

# サイバー攻撃による重要インフラサービス停止を想定した サイバー版ハザードマップ作成の試み

山田 祐也<sup>1,\*</sup> 後藤 厚宏<sup>1</sup>

**概要**：重要インフラを標的としたサイバー攻撃の増加によって、重要インフラのサービス停止リスクがある。筆者らは、企業の事業継続計画や自治体の復旧計画に寄与するサイバー版のハザードマップを検討してきた。本稿では、地理情報システムを用いて異なる重要インフラ分野間の依存関係および各重要インフラを構成する設備のネットワーク構造を地図上に表現することを試みた。

**キーワード**：重要インフラ、事業継続、BCM、レジリエンス

## Attempt to create a cyber hazard map of critical infrastructure service outages

Yuya Yamada<sup>1,\*</sup> Atsuhiro Goto<sup>1</sup>

**Abstract:** There is a risk of service outage of critical infrastructure due to the increase of cyber attacks targeting critical infrastructure. The authors have been studying a cyber version of hazard maps that can contribute to business continuity planning for companies and recovery planning for local governments. In this paper, we attempted to represent on a map the dependencies among different critical infrastructure fields and the network structure of facilities that constitute each critical infrastructure using a geographic information system.

**Keywords:** Critical Infrastructure, Business Continuity, BCM, Resilience

### 1. はじめに（研究の背景）

重要インフラを標的としたサイバー攻撃の増加によって、重要インフラのサービス停止リスクがある。重要インフラは社会経済活動の基盤であり、重要インフラの停止は社会に重大な影響を及ぼすため、予め被害・復旧想定を行い、社会全体で被害軽減や早期復旧のための事前対策を取り組むことが重要である。筆者らは被害・復旧想定の試みとして、サイバー攻撃による重要インフラのサービス停止がユーザ企業の事業継続に及ぼす被害特性を明らかにすることを目的に、重要インフラ同士や重要インフラとユーザ企業間の物理的な依存関係をモデル化し、シミュレートする手法を提案した[1]。本稿では、地理情報システムを使用し、重要インフラ分野同士の依存関係を地図上に表現する方法を検討する。本稿の構成は以下の通りである。

- 第2章では、筆者らがこれまでの取り組んできた、サイバー攻撃による重要インフラのサービス停止がユーザ企業の事業継続に及ぼす被害特性および復旧特性をシミュレートし地図上に表現する「サイバー版ハザードマップ」の作成を目指したシミュレーション手法について紹介する。

- 第3章では、地理情報システムを用いて異なる重要インフラ分野間の依存関係および各重要インフラを構成する設備のネットワーク構造を地図上への表現を試みる。

### 2. 本研究におけるこれまでの検討

一般に、電力や通信、石油などの重要インフラはユーザ企業が事業を行うために必須な資源(ボトルネック資源[2])となっており、重要インフラの供給が停止すると企業は事業を継続することができない。そのため、重要インフラの停止リスクを考慮し、被害軽減や早期復旧の対策を講じることはユーザ企業にとって不可欠である。

一方で、重要インフラが持つ相互依存関係などの特徴のため、サイバー攻撃による重要インフラのサービス停止がユーザ企業の事業継続に及ぼす被害特性は自明ではない。図1は、サイバー攻撃による重要インフラ停止がユーザ企業の事業継続に及ぼす間接被害の例である。電力インフラは、石油インフラや通信インフラの各設備にとって必須の資源となっており、言い換えれば、石油インフラと通信インフラは電力インフラに依存している。電力インフラがサ

1 情報セキュリティ大学院大学  
Institute of Information Security  
\* mgs235502@iisec.ac.jp

イバー攻撃によって停止し広域の停電が発生したと想定すると、ユーザ企業にとっての被害は停電だけではなく、通信障害や燃料の調達難という形で現れる可能性がある。

筆者らは、サイバー攻撃による重要インフラのサービス停止がユーザ企業の事業継続に及ぼす被害特性および復旧特性をシミュレートし地図上に表現する「サイバー版ハザードマップ」の作成を目指して取り組んでいる。図2は架空のサイバー版セキュリティマップの表示画面である。京北変電所がサイバー攻撃によりサービス停止すると宮戸変電所が停電になり、宮戸変電所から電力供給を受ける朝霞浄水場も停電、断水が発生する様子を表現している。

