ICT基礎講座

Close-Up クローズアップ

システム障害とBCP

対策の大前提は「障害は必ず発生する」という発想

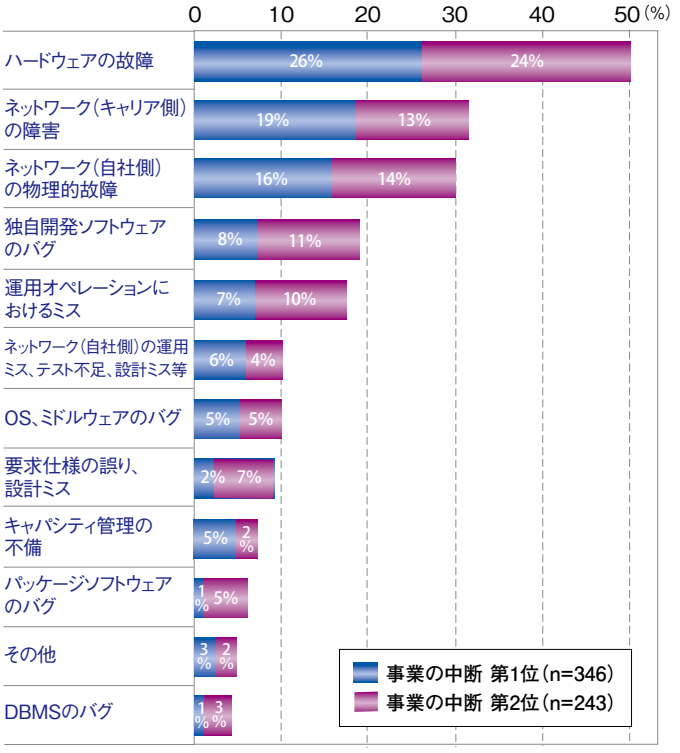
私たちの生活は、幅広い分野で情報システムの安定稼働に支えられている。しかし、故障しないコンピュータはなく、ソフトウェアにバグがないことを保証することもできない。震災や洪水のような大きな災害に対しての対応も迫られている。システム障害を想定し、その被害を最小限にとどめるための策を考えておこう。

障害はなぜ起きるのか？

図1は、社団法人日本情報システム・ユーザー協会が行った「第17回企業IT動向調査2011（10年度調査）」において、事業の中断にまでいたった重大なシステム障害の一次原因を分類したものだ。

障害原因の1位～3位の「ハードウェアの故障」「ネットワーク（キャリア側）の障害」「ネットワーク（自社側）の物理的故障」といった不慮の事故は、毎年上位を占めている。次いで多いのが「独自開発ソフトウェアのバグ」、そして「運用オペレーションにおけるミス」と続いている。また「その他」には「ウイルス」が原因という回答もあり、今後はサイバーアタックによるシステム障害に向けた対策も必要になってくるだろう。

独自開発ソフトウェアのバグによる事業の中断の割合は、2008年度5%、2009年度6%、2010年度8%と増加傾向にある。独立行政法人 情報処理推進機構（IPA）による2010年1月から2011年6月に報道されたシステム障害の調査においても、原因が発表されている19件のうちソフトウェアのバグによるものが8件発生したという報告がある。企業側にも然るべき対策が求められる。



■図1　システム障害による事業中断にいたった障害の主な一次原因

原因別に見るシステム障害

前項の障害の要因を整理して次の5つに分類し、それぞれの原因別に実際に起きたシステム停止の事例からその対策を検討した。

●すべての機器が原因となるハードウェア障害は管理ツールを利用したメンテナンスで防ぐ

データベースサーバが故障した。ハードウェアは二重化されていたが、システムが故障を認識せず、自動的に別のサーバに切り替わらなかった

ハードウェア障害は、システムを構成する機器とそれらを制御する仕組みのいずれかの故障や不具合が原因となる。停電や落雷、ノイズなどの外部要因で故障が引き起こされることもある。

対策として、機材の冗長化や、複数の機材による分散構成をとって障害箇所の負荷を他に振り向ける仕組みを構築することが考えられる。しかし、ハードウェアの冗長化が進むと障害が発生してもシステムが動き続ける場合もあり、障害の発生に気付かないことがある。そのため定期的に点検する、障害の検出や原因箇所を特定する、通知機能を備えた管理ツールを導入する、外部の監視サービスを利用するなど常に動作状況を監視し障害を見逃さないようにすることも大切だ。

障害を検知した場合は、たとえ小さな障害であっても放置せず、原因を追求して適切に対処し、システムが正常に稼働していることを確認するといった基本的な対応を心がけることも必要だ。小さな障害が大きな障害を誘発したり、正常に稼働しているという思い込みが長時間にわたるシステムダウンにつながったという事例も報じられている。しっかりした体制を整えておきたい。

