

Security (**not only cyber**) **by** Cloud & **of** Cloud -- from the **cores** to the **edges** --

1. クラウド基盤のセキュリティー
2. 新しい三方良し for Carbon Neutral
3. De-Silo-ing with Zero-Trust in IT&OT
4. IoF(Function)xAIxData が前提
5. CS から P2P への振り子
6. サイバーセキュリティ ガイド

CSA Japan 会長

東京大学 大学院 情報理工学系研究科 教授

江崎 浩 (Hiroshi ESAKI)



Security (not only cyber) by Cloud & of Cloud

-- from the cores to the edges --

1. クラウド基盤セキュリティ

2. 新しい三要素

3. De-Silo

4. IoF (Internet of Functions)

5. CS (Cloud Security)

6. サイバーセキュリティ

✓ 運用の継続性

(e.g., 甚大災害、戦争、
政治、エネルギー)

✓ DFFT (Data Free Flow w/ Trust)

✓ 地球温暖化対策

東京大学 大学院 情報理工学 教授

江崎 浩 (Hiroshi ESAKI)



クラウド化の変遷 around me

- インターネット Ph.1 = UNIX
- インターネット Ph.2 = Webサービス
 1. 最初は P2P : Security by DIY == Zero-Trust
 2. その後に CS(Client-Server) へ : 閉じたサーバークラスター空間
 3. VM(Virtual Machine) が、登場し始める。。。最初は、非力だったあ。。。。
 4. さらに、CDNへ : サーバーを守ってあげる
- インターネット Ph.3 = IoT (Internet of Things)
- インターネット Ph.4 = IoF(Internet of Function)



クラウド化の変遷 around me

- インターネット Ph.1 = UNIX
- インターネット Ph.2 = Webサービス
- インターネット Ph.3 = IoT (Internet of Things)
 - デジタル データが、地球上で自由に飛び回る。
 - サーバークラスタ(=クラウド)がデータを集めまくる
- インターネット Ph.4 = IoF(Internet of Functions)
 - Functions(=Virtual Machine)もThings(=Physical Machine)も、地球
 - ➔ Zero-Trust に 回帰ですかね。



クラウド化の変遷 around me

➤ なんか、、、言い出すようになってきた。。。。

- ◆ SprInternet
- ◆ Sovereign
- ◆ Mal-function, Mal&Faked-Data/News
- ◆ Economical Security
- ◆ De-Coupling, e.g., GDPRP



How live
with
DFFT ?



～ デジタル インフラ ～
as a
デジタル田園都市国家構想



(3) データセンター／海底ケーブル等

11

整備方針

※ 主な改訂内容は赤字

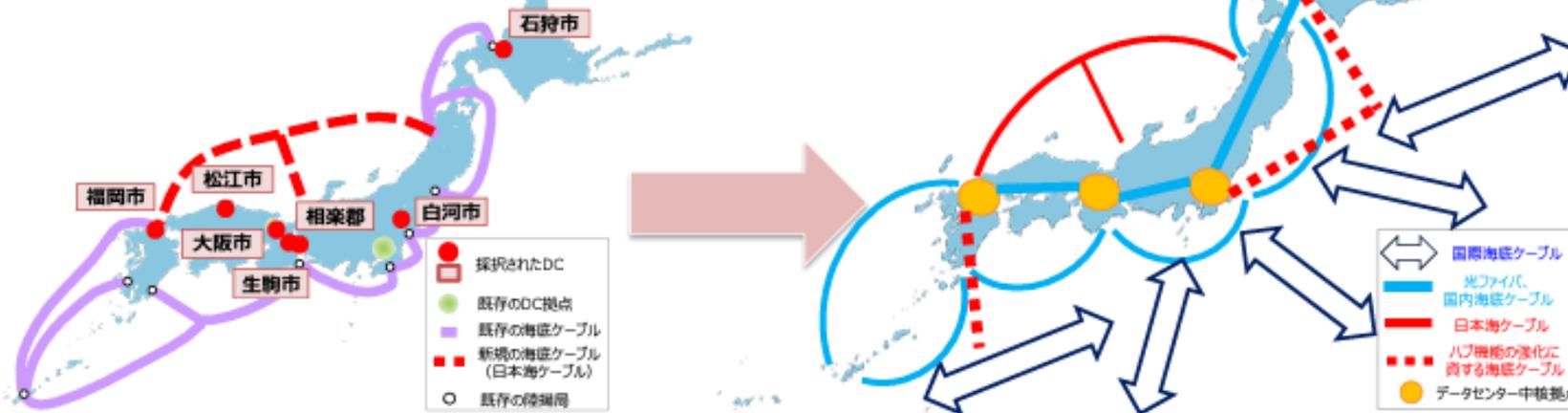
1 データセンター

- 経済産業省と連携し、地域を分散して**10数カ所の地方拠点を5年程度で整備**。地方拠点は、レジリエンス強化、再生可能エネルギー等の効率的活用、通信ネットワーク等の効率化の3点を勘案して整備
- 当面は、北海道や九州のようなエリアにおいて、**東京・大阪を補完・代替する第3・第4の中核拠点の整備**を促進
- 有識者会合※の議論等を踏まえ、**グリーン化**に向けた取組やMEC（モバイルエッジコンピューティング）との連携等を注視しつつ、関係省庁と連携し、**更なる分散立地の在り方や拠点整備等に必要な支援**を検討

