Vol.2014-DPS-158 No.40
Vol.2014-CSEC-64 No.40
2014/3/7

サービス定義情報を用いたアプリケーション可用性の定量評価に関する一考察

新 麗[1,a)]　加藤 雅彦[2,b)]　梨和 久雄[2,c)]

概要：組織内ネットワークの重要情報を狙った攻撃が後を絶たない．攻撃者は組織内ネットワークに侵入し，組織内から組織外へ通信することによって重要情報の窃取を行う．そのような攻撃への対策として攻撃通信の遮断が有効であるが，遮断方法によってはアプリケーション利用に支障をきたすことが考えられる．そこで，利用アプリケーション群をサービスとして定義し，組織内ネットワークと対応付けることによって，通信遮断によるサービスへの影響を定量的に評価する手法を考案し，検証を行った．

キーワード：標的型攻撃対策，ネットワーク設計，サービス定義

1. はじめに

組織が持つ重要情報の窃取を目的とし，組織内ネットワークに侵入する標的型サイバー攻撃が年々増加傾向にある [1]．攻撃方法はますます巧妙化しており，防御どころか侵入の検出さえも困難になっているのが現状である．具体的な攻撃方法として不正アクセスや USB メモリからのウイルス感染などが知られているが，近年注目を浴びているのは，電子メールを通じて特定組織にマルウェアを送り込む「標的型メール攻撃」である．

組織内ネットワークは，入口つまり外部接続との境界にファイアウォールなどを構築して内部ネットワークへの侵入を防いでいるのが一般的である．メールに添付されたのが既知のマルウェアであれば，同様に境界や利用者のウイルス検知ソフトなどで検知することができる．しかし標的型メール攻撃に添付されるマルウェアは，対象となる組織に適合するように調整がされており他組織では利用されていないことが多く，従来のウイルス検知ソフトでは発見しにくくなっている．また，標的型メールの被害を防ぐために，利用者がメールにマルウェアが埋め込まれていることを見抜けるよう注意喚起も行われているが，標的型メールはますます巧妙化しており，感染を完全に防ぐことは困難である．つまり標的型攻撃は，これまでのように境界で侵入を防ぐのは難しいと言わざるを得ない．

そこで，たとえ侵入されても防御や検出ができるよう，組織内ネットワークでも対策を施すことが必要となってくる．対策の目的は侵入拡大を防ぐことであるため，拡大経路を減らすことが重要となる．しかし現状では，拡大経路遮断の判断は管理者のノウハウにかかっており，最も有効な対策が取られているかの判断が困難である．また，経路遮断は他の通信への影響が大きいが，通信機器で行われてしまうとその上で動作するアプリケーションへの影響が考慮されにくい．場合によっては，重要アプリケーションにアクセスができなくなり，利用者に多大な影響を与えることもある．

本研究では，組織内ネットワーク上を構成するネットワーク機器とアプリケーションなどの情報を統合し，感染経路遮断による影響，つまりアプリケーションの可用性を数値化することを試みた．利用アプリケーション群をサービスとして定義し，組織内ネットワークの接続性と共に到達性を定量的に計算する．この値をもって管理者が最適な経路遮断が行えるようになることを目指し，検証を行った．

本稿では，まず 2 節において標的型メール攻撃の傾向と対策の課題についてまとめる．3 節では，脆弱性やネットワークの定量評価についての既存研究を概観し，本研究の立場を明らかにする．4 章ではネットワークの到達性の数値化を試み，5 章ではネットワーク分離を行うにあたってのアプリケーションへの影響の指標を定義する．最後に 6 章で本研究の考察と今後の課題についてまとめる．

[1] 株式会社 IIJ イノベーションインスティテュート
IIJ Innovation Institute Inc., Chiyoda, Tokyo 101–0054, Japan
[2] 株式会社インターネットイニシアティブ
Internet Initiative Japan Inc.
[a)] ray@iijlab.net
[b)] masa@iij.ad.jp
[c)] hnashiwa@iij.ad.jp

2. 標的型メール攻撃の傾向と対策の課題

標的型攻撃を行う攻撃者は，従来のように総当たり攻撃をしかけるのではなく，攻撃対象とする組織に対して事前に組織構成や個人などの調査を行い，送信元を詐称した上でマルウェアを添付したメールを送りつけるとされている．実際の攻撃事例を見ると，組織名や部署名が実在する場合もあり，事前に調査されている事実は否めない．実在組織からのメールであれば受信者が疑問をいだきにくく，長期間にわたって攻撃に気づかなかったという事例も確認されている．

