2011年2月10日個別講演2-4(30 min.)
情報セキュリティカンファレンス2011_発表資料


# 制御系システムの「回復」に関する提案

## ～ GPG「GxP法規制コンピュータシステムの運用」を参考に～

2011年2月10日

ITエンジニアリング株式会社

製薬ソリューション部　横井 昭彦

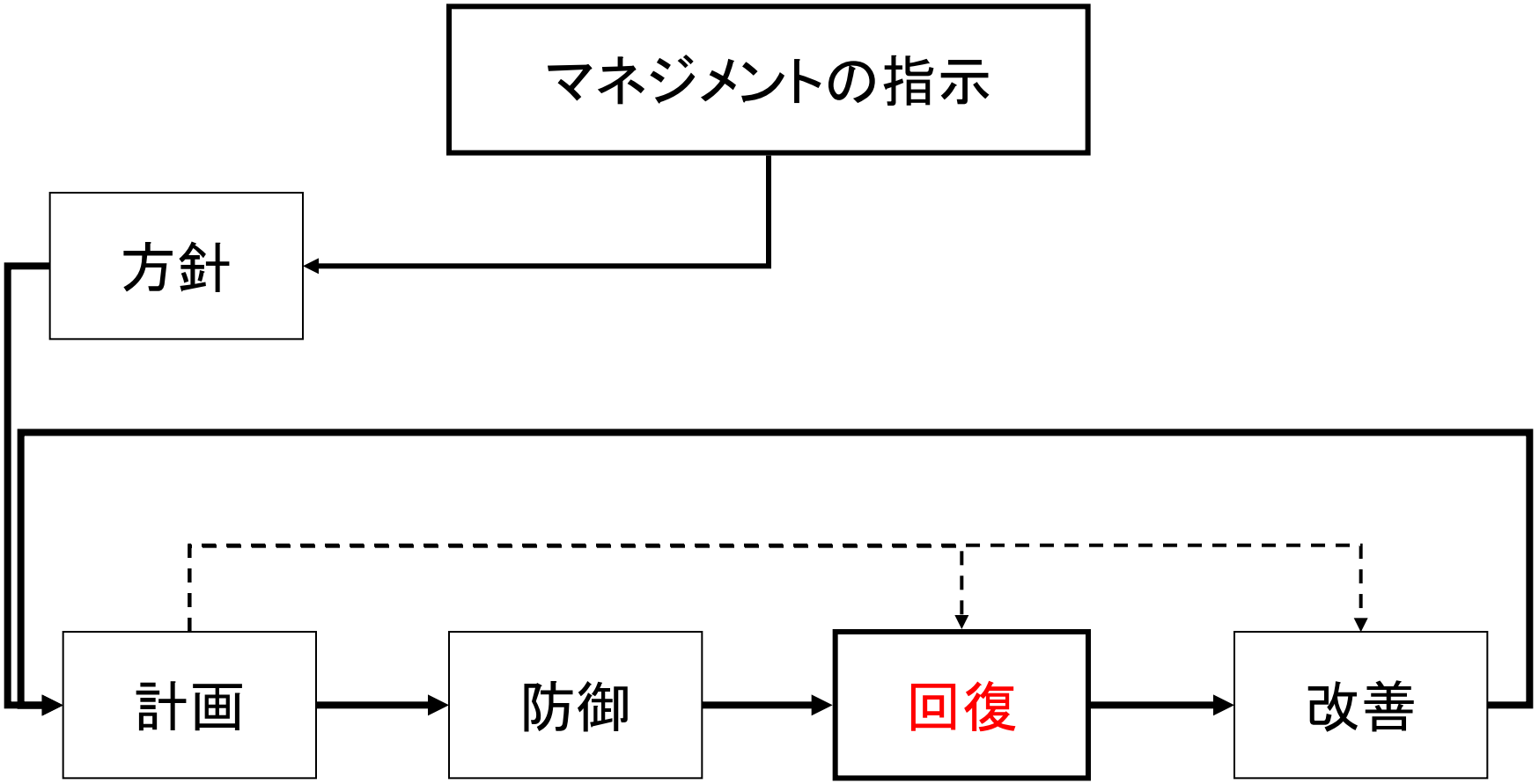
★

# 目　次



★

# セキュリティ管理サイクルと回復




★

# セキュリティ管理における重要ポイントの例

- システム台帳の作成・維持
  - 名称、供給者（サプライヤ等）、導入年月
  - システムの概要
  - リスクセスメントの結果
  - 供給者品質レベルの評価