※ デジタルインフラ（DC等）整備に関する有識者会合

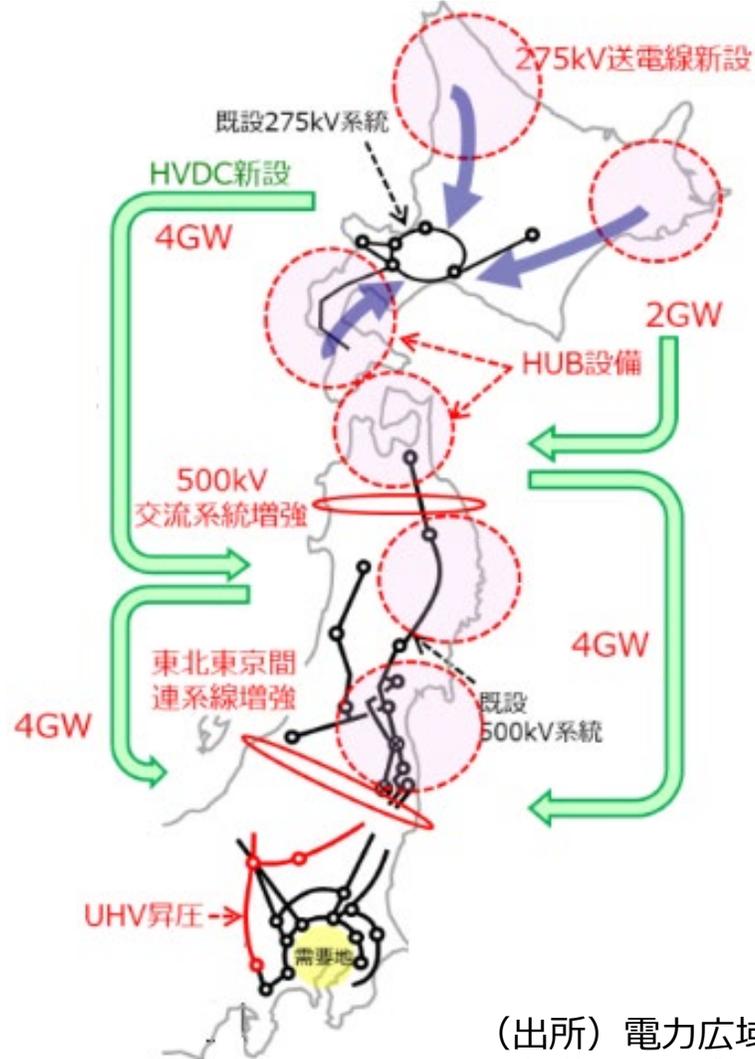
2 海底ケーブル等

- **2026年度中に日本周回ケーブル（デジタル田園都市スーパーハイウェイ）を運用開始、陸揚局を分散立地**
- **国際的なデータ流通のハブとしての機能強化**に向けた取組を促進
- 国際海底ケーブルや陸揚局の**安全対策を強化**

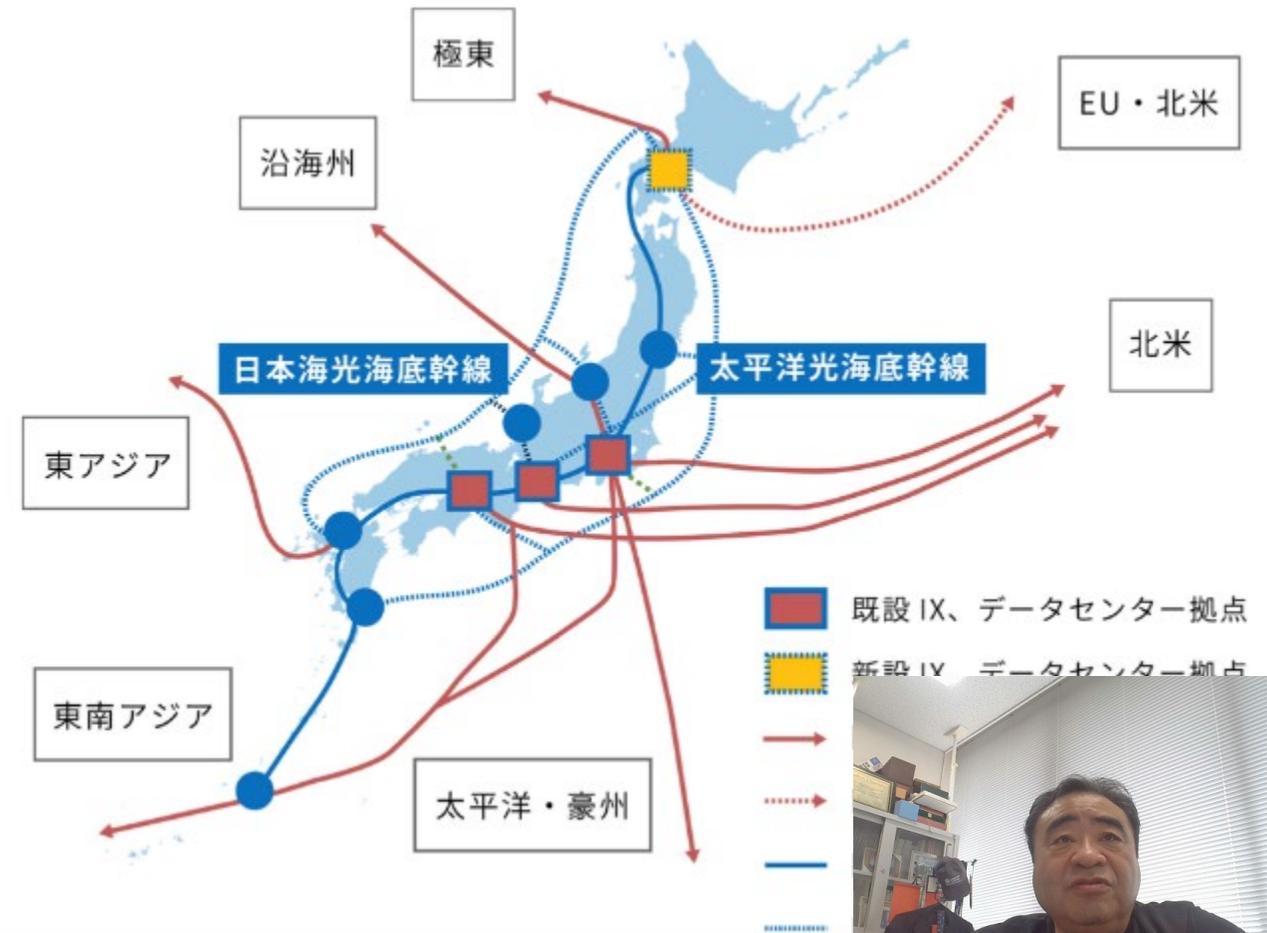


As a デジタル田園都市国家構想(Digital Garden City Initiative)

Electric Power



Information



(出所) 電力広域的運営推進機関：広域系統長期方針（広域連系システムのマスタープラン）（第1期）
北海道ニューピアデータセンター研究会提言書：「北海道をデータセンターのパラダイスに」（2022.4）



【Key Message】

Transfer cost
= **E**nergy **P**roductivity...

Material >> **E**lectricity >> **D**igital bits
(**P**ower) (digital **F**unction)

