特集論文

FA製品でのサイバーセキュリティーやAI関連の法令規格対応

藤島光城*
Mitsushiro Fujishima

*名古屋製作所

Compliance for FA Products with Cyber Related Laws and Regulations Such as Cybersecurity

要　旨

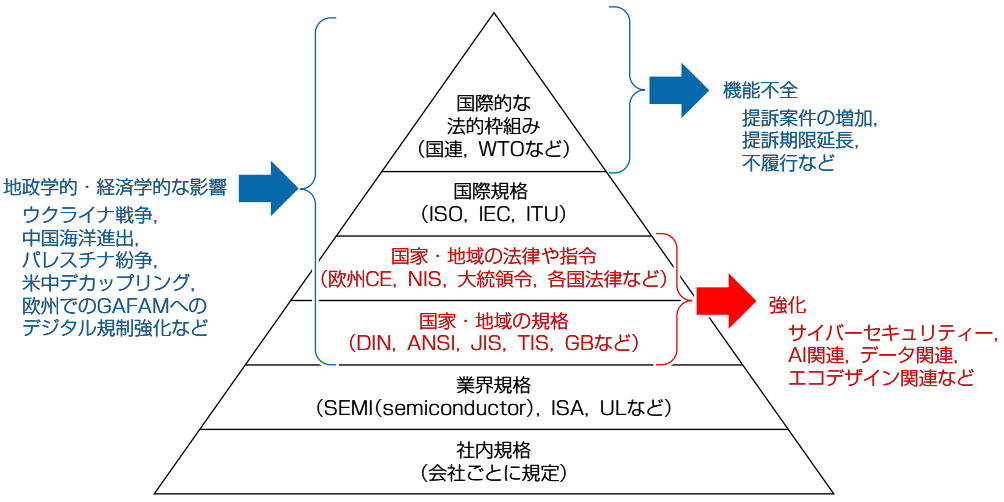
海外市場に製品やサービスを投入する多くの企業にとって，従来の電気安全法や有害物質を規制した欧州RoHS(the Restriction of the use of certain Hazardous Substances in electronic equipment)指令などフィジカル関連の法令規格への体制や人材育成はできているが，サイバーセキュリティーやAIなどのデジタル関連(以下“サイバー関連”という。)の法令規格への体制や，人材育成は十分とは言えない状況にある。この状況は法令規格違反が大きなニュースになる現代では企業経営を揺るがしかねない問題に発展する危険性もある。

また，各国や地域のサイバー関連の法令規格に迅速かつ真摯に取り組むことは，様々な変革で企業競争力の底上げにつながる。

1. ま え が き

現在，製造DX(Digital Transformation)や産業IoT(Internet of Things)，第４次産業革命など世界中の工場やオフィスの情報をデジタル化して，インターネットによってリアルタイムにデータ共有することで製造変革やビジネスモデル変革を実現し，また，Society 5.0やSDGs(Sustainable Development Goals)等で環境問題の解決や人の幸福を追求するウェルビーイング(Well-being)を実現する社会変革が進みつつある。

このような世界規模で大きな変革が進む中では，国や地域を超えたグローバリゼーションでの協力体制が必要である。しかし，**図１**に示すように近年のウクライナ戦争や中国の海洋進出，中東でのパレスチナ問題，米中のデカップリングや欧州での米GAFAM(Google，Amazon，Facebook，Apple，Microsoft)へのEU一般データ保護規則(European Union, General Data Protection Regulation：GDPR)など，“地政学的・経済学的な影響”からディグローバリゼーション(＝脱グローバリゼーション)の流れも活発化し，国際的な紛争や貿易問題を調停する機関である国連やWTO(世界貿易機関：World Trade Organization)の“機能不全”も指摘されている。



ISO：International Organization for Standardization，IEC：International Electrotechnical Commission，ITU：International Telecommunication Union，
CE：Conformite Europeenne，NIS：Network and Information Systems Directive，DIN：Deutsches Institut für Normung，
ANSI：American National Standards Institute，JIS：Japanese Industrial Standards，TIS：Thailand Industrial Standards，
GB：Guo jia Biao zhun，ISA：International Society of Automation，UL：Underwriters Laboratories Inc.