- リスクベースアプローチに基づいた管理
  - 消費者の安全（例えば医薬品では、患者の安全）
  - 製品の品質
  - データの完全性

★

# 医薬品製造とコンピュータシステムの品質保証

- 医薬品製造では、サリドマイド事件に代表されるような悲劇を発生させないために、**「プロセスが意図した目的に適合していることを確認しそれを維持し、確認した結果を文書化すること」**を法規制として各国の規制当局が求める
  - これをバリデーションと呼ぶ

- コンピュータシステムの普及、重要工程への関わりの飛躍的な拡大に対応するためのバリデーション
  - CSV（コンピュータシステムバリデーション）

★

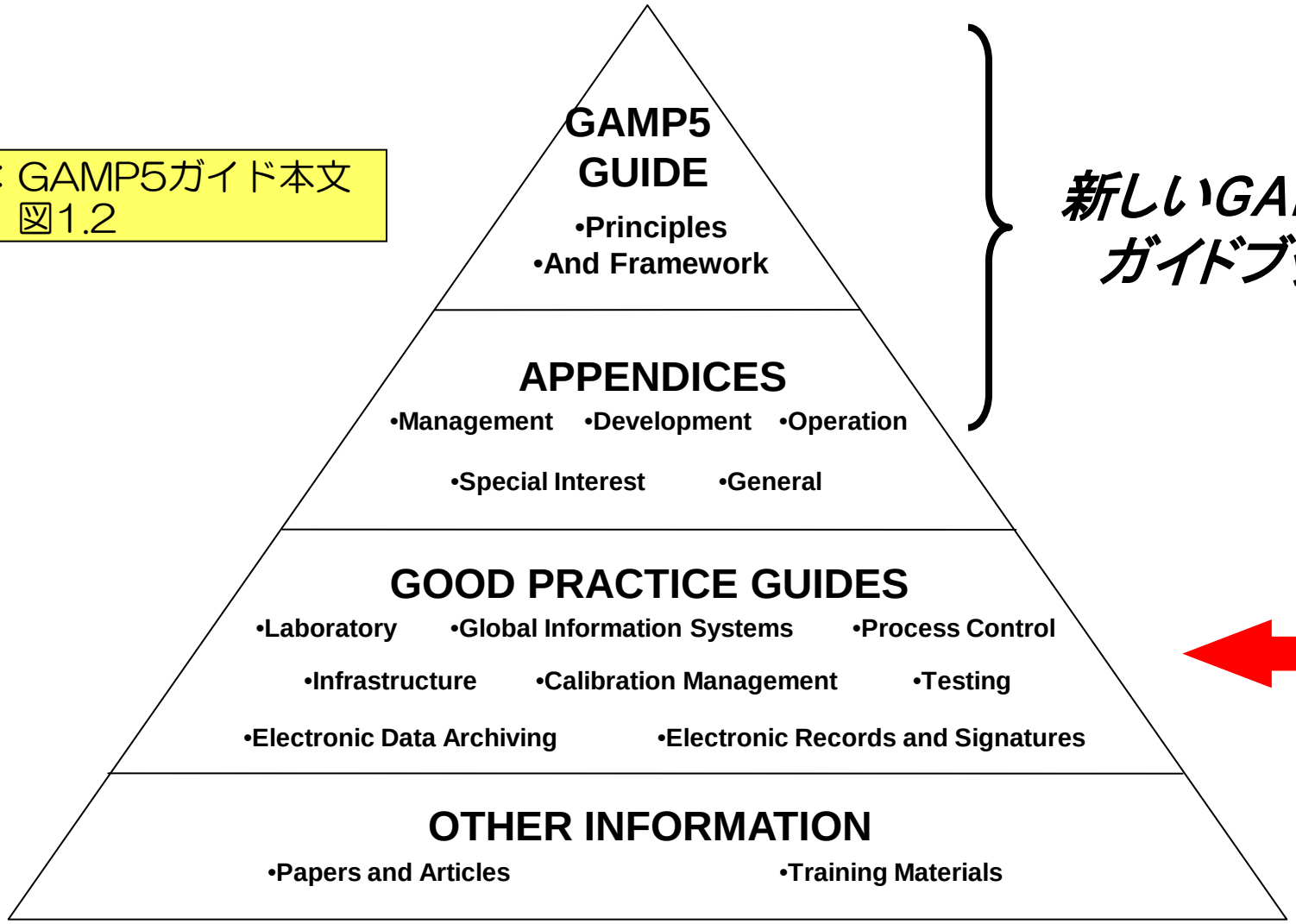
# GAMPガイドとは？

- 医薬品製造に関係するコンピュータ化システムのCSVに関するガイドライン
- 医薬品に関係する国際的なエンジニア団体であるISPE（本部は米国）傘下のGAMPフォーラム(GAMP COP)が発行
- 最新版は2008年2月に発行されたGAMP5ガイド（日本語版は2009年3月に発行）
- セキュリティ管理は付属資料O（運用）の１１に記載

★

# GAMP5ガイドの文書体系とGPG

出典：GAMP5ガイド本文
図1.2




新しいGAMP5
ガイドブック

★

# 「運用フェーズにおけるCSV」 GPGの紹介①

- 正式名称は、GAMP Good Practice Guide “A Risk-Based Approach to Operation of GxP Computerized Systems”

  A Companion Volume to GAMP5

- 医薬品製造に関係するコンピュータシステムのCSVでも運用フェーズに特化した解説書

- 英語版は2010年に発行、日本語版は2011年4月に発行の予定

★

# 「運用フェーズにおけるCSV」 GPGの紹介②

- コンピュータシステムの回復については、14章「BCP (Business Continuity Management)」にて解説

- セキュリティ管理については、 15章「Security Management」にて解説

- 本GPGにて、BCPのサブセットと規定する「DRP(Disaster Recovery Planning)」には『回復』に関係する記述が含まれる

