2003－ＤＳＭ－31　（10）
2003／11／26

オペレーショナルリスク計量のためのネットワーク監視方式

増岡 義政† 直野 健† 亀山 伸†
E-mail: {masuoka, naono, skameyam}@crl.hitachi.co.jp

概要 企業内部における情報システムの運用管理操作ミスなどの事象(損失事象)により発生する損失を,自社のリスクとして評価するオペレーショナルリスクの計量が,特に金融機関で重要になっている.本稿では,運用管理ミドルウェアを用いてオペレーショナルリスク計量の自動化を実現するための課題と解決策を検討した結果を述べる.検討の結果,運用管理ミドルウェアの既存機能の拡張によりオペレーショナルリスク計量を自動化できる見通しを得た.特に損失事象を漏れなく収集したかどうかを検証する機能については,ネットワークを監視するサーバを設けることにより実現できる見通しが得られた.

A Network Monitoring Method for Operational Risk Evaluation

Yoshimasa Masuoka† Ken Naono† Shin Kameyama†
E-mail: {masuoka, naono, skameyam}@crl.hitachi.co.jp

Abstract This article explains a method to automatically evaluate the operational risk inside organizations, which becomes important especially in financial organizations. The risk evaluation method can be implemented as an extension to the system management middleware. This article shows the outline of the automated risk evaluation and especially focuses on the network monitoring functionality to prove that the collected operational loss events, which is the primary input in the risk evaluation procedure, is complete.

1.はじめに

システム運用管理における操作ミスなどの事象(損失事象)によって企業内部で発生する損失を,自社のリスクとして評価するオペレーショナルリスクの計量が,特に金融機関で重要となってきている.本稿では,オペレーショナルリスク計量に伴う企業のコスト増を抑制するため,計量作業の自動化を,システム運用管理ミドルウェア(例えば[3])の機能として実現する場合の課題と解決策を検討した結果を述べる.

オペレーショナルリスク計量の自動化においては,特に個別の損失事象を漏れなく収集したか検証する機能の実現が未解決である.本稿では特にこの課題の解決策に着目し,ネットワークを監視するサーバを設けることにより,端末を含む企業内部のすべての計算機において損失事象を収集しているかどうかを検証する方式を提案する.

本稿では,２章で基盤となる運用管理ミドルウェア・アーキテクチャを提示し,３章でオペレーショナルリスクの定義と計量方法,４章で計量の自動化とその問題点,および解決策について説明する.

2.運用管理ミドルウェア・アーキテクチャ

図 1 に本研究における基盤となる運用管理ア

† (株)日立製作所 中央研究所
† Central Research Laboratory, Hitachi, Ltd.

ーキテクチャのモデルを示す．同モデルでは，機器の状態やエラーメッセージなどの運用管理情報は，業界標準の情報モデル(例えば CIM: Common Information Model)に基づいて仮想化される．また，運用管理製品は，各種機器の運用管理情報を提供する管理オブジェクトと，管理オブジェクトの提供する運用管理情報を利用・分析して，自動運用管理や管理者へのレポーティングなどを行う運用管理 AP の２種類に分かれ，両者がオープンなプロトコル（標準メッセージバス）によって接続されることになる．

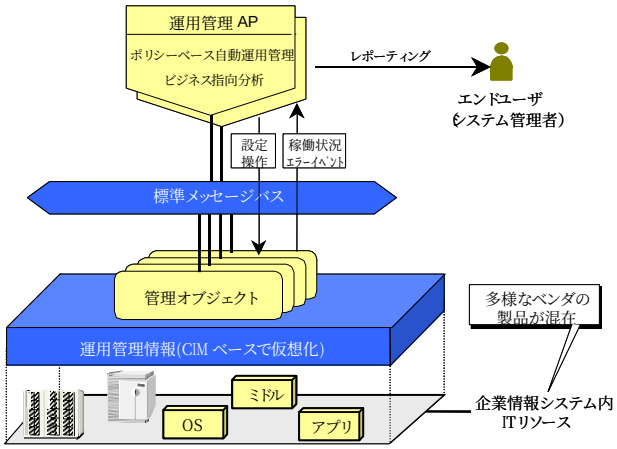

図 1 運用管理ミドルウェア・アーキテクチャ

本運用管理アーキテクチャにより，さまざまな運用管理製品の相互運用性が高まり，あるシステムの管理オブジェクトが提供する情報を他のシステムにおいて利用できるようになる．即ちこれにより多様なシステムの機器を運用管理ミドルウェアによって一元的に運用管理できるようになる．