筆者らは、自然災害分野における被害シミュレーション手法[3][4]を参考に、サイバー攻撃による重要インフラのサービス停止がユーザ企業の事業継続に及ぼす被害特性のシミュレーション手法を提案した[1]。具体的には、以下の3つのモデル・パラメータで構成されるシミュレーションの枠組みを提案し、各モデル・パラメータについて検討した。また、重要インフラの構成要素モデルを用いてシミュレーションを試行した。

#### ・重要インフラの構成要素モデル

重要インフラの相互依存関係を表現するために用いるモデルである。各重要インフラの構成要素、他の重要インフラへの依存関係、依存パラメータ(各構成要素にどの程度依存しているのか)、被害特性(どの構成要素が停止しやすいのか)を記述する。

#### ・設備のサイバー依存マップ

重要インフラ同士の地理的な関係を記述するモデルである。設備のサイバー依存マップは重要インフラの構成要素モデルを元に具体的な設備と対応付けて作成される。

#### ・サービス復旧パラメータ

サイバー攻撃から直接被害を受けた重要インフラ自体の復旧特性を表現するために用いるパラメータである。ある重要インフラの構成要素がサイバー攻撃を受け機能を停止・縮退した場合に、機能停止・縮退後の時間経過と機能復旧度合いの関係を示す。

図3は、提案手法のユースケースである。まず、各重要インフラ事業者が自社の管理する重要インフラについて重要インフラの構成要素モデルと設備のサイバー依存マップ、サービス復旧パラメータを作成し国・自治体に提供する。国・自治体は各重要インフラ事業者から提供されたモデルやパラメータを集約し、シミュレーションツール(サービス)として提供する。シミュレーションツールは、ユーザ企業が自社のBCM(事業継続マネジメント)を検討するた

めの材料として参照したり、国・自治体が大規模なサイバー攻撃に対する社会のレジリエンスを検討するための材料として利用することを想定する。

重要インフラの構成要素モデルについて、書式を定義し、重要インフラ分野毎の構成要素モデルを作成した。図1のケースを構成要素モデルで表現すると、図4のようになる。ユーザ企業が事業を行うための電力、通信インフラサービスが十分に供給されるには各構成要素が100%機能している必要があると仮定し、サイバー攻撃による電力インフラの停止が、石油インフラや通信インフラの構成要素の機能縮退としてユーザ企業に影響を及ぼすことを表現している。提案した重要インフラの構成要素モデルを用いて重要インフラ停止時のユーザ企業の被害特性についてシミュレーションの試行を行った。

また、他重要インフラの影響が遅れて現れる場合について検討し、システム・ダイナミクスを参考にストックの概念を導入した[5]。石油インフラは、仮に油槽所からガソリンスタンドへの燃料輸送が縮退したとしても、ガソリンスタンドのタンクに燃料在庫がある限りは、ユーザ企業への燃料供給を継続することができる。また、自家発電設備を持つ通信インフラも、停電後すぐに機能が停止するわけではなく、燃料備蓄があれば、機能を継続することができる。重要インフラの構成要素モデルに備蓄や在庫という構成要素を追加することで表現可能にした。

さらに、法制度や協定などの組織間の関係が構築されていなければ円滑な自治体・企業間連携は行えないことが想定されることから、サイバー攻撃による重要インフラサービス停止時の自治体・企業間連携について検討した[6]。自然災害の法制度や事前協定の調査をとおして、サイバー攻撃でも類似の仕組みが存在するのか、自然災害のために整備されている各種制度、協定がサイバー攻撃時にも適用可能かどうか検討し、自然災害とサイバー攻撃の被害特性や復旧特性の差分について考察した。災害対策基本法とサイバーセキュリティ基本法の比較では、自然災害では災害対策基本法において重要インフラ停止による間接被害に対する復旧・復興についての連携の枠組みが整備されている一方で、サイバーセキュリティにおいてはサイバー攻撃からの重要インフラの防護とサイバー攻撃による重要インフラ設備の直接被害からの復旧が主な検討対象であり、他重要インフラ事業者同士での連携の枠組みが不十分であることが示唆された。

