Empowered by Innovation NEC

セキュアOSによる内部統制の強化

2006年6月

NECソフトウェア東北 株式会社

Agenda

1. 内部統制とは
2. 内部統制と情報セキュリティ
3. セキュアOSによる内部統制の強化
4. セキュアOS適用事例
   ～バックエンドのセキュリティを支えるセキュアOS～

1．内部統制とは

1．なぜ今、内部統制が求められるのか？

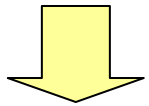
1．企業の不祥事多発

（1） 米国における不祥事の続発

・エンロン、ワールドコム、・・・・・

（2） 日本における不祥事の続発

・コクド/西部鉄道、カネボウ、ライブドア・・・・・



2．不祥事件の対応策：投資家の保護強化策

・米国：SOX法＝米国企業改革法（ Sarbanes-Oxley Act）における**内部統制の要求**

・日本：会社法および証券取引法の改正に**内部統制の要求**

※会社法改正（2006年5月施行）
→大手企業の内部統制システム構築の基本方針策定の義務化

2. 内部統制の目的

内部統制とは法律や企業ルールに基づき、不正やミスのない効率的・効果的な経営・業務を遂行し、会社全体をコントロールする仕組みを表す。

内部統制の目的

①経営および業務の有効性及び効率性を高めること

②組織の財務報告の信頼性を確保すること

③事業活動に関わる法令等を遵守すること

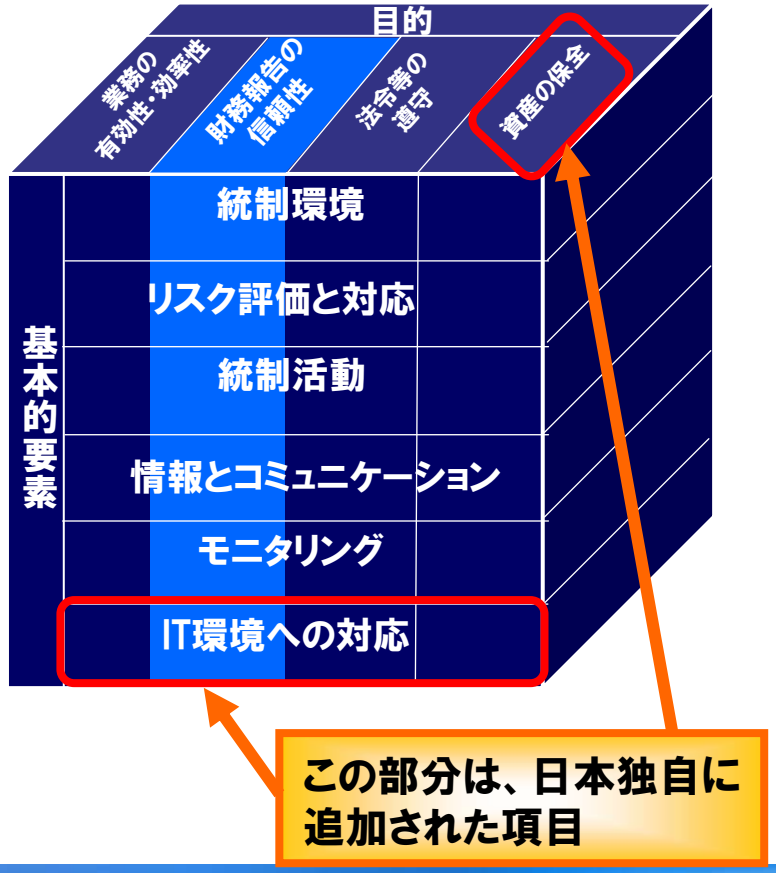
④資産の取得、使用、処分が正当に行われるよう、資産の保全を図ること　※1

※1：この部分は、日本独自に追加された項目

3. 内部統制の構成要素

企業等の4つの目的の達成のために、企業内のすべての者によって遂行されるプロセスであり、6つの基本的要素から構成される

【内部統制フレームワーク】



6つの基本的要素

①統制環境

経営理念、経営方針など経営トップの誠実性・倫理観が重要

②リスクの評価と対応

経営リスクの認識、分析、評価を行いリスク対応方針を決定すること

③統制活動

指示や命令に対する方針や手続き（承認、権限、査閲、評価など）

④情報とコミュニケーション

必要な情報が適宜、適切に伝えられること

⑤モニタリング

内部統制の有効性・効率性を継続的に監視・評価するプロセスや是正

⑥IT環境への対応

業務に組み込まれているITを活用すること

「IT全般統制」と「業務処理統制」の2つがある

2. 内部統制と情報セキュリティ

1．内部統制の基本的要素としての「ITへの対応」

「ITへの対応」を情報システムとして捉える場合には、「ITの利用」は「業務処理統制」に、「ITの統制」は「IT全般統制」に相当するとみなす

ITへの対応

IT環境への対応

社会及び市場におけるITの浸透度、組織のITの利用状況　等

ITの利用及び統制

ITの利用　ITを有効かつ効率的に利用すること

業務処理統制
個々のアプリケーションシステムにおいて、承認された取引が全て正確に処理され、記録されることを確保する、コンピュータ・プログラムに組み込まれた（自動化された）統制活動

- インプット・コントロール
- プロセス・コントロール
- アウトプット・コントロール
- データ・コントロール
- アクセス・コントロール

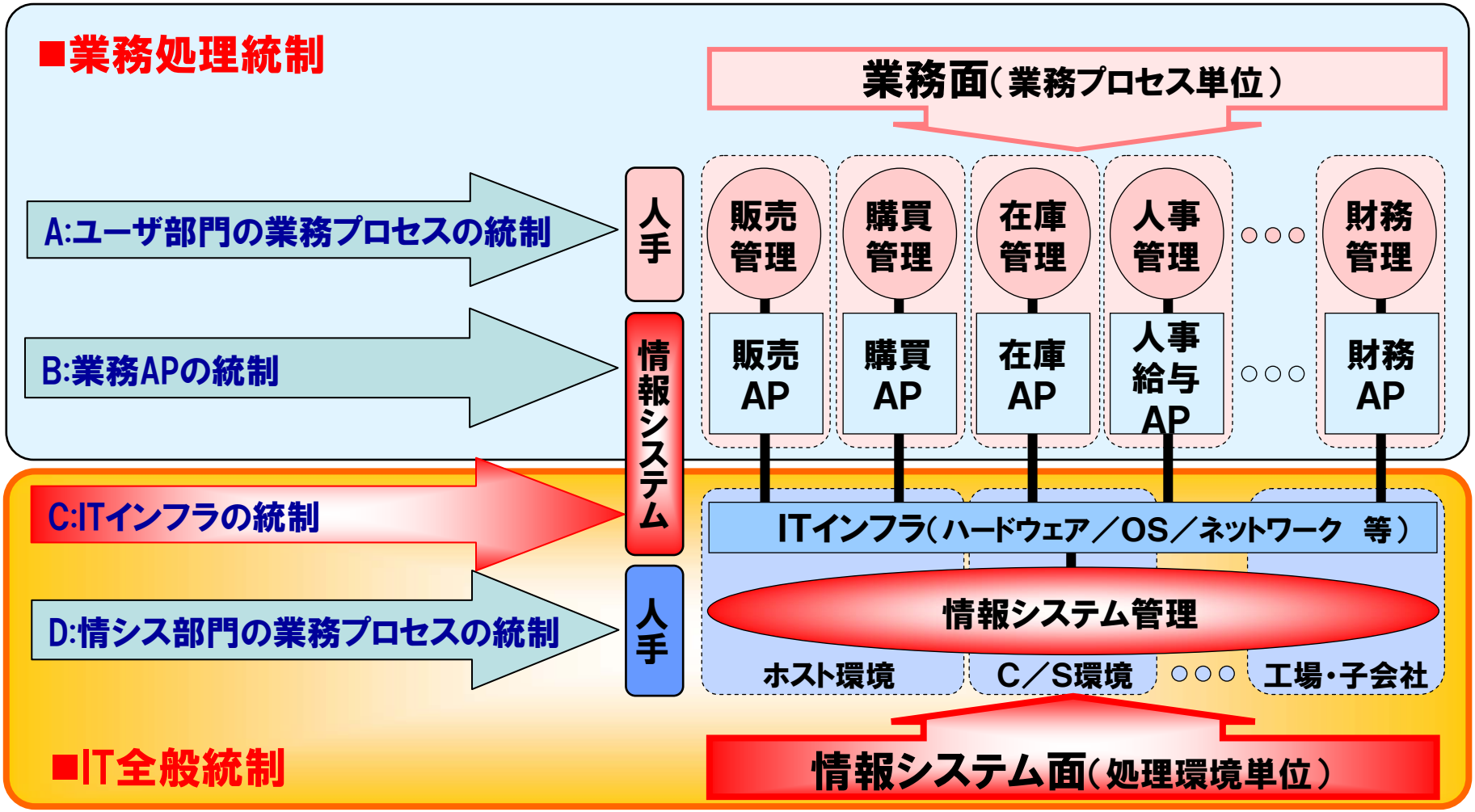
ITの統制　業務に組み込まれて利用されているITに対して、予め適切な方針と手続を定め、他の基本的要素を有効に機能させること

