社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

電力供給ネットワークへの依存性を考慮した 構内情報通信ネットワークの脆弱性に関する一検討

小川祐紀雄† 長谷川 剛†† 村田 正幸†††

† 室蘭工業大学 情報メディア教育センター 〒 050–8585 北海道室蘭市水元町 27-1
†† 大阪大学 サイバーメディアセンター 〒 560–0043 大阪府豊中市待兼山町 1–32
††† 大阪大学 大学院情報科学研究科 〒 565–0871 大阪府吹田市山田丘 1–5
E-mail: †y-ogawa@mmm.muroran-it.ac.jp, ††hasegawa@cmc.osaka-u.ac.jp, †††murata@ist.osaka-u.ac.jp

あらまし 本稿では、情報通信ネットワークの電力供給ネットワークへの依存性に着目し、電力供給ネットワークの障害時における情報通信ネットワークの脆弱性の評価を行う。まず、障害時における電源停止範囲の観点から電力供給ネットワークのトポロジをモデル化し、システム全域での通信帯域を指標とした情報通信ネットワークの脆弱度を提案する。次いで、四つの建物からなる構内設備情報をもとに情報通信ネットワークの脆弱度を評価する。その結果、データセンタに集約される通信の場合、全トラヒックが遮断される確率が 0.01 程度であるが、データセンタ内のサーバやスイッチに UPS を適用することで改善が図れ、各部屋に分散される通信の場合、同確率が 0.003 程度であるが、100 台以上の UPS を割り当てても改善効果が小幅に止まることを明らかにする。
キーワード 電力供給ネットワーク、構内情報ネットワーク、依存性、脆弱度、UPS

A Study of Vulnerability of Campus-wide Information Communication Networks Considering Dependency on Power Distribution Networks

Yukio OGAWA†, Go HASEGAWA††, and Masayuki MURATA†††

† Center for Multimedia Aided Education, Muroran Institute of Technology
†† Cybermedia Center, Osaka University
††† Graduate School of Information Science and Technology, Osaka University
E-mail: †y-ogawa@mmm.muroran-it.ac.jp, ††hasegawa@cmc.osaka-u.ac.jp, †††murata@ist.osaka-u.ac.jp

Abstract Information communication networks depend on power delivery from power distribution networks. We therefore evaluate vulnerability of information communication networks when power distribution networks partly/completely stop power supply. We first describe a topology model of the power distribution network in campus buildings from the perspective of power failure domains, and propose the vulnerability of the corresponding information communication network, in which the metric is the bandwidth of system-wide traffic flows. We then evaluate the vulnerability of a campus-wide information communication network. The results indicate that, in the case when all traffic flows concentrate in a data center, the probability of high vulnerability (which blocks all the communications) reaches 0.01 but this is improved by applying UPSs to the servers and their neighbor switches in the data center. On the other hand, in the case when traffic flows are distributed to each room in the campus, the probability is 0.003 but this vulnerability is little improved by applying more than a hundred of UPSs.
Key words power distribution network, campus-wide information network, dependency, vulnerability, UPS

1. はじめに

インターネットや企業情報ネットワークなどの情報通信ネットワーク（以下、情報ネットワークと記す）は、一般的に基幹部分には冗長化構成を採用しており、情報ネットワーク自身の障害に対しては一定レベルの可用性を有している。一方、電力供給ネットワーク（以下、電力ネットワークと記す）に対しては、電力を供給され制御を行うといった機能的な依存関係や、

同一の地理的な場所に設置されるといった空間的な依存関係を有する [1]。例えば、地震の際に、広域情報ネットワークにおいて情報機器の電源が失われたり、情報ネットワークと電力ネットワーク双方の機器やケーブルが収容されている建物や管路が損壊したりするといった事例が報告されているが [2]、従来の情報ネットワークの可用性に関する検討は、このような依存性を十分には考慮していない。そこで、本研究は、このような電力ネットワークとの依存関係を考慮した上での情報ネットワークの可用性・頑強性の向上を目的とする。

情報通信ネットワークと電力供給ネットワークの相互依存性に起因する大規模障害の事例として、2003 年 9 月のイタリア大停電において、一つの発電所の停止により通信ネットワークノードが停止し、これによりさらに別の発電所が停止するといった連鎖により障害が大規模化したことが報告されている [3]。このように、通信ネットワークは電源ネットワークから電源を供給され、電源ネットワークは通信ネットワークにより制御されるという相互依存性を持つ場合に、全域障害を引き起こす最小ノード数 [4]、全域障害を引き起こさない電力負荷制御 [5]、情報ネットワークをスケールフリーなどのモデルで表した時の通信効率 [6] が示されている。しかしながら、従来の情報ネットワークと電力ネットワークの依存性を考慮した可用性向上に関しては、国家規模といった広域のみが検討の対象であった。

