経済産業省 御中

令和２年度
サイバー・フィジカル・セキュリティ対策促進事業
（サプライチェーン・セキュリティ対策に関する調査）
報告書

2021 年 3 月 12 日

株式会社三菱総合研究所
デジタル・イノベーション本部

目 次

1. 背景・目的 1

1.1 背景 1

1.2 目的 1

2. サプライチェーン上の取引先に求めるセキュリティ要件に関する調査 2

2.1 国内企業が取引先に求めるセキュリティ要件 2

2.2 海外での議論の把握 9

3. サプライチェーンを支える基盤インフラ技術に関する調査 19

3.1 基盤インフラ技術の最新動向 19

3.2 基盤インフラ技術に関して求められる政策の検討 36

4. サプライチェーン・セキュリティに関する国内外の法令・政策等に関する調査 44

4.1 調査概要 44

4.2 ランサムウェアによる被害の実情及び支払いの可否に対する議論の動向、その他の対応における注目すべき事案 44

4.3 脅威インテリジェンスサービスにおける注意すべき法令上の問題についての調査 54

4.4 情報セキュリティサービス提供者と法執行機関・監督官庁などとの協力 84

図 目 次

図 2-1　サプライチェーンマネジメント（SCM）とエンジニアリングチェーンマネジメント（ECM）.....6
図 2-2　ICT Supply Chain Risk Management タスクフォースの沿革.....11
図 2-3　ICT Supply Chain Risk Management タスクフォースの主な取組・構成組織....12
図 2-4　サプライチェーンリスクに対するタスクフォースの推奨事項.....15
図 2-5　スコアカード方式（例）.....16
図 2-6　CPIC 認証と EDSA 認証の違い.....16
図 2-7　ICT SCRM WG2 における脅威分類とスコアカード評価項目案の比較.....17
図 2-8　CPSF とスコアカード評価項目案の比較.....18
図 3-1　基盤インフラの範囲.....19
図 3-2　検討の方向性①アーキテクチャとアプリケーションのイメージ.....20
図 3-3　検討の方向性②スーパーシティの想定.....20
図 3-4　スーパーシティ全体のアーキテクチャ例.....34
図 3-5　スーパーシティ（電力）のアーキテクチャ例.....34
図 3-6　スーパーシティ（スマートファクトリー）のアーキテクチャ例.....35
図 3-7　スーパーシティ（自動車）のアーキテクチャ例.....35
図 3-8　基盤インフラ技術研究開発のスコープ.....38

表 目 次

表 2-1　評価項目の体系 2
表 2-2　CPSF と評価項目の関係 3
表 2-3　CPSF と評価項目の関係 3
表 2-4　評価項目案に対するご意見 5
表 2-5　詳細評価項目（案） 7
表 2-7　「Charter of Trust」10 の原則 9
表 2-8　ICT SCRM タスクフォース　4 つの WG 概要 13
表 2-9　ICT SCRM タスクフォース　各 WG の成果と今後の取組方針 14
表 3-1　「基盤インフラに関する勉強会」構成員 21
表 3-2　プレ会合　開催概要 22
表 3-3　第 2 回勉強会　開催概要 22
表 3-4　プレヒアリング結果 24
表 3-5　ヒアリング結果 27

1. 背景・目的

1.1 背景

我が国では、サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会「Society5.0」の実現を提唱している。

「Society5.0」では、データの流通・活用を含む、より柔軟で動的なサプライチェーンを構成することが可能。一方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という新たなリスクへの対応が必要。2019 年にフランスで開催された G7 ビアリッツ・サミットの首脳宣言においても、「我々は、5G ネットワーク及びサプライチェーンにおけるセキュリティの脆弱性により引き起こされる脅威に対処する必要性につき一致している。」とされている。

1.2 目的

本事業では、このように複雑化するグローバルなサプライチェーン全体でのセキュリティ確保に向けて必要となる施策や各国動向等について調査を実施した。

具体的には、以下の項目について調査を行った。

- サプライチェーン上の取引先に求めるセキュリティ要件に関する調査
- サプライチェーンを支える基盤インフラ技術に関する調査
- サプライチェーン・セキュリティに関する国内外の法令・政策等に関する調査

2. サプライチェーン上の取引先に求めるセキュリティ要件に関する調査

2.1 国内企業が取引先に求めるセキュリティ要件

企業が取引先に求めるセキュリティ要件についてとりまとめた。

具体的には、取引先の組織のセキュリティマネジメントの確認、取引を行う製品等のセキュリティ機能の確認、取引を行う製品等がセキュアに開発されているかどうかの確認等、確認項目には取引先に求めるの視点を含めた。

なお、本検討については、ロボット革命イニシアティブ「IoT による製造ビジネス変革 WG 産業セキュリティ AG」と連携して実施した。

2.1.1 セキュリティ評価項目試案

令和元年度の経済産業省委託事業において、「The Cyber Product International Certification（CPIC）」における評価項目試案がまとめられている。この評価項目の体系を活用し、サプライチェーンの観点で必要な要素を洗い出し、取引先に求めるセキュリティ要件を検討した。

表 2-1　評価項目の体系

評価項目					評価対象	スコアカードによる評価		
						標準的	低リスク（組織）	低リスク（機器）
大項目（評価の枠組）		中項目（想定される脅威）	中項目（期待される対策概要）	小項目（具体的対策の例）	該当／対象外	セルフアセスメント	第三者認証／外部監査	ペネトレーションテストの実施等
① 全体（組織の管理体制）	電力関連機器ベンダの組織全体におけるセキュリティガバナンス	・機器に関連する情報資産の侵害（漏えい/改ざん/破壊/利用停止等）	・経営層の責任と方針の明示 ・組織的リスクマネジメントに基づく情報保護 ・関連会社を含めた統制	組織全体のセキュリティポリシーが文書化されている			ISMS/CSMS等により代替保証	
				組織のセキュリティ対策が、リスク分析に基づき継続的に改善されている				
				組織の保有する情報資産を一覧化し、記録及び管理をしている				
				組織が開発及び保守するシステムにおいて、統一的に守られるべきセキュリティ規則が定められている				
		・関連法規等への違反（業法・地域規制、プライバシー法規等）	・教育の実施によるミスの防止 ・内部不正の抑止	組織内の人員及び関係者の役割・責任等が定められ、周知と教育が実施されている				
				組織内の人員及び関係者のIDとアクセス制限が管理され、ログを検証されている				

評価項目については、以下の考え方で整理した。

- カテゴリ毎のセキュリティ目標に対する想定脅威の概要と期待される対策を整理
- 特に、製品・機器に関する脅威に着目し、カテゴリに関する議論を行いやすい粒度を意識
- 小項目は中項目を細分化する形で参考情報として記載（動的に変遷する前提）

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）との対応関係を見ると、基本コンセプトの違いとして、サプライチェーン全体のサイバーセキュリティ対策を対象とするCPSFに対し、スコアカード案は製品・サービスの評価を対象としている。

CPSF（第Ⅲ部）におけるサプライチェーン（SC）項目は、調達元組織が複数の調達先を評価する目的で利用するが、スコアカード案は、製品・サービス提供元（調達先）が、複数の調達元へ説明する目的で利用する。

表 2-2　CPSF と評価項目の関係

ID	要求事項	スコアカード案との対応関係
CPS.SC-1	取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する。	直接の対応関係なし（メタ要求に該当）。調達元の基準において、製品・サービスセキュリティ品質基準、責任範囲を合意するためにスコアカードを活用可能と考えられる。
CPS.SC-2	自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	直接の対応関係なし（メタ要求に該当）。重要業務で用いると判断された製品・サービスを評価する際の基準としてスコアカード案が活用されること等が考えられる。
CPS.SC-3	外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	間接的に対応。製品に係る組織的対策は「①全体（組織）」でスコアカード項目案においても評価されている。
CPS.SC-4	外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する**他組織の提供する製品・サービスが適合していることを確認**する。	最も直接的な対応関係がある。適合性の確認のためにスコアカードを用いることが可能。ただし、スコアカード案は、製品に係る周辺プロセスまでを対象とし、間接的に他項目の評価を含む。直接的には、「③製品セキュリティ」が該当。
CPS.SC-5	取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	間接的に対応。製品に係る人員及び関係者の役割等（①全体（組織））や、製造設備の要員管理等（⑦工場セキュリティ）に対応。
CPS.SC-6	取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	間接的に対応。製品のテスト（②ECM）等。監査は、実施済であれば当該項目のスコアが好評価になる。他の形式の評価の一種としてスコアが該当すると考えられる。
CPS.SC-7	取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	直接の対応関係なし（メタ要求に該当）。スコアが不正（虚偽のセルフアセスメント等）であった場合に、評価組織からのペナルティ制度を運営するような場合に該当。
CPS.SC-8	自組織が、関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報(データ)を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	間接的に対応。製品に係るSLAの明示、文書の開示等（⑤SCM上流）。
CPS.SC-9	サプライチェーンにおけるインシデント対応活動を確実にするために、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。	間接的に対応。製品に係る脆弱性対応、パッチ配信等（⑥SCM下流）。
CPS.SC-10	取引先等の関係する他組織との契約が終了する際(例：契約期間の満了、サポートの終了)に実施すべきプロシージャを策定し、運用する。	間接的に対応。製品に係るSLAの明示（⑤SCM上流）、廃棄手順・サービス終了条件等（⑥SCM下流）
CPS.SC-11	サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する。	直接の対応関係なし（メタ要求に該当）。各組織のスコアカード利用方針や、スコアカード方式自体の継続的改善等に関係。

出所：”Threat Evaluation Working Group: Threat Scenarios”
https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report_0.pdf
（2021 年 3 月 10 日閲覧）を基に三菱総合研究所作成

表 2-3　CPSF と評価項目の関係

脅威カテゴリ	代表的な脅威の例	スコアカード評価項目案との比較
1. 偽造部品	偽造製品の流通・利用、偽造部品（HW/SW）の製品への組込み、配送過程での不正改ざん、偽造証明書、偽造サイト等。	偽造品が出回る脅威そのものは、項目案の脅威には直接対応しない。偽造部品の組込みは「⑦工場セキュリティ（製造工程）」、「⑥SCM下流（配送過程での不正改ざん）」に該当する。
2. サイバーセキュリティ	情報の漏えい、改ざん、不正アクセス・マルウェア被害等。ベンダからの情報漏えい、サプライヤ内での不正機能埋め込み等。	大半の項目案は本カテゴリに属する。範囲が多岐にわたり、①～⑦の要素を含む。機器とサービスの双方を対象としている。その他の要素として、社内情報システムを対象とした情報収集を含む。
3. 内部セキュリティの運用と管理	知識の欠如・教育の不足や、情報の管理運用不備（廃棄含む）、不十分なパスワード設定・アクセス制御等。	「①全体（組織）」の管理体制に該当する脅威が多く含まれる。製品の廃棄等の視点からは、「⑥SCM下流」にも一部該当すると見なせる。
4.システム開発ライフサイクル・プロセス・ツールに対する攻撃	マルウェアの混入、コンポーネントの開発段階における不正、リポジトリの操作、更新・配布機構の操作、OSSの脆弱性、海外製コンピュータ等。	「②ECM」「③開発環境」に該当する脅威が多く含まれる。組み込み機器関連の脅威は「⑦工場セキュリティ（製造プロセス）」にも関係する。
5. 内部脅威	内部不正やスパイの侵入、修理・メンテナンス中の改ざん等。	原則として「①全体（組織）」の内部不正に該当。ICT SCRMの分類はかなり細かいが、必要な対策は大きく変わらないものと見られる。
6. 経済的リスク	サプライヤの財務リスク、破綻・買収リスク、品質リスク、ロックインリスク、サプライヤー外部からの意思決定への関与、ずさんな管理に関する問題等。	項目案では該当する脅威を含めていない。サプライチェーンに関する企業経営リスク等を整理したものであり、サイバーリスクではない。
7. サプライチェーン固有のリスク	部品・材料の脆弱性を継承、サプライチェーン内の不正・改ざん、サプライチェーン構造の深さ、トレーサビリティの欠如、輸送・出荷中の改ざん、コンプラ違反、各レベルの品質保証不足、不十分な検品、情報開示・検査権限の不足等。	「⑥SCM上流」に該当するサプライヤからの調達プロセスに関する脅威を中心に、「③開発環境」「⑦工場セキュリティ」の範囲まで言及。サイバーに限定せずサプライチェーンの構造的問題にまで切り込んでいる。
8. 法的リスク	知財・ライセンス（国際的係争を含む）、消費者・中小企業からの訴訟リスク、個人情報、コンプライアンス、犯罪への関与、制裁違反等。	範囲としては「①全体（組織）」に該当するものだが、ICT SCRMは分類がかなり細かい。エンティティリストに言及している点も特徴。
9. 外的サプライチェーンリスク	自然災害、地政学的リスク、労働問題、国際貿易問題、ガバナンスの問題、OSSにおける国際的貢献度の低下等。	サプライチェーン全体へ混乱を与える脅威であり、直接的なサイバーリスクではない。項目案とも直接対応はしない。

①：全体　②：ECM　③：開発環境　④：製品・サービス　⑤：SCM上流　⑥：SCM下流　⑦：工場セキュリティ

洗い出した評価項目については関係者の意見を踏まえて見直しを行った。

現状、具体的な項目を定めているケースは少ないが、今後の項目策定に関してはニーズもあると考えられた。ただし、製品・サービスそのものの要件をどこまで定めるかは要検討である。

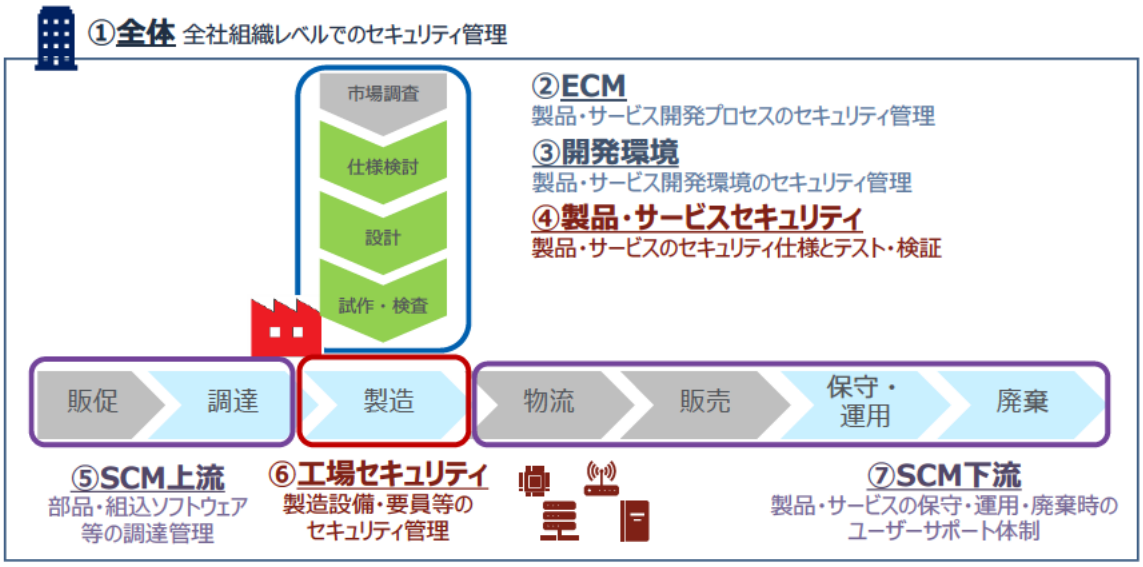
表 2-4　評価項目案に対するご意見

	(1) サプライヤーへの要件に既に記載されている項目	(2) 今はまだ記載されていないが、今後は記載したがよいと思われる項目
A社	① 全体(組織の管理体制)に関する3項目	③ 製品セキュリティ（製品：一般）以外の23項目
B社	●製品、委託開発物の調達先 管理体制に関する要求事項（①⑥）32項目 製品・委託開発物に対する要求事項（④）11項目 ●運用サービス委託先 管理体制に関する要求事項（①⑥）32項目 委託サービスに関する要求事項（③）12項目	－
C社	●CSRへの取組において以下項目の調査を依頼 1)人権・労働、2)安全衛生、3)公正・倫理、 4)安全・品質、5)情報セキュリティ、 6)マネジメントシステム、7)社会貢献 ●情報セキュリティに関する項目は以下の通り。 コンピュータウィルスやサイバーアタックの防護策を講じているか？ 個人情報を適切に管理し、情報漏洩防止に取り組んでいるか？ 適切な機密情報管理を実施しているか。	・ISMSによる情報セキュリティ管理が有効性の認識から、「スコアカード方式」の項目においても、IEC 62443-2-1に該当する項目具体的な候補。 ・脆弱性ハンドリング体制（情報開示、パッチ適用等）へのニーズも高まっている。
D社	・標準的な要求項目についてはカバー済み ・事業ごとに要求レベルが異なる箇所についてはカバーしていない箇所もあり、要検討	特になし

サプライチェーンの観点で必要な要素については、「サプライチェーンマネジメント（Supply Chain Management：SCM）」及び「エンジニアリングチェーンマネジメント（Engineering Chain Management：ECM）」の考え方を用いて、以下の項目を洗い出した。

① 全体（全社組織レベルでのセキュリティ管理）
② ECM（製品・サービス開発プロセスのセキュリティ管理）
③ 開発環境（製品・サービス開発環境のセキュリティ管理）
④ 製品・サービスのセキュリティ（製品・サービスのセキュリティ仕様とテスト・検証）
⑤ SCM 上流（部品・組込ソフトウェア等の調達管理）
⑥ 工場セキュリティ（製造設備・要員等のセキュリティ管理）
⑦ SCM 下流（製品・サービスの保守・運用、廃棄時のユーザサポート体制）

なお、上記の整理については、検討の結果、サービスにも適用可能であるとして、製品及びサービスにおける SCM 及び ECM としてとりまとめた。



出所：「IoT による製造ビジネス変革 WG 産業セキュリティ AG」資料を基に三菱総合研究所修正

図 2-1 サプライチェーンマネジメント（SCM）とエンジニアリングチェーンマネジメント（ECM）

表 2-5　詳細評価項目（案）

評価項目					評価対象	スコアカードによる評価			他の評価基準との対応							
						標準的	低リスク（初期）	低リスク（機器）	国際標準・他国の標準					国内外の標準		
大項目（評価の枠組）		中項目（設定される領域）	（維持される対策状態）	小項目（具体的対策の例）	該当／対象外	セルフアセスメント	第三者認証／外部監査	ペネトレーションテストの実施有無	IEC 62443-3シリーズ	IEC 62443の要件	NIST CSF	NIST SP 800-53 Rev.5 (Draft)	NERC CIP	電力制御システムセキュリティガイドライン（電制ガイド）	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）	
① 全体（組織の管理体制）	電力関連機器ベンダの組織全体におけるセキュリティガバナンス	・機器に関連する情報資産の保護（盗まれ（改ざん/破壊/利用停止等） ・関連法規等への遵守（属国・地域規制、プライバシー法規等）	・経営層の責任と方針の明示 ・組織的リスクマネジメントに基づく情報保護 ・関連会社を含めた統制	組織全体のセキュリティポリシーが定義されている			初期/CSMS等による内部監査		IEC 62443-2-1 4.1	組織のセキュリティマネジメント方針の定義と	ID GV-1, ID GV-2, ID GV-3	PM-1, PM-2, 別ガイドでのセキュリティ管理策ファミリID（XX-1）管理策	PS-7, PM-1, PM-2, 別ガイドでのセキュリティ管理策ファミリID（XX-1）管理策	CIP-003-S R1・1.1~1.9, R2, R3, R4, CIP-004-S 1 R1, R3	電制GL 第2-1章, 第3-3章	CPS GV-1, CPS GV-2	
				組織のセキュリティ対策が、リスク分析に基づき継続的に改善されている					IEC 62443-2-1 4.2, 4.3, 4.4	リスク分析手法の選択、リスク分析の実施、リスクへの対処、リスクの監視、継続的改善	ID RE-3, ID RA-1, ID RA-2, ID RA-3, D RA-4, D RA-5, ID RA-6, D SC-2, RS IN-1, RS IM-2, RS MI-3, RS AN-5	PM-4, PM-9, PM-11, PM-12, PM-15, PM-16, SA-14, CA-2, CA-7, CA-8, RA-2, RA-3, RA-5, SA-5, SA-11, SA-12, SI-2, SI-4, SI-5, SA-15, CP-2, IR-4, IR-8	CIP-003-S R1・1.2~1.5 1.7, R2・2.4, CIP-007-S R2, R3, R4・4.1, CIP-008-S R1・1.1, R2, R3, CIP-010-1 R3	電制GL 第4-1章	CPS RE-2, CPS RA-1, CPS RA-2, CPS RA-3, CPS RA-4, CPS RA-5, CPS RA-6, CPS SC-2, CPS IM-1	
				組織の保有する情報資産を一覧化し、記録及び管理をしている					IEC 62443-2-1 5.9	資産の識別、情報の格付け、記録と管理、	ID AM-1, ID AM-2, ID AM-3	CM-8, PM-5, AC-4, CA-3, CA-9, PL-8	CIP-002-S 1 R1, R2, CIP-003-S R1・1.2, R2, CIP-005-S R2, CIP-011-1 R1	電制GL 第3-1章, 第3-2章	CPS AM-1, CPS AM-3, CPS AM-4	
				組織が開発及び保守するシステムにおいて、統一的に守られるべきセキュリティ規範が定められている					IEC 62443-2-1 5.8	セキュリティ事件定義、テスト、変更管理、セキュリティとセーフティの統合、維持管理、パッチマネジメント、ウイルス対策、バックアップと復旧	ID BE-5, PR AC-3, PR IP-1, PR IP-3, PR IP-4, PR IP-9, DE CM-3, DE CM-4, DE CM-5, DE CM-7, DE DP-4, RS RP-1, RS CO-2, RS CO-3, RS MI-1, RS MI-2	CM-2, CM-3, CM-4, CM5, CM-6, CM-7, CM-9, SA-10, CM-4, CP-4, CP-9, SI-3, SI-4, AC-2, AU-12, AU-13, CA-7, CM-10, CM-11, PE-3, PM-6, PE-20, SI-4, CP-2, CP-10, IR-4, IR-8	CIP-003-S R1・1.1, 1.2, 1.4, 1.5~1.7, 1.9, R2・2.1, 2.4, CIP-004-S 1 R3, R4, R5, CIP-005-S R1, R1・1.5, R2, CIP-006-S R1・1.5~1.7, CIP-007-S R3, R4, R5, CIP-008-S R1, R2, R3, CIP-009-S R1, R3, CIP-010-1 R1, R2	電制GL 第5-1章, 第5-2章, 第5-3章, 第5-5章	CPS IP-1, CPS IP-4, CPS CM-3, CPS CM-6, CPS RP-1, CPS MS-1	
			・要害の実施によるエスの防止 ・内部不正の抑止	組織内の人員及び関係者の役割、責任等が定められ、周知と教育が実施されている					IEC 62443-2-1 5.2	要員の責任定義、雇用と配置、異動の分離、採用	ID AM-5, PR AT-1, PR AT-2, PR AT-3, PR AT-4, PR AT-5, PR IP-10, RS CO-1	CP-2, RA-2, SA-14, SC-6, AT-1, AT-2, AT-3, AT-4, PS-7, SA-9, SA-16	CIP-003-S R1・1.1~1.9, R2・2.1, R4, CIP-004-S 1 R1, R2, R2・Pa 1.2 1.6, CIP-005-S R1, CIP-006-S R2, CIP-008-S R1, R2, R3, CIP-009-S R1・1.1, R2	電制GL 第2-2章	CPS AM-6, CPS AT-1, CPS AT-2, CPS AT-3,	
				組織内の人員及び関係者のIDとアクセス権限が管理され、ログを保管されている					IEC 62443-2-1 5.5, 5.6, 5.7	特権の管理、個人の識別、飛行プロセス、アカウントの記録、不要アカウントの停止 削除、レビュー、監査、デフォルトパスワードの変更 認証ポリシー、全てのユーザの認証、管理権アカウントの認証強度、重要システムへのアクセス記録 監査、リモートユーザー認証、ルール強化の処理 認可ポリシー、論理的認可 物理的認可、役割に基づく認可、重要システムの多要素認証	PR AC-1, PR AC-3, PR AC-4, PR AC-7, PR IP-1, PR IP-3	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24, CM-2, CM-3, CM-4, CM5, CM-6, CM-7, CM-9, SA-10, IA-1, A-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, SC-15	CIP-003-S R1・1.1, 1.2, 1.3, 1.4, 1.7, 1.8, R2・2.1, 2.2, 2.3, CIP-004-S 1 R4, R5, CIP-005-S R1, R2, CIP-006-S R1, R2, CIP-007-S R5	電制GL 第5-4章, 第5-7章, 第5-8章	CPS AC-1, CPS AC-3, CPS AC-4, CPS AC-5, CPS AC-6, CPS AC-8, CPS IP-1	
			・組織境界への不正アクセスからの保護 ・組織境界へのマルウェア感染対策	組織拠点の物理セキュリティ境界が確立され、予期せぬ侵入から保護されている					IEC 62443-2-1 5.3	物理セキュリティとサイバーセキュリティの統合、物理セキュリティ境界の確立、入退管理、環境的保護からの保護、監視と警報	ID BE-5, PR AC-2, PR IP-5, PR PT-2, PR PT-3, DE CM-2	PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-18, PE-12, PE-13, PE-14, PE-15, PE-18, PE-20, AC-3, CM-7, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8, CA-7, PE-3, PE-6	CIP-003-S R1・1.1~1.9, R2・2.2, CIP-004-S 1 R4, R5, CIP-005-S R2, CIP-006-S R1, R2, CIP-007-S R5, CIP-009-S R1	電制GL 第5-6章, 第5-7章	CPS AC-2, CPS IP-5, CPS PT-2, CPS CM-2	
				組織内のネットワークがセキュリティレベルに応じて分割され、必要な本事で保護されている					IEC 62443-2-1 5.4	セキュリティゾーンの分割、異リスクシステムの隔離又は分割、制御ネットワークへの不要な通信のブロック	PR AC-4, PR AC-5, PR AC-7, PR DS-7, PR PT-3, PR PT-4, DE CM-1	AC-1, AC-2, AC-3, ACS, AC-6, AC-14, AC-16, AC-24, AC-4, AC-10, SC-7, CM-7, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	CIP-003-S R1・1.1, 1.2, 1.4, 1.7, 1.8, CIP-004-S 1 R4, R5, CIP-005-S R1, R2・1.5, R2, CIP-007-S R1, R5, CIP-010-1 R2	電制GL 第5-1章, 第5-2章	CPS AC-4, CPS AC-7,CPS PT-2, CPS CM-1	
		・インシデント発生時の被害拡大（機器関連インシデント対応の場合等）	・インシデントレスポンス体制の構築	対象等を想定した事業継続計画、復旧手順が用意されている					IEC 62443-2-1 5.1	復旧措置、事業継続計画、役割と責任の定義、計画のテストと更新	ID BE-5, RC RP-1, RC CO-2, RC CO-3	CP-2, CP-11, CP-10, IR-4, IR-8, SA-13, SA-14	CIP-003-S R1・1.1, 1.6, CIP-007-S R4, CIP-009-S R1, R2, R3	電制GL 第4-1章	CPS RP-3, CPS CO-2, CPS CO-3	
				全社的なセキュリティインシデント対応組織を等し、対応計画 事務手順書の確定、訓練の実施、改善活動等を行っている					IEC 62443-2-1 5.10	インシデント対応計画、事務手順の確立、事異原因、演習、インシデントの変遷、問題への対処、改善	ID BE-5, ID RA-3, PR AT-1, PR AT-2, PR AT-4, PR AT-5, PR IP-7, PR IP-9, PR PT-1, DE AE-3, DE DP-4, RS RP-1, RS CO-2, RS CO-3, RS AN-1, RS IM-1, RS IN-2, RC RP-1, RC IM-1, RC IM-2, RC CO-1, ID SC-5,	RA-3, SI-5, PM-12, PM-16, CP-2, CP-4, CP-10, CP-11, IR-3, IR-4, IR-6, IR-8, IR-9, AT-1, AT-2, AT-3, AT-4, CA-2, CA-7, PL-2, PM-6, AU Family, IR-5, SI-4, SA-13, SA-14	CIP-003-S R1・1, 1.1~1.9, R2・2.1, 2.4, R4, CIP-004-S 1 R1, R2, CIP-006-S R1・1.5~1.9, 2.3, R2, R2・2.2, CIP-007-S R4, R4・4.1, 4.3, 4.4, CIP-008-S R1, R2, R3, CIP-009-S R1, R2, R3, CIP-010-1 R3	電制GL 第7-1章~第7-4章	CPS RA-3, CPS SC-9, CPS AT-1, CPS IP-7, CPS PT-1, CPS AR-3, CPS RP-1, CPS RP-3, CPS RP-4, CPS CO-1, CPS IM-1, CPS IM-2	
② SDH（開発プロセス）	電力関連機器ベンダの製品責任プロセスにおけるセキュリティ対策	・不十分なセキュリティ事件	・脅威分析に基づいたセキュリティ事件定義	製品開発プロセスに個別セキュリティ管理策が含まれている			社内部署の組織等を精査することで回答		IEC 62443-4-1 SM	開発工程管理、スコープ管理、開発環境管理、ファイル管理、構成管理、外部コンポーネント利用要件、第三者脆弱性の改善ルール、継続的改善	–	–	–	電制GL 第6-1章	–	
				製品のユースケース等を基本方針策定時点で行い、製品セキュリティ事件を定義している					IEC 62443-4-1 SR	製品のコンテキスト、脅威モデル、製品セキュリティ事件、セキュリティ事件のレビュー	–	–	–	電制GL 第6-1章	–	
		・セキュリティ事件の実装不備	・セキュア・バイデザイン ・セキュア開発	製品の設計時点でセキュリティ事件を特定している					IEC 62443-4-1 SD	セキュア設計原則、必要の最限化、セキュリティ設計のレビュー、ベストプラクティスの参照	–	–	–	電制GL 第6-1章	–	
				製品の開発時点でセキュアコーディング規則を行っている					IEC 62443-4-1 SI	セキュア実装レビュー、セキュアコーディング規約	–	–	–	–	–	
		・脆弱な実装の検出漏れ	・セキュリティテスト ・脆弱性識別試験（スキャン） ・ペネトレーションテスト	製品のセキュリティ機能要求テスト（事件実装確認）を実施している					IEC 62443-4-1 SVV	セキュリティ事件のテスト、脅威調査テスト、脆弱性試験、ペネトレーションテスト、テスターの独立性 ＊事件を適当化するか	–	–	–	–	–	
				製品の脆弱性識別（スキャン）試験を実施している					IEC 62443-4-1 SVV	セキュリティ事件のテスト、脅威調査テスト、脆弱性試験、ペネトレーションテスト、テスターの独立性 ＊事件を適当化するか	–	–	–	–	–	
				製品の機能に対するペネトレーションテストを実施している					IEC 62443-4-1 SVV	セキュリティ事件のテスト、脅威調査テスト、脆弱性試験、ペネトレーションテスト、テスターの独立性 ＊事件を適当化するか	–	–	–	–	–	
③ 製品セキュリティ（製品：一般）	電力関連機器に求められる一般的セキュリティ事件	・機器、ユーザーへのなりすまし ・中間者攻撃	・機器とユーザの認証	各々の製品機能が実施され、正しく認証される				セキュリティ試験や、ペネトレーションテストの成績実施によって証明	IEC 62443-4-2 CR 1	ユーザー属性と認証、ソフトウェアおよびデバイスの認証、アカウント管理、制御アクセス管理、暗号鍵の強度、認証も含例の準備、信頼できないネットワークからのアクセス制御	–	–	–	–	–	
				機器ユーザーのアカウントが管理され、正しく認証される					IEC 62443-4-2 CR 1	ユーザー属性と認証、ソフトウェアおよびデバイスの認証、アカウント管理、制御アクセス管理、暗号鍵の強度、認証も含例の準備、信頼できないネットワークからのアクセス制御	–	–	–	–	–	
		・機器への不正アクセス	・アクセス制御とモニタリング	外部ネットワーク、制御アクセス等の制御、管理を行っている					IEC 62443-4-2 CR 1	ユーザー属性と認証、ソフトウェアおよびデバイスの認証、アカウント管理、制御アクセス管理、暗号鍵の強度、認証も含例の準備、信頼できないネットワークからのアクセス制御	–	–	–	–	–	
				ネットワーク境界はアクセス制御等により保護されている					IEC 62443-4-2 CR 5	ネットワーク分離、ゾーン境界防御、FW通信の制限、アプリケーションの区分	–	–	–	–	–	
				物理診断ポートとテスト/FWの利用は制限されている					IEC 62443-4-2 CR 2	認証の強度、制御利用制限、モバイルデバイス利用管理、セッションロック 切断、監査可能ログ、共用防止、物理診断ポートとテスト/FWの利用制限	–	–	–	–	–	
				監査ログが記録され、保護されている					IEC 62443-4-2 CR 2	認証の強度、制御利用制限、モバイルデバイス利用管理、セッションロック 切断、監査可能ログ、共用防止、物理診断ポートとテスト/FWの利用制限	–	–	–	–	–	
		・機器への不正コマンドインジェクション	・入力値検証	入力値は検証され、不正な入力が拒止されている					IEC 62443-4-2 CR 3	通信の完全性、不正コードからの保護、セキュリティ機能維持、ソフトウェアとデータの完全性、入力値検証、エラー処理、外部標準利用の監査、アップデートのサポート、物理診断ポート告 改ざん検知、重要の復旧の維持、所有者の復旧の維持、起動プロセスの完全性	–	–	–	–	–	
				起動プロセスが不正操作の影響を受けない					IEC 62443-4-2 CR 3	通信の完全性、不正コードからの保護、セキュリティ機能維持、ソフトウェアとデータの完全性、入力値検証、エラー処理、外部標準利用の監査、アップデートのサポート、物理診断ポート告 改ざん検知、重要の復旧の維持、所有者の復旧の維持、起動プロセスの完全性	–	–	–	–	–	
		・機器の機密データ盗聴、改ざん	・通信の暗号化、署名検証 ・信頼ある通信プロトコル選択	通信データが改ざんから保護されている					IEC 62443-4-2 CR 3	通信の完全性、不正コードからの保護、セキュリティ機能維持、ソフトウェアとデータの完全性、入力値検証、エラー処理、外部標準利用の監査、アップデートのサポート、物理診断ポート告 改ざん検知、重要の復旧の維持、所有者の復旧の維持、起動プロセスの完全性	–	–	–	–	–	
				外部との機密データ通信は必要な強度で暗号化されている					IEC 62443-4-2 CR 4	情報の機密性、情報の消去、暗号の利用	–	–	–	–	–	
				機器に保存された機密データは必要な強度で暗号化されている					IEC 62443-4-2 CR 4	情報の機密性、情報の消去、暗号の利用	–	–	–	–	–	
		・機器データ、ソフトウェアの改ざん	・耐タンパ性、データ保護	物理的な耐タンパ性が確保されている					IEC 62443-4-2 CR 3	通信の完全性、不正コードからの保護、セキュリティ機能維持、ソフトウェアとデータの完全性、入力値検証、エラー処理、外部標準利用の監査、アップデートのサポート、物理診断ポート告 改ざん検知、重要の復旧の維持、所有者の復旧の維持、起動プロセスの完全性	–	–	–	–	–	
				真セキュリティモジュールはネットワークから分離されている					IEC 62443-4-2 CR 5	ネットワーク分離、ゾーン境界防御、FW通信の制限、アプリケーションの区分	–	–	–	–	–	
				機器のソフトウェアが標準データが改ざんから保護されている					IEC 62443-4-2 CR 3	通信の完全性、不正コードからの保護、セキュリティ機能維持、ソフトウェアとデータの完全性、入力値検証、エラー処理、外部標準利用の監査、アップデートのサポート、物理診断ポート告 改ざん検知、重要の復旧の維持、所有者の復旧の維持、起動プロセスの完全性	–	–	–	–	–	
		・機器へのサービス不能攻撃、災害・事故	・セーフモード ・バックアップ	動作異常時にも機器のログへのアクセスを確認できる					IEC 62443-4-2 CR 6	ログアクセスの保証、ログの継続監視	–	–	–	–	–	
				サービス不能攻撃を受けた際にも最低限の機能が維持される					IEC 62443-4-2 CR 7	DoS攻撃対策、リソース管理、制御システムのバックアップ、復旧と再構築、非常電源、最小機能の確保、設定ファイルの保護	–	–	–	–	–	
				データのバックアップが取得され、復旧が可能である					IEC 62443-4-2 CR 7	DoS攻撃対策、リソース管理、制御システムのバックアップ、復旧と再構築、非常電源、最小機能の確保、設定ファイルの保護	–	–	–	–	–	
				機器の設定ファイルは保護されており、再利用可能である					IEC 62443-4-2 CR 7	DoS攻撃対策、リソース管理、制御システムのバックアップ、復旧と再構築、非常電源、最小機能の確保、設定ファイルの保護	–	–	–	–	–	