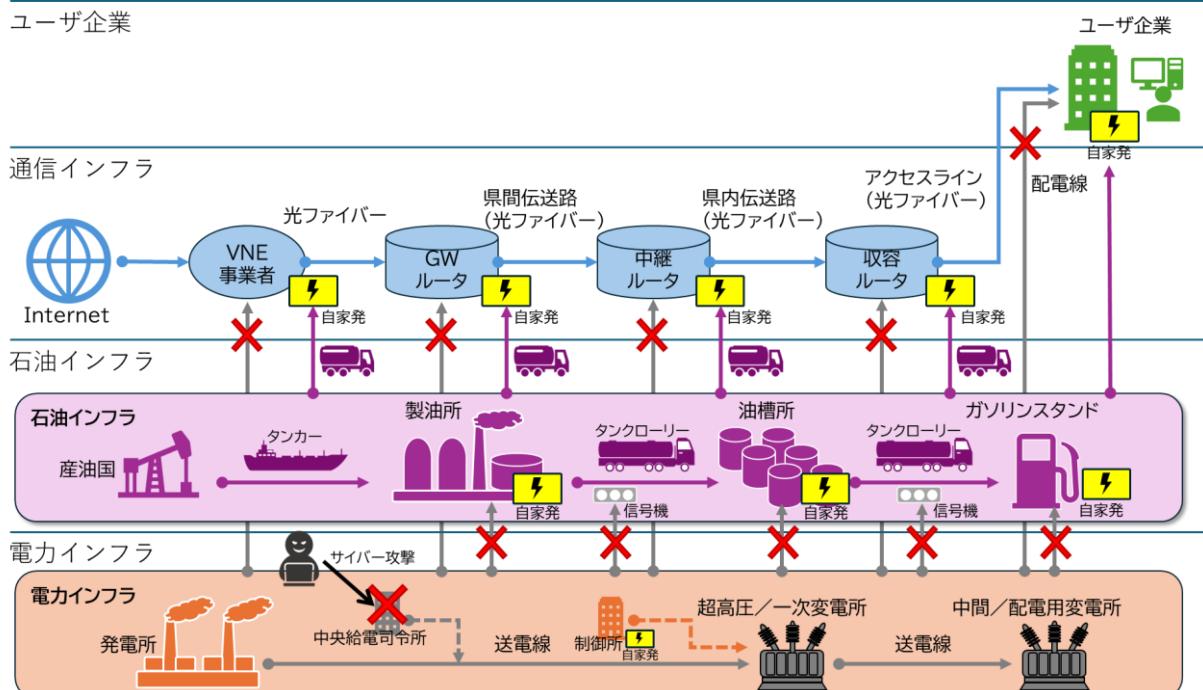


図1 サイバー攻撃による重要インフラ停止がユーザ企業の事業継続に及ぼす間接被害の例



図2 サイバー版セキュリティマップの表示画面(架空)