一方、都市や複数建物の規模の情報ネットワークを基盤とするスマートシティ、スマートビルティング (都市、建物規模でのセンシング情報の高密度収集と各種機器のインテリジェント制御) は、社会への適用が強く期待される分野である [7]。これにより、より多くの社会システムが情報ネットワークへの依存を強めるため、情報ネットワーク自身の可用性はもちろんのこと、電源が失われた際の情報ネットワークへの影響抑制や、UPS(Uninterruptedly Power Supply, 無停電電源装置) の最適配置といった、電力ネットワークとの依存性を考慮した情報ネットワークの可用性向上が欠かせない。そこで、本稿では、スマートビルティングへの適用を念頭に、複数建物からなる構内の規模を対象として、電源供給に関する情報ネットワークの電力ネットワークに対する依存性に着目し、情報ネットワークの可用性に関する基礎的な定式化を行う。まず、障害時における電力供給停止範囲の観点から電力ネットワークのトポロジモデルを提案する。さらに、構内規模の電力ネットワークが木構造であることを考慮し、電力ネットワークでの障害発生位置に依存した情報ネットワークの脆弱度を提案する。また、電源障害に対する情報ネットワークへの電力供給の冗長化手法として、一般的に UPS をネットワーク機器に備えることが考えられるが、全機器に UPS を備えることは現実的ではないため、情報機器に対する UPS 割り当て優先度を提案する。次いで、数千人規模の大学構内設備情報をもとに、電力ネットワーク障害時の情報ネットワークの脆弱度の評価を行う。評価では、データセンタに集約されるトラヒックと、構内各部屋に分散したトラヒックの場合で、脆弱性や UPS 配置効果が異なることを明らかにする。

以下、2. 章で関連研究を説明し、3. 章では電力ネットワークのトポロジのモデル化、4. 章において情報ネットワークの脆弱性の定義を行う。5. 章でトラヒックモデルを示し、6. 章で評価を行う。そして、最後に 7. 章でまとめと課題を述べる.

2. 関 連 研 究

重要基盤間の依存性　社会経済活動に不可欠な重要基盤システムは、情報ネットワークと電力ネットワークの他に、交通システム (鉄道、道路) やライフライン (ガス、水道) の他、医療・金融・行政システムなどを含むが、これらシステム間の相互依存関係が分類されている [8, 9]。最も簡易な分類は、機能的依存と空間的依存の二分類であり、機能的な依存は、一つの基盤が他の基盤からの入力や操作を必要とする状況を指し、空間的依存は、複数基盤の物理的構成要素が同一の場所に配置され外的要因から同時に影響を受ける状況を指す [10]。複数建物からなる構内における情報ネットワークおよび電力ネットワークの場合、機能的依存として情報ネットワークの各機器が電力ネットワークから電力を供給される点、電力ネットワークの電力供給量を左右するエアコンなどの制御を情報ネットワークが行うことがある点が挙げられる。なお、電力ネットワーク自身の制御は、情報機器間の情報ネットワークとは別系統のネットワークとして構築されることが多く、制御に関する直接的な依存はない。また、空間的依存として、物理配線用の EPS（Electric Pipe Shaft, 電気配線シャフト）やケーブルラックの共同利用が挙げられる。これらは建物の建築時の設計要件として決定されており、後からの変更はできない。空間的な依存関係を持つ場合は、火事や地震などの際に物理的破壊を同時に受けるリスクが高いだけでなく、各基盤の構成機器が非常時用電源などのリソースを共有することが安定稼働に対するリスクを高めている。本稿では、これらの依存関係のうち、最も基本的な依存関係の一つである電力供給に関する依存性を扱う。

情報ネットワーク内多層間の依存性　情報ネットワーク (エンドシステムを含む) のみを対象とした場合においても、システム内でさらに多層化されているため、各層間の機能的あるいは空間的依存関係により障害が大規模化する恐れがある。代表的な多層化の例は、一つの物理層に複数の論理層が機能的に依存している場合であり、広域情報ネットワークにおける物理リンクの障害による論理リンクの多重障害 [11, 12]、データセンタにおける物理サーバの障害による仮想ネットワークの多重障害 [13]、物理機器の電源障害による仮想ネットワークの多重障害 [14] において、物理層の構成を前提条件として固定し、各論理層の構成を最適化することで、物理層の障害時における論理層への影響を軽減している。また、複数事業者の物理/論理ネットワークが空間的依存関係にある場合に、自然災害などの影響の波及が論じられている [15]。本稿では重要基盤間の機能的依存を扱うが、そのような基盤間の依存性モデルと情報ネットワークの各層間の依存性モデルは、相互に応用が可能である。