評価項目					評価対象	スコアカードによる評価			他の評価基準との対応						
						標準的	低リスク（組織）	低リスク（機器）	国際標準・各国の標準					国内外の標準	
大項目（評価の枠組）		中項目（想定される脅威）	（期待される対策要件）	小項目（具体的対策の例）	該当／対象外	セルフアセスメント	第三者認証／外部監査	ペネトレーションテストの実施例	IEC 62443シリーズ	IEC 62443の要件	NIST CSF	NIST SP 800-53 Rev.5 (Draft)	NERC CIP	電力制御システムセキュリティガイドライン（電制GL）	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）
⑥ SOM上流（調達管理プロセス）	電力関連機器のライフサイクル下流（調達）におけるセキュリティ要件	・権限な責任分界のセキュリティ対策（対策漏れが生じる）	・SLAの明示 ・責任者と問い合わせ窓口の明確化	製品、サービスの開発等へ適守すべき規格が明記されている			PSIRT等の関与によって最新		IEC 62443-3-4 SP 01	製造製品、サービスに関与する要員の適正な配置、責任、力量、手順の明記（セキュリティ要求、機密データ保護）、要員の違反調査、セキュリティ関連窓口の設置、セキュリティ責任者の報告、緊急変更の通知	ID SC-1, ID SC-2, ID SC-3	SA-9, SA-11, SA-12, RA-3, SA-14, SA-15, PM-9, RA-2	CIP-013-1 R1, R2	電制GL 第2-1条, 第2-2条	CPS SC-1, CPS SC-2, CPS SC-3, CPS SC-11
				製品、サービスのセキュリティ責任者及び問い合わせ窓口が明示されている					IEC 62443-3-4 SP 01	製造製品、サービスに関与する要員の適正な配置、責任、力量、手順の明記（セキュリティ要求、機密データ保護）、要員の違反調査、セキュリティ関連窓口の設置、セキュリティ責任者の報告、緊急変更の通知	ID SC-1, ID SC-2, ID SC-3	SA-9, SA-11, SA-12, RA-3, SA-14, SA-15, PM-9, RA-2	CIP-013-1 R1, R2	電制GL 第2-1条, 第2-2条	CPS SC-1, CPS SC-2, CPS SC-3, CPS SC-11
				製品、サービスのセキュリティ水準を保証する文書等の提示が可能である					IEC 62443-3-4 SP 02	製造製品、サービスのセキュリティ水準を保証する文書の提示、利用するセキュリティ分析ツール等の脆弱度力、セキュリティ強化方法を説明する文書の提示	ID SC-2	AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12	CIP-013-1 R3	電制GL 第4-1条	CPS SC-7, CPS SC-8
		・不十分な理解に基づいた機器調達（設定ミスや標準外の利用による脆弱性）	・機器の構成及び機能に関する文書の提供 ・機器の設定に関するガイダンスの提示	機器 ソフトウェアのセキュリティ機能の全体構成について、説明可能な文書等の提示が可能である			最新情報マニュアル等の（郵送等）アップロードにより提供		IEC 62443-3-4 SP 03	調達する機器 ソフトウェア等のリスクアセスメント、ネットワークセキュリティ設計の確認、脆弱性情報管理、安全な停止同期、監視化、操作端末の不正利用対策（セッションロック）、操作端末へのアクセス制限、最小限の特権分与など、データ通信の保護、機密データ保存場所の立案化	–	–	–	–	–
				機器に関連ネットワーク方式及びセキュリティ実装について、説明可能な文書等の提示が可能である					IEC 62443-3-4 SP 04	無線接続方式の制限、アクセス制御	–	–	–	–	–
				安全計装システムのセキュリティ機能に関する制限と要件を与える文書等の提示が可能である					IEC 62443-3-4 SP 05	リスクアセスメント、ネットワーク管理の影響評価、リモートアクセスの設定、安全計装システムとの不要な通信の遮止、操作端末の制限、監視化、無線接続の場合、安全計装システムの有効/管理を切り替えるユーザーインターフェース	–	–	–	–	–
				機器 ソフトウェア等の構成管理に関する制限と要件を与える文書等の提示が可能である					IEC 62443-3-4 SP 06	管理機能説明 管理機能説明、調査仕様、設定値	–	–	–	–	–
				機器へのリモートアクセス方式及びセキュリティ実装について、説明可能な文書等の提示が可能である					IEC 62443-3-4 SP 07	実装のある遠隔 方式、接続構成の説明、接続時の方法の説明、接続の準備	–	–	–	–	–
⑤ SOM下流（製品保守運用プロセス）	電力関連機器のライフサイクル上流（物流・保守・廃棄）におけるセキュリティ要件	・攻撃者による他ログイン認証性の悪用	・機器に関する不具合、脆弱性情報の受付 ・脆弱性対策情報発信のコントロール	製品のユーザー及び外部機関等から、機器の脆弱性等セキュリティに関する問題の報告、情報提供を受け付けている			PSIRT等の関与によって最新		IEC 62443-4-1 DM	セキュリティ関連問題の受付、評価、発信、定期的まとめ	–	–	–	–	–
				報告されたセキュリティに関する問題は、分析、対応策を管理した後、情報の発信を実施している					IEC 62443-4-1 DM	セキュリティ関連問題の受付、評価、発信、定期的まとめ	–	–	–	–	–
		・攻撃者による未対応の脆弱性の悪用	・アップデート機能の提供 ・修正プログラム、パッチの提供	セキュリティアップデートの正当性検証　アップデート実施方式等に関する文書等の提示が可能である					IEC 62443-4-1 SUM	セキュリティアップデート提供、文書化、他界コンポーネントやOSのアップデート、パッチの適時配信	–	–	–	–	–
				他のOS及びコンポーネントのアップデートに関する対応方針が定まっている					IEC 62443-4-1 SUM	セキュリティアップデート提供、文書化、他界コンポーネントやOSのアップデート、パッチの適時配信	–	–	–	–	–
				修正プログラム、修正パッチが適時提供される					IEC 62443-4-1 SUM	セキュリティアップデート提供、文書化、他界コンポーネントやOSのアップデート、パッチの適時配信	–	–	–	–	–
		・機器の誤った（関係外の）取扱いを誘った攻撃	・機器の堅牢化、安全な初期設定 ・推奨される手順に従った廃棄	機器を安全に設定し堅牢化するためのマニュアルが提供される							–	–	–	–	–
				機器の安全な利用、廃棄を行うためのマニュアルが提供される							–	–	–	–	–
				ユーザーアカウントの安全な設定、利用を行うためのマニュアルが提供される					IEC 62443-4-1 SG	文書化、監視化、安全な運用、安全な廃棄、廃棄管理、多層防御運用（GDガイダンスを提供）	–	–	–	–	–
④ 工場セキュリティ（製造プロセス）	電力関連機器ベンダの製品工場、開発施設、システムのセキュリティ対策	・機器のソフトウェア改ざん、不正な部品の組込み	・開発段階からの脆弱管理（外部委託先含む） ・脆弱の種類管理、コマンド制限 ・外部記憶媒体管理、マルウェア対策	製造設備の人員及び関係者のIDとアクセス制御が管理され、ログが検証されている			CSMS もしくは ISASCE制御系認証 のセルフアセスメント実施		IEC 62443-3-3 SR 1	ユーザーアクセス制御、ネットワークアクセス制御、アカウント管理、認証管理、鍵管理、信頼できないネットワークからのアクセス制御	FR AC-1, FR AC-3, FR AC-6, FR AC-7, FR PT-2, FR PT-3	IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, AC-1, AC-2, AC-3, AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, AC-16, AC-17, AC-19, AC-20, AC-24, SC-15, PE-2, PS-3, IA-2, CM-7, MP-2, MP3, MP-4, MP-5, MP-7, MP-8	CIP-003-8 R1 - 1.1, 1.2, 1.4, R2 - 2.3, CIP-004-6 1 R4, R5, CIP-005-6 R1, R2, CIP-007-6 R5			
				製造設備で用いる端末等では、入力値の検証　コマンド実行の制限等により不正コード実行を防止している					IEC 62443-3-3 SR 3	通信の完全性、不正コードからの保護、セキュリティ機能維持、ソフトウェアとデータの完全性、入力値検証、エラー処理、外部媒体利用の監督	PR AC-5, PR DS-1, PR DS-2, PR DS-6, PR DS-7, PR PT-4, PR PT-5, DE CM-4, DE CM-5, DE DP-3	AC-4, AC-10, SC-7, MP-8, SC-6, SC-8, SC-11, SC-13, SC-16, SC-28, SI-7, CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SI-3, SI-8	CIP-003-8 R1 - 1.2, 1.7, 1.8, R2 - 2.3, CIP-004-6 1 R2 - 2.1, R4, R5, CIP-005-6 R1, R2, CIP-006-6 R3, CIP-007-6 R1, R3, R5, CIP-008-6 R2, CIP-010-1 R1, R2, CIP-011-1 R1, R2	電制GL 第5-2条, 第5-5条, 第5-6条	CPS AC-7, CPS DS-2, CPS DS-3, CPS DS-4, CPS DS-10, CPS DS-11, CPS PT-3, CPS CM-3, CPS CM-4, CPS DP-3
				製造設備で用いられる外部記憶媒体は、利用前に安全性の検証を行っている					IEC 62443-3-3 SR 3	通信の完全性、不正コードからの保護、セキュリティ機能維持、ソフトウェアとデータの完全性、入力値検証、エラー処理、外部媒体利用の監督	PR AC-5, PR DS-1, PR DS-2, PR DS-6, PR DS-7, PR PT-4, PR PT-5, DE CM-4, DE CM-5, DE DP-3	AC-4, AC-10, SC-7, MP-8, SC-6, SC-8, SC-11, SC-13, SC-16, SC-28, SI-7, CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SI-3, SI-8	CIP-003-8 R1 - 1.2, 1.7, 1.8, R2 - 2.3, CIP-004-6 1 R2 - 2.1, R4, R5, CIP-005-6 R1, R2, CIP-006-6 R3, CIP-007-6 R1, R3, R5, CIP-008-6 R2, CIP-010-1 R1, R2, CIP-011-1 R1, R2	電制GL 第5-2条, 第5-5条, 第5-6条	CPS AC-7, CPS DS-2, CPS DS-3, CPS DS-4, CPS DS-10, CPS DS-11, CPS PT-3, CPS CM-3, CPS CM-4, CPS DP-3
		・機器に関連する機密情報（ソースコード等）の抽出し	・重要ネットワークへのアクセス制御 ・機密データの暗号化	製造設備内のネットワークは重要性を考慮して分割されている					IEC 62443-3-3 SR 4	情報の機密性、外部ネットワーク通信の暗号化、信頼領域境界、データの暗号化	PR DS-1, PR DS-2, PR DS-3, PR IP-6	MP-8, MP-8, SC-8, SC-11, SC-12, SC-28	CIP-003-8 R1 - 1.2, 1.8, R2 - 2.3, CIP-004-6 1 R4, R5, CIP-005-6 R1, R2, CIP-007-6 R3, CIP-011-1 R1, R2	電制GL 第5-3条	CPS DS-2, CPS DS-3, CPS DS-4, CPS IP-6
				製造設備のネットワークのアクセス制御が行われている					IEC 62443-3-3 SR 2	ユーザー権限管理、管理者権限、多段の二重化、無線利用制御、セッション管理、ログ監査、共認防止	PR AC-3, PR AC-4, PR AC-6, PR AC-7, PR PT-1, DE AE-2, RS AN-3	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-17, AC-19, AC-20, AC-24, SC-15, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3, CA-7, IR-4, SI-4, AU-7	CIP-003-8 R1 - 1.1, 1.2, 1.4, 1.5, 1.6, R2 - 2.2, CIP-004-6 1 R4, R5, CIP-005-6 R1, R2, CIP-006-6 R1 - 1.6, 1.8, 1.9, 2.3, R2 - 2.2, CIP-007-6 R4, R4 - 4.3, 4.4, R5, CIP-008-6 R1, R2, CIP-009-6 R1 - 1.5	電制GL 第5-6条, 第5-7条, 第5-8条	CPS AC-4, CPS AC-5, CPS AC-6, CPS AC-8, CPS PT-1, CPS AR-2, CPS AN-2
				製造設備内の重要な通信及びデータがおかみから保護されている					IEC 62443-3-3 SR 1	ユーザーアクセス制御、ネットワークアクセス制御、アカウント管理、認証管理、鍵管理、信頼できないネットワークからのアクセス制御	PR AC-1, PR AC-3, PR AC-6, PR AC-7, PR PT-2, PR PT-3	IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11, AC-1, AC-2, AC-3, AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, AC-16, AC-17, AC-19, AC-20, AC-24, SC-15, PE-2, PS-3, IA-2, CM-7, MP-2, MP3, MP-4, MP-5, MP-7, MP-8	CIP-003-8 R1 - 1.1, 1.2, 1.4, 1.5, R2 - 2.3, CIP-004-6 1 R4, R5, CIP-005-6 R1, R2, CIP-007-6 R5	電制GL 第5-6条, 第5-7条, 第5-8条	CPS AC-1, CPS AC-3, CPS AC-4, CPS AC-8, CPS AC-9, CPS PT-2
				製造設備外のネットワーク通信は暗号化されている					IEC 62443-3-3 SR 3	通信の完全性、不正コードからの保護、セキュリティ機能維持、ソフトウェアとデータの完全性、入力値検証、エラー処理、外部媒体利用の監督	PR AC-5, PR DS-1, PR DS-2, PR DS-6, PR DS-7, PR PT-4, PR PT-5, DE CM-4, DE CM-5, DE DP-3	AC-4, AC-10, SC-7, MP-8, SC-6, SC-8, SC-11, SC-12, SC-16, SC-28, SI-7, CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SI-3, SI-8	CIP-003-8 R1 - 1.2, 1.7, 1.8, R2 - 2.3, CIP-004-6 1 R2 - 2.1, R4, R5, CIP-005-6 R1, R2, CIP-006-6 R3, CIP-007-6 R1, R3, R5, CIP-008-6 R2, CIP-010-1 R1, R2, CIP-011-1 R1, R2	電制GL 第5-2条, 第5-5条, 第5-6条	CPS AC-7, CPS DS-2, CPS DS-3, CPS DS-4, CPS DS-10, CPS DS-11, CPS PT-3, CPS CM-3, CPS CM-4, CPS DP-3
				製造設備内の機密データは暗号化して保存されている					IEC 62443-3-3 SR 4	情報の機密性、外部ネットワーク通信の暗号化、信頼領域境界、データの暗号化	PR DS-1, PR DS-2, PR DS-3, PR IP-6	MP-8, MP-8, SC-8, SC-11, SC-12, SC-28	CIP-003-8 R1 - 1.2, 1.8, R2 - 2.3, CIP-004-6 1 R4, R5, CIP-005-6 R1, R2, CIP-007-6 R3, CIP-011-1 R1, R2	電制GL 第5-3条	CPS DS-2, CPS DS-3, CPS DS-4, CPS IP-6
		・機器供給の起害	・バックアップ ・非常電源	動作異常時等にも機器のログへのアクセスを確保できる					IEC 62443-3-3 SR 5	ネットワーク分離、重要ネットワークの物理的隔離、ゾーン境界の保護、デフォルト拒否の原則、フェールクローズ、冗長構成の制限	PR AC-5, PR DS-5, PR DS-7, PR PT-2, PR PT-3, PR PT-4, DE CM-1, RS MI-1, RS MI-2	AC-2, AC-3, AC-4, AC-10, SC-7, SC-8, SC13, SC-31, SI-4, CM-7, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8, AU-12, CA-7, CM-3, SC-5, IR-4	CIP-003-8 R1 - 1.2, 1.4, 1.5, 1.7-1.9, R2 - 2.3, 2.4, CIP-004-6 1 R4, R5, CIP-005-6 R1, R2, CIP-006-6 R1 - 1.5, 1.7, CIP-007-6 R1, R3, R4, R5, CIP-008-6 R2, CIP-010-1 R2, CIP-011-1 R1, R2	電制GL 第5-1条, 第5-2条	CPS AC-7, CPS DS-4,CPS PT-2, PS CM-1, CSP ME-1
				データのバックアップや非常電源等により、異常発生時にも最低限必要な機能の稼働が維持される					IEC 62443-3-3 SR 6	ログアクセスの保護、ログの継続的監視	PR IP-7, PR MA-2, PR PT-1, DE AE-2, DE CM-1	CA-2, CA-7, CP-2, IR-4, IR-8, PL-2, PM-6, MA-4, AU-6, SI-4, AC-2, AU-12, CM-3, SC-5, SC-7, SI-4	CIP-003-8 R1 - 1.3, CIP-005-6 R1 - 1.5, R2, CIP-006-6 R1 - 1.6, 1.8, 1.9, 2.3, R2 - 2.2, R3, CIP-007-6 R4, R4 - 4.3, 4.4, CIP-008-6 R1, R2, CIP-010-1 R1, R3	電制GL 第5-7条, 第5-8条	CPS IP-7, CPS MA-2, CPS PT-1, CPS AR-2, CPS CM-1
				サービス不能攻撃を受けた際にも最低限の機能が維持される					IEC 62443-3-3 SR 7	DoS攻撃対策、リソース枯渇の防止、バックアップ、異常からの復旧、非常電源、最小機能の原則、設定ファイルの保護	ID IM-5, PR DS-4, PR IP-1, PR IP-3, PR IP-4, PR IP-5	AC-4, AC-5, AC-6, PE-19, PE-3, PE-6, SC-7, SC-8, SC-13, SC-31, SI-4, PE-19, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10, CP-4, CP-6, CP-9, PE-10, PE-12, PE-13, PE-14, PE-15, PE-18	CIP-003-8 R1 - 1.1–1.9, CIP-007-6 R3, R4 - 4.3, CIP-009-6 R1, R3, CIP-010-1 R1, R2	電制GL 第4-1条, 第5-2条, 第5-3条	CPS DS-6, CPS DS-7, CPS IP-1, CPS IP-4, CPS IP-5

2.2 海外での議論の把握

2.2.1 サイバーセキュリティに関する憲章「Charter of Trust」

「Charter of Trust」は、2018 年にミュンヘン安全保障会議（Munich Conference on Security Policy：MSC）において発表されたサイバーセキュリティに関する憲章である。

デジタル化により多数のデバイスがインターネットにより接続される状況においては、サイバー攻撃による社会への影響が深刻になりつつある。このような背景から、「個人や企業のデータを保護する」「人、企業、インフラへの被害を防ぐ」「ネットワーク化されたデジタル世界への信頼が定着し、成長する信頼基盤を構築する」ことを目的にグローバル企業や組織のイニシアティブとして、シーメンスによって開始された。

参加団体は 17 団体、賛同パートナーは 6 団体である（2021 年 3 月時点）。

○参加団体

AES、エアバス、アリアンツ、AtoS、シスコ、デルテクノロジーズ、IBM、
インフィニオン、三菱重工、MSC、NTT、NXP、SGS、シーメンス、ドイツテレコム、
TOTAL、TUV ズード

○賛同パートナー

BSI German Federal Office for Information Security、
Hasso plattner institute university of potsdam、Canadian Centre for Cyber Security、
Graz University of Technology in Austria、CCN National Cryptologic Center of Spain、総務省

表 2-6 「Charter of Trust」10 の原則

No.	項目	説明
1	サイバー及び IT セキュリティの所有権	• 特定の省庁と CISO を指定することにより、政府および企業の最高レベルでサイバーセキュリティの責任を固定します。明確な対策と目標、および組織全体の正しい考え方を確立します–「それはすべての人の仕事です」。
2	デジタルサプライチェーン全体の責任	• 企業（および必要に応じて）政府は、明確に定義された必須の要件を使用して、すべての IoT レイヤーにわたって適切な保護を保証するリスクベースのルールを確立する必要があります。次のようなベースライン基準を設定することにより、機密性、信頼性、整合性、および可用性を確保します。 • **ID とアクセスの管理**： 接続されたデバイスには、許可されたユーザとデバイスのみがそれらを使用できるようにする安全な ID と保護手段が必要です。 • **暗号化**： 接続されたデバイスは、必要に応じて、データの保存と送信の目的で機密性を確保する必要があります。 • **継続的な保護**：企業は、安全な更新メカニズムを介して、製品、システム、およびサービスの合理的なライフサイクル全体にわたって更新、アップグレード、およびパッチを提供する必要があります。

3	デフォルトのセキュリティ	• 最高の適切なレベルのセキュリティとデータ保護を採用し、製品、機能、プロセス、テクノロジー、運用、アーキテクチャ、およびビジネスモデルの設計に事前に構成されていることを確認します。
4	ユーザ中心主義	• 合理的なライフサイクルを通じて信頼できるパートナーとして機能し、製品、システム、サービス、およびお客様のサイバーセキュリティのニーズ、影響、リスクに基づいたガイダンスを提供します。
5	イノベーションと共創	• ドメインのノウハウを組み合わせ、サイバーセキュリティの要件とルールに関する企業と政策立案者の間の共同理解を深めて、サイバーセキュリティ対策を継続的に革新し、新しい脅威に適応させます。契約上の官民パートナーシップを推進し、奨励する。
6	教育	• 将来に必要なスキルと仕事のプロファイルの変革をリードするために、大学、専門教育、トレーニングの学位コースとして、学校のカリキュラムに専用のサイバーセキュリティコースを含めます。
7	重要なインフラストラクチャとソリューションの認定	• 企業（および必要に応じて）政府は、重要なインフラストラクチャおよび重要な IoT ソリューションについて、（特に生命と手足が危険にさらされる将来性のある定義に基づいて）必須の独立したサードパーティ認証を確立します。
8	透明性と対応	• 新しい洞察、インシデントなどに関する情報を共有するために、産業用サイバーセキュリティネットワークに参加します。重要なインフラストラクチャに焦点を当てている今日の慣行を超えたインシデントを報告します。
9	規制の枠組み	• 規制と標準化における多国間協力を促進し、WTO の世界的な範囲に一致する公平な競争の場を設定する。サイバーセキュリティのルールを自由貿易協定（FTA）に含める。
10	共同イニシアチブ	• 過度の遅延なしにデジタル世界の様々な部分で上記の原則を実装するために、関連するすべての利害関係者を含む共同イニシアチブを推進します。

出所：Charter of Trust（https://www.charteroftrust.com/about/（2021 年 3 月 10 日閲覧））を基に三菱総合研究所作成

2.2.2 米国 DHS「ICT Supply Chain Risk Management （SCRM）Task Force」

(1) ICT SCRM タスクフォースの沿革

2018 年 10 月 30 日、米国国土安全保障省（DHS）はサイバーサプライチェーン・リスク管理（C-SCRM）プログラムの一環として、情報通信技術（ICT）サプライチェーンのリスクに対処するための戦略策定に関する官民パートナーシップである ICT Supply Chain Risk Management Task Force（ICT SCRM タスクフォース）を設置した。

タスクフォースは、ICT サプライチェーンに内在しうるリスクや脆弱性を特定し、サプライチェーン全体としてセキュリティを強化することを目的としている。

連邦調達におけるサプライチェーン・セキュリティ確保に向けた取組も進めており、2018 年の SECURE Technology Act に基づき設置された FASC（Federal Acquisition Security Council）と連携し、FASC の推進に有益な情報の提供や支援を行っている。

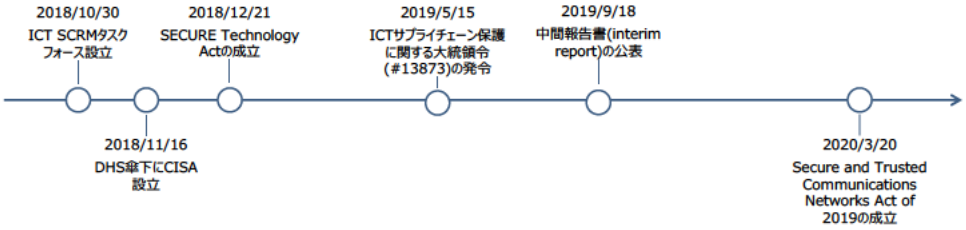


図 2-2　ICT Supply Chain Risk Management タスクフォースの沿革

＜参考＞

SECURE Technology Act：サプライチェーンのセキュリティ脅威を軽減することを目的とした法律で、正式名称は Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act。それまでに上院/下院に提出された、Public-Private Cybersecurity Cooperation Act, Hack the Department of Homeland Security Act of 2018, および Federal Acquisition Supply Chain Security Act of 2018 の内容を併せたもので、サプライチェーンに関する項目としては、サプライチェーンリスクを評価する基準やプロセスの開発を行う FASC(Federal Acquisition Security Council)の設立等が規定されている。FASC の議長は OMB が務め、そのほか、DHS/CISA, ODNI, DoD/NSA, DoJ/FBI, DoC/NIST が含まれる。

Secure and Trusted Communications Networks Act of 2019：国家安全保障上のリスクをもたらす ICT 機器・サービスが米国ネットワークに侵入することを防止することを目的とした法律。連邦通信委員会(FCC)が当該機器・サービスのリストを作成・公開し、FCC の補助金や助成金を受ける通信プロバイダは、当該機器を調達していないか年次で報告する必要がある。情報共有の枠組みについては、NTIA(国家電気通信情報管理庁, 商務省傘下)から ICT 製品のプロバイダおよびサプライヤに対して、サプライチェーンリスクに関する情報を共有することが規定されており、この方法について、DHS の活動(ICT SCRM タスクフォースの活動)と可能な範囲で協力することが規定されている。

(2) ICT SCRM タスクフォースの主な取組・構成組織

ICT SCRM タスクフォースは ICT サプライチェーンのセキュリティ強化のためのリスク管理戦略の特定と開発を目的とし、4 つのワーキンググループ(WG)を設置し、様々な取組を推進している。

タスクフォースには、40 程度の民間企業と 20 程度の政府機関によって構成される。

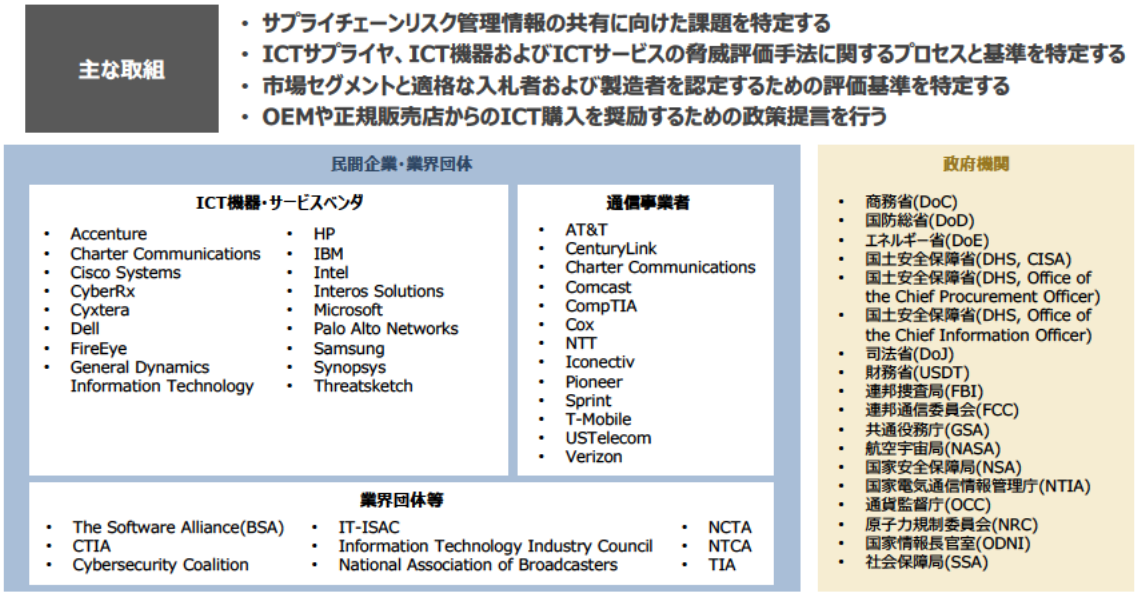


図 2-3　ICT Supply Chain Risk Management タスクフォースの主な取組・構成組織

(3) ワーキンググループ活動

ICT SCRM タスクフォースでは、以下の 4 つのワーキンググループ（WG）を立ち上げている。

- WG1：Information Sharing
- WG2：Threat Evaluation
- WG3：Qualified Bidder Lists & Qualified Manufacturer Lists (QBL/QML)
- WG4：Policy Recommendation to Initiatives Purchase of ICT from OEM or Authorized Reseller

