

情報システム担当が選ぶ

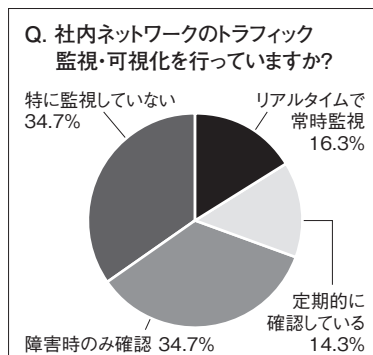
ネットワークインフラ

第6回

ネットワークの監視、7割が事後対応

ネットワーク障害や情報漏えいは、多くのケースで「起きてから気づく」ことになります。今回のアンケートによると、社内ネットワークをリアルタイムで常時監視している企業は16.3%にとどまり、約70%が「障害時のみ確認」または「特に監視していない」という結果でした。目に映らない通信は、対策を怠ると対応の遅れや被害拡大につながります。今回は、ネットワークの可視化と監視がなぜ重要なのかを、できる限りわかりやすく整理します。

図1 アンケート結果（回答数 49 票）



7割の企業が事後確認が未監視

●「社内ネットワークのトラフィック監視・可視化を行っていますか？」

今回のアンケートは、SNS上

で情報システム担当者を対象に実施し、49名から回答が寄せられました（図1）。

このアンケート結果で目を引くのは「障害時のみ確認」と「特に監視していない」が、いずれも34・7%で並んでいる点で、全体の約7割が、普段はネットワークの状態を継続的に把握できていないことになります。

一方で「リアルタイムで常時監視」と答えた企業は16・3%にとどまりました。裏を返せば8割強の企業が常時監視できていないことになります。

問題は、中小企業の現場において、これは別段珍しいことではな

株式会社ピーエスアイ
管理部広報担当

内藤 純一

URL <https://www.psi.co.jp>

E-mail support@psi.co.jp

いという現実です。多くの職場でネットワークは「つながっていて当たり前」で、メールが送れる、クラウドに入れる、Web会議ができるなど、そうした日常が続く限り、内部の通信状況まで意識する機会はありません。ただし、ここに落とし穴が存在します。

しかも、ネットワークの問題は完全停止だけではありません。

- ・通信が少し遅くなる
- ・特定の端末の外部通信が増える
- ・負荷が高まる時間帯が不自然

などの変化は、障害の発生前や攻撃の進行中に現れる場合があります、監視・可視化していないと変化に気づくことができないのです。

なお、今回の調査はSNS上で実施した49名へのアンケートであるため、回答者の企業規模や業種には一定の偏りがある可能性があります。

とはいえ「監視は重要だとわかつていても、継続的に監視している企業はまだ少ない」という傾向を示す材料にはなりません。

ネットワークの

「監視・可視化」の重要性

●原因の切り分けと対応判断

「監視・可視化」と聞くと、専門の監視センターや大企業向けのしくみを思い浮かべる方もいるかもしれませんが、本質はいたって単純で、まずは社内ですぐ「どこが、どれくらい、どこと通信しているのか」を把握できる状態にすることが出発点になります。

例えば、道路管理であれば「どこで渋滞しているのか、どこに車が集まっているのか、どこで事故が起きているのか」がわからなければ、対策の打ちようがありません。

ネットワークも同じで「どの回線が混んでいるのか、どの機器に通信が集中しているのか、いつもと違う動きがあるのか」が見えていなければ、原因の切り分けや対応への判断も遅れます。

しかも、ネットワークは社員のパソコンだけで成り立っているわけではありません。クラウドサー

ビス、Web会議、無線LAN、複合機、監視カメラ、入退室管理、各種IoT機器まで、多くの機器が同じ基盤につながっており、どこかひとつで起きた不具合や不審な通信が、思った以上に広い範囲へ影響することもあります。

ここで注意すべきは、仮に異常な通信量や通信先が見つかったとしても、それだけで「攻撃」と直ちに断定できない点です。新しいクラウドサービスの導入やバックアップ処理、ソフトウェア更新など、正当な業務通信である可能性も否定できないからです。

●変化を数字と記録で確認

だからこそ「監視」は、断定的なためというより、調査すべき変化に早く気づくためのしくみとして考えるのが適切です。

通信障害のシーンも同じで、利用者の体感では「今日は少し遅い」としか感じなくても、裏で特定の回線が飽和状態になっていた、機器のエラーが増加していた、ということがあります。感覚だけでは

曖昧だったものを、数字と記録で確認できるようにする。それが「可視化」の価値です。

NIST（米国立標準技術研究所）の「NISTSP800-137」でも、継続的監視は、資産や脅威、脆弱性、セキュリティ対策の有効性を把握するための取り組みとされています。

