

安心ネットワーク環境を実現するマネジドセキュアネットワークソリューション Managed Secure Network Solution for Reliable Networks

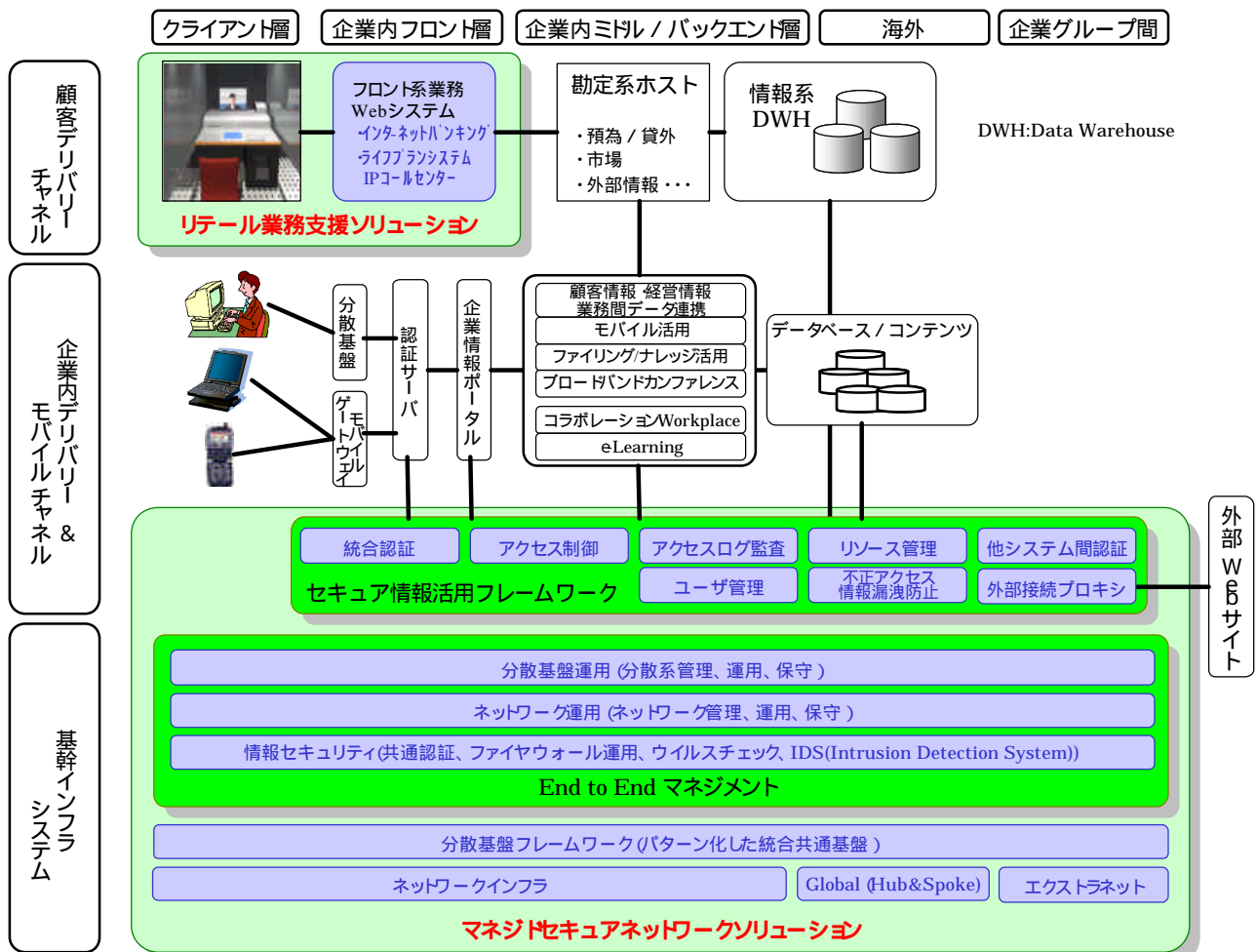
要 旨

金融機関では、お客様への安定したサービスの提供を目的として、コピキタス社会を支えるコアネットワークの再構築に注力している。それを受け、ネットワーク市場では、従来のネットワーク構築サービスが、ネットワークのトータルインテグレーションや運用アウトソーシングまでへと急速に拡大している。また、金融系 IT システムは能力向上と共に、企業業務遂行の根幹の位置付けになっており、システムの障害が企業存続の危機に陥れる場合もある。

