CISO STRATEGY

企業のリスクをマネージする戦略考

さまざまなトラブルによって引き起こされる被害。被害を受けてから、通常の状態に復旧させる作業には、単なる機能復旧だけではなく、トラブルの再発防止対策が求められる。
被害からの復旧はさまざまな技術を総動員する場面でもある。
復旧作業において私たちは何を考えるべきなのか。

最終回 **被害からの復旧**

text : 山口英 奈良先端科学技術大学院大学情報科学研究科教授

2つの選択：復旧か調査か

セキュリティー管理作業の中で一番頭を悩ませることは、トラブルが発生したときに、どのように解決して決着をつけるのかという道筋を組み立てていくことである。結論から言えば、この問題には単純な解決方法はないのである。それぞれの状況に応じて対応するしかない。なぜならば、この問題は拮抗する2つの要求を満足させつつトラブルを解決しなければならないという構造があるからだ。

2つの要求とは、「サービスの迅速な復旧」と「トラブルを引き起こした原因の解明」である。このどちらを優先させるのか、あるいは、どちらに重きを置いて作業をするのかで、実際の復旧のプロセスが大きく変わってしまう。

現在、私たちが使っている情報通信システムは数年前とは大きく様変わりし、業務に密接に連携するシステムとして、多種多様な業務に深く組み込まれている。情報通信システムが研究開発部門に限定的に使われているケースは、現在ではほぼ皆無であろう。たとえば、電子メールサービスが業務時間内に午前中3時間ほど止まっただけで、その日の仕事の段取りが立てられなくなるような環境で作業をしている人も数多くいるだろう（当然筆者もその1人である）。

トラブルが発生すれば、多くのユーザーに甚大なインパクトを与えるというのが、現在の情報通信システムの真の姿である。このため、システムにトラブルが発生すると、迅速に復旧させてサービスを再び提供することが強く求められる。また復旧までの時間がかかればかかるほど、経済的な損失が大きくなるというのも通常の考え方だ。

その一方で、復旧を迅速にすればするほど、失うものも出てくる。それは、なぜトラブルが発生したのかという「トラブル発生原因」を探る活動を円滑に行うための環境である。原因調査の視点から考えれば、何が起こったかを知るためには、トラブル発生時点での状況を保全し、トラブル発生状況などの情報収集を十分かつ円滑に行うことが必須である。このため、復旧作業によって状況保全が壊されるようなことはできる限り避けたいと考えるのは当然なのである。

また、保険の適用を受ける場合、あるいは、司法当局に対して告発を行う必要があるような場合には、かなり徹底した情報収集を行って、事後対応を滞りなく行えるようにすることが求められる。このような理由から、復旧作業を休止させてでも、状況情報を収集することが必要な場合も多い。ただし、復旧作業を休止し続ければ、経済的な損害が大きくなることは前述のとおりである。

したがって、この2つの要求をうまく折り合いを付けながら復旧の実作業に取り組まなければならない。当然だが、発生したトラブルの規模や内容によって、折り合いの付け方は変化するので、この問題を片づけるための特効薬はなく、それぞれの状況に応じて判断しなければならない。しかし、この問題をもっとうまく解決するための工夫はある。

二重化と演習で復旧を支えよ

トラブルが発生し、ユーザーからのサービス再開要求の「圧力」に迅速に応えるとはいっても、慌てて復旧作業をすることなく、かつ原因調査を並行して進められる環境を作ることはできないのだろ

うか。

たとえば、システムの二重化を行い、片方のシステムがダウンしたとしても、直ちに他方のシステムで継続できるようなサービスを提供する構造を組み立てることは可能である。確かに処理能力は半減するかもしれないが、サービスを引き続き提供できるので、ユーザーからの不満はかなり抑えることができるだろう。しかも、トラブルを引き起こしたシステムの復旧作業と調査作業のための時間的な余裕を得ることも同時に可能となる。

システムの二重化は、サービス停止を引き起こす確率を少なくするだけではなく、トラブル対応のための時間稼ぎをするための機構とも捉えることができる。このようなサービスを構築するときに、同時にシステムも二重化することでトラブル対応について考慮された構造にすることも、システム管理のうえで大きな効果が期待できるのだ。

