

Solaris Innovation Forum 2008

IT全般統制の実例紹介 ～Senju Familyのご紹介～

2008年6月5日

株式会社野村総合研究所
システムマネジメント事業本部
千手事業部
大方 潤

j-ohkata@nri.co.jp

アジェンダ

I. はじめに

II. IT全般統制への取り組み

III. サン・マイクロシステムズ様との連携事例

I. はじめに

II. IT全般統制への取り組み

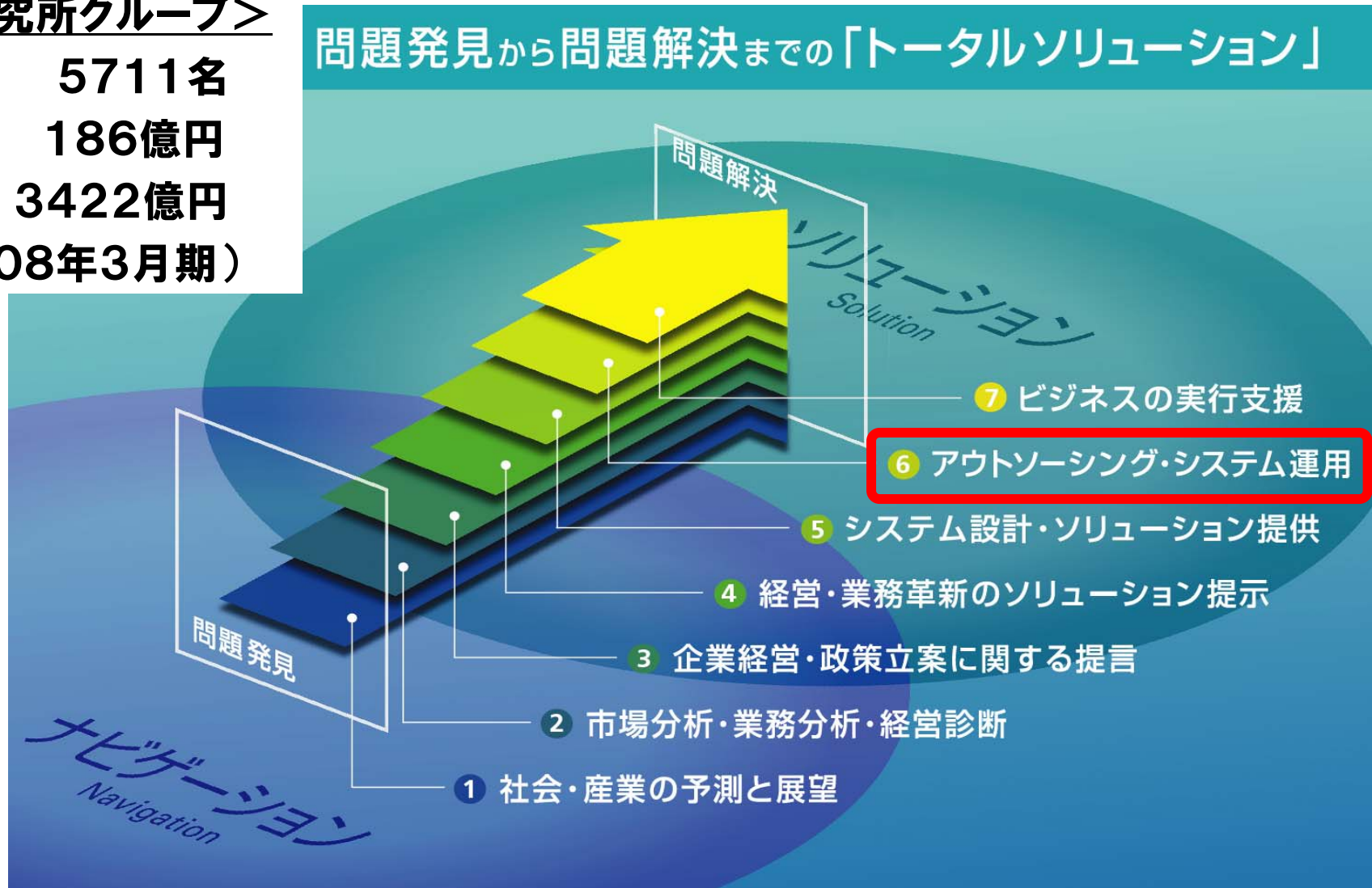
III. サン・マイクロシステムズ様との連携事例

1. はじめに NRI野村総合研究所グループのご紹介

<野村総合研究所グループ>

- 従業員数： 5711名
- 資本金： 186億円
- 売上高： 3422億円
(2008年3月期)

問題発見から問題解決までの「トータルソリューション」



1. はじめに システムマネジメント事業への取り組み

<自社で運用改革推進>

インソース

主な提供サービス

運用改革コンサル

ITIL導入支援(SSMF)

運用基盤構築

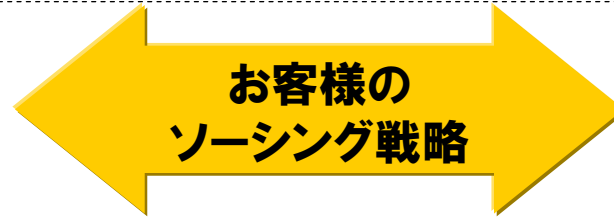
運用ツール提供

教育・研修支援

データセンターコンサル

セキュリティコンサル

⋮



<新たな器で運用改革を実現>

アウトソーシング

(300社強)

弊社における主な改革

<見える化;継続>

① SLMによるSL向上

② 自動化・無人化

③ プロセス改革(ITIL)

④ 教育・資格制度

⑤ 開発部門へのけん制

⑥ コンプライアンス(SOX法等)

⑦ セキュティ・安全対策

<運用改革>

サービスレベル(品質)向上

運用コスト削減

リスク管理(セキュリティ、安全対策)

コンプライアンス

アウトソーシング

①

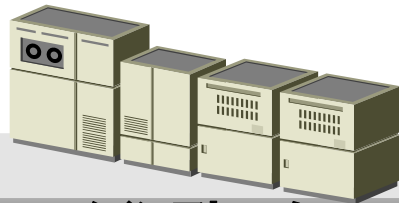
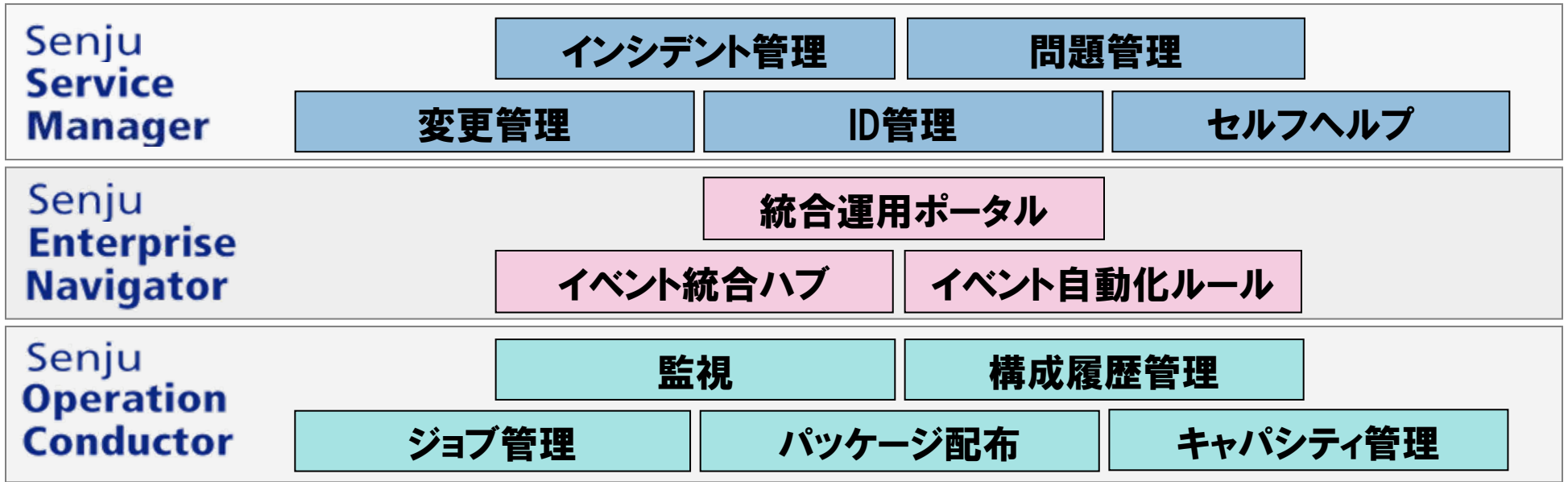
運用改革支援サービス