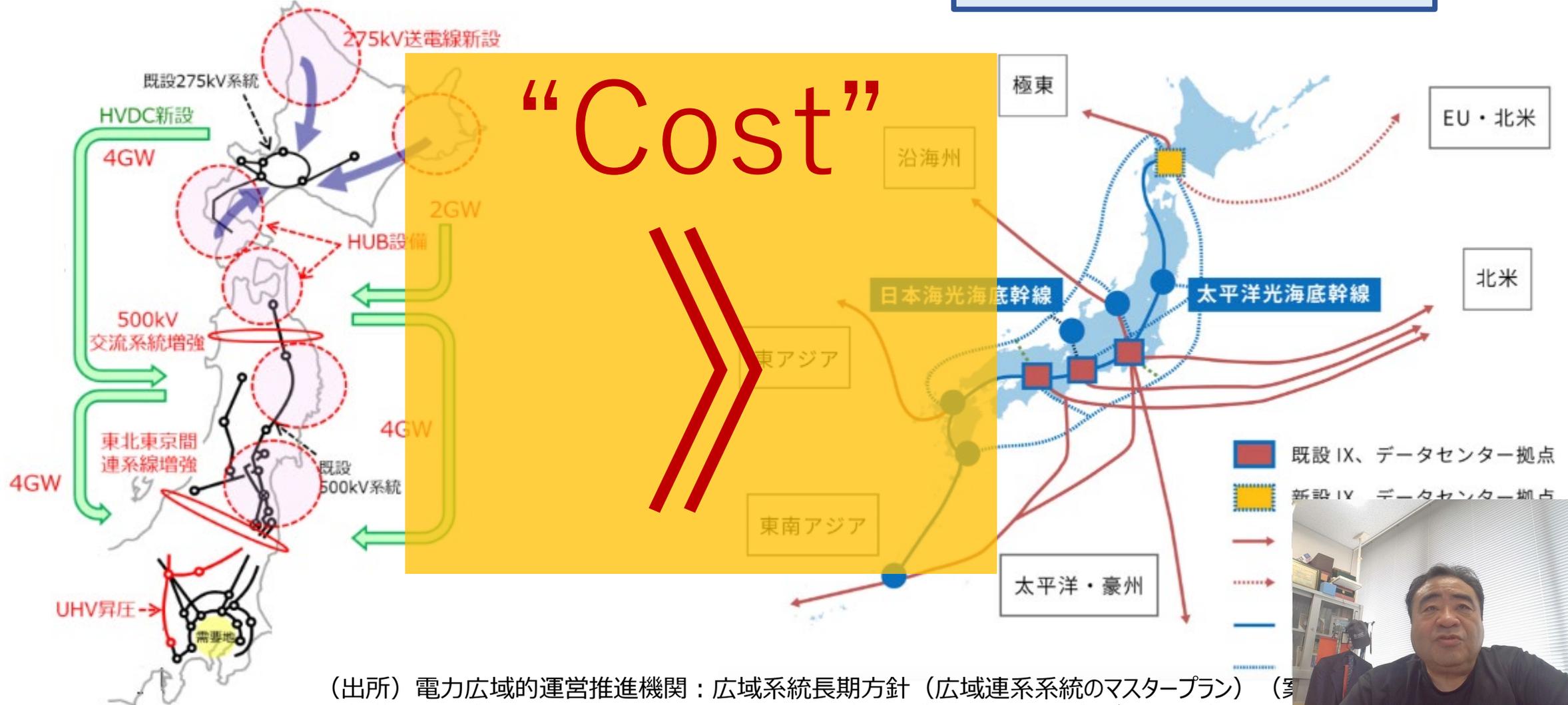
x0000 : **x00** :



As a デジタル田園都市国家構想(Digital Garden City Initiative)

Electric Power

Information

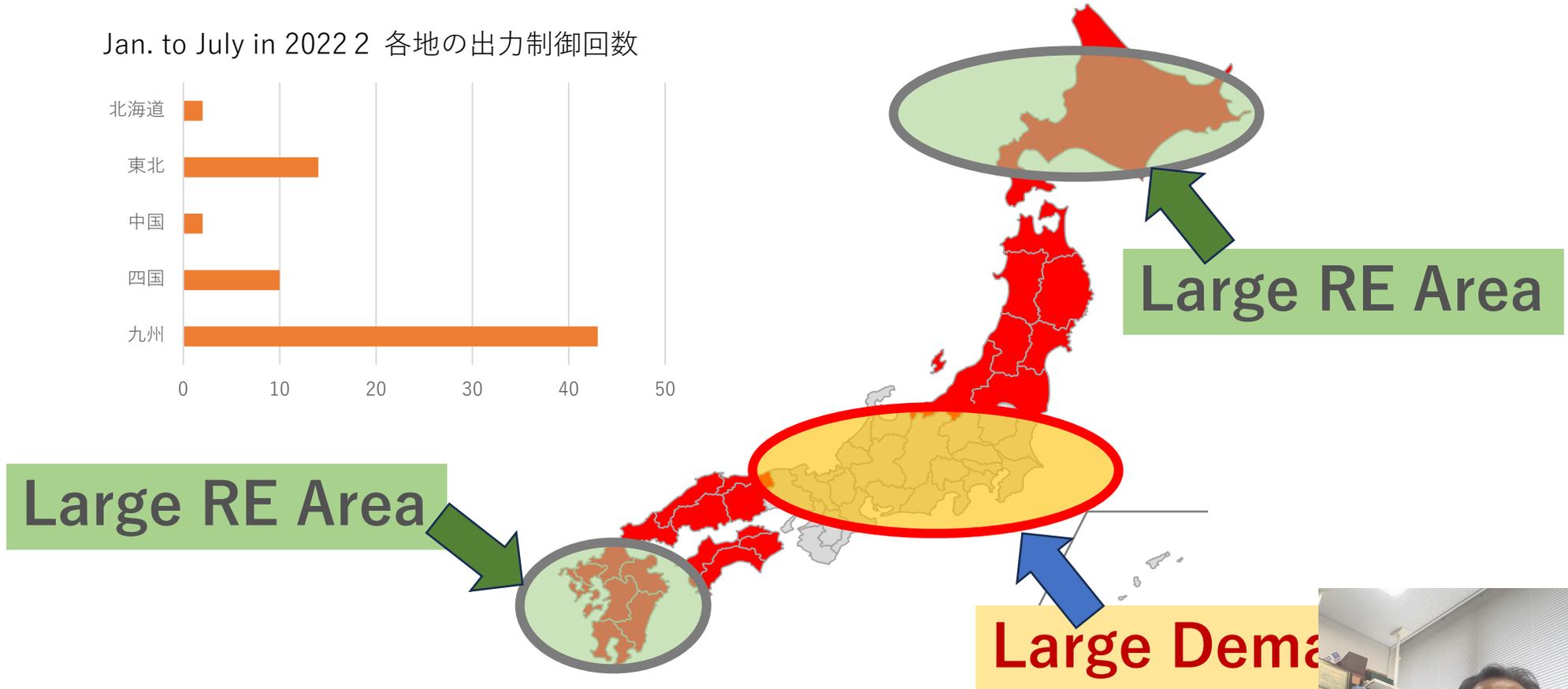
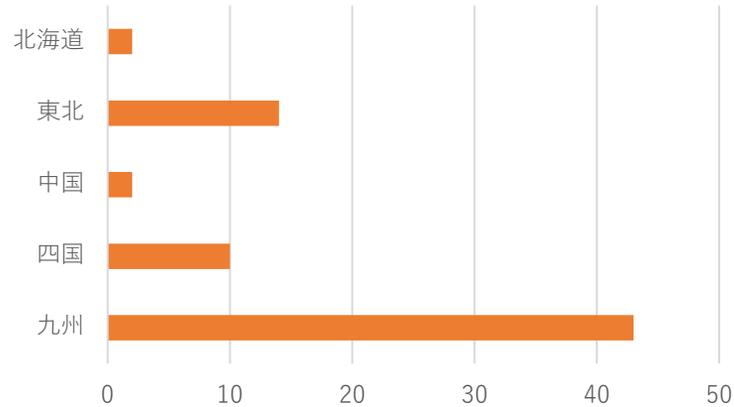


(出所) 電力広域的運営推進機関：広域系統長期方針（広域連系システムのマスタープラン）（第
北海道ニューピアデータセンター研究会提言書：「北海道をデータセンターのパラダイスに」（2022.4