図１-法令規格の影響力の変化

このような国際情勢の中で，中国はインターネットにも国境があるとして，2017年６月に中国サイバーセキュリティー法(以下“中国CS法”という。)を施行した。また，今後も2024年に欧州CRA(Cyber Resilience Act)やAI規則案，データ法，デジタル製品パスポートなどサイバー関連の法令規格や要件の新設や強化が続々と検討されている。

また，近年のSNS(Social Networking Service)等の普及で情報が拡散し炎上する社会環境下では，たとえ製品の品質に問題がなくても，法令規格等に対して違反した企業のイメージダウンによって経営に与えるダメージも非常に大きいことは言うまでもない。

本稿では，既に施行された中国CS法や，今後施行が予定される欧州CRAの概要や経緯について述べるとともに，今後の課題について述べる。

2．中国CS法

中国CS法は海外からのサイバー攻撃や中国国内の企業秘密漏洩(ろうえい)，及び個人情報流出などの国家安全を保障するため，中華人民共和国主席自らが署名し発行された法律である。関連法も多く発行されており特に“サイバーセキュリティー法”“データセキュリティー法”“個人情報保護法”の関連三法が重要とされている。

この法律には“報告義務”もあり，違反した場合は是正勧告，警告，罰金，営業許可の取消し，“違反に関わった人”に対する罰金や刑事責任も科せられる。また，中国CS法は国防にも関連するため，海外企業にとって最近強化された“反スパイ法”の影響も無視できず中国域内で活動する従業員の安全確保のためにも遵守が必要な状況である。

2.1　中国CS法の調査経緯と課題

2015年６月に中国CS法の草案が出され，2016年11月に全国人民代表大会常務委員会で可決，公布され，2017年６月から施行された。同時期に公開された“ネットワーク重要設備及びネットワークセキュリティー専用製品目録”(2017年第１号，2023年７月に改定)に三菱電機FA分野でも該当製品があり先行調査を開始した(**表１**)。

表１−ネットワーク重要設備及びネットワークセキュリティー専用製品目録(2017年第１号公布から一部抜粋)

分類	設備／製品名称	要求範囲
ネットワーク適用の重要設備	ルーター	スループット(双方向)≥12Tbps，ルーティングテーブル容量≥550,000
	スイッチ	スループット(双方向)≥30Tbps，パケットスイッチングレート≥10Gpps
	サーバー	CPU数≥８個，CPU一つ当たりのコア数≥14個，メモリー容量≥256GB
	PLC	基本演算処理速度≤0.08μs
ネットワークセキュリティー関連製品	データバックアップマシン	バックアップ容量≥20T，バックアップ速度≥60MB/s， バックアップ時間間隔≤１h
	ファイアーウォール	スループット≥80Gbps，最大同時セッション数≥3,000,000， １秒当たりの新規セッション数≥250,000
	ウェブアプリケーション・ファイアーウォール	スループット≥６Gbps，最大HTTP同時セッション数≥2,000,000
	Intrusion Detection System (不正侵入検知システム)	最大検出速度≥15Gbps，最大同時セッション数≥5,000,000
	Intrusion Prevention System (不正侵入防止システム)	最大検出速度≥20Gbps，最大同時セッション数≥5,000,000
	セキュアゲートウェイ	スループット≥１Gbps，システム遅延≤５ms

PLC：Programmable Logic Controller，HTTP：Hyper Text Transfer Protocol
出典：中国公開情報：ネットワーク重要設備及びネットワークセキュリティー専用製品目録(2017年第１号)

当社にとって当時最大の課題は，該当製品に対するこの法律の国家規格(中国GB規格)がまだ策定されておらず，さらにサイバーセキュリティーの適合性評価基準や評価機関，最終的に認証を与える機関等が不明であった点である。

