国立研究開発法人 産業技術総合研究所
サイバーフィジカルセキュリティ研究センター
2020 年 1 月

(SIP)/重要インフラ等におけるサイバーセキュリティの確保
（b1）研究開発技術の社会実装を促す適合性確認のあり方の研究開発
成果報告（概要版）

1. 背景・目的

近年、世界中で重要インフラを対象としたサイバーセキュリティ脅威が増加の一途を辿っている。マルウェア感染によって、ウクライナでは停電、米国では鉄道運行停止、サウジアラビアでは石油精製所が 1 週間以上停止し PC データの全削除に追い込まれている。日本国内でも、大事故にはつながっていないものの、重要インフラ組織の 35%がランサムウェア被害を経験しているとの報告がある。また、サイバー攻撃によって、米国で都市の一部が停電した事例がある。機器等の脆弱性を突いたサイバー攻撃は益々増加すると予想され、2019 年 1 月開催の世界経済フォーラムでも、サイバー攻撃による重要インフラの機能停止は、自然災害や気候変動に並び、現代世界にとっての大きなリスクのひとつだと警告している。

日々進化・高度化する脅威に対抗するには、ライフサイクル全体にわたっての強化、すなわち、企画・設計・製造時のセキュリティの作りこみと運用時に不審な挙動をいち早く検知する能力の強化が求められる。サイバーセキュリティ戦略（2015 年 9 月閣議決定）でも、セキュリティ バイ デザイン（security by design）の考えが不可欠と指摘している。社会システムにセキュリティを広く実装するには、更に、実効性のあるサイバーセキュリティ対策を基準・制度化し、それらへの適合性を確認する仕組み作りが必要である。

本研究では、国内外の政府機関、セキュリティ関連団体、企業等へのヒアリング・調査に基づき、我が国を取り巻く状況を考慮した上で、従来になく有効でかつ速やかに社会実装が可能なセキュリティ適合性確認の仕組みと社会実装のあり方を検討した。適合性確認を容易にすることによって、SIP の各開発技術の国際競争力強化に間接的に寄与することを目的にした。

2. 実施成果概要

実施内容は、サイバーセキュリティの重要インフラ等への実装における有効かつ速やかな適合性確認の仕組みの調査、評価（以下の①から④）及びそれを支える各種ツールの研究（⑤と⑥）である。

①「SIP/重要インフラ等におけるサイバーセキュリティの確保」の技術に関する動向実態調査

国内外の制度・基準、それらに関わる組織の動向、更に業界や社会の動向を調査した。

欧米の制度・基準を調査した結果、欧米ではセキュリティのマネジメントフレームワークと脅威分析技術の開発が進んでおり、日本はそのキャッチアップが急務である。日本での制度・基準の設計にあたり、次の 3 点が重要である。

第一に、日米欧の基準の対応関係を明確化し、相互運用性を向上することが重要である。サイバーセキュリティは本質的にボーダレスであり、今後の国際商取引のさらなる活発化に鑑みると、欧米基準とのギャップを低減し、欧米の各基準へもスムーズに適合できる基準と仕組みづくりをすることが重要である。第二に、公的強制と自主規制の最適なバランスが重要である。日米欧とも、基準と適合性確認の仕組みは、法律に基づく強制基準、業界の自主規制基準、事業者毎の

内部基準の3階層で構成されており、政府、業界、事業者の三者が連携し、役割分担をして、推進されている。2019 年 6 月に施行された EU のサイバーセキュリティ法では、認証フレームワークに 3 段階の認証を設けている。第三者評価と自主評価による認証を使い分けているのは、このようなバランスを考慮した結果であろう。 第三に、セキュリティとセーフティの相互影響を考慮した、セキュリティ規格とセーフティ規格の関連付けが重要である。従来、両者は別々に検討されてきたが、サイバーフィジカル時代には、セキュリティ単独ではなく、セキュリティとセーフティ両方の規格を考慮した、製造や適合性確認が必要となる。
サイバーセキュリティの脅威は、多様化・高度化し、攻撃対象が拡大している。攻撃対象は、IT システムだけでなく、IoT や制御システムなどあらゆるものが攻撃対象になり、実際に世界中で数多くの攻撃が行われている。車、ATM、送電システム等についても、脆弱性や具体的な攻撃法が提示されている。また、セキュリティを製品に作り込むことも重要ではあるが、新たな脅威に対して完全に予防するのは限界があるので、早期発見・対処がトレンドになっている。

