特集
Special Feature

［DX（デジタル・トランスフォーメーション）時代のサプライチェーン・セキュリティ］

1 サプライチェーンにかかわるセキュリティを確保するための仕組みと制度

基 応 専 般

～社会的な説明責任を果たすためのアプローチ～

石黒正揮 | （株）三菱総合研究所

サプライチェーン脅威の拡大

Web サービスの情報基盤を提供するディジタル・プラットフォーマ，ディジタル・サービスの集約・提供を行うアグリゲータ，消費者自らが Web サービスを生み出すプロシューマなどさまざまな企業等などから構成されるビジネス環境（「ビジネス・エコシステム」と呼ぶ）を活用することで新しい価値を迅速に生みだす成功事例が増えている．従来から巨大なサプライチェーンを構成する自動車産業においても，系列による固定的なサプライチェーンから，AI ベンチャー，タクシーや鉄道など移動手段を組み合わせたサービスを提供する MaaS（Mobility-as-a-Service）事業者など新しいプレイヤとの連携を積極化し，自前主義からスピードとイノベーションを重視した分野横断的なビジネス・エコシステムへと業界構造が変革している．

一方で，サプライチェーンやエコシステムの変革に伴い，多様な主体（ステークホルダ）がかかわることでセキュリティ・リスクが増大している．情報処理推進機構による「情報セキュリティ 10 大脅威 2020」では，サプライチェーンの弱点となる企業への攻撃が，組織に対する 10 大脅威の上位に位置付けられ，サプライチェーンを通じたセキュリティの確保が重要な課題としている．また，イギリス政府 CERT-UK の調査レポート[☆1]では，サプライチェーンにおけるセキュリティリスクの 92% は脆弱な中小企業を狙ったものとしている．

近年，5G 通信インフラにおいて米国政府が中国ベンダ数社の製品に安全保障上の問題があるとして国際貿易における製品排除に動いている．米国では，2011 年に偽装品に関する国防省への報告が義務化されており（GIDEP（Government-Industry Data Exchange Program）），2011 年から 2015 年までにマイクロチップの偽装品などを含む 450 件以上の偽装品に関する報告がなされサプライチェーンにかかわる脅威について危機感が強い．

サプライチェーンにかかわるセキュリティ脅威を取引にかかわる組織（ステークホルダ）と開発から廃棄に至るライフサイクル・プロセスを 2 軸として俯瞰したものが図 -1 である．

脅威は，開発の上流から廃棄に至るまで全体に渡り存在する．近年は，プロセッサへの不正ロジック，バックドアの組込みなどハードウェア・トロイの脅威も高まっており，ソフトウェアによるセキュリティだけでは対策が困難である．

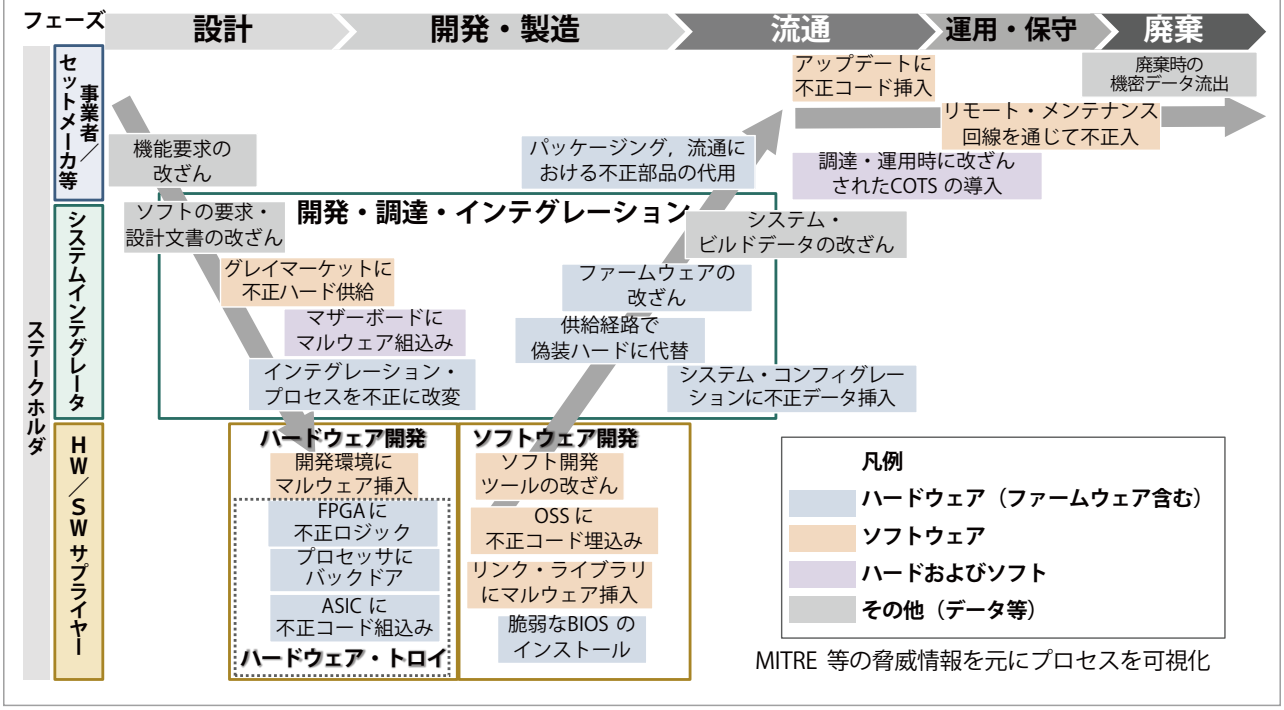
このようにサプライチェーンの複雑化・グローバル化と，サプライチェーン・インシデント（事故）の増加により，企業，政府におけるサプライチェーン・セキュリティに対する危機感が高まっている．

