第413回NRIメディアフォーラム

エマージングテクノロジーと「ちょうどいい」セキュリティガバナンス

グループマネージャー　木村　匠
シニアセキュリティコンサルタント　内橋　七海
シニアセキュリティコンサルタント　藤村　了
セキュリティコンサルタント　南朴木　里咲

NRIセキュアテクノロジーズ株式会社
マネジメントコンサルティング事業本部
グローバル・リサーチコンサルティング部

2026年8月28日

NRIセキュアテクノロジーズ
NRI SecureTechnologies

Envision the value,
Empower the change

1 「エマージングテクノロジー」とは

2 エマージングテクノロジーにおけるセキュリティの論点

3 「ちょうどいい」セキュリティガバナンスの重要性

4 まとめ

1.「エマージングテクノロジー」とは

エマージングテクノロジーとは何か？

単なる新興技術ではない。根本的に新しく、急速に成長し、多くの分野を融合させる相乗効果を発揮しながら社会全体への影響力をもつテクノロジー。その影響には不確実性が伴う

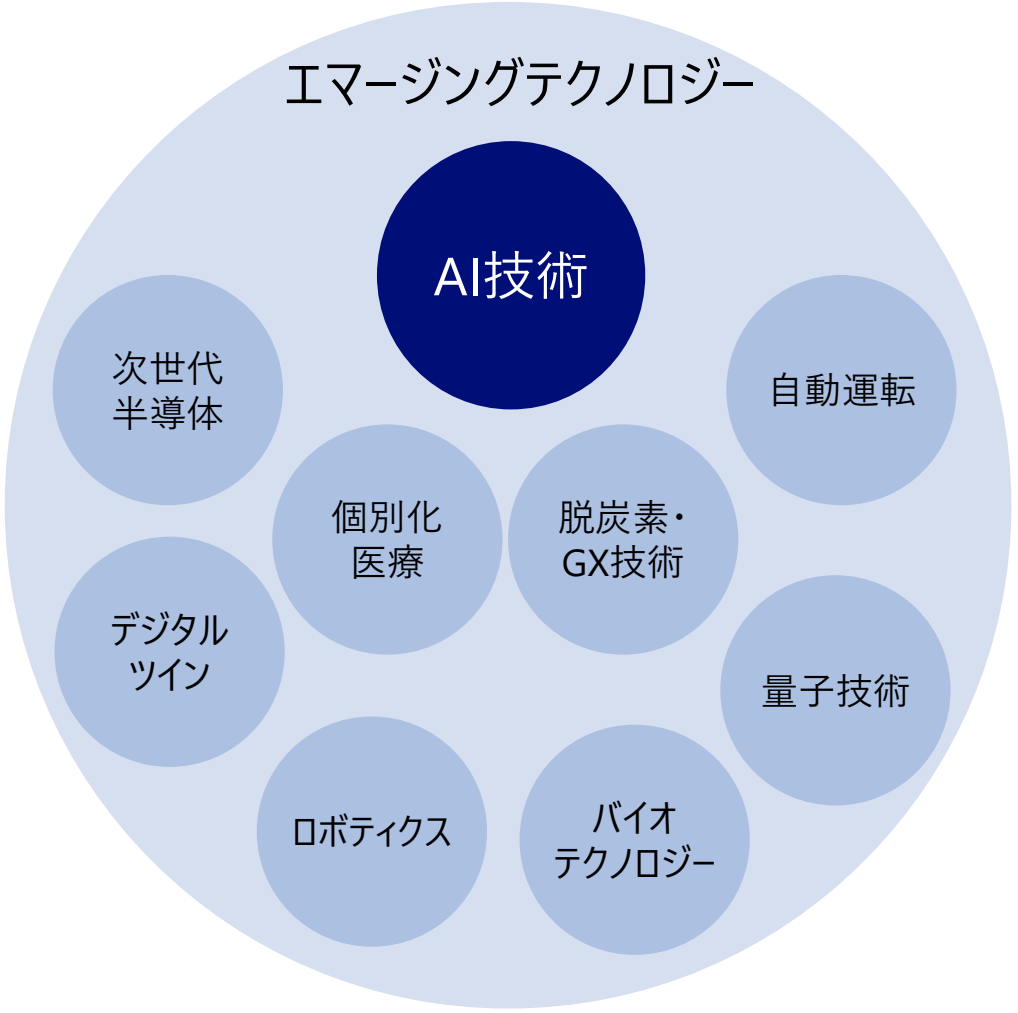
エマージングテクノロジーの特徴

①根本的な新規性（Radical Novelty）	従来とは根本的に異なる考え方や仕組みにより目的を達成する
②急速な成長（Fast Growth）	技術に関わる主体、資金、研究、プロトタイプにおいて同領域の技術よりも急速に成長する
③凝集性（Coherence）	初期段階では単一的な技術に見えるが、成熟するにつれ多分野を融合した相乗効果を発揮
④顕著な影響力（Prominent Impact）	社会全体に対して、制度、知識生産プロセスを大幅に変革する潜在能力を持つ
⑤不確かさと曖昧さ（Uncertainty and Ambiguity）	技術の用途が流動的かつ幅広いため、社会への影響の予測が困難

