社団法人 日本電気計測器工業会
Japan Electric Measuring Instruments Manufacturers' Association

# 計測展2011 TOKYO JEMIMA委員会セミナー
# 生産制御システムセキュリティの技術動向

2011.11.18

PA・FA計測制御委員会
セキュリティ調査・研究WG

# WGのご紹介 (1)

- **目的**
  製造業分野におけるセキュリティ標準化動向、技術等の調査・研究活動を進め、会員企業、ユーザにフィードバックする。

- **設立**
  2005年4月

- **メンバ**
  横河電機㈱ 、㈱山武、㈱東芝、富士電機 ㈱
  ㈱日立ハイテクコントロールシステムズ、㈱日立製作所

- **活動実績**
  1. ISA SP99　TR2を利用したセキュリティ対策の実践
  2. NIST SPP-ICS ver1.0を利用したセキュリティ要件の分析および役割明確化
  3. セキュリティ標準規格の調査
  4. ＣＰＮＩグッドプラクティスの検討
  5. セキュリティ評価ツールの調査

# WGのご紹介 (2)

## ・外部団体との協力関係

- SICE (計測・制御ネットワーク部会)
- JEITA (制御・エネルギー管理専門委員会)
- JPCERT/CC
- IPA (独立行政法人情報処理推進機構)
- IEC/TC65/WG10 国内委員会

## ・広報活動

- 計測展委員会セミナー
- JPCERT/CC
  制御システムセキュリティカンファレンス
- 計装制御技術会議
- SICE Annual Conference

# 本日の内容

PART1
生産制御システムセキュリティの現状

PART2
セキュリティ評価ツールSSATのご紹介

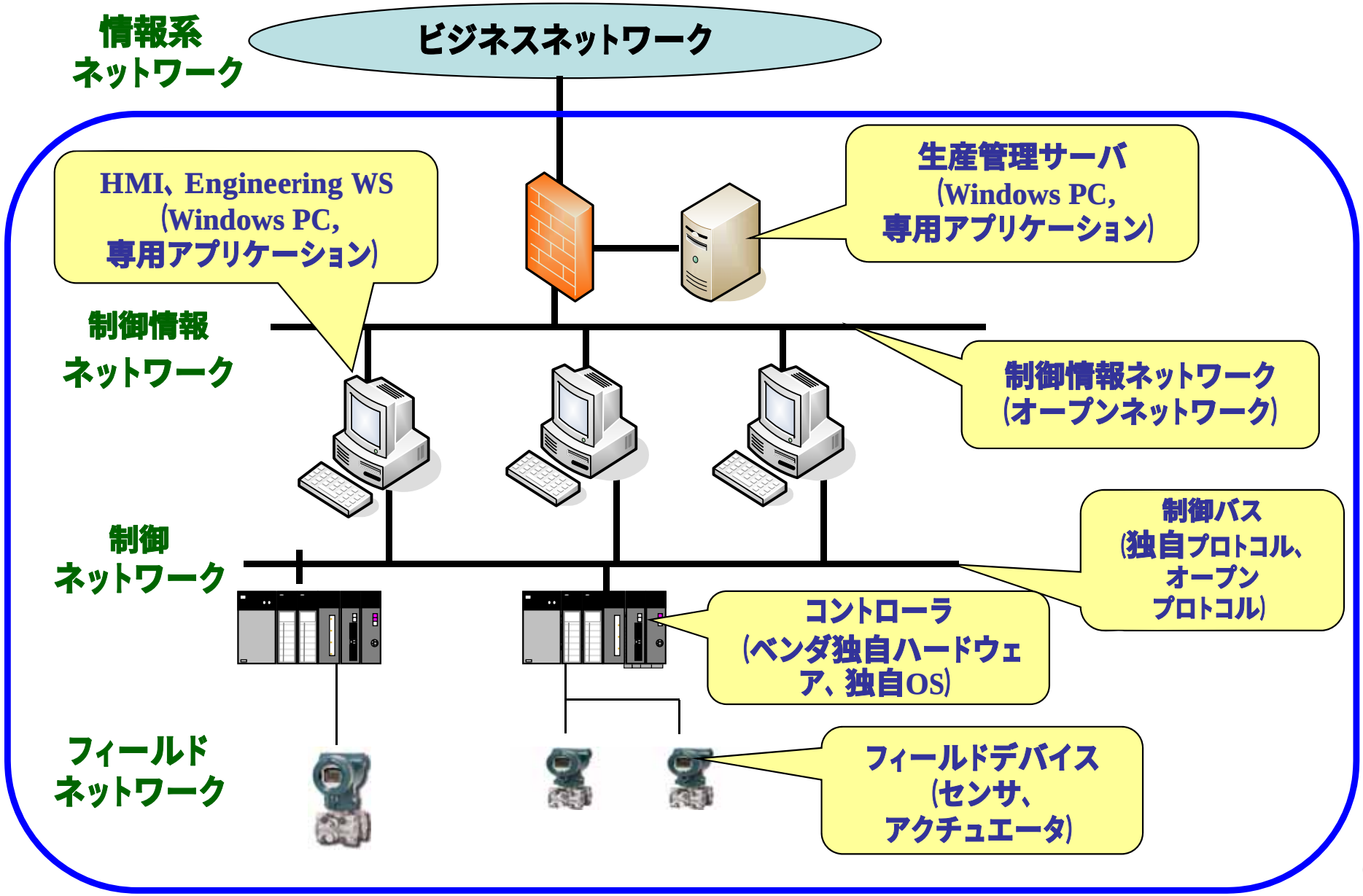
PART3
セキュリティ評価ツールSSATの改良

JEMIMA

PART 1

# 生産制御システム セキュリティの現状

# 生産制御システム概要



# 生産制御システムセキュリティの背景

**制御システムにおいて情報連携の重要性が高まっている**

見える化（経営，生産管理，操業）

＋

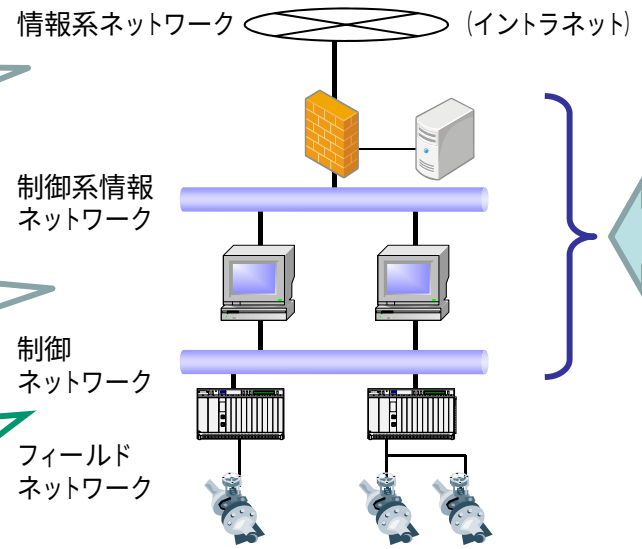
技術の共通化の進展

- オープン技術
- マルチベンダ

ロット別コスト
環境対策

中間在庫
トレーサビリティ
生産性向上

時間短縮
作業正確性向上




- ハードウェア（x86, LAN用LSI）
- OS（Windows, Linux）
- ネットワーク（Ethernet, 無線LAN）
- プロトコル（OPC, 産業用Ethernet）
- アプリケーション（ﾃﾞｰﾀﾍﾞｰｽ, Web）

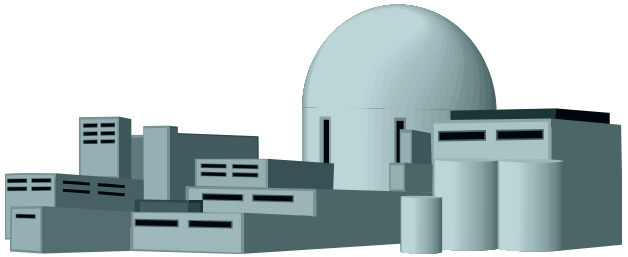
OPC：OLE for Process Control

外部からの干渉を受けやすくなる

⇒被害防止のための対策が必要になる

# 現実化する脅威

- **Stuxnet事件：「新しいタイプの攻撃」の出現**
  - **概要**
    - 2010年7月に発見された**新種のウイルス**
    - 解析の結果、**特定のPLCシステムを標的としていること**が判明
    - 2010年11月にイランのウラン濃縮施設の遠心分離機が感染
      **約8400台の遠心分離機が停止**
  - **特徴**
    - **特定のプラントを狙った「標的攻撃」**
      → 「ITシステム攻撃のとばっちり」ばかりではなくなってきた
    - **複数の未対策脆弱性を悪用した「ゼロデイアタック」**
      → ウイルス対策ソフト等では対処困難
    - **制御システムに関する高度な知識が悪用されている**
      → 関係者に対する性善説が覆された
    - **不正に入手された正規のデジタル署名が付加されている**
      → デジタル署名は安全の担保にならなかった
    - **USBメモリを介して感染した可能性がある**
      → ファイアウォールなどを用いた境界防衛では阻止できなかった



**→ より一層の警戒･対策が必要**

# 情報セキュリティ確保の３要件

- 第三者の悪意のある行為に対するシステムの
  セキュリティ確保には C.I.A.の３つの要件があります

**機密性：C onfidentiality**

情報を不適切な人間には決して見せないようにすること

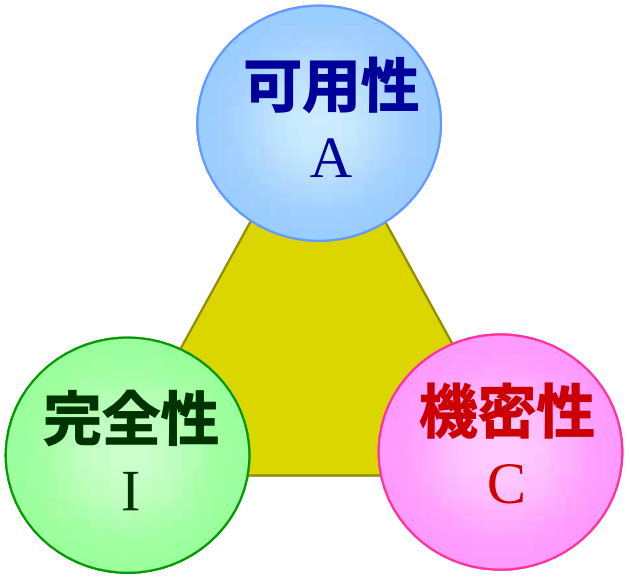
**完全性：I ntegrity**

情報が完全な形で保たれ、不正によって改ざんされたり
破壊されないこと

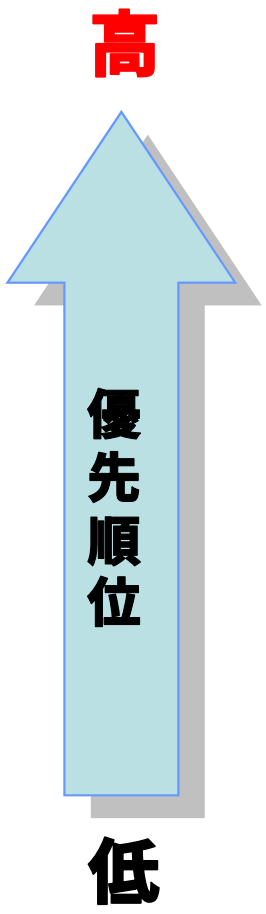
**可用性：A vailability**

情報や資源がいつでも利用できること

**ITシステムと生産制御システムにおいては
3条件の保護する優先度が異なる**



# ITシステムと生産制御システムの違い (1)




## ITシステム

- C：機密性
- I：完全性
- A：可用性

●情報の保護が優先

## 生産制御システム

- A：可用性
- I：完全性
- C：機密性

●生産の継続が優先

# ITシステムと生産制御システムの違い (2)

| | 内　容 | 生産制御 シ ス テ ム | IT　シ ス テ ム |
|---|---|---|---|
| 1 | 性能要件 | 応答性能が重要。遅延は重大問題 | 応答性能よりもスループットが要求される |
| 2 | 可用性 | システムの再起動は許されない場合が多い | 運用上必要であればシステムの再起動が許容 |
| 3 | 即時性 | 緊急処置に対する人間の操作を妨げてはならない | 即時性を要求する緊急処置は少ない |
| 4 | ライフタイム | 15-20年と長い | システム、機器のライフタイムは3-5年が中心 |
| 5 | 守るべき資産 | 制御に直接関係する端末装置（プロセス制御装置のようなフィールド装置）を第一に保護 | IT資産および情報を第一に保護している |
| 6 | システム運用 | 独自OSが多く、アップデートの自動化の仕組みが出来ていない | 汎用OSを用いて設計されており、アップデートは自動化された仕組を利用でき容易である |
| 7 | リソース（メモリやディスク容量） | 最小メモリやその他リソースで生産プロセスを支援するように設計されており、セキュリティ機能もその範囲内で追加されている | セキュリティ対策などのために、システムは十分なリソースを持っていることが一般的である |
| 8 | 通信 | 標準プロトコルの他に専用プロトコル、通信設備が含まれるため、ネットワークは複雑となり、専門の技術者が必要 | ワイヤレスも含め、標準的な通信プロトコルが使用される |
| 9 | サポート | サービスサポートは通常1ベンダーによる。 | 機器メーカーによる様々な支援体制がある |
| 10 | 危機管理 | 人、環境の安全性が第一、次がプロセスの保護である | データ機密性及び完全性を第一に管理する |

# 生産制御システムセキュリティの課題

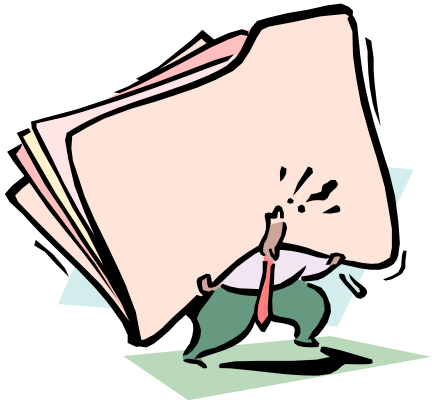
出典：IPA「重要インフラの制御システムセキュリティとITサービス継続」

- **課題1：オープン化に伴う脆弱性リスクの混入**
  - 汎用製品，標準ネットワークの採用
    ⇒ 脆弱性の課題も引き継ぐ（例：USBメモリ，ネットワーク侵入）
- **課題2：長期利用に伴うセキュリティ対策技術の陳腐化**
  - １０～２０年の間に，対策が更新されない可能性あり
- **課題3：可用性重視に伴うセキュリティ機能の絞り込み**
  - ウイルス検査プログラム負荷のシステムに対する影響
  - セキュリティパッチ導入によるシステム稼働率への影響