☆1 CERT-UK, Cyber-security risks in the supply chain.

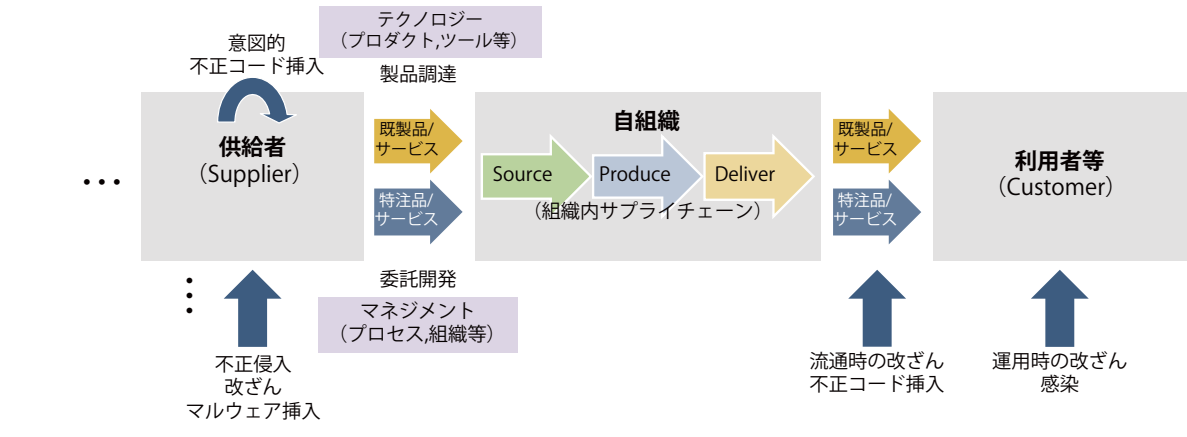
サプライチェーンの構造と脅威

サプライチェーンの構造と脅威の関係を一般化したものが図 -2 である．

サプライチェーンは製品・サービスの供給者から最終利用者に向けて多段的につながっている．サプライチェーン脅威としては，供給者の開発プロセスへの不正侵入，改ざん，マルウェア挿入や流通過程での不正コードの挿入，運用・アップデート時の改ざんなどが挙げられる．調達・供給は，既成品と特注（委託開発）に大きく分かれ，適用できる対策に違いがある．既成品等の場合，開発プロセスに関与できないため対象製品・サービスに対して検証技術などのテクノロジーを適用しセキュリティを確保する．特注の場合，開発や SI の発注から受入れに至るまでのプロセスにおける管理・監査等のマネジメ



■図 -1　サプライチェーン・プロセスにおける主なセキュリティ脅威



■図 -2　サプライチェーンの一般的な構造と脅威の関係

ントを適用することも可能である.

サプライチェーンセキュリティ基準の活用アプローチ

サプライチェーンセキュリティに活用できる基準等は既存のものだけでも多数存在するが，基本構造，目的，産業分野への特化など関係性が複雑であり，適切な基準群を組み合わせて，適切なレベルとコストで対策することが難しい. 図-3 は, サプライチェーンにかかわる基準，標準等を，現在の導入状況に応じて，どのように追加補強し包括的な対策を実現するかについて選択の考え方を俯瞰したものである.

