平成22年度「サイバー攻撃動向等の環境変化を踏まえた重要インフラのシステムの堅ろう化に関する調査」報告書＜概要版＞

平成23年3月　株式会社 日立製作所

1. 目的と重要インフラの定義

- **目的**
  - 本調査は、重要インフラを取り巻く環境の変化のうち、主に「サイバー攻撃に対する重要インフラシステムの堅ろう性確保」との視点で、内閣官房情報セキュリティセンターとして取組むべき政策課題の検討に必要な基礎的な情報収集及び分析を行うことを目的とする
- **対象とする重要インフラと重要システム**

重要インフラ分野		IT障害やその影響の例	対象となる重要インフラ事業者等（注1）	対象となる重要システム例（注2）
情報通信		・電気通信サービスの停止 ・電気通信サービスの安全・安定供給に対する支障等 ・放送サービスの停止	・主要な電気通信事業者 ・主要な放送事業者	・ネットワークシステム ・オペレーションサポートシステム ・ニュース・番組制作システム ・編成・運行システム
金融	銀行 生命保険・損害保険 証券会社 金融商品取引所	・預金の払い出し、振込等資金移動、融資業務の停止 ・保険金の支払い停止 ・有価証券売買の停止　等	・銀行、信用金庫、信用組合、農業協同組合等 ・生命保険・損害保険・証券会社　等 ・金融商品取引所　等	・勘定系システム ・資金証券系システム ・国際系システム ・対外接続系システム ・保険業務システム ・証券取引システム ・取引所システム　等 （オープンネットワークを利用したサービスを含む。）
航空		・運航の遅延、欠航 ・航空機の安全運航に対する支障等	・主たる定期航空運送事業者 ・国土交通省（航空管制・気象）	・運航システム ・予約・搭乗システム ・整備システム ・貨物システム ・航空管制システム ・気象情報システム
鉄道		・列車運行の遅延、運休 ・列車の安全安定輸送に対する支障等	・JR各社及び大手民間鉄道事業者等の主要な鉄道事業者	・列車運行管理システム ・電力管理システム ・座席予約システム
電力		・電力供給の停止 ・電力プラントの安全運用に対する支障等	・一般電気事業者、日本原子力発電（株）及び電源開発（株）	・制御システム ・運転監視システム
ガス		・ガスの供給の停止 ・ガスプラントの安全運用に対する支障等	・主要なガス事業者	・プラント制御システム ・遠隔監視・制御システム
政府・行政サービス		・政府・行政サービスに対する支障 ・個人情報の漏洩、盗聴、改ざん	・各府省庁 ・地方公共団体	・各府省庁及び地方公共団体の情報システム（電子政府・電子自治体への対応）
医療		・診療支援部門における業務への支障等	・医療機関	・診療録等の管理システム （いわゆる電子カルテ、遠隔画像診断）
水道		・水道による水の供給の停止 ・不適当な水質の水の供給　等	・水道事業者及び水道用水供給事業者（ただし、小規模なものを除く。）	・水道施設や水道水の監視システム ・水道施設の制御システム等
物流		・輸送の遅延・停止 ・貨物の所在追跡困難	・大手物流事業者	・集配管理システム ・貨物追跡システム ・倉庫管理システム

「重要インフラの情報セキュリティ対策に係る第2次行動計画」（2009年2月3日情報セキュリティ政策会議） 別紙1

2. 事例に基づく重要インフラのシステムの堅ろう性に関する調査・分析

（1）日本における「サイバー攻撃」「重要システム」「システムの堅ろう性」の定義

サイバー攻撃*	DDoS・DoS 攻撃、不正侵入、重要情報の詐取、データ改ざん・破壊、不正コマンド実行等、情報通信ネットワークや情報システムを利用した電子的攻撃。
重要システム	重要インフラサービスを提供するために必要な情報システムのうち、重要インフラサービスに与える影響の度合いを考慮して、重要インフラ事業者毎に定めるものである。
システムの堅ろう性*	システムをサイバー攻撃から守り、サービスを安定的に提供できることとし、以下のようなシステムを「堅ろう性が高い」とみなす。 ・サイバー攻撃を受けにくいシステム ・サイバー攻撃を受けてもサービスを停止させないシステム ・サイバー攻撃によりサービスの一部が停止してもそれ以上拡大させないシステム ・サイバー攻撃によりサービスが停止しても早期に復旧できるシステム

