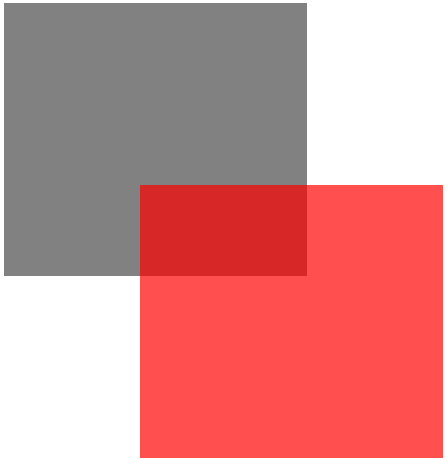
JDCC
日本データセンター協会
Japan Data Center Council

建物設備システムリファレンスガイドとファシリティインフラWGの紹介



2017年 2月 21日

JDCC　ファシリティインフラWG事務局
㈱竹中工務店
粕谷　貴司

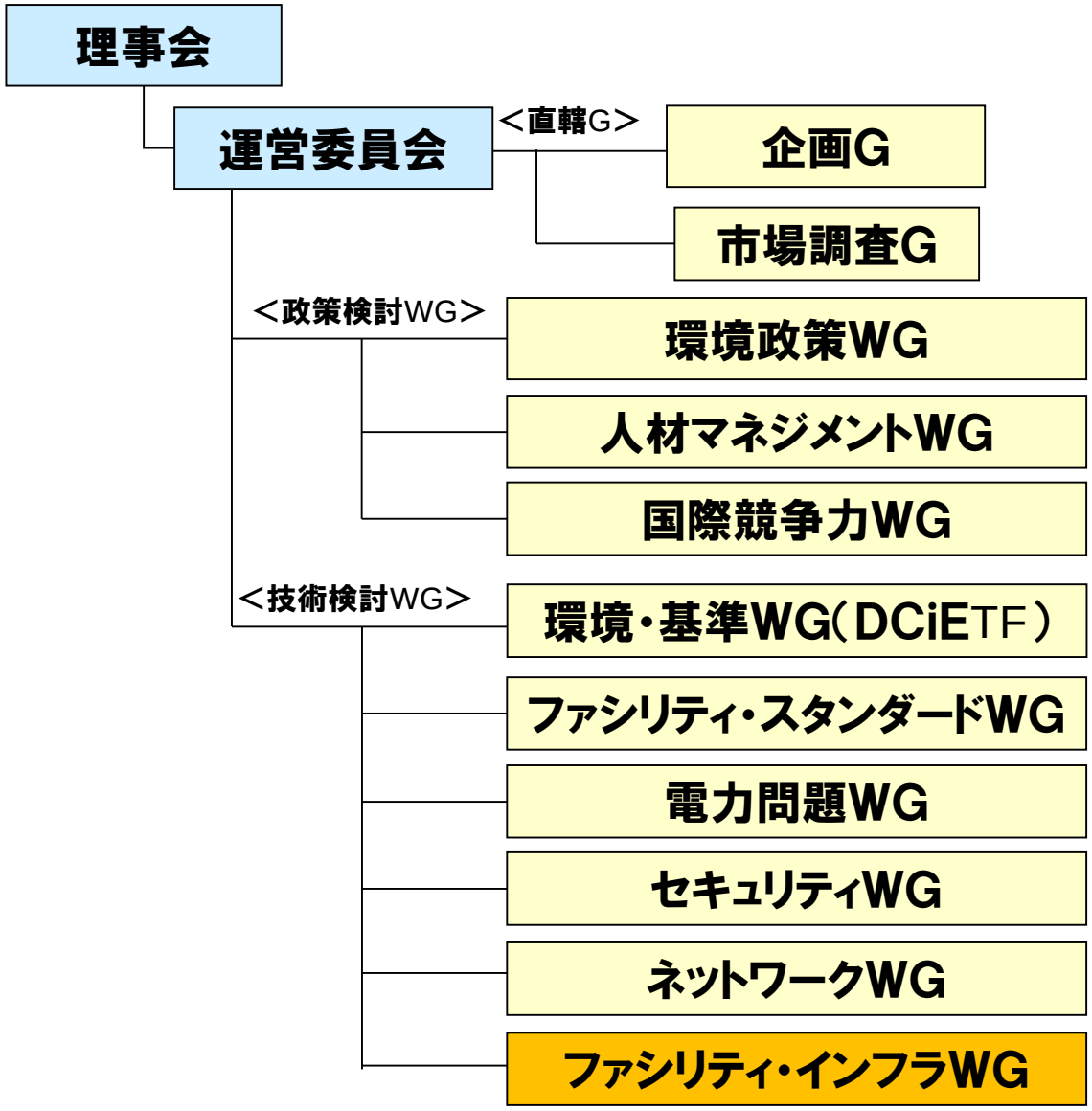
アジェンダ

①ファシリティ・インフラWGについて

②建物設備システム(BAシステム)について

③建物設備システムリファレンスガイド

JDCC組織体制



- 活動企画・プロモーション
- 他団体とのアライアンス推進
- DC業界統計・ユーザ調査
- 東京都環境確保条例への提言
- DC事業の課題と必要な人材像策定
- 国内DC競合力向上施策検討・提言
- DC省エネ測定方法の標準化策定
- 国内DC施設基準の策定
- 電力問題への対応
- DCセキュリティ動向調査
- クラウドDCネットワーク推奨モデル策定
- 建物設備の情報インフラの推奨モデル策定

GUTP組織体制

東大グリーンICTプロジェクト
プロジェクトリーダ：東大／江崎教授
サブリーダ：首都大／山本教授

ステアリング委員会（主査：中村（三菱総合研究所））

東京大学、首都大学東京、都環境科学研研究所、電気設備学会、
大塚商会、シムックス、新菱冷熱工業、ダイキン工業、
ディー・エス・アイ、パナソニック、三菱総合研究所、ユビテック、

オリンピック 特別チーム
主査；中村（三菱総合研究所）
副査；江崎（東京大学）
山本（首都大学東京）
藤原（都環境科学研究所）

WG体制

制御実証実験WG
主査：藤村（アズビル）
副査：豊田（ディー・エス・アイ）

DCEM WG
主査：江崎（東京大学）
副査：松本（NTTデータ先端技術）
浅井（東京大学）

認証WG（2014年度）
主査：伊藤（ユビテック）
副査：天辰（コムツァイト）

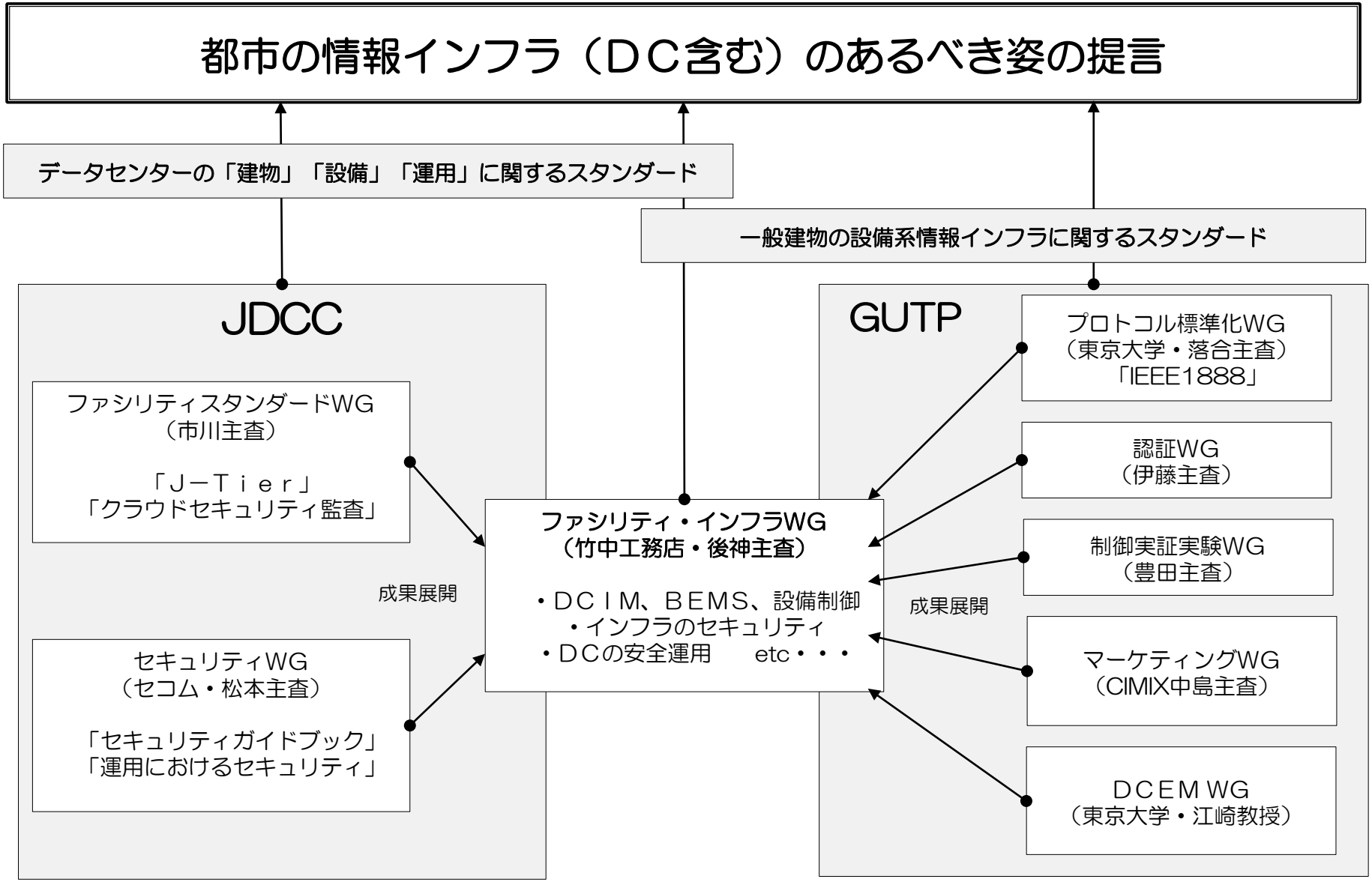
プロトコル標準化WG
主査：落合（東京大学）
副査：百瀬（シスコ・システムズ）
石山（東芝）

