Computer Security Symposium 2016
11 - 13 October 2016

固有値解析を用いたネットワーク攻撃効果に関する考察

石丸 歩[1]　田中 秀磨[1]

概要：近年，情報通信技術の発展によって社会インフラがシステム上で管理されるようになりつつあり，それらを狙った大規模なサイバー攻撃が発生することが予想されるようになった．サイバー攻撃は不正な行為であるが，インターネット回線を通して行われている以上，国際標準規格が定める技術仕様に従わざるを得ない．そのため，サイバー攻撃は IP 情報も含めた攻撃者情報を有している．その IP 情報を用いて攻撃者ネットワークを導出し，行列の固有値解析によって攻撃の有効性を考察している先行研究が存在する．しかしながら，先行研究ではセキュリティレベルを考慮していない．本研究ではその課題の改善を Total Accessibility Matrix を用いて考察する．

キーワード：攻撃者情報，固有値解析，Total Accessibility Matrix

A study on effectiveness of network attack using analysis of eigenvalues

Ayumi Ishimaru[1]　Hidema Tanaka[1]

Abstract: Network communication is based on IP packets which are standardized by international organization. Therefore, Network attack does not function without following the standardized manner. Hence, Network attack also leaks adversaries' information in their IP packets. In previous studies, malicious topology maps are derived using these IP packet informations. And the effectiveness of Network attack is evaluated by increasement in eigenvalue of topology matrix (Adjacency matrix and Laplacian matrix). However, previous method does not consider security level of each node. In this paper, we propose the solution to this problem and the improvement of previous method using Total Accessibility matrix.

Keywords: Attacker information, eigenvalue analysis, Total Accessibility Matrix

1. 研究背景及び目的

近年の情報通信技術の進歩により，インターネットは今や我々の生活に欠かせないものとなった．同時にサイバー攻撃と呼ばれるインターネットの不正利用も増加しており，今後インターネットシステムが大規模化するほど大規模なサイバー攻撃が発生することが予想される．一方で，インターネット回線を利用している以上，サイバー攻撃もまた国際標準規格が定める技術仕様に従わざるを得ない．その結果として，サイバー攻撃は悪質なデータと同時に攻撃者に関する情報も有している．この事実に基づいて，ハニーポットプロジェクトやダークネット観測といった技術が存在する．それらはサイバー攻撃手法の解析や，大規模な攻撃の観測に利用されており，これらの観測に基づいてアクセス制限等の対策手段を講じている．このような攻撃観測データの受動的な利用は既に実施されている．しかしそれらの観測から得た情報を攻撃者に対して（カウンター）サイバー攻撃に利用するような能動的立場の先行研究は存在するものの希少であり，課題も多い．

本研究では，先行研究 [1] の課題の 1 つであった各ノードの攻撃耐性のパラメータ化を考慮して国家規模の組織を背景に持つクラッカー集団へのサイバー攻撃を考察する．攻撃耐性のパラメータ化にあたって，ネットワーク内の各ノードの重要性がセキュリティレベルの強度を表していると仮定し，各ノードの重要性を Total Accessibility Matrix

[1] 防衛大学校 理工学研究科
Graduate School of Science and Engineering, National Defense Academy

を用いて定量化する．定量化した結果から得られた各ノードの重要度をもとに，対象のネットワークに対して複数のノードを破壊する攻撃を行ったところ，攻撃シナリオ次第ではセキュリティレベルの低いノードを複数攻撃することでより高い攻撃効果を得られるということを発見した．

2. 複雑ネットワークの解析

複雑ネットワークは，世の中に実在するネットワークにおける，統計学的性質を研究する分野である [2]．先行研究 [1] ではネットワークダイナミクスとして発展している固有値を用いたネットワーク解析技術を応用している．本節では，その複雑ネットワークの解析技術について概略を示す．

2.1 隣接行列

G を n 個のノードを持つネットワークとする．G は $n \times n$ の隣接行列 A で表され，隣接行列の要素 $A_{i;j}$ $(1 \leq i; j \leq n)$ は以下のように表される．

$$A_{i;j} = \begin{cases} 1 & (i \text{ link to } j) \\ 0 & (\text{otherwise}) \end{cases} \quad (1)$$

