2014 年 3 月 13 日

独立行政法人情報処理推進機構（IPA）

制御システムのセキュリティ評価に関する EU レベルでの連携体制の確立

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 Practices for an EU ICS Testing Coordination Capability*” 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/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/good-practices-for-an-eu-ics-testing-coordination-capability/good-practices-for-an-eu-ics-testing-coordination-capability

産業制御システム（ICS）に汎用的な情報技術（IT）が活用されるようになり、これに伴うセキュリティ上の懸念が指摘されるようになってそれなりの時間が経つ。ICS 業界では、標準化団体や官民イニシアチブなどによって策定された標準やガイドラインに基づき、セキュリティ対策への取組みを進めている。しかし、開発プロセスにおけるセキュリティ意識の不足、迅速かつ客観的なテスト・評価の必要性など、改善の余地がある。これらの課題は、制御システム、コンポーネント、プロセスを一定のセキュリティ要件に基づき評価するテストベッドや認証制度の確立によって対処することができる。同様のテストベッドや認証制度の検討は、ENISA の 2011 年のレポート“*Protecting Industrial Control Systems: Recommendations for Europe and Member States*”でも、推奨施策の 1 つとして提言された。

本レポートの目的は、欧州および諸外国における ICS のセキュリティ評価に関する取組みの現状調査、およびその結果に基づき、欧州のニーズに合った「EU レベルでの制御システムのセキュリティ評価のための連携体制（EU ICS Testing Coordination Capability）（以下、連携体制）」の検討にあたっての提言を行うことにある。

現状調査については、文献等による机上調査、ICS セキュリティの専門家へのアンケートおよびインタビューを通じて得た調査結果を、検討にあたっての 6 つの重要なポイントに分けて纏めている。また、提言については 7 つの提案を行い、各提案の実現に向けたステップ、達成状況を測るためのメトリクス、主導的役割を果たすべき組織などを纏めている。

◆ICS のセキュリティ評価に関する取組みの現状

以下に、欧州以外を含む諸外国における ICS のセキュリティ評価に関する取組みの現状について、調査結果を 6 つのポイントに分けて纏める。

1. ICS のセキュリティ評価の現状
   - 欧州における ICS のセキュリティ評価は、各国バラバラで調和性がない
   - 欧州には、ICS セキュリティに関する教育・訓練を受けられる環境がない
   - 欧州における ICS のセキュリティ評価手法はまだ成熟しておらず、“欧州の取組み”として欧州

を主導できるような包括的な欧州レベルのイニシアチブはない
- 評価機関や事業者による、認証制度への関心は高い
- ICS セキュリティの現状を変えるには、ユーザである事業者による ICS ベンダへのプレッシャー（セキュリティの要求）が鍵となる

2. 連携体制づくりにおける考慮事項
- 独立した評価、テスト、認証が必要
- 政策等による後押しが必要な可能性あり（米国の NSTB/INL[1]は 9.11 同時多発テロ後に、また、日本の CSSC[2]は東日本大震災後に加速）
- 新しい標準を作るのでなく、ISA/IEC-62443 など既存の標準を活用するのが妥当
- 成功させるには、利害関係者全員にとって何らかの利があるものにすることが必要
- ICS への侵入は繋がっているシステムのどこからでも起こり得るため、評価を一部の最重要機器に限定するのではなく、体系的・包括的なアプローチが必要（テスト環境でのテストより、ペネトレーションテスト等の方が効果的か。但し、評価者の技量に依存しがちなため、評価が一貫性を欠く可能性もあり）
- セキュリティ評価を義務付けることの是非
- ベンダに対し、発見された脆弱性を修正させる仕組みの検討

3. 認証制度のモデルおよび方法論
- テストセンター（testing facilities）と認証制度のどちらか片方でなく、両方の確立が必要[3]。
  なお、認証制度に最も期待を寄せているのは事業者（機器の導入時に自社でテストを行っており、自社のやり方が一定の標準に準拠していることを示せるようになるため）
- NERC CIP 基準[4]や CC[5]を引き合いに、“標準”への準拠と認定が本当にセキュリティ向上に役立つか、根強い議論あり
- 何を認定すべきか（機器、開発プロセス、セキュリティ機能、システムアーキテクチャ全体、テストベッド等）の検討要
- 認証制度の確立と運用にあたって各利害関係者に求められる役割には、利害関係者の合意と公的機関による主導が必要
- 「評価結果の受容度」と「評価テストの包括性」は、成功度を測る最大の物差しとなる
- EU の複雑性を考慮すると、認定機関（Accreditation Organization）を頂点とする分散型モデル(Distributed Model)が望ましい
- テストセンターごとに業務をセグメント化する（「業界」でセグメント化することが妥当か）