各 WG の概要を表 2-7、成果と今後の取組方針を表 2-8 に示す。

表 2-7　ICT SCRM タスクフォース　4 つの WG 概要

No.	WG1: Information Sharing	WG2: Threat Evaluation	WG3: Qualified Bidder Lists & Qualified Manufacturer Lists (QBL/QML)	WG4: Policy Recommendation to Initiatives Purchase of ICT from OEM or Authorized Reseller
WG の概要	**官民でサプライチェーンリスク情報をより効果的に共有するための共通フレームワークを策定する。**	**サプライチェーン脅威評価のプロセスと基準を特定する。**(リスク評価ではなく脅威評価を行うことで、SCRM エコシステムをより広範に分析する。)	**市場セグメントの特定と、適格な入札者のリスト(QBL)および製造者(QML)のリストを策定するための評価基準を特定する。**	**OEM や正規販売店からの ICT 製品・サービスの購入を奨励する政策を提言する。**これにより、製品の真正性や完全性を保証する。
WG の主な論点	・どのような情報がサプライチェーンリスクを軽減する上で最も価値があるか。 ・その情報に対してアクセスできる方法やフォーラムは存在するか。 ・アクセスできる方法やフォーラムが存在しない場合、どのような理由や障壁が存在するか。	・ICT サプライチェーンに対するセキュリティ脅威シナリオは何か。 ・既存のリスク管理プラクティスは活用可能か。反対に、作成した脅威評価プロセスは、サプライチェーンリスク管理にどのように活用可能か。	・QBL/QML に含めるべき ICT 機器を決定するためのプロセスは何か。 ・QBL/QML に含めるべき ICT 機器は何か。 ・QBL/QML の評価基準は何か。	・正規でない販売ルートで取引される機器にはどのようなセキュリティ脅威が含まれうるか。 ・偽造された ICT 製品・サービスは製造業者にどのような影響を与えうるか。 ・どのような業界が、認定された再販業者に限定するアプローチを取っているか。
取組概要	・どのような脅威情報が、サプライチェーンリスク態勢を変更、適応または修正しうるかを理解する。	・サプライヤ、製品、サービスの脅威評価を実施するための一連のプロセスと基準を作成する。 ・作成したプロセスと基準に基づき、サプライチェーンリスクを評価する脅威ベースのフレームワークを確立する。	・政府調達における QBL/QML の利用状況を理解し、脅威に対してどのように対処しているかを確認する。 ・QBL/QML を策定・活用する際の組織の意思決定に役立つ手順を開発する。 ・WG2 で特定された脅威評価基準を活用し、リスト改善のための要因を特定する。 ・SCRM の評価基準を適切に活用している QBL/QML のユースケースを特定・開発する。	・会議やワークショップの開催や結果の分析を行う。 ・国防等、重要品目の購入を OEM または認定再販業者に限定するアプローチを取っている業界のベストプラクティスを特定する。 ・得られた提言案について、既存の取組との整合を取るために、専門家の意見を得る。

出所：”ICT SCRM Task Force: Interim Report”
https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf （2021 年 3 月 10 日閲覧）に基づき三菱総合研究所作成

表 2-8　ICT SCRM タスクフォース　各 WG の成果と今後の取組方針

No.	WG1: Information Sharing	WG2: Threat Evaluation	WG3: Qualified Bidder Lists & Qualified Manufacturer Lists (QBL/QML)	WG4: Policy Recommendation to Initiatives Purchase of ICT from OEM or Authorized Reseller
1 年目の取組・成果	・業界関係者と議論を行い、多くの情報が利用可能であるものの、その情報源が殆ど知られていない、手頃な価格で入手できない、または容易にアクセスできないことを特定した。 ・リスクを軽減する上で最も価値の情報は、疑わしい、もしくは既知の脅威アクターに関する情報であることを特定した。 ・特に、疑わしいサプライヤの行動を開示するメカニズムは存在するものの、法的な問題があり、業界として中傷的な情報を共有することに障壁があることを特定した。	・サプライヤに存在する脅威について、NIST SP 800-161※1 で定義されたカテゴリを使用し、脅威の発生源や事象等、脅威を特徴づけるための追加情報を収集した。 ・脅威源と脅威シナリオを含んだ脅威リストを作成した。 ・脅威リストを 9 つのカテゴリに分類した。	・QBL/QML の現在の要求事項について、専門家を含めた議論を行い、QBL/QML 活用の推奨事項を策定するとともに、複数のユースケースを検討した。 ・組織が QBL/QML を活用する際の基準として活用できる確認事項を特定した。	・DFARS 規則、SAE AS6496、ISO/IEC 20243 等の規格の内容をに基づき、OEM や正規販売店からの ICT 製品・サービスの購入を奨励する政策を提言した※2。 ・提言は、タスクフォース全体の執行委員会で全会一致で合意され、FASC に提出された。
2 年目以降の取組	・上記の法的な問題に関する知識を有する専門家を特定し、脅威アクターに関する情報共有の方法について法的レビューを行う。 ・レビュー結果を考慮し、法的問題を解決する内容を含んだ、具体的な勧告事項を策定する。	・サプライヤに対する脅威評価の手法を、製品やサービスに対する脅威評価に適用する。 ・NIST SP 800-161 に記載されているリスク管理フレームワークを活用し、特定のリスク評価において適用できる脅威シナリオを開発する。	・政府調達における QBL/QML の利用状況を理解し、脅威に対してどのように対処しているかを確認する。 ・QBL/QML を構築するか、依拠するかの判断を組織に知らせる際の一連の要因を文書化する。 ・SCRM の評価基準を適切に活用している QBL/QML のユースケースを特定・開発する。 ・WG2 で特定された脅威評価基準を活用し、リストの改善を行う。	・（提言の提出により、WG4 の主な目的は達成されたとし、今後は将来検討される可能性がある論点について取組むとしている。） ・SCRM に関与する役割毎に、教育機会と主要な学習目標を特定する。 ・ICT ベンダが自社の SCRM プラクティスを作成するための標準的なテンプレートを開発する。

※1　“Supply Chain Risk Management Practices for Federal Information Systems and Organizations”

※2 提言のタイトルは“Procurement of Information and Communications Technology from Original Equipment Manufacturers, their Authorized Channels, or other Trusted Supplier(s)”

出所：”ICT SCRM Task Force: Interim Report”
https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf （2021 年 3 月 10 日閲覧）に基づき三菱総合研究所作成

2020 年 4 月 23 日、CISA は ICT サプライチェーンリスクに対する認識を高めることを目的としたファクトシートを公開している。ファクトシートでは、サプライチェーンリスクを認識するために組織が実施すべき事項を 6 ステップに整理しており、これらのステップを実施することで効果的な SCRM プラクティスを構築することができるとしている。

出所：”ICT Supply Chain Risk Management Fact Sheet”
https://www.cisa.gov/sites/default/files/publications/factsheet_ict-scrm_508.pdf（2021 年 3 月 10 日閲覧）
に基づき三菱総合研究所作成

図 2-4　サプライチェーンリスクに対するタスクフォースの推奨事項

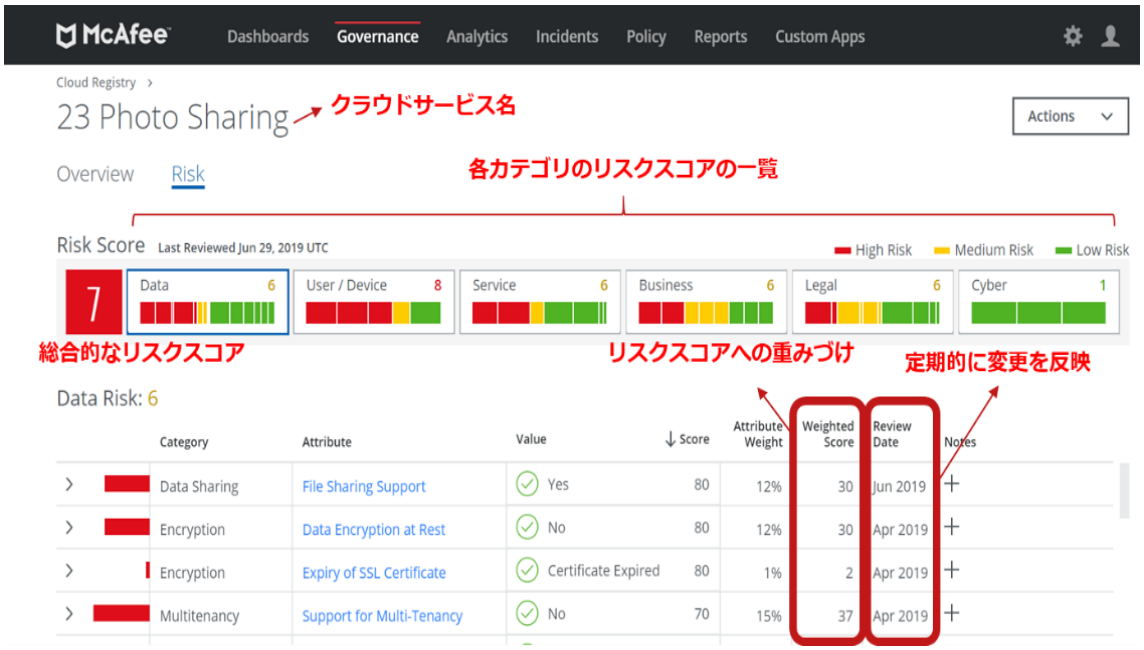
2.2.3 The Cyber Product International Certification Initiative

「The Cyber Product International Certification （CPIC） Initiative」（CPIC）とは、電力分野におけるサプライチェーン・セキュリティ対策として、米国・英国・イスラエルを中心とする製品認証の枠組みを視野に入れた国際的なイニシアティブである。

CPIC の方針は以下の通りである。

- グリッド運用に特に重要なハードウェア及びソフトウェア製品における、業界主導による認証基準を確立する。
- サプライチェーンリスク管理の強化のため、どの製品を対象とするか、厳格な優先順位付けを行う。
- サプライチェーンリスク管理に関する取組を一元化するため、電力事業者及びベンダー等個々の事業者の協力体制を構築する。
- 米国、英国、イスラエル、その他の国々から協力者を集め、国際的なアプローチを行う。

様々なサプライチェーンリスクに対応するために、製品ベンダとユーザ組織の両方に寄与し、相互に活用できる評価スキームを想定している。また、リスクを動的に捉えることを目的として、スコアカード方式の製品評価の採用を想定している。



出所：McAfee 社 MVSION Cloud

図 2-5　スコアカード方式（例）

電力分野でも活用可能な制御製品向けのセキュリティ認証である EDSA 認証との違いを見ると、CPIC 認証の方がより範囲が広く、動的にリスクを反映する形を目指していることがわかる。

項目	CPIC認証	EDSA認証
目的	サプライチェーンリスク管理 エンドユーザーの調達時のリスク判断（コストとの比較判断も含めて）に活かすことを目指す。	制御システムのコンポーネント（製品）のサイバー攻撃に対する基本的な耐性を示す。エンドユーザーの仕様書に盛り込まれることを目指す。
主体	CPIC認証機関（US、欧州、日本、イスラエルなどに設置される予定）	ISCIによって認定された認証機関（日本ではCSSC認証ラボラトリ）
方法	リスクスコアカード形式・ベンダー自己認証 （＋CPIC機関の事後アセスメント）、要件を全てを満たすこと求めないチェックリスト形式、更新は動的に反映（別途資料参照）	EDSA認証機関がISCSの定めたスキームによる静的アセスメント（更新した場合は再取得が必要）。要件をすべて満たすことが前提。
対象範囲	製品セキュリティ・開発体制（V字モデル）・事業者管理体制・調達先管理・保守運用体制（EDSA認証）	製品セキュリティ（セキュリティ仕様・実機の堅牢性テスト）・開発体制（V字モデル）
コスト	未定（エンドユーザーのサブスクリプションとアセスメント費用など）自己認証とすることでハードルをさげる	ベンダー負担（エンドユーザーは製品価格という形で負担）１型式：1,000万円程度。
実績	現時点ではなし	国内実績ありだが限定的
課題	（日本においては）実施主体が決まっていない（その他は別紙）	規制でない。エンドユーザーの仕様書に反映されていない。 静的なアセスメントのため、更新時の反映が手間。 グローバルもビジネス化失敗。一方的なベンダー自己負担。

出所：McAfee 社

図 2-6　CPIC 認証と EDSA 認証の違い

ICT SCRM WG2 における脅威分類とスコアカード評価項目案の比較を見ると、スコアカード評価項目案の多くが、ICT SCRM WG2 における脅威のうち「サイバーセキュリティ」に含まれることがわかる。

脅威カテゴリ	代表的な脅威の例	スコアカード評価項目案との比較
1. 偽造部品	偽造製品の流通・利用、偽造部品（HW/SW）の製品への組込み、配送過程での不正改ざん、偽造証明書、偽造サイト等。	偽造品が出回る脅威そのものは、項目案の脅威には直接対応しない。偽造部品の組込みは「⑦工場セキュリティ（製造工程）」、「⑥SCM下流（配送過程での不正改ざん）」に該当する。
2. サイバーセキュリティ	情報の漏えい、改ざん、不正アクセス・マルウェア被害等。ベンダからの情報漏えい、サプライヤ内での不正機能埋め込み等。	大半の項目案は本カテゴリに属する。範囲が多岐にわたり、①~⑦の要素を含む。機器とサービスの双方を対象としている。その他の要素として、社内情報システムを対象とした情報収集を含む。
3. 内部セキュリティの運用と管理	知識の欠如・教育の不足や、情報の管理運用不備（廃棄含む）、不十分なパスワード設定・アクセス制御等。	「①全体（組織）」の管理体制に該当する脅威が多く含まれる。製品の廃棄等の視点からは、「⑥SCM下流」にも一部該当すると見なせる。
4.システム開発ライフサイクル・プロセス・ツールに対する攻撃	マルウェアの混入、コンポーネントの開発段階における不正、リポジトリの操作、更新・配布機構の操作、OSSの脆弱性、海外製コンピュータ等。	「②ECM」「③開発環境」に該当する脅威が多く含まれる。組み込み機器関連の脅威は「⑦工場セキュリティ（製造プロセス）」にも関係する。
5. 内部脅威	内部不正やスパイの侵入、修理・メンテナンス中の改ざん等。	原則として「①全体（組織）」の内部不正に該当。ICT SCRMの分類はかなり細かいが、必要な対策は大きく変わらないものと見られる。
6. 経済的リスク	サプライヤの財務リスク、破綻・買収リスク、品質リスク、ロックインリスク、サプライヤー外部からの意思決定への関与、ずさんな管理に関する問題等。	項目案では該当する脅威を含めていない。サプライチェーンに関する企業経営リスク等を整理したものであり、サイバーリスクではない。
7. サプライチェーン固有のリスク	部品・材料の脆弱性を継承、サプライチェーン内の不正・改ざん、サプライチェーン構造の深さ、トレーサビリティの欠如、輸送・出荷中の改ざん、コンプラ違反、各レベルの品質保証不足、不十分な検品、情報開示・検査権限の不足等。	「⑥SCM上流」に該当するサプライヤからの調達プロセスに関する脅威を中心に、「③開発環境」「⑦工場セキュリティ」の範囲まで言及。サイバーに限定せずサプライチェーンの構造的問題にまで切り込んでいる。
8. 法的リスク	知財・ライセンス（国際的係争を含む）、消費者・中小企業からの訴訟リスク、個人情報、コンプライアンス、犯罪への関与、制裁違反等。	範囲としては「①全体（組織）」に該当するものだが、ICT SCRMは分類がかなり細かい。エンティティリストに言及している点も特徴。
9. 外的サプライチェーンリスク	自然災害、地政学的リスク、労働問題、国際貿易問題、ガバナンスの問題、OSSにおける国際的貢献度の低下等。	サプライチェーン全体へ混乱を与える脅威であり、直接的なサイバーリスクではない。項目案とも直接対応はしない。

①：全体　②：ECM　③：開発環境　④：製品・サービス　⑤：SCM上流　⑥：SCM下流　⑦：工場セキュリティ

出所：” Threat Evaluation Working Group: Threat Scenarios”
https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report_0.pdf
（2021 年 3 月 21 日閲覧）を基に三菱総合研究所作成

図 2-7　ICT SCRM WG2 における脅威分類とスコアカード評価項目案の比較

また、「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）」との違いを見ると、基本コンセプトの違いとして、サプライチェーン全体のサイバーセキュリティ対策を対象とする CPSF に対し、スコアカード案は製品・サービスの評価を対象としている。ゆえに、それぞれ以下の目的で利用可能であると整理できる。

- CPSF（第Ⅲ部）における SC 項目は、調達元組織が複数の調達先を評価する目的で利用
- スコアカード案は、製品・サービス提供元（調達先）が、複数の調達元へ説明する目的で利用

ID	要求事項	スコアカード案との対応関係
CPS.SC-1	取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する。	直接の対応関係なし（メタ要求に該当）。調達元の基準において、製品・サービスセキュリティ品質基準、責任範囲を合意するためにスコアカードを活用可能と考えられる。
CPS.SC-2	自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	直接の対応関係なし（メタ要求に該当）。重要業務で用いると判断された製品・サービスを評価する際の基準としてスコアカード案が活用されること等が考えられる。
CPS.SC-3	外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	間接的に対応。製品に係る組織的対策は「①全体（組織）」でスコアカード項目案においても評価されている。
CPS.SC-4	外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する**他組織の提供する製品・サービスが適合していることを確認**する。	最も直接的な対応関係がある。適合性の確認のためにスコアカードを用いることが可能。ただし、スコアカード案は、製品に係る周辺プロセスまでを対象とし、間接的に他項目の評価を含む。直接的には、「③製品セキュリティ」が該当。
CPS.SC-5	取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	間接的に対応。製品に係る人員及び関係者の役割等（①全体（組織））や、製造設備の要員管理等（⑦工場セキュリティ）に対応。
CPS.SC-6	取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	間接的に対応。製品のテスト（②ECM）等。監査は、実施済であれば当該項目のスコアが好評価になる。他の形式の評価の一種としてスコアが該当すると考えられる。
CPS.SC-7	取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。	直接の対応関係なし（メタ要求に該当）。スコアが不正（虚偽のセルフアセスメント等）であった場合に、評価組織からのペナルティ制度を運営するような場合に該当。
CPS.SC-8	自組織が、関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報(データ)を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。	間接的に対応。製品に係るSLAの明示、文書の開示等（⑤SCM上流）。
CPS.SC-9	サプライチェーンにおけるインシデント対応活動を確実にするために、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。	間接的に対応。製品に係る脆弱性対応、パッチ配信等（⑥SCM下流）。
CPS.SC-10	取引先等の関係する他組織との契約が終了する際(例：契約期間の満了、サポートの終了)に実施すべきプロシージャを策定し、運用する。	間接的に対応。製品に係るSLAの明示（④SCM上流）、廃棄手順・サービス終了条件等（⑤SCM下流）
CPS.SC-11	サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する。	直接の対応関係なし（メタ要求に該当）。各組織のスコアカード利用方針や、スコアカード方式自体の継続的改善等に関係。

図 2-8　CPSF とスコアカード評価項目案の比較

3. サプライチェーンを支える基盤インフラ技術に関する調査

3.1 基盤インフラ技術の最新動向

3.1.1 調査概要

5G 技術や次世代クラウド基盤技術など、サプライチェーンを下支えする基盤インフラ技術の構成要素、アーキテクチャ、セキュリティ等に関して調査を行った。

(1) 背景・目的

今後の社会インフラ（電力、工場等）は仮想化基盤の上のアプリケーション（ソフトウェア）として実現される可能性がある。社会機能を維持していくために、その基盤（物理基盤、仮想化基盤）を構築、維持、運用・保守する能力の確保が必要と考えられる。

そこで、本調査では、基盤インフラが抱える課題について包括的に検討し、我が国としての基盤インフラ構築、維持、運用能力の獲得に向けて、幅広い専門家からなる勉強会を通じて、今後必要な施策に資する課題整理等を行った。

特に、次世代基盤インフラを支える各種技術のうち、我が国において優先して獲得する技術について、明確化した。

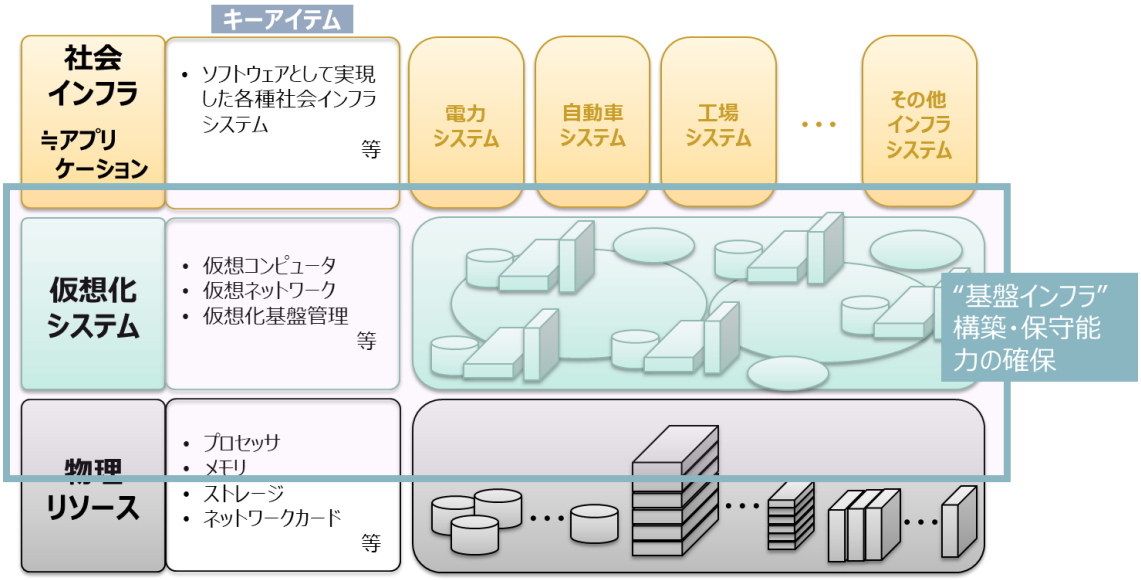


図 3-1　基盤インフラの範囲

(2) 検討の方向性

必要な基盤インフラ技術の検討にあたり、アプリケーション（ユースケース）を踏まえて、各ユースケースを実現するアーキテクチャから、全体の共通要素として「基盤インフラ」を設定し、開発すべき技術要素を明らかにするアプローチとした。

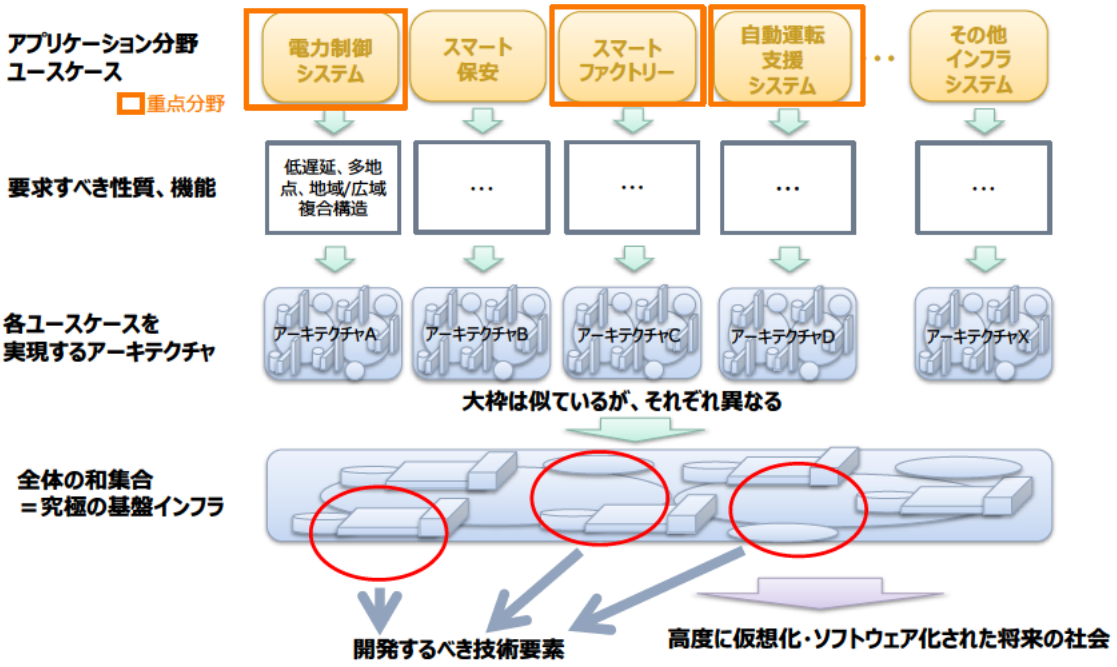
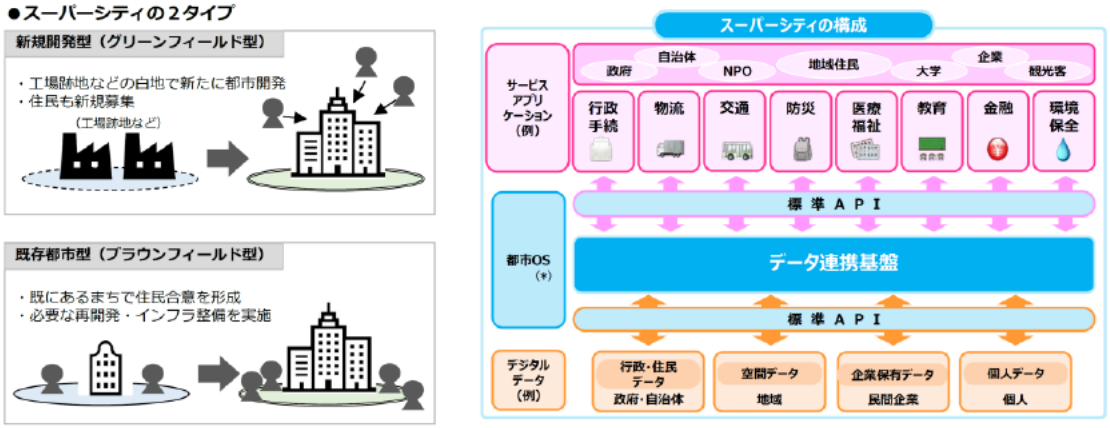


図 3-2　検討の方向性①アーキテクチャとアプリケーションのイメージ

また、各ユースケースを実現する共通要素を踏まえた「基盤インフラ」の利用シーンとして「スーパーシティ」を想定し、2025 年の大阪万博での実装も視野に入れて検討を進めた。

【参考】スーパーシティ構想
- 5/27に「スーパーシティ法（改正国家戦略特区法）」成立。従来の国家戦略特区制度を基礎として法制度を整備。
- 複数分野の同時の規制改革や、複数の先端的サービス間でデータを収集・整理し提供するデータ連携基盤の整備事業を法定化し、事業の実施主体が国や自治体等に対し、その保有するデータの提供を求めること等を可能にした。
- 今後、ごく少数のエリアを（透明なプロセスで）選定。



出所：左下図：内閣府資料（https://www kantei.go.jp）
右下図：内閣府資料（https://www.cao.go.jp/houan/doc/201_1gaiyou.pdf）

図 3-3　検討の方向性②スーパーシティの想定

3.1.2 調査手法

調査は、文献調査、ヒアリング調査、及び勉強会による議論により実施した。

(1) 勉強会の設置

基盤インフラ技術に関する検討を進めるべく、勉強会を設置した。

勉強会を開催するため、構成員の委嘱、検討会の日程調整、開催案内（出欠確認）の作成・発信、オンライン会議手段の確保、資料の準備、議事録の作成等を行った。

勉強会の構成員は、昨年度に設置した勉強会をベースとし、表 3-1 の通り構成した。

表 3-1 「基盤インフラに関する勉強会」構成員

No.	お名前	ご所属
1	浅井 大史	株式会社 Preferred Networks リサーチャー
2	飯田 健一郎	NTT リミテッド・ジャパン株式会社 代表取締役社長
3	上坂 利文	NEC サービスプラットフォーム事業部 事業部長
4	江崎 浩（座長）	東京大学大学院情報理工学系研究科 教授
5	大江 将史	国立天文台情報セキュリティ室助教/情報セキュリティ室次長
6	太田 雅浩	富士通 クラウドサービス事業本部 理事 本部長
7	奥野 通貴	株式会社 日立製作所 研究開発グループ テクノロジーイノベーション統括本部 エレクトロニクスイノベーションセンタ コネクティビティ研究部 部長
8	榊原 彰	日本マイクロソフト株式会社 執行役員 最高技術責任者
9	佐藤 剛	NTT コミュニケーションズ クラウドサービス部 担当部長
10	澁澤 栄	東京農工大学 卓越リーダー養成機構 教授
11	関谷 勇司	東大情報理工学教育研究センター 教授
12	田中 良夫	産業技術総合研究所 セキュリティ・情報化推進部 部長
13	冨安 寛	NTT データ 技術革新統括本部 執行役員 本部長
14	成迫 剛志	デンソー
15	平井 真樹	NEC サービスプラットフォーム事業部 部長代理
16	藤澤 克樹	九州大学 マス・フォア・インダストリ研究所
17	濱野 賢一朗	NTT データ 技術革新統括本部技術開発本部 先進コンピューティング技術センタ
18	松本 修	富士通 クラウドサービス事業本部 ファウンデーションビジネス事業部 事業部長
19	丸山 宏	株式会社 Preferred Networks フェロー
20	宮田 裕章	慶應義塾大学医学部 教授

（2020 年 9 月 1 日時点）

(2) 勉強会の開催

勉強会については、昨年度に引き続く形で開催した。昨年度は 1 回の会合を実施したため、今年度は「プレ会合（メール審議）」及び「第 2 回」として勉強会を開催した。開催概要は以下の通りである。

表 3-2　プレ会合　開催概要

日時：2020 年 8 月 19 日(水)　～　2020 年 8 月 26 日（水） 開催形態：メール審議 議事（意見をいただきたい内容）： (1) 研究開発の方向性について (2) 調査結果について 配布資料 討議資料

表 3-3　第 2 回勉強会　開催概要

日時：2020 年 9 月 1 日（火）10:00～12:00 開催形態：オンライン開催（WebEX） 議事： 1. 開会 ・趣旨説明 ・委員紹介 2. 議事 (1) 資料説明 (2) 自由討議 3. 閉会 配布資料 議事次第 資料 1. 委員名簿 資料 2. 第 2 回勉強会検討資料 資料 3. 研究開発計画（骨子素案）

3.1.3 文献調査結果

(1) スーパーシティ内のアプリケーション動向（電力）

1) 発電システム

- 発送電分離や小容量電源の増加により、送配電事業者の制御所に依らず、発電事業者自らが発電というアプリケーションを統合的に管理するアーキテクチャの重要性が高まる可能性がある。
- 拠点内制御ネットワークに仮想化技術を適用する場合、仮想ネットワーク技術を活用し、複雑化するケーブル配線の単純化の効果等が期待できる。
- 遠隔制御を高度化し、より細やかな操作を実現するためには、低遅延・高品質・セキュアな通信を実現し、アナログ通信の性能に近づけていく努力が必要となる。

2) VPP/DR（仮想発電所/ディマンドレスポンス）

- アグリゲータは物理的な場所に限定されず、リソースを集約し一体として扱うことを可能とする仮想基盤とみなせる。システムはクラウド上に構築されることが基本であり、API を利用して機能を実現する。また、系統内で大規模な発電所と同等の意味合いを持つため、高可用性・高信頼性を保った稼働が求められる。
- スマート化された大量のリソースを統合監視するためには、DERMS（分散電源マネジメントシステム）とリソース間のネットワークを高品質に保つと同時に、なりすまし等を防止するためのセキュリティ実装が求められる。
- スマートメーターデータは一般送配電事業者の所管する専用ネットワークを通じて収集される。メーターデータは様々な活用可能性が期待されており、大量のメーターから様々なデータの収集を、安定かつ低コストで可能とする通信インフラ技術への期待がある。

