



2007
ALTIBASE DBMS Day

KT異常トラフィック検知/分析/制御システム(KAPS)

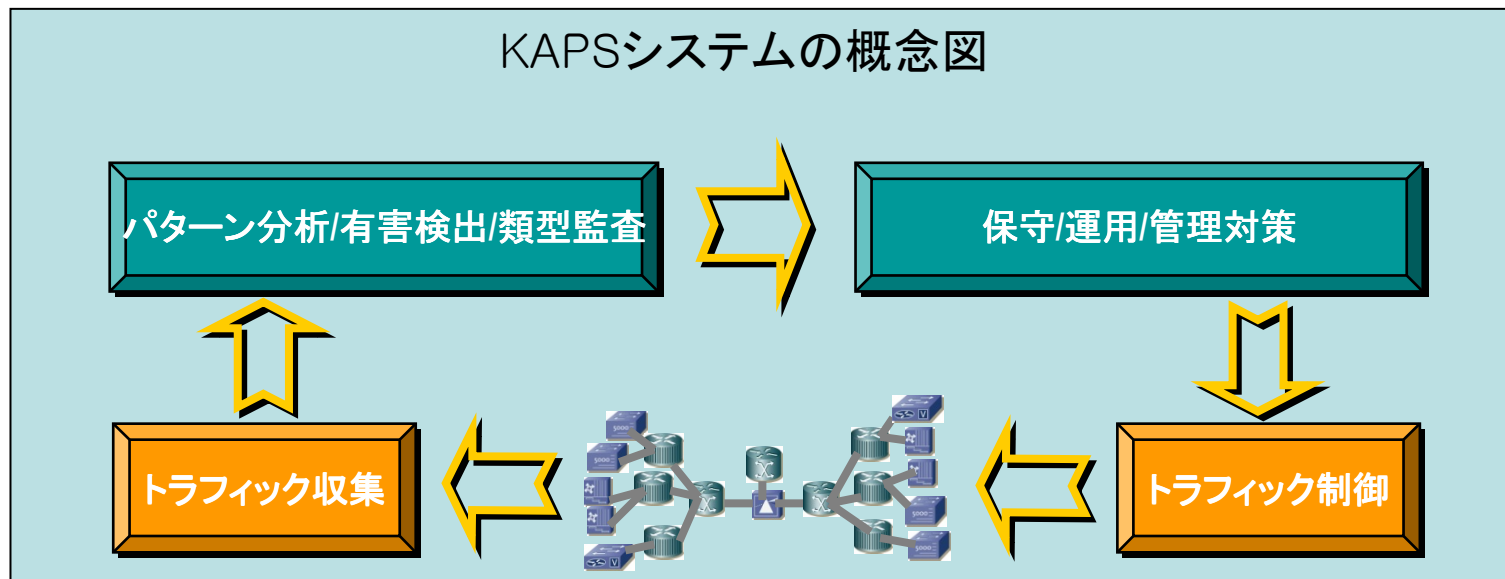
DMX Korea










KAPS (KORNET Abnormal Traffic Audit & Provisioning System) の概要

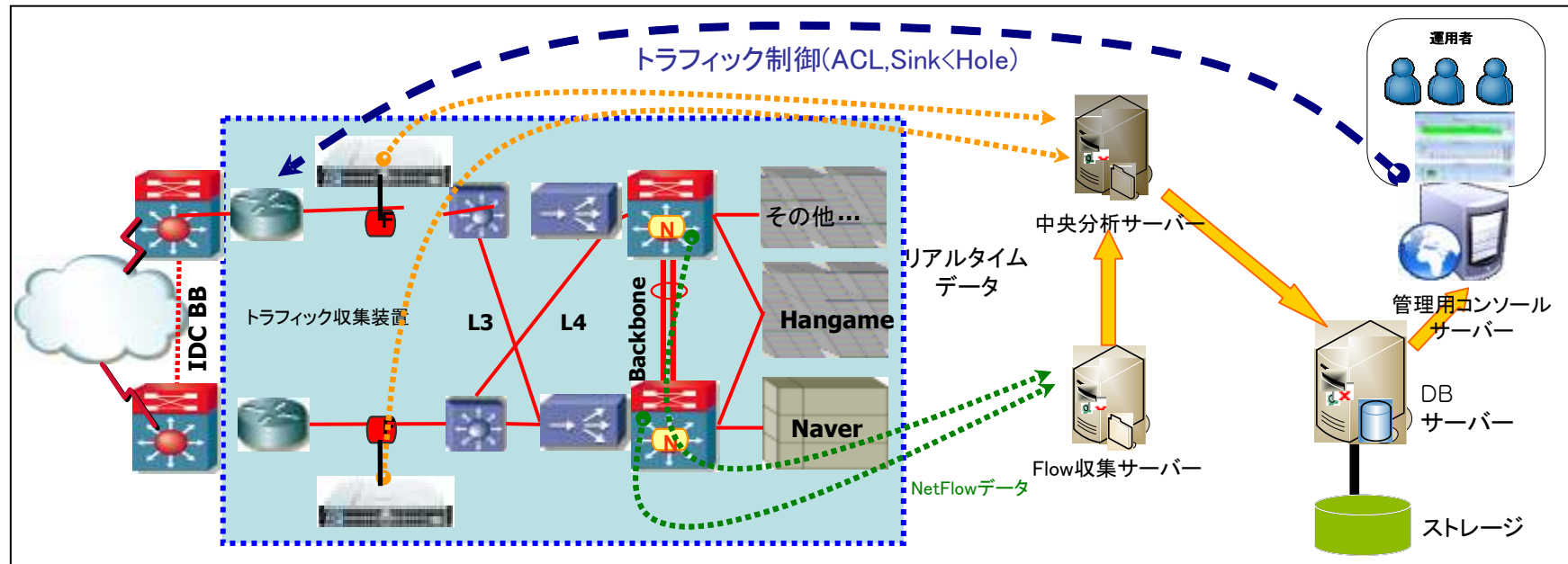
- 1/25 大乱 (2003年1月25日のDDoS攻撃によるISP無力化)対応システム
- 網事業者レベルでの対応戦略の必要性を痛感 (端末、システム保護戦略とは区別)
- 正常トラフィック(DNS, DHCP, HTTP 等)を装った攻撃の探知システムの必要を提起
- 大規模/全国的ネットワークに適用可能な探知/分析/制御システムの必要性が台頭





システム構成、及び動作概要

区分	概要
トラフィック収集装置 	リアルタイムトラフィック収集中央分析サーバーにデータを送信
Flow収集サーバー 	ネットワーク装置から発生するNetFlowデータを収集し、中央分析サーバーに転送
中央分析サーバー 	収集装置、Flow収集サーバーから提供されるトラフィック情報からリアルタイムで検知、分析を実行
DBサーバー 	リアルタイムトラフィックイベントの統計データを蓄積し、照会に対応
管理用コンソール 	制御及び管理を実行し、トラフィック学習によるパターンプロファイル生成機能を提供





