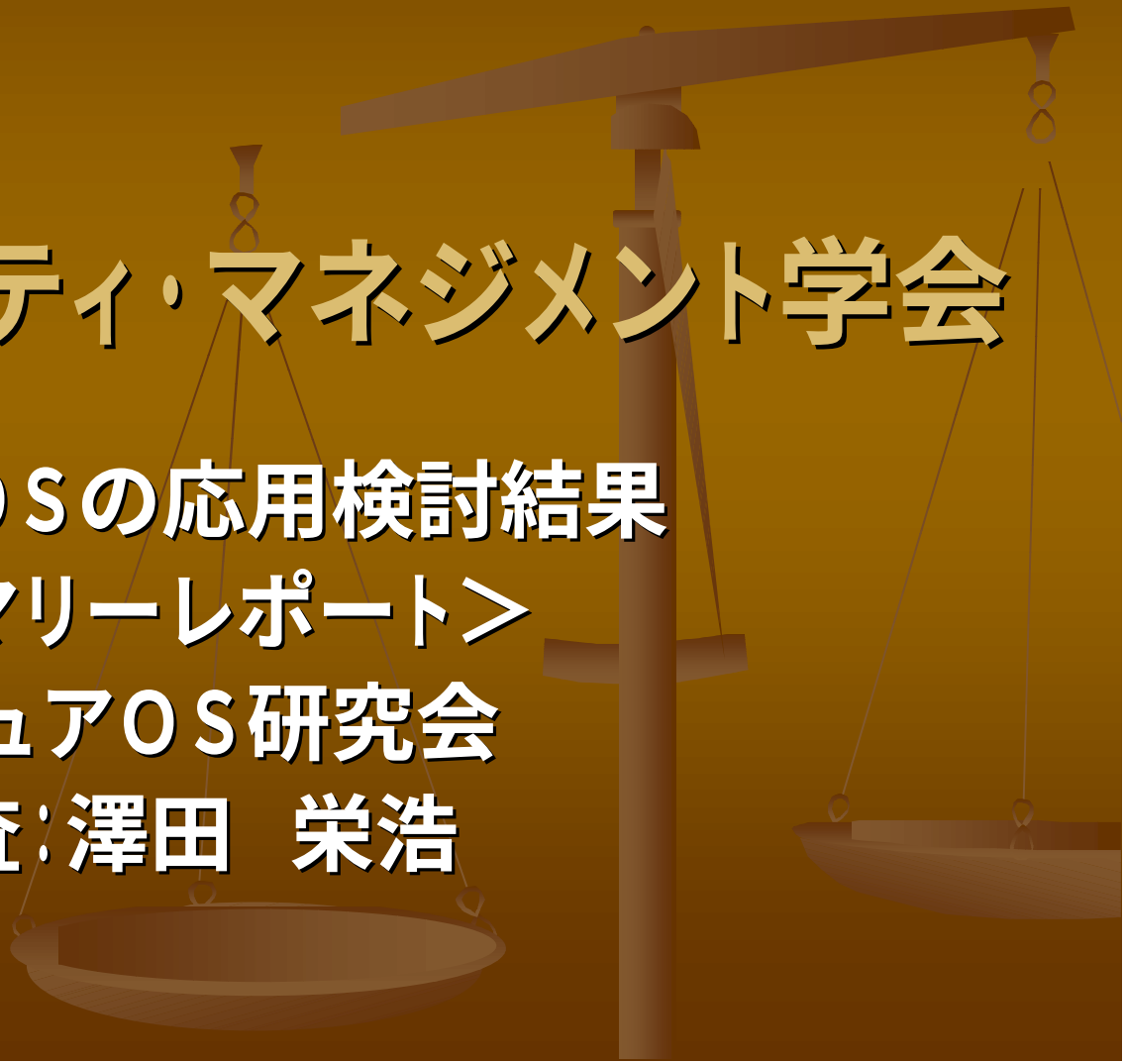
第4回セキュアＯＳカンファレンス



日本セキュリティ・マネジメント学会

セキュアＯＳの応用検討結果
＜サマリーレポート＞

セキュアＯＳ研究会
主査：澤田　栄浩

研究会メンバーのご紹介

- 金子 敏信、大井 正浩、石崎 靖敏、富山 茂、中根 勝行、青木　信義、一瀬 智司、田場 和弘、鮫島 吉喜、中本　雅寛、田吹 隆明、三浦 大像、松原 克弥、長谷川 誠志、橋本 真智子、伊藤 昇、山内 直樹、和田 康、原田　季栄、橋本 純生、清水 惠子、川口 元、力 利則、高橋 陽一、五十嵐 智、松並　勝、佐藤　祐介、済賀　宣昭、森住　哲也、河本　高文、木村　隆幸、山口　義一、沼口 大輔、桝本圭株、佐瀬　泰紀、福井　淳、澤田 栄浩