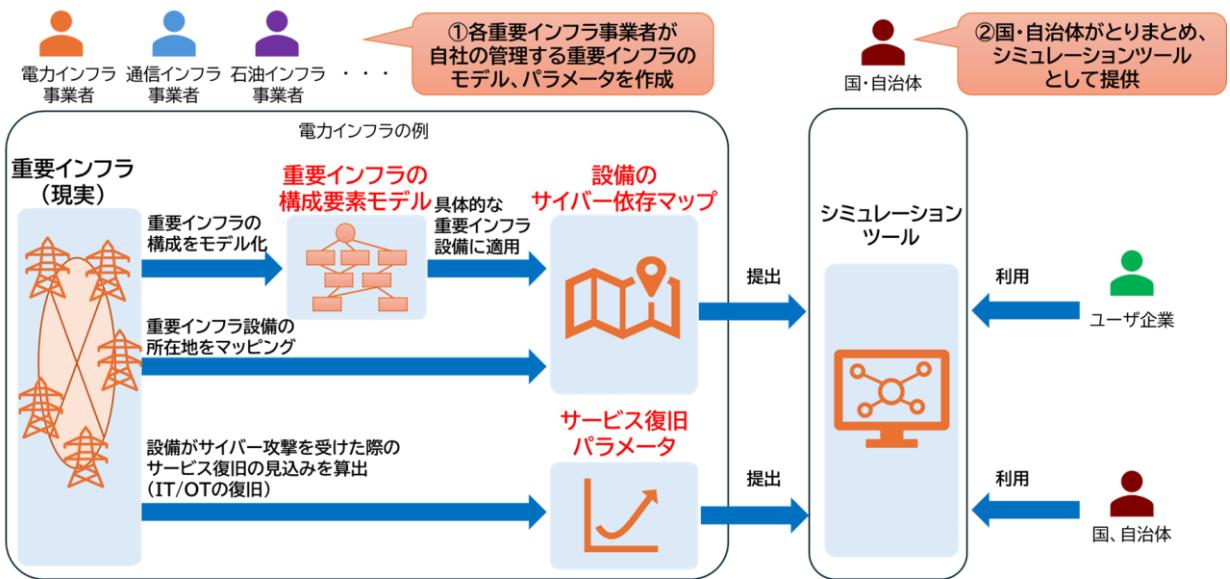


図3 提案手法のユースケース

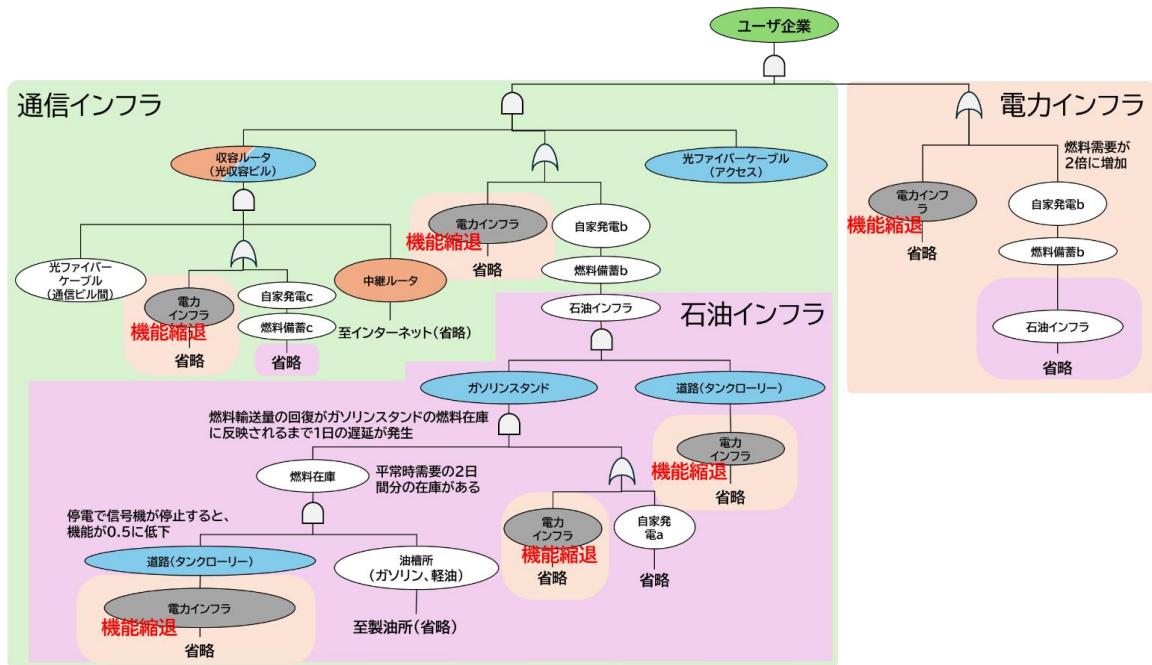


図4 重要インフラの構成要素モデルの例

### 3. 地理情報システムでの表現

図 2 で示したサイバー版ハザードマップを実際に作成することを試みる。まず、サイバー版ハザードマップ作成に必要な要素を整理する。

#### ・各重要インフラ設備の所在地

重要インフラ設備の地理的な場所を表す。重要インフラによっては所在地が公開されている。例えば、浄水場の国土交通省の国土数値情報ダウンロードサイト[7]から入手可能である。一方で、電力インフラなどの重要インフラ分野では、正確な所在地は入手困難である。電力については、仮の所在地を用いることとした。