また，社内では電気安全法や有害物質を規制した欧州RoHS指令など，ハードウエア面(フィジカル)での法令規格の体制や人材は育成できていたが，サイバーセキュリティーなどソフトウエア面での最新のサイバー関連技術の法令規格に対する体制や，人材育成は十分とは言えない状況であった。

2.2　中国CS法への対応

この法令の規格を策定する中国の標準化委員会(SAC/TC28，TC260，TC124)や，評価や認証の候補機関に問合せを行いながら，中国CS法で求められる要件や，評価や認証の時期，評価機材の手配などの該当製品の対応計画を立てた。

また，社内全体の製品やサービスのセキュリティーレベル向上やインシデント発生時に対応を行う組織であるPSIRT

(Product Security Incident Response Team)[1]や，中国拠点や販売拠点との連携体制を構築し，中国及び日本国内に専門の要員を配置，育成するなどの対策を実施した。

2018年３月に公表された“ネットワーク重要インフラ設備及びネットワークセキュリティー専用製品のセキュリティー評価及び認証を実施する機関のリスト(第１回)”で該当機関が明らかになったが，該当リストにはそれ以前から候補として挙がっていた機関が含まれており，早期に関係性を構築しておいたことで，該当製品に対する評価及び認証等が比較的スムーズに行えた点からも，2017年から始めた先行調査の意義は大きかった。

また，2022年12月～2023年10月にかけて該当製品のGB規格(技術要件，試験方法)が公開されたが，現地拠点経由で策定中の規格の適正化に向けて意見を出した。この認証取得は中国関連法令や国家標準規格に準拠した適切なセキュリティー対策済みの製品であることが公的に証明され，取引先やユーザーに対して政府認証を受けた証しとしてアピールできるメリットがある。

なお2017年当初，製品認証取得の対応時期の猶予期間は2019年１月までであったが，実際には2023年７月以降に延期された。現在では中国国内で認証を取得していないものは原則販売できなくなっている。また，中国政府の調達リストにも掲載されないため，中国企業の20%を動かすとされている国有企業への販売もできない。当社FAの該当製品は2023年６月までに評価を完了し認証を取得済みである。

3. 欧州CRA

欧州CRAは欧州域内の法的枠組みの中で有効になる法律である。例外を除いて“デジタル要素を備えた全ての製品が対象”になり対象範囲が広い。また，EU指令がCRAに準拠する形式で改定＆承認されるため，デジタル製品で“CEマーキング”を取得するにはCRA対応が必須になる。

ほかにもインシデントや脆弱(ぜいじゃく)性の“報告義務”も必要であり，それらなしにEU市場で製品を販売できない。

さらに違反時の罰則として最高1,500万ユーロ又は当該企業の全世界売上高の2.5%のどちらか高い方の罰金と厳しい規定がある。

3.1　欧州CRAの調査経緯と課題

欧州でのサイバーセキュリティーに関する取組みとして，2016年８月にネットワーク及び情報システムに関するリスク対策やインシデントの対処能力，安全水準の向上を掲げてNIS指令が施行された。また，2018年５月には一般データ保護規則であるGDPRが施行された。さらに2019年６月に欧州ネットワーク・情報セキュリティー機関であるENISA(European Network and Information Security Agency)の権限強化や，サイバーセキュリティー認証制度の整備のためにEUサイバーセキュリティー法が施行された。

この時点までは具体的なデジタル製品のサイバーセキュリティーに関する必須要件が含まれていなかったが，2022年９月に欧州委員会から欧州CRAの草案が発表され，重要なデジタル製品リストのクラスⅠ(低リスク)，クラスⅡ(高リスク)に当社FA分野の該当製品があり先行調査を開始した(**表２**)。

表２-重要なデジタル製品(欧州CRA草案から一部抜粋)[注1]