②

ノウハウの提供

1. はじめに

Senju Familyのご紹介



メインフレーム



ネットワーク機器



サーバ



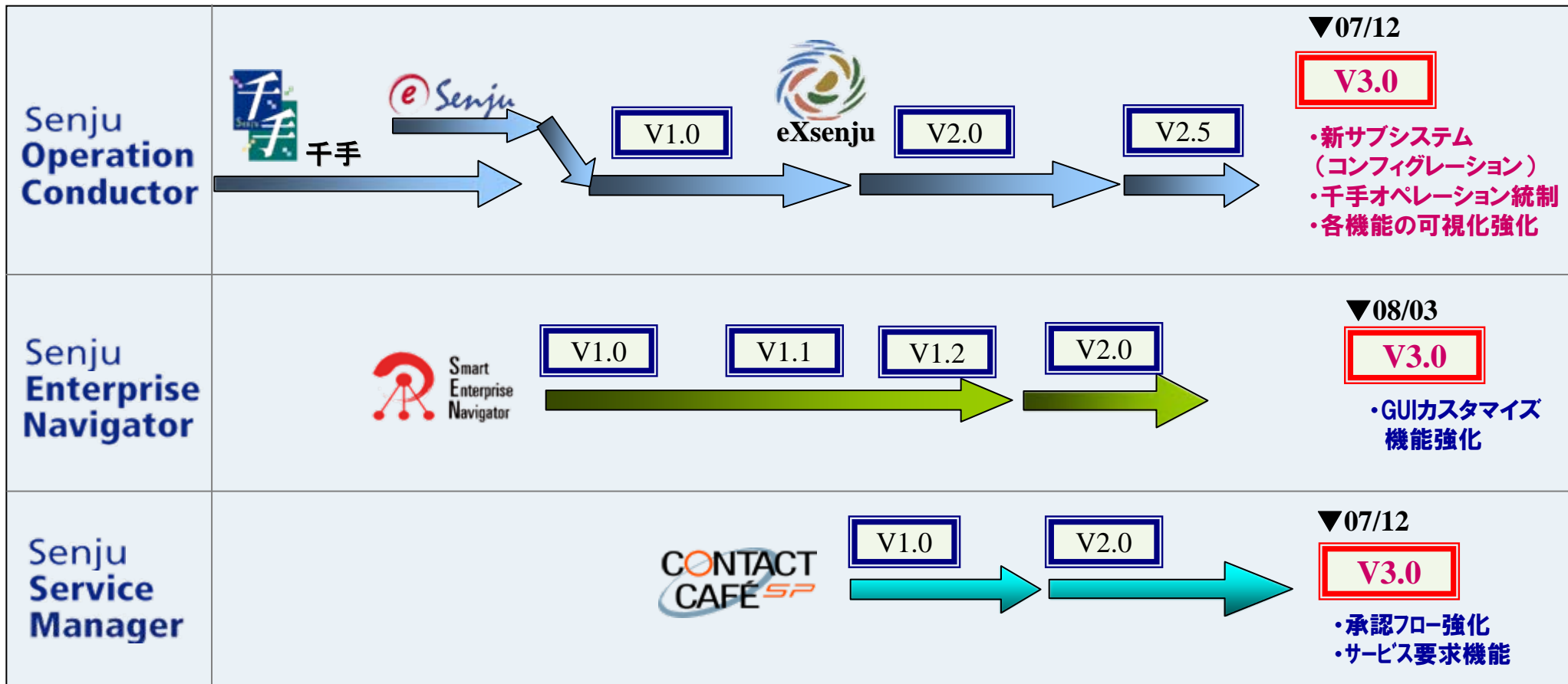
アプリケーション

I. はじめに

Senju Familyロードマップ



1994

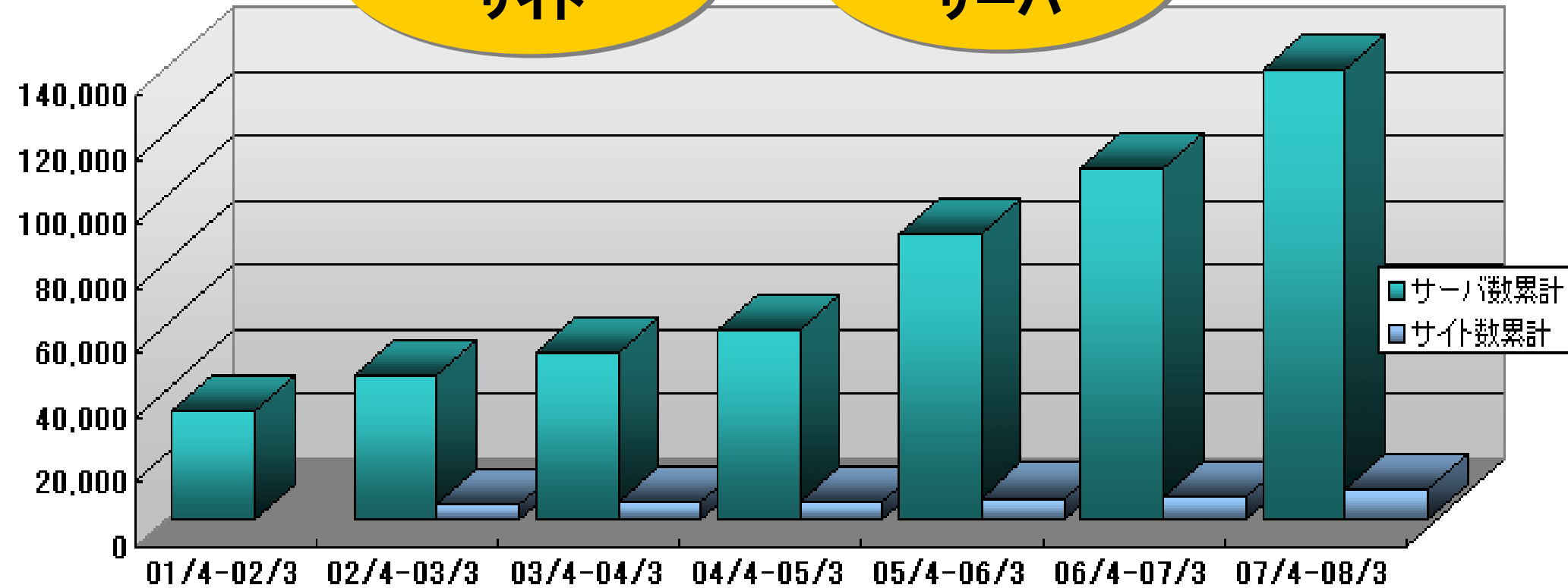


Ⅰ. はじめに SenjuFamilyの実績

●2008年3月現在

9,800
サイト

140,000
サーバ



1. はじめに

Senju FamilyのSolarisへの対応

Solaris x86に対応

国内運用管理製品として、いち早く対応

Solarisコンテナ上での稼働検証実施

Sun Ray監視の稼働検証実施

⋮



OSや環境の違いを運用管理ツールで吸収



混在環境での運用管理機能を提供

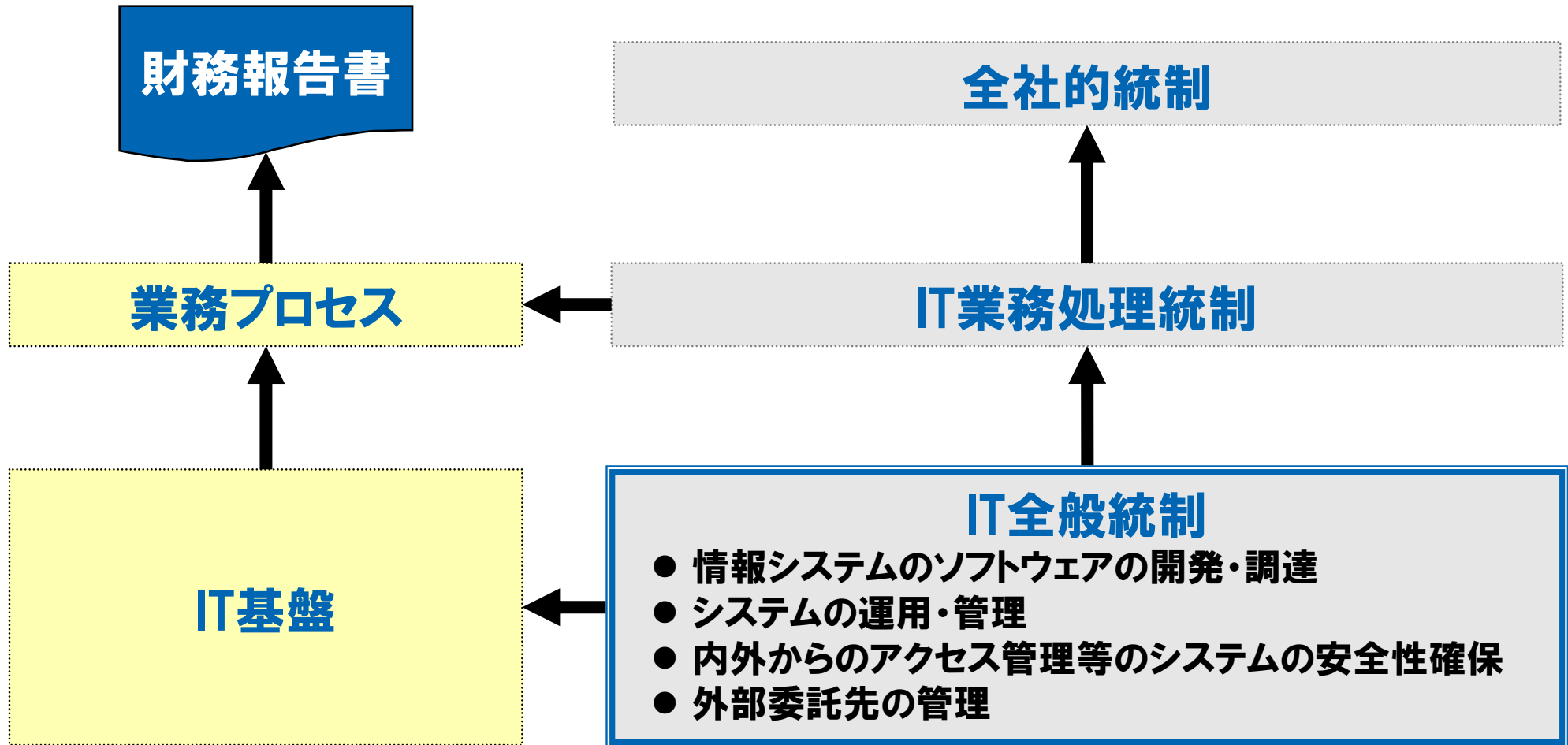
I. はじめに

II. IT全般統制への取り組み

III. サン・マイクロシステムズ様との連携事例

II. IT全般統制への取り組み

IT全般統制のおさらい 正しい財務報告のためのIT全般統制



(出所:システム管理基準 追補版(財務報告に係るIT 統制ガイダンス)をもとにNRIで作成)

II. IT全般統制への取り組み

IT全般統制のおさらい やるべきことは多いが・・・

情報システムのソフトウェアの開発・調達

ソフトウェアの開発・調達

IT基盤の構築

変更管理

テスト

開発・保守に関する手続きの策定と保守

システムの運用・管理

運用管理

構成管理

データ管理

内外からのアクセス管理等の システムの安全性確保

情報セキュリティフレームワーク

アクセス管理等のセキュリティ対策

