第4回 セキュアOSカンファレンス
虎ノ門パストラル(新館5F マグノリア) B-4 15:30～16:10

Trusted で オープン な内部統制

～ IT業務処理統制における セキュアOSの役割 ～

2006.6.15

インフォコム株式会社
フロンティア事業本部　セキュリティソリューション部
セキュリティソリューショングループ
セキュリティコンサルタント 正木 義和

アジェンダ

1. 弊社 会社概要
2. J-SOX法におけるITのアプローチ
3. 正当性の証明
4. 現在の情報システムの問題
5. 解決に向けての観点
6. システム統制に向けて、セキュアOSの適用
7. セキュアOSがもたらすビジネスリスク回避
8. セキュアOS”PitBull”
9. 最近の実績
10. ロードマップ

弊社 会社概要

- 名称: インフォコム株式会社
- 設立: 1983年 (2001年4月にインフォコム㈱と㈱帝人システムテクノロジーが合併)
- 資本金: 15.9億円 (2002年3月にジャスダック上場)
- 主要株主: 帝人株式会社(50.1%)
- 社員数: 609名(2005年3月)
- 事業内容: 情報通信総合サービス業
- トラステッドOS/セキュアOSへの取り組み
  - 1997年よりトラステッドOSの研究を帝人㈱システム技術研究所で開始
  - 1999年に㈱帝人システムテクノロジーが米国Argus社の総輸入代理店となり、トラステッドOSの先駆者的立場で国内販売を開始。
  - 以後、ハイエンドのサーバ セキュリティ ソリューションとして、e-Japanシステムを初め、中央官公庁、防衛・警察関係機関、国立大学、金融機関、各種企業システム等で多数の導入実績を持つ。

J-SOX法におけるITのアプローチ

PITBULL

J-SOX法におけるITのアプローチ ①

- **米国企業改革法(SOX法)** Sarbanes Oxley Act of 2002
  - 株式の時価総額が 7500万ドルを超える米国籍の米国市場上場企業に適用。時価総額7500万ドル以下の上場企業と、日本やヨーロッパなど外国籍の上場企業には07年から適用

倣って

- **金融商品取引法 (J-SOX法)**
  - 2005年12月　金融庁の企業会計審議会内部統制部会が「財務報告に係る内部統制の評価及び監査の基準案」を公表
  - 2006年06月07日　金融商品取引法　参院本会議 可決 成立した

    ⇒ 適用は、2008年4月1日からの事業年度か？

J-SOX法におけるITのアプローチ ②

SOX法が求める内部統制の整備とは

- **SOX法遵守＝内部統制の整備**
  - 企業改革法対応で先行した米国企業において、最も影響が大きかったのは同法404条が規定している「内部統制」の整備だとされる。
  - しかし法律のどこにも、どうすれば「内部統制」の整備がなされていることを証明する手段を提示してはいない。
- **COSOフレームワークへの準拠**
  - 米国企業改革法によるところの「内部統制」の整備については、COSO（1992年：トレッドウェイ委員会組織委員会）のフレームワークに準拠する。
  - 日本版SOX関連法についても金融庁が公表した基準案に準拠する必要があり、この基準案も“COSOフレームワーク”にならったものである。

J-SOX法におけるITのアプローチ ③

日本の「基準」が示す内部統制の基本的な枠組み

- **金融庁の内部統制に関する定義**
  - 「財務報告にかかる内部統制の評価および監査の基準（案）」における内部統制の定義は、基本的にこのCOSOのフレームワークにならいながら、その目的として「資産の保全」を、構成要素として「ITへの対応」を追加している。
- **ITへの対応**
  - ITに関する記述についてはCOSOフレームワークにおいても、その構成要素に存在しているが、現在の企業経営についてITの利用が不可欠である時代背景を考慮し、基準案については「ITへの対応」という項目が独立した構成要素として追加された。

