ログ管理の課題を解決する
「統合ログ管理ソリューション」のご紹介

2007年11月19日
日本ユニシス株式会社
共通利用技術部
伊藤　直行

UNISYS

目次

1 ログを取り巻く環境の変化

2 ログ管理の実践ポイント

3 ログの課題を解決する統合ログ管理ソリューション

4 ログ活用におけるケーススタディ

1 ログを取り巻く環境の変化

2 ログ管理の実践ポイント

3 ログの課題を解決する統合ログ管理ソリューションログ

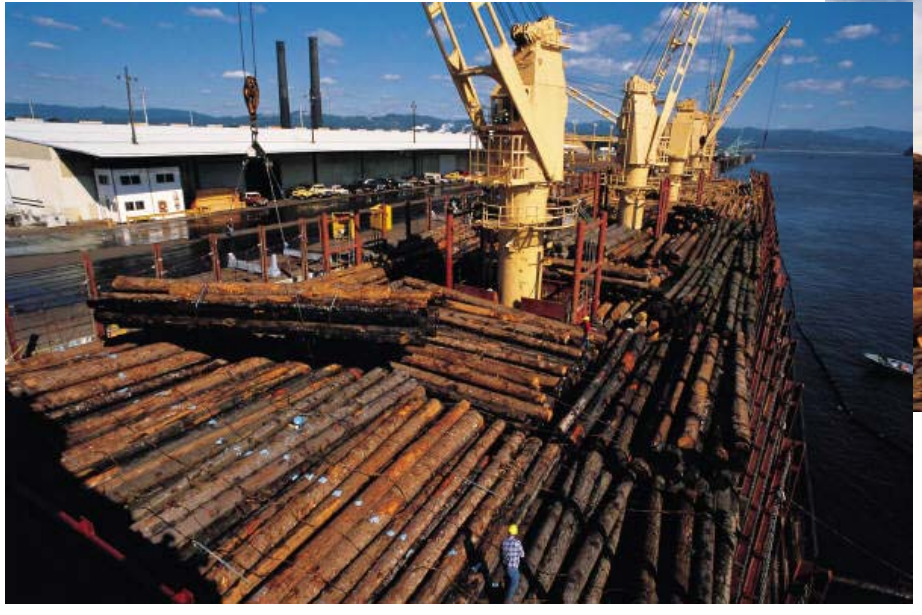
4 ログ活用におけるケーススタディ

1-1. ログの語源は？

UNISYS

「航海日誌(logbook)」

船の速度を測るのに丸太（log）に一定間隔に結び目のあるロープをくくりつけて浮かべていたことに由来(出典: ウィキペディア(Wikipedia))



1-2. コンピュータにおける「ログ」とは？

UNISYS

現代の解釈：「情報システムにおける履歴情報（4W1H）」

1. Who　　誰が？（処理の実行者）
   ⇒ ログに出力されたIDが特定の個人と紐付けされている
2. When　　いつ？（処理の時間）
   ⇒ タイムスタンプ等で正確な時刻が利用されている
3. What　　何を？（処理の対象）
   ⇒ ファイル名、DB等から何に対する行為か指定できる
4. Where　　どこで？（処理の実行場所）
   ⇒ IPアドレス、サーバ名、フォルダ名等から指定できる
5. How　　どうした？（処理内容）
   ⇒ 処理した内容が、ログから理解できる

システム担当

内部統制担当

When?　How?　Who?

```
Nov 11 00:00:00 kei newsyslog[16431]: logfile turned over
Nov 11 00:03:39 kei sendmail[16745]: gAAF3dF2016745: from=root, /var/log/maillog の例
nrcpts=1, msgid=<200211101503.gAAF3dF2016745@kei.example.co.jp>, relay=root@localhost
Nov 11 00:03:39 kei sendmail[16745]: gAAF3dF2016745: to=root, ctladdr=root (0/0),
delay=00:00:00, xdelay=00:00:00, mailer=relay, pri=30278, relay=localhost.example.co.
[127.0.0.1], dsn=4.0.0, stat=Deferred: Connection refused by localhost.example.co.jp.
Nov 11 00:06:59 kei sendmail[17018]: gAAF6x9N017018: from=root, size=288, class=0,
nrcpts=1, msgid=<200211101506.gAAF6x9N017018@kei.example.co.jp>, relay=root@localhost
Nov 11 00:06:59 kei sendmail[17018]: gAAF6x9N017018:
delay=00:00:00, xdelay=00:00:00, mailer=relay, pri=3
[127.0.0.1], dsn=4.0.0, stat=Deferred: Connection re
```

メールサーバ（sendmail）のログの例

UNISYS

＜かつては・・＞　システムトラブルの解析が主要用途

- アプリケーションのデバッグが主目的(=トレースログ)
- システムが安定稼働期に入ってから意味のないデバッグコードの出力を抑制し、システムへの負荷を軽減するケースが多い
- MFシステム、一昔前のオープン系システムが対象

→　ログの利用範囲は限定的だった

```
N 07/06/19 19:02:41 REL dsms_rel_CONSTRUCTOR 2163 : dsms_rel_CONSTRUCTOR.c 71  : メソッドの開始。
N 07/06/19 19:02:41 REL dsms_rel_CONSTRUCTOR 2163 : dsms_rel_CONSTRUCTOR.c 76  : argv[1] = hpd3
N 07/06/19 19:02:41 REL dsms_rel_CONSTRUCTOR 2163 : dsms_rel_CONSTRUCTOR.c 76  : argv[2] = fireu210
N 07/06/19 19:02:41 REL dsms_rel_CONSTRUCTOR 2163 : dsms_rel_CONSTRUCTOR.c 76  : argv[3] = hpd3-stn
N 07/06/19 19:02:41 REL dsms_rel_CONSTRUCTOR 2163 : dsms_rel_CONSTRUCTOR.c 76  : argv[4] = /home/dstsms/ds_test/rel_test/keiyu
W 07/06/19 19:02:41 REL dsms_rel_CONSTRUCTOR 2163 : rel_cmn_attrconf.c 170 : accessエラー
W 07/06/19 19:02:41 REL dsms_rel_CONSTRUCTOR 2163 : rel_cmn_attrconf.c 620 : /opt/dsms/dbbase/rel/AttrConf.stn がない(チェック)
N 07/06/19 19:02:41 REL dsms_rel_CONSTRUCTOR 2163 : rel_cmn_filelock.c 230 : 非ロック
N 07/06/19 19:02:42 MRB dsms_mrb_GetPort 2174 : dsms_mrb_GetPort.cli.c 42  : 処理開始
N 07/06/19 19:02:42 MRB dsms_mrb_GetPort 2174 : dsms_mrb_GetPort.c 36  : 処理開始
N 07/06/19 19:02:42 MRB dsms_mrb_GetPort 2174 : dsms_mrb_GetPort.c 58  : 正常終了
```

