将来のICT社会における
サイバーセキュリティ研究・開発テーマの調査

2023年6月
内閣官房内閣サイバーセキュリティセンター(NISC)

※本調査はNISCの委託により、ボストン・コンサルティング・グループ合同会社が実施したものです。

Agenda

1. 目的・本プロジェクトの概要
2. ①守るべき対象・社会の変化に関する調査
3. ②ICT社会の変化に伴うセキュリティ課題の調査
4. ③研究・開発テーマの提言
5. 今後の研究・開発テーマの検討について

本事業の背景と目的、実施内容

背景と目的

2021年9月にサイバーセキュリティ戦略が改定され、
デジタルトランスフォーメーション(DX) とサイバーセキュリティの同時推進等のメッセージが盛り込まれる中、研究開発についてはサプライチェーンリスクへの対応やAIセキュリティ等の内容が盛り込まれた

その後、近年ではDXの普及とともに量子や6G (Beyond 5G) のような次世代技術の研究開発が進むとともに、国際情勢の複雑化、社会経済構造の変化等により、安全保障の裾野が経済分野やサイバー分野に急速に拡大し、経済安全保障推進法の成立や防衛3文書の改定等の動きが発生している

本事業の目的は、上記のような動向を踏まえつつ、
短期(2025, 6年頃)、中長期(2030年以降) 各々の観点で
ICT社会の変化を幅広に予測し、その社会の到来に備え先手を打つべく、注力すべきサイバーセキュリティ研究・開発テーマを発掘することにある

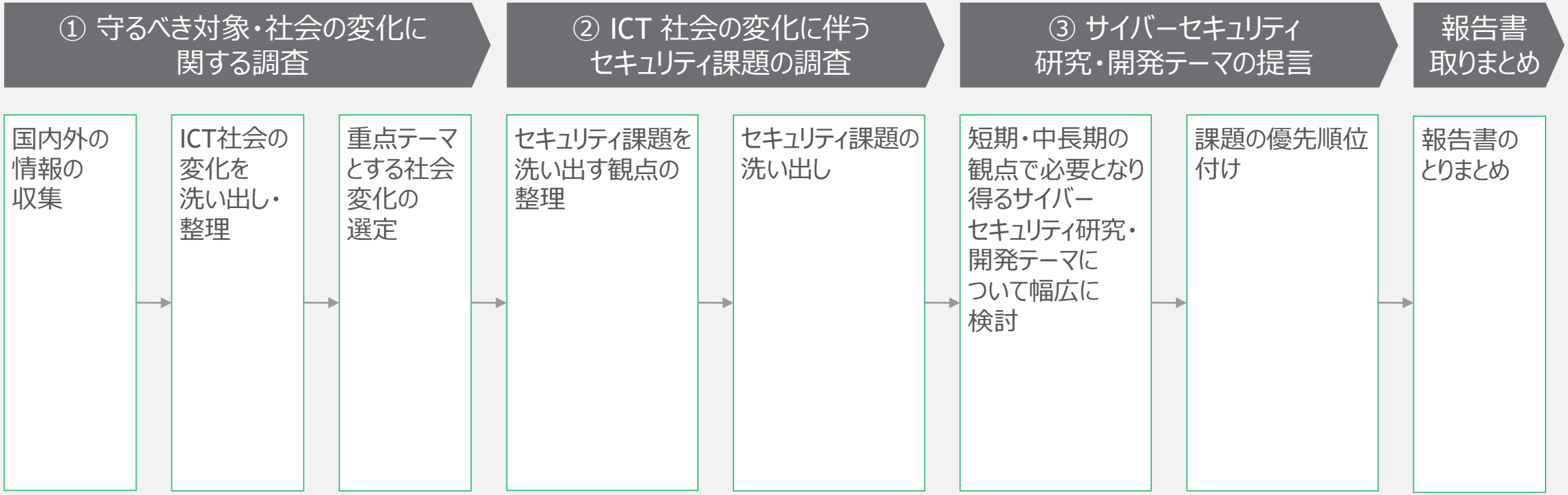
本調査研究の実施内容とゴール

- 下記の①～③を実施し、報告書にまとめる
  - ① 守るべき対象・社会の変化に関する調査
  - ② ICT 社会の変化に伴うセキュリティ課題の調査
  - ③ サイバーセキュリティ研究・開発テーマの提言

- 本事業のゴールとしては、先の通り、「短期 (2025, 6年頃)、中長期 (2030年以降) 各々の観点でICT社会の変化を幅広に予測し、サイバーセキュリティの研究・開発テーマの抽出及び優先順位付けを行う

※ただし、今後の方向性を決めるものではなく、あくまで様々な可能性を広い集めることで、今後の検討の一助とする

本事業の実施内容


① 守るべき対象・社会の変化に関する調査
② ICT 社会の変化に伴うセキュリティ課題の調査
③ サイバーセキュリティ研究・開発テーマの提言
報告書取りまとめ
国内外の情報の収集
ICT社会の変化を洗い出し・整理
重点テーマとする社会変化の選定
セキュリティ課題を洗い出す観点の整理
セキュリティ課題の洗い出し
短期・中長期の観点で必要となり得るサイバーセキュリティ研究・開発テーマについて幅広に検討
課題の優先順位付け
報告書のとりまとめ

Agenda

1. 目的・本プロジェクトの概要
2. ①守るべき対象・社会の変化に関する調査
3. ②ICT社会の変化に伴うセキュリティ課題の調査
4. ③研究・開発テーマの提言
5. 今後の研究・開発テーマの検討について

深掘りする社会変化選定基準の考え方

i インプットとなる国内外の情報を収集

国内外の国/企業の戦略レポートや、BCG内の知見を最大限活用して広くインプットを収集

- 国内外の幅広いレポートからの情報抽出
  - 「目指すべき社会の実現に必要な社会変化」を記載したバックキャスト系の資料と、「客観的に起こりうる社会変化」を記載したフォアキャスト系の資料の双方を参照
  - 加えて、発行主体の属性 (産業系/政府系/学問系) や、地域 (日本/米国/EU/その他) でも多様性を確保

ii ICT社会の変化を洗い出し・整理

iの検討結果を元に社会変化を整理。さらにICT社会の変化を抽出

- PESTを軸として、短期及び中長期における社会変化を整理。社会変化に対する守るべき対象も初期的に整理

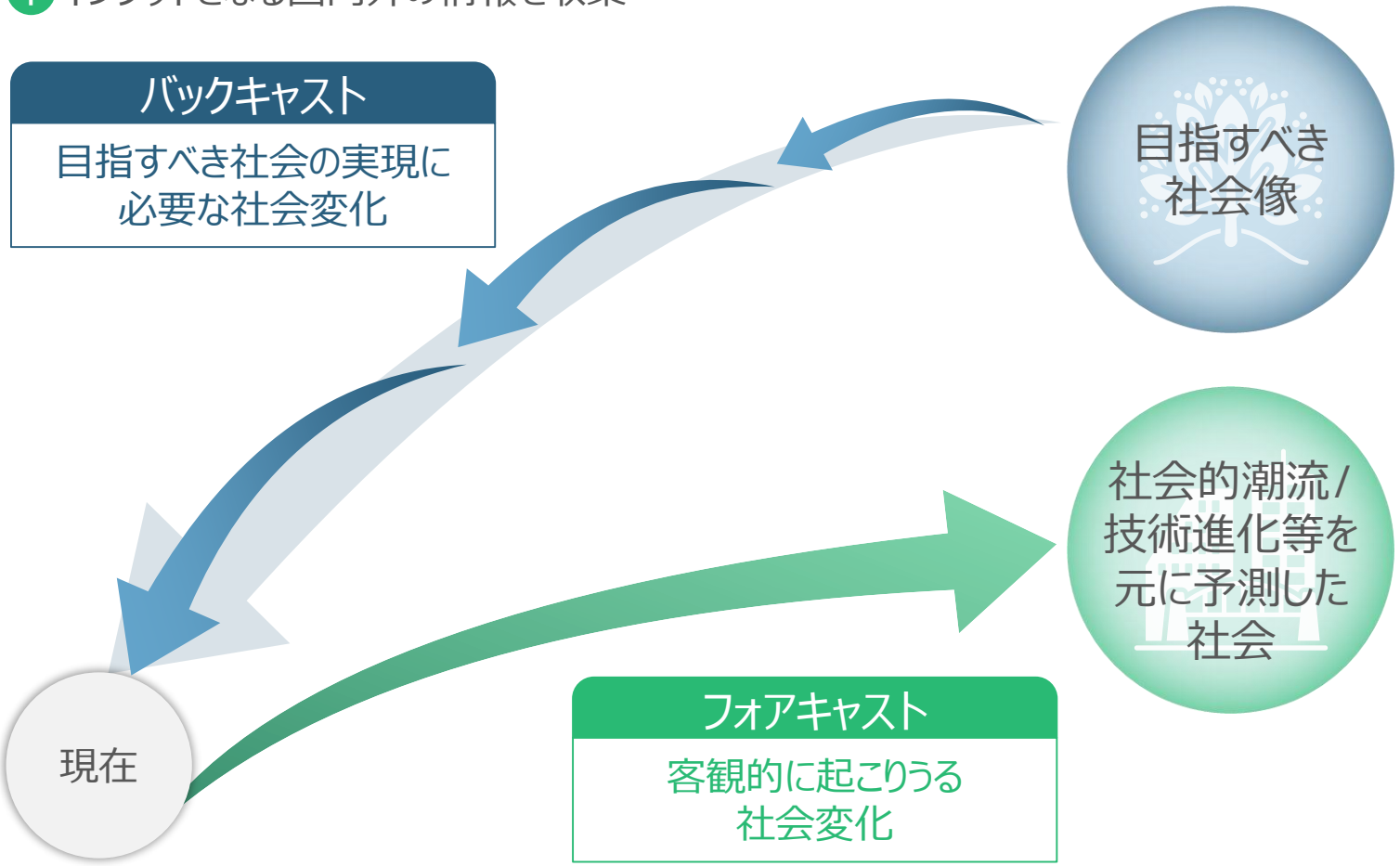
iii 重点テーマとする社会変化の選定

整理したICT社会変化の中で、どの変化を優先的に深掘りするかを重要性/実現可能性の観点から選定

- ICT社会変化において、特に重要性/実現可能性の高い社会変化を深掘りすべき重点テーマとして選定
  - 政府の他政策でも広く言及されている注目度の高い領域として、3つのテーマを選定
  - 上記以外で、幅広いレポートによって言及されている社会変化を選定

客観的な推論を元に社会変化を予測する「フォアキャスト」と、目指す社会像を定義し、実現されるべき社会変化を洗い出す「バックキャスト」の資料の双方を活用

ⓘインプットとなる国内外の情報を収集



客観的な「フォアキャスト」と目標から逆算する「バックキャスト」の双方の資料を併用

これにより幅広い社会変化を抜け漏れなく抽出する

産官学と国、社会変化の予測方法の観点から幅のある文献を設定

ⓘ インプットとなる国内外の情報を収集

分類	国名等		発表機関	資料名	フォアキャスト	バックキャスト
産業系	日本	1	MRI	未来社会構想2050	✓	✓
	日本	2	経団連	産業技術立国への再挑戦		✓
	日本	3	未来工学研究所	国・機関が実施している科学技術による将来予測に関する調査		✓
	米国	4	BCG	Mapping the Future: Megatrends Overview	✓	
	国際団体	5	World Economic Forum (WEF)	Global Risks Report 2022	✓	
政府系	日本	6	内閣官房	デジタル田園都市国家構想		✓
	日本	7	内閣官房	防衛3文書 (「国家安全保障戦略」・「国家防衛戦略」・「防衛力整備計画」)	✓	✓
	日本	8	総務省	2030年頃を見据えた情報通信政策の在り方		✓
	日本	9	総務省	令和4年版情報通信白書	✓	✓
	日本	10	文部科学省	令和2年版科学技術・イノベーション白書	✓	
	日本	11	国土交通省	国土の長期展望		✓
	米国	12	NIC	Global Trends 2040	✓	✓
	EU	13	欧州委員会	BOHEMIAの19の未来シナリオ		✓
	韓国	14	KISA	2030未来社会変化及びICT8大有望技術のサイバー脅威展望	✓	
学術系	日本	15	日本学術会議	未来からの問い	✓	✓
	米国	16	Wharton School	2030 How today's biggest trends will collide and reshape the future of everything	✓	

ICTと関連性の深い社会変化を10個抽出

1. 政治 (Political)

1A. 安全保障の難化
(サイバー安全保障の激化)

1B. デジタル国家の加速

2. 経済 (Economic)

2A. 経済安全保障の深化

2B. デジタル経済での
データの価値・重要性
の向上

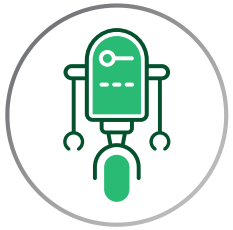
2C. 非対面サービス産業の
成長

3. 社会 (Social)

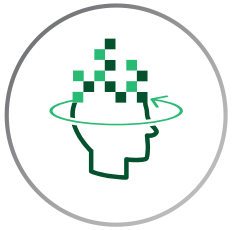
3A. デジタル空間の拡大
(仮想現実の拡大・実空間との融合)

3B. 生活インフラのデジタル化

4. 技術 (Technological)



