



「統合ログ管理によるIT統制の実現とその具体的事例」

2007年2月9日
インフォサイエンス株式会社
プロダクト事業部

Infoscience

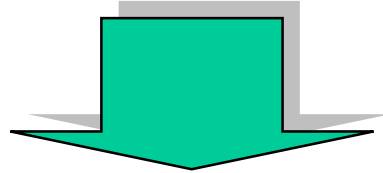
Infoscience Corporation
www.infoscience.co.jp
info@logstorage.com
Tel: 03-5427-3503 Fax: 03-5427-3889

1. はじめに ～内部統制とログの関係～
2. 各基準案に見るログ管理の必要性
3. ログ管理における課題
4. 統合ログ管理による課題解決
5. 導入・活用事例
6. まとめ

1. はじめに



内部統制で何をすべきか・・・



金融商品取引法実施基準草案公開
システム管理基準 追補版公開

内部統制をどう実現すべきか

各種基準案の公開により、「何をすべきか」というフェーズから、「どう実現すべきか」というフェーズに移り、具体的なITソリューションの選定に入っている。

例えば、証跡の取得・管理はどうか

(クライアント操作記録、データベースアクセス記録、メールアーカイブ、ログ収集・分析...)

コンプライアンス(法令遵守)

金融商品取引法
(日本版SOX法)

新会社法

個人情報保護法

様々なコンプライアンス上の要求の中で共通するのは、「証跡を残す」ということである。

内部統制の基本的要素に挙げられている「モニタリング」は、内部統制が有効に機能していることを継続的に評価するプロセスを表しており、そのための判断材料として「監査証跡＝ログ」を残さなければならない。

また、ITへの対応を踏まえた内部統制には、システムの運用状況のログ(記録)を適切に管理し、保管することも求められている。

内部統制の基本的要素

1. 統制環境
2. リスクの評価と対応
3. 統制活動
4. 情報と伝達
5. **モニタリング(監視活動)**
6. **IT(情報技術)への対応**

2. 各基準案に見るログ管理の必要性



「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(公開草案)」

企業会計審議会内部統制部会より、2006年11月21日に公開。
財務報告に係る内部統制の評価及び監査の基準案を実務に適用する場合の
詳細な実務上の指針。

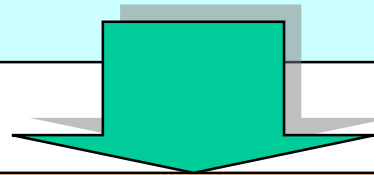
モニタリング

モニタリングとは、内部統制が有効に機能していることを継続的に評価するプロセスをいう。

モニタリングにより、内部統制は常に監視、評価及び是正されることになる。モニタリングには、業務に組み込まれて行われる日常的モニタリング及び業務から独立した視点から実施される独立的評価がある。両者は個別に又は組み合わせて行われる場合がある。

モニタリングの有効性を確保するためのITの利用

統制活動の有効性に関する日常的モニタリングは、日常の業務活動を管理するシステムに組み込み自動化することで、より網羅的に実施することが可能となる。その結果、独立的評価に当たってリスクを低く見積もることができるため、独立的評価の頻度を低くしたり、投入する人員を少なくすることも可能となる。



ITを利用した企業内の全ての活動記録の収集、日常的モニタリング(監視)により、リスク及びコストを下げるができる。

「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)(案)」

経済産業省より、2007年1月19日に公開。

「システム管理基準」を活用している企業が、財務報告に関わる内部統制で求められている「ITへの対応」との間の具体的な対応関係を明らかにしたものの。

運用の実施記録、ログの採取と保管

「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」

「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。

統制の例と統制評価手続の例

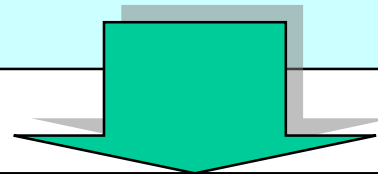
リスク: 運用時の不正な操作を発見できない

統制の例

情報システムとデータ処理について、企業にログ採取・分析についての方針があり、それに基づいてログが採取されて、必要な項目がモニタリングされている。

統制評価手続きの例

企業に、ログ採取に関する方針があることを確かめる。次に、必要なログ(不正操作等のモニタリングに必要な項目)が記録され、保管されていること、また、保存されたログを利用できることを確かめる。



明確な方針を立て、それに基づいてログ管理が行われているか？

統制の例と統制評価手続の例

リスク: 情報システムが処理するデータの信頼性が保証されない

統制の例

情報システムとデータ処理のログが取得されて、ログファイルの完全性、正確性、正当性を保証される(ログが改ざんされずに記録され、保管されている)。

統制評価手続きの例

ログの記録や保管に際して、改ざんや削除ができないかについて確かめる。
(例えば、情報システムとデータ処理に関する操作状況を調査する。調査した時間帯のログのサンプルを取得する。入手したサンプルをもとに、取得されたログの完全性と正確性を確かめる)。

