課題だけに囚われていると、現時点では容易に想定することが難しい未来の変化に対して脆弱な状況に陥る可能性がある。例えば、人間がネットワークに常時つながり、AI などによって能力が拡張した場合、自分の判断の主体は、自分なのか、ネットワークに常時つながった他者なのか、あるいは AI なのかが明確ではなくなり、自分と他者、組織、社会との境界、すなわち自己の概念が曖昧になっていく可能性がある。こうした中で、サイバーセキュリティの考え方として、サイバー空間を構成する情報システムに対する脅威への対応のみならず、人間社会を構成し、個々の機能を持つ様々なモジュール（人間と AI が一体になったもの（能力が拡張された人間）や、人間を取り巻く環境など）同士の関係性に着眼し、「人間とは何か」という問いかけをしながら、「情報システム」だけでなく、「人間」や「社会」を一体として捉えることが重要になってくると考えられる。本章では、多様な価値観を持つ人間の思いが実現でき、人間が安心して暮らすことのできる社会システムの実現に向け、想定することが難しい未来が起こりうる中長期を見据え、各組織が研究開発の方向性やテーマを議論するためのサイバーセキュリティの一つの考え方を示すこととする。	表現の見直し
### （１）情報通信技術（IT）の進化による人間の多様な価値観の実現 歴史的に、人間は「道具」を使い、「環境」を変えること、いわば人間の能力の拡張によって、文明が発展し、人間の生活を安全で豊かなものにしてきた。そして、１．（２）①で触れたように、人間は、情報通信技術（IT）の進歩によって、人間と情報の関係性については、①情報の環境化~~（インターネットの普及により、多くの情報が身の回りにあふれること）~~、②環境の情報化~~（IoT により、IT が実世界と結びつき、センサーが実世界から収集したデータを基に実世界を変えることができる時代）~~、さらには、③環境の知能化~~（実世界から収集したデータがビッグデータとして蓄積され、そこから有用な情報を取り出すために人工知能が活用されること）~~を実現してきた。こうしたサイバー空間の発展は、超高齢化社会と人口減少社会といった課題に直面する我が国において、質の高い遠隔医療や遠隔教育等をもたらすだけでなく、グローバルには、公共領域において必ずしも声を持てなかった社会的弱者や途上国の村落部に住む人々にもサイバー空間にアクセスし、情報収集や発信を可能とする変化をもたらすに至っている。今後さらに、全てがつながる環境が整備され（全てがつながることが発展し）、さらに以下に記載するような AI や AR・VR 等の情報通信技術（IT）のより一層の進化により、サイバー空間は、多様な価値観	第１章と重複するため簡略化

改訂案	備考
を承認し、人々の期待、物理的な欲求のみならず精神的な欲求をも満たし、より良い社会を形成する基盤として拡張していく可能性がある。 **① つながりの指数関数的な拡大と深化** IoT の普及によって環境の情報化が進んでいく中で、モノ同士の関係、人間とモノの関係や、社会とモノの関係、さらには、人間同士の関係までもが変化し、より密接で価値のあるつながりへと深化していく可能性がある。そして、今後は、人やモノから取得したデータの共有や活用にとどまらず、多様な物事のプロセスや人の豊かな体験までも結びつけるようになっていく可能性がある。 **② AI（人工知能）** いままでの人工知能は、人間が現実世界の対象物を観察し、「どこに注目」するかを見ぬいて（特徴量を取り出して）、モデルの構築を行った上で、その後の処理についてコンピュータを用いて自動で行うものであった。しかし、近年のコンピュータの演算能力の向上等により、人間の発達と同じような技術進化（認識能力の向上、運動能力の向上、言語の意味理解という順で技術が進展）が可能なディープラーニングによって、「与えられた目的」に対して、それを実現する手段は、学習を通じてますます賢くできるようになる。これによって、いままでは人間がモデルを改善することによって工業化を進めてきたが、モデルそのものが認識能力や運動能力を持つことによって根本的に産業の仕組を変える可能性がある。一方で、人工知能は、目的を与えられたときに、問題解決をすることにとどまり、生命のように自己の保存や複製、仲間を守るなどといった目的を持つものではない。このため、今後は、人間が人工知能に対して与える目的自体の是非の議論のほうがより重要となってくることに留意すべきである。 **③ AR（拡張現実）・VR（仮想現実）** サイバー空間においては、AR・VR 技術などによって、人間の物理空間の感覚をサイバー空間上で実現しようとする取り組みが行われている。AR 技術は、物理空間とバーチャル空間が連続することによって、高齢化社会においても、物理的・身体的制約のない生産、労働、創造性の提供が可能となる可能性がある。また、VR は、身体を介した一人称の体験をパブリッシュ（本人が知覚可能な体験として、コピー・伝送・再生）することが可能なシステムであり、その一つであるテレイグジスタンスによって、地域間の格差を減らすことが出来ることや、サイバー空間を使って他人に変身することによって、人種的な偏見の減少やうつ病の治療に貢献できる可能性がある。これらは、人間にこれまでになかった体験を提供し、人間の精神的な豊かさなどの高次の欲求を満たす上で、大いに貢献することが期待される技術である。	