出所）Daniele Rotolo, Diana Hicks & Ben R. Martin “What is an emerging technology?”（日本語訳はNRIセキュアにて作成）

AIはエマージングテクノロジーの一部

目下はフロンティアAIをはじめとするAI技術への注目が集まっている状況。ただし、AI技術はエマージングテクノロジーのほんの一部でしかない



エマージングテクノロジーの具体例

2025年に英国政府が実施した、エマージングテクノロジーがもたらすセキュリティへの影響に関する調査研究にて、技術同士の融合によるメリットやセキュリティ上の脅威が示されている

- 英国科学・イノベーション・技術省（DSIT）は、エマージングテクノロジー同士が**技術の融合（Technology Convergence：無関係だった技術が密接に統合される傾向）**を伴いながら発展する点に着目した調査研究を実施
- 文献調査による分析に基づき、**学術論文上頻繁に言及される技術の組み合わせで、かつサイバーセキュリティに関連する関心が高まっているもの**が提示されている

英国DSITによる調査研究で示された技術の融合例により実現されることと、想定される脅威

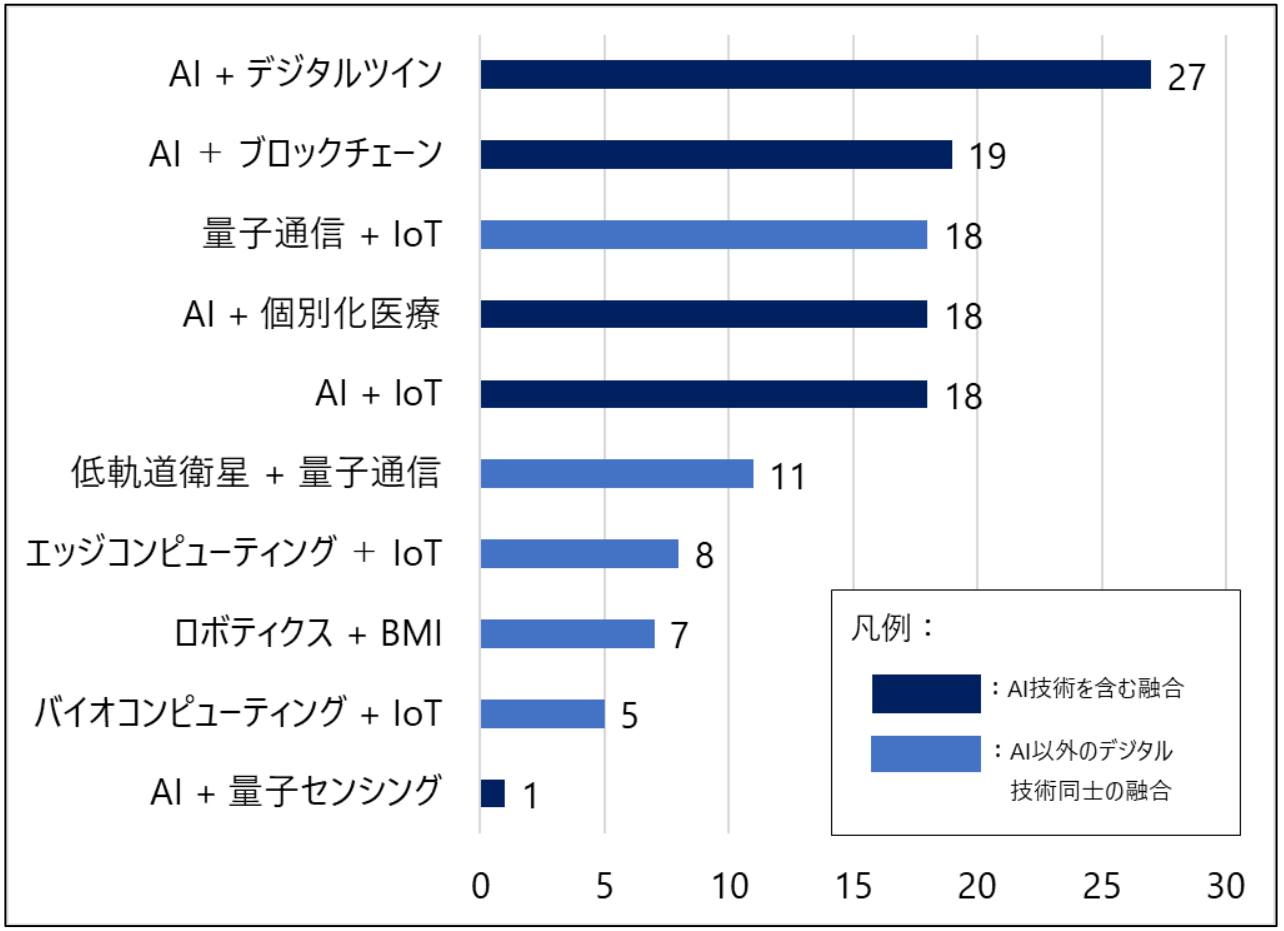
技術の融合例		融合により実現されることの例	考えられるセキュリティ上の脅威
技術1 影響力が大きい主要技術	技術2 より多様な技術		
AI	デジタルツイン	物理的な資産の予測的なメンテナンス	デジタルモデルに誤ったデータが注入されることで資産が損傷する
AI	個別化医療	膨大なデータセットを用いた高精度な診断や治療計画策定	AIへの敵対的攻撃による、誤診断や不適切な治療計画の立案
ロボティクス	ブレイン・マシン・インターフェース（BMI）	神経信号を読み取り義手等を操作することによる生活支援	利用者の思考や感情に関する情報を含む脳波データの漏えい