4A. ヒトの物理的な活動を
代替する技術
(ロボット・ドローン) の
発展



4B. 人間機能の拡張

4C. 幅広い社会変化の
基盤となる情報処理
等の技術の革新

ICTと関連性の深い社会変化に関する潮流を整理 (1/2)

ii ICT社会の変化を洗い出し・整理

分類	変化の方向性	ICTに係る潮流	短期 (2025年頃)	中長期 (2030年頃)
1. 政治 (Political)	1A. 安全保障の難化 (サイバー安全保障の激化)	国家の安全保障として、陸海空の伝統的な手段に加えサイバー安全保障が重要な役割	• ウクライナ紛争を契機とした、国家間サイバー攻撃の増加 • 各国のサイバーセキュリティ組織の拡充 • 行政におけるサイバー空間の広がり • データ価値の重要性の拡大に伴う国家間のサイバー安保紛争の頻発	• 国家間のサイバー安全保障競争の激化 • 各国がハクティビストやハッカーグループを抱えることによる攻撃主体・手段の多様化/攻撃の常態化 • 急激な変化や権力の移動による紛争増加の可能性 • 中東や南アジアを中心とした地域的な不安定さが波及し、世界的な不安感の増加
	1B. デジタル国家の加速	議会や投票等の政府機能や国民が実施する各種申請や手続等の行政機能のデジタル化が加速する	• 行政手続きのデジタル化 • マイナンバーの活用の拡大 • ガバメントクラウドの導入 • デジタルに関わる法制度の拡充 • 政府主導のDXの加速化	• 政治活動のデジタル化 (オンライン投票、デジタル議会) • 信頼あるデータ流通 (DFFT) の実現・拡大 • 政府機能のクラウド化の進展 • ITによる社会インフラの効率的な維持管理
2. 経済 (Economic)	2A. 経済安全保障の深化	ICT発展の経済恩恵を受ける一方、ICT製品(ハードウェア・ソフトウェア)における海外依存やサプライチェーンマネジメントが、経済的な安全性を保障する上での懸念事項となる	• 社会基盤における海外製アセット (例: クラウド) 利用増加 • 国家/各企業の国内外へのサプライチェーンの広がり • 3Dプリンティング技術の産業利用増加 • 日本におけるデータセンターの一極集中の継続	• 社会基盤における海外製アセット (例: クラウド) への依存の増大 • デジタル化による、良好な地域経済循環の構築 • 成熟した3Dプリンティング技術によるグローバルバリューチェーンの変革 • データセンター地域被災による通信障害の可能性
	2B. デジタル経済でのデータの価値の向上/データを取り扱う技術の進化	データへの分析能力が高まるにつれデータがもたらす価値は向上し、様々なサービスへの利用のみならず経営判断へのインプットとしても重要な判断材料となる	• データドリブン経営の普及 • 情報銀行等の個人情報取り扱いサービスの台頭 • 個人情報関連規制の進化 • AIの進化によるデータ分析の効率向上	• デジタル経済でのデータの価値・重要性の向上 • データ産業の活性化に伴うブロックチェーンや量子計算機等の新技術の需要増加 • 個人情報保護に関する不安の増加に伴う関連技術開発需要の増加 • 各国間データ影響利用の増加によるデータ価値の向上

	2C. 非対面サービス産業の成長	対面で実施されていた銀行の窓口業務や購買手続等のサービスが、ICTの発展によりオンライン化・無人化が加速する	• 「非対面型ビジネスモデル」への転換 (セルフレジの普及等)
			• オンラインでの本人確認の常識化
			• 拡張現実の普及による物理サービスのデジタル化
			• ロボット技術の進化による単純労働のICT化
				• 非対面サービス産業の成長
				  - 無人店舗
				  - 遠隔医療
				  - 遠隔教育
				• 非対面のサービスの普及による雇用環境の変化

ICTと関連性の深い社会変化に関する潮流を整理 (2/2)

ⅱ ICT社会の変化を洗い出し・整理

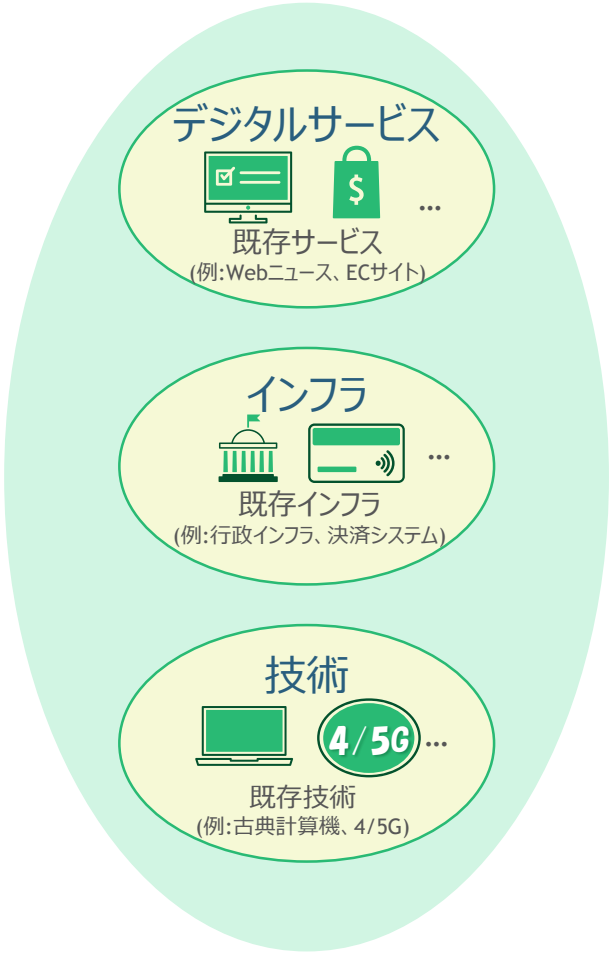
分類	変化の方向性	ICTに係る潮流	短期 (2025年頃)	中長期 (2030年頃)
3. 社会 (Social)	3A. デジタル空間の拡大 (仮想現実の拡大・実空間との融合)	ICTの発展によりデジタル空間が広がり、デジタル空間内においても実空間のような社会が形成され、仮想的な現実として多くの人がデジタル空間上で生活するようになる	• メタバース・デジタルツイン等仮想融合技術の台頭 • 仮想世界の広がり (AR,VR, MR) • IoT機器の発展による、インターネット接続機器の増加	• メタバースでの活動拡大 • 仮想現実の拡大・実空間との融合 • 通信の大容量化によるデジタル空間のリアルタイム性向上 • IoT機器の普及による、生活空間のデジタル化 • メタバース・デジタルツイン等仮想融合技術の普遍化 • ICT活用による地域企業の商圏拡大・地域の活性化
	3B. 生活インフラのデジタル化	金融サービスや交通手段等の生活インフラのデジタル化が進行し、災害対策や治安維持等の都市全体の機能もデジタル化する	• キャッシュレスの普及 • オンライン身分証明の普及 • モビリティ多様性拡大及び関連技術開発 (自動運転車、電動キックボード、電気自動車 等) • オンラインヘルスケアの台頭	• スマートシティの台頭 • 所有から共有、コト消費へとシフト • 自動運転技術の普及及び、一部で「空飛ぶクルマ」等も進展 • オンラインと対面を組み合わせた、多様なニーズを満たすヘルスケアの実現 • ICTによる省電力化の進展とグリーン社会実現への貢献

4. 技術 (Techno-logical)	4A. ヒトの物理的な活動を代替する技術(ロボット・ドローン)の発展	単純作業を基点に人間が実施していた作業をロボットが実施するようになり、将来的には人間と同等の動作をし人間の生活を支えるようになる	• 特定産業におけるロボット利用の拡大
			  - 物流
			  - 農業
			  - 介護・医療
			  - 災害現場
				• 特定産業に限らない日常へのロボットの普及
				• 分身ロボット/アバターと呼ばれる自分自身の分身の実現
				• 災害対策ロボット、宇宙ロボットの実現
				• 生活支援 (ロボットアシスタント、小型外骨格 等)

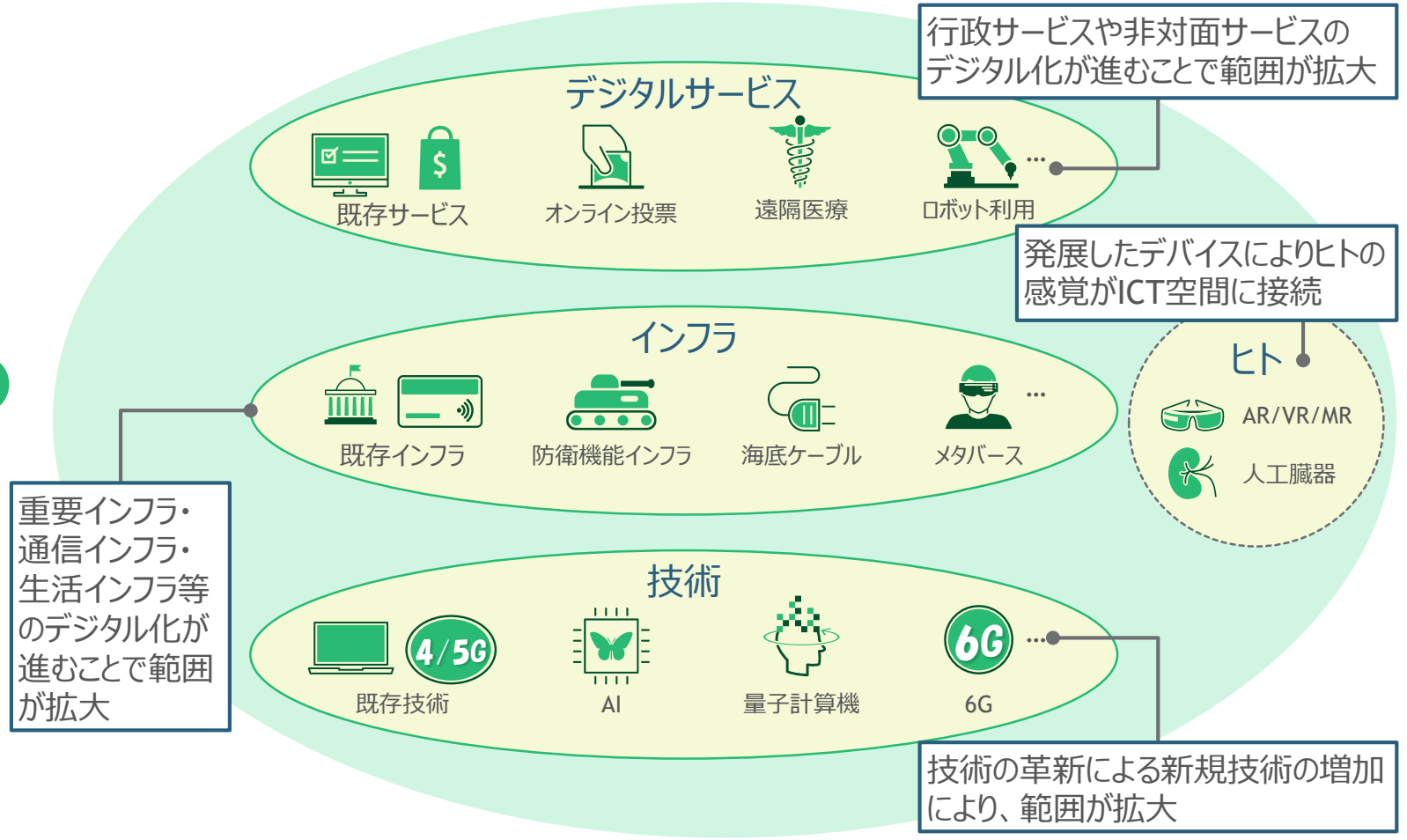
	4B. 人間機能の拡張	ICTの発展が、身体 (外骨格・義体等)・知覚 (感覚の拡張/置換)・存在 (デジタルによる体外離脱 等)・認知 (AIと人間の融合) の4方向から人間機能を拡張する	• 身体機能を拡張・代替する技術の発展 • 専用デバイスを用いた他人の視点のジャック • 仮想世界の広がり (AR,VR, MR)	• 技術による身体機能の拡張・代替によるハンディキャップの克服 • アバターを用いたデジタル空間へのダイブ • 人工臓器の発展による、人間の臓器の簡単な置換 • ブレインテック×サイバーの台頭
	4C. 幅広い社会変化の基盤となる情報処理等の技術の革新	6Gのような新しい通信技術や量子計算機のような新しい計算技術によって、デジタルにおけるケイパビリティが大幅に向上し、ICTにおけるパラダイムシフトが起き得る	• 量子計算機の台頭 • AIの利用シーン増加 • 5Gの普及による、IoTの促進 • ブロックチェーン/Web3.0の進展	• 量子計算機の浸透 • AIの進化 (人間並みの知能→シンギュラリティ) • 6Gの実用化

デジタル化範囲の拡大や新規技術の台頭によって、守るべき対象の範囲も拡大

現状の守るべき対象イメージ



中長期以降の守るべき対象イメージ



それぞれの社会変化による守るべき対象の変化を整理(1/2)