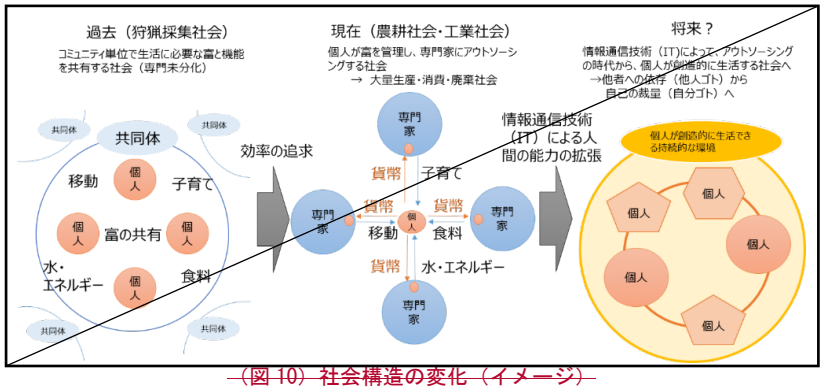
改訂案	備考
④ その他の技術の進展（クロスモーダルメカニズムの活用など） AI や AR・VR のように、既にその技術の実用化が進められており、人間が知っている能力の拡張だけでなく、今後、研究が進むことによって発見される、人間が未だ知らない能力の拡張の可能性があることにも留意をしていくことが必要である。~~例えば、人間の様々な感覚が互いに交わり、相互に作用することは、クロスモーダルメカニズムと言われており、それを活用することにより、イノベーションの可能性がある。人間の感覚のうち、文字や数字に色が付いて見えたり、何かを味わうと手に形を感じたりする現象は共感覚と呼ばれるが、今後、脳活動を可視化する技術が飛躍的に進み、共感覚の研究も進展を遂げ、様々なタイプの共感覚現象が脳の中で起こっていることが確かめられる可能性がある。また、共感覚が万人に備わった機能であるなら、それが VR や IoT、AI と連携し、クロスモーダルメカニズムを活用することにより、幅広いイノベーションの可能性を秘めている。~~ また、人間の脳と機械の情報伝達を仲介する機器の研究によって、バイオニック義肢を実現し、それは通常の人間の強度を超えたものとなる可能性も存在している。	文意に変更はなく簡略化
 ~~（図９）サイバー空間と人間の関係~~	簡略化
（２）サイバーセキュリティ研究の広がり~~考え方の再定義~~ 普通に使っている言葉が見方を縛ってしまうことがある。辞書に載っている意味も含めてその概念の中に既に現代的な偏りが潜んでいるので、このことを認識した上で考えてい	表現の見直し

