Log Option は、統合ログ管理をおこなうためのオプション製品です。System Answer シリーズとあわせてご利用いただくことで、ルーター、スイッチおよびサーバーなど各種ネットワークシステムの性能情報と、各機器が出力するシスログ、イベントログ、アプリケーションログをもとにした、詳細かつ正確なネットワークシステムの稼働状態など、運用に必要な情報を一元管理することが可能になります。

1 特長

Log Option の特長は、多種多様なログを収集方式にとらわれることなく、統一されたフォーマットで扱えることです。それぞれのログは記述形式が異なるため、ツールを用いず人手でおこなおうとすると、ログを読み解く知識と集計するための手間が必要となります。Log Option は、異なる種類のデータに同一の意味づけ（タグづけ）をおこなうことで、ログ形式の違いを吸収して扱うことができます。つまり、データの羅列にしか過ぎないログを、人間が見てわかる形式に容易に変換して、活用することが可能です。

管理面

- 一元管理
- 保護機能
- アクセス制限
- 長期・圧縮保管
- セキュリティ強化
- PCI DSS / ISMS

運用面

- 即時アラート
- 定期レポート出力
- 検索・分析
- 暗号化
- 監視自動化
- ログ容量削減

2 System Answer シリーズとの連携

System Answer シリーズと Log Option を連携することにより、性能情報とログ情報の統合管理が可能となり、障害の予兆検知や予防保守をおこなうことができます。また、システム障害やセキュリティ事故が発生した場合でも、その影響範囲の把握から原因究明のためのピンポイントでのログ調査までを一貫しておこなうことができるため、可用性と安全性を兼ね備えたシステム運用が可能となります。さらに、Log Option のレポート機能により、System Answer シリーズで検知したアラート分析やレポート出力もおこなうことができます。

System Answer シリーズ		+ LOG OPTION
性能監視 / リソース監視 性能・リソース情報を分析することで、早期の原因究明や根拠ある再発防止対策を提示。	**原因究明を迅速におこないたい** 障害発生時のアプリケーションログを把握しようとすると、該当サーバーに個別にログインする必要があり、原因究明に時間がかかる。	**詳細なログ取得** 各種機器のテキストログを取得し、一元管理。障害やセキュリティ事故発生時の詳細な証跡ログを把握し、迅速な復旧・対策が可能。
キャパシティ計画 CPU 、メモリー、ディスク情報などの性能情報をもとに将来予測をおこない、どの程度システムを増強すべきか、根拠ある対策を立案。	**具体的な対策を取りたい** 性能情報で全体的な傾向は把握できるが、アプリケーションレベルでの詳細な傾向が把握しにくい。	**豊富なログ収集** 各種サーバー / アプリケーションログを横断的に一元管理し、どのアプリケーションがリソースに影響を与えているかを分析して、計画立案が可能。
予防保守 性能情報の傾向を学習することで、サイレント障害の検知をおこない、トラブルを未然に防止。	**障害を予防したい** 性能監視だけでは把握しにくいアプリケーションの挙動の変化や、セキュリティ事故につながる不審なアクセス / 挙動を掴みたい。	**ログ分析による検知** ログの横断追跡によって「いつ誰が何をしたのか」を把握し、検知条件に合致したアラート通知も可能。障害や事故につながる挙動を早期に発見可能。
レポート 性能情報を簡単にレポート出力。システム全体の把握や、月次 / 週次レポートなどの報告書に活用。	**さまざまな脅威に対応したい** 性能監視では把握できないアプリケーションログを取得し、必要があれば取得結果を証跡レポートとして出力したい。	**集計レポート出力** 収集したログの集計結果を表やグラフで出力することができ、証跡として活用可能。また、その結果を月次や週次で定期的に自動出力が可能。(出力形式：html , pdf , csv , png , txt)

3 効果・活用例

課題：サーバーアクセス遅延の原因調査

突然、監視対象の Web サーバーへのアクセスが遅くなり、サービス品質の低下が懸念される状態に陥った。早急かつ的確な原因の特定と対処が必要になった。

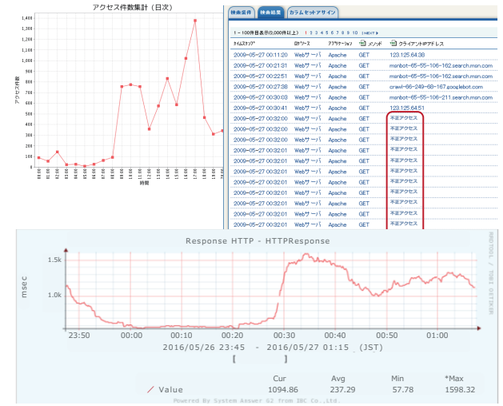
分析：ログ分析による原因特定

System Answer シリーズを利用して分析した結果、通常よりも HTTP のレスポンスが悪化していることが判明した。

Log Option を活用して事象発生時のログを確認したところ、特定の通信元から大量にアクセスを受けていることがわかり、外部からの不正アクセスによるものと判断した。

対策：適切な対処策の実施 / 調査結果の詳細な報告

不正アクセスを防止するため、該当する通信をブロックすることで問題が解消された。System Answer シリーズおよび Log Option から事象発生時のレポートを抽出し、詳細な報告書を迅速に提出することができた。



4 提供形態

ET：エントリー　WG：ワークグループ　ST:スタンダード　EH：エンハンスト　EP：エンタープライズ　AD：アドバンスト

エディション		ET	WG	ST	EH	EP	AD
拡販モデル		エントリーモデル	スケールアップ・モデル			スケールアウト・モデル	
概要		小規模向け エントリーモデル	スモールスタートでのログ管理。 1 台で収集性能の拡張をおこなう。			拠点・目的ごとのログ管理やすべてのログを統合管理。複数並列処理で収集・検索性能の拡張をおこなう。	
ライセンス	コンソールサーバー	1 台	1 台			1 台	1 台
	LogGate	1 台	1 台			2 台	2 台（追加可能）
	クライアントライセンス （ログ収集対象サーバー台数）	50 台 （追加不可）	5 台（追加可能）			無制限	無制限
	集計モジュール	○	オプション			○	オプション
	検知モジュール	○	オプション			○	オプション
	レポートモジュール	○	オプション			○	オプション
Event Log Collector (ELC)		×	×	○	○	○	○
LogGate の追加		×		×		○	○
複数 LogGate の横断検索・分析		×		×		×	○
検索専用 LogGate の設置		×		×		×	○
LogGate 冗長構成		×		○ (Active - Standby)		○ (Active - Standby)	○ (Active - Active)
LogGate 収集性能 （1 台あたりの目安）		100 行 / 秒	1,000 行 / 秒	2,000 行 / 秒	3,000 行 / 秒	4,000 行 / 秒 (2,000 行 / 秒)	6,000 行 / 秒 (3,000 行 / 秒)
コンソールサーバー冗長化		×	○	○	○	○	○

※ 収集性能は目安
※ 「行 / 秒」は受信してから利用可能な形式になるまでの全体の収集性能を表す。受信のみを表す「eps」とは単位が異なる