J-SOX法におけるITのアプローチ ④

ITへの対応について

- **基準案の中での定義**
  - 「基準案」によれば、「ITへの対応」とは、「組織目標を達成するために予め適切な方針と手続きを定め、それを踏まえて、業務の実施において楚々機の内外のITに対し適切に対応すること」と定義され、「IT環境への対応」と「ITの利用と統制」から構成される。
  - 即ち、現在も各企業で運用されている情報システムが内部統制上重要な位置付けにあり、内部統制の整備において、情報システム部門の役割は非常に大きいことを示している。
  - ITへの対応を「財務報告の信頼性」に基づいて考える場合においても、決して経理部門周辺の対応だけでは充分ではなく、営業部門をはじめとする複数の業務部門の全プロセスが統制の対象となる。

J-SOX法におけるITのアプローチ ⑤

「IT業務処理統制」と「IT全般統制」の位置づけ

- **IT業務処理統制**
  - 業務の大部分はアプリケーション・システムによってサポートされている。これらのアプリケーション・システムでは、すべての取引データが過不足なく正確に入力され、処理され、出力されるようになっている必要がある。これを担保する仕組みが「IT業務処理統制」として要求される。
- **IT全般統制**
  - 一方、これらのアプリケーション・システムが業務要件に基づいて開発・運用され、かつ継続的・安定的に稼働することを保証するには、基盤となるシステム・インフラ（ハード、ソフト、ネットワークなど）が適切に管理されている必要がある。複数のアプリケーションに共通する統制を「IT全般統制」と呼び情報システム部門の活動そのもの統制を要求している。

