表：サプライチェーンサイバーリスクに関する主要ガイドライン一覧（ITに関するもの）

（2019年12月）

1.国内外で発行されている、重要インフラ産業・大企業の調達活動（主として委託）を想定した文書

国名	文書名	現行版発行日	発行元	対象と概要	URL
日本	サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）v1.0	2019年4月18日	経済産業省	民間事業者向け。リスク源の洗い出しや企業等におけるセキュリティポリシーの策定及び対策の実装等を規定	https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html
日本	サイバーセキュリティ経営ガイドラインv2.0	2017年11月16日	経済産業省、情報処理推進機構	経営者向け。経営者が認識すべき3原則のひとつにサプライチェーンのセキュリティ対策、サイバーセキュリティ経営の重要10項目に「ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握」を盛り込む	https://www.meti.go.jp/policy/netsecurity/mng_guide.html
日本	情報セキュリティポリシーサンプル改版（1.0版）	2016年3月29日	日本ネットワークセキュリティ協会	情報セキュリティポリシーのサンプル。文書03に外部委託先管理規程を収録	https://www.jnsa.org/result/2016/policy/
日本	アウトソーシングに関する情報セキュリティ対策ガイダンス	2009年6月1日	経済産業省	アウトソーシングにおける情報セキュリティリスクと管理策、チェックシートで構成。全社的なアウトソーシング戦略に基づいたリスク管理体制の構築を重視	https://www.meti.go.jp/policy/netsecurity/docs/secgov/2009_OutsourcingJohoSecurityTaisakuGuidance.pdf
米国	Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force Interim Report	2019年9月18日	Cybersecurity and Infrastructure Security Agency	重要インフラ産業が依存するインフラという観点からICTをとらえ、ICTサプライチェーンリスク管理の要点を議論した結果の中間整理。主に5Gを念頭においたもの	https://www.cisa.gov/publication/ict-scrm-task-force-interim-report
米国	NIST Special Publication 800-37 Rev.2 Risk Management Framework for Information Systems and Organizations	2018年12月20日	National Institute of Standards and Technology	全業種対象のリスク管理フレームワークで、情報セキュリティ管理策を含む。Rev2でサプライチェーンリスク管理が盛り込まれた	https://doi.org/10.6028/NIST.SP.800-37r2
米国	NIST SP800-171 Rev.1 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	2018年6月7日	National Institute of Standards and Technology	米国連邦政府以外の防衛調達関連事業者が対象。システムや組織にCUI（非機密区分の重要情報）が存在する場合に、機密性を確保するための推奨セキュリティ要件。2019年6月にRev.2ドラフトが公開された	https://doi.org/10.6028/NIST.SP.800-171r1
米国	Framework for Improving Critical Infrastructure Cybersecurity Version 1.1	2018年4月16日	National Institute of Standards and Technology	重要インフラ組織が対象。サイバーセキュリティリスクの管理・削減のための標準、ガイドライン、慣行に基づくガイダンス。特にID.BE（事業環境）とID.SC（サプライチェーンリスク管理）がサプライチェーンリスクの管理項目を規定する	https://www.nist.gov/cyberframework/framework
米国	Cloud Computing Security Requirement Guide v1r3	2017年5月6日	Defense Information Systems Agency	米国国防省のクラウドサービス調達に関するセキュリティ要件。FedRAMPに独自の要件項目を追加	https://rmf.org/wp-content/uploads/2018/05/Cloud_Computing_SRG_v1r3.pdf
米国	NIST SP800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations	2015年4月9日	National Institute of Standards and Technology	連邦政府組織に対するICTサプライチェーンリスク管理策。付録には脅威事象（Appendix C）や脅威シナリオと分析枠組（Appendix D）を収録	https://doi.org/10.6028/NIST.SP.800-161
米国	Third-Party Relationships: Risk Management Guidance	2013年10月30日	Office of the Comptroller of the Currency	米国の中央銀行と連邦金融機関向け。発注時の委託先選択、契約管理、継続的モニタリング、独立したレビュー等を要件として挙げている	https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html
米国	Federal Risk and Authorization Management Program	2011年12月8日	General Services Administration	クラウド製品・サービスが対象の認証プログラム。NIST 800-53で定められた標準に適合するサービスプロバイダを認証する。クラウド製品・サービスのセキュリティ水準評価や認証、継続的モニタリングを規定	https://www.fedramp.gov/documents/
EU	Good Practices for Security of Internet of Things in the context of Smart Manufacturing	2018年11月19日	European Union Agency for Cybersecurity	製造業のIoTが対象。インダストリー4.0とスマートマニュファクチャリング実現におけるセキュリティ事項。サプライチェーン全体におけるセキュリティは特にEndpoints Lifecycle、Training and Awareness、Third Party Managementに記載あり	https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot
EU	Directive on security of network and information systems (NIS Directive)	2016年7月6日	European Commission	EU域内における通信インフラ、情報システムのセキュリティレベル向上と連携を目的として整備された。14原則のひとつとしてサプライチェーンを挙げ、各国の制度整備を求めた	https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
EU	Cloud Computing: Benefits, risks and recommendations for information security Rev.B	2012年12月1日	European Union Agency for Cybersecurity	クラウドコンピューティングサービス利用者向け。サプライチェーンにおける障害を取り上げた章では、クラウドサービス事業者が調達するサービス等の停止が連鎖的影響を及ぼす可能性を指摘している	https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security
英国	NCSC Cyber Assessment Framework	2019年9月30日	National Cyber Secuity Centre	英国におけるNIS Directiveの制度化を目的として整備された。Objective A（セキュリティリスク管理）でサプライチェーンを考慮	https://www.ncsc.gov.uk/blog-post/the-cyber-assessment-framework-3-0
英国	Supply chain security guidance	2018年1月28日	National Cyber Secuity Centre	大企業、重要インフラ、公共サービス組織向けに、サプライチェーンセキュリティ向上に資するプロセス12項目とサプライチェーン攻撃事例、評価項目等をまとめたもの	https://www.ncsc.gov.uk/collection/supply-chain-security
オーストラリア	Cyber Supply Chain Risk Management	2019年11月6日	Australian Cyber Secuity Centre	全組織を対象に、サイバーサプライチェーンリスク管理施策リストを提供。契約内容（例：業務委託、MSP、CSP等）ごとに実践ガイドあり	https://www.cyber.gov.au/publications/cyber-supply-chain-risk-management
団体	COBIT 2019	2018年11月13日	ISACA/IT Governance Institute	業種を限定しないITガバナンスフレームワーク。成熟度モデルを採用。APO13: Manage Security、DSS05: Manage Security Servicesがサプライチェーンサイバーセキュリティ管理を扱う	http://www.isaca.org/COBIT/Pages/COBIT-5-japanese.aspx
団体	CSA Security Guidance for Critical Areas of Focus in Cloud Computing v4.0	2018年11月9日	Cloud Security Alliance	クラウドコンピューティングサービスの提供者、利用者向け。のセキュリティガイダンス。双方に対し、契約による合意や定期的報告等を実施することなどを推奨する	https://cloudsecurityalliance.org/research/guidance/
団体	Payment Card Industry Data Security Standard ver3.2.1	2018年5月21日	PCI Security Standards Council	カード決済データの取り扱いや伝送などのセキュリティ管理基準。「要件 12: セキュリティポリシー」に委託内容確認の契約管理面からの要件が記載されている	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_2_1_JA-JP.pdf
団体	ISF The Standard of Good Practice for Information Security 2018	2018年3月23日	Information Security Forum	（会員組織のみ入手可能）企業の情報セキュリティ管理策をまとめたもの。サプライチェーンに関する章では、サプライヤ管理とアウトソーシング、クラウドコンピューティングの管理策を示す	（会員組織のみ入手可能）
団体	ISO/IEC/IEEE 15288:2015 Systems and software engineering — System life cycle processes	2015年5月15日	ISO/IEC/IEEE	システムライフサイクル管理用の標準。ハードウェア、ソフトウェア、データ、人間、プロセス、手順、施設、材料等の管理を含む	https://www.iso.org/standard/63711.html
団体	ISO/IEC 27036-3:2013 Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security	2013年11月15日	International Organization for Standardization/International Electrotechnical Commission	ICTサプライチェーンの製品・サービスの調達、供給が対象。管理策ではISO/IEC 15288、ISO/IEC 12207、ISO/IEC 27002を使用する	https://www.iso.org/standard/59688.html
団体	ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements	2013年10月1日	International Organization for Standardization/International Electrotechnical Commission	情報セキュリティマネジメントシステム構築、運用に関する規格。A.15供給者管理にサービス提供元、業務委託先の管理（選定方針、契約管理）が記載されている。クラウドコンピューティングサービス提供・利用に関する管理策からなるアドオン認証ISO/IEC 27017が存在する	https://www.iso.org/isoiec-27001-information-security.html
団体	ISO 28000:2007 Specification for security management systems for the supply chain	2007年9月15日	International Organization for Standardization	物流を中心とするサプライチェーンセキュリティ管理の検討項目群。サイバー空間に由来する脅威も考慮することを求めている	https://www.iso.org/standard/44641.html