第4回セキュアＯＳカンファレンス

組込系システムへの セキュアOS応用研究

ワーキング･グループ　1
幹事：鮫島　吉喜

情報機器の広がり


産業向け
センサ
鉄道車両
PBX
バックボーンルータ
工業機械
POS端末
医療機器
自動車
複合機
PCサーバ
組込み機器
PC WS
白物家電
ゲーム機
ホームルータ
家庭用プリンタ
携帯電話
PDA
DVD/HDレコーダ
ノートPC
消費者向け

組込みシステムへの脅威

- 常時電源ONでウィルス感染、攻撃を受ける可能性が高い
  - 携帯機器では無線で知らない間に接続、攻撃される可能性が高い
  - ウィルス対策ツールが普及していない
  - 自動更新が一般的ではない
- Cやアセンブラの割合が高く、脆弱性を作りこみやすい
- 電話番号や写真などのプライベートな情報が多い
- 自動車や医療機器では、攻撃が人命に直接かかわる
- 利用者のセキュリティに対する意識が低い

組込みシステムの分類
(機器制御型)

- 高信頼性、高リアルタイム性を要求される
- ハードウェアリソースに余裕がない
- μITRONやVxWorksなどスレッド系OSで、メモリ保護機能がない
- 自動車の制御系、白物家電、医療機器など

組込みシステムの分類 (コンテンツ処理型)

- 映像やテキストのコンテンツ処理中心
- 多機能、操作性の良さが求められる
- 比較的ハードウェアリソースに余裕がある
- Linux、Windows、Symbianなどメモリ保護機能がある
- 携帯電話、DVDレコーダ、カーナビなど

