IoT Acceleration Consortium

資料４

海外のIoT機器の動向

2017年12月11日

IoT推進コンソーシアム

IoTセキュリティWG事務局

EUの動向

これまでのＥＵの動き

IoT Acceleration Consortium

・2017年9月13日、ユンカー欧州委員会委員長の施政方針演説でサイバーセキュリティに関する言及があり、これを受けたデジタル単一市場の施策の一環として、新たにサイバーセキュリティ認証フレームワークの導入を検討していく旨公表。併せて、サイバーセキュリティに関するENISA規則※の修正提案を承認。

・同年11月20日には、ENISAが、「IoTのベースラインセキュリティの推奨事項」を発表。

※Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')

1．欧州委員会がENISAの評価の中間報告をもとに複数のオプションを提案（2017年7月7日）
　①ENISAの今後の組織と戦略の方向性
　②欧州デジタル単一市場におけるサイバーセキュリティ認証フレームワーク（Cybersecurity Act）

2．パブリックコメント（2017年7月7日 - 2017年8月4日）

3．インパクトアセスメント発表（2017年9月8日）
　欧州委員会がENISAの過去の実績を評価するとともに、提案内容について、パブリックコメント、有識者の意見、関係者へのアンケート等を元に各オプションを採用した場合の影響を評価

4．ユンカー欧州委員会委員長による施政方針演説の中で、サイバーセキュリティについて言及
欧州委員会がインパクトアセスメントを元にしたENISAの修正提案を承認（2017年9月13日発表）
　※提案（Cybersecurity Package）の承認であって、提案内容をそのまま採択したわけではない

　①ENISAを恒久的な機関として機能を強化
　　・当初噂されていたEUのセキュリティ庁ではない
　　・EUにおけるセキュリティの標準化や認証に関する業務が含まれることになった
　②セキュリティについて各国、セクター別の支援を行い、認証および表示の枠組みについて既存の認証メカニズムに基づいて構築することを提案
　　・直接的な運用認証制度は導入しない
　　・新たな技術標準の開発は行わない
　⇒次頁　詳細

5．ENISAが「IoTのベースラインセキュリティの推奨事項」を発表（2017年11月20日）
　一般的な課題を抽出し、関係者が解決するために有用となる考え方やツール（既存の規格、ガイドライン、研究資料等）やベストプラクティスを紹介するレポート。

欧州のサイバーセキュリティ認証フレームワークのポイントと欧州委員会にて承認された提案

IoT Acceleration Consortium

欧州のサイバーセキュリティ認証フレームワークのポイント	○ICT機器とサービスについて、**サイバーセキュリティ認証フレームワーク(Cybersecurity Certification Framework)を構築し、欧州内におけるサイバーセキュリティ認証制度を確立する**ことで、欧州におけるデジタル単一市場の信頼性、セキュリティを確保する。 ○欧州サイバーセキュリティ認証フレームワークは、**法の定めがない限り自主的なもの(voluntary)であり、直ちに事業者に規制を課すようなものではない**。
欧州委員会にて承認された提案	ICT機器およびサービスのための欧州サイバーセキュリティ認証フレームワークを確立し、サイバーセキュリティ認証の分野におけるENISAの本質的な機能および任務を規定する。 現在の提案は、欧州のサイバーセキュリティ認証制度を支配する規則の全体的な枠組みを定めている。 この提案では、**直接的な運用認証制度を導入するのではなく、特定のICT機器/サービスのためのサイバーセキュリティ認証制度をENISAが作成**する。 この認証制度では、**製品が遵守する必要のある技術要件および評価手順に関して既存の基準を使用し、技術標準自体を開発しない。**（例えば、現在、**SOG-IS MRA**スキームで国際CC規格に照らしてテストされているスマートカードなどの機器に関するEU全体の認定は、このスキームをEU全体で有効にすることを意味する。） 欧州のサイバーセキュリティ認証制度が採用されると、ICT機器の製造業者またはICTサービスの提供者は、自らの選択した適合性評価機関に自社の機器またはサービスの認証申請書を提出することができる。適合性評価機関は、指定された特定の要件を満たしていればその証明書を発行する。 **監視、監督、執行の任務は加盟国に委ねられている。**加盟国は、1つの認証監督当局を提供しなければならない。この権限は、適合性評価機関のコンプライアンスと、自国の地域に設置された適合性評価機関が発行した証明書と、この規則および関連する欧州のサイバーセキュリティ認証制度の要件とを監督することを任される。