また、トラブル発生時の原因解析のための情報収集を、システムのバックアップ作業と同時に行っておくということも考えてもよいだろう。たとえば、主要なサービスのログはバックアップ作業時に同時に記録するようにするとか、システムの稼働状況を確認するための情報を同時に収集しておくというようなことも効果が高い。あるいは、従来のUNIXシステムでのアカウンティングシステムのように、「誰が」「いつ」「どのような」プロセスを立ち上げて、どのようなファイルに対してアクセスしたのかといった情報を効率よく収集する機構を有効にしておく、ということも考えられるだろう。このように、日常的に情報収集する体制づくりも重要だ。

また、実際にトラブル発生を想定して、予行演習を行うのも悪くないアイデアだ。予行演習をするためには、いろいろな人たちが巻き込まれるトラブルを仮定し、その対応手順を考えてみることから始まる。そして、実際にその対応手順どおりに作業を進めていくと、意外とその手順が機能しないことが判明したり、あるいは人員不足が露呈したりすることが多い。

予行演習そのものは、具体的なトラブルに対応するための準備ということも考えられるが、それ以上に「トラブルへの対応に携わる人たちの間での意識の摺り合わせ」や「その手順に対する勘所を得ること」につながるので、どんな組織でも一度はやったほうがよい。

また、複数回実行できるチャンスがあるのであれば、同じシナリオに基づいた演習を繰り返すのではなく、異なる側面からの評価が可能な別の演習を行うことのほうが役立つだろう。というのも、もともと想定できるトラブルに対して同じ対策を何度も演習することは、対応の精緻化にはつながるだろうが、実際のトラブルへの対応能力が改善されるわけではない。つまり、トラブルというのは、元来想定してなかった原因から発生することが多いのが常だからである。

もしも想定していたトラブルであれば、確実に行える対応への準備ができるはずで、大きなトラブルが発生することは稀になるはずである。また、ルーチン作業の中で処理できるようになっていてしかるべきである。

この意味でも、創意工夫に富んだ、毎回異なる演習を行うことで、トラブル対応への基礎体力作りを進めるという目的を持つことが重要だろう。

戦略1

トラブルからの復旧作業では、サービス再開のための復旧作業と、原因究明のための情報収集を両立させる必要がある。そのためにも、日頃から情報収集基盤を作り、システムの二重化で復旧に使える時間を稼ぎ、さらにはトラブル対応の演習を行うことで復旧作業の円滑化を図ることが重要である。

現場監督の「悩み」の解決策

復旧作業では、作業に携わる人の作業権限が確保されているかどうかということは十分に考えなければならない。

大規模なシステムがダウンしたときに、そのシステムを復旧させるためにいくつもの作業をうまく優先順位を付けて作業していかなければならないことが多い。そして、多くの場合、ユーザーが望むサービスを再開するためには、関連するほかの作業を先に行わなければならない。このようなときに、復旧作業にあたる現場責任者が十分な意思決定権限を持ち、現場責任者が考える最良の手順で作業が遂行されるべきである。同時に、周りから責任者に持ち込まれるクレームや雑多な情報といった「雑音」をうまく取り扱うことや、復旧作業をより迅速にしろというような「圧力」、さらには、現場責任者が望まない形での復旧作業や原因調査作業への「介入」を排除することも大切だ。同時に、周りも現場責任者が誰で、誰が作業全体を率いているかについて正しく知っておくことも必須だ。

復旧作業では、その作業の順番や進め方はそれぞれの状況ごとに考えなければならない。その作業の決定方法についても、トラブルが生み出した影響と、トラブルを解決する手順の複雑さとの両方を勘案しながら作業を進める必要がある。すなわち、実際にトラブルの発生現場をしっかりと見ることができる立場のスタッフだけが、復旧作業で発生する問題を解決できる立場にいることになる。これを考えれば、トラブルの発生現場を掌握している現場監督に対して、トラブルからの復旧作業すべてを担当できるための権限委譲が行われてこそ、迅速な復旧活動が可能になるだろう。

ところが、この権限委譲をきちんとしないまま復旧作業に入ってしまう組織も多

い。このような場合、現場スタッフは何かしようとしても、常に名目上の責任者に対して確認と作業遂行の承認、さらには定期的な報告などが必要になってしまう。このことは単に復旧作業を遅らせるだけであり、実質的には、復旧作業を助けることはほとんどない。