ただし，$A_{i;i}$ は自身へのリンクを意味するので，$A_{i;i} = 0$ とする．i 番目のノードの次数は i 行に存在する 1 の総数である．なお，$A_{i;j}$ と $A_{j;i}$ は同じ値となる．大きな次数のノードをハブノードと呼ぶ．$\lambda(A)$ は以下の特性方程式から得られる隣接行列 A の固有値である．また，固有値 $\lambda(A)$ はそれぞれに対応する固有ベクトル $I(L)$ を持つ．

$$det(\lambda I - A) = 0 \quad (2)$$

これは n 次の特性方程式であるから，固有値は $m(1 \leq m \leq n)$ 個存在する．$\lambda_{max}(A)$ を λ の最大値とする．これはハブノード同士の連結度を示すので，$\lambda_{max}(A)$ はネットワークにおける“ 拡散速度”を表す．

2.2 ラプラシアン行列

ネットワーク G はラプラシアン行列 L によっても表される．$L_{i;j}(1 \leq i; j \leq n)$ はラプラシアン行列 L の要素である．

$$L_{i,j} = \begin{cases} d_i & (i = j) \\ -1 & (i \text{ link to } j) \\ 0 & (\text{otherwise}) \end{cases} \quad (3)$$

d_i は i 番目のノードの次数である．ラプラシアン行列 L の固有値は式 (2) に示す隣接行列の固有値と同様の方法で求められる．よって，ラプラシアン行列 L からは $m(1 \leq m \leq n)$ 個の固有値を得ることができ，最小固有値 $\lambda_1(L)$ は必ず 0 になる．この時，固有値 0 の固有ベクトルの成分は全て 1 になる．また，0 より大きく，他の固有値と比べて最小であるものを G の第 2 最小固有値 $\lambda_{min}(L)$ と呼ぶ．G が連結であるとは，ネットワーク上の任意の 2 ノード u, v に対して，u から v へ至るパスが存在することを指す．$\lambda_2(L)$ が正の値をとる場合に限り，G は連結である．このとき，$\lambda_2(L) > 0$ は G の第 2 最小固有値 $\lambda_{min}(L)$ である．

$$0 = \lambda_1(L) \leq \lambda_2(L) \leq ... \leq \lambda_{max}(L) \quad (4)$$

連結でないネットワークを非連結と呼び，固有値 0 の個数と同じ数だけネットワークを分割できることが知られている．例えば，$\lambda_2(L) = 0$ の場合，G は非連結となり，2 つに分割される．ネットワークの連結性を保持するためには，第 2 最小固有値 $\lambda_{min}(L)$ を正の値に保つことが必要である．このような性質から，第 2 最小固有値 $\lambda_{min}(L)$ は G の代数的連結度と呼ばれる．なお $\lambda_{min}(L)$ が大きい値をとるとき，ネットワークは高い連結性を持つ．また，最大固有値 $\lambda_{max}(L)$ は通信の遅延の起こりにくさを表す．これらの固有値比 $R = \lambda_{min}(L)/\lambda_{max}(L)$ によってネットワーク内の同期の起こりやすさが評価できる．固有値比 R が大きい値をとるとき，ネットワークの“ 収束”が起きやすくなる．

3. 先行研究の手法

先行研究 [1] では，サイバー攻撃が有している攻撃者情報を能動的に利用し，国家規模の組織を背景に持つクラッカー集団へのサイバー攻撃について考察している．先行研究では，クラッカーが存在する地域のネットワーク (敵国ネットワーク) を対象とし，攻撃シナリオに従って対象の弱体化を試みる．弱体化のための戦術は 3 通りあり，これら 3 つの戦術を実行した結果から得られるそれぞれの効果は，ネットワークの隣接行列とラプラシアン行列を用いた固有値解析手法により求められることが示されている．

3.1 攻撃シナリオの概要

サイバー攻撃がもたらす脅威のシナリオは数多く存在するが，先行研究では以下の 2 つのシナリオが示されている．

攻撃シナリオ 1： マルウェア及び偽情報の拡散
攻撃シナリオ 2： 情報の集中と混乱

攻撃シナリオ 1 の目的は，敵国ネットワークにマルウェアや偽情報を速やかに拡散させることにある．この攻撃シナリオでは，敵国ネットワークの複数のサーバーに対してマルウェアや偽情報を与え，隣接するサーバーやルーターを介して次々に情報が伝播していくような攻撃を想定す