正当性の証明

PITBULL

正当性の証明

情報システム部門の守備範囲

広い守備範囲の中で、正当性を確保する事は
どうすればいいのか？

現在の情報システムの問題

PITBULL

現在の情報システムの問題 ①

現在の情報システム運用の実態

- 運用の外部委託
- アプリの肥大
- ネットワークの複雑さ

全体の把握が出来ていない

“統制”を実現する“下地(基盤)”が未整備

現在の情報システムの問題 ②

対策に向けて

決められた事が、決められた通りに
実施されている事・・・を保証することが近道

例えば・・・
- アプリケーションの動作
- 管理者の操作
- 情報(データ)へのアクセス
- 他システムとのやりとり

} どうすれば、保証になる？

解決に向けての観点

PITBULL

infocom

解決に向けての観点

情報システムの保証

- 情報システム 部門
- 情報システム アプリケーション
- 情報システム 運用者

} ポリシー策定

システムの動作が、本来の目的通りになるようにポリシーを策定し、システムに“与える”事で証明が可能

システム統制に向けて、セキュアOSの適用

PITBULL

infocom

システム統制に向けて、セキュアOSの適用 ①

システムの目的に見合ったポリシー設計

- アプリケーションの動作について
- システム運用管理者の操作について
- 情報(データ)へのアクセスルールについて
- サービス利用者の利用内容について

それぞれのポリシーを厳重に設計
セキュアOSを使って“構築”する → **統制基盤の実現**

“監査”可能な統制基盤の実現により、統制を可能に！

infocom

セキュアOSがもたらすビジネスリスク回避

PITBULL

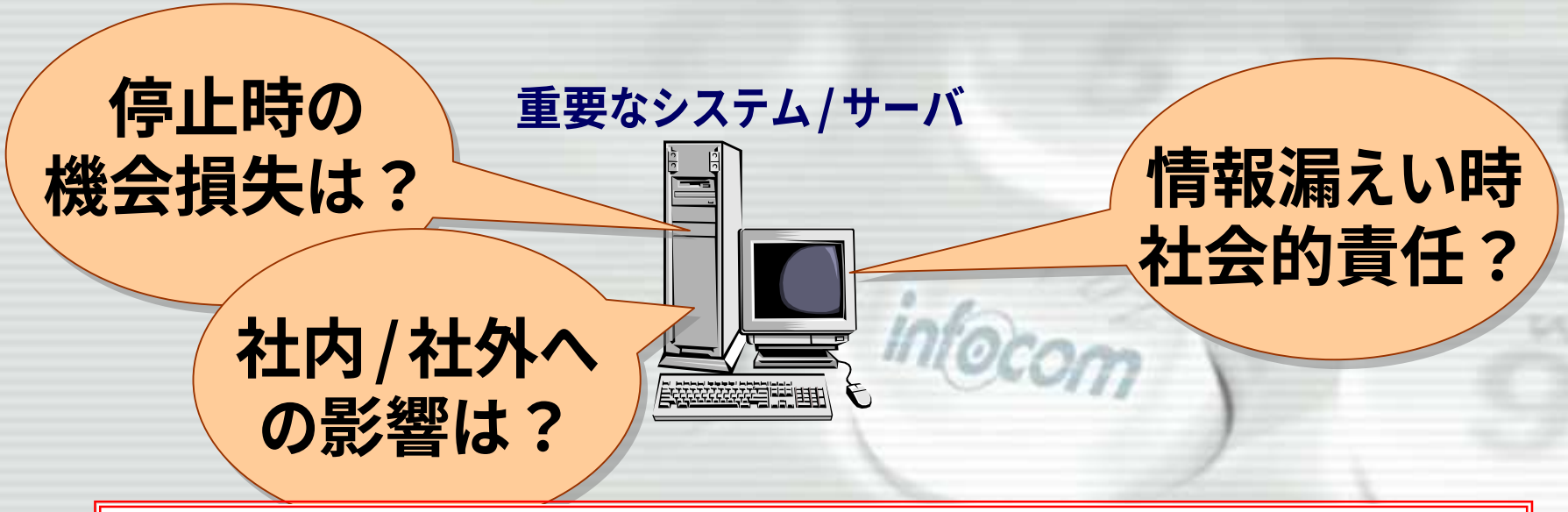
infocom

セキュアOSの導入は、統制の基盤的効果だけではない・・・

infocom

セキュアOSがもたらすビジネスリスク回避 ①

『システム環境の現状からサーバ停止は致命傷』



”サーバ停止”、“サーバサービス停止”のリスクを
本当に想像出来ているか？

セキュアOSがもたらすビジネスリスク回避 ②

サーバ・サーバサービスを停止しない

セキュアOSを導入する事は、単なる統制・セキュリティ効果だけでは無く、自社の ビジネスの安定稼動への必須手段である。
つまり、重要なサーバシステムを“止めない”事が肝心です。