機器制御型の対策

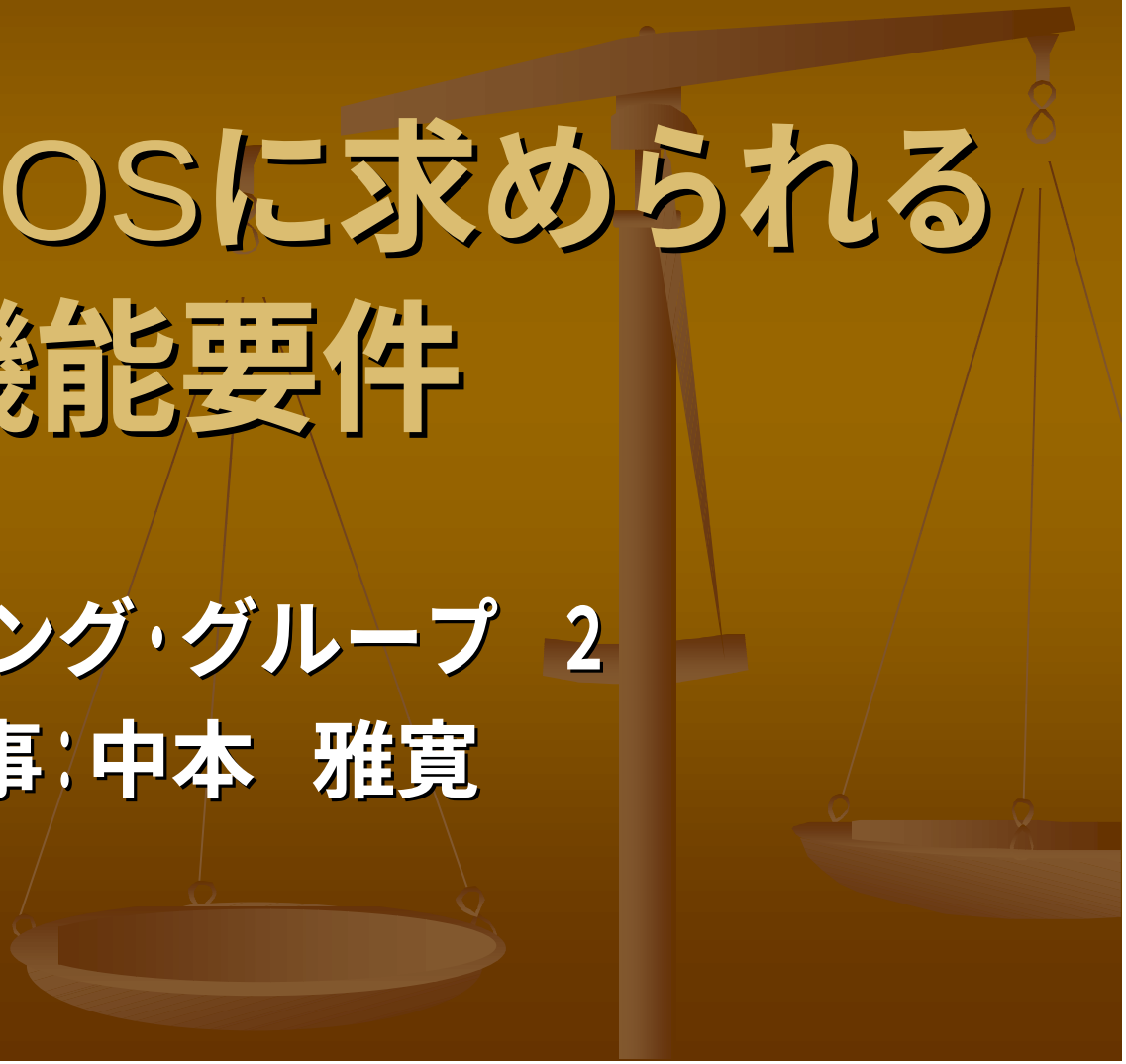
- 脆弱性を作りこまない開発プロセスの作成
  - 要件定義: 脅威が発生しにくい仕様にする
    - 便利だが、悪用されやすい機能を落とす
    - データのサイズの制限/固定
  - 脅威の洗出し: 対策の優先度付けの材料にする
    - 攻撃の種類や手法、攻撃者の意図
    - 攻撃者の意図やメリット、攻撃のコスト
  - 設計: ユーザ認証、暗号化、アクセス制御等の機能要件
  - 実装: セキュアプログラミング、ツールによる検査
  - テスト: 既存の攻撃、規定外データによるテスト
  - 開発チームやセキュリティの専門家によるレビューが重要

コンテンツ処理型の対策

- 既存の対策
  - 脆弱性を作りこまない開発
  - 攻撃対策ツールの利用: libsafeやStackGuardなどのバッファオーバフロー攻撃対策
  - 仮想マシンの利用: ダウンロードプログラムの安全な実行
- これからの対策
  - セキュアOSの利用
    - 強制アクセス制御、最少特権
    - 被害範囲の限定と踏み台(ボット)化防止
  - 仮想化技術の利用
    - 一つのCPU上で複数のOS: リアルタイムOSと汎用OS
    - 用途に応じてOSごと分離、ウィルス侵入や情報漏洩を防止

第4回セキュアOSカンファレンス

セキュアなOSに求められる機能要件



ワーキング・グループ　2
幹事：中本　雅寛

背景・目的

- 特定課題とは?
  - 電子政府システムに求められるセキュアなOSの機能要件の調査
- 背景
  - 電子政府システムに求められるOSのセキュリティ機能
    - 国民の個人情報、重要な情報資産を扱うシステム
    - 機密性、データ完全性、共に重要要件
- 目的
  - セキュリティについて、OSとして出来ること、すべきこと、の明確化
    - システム基盤(OS)で提供できるセキュリティ機能を探る
    - セキュリティ要件を明確化する方法
    - どの程度、セキュリティを実現すれば良いのかの指標を探る

データ

- 主に調査･研究対象として以下を参照した。
  - Trusted Computer System Evaluation Criteria (TCSEC)
    - DoD 5200.28-STD
  - 及び、Rainbow Series Library
  - Common Criteria for Information Technology Security Evaluation (CC)
  - OS関係のCC　Protection Profile
  - CIM (Consistency Instruction Manual for development of US Government Protection Profiles)

米国政府機関作成のProtecion Profile(1)