る．攻撃シナリオ 2 の目的は，敵国ネットワーク内において，目標とする地域と他の地域の情報に差異を生じさせることで攻撃対象の情報を混乱させることにある．この攻撃シナリオは，インターネット技術の特性の一つである情報共有の即時性に基づいている．これは，うわさの伝播（または攻撃シナリオ 1 のようにマルウェアの伝播）と似ているが，いくつかの異なる情報を拡散させるという点において異なっている．例えば，異なる 2 つの情報を異なる方向から流すことで，収束地点では情報が混交して意思決定が困難になる．さらにこれを応用すれば，世論誘導や扇動を実行できる可能性がある．

これら 2 つの攻撃シナリオの効果は攻撃対象となるネットワークの固有値解析で見積もられる．攻撃シナリオ 1 の効果は隣接行列の $\lambda_{max}(A)$ が示す“ 拡散速度”で，また攻撃シナリオ 2 の効果はラプラシアン行列の固有値比 R が示す“ 収束”で評価することができる．攻撃者は敵国ネットワークを解析することで，より効率的な攻撃シナリオを選ぶことができる．

一方で，ネットワーク攻撃には DDoS 攻撃，XSS ，不正サーバーによるサービスの遅滞等の様々なものが存在する．これらの戦術では敵国ネットワークに影響を与え，形状や特徴に変化をもたらす可能性も存在する．それゆえ攻撃者は攻撃シナリオを選び，戦術ごとの効果を議論する必要がある．先行研究では以下の 3 つの戦術を考え，ネットワークの特徴を変化させている．

戦術 1： サーバー停止型（サーバー破壊）
戦術 2： リンク増設型（工作サーバー設置）
戦術 3： 複合型（サーバー破壊及び工作サーバー設置）

攻撃シナリオと 3 つの戦術を組み合わせて攻撃戦略と呼び，先行研究では攻撃目標の全数探索によって最適な攻撃効果をもつ攻撃戦略を導出している．

3.2 先行研究における課題

先行研究で提案された手法では，すべてのノードのセキュリティレベルが同等のものとして設定されており，さらに実質的にゼロに設定されている．しかし現実のネットワークではそれぞれのノードは独自の役割（ルーターや web サーバー，メールサーバー，クライアント等）を持つ．それゆえ，各ノードにはその役割に応じた固有のセキュリティレベルが与えられている．さらに，同じ役割を有した 2 つのノードがあったとしても，基幹ネットワークに属しているか末端のネットワークに属しているかで，それらのセキュリティレベルは異なる．結果として，セキュリティレベルは様々であり，統合的な方法によりそれらを設定することは現実的ではない．

そこで本研究では，先行研究で考慮されていないセキュリティレベルを推定するために，各ノードのセキュリティレベルがノードの重要性に依拠していると仮定した．先行研究では各ノードの重要性を評価しておらず，全数探索で攻撃をシミュレートしていたが，本研究では各ノードの重要性を定量的に評価し，その結果に基づいて攻撃対象ノードの探索を実行する．自明であるが，重要度の高いノードは攻撃が困難であり，低いノードは容易であると仮定する．

4. 攻撃耐性のパラメータの導出

第 3.2 節で述べた先行研究の課題を解決するために，本研究では Total Accessibility Matrix [3] を用いて各ノードの重要性を定量的に評価する．スケールフリーなネットワークは特定の重要なノードをピンポイントで狙った攻撃に対して脆弱である．その脆弱性をカバーするために重要度の高いノードに高いセキュリティレベルを設定することが一般的である．また，重要なノードほど何かが起こった際にはネットワークに大きな影響を及ぼすのは自明である．従って，より多くのパスを保有しているノードは重要性が高いと仮定すれば，Total Accessibility Matrix の評価値でこれを判断できる．

4.1 Total Accessibility Matrix

Total Accessibility Matrix とは，輸送システムのジオグラフィとして用いられるものであり，そのネットワークにおけるアクセシビリティを示すものである．これは，あるノードと他のノードを繋ぐためのリンクが消失したり，その 2 点間を中継するノードが破壊されるといった事態が生起した際，それ以外のノードやリンクを使用したパスがどれだけ存在するかを示すものである．