サプライチェーンセキュリティの確保のためには，以下の手順で関連基準を選択し組み合わせることで，コストと対策レベルのバランスを確保することが妥当である.

①ベースとするフレームワークの選択

代表的なセキュリティ・フレームワーク（NIST Risk Management Framework, Cybersecurity Framework, ISO/IEC 27000 シリーズなど）をベースとして選択し対策の全体構造を設定し，②以下の具体化を検討する.

②産業分野に応じた基準の追加選択

産業分野固有の対策と経済性を高めるカスタマイズを行った基準を選択し，対策コストと達成レベルの費用対効果を高める.

③重点課題による選択

改ざん検査，調達，偽装対策など重点課題に応じて強化したい対策基準を選択・導入する.

さらに具体的な選択方法の詳細については割愛するが，各領域に精通した専門家との協力により組合せを検討することも有効である.

説明責任とセキュリティ・アシュアランス

サプライチェーンにおいては，各ステークホルダ

①ベースとするフレームワークの選択

	NIST 利用	現在利用フレームワーク無	ISO/IEC利用	産業固有または組織固有の基準
セキュリティフレームワーク	NIST Risk Management Framework SP800-53	NIST Cybersecurity Framework 経済産業省　サイバーフィジカルセキュリティ対策フレームワーク	ISO/IEC 27001 ISO/IEC 27002	Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance
サイバーサプライチェーン	NIST SP800-161 NIST SP800-171 NIST IR 7622	IoT推進コンソーシアムIoT セキュリティガイドライン	ISO/IEC 27017	FFIEC, OCC Guideline IEC/ISA62443-2-4 FS-ISAC 3rd Party Software security control Types Cybersecurity Procurement Language for Energy Delivery Systems
産業別標準・認証	NIST SP800-82 NIST IR 7628	Energy Sector Cybersecurity FW Implementation Guidance Cybersecurity and Risk Management Best Practice: CSRIC WG4	ISO/IEC 27011 ISO/IEC 27015 ISO/IEC 27019	NERC CIP; C2M2 CSRIC TISAX AIAG Cyber Security 3rd Party Information Security UL VCSP
ソフトウェア完全性（改ざん検査）	SAFECode Software Integrity guidelines			
セキュリティ調達	ANSI/ESD S20.20-2007; C-TPAT; AEO; TAPA; Electronics Industry Citizenship Coalition(CICC); Dodd-Rrank Conflict Mineral Requirements			
偽装対策	SAR Standards, MITRE Attack Pattern			
適合性評価	Common Criteria(ISO/IEC 15408) Certification, The Open Group Trusted Supplier Program; AZLA Accreditation; ISO9001 Certification , EDSA Certification, UL CAP			

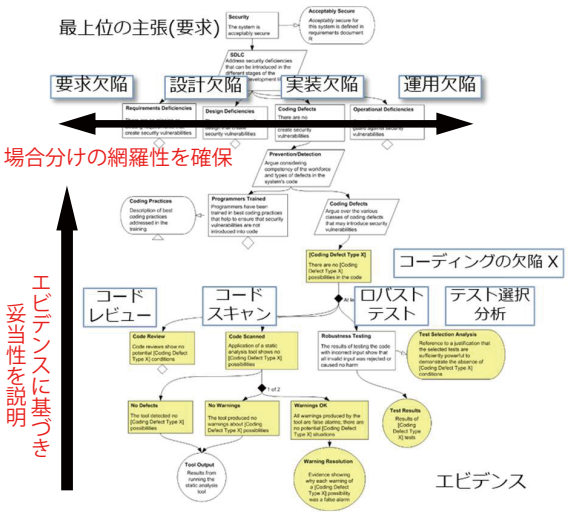
②産業分野に応じた基準の選択

③重点課題による選択

■図-3　サプライチェーン・セキュリティ基準等の選択指針と手順

によるセキュリティ確保は必要条件であるが，セキュリティを確保していることをほかのステークホルダに説明し信頼を得ることができなければ十分とは言えない．特に，調達元に課される事故責任が厳格になればなるほど，調達先に対する説明責任の要求レベルは高くなる．**セキュリティ自体の強化と，他のステークホルダに対してセキュリティの説明責任を果たしていることは必ずしも一致しない．**高いセキュリティを達成していても，グローバルに通用する説明責任を果たさなければ契約が獲得できないなど企業にとっては影響が大きい．ステークホルダ間での信頼性の確保を意味する Trustworthiness（信頼性保証）という概念について，NIST SP800-39 では，「Trustworthiness は，セキュリティ機能とアシュアランスの 2 つの異なる概念の組合せ」として定義されている．

