INEEL/EXT-04-02264

# Control Systems Security and Test Center

# 人的セキュリティガイドライン

Idaho National Engineering and Environmental Laboratory
（米国アイダホ国立工学・環境研究所）

2004年9月30日

邦訳： 一般社団法人 JPCERT コーディネーションセンター

INEEL/EXT-04-02264

# 人的セキュリティガイドライン

**Control Systems Security and Test Center**
**Idaho Falls、Idaho 83415**

作成：
DHS（Department of Homeland Security:米国国土安全保障省）
DOE Idaho Operations Office
DE-AC07-99ID13727

2004年9月30日

邦訳：
一般社団法人 JPCERT コーディネーションセンター

# 要約

多くの重要な産業や重要インフラが、自動化された制御システムに大きく依存している。制御システムを操作する人員の信頼、能力、運用上の安全を保証するためには、9.11以降の脅威に対処する有効な人的セキュリティプログラムが必要である。

2003年8月14日に米国で発生した最大規模の停電の原因は、人員の能力不足と教育・訓練不足、コミュニケーション不足、設備の不備であったことが判明し、停電の調査委員会は、政府機関による法規制、監視、違反への罰則を勧告した。この停電を深刻化させた要因は、人の行動の問題であった。しかし現在では、さまざまな産業や政府機関が人的セキュリティガイダンスを提供している。本書では、米国で全国的に認知されている7つの産業団体と政府機関の推奨事項に基づいて作成された人的セキュリティプログラムガイダンスを紹介する。

本書に示すガイダンスでは、人的セキュリティについて、信頼、能力、運用上安全な環境という3つのカテゴリを対象としている。信頼のカテゴリには、身元調査、身体的適性、知的適性、精神的適性、行動観察、自主的及び継続的な評価が含まれる。能力のカテゴリには、教育と経験、訓練（各機器、初期訓練、継続的訓練）、セキュリティ意識、試験による認定が含まれる。運用上安全な環境のカテゴリには、脆弱性及びリスク評価、ヒエラルキ、社内、社外、業者/ベンダの監査及び規則執行、緊急時対応計画、制御システムのアクセス制御、IDと認証、緊急時の連絡体制が含まれる。

信頼でき能力があり安全な人材を採用しスクリーニングすることは、制御システムのセキュリティを確保する上で非常に重要であり、本書の人的セキュリティガイダンスを広範囲に適用できる。ただし、本書の人的セキュリティガイドラインは汎用的な内容であるため、各設備の規模、場所、種類、既存のセキュリティ対策に基づいた個別の人的セキュリティプログラムが必要である。組織は、セキュリティベースの各種規格と手順に従って、従業員、コミュニティ、供給/流通ネットワークを保護する責任を認識し、その役割を果たす必要がある。

本翻訳文書は、一般社団法人JPCERT コーディネーションセンターが、原書の著作権を保有する アメリカ国土安全保障省（U.S. Department of Homeland Security: DHS）の許諾を得て翻訳したものです。

日本語版の内容について、原書に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありませんので、必要に応じて CSSP（Control Systems Security Program）のホームページより原書 ″Control Systems Security and Test Center : Personnel Security Guidelines″ をご参照ください。

また、翻訳監修主体は本文書に記載されている情報により生じる損失または損害に対し、いかなる人物あるいは団体にも責任を負うものではありません。

なお、当文書に関わる最新情報は以下の CSSP のホームページをご参照ください。

http://www.us-cert.gov/control_systems/

# 目次

# 表

# 略語

| | |
|---|---|
| API | American Petroleum Institute（米国石油協会） |
| CCST | Certified Control System Technician |
| CFR | Code of Federal Regulations（連邦規則集） |
| CIDX | Chemical Industry Data Exchange（化学業界向けデータ交換標準） |
| CNN | Cable News Network（ケーブルニュースネットワーク） |
| DHS | Department of Homeland Security（国土安全保障省） |
| DOE | Department of Energy（エネルギー省） |
| EPA | Environmental Protection Agency（環境保護庁） |
| ID | Identification |
| ISA | Instrument Society of America（国際計測制御学会） |
| NERC | North American Electric Reliability Council（北米電力信頼度協議会） |
| NRC | Nuclear Regulatory Commission（原子力規制委員会） |
| SDWA | Safe Drinking Water Act（安全飲料水法） |
| SVA | Site Vulnerability Assessment |
| U.S. | United States（アメリカ合衆国） |

# 1. はじめに

**はじめに**

- 組織は、自動化された制御システムに大きく依存している。
- 信頼、能力、運用上の安全は、制御システム運用の安全確保のために非常に重要である。
- 一部の組織は、9.11以降の脅威を反映するために人的セキュリティプログラムを更新する必要がある。
- 本書では、米国で全国的に認知されている7つの産業団体と政府機関の推奨事項に基づいて作成された人的セキュリティプログラムガイダンスを紹介する。

本書は、CSSTC（Control System Security and Test Center）が、Near-term Center Operations Task（短期センター業務タスク）である『Control Systems Personnel Security Guidance』（制御システム人的セキュリティガイダンス）の一部として作成したものである。このタスクの目的は、主要な産業と政府機関の人的セキュリティガイダンスを比較して、これまでのプラクティスに基づき、デジタル技術に基づく制御システムに大きく依存する重要インフラ設備向けのガイドライン集を策定することである。このタスクは、US-CERTの制御システムセキュリティ国家戦略（National Strategy for Control Systems Security）のゴール4、すなわち、「安全でないプラクティスに関する問題の認識と教育を通じて、プラクティスの改善と適切なセキュリティポリシーのための基盤作り」への模索を部分的に支援するものである。

組織の制御システムの安全確保と運用には、信頼でき能力があり運用上安全な人材を獲得することが非常に重要である。つまり、人的セキュリティプログラムは最優先課題である。本書で使用する「組織」とは、法人かどうかや公共か民間かを問わず、独自の機能と管理体制を備えた会社、企業、事業、団体、またはそれらの組み合わせにおいて、そこで働く人々の集団を指す。石油、ガス、流通システムなど国の重要な産業、化学プラントなどの産業設備、発電や配電設備などのインフラ、交通インフラは、制御システムに大きく依存する組織であり、制御システムのセキュリティが大きな課題となっている組織の例である。