IT全般統制
業務処理統制が*有効に機能する環境を保証する間接的な統制活動*

- ①組織及び計画
- ②企画・開発プロセス
- ③運用プロセス
- ④維持・保全プロセス
- ⑤情報セキュリティ
- ⑥事業継続/災害対策
- ⑦外部委託

2. 業務処理統制/IT全般統制と情報システム

人の面、ITの面、両方から統制をかけて、リスクの低減を図る



システムのバックエンドを支える「IT統制」は重要!!

3. IT統制による信頼性保証

IT統制により情報セキュリティプロセスを適切にコントロールすることで企業の信頼性の確保、企業価値の向上を図る

代表的な情報セキュリティ プロセス

①セキュリティポリシー・基準・規定
②セキュリティ管理体制
③個人認証方法
④ウィルス対策
⑤アクセス制御
⑥アクセスログ取得・保管

セキュアOSが最も得意とするプロセス

セキュアOSによる
内部統制の強化を実現！

3. セキュアOSによる内部統制の強化

1．セキュアOSとは

通常のOSのセキュリティを強化したOS、またはそれを強化させる製品のことを指します。

強化のポイントとなるのは、以下の2点です。

1）**強制アクセス制御機能**

管理者（rootやAdministrator）に対してもアクセス制御を強制できるため、万が一管理者権限を乗っ取られた場合でも機密情報ファイルを保護することが出来ます。

2）**管理者特権の排除（最少特権）**

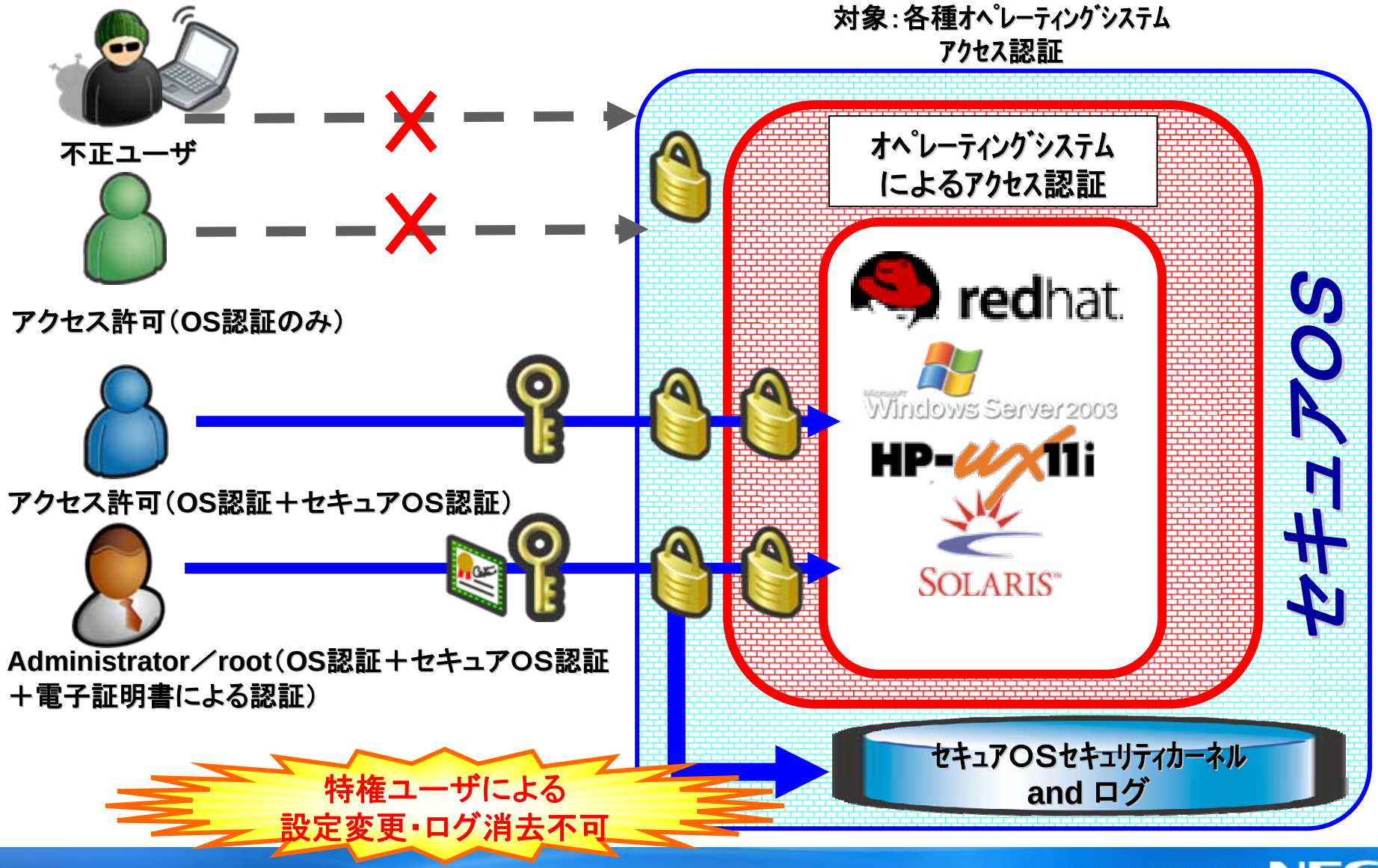
ユーザやプロセスごとに必要最少限の適切なアクセス権限を付与することで、権限が侵害された場合のリスクを軽減することが出来ます。