Total Accessibility Matrix (T) は，隣接行列から導出することができる．n 個のノードを有するネットワーク G があったとき，ネットワーク G は $n \times n$ の隣接行列 A で表される．このとき，ネットワーク G 内に存在する 2 ノード間の距離の中で最長のパス（ネットワークダイアメータ）を l として，

$$T = A + A^2 + A^3 + ... + A^l \tag{5}$$

となる．式 (5) によって導出された Total Accessibility Matrix (T) の各行について和を算出する．各行はそれぞれネットワークのノードを示しており，算出された行の値の和が，ネットワーク G における各ノードのアクセシビリティを表している．この値が大きいほどより多くのパスを有しており，アクセシビリティが良好であるということになる．以下，i 行目（i 番目のノード）のアクセシビリティの評価値を $\Sigma_i(T)$ と表す．

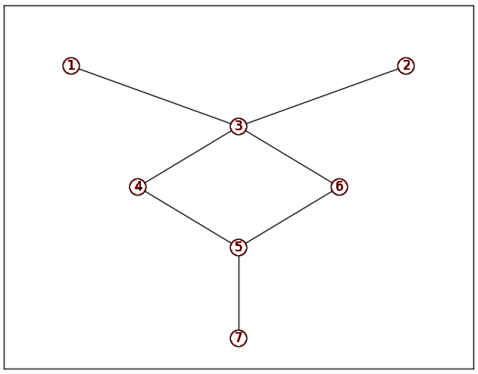

図 1　7 ノードのネットワーク

Fig. 1　7 node network.

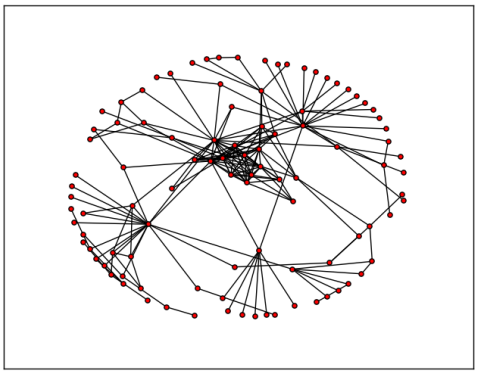

図 2　C 国首都近辺 100 ノードによるネットワーク

Fig. 2　100 node network of capital area in country C.

4.2　計算例

図 1 に示す 7 ノードのネットワークを用いて，各ノードのアクセシビリティの算出例を示す．この図から以下の隣接行列 A を得ることができる．

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \tag{6}$$

図 1 より $l = 4$ であるから，このネットワークにおける Total Accessibility Matrix(T) は，式 (5) から以下のように導くことができる．

$$\begin{aligned} T &= A + A^2 + A^3 + A^4 \\ &= \begin{pmatrix} 5 & 5 & 5 & 7 & 2 & 7 & 2 \\ 5 & 5 & 5 & 7 & 2 & 7 & 2 \\ 5 & 5 & 24 & 7 & 16 & 7 & 2 \\ 7 & 7 & 7 & 13 & 6 & 13 & 6 \\ 2 & 2 & 16 & 6 & 16 & 6 & 4 \\ 7 & 7 & 7 & 13 & 6 & 13 & 6 \\ 2 & 2 & 2 & 6 & 4 & 6 & 4 \end{pmatrix} \end{aligned} \tag{7}$$

式 (7) における T の各行の和が，各ノード i のアクセシビリティ $\Sigma_i(T)$ を示している．このネットワークの場合は以下の通りとなる．

$$\begin{aligned} &\Sigma_1(T) = 33 \quad \Sigma_2(T) = 33 \quad \Sigma_3(T) = 66 \\ &\Sigma_4(T) = 59 \quad \Sigma_5(T) = 52 \quad \Sigma_6(T) = 59 \\ &\Sigma_7(T) = 26 \end{aligned}$$

アクセシビリティはノードの次数と大きく関係しているが，第 1 ノードと第 7 ノードの比較から，同じ次数であっても異なる場合があることが分かる．これは，各ノードのアクセシビリティがリンクしている先にあるノードのアクセシビリティとも関連があることが理由である．従って，単に次数の大小を基準にするよりもノードの重要性を表しているため，本研究の目的に合致していると考えられる．