標的型メール攻撃の典型的な攻撃パターンは図 1 のように，計画立案，攻撃準備，初期侵入，基盤構築，内部侵入，目的遂行，再侵入の 7 つの段階があるとされている [2]．初期侵入で防御できるのが理想ではあるが，それが困難であれば，その後の段階での防御を行い目的遂行を阻止すれば，情報窃取の被害は免れる．そこで、この基盤構築，内部侵入の段階でのマルウェア検知および防御が重要となってくる．つまり，組織内ネットワークで防御する必要があるのである．

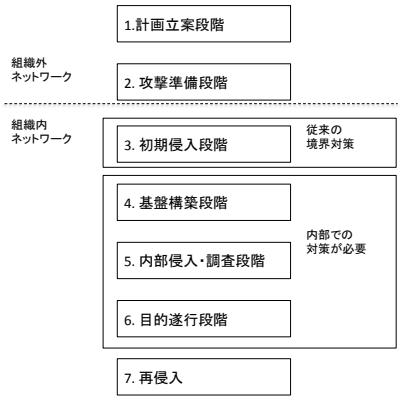

図 1　標的型メール攻撃の攻撃段階

境界での防御を前提として構築されている従来の組織内ネットワークは，内部には脅威はいないことを前提としており，いったん侵入されると防御はおろか検出する手段もない．一般利用者の通信を管理していないため区別がつきにくく，マルウェアにとっては，検出されずに組織ネットワーク上の他の機器にもアクセスができ，最終的に重要情報にたどりつくことも可能となる環境である．このような感染経路の拡大を防ぐためには，組織内ネットワークのアクセスを制限あるいは遮断していく必要がある．

しかし組織内ネットワークには多数の利用者がおり，多様なアプリケーションが動作している．ネットワークアクセスを制限した場合，マルウェアだけでなく他の利用者やアプリケーションも影響を受けて動作しなくなる可能性もある．組織内ネットワークが社会活動のインフラとなりつつある現在，ネットワークへのアクセスがむやみに制限されることは活動の停止につながりかねない．従って、ネットワークアクセス制限を行う場合には，それによって影響を受ける利用者やアプリケーションをなるべく少なくする必要がある．

一般にネットワークアクセス制限による影響の判断は機器が中心になりがちである．例えば多数の機器と接続する機器に対してアクセス制限をかけると，影響を受ける利用者が多いと判断する可能性が高い．しかし実際は，その利用者とアプリケーションとの間に該当する機器が存在しない場合には，影響は少ないはずである．このような場合に最適な判断を行うには，機器の情報とアプリケーションの利用状況を対応づけることが必要である．現状では，機器レベルでのネットワークの到達性でさえも、数値化せず構成情報を元に判断されていると考えられる．

本研究では，まずネットワークの到達性を数値化することを試みる。機器つまり OSI モデルにおける物理層での到達性，データリンク層における到達性，ネットワーク層における到達性の 3 つを算出する．次に，アプリケーション群と利用者をサービスとして定義し，重要度を与える．さらにネットワークの到達性と対応づけることによって，アプリケーションへの影響を算出する．

3. 関連研究

情報システムを脆弱性の点で数値化・評価するものとしては，共通脆弱性評価システム (CVSS, Common Vulnerability Scoring System) が普及している．管理母体は FIRST(Forum of Incident Response and Security Teams)[3] であり，FIRST の SIG(Special Interest Group) である CVSS-SIG[4] で適用推進や改善が行われている．CVSS はベンダーに依存しない共通の評価方法を提供しているため，脆弱性の深刻度を同一の基準の下で定量的に比較することが可能となっている．脆弱性そのものの特性を評価する基本評価基準 (Basic Metrics)，現在の深刻度を評価する現状評価基準 (Temporal Metrics)，利用環境も含めた最終的な脆弱性の深刻度を評価する環境評価基準 (Environment Metrics) の 3 つの基準で評価を行う．このうち環境評価基準では，二次的被害の可能性 (Collateral Damage Potential) と影響を受ける対象システムの範囲 (Target Distribution) とを評価する必要がある．現状では 5 － 6 段階が定義されているが，どの段階に属するかを定量的に評価する手段がない．

