CISO STRATEGY

企業のリスクをマネージする戦略考

システムが安定して稼働し、サービスを途切れなく提供することが、セキュリティーの達成目標である。そして、それはシステムの耐故障性確保、つまりシステムの稼働確保にもおよぶ。なにも外部からの攻撃やウイルスと戦うことだけがセキュリティー管理ではない。稼働確保のための基本的な技術をもう一度見直そう。

第十回 稼働確保とセキュリティー管理

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

セキュリティー管理の役割を整理

この連載では繰り返し述べているが、セキュリティー管理とは、ひと言で言えば、「管理対象である情報通信システムがどのような状態に保たれるべきかを定義し、その状態をできる限り維持することに努力する一連の作業」である。

セキュリティー管理をこのように定義した場合、セキュリティーポリシーとは、「保たれるべきシステムの状態はどのようなものであるかを整理し、その状態を維持するための作業に関して基本的な考え方を記述すること」といえる。

また、システムのあるべき姿（状態）から逸脱してしまう可能性がある事象を、システムに対する脅威と捉える。通常は、どんなに単純なシステムであっても多種多様な脅威が存在するので、それぞれの脅威の損害期待値等を勘案してリスク評価を行い、各脅威への対策の優先度を決め、それに従ってセキュリティー管理の具体的な作業を実施する。

さて、システムがあるべき姿とはどのような状態なのか。少し大雑把ではあるが、次の4つの条件を満たしている状態と定義する場合が多いだろう。

(1) 稼働しているシステムが予期しない形で停止することはないし、また停止しているシステムが予期しない形で稼働することもない。
(2) 利用者ごとに適切な権限が与えられ、その権限の範囲を逸脱する行為をしないようにすること。仮に利用者が権限の範囲を逸脱しようとしても、それが防御され、その行為自体が検出されること。
(3) システムが管理する資源の割り当てが円滑かつ安全に行われ、システムが稼働するのに必要な資源が枯渇しないように維持されること。
(4) システムがどのような状態になっているかを説明できるようになっていること。

システム管理との関係

セキュリティー管理は、システム管理のために行われる一連の作業に含まれるものだ。しかし、他のシステム管理作業と独立して考えることはできない。他のシステム管理作業と相互に深く関係し合うのが普通である。「システムのあるべき姿」をもう一度見直してみてほしい。セキュリティー管理の立場から見てぴたりと当てはまる「あるべき姿」であるが、セキュリティー管理においてはなにも特別な考え方ではない。システム管理全般から考えても「あるべき姿」である。

システム管理を真面目に適正に行っていれば、セキュリティー管理を行うのは必然的なことである。適切に設計されて実行されているシステム管理がなければ、セキュリティー管理を構築することはできない。

この意味において、最近になってセキュリティー管理が重要だと声高に述べ、最優先の作業であるかのように述べる専門家もいるが、その一方的な論調には筆者は素直に賛同できない。セキュリティー管理はシステム管理の一連の必須作業の1つであり、他のシステム管理作業とはけっして切り離して考えることはできないのだ。

したがって、今までセキュリティー管理が適正に行われてきていなかったので、これからセキュリティー管理をしっかりしなければならないと考えている組織に読

者の皆さんが所属しているとしたら、同時にシステム管理全般についても再点検し、管理体制を作り直す必要があるだろう。セキュリティー管理だけを特別視する組織だとしたら、まず確実にシステム管理の本質が理解されていないと考えられるからだ。

止まらないことの難しさ

本題に戻ろう。セキュリティー管理の中でも重点目標として「システムの稼働確保」がある。簡単に言えば、システムが予定どおりに稼働し、不測の事態で停止しないように管理作業を行うことである。言い換えると、稼働中のシステムが停止しないようにし、安全な起動や停止を実施し、サービスを計画どおりに提供するための維持管理をすることである。

これを実行するためには、何がシステムを停止させてしまう可能性があるか、そしてそのリスク対策として何をすべきなのかを考えなければならない。ところが、システムの稼働確保のために考えられるリスクに思いを巡らすと、多種多様なものがあることに気づくだろう。

たとえば、電源問題を考えてみよう。情報通信システム構成の設計においては、電源周りについては十分に考えておかなければならない要素である。通常は、UPSを用意して停電や電源瞬断があったとしても、システムが停止しないような対策をするだろう。しかし、これだけで十分な対策であると言えるだろうか。