5.　本研究における実験

本研究では結果を比較するため，先行研究 [1] で用いたデータと同じものを用いる．

先行研究でのデータの取得方法は以下のとおりである．まず，防衛大学校のダークネット観測により C 国からの IP アドレスを抽出し，合計 3,674 個の IP アドレスを得た．次に *traceroute* コマンドを実行し，経路情報に欠損の生じなかった計 2,119 件の IP アドレスをデータとして利用し，対象のネットワークを推定する．結果として，先行研究では 2,119 個の IP アドレスを持ち，3,819 本のリンクを持つネットワークを推定している．しかし，この規模のネットワークを解析するには計算能力が不足していたとして，先行研究ではネットワークを C 国の首都部と見られる地域に限定し，ノード数 100 個，リンク数 187 本のネットワークが攻撃対象となった（図 2 ）．先行研究は，この推定されたネットワークに対して攻撃をシミュレートし，攻撃効果を向上させる攻撃シナリオと戦術の組み合わせを考察した．先行研究では戦術 1 において攻撃対象のノード数は 1 であり，戦術 2 では増設する工作サーバー数が 1 ，リンク数は 2 であった．本研究では戦術 2 は実行せず戦術 1 のみとし，攻撃対象のノード数を原則 3 個までとして実験を行う．

実際の攻撃は，踏み台のサーバーを介して実行されることが多く，クラッカーの IP アドレスを直接知ることは困難である．しかしながら，踏み台 PC が意図的に攻撃に参

加していない場合であっても，実際にダークネットにアクセスを実行したので，先行研究と同様に本研究においてもクラッカーとしてみなす．ただし，いくつかの踏み台サーバーの検知方法が既に知られている [4], [5], [6].

5.1 攻撃耐性を考慮したネットワーク実験

5.1.1 Total Accessibility Matrix の導出

先行研究と同様の手法により敵国ネットワークを導出し，隣接行列 A を求める．この行列をもとに，第 4 節で示した手法を用いて Total Accessibility Matrix を導出する．本研究では，ネットワークダイアメータ l を Python の *diameter* コマンドで算出した．これは，先行研究と同様に Python によるプログラムを利用しているためである．その結果，$l = 7$ であった．この値をもとに Total Accessibility Matrix によって各ノードの $\Sigma_i(T)$ を求めた結果を図 3 に示す．図 3 の横軸はノード（横軸には 100 個ノード並んでいるが，図 3 では紙面の都合上すべてのノード番号は記載されていない.），縦軸は $\Sigma_i(T)$ を示す．

本研究の方針から，重要度でソートした方が都合が良いので，図 3 は $\Sigma_i(T)$ の小さい順に並べている．この図から，ネットワーク内のノードのアクセシビリティ $\Sigma_i(T)$ は昇順から 69 番目のノードを境に大きく上昇を始めていることが分かる．よって，ネットワーク内のアクセシビリティを表す数値の閾値を 69 番目のノードが有する $1.75E+06$ として設定した．つまり，以降では $\Sigma_i(T) < 1.75E+06$ のノードは重要ではないので攻撃が容易であり，$\Sigma_i(T) \geq 1.75E+06$ のノードは重要度が高いため攻撃が成功する確率は低いと仮定する．

5.1.2 ネットワーク内のノード破壊

前述のように，本研究では戦術 1 のみを実行する．ただし，攻撃対象とするノードは $\Sigma_i(T) < 1.75E+06$ から 2 個又は 3 個の場合と，$\Sigma_i(T) \geq 1.75E+06$ から 2 個又は 3 個の場合に分け，攻撃を実施した結果の比較を行う．従って，計 4 通りの戦術 1 を実行した．その実行の計算コストを表 1 に，その結果を表 2 に示す．なお，本実験は Windows 10 Home 64bit，Intel(R) Core(TM) i7-6700CPU @ 3.40GHz，実装メモリ 8.00GB，プログラムは Python 3.5.1 (Anaconda4.0.0) の計算環境で実施した．計算コストの単位は固有値の計算回数であり，$\lambda_{max}(A)$ と R を同時に出力するプログラムである．ノードを破壊する際に要した時間は，2 個の場合は $\Sigma_i(T) < 1.75E+06$ と $\Sigma_i(T) \geq 1.75E+06$ のプログラムを同時に実行して約 1 時間であり，3 個破壊する場合も同様にして約 1 日程度要した．

表 2 において，「単一破壊」は先行研究の手法による結果と同じである．先行研究 [1] では，$\lambda_{max}(A)$ の初期値と攻撃結果に変化がない点について詳細な考察がなされている．また，R に関しては，図 3 において 50 番目のノード（ノード番号 38 ，$\Sigma_i(T) = 5.12E+05$ ）を攻撃対象としたことが示されている．