3.オペレーショナルリスクの定義とその計量

3.1 オペレーショナルリスクの定義

オペレーショナルリスクの計量とは，企業内部の操作ミスやシステム障害，不正行為などの事象（損失事象）により企業が被る損失を，その企業のリスクとして評価することである．オペレーショナルリスクに該当する損失事象は，国際決済銀行(BIS: Bank for International Settlements)の Basel Committee on Banking Supervision（以下本報告では「バーゼル委員会」）において定められている[1]．その範囲は多岐にわたるが，そのうち下記が企業情報システムに関わる．

(1) 内部者の不正アクセス
(2) 外部者の不正アクセス
(3) システム障害
(4) オペレータの操作ミス
(5) システム保守運用管理者の操作ミス

バーゼル委員会では，上記(1)～(5)を含む損失事象が一金融機関で発生した結果，国際金融システム全体が不安定になるのを防止するため，各金融機関に自行のオペレーショナルリスクを計量させ，その結果に見合う自己資本を準備することを義務付ける規制を新 BIS 規制に盛り込もうとしている．規制の施行は 2006 年の予定であるが，予定通り施行されれば，少なくとも国際金融決済に携わる金融機関は，自行のオペレーショナルリスクの計量が義務付けられることになる．

3.2 オペレーショナルリスクの計量作業

オペレーショナルリスク計量は，大別して図 2 に示す４つの作業から成る[2]．いずれの作業も，運用管理コスト削減と人的作業による新たなエラーの可能性低減の観点から，自動化することが望まれている．運用管理ミドルウェアによりオペレーショナルリスク計量を自動化しようとする場合は，具体的には下記の作業の自動化を図らなくてはならない．

(1) 損失事象データの収集

オペレーショナルリスクに対応する損失事象を，内部データとして収集する．収集する損失事象データは，下記を含む必要がある．

- 発生日時
- 損失事象の種類

損失事象の種類については，種類の定義および分類方法がバーゼル委員会により提示される予定であり，現行の案が文献[1]に示されている．

手作業で行う場合は，損失事象データの収集は，損失事象の発生時点で事故報告書を作成して，データベース等に蓄積することによって行うのが普通である．

(2) 損失事象と損失額の対応付け

収集した損失事象データにつき，損失額を対応付ける．損失額は損失事象の発生現場で決定できる場合もあるが，多くの場合，本社または本店の担当者の審査により決定される．手作業で行う場合は，損失額の対応付けは，通常事故報告書の作成時に併記するか，損失事象の種類ごとに平均損失額をあらかじめ決めておき，個別の損失事象データに平均損失額を対応付ける．

(3) オペレーショナルリスクの計算

一定期間内に発生した損失事象と，損失事象のそれぞれに対応付けられた損失額から，オペレーショナルリスクを計算する．計算方法は，現時点ではいくつか提案されている段階[1]で未定であるが，新 BIS 規制の施行までに，バーゼル委員会によって制定される予定である．

(4) 収集した損失事象データの完全性の検証

(1)で収集した損失事象データが，一定期間内に企業内で発生した損失事象をすべて含んでいるか検証する．検証が必要なのは，収集した損失事象データに漏れがある場合，計量したオペレーショナルリスクが正確であることを外部に保証できなくなるためである．損失事象データの収集を手作業で行う場合，完全性を検証する確実な方法は現状なく，企業内の事故報告制度を整備することによりカバーするしかない．