情報セキュリティインシデントの管理

外部委託先の管理

外部委託先との契約

外部委託先とのサービスレベルの定義と管理

(出所:システム管理基準 追補版(財務報告に係るIT 統制ガイダンス)をもとにNRIで作成)

II. IT全般統制への取り組み

IT全般統制のおさらい 優先度の高い3項目

監査事例や事例に基づいたNRIの考える必須項目

アクセス管理・ID管理

- アクセス管理等の方針を定めていること
- 内外からのアクセス管理などのシステムの安全性が確保されていること

変更管理・構成管理

- 変更について、所定の承認を得ていること、及びその過程が適切に記録及び保存すること
- システム把握及び、それを支援するIT基盤を把握すること

インシデント管理・問題管理

- 障害や故障等の状況の把握、分析、解決等の対応が適切に行われていること

(出所:財務報告に係る内部統制の評価及び報告(案)及び監査(案)をもとにNRIで作成)

II. IT全般統制への取り組み Senju Familyの取り組み

■「運用管理ツール」と聞いて、思い浮かぶもの

- サーバの稼動監視
- サーバの自動運転(ジョブスケジュール)
- ネットワークの監視
- キャパシティ管理

他



■IT全般統制で、「運用管理ツール」は有効？

- 不備を未然に防ぐためには、有効な手段
 - ・「運用管理ツール」で、どこまで防ぐことができるのか？
 - ・既存の「運用管理ツール」以外に、何をしなくてはならないのか？

IT全般統制における「運用管理ツール」の
活用事例の紹介



II. IT全般統制への取り組み Senju Familyの取り組み

■IT全般統制で実施すべき事

- 不正IDでのアクセスがない
- 承認されたIDでの作業が承認の範囲を超えていない
- 実行プログラムが、不正に書き換えられていない
- データが、不正に書き換えられていない