トレースログの一例

エラー原因の発生ポイント

1-4. ログが注目される理由

UNISYS

＜昨今は・・＞

IT内部統制と情報セキュリティのために、ログが注目されている

人が情報システムに指示した行為には、必ずログが発生する。
その行為をモニタリングする為には、エラー情報だけでなく、インフォメーション情報にも注目しなければならない。




log → 正当な業務処理 → システムは、正当な処理を記録する

log → ヒューマンエラー → システムは、ミスを記録する

log → システムトラブル → システムは、トラブルを記録する

log → 不正 → システムは、不正を記録する

1-5. ログ管理をしなければならない根拠

UNISYS

財務報告に係る内部統制の評価及び監査に関する実施基準　より 抜粋　2007.2.15　金融庁
II. 財務報告に係る内部統制の評価及び報告

②　記録の保存

財務報告に係る内部統制について作成した記録の保存の範囲・方法・期間は、諸法令との関係を考慮して、企業において適切に判断されることとなるが、金融商品取引法上は、有価証券報告書及びその添付書類の縦覧期間（５年）を勘案して、それと同程度の期間、適切な範囲及び方法（磁気媒体、紙又はフィルム等）により保存することが考えられる。

記録・保存に当たっては、後日、第三者による検証が可能となるよう、関連する証拠書類をあわせて保存する必要がある。

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）より 抜粋　2007.3.30　経済産業省
第Ⅳ章 IT 統制の導入ガイダンス

c．運用の実施記録、ログの採取と保管

3-(2)-①-ホ	情報システムはアクセス記録を含む運用状況を監視することが望ましく、また、情報セキュリティインシデントを記録し、一定期間保管すること⇒（*システム管理基準　Ⅳ運用２（９）*）。
3-(2)-①-ヘ	情報システムで発生した問題を識別するために、システム運用の作業ログ・障害の内容ログ及び原因ログを記録し、保管すること。 取得されたログは、内容が改ざんされないように保管することが望ましい⇒（*システム管理基準　Ⅳ運用２（１１）～（１２）*）。

1 ログを取り巻く環境の変化

2 ログ管理の実践ポイント

3 ログの課題を解決する統合ログ管理ソリューション

4 ログ活用におけるケーススタディ

UNISYS

●「NIST SP800-92」

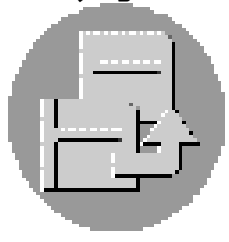
ログ管理のバイブル、ベストプラクティス集

- 米国商務省管轄の標準技術研究所が作成。
- ログ・マネジメントに関する組織のあるべき姿（ポリシー・管理指針）を明示。
- ログ管理（構築、管理手法）に関する書物としては充実度が非常に高い。
  - ◆システムの影響度に応じた、ログの保存期間や更新頻度、ログ管理システムへの転送頻度、分析頻度等について記載。
- 要素技術についても言及。暗号化方式、SIM、SEM、syslog、SNMP等々。
- http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

UNISYS

ログを安全な場所に退避する

- 監査証跡としての改ざん防止の必要性
- ベストな対策はリモートの”要塞化された“サーバに転送すること
  - ◆削除・変更されてもログサーバ側で正当性が確認可能
- 転送時の暗号化機能があると尚可
  - ◆転送プロトコル　IPSec、SSL等
  - ◆暗号化アルゴリズム　MD5、SHA-1、SHA-256等
- 長期保管用の「安全な場所」はWORM(Write-Once-Read-Many)メディアがお奨め
  - ◆CD/DVD-R、LTO4、UDO、アーカイビング・ストレージ(日立　HCAP、EMC Centera)等
  - ◆ただし長期保存向きの光学式媒体(MO、CD/DVD)は容量が少ない



UNISYS

ログを保存するストレージリソース(ディスク、テープ)への考慮

- 「なにか」あった時の暫定保存
  - 大規模システム、短期間での構築を余儀なくされるシステムで散見
  - 取得目的が不明確なケースが多いので取捨選択できていない
- 種類によっては大量のログを出力するものもある
  - (例) Windowsイベントログ　500GB/月、F/W、IDSのログ　1TB/月
- 必要なログデータの取捨選択を後回しにした場合、その間、リソース(ディスク、テープメディア、ランニングコスト)の無駄遣いとなる
  - LTO3テープ1本あたり2万円強
  - ハイエンドSANディスク　1TBあたり500～2000万円
  - テープ保管庫コスト(設置代、購入代)

UNISYS

ログの世代管理を忘れずに

- ログファイルの最大サイズの設定
  - 製品によってはログの種類毎に最大ログサイズを定義することが可能だが実質的な制限サイズが異なる場合がある。

    （例：Windowsのイベントログは4GBまで設定可能だが実際は300MBまで）
- ログサイズが一杯になったときの動作設定
  - 上書き？他のログファイルにサイクルアップ？処理停止？
  - MS製品ではデフォルト動作が上書きなので、設定変更かバックアップが必要
- 世代数の設定
  - 使用可能なディスク容量やサイクルアップ期間等に依存