組織は、安全性の維持、経済活動の維持、公共の安全衛生の保護、環境保護のために制御システムに依存している。このような制御システムは、重要な産業を監視及び管理する重要インフラの一部である。制御システムの安全は、それを運用する人員に左右される。2001年9月11日以降、多くの組織が、個々の人員が果たす責任に基づいて、人的セキュリティプログラムの見直しを行ってきた。政治や社会の情勢の世界的な変化が動機となる意図的な行為により、新たな脅威がもたらされていることを、組織は認識しなければならない。

この新たな脅威に対応して、いくつかの組織では、制御システムと重要情報への不正アクセスを防ぐために、人的セキュリティプログラムの導入や改訂の必要が生じている。

さらに、人的セキュリティと制御システムの完全性のために、信頼性と能力の具体的な基準を定める必要がある。人的セキュリティプログラムは、保護対象の情報や制御室へのアクセスを人員に許可するに先立ち、人員の経歴、技能、業務上の制約を検討するものでなければならない。このプログラム全体の目的は、アクセス権限が与えられた人員が、信頼でき能力があり、運用上安全であることを保証することにある。また、従業員と職務環境を含めた組織は、他の人員や社会の安全衛生に影響を及ぼしかねない、許されないセキュリティリスクの要因とならないように、安全な運営を行う必要がある。

本書では、米国で全国的に認知されている以下の7つの組織が推進する人的セキュリティプラクティスを精査、分析した結果に基づいて、人的セキュリティプログラムのための推奨事項とガイドラインを示す。

- ISA（Instrumentation, Systems, and Automation Society:国際計測制御学会）
- NRC（Nuclear Regulatory Commission:原子力規制委員会）
- DOE（Department of Energy:エネルギー省）
- EPA（Environmental Protection Agency:環境保護庁）
- NERC（North American Electric Reliability Council:北米電力信頼度協議会）
- API（American Petroleum Institute:米国石油協会）
- CIDX（Chemical Industry Data Exchange：化学業界向けデータ交換標準）

本書は、信頼、能力、安全な環境という3つの主な概念にわたり編成されている。これらの概念は、本ガイダンスの目的から次のように定義される。

- 信頼とは、信頼性、完全性、適性の尺度であり、各人員が、安全な運用に対するセキュリティ脅威にならないことを保証する基準として使用される。
- 能力とは、人員に経験と技能があり、人的セキュリティプログラム、及び任命された作業範囲の技術要件について必要な知識を有し、理解していることを示す。
- 運用上安全な環境とは、毎日の安全な運用を保証するために必要な制御システム、オペレータ、優れた管理策、セキュリティ上の制約などを幅広く含み、信頼でき能力のあるオペレータが職務についていることが前提となる。

## 1.1 適用範囲

本書は、組織での利用を目的としており、制御システムの人員（施設内の制御システムに直接アクセスするオペレータを含む）に適用すべきセキュリティ対策の推奨事項を提示する。組織は、業者、下請業者、ベンダによって採用されている人的セキュリティプログラムを適用する場合もある。その場合、本書のガイダンスに合わせてプログラムを部分的に差し替え、補足、複製することにより、本書のガイドラインの要件を満たす必要があ

る。

組織には、業者、ベンダ、その他関係する制御システム人員のアクセス権限の割り当て、削除、取り消しを行う責任がある。本書では、推奨されるガイドラインを次の領域に分類する。

1 信頼

2. 能力

3. セキュアな環境

# 2. 背景

**背景**

- 米国最大の停電の原因は、要員の能力不足と訓練不足であった。
- 調査委員会は、法規制の施行により、政府による監督と違約金を課すことを勧告した。
- 業界と政府による監督機関は、人的セキュリティに関する勧告を行っている。
- 人的セキュリティプランを更新している組織もあれば、更新していない組織も存在する。

2003年8月14日、過去最大規模の停電が米国を襲った。その経済的損害は、オハイオ、ミシガン、ペンシルベニア、ニューヨーク、ニュージャージー、バーモント、マサチューセッツ、コネチカット、オンタリオなど広い地域に及んだ。調査委員会が設置され、停電の原因究明と再発防止に向けた勧告が行われた。2004年5月18日、CNNのWebサイト（www.cnn.com）に、「8月14日の停電の原因は、オハイオ州アクロンのファーストエナジー社のコミュニケーション不足、設備の不備、訓練不足である」という記事が掲載された。調査委員会は、信頼性に関する法規制の施行により、政府による監視と違反への罰則を課すことを勧告したが、「電力業界は現在、自主的な要求事項を定めている・・・・この要求事項は民間団体である北米電力信頼度協議会（North American Electric Reliability Council）によって管理されているが、この団体には罰則権限はない」。さらに、調査委員会は、「オペレータ、信頼性コーディネータ、サポート要員に対する教育及び認定要件を改善すること」及び「送電網の物理的安全性とサイバーセキュリティを向上させること」（停電は回避可能だった）と勧告した。DOEの発表によると、この停電による経済的損害は約60億ドルにのぼった（「Transforming the Grid to Revolutionize Electric Power in North America」より）。8月14日の停電を深刻化させた要因は、人の行動の問題である。

さまざまなガイドラインを通じて制御システムを保護する必要性は、組織において長い間認識されている。現時点で各組織が人的セキュリティガイドラインを導入しているため、さまざまな人的セキュリティ計画の見直しが行われた。現在、組織が重点を置いているのは、国内外のテロリズムから制御システムを守るためのセキュリティである。これらの各組織では、社会、従業員、環境、経済活動に関連するリスクの種類を評価し、リスクや脆弱性を緩和するためのガイダンスを特定するというアプローチを採用している。本書の作成にあたり、米国国土安全保障省（DHS）は、制御システムの人員に関して次の組織の最新文書を精査した。

- API（American Petroleum Institute:米国石油協会）
  - APIは、米国内に石油ガス施設を所有しており、資産の保護と安全確保に自主的に取り組んでいる。この組織は、商用運営と設備の可用性に強い利害関係をもっている。

APIは、さまざまな民間組織からの会員で構成され、違反への罰則権限がある。

- APIの使命は、消費者ニーズを満たすために不可欠な、強固で発展力のある米国の石油及び天然ガス産業を、効率的かつ環境保全に貢献する方法で支援し、国の政策に影響を与えることにある。

