## 3.31 障害対策マニュアルに関する教訓（T31）

### 教訓 T31　復旧手順は、システムとその環境の変化に対応させ常に最新に！

### 問題

A社では、各工場に置かれた制御装置を専用回線でつないだネットワークを構築していた。

ある日の早朝、A社の制御装置の稼働状況が集中監視センターから確認できなくなった。

監視センターの監視員が原因を調査したところ、ネットワーク障害が発生していることが判明した。その後センターのルータが故障していることが判明し、そのルータの交換を行い、昼頃ネットワークを再度立ち上げた。

その後、監視員は、障害対策マニュアルに従い、稼働再開のため「全リセット」機能（各制御装置の障害復旧後に障害時の仕掛中の稼働情報をリセット）を実行した（図 3.31－1①）。しかし、正常に作動せず、さらに制御装置のいくつかがハングアップ状態となり、復旧が大幅に遅れた。

制御装置には新型機種と旧型機種が混在していたが、障害となったのは旧型の制御装置であった（図 3.31－1②）。

そこで監視員は現地に赴き、ハングアップ状態の旧機種の制御装置に対して1台ごとに再立ち上げ（リセット）を実施した（図 3.31－1③④）。

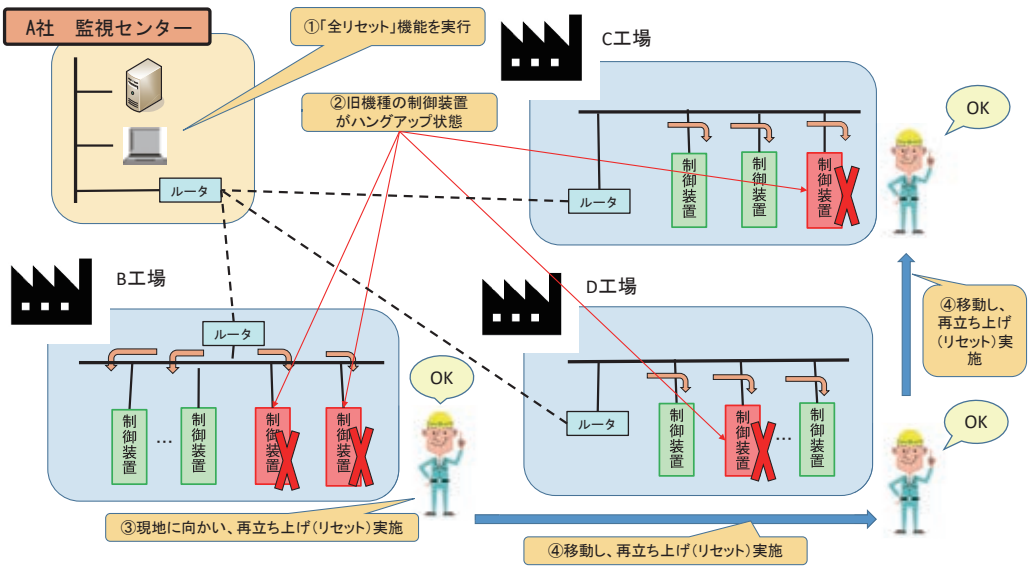


図 3.31－1　障害状況

## 原因

直接原因は、障害対策マニュアルの記述が曖昧であり、本来使用する必要がなかった機能を実行したことであった。

監視員は、障害対策マニュアルにしたがって一連の操作を行った。マニュアルの手順では、「全リセット」機能を使用するようになっていたが、この機能は、今回のようなすべての制御装置が正常に停止した場合には使う必要がなく、ネットワーク復旧後には、通常の立ち上げ時に行っている制御装置への「稼働開始」機能を実行すればよかった。また、「全リセット」機能は、システムの初期リリース時に保守用として作られて以来、全く使われておらず、その後の制御データの増大にともなっても、システム拡張や機能追加時にもテストされていない機能であった。当然、データ量増大時の旧型制御装置の動作性能への影響についても十分な確認テストが行われていなかった。

根本原因は、本来使用すべきでない機能が障害復旧手順として障害対策マニュアルに記載されており、そのような誤った記述のマニュアルが更新されずに放っておかれたことによるものであった。

システム障害の原因がすぐに突き止められ、その原因から復旧の道筋が明確になった場合の復旧作業は、ある意味簡単であろう。しかし、今回のように当初原因が分からず、その原因をつかむのに時間がかった場合や、想定していなかった障害の場合、その復旧手順は複雑になり、従来のマニュアルの手順ではうまくいかない事態が発生する。

まとめると、以下のような課題が存在した。

**⑴ 今までにない（想定されない）事象が起きた場合のマニュアルやオペレーションの在り方**

- 二次障害を回避するオペレーションはあったのか
- オペレータは常にマニュアルに従うべきか

**⑵「滅多に使わない機能」の管理、運用方法**

- その機能は，オペレーションマニュアルでどのように扱うべきか
- その機能は、事前に，どこまでテストされるべきであるか

このような課題に対して、関係者が集まって議論することが必要であった。

## 対策

システム障害対策マニュアルは、障害発生時に原因をどう突き止めるか、そこからどのように復旧するかをまとめている。

今回のシステム障害は、その頼るべきマニュアルが、障害時に使える記述になっていなく、また内容も管理されていなかったので、A 社では、「障害復旧改善に向けた障害対策の最新化する運用」を設定することにした（図 3.31－2）。