出所）DSIT "Emerging technologies and their effect on cyber security"をもとにNRIセキュアが作成

エマージングテクノロジーの具体例

前述の英国政府の調査によると、学術論文で頻繁に言及されている内容には、AI技術を含む融合だけでなく、AI以外のデジタル技術同士の融合も多く見受けられる

英国DSITによる調査研究でのレビュー対象となった研究論文の数



出所）DSIT “Emerging technologies and their effect on cyber security”をもとにNRIセキュアが作成

「統合イノベーション戦略2026」では、17の重要技術領域における研究開発の強化を明言している

- 2026年7月14日、日本政府が「統合イノベーション戦略2026」を閣議決定
- 将来の日本の科学技術をけん引する潜在力を有する新興技術や基盤技術として、17の重要技術領域を選定

「統合イノベーション戦略2026」で選定された17の重要技術領域

造船	航空	デジタル・サイバーセキュリティ
農業・林業・水産	資源・エネルギー安全保障・GX	防災・国土強靱化
先端医療	製造・マテリアル	モビリティ・輸送・港湾ロジスティクス
海洋	防衛産業	AI・先端ロボット
量子	半導体・通信	バイオ・ヘルスケア
フュージョンエネルギー	宇宙	

出所）内閣府「統合イノベーション戦略2026」 https://www8.cao.go.jp/cstp/tougosenryaku/2026.html

「統合イノベーション戦略2026」では、研究上のセキュリティ確保や大学等における サイバーセキュリティ対策推進にも言及している

「統合イノベーション戦略2026」の6つの柱

- ①知の基盤としての「科学の再興」
- ②技術領域の戦略的重点化
- **③科学技術と国家安全保障との有機的連携**
- ④産学官を結節するイノベーション・エコシステムの高度化
- ⑤戦略的科学技術外交の推進
- ⑥推進体制・ガバナンスの改革

研究セキュリティの確保および
大学等のサイバーセキュリティ対策推進に関する言及

③　科学技術と国家安全保障との有機的連携

国家安全保障分野の情勢が大きく変化する状況を踏まえ、産学官が連携して、デュアルユース技術の研究開発や人材育成を行うほか、安全保障分野におけるエコシステムを構築する。

具体的には、関係省庁・産学官との連携の下、基礎的段階を含めたデュアルユース技術の研究開発を推進するとともに、例えば、オフキャンパス構想も念頭に、大学や国研等におけるセキュアな防衛研究基盤の整備に取り組む。経済安全保障重要技術育成プログラム（K Program）後継の制度設計について具体化を進める。また、海外の国家や非国家による研究への不当な干渉や技術流出を防止するため、特定研究開発プログラムにおける研究セキュリティを確保するとともに、大学等におけるサイバーセキュリティ対策を推進する。

出所）内閣府「統合イノベーション戦略2026」　https://www8.cao.go.jp/cstp/tougosenryaku/2026.html

日本発の破壊的イノベーション創出を目指す国の大型研究プログラム「ムーンショット型研究開発制度」では、2040～2050年までに達成を目指す、大胆な研究内容を掲げている

- 2026年現在、以下10項目の目標が設定されている
- 2020年の制度始動時の目標は1～6のみだったが、以降、順次目標が追加されている

ムーンショット型研究開発制度で掲げられている10の目標

出所）内閣府「ムーンショット型研究開発制度」 https://www8.cao.go.jp/cstp/moonshot/index.html

例えば目標1では、身体的能力や認知能力を拡張できるサイバネティック・アバター（CA）の研究開発が進められており、2030年までにロボットでの遠隔就労の実証を行うとしている

サイバネティック・アバター生活

- 2050年までに、望む人は誰でも身体的能力、認知能力及び知覚能力をトップレベルまで拡張できる技術を開発し、社会通念を踏まえた新しい生活様式を普及させる。
- 2030 年までに、対話・保持・移動能力を拡張させ、体験共有や技能融合を可能とするアバター又はロボットによる遠隔就労の概念実証を行い、民間投資対象となり得るアバターを開発する。
- 2030年までに、BMI(※1)を用いて人が想像する文字や画像を精度良く推定することにより、障害を持つ人のコミュニケーションを改善できる技術の概念実証を行い、その後の臨床試験に向けた資金を確保する。
- 2030年までに、体内に入れたアバターとの体外通信を可能とし、副作用の少ない治療技術の概念実証を行い、その後の臨床試験に向けた資金を確保する。