Electrical Power shortage in spring and winter in Japan

- 2022年再エネ出力制御は四国・中国・東北・北海道電力管内に拡大

Jan. to July in 2022 各地の出力制御回数



【資料】 ビットメディア 代表取締役社長 高野 雅晴 氏
第4回イベント (2022年9月28日)
「データセンターの地域エネルギー貢献」



東数 西算(2021 第13期全人代)



100

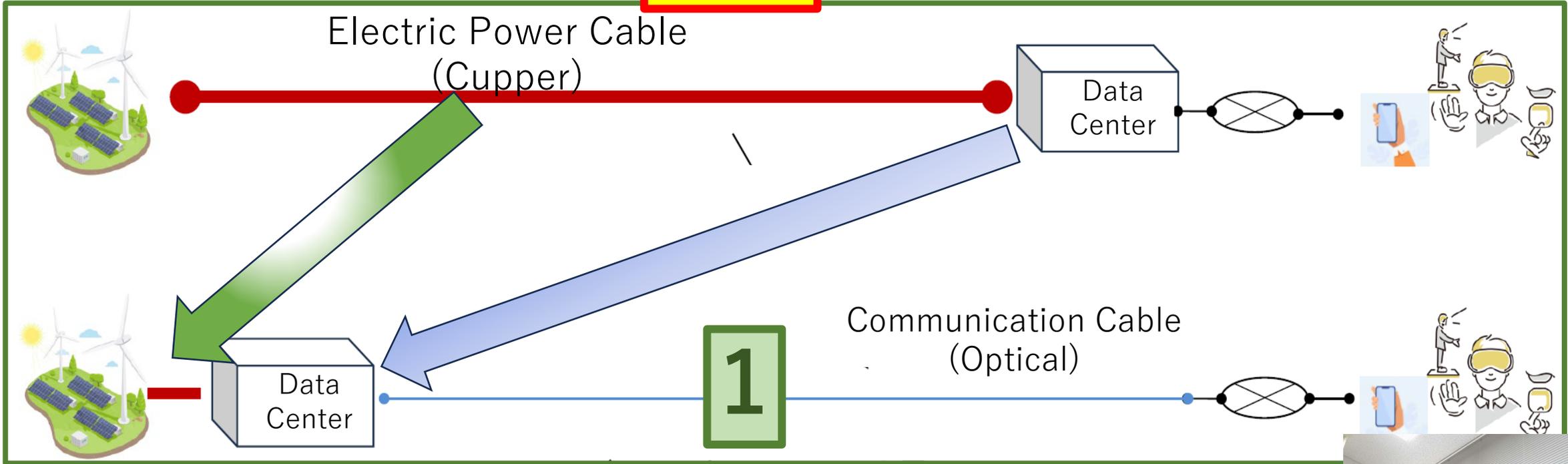
Electric Power Cable
(Copper)

Data Center

Communication Cable
(Optical)

Data Center

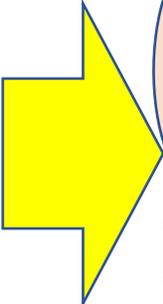
1



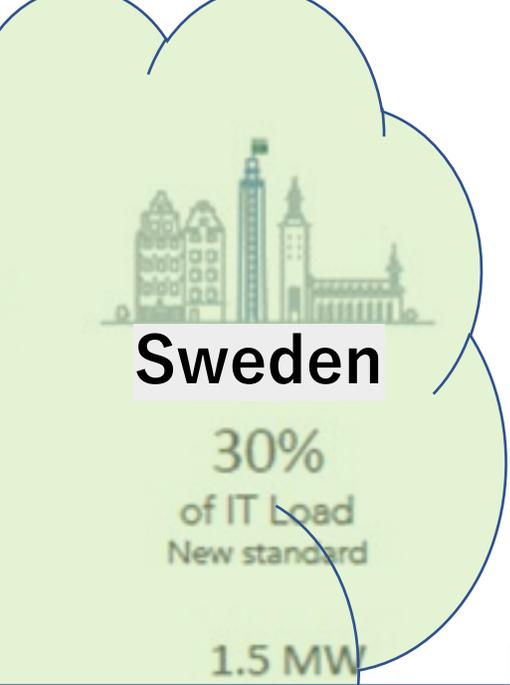
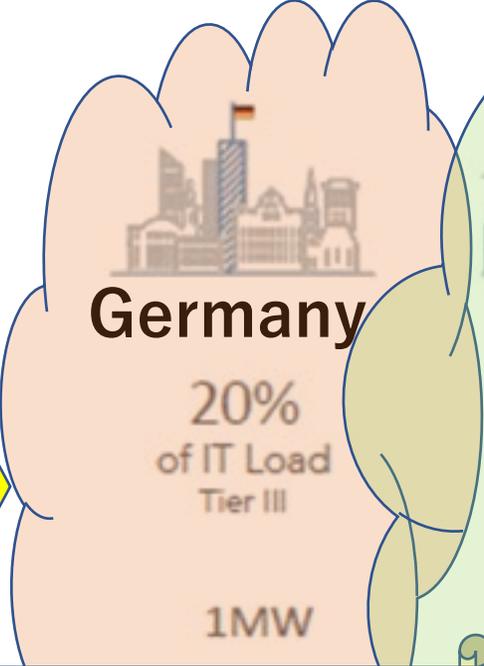
Business case

BMW in Germany

Before



After



**Small latency
&
Critical data
at {dark-side}DC**

**Allowing large latency
&
Non-Critical
at cheap and**



Transfer DCs to energy clean sites (Iceland & Sweden)

✓ 100% Renewal Energy (Hydro & Geothermal)



1. Gentle & contribute to Earth

- ✓ by use of renewal energy (RE-100)
- ✓ by use of cool air (EP-100)

2. Cost👉 & Productivity👈 (EP-x000)

Replacing power cable (copper)