UNISYS

時刻同期は必須

- 時刻同期の仕組み（NTPサーバ等）を既存のシステムに導入すべき（少なくとも各システム単位での同期は必須）
- 各システム内のサーバ、デバイス間で時間がずれていたら証跡として使い物にならない
- 時系列がバラバラであれば、事象（イベント）のトレースもできなくなってしまうため、結果としてインシデントの追及不能に陥ってしまう可能性が高い



2-6. 実践ポイント5

UNISYS

ログ出力時の既存システムへの影響を考慮

- 製品導入時のロギング設定の多くは無効
- ロギング・レベルの十分な検討（デバッグレベルのものまで必要かどうか）
- 不要なログの出力抑制（プログラム開発時点のデバッグコードの残留）
- 不要なコードが多いと「いざ」という時の解析作業が困難
- ディスク容量の監視等、運用面での考慮
  - ◆F/Wのsyslog等は大容量（数十GB/日）
  - ◆ディスクフルに注意（syslogは自動的に出力を停止）

UNISYS

ログのセキュリティを考慮

- ファイルサイズが減った時に警告を発する設定（※TripWire等）
- 出力先はデフォルトのパス以外に設定（攻撃者から発見しにくくする為）
- 変更権限のない悪意あるユーザに対する改ざん検知・防止策
  - ◆厳重なユーザアカウント管理
  - ◆ログ・ファイルに対する適切なアクセス権の設定（必要最小限の特権を付与）
- root権限の奪取対策
  - ◆TripWire等でシステムファイルの改ざん検知

※TripWire：ファイルの改ざん等をハッシュ関数や電子署名で検知するツール

2-8. 実践ポイント7

UNISYS

ログの保存期間は分析頻度に反比例する

- ログの分析頻度が高い場合（数回/日程度）は、高影響度システムでもログの保存期間は3～12ヶ月程度（※NISTの考え方）
- 国内企業の大部分は保存しているものの定期的分析までは実施できていない
- 分析がほとんどできていない場合は、重要なログ（機密情報へのアクセスログ等）を選定し3～5年保存を推奨
  - ◆ 不正アクセス禁止法やコンピュータ関連の刑法（電子計算機使用詐欺罪、電磁的記録不正作出及び供用罪等）の時効が大よそ3～5年となっているのが根拠
  - ◆ 事件発生時の裁判証拠としてログを利用するケースを想定

2-9. 実践ポイント8

UNISYS

（可能であれば）システム構築の初期段階から統合ログ管理システムの導入を検討すべき

- 安定稼動している既存システムへの途中参入は慎重に検討すべき（エージェントレスが推奨）
- ログ出力によるシステムリソースへの影響を考慮
  - ◆DB監査ログは多少影響あり（10%～20%）
- 既存のログ集約サーバとの整合性を考慮（syslogサーバ等）
- 既存のログデータの移行要件（要不要を検討）

1 ログを取り巻く環境の変化

2 ログ管理の実践ポイント

3 ログの課題を解決する統合ログ管理ソリューション

4 ログ活用におけるケーススタディ

3-1. ログ管理の先進国、米国企業におけるログ領域の課題は？

UNISYS

- ✓ 統合管理ができていない。セキュリティ上の問題を調査するに当たり、複数のユーザ・インターフェースにログインする必要がある。
- ✓ **高価なファイル共有システムにログを保管する傾向にある。**
- ✓ 異なるデバイスからのログを集中管理できない。
- ✓ 規制に対するコンプライアンスを実現する上で、時系列にログを保管できない。
- ✓ ログの破損、修正などにより、ログデータの完全性を保証できない。
- ✓ 異なるデバイスから出力される**ログの調査に時間が掛かりすぎている。**
- ✓ 独自にログ管理を行う場合、その作業は非常に面倒であり、得てして収集・保管に止まり、**分析やレポート機能までは実装できていない。**