分類	変化の方向性	守るべき対象		守るべき理由
		現状	中長期以降	
1. 政治 (Political)	1A. 安全保障の難化 (サイバー安全保障の激化)	• 行政システム • 重要インフラ • 国家や企業の機密情報	• デジタル化範囲の広がった行政システム • 防衛系システム等を含む、デジタル化範囲の広がった重要インフラ • 国家・企業のデジタル化の加速により増加した国家や企業の機密情報 • 海底ケーブルなどの通信インフラ	• 国家機能を支える行政システム・重要インフラ(特に防衛系システム)や機密情報に対する、サイバー犯罪・テロ拡大等のリスクが高まっているため • 海底ケーブルなどの通信インフラへの攻撃によりデジタル空間で孤立する危険性があるため
	1B. デジタル国家の加速	• 行政システム • デジタルID • デジタルIDに紐づく個人情報	• デジタル化範囲の広がった行政システム • 完全に普及したデジタルID • デジタルIDに紐づく個人情報	• デジタル国家の機能を停止する攻撃のリスクが高まっているため • データ流通が広がる中、マイナンバー等のデジタルID及びそれに紐づく個人情報の漏洩や不正利用のおそれがあるため
2. 経済 (Economic)	2A. 経済安全保障の深化	• 海外アセット(情報基盤やサービス、API)を利用するシステム	• 国家・企業のデジタル化の加速により増加した海外アセット(情報基盤やサービス、API)を利用するシステム	• 広く利用されている海外アセット(情報基盤やサービス、API)の調達リスクや急な停止リスク、その他のサプライチェーンリスクは経済活動に甚大な影響を与えるため
	2B. デジタル経済でのデータの価値・重要性の向上	• データ • データ価値を生み出すデータベース、ソフトウェア、アルゴリズム	• 国内外で流通され、増加したデータ • 国内外の人のデータ主権 • データ価値を生み出すデータベース、ソフトウェア、アルゴリズム	• データ価値が増大する中、データ主権やデータ自体を保持することの重要性が高まっているため • データベースやソフトウェア、アルゴリズムによって上記のデータ価値が担保されているため
	2C. 非対面サービス産業の成長	• 限定的な非対面サービス/インフラ	• 非対面サービス • 非対面サービスを支えるインフラ • 利用するユーザの正当性	• 非対面サービスが社会における重要度を増しており、停止等のリスクが発生した際の社会影響が高まっているため • 非対面のため従来よりなりすましリスクが高くなるため

それぞれの社会変化による守るべき対象の変化を整理(2/2)

分類	変化の方向性	守るべき対象		守るべき理由
		現状	中長期以降	
3. 社会 (Social)	3A. デジタル空間の拡大 (仮想現実の拡大・ 実空間との融合)	• Web1.0~2.0でつながっているデジタル機器等	• メタバースに関わるプラットフォーム • メタバースアカウント • メタバース上の所有物・著作権 • メタバースに接続される物理的デバイス(AR/VR/MR)	• メタバースが社会でより広く活用されることに伴い、プラットフォーム、アカウントの侵害が個人や社会機能に与える影響が高まりうるため • メタバース上での所有物・著作物の普及や、その価値の向上に伴い、その侵害リスクも高まるため • メタバースに接続される物理的デバイス(AR/VR/MR)の普及に伴い、乗っ取りのリスクも高まるため
	3B. 生活インフラのデジタル化	• 限定的なデジタル化された生活インフラ(銀行の勘定システムなど)	• デジタル化された重要インフラ生活に関わる電子機器 • 個人情報・生活に関わるデータ	• 重要インフラ(電力・ガス・水道網・医療サービス・交通網(自動車・鉄道・航空)・物流サービス・金融機関・産業系インフラ)のデジタル化により、サイバー犯罪のリスクが高まるため • 生活に関わる電子機器(ウェアラブルデバイス、カメラ、メーター等)により多くの個人情報・生活データが蓄積されるようになるため
4. 技術 (Techno-logical)	4A. ヒトの物理的な活動を代替する技術 (ロボット・ドローン) の発展	• 限定的に利用されているロボット・ドローン	• 人命／身体の安全 • 施設 • インフラ • ロボット・ドローン	• ロボット・ドローンの誤作動や乗っ取り、機能停止等が、人命／身体の安全や施設・インフラの侵害に繋がるため
	4B. 人間機能の拡張	• 特になし	• 本来の人間機能 • 人間機能を拡張するデバイス・サービス	• 人間機能を拡張するデバイスやサービスの誤動作や乗っ取りは、国民生活に影響を与えるだけでなく、本来の人間機能にも影響を与えうるため
	4C. 幅広い社会変化の基盤となる情報処理等の技術の革新	• 従来から利用されている技術	• 既存の暗号化方式 • 既存の暗号化方式によって暗号化されたデータ • 量子コンピュータ・量子ネットワーク • AI • 情報通信の発達により仮想化された通信インフラ • 物理的なインフラ	• 既存の暗号化方式やそれによって暗号化されたデータが、量子コンピュータ関連技術の進展に伴い、陳腐化しうるため • 量子コンピュータ・量子ネットワークの実用化により不正な動作や乗っ取りリスクが高まるため • AIの活用が社会で広がることで、不正な動作や乗っ取り、機能停止等の社会的影響が高まるため • 情報通信の発達により拡大した仮想化された通信インフラや、物理的なインフラの不正な動作や乗っ取り、機能停止等のリスクが高まるため

(参考) ICTの発展以外が主たる要因である社会変化も含む社会変化一覧

ii ICT社会の変化を洗い出し・整理

青字: ICTの発展が主たる要因の社会変化　　黄字: ICTの発展以外が主たる要因の社会変化

分類	変化の方向性	潮流
1. 政治 (Political)	安全保障の難化 (サイバー安全保障の激化)	国家の安全保障として、陸海空の伝統的な手段に加えサイバー安全保障が重要な役割を果たすようになる
	デジタル国家の加速	議会や投票等の政府機能や国民が実施する各種申請や手続等の行政機能のデジタル化が加速する
	政府の役割の変化	市民主導型の社会課題の解決社会や行政サービスの効率化により、政府の求められる役割が変化する
2. 経済 (Economic)	経済安全保障の深化	ICT発展の経済恩恵を受ける一方、ICT製品(ハードウェア・ソフトウェア)における海外依存やサプライチェーンマネジメントが、経済的な安全性を保障する上での懸念事項となる
	デジタル経済でのデータの価値の向上 / データを取り扱う技術の進化	データへの分析能力が高まるにつれデータがもたらす価値は向上し、様々なサービスへの利用のみならず経営判断へのインプットとしても重要な判断材料となる
	非対面サービス産業の成長	対面で実施されていた銀行の窓口業務や購買手続等のサービスが、ICTの発展によりオンライン化・無人化が加速する
	循環社会への変化	脱炭素化の浸透による再生可能エネルギーやシェアリングエコノミーの普及により、循環社会になり環境負荷が低減
3. 社会 (Social)	デジタル空間の拡大 (仮想現実の拡大・ 実空間との融合)	ICTの発展によりデジタル空間が広がり、デジタル空間内においても実空間のような社会が形成され、仮想的な現実として多くの人がデジタル空間上で生活するようになる
	生活インフラのデジタル化	金融サービスや交通手段等の生活インフラのデジタル化が進行し、災害対策や治安維持等の都市全体の機能もデジタル化する
	雇用体系の変化	テレワークの普及や自由業の増加による働き方の変化や、AIの普及による人に求められるスキルの変化が発生する
	人口動態の変化	少子高齢化の進行や健康機関の延長、移動手段の発展により、都市部/地方部の人口比率や年齢層が変化する
	コミュニティの多様化	移動手段やデジタルの発展から物理的距離・言語の壁が解消され人との関わり方が変化し、コミュニティが多様化する
4. 技術 (Techno-logical)	ヒトの物理的な活動を代替する技術 (ロボット・ドローン)の発展	単純作業を基点に人間が実施していた作業をロボットが実施するようになり、将来的には人間と同等の動作をし人間の生活を支えるようになる
	人間機能の拡張	ICTの発展が、身体 (外骨格・義体 等)・知覚 (感覚の拡張/置換)・存在 (デジタルによる体外離脱 等)・認知 (AIと人間の融合) の4方向から人間機能を拡張する
	幅広い社会変化の基盤となる情報処理等の技術の革新	6Gのような新しい通信技術や量子計算機のような新しい計算技術によって、デジタルにおけるケイパビリティが大幅に向上し、ICTにおけるパラダイムシフトが起き得る

政府の他政策でも広く言及される3つのテーマ (1A, 2A, 3A) をまず重点テーマとして選定。加えて、言及するレポート数が多い社会変化を重要性/実現可能性の高い変化と判断

ⅲ 重点テーマとする社会変化の選定

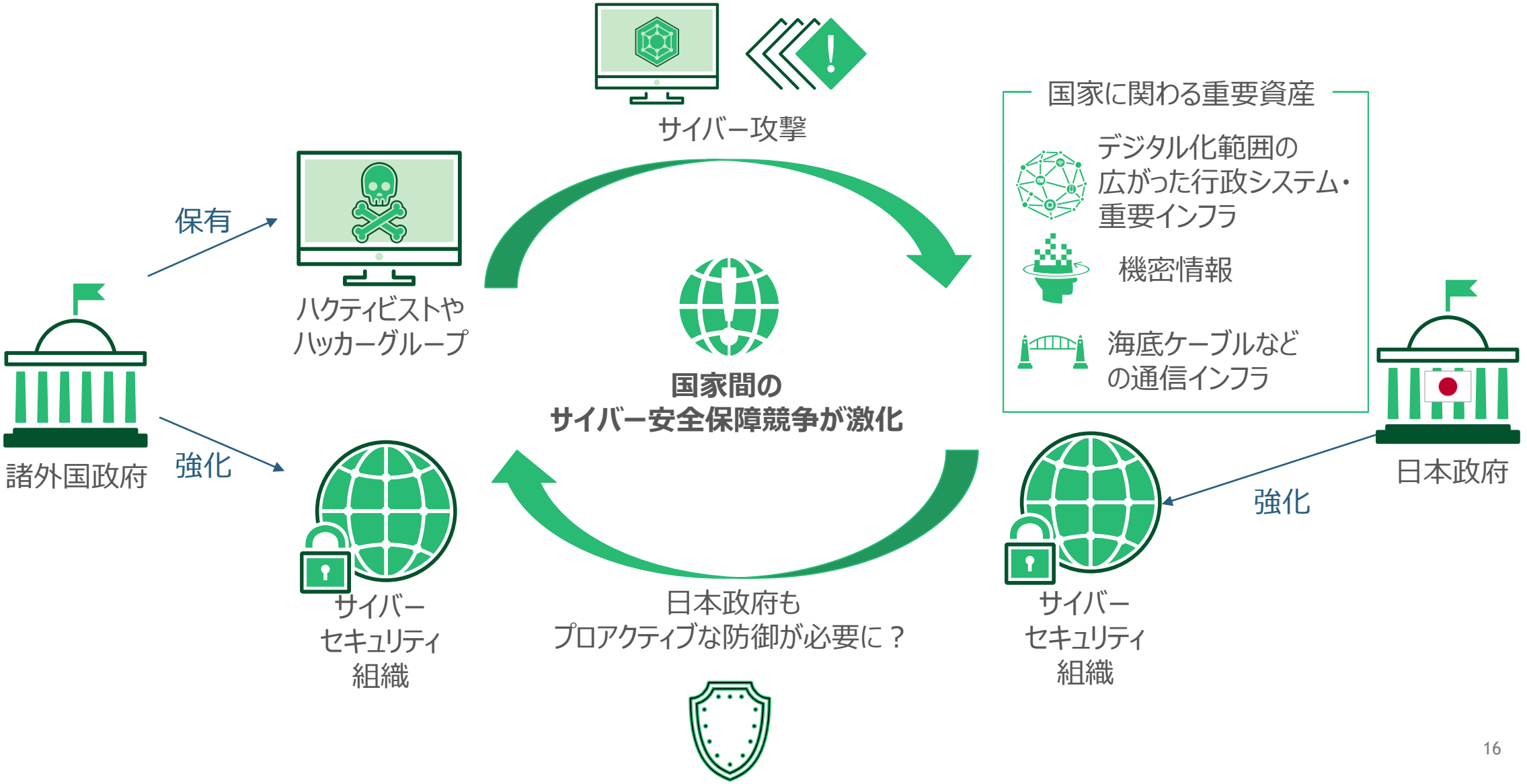
考え方

- 政府の他政策でも広く言及されている領域として、注目度の高い3つのテーマ (以下1A, 2A, 3A) を選定
- 加えて、資料の75% (12以上) のレポートで言及されている社会変化を重要性/実現可能性の高い変化として追加

分類	変化の方向性 ■: 重点テーマ	産業系					政府系									学術系	
		1 MRI	2 経団連	3 未来工学研究所	4 BCG	5 WEF	6 内閣官房① (デジ田)	7 内閣官房② (防衛)	8 総務省① (2030の在り方)	9 総務省② (情報通信白書)	10 文部科学省	11 国土交通省	12 NIC	13 欧州委員会	14 KISA	15 日本学術会議	16 Wharton School
1. 政治 (Political)	1A. 安全保障の難化 (サイバー安全保障の激化)	✓		✓	✓	✓		✓	✓				✓	✓	✓	✓	
	1B. デジタル国家の加速						✓		✓	✓		✓		✓	✓		
2. 経済 (Economic)	2A. 経済安全保障の深化	✓	✓		✓	✓	✓	✓	✓	✓			✓			✓	✓
	2B. デジタル経済でのデータの価値・重要性の向上				✓					✓			✓	✓	✓	✓	
	2C. 非対面サービス産業の成長			✓						✓	✓	✓			✓		✓
3. 社会 (Social)	3A. デジタル空間の拡大 (仮想現実の拡大・実空間との融合)	✓	✓	✓	✓	✓			✓	✓	✓	✓			✓		
	3B. 生活インフラのデジタル化	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓		✓
4. 技術 (Techno-logical)	4A. ヒトの物理的な活動を代替する技術 (ロボット・ドローン) の発展		✓	✓	✓		✓		✓	✓	✓		✓	✓		✓	✓
	4B. 人間機能の拡張		✓	✓		✓					✓			✓			✓
	4C. 幅広い社会変化の基盤となる情報処理等の技術の革新	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓

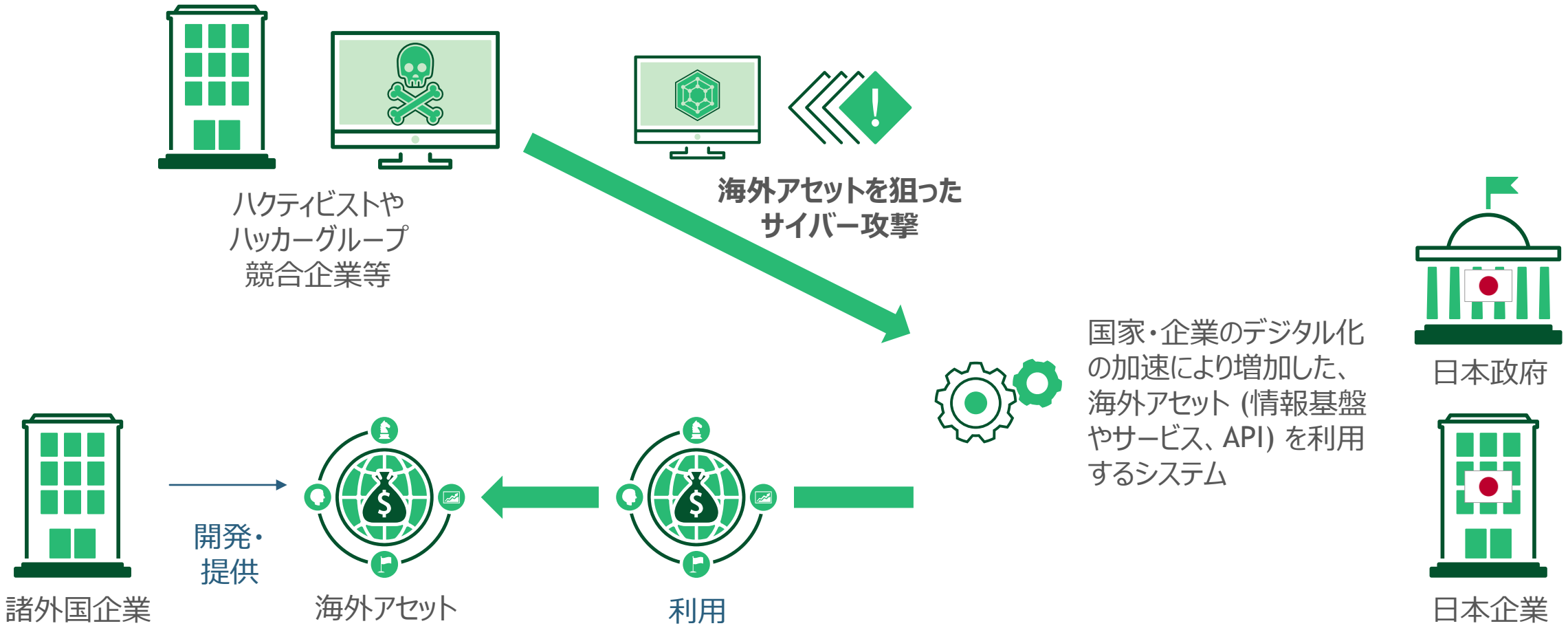
国家の安全保障として、陸海空の伝統的な手段に加えサイバー安全保障が重要な役割を果たすようになる

「1A: 安全保障の難化 (サイバー安全保障の激化)」のイメージ



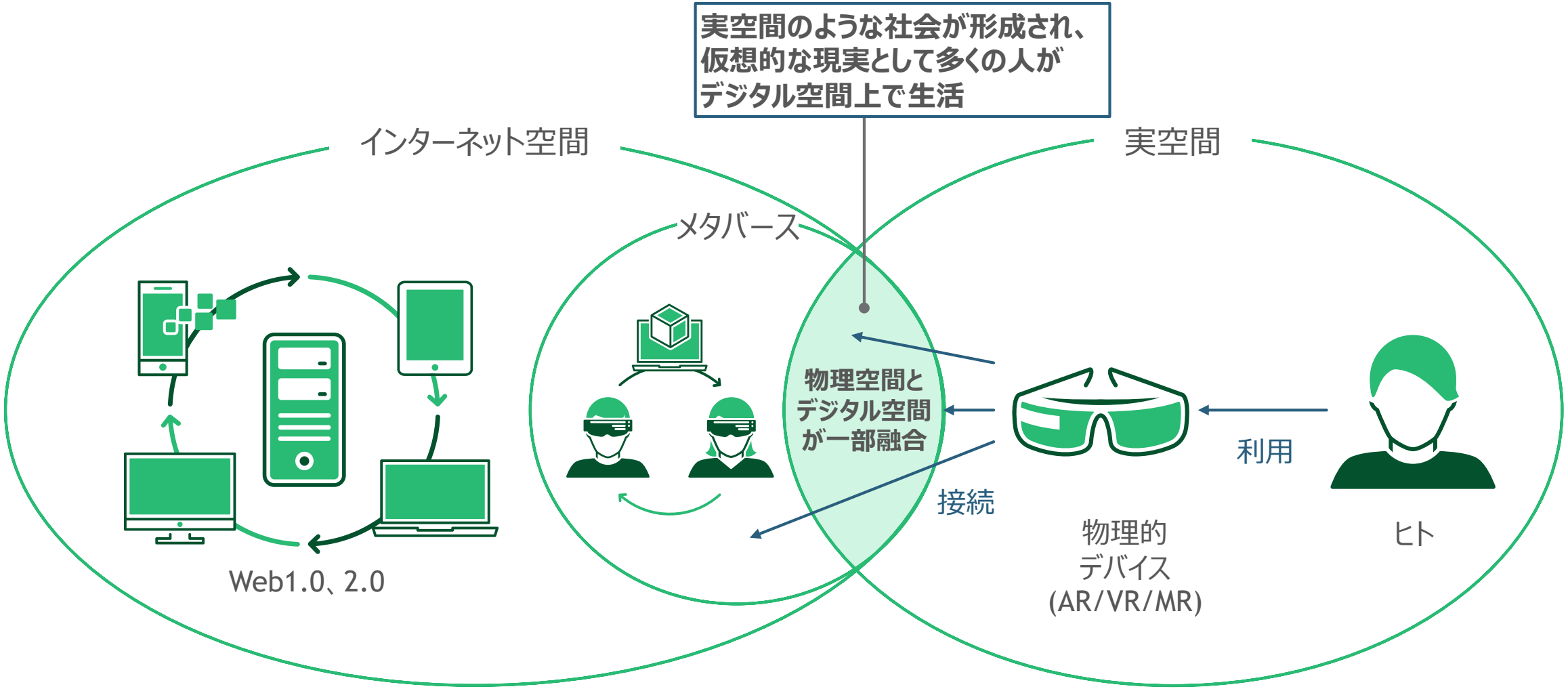
ICT発展の経済恩恵を受ける一方、ICT製品(ハードウェア・ソフトウェア)における海外依存やサプライチェーンマネジメントが、経済的な安全性を保障する上での懸念事項となる

「2A: 経済安全保障の深化」のイメージ



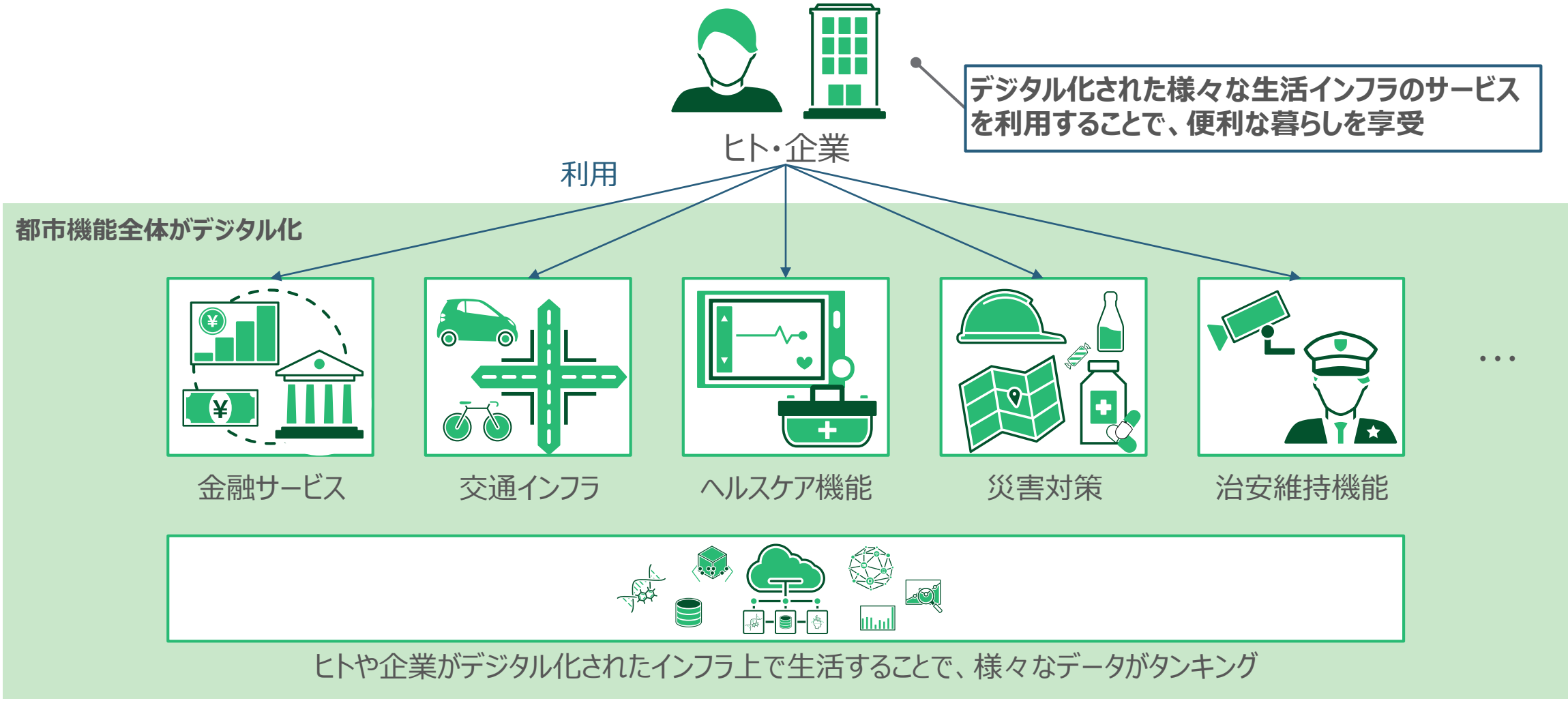
ICTの発展によりデジタル空間が広がり、デジタル空間内においても実空間のような社会が形成され、仮想的な現実として多くの人がデジタル空間上で生活するようになる

「3A: デジタル空間拡大 (仮想現実の拡大・実空間との融合)」のイメージ



金融サービスや交通手段等の生活インフラのデジタル化が進行し、災害対策や治安維持等の都市全体の機能もデジタル化する

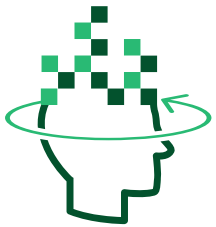
「3B: 生活インフラのデジタル化」のイメージ



6Gのような新しい通信技術や量子計算機のような新しい計算技術によって、デジタルにおけるケイパビリティが大幅に向上し、ICTにおけるパラダイムシフトが起き得る

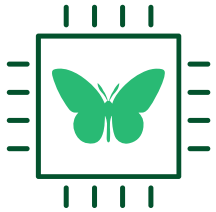
「4C: 幅広い社会変化の基盤となる情報処理等の技術の革新」のイメージ

情報処理等の技術革新要素



AIの進化
(人間並みの知能→シンギュラリティ)

…



量子計算機

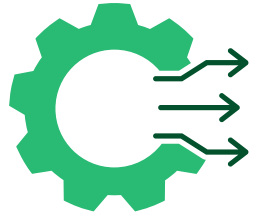
6G (Beyond 5G)

プラスの影響

マイナスの影響

技術革新により、ICTにおけるパラダイムシフトが発生

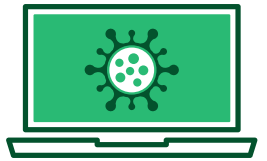
デジタル空間の拡大



生活インフラのデジタル化

…

古い暗号化技術の解析



新型マルウェアの自動作成

…

Agenda

1. 目的・本プロジェクトの概要
2. ①守るべき対象・社会の変化に関する調査
3. ②ICT社会の変化に伴うセキュリティ課題の調査
4. ③研究・開発テーマの提言
5. 今後の研究・開発テーマの検討について

