

The Role of **Network Visibility**
in IT Operational
Risk Management
== IT 運用管理における
ネットワーク可視化の役割 ==



著者 **Dirk Paessler**

(訳 **ジュピターテクノロジー株式会社**)

目次

目次	2
経営者の皆様へ.....	3
運用リスクの分類.....	3
リスク分類.....	4
技術リスク	4
法的小よび人事リスク	4
自然あるいは人的災害	5
3 段階計画	5
ステップ1：リスト作成とビジネスコストに合わせたランク付け	5
ステップ2：価格低減	6
ステップ3：複数年計画.....	7
大きな展望：リスク低減とネットワーク	7
WiFi ネットワークは危険が多い	8
リスク管理と Paessler	9
PRTG ネットワークモニタ	9
SNMP ヘルパー	9
結論	9

経営者の皆様へ

生命には危険が満ちています。それが不可避であるならば賢者や賢明な組織は、それによるリスクを低減し、損失を管理するために必要な資源を投入します。

ビジネスにおけるリスク管理は保険と同義語です。IT においては特定の問題を決する技術的に焦点が当てられていましたが、事前の計画はあまり重視されていませんでした。そのような場当たりの問題解決は、所有資源の非有効活用という大きな欠点を抱えています。また IT では、2つのリスクのサブセットが注目されがちです。マルウェアとデータリカバリーです。そのため、注目されるべき他のリスクを見逃し勝ちでした(Gartner レポート”IT Risk Management: A Little Bit Moe Is a Whole Lot Better”)

一方、過剰なリスク管理は、他の投資すべき資源を、浪費しつくします。必要なのはバランスです。資源の配分においては最小のコストで最大のリスク低減できることが必要です。IT 運用リスク管理の多くの場面でネットワーク管理の重要性が無視されてきました。スイッチ故障や過負荷のような発生可能性の有るネットワーク問題を管理するためにネットワーク管理ソフトウェアに投資することには必然性があります。しかしビジネスネットワーク経由での不適切なダウンロードを発見し、ビジネス速度を最適化するためにネットワークトラフィックを分類し優先度をつけることも重要です。言い換えれば、0.1 秒の遅れが機会損失につながる世界では、これらは最優先の課題です。

IT が直面しているリスクの包括的で詳細な検証は www.isaca.org/CobiT の CobiT 4.1 で入手可能です。この論文では IT と特にネットワーク運用のリスクに焦点を当てています。全体の IT 運用リスク低減ストラテジーで、発見、分類、計画の 3 段階について説明しています。その過程でビジネスにとってはネットワーク監視がキープレイヤーであるとしています。

運用リスクの分類

悪いニュースですが、リスクをなくすることは不可能です。リスク管理の終着点は問題を明確にし、管理し、その影響をビジネスで許容できるレベルにまで下げることです。ビジネスを行うコストで受け入れられないリスクは、残ることになります。

中小企業では少し状況が異なっております。リスクを低減させる資源不足のため有る程度のリスクが残ることは覚悟しなければなりません。

望ましくないことですが中小 IT 組織は将来のあり方を考慮したリスク管理なしで、しばしば脅威ベースの対症療法を行います。ネットワークがもたらすウィルスは脅威です。そこで IT 担当者はアンチウィルスソフトウェアをインストールします。侵入が脅威になると、IT 担当者は外部からの侵入を防御するためにファイアウォールをインストールします。全てこのような調子です。

このアプローチは2つの重要な問題を含みます：

第一の問題は近視眼的であることです：全体のリスクポートフォリオ（通常技術的に解決可能）の一部だけに目をむけています。

第二に対応が小出しであり、受身であることです：その結果、それぞれの対策はその問題しか解決しないために、デバイスやサービスが増加し、集中管理ができず、“消火に追われる”ために、ITグループは先のことを考えることができません。一旦引き返しリスク計画を作成すべきです。

リスク分類

IT担当者は3種類の運用リスクに直面しています：

技術リスク

旧来のIT担当者が重視します。装置故障からネットワークによるウィルス、ワームそして斬新なDoS攻撃、侵入試行、建物外からの無線による不法アクセスまで広範囲です。

これらの問題の対処の多くは技術的に可能です。しかし明確なポリシーも重要です。ポータブルデバイスでは強力なファイアーウォールやアンチウィルスシステムを実行することはルール強制の例です。他の例は従業員が自分で管理できない、そして保護不可能なWiFiノードなどをインストールできない規則を作ることです。