⋮



ないこと

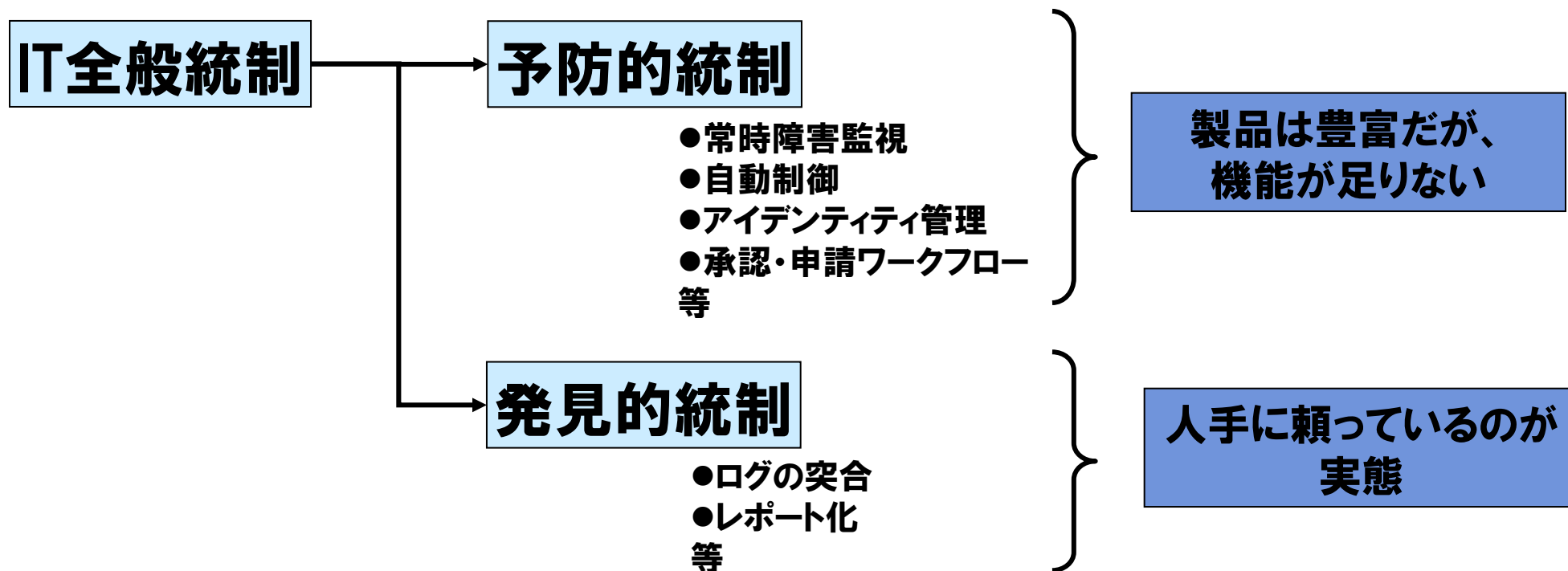
を証明する必要がある



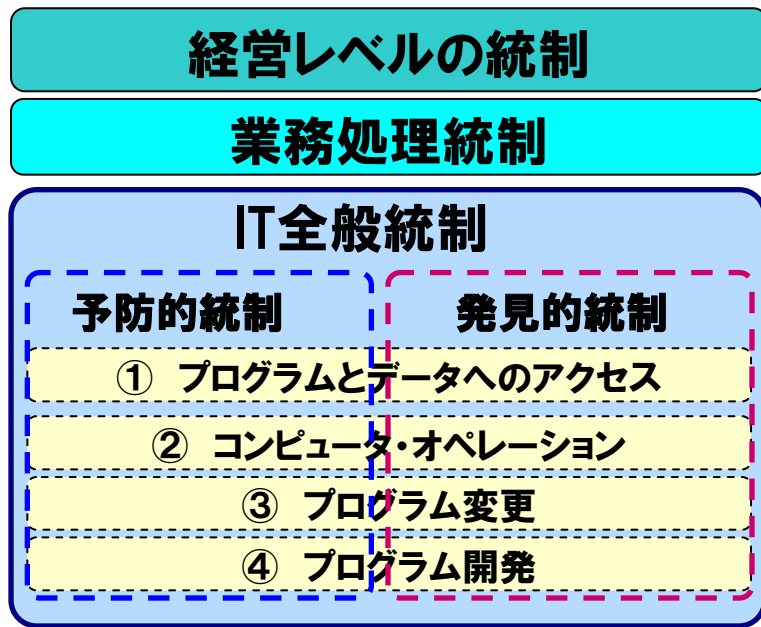
II. IT全般統制への取り組み Senju Familyの取り組み

■ ない事を証明するには・・・

- 予防的統制で、証明する事が理想だが、実際には限界がある。
- 発見的統制でのフォロー及び、自らの検証が必要



II. IT全般統制への取り組み Senju Familyの取り組み



既存ツールの強化
Senju Operation
Conductor:
コンフィグレーション機能
の追加

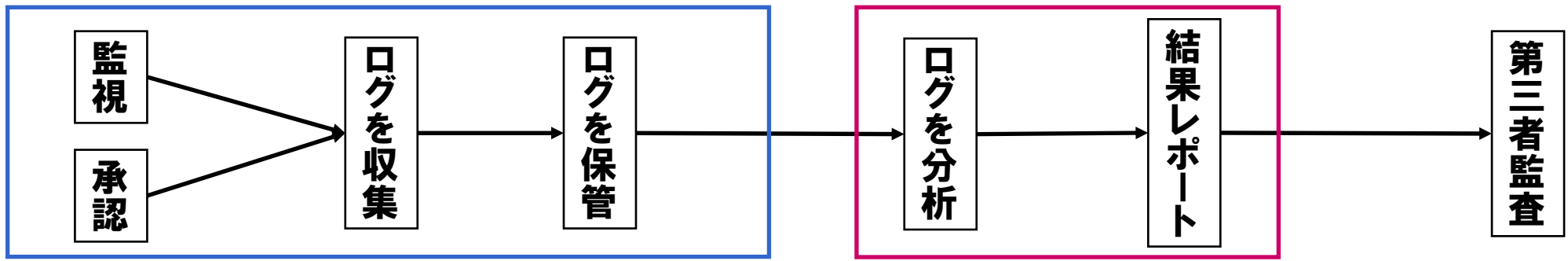
新機能の投入
SJX(仮称):
発見的統制の支援

新たな業務

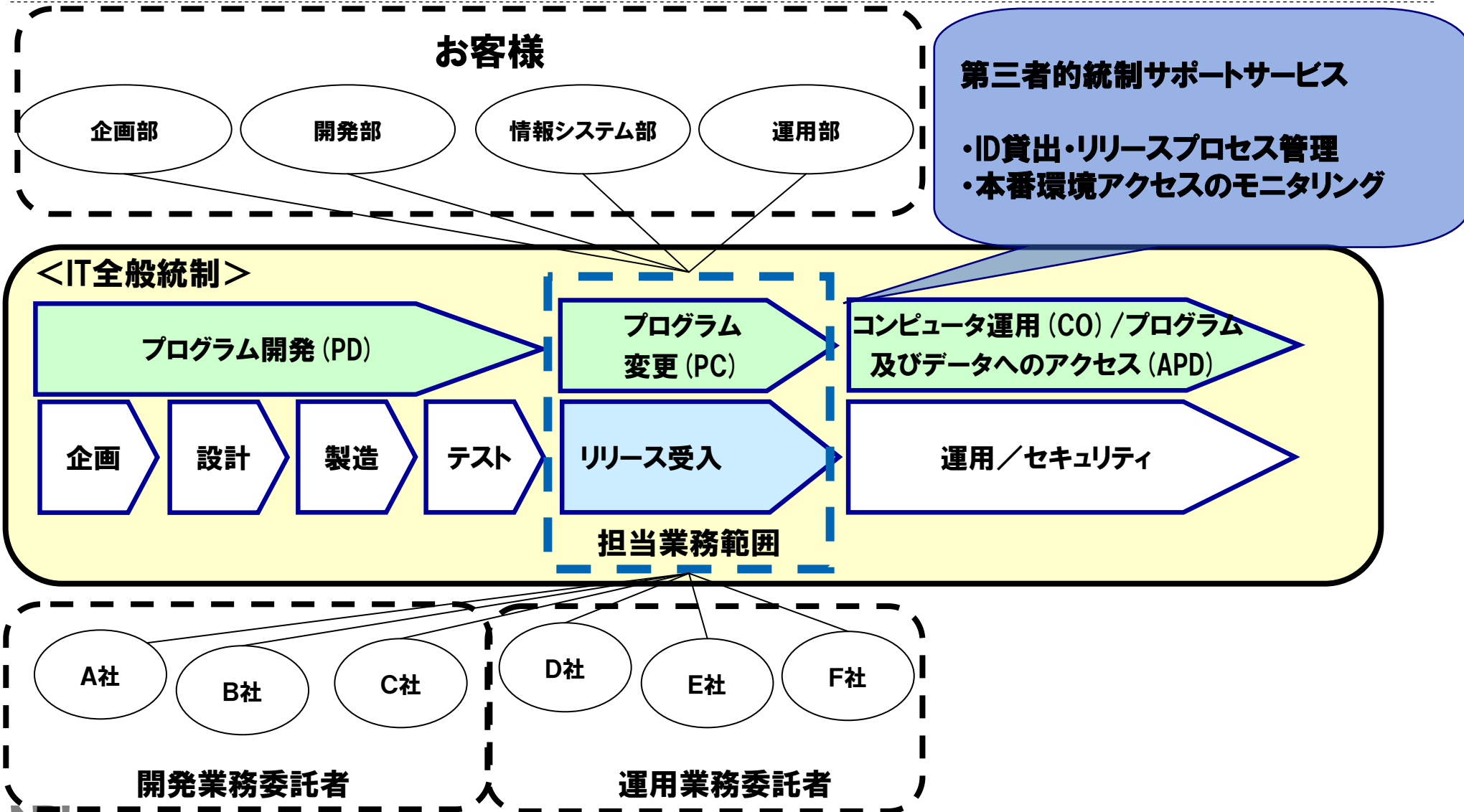
<業務の流れから見ると...>

<既存ツールの強化>

<新機能>

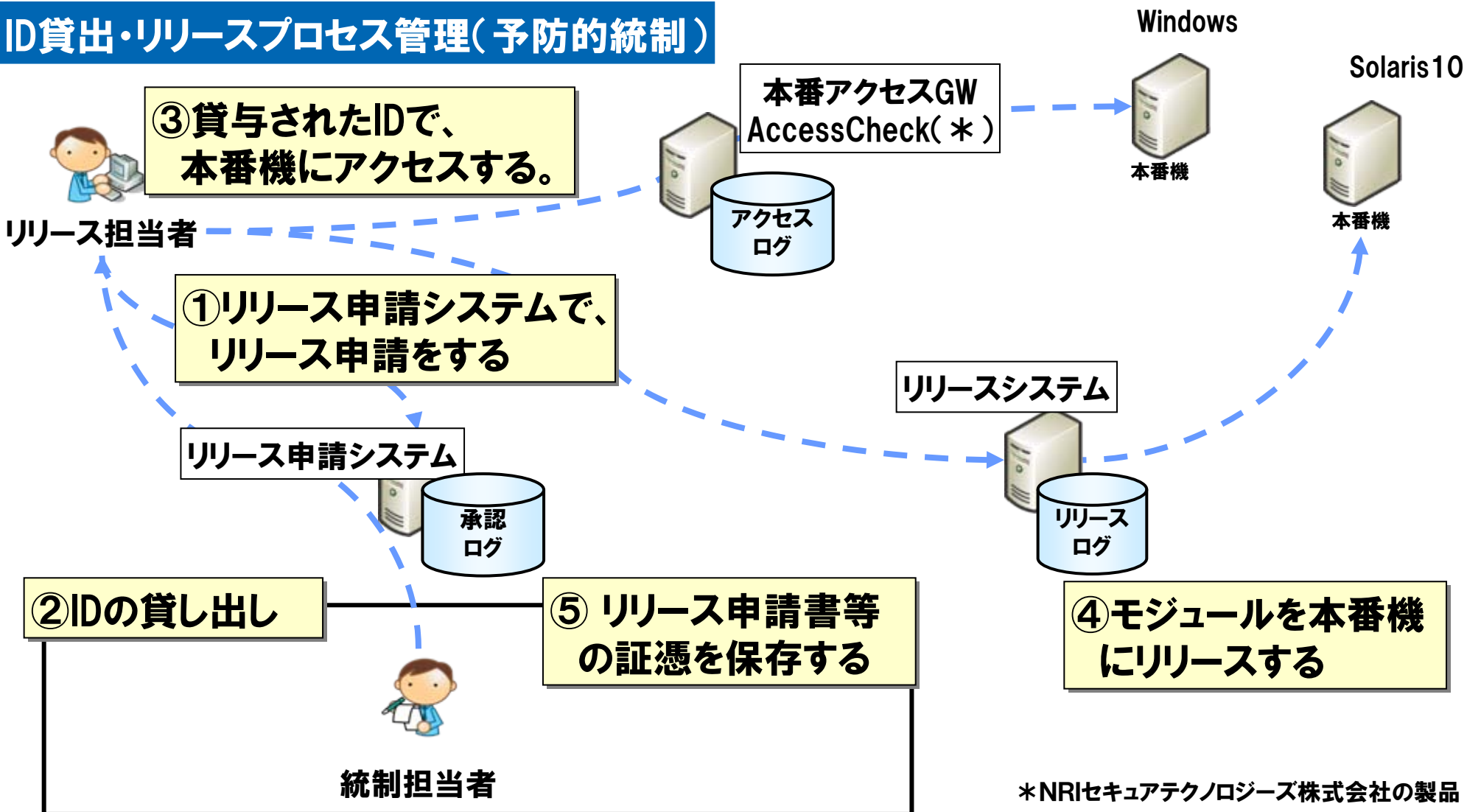


II. IT全般統制への取り組み IT全般統制サービス業務での活用事例



