都市ガス業界における制御系システムのセキュリティ対策強化のための活動紹介

一般社団法人　日本ガス協会
技術部　保安技術G
北浦　史郎

■都市ガス事業者について

都市ガス事業者　⇒208社／日本全国

大手ガス事業者：　4社

東京・大阪
東邦（名古屋）
西部（福岡）

準大手ガス事業者：　6社

北海道・仙台（福島）
京葉（千葉）・北陸（新潟）
静岡・広島

■都市ガス事業者について

中小ガス事業者

⇒198社／日本全国

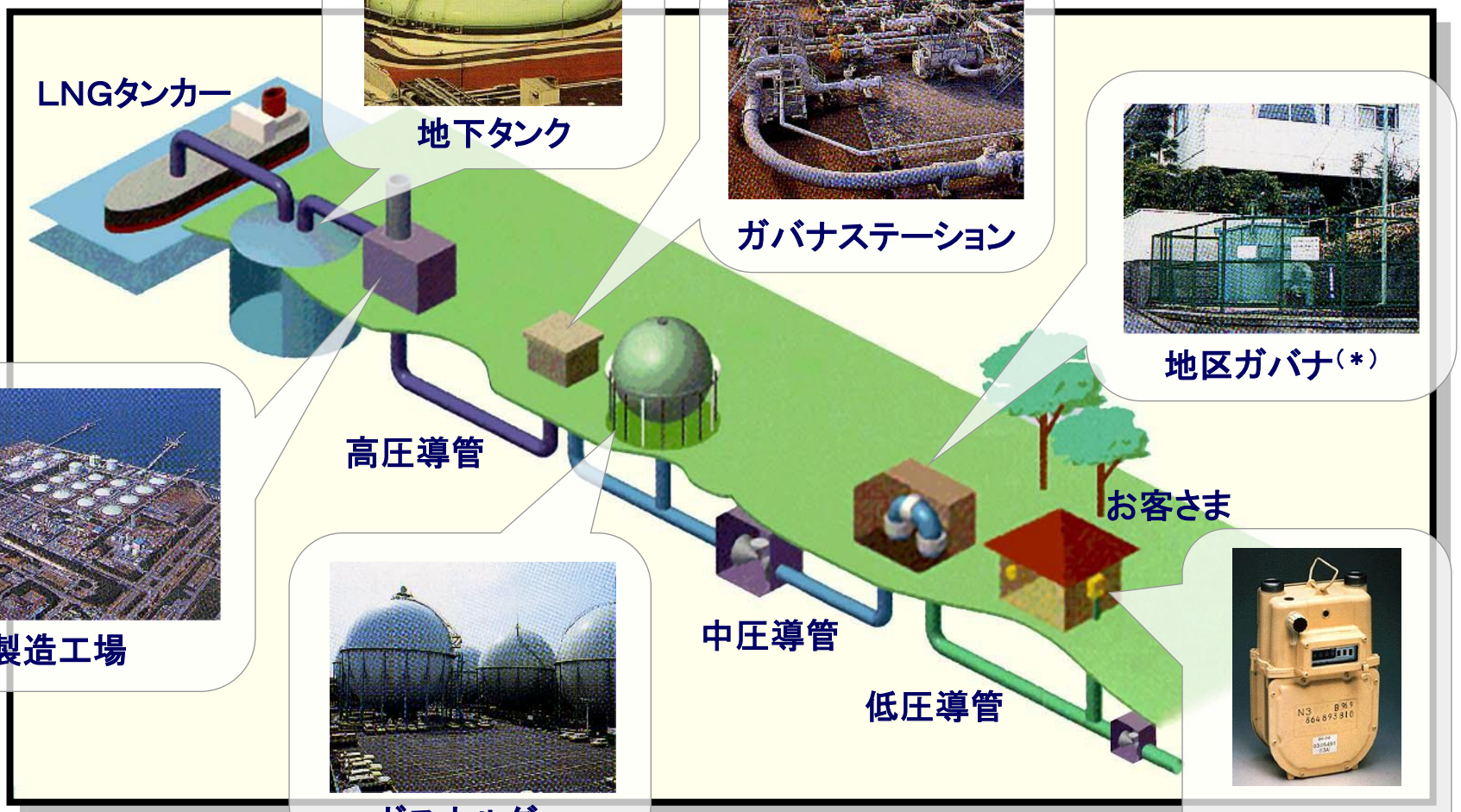
・需要家数・社員数は少ない

・公営（市営・町営）も多い

■都市ガス事業者の制御系システムとは。。。。

都市ガス事業者のインフラ概念図

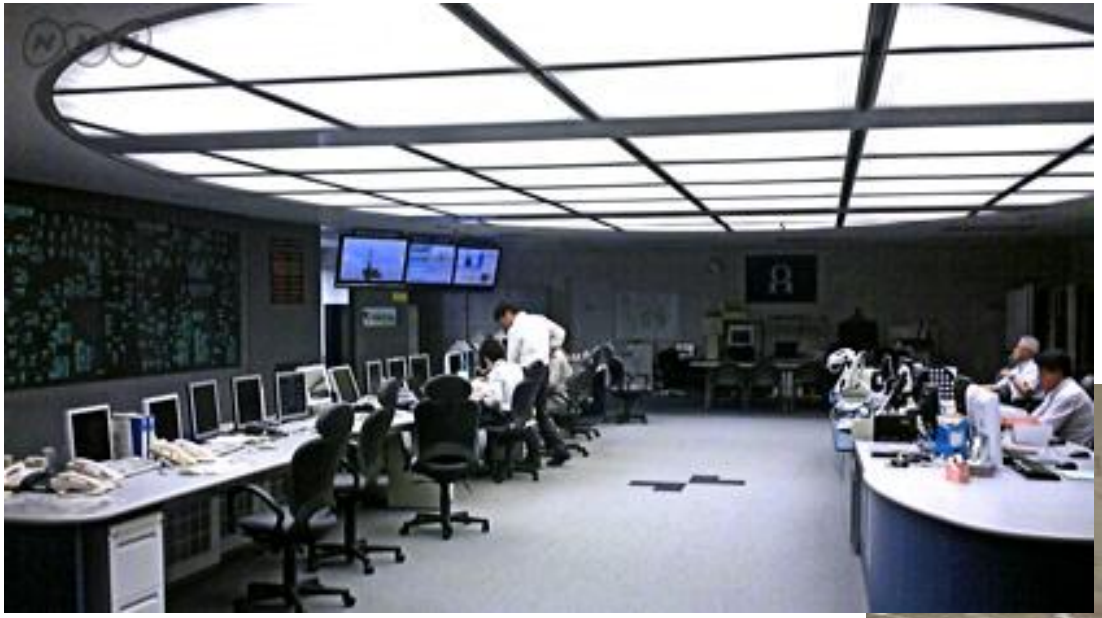
（＊）ガバナ：圧力調整器



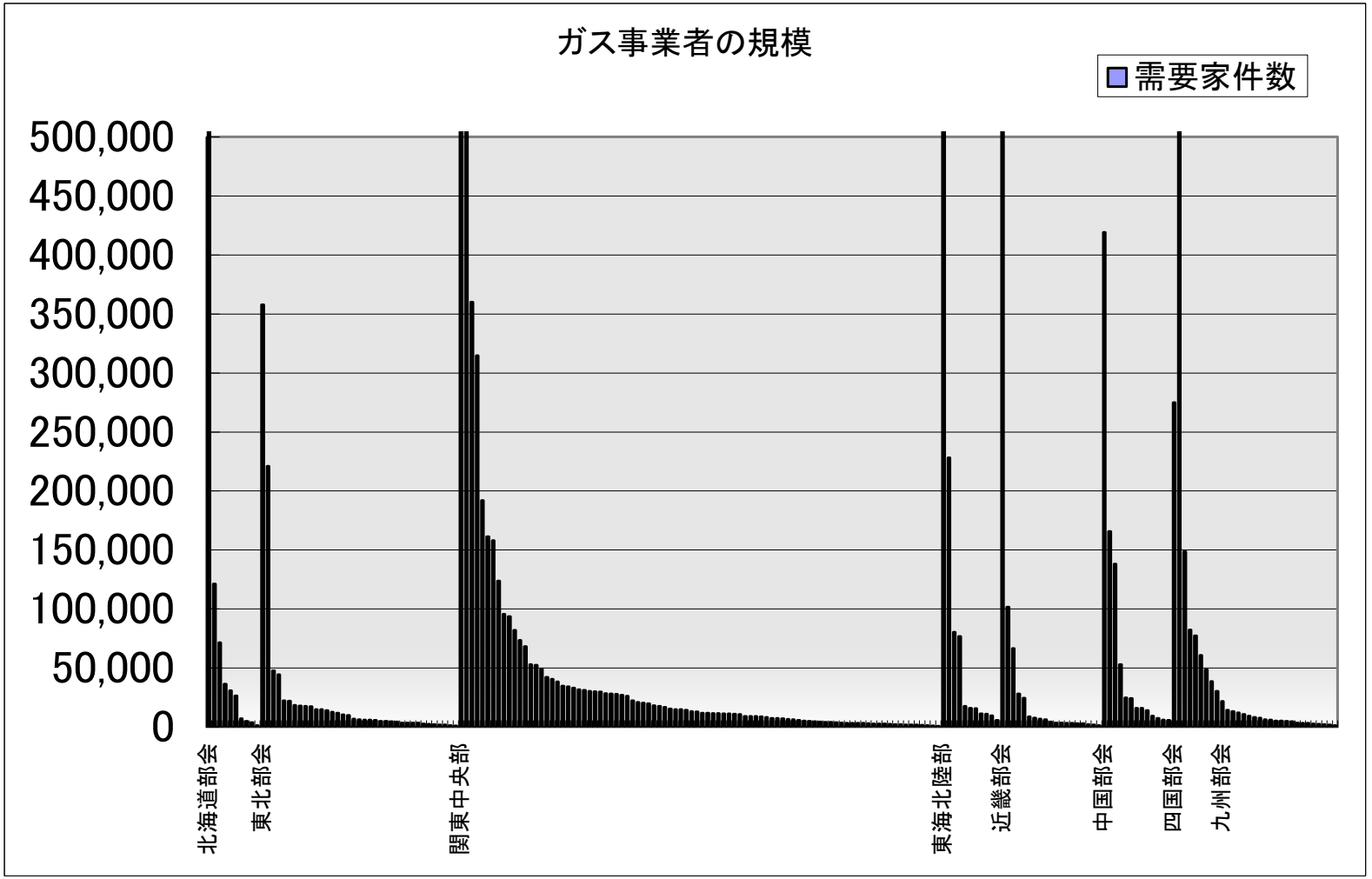