出所）内閣府「ムーンショット目標１」 https://www8.cao.go.jp/cstp/moonshot/sub1.html

セキュリティの観点で着目すべきエマージングテクノロジーの種別

まずは既に頭角を現している技術（直近では主にフロンティアAI）への対策が最優先となる。次いで、実装途上だが今後台頭すると考えられる技術への向き合い方も視野に入れるべき

エマージングテクノロジーの分類		具体例	社会への影響可能性の例
既に頭角を現している技術		**フロンティアAI**（最先端のAI技術・モデル）	従来は発見が困難であった脆弱性が短期間に大量に発見される
実装/普及途上にある技術	AIとの相乗効果がある技術	**デジタルツイン**（仮想空間で現実空間をモデリングする）	デジタルでのデータ改ざんが物理世界での損傷を引き起こし得る
	新規のデジタル関連技術	**サイバネティック・アバター**（遠隔操作でき自分の体と同じように感覚を共有）	リアルタイムの身分偽装・本人確認（KYC）の難化

2. エマージングテクノロジーにおけるセキュリティの論点

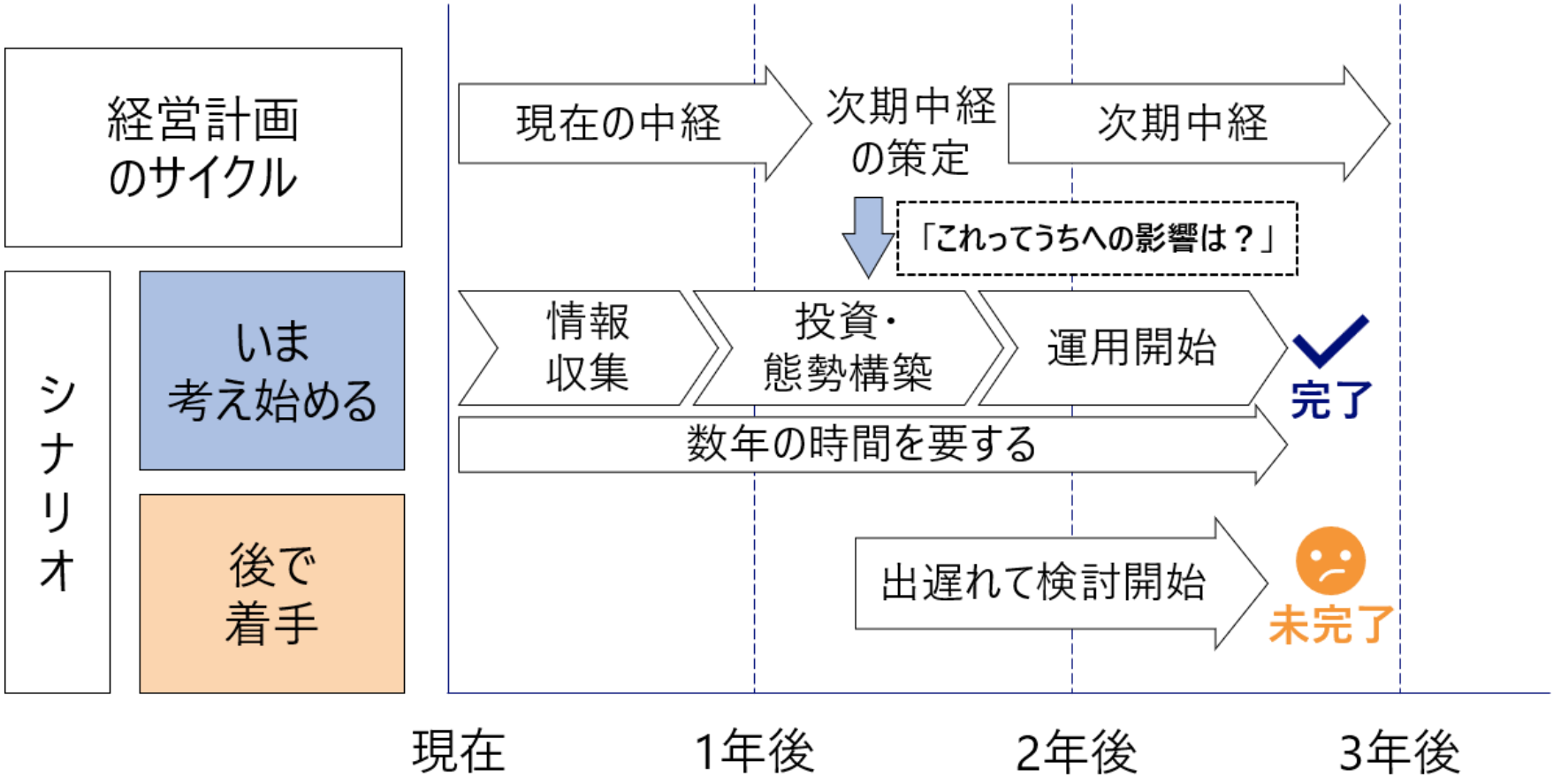
エマージングテクノロジーはなぜサイバーセキュリティに関係するか？

エマージングテクノロジーが社会実装される際、倫理的・法的・社会的課題（ELSI）が生じる。サイバーセキュリティは、エマージングテクノロジーに関するELSIの典型的な例