★

# 「運用フェーズにおけるCSV」 GPGの紹介③

- 本GPG14章では、BCP（ビジネス継続計画）とDRP（災害復旧計画）を、以下の内容と規定
  - BCPでは、自然災害や騒乱等への対応は一般的なビジネス継続管理に任せて、法規制対応や公衆衛生に関する場合に限定した継続計画と規定
  - BCPは、業務・作業プロセスをベースに検討⇒プロセスオーナの所掌
  - DRPは、コンピュータシステムがベースに検討⇒システムオーナの所掌

★

# 「運用フェーズにおけるCSV」 GPGの紹介④

- 本GPG14章では、BCP以下の２つの活動を定義
  - Fail-Over
    - 通常業務プロセスから代替業務プロセスへの切替
    - 具体的には、手作業、紙記録による作業、あるいは代替コンピュータシステムを利用した作業
  - Fail-Back
    - 代替業務プロセスから通常業務プロセスへの復帰

★

# 「運用フェーズにおけるCSV」 GPGの紹介⑤

- 本GPG14章では、DRPの内容と文書化について、次のように記述
  - DRPは各システム別に実施すべき内容が異なることから、個別に文書化すべき
  - 文書化では、以下の内容を含むべき
    - 方針、範囲、責任
    - （前提条件、相互依存を含む）退避、復旧の手順
    - 構成管理の変更
    - 環境、データベースとの同期
    - 復帰後の確認と記録の文書化
    - 承認およびリリース

★

# 目　次



★

# 回復フェーズの特徴

- コンピュータシステムの回復は、セキュリティに起因した場合でも、設備や構成要素の故障等他の理由による回復と基本的に同一の内容

- 回復（復旧）は以下の手順をとるのが一般的
  - 隔離された小規模な範囲での性能確認から開始して、次第に規模を拡大
  - 工場系での特徴
    - 現場レベルの性能確認から開始して、段階的に上位系（MES,ERP等）へ拡大
    - 一番最初のステップは手動運転による確認

★

# 回復作業の実施において必須となる文書

- 該当するコンピュータシステムの一覧表
  - 厚生労働省ガイドラインでは「システム台帳」
- 対象システムの回復に関する計画書
- 対象システムに関するリスクアセスメント結果を考慮した操作手順書(SOP)