●想定外のデータが招くシステムダウンは開発段階からの入念な検証で防ぐ

システムが停止した原因は、全角で転送すべきデータが半角で送られてきたことだった

ソフトウェアの不具合に起因する障害は、想定外のデータがトリガーとなるケースが多い。日付データが不正値になっていた、受け取った文字コードが違っていた、明らかな入力ミスをシステム側が受け付けたといった例もある。

結果論ではあるが、こうした障害を経験した企業の多くが障害を防ぐチャンスはあったと言う。稼働前の設計やテストの段階では、設計の不備やテストの漏れを見落としていることが多い。想定不足や思い込み、油断などによるものだ。稼働後では障害の予兆を捉えられなかった場合が多い。システムを常時監視し動作の変化を捉えていても、障害の予兆と見なす「基準」を明確にしていないと、その変化と障害が結びつかず、「変化している」という情報を担当者間で共有できない。そのため適切に対処することが難しい。

ソフトウェア障害は稼働直前のテストだけでは防げない。企画段階における要件定義や基本設計の時点から、工程ごとに仕様や設計に誤りや漏れがないか、設計どおりに構築されているかといったレビューやテスト仕様の策定を地道に重ねることで防げるものも多い。テスト段階では開発者だけでなく専門の担当者による実施や、ツールの効果的な利用が単純ミスや想定漏れ、確認漏れを防止する。そして運用時には、システムの挙動の変化に基準を設け、変化量に応じた対応策を決める、情報共有を徹底するなどの標準化を図ることが求められている。

●慣れない操作が巻き起こす運用ミスは手順書の整備と定期的な訓練で防ぐ

ネットワークに異常が起きた原因は、2年に一度の部品交換時の設定ミスだった

運用時の操作ミスに起因する障害のほとんどは、日常のオペレーションとは異なる状況で発生している。新システムへデータを移行する際に手順を誤った、ハードウェアを増設したあとの設定を誤った、小さな障害が起きたあとの復帰操作でミスをした、などである。

運用ミスを防ぐには、多様なシナリオを想定した運用手順書の作成と定期的な運用訓練を実施することが肝心だ。もちろん、関連する資料の保管場所も明確にしておく必要がある。

特にミスを起こしやすい操作や実行頻度の低い操作では、手順書の確認と訓練を繰り返すことで操作に慣れたり、コマンド入力の代わりにスクリプトで実行させる、操作を自動化させるなどの工夫が単純ミスを防ぐことにもつながる。

日ごろの訓練で発生したミスに対しては、担当者への注意喚起や手順書の見直しだけでなく、誤った操作にはアラートを出す、場合によってはプログラムを作り直すなどシステム側での対応も有効な対策の一つである。

●キャパシティ飽和によるシステム障害はサーバの処理能力強化と計画的なシステム拡張で防ぐ

・キャンペーン初日に大量のデータ処理が発生し、翌日になっても処理しきれずにシステムがダウンした
・ネットワーク機器の障害が復旧したと同時に大量の再送処理が発生し通信ができなくなった

システムの設計時には、最大の処理量を想定し、負荷に耐えられるようにある程度のゆとりを持たせてシステムを構成する。しかし、開発時に余裕を見込んでいても運用開始後に想定を超えたデータ量になったり、突発的にアクセスが増加することがある。その結果、キャパシティ飽和となりシステム障害を引き起こす。

処理量の増加に対して、Web サーバなどはロードバランサーで複数の機材に処理を振り分けて負荷を分散させる、一元管理の必要なデータベースは、データベースの分割、データ構造の改良で処理能力の増強を図るなど柔軟な対応が可能だ。あらかじめ処理の限界値が判定できるようなテストを行うなどし、処理が一定量に達するとアラートを出す仕組みを導入することで、事前に負荷を分散させることもできる。

並行して、業務量や顧客数の増加にあわせて、高性能サーバへの置き換えやサーバ増設などのシステム拡張をタイムリーに行っていく必要がある。ボトルネックとなる箇所を監視しながら、中長期的な視野で計画的に機器の増設を行う、あるいは、サーバを仮想化して、既存のハードウェア資源を活用しながら処理量の変化に対応することも有効な手立てとなる。