説明責任を果たす上で，何をどの程度やならなければならないか？　その判断を行う上でアシュアランス・ケースの考え方が重要である．アシュアランス・ケースは，システムに関する主張や要求が満たされていることを根拠情報（エビデンス）と論証に基づき体系的，客観的に示すための説明文書である．機能安全規格の認証においては，アシュアランス・ケースの提示が要件化されており，セキュリティ分野では，IT 機器のセキュリティ認証基準 ISO 15408（コモン・クライテリア）の評価保証は同様の考え方に基づいている．図 -4 は，アシュアランス・ケースの例を示すものである．



出所）Arguing Security . Creating Security Assurance Cases, CMU/SEI,を元に作成

■図 -4　アシュアランス・ケースのイメージ

たとえば，ソフトウェアの欠陥がないことを示す場合に，要求欠陥，設計欠陥，実装欠陥，運用欠陥等がないことなどを体系的，網羅的に示しつつ，それらを階層的に掘り下げることで，最終的にはテスト結果のデータなどのエビデンス（根拠情報）まで視覚的に示すものである．アシュアランス・ケースの論証は納得性のある説明ができることが重要であり，固定的なやり方ではなく柔軟に考え方を示すことで対応可能である．国際標準に基づく認証に慣れていない国内企業の中には，セキュリティ要求事項に対して，硬直的な対応にこだわり対策コストがかさむことで競争上の不利を招くケースが見られるが，要求事項の本質を理解することで，柔軟な説明が可能であり，説明責任を確保しつつ，意味の無い不必要な対策コストを低減することがセキュリティ・アシュアランスを実現する上で重要となる．

サプライチェーン・ガバナンス

インフラ・システムの構築・運用においては，市場メカニズムに任せていただけではセキュリティ対策投資が十分に進まないということがセキュリティ経済学の研究で示されている．インフラ事故発生時のインフラ事業者に対する事故責任の明確化，損害額の適切なリスク定量化と把握，発注者と受注者のセキュリティ技術の理解に関する情報の非対称性などが原因となり，インフラ事業者が必要なセキュリティ対策予算を確保することができず，技術的なセキュリティ対策を受託するベンダのインセンティブの低下，モラルハザードを招くためである

(図 -5) [☆2]．このような問題は，サプライチェーン・ガバナンスの欠如と言うことができる．

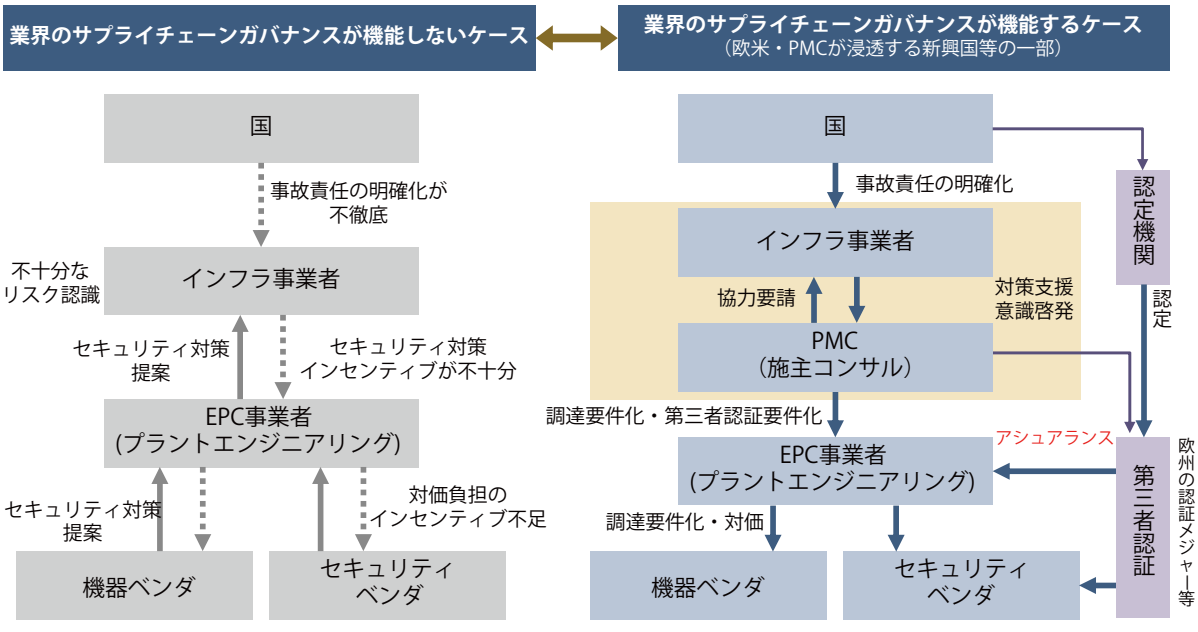
このような問題を解決するためには，インフラ事業者に対する事故責任の明確化とともに，インフラを構築するエンジニアリング会社と技術的に対等に渡り合える専門家による PMC（Project Management Consultant）を設置することで，必要なセキュリティ対策の要件化とそれに対する適合性確認または第三者認証によるセキュリティ・アシュアランスが重要となる．