また，ネットワークシステムの表現モデルである NSQ モデル [5] を定義し，ネットワークシステムの脆弱性影響度の定量化と可視化の研究 [6] が進められている．

さらに，脆弱性による影響を遷移グラフで表しユーザに提示する研究 [7] によれば，端末ベースでの影響度を特定することは可能となるが，攻撃により動的に変化するネッ

トワークシステムの影響度を評価することは困難である．

4. ネットワーク到達性の数値化

標的型攻撃パターンの基礎構築の段階においては，端末の情報と構成情報を入手し，バックドアを開設するとされている．内部侵入は，他端末への侵入，サーバ侵入，管理者情報の窃取を試みるとされる段階である．どちらの段階も，侵入した端末からネットワークを介して情報の収集や侵入を行っている．つまり，当該の端末から到達できる機器や端末は侵入される可能性が高いことになる．これを防ぐためには，到達できる端末を減らすためにネットワークを分離する方法がある．本研究では，ネットワークの分離によって侵入の可能性の変化することを確認するため，当該の端末からネットワークを介して到達できる範囲の数値化を試みた．

4.1 組織ネットワークの構成

組織内ネットワーク上には，利用者が使うクライアント機器とアプリケーションが動作するサーバ，情報共有するためのファイルサーバなどが存在する．昨今ではネットワーク機器がすべて直接にインターネットに接続されることは稀であり，インターネットとの接続点を境界としたネットワークが構成されるのが一般的である．本研究で対象とする組織内ネットワーク例を図 2 に示す。

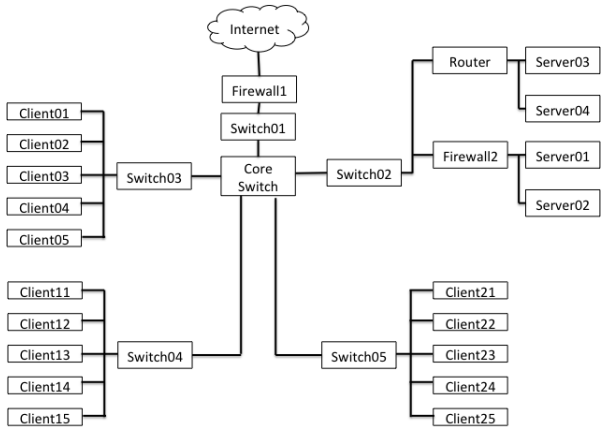

図 2 組織内ネットワークの例

図 2 の組織内ネットワークは，ルータ，スイッチや Firewall などのネットワーク機器，Web アプリケーションが動作するサーバ，および一般利用者が使用するクライアント PC で構成されている．各機器の接続，VLAN や IP アドレスなどのネットワーク上のリソース情報は一括管理しており，管理されていない機器や接続はないものとする．

4.2 ネットワーク構成のモデル化

本研究は組織内ネットワークでの防御が目的であるため，組織外のネットワークへの到達性を考慮する必要はない．従って，図 2 のような組織内ネットワークはグラフとしてモデル化することができる．機器と物理的な回線の L1 接続，VLAN などの L2 仮想ネットワーク，および L3 の IP ネットワークそれぞれにおいてグラフを作成し，それぞれの相関関係も管理する．

L1 は，組織内ネットワークを構成する機器とその接続であり，図 2 と同じ形状となる．L2 はブロードキャストが到達するドメインと考えると，VLAN などで構成された範囲となる．例えば，クライアントのドメインとサーバのドメインを VLAN など仮想ネットワークで分離している場合には，L2 ネットワークが到達する機器は，図 3，4 のように表現できる．L2 のブロードキャストをグラフとして表現する場合には，各ノードはすべてのノードと接続された図となる．

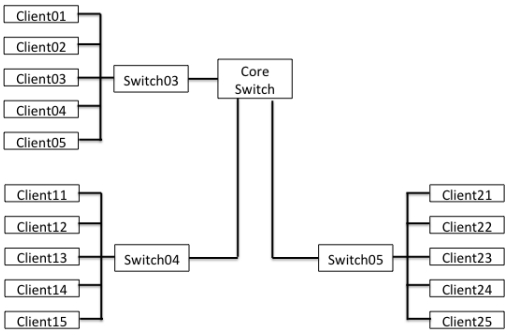

図 3 クライアントドメイン (L2)

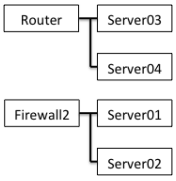

図 4 L2 のサーバドメイン (L2)