戦略2 復旧作業にあたる現場責任者には、全権委任型の権限委譲を行うことが大切だ。特に必要な作業が現場で判断できないような状況では、円滑な復旧作業も不可能に近い。

権限とモラルのバランスを保て

もう1つ考えなければならないのが、復旧に携わる現場責任者は、同時に組織内の人間に対する調査を行わなければならいこともあるということだ。「トラブル発生の犯人は誰か」「トラブルの原因は何にあるのか」「どのようなことを改善しなければならないのか」という問題を解決しながら、復旧作業を遂行することになってしまうのだ。特にトラブルを引き起こしたのが内部の人間であると、往々にして復旧作業は同時に犯人探しにもなってしまう。このため、トラブルが発生した部署でいろいろと調査しようとしても、その調査が「明に」「暗に」内部者によって妨害されたり、非協力的な態度をとられたりすることは日常茶飯事である。

このような状況を乗り越え、実質的な作業を進めていくためには、現場責任者がどれだけの権限を持つのかが成否を分ける鍵を握っていることになる。

権限委譲をバックに復旧作業をするとはいえ、同時に復旧作業責任者には高いモラルも要求される。偏りのない合理性を持った原因究明活動とならなければ、ユーザーは面倒なことに巻き込まれるのを避けようと非協力的になる。これは当然のことだ。この意味で、復旧作業の現場責任者は本当に悩み多き作業を貫徹しなければならない。

現場責任者への権限委譲は、復旧作業の加速材である。さらに現場責任者が高いモラルを維持しながら合理的な作業をすることは、原因調査のための触媒となることを肝に銘じておかねばならない。

戦略3 復旧作業の現場責任者は、トラブル発生の原因究明に必須である関係者の協力を得るために、自らの活動において高いモラルを維持し、同時に合理的な作業と判断を行うことに努力しなければならない。

事後調査にも十分に力を注げ

トラブルが発生すると、どうしても復旧作業だけに注力し、トラブルを食い止めてサービスを再開できただけで満足してしまうケースが多い。

システム運用に直接携わるオペレーターの場合には、それでもよいだろう。しかし、復旧作業責任者としては、それだけで終わらせてはならない。最終的にトラブルとその復旧作業は何であったのかを明らかにする事後調査の作業を完了させる必要がある。

第一に、どのようなトラブルに対しても原因解明の努力を怠ってはならない。

原因解明を尽くしてない段階では、復旧作業は完了していないかもしれないのだ。実際の話だが、あるウェブサイトでシステムがダウンしてファイルのいくつかがなくなってしまっていたという事故があった。復旧作業者は、単純にバックアップテープからファイルを書き戻し、そのまま運用を再開した。このトラブルは根が深く、システムに仕込まれたワーム（Worm）がせっせとファイルを消していく作業の途中でシステムがダウンしただけだったのだ。したがって、システムを再起動させても再びワームが仕込まれ、システムがダウンするということを繰り返した。

原因を突き止めていれば、バックアップから書き戻すだけではなく、さらにワームの侵入を許してしまったセキュリティーホールを潰すことも必要であったことが、復旧責任者にはわかったに違いない。このように、単純にサービスを再開させても復旧作業は終わりではない。原因を突き止めて、行った復旧作業は原因と照らし合わせて妥当性があるかどうかを考えなければならないのだ。

第二に、復旧作業の費用を常に考えなければならない。

トラブルが発生した場合に、もしも事前に適切な投資をシステムに対して行っていれば、復旧作業に使った費用を大幅に圧縮できる可能性がある。この視点からシステムを見直し、場合によっては追加投資を行って改良をする。さらには、次の大規模なシステム更新時に適切な投資を行えるように、トラブル復旧から得た知見を確実に次へとつなげていくようにする。トラブル発生直後は、このような検討を行うためのよい機会である。このとき、合理的な議論をするためにも、費用対効果の面からの議論を考えることが重要である。

その意味で、特に大規模なトラブルが発生した場合には、そのトラブルから復旧するのに要した「資源」「時間」「工数」「費用」、さらには「トラブル」によって被った損害などを記録し、後でシステム改善につながる適切な議論にしていくことが必要となる。

第三に、復旧作業の段取り、実際の作業の実施で障害となった要素を調べ、その障害を取り除くことを検討しなければならない。

十分な権限委譲がなされてないと判断できるようであれば、そのためのメカニズムを考えなければならない。内部調査を

復旧責任者ができなければ、第三者機関を使うという検討も必要だろう。復旧作業に伴う障害を軽減し、迅速に、また適切に復旧作業が行えるように環境を整備することも、復旧責任者の職務である。