ログは正しく、安全に保管されているか？

3. ログ管理における課題



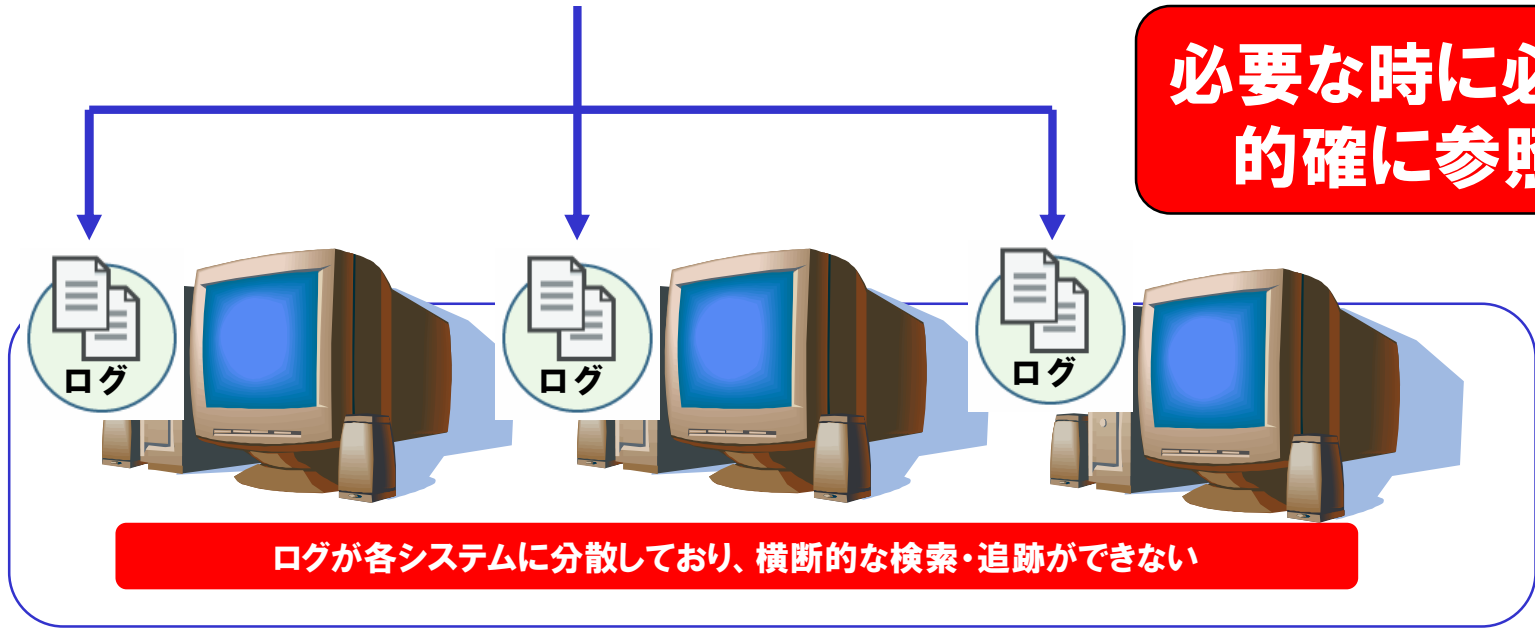
ログが保管されている「だけ」の状態

ログ管理を始めてみたものの・・・



管理人・監査人など

- 複雑な操作でログを調査し、探し回る必要がある
- ログに必要な情報が記録されていない
- 各システムでログの保管期間が異なる
- 各システムで出力されているログの原本性が保証できない



必要な時に必要なログが
的確に参照できない

ログが各システムに分散しており、横断的な検索・追跡ができない

1. ログ管理ポリシー

2. ログの一元管理

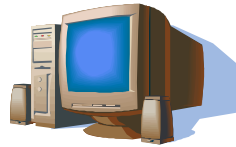
3. ログの長期保存

4. 異なるシステムのログ横断

5. ログ改ざんの防止・原本保証

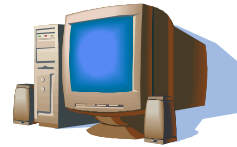
課題

自社の情報システム内にある、あらゆるサーバ、アプリケーション、ネットワーク機器が**出力すべきログ**を洗い出さなければならない



認証サーバ

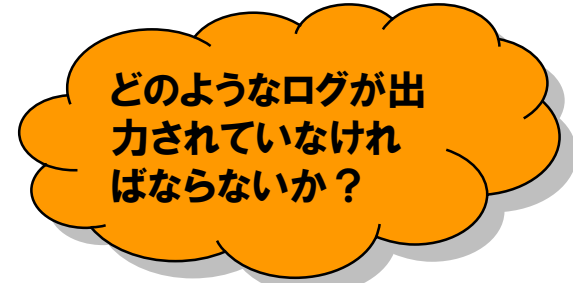
- 認証成功 / 失敗ログ
- ユーザの追加 / 更新 / 削除ログ
- ...



業務サーバ

- 業務トランザクションログ
- ...
- ...

システム、OSのログ



どのようなログが出力されていないかなければならないか？



各システム毎に収集するログ



全システムで共通的に収集するログ

ポイント

サーバ、アプリケーション、ネットワーク機器によって収集すべきログは異なる。
また、ログの内容についても、何を含むべきか検討が必要

ログ管理ポリシーの策定

ログ収集対象の検討例

No	ログ収集対象 (ホスト名)	IPアドレス	アプリケーション	アクション	記録項目 (ログの内容)	...
1	host01	192.168.0.1	Firewall	deny	ソースIP、デスティネーションIP...	
2	Host02	192.168.0.2	業務A	登録	ユーザ名、アクション...	
				更新	ユーザ名、アクション...	
				削除	ユーザ名、アクション...	
3	host04	192.168.0.3	認証	ユーザ追加	ユーザ名、追加ユーザ名、グループ名...	
4				ユーザ削除	ユーザ名、削除ユーザ名...	

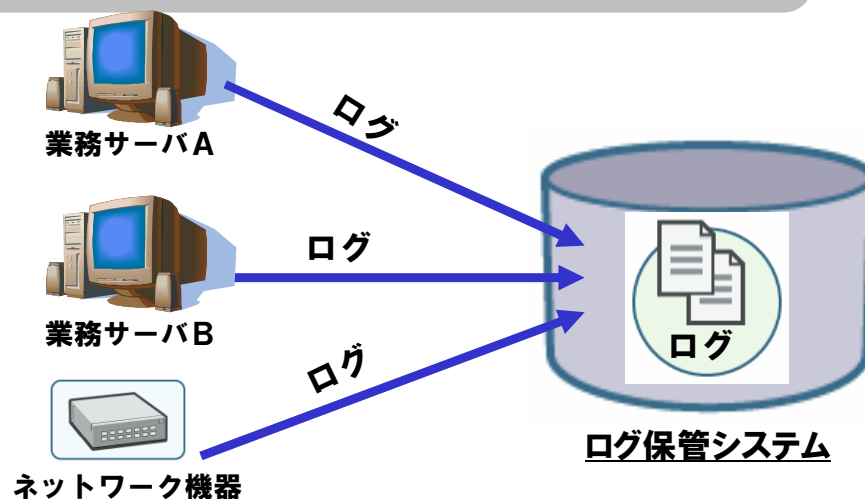
課題

自社の情報システム内にあるサーバや、ネットワーク機器に分散しているログを一元管理しなければならない

ログを一元管理する効果

点在するログを一元管理することで、システム間で関連のあるログの突合せや分析が可能になる。

ログの一元管理は、後述する「横断的な検索・分析」の第一歩。



ポイント

ログの出力方法は各システムによって異なるが、それらを残さず収集し、一元管理する仕組みが必要

必要な全てのログを収集・保管する。一部でも抜けがあってはならない

各システムの時刻同期を行い、ログのタイムスタンプの統一が必要

タイムスタンプにズレがあると、正確な追跡・監査ができない

課題

膨大な量のログを長期間保管しなければならない

ログの保管期間

ログの保管期間はポリシーを定めて保管する。ログはその保管期間を最低でも1年以上とするのが一般的であり、有価証券報告書及びその添付書類の縦覧期間である「5年」を勘案し、ログの保管期間も5年と定める企業も多い。

