都市防災におけるフェイルセイフ設計

小林　正美

1. はじめに

都市で起こる災害（都市災害）では，自然現象によって引き起こされる直接的な被害もさることながら，人為的につくられた都市そのものがもつ構造によって，後につづいて，被害が連鎖的に発生し，指数的に拡大していくところに大きな特徴がある．都市防災のための工学的な対策には，自然の力による直接的な被害（自然災害）を軽減するための防災工学的なアプローチと，不幸にも何らかの直接被害が発生してしまった場合に対して，その後に発生する間接被害や2次災害を防ぎ，小規模で終わらせ，少なくとも人命の安全だけは確保しようとする安全工学的なアプローチがある．本稿は，地震に対する都市防災を例にして，地震時の2次災害から人々の安全を確保するため，火災延焼やエネルギー供給停止被害をおさえる安全装置としてのフェイルセイフシステムに焦点をあて，都市の安全設計の考え方を説明するものである．

2. 安全設計の原理

安全とは，安らかで災害の危険のないこと，特に人間の死傷につながるような危険のない状態として定義される．一方，人間がつくる製品や構造物，そしてシステムについては，その機能に対して信頼性が求められる．人身事故を起こさないことが安全であり，部品やシステムが故障しないことが信頼である．安全や信頼が確率で定義されると，それぞれ安全度と信頼度（reliability）となる．そして安全度は，故障が人命の危険に結びつく確率（危険度）を1から引いたものである．

工業製品やシステムでは，故障が発生しないように，またもし故障が発生してもすぐにシステムや製品が使用できなくならないようにするための技術として，信頼性設計が発達してきた．信頼性設計[1]では，まず部品やシステムの単純化と標準化が求められる．そして部品や機器が故障しても，予備機，予備部品の設置により製品としての機能，性能が満足されるような冗長化が，基本的な技術となる．構造物や機械では，従来より，余裕率や安全率など，与えられた部品の定格以上の強度や余裕を見込んで設計する，安全係数を用いた設計法が用いられてきた．同様な考えを電子機器等に適用したものがディレーティング（derating：負担軽減）であり，そこではストレス（負荷）を軽減することで，故障率を低減させている．近年，コンピュータの信頼性確保のために広く使用されるようになった技術に，フォールトトレランス（fault tolerance：耐故障性）がある[2]．フォールトトレランスの設計とは，誤り（error：構成要素の異常な出力）の発生にもかかわらず，障害（failure：ユーザーに対するサービスの異常）を生じさせないか，一時的に障害を引き起こしても自動的に正常な動作を回復するようなシステムに設計しておくことである．フォールトトレランスの設計技術には，故障時にシステムの最小必要機能を残し，その影響を性能の低下のみにとどめようとするフェイルソフト（fail-soft）と，故障がより重大な故障につながらないように，システム機能を安全側に停止させるフェイルセイフ（fail-safe）の技術がある．このうちフェイルセイフは，特に人間の命を守るために生まれ普及してきた技術であり，システムの内部に故障が発生した場合，サービスに誤った出力を出すことはあっても危険な出力は生じない設計にしておくことといえる．したがって厳密な意味では，フェイルセイフはフォールトトレランスではないが，一般的にはそれは，システムの一部に故障が起きてもシステム全体に与える影響を少なくし，故障を災害まで発展させない機構という，広い意味で使われている．そのようなシステムをつくるフェイルセイフ設計の原理を，近藤[3]は，図1のようなモデルで説明している．

図1の(a)は多経路荷重構造，重複構造あるいは並列（リダンダント）構造などと呼ばれるもので，複数個のユニットで並列構造や m out of n（n個のうちm個が作動すればよい）の構造をつくり，たとえば1本が破損しても2本が完全ならば，破壊することがないようにし