可視化で見る3要素

●実際に何を見ればよいのか

最初からすべての通信を細かく理解しようとすると難しくなりがちなので、中小企業においては、以下の3要素に分けて整理します。

- ① 機器の状態
- ② 通信の流れ
- ③ イベントの記録

① 機器の状態
ここでは「SNMP※1」というしくみがよく使われます。これはネットワーク機器の状態情報を取得するための管理方式で、例えば

「スイッチやルーターのポートが生きているか、通信量がどの程度か、エラーが増えているか、CPUやメモリに無理がかかっているか」などの、情報を確認できます。つまり、機器の「体温」や「脈拍」を見るようなものです。

L2（データリンク層）の観点では、ポートの稼働状況、VLANの状態、エラーや廃棄パケットの増加などが手掛かりになります。

② 通信の流れ

ここでは、
「NetFlow※2」
「IPFIX※3（フロー情報）」
「sFlow※4（パケットやカウンターのサンプリング情報）」
などが利用され、これにより送信元や宛先、通信量、時間帯、利用されたポートなどを把握できます。通信の中身をすべて読むのではなく「どの道路に、どの車が、どれだけ流れているか」を見るイメージです。

L3・L4（ネットワーク層・トランスポート層）の観点では、送信

※1 SNMP（Simple Network Management Protocol）：ネットワークにつながるルーターやサーバーなどの機器を監視・管理するための通信ルールです。
※2 NetFlow（ネットワークフロー）：Cisco社が開発したネットワークの通信トラフィックを監視・分析するための技術です。
※3 IPFIX（IP Flow Information Export）：ネットワーク上を流れる通信データ（IPフロー）を監視・分析するための標準プロトコルです。
※4 sFlow（エスフロー）：ネットワーク機器（ルーターやスイッチなど）を流れるトラフィックを監視するための技術です。

元・宛先IPアドレス、ポート、セッションの傾向や通信量などを把握できます。

③ イベントの記録

ここでは「Syslog^{※5}」が代表的です。「機器の起動、設定変更、認証失敗、リンク断、警告メッセージ」など、ネットワーク機器やサーバーが発した出来事を記録します。

さらに、アプリケーション識別に対応した機器や分析製品を利用すれば、どのアプリケーションやクラウドサービスが使われているかを把握できる場合があります。SIEM^{※6}やNDR^{※7}は、こうした複数のログや通信情報を横断的に分析し、異常の兆候を見つけるためのしくみとして位置づけるとわかりやすいです。

以上の3要素は、別々のものではありません。機器の状態、通信の流れ、イベントの記録を組み合わせて「なぜ遅いのか」「どこが怪しいのか」を多面的に見ら

れるようになります。

ネットワークベンダーの視点でいえば、可視化とは単にグラフを並べるのではなく、複数の情報をつないで現場判断をしやすくすることであり、IPFIXは、トラフィックフロー情報を標準的に転送するための仕様として定義されています。

「ログ」と「監視」は 何が違うのか

● ログは材料、監視は仕掛け

可視化の話になると「ログ（記録）を取っていれば十分だ」と考える方もいます。確かにログは重要ですが、何が起きたかを後から確認するには、記録がなければ始まりません。以下のようにログと監視は同じものではありません。

ログ…機器やシステムで発生した出来事を残す記録

監視…ログや通信情報を継続的に評価し、異常やしきい値超過を検知した際に通知するしくみと運用

つまり、ログは「材料」、監視はそれを使って気づく「仕掛け」と考えればわかりやすいでしょう。例えば、深夜に普段見られない外部通信が発生したとします。

ログだけなら、翌日調べた際に初めて気づくかもしれません。しかし、監視のしくみがあれば、その時点で「いつもと違う通信が起きている」と把握できる可能性があります。障害対応でも同じで、普段より回線使用率が急上昇した瞬間に通知が来れば、利用者からの問い合わせを待つ前に状況を確認することができず。

もちろん、ログは事後調査だけに使うものではありません。現在ではSIEMなどにリアルタイムで集約し、異常検知に活用する運用も一般的です。NISTのログ管理ガイド「SP800-92」でも、ログはインシデントの特定や調査、運用上の問題発見に活用できる重要な記録として扱われています。