一般的に、長期間ログを保管する場合の量は膨大になるため、ログ保管システム導入の際はサイジングが重要になる。

ポイント

事前のログ量の見積もり(それに応じた保管用ストレージの用意)が必要

拡張性の高いシステムの導入(主にログ保管領域の拡張)が必要

事前にログ量が見積もれないことが多く、且つログは年々増加する

保管したログの利用(検索やレポーティング)を想定したハードウェアのサイジングが必要

膨大なログの中から、必要な時に、必要なログを取り出す必要がある

課題

保管しているログを横断的に検索・分析できなければならない

横断的な検索・分析

複数のシステムに跨るような業務プロセスの場合、1つのシステムから得られるログだけでは、そのプロセス全体の妥当性・正当性は判断できない。

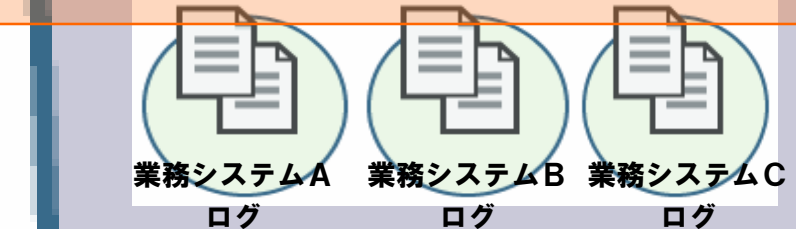
こうした場合、複数システムのログを横串(横断的)にした、検索・分析が有効である。

検索結果

2007/2/9 10:00:01	業務システムA	トランザクションA-1開始...
2007/2/9 10:00:03	業務システムA	トランザクションA-2開始...
2007/2/9 10:00:05	業務システムB	データ受信...
2007/2/9 10:00:06	業務システムB	データ登録...
2007/2/9 10:00:07	業務システムC	...
...		

業務処理の流れ

関連システムのログを横串検索・分析



ログ保管システム

ポイント

収集したログを全て横断的に検索・分析できる仕組みが必要

ログ横断検索の詳細イメージ

ユーザ名:「inamura」で検索(行動追跡)



[認証サーバのログ]

2007-01-19 08:39:40 192.168.0.1 Auth1:login_success,src_ip=192.168.0.10,username=inamura

[業務システムAのログ]

2007-01-19 08:42:21 192.168.0.2 App1:name=inamura,act=download,filename=userlist.xls...

[データベースサーバのログ]

2007-01-19 08:43:50 192.168.0.3 DB1: uid=inamura,action=select...

ログの内容はサーバ、アプリケーション、ネットワーク機器毎に異なり、多種多様であるが、統一的に扱える必要がある。

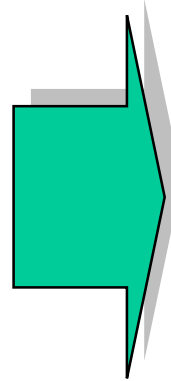
課題

記録されたログを安全に保管しなければならない

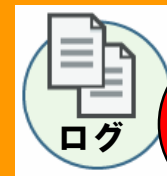
ログの改ざん

ログが改ざんされた場合、当然そのログは監査証跡として意味を成さないため、それを防止する必要がある。

また併せて、「改ざんされていないことの証明」も、そのログが監査証跡足りうるか、といった判断を行う上で重要になる。



ログの原本保証が重要となる。

原本
保証

ポイント

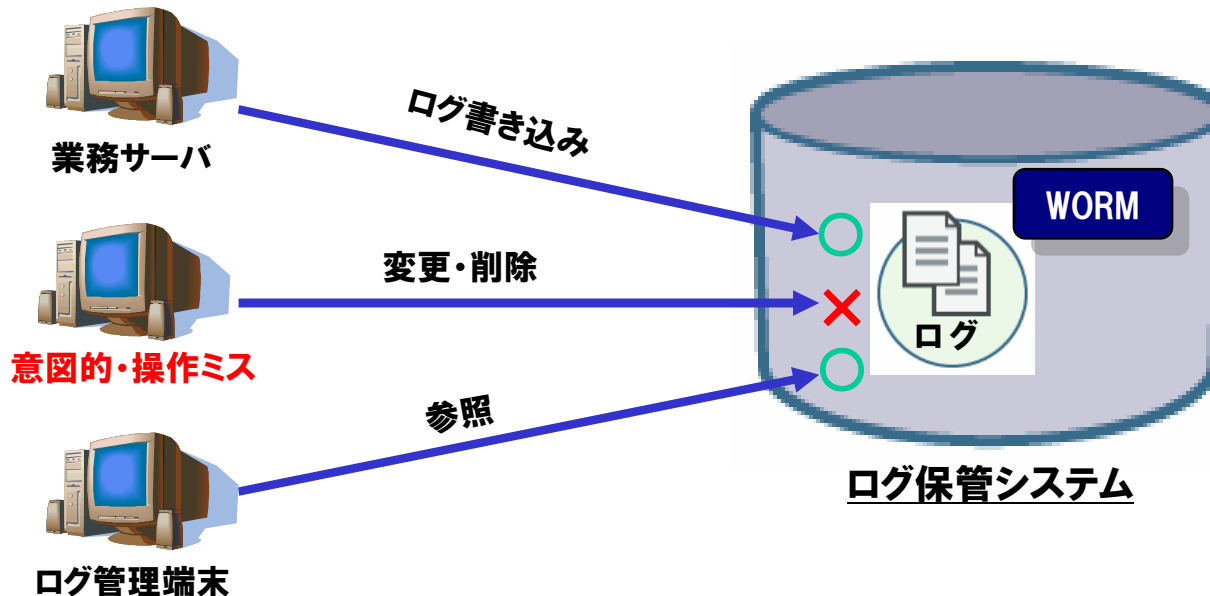
以下のような仕組みを用いてログの改ざんを防止することが必要

- ・アクセス権限による改ざん防止
- ・WORMによる改ざん防止(後述)

ログに電子署名を付与するなど、ログが改ざんされていないことを証明することが必要

WORM (Write Once Read Many)