	製品名
クラスⅠ(低リスク)	20. マイクロコントローラー，21. ASIC及びFPGA，22. PLC，DCS，CNC，SCADA，産業オートメーション及び制御システム(IACS)(クラスⅡ製品以外)
クラスⅡ(高リスク)	7. 産業用のルーター，モデム，スイッチ，12. PLC，DCS，CNC，SCADA，産業用オートメーション及び制御システム(IACS)，14. ロボットセンシング及びアクチュエーター・コンポーネント及びロボットコントローラー

ASIC：Application Specific Integrated Circuit，FPGA：Field Programmable Gate Array，
DCS：Distributed Control System，CNC：Computerized Numerical Control，
SCADA：Supervisory Control And Data Acquisition，IACS：International Annealed Copper Standard
(注１)　欧州CRA公布時には該当製品の見直しが入る見込み
出典：欧州公開情報：重要なデジタル製品(欧州CRA草案)

現在，欧州委員会，議会，理事会の三者間対話(トリローグ)が完了し，2024年度の公布に向けて準備中である。また，“製品適用”の施行時期は，草案段階では2025年末を目指すとされていたが，トリローグで若干延期の方向で調整されている。ただし，この法案は2022年２月の地政学的な問題(ウクライナ戦争)が発生し，実際に多くのウクライナのインフ

ラ設備がサイバー攻撃の被害を受けたため，早期の施行が望まれている状況に変わりはない。

なお，インシデントや脆弱性の“報告義務”は“製品適用”より早く施行される見込みである。

3.2　欧州CRAの対応

2023年1月に草案に対する意見公募(パブリックコメント)があり，欧州で日本の産業界を代表して活動しているJBCE(Japan Business Council in Europe)[2]と連携し，海外からは時差もあるため24時間以内のENISAへの“報告義務”の遵守が難しい点や，報告開始時点の定義が不明確など，当社からも意見を出して働きかけを実施した。

現時点では中国CSの経験を生かして本社を含めた体制を構築しつつ，自社のデジタル製品での欧州市場投入品をリストアップし，該当製品に対して次に挙げる欧州CRAの主な要件への対応を検討している。

⑴　SBOM対応

SBOM(Software Bill of Materials)とはソフトウエア部品表のことで，製品に含まれるOSS(Open Source Software)等のソフトウエア・コンポーネントや，その依存関係をリスト化したものである。SBOMを活用すればサプライチェーンに潜む脆弱性リスクの可視化が可能である。

⑵　報告義務対応，脆弱性修正対応

インシデントや脆弱性情報を一元管理するとともに，ENISAへの報告体制や，製品やサービスへの脆弱性対応を迅速に行える開発体制が必要である。

⑶　製品及び開発プロセスのへの対応

コンポーネントに関するセキュアな製品開発のプロセスやライフサイクル全体でのセキュリティー対応プロセスを規定したIEC 62443-4-1や，産業制御システム向けセキュリティー技術要件であるIEC 62443-4-2等が有力な規格候補として挙がっている。

これら以外も多くの要件があるため，注意が必要である。また，欧州CRA公布後も具体的な適合性評価方法などの準拠すべき整合規格や，関連法令(AI規則案，機械規則，無線指令など)への影響など，不確定要素も多いため，施行開始までは引き続き情報収集に努める必要がある。

4．今後の課題と対応

欧州では欧州CRA以外にもAI規則案，データ法，デジタル製品パスポート等，また中国や米国などでも欧州同様のサイバー関連の法令規格の新設や強化が検討されている。中国CS法など一部は既に施行され始めているが，罰則が科される猶予期間も含めて考えると，その多くが2030年頃までに順次対応が求められる状況にある。

しかしながら**2章**や**3章**で述べた対応事例は決して順調に進んだわけではない。新たなサイバー関連の法令規格ということに加えて，各国や地域で個別の対応が必要であり，該当製品の担当部門だけで情報収集し，対応するには能力的にもリソース的にも不足した状況であった。