# 課題対策の現状

**生産制御システムに対するセキュリティ対策：**

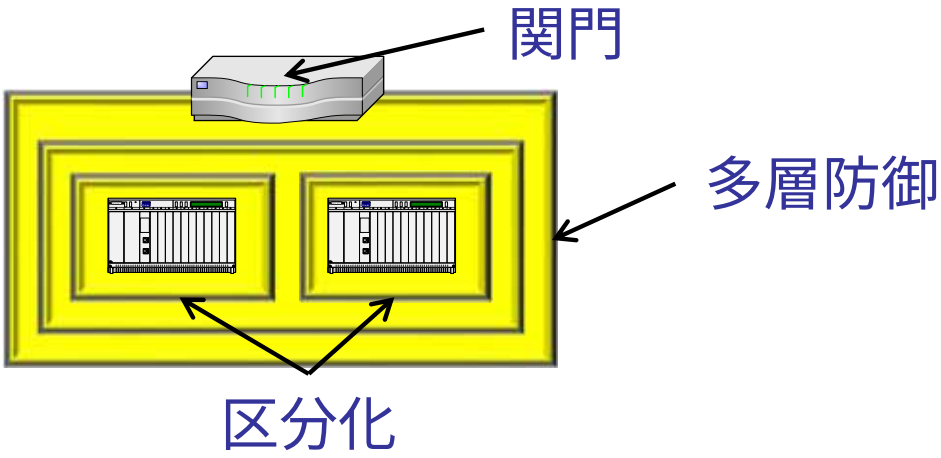
対策が必要であることは判っているが、何をどうすれば良いか判断がつけにくい。



**基本戦略：**

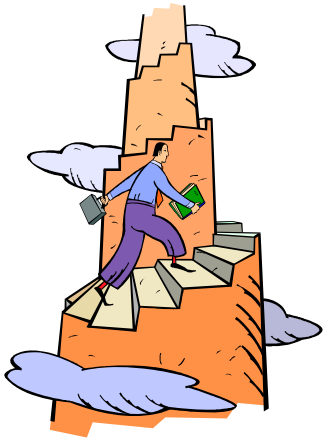
・独立した複雑なセキュリティシステムより，シンプルな対策を「重ねる」

・シンプル/安易なセキュリティはない
繰り返して見直す，**PDCAサイクルを回すこと**が重要



# ＰＤＣＡサイクルの具体策

| | 制御系セキュリティに使えるツール･規格 例 |
|---|---|
| Plan | ISA-99<br>NIST SP800-53/82<br>**各種**Good Practice<br>**セキュリティ評価ツール** |
| Do | ISA-99<br>**脆弱性スキャナ**<br>**侵入検知システム** (IDS) |
| Check | **ログ監査**<br>**侵入検知システム** (IDS)<br>**脆弱性情報** |
| Act | ISA-99<br>NIST SP800-53/82<br>**各種**Good Practice |

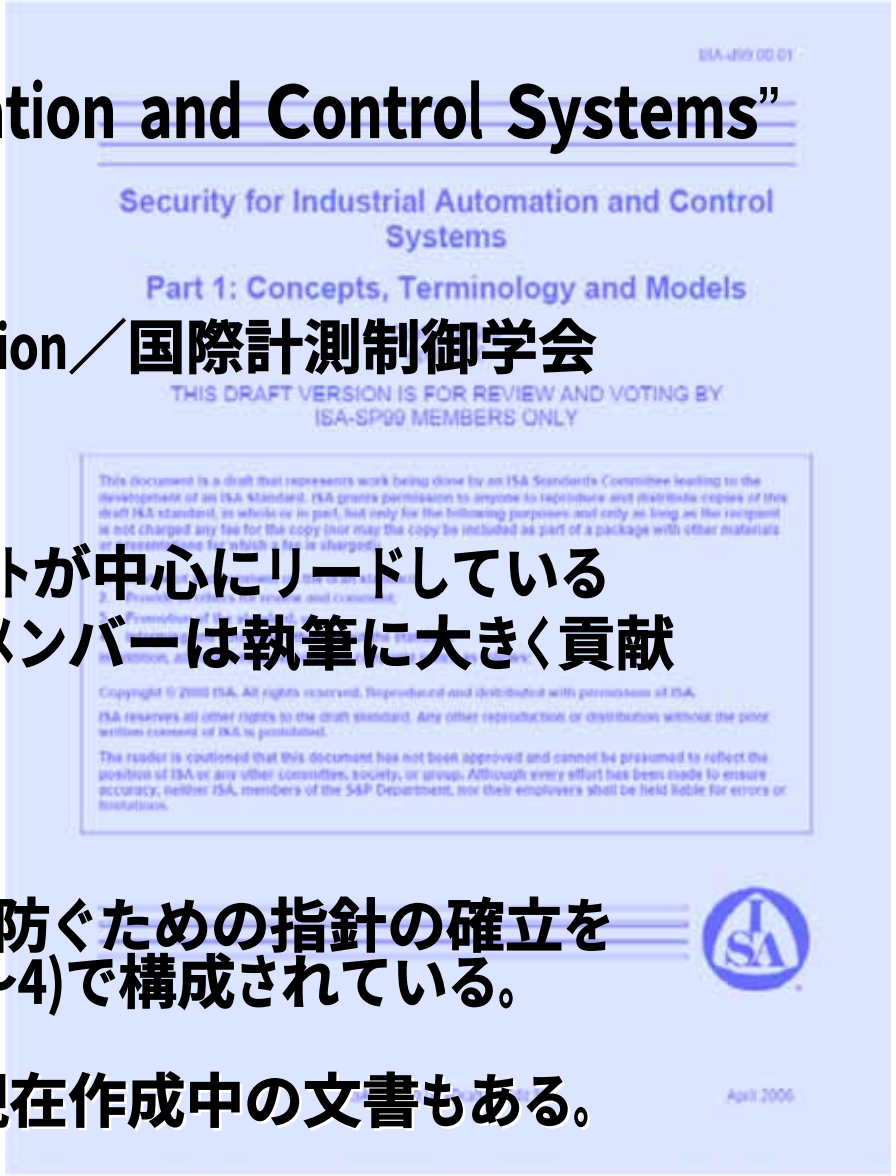


**WGメンバー**

# セキュリティ標準：ISA-99

- **名称**
  - “Security for Industrial Automation and Control Systems”
- **団体**
  - ISA：International Society of Automation／国際計測制御学会
- **参加メンバー**
  - システムインテグレータ/コンサルタントが中心にリードしている
  - エンドユーザも参加しており，一部のメンバーは執筆に大きく貢献
  - システムベンダーもひと通り参加
- **内容**
  - 生産制御システムへの電子的侵入を防ぐための指針の確立を目的としており、4つのパート(Part 1～4)で構成されている。

  各文書は順次レリースされているが、現在作成中の文書もある。



# セキュリティ標準：NIST SP800

- 団体
  - NIST：National Institute of Standards and Technology
    ／米国国立標準技術研究所
- メンバー
  - 401の組織，32カ国(2008年10月現在)
  - 制御機器ベンダ(Rockwell, Honeywell,…)，ITベンダ(Cisco, SUN, …)，
    ユーザ(Exxon Mobil, BP, Dupont, …)，コンサルタント(KEMA, …)，
    公的機関(NSA, 経産省, …)
- 内容

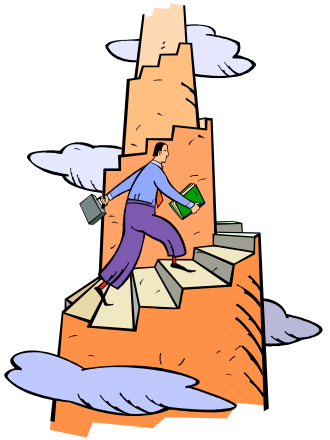
  SP800シリーズと名付けたコンピュータセキュリティに関する特別文書
  (Special Publications) が約100件公開されている。
  2つの文書が生産制御システムコミュニティに当てはまる。

  SP800-53　Recommended Security Controls for Federal Information Systems
  ／連邦政府情報システムにおける推奨セキュリティ管理策

  SP800-82　Guide to Industrial Control System Security
  ／産業用制御システムセキュリティのためのガイド

# ＰＤＣＡサイクルの具体策

| | 制御系セキュリティに使えるツール･規格 例 |
|---|---|
| Plan | ISA-99<br>NIST SP800-53/82<br>**各種**Good Practice<br>**セキュリティ評価ツール** |
| Do | ISA-99<br>**脆弱性スキャナ**<br>**侵入検知システム** (IDS) |
| Check | **ログ監査**<br>**侵入検知システム** (IDS)<br>**脆弱性情報** |
| Act | ISA-99<br>NIST SP800-53/82<br>**各種**Good Practice |



セキュリティ評価ツールの検討

**WGメンバー**

PART 2

# セキュリティ評価ツール SSATのご紹介

# SSAT とは？

## SSAT とは？

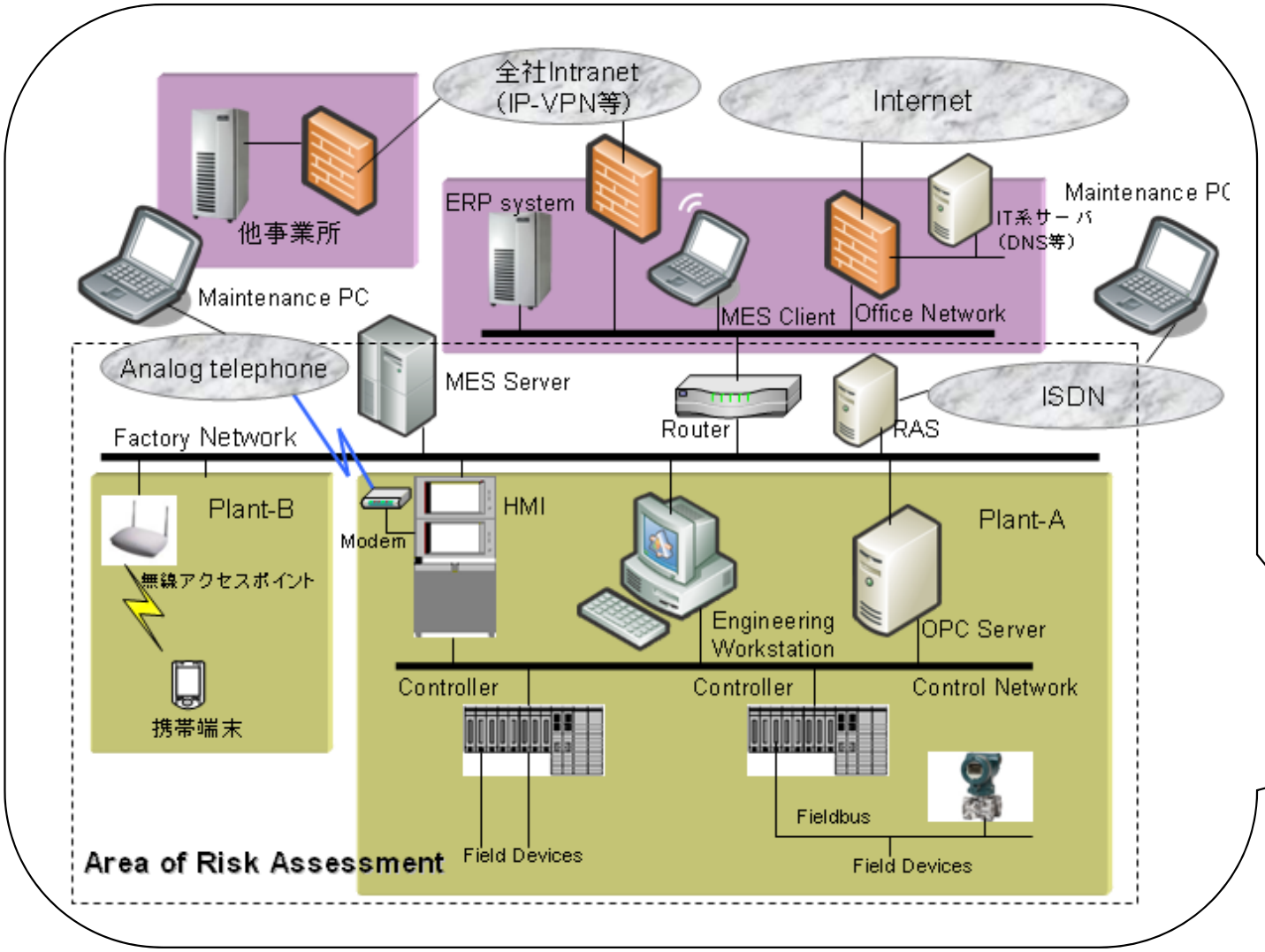
- 英CPNI が開発した生産制御システム向けのセキュリティ評価ツール
  (SCADA Self Assessment Tool の略)


## 日本版SSAT　（共同監修版）

- JPCERT/CCと共同で、ツールの評価／標準的な制御システムモデルへの適用を行い、分かりやすく，使いやすい和訳版にするための検討実施
- このたび和訳初版となる“日本版SSAT”の提供を開始しました