1度記録された内容は変更不可能、参照は何度でも可能という仕組み。
 ログは、一度書き込まれた後で内容が書き換えられてはいけませんが、何度も参照されるという特性を持つため、この仕組みが利用できる。



WORMの実現方法として、専用ストレージを利用するハード的な方法と、APIを利用するソフト的な方法がある。

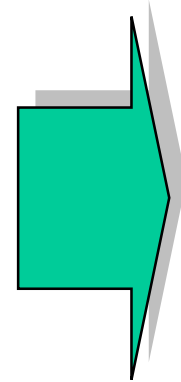
4. 統合ログ管理による課題解決



統合ログ管理とは

ログ管理に求められる全ての機能・要件を備え、それらを統合的に扱えるソリューション

統合ログ管理システム	
一元管理機能	収集・保管
長期保存機能	
改ざん防止・原本保証機能	
ログフォーマット吸収機能	
横断追跡機能	監査
高速検索機能	
分析・集計機能	
レポートニング機能	
リアルタイム検知機能	



純国産 統合ログ管理システム



沿革

2002/2	Ver.1 リリース
2003/9	Ver.2 リリース
2004/2	Ver.2.1 リリース (個人情報保護法)
2004/6	Ver.2.2 リリース
2005/3	Ver.2.3 リリース
2005/10	Ver.2.4 リリース
2006/1	Ver.2.5 リリース
2006/11	Ver.3.0 リリース (日本版SOX法)

ログ管理に求められる機能の実現

① ログの一元保管

- Syslog、FTP、Agentからの受信など、ログを受け付ける様々な口を持っている
- 収集される多種多様なログは、ログフォーマット定義により統一的に扱うことが可能

② ログの長期保管

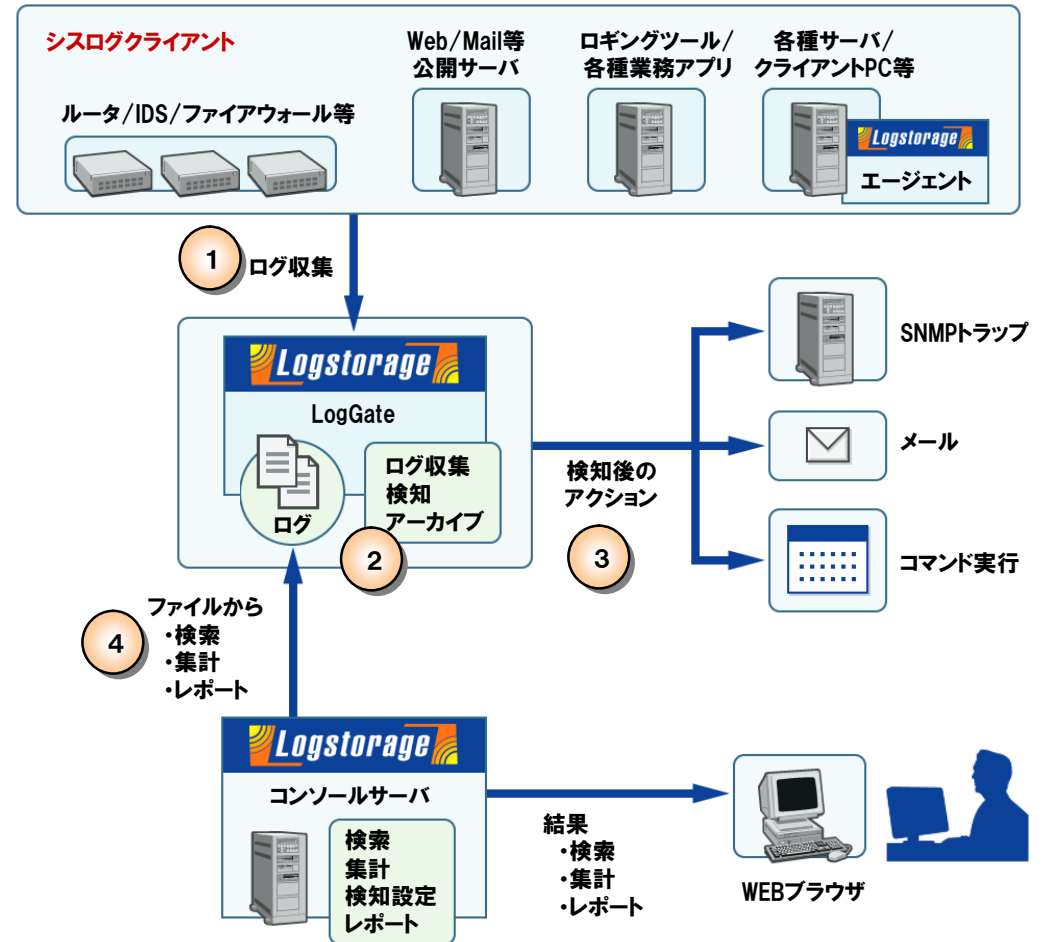
- ログは共有ストレージ上に保管され、ログ量の増加に対してはストレージの増設のみで対応可能
- アーカイブ機能により、定期的にテープなどの外部デバイスに圧縮・移動することが可能
- WORM機能を持ったストレージ、APIを用いたログの保管が可能

③ リアルタイム検知

- ポリシー違反に関するログをリアルタイムに検知し、管理者へメールを送信することなどが可能

④ 横断検索・追跡／集計／レポート

- ログに対するアクセスは全てWebブラウザからGUIを使用した操作にて可能
- 検索はインデックスの利用が可能



• ブラウザで簡単に検索条件を設定し、検索結果を表示

• 複雑な検索条件を保存

- パターン化された検索を定型化
- 保存された検索条件を読み出し、条件を変更して検索が可能

• ハイライト機能

- 特定のログをハイライト表示

The screenshot shows the Logstorage web interface. On the left is a navigation menu with options like '検索' (Search), 'Fire Wall', 'ツール', '集計', '検知', 'レポート', 'ログフォーマット管理', 'システムの設定', and 'ユーザ管理'. The main area is titled '検索条件' (Search Conditions) and includes a search bar for 'LogGateグループ' (LogGate Group) set to 'group1'. It features date selection (today, yesterday, previous, previous month) and a time range selector from 2006/01/22 00:00 to 2006/01/22 23:59. There are dropdowns for 'アプリケーション' (Application) set to 'Windows 監査ポリシー' and 'アクション' (Action) set to '全て' (All). A '検索' (Search) button is visible.