ELSIの分類	エマージングテクノロジー×サイバーセキュリティにおいて考えられる課題
Ethical（倫理的）	法的な定めがない状態で、エマージングテクノロジーに関するセキュリティ上の脅威分析や対策はどこまでやるべき？
Legal（法的）	新たに生じ得る規制にどのように対応する？
Social（社会的）	エマージングテクノロジーに関連して発生するセキュリティインシデントによる「炎上」にどう対応する？

早期にエマージングテクノロジーのセキュリティを検討することの意義

（セキュリティに限らず）投資や態勢整備には少なくとも数年単位の時間を要する。早期に考え始めなければ、次期経営計画等の際に「いきなり」オーダーが降ってくることも



エマージングテクノロジーに関係する主体

エマージングテクノロジーのセキュリティ対策は、開発者・提供者・利用者それぞれに責任がある。各主体の役割・責任を明確化し、リスクを特定することがセキュリティ対策の前提となる

主体	定義	主体の例	役割
開発者	研究開発・製品化を行う主体	• 研究機関 • 大学 • 企業（R&D部門） • スタートアップ	• 基盤技術の確立 • 安全性の検証 • セキュリティ実装
提供者	サービス・製品を提供する主体	• SaaS事業者 • プラットフォーマー • 製造業者	• リスク評価 • 利用規約の整備 • インシデント対応
利用者	サービス・製品を利用する主体	• 民間企業 • 行政機関 • 個人ユーザー	• 適切な利用 • リスクの理解 • インシデント報告

エマージングテクノロジーが社会実装に至るまでのセキュリティの論点

技術の成熟度に応じて、「研究セキュリティ」「セキュリティ・バイ・デザイン/プライバシー・バイ・デザイン」「アジャイルガバナンス」という主に3つのセキュリティ上の論点がある

■ 各主体が直面するセキュリティ課題をライフサイクル全体で把握することで、自社に波及するリスクを予見・評価できる

段階	研究開発	事業化	社会実装
論点 / 主体	① 研究セキュリティ	② セキュリティ・バイ・デザイン / プライバシー・バイ・デザイン	③ アジャイル・ガバナンス
開発者	情報管理体制の徹底	セキュリティ・プライバシー保護対策を実装	攻撃動向に基づく技術的対策の更新
提供者	事業化段階で出現する主体	利便性低下の阻止や取得データのリスク評価	法的・倫理的課題における利用者との合意
利用者	社会実装段階で出現する主体		自組織に合わせた利用ガイドラインの策定・見直し

① 研究セキュリティ

【論点①】研究セキュリティによる情報管理と技術流出防止は、エマージングテクノロジーの研究開発の初期段階から不可欠。国家安全保障と競争力維持の基盤となる

研究セキュリティの定義

機微情報・技術の流出等といった国家安全保障上のリスクから研究活動を保護するために研究者に求められる行動のこと

エマージングテクノロジーにおける研究セキュリティの重要性

AIや量子分野等、軍事転用が可能なデュアルユース技術は、技術流出した際に国家安全保障上のリスクになる可能性が高い。また、国際研究において、研究機関の情報管理体制が求められる等、健全な研究活動が求められる傾向にある

主体別のアクション

開発者	提供者	利用者
• 情報管理体制の構築 • アクセス制御の実装 • 研究データの暗号化	事業化段階で出現する主体	社会実装段階で出現する主体

研究セキュリティを考慮しなかった際に想定されるリスクの例

量子分野

・既存の暗号の解読を狙った未公開の理論・実験データの持ち出し

バイオテクノロジー分野

・危険な病原体や毒素のデジタル設計データの流出・悪用
・大規模な個人ゲノム情報の漏えい

② セキュリティ・バイ・デザイン / プライバシー・バイ・デザイン

【論点②】設計段階からセキュリティとプライバシー保護を組み込むことで、最終的な対策のコストとリスクを低減することができる

セキュリティ・バイ・デザイン / プライバシー・バイ・デザインの定義

設計・開発の初期段階からセキュリティとプライバシー保護を組み込む考え方のこと

エマージングテクノロジーにおけるセキュリティ・バイ・デザイン/プライバシー・バイ・デザインの重要性

エマージングテクノロジーの事業化および社会実装後の脆弱性対策や漏洩事故による莫大な手戻りによる後付けのセキュリティ対策コストの軽減に不可欠である。また、新技術に対する社会的な信頼を獲得し、安全でスピーディーな社会実装を実現可能

主体別のアクション

開発者	提供者	利用者
• 脅威モデリングの実施 • 最小権限原則の適用 • 収集データ最小化の実践	• 技術制御による利便性の低下防止 • データの法的な取り扱い検討 • ユーザーへの透明性確保 • インシデント対応体制構築	社会実装段階で出現する主体