L3 のグラフは，IP の接続性で構成する．IP アドレスを持たないものは構成図には現れないため，スイッチは含まれなくなる．IP の接続性を表した例を図 5 に示す．図 5 は組織内のほぼすべての機器やサービスに IP で到達できることを示している．L3 もすべてのノードに対して双方向に通信可能であるため，グラフとして表現する場合には，各ノードはすべてのノードと接続された図となる．

なお，IP の到達性はルーティングやアクセス制御の設定によって変更が可能であり，実際の環境に合わせるにはそれらの設定を反映していく必要がある．

4.3 組織内ネットワークの到達性

以上のモデル化に基づき，組織内におけるネットワーク到達性の数値化を試みる．

到達範囲を表すグラフは，L1, L2, L3 それぞれの接続性

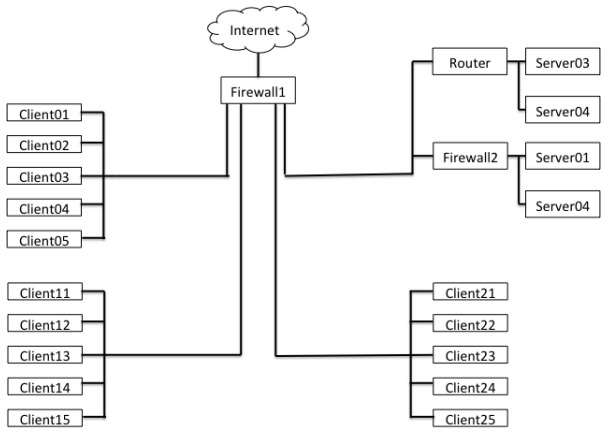

図 5　L3 の接続図例

や設定情報から作成する．ある機器がマルウェアに侵入された場合，そこを起点として組織内で到達できるノードの数を数え上げることで到達度を算出する．到達の定義はマルウェアが利用するネットワーク探索技術によるため，L2 での探索であれば L2，IP での探索であれば IP の到達範囲が対象となる．

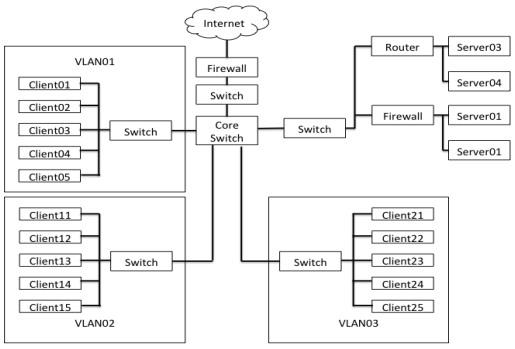

図 6　VLAN によるネットワーク分離例

例えば，*Client01* を起点として *IP* の到達性を考える．もし，組織内ネットワーク内がすべて *IP* でアクセス可能ように設定・運用されていた場合には，*Client02-05, Client11-15, Client21-25* のすべてクライアント機器 *14*，*Server-01-04* のサーバ機器 *4*，および *Firewall* 機器 *2* の合計 *20* となる．

次に，図 *6* のように，*Client01-05* は *VLAN01*，*Client11-15* は *VLAN02*，*Client21-25* は *VLAN03* に属しており，*VLAN01*，*VLAN02*，*VLAN03* の間での相互に接続はしないよう設定されている場合を考える．サーバ機器と通信する必要はあるため，*Switch02* において，*VLAN01*，*VLAN02*，*VLAN03* と *Server01-04* とは通信できるように設定はしてあるものとする．すると *Client01* を起点として到達できるクライアント機器は *Client02-05* の *4* のみとなり，サーバ機器と合わせた合計は *10* となる．

ネットワーク設計段階から分離を考慮し設定・運用を行っていれば，到達するネットワークの範囲が狭くなり，マルウェア被害拡大の可能性を減らすことができる．

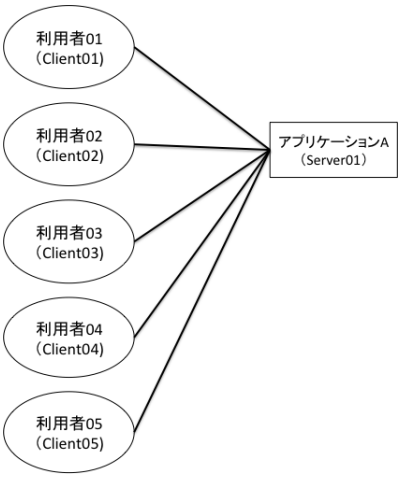

図 7　アプリケーションと利用者の定義

5. サービス定義によるアプリケーションへの影響

ネットワーク到達性の数値化により，組織内ネットワークの分離設計とマルウェアの被害拡大の可能性とを定量的に評価することが可能となった．到達範囲が把握できれば，もし標的型攻撃によりマルウェアが侵入した場合の緊急的なネットワーク分離の判断もしやすくなる．

