2016 年 4 月 27 日
独立行政法人情報処理推進機構（IPA）

# “EU 加盟国における重要インフラの制御システムのサイバーセキュリティ確保に向けた取組みの成熟度” 概要

本概要は、欧州ネットワーク情報セキュリティ機関（ENISA）発行の“*Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors*”の概訳となります。内容の詳細につきましては、原文をご確認ください。
URL：
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/maturity-levels

監視制御システム（SCADA）を含む制御システム（以下、ICS）は、国の産業を支えるとともに、大規模な産業事故や環境汚染を防ぐのにも重要な役割を果たしている。その重要性ゆえに、悪意ある攻撃の標的象にもなっている。米国土安全保障省の ICS-CERT[1]によれば、ICS に対するサイバー攻撃は報告されているものだけで 2009 年から 2014 年の間に 27 倍以上増加している。

本報告書は、ENISA が実施した EU 加盟国における ICS のセキュリティ確保に向けた取組みの現状と実施されているグッドプラクティスの調査の結果、および今後の改善のための提言を記すものである。

調査は、EU 加盟国における ICS セキュリティに関する取組み、法規、戦略（政策）、推進体制等に関する文献調査（政府関連組織が発行した公的資料に限定）、および加盟国 8 ヶ国 [2]の関係者へのヒアリング調査により実施した。

成熟度は、「ICS-SCADA Cyber Security Maturity Model」を開発し、これに基づき評価を行った。その結果、国の取組みの成熟度として、成熟度の高い順に以下の 4 つのプロファイルを導出した。

- 取組先進国（Leaders）
- 能動的取組国（Proactive Supporters）
- 受動的取組国（Reactive Supporters）
- 取組新興国（Early Developers）

以降に、ICS-SCADA Cyber Security Maturity Model と導出された 4 つのプロファイル、加盟国の現状とグッドプラクティス、および今後に向けた提言の概要を示す。

[1] ICS-CERT: Industrial Control Systems Cyber Emergency Response Team
https://ics-cert.us-cert.gov/
[2] エストニア、フランス、ドイツ、リトアニア、オランダ、ポーランド、スペイン、スウェーデン

## ◆ ICS-SCADA Cyber Security Maturity Model

ICS-SCADA Cyber Security Maturity Model では、成熟度を測る指標として、3 つの大項目と、各大項目を更に 3 つに分けた 9 つの中項目を定義している。

原文 表 1: ICS-SCADA Cyber Security Maturity Model Dimensions

| 大項目 | 中項目 | 説明 |
|---|---|---|
| **法規（Legislation）** | 加盟国において、ICS のセキュリティに関する法規がどの程度整備されているか（官民の責任と役割の明確化、法規の立案、政策等） | |
| | EU 指令&加盟国の法規 | 加盟国および EU が、ICS のセキュリティを後押しするための政策をどのように検討しているか |
| | 標準の適用 | ICS のセキュリティ強化のため、国際標準や業界標準を活用しているか |
| | グッドプラクティスの導入 | 重要インフラ事業者が実施しているグッドプラクティスを把握し、これを共有するための仕組みを整備しているか |
| **支援策（Support）** | 加盟国において、重要インフラ事業者における ICS のセキュリティ強化が支援されているか（事業者のセキュリティ意識向上施策の実施、グッドプラクティスの収集と展開等） | |
| | インセンティブ | 重要インフラ事業者を支援し、事業者におけるセキュリティ対策を奨励しているか |
| | 教育・訓練 | 学術界を支援し、ICS セキュリティに関する知見の教授と発展を促進しているか |
| | インシデント対応組織 | ICS におけるインシデント対応を支援する専門組織があるか |
| **状況把握・改善（Local Conditions）** | 加盟国において、ICS のセキュリティ向上の余地（機会）や課題がどう特定され、取り組まれているか | |
| | 改善の仕組み | ICS セキュリティの改善をどう効率的に計画・実施しているか |
| | 教訓を生かす仕組み | 改善の取組みの結果を評価し、適切な是正施策を実施しているか |
| | 制約 | 改善の障害となっている制約事項にどの程度対処できているか |

調査では 9 つの中項目の実施状況を評価するための質問事項（82 項目）を策定し、質問ごとに加盟国における実施状況を以下の 5 段階で評価した。

- 実施していない（Basic）
- アドホックに実施している（Developing）
- 基本的な取組みが確立され、とりあえず実施している（Established）
- ICS に対する深い知識と理解を以って実施している（Advanced）
- 現状必要とされているレベル以上の取組みを実施している（現状への取組みはもちろん、将来的に予測される課題やニーズに対する検討を含めた取組みがなされている）（Leading）