3. 電力ネットワークのトポロジモデル

本章では、電力ネットワークのトポロジのモデル化について説明する。従来の電力ネットワークのみを対象とした研究では、

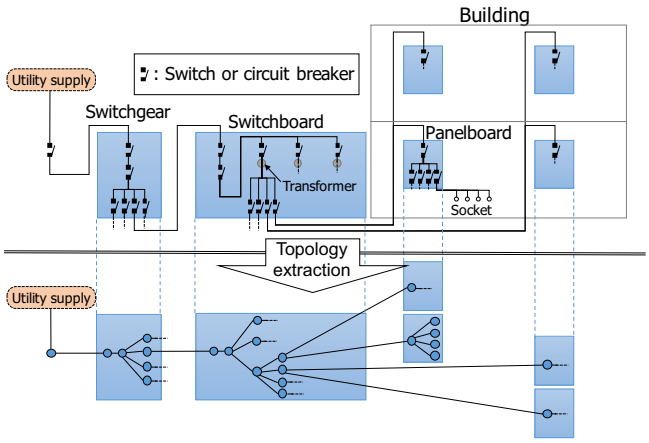

図 1　電力ネットワークのトポロジのモデル化

電圧の変化を捉える観点から、変圧器や電力回線分岐点をノードとして表し、その間をリンクで接続するトポロジが提案されている [16,17]。それに対し、本研究では、電力ネットワークの障害時における電力供給先への影響範囲の観点からトポロジを表現する。

図 1 の上図は、構内電力ネットワークの一例であり [18]、下図はそのトポロジを表した図である。一般に、構内電力ネットワークは、電力会社から電力を電気室 (switchgear) で受けた後、建物毎に設けられた配電盤 (switchboard) において 6600V から 210V/105V へと降圧したのち建物内の各フロアに分岐させる。さらに、各フロアに設置された分電盤 (panelboard) にて分岐して各部屋の電源コンセントへと電力を供給する。電力ネットワークに何らかの障害が発生した場合は、その影響を最小化するよう、最適な位置の開閉器 (switch) あるいは遮断器 (circuit breaker) において下流の回線が切り離され、その範囲内の電源コンセントからの電力供給が停止する。従って、障害時の影響範囲を論じる場合には、開閉器および遮断機をノードで表すと解析が容易になる。また、配電盤から分電盤への接続など、電力ケーブルは途中の分岐回路にて分岐する構成であるが、その分岐点にはノードを置かず開閉器・遮断機間を直接リンクで接続するトポロジで表しても、障害時の影響範囲の解析には影響しない。以上より、障害時のネットワークの切り離し点である開閉器と遮断器をノードとして表しその間をリンクで接続するシンプルなトポロジとする。これにより、電力ネットワークの障害時の影響範囲を容易に求めることが可能になる。

4. 情報ネットワークの脆弱度の定義

本章では、図 2 を参照しつつ情報ネットワークの脆弱度の定義を行う。

4.1 変数の定義

電力ネットワーク、情報ネットワーク、および、それらに関連する変数を次のように定める。

- $\mathbf{G}_{\mathrm{PD}} = (P, E)$: 電力ネットワーク。ノード（開閉器、遮断器）集合 P とリンク集合 E からなる有向グラフで表す。ノード $k \in P$ の下流に位置するエンドノードの集合を $P_{\mathrm{end}}(k)(P_{\mathrm{end}}(k) \subset P)$ とする。ノード $k \in P$ 自身がエンドノードである場合は、$P_{\mathrm{end}}(k) = \{k\}$ である。なお、以降では、電力ネットワークのノードを電力ノードと呼ぶ。