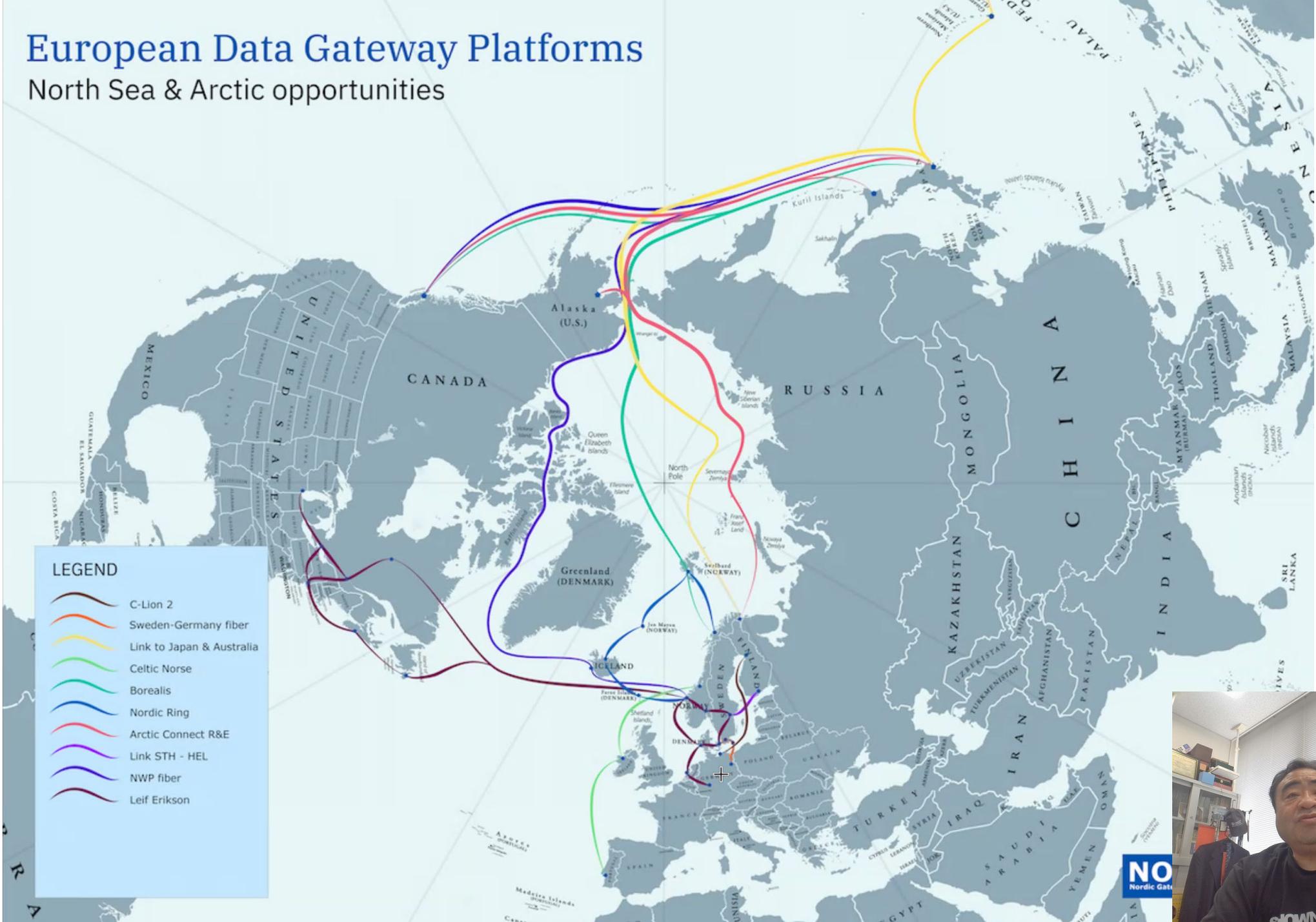
to

tele-communication cable (glass)



European Data Gateway Platforms

North Sea & Arctic opportunities



Security (**not only cyber**) **by** Cloud & **of** Cloud -- from the **c**ores to the **e**edges --

1. クラウド基盤のセキュリティー
2. **新しい三方良し for Carbon Neutral**
3. De-Silo-ing with Zero-Trust in IT&OT
4. IoF(Function)xAIxData が前提
5. CS から P2P への振り子
6. サイバーセキュリティー ガイド



～新しい 三方良し～ 至宝(4方良し)に by cloud

① 脱炭素: {Googleの事例}
Computer-go-to-DC(85%削減),
DC-go-to-REPP(収支)+株価・投資

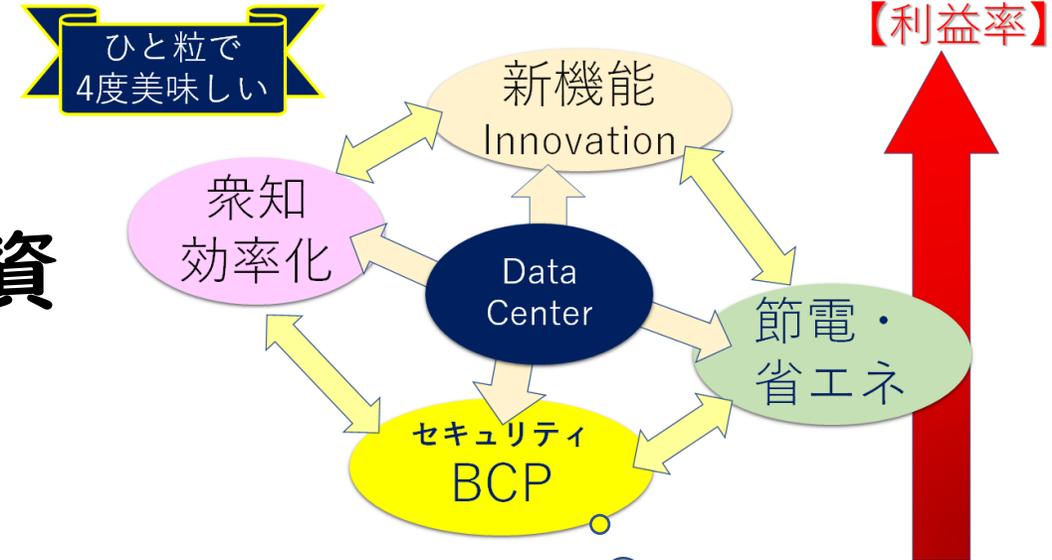
② 価値創造(DX)

③ 組織強靱化

自然災害・サイバー攻撃 対策

(*)Gift: オフィスライフタイム経費、働き方改革

④ {時間と資源の}無駄削減(by DX with DC)
資源とエネルギーを同時に削減可能!



“Cloud-by-Default” for **multiple pay off**

(June 2018 by Japanese gov.)

1. サイロ構造の各省庁のシステムを共有のインフラとして相互接続させ、省庁の壁を越えたデータの自由な利用を実現する。
2. 基盤のサイバーセキュリティ対策は、専門家に任せる。
(*）オンプレ施設担当人事の固定費削減も兼ねる。
3. CAPEXとOPEX, {人件費を含む,} を削減する。
(*）ハード・ソフト・人：所有(BS) から 利用(PL)
4. 自然災害&サイバー攻撃に対するBCPを拡充する。
5. 地球温暖化への貢献として、省エネを実現する。



“Cloud-by-Default” for **multiple pay off**

(June 2018 by Japanese gov.)

