Japan Computer Emergency Response Team Coordination Center
電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2016.03.04 14:23:15 +09'00'

ガ、スマート!

JPCERT/CC
制御システムセキュリティカンファレンス2016資料

都市ガス業界における制御系システムの セキュリティ確保の取組みについて – サイバー演習の紹介を中心に –

2016年2月17日

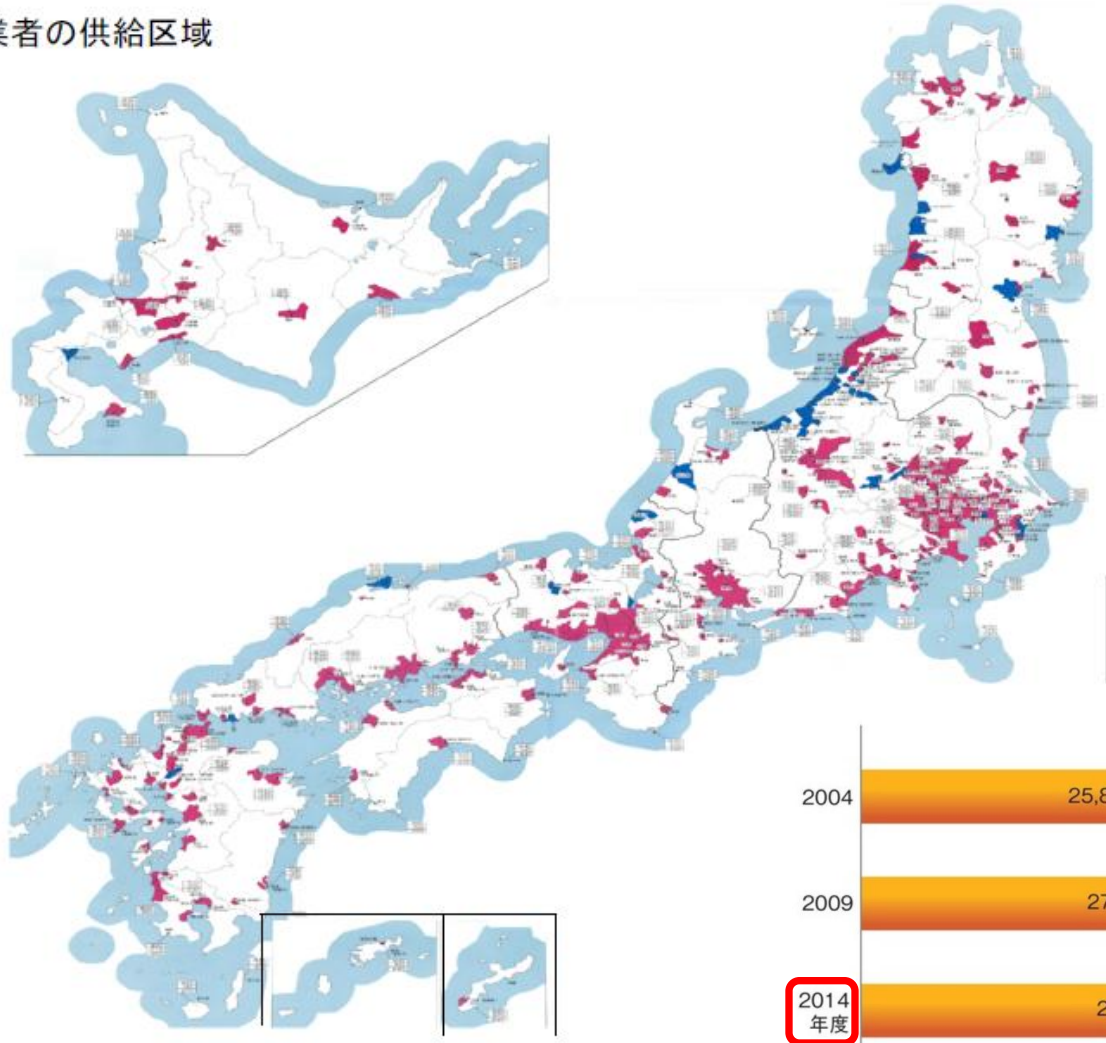
一般社団法人　日本ガス協会

目次

はじめに －都市ガス事業の概要－

① 全国に2,973万件のお客さま（2015年3月末時点）

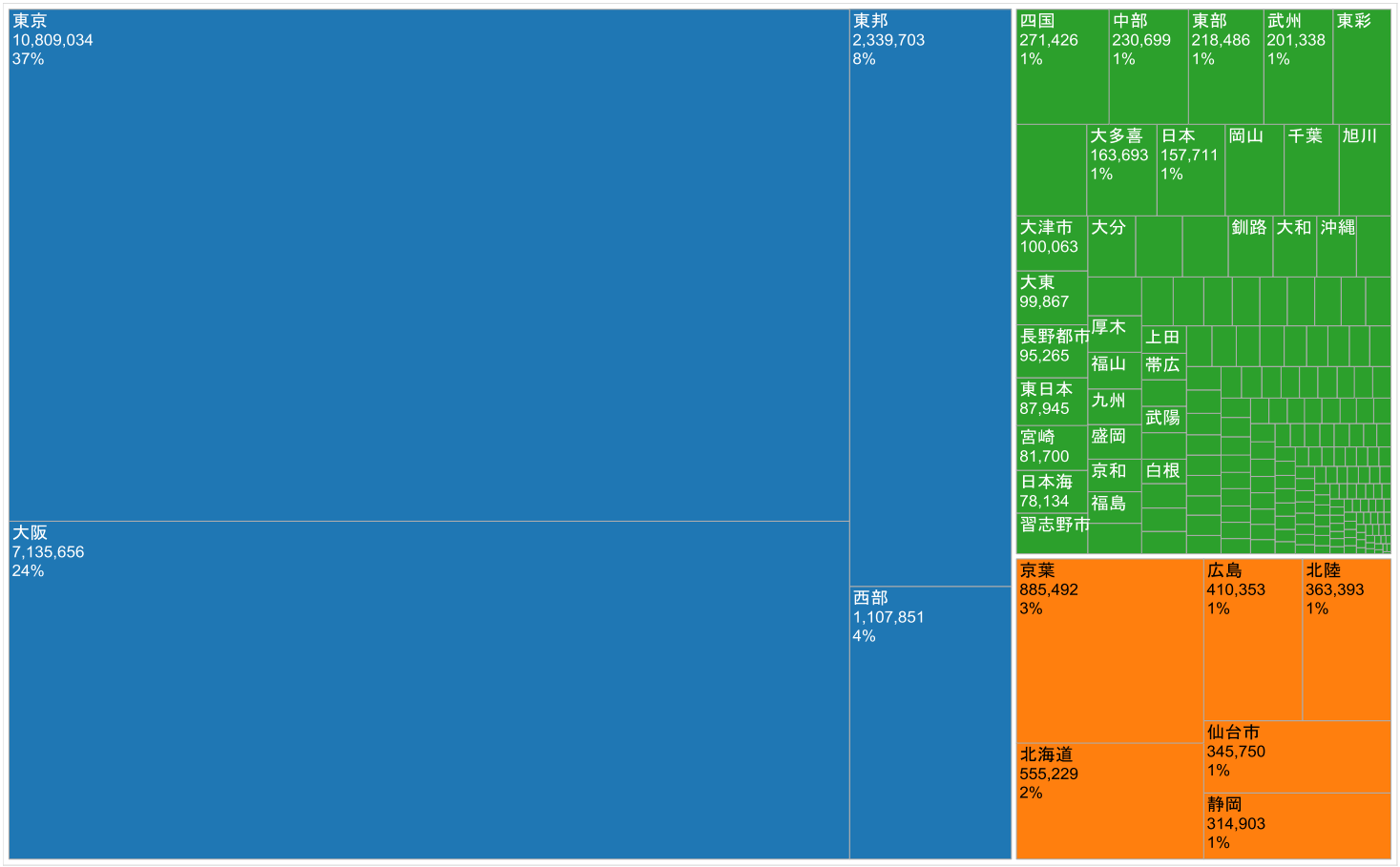
■一般ガス事業者の供給区域



② 206社の都市ガス事業者がガスを供給