しかし到達性の数値は，接続性の情報のみに基づいており，利用者やアプリケーションおよびその使い方に関する情報は考慮していない．利用者の活動 *(*部署など*)* や利用するアプリケーション，扱う情報などによって，利用頻度や重要性に差があると考えられる．たとえば，利用者全員が毎日利用するアプリケーションと月末に *1* 度だけ利用するアプリケーションとでは，分離したときに受ける影響が異なる．マルウェア侵入が検出されれば防御としてネットワーク分離はやむを得ないが，影響を受ける範囲が大きいと接続性が大幅に低下する上に復旧にも時間がかかり活動低下をまねく．

このような情報を考慮するために，組織内ネットワーク上で提供する機能を「サービス」として定義した．そしてアプリケーションと利用者，そしてそれを実現するための機器や機能を定義することを「サービス定義」と呼ぶ．サービスを定義し，さらにその重要性の違いも考慮し，アプリケーションへの影響の数値化を試みた．

5.1 サービス定義

本稿では，アプリケーションと利用者数，およびアプリケーションの重要度でサービスを定義する．アプリケーションと利用者は，認証情報などを利用することによって図 *7* のように規定できる．

接続情報を利用すれば図 *8* のようにアプリケーションと

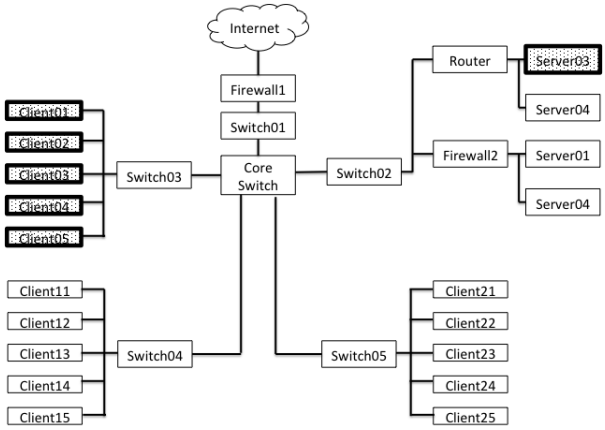

図 8　サービスと接続性の対応

利用者と機器とが対応づけられ，サービスの定義が可能となる．網掛けとなっている *Client01-05* とアプリケーションが稼働する *Server03* が図 *7* のサービス定義に対応づけられた機器である．

重要度は，最高を *5*，最低を *1* として *5* 段階で定義する．アプリケーションの重要度の決定は，組織内での判断が必要であり，自動生成は難しいため，ここでは管理者など組織の責任者が規定するものとする．

5.2　アプリケーションへの影響の数値化

定義されたサービスをもとに，アプリケーションへの影響の数値化を試みた．

算出される数値は，ネットワークを分離したときにサービスが影響を受ける度合いを示すことを目標とする．よってアルゴリズムは，*p:* 重要度，*n:* 利用者数 として数式 *(1)* のように定義した．得られた数値をアプリケーション影響指標と呼ぶ．

$$v = \sum p \times n \tag{1}$$

この式から図 *2,* 図 *7* に当てはめて具体的な数値を算出する例を示す．

利用者 *01-05* が利用するサービスはアプリケーション A とアプリケーション B の *2* つであり，重要度と利用する機能は以下のように定義されているとする．

- アプリケーション A
  重要度:　*3*
  利用する機能:　*Server03* との通信
- アプリケーション B
  重要度:　*1*
  利用する機能:　*Firewall1,* インターネット接続

アプリケーション A が稼働しているサーバ *server03* が侵入され，インターネットを通じて組織外にある攻撃者のサーバと通信していることを検知し，ネットワークを分離することで対処する場合を考える．ネットワークを分離するための設定を投入できる機器は，*Router* か *Firewall1* である．攻撃者と *Server03* との通信を遮断する場合，*Router* で *Server03* を組織内ネットワークから切り離すか，*Firewall1* でインターネット接続を止めることを考える．