一歩間違えると、無駄な投資コスト、作業効率低下を生み出す「負の源泉」になりえる！！

3-2.「統合ログ管理」を失敗しないために・・・

UNISYS

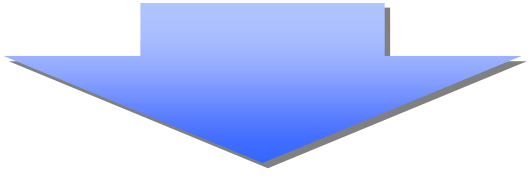
構築後の実運用を考え、設計・構築することが重要！

ログ管理・活用を行って業務の効率が悪くなってはいけません

設計・構築すれば終わりではなく、継続できる仕組みが必要

運用を、どこまで効率的に実施できるか？を考える
どこまで自動化するか、人手と自動化の境目が肝心

作成したレポートなど報告するルート・仕組みも考える
例えば、報告書は誰が作って、誰が確認（承認）するのか？



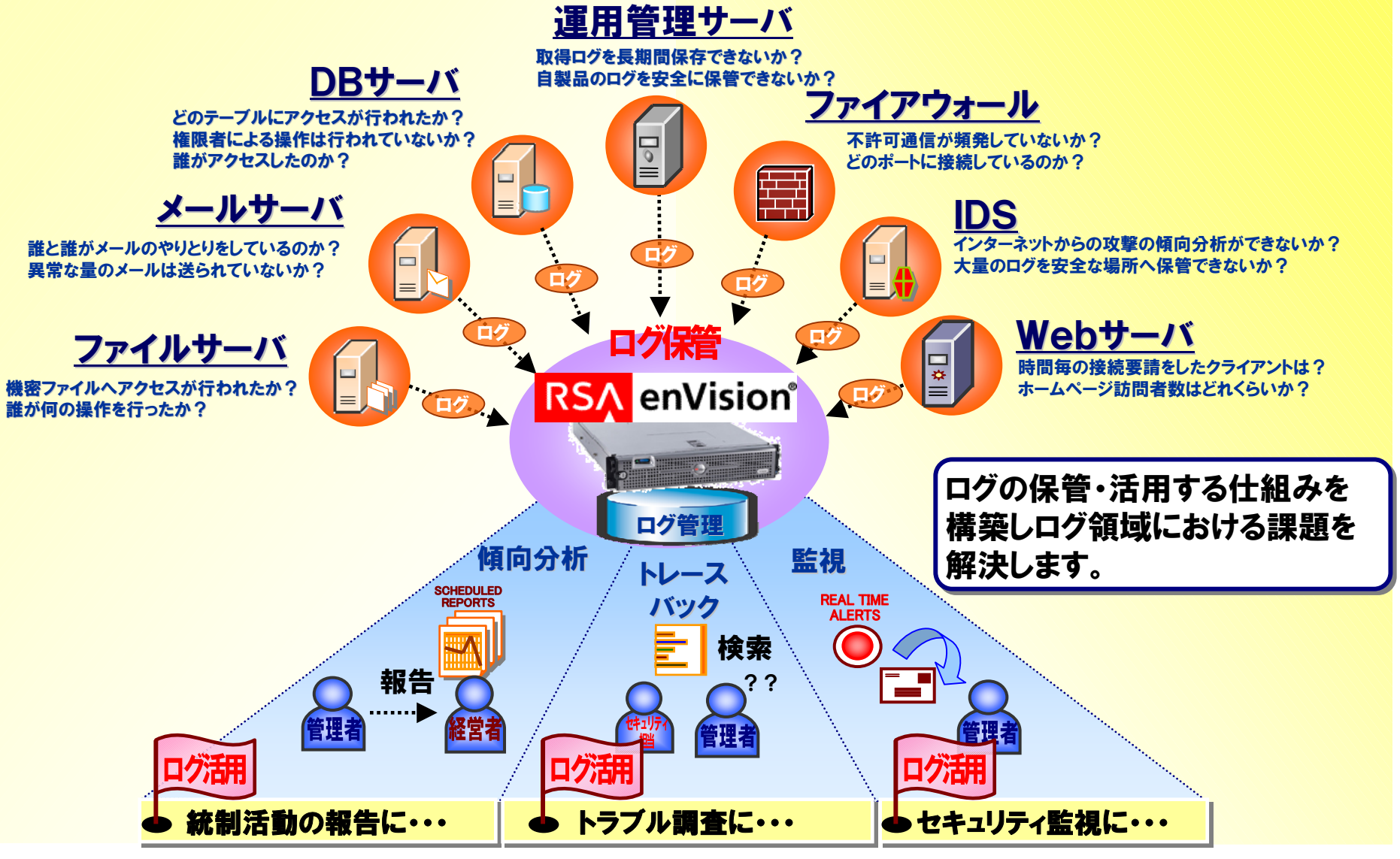
貴社に存在する多数の情報システムにあった形の
最適な統合ログ管理ソリューションとは？

3-3. 統合ログ管理ソリューションの全体像

UNISYS

IT全般統制・監査

情報セキュリティ



ログの保管・活用する仕組みを構築しログ領域における課題を解決します。

3-4. RSA enVisionの機能概要

UNISYS

RSA enVision®

ネットワーク上のログ収集

エージェントレスで、ネットワーク、アプリケーション、サーバなどの様々なログをアプライアンス内に格納！

ログのデータベース管理

ログ管理機能に特化した独自データベース を利用して、高速収集、高圧縮、暗号化、イベント指向でのログ管理が可能！

ログ調査（Forensic）

ブラウザによる直感的な運用環境を提供。
迅速かつ正確な調査が可能！

レポート出力（Audit）

各法制度やログカテゴリに応じた800種類以上のテンプレートを用意。定期的な自動出力も可能！

リアルタイムアラート

個々のログに対して任意の条件でアラート設定が可能。管理者へのメール通知やコマンド実行機能等も実装！

相関分析（Correlation）

各デバイスから出力されるログを任意の条件で組み合わせての、相関アラートを出力可能！テンプレートは70種類以上！！

3-5. ネットワーク上のログ収集

UNISYS

エージェントレスで幅広いデバイスのログを収集可能！

Syslog
/Syslog-ng

Syslog転送

Windows
イベントログ

Event Log APIによるログ取得

RSA enVision®

ODBCによるログ取得

DBアクセスログ

FTP転送

テキストログ

基本的にエージェントは不要。
ただし、テキストログ取得の際にFTP機能が無いものに関してはエージェントにて対応。

3-6. 多種多様なログに対応

UNISYS

エージェントレスであらゆる標準のログ出力プロトコルに対応し、FTP クライアントも利用可能

Syslog / Syslog NG　SNMP　Windows イベントログ API　テキストファイル（タブ/スペース/カンマ区切り、など）

Cisco IDS POP/RDEP/SDEE　XML ファイル（HTTP 取得）　CheckPoint OPSEC　ODBC（リモートDB接続）

120種類以上のデバイス/APのログフォーマットに対応し、ユーザー独自APのログも収集可能

Access Control
-ActivIdentity　-Cisco ACS
-RSA SecurID
-Toplayer　.etc

Anti-Virus
-Symantec
-Trend Micro
-McAfee　.etc

Database
-Oracle
-IBM DB2
-MS SQL Server　.etc

Other
-IBM MainFrame　-nCircle
-Tripwire　-Qualys
-NetAPP Data ONTAP .etc

Firewall
-Checkpoint　-CyberGuard
-Cisco PIX　-Fortinet
-Nortel Alteon　-SonicWall
-Juniper Netscreen
-Secure Computing　.etc

VPN
-Checkpoint VPN-1　-Juniper SSL-VPN
-Cisco VPN3000　-Nortel Contivity
-Nokia IP
-Celestix
-CrossBean
.etc

IDS/IPS
-CheckPoint　-ISS
-Cisco Secure IDS　-McAfee
-Juniper IDS　-SNORT
-Tripping Point　-TopLayer
.etc

OS
-Apple Mac OS X
-IBM AIX　-Microsoft Windows
-Free BSD　-RedHat Linux
-HP_UX　-Sun Solaris　.etc

Router/Switch
-Cisco　-Cisco Catalyst
-Juniper　-Extreme
-Nortel
-Foundry　.etc

Web
-Apache　-Blue Coat
-Cisco Content Engine
-WebSense　-NetCache
-MS IIS　-InterSafe　.etc