改訂案	備考
かないと創造的な発想は生み出されない。例えば、~~「サイバー」という言葉の使われ方自身が既に歴史的に偏っている。一般に英語でも日本語でもサイバーという言葉は、インターネットが形成するであるとか、コンピュータに関するというような限定が付されていて、それらに関連する未来的な形容詞として固定されている。しかし原義であるノーバート・ウィナーの「サイバネティクス」は、人間を含む動物たちの身体とマシンとを、同一のメカニズムでコントロールするシステムを探索する新しい研究領域を指していた。サイバネティクスの副題が「Control and Communication in the Animal and the Machine」であることは示唆的で、主体としての人間とデバイスとしてのコンピュータのインターフェースそのものを問うものであった。当時の既存の述語は皆どこか一方に偏りがあり、この領域の将来の発展まで含めて論ずるには不適当であるとの自覚から「サイバネティクス」という新語が使われたのは教訓となる。すなわち~~「サイバー」という言葉が、対象でしかないコンピュータネットワークに視野が限られていることで、主体としての人間の能力やその変化に対する考察が弱くなっている可能性がある。情報機器によって構成される仮想上の空間としての「サイバー空間」のコントロールという議論だけになってしまうと、人間の能力の拡大や衰弱、感覚やリアリティの変化のコントロールが見落とされる危険性がある。本項では、将来的なサイバー空間の拡張を踏まえ、改めてサイバーセキュリティについて考えることとする。 **① 将来の技術進歩を基本とした考え方（フォアキャスト）** これまで、サイバーセキュリティについては、情報通信技術（IT）の進歩を見据え、攻撃に対する防御の構図の中で、予防・検知・防御・復旧のプロセスを着実に行うことを中心に、必要な制度設計や技術開発等が進められてきた。具体的には、マルウェア対策やDDoS対策、暗号、認証、マネジメント等が挙げられ、これらの技術は、これまでの構図の中で一定程度、有効に機能してきた。また、近い将来においては、攻撃に対して技術的な防御を高めていくアプローチだけでは問題解決が困難な可能性があることから、第２章で述べたように、今後は、ビジネスのプロセスやライフサイクルを含めて取り組み、多角的なアプローチによって対策が行われることも重要である。 さらに、（１）で示したように、コンピュータ能力の急速な向上をはじめとして情報通信技術（IT）は急速な進歩を遂げていることに加え、IoTやAIといった現時点で時代の主流となっている技術の先の様々な独自性の高い技術開発も行われている。これらの将来の技術の進歩が、攻撃に対する防御の構図の中で、人間に与える影響を見通す（フォアキャスト）ことにより、様々な研究開発のアイデアが生まれる可能性がある。例えば、以下に示すような、新たなサイバー空間上における攻防の問題が起こる可能性もある。[5] ・ 個人Ａの脳と連携したAI・ロボットが個人Ｂにより不正に操作され、個人Ｂが個人Ａを	文意に変更はなく簡略化

5 AIネットワーク化検討会議「AIネットワーク化の影響とリスク」（平成28年6月20日）

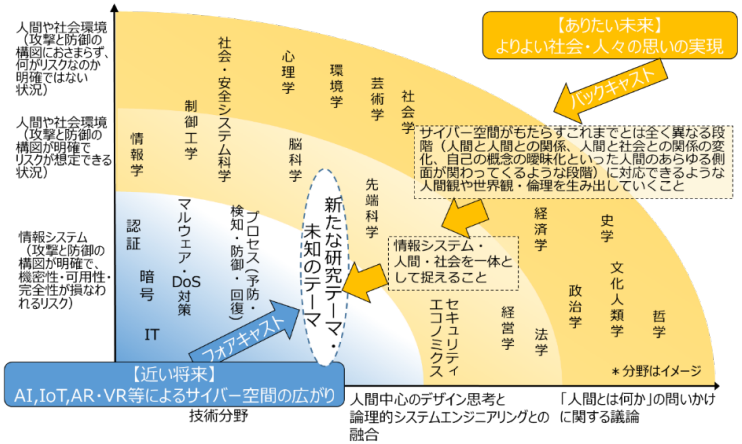
改訂案	備考
利用して犯罪を実行する、人間に対する乗っ取りのリスク ・ロボットにより摂取する情報等を操作されることにより、利用者の意思決定や判断のプロセスが操作されるリスク	表現の適正化
② フォアキャストのアプローチの限界 将来の技術進歩の外挿（フォアキャスト）によるアプローチは重要である一方、~~既に1960年代にマーシャル・マクルーハン は、「われわれはまったく新しい状況に直面すると、つねに、最も近い過去の事物とか特色に執着しがちである。われわれはバックミラーを通して現代を見ている。われわれは未来に向かって、後ろ向きで進んでいく」[8]と述べている。すなわち、~~現在の社会システムや人間観、世界観、倫理の常識が、未来においては根本的に変化してしまう可能性があるにもかかわらず、これらの常識を前提として技術進歩を外挿していくフォアキャストのアプローチのみでは限界が来る可能性がある。	文意に変更はなく簡略化
~~人類は、1万年ほど前に農耕が開始されるまでは、狩猟採集社会であったとされ、この社会では食料を獲得してから消費するまでには分配が繰り返されていたとする説や、優秀なハンターは、節制することにより、威信を獲得する機会を自ら制限したとする説などがあるが、基本的には、平等な人間関係を形成するための平準化メカニズムがあったとされている。その後、農耕社会以降の世界においては、食料を財として貯蓄することができるようになり、貨幣や金融を基本とした経済社会が発展し、工業社会になり大量生産、大量消費、大量廃棄が行われるようになった。その過程において、分業化、専門化による効率性が追求され、様々な経済社会の仕組みが形成された。~~	文意に変更はなく簡略化
~~この先、社会システムや人間がどのような変化を遂げるのかについて、例えば、マクルーハンの主張が参考になる可能性がある。マクルーハンは、メディアの効果や影響を「強化」「衰退」「回復」「反転」の4つの「問いかけ」をすることによって見るという理論（テトラッド）を唱えた。[9]この理論が示すように、ある価値観を持つ人間の期待や欲求を満たすための解決策を探り、ある側面が「強化」されると、それに伴ってある側面は廃れ、取って代わられる可能性がある（「衰退」）。同時に、かつて廃れてしまったものを「回復」したり、解決策が極限まで押し進められたときには、転じて何か別のものを生み出す可能性がある（「反転」）。これらのある側面が「強化」された結果による影響は、異なる価値観を持つ人々や社会に様々な副作用をもたらす可能性がある。例えば、貨幣や金融について考えると、これまでの経済社会の発展で経験したように、交換や消費、貯蓄や投資、さらには専門分化を「強化」することになる。一方で貨幣によらない信用の仕組や贈与経済を「衰退」させ、ヒエラルキーを「回復」させることになる。しかし、貨幣経済が先鋭化されていくと、「反転」として、デジタル通貨により格差は拡大し、多くの貨幣を「持たない人」は、貨幣による交換や消費がなかなかできなくなる中で、新しい生き方を模索していく可~~	文意に変更はなく簡略化