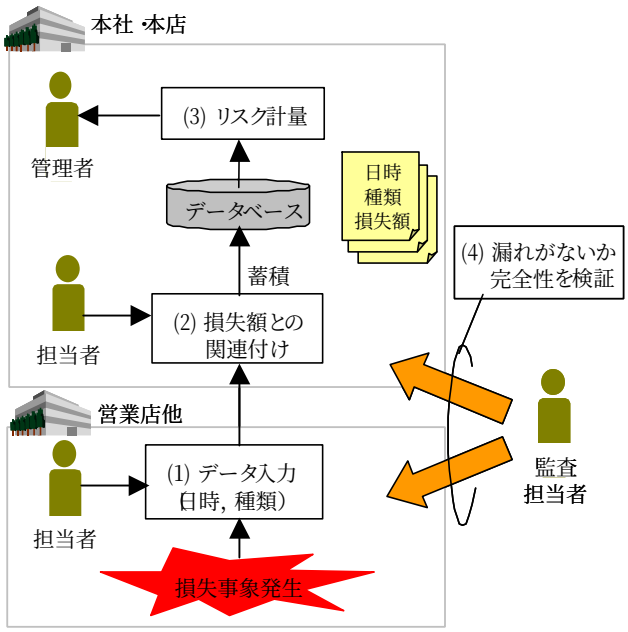

図 2 オペレーショナルリスク計量作業

4.運用管理ミドルウェアによるオペレーショナルリスク計量の自動化

4.1 オペレーショナルリスク計量の自動化方式の検討

3.2 節(1)～(4)から成るオペレーショナルリスク計量作業を，運用管理ミドルウェアにより自動化するための方式を検討した．本節ではその結果を述べる．

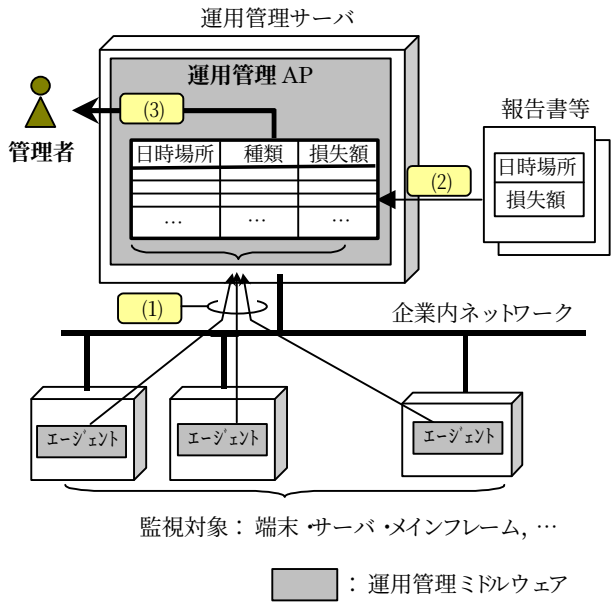

図 3 運用管理ミドルウェアによるオペレーショナルリスク計量の処理の流れ

標準的な企業情報システムの構成と，運用管理ミドルウェアを用いたオペレーショナルリスク計量の処理の流れを図 3 に示す. 図 3 において，企業内の機器（端末，サーバ，メインフレームなど）は企業内ネットワークに接続されており，企業内のエンドユーザはこれらの機器を操作することにより業務を遂行する．企業内ネットワークは，Ethernet などの標準的なネットワークを想定し，ファイアウォール等のセキュリティ技術により，企業外からは隔離されている．

また，図 3 において，運用管理ミドルウェアはエージェントおよび運用管理 AP から構成される．エージェントは企業情報システム内の監視対象となる端末，サーバ，メインフレーム等に配置されており，実行されているアプリケーションが出力するログやトレースを監視する．エージェントは，オペレータの操作ミス，システム障害，および不正アクセスの発生時には，アプリケーションがログまたはトレースに出力するエラーメッセージを検出し，エラーイベントを運用管理 AP に配送する．一方，運用管理 AP は，エージェントから配送されるエラーイベントを受信し，管理者の要求に応じてオペレーショナルリスクの計量を行う．