Below the search settings, the search results are displayed in a table. The table has columns for 'TIME STAMP', 'シスログクライアント' (Syslog Client), 'ファシリティ' (Facility), 'プライオリティ' (Priority), 'アプリケーション' (Application), and 'ログメッセージ' (Log Message). The results show various cron jobs and system messages, with one entry highlighted in red: '2006/01/26 15:12:12 メールサーバ auth info suコマンド su@am_unix[7320]: session closed for user root'.

- 検索を繰り返しながら、ログを追跡

- ログの一覧より、マウスにて絞り込みたい検索キーワードを選択

- ログ追跡の操作で選択したキーワードを検索条件に自動追加、再検索

priority: notice --

検索 保存 キャンセル ログを改行しない

検索条件追加

クリック

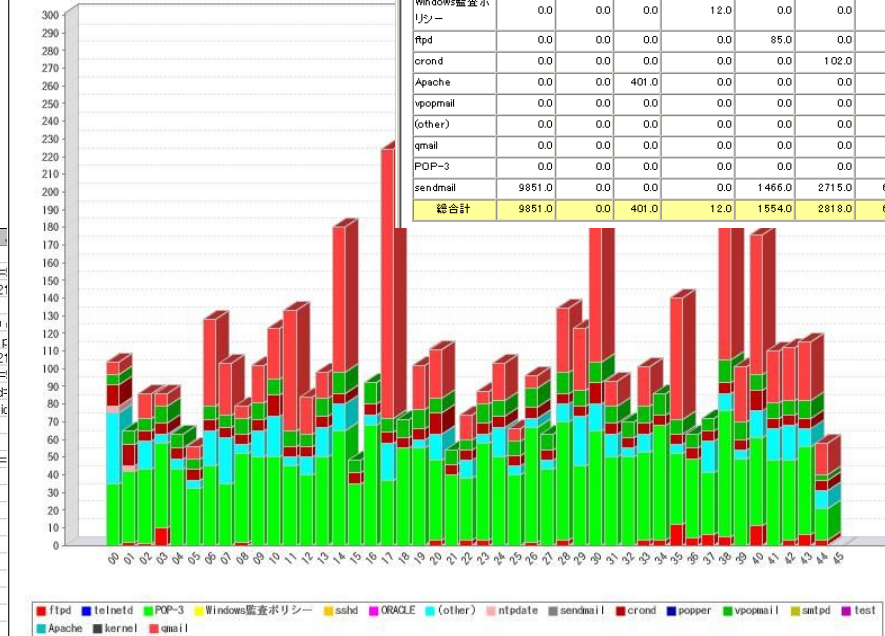
TIME STAMP	シスログクライアント	ファンリティ	プライオリティ	アプリケーション	ログメッセージ
2004/02/13 09:44:09	qmailサーバ	mail	notice	vpopmail	vpopmail[13201]: vchkpw: login success s
2004/02/13 09:44:09	qmailサーバ	mail	notice	vpopmail	vpopmail[13206]: vchkpw: login success r
2004/02/13 09:44:02	qmailサーバ	mail	notice	vpopmail	vpopmail[13197]: vchkpw: login success t

- ログの検索、集計、検知履歴のレポート機能
- 定期的な実行
 - 時間毎、日毎、週毎、月毎
- 多様な出力フォーマットに対応
 - PDF、HTML、CSVなど
- レポート出力条件を保管して作業を定型化
- XSLTによるカスタムレポート
- 外部レポートエンジンとの連携
- コマンドからのレポート作成

CSV出力例

	A	B	C	D	E	F	G	H	I
1	2004/10/6 11:01	127.0.0.1	cron	info	CROND[6512]: (root) CMD (run-parts /etc/cron.hourly)				
2	2004/10/6 11:03	127.0.0.1	auth	info	sshd(pam_unix)[6519]: session opened for user thino by (uid=				
3	2004/10/6 11:03	127.0.0.1	authpriv	info	sshd[6517]: Accepted password for thino from 192.168.254.21				
4	2004/10/6 11:09	127.0.0.1	syslog	notice	syslog-ng[3640]: STATS: dropped 0				
5	2004/10/6 11:17	127.0.0.1	auth	notice	sshd(pam_unix)[6637]: authentication failure; logname= uid=0,				
6	2004/10/6 11:17	127.0.0.1	authpriv	info	sshd[6637]: Failed password for thino from 192.168.254.21				
7	2004/10/6 11:17	127.0.0.1	authpriv	info	sshd[6637]: Accepted password for thino from 192.168.254.21				
8	2004/10/6 11:17	127.0.0.1	auth	info	sshd(pam_unix)[6639]: session opened for user thino by (uid=				
9	2004/10/6 11:18	127.0.0.1	auth	notice	su(pam_unix)[6676]: authentication failure; logname=thino uid=				
10	2004/10/6 11:18	127.0.0.1	auth	info	su(pam_unix)[6677]: session opened for user root by thino(uk				
11	2004/10/6 11:22	127.0.0.1	authpriv	info	xinetd[2077]: START: telnet pid=6744 from=192.168.254.139				
12	2004/10/6 11:22	127.0.0.1	auth	info	chiba[6745]: LOGIN ON pts/3 BY chiba FROM chiba				
13	2004/10/6 11:22	127.0.0.1	auth	info	login(pam_unix)[6745]: session opened for user chiba by (uid=				
14	2004/10/6 12:01	127.0.0.1	cron	info	CROND[6881]: (root) CMD (run-parts /etc/cron.hourly)				
15	2004/10/6 12:09	127.0.0.1	syslog	notice	syslog-ng[3640]: STATS: dropped 0				
16	2004/10/6 13:01	127.0.0.1	cron	info	CROND[7016]: (root) CMD (run-parts /etc/cron.hourly)				
17	2004/10/6 13:09	127.0.0.1	syslog	notice	syslog-ng[3640]: STATS: dropped 0				
18	2004/10/6 13:14	127.0.0.1	auth	info	sshd(pam_unix)[6519]: session closed for user thino				
19	2004/10/6 13:17	127.0.0.1	auth	info	su(pam_unix)[6677]: session closed for user root				
20	2004/10/6 13:17	127.0.0.1	auth	info	sshd(pam_unix)[6639]: session closed for user thino				
21	2004/10/6 14:01	127.0.0.1	cron	info	CROND[7155]: (root) CMD (run-parts /etc/cron.hourly)				
22	2004/10/6 14:09	127.0.0.1	syslog	notice	syslog-ng[3640]: STATS: dropped 0				
23	2004/10/6 15:01	127.0.0.1	cron	info	CROND[7304]: (root) CMD (run-parts /etc/cron.hourly)				
24	2004/10/6 15:09	127.0.0.1	syslog	notice	syslog-ng[3640]: STATS: dropped 0				
25	2004/10/6 16:01	127.0.0.1	cron	info	CROND[7457]: (root) CMD (run-parts /etc/cron.hourly)				
26	2004/10/6 16:09	127.0.0.1	syslog	notice	syslog-ng[3640]: STATS: dropped 0				