- CIDX（Chemical Industry Data Exchange）
  - CIDXは、グローバルな化学業界のバリューチェーンに参加する企業の上級管理職で構成され、資産の保護及び安全確保に自主的に取り組む組織である。この組織は、商用運営と設備の可用性に強い利害関係をもっている。CIDXは、さまざまな民間組織からの会員で構成され、違反への罰則権限がある。
  - CIDXの使命は、化学業界各社と取引相手との間の業務の簡易化、高速化、コスト軽減である。
- NRC（Nuclear Regulatory Commission:原子力規制委員会）
  - NRCは、原子炉、核原料、廃棄物の規制を定め、核物質と核施設を使用する民間組織が連邦行政命令集（CFR）10条、法律、法規、政策で定められた要件を遵守することを求める。NRCは、民間核施設の従業員ではない米国政府職員で構成され、違反への罰則権限がある。
  - NRCの使命は、副産物、原子力源、特殊な核物質の民間人による使用に関する法規則を定めることにより、公衆衛生及び安全の十分な確保、防衛・治安の推進、環境保護を実現することである。
- DOE（Department of Energy:エネルギー省）
  - DOEは、DOEの各局、本部、本部運用部、安全管理局によって発行された要求事項に、すべてのDOE要素及び設備が準拠することを義務付けている。DOEは、DOE設備を監督する米国政府職員で構成され、違反への罰則権限がある。
  - DOEの使命は、米国経済とエネルギー安全保障を発展させ、科学技術の革新を促し、国内の核兵器施設の環境浄化を保証し、国家の安全を保護することである。
- EPA（Environmental Protection Agency:環境保護庁）
  - EPAは、すべての組織を統制する機関であり、CFR第40条、法律、法規、政策への遵守を義務付けている。EPAは、各組織を監督する米政府職員で構成され、違反への罰則権限がある。
  - EPAの使命は、人の健康と環境の保護である。
- NERC（North American Electric Reliability Council:北米電力信頼度協議会）
  - NERCは、電力業界に勧告を行い、電力インフラシステムの保護に適用するガイダンスを提示する。NERCは、任意の非営利組織であり、業界の利益で成り立っているため、違反への罰則権限はない。

- NERCの使命は、大型電力システムの信頼性、適合性、セキュリティを確保することにある。

- ISA（Instrumentation, Systems, and Automation Society:国際計測制御学会）
  - ISAは、制御システム業界に勧告を行い、セキュリティ向上のためのガイダンスと訓練を提供する。ISAは、任意の非営利組織であり、業界の利益で成り立っているため違反への罰則権限はない。
  - ISAの使命は、世界の技術者及び組織の効果を最大限に高め、あらゆる産業と応用分野における計測、システム、自動化の科学、技術、及び手法を発展させ応用させることにある。

# 3. 推奨されるガイドライン

## 3.1 信頼

**具体的なガイドライン**

- 信頼
  - 身元調査
  - 身体的適性、知的特性、精神的特性
  - 行動観察
  - 自主的及び継続的評価
- 能力
  - 教育と経験
  - 訓練（機器、初期、継続的訓練）
  - セキュリティ意識
  - 試験による認定
- セキュアな環境
  - 脆弱性とリスクの評価
  - ヒエラルキ
  - 内部監査、外部監査、業者/ベンダの監査
  - 規制執行
  - 緊急時対応計画
  - 制御システムアクセス制御
  - IDと認証

**身元調査**

組織は人員に対して、過去のすべての雇用主の就業証明書を取得するか、就業証明書のすべての内容を明確かつ判読可能な形式で示した文書を作成することを求める。雇用情報の確認を行う担当者全員に対して、以下の詳細な連絡先情報を提示する。

- 名前
- 住所
- 電話番号
- 雇用時からの役職の説明
- 現在の会社名、電話番号、住所

要求されるセキュリティアクセス許可によっては、その人員の前の管理者に対して、すべてのフォームに署名を求める。雇用主に直接確認できない場合は、雇用時の同僚が署名し、それを公証人が認証する方法を採用する。さらに、雇用主がその雇用期間について確認できない説明を詳細に記載する。すべての文書は、記録として永久保存する。身元調査では、最低限、以下について確認する。

- 窃盗または暴力犯罪の前科
- 逮捕歴
- 職場での暴力または恐喝行為
- 個人の識別情報
- 職務経歴
- 学歴
- 前科

- 自動車の運転記録
- クレジット記録
- 徴兵歴
- 専門家認定
- 陰性の薬物検査結果

**身体的適性**

オペレータは、免許を持つ医師による身体検査に合格する必要がある。この検査では、組織が定めた職務に関する適性プログラムに基づいて、職務の実施に必要な身体能力を測定する。

**知的適性**

組織の工程管理の効果的実施に直接関与する職務に就く人員は、注意を怠らない性質と、適切な判断、命令の遂行、担当職務の理解などの能力があることを証明する必要がある。このような職務に就く人員は、適切な判断力と表現力によって、職務に必要な書面、口頭、音声、目視などの手段による正確なコミュニケーション能力が求められる。てんかんや糖尿病の病歴や診断がないことが条件になるが、このような病歴や診断歴がある場合には、適切な投薬によって症状の抑制が可能であり、職務中に昏睡状態や意識不明状態に陥ることはないという証明書を提出する必要がある。

**精神的適性**

信頼性に影響を与える可能性のあるあらゆる顕著な精神的特性について、考えられる影響を評価する必要がある。制御システムのオペレータは、情緒不安定であってはならない。また任命された職務の効果的遂行の妨げになりかねないセキュリティ上の脅威をもたらす組織と協力関係があってはならない。この判定は、免許を持った精神分析医や医師など、情緒不安定の診断に関する訓練を受けた者が行う。

**行動観察**

個人の行動について、放置すると公衆の安全衛生に弊害をもたらす可能性がある行動の変化を観察する必要がある。人員は、アルコール依存症または薬物依存症の病歴または診断があってはならない。ある場合は、職務遂行が可能であるという合理的判断基準となる更生プログラムを完了したことを示す証明書を提出する。

**自主的評価**

組織は、職務遂行のための認定とセキュリティに関する情報を報告する機会を従業員に与える必要がある。

**継続的な評価**

担当の管理者が人員を継続的に観察し、セキュリティに関する職務の遂行上、情緒不安定の兆候がみられた場合には適切な是正策を講じられるように調整する。担当の管理者によって情緒不安定の兆候が報告された場合は、免許を持ち、訓練を受けた担当者が確認を行う。