# モデルシステムによる評価

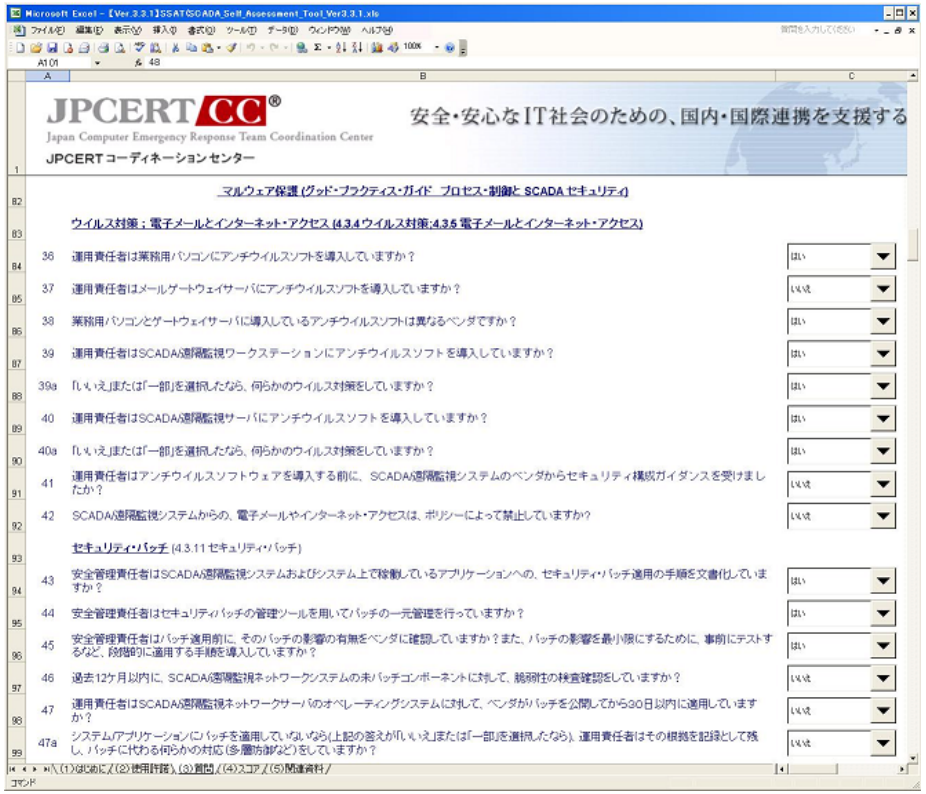
**WGメンバーが検討し、今回ツールを適用した一般的な生産制御システム例**




# SSAT の特徴

## 特徴は？

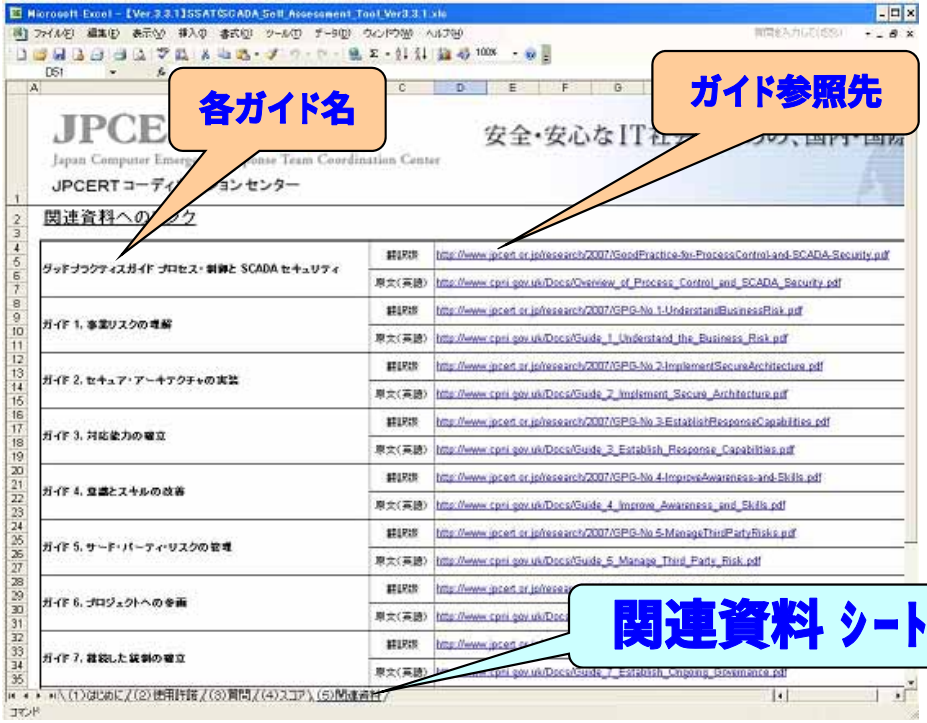
- SCADA に特化しているセキュリティ評価ツール
- 導入･操作が容易(Excelベース)
- 評価は短期間で実施可能(約120の設問に択一回答)
- 和訳参考資料が豊富

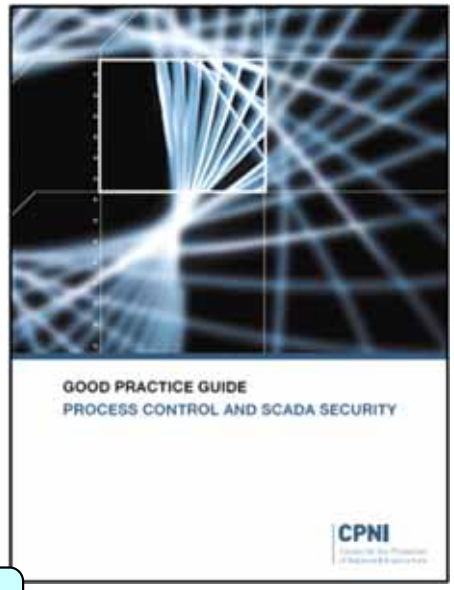



**制御システムの構築と運用に関するセキュリティ上の問題項目を手軽に抽出でき、バランスの良いセキュリティ対策を行うことができます**

# グッド・プラクティス・ガイド

- **セキュリティ基準は CPNI が公開しているグッド・プラクティス・ガイド「プロセス・制御と SCADA セキュリティ」がベース**
  - グッド・プラクティス・ガイドは複数のガイドに分かれている



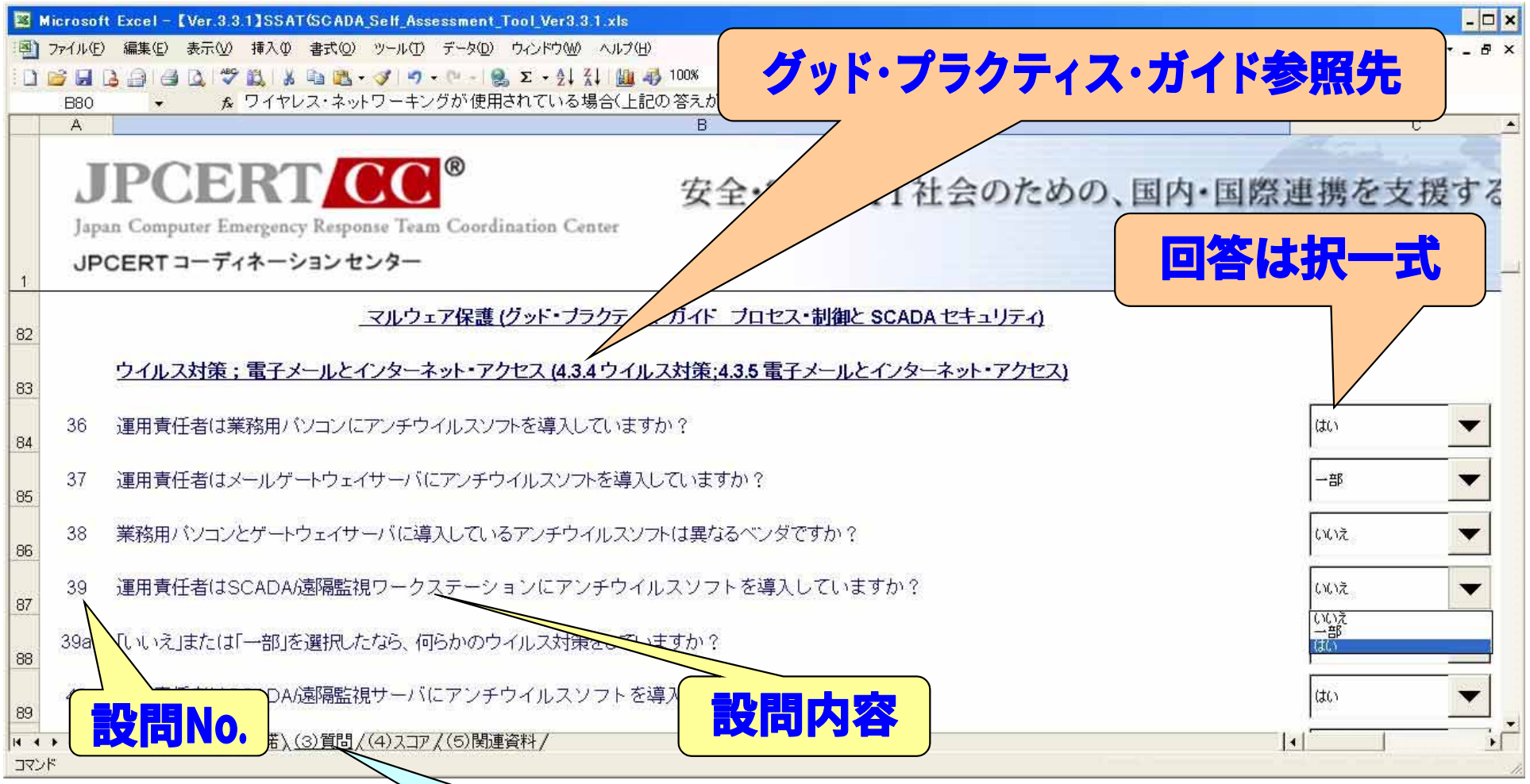

原文(英語)

和訳版

**SSATと本ガイドを併用することで、セキュリティに従事していない担当者の方にも、より深い理解を得ることができます**

# SSAT の設問例 1

- **設問例1**



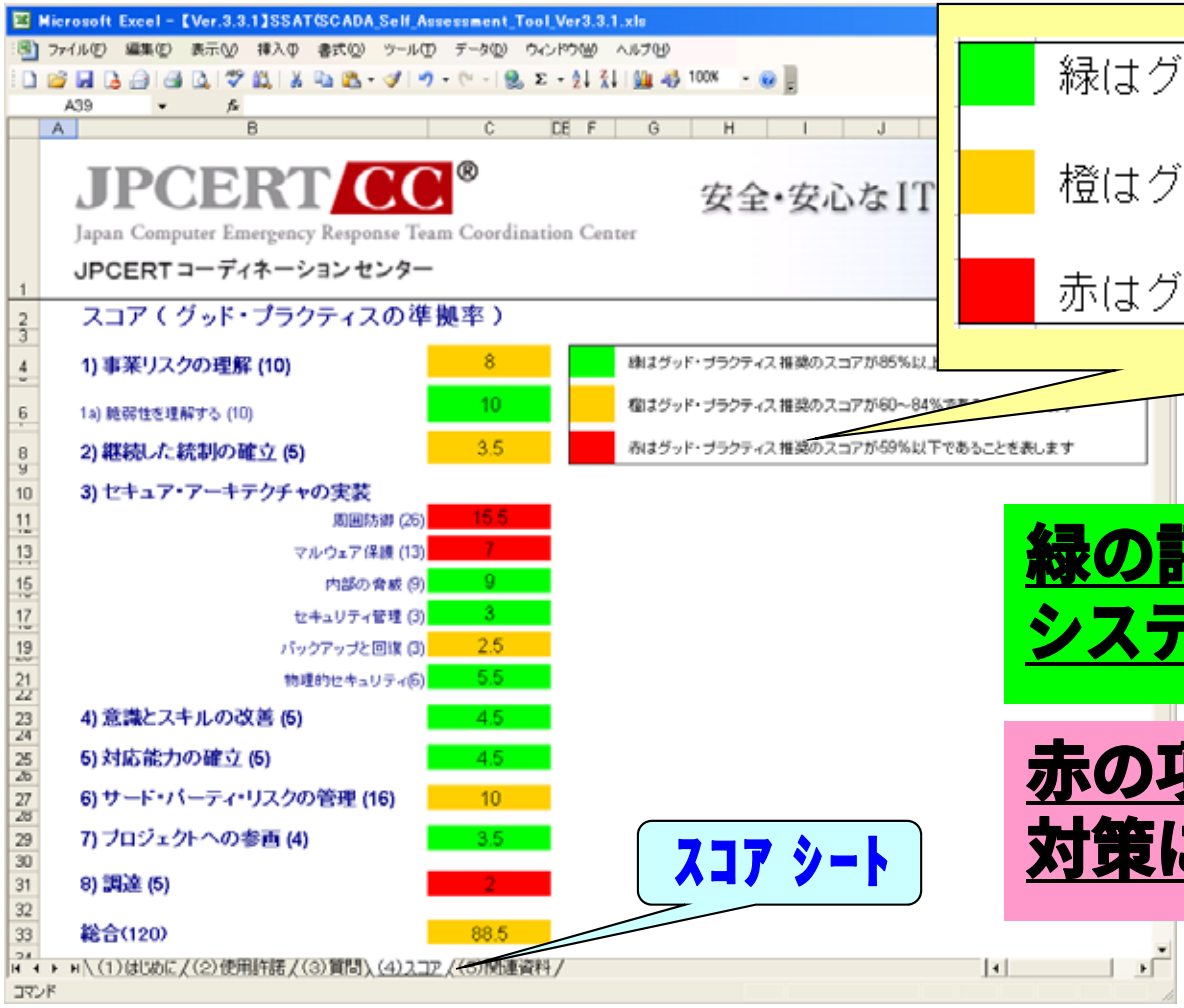
# SSAT の設問例 2

- **設問例2**
  - **択一式 (はい、いいえ、一部 など)**
    - すべてのSCADA/遠隔監視システムへの接続について、業務上の必要性を確認し、それを承認していますか？ (設問No.13)
    - 業務用パソコンにアンチウィルスソフトを導入していますか？ (設問No.36)
    - システム/アプリケーションにパッチを適用していないなら、その根拠を記録として残し、パッチに代わる何らかの対応 (多層防御など) をしていますか？ (設問No.47a)

# SSAT の評価結果例

## 評価結果(例)

➢グットプラクティスガイドの準拠率を3段階で評価




緑はグッド・プラクティス推奨のスコアが85%以上

橙はグッド・プラクティス推奨のスコアが60～84%

赤はグッド・プラクティス推奨のスコアが59%以下

**緑の評価が多いほどセキュアなシステムといえます**

**赤の項目においては、セキュリティ対策による改善が望まれます**

# 参考URL

- セキュリティ評価ツール(日本版SSAT)：

  関連情報/ツール入手先 (JPCERT/CCサイト)

  http://www.jpcert.or.jp/ics/ssat.html

- グッド・プラクティス・ガイド
  プロセス制御とSCADAセキュリティ(和訳版)：

  関連情報 (JPCERT/CCサイト)

  http://www.jpcert.or.jp/ics/information02.html

Part 3

# セキュリティ評価ツール SSATの改良

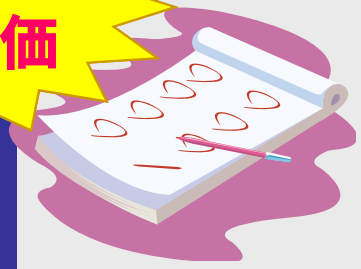
# 昨年度から今年度までの活動全体像

## 2010年度活動

日本語版
SSAT作成

SSAT公開
(2011.4)

良い評価
悪い評価



利用者アンケート

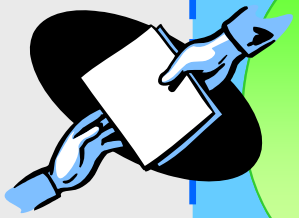
検討作業で
見えてきたことを
ご紹介します

## 2011年度活動

SSAT改良に向けた検討

- 役割の評価
- 重要度の評価
- 難易度の評価

WGメンバーでの再検討



利用者との情報交換

SSATの改良

- 設問数の見直し
  (重要度によって絞込む等)
- 設問内容の見直し
  (レベル分けして簡易に)

現在の
フェーズ

SSAT改良版公開
(予定)

# 発表内容（アジェンダ）

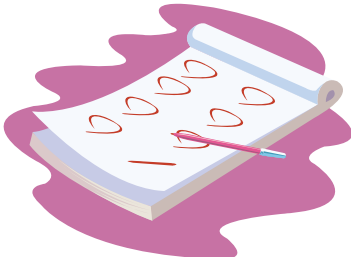
1. 検討課題
2. 検討結果
3. おすすめセキュリティ施策紹介
4. 改良に向けた取り組み
5. まとめと今後の課題