## ◆ 4 つの Maturity Profiles

評価の結果、国の取組みの成熟度として、成熟度が高い順に以下の 4 つのプロファイルを導出した。

- 取組先進国（Leaders）
- 能動的取組国（Proactive Supporters）
- 受動的取組国（Reactive Supporters）
- 取組新興国（Early Developers）

各プロファイルについては、当該プロファイルの特性、SWOT 分析結果[3]、重点的に取組んでいる分野を可視化したレーダーチャート（図 1、図 2）で説明している。

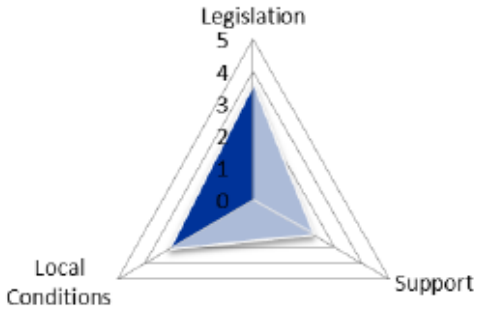


図 1：大項目を評価軸にしたレーダーチャート

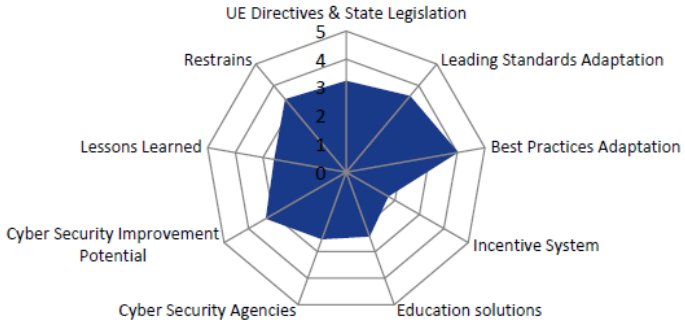


図 2：中項目を評価軸にしたレーダーチャート

以下に、各プロファイルの概要を示す。

※本概要では、各プロファイルの特性および SWOT 分析結果について紹介しています。レーダーチャートとその分析については、原文をご確認ください。

● Profile 1： 取組先進国（Leaders）

取組先進国（Leaders）は、ICS セキュリティに関して確たるアプローチを持っており、それを実行するための法規が整備されている。重要インフラ事業者にはインシデントを報告することが義務付けられ、一定のセキュリティ基準への準拠を確実に行わせるためのインセンティブが提供されている。政府と重要インフラ事業者のセキュリティ意識は高く、官民の連携もできている。対策の研究開発には大学や研究機関も関与し、国際標準等を活用した独自のガイドライン作り等も行われている。対策実施状況は監査等を通じてモニタリングされているほか、“security by design”の考え方に則り ICS のセキュリティが設計段階から考慮され確保されるよう、ICS のセキュリティ認証制度の導入を予定している。

[3] SWOT 分析は、ある取組主体における目標達成のための戦略立案を支援する分析手法。自組織を取り巻く内部環境および外部環境を「強み（Strengths）」「弱み（Weaknesses）「機会（Opportunities）」「脅威（Tthreats）」の 4 つの観点から分析する。

表 2: 取組先進国(Leaders)の SWOT 分析

| | 強み(Strengths) | 弱み(Weaknesses) |
|---|---|---|
| 内部環境 | • ICS セキュリティの改善に関する長期的計画を有する<br>• 重要インフラ防護における ICS の役割をよく理解している<br>• 重要インフラ事業者と政府の協力関係が確立されている<br>• “security by design”を促進する ICS のセキュリティ認証制度の導入を予定している | • ICS セキュリティの改善を促進するインセンティブが欠如している<br>• ICS セキュリティに関する研究開発がまだ殆どない |
| | 機会(Opportunities) | 脅威(Threats) |
| 外部環境 | • EU 加盟国の間で ICS セキュリティのグッドプラクティスが共有されている(取組新興国は取組先進国の経験から学べる可能性がある) | • ICS セキュリティの専門家が不足している(多くの場合、ICS セキュリティの問題に IT セキュリティの専門家が対応している) |

- Profile 2: 能動的取組国(Proactive Supporters)

能動的取組国(Proactive Supporters)は、ICS セキュリティの継続的向上に必要なツールを重要インフラ事業者に提供することに注力しており、政府による強力な支援と官民パートナーシップを特徴としている。対策技術の開発は内部関係者(政府、重要インフラ事業者)と外部関係者(大学、民間企業)との密接な協力のもとで行われ、そのための情報共有プラットフォームやワーキンググループが整備されている。重要インフラ事業者を支援し、セキュリティ対策を奨励するためのインセンティブが提供されているほか、必要な情報やトレーニングを提供することで ICS セキュリティに関する意識および理解の向上に尽力している。