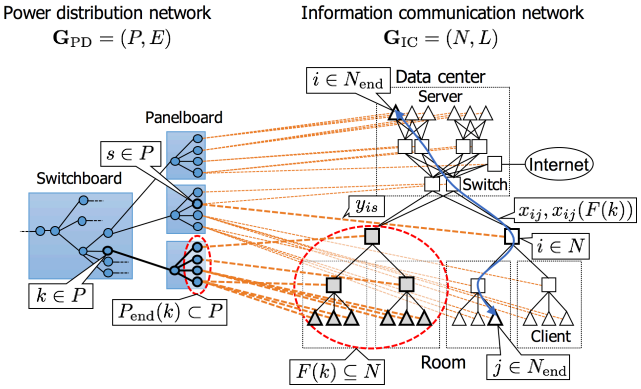

図 2　電力ネットワークと情報ネットワークのモデル概要

- $\mathbf{G}_{\mathrm{IC}} = (N, L)$: 情報ネットワーク。ノード（スイッチ、サーバ、クライアント）集合 N とリンク集合 L からなる無向グラフで表す。エンドノード（サーバ、クライアント）の集合を $N_{\mathrm{end}}(N_{\mathrm{end}} \subset N)$ とする。なお、以降では、情報ネットワークのノードを情報ノードと呼ぶ。
- x_{ij}: 情報ネットワーク $\mathbf{G}_{\mathrm{IC}}$ においてエンドノード $i \in N_{\mathrm{end}}$ からエンドノード $j \in N_{\mathrm{end}}$ へ送信されるトラヒックの帯域。
- $x_{ij}(F)$: 情報ネットワーク $\mathbf{G}_{\mathrm{IC}}$ において、情報ノード集合 $F \subseteq N$ が失われた時の、エンドノード $i \in N_{\mathrm{end}} \setminus F$ からエンドノード $j \in N_{\mathrm{end}} \setminus F$ へ送信されるトラヒックの帯域。
- $y_{is} \in \{0, 1\}$: 情報ネットワークへの電力供給を示す二値変数。情報ノード $i \in N$ が、電力ネットワークのエンドノード $s \in P$ から電力を得ている時に $y_{is} = 1$、それ以外の時に $y_{is} = 0$ とする。
- $F(k)$: 電力ノード $k \in P$ の下流に位置する電力ネットワークのエンドノードから電力を得ている情報ノードの集合 $(F(k) \subseteq N)$。

4.2 電力ネットワークの障害に対する脆弱度

情報ネットワークの脆弱度は、障害影響下の情報ノードやリンクを取り除いた後に、情報ネットワークの性能が相対的にどの程度低下するかを示す [19]。本稿では、電力ネットワークの障害時に情報ノードが影響を受けることに着目し、情報ノード集合 $F \subset N$ が失われた時の脆弱度 $V(F)$ を、通常時の全体トラヒック帯域 W に対する情報ノード集合 F 消失により失われるトラヒック帯域 $W(F)$ の比率により表す。

$$V(F) = \frac{W - W(F)}{W} \tag{1}$$

$$W = \sum_{i \in N_{\mathrm{end}}} \sum_{j \in N_{\mathrm{end}}} x_{ij} \tag{2}$$

$$W(F) = \sum_{i \in N_{\mathrm{end}} \setminus F} \sum_{j \in N_{\mathrm{end}} \setminus F} x_{ij}(F) \tag{3}$$

本稿では、各電力ノードの障害確率は等しいと仮定し、電力

ネットワークの障害に対する情報ネットワークの脆弱度平均値 $\overline{V}$ を下記式で定義する。

$$\overline{V} = \frac{1}{|P|}\sum_{k\in P} V(F(k)) \tag{4}$$

式 (4) において、$F(k)$ は次の集合で表される。

$$F(k) = \{i \mid i \in N, k \in P, s \in P_{\mathrm{end}}(k), y_{is} = 1\}) \tag{5}$$

4.3 情報ネットワークにおける UPS 適用優先度

情報ノードに対して電源冗長化のために UPS を割り当てる場合に、UPS 適応先の情報ノードの優先度を規定する。本稿では、情報ノード $i \in N$ の脆弱度 $V(\{i\})$ と障害確率 p_i を用いて、

$$p_i V(\{i\}) \tag{6}$$

の値がより大きな情報ノードに対して UPS を優先的に割り当てる。p_i に関して、本稿では電力ノード $k \in P$ の障害のみを考え、次式で定義する。

$$p_i = \frac{1}{|P|}\sum_{k\in P} \mathtt{INCLUDE}(F(k), i) \tag{7}$$

$$\mathtt{INCLUDE}(F(k), i) = \begin{cases} 1 & (i \in F(k)) \\ 0 & (i \notin F(k)) \end{cases} \tag{8}$$

5. 構内トラヒックモデル

本章では情報ネットワークのエンドノード間のトラヒック行列を定義する。構内ネットワークにおけるトラヒックとして、データセンタと各部屋の通信、各部屋内・間の通信の二通りを対象とする。