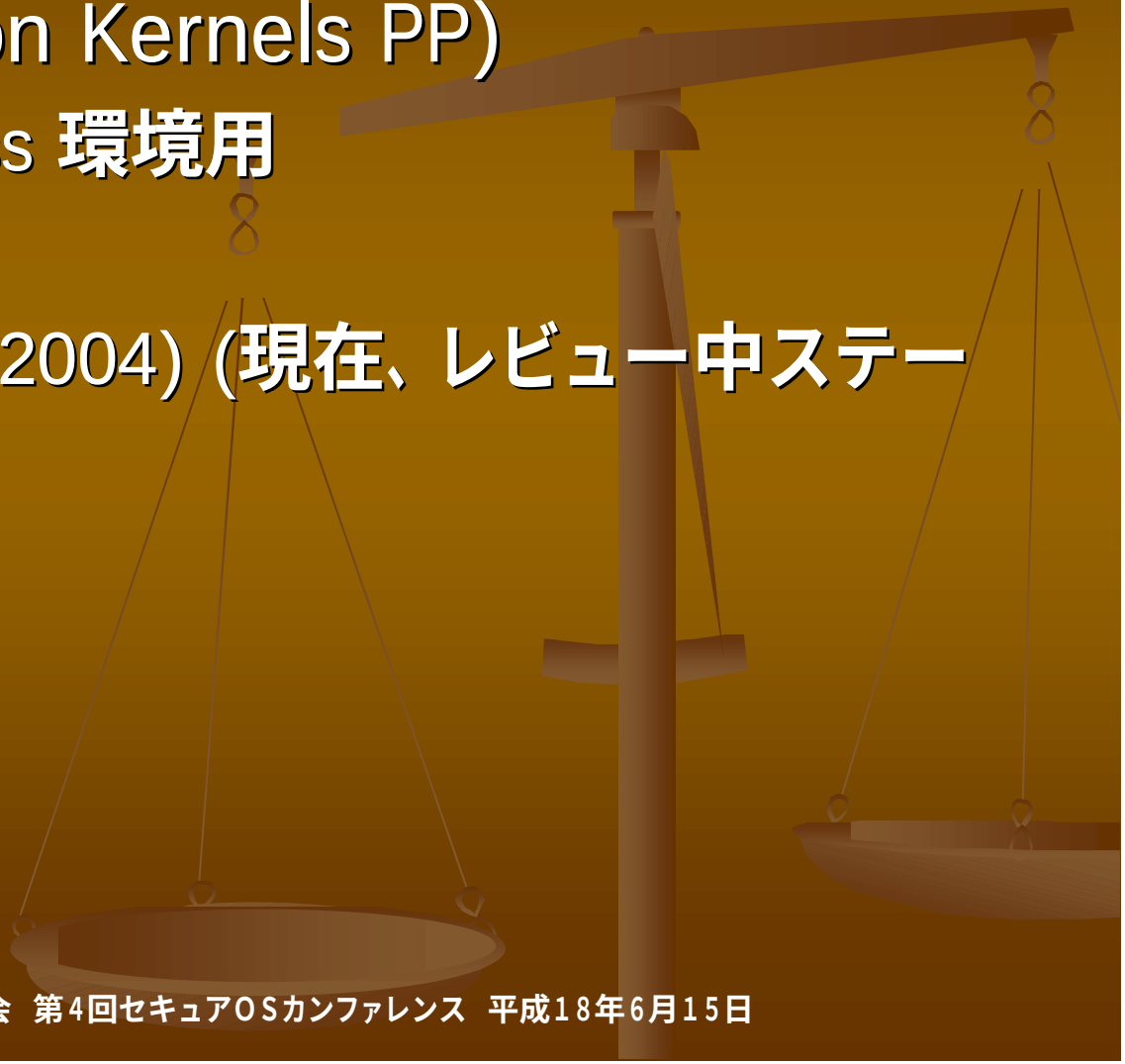
- CAPP (Controlled Access PP) Ver.1.d (Oct./1999)
  - TCSEC C2クラスをCCスキームへ移行版
- LSPP (Labeled Security PP) Ver.1.b (Oct./1999)
  - TCSEC B1クラスをCCスキームへ移行版
- RBACPP(Role-based Access Control PP) Ver.1.0 (Jul./1998)
  - NIST作成
  - FC(Federal Criteria) CS3プロファイルのCCスキーム移行版。
    - Minimum要件のみ記述