(2) スーパーシティ内のアプリケーション動向（スマートファクトリー）

- 多品少量生産をニーズに製造ラインの柔軟化が求められることから、コントローラ間ネットワークの無線化が進展する。また、映像分析やロボ協調を背景に、情報系ネットワークの無線化も進む。これにより、様々なネットワークが統合された工場ネットワークの必要性が高まる。
- PLC のソフトウェア化や製造装置の遠隔制御により、フィールドネットワークも無線化。MEC PLC によるフレキシブル製造の実現も想定される。

(3) スーパーシティ内のアプリケーション動向（自動車）

- 自動運転では、クラウド、MEC、車載のどこでコンピューティングを行っても車は意識しなくていいアーキテクチャが想定される。周辺環境まで含めた拡張されたクラウドのような基盤が必要になると考えられる。
- 電気自動車の技術の発展により、自動車サービスと他の産業分野サービスとの接続が

拡がることが予想される。

(4) スーパーシティ内のアプリケーション動向（スマート保安）

- IoT の活用による運転効率や保安の効率化を進める一方、セキュリティリスク等の観点から、ハイリスクである制御ネットワークとは独立した仮想ネットワーク上でのデータ収集・解析のアプリケーションを実現可能
- 無線ネットワークやドローン等を活用することで、ケーブルを延伸することが難しい場所や、人間が立ち入りにくい場所のモニタリング基盤の実現が期待される。

3.1.4 ヒアリング調査結果

(1) プレヒアリング結果

勉強会（プレ会合）に先駆けて実施した、勉強会委員や関連研究者等へのプレヒアリング結果を以下に示す。

表 3-4　プレヒアリング結果

No.	内容
A氏 （電力）	• 抽象度を上げた場合、共通項は仮想サーバ技術と仮想ネットワーク技術に収れんするのではないか。 • サイバー・フィジカルの要素は重要。アプリケーションの視点から必要な仮想基盤技術を検討するべき。
B氏 （自動車）	• 自動運転では、エッジコンピューティングを行う場所が移動する点に特徴がある。イメージとしては、クラウド、MEC、車載のどこでコンピューティングを行っても車は意識しなくていいアーキテクチャとなる。周辺環境まで含めた拡張されたクラウドのような基盤が必要になるのではないか。 • サービスメッシュを活用したデータとアプリのやりとりは機能だけではなく、運用、セキュリティ等の非機能も重要。 • 分散コンピューティングにおいて、仮想ノードがゼロトラストで動くようにするためには、ソフトだけでなくハードも関係する。ソフトウェア処理を行うために最も効率がよいハードウェアができればコストパフォーマンスは向上する。
C氏 （ベンダ）	• ネットワーク技術であれば、マルチテナントとしてのセキュリティ、仮想的に独立した安全なネットワークの需要はあるのではないか。現状は基幹や地域の専用網が非効率に点在している部分がある。 • 国内で技術を持つかだけでなく、オープン技術か商用技術かの観点も必要。安定性を重視する領域では商用技術がまだ強い。国内外の観点では、同盟国との協力も選択肢となるのではないか。 • 単独の企業で基盤技術開発を実施するのは厳しい。国内での技術開発はオープンソースにコミットする座組を作るのが有効ではないか。オープン技術は、二つ以上のオープンソースで同じものを開発し、依存性を回避する必要がある。 • 共通基盤技術は公共財の性格を帯びてくる。取引場のように必要量を競売するような形式もありえるかもしれない。 • 実証においては、変革の必要性が強い状況にある自治体等も選択肢ではないか。
D氏 （研究機関）	• 仮想化技術の適用範囲を考える時にレジリエンスの観点は重要。基盤がダウンした時に産業インフラや制御システムに近いサービスほどロバストである必要がある。依存関係も必ず複雑化する。スーパーバイザのようなものも必要になるはず。 • 地域インフラを仮想基盤として実装することは各国で行うべき範囲。メガプラットフォーマーはデータ基盤は作るが、個人に手を差し伸べる部分までは、中々手を出さない。 • 交通サービスでいえば、ローカルシステム単独で自動運転や信号制御は破綻しない仕組みが必要。電力サービスもデマンド制御に該当するような範囲は、

No.	内容
	BEMS 側で出来ることが望ましい。 • 全体のシステムがダウンすることは許されない。ドメイン毎の特性により、品質要件、冗長性等の要件が異なる。 • ドメインの特性やローカルな規制要件を仮想基盤上で実現、管理運用するための技術は重要になると思う。 • 制御に関連する通信は低遅延要請が強い。遅延がイラつきで済むサービスか、制御の失敗になるかでは大きく異なる。 • 現状で LTE は障害時に全体がダウンするが、ローカル 5G は個別に生き残る可能性がある。また、伝送距離の短さが逆に規制対象にならないという自由度を生んでいる面もある。 • データの計測から考えていかないと、特定のドメインは他のドメインに追従するだけの存在になるおそれがある。 • 電力や交通等は低遅延で信頼性のあるネットワークが必要。スマート工場や保安は映像を使う場合に大容量 NW が欲しい。
E氏 (ベンダ)	• 低レイヤの基盤構造は海外製品に依存している現状。自前で賄いきるのは難しい。クラウドに関しては、コンピューティングリソースが特に難しいが、通信機器も Nokia、Ericsson が強く、国産では NEC くらいではないか。 • ミドルウェア、フレームワークの領域でも例えば機械学習では、Tensorflow や PyTorch が強く、Chainer も終了する方向となった。MEC のフレームワークとしては、Saguna 等があるが見通しは不透明。上層ミドルやアプリ、API マネジメントに注力すべきではないか。 • ５G でいえば、NFVO,VNEM の部分に課題がある。ソリューション要件に応じた E2E オーケストレーション技術が必要。RAN/コア網の双方の機能ブロックインターフェースについてオープン化された前提(現状で O-RAN Alliance が存在)、クラウドネイティブアーキテクチャで、マイクロサービス化、コンテナ化、CI/CD、運用の完全自動化が理想。 • 5G システム全体で見た時に、部分的障害が全体のダウンやパフォーマンス低下につながらないよう、障害点の早期発見や切離し、CU や DU（アンテナまではいかない程度）までを MEC として必要な機能を配備し、分散コンピューティングバリエーションを強化。E2E での関係するすべての機能を統合制御し、マルチテナント、複数管理主体向けへの拡張する。 • 5G 全体のソフトウェアセキュリティガイドライン、ハードウェア脆弱性検知データプライバシーの需要も根強い。 • 特定分野の活用について、例えば工場の無線化における通信要件としては、（HMI-PLC 等のコントローラ間 NW の無線化）数十 ms～数百 ms/ 品質 10^-6/ 帯域：数 Mbps 高品質、低遅延（ビデオ等、ロボ協調の世界）～数秒/ 品質 －/ 帯域：数十 Mbps～数 Gbps 超広帯域（フィールドネットワークの無線化）数 ms～数十 ms 品質 10^-6 帯域：数 Mbps 超低遅延、高品質といったような要求が大まかにはあるのではないか。
F氏 (ベンダ)	• 全てを日本製で賄うのは難しいため、適用範囲は明確にする必要はある。OSS を利用するという選択になると思う。 • デジタルツインのように現場と仮想空間に同じものが存在し、一対一に対応しているような世界観であればわかりやすい。5G では低レイヤから上位層にあげる部分は明らかに仮想化技術であると思う。デジタルツインで下を上にあげる部分がどうなるかが重要。その上にアプリケーションがあるという形が自然。 • ID 基盤等のバージョンアップで他がダメージを受けることもあるので、統合基盤内で管理できていることは重要。 • ハイブリッド基盤も当たり前になってくるイメージ。ただし、エッジはエッジでリソースを確保しておいてほしい領域は必ずある。
G氏 (ベンダ)	• ミドルウェア層の技術が欠けてきてしまっていると思う。パブリッククラウドの PaaS に慣れ始めてしまったユーザは同等の UX を求める。 • 可用性を担保した DB 基盤のミドルウェア、メッセージ基盤のミドルウェアに課題意識がある。 • パブリッククラウドの背後で失われてしまっている技術には懸念がある。MySQL は OSS だが、MySQL をスケールさせる基盤技術（例えば Amazon RDS）や BigQuery のようなサービスはクラウドサービス事業者に閉じている。手元で動かしたくても代替手段がない。 • 国内にも技術要素はあると思うが、需要サイドに１から作りたいというモチベーションはなかなかないと思う。 • DB の話には特に危機感がある。他社とも連携して、PostgreSQL をスケールアウトさせるための取組みは行っている。アメリカやロシアからも関心を持たれている。国の施策からは学識者からのサポートやユーザ企業の実証への橋渡し等は有効と思う。 • 人材育成は重要だが、基盤技術を手放している現状では育成後にも海外への離脱リスクはある。手元に技術がいる。 • パグリッククラウドの背後に潜む技術を明確にするといい。分散合意のミドルウェアやサーバサイドのゼロトラスト技術等もある。

No.	内容
H氏 (ベンダ)	• 仮想基盤技術を適用する分野によって個別の特徴が分かれる部分は多いと考える。アプリケーションの要件の違いがフィジカル層で必要になるスペックの違いになるケースもありえる。和集合を考える際に、現実的でない大きさの基盤にならないよう配慮が必要。 • IoT システムにおいて、IT の領域は標準化が進んでいる分、共通化しやすい部分が大きいと思われる。一方で、OT 領域は、インターフェース間の仕様差が大きく、ベンダ依存もある。インターフェース交換を行う層が求められるのではないか。通信プロトコルにも個別仕様が多いため、標準化によるベンダの壁を越えた相互運用性の確保が前提になる。 • IT と OT の境目のセキュリティをどう確保するかが重要。OT 系で組込系 OS で稼働しているシステムには、クラウドのセキュリティサービスがそのまま適用できないことがある（同じ Linux であっても、Runtime の不足等が起こる）。エッジサイドにクラウドのサービスをオフロードして同等のアプリケーションを動かすような工夫も必要ではないか。 • 共通 MIB（Management Information Base）とベンダ固有 MIB に関して、共通 MIB 部分は同じものを使うようにしていかなければデバイスが多くなりすぎてしまう。
I 氏 (ベンダ)	• 基盤のライフサイクルを意識しなければいけない。ハードとソフトで異なる。構成要素の長期利用は製品ライフサイクルが終了リスクもあるため、切替え戦略も必要。高頻度の更新がある部分は無停止でアップデートする技術等も重要になる。 • ハイパーバイザー（HV)の技術が大事である。ハードの更新に影響されない HV が理想。基盤を持っていないと重要性にも気づけない。CPU の脆弱性をなぜ他人事で済ませられたのか、という問題。少なくともスキル面では手の内に押さえるべき。 • エッジには横のスケーラビリティ技術だけではなく、縦のスケーラビリティも必要。電力消費や冷却の最適化も求められる。 • ゼロトラストのように完全に守り切れないことを前提にしたコンセプトは必要。進化する脅威へ社会基盤も対応しなければならない。 • データ層では、AI が学習するためのデータをどこに貯めるかは重要。セキュリティの問題もあるが、パブリッククラウドでは、置くときは無料で出来たとしても、引き出すときに大きな費用がかかることがある。エッジに公的な主体の管理するデータプール等あると嬉しいのでは。 • 仮想基盤も物理基盤の上に構築されるため、物理的な冗長性は要考慮。基盤にソフトウェアを適合させる領域も日本は苦手。 • デバイスは北米製品に依存。ロックインの懸念もあるが、競争はあり、OSS もあるため実害はあまり感じていない。 • OSS のトップリーダーと企業で引っ張り合いにならないように、重点領域と競争領域は見極めないといけない。自動車のように世界的にシェアが高い産業分野では、欧米に対しても頑張れるのではないか。 • 研究開発体制の組成も重要。方向性を揃えて無駄を排除。国産の製品を売るという形にはこだわらない方がいいのではないか。
J 氏 (ベンダ)	• プラットフォームの米国依存については、EU の GAIA-X が協調路線をとるか、競合路線をとるかは気にしている。 • ユーザはいまだにクラウドにデータを置くことに慎重な面もある。エッジは逆に受け入れられやすいかもしれない。 • 製造業の生産現場ではエッジだけで出来ることもかなり多く、必ずしもクラウドと接続する必要があるということでもない。エッジでのデータ解析による予防保全の取組み等も進んでいる。外部ネットワークにデータを渡す際には必要性の検討が重要ではないか。 • 無線化はコストメリットには期待するが、切断リスクへの懸念が受け入れられるかは未知数。FA 機器のセキュリティを担保するのであれば、ゼロトラスト的な発想による保護も求められてくる。 • 製造業における仮想基盤の適用先としては、サプライチェーンのトレーサビリティ確保は重要と考えている。配送は必ず施設をまたがるため、共通の仕組みが欲しい。宅配業者のデータフォーマットに標準化する等も考えられる。ブロックチェーンも有望。

(2) ヒアリング結果

勉強会後に実施した、勉強会委員へのヒアリング結果を以下に示す。

表 3-5　ヒアリング結果

No.	内容
A委員 (2 回)	• 1 社の基盤上で複数のユーザが乗るならやりやすいが、複数社の基盤上となると難しくなる。特に、ネットワーク制御や認証などが難しい。 • 複数社前提であれば、最終形として、事業者同士を結ぶところを考えるか、あるいは基盤層のミドルウェア的なもの（全体をカバーするもの、オーバーレイ）が必要になる。そこを作り上げるための技術や、ユーザ層の要求をどう実現するかに関係する。調査も大きな割合を占める研究課題になる。 • 認証やネットワーク形成が取り出しやすい課題と考える。ネットワークのセパレーションの上で複数事業者が動くとすると、認証を行い、コンポーネント単位でデータを受け渡しできる認証基盤が必要となる。認証だと中央集権的になるので、誰が作るのかが課題。 • 認証とは、部品を繋げるための認証であり、部品を繋げて作ったサービスの上のユーザ認証は各事業者がやる。認証と認可を受け持つ IDP（Identity Provider）のような仕組み。 • 処理をコアにするかエッジにするかの技術は 5G にないので開発すべき。一方で、コアとエッジが複数事業者になっても実現できるような基盤を考えるべき。その時にミドルウェアが必要になる。そのミドルウェアが処理をコアにするかエッジにするかの振り分けを行うか、ユーザ側で指示できるような基盤とすべき。 • オーバーレイ的に折り返しを早くするためにエッジに導くのはすぐにできるが、今の携帯の技術は一旦コアを折り返しになっているので、コア折り返ししないで分散基盤として活かす通信技術はまだ無い。 • 最もクリティカルでコストがかかるところを共通化することが重要ではないか。スケーラビリティする上で、認証 ID の統一基盤があって、認証 ID により自社と他社のリソースが区別される部分と、適切に共有できる部分がある、ということを最初に実現すべきではないか。 • 基盤インフラのアーキテクチャは誰もわからない。まずはアーキテクチャを考えることが必要である。 • 検討体制も難しい。個々の技術は、それぞれ得意な各社に委託すればよいだろうが、それらを統合するための組織が必要である。オーケストレーションのための組織が必要である。それを初期の研究課題にしても良いのではないか。 • エッジは通信キャリアに頼る部分が多く出てきそうである。認証・ID 基盤とスケーラビリティの基盤、データの連携・管理基盤が必要なのではないか。その実現のために、仮想化技術やコンピューティング技術等が入ってくる。
B委員 (2 回)	• スーパーシティであれば、様々なユースケースが活かせるのではないか。分散クラウドのようなものも、スーパーシティであれば、NW やコンピューティングリソースなども多様性が求められるので、都市設計と一緒にやる必要がある。 • ユースケースを想定すると、いくら良い技術でも使えないこともある。計算性能やストレージ性能は大規模化しても国内企業で可能だと思うが、エッジにリソースに置くなどは伝送の遅延がありなるべくフロントに置くことになる。一方で、分散が広がると管理機能が現状では限界がある。 • 具体的に必要な技術としては、まずクラウド基盤の多層化、分散クラウド基盤があるのではないか。BCP を考えると、オペレーションの拠点・人も含めて分散が必要ではないか。 • セキュリティについては、本人性確認の検討、セキュリティの実装技術の標準化が必要である。 • 産業別に要求されることに対して越えなければいけないハードルの設定は、産業側（自動車、小売等）から出てくるのではないか。電力、自動車など、具体化すればキャパシティが足りない、距離が遠い等の要件は出てくる。また、活用シーンがコストに見合わずなかなかできない部分がある。効率性やマネタイズを組むことが課題である。
C委員 (2 回)	• 認証・サイバーセキュリティに係る部分は、様々なレイヤーのセキュリティをどのようにゼロトラストアーキテクチャに持って行くかが課題ではないか。 • スマートシティについては、平成 30 年度の SIP でアーキテクチャが検討されており、リファレンス・アーキテクチャ、ホワイトペーパーが公表されている。 • 分野横断的に大量データの収集・蓄積・解析を可能とする管理技術については、スーパーシティ等の内部で大量のセンサ・デバイスのデータを対象としたデータ集配信技術が必要になるのではないか。ライフレコードやヘルスケアレコード等の個人情報の扱いも必要となる。

No.	内容
D委員 (2回)	• エッジコンピューティングの性能がどれくらい出るか等は見えているが、何年後にアウトプットするか。万博のユースケースイメージがあると、あるものを使って形を見せることができるのではないか。 • NW基地とサーバ（仮想マシン）が一体化して、F/Wやロードバランサが S/W で実現される。NWとサーバの境目が無くなってきている。NWプロセッシングをするのか、コンピューティングプロセッシングをするのかで性能は違ってくるため、そこはチャレンジ的な課題となる。 • 5Gトライアルは、欧米系の技術も活用されており、日本産業の復活につながるかどうか。AIの場合はデータを貯める時間が必要である。インフラのトライアルをしてユースケースを増やしていくことが必要だと考えている。
E委員 (2回)	• ある分野を想定し、多様な要件や現場環境における実証を行うことが良いのではないか。多種多様なアプリケーション要件、周期的・低遅延通信（制御通信など）、多端末・大容量伝送（遠隔監視など）、ベストエフォート（オフィスPCなど）等、様々な現場環境・制約があり、障害物や干渉などで通信環境が常に変化する、あるいは限られた計算処理能力（端末側の制約等）あるなかで、どのように活用できるものを構築していくかが重要である。
F委員 (2回)	• メガクラウドは利便性が高くロックインに陥る可能性がある。特に、「永続層」を実現する技術・サービスの獲得（特にDB as a Service、Queue as a Serviceの部分）について、既存のミドルウェア等をベースに、オープンソースコミュニティと連携しながら開発を行う。成果はOSSで公開して育てていくのが良いと考えている。 • 各国が独自にサービスをつくることは経済合理性が無いため、自分でわかっているものが世界中で使われた方が国益にかなうのではないか。
G委員	• データ基盤、トラスト基盤、データ流通について検討している。ドコモのプレスリリースが出ていたものが近い。ハードウェアが地に足のついたもの。サービスの開発者は日本人ではなくともよく、ソフトウェア技術に力を入れ、付加価値をつけながら、オペレーション用のソフトウェアだけ日本が提供し、それに対応したハードだけを日本が作るというもの。 • 抽象化レベルを再定義することで、より柔軟な抽象化＝API（アプリ寄り）によって、疎結合なシステムをコアに持っていれば、最低限の機能はオープンソースで作るとなると、エコシステムが自由な形で発展するのではないか。インターフェース、機能としてそこがベースとなりつつ、速度などで差別化が図れるのではないか。 • 基盤に対してステークホルダーになれること、すなわち強みのある技術は変遷していくが、コアにある技術に対してエコシステムに取り入れられることが重要であり、コアに対して発言力を持っていないといけない。 • 日本で一番強みがあるところは難しいが、工場系、工作機械、自動車産業など、強みがあるビジネスを妨げずに、ソフトウェア化が進む中で新たな競争力を育てていくのではないか。今は、スマートフォンなどのOSを作る会社が強いが、全てプラットフォーマーに握られずに、見えているものから発展していくことが重要では。通信は土管、半導体は利益率が低いと呼ばれ、付加価値を本来つけられるのに、日本が技術を手放してしまったこともある。トヨタも強いが、モビリティに力を入れている。車が移動する箱としてソフトに変わっている。そういうことを手助けする、損なわないような形のインフラ基盤としていくことが重要である。 • オープン戦略とクローズド戦略の取り方は難しい。オープンソースコミュニティの敷居の低さをうまく使い、ハードをうまく取り込んで産業を強くしていくのがよいのでは。 • 相互接続検証や実証はよくやられているが、研究開発は事業に関わるので難しい。アーキテクチャは変わるものとして、競争領域と非競争領域を整理することが重要である。そして、継続的な発展が必要である。 • 新しいビジネスを生み出すのは企業の使命である。基盤が日本になければ、参入障壁となる。オープン化をすることにより、強みのある産業を維持するとともに、新しい産業を生み出すということが必要である。付加価値がどんどん情報になっているので、通信的な考え方、自立分散協調という考え方を入れていくことが有効だろう。 • 相互接続や実証のところはオープンにしやすいが、研究開発となると1社となってしまう。学の役割が重要ではないか。ある意味中立でコア技術を開発する場として、複数の企業を取り持つような形で研究開発を進めたらよいのではないか。 • 個人（indivisual）が見えるという場も必要である。官としては、スポンサーする企業、人材を送り出す企業へのサポートが有効ではないか。コミュニティは「人」なので、コミュニティに対しては「人」の支援が必要。

No.	内容
H委員	• これまで取り組んできたレイヤー分業モデルは世界との接続性が担保されるメリットがある。しかし、スペックがかなり飛躍するところでは、今までのレイヤー分業モデルでは実現できないと思ったため、フルスタックの見直しを行う方針とした。サービスオリエンテッドで検討しないといけないと考えており、サービス実現のための要求条件について議論しているところ。 • ユースケースは、2030 年を目標年度として定めて、各社からワークアイテム（ユースケース）を出してもらった。 • 既存のアーキテクチャをすべて置き換えるつもりはなく、新しい技術でしか実現できないサービスの実現を目指している。2 桁レベルの改善を実現するためのアーキテクチャがどうあるべきか議論中であり、一つのレイヤーだけではなく、レイヤー全体として検討すべきだと考えている。 • 世の中は性能を要求してくるが、電力消費量とスピードの融和の解は、現状の延長線上には無いと考えている。デジタルツインが標準化されてくると、その流れの中で現在の標準とは別のものに変わってくることを期待している。ユースケースを見せながら技術を普及させ、ゆくゆくは日本の技術でうまく競争優位なものを持っておきたい。 • WG 活動では様々な議論がなされており、その中にはアーキテクチャ議論も含まれる。テーマに対して、WG やタスクフォース（TF）が設定されたり割り当てられたりして議論が行われている。これからも短い間隔で様々な成果を作成・公開していこうと考えている。業界の様々な方が集まる場ではコンセンサスを形成していくことが重要なので、具体的なドキュメント（内容・議論）に落とし込むことが重要と思う。
I 委員	• 現在勉強会で示されているアーキテクチャは、すでにクラウドサービスで網羅されている。社会インフラ部分はインダストリー毎にアーキテクチャを作るのだと思う。 • メガクラウドと日本が圧倒的に違うのは物理リソースのレイヤーである。メガクラウドの設備投資費は年間数千億円レベルであり、DC のリージョンは世界中に広がる。さらに、世界中のリージョンをつなぐケーブル（海底含む）も他社と共同で張り巡らせている。今から IaaS に参入するのは得策ではない。 • 逆に、IaaS よりも、PaaS や SaaS といった上のレイヤーはまだ投資が少なくて済むので、ありうるのではないか。日本は欧米と比較して SIer に構築ノウハウが集積されているので、電力や事業者等のアプリエリアのサービスを確立することは優位ではないか。 • あとは、ゲームチェンジの技術を考えることはありえるかも知れない。

（同一委員に複数回ヒアリングしているケースはまとめて記載）

3.1.5 勉強会における議論

(1) プレ会合における論点と課題

プレ会合において提示された研究開発テーマの検討に関連する論点・課題は以下の通り。
（なお、一部、プレ会合に先駆けて実施したプレヒアリング結果からの検討内容を含む）

1) アプリケーションの想定（共通的に求められる機能の想定、個別の産業分野への適用性・ギャップ等）

- スーパーシティ（大阪万博）実証等を題材として考えることに概ね異論は見られず、前提としてよいのではないか。
- 個別分野課題の解決に活用可能な技術である必要がある。共通化部分が個別機能の性能をどう向上できるか。
- アプリケーション間連携は API 実装前提で考えるべきである。API 認証機能の強化も必要ではないか。

2) サービス／データ層を支える技術（仮想コンピューティング、エッジ基盤、サービスメッシュ管理、ビッグデータ解析等）

- 産業アプリケーションが稼働する基盤は、クラウドに依存せず災害時も必須機能は独立稼働可能であるべきではないか。
- 安定したエッジ基盤の開発を行うため、クラウド・エッジ間のマルチテナントを想定したスケーラビリティ管理、障害の検知・復旧、高エネルギー効率計算、アプリ機能無停止でインフラ基盤を更新等の技術等が求められるのではないか。
- スマート工場ではエッジ AI 活用も進展。データ処理基盤、保存ストレージもエッジ側で実現すべきか。コスト面に有利も。

3) 転写層を支える技術、フィジカル層との接続（仮想ネットワーク、ゼロトラストネットワーク、データ取得技術等）

- 単にスライシングでは新規性が不足。産業分野の要件が仮想ネットワーク技術によってどう実現されるべきか。
- 転写層でも前処理と分散処理が必要ではないか。日本の地理的特性から隣接地域と協調することは有効ではないか。
- IoT 終端は様々な OS、データフォーマットが混在。汎用的な集配信基盤開発がデータ活用のために必要ではないか。
- ネットワーク内のノードは信頼すべきではない。多様なノードの接続を前提としたゼロトラストセキュリティが必須ではないか。

4) 研究開発の進め方（OSS との関わり方、人材育成等）

- コア技術には OSS を活用すべきだが 1 社では難しい。チームとして OSS にコミットし、日本の影響力を向上させることを考えるべきではないか。ただし、OSS は開発コミュニティである点には注意し、運用を担う責任ある主体も必要。
- 特にミドル層の技術が失われつつある。パブリッククラウドベンダに閉じた技術が増えつつある。ハイパーバイザの技術やデータベース統合管理等の技術が国内技術者から失われないようにすべきではないか。
- 規制改革やデータの標準化等は研究開発と同時に求められる。特に OT 領域では現状バラつきが大きい。

(2) 第 2 回勉強会における論点と課題

第 2 回勉強会において提示された研究開発テーマの検討に関連する論点・課題は以下の通り。

1) 議論の方向性について

- スーパーシティを想定すること、仮想基盤技術を中心に据えること等の根幹部への異論はなし

- アーキテクチャの捉え方、現時点でどの程度まで具体的なアーキテクチャの想定を持つのかについての議論あり。研究開発体制内にアーキテクチャの検討自体を行うチームを設置する方向で一定の合意を得た。また、アーキテクチャ検討時に求められる論点への意見あり（個別の SLA 要求へどこまで応えるか、レジリエンス、ID 基盤、横断的セキュリティ）。
- 例示したテーマに加えて個別テーマのアイデアを提示する意見も数件あり（データのコンソリデーション、個人情報管理）
- 進め方部分では、運用技術と人材育成のテーマの取扱いに関する議論があったが、国内で有すべき技術スタックとそれを扱える人材が必要という整理で着地。

2) 分野別テーマについて

a. 分野別テーマについて（電力）

- 電力会社との会話でもディマンドレスポンス、アグリゲーションサービスが拡大する中でオープン化が進んでいる状況認識を共有している。
- 送配電や発電の所までリーチして、データを取得するかという点には迷いがあるのが実態。レイヤを分けて考えるしかない。
- 安全性、事業継続性が大きな課題となる。スーパーシティを想定することのメリットとしては、送配電まで管理するイメージをもたず、アグリゲータの範囲で考えられる点がある。

b. 分野別テーマについて（スマートファクトリー）

- データをどう取得するかが重要。単純に取得データを貯めて自動でアプリケーションを動かすよりもエッジ寄りで高度かつ複雑な処理を行えるようにすることが重要。
- リアルタイム処理をどう扱うかは問題になってくる。
- 現状、エッジ側で電力と計算資源を大量消費してリッチな処理はできない。ある程度の上限を仮定している。

c. 分野別テーマについて（自動車）

- 自動運転システムのどの範囲までをスコープとするかで情報量やリアルタイム性の要求及び難易度は大きく異なる。路地裏の走行や高性能ダイナミックマップまでいくとテーマが発散する。
- 社会インフラ基盤としてのテーマ性では信号制御等の交通管制の方が取り組みやすいかもしれない。
- エッジコンピューティングに関してはオートモーティブコンソーシアムがあり、インテリジェントドライビングのユースケースも整理されている。様々なベンダが参加し API 開発もされている。
- コネクテッドカーの取組みとして、CAN データの蓄積も始まっている。車載システムに何を乗せるのかも議論されているが、責任を誰が負うかが難しい。地図等の情報共

有がやりやすいのではないか。国全体で行えるのであれば望ましいのではないか。
- 自動運転自体の研究テーマは競争領域の面で難しい。他サービス連携の方がやりやすいのではないか。

d. スーパーシティ全体について

- アーキテクチャから､将来この分野はこういう要件が入るということを意識しながら、システムを考えていくフィードバックループが重要。end-to-end の SLA が重要。
- すべてのアプリの要件に応えられる基盤を作れるかには疑問。SLA の違いが個別の垂直統合アーキテクチャに陥る懸念がある。分野横断の理解に基づく SLA 定義が必要。
- アプリの要求に従おうとするアプローチは要求 SLA が高くなりがち。誰かに合わせすぎないという事も課題であり、折り合いのつけ方も考えなければならない。
- 電力では要求されるべき性能を均一に出せるような気がするが、ファクトリーなどは業界の中でも大きさやモノが異なるので、要求事項は様々になるのではないか。共通化できるかにやや懸念。
- 電力や自動車のアーキテクチャの議論は規制体系にまで踏み込まざるを得ない。クラウド側で制御をすることになると、制御についての責任もクラウドに移行する。一方で、軽いテーマは事業者サイドで議論できる。
- エッジ側で処理できる情報量は比較的大きいのではないか。
- スマート保安は METI として取り組もうとしている範囲なのでやりやすさもあるが、将来ある程度の標準化をするなかでの課題も見込まれる。また、ほとんどの処理がクラウドになるかもしれない。
- 自動車と電力にまたがる範囲で､EV 充電をどうするかは課題である。電力網に供給される電力量が EV 普及と共に不足することは明らかであり、充電量予測に基づく系統制御等は着眼点になるだろう。
- 自動車と電力制御システムで求められる応答速度は異なるだろう。同じプラットフォームで制御するのであれば、要件を整理して共通認識を持つことが必要。

3) 研究開発計画について

a. テーマ選定について

- アーキテクチャがスコープなのか、アーキテクチャ内で用いる技術がスコープなのかが混乱しないようにしないといけない。技術自体はアプリケーション毎に異なっても構わないのではないか。
- 個々のテーマ検討を別々に行ってしまうとアーキテクチャが別々のものになってしまう。全体を横串で見るアーキテクチャ検討チームが必要ではないか。
- 異なる SLA を実現するために技術を各産業分野にどうデプロイするかが課題となろう。

- レジリエンスの観点を含めるべき。壊れる時は壊れることを認識した上で設計する。
- どの分野にどういう事象があった場合に連動してどういう影響が起きるかリスク分析

を実施すると効果的ではないか。

- スマートシティでは大量のセンサがデータを収集する。N×M のデータ流通の中でデータをコンソリデーションし、品質を高める管理技術は必要と考えるが、あまり現状で取り組まれていないのではないか。

- 認証と ID 基盤はアーキテクチャ全体により幅広く関わってくる認識である。モノの ID については、分野毎に異なる ID があり、全体のスコープの中でベストなものを検討しないといけない。
- セキュリティも全体に薄く広くかかってくる。横の広がりや分野毎の広がりもあり、それぞれにトラストアンカーがある。マイクロコンピューティングでも論点になるだろう。
- ゼロトラストアーキテクチャは理想であるが、あまりに理想的構成を前提とすると性能面の負荷も大きいので注意が必要。システムがそれぞれ独立した上で連携するという構成の検討も必要では無いか。