つまり、“何でも出来る”管理者特権を排除するため、rootやAdministratorへの権限昇格による不正行為を防ぐことが出来ます。

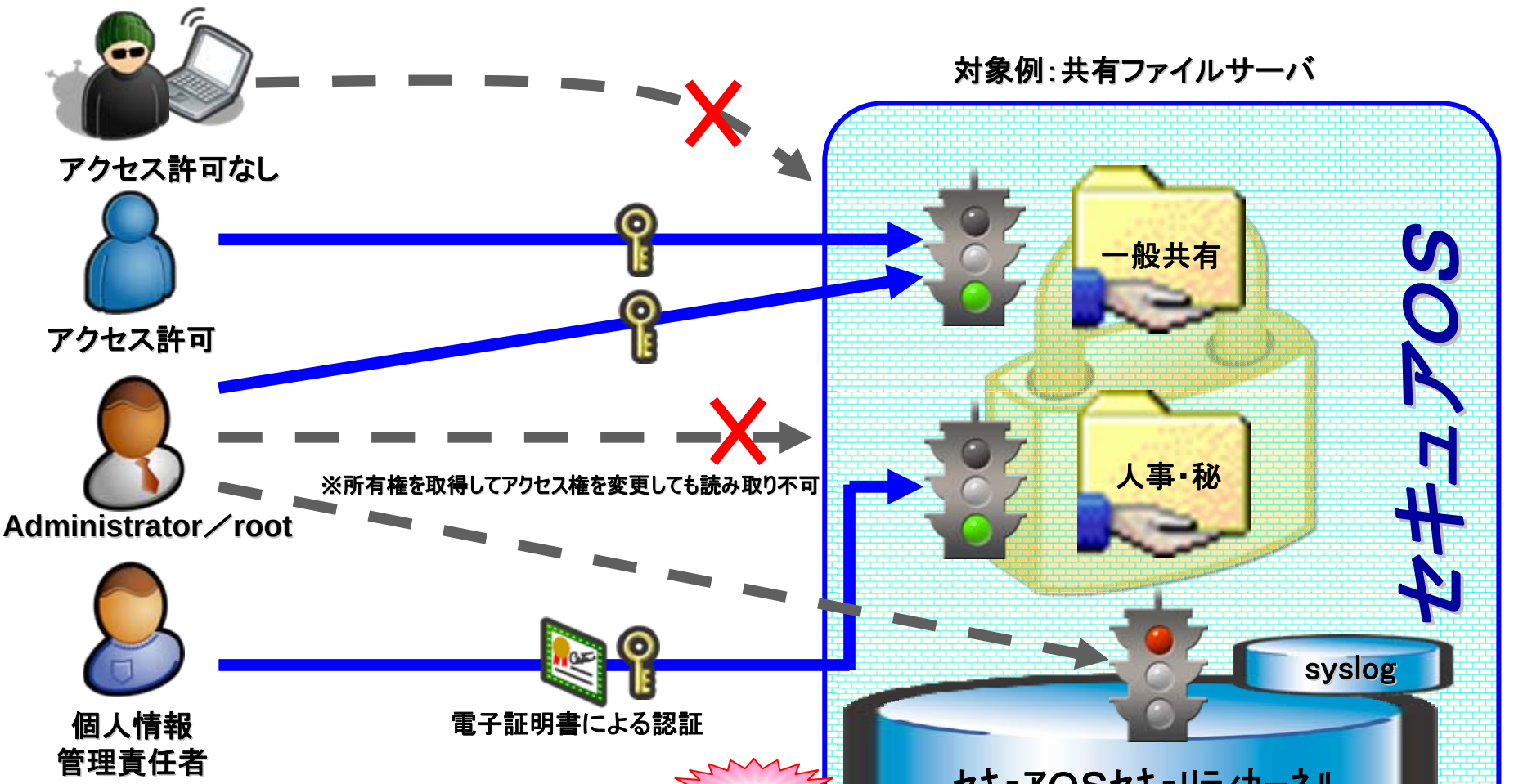
これらが一般的にセキュアOSと呼ばれる製品の主要機能となります。

内部統制として期待できる効果は・・・・

2. 機密データへのアクセスにおける識別と認証



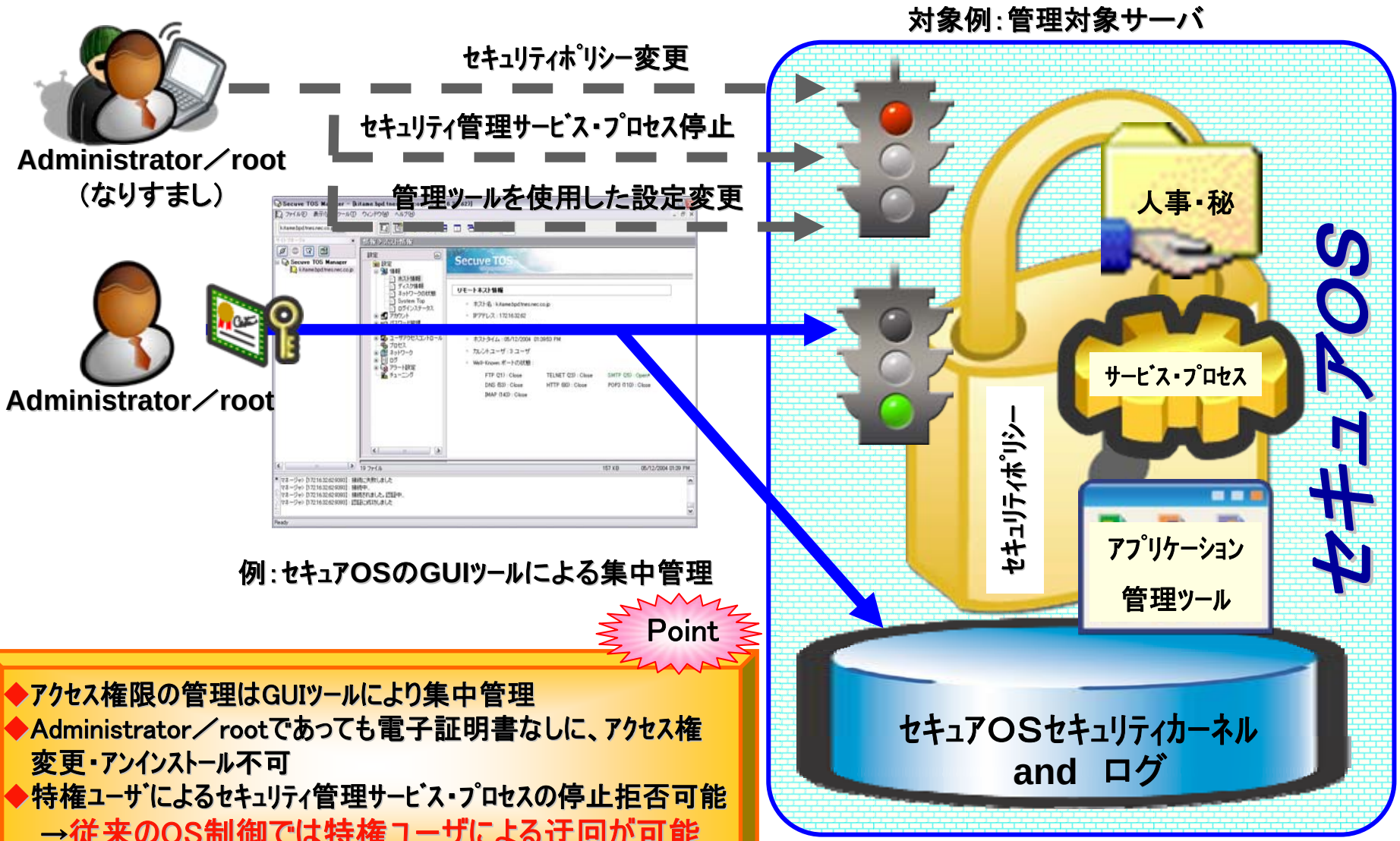
3. 機密データへのアクセス制御



Point

◆Administrator／rootであってもアクセス不可を実現
◆Administrator／rootであってもアクセス権変更による回避不可
→従来のOS制御では特権ユーザによる迂回が可能