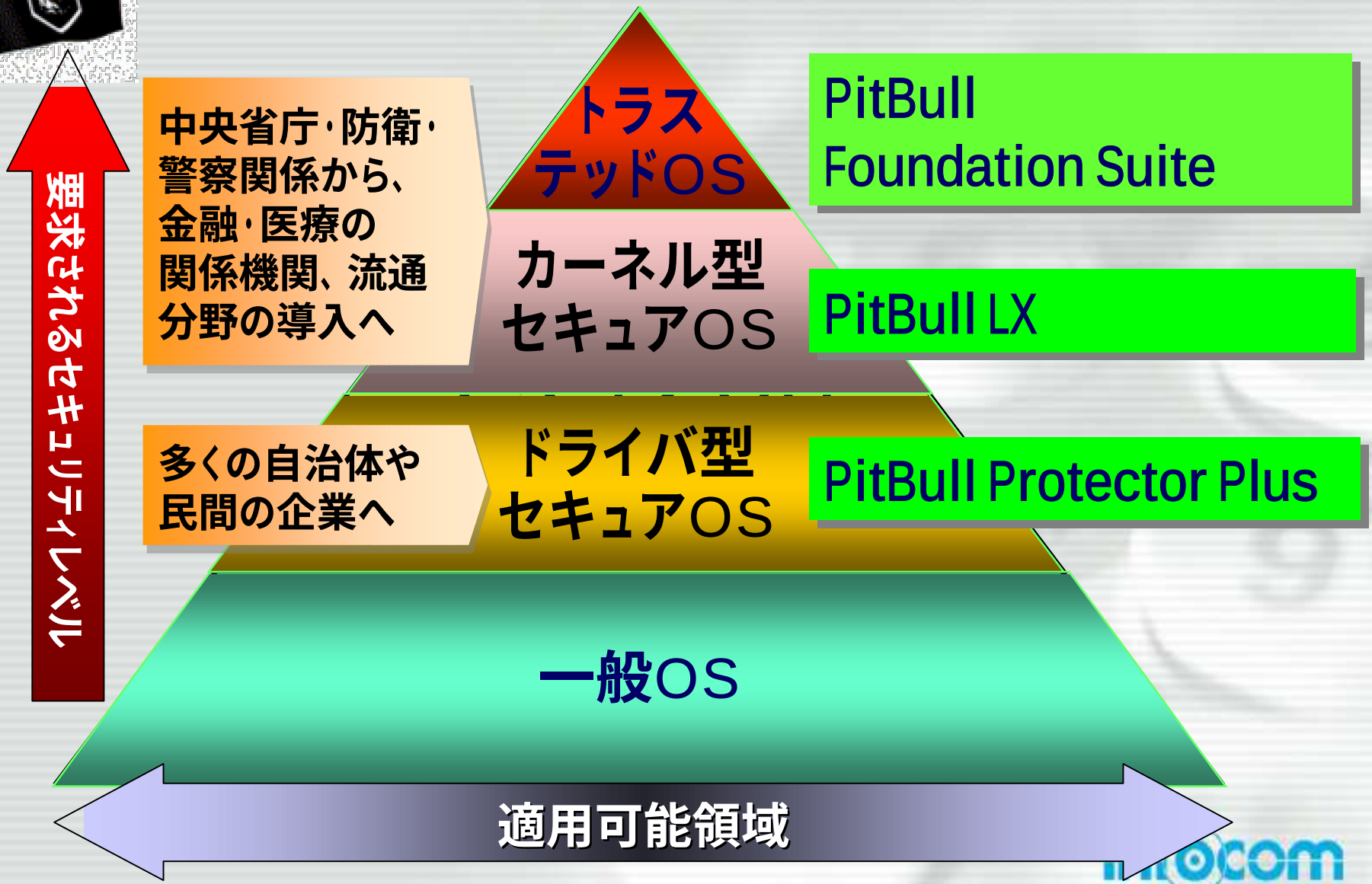
セキュアOS は、最良の手段

セキュアOS”PitBull”

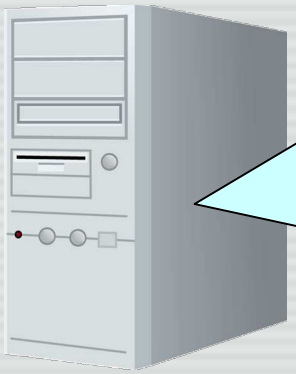
PITBULL

infocom

セキュアOS"PitBull"ファミリー



セキュアOS ”PitBull”の特徴



サーバ機器

一般的なサーバシステムの構造

業務
アプリケーション

セキュリティ
アプリケーション

DB
データベース

OS(UNIX、Windows※等)

PITBULL

サーバOSに “追加”導入
- 現在のサーバもセキュアOS化可能
- 計画中の新規システムなら最適適用

※Windows対応は、ProtectorPlus製品になります。

PitBullが効果を発揮する導入先(一例)

◆適用システム例 ◆

- ハッキングから守りたいインターネットサーバ
  (Webサーバ、メール/DNSサーバ等、DMZ上のサーバ)
- 顧客情報や患者情報、経営情報など情報漏洩させたくないサーバ
- ミッションクリティカルでサービス(サーバ)の停止が困難な業務サーバ
- 稼動中のサーバで、パッチ適用やサービス停止が難しいサーバ
- 稼動中でシステム変更が難しく思い切ったセキュリティ提案ができないサーバ
- 多数サーバを持ち、パッチ適用など運用コストを削減させたい顧客
- セキュリティに多大な投資はできないが対策の必要性を感じている顧客