ビジネスWG（2014年度）
主査：江崎（東京大学）
- コミュニケーションSWG
- 国際連携SWG ・・・

設計標準化WG
主査：藤原（都環境科学研究所）
副査：豊田（電気設備学会）
加井（ダイキン工業）

ファシリティ・インフラWG（2014年度）
主査：後神（竹中工務店）
副査：松本（セコム）

FI－WGの位置づけ、活動目的



ファシリティ・インフラWGの活動内容

① BAシステムに対する脅威を正しく共有する

② 脅威に対する対策を共有する

③ 国内外の基準・標準の紹介

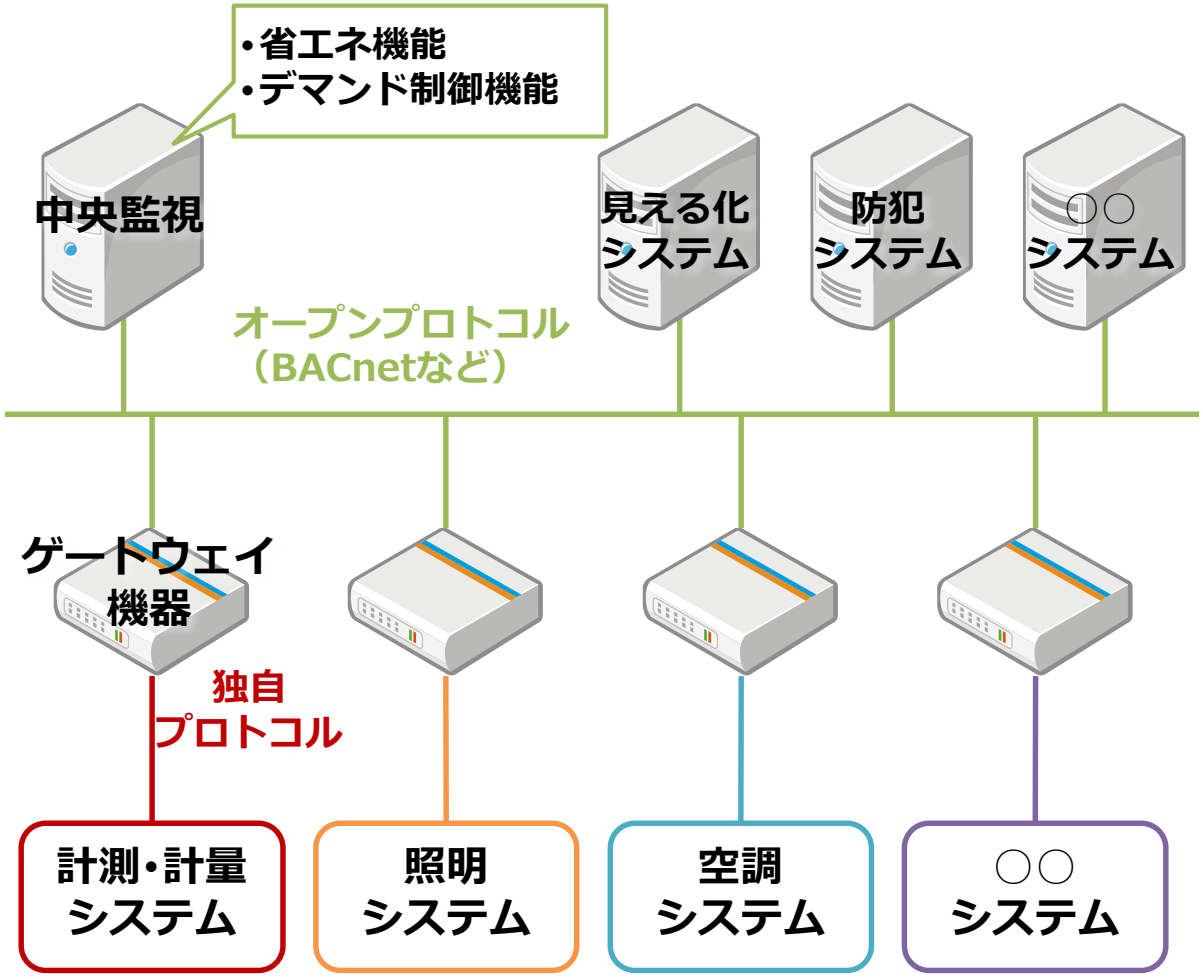
④ BAシステムの設計・構築のためのガイドライン作成

建物設備システム（BAシステム）について

※ BA：Building Automation

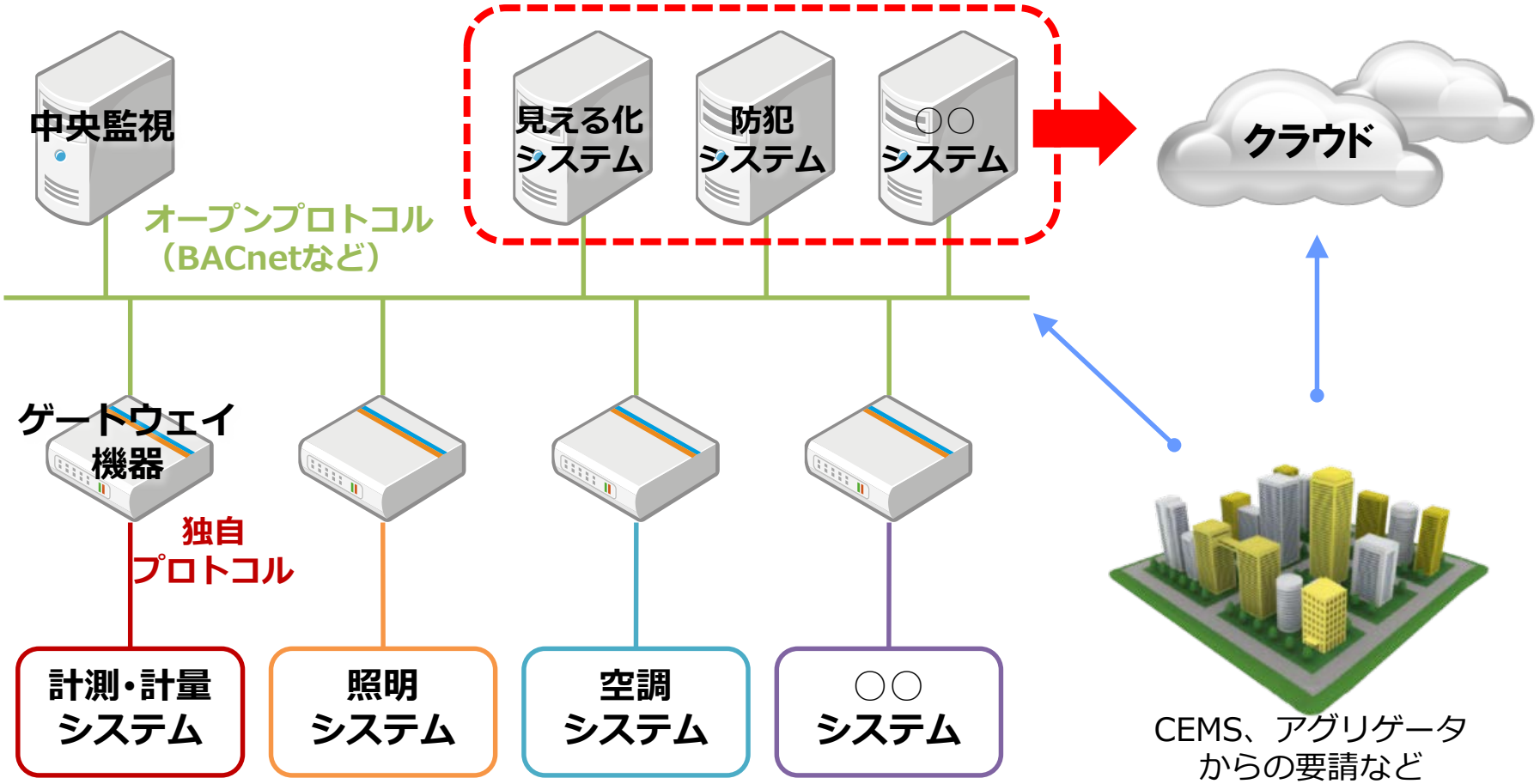
BAシステムの高度化、クラウド化

従来的なビル設備は、クローズなシステム構成が一般的



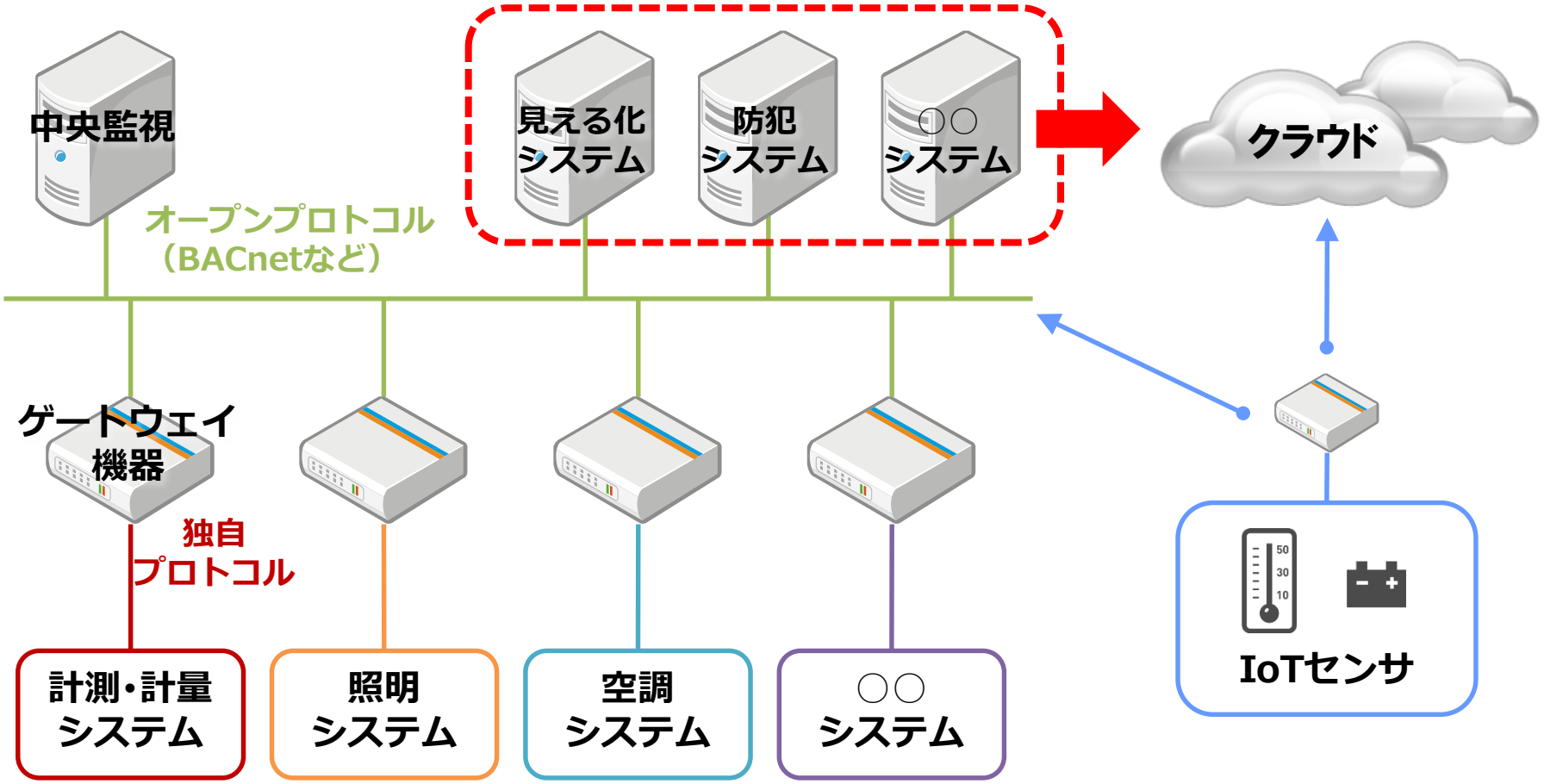
BAシステムの高度化、クラウド化

**クラウドとネットワーク回線の低廉化、高信頼性から、
一部のシステムはクラウドに移行する時代に**



IoTの進展

- Internet of Things
  - 様々なデバイスがネットワークに接続してくる



BAシステムへの脅威が顕在化

ネットワークを通じた脅威は年々拡大の傾向にある

事例	概要	備考
顧客情報流出	内部犯による情報漏えいや、外部からの攻撃等による情報の流出	
クラウドの 個人写真暴露	個人写真用クラウドストレージへの攻撃。 写真から位置情報等も流出。	
軍事兵器開発施設の 機能停止	OS等の脆弱性を利用したウィルスによって、制御システムを攻撃、制御を乗っ取り、核燃料施設の遠心分離器を破壊した。	イラン、Stuxnetの事例
POSレジのカード データ盗難	インターネットから、POS端末をマルウェア感染させ、買い物客のクレジットカード情報などが大量に流出した。	米Targetの事例
BACnetシステム 検索行為の検知	BACnetを使った通信端末を検索し、攻撃をかけることで情報流出や、制御の乗っ取りを行う。	警察庁から注意喚起の発表があった。

BAシステムへの脅威が顕在化

建物側でのセキュリティ対策が必要に！

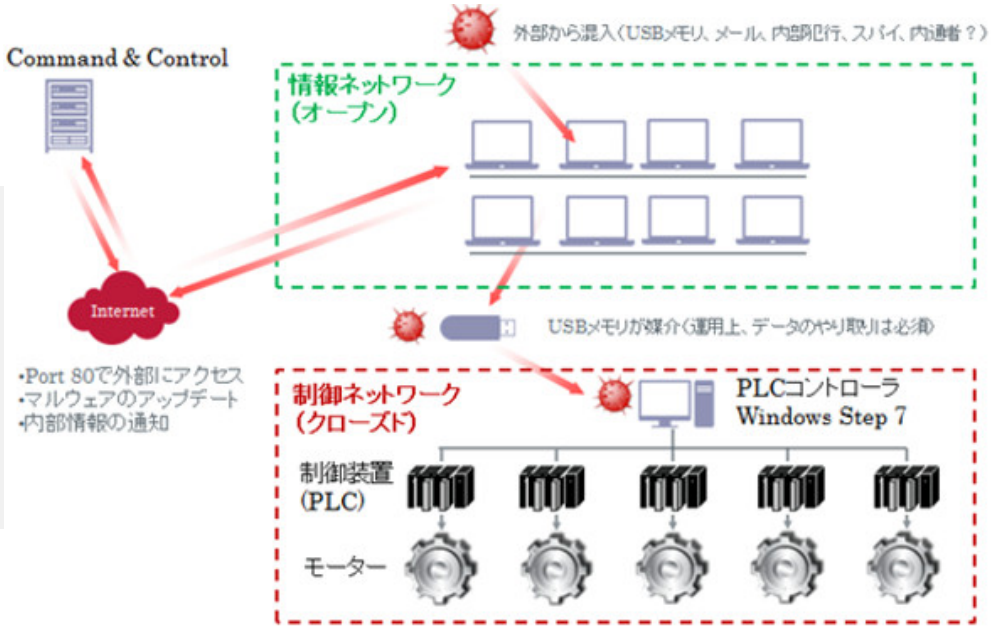
事例	概要	備考
顧客情報流出	内部犯による情報漏えいや、外部からの攻撃等による情報の流出	
クラウドの個人写真暴露	個人写真用クラウドストレージへの攻撃。写真から位置情報等も流出。	