#### ・サービスを提供しているエリア

ある浄水場が水道を供給しているエリアのように、各重要インフラ設備がサービスを提供しているエリアを表す。今回では、仮に重要インフラからの半径で表現している。

#### ・各重要インフラ設備間の依存関係

重要インフラ設備同士の関係性およびある設備が停止した際の被害特性を表す。重要インフラの構成要素モデルを元に作成される。今回は、仮で中央給電指令所、超高压変電所、配電用変電所、浄水場の依存関係を表現した。

実際に地理情報システム上で表現を試みた。地理情報システムは QGIS を使用した。図 5 は、電力インフラの設備(中央給電指令所、超高压変電所、配電用変電所)と浄水場の依存関係を表現している。各重要インフラの所在地をノード、サービスを提供しているエリアをノードを中心としたポリゴン、各重要インフラ設備間の依存関係をリンクとして表すことで、サイバー版ハザードマップの一部を表現することができた

今後は、各重要インフラ設備に「状態」という情報を持たせ、ある重要インフラ設備のサービスが停止した際に、他の重要インフラ設備の状態が「停止」になるような表現を目指す。

---

1 情報セキュリティ大学院大学  
Institute of Information Security  
\* mgs235502@iisec.ac.jp

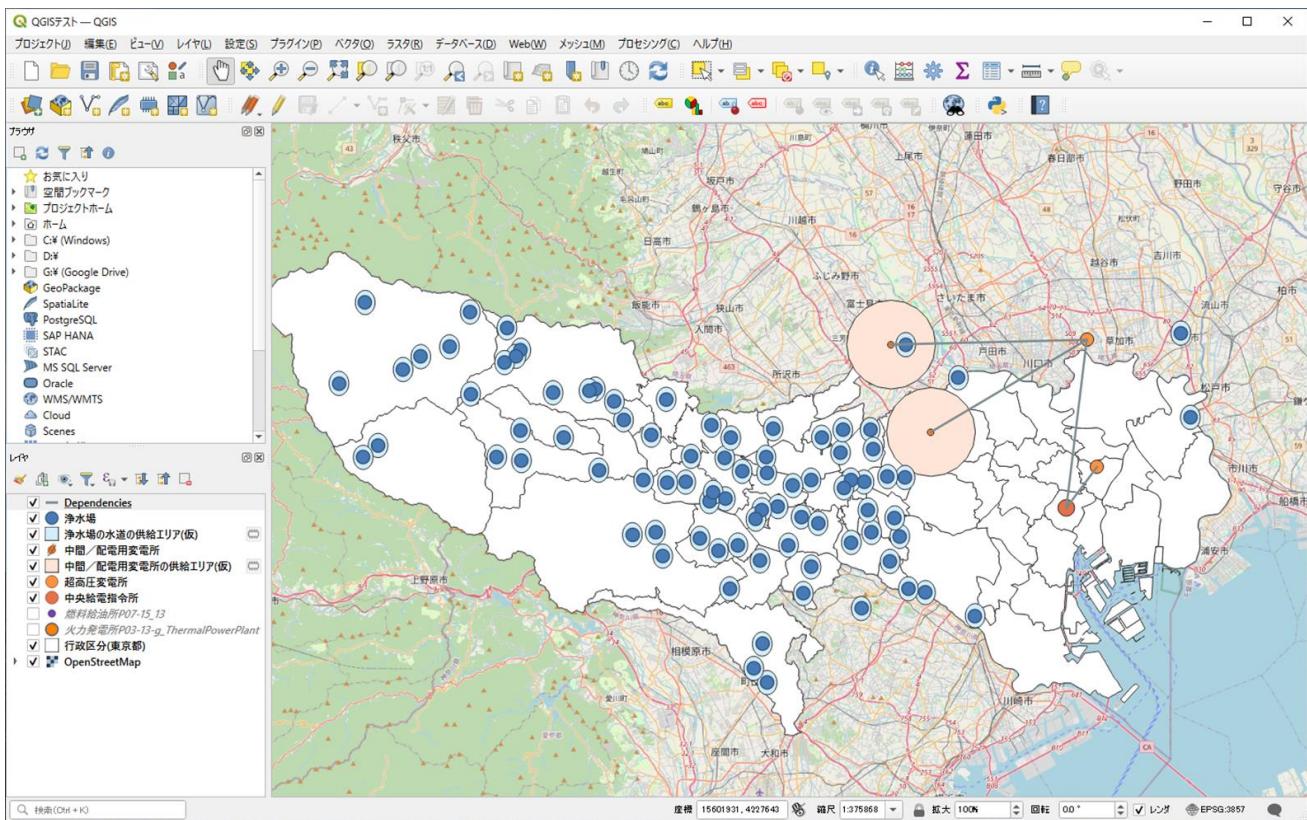


図 5 地理情報システム上での依存関係の表現例

## 参考文献

- [1] 山田祐也, 後藤厚宏, "サイバー攻撃による重要インフラのサービス停止がユーザ企業の事業継続に及ぼす間接的被害のシミュレーション手法", コンピュータセキュリティシンポジウム 2024 論文集, pp.782-789, Oct.2024.
- [2] 中小企業庁, "中小企業 BCP 策定運用指針 ~緊急事態を生き抜くために~ 3.1 事業を理解する", [https://www.chusho.meti.go.jp/bcp/contents/level\\_a/bcpgl\\_03a\\_1.html](https://www.chusho.meti.go.jp/bcp/contents/level_a/bcpgl_03a_1.html), (参照 2025-01-16).
- [3] 片岡正次郎, 白戸智, 牛島由美子, 高宮進, "インフラシステムの災害復旧過程のモデル化と震災復旧シミュレーション", 土木学会論文集A 1 (構造・地震工学) Vol.69, No.1, p.1-19, Jan.2013.
- [4] 漆原史也, 吉田壮一郎, 岩崎翔吾, 柳沢隆己, 小森健一郎, 市川学, 中井豊, "災害復旧シミュレータによるインフラ被害の可視化とその活用", 第 22 回社会システム部会研究会, p.98-105, Mar.2020.