- データの利活用はマネタイズの観点で重要であるが、オープンデータだけでは差別化出来ない。ローカルデータを収集する上で、個人情報を扱える基盤の需要は高いのではないか。

b. 研究開発の進め方について

- 万博を含め技術の適用先は具体的である方が理解を得られやすい。万博に集まってきたデータの中で近い考えの取組みがないかチェックしたい。
- 短期的な成果を目標とする範囲と、中長期的な取り組みを要する範囲は区別すべきだろう。
- サステイナブルな運用をするチームを実現するためには運用技術も重要である。また、人材育成、コミュニティ形成も必要になる。
- 事業者が担う差別化部分と個々の部分を OSS 化していく部分の見極めが重要。日本にどういう技術を残すかという視点でも検証する必要がある。電力分野で SLA に従った制御をどう行うか等は有望テーマに思える。
- 技術と人材は両方必要であり、日本の中で基盤を運用する技術を持った人間も育てる必要がある。リソースが限られるため、注力分野の見定めは必要。
- アーキテクチャのデザインにも技術が必要。構想図から実際に使える所に落とす所までに距離がある。
- 法律まで扱えるアーキテクトが必要であり、その定義までこの勉強会で視野に入れようとしている。

3.1.6 アーキテクチャの設定

3.1.3 ～ 3.1.5 の調査結果を踏まえ、電力・スマートファクトリー・自動車の各分野、及

びスーパーシティにおけるアーキテクチャ例を以下の通り設定した。

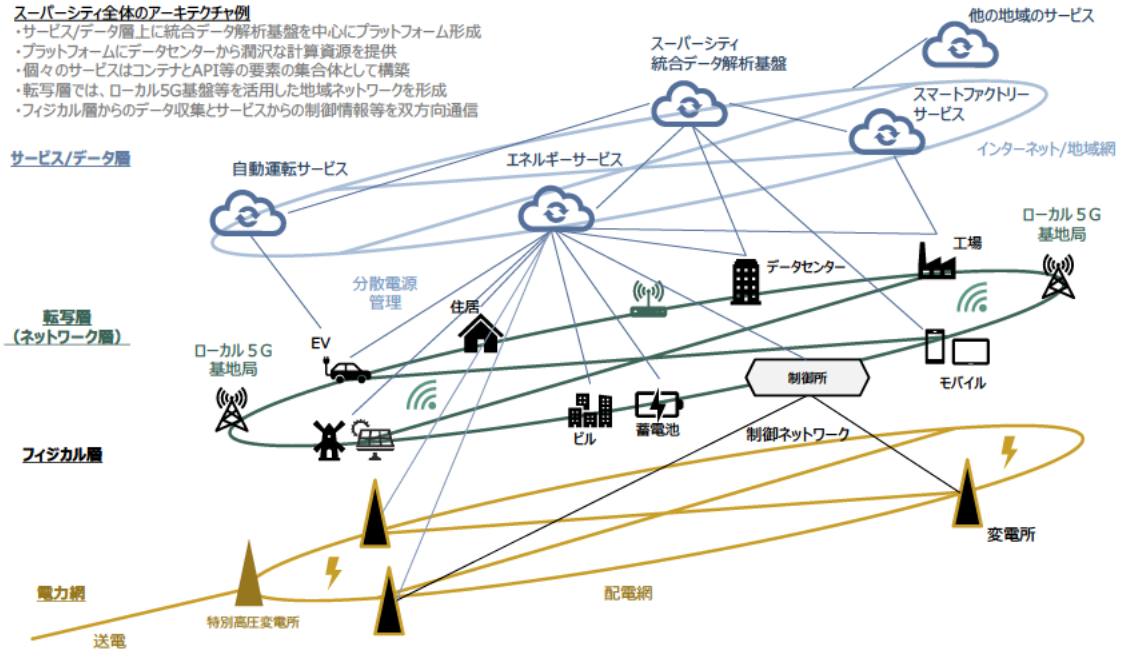


図 3-4　スーパーシティ全体のアーキテクチャ例

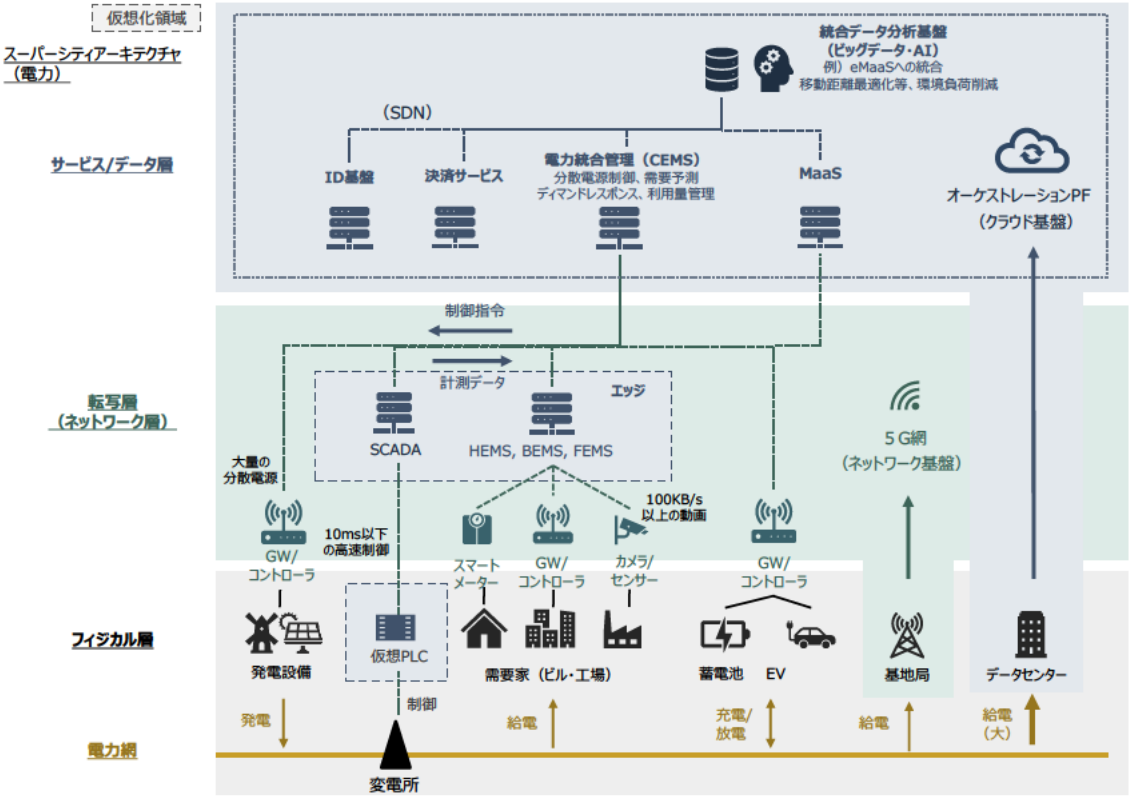


図 3-5　スーパーシティ（電力）のアーキテクチャ例

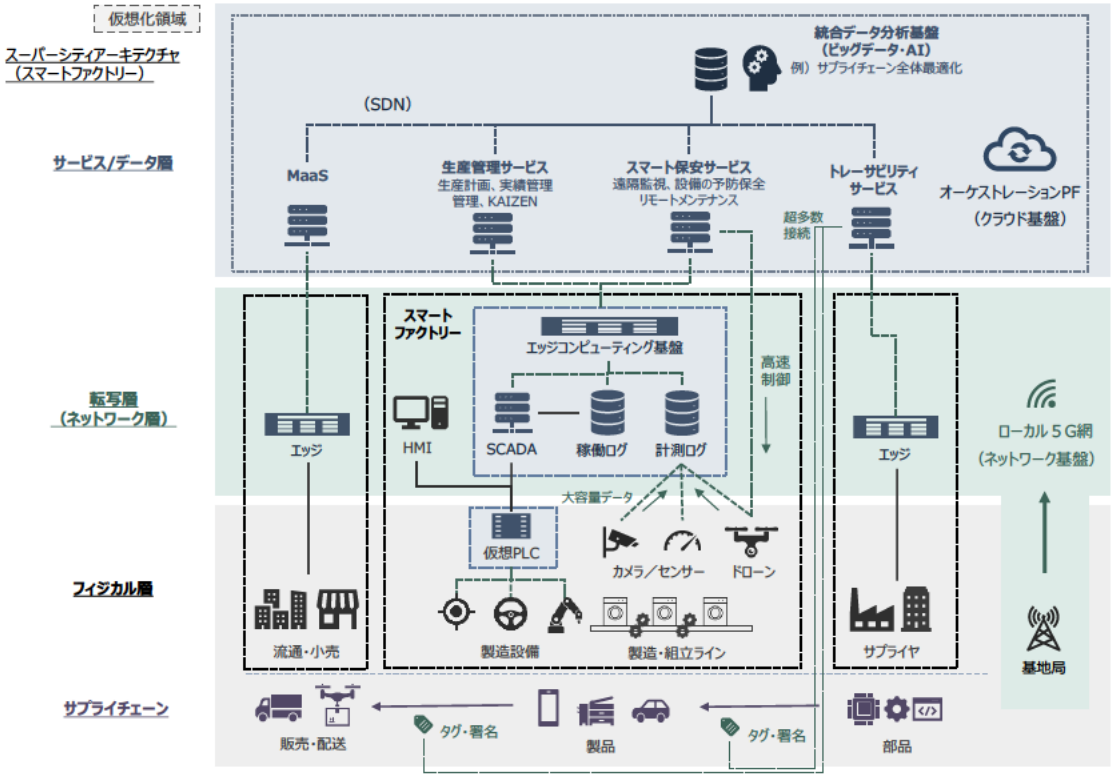


図 3-6　スーパーシティ（スマートファクトリー）のアーキテクチャ例

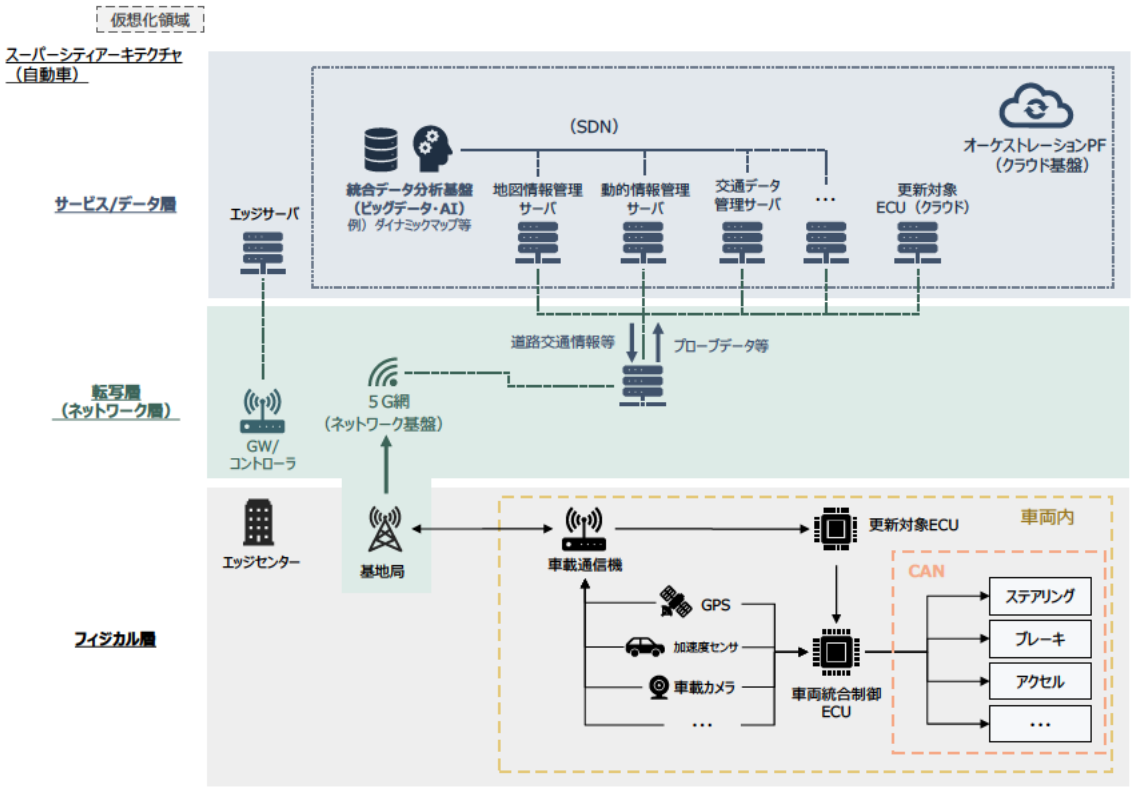


図 3-7　スーパーシティ（自動車）のアーキテクチャ例

3.2 基盤インフラ技術に関して求められる政策の検討

3.2.1 論点整理

3.1 節の調査結果を踏まえると、基盤インフラ技術を我が国に確保するために必要な事項は以下のようにまとめられる。

【次世代基盤インフラの検討プロセス・体制】

A) アーキテクチャを議論すべきである。基盤インフラのアーキテクチャは誰もわかっていない状況であり、各社が集まって集中的にアーキテクチャの検討を行う必要があるのではないか。

B) 個々のテーマ検討を別々に行ってしまうとアーキテクチャが別々のものになってしまう。全体を横串で見るアーキテクチャ検討チームが必要ではないか。それを初期の研究課題にしても良いのではないか。

C) 相互接続や実証はオープンに実施しやすいが、研究開発は個別に実施することになることから、中立でコア技術を開発する役割として、学の役割が重要ではないか。

D) 個人が見えるという場も必要である。官としては、人材を送り出す企業へのサポートが有効ではないか。コミュニティは「人」なので、コミュニティに対しては「人」の支援が必要である。

【研究開発の方向性・戦略】

A) クラウド（IaaS）については、物理層含め、外資メガクラウドが長年にわたって数千億円規模で投資・構築してきたシステム/サービスであり、今から「国産クラウド」として構築しても対抗は難しいのではないか。

B) アプリケーション等上位のレイヤは日本の SIer に蓄積があるのではないか。日本に強みのある製造業等のビジネスを妨げずに、ソフトウェア化の競争力を育て、ソフトウェア提供の中でハードウェアへのフィードバックがあるのではないか。

C) メガクラウドは利便性が高くロックインに陥る可能性がある。変わらない「永続層」を実現する技術・サービスの獲得が必要ではないか。

D) 処理をコアにするかエッジにするかの技術は 5G にないので開発すべき。一方で、コアとエッジが複数事業者になっても実現できるような基盤を考えるべき。その時にミドルウェアが必要になる。そのミドルウェアが処理をコアにするかエッジにするかの振り分けを行うか、ユーザ側で指示できるような基盤とすべき。

E) ある分野を想定し、多様な要件や現場環境における実証を行うことが良いのではないか。多種多様なアプリケーション要件、周期的・低遅延通信（制御通信など）、多端末・大容量伝送（遠隔監視など）、ベストエフォート（オフィス PC など）等、様々な現場環境・制約があり、障害物や干渉などで通信環境が常に変化

する、あるいは限られた計算処理能力（端末側の制約等）あるなかで、どのように活用できるものを構築していくかが重要である。

F) 認証と ID 基盤はアーキテクチャ全体により幅広く関わってくる認識である。モノの ID については、分野毎に異なる ID があり、全体のスコープの中でベストなものを検討しないといけない。ネットワークのセパレーションの上で複数事業者が動くとすると、認証を行い、コンポーネント単位でデータを受け渡しできる認証基盤が必要となる。認証だと中央集権的になるので、誰が作るのかが課題。

G) セキュリティも全体に広く関わる課題である。ただし、ゼロトラストアーキテクチャの理想的構成を前提とすると性能面の負荷も大きいので注意が必要である。

H) スマートシティでは大量のセンサがデータを収集するため、データ流通の中でデータをコンソリデーションし、品質を高める管理技術が必要と考える。

I) レジリエンスの観点を含めるべきである。壊れることを認識した上での設計、分野と分野が連動した影響等のリスク分析が効果的ではないか。

J) 事業者が担う差別化部分と個々の部分を OSS 化していく部分の見極めが重要。日本にどういう技術を残すかという視点でも検証する必要がある。

【人材育成に必要な環境や目指す人材像】

A) サステイナブルな運用をするチームを実現するためには運用技術も重要である。また、人材育成、コミュニティ形成も必要になる。

B) 技術と人材は両方必要であり、日本の中で基盤を運用する技術を持った人間も育てる必要がある。リソースが限られるため、注力分野の見定めは必要。

3.2.2 政策の方向性

(1) 基盤インフラ技術に関する研究開発

3.1 節の調査結果を踏まえると、基盤インフラ技術を我が国に確保するために必要な事項は以下のようにまとめられる。

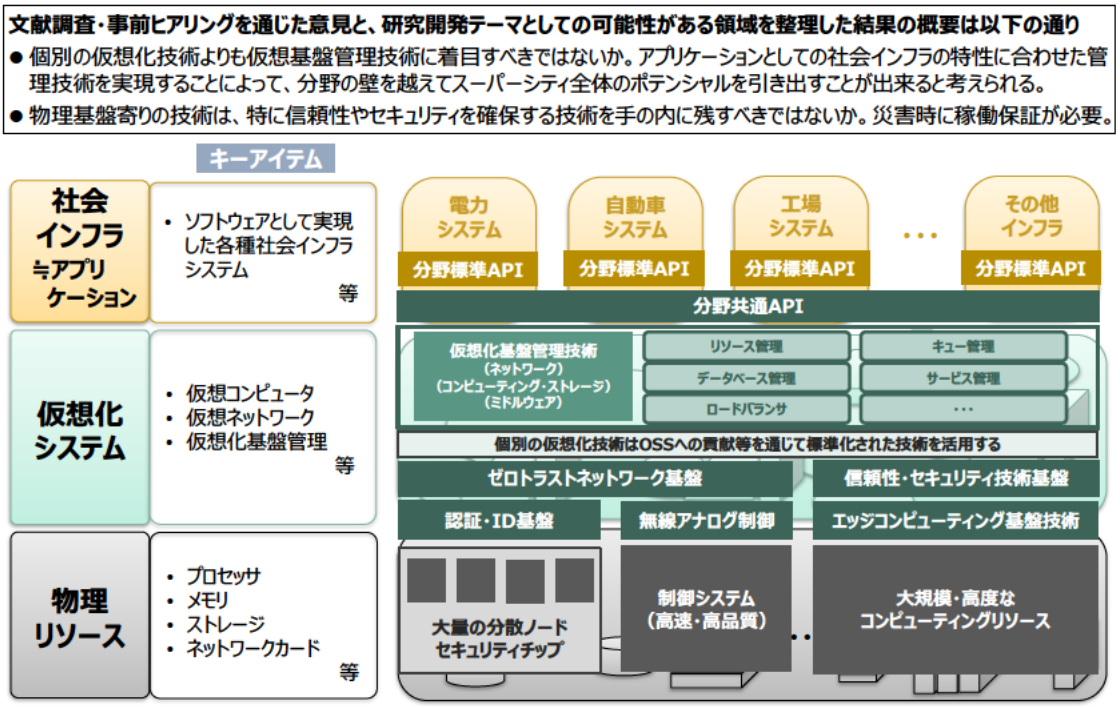


図 3-8　基盤インフラ技術研究開発のスコープ

(2) 研究開発計画（案）の策定

基盤インフラ技術研究開発を進めるにあたり、研究開発に必要な内容をまとめた研究開発計画（案）を策定した。

以下に研究開発計画（案）の記載内容を示す。

なお、本記載内容は「案」としてとりまとめたものであり、内容については、今後の検討に応じて修正していくことを想定している。

1) 概要

我が国では、サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会「Society5.0」の実現を提唱している。「Society5.0」では、データの流通・活用を含む、より柔軟で動的なサプライチェーンを構成することが可能であり、5G 技術や次世代クラウド基盤技術など、サプライチェーンを下支えする基盤インフラ技術の確保が求められる。また、今後の社会インフラ（電力、工場等）は仮想化基盤の上のアプリケーション（ソフトウェア）として実現される可能性が高まっている。

このような社会機能を維持していくために、その基盤（物理基盤、仮想化基盤）を構築、維持、運用・保守する能力の確保が必要である。

2) 意義

経済産業省では、本研究開発に先立ち、我が国としての基盤インフラ構築、維持、運用能

力の獲得に向けて幅広い専門家からなる勉強会を開催し、基盤インフラが抱える課題に係る包括的な検討、今後必要な施策に資する課題整理等を行った。特に、次世代基盤インフラを支える各種技術のうち、我が国において優先して獲得すべき技術について明確化した。

これらの検討成果を踏まえ、基盤インフラの構築等に資する技術の研究開発等を実施し、我が国の基盤インフラの構築、維持、運用を行う能力の獲得を目標とする。

3) 研究開発内容

a. 研究開発項目

以下 A～F の項目について、研究開発を実施する。研究開発項目は、技術動向や市場動向等を踏まえ、必要に応じて柔軟に追加・変更する。

また、研究開発項目毎もしくは個々の開発テーマ毎に開発目標を設定し、研究開発の進捗状況管理の一環として、当該目標の達成状況を独立行政法人情報処理推進機構（IPA）が評価する。必要な場合には、開発目標の見直しを行う。

A)　次世代基盤インフラのアーキテクチャ及び標準化に係る検討（委託）

- 分野横断的ユースケースを想定する次世代基盤インフラに求められるアーキテクチャの及びアーキテクチャ内で標準化されるべき技術・運用の調査・検討を行う。以下のような要素を含む調査・検討を行うこと。
  - 電力や交通システムといった複数分野のユースケースにおいて求められるアーキテクチャの構成・機能等に係る調査検討
  - 共通的に求められる技術・API 等に係る開発・運用の標準化に係る検討
  - エッジ基盤とクラウド基盤の機能配置に係る検討
  - 故障や災害、セキュリティインシデント等の際に求められる復旧能力に係る検討
  - B)以降に記述する個別開発テーマにおいて共通化されるべき技術要素の管理

B)　分野横断的に大量データの収集・蓄積・解析を可能とするための高スケーラビリティを持つサービス（基盤領域）におけるサービス・技術の開発（委託）

- 以下に示すような要素を含む技術の研究開発を行う。
  - クラウドサービスをミドルウェアレベルでスケールアウト構成を実現する技術の開発
  - マネジメント・サービスを実現する技術（運用支援）
    例）DB as a Service、Queue as a Service の実現

C)　エッジ基盤とクラウドの垂直スケーラビリティとエッジ基盤等の限られた計算資源で実現可能な高効率データ分析・処理を実現する技術（委託）

- 以下に示すような要素を含む技術の研究開発を行う。
  - 多様なアプリケーション要件や物理的環境（工場内等）への対応を可能とする

ミドルウェアの開発

- パブリック 5G とキャリア IaaS を活用したリアルタイムソリューションの実現
- エッジ基盤等の限られた計算資源上で高速・高エネルギー効率で処理する計算技術
- エッジ／クラウド間及び複数のエッジ間で、異なる産業分野のアプリケーションを跨いだ計算ノードを統合管理する技術

D) 電力や交通システムといった分野毎の特性にあった性能でスライシングした仮想ネットワーク領域を動的に確保する技術

- 以下に示すような要素を含む技術の研究開発を行う。
  - 各デバイスのチップ等の情報や通信データの内容によって対象分野・用途を解析する技術
  - 規制・標準等に関するデータとスーパーシティ内の各種ログデータを統合管理する技術
  - データ等の解析結果に応じてネットワーク割当の最適制御を動的に行う技術
    （例）大量・超高速の分散電源制御と大容量のスマート保安のネットワーク領域をネットワークスラインシングにより分割し、国内の規制要件を維持した範囲内で、ネットワーク利用状況に応じた最適な割当品質を動的に更新する。

E) 次世代基盤インフラに共通的に求められるに認証・サイバーセキュリティ技術に係る検討

- 次世代基盤インフラ上で共通的に求められる認証・以下に示すような機能等を実現する技術の開発を行う。以下のような要素を含む技術の研究開発を行うこと。
  - 各デバイス、ネットワーク、サービス等を最適な範囲の信頼の基点によって統合認証する
  - デバイス間の通信や状態の振舞を統合解析し、不正な挙動の検知を行う
  - データの検証による負荷が小さい低遅延のゼロトラストネットワークの形成
  - IoT デバイスの個別通信データ仕様等に依存しない通信解析を行う
    （例）スーパーシティ共通ネットワークに接続するカメラや工場の外接 FW 等を識別・認証し、ネットワーク内の振舞いと電力利用量等のデータを統合解析し、不正検知を実施

F) サーバ等のセキュリティを確保する基盤管理プラットフォーム技術

- 以下に示すような機能等を実現する技術の開発を行う。
  - エッジ基盤上で稼働するサービスメッシュ管理技術
  - アプリケーション間の API 通信において、API の安全性を検証する技術
  - コンテナや設定等の配置前に脆弱性を検証する技術
  - 機微な情報を暗号化された仮想マシン・コンテナ上で処理する技術
  - プラットフォーム内の暗号鍵を統合的に管理する技術

b. 研究開発期間

研究開発項目 A～F は、研究開発開始時点から原則 5 年以内で実施することとし、必要な場合には、個々の研究開発の性質等に応じて、柔軟に対応するものとする。

なお、研究開発終了時点で実用化に向けた課題が残る場合であって、終了時継続評価（実施者の希望を踏まえて評価の実施有無を判断）の結果、必要性が認められた場合には、追加的に継続研究開発を実施することとする。

継続研究開発を希望する可能性がある場合、実施者は、公募に対する提案書に、想定される継続研究開発の内容、想定される追加的な実施者及び再委託先、想定される研究開発費を記載することとする。

4) 実施体制

a. 役割分担

本事業では、商務情報政策局が研究開発の方針決定等、IPA が研究開発の進捗状況管理等、公募により採択された実施者が研究開発の実施を担う。

商務情報政策局は、本事業を実施する上での重要な方針（研究開発計画、予算配分等）を決定するとともに、研究開発の進捗や技術動向・市場動向等を踏まえ、必要に応じて、研究開発計画等の見直しを行う。また、事業を円滑に進める観点から、必要に応じて IPA や実施者に対して指示 を行う。

IPA は、本事業を実施するための公募による実施者の採択、契約締結・助成金交付を行う。また、 本事業の研究開発成果の最大化に向けて、実施者による研究開発の進捗状況管理（実施者による研究開発の進捗状況の把握、実施者に対する必要な指示、各種委員会の開催を通じた評価等）や調査等、また、当該成果の普及に向けた広報等 を実施する 。

研究開発の実施者は、実用化や社会実装を見据えて研究開発に取り組む。当該実施者は、企業や研究機関等（以下、「団体」）のうち、原則として日本国内に研究開発拠点を有するものを対象とし、単独又は複数で研究開発を実施する。ただし、研究開発を実施する上で、国外の団体の特別な研究開発能力や研究施設等を活用する必要がある場合には、当該団体と連携して研究開発に取り組むことができる。

なお、本事業の実施に関する詳細（公募の進め方、採択審査における審査基準、各種委員会やステージゲート審査等を含む研究開発の進捗状況管理の方法、調査・広報の内容、研究開発費返還制度における費用対効果指標の達成状況の評価方法等）については、IPA が商務情報政策局 に相談の上、商務情報政策局が決定する。

また、IPA は提案者及び実施者から受領した資料や営業秘密に係る情報（事業化計画や売上高等）については、組織内の実施体制を適切に構築した上、機密保持のために十分な措置を講ずるものとする。

b. 研究開発の進捗把握・管理

IPA は、研究開発の実施者と緊密に連携し、各開発テーマの研究開発の進捗状況を把握する。また、外部有識者等で構成する委員会を組織し、定期的（年数回程度に評価を実施し、開発目標 の達成見通しを常に把握するとともに、予算の必要性や実施体制の妥当性を精査する。また、各開発テーマの研究開発の進捗状況、開発目標の達成見通し、成果の事業化の見通し等について、定期的に商務情報政策局に報告し、商務情報政策局からの指示に従い、必要に応じて、開発テーマ毎の予算配分の増加や縮小、実施体制の再構築等を行う。
また、研究開発を効率的かつ効果的に実施するため、商務情報政策局からの指示に従い、各開発テーマの研究開発開始から終了までの中間時点を目途に、ステージゲート審査を実施する。当該審査を通過しなかった開発テーマについては、審査後３か月を目途に研究開発を終了する。当該審査を通過した開発テーマについても、審査結果を踏まえ、必要に応じ、研究開発の加速、縮小、実施体制の変更（例：再構築、統合等）、実施形態の変更等を行う。
なお、当該審査等の委員会での評価に当たっては、研究開発の進捗や成果、情勢変化を踏まえた最新の事業化見通しとこれに向けた取組状況、費用対効果等に係る総合的な評価を行う。

5) 評価

評価委員会による毎年度末の評価の前に、研究開発責任者による自己点検を実施する。

6) 出口戦略

研究開発成果については、参画企業が主体となって製品化を進め、各産業分野への導入を推進する。一部の成果は、IP（知的財産権）化して関連するベンダにライセンス供与し、その普及を目指す。また、より広く本プロジェクトの成果を普及させるため、一般の認知、理解を高めるイベント（シンポジウムやセミナー、国際会議など）にも取組む。

7) その他

a. 研究開発成果の取り扱い

実施者は、研究成果の普及に努め、IPA は、実施者による研究成果の広範な普及の促進に努める 。
本事業の成果に依る知的財産や研究開発データの取り扱いについては、経済産業省が定める「委託研究開発における知的財産マネジメントに関する運用ガイドライン」及びその別冊である「委託研究開発におけるデータマネジメントに関する運用ガイドライン」に従うことを原則する。IPA が委託を行って実施する開発テーマについては、開発テーマ又は開発テーマを構成する研究項目毎に知財委員会を委託先に設置し、知財委員会において、研究開発成果に関する論文発表及び特許等（以下、 「知財権」）の出願・維持等の方針決定等のほ

か、必要に応じて、知財権の実施許諾に関する調整等がなされるよう、IPA が助言・指導を行う。

b. 実施期間

本事業を終了する時期は 2025 年度とし、2 年に 1 回、見直しを行う。

c. 事後評価

事後評価は、本事業の終了後に経済産業省が行う。

d. 研究開発計画の見直し

商務情報政策局は、研究開発の進捗や技術動向・市場動向等を踏まえ、必要に応じて研究開発計画（研究開発項目、研究開発期間、開発目標、実施体制等）を見直す。

4. サプライチェーン・セキュリティに関する国内外の法令・政策等に関する調査

4.1 調査概要

検討会の議論動向等を踏まえ、IoT 機器・システムやデータセンターの基盤技術のセキュリティに関する技術動向調査を行った。

4.2 ランサムウェアによる被害の実情及び支払いの可否に対する議論の動向、その他の対応における注目すべき事案

4.2.1 各国における代表的なランサムウェア被害事案

(1) 概念

ランサムウェアは、コンピュータシステム上のデータを暗号化してエンドユーザが使用できないようにする犯罪者によって配備された悪質なソフトウェア、又はマルウェアの一種であると定義することができる。サイバー犯罪者は、身代金が支払われるまでデータを人質にする。身代金が支払われない場合、被害者のデータは無期限に利用できないままになったり、一般の人々に公開されたりする可能性がある。

(2) 歴史

最初のランサムウェアは、1989 年の PC Cyborg であるとされる[1]。この攻撃は、エイズ研究者のジョセフ・ポップ博士が、90 カ国以上のエイズ研究者にフロッピーディスク 2 万枚を配布し、その中にはアンケートを使って個人のエイズ発症リスクを分析するプログラムが含まれていると主張して実行させたものである[2]。このランサムウェア攻撃は、「AIDS トロイの木馬」又は「PC サイボーグ」といわれている。

その後、2000 年代までは、ランサムウェアは、一般的ではなかった。その後、2000 年代中盤に RSA 方式（1024 ビット鍵）で暗号化される方式のランサムウェアが出現した。具体的には、TROJ／RANSOM.A（2006 年）[3]、Archiveus（2006 年）、Gpcode（2006 年）[4]などがある。また、2011 年には、マイクロソフトライセンス認証を模倣するランサムウェアが発生した。これは、利用者が、真正な通知との違いがわからないために、国際電話番号に電話をしてしまい高額な国際電話料金を発生させるというものであった。その後、種々のランサ