# さらなる改良に向けた課題

## ● SSATのさらなる改良に向けた課題抽出

SSAT利用者の**アンケート結果**から**改良に向けた課題を抽出！**

1. **設問数をより少なくできないか！**
   - NTOのグッドプラクティス(39問)程度になると良い



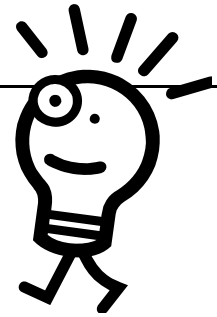
SSAT利用者アンケート

2. **内容がわかりづらい設問がある！**
   - まだ用語や表現が難しい設問がある
   - 抽象的すぎる設問はブレイクダウンしたほうがわかりやすい

3. **現場の担当者が回答しづらい設問がある！**
   - 経営者に対する設問には答えられない
   - 誰に対する設問なのか明かにして分けたほうが良い

4. **何をすれば良いのかわかりづらい設問がある！**
   - 判断基準がわかりづらく回答が難しい設問がある
   - 要件自体が難しすぎて実現困難な設問がある

# 課題の検討



## 1. 『設問数が多いこと』に対して

- 無闇に設問数を減らすとバランスが悪くなる
- 重要度を評価して優先順位付けをすることは可能？

☞ 各設問の重要度を評価して優先順位付けを試みる・・・【重要度の評価】

## 2. 『わかりづらい設問』に対して

- わかりづらい・回答しづらい設問がまだ残っている

☞ 回答難易度を評価して改善すべき設問を抽出する・・・【回答難易度の評価】

## 3. 『現場の担当者が回答しづらい設問』に対して

- 誰に対する質問かを再整理すれば回答しやすくなるかも？

☞ 各設問の対象者を再整理する　【役割の再整理】

## 4. 『何をすれば良いのかわかりづらい設問』に対して

- 現場の実情では実現困難な設問がある

☞ 実現難易度を評価して改善すべき設問を抽出する・・・【実現難易度の評価】

☞ **各設問の役割を再整理し、重要度・回答難易度・実現難易度を評価して要改良項目を抽出!!**

# 発表内容（アジェンダ）

1. 検討課題
2. 検討結果
3. おすすめセキュリティ施策紹介
4. 改良に向けた取り組み
5. まとめと今後の課題

# 検討1：役割の再整理

- **目的**
  - 各設問について「誰に対する設問か」を明らかにする
    - 回答しやすくなるかもしれない
    - 分担により担当者ごとの設問数を減らせるかもしれない
- **方法**
  1. 登場人物を想定
     - SSATの設問項目に登場する次の人物を想定
       - 経営者
       - 運用担当者
       - 安全管理責任者
       - ベンダ
  2. 各設問について、登場人物の役割を検討
     - 次の役割を想定
       - 責任者
       - 実担当者
       - 情報提供者
  3. WGメンバーの検討結果を持ち寄ってWGで検討

# 検討2：重要度の評価

- **目的**
  - **各設問について「重要度」を明らかにする**
    - 重要度で優先順位付けを行って設問を整理することにより**SSAT導入の敷居を下げられるかも**しれない
- **方法**
  1. **主観評価で重要度を評価**
     - まずは**WGメンバーの主観尺度**で**「高」「中」「低」の3段階**に評価
  2. **WGメンバーの評価を持ち寄ってWGで検討**
     - 集計結果を検討して**WGとしての重要度を判定**

# 検討3：難易度の評価

- **目的**
  - **各設問について「難易度」を明らかにする**
    - 難易度の高い項目に対して対策を打つことで**SSATの難易度を下げられるかも**しれない
- **方法**
  1. **2種類の難易度について評価する**
     - 「回答難易度」：**『回答のしやすさ』**を評価
     - 「実現難易度」：**『要件を満たすための施策の難易度』**を評価
  2. **WGメンバーの評価を持ち寄ってWGで検討する**
     - 集計結果を検討して**WGとしての難易度を判定**

# 検討結果

役割の再整理で
見えてきたことは？

重要度の評価で
見えてきたことは？

難易度の評価で
見えてきたことは？

## 役割，難易度の検討結果

| セクション名 | 設問数 | 担当者 | | | | | | | | | | | | 重要度 | | | 回答難易度 | | | 実現難易度 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 安全管理責任者 | | | 運用責任者 | | | 経営者 | | | ベンダSIer | | | | | | | | | | | |
| | | ◎ | ○ | △ | ◎ | ○ | △ | ◎ | ○ | △ | ◎ | ○ | △ | 高 | 中 | 低 | 高 | 中 | 低 | 高 | 中 | 低 |
| システムとビジネスリスクを理解する | 3 | 3 | | | | 3 | | | | | | | 1 | 3 | | | 1 | 2 | | 1 | 2 | |
| 脅威を理解する | 4 | 4 | | | | 4 | | | | | | | 2 | 3 | 1 | | | 2 | 2 | 2 | 2 | |
| 影響を理解する | 2 | 2 | | | | 2 | | | | | | | 1 | | 2 | | | 1 | 1 | 2 | | |
| 事業リスクの継続的な評価 | 1 | 1 | | | | 1 | | | | | | | 1 | 1 | | | | 1 | | 1 | | |
| 脆弱性を理解する | 2 | 2 | | | | 2 | | | | | | | 2 | 2 | | | | 2 | | 2 | | |
| 継続した統制の確立 | 5 | 4 | 1 | | | 3 | | 3 | 2 | | | | | 3 | 2 | | | | 5 | 1 | 2 | 2 |
| ネットワークアーキテクチャ | 5 | 5 | | | | 3 | | | | | | | 3 | 5 | | | | 2 | 3 | 2 | 2 | 1 |
| ファイアウォール | 6 | 6 | | | 2 | 4 | | | | | | | 6 | 2 | 4 | | | | 6 | | 5 | 1 |
| リモートアクセス | 7 | 6 | | | 1 | 6 | | | | | | | 4 | 3 | 4 | | | 2 | 5 | | 5 | 2 |
| システム監視 | 5 | 3 | 2 | | 2 | 3 | | | | | | | 4 | | 5 | | | 2 | 3 | 2 | 3 | |
| セキュリティ試験 | 3 | 3 | | | | 3 | | | | | | | 3 | | 3 | | | | 3 | 3 | | |
| ワイヤレスネットワーキング | 2 | 2 | | | | 2 | | | | | | | 2 | | 2 | | | 1 | 1 | 1 | 1 | |
| ウイルス対策 | 9 | 9 | | | 1 | 8 | | | | | | | 9 | 4 | 5 | | | | 9 | | 7 | 2 |
| セキュリティパッチ | 6 | 4 | 2 | | 2 | | | | | | | | 6 | 3 | 3 | | | 4 | 2 | 5 | 1 | |
| システムの強化 | 1 | | 1 | | 1 | | | | | | | | 1 | 1 | | | | | 1 | | 1 | |
| パスワードとアカウント | 6 | 3 | 3 | | 5 | 1 | | | | | | | 4 | 2 | 4 | | | 1 | 5 | | 5 | 1 |
| 転入者と転出者用のプロセス | 2 | 2 | | | | 2 | | | | | | | 1 | 1 | 1 | | | | 2 | | 2 | |
| 要員の身元確認 | 2 | 2 | | | | 2 | | 2 | | | | | | | 2 | | | 1 | 1 | 2 | | |
| 機器接続手順 | 1 | 1 | | | | 1 | | | | | | 1 | | 1 | | | | | 1 | | 1 | |
| 変更管理 | 2 | | 2 | | 2 | | | | | | | | 1 | 1 | 1 | | | 1 | 1 | | 2 | |
| バックアップと回復 | 4 | | 4 | | 4 | | | | | | | | 2 | | 4 | | | 1 | 3 | 3 | 1 | |
| 物理的セキュリティ | 6 | 6 | | | 5 | 1 | | | | | | | 3 | 2 | 4 | | | 1 | 5 | | 6 | |
| 意識とスキルの改善 | 5 | 4 | 1 | | 1 | 4 | | 2 | | | | | | | 5 | | | 3 | 2 | | 5 | |
| 対応能力の確立 | 5 | 4 | 1 | | 1 | 4 | | 1 | 1 | | | | 2 | 3 | 2 | | | | 5 | 1 | 4 | |
| サードパーティリスクの管理 | 12 | 7 | 5 | | 6 | 5 | | | | | | 1 | 9 | | 12 | | | 11 | 1 | | 12 | |
| サポート組織からのリスクの管理 | 5 | | 5 | | | 5 | | | | | 3 | 2 | | | 5 | | | 4 | 1 | | 5 | |
| プロジェクトへの参画 | 4 | 4 | | | | 4 | | | | | | | 1 | | 4 | | | 4 | | 1 | 3 | |
| 調達 | 5 | 1 | | | 1 | | | 5 | | | | 1 | 1 | | 5 | | 1 | | 4 | 1 | 2 | 2 |
| 合計 | 120 | 88 | 27 | | 34 | 73 | | 13 | 3 | | 3 | 5 | 69 | 40 | 80 | | 2 | 46 | 72 | 30 | 79 | 11 |
| 比率 | | 73 | 31 | | 28 | 83 | | 11 | 9 | | 3 | 38 | 58 | 33 | 67 | | 2 | 38 | 60 | 25 | 66 | 9 |

役割
検討結果

重要度
検討結果

難易度
検討結果

◎責任者　○実担当者　△情報提供者

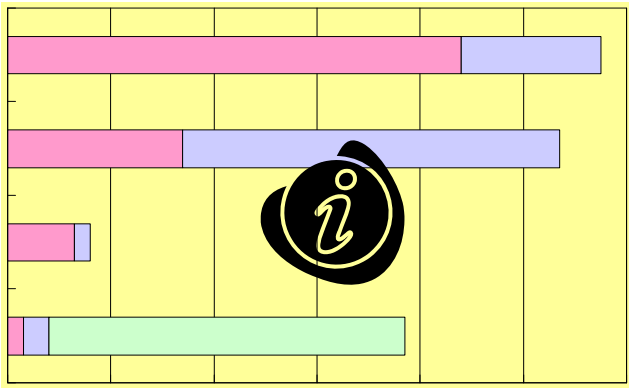
# 検討結果1：役割の再整理

## ● 役割の再整理で見えてきたこと

検討結果

### 「責任者」と「実担当者」を再整理した結果について

- **役割はあまり分散しなかった**
  - 責任者：88%の項目で安全管理責任者の役割
  - 担当者：73%の項目で運用責任者の役割



役割分類結果グラフ（付録参照）

☞ **役割の明確化による負荷分散は難しい**

- **ベンダの役割が大きいことがわかった**
  - 情報提供者： 69%の項目でベンダの役割
  - ベンダが情報提供しないと実現不可能な項目もある

☞ **セキュリティ向上のためにはベンダの協力が不可欠**

- **経営者が「責任者」「実担当者」になるケースは少なかった**
  - 11%の項目で責任者または担当者の役割
  - **経営者は「責任者」「担当者」の活動を指示・承認・支援する立場で参画**

# 検討結果2：重要度の分類

- **重要度での分類結果**
  - 6割程度が「重要度：中」
  - 3割程度が「重要度：高」
  - 「重要度：低」の項目は無し
- **重要度について 意見が一致しない項目あり**