このような背景を踏まえ、三菱電機インフォメーションシステムズ(株) (MDIS) では、金融機関向けソリューションとして、ネットワークインフラ構築・運用をワンストップでサポートする“マネジドセキュアネットワークソリューション”と、金融機関の顧客を対象とした“リテール業務支援ソリューション”を提供している。

本稿では、主にマネジドセキュアネットワークソリューションについて述べ、金融系 IT システムのネットワークと分散基盤の構築・運用及び情報セキュリティの包括的管理など、金融基幹系分散ネットワークシステムにおけるクライアントからサーバまでの End to End マネジメントに関する技術を紹介する。

システム障害によるリスクを減少させるため、発生障害の影響範囲把握、障害復旧に向けた自動的な対応、原因の絞り込みなど、従来には無かった高度な機能を提供している。金融機関の大規模な分散系システムでは、多数のサーバ、クライアント、業務システムが動作しており、システムの安定稼働、コスト削減のために、非常に重要なソリューションである。



マネジドセキュアネットワークソリューション

ネットワーク運用と分散基盤運用及び情報セキュリティの各コンポーネントを組み合わせ、お客様のニーズにあった、分散系システムのネットワーク構築・運用ソリューションをワンストップでトータルに提供する。

1. ま え が き

近年、企業の IT システムは、能力向上と共に業務遂行の根幹の位置付けとなっている。IT システムの障害や情報セキュリティ侵害の影響が、金融機関では特に経営的な課題として重要となっており、IT リスクマネジメントの視点から以下 2 点の極小化が最大の課題となっている。

(1) システム障害によるリスク

企業本来の業務を遂行する基幹系システムのみならず、メール、事務処理、ポータルなどいわゆる分散系システムも、今やシステム障害により停止することは、企業業務の遂行を円滑に実行することの妨げになるばかりでなく、企業の社会的信用度の失墜につながる可能性もあり、システム障害による経営へのリスクが増大している。

(2) 不正行為により被る損失リスク

情報漏洩が新聞紙上をにぎわすことも度々あり、2005 年 4 月施行の個人情報保護法に伴い、システム安全対策の具体的な実現方式のガイドラインが関係各省庁より示されている。

本稿では、上記 2 つのリスクのうち、システム障害によるリスクを極小化し、システム安定稼働を実現するための方式について述べる。

2. マネジドセキュアネットワークソリューション

金融機関では、徹底的なコスト効率を追求した IT、新商品への高い対応力を持つ IT を求めている。また、金融業態間の各種制度の段階的な撤廃と非金融機関をも巻き込んだ合併なども進んでいる。

MDIS では、このような背景を踏まえ、コンサル・設計・構築・保守・運用技術の統合を具現化し、ネットワーク構築・運用のワンストップサービスとしてマネジドセキュアネットワークソリューションを提供している。

図 1 は、マネジドセキュアネットワークソリューション全体のモデルを示している。ネットワークインフラソリューションは、ネットワークインフラの構築を始め、回線、モバイルの構築を提供する。ネットワークマネジメントは、ネットワーク運用、分散系システム運用管理システムの構築・運用、セキュリティシステムの構築・運用を提供する。

3. 分散系システム運用における課題

金融基幹系の IT システムに代表される大規模な分散系システムでは、ネットワークやサーバ、アプリケーションが連携し、業務システムを構成している。これらのシステムにおける課題は、次のものが挙げられる。

(1) 業務影響範囲把握

大規模なシステムでは、障害発生時に業務システムへの影響範囲を正確に把握することが困難である。

(2) ノウハウに依存した障害対応

複雑な連携で構成されるシステムでは、サーバ間やミドルウェア間の連携が多岐に渡るため、システムを熟知した技術者のノウハウに依存した障害対応が行われている。

(3) 変更管理情報の更新

分散系システムでは、構成の変更が随時実行されるため、構成情報を常に最新状態で維持管理することが困難であり、コストがかかる。

(4) 関係者全員の情報共有

分散系システムでは、関係者が多数連携し、解析及び対処を実行する。システムの状態を的確に把握し、情報を迅速に共有し、分析しながら対処を決定していく必要がある。

4. 運用高度化のアプローチ(End to End マネジメント)