適合性評価国際標準と認証制度

セキュリティ対策の説明責任を向上させる手段として，ISO/IEC 17000 適合性評価に対応した認証制度等がある．これには，第三者認証と自己適合宣言がある．サイバーセキュリティにかかわる国際標準，認証制度は国，標準化団体により整備が進められている．これらの標準，規準等の中から自組織に有効なものを選択し，適合性評価を実施することは，説明責任を向上させる有効な手段である．図 -6 は，セキュリティ分野の適合性評価にかかわる制度を分類したものである．

制度は，政府による強制基準（規制），政府調達基準，任意制度に分けることができる．電力などの重要インフラで事故の影響が大きい場合，強制基準となる例がある．また，認証制度 CC（Common Criteria），CMVP（Cryptographic Module Validation Program）などは政府調達基準とする国は多く，国際相互承認が進み，認証取得件数は増加傾向にある．また，EDSA（Embedded Device Security Assurance）などプラント分野における国際的な調達要件や ISMS（Information Security Management System）などサイバー保険料の割引に認証取得が条件とされる例もある．セキュリティ対策を促進し，サプライヤー間の説明責任を向上させる上で，各分野のリスクと要求レベルに応じてこのような選択肢を活用することは効果的である．産業分野ごとに，脅威トレンドや損害リスクの規模，システムに要求されるレベルの違いが大きいため，図 -3 でも

☆2 詳細は，特集「ディジタルエコノミー時代のサイバーセキュリティ」，サイバーセキュリティ経済学，情報処理，Vol.59, No.12 (Dec. 2018) を参照．



■図 -5　サプライチェーンの責任関係とガバナンスの課題

示した通り，汎用的な共通フレームワークと産業別，目的別に具体化した基準など自組織に適した基準を適切に選択できることはきわめて重要である．

今後の課題と展望

以上の動向および制度・仕組みを踏まえ，改めて今後の課題をまとめると以下の通りである．

- **対策フレームワークと分野最適化した基準の整備の必要性**
  フレームワークに対して分野のリスク，要求レベルに応じて適切にカスタマイズした基準が未整備な分野についてはカスタマイズが期待される．現在整備中の自動車分野，医療機器分野などが例である．
- **セキュリティ・アシュアランスに関する基盤整備**
  セキュリティ強化自体と他のステークホルダへの説明責任の確保の違いを意識し，グローバルに受け入れられるセキュリティ・アシュアランスのガイダンスやテンプレート集の作成が期待される．
- **サプライチェーン・ガバナンスの確保**
  業界のリスクに応じてステークホルダの責任および関係者の責任分界点の明確化と業界ガイドラインの整備が必要である．
- **ディジタル・トラスト・プラットフォームの構築**
  サプライチェーンを通じた信頼の連鎖の確保のための技術的，組織的なセキュリティ評価認証結果の情報共有プラットフォームの構築は有効である．

以上のような取り組みを通じて，今後進展するディジタル・エコシステムやサプライチェーンにおけるセキュリティの向上が期待できる．

(2020 年 11 月 2 日受付)