強力なネットワーク監視ツール、たとえばPaessler PRTG ネットワークモニタなど、はネットワークの、通常とは異なる疑わしいアクティビティに対してすぐに警告を出しそのトラフィックの原因を特定できます。

法的および人事リスク

これらは法律遵守の問題です。訴訟に備えEメールを保存すること、従業員による不適切コンテンツのダウンロードが競合会社の訴訟対象にならないようにすること、従業員のサボタージュやスパイ活動を避けることなどを含みます。

これらの脅威は技術で明確な解決をもたらすことはできないため管理が困難です。

明確な人事政策と良好な管理がこれらのリスクを低減するキーです。

管理者は良い管理技術の訓練を受けるべきです。良い従業員は管理者に昇進し、良い管理者になる、という考えはよくある間違いです。

しかしネットワーク管理者はいくつかの可能性の有る問題を部下に提供できます。それらのいくつかはPaessler PRTGのようなツールで検知できます。これはネットワークトラフィックや帯域使用の分類などをリアルタイム監視できます。

自然あるいは人的災害

洪水、地震、嵐、これらはめったに発生しませんが、甚大な被害をもたらします。

これらのリスクを管理する適切なストラテジーを定義することはリスク管理でも、もっとも困難な仕事の一つです。

異なる価格で、異なる保護レベルの多数のストラテジーがあります。これらはビジネス全体の中で判断されるべきことです。

しかし災害管理は常識からスタートすべきです。

今日のネットワーク化された世界では、小規模組織であってもデータセンターを、災害多発地域から遠方で、近代的な、安全な建物（他の顧客と共有のことが多い）に設置できます。あるいは IT 機能をより安全な社外アウトソーシングや SaaS プロバイダーに委託することもできます。

繰り返しになりますが、Paessler 社から提供されるようなネットワーク管理ツールはこのようなリスク管理にとって重要です。どちらにせよネットワークの重要性は、顧客に IT サービスを提供する根本です。

3 段階計画

多数の小規模 IT 利用者は犯罪的なほど計画を作成しませんが、過剰なプランも避けなければなりません。中小利用者にとって、そして大規模利用者にとってもリスク管理計画は、変則的な升目を埋めるような仕事です。

ステップ1: リスト作成とビジネスコストに合わせたランク付け

この試みの第一ステップは各 3 カテゴリーの主要なリスクを見つけることです。

入手可能で最も完成度の高い標準リスク一覧は CobiT の IT ガバナンスフレームワークの一部です。しかしこれは IT 組織が望む範囲を大幅に逸脱している可能性があります。

各プロジェクトは、決して必要でない、またはほとんど必要でない、あるいは予算や計画が現実的でない可能性のあるものをたくさん含みます。

包括リスク表の作成に簡単ですが、ビジネスコストと重要性による順位付けは困難です。

リスク表は一般性がありますがビジネスコストは組織により大きく異なります。

たとえば金融トレーダーはトランザクション転送にわずかな遅延も許容しませんが、製造業は発注処理遅れは許容します、しかし ERP システムの処理速度は必要とします。これは各リスクの合計ビジネスコスト計算が困難なことを意味します。

計画立案者は経営者と相談し、同様なマーケットの他組織から業界やその仲間から提供さ

れる一般論を入手しがります。

その推測は正確である必要は無いですが、持っていることが重要です。それはリスク低減にどのくらい投資が必要かを決定する基礎になります。組織をウィルスやワームのような脅威から保護するために何に焦点をあてるかを決定しなければなりません。

しかし他にも計画作成にとって重要な質問があります。

他のリスクに比較しどのくらい費用がかかるか

その投資の結果を得るにはいつか

この質問に対する回答の一部は IT 関連の被害額です。

イベントの可能性を展望する必要があります。ウィルスはいつも問題になりますが、個々に見ると小さなコストで対応でき大きな混乱になりません。大災害の発生確率は小さいですが、ビジネスを壊滅させる可能性があります。