■例えば東京ガスでは・・・

①需要家数:
　都市ガス:1000万件
②社員数:　7000人

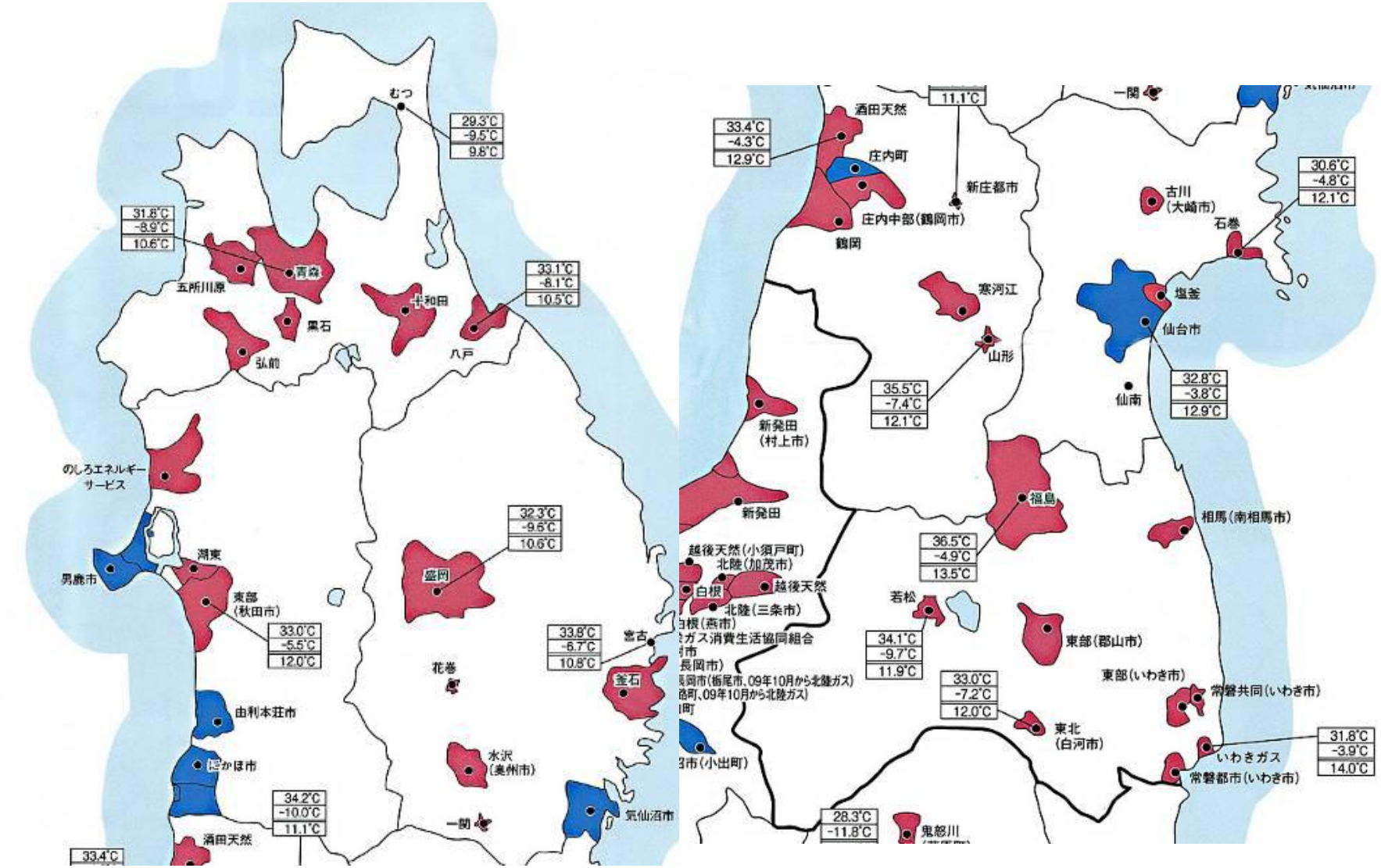
■例えば東京ガスでは・・・



■都市ガス事業者について



■都市ガス事業者について



■　制御系システムのセキュリティ対策への活動と、その課題。。。

■日本ガス協会でのWG活動等

「サイバーテロ対策検討WG」

２００６年度から大手ガス事業者で組織活動

・NISC発足への対応

▪IPA「重要インフラの制御システムセキュリティとITサービス継続に関する調査報告書」への対応

⇒　都市ガス事業者業界でも***制御系システムを対象としたセキュリティ対策の必要性***を認識

⇒　大手ガス事業者が中心となりの
制御系システムセキュリティーガイドライン策定

今年度は、中小ガス事業者を含めた都市ガス業界全体でのセキュリティー支援を目標として啓発活動を展開中！