5.1 重力モデルの適用

時間変動を考慮しない簡易なトラヒックモデルとして重力モデル [20] を適用する。送信元エンドノード $i \in N_{\mathrm{end}}$ から送信先エンドノード $j \in N_{\mathrm{end}}$ へのトラヒック帯域 x_{ij} は、送信元 i からの斥力 O_i、送信先 j の引力 T_i に比例し、i と j 間の距離 d_{ij} に反比例するように表される。

$$x_{ij} = c_i \frac{O_i T_j}{d_{ij}^{\alpha_i}} \quad (\forall i \in N_{\mathrm{end}}, \forall j \in N_{\mathrm{end}}) \tag{9}$$

上記において、α_i は、エンドノード間の距離のトラヒック帯域への影響度を規定するための定数である。また、c_i は正規化のための定数であり、次式で計算される。

$$c_i = \frac{1}{\sum_{j\in N_{\mathrm{end}}} \frac{T_j}{d_{ij}^{\alpha_i}}} \quad (\forall i \in N_{\mathrm{end}}) \tag{10}$$

5.2 データセンタと各部屋のトラヒック（集約トラヒック）

送信元エンドノード i がデータセンタあるいはインターネット上のサーバ、送信先エンドノード j が各部屋のクライアントの場合、トラヒック帯域はノード距離 d_{ij} には非依存であるため、$\alpha_i = 0$ とする。斥力 O_i は、サーバからの出力帯域で表し、引力 T_j は、各部屋のクライアントに割り当てられた電力容量で表す。以降では、このトラヒックを集約トラヒックと呼ぶ。

5.3 各部屋間・内のトラヒック（分散トラヒック）

送信元エンドノード i が部屋に設置されたサーバ（例えば、ファイルサーバ、プリンタやスキャナ）の場合は、ほぼ近傍のみで利用されると考えられることから、ノード距離 d_{ij} の影響を強くするため $\alpha_i = 2$ とする。斥力 O_i、引力 T_j の表し方はデータセンタとの通信の場合と同様とする。以降では、このトラヒックを分散トラヒックと呼ぶ。

6. 構内ネットワークを対象とした脆弱度評価

数千人規模の大学における構内環境を参考にしつつ、四つの建物からなる構内の情報ネットワークおよび電力ネットワークを対象として、集約トラヒックおよび分散トラヒックのそれぞれに場合において情報ネットワークの脆弱度を評価した。

6.1 評価条件

大学構内の四つの建物の設備情報を元に、評価用データを作成した。電力供給ネットワーク $\mathbf{G}_{\mathrm{PD}}$ は、図 1 下図の類似トポロジを持ち、電力会社からの受電ノードから下流に向かって枝分かれしていく構成である。電力ノード数 $|P|$= 1192、リンク数 $|E|$= 1191 であり、エンドノード（分電盤の配線用遮断器）数は 1005 であった。また $|P_{\mathrm{end}}(k)|$ の平均値は 8.9 であった。

情報通信ネットワーク $\mathbf{G}_{\mathrm{IC}}$ は、図 2 右図の類似トポロジを持ち、情報ノード数 $|N|$= 1720、リンク数 $|L|$= 1733 である。エンドノード数 $|N_{\mathrm{end}}|$= 1266 であった。エンドノードは簡略化した構成とし、データセンタが送信元となるサーバとして、データセンタ内のインターネット公開用サーバ、イントラネット用サーバ、データセンタ外のインターネット上サーバを各 1 ノードずつ用意した。また、各部屋用のサーバを 1 ノードずつ用意し、クライアントは電力ネットワークのエンドノードが各部屋に電力供給している場合に、そのエンドノードに対応させて 1 ノードを用意した。以上の構成により、エンドノードの内訳は、サーバ 323 ノード（データセンタ 3 ノード、各部屋 320 ノード)、クライアント 943 ノードであった。また、エンドノード以外のノード（スイッチ）は 454 ノードであった。

トラヒック行列について、データセンタの各サーバのデータ送信帯域は、データセンタ内のインターネット公開用サーバでは 76Mbps、イントラネット用サーバ 1.3Mbps、データセンタ外のインターネット上サーバでは 161Mbps とした。また、各部屋のサーバのデータ送信帯域は各サーバノードに供給される電力容量に比例させ、最大で 100Kbps とした。