需要家件数ベースで大手４社・準大手６社の計10社が全体の８割超を占める。

事業規模により事業者の所有する設備や制御システムは大きく異なる。

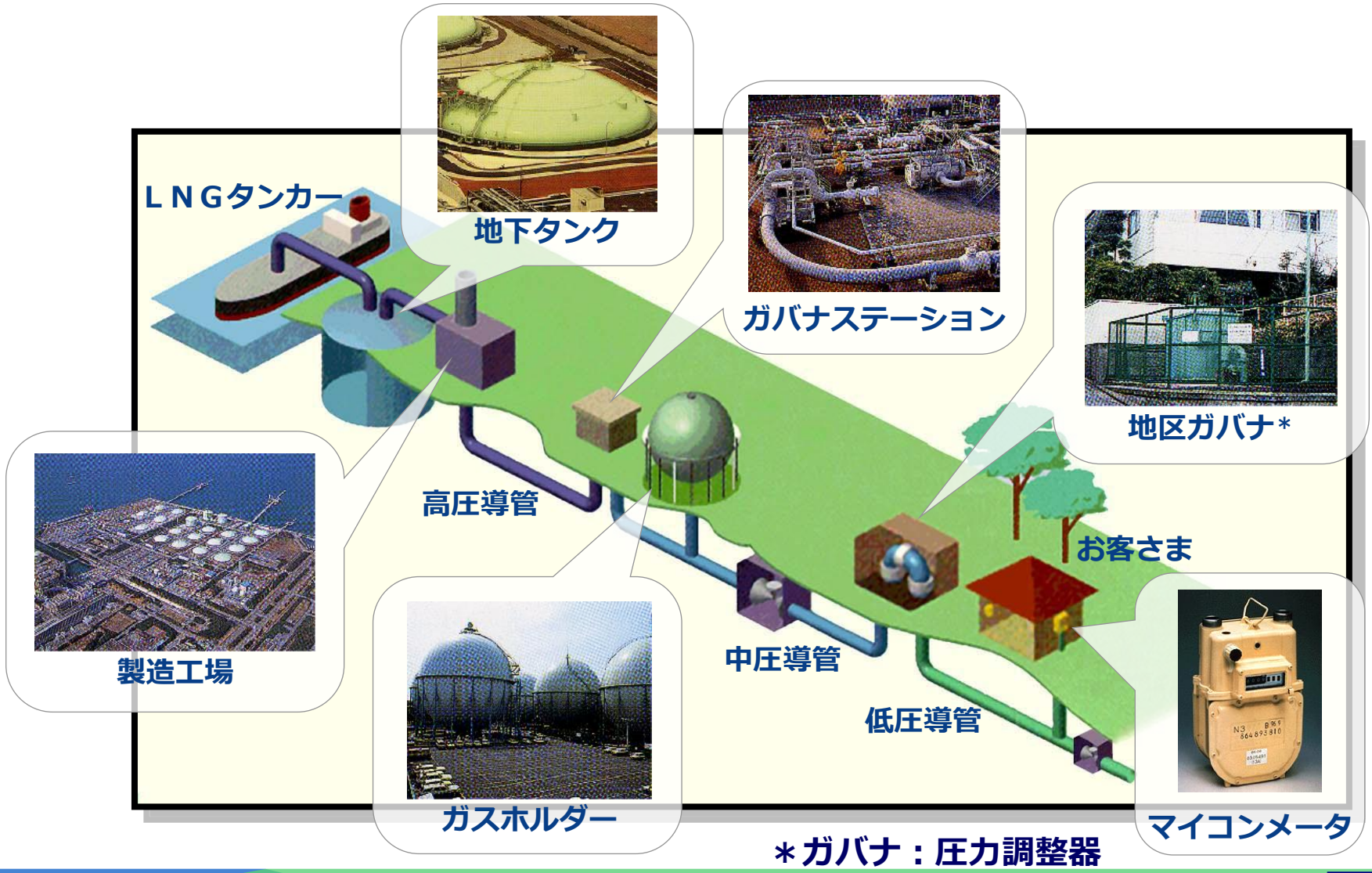


《凡例》

事業者名
需要家件数
割合

※事業者数は2016年1月末時点、需要家数は2014年3月末時点のデータによる

③ ガスをお届けするまで



＊ガバナ：圧力調整器

目次

都市ガス事業で特に意識している脅威

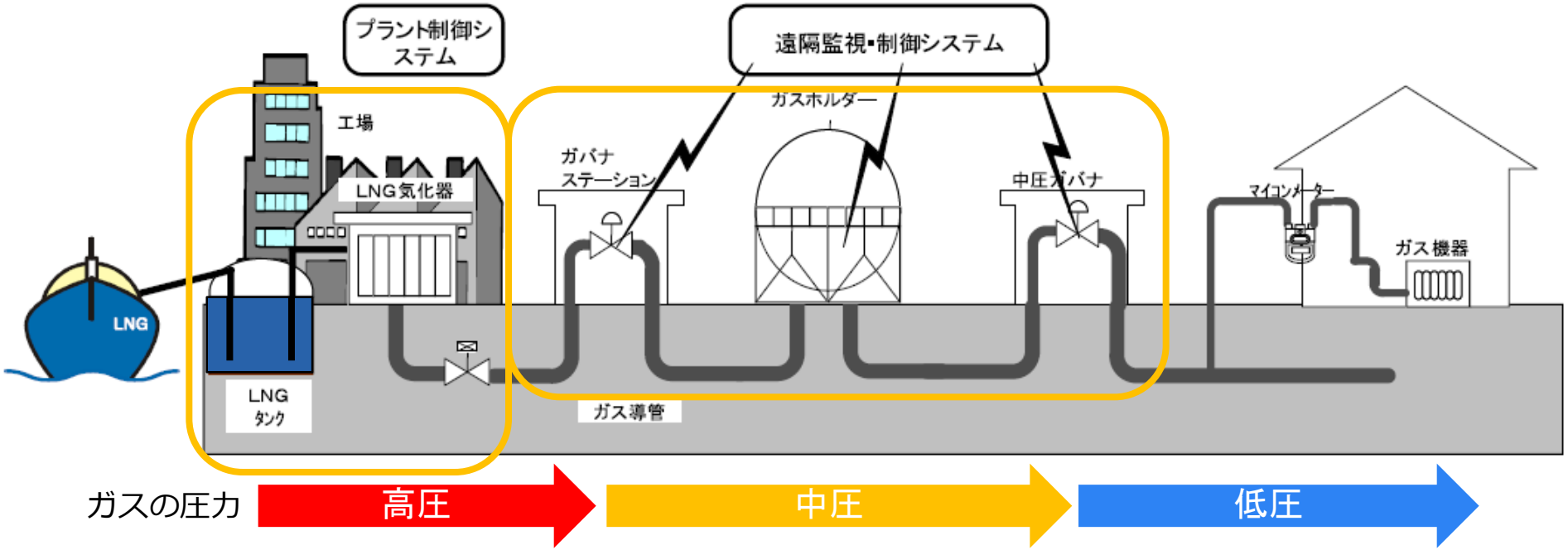
■国の情報セキュリティ対策の中で、一般ガス事業者は重要インフラ事業者として位置付けられている。ガスの安定供給を第一の使命と考えており、**供給支障を回避**する観点から、**製造・供給に関わる制御系システムへの攻撃**（外部からの不正アクセスやDoS攻撃、コンピューターウィルス感染等）**を重視**し、様々な対策をとっている
■製造支障や供給支障に至れば、ガス事業法に則り行政に報告を行う