米国政府機関作成のProtection Profile(2)

- SLOSPP(Single-Level OS PP)
  - Medium Robustness 環境用
  - シングルレベルセキュリティ環境のOS用PP
  - Ver.1.22 (Jun./2001)　(リリース版)
    - EAL 4+ (CC 2.1)
  - Ver.1.67 (Oct./2003)　(現在、レビュー中ステータス)
    - EAL 4 (CC 2.1)
- MLOSPP(Multi-Level OS PP)
  - Medium Robustness 環境用
  - マルチレベルセキュリティ環境のOS用PP
    - 機密性とデータ完全性についての情報フロー制御の要件
  - Ver.1.22 (May./2001)　(リリース版)
    - EAL 4+ (CC 2.1)
  - Ver.1.68 (Feb./2004)　(現在、レビュー中ステータス)
    - EAL 4 (CC 2.1)

米国政府機関作成のProtecion Profile(2)

- SKPP (Separation Kernels PP)
  - High Robustness **環境用**
  - **仮想環境用**　PP
  - Ver0.621　(Jul./2004) (**現在、レビュー中ステータス**)



その他OS用Protection Profile

- BSI(ドイツ)作成のP.P.
  - Discretionary Information Flow Control (SU) V.2.01 (Sep./2002)
  - Discretionary Information Flow Control (MU) V.2.01 (Sep./2002)
    - セキュリティ要件に応じた情報フロー制御のルールによる防御。
- 韓国作成のP.P.
  - Label-based Access Control System Protection Profile for Government V1.0 (Feb./2004)
    - US IATF、LSPP, MLOSPPを参照している。

日本のCommon Criteriaに対する取り組み

- ISO/IEC 15408
  - JIS X　5070 (2000年)
    - 情報セキュリティ認証・評価制度体制(JISEC)
- 「政府機関の情報セキュリティ対策のための統一基準(2005年12月版(全体版初版))」
  - 「情報システムのセキュリティ責任者は、構築する情報システムに重要なセキュリティ要件があると認めた場合には、当該情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書(ST:Security Target)のST評価・ST確認を受けること。(後略)」

MLOSPP V1.68

- **選択理由**
  - MAC (強制アクセス制御) 要件
    - CAPP ← TCSECのC2クラス
    - *LSPP ← TCSEC B1クラス*
      - *BLPモデル*
  - MIC (強制完全性制御) 要件
    - *Bibaモデル*
  - CCスキーム下で新規に作成
    - COTS(Commercial-off-the-Shelf)戦略
    - 暗号技術要件に対応
    - *MLOSPP ← LSPPベース*
      - SLOSPP ← CAPPベース
  - V1.22 vs V1.68
    - V1.22は正式リリース版。V1.68はレビュー中ステータス。
    - **V.1.68の記述が技術的により適切**