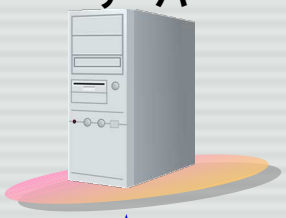
インターネット側・イントラネット側を問わず
管理対象の全サーバに適用可能！

PitBullによる『安心サーバ運用』への期待

セキュリティへの不安から残業・夜勤・休日出勤など時間を余計に確保して、さらに短い時間でのテストと評価で本番へ適用。 大変なので見切り適用も？

時間に追われる対応
見切り本番適用
過度なストレス環境

通常OS
サーバ



サービス開始

セキュアOS
サーバ

対象調査 → パッチ入手 → テスト実施 → 内容評価 → 本番適用

セキュリティホール発生

対象調査 → パッチ入手 → テスト実施 → 内容評価 → 本番適用

セキュリティホール発生

対象調査 → パッチ入手 → テスト実施 → 計画的なテスト実施 → 内容評価

パッチ確認 → パッチ適用 → 定期保守

パッチ適用 → パッチ確認

PitBullが不正な動きを封じる事から、パッチの適用に慌てる必要は無く、十分に必要なテストと評価を実施してから定期保守などのタイミングで適用する。

慌てない！
十分なテスト・評価！
安定したサービス提供
パッチの計画適用

最近の実績

PITBULL

最近の実績 ①

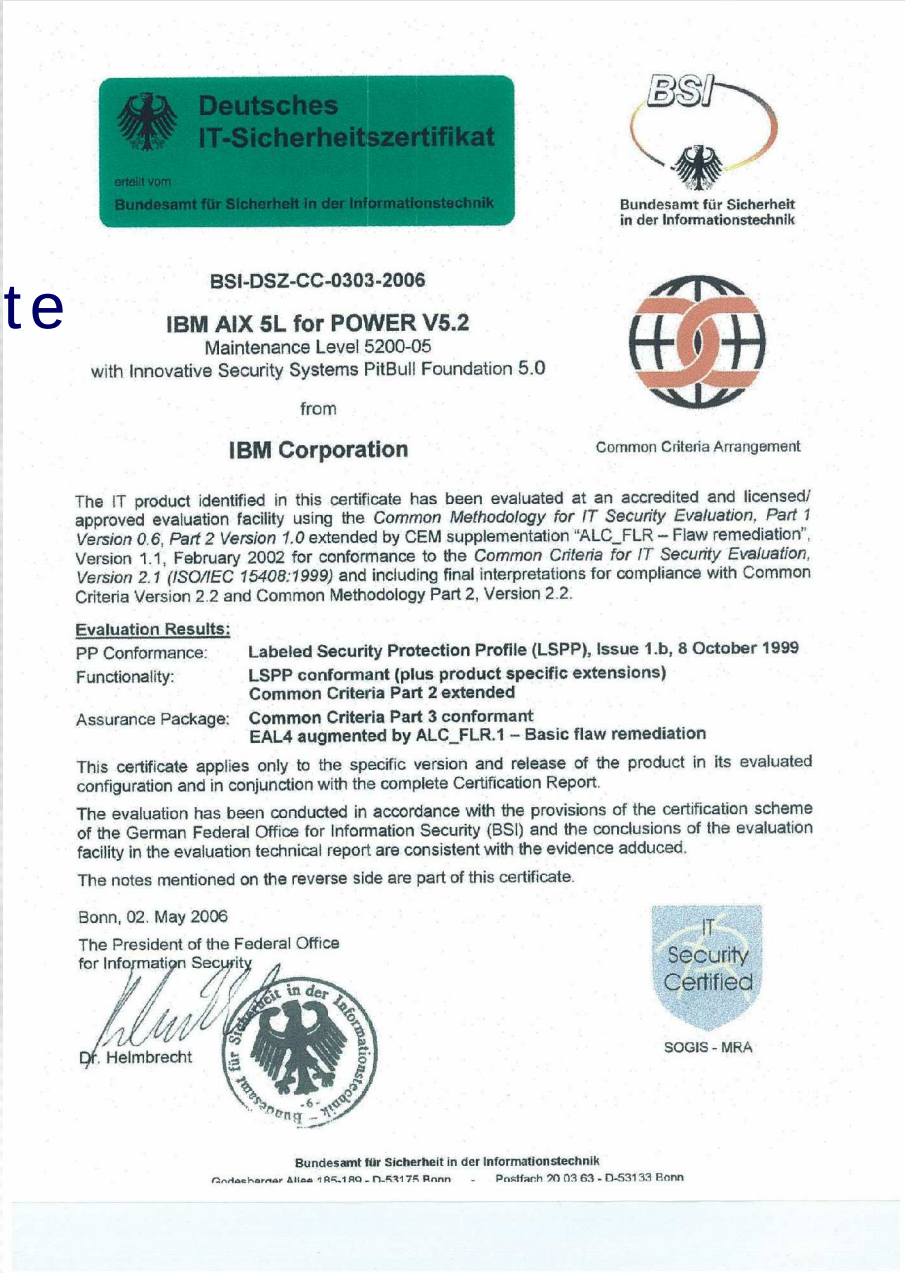
- 内閣官房情報セキュリティセンターの報告書への記載
- 中央省庁の基幹システムへの全面導入
- 証券会社のｲﾝﾀｰﾈｯﾄ公開系ｻｰﾋﾞｽｼｽﾃﾑへの導入
- 電力会社のｲﾝﾀｰﾈｯﾄ公開系ｻｰﾋﾞｽｼｽﾃﾑへの導入
- 上場企業 基幹DBｼｽﾃﾑ情報漏えい対策への導入