インシデントの内容	速報	詳報	報告先＊3
製造支障事故＊1であって、ガス発生設備の運転停止時間が24時間以上のもの	事故発生から24時間以内可能な限り速やかに	事故が発生した火から起算して30日以内	経済産業大臣　及び所轄産業保安監督部長
製造支障事故＊1であって、ガス発生設備の運転停止時間が10時間以上24時間未満のもの			所轄産業保安監督部長
供給支障事故＊2であって、ガスの供給が停止し、又はガスの供給を緊急に制限したガスの使用者の数が500以上のもの			経済産業大臣　及び所轄産業保安監督部長
供給支障事故＊2であって、供給支障戸数が30以上500未満のもの			

これまでインシデント発生事例無し

＊1　製造支障事故：ガスの製造に支障を及ぼした事故
＊2　供給支障事故：ガスの供給に支障を及ぼした事故
＊3　速報および詳報は、法定の報告先の他、日本ガス協会にも情報提供を行う

都市ガス事業における制御システム



①プラント制御システム（製造系）

ガスの製造（原料の気化、熱量調整、付臭等）のために圧力・流量の制御及び監視を行うシステム

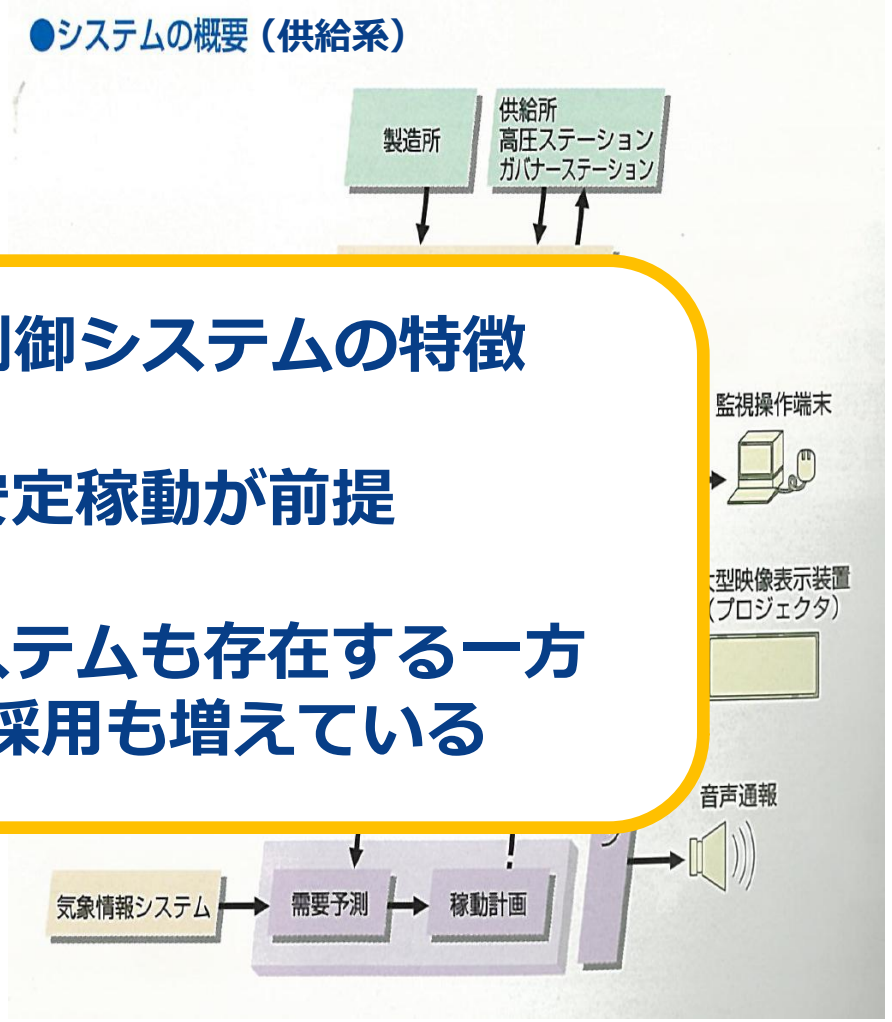
②遠隔監視・制御システム（供給系）

供給ライン圧力・流量の監視や遠隔遮断弁・ガバナ等の制御を行うシステム

参考イメージ

●大阪ガス 本社中央司令室（供給系）

●システムの概要（供給系）



ガス事業における制御システムの特徴

・２４時間３６５日の安定稼動が前提
・長いライフサイクル
・ベンダ独自仕様のシステムも存在する一方
　汎用OS・通信仕様の採用も増えている

●大阪ガス 製

泉北製造所LNG貯蔵タンク

出典：大阪ガス パンフレット「中央保安司令部」

（ご参考）安定供給につながるガスの特性

都市ガスは、以下のような特性を持ち、制御システムの停止が、ガスの供給停止に直ちに結びつくことはありません。ガス事業における制御系システムは、主に運転の自動化と遠隔化による効率向上を目的として利用されています。

このため、全体の中で多数を占める中小事業者においては、制御系システムを必要としないケースが多く見られます。

●圧力保持機能（ガスは貯められる、貯まっている）

「ホルダー」（ガスタンク）を持ち、製造停止が即時ガス供給の停止には至りません。

気体（圧縮性流体）エネルギーとして、導管（パイプライン）そのものにも「ホルダー」同様の圧力保持機能を有しています。

●設定値保持機能

「ガバナ」（圧力調整器）の圧力設定機能は機械構造であり、遠隔制御が不能になった場合でもその時点の設定値が保持され、ガス自らが保持する圧力により動力を要さずガス供給が維持されます。

