カスケード故障に対する意図的ノード除去による防御策の効果

杉下　佳辰[1]・日下部　貴彦[2]・朝倉　康夫[3]

[1]学生非会員　東京工業大学大学院　理工学研究科土木工学専攻（〒152-8552 東京都目黒区大岡山2-12-1-M1-20）
E-mail: k.sugishita@plan.cv.titech.ac.jp

[2]正会員　東京工業大学助教　理工学研究科土木工学専攻（〒152-8552 東京都目黒区大岡山2-12-1-M1-20）
E-mail: t.kusakabe@plan.cv.titech.ac.jp

[3]正会員　東京工業大学教授　理工学研究科土木工学専攻（〒152-8552 東京都目黒区大岡山2-12-1-M1-20）
E-mail: asakura@plan.cv.titech.ac.jp

局所的な故障源から過負荷故障がネットワーク内を波及していく現象をカスケード故障と呼ぶ．ネットワークの繋がり方によっては，たったひとつのノードの故障がネットワーク全体に壊滅的な損害をもたらし得ることが明らかになっているが，カスケード故障に対するひとつの有効な防御策として，意図的ノード除去による防御策（Intentional Removals, IRs）が提案されている．これは，局所的故障の発生直後に，ある一定の割合で媒介中心性の低いノードを意図的に除去する防御策である．本研究では，媒介中心性の高い複数のノードが選択的に攻撃された場合のIRsによる防御効果を評価した．この結果，より多くの媒介中心性の高いノードが選択的に攻撃された場合，それに応じて高い割合で媒介中心性の低いノードを除去することでより効果的に損害を抑制できることを確認した．

Key Words : *Cascading failures, Defense strategy, Intentional Removals,Targeted attacks*

1. 序論

現代社会にはインターネットなどの通信網，電力供給網，そして道路網，鉄道網，航空網を含む交通網など，ありとあらゆるものがネットワークとして存在している．これらのネットワークは相互に依存しあって機能し，我々の生活をより豊かなものとしている[1)]．しかし，近年になって，このような複雑な相互依存性をもつシステムに潜む危険性に注目が集まるようになってきた[2)]．Helbing[3)]はこのようなシステムの複雑性が増大すればするほど，そして，相互の依存性が強まれば強まるほど，システム全体が不安定かつ制御不能な状態に陥る危険性が高まると指摘している．現実社会に莫大な被害をもたらした実例としては，2003年に発生したイタリア大停電が挙げられる．Buldyrev et al.[4)]は，この大停電は，電力供給網と通信網の相互依存性によってより広範囲に渡って拡大したと指摘している．Bacher and Näf[5)]によれば，この停電は，スイスにおいてたったひとつの電線が強風によって倒れた木によって断線し，これが電力供給網の流れを変えたことで他の電線に負荷がかかって過負荷によって故障し，この過負荷故障がイタリアの広範囲に渡って拡大したことが原因であると報告している．電力供給網の障害が，電力の供給によって機能する通信網の障害をもたらし，その一方で，通信網によって制御されている電力供給網が適切な制御を受けられずに障害がより拡大してしまったということである．このように，局所的な故障源から過負荷故障がネットワーク内を波及していく現象をカスケード故障（Cascading failures）と呼ぶ．カスケード故障は電力供給網に限って生じる現象ではなく，ネットワーク内に流れが存在する全てのネットワークにおいて生じ得る現象であるため，カスケード故障という現象の理解は重要である．

カスケード故障に関する研究はおよそ10年に渡って集中的に行われてきた．Motter and Lai[6)]はノードに容量を設定し，そのノードにかかる負荷が容量を超えた場合に過負荷によって故障すると考え，ノードの過負荷故障がネットワークを伝搬するモデルを提案した．また，たったひとつのノードの故障がネットワーク全体に壊滅的な損害をもたらし得ることも示した．Crucitti et al.[7)]は，リンクの効率性を設定し，ノードにかかる負荷がノードの容量に漸近した場合に，そのノードの持つリンクの効率性を