表 1 各計算実施における計算コスト
Table 1 Cost of caluculation

破壊ノード個数	計算コスト
1 個（先行研究）	100
2 個	
$\Sigma_i(T) < 1.75E+06$ の場合	2,278
$\Sigma_i(T) \geq 1.75E+06$ の場合	496
3 個	
$\Sigma_i(T) < 1.75E+06$ の場合	50,116
$\Sigma_i(T) \geq 1.75E+06$ の場合	4,960

表 2 ノード破壊結果
Table 2 Results of crush nodes

破壊ノード	$\lambda_{max}(A)$	R
初期値	10.0785	0.005487
単一破壊	10.0785	0.005950
2 個破壊		
低いノード	10.0785	0.006012
高いノード	8.1784	0.003868
3 個破壊		
低いノード	10.0785	0.006455
高いノード	7.5304	0.000973

5.2 考察

5.2.1 拡散速度 $\lambda_{max}(A)$

先行研究 [1] で示されているように，攻撃シナリオ 1 において戦術 1 の効果はないことが解析されている．ネットワークはノード数 n とリンク数 l で決定される．ここから，固有値が最大となるネットワークも一意に決定され，その時，隣接行列の最大固有値 $\lambda_{max}(A)$ は $n-1$ となる．一方，与えられたネットワークはリンク数 l が制限されている．完全グラフよりもリンク数が増えるネットワークは存在しないので，リンク数の最大値は $l_{max} = {}_nC_2$ となる．このように n の値が決定されるとリンク数の最大値が決定される．これを戦術 1 に当てはめて考えた場合，n を減少させ，l 及び固有値 λ も減少させるものであると見なせる．このことから，攻撃シナリオ 1 において戦術 1 は効果がないという事実を導くことが出来る．このことは表 2 に表す結果からも確認できる．特にアクセシビリティの低いノードを複数攻撃した結果は，初期値と同じ結果を保っており，ネットワークの性質を変化させていない．

一方で，アクセシビリティの高いノードを攻撃した場合，$\lambda_{max}(A)$ は大きく低下する．この理由も先行研究で示されている理由から導くことができ，直感と矛盾しない．特に，次数の集中した上位 5 パーセントの頂点がダウンした場合，系全体の平均経路長は約 2 倍にまで増大する [7] という，ネットワークにおけるスケールフリー性の脆弱性の