②適合性確認に用いられる主要ガイドラインの比較分析と提言

①に述べたように、日米欧の基準の対応関係を明確化することが重要である。対応関係を明確化するとは、二つの基準があった場合に、一方の基準の他方の基準に対する過不足や詳細度の差異を明確にすることである。更に、ひとつの基準の中でも要求事項の間の関係がある。これらが基準の分析では重要であるが、従来、人手で分析がなされていた。本研究では、自然言語処理技術を使って、サプライチェーンに係るセキュリティ要件を対象とした米国の SP800-161 と ISO/IEC 27036 とを、政府のセキュリティ要件を対象とした我が国の政府統一基準と米国の SP800-53 とを、それぞれ構成及び条文レベルで比較した。SP800-161 と ISO/IEC 27036 との比較では、異なるプロセスモデルに基づくものの、相補的関係にあり、併用が可能かつ有用であることが確認できた。本成果は、SIP プロジェクト内で紹介して、他の研究課題で活用された。また、政府統一基準と SP800-53 との比較では、緊急時対応計画・プライバシー・トレーニングについて、SP800-53 の方がより詳細に規定していることがわかった。これらの要件は運用時には対応が必須であることから、本研究開発の成果として、関連する要件を政府統一基準に早急に追加することを提言する。

図 SP800-53の自己相関分析

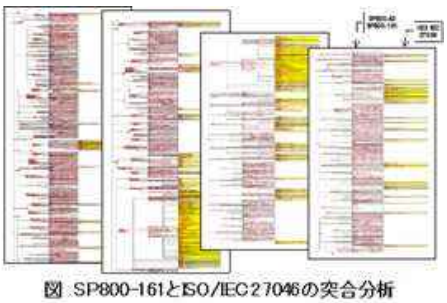
図 SP800-161とISO/IEC 27046の突合分析

本手法によって、分析が省力化できることを定量的に示すことができた（例：12 人月の作業を 0.5 人月に削減）。この手法は、ある基準に適合した製品を別の基準にも適合させたい場合に、広く活用できる手法である。また、基準の比較分析結果自体も、重要インフラの開発企業だけでなく、基準を作る側にも参考情報になる。③のケーススタディは、本分析手法を活用して実施した。

③「SIP／重要インフラ等におけるサイバーセキュリティの確保」の技術に関する適合性確認の仕組みと社会実装のあり方の調査と評価

制度面における適合性確認の仕組みの設計において重要なポイントは、①で述べた。EU のサイバーセキュリティ法の認証フレームワークのような、第三者評価と自主評価による認証のレベル分けは、今後のひとつのあり方であろう。また、SIP 開発技術と規格との関係については、1) (a1)真贋性判定技術と SP800-53 の対応関係分析、2) ②の政府統一基準と SP800-53 を参考に(a2) 動作監視・解析技術の適合性確認のケーススタディを実施した。前者については、SIP プロジェクト内で報告し、他の研究課題でも活用された。

重要インフラシステムのサイバーセキュリティには、共通的要件として、堅牢化・適応性・即応性・協調性が要求される。これらを満たすためには、基準に基づく組織的防御と要素技術に基づくシステム防御に加え、運用保守体制に基づく復旧対応が必要である。(a2) 動作監視・解析技術によって異常検知されても、復旧対応が迅速に行われないと、異常状態が続き、社会に混乱を来たす。監視製品/サービスには復旧対応を要件にすべきであり、このような要件を政府統一基準でも盛り込むべきであると結論した。

