サイバーフィジカル時代の経営とセキュリティ

クロサカタツヤ（株式会社 企）

2022年12月13日

自己紹介：クロサカタツヤ

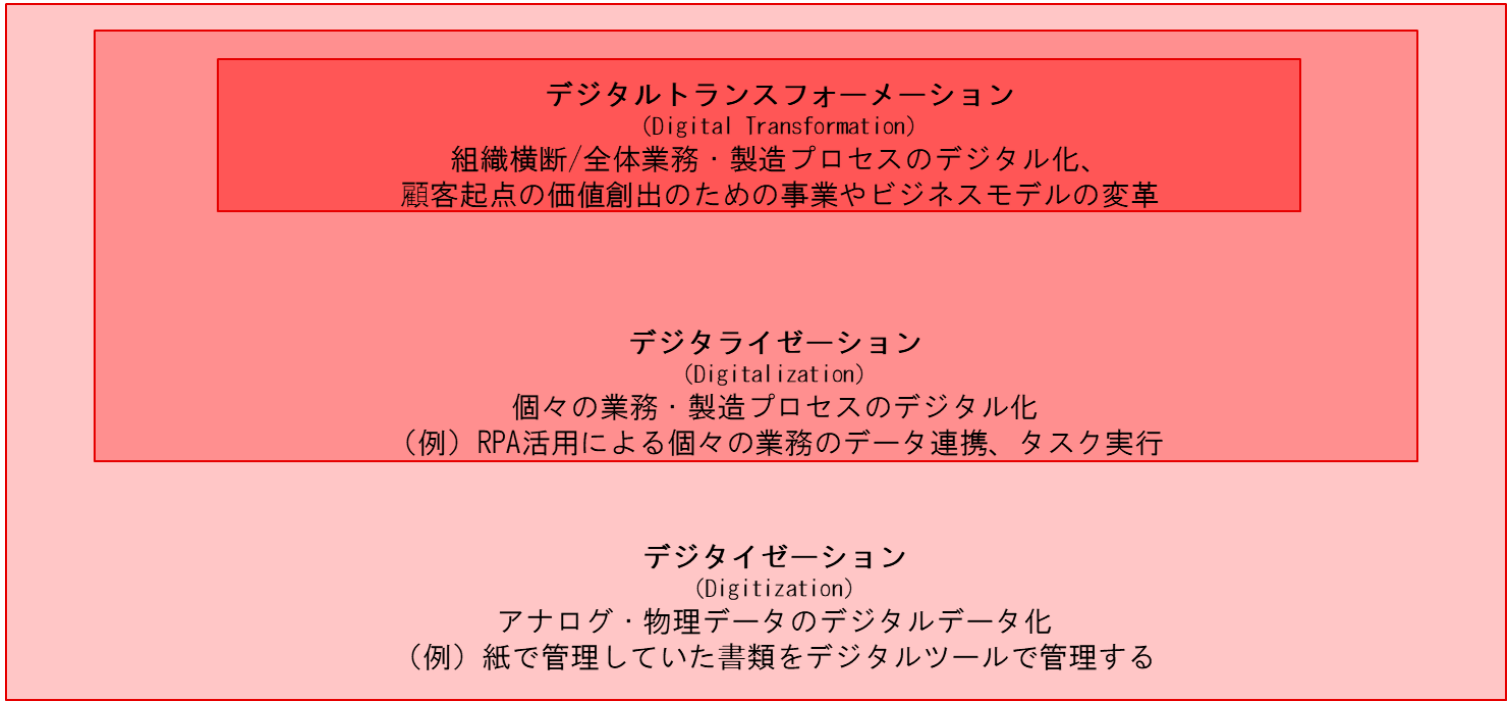
株式会社 企（くわだて）　代表取締役
慶應義塾大学大学院政策・メディア研究科　特任准教授

【略歴】
1999年慶應義塾大学大学院政策・メディア研究科修了。三菱総合研究所を経て、2008年に株式会社 企（くわだて）を設立。通信・放送セクターの経営戦略や事業開発などのコンサルティングを行うほか、総務省、経済産業省、OECD（経済協力開発機構）などの政府委員を務め、政策立案を支援。2016年からは慶應義塾大学大学院特任准教授を兼務。
近著『5Gでビジネスはどう変わるのか』（日経BP刊）。