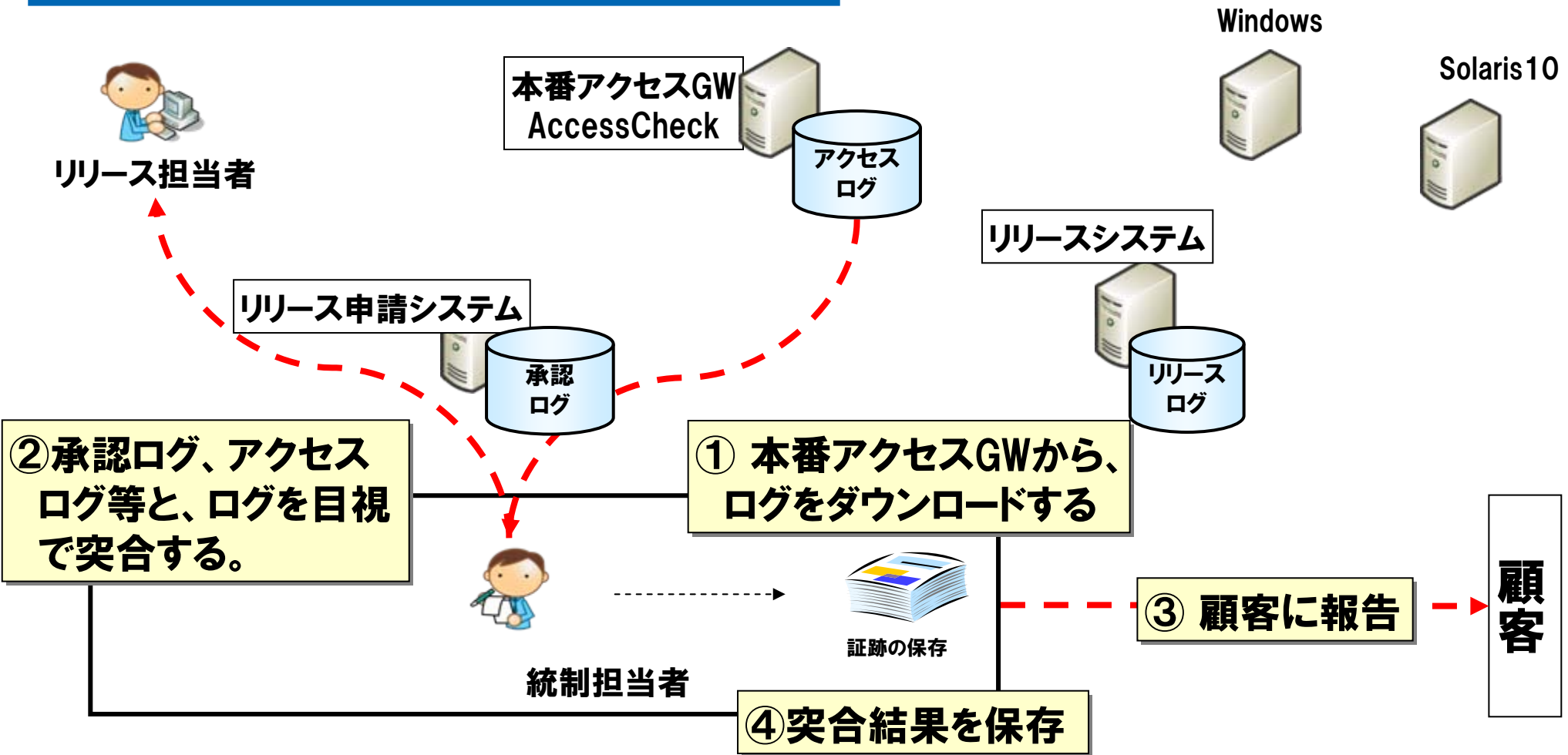
II. IT全般統制への取り組み IT全般統制サービス業務での活用事例

ID貸出・リリースプロセス管理(予防的統制)



II. IT全般統制への取り組み IT全般統制サービス業務での活用事例

本番環境アクセスのモニタリング(発見的統制)



II. IT全般統制への取り組み

IT全般統制サービス業務での活用事例

■課題

- ログチェックが手作業のため、高負荷、高コストな上、信頼度が低い。
- 監査を重ねるごとに検査すべき項目が増大する傾向にある
 - ・ これまで以上に項目・証跡の精度が問われる

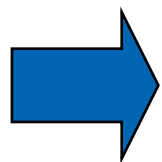
■課題の要因

項番	課題	モニタリング項目	運用状況と課題
1	踏み台によるアクセスが未検知	不正アクセスの検出	実施中だが、 負荷が高い
2	開発者が、未承認のローカルIDとパスワードを使用している	不正アクセスの検出	
3	Windowsは、GUIによるアクセスとなり、モニタリング可能な証跡がない。	不正アクセスの検出	未実施
4	監査人のチェック方法と実際のチェック方法が異なっている	実機上のログイン／ログアウト情報の把握	実施中だが、 信憑性が低い