軍事兵器開発施設の機能停止	OS等の脆弱性を利用したウィルスによって、制御システムを攻撃、制御を乗っ取り、核燃料施設の遠心分離器を破壊した。	イラン、Stuxnetの事例
POSレジのカードデータ盗難	インターネットから、POS端末をマルウェア感染させ、買い物客のクレジットカード情報などが大量に流出した。	米Targetの事例
BACnetシステム検索行為の検知	BACnetを使った通信端末を検索し、攻撃をかけることで情報流出や、制御の乗っ取りを行う。	警察庁から注意喚起の発表があった。

Stuxnet（制御システムを狙った初のマルウェア）

- Windowsの脆弱性を利用したコンピュータウィルスで、インターネットやUSBメモリを経由して、感染する。
- イランの核燃料施設へ米とイスラエルの両国政府が協力してサーバー攻撃。同施設の遠心分離器を物理的に破壊した。（クローズドシステムだが、USBメモリ経由で汚染）

POINT

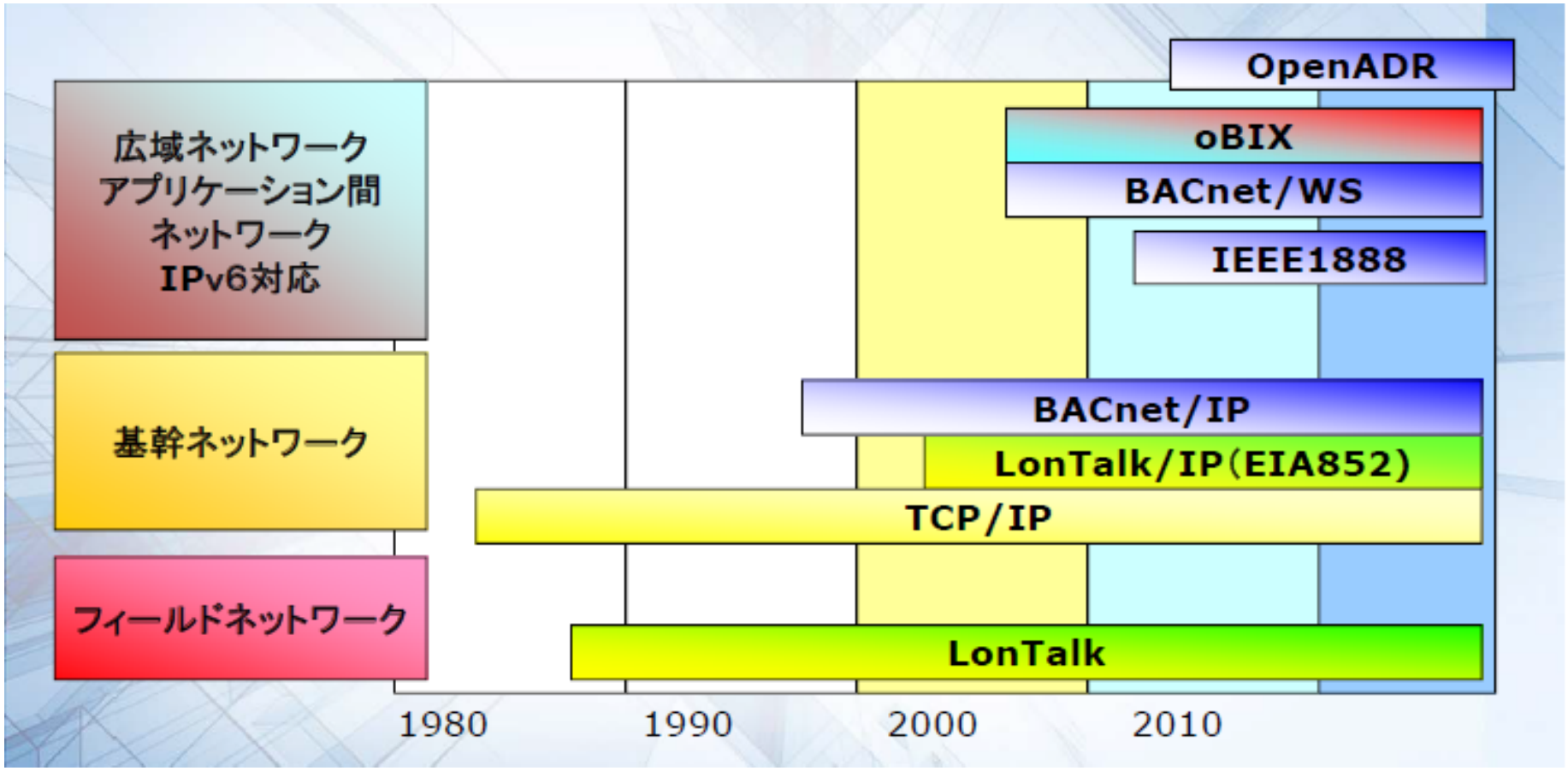
- 制御システムもサイバー攻撃の対象になっている。
- システムだけでなく、ハードウェアの破壊も伴う場合がある。



http://monoist.atmarkit.co.jp/mn/articles/1312/26/news002.html

【参考】建物設備システムのプロトコル

- 外部連携のためのWebService系のプロトコルの規定も進んでいる
- 欧州ではKNXが一般的になってきている
- IoT、サイバーセキュリティへの対応のためのプロトコルのアップデートが議論されている



出展：LONMARK JAPAN資料

建物システムハッキング事例

- KNX/IPで構成されたホテルシステムへ不正アクセスし、実際に操作された

http://scan.netsecurity.ne.jp/article/2014/09/10/34815.html

特集／特集

2014年9月10日（水）10時15分

[DEF CON22 レポート] 中国の五つ星ホテルが「暇つぶしハッキング」の犠牲に

「モノのインターネット」の安全性が不安視される中、DEF CON 22 のブリーフィングで、一人のセキュリティコンサルタントが 200 以上の客室を持つ五つ星ホテルのセキュリティを「退屈しのぎに」破った際の様子が、本人の口から語られた。

Trusted Computing Group の元代表でもあるセキュリティコンサルタントの Jesus Molina Milina Terriza が、中国で滞在した高級ホテル「St Regis Shenzhen」では、それぞれの客室内に備え付けられた iPad が室内の照明やテレビ、ブラインドの開閉、温度管理などを制御していた。