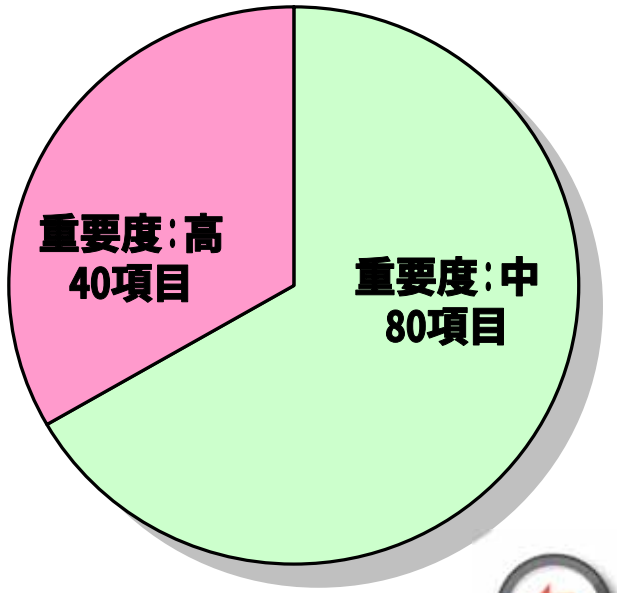
**意見が一致している項目**

- 明快でわかりやすいのかもしれない

**意見が一致しなかった項目**

- 基準の違い (基準を設定していなかったため)
- 知識・経験の違い
- ゆれ・誤差・間違い
- 項目に問題があるのかもしれない

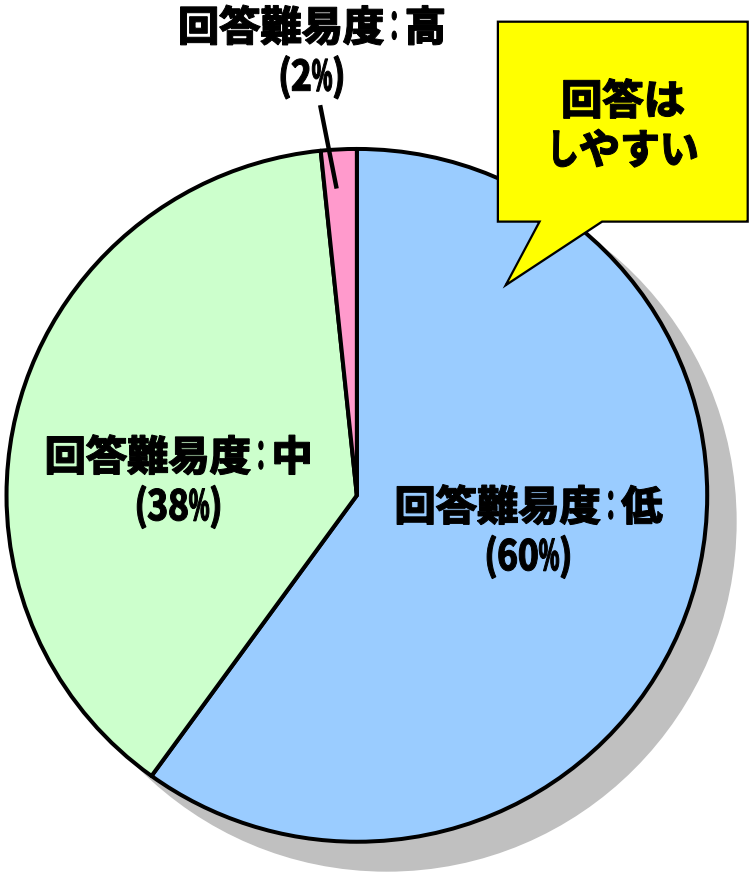
（多義的に理解できてしまう？　わかりづらい？）



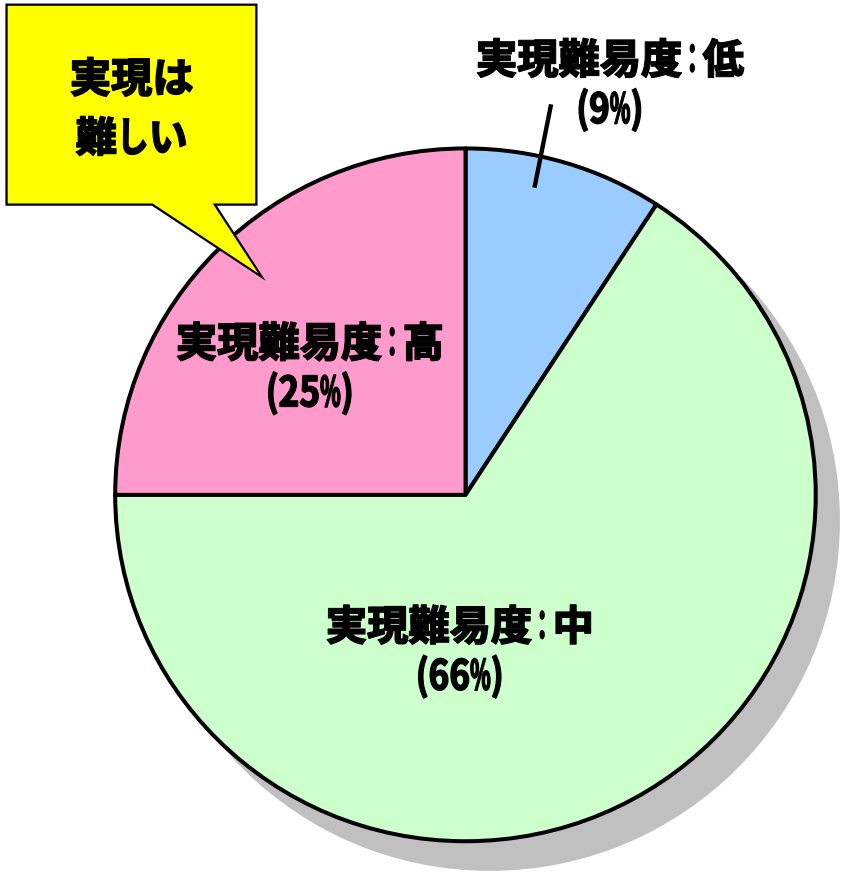

重要度の分類

検討結果

# 検討結果3：回答難易度と実現難易度



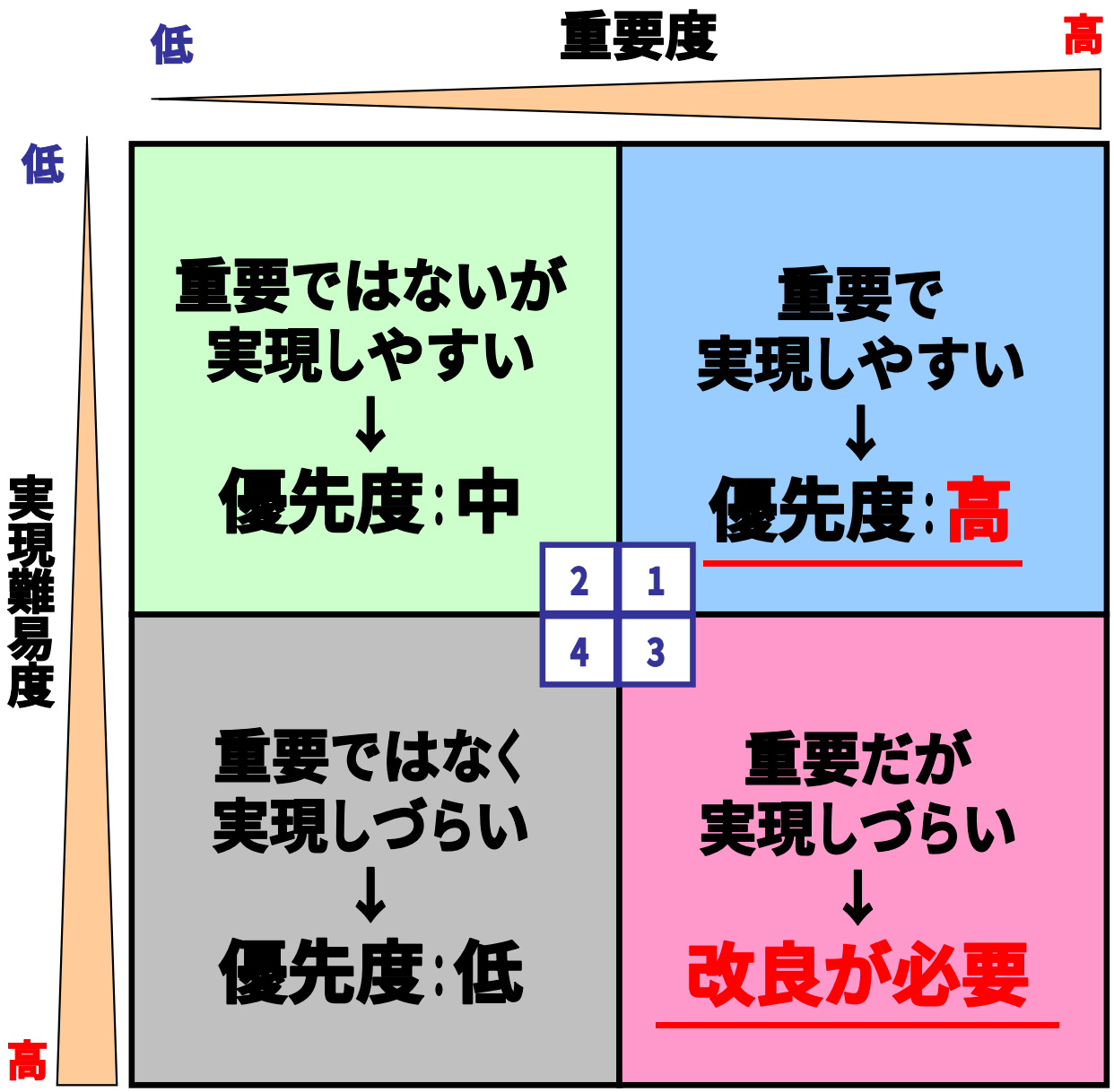

設問の回答難易度



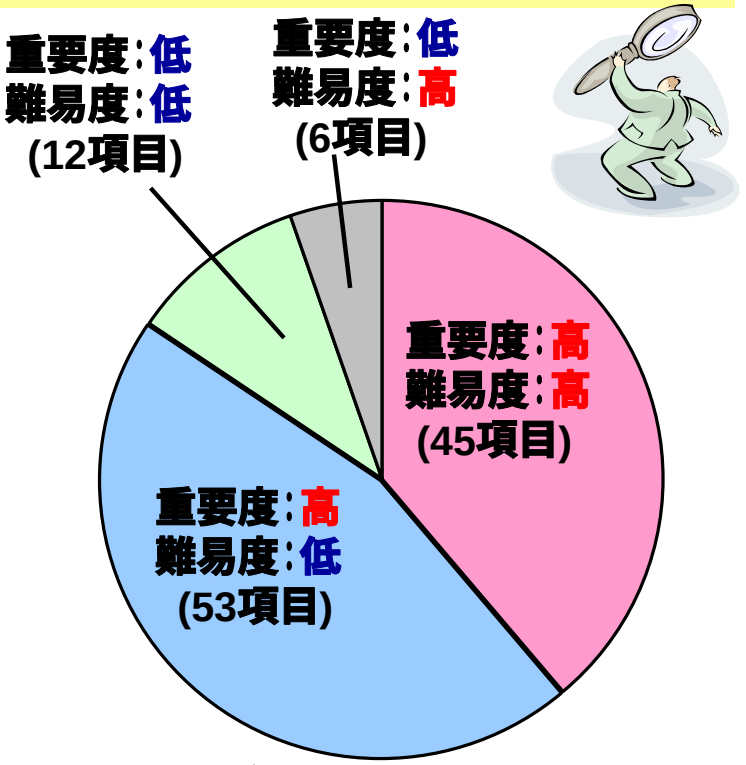

設問の実現難易度

**重要度と実現難易度から**
**見えてくるものとは．．．**

# 重要度と回答難易度から見えてくること




**優先順位が見えてくる！**




各分類の設問数

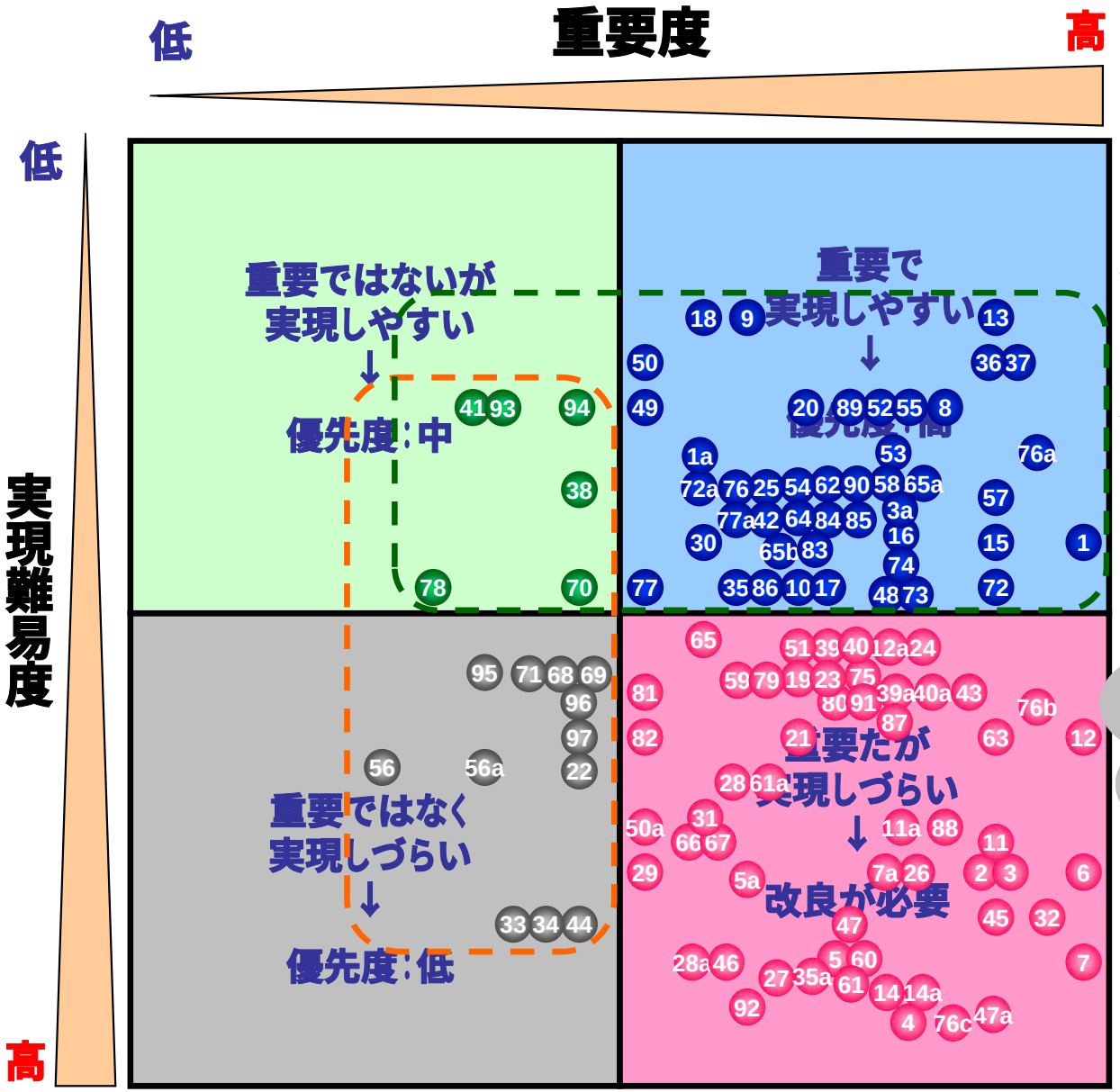
優先順位1）難易度：低，重要度：高（第1象限）

優先順位2）難易度：低，重要度：低（第2象限）

優先順位3）難易度：高，重要度：高（第4象限）

優先順位4）難易度：高，重要度：低（第3象限）

# WGメンバー評価結果をプロット




**重要度・難易度について、WGメンバーの評価（平均値）をプロット**

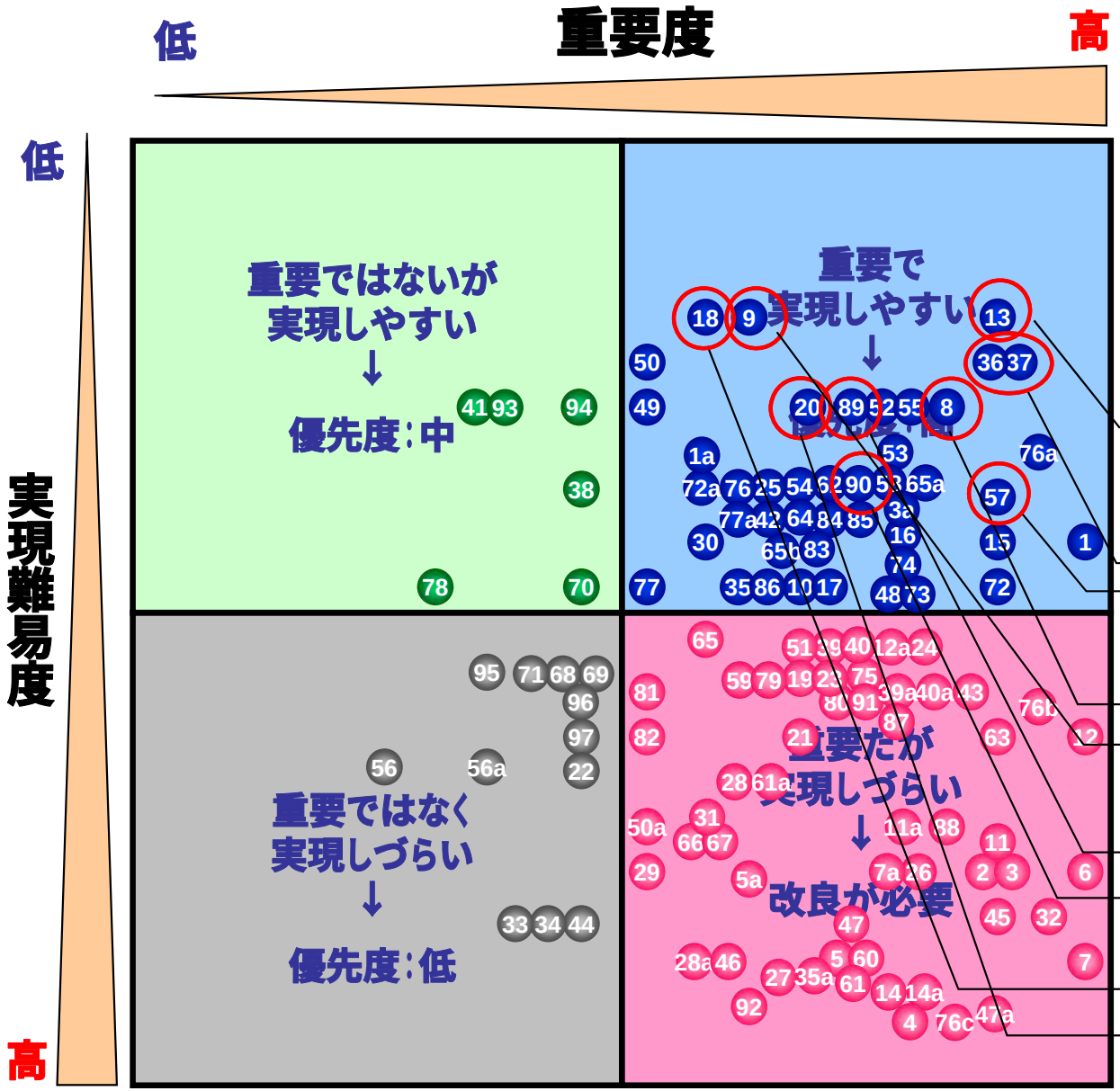
- ✓ **重要度が低い**と判断された項目（第2, 第3象限）⇒ **少ない**
- ✓ **難易度が低い**と判断された項目（第1, 第2象限）⇒ 全体の**4割**程度