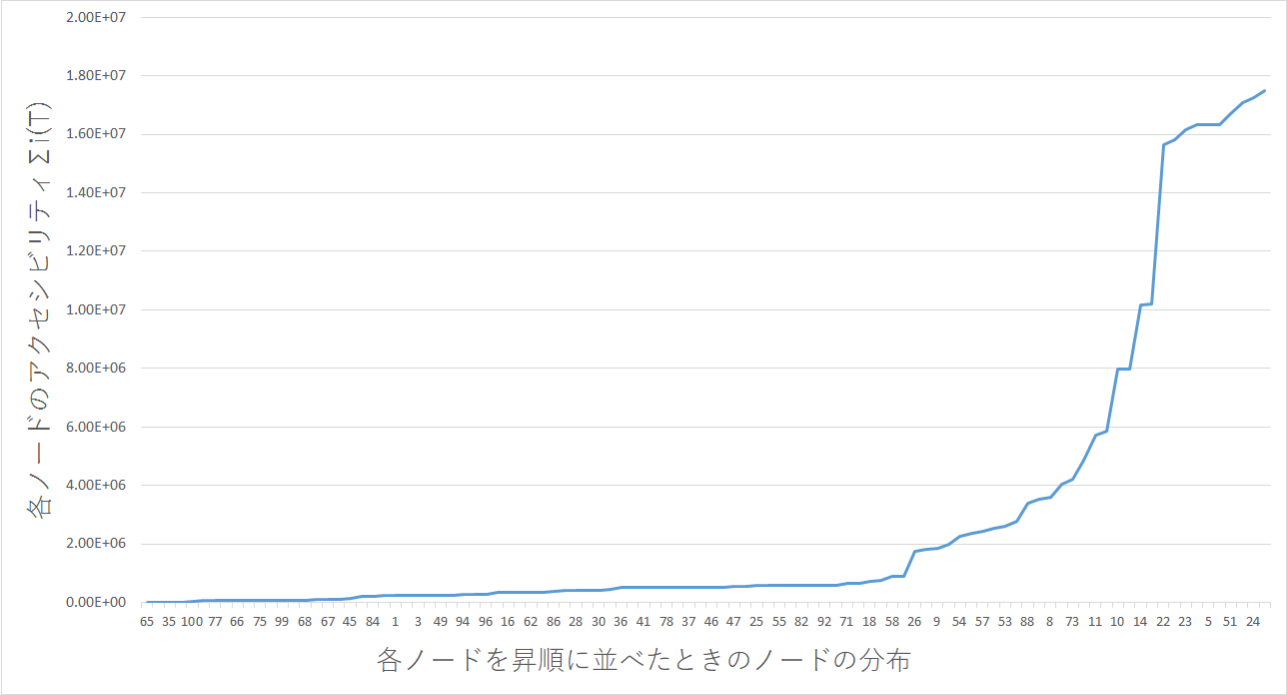

図 3　各ノードのアクセシビリティ

Fig. 3　Accessibility of a Node.

ためである．以上の考察より，攻撃シナリオ 1 から離れて単純に敵国のネットワークを機能不全にする場合については，アクセシビリティの高いノードを集中的に攻撃すると高い効果が得られると考えられる．この方針もまた直感と矛盾しない．ただし，アクセシビリティの高いノードはセキュリティレベルが高く設定されていることが一般的であり，実際に攻撃することは困難である．

以上のことから，マルウェア拡散等を実施する攻撃シナリオ 1 を考えた場合，単一ノード破壊のみならず複数ノードを破壊した場合でも，ネットワークの形状を攻撃者に有利な形に変化させることはできないことが確認できた．

5.2.2　収束性 R

表 2 に示す結果から，重要性の低いノードを複数攻撃することで R が改善していくことが分かる．これは，重要性の低いノードへの情報分散を抑えているためであると予想される．逆に重要性の高いノードを破壊した場合，情報が分散してしまい，収束性が悪化すると考えられる．

この予測を確認するため，表 2 では 3 個までのノードを攻撃対象としたが，下位 15 個のノード全てを攻撃対象とした実験も行った．なお，これらは $6.38E+03 \leq \Sigma_i(T) \leq 7.35E+04$ であり，下位 16 番目のノードは $\Sigma_i(T) = 1.02E+05$ なので，ちょうど桁数が 4 桁以下の集合となっている．その結果 $R = 0.008351$ となり，攻撃効果は 3 個ノードを破壊するよりも高まった．一方，逆に $1.02E+07 \leq \Sigma_i(T) \leq 1.75E+07$ である上位 12 個ノードを攻撃した場合，$R = 0.000855$ となり，本研究で実験を行った中では最も低い R の値をとる結果となった．

また，閾値となっている 68 番目と 69 番目のノードを境として，1〜68 番目のノードを全て破壊した場合と 69〜100 番目のノードを全て破壊した場合で固有値比 R を比較した．前者は $R = 0.04908$，後者は $R = 0.0246$ となり，$\Sigma_i(T)$ の低いノードを破壊した場合の方が固有値比 R がより増大する結果となった．しかし，$\Sigma_i(T)$ の高い 69〜100 番目のノードの中から，$\Sigma_i(T)$ の数値が 7 桁以上のノードを 1 つだけ破壊せずに残した場合，全ての組み合わせにおいて $R = 0.08768$ となり，より高い収束性を示すことが確認できた．このことから，情報が $\Sigma_i(T)$ の高いノードに限定的なパスから伝達されることにより，収束性が高まっていると考えられる．ただし，69 番目以降のノードについては高いセキュリティレベルが設定されているということが一般的であるため，攻撃の実現性については低く，圧倒的に攻撃者優位の設定でなければ実行はできないと考えられる．

以上のことから，情報が収束する核となるノードを破壊した場合は，ネットワーク全体の情報の収束性が低下するということも確認できる．つまり，収束性を高めて攻撃シナリオ 2 をより攻撃者優位にするためには，$\Sigma_i(T)$ の高いノードを攻撃するよりも $\Sigma_i(T)$ の低いノードから複数を選択して攻撃する方が効果的であると結論できる．よって，攻撃シナリオ 2 を実行する場合はネットワークの中核となっている攻撃耐性の高いノードを攻撃するよりも，末端の複数を攻撃した方が攻撃効率の向上及びセキュリティの