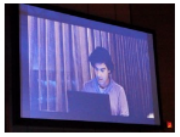
退屈した Molina が、その iPad を調べてみたところ、それはゲスト専用のネットワークに接続されており、オートメーションのコマンドは「KNX/IP」プロトコルを利用していた。「KNX/IP」は 1990 年に開発されたネットワーク通信プロトコルで、欧州と中国で広く利用されている。そのウェブページの説明によると、「世界で唯一の商用・居住用のビルコントロールのオープンスタンダード」であるという。

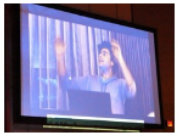

DEF CON22 で講演する Molina 氏

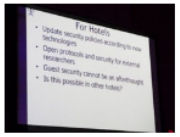

ホテルに備え付けられていた iPad


iPad とゲストネットワーク


ゲストネットワークと KNX ネットワーク


さっそくテストを行う Molina 氏


テスト成功の瞬間

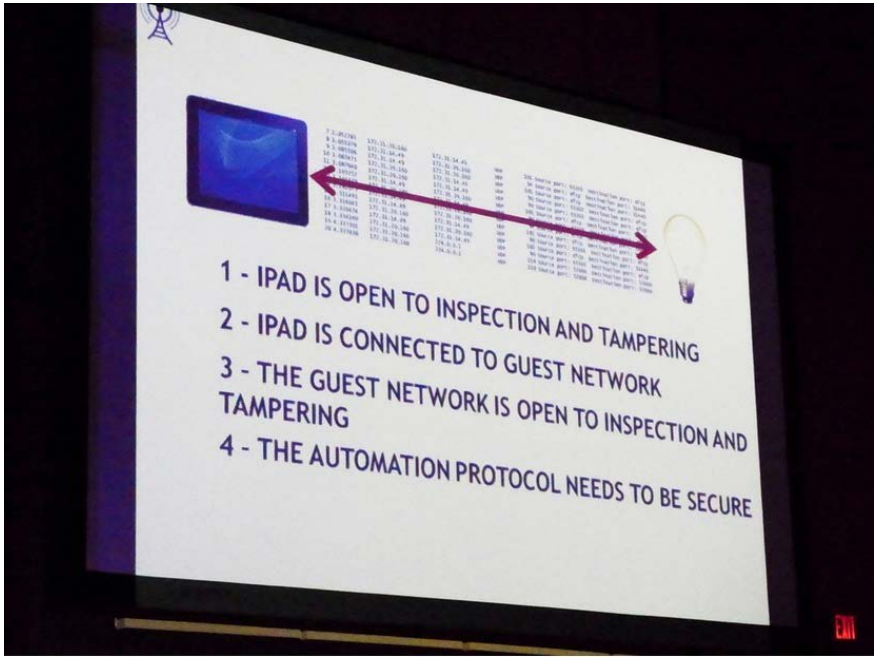


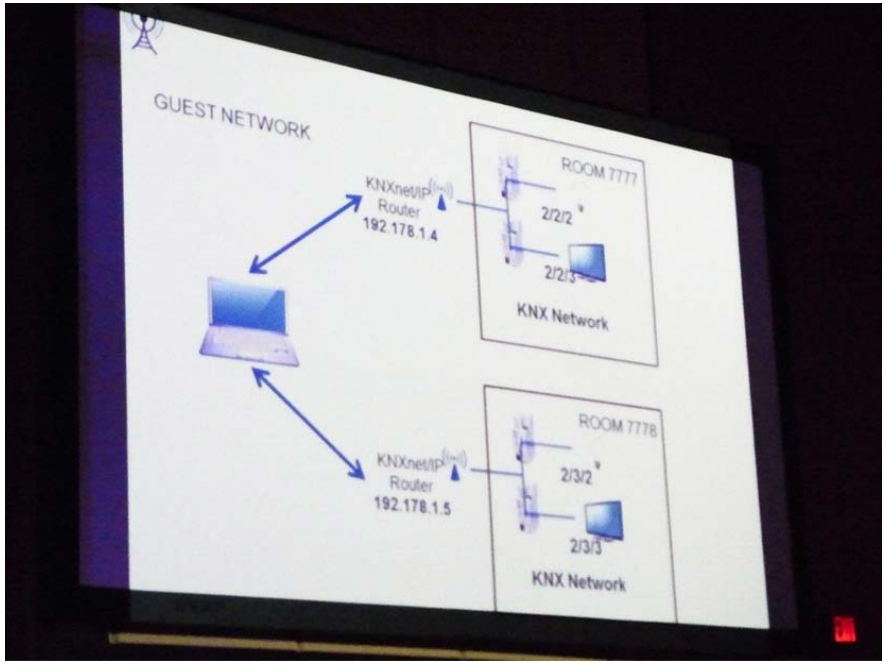
Molina 氏によるホテル業界へのアドバイス

建物システムハッキング事例

- IPアドレスを推測し、別な客室の機器（照明、空調、テレビなど）に対して、リバースエンジニアリングしたKNXコマンドを送って不正に操作できることを確認した。

ゲストネットワークと、客室制御用のネットワークが同一セグメントであり、認証等が考慮されていなかった。





http://scan.netsecurity.ne.jp/article/2014/09/10/34815.html

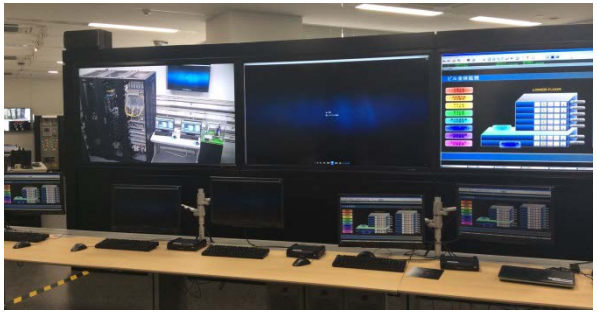
背景のまとめ

- BAシステムのクラウド化が進行している
  1. もうBAシステムは「閉じたシステム」では済まされない
  2. 今後、クラウド化はますます進んでいく
  3. 高度なエネルギーマネジメントシステム、建物群管理などクラウドならではのシステム、サービスが提供され始める
  4. IoTとの統合も進むと考えられる

- インターネット、ネットワークを介した攻撃は高度化し、様々な手法を使って、BAネットワークにも侵入してきている
  1. BAネットワークにも適切なセキュリティ対策、マネジメントが必要に（業務システムレベルの検討など）

CSSC（制御システムセキュリティセンター）

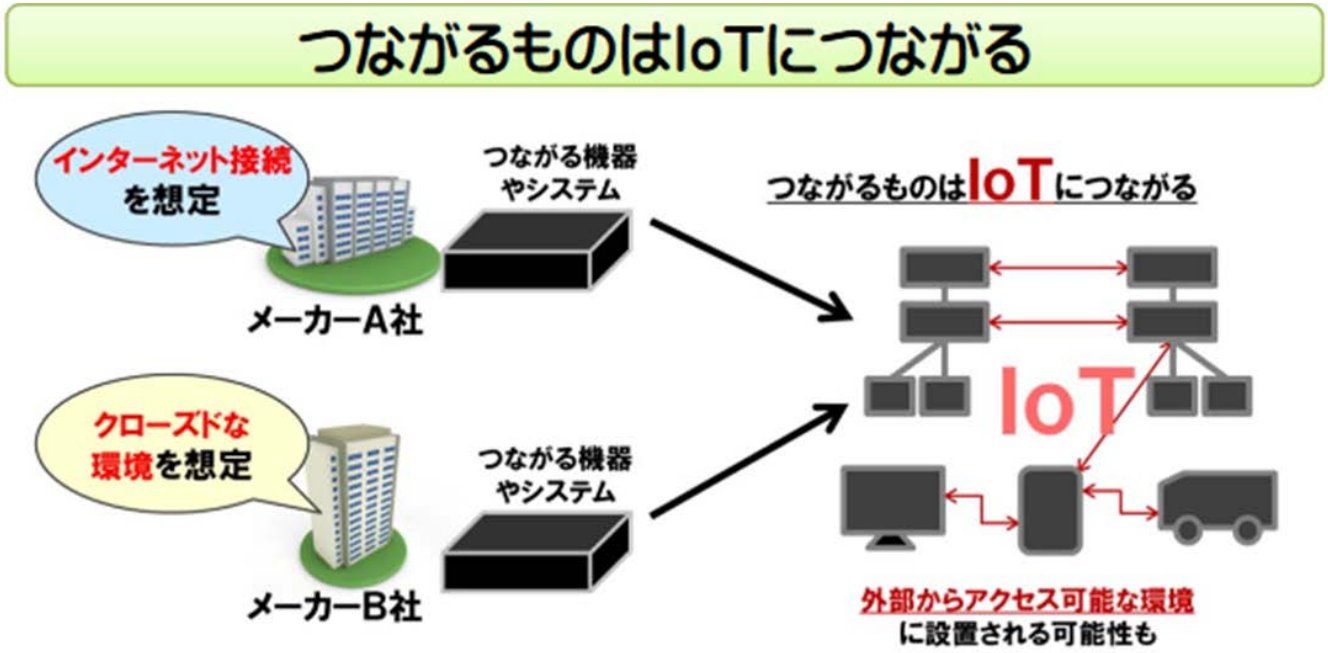
- 国民の生活を支える制御システムのセキュリティ強化と認証を使命として、2012年3月に発足。
- 研究開発や人材育成、ガイドブックの制作なども行っている。
- サイバーセキュリティの演習なども施設を使って定期的に実施。



東北多賀城本部（THHQ）の様子

IoTのセキュリティについて

- IoTのセキュリティについてガイドが策定され始めた
  - 2016.6　　分野別セキュリティガイドライン（CCDS）
  - 2016.7　　IoTセキュリティガイドライン（IoT推進コンソーシアム）
  - 2016.10　　IoTセキュリティガイドライン（トレンドマイクロ）