そこで情報を入手した筆者所属部門で，該当する法令規格を正しく解釈をするために，公開された海外のWebサイトを調査し，不明点は調査会社やコンサルタントを活用し情報を収集した。また，海外拠点や販売店，海外業界団体などへ調査協力を依頼した。同時に社内の関係者も多岐にわたったため，各関係部門を集めて定期的に打合せをするなど周囲を粘り強く説得した結果，中国CS法や欧州CRAに関しては継続的に相談や対応ができる推進部門と担当者が明確化された。

他のサイバー関連の法令規格に関しても同様な体制が必要であり，特にAIなどではデジタル技術の要素が異なるため，同じ体制では推進できない課題がある。

この課題に対して，例えば市場投入する海外拠点や販売拠点から現地のサイバー関連の法令規格情報を入手し，それだけではなく社内でも伝達の途中で情報が途切れることなく末端の設計者にまで情報が届くように，法令規格に関する一元管理や，役割を明確にしたリソースの確保が必要である。

また，欧州JBCEやJETROなど海外で活動している産業関連団体や，政府機関との情報共有体制を構築し，得られた情報から海外市場投入済み製品の変更要否，市場投入継続時の費用(脆弱性発見時の対応)など，ビジネス影響度を調べ，場合によっては市場投入を中止する等の判断が必要である(**図2**)。

総じて，従来のフィジカル関連の法令規格体制をサイバー関連の法令規格へも対応できる体制に強化することや，サイバー関連に精通した人材の育成と強化が必要である。これは日本企業の多くが解決すべき共通課題である。

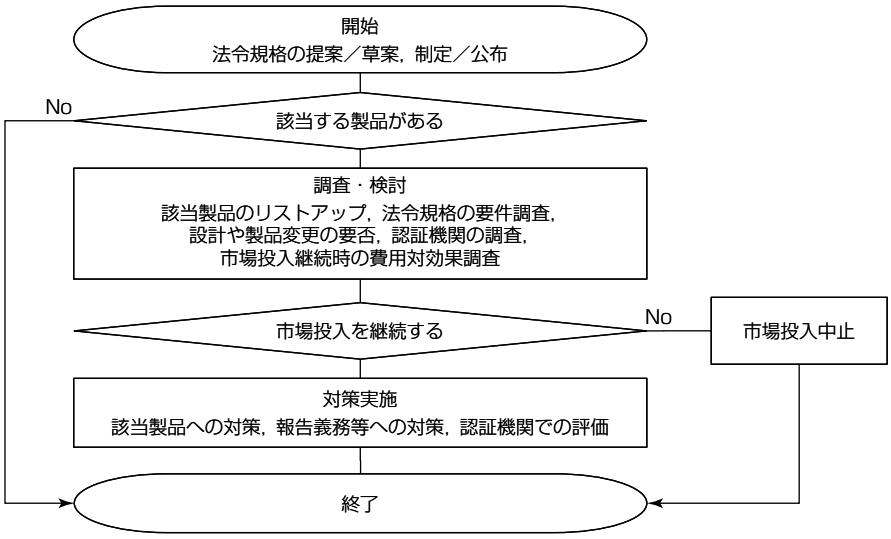


図２−法令規格対応のフローチャート

5. む　す　び

世界規模で様々な変革が進む中，近年の地政学的・経済学的な課題からディグローバリゼーション化が進み，中国CS法や欧州CRA，そして今後はAI規則案，データ法，デジタル製品パスポートなど，サイバー関連の法令規格や要件の新設や強化が検討されている。

海外へ製品を市場投入する企業の経営者や管理者は，このような変化に対応するために，あらかじめ適切な人員を配置し，人材育成を強化するとともに組織的な体制を構築することが急務と言える。

各国や地域のサイバー関連の法令規格に迅速かつ真摯に取り組むことで，製造変革やビジネスモデル変革，社会変革など様々な変革に人的かつ組織的に適応できるようになるため，企業競争力の底上げにつながる。本稿がその一助になれば幸いである。

参 考 文 献

(1)　三菱電機PSIRT
https://www.MitsubishiElectric.co.jp/psirt/
(2)　JBCE(Japan Business Council in Europe)
https://www.jbce.org/ja/