## 3.2　能力

### 教育と経験

人員は、高等学校を卒業しているか、あるいは実務で必要な基本的な数学、言語、論理展開の能力を測定できる高等学校卒業相当の能力試験に合格し、担当職務に要求される能力と知識を有している必要がある。また、雇用主によって規定される、担当職務に要求される適切なレベルのオペレータの認定取得のために、規定された最低限のOJTを受けていることが求められる。

### 訓練

組織が事業計画または危機管理計画で指定した担当業務または職務を行うための訓練が必要な人員は、配属前に、組織が文書にまとめた訓練及び資格認定計画に従って、担当業務及び職務の訓練を受ける。人員は、適切なレベルのオペレータ認定を取得するために、所定の訓練を受ける必要がある。オペレータは次のような専門科目に関する訓練を受ける必要がある。

- 制御理論
- アナログ及びデジタルエレクトロニクス
- マイクロプロセッサとコンピュータ
- 特定分野の計装の運用と保守
- 電気の基本
- ベンダ独自の機器に関するベンダ認定

組織は、必要に応じて、以下を測定及び制御する装置に関する訓練を実施する。

- レベル
- 温度
- 圧力
- 流量
- 力
- 電力
- 位置
- 動き
- 物理的特性
- 化学組成

### セキュリティ意識

人員は、セキュリティ意識に関する説明及び訓練を継続して受ける。人員が組織を保護する役割である場合は、次の科目に関する訓練を含める必要がある。

- 敵対する団体の活動
- 敵対する団体の動機と目的
- 敵対する団体が目的達成のために取り得る戦術と武力
- 組織の設備または輸送手段に対して取り得る破壊行為に使われる装置と機器の認識
- 設備の警備体制と警備行動
- 物理的及びサイバーセキュリティ境界の種類
- 敵対する団体が目的達成に取り得る武器
- ロック及び主要な制御システム境界
- 設備の潜在的な脆弱性と破壊行為の被害
- 使用する警報システムの種類
- 制御システム情報の保護
- アクセス制御システムの操作
- 侵入行為が確認または試行された場合の危機管理対応
- コンポーネント障害後の制御システムの操作
- パスワード、ネットワーク設計、プロセスの詳細、回路図など、セキュリティ情報のソーシャルエンジニアリングや不正な問合せ

### 継続的な訓練

組織は、テクノロジの変化に対応し、最先端の知識を採用し、新技術を理解することが求められる。認定期間の終了後、人員が認定を更新できるかできないかを再度確認する必要がある。組織は、オペレータが保有している認定レベルに基づいて、認定の更新及び期限切れに応じた訓練要件を定める。また、認定期間が切れた人員の再認定のための手続きを定める。この手続きには、人員の経験のレビュー、訓練、再試験を含める。

### 認定試験

従業員が制御システムの運用を行う場合は、事前に認定が必要になる。この認定を得るためには、次の内容に関する知識を確認する試験に合格する必要がある。

- キャリブレーション
- ループチェック

- トラブルシューティング
- 保守/修理
- プロジェクト編成
- 独自仕様のシステム

試験では、選択問題と記述問題を出題し、知識やスキルの実施能力を確認することが望ましい。

## 3.3　セキュアな環境

### 脆弱性とリスクの評価

リスクの評価、運用リスクに関する意思決定、制御システム運用に関わるリスクの軽減目標の達成には、SVA（Security Vulnerability Assessment：セキュリティ脆弱性評価）プロセスが必要である。SVAでは、次の項目の特定と分析を行う。SVAでは、次の内容を特定及び分析する。

- 制御システムに関連したインシデントの原因になり得る実際のイベントまたは潜在的なイベント
- 制御システムに関連する潜在的なイベントの可能性とその結果
- リスクが及ぶ範囲とリスク軽減の活動を比較検討するための包括的かつ統合された手段
- リスク軽減の活動を選定し導入するための、体系的で容易に伝えられる手段
- SVAプロセスの改善目標に基づいて、プログラムの成果を追跡する手段
- 政府機関と組織で脅威情報を共有するためのコミュニケーションプログラムを確立する手段

上記に加えて、テロリストによる攻撃リスクを評価する必要がある。攻撃リスク評価では、行為や攻撃が行われる可能性、テロリストの行動のタイプ、それが及ぼす結果を、システムの規模や場所によって判定する。この評価には、以下を対象とする潜在的なリスクを含める。

- 作業員
- 環境及び周辺の地域社会
- ローカル、地域、国レベルの経済への影響
- 近接または相互依存関係にある設備とインフラ

利用可能なすべての情報を意思決定プロセスに盛り込むことは、セキュリティ管理フレームワークの重要な要素の1つである。オペレータが制御システムにとって重大なリスクを理解する上で影響を及ぼす情報は、さまざまな情報源からくる可能性がある。このような情報を収集及び分析する場合、オペレータは最も有利な立場にある。オペレータは、入手した情報を統合することによって、インシデントのリスクが最大になる部分を特定し、リスク軽減のための賢明な意思決定を支援することができる。

さらに、このような情報に対して厳重に安全対策を講じ、情報提供を「知るべき」人員のみに限定する点も考慮する必要がある。脆弱性分析とリスク評価では、資産 (資産損

失の影響)、脅威、対応策の重大度に優先順位を割り当てる方法が提示される。多くの場合、リスク及び脆弱性の評価には、チェックリストによる検査が利用される。チェックリストには、リスク評価の概念に関する標準的なアプローチの概要や、評価プロセスの各ステップで使用される質問と考慮点が記載される。このようなリスク評価では、事業全体と脆弱性に重大な影響を与える可能性のある設備を特定することができる。

### ヒエラルキ

人員は、制御システムの区分と同等以上の基準に対して認定を受ける。各制御システムを担当するオペレータは、そのシステムの区分と同等以上の有効な認定を取得しているものとする。プロセス制御/システムの完全性に関して、潜在リスクに影響を与えるような意思決定を行う、すべての人員に認定取得を求める必要がある。また、組織は業務シフトごとに、指定された認定を取得したオペレータを配置する。

### 内部監査

セキュリティ評価手法やリスク緩和策の成否について、組織は情報収集と定期的な評価を行う必要がある。また、組織はセキュリティ管理の適切な意思決定を支援するために、管理体制と手順の有効性も評価する必要もある。たとえば、見直すべき項目には次のものが含まれる。

- セキュリティ及び環境に関する現行の規制
- 妥当性と有効性の検査
- 遵守と違反の統計
- 執行と管理のフォローアップ
- 人的セキュリティプログラムの予算と人員配置
- 訓練が妥当で最新であること
- 訓練要件と試験の成績
- データ管理システム
- SVAの結果、精度、アクション項目