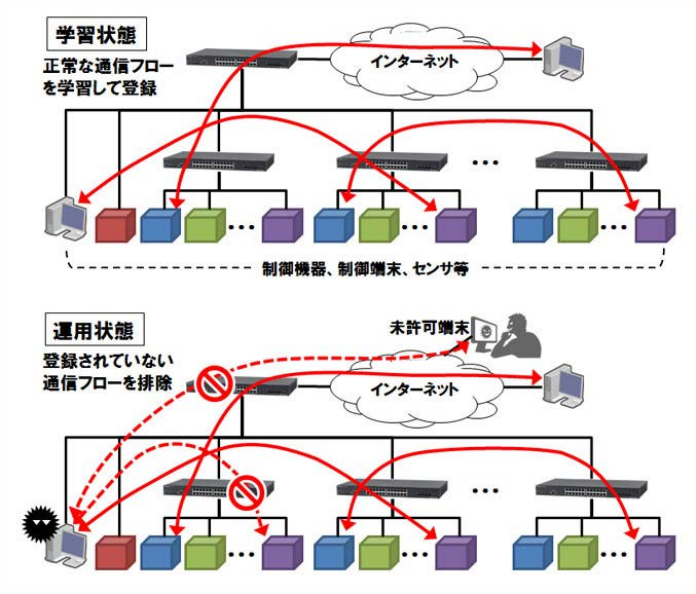


IoTセキュリティガイドライン ver1.0 概要より引用

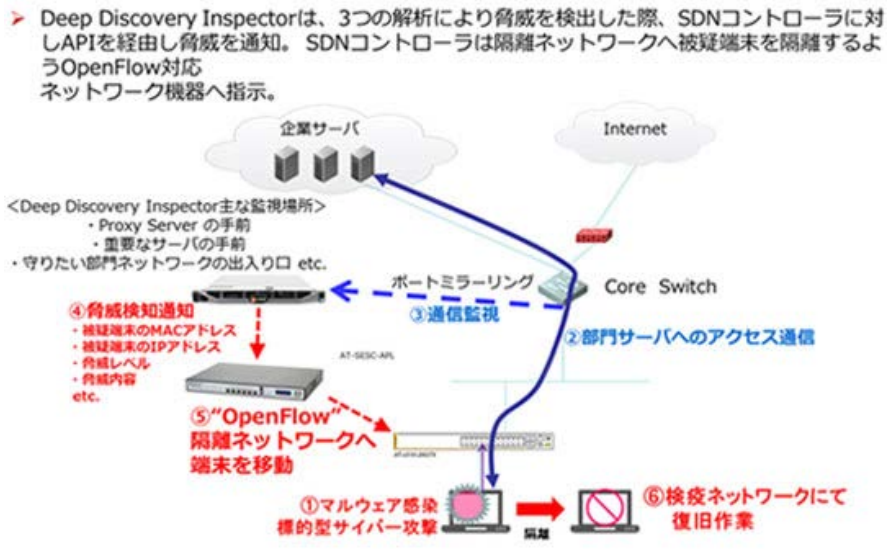
ビル向けのプロダクト・ソリューション

- セキュリティHUB （CSSC＆アラクサラネットワークス
  ホワイトリスト自動生成機能付きLANスイッチ
  http://www.alaxala.com/jp/news/press/2015/20150525.html
- SDNソリューション
  ネットワーク監視と動的なネットワーク制御
  https://www.allied-telesis.co.jp/support/net.service/index.html

業務システムの考え方を
ビル設備に



AX2530Sシリーズの動作：HPより引用



https://www.allied-telesis.co.jp/sdn/solutions4.html

ビルでのセキュリティ対策の課題

- 高度な知識が要求される
  - 建物設備設計者、建物管理技術者のスキルセットに合わない
- クローズドシステムを前提に設計されている
  - コントローラにはセキュリティ対策ソフトが入らない
  - 専用端末なので安全だといわれる
- どこまで対策すればよいのか分からない
  - リスクと脅威の定量化ができず、正しい投資判断ができない

正しい知識と対策のポイントを広める

建物設備システムリファレンスガイド

ファシリティ・インフラWG

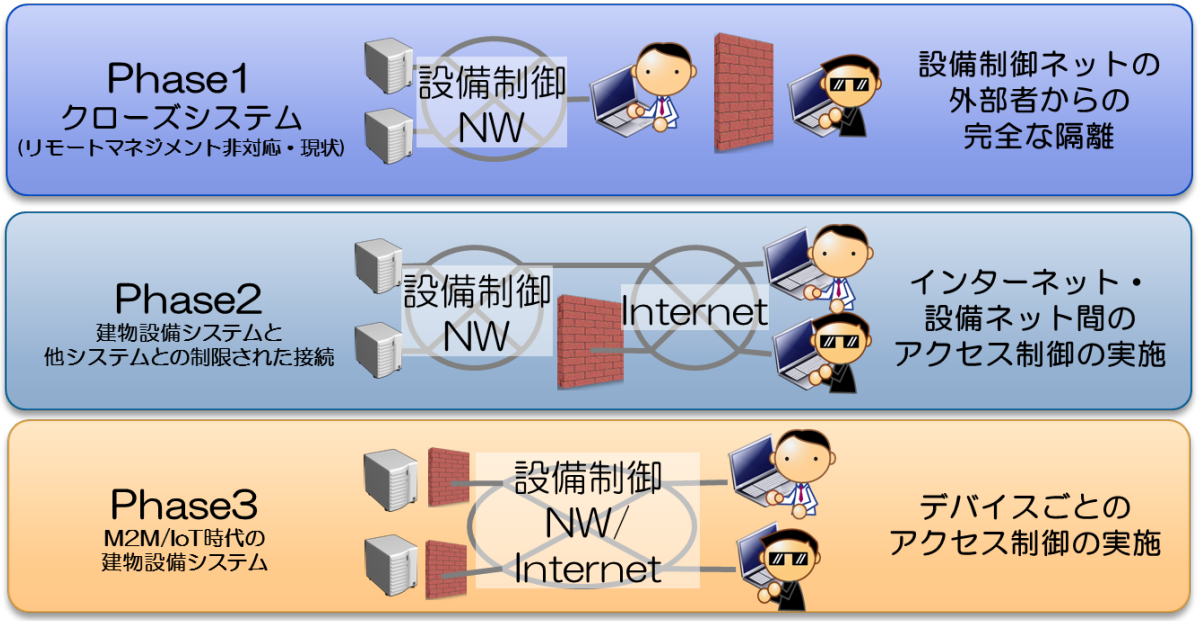
建物設備システムリファレンスガイド

現状、GUTP／JDCCの会員のみ参照可能なドキュメント

目的

- 建物設備システム、およびそれを監視制御する中央監視システムを主な対象とし、近年の技術動向やセキュリティリスクを踏まえて、その「あるべき姿」を提言する

- 建物の設計時だけでなく、運用時に必要となる留意・要求事項も参照できるよう配慮。
  建物の設計者、建物管理者、ビルオーナー、データセンター事業者、
  社内の情報システム部門の方など、幅広い読者を対象としている。
  （多様なステークホルダーとの情報共有のためのガイドブック）



建物設備システムの3つのフェーズ

ページ構成

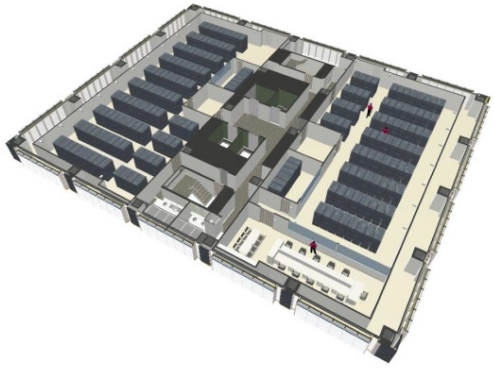
第１章　本リファレンスガイドについて
ドキュメントの概要、解説

第２章　建物設備システムセキュリティの管理策
これからの建物設備システムの設計要件、21の管理策

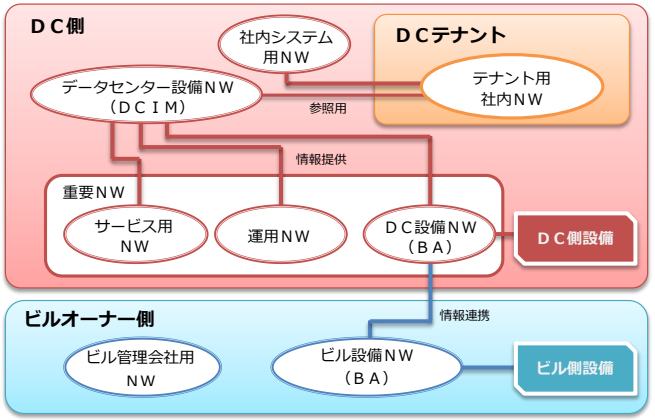
第３章　モデルケース・データセンター
モデルケースの建物を想定し、セキュリティについて考察

第４章　建物設備システム・セキュリティプラクティス
具体的な設計例を示して、脅威、対策などを例示

モデルケース・データセンター



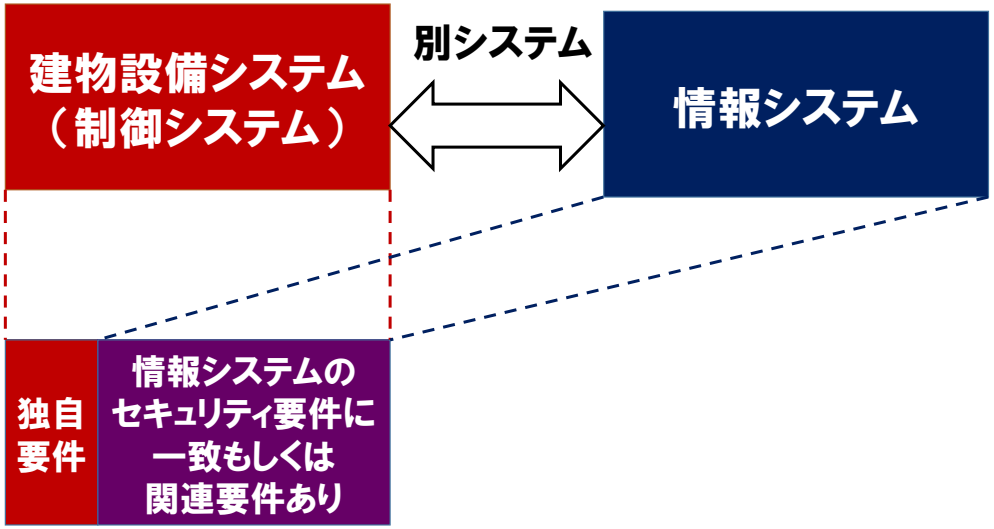
モデルケース・データセンター
（フロアプラン）



モデルケース・データセンター
（ネットワーク構成）

対象領域

- 本リファレンスガイドの内容は、制御システムの中でも、建物設備に特化したものとなっています。ISMS、CSMSと関連は深いですが、建物設備独自に培った慣習を踏まえて作成しています。