ステップ2: 価格低減

正確である必要はなく、提案要求文書を作成する必要もありません。インターネット検索や過去の経験による見積もりで十分です。計画作成者はコストにはスタッフの能力や時間も支払い金額と同様に含むことを認識する必要があります。多くの場合ハードウェアやソフトウェア購入とインストレーション費用を含むことは当然です。他の場合、特に災害リカバリーでは、採用する戦略は要求する効果と費用で大きく異なります。

組織にとっての最善の決定は各種要因に依存します：

長時間のダウンタイムに対する許容度

問題解決に利用できる資源

大災害を乗り越える能力

大災害後も生き残るには高額な費用を浪費するリモートサイドデータリカバリー(DR)が必要であり、小企業には対応できません。代案として、全ての会社にできることはテープバックアップやポルトストレージの利用であり、それが会社にとっての真の DR かどうかは別問題として、現実的な DR ソリューションです。しかし、もっと前向きのソリューションは SaaS プロバイダーの利用や DR アウトソーシングであり、これらは真剣に考慮する選択肢です。

計画作成者はリスクを低減するコストが予想される損失額より大きいことに気づくかもしれません。この場合そのリスク低減は投資価値がありません。

低減策を決定する場合は経営層が表明するリスクに対する相対的許容度を考慮しなければなりません。

ステップ3: 複数年計画

リスク低減には継続した努力が必要です。なぜなら可能な資源はニーズを満たすには不足することが多いため、複数年計画が必要です。リスクは時間とともに変化するため、いつでも新たな取り組みが必要です。

ウィルスのリスクはいつもあります。しかし実際のウィルスは変化します。その組織がリスクの処理のベテランであっても、油断してはいけません。

新たなリスク、例えば無線ネットワークなどはいつでも登場します。組織の新たな市場への参入や業務の変更、吸収合併などはリスクの基本を変化させます。

大きな展望: リスク低減とネットワーク

リスク管理計画作成者は、その対策による動作がネットワーク全体に、そして他の IT 計画にどのように影響するかを考慮しなければなりません。

リスク低減策でコスト以上に考慮すべきことは、社内サービスまたは外部契約で行うかということです。

しばしばその決定は、相対的なコスト比較、特定の知識や経験の有無、社内ポリシーによります。

しかし注意深い決定は、全体のリスク発見のあり方を見直す効果的な方法にもなります。業者はあるリスク、データリカバリーや DR、を上げますが企業はサービスレベルアグリーメント(SLA)やその合意が長期的には満たされないリスクには寛容です。もし IT 担当者がリスク低減のある領域でその投資を減らすことができれば、ビジネスが現在依存しているサービスを管理する投資ができます。

ネットワーク管理は重要なツールですがリスク低減にはあまり利用されていません。この技術は主要なネットワーク機器故障、自動切換えや交換などに関連しており、ネットワーク管理システムのインストレーションをおこなう明白で重要な理由です。しかしそれは他の領域のリスク管理にも間接的に利用できます。

ネットワークリスクに関係する一つの重要な領域はトラフィック過負荷によるデータ転送遅れです。

VoIP はこの遅れが致命的であり、VoIP を導入する場合は、トラフィック優先順位付けを確実にし、他のデータ転送が音声パケットに遅れが生じさせないようにしなければなりません。

他のアプリケーションでのデータ転送遅れが問題になることがあります。例えば、トランザクション転送の時間的な遅れは航空業界や、通貨、証券、消費者むけ物品の貿易に損失を与えます。

今日の高度に自動化されたリアルタイム工場では、データ転送のわずかな時間的な遅れが

生産ラインの遅延になり製造時損失につながります。JIT(Just-In-Time)環境の自動発注や出荷データの消失は致命的です。そこで多くの生産環境では、完全なネットワーク管理で重要データの遅れがないことだけで ROI を達成します。

良好なネットワーク管理はシステムのデータ混雑や他のシステム問題を明確にするために有効です。高度にモバイル環境が発達した今日では、管理者や多くの知識労働者はラップトップや他のデバイスを、社内ネットワークの保護範囲外に持ち運びますが、マルウェアを企業ファイアウォール内部に持ち込む危険をはらみます。