セキュリティ施策としては、**難易度が低く、重要なもの**から始めるのが良さそう

**ポイント**

**やりやすく、重要な施策から始めてみる**

# おすすめセキュリティ施策




**難易度が低く、重要なものを「おすすめセキュリティ施策」としてピックアップ**

**「簡単なことから始める」という発想**
**※類似項目は1項目として整理**

**13:** すべての接続について業務上の必要性が確認されているか？

**36, 37, 57:** アンチウイルスソフトを導入しているか？

**8, 9:** セキュリティの責務を明確にしているか？

**89, 90:** 開発プロジェクトにセキュリティの責任者を配置し影響を考慮しているか？

**18, 20:** ファイアウォールに関するトレーニングを受講し適切に設定しているか？

# 発表内容（アジェンダ）

1. 検討課題
2. 検討結果
3. おすすめセキュリティ施策紹介
4. 改良に向けた取り組み
5. まとめと今後の課題

# 5つのおすすめセキュリティ施策

ポイント
やりやすく、重要な施策から始めてみる

## 【難易度が低く重要度の高い項目】

1. **継続した統制の確立 (責任の明確化)**
   ⇒ 設問8, 9：セキュリティの責務を明確にしているか？
2. **ネットワークアーキテクチャ (ネットワーク接続の管理)**
   ⇒ 設問13：すべての接続について業務上の必要性が確認されているか？
3. **ファイアウォール (設定の強化)**
   ⇒ 設問18, 20：ファイアウォールに関するトレーニングを受講し適切に設定しているか？
4. **ウィルス対策・機器接続手順 (アンチウィルスソフトの導入)**
   ⇒ 設問36, 37, 57：アンチウイルスソフトを導入しているか？
5. **プロジェクトへの参画 (開発でのセキュリティ考慮)**
   ⇒ 設問89, 90：開発プロジェクトにセキュリティの責任者を配置し影響を考慮しているか？

# 発表内容（アジェンダ）

1. 検討課題
2. 検討結果
3. おすすめセキュリティ施策紹介
4. 改良に向けた取り組み
5. まとめと今後の課題

# 改良に向けた取り組み

## ● 検討結果と取り組み

**検討結果**

1. 回答難易度・実現難易度の高い項目があった
2. 回答難易度・実現難易度の判定が割れた項目があった
3. 代替施策に関する項目で回答や実現難易度が高いものがあった

（例）設問40a
「いいえ」または「一部」を選択したなら何らかのウイルス対策をしていますか？
→ アンチウイルスソフトウェアに代わるウイルス対策とは何かわかりづらく実現難易度が高い

**取り組み**

読み手によって違う内容に見えている可能性がある
下記項目に対して、その**要因を推定**して**対策を検討**する。

- **回答難易度**、**実現難易度**が**高い**項目
- **回答難易度**、**実現難易度**の**評価**が**割れた**項目
- **代替施策**に関する項目

WGメンバーで原因と対策を再検討

**要検討項目を抽出!!**

# 要検討項目抽出結果

- **抽出結果**

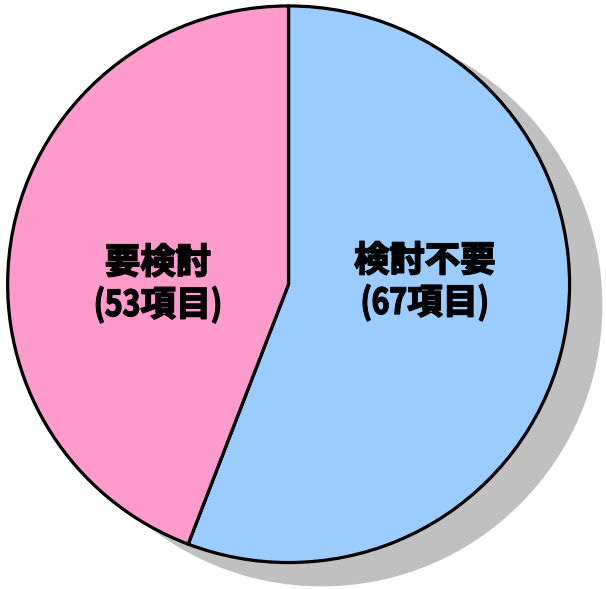
**改良対象の項目：　53**

【内訳】　※重複あり

- 回答難易度が「高」の項目：　10
- 実現難易度が「高」の項目：　31
- 回答難易度評価が割れた項目：　13
- 実現難易度評価が割れた項目：　12
- 代替施策に関する項目：　10

**改良のために要因分析が必要**

**改良対象外の項目：　67**




要検討項目の抽出結果

# 改良要因

- **設問の難易度を上げている要因**
  1. **表現･用語がわかりづらい**
     - 用語の説明がほしい
     - 適切な用語へ置換してほしい
  2. **実現方法･要求レベルがわからない**
     - 例示や参考資料がほしい
  3. **内容は理解できるが実現が難しい**
     - 「すべての」などの語を含む設問については実現が困難
     - 要件が緩和されないと実現は困難
  4. **内容は理解できるが要件通りに実現することは難しい**
     - 現場の現状に合った実現方法を許容してほしい

# 改良対策

## ● 設問の難易度を下げるための対策

対策例は付録7を参照

### 1. 表現･用語がわかりづらい

- 設問の**表現を改善**する！

※昨年度活動で検討されていることもあり、数は少なかった。

### 2. 実現方法･要求レベルがわからない

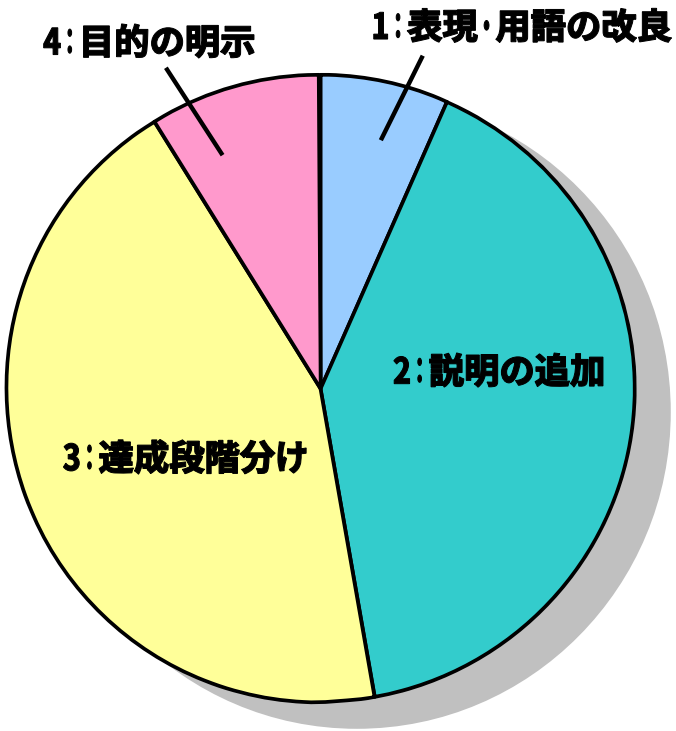
- 設問に**解説を追加**する！

※全般的に多く見られた
※SSATとGPGだけでは何をすれば良いのか、どう判定すれば良いのか解りづらい

### 3. 内容は理解できるが実現が難しい

- **難易度の低い要求事項を用意**する！

※リスクアセスメントや脆弱性検査に関する項目に多かった
※脆弱性検査についてはSSATによる検査で代用することも可能？
※「30日以内」などの制限付きの項目に多かった




要検討項目への対応 (重複ありで集計)

### 4. 内容は理解できるが要件通りに実現することは難しい

- **目的を明示して**代替施策を**検討しやすく**する！

※「BS7858への準拠」など扱いづらい文書への準拠が求められる項目で代替項目の検討が必要

対策例

# 発表内容（アジェンダ）

1. 検討課題
2. 検討結果
3. おすすめセキュリティ施策紹介
4. 改良に向けた検討
5. まとめと今後の課題

# まとめと今後の課題

- まとめ
  - SSATを中小規模システムでも利用しやすくする検討を実施
    - 重要度・難易度を評価して改良すべき項目を抽出した
      - ☞現状、「回答しやすいが実現は難しい」という状態
    - 改良方法を検討し、改良すべき項目と改善の方向性が定まった
      - ☞説明の追加、項目のレベル分け
  - 生産制御システムセキュリティ分野への貢献
    - SSATの改良を通じて、
      生産制御システムセキュリティの底上げに貢献していく
- 今後の課題
  - 利用者の意見を参考に改良版SSATを作成して成果を公開
    - 日本ガス協会様など、利用者と意見交換しながらより使いやすい形に改良する