セキュリティ・バイ・デザイン/プライバシー・バイ・デザインを考慮しなかった際に想定されるリスクの例

自動運転・自律型モビリティ分野

・外部からのハッキングやセンサー偽装によるシステム乗っ取り
・出荷後の脆弱性発覚による大規模リコール

ブレイン・マシン・インターフェース分野

・脳波データ（思考・感情のシグナル）の不正取得やデータの改ざん

③ アジャイル・ガバナンス

【論点③】急速に進化するエマージングテクノロジーには、硬直的な規制や対策ではなく、社会・技術動向に応じた継続的な対策のアップデートや主体同士の連携が不可欠

アジャイル・ガバナンスの定義

技術・社会の変化に応じて規律を柔軟に見直し、継続的に改善するガバナンスのこと

エマージングテクノロジーにおけるアジャイル・ガバナンスの重要性

エマージングテクノロジーは急速に進化するため、従来の固定的な規制では技術の進展速度に追いつけず、イノベーションの阻害やリスク対応の遅れにつながる。各主体同士が継続的に連携し、合意形成していくことが必要

主体別のアクション

開発者	提供者	利用者
• 攻撃動向に基づく技術的対策の更新 • 脆弱性の迅速な修正 • セキュリティパッチの継続的提供	• 法的・倫理的課題における利用者との合意形成 • 利用規約の継続的見直し	• 自組織に合わせた利用ガイドラインの策定・見直し • インシデント報告 • セキュリティ意識の醸成

アジャイル・ガバナンスを考慮しなかった際に想定されるリスクの例

宇宙産業分野

・宇宙ゴミの削減ルールや軌道・周波数の割り当ての更新の遅れによる衛星同士の衝突や電波干渉が発生

ナノテクノロジー分野

・新世代のナノ素材に対する安全評価基準の策定の遅れによる人体被害・環境汚染

3.「ちょうどいい」セキュリティガバナンスの重要性

「ちょうどいい」セキュリティガバナンスとは？

適切なエマージングテクノロジーの利活用は社会発展の起爆剤となる。ポジティブリスクの増大とネガティブリスクの低減の双方を意識した、「ちょうどいい」ガバナンスの意識が不可欠

- エマージングテクノロジーがもたらす利便性等の**ポジティブリスクが意識されず、ネガティブリスクのみが意識される場合、過度な統制**につながりイノベーションが阻害され得る
- 一方で、セキュリティ/プライバシーの問題等の**ネガティブリスクに目をつむりすぎると無秩序な利用**につながり、ステークホルダーの信頼を失いかねない
- **ポジティブリスクが意識されつつもネガティブリスクが十分に低減**された、**ちょうどいいガバナンス**の実現が目指されるべき

過度な統制

イノベーションが生まれにくく、
価値創出に繋がらない

ちょうどいいガバナンス

ポジティブリスクが意識されており、
かつ、ネガティブリスクが十分に低減されている

無秩序

リスクが顕在化しやすく、
ステークホルダーの信頼を失ってしまう

AI利活用における「ちょうどいい」ガバナンスの例

真に回避すべきリスクは抑えつつ、スモールスタートでガバナンスを運用開始する。運用しながら適宜改善を図り、社会や技術の変化にも対応することが重要

AIのガバナンス構築および運用・改善の対応事例

ガバナンス構築

① AIのユースケースや利用パターンの特定

② 想定される脅威やリスクの導出

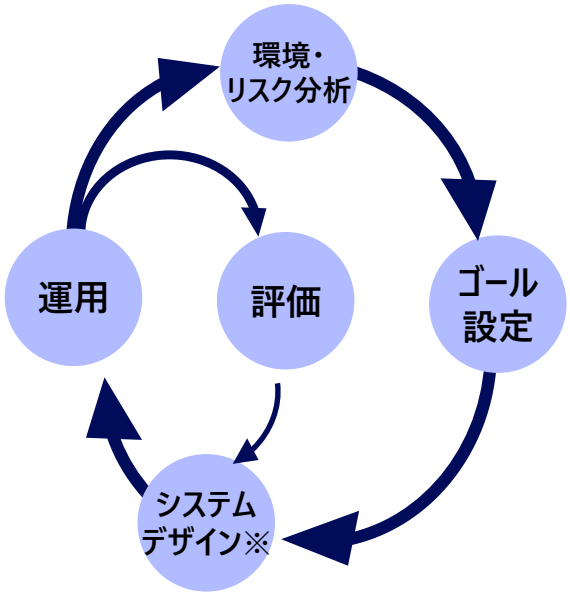
③ 脅威・リスクを基に対策と運用を検討

④ 既存の社内ガバナンス態勢への組み込み

ガバナンス運用・改善

⑤ 運用と並行で継続的に改善（アジャイル・ガバナンス）

外部環境の変化



ステークホルダーに対する透明性・アカウンタビリティ（公平性等）

※社内の規程・運用整備等を通じたマネジメントシステムの設計を指す（情報システムとしてのAIシステムの設計を指すものではない）

出所）総務省・経済産業省「AI事業者ガイドライン（第 1.2 版）」の「E. AI ガバナンスの構築」をもとにNRIセキュアが作成

AI活用想定の業務ユースケースをヒアリングや業務資料から棚卸しし、各ユースケースで想定されるリスクを整理する

- 要点を押さえたセキュリティ対策・運用ルールを策定するため、社内のAIユースケースや利用パターンを特定し、重要なリスクを把握する
- 脅威やリスクの導出にあたっては、AIガバナンス関連の法規制・ガイドラインにおける要求/提示内容、インシデント事例も調査する