ICT 社会の変化に伴うセキュリティ検討課題の調査の考え方

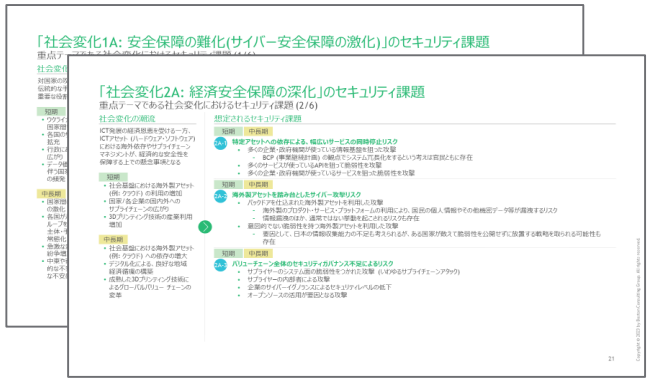
考え方

海外の政府におけるサイバーセキュリティの取組の調査、各種ガイドライン、情報発信資料、BCG社内の知見等のリソースを活用しつつ、短期・中長期の各社会変化に伴うセキュリティ課題を幅出

- 以下のようなリソースを含む、各種リソースを活用
  - 海外におけるサイバーセキュリティの取組の調査資料
    例) Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats(CISA)
  - 各種ガイドライン
    例) 自動運転車の安全技術ガイドライン(国土交通省)/IoT セキュリティガイドライン(総務省)
  - ニュース記事
    例) 機械学会誌 特集「つながる機械 機会と通信の融合」寄稿「自動車分野のサイバーセキュリティの展開」(MRI)

各専門分野への造詣の深い大学教授やテクノロジー企業のエキスパート等の有識者へのヒアリングを通して、上記で幅出ししたセキュリティ課題を補完

- 以下のような有識者を含む、24名へヒアリングを実施
  - 秘密計算、データマイニング、インテリジェントユーザインタフェースを専門とする教授
  - サイバー/情報セキュリティ、電子認証付署名、電子政府システムを専門とする教授
  - アクティブサイバーディフェンス等の最先端セキュリティを扱う会社のCEO



各社会変化に紐づくリスクを
大項目レベルで20、
中項目レベルで80抽出
後段で研究テーマを検討できるレベルまで具体化

重点テーマである社会変化について、重要な研究テーマに繋がりうるセキュリティ課題を整理

社会変化のセキュリティ課題の整理

社会変化	ICTに係る潮流	想定されるセキュリティ課題
1A: 安全保障の難化 (サイバー安全保障の激化)	国家の安全保障として、陸海空の伝統的な手段に加えサイバー安全保障か重要な役割を果たすようになる	• 戦争のハイブリッド化 (物理的な攻撃とサイバー攻撃の融合が進む) に伴い、サイバー攻撃により国として機能不全を起こされるリスク • サイバー攻撃によりサイバー諜報 (cyberespionage) をされるリスク • 情報の兵器化により、内政のコントロールを失うリスク • 旧来的な軍事力と同様、サイバー安全保障分野での対応能力が外交上の発言力に影響する可能性 • 攻撃手法の多様化による守るべき対象の拡大に伴う、慢性的なセキュリティ対策リソース不足
2A: 経済安全保障の深化	ICT発展の経済恩恵を受ける一方、ICTアセット (ハードウェア・ソフトウェア) における海外依存やサプライチェーンマネジメントが、経済的な安全性を保障する上での懸念事項となる	• 特定アセットへの依存による、幅広いサービスの同時停止リスク • 海外製アセットを踏み台としたサイバー攻撃リスク • バリューチェーン全体のセキュリティガバナンス不足によるリスク
3A: デジタル空間の拡大	ICTの発展によりデジタル空間が広がり、デジタル空間内においても実空間のような社会が形成され、仮想的な現実として多くの人がデジタル空間上で生活するようになる	• メタバースのアカウントの乗っ取りにより、重要インフラ・情報等へのアクセス権を奪われるリスク • メタバースプラットフォームそのものへの攻撃による、プラットフォームの停止やプラットフォームからの情報漏洩リスク • VR/AR/MRデバイスあるいはメタバースを操作し、サービス利用者に身体的・精神的攻撃をされるリスク • メタバースで取引される作品 (オブジェクト・アバター等) の権利問題に伴う金銭的なリスク • 人格のなりすましにより、本人が実社会で悪影響を受けるリスク
3B: 生活インフラのデジタル化	金融サービスや交通手段等の生活インフラのデジタル化が進行し、災害対策や治安維持等の都市全体の機能もデジタル化する	• 金融/交通/電力/物流等の重要インフラのデジタル化により、インフラがサイバー攻撃を受けるリスク • 生活に関わる電子機器をサイバー攻撃を受けるリスク
4C: 情報処理・通信等における技術革新	6Gのような新しい通信技術や量子計算機のような新しい計算技術によって、デジタルにおけるケイパビリティが大幅に向上し、ICTにおけるパラダイムシフトが起き得る	• 量子コンピュータの技術革新によるリスク • AIの技術革新によるリスク • 分散型アーキテクチャ固有の脆弱性によって引き起こされる資産流出リスク • 5G (短期) / 6G (中長期) 等の新しい通信技術に関するリスク • その他、未想定の技術革新によるリスク

その他社会変化についても、重要な研究テーマに繋がりうるセキュリティ課題を初期的に抽出

深堀する重点テーマ以外の社会変化に関する、セキュリティ課題の非網羅的なピックアップ結果

社会変化	ICTに係る潮流	想定されるセキュリティ課題の例 (社会の変化に伴い、継続的に調査・検討の余地あり)
1B: デジタル国家の加速	議会や投票等の政府機能や国民が実施する各種申請や手続等の行政機能のデジタル化が加速する	• IDの偽装により国家サービスの提供に問題が生じるリスク • デジタルディバイドにより国家サービスの利便性を享受できない国民が残されるリスク
2B: デジタル経済でのデータの価値の向上 / データを取り扱う技術の進化	データへの分析能力が高まるにつれデータがもたらす価値は向上し、様々なサービスへの利用のみならず経営判断へのインプットとしても重要な判断材料となる	• 個人情報保護とデータ活用が両立できないことで、個人情報の漏洩あるいはデータ活用の停滞のいずれかが起きるリスク
2C: 非対面サービス産業の成長	対面で実施されていた銀行の窓口業務や購買手続等のサービスが、ICTの発展によりオンライン化・無人化が加速する	• IDの偽装により非対面サービスの提供に問題が生じるリスク • より多種のデータ (触覚、味覚、嗅覚 等) を受信できるようになることで、五感への攻撃を受けるリスク
4A: ヒトの物理的な活動を代替する技術 (ロボット・ドローン) の発展	単純作業を基点に人間が実施していた作業をロボットが実施するようになり、将来的には人間と同等の動作をし人間の生活を支えるようになる	• ロボット・ドローンへのサイバー攻撃を受けるリスク
4B: 人間機能の拡張	ICTの発展が、身体 (外骨格・義体等)・知覚 (感覚の拡張/置換)・存在 (デジタルによる体外離脱 等)・認知 (AIと人間の融合) の4方向から人間機能を拡張する	• 人工臓器や装着デバイス等の人間機能拡張のデバイスへの攻撃を受けるリスク • 生体情報の侵害リスク

「社会変化1A: 安全保障の難化(サイバー安全保障の激化)」のセキュリティ課題

重点テーマである社会変化におけるセキュリティ課題 (1/6)

社会変化の潮流

国家の安全保障として、陸海空の伝統的な手段に加えサイバー安全保障が重要な役割を果たすようになる

短期

- ウクライナ紛争を契機とした、国家間サイバー攻撃の増加
- 各国のサイバーセキュリティ組織の拡充
- 行政におけるサイバー空間の広がり
- データ価値の重要性の拡大に伴う国家間のサイバー安保紛争の頻発

中長期

- 国家間のサイバー安全保障競争の激化
- 各国がハクティビストやハッカーグループを抱えることによる攻撃主体・手段の多様化/攻撃の常態化
- 急激な変化や権力の移動による紛争増加の可能性
- 中東や南アジアを中心とした地域的な不安定さが波及し、世界的な不安感の増加

想定されるセキュリティ課題

短期 中長期

1A-1 **戦争のハイブリッド化 (物理的な攻撃とサイバー攻撃の融合が進む) に伴い、サイバー攻撃により国として機能不全を起こされるリスク**

- サイバー犯罪・テロの拡大 (行政システム・重要インフラの停止等を企図した、重要施設やシステムへの攻撃)
  - 地政学的に対立関係にある国に限らず、政治的思想の異なる主体を攻撃するハクティビストからの攻撃を受ける可能性が存在
- サイバー犯罪・テロの拡大 (防衛系システムの停止等を企図した、重要施設やシステムへの攻撃)
- サイバー犯罪マーケットプレイスの拡大
- 物理的手段として、海底ケーブルの切断攻撃

短期 中長期

1A-2 **サイバー攻撃によりサイバー諜報 (cyberespionage) をされるリスク**

- 対外情報収集を目的としたサイバー諜報
  - 国家機密を取得することで、サイバー攻撃に役立てたり、偽情報を流布させたりすることに活用していくことが可能
- 経済情報収集を目的としたサイバー諜報
  - 特に技術先進国である国に対する攻撃可能性が高く、取得した情報をもとに攻撃者が自国の技術進化を狙ったり、自国企業の利益を増加させたりすることが考えられる

短期 中長期

1A-3 **情報の兵器化により、内政のコントロールを失うリスク**

- コンプロマート (情報素材) を用いた偽情報キャンペーンによる内政干渉
- 特定の情報を流すことによる内政干渉

中長期

1A-4 **旧来的な軍事力と同様、サイバー安全保障分野での対応能力が外交上の発言力に影響する可能性**

- サイバー安全保障分野での対応能力不足により、外交上の発言力が小さくなる可能性

短期 中長期

1A-5 **攻撃手法の多様化による守るべき対象の拡大に伴う、慢性的なセキュリティ対策リソース不足**

- セキュリティ人材及び対策コストの不足

「社会変化2A: 経済安全保障の深化」のセキュリティ課題

重点テーマである社会変化におけるセキュリティ課題 (2/6)

社会変化の潮流

ICT発展の経済恩恵を受ける一方、ICTアセット (ハードウェア・ソフトウェア) における海外依存やサプライチェーンマネジメントが、経済的な安全性を保障する上での懸念事項となる

短期

- 社会基盤における海外製アセット (例: クラウド) の利用の増加
- 国家/各企業の国内外へのサプライチェーンの広がり
- 3Dプリンティング技術の産業利用増加

中長期

- 社会基盤における海外製アセット (例: クラウド) への依存の増大
- デジタル化による、良好な地域経済循環の構築
- 成熟した3Dプリンティング技術によるグローバルバリュー チェーンの変革

想定されるセキュリティ課題

短期 中長期

2A-1 特定アセットへの依存による、幅広いサービスの同時停止リスク

- 多くの企業・政府機関が使っている情報基盤を狙った攻撃
  - BCP (事業継続計画) の観点でシステム冗長化をするという考えは官民ともに存在
- 多くのサービスが使っているAPIを狙って脆弱性を攻撃
- 多くの企業・政府機関が使っているサービスを狙った脆弱性を攻撃

短期 中長期

2A-2 海外製アセットを踏み台としたサイバー攻撃リスク

- バックドアを仕込まれた海外製アセットを利用した攻撃
  - 海外製のプロダクト・サービス・プラットフォームの利用により、国民の個人情報やその他機密データ等が漏洩するリスク
  - 情報漏洩のほか、通常ではない挙動を起こされるリスクも存在
- 意図的でない脆弱性を持つ海外製アセットを利用した攻撃
  - 要因として、日本の情報収集能力の不足も考えられるが、ある国家が敢えて脆弱性を公開せずに放置する戦略を取られる可能性も存在

短期 中長期

2A-3 バリューチェーン全体のセキュリティガバナンス不足によるリスク

- サプライヤーのシステム面の脆弱性をつかれた攻撃 (いわゆるサプライチェーンアタック)
- サプライヤーの内部者による攻撃
- 企業のサイバーイグノランスによるセキュリティレベルの低下
- オープンソースの活用が要因となる攻撃

「社会変化3A: デジタル空間の拡大」のセキュリティ課題

重点テーマである社会変化におけるセキュリティ課題 (3/6)

社会変化の潮流

ICTの発展によりデジタル空間が広がり、デジタル空間内においても実空間のような社会が形成され、仮想的な現実として多くの人がデジタル空間上で生活するようになる

短期

- メタバース・デジタルツイン等仮想融合技術の台頭
- 仮想世界の広がり (AR,VR,MR)
- IoT機器の発展による、インターネット接続機器の増加

中長期

- メタバースでの活動拡大
- 仮想現実の拡大・実空間との融合
- 通信の大容量化によるデジタル空間のリアルタイム性向上
- IoT機器の普及による、生活空間のデジタル化
- メタバース・デジタルツイン等仮想融合技術の普遍化
- ICT活用による地域企業の商圏拡大・地域の活性化

想定されるセキュリティ課題

中長期

3A-1 メタバースのアカウントの乗っ取りにより、重要インフラ・情報等へのアクセス権を奪われるリスク

- 国家機密や個人情報へのアクセスが可能なアカウントを奪われることによる情報漏洩リスク
- 人命にかかわる操作の権限をもつアカウントを奪われることによる人命リスク
- 重要インフラの操作権限をもつアカウントを奪われることによるリスク

