Vol.2015-DPS-162 No.7
Vol.2015-CSEC-68 No.7
2015/3/5

サービス定義情報を用いたセキュリティ対策効果の評価指標の検討

新 麗[1,a)]　加藤 雅彦[2,b)]　梨和 久雄[2,c)]　小林 稔[2,d)]

概要：組織内ネットワークでのセキュリティインシデントに対する被害軽減策として，ネットワークを遮断する方法がある．ネットワークの遮断方法によって利用者への影響が異なるため，より影響の少ない方法を選択することが望ましい．そこで，ネットワーク構成，アプリケーション，アプリケーションを利用するためのネットワーク要件をモデル化してサービスとして定義し，ネットワーク遮断の影響を計算するアルゴリズムを提案する．本アルゴリズムにより，利用者への影響を定量的に評価することが可能となり，より影響の少ない方法を選択できるようになった．

キーワード：標的型攻撃対策，サービス定義，影響度，ネットワーク設計

Metrics of security measures effect based on the Service Defined Information

Abstract: Network Blocking is one of the effective method to prevent from security incident on the internal network. Because many users will be disconnected from the application when network is blocked, the network operator should select minimum affected method. In this paper, we propose the algorithm that calculates the affect of blocking based on service defined information that includes modeled network topology, applications, network requirements . The algorithm makes it possible for network operator to select the best method to block the network using impact index.

Keywords: Targeted Attack, Service Defined Information, Security Impact, Network Design

1. はじめに

近年，企業などの組織ネットワークに侵入し重要情報を窃取する，標的型サイバー攻撃が問題となっている [1]．具体的には，攻撃する組織に何らかのマルウェアを送り込み，組織内の情報を外部のサーバ等に送信する手法が知られている．従来の防御の仕組みは，ネットワークの入口，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．しかし，標的型サイバー攻撃は組織内 PC の利用者をだましてマルウェアを実行させ，内部ネットワークから外部ネットワークへ通信を行うため，従来の防御の仕組みでは侵入を完全に阻止することが困難である．

PC がマルウェアに感染するのを防ぐ手段としてはアンチウイルスが広く利用されているが，標的型サイバー攻撃においてメール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，従来のアンチウイルスでは発見しにくくなっている．実際に手口は年々巧妙化し，平成 25 年度には，同一内容のメールを複数の宛先に送付する「ばらまき型」のメールが減少し，事前にメールのやりとりを行って不自然ではない状況を作ってからマルウェアを送付する「やりとり型」の攻撃が増加したと報告されている [2]．アンチウイルスでも完全に防御することはますます困難になっている．

従来の防御の仕組みを補完するため，組織内ネットワー

[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 101–0071, 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
[d)] mkobayashi@iij.ad.jp

クにおける対策の必要性が重要となっており，さまざまな取組みが行われている．マルウェアの早期検知は必須であるが，検知された後の対応も重要である．情報の窃取を最小限にとどめるには，マルウェア感染が確認された場合に，該当する PC やネットワークを遮断することが有効な対策である．しかし組織内ネットワークが組織活動の基盤になっている場合，大規模なネットワーク遮断は大きな影響をもたらす．例えば，重要な契約に関わるアプリケーションがネットワーク遮断によって使えなくなると，大きな損害が出ることは容易に想像がつく．

マルウェア対策を行う組織のネットワーク管理者が，組織の活動に精通しておりネットワークおよびアプリケーションを完全に把握していれば，マルウェアによる情報の窃取を防ぎつつも組織活動を継続できるよう最適な遮断方法を発見し，実行することも可能であろう．しかし，組織内ネットワークで動作するアプリケーションが増加し、仮想化などでネットワークが複雑化していく状況において，ネットワーク管理者がすべての通信内容やアプリケーションを完全に把握することは困難になりつつある．また，ネットワーク遮断は機器の設定変更を伴うため，ネットワーク管理者がその対応を行う場合には状況の把握や影響範囲の検証をした上で設定を投入するため時間がかかり，人的ミスも起こりやすい．解決策として，ネットワーク管理者が行うネットワーク遮断の影響判断を自動化することが有効であるが，単純なネットワーク遮断は前述のとおり組織内活動に重大な影響を及ぼしかねない．よって，その前段階として選択した遮断方法が最適かどうかを判断するための指標が必要となる．

そこで本研究では，ネットワーク遮断により組織内アプリケーションが受ける影響を影響度として数値化することを試みる．まず，組織内ネットワーク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て管理することで，アプリケーションへの影響を考慮した上でネットワークの接続性と到達性を定量的に計算可能とした [3]．さらに本稿では，アプリケーションの利用を組織活動としての業務として定義し、ネットワーク遮断が業務に与える影響を数値化した．数値化することで影響度が比較可能となり，その情報を元に管理者が最適な遮断方法を判断できることを目指し，数値の有効性を検討した．