★

# 回復作業開始前に実施すべき作業

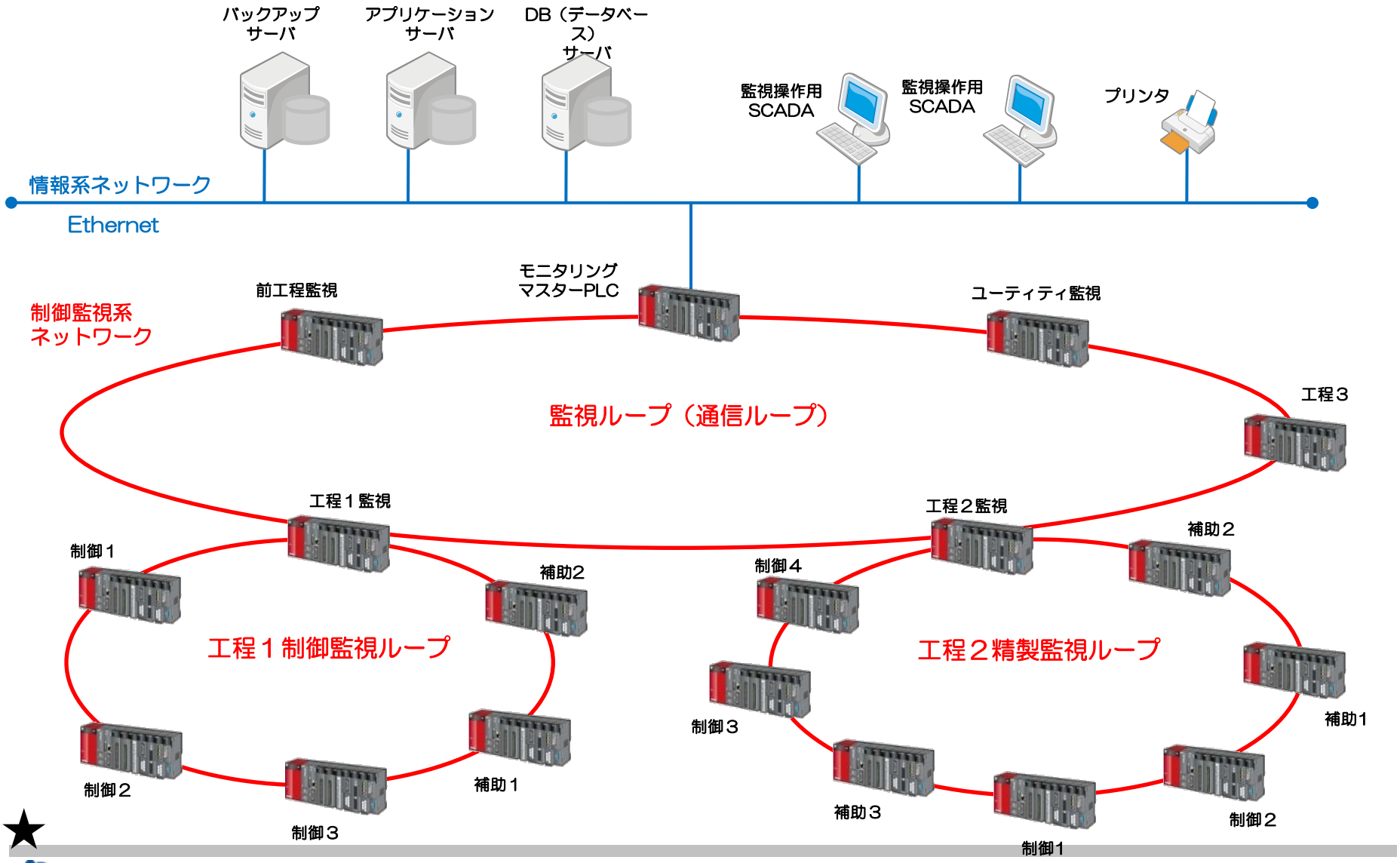
・汚染された装置の入替

・正常ソフトウエアの再インストール

・手動運転による装置動作の確認

★

# 本講演で想定したモデルシステムの構成



# 本講演で想定したモデルシステムの概要

- 複数のPLCからなる制御ブロックが複数存在（全体では数十台のPLC）
  - 工程１～y、ユーティリティ、通信ループ
- SCADAを内蔵する管理用PCが上位PCとして全工程を管理・制御
- 管理用PCは、上位システム（MESのような製造管理システム、またはERPのような業務管理システム）とのインタフェースも有する