■国、関係団体への対応

A.　NISC（内閣官房情報セキュリティセンター）
「ガスセプター」として、総会・幹事会、WGに参加

B.　METI（経済産業省）
制御システムセキュリティ検討TF　委員参加
「普及啓発WG」 委員参加
（経営者向け啓発策検討）

C.　JEMIMA・JPCERT
制御系システム　診断ツール（SSAT）の
ユーザー現場向けの検討

■都市ガス事業者の制御系システムの課題

① セキュリティー重要性の認識度が、各社で大きく異なる。

② セキュリティーの品質、費用投資も各社判断で大きく異なる。

■都市ガス事業者の制御系システムの課題

③ 各社の制御系システムのセキュリティーレベルアップ
⇒各社の機密事項であるため
情報共有化がむづかしい
⇒業界の組織として、本部分では力量不足

④ 制御系システムのセキュリティー対策のむづかしさ
（事務処理情報系システムと異なる特徴）

⑤ 模範回答（100点）のセキュリティーレベルが
定義できない

■　今年度の活動状況をご紹介します！

■日本ガス協会でのWG活動（業界としてできること）

■今年度活動

① 制御系システムセキュリティーガイドライン策定
診断ツール作成
（ガス版SSATの作成）

②セキュリティー事例集作成
（現場向けのセキュリティ教育の実施）

⇒ これらをもとに、

都市ガス事業者啓蒙活動中！

■日本ガス協会でのWG活動（業界としてできること）

■以降は、今年度「地方説明会」で使用しているPPTです。

読売新聞 （平成24年1月22日朝刊 1面掲載内容）

車や化学工場の製造ラインを管理する制御システムがコンピューターウイルスに感染し、操業停止に追い込まれるなどの深刻な被害が少なくとも国内で10件発生（METI調査）

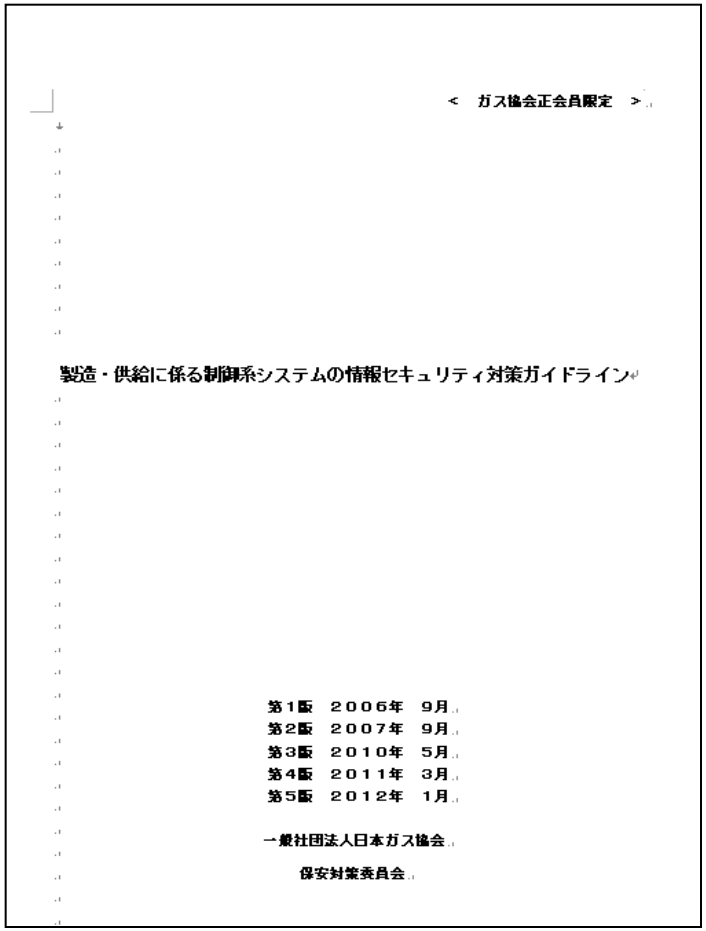
制御システムを狙うサイバー攻撃は海外で増加しており、経済産業省は来春までに安全性を審査する機関などを新設する方針を決めた。

国内でも制御系システムに被害が発生していた！

⇒METIが審査認証の二機関新設へ

- 安全審査認証機関
- 緊急時対処機関

「制御系システムの情報セキュリティーガイドライン」
⇒ガイドライン配布説明と
チェックツールの実施をお願いします！



＜　ガス協会正会員限定　＞

製造・供給に係る制御系システムの情報セキュリティ対策ガイドライン

第1版　2006年　9月
第2版　2007年　9月
第3版　2010年　5月
第4版　2011年　3月
第5版　2012年　1月

一般社団法人日本ガス協会

保安対策委員会

本日の説明会でお渡ししたものについては、**JGAのHPからダウンロード**利用できます（近日中に通知予定）

- 「製造・供給に係る制御系システムの情報セキュリティ対策ガイドライン」は、**事業者代表の１０社向けに、「内規」の策定・改定を支援するために作成したガイドライン**です。

