Formative System Engineering

信頼関係に基づくシステムセキュリティの構造記述

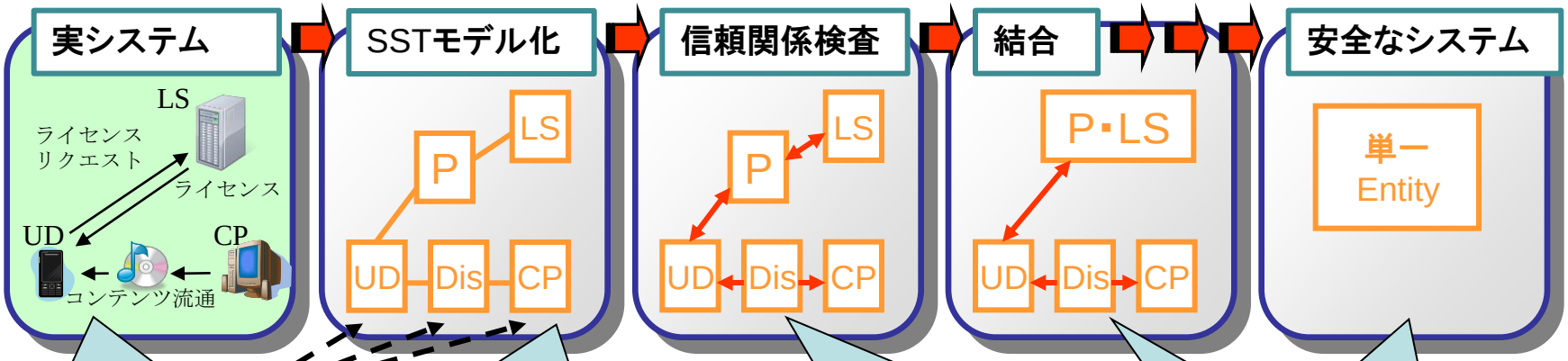
多くのシステムセキュリティ事故・犯罪⇒安全なシステム開発は難しい…なぜ？

脆弱性の発見が困難	⇒ システムが複雑。脆弱性は隠れている。
安全性の理解が困難	⇒ 要件が曖昧。検証が困難。

システムのセキュリティの状態を明確に表現し解析する方法が要求される

システムセキュリティ記述・解析法(System Security on Trust)の開発

SST適用例



デジタル・ライツ管理システム
- LS:ライセンス・サーバ
  コンテンツ利用ライセンス販売
- UD:ユーザ・デバイス
  ライセンス購入、コンテンツ利用
- CP:コンテンツ・プロバイダ
  コンテンツ(ゲーム等)作成・流通

識別子(認証データ)
- 秘密情報
- 資格提示系
- 信用検証系
- 隣接情報

SST図
システム要素(プロセス、通信、ユーザ)はすべてEntity

Entity
SST図は、Entityを接点、隣接関係を辺としたシステムグラフ

信頼関係(相手を信頼するとは)
- 相手の認証データが十分な強度
- 情報交換のたびに継続的に認証可能(相手の資格提示系のデータを信用検証系で検証可能)
- 資格提示系のデータに実時間要素が含まれる

Entityの結合
- 隣接するEntity同士が相互に信頼関係にある場合、Entityを結合し一つのEntityとして扱う

安全性検証
- すべてが結合できれば安全
- あるEntity Aから信頼できないEntityはAからは脆弱性がある(別Entityに置換え可)