データベースの役割とChallenge

データベース の役割	トラフィック DB	▪ 異常有無判断用の個別トラフィックデータをリアルタイムで保存するためのデータベース (トラフィック総量、プロトコル、発信/着信ポート、発信/着信IP、IP Flow、Flag等個別データのリアルタイム保存)
	Flow Data DB	▪ イベント詳細分析用総合トラフィックデータを保存するためのデータベース (L4トラフィック情報が全て含まれているデータの保存用 - トラフィック相関関係分析用として使用)
	イベントDB	▪ イベント高速処理のためのデータベースで、大容量のイベントを処理

Challenge	トラフィック DB	▪ 1G, 2.5G, 10G 各区間において収集されたトラフィックの元データの膨大さ ▪ 1G : 収集期別平均40万件/分あたり(約15区間) ▪ 2.5G : 収集期別平均250万件/分あたり(約75区間/同時15区間) ▪ 10G : 収集期別平均800万件以上/分あたり(約5区間) ▪ 1次分析を経てフィルタリングされた約10%以内の情報を30秒以内に保存しなければならない
	Flow Data DB	▪ 1分以内に収集されたトラフィックの有害性の有無を判断できるように、高速検索/照会を提供しなければならない
	イベントDB	▪ 発生したイベントとイベント解釈/敷衍説明のための連関データの保存 ▪ イベント間の関連の分析のための高速データ処理の実行