1. サイロ構造の各省庁のシステムを共有のインフラとして相互接続させ、**省庁の壁を越えたデータの自由な利用**を実現する。
2. **基盤のサイバーセキュリティ対策は、専門家に任せる。**
(* オンプレ施設担当人事の **固定費削減** も兼ねる。
3. **CAPEXとOPEX**, {人件費を含む,} を削減する。
(* ハード・ソフト・人：所有(BS) から 利用(PL)
4. 自然災害&サイバー攻撃に対するBCPを拡充する。
5. 地球温暖化への貢献として、省エネを実現する。

率 (効率性)
相



Security (**not only cyber**) **by** Cloud & **of** Cloud -- from the **c**ores to the **e**edges --

1. クラウド基盤のセキュリティー
2. 新しい三方良し for Carbon Neutral
3. **De-Silo-ing with Zero-Trust in IT&OT**
4. IoF(Function)xAIxData が前提
5. CS から P2P への振り子
6. サイバーセキュリティー ガイド

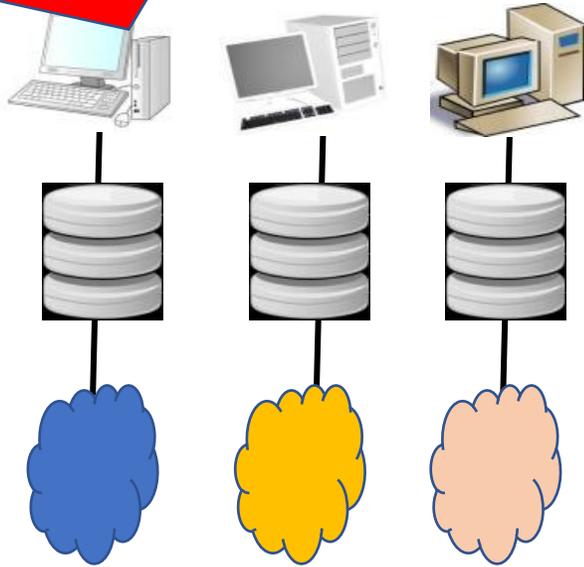


De-Silo-ing with Zero-Trust

攻める(生き残る)ために、
(ITとOT間の)壁は壊される...



ビッグデータ解析・DX
実現の "大" 障壁・障害



垂直統合型モデル
(閉域システム)

これが、「デジタル化」
だった。

1. 独自技術のサイロの中での閉じた
“なんちゃって” のデジタル化
2. システム間の接続は「アナログ」
3. Once Onlyの敵対遺伝子



ビッグデータ解析・DX
実現の "大" 障壁・障害

アンバンドル化
= $\text{IoT} \rightarrow \text{IoF}$

"De-Silo-ing"

"既得権益"

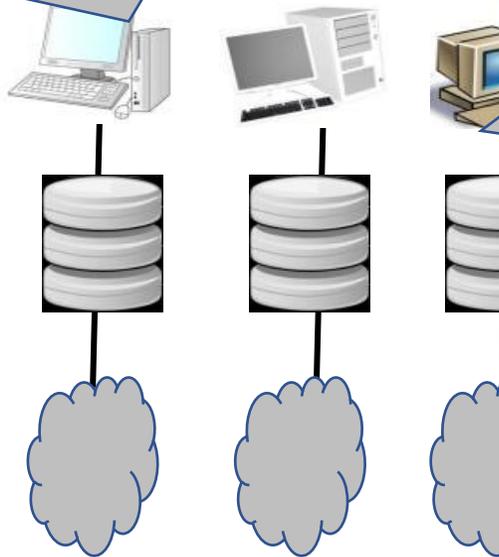
垂直統合型モデル
(閉域システム)

水平統合型モデル
(連携・協調プラットフォーム)



ビッグデータ解析・DX
実現の "大" 障壁・障害

アンバンドル化
= オンライン化



垂直統合型モデル
(閉域システム)

必須となる
サイバーセキュリティ対策
(not only Things, but also Functions)



攻めるための守り



2018年4月 公開

第5期 総合科学技術基本計画
～ Society 5.0 ～
データ連携 SWG



Society5.0 で重きを置くべき課題

「また、製品やサービスを提供する際には、任務保証の考え方に基づき取り組むことが重要であり、また、**セキュリティ品質の実現が欠かせない**。セキュリティ品質を確保するための費用はコストでなく価値を生み出すための投資である。その実現には、企画・設計段階からセキュリティ確保を盛り込む**セキュリティ・バイ・デザインの考え方**を持ち、開発時や運用時においては個々のIoTシステムの階層構造を踏まえたデータとIoTシステム全体のセキュリティ確保を図ること、異なる分野を連携協調させる際にはIoTシステム間の相互連携を図り、IoTシステム全体としてのセキュリティを確保すること、の2点が重要である。さらに、日々進化し高度化するサイバー攻撃に対応するためには、セキュリティ確保のための人材育成も必要な取組である。セキュリティ技術の高度化及び社会実装の推進については、**重要インフラ等から優先的に対応する**。具体的には、サイバーセキュリティ技術の研究開発を推進するとともに、**業界内・業界間でのサイバー攻撃等の情報共有を共通化・自動化を実現する仕組みを構築**し、さらに業種間を跨ぐ情報共有の環境整備に取り組む。これにより、イベント単位で短期間の設置**セキュリティオペレーションセンター（Security Operation Center 以下「SOC」という。）**の整備促進や業界間のSOC整備の促進にもつ



アーキテクチャの前提条件 (by default)*

1. オンライン性 (デジタル前提の次の段階)
2. 相互接続性・相互運用性
3. グローバル性
①技術仕様、②接続性
4. 構造化データ
5. ユニークID (グローバルIDとのマッピング)
6. ハードウェアとソフトウェアのアンバンドル
(例) マイナンバー: ①番号、②機能、③カード のアンバンドル化
7. **ゼロ・トラスト**
① 多層防御は支援でしかない、②ハード(&人)もソフトも移動可能にする。
8. エンドユーザによる利用経験・体験
9. オープン・ソース
10. {激甚}災害対応性(オンプレとクラウドの連携、分散クラウド)

* 前提条件を満足しない場合には、合理的な理由の



Security (**not only cyber**) **by** Cloud & **of** Cloud -- from the **cores** to the **edges** --

1. クラウド基盤のセキュリティー
2. 新しい三方良し for Carbon Neutral
3. De-Silo-ing with Zero-Trust in IT&OT
4. **IoF(Function)xAIxData が前提**
5. CS から P2P への振り子
6. サイバーセキュリティー ガイド



Cloud = OT + IT

攻める(生き残る)ために、
人工知能(AI)xデータが前提に!!



Cloud for Cloud

AI for Cloud



データの質&内容に依存



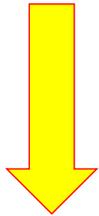
Security (not only cyber) by Cloud & of Cloud -- from the cores to the edges --

1. クラウド基盤のセキュリティー
2. 新しい三方良し for Carbon Neutral
3. De-Silo-ing with Zero-Trust in IT&OT
4. IoF(Function)xAIxData が前提
5. CS から P2P への振り子
6. サイバーセキュリティー ガイド