真面目にシステムのことを考えると、次のようなことも考えなければならない。

(1)システム本体に用意されている電源ユニットそのものが二重化されているシステムを利用する。これにより電源ユニット故障の問題を避けることができる。

(2)電源ユニットが二重化されているならば、それぞれのユニットに対して別々のUPSを用意して接続する。

(3)各UPSは、別々の電源供給回路に接続して、単一のブレーカー断によって両方の電源供給が停止しないようにする。

上記3点の対策は、現在のデータセンターのシステム環境では普通に行われていることである。しかし、本当にこれで十分なのだろうか。もう少しシステムのことを考え進めていくと、まさにパラノイア的(妄想的)に想像力を膨らませ、その対策を考えてしまう。

たとえば、電力会社からの供給回線が1つだけでは不安なので、別々の供給回線を用意し、1つの引き込み回線に障害が発生したとしても大丈夫なようにしておくことを真剣に考えているデータセンターもある。またUPSによって可能となる電源供給も10分というようなものではなく、12時間というような長時間を考えているところもある。

さらに、場合によっては自家発電設備を用意して、電力喪失事故に備えているデータセンターも多い。特に阪神淡路大震災では、建物倒壊や通信回線断といった被害をほとんど受けなかったビルであっても、電源供給が48時間近く停止した地域が広くあった。このことを教訓にして、真剣に自家発電設備を用意した組織も数多くあると聞いている。

このように見ていくと、「システムの稼働確保」に重点を置いた電源設計を見ただけでも、単純かつ低コストな対策から大がかりな対策までを施す可能性があると言えよう。

さらに深く考えていくと、電源問題だけではなく、それ以外にも多くのリスクに対応していく必要があるのだ。このため、システムの稼働確保をどのようにしていくのかという問題については、幅広い視野と洞察力をもって対策を考えなければならないということがわかるだろう。

では、この問題はどのように考えたらよいのだろうか。

障害からシステムを守る基本

システムの稼働確保問題を考える場合に定石とも言える方法がある。それが、Single Point of Failureの除去である。

Single Point of Failureとは、ある場所の単一故障によってシステム全体の稼働が停止してしまうことである。電源事故対策で考えると、システムに用意されている1つだけの電源ユニットは、まさにSingle Point of Failureと言える。

Single Point of Failureを発見すること、発見したSingle Point of Failureの与えうる影響を評価すること、そして、そのSingle Point of Failureを除去する作業を行うことが、まさに障害からシステムを守る基本である。

Single Point of Failureの除去には、通常は予備機材を用意するのが一般的である。たとえば、単一のコンピュータシステムは、それ全体がSingle Point of Failureになってしまう。そこで、負荷分散装置(ロードバランサー)を使って2台のシステムに負荷を分散させるようにして、1台のシステムが故障したとしても大丈夫なようにしておくことで対応する。またネットワーク機器の場合には、すべてがSingle Point of Failureになるケースが多い。このため、ネットワーク機器と回線に関しても冗長化(二重化)していくことが一般的に行われる。

このように、システムを構成する要素から、システム全体、さらには回線やネットワークといったところまで、くまなく調べてSingle Point of Failureを発見し、その除去を冗長化によって対処していくのが定石である。また、最近ではそのための機器やソフトウェアが数多く提供され

ている。いろいろなレベルでのSingle Point of Failureを取り除くことができるし、また同時にどのような技術が利用可能かをたえず調べておくことも、運用技術者として重要なことだ。

戦略1 Single Point of Failureを見つけ、冗長化を施してシステムが稼働停止にならないようにすることが定石である。

突発事故は常に念頭に置く

Single Point of Failureを除去するようにシステムを構築していても、想定される脅威によっては冗長化が単純にできないものもある。それが大規模災害である。

たとえば、システムを設置しているデータセンターに不審者が侵入してシステムを破壊し、全面的に利用できない状況が発生する可能性を考えてみよう。あるいは、大地震が発生し、東京一帯が壊滅的な打撃を受けたとしよう。このような場合、単純にシステムのSingle Point of Failureを除去しているだけでは対応しきれない。システム全体が壊滅してしまう可能性が否定できないからだ。