Universal Devices Support

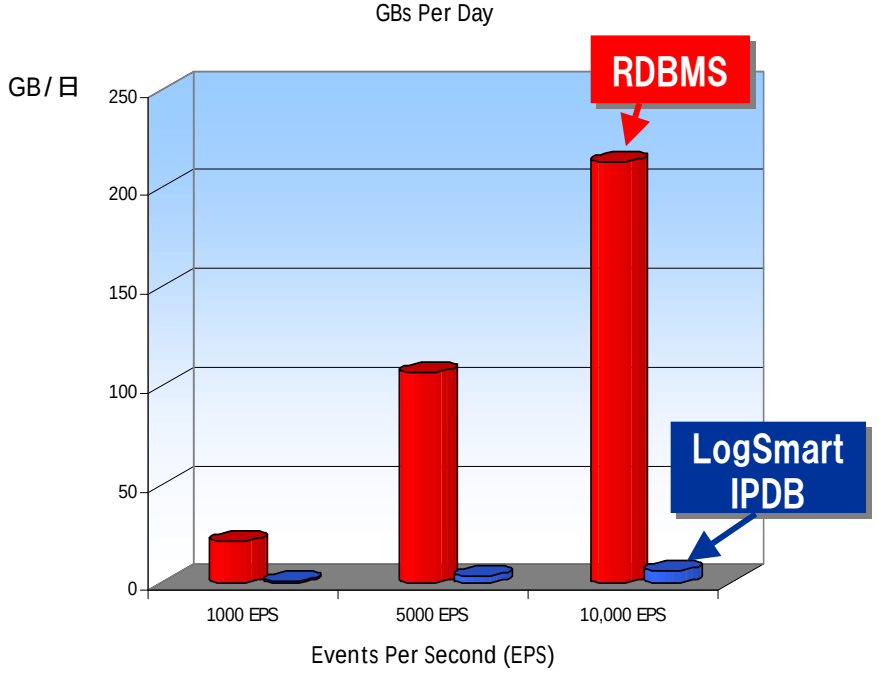
独自の XML Parsing により、未サポートデバイスのログを認識できるようにカスタマイズ可能