セキュリティインシデントを詳細に記録しておくことによって、管理者は傾向を特定し、事実を集めて調査を成功に導くことができる。また、インシデント管理ソフトウェアを活用しているセキュリティ管理者もいる。このようなソフトウェアは、グラフ作成や検索機能により、攻撃や損失発生のパターン識別やセキュリティの問題特定に役立つ。インシデントデータが報告され記録された場合、そのデータは分析目的のみのために利用する。管理者は、インシデント報告の経路を複数確立する必要がある。たとえば、監査担当者の

電話番号と電子メールアドレスの両方を用意するなどを決める。また、一部の会社は、匿名で使用できる従業員用ホットラインを設置し、従業員に疑わしい事例の報告を奨励している。また、セキュリティインシデントの報告を従業員の義務として定めるのも有効である。管理者は定期的に取引履歴を分析し、基準から外れた内容がないか確認する。管理者は、ユーザ認証チェックに加えて、通常とは異なる時刻、頻度、長さのアクセスに注意を払う。組織は、人的セキュリティプログラムの実施日から12カ月以内に監査を行い、本ガイドラインの要件が満たされているかを確認することを検討する必要がある。

**外部監査**

人的セキュリティプログラムでは、プログラムの改訂及び実施において、外部組織に対して継続的な審査を求める必要がある。利害関係者で構成される委員会または諮問委員会を設置することを強く推奨する。たとえば、利害関係者には、次が含まれる。

- オペレータ
- 環境/公衆衛生関連団体
- 警察/警備団体
- 一般大衆
- 一次業者と下請業者
- プロセス制御の技術支援プロバイダ
- 組織の管理者
- 訓練担当者

組織は、数年ごとに外部審査を実施する。

**業者/ベンダの監査**

組織は、業者またはベンダの人的セキュリティプログラムを採用する場合、記録にアクセス可能でなければならず、業者またはベンダのプログラムを12カ月ごとに監査することによって本ガイドラインの要件が満たされているかを確認することを検討する。また、所見、推奨事項、是正処置を含め、業者またはベンダの人的セキュリティプログラムの有効性に対して責任を持ち続けることが求められる。

**懲戒処分**

組織は、オペレータ認定の一時停止や、オペレータの不正行為に対して適切な懲戒処分を行う能力を有する。不正行為には、次のようなものが含まれる。

- 詐欺行為

- アプリケーションの改ざん
- 運用記録の改ざん
- オペレーションでの重大な過失
- 不適性
- 担当職務の遂行の過程での、適切な配慮または判断を怠る
- セキュリティ違反の傾向

**緊急時対応計画**

組織の緊急時対応計画では、主要な参加者に計画の効果的な実施に必要なスキルと知識があることを保証するために、参加者の訓練を実施する。主な対応者を対象とする訓練及びオリエンテーションプログラムを作成し、これを定期的に見直す。定期的な演習には、該当する場合は法執行機関、消防署、諸機関からの初期対応など、各種シナリオを含める。すべての演習が終了した時点で、全体的な「確認事項と反省点」をまとめ、緊急時対応計画に盛り込む。さらに、「確認事項と反省点」に基づいて、以後の訓練及びオリエンテーションセッションを実施する。

組織は、セキュリティ条件に基づいて、オペレータなどの人員に対して助言及びコミュニケーションを行う手段を整備する。また、該当機関との緊急連絡方法及び連絡先を定める手段を検討する必要がある。該当機関に連絡するためのハードウェアと手段の両方において、予備の緊急連絡方法を検討する必要がある。

**制御システムアクセス**

制御システム領域には、電子的なまたは生体認証によるアクセス制御システムを備えたゲートや改札口を設置し、入退出を記録して、以下のような制御システム領域の物理的な安全性を確保する。

- モーター制御センター
- ラックルーム
- サーバルーム
- 通信ルーム
- 制御システムルーム

システム領域へのアクセス制御には、次に示す物理的管理策を使用する。

- サインインログ
- 写真付きのIDバッジ

- キーカードと番号バッド
- テレビ監視システム

次に示すサイバーセキュリティ対策を検討する。

- 有効な設定がなされたファイアウォール
- 最新の更新ファイルによるウィルス保護
- 現場から業務ネットワークを隔離するDMZ
- 侵入検知システム
- 暗号化モジュール

階級や慣例によるアクセス許可ではなく、「最小限のアクセス」、「情報を必要な人だけに開示する（Need to Know）」、「機能分離」の原則に従い、ユーザに権限を与える手順を厳密に管理する。権限のある人員のみに中央コンピュータルームへの物理的なアクセスを許可し、訪問者はすべて監視する。

### IDと認証

制御室へのアクセスには、定期的に変更される推測されにくいパスワードまたは多要素認証を使用する。多要素認証では、「知識（あなたが知っていること）」（パスワード、宛先IPアドレス、電話番号など）、「所持（あなたが持っているもの）」（トークン、デジタル証明書）、「属性（あなた自身）」（生体認証など）を使用する。

# 4. 結論

本書に示した概念は、制御システムを担当する人員のセキュリティに広く適用でき、人的セキュリティガイダンス策定の出発点となる。ただし、当然ながら本書のセキュリティガイダンスは汎用的なものである。したがって個々の組織は、関係者と協力して、組織自身についてさらに詳細な評価を実施し、組織の資産を保護するための最善の方法を決定する必要がある。なぜなら、潜在的な脅威と適切なセキュリティ対策は、組織の規模、場所、設備の種類、すでに実践されているセキュリティ手段によって大きく異なるためである。組織の制御システムのセキュリティを確保するためには、信頼でき、能力があり、安全な人材を採用しスクリーニングすることの重要性を認識して、プロアクティブで明確な人的セキュリティプログラムを策定することが最優先課題である。組織は、セキュリティベースの各種規格と手順に従って、従業員、コミュニティ、供給/流通ネットワークを保護する責任を認識し、その役割を果たす必要がある。これには、信頼性があり安全な人的セキュリティプログラムの策定、制御システムへのアクセスとインフラの保護、地域の緊急時対応チームとの訓練などが含まれる。