そのようなリスクの兆候の最初は大量のスパムや DoS メッセージを送信するゾンビの存在です。あるいは組織内に拡散するワームです。これらはネットワーク管理ツールではトラフィックのスパイクとして明確に捉えることができます。ネットワーク管理ツールは主要な問題の追跡ツールでもあり、その結果、原因であるシステムを停止させることも可能です。

WiFi ネットワークは危険が多い

多数のデバイスがネットワークに接続されている場合、ネットワーク管理が困難です。それらはアプリケーションとモバイルデバイスの互換性問題から、部外者や未承認デバイスからのネットワークアクセスまで広範です。

ネットワークはしばしば物理的な壁を越えることがありますが、この場合不特定多数からの攻撃に対する脆弱性ができ、企業アプリケーションやデータを道路や駐車場から盗聴される可能性があります。

WiFi モデムのネットワークへの接続は、驚くほど簡単です。ネットワーク管理者が無線モデムを企業のネットワークに接続すると、未承認 WiFi ネットワークがオフィスを徘徊していることをしばしば発見します。従業員が WiFi アクセスコントロール機能を有効にしないことは、部外者が会社のファイアウォールをバイパスするルートを開き、侵入あるいはマルウェアを拡散させる可能性を残します。

明確なネットワーク管理は IT 担当者が無線ネットワークのリスクを発見し、無線環境を完全な管理下におくことを可能にします。

ネットワークトラフィックをいつも監視することはビジネスデータタイプや量が劇的に変化している今日は、特に重要です。最近までは知識労働者にとってのデータは文字でしたが、今やグラフィックやデジタルオーディオ・ビデオが大量に加わりました。これらは文字データ用に構築されたネットワークでは容易に過負荷になります。本質的なビジネストラフィックと娯楽のため、あるいは悪質なものを区別することは非常に困難です。

YouTube のようなサイトもこのトラフィックの発生源の一つといえますが、多くはビジネスのためのものです。たとえばビジネスでは出張が、オフィスのスタジオや自分のデスクからの電話会議やテレビ会議で置き換えられました。その結果、多くの旅費削減、旅行時

間削減による生産性向上、従業員モラルアップなどをもたらしました。

このようなトラフィックの急激な増加は、ネットワークトラフィックスパイクのリスクを増加し、ネットワークサービスの低下をもたらします。Paessler PRTG のような良好なネットワーク管理ツールはネットワークデバイスの成長パターンを反映し、このようなリスクから保護する最前線のツールであり、ネットワークトラフィックの増大や、ネットワーク容量の計画のためのデータを提供します。

リスク管理と Paessler

Paessler 社は数種類のアプリケーションを提供しています。これらは中小企業ビジネスでネットワークの重要な要素を詳細に見るための完全なネットワーク監視に適していますが、もちろん大企業や超大企業でも使用可能です。他社製品と異なり、Paessler 社は最近全てのツールのアーキテクチャを変更しました。最適な技術をベースに機能と有効性と使いやすさを改善しました。

PRTG ネットワークモニタ

稼働監視、ネットワークトラフィック、使用率分類のための Windows アプリケーションです。Paessler 社の旧製品 IPCheck サーバー監視と、PRTG トラフィックグラフィックを一つの製品に統合しました。PRTG は重要なネットワーク資源を監視し、システム障害や性能問題を即座に検知し、停止時間や業務への悪影響を最小化します。ライブ監視と長期監視はネットワークデバイスの帯域使用やメモリー、CPU の使用率測定を行います。

SNMP ヘルパー

Windows サーバーやワークステーションの詳細な性能情報を収集するためのものです。数回のマウスクリックで数千のパラメータやパフォーマンスカウンターの監視が可能です。

各ツールは商用ライセンスとして提供されます。しかしフリーウェア版も用意されておりこれらは製品購入前に、その機能を確認するために使用できます。

結論

重要なことですが保障はありません。生命にはリスクがたくさんあり、どのような組織もそのリスクをある程度は受け入れなければなりません。リスク管理は悪いことが何も発生しないことを保障するものではありません。最高度に安全な環境においてさえも問題は発

生します。逆に言えば、リスク管理の目的はコスト面と生き残るという目的に対し受け入れ可能なレベルまでに、危険を減少させることです。IT 担当者がそれを管理できれば、リスク管理は成功したといえます。