*「サイバー攻撃」「システムの堅ろう性」については、本調査において暫定的に定義を策定

2. 事例に基づく重要インフラのシステムの堅ろう性に関する調査・分析
（2）海外と日本における定義又は概念の比較

- **海外の定義又は概念と、日本の定義を比較・検証した結果、国・地域によって詳細度は異なるものの、基本的な考え方に大きな差異はないといえる**
  - **「重要システム」の定義については、英国では国として細かく定めているが、それには2つの背景が考えられる**
    - 英国はEUの加盟国であり、EUでは「重要インフラ」の特定基準は加盟国によって決定する
    - 英国では、過去に大洪水、テロにより重要インフラの大規模な被害を経験していることから、より具体的に守るべき重要インフラが選定できるようにしている
  - **米国における各定義等は、同時多発テロを受けた後に、急速に整備が進められているが、その内容は、日本の定義と近い表現である**
  - **海外と日本の考え方に大きな差異はないが、今後再度定義の検証が必要**
    - ✓ 「サイバー攻撃」は不確定要素が多いため、5年程度経過したのちに　再度検証が必要
    - ✓ 「重要システム」「システムの堅ろう性」の双方は更なる検討の中で、レベル分けを行うことによって運用が明確になる

2. 事例に基づく重要インフラのシステムの堅ろう性に関する調査・分析

(3)海外のシステムがサイバー攻撃を被った要因

- **海外事例の分析により、システムがサイバー攻撃を被った要因をとして、我が国の重要システムの堅ろう化の視点で特に注意すべき代表的な6つの要因を抽出した**

【要因①】「重要インフラ」と外部との接続経路の問題

【要因②】「重要システム」へのアクセス者に対する認証管理の問題

【要因③】「重要システム」を構成する機器の物理的な防御対策(鍵付筐体による内部機器の防御等)の問題

【要因④】 独自システムとオープンシステムの脆弱性の問題

【要因⑤】 人的側面の管理の問題

【要因⑥】 新たな攻撃手法への対策の問題

2. 事例に基づく重要インフラのシステムの堅ろう性に関する調査・分析
(4)重要インフラ事業者へのヒアリング結果に基づいた対策状況

ア)「サイバー攻撃を受けにくいシステム」の観点

- **重要システムと外部との接続経路への対策**(要因①への対応)
  - インターネットへ接続したシステムと重要システムを分離することで攻撃経路を絶っている
  - 外部記録媒体接続ポートを物理的に閉鎖することで攻撃経路を絶っている
- **重要システムへのアクセス者に対する認証管理**(要因②への対応)
  - 技術的なアクセスコントロールにおいて攻撃経路を絶っている
- **重要システムを構成する機器の物理的な防御対策**(要因③への対応)
  - 入退室管理の徹底や、建物の構造等で物理的な攻撃経路を絶っている
- **オープンシステムの脆弱性の管理**(要因④への対応)
  - 重要システムには独自システム構成をとっている
  - 外部記録媒体を使用する前にはウィルスチェック専用端末でチェックを行ってから使用している
- **人的側面の管理**(要因⑤への対応)
  - 組織に関連する人員(従業員、委託先作業員等)へのサイバー攻撃を含む情報セキュリティ教育を定期的に実施し、組織内の規定や法・条例等を遵守させ、適性を見ながら　適正配置している
  - 重要システムの操作には勤続年数の長い信頼のできる役職付の人員を配置している
- **新たな攻撃への対応**(要因⑥への対応)
  - 組織内の専門部署や情報管理施策計画の中で、常に最新リスクについて検討している

2. 事例に基づく重要インフラのシステムの堅ろう性に関する調査・分析

(4)重要インフラ事業者へのヒアリング結果に基づいた対策状況

イ)「サイバー攻撃を受けてもサービスを停止させないシステム」の観点

- **重要システムと外部との接続経路への対策**(要因①への対応)
  - 外部との接続点について、サイバー攻撃を防御・検知する仕組みを導入している
- **重要システムへのアクセス者に対する認証管理**(要因②への対応)
  - 技術的なアクセスコントロールを強化している(同時にアクセスできるアカウント数の制限等)
- **重要システムを構成する機器の物理的な防御対策**(要因③への対応)
  - システムやオフィスを二重化し、バックアップを持つ構成(アクティブ/スタンバイ)、または両系とも現用として運用する構成(アクティブ/アクティブ)を採用している
- **オープンシステムの脆弱性の管理**(要因④への対応)
  - オープンなシステムと独自の構成を組み合わせることで、攻撃を受けた場合でも影響が拡大しにくい構成としている
  - オープンシステムに対しては、セキュリティ対策ソフトを導入している。また、セキュリティパッチについては適用時の影響を検討し問題ないことが確認できた上で適用している
- **新たな攻撃への対応**(要因⑥への対応)
  - 組織外での事故事例をもとに、自組織において対策を講じている

2. 事例に基づく重要インフラのシステムの堅ろう性に関する調査・分析

(4)重要インフラ事業者へのヒアリング結果に基づいた対策状況

ウ)「サイバー攻撃によりサービスの一部が停止してもそれ以上拡大させないシステム」の観点

- **人的側面の管理**(要因⑤への対応)
  - 攻撃を受けて重要システムが停止した場合や、重要システムが攻撃を受けているために重要サービスの維持へ影響を与えかねない場合には当該システムを切断し、手動で重要サービスを維持できる体制をとっている
  - 上記の様な対策を、重要サービスの維持に関する緊急時の対応手順、BCP等で明文化している
  - 緊急時の対応手順、BCPに則り、組織の人員や委託先作業員を含めた演習を実施している

エ)「サイバー攻撃によりサービスが停止しても早期に復旧できるシステム」の観点

- **人的側面の管理**(要因⑤への対応)
  - 通信の断絶で中央制御室から制御システムのコントロールが不可となったことにより、サービスが停止してしまった場合には、各拠点へ人員を出動させ、拠点間で連絡を取り合ってコントロールすることでサービスを復旧できる体制をとっている。また、対応に必要な人員を確保している
  - 上記の様な対策を、重要サービスの復旧手順、BCP等で明文化している
  - 復旧手順、BCPに則り、組織の人員や委託先作業員を含めた演習を実施している

2. 事例に基づく重要インフラのシステムの堅ろう性に関する調査・分析
(5)堅ろう性に関する提言

- **堅ろう性をより実戦的に高めるには、情報セキュリティ対策を「システム構成の層」と「人的構成の層」からなるものと捉え、それぞれのバランスに配慮して運用管理する「多層防御」が必要**

- **「システム構成の層」に関する提言**
  - 独自システムであっても攻撃を受ける可能性は常にあることを認識すること
  - 物理的・システム技術的・運用技術的の様々な角度から防御をし、管理徹底することが必要

- **「人的構成の層」に関する提言**
  - 正規社員の管理に加え、サプライチェーンを構成する人員、研究員(留学生、インターンシップ生)人員についても、適正配置、教育、演習を実施し、技術やモラルを維持向上させることが、重要インフラサービス維持の為の重要の鍵になる。また、重要サービスが完全に停止してしまうという危機的状況を回避するために、手動操作を担う人員の確保も重要である。

3. 重要インフラの事業継続計画（BCP）の在り方に関する調査
（1）日本のBCPの概況

- **日本のBCPの特徴**
  - 日本では地震や台風被害の発生率が高いことから、事業継続ガイドライン等においては、地震や天災等に対する「災害対策」が主眼とされており、本調査の目的である「サイバー攻撃」をリスクとしてフォーカスしているガイドラインは殆ど見当たらない
  - ただし、昨今では業務の運用維持には必要不可欠ともいえる「ITサービス」の事業継続に関するガイドラインは、災害対策ガイドラインと対になる形で発行されるケースが少なくない

- **日本のBCPと国際規格**
  - 日本における事業継続マネジメントに対する第三者認証制度については、一般財団法人日本情報経済社会推進協会（JIPDEC）がBCMS適合性評価制度を2010年4月より開始しており、認証基準は英国の「BS25999-2：2007」を採用
  - 国際規格化に先立った公開仕様書として2007年に発行された「ISO/PAS22399」では、日本の国内規格 「事業継続計画策定ガイドライン（経済産業省、2005 年発行）」、「事業継続ガイドライン一版（内閣府中央防災会議専門調査会、2005 年発行）」が参考規格として参照

- **日本政府が策定したガイドライン**
  - 事業継続ガイドライン二版（内閣府）
  - 事業継続計画策定ガイドライン（経済産業省）

3. 重要インフラの事業継続計画（BCP）の在り方に関する調査
（2）海外のBCPの概況

- **英国政府が策定したBCP施策**
  - 2004年民間緊急事態法（Civil Contingencies Act 2004）
  - 発行者：英国議会
  - 発効日/開始日：2004年11月18日成立
  - 背景：2000年以降の燃料危機や洪水の多発、また2001年の英国内口蹄疫や米国同時多発テロの発生等、従来の法律が緊急事態として定義していた国際戦争やストライキ以外の新しい脅威への対応として発効された

- **米国政府が策定したBCP施策**
  - 民間組織におけるインシデント対応の審査及び認証プログラム(PS-Prep)
  - 主管：米国国家安全保障省
  - 発効日/開始日：2007年8月
  - 背景：2001年米国同時多発テロや、2005年のハリケーンカトリーナ被災の際には、民間企業にも大きな被害が発生し市民生活への影響が拡大した事、及び事前に緊急事態対応計画類を準備していた企業は比較的被害が少なかった事も踏まえ策定された

3. 重要インフラの事業継続計画（BCP）の在り方に関する調査
（3）重要インフラ事業者へのヒアリング結果から得られたBCPの概況

- **一般的に、BCP本体には当該組織の業務上のリスクとその対応策が記載されており、 外部公開にそぐわないため非公開文書として扱われるが、事業者へのヒアリングにより得られたBCPの特徴は以下のとおり**

- **BCPの主な想定リスクとその対処法**
  - 災害 → 被害を受けた業務の早期再開を目的とした業務復旧型
  - 新型インフルエンザパンデミック → 必要最低限の業務に絞り込み、その継続を目的とした業務縮退型
  - ICTに関しては、障害等の技術的リスクがあることは認識されているが、BCPに含まれていない
    - 個別に緊急時対応マニュアルとして対応

- **BCPの見直し**
  - 年に1回実施
  - 重要業務の継続に不可欠なシステムの見直しは、
    情報資産の棚卸や年度の切り替わり時期に実施

3. 重要インフラの事業継続計画（BCP）の在り方に関する調査
（4）重要インフラ事業者へのヒアリング結果から得られたBCP演習の概況

- **演習の詳細シナリオは非公開文書として位置づけられているが、ヒアリングにて得られたBCP演習の特徴は以下のとおり**

- **演習シナリオ**
  - 災害対応訓練と併せて実施
  - 発生原因を決定してシナリオを作成し、正しく復旧できることを確認

- **演習の特徴**
  - BCPの実効性を検証することよりも、災害対応の訓練を行うことが主眼
  - ITシステムについてはシステム障害対応訓練として実施

3. 重要インフラの事業継続計画（BCP）の在り方に関する調査
（5）BCPに関する提言

- **BCPガイドライン内容の拡充**
  - 考慮すべきリスクについて、ITに関連するリスクも、「サイバーセキュリティを考慮する」などより具体的に例示する必要がある
  - ITシステムの緊急時の対応もBCPに関連付けるよう、ガイドラインに示す必要がある
  - 緊急時におけるセキュリティ水準の低下についてもBCP検討の際に盛り込むよう、ガイドラインに示す必要がある
- **重要インフラ分野毎のガイドラインの作成**
- **重要業務の継続に不可欠なシステムの抽出**
- **実効性のある演習と評価の実施**
  - 演習の実施、内部での監査を充実させる他、第三者認証制度の活用を促すことが必要である

3. 重要インフラの事業継続計画（BCP）の在り方に関する調査
（6）BCP演習に関する提言

- **BCP演習内容の拡充**
  - 発生原因には注目せず、「IT不通になった場合」等の発生事象から考えて復旧させる演習にすることが必要
  - 復旧が困難な演習シナリオとし、BCPの問題点を洗い出す演習内容にすることが必要
  - サプライチェーン・マネジメントを考慮した演習を実施することが必要

- **事業継続と情報システムの関わりを考慮した演習の実施**
  - 情報システムの復旧演習は、システム障害からの復旧だけを目的とするのではなく、事業全体のBCP演習の一環としてとらえ、重要インフラの各分野の特徴に応じて実施することが必要

- **分野合同演習**
  - 国として重要インフラの各分野の特徴に応じたBCPの策定レベル等を示すために、例えば、セプターカウンシル等との連携の中で、重要インフラ分野間で現実的（実効的）な策定レベル等を見極めていくことも重要だと考えられる。検討された策定レベル等を確認するための分野合同演習を実施できる環境を整えていくことも必要