短期 中長期

3A-2 メタバースプラットフォームそのものへの攻撃による、プラットフォームの停止やプラットフォームからの情報漏洩リスク

- DDOS攻撃等によるプラットフォーム停止リスク
- メタバースプラットフォームの運営社にのみ可能な操作権限を奪われることによる混乱のリスク
- メタバースプラットフォームが保有するデータの漏洩による個人情報漏洩リスク
- メタバース内で他ユーザのハッキングリスク
- メタバースプラットフォームでの悪意ある行動のリスク

短期 中長期

3A-3 VR/AR/MRデバイスあるいはメタバースを操作し、サービス利用者に身体的・精神的攻撃をされるリスク

- デバイスのハックにより、身体的な攻撃を受けるリスク
- デバイスのハックにより、精神的な攻撃を受けるリスク

短期 中長期

3A-4 メタバースで取引される作品 (オブジェクト・アバター 等) の権利問題に伴う金銭的なリスク

- メタバース上での制作物の著作権を侵害されるリスク
- メタバース上での所有物を奪われるリスク

中長期

3A-5 人格のなりすましにより、本人が実社会で悪影響を受けるリスク

- 著名人を名乗るアカウントが作られ、偽発信等による名誉棄損されるリスク
- 権限を持つ人を名乗るアカウントが偽の命令を下すことで、混乱を招かれるリスク
- 知人を名乗るアカウントを信用してしまうことにより、偽情報を信じる・不利な取引を許可する等を行うリスク

「社会変化3B: 生活インフラのデジタル化」のセキュリティ課題

重点テーマである社会変化におけるセキュリティ課題 (4/6)

社会変化の潮流

金融サービスや交通手段等の生活インフラのデジタル化が進行し、災害対策や治安維持等の都市全体の機能もデジタル化する

短期

- キャッシュレスの普及
- オンライン身分証明の普及
- モビリティ多様性拡大及び関連技術開発 (自動運転車、電動キックボード、電気自動車 等)
- オンラインヘルスケアの台頭

中長期

- スマートシティの台頭
- 所有から共有、コト消費へとシフト
- 自動運転技術の普及及び、一部で「空飛ぶクルマ」等も進展
- オンラインと対面を組み合わせた、多様なニーズを満たすヘルスケアの実現
- ICTによる省電力化の進展とグリーン社会実現への貢献

想定されるセキュリティ課題

中長期

3B-1 金融/交通/電力/物流等の重要インフラのデジタル化により、インフラがサイバー攻撃を受けるリスク

- サイバー攻撃により電力・ガス・水道網を攻撃されるリスク
- サイバー攻撃により、医療サービスの提供が不能になるリスク
- サイバー攻撃により、交通網 (自動車・鉄道・航空) の安全性と継続性が侵害されるリスク
- サイバー攻撃により、物流サービスが滞るリスク
- サイバー攻撃により、金融機関の信頼が失われるリスク
- サイバー攻撃により、産業系インフラの安定と継続性が侵害されるリスク

短期 **中長期**

3B-2 生活に関わる電子機器がサイバー攻撃を受けるリスク

- サイバー攻撃により、電子機器を操作され、物理的・身体的な影響を受けるリスク
- サイバー攻撃により、カメラやメーター等が操作され、個人情報や生活に紐づくデータ (位置情報含む) を盗まれる可能性
- サイバー攻撃により、個人情報や生活に紐づくデータを改竄される可能性

「社会変化4C: 情報処理・通信等における技術革新」のセキュリティ課題 (1)

重点テーマである社会変化におけるセキュリティ課題 (5/6)

社会変化の潮流

6Gのような新しい通信技術や量子計算機のような新しい計算技術によって、デジタルにおけるケイパビリティが大幅に向上し、ICTにおけるパラダイムシフトが起き得る

短期
- 量子計算機の台頭
- AIの利用シーン増加
- 5Gの普及による、IoTの促進
- ブロックチェーン/Web3.0の進展

中長期
- 量子計算機の浸透(2030,40年以降見込み)
- AIの進化(人間並みの知能→シンギュラリティ
- 6Gの実用化

想定されるセキュリティ課題

中長期

4C-1 量子コンピュータの技術革新によるリスク
- 汎用量子コンピュータの実現 (2030年以降の想定) により既存の暗号 (RSA等) が破られ、既存暗号が使えなくなるリスク
- 汎用量子コンピュータが登場したのちに解読を行う「store now, break later」攻撃のリスク
- ポスト量子暗号 (PQC) への移行には時間がかかるというリスク
- 量子インターネット、量子コンピュータへの攻撃の登場
  - 量子インターネット、量子コンピュータが汎用化されたのち、それらへの攻撃手法が登場することが想定される

短期 中長期

4C-2 AIの技術革新によるリスク
- 技術革新により、社会における活用機会が拡大したAIに対して、AI固有の脆弱性を突いた攻撃が行われるリスク
- AIの悪用により、サイバー攻撃の巧妙化及び複雑化が進むリスク

短期 中長期

4C-3 分散型アーキテクチャ固有の脆弱性によって引き起こされる資産流出リスク
- Web3.0では欠陥へのパッチ適用に時間がかかり、その間に脆弱性が放置されることにならざるをえない
- ITリテラシーの低い人が知識不足によりリスクに直接さらされるように
- 分散型システムの価値が高まる中、攻撃を受ける可能性が増加するリスク
- Web3.0アプリのフロントエンドはweb2.0のテクノロジーに現状依存していることによる脆弱性も存在
- 分散型アーキテクチャはトレーサビリティが担保されている一方、各ブロックそのものの内容証明はないため、信頼性の担保ができない点も課題

「社会変化4C: 情報処理・通信等における技術革新」のセキュリティ課題 (2)

重点テーマである社会変化におけるセキュリティ課題 (6/6)

社会変化の潮流

6Gのような新しい通信技術や量子計算機のような新しい計算技術によって、デジタルにおけるケイパビリティが大幅に向上し、ICTにおけるパラダイムシフトが起き得る

短期

- 量子計算機の台頭
- AIの利用シーン増加
- 5Gの普及による、IoTの促進
- ブロックチェーン/Web3.0の進展

中長期

- 量子計算機の浸透 (2030,40年以降見込み)
- AIの進化(人間並みの知能→シンギュラリティ
- 6Gの実用化

想定されるセキュリティ課題

短期　中長期

4C-4　5G (短期) / 6G (中長期) 等の新しい通信技術に関するリスク

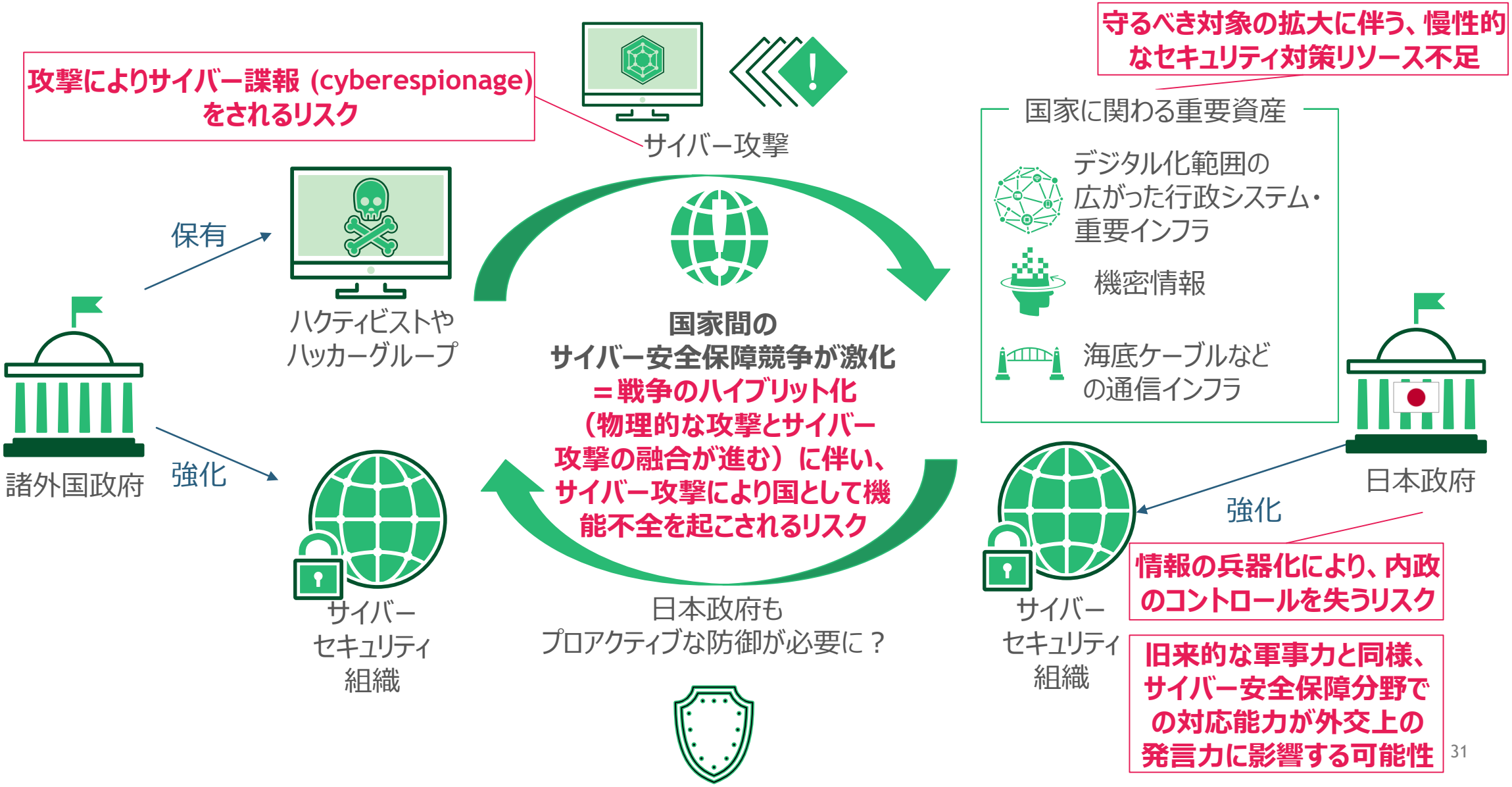
- 仮想化のためのAI活用が進むことにより深刻度を増すAI汚染のリスク
- なりすましや不正アクセスのリスク
- 通信事業者が増える/オープンソース技術の活用が増えることによる、セキュリティレベルの低下リスク
- (6G) 無線の盗聴、ジャミング、コンタミ侵害等のサイバーフィジカルリスク
- (6G) 体内センサー活用による、人命に係るリスク
- (6G) 極限環境での利用に伴う、セキュリティ機能の低下・異常動作

中長期

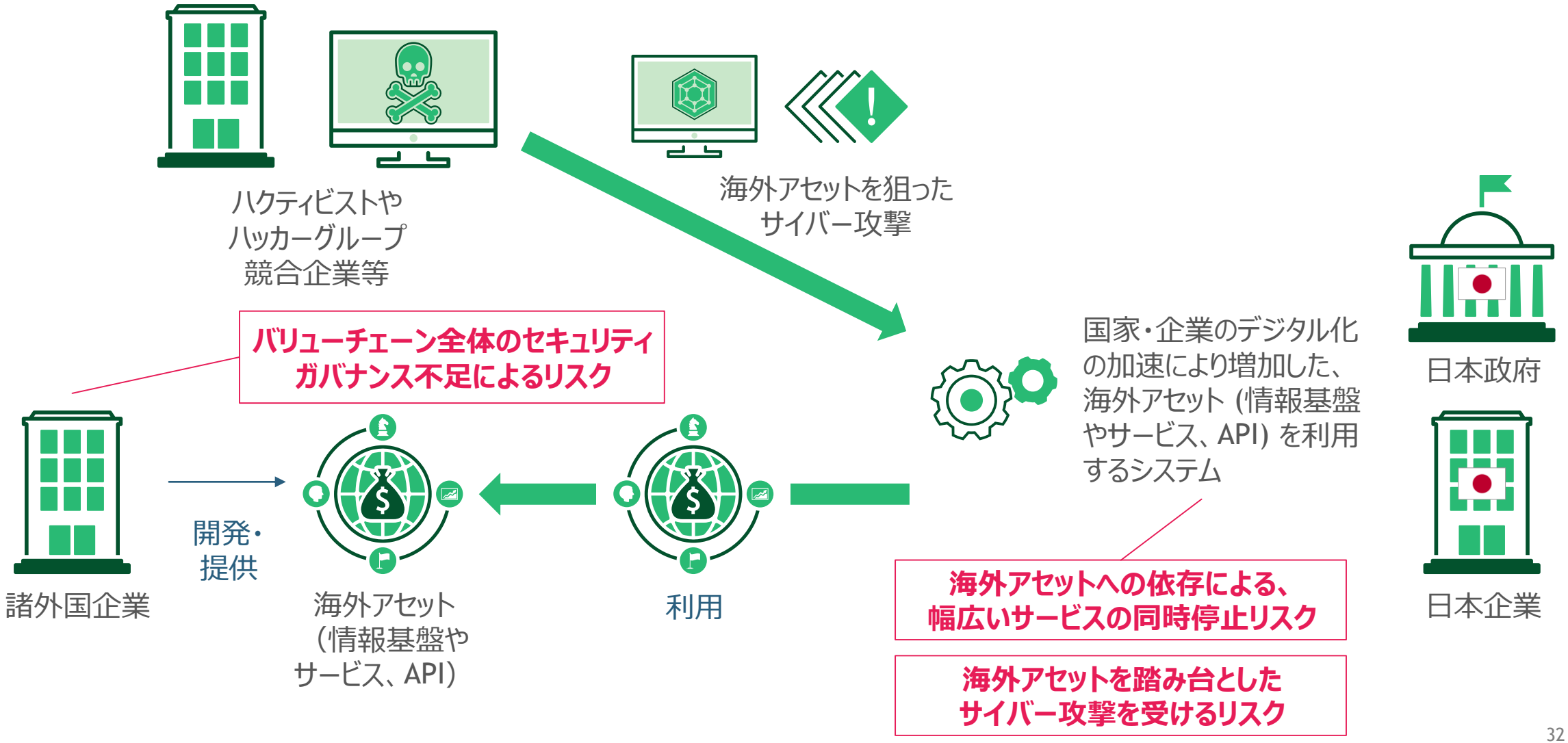
4C-5　その他、未想定の技術革新によるリスク

- サイバー攻撃により、電子機器を操作され、物理的・身体的な影響を受けるリスク
- サイバー攻撃により、カメラやメーター等の操作により、個人情報や生活に紐づくデータ (位置情報含む) を盗まれる可能性
- サイバー攻撃により、個人情報や生活に紐づくデータを改竄される可能性

