特集

経済安全保障に向けたセキュリティ・アシュアランス
～信頼の基盤構築のためのアプローチ～

編集にあたって

石黒正揮 | （株）三菱総合研究所
竹之内隆夫 | LINE ヤフー（株）☆1
手塚　悟 | 慶應義塾大学

米中対立の深刻化，ウクライナ情勢の悪化などの国際情勢の変化に伴い各国および国家間の経済安全保障にかかわる政策検討が加速している．米国防総省では，「サイバー空間」を陸・海・空・宇宙空間に次ぐ「第五の戦場」であると定義しており，国家が背後にいるサイバー攻撃について，脅威となる国家を特定した上で，名指しで非難する取り組み（パブリック・アトリビューション）を強化している．また，サイバー攻撃により，サプライチェーンを通じた企業に波及し大きな被害をもたらす事故が増加している．たとえば，国内では，基幹産業である自動車メーカーの工場が停止するなどの事故が発生している．また，海外では，電力，石油化学プラントなど重要インフラに対するサイバー攻撃による実経済に大きな被害をもたらす事故が増加している．

サイバー攻撃は，国家間の対立において真っ先に利用されるケースが増加しており，経済安全保障を確保する上でサイバーセキュリティが重要になっている．

このような情勢のもと各国において経済安全保障にかかわる法制度の整備や外交を通じた国家間の戦略的対話が活発化している．日米豪印戦略対話（QUAD：Quadrilateral Security Dialogue）においては，インド太平洋地域におけるサイバーセキュリティを確保するための共同原則として，政府調達においてセキュア・ソフトウェア開発の共通的な枠組みを導入することに合意している．

グローバル化した世界経済においては，経済安全保障を一国で確保することは困難であり，友好国による国際ルールの整合化が必要となる．このような国際ルールへの整合化の立ち遅れは，友好国との経済安全保障の障害となりかねない．たとえば，主要先進国においては，国家機密等を扱う職員に対して，その適格性を審査するセキュリティ・クリアランス制度が整備されているが，これまで日本では制度化されておらず，経済安全保障上の障害となることから法制度化が行われた．

☆1　2024 年 7 月 1 日より（株）Acompany

さらに，国際規範やルールへの対応においては，国家間の信頼の構築が重要になる．そのためには，グローバル・スタンダードに則り，エビデンスと論証に基づく説明責任（アカウンタビリティ）を果たすことにより信頼を構築することが求められる．このようなセキュリティに関するエビデンスと論証に基づき信頼を付与することをセキュリティ・アシュアランスと呼ぶ．米国防総省の調達規則 DFARS[☆2] においては，日本企業を含む国内外の契約企業やサプライヤーに対して NIST が定めたセキュリティ基準「NIST SP800-171」を義務化している．

このような経済安全保障にかかわる国際情勢を踏まえて，本特集では，以下のような観点に注目し，経済安全保障を確保する上でサイバーセキュリティにかかわる重要な取り組み動向，今後の課題や展望についてまとめることとした．

- **友好国による国際ルールの整合化**
  友好国とのグローバルな経済取引を維持するために，友好国と国際ルールの整合化の方向性を見据えたサイバーセキュリティの取り組みが求められる．（第 1 章，第 2 章，第 3 章）
- **アカウンタビリティの確保**
  友好国から信頼されるためには，グローバルに受け入れられる合理性に基づく説明責任（アカウンタビリティ）を果たすことが求められる．サイバーセキュリティ自体の向上とアカウンタビリティの向上は，必ずしも一致しない．合理的な説明責任が不十分であれば友好国による経済安全保障の枠組みから外されるリスクがある．（第 3 章，第 4 章，第 5 章）
- **トラストの基盤構築**
  信頼を構築する基盤として，製品やサービスのセキュリティだけでなく，サイバー空間上で信頼できる企業や人などの主体の認証と信頼のネットワークを構築する仕組みが重要になる．（第 1 章，第 5 章）

以上のような観点を実現するためは，国家間の調整，制度構築，グローバルなサプライチェーンを通じた基盤や枠組みの構築が必要になる．このようなことから，本特集では，サイバーセキュリティにかかわる政策，技術，組織の国際動向に詳しい専門家により幅広い視点をカバーしつつ，最新の具体的な動向から今後の課題や展望についてとりまとめた．

経済安全保障については，近年の地政学リスクの変化に伴い急速に法制度の検討が進められている．これに対応したサイバーセキュリティの制度検討や国際整合化は重要な課題となっている．本特集を通じて，経済安全保障に向けたサイバーセキュリティにかかわる問題認識や目指す方向性を提示することで，国や企業等における今後の取り組みの検討につながれば幸いである．