---

[1] NSTB/INL: National SCADA Test Bed at Idaho National Laboratory
[2] CSSC: 技術研究組合制御システムセキュリティセンター（Control System Security Center）
[3] IPA 補足: 2011 年度のレポートの推奨施策では、テストベッドまたは認証制度のどちらかの立ち上げが提唱されていた
[4] NERC CIP: North American Electric Reliability Council Critical Infrastructure Protection
[5] CC: Common Criteria

4. 利用可能なリソース
   - 最も受け入れられている運用（財務）モデルは「官民パートナーシップ」型
   - 諸外国のケースでは、政府による初期投資が必要であった（その後民間投資に移行、または移行を意図）
   - 諸外国の成功例を見ても、成功要因は 1 つではなく複数の要因が作用（リソースの可用性、政策による後押し、利害関係者間における信頼関係の確立などがしばしば挙げられる）
   - 信頼関係を維持するためにも、ベンダの機器・サービスの機能やセキュリティ機能等を比較したり、公開したりしない方がよい
   - 情報技術（IT）／制御・運用技術（OT）を始め、多岐な分野にわたる専門家によるチームが必要
   - 連携体制（の運用組織）において関係業界の専門家を中長期に雇用し、専門知識・経験の共有やテスト手法等を習得することが必要（専門家の派遣元組織、連携体制どちらにとっても有益）

5. 主な制約、リスク、脅威等
   - 利害関係者と連携体制の信頼関係の構築が、最大の組織的課題
   - 信頼を勝ち取る鍵は、テストベッドの独立性（連携体制は、幅広い組織を内包しつつ、組織の規模に関係なく全利害関係者が平等で、非ベンダ依存であるべき）
   - ICS の運用環境に特有の技術的多様性は、テストに「包括性」および「迅速さ」が求められるという点で最大の課題
   - 伝統的に、ICS 業界で使われているガイドラインはより一般的で、明確な指示を示すものではない。テストを行うにはテスト要件が必要となるが、合意を取るのはほぼ不可能に近い（但し、完全な合意なしにスタートした標準の中にも、効果的と見られている標準もあり、叩き台として活用するのはあり）
   - 何を重要インフラと見なすかを含め、重要インフラには各 EU 加盟国で様々な法規が存在しており、EU 統一的な標準等を適用する上で大きな課題の 1 つ
   - 官民パートナーシップを運用する上で、適切なビジネスモデルが必要

6. 他の利害関係者との連携
   - 連携体制（の運用組織の）理事会には個々の企業を入れず、業界団体等に限る。また、信頼関係の確立のため、理事会のメンバは可能な限り固定する
   - 欧州および国際的な CERT[6]との連携が必要
   - 脆弱性の公開および取扱いに関する議論の実施
   - テストセンターに、発見した脆弱性の解消をベンダに促すことができる何らかの力を与える
   - 普及啓発活動に利害関係者を巻き込むと良い
   - テスト環境の教育目的での使用も促進する

◆連携体制の検討・導入に関する提言

以下に、連携体制を確立するにあたっての提言を纏める。（※本概訳では、提言の概要のみを纏めて

[6] CERT: コンピュータ緊急対応チーム（Computer Emergency Response Team）

います。実施のステップ等については、原文を参照ください）

【提言 1】 運用（財務）モデルは官民パートナーシップとするが、行政（EU）がコーディネーターとして、取組みのビジョンや戦略の策定など、主導的役割を果たす

調査の結果から、初期投資を含め、取組みを推進するには行政の積極的関与が必要であるほか、以下のような理由からも、公的機関が主導的役割を果たすことによるメリットが考えられる。

- 公的機関は市場競争の原理から外れているため、信頼の構築にあたって民間企業より前向きである可能性が高い
- 連携にあたり、公的機関同士の横のつながりが活用できる（プレッシャーも掛けやすい）
- 中立的な立場で、国や組織を問わず、窓口（POC）の役割を果たすことが可能

【提言 2】 信頼でき、機能する理事会の設置

先ずは、将来的に理事会となるワーキンググループ（WG）を設置する。WG には全ての重要関連組織の代表者と、技術、ビジネス、法律など ICS に係わるあらゆる分野の専門家を集め、EU の公的機関が主導する。個々の企業は WG（理事会）のメンバとせず、業界団体やコンソーシアムの代表をメンバとすることが奨励される。WG（理事会）では、連携体制の目標やビジョン、戦略を定め、認証制度やテストセンターの設立の是非について検討する。また、利害関係者の信頼を得るため、高い独立性を保つほか、情報共有は合意したルールに基づき注意を払って行う必要がある。