建物設備システムとして
必要となるセキュリティ要件

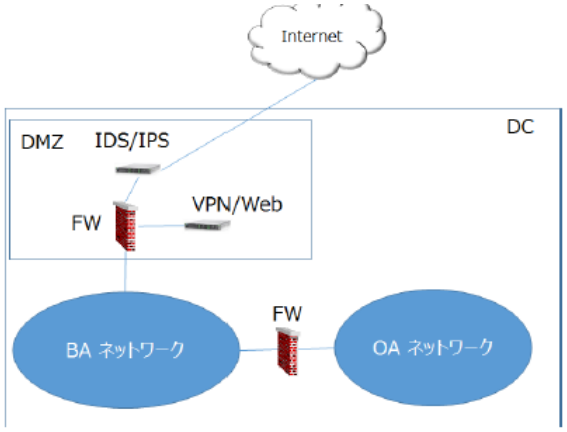
建物設備システム設計の要件

① 外部ネットワークへの接続を前提にした設計・実装・運用・管理

- 建物設備システムを構成する機器すべてに、インターネットに接続される可能性が存在することを前提にした、設計・実装・運用・管理が求められる

② オープンシステムを前提にした設計・実装・運用・管理

- 組み込みシステムから、汎用性の高いOSを利用したコントローラが一般化。
- ブラックボックス化したソフトウェアモジュールを含むソフトウェア群が存在することを前提に、現在の情報システムと同等のサイバーセキュリティ対策が必要



建物設備システム設計の要件

③ ライフサイクルマネジメントを前提としたサプライチェーン

- 出荷済みのシステムに対しても、継続的なサイバーセキュリティ対策が実施可能な体制と契約関係を構築する必要

④ 既存建物設備システムとの一貫性を前提としたセキュリティ対策

- 現状のセキュリティリスクを可視化（見える化）した上で、リスクの大きさに応じて、セキュリティ対策の計画を立案し、実践していくことが重要

建物設備システムの導入・運用・管理のためのサプライチェーン

セキュリティ実現の為のプロセス

- セキュリティ実現の為のプロセス　NIST「Guide for Conducting Risk Assessments（SP800-30）」を参考に、建物設備システムのプロセスを規定

設備に起き得る被害・障害として、避けなければいけないことをリストアップ

①設備の特徴の定義

②脅威・ぜい弱性分析・リスクの判断を行う

③要因を攻撃されない管理策の検討

④選択した管理策の有効性の評価

21の管理策

- **建物設備システムにおけるセキュリティ管理策として21項目を抽出。より具体的なセキュリティ対策の例示を行う。**

物理的設計における管理策	
1	建物設備システムの重要な構成機器(端末・コントローラー・ネットワークを含む)を設置した室・空間は専用のものとすること
2	建物設備システムの構成機器(端末・コントローラー・ネットワークを含む)を設置された室・空間においてはアクセス制御と入退室記録の管理を行うこと
3	建物設備システム端末においては、建物設備システム以外のネットワーク・メディアが不用意に接続されることが無いよう保護措置を取ること
建物設備システム構築時における管理策	
4	建物設備システムを構成する機器リストならびに構成図を作成すること
5	建物設備システムネットワークと他ネットワークの分離を行うこと
6	建物設備システム端末上でのウイルス対策を実施すること
7	サポートされないソフトウェアは利用しないこと
8	不要なサービスを無効にすること
9	パスワードのルールを定め、徹底すること
10	出荷時（デフォルト）のパスワードを変更すること
設備システム運用時における管理策	
11	建物設備システムのネットワークに接続する機器（PC、可搬媒体等）のウイルス検疫は事前に実施されていること
12	建物設備システムのセキュリティ監視手順，インシデント対応手順を整備し、その教育と訓練を定期的に実施し、継続的に対応能力の向上に努めること
13	リモート接続のルールを策定すること
14	適切にマネジメントシステムが運用され、機能していることを評価すること
15	建物設備システムの最新構成情報の管理すること
16	建物設備システムに対する脆弱性と脅威を把握しておくこと
17	建物設備システムのバックアップデータを取得すること
18	要員のアカウント管理を厳密に行うこと
19	建物設備システムのセキュリティ脆弱性に関する情報を定期的に入手し、必要に応じてセキュリティパッチを適用すること
20	建物設備システムの稼動状況やログを定期的に確認すること
21	建物設備システムの重要な構成機器(端末・コントローラー・ネットワークを含む)を設置した室・空間への訪問者のアクセスには関係者が付き添うこと

21の管理策：例

- 項目名、参照しているドキュメント、説明文から構成される

[No.4] 建物設備システムを構成する機器リストならびに構成図を作成すること			
J-CLICS	ISO/IEC 27001	FISC 第８版	NIST IR7628
Step2 3	8.1	運 4, 57, 66	SG.CM-2

建物設備システムにおいて、管理されていない機器からウィルス感染が広がるインシデントが発生しています。資産を管理することで、セキュリティリスク、脆弱性を把握することにつながり、セキュリティ対策計画の立案につなげることができます。したがって、システムを構成するコンポーネントの台帳や、ネットワーク構成図を整備し、常に最新化することが求められます。

物理的設計における管理策

1. 建物設備システムの重要な構成機器を設置した室・空間は専用のものとすること

2. 建物設備システムの構成機器を設置された室・空間においてはアクセス制御と入退室記録の管理を行うこと

3. 建物設備システム端末においては、建物設備システム以外のネットワーク・メディアが不用意に接続されることが無いよう保護措置を取ること

建物設備システム構築時における管理策

4. 建物設備システムを構成する機器リストならびに構成図を作成すること
5. 建物設備システムネットワークと他ネットワークの分離を行うこと
6. 建物設備システム端末上でのウィルス対策を実施すること
7. サポートされないソフトウェアは利用しないこと
8. 不要なサービスを無効にすること
9. パスワードのルールを定め、徹底すること
10. 出荷時(デフォルト)のパスワードを変更すること

建物設備システム運用時における管理策

10. 建物設備システムのネットワークに接続する機器のウィルス検疫は事前に実施されていること
11. 建物設備システムのセキュリティ監視手順，インシデント対応手順を整備し、その教育と訓練を定期的に実施し、 継続的に対応能力の向上に努めること
12. リモート接続のルールを策定すること
13. 適切にマネジメントシステムが運用され、機能していることを評価すること
14. 建物設備システムの最新構成情報の管理すること
15. 建物設備システムに対する脆弱性と脅威を把握しておくこと
16. 建物設備システムのバックアップデータを取得すること
17. 要員のアカウント管理を厳密に行うこと
18. 建物設備システムのセキュリティ脆弱性に関する情報を定期的に入手し、必要に応じてセキュリティパッチを適用すること
19. 建物設備システムの稼動状況やログを定期的に確認すること
20. 建物設備システムの重要な構成機器（端末・コントローラ・ネットワークを含む）を設置した室・空間への訪問者のアクセスには関係者が付き添うこと

建物設備システム運用時における管理策

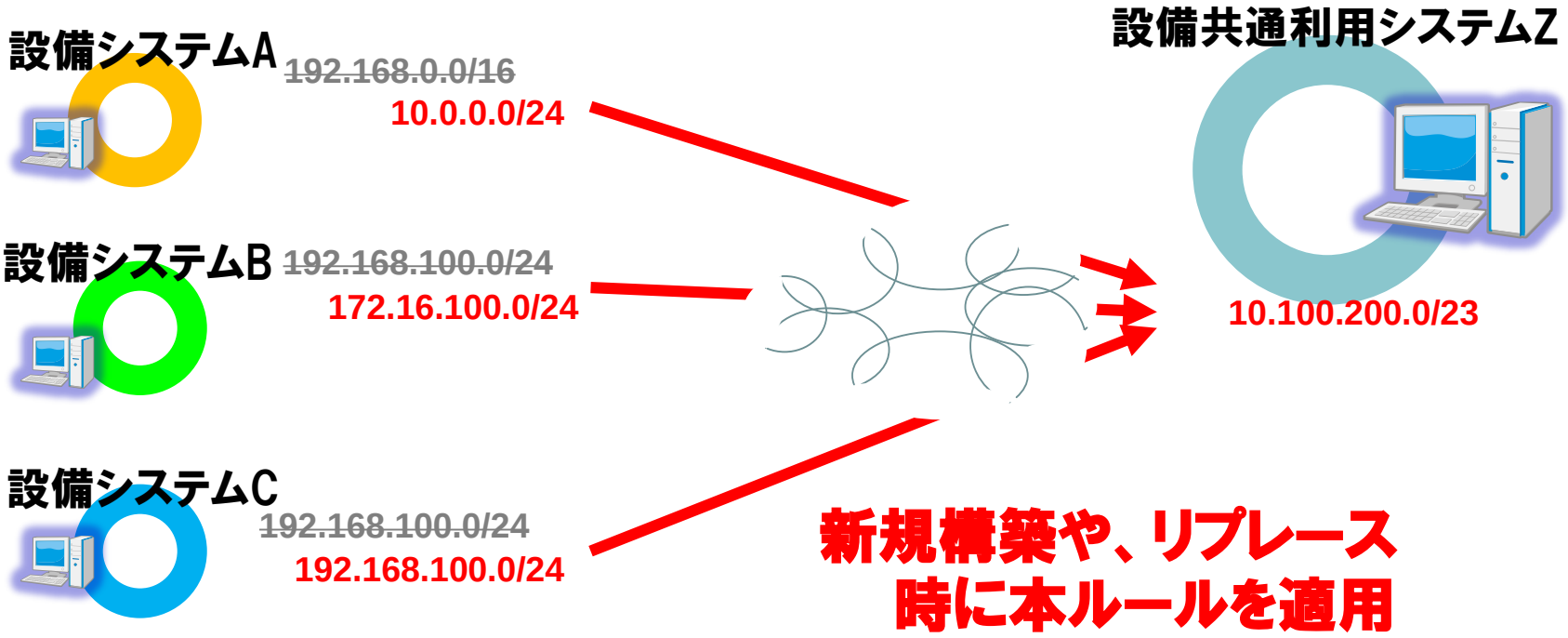
11.**建物設備システムのセキュリティ監視手順，インシデント対応手順を整備し、その教育と訓練を定期的に実施し、 継続的に対応能力の向上に努めること**