~~8 マーシャル・マクルーハンほか「メディアはマッサージである」（1967年）~~
~~9 マーシャル・マクルーハンほか「メディアの法則」（1988年）~~

改訂案	備考
~~能性がある。「シェアリング・エコノミー」は、その一つと捉えることができ、個々人が、専門性を伴わずに経済を営むライフスタイルが創造できる可能性がある。すなわち、これは貨幣経済の原理を推し進めていくことで、逆に貨幣を必要としない融通のソリューションが選択され、貨幣が「衰退」する可能性があることを示唆している。また、ものづくりについても、産業革命以来、生産と消費が分断され、多くの人々が生産者であることをやめ、大量生産で生み出された製品を一方通行で利用する消費者となっていたが、デジタルファブリケーションの進展によって、再び個人にものづくり力を取り戻すこととなり、個々人の価値観に応じた製造と利用とが双方向で行われる仕組みへと変化する可能性がある。さらに、身体の移動についても、テレイグジスタンスによって実際に身体を移動することなく、身体機能の瞬間的な空間移動を可能とすることで、「職場」と「住環境」の空間的制約から解放し、様々な労働参加を実現する可能性がある。このように、~~サイバー空間における情報通信技術（IT）の進化は、これまでの経済社会の中で形成されてきた、「雇用／被雇用」や「生産者／消費者」といった様々な関係が変質していく可能性を内包するものである。そして、潤沢な情報資源が共有され個々人に届けられる社会においては、アウトソーシングする時代から、創造的に生活する個々人の時代へと回帰~~「回復」~~し、他者に依存していた自分の生活を、自分のこととして創意工夫し自己実現を図り、それを人々の多様なつながりで共有することによって、さらなる創造を図ることが可能となる。  ~~（図 10）社会構造の変化（イメージ）~~ こうした考察から明らかなように、前提となっている知識を外し、壊すことによって、問題解決に向けた「問い」が深まり、動いていくということに留意する必要がある。その中で、サイバー空間が人間や社会にもたらすことについて、以下に関連する問題の例を示す。	表現の見直し 簡略化