【製造系】LNG受入基地における製造フロー

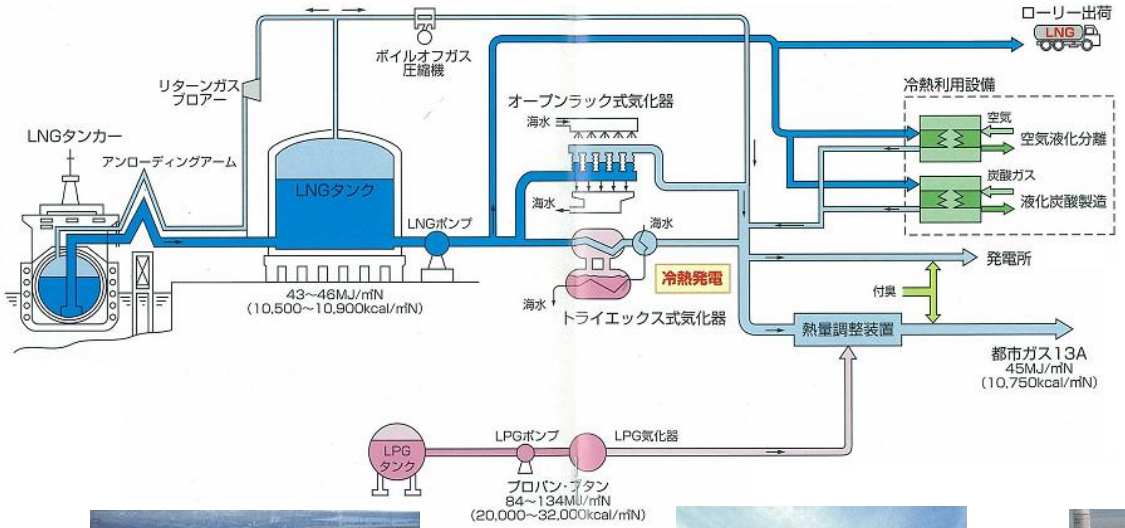

BOG圧縮機


中間熱媒体式
（トライエックス式）気化器


オープンラック式気化器


ローリー出荷設備


BOG再液化装置




冷熱利用設備


熱量調整装置


アンローディングアーム


LNG内航船


地下式LNG貯槽

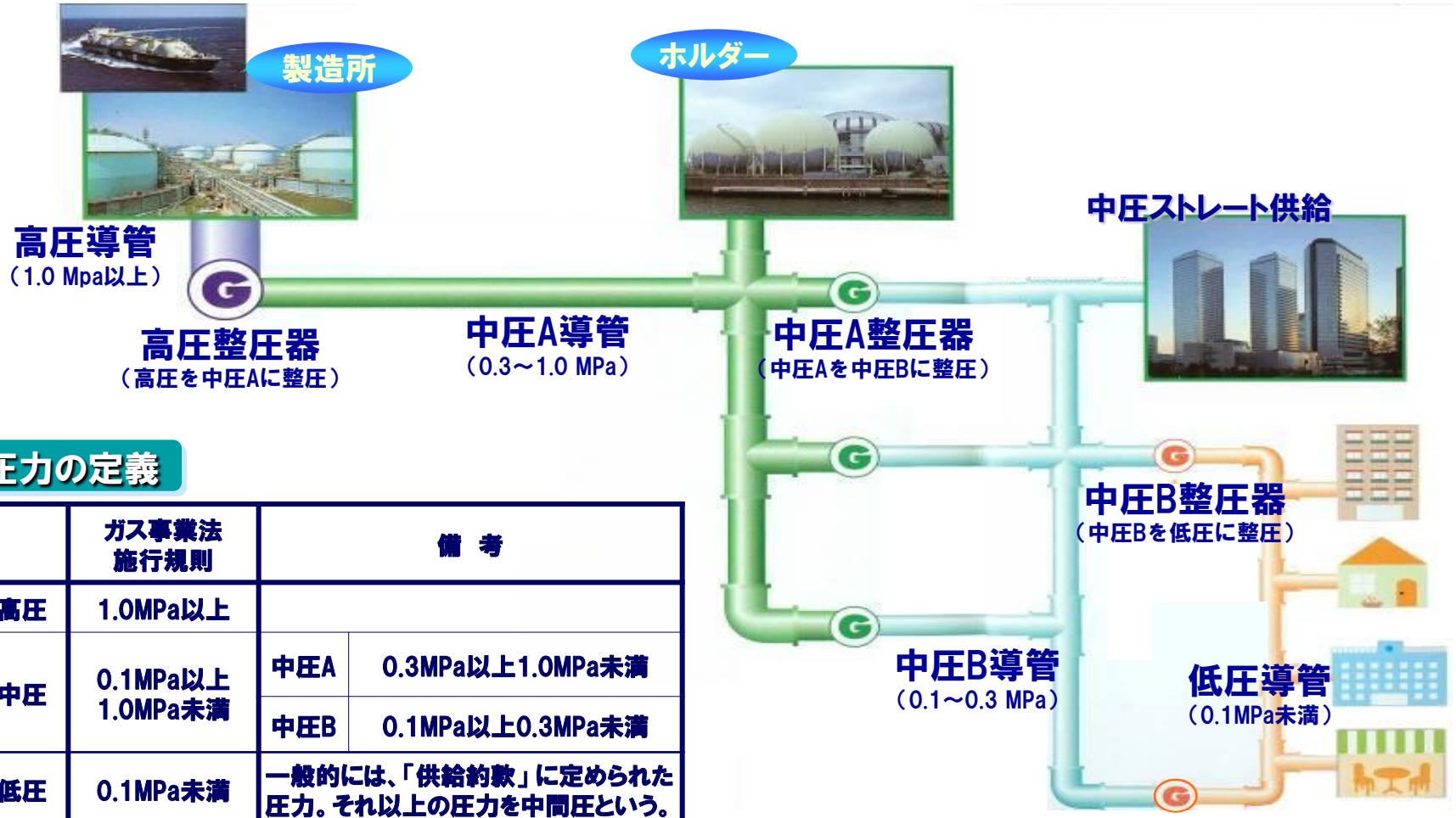

PC式LNG貯槽


ピットイン式LNG貯槽

※パイプラインでの卸供給に依るなどし、製造所を持たないガス事業者もある

【供給系】導管における供給フロー

■都市ガスは輸送効率を高めるために高圧や中圧で送出し、ガバナ(整圧器)により減圧し、お客さまに供給される

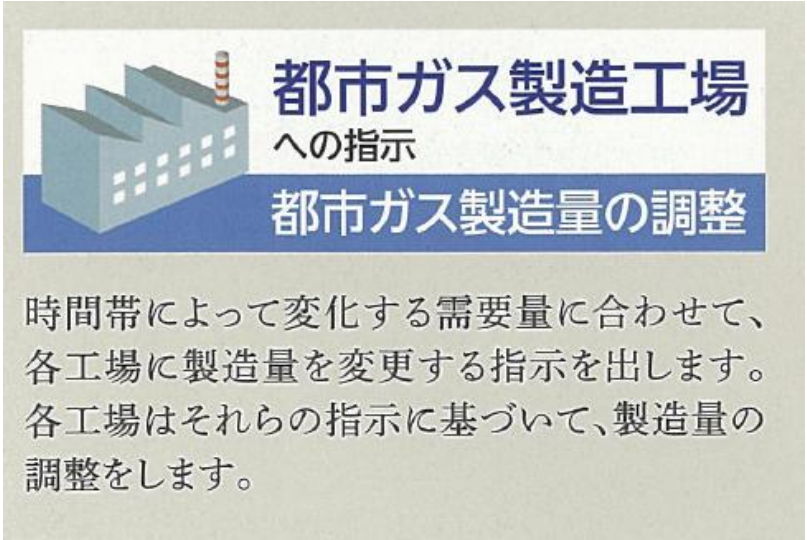


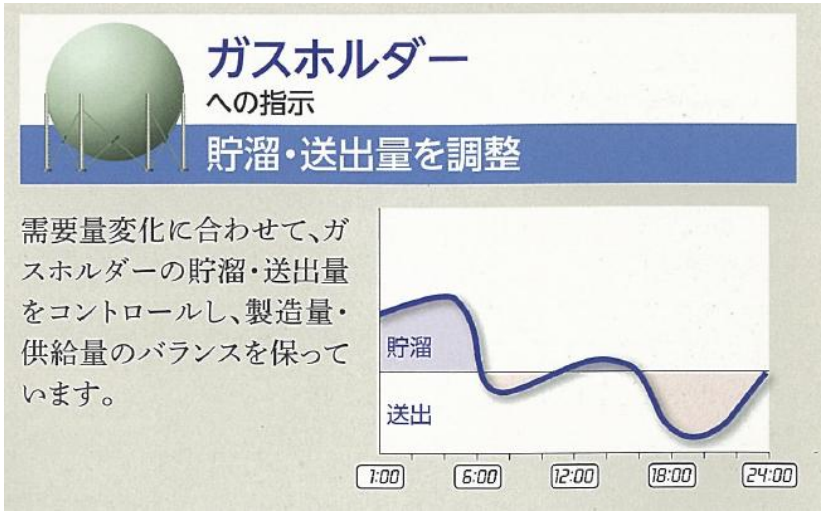
圧力の定義

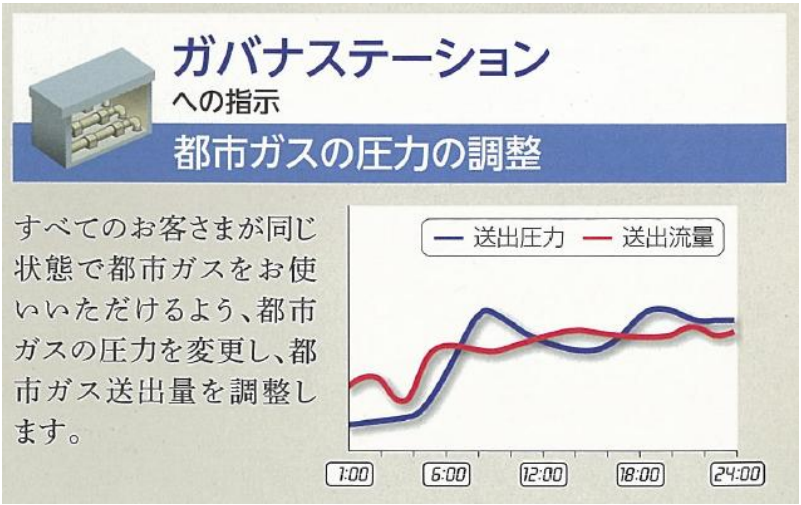
	ガス事業法施行規則	備　考	
高圧	1.0MPa以上		
中圧	0.1MPa以上1.0MPa未満	中圧A	0.3MPa以上1.0MPa未満
		中圧B	0.1MPa以上0.3MPa未満
低圧	0.1MPa未満	一般的には、「供給約款」に定められた圧力。それ以上の圧力を中間圧という。	