こばやし　まさみ　京都大学大学院環境地球工学専攻
〒606 京都市左京区吉田本町

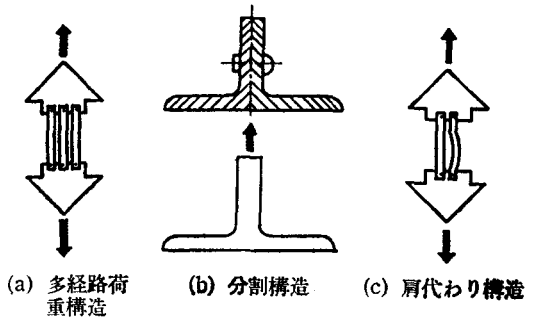

図 1　フェイルセイフ設計の考え方

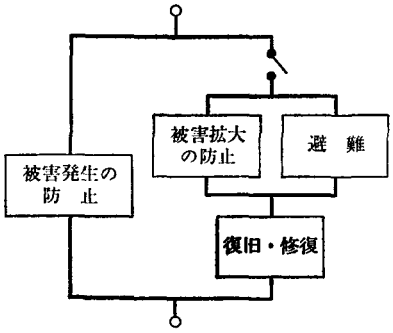

図 2　都市の防災システム

ておくものである．航空機などで複数のエンジンを備えておき，1基のエンジンが故障しても失速することがないようにしておくことなどがこれに相当する．

図1の(b)は，分割構造または組合せ構造というもので，1個のT字型部材を図の上方に示すように2個以上に分割しておき，それらの分割部材が結合してT字型部材の役割をするような設計であり，破壊が生じてもそれは分割部材の一方だけで止まり，全体の破壊がないようにした構造を意味する．

図1の(c)は，肩代わり構造，支援構造または待機並列構造と呼ばれるもので，最初は左の部材が荷重に耐えているが，そのうちこれが切断することがあると，それまで遊んでいた右の部材が引っ張りで真っすぐに伸びて，荷重を受け持つような構造である．化学プラントでは重要な制御機器は，電源・空気源が二重になっており，停電になった場合は非常電源に，また空気源が停止した場合は，窒素に自動的に切り替わるようになっている．

図1の(d)は，荷重軽減構造で，左側を右側に比較して故意に弱くしておき，左側が破損しても荷重が右側に移り，致命的な破壊にならないような構造を意味しており，圧力容器に装備されている破裂板などがこれに相当する．

図1の(a)，(c)の構造形式は，それぞれ冗長設計での並列冗長，待機冗長のシステムとも呼ぶことができるように，フェイルセイフシステムの多くは，冗長設計でも説明が可能である．フェイルセイフのシステムとは，過電流制御のヒューズで代表される安全装置であり，その意味では，図1の(b)と(d)が，フェイルセイフ設計に固有な構造ということもできる．なお冗長系をつくるには，①同一要素を並べる，②同一機能をもつ要素を並べる，③機能的差のある要素を並べる，の3つの方法があるが，フェイルセイフシステムは，本来，主たるシステムの安全装置になるので，主システムに対しては，③の冗長系になるのが基本的な姿である．

3.　都市防災のシステム

都市は製品ではないが，その役割や活動をシステムとしてみると，そこに人々が集まり住まい，日々の生活がいつもどおりに繰り返されている状態が，システムとしての都市の定常状態となる．都市の防災システムは，この定常状態を，地震などの自然災害が発生しても維持し続けていくために備えられるものであり，図2のような構成のものとしてとらえられる．すなわち都市防災のシステムは，都市に異常でかつ急激な環境変化が発生した場合に作動するシステムであり，その目的は，自然災害などを起因にする急激な環境変化があっても都市での活動を中断させることなく，都市の物理的構造と機能に定常状態の維持を図り，たとえ構造物等に直接的な被害があっても，それに続く間接的な被害を最小限度にとどめ，少なくとも人的な被害の発生は回避し，災害が治まった後にはできるだけ早く修復・復旧を行なって，以前の定常的な状態に戻すことにある．

都市の防災システムは，都市本来の機能からすれば，災害の発生の危険がある場合のみ作動する予備的，付属的な安全装置である．図2の各サブシステムの個別の目的を説明すると，被害発生の防止は，都市が異常な自然現象に襲われても被害が出ないように，予防的対策をあらかじめほどこしておくことである．これは，たとえば構造物についていえば，想定する地震の強さ（設計荷重）に対応させて設計強度を数倍にとっておき，被害の発生を未然に防ごうとするものであり，通常は，安全係数を余裕をもって大きくとる余裕設計（過剰設計）で対応される．しかしこの安全係数にどの程度までの値をとればよいかには（2倍がよいのか5倍がよいのか，とい

ったこと），たとえ構造物や材料の設計強度と，外力である設計荷重の確率密度関数が得られたとしても，その妥当な決め方といったものはない．この想定される荷重に対して，余裕をもった設計強度をとることでの予防対策は，予想される荷重以上の設計強度をもたせる通常の設計方法となんら変わらないところもあるので，特にこれだけでは安全設計と呼ばない場合もある．この十分に余裕をとるという予防システムが有効に働くと，異常な自然現象があっても被害の発生は未然に防がれ，都市は通常の活動がそのまま持続される．