改訂案	備考
a．感覚の一部が制限されたコミュニケーションによる影響 人間がサイバー空間に対して意識を向ける時間が増加し、現実空間において積み重ねる人生の「経験」よりも、サイバー空間における「経験」が増えている可能性すらある。~~これまで、人間は長い間、物理空間において他者を視ることや、声を聴くことだけでなく、匂いを嗅ぐ、身体に接触する、さらには、共感覚を使う、といったように、多彩な感覚によって世界を認識し、人間関係をつくりあげ、社会を形成してきた。~~サイバー空間への過剰な接続・依存は、人間にとって不変の生物学的条件としての感覚の一部が制限された状態のコミュニケーションに偏ることになり、情動や信頼に基づく人間関係や人間の「こころ」に影響を及ぼす可能性がある。	文意に変更はなく簡略化
b．人間の環境への適応の問題 人間の環境への適応を前提にすれば、新しい技術による環境の知能化によって、人間はその環境に適応する可能性がある。例えば、~~環境に応じて身体（感覚・運動）が適応的に変化する運動適応の例としては、~~情報通信技術（IT）の進展によって、モビリティの自動操縦の可能性が高まっているが、その結果、人間は操縦に必要な身体の能力が低下するリスクが挙げられる。情報通信技術（IT）の急速な発展によって人間の身体そのものに対し、何らかの影響を及ぼす可能性がある。	文意に変更はなく簡略化
c．知能化した環境からの影響により、自己の意志が希薄になる問題 人間にとってサイバー空間は、人間がつくりあげた道具にすぎない。しかし、サイバー空間においては、物理空間同様に、人間が意識を向けることによって人間が経験をし、影響を受ける場である。~~アフォーダンス理論においては、人間がその環境を探索することによって、環境自体が人間に対して意味を与えることを示唆しているが、サイバー空間によって、この意味づけがより強固なものとなり、人間が様々な影響を受ける。その結果、人間の主体性が分散化して、自他の境界が曖昧になる、自分、そして自分のまわりの社会はどうありたいかという意志が希薄になっていく可能性がある。すなわち、~~人間が、知能化した環境であるサイバー空間を通じて様々な恩恵を受ける一方で、サイバー空間に人間が操られるようにすらなる可能性や、自分そして、自分のまわりの社会は、どうありたいかといった自己の意志が希薄になっていく可能性がある。	文意に変更はなく簡略化
d．サイバー空間において異質性が共存するための調整 サイバー空間においては、物理空間における人間関係とは大きく異なり、人・モノの一部の側面がインターネットにより地球規模でつながっているため、むしろ、つながる人・モノの物理空間における経験などの違いに起因する異質性が顕著になっている可能性がある。~~例えば、地球上で生活を営む人々の価値観は、それぞれの国や地域の歴史や文化、宗教などによって形成されるとともに、その時代の社会・経済情勢からの影響を受け、極め~~	文意に変更はなく簡略化

改訂案	備考
~~て多様であり、時代によって変化していくものである。こうした価値観の多様性に加え、そこに AI という様々な価値観を持った人間の経験を学習した知能がつながることになる。このように、~~サイバー空間は、物理空間も含めた様々な環境や経験に基づく、多様な価値観を持った異質性が共存していることにより、イノベーションを生み出す場でもあると同時に、異なる価値観による対立を生み出す場ともなり得る。こうした対立の調整が様々な方法によって適切に行われることが必要である。	
③ サイバーセキュリティ研究の広がりの考え方の再定義 前提となっている知識を外し、壊した上で、未来の問題解決に向けた「問い」を深めていく上で、人間を中心に考えていくアプローチが重要になっている。~~「人間とは何か」という問いかけは昔から存在するが、現代においては、脳の機能の解明が進むなど、かつてない繊細なレベルで議論ができるようになっている。人間や社会環境をも巻き込んだサイバー空間の急速な拡大によって、「人間とは何か」という昔からの問いかけを、改めて議論せざるを得ない新しい時代を迎えているとも言える。~~サイバー空間がもたらす、これまでとは全く異なる段階（人間と人間との関係、人間と社会との関係の変化、自己の概念の曖昧化といった人間のあらゆる側面が関わってくるような段階）に対応できるような人間観や世界観・倫理を生み出していくことが人文社会学者に求められている。これは、人文社会科学が、突出した技術社会を監督・制御する構図ではなく、人文社会科学の役割について新たなフロンティアが出現しているとも言え、情報通信技術（IT）と関連する様々な分野との協業により、よりよい社会や人々の思いが実現できるようなありたい未来に向けて、新たな人間観・世界観・倫理が醸成されていくことが期待される。そして、その人間観・世界観・倫理の下で、~~新たなサイバーセキュリティの考え方として、~~「情報システム」だけでなく、「人間」や「社会」を一体として捉えることで、サイバーセキュリティ研究における新たなテーマや未知のテーマの発見やその広がりにつながるものと考えられる。それにより、多様な価値観を持つ人間の思いが実現でき、人間が安心して暮らすことのできる社会システムを創造し、人類社会の持続可能性という課題を世界に先駆けて解決することにつながる。	表現の見直し 簡略化 表現の見直し 表現の見直し