PDF出力例



表集計

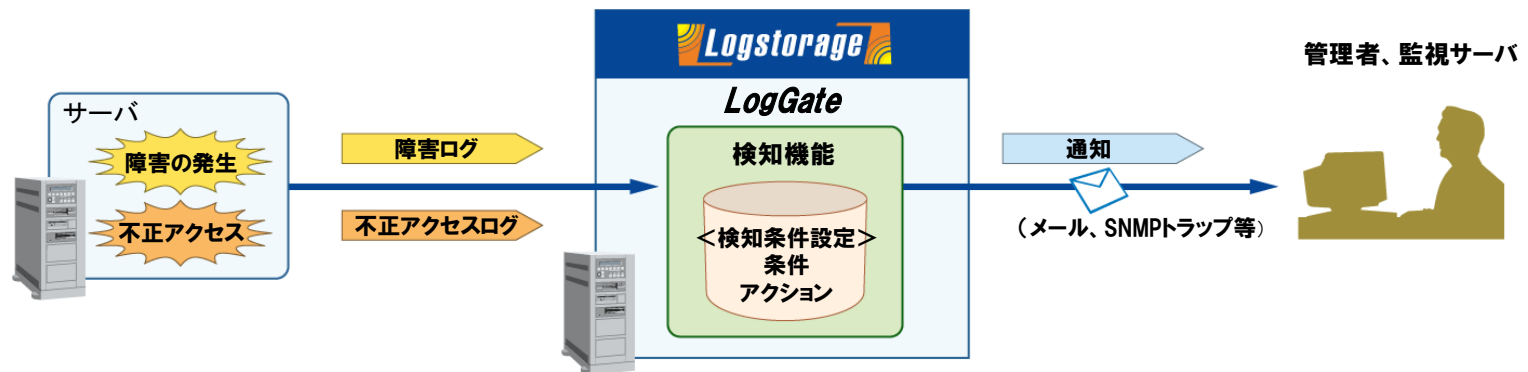
概要: アプリケーション、サーバ毎の件数

作成日: 2004/1

アプリケーション	サーバ											
	SMTPサーバ2	Oracleサーバ	Webサーバ	WindowsClient	SMTPサーバ5	SMTPサーバ3	SMTPサーバ11	アプリケーションサーバ1	アプリケーションサーバ2	qmailサーバ	SMTPFEED	アプリケーションサーバ4
ORACLE	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
telnetd	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
sshd	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
kernel	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
popper	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
smtspd	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
mysql	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
vsFTP	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
ntpdate	0.0	0.0	0.0	0.0	3.0	1.0	0.0	1.0	0.0	1.0	0.0	1.0
Windows監査ポリシー	0.0	0.0	0.0	12.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
ftpd	0.0	0.0	0.0	0.0	85.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
crond	0.0	0.0	0.0	0.0	0.0	102.0	0.0	102.0	0.0	0.0	0.0	102.0
Apache	0.0	0.0	401.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
vpopmail	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	403.0	0.0	0.0
(other)	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	360.0	134.0	0.0
qmail	0.0	0.0	0.0	0.0	0.0	0.0	3.0	0.0	0.0	1277.0	0.0	0.0
POP-3	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2136.0	0.0	0.0
sendmail	9851.0	0.0	0.0	0.0	1466.0	2715.0	605.0	35.0	0.0	0.0	369.0	35.0
総合計	9851.0	0.0	401.0	12.0	1554.0	2818.0	608.0	138.0	0.0	4177.0	503.0	138.0