本稿では，まず 2 章においてネットワークによるセキュリティ対策技術およびリスク評価の先行研究を概観し，本研究の目的を明らかにする．3 章では，影響度を計算するための業務モデルを定義し，それに基づき 4 章で影響度を算出するアルゴリズムを提案する．最後に 5 章で本研究の考察と今後の課題についてまとめる．

2. 関連研究

本章では，本研究の関連研究として，組織内ネットワークの管理によるセキュリティ対策およびリスク評価についてまとめる．SDN や Openflow の技術により，ネットワークの管理技術、切替技術は大きく発展してきた．リスク評価に関しては標準化も進んでいるが，まだネットワークとの連携した形での研究は進んでいない．

2.1 ネットワークによるセキュリティ対策

マルウェア感染など，組織内ネットワークにセキュリティ脅威がある場合は，当該機器をまずネットワークから切り離すことが推奨される [4]．しかし同時に再発防止等のためにマルウェアを解析する必要もあり，単純に切り離すのではなく検知されることなく隔離することが求められることもある．ネットワークが切断されたり変更されたりすると検知されないようふるまいを変えるマルウェアもあることから，マルウェアの通信を中断しないように経路を選択し，応答も変化しないよう切り替える研究が行われている [5]．

また SDN 技術を連携することで，マルウェアに感染した端末を隔離する技術は，すでに製品としても登場し始めている．SDN 機器にセキュリティ機能を持たせて監視しておき，不審な端末を発見すると隔離するソリューション [6] は，Openflow を利用している．隔離を動的に行うことで検知から回復までの時間が大幅に短縮されているが，隔離する際にはその影響は考慮されていない．同様に脅威検知システムと SDN を連携させるソリューション [7] は，仮想オフィスネットワークコントローラとの連携で不正アクセスを動的に遮断・隔離する．いずれも，隔離のためのネットワーク切替を動的に実行する点で SDN を活用しセキュリティを向上させているが，ネットワーク切替によるアプリケーションへの影響は考慮していない．

2.2 リスク評価

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)[8] であり，FIRST の SIG(Special Interest Group) である CVSS-SIG[9] 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，金岡らはネットワークシステムの表現モデルである NSQ モデル [10] 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 [11] を進めている．

さらに，神宮らは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方式 [12] 提案している．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．

2.3 ネットワーク遮断影響度評価

前述したように，SDN 技術によりネットワークの切替が容易になり，プログラムで行えるようになったことで，ネットワークの柔軟性は格段に上がった．その柔軟性を利用して，セキュリティ対策に応用する研究も製品も数多く登場している．しかし，ネットワーク切替は組織内ネットワーク上で動くアプリケーション等に対して影響の大きい作業である上に，切り替え方法は一通りではないことも多い．最適な切替方法を選択するのはいまだ管理者の知識に頼っており，定量的に判断するモデルおよびアルゴリズムが存在しない．そこで本研究では，ネットワーク切替のなかでもセキュリティ対策として最もよく行われるネットワーク遮断に注目し，遮断が組織内ネットワーク上のアプリケーションや業務に対して与える影響を影響度として数値化することを目的とする．影響度を利用すれば，リスク評価とネットワーク切替を連携させることができ，業務に与える影響を最小限にしつつセキュリティリスクを減らすことができる．

3. 影響度モデル

本節では，ネットワーク遮断により組織活動が受ける影響度を計算するために，組織活動としての業務と，組織内のアプリケーションおよびネットワークとの関連性のモデル化について説明する．業務とは，その組織において，特定の目的を遂行するためにアプリケーションおよびネットワークを利用する手順が定義できる単位と定義する．例えば，勤怠管理業務などの組織における活動を指す．

特定の業務の目的を遂行するためには，業務の従事者が利用する端末から業務を実現するアプリケーションまでの通信経路を確保する必要がある．例えば勤怠管理業務であれば，業務の従事者の端末から勤怠管理サーバへアクセスできる通信経路となる．さらに細かく見ると，従事者がブラウザを利用して勤怠管理サーバへアクセスするためには，まず勤怠管理サーバの URL の IP アドレスを知るため，DNS サーバへ問い合わせが発生する．つまり，従事者の端末からは DNS サーバおよび勤怠管理サーバへ直接，間接を問わず物理的に接続され、さらに IP 上の設定、ルーティング、ポート設定までが正しく行われた経路が確立されている必要がある．このように業務遂行に必要な通信経路を通信要件と定義する．ネットワーク遮断とは，いずれかの通信要件が成り立たなくなるということと言える．