【供給系】遠隔監視・制御システムの役割例

■平常時：都市ガスの製造・供給状況を監視・制御
■地震時：地区ガバナ（圧力調整器）に遠隔の遮断指示
（遮断機能の有無は事業者により異なる）



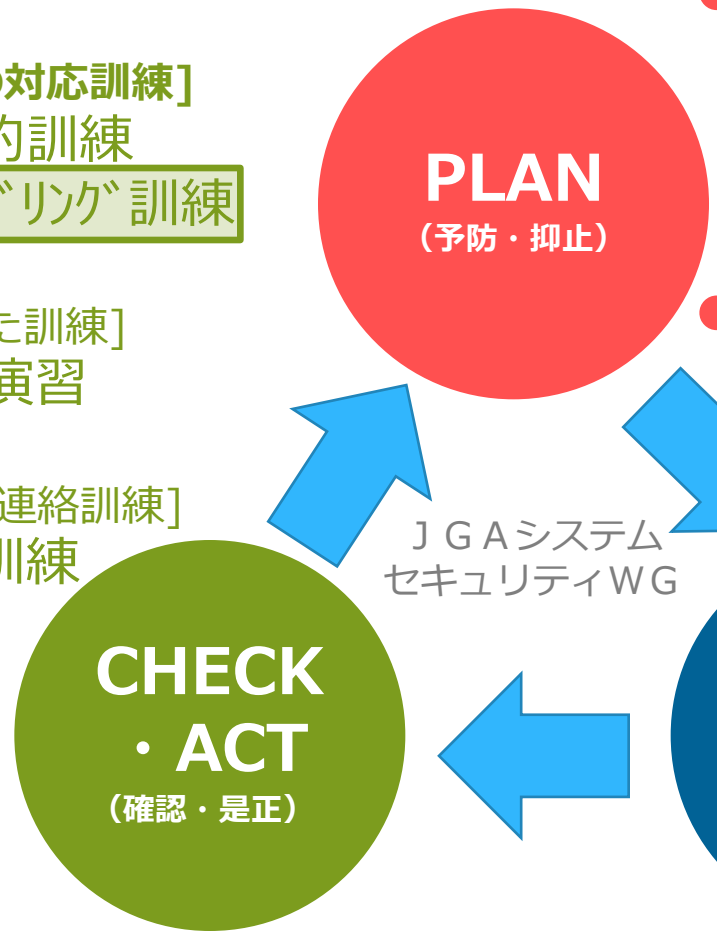




イラスト出典：東京ガス パンフレット「東京ガス 供給指令センター 都市ガスをみなさまの暮らしへ」

目次

日本ガス協会によるサイバーセキュリティー支援活動例



[サイバー攻撃発生時の対応訓練]
- NISC分野横断的訓練
- JGAｲﾝｼﾃﾞﾝﾄﾊﾝﾄﾞﾘﾝｸﾞ訓練

[模擬製造ﾌﾟﾗﾝﾄを用いた訓練]
- CSSCサイバー演習

[NISC-省庁-ｾﾌﾟﾀｰ間の連絡訓練]
- NISCセプター訓練

- 安全基準の整備と周知活動
  - 「製造・供給に関わる制御系ｼｽﾃﾑの情報ｾｷｭﾘﾃｨ対策ｶﾞｲﾄﾞﾗｲﾝ」
  - 「ｲﾝｼﾃﾞﾝﾄﾊﾝﾄﾞﾘﾝｸﾞﾏﾆｭｱﾙ作成ｶﾞｲﾄﾞ」
  - 「都市ガス事業者における情報ｾｷｭﾘﾃｨ対策のまとめ」
- 正会員アンケート調査

- 情報共有体制の構築
  - J-CSIP/C4TAP/JPCERT早期警戒情報

NISC　：内閣サイバーセキュリティーセンター
CSSC　：技術研究組合　制御システムセキュリティセンター
J-CSIP　：サイバー情報共有イニシアティブ　（運営：IPA）
C4TAP　：標的型攻撃に関する情報共有体制　（運営：NISC）
JPCERT：　（一社）　JPCERTコーディネーションセンター

目次

インシデントハンドリング訓練の実施計画

2013年度にガス分野に特化したシナリオを構築し、５ヵ年計画で大手事業者から段階的に訓練を実施。

（参加対象：情報系・製造系・供給系の担当者・管理者）

４年目となる2016年度で大手・準大手10社に対する訓練が一巡しこれまでの知見を活かしながら中規模事業者へ展開を予定している。

実施スケジュール

２０１３年度	２０１４年度	２０１５年度	２０１６年度	２０１７年度以降
訓練実施準備、 ＷＧ委員事業者にて訓練	準大手事業者への展開に向けた合同訓練	２０６事業者への展開を見据えた準大手事業者での訓練	２０６事業者への展開を見据えた準大手事業者での訓練	２０６事業者へ展開 ※前年度全国説明会等で希望調査を実施
訓練シナリオ作成 訓練実施（大手４社）	訓練実施 （準大手６社合同）	訓練実施 （準大手３社）	訓練実施 （準大手３社）	訓練実施 （希望事業者数社）

演習の目的とシナリオ概要

【目的】

- 国家レベルで大規模サイバー攻撃が発生した際の対応の判断や社内外への連絡を体験し、自社において**現状定められている判断基準や連絡経路の妥当性を考察**する
- 大規模サイバー攻撃発生時に、想定外の状況（例えば、対応人員や対応時間といったリソースが十分に確保できない状態）において、**優先して実施するべき事項を検討・ディスカッション**する

【シナリオ概要】

- 日本の政府機関、重要インフラ事業者を対象とした大規模サイバー攻撃が発生し、都市ガス大手事業者にも数多くの標的型メールが着弾し、またDDoS攻撃やウェブサイト改竄等が発生する
- その後、供給・生産の制御システムにも、サイバー攻撃を思わせる異常が生じる。そのような状況下で発生する事象にどのように対応するか、判断及び社内外への連絡等に焦点をおいた演習を実施するもの。

シナリオの背景設定

サイバー攻撃

■ 日本を対象としたサイバー攻撃
（**大衆迎合的**なサイバー攻撃）
- 歴史的な背景等から他国において反日感情が高まる毎年同じ時期に、サイバー攻撃が発生している（例：918攻撃）
- 社会情勢等の現実世界の事象に対して反日の動きがあると、連動してサイバー攻撃が発生している（例：#OpJapan, #OpKillingBay など）

特性：予測可能な攻撃であり、対策を取りやすい。主にインターネットに露出したシステムに対する攻撃

■ エネルギー事業者の情報窃盗を目的としたサイバー攻撃
（**標的型攻撃**による情報摂取）
- 世界的に、国家機密や先進国のメーカー、エネルギー事業者等の知的財産窃盗を目的としたサイバー攻撃が発生している

特性：見つからないように攻撃が実施され、侵入されていることに気づきにくい。内部の情報システム及びクローズドネットワークシステム（製造・供給システム等）に対する攻撃

社会情勢

■ 歴史認識の相違
- 日本と近隣国の間で、主に太平洋戦争に関連する歴史認識の相違が継続している

■ 日本の島嶼エリアを巡る動き
- 東シナ海の島嶼エリアにおいて、日本の商社が出資する資源開発の話題が、日本及び近隣国のニュース番組で報道された。それに伴い、近隣の島嶼部の領有権を主張する他国において、反日の主張が上がっている