低下させることで，リンクの効率性の低下が次々と発生する現象をモデル化した．Simonsen et al.[8]は，より動的なフローを考慮した場合には，ある定常状態から別の定常状態に移る際の過渡現象がネットワークのカスケード故障に対する脆弱性を高めることを示した．Sugishita et al.[9]は，相互依存性をもつネットワークの依存の度合いがネットワークのカスケード故障に対する脆弱性に与える影響を分析し，弱い依存性が脆弱性を急激に高める可能性があることを示した．また，Sugishita et al.[10]は，ネットワーク内で部分的なノードの容量低下が発生した場合のネットワークの脆弱性に与える影響を分析するモデルを提案した．

カスケード故障をモデル化する研究に加えて，カスケード故障に対する防御策についても考えられている．容易に想像できる防御策として，ネットワークに新たなノードやリンクを追加したり，ノードの容量を増大させてネットワークを頑強にする予防的な防御策が考えられる．しかし，このような策は，多くの場合，実行するのにコストや時間がかかってしまうものと思われる．そこで，より少ないコストや時間で実行可能な策として，Motter[11]は，局所的故障の発生直後にネットワーク内の媒介中心性の低いノードをある一定の割合で除去する策（Intentional Removals, IRs）を提案している．媒介中心性は，そのノードが他のノード間の流れをどの程度媒介しているかを表す指標であるが，この指標値が低いということは，そのノードが他のノード間の流れの媒介に貢献していないにも関わらず，そのノードからの流れの発生，及び，そのノードへの流れの集中を生んで，他のノードに負荷をかけているノードであるとみなすことができる．そこで，この防御策IRsは，局所的故障発生直後にこれらのノードをある一定の割合で，あえて除去することで，他のノードにかかる負荷を減らし，最終的なダメージを軽減するという戦略に基づいた防御策である．

本研究では，ハブへの攻撃に脆いとされるスケールフリーネットワークを分析対象とし，複数のハブへの選択的攻撃に対しては，ノードの容量を増大させる事前的防御のみで耐えることは難しいことを示すと同時に，このような攻撃による損害を抑制するためには，比較的大きな除去率でIRsを講じることが効果的であることを示す．

2. 本研究の手法

本章では，本研究で用いる手法について説明する．第1節a)ではMotter and Lai[6]が提案するカスケード故障モデルについて説明し，b)ではネットワークが受けた損害の評価指標を示し，c)では選択的ノード攻撃について説明する．そして，第2節ではMotter[11]が提案するカスケード故障に対する意図的ノード除去による防御策（Intentional Removals, IRs）について説明する．

(1) カスケード故障

a) カスケード故障モデル

第2章第1節a)では，本研究で用いるMotter and Lai[6]が提案するカスケード故障モデルを説明する．

あるネットワークWが与えられている時，このネットワークWでは，単位時間ごとに，W内の同じ連結成分に属する全てのノードペア(i,j)間で単位量のフローが最短経路を通って流れると仮定する．このように仮定すると，ノードkにかかる負荷は媒介中心性に等しくなる．すなわち，負荷L_kは，

$$L_k = \sum_{i \neq k \neq j} \frac{\sigma_{ij}(k)}{\sigma_{ij}} \quad (1)$$

のようにかける．ここで，σ_{ij}はノードiからノードjの最短経路数であり，$\sigma_{ij}(k)$はσ_{ij}のうちノードkを通る最短経路数である．

次に，ノードの容量を定義する．ノードkの容量をC_kとする．C_kは一定であるとし，$L_k > C_k$が成り立った場合には，ノードkは過負荷によって故障すると考え，ネットワークから除去する．

今，初期状態$(t = 0)$のネットワークWを$W(0)$と表し，この状態でノードkにかかる負荷L_kを$L_k(0)$と表すことにする．この$L_k(0)$を用いてノードkの容量C_kは

$$C_k = (1 + \alpha)L_k(0) \quad (2)$$

で定義されるものとする．ここで$\alpha(\geq 0)$を耐久性パラメータと呼ぶことにする．$\alpha \geq 0$の条件は，$W(0)$ではどのノードも過負荷故障を起こしていないことを保障するものであり，言い換えれば$L_k(0) \leq C_k \forall k$を成り立たせる条件である．本研究では，この$W(0)$の状態から局所的故障，及び，過負荷故障によってノードが次々と除去されていく現象をカスケード故障と呼ぶことにする．