●個人や企業が標的のサイバー攻撃にはウイルスを拡散させないシステムで情報流出を防ぐ

取引先担当者の名前を騙ったメールに添付されたファイルを開いたらウイルスに感染し、IPアドレスなどの情報が漏えいした

近年、増加傾向にあるのが事業を妨害するサイバーアタックだ。Webサイトへの「DoS攻撃」を思い浮かべる方が多いだろう。インターネット上にある特定のサーバに対して集中的にアクセスし、サーバやネットワーク機器の性能を使いきって、サーバをダウンさせる。

2011年に報じられた「標的型メール」による攻撃は、より深刻で恐ろしい。感染したウイルスにより利用者のIDとパスワードが

盗まれ、国会議員の一部ならびに関係者のメールなどが盗み見できる状態になったという。海外ではさらに、発電所などの工業プラント向けシステムの不正操作を狙う「ボットネット型マルウェア」の例もあり、サイバー攻撃は不特定多数ではなく、特定企業や特定の個人を狙う時代になってきている。

標的型メールはタイトルや本文、発信元が巧妙に作られており、完全に遮断するのは難しい。実際、セキュリティ会社の社内演習でもだまされた社員がいたという。

サイバー攻撃に対しては、ウイルスの侵入を防ぐだけでなく、ウイルスの広がりを抑える出口対策の重要度が高まっている。専門の情報セキュリティ担当者と連携して情報システムのセキュリティ強化に取り組んでおきたい。また社内への啓発活動も忘れてはならない。セキュリティソフトの適用とOSを常に最新の状態にアップデートすること、不審メールや怪しいWebサイトへの警戒、重要な情報の暗号化といった基本部分は、システムを利用する一人ひとりが最低限守らなければならない。

●システム障害は必ず起きる

システム障害は、社内外のさまざまな要因で発生する。したがって、情報システム部門は、障害をいち早く検知する、障害発生時の対処方法を決めておくなど、「システム障害は必ず起きる」という前提で、障害発生を見据えた対策をたてておく必要がある。

例えば障害発生時にシステム全体の状況を把握する方法をあらかじめ決めておく、原因を判明しやすくするための工夫をシステムに盛り込んでおく、ベンダーとの役割分担を明文化しておくなどは、システム構築時から想定しておく。障害発生時に特定の人に作業を集中させないためには、情報を収集する人、経営層や関係者に報告する人、システム復旧作業にあたる人など、関係者の役割を決めておくことも必須になる。さらに日ごろから外部の障害事例へのアンテナを高くしておくことで、復旧時間を短縮するだけでなく障害を未然に防げるかもしれない。

対策をたてたら定期的な訓練も必須だ。緊急時の対処方法を関連部門全員が共有するとともに、時間や曜日、重点テーマを変えて実施することで、さまざまな場面に対して計画を検証しておくことができる。

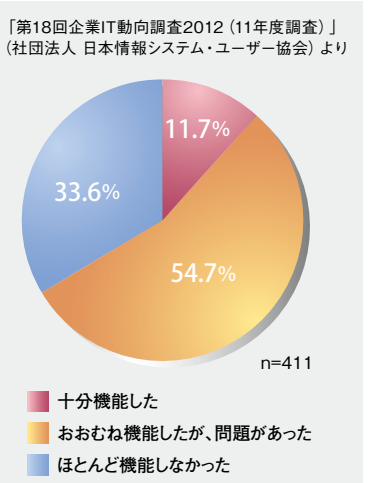
システム障害はシステムが停止した時間だけの損害では済まないことが多い。ビジネスで最も重要な企業の信用を失墜し、損害賠償に発展する可能性もある。システム障害による被害を極小化するためには、情報システム運用の基本的なオペレーションを地道に実行し続けるとともに、それでも発生する障害を想定して対応策を練っておくことが重要だ。

BCPとICT部門

事業継続計画（BCP：Business Continuity Plan）とは、災害や事故により一時的に事業活動が低下した場合でも、中核となる事業を継続させる、また、そのための回復時間をできる限り短縮し、早期に回復させることで損失を最小限に抑え、事業を継続させていくための計画をいう。

2011年に発生した東日本大震災やタイの洪水により生産現場の被災や、部品不足を経験した企業は多い。世界中のビジネスに影響が出た。「自然災害だから仕方ない」ではすまされない。最近では、「BCPがなければ取引停止もありうる」と、BCPの策定と実行を取引条件とする企業が増えているという。しかし、2011年11月に実施された調査結果でも、現実には半数以上の企業がいまだにBCPを策定していないと報告されている。