■ X国内の動き
- 高等教育を受けたにも関わらず就職先のない若年層が、サイバー犯罪により金銭を得ている。他国のインフラに関して情報窃盗を行った上で入念な調査を行い、キル・スイッチを仕掛け、それを営利目的に活用しようと試みている攻撃者も存在する

状況付与カードの一例

●演習では計３時間で50枚弱の状況付与カードを付与する。
同じカードは必ずしも全てのチームには配布されず、情報量には偏りをもたせている。

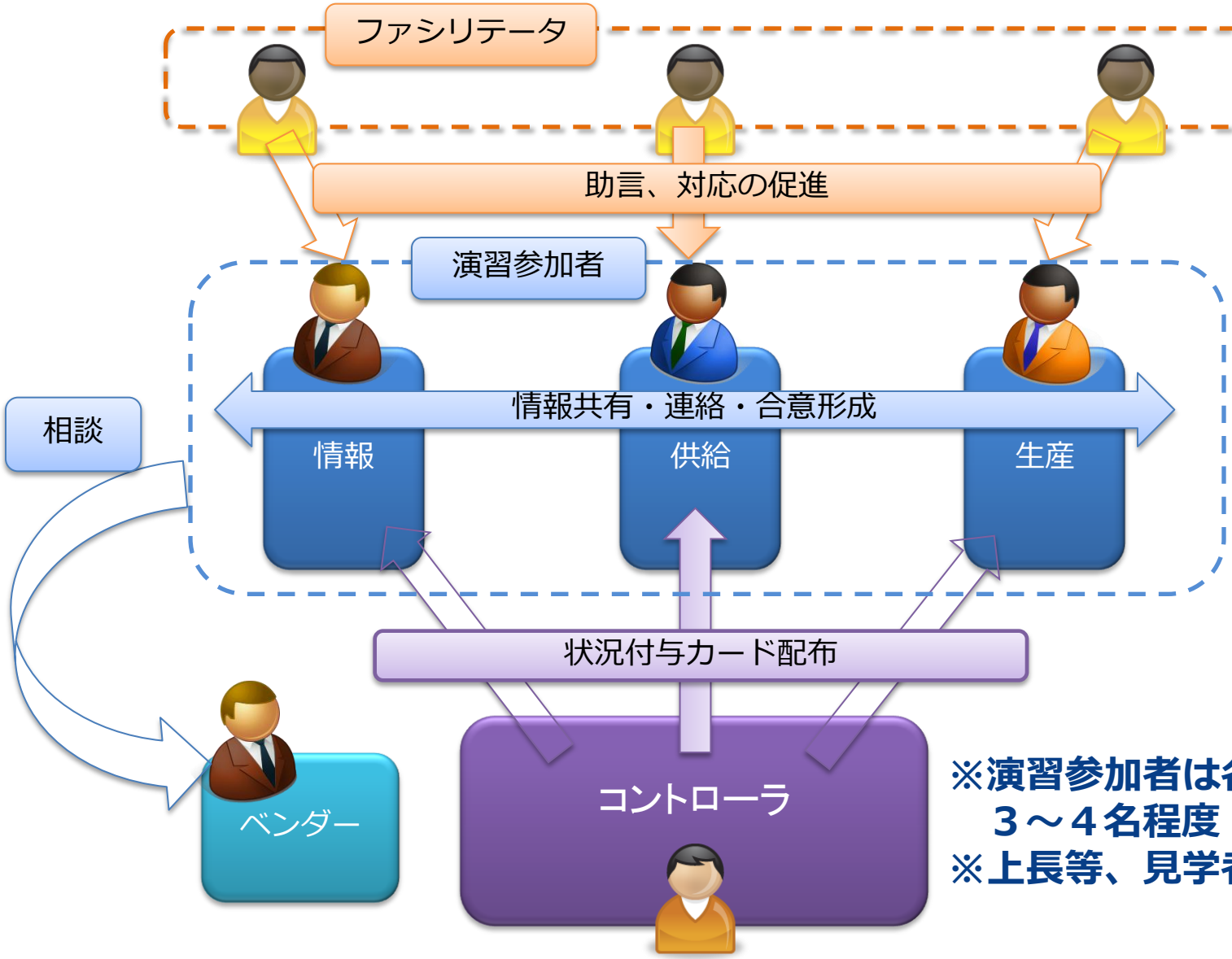
2015年度　ガス事業者　インシデントハンドリング訓練

事業者名	●●ガス株式会社		
番号	5011		
付与時間			
手段	カード		
想定時刻	2015/9/3 17:00		

送信元	●●ガス　製造オペレータ	送信先	●●ガス　製造システム担当
件名	[製造システム監視端末についての連絡] P工場（LNG基地）において監視端末1台の故障：電源が入らなくなったとの連絡		
概要	P工場（LNG基地）において監視端末1台の故障：電源が入らなくなったとの連絡 監視端末を操作していたところ、突然ブルースクリーンになり、システムが停止		

伝達内容
本日　4時　監視端末を操作していたところ、突然ブルースクリーンになり、システムが停止した。 電源のOFF/ONするも再起動がかからない状態。台数は1台。

演習の参加者関係図



※演習参加者は各チーム
　３～４名程度
※上長等、見学者も多数あり

運営側の役割設定

事業者

＜ファシリテーター（進行係）＞
・状況カードの受取り、班員へ記載内容を説明する。
・各班員に各社での対応方法を聞く。
・班としての対応決定を促す。
（正解を導き出すことが目的ではないため、意見が分かれた場合は、仮で班の対応を決める）
※班の対応は班員で話し合った上で決める
・班の対応について、①班員に行動を、②記録係に記録を指示する。
・タイムキーパー