(参考)LSPPとMLOSPPの機能要件比較

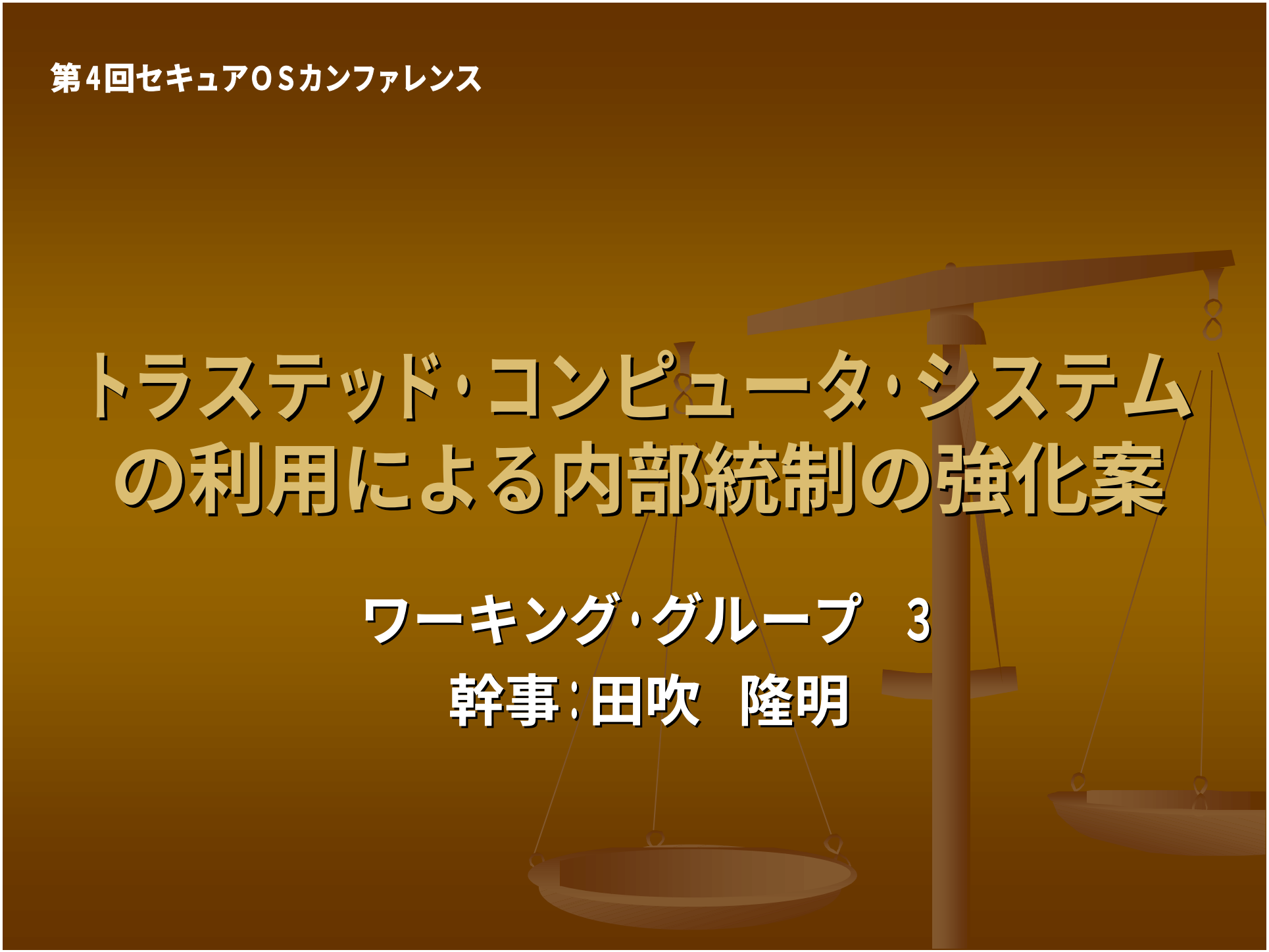
- CC(V 2)のセキュリティ機能要件 の対応

機能要件	LSPP	MLOSPP
Security Audit (FAU)	○	○
Communication (FCO)	–	–
Cryptographic support (FCS)	–	○
User data protection (FDP)	○ (MAC)	○ (MACとMIC)
Identification and authentication (FIA)	○	○
Security management (FMT)	○	○
Privacy (FPR)	–	–
Protection of the TOE functions (FPT)	○	○
Resource utilization (FRU)	–	○
TOE access (FTA)	–	○
Trusted path/channels (FTP)	–	○

利用環境によって異なるPP機能要件

- マルチユーザとシングルユーザで求められる環境は違うはずであり、プロテクションプロファイルも違ってくるようである
- TCSECやMLOSーPPはマルチユーザ、マルチクラシフィケーション（情報格付けが2つ以上に分かれている）システムが対象である
- SLOS-PPはマルチユーザ、シングルクラシフィケーションでは有効

第4回セキュアOSカンファレンス



トラステッド・コンピュータ・システムの利用による内部統制の強化案

ワーキング・グループ　3

幹事：田吹　隆明

WG3 の目的

- 監査の視点からの　トラステッド・コンピュータ・ システム を検証
- Sarbans Oxley 法 (SOX法) 及び日本版SOX法案の要求事項と　トラステッド・コンピュータ・システム の関連の検討

TCSEC及び監査ガイド

［1］ DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA , DOD 5200.28-STD December 26, 1985,

邦訳 日本セキュリティマネジメント学会 セキュアOS研究会

http://www.jtsl.co.jp/japanese/lab/society/tcsec.pdf

［2］ A Guide to Understanding Audit in Trusted System, National Computer Security Center, NCSC-TG-001, Library NOS-228,470, 28 July 1987