これに対して右側のシステムは，都市の構造物がなんらかの被害を受けた後に作動する安全装置（システム）であり，直接被害に続いて発生する2次被害や間接被害をできるだけ軽微に終わらせる「被害拡大の防止」と，人命の安全を確保する「避難」，さらにできるだけ早くもとの正常な状態に機能回復させる「復旧・修復」のシステムからなる．このうち「被害拡大の防止」と「避難」からなる並列系の部分は，典型的なフェイルセイフシステムを構成しており，避難は，被害拡大の防止ができなかった場合（フェイルセイフシステムの自体での故障の発生）の，安全側の出力として位置づけられる．

4. フェイルセイフシステムとしての都市のブロック化

都市が地震に襲われた場合の被害には，建物のライフラインの倒壊や破損といった直接害の他に，地震火災による被害や交通や電気，ガス，水といった物流やエネルギーの供給停止で発生する被害がある．これらに対して，図2の「被害拡大防止」と「避難」からなるフェイルセイフのシステムを都市に組み込み，うまく機能させる方法として，都市を被害拡大に対して相互に独立な地区に分割しておくブロック化法がある．このブロック化は，図1で示したフェイルセイフの設計方法の中では，(b)の分割構造に該当するものである．

地震火災による被害拡大をおさえるには，まず火を消すことである．これには市民が自力で行なう市民消火と，公設消防力による消火・延焼防止活動があるが，道路が使用できる程度の災害状況の場合は，公設消防力による消火活動が有効な働きをする．しかし，消防力も都市防災でのフェイルセイフのシステムではあるが，地震時にはライフラインの破壊が起こり，道路交通の遮断や消防水利の供給停止などで，消防力が十分に活動できない場合も十分想定される．そのような場合に備えて，都市の物理的構造物によって火災の延焼被害を防ぐために，不燃建築物や広幅員の道路，オープンスペースなどでつくる防火帯によって，延焼のおそれのある地域を分割しておく方法が，都市のブロック化である．これは建物の火災安全では，区画化（コンパートメンテーション：Compartmentation）として普及している安全設計法であり，不燃材料でできた壁で建物内を細かく区画化し，開口部には防火戸（扉）や防火シャッターなどを装置し，火災時にはそれらを閉じて火災を封じこめ，火災被害を一定規模以内に収めてしまう対策である．

一方，ガス，水道といったネットワーク形態でサービスが行なわれるライフライン施設でも，地震時管路網破損による供給停止被害の軽減を図るために，管路網のブロック化が有効な対策となる[4]．これは管路網に供給遮断装置（バルブ）を取りつけていくつかの小ブロックに分断できるようにしておき，地震時に早急に修理できず他のブロックにも影響をおよぼすような管路破損が発生したブロックのみを供給停止（孤立化）し，その他のブロックには引き続き供給を継続し，供給停止の被害を受ける戸数の軽減を図ろうとするものである．このようなブロック化が効果があるのは，管路破損に地域的なかたよりがある場合で，供給エリア全域にわたって多数の管路破損が発生する大地震での有効性まで求めるものではない．しかしこのブロック化は復旧過程においても効果を発揮し，すべての破損箇所は修復完了を待たずとも修理点検を終えたブロックから順次供給を再開していけるので，ブロック化がされていない場合に比べ，各戸の平均供給停止日数が短縮される．

火災の延焼のおそれがある地域，および管路破損の発生のおそれがある供給管路網の双方のブロック化ともに，それぞれどのような大きさのブロックに分類しておけばよいかが，安全設計上の課題となる．出火や管路破損の発生場所といった直接被害の発生場所があらかじめ特定できる場合は，危険物の隔離と同じ考えで，その範囲だけをブロック化すればよい．しかしそれら直接被害の発生場所とそれによって引き起こされる間接被害（延焼被害，供給停止被害）の規模は，地盤条件や世帯数（戸数）などの違いから，地域的に変化することが普通である．またブロック化の数もできるだけ細かく分割できていることが安全側の措置となるが，コストなどの制約から，ある一定規模までしかできないことが一般的である．このブロック化の仕方については，定められた分割数のもとでは，分割されたブロック相互の被害量期待

値が等しくなるように分割することにより，全体の被害量期待値の和にも最小値が与えられる[5].