BCPが策定されていても実際に機能しなければ意味がない。図2をご覧いただきたい。BCPを策定し、東日本大震災で直接または間接的に被害を受けた企業への調査では、



■図2 東日本大震災時におけるBCPの機能状況

■表1 製造業A社が策定した災害時における各システムの重要度

重要度	復旧目標時間	説明	システム名称	バックアップ体制
S	0時間	従業員の安否確認、災害対策に必須	安否情報、認証など共通基盤、IP電話、電子メール、イントラネット	東京・大阪で並行稼働
A	2時間	顧客に直接影響を及ぼす	社外向けホームページ、注文受付、受注出荷、通販	バックアップ環境を準備
B	2日間	中断の機能が顧客に影響を及ぼす	取引確定、売掛金請求、販促費精算、支払い	非被災側でシステムのリカバリを検討中
C	1週間/1カ月	中断の影響が社内に影響を及ぼす	需給計画、製造計画、営業支援/経理、人事	
D	1カ月以上	代替手段で当面の業務が継続可能	予算編成、その他情報系	—

■図3 Systemwalker Centric Managerの概念図（他社運用管理製品との連携）

BCPが十分機能した企業は11.7%に過ぎず、88.3%の企業が何らかの問題があったと回答した。BCPは策定したあとも、訓練、検証、改訂を繰り返して磨き続けることが必要だ。

●ICT部門に期待されることは

緊急事態に際しては、目先の障害対応に走ることなく、BCPに沿って行動することが重要だ。そのためには緊急時に十分機能するBCPを策定する必要がある。

一般的なBCP策定プロセスでは、想定されるリスクを洗い出し、継続するべき事業および最優先で復旧するべき中核となる事業を特定し、それぞれの事業に対して必要となるインフラやシステムなどの復旧手順やバックアップ体制との連携、復旧目標時間を明確にしていく。事業継続に必要な項目すべてに対して優先順位をつけて決定する作業は、時間のかかる地道な作業だ。通常とは異なる状況を想定してシステムの整備を進める必要もある。

表1の災害時におけるシステム復旧対策は、A社の情報システム部門が立てたものだ。ICT部門はシステム構築の際に業務を分析し、また日々の運用で発生する障害とその対応を通じて、重要な業務と関連するシステムを把握している。ICT部門が中心になってBCP策定にあたることが期間の短縮につながる場合も多い。いざというときに慌てないためには、BCP策定後も防災訓練にあわせて見直しをかけるなど、定期的に確認・判断する体制をとっておくことが望ましい。

今日ではICTが機能しなければ事業活動が成り立たない企業が多い。それだけにBCPの策定と運用にあたりICT部門への期待が高まっている。

富士通の取り組み

情報システムの安定稼働は企業活動の大前提となっている。この安定稼働を支えるために富士通は、システム管理ツール、バックアップシステム、仮想化基盤など多くの製品やサービスを提供している。

事業拠点ごとに運用システムのベンダーが異なるケースは意外に多いのではないだろうか。異なるベンダーから提供される管理ツールを併用し、煩雑で一貫性のない操作で運用していると、操作ミスを招きやすい。運用管理システムに障害が生じると機器の状況がつかめなくなる。そうしたマルチベンダーでのシステムの統合運用管理を実現するのがSystemwalker Centric Manager（システムウォーカーセントリックマネージャー）だ（図3）。

各事業拠点の運用管理システムは、監視サーバで一元的に管理する。監視サーバは最大4重化までの冗長構成をとることができるので、監視サーバを4地区の遠隔地に設置し冗長化させることも可能。災害時の備えとしても期待できる。

発生したイベントに対して、あらかじめ対処するためのアクション（コマンド、スクリプト、プログラムなど）を登録し障害対処の自動化を図るなど、止まらないシステムを実現するツールだ。

情報システムは、日に日に高速・大容量・複雑・高度になり、それにつれてシステム障害の要因も増加する。富士通は、ネットワークからハード・ソフト、サービスなど幅広い製品やサービスの開発・提供を通じて、情報システムのさらなる安定稼働を実現し、お客様の事業継続を支援していく。

●富士通関連サイト
○Systemwalker Centric Manager
http://systemwalker.fujitsu.com/jp/centricmgr/

<参考資料>
○『重要インフラ情報システムの信頼性向上の取組みガイドブック』
http://sec.ipa.go.jp/reports/20110330.html
○経済産業省による「企業の IT 投資動向に関する調査」（企業 IT 動向調査 2011）
http://www.juas.or.jp/servey/it11/index.html
○『企業 IT 動向調査 2012』
http://www.juas.or.jp/servey/it12/index.html
○ 動かないコンピュータその後
http://itpro.nikkeibp.co.jp/article/COLUMN/20110307/358043/
○ ビジネスを止めないシステム
http://itpro.nikkeibp.co.jp/article/COLUMN/20070801/278847/

〈監修〉：編集委員　岡嶋 友　アットホーム㈱