今年度に入ってからも、外資系金融機関の新規ｲﾝﾀｰﾈｯﾄ公開系ｻｰﾋﾞｽｼｽﾃﾑへの検討も進行しており、重要ｲﾝﾌﾗの基幹システム、公開系ｻｰﾊﾞｼｽﾃﾑへの導入が予定されている。

最近の実績 ②

- PitBull Foundation Suite (TrustedOS)
  ⇒ AIX5.2版 EAL4+
  2006年5月2日取得

多くの基幹系システムで利用されているAIX5.2に対して、非常にニーズが高かったTrustedOSとしての環境が提供可能になりました。



Deutsches IT-Sicherheitszertifikat
erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI
Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0303-2006

IBM AIX 5L for POWER V5.2
Maintenance Level 5200-05
with Innovative Security Systems PitBull Foundation 5.0

from

IBM Corporation

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0* extended by CEM supplementation "ALC_FLR – Flaw remediation", Version 1.1, February 2002 for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

PP Conformance:	**Labeled Security Protection Profile (LSPP), Issue 1.b, 8 October 1999**
Functionality:	**LSPP conformant (plus product specific extensions) Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant EAL4 augmented by ALC_FLR.1 – Basic flaw remediation**

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 02. May 2006

The President of the Federal Office for Information Security

Dr. Helmbrecht

IT Security Certified
SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn

ロードマップ

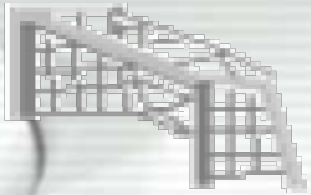
PITBULL

ロードマップ

- PitBull Foundation Suite (TrustedOS)
  ⇒ AIX5.3版 2006年末 CC認証取得予定
- PitBull Foundation Suite (TrustedOS)
  ⇒ Linux版 2006年末(～12月) サポート予定
  ⇒ CC認証取得予定
- PitBull Protector Plus (セキュアOS)
  ⇒ 2006年秋 メジャーバージョンアップ予定

ご清聴、ありがとうございました。

PITBULL



インフォコム株式会社
フロンティア事業本部　セキュリティソリューション部
セキュリティソリューショングループ
セキュリティコンサルタント 正木 義和
E-mail : y.masaki@infocom.co.jp

infocom