- １０社以外のガス事業者においても、本ガイドラインを参考とし、**制御系システムの情報セキュリティの向上を図る**ことをお奨めします。

「制御系システムのセキュリティチェック」のお願い

⇒　チェックの実施と実施結果をＪＧＡへメール送付してください。

製造・供給の制御系システムにおける情報セキュリティーチェックについて（平成23年度分）

実施日（チェック日）＿＿＿＿＿＿＿＿

会社名＿＿＿＿＿＿＿＿

事所＿＿＿＿＿＿＿＿

実施担当者の氏名＿＿＿＿＿＿＿＿

電子メール＿＿＿＿＿＿＿＿

電話番号＿＿＿＿＿＿＿＿

【注意】
回答は、別紙回等用紙に記載し、提出してください。

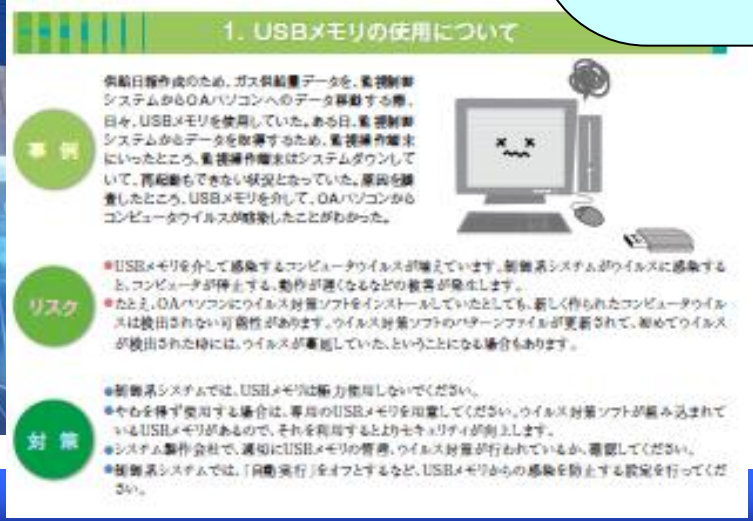
番号	チェックポイント	チェック質問事項	回答	【参考】ガイドライン記載箇所	
1. 情報セキュリティーの規定化					
1	「製造・供給に係る制御系システムの情報セキュリティ対策ガイドライン」は、ガス事業者代表の10社が、「内規」の策定・改定を支援するために作成したガイドラインです。 現在、ガス製造・安定供給の継続及び維持は、情報システムへの依存度が高くなっており、事業者自らが定める「内規」等で、情報セキュリティ対策の項目および水準が明文化することが重要です。 策定した「内規」に沿った具体策（IT障害の未然防止策、拡大防止策、自主施策、体制整備等）を経営レベルで推進し、実効性のある情報セキュリティ対策を検討し、確実に実現し、PDCAの好循環サイクルを確立することが望まれます。 10社以外のガス事業者においても、本ガイドラインをお考えとし、制御系システムの情報セキュリティの向上を図ることをお奨めします。	情報セキュリティ対策の項目および水準を明文化するための「内規」等を定めていますか？	①はい ②いいえ	1. ガイドライン策定の目的	8
2		情報セキュリティを取り巻く環境の変化に応じて、適宜、内規の見直しを行っていますか？	①はい【前回見直し時 ②いいえ		
3		セキュリティ水準を高められるよう、PDCAのサイクルを確立していますか？ ※参考 PDCA（Plan－Do－Check－Act の略）です。品質改善や環境マネジメントでよく知られた手法で、次のステップを繰り返します。 1.Plan：問題を整理し、目標を立て、その目標を達成するための計画を立てます。 2.Do：目標と計画をもとに、実際の業務を行います。 3.Check：実施した業務が計画通り行われて、当初の目標を達成しているかを確認し、評価します。 4.Act：評価結果をもとに、業務の改善を行います。	①はい ②い		
4		経営層も含め、内規に定めた内容が実施されるよう会社として取り組んでいますか？	①はい ②いいえ		
2. 組織・体制及び資源の対策					
5	IT障害発生時における当該事業者内および関係者間での連絡・連携体制を定めておくことが必要です。 また、IT障害の発生想定訓練および情報伝達訓練により、対処方法を適宜確認しておくことが必要です。	情報セキュリティ対策を実施する社内組織は責任と権限が業務分掌で明示されていますか？	①はい ②いいえ		
6		経営層は、リスクマネージメントの一つとして、IT障害発生時のリスクを認識し、組み込んでいますか？ ※参考 IT障害：制御系システムが、設計時の期待どおりの機能を発揮せず、ガスの供給支障に至る可能性があると考えられるもの。	①はい ②いいえ		