表 3: 能動的取組国(Proactive Supporters)の SWOT 分析

| | 強み(Strengths) | 弱み(Weaknesses) |
|---|---|---|
| 内部環境 | • 密接な官民パートナーシップが確立されている<br>• 大学・研究機関も関与している<br>• 多くの教育対策を開発している<br>• ICS セキュリティイニシアチブに対して構造的な資金援助を得ることができる | • 極めて基本的な法規しか整備されていない<br>• セキュリティ改善のための仕組みが体系的でない |
| | 機会(Opportunities) | 脅威(Threats) |
| 外部環境 | • 重要インフラと政府の関係が良好なため、民間で開発されたグッドプラクティスを収集・展開するのが容易である | • 緩い法規や杜撰な計画により、将来「間違っている」または「有効でない」と判明する可能性が高い施策を実施しかねない |

- Profile 3：受動的取組国（Reactive Supporters）

受動的取組国（Reactive Supporters）は、問題が発生したら対応していくアプローチを取っており、主に発見された脆弱性への対処、および発生したインシデントへの対応に注力している。ワーキンググループは業界ごとの縦割りで組織され、グッドプラクティスや教訓を収集している。ICS セキュリティの改善に関する取組みは多くの場合非公式で、IT セキュリティと一緒にされているケースが多い。

表 4：受動的取組国（Reactive Supporters）の SWOT 分析

| | 強み（Strengths） | 弱み（Weaknesses） |
|---|---|---|
| 内部環境 | • 密接な官民パートナーシップが確立されている<br>• 厳しい監査およびインシデント報告に関する法規が整備されている | • 能動的でなく、受動的なアプローチを取っている<br>• ICS を従来の IT のように扱っている<br>• アドホックなイニシアチブ（杜撰な計画）となっている<br>• ICS セキュリティに対する義務やガイダンスが存在しない |
| | 機会（Opportunities） | 脅威（Threats） |
| 外部環境 | • ICS が直面している既存の脅威をよく理解しており、他の加盟国に広めることができる | • 緩い法規や杜撰な計画により、将来「間違っている」または「有効でない」と判明する可能性が高い施策を実施しかねない |

- Profile 4：取組新興国（Early Developers）

取組新興国（Early Developers）は、重要インフラの定義や、ICS に関するサイバーセキュリティ上の課題の検討が始まったのがここ 2、3 年のことで、重要資産（critical assets）のリストを作成したばかりか、未だそうしたものが無く、ICS セキュリティガイドラインも作られていない。官民パートナーシップや学術界の関与は非常に初期的な段階で、ICS のサイバーセキュリティに関する知識もあまりなく、グッドプラクティスや標準のことも殆ど知らない。

表 5：取組新興国（Reactive Supporters）の SWOT 分析

| | 強み（Strengths） | 弱み（Weaknesses） |
|---|---|---|
| 内部環境 | • 重要インフラ防護に関するごく基本的な法規（土台）は多くの場合存在している<br>• 長期的計画を有する（但し、取組先進国に比べれば非常に初期段階のもの） | • 官民パートナーシップについて、殆どまたは全く存在しない<br>• ICS を従来の IT のように扱っている<br>• 重要資産をどう守るべきか、ガイドラインが存在しない<br>• ICS セキュリティに関する専門知識（あるいは経験）が不足している |
| | 機会（Opportunities） | 脅威（Threats） |
| 外部環境 | • 他の成熟度の高い加盟国から、経験等を学べる可能性がある<br>• 他の国の ICS セキュリティに関する資料やプログラムなどを活用することができる | • ステークホルダ間の不審（信頼感の低さ）が ICS のセキュリティ改善への大きな障害となる可能性がある |

## ◆ 加盟国の取組事例とグッドプラクティス

以下の 12 のテーマについて、加盟国における取組事例やグッドプラクティスを紹介している。

- 組織・体制
- 法規・政策
- 資産
- 監査・認証
- インシデント対応
- インセンティブ
- セキュリティ意識向上
- トレーニングの提供
- 研究開発
- 情報共有
- 官民パートナーシップ
- 目標・課題