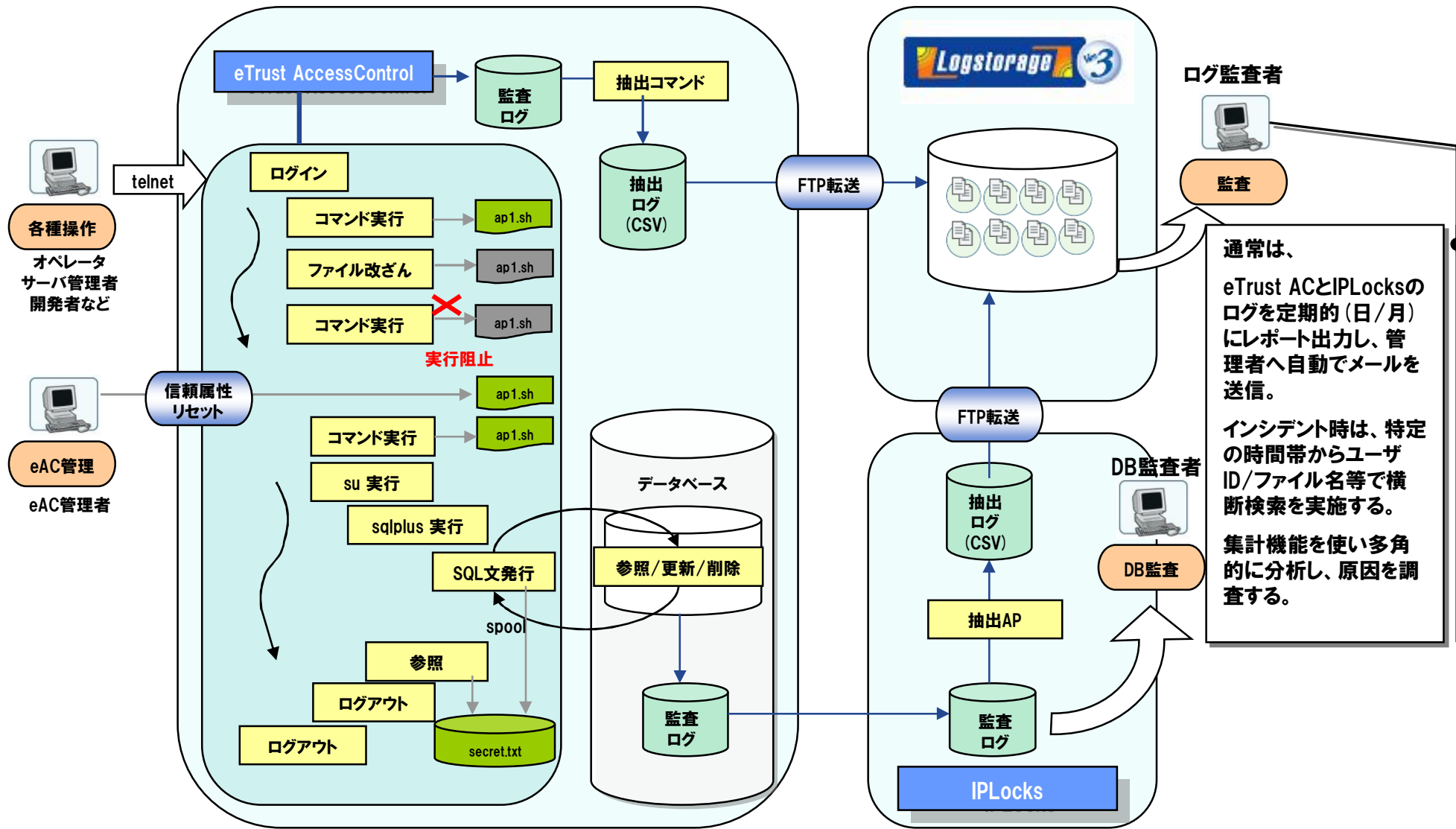
• ログの検知条件と通知方法を設定

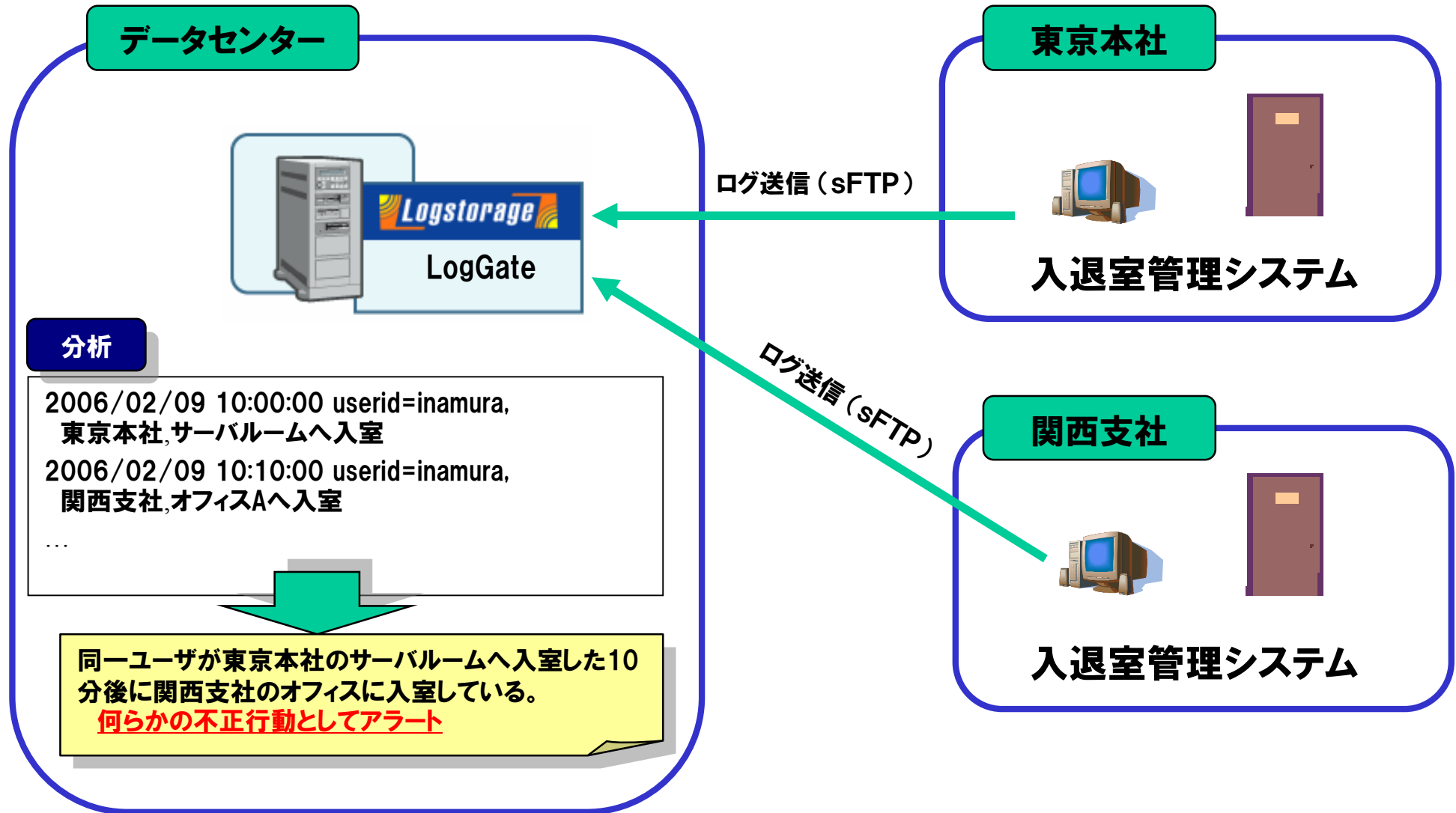
- ログの発生頻度による検知
- 異なる種類の複数ログの組み合わせによる検知(シナリオから検知)
- 時間や曜日別に検知
- 検知後のアクション(通知) 間隔制御
- 同時に複数のアクションが可能
- 置換パラメータに対応
 - 例) 置換パラメータを使い、ログメッセージを通知メールに貼り付ける
- 外部コマンドの実行
 - 例) 不正アクセスを検知し、ポートを閉じるスクリプトを実行する