[1] https://www nomoreransom.org/ja/ransomware-qa html　また、https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time　による。
[2] このマルウェアプログラムは、このプログラムは、最初はコンピュータの電源を 90 回入れただけで起動し、コンピュータの電源が入らない状態のままにするもので、マルウェアは 189 ドルの支払いを要求するメッセージを表示し、さらにソフトウェアのリース料として 378 ドルを要求するものであった。
[3] https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Ransom-A/detailed-analysis.aspx　また、「30 分ごとにファイルを一つずつ消していく「Troj/Ransom-A」（https://gigazine net/news/20060501_troj_ransom_a/）
[4] 「ランサムウェア「Gpcode」で暗号化されたファイルの復元方法が公開」（https://www.itmedia.co.jp/enterprise/articles/0806/18/news102 html）

ムウェアが流行した。その手法は、OS もしくはブラウザをブロックするタイプと暗号化するものとに分けられる。

例えば、カスペルスキー社の報告[5]によれば、2015 年度（2015 年 4 月から 2016 年 3 月、以下同じ）におけるランサムウェアの被害件数は、2014 年度に比較して、17.7%増加しており、2016 年度は、11．4%増加している。また、特に暗号化のタイプのランサムウェアが急激に増大したことが報告されている。被害者の傾向は、従前は家庭ユーザが一般的であったが、その後、企業を狙ったランサムウェアが出現・増加している。もっとも、同社の調査によれば、2017 年度においてランサムウェアは、30%ほど減少したが、2018 年度においては、ランサムウェアの被害が再度、増大している。

(3) 報道等がなされた事件

ランサムウェアで世界的な被害を惹起したものとしては、WannaCry（2017）、NotPetya（2017）などがある。それ以外に各国で特徴的な被害を惹起したものとしては、以下のような事例がある。

1) 米国

SamSam ランサムウェア事件（2018）は、特にアメリカの地方自治体に対して被害を惹起した。具体的には、2018 年 3 月にアメリカ・アトランタ市のシステムに対して攻撃がなされ、市や警察などの公共機関が機能不全に陥っただけでなく、バックアップデータをも失われたという事件を引き起こしている[6]。

Ryuk（2020）は、アメリカの病院等を標的にしたランサムウェアである。また、米国の郡（カウンティ）も被害にあっており、多額の身代金を支払わなければならなかったとされている[7]。

Robinhood（2019）は、北米の 2 都市、ノースカロライナ州グリーンビルとメリーランド州ボルチモアの重要な IT システムをロックし、対応する公共サービスを停止させたと報道されている[8]。

---

[5] https://securelist.com/pc-ransomware-in-2014-2016/75145/
2016 年度は、KSN Report: Ransomware in 2016-2017（https://securelist.com/ksn-report-ransomware-in-2016-2017/78824/）、
2017 年度については、KSN Report:Ransomware and malicious cryptominers 2016-2018（https://securelist.com/ransomware-and-malicious-crypto-miners-in-2016-2018/86238/）
その後、2019 年以降については同社によるランサムウェアに集中した調査は見当たらないが、一般的なものとして「2019 年のストーリー：ランサムウェア猛威の下の街」（Story of the year 2019: Cities under ransomware siege）（https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/）

[6] SamSam についての詳細な分析としてソフォス「SamSam: 600 万ドル (約 6 億 7000 万円) 近くの身代金を手にしたランサムウェア」（https://www.sophos.com/ja-jp/press-office/press-releases/2018/08/samsam-the-almost-6-million-ransomware.aspx）がある。

[7]後述の 「ランサムウェア その実態と対応（What it is & What to Do About It）」による。

[8] この記事としては「新種のランサムウェア RobbinHood がアメリカの自治体を攻撃」（https://www.acronis.com/ja-jp/blog/posts/xin-zhong-noransamuuearobbinhoodgaamerikanozi-zhi-ti-wogong-ji）。また、上記「ランサムウェア その実態と対応（What it is & What to Do About It）」においても言及がなされている。

2) 英国

英国において、被害が多く、また、特徴的なものとして報道されている[9]事件としては、以下があげられる。NHS 事件（2017）は、WannaCry によって、NHS（国民保健サービス）の多数のコンピュータが停止を余儀なくされたという事件である[10]。Reckitt Benckiser 事件（2017）は、NotPetya によって、英国の製薬会社である Reckitt Benckiser が、薬品の製造とその配送に支障を来して多大な損害を被ったという事案である。Eurofins Scientific 事件（2019）は、上述の Ryuk によって科学捜査サービスプロバイダが、ランサムウェアに感染し、血液や DNA サンプルの分析に支障が生じたという事件である[11]。The Police Federation of England and Wales (PFEW)事件（2019）は、警察官の労働組合である PFEW が、ランサムウェアによってデータベースやシステムが影響を受けて、データにアクセスができなくなったという事案である[12]。

3) ドイツ

IT セキュリティ庁（BSI（Bundesamt für Sicherheit in der Informationstechnik））が発行している「Ransomware Bedrohungslage, Prävention & Reaktion 2019」(以下「Ransomware 2019」[13]という)において、ランサムウェアの用いる動機や被害状況及び、それの対策についての議論がなされている。

ランサムウェアの被害として、会社の営業が害されること等によるコストという意味での固有の損害、レピュテーション侵害、さらに契約の相手方等の第三者への損害の 3 つがあると整理される（Ransomware 2019、8 頁、以下同じ）。ランサムウェアを用いる攻撃者の動機は金銭的な利益、（政治的、経済目的）破壊的活動、憂さ晴らし等がある（同 10 頁）。

大企業の被害の実例としては 2019 年の Norsk Hydro 社の例がある。同社はランサムウェア LockerGoGa の被害者となった。同社は 35,000 人の従業員を抱えるアルミニウムの製造業を営む会社である。インシデントの際、同社の多くの IT システムがランサムウェアに感染した。同社は身代金を支払わず、既存のバックアップを使ったものの、ウェブサイトには一時的にアクセスができなくなり、4 週間にわたってマニュアルでの稼働を余儀なくされた。結局、最大＄43,000,000 の損害が出た（同 11－12 頁）。

4) 日本

日本においては、2020 年 4-12 月において警察庁への相談が 23 件あったことが報道されている[14]。また、新聞報道された事件としては、カプコムの二重恐喝のランサムウェアの被害、ホンダの事案等がある。

---

[9] 以下の事案は、“The top 5 ransomware attacks in the UK and their hidden costs on business”による（https://www.acronis.com/en-gb/articles/ransomware-attacks/）。

[10] 詳細な報道として BBC「英医療機関、ランサムウェアの被害拡大を懸念」（https://www.bbc.com/japanese/39918853）がある。

[11] “UK Law Enforcement Data Put at Risk in “Highly Sophisticated” Eurofins Scientific Attack”（ https://www.cbronline.com/news/eurofins-scientific-hacked）

[12] ” Brit Police Federation cops to ransomware attack on HQ systems” https://www.theregister.com/2019/03/21/police_federation_ransomware_attack/

[13] https://wod.wowow.co.jp/content/080281

[14] 国家公安委員会委員長（代理）記者会見要旨（https://www npsc.go.jp/pressconf_2021/03_04.htm）

4.2.2 各国におけるランサムウェアにおける脅迫金支払いの可否についての法的な助言・ガイドライン等の分析

1) 米国

a. サイバーセキュリティ及びインフフラストラクチュアセキュリティ庁（CISA）

米国のサイバーセキュリティ及びインフフラストラクチュアセキュリティ庁（CISA）は、総合的なランサムウェア対応についての情報を整備している[15]。

そこでは、ランサムウェア対応の会議のビデオ（ウェビナー）、「CISA、MS-ISAC、NGA及び NASCIO[16]によるランサムウェア攻撃からの保護のための即時行動の推奨事項」、CISAの分析などが紹介されている。そこで注目すべきものが、CISA と MS-ISAC による 2020 年9 月の「共同ランサムウェアガイド」になる。このガイドは、パート１　ベストプラクティスとパート２　対応チョックリストからなる。パート 1 においては、準備すること、感染のベクターとして、脆弱性・誤った設定、フィッシング、感染の前兆、サードパーティやマネージドサービス提供者があげられている。パート 2 においては、探知の分析、封じ込みと消去、リカバリと事件後の活動、コンタクトリストがあげられている。

このガイドでは、ランサムウェアに対して支払う行為に対して「身代金を支払っても、データが復号化され、又はシステムやデータが危険にさらされることがなくなるわけではありません。CISA、MS-ISAC、及び連邦法執行機関は身代金の支払いを推奨していません。」というコメントがなされている。

b. FBI

米国連邦捜査局（FBI）は、ランサムウェアについての情報をまとめている[17]。そこでは、ランサムウェアとはどういうものか、また、ランサムウェアの被害にあわないための助言、また、IC3 の資料へのリンクが紹介されている。また、2016 年 4 月に既に、ランサムウェアの被害が増加傾向にあるとして、ニュースリリースで「FBI は、ランサムウェア攻撃に対して身代金を支払うことを支持していません。身代金を支払っても、組織がデータを取り戻せるという保証はありません。身代金を支払った後、組織が復号鍵を手に入れられなかったというケースを見たことがあります。身代金を支払うことは、現在のサイバー犯罪者がより多くの組織を標的にすることを助長するだけでなく、他の犯罪者がこの種の違法行為に関与する動機付けにもなります。そして最後に、身代金を支払うことで、組織は、犯罪者に関連した他の違法活動に不用意に資金を提供している可能性があります。」と伝えている[18]。

---

[15] https://www.cisa.gov/ransomware　なお、このサイトは、2021 年 1 月に整備されたものである（https://www.cisa.gov/news/2021/01/21/cisa-launches-campaign-reduce-risk-ransomware）。

[16] サイバーセキュリティ・インフラセキュリティ庁（CISA）、マルチステート情報共有・分析センター（MS-ISAC）、全米知事協会（NGA）、全米州最高情報責任者協会（NASCIO）になる。

[17] https://www fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

[18] ” Incidents of Ransomware on the Rise Protect Yourself and Your Organization”のニュースリリースによる。（https://www fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise）また、このことを報道するものとして、FBI announcement: paying the ransom is a bad idea（ https://blog malwarebytes.com/security-world/2016/05/fbi-announcement-paying-the-ransom-is-a-bad-idea/ ）、High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations（https://www.ic3.gov/Media/Y2019/PSA191002）

c. IC3

IC3 は、インターネット犯罪申立センター（Internet Crime Complaint Center）である。その使命は、インターネットを介した犯罪行為の疑いに関する情報を連邦捜査局に提出し、法執行機関や業界のパートナーとの効果的な協力関係を構築するために、信頼性の高い便利な報告メカニズムを一般の人々に提供することである。IC3 のサイトでは、ランサムウェアについて、「ランサムウェアの被害者は、感染を連邦法執行機関に届けること」（2016 年 9 月）[19]、「米国企業及び組織を脅かすインパクトの高いランサムウェア攻撃」（2019 年 10 月）[20]、「ランサムウェア　その実態と対応（What it is & What to Do About It）」（2021 年 1 月）[21]が公表されている。もっとも、これらのほとんどは、ランサムウェアとは何か、そのための防御のためのベストプラクティスを叙述するものであり、法的な関係についての分析はなされていない。

d.　財務省による制裁[22]

米国財務省外国資産管理室（OFAC：Office of Foreign Assets Control）は、「ランサムウェアに対する支払いを促進することに対する制裁の可能性についての助言」（Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments）を公表している[23]。

この助言においては、悪意あるサイバー攻撃者に対して種々の制裁プログラムを有しており、そのなかにランサムウェアの攻撃者とそれを促進したものに対しての制裁も含まれていることが明らかにされている。具体例として、2016 年にクリプトロッカーの被害に対してその開発者であるエフゲニー・ミカイロビッチを指名手配した。2018 年に SamSam ランサムウェアに関連して、そのサイバー攻撃に対して重要な支援をなしたとして２名のイラン人を指名手配し、ランサムウェアの資金を送り込んだ仮想通貨のアドレスを特定した。また、ラザルスグループ（WannaCry2.0）、イービルコープ（Dridex）への指名手配も紹介されている。

制裁で指定されている犯罪者・敵（adversaries）に対して、ランサムウェアの支払いを促進（Facilitating）することは、彼らの違法な目的を利得させ、進めることになる。それは、国家安全保障を脅かし、対外ポリシーに反する行為とされる。

国際緊急経済権限法（IEEPA）又は敵国との取引法（TWEA）[24]のもと、 米国人は、OFAC の特別指定国民・凍結者リスト（SDN リスト）、その他の凍結者、及び包括的な国や地域の禁輸措置の対象となっている者（キューバ、ウクライナのクリミア地域、イラン、北朝鮮、シリアなど）の個人又は事業体（以下「者」）との間で、直接又は間接的に取引に関与することが一般的に禁止されている。また、IEEPA に基づく違反を引き起こすあらゆる取引も

---

[19] ”Ransomware Victims Urged to Report Infections to Federal Law Enforcement”（ https://www.ic3.gov/Media/Y2016/PSA160915）

[20] “High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations”（https://www.ic3.gov/Media/Y2019/PSA191002）

[21] https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf

[22] 米国におけるマネーロンダリングへの対応の基礎的な知識としては、岡崎正江「米国内国歳入庁におけるマネーロンダリングへの取組」（税大ジャーナル　5　2007 年 6 月）（https://www nta.go.jp/about/organization/ntc/kenkyu/backnumber/journal/05/pdf/07.pdf）がある。

[23] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
なお、これを紹介する記事として、Alex Scroxton「ランサムウェアの身代金支払いを支援すると罰金&制裁対象に」（コンピュータウイーク 2020 年 11 月 18 日号）がある。

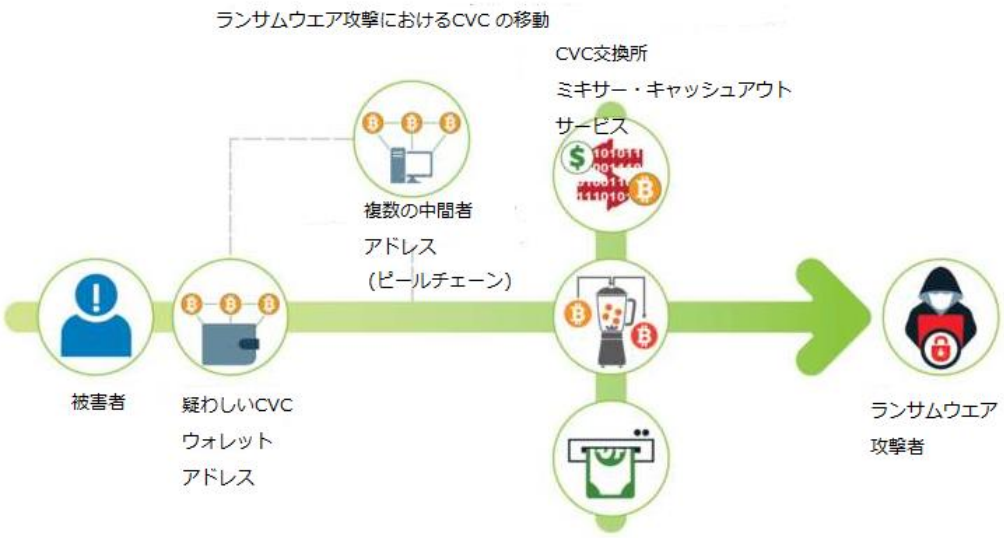
[24] 50 U.S.C. §§ 4301–41; 50 U.S.C. §§ 1701–06

禁止されている。OFAC は、厳格責任に基づいて制裁違反に対して民事罰を課すことがありうる[25]。これらの規定は、サイバー保険、デジタルフォレンジックス、インシデントレスポンスや金融サービスにかかわる者に適用されるのであり、その制裁規定に違反しないようにしなければならないとされる。また、FinCEN 規則にも準拠しなければならない。これらの違反については、事案毎のアプローチにより、免許付与において考慮されることがありうる。また、ランサムウェアの被害者については、制裁関連者（sanctions nexus）を含みうると考えた場合には、直ちに OFAC に連絡することが推奨されている。また、攻撃が金融機関をも含む者である場合には、財務省サイバーセキュリティ重要インフラ防護局に連絡することが推奨されている。

e. FinCEN アドバイザリ

財務省の金融犯罪取締ネットワーク（Financial Crimes Enforcement Network、FinCEN）も、「ランサムウェア及び支払いを促進するための金融機関の利用についての助言」（Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments）を 2020 年 10 月に公表している[26]。この助言は、 (1)ランサムウェアの支払い処理における金融仲介機関の役割、(2)ランサムウェアと関連する支払いの傾向と類型、(3)ランサムウェア関連の金融レッドフラッグ指標、(4)ランサムウェア攻撃に関連する情報の報告と共有について論じている。

ランサムウェアの支払い処理における金融仲介機関の役割においては、いくつかのステップを踏んで、ランサムウェアの支払いがなされていることが説明されている。具体的には、その過程は、次の図で示される。



この図は、多くのランサムウェアのスキームは兌換可能な仮想通貨(convertible virtual

[25] これらの制裁について考慮されるべき事項については、執行ガイドライン（31 CFR Appendix A to Part 501 - Economic Sanctions Enforcement Guidelines.－https://www.law.cornell.edu/cfr/text/31/appendix-A_to_part_501）がある。また、コンプライアンス・プログラムについては、OFAC がその枠組みについて公表している（「OFAC コンプライアンス・コミットメントの枠組み」参照（A Framework for OFAC Compliance Commitments）（https://www.piclub.or.jp/wp-content/uploads/2019/09/Framework-for-OFAC-Compliance-Commitments-1.pdf）。

[26] https://www fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf

currency－CVC)を含んでいることを示している。ランサムウェアの被害者は、通常、電信送金や自動化されたクリアリングハウス、クレジットカード決済で CVC 交換所への送金し、ランサムウェアの加害者が指定する CVC の種類と金額に従い購入する。次に、被害者は CVC を、一般には、交換所がホストしているウォレットから、加害者の指定口座又は CVC のアドレスに送金する。そして、ミキサーやタンブラーなど様々な手段を使って資金を洗浄し、他の CVC への交換や多くの口座や取引所をまたいだ取引が行われ、海外拠点の取引所やアンチマネーロンダリングとテロ資金調達への対応（AML/CFT）の管理が弱い法域のピアツーピア（P2P）交換所へ資金が移動される。

このようなスキームに対して、デジタルフォレッジックス・インシデントレスポンス（DFIR）会社とサイバー保険会社（cyber insurance companies (CICs)）が、ランサムウェアの被害者に対して防護と緩和のサービスを提供している。それらの会社は、ときによっては、被害者からの資金を受領してランサムウェアの支払いを促進することもある。この場合、資金移動となり、マネー・サービス・ビジネス（Money Service Businesses、MSB）と解される。MSB は、銀行秘密法（Bank Secrecy Act）における疑わしい取引報告の義務（suspicious activity reports、SARs）の義務が課されることになる。この点についての OFAC のガイダンスは、上述のとおりである。

ランサムウェアと関連する支払いの傾向と類型においては、烈度と狡猾さが増していることが論じられている。特に狡猾さについては、「ビッグゲーム・ハンティングスキーム」「犯罪者集団のパートナーシップ・リソース共有」「二重恐喝スキーム」「匿名性強化暗号通貨（Anonymity-Enhanced Cryptocurrencies (AECs)）」「ファイルなしのランサムウェア」について説明がなされている。

ランサムウェア関連の金融レッドフラッグ指標において、FinCEN は、金融機関がランサムウェア攻撃に関連した不審な取引を検出、防止、報告する際に役立つよう、ランサムウェア関連の不正行為を示す金融レッドフラッグ指標を特定していることを論じている。具体的には、サイバー指標、口座開設の際などに、支払いがランサム事件に関することを明らかにすること、顧客の兌換可能な仮想通貨口座がランサムの支払いと結びつくという分析と一致すること、ランサムウェアの標的になるハイリスクの企業とランサムウェアの支払いを促進する企業（例えばフォレンジックス企業）との間の取引であること、フォレンジックス企業等が顧客企業から、資金を受領し、受領後、同額を兌換可能な仮想通貨で送金していること、などがあげられている。

ランサムウェア攻撃に関連する情報の報告と共有については、上記の場合において、疑わしい取引（SAR）として報告義務があること、また、法の定めによりその情報共有によって民事損害賠償を問われることがないことが述べられている。

2) 英国

英国におけるランサムウェア対応についての政府関係のコメントはあまり多くはない。代表的なものは、以下のとおりである。

a. NCSC

英国の国家サイバーセキュリティセンター（NCSC）は、「マルウェアとランサムウェア

攻撃を緩和するーマルウェアとランサムウェア攻撃から組織をどのようにして防御するか」（Mitigating malware and ransomware attacks－How to defend organisations against malware or ransomware attacks）というページでガイダンス[27]をまとめている。そこでは、マルウェアの概念、アクション１（バックアップ）、アクション２（マルウェアの拡散防止）、アクション３（マルウェアの実行防止）、アクション４（インシデントに備える）、既に感染してしまったら、追加のアドバイスの項目に分けて論じられている。このガイダンスの中で、「支払うべきでしょうか（Should I pay the ransom?）」というガイダンスがある。

そこでは、法執行機関は、身代金要求の支払いを奨励したり、支持したり、容認したりしないこと、身代金を支払ったとしてもデータやパソコンにアクセスできる保証はないこと、コンピュータはまだ感染しること、犯罪者集団に金を払うことになること、将来的には狙われやすいことがあげられている。また、攻撃者は、支払いが行われない場合にはデータを公開すると脅迫してくることがあるが、それに対しては、組織はデータ流出の影響を最小限に抑えるための対策を講じる必要があり、NCSC の「バルク個人データの保護に関するガイダンス」[28]と「ロギングと保護監視のガイダンス」[29]が役立つことが述べられている。

なお、英国においても、ランサムウェアの攻撃者からの要求に応じて、支払いをなすことは、資金洗浄及びテロリスト金融犯罪の対象となりうる。この点についての金融規制機関からの助言等[30]については、現時点においてはみつからない。

b. 資金洗浄及びテロリスト金融犯罪について

そこで、資金洗浄及びテロリスト金融犯罪の対象となりうることについて[31]分析する。

英国においては、2002 年犯罪収益法（POCA; Proceeds of Crime Act 2002）[32]、2000 年テロリズム法（Terrorism Act 2000）、2017 年資金洗浄、テロリスト資金供与及び資金移転規則（Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017）が、上記の資金洗浄及びテロリスト金融犯罪についての対応策の枠組みを定めている。2002 年犯罪収益法は、327 条以下で、犯罪収益の隠匿、転換、移転等を犯罪としている。また、テロリズム法は、資金獲得（同 15 条）、資産の使用もしくは保有（16 条）などを犯罪としている。したがって、ランサムウェアの支払いそれ自体は、違法とはいえないものの、相手先が、誰に、どのような状況で支払われたかによっては、マネーロンダリングやテロリストの資金調達犯罪が行われる可能性があり、具体的な事実については常に専門家のアドバイスを求めるべきであるとされる[33]。

---

27 https://www ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
28 https://www ncsc.gov.uk/collection/protecting-bulk-personal-data
29 https://www ncsc.gov.uk/collection/mobile-device-guidance/logging-and-protective-monitoring
30 なお、英国財務省及び内務省「資金洗浄及びテロリスト資金供与についての国家リスク評価（National risk assessment of money laundering and terrorist financing 2020（https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf））においては、サイバー犯罪が、資金洗浄やテロリスト資金と関連の深いものであり、ランサムウェアもそのひとつであるという記述がある（3.22）。
31 この点については、OUT-LAW NEWS “Cyber attacks: due diligence essential prior to paying ransoms”（https://www.pinsentmasons.com/out-law/news/cyber-attacks-due-diligence-essential-prior-to-paying-ransoms）、”Money Laundering and Terrorist Financing”（https://www.barcouncilethics.co.uk/wp-content/uploads/2017/10/Money-Laundering-and-Terrorist-Financing-2.pdf）など参照
32 なお、分析については、坂東俊矢「英国における「行政による不法収益の剥奪、財産の隠匿・散逸防止制度、及び集団的消費者被害救済制度」の実際」（https://www.caa.go.jp/policies/policy/consumer_system/other/method_for_property_damege/report/pdf/1_UK.pdf）
33 前記 OUT-LAW NEWS

3) ドイツ

a. ランサムウェア対策

ランサムウェア対策は、Ransomware 2019 において、予防、対応に分けて論じられる。予防においては、感染を予防する方策（迅速なソフトウェア・アップデート、攻撃範囲の最小化、スパムメールの取扱い、管理者アカウントの安全な取扱い、ウィルスの保護等）、バックアップ、従業員の意識改革、といった観点から論じられる。技術的な推奨事項だけでなく、従業員への啓蒙も重要だとされている。例えば、意識向上キャンペーンや従業員のトレーニングにおいては、悪意のあるプログラムの感染方法について、email の添付ファイルを誤って開くことによる侵入や、信頼されていない Web サイトへのアクセス（ドライブバイエクスプロイト）という 2 つの重大な感染方法が常に問題とされる。特に、被害者側の誤った行動は、ソーシャルエンジニアリングによる場合もある。私的な関係を装ったり、利益を約束したりするソーシャルエンジニアリングに対しては、レポートやニュースを盲目的に信頼しないということが何よりも重要である。どんなに魅力的であっても、当該ニュース等を信頼して、求めに応じてクリックなどしてはならない。例えば Ransamware 2019 では、怪しい事象に遭遇した場合には、クリックではなく、そこに書いてある連絡先に電話をしてみることを推奨している。

対応については、身代金の必要性、苦情（Anzeige）の申立て、インシデント対応、外部のエキスパートの支援があげられている（Ransamware 2019, 22 頁）。

BSI は、身代金の必要性に関し、予め準備をし、損害が発生したときにその準備を実行しつつ、支払をしてはならない、と強く述べる。恐喝の成功経験によって、攻撃者はさらなる恐喝について動機付けを得る。身代金はさらなるマルウェアの開発に利用され、その拡大を促進し、さらにその態様もより洗練されたものにしてしまう。そもそも、攻撃者が身代金を受け取ることで約束を守って暗号化を解除する保障はないし、現にそうした事例がある。

次に警察に被害届を出すことは重要である。警察は、例えば、身代金の流れを追う、C&C サーバを監視して情報を取得する等の、ランサム企業や CERT が遂行できない捜査をすることができる。結局のところ、ランサムウェアのビジネスモデルは、追跡のプレッシャーによってのみ打ち破ることができ、こうして行為者は特定され、終局的に有罪の判決がなされることで、同人に他の犯罪の遂行をできなくさせることができる。連邦及び州警察は、苦情を受け付ける電話相談窓口をつくって、サイバー犯罪の被害者となった企業にアドバイスをし、苦情に基づいてサポートを行っている。

インシデント対応早期に感染したコンピュータのネットワーク接続（無線を含む）を切る必要がある。その上で、ログデータの助けを借りて、例えば、ネットワークドライブへのアクセスに基づいて影響を受けたコンピュータを特定していく。さらに暗号化されたファイルのメタデータ、例えば、どのユーザアカウントがそのファイルを作成したか、といったことも、感染したシステムについての一定の情報源となる。

フォレンジックを行うか否かは早期に決定しなければならない。一次キャッシュやハードディスクのバックアップを従業員により、影響を受けたシステムのさらなる修理や再起動が行われる前にしておくべきである。そうでないとフォレンジックが著しく困難になる

か不可能になってしまうかもしれない。フォレンジックの経験がない場合には、エキスパートに相談すべきである。

データの再作成が行われる前に感染したシステムの再インストールが必要である。OS は、信頼できるデータ媒体から持ってくる必要がある。

いくつかの条件の下（ランサムウェアが Windows 内に暗号化しないで、又は消去しない形でコピーを保持している場合やランサムウェアの暗号化が不完全である場合、そしてフォレンジックによる復元が可能である等）で、バックアップによるデータの保護を用いずとも、部分的又は完全なデータの復元が可能である。しかし、大概は復元できると期待しない方が良い。結局、インシデント対応は、原状回復というよりは、損害を限定し、感染源を特定して、そこを塞いで再感染を防止し、システムを設定し直してデータを再作成するという方法を採ることになる。

なお、インシデントに対応できる独自の IT セキュリティチームや CERT 等をもたない企業が被害を受けた場合には、外部の有償サポートを受けることが推奨されうる。BSI は、そうしたサービスをリスト化して公表している。ランサムウェアの被害者は、アンチボットネットアドバイザリーセンターのエキスパートに質問して回答を得ることができる（同 22-23 頁）。

b. ランサムウェアに対抗する法的構成

上記のようなランサムウェアの頒布は、通例、恐喝未遂の構成要件（刑法 253 条 1 項、3 項）だけでなく、データ変更罪（刑法 303 条 a、「隠匿」（処分権者のアクセスを排除して利用できなくさせること（BT-Drs.10/5058, 34）の類型にあたるとされる(Tobias Singelnstein/Louisa Zech in Hornung/Schallbruch, IT-Sicherheitsrecht, Rn 66) ）、さらには、コンピュータ・サボタージュ罪（刑法 303 条 b）に該当し、かつ特に刑法 303 条 b の罪については、2 項、そして組織的に行為が行われる場合には 4 項 2 号にも該当しうる(より重い犯罪となる、詳しく末尾の条文資料参照)とされる(Salomon、 Cybercrime und Lösegeld - Strafbarkeit der Zahlung von Lösegeld als Reaktion auf Erpressungstrojaner, MMR 2016, 575, 576)。

4.2.3 我が国への示唆について

以上の検討の結果、ランサムウェアに対する支払いの可否・是非という観点については、ランサムウェアに対する支払いの法的な問題については、以上の調査の結果、資金洗浄やテロリストへの支払い対応という観点が重要なことが明らかになった[34]。また、コンプライアンス等の体制構築の問題も存在する。

[34] また、ドイツ刑法 303 条 a, b は、我が国の私用電磁的記録毀棄罪等と異なり、その内容や価値を問わず、保存されたデータ全体を無権限の変更から保護する点で、無差別的なランサムウェアによる攻撃に対して使いやすい規定となっている。我が国は文書毀棄に対応する電磁的記録毀棄しか持たず、器物損壊罪に対するデータ損壊を持たないが、ドイツはそれを持っている点が重要な相違であり、我が国においても、ランサムウェアの使用それ自体を処罰する規定の整備も重要になってくるかもしれないという指摘もなされる。

これらの問題点は、後述の脅威インテリジェンスへの対応における重要な論点とも一致するので、我が国における検討については、第２　脅威インテリジェンスの利用の法律問題において総合的に考察する。

4.3 脅威インテリジェンスサービスにおける注意すべき法令上の問題についての調査

4.3.1 脅威インテリジェンスの概念

(1) 概念

脅威インテリジェンスという用語が注目を浴びている。我が国においても「脅威インテリジェンスの活用によって、従来のセキュリティ対策では見逃されていた高度なサイバー攻撃の検知、特定の業界・業種を標的とした巧妙なサイバー攻撃の防御が可能となります」などと注目を浴びているところである。

具体的な定義について、明確なものは、存在しないが、本報告においては、情報資産に対する脅威に関する情報セキュリティ目的のためのインテリジェンスもしくは、それを構成するデータとする。攻撃者の動機、標的、攻撃行動を理解するためのデータであり、セキュリティインシデントに関する情報交換のためのアプローチが対象とする情報もしくはその分析手法ということができる[35]。また、インテリジェンスとされるので、単なるデータや情報ではなく、それらを特定の目的に役立つように処理されることによって、関連し、行動に利用でき、価値のあるもの、である必要がある[36]。

脅威インテリジェンスは、各国の政策としても注目を引いているが、これは、2017 年の WannaCry と NotPetya の事件が政府の関心をひいたこと、2018 年 5 月には、欧州議会が、ロシア連邦と北朝鮮が国際法に違反していると非難したこと、国際的対応を呼びかけたこと、もし、政府と多国籍企業が情報を共有したら、これらのキャンペーンの戦略、程度、タイムスケールに対する理解が、向上すると考えられること、などがその要因であると考えられている。