➡ **サイバー演習の実施を推奨**

http://www.css-center.or.jp/

特徴的な管理策

- 建物設備ネットワーク内のIPアドレスの適切な設計、組織間連携についても、簡単に記述を行っている。
  → 第二版以降で拡充を予定。



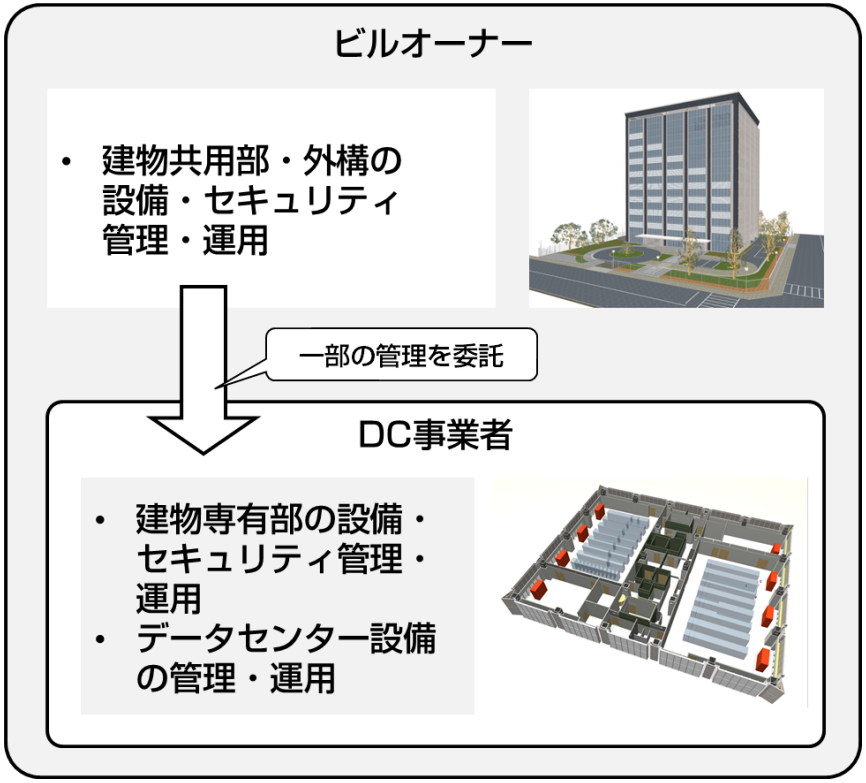
21の管理策の使い方

- リスト化して共有することで、コミュニケーションツールとして利用
- 設計、運用時のチェックの他に、**発注仕様、調達要件**となることを想定
- 補足事項を追加したチェックリストを第2版で整備する予定

No.	管理策	○○における対策案	管理策を実施しない場合のリスク例	各管理策に対応するガイドライン項目			
				J-CLICS	ISO/IEC 27001:2013	FISC 第8版	NIST IR7628
物理的設計における管理策 (3.4)							
1	建物設備システムの重要な構成機器(端末・コントローラー・ネットワークを含む)を設置した室・空間は専用のものとすること	中央監視システム、電力監視システム、入退管理システム等は防災センターに設置。監視カメラ装置などはサーバ室に設置する。コントローラ類は原則EPS内に設置し、各種盤についても鍵施錠管理を行う。	建物設備システム関係者以外がシステムを誤って操作することにより、システムが誤動作・停止する	Step1 1	11	設54-55,82,83-1 運11-13	SG.AC-4 SG.PE-2,3
2	建物設備システムの構成機器(端末・コントローラー・ネットワークを含む)を設置された室・空間においてはアクセス制御と入退室記録の管理を行うこと	防災センター、サーバ室については最高のセキュリティレベルとすることで、アクセス制御を行い、入退室記録も十分な容量確保する。コントローラ類については、防災センター内の鍵BOXによるカードリーダでアクセス制御を行う。	不審者の侵入により建物設備システムが破壊される	Step1 3	11	運11-13	SG.PE-3,10
3	建物設備システム端末においては、建物設備システム以外のネットワーク・メディアが不用意に接続されることが無いよう保護措置を取ること	各システム端末ではUSBポートガードにより、管理されていないUSBメモリの接続を防止し、外部メディアオートラン機能を無効化する。同様にEPS内にある設備系ネットワーク機器（スイッチなど）にもポートロックをかける。	セキュリティ対策が不十分なシステム・メディアがウイルス感染し、建物設備システムへ拡散する	--	11	運57	SG.CM-5
建物設備システム構築時における管理策 (3.5)							
4	建物設備システムを構成する機器リストならびに構成図を作成すること	竣工図面と納入仕様書により構成を管理する。改修時もタイムリーな更新を心がける。	セキュリティリスク、脆弱性を把握できないことにより、管理されていない機器からウイルス感染が広がる	Step2 3	8.1	運4, 57, 66	SG.CM-2
5	建物設備システムネットワークと他ネットワークの分離を行うこと	建物設備ネットワークとしては独立して構成し、マルチメディアネットワーク等の接続は行わない。IPv6を用いた通信制御を行うことで不正通信を排除するとともに、IPsecやSSL/TLS通信によって傍受や改ざんの防止、不正通信の排除を行い、ファイアウォール等による通信制御、侵入検知も実施する。	他ネットワークのシステムに入り込んだウイルスが建物設備システムに感染する、もしくは、建物設備システムで感染したウイルスが他ネットワークへ波及する	Step2 4	13.1	運6, 56 技43, 44	SG.SC-7, 30
6	建物設備システム端末上でのウイルス対策を実施すること	建物設備システム端末に挿入する可搬記憶媒体の事前ウィルスチェックを実施する。 ※中央監視システム等へのホワイトリストソフト、セキュリティパッチの適用は追加コストと動作検証の必要から構築時は適用が難しい。	端末がウイルス感染してもウイルスを検知できない	Step2 6	12.2	運30 技49-51	SG.SC-16, SG-SI-3
7	サポートされないソフトウェアは利用しないこと	設備システムについて専用端末として運用を行う。	残存したままのセキュリティ脆弱性を利用して攻撃される	Step2 8	14.2	運72,73	SG.SA-3, 4
8	不要なサービスを無効にすること	同上	不要なサービスがセキュリティホールになり、攻撃の踏み台になる	Step2 8	12.6	運72,73	SG.PL-2
9	パスワードのルールを定め、徹底すること	利用端末においては、パスワードの定期的な変更を実施する。	簡単なパスワードは容易に推測され、建物設備システムがクラッキングされる	Step 1 3	9.3	運17, 技35	SG.AC-21
10	出荷時（デフォルト）のパスワードを変更すること	同上	マニュアル上で公開されているデフォルトパスワードを用いて容易に攻撃される	Step 1 3	9.3	運17, 技35	SG.CM-10
設備システム運用時における管理策 (3.6)							
11	建物設備システムのネットワークに接続する機器（PC、可搬媒体等）のウイルス検疫は事前に実施されていること	接続される機器については、所定のウィルス対策・検疫を受けたもののみとルールを決める。	ウイルス感染機器を不用意に、建物設備システム又は建物設備システムネットワークに接続した場合、即時感染する	Step 1 2	12.2	運30、技49-51	SG.SI-3

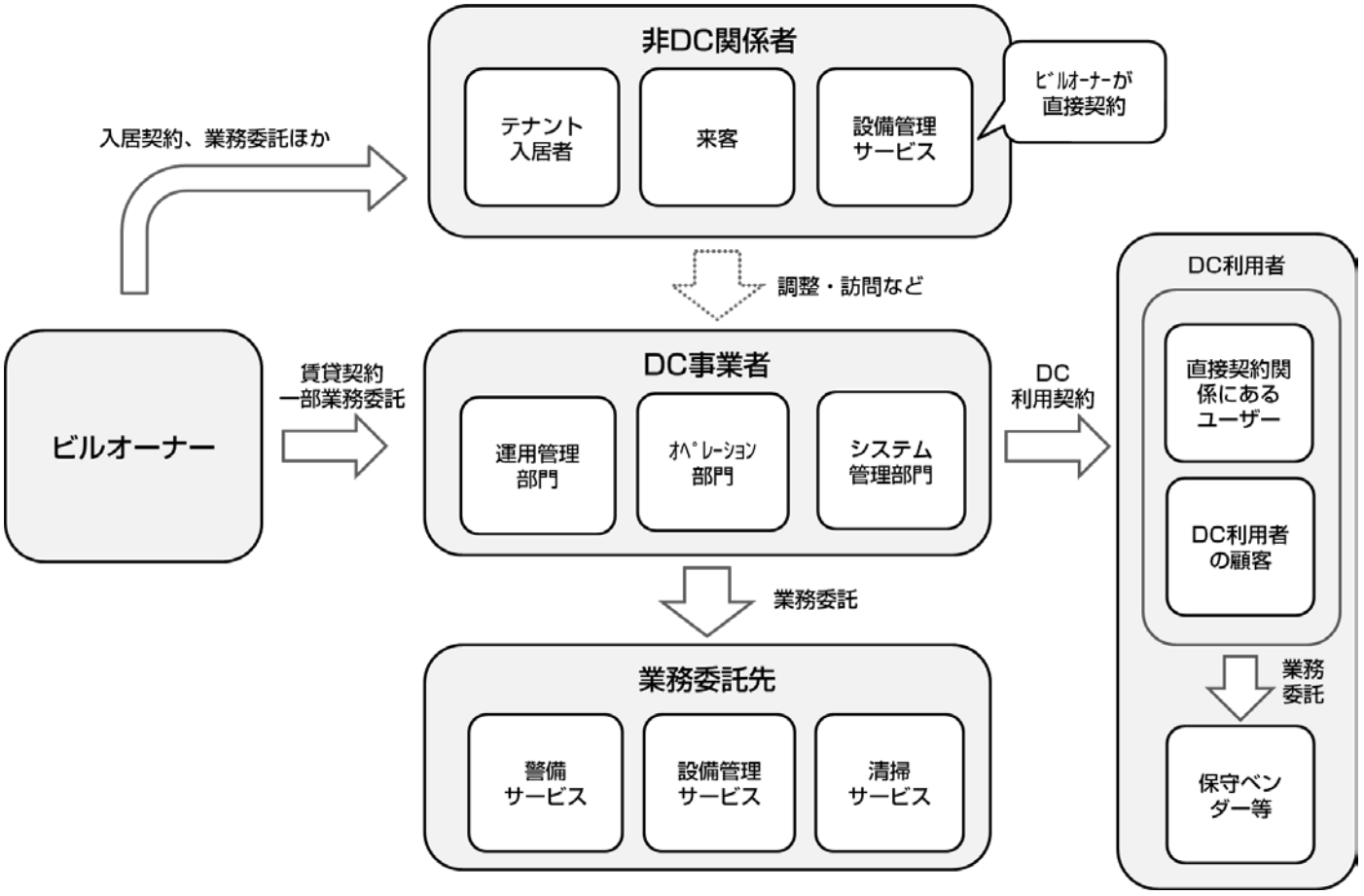
モデルケース・データセンター

- 架空のデータセンターを題材として、第2章で述べた管理策に照らし合わせながら、モデルケースとしてのデータセンターのサービス・建物・設備・運用についてセキュリティの検討を行う。