具体的には、障害対策マニュアルを常に最新版の状態に保てるように、障害対策マニュアルを維持

管理する運用ルールを定め、実践していく体制を作った。

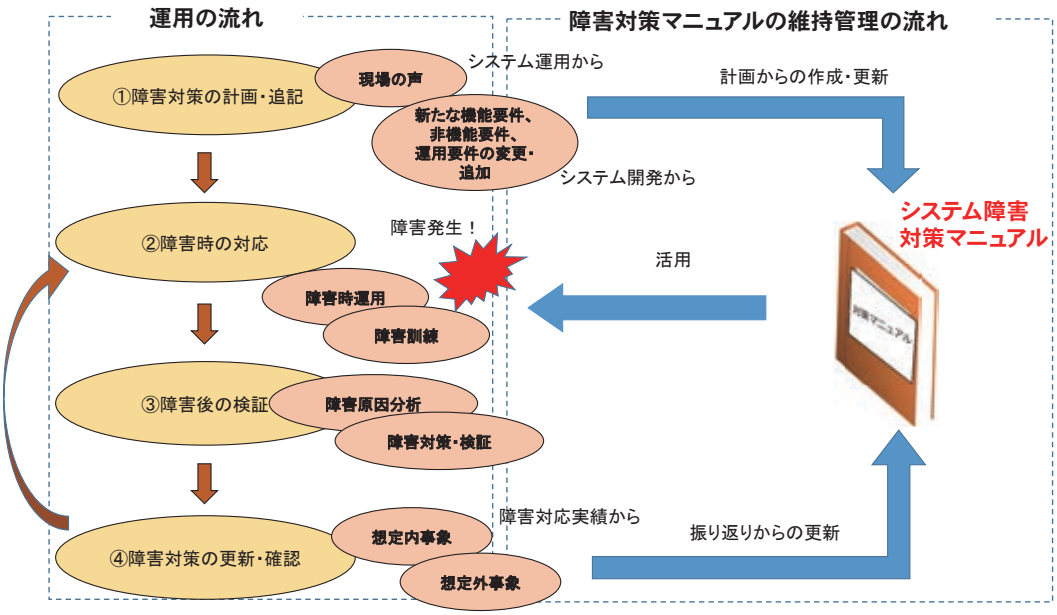


図 3.31－2　運用と障害対策マニュアルの維持管理の流れ

### ⑴ 障害対策の計画・追記

- 障害対策は、障害時に障害対策マニュアルのどこを見れば良いか、どこから作業を行えば良いか、どの手順（フローチャート）で行えば良いか、が担当者にすぐにわかるものとする。
- そのためにも、現場の声を聴き、現場の声を反映させる障害対策マニュアルとする。
- 障害対策マニュアルが正確であることを確認する、検証、障害訓練を計画する。

### ⑵ 障害時の対応

- 障害対策マニュアル通りに実行する。復旧しなかった場合は、エスカレーションを実行する。
- その対応が，障害対策マニュアルの手順通りにできたかどうか記録する。
- 障害対策マニュアルにない想定外の事象にどう対処したか記録する。

### ⑶ 障害後の検証

以下の観点などを検証する。

- その対応は、正しい行動だったのか
- 障害対策マニュアルにない行動だった場合、なぜそのように行動したのか
- その対応がマニュアル通りとしても、正しい行動だったのか
- その機能が事前にどこまでテストされていたのか

### ⑷ 障害対策の更新・確認

- 新たな障害に対応した後に、その際に実施した対策を追加する場合は、手順が明確になっている「想定する事象への対応」と、万が一、手順通りにいかなかった場合の「想定外の事象への対応」の両方についてのフローを障害対策マニュアルに記述し、システム障害時の対応を検証する。

  「想定外の事象対応」を記述することは、例えば「想定外の事象」が起きた場合は、緊急対策本部を立て、関係者にすぐ連絡する、お客様対応部門への連絡、などの危機管理対応を障害対策マニュアルに明記することを指す。
- 制御データ量の増大、新規機能追加、機能変更が発生した場合についても、同様に、「想定する事象対応」と「想定外の事象対応」の両方について、障害対策マニュアルに記述し、そのマニュアル通りにシステムが復旧することを検証する。

## 効果

A社は、今回のネットワーク障害時における稼働再開までの手順とマニュアルの見直しを行い、常にマニュアルを中心にした、システム運用を開始した。それにより、以下の効果が生まれた。

a) システム運用と、障害対策マニュアルを関連付けながら行うので、システム障害対策が運用の中心として位置づけられるようになり、障害対策マニュアルが置き去りになる事態を防ぐことができた。

b)「機能の解説」から「障害対策」を中心とした障害対策マニュアルへ修正したことにより、障害対応の手順（フローチャート）を明確にすることができた。具体的には、以下のような効果が表れた。

- 障害時は、マニュアルのフローにしたがって実施できるようになり、手順も確認しやすくなった。
- 新たな障害パターンについての追加記述も関係者の合意を取りながら行えるようになった。
- 監視員の対応が明確になった。
- 障害対策の訓練や教育が、マニュアルを中心に行うことができるようになった。
- 障害発生時に連絡すべき関係者が明確になった。

## 教訓

システム障害対策マニュアルは、どのシステム部門も管理しているが、システムを取り巻く環境の変化やシステム更改に合わせたマニュアルの更新が追いつかず、後回しにされる場合もよくある。そのため、いざ障害が発生しても、マニュアル通りに行うことを躊躇して対応が遅れたり、いざ行うと当該事例のような二次的障害を引き起こしてしまったりと、システム障害の影響範囲を拡大してしまう。

この教訓は、「システム障害対策マニュアルは常にシステム運用の中心として管理すべきもの」であり、そのためには、「システム障害対策マニュアルは、常に最新にしていくべきこと」を教えてくれる。