PI4のパブリックコメントにおける反応

IoT Acceleration Consortium

（PI4としてではなく、PI4を構成するVDMA、ZVEI等の団体やドイツ企業の意見）

1．**Don’t put the cart before the horse**
拙速な規制に反対　→　適合性評価に関する議論に移る前に、その範囲とニーズを定義
- セクター別の議論が必要
- 議論は、幅広い関与と受容を保証する標準化団体のような、業界をリードする代表的なプラットフォームで行われなければならない
- 汎用目的のIEC 62443や道路車両用のISO / AWI 21434などの国際標準の使用は、エンジニアリング製品のサイバーセキュリティを向上させる有望なアプローチ（既にかなりのレベルのセキュリティとほとんどの場合、柔軟な方法で確実に確保している）
- コモンクライテリア等の複雑なスキームは、作成されていない領域とその場所で適用

2．**Cybersecurity is a moving target**
必須の第三者認証またはラベル付けに基づく厳格なアプローチは不適切
- フレームワークも特定の実施措置ではなく、リスクアセスメントに基づいて要件を定義すべき

3．**Keeping pace with future technologies**
技術開発による解決策を阻害しない
- フレームワークも特定の実施措置ではなく、リスクアセスメントに基づいて要件を定義すべき

4．新たな規制が必要な場合はNFLで
必須の要件を定義し、必要なリスク分析を実施し、技術ファイルを作成し、**製造業者の宣言（Decision 768/2008 / ECの適合性評価モジュールA）に基づいてコンプライアンスを実行を企業に任せる**

VDMA：ドイツ機械工業連盟
ZVEI　：ドイツ電気・電子工業連盟

IoTのベースラインセキュリティの推奨事項

ENISAが2017年11月20日に発表した、IoTのセキュリティに関する一般的な課題を抽出し、関係者が解決するために有用となる考え方やツール（既存の規格、ガイドライン、研究資料等）、**具体的な産業分野（スマートホーム、スマートカー等）を念頭においたベストプラクティスを紹介するレポート**。

※NISTのSPシリーズに似た体裁であるが、分析と課題抽出がメインで、対策については初歩的な一般論の範疇であり、IoTセキュリティの入門書的。
※ENISAは自ら技術的な規格や仕様の策定は行わないこととなったことから、このレポートで取り上げられているドキュメント類がENISAの認定する認証のベースとなる可能性がある。

1．ENISAはIoTSEC（専門家グループ）を立ち上げ、AIoTIとの連携を強化
2．NISTに準拠する傾向
3．当面、情報システム系を重視し、**IIoTについては当事者によるセクター別の動向を注視するように思われる**

【ENISAが今後推進する内容】

1．IoTセキュリティへの取り組みや規制の調和を推進
2．IoTサイバーセキュリティの必要性についての意識を高める
3．IoTのための安全なソフトウェア/ハードウェア開発ライフサイクルガイドラインを定義
4．IoTエコシステム間の相互運用性のためのコンセンサスを確立
5．IoTセキュリティのための経済的・行政的インセンティブの育成
6．安全なIoT製品/サービスのライフサイクル管理の確立
7．IoT利害関係者間の責任の明確化

米国の動向

サイバーセキュリティに関する大統領令

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure（連邦ネットワークおよび重要なインフラストラクチャに対するサイバーセキュリティの強化に関する大統領令）　2017年5月11日

①連邦政府のネットワーク　②重要インフラ　③国家／国民のための**サイバーセキュリティ(ボットネット対策含む)に関して各連邦政府機関の長に対し、期限以内に大統領に報告書を提出するよう指示したもの**

