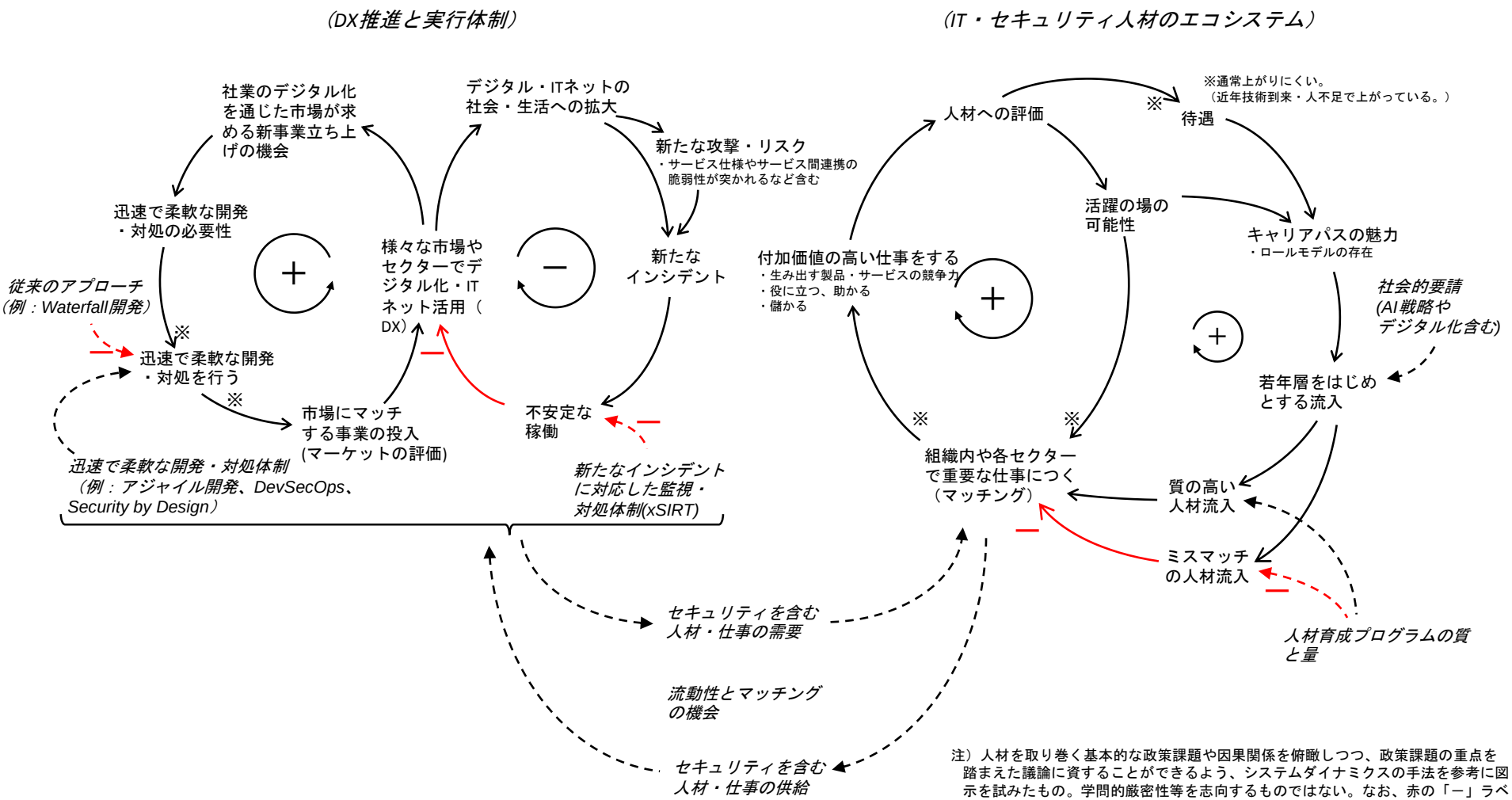
（政策議論のための補助フレームワーク）

資料1-2

DX with Cybersecurity の推進

（日本でDXが進み、セキュリティが保たれること、あるいは同時推進）



注）人材を取り巻く基本的な政策課題や因果関係を俯瞰しつつ、政策課題の重点を踏まえた議論に資することができるよう、システムダイナミクスの手法を参考に図示を試みたもの。学問的厳密性等を志向するものではない。なお、赤の「－」ラベルの矢印は負の因果関係を示す。また、「＋」とあるループは正のフィードバックループまたは増強ループ、「－」は負のフィードバックループまたは平衡ループと呼ばれる。「※」は因果に複雑さや遠さが含まれる関係を試みに示し、点線はループの外からの入力をイメージしている。

（参考１）

従来の構図

○ ユーザ企業にとってITは人ごとで丸投げ

○ 丸投げを受けるベンダーと多重下請け構造

- ー 社内のシステム・ソフト
- ー 会社・部門毎のカスタマイズや複雑化したシステムの維持
- ー 付加価値が高くない
- ー 下請けの専門人材が人月工数で仕事
- ー ユーザ企業の内部にノウハウが蓄積しにくい