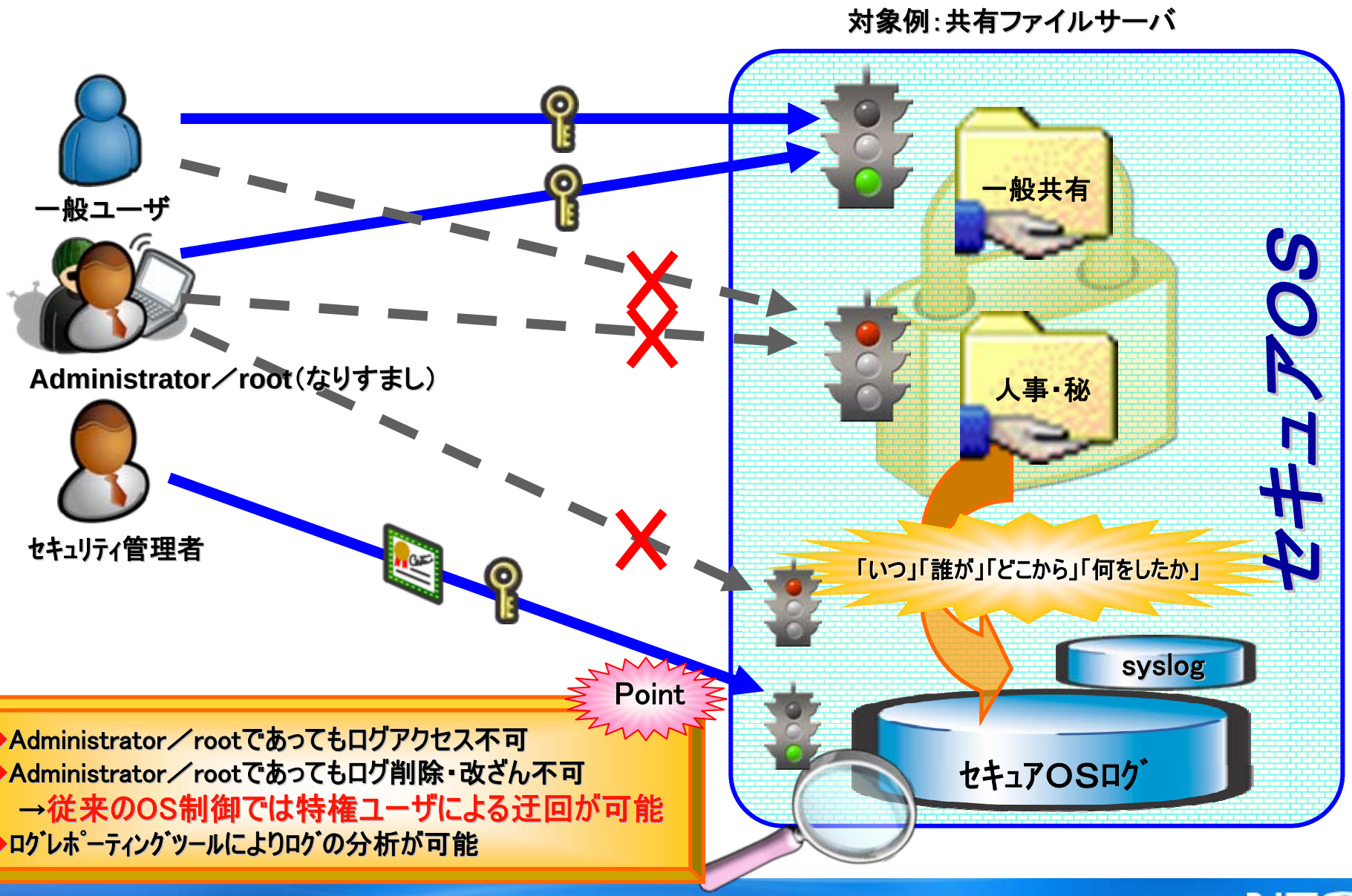
4. 機密データへのアクセス権限の管理



Point

- ◆アクセス権限の管理はGUIツールにより集中管理
- ◆Administrator／rootであっても電子証明書なしに、アクセス権変更・アンインストール不可
- ◆特権ユーザによるセキュリティ管理サービス・プロセスの停止拒否可能
  →従来のOS制御では特権ユーザによる迂回が可能

5. 機密データのアクセスの記録



Empowered by Innovation NEC

4. セキュアOS適用事例

～バックエンドのセキュリティを支えるセキュアOS～

バックエンドセキュリティ適用事例

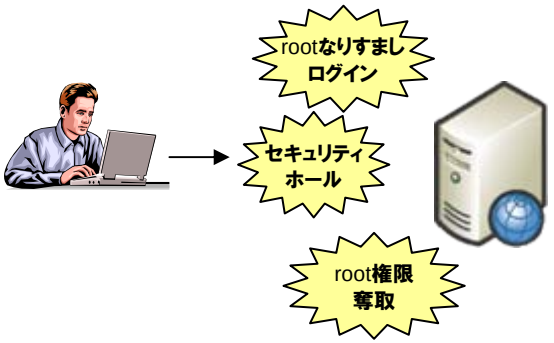
- 公開Webサーバ
- ファイル共有サーバ
- その他サーバ
  - データベースサーバ
  - ActiveDirectoryサーバ
  - セキュリティ管理サーバ
  - ログ管理サーバ

適用事例① 公開Webサーバ（1/2）

- **脅威**
  - ✓ 管理者パスワード漏えいによる不正ログイン
  - ✓ セキュリティホールを突いた不正侵入、管理者権限の奪取
- **リスク・被害**
  - ✓ コンテンツ改ざん
  - ✓ プログラム停止によるサービス妨害（機会損失）
  - ✓ 不正プログラムの組込み
    ⇒ 情報漏えい、フィッシング詐欺等の踏み台（信用失墜）

セキュアOSを適用すると

もし侵入に成功しても・・・



セキュアOSで防御

- シェルや任意コマンドの実行
- システム設定変更
- コンテンツデータ／ログの改ざん
- 不正プログラムの組込み

適用事例① 公開Webサーバ（2/2）

◆ ポリシー設定例(一部)

セキュアOSの アクセスコントロールリスト

Subject	操作	ポリシー
/usr/sbin/httpd	Read	許可
root	Read	許可
webmaster	Read/Write	許可
デフォルト		拒否

Subject	操作	ポリシー
root（＋電子証明書）	All	許可
デフォルト		拒否

Webサーバ

/var/www/html/
（コンテンツ格納ディレクトリ）

/etc
（システム設定ファイル）
/bin, /sbin, /usr/bin, /usr/sbin
（管理コマンド）
/var/log/
（ログ格納ディレクトリ）

- ✓ http デーモン からは コンテンツの 参照のみ許可
- ✓ root ユーザ からは コンテンツの 参照のみ許可
- ✓ webmaster（コンテンツ管理者）は コンテンツの データ更新を許可
  ※ 電子証明書を用いた厳密なユーザ認証を組み合わせることも可能