突破の両面で効率的であると予想できる．

攻撃シナリオ 2 では，複数の情報を拡散させることで混乱を促すことを目的としている．そのため，情報を収束させたい目標ノードが定まっている場合は固有ベクトルを用いて情報の入力ノードを探索する必要がある．

ここまでを攻撃戦略と捉えるならば，単純に R の値だけでの効果の評価では不足していると考えられる．R 及び固有ベクトルによる評価手法については今後の課題である．

6. 結論及び今後の課題

6.1 結論

一般に，正常なネットワーク利用を阻害するという点において，サイバー攻撃は迷惑な行為である．しかし，そのサイバー攻撃の中には攻撃者情報が含まれており，先行研究 [1] ではその情報を利用したサイバー攻撃戦略を提案している．しかし，先行研究ではすべてのノードのセキュリティレベルをゼロとして設定しており，現実的な攻撃戦略となっていない．そこで本研究では，Total Accessibility Matrix を用いてネットワークを解析し，ネットワーク内のノードのセキュリティレベルを想定して，セキュリティレベルの低いノードを攻撃することで得られる攻撃効果を導出した．結果として，攻撃シナリオ 1 における戦術 1 は先行研究で示されている解析を確認することとなり，重要度の低いノードを複数選択して攻撃するという実現性の高い提案であっても有効ではないという結論が得られた．また，攻撃シナリオ 2 における戦術 1 は，複数の重要度の低いノードを攻撃することが収束性 R の改善において有効であることが確認できた．

6.2 今後の課題

今後の課題として，主に以下の 3 点があげられる．

まず 1 点目として，本研究内容の普遍性の確認がある．本研究においては，実験の対象となっていたのは C 国のネットワークのみであった．この結論が他のネットワークでも普遍的であるかを確認するために，他のネットワークにおいても同様の実証をする必要があると考えられる．先行研究 [1] では C 国の他に B 国への攻撃結果が示されている．同様に B 国に対する評価を実行する予定である．

次に，戦術 2 の試行があげられる．先行研究ではノード破壊のほかに，リンク増設という戦術も実行しており，ノードを破壊するよりも攻撃効果を上昇させるという結果を得ている．しかし，本研究においてはまだノード破壊の戦術しか実験できておらず，リンク増設の戦術を攻撃耐性に応じて実行した場合の結果は得られていない．攻撃耐性の低いノードに限定してリンクを増設した場合でも攻撃効果は上昇するのか，今後検証する予定である．

そして最後に，$\lambda_{max}(A)$ 及び R の閾値を導出である．本研究及び先行研究では，$\lambda_{max}(A)$ 及び R の初期値との比較から攻撃効果を見積もっている．しかし，初期値からどれだけ値が増加すれば攻撃結果に貢献できるのかは未だ明らかにしていない．現実的で且つ十分な攻撃効果を得るための $\lambda_{max}(A)$ 及び R の閾値を導出することは今後の課題である．

また，第 5.2.2 節で示したように固有ベクトルを評価量に加えることで，攻撃シナリオ 2 の評価はより現実性が得られると考えられる．これも今後の課題とする．

参考文献

[1] 籠谷健吾, 岩井啓輔, 田中秀磨, 黒川恭一： トポロジー解析によるネットワーク攻撃に関する考察, 日本オペレーションズ・リサーチ学会 2015 年春季研究発表会, 64-65, (2015)

[2] 羽田野直道： 複雑ネットワーク: 統計物理学の視点, 物性研究・電子版編集委員会, (2014)

[3] Taaffee, Gauthier： Geography of Transportation, Ch.5 (1973)

[4] D. Takeo, M. Ito, H. Suzuki, N. Okazaki, A. Watanabe : Proposal of a Detection Technique on Stepping-stone Attacks Using, Connection-based Method , IPSJ Journal, Vol.48, No.2, Page.644-655, (2007)

[5] K. Kisamori, A. Shimoda, T. Mori, S. Goto： Analysis of Malicious Traffic Based on TCP Fingerprinting , IPSJ Journal, Vol.52, No.6, Page.2009- 2018, (2011)

[6] R. Yokota, R. Okubo, N. Sone, M. Morii： affect of the honeypot on the darknet observation, part 2 , IEICE technical report, Vol.2013-GN-88, No.16, Page.1-4, (2013)

[7] Albert, R. et al.： Error and attack tolerance of complex networks, Nature 406, pp. 378-382 (2000)