このような話をすると、「そんな荒唐無稽な状況を想定する必要があるのか。そんなことが起きるものか」と言う人も多い。しかし、過去10年を思い出してほしい。大地震はめったに発生しないと誰もが信じていた神戸辺りで、阪神淡路大震災が発生し、米国ではハイジャックされた飛行機がビルに突っ込み、国際的な金融センターは一瞬にして壊滅した。さらに、自爆テロによって世界中の主要ビルが破壊される可能性が跳ね上がってしまったのである。これを考えると、東京で定常的に爆弾テロが発生し、挙句の果てに大地震が東京を襲うということが現実味を帯びないと言い切れるだろうか。

隕石によるシステム破壊や火星人によるシステム盗難までを考えなさいとまでは言わない。しかし、過去10年間の突発事故を考えてみると、地震、短時間集中豪雨による浸水、火災などは十分考える必要がある。また、爆弾テロなどによる破壊行為も、日本ではまだまだ確率が低いのかもしれないが、当然考えておく必要があるだろう。もちろん、この種の突発事故に対応しなければならないシステムは限定されるが、多くのユーザーにサービスを提供しているシステムの場合には、一度は検討したほうがよいだろう。

さて、この種の突発事故に対する対応策にも定番がある。それは物理的に離れた場所に、バックアップシステムを用意しておくことである。同時にシステムが壊滅しない距離にシステムを隔離して設置し、どちらかのシステムが故障しても大丈夫なように対応するのである。

典型的には、東京と大阪にサーバーを置くという形態である。あるいは、最近では国際回線の急速な広帯域化を考えて、システムを日米2か所に分散して設置するところもある。このように、物理的にシステムを分散して設置するということは当たり前のことと考えるべきだろう。

戦略2 バックアップシステムを物理的に数百km以上隔離して設置し、大規模災害に備えるのもシステムの稼働確保での定石である。

大規模災害への対策は入念に

余談となるが、いま東京を関東大震災や阪神淡路大震災クラスの大地震が襲ったとしよう。わが国の経済活動は壊滅的な打撃を受けると思われるが、その中でもしぶとく生き残っていられる企業はどのくらいあるだろうか。あるいは東京はどのくらいの期間で復興できるのだろうか。1990年代中盤からのIT重視政策により、これだけコンピュータとネットワークに大きく依存した日本社会を作り出してしまったにもかかわらず、大規模災害への対策は不十分であると思う。

筆者自身は1995年の阪神淡路大震災に大阪で遭遇したが、その衝撃は想像を絶するものであった。いまだに生々しく記憶に刻み込まれている。しかし、現在の情報通信システムに大きく依存した社会は、残念ながら一度も阪神淡路大震災クラスの大地震の洗礼は受けていない。したがって、私たちは一度も経験してないことを、次に起こるであろう大震災では対処しなければならない。この意味で、私たちはもっと入念に検討をすべきだと常々思うのだ。

人的事故も稼働確保を阻止する

さらに、システムの稼働確保を阻止する大きな要因の1つに「人」がある。今回紹介した定石や定番の考え方で、システムに冗長性を確保したものの、土壇場で人間が介在することによってトラブルが発生することがある。

たとえば、こんなことが実際にあった。情報提供を行うシステムで、バックアップ用のシステムを用意しておきながら、予算的な問題で負荷分散装置を用意することができなかった。そのため、障害発生時にはオペレーターがネットワーク回線をつなぎ直すというシステムを考えた。

当然、この2つのシステムの内容は同期するように設定しておかなければならない。しかし、実際にトラブルが発生したときには、見事にこの装置は機能しなかった。管理者が、2つのシステムの内容を同期させる作業を忘れていたために、システムの内容が古いまま放置されていたのだ。この例とは別に、トラブル発生時のために確保していた保守部材を、管理者が勝手に他の目的のために流用していたケースもある。

このように、人は決められたことを的確

にやらなかったり、約束を破ってしまったりすることがある。このため稼働確保の重要な作業を、管理者を含めた人間が行うようなシステム運用を設計してしまうと、人間の質が問題となってしまうこともあるのだ。つまり、人間がSingle Point of Failureになってしまうのである。この「人」問題については、筆者は1つのルールを持っている。常々、判断をするのは人間がすべき行為だと思っているが、必要なタイミングで必要なことを短時間でやるという作業については、人間は大変不得手なので信用しないというルールだ。