ポイント！

- root 権限が奪われても、コンテンツデータ改ざん不能
- Apache の権限が奪われても、シェル、その他コマンド操作不能

適用事例② ファイル共有サーバ（1/2）

◆ 脅威

- ✓ 管理者パスワード漏えいによる不正ログイン
- ✓ 外部業務委託者・システム管理者による機密情報への不必要なアクセス
- ✓ 外部業務委託者・システム管理者の権限濫用

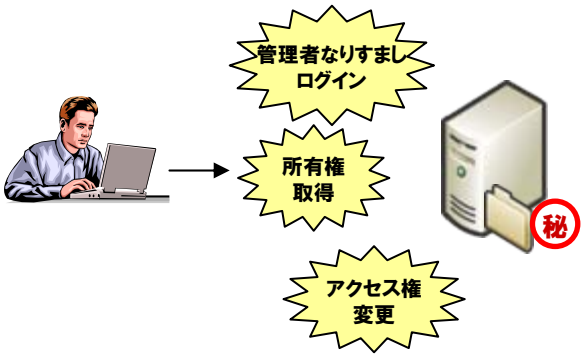
システム管理者は、自身に対するアクセス権を変更することが可能

◆ リスク・被害

- ✓ 機密情報、個人情報などの情報漏えい

セキュアOSを適用すると

管理者でログインできても



セキュアOSで制限

- 機密情報へのアクセス／閲覧
- 重要データやログの書き換え

適用事例② ファイル共有サーバ（2/2）

◆ ポリシー設定例(一部)

セキュアOSの アクセスコントロールリスト

Subject	操作	ポリシー
Administrators	All	拒否
stuff	All	許可
デフォルト	All	拒否

ファイルサーバ

C:¥DATA¥人事

（機密情報格納フォルダ）

- ✓ 関係業務部門からは 機密情報への アクセス許可
- ✓ Administrator(システム管理者)からは 機密情報へのアクセス拒否

※ 所有権の取得とアクセス権変更は可能(任意アクセス制御)
ただし、セキュアOSのアクセス制御(強制アクセス制御)が優先

ポイント！

- システム管理者がファイル所有権を取得し、自身に対するアクセス権を変更しても機密情報へのアクセスを禁止することが可能

適用事例③ その他サーバ（1/2）

◆ 対象サーバ

- ✓ データベースサーバ
- ✓ ActiveDirectory サーバ
- ✓ **セキュリティ管理サーバ**
- ✓ **ログ管理サーバ**

◆ 脅威

- ✓ システム管理者（なりすまし）による以下の行為を防げない
  - ➢ データベース管理コマンド、操作コマンドを使用した不必要なDBアクセス
  - ➢ 不正行為に利用するためのユーザアカウント追加
  - ➢ **自身に対するセキュリティポリシー変更、セキュリティ設定解除**
  - ➢ **ログの書き換え／消去による証拠隠滅**

◆ リスク・被害

- ✓ 機密情報、個人情報などの情報漏えい

セキュアOSを適用すると

管理者でログインできても

（共有アカウント）

セキュアOSで制限

- 管理者コマンド/ツールの実行
- セキュリティ解除
- 重要データやログの書き換え

適用事例③ その他サーバ（2/2）

◆ ポリシー設定例(一部)

セキュアOSの アクセスコントロールリスト

Subject	操作	ポリシー
Administrator	All	拒否
Administrators	All	許可
デフォルト	All	拒否

管理者コマンド
管理ツール

Subject	操作	ポリシー
システム	All	許可
アプリケーション	All	許可
デフォルト	All	拒否

システムログ
アップリケーションログ

- ✓ Administrator（共有アカウント/パスワード）からは アクセス拒否
- ✓ Administrators（管理者グループメンバ）からは アクセス許可
  - ※ 管理者グループに所属するユーザにのみ管理者権限を許可
    管理者作業のログ履歴は、追跡が可能なログインアカウント名で出力
  - ※ 電子証明書を用いた厳密なユーザ認証を組み合わせることも可能
- ✓ ログへの書き込みは、システム、アプリケーションからのみ許可

ポイント！

- 複数ユーザによる管理者アカウント／パスワードの共有を禁止し、ログインアカウント名による管理者作業のログが取得可能

バックエンドセキュリティはセキュアOS！！

「内部統制は業務パッケージ製品の導入やセキュリティ製品の導入だけで実現できるものではありません。また、いくら万全な業務処理統制のしくみを構築しても、それを支えるOSのセキュリティが従来のまま変わらなければ、”砂上の楼閣”です。

セキュアOSは、業務処理統制が有効に機能する環境を保証するツールとして非常に有効です。**バックエンドセキュリティ**は**「セキュアOS」**にお任せください。

ご清聴ありがとうございました。

Empowered by Innovation

SecuveTOS とは

不正アクセスによる情報漏えい、サイバーアタック、未知のワーム感染など様々な脅威から情報システム/情報資産を守るためにOSそのもののセキュリティを強化するソフトウェア(セキュアOS)です。

	従来OS（問題点）	従来OS + SecuveTOS
DMZ上の公開サーバ	•管理者パスワードが漏えいするとサーバが完全に乗っ取られてしまう •セキュリティホールが存在すると、インターネットユーザから許可していないはずのアクセスができてしまう （※ワームも同様な手口により侵入/感染）	万一、侵入されても重大な被害なし ↓ 強固なセキュリティを実現
ファイアウォール		
内部情報システムサーバ	•管理者ユーザ※に対して、必要以上のアクセスを許してしまう（人事情報、個人情報、etc） •管理者ユーザ※はセキュリティの解除やログ消去ができる(管理者による不正を防げない） •情報漏えい事件が起きると管理者ユーザが疑われる　管理者の正当性を立証できない ※管理者"なりすまし"ユーザを含む	管理者権限の濫用を防止 管理者の正当性を立証 ↓ 強固なセキュリティを実現 抑止効果の実現

お客様の声は・・・・

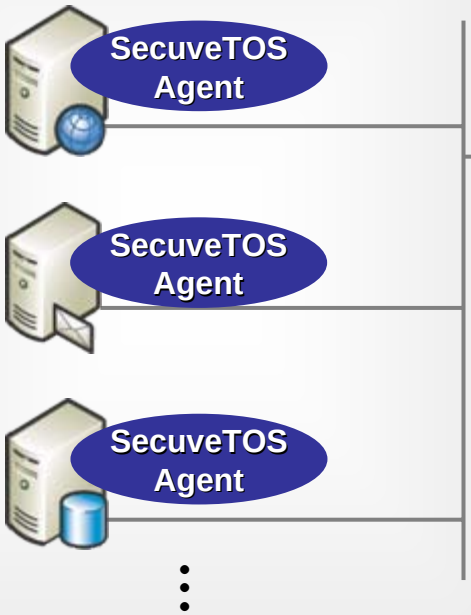
- ✓ コマンドベースの設定は難しすぎる・・・何とかならない？
  - ➢GUIベースの管理ツールが必要
- ✓ サービスポートを利用できるプログラムを制限できたら良いのに・・・
  - ➢ネットワーク制御機能が必要
- ✓ セキュアOSでもセキュリティ管理者のID、PASSが漏れたら同じでしょ？
  - ➢電子証明書による厳密な認証が必要
- ✓ 何か不正なアクセスが行われたらすぐに知らせてくれないと・・・・
- ✓ 管理ツールは増やしたくない！監視ツールは統合したい！
  - ➢リアルタイム警告機能が必要
- ✓ ログが取れてるのは分かるけど、中身が分からない！
  - ➢ログレポーティング機能が必要