AIユースケースと脅威・リスクの整理の例

AI活用想定の業務ユースケースの例

業務	インプット	アウトプット	使用用途
• 問合せ受付	• 顧客の音声データ • 顧客のWebフォーム入力データ	• 問合せ情報データ	• 社内利用 • 顧客送付（問合せ内容確認）

AI活用により想定されるリスクの例

リスク分類	リスク例	リスクレベル
データ品質	音声認識等の精度不足による誤入力や誤出力が、登録内容の不備につながる	低
偽・誤情報の出力	入力データの参照違いに起因する誤出力により、問合せに対して不適切な対応を行ってしまう	中
プライバシー保護	顧客の個人情報や企業の非公開情報が漏えいする	高
セキュリティ確保	プロンプトインジェクション等の攻撃により、チャットボットが不正操作されシステムが侵害される	高

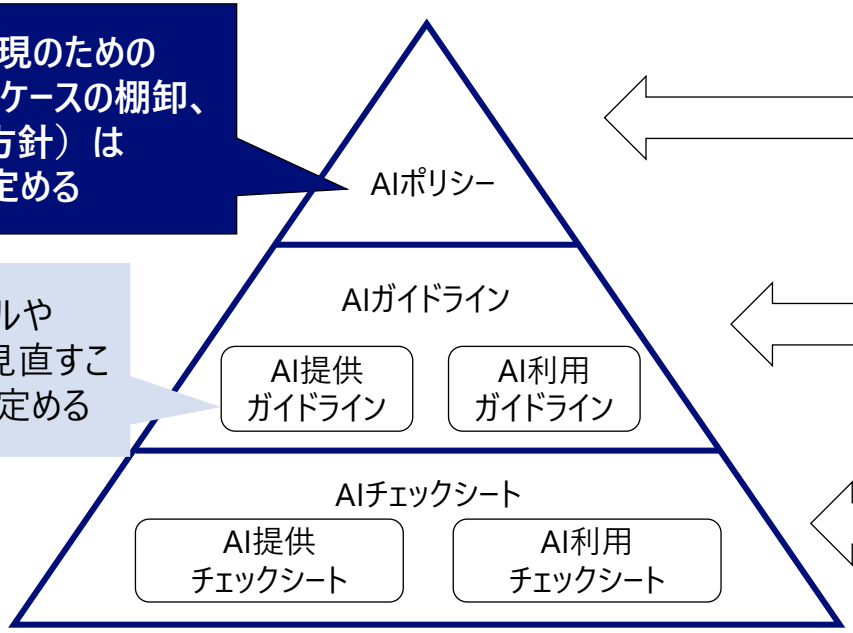
代表的な業務ユースケースを議論の土台とし、リスクレベルを踏まえてルールを検討する。また、既存の社内ガバナンス関連ルールとの整合性を確保することで、実効性を高める

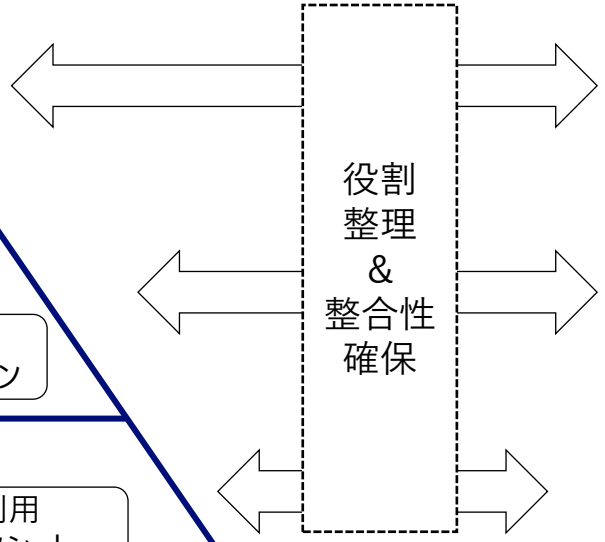
- **セキュリティインシデント等のネガティブリスクを極小化することのみを目的とするのではなく、AI利用により得られるポジティブリスクとのバランスも考慮して（＝「ちょうどいい」）ルールを定める**
- AI利用を促進するため、ルールは極力シンプルで運用しやすいものとし、既存のルール・体制に組み込む
- 運用ルールやセキュリティ対策は随時見直す前提で定めるが、アジャイル・ガバナンスの実現に必要な仕組みは、ガバナンス構築時に確立する