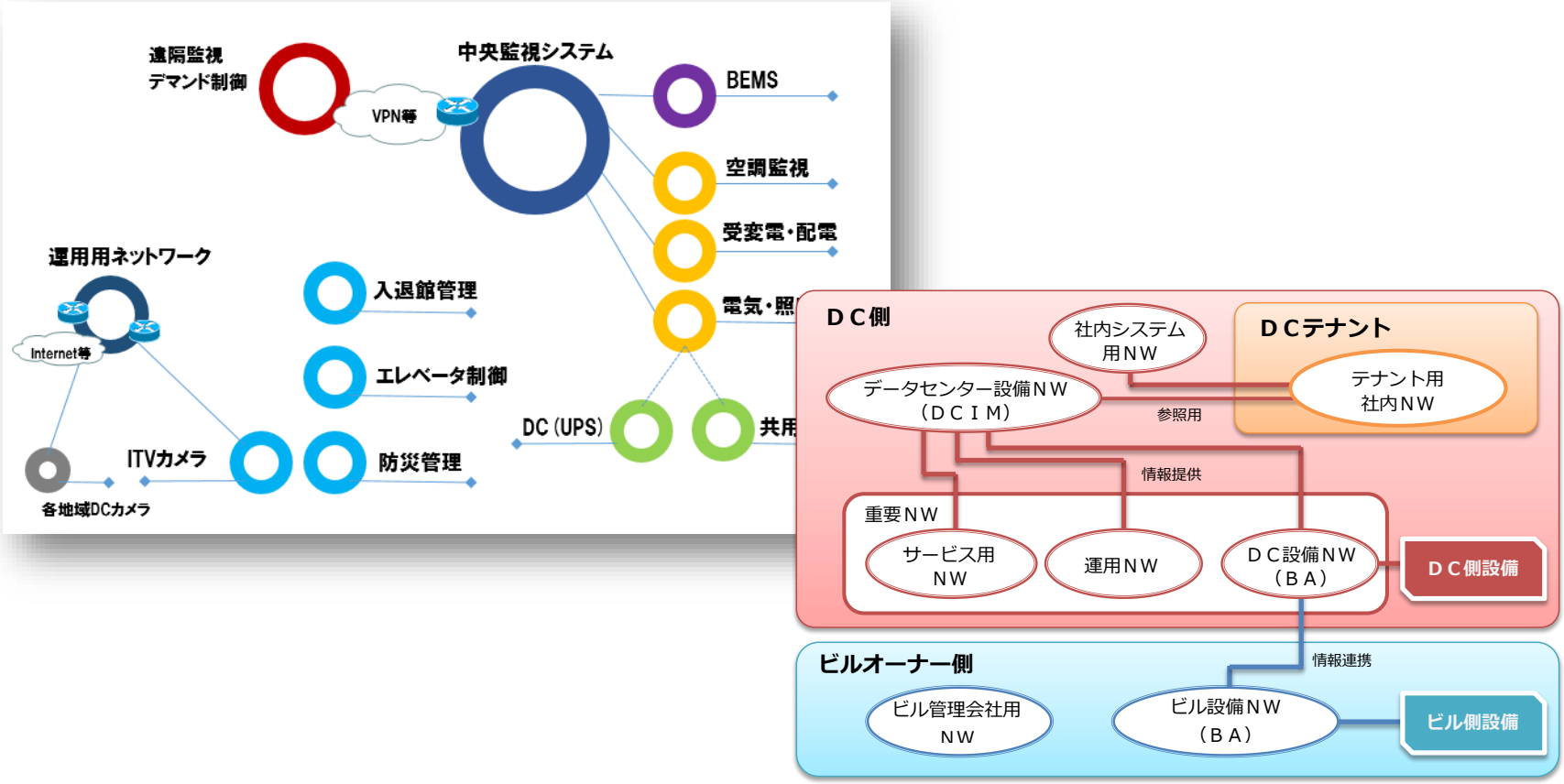
データセンター事業者概要

- 実際のデータセンター事業者の運用実態を鑑みて、契約関係を仮定している



建物設備システムについて（1）

- ビルオーナー側の建物設備システムと、DC側の管理システムがあり、それぞれにどのような脅威があるのか考察する



システム運用体制

- 建築設備システムにおける、監査・マネジメントへ対応が抜けており、セキュリティ上、それらが大きな課題に

<table>
<tr><th></th><th>商用システム</th><th>顧客システム</th><th>社内ﾊﾞｯｸｵﾌｨｽ
システム</th><th>設備システム</th></tr>
<tr><td>計画</td><td rowspan="2">システム
企画/開発
部門</td><td rowspan="2">顧客</td><td rowspan="4">情報システム
部門</td><td rowspan="4">ファシリティー
マネジメント
部門</td></tr>
<tr><td>構築</td></tr>
<tr><td>運用</td><td colspan="2">システム運用部門</td></tr>
<tr><td>改善維持</td><td>システム企画/
開発部門</td><td>顧客</td></tr>
<tr><td>監査</td><td>内部／外部</td><td>顧客／内部</td><td>内部／外部</td><td rowspan="2">対応組織
なし</td></tr>
<tr><td>ﾘｽｸﾏﾈｼﾞﾒﾝﾄ</td><td>ISMS/CSMS
対応組織</td><td>ISMS/CSMS
対応組織</td><td>ISMS/CSMS
対応組織</td></tr>
</table>

建物設備システムについて（2）

■ 管理策とモデルケースにおける対策を示す

No.	管理策	モデルケースにおける対策
物理的設計における管理策 (2.3.1)		
1	建物設備システムの重要な構成機器(端末・コントローラー・ネットワークを含む)を設置した室・空間は専用のものとすること	建物設備・構成機器を設置した室・空間を専有で設計した。
2	建物設備システムの構成機器(端末・コントローラー・ネットワークを含む)を設置された室・空間においてはアクセス制御と入退室記録の管理を行うこと	建物設備・構成機器を設置した室・空間のアクセス制御と入退室記録の管理を行うようにした。階によってアクセスレベルが異なるためエレベータの乗降制御を行い、部屋ごとにカードリーダーによるアクセス制御を行っている。
3	建物設備システム端末においては、建物設備システム以外のネットワーク・メディアが不用意に接続されることが無いよう保護措置を取ること	端末のUSBポートを塞いだり、施錠可能な筐体やラックなどに収めるなどして、基本的に利用できないようにしている。
建物設備システム構築時における管理策 (2.3.2)		
4	建物設備システムを構成する機器リストならびに構成図を作成すること	建物改修時に作成した設備図面や納入仕様書で構成を管理している。詳細な管理までは行えていない。
5	建物設備システムネットワークと他ネットワークの分離を行うこと	建物設備とデータセンター設備の一部は一体で管理されているため、建物設備システムへの攻撃による、データセンターへ影響も懸念される。

建物設備システムセキュリティ・プラクティス

- モデルケース・データセンターにおいて起きうるセキュリティ・インシデントを紹介し、それに対応するセキュリティ管理策を、21の管理策を参照しながら紹介していく

① 基本的な情報セキュリティ対策の不備を突いた攻撃

② 建物設備システム関連携の不備による事故

③ 建物設備システムを構成するミドルウェア経由の攻撃

④ データセンターを目標とした標的型攻撃

基本的な情報セキュリティ対策の不備を突いた攻撃

背景

- 架空のデータセンターを含む建物内で紛失物が発生した際にはまずは警備室や防災センター等に申告・届けるのが通常です。

発生

- 架空のデータセンターに不満を持った顧客側のシステム構築SEが、意図的な行動としてウィルスに感染したUSBをエントランスに紛失物を装い落しておきました。
  該当物は警備室に届けられセキュリティ意識や教育不足の中で持ち主を探すことを第一に考える警備員が①そのUSBを制御システム管理コンソール等のネットワークに接続したパソコン上で確認を行おうとしてウィルスが制御システムに広がってしまい、システムが不安定になりました。

基本的な情報セキュリティ対策の不備を突いた攻撃

把握-事後対応

- 架空のデータセンター事業者は、入退館システムが正常動作しないことに気付き、調査した結果、対象システムがウィルスに感染したことを把握しましたが、システム復旧まで時間を要することで顧客入館の手動対応等を行うことで、データセンター利用顧客に対する信頼やサービス品質の低下を招くことになりました

リスク解説

- 外部媒体のネットワーク接続時の事前ウィルスチェック確認不備

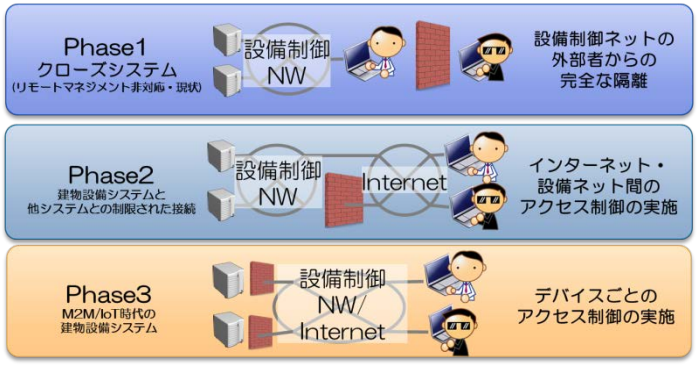
有効な管理策

- No.11：建物設備システムのネットワークに接続する機器（PC、可搬媒体等）のウィルス検疫は事前に実施されていること

まとめ

- **建物設備システムの顕在化**
  - 2012年　技術研究組合制御システムセキュリティセンター（CSSC）設立
  - 2014年　サイバーセキュリティ基本法の制定
  - 2014年　ビル管理システムに対する警察庁からの注意喚起

建物設備システムリファレンスガイド



- 建物設備システムの「あるべき姿」を目指す
- 21の管理策を規定
- モデルケース・データセンターを用いて
  建物設備システムの各種脅威について考察
- セキュリティ・プラクティスによって、
  具体的な建物設備システムの脅威を紹介

リファレンスガイドに対する声

① 建物設備システムについて書かれた網羅的なガイドで、非常に勉強になる

② もうすこし具体的な対策例がほしい

→ セキュリティはこれなら万全ということはなく、画一的な対策はリスクにもなるので、あえて記載していません

③ ２１の管理策には理想的な方法が書かれており、実際の構築の際にベンダーに対応できない、または追加費用がかかると言われた。

→ ガイドとして共有することで、発注主、設計者、管理者、ベンダーそれぞれの対応レベルが向上することを願っています

今後の活動予定

- 建物設備システムリファレンスガイドの普及、啓発
  - 講習会の実施　→　今後、各章ごとの詳細な講習会を企画予定
  - 関連団体、メーカー等との意見交換
  - 関連ガイドブック、スタンダードとの連携
  - 意見をもとにしたガイドの改訂
- 上記ガイドの改訂作業
- ファシリティのセキュリティに関する勉強会の実施

NPO法人　日本データセンター協会
http://www.jdcc.or.jp/

お問合わせ　info@jdcc.or.jp