6.2 評価結果

6.2.1 情報ノード障害時の脆弱度

評価対象の情報ネットワークの脆弱度に関し、まず、情報ノード $i \in N$ 単体の障害時における情報ネットワークの脆弱度 $V(\{i\})$ を評価した (図 3)。図 3 の横軸は、情報ノード $i \in N$ の識別子であり、集約トラヒックの場合における脆弱度 $V(\{i\})$ の降べき順に並び替えている。また、concentrated traffic flow は集約トラヒックの場合、distributed traffic flow は分散トラヒックの場合を指す。

$i = 1 \cdots 6$ の各ノードは、データセンタのノード（サーバおよびサーバを収容するスイッチ）に相当する。これらは、集約

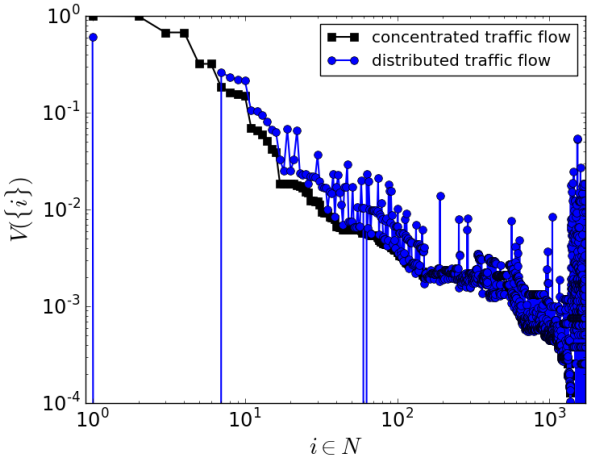

図 3　情報ネットワークのノード単体障害時の脆弱度

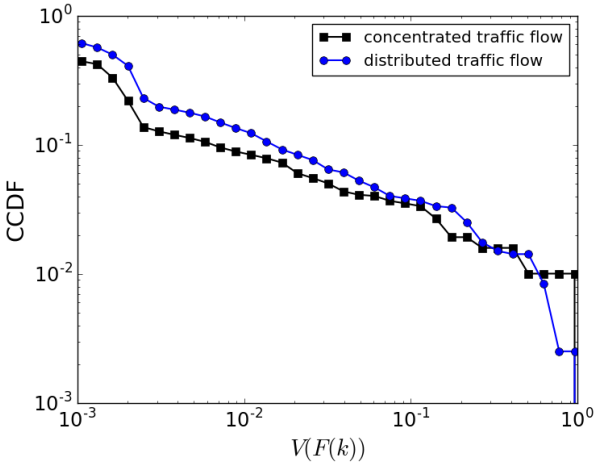

図 4　電力ネットワーク障害時の情報ネットワークの脆弱度分布

トラヒックの場合に、全てのクライアントとのトラヒックを処理するノードであり、これらのノードの障害時に脆弱度 $V(\{i\})$ は最大付近になる。一方、分散トラヒックの場合は、これらのノードを経由しないため脆弱度 $V(\{i\})$ は 0 である。

$i = 7 \cdots 16$ の各ノードは、各建物のトラヒックを束ねるエッジスイッチに相当する。また、$i = 17 \cdots 156$ の各ノードのほとんどは、各部屋のクライアントやサーバを収容するスイッチに相当する。分散トラヒックの場合には各部屋のサーバにトラヒックが集約されるため、集約トラヒックの場合に比較して、脆弱度 $V(\{i\})$ が大きくなる。

$i = 157 \cdots 1375$ の各ノードの多くはクライアントに相当する。分散トラヒックの場合が集約トラヒックの場合より大きくなっているノードは、各部屋のスイッチに相当する。

また、$i = 1376$ 以降の各ノードは各部屋に設置されたサーバに相当する。このとき、集約トラヒックでは、脆弱度 $V(\{i\})$ は 0 である。

6.2.2　電力ネットワーク障害時の脆弱度

電力ノード $k \in P$ で障害が発生した時の情報ネットワークの脆弱度 $V(F(k))$ の相補累積分布 (Complementary Cumulative Distribution Function (CCDF)) を、集約トラヒック、分散トラヒックに分けて図 4 に示す。

$V(F(k)) > 0.6$ の大きな脆弱度の障害の発生確率は、集約トラヒックの場合がより大きく約 0.01、分散トラヒックの場合は約 0.003 である。$V(F(k)) > 0.6$ となる障害は、全ての情報ノードの電源停止、あるいは、全データセンタノードの電源停止の何れかの場合である。全情報ノードの電源停止は、電力ネットワークの最上流に位置する電力ノードの障害により発生する。集約トラヒックの場合は、この全情報ノード電源停止の場合に加え、データセンタの各サーバ・スイッチが同一分電盤から電力を供給されているため、この分電盤周辺に位置する電力ノードの障害の場合に全データセンタノードが電源停止となる。一方、分散トラヒックの場合は、全情報ノード電源停止の場合のみである。なお、データセンタ内のスイッチは冗長化されているが、本稿の評価では同一分電盤に接続する構成としたため、ほとんど機能しない。