3 章で述べた分散系システムの運用管理における課題を解決するためには、現在行われているネットワークやサ

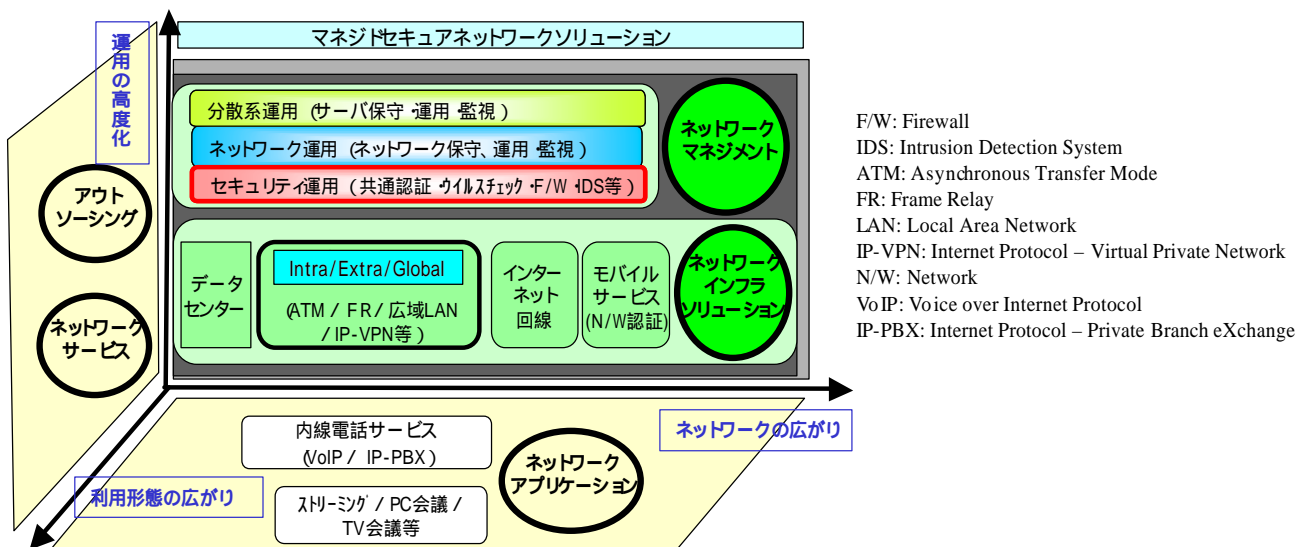


図 1 . マネジドセキュアネットワークの全体モデル

ーバ、アプリケーションを個別に管理するやり方から、業務システムの端点（エンド）から端点（エンド）までを業務視点で管理するやり方、すなわち End to End マネジメント（E2E）に変えて行く必要がある。E2E マネジメントは、個別管理で得るメッセージや、情報を統合する情報収集・統合機能、これらを基に業務影響範囲把握、既知障害対応、未知障害対応、障害原因の絞り込みなどを行う高度分析機能及び収集した情報や分析結果の情報共有機能から構成される（図2）。また、これらは、将来的には、運用管理の自律化へつながるものである。

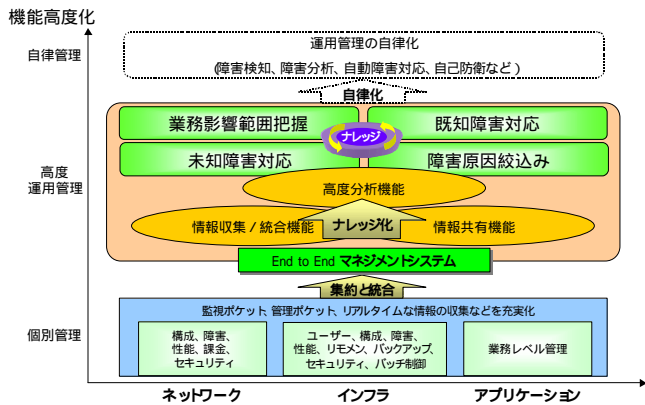


図2. 運用高度化のアプローチ

以下にこれらの高度運用管理機能について述べる。

4.1 業務影響範囲把握

業務影響範囲把握には、業務システムを構成するサーバの最低限の情報（IP アドレスまたはホスト名、サーバ間の連携情報）を、業務定義情報として予め設定しておく。

構成情報を自動収集するなど、システムが拡張・変更されても設定情報の更新が少なく済むようにしておくことで、運用段階での維持管理コストを削減することができる（図3）。