(2) 分類

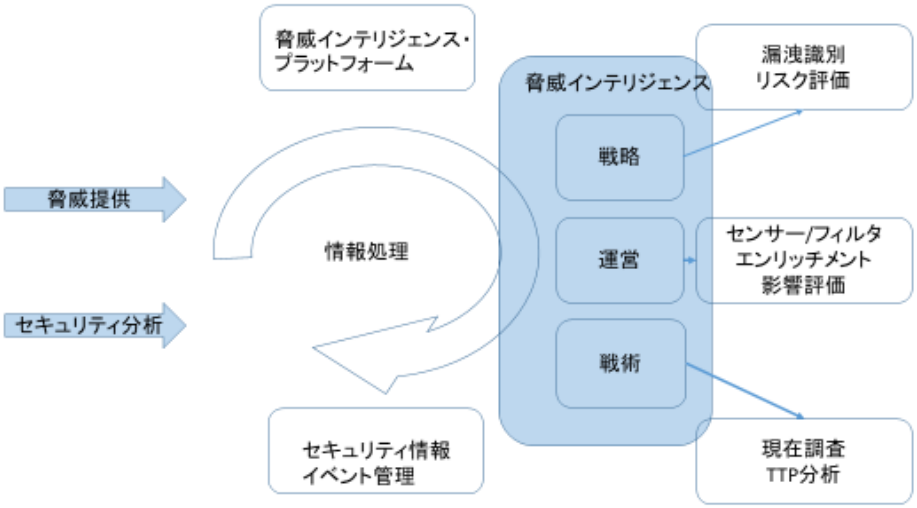
脅威インテリジェンスのプロセスは、以下の図を用いて説明することができる[37]。

---

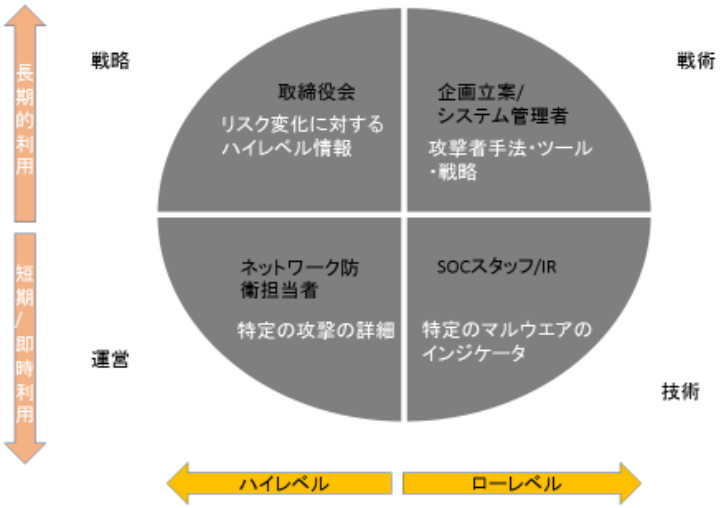
[35] Friedman & Bouchard「サイバー脅威インテリジェンスの明確なガイド（Definitive Guide to Cyber Threat Intelligence）」は、「サイバー脅威インテリジェンスとは、敵対者やその動機、意図、方法に関する知識であり、企業の重要な資産を保護するために、あらゆるレベルのセキュリティやビジネスに役立つ方法で収集、分析、普及されている」と定義している（http://cyber-edge.com/wp-content/uploads/2016/08/Definitive-Guide-to-CTI.pdf）。その他、は、「脅威インテリジェンスとは、脅威行為者の動機、標的、攻撃行動を理解するために収集、処理、分析されるデータをいう」と定義している（https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/）。

[36] この部分については「脅威インテリジェンス共有：現状及び要求事項（D5.1 Threat Intelligence Sharing: State of the　Art and Requirements」（https://protective-h2020.eu/wp-content/uploads/2017/07/PROTECTIVE-D5.1-E-0517-Threat-Intelligence-Sharing.pdf）による。

[37]「脅威インテリジェンス共有：現状及び要求事項」15 頁。



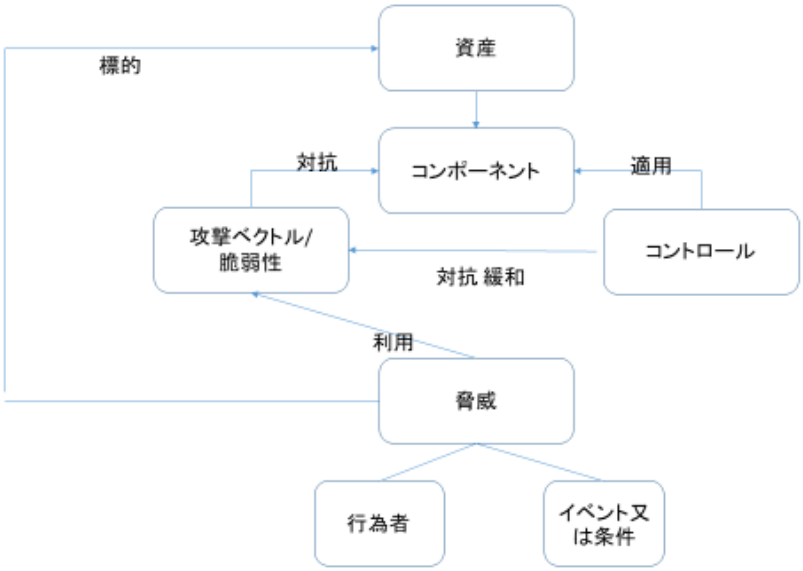
これは、サイバー脅威インテリジェンスが、戦術（脅威指標を用いて積極的に敵を探し出し、敵から防御するなどの技術的な情報。）、運用（敵対者の動機や意図、能力（TTP-Tactics, Techniques, and Procedures-戦術・技術・手順-を含む）に焦点を当てた情報）、戦略（ビジネス上の意思決定やサイバーセキュリティへの直接投資を通知するために使用される脅威に関連するリスクや意味合いについての情報）に分けられること、それらがプラットフォームの上で、イベント管理をもとに、情報の取り扱いのプロセスとしてなされることを物語っている。この戦術、運用、戦略のそれぞれのインテリジェンスの要求者と具体例については、以下の図で示すことができる[38]。



また、資産・脅威・コントロールの関係については、以下の図で示すこともできる[39]。

[38] D.Chismon ほか"Threat Intelligence:Collecting, Analysing, Evaluating"（ http://www.icsdefender.ir/files/scadadefender-ir/paygahdanesh/gheyreboomi/BehtarinRaveshha/CPNI%20-%20Threat%20Intelligence%20-%20Collecting%20Analysing%20Evaluating.pdf）6 頁。

[39] Michael Muckin ほか「サイバーセキュリティに対する脅威によるアプローチ」(A Threat-Driven



4.3.2 脅威インテリジェンスにおけるインテリジェンスの生成方法等

(1) 脅威インテリジェンスを構成するデータ

脅威インテリジェンスがどのようなデータを処理することによって得られるかという点についていえば、「サイバー脅威インテリジェンスの明確なガイド」は、レベル１（脅威インディケータ）、レベル２（脅威データフィード）、レベル３（戦略的脅威インテリジェンス）に分けて論じている。

レベル１（脅威インディケータ）とは、又は危殆化（compromise）の指標（IOC）は ある種の攻撃や危殆化の可能性を示すエンティティをいう。最も一般的なタイプは、ファイルハッシュ（署名）、攻撃に関連したドメインや IP アドレスの評判データである。技術的には、マルウェアの分析から得られるフィンガープリントが、代表的なものであるが、これは実際のマルウェア以外にもハニーポット、スキャナーから得ることができる。また、攻撃者のドメインや IP アドレスも、このような情報を形作る。実際の脅威インテリジェンスとして、このような情報が実際に提供されてもいる。

レベル２（脅威データフィード）は、脅威指標を分析し相関性のある情報をいう。これらは、セキュリティチームが攻撃に関連するパターンを特定するのに役立つし、また、インシデント対応（IR）チームが悪意のあるソフトウェアファイルの挙動を理解するのに役立つマルウェア分析も含まれている。

レベル３の戦略的脅威インテリジェンスは、アンダーグラウンドのモニタリング等によって得られる標的企業に対する特定の敵の情報をいう。この情報は、敵の動機・意図・戦略・技術・プロセスに関するものである。この情報は、その取得方法がアンダーグラウンドのモニタリング等によって得られることから、特に検討すべき事項がある。

Approach to Cyber Security)(http://ce.sharif.edu/courses/95-96/2/ce746-1/resources/root/Resources/Lockheed%20Martin%20Threat-Driven%20Approach%20whitepaper.pdf)

(2) 特に問題となる脅威インテリジェンスデータの取得方法

脅威インテリジェンスデータの取得方法として、問題点を引き起こしそうな取得方法について、例示しておく。具体的な手法としては、（1）仮想人格による HUMINT（2）ダークマーケット調査（3）ハニーポット（4）ビーコン（5）シンクホール（6）ハックバックなどがある。

1) 仮想人格による HUMINT

仮想人格による HUMINT（バーチャル HUMINT、脅威カウンター・インテリジェンス収集）とは、ネットワークにおける仮想人格を構築し、その仮想人格と通信する相手に関する情報を収集し、それをもとに、脅威の主体、ツール、技術を分析等することによってインテリジェンスを提供するプロセスである。仮想人格とは、現実には存在しない人格であり、実在の組織等との関連性を有せず、また、それを示唆しない人格であることをいう。実在の人格を偽って名乗る場合については、名誉毀損・業務妨害の問題が発生しうるが、架空の人格になりすますという場合には、そのような問題ではない。かかる仮想人格による情報取得の問題点について、①無権限アクセス／権限超過に関する問題②人格に関する問題③通信の傍受の問題④個人情報の領域外移転などの問題を考察することができる。

2) ダークウェブ調査

ダークウェブ調査というのは、通常のアクセスではアクセスしえないネットワークにおいて交換されている情報についての情報収集・分析行為をいう。当該ネットワークにアクセスするためには、通常のウェブブラウザではなく、Tor などのブラウザを利用したりする必要がある。また、特別のアクセス制限のかかっている会議室にアクセスしたりすることもある。そこでは、違法性が高い情報や物品が取引されており、犯罪の温床ともなっているとされる。

3) ハニーポット

ハニーポットとは、故意に外部からの進入を容易にした囮用のネットワーク機器をいう。マルウェアの感染活動等の検知を目的にネットワーク上に設置する（「総務省の情報セキュリティ政策」資料より）。もし、会社・組織が、国境をこえて、ハニーポットを用いて、マルウェアの情報や通信ログを収集したとした場合に、法的な問題が発生するのかということが議論されうる。

4) ビーコン

このビーコンの技術であるいわゆるウエブビーコンは、HTML を利用したメールやウェブページの閲覧者を識別する仕組みのことをいう。メールやウエブに埋め込まれた要素の解釈・表示に際してなされるサーバへの通信を分析することによって閲覧者が、IP アドレス、プロバイダホスト名、閲覧時刻、閲覧時間、閲覧した URL、そのページの参照元、検索ワード、（JavaScript を利用した場合）利用しているブラウザの種類、モニタの解像度な

どの情報を得ることができる。これについて、継続的なキャンペーンを行っている攻撃者にわざと「囮」のデータを取得させてその囮のファイルを開いた場合にビーコンがその攻撃者の情報を送ってくるということが可能である。そのような行為について、どこまでが許容され、どこからが許容されないのか、という問題が生じうる。

5) シンクホール[40]

シンクホールは、DNS シンクホールといわれ、不正なホストへの解決のリクエストを要求された場合、他の（C&C サーバ以外の）IP アドレスを返すことによりクライアントが不正な C&C サーバなどに接続するのを防止する機能である。ブラックホール DNS（パケット・ブラックホール）などとも呼ばれる。この場合、通信の傍受やネットワークの中立性との関係はどうであるのかという問題が発生しうる。

6) ハックバック

報復的ハッキング（Retaliatory Hacking）は、別名、「アクティブ・ディフェンス[41]」「バック・ハッキング」「ハックバック」「攻撃的対抗措置（offensive countermeasures）」などといわれている。ハックバックというのは、一般によく利用される用語であるということができる一方で、それゆえに法的にはきわめて多義的な意味であるといえる。

4.3.3 各国における脅威インテリジェンスサービスの利用と留意点

4.3.2 節でみたような脅威インテリジェンスにおける情報の取得方法が、特に戦略的脅威インテリジェンスにおいては、法的に種々の論点を含みうるものであることから、各国においてこれらの論点をもとに、どのような対応が考えられるのか、ということについてみていくものとする。

(1) 米国一般論

1) 脅威インテリジェンスの利用

サイバー脅威インテリジェンス（cyber threat intelligence; CTI）とは、サイバー脅威に関するデータを収集・加工して有益な情報とした上で、当該情報を加工・分析して意思決定に用いることのできる形態にしたものである[42]。すなわち、サイバー作戦（cyber operation）を

---

[40] https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523

[41] 「Active Cyber Defense (ACD)」というときには、米国国防総省の「脅威及び脆弱性についての発見、探知、分析、対応のための同調された、リアルタイムの作戦」という考え方及びそれにともなう活動をいうのが一般である。この ACD の活動は、そのために、センサー、ソフトウェア及び諜報を利用することによりネットワークスピードで作戦を実行することになる。この作戦のために、サイバー状況に対する意識及びサイバー防衛アクションプラン・実施がなされる。

[42] CREST, “What is Cyber Threat Intelligence and how it is used ? “ (https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf) 7 頁参照。

実施する敵の能力、機会、意図に関する分析された情報である[43]。

近年、政府機関、私企業におけるサイバー攻撃[44]に対する防御や法執行等において、CTIの重要性は高まっており、CTIを提供するサービスも数多く登場している。

SANSの調査に協力をした世界各国の240以上の諸組織（サイバーセキュリティサービスプロバイダ、金融機関、政府機関、技術系が多くを占める）では、CTIを利用又は生成すると回答した組織が全体の85.0%であり（2021年）、前年の7%増となっている[45]。その多くは、組織内と外部のリソースを組み合わせて活用しているが（55.7%、2021年）、社内のみでCTIを生成・利用している割合は36.5%（2021年）と前年の5%増となっている[46]。

CTIは、最近では、通常の方法ではアクセスできないダークウェブ（「闇サイト」とも呼ばれる）において収集されることが多くなっており、自社でダークウェブをモニタリングする、又はダークウェブをモニタリングするサービスを購入するといった方法によって収集されている[47]。ダークウェブは犯罪の温床となっているところ、かかるダークウェブに潜入し、一定の活動することが各種法令に違反しないかが問題となっている。

2) 脅威インテリジェンスの利用における法的留意点

a. インテリジェンスサイクルと法的留意点

CTIも通常のインテリジェンスと同様に、生成から配付に至るまでのインテリジェンスサイクルがある。すなわち、計画/要件（planning/requirements）、収集（collection）、処理（processing）、分析（analysis）、配付（dissemination）である。

[48]

「計画/要件」とは当該組織においてどのようなCTIを生成するかを定めること、「収集」とはCTIのもととなるデータ・情報を収集すること、「処理・分析」は収集したデータ・情報を一定の文脈のもと照合、編纂し、サイバーセキュリティ上の意思決定に有用な形に処理分析すること、「配付」は必要とする組織・部署に生成されたCTIを配付すること、であ

[43] SANS, “2021 SANS Cyber Threat Intelligence (CTI) Survey” (https://www.domaintools.com/resources/survey-reports/sans-2021-cyber-threat-intelligence-survey) 2頁。
[44] 「サイバー攻撃」という用語は、本稿においては、特段の記載のない限り、コンピュータシステムに対し、ネットワークを通じて、破壊活動、データ窃取、データ改ざんを行う等システムの所有者・管理者の望まないことを行う活動全般をいうものとする。
[45] 前掲SANS、3-4頁。
[46] 前掲SANS、5頁。
[47] 例えば、https://apmg-international.com/article/using-dark-web-threat-intelligence など。
[48] 前掲SANS、6頁。

る。

このサイクルにおける各段階のうち、法的に留意すべきは、特に「収集」及び「配付」となる。なぜなら、「収集」においては、外部（特にダークウェブなど）からの情報収集方法や個人情報の収集管理について一定の法令を遵守する必要があり、「配付」においては、特に CTI を外部（CTI サービスプロバイダ）から調達する組織について、その CTI の生成過程の適法性まで考慮すべきかという問題があるからである。さらに、CTI を外部と共有する場合にも一定の法的問題が生じる。

このうち、「収集」に関し、米司法省（DoJ）サイバーセキュリティユニット（CsU）[49]は、2020 年 3 月、「サイバー脅威に関する情報をオンラインで収集し、不正なソースからデータを購入する際の法的な考慮事項」（"Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources"）[50]というガイダンスを発表した。これは、法的拘束力のないものであるが、①ダークマーケットからの CTI の収集及び②違法な情報等（マルウェア、セキュリティの脆弱性、盗まれた自己データ等）の購入が連邦法に違反するかについて考え方の指針を与えるものである[51]。

以下これを踏まえて米国における CTI 利用における法的留意点について述べる。

b. アクセスにおける問題（不正アクセス、なりすまし）

前述のように CTI は、ダークウェブにおけるダークマーケット[52]において収集される場合があるところ、ダークマーケットに潜入して情報を受動的にモニタリングする行為それ自体が法令違反になる可能性は少ないとされる。

もっとも、ダークマーケットに不正アクセスした場合には、法的問題が生じる。例えば、許可なしにそのようなフォーラムにアクセスしたり、そのフォーラムで発生した通信をひそかに傍受したりする場合は、コンピュータ詐欺・不正利用防止法 （Computer Fraud and Abuse Act ; CFAA）[53]（18 U.S.C.§1030[54]）及び通信傍受法（18 U.S.C.§2511）に触れるおそれがある。また、脆弱性を悪用したり、盗まれた認証情報を使用したりするなど、不正な方法でフォーラムにアクセスすると、CFAA 及びアクセスデバイス不正行為防止法(18 U.S.C.§1029)などの法令に抵触するおそれがある。

また、架空の人物になりすまして、偽のオンライン ID を使用してアクセスすることは連

---

[49] DoJ 犯罪部門コンピュータ犯罪及び知財課内の組織。2014 年 2 月、犯罪者の電子的監視やコンピュータ詐欺・不正利用防止法（CFAA）がサイバーセキュリティに対してどのような影響を与えるかに関する専門家の助言と法的ガイダンスの中核ハブとして設置された（https://www.justice.gov/criminal-ccips/cybersecurity-unit）。

[50] https://www.justice.gov/criminal-ccips/page/file/1252341/download（原文）。翻訳は別紙参照のこと。

[51] 同ガイダンスでは専ら連邦法違反について論じており、州法や外国法が別途適用される可能性があるとの断りがある（同 2 頁）。

[52] 同ガイダンスでは、ダークマーケットについて、「ダークマーケットは、TOR（オニオンルーター）ネットワーク上にあり、オンライン通信の発信元を特定しにくくするために設計されたコンピュータの集合体である。TOR ネットワークでは、通信を暗号化し、世界中の一連のリレーを介してルーティングすることで、発信元を追跡しようとする試みを阻止する。TOR 秘匿サービス「ダークウェブ」は、TOR ブラウザを使用しないとアクセスできないサイトである。TOR 秘匿サービスとして動作しているサイトの位置は隠蔽されており追跡が困難であるため、違法行為に関連するサイトのホスティングに適した技術である。」とする（同注 4）。

[53] CFAA は、日本の不正アクセス禁止法に類似する規律を定める法律である（1986 年制定）。

[54] 合衆国法典（U.S.C.）18 巻 1030 条（コンピュータに関連した詐欺その他の関連行為）を意味する。米国の法律は、一部の例外を除きすべて、制定後に合衆国法典の関係個所に組み込まれ編纂される。この際、一つの法律に含まれる条文がすべて同じ個所にまとまって組み込まれるとは限らないため注意が必要である。

邦刑事法に違反しないが、実在の人物になりすました場合には、州法によってはプライバシー違反の民事的な問題が生じる。また、架空の人物であっても政府職員を装った場合には連邦刑法（18 U.S.C.§912）に抵触するおそれが生じる[55]。

c. ダークマーケットにおけるコミュニケーション

有用な情報を得るためには、ダークマーケットで活動する者らとコミュニケーションをとり、その信頼を得る必要がある場合がある。その際も、提供した情報が犯罪に使用された場合には犯罪の幇助・教唆（aid and abet）となる可能性がある。また、犯罪の共謀に参加し、その犯罪の実行に同意した場合には共謀罪が成立する可能性もある（なお、不正アクセス罪を定める CFAA 第 1030 条は、共謀罪や未遂罪も可罰的としている[56]）。

また、実際に起訴、有罪とならなくとも、犯罪捜査の対象となるおそれもある。

そのため、同ガイダンスでは、犯罪の実行に使用される真実の情報を提供しないよう呼びかけている。その上で、真の目的・意図を疑われ捜査に巻き込まれないためにも、

- 情報収集活動を行う前に法執行機関にその旨知らせて関係を築くこと
- 担当者が従うべき行動規則又はコンプライアンス・プログラムを策定し、法律家の確認を得ておくこと
- 担当者が実際に行った活動と収集した情報の記録をとっておくこと

を強く推奨している。

d. 盗まれた情報、マルウェア、セキュリティ脆弱性の購入

より積極的なサイバーセキュリティ活動として、担当者がダークマーケットで売りに出されている盗まれた情報、マルウェア、セキュリティ脆弱性を購入するという場合がある。同ガイダンスでは、売主が誠実とは限らず、代金を受け取って売買目的物を提供しない、盗難データの写しを破棄するとの約束を破る、等々のリスクがあることに言及する。その上で購入する際には、データの所有権、データの性質、売主の身元に鑑み、法令違反となるおそれがあることを指摘する。

なお、これらの注意事項は、CTI を扱うサイバーセキュリティ企業から一般企業が CTI 等を購入する場合（前述のインテリジェンスサイクルの「配付」における法的問題）にも同様にあてはまる。

ア）データの所有権

自己の盗まれた情報を買い戻すことは法令に違反しない。他人の盗まれた情報を購入することは、その目的によっては、なりすまし罪（identity theft）[57]又は営業秘密窃取になりうる。もっとも、買い取った情報の中に他人の個人情報や営業秘密が含まれる場合もありうる。

---

[55] 同ガイダンス 3 頁、6 頁。

[56] 18 U.S.C.§1030(b)。本書後記訳注 9 参照。

[57] 18 U.S.C. § 1028(a)(7)は、Identity Theft and Assumption Deterrence Act により加えられた条文である。「情を知って、法的権限なく、連邦法違反の不法な行為又は州法その他の法律における重罪を実行、教唆、幇助する意図で、他人の身分を証明する手段を譲渡又は使用すること」についてなりすまし（identity theft）犯罪として最大 15 年の有期刑と定める。

その場合でも、犯罪の意図や他人の経済的利益に供する目的のない限り犯罪が成立する可能性はないが[58]、他人の情報があることを知りつつ適切な措置をとらない場合にはかかる犯罪の故意や目的が推認され、犯罪捜査や個人による調査（個人情報の場合）の対象となるおそれがある。

したがって、同ガイダンスでは、第三者のデータが含まれていることが判明した段階で、速やかに分離し、それ以上アクセス、確認、使用しないようにした上で、法執行機関又は所有者に知らせ、一連の対応を文書化することを推奨する。

イ）データの性質

脆弱性やマルウェアを購入することは通常、法令に違反しないが、同ガイダンスでは 2 つの例外を挙げる。

一つは、電子通信をひそかに傍受するように設計されたソフトウェアである。「電子、機械その他の装置の設計が、有線、口頭又は電子通信の秘密裡の傍受の目的に主として有用であることを知り、又は知りうる場合に、当該装置」の意図的な所持・販売を禁止する通信傍受法（Wiretap Act）に違反する可能性を指摘する[59]。

もう一つは、後述の売主の身元に関係する問題である。

ウ）売主の身元

売主がテロ組織と関係していることを知って取引をした場合、外国のテロ組織と指定されたグループに物質的支援を提供すること、又は提供しようとすること、もしくはそのような共謀を行うことを禁じた 18 U.S.C.§ 2339B 違反として刑事責任を問われうる。

販売者が経済制裁又は貿易制裁の対象であることを知って、又は知り得たのに取引をした場合は、国際緊急経済権限法（IEEPA）に基づき刑事責任を追及されうる。

もっとも、ダークマーケットで取引をする場合、売主は身元を隠しているため、上の 2 つの刑事責任が立証される可能性は低いと指摘されている。

もっとも、IEEPA は、刑事責任だけでなく、民事上の責任も定めており、この場合、当事者は、取引の相手方が貿易又は経済制裁の対象となっていることを知らなかったとしても制裁金が課されうる（厳格責任）。このリスクを軽減するため、IEEPA の民事的執行を管轄する米国財務省海外資産管理室（OFAC）は、各企業においてリスクベースのコンプライアンス・プログラムを実施することを奨励している。

e. CTI を外部と共有する場合の法的問題

CTI の共有は、政府・民間間、民間・民間間がありうるが、米国では、連邦政府との CTI の共有は、2015 年サイバーセキュリティ情報共有法（Cybersecurity Information Sharing Act; CISA[60]）に定められている。

連邦政府との共有については、CISA 上、以下における免責措置（FOIA や行政処分等から

---

[58] 18 U.S.C. §§ 1029(a)(1)-(8), (10); 18 U.S.C. § 1832(a)参照。identification fraud (18 U.S.C. § 1028), credit card fraud (18 U.S.C. § 1029), computer fraud (18 U.S.C. § 1030), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), or financial institution fraud (18 U.S.C. § 1344)

[59] 18 U.S.C. § 2512(1)(b)

[60] 6 U.S.C. §1501～。

の免責）が施されているが、その他の私企業間等での共有については、当該免責措置はとられないため注意が必要である[61]。また、当該免責措置の適用は、たとえ連邦政府と共有する場合であっても、国家安全保障省（DHS）の提供するプロセス（自動インディケータ共有（Automated Indicator Sharing (AIS)や指定されたウェブサイト・メール・郵便での共有）で共有した場合に限られる。なお、情報共有分析センター（ISACs）や情報共有分析組織（ISAOs）と共有する場合は、ISACs や ISAOs が DHS のプロセスに従って連邦政府と情報共有するため、当該免責措置が適用される[62]。

ア）情報開示請求に基づく開示請求

米国では、情報自由法（Freedom of Information Act; FOIA）[63]に基づき、例外事由にあたらない限り、請求に応じてすべての政府情報が公開されることとなっている。そのため、政府と共有した情報が FOIA に基づく請求によって開示される懸念がありうる。

これについては、2015 年サイバーセキュリティ情報共有法（Cybersecurity Information Sharing Act; CISA[64]）において、脅威インテリジェンスの共有については FOIA による開示請求から除外される旨明示され、かつ、州法に基づく開示請求からも除外されるとされた[65]。

イ）プライバシー違反の懸念

CISA において連邦政府等と共有できるサイバー脅威情報は、サイバー脅威インディケータ及び防御策（defensive measures）である。「サイバー脅威インディケータ」とは、悪意のある偵察、セキュリティコントロールを破る方法又はセキュリティ脆弱性の悪用、セキュリティ脆弱性、正当なユーザにセキュリティコントロールを破らせたり脆弱性を悪用させたりする方法、悪意のあるサイバーC&C、インシデントによって実際又は潜在的に生じた害、その他のサイバーセキュリティ脅威、その組み合わせをいう[66]。「防御策」とは、既知又は予想されるサイバーセキュリティ脅威又はセキュリティ脆弱性を検知、防止、緩和する情報システム又は情報システム上で保存、処理、送信される情報に適用される対応、装置、手順、シグネチャ、技術、その他の措置をいう。このように、個人情報は、共有すべきサイバー脅威情報には含まれない。

そして、CISA においては、私企業において、脅威データを共有する場合には、データ内容を確認して個人情報を削除することが求められている[67]。

それに反して、セイバーセキュリティ目的に扶養な個人情報が含まれることを知って脅威データを共有し、それが外部に漏れた場合には、私企業は責任を問われる可能性がある。

---

[61] 例えば、正当な理由があれば他社に対する訴訟におけるディスカバリ（証拠開示）手続により自社の CTI が開示されるということがありうる。
[62] 6 U.S.C. §1505(b)(1)。「2015 年サイバーセキュリティ情報共有法において非政府組織が連邦政府とサイバー脅威インディケータ及び防御策を共有するためのガイダンス」（https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf）15 頁。
[63] 5 U.S.C. § 552。
[64] 6 U.S.C. §1501～。
[65] 6 U.S.C. §1504(d)(3)
[66] 6 U.S.C. §1501(6)
[67] 6 U.S.C. §1503(d)(2)

ウ）政府の措置又は民事責任からの免責

CISA においては、CTI の共有につき CISA の手続に従って行われる限り民事上の責任は免除されると明記された[68]。また、共有された CTI に基づいて政府による規制・制裁がされることもない[69]。

もっとも、訴訟のディスカバリ手続で開示される可能性はあり、国外における訴訟については保護を及ぼしていない点に留意する必要がある。

エ）その他

以上の通り、情報共有に伴って、一定の法的保護が施されているものの、データが共有されたのにそれに基づいて行動しなかった場合には、法的責任が伴うことに注意が必要である[70]。サイバー攻撃等によりデータ流出等が生じ、ユーザ等から民事上の責任を問われた場合、私企業が「合理的（reasonable）」な措置をとったかが判断基準となるところ、脅威インテリジェンスを共有している場合には、それを認識していることを前提として合理性が判断されうる、ということである。

(2) 英国

英国において脅威インテリジェンスサービス[71]の利用についてふれた文献は、非常に多い。例えば、「政府におけるサイバー脅威インテリジェンス：意思決定及び分析のためのガイド」（Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts）[72]は、サイバー脅威インテリジェンスの全方面にわたるガイドラインであり、特に政府におけるサイバー脅威インテリジェンスの利用について解説している。ここでは、ダークウェブでの情報に関しては、インテリジェンスは、オープンソースから得られるものがきわめて多く、ダークウェブの情報を取得することは推奨しないとしている。違法なコンテンツについてアドバイスを求めるときは、NCSC（国家サイバーセキュリティセンター）に相談するか、国家犯罪庁（National Crime Agency (NCA)）に相談するようにとされている。また、政府部門のネットワークについては、Tor ノードに対しての接続をできないようにすることが推奨されている（同書　5.1.3）。また、ヒューミントのソースについての実務規範があり、必要に応

---

[68] 6 U.S.C. §1505(b)(1)
[69] 6 U.S.C. §15054(d)(5)(D)(i)
[70] “Legal Implications of Threat Intelligence Sharing” Sans Cti Summit 2018（https://ciampeathehomedesignings.com/）
[71] 英国においてサイバー脅威インテリジェンスにふれた文献等は、枚挙にいとまがない。公的な団体等から公表されたものとしては、また、イングランド銀行の CBEST　（規制当局の監督ツールキット）についてのガイドである「CBEST　－脅威インテリジェンスによる評価」（CBEST Threat Intelligence-Led Assessments、https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide）がある。
[72] https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf）　また、この分析は、「不知を探索する　脅威ハンティングのガイド」（“Detecting the Unknown:
A Guide to Threat Hunting”　https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Detecting-the-Unknown-A-Guide-to-Threat-Hunting-v2.0.pdf）「あなたの存在をコントロールする　デジタルリスクとインテリジェンス」（Controlling Your Exposure: A　Guide to Digital Risk and　Intelligence）（https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Controlling-Your-Exposure-A-Guide-to-Digital-Risk-and-Intelligence-v2.0.pdf）、とシリーズをなすものである。

じて、それを参照するようにとされている（同 5.1.6）。

また､他のガイダンスとして CREST｢サイバー脅威インテリジェンスの概念と利用｣(What is Cyber Threat Intelligence and how is it used?）がある[73]。CREST は、情報セキュリティ技術市場を代表し、サポートする国際的な非営利の認定・認証機関である[74]が、この報告書は、サイバー脅威インテリジェンスの実践と調達に関する実践的なアドバイスを提供する入門書である。サイバー脅威インテリジェンスを支える重要な概念と原則を概説し、組織がサイバー脅威インテリジェンスを使用して、潜在的なサイバーを予防、検出し、セキュリティインシデントに対応する方法を解説している。また、必要な能力を備えた適格なサプライヤを選択するためのガイダンスと基準も提示している。同書では、外部の脅威インテリジェンスの利用について、「安心感」があるとして、脅威情報収集のいくつかの側面では、脅威の行為者や潜在的に悪意のある人との相互作用を伴うこと、コンテンツの収集で避けられないリスクの一部を軽減するために、外部の脅威インテリジェンス・サプライヤを利用することができることが触れられている。これらのプロバイダーは､これらの課題にも精通しており、リスクと潜在的な法的問題を解決することができるとされる。そこでは、関連する規定として 1998 年人権法（第 8 条）、2000 年調査権限規制法（RIPA）、1990 年コンピュータ不正使用法、2018 年データ保護法（DPA）、1996 年刑事手続捜査法（CPIA1996）、2010 年贈収賄法、2002 年犯罪収益法（POCA）などがあげられている[75]。