表：サプライチェーンサイバーリスクに関する主要ガイドライン一覧（ITに関するもの）

2.国内で発行されている、受託者あるいは中小企業の事業活動を想定した文書

国名	文書名	現行版発行日	発行元	対象と概要	URL
日本	中小企業の情報セキュリティ対策ガイドライン第3版	2019年12月19日	情報処理推進機構	中小企業と個人事業者が対象。情報セキュリティ対策に取り組む際の、(1)経営者が認識し実施すべき指針、（2）社内の対策手順を紹介している。付録に 「リスク分析シート」「中小企業のためのクラウドサービス安全利用の手引き」など	https://www.ipa.go.jp/security/keihatsu/sme/guideline/
日本	SECURITY ACTION	2017年4月28日	情報処理推進機構	中小企業の情報セキュリティ対策ガイドライン付録への取り組みと情報開示を二階層に区分。企業は付録記載内容に沿って情報セキュリティ対策の取り組み水準を自己宣言する	https://www.ipa.go.jp/security/security-action/sa/index.html
日本	情報サービス産業における適正な業務委託契約運用のためのガイドライン	2016年3月29日	情報サービス産業協会	業務委託契約に関する注意点をまとめたもの。受委託者間のセキュリティレベルの相違も考慮している	https://www.jisa.or.jp/Portals/0/report/jisa_entrust_guideline201603.pdf