業務の性質によっては，遂行するために利用するアプリケーションおよびネットワークが 1 つだけではなく複数ある場合がある．例えば特定の情報を収集する場合は，社外 Web ページへのアクセスと問合せなどのメールとの両方を利用することが想定される．この場合は，それぞれのアプリケーションおよびネットワークにアクセスする通信要件が異なるため，影響度は分けて計算する必要がある．そこで，1 つの通信要件に対応する業務を業務コンポーネントとし，業務は業務コンポーネントの集合であると定義する．

ある業務が複数の業務コンポーネントで構成される場合，ネットワーク遮断による一部の業務コンポーネントの停止が業務全体に与える影響は業務の性質によって異なる．例えば特定の情報を収集する業務は，社外 Web ページへのアクセスができなくなってもメールで問合せが可能であれば業務が完全に停止するわけではなく，一部業務だけが影響を受けることになる．しかし，メールの問合せが不可能な業務であれば，社外 Web ページにアクセスができないと業務全体が完全に停止する．このような条件を影響度計算に反映するために，各業務コンポーネントの停止が業務全体にどの程度の影響を与えるかを重みとして示す数値を，業務コンポーネント配分と定義する．また，各業務コンポーネントが業務の遂行に対してどのように関係するかを記述する，業務遂行条件を定義する．

次節以降では，以上の定義の詳細と記述方式を説明する．

3.1 業務モデル

業務とは，その組織において，特定の目的を遂行するためにアプリケーションおよびネットワークを利用する手順が定義できる単位とする．業務は，アプリケーションおよびネットワークの実装とは切り離した上で，業務コンポーネントに対応づける．

各業務は，組織活動としての役割を考えるとその性質によって重要度が定義できる．また，例えば経理操作は月末など特定の時期に繁忙期を迎えアプリケーションおよびネットワークへのアクセスが増えるなど緊急性が変化することもある．このような情報はネットワーク遮断により受ける影響が異なってくるため計算に必要なパラメータである．本研究では，重要度および緊急度を業務の定義に含めることで影響度の計算に利用する．

加えて，組織で行われている業務に与える影響度を比較するために，従事している人数を考慮する．ただし，従事する人数が多いだけで重要度などの条件に関わらず影響度が大きくなることも考えられるため，このパラメータは正規化して利用する．

業務 x に対する業務 $G(x)$ の重要度、緊急度、従事者の人数は、以下のように定義する．この 3 つはシステムに依存しない数値である．

重要度 p

- 業務の重要性を表す指標
- 固定値
- $p(x) = (0, 1]$

緊急度 e

- 業務の緊急性によって値を増減する指標
- 時間によって変動する値
- $e(x) = [0, 1]$

業務 G の従事者の人数 l

- 業務従事者の人数

3.2 業務コンポーネント

業務コンポーネントは，業務を遂行するにあたって利用する手順やアプリケーションである．業務は業務コンポーネントの集合として定義される．業務 x 対して c 個の業務コンポーネントがある場合，それぞれの業務コンポーネントを $Gcs(i)$ として，業務コンポーネント全体 $Gc(x)$ は，

$$Gc(x) = \{Gcs(1), Gcs(2), ...Gcs(c)\}$$

で表される．

業務コンポーネントには，ネットワーク遮断によって業務全体に与える影響を示すための重みである，業務コンポーネント配分 D を定義する．ある業務コンポーネントが利用できなくなった場合に，業務がどの程度できなくなるかを表す数値である．業務コンポーネント $Gc(x)$ に対する業務コンポーネント配分 D は任意に定義可能とし，

$$D = \{d(Gcs(1)), d(Gcs(2)), ...d(Gcs(c)\}$$

で表されるリストとする．

業務コンポーネントがすべて稼働している状態を 1 とすると，業務コンポーネント配分の合計は必ず 1 であり，

$$\sum_{k=1}^{s} d(k) = 1$$

が成り立つ．

3.3 業務遂行条件

業務を遂行するにあたり，一部の業務コンポーネントの停止が他のコンポーネントに影響を与えるかどうかを評価するため，業務遂行条件を定義する．業務 x に対する業務遂行条件 $S(x)$ は，各業務コンポーネント間の関係性を示す論理式として、例えば次のように表す．