**結論**

- 信頼でき能力があり、安全な人材を採用しスクリーニングすることは、制御システムのセキュリティを確保するために非常に重要である。
- 人的セキュリティの概念は、広い範囲に適用できる。
- 本書の人的セキュリティガイドラインは汎用的であるため、各設備の規模、場所、種類、既存のセキュリティ対策に基づいた調整が必要になる。
- 組織は、セキュリティベースの各種規格と手順に従って、従業員、コミュニティ、供給/流通ネットワークを保護する責任を認識し、その役割を果たす必要がある。

9.11以来、多くの組織が制御システムの人的セキュリティプログラムの再評価を行っており、規模、地理的な場所、従業員やコミュニティに対する潜在リスク、潜在的な攻撃リスクなどに基づいて人的セキュリティプログラムの改善に自主的に取り組んでいる。潜在的及び実際のセキュリティ脅威を適切に評価及び対処するために、DHSは選ばれたセキュリティプログラムガイダンスを評価し、この人的セキュリティガイダンスを作成した。本ガイダンスは、組織のデザイン、安全性、環境保護、緊急時の対策、破壊行為からの保護にかかわる信頼、能力、運用上安全な取り組みという強固な土台を基礎としている。

# 5. 参考文献


"Blackout Was Preventable, Probe Finds," (www.cnn.com/2004/US/04/05/blackout.report/index.html), May 18, 2004

Parks, Bill, 2003, "Transforming the Grid to Revolutionize Electric Power in North America," *U.S. Department of Energy, Edison Electric Institute's Fall 2003 Transmission, Distribution and Metering Conference, October 13, 2003.*

**DOE**

DOE M 472.1-1B, *DOE Personnel Security Program Manual,* July, 2001.

DOE O 472.1C, *Personnel Security Activities,* March, 2003.

**NRC**

10 CFR 73.56, *Personnel access authorization requirements for nuclear power plants*

10CFR 73.57, *Requirements for criminal history checks of individuals granted unescorted access to a nuclear power facility or access to Safeguards Information by power reactor licensees.*

**API**

*Security Guidelines for the Petroleum Industry (Second Edition)*

**ISA**

ISA-TR99.00.01-2004, *Security Technologies for Manufacturing and Control Systems*

ISA-TR99.00.02-2004, *Integrating Electronic Security into the Manufacturing and Control Systems Environment.*

*ISA Certified Control System Technician (CCST) Program* (www.isa.org)

**EPA**

Federal Register SDWA Section 1419, *Guidelines for the certification and re-certification of operators of community and non-transient, non-community public water systems.*

**CIDX**

*Site Security Guidelines for the U.S. Chemical Industry* (American Chemistry Council Chlorine Institute, Inc. and Synthetic Organic Chemical Manufacturers Association)

*Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.0, Preliminary Draft.*

**NERC**

*Security Guidelines for the Electricity Sector* (Version 1.0)

# 付録A

# 組織の基準比較

# 付録A

# 組織の基準比較

表 A-1 組織の基準比較

| 概念 | 基準 | ISA | NRC | DOE | | NERC | API | CIDX |
|---|---|---|---|---|---|---|---|---|
| 信頼 | 身元調査 | 以前の雇用主が署名した就業証明書、事実に反しないID、学歴、クレジット履歴、犯罪歴、自動車の運転記録、運転免許証の履歴、徴兵履歴 | 職務経歴、指紋によるID検証、学歴、クレジット履歴、犯罪歴、自動車の運転記録、運転免許証の履歴、徴兵履歴 | 職務経歴、ID検証、学歴、クレジット履歴、犯罪歴、自動車の運転記録、運転免許証の履歴、徴兵履歴 | 経歴、ID検証、学歴、クレジット履歴、犯罪歴、自動車の運転記録、運転免許証の履歴、徴兵履歴 | 職務経歴、ID検証、学歴、クレジット履歴、犯罪歴、自動車の運転記録、運転免許証の履歴、徴兵履歴 | 職務経歴、ID検証、学歴、クレジット履歴、犯罪歴、自動車の運転記録、運転免許証の履歴、徴兵履歴 | 職務経歴、ID検証、学歴、クレジット履歴、犯罪歴、自動車の運転記録、運転免許証の履歴、徴兵履歴 |
| | 身体的適性 | 該当なし | オペレータは、担当職務の遂行能力を測定する身体検査に合格する必要がある。検査は、免許を持った医師が行う。 | オペレータは、担当職務の遂行能力を測定する身体検査に合格する必要がある。検査は、免許を持った医師が行う。 | なし | 該当なし | 該当なし | 該当なし |
| | 知的適性 | 該当なし | オペレータは、検査により、正しい判断、指示の実行、担当職務の理解、コミュニケーションなどの能力を有することを示す。 | 該当なし | なし | 該当なし | 該当なし | 該当なし |
| | 精神面の評価 | 該当なし | 検査により、信用、情緒不安定、信頼性に影響を与える精神的特性があるかどうかを評価する。 | 該当なし | なし | 該当なし | 該当なし | 該当なし |
| | 行動観察 | 該当なし | 弊害につながりかねない行動変化を検知する。アルコール依存症または薬物依存症の病歴がないこと。 | 該当なし | なし | 該当なし | 該当なし | 該当なし |
| | 自主的評価 | 該当なし | 職務執行のための認定に関する情報を報告する機会を要員に与える。 | 職務執行のための認定に関する情報を報告する機会を要員に与える。 | なし | 該当なし | 該当なし | 該当なし |