検討の結果，図 3 のような通常の構成の運用管理ミドルウェアにより，3.2 節(1)〜(3)のオペレーショナルリスク計量の作業は下記のように自動化することができるが，(4)は，通常の運用管理ミドルウェアの構成では，完全性を検証できないという問題があることが分かった. (1)〜(4)それぞれの作業につき，自動化の実現可能性を検討した結果を下記に示す．

(1) 損失事象データの収集

損失事象データの収集は，エージェントおよび運用管理 AP によって行うことができる．運用管理ミドルウェアの提供するエージェントは，自分の配置された機器内で発生したエラーを検出し，マネージャに送信する機能を持つため，その機能を利用すればよい．配送されるエラーイベントは，企業情報システムで実行されているアプリケーションによって異なるため，そのエラーイベントがどの損失事象に相当するか特定するのは，エラーイベントを受信した運用管理 AP 側で行う．

(2) 損失事象と損失額の関連付け

運用管理 AP が損失事象の種類を特定した後で，その損失事象と損失額を関連付ける必要がある．損失額は，企業情報システム内だけで特定できない場合が多いため，本作業の完全な自動化は困難と思われる．例えば下記の方法により解決できる．

- あらかじめ，損失事象の種類ごとに，損失額の平均値を決めておき，運用管理 AP に設定しておく．運用管理 AP は，損失事象の種類

を特定したら，入力された平均値を損失額として用いる．この方法では，作業は自動化されるが，損失額の誤差が避けられないため，外部(例えばバーゼル委員会)に対して計量結果の妥当性を示す必要がある．

- 運用管理 AP が損失事象の種類を特定した時点で管理者に連絡し，損失事象の発生場所を通知する．管理者は報告書等の調査を実施して，運用管理 AP のユーザインタフェースを用いて損失額を入力する．この場合，損失額の平均値を用いる方法に比べてより正確な損失額の入力が可能だが，一部管理者の手作業が必要となる．

(3) オペレーショナルリスクの計算

蓄積された損失事象データからオペレーショナルリスクを計算する作業は，運用管理 AP によって自動的に実行できる．計算式は，バーゼル委員会が制定する計算式を利用可能である．

(4) 収集事象の完全性の検証

図 3 のように，オペレーショナルリスク計量向けに運用管理 AP を設け，エージェントに各機器の障害を監視させるだけでは，収集した損失事象データに漏れがないことを検証することができない．具体的には，営業店などの現場で，エージェントの動作していない（またはエージェントが停止している）端末がネットワークに接続されている場合，その端末の操作ミスにより損失事象が発生すると，運用管理 AP にはイベントが配送されないため，損失事象データの収集から漏れてしまう．

本作業の自動化につき，解決策を検討した．次節に検討結果を示す．

4.2 完全性検証機能

本節では，収集事象の完全性検証機能(3.1 (4))の実装方式について検討した結果を述べる．以下，企業情報システムの構成は 4.1 節で述べた構成と同じである．

(1) アプローチ

エラーを監視するエージェントが，企業内ネットワークに接続されている計算機上で動作しているかどうかを調べる機能を設け，エージェントが動作していない計算機が存在しないことを検証できれば，収集事象の完全性を検証できる．そこで，企業内ネットワークのトラフィックを監視するミドルウェアを設け，もしエージェントの実行されていないマシンが企業内ネットワークを用いて通信を行った場合は検出する機能を実装すればよい（図 4）．