TCSECによるトラステッド・システムの監査についてのガイド

日本版SOX法

- 平成17年12月8日に企業会計審議会内部統制部会

「財務報告に係る内部統制の評価及び監査の基準のあり方について」

- 構成
  - Ⅰ内部統制の基本的枠組み
  - Ⅱ財務報告に係る内部統制の評価及び報告
  - Ⅲ財務報告に係る内部統制の監査

内部統制の基本的枠組み

- COSOフレームワークを利用
- 目的

  ①有効性、効率性　②財務報告の信頼性　③法令の遵守

  ④資産の保全
- 基本要素

  ①統制環境　②リスク評価と対応　③統制活動

  ④情報と伝達　⑤モニタリング（監視活動）

  ⑥ITへの対応

ITへの対応

- 内部統制の評価と報告
  - 全社的内部統制
  - 業務プロセスに係わる内部統制の評価
    - 業務処理統制：業務アプリケーション
    - 全般統制：ITインフラ
  - 財務報告に係わる内部統制の監査
    - 「内部統制報告書」→監査人の評価→「内部統制監査報告書」

ITの内部統制確保のポイント

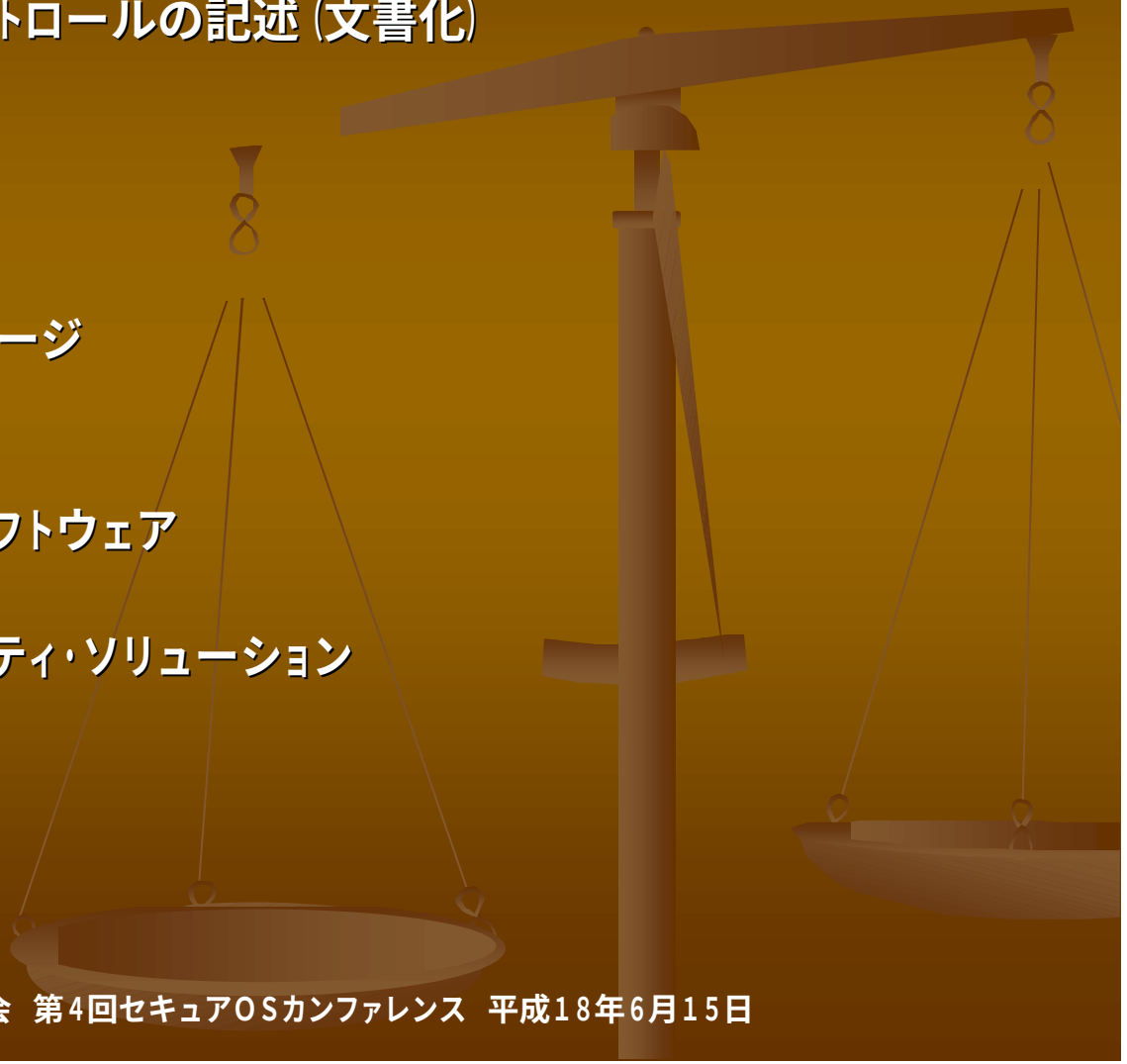
- 今日の企業のIT環境
  「…必然的に関わる内外のITの利用状況…」
  - ITの統制は外部の接続先と相互に影響する
- 信頼性
  - 適時かつ正確な情報であること
  - 網羅性、正確性、正当性、維持継続性
- 権限と責任の明確化
  - システムオーナのロール（役割と責任）
  - ロール（役割）、ルール（規則）、ルート（経路）