II. IT全般統制への取り組み IT全般統制サービス業務での活用事例

■ Senju Familyの機能を活用して統制方法を変更

ゲートウェイのログを
目視する

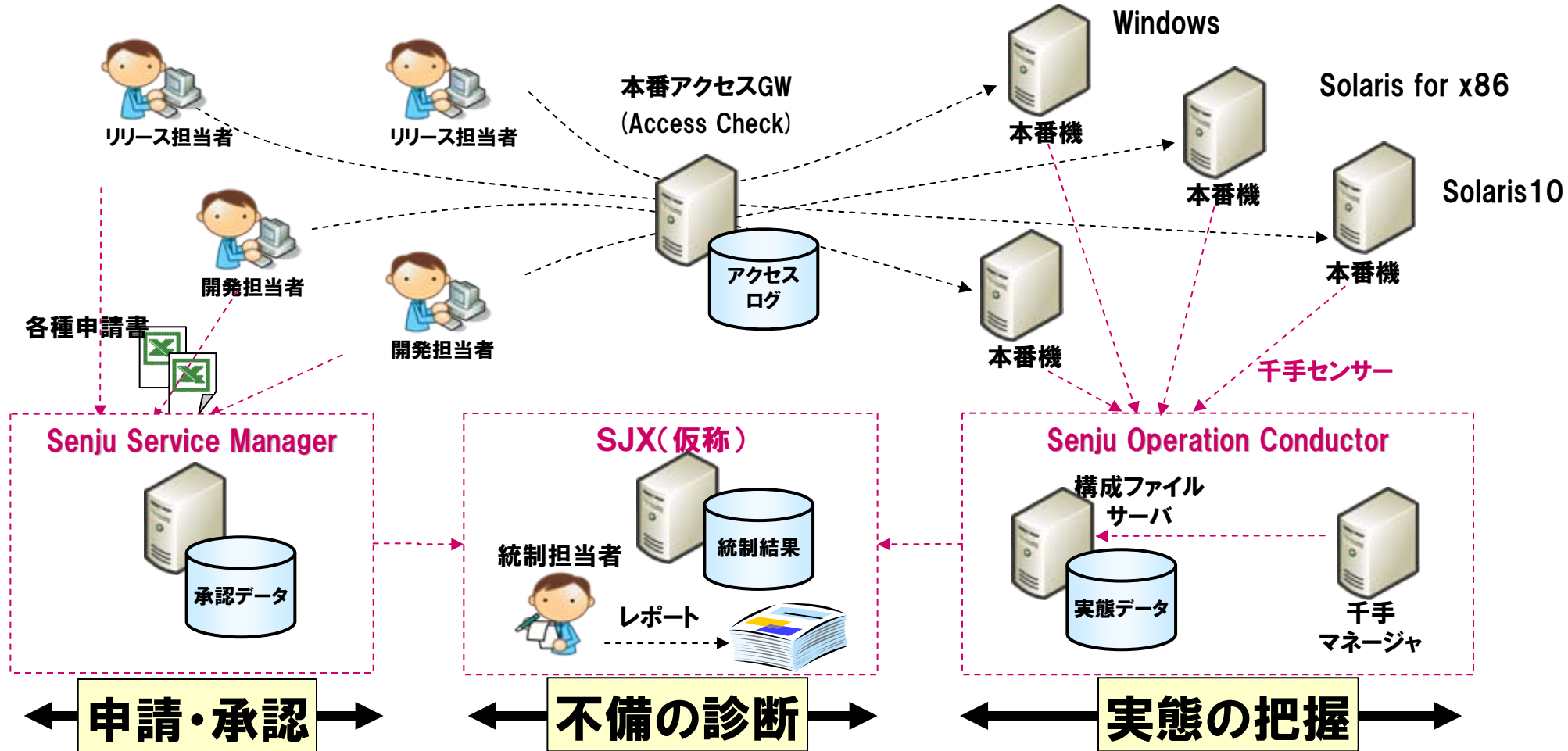


承認データと本番環境へのアクセスログや
ファイル変更を突合し、未承認のアクセス、
未承認のファイル更新を見つけ出す

■ 新しい統制方法に必要なSenju Familyの機能

分類	機能
実態の把握 (Senju/OC)	ファイルの更新の監視
	アカウント毎のログイン/ログアウトの監視
申請・承認 (Senju/SM)	申請/承認の電子化
	IDの管理
不備の診断 (SJX(仮称))	承認ログとファイル更新の不整合の検出
	承認ログとログイン/ログアウトの不整合の検出

II. IT全般統制への取り組み IT全般統制サービス業務での活用事例



発見的統制の自動化、効率化、高度化を実現

II. IT全般統制への取り組み

「Senju FamilyによるIT全般統制ソリューション」のご紹介

■事例から学んだ課題

- 本番環境のパスワードの管理責任者が不明確。
- 本番環境のパスワードを、実は開発担当も知っている。
- 誰がログインしたか証跡が残っていない。
- アクセス承認の証跡が残っていない。
- プログラムのリリース承認の証跡が残っていない。
- 単純に対応すると・・・
 - ・現状の整理や今後の対策などの検討から開始し、対応完了までに時間がかかる。
 - ・これまで実施してない運用業務が発生し、運用コストが増大。



導入負荷が少なく、運用も考慮されたソリューションが必要

II. IT全般統制への取り組み

「Senju FamilyによるIT全般統制ソリューション」のご紹介

■ Senju Familyによる内部統制モニタリングソリューション

- プログラムリリース統制ソリューション
- 本番環境アクセス統制ソリューション

IT統制及び監査対応を効率化!
プログラムリリース統制ソリューション

こんな事は
ありませんか?

- いつの間にか、承認されていないプログラムがリリースされていた!
- プログラム変更業務が統制されていない!
- 新たな運用業務発生による運用コスト増大が心配!

現状の課題

- ☑ プログラムを「何時」「誰が」「誰の承認を得て」変更したかを管理できておらず、どのプログラムがリリースされているか把握していない
- ☑ プログラムのリリースや認証での証跡が残っていない、もしくはリリースされた内容と承認された内容が一致しない
- ☑ 承認されたプログラム変更が行われたかを証明するためのログ確認負荷が大きい

Senju Family による解決策

承認フローによる予防的統制をベースに、
構成情報変更履歴確認や承認結果との突き合わせを行う見易い統制の自動化にて、統制の精度を向上

Senju Family によるソリューション概要

- 1 開発環境からリリースされたプログラム
- 2 開発環境からリリースされたプログラムのリリース承認
- 3 マネージメントによるプログラムのリリース承認
- 4 開発環境からリリース承認されたプログラムの承認
- 5 承認されたプログラムのリリース承認結果
- 6 承認されたプログラムのリリース承認結果
- 7 承認されたプログラムのリリース承認結果
- 8 承認されたプログラムのリリース承認結果
- 9 承認されたプログラムのリリース承認結果

Senju Family 製品の具体的な詳細は、こちらをご覧ください。>

本番環境へのアクセスを確実に統制!
本番環境アクセス統制ソリューション

アクセス制御、
全部のアクセスログを確認、
そもそも現状の把握...

できていますか?

現状の課題

- ☑ 本番環境へアクセスするための承認フローがない
- ☑ 本番環境に未承認アクセスがなかった事の証明ができない、もしくは未承認の本番環境のアクセスがないことを証明するために、ログを手作業で確認するのは無理
- ☑ 「いつ」「誰が」「どこに」アクセスしたかのログと承認証跡の突き合わせは困難

Senju Family による解決策

統制知識がなくても日々の運用の一部として、承認されたアクセス申請に基づいた本番環境への
確実なアクセス制御・予防的統制と見易い統制に掛ける工数を大幅に省力化

Senju Family によるソリューション概要

- 1 承認されたプログラムのリリース承認結果
- 2 承認されたプログラムのリリース承認結果
- 3 承認されたプログラムのリリース承認結果
- 4 承認されたプログラムのリリース承認結果
- 5 承認されたプログラムのリリース承認結果
- 6 承認されたプログラムのリリース承認結果
- 7 承認されたプログラムのリリース承認結果
- 8 承認されたプログラムのリリース承認結果
- 9 承認されたプログラムのリリース承認結果

Senju Family 製品の具体的な詳細は、こちらをご覧ください。>

II. IT全般統制への取り組み

「Senju FamilyによるIT全般統制ソリューション」のご紹介

プログラムリリース統制ソリューションの概要

承認フローによる予防的統制をベースに、構成情報変更履歴確認や承認結果との突合せを行う発見的統制の自動化にて、統制の精度を向上

承認フローを通じた
承認無き登録の回避

予防的統制



マネージャ

承認 ↓

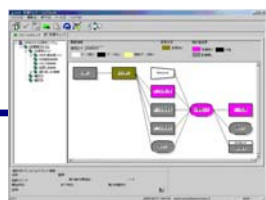
プログラムの情報を自動収集し、
「どのような変更を実施したか」
の変更履歴を管理