WG委員

＜記録係＞
・状況毎に、班で対応したことを記録する
・最後のまとめ時に、班員の感想を記録する
・必要に応じ、ファシリテーターを補助する

外部

＜コントローラー＞
・全体（３つの班）の進捗を確認しながら状況カード配布

外部

＜ベンダー＞
・各班より調査依頼を受け付ける。また、必要に応じ、相談に乗る

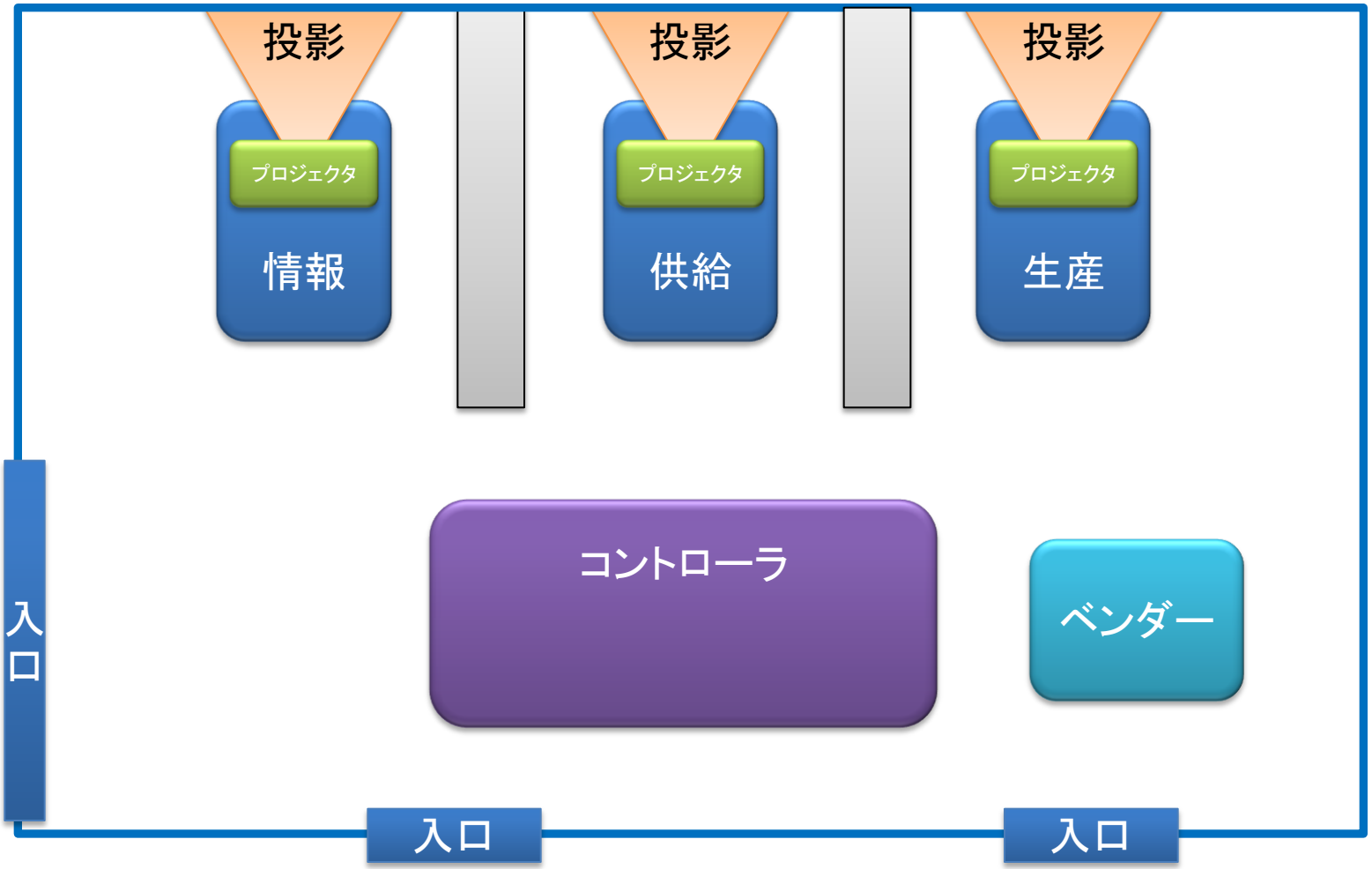
演習上の取決め

- **基本的なコミュニケーション**
  - 口頭（会場に制御機器の準備無し）
  - レポート用紙を使用したメモの授受
- **報告・連絡内容の記録**
  - 当局や社外、社内の別部門等、チーム外への報告・連絡内容は模造紙/ホワイトボードに記録を残す
- **付与表に記載される連絡先（メールアドレス/電話番号/URL）の扱い**
  - 参考情報として扱う（演習内での実際のアクセス不要）
- **日時の扱い**
  - 現実の日時でなく、状況付与表に記載されている「想定時間」を演習上の基準日時とする

演習当日のスケジュール

時間	内容	担当者
１０：００	挨拶	ＪＧＡ事務局
１０：０５	今年度の訓練の目的と位置づけ	ＪＧＡ事務局
１０：１０	セキュリティに関する講演	外部のセキュリティ関連事業者様
１０：３０	演習の説明	外部のセキュリティ関連事業者様
１１：００	演習（シナリオカード１～１８番）	班毎
１２：００	休憩	
１３：００	演習（シナリオカード１９番以降）	班毎
１５：００	休憩	
１５：１５	振り返り、まとめ	班毎
１５：４５	まとめの発表	班員１名ずつ（３班×１０分）
１６：１５	フィードバック	ＷＧ委員 外部のセキュリティ関連事業者様
１６：４５	質疑応答、フリーディスカッション	
１７：００	終了	

会場セッティングイメージ



演習風景

（参考）受講者の声・気付き（情報系①）

- 標的型攻撃の情報提供を受けるものの、日常から情報過多であり整理・線引きが難しい（実際の連携に至らないこともある）
- 何か深刻な事態発生後に動いた。制御の事後報告もあったが日常から情報連携（横・縦）が重要。ただし内容の見極めが難しい。
- 専門的な情報をかみ砕く能力が必要。自社でできなければ相談先を押さえておく必要がある。（緊急駆けつけサービスもある）
- “[Webサイトベンダー]お客さまからの●●ガスホームページ改ざんの調査報告”での課題認識
  - ・被害特定をどうするか？
  - ・改ざん・個人情報漏えい原因が不明
  - ・原因調査を進めるための証拠保全の必要性
  - ・関係方面への報告内容の取り決め
  - ・HP管理部門の了承とりつけとIT側の素早い情報提供（何を優先させるかの合意）
- （よかった点）国との情報提供ルートが明らかになった

（参考）受講者の声・気付き（情報系②）

- 各外部組織（社内外）への連絡・共有条件が不明確であり、都度判断となっていた
- 警察への被害届の提出の基準も明確になっているとよかった
- 生産、供給にどういう事象であれば連携する、しないをあらかじめ社内で決めておくべき
- 被害の規模に応じて社内の対策室などを立ち上げる必要がある、基準をどうするか、
- 社内でのエスカレーションフロー、基準を定めておく必要がある
- 各インシデントの状況を把握するのが困難だったので、フォーマットなどを整備しておくのがよい
- 製造、供給との行ったり来たりが多かったので、ファイルサーバや掲示板などの活用もあれば
- パソコン障害のベンダーへの対応依頼が漏れていた（実際にもれなく対応するためにはインシデント発生時の連絡すべき先の一覧などが必要）
- NISC、JPCERT、J-CSIP、JGAなど、報告先や連携先が多数ある状況は課題だと感じた
- 今後の個社でのインシデント訓練も必要

（参考）受講者の声・気付き（製造系①）

- 基準が担当者次第
- 生産部門の非常体制をとる基準を決めるのは難しい
  - ・情報部門のインシデントにも関わらず体制を組むか？
  - ・全社非常事態体制移行基準が不明確
  - ・現場の体制の変更基準（監視体制）決まっていない
- ＪＧＡでの取りまとめがあれば、いい。
  - ・関係ないと思われることも、情報共有には、・・・
  - ・いろいろな情報があると、受け取ったほうも困る。
  - ・どこで、線引きをすればいいかを、あらかじめ決めておくことは難しいと考えられる。
- 異常の確認方法が不明確。稼働の正常はわかるが、サイバー攻撃を受けてないかがわからない。
- システムバックアップの有無
  - ・定期点検時採取
  - ・バックアップ基準、マニュアルの有無
  - ・リストアーはベンダーに依頼