局所的故障は$t = 1$で発生すると考え，あるノードを$W(0)$から除去する．この除去によってできるネットワークを$W(1)$で表す．これによって，$W(0)$の状態から除去されたノードを通過していた流れの最短経路が変化し，新たに別のノードに負荷がかかることになる．すなわち，ネットワーク全体で負荷が変わる．そこで$W(1)$の状態でノードkにかかる負荷$L_k(1)$を計算する．更新された$L_k(1)$について，$L_k(1) > C_k$が成り立つノードは過負荷によって故障すると考え，$W(1)$から除去する．これによってできたネットワークを$W(2)$とする．これにより，さらにネットワーク全体の負荷が変わり，新たに過負荷故障を起こして$W(2)$から除去されるノードが生じ，ネットワークが$W(3)$に更新される．このように連鎖的な過負荷故障が発生しネットワークが更新されていく．$t = n$のネットワークを$W(n)$と表すことにすると，

この故障の連鎖は，$t = n'$で$W(n')$のすべてのノードkにおいて，$L_k(n') \leq C_k$が成り立ったときに止まり，ネットワークは$W(n')$の状態に落ち着く．なぜなら，ノードが除去され，OD間に経路がなくなれば，そのODのフローはネットワークに負荷されないため，ノードが除去されるにつれて負荷も減少していくためである．

以上のように，ネットワークで局所的故障が発生し，これがトリガーとなり，連鎖的な過負荷故障によってノードが次々と除去されていくモデルがMotter and Lai[6]が提案するカスケード故障モデルである．

b) 評価指標

第2章第1節a)の$W(n')$に落ち着いたネットワークにおいてネットワークの受けた損害を評価する．評価指標は，$W(n')$での最大連結成分（ネットワーク内で最も大きなノードの塊）の大きさ（ノード数）を$W(0)$での最大連結成分の大きさで割った値をSとし，これを評価指標とする．すなわち，$W(0)$でのネットワークは必ずしも連結である必要はない．Sが大きければ大きいほど，$W(n')$における最大連結成分の相対的な大きさが大きいことを意味し，ネットワークが受けたダメージが小さいと解釈できる．

c) 選択的ノード攻撃

第2章第1節a)では，局所的故障として，「あるノードを$W(0)$から除去する」と表現したが，この「あるノード」を本研究ではネットワーク内の中心的なノードとする．そしてそれらを選択的に攻撃して$W(0)$から除去することを考える．本研究では，媒介中心性が高いノードを中心的なノードと考えて選択的に攻撃する．前述のとおり，媒介中心性の値が大きければ大きいほど，他のノード間の流れの媒介に貢献していると捉えることができ，その貢献度が高いノードをネットワーク内の中心的なノードであるとみなすことができる．選択的ノード攻撃とは，ネットワーク内で流れの媒介の観点から中心的な役割を担うノードを狙った攻撃と定義する．ここで，媒介中心性が高い方からノードを順に並べ，全ノード数に占める割合がpとなる数のノードを選んでネットワーク$W(0)$から除去することを指す．例えば，ノード数が100のネットワークにおいて，$p = 0.05$で選択的攻撃を行った場合，媒介中心性の高い方から5つのノードを選択して$W(0)$から除去する．本研究では，このpを攻撃率と呼ぶことにする．

(2) 意図的ノード除去による防御策

本研究で用いる，Motter[11]が提案する意図的なノード除去によるカスケード故障に対する防御策(Intentional Removals, 以下IRs)について説明する．

カスケード故障に対する防御策は，大きく分けて事前防御策と事後防御策のふたつに分けることができる．事前防御策としては，局所的故障が発生する前に，ネットワークにノードやリンクを追加する策や容量を増大させる（第2章第1節a)の耐久性パラメータαを大きくする）策などが考えられる．一方で，カスケード故障発生後に故障の拡大を抑えるものが事後防御策である．IRsはこの事後防御策のひとつである．事前防御策であるノードやリンクの追加，および，容量を増大させる等の策は，一般的にはコストや時間がかかるものだが，IRsはより少ないコストや時間で実行可能と考えられる．