【主な役職等】

- 総務省　電気通信事故検証会議（2022年～）
- 総務省 デジタル時代における放送制度の在り方に関する検討会 小規模中継局等のブロードバンド等に よる代替に関する作業チーム 構成員（2022年～）
- 公正取引委員会 デジタルスペシャルアドバイザー（2021年～）
- 内閣官房デジタル市場競争本部　Trusted Web推進協議会委員／同TF座長（2020年～）
- 総務省 ICTサービス安心・安全研究会 消費者保護ルールの検証に関するWG委員（2018年～）
- IoT推進コンソーシアム データ流通促進WG 委員（2018年～）
- インフォメーションバンクコンソーシアム 監事（2018年～）
- OECD日本政府代表団員（2009年～）
- 総務省 消費者保護ルール実施状況のモニタリング定期会合（2016年～）
- IPA専門委員（人工知能）、等

ＤＸとは何か？

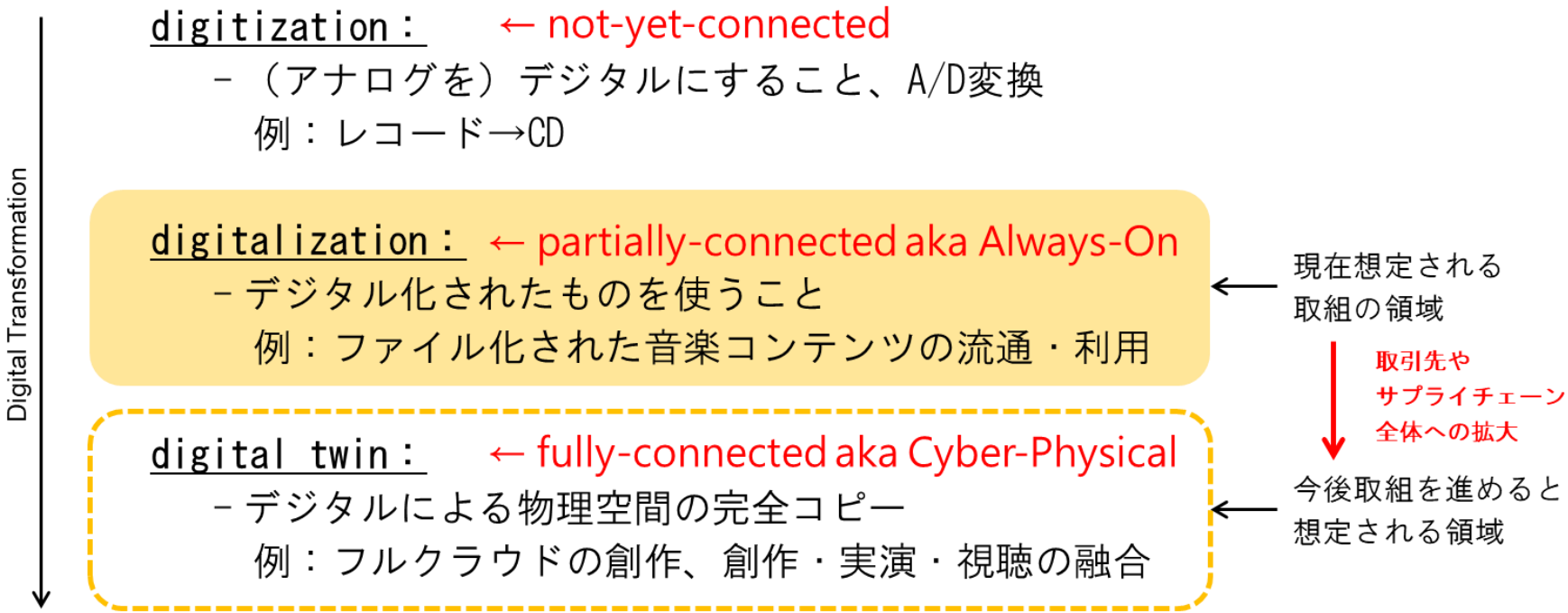


「企業が外部エコシステム（顧客、市場）の破壊的な変化に対応しつつ、内部エコシステム（組織、文化、従業員）の変革を牽引しながら、第３のプラットフォーム（クラウド、モビリティ、ビッグデータ／アナリティクス、ソーシャル技術）を利用して、新しい製品やサービス、新しいビジネスモデルを通して、ネットとリアルの両面での顧客エクスペエンスの変革を図ることで価値を創出し、競争上の優位性を確立すること」

出所　経済産業省「デジタルトランスフォーメーションを推進するためのガイドライン」

ＤＸとは何か？

- DXはゴールではなく「永遠に続く運動」であり、人間はもはやそこから逃れることは不可能
- デジタライゼーションの次はデジタルツイン（サイバーフィジカル）の実現



ＤＸの真価は効率化ではなく「機会の拡大」

出所　弊社撮影

- 「Amazon Goは無人店舗」という致命的なウソ
  - 入口に堂々と書かれた真実
  - 従業員は日本のコンビニより多い
  - 店舗フォーマットはすでに多様化

- 社会の本質的なニーズはどちらにあるか

「効率化」のためのデジタル

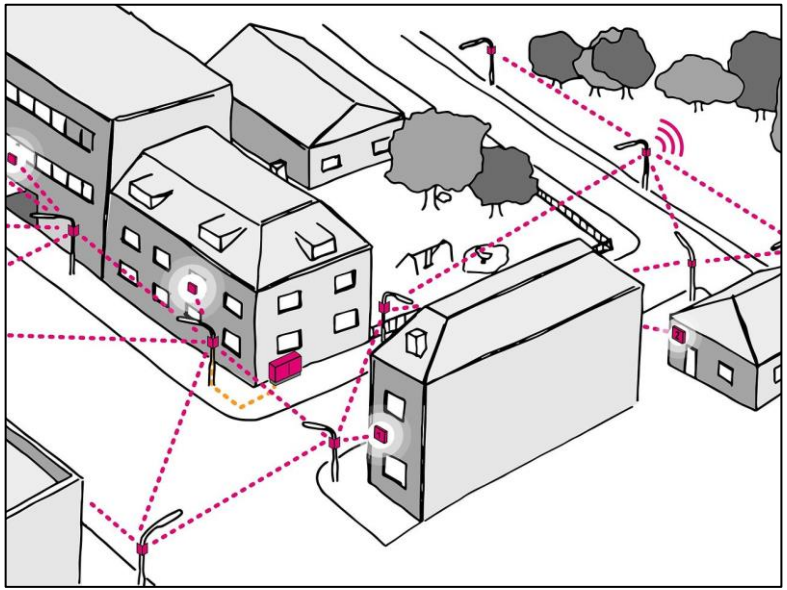
  - 無人コンビニ
  - 認知症患者を「監視」するためのセンサー

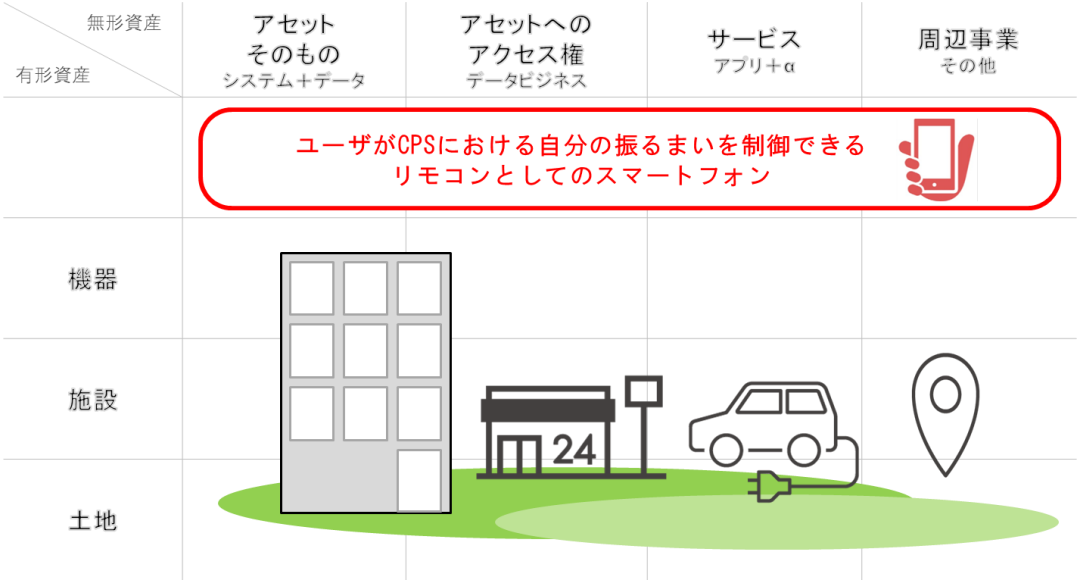
「機会の拡大」のためのデジタル

  - Amazon Go
  - 認知症患者が「お散歩」するスマートシティ

デジタルの高度化は空間のＤＸに向かう

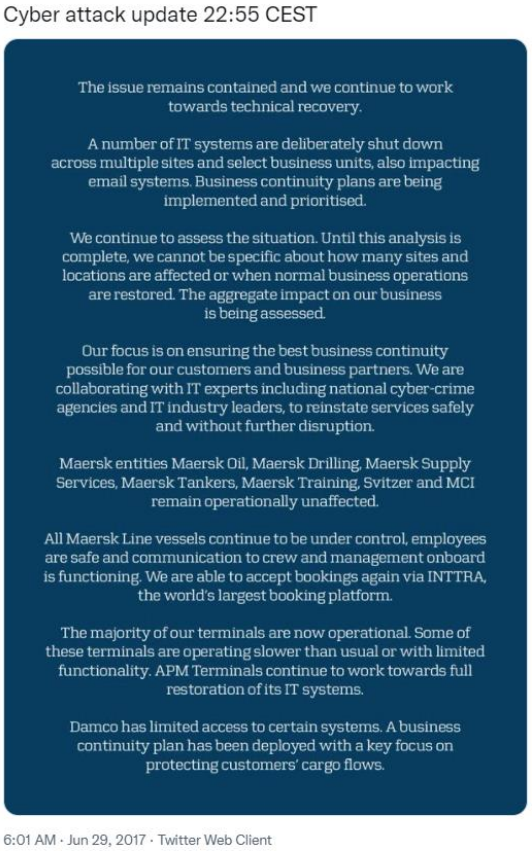
- 「つながったら便利」ではなく「つながらなければ無意味」の時代の到来
- スマートデバイスはただのリモコン（操作のための小窓）となり、フィジカルスペースがデジタルサービスの舞台になる





出所：https://www.telekom.com/en/company/details/virtual-fiber-563322

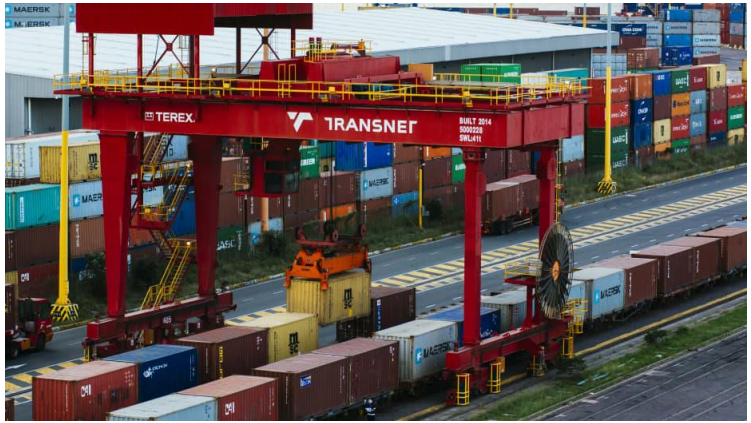
フィジカルスペースへ向かうサイバー攻撃：海運分野の例



- 2017年6月に発生したMaerskの大規模インシデント
  - 発端は、ウクライナ・オデッサのMaerskオフィスにあったPCの会計ソフトM.E.Doc、その外部サーバにマルウェアが仕組まれていた
  - ウィルス発動後、即座にデンマークの本社システムに感染が広がり、そのわずか7分後には世界130カ国のオフィスで不具合発生
  - データ汚染はもちろん、5万台近いPC、サーバ、プリンタ等の周辺機器が破壊、またスマートフォン等にも障害が及んで通信が断絶
  - 業務が全面的に停止し、結果として3億米ドル相当の実害が発生
  - ナイジェリアの同社オフィスで停電が発生したことで、感染から「偶然」免れたデータを物理的にコピーし、デンマークへ輸送することで、10日間程度で業務プロセスと情報システムを復旧
  - これがなかったら、Maerskの業務は6か月停止し、我が国を含む世界の海運にとって悪夢となった可能性もあった

出所　インシデント発生直後のMaersk社ツイート

フィジカルスペースへ向かうサイバー攻撃：海運分野の例



- 海運業界を狙った標的型攻撃（主にランサムウェア）の例
  - 2020年4月：スイス・イタリアMSCがネットワーク停止
  - 2020年5月：豪Tollが巨大な取引データ窃取
  - 2020年9月：フランスCMA-CGMが顧客データ流出
  - 2020年9-10月：国際海事機関（IMO）が業務を一時停止

- 港湾を狙った標的型攻撃の例
  - 2021年7月、南アフリカ国営物流会社TRANSNET社の同国主要港湾ターミナルが7月22日に大規模なサイバー攻撃を受け、同社の通常操業機能が中断し不可抗力宣言が発表
  - コンテナターミナルの出荷システムは手動に切り替えられ、ケープタウン港、ポートエリザベス港、グクラ港、ダーバン港等、南アの主要な港湾の操業が大幅に中断

出所　South Africa port operations halted and workers reportedly put on leave after major cyberattack (CNBC)
https://www.cnbc.com/2021/07/27/transnet-halts-port-operations-in-south-africa-after-major-cyberattack.html

フィジカルスペースへ向かうサイバー攻撃：海運分野の例

- 海運業界が狙われる理由
  - ボトルネックが発生・特定されやすい
  - 当事者が限定的
  - 情報化が発展途上
  - ITとOTの混在による被害拡大リスク

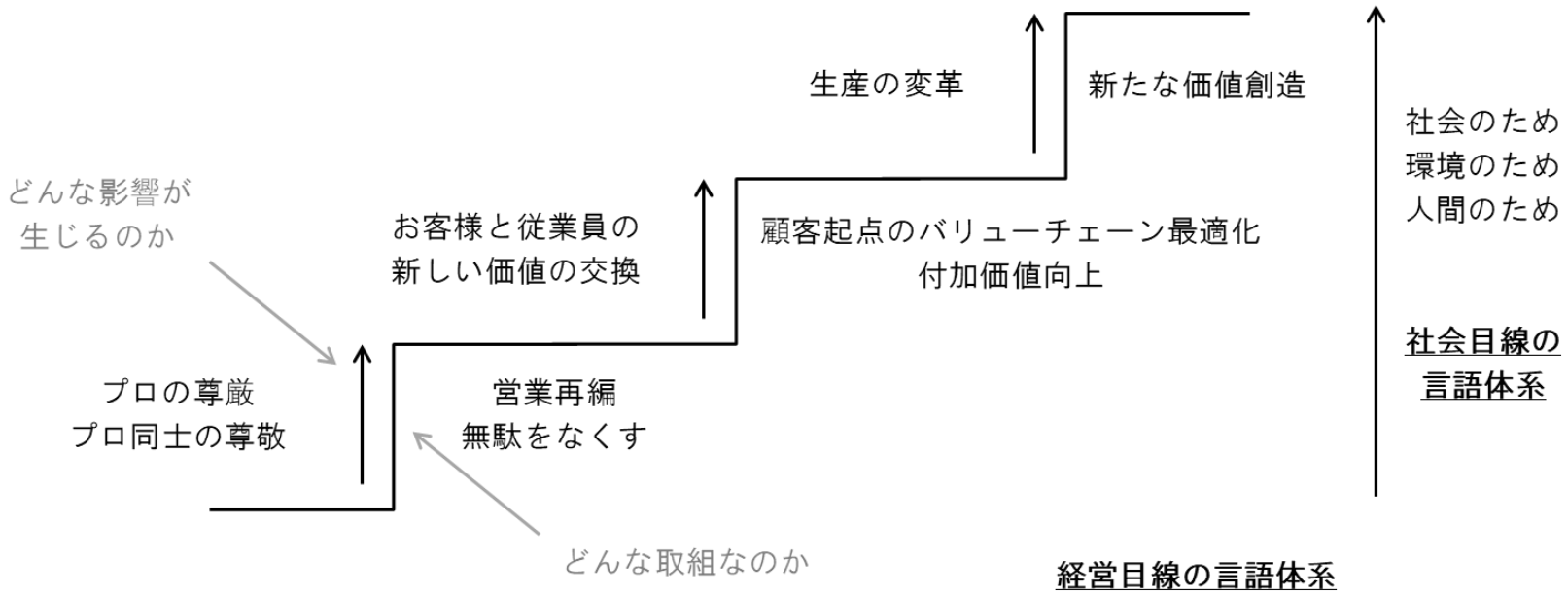
- 港湾のリスク・脆弱性
  - 港湾はボトルネックになりやすい
  - 港湾はステークホルダが多様で複雑
  - 港湾事業者だけでのセキュリティ対策に限界
  - 港湾設備の特殊性
  - 港湾業務の繁忙による対策の劣後