Router で止める場合には，アプリケーション影響指標は，$3 \times 5 = 15$ となる．インターネット接続を止める場合には，$1 \times 5 = 5$ となる．よってこの場合では，インターネット接続を停止するほうが影響指標が低いという結果となる．

このように各アプリケーションの重要度と利用者を定義して数値化を行えば，最適な分離箇所を定量的に算出することが可能となり，自動化への応用が容易となる．

6.　考察と今後の課題

ネットワーク到達性の数値化により，到達範囲の比較が容易に行えるようになった．組織内ネットワーク上のどこにでも到達できるよりは分離されているほうが，攻撃の被害を軽減できる可能性が高くなることを数値で示した．直感的には知られていたが，数値化することで効果を確認しやすくなった．緊急避難的に分離・切断する場合にも，被害がおよぶ可能性のある範囲が明確にわかり，適切な対応がしやすくなることが期待できる．

またサービス定義により，ネットワークを切断する場合の影響を指標として示した．ネットワーク機器と物理接続の情報に基づいて定性的に切断箇所を決定していたが，影響指標を導入することで，アプリケーションまで考慮し，ネットワーク上での利用状況を反映した定量的な値をもとに，切断箇所を決定することができるようになった．サービス定義は，切断時の対処だけでなく，ネットワークの分離設計にも利用できることが期待される．

本研究を実用化していくための課題としては，数値化を行うための根拠となる正確なサービス定義および接続情報の取得がある．理想的には組織内ネットワークの仕様策定時にはサービスも利用者も想定しており，接続機器もすべて管理されていると考えられる．しかし現実には，時間がたつに従って情報が分散したり拡張時に整合性が取れなくなったりすることがある．情報が正しくなければ正しい数値は得られず，適切な対処ができなくなる恐れがある．情報を確実に蓄積することと，自動収集を組み合わせた情報管理の手法が必要である．

また本研究において，サービス定義はアプリケーションへの到達性で判断したが，ネットワークとして到達しても認証されなければ情報の窃取には至らないよう設計されていることも考えられる．重要な情報に対しては，ネットワークと認証と二重に守ることも考えられ，その場合の指標には多重の対策に関する評価も考慮していく必要がある．

今後は，指標をさらに詳細化し精度をあげていくと共に，情報の取得手法の開発を進める予定である．また，サービス定義を用いてネットワーク機器を自動的に設定する技術

も合わせて開発を進めており，本研究で算出した指標を反映した設定を迅速に行えるよう，連携を検討していく．

参考文献

[1] 独立行政法人情報処理推進機構 *(IPA):* 標的型攻撃メールの傾向と事例分析*¡2013* 年*¿* ～ますます巧妙化、高度化する国内組織への標的型攻撃メールの手口～*(online),* 入手先 ⟨http://www.ipa.go.jp/files/000036584.pdf⟩ (2014.02.06).

[2] 独立行政法人情報処理推進機構 (IPA): 『標的型メール攻撃』対策に向けたシステム設計ガイド (online), 入手先 ⟨http://www.ipa.go.jp/files/000033897.pdf⟩ (2014.02.07)

[3] FIRST(Forum of Incident Response and Security Teams) (online), 入手先 ⟨http://www.first.org/⟩ (2014.02.07)

[4] Common Vulnerability Scoring System (CVSS-SIG) (online), 入手先 ⟨http://www.first.org/cvss⟩ (2014.02.07)

[5] 金岡晃, 藤堂伸勝, 加藤雅彦, 岡本栄司:ネットワークシステムの安全性定量化に向けた新たな表現モデルとアクセス制御解析, 2008 年 暗号と情報セキュリティシンポジウム (SCIS), 2008.

[6] T. Harada, A. Kanaoka, E. Okamoto, M. Kato: Identifying Potentially-Impacted Area using CVSS for Networked Systems, Proceedings of The First Workshop on Convergence Security and Privacy (CSnP), July 2010.

[7] 神宮真人, グレゴリー ブラン, 奥田剛, 山口英, 脆弱性がもたらす影響をトレース可能な遷移グラフの提案コンピュータセキュリティシンポジウム 2011(CSS2011), pp.205-210, 2011 年 11 月.