- [5] 山田祐也, 後藤厚宏, "サイバー攻撃による重要インフラのサービス停止がユーザ企業の事業継続に及ぼす間接的被害特性の検討", 第 15 回横幹連合コンファレンス, C-6-7, Dec.2024.
- [6] 山田祐也, 後藤厚宏, "サイバー攻撃による重要インフラサービス停止時の自治体・企業間連携についての検討", 信学技報, vol. 124, no. 422, ICSS2024-94, pp. 195-202, Mar.2025.
- [7] 国土交通省, "国土数値情報ダウンロードサイト", <https://nftp.mlit.go.jp/ksj/>, (参照 2025-08-22).

## 作業用(提出時に削除予定)

1 山田祐也, 後藤厚宏, "サイバー攻撃による重要インフラのサービス停止がユーザ企業の事業継続に及ぼす間接的被害のシミュレーション手法", コンピュータセキュリティシンポジウム 2024 論文集, pp.782-789, Oct.2024.

2 中小企業庁, "中小企業 BCP 策定運用指針 ~緊急事態を生き抜くために~ 3.1 事業を理解する", [https://www.chusho.meti.go.jp/bcp/contents/level\\_a/bcpgl\\_03a\\_1.html](https://www.chusho.meti.go.jp/bcp/contents/level_a/bcpgl_03a_1.html), (参照 2025-01-16).

3 片岡正次郎, 白戸智, 牛島由美子, 高宮進, "インフラシステムの災害復旧過程のモデル化と震災復旧シミュレーション", 土木学会論文集 A 1 (構造・地震工学) Vol.69, No.1, p.1-19, Jan.2013.

4 漆原史也, 吉田壮一郎, 岩崎翔吾, 柳沢隆己, 小森健一郎, 市

川学, 中井豊, "災害復旧シミュレータによるインフラ被害の可視化とその活用", 第 22 回社会システム部会研究会, p.98-105, Mar.2020.

5 山田祐也, 後藤厚宏, "サイバー攻撃による重要インフラのサービス停止がユーザ企業の事業継続に及ぼす間接的被害特性の検討", 第 15 回横幹連合コンファレンス, C-6-7, Dec.2024.

6 山田祐也, 後藤厚宏, "サイバー攻撃による重要インフラサービス停止時の自治体・企業間連携についての検討", 信学技報, vol. 124, no. 422, ICSS2024-94, pp. 195-202, Mar.2025.

7 国土交通省, "国土数値情報ダウンロードサイト", <https://nftp.mlit.go.jp/ksj/>, (参照 2025-08-22).