発見的統制

Solaris10
Solaris on x86
Solaris of x64
等、OSの違いをツールで吸収

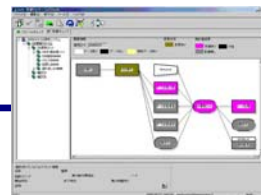


開発環境



プログラム

ゲートウェイサーバ



プログラム



本番環境

承認されたプログラム変更と実際にリリース
されたプログラムの突合せを自動化

発見的統制

既存の環境に追加導入可能

II. IT全般統制への取り組み

「Senju FamilyによるIT全般統制ソリューション」のご紹介

本番環境アクセス統制ソリューションの概要

統制知識がなくても日々の運用の一部として、承認されたアクセス申請に基づいた本番環境への
確実なアクセス制御 予防的統制と発見的統制に掛かる工数を大幅に省力化

Solaris 10
Solaris on x86
Solaris of x64
等、OSの違いをツールで吸収

承認フローを通じた
承認無き本番環境へのアクセスの回避

承認されたアクセス申請に
基づいた本番環境への確実なアクセス制御

予防的統制



マネージャ

承認

アクセス

ゲートウェイサーバ



アクセス

予防的統制



本番環境

発見的統制



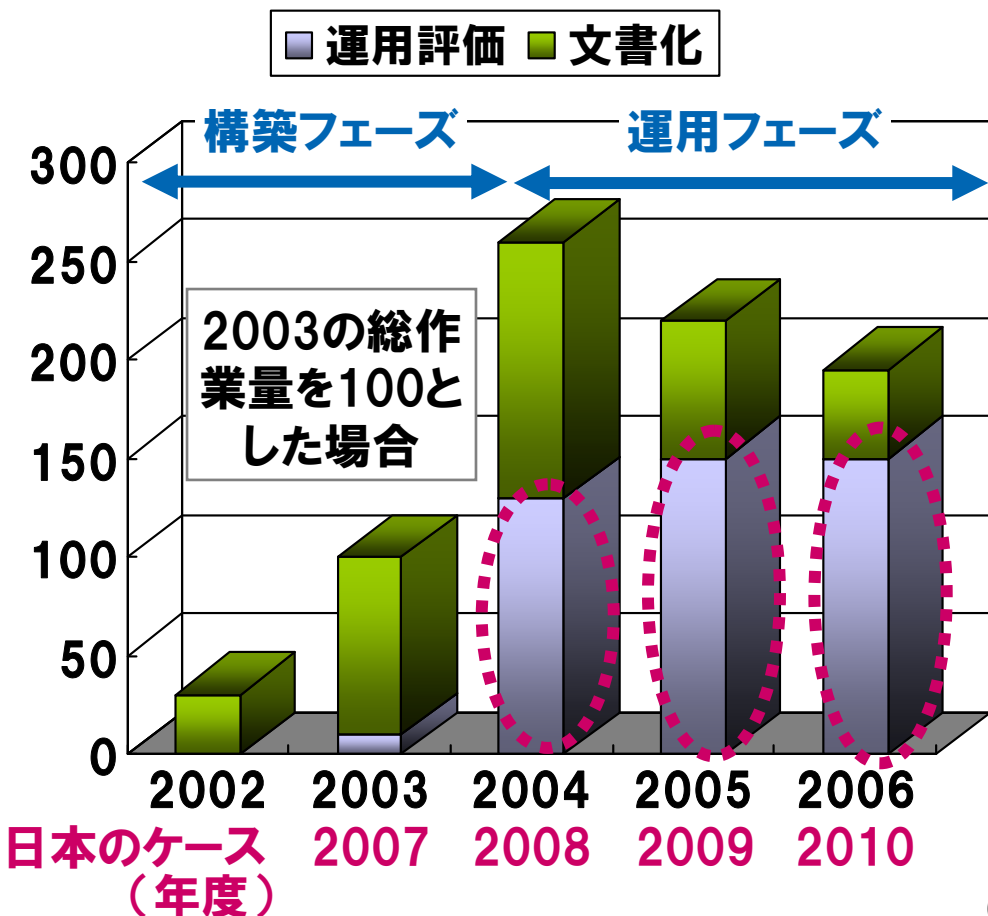
開発担当者

承認されたアクセス申請と本番環境への
アクセスログの突合を自動化

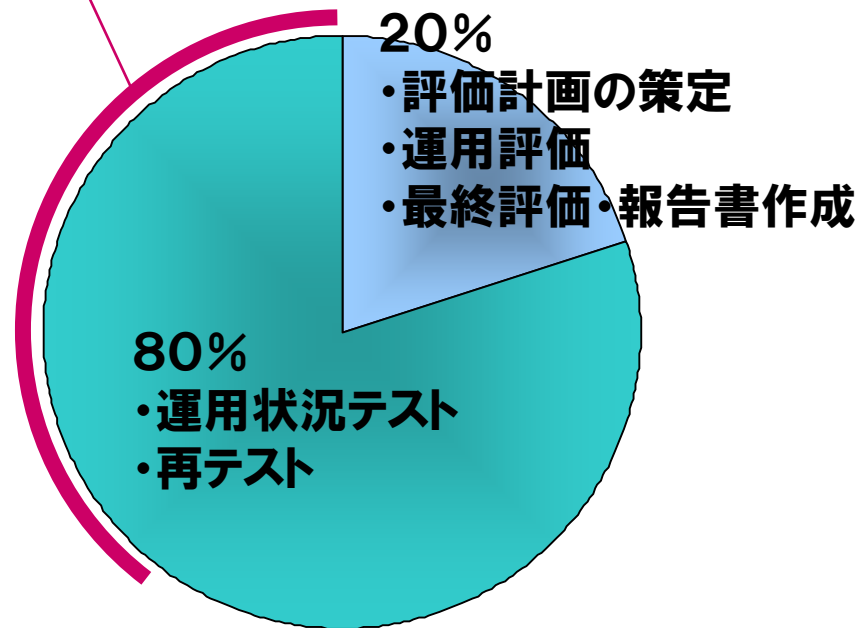
既存の環境に追加導入可能

II. IT全般統制への取り組み 統制・カイゼンにポイント

■先を見据えた徹底的な自動化が必須



テスト作業の半分は
証憑・証跡探し



(米国SOX対象企業へのヒアリングをもとに、NRIにて作成)

I. はじめに

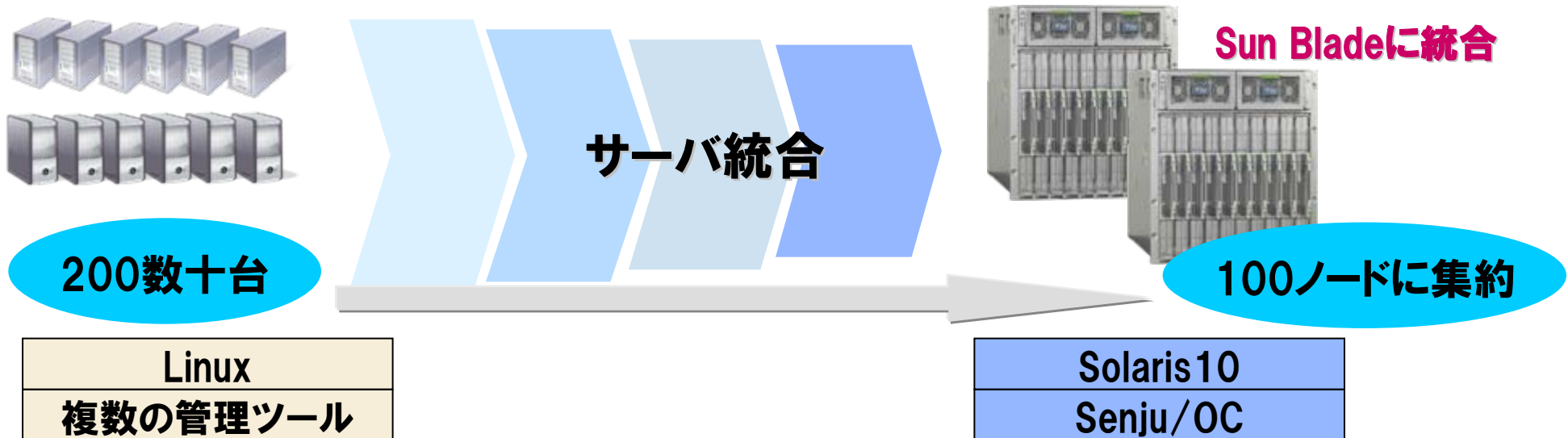
II. IT全般統制への取り組み

III. サン・マイクロシステムズ様との連携事例

Ⅲ. サン・マイクロシステムズ様との連携事例 サーバ統合 SunBlade + Solaris + Senju Family

■ 某ASPサービス

- B to Bのサービス拡大に伴い、急激にサーバが増加。(品質低下・管理負荷・コスト増)
- サーバ統合、DC移転、システム監視基盤再構築等を実施
 - ・ アプリケーションの移行 Linux⇒Solaris10
 - ・ サーバ Sun Bladeによるサーバ統合(Solarisコンテナによる仮想化)
 - ・ 運用管理ツール Solaris x86/x64に対応した運用管理ツールとして「**Senju Operation Conductor**」で統合管理



