2013 年 12 月 25 日

独立行政法人情報処理推進機構（IPA）

【CERT 向け】制御システムのインシデント対応のためのベストプラクティスガイド
～産業制御システムの緊急事態対応機能の整備にあたっての考慮事項～

本概要は、欧州ネット・情報セキュリティ機関（ENISA：European Network Information Security Agency）が発行する、“Good practice guide for CERTs in the area of Industrial Control Systems - Computer Emergency Response Capabilities considerations for ICS -”の、主にExecutive SummaryとConclusionの概訳となります。

内容の詳細につきましては、原文をご参照ください。

URL：

http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/ics-cerc/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems

産業制御システム（ICS）は、エネルギー供給、水処理、輸送、防衛、食品加工などを含む産業プロセスにとって必要不可欠なものである。現代の ICS は過去のような隔離されたシステムでなく、インターネットに接続される傾向にある。これに伴い、サイバー脅威によるリスクも増大している。ICS は犯罪者やテロリスト、国家の情報機関にとっても大きな利益を生む標的であり、ICS のインシデントに迅速に対応し、影響を留める能力は、国家、欧州、また世界が重要インフラのサイバーセキュリティを強化し、守る上での鍵となる。

本ガイドは、ICS に緊急事態対応機能（ICS Computer Emergency Response Capabilities：ICS-CERC）を提供する役割を担う組織に、グッドプラクティスを提供することを目的としている。本ガイドの内容は、実際に ICS をサポート範囲としている CERT の現行のプラクティス、および以前に ENISA が国家／政府 CERT に必要な基本機能について調査を行った際の調査結果に基づいている。本ガイドでは ICS-CERC の基本となる機能として、以下の 4 つの機能を説明している。

- 基本機能＜Mandate Capabilities＞ ・・・ 原文 2.1 節
  ICS-CERC を確立するためのプロセスおよび手順、通常の IT システム向け CERT との相違、およびこれに伴い考慮すべき事項、また、確立したい ICS-CERC のレベル（特定の重要インフラ業界、国家、地域、グローバル）の位置付けと利点・欠点などを説明。

- 運用機能（技術面）＜Operational Capabilities（Technical）＞ ・・・ 原文 2.2 節
  提供するべき ICS-CERC サービス（特にインシデント対応）、およびそれらのサービスに関する考慮事項などについて説明。立ち上げた ICS-CERC をどう維持・改善していくかについても簡単に触れている。

- 運用機能（組織面）＜Operational Capabilities（Organizational）＞ ・・・ 原文 2.3 節
  ICS-CERC サービスの提供に伴う、スタッフのスキル要件、採用にあたっての考慮事項など、組織

面に関する事項について説明。特に、スタッフの教育・訓練の重要性を強調しているほか、ICS-CERC サービスの提供に適した母体組織の条件（具体的には、国の重要情報インフラ防護（CIIP）政策の実行にあたって、重要な位置付けにある組織が望ましい）、といった話題も取り上げている。

- 連携機能＜Co-Operational Capabilities＞ ・・・ 原文 2.4 節
  ICS-CERC サービスを提供する他の CERT や、ICS 関係者との連携およびその重要性について説明。具体例として、ICS ベンダ、国内 CERT 等との国内連携、および ICS セキュリティに関わる国際的な取組み（International Council on Large Electric Systems（CIGRE）、European Network for Security of Control and Real Time Systems（ESCoRTS）等）との国際連携について取り上げている。

結論

ICS-CERC サービスの確立および提供には制御システム特有の課題が壁として存在するが、これまでに欧州や世界で培われてきたグッドプラクティスや教訓を活用すれば、取組みはずっと容易になると考えられる。

- IT と ICS における相違の認識と適応
  ICS-CERC サービスを提供する者として忘れてはならないのは、通常の IT システムでは機密性が最重要視されるが、ICS では可用性が最重要視されることである。これは、ICS が重要インフラの運用に必要不可欠な要素であり、ICS の障害が、長時間の停電や交通機関の停止、生態系への壊滅的損壊など、経済や人命に影響を及ぼす可能性があることに起因する。こうした危機的状況に立ち向かい、対処するには、巧く機能している既存の IT システム向け CERT を ICS に適応させ、適切に機能させることが重要となる。

- 重要インフラ政策における必要事項の明確化
  重要インフラの防護は国益に関わる問題であり、多くの国の CIIP に関する国家戦略や法規などに組み込まれているが、その中で基本的な事項、特にサイバーインシデント発生時の対応等は明確にされているべきである。

- 信頼の確立と透明性の確保
  iCS-CERC チームがぶつかる最初の課題は、インシデントに関する情報収集である可能性が高い。重要インフラ事業者やベンダ、ネットワークサービスプロバイダは、インシデントの報告を法的に義務付けられている訳ではなく、情報の共有に積極的でないことが多い。従って、ICS-CERC チームは、自分たちが信頼できること、および業務プロセス・手順の透明性を示し、データや情報の扱いに関して関係者から全福の信頼を得ることが肝要となる。

- スタッフの採用
  ICS-CERC チームのスタッフの採用には、適切な検討が必要となる。採用にあたっては、重要イン

フラに甚大な損害をもたらしかねない問題や機微な情報を取り扱うことを踏まえ、徹底的な身元調査を行うほか、重圧下でも業務が遂行でき、連絡があればすぐに動くことができ、それが時間外でも厭わないといった「やる気」が要求される。

- 関連組織との協力・連携

  ICS-CERC チームは、CIIP 戦略担当機関、警察、情報機関、行政（連邦、地域、ローカルレベル）とパートナーを組んでインシデント対応を纏め、重要インフラ事業者、運用者、ベンダ等と定期的な会合を持ち、脅威や対策その他について、グッドプラクティスを幅広く共有する事が必要となる。

以上