大切なのは「記録している」と「気づける」は、別だと理解することです。異常の早期発見を目的

とする場合、ログを残すだけではなく、その内容を継続的に見て、変化を判断し、必要に応じて知らせるしくみが求められます。

ログの保存自体は、法令対応や監査、事後調査の側面からも重要ですが、監視までつなげて初めて日々の運用改善や初動対応に生きてきます。

ネットワークの監視が 続かない理由

● 運用改善の材料として使う

現場で監視が定着しにくい理由は、技術の問題だけではなく、むしろ多いのは「見えるようにはしたが、運用が続かない」というケースです。

代表的なのは、通知が多すぎる問題です。監視のしくみを入れた直後は、少しでも異常を見逃したくないという思いから、あらゆる通知を有効にしがちです。

しかし、毎日のように大量のアラートが届くと、現場では次第に見なくなってしまうです。これで

※5 Syslog（シスログ）：サーバーやネットワーク機器が自身の動作状況やエラー発生の記録（ログ）を収集・一元管理するための規格・プロトコルです。

※6 SIEM（Security Information and Event Management）：ファイアウォールやサーバーなど、ネットワーク上のさまざまなIT機器からログデータを一元的に収集し、それらを分析してセキュリティ上の脅威をいち早く検知・通知するシステムです。

※7 NDR（Network Detection and Response）：ネットワーク上の通信トラフィックをリアルタイムで監視し、サイバー攻撃や異常な挙動をAIなどで検知・遮断するセキュリティ対策です。

は、肝心の重大な異常も埋もれてしまします。

逆に、通知を減らしすぎると、本当に気づくべき変化を見逃します。大切なのは、業務実態に合わせて「即時通知するもの」と「設定日時にまとめて確認するもの」を分けることです。

例えば「重要機器の停止や回線断は即時通知」「通信量の増加やエラーの傾向は日次確認」といった設計にすると、無理なく続けやすくなります。

また、監視結果を「担当者だけが知っている情報」にしないことも重要です。障害時に誰へ連絡するのか、どこまでを社内で判断し、どこから外部ベンダーへ相談するのかを整理しておく、初動が速くなります。

月に一度でもアラートの件数や傾向を振り返れば「同じ場所でも何度も負荷が高まっている」「特定の曜日だけ通信が増えている」といったパターンにも気づきやすくなります。

つまり監視は、障害発生時だけ

のしくみではなく、日々の運用を少しずつ良くしていくための材料として使うことが大切なのです。

ポイントを絞って 小さく始める監視

●異常な通信量を把握する

では、どこから始めればいいのか。中小企業では完璧を目指すよりも、止まると困る場所から小さく始めてください。

例えば「本社のインターネット回線、基幹スイッチ、主要サーバー、ファイアウォール、無線LANの中核機器」など、業務影響の大きいポイントに絞って可視化するだけでも効果があります。

すべての端末やすべての通信を一度に見る必要はありません。重要な場所の利用率やエラー、異常な通信量を把握できる状態をつくるのが第一歩です。

次に大切なのは、正常の姿を知ることです。「どの時間帯に負荷が高まるのか、月末や朝礼前に偏りがあるのか、クラウド利用が増

える時間はいつか」などの傾向がわかると、異常が見つけやすくなります。監視は、異常を見るだけではなく「普段通り」を知るための取り組みでもあります。

さらに、監視対象を社内だけにしてしまう思考が、見落としを生ぜさせます。今日、多くの業務がクラウドサービス上で動いています。利用者の体感としては社内ネットワークの問題に見えても、実際には「ルーターなどのインターネット出口の混雑、DNS応答、認証基盤とのやり取り」などが影響している場合があります。

特に、Web会議やSaaS（ネット経由で利用するソフトウェア）では、わずかな不調でも利用者は「全部遅い」と感じます。だからこそ、社内機器の状態だけではなく、インターネット出口や主要クラウドへの接続状況もあわせて見ておくと、障害時の切り分けがとてスムーズになります。

監視は原因を決めつけるためではなく、確認すべき範囲を早く絞り込むための手掛かりでもあるの

です。

また、監視とは、誰かが一日中モニターを見続けることではありません。「一定のしきい値を超えたときだけ通知する、毎朝ひと目で状態を確認する、週に一度だけ傾向を見る」などの運用でも、何も見えていない状態よりは大きく前進します。こうした小さな取り組みから、ネットワーク運用の一定の改善が期待できます。

【まとめ】

可視化や監視の目的は、異常に早く気づき、判断し、必要であれば動けるようにすることです。

まずは、重要な回線や機器を「見える化」する。それだけでも障害やセキュリティ対応において質の改善となり、早く気づくことで被害抑制の可能性も高まります。

ネットワークは、普段は目立たない存在です。だからこそ「見えるようにしておく」ことに価値があります。監視とは、何かを疑うためだけではなく、業務を止めないための備えなのです。