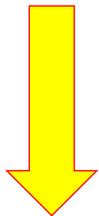


コンピュータネットワーク **第3の波**

分散



集中



分散

■ 第1の波: ウェブ

■ 第2の波: クラウド



■ 第3の波: IoT → Edge Cloud





New Requirements

- ✓ Latency {by M2M}
- ✓ Privacy & Security
- ✓ Resiliency {against disconnect}

ロボットの協調

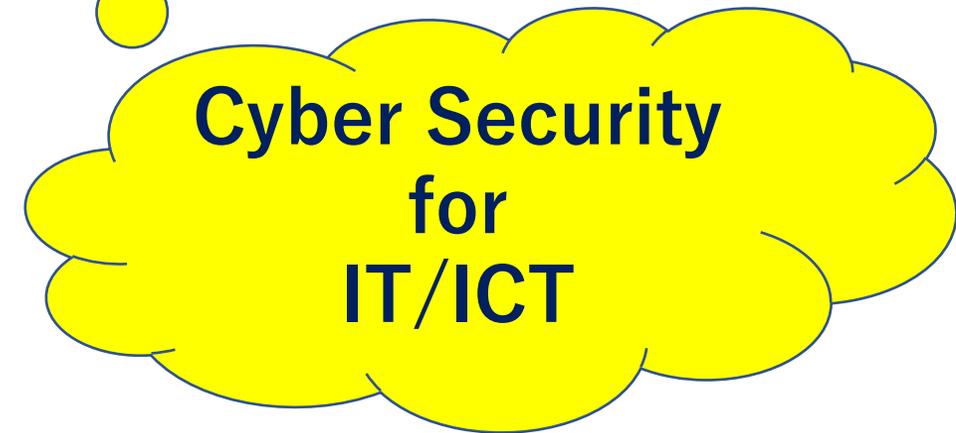
制御系・アクチュエータの協調



Security (**not only cyber**) **by** Cloud & **of** Cloud -- from the **c**ores to the **e**edges --

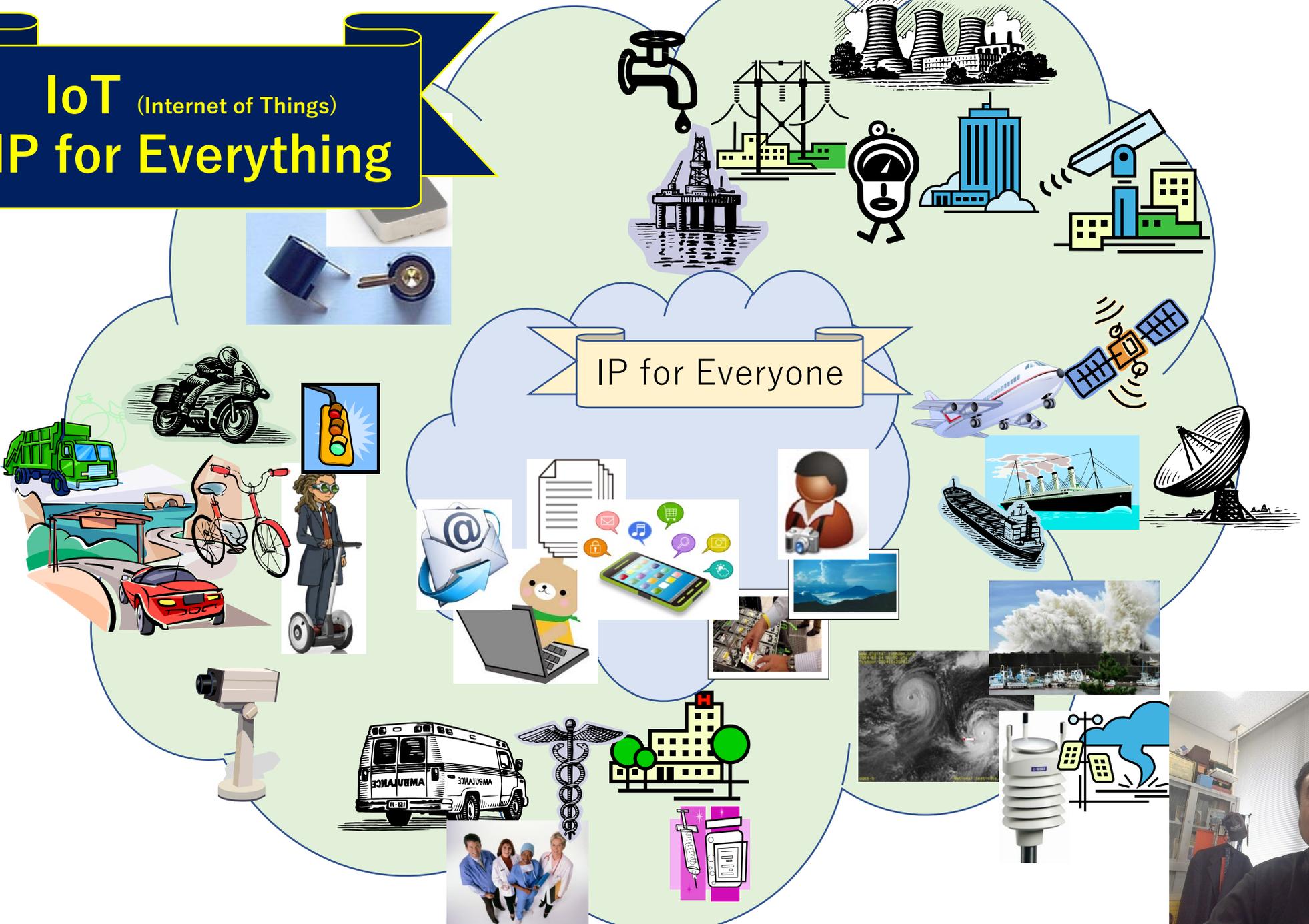
1. クラウド基盤のセキュリティー
2. 新しい三方良し for Carbon Neutral
3. De-Silo-ing with Zero-Trust in IT&OT
4. IoF(Function)xAIxData が前提
5. CS から P2P への振り子
6. **サイバーセキュリティー ガイド**





IoT (Internet of Things) IP for Everything

IP for Everyone



IoT (Internet of Things) IP for Everything

Cyber Security
for
OT systems

さらに、
Internet of
Functions ^

IP for Everyone

そうすると、
Zero-Trust



～ 経済産業省 ～ 産業サイバーセキュリティ研究会

▶ ワーキンググループ1 (制度・技術・標準化)

▶ ワーキンググループ1 (分野横断サブワーキンググループ)

▶ 『第2層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

▶ サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース

▶ ワーキンググループ1 (ビルサブワーキンググループ)

▶ ワーキンググループ1 (宇宙産業サブワーキンググループ)

▶ ワーキンググループ2 (経営・人材・国際)

▶ ワーキンググループ3 (サイバーセキュリティビジネス化)

ビル、電力、
宇宙産業、工場

▶ ワーキンググループ1 (電力サブワーキンググループ)

▶ ワーキンググループ1 (工場サブワーキンググループ)





～ 経済産業省 ～ 産業サイバーセキュリティ研究会

▶ ワーキンググループ1 (制度・技術・標準化)

データセンターのガイドブックをもとに作成。インシデント対応を追加(2020年)

▶ サイバーセキュリティ・セキュリティ確保に向けたソフトウェア開発手法等検討タスクフォース

▶ ワーキンググループ1 (ビルサブワーキンググループ)

▶ ワーキンググループ1 (宇宙産業サブワーキンググループ)

▶ ワーキンググループ2 (経営・人材・国際)

▶ ワーキンググループ3 (サイバーセキュリティビジネス化)