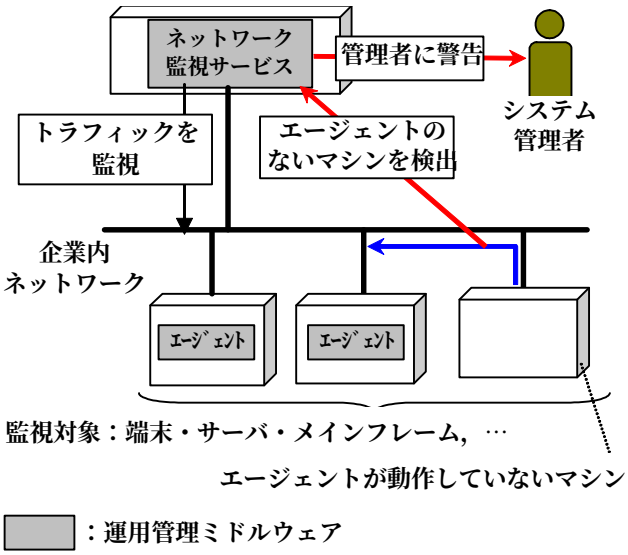

図 4 完全性検証機能のアプローチ

(2) 実装方式

エージェントが動作していない機器の検出方法を図 5 に示す．本方式では，ネットワーク監視サービスにおいて，下記の処理を実行する．

(1) ネットワーク監視サービスは，企業内ネットワークを流れるすべてのパケットを取得し，含まれる送信元および送信先の IP アドレスおよび送信先の MAC アドレス(Media Access Control アドレス)を読み出す．

(2) 次にネットワーク監視サービスは，取得したアドレスを検査済のアドレスのリストと照合する．検査済のアドレスのリストは，ネットワーク監視サービスが保持している．

(3) 取得したアドレスが検査済のアドレスのリストにないときは，ネットワーク監視サービスは，取得したアドレスに対応する機器上でエージェントが実行されていると仮定して，そのエージェントとの通信を試行する．

(4) 試行した通信が失敗したら，そのアドレスの機器上ではエージェントが動作していないと判定して，システム管理者に警告する．通信が成功したら，検査済のアドレスのリストにそのアドレスを追加する．

本方式のネットワーク監視サービスは，第２章で述べた運用管理アーキテクチャに基づく運用管理ミドルウェアであれば容易に実装できる．なぜなら，第２章の運用管理アーキテクチャにおいては，各機器で動作するエージェントは管理オブジェクトとして仮想化されるため，ネットワーク監視サービスは，エージェントとの通信を試行する際に，機器の種類を意識する必要がなく，取得した IP アドレスまたは MAC アドレスだけを用いてエージェントと通信を試行することができるからである．

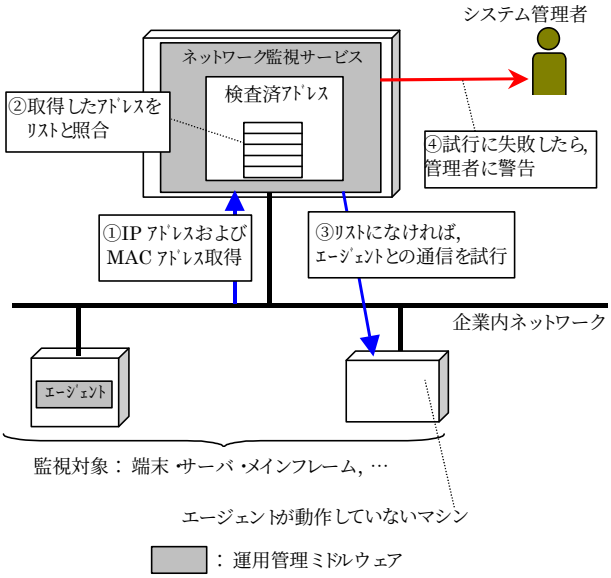

図 5 完全性検証方式の実装方法

5.おわりに

運用管理ミドルウェアによる運用管理コストの削減を目指したオペレーショナルリスクの計量作業の自動化方式と，その中で特に問題となる損失事象収集の完全性検証方式の検討結果につき説明した．今後，ネットワーク監視による完全性検証方式の性能評価を行い，効果を検証する予定である．

文　献

[1] Basel Committee on Banking Supervision, “Working Paper on the Regulatory Treatment of Operational Risk” (Electronic Version), http://www.bis.org/publ/bcbs_wp8.pdf, Sep. 2001

[2] 三菱信託銀行オペレーショナル・リスク研究会編，「オペレーショナル・リスクのすべて」，東洋経済新報社, 2002 年３月

[3] 久芳　靖，鞍掛稔也，尾山壯一，「Harmonious Computing を支えるミドルウェアへの取り組み」，日立評論, Vol. 85, No.7, pp. 519-522, 2003 年 7 月