**組織・体制**および**法規・政策**では、2008 年の EU 指令「Council Directive 2008/114/EC」により、加盟国は重要インフラ業界（事業者）の特定、セキュリティ対策状況の確認および改善の検討、体制（役割分担や責任）の整備等に取り組むことが義務付けられ、各国の重要インフラ防護（CIP）の取組みの基盤となっている。関連法規は「インシデント発生時のへの報告」、「一定のセキュリティ基準への準拠」、「CIP 計画の策定」を義務付けるものが主だが、各国によってレベルやアプローチは様々となっている。

**情報共有**では、多くの加盟国では業界ごとにワーキンググループを設置して事業者同士および国との情報共有を図っているが、事業者と国の信頼関係の構築が課題となっている。

**監査・認証**では、多くの加盟国が将来的な導入を検討している。現時点では、ドイツが事業者（システム）に対して一定のセキュリティ基準への準拠と 2 年ごとの監査を行う制度の整備を進めているほか、フランスが、ICS 機器およびサービスが一定のセキュリティレベルを満たしていることを示すセキュリティ認証制度の整備を進めており、成功すれば他国にも広がる可能性がある。

**インシデント対応**では、現状、対応能力が IT インシデントへの対応に限られているという課題がある。スペインでは内務省下の National Centre for Critical Infrastructure Protection（CNPIC）と産業・エネルギー・観光省下の National Institute of Cybersecurity（INCIBE）が協力して重要インフラのインシデント対応を専門とする対応チームを立ち上げ、重要インフラ事業者でインシデントが発生した際に事業者が対応サービスを利用できる取組みを始めている。

**インセンティブ**では、多くの加盟国は「サイバーセキュリティ対策の実施は重要インフラ事業者の責任であり、国がインセンティブを与えるべきものではない」と考えている。一方で、事業者はインセンティブを期待しており、主なものとして、「サイバーセキュリティ対策に対する助成金の支給」、「税控除」、「保険料の減額」が挙げられた。なお、唯一エストニアは助成金制度を設けている。

**セキュリティ意識向上**では、多くの加盟国が ICS セキュリティに関するガイドライン等を発行している。中には母国語だけでなく英語でも提供され、他国での活用を可能にしているものもある（付録 A に英語版が存在する有用な資料の例示あり）。

**トレーニング**および**研究開発**は、殆ど取組みがないが、スペインで INCIBE がオンライントレーニングコースを提供しているほか、同じくスペインのレオン大学で ICS セキュリティの研究開発を中心とした修士課程の

開設や、ICS テストベッドの整備が検討されている。

**目標・課題**では、成熟度の低い国はセキュリティ意識の向上および情報共有の促進を挙げ、高い国は ICS 製品のセキュリティ品質向上を挙げる傾向が見られた。課題としては、ICS 資産および相互依存性が特定できていないことや、情報共有意欲の低さ、人材（ICS セキュリティ専門家）の不足などが挙げられた。

## ◆ 提言

以下に、加盟国における ICS セキュリティ強化のための 6 つの提言をまとめる。

- 提言 1：ICS セキュリティ取組みと国のサイバーセキュリティ戦略／CIIP 施策との同調
  現状の ICS セキュリティ施策は、従来のサイバーセキュリティ戦略や CIIP 施策と必ずしも同期していない。政策策定者は、ICS セキュリティを国の関連戦略に含め、統合性を持たせることが重要となる。
- 提言 2：ICS に特化したサイバーセキュリティ基準の策定
  既存の ICS 向けのサイバーセキュリティ基準、業界ガイドライン、グッドプラクティスガイド等を活用し、当該国が必要とするレベルの ICS サイバーセキュリティ基準を策定する。
- 提言 3：情報共有ルールの業界横断、EU レベルでの標準化
  事業者の不審感の払拭および情報共有意欲向上のため、インシデントの報告方法や情報共有ルールを整備・標準化し、関係者のコミュニケーション改善を支援する。
- 提言 4：ICS セキュリティ意識の向上
  事業者だけでなく、政策決定者の意識向上を図る。深刻なインシデント等の発生に付随する事後的・単発的な向上でなく、継続的な意識向上を狙う取組みを行う。
- 提言 5：ICS セキュリティに関する教育・トレーニングの促進
  ICS に対する高度かつ執拗なサイバー攻撃を防ぐには、ICS およびセキュリティに対する深い理解が不可欠となる。政府、事業者、ベンダが協力し、トレーニングプログラム等の立ち上げにより人材育成を促進することが必要となる。
- 提言 6：ICS セキュリティに関する研究開発およびテストベッドの促進
  政府および ICS ベンダは、将来的な脅威も見据え、研究開発を促進・支援することが必要となる。また、テストベッドを通じた“security-by-design”の改善やイノベーションを後押しする。

以上