- 例 1:

$$S(x) = Gcs(1) \cap Gcs(2) \cap .. \cap Gcs(c)$$

- 例 2:

$$S(x) = Gcs(1) \cup Gcs(2) \cap .. \cap Gcs(c)$$

3.4 通信要件

各業務コンポーネントを遂行するために必要となる通信経路を通信要件と定義する．IP による通信の場合，通信経路の確保とは，通信元 IP アドレスと通信先 IP アドレスが，通信先ポートやプロトコルなど設定とともに接続されていることである．通信元と通信先で特定される通信を通信ルール r と定義し，次のように表す．

$$r = (srcIP, dstIP, DstPort, Protocol)$$

srcIP: 通信元 IP アドレス
dstIP: 通信先 IP アドレス
DstPort: 通信先のポート
Protocol: 通信プロトコル

ある通信ルール r(t) は、すべてのパラメータが揃い、かつ通信経路を確保するようにシステムの設定が完了している場合にのみ成立する．

通信要件は，業務コンポーネントの遂行に必要な通信ルールの集合である．前述したように，業務アプリケーションへアクセスする場合には，名前解決等の通信が自動的に行われている．例えば社外へメールを送信する場合，図 1 のようにまず DNS サーバへ問合せを行い，それから社内メールサーバへアクセスするという手順になる．さらに社外に送信する場合にはメールサーバ間でのプロトコルに従い，DNS 問合せと社外のメールサーバへのアクセスが行われる．

通信要件 R が，h 個の通信ルールで構成される場合，

$$R = \{r(i) | i = 1, .., h)\}$$

となる．通信要件は，通信ルールがすべて成立しているときにのみ成立し，一部の通信ルールに障害があったり遮断されている場合には成立しない．つまり，h 個の通信ルールをもつ通信要件 Rv は，

$$Rv = r(1) \cap r(2) \cap ... \cap r(h) \quad (1)$$

で表される．

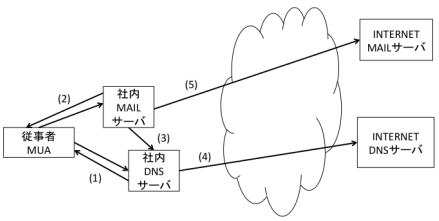

図 1 社外へのメール送信に対する通信要件

4. 影響度アルゴリズム

以上の定義をもとに，ネットワーク遮断時の業務への影響度を計算するアルゴリズムを提案する．

手順の概要は次の通りである．ネットワークの遮断により，通信要件 tR が成立しない場合，条件 (1) から，その通信を含む業務コンポーネント $tGcs$ も停止し，ある従事者 tl が業務 $tG(x)$ の一部を遂行できなくなる．業務コンポーネント $tGcs$ を利用する従事者ごとに影響度を計算して個人ごとの影響度を算出し，それを積算することで，業務 tG に対する影響度とする．さらに，通信要件 tR つまり業務コンポーネント $tGcs$ が他の業務 $tGcs(y)$ でも利用されていた場合，$tGcs(y)$ の従事者も影響を受ける．同様に影響を受ける業務のすべてに対して積算した数値を，ネットワーク遮断時の全社員の全業務に対する影響度とする．

以下で具体的な算出方法を説明する．

4.1 業務コンポーネント成立条件

ある業務の従事者 a が遂行できなくなる業務 G(t) は，成立していない通信要件に対応する業務コンポーネント，業務コンポーネント配分，業務遂行条件から算出できる．

遮断された通信要件 $tR(s)$ に対応する業務コンポーネント $tGcs(s)$ が含まれる業務 tG において，まず業務遂行条件 $vG(t)$ を計算する．業務遂行条件は，各業務コンポーネントの関係を示しており，依存がない場合は定義されている条件から，$vG(t) = 1or0$ が得られる．成立していない業務コンポーネント $tGcs(s)$ は，$tGcs(s) = 0$ である．

$vG(t) = 1$ の場合は業務は成り立つが，業務コンポーネント $tGcs(s)$ が成立していない分の影響を受けるため，完全停止はしないが一部は動作しない，という状態になる．業務コンポーネントが複数ある場合につまり，ネットワーク遮断時に影響を受けるのは，

$$vG * tGcs = 0 \tag{2}$$

を満たす業務である．

4.2 影響度算出アルゴリズム

影響度は，条件 (2) を満たす業務および業務コンポーネントの加算で表される．計算においては，影響を受ける業務を抽出したいことから，影響を受ける業務が 1 と算出され計上できるよう否定を取り，業務の重要度 $p(t)$，緊急度 $e(t)$，および業務コンポーネント配分 $D(Dcs(s))$ の積をとり，さらに従事者 1 人当たりの数値にするため $vG(t)$ 従事する人数 L で除算して以下の通りある従事者がある業務において受ける影響度 I(a) を算出する．