（2024 年 6 月 8 日）

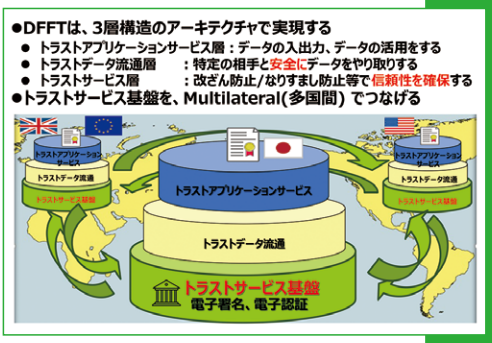
☆2 Defense Federal Acquisition Regulation Supplement

概要

1 国家安全保障・経済安全保障・社会保障におけるサイバーセキュリティ戦略
―国際相互認証を踏まえたデジタルトラストの必要性―

手塚　悟　慶應義塾大学

国家安全保障・経済安全保障・社会保障におけるサイバーセキュリティ戦略において，特に国際相互認証を踏まえたデジタルトラストの必要性について解説した．昨今のデジタルトレードの進展により，国際間におけるデータのやりとりにおいて，なりすましや改ざんの問題がきわめて深刻である．この問題を解決するために，国際相互認証の方法論と3層構造アーキテクチャを示すことで安心安全なデジタルトラストのサイバー空間を構築することができる．



2 経済安全保障におけるサイバーセキュリティにかかわる課題と展望
―国際規範・枠組みを見据えたサイバーセキュリティのニューノーマル―

石黒正揮　（株）三菱総合研究所

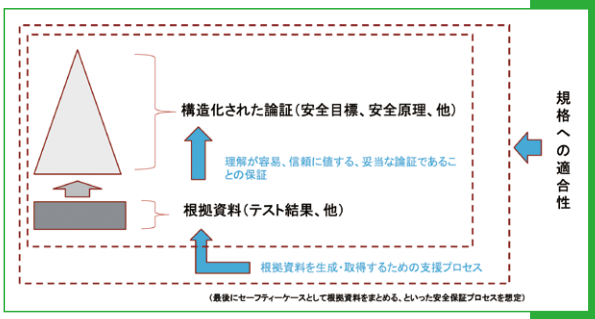
米中対立の深刻化，ロシアのウクライナ侵攻などに伴い経済と安全保障にかかわる地政学リスクの高まりとともに，サイバーセキュリティにかかわる攻撃や事故が拡大している．経済安全保障推進法の4本柱は，いずれもサイバーセキュリティと関係が深い．これら動向を踏まえて，今後，(1) 国際規範を見据えたサイバーセキュリティ，(2) コストを考慮したデリスキリング，(3) 脅威・脆弱性の統合インテリジェンスなどの取り組みが重要になることを示す．

概要

3 国際標準とアシュアランスケースの取組み

田口研治 | UL Solution

国際標準においては，さまざまなアシュアランスケースが安全性やセキュリティに関する保証のために利用されている．安全性の保証にはセーフティケースが安全の論証や認証のための根拠資料として利用されている．本稿では，セーフティケースついて正しく理解するための歴史的背景，モデリング記法，最新の動向として自動運転車や人工知能・機械学習の安全性に対するアプローチを紹介することで，全体的な概要を説明する．



4 セキュリティ・アシュアランスとソフトウェア・サプライチェーン・リスク管理

松岡正人 | 日本シノプシス合同会社

ソフトウェア・サプライチェーン・リスク管理はソフトウェアに起因するビジネス上のリスクを低減するための新たなアプローチとして，2021 年の EO14028 以来，FDA，EU などによる新しい規制，法律，ルールに採用された．ソフトウェアの不具合，欠陥，脆弱性に起因する障害や事故，対策について，米国を例に時系列で振り返り，どのような状況や事由によってソフトウェア・サプライチェーン・リスク管理が登場することとなったのか考察してみる．

5 経済安全保障に向けたソフトウェアサプライチェーンセキュリティの重要性

美崎敦也　富田佑実 | サイバートラスト（株）

近年，取引相手などのステークホルダーについて組織，システム，製品，サービス，データ等に関するセキュリティを客観的，合理的に確保するための仕組みとしてサプライチェーンセキュリティが強く求められている．サプライチェーンセキュリティを行うための手法として，古くから利用されている SCAP と近年，注目を集める SBOM を比較しそれぞれの特徴について解説する．