（図2~~11~~）サイバーセキュリティ研究の広がり

（３）想定できない変化に対応するための全体設計（デザイン）

バックキャストによるアプローチにおいて、想定できない変化に対応したサイバーセキュリティを考え、「情報システム」「社会」「人間」を一体として捉え研究開発の内容を検討する際、科学技術をベースとして、供給者主導で行うものだけでなく、社会的なプロセスやコミュニティによる需要者主導で行うものも必要である。その際の全体設計の方法論として、目的思考的に俯瞰性と系統性を論理的に考えるシステムエンジニアリングと、論理性では見えてこない人の感情的・感覚的側面を人間中心的に扱いながら多様性を活かして試行錯誤を繰り返すデザイン思考とを融合するアプローチが有効な可能性がある。

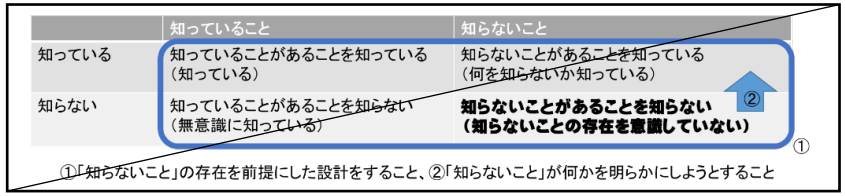
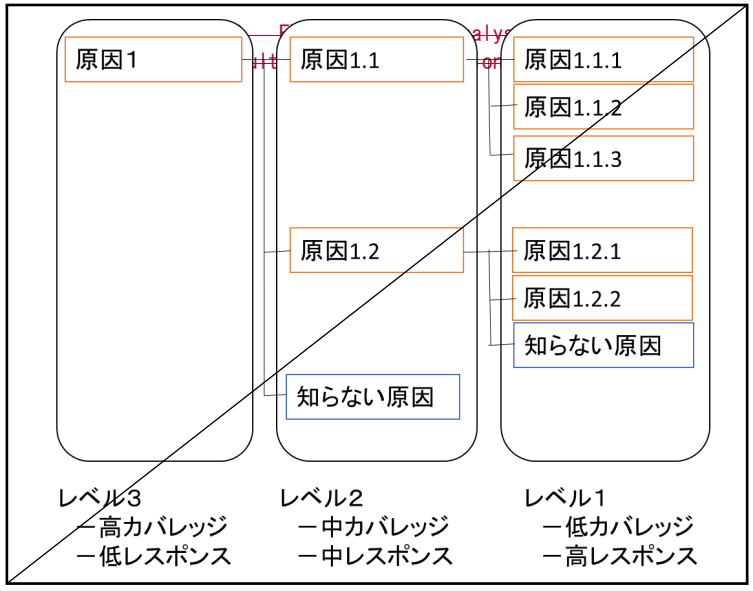
~~（図 12）は、人間と対象物との知っている・知らないの関係性を示したものであるが、右下の領域のように、~~人間には知らないことの存在すら認識していないことがあり、こうした問題はそれを取り巻く状況の変化によって顕在化する可能性がある。例えば、~~コロンブスの大航海を経た 16 世紀以降、嗜好品である「たばこ」は、「鎮静効果がある」として、世界中に広まっていった。20 世紀の前半までは、死因のうち、高い割合を感染症が占めていたが、感染症等の研究が進んだ結果、人間の寿命が大きく延びる一つの要因となる状況の変化があった。現在は、たばこが肺がんの原因の一つであり、肺がんは死因の第５位であることが知られているが、たばこと肺がんの因果関係について世界的に研究が進んだのは 1960 年以降である。すなわち、たばこは長い間「鎮静効果がある」として広く愛用されてきたが、人間の寿命が延びるという状況の変化によって、「がん」が死因の上位になり、発がんに関わる要因を探す疫学研究として、肺がんのリスク要因としてのたばこに関する研究が進んだ~~