★

# モデルケースにおける回復の手順①

- 【手順１】最初に回復させる工程xと通信ループとの接続を解除
- 【手順２】 工程xで回復する機能（PLCの該当するモジュール）＜⇒機能Aと規定＞を選定
- 【手順３】機能Aに関して、手動運転で動作の健全性を確認

★

# モデルケースにおける回復の手順②

- 【手順４】機能Aに関して、PLCの単機能運転で健全性を確認
- 【手順５】機能A以外の工程xの機能を手動運転で動作の健全性を確認
- 【手順６】機能A以外の工程xの機能をPLCの単機能運転で動作の健全性を確認

★

# モデルケースにおける回復の手順③

- 【手順７】工程xの全機能に関して、工程x 内PLCの統合運転で健全性を確認
- 【手順８】１～yでのx以外の工程およびユーティリティについても、手順１から手順７と同じ手順で健全性を確認
- 【手順９】通信ループについても、手順１から手順７と同じ手順で健全性を確認

★

# モデルケースにおける回復の手順④

- 【手順10】工程1～y、ユーティリティと通信ループを接続
- 【手順11】上位PCを起動して、健全性を上位PC単独で確認
- 【手順12】上位PCと全てのPLCを対象として、健全性を確認

★

# 回復作業で必要な文書類

- 構成する各PLCに関する資料
  - 機能一覧表
  - モジュールの一覧と機能対応表
- 回復作業に関するSOP（標準操作手順書）
  - モジュール別に回復する場合には、モジュール別SOPも必須
- DRP（災害復旧計画書）および関係する作業手順書

★

# 目　次



★

# 説明責任

- セキュリティを含む各種管理業務では、「方針に従ってきちんと実行されている」と説明できることが重要ではないか？
  - 絶対的に実施・維持すべき事項が存在
    - ＩＤ・パスワードに関する従業員の教育
  - ビジネス上のリスクとコンプライアンス対応を両立させる管理体制の実現（継続的な改善活動が有効）

★

# リスクアセスメントに基づく管理

- 説明責任をコストインパクト最小で実現するには、リスクアセスメントに基づく管理が最も有効
  - 方針管理へのリスクの明記
  - 客観的な評価指標に基づくリスクの算出
    - 固有技術の専門家との協調

★

# GPG「ＩＴインフラ管理」の6.3章

- 情報セキュリティの目的
  - 機密性：情報は権限のある要員だけがアクセス可能であることを保証
  - 完全性：情報の正確性と完全性、および処理方法の保護
  - 可用性：権限のあるユーザが、情報とその関連するリソースに必要に応じてアクセスできることの保証

- 情報セキュリティ管理項目の例
  - セキュリティ事象管理
  - 侵入検知
  - サーバの強化（例えば、不要なアプリケーション・ツールの削除、および未使用ポートの閉鎖）
  - ウイルス定義ファイルの更新
  - ソフトウエア入手先の考慮（例えば、承認されているサプライヤから）
  - 災害復旧計画
  - ユーザアクセス管理

★

# お問い合わせ先

ITエンジニアリング株式会社

〒221-0031　横浜市神奈川区新浦島町1-1-25

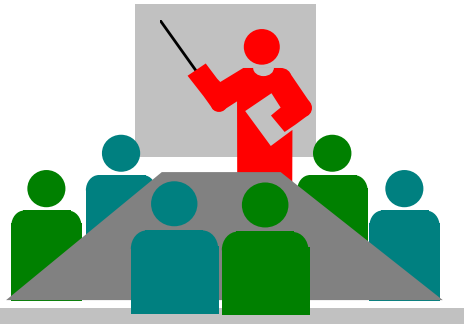
ﾃｸﾉｳｪｲﾌﾞ 100ビル

製薬ソリューション部

横井　昭彦　yokoi@ite.co.jp

TEL:045-441-9055,　FAX:045-441-9130

URL: http://www.ite.co.jp/



★