「1A: 安全保障の難化 (サイバー安全保障の激化)」のセキュリティ課題イメージ



「2A: 経済安全保障の深化」のセキュリティ課題イメージ



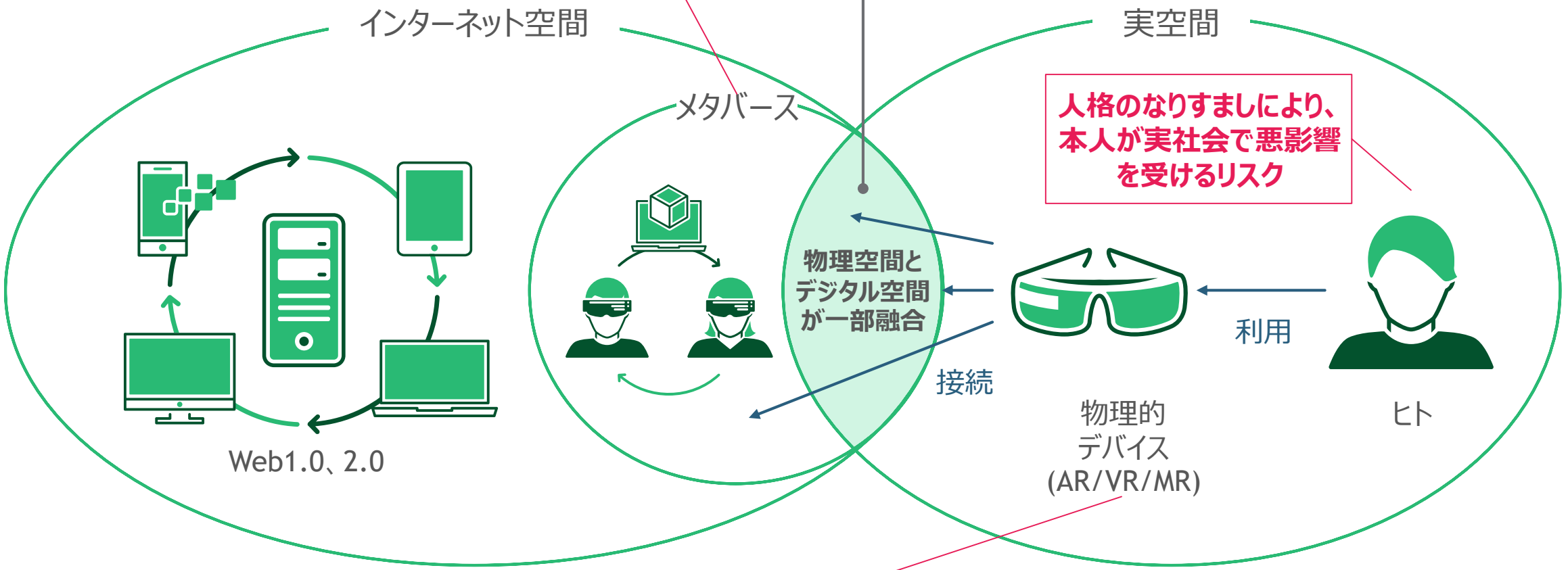
「3A: デジタル空間拡大 (仮想現実の拡大・実空間との融合)」のセキュリティ課題イメージ

メタバースプラットフォームそのものへの攻撃による、プラットフォームの停止やプラットフォームからの情報漏洩リスク

アカウント乗っ取りにより、重要インフラ・情報などへのアクセス権を奪われるリスク

実空間のような社会が形成され、仮想的な現実として多くの人がデジタル空間上で生活

メタバースで取引される作品の権利問題に伴う金銭的なリスク



VR/AR/MRデバイスあるいはメタバースを操作し、サービス利用者に身体的・精神的攻撃をされるリスク

「3B: 生活インフラのデジタル化」のセキュリティ課題イメージ

都市機能全体がデジタル化したことによって、様々な重要インフラがサイバー攻撃を受ける可能性

生活に関わる電子機器をサイバー攻撃を受けるリスク

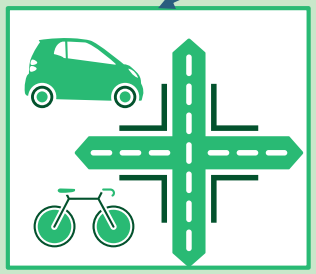
デジタル化された様々な生活インフラのサービスを利用することで、便利な暮らしを享受

ヒト・企業

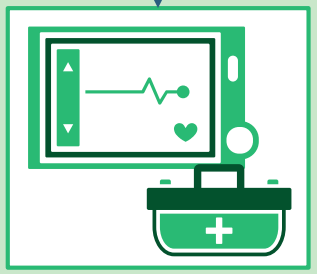
利用

都市機能全体がデジタル化

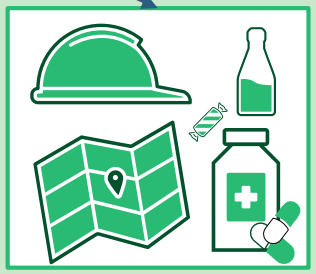
金融サービス



交通インフラ



ヘルスケア機能



災害対策

治安維持機能

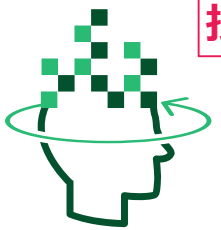
…

ヒトや企業がデジタル化されたインフラ上で生活することで、様々なデータがタンキング

「4C: 幅広い社会変化の基盤となる情報処理等の技術の革新」のセキュリティ課題イメージ

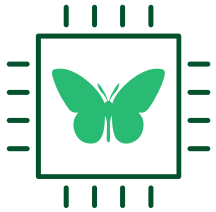
情報処理等の技術革新要素

その他、未想定の技術革新によるリスク



AIの進化
(人間並みの知能→シンギュラリティ)

…



量子計算機

6G (Beyond 5G)

5G (短期) / 6G (中長期) 等の新しい通信技術に関するリスク

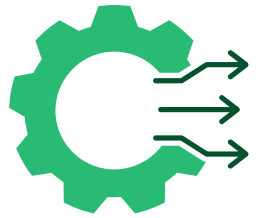
分散型アーキテクチャ固有の脆弱性によって引き起こされる資産流出リスク

プラスの影響

技術革新により、ICTにおけるパラダイムシフトが発生

マイナスの影響

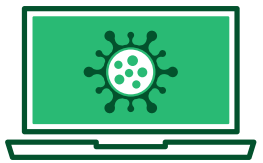
デジタル空間の拡大



生活インフラのデジタル化

…

古い暗号化技術の解析



新型マルウェアの自動作成

…

量子コンピュータの技術革新によるリスク

AIの技術革新によるリスク

Agenda

1. 目的・本プロジェクトの概要
2. ①守るべき対象・社会の変化に関する調査
3. ②ICT社会の変化に伴うセキュリティ課題の調査
4. ③研究・開発テーマの提言
5. 今後の研究・開発テーマの検討について

セキュリティ課題への対策に必要な研究・開発テーマを洗い出し、優先順位付けを実施

研究・開発テーマの検討プロセス

研究・開発テーマの洗い出し

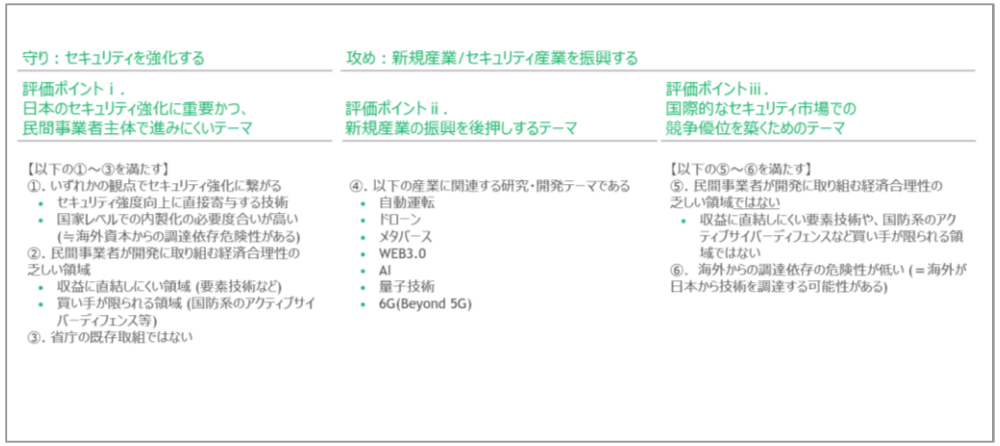
実施
イメージ

セキュリティ課題		対策	研究・開発テーマ
7A-1 特定サービスへの依存による、幅広の同リスク		特定 ・重要システムの依存先の把握	① 国全体・企業単位でネットワーク/アセット管理を効率よく行うシステム・技術の開発
セキュリティ課題		対策	研究・開発テーマ
1A-1 戦争のハイブリッド化に伴い、サイバー攻撃により国として機能不全を起こされるリスクサイバー攻撃によるサイバー課報をされるリスク	特定	・日本にとっての重要インフラ・施設・情報を整理し、そのアクセシビリティ及びセキュリティ強度を把握	① 重要資産の重要性やアクセシビリティ、セキュリティ強度を定量的に評価するセキュリティ経済学の研究
1A-2		・日本を攻撃し得る国/ハクティビストの攻撃手法の特徴を把握	② 攻撃者の特徴の自動抽出・判定技術の研究開発
			③ 日本を攻撃し得る攻撃者の最新動向把握を目的としたハニーポット、サンドボックス、ターピットの活用
			④ IoCを収集・分析し脅威インテリジェンス情報に昇華させ、国から日本国民や企業向けに周知するプロセスを作成
			⑤ 日本を攻撃し得る攻撃者の最新動向把握をもとにした、攻撃予測の研究
	防御	・重要施設の情報管理手法のセキュア化のため、ガイドラインを作成し実行(エアギャップ等も選択肢のひとつ)	⑥ 重要度に応じた情報管理手法のセキュア化のための要件及び、要件を満たすための実行内容の検討
		・重要データの管理でクラウドを利用する場合の秘匿及び、計算もセキュアに実施できるクラウド技術	⑦ クラウドデータを計算可能な準同型暗号の開発
			⑧ CPUの中のトラステッドスペースで計算を行う手法
			⑨ マルチパーティ計算を利用した分散型計算によるリスク分散
			⑩ 重要データの分散保管を可能にする、学習データを分散させたままモデルの学習をおこなう連合学習(Federated Learning)の実装
		・サイバー攻撃の難易度をあげるシステム、環境づくり	⑪ TCP/IPよりも傍受・課報のリスクの少ない新規プロトコルの設計
			⑫ 攻撃者の目的阻害(Denial & Deception)のためのディセプションテクノロジーの開発
		・重要インフラのサイバーフィジカル面の防御力向上	⑬ 航空機や船舶等での無線通信のセキュリティ向上のための規格の研究(現状の規格は脆弱性があるアップデートが必要)
			⑭ GNSSに過度に依存しない時空間同期技術の研究開発
	検知	・ダークウェブの探索や他国政府との連携による、最新の攻撃主張(マルウェア等)の情報収集及び検知機能への反映	⑮ 他国政府と効率よく情報連携(手動での作業を極力削減)するための情報基盤の開発
			⑯ 日本国のアセットへの攻撃を検知するためのネットワーク/アセット監視システムの構築
		・ダークウェブでの取引を監視し、情報漏洩を検知	⑰ ダークウェブの取引を監視し、日本国が関わる情報漏洩を検知するようなツールの開発
		・重要インフラの監視(海底ケーブルといった物理的な物を含む)	⑱ 重要インフラ(民間含む)の不審検知の精度向上及び省力化を目的とした自動化技術
			⑲ 情報を盗まれたことを検知するための、ビーコン活用手法
			⑳ IoT技術を活用した、人が監視困難なインフラ(海底ケーブル)の物理的な損害の監視・発見技術