謝辞　本稿は，内閣サイバーセキュリティセンターの「サプライチェーンリスク対応のための技術検証体制構築に関する調査」，経済産業省の「平成 30 年度高度な自動走行システムの社会実装に向けた研究開発・実証事業（自動運転が活用されうるコネクテッド技術に関する国内外動向調査）」，NEDO の「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に関する検討」等の委託調査において（株）三菱総合研究所が実施した成果等を参考まとめたものです．調査等を通じて，内閣サイバーセキュリティセンター，経済産業省自動車課，内閣府 SIP プロジェクトの皆様に大変にお世話になりました．皆様には深く感謝を申し上げます．

■石黒正揮（正会員）　masa@mri.co.jp

博士（情報科学）．東京大学大学院理学系研究科情報科学専攻修士課程修了．現在，（株）三菱総合研究所サイバーセキュリティ戦略グループ．専門は，サイバーセキュリティ，ディジタル戦略，ディジタル・エンジニアリング，AI/ 数理データ解析，リスク評価，日米欧アジアにおけるセキュリティ政策・技術戦略，セキュリティ経済学，ディジタル経済学．調査コンサルティングに従事する．

区分		認証制度		スキーム オーナ	基準／標準	認定機関	認証機関	国際相互承認MRA	概要
政府	任意	CSMS		（METI/JIPDEC）	CSMS認証基準（IEC 62443-2-1相当）	JIPDEC	JQA, BSI Japan	なし	制御システムを対象としたセキュリティマネジメントシステム
政府	任意	ISMS		（METI/JIPDEC）	ISO 27000シリーズ	JIPDEC	JQA, TUV Rheinland, DNV	IAFで検討中	組織の情報セキュリティに関するマネジメントシステム．セキュリティ向上と国際的な信頼向上が目的
政府	政府調達基準※	Common Criteria	CCEVS	NIAP（NIST,NSA）	ISO/IEC 15408	NIAP	NIAP（CC testing Lab's）	CCRA 17カ国	IT関連製品（複合機，情報システム，ICカード，ソフトウェア等）の情報セキュリティ（JISEC 制度 2001 年創設，2003年CCRAに加盟）
政府	政府調達基準※	Common Criteria	JISEC	（経産省/IPA）	ISO/IEC 15408	IPA/NITE	IPA（ECSEC等）		
政府	政府調達基準※	CMVP	CMVP	米NIST/ 加CSEC	FIPS 140-3 ISO/IEC19790	NIST（NVLAP）	CygnaCom, InfoGuard等	NIST-IPA 共同認証（2012 年）	暗号モジュールの暗号アルゴリズムの実装と鍵，ID，パスワード等の重要情報のセキュリティ確保（CMVP1995開始，JCMVP2007 年正式運用開始）試験ツールJCATTを用いて実施するため，暗号アルゴリズムの深い知識は不要．
政府	政府調達基準※	CMVP	JCMVP	（経産省/IPA）	JIS X 19790（FIPS 140-3）	IPA/NITE	IPA（ITSC, ECSEC等）		
政府	強制	NERC-CIP		FERC	CIP V5	FERC	NERC	なし	電力事業者等に対するサイバーセキュリティ対策
政府	強制	中国CCC		国家認証認可監督管理委員会（CNCA）	中国国家標準（GB）	CNCA	指定認証期間（CQC等）	なし	輸入されるIT セキュリティ製品，自動車関係，電気製品等の指定製品の安全確保，環境保全（中国政府調達品の自国品優遇制度の懸念あり）
民間	任意	EDSA/ISASecure		ISCI	EDSA標準（IEC 62443-4-2 等に相当）	ANSI/ACLASS（米国）	Exida	IAF	制御システム・コンポーネントのセキュリティ確保．Wurldtech, Achiless等のツールを用いる
民間	任意	EDSA/ISASecure		ISCI	EDSA標準（IEC 62443-4-2 等に相当）	JAB（日本）	CSSC CL		
民間	任意	CAP		UL	UL 2900（IEC 62443参照）	（ANSI規格になった場合，OSHA）	ULのみ	なし	ネットワーク接続型製品ならびにシステムのサイバーセキュリティ確保．Synopsisのツールなどを用いる
民間	任意	TUV SUD IEC 62443 certification		TUV SUD	IEC 62443-4-1, 3-3, 2-4	—	TUV-SUみ	なし	制御システムの管理，システム，コンポーネントに関するセキュリティ確保
民間	任意	情報セキュリティ格付		（株）ISレーティング	マネジメント成熟度等	—	（株）ISレーティング	なし	企業や組織が取り扱う技術情報，営業機密，個人情報についてセキュリティのレベルを格付

■図 -6　適合性評価等にかかわる制度の整理