$V(F(k)) < 0.1$ の小さな脆弱度の障害の発生確率は、集約トラヒックの場合より、分散トラヒックの場合の方が若干大きい。$V(F(k)) < 0.1$ となる障害は、情報ネットワークにおいて各建物からの通信を束ねるエッジスイッチからクライアント側の一部の範囲に属する全ノードが電源停止となる場合である。分散トラヒックの場合、クライアント、クライアントを収容するスイッチに加えて、各部屋のサーバが電源停止となるため、集約トラヒックの場合に比較して $V(F(k))$ が大きくなる。

6.2.3　UPS 適用による脆弱度の低減

式 (6) にしたがって情報ネットワークに UPS を追加した時の脆弱度平均値 $\overline{V}$ の低減を図 5 に示す。脆弱度の高い情報ノードから順に UPS を割り当てる、UPS 適用台数の増加に従い、図 4 の脆弱度分布の高脆弱度 ($V(F(k)) = 1$) の部分から順に、障害発生確率が低下していき、平均値 $\overline{V}$ が低下する。なお、電力ネットワークの最上流に位置する電力ノードの障害時は、全電力ノードが電力供給を停止するため、このとき少数の UPS を情報ネットワークに割り当てても効果は現れない。このような最上流に位置する電力ノードは全電力ノードの 0.3%存在するが、この電力ノードの障害による全情報ノード停止の場合を除いて高脆弱度域の改善を示すために、脆弱度 $V(F(k))$ 分布の 99.7 パーセンタイル値を図 5 に追加した。

集約トラヒックの場合は、データセンタの各サーバ・スイッチから UPS が追加される。大量トラヒックを集約するデータセンタの 6 ノードに UPS を適用した段階で、99.7 パーセンタイル値が大きく下がるため $\overline{V}$ は低下する。一方、分散トラヒックの場合は、より多くのトラヒックを集約するエッジスイッチ、クライアント数が多い部屋のスッチやサーバの順に UPS が割り当てられる。ただし、トラヒックが分散しているため脆弱度は大きく低下しない。集約トラヒック、分散トラヒックともに、数百台の UPS を適用するまでは小幅な改善幅に止まる。

7.　おわりに

本稿では、四つの建物からなる構内環境を対象に、電力ネッ

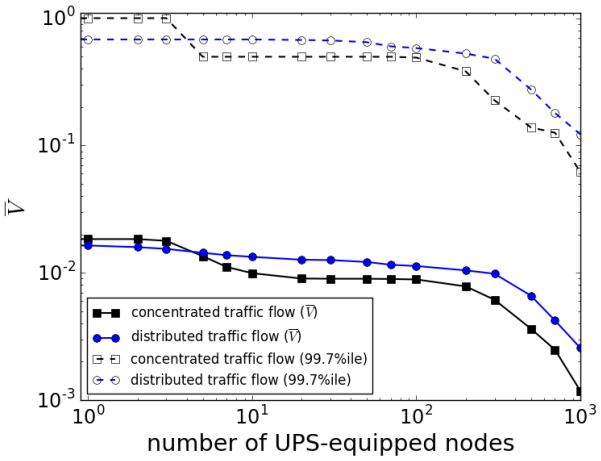

図 5　UPS 追加による情報ネットワークの脆弱度の改善

トワークの障害時における情報ネットワークの脆弱性の評価を行い、次の結果を示した。多数のデータセンタ機器が同一の分電盤から電力を得ている場合、電力ノードの障害によりデータセンタ機器の同時電源停止が発生する。データセンタにトラヒックが集約される場合、データセンタ機器の同時停止により全トラヒックが遮断されるため、脆弱度が 1 となる確率が 0.01 と高くなるが、データセンタ機器に対して UPS を適用すれば、ネットワーク全体の脆弱度が改善される。一方、各部屋にサーバが分散している場合、全面通信断となるのは全ての情報ノードが同時に電源停止となる場合のみであり、脆弱度が 1 となる確率は 0.003 程度と相対的に低くなる一方で、一つ一つの機器への UPS 適応は、情報ネットワーク全体として見た場合には脆弱度の小幅な改善に止まる。

今後の課題として、トラヒックや電力消費の動的な変化をとらえ、必要時に情報ネットワークから電力ネットワークのフィードバック制御・最適化を行うことが挙げられる。

文　　献

[1] G. D'Agostino and A. Scala, Networks of Networks: The Last Frontier of Complexity, Springer Publishing Company, Incorporated, Jan. 2014.