AIガバナンスのルール体系の例

アジャイル・ガバナンス実現のための仕組み（定期的なAIユースケースの棚卸、リスク評価等の実施方針）は最上位のルールで定める

個別具体的な運用ルールやセキュリティ対策は、柔軟に見直すことを想定し、下位の文書で定める





既存のガバナンス関連文書

【例】
・セキュリティ
・品質管理
・知的財産
・法務、広報 等

AIガバナンス構築・運用の例　⑤運用と並行で継続的に改善

「アジャイル・ガバナンス」の考えに基づき、継続的にガバナンスの見直し・改善を行うことで、時流の変化への対応と、運用成熟度の向上を図る

- **継続的にリスクと対策の見直しを行うことで、エマージングテクノロジーの特性である、技術の急速な成熟や不確実性に起因するリスクにも対応できる**
- 社内外の状況を考慮して、状況に適したルールとなるように運用を見直すことは、AI利用の促進や適切な管理を実現し続けることにもつながる

継続的な運用改善で反映する要素と効果の例

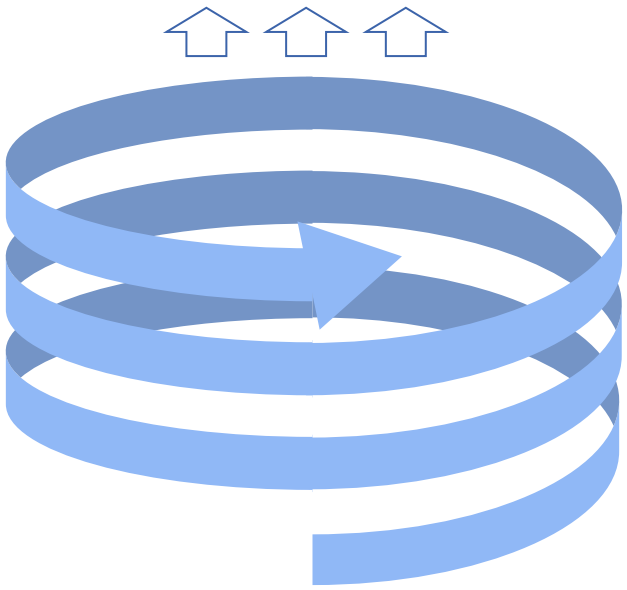
エマージングテクノロジーの特性

- AI技術の発展
- 技術自体の特性から想定されるリスク

社内のAI利用状況

- 社内のAIユースケース/利用パターン
- 各AIユースケースにおける想定脅威・リスク

新たなリスクへの対策
「ちょうどいい」ガバナンスの維持
セキュリティや運用の成熟度向上



内部環境

- AIガバナンスルールの運用上の課題
- 他のガバナンスルールや組織体制の変化

外部環境

- AI関連の社会動向（法規制、大規模インシデントの発生状況等）
- 取引先や業界団体からの要請

4. まとめ

まとめ

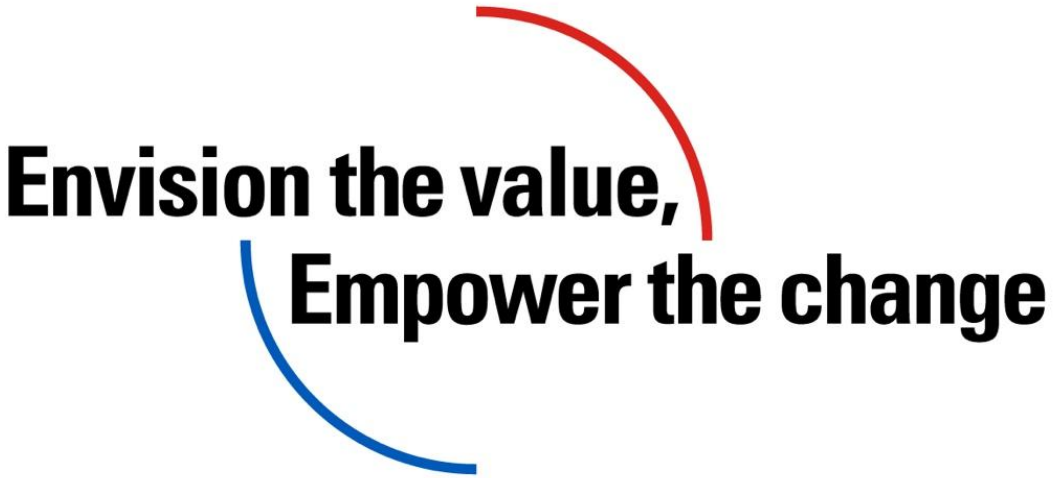
エマージングテクノロジー（AIやその先）は事業に大きな影響を与えるため、正負双方の観点の考慮が不可欠。まずはスモールスタートで、自社に「ちょうどいい」ガバナンス構築を目指すべき

■ **エマージングテクノロジーは単なる「新しい技術」ではない。**
事業にポジティブ/ネガティブ双方の観点で大きなインパクトを与える

■ AIが目下最重要なエマージングテクノロジーであることは間違いないが、**「AIに連なるもの」や「AIの次」がある**

■ 脅威やネガティブリスクという観点に加え、**ポジティブリスクという観点でもリスクを眺めるという「ちょうどいい」ガバナンス**が重要

■ 全社的な取り組みに着手するのが難しい場合は、**一部の部門からでもまずはスモールスタートで歩み始める**ことが、「ちょうどいい」ガバナンスの構築に繋がる


Envision the value,
Empower the change