表A-1（続き）

| **概念** | **基準** | **ISA** | **NRC** | **DOE** | **EPA** | **NERC** | **API** | **CIDX** |
|---|---|---|---|---|---|---|---|---|
| 信頼 | 継続的な評価 | 該当なし | 信用、情緒的安定性、信頼を示す指標を継続的に監視する。 | 信用、情緒的安定性、信頼を示す指標を継続的に監視する。 | 信用、情緒的安定性、信頼を示す指標を継続的に監視する。 | 信用、情緒的安定性、信頼を示す指標を継続的に監視する。 | 信用、情緒的安定性、信頼を示す指標を継続的に監視する。 | 信用、情緒的安定性、信頼を示す指標を継続的に監視する。 |
| 能力 | 教育と経験 | 業種に関する経験 | 高校卒業資格、またはGEDまたは同等の試験、業種に関する経験 | 高校卒業資格、またはGEDまたは同等の試験、業種に関する経験 | 高校卒業資格、またはGEDまたは同等の試験、業種に関する経験 | 高校卒業資格、またはGEDまたは同等の試験、業種に関する経験 | 高校卒業資格、またはGEDまたは同等の試験、業種に関する経験 | 高校卒業資格、またはGEDまたは同等の試験、業種に関する経験 |
|  | 訓練 | 制御理論、アナログ及びデジタルエレクトロニクス、マクロプロセッサ及びコンピュータ、特定分野の計装の運用と保守、配管、電気の基本知識 | 各オペレータを対象に、組織の指定に基づいて訓練を実施する。 | 各オペレータを対象に、組織の指定に基づいて訓練を実施する。 | 各オペレータを対象に、組織の指定に基づいて訓練を実施する。 | 各オペレータを対象に、組織の指定に基づいて訓練を実施する。 | 各オペレータを対象に、組織の指定に基づいて訓練を実施する。 | 各オペレータを対象に、組織の指定に基づいて訓練を実施する。 |
|  | セキュリティ意識 | 該当なし | セキュリティの認識に関するセッション及び訓練を継続的に実施する。 | セキュリティの認識に関するセッション及び訓練を継続的に実施する。 | セキュリティの認識に関するセッション及び訓練を継続的に実施する。 | セキュリティの認識に関するセッション及び訓練を継続的に実施する。 | セキュリティの認識に関するセッション及び訓練を継続的に実施する。 | セキュリティの認識に関するセッション及び訓練を継続的に実施する。 |
|  | 継続的な訓練 | テクノロジの変化に対応することにより、最新技術を採用する。 | テクノロジの変化に対応することにより、最新技術を採用する。 | テクノロジの変化に対応することにより、最新技術を採用する。 | テクノロジの変化に対応することにより、最新技術を採用する。 | テクノロジの変化に対応することにより、最新技術を採用する。 | テクノロジの変化に対応することにより、最新技術を採用する。 | テクノロジの変化に対応することにより、最新技術を採用する。 |
|  | 認定試験 | 試験結果に基づいて認定を行う。 | 試験結果に基づいて認定を行う。 | 試験結果に基づいて認定を行う。 | 試験結果に基づいて認定を行う。 | 試験結果に基づいて認定を行う。 | 試験結果に基づいて認定を行う。 | 試験結果に基づいて認定を行う。 |
|  | 機器に関する訓練 | レベル、温度、圧力、流量、力、電力、位置、動き、物理的特性、化学組成を測定及び制御する機器を使用する。 | レベル、温度、圧力、流量、力、電力、位置、動き、物理的特性、化学組成を測定及び制御する機器を使用する。 | レベル、温度、圧力、流量、力、電力、位置、動き、物理的特性、化学組成を測定及び制御する機器を使用する。 | レベル、温度、圧力、流量、力、電力、位置、動き、物理的特性、化学組成を測定及び制御する機器を使用する。 | レベル、温度、圧力、流量、力、電力、位置、動き、物理的特性、化学組成を測定及び制御する機器を使用する。 | レベル、温度、圧力、流量、力、電力、位置、動き、物理的特性、化学組成を測定及び制御する機器を使用する。 | レベル、温度、圧力、流量、力、電力、位置、動き、物理的特性、化学組成を測定及び制御する機器を使用する。 |

表A-1（続き）

| 概念 | 基準 | ISA | NRC | DOE | EPA | NERC | API | CIDX |
|---|---|---|---|---|---|---|---|---|
| セキュアな環境 | 脆弱性とリスクの評価 | 該当なし | 制御システムは、健康、セキュリティ、破壊行為、インフラストラクチャの潜在的リスクを示す指標に基づいて分類する（複雑さ及び規模の評価を含む）。 | 制御システムは、健康、セキュリティ、破壊行為、インフラストラクチャの潜在的リスクを示す指標に基づいて分類する（複雑さ及び規模の評価を含む）。 | 制御システムは、健康、セキュリティ、破壊行為、インフラストラクチャの潜在的リスクを示す指標に基づいて分類する（複雑さ及び規模の評価を含む）。 | 制御システムは、健康、セキュリティ、破壊行為、インフラストラクチャの潜在的リスクを示す指標に基づいて分類する（複雑さ及び規模の評価を含む）。 | 制御システムは、健康、セキュリティ、破壊行為、インフラストラクチャの潜在的リスクを示す指標に基づいて分類する（複雑さ及び規模の評価を含む）。 | 制御システムは、健康、セキュリティ、破壊行為、インフラストラクチャの潜在的リスクを示す指標に基づいて分類する（複雑さ及び規模の評価を含む）。 |
|  | ヒエラルキ | 3つの認定レベル | オペレータは、制御システムの区分と同等以上の認定を取得する。 | オペレータは、制御システムの区分と同等以上の認定を取得する。 | オペレータは、制御システムの区分と同等以上の認定を取得する。 | オペレータは、制御システムの区分と同等以上の認定を取得する。 | オペレータは、制御システムの区分と同等以上の認定を取得する。 | オペレータは、制御システムの区分と同等以上の認定を取得する。 |
|  | 内部監査 | 該当なし | 2年に1回 | 2年に1回 | 3年に1回 | 2年に1回 | 実施を推奨 | 3年に1回 |
|  | 外部監査 | 該当なし | 該当なし | 該当なし | 5年に1回 | 実施を推奨 | 実施を推奨 | 実施を推奨 |
|  | 業者/ベンダの監査 | 該当なし | 12カ月に1回 | 12カ月に1回 | 実施を推奨 | 実施を推奨 | 実施を推奨 | 実施を推奨 |
|  | 規制執行 | オペレータ認定の一時停止や、オペレータの不正行為に応じた規則の執行などを行う権限。 | オペレータ認定の一時停止や、オペレータの不正行為に応じた規則の執行などを行う権限。 | オペレータ認定の一時停止や、オペレータの不正行為に応じた規則の執行などを行う権限。 | オペレータ認定の一時停止や、オペレータの不正行為に応じた規則の執行などを行う権限。 | オペレータ認定の一時停止や、オペレータの不正行為に応じた規則の執行などを行う権限。 | オペレータ認定の一時停止や、オペレータの不正行為に応じた規則の執行などを行う権限。 | オペレータ認定の一時停止や、オペレータの不正行為に応じた規則の執行などを行う権限。 |
|  | 緊急時対応計画 | 該当なし | 緊急時対応を効果的に実行するために必要となるスキルと経験をオペレータが持っていることを確認する。 | 緊急時対応を効果的に実行するために必要となるスキルと経験をオペレータが持っていることを確認する。 | 緊急時対応を効果的に実行するために必要となるスキルと経験をオペレータが持っていることを確認する。 | 緊急時対応を効果的に実行するために必要となるスキルと経験をオペレータが持っていることを確認する。 | 緊急時対応を効果的に実行するために必要となるスキルと経験をオペレータが持っていることを確認する。 | 緊急時対応を効果的に実行するために必要となるスキルと経験をオペレータが持っていることを確認する。 |
|  | 制御システムアクセス | 該当なし | サインインログ、写真付きIDバッジ、キーカードと番号パッド、TV監視システム、ファイアウォール、ウィルス保護、侵入検知システム（IDS） | サインインログ、写真付きIDバッジ、キーカードと番号パッド、TV監視システム、ファイアウォール、ウィルス保護、侵入検知システム（IDS） | サインインログ、写真付きIDバッジ、キーカードと番号パッド、TV監視システム、ファイアウォール、ウィルス保護、侵入検知システム（IDS） | サインインログ、写真付きIDバッジ、キーカードと番号パッド、TV監視システム、ファイアウォール、ウィルス保護、侵入検知システム（IDS） | サインインログ、写真付きIDバッジ、キーカードと番号パッド、TV監視システム、ファイアウォール、ウィルス保護、侵入検知システム（IDS） | サインインログ、写真付きIDバッジ、キーカードと番号パッド、TV監視システム、ファイアウォール、ウィルス保護、侵入検知システム（IDS） |
|  | コミュニケーション | 該当なし | 緊急時の該当機関との連絡と問合せ先情報を整備する。 | 緊急時の該当機関との連絡と問合せ先情報を整備する。 | 緊急時の該当機関との連絡と問合せ先情報を整備する。 | 緊急時の該当機関との連絡と問合せ先情報を整備する。 | 緊急時の該当機関との連絡と問合せ先情報を整備する。 | 緊急時の該当機関との連絡と問合せ先情報を整備する。 |