3-7. ログの独自データベース管理

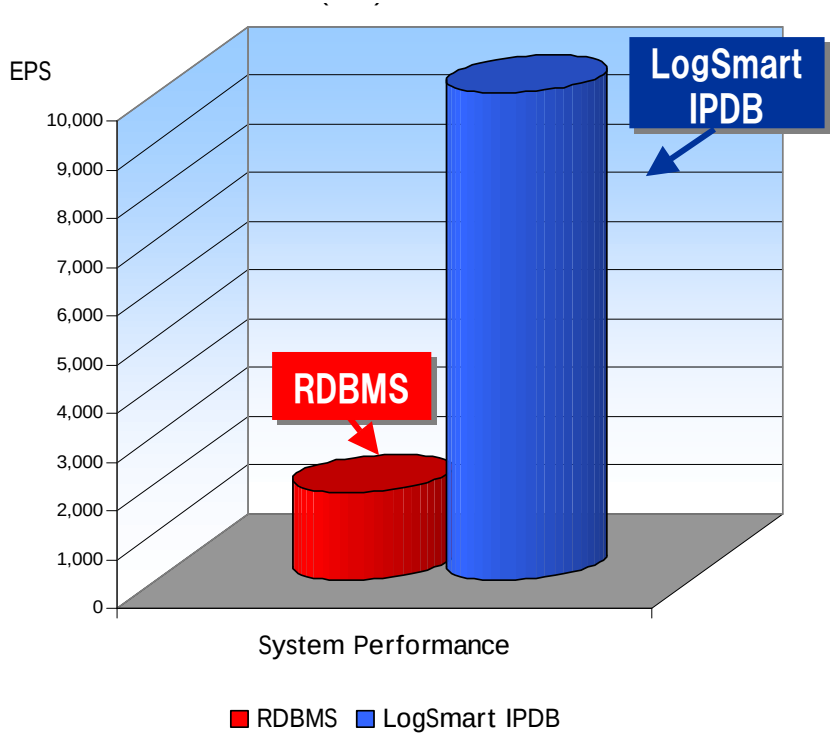
UNISYS

ログ収集に特化したデータベース【LogSmart IPDB】により、様々な機器のログを高速に収集！

ストレージの優位性



収集効率の優位性



圧縮率：70%～95%

例：2GB/日　のログ収集 ⇒ 730GB/年

→70%圧縮：219GB/年

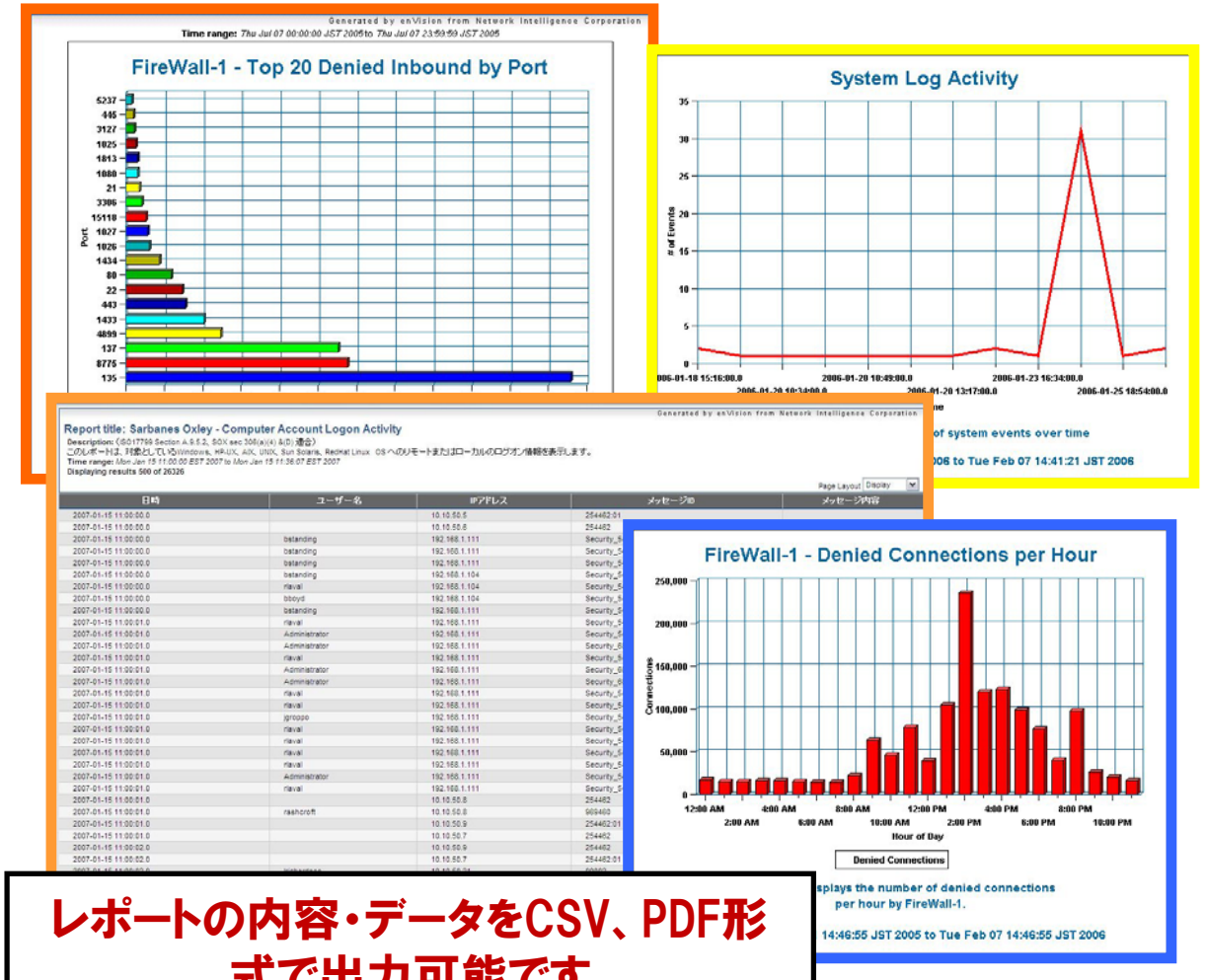
年間500GB以上の容量削減！

EPS (Event Per Second)・・・1秒間に収集できるログの数

3-8. 豊富なレポート・テンプレート

UNISYS

簡単な設定で利用できる800種類以上のテンプレートを標準装備



レポートの内容・データをCSV、PDF形式で出力可能です

テンプレート例

- Windows
  - ログオン/ログオフ
  - ファイルアクセス
- ファイアウォール
  - 接続ポート　トップ20
- SQL Server
  - ログイン失敗
- SOX法関連
  - 会計データへのアクセス
- FISMA関連
  - アカウント管理

etc・・・

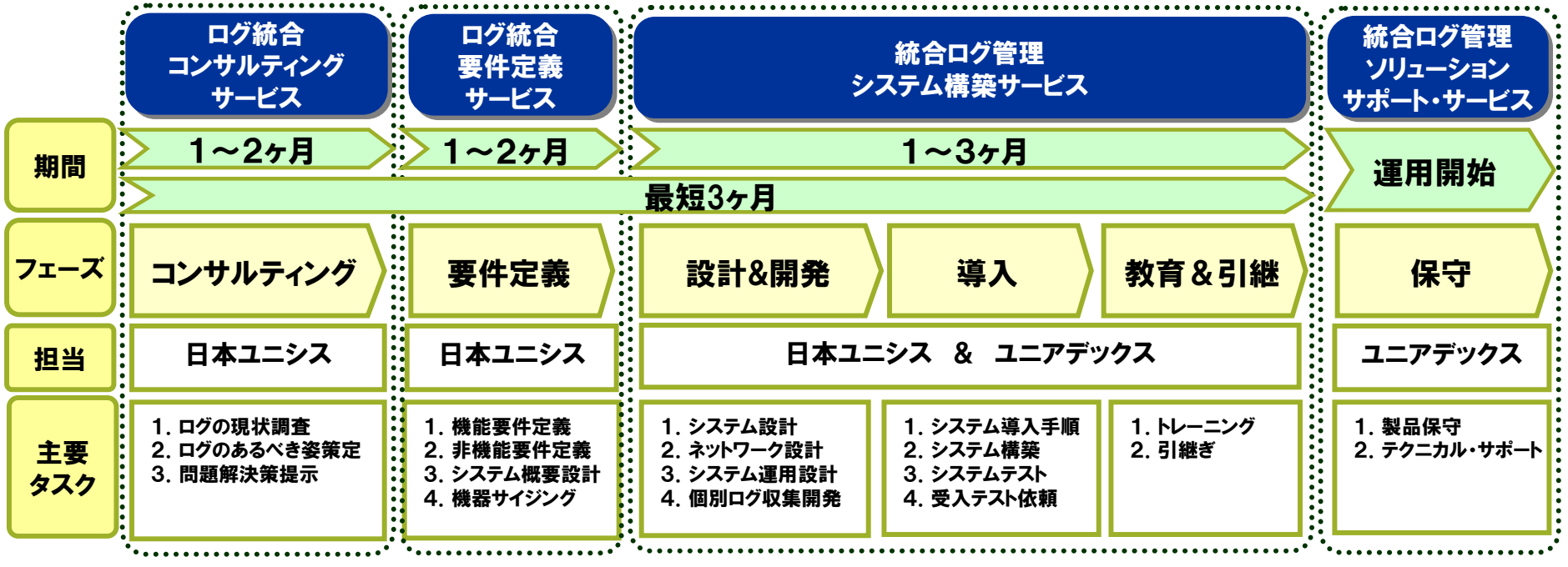
3-9. 統合ログ管理ソリューション・サービスの全体像

UNISYS

◇統合ログ管理ソリューションの概要

ログ統合コンサルティングサービス	独自のフレームワークを採用し、ログ管理のあるべき姿への最適なルートを提言
ログ統合要件定義サービス	ログ活用方針に基づき、ログの収集・保管・分析・報告する仕組みを具現化
統合ログ管理システム構築サービス	統合ログ管理システムを導入・運用する仕組みを設計し、構築する
統合ログ管理ソリューションサポート・サービス	数多くのサポート経験を、ナレッジDBに納め、迅速かつ適確に回答