★ 顧客要求目標：3分以内に検知、5分以内に対応

2003年(一次): ディスク型データベースでのシステム構築

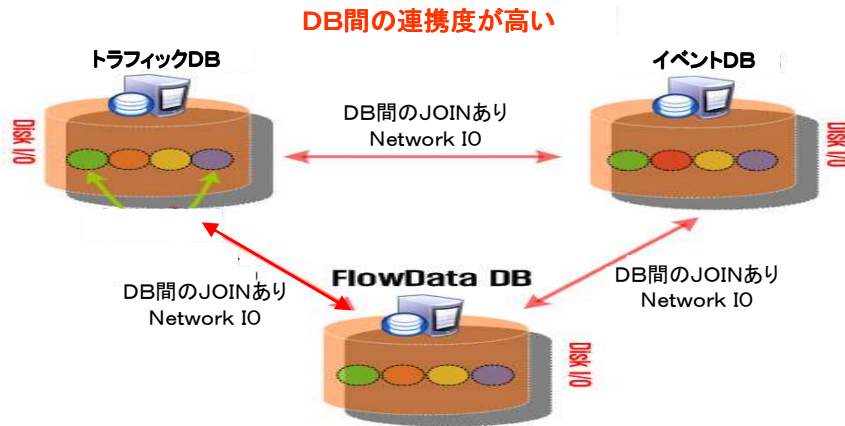
2005年(2次): ディスク型データベースの増設

しかしながら、投資費用や物理的な拡張が限界となってきた。

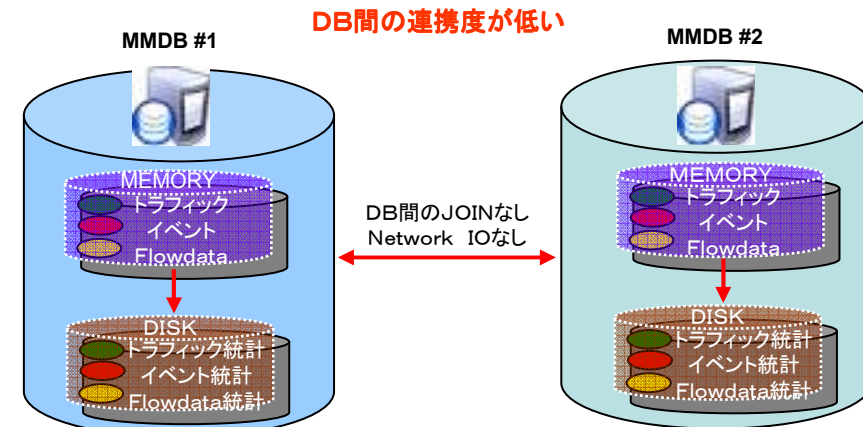


ALTIBASE ソリューション for KAPS

改善前(問題点)