次に避難は，都市が地震災害に襲われた場合に，人命の安全確保のために最後にとられるフェイルセイフの手段である．避難途中の道路での安全が保証される場合，避難問題は物流問題と同じになる．与えられた避難地に避難が必要な人々をできるだけ早く移動させるため，どこの人をどの避難地に向かわせたらよいかの問題は，人々の総移動量（∑人数×移動距離）の最小化をもたらす住民の避難地への配分問題となり，それはＬＰ問題として定式化される．しかし，避難途中の火災の延焼状況によって避難経路の安全が左右される場合や，また近い所や行き慣れているところに避難したいといった住民感情を考慮して計画する場合には，個別の計画ごと，火災の延焼状況と人々の避難の状況を組み合せたシミュレーションを行ない，計画の妥当性が検討される．

しかし避難は，できれば避難などしなくて済む状況が最も望ましい．避難においても，避難が必要になる地域，すなわち木造家屋が密集連続するような地域を防火帯によってブロック化しておくことが，避難を少なくし，また容易に行なわせるうえでもきわめて有効な方法となる．地域を防火帯で細かく分割しておけば，分割された全部の地区で同時に延焼火災が発生する確率はかなり低くなり，内部に延焼火災が発生し，避難が必要となる地区については，隣接する地区の中で1件も延焼火災が発生しなかったところに避難すれば，遠い避難地にゆかずとも安全な避難が可能となる．ブロック化を細かく行なうことで，この避難の安全度は大きく向上し，それは簡単な確率計算で確かめられる[6].

最後に，先にも述べたように，供給管路網の復旧・修復についても，その都市的なネットワークをブロック化しておくことが，供給停止被害の軽減のためにも有効な働きをする．その時のブロック化の仕方は，修復期間中の被害を復旧所用時間×需要家数などで表わしたときに，一定の分割数での対象エリアの最適な分割の仕方として，分割されたブロック相互での被害量が等しくなるような分割が，ここでも全体としての被害量に最小値をもたらす分割になる[7].

5. ブロック分割の規準とその効果の算定

地震火災による延焼危険を例にして，以上に説明したブロック化法について，均質・一様な地域条件が成立するとした場合の，ブロック分割の規準とその効果を計算によって示す．対象には木造家屋（世帯）が連続密集している地区をとりあげ，そこでは1件でも延焼火災が発生するとその地区すべてが延焼し，また人々はその地区の外には避難できないものとする．

地震時に延焼火災が発生する確率は各世帯を通じて一定 p をとり，各世帯での延焼火災発生は確率統計的に独立であるとした場合，n 世帯からなる地区で x 件の延焼火災が発生する確率 P_x は，平均 $m=np$ 件のポアソン分布で与えられる．

$$P_x=m^x\cdot e^{-m}/x! \tag{1}$$

ただし，$m=np$，$x=0,1,2,\cdots$

n 世帯数からなる地区で，1件以上の出火がある確率は $1-P_0$ となるので，n 世帯からなる地区の焼失世帯数（被害量）期待値 $f(n)$ は，次式で表わされる．

$$f(n)=n(1-P_0)=n(1-e^{-np}) \tag{2}$$

いま，木造家屋の連続する世帯数 A なる地区を，防火帯により世帯数 n と $A-n$ の2つのブロックに分割した場合，地区全体の被害量期待値 Q，その1次微分 dQ/dn は，次式で与えられる．

$$Q=f(n)+f(A-n) \tag{3}$$

$$dQ/dn=f'(n)-f'(A-n) \tag{4}$$

(4)式は，$n=A-n$，すなわち $n=A/2$ において $dQ/dn=0$ となり，Q はそこで極値をとる．そして $f'(n)$ が $0<n<A$ で増加関数であれば，$0<n<A/2$ で $dQ/dn<0$，また $A/2<n<A$ で $dQ/dn<0$ となるので，この極値は最小値となる．$f(n)$ が(2)式で与えられる場合に，$f''(n)$ は(5)式で与えられる．したがって $Ap<2$ の時には，$0<n<A$ において $f''(n)>0$ が成立し，$f'(n)$ は増加関数となり，$n=A/2$ での分割の被害量期待値に最小値が保証される．

$$f''(n)=pe^{-np}(2-np) \tag{5}$$

しかし，$n=A/2$ で $f''(n)<0$ の場合，すなわち $Ap>4$ の場合には，$n=A/2$ である分割の方が極大値を与えてしまうことになる．

4000世帯（$A=4000$）の木造家屋が連続する地区を例にして，ブロック化の効果を計算で示す．いま，世帯当りの延焼火災出火率が $p=1/5000$ であり（$Ap=0.8$），地区に何のブロック化もない場合，この地区の被害量期待値は $Q=4000(1-e^{-0.8})=2203$ である．これを防火帯により相互に延焼のない2000世帯の2ブロックに分割した場合，その被害量期待値は，$Q=2\times2000(1-e^{-0.4})=1319$ に減少する．またこれを1000世帯と3000世帯のブロ