◇統合ログ管理ソリューション提供体系



3-10. サービスのスタート地点

UNISYS

お客様の要件により提供するサービスのスタート地点が変わります。

収集ログ・活用方針が明確でない場合

スタート

ログ統合
コンサルティングサービス

既に、収集するログ・活用方針が決定している場合

スタート

ログ統合要件定義サービス

スタート

統合ログ管理
システム構築サービス

設定は導入時の本体設定のみ
製品のみの販売も可能

統合ログ管理ソリューション
サポート・サービス

1 ログを取り巻く環境の変化

2 ログ管理の実践ポイント

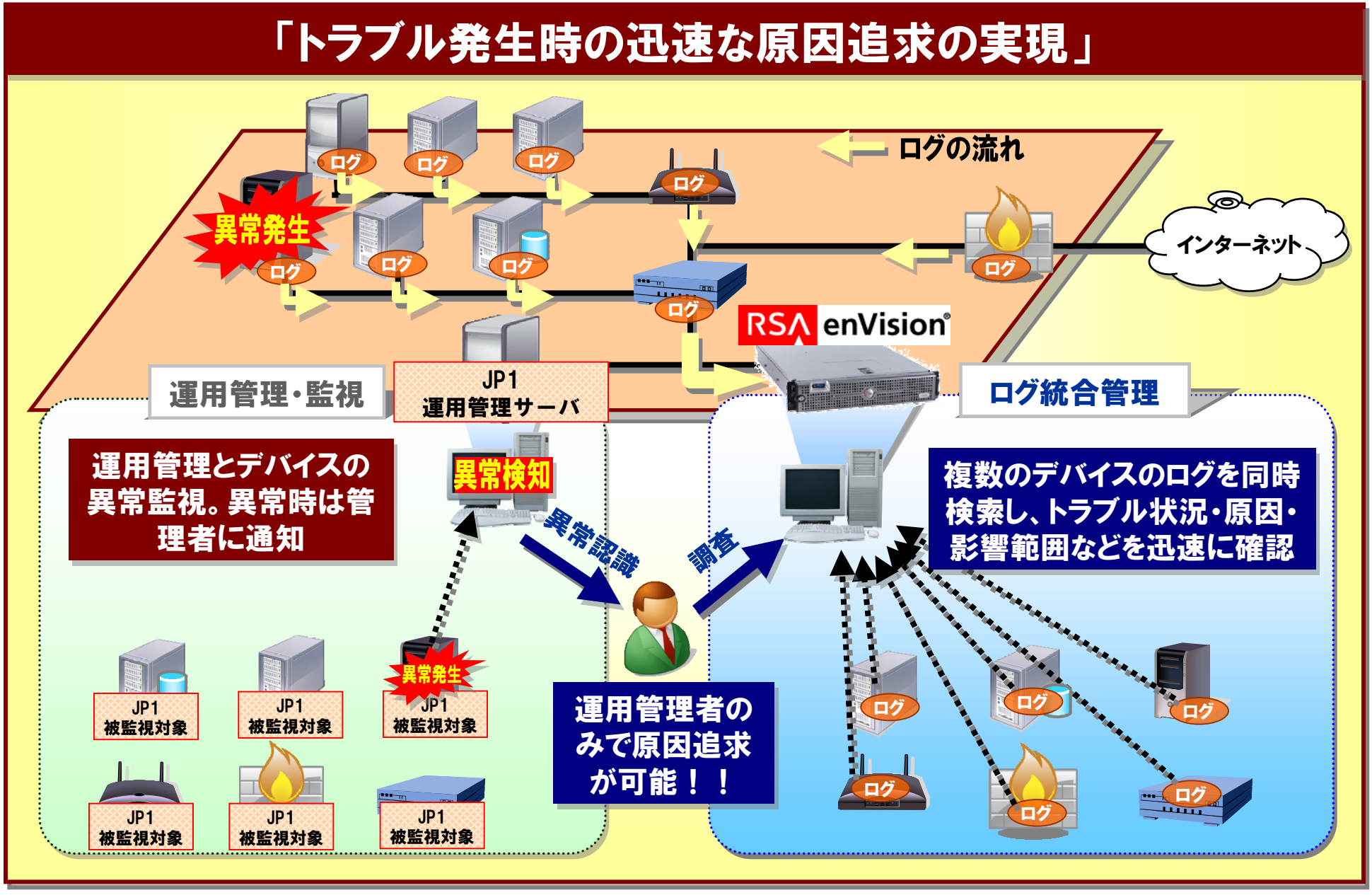
3 ログの課題を解決する統合ログ管理ソリューション

4 ログ活用におけるケーススタディ

4-1. システムトラブル対策　RSA enVisionとJP1の連携

UNISYS

「トラブル発生時の迅速な原因追求の実現」



4-2. IT統制におけるログの活用例1 「発見的統制」への対応

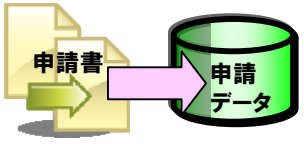
UNISYS

【目的：運用管理システムのID管理のモニタリング】

JP1をベースとした運用管理システムのIDの作成、アクセス権の変更、IDの削除に関しての、誰がいつ承認し、実行したかを**ログからの情報と突合せ**を行う。

ユーザー新規作成の申請

承認者



電子ワークフローシステムで申請された申請データに対して内容を確認し承認する

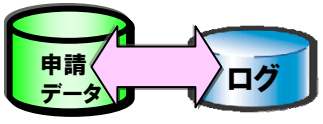
ユーザーの新規作成

システム担当

JP1/Baseに対して申請された内容に基づいてID追加作業を行う
⇒履歴ログが出力される

定期的な評価

内部統制担当



申請書データと履歴ログを突合せし、ルールが守られているか確認する

評価に利用するレポート例

- 財務システムへの管理権限アクセス
- 各サーバへのログオン活動監視
- 各アカウント毎のログオン状況一覧
- 人事リソースデータの変更管理とアクセス管理
- 稼動ソフトウェアのイベント管理
- システム監査データの管理
- 無効アカウントのレポート
- 会計データへのアクセス
- 全てのログイン、認証失敗の管理
- 悪意のあるソフトウェアの活動レポート
- 運用変更管理レポート
- パスワードの変更/期限切れの管理
- ソースコードへのアクセス管理
- 外部ドメインからのユーザ活動管理