# 全体のまとめ

- セキュリティ評価ツールやガイドラインなどを活用して
  セキュリティ対策に関する情報共有と協力体制を
  関係者間で築いていきます。

# 本日は、ありがとうございました。

## お手数ですが、アンケートの
## ご記入をお願いします

# 付録

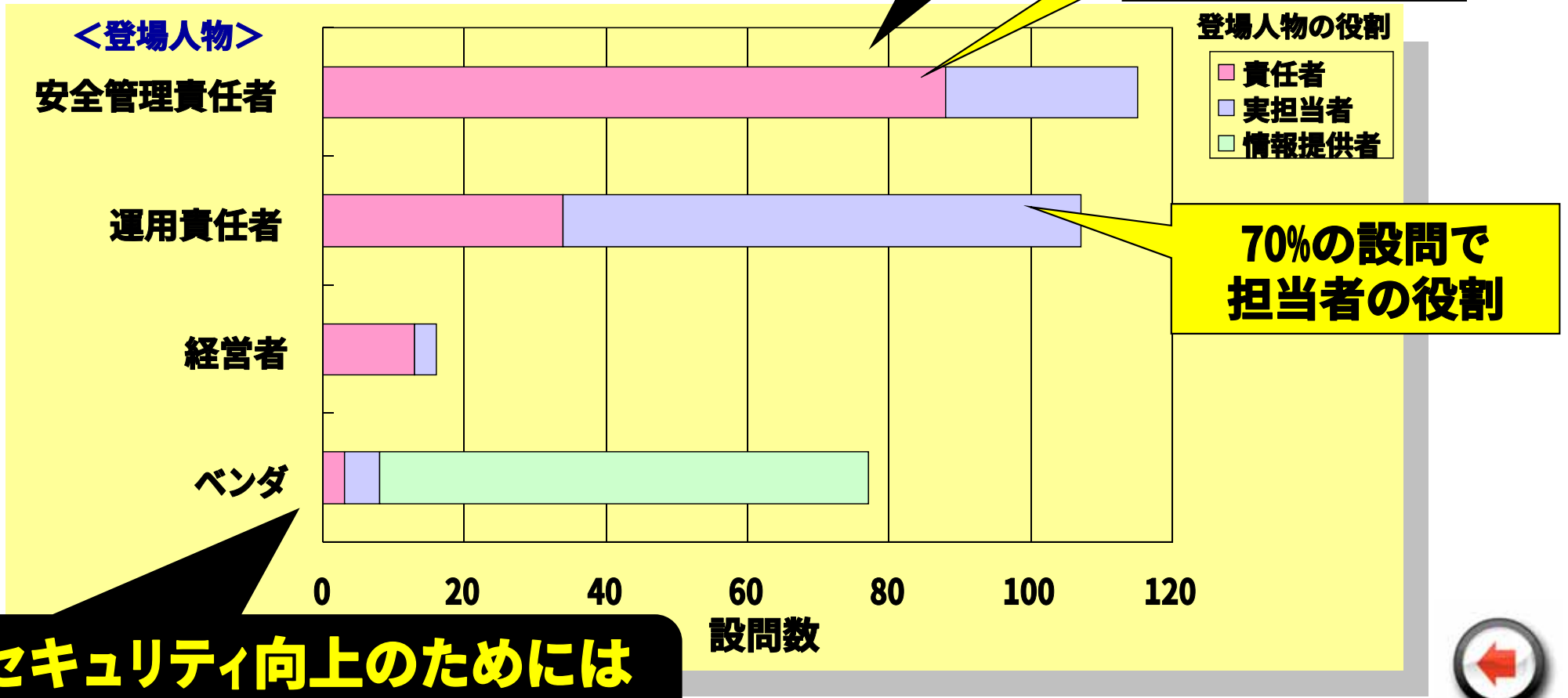
# 付録1) 役割分類結果グラフ

役割の明確化による
負荷分散は難しい

- **検討結果：役割の再整理**

  設問120問について、
  各登場人物の役割を重複ありで分類

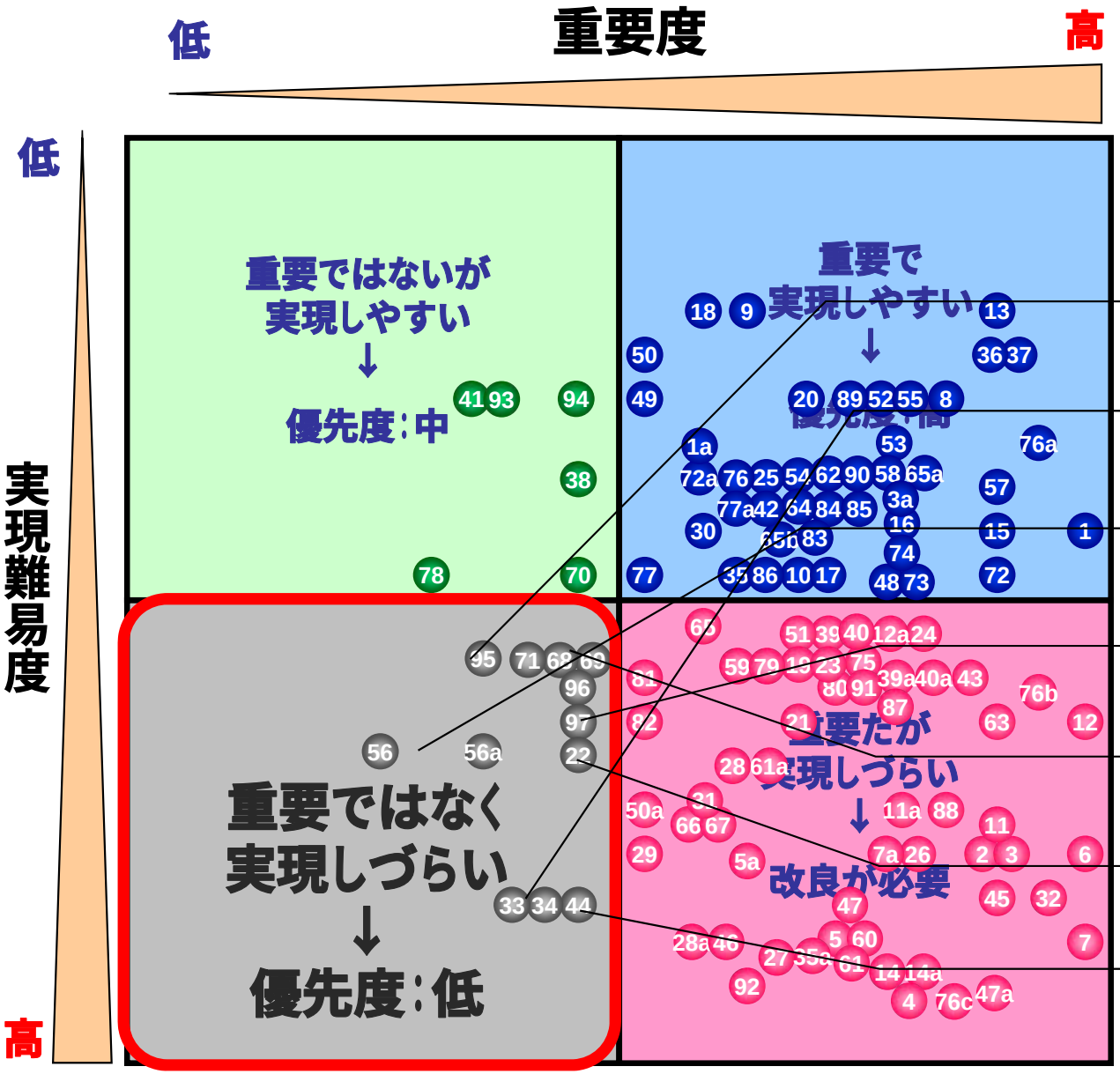
88%の設問で
責任者の役割




70%の設問で
担当者の役割

セキュリティ向上のためには
ベンダの協力が不可欠

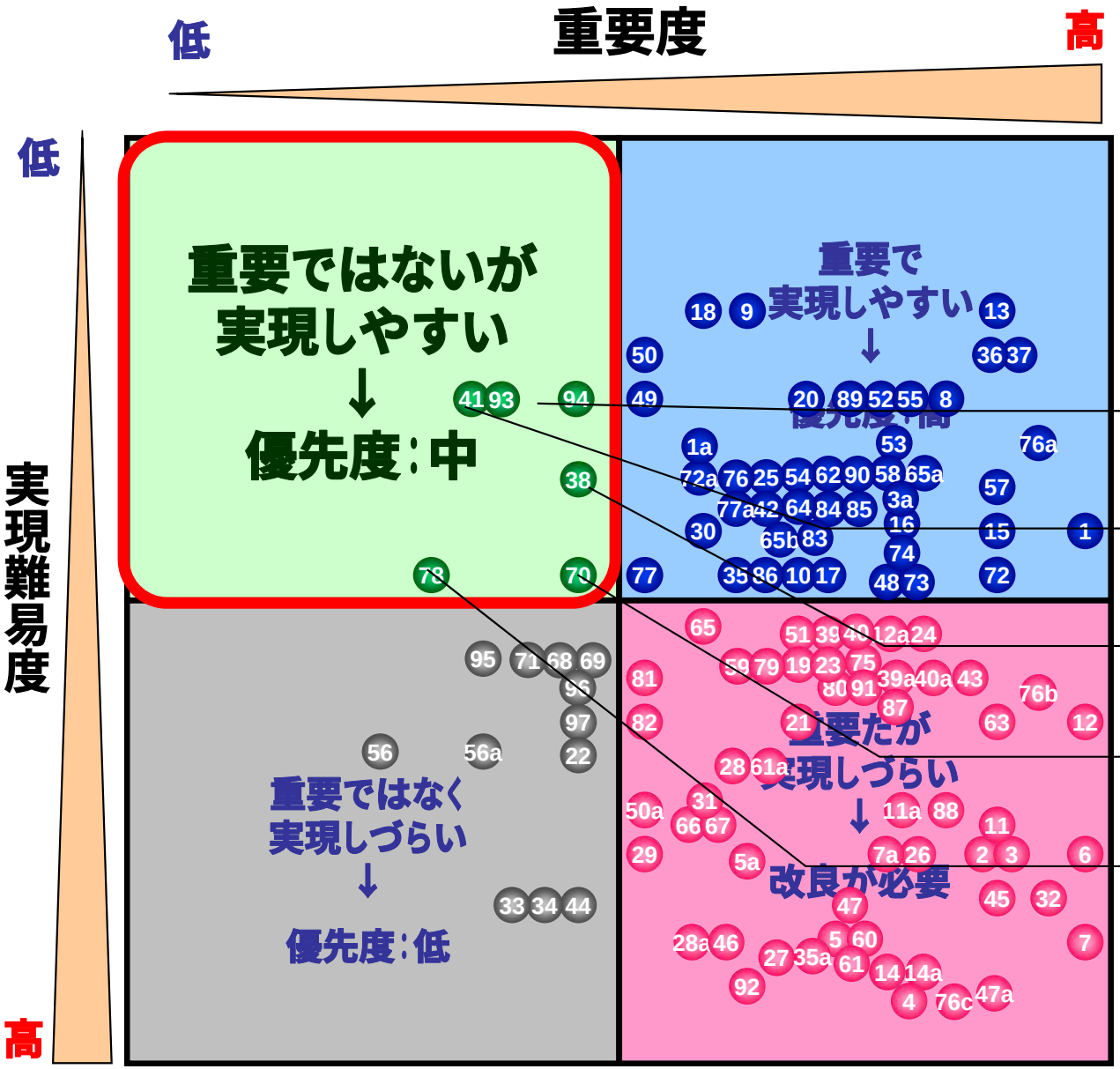
# 付録2) 優先度の低い設問項目




## (参考)
## 重要度が低く、難易度が高い SSAT設問項目

- **95:** 「コントロールシステムのサイバーセキュリティ調達基準」を利用しているか？
- **33, 34:** 定期的に侵入テストを行なっているか？
- **56, 56a:** BS7858:2006などの人事ガイダンスに従って採用しているか？
- **38:** アンチウイルスソフトはゲートウェイとPCで異なるベンダか？
- **68, 69:** 社内, 社外向けに注意喚起プログラムがあるか？
- **22:** すべてのリモートアクセスの監査を行なっているか？
- **44:** パッチの一元管理を行なっているか？

# 付録3) 優先度が中程度の設問項目




## (参考)
## 重要度が低く、難易度が低い SSAT設問項目

- **93, 94:** 「コントロールシステムのサイバーセキュリティ調達基準」を知っているか？
- **41:** ベンダからセキュリティガイダンスを受けているか？
- **38:** アンチウイルスソフトはゲートウェイとPCで異なるベンダか？
- **70:** 担当者がセキュリティ教育を受ける機会があるか？
- **78:** セキュリティロードマップの提示をベンダに求めているか？

# 付録4) 要検討項目抽出ルール

- 要検討項目として下記ルールで項目を抽出する
  - 回答難易度、実現難易度が「高」の項目
    - メンバーによる判定の最頻値が「高」の項目
    - 「高」と「中」が同一数の場合には「中」と判定
  - 回答難易度、実現難易度の評価が割れた項目
    - メンバーによる判定で「高」と「低」の両方があった項目
  - 代替施策に関する項目
    - 例：40a:「いいえ」または「一部」を選択したなら何らかのウイルス対策をしていますか？

# 付録5) 設問項目の改良対応種別分類

## 設問項目の改良対応種別分類 (概要)

| No. | セクション名 | 設問数 | 要検討設問数 | 改良対応種別 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|---|---|
| 1 | システムとビジネスリスクを理解する | 3 | 1 | | 1 | | |
| 2 | 脅威を理解する | 4 | 2 | 1 | 2 | 1 | |
| 3 | 影響を理解する | 2 | 2 | | 2 | 2 | |
| 4 | 事業リスクの継続的な評価 | 1 | 1 | | 1 | 1 | |
| 5 | 脆弱性を理解する | 2 | 2 | | 2 | 2 | |
| 6 | 継続した統制の確立 | 5 | 3 | 1 | 2 | 1 | 1 |
| 7 | ネットワークアーキテクチャ | 5 | 2 | 1 | 2 | 1 | |
| 8 | ファイアウォール | 6 | 2 | | 2 | 1 | |
| 9 | リモートアクセス | 7 | 3 | | 2 | 3 | |
| 10 | システム監視 | 5 | 3 | | 3 | 3 | 1 |
| 11 | セキュリティ試験 | 3 | 3 | | 3 | 3 | |
| 12 | ワイヤレスネットワーキング | 2 | 1 | | 1 | 1 | |
| 13 | ウイルス対策 | 9 | 3 | | 2 | 3 | |
| 14 | セキュリティパッチ | 6 | 5 | 1 | 3 | 4 | 2 |
| 15 | システムの強化 | 1 | | | | | |
| 16 | パスワードとアカウント | 6 | 4 | | 1 | 4 | 1 |
| 17 | 転入者と転出者用のプロセス | 2 | 1 | | 1 | 1 | |
| 18 | 要員の身元確認 | 2 | 2 | | 2 | 1 | 2 |
| 19 | 機器接続手順 | 1 | | | | | |
| 20 | 変更管理 | 2 | 2 | | 1 | 1 | |
| 21 | バックアップと回復 | 4 | 3 | | 1 | 3 | |
| 22 | 物理的セキュリティ | 6 | 1 | | 1 | | |
| 23 | 意識とスキルの改善 | 5 | 3 | 2 | | 1 | |
| 24 | 対応能力の確立 | 5 | 1 | | 1 | | |
| 25 | サードパーティリスクの管理 | 12 | 1 | | 1 | 1 | 1 |
| 26 | サポート組織からのリスクの管理 | 5 | | | | | |
| 27 | プロジェクトへの参画 | 4 | 1 | | | 1 | |
| 28 | 調達 | 5 | 1 | | | 1 | |
| | 合計 | 120 | 53 | 6 | 37 | 40 | 8 |
| | 比率 | | 44 | 7 | 41 | 44 | 9 |

1：設問の表現を改善する
2：設問に解説を追加する
3：難易度の低い要求事項を用意する
4：目的を明示して代替施策を検討しやすくする

(各項目について重複ありで分類)

**分類 2, 3 の項目が多い**

2: 設問に解説を追加する

3：難易度の低い要求事項を用意する

**解説の追加と低難易度の設問設定で改善**

# 付録6) おすすめ施策例

1. **継続した統制の確立 (責任の明確化)**
   設問8, 9: セキュリティの**責務を明確**にしているか？
2. **ネットワークアーキテクチャ (ネットワーク接続の管理)**
   設問13：すべての接続について**業務上の必要性が確認**されているか？
3. **ファイアウォール (設定の強化)**
   設問18, 20：ファイアウォールに関する**トレーニングを受講し適切に設定**しているか？
4. **ウィルス対策・機器接続手順 (アンチウィルスソフトの導入)**
   設問36, 37, 57: **アンチウイルスソフトを導入**しているか？
5. **プロジェクトへの参画 (開発でのセキュリティ考慮)**
   設問89, 90: 開発プロジェクトに**セキュリティの責任者を配置し影響を考慮**しているか？

# おすすめセキュリティ施策例 1
# 継続した統制の確立

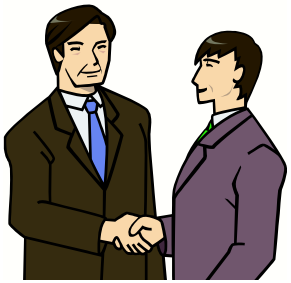
**設問8:経営者は安全管責任者の責務を明確にし、適切な支援を行っていますか？**