本研究では，局所的故障の発生直後，連鎖的故障の進展前，すなわち第2章第1節a)のネットワークが$W(1)$から$W(2)$に移るその間に，時間遅れを伴うことなく防御策を講じることができると仮定する．局所的故障発生直後に，ネットワーク内の媒介中心性の低いノードをある一定の割合fで除去することを考える．媒介中心性が小さいほど，流れの媒介に貢献しておらず，その一方で流れを発生，集中させて他のノードに負荷をかけているノードとみなすことができるため，このようなノードを意図的に除去することで，他のノードにかかる負荷を減らし，カスケード故障後のネットワークの最終状態（第2章第1節a)の$W(n')$）で生き残るノードを増やして最大連結成分を大きくするという防御策である．本研究では，このfを除去率と呼ぶことにする．攻撃率p, 除去率fを変化させて第2章第2節b)で説明した最大連結成分の相対的大きさSがどのように変化するかを分析する．

3. 分析

(1) 分析内容

スケールフリーネットワークに第2章で説明した手法を適用する．スケールフリーネットワークは選択的なハブへの攻撃に極めて脆い性質を持つことが知られている．防御なしでは壊滅的な損害をもたらすと推測される攻撃に対して，耐久性パラメータαを0.05,0.5, 1.0と増大させる事前防御策による防御効果を分析すると同時に，事後防御策IRsによってどの程度，損害を抑制できるかについても分析する．耐久性パラメータαを増大させることは，大きな容量でネットワークを設計してより効果的な事前防御を施すことに対応する．このネットワークに対して攻撃率pを増大させて攻撃することは，より多くのノードを選択的に攻撃していくことに対応する．IRsの除去率fを増大させることは，攻撃直後により多くの媒介中心性の低いノードを意図的に除去する防御策を講じることを意味する．そして評価指標であるSが増大することは，最終状態$W(n')$においてより大きな最大連結成分が存在できていることに対応する．

(2) 手法の適用

a) $\alpha = 0.05$の場合

耐久性パラメータ$\alpha = 0.05$と設定した場合の評価結果を図-1に示す．この条件設定は，初期状態$W(0)$においてノードkにかかる負荷L_kに対して，容量C_kには5%しか余裕がないことを意味するため，選択的攻撃に対して極めて脆いことが推測できる．図-1を見ても攻撃率$p = 0.002$，すなわち，最も媒介中心性の高いひとつのノードを攻撃した場合でも，$S \approx 0.01$ほどのダメージを受けており，ネットワークがほぼ分断されていることがわかる．しかし，除去率$f \approx 0.25$のIRsを講じることによって，$S \approx 0.63$程度まで向上できていることがわかる．さらにpを0.012まで増やした場合に対しても，$f \approx 0.75$程度の大胆なIRsによって，$S \approx 0.20$程度まで向上できることが確認できた．このように，攻撃率pが増大しても，一定の範囲まで除去率fを増大させることで，防御効果が高まることが確認できた．

b) $\alpha = 0.5$の場合

耐久性パラメータ$\alpha = 0.5$と設定した場合の評価結果を図-2に示す．この条件設定は，初期状態$W(0)$においてノードkにかかる負荷L_kに対して，容量C_kは50%程度の余裕があることを意味する．すなわち，5%しか余裕が無かったa)の状態から容量を45%増大する事前防御を施した場合と捉えられる．図-2の通り，この場合もa)と同様に，攻撃率pが大きくなるにつれてIRsの最適な除去率も増大していることがわかる．$p = 0.002$では防御なしでも$S \approx 0.71$程度の小さな損害しか被っていないが，$p = 0.006$では$S \approx 0.05$程度の大きな損害を受けている．すなわち，たとえ耐久性パラメータαを0.05から0.5へと増大させて事前防御を行ったとしても，たった3つのノードへの選択的な攻撃への抑制にはほとんど効果がないことを意味している．その一方で，事後的防御策の効果は期待できることがわかる．