○ メンバーシップ型雇用

DXを実現する構図
（＝図のサイクルを回す構図）

○ ユーザ企業の主体的なIT活用とDX実施

○ ユーザ企業の主体性と専門ベンダーを使う意識

- ー 社業を担い顧客価値を生み出すシステム・ソフト
- ー 事業（社業）の自社ならではの基幹部分のコンピテンシーをシステム・ソフトで実現
- ー 付加価値が高い
- ー 専門人材の能力発揮
- ー 蓄積したノウハウを活かし更に発展・改善

○ ジョブ型雇用

鍵と考えられるもの

・ユーザ企業におけるIT・セキュリティ人材の活躍 （前ページの推進）

・ユーザ企業においてDX経営・事業を担う者が「＋IT」「＋セキュリティ」知識を補充できる環境 （併せて推進する必要あり）

（参考２）

○ なぜサイバーセキュリティ政策の観点からも、DX推進を重視するのか。

・重要かつ構造的な政策課題（ユーザ企業における人材不足や次世代にとってのキャリアの魅力等）をwin-winで解決できる可能性があるため。

・相当数の企業は、それぞれが置かれた競争環境やウィズコロナでDXを進めると考えられ、何にせよ、DXに伴うセキュリティ政策課題を検討する必要があるため。

・業界や業界内によってDXの進展に差が出ると、セキュリティの差になり得るが、サイバーセキュリティ政策上、それは望ましくないため。（攻撃者は弱いところを狙うため）

サイバーセキュリティに係る人材の確保、育成、活躍の促進

（政策議論のための補助フレームワーク）
※経営層・戦略マネジメント層を加えた全体像と政策インプット

DX with Cybersecurity の推進

経営層

【経産省】
・サイバーセキュリティ経営ガイドライン（2017,ver.2.0）
＋ガイドライン実践のためのプラクティス（2020.6）
＋ガイドライン実践状況の可視化ツール（2020.3, β版）

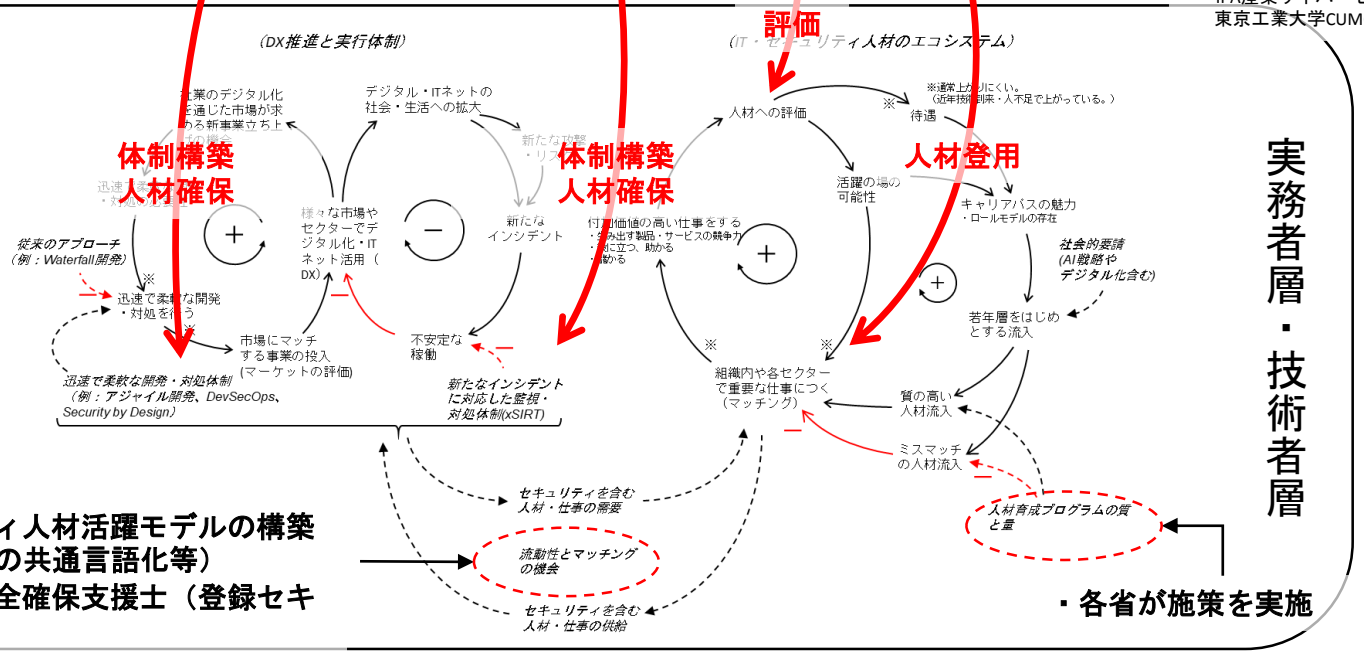
「＋IT」「＋セキュリティ」知識

戦略マネジメント層

戦略マネジメント層の育成・定着

【経産省】
・戦略マネジメント層育成教育
2018～
IPA産業サイバーセキュリティセンター（ICSCoE）
東京工業大学CUMOT

実務者層・技術者層



【経産省】
・セキュリティ人材活躍モデルの構築（役割定義の共通言語化等）
・情報処理安全確保支援士（登録セキスペ）制度

・各省が施策を実施