[2] 総務省, "情報通信白書平成 23 年度版, 東日本大震災における情報通信の状況." `http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h23/pdf/n0010000.pdf`, Aug. 2011. accessed Feb. 8, 2017.

[3] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," Nature, vol.464, pp.1025–1028, April 2010.

[4] M. Parandehgheibi and E. Modiano, "Robustness of interdependent networks: The case of communication networks and the power grid," 2013 IEEE Global Communications Conference (GLOBECOM), pp.2164–2169, Dec 2013.

[5] M. Parandehgheibi, E. Modiano, and D. Hay, "Mitigating cascading failures in interdependent power grids and communication networks," Proceedings of 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp.242–247, Nov 2014.

[6] W.K. Chai, V. Kyritsis, K.V. Katsaros, and G. Pavlou, "Resilience of interdependent communication and power distribution networks against cascading failures," Proceedings of 2016 IFIP Networking Conference (IFIP Networking) and Workshops, pp.37–45, May 2016.

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys Tutorials, vol.17, no.4, pp.2347–2376, June 2015.

[8] S.M. Rinaldi, J.P. Peerenboom, and T.K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," IEEE Control Systems, vol.21, no.6, pp.11–25, Dec. 2001.

[9] W. Wallace, D. Mendonca, E. Lee, J. Mitchell, and J. Chow, Impacts of and Human Response to the September 11, 2001 Disasters: What Research Tells Us, ch. Managing Disruptions to Critical Interdependent Infrastructures in the Context of the 2001 World Trade Center Attack, pp.165–198, Natural Hazards Research and Applications Information Center, University of Colorado, 2003.

[10] R. Zimmerman, "Decision-making and the vulnerability of interdependent critical infrastructure," Proceedings of 2004 IEEE International Conference on Systems, Man and Cybernetics (IEEE SMC), pp.4059–4063, Oct. 2004.

[11] M. Parandehgheibi, H.W. Lee, and E. Modiano, "Survivable paths in multilayer networks," Proceddings of 2012 46th Annual Conference on Information Sciences and Systems (CISS), pp.1–6, March 2012.

[12] G. Hasegawa, T. Horie, and M. Murata, "Proactive recovery from multiple failures utilizing overlay networking technique," Telecommunication Systems, vol.52, no.2, pp.1001–1019, Feb. 2013.

[13] Y. Ogawa, G. Hasegawa, and M. Murata, "Virtual network allocation for fault tolerance balanced with physical resources consumption in a multi-tenant data center," IEICE Transactions on Communications, vol.98, no.11, pp.2121–2131, Nov. 2015.

[14] P. Bodík, I. Menache, M. Chowdhury, P. Mani, D.A. Maltz, and I. Stoica, "Surviving failures in bandwidth-constrained datacenters," Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pp.431–442, Aug. 2012.

[15] P. Das, M.R. Naeini, N. Ghani, and M.M. Hayat, "On the vulnerability of multi-level communication network under catastrophic events," Proceedings of International Conference on Computing, Networking and Communications (ICNC), Jan. 2017.

[16] S. Bolognani, N. Bof, D. Michelotti, R. Muraro, and L. Schenato, "Identification of power distribution network topology via voltage correlation analysis," Proceedings of 52nd IEEE Conference on Decision and Control, pp.1659–1664, Dec. 2013.

[17] J.P. Satya, N. Bhatt, R. Pasumarthy, and A. Rajeswaran, "Identifying Topology of Power Distribution Networks Based on Smart Meter Data," eprints arXiv:1609.02678v1, Sept. 2016.

[18] Electrical Engineering Portal, "Siemens basics of energy and automation guides." `http://electrical-engineering-portal.com/download-center/books-and-guides/siemens-basics-of-energy`, Feb. 2016. accessed Feb. 8, 2017.

[19] V. Gol'dshtein, G.A. Koganov, and G.I. Surdutovich, "Vulnerability and Hierarchy of Complex Networks," eprint arXiv:cond-mat/0409298, Sept. 2004.

[20] J.P. Kowalski and B. Warfield, "Modelling traffic demand between nodes in a telecommunications network," Proceedings of Australian Telecommunication Networks & Applications (ATNAC), Dec. 1995.