【提言 3】 特定の活動を行うワーキンググループの設置

個々の活動を実際に行う WG を設置する。例えば以下のような WG が考えられる。

- 技術委員会： 技術的課題について検討する。ERNCIP[7]、EuroSCSIE[8]、SCADALab 等と連携
- コミュニケーション部門： レポートの公開等、活動内容を普及する
- 財務顧問委員会： 運用（財務）モデル検討の際にアドホックに設置し、理事会を支援する
- 法制顧問委員会： 各国の ICS を取り巻く複雑な法規上の問題に関し、活動を支援する

【提言 4】 EU の状況に応じた運用（財務）モデルの検討

連携体制の確立には資金が掛かる。認証制度のビジネスへの活用を期待する大手ベンダや事業者などが纏まった資金を提供することも考えられるが、民間企業が成否の不明な初期段階で大金を投資するかは疑わしい。諸外国の事例でも、国土安全保障や経済産業を担う省庁が初期費用を出資しているケースが多い。EU であれば参加加盟国で予算を組むといった方法や、企業は機器の提供や専門家の派遣といった形で協力する、会費制にするなども考えられ、EU に合った運用（財務）モデルを検討する。

[7] ERNCIP: European Reference Network for Critical Infrastructure Protection
[8] EuroSCSIE: European SCADA Control Systems Information Exchange

【提言 5】 分散型モデルの実現可能性の調査（フィージビリティスタディ）の実施

欧州は、EU と加盟国、欧州レベル・各国レベルでの政策、法規、企業、標準、様々なイニシアチブ等が、非常に複雑な状況を形作っている。しかし、欧州という規模とこの多様性を活用し、EU の公的機関が各国のテストセンターを認定し、ISC セキュリティ評価に関する専門知識のネットワークを構築することもできる。法規上の問題など共通の問題を共有・解決できるほか、テストセンターごとに専門分野を持つことも可能になり、ICS の運用環境に特有の技術的多様性にも対応できるようになると考えられる。但し、各テストセンターの評価の質を維持する方法の検討も必要となる。

【提言 6】 他の ICS セキュリティ関連組織との連携の確立

連携体制を通じて、EU における既存の ICS セキュリティ評価関連組織を特定・調整し、EU 外部の ICS セキュリティ評価関連組織に対する POC としての役割を果たす。連携は、セキュリティ評価に関わる組織だけでなく、ICS セキュリティに関係する様々な組織とも協力し、ノウハウを共有することが望ましい。また、警察組織との連携や、EU 版 ICS-CERT（仮）がテストセンターで発見された脆弱性情報を取り纏めるといった連携も考えられる。

【提言 7】 ICS のセキュリティ評価に関するナレッジマネジメントプログラムの立ち上げ

ICS セキュリティに関わる技術者は、ICS 一筋でやってきた技術者か、IT セキュリティから ICS に分野を広げた技術者のどちらかであり、しばしば相互理解に至れない状況が発生している。とは言え、連携体制には両者とも必要である。更に言えば、ICS の中でも原子力、水道、鉄道など、様々な異なる分野の専門知識が必要であり、知識や経験、ノウハウを交換するための仕組みが必要となる。公共・民間の多様な分野から、人財が短期～長期、あるいはプロジェクト単位で連携体制（の運用組織）に派遣され、連携体制の一員として従事することで、知識を集約していくことができるようになる。

◆終わりに

多くの課題は今後も引き続き議論の的になると思われるが、攻撃者が ICS に関する高度な知識を持ち始め、日々リスクが高まっていく中、全ての ICS 関係者が協力して ICS セキュリティの向上に取り組むことの必要性は明らかである。先ずは、連携体制の目標、ミッション、ビジョンを決めるにあたっての戦略が必要となる。目標は、明確で、持続性があり、かつ将来的な要件にも適応できるよう柔軟性がなければならない。また、連携体制の最大の課題は利害関係者の信頼を得られるかであり、全利害関係者それぞれに利をもたらしつつ、独立性を保てるかが鍵となる。

ENISA は、この調査を受けて立ち上がるイニシアチブに官民全ての関係者が参加することを強く要望すると共に、連携体制の実現に向けてイニシアチブを主導していく所存である。

以上