4-3. IT統制におけるログの活用例2 「発見的統制」への対応

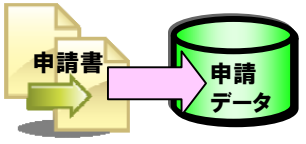
UNISYS

【目的：財務システムのプログラム変更管理のモニタリング】

財務システムおよび関連システムのプログラムの変更、削除に関して、誰がいつ承認し、実行したかを**ログからの情報と突合せ**を行う。

プログラム変更の申請

承認者



電子ワークフローシステムで申請された申請データに対して内容を確認し承認する

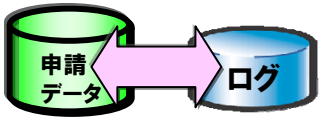
プログラムの変更

システム担当

JP1/NETM/DMを使用しプログラムの変更作業を行う
⇒履歴ログが出力される

定期的な評価

内部統制担当



申請書データと履歴ログを突合せし、申請内容通りに変更されているか確認する

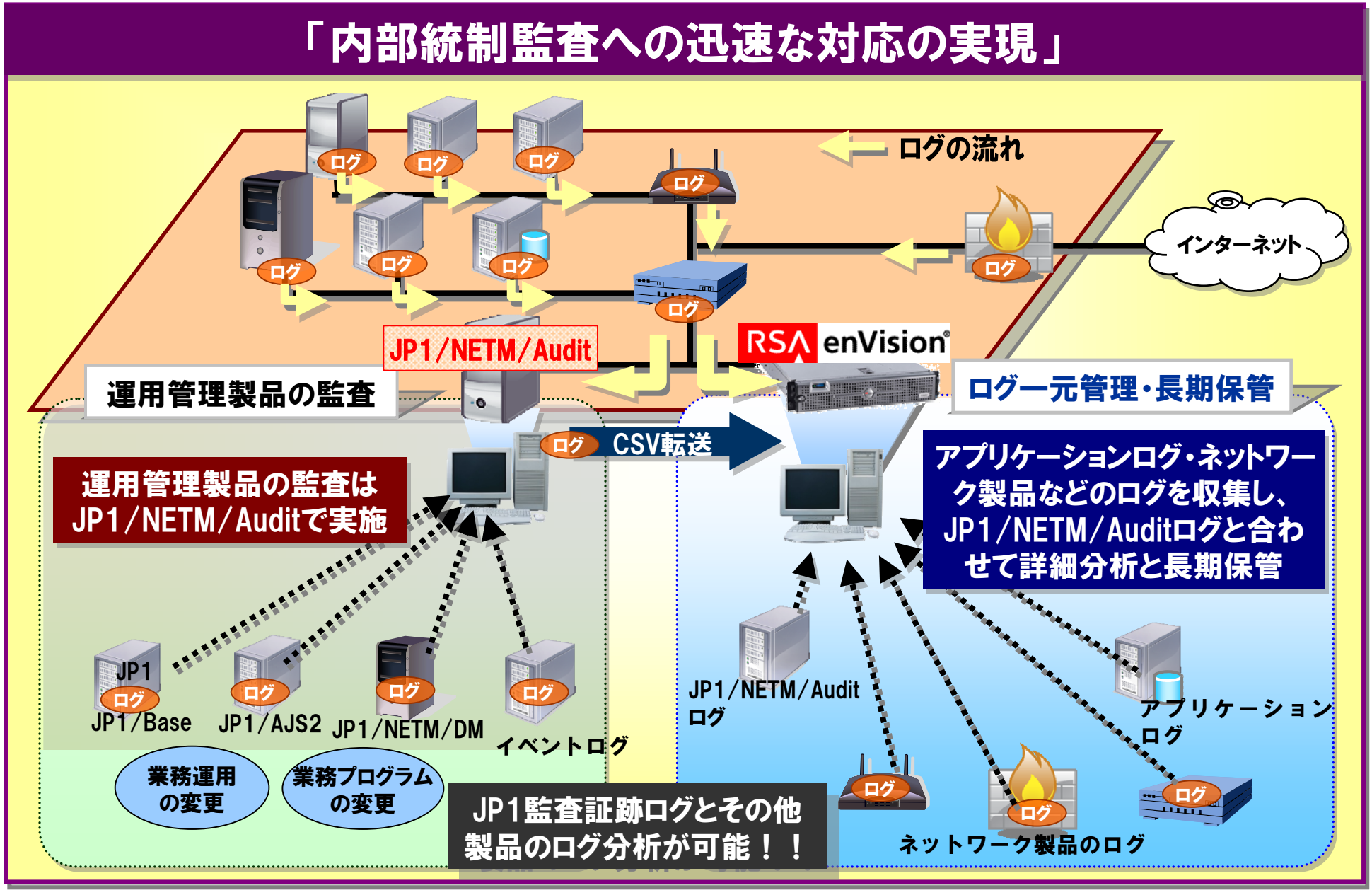
（例）プログラムのチェックイン・チェックアウト手順
- 本番プログラムを更新するシェル・スクリプトを必ず通じて実行するルールを確立し、その中で**操作履歴のログ**を出力するようにする。
- プログラム変更管理ツールやJP1/NTM/DMのような配布管理ツールの**実行履歴ログ**を活用する。

4-4. RSA enVisionとJP1/NETM/Audit-Managerの連携イメージ

4-5. IT統制におけるログの活用例3

UNISYS

「内部統制監査への迅速な対応の実現」



UNISYS

日本ユニシス株式会社

http://www.unisys.co.jp/

お問い合わせ先

http://www.unisys.co.jp/security/log_management.html

日本ユニシスホームページから『統合ログ』を検索してください