SecuveTOS自体の進化が必要！

機能強化1．GUIによる一元管理

◆ SecuveTOS Agent

保護対象サーバごとに導入するセキュリティモジュール
（各種プラットフォームに対応）



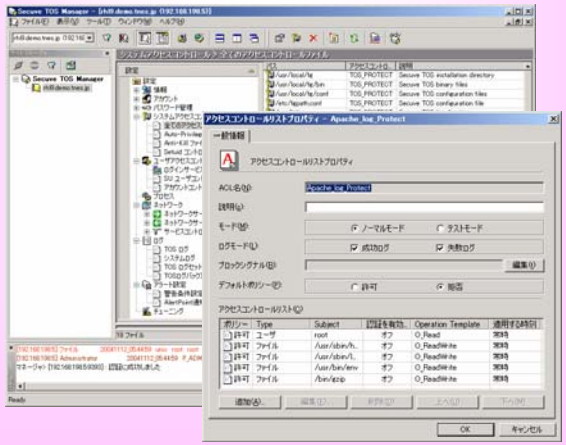
- **Windows系サーバ（WindowsNT4.0 / 2000 / 2003）**
- **Linux**
- **UNIX（Solaris, HP-UX, AIX）**

◆ SecuveTOS Manager

セキュリティ管理用PCに導入するAgent管理用ソフトウェア（Windowsソフトウェア）

各Agent への接続時 にはAgent が発行する電子証明書を使用した認証が必要

Manager

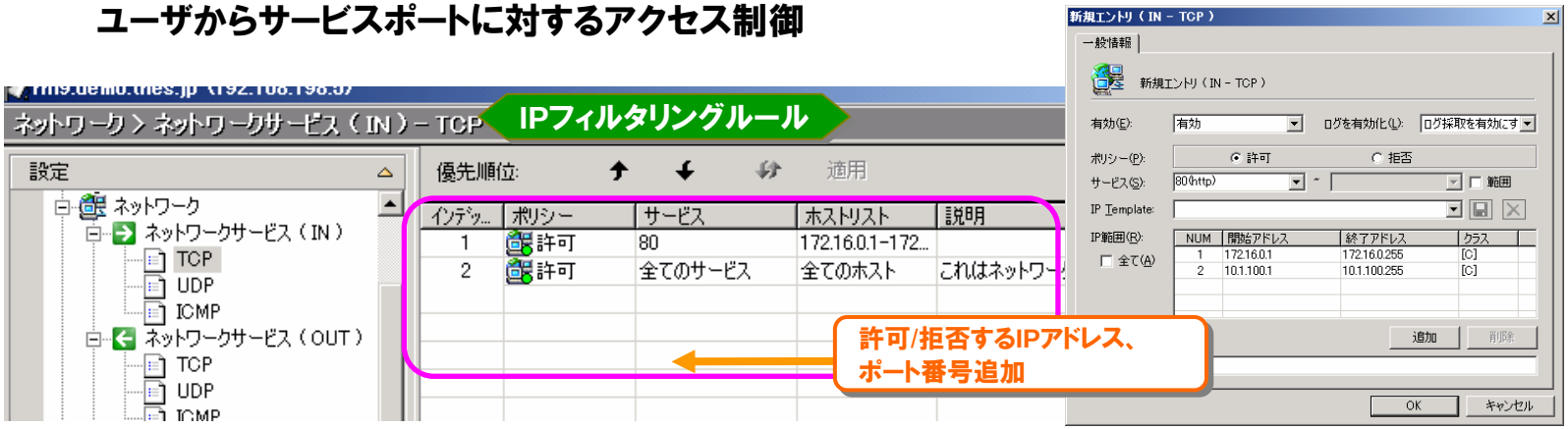


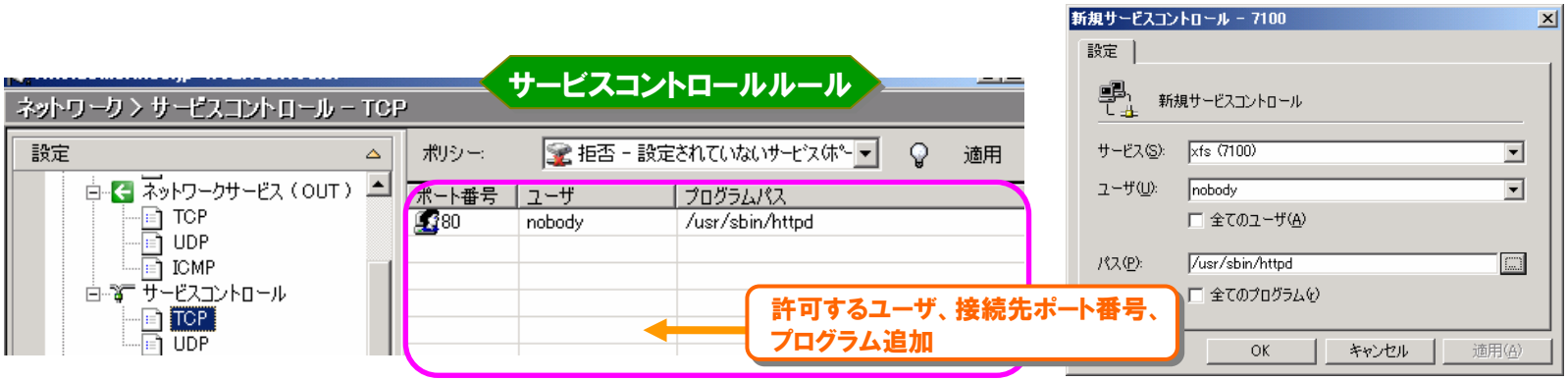
機能強化2. ネットワークサービス制御

◆ ネットワークサービス制御

**ネットワークサービスに対するアクセス制御機能により、外部ネットワークからの不正アクセスや
イントラ内における機密情報サーバなどへの不必要なアクセスを防止します。**

- ✓ **ネットワークサービス（IN / OUT）**
  IPフィルタリングによるネットワークアクセス制御
- ✓ **サービスコントロール**
  ユーザからサービスポートに対するアクセス制御