米国の現状と問題点

- 統制上の問題点
  - 不完全な職務分離
  - 会計システムのOSに関するアクセスコントロールの不備
  - 会計システムのDBに関するアクセスコントロールの不備
  - 開発要員が本番環境で本番処理を実施可能
  - 多くのユーザが特権ユーザ権限を行使可能
  - システム文書が実際のプロセスと合っていない
- 改善対策にITの的確な活用が不可欠
- 会計・法律の専門家→ITの専門家が中心的役割

SOX法整備の手順（事例）と問題点

- 実務上の対応：ITの利活用が不可欠
  - ビジネスプロセスとコントロールの記述（文書化）
  - テストと改善
  - 経営者の評価
  - 外部監査人の評価
- ツール等事例
  - IT業務統合管理パッケージ
  - 内部統制評価サービス
  - 文書化支援ツール
  - アイデンティティ管理ソフトウェア
  - ログ解析ツール
  - データベース・セキュリティ・ソリューション
- ストレージ能力の強化
- スプレッドシート問題



現状の問題点

- アクセス権
  - アプリケーション内にアクセスコントロールのロジック、識別と認証を実装

  → プログラムの巨大化による品質への悪影響は？

  → データオーナがアプリケーション自身で良いのか？
- 役割分担と特権管理
  - 現実社会とシステム上の役割･特権が乖離
  - システム管理者特権は特権集合の塊
- アクセス制御
  - 既存のOSでは細かなアクセス制御が事実上困難

TCSEC/ガイドから

C1	C2	B1	B2	B3
・識別と認証 ・任意裁量アクセス制御(DAC) ・データとユーザの分離				
	・監査証跡の生成 ・制御付きアクセス制御 ・ユーザの個別属性			
		・強制アクセス制御(MAC) ・ラベル付きのセキュリティ保護 ・マルチレベル装置への出力		
			・隠れストレージチャネルの利用検出 ・構造化された保護 ・リファレンスモニタ ・最少特権	
				・侵入の検出と記録、耐性

トラステッド・システムとIT統制

- IT統制を支えるトラステッド・システム
  - 識別と認証
    - アプリケーションからOSまで一貫した統制が実現可能
  - モニタリングと記録
    - システムの高度なモニタリング機能、強力な保護機能が監査の信頼性を高める
  - 最少特権及びアクセス制御
    - 特権制御、アクセス制御をアプリケーションから切り離す
    - 現実社会とシステムの特権のギャップがなくなる
  - アプリケーションからセキュリティ機能を分離できる

✓トラステッドOSを用いる場合、初期段階でシステム内、システム間で一貫した統制を設計する必要がある

まとめ：トラステッドOS

① 従来システムよりも内部統制の強化に適している（従来OSでは役割・権限の反映が困難）

② セキュリティ侵害の影響が小さい

③ 内部監査/「内部統制報告書」の信頼性の向上が期待される

内部統制の強化、J-SOX法（案）の要求へのソリューションとして期待される

第4回セキュアOSカンファレンス

ご清聴ありがとうございました