また、以前から用意されている復旧作業マニュアルのようなものがあれば、「その改訂が必要かどうか」また「どのように改訂するのか」といったことも考える必要がある。

第四に、事後調査の結果を明確に報告することである。

特に、組織内の人間によってトラブルが人為的に引き起こされた場合には、その取り扱いには慎重さが必要となるが、絶対にもみ消すようなことがあってはならない。セキュリティー管理では、ユーザーのモラルに全面的に依存するシステムを作ってはならない。しかし、ユーザーのモラルに依存する面がなくなるわけではない。したがって、ユーザーが「モラルを高く維持できる」「組織に対する忠誠心を高く維持できる」ような環境作りが必要である。システムに対して人為的に障害を引き起こすことができても何もおとがめなしでは、ユーザーのモラルが低下することは確実である。この意味で、起こったことを正しく理解し、組織としての適切なけじめを付ける処理も重要なことである。復旧責任者はそこまで見届けることが重要となる。

第五に、必要があれば司法当局への告発も含めた法的対応を行うことを、経営陣に対して進言すべきである。

被害額が尋常でない場合、またトラブルの発生原因を調べて違法性を伴った行動が発見された場合には、法的な対応を取ることに躊躇する理由はないだろう。また、適切な法的対応を取らなかったことが、逆に後々新たな責任追及の火種になることもある。この意味で、法的対応も視野に入れた事後調査を、必要に応じて徹底して行うべきである。

戦略4 復旧責任者は事後調査にも十分な力をかけること。事後調査から知見を得ることこそが、トラブルから利益を得る唯一の道である。

失敗から学べ！

実はトラブルはすばらしい教師である。トラブルが発生したとき、「組織はどのように振る舞うのか」「責任体制をどのように駆動させるのか」「実際にトラブルが発生したときの対応体制は十分だったのか」「業務を継続するためのツールは用意されていたか」、また「自分自身はどのように行動し、その行動に改善すべき点はなかったのか」。

このような視点から組織運営を見直す最高の教師と言える。この意味で、トラブルをきっかけとして組織とシステムのあり方を見直すためのチャンスをもらったと考えるべきなのである。これが、失敗から学ぶことの本質であると筆者は考える。これは何も筆者だけが言っているのではなく、これまで多くの先人たちが同じ趣旨のことを何度も表現を変えて述べている。

しかし、筆者の周りで最近発生したいろいろな事故を見ていると、どうも復旧を迅速に行い、その後（最悪なことに）トラブルがなかったかのごとく振る舞うという傾向が、組織にも個人にも強いように感じる。「トラブルの隠蔽」までのひどい状況になっていないところがまだ救いではあるが、しかしトラブルから学ぼうとする姿勢があまりにも弱いと思えてならない。組織とシステムを改善する絶好の機会をみすみす逃してしまっては、「もったいない」というひと言に尽きるのだ。

もう1つ、トラブルへの対応は人の度量を測る最高のバロメータであることも知っておかなければならない。つまり、復旧作業というのはエンジニアの技量を測るためのよいフィールドになっているのだ。

トラブルからの復旧作業で力を持って働けるエンジニアは、技量もあり、また高いマインドを持っていることが多い。同時に、復旧作業は「上司」の度胸を測る最高のフィールドでもある。この意味で、トラブルは、単に技術的なものだけではなく、「エンジニアの腕と度量」「管理者・経営者の肝っ玉」についても教えてくれるのだ。技術だけでなく「人」に対しても多くのことを学ばせてくれる。

さらにもう1つ、失敗から学ぶことの重要性は、「組織として失敗が何によって引き起こされたのか」「何が問題であったのか」という教訓を、いかに組織の長期記憶に組めるかを知ることができるからだ。

力のある企業であればあるほど、実は社員が学んだ知見を共有して再利用するという意識が大変に強い。一度経験したことは、経験した人が得た知見をベースに取り組めば未経験の人よりもうまく対応できるのは当たり前の話だ。その意味で、トラブルについて、そこから得られた知見をいかに再利用するかについての取り組みは、将来的に同種のトラブルの発生を抑えるという点で大きな意味がある。

最近、システム運営でも、その効率化ばかりが追求され、結局トラブルが起きてもその原因追究が十分ではなく、その結果、大きなトラブルを見落としているのではないかと思われるような事態がしばしば見られる。同じようなトラブルを何度も繰り返し引き起こすのは、エンジニアの質の問題もあるが、それ以上に組織としてトラブルから学んだことを再利用する姿勢がないからにほかならない。

この意味で、失敗から学ぶことは数多くあるのだ。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp