先端科学技術の倫理 個人課題

高林秀
三宅研究室 博士前期課程 1 年
V-CampusID : 23vr008n

November 11, 2023

Abstract

本稿は本年度必修授業の先端科学技術の倫理の個人課題レポートである。

Contents

1 課題 1

1.1 課題内容

以下の文章の要旨をまとめる。

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

1.2 本文

この論文は、米国連邦政府（以下、連邦政府）に対し、非連邦システムと組織の非機密情報を保護するためのセキュリティ要件を提示するものである。

本論文が提供する要件は以下の場合において適用されるものである。

1. CUI が連邦政府以外のシステムや組織に常駐している場合
2. 連邦政府以外の組織が、連邦政府機関に代わって CUI を収集または管理していない場合、または連邦政府機関に代わってシステムを使用または運用していない場合。
3. CUI レジストリに記載されている CUI カテゴリについて、権限を付与する法律、規則、または連邦政府全体の方針によって規定される保護要件がない場合

なお本論文は、連邦政府機関とそれ以外の組織との間で締結される契約書や、その他の合意において、連邦政府機関が使用することを意図するものである。

1.2.1 第 1 章: 本論文の概要・構成と対象者について

この章では、本論文の概要、目的、対象読者、本論文で要求される要件の適用範囲について述べている。

本論文の目的　本論文は、CUI[1]の機密性を保護するために、推奨されるセキュリティ要件を連邦政府各機関に提供するものである。

本論文の対象読者　本論文は以下の属性に該当する人物を想定し記載されている。

- システム開発ライフサイクル (SDLC) の責任者
- 契約や合意の担当者
- 情報システムセキュリティ監督者
- セキュリティ評価を行う監査人

これらの属性にあたる、連邦政府機関および非連邦政府機関の人間で、下記のような役割をになっている人物を対象読者に想定するものである。

- 連邦政府機関の人物
  - ルールを作って他の人や組織に伝える役割を担っているチームや人
- 非連邦政府機関の人物
  - 連邦政府に定められたルールの順守義務を帯びている組織や人

[1]CUI (Controlled Unclassified Information) の略。管理された非機密情報の意味。連邦政府内の非機密情報のカテゴリのことで、連邦政府の各機関が取り扱う安全保障および原子力に係る情報のうち、機密（Classified）指定には至らないが適切に保護すべき情報を指す。2001 年の米国同時多発テロにおける情報共有・連携の失敗を教訓とし、連邦政府、州政府、部族政府、また各機関が別個で制定してきた非機密情報に対する取り扱いを統合する目的で制定された。

CUI 情報を扱う際の取り決め　本章では、連邦政府が CUI を扱う際に従うべき規則とその保護責任について述べられている。詳細な内容は省略するが、具体的に以下の規則が定められている。

- 連邦情報処理標準 (FIPS)[2] 199 および 200 の条件の一部を満たすこと
- NIST Special Publication 800-53, 800-60 示す条件の一部を満たすこと

連邦政府が CUI 情報を保護する責任は、その情報が政府機関以外と共有されても不変であり、連邦政府のシステム以外を使って CUI 情報を扱う際には、政府機関のシステムで扱う場合と同様の保護を行う必要がある、と示されている。

1.2.2　第 2 章: 非連邦政府機関における CUI 保護のガイドライン

本章では、連邦政府以外のシステムおよび組織における CUI を保護するために推奨されるセキュリティ要件を策定するための前提条件と方法論についての説明。

CUI 保護の前提条件　本論文に記載されている推奨セキュリティ要件は、以下の 3 つの基本的前提に基づいて策定される。

1. CUI 保護に関する法規制の一貫性
2. CUI 保護のためのセーフガードの一貫性
3. CUI の機密性影響値が FIPS 199 で定義される中程度の値を下回らないこと

これらの前提条件は、連邦政府か非連邦政府のシステムに関わらず不変であることが示されている。

CUI 保護のためのセキュリティ要件の大枠　CUI を保護するためのセキュリティ要件は以下 2 つの要件から成る。

1. 基本セキュリティ要件：連邦政府の情報とシステムのセキュリティに関する基本的なルール
    - 物理的な安全の確保：CUI 情報を安全に、物理的に制御して保管する必要性
    - CUI にアクセス可能な人間を限定すること
    - CUI を廃棄する際に外部に漏洩しないようにすること
2. 派生セキュリティ要件：基本セキュリティ要件を満たすために必要な追加要件
    - 記録メディアには CUI であることの印、配布期限を明記すること
    - CUI を有する記録メディアへのアクセスを制御し、持ち出しの際はその管理・保護責任を負うこと

[2]アメリカ国立標準技術研究所 が発行している標準規格で、軍事以外全ての政府機関及び請負業者による利用を目的として米国連邦政府が開発した公式発表の情報処理標準規格

- CUI を有する記録メディアが物理的に保護されていない場合、輸送時には暗号化機構を使用する必要があること
- 記録メディアの所有者がいない場合、その記録メディアを使用することはできないこと
- CUI のバックアップの機密性も保護すること

1.2.3 第 3 章: 非連邦政府期間における CUI 保護の 14 の要件

この章ではより具体的な CUI 保護のための 14 の要件について述べられている。また、これらの要件を元に、CUI を扱うシステムのユーザー承認方法の指針や維持に関する指針が示されている。

2 課題 2

2.1 課題内容

2.2 解答

3 課題 3

3.1 課題内容

3.2 解答