c) $\alpha = 1.0$の場合

耐久性パラメータ$\alpha = 1.0$と設定した場合の評価結果を図-3に示す．初期状態$W(0)$においてノードkにかかる負荷L_kに対して，容量C_kは100%もの十分な余裕があることを意味しており，a)の状態から95%の容量増大による事前防御を施した状況と捉えられる．実際，$p = 0.002$の場合には，防御なしでも$S \approx 0.86$と損害はそこまで大きくなく，むしろIRsを講じることによって損害が大きくなってしまっている．一方で，$p = 0.010$とした場合には，防御なしの場合に$S \approx 0.02$程度の非常に大きな損害を被っていることがわかる．これは，たとえ耐久性パラメータを$\alpha = 1.0$と容量に大きな余裕を持たせてスケールフリーネットワークを設計したとしても，500のノードのうちたった5つのノードを選択的に攻撃することによって壊滅的な損害を引き起こすということである．すなわち，容量を増大させるなどの事前的な防御策のみによってスケールフリーネットワークをハブへの攻撃に対して頑強にすることは難しいことを示唆している．とりわけ複数のハブへの選択的な攻撃による損害を抑制するためには，場合によっては，$f \approx 0.60$程度の大胆なIRsを講じることによって事後的にネットワークを防御することが効果的であると言える．

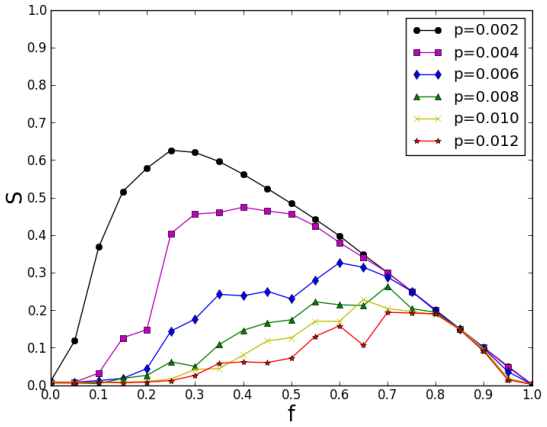

図-1 S, p, fの関係（$\alpha = 0.05$）

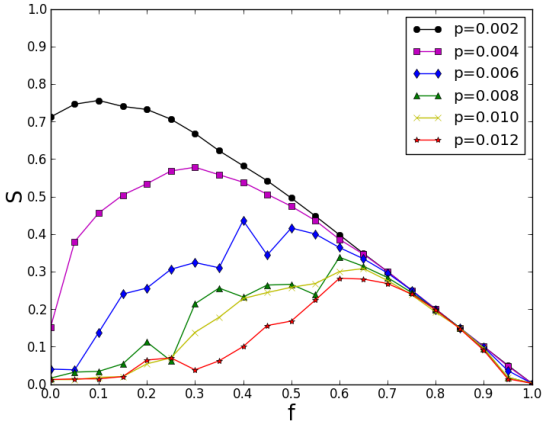

図-2 S, p, fの関係（$\alpha = 0.5$）

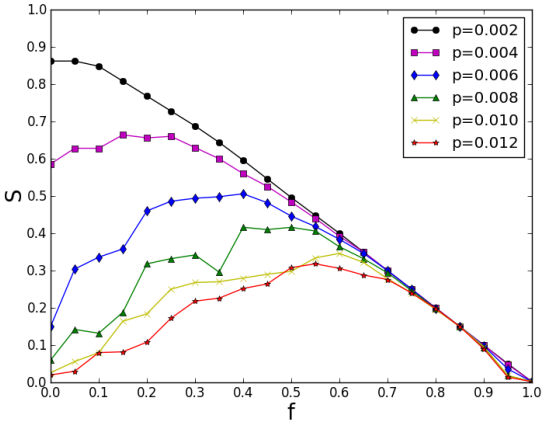

図-3 S, p, fの関係（$\alpha = 1.0$）

4. 結論

本研究では，媒介中心性の高い複数のノードが選択的に攻撃された場合，攻撃を受けた直後に媒介中心性の低いノードをある一定の割合で意図的に除去する防御策（IRs）の効果を検証した．その際，攻撃率pとIRsの除去率fの関係について考察した．その結果，pが増大する（より多くのノードを攻撃する）につれて，初期状態$W(0)$に対する最終状態$W(n')$の相対的な最大連結成分の大きさSを最も増大させることができる最適な除去率fも同様に増大することが確認できた．また，ネットワークが極めて脆弱な場合（例えば耐久性パラメータ$\alpha = 0.05$）でも，IRsによって効果的に損害を抑制できることが示された．さらに，スケールフリーネットワークにおいては，たとえ容量を大きく（例えば$\alpha = 1.0$）設定し，カスケード故障に対して事前的な防御策を施したとしても，複数のハブへの攻撃に耐えることは難しく，このような攻撃を抑制するためには，比較的大きな除去率fでIRsを講じることで損害を抑制することが効果的であることが示唆された．容量増大による事前防御策によってスケールフリーネットワークのハブへの攻撃に対する脆弱性を改善することは難しいが，攻撃を受けた直後に適切な防御策を講じることで，この脆弱性をある程度補える可能性が示唆されたと言える．