実施
内容

「②ICT社会の変化に伴うセキュリティ課題の調査」にて抽出した
セキュリティ課題に対し、有識者インタビュー / 各種調査を通じて
IDPRR(特定/検知/防御/対応/復旧)の観点で対策を幅出し。
その上で、その実現に必要な135の研究・開発テーマを抽出

研究・開発テーマを優先順位付け



守り：セキュリティを強化する	攻め：新規産業/セキュリティ産業を振興する	
評価ポイントⅰ. 日本のセキュリティ強化に重要かつ、 民間事業者主体で進みにくいテーマ	評価ポイントⅱ. 新規産業の振興を後押しするテーマ	評価ポイントⅲ. 国際的なセキュリティ市場での 競争優位を築くためのテーマ
【以下の①～③を満たす】 ①. いずれかの観点でセキュリティ強化に繋がる • セキュリティ強度向上に直接寄与する技術 • 国家レベルでの内製化の必要度合いが高い(≒海外資本からの調達依存危険性がある) ②. 民間事業者が開発に取り組む経済合理性の乏しい領域 • 収益に直結しにくい領域(要素技術など) • 買い手が限られる領域(国防系のアクティブサイバーディフェンス等) ③. 省庁の既存取組ではない	④. 以下の産業に関連する研究・開発テーマである • 自動運転 • ドローン • メタバース • WEB3.0 • AI • 量子技術 • 6G(Beyond 5G)	【以下の⑤～⑥を満たす】 ⑤. 民間事業者が開発に取り組む経済合理性の乏しい領域ではない • 収益に直結しにくい要素技術や、国防系のアクティブサイバーディフェンスなど買い手が限られる領域ではない ⑥. 海外からの調達依存の危険性が低い(＝海外が日本から技術を調達する可能性がある)

左記で抽出した、研究・開発テーマを複数の考え方で評価。
今後、いずれのテーマに投資・注力をするかの優先順位付けを行い、
大きな方向性を示す

幅出しした研究・開発テーマを、注力すべき研究・開発領域ごとにカテゴライズ

考え方

PEST分析により重点テーマとして選定した社会変化と発掘した研究・開発テーマの関連性を整理し、取り組む目的を明確化。将来の社会変化に備え、注力すべき研究・開発領域としてカテゴリレベルで纏めた

カテゴライズの結果

1 サイバー安全保障の激化・生活インフラ（重要インフラ）のデジタル化進展に伴う、サイバー攻撃の増加と守るべき対象・攻撃手法の多様化への対応

- 1-1 アクティブサイバーディフェンス
- 1-2 パッシブサイバーディフェンスのアップデート
- 1-3 増加するサイバーフィジカルリスクへの対応
- 1-4 データ利活用の拡大に対応するデータセキュリティ

2 経済安全保障の深化に伴うサプライチェーン複雑化への対応

- 2-1 国産技術の確保/育成
- 2-2 海外技術の信頼性検証/安全な活用
- 2-3 サプライチェーン上のサイバーセキュリティギャップの解消

3 拡大するデジタル空間のサイバーセーフティ確保

- 3-1 メタバースでの人々の安全を守る
- 3-2 分散型システム (web 3 等) を支えるセキュリティ

4 社会の基盤となる技術の革新への対応

- 4-1 量子技術の発展を前提にした変化への対応
- 4-2 Security for AI/AI for Security
- 4-3 Beyond5G (6G含む) セキュリティ

研究テーマの抽出に当たって、3つの異なる考え方で優先順位付けを実施

研究テーマの優先順位付けについての考え方

評価ポイントⅰ.
日本のセキュリティ強化に重要かつ、民間事業者主体で進みにくいテーマ

【以下の①～②を満たす】

①. いずれかの観点でセキュリティ強化に繋がる
- セキュリティ強度向上に直接寄与する技術
- 国家レベルでの内製化の必要度合いが高い (≒海外資本からの調達依存危険性がある)

②. 民間事業者が開発に取り組む経済合理性の乏しい領域
- 収益に直結しにくい領域 (要素技術等)
- 買い手が限られる領域 (国防系のアクティブサイバーディフェンス 等)

特に国の防衛や公共サービスなど、国家機能そのものの
セキュリティに寄与するものについては重要度が高い

評価ポイントⅱ.
新規産業の振興を後押しするテーマ

③. 以下の産業に関連する研究・開発テーマである
- 自動運転
- ドローン
- メタバース
- WEB3.0
- AI
- 量子技術
- 6G(Beyond 5G)

評価ポイントⅲ.
セキュリティの国際市場での競争優位を築くためのテーマ

【以下の④～⑤を満たす】

④. 民間事業者が開発に取り組む経済合理性のある領域
- 収益に直結しにくい要素技術や、国防系のアクティブサイバーディフェンス等買い手が限られる領域ではない

⑤. 海外からの調達依存の危険性が低い (＝海外が日本から技術を調達する可能性がある)

複数の条件を満たすものは相対的に優先度が高い

評価ポイントｉ (日本のセキュリティ強化に重要かつ、民間事業者主体で進みにくいテーマ)

基準: 以下の①～②を満たす
①. いずれかの観点でセキュリティ強化に繋がる (セキュリティ強度向上に直接寄与する技術 / 国家レベルでの内製化の必要度合いが高い (≒海外資本からの調達依存危険性がある))
②. 民間事業者が開発に取り組む経済合理性の乏しい領域 (収益に直結しにくい領域 (要素技術 等) / 買い手が限られる領域 (国防系のアクティブサイバーディフェンス 等))
なお、特に国の防衛や公共サービスなど、国家機能そのもののセキュリティに寄与するものについては重要度が高い

目的	研究・開発テーマのカテゴリ	研究・開発テーマ (一部抜粋)
1 サイバー安全保障が激化・生活インフラのデジタル化により進む、ｻｲﾊﾞｰ攻撃の増加と攻撃対象及び手法の多様化に対応	1-1 アクティブサイバーディフェンス	• 攻撃者の目的阻害 (Denial&Deception) のためのディセプションテクノロジーの開発 • 悪意あるボットネット破壊を目的とした検知・破壊手法
	1-2 パッシブサイバーディフェンスのアップデート	• 攻撃者の特徴の自動抽出・判定技術の研究開発 ― 日本を攻撃し得る国/ハクティビストの攻撃手法の特徴をプロアクティブに把握するために実施 • 国が保有するデータを基にしたセキュリティアシュアランス判断技術の開発 • 国としてトラストアンカーとなるための認証基盤の構築 ― 生活インフラに接続するエンティティの正当性は、政府等のトラストフルな組織が保障することが望ましい
	1-3 増加するサイバーフィジカルリスクへの対応	• ECUへ実装するセキュアな軽量暗号の開発 • サイバーフィジカルセキュリティとセーフティの融合関連の研究
	1-4 データ利活用の拡大に対応するデータセキュリティ	• 重要情報やクラウドに格納されたデータを暗号化したまま計算できる秘密計算の開発
2 経済安全保障に関連し、サプライチェーン複雑化に対応	2-1 国産技術の確保/育成	• データバックアップのためのコントロール可能な自国内のデータセンター整備 ― 重要データを確実に保護するためにはデータセンター内製化が望ましい • Software Bill Of Materials：ソフトウェア部品表作成用のツール(API)の開発
	2-2 海外技術の信頼性検証/安全な活用	• クラウドサービスにセキュアにデータを格納するための信頼できる鍵管理システム式の開発 • 不正機能や未知脆弱性の自動検出技術の研究開発 • 不審通信を検知するアルゴリズムの開発 (単一ログまたは複合ログによる検知)
3 拡大するデジタル空間のサイバーセーフティ確保	3-1 メタバースでの人々の安全を守る	• 個人認証技術の強化のためのデータベースの整備 ― 将来的には脳波等、生体認証の中でもより高度な情報が認証に使用されることを想定 • 現状の法制度では罰せないデジタル空間の犯罪の明確化及び法整備へ向けたロードマップの検討
	3-2 分散型システム (web3 等)を支えるセキュリティ	• 分散型アーキテクチャにおける、よりセキュアの運営手法の研究 (信頼の分散 等)
4 社会の基盤となる技術の革新への対応	4-1 量子技術の発展を前提にした変化への対応	• 量子インターネット、量子コンピュータへの攻撃手法の継続的な研究と対策方針の整理、およびその啓発
	4-2 Security for AI / AI for Security	• AIの悪用事例の継続的な研究と対策方針の整理、およびその啓発
	4-3 Beyond5G (6G含む)セキュリティ	• 超高速通信、超低遅延、超高信頼通信、超カバレッジ拡張、超低消費電力を実現するための規格及び、セキュリティ仕様の検討

評価ポイント ii (新規産業の振興を後押しするテーマ)

基準: 以下の産業に関連する研究・開発テーマである
- 自動運転 / ドローン / メタバース / WEB3.0 / AI / 量子技術 / 6G (Beyond 5G)

分類	研究・開発テーマ (一部抜粋)
自動運転の実用化を支えるセキュリティ	• AIを利用した自動運転における、不正なデータを送り込み、誤検知、過検知を引き起こすように学習させる攻撃手法を防止する技術の開発 • 異なる国・企業によって製造された、異なる通信規格を持つ車同士の通信方法に関する研究
物流 (ドローン、船舶、航空機等) のIoT化を支えるセキュリティ	• 航空機や船舶等での無線通信のセキュリティ向上のための規格の研究 (現状の規格は脆弱性があるアップデートが必要) • GNSSに過度に依存しない時空間同期技術の研究開発
メタバース業界における日本の優位性を支えるセキュリティ	• マイナンバー基盤等の、国がトラストアンカーの本人確認を電子的に可能なサービスの実現
WEB3.0等の分散システム分野における日本の優位性を支えるセキュリティ	• 分散型システムにおけるトラストアンカーの在り方 (分散的な集合知に基づくのか、信頼に足るエンティティが担うのか、等)及び必要なトラスト確保技術の研究
量子分野における日本の優位性を支えるセキュリティ	• 量子インターネット、量子コンピュータへの攻撃手法の継続的な研究と対策方針の整理、及びその啓発
AI分野における日本の優位性を支えるセキュリティ	• 秘密計算に対応した機械学習モデルの構築の理論研究
Beyond5Gにおける日本の優位性を支えるセキュリティ	• 無線の盗聴、ジャミング、無線のコンタミ侵害等のサイバーフィジカル攻撃の検知手法の開発
その他産業のDX化を支える基盤セキュリティ	• 国としてトラストアンカーとなるための認証基盤の構築

“Security for AIの研究により、多分野でのAI活用を後押し可能

“セキュアな認証は産業のDX化を後押し可能

評価ポイントiii (セキュリティの国際市場での競争優位を築くためのテーマ)

基準: 以下の④・⑤を満たす
④. 民間事業者が開発に取り組む経済合理性のある領域
⑤. 海外からの調達依存の危険性が低い (＝海外が日本から技術を調達する可能性がある)

分類	研究・開発テーマ (一部抜粋)
Identify / 特定	• シャドーIT (管理しきれていない機器やソフトウェア) を検知し、ネットワーク/デバイスの構成を把握する技術 • Software Bill Of Materials: ソフトウェア部品表作成用のツール (API) の開発
Protect / 防御	• マルチパーティ計算を利用した分散型計算によるリスク分散 • 複数の生体要素を組み合わせた (手のひら静脈×顔、顔×虹彩等) マルチ生体認証の実装 • 極限環境でも正常作動する部材についての研究開発
Detect / 検知	• 重要インフラ (民間含む) を国家規模で監視した際の、不審検知の精度向上及び大量データ処理の省力化を目的とした管理・自動化技術 • 不正機能や未知脆弱性の意図性評価技術の研究開発 (故意か過失かの判断指標) • AIを活用して作成されるマルウェアの検知率を向上させるための検知手法の強化
Respond / 対応	• 通信の回復の際、特に重要な通信から優先して復旧させることを目的としたアルゴリズムあるいはシステム • 検知内容を自動的に分析するオーケストレーションツールの開発
Recover / 復旧	• デジタルフォレンジックの効率を上げるためのツール・自動化技術 (AI活用も含む) の開発

“ 複数の有識者より、品質の高さは日本の強みとの指摘があり、ポテンシャルは一定存在する見込み

Agenda

1. 目的・本プロジェクトの概要
2. ①守るべき対象・社会の変化に関する調査
3. ②ICT社会の変化に伴うセキュリティ課題の調査
4. ③研究・開発テーマの提言
5. 今後の研究・開発テーマの検討について

今後の研究・開発テーマの継続的な見直し手法について

社会変化の精査

本調査の対象とした国内外の幅広いレポートの更新版の確認

その他、発行主体の属性 (産業系/政府系/学問系) 別の新規のレポートの探索／精査

セキュリティ課題の精査

海外におけるサイバーセキュリティの取組の調査等について、更新版を確認

(特に新しい社会変化について)
セキュリティに関するガイドライン等を精査

取り組み中の研究・開発テーマの評価

研究・テーマを推進中のテーマについて、進捗状況を評価 (当初計画通り成果が出る見込みか)

当該テーマについて、代替技術の発展や、海外でのブレークスルーなど環境変化を確認

国家戦略の変化などの整理

研究・開発テーマの選定に影響を与えうる、国家としての目指す姿等の変化について整理

研究・開発テーマの再評価

左記を元に研究・開発テーマを改めて幅出し

優先順位の考え方／評価方法を見直した上で、それぞれを評価し、改めて研究・開発テーマを精査