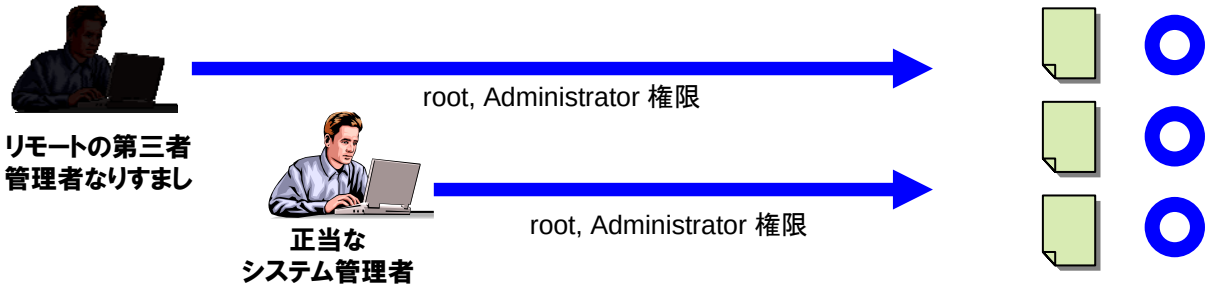




機能強化3．電子証明書による認証

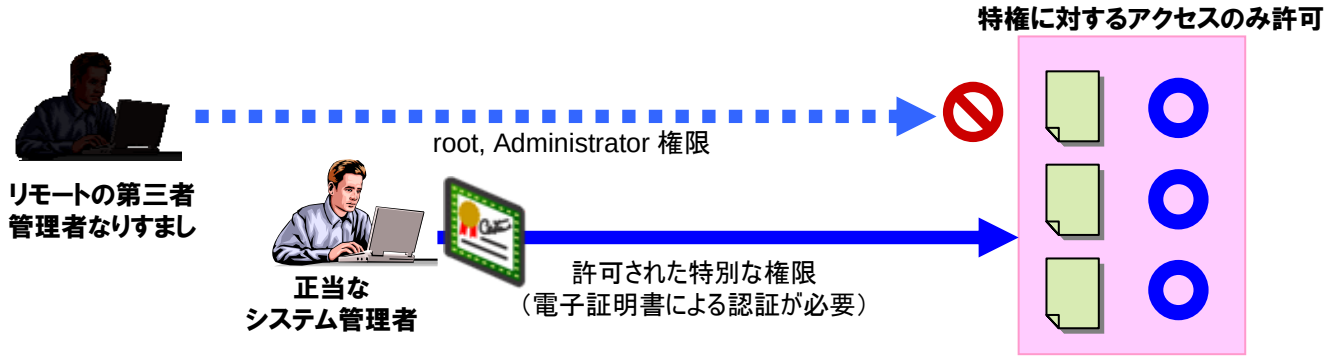
● ID／パスワードによる認証

パスワードが漏えいした場合、または管理者権限が奪われた場合、
正当なシステム管理者 と 悪意のある第三者との区別ができない



● 電子証明書による認証

電子証明書を持つ正当なシステム管理者にのみ権限を与えることができる

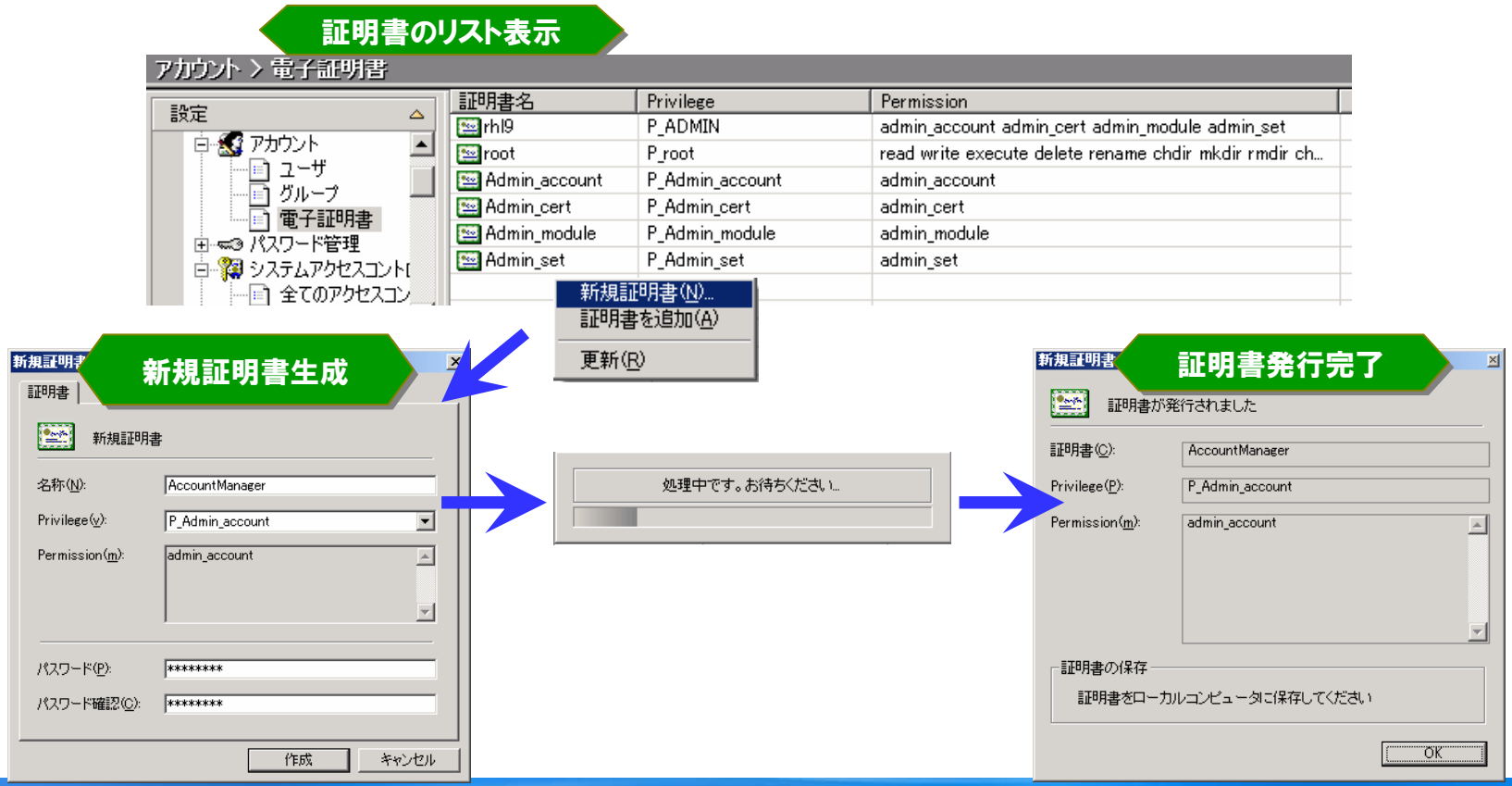


機能強化4. 電子証明書の管理

◆ 電子証明書の管理

電子証明書の生成、削除、リスト表示などの管理機能を備えています。
ユーザアカウント管理、アクセスコントロール設定の変更、Webコンテンツ更新など、重要ファイルへのアクセスを許可する特別な権限(特権)に対して電子証明書を発行することができます。