III. サン・マイクロシステムズ様との連携事例

データベース統合(データ分析) Solaris + SybaseIQ + MS-Datastudio + Senju Family

■某地銀様のデータ分析

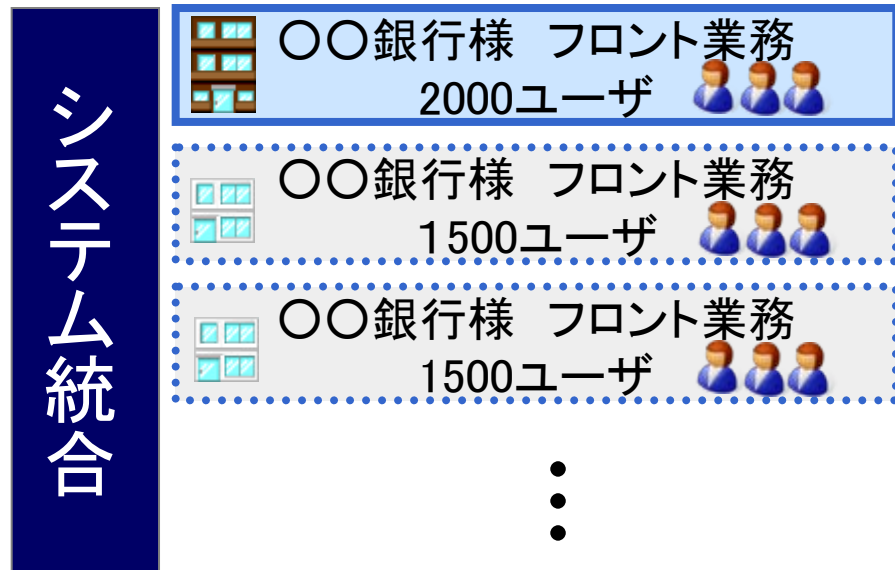
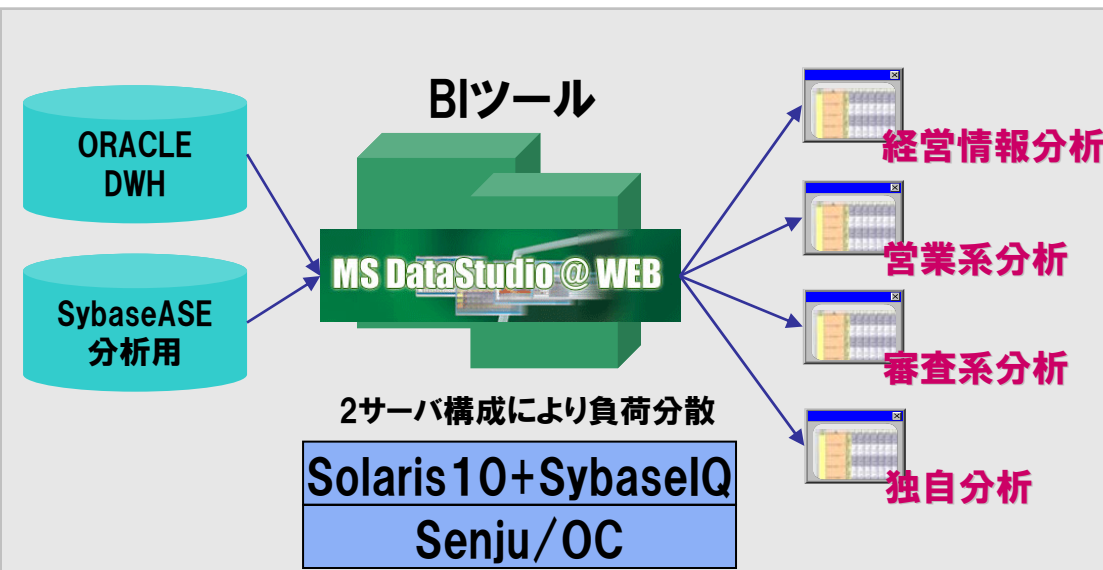
●BIツールを導入

- ・ BIツール
- ・ DB
- ・ 運用管理ツール

マイルストーン社 MS-DataStudio

SybaseIQ

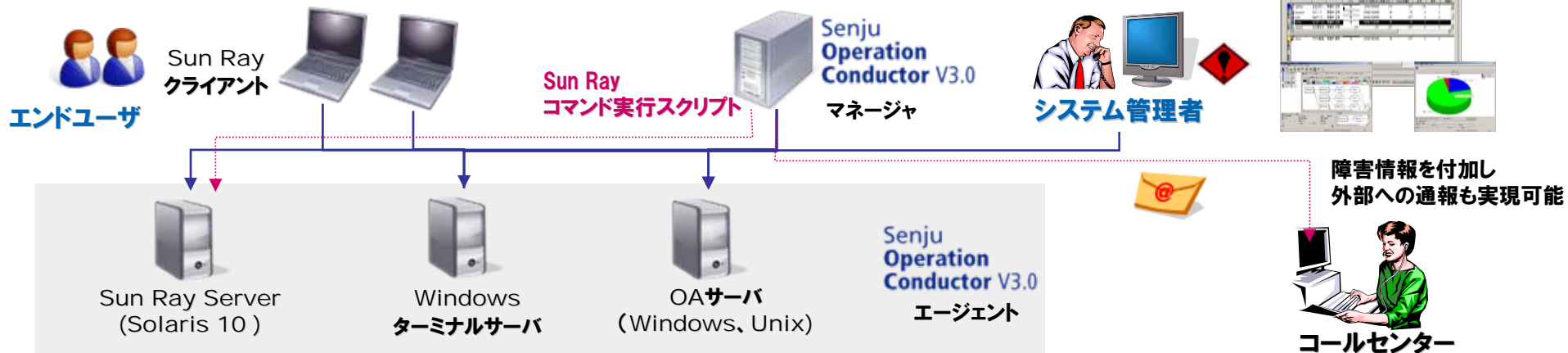
Solaris 10+SybaseIQ環境での実績がある
「**Senju Operation Conductor**」で統合管理



III. サン・マイクロシステムズ様との連携事例 Sun Ray監視ソリューション Sun Ray+Senju Family

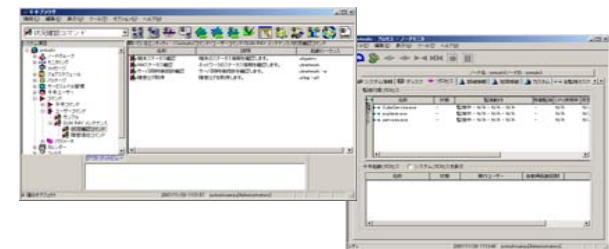
■Sun Ray環境の統合監視

- Senju/OCマネージャより、Sun Rayサーバを監視。
- 不具合を検知した際は、外部通報も自動化(障害メール、パトランプ)



■特徴

- Sun Ray環境で、障害として検知すべき事象を検知するための**監視テンプレート**を用意
- Sun Ray環境向け、**障害切り分け、復旧コマンド**を用意



最後に

- 基幹業務に安心して、Solaris x86を導入してください
- 基幹業務に安心して、Solarisコンテナを導入してください

⋮

 **があります**

お問い合わせは → senjuinfo@nri.co.jp

NRI

未来創発

Dream up the future.

お問い合わせは → senjuinfo@nri.co.jp