チェックツールの実施は、近日中に通知にて依頼します。

頂いた結果は、**業界として傾向を分析**して来年度の施策検討に繋げます！

「制御系システムの情報セキュリティーリスク事例集」

⇒　システム利用者へのセキュリティ教育をお願いします！



本日の説明会でお渡ししたものについては、**JGAのHPからダウンロード**利用できます（近日中に通知予定）

正会員限定

ウィズガス

一般社団法人
日本ガス協会

制御系システムの情報セキュリティリスク事例集

事例５

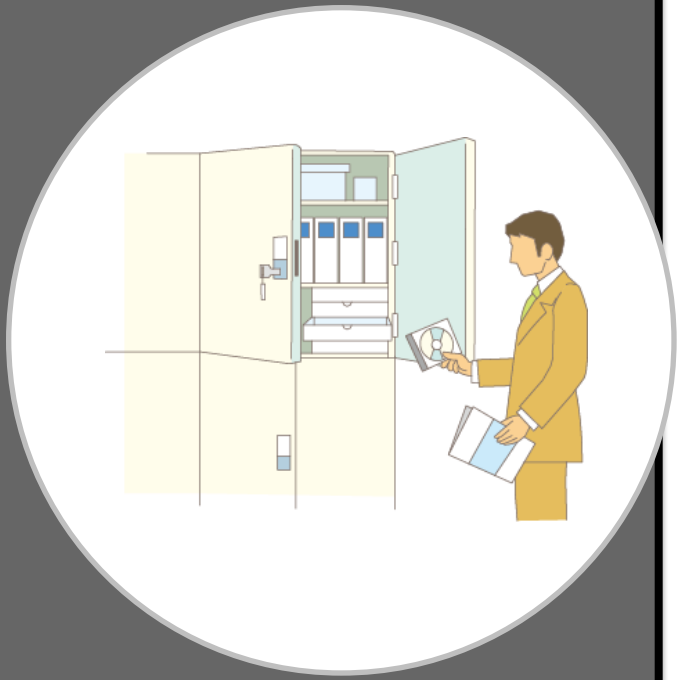
事故発生時の対応マニュアルや連携体制の整備

事例５

事故発生時の対応マニュアルや連携体制の整備

ある日、制御監視システムのシステムサーバが不調となり、オペレーターがシステム納入会社に連絡したが、同社は、経営不振で倒産していた。

別のシステムベンダーに、緊急対応を依頼したが、システムの説明資料がないこと、バックアップデータが最新であるか不明であること、対応する部品は製造停止で既にないなどの状況でシステム復旧に長期間を要する事態となった。



事例５

事故発生時の対応マニュアルや連携体制の整備

リスク

- 制御系システムにＩＴ障害が発生すると、全端末の初期化・再設定、工場の操業停止など想像以上の影響を受ける場合があります。
- 保守ベンダーとの緊急連絡対応が遅れたり、対応に必要なマニュアル、最新のバックアップがない場合、早期復旧ができなかったり、被害が拡大する危険性があります。

対　策

- 社内緊急対応マニュアルの準備や保守ベンダーとの非常時の連携体制を構築しましょう。
- システムのバックアップは、定期的に最新のものを用意しておきましょう。

■　最後に、次年度の計画として。。。。

■次年度の活動として

■サイバーテロ対策訓練の実施検討

■都市ガス事業者経営者に向けた啓発活動

⇒　今年度のガス版SSATでの
　　実施結果データの分析報告

⇒　制御系システムのセキュリティー対策強化のお願い

おわり

ご清聴ありがとうございました。