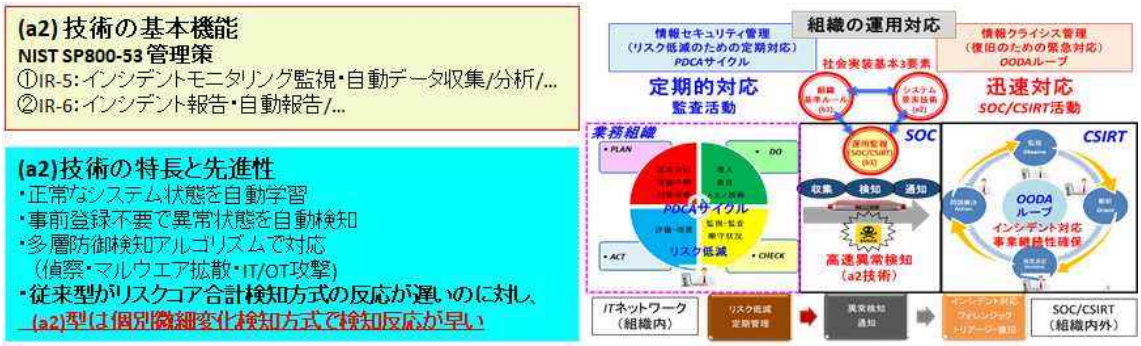

図 (a2) 動作監視・解析技術のケーススタディ

④「SIP／重要インフラ等におけるサイバーセキュリティの確保」の技術に関する国際標準化活動

法的強制のある認証機関及び私的な認証機関について、国際間相互認証のための方法を検討した。各産業界の標準は、各国(欧州の場合は EU の場合もある)の規制に従うものの、業界毎の特性に応じて、分野別に国際標準化の検討を進めることが望ましい。重要インフラ等におけるサイバーセキュリティの確保でも、海外規格との適合性は重要であり、規格の国際標準化が強く求められる。このような国際標準化が必須の分野では、官民一体の交渉と調整が必要である。

③の監視製品/サービスに対する復旧対応の要件化については、適用する重要インフラセクターの標準化委員会でインフラ特有の必要事項を標準化する一方、重要インフラ共通で利用される技術部分については、セキュリティを対象とする委員会で標準化すべきと結論した。

⑤適合性確認の仕組みに必要となるツールの研究(要求分析プロセス支援ツール)

自然言語処理のトピックモデル分析を使い、システムの規格への準拠性確認や規格間の関係を評価する、要求分析プロセス支援ツールを適用試行し、確認を完了した。本ツールにより、単一規格内の自己相関分析及び複数規格間の突合分析を可視化することが可能となる。また、ツー

ルの利用により、規格間の整合性を確認し易くなり、多数のセキュリティ規格が乱立している中で、自組織のガイドラインの見直しや更新を効率良く行うことが期待できる（規格間の整合性確認は、手作業の 5%程度の期間で実施可能）。②は、本ツールを適用して実施した。
ツールによる自動化によって誰が実施しても同等の結果が得られる一方、規程間で記述の視点が異なる場合に事前処理が必要となる課題もある。現状では、有意な結果を得るには、分析対象に関するセキュリティ全般の知識を有する技術者による実施が必要である。

⑥適合性確認の仕組みに必要となるツールの研究（セキュリティ・セーフティ可視化支援ツール）
セキュリティとセーフティの双方の観点からの適合性確認を行うツールの基本原理を構築し、適用性の検証を行った。1 で述べたように、製品開発には、セキュリティ バイ デザインの開発が今後より一般化するであろう。よって、適合性確認は、セキュリティ バイ デザインの開発手法への適用が、より重要になる。本研究では、セキュリティ バイ デザインを前提とした適合性確認ツールを研究した。
基準・規格からゴール指向分析を基にした基準・規格を満たすための必要事項の構造を示すテンプレートを準備し、開発過程において基準・規格に準拠していることの証拠を生成して、上記の規格テンプレートと証拠との比較によって、製品等が基準・規格に適合していることを判断可能にするための手法を開発した。この手法は、製品の適合性確認を企業内で実施する場合に活用できる。

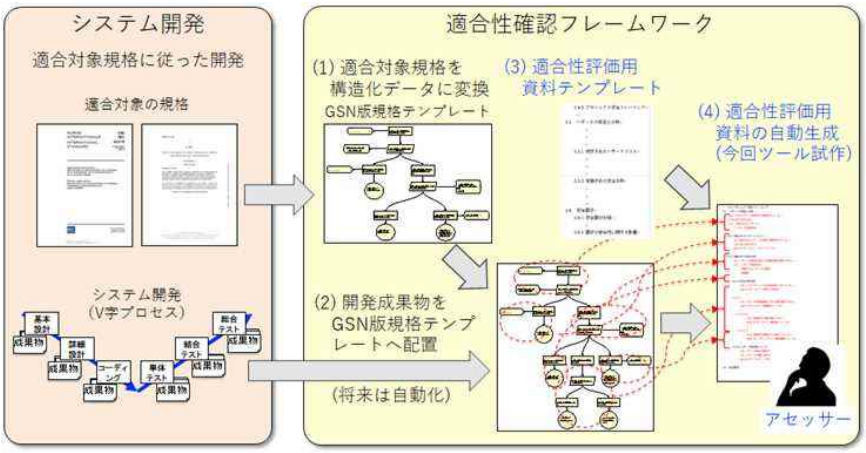

図 開発プロセスにおける基準・規格への適合性確認のしくみ

3. 今後の予定

重要インフラ事業者からの要求に応じて、普及展開を共同研究として実施する。

4. 謝辞

本研究は，内閣府が進める戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」（管理法人：NEDO）によって実施されました。