# 付録B

# 新しい記事

# 停電は防げた、調査で明らかに

**2003年の停電はテロリスト攻撃によるものではないと調査委員会が結論付ける**

2004年5月18日（火）東部夏時間午後11:21（0321グリニッジ標準時）

**（CNN）―米国の8つの州とカナダの1つの州を暗闇に陥れた昨夏の停電は、防げたはずであり、テロリストの攻撃やサイバー攻撃によるものではない。調査委員会は、月曜日に発表した最終報告でそう結論付けた。**

調査委員会の共同委員長を務める合衆国エネルギー庁長官、スペンサー・エイブラハムとカナダの天然資源省大臣、R・ジョン・エフォードは、勧告推進のために同委員会はさらに一年間活動を続けると述べた。

8月4日に始まった停電は、米国を襲った停電の中でも過去最大規模。影響は、オハイオ州、ミシガン州、ペンシルベニア州、ニューヨーク州、ニュージャージー州、バーモント州、マサチューセッツ州、コネチカット州、及びカナダのオンタリオ州の全部または大部分に及んだ。

ニューヨーク市を含むほとんどの地域では翌日の終わりまでに復旧したが、一部の地域では数日に渡って停電が続いた。

委員会は特に米国とカナダでの政府による監視と違反への罰則を含む信頼性確保規制義務化の必要性に重点を置いて検討を行った。

電力業界は現在、停電防止を目的とする自主的な要求事項を定めている。この要求事項は、民間団体である北米電力信頼度協議会（North American Electric Reliability Council）によって管理されているが、この団体には罰則権限はない。

委員会によると、停電時には多くの信頼性確保規則が無視されたという。

「報告書は、停電を防げたこと、また、我々の電力システムの信頼性向上のために米国、カナダの両国が直ちに行動しなければならないことを明確に示している」と両委員長は声明の中で述べている。

報告書によると、委員会が11月に中間報告書を発行した後、分科委員会のメンバーがテロリスト関与の可能性を引き続き検討していたという。

アルカーイダの犯行声明があったことは認めているものの同組織の関与を示す証拠はなかったと報告書は結論付けている。

中間報告書と同様に、8月14日の停電はオハイオ州アクロンに本拠を置くファーストエナジー社

（FirstEnergy Corp.）が大部分の責任を負い、同社のコミュニケーション不足、設備の不備、訓練の不足に原因があるとした。

委員会は、オハイオ州の3つの停電はファーストエナジー社のオペレータによって封じ込められるべきだったという。

封じ込められなかったために停電が波及し、最終的には5千万人に電気が届かなくなった。

「ファーストエナジー社のオペレータは［8月14日に］関係する情報を得ていた、しかし、それらの手がかりから、これから起きようとしている問題に気付かなかった。関係情報には、ファーストエナジー社の西部制御センターから断線の可能性に関する問合せの電話なども含まれていた」と報告書は述べている。

委員会によると、高電圧システムの障害はわずか７分でオハイオ州のクリーブランドとアクロン地区から米国北西部の大部分とカナダに波及したという。

ファーストエナジー社は停電の数日後、停電の1時間前に自社所有のうち3つ送電路、及び共同所有の1つの送電路が失われていたことを認めた。また、同社のコンピュータ警告システムも機能していなかったと話した。

委員会は、電力障害の一部は樹木が電線に触れていたことが原因だったと述べている。

委員会による勧告は以下の通り。

- 北米電力信頼度協議会の制度的枠組みを強化し、監視の対象となる企業からの独立性を確保するために資金調達の仕組みを作ること。
- ファーストエナジー社は6月30日までに不備に対処すること。
- オペレータ、信頼性コーディネータ、サポート要員に対する教育及び認証要件を改善すること。
- 送電網の物理的安全性とサイバーセキュリティを向上させること。

# 謝辞

本書は、DHSの指揮のもと、いくつかの組織が提供している人的セキュリティガイダンスの文書をレビューすることによって作成された。上記の文書には、DHSによる本書の作成作業を支援することを目的とした文書と、インターネット上で現在も入手可能な文書が含まれる。本書では、CIDXの「Preliminary Draft Guidance for Addressing Cyber security in the Chemical Sector, Version 2.0」及びAPIの「API Standard 1164, SCADA Security, First Edition」を資料として使用した。これらの資料は、各組織の会員をサポートする目的で作成され、重要なインフラストラクチャの保護対策においてリーダーシップを発揮する企業の例となっている。本書の作成作業では民間による資金提供を受け、本書に対する著作権保護は多くの引用が除外対象となる。ここに、本書の作成における支援と多大な貢献及び努力に対して感謝の意を表す。