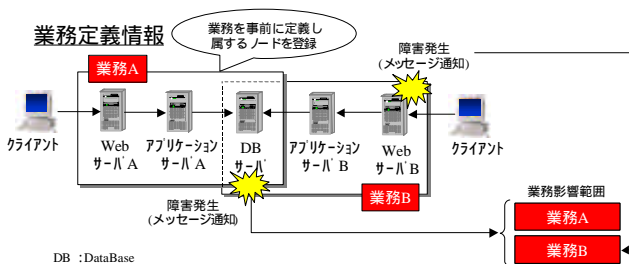


図3. 業務影響範囲把握

業務Aは、WebサーバA、アプリケーションサーバA及びDBサーバから構成されており、業務Bは、WebサーバB、アプリケーションサーバB及びDBサーバから構成されている例を示す。DBサーバまたはWebサーバBから障害メッセージを検知した場合、業務定義情報を参照することにより、A及びBの業務へどのように影響を及ぼすかを自動判断する。個別の障害メッセージを検知した

時に、システム全体の中での影響範囲や関連業務を抽出できることは、対策の緊急性や対応者の選定に有効であり、障害対応の初期段階で必須となる情報である。

4.2 既知障害対応

組織化された運用管理体制を有する業務システムでは、システムで発生した障害などに対応する手順書が完備されている。障害が発生した場合、オペレータはシステム管理ツールが出力するメッセージなどをインデックスにして、対応する手順を検索し、一次対処やデータ収集を行う。

しかしながら、対処のために使用するコマンドに対する知識や出力結果の判断などは、オペレータのスキルに依存するため、複雑な対処手順が必要な障害が発生した場合、遠隔のシステム管理者や、サービスデスクなどに問い合わせる必要があり、迅速な障害復旧の妨げとなっている。

既知障害対応は、明文化された対応手順をコンピュータ上で実行可能な形式に変換し、システムで発生した障害に対応して動作させることで、障害に対する一次対処の迅速化をねらっている。また、対処まで自動化できない複雑な障害においても、障害解析のための情報収集を対応手順として自動化させる事によって、解決までの作業効率化を図ることができる。既知障害対応の構成を図4に示す。

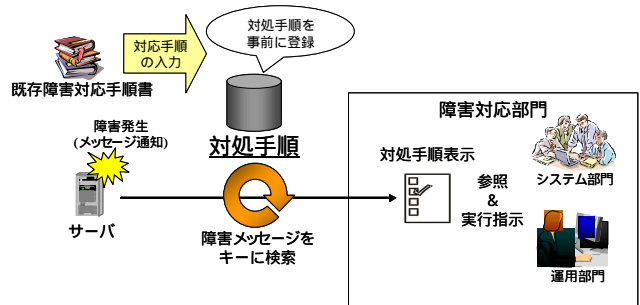


図4. 既知障害対応

既知障害対応は、コンピュータ上で動作可能な形式に変換した対応処理、それらを登録するデータベース、システム管理ツールとの連携機能から構成される。システム管理ツールが障害（メッセージ）を検出すると、データベース上の対処処理を検索して実行する。

4.3 未知障害対応

システムで障害が発生した場合、原因の特定や復旧に向けて様々な機器情報の収集が必要である。しかしながら、情報収集のために使用される特殊コマンドは、一般ユーザが使用するコマンドとは異なり、熟練管理者でなければ使いこなすことが困難なものが多い。そのため、障害発生後に召集された熟練者が、現地のオペレータに対して詳細な指示を出しながら情報収集を行い、一通り情報が集まった後で、それらを参照しながら原因調査等の解析作業を行っ

ている。

未知障害対応は、システム管理ツールが検出した障害メッセージを基に、その発生元となった機器に対する情報収集を自動化することで、以降の障害解析の作業効率化をねらっている。未知障害対応の構成を図5に示す。

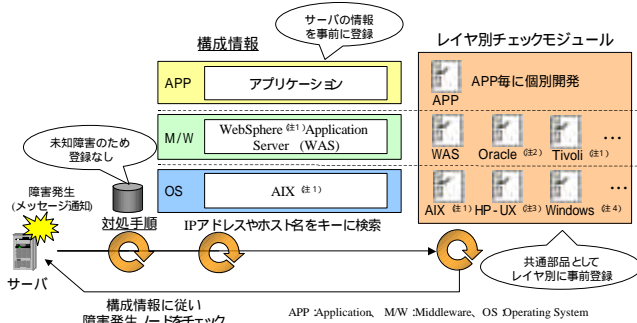


図5．未知障害対応

システム管理ツールが検出したメッセージを解析し、メッセージの発生元となった機器のIPアドレスやホスト名を抽出する。それらをキーに、あらかじめ登録されている機器の構成情報(OS,ミドルウェア,アプリケーションなど)の検索及び構成要素を診断するチェックモジュールを実行させる。