今後の方針として，意図的ノード除去の施行に遅れが生じた場合の影響について分析することが挙げられる．本研究では，意図的ノード除去は，$W(1)$と$W(2)$の間に，迅速に防御策を講じることができると仮定しているが，現実的には，このような迅速な策を行うことが難しい状況も考えられる．例えば，$\alpha = 1.0$のように耐久性パラメータが大きい場合は，壊滅的な損害に至るまでのタイムステップ数（n'）が大きくなると推測される．このような場合には，IRsに遅れが生じたとしても，効果的となる可能性がある．IRsの遅れによる影響を分析した研究はなく，今後の課題である．

参考文献

1) Rinaldi, S. M., James, P. P. and Terrence, K. K. : Identifying, understanding, and analyzing critical infrastructure interdependencies, *Control Systems, IEEE*, Vol. 21, No. 6, pp. 11-25, 2001.
2) Vespignani A. : Complex networks: The fragility of interdependency, *Nature*, Vol.464, No.7291, pp.984-985, 2010.
3) Helbing D. : Globally networked risks and how to respond, *Nature*, Vol.497, No.7447, pp.51-59, 2013.
4) Buldyrev, S. V., Roni, P., Gerald, P., Stanley, H. E. and Havlin, S. : Catastrophic cascade of failures in interdependent networks, *Nature*, Vol.464, No. 7291, pp.1025-1028, 2010.
5) Bacher, R. and Näf, U. : Report on the blackout in Italy on 28 September 2003, *Swiss Federal Office of Energy (SFOE)*, 2003.
6) Motter. A. E. and Lai, Y. C.: Cascade-based attacks on complex networks, *Physical Review E*, Vol. 66, p. 065102, 2002.
7) Crucitti, P., Latora, V. and Marchiori, M.: Model for cascading failures in complex networks, *Physical Review E*, Vol. 69, No. 4, p. 045104, 2004.
8) Simonsen, I., Buzna, L., Peters, K., Bornholdt, S. and Helbing, D. : Transient Dynamics Increasing Network Vulnerability to Cascading Failures, *Physical Review Letters*, Vol. 100, pp. 218701-218705, 2008.
9) Sugishita, K., Sakai, K. and Asakura, Y. : Vulnerability Assessment for Cascading Failures in Interdependent Networks, *3rd Symposium of the European Association for Research in Transportation (hEART)*, 2014.
10) Sugishita, K., Kusakabe, T. and Asakura, Y. : Cascading Failures in a Road Network depending on External Systems, *6th International Symposium on Transportation Network Reliability (INSTR)*, 2015.
11) Motter, A. E. : Cascade control and defense in complex networks, *Physical Review Letters*, Vol. 93, No. 9, p. 098701, 2004.
12) Barabasi, A. L. and Albert, R. : Emergence of scaling in random networks, *Science*, Vol. 286, No. 5439, pp. 509-512, 1999.

（？受付）

EFFECT OF INTENTIONAL REMOVALS OF NODES AS A DEFENSE STRATEGY AGAINST CASCADING FAILURES

Kashin SUGISHITA, Takahiko KUSAKABE and Yasuo ASAKURA

Cascading failures is a phenomenon where a local failure triggers a global propation of failures, leading to severe damage to the whole network. It is already shown that even if only a single node is broken, it can lead to catastrophic damage to the network. One important question is how we can defense and control cascading failures. One costless strategy of defense is known as Intentional Removals (IRs). This strategy is based on the concept of removing unimportant nodes intentionally right after a local failure in order to lighten the load of other nodes and to mitigate the damage eventually. This study investigates the performance of IRs against targeted attacks on several important nodes.