ックに分割しておいた場合には，$1000(1-e^{-0.2})+3000(1-e^{-0.6})=1535$ である．これが $p=1/500$ のとき，すなわち $Ap=8$ の場合には，何もブロック化がされてない場合の被害者期待値が $Q=3999$，それを2000世帯ずつの2ブロックに分割した場合は，$Q=3927$ となり，この時は，1000と3000の2ブロックに分割した場合の期待値，$Q=3857$ を上まわる結果になる．

なお，$p=1/5000$ の場合で，ブロック化が何もない状態の（避難）安全度を，そこで延焼火災が1件も発生しない確率で表わせば，それは $e^{-0.8}=0.449$ となる．そこが2つのブロックに分割されている場合，一方で火災の発生があってももう一方でなければ，そこに避難することで安全が確保されるものとすれば，2000世帯の2ブロックからなる地区の避難安全度は，双方のブロックとも火災発生がある場合の排反事象の確率として，$1-(1-e^{-0.4})^2=0.891$ で与えられる．

6. おわりに

扱うシステムの作動を確実にするための技術として，冗長設計をはじめとする信頼性設計があり，そのシステムが故障などを起こした場合に，少なくとも人間には危害が及ばないようにするための安全装置をつくるフェイルセイフ設計がある．そしてこのフェイルセイフの装置の作動を確実にするために，そこにまた冗長設計が用いられる．すなわち安全設計には，冗長設計の入れ子構造の繰り返しが本質的に起こり，この冗長という余裕をどれだけとったらよいかについては，余裕（過剰）設計での安全係数と同じく，その合理的な決め方は存在しない．

都市防災のための安全設計では，たっぷり余裕をとっておく余裕設計と，フェイルセイフの設計が基本になろう．フェイルセイフの設計としては，都市をブロック化しておくことが（どこまで細かく分割すべきかは別の問題として），被害拡大の防止から始まり，避難，そして復旧のシステムにおいても，各々の効果をあげるために一貫して有効な方法となる．このブロック化は，都市をそれぞれに独立な小さなブロックに分割しておくことであるから，当然これも，都市を並列冗長のシステム構成にしておくことと同じになる．

都市のような，電子機器とは異なるマクロなシステムについての安全設計は，ブロック化でみられるような，その物理的構成を単純で維持管理の楽な頑強な構造，すなわちロバスト（robust）な構造にしておくことが基本であろう．このようなブロック化が有機的かつ階層的に行なわれていけば，それは停電，断水，交通渋滞などの都市の機能を阻害する日常的な「故障」にも対応できる装置となり，いずれは都市のフォールトトレランス設計（耐故障設計）と呼ばれるものになろう．

参考文献

[1] 小野寺勝重：保全性設計技術，日科技連，1989.10

[2] 当麻喜弘，南谷　崇，藤原秀雄：フォールトトレラントシステムの構成と設計，槇書店，1991.3

[3] 近藤次郎：安全を設計する，講談社，1979.11，pp. 160-164

[4] 小林正美：地震に対する都市ライフラインシステムのブロック化に関する基礎的研究，ガス，水道供給管路網のブロック化，都市計画学会学術研究発表会論文集，第17号，1972.11，pp.547-552

[5] 小林正美：地震火災に対する都市のブロック化に関する基礎的研究，日本建築学会大会学術講演梗概集，1972.10，pp.2189-2090

[6] 小林正美：広域避難計画論，防火帯地区分割に基づく避難計画，日本建築学会論文報告集，1971.8，pp. 126-132

[7] 能島暢呂，亀田弘行：ライフライン・ネットワークの震後復旧における最適戦略に関する基礎的研究，京都大学防災研究所年報，第34号，B-2，1991.3，pp. 27-44

＜事務局インフォメーション＞

●平成5年度秋季研究発表会(つくば)開催予定場所・日程変更のお知らせ!!

すでに12月号イエローページでお知らせしました場所・日程（含RAMPシンポジウム）は，事情変更により少し変わることとなりました．詳細は本月号巻末イエローページをご覧ください．