**設問9:経営者はSCADA/遠隔監視セキュリティに関する日々の責任を文書化していますか？**

**①安全管責任者の責務を明確**

**⇒ 事業リスクの理解が重要。**

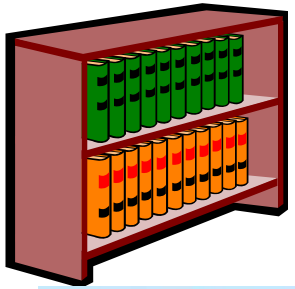
**経営者は事業リスクを理解し、**
**安全責任者の支援を実行する。**



**②責任の文書化**

**⇒ 責任の範囲や境界を明確にすることが重要。**

**責任範囲を明確にし、文章化を実施する。**



**効果的な統制フレームワークは、明確な役割と責任、プロセス制御セキュリティのリスク管理についての最新のポリシーおよび標準を明確にし、このポリシーおよび標準が守られることを保証する。**

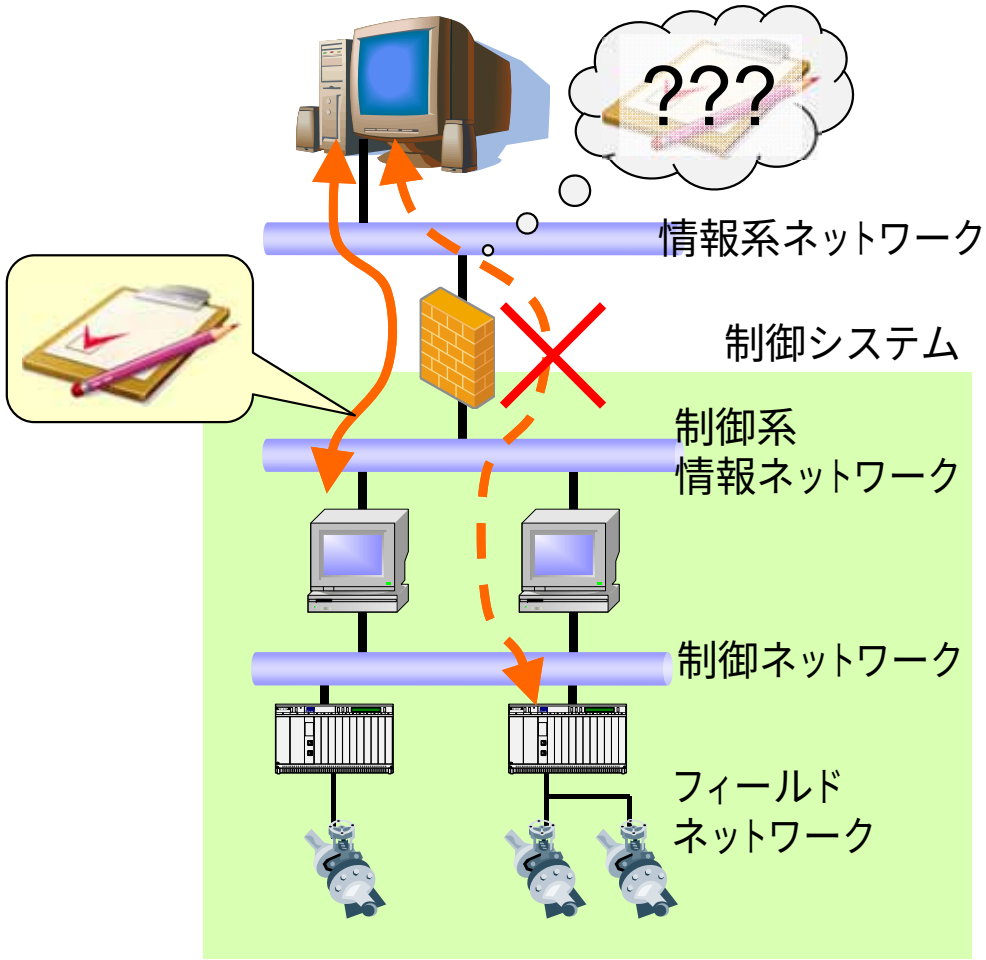
# おすすめセキュリティ施策例 2
# ネットワーク・アーキテクチャ

**設問13: すべてのSCADA/遠隔監視システムへの接続について、業務上の必要性を確認し、それを承認していますか？**

＜原則＞
制御システムとそれ以外のシステム（例えば経営情報系）との接続は、**正当な事業上の理由があるものだけ**にする。

事業上の必要性がない接続は、継続的な監視や検証、メンテナンスの対象として認識されない

脆弱性を抱えたまま放置され、システムへ侵入される足掛かりとなる危険性あり



# おすすめセキュリティ施策例 3
# ファイアウォール

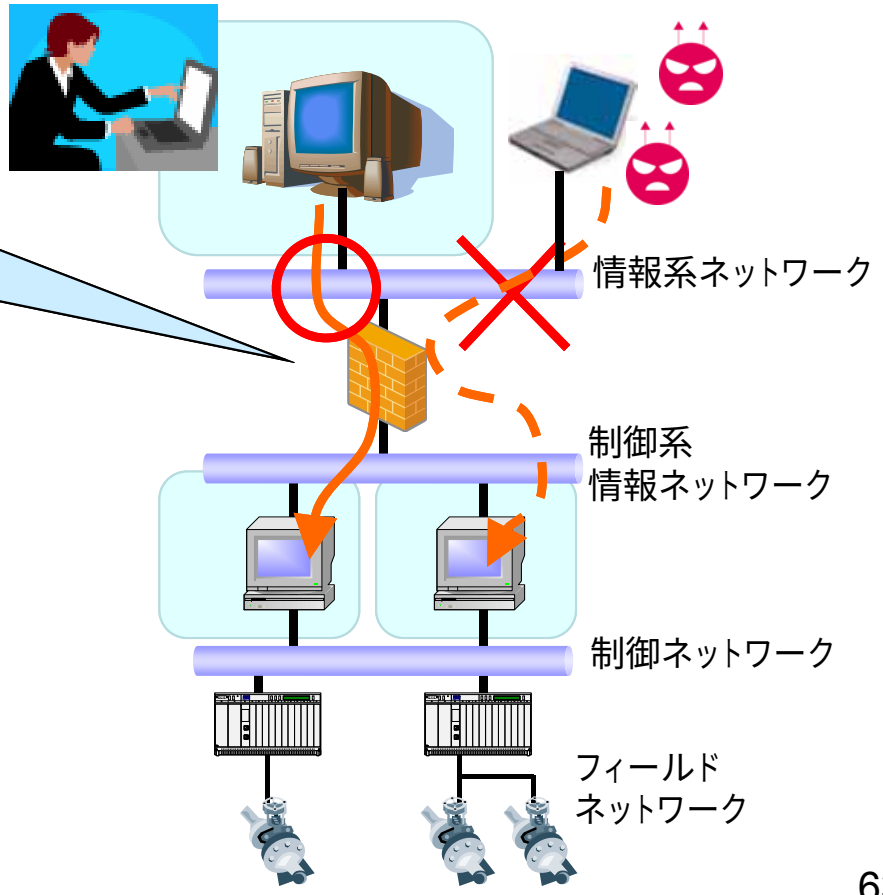
**設問18: 現行のファイアウォール機種で、ベンダか専門家のトレーニングを受けましたか？**

**設問20:ファイアウォールのデフォルトポリシーは「すべての通信を拒否する」にしていますか?**

**＜原則＞**
**制御システムとそれ以外のシステムとの接続は、必要最小限の通信のみ許可し、それ以外は拒否する。**

送受信先アドレスや機能に必要な通信ポートのみに限定し、フィルタをかける。

**設定方法や使用する通信ポート情報に関して、ベンダから情報入手やトレーニングを受けることが望ましい。**



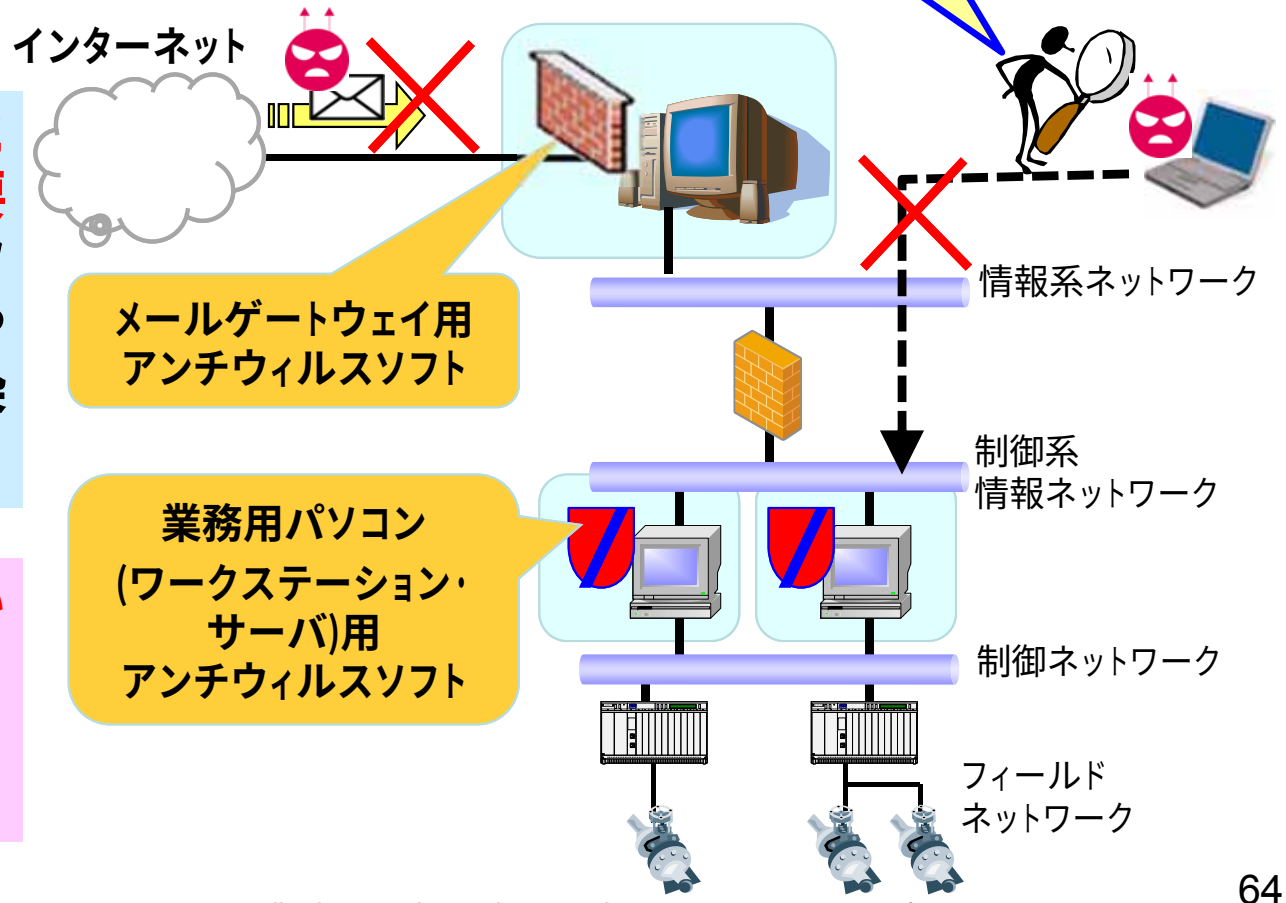
# おすすめセキュリティ施策例 4
# ウィルス対策・機器接続手順

**設問36, 37: 業務用パソコン・メールゲートウェイサーバにアンチウィルスソフトを導入していますか?**

**設問57:機器をSCADA/遠隔監視ネットワークに接続する前に、それらがウイルスやワームに感染していないことを確認する手順がルール化されていますか?**

マルウェアの**侵入／感染経路となる機器やシステム構成上の要となる機器**にアンチウィルスソフトを導入し、マルウェアの侵入や万が一侵入された場合の感染拡大を防ぐ。

アンチウィルスソフトを搭載できない場合（性能上の制約など）、
それに代わる保護対策を検討する
例：人間による監視強化



# おすすめセキュリティ施策例５
# プロジェクトへの参画

**設問89: 制御システムに関連するITプロジェクトの初期段階でSCADA/遠隔監視システムに対して、(プロジェクトが及ぼす)影響があるかどうかを確認するよう義務付けていますか？**

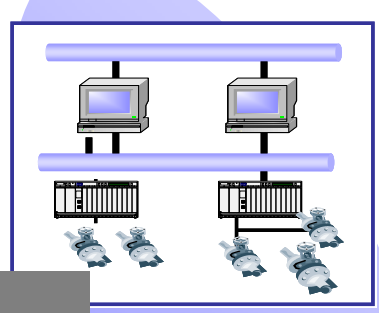
**設問90: プロセス制御セキュリティに関係するプロジェクトでは、プロジェクトライフサイクルを通してセキュリティ問題に責任を持つ責任者（例：セキュリティ・アーキテクト）はいますか？**

**制御システムに関連するITプロジェクト**

**設問89**

＜原則＞
プロセス制御システムに影響を与えるすべてのプロジェクトを特定し、その**開発の初期段階から参画**する。

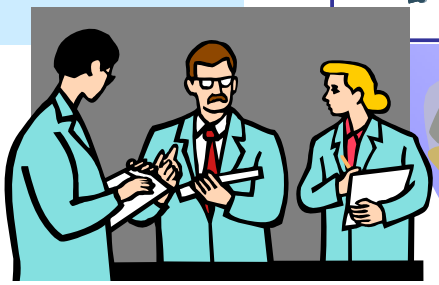
SCADA/
遠隔監視システム

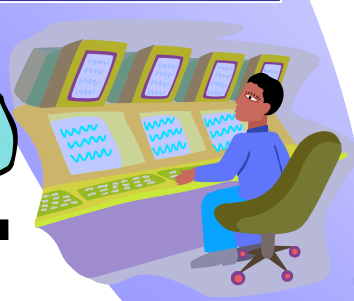


**プロセス制御セキュリティに関係するプロジェクト**

**設問90**

＜原則＞
プロジェクトの全ライフサイクルに渡って**セキュリティ・リスク管理の責任者**となるセキュリティ・アーキテクトを**任命**する。





プロジェクトに関係するプロセス制御セキュリティ・リスクを効果的に管理するために、どのプロジェクトが計画され実施されているか、よく見通せることが必要

セキュリティ要件を、プロジェクト仕様や購入契約書に組み込める能力を持った有識者を配置することが必要

# 付録7) 改良対応例

- 1. 設問の表現を改善する 
- 2. 設問に解説を追加する 
- 3. 難易度の低い要求事項を用意する 
- 4. 目的を明示して代替施策を検討しやすくする 

# 付録7) 改良対応例

## ● 1. 設問の表現を改善する

### 設問68

- SCADA/遠隔監視チーム内に、何らかの注意喚起プログラム/活動/計画（一般的なプロセス制御セキュリティ意識、警戒すべき事柄と対処法、プロセス制御セキュリティ障害とその影響の例など）はありますか？

表現をより具体的に改善

- SCADA/遠隔監視チーム内で、定期的に制御システムにおける障害時の影響や対処方法、セキュリティ意識の向上を目的とした取り組みを行なっていますか？

# 付録7) 改良対応例

## ● 2. 設問に解説を追加する

### 設問2

- 安全管理責任者はシステムの事業リスクを、定められた手順に則って評価していますか？(例：リスクの発生の可能性とリスクが発生した結果として予想できる影響でリスクを表します)

**解説文書への参照を追加**

- 安全管理責任者はシステムの事業リスクを評価していますか？（リスクは、制御システムにおいて脅威が発生した際に生じる結果を指します。詳しくは Good Practice Guideline No.1の 3.4.2事業リスクの評価の項目を参照してください）

# 付録7) 改良対応例

## ● 3. 難易度の低い要求事項を用意する

### 設問47

- 運用責任者はSCADA/遠隔監視ネットワークサーバのオペレーティングシステムに対して、ベンダがパッチを公開してから**３０日以内に適用**していますか？

**条件を緩和した項目を追加**

- 運用責任者はSCADA/遠隔監視ネットワークサーバのオペレーティングシステムに対して、ベンダがパッチを公開した場合に**パッチ適用の必要性を検討**していますか？

# 付録7) 改良対応例

## ● 4. 目的を明示して代替施策を検討しやすくする

### 設問56

- SCADA/遠隔監視スタッフは**BS7858: 2006標準またはCPNIの人事ガイダンスに従って**採用していますか？

**目的を明示して代替施策を提示**

- **制御システムのもつ重要性や特異性を理解したスタッフを採用するために、社内外の人事セキュリティ基準や規定**を準備していますか？