ビル、電力、
宇宙産業

発電・送電・配電のすべて、
さらに需要家へ。

▶ ワーキンググループ1 (電力サブワーキンググループ)

▶ ワーキンググループ1 (工場サブワーキンググループ)

組み立て工場を見本に。今後
界、半導体業界、プラント
の予定



工場セキュリティガイドライン 概要編

Cyber Security Guideline in Factory

<https://www.edgexcross.org/ja/data-download/pdf/ECD-TE4-0009-01-JA.pdf>



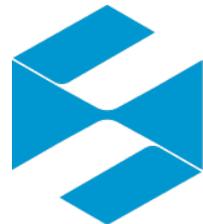
EDGE CROSS
CONSORTIUM

Est. in 2017



Green
university of **Tokyo**
Project

Est. in 2008



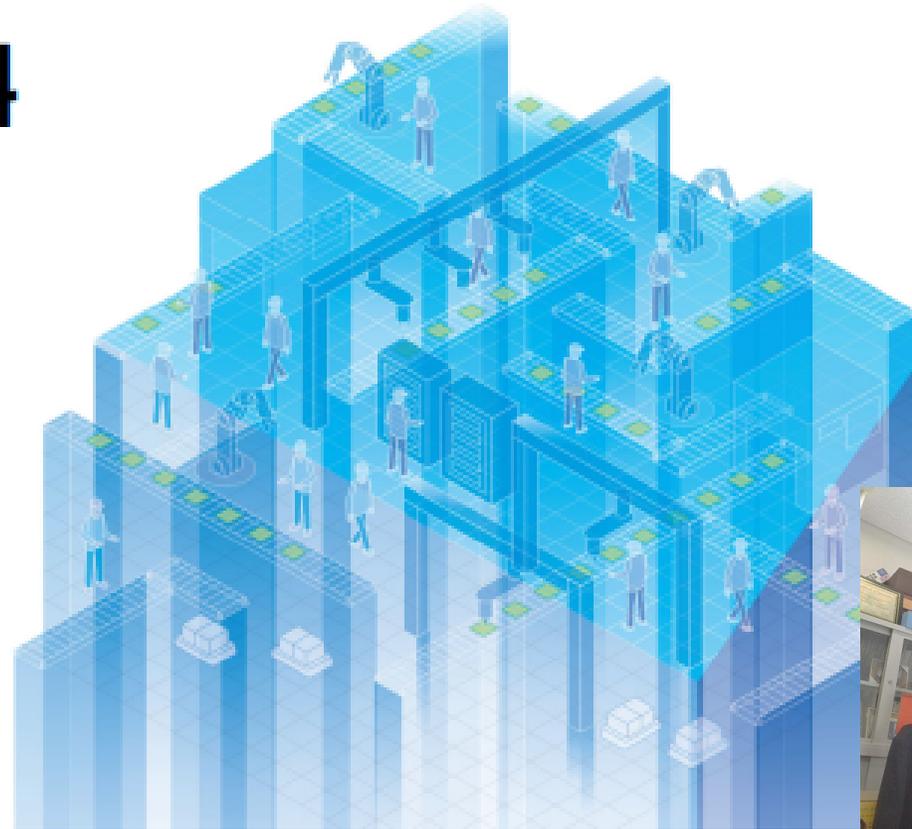
経済産業省

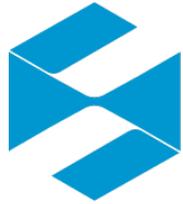
Ministry of Economy, Trade and Industry



「工場システムにおける サイバー・フィジカル・セキュリティ対策 ガイドライン」概要資料

経済産業省
サイバーセキュリティ課
産業機械課





経済産業省

Ministry of Economy, Trade and Industry

- 工場システムにおける
サイバー・フィジカル・セキュリティ対策ガイドライン
 - https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html
- [工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインVer1.0](#)
- [「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」概要資料](#)
- [「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」付録E チェックリスト](#)

- [産業サイバーセキュリティ研究会WG1（制度・技術・標準化）](#)
- [工場サブワーキンググループ](#)



サイバー対策 企業格付け

5段階で、25年度いも

取引先の対応力を可視化

経産省

経産省は企業のサイバー攻撃対策を格付けする制度を2025年度にも始める。各社の対策を5段階で評価し、取引先がどこまで対策をとれているかが分かるようにする。サプライチェーン(供給網)の弱点を狙う攻撃が増える中、産業全体で対応力を高める。

経産省が近くサイバーセキュリティの研究会で案を示す。サイバー対策の度合いを5段階で格付けする。自動車や工場など分野ごとのガイドラインや海外事例をもとに各段階の基準を定める。今後、詳細を検討する。

レベル1〜2は企業に最低限求める対策を指す。①ソフトウェアの定期更新②機密事項へのアクセス制限③情報漏洩時の対応手順などが基準となる見込みだ。レベル3〜4は供給網の一端を担う企業向けで強固な情報管理の体制を整えることを想定する。

サイバー対策の格付けの概要			
レベル	対象企業	想定される要件	認定方法
1~2	最低限の対策が必要な中小など	・ソフトウェアの定期更新 ・機密事項へのアクセス制限	自己宣言
3~4	取引先と供給網を構築する企業	責任者の配置など情報管理の強化	自己宣言/ 第三者認証
5	電気・鉄道など重要インフラ関連	・攻撃情報の迅速な官民共有 ・早期復旧の手順を事前に策定	第三者認証

経産省は格付けを通じ、企業に自社の取り組みの強化を促すだけでなく、取引先がどれだけサイバー対策の対応力があるかが把握しやすくなる。格付けが低い企業は取引を避けられる可能性があるため、結果的に産業全体で対応力が高まる効果が見込まれる。

KPMGコンサルティングの澤田智輝パートナーは「発注元にとっては情報の機密度に応じて、どのようなサービス・企業を選べばよいかの判断基準となる。受注側からみても(民間の)セキュリティ評価や監査を何度か受ける必要がなくなり、効率化につながる」と分析する。

政府調達でもレベル4以上など一定の基準を満たす企業を対象にする方針だ。補助金の支給要件にすることも検討する。経産省は24年度から産業用ロボットなどIoT機器でサイバー対策の認証

制度を始めると、この計画も参考に企業版の新制度を作る。総務省の情報通信白書によると、サイバー攻撃関連の通信数は22年までの5年で3・4倍に増えた。供給網の混乱を狙った攻撃も多い。

日米、核融合

首脳会談、共同声明で調

日米両政府は核融合発電の実用化に向けた連携体制を強化する。10日の

日米首脳会談に合わせ、両国間の協力について盛り込んだ共同声明を出す



Security (**not only cyber**) **by** Cloud & **of** Cloud -- from the **cores** to the **edges** --

1. クラウド基盤のセキュリティー
2. 新しい三方良し for Carbon Neutral
3. De-Silo-ing with Zero-Trust in IT&OT
4. IoF(Function)xAIxData が前提
5. CS から P2P への振り子
6. サイバーセキュリティ ガイド