出所　東京都港湾局ツイッター　https://twitter.com/tocho_kouwan/status/773436899876806656/photo/2

どうして躓くのか：ステークホルダーの視点の欠如

- ステークホルダーを厳格かつ詳細に定義できていない
- ステークホルダーによる視点の違い・価値の違い・言語の違いを理解できていない
- 結果としてシステム全体のペインポイントが特定できない

ユーザ目線／従業員目線の言語体系



どうして躓くのか：企業活動が体系化できていない可能性

- ポリシー（方針）、ガバナンス（統治）、マネジメント（管理）、テクノロジー（技術）の区別は明確か
- 守るべき資産、相対する相手、関係者の生態を理解した上で、自社の取組で必要／不要の区別はできているか

アプローチ	内部統制	コーポレート ガバナンス	スチュワードシップ コード	厳格責任の対応 （製造物責任法等）
目的	**リスク管理**	**ステークホルダーの 利益最大化**	**受託者責任の明確化 （例：取引先への信用提供）**	**消費者保護と 責任分界の両立**
取組の ポイント	• 既存の取組との整合 • インセンティブ管理 • 社内定着	• ステークホルダー間の均衡の実現 • 司法的役割（監査や裁定）の提供	• 外部から委託された業務や資産に対する責任	• 責任分界の設定（特に消費者とB2C企業間） • 責任領域の厳格対応
指向性	社内を 指向	←	→	社外を 指向

無謬の妄想を捨てて「現実的なセキュリティ」を目指す

- 基本的なスタンス
  - 最初から完璧を求めない
  - できるだけ早く直す
  - 守る対象（モノ・コト・資産）を特定する
- ハード（設備）
  - 汎用化、多重化、冗長化
    - 特殊な専用設備ほど復旧が遅くなる
- ソフト（運用）
  - 個人の責任追及ではなく全体の原因究明
  - 現場を委縮させないことが「早く直す」の要諦
- プロの支援を受ける
  - もはや「敵方」はプロの犯罪者
  - さらに言えば「正規の軍隊」（cf. ウクライナ戦争）

「壁」をどう乗り越えるか

- 内発的な取組の難しさ
  - 危機が起きてから、という「後手」の対応になりやすい
  - 課題が顕在化しないと「予算化」しづらい
  - でも、起きてからでは遅い
- 「日常的な感覚」を活かす
  - 実は日本人は「個人として」すでにDXを実現している
  - 日常感覚を業務にどう取り込むかがカギ
  - 特別なことをしようとせず、日常感覚・日常業務の一歩だけ先にセキュリティがある、という理解の醸成が必要
- たとえば…
  - プライベートでの、サイバー空間上のちょっとしたトラブルや炎上体験を共有する「雑談」から始める

デジタルが「責任ある社会インフラ」になるために

- 伝統的社会インフラと同水準の安全をデジタルで作る
  - 電気・ガス・水道と同水準のデジタルインフラを目指す
  - 求められるものは、無事故ではなく迅速な復旧
  - すでに経済安保では「インフラ以上」を求められ始めている

- “Don’t trust, verify” → “Trust, but verify”
  - すべてを疑ったら社会生活は成立しない
  - 信頼とは「まず任せてみる」ということ
  - その上でふとした違和感を覚えたら正直に「検証」する