$$I(a) = \overline{vG * tGcs} * p(t) * e(t) * D(Dcs(s))/L \tag{3}$$

次に，遮断された通信要件の影響度を組織全員の従事者 H 人について加算することで，特定の業務に対する影響度 I(g) を算出する．

$$I(g) = \sum_{j=1}^{H} I(j) \tag{4}$$

最後に，遮断された通信要件の影響度を，すべての業務 K と従事者 H について加算し，ネットワーク遮断が組織全体に与える影響度 I とする．

$$I = I(g) = \sum_{k=1}^{T}\sum_{j=1}^{H} I(j)(k) \tag{5}$$

4.3 影響度の可視化

本アルゴリズムで算出した影響度は，組織における全業務に対して，影響を受ける全業務コンポーネントととらえることができる．図 2 は，業務 $G(i)$ と業務コンポーネント $Gc(i)(j)$、従事者 $H(i)$ とを表で示したものである．従事者 $H(i)$ が従事してしていない業務は白抜きで表す．各業務 $G(i)$ の横幅は，重要度 $p(i)*$ 緊急度 $(i)/$ 従事する人数 L であり，各業務コンポーネント $Gc(i)(j)$ の幅は，業務コンポーネント配分に応じて決まる．

図 2 において濃灰色で示されるのが，通信要件が遮断されて影響を受ける業務コンポーネントである．すると影響度は，濃灰色の部分を合計した面積だととらえることができる．通信要件の遮断方法により，合計面積が変化するため，影響度の差異が比較できる．

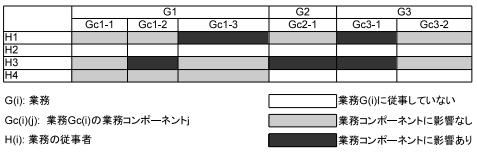

図 2 影響度のイメージ

5. まとめと今後の課題

組織内ネットワークからの情報窃取の被害を軽減するにあたり最適なネットワーク遮断方法を発見するために，業務が受ける影響度を算出するアルゴリズムを提案した．

今後は，さらに現実的なアプリケーションやネットワークを想定して検証を行う予定である．また，業務をトップダウンで定義できるのは，ワークフローが確立している組織や業務に限られ，例外がある場合には定義の見直しが必要である．緊急度や業務コンポーネント配分などに変更があった場合にデータを管理していかなければならず，どこまで厳密に行うかは管理コストとの兼ね合いとなる．現実的なシステムに応用するにあたっては，データ作成・管理の点に関しても考慮していく．

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⟩(2015.02.06).
[2] 警察庁警備企画課・情報技術解析課, ”平成 25 年中のサイバー攻撃の情勢及び対策の推進状況について”, 2014.2.27(online), 入手先 ⟨http://www.npa.go.jp/keibi/biki3/260227kouhou.pdf⟩ (2015.02.06).
[3] 新 麗, 加藤雅彦, 梨和久雄, ”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”, 情報処理学会, 研究報告コンピュータセキュリティ（CSEC）,2014-CSEC-64(40),1-6 (2014-02-27).
[4] 米国立標準技術研究所, ”コンピュータセキュリティインシデント対応ガイド”, 2008 年 (online), 入手先 ⟨http://www.ipa.go.jp/files/000015367.pdf⟩(2015.02.07).
[5] 来間一郎, 甲斐賢, 木城武康, 磯部義明, ”SDN によるマルウェア調査のためのネットワーク切り替え手法”, 情報処理学会, 研究報告コンピュータセキュリティ（CSEC）,2014-CSEC-66(18),1-8 (2014-06-26).
[6] 株式会社 NTT データ, ”標的型攻撃による被害を最小限に抑制し、速やかに安全な状態へ回復”, 2014.10.15 (online), 入手先 ⟨http://www.nttdata.com/jp/ja/news/release/2014/101500.html⟩ (2015.02.07).
[7] 株式会社ストラトスフィア, ”ストラトスフィア、脅威検知システムと SDN 技術を連携させるエンタープライズ向け次世代型セキュリティソリューションを発表”, 2014.12.11 (online), 入手先 ⟨http://www.stratosphere.co.jp/press/2014/1211.html⟩ (2015.02.07).
[8] FIRST(Forum of Incident Response and Security Teams) (online), 入手先 ⟨http://www.first.org/⟩ (2015.02.07)
[9] Common Vulnerability Scoring System (CVSS-SIG) (online), 入手先 ⟨http://www.first.org/cvss⟩ (2015.02.07)
[10] 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.
[11] 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.
[12] 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.