この意味では、実際のバックアップシステムへの切り替えや、システムのデータの同期などの処理については、できる限り自動化し、システムが確実に処理をするように設計することが肝要だと考えている。システムの稼働確保について命運を人間に託すのには、人間はいい加減で不確か過ぎるのだ。

戦略3 人間は常にSingle Point of Failureになりうる構成要素だと考えるべきだ。人間にシステム稼働確保の命運を託してはいけない。

コストに対する考え方をもつべし

ここまで、システムを停止させない対策として考えるべきことを述べてきた。しかし、もう1つ十分に考えなければならないことが、「コストの問題」である。

たとえば、WWWサービスを提供しているシステムがあったとしよう。これまでに述べた考え方で冗長性を確保すると、Single Point of Failureの除去を考えてシステムを二重化し、さらに突発事故対策も考えると、結局システムは最低でも4台は必要になり、さらに負荷分散装置としてローカルに分散させるために2台必要となり、さらに広域ネットワーク上で分散させるために2台必要となる。このように考えると、単純に1台のシステムでサービスを提供する場合と比較すると、4倍以上のコストがかかることになる。

システムを停止させないようにするためには、コストがかかるのは当たり前の話である。しかし、あまりにもコストが高くなることから、経営陣の説得が困難になることも多い。このような場合にはどのようにしたらよいのだろうか。

費用問題を考えた場合に、経営陣を説得する方法としては、純粋にセキュリティー管理で行われるリスク評価（リスクアセスメント）の手法を使うことが最適と言えよう。つまり、損害額期待値を計算し、その損害額期待値の何パーセントを対策に投入するかという論法で説得を行うのだ。さすがに最近ではセキュリティー管理について経営者側も理解を示すようになり始めていることから、リスク評価についても多くの経営者に対して説得力をもつようになってきているのだ。その意味で、リスク評価をシステムの稼働確保のためのコスト算定に使ってみるのも悪くないアイデアである。

戦略4 システムの冗長性を確保するためのコストについては、リスク評価をもとに妥当性を検討するのは良い考え方だ。

本当に止まってしまったときは？

本来、多重故障の発生確率は非常に低く、滅多に発生することはないと考える。冗長性確保では、単一故障だけを対象に設計することが多い。しかし、実際に多重故障が発生してしまうこともあり、それによってシステムが停止してしまうこともある。「絶対に大丈夫なシステム」を作ることは理論的には不可能であり、確率として停止する可能性が低いシステムを作ることが精一杯である。

本当にシステムが不測の事態で停止してしまったとしよう。このとき、管理者は何をすればよいのだろうか。

1つは、稼働再開を短時間で果たすために、できる限り短時間にシステム停止の原因を特定し、原因の除去と稼働再開のためのさまざまな方策を考えて、可能性の高い方法を復旧することである。これは緊急事態の、本来想定されていない状況での対応であるから、創意工夫と大胆な発想も求められる。時には、従来の管理構造から離れて対策を組み立てることが必要になる場合もあるだろう。

もう1つ管理者が行わなければならないことは、システムが停止した原因を特定し、誰が賠償責任を持つのかを考えることである。もちろん、場合によっては誰も責任をとれない状況もあるかもしれない。しかし、多くの場合には、事故を引き起こした原因が存在し、その原因を作り出した人や組織があるはずだ。賠償責任を負わせるのに必要な情報を収集して保存しておくことも十分に考えておかなければならない。

戦略5 システムが止まってしまったら、その回復に全力をかけるとともに、その賠償責任を負う人（組織）が誰かも考えながら証拠を確保することも忘れないことが大事である。また、そのための道具も用意しておこう。

セキュリティー管理には総合力

システムの不測の停止を避けることは、システム管理において重要であるが、セキュリティー管理においても重要な実現目標となる。管理対象となる情報通信システムを停止させないための方策設計や対策実装などを考えることで、セキュリティー管理においても総合的な力が必要になることがわかるだろう。

セキュリティー管理は、他のシステム管理作業と不可分である。さまざまな力がセキュリティー管理に力を与えるのだ。

［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