分野間データ連携基盤の整備に向

http://www8.cao.go.jp/cstp/tyousakai/datar

まず、繋げて動かす！
民間の邪魔をしない！

[1] 相互接続ファースト

- P.4

なお、当該基盤の構築のプロセスにおいては、**統一的な技術仕様の策定や実装を待つことなく、迅速に（agileに）**分野間のデータ連携が行われることを目指すべきであり、その実現に向けて、共通語彙、ＡＰＩ、メタデータの仕様等を広く公開し、**利用・導入される技術仕様の透明性を確保することで、相互接続性・連携稼働性を向上し、データ連携の促進を図る。**すなわち、分野間の相互接続性の実現を優先し、分野毎のデータ連携基盤の構築によって培われた**開発・実運用の経験を共有し**さらに当該システムの
続的なＰＤＣＡサイクルによる段階的整備を迅速に（

もう一つ！
1. 標準化を目的にしない。
2. 標準化を補助金の
   梃子にしない。

[2] セキュリティーの確保

- P.15-16

iv）**サイバーセキュリティの確保**

- IoTで全てのヒトとモノがつながるSociety 5.0 では、サイバー攻撃の起点が増大するとともに、**複雑につながるサプライチェーン**を通じてサイバーリスクの範囲が拡大する。また、サイバー攻撃による影響がフィジカル空間にまで達するリスクがある。データ流通市場の活性化が進み、大量のデータが**グローバルサプライチェーンにおいて連携**し、データの利用・再販が進むことを想定すると、**ハイレベルなサイバーセキュリティ対策を備えた分野間データ連携基盤**を構築することが重要である。

経済産業省「産業サイバーセキュリティー研究会」

1. **サプライチェーン**(=3層構造のValue Creation Network)としてのサイバーセキュリティー
2. **経営・財務**&**企業統治(監査)**への包含
3. 産業分野ごとに対応策を立案・実施
   a. **全産業共通 と 産業分野ごと での 2階建て構造**
   b. **全産業での データセンターの利用**
4. **{シニア}人材**の確保と活用

経産省
仕込中

頭にくる? 常套手段(=ビジネス慣習)

1.調達
2.監査

1. 外部とは接続されませんので 安心してください。
   ✓安全な環境ですので事故は発生しません ➔ 無策・非対応
2. 独自技術ですので、『安全』かつ『安価』です。
   ✓独自技術で顧客を囲い込み(=ロックオン) ➔ PLもBSも“悪化”
   ✓でも、オープン技術がどんどん浸食中
3. お客様がご希望されます機能を提供することは、
   ① 不可能です(実は可能であることは知っている!!)。
   ② 新たに大きな開発費用と検証費用が発生します。➔ 事実ですが…
   ③ 他社との接続をしますと動作保証の対象外になります。➔ 脅し
4. 仕様変更・追加は、コスト増加(=避けるべき)につながります。
   ✓Updateは『行わない(will not)』 &『行えない(can not』
5. 納期と予算を守るためには、冒険しない方が。➔忖度(脅し)

バックアップ

ということで、重要な 考え方と 施策

1. 個別システムごとのサイバーセキュリティー対策
   ➔ サプライチェーン(=value creation network)としての対策
2. 既存システム と 新規システム
   a. 既存システムへの 緊急対策
   b. 新規システムへの 戦略的対策 (“調達条件“)
3. 利益にならなかったコスト部門に 利益を出させる！!
   a. 財務管理・財務表への包含
   b. 潜在的損失項目(BS&PL) vs 損失削減投資(PL)
4. 『実装機能』の確認・認証
   ➔ 『統治耐性 と プロセス(手順)』の確認・認証

1.調達
2.監査機能
3. IR 評価

分野間データ連携基盤の整備に向けた方針(2018年4月)