（参考）受講者の声・気付き（製造系②）

■ 情報連絡、体制

・事前に連絡体制が確立されていないと障害発生時に混乱する。

・誰がベンダーに連絡して、緊急連絡先を作成するのか。
（規定、連絡表の作成）

・状況をベンダーに的確に伝えることが大事。行動をおこせない。行動を起こすには　まずベンダーに連絡して安全であるか確認する。

■ 確認の方法

・周知の方法はメールでよいのか。感染しないか。周知は、まず情報分門に電話で連絡したらどうか。情報分野に連絡して、対応をいただく。

・誰が纏め、確認するのか。確認の方法は確立されているか。何のシステムに問題があるのか判断できない。（情報系か制御系か）

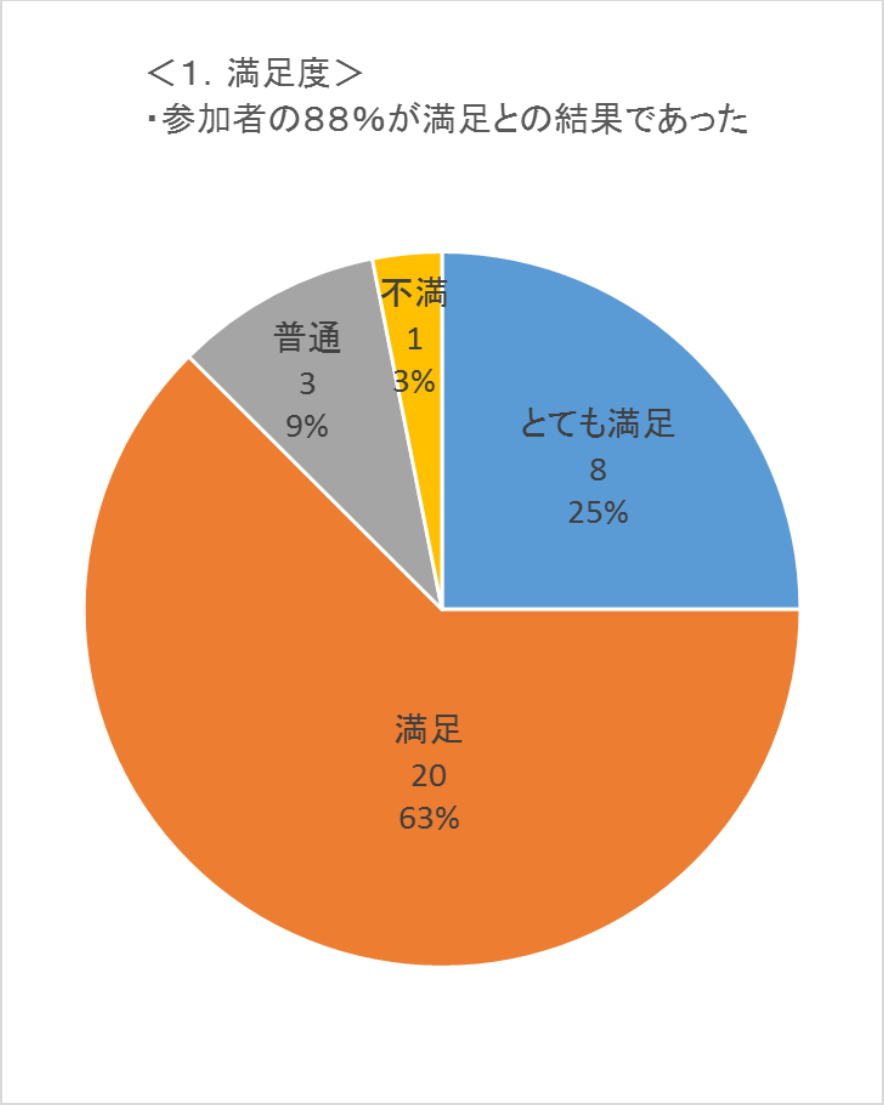
・バックアップシステムは安全か、制御に繋がっているが。納期がかかる部品は、予備品として保有する。

■ インシデント、ウィルス関連によるものか。製造に支障がないか。制御系を切り離してもよいかどうかベンダーに連絡。手順書を作成しておく。
（一次対応を明確化）

2015年度の参加者アンケートから

①全体的な満足度
→参加者の８８%が「満足」

②演習時間の長さ
→大多数が「適切」と回答

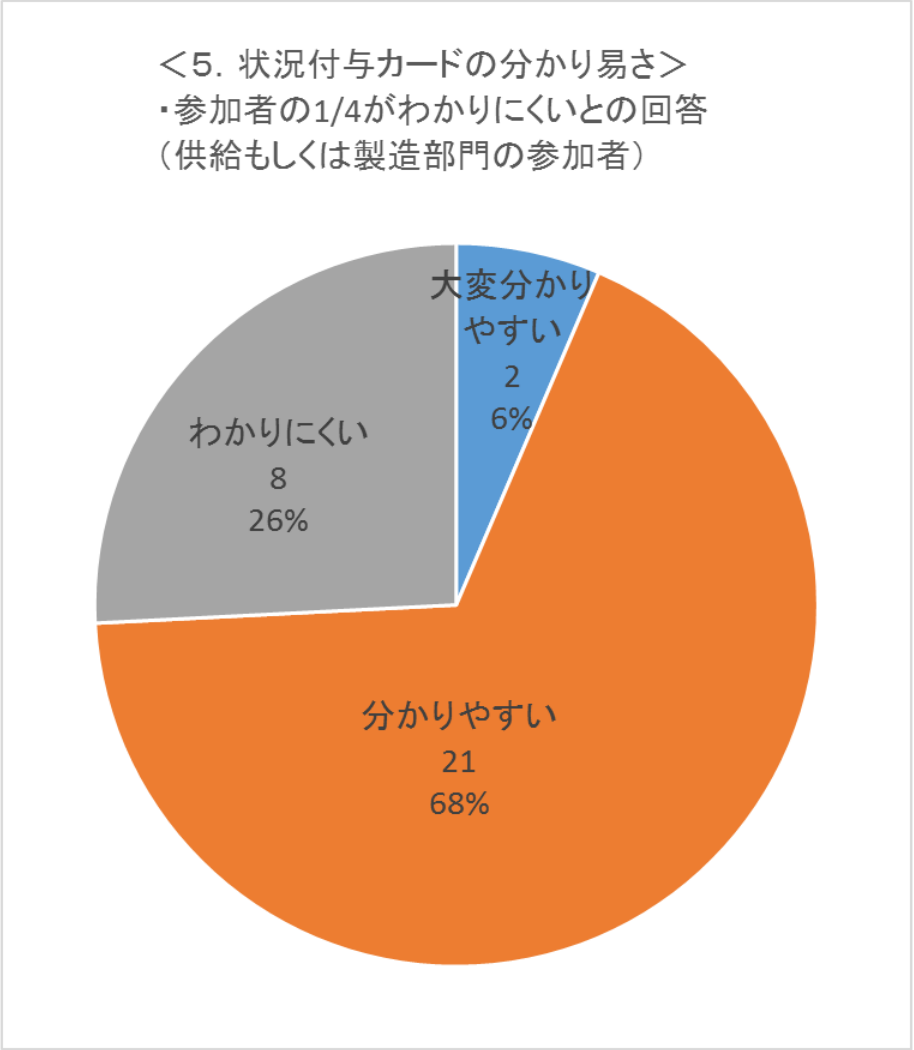


2015年度の参加者アンケートから

③状況付与カードの分かり易さ

→参加者の７４%が
「分かりやすい」
「大変分かりやすい」と回答

＊個社別のシナリオカスタマイズに対する評価が高かった
＊供給・製造班から専門用語やサイバー攻撃に関する基礎知識のインプットを要望する声が複数挙がった
＊自社システム概要について事前の相互理解が望ましい



2015年度の参加者アンケートから

④実際への活用

→大多数が「活用できそう」・「大いに活用できそう」と回答した一方で「実際のインシデント対応には使えない」「実際にはマネージャの指揮の下、行動する」等の意見も挙がった

＊演習時のリーダーを上長と仮定するのも一案

⑤意識の変化

→大多数が「変化した」と回答

＊社内横断的な訓練であることについて評価が高かった。一方で「制御システムはクローズなのでサイバー攻撃は考えにくい」という意見も挙がった。制御システムのウィークポイントを当日の講演会で伝えることを検討

2015年度の参加者アンケートから

⑥演習説明者の分かりやすさ

→大多数が「分かりやすい」「とても分かりやすい」と回答。
一方で「用語などサイバー関連の知識が無い」「どのような立場で臨めばよいのか分からなかった」等の意見も出た。
＊事前説明会でサイバー攻撃の基礎的なレクを行うことを検討

⑦ファシリテータの助言

→全ての回答が「有意義」「大いに有意義」の何れかであった
＊訓練経験者によるファシリテーションが有用であることを再認識

目次

終わりに

周知の通り、情報セキュリティを確保するためには多面的な（技術的／物理的／人的）対策が必要となる。今回ご紹介させて頂いたインシデントハンドリング訓練はその内のごく一部の、人的対策に焦点をあてたものである。ガス業界ではサイバーインシデント対策も保安活動の一部と捉えており、非常時への備えとして防災訓練同様、人的側面における実践的な訓練が不可欠と考えている。
今後も、より一層セキュリティ対策を強化するために、JPCERT/CC様を始めとする関係各位に、引続きご支援・ご助言を賜りたい。また、本日のご紹介が皆さまのご検討の一助になれば幸いである。

ご清聴ありがとうございました