図5の例では、メッセージを通知した機器はサーバであり、OSにAIX,ミドルウェアにWebSphereが動作している。これらを構成情報から検索し、さらに各チェックモジュールをサーバ上で動作させる。これらの処理を自動化することで、障害発生から情報収集までの作業を大幅に短縮させることが可能となる。

4.4 障害原因絞込み

大規模な分散システムでは、多数のコンピュータやネットワーク機器が関連して動作しているため、ある機器で発生した障害が伝播して他の機器や業務に影響を与え、それをシステム監視ツールが障害として検出する場合がある。

このようなケースでは、最終のメッセージ発生元の機器を解析しても原因を見つけることが出来ないため、障害解析作業は困難を極め、結果としてシステム管理者に大きな負担を強いることになる。

障害原因絞込みでは、前節で示した未知障害対応の構成情報に加えて、業務に関連した構成情報を利用する。図6に障害原因絞込みの例を示す。

システム管理ツールがWebサーバAで障害を検出した場合、WebサーバAで未知障害対応で示したチェックモジュールを実行する。異常箇所を検出できなかった場合は、構成情報を参照し、業務Aに関連するアプリケーションサーバAを検索するが、ここでWebサーバAとアプリケーションサーバA間のネットワーク機器を経路情報探索コマンド(traceroute)などによって探索し、検出されたネ

ットワーク機器に対してチェックモジュールを実行する。以上の処理を、依存関係定義情報を参照して業務Aに関連する機器に対して実行していく。

障害は処理の連携を通して伝播していくため、業務関係情報による絞込みは有効と考えられる。また、障害箇所特定に至らなくとも、関連処理の情報を自動的に収集することで、以降の解析作業の効率化も期待できる。

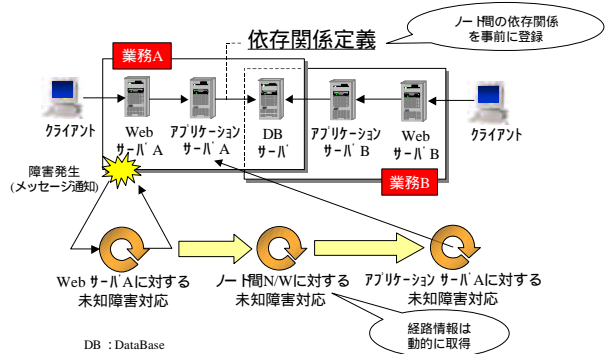


図6．障害原因の絞込み

5.むすび

大規模分散系システムのシステム障害によるリスクを減少させるため、発生障害の影響範囲把握、障害復旧に向けた自動的な対応、原因の絞込みなど、従来には無かった高度な機能及び手法を紹介した。

現在、この手法をプロトタイプしたものが完成した段階であり、今後は、構成情報構造の見直しや自動収集処理等の改善を実施していく所存である。

参考文献

- (1) 菊竹秀夫,ほか:金融情報システム向けセキュア情報活用ソリューション,三菱電機技報,77, No.4, 251~254(2003)
- (2) 相浦利治,ほか:運用管理の高度化,2004信学会総大会A-9-3,電子情報通信学会(2004)
- (3) 宮内直人,ほか:ネットワーク障害の故障診断方式に関する検討,TM研究会,電子情報通信学会(2004)
- (4) 森一,ほか:サーバの依存関係を利用したシステム構成管理の支援方法,DSM研究会,2003-DSM-31,情報処理学会(2003)
- (5) 飯島正,ほか:ネットワークエージェント技術を用いた業務指向分散システム管理の構想,KBSE研究会,電子情報通信学会(2004)

(注1) WebSphere, AIX, Tivoliは、米国IBM Corporationの登録商標である。
(注2) Oracleは、米国Oracle Corporationの登録商標である。
(注3) HP-UXは、米国Hewlett-Packard Companyの登録商標である。
(注4) Windowsは、米国Microsoft Corporationの登録商標である。