http://www8.cao.go.jp/cstp/tyousakai/datarenkei/3kai/3kai.html

- P.15-16

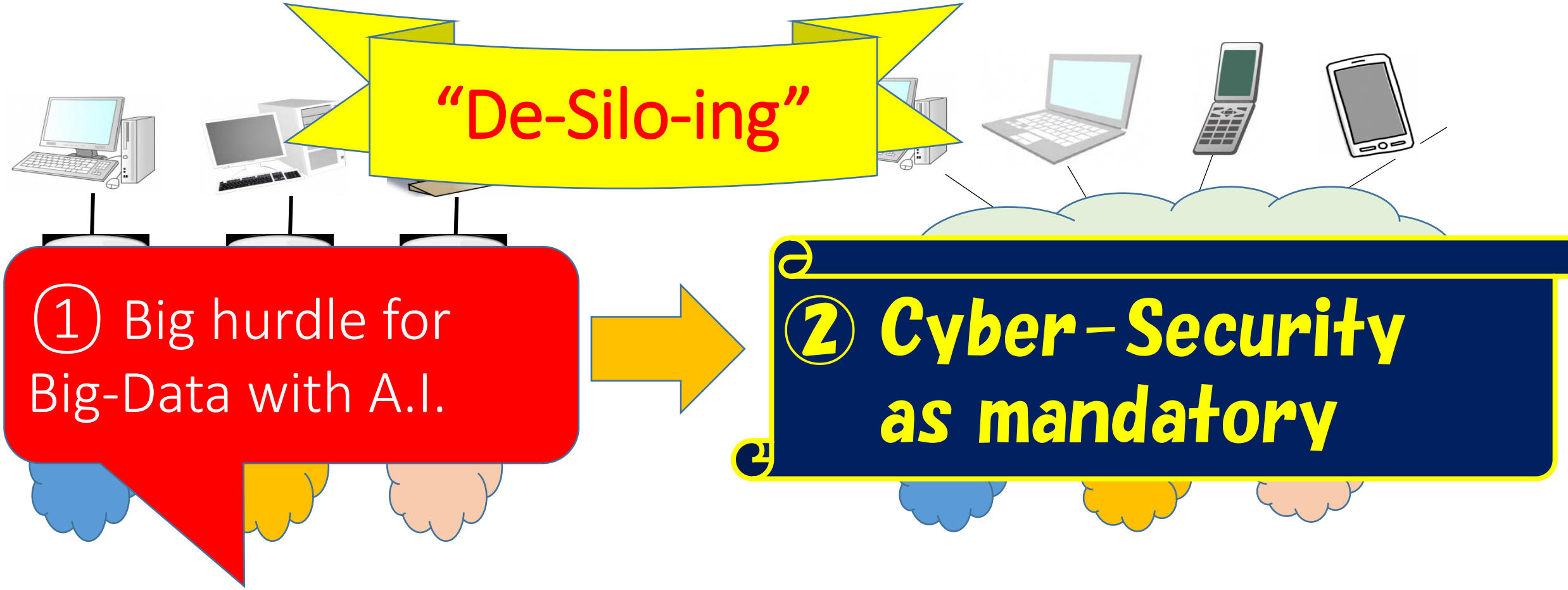
  ii）**民間データセンターの活用**

  - データセンターについては、その維持管理やサイバーセキュリティ対策に必要な人的リソースの継続的な確保が懸念される。また、最先端のＩＣＴ技術の導入の観点からも、分野毎のデータ連携基盤、**分野間データ連携基盤は競争原理が働く民間企業が運営する最新のデータセンターを活用することが望ましい。**

Risks of IoT (Internet of Things) systems;

IoT people loves "own private silo"

1) Not "the I" (Internet),
   but "an i" (internet)
2) Poor security measures…..
   Needs Security-by-Design for Trust
3) Closed open source cloud forums
   Needs Interoperability



Vertical Lock-on
by silo (stove & pipe)

Horizontal Cooperation
e.g., data-centric

さて、、では、IoT Device って？

IoT Devices

- Long time ago : **Analogue Machinery Operation**
- 20th century : **Program(=Digital) Operation**
  - No logging, no memory
  - Software Defined, but Fixed program

- 21st century : **“On-line” Operation**
  - Generate digital data and send it to DC
  - Analyze data and sent it to device to control it
  - Software Defined Infrastructure with on-line updating

IoT Devices

- Long time ago： **Analogue Machinery Operation**
- 20th century : **Program(=Digital) Operation**
  - No logging, no memory
  - Software Defined, but Fixed program
- 21st century : **“On-line” Operation**
  - Generate digital data and send it to DC
  - Analyze data and sent it to device to control it
  - Software Defined Infrastructure with on-line updating

記憶喪失
(洗浄)

無限の
“落書き”
が可能

IoT Device： 今後の前提条件

- 当然ですが、ネットワークにつながる。

賢くなる。
成長する。

消えていく
専用媒体

そうすると。

1. 『知性』 が 背後に 存在。
2. 『機能』 が 変更&注入 可能。

IoT Device： 今後の前提条件

- 当然ですが、[illegible]ろ。

そうす[illegible]

1. 『[illegible]存在』
2. 『機能』が変更&注入可能。

SDI;
Software Defined
(code-based)
Infrastructure

[illegible]えていく
専用媒体