文意に変更はなく簡略化

文意に変更はなく簡略化

改訂案	備考
~~とも考えられる。16 世紀から 20 世紀前半までの長い間、そのような研究の視点はなかった可能性が高い。[10,11,12]~~また、サイバー空間でいえば、電子メールの黎明期の 1980 年代に「標的型メール攻撃について知らない」ということを多くの人は意識していなかった可能性があり、標的型メール攻撃対策技術が進んだのは、2010 年以降である。~~このようなこれらの~~過去の例を踏まえると、①その仕組みの中で、「知らないこと」、すなわち知らないリスクや脅威があることを前提にした設計をすること、あるいは、②知らないリスクや脅威（未知のリスクや脅威）を明らかにしようとする努力、を実践していれば、その分野のセキュリティ技術で先手を打つことができる。特に、①のような設計は、デザイン思考でも行なわれているように、知らないことを見つけ出すための人間中心の試行錯誤的活動を内包した設計を目指したものであり、知らないリスクや脅威がどのようなものであったとしても、安全・安心を適切に確保できるようなシステムを考えることから始まるものである。その際、社会を構成する多様な人間の価値観や規範が多様であることを想定しておく必要がある。すなわち、対象（物）そのものに関する複雑性や不確実性だけでなく、向き合う人間の側からみたリスクや脅威に対する多義性を意識することが必要である。その中で、何を削減・回避すべき重大なリスクとみなすか、因果連鎖のうちでどこまで危害や便益として考慮すべき影響範囲とするかは一義的には決まらず、根本的には個人の価値判断に依存する。このため、合意形成の在り方については、必ずしも一意的なものではなく、リスクや脅威に対する多義性の中で、様々な考え方が共存する可能性がある。 ~~また、①を実現するための手段として、宇宙機の設計に用いられている手法が参考となる。宇宙機の設計においては、長いミッションにおいて自律的に内部の故障原因を検知し、対策を施すシステムの設計が不可欠である。そして、その故障原因は、設計段階で予め全てを知ることは困難である。このため、（図 13）に示すような階層化 FDIR 設計[13]という手法が採られるケースがある。これは設計時の故障の原因について、抽象度に応じてレイヤーを設け、それぞれのレイヤーごとに故障の原因を検知する仕組みを導入するものである。（図 13）のレベル 3 のレイヤーは最も抽象度が高く、下のレイヤーでは予め知ることができなかった原因も含め、広範囲の故障の原因をカバーすることができるが、一方で、このレイヤーでの検知では、より具体的な故障原因が生じてから時間が経っている可能性がある（低レスポンス）。このため、できるだけ、具体的な故障原因の検知も同時に行えるよう、可能な限り故障原因の想定は具体化もしておくことが必要である。~~	文意に変更はなく簡略化

~~10 JT ウェブサイト「たばこの基礎知識　世界の歴史」~~
~~https://www.jti.co.jp/tabacco/knowledge/society/history/world/index.html~~
~~11 日本学校保健会　喫煙防止教育パンフレットの解説　たばこの歴史~~
~~http://www.hokenkai.or.jp/3/3-5/3-55-01.html~~
~~12 WHO ファクトシート　死亡原因トップ 10（2015 年世界死亡原因トップ 10）~~
~~13 白坂成功、堀田成紀、蒲原信治「階層化 FDIR による高安全性航法誘導制御系の提案と宇宙ステーション補給機「こうのとり」での実現」、計測自動制御学会産業論文集、Vol. 10, No. 11, 91/99(2011)~~

改訂案	備考
このような、知らない（未知の）故障原因も含めてカバーしつつ、知っている（既知の）故障原因については、レスポンスの速度を確保するために設計に組み込むといった考え方、さらには、人々の異なる価値観や規範の多様性に起因するリスクの多義性を視野に入れる考え方は、情報通信技術（IT）の急速な進歩の中で、社会が変化し、多様な価値観を承認することにより人々の精神的な欲求までも満たせるようになっていく中で、情報システム、社会、人間を一体として捉え、安全・安心の観点を含めて全体を設計（デザイン）していく上で、活用できる可能性がある。	
	簡略化
~~（図 12）人間と対象物の知っている/知らないの関係~~	
	簡略化

