

# 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

## Simulation Method for Damage on User Companies Business Continuity Caused by Cyber Attacks on Critical Infrastructure

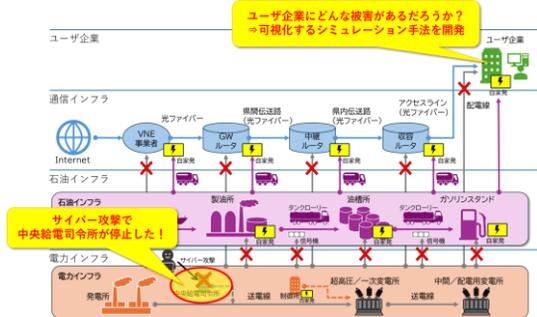
山田祐也・法制倫理分科会・情報セキュリティ大学院大学

Abstract: There is a risk of service outage of critical infrastructure due to the increasing number of cyber attacks targeting critical infrastructure facilities. This study proposes a simulation method for the indirect damage that service outages of critical infrastructure due to cyber attacks may cause to the business continuity of user companies, based on the simulation of damage caused by natural disasters. The simulation method consists of a framework with three models and parameters. In addition, the "Component Model of Critical Infrastructures," which models the dependencies among critical infrastructures and between critical infrastructures and user companies, is examined, and a model format that can express the characteristics of cyber-attacks is proposed. We will conduct simulations using the proposed format and confirm the effectiveness of the proposed model. In addition, we will discuss the scalability of the "Critical Infrastructure Component Model. This method is expected to contribute to the formulation of recovery plans for user companies' business in case of outage or contraction of critical infrastructure services due to cyber-attacks.

### 1. 研究背景と目的

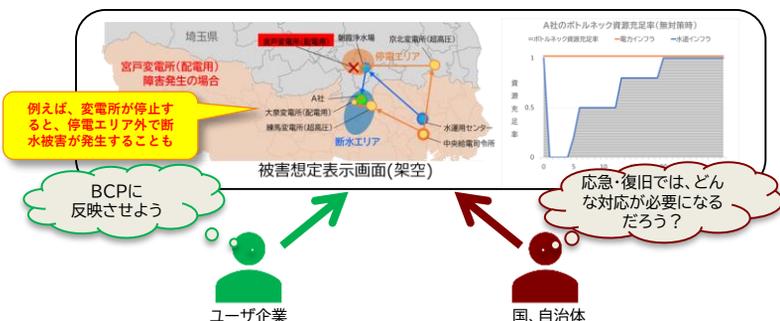
#### ●サイバー攻撃による重要インフラ停止が企業に及ぼす被害

- 多くの企業にとって、重要インフラは事業運営に必須な資源
- 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については検討が不十分 ⇒被害特性を可視化するシミュレーション手法を開発



#### ●サイバー版ハザードマップをつくりたい

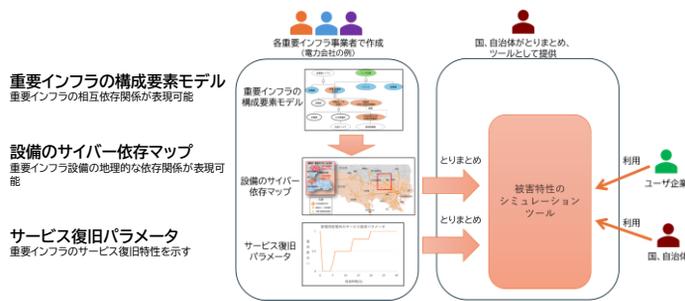
- サイバー攻撃によりある重要インフラ設備が停止したら、被害特性(被害範囲や他の重要インフラへの影響など)や復旧特性はどうかのわかる
- 自然災害のハザードマップのように、企業や自治体が対策を検討するための材料になる



### 2. シミュレーションの枠組みとモデル化手法の提案

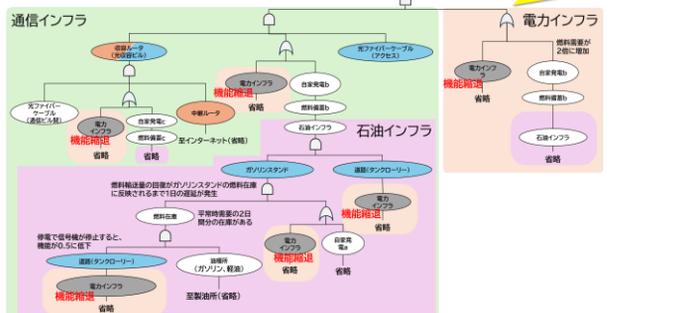
#### ●シミュレーションの枠組みを提案

- 重要インフラの構成要素モデル、設備のサイバー依存マップ、サービス復旧パラメータの3つのモデル、パラメータからなるシミュレーションの枠組みを提案



#### ●重要インフラの構成要素モデルを定義

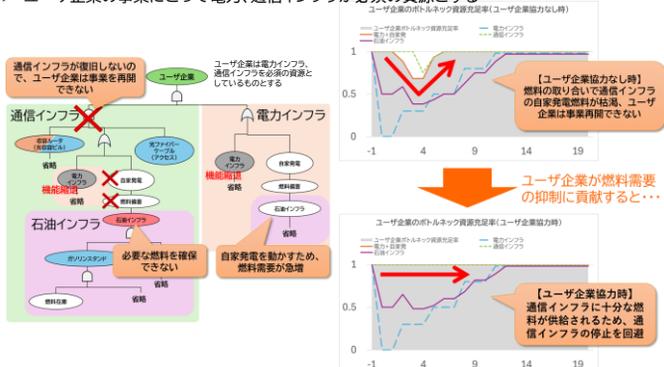
- 重要インフラの構成要素モデルの書式を定義
- 各重要インフラ分野の構成要素モデルを作成



### 3. シミュレーションの試行

#### ●提案モデルを用いてシミュレーションを試行

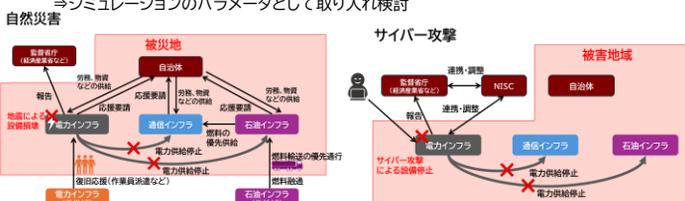
- サイバー攻撃により電力インフラが停止したと仮定して、シミュレーションを試行
- 対象重要インフラは、電力、通信、石油インフラとする
- ユーザ企業の事業にとって電力、通信インフラが必須の資源とする



### 4. 組織間連携の枠組みの検討

#### ●サイバー攻撃では、重要インフラ停止被害発生後の連携に課題

- 自然災害では、被災後に自治体や重要インフラ事業者が連携する枠組みが整備されている
- サイバー攻撃では、自治体や重要インフラ事業者の連携の枠組みが不十分
- 重要インフラ停止時の被害の大きさや復旧速度に影響を与える可能性がある ⇒シミュレーションのパラメータとして取り入れ検討



### 5. 今後

- サプライチェーン、自然災害のシミュレーションとのタイアップ
- 重要インフラ停止被害発生後の組織間連携の枠組みのあり方について深掘り
- サイバー攻撃による重要インフラ停止が及ぼす社会への影響と社会全体の復旧手順の検討(社会全体のレジリエンスについての検討)