5. 導入・活用事例

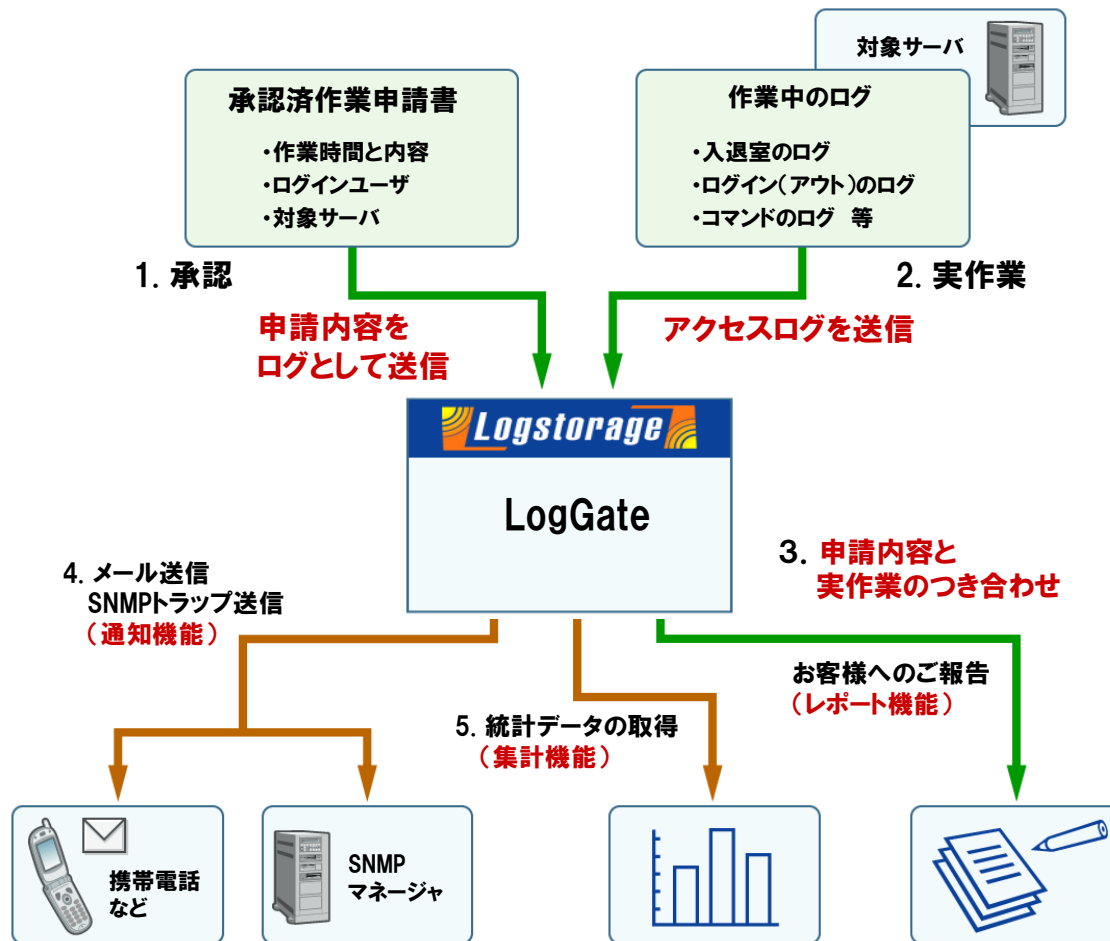






利用方法

1. 対象サーバへの操作申請書の承認を通す
- 申請内容をログとしてログストレージが収集
2. 対象サーバへの実作業中のアクセス管理
- 作業中のアクセスログをログストレージが収集
3. レポート機能を活用し、ログ監視
- 事前に申請された内容にあわせて入退出及びログインなどがされているかをつき合わせ
4. 通知機能を活用し、操作中のエラーログを実作業中の担当者、または管理者に通知
5. 集計機能を活用し、操作中行ったアクション毎の件数や対象となったデータの変更・削除の件数を集計



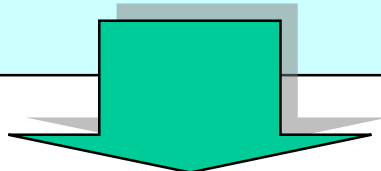
6. まとめ



統合ログ管理

多種多様な形式のログを、**一元的に長期間、原本性**を保ったまま保管する。

また多種多様なログを**横断的に検索・分析**することができ、ポリシー違反のアクティビティを**リアルタイムに検知**することができる。



内部統制において重要な役割を果たす証跡管理に、統合ログ管理の機能は必須です。

ポイントのまとめ

ログ管理ポリシー

- | | |
|---|--------------------------------------------------------------|
| 1 | サーバ、アプリケーション、ネットワーク機器によって収集すべきログは異なる。ログの内容について、何を含むべきか検討を行う。 |
|---|--------------------------------------------------------------|

ログの一元管理

- | | |
|---|----------------------------------------|
| 2 | ログの出力方法は各システムによって異なるが、それらを残さず収集し一元管理する |
| 3 | 各システムの時刻同期を行い、ログのタイムスタンプを統一する |

ログの長期保管

- | | |
|---|-------------------------------------|
| 4 | 事前のログ量の見積もり(それに応じた保管用ストレージの用意) |
| 5 | 拡張性の高いシステムの導入(主にログ保管領域の拡張) |
| 6 | 保管したログの利用(検索やレポート)を想定したハードウェアのサイジング |

異なるシステムのログ横断

- | | |
|---|-------------------------------|
| 7 | 収集したログを全て横断的に検索・分析できる仕組みを用意する |
|---|-------------------------------|

ログの改ざん防止

- | | |
|---|------------------------------------------------------------------|
| 8 | 以下のような仕組みを用いてログの改ざんを防止する
・アクセス権限による改ざん防止
・WORMによる改ざん防止(後述) |
| 9 | ログに電子署名を付与するなど、ログが改ざんされていないことを証明する |

開発元

- インフォサイエンス株式会社
- 〒108-0023 東京都港区芝浦2-4-1インフォサイエンスビル
- <http://www.infoscience.co.jp/>

お問合せ先

- インフォサイエンス株式会社 プロダクト事業部
- TEL 03-5427-3503 FAX 03-5427-3889
- <http://www.logstorage.com/>
- mail : info@logstorage.com

インフォサイエンス株式会社 Infoscience
(1Fにローソンのあるビル)



Logstorageに実装された機能およびロジックは特許出願中です。

- » 出願番号 特願2001-341113
 - » 名称 ログ情報管理装置及びログ情報管理プログラム
- ※ 仕様は予告なく変更することがあります。

END

「統合ログ管理によるIT統制の実現とその具体的事例」

2007/2/9

インフォサイエンス株式会社 プロダクト事業部

稲村 大介