改訂案	備考
４．研究・産学官連携の推進方策と産学官エコシステムの構築 （資料２－３を参照）	

改訂案	備考
## ~~4~~5．まとめ ・サイバーセキュリティの研究開発において、多様な価値観を持つ人間の思いが実現でき、人間が安心して暮らすことのできる社会システムを創造していくことを前提として、イノベーションを起こし、国際競争力の強化等を図っていくためには、近い将来と中長期的な社会・経済と情報通信技術（IT）の利活用の進化を視野に入れることが重要である。	
・基本的な考え方として、近い将来においては、後追い的な~~多層防御の~~サイバーセキュリティだけでは対処が困難な可能性があり、視野を広げてサイバーセキュリティ対策を捉え、研究開発に取り組んでいくことが期待されることを示した。	前章までの表現の見直しに伴うもの
・また、中長期的な視点においては、アウトソーシングする時代から、創造的に生活する個々人の時代へと回帰~~「回復」~~し、自分の生活を創意工夫して自己実現を図り、それを生活者同士で共有することによって、さらなる創造や共創が可能となるような時代へと変化する可能性を示唆し、サイバーセキュリティ研究の広がり~~の考え方を再定義~~（「情報システム」だけでなく、「社会」や「人間」を一体として捉えた新たなテーマ・未知のテーマの発見~~セキュリティ~~）がもたらす将来の可能性~~することが必要であること~~を示した。そして、サイバー空間がもたらす、これまでとは全く異なる段階（人間と人間との関係、人間と社会との関係の変化、自己の概念の曖昧化といった人間のあらゆる側面が関わってくるような段階）に対応できるような人間観や世界観・倫理を生み出していくことが重要であることを示した。	前章までの表現の見直しに伴うもの 前章までの表現の見直しに伴うもの
・今後、こうした考え方について、これまでのサイバーセキュリティ技術の専門分野にとどまらず、人文社会科学も含めた国内外の幅広い分野における研究組織や研究者に対し発信し、普及啓発活動に取り組むこととする。総合科学技術・イノベーション会議や IT 総合戦略本部等における取り組みとの連携を図りつつ、内閣サイバーセキュリティセンター（NISC）を中心に、我が国のサイバーセキュリティに関連する研究開発の状況について把握に努め、本戦略の内容について、フォローアップを行うこととする。併せて、NISC 及び関係府省庁の連携の下、具体的なサイバーセキュリティの研究分野やテーマについて検討を行うなど本戦略を具体化させるための取組を行い、適時、本戦略の見直しを検討することとする。	
・最後に、本戦略が我が国の研究機関・組織におけるサイバーセキュリティの研究開発について議論・検討を行う上で活用され、我が国の強みを活かしたイノベーションが実現し、各研究組織における取り組みがグローバルなサイバーセキュリティの向上に貢献できることを期待する。	

改訂案	備考
~~（参考）各府省の研究開発の例~~ 関係府省：各府省の研究開発の例 内閣府：・戦略的イノベーション創造プログラム（SIP）に「重要インフラ等におけるサイバーセキュリティの確保」を新規課題として追加し、府省庁の枠や旧来の分野の枠を超えた研究開発を推進 総務省：・標的型攻撃研究の基盤となる組織内ネットワークのリアルタイム分析環境及び大規模蓄積環境を整備（NICT） ・サイバー攻撃観測技術を高度化するための能動的観測システムの開発及び実証実験を実施（NICT） ・パーソナルデータの利活用に向け、暗号化したままビッグデータ解析や機械学習を行う技術を開発（NICT） ・IoT の展開に伴って生じる新たな社会ニーズに対応する機能性暗号や軽量暗号・認証技術を開発（NICT） 文部科学省：・M2M を含めたサイバー攻撃に関する通信データ等を収集し、共有する体制の構築を開始（NII） ・ビッグデータや AI（人工知能）等、社会・技術の変化を先取りした研究開発について推進 経済産業省：・システムの挙動を解析し、サイバー攻撃を検知する技術開発や、ホワイトリスト技術に関する研究を実施（CSSC） ・ソフトウェア工学について、大規模ソフトウェアの解析ツールを開発し、自動車等組込みシステムを題材に有効性を検証（AIST） ・暗号技術において、暗号化したままデータ処理や認証・認可を実現する高機能暗号技術について、高速処理を可能とする新方式や暗号文サイズが世界最小値となる技術を開発（AIST） 総務省・経済産業省：・暗号技術評価委員会及び暗号技術活用委員会を開催し、暗号技術の安全性に係る監視及び評価、新世代暗号に係る調査、暗号技術の安全な利用方法に関する調査、暗号の普及促進、セキュリティ産業の競争力強化に係る検討、暗号政策の中長期的視点からの取り組みの検討等を実施（NICT・IPA）	簡略化 （研究開発戦略専門調査会で別途整理（サイバーセキュリティ研究・技術開発取組方針（令和元年５月）等））