作業者ごとに必要最小限の権限(最小特権)を付与し、異なる電子証明書を発行することも可能です。

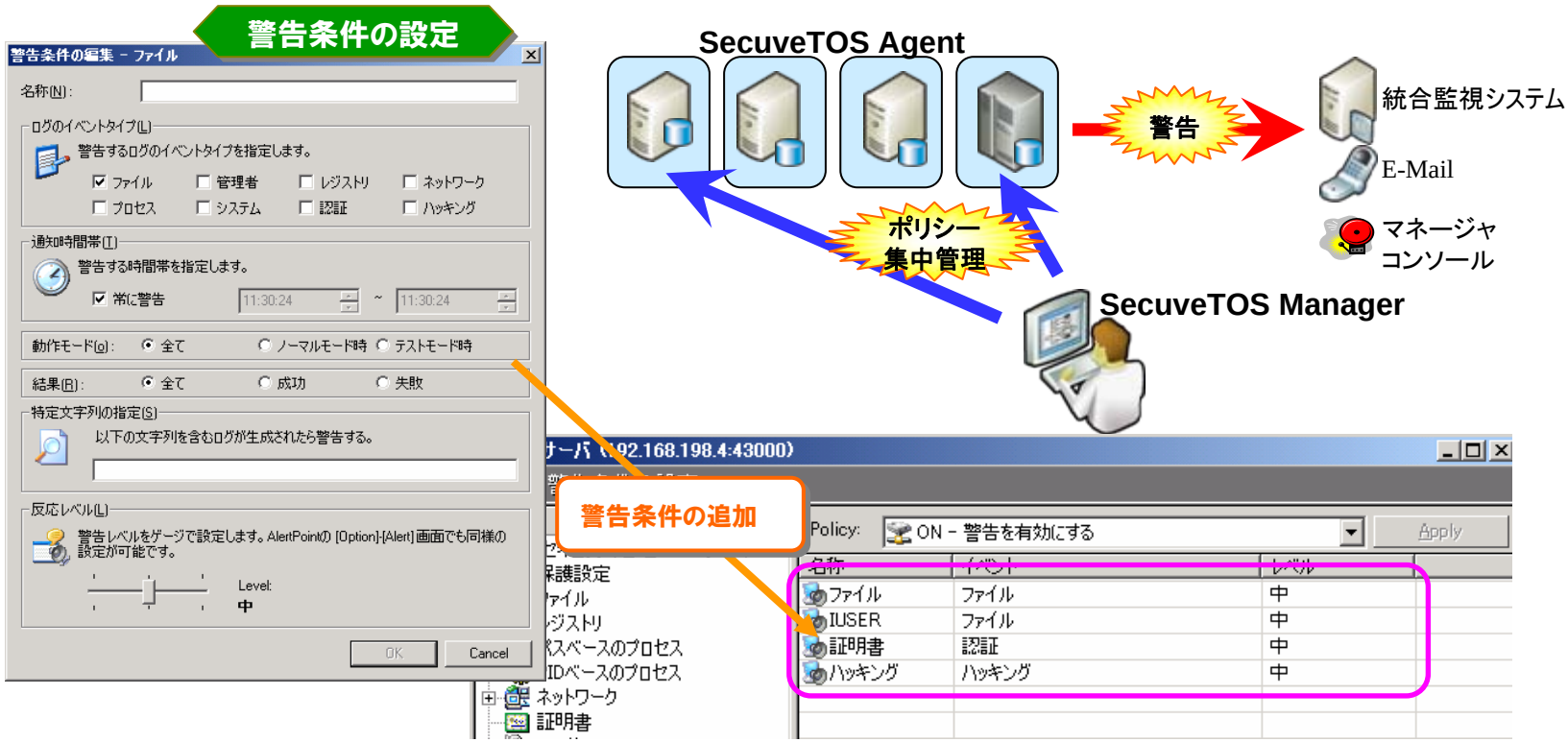


機能強化5. リアルタイム警告

◆ リアルタイム警告機能

特定のイベント発生時、あらかじめ指定した先へリアルタイムで通報します。
以下の通報手段を指定可能です。

- ✓ SecuveTOS マネージャコンソールへのポップアップ
- ✓ E-Mail アドレスへのメール送信
- ✓ SNMP Trap　※ すでに導入済みの統合監視システムへの通報

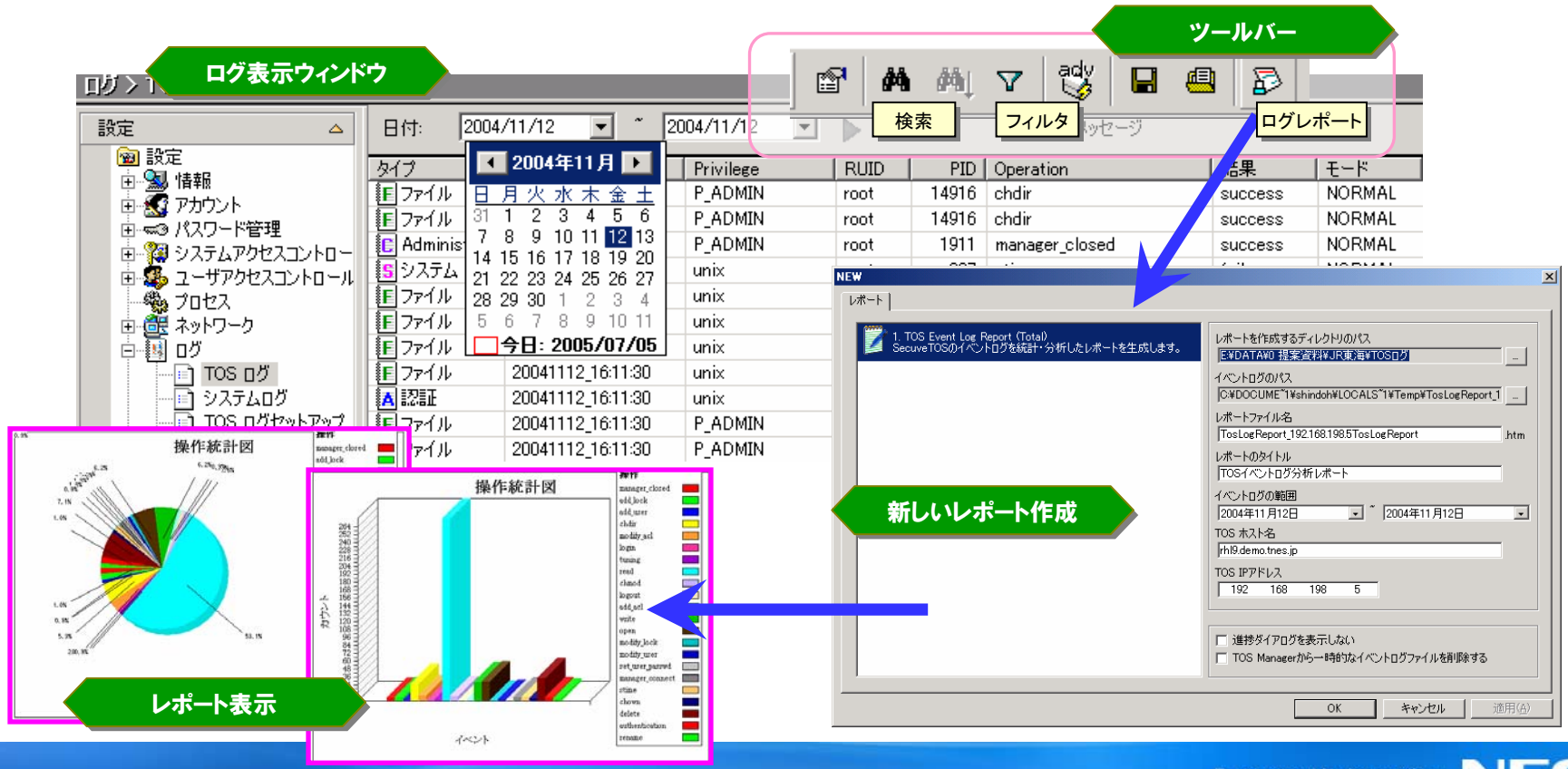


機能強化6．ログレポーティング機能

◆ ログレポーティング機能（ログレポータ）

SecuveTOSのセキュリティ監査イベントログに基づいた統計データを提供します。セキュリティ管理者による定期的なアクセス状況の診断が可能です。

- ✓ **監査イベントタイプ別の統計データ**
- ✓ **操作（オペレーション）別の統計データ**
- ✓ **プロセスイベント（成功/失敗）とユーザ別の統計データ**



SecuveTOSついてのお問い合わせ先

■お問合せ

◇NECソフトウェア東北
ITソリューション事業部 ソリューション営業部

電子メール　：sales@tnes.co.jp

Webサイト　：http://www.tnec.co.jp/products/tos.html