これを受け、NTIA（米国商務省電気通信情報局）は「ボットネットおよびその他の自動化された脅威に対するステークホルダーアクションの促進」に関するコメントの要請（RFC）を実施し、47件のコメントをもとに報告書を発表
https://www.ntia.doc.gov/files/ntia/publications/rfc_comment_summary_20170918.pdf

【概要】

①不必要なコストと革新の遅れをもたらす可能性のある国固有の基準や規制ではなく、効果的なグローバルなアプローチを達成するためには、国際基準とベストプラクティスが必要

②NISTのサイバーセキュリティフレームワークやNTIAのマルチステークホルダープロセスを含む、自発的かつコンセンサスベースの業界および地域社会主導のプロセスが大いに支持された（ 政府があまりにも大きな規制上の役割を果たすことに反対する強い声が多くあった）

【IoT機器に関する主な意見】

①既存のアプローチやベストプラクティスの共有
②安全なテクノロジの構築、展開、および取得を容易にする認証と標準の重要性
③信頼できる第三者による商品が安全であることまたは標準に準拠していることの認定

意見は多様

※大統領令への報告書草案は2018年1月5日からのパブコメを経て、2018年5月11日に最終報告書として発表の予定

『Framework for improving Critical Infrastructure』(サイバーセキュリティフレームワーク)の改訂について①

2014年2月、アメリカ国立標準技術研究所(NIST)は、サイバーセキュリティ対策の全体像を示す『Framework for improving Critical Infrastructure』(サイバーセキュリティフレームワーク)を公表

セキュリティ・フレームワーク・コア

特定：最初に、組織としてサイバーセキュリティに関する方針を決定する”、“どのようなリスクがあるかを特定する”等

防御：リスクの多寡に応じて適切な予防策を講じる

検知：防御策を監視することで突破されそうになった（あるいはされた）ことをいち早く察知する

対応：異常が検知され必要な暫定処置を講じる

復旧：恒久措置を施し元通りの状態に回復させる

他の規格との比較

NISTフレームワーク	安全対策基準（FISC）	ISO27001 情報セキュリティマネジメントシステム	ISO27031 事業継続のための情報および通信技術の準備態勢に関する指針に基づくマネジメントシステム	ISO22301 事業継続マネジメントシステム
特定	◎	◎	△	○
防御	◎	◎	△	△
検知	◎	◎	△	○
対応	◎	○	○	○
復旧	◎	△	○	○

（◎：比較的強い関連性が認められる、　○比較的関連している、　△部分的に関連している）

既存の標準規格、ガイドライン、ベストプラクティスをマッピング

NISTフレームワークはあくまでも**ITシステム**に関連する情報を保護するためのセキュリティについてであり、産業IoTに特徴的な「モノ」や「サービス」に対することはほとんど考慮されていない。

出典:「重要インフラのサイバーセキュリティを向上させるためのフレームワーク 1.0版」(英和対訳版)

『Framework for improving Critical Infrastructure』(サイバーセキュリティフレームワーク)の改訂について②

2017年1月及び12月に、アメリカ国立標準技術研究所(NIST)は、サイバーセキュリティフレームワークのversion 1.1(Draft1及びDraft2)を公表

最も大きな改訂内容はSecurity Framework Coreの「特定」に**Supply Chain Risk Management（SCRM）のカテゴリー追加**

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management

【Version 1.1の主な改定内容】

- ●サイバー攻撃のライフサイクル
- ●サイバーセキュリティの測定
- ●テクニックの参照
- ●中小企業の意識とリソース
- ●ガバナンスと企業リスク管理

記載内容の拡充とそれに伴うサブカテゴリーの追加や名称変更などが中心

※今後の改定予定

1 信頼メカニズム
2 サイバー攻撃のライフサイクル
3 サイバーセキュリティ人材
4 サイバーサプライチェーンのリスク管理
5 連邦機関のサイバーセキュリティアライメント
6 ガバナンスと企業リスク管理
7 アイデンティティ管理
8 国際的側面、インパクト、アライメント
9 サイバーセキュリティの測定
10 プライバシーエンジニアリング
11 参照手法
12 中小企業の意識とリソース