改善後の効果

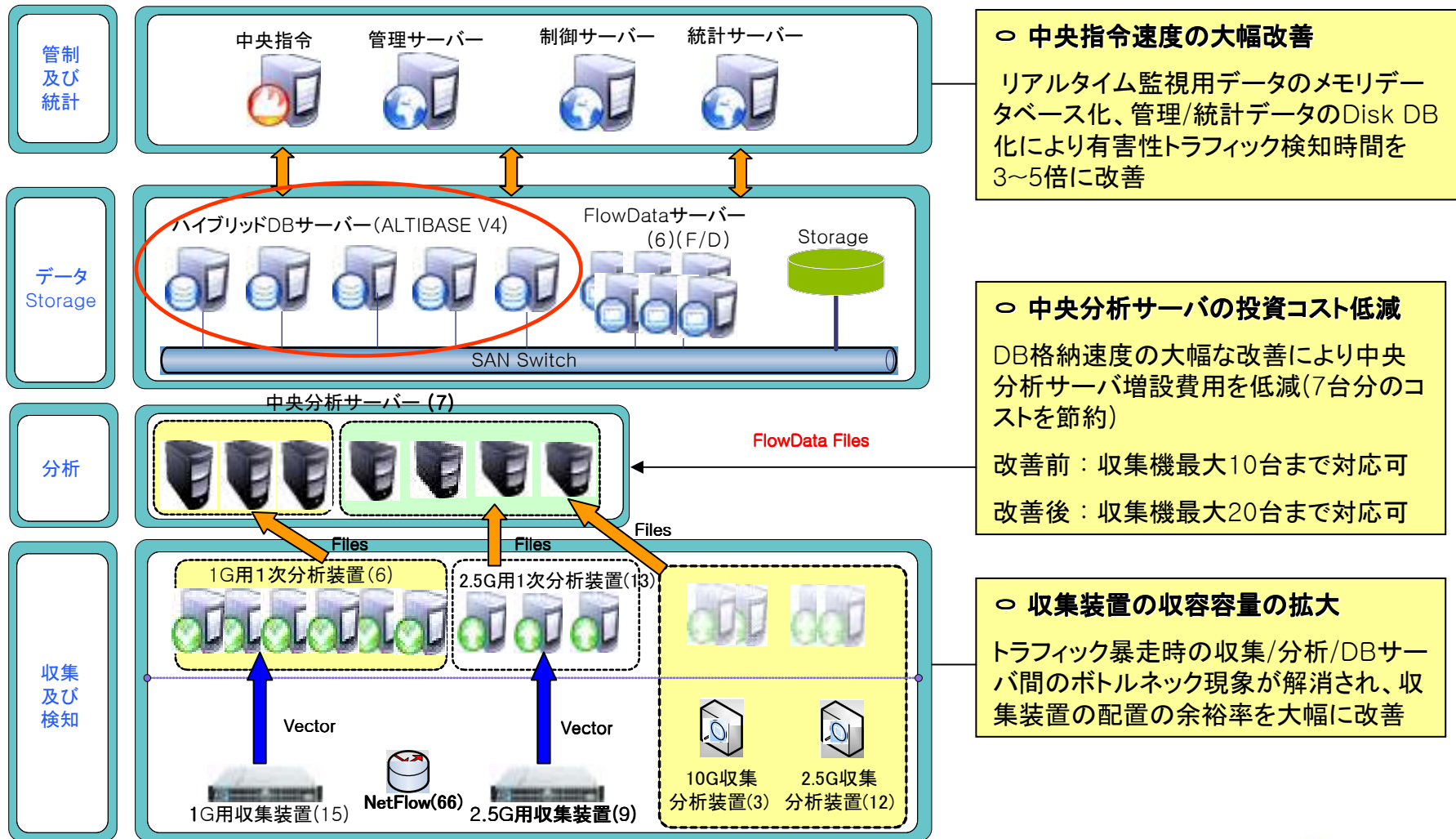


- 機能別の配置によりDBMS間の関連性が高い
 - DBMS間のDB LinkによるNetwork I/O処理負荷
- データ特性格の処理構造となっていないため、非効率
 - 大容量データのDisk保存によるDisk I/O 処理負荷
 - 多量のイベントの相関関係の分析及びDB処理負荷
- 詳細分析用データ処理遅延
 - 収集区間拡大(10G, 2.5G)に従うデータ増加
 - 大容量DB保存及び照会/分析・処理の遅延
- 収集区間拡大に伴い、事実上データ処理が不可能に
- データ照会の応答時間の遅延(分単位の所要時間)

- ハイブリッドメモリデータベースにより通じたりアルタイム大容量データ処理を改善
- データ特性格の処理構造に変更することで処理効率を向上
 - リアルタイム性データのメモリ処理によるDisk I/O遅延改善
 - 収集装置別に垂直的な機能統合を行ないNetwork I/O改善
- データ保存速度の向上 約8~10倍アップ(数十秒 ~ 数秒以内)
- データ照会速度の向上 約20倍アップ(数十秒 ~ 2秒以内)
- メモリ増設のみでデータ格納容量を拡大可能
- メモリとディスクを同時にサポートすることでデータ処理効率アップ
- データ照会応答速度の画期的な改善により攻撃への対応力アップ



KAPS システム改善の概要



○ **中央指令速度の大幅改善**

リアルタイム監視用データのメモリデータベース化、管理/統計データのDisk DB化により有害性トラフィック検知時間を3~5倍に改善

○ **中央分析サーバの投資コスト低減**

DB格納速度の大幅な改善により中央分析サーバ増設費用を低減(7台分のコストを節約)

改善前：収集機最大10台まで対応可
改善後：収集機最大20台まで対応可

○ **収集装置の收容容量の拡大**

トラフィック暴走時の収集/分析/DBサーバ間のボトルネック現象が解消され、収集装置の配置の余裕率を大幅に改善



プロジェクト後記

プロジェクトの初期に、データベースの変更に伴う危険性(開発の負担、試行錯誤など)から、一部の顧客や競合会社からの反対の声が上がっていた。

競合会社:アプリケーションの全面改修が必要。期間内のリリースは不可能!

顧客:従来システムが安全では?運用の負担は?やり遂げることが出来るのか?

開発者:開発できるのか?サポートは大丈夫なのか?

Anyway! Mission Complete!!! Because ~

ALTIBASEの技術力 + SI会社の推進力 + 顧客の信頼

- 既存DBMS基盤アプリケーションのHybrid DBMSへの移行開発のサポート
- SQL Queryチューニングサポート(開発者教育及びQuery文個別チューニングサポート)
- 業務要件を実現するためのAltibase V4 機能アップデート
- 活発な営業サポート(製品ロードマップ、サポートプロセス、顧客対応等)
- 強い意志と推進力!!! それと、ベンダーとの信頼!



終わりに

技術力+推進力+信頼

- 既存製品に慣れている開発者からの反発が予想より強かった。
- 開発期間中、予想できなかった障害が頻繁に発生(反発がさらに強くなった)
- ベンダーからのサポートは期待値を越えられない(ベンダーと顧客企業との間の永遠の課題)
- 顧客はいつも結果を重視する(ベンダーの言い訳はNG!)

- 顧客に対し、システムはいつも有用なツールであると同時に、不満の対象である。
- 完璧ではないが、最善を尽くしたプロジェクトとして顧客に記憶されることを期待する。
- とにかく、顧客はシステムを愛し継続して発展することを望んでいる。



**We are still going on with
both customer and Altibase!**