(3) ドイツ

不法な情報源からのデータの購入等に対する規制が最近になって刑法に入れられた点に特徴がある。我が国における類似の規制には不正競争防止法 21 条 1 項各号の営業秘密侵害罪や割賦販売法 49 条の 2 等を挙げることができるかもしれないが、同条の罪は情報の価値に基づいた保護であって、ハッキング等、獲得過程の不正性に着目したものではない。それゆえに、事実上、ダークウェブ対策を狙ったものでもない。これに対して、ドイツ刑法 202 条 d のデータ故買罪は、ある程度ダークウェブ対策にも焦点を当てたサイバーセキュリティの維持のための規定だと理解することができる。

2015 年の刑法改正で入ったデータ故買罪は，無権限アクセス罪、データ傍受罪その他の違法な行為により獲得されたデータの移転を包括的に処罰しようとする規定である。

処罰の欠缺があるのでデータ故買を独立して処罰する必要があるとされた。すなわち、まず、本罪が挿入される前にも、既に刑法 202 条 c が、無権限アクセス等の遂行のために使われるパスワードや保護コードの転売等を禁止しているところではあった。もっとも、同規定では、それらに保護の範囲が限定され、無権限アクセス等で取得された場合を除き（この場合は刑法 202 条 a で保護されうる）、キャッシュカードやクレジットカードに関するデータの保護ができなかった（BT-Drs. 18/5088, 25）。データ故買にのみ関与する者は、故買の時点では既に先行する無権限アクセス罪等が終わっているから、故買自体を処罰する規定が

---

[73] https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf

[74] https://www.crest-approved.org/index html　なお、設立時においては、The Council of Registered Ethical Security Testers（Crest）であって、英国で侵入テストのための業界団体及び職業団体という性格を有していた。

[75] データ保護法の部分は、GDPR に対応した 2018 年と修正した。なお、調査権限法については、シギントについての 2016 年調査権限法とヒューミントに関する 2000 年調査権限規制法とがあり、現時点においては、双方と関連性があるものと考えられる。

ない限り、先行犯罪の共犯として処罰できなかった（BT-Drs. 18/5088, 25）。また、データの購入者において当該データを用いて犯罪をするつもりがない限り、当該データを使ったコンピュータ詐欺等を検討することも難しい（BT-Drs. 18/5088, 25）。連邦データ保護法や不正競争防止法上の営業秘密保護の規定では、客体が限定されすぎる（BT-Drs. 18/5088, 25-26）。

以上の考慮に基づいてデータ故買罪が刑法 202 条 d として入れられた。本罪の保護法益はデータの形式的な秘密（das formelle Datengeheimnis）である（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 3）。データの形式的な処分権といってもよい（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 3, 14）。データの内容は要保護性との関係では重要でない（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 6）。処分権者は、基本的にデータを収集し、保存した者のことであり、データ媒体の所有や占有の帰属自体は決定的ではないし（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 14）、データ保護法上の権利とここでいう処分権の双方が同一人に帰属することはありえるが、データ保護法上の関係者であるか否かは判断にあたって意味はない（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 15）。

客体は、一般にアクセスができず、かつ他の者が違法な行為により獲得したデータである。一般にアクセスできるデータについては、その利用により上記法益の侵害はない、とされる（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 12）。「一般にアクセスできる」とは、ログイン、許諾、対価の支払いなく、あるいは事前にアカウント登録、許諾、対価の支払いをすることによって、利用可能になっていることをいう（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 12）。公開されている著作物も、有償の場合も含め、「一般にアクセスできる」に該当するゆえに、著作権侵害によって得られた著作物も、本罪の客体の要件を充たさない（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 12）。

違法な行為により獲得したデータというときの違法な行為には幅広い違法行為が含まれる。行為者の責任要件の具備や告訴は不要である（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 13）。無権限アクセス（刑法 202 条 a）やデータ傍受（刑法 202 条 b）だけでなく、処分権者の形式的な処分権に対しても向いている行為によってデータが取得されているのであれば、窃盗、詐欺、コンピュータ詐欺等により獲得される場合も含む（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 13）。一方で、ポルノの頒布のような公共の利益を害するだけの場合、並びに連邦データ保護保護法上、可罰的な行為の場合（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 16）、単なる契約違反、契約上のアクセス制限の違反、及び著作権を侵害してデータを複製する場合には、当該行為は形式的な処分権に向けられたものではないから、ここでいう違法な行為による獲得にはならない（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 17）。

4.3.4 米国司法省「オンラインサイバー脅威インテリジェンスを収集し、不法な情報源からデータを購入する際の法的考慮事項」の翻訳及び解説（暫定版）

(1) 米国司法省「オンラインサイバー脅威インテリジェンスを収集し、不法な情報源からデータを購入する際の法的考慮事項」の翻訳

前掲「サイバー脅威に関する情報をオンラインで収集し、不正なソースからデータを購入

する際の法的な考慮事項」を、JNSA から提供された下訳を参考に、別紙の通り正式に翻訳した。

(2) 米国司法省「オンラインサイバー脅威インテリジェンスを収集し、不法な情報源からデータを購入する際の法的考慮事項」の解説

同ガイドラインの翻訳に訳注をつけた部分につき米国法の見地から解説を付加する。

1) 訳注 1

ダークマーケットに不正アクセスした場合、CFAA（18 U.S.C.§1030「コンピュータに関連した不正及び関連する行為」）違反となりうると指摘されている。具体的に 18 U.S.C.§1030(a) の概要[76]を見ると以下の通りである。

(a) 以下のいずれかの行為をした者は罰せられる。

(1) 無権限で又は授与されたアクセス権限を超過して，コンピュータにアクセスし、政府によって保護された情報を取得し、故意に他者に送信等した者。

(2) 権限なく、又は、権限を超えてコンピュータに故意にアクセスし、それによって、以下の情報を取得した者。

(A) 金融機関もしくは 15 巻 1602(n)条に定めるカード発行者の金融記録に含まれる情報、又は、公正信用報告法（15 U.S.C.§1681 以下）に定める消費者報告機関における消費者に関するファイルに含まれる情報、

(B) 合衆国のいずれかの省庁からの情報、

(C) いずれかの保護されたコンピュータ（専ら金融機関や合衆国政府が用いるコンピュータ又は州際もしくは外国との取引もしくは通信に用いられるコンピュータ）からの情報

(3) 故意に、権限なく、合衆国政府のコンピュータであって、一般公衆がアクセスできないものにアクセスし、合衆国政府の使用に影響を及ぼした者

(4) 情を知って、詐欺の意図で、保護されたコンピュータにアクセスし、その行為が詐欺を助長するものであり、何らかの価値のあるものを取得した者

(5) (A) 情を知って（knowingly）、プログラム、情報、コード又はコマンドを送信し、この行為によって、意図的に、権限なく、保護されたコンピュータに対し損害を与えた者

(B) 意図的に(intentionally)、権限なく、保護されたコンピュータにアクセスし、この行為によって、無謀に（recklessly）損害を惹起した者

(C) 意図的に(intentionally)、権限なく、保護されたコンピュータにアクセスし、この行為によって、損害及び損失を惹起した者

[76] 逐語訳ではないため注意されたい。原文は、https://www.law.cornell.edu/uscode/text/18/1030 参照。

(6) 情を知って、詐欺の意図で、コンピュータを無権限でアクセスできるパスワード又はそれに類似の情報を譲渡その他の処分をした者であって、

(A) 当該譲渡等が州際取引又は外国取引に影響を及ぼした場合

(B) 当該コンピュータが合衆国政府によって用いられるものである場合

(7) 金員その他の価値ある物を人から奪う意図で、以下を含む通信を、州をまたいで又は外国との間で送信した者

(A) 保護されたコンピュータに損害を生じさせるとの脅迫

(B) 保護されたコンピュータから権限なく、又は権限を超えて情報を取得するとの脅迫

(C) 保護されたコンピュータの損害に関連して金員その他の価値ある物の要求

正当なサイバーセキュリティ目的でダークマーケットに不正アクセスした場合、該当しうるのは、18 U.S.C.§1030(a)(2)(C)、(a)(4)である。CFAA は、従前よりかなり拡張的に適用されてきているという背景があるため[77]、十分に注意する必要がある。

2) 訳注 2

アクセスデバイスとは、「金員、物品、サービスその他価値ある物を取得するために、又は、資金移動を開始するために（専ら書面に端を発する移動を除く）、それ単体で、又は他のアクセスデバイスと合わせて用いることのできる、カード、プレート、コード、アカウント番号、携帯端末のシリアルナンバー（ESN）、携帯端末の識別番号、個人識別番頭、その他の電気通信サービス・施設・装置の識別子、その他のアカウントにアクセスのための手段」を意味する（18 U.S.C.§1029(e)(1)）。例えば、アカウントにアクセスするためのパスワードもアクセスデバイスに該当する。

18 U.S.C.§1029（「アクセスデバイスに関連した不正及び関連する行為）は、アクセスデバイスの所持等を犯罪と定める。すべての類型について、「*情を知って（knowingly）、かつ、詐欺の意図をもって*」という主観的要件が要求されており、サイバーセキュリティ目的を有していることにより自動的にこの主観的要件がないということにはならないが、犯罪の動機を持たずにダークマーケットにアクセスし、盗難データ等を購入する場合には、これに基づき起訴される可能性は低い。

訳文は以下の通りである[78]。

(a) 以下に該当する者は、当該行為が州際取引又は外国商取引に影響する場合には、本条(c)に定める法定刑によって罰せられる。

(1) 情を知って（knowingly）、かつ、詐欺の意図をもって、一つ以上の偽アクセスデバイス（counterfeit access devices）を製造、使用、不正に売買をした者

---

[77] 「権限なく（無権限）」という構成要件について、使用約款違反の場合も含まれるとされており、使用約款違反が民事上の責任のみならず、刑事上の責任につながることについて強い批判があるものの法改正には至っていない。*United States v. Swartz, 357 F.2d 322（被告人は、ハーバードの学生で論文アーカイブである JSTOR のアカウントを所持していたところ、MIT のコンピュータを使用して JSTOR にアクセスし、そこから 400 万以上の記事を自己のパソコンに自動ダウンロードしようとし、その過程で JSTOR のコンピュータの機能を損ない、MIT のサーバーをダウンさせ、MIT の他のコンピュータからのアクセスを不可能にしたことにより、通信詐欺（wire fraud）、コンピュータ詐欺、不正アクセスによる情報取得、不正アクセスによるコンピュータ損害等により逮捕、起訴され、公判中に被疑者が自殺した。）参照。*

[78] なお、1029 条(b)は、同条(a)の行為の未遂、共犯についての定めである。

(2) 情を知って（knowingly）、かつ、詐欺の意図をもって、1 年間において一つ以上の偽アクセスデバイスを不正に売買し、又は使用し、かつ、その行為によって、当該期間中に累計 1000 ドル以上の価値を得た者

(3) 情を知って（knowingly）、かつ、詐欺の意図をもって、15 個以上の偽アクセスデバイス又は無権限アクセスデバイス（unauthorized access devices）を所持する者

(4) 情を知って（knowingly）、かつ、詐欺の意図をもって、デバイス製造装置（device-making equipment）を製造、管理、所持、不正に売買した者

(5) 情を知って（knowingly）、かつ、詐欺の意図をもって、一つ以上のアクセスデバイス（access devices）を一人以上の者に発行し、1 年の間に 1000 ドル以上の価値を取得する取引を成立させた者

(6) アクセスデバイスの発行者の権限なく、情を知って（knowingly）、かつ、詐欺の意図をもって、以下を人に求めた者

(A) アクセスデバイスの提供、又は、

(B) アクセスデバイスに関する情報若しくはアクセスデバイスを取得するためのアプリケーションの販売

(7) 情を知って（knowingly）、かつ、詐欺の意図をもって、通信サービスの無権限使用を取得するために改ざん又は変更された通信装置を使用、製造、不正に売買、所持、管理する者

(8) 情を知って（knowingly）、かつ、詐欺の意図をもって、スキャニングレシーバー[79]を使用、製造、取引、管理、保有、所持する者

(9) （略）

(10) クレジットカードの加盟店又はその代理人の権限なく、情を知って（knowingly）、かつ、詐欺の意図をもって、他人に、アクセスデバイスによって生成された 1 つ以上の証拠又は記録を、支払のために、加盟店又はその代理人に対し、提示させた者

3) 訳注 3

18 U.S.C.§1030 (e)(2)(B)は、CFAA の域外適用の根拠規定である。訳文は以下の通りである

(e)(2) 「保護されたコンピュータ」とは、以下のいずれかのコンピュータを意味する。

(A) （略）

(B) 州際間又は外国との取引又は通信に使用されるものであって、米国の州際間又は外国との取引又は通信に影響を及ぼす方法で使用される米国外に所在するコンピュータも含む。

[79] 「スキャニングレシーバー」とは、119 章に違反して音声通信（wire communication）もしくは電気通信（electronic communication）を傍受するために、又は、携帯端末のシリアルナンバー（ESN）、携帯端末の識別番号、電気通信サービス・装置・ツールのその他の識別子を傍受するために使用されるデバイス又は装置を意味する。

4) 訳注 4

*hiQ Labs, Inc. v. LinkedIn Corp.*事件は、ボットを使用して LinkedIn の公開プロフィール情報を web スクレイピングしていたデータ分析会社 hiQ Labs, Inc.に対して、LinkedIn が停止通告書（cease-and-desist letter）を送付したことについて、hiQ Labs, Inc.が、LinkedIn による停止通告を解除する旨の仮処分（preliminary injunction）及び CFAA 違反等がないことの確認判決を求める訴訟を起こしたものである。地裁において hiQ Labs, Inc.の求める仮処分が認められたところ、連邦高裁においてもこれを支持する判決を下した。

仮処分に対する控訴の判断の基準は、原判決が裁量の範囲を逸脱したか、という控訴人にとってはハードルの高いものであって、仮処分の要件は、(1)本案で勝訴の可能性があること、(2)仮処分がなければ回復不能な損害（irreparable harm）が生じるおそれがあること、(3)利益較量（balance of equities）上仮処分をすべきこと、(4)仮処分が公共の利益に資すること、であり[80]、本件では、LinkedIn に使用を中止されると原告の事業が停止してしまうという強力な事情があったため（(2)の要件）、公開情報についての web スクレイピングが CFAA 違反にあたらないかについて直接判断したものではない。もっとも、停止通告書を受領した後のスクレイピングは CFAA 上の「無権限（without authorization）」にあたり CFAA 違反にあたりうるとの LinkedIn の主張に対し、詳細な検討を加えている。その中で、最近の高裁判決では企業の利用規約違反を「無権限」とする契約ベースの解釈が否定されていると指摘した上で、CFAA は、(1)アクセスが一般に公開されアクセスに許可が必要のない情報、(2)アクセスに許可が必要であり許可が与えられた情報、(3)アクセスに許可が必要であり許可が与えられていない情報を想定しており、本件の情報は(1)にあたるとし[81]、一般に公開されたデータへのアクセスは CFAA 上の無権限アクセスにあたらないと結論づけたことは注目に値する。

現在、仮処分の判断につき最高裁に係属中である[82]。

これに対し、*Konop v. Hawaiian Airline,Inc.*事件は、被告会社の労働組合の運営に反対する被告会社の従業員であった原告が、被告会社等を批判するサイトをクローズトの環境で立ち上げ、会社幹部に見せない等と定めた利用規約に同意した他の従業員に限りアカウントとパスワードを付与していたところ、一部の従業員がその付与されたアカウントとパスワードを幹部に渡し、被告会社が原告のサイトを数十回にわたり閲覧していたことにつき、原告が通信傍受法や保存通信法（Stored Communications Act; SCA）違反を主張して提訴したという事件である。なお、通信傍受法違反で認められる民事上の損害額は SCA 違反の場合よりも大きいためにいずれの法律違反が認められるかが問題となった。この点、高裁は、同サイトは、「電子通信（electronic communication）」にあたるが、傍受（interception）は送信中のデータを見ることであって保存中のデータを閲覧することは含まれないとして通信傍受法違反は認めなかった。しかし、SCA では、「電子通信サービスが提供される施設に故意に権限なく（without authorization）アクセス」した場合を法令違反としているところ[83]、「無権限」の定義には触れずに原被告とも無権限であることを認めているとして被告の SCA 違反

---

[80] Munaf v. Geren, 553 U.S. 674, 128 S.Ct. 2207, 2218-19 (2008)
[81] *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019)、29-30 頁。
https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2019-09-09 html
[82] https://www natlawreview.com/article/hiq-files-opposition-brief-supreme-court-linkedin-cfaa-data-scraping-dispute
[83] 18 U.S.C. § 2701(a)(1)

の主張を認めた。ここでは、他人のユーザアカウントとパスワードを使用して当該他人の承諾を得て制限サイトに入ることが「無権限」とされていることになる。

SCA も CFAA も「無権限」アクセスを違法としているところ、「無権限」の定義を定めていない[84]。そのため、本書注 77 にも述べたように、運営者の設定する利用規約違反も「無権限」とされて刑事責任が問われうる状況があり、それに対して批判があり改正の試みがなされているものの実現していない。2010 年に改訂（第 2 版）されたサイバー犯罪起訴に関する司法省発行のマニュアル「Prosecuting Computer Crimes（コンピュータ犯罪の起訴）」[85]では、18 U.S.C.§1030 において無権限アクセスと同様に犯罪とされる「権限超過（exceeding authorized access）」アクセスの要件である「権限超過」の立証として、利用規約（terms of use）違反を示せばよいとされている[86]。もっとも、同マニュアルにおいても、故意による利用規約違反のみで 1030(a)(2)(C)に基づく犯罪が成立するとすれば警察に過大な権限を付与し、インターネットを使用する市民に対する不意打ちとなる、と判示した United States v. Drew 事件（地裁判決）[87]について言及している[88]。最近は、利用規約違反は無権限としない旨の判例が出てきている[89]。

5) 訳注 5

サイバー・タスク・フォース（CTF）は、FBI の 56 の地方局に存在する。情報共有、インシデント対応、共同法執行、インテリジェンス活動を通じて国内のサイバー脅威の捜査に携わることをミッションとする。全国サイバー捜査ジョイント・タスク・フォース（National Cyber Investigative Joint Task Force; NCIJTF）が連邦レベルでの捜査を担当するのに対し、CTF は州・地方レベルでの捜査を主に担当するが、NCIJTF とも常に連携を図っている[90]。

合衆国シークレットサービス電子犯罪タスク・フォース（ECTF）は、2001 年米国愛国者法において設置が義務付けられた組織で、教育機関、民間、地方・州・連邦法執行機関が協力して「重要インフラ及び金融決済システムに対する潜在的なテロ攻撃を含む様々な形態の電子犯罪を防止、検知、調査する」ための組織である[91]。

6) 訳注 6

18 U.S.C.§912 は、連邦政府の役員や従業員になりすます行為を禁じる。訳文は以下の通りである。

> *連邦政府その他の省庁、その職員の権限を有する職員又は従業員であると偽り、もしくはなりすますこと、又はそのように偽り、なりすまして、何らかの金員、書類、*

---

[84] *Konop v. Hawaiian Airline,Inc.*, 302 F.3d 868, 876 (9th Cir. 2002)、注 8。https://caselaw findlaw.com/us-9th-circuit/1167429 html#footnote_8
[85] 同ガイドライン注 46 記載の出版物である。
[86] 同マニュアル 8-9 頁。https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf
[87] United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009)
[88] 同マニュアル注 3。
[89] Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016)（ウェブサイトの利用規約違反のみでは―他に何もない限り―CFAA 上の責任は成立しない。）、United States v. Nosal, 676 F.3d 854, 858 (9th Cir. 2012)（「CFAA について会社のコンピュータ使用制限違反や忠実義務違反まだ CFAA の適用を広く及ぼす解釈をする他の高裁の判断は説得的ではない。」）
[90] https://www fbi.gov/file-repository/cyber-task-forces-fact-sheet.pdf/view
[91] https://obamawhitehouse.archives.gov/files/documents/cyber/United%20States%20Secret%20Service%20-%20Electronic%20Crimes%20Task%20Forces.pdf

文書その他の価値のある物を要求もしくは取得した場合、本章に従って罰金又は/及び3 年以下の有期刑が科される。

7) 訳注 7

誘発（solicitation）罪は、通常、(1)他人に犯罪を実行させる目的で、 (2)他人に犯罪を実行するよう奨励し、又は他人に贈賄、要求、命令すること、を構成要件とする。日本法における教唆・幇助（aid and abet）では、他人（正犯）が犯罪の実行行為に出る必要があるが、誘発罪では正犯の実行行為は必要なく、単独で成立する。また、誘発を受けた者が犯罪行為を行う意思がない、又はできない場合でも成立する。さらに、共謀（conspiracy）罪では通常、犯罪の合意に沿った犯罪に向けた何らかの明白な行為（overt act）が必要であるが、誘発罪ではそれも不要である。

8) 訳注 8

18 U.S.C.§2 は、正犯の定義を定める。訳文は以下の通りである。

(a) 連邦犯罪を犯した者、その実行を幇助、教唆、助言、命令、誘導し、もしくは実行させた者は、正犯として処罰される。

(b) 本人もしくは他人によって直接実行された場合、連邦犯罪となる行為を故意に惹起した者は、正犯として処罰される。

18 U.S.C.§371 は、共謀に関する規定であり、訳文は以下の通りである。

連邦犯罪を犯し、又は合衆国その他の省庁を欺罔するために、何らかの方法、目的により、2 人以上の者が共謀し、そのうち1 人以上の者が共謀の目的を達成するための何らかの行為をした場合、本章に従って罰金又は/及び5 年以下の有期刑が科される。（略）

9) 訳注 9

18 U.S.C. § 1030(b)は、18 U.S.C.§1030「コンピュータに関連した不正及び関連する行為」における共謀罪及び未遂罪の規定である。一般的な共謀罪には、共謀（合意）の他、1 人以上の者が共謀の目的を達成するための何らかの外形的行為をすることが必要であるが（18 U.S.C.§2）、§ 1030 の共謀ではそうした行為は必要なく共謀だけで足りるとされている。

したがって、この場合、構成要件は、共謀の事実と共謀の故意のみとなる。担当者がフォーラムにおいて他人とコミュニケーションを図り外観上共謀があるように見える場合には、共謀の故意がないことを示すことが、無用な捜査に巻き込まれないために非常に重要となる。したがって、同ガイダンスが指摘するように、セキュリティ目的で行動している担当者は、共謀の故意がないことを示すため、事前に FBI 等に連絡をし、行動規則を遵守し、活動履歴を記録するなどすることが重要となる。

18 U.S.C. § 1030(b)の訳文は以下の通りである。

(b) 本条(a)（18 U.S.C. § 1030(a)）の犯罪を実行を共謀し、又はそれを実行しようとする者は、本条(c)項の通り罰せられる。

10) 訳注 10

18 U.S.C. § 1832 は、営業秘密の窃取に関する規定であり、訳文は以下の通りである。

(a) *州際間取引又は外国取引で使用されている、もしくは使用されようとしている製品又はサービスに関連する営業秘密を、その所有者以外の者の経済的利益に供する目的（intent）で、又は、その営業秘密を害することを目的として、もしくはそれを知りながら、以下のことを知りつつ（knowingly）行った場合には、本条(b)に定める場合を除き、本章に従って罰金又は及び10 年以下の有期刑が科される。*

(1) 当該情報を窃取し、権限なく私用に供し、横領し、持ち去り、もしくは隠し、又は詐欺、術策、欺罔により取得した場合

(2) 当該情報を、権限なく、複写、複製、スケッチ、描画、撮影、ダウンロード、アップロード、変更、破棄、コピー、転送、送信、郵送、通信又は譲渡した場合

(3) 窃取され、権限なく横領、取得、変更されたことを知りつつ、当該情報を受領、購入、所持した場合

(4) (1)から(3)に定める罪の未遂

(5) (1)から(3)に定める罪を犯すために、2 人以上の者が共謀し、そのうち1 人以上の者が共謀の目的を達成するための何らかの行為をした場合。

このように、営業秘密の窃取の罪が成立するには、所有者以外の者の経済的利益に供する目的又は営業秘密を害する目的もしくは害することについての悪意（害することを知っていること）が必要である。したがって、セキュリティ目的で脆弱性等を購入する場合には、これらの主観的要件がないことを後日示すことができるように行動していくことが重要となる。

11) 訳注 11

18 U.S.C.§ 2339B は、情を知って（knowingly）、外国のテロ組織に重要な支援又は資源（material support or resources）[92]を提供すること、又は提供しようとすること、もしくはそのような共謀を行うことを禁じている。「情を知って（knowingly）」とあるため、犯罪が成立するためには、外国のテロ組織に支援を提供していること、すなわち取引の相手方が外国のテロ組織に関係していることを知っている必要はあるが、テロ活動を支援する具体的な意図を有している必要はない[93]。

よって、セキュリティ担当者やその帰属するセキュリティ企業が、取引の相手方についてテロ組織と関係していることを知らなければ、この犯罪は成立しないが、主観的な要件について無用な捜査に巻き込まれないためにも、そして、後述の民事的責任を追及されないためにも、コンプライアンス・プログラム等を厳格に遵守する必要がある。

なお、本罪には域外規定があり（同条(d)）、行為者が合衆国民である場合や、行為後に合

[92] 「重要な支援又は資源（material support or resources）」とは、有形無形の資産又はサービスを意味し、通貨、通貨代替物、有価証券、金融サービス、宿泊施設、訓練、専門家の助言・支援、隠れ家、虚偽の文書・身分証明書、通信装置、施設、武器、致死物質、爆発物、人員（1 人以上の個人で行為者本人を含む）、輸送を含むが、医療品又は宗教的物質は含まない、とされる（18 U.S.C.§ 2339A(b)(1)）。

[93] *Holder v. Humanitarian Law Proj.*, 561 US 1, 17 (2010)

衆国に滞在している場合、州際間取引や外国取引に影響する場合には適用されるとあるため、広範囲で適用されることに注意が必要である。

12) 訳注 12

国際緊急経済権限法（International Emergency Economic Powers Act; IEEPA）は、1977 年に施行された法律である。対敵貿易法（Trading with Enemy Act）が大統領に戦時に限り対外的な経済制裁の権限を認めるのに対し、IEEPA は、戦時のみならず平時においても、米国外において、米国の国家安全保障、外交政策、経済に対し、異例かつ重大な脅威がある場合に[94]、大統領が国家緊急事態宣言を発付して、指定国・国民が関与する取引又は指定国等が利害関係を有する財産の使用、譲渡、輸出入等[95]を調査、規制、禁じる制裁を行うことを認めるものである[96]。2020 年 12 月時点で同法に基づき有効な国家緊急事態宣言は 40 あり[97]、2020 年 11 月に発令されたトランプ政権下における中国に対する証券投資の経済制裁も同法に基づくものである[98]。

IEEPA 違反、その未遂、共謀、教唆・幇助に対しては、民事上の制裁金及び刑事上の法定刑が定められている。なお、IEEPA に基づく刑事訴追は司法省の国家安全保障部（National Security Division）が、民事上の責任追及は米国財務省海外資産管理室（OFAC）が担っている。根拠条文は、具体的には以下の通りである。

50 U.S.C. § § 1705

(a)　（略）

(b)　民事上の制裁金

本条(a)に定める違法行為（注：IEEPA 違反、その未遂、共謀）を行った者は、以下のいずれか大きい額を超えない金額の民事上の制裁金が課される。

(1) 250,000 ドル、又は

(2) 制裁金が課される違反の基礎となる取引額の 2 倍の額。

(c)　刑事上の法定刑

本条(a)に定める違法行為（注：IEEPA 違反、その未遂、共謀）を、故意に行い、故意に行おうとし、又はその実行について故意に共謀し、もしくは幇助・教唆した者が有罪判決を受けた場合、1,000,000 ドル以下の罰金、又は、自然人の場合は同額の罰金もしくは/及び 20 年以下の有期刑が科される。

この条文から明らかなように、刑事責任を追及する場合には、行為者に故意が必要であるから（すなわち過失犯規定はない）、セキュリティ担当者がセキュリティ目的で経済制裁対象と知らずに取引した場合に起訴されることはまずない。もっとも、捜査に巻き込まれる可

---

[94] また、IEEPA に含まれる規定（50 U.S.C. § § 1701-1707）ではないが、米国国民によって開発された技術や専有情報をサイバー空間における経済スパイ又は産業スパイ活動を、情を知りながら要求、関与、支援、推進、又はそれにより不当に多大な利益を得た外国人について、大統領は、IEEPA に基づいて、その取引を禁じ、資産を凍結することができる、との規定もある（50 U.S.C. § § 1708(b)(1)(2)）。当該外国人は、特別指定国民・凍結者（Specially Designated Nationals and Blocked Persons; SDN）に登録される。

[95] 資産凍結も含まれるが、資産没収は戦時の場合に限られる（50 U.S.C. § § 1702(c)）。

[96] 50 U.S.C. § § 1701, 1702

[97] 梅川健「アメリカ大統領権限と緊急事態法制：国際緊急経済権限法と経済制裁を中心に」1-2 頁。（https://www.cistec.or.jp/publication/journal_mokuji/2101-04_tokusyuu01.pdf）

[98] 同経済制裁は、「共産党軍需企業に融資する証券投資の脅威への対応策（Addressing the Threat from Securities Investments that Finance Communist Chinese Military Companies）」という大統領命令に基づく。

能性はあるため、故意がないことを示すことができるようにしておくべきである。

これに対し、民事上の責任を追及する場合には、条文上明らかなように、故意は要求されておらず、同ガイダンスでも指摘されているように[99]、「厳格責任」に基づいて、すなわち、取引相手が指定国であると知らなかったことに過失がある場合はもとより過失がなくても、民事上の制裁金が課される場合がある。

したがって、ダークマーケットにおいて情報等を購入するセキュリティ企業等は、現在存在する制裁の対象国と制裁内容を常時把握しておく必要がある。その方法として、OFAC は、「A Framework for OFAC Compliance Commitments（OFAC コンプライアンス取組みのための枠組み）」[100]という文書において、各組織において、制裁コンプライス・プログラム（sanctions compliance program; SCP）を策定しておくことを求めており、SCP に組み込むべき要素、そこでの考慮要素について説明している。民事上の制裁金を課すかどうかの判断にあたっては、適切な SCP が存在するか、それが適切に運営されているかが斟酌され、適切な場合には制裁金が課されない又は軽減される、としている[101]。

具体的に SCP に組み込むべき要素としては、(1)経営陣の関与、(2)リスク評価、(3)内部統制、(4)テスト及び監査、(5)研修、の 5 つである。各要素で組み込むべき事項は以下の通りである。

(1) 経営陣の関与：

(i) 経営陣が SCP を確認・承認していること。

(ii) SCP を実際に運用する部署に対し、経営陣が、必要な権限を付与しており、当該部署から経営陣に対し、直接報告できる体制を整備していること。

(iii) SCP を実際に運用する部署が人材、専門知識、情報技術等について十分なリソースを得られるように、経営陣において取り計らい続けていること。

(iv) 経営陣が、組織全体において「コンプライスの文化」を醸成すること。

(v) 経営陣において、明白な法令違反の重大性について理解し、将来的に明白な違反が起きないように必要な措置をとること。

(2) リスク評価

(i) 組織において、潜在的なリスクに応じた必要十分な頻度及び方法において OFAC リスク評価を実施すること（なお、OFAC の経済制裁執行ガイドライン[102]に、リスク評価に使用することのできる OFAC リスクマトリクスが添付されている。）。

(ii) 組織において、特定したリスクについて特定、分析、対応する方法論を開発していること。

---

[99] 同ガイダンス 13 頁。

[100] https://www.american-club.com/files/files/cir_33_19_p2.pdf。なお、同ガイダンスにあるリンク先は、制裁プログラムの情報に関する OFAC のサイトであり、同文書そのものへのリンクではないため、注意されたい。

[101] 前掲枠組み 1 頁。

[102] 31 C.F.R. Part 501 別紙 A。なお、C.F.R.は、連邦規則集（Code of Federal Regulations）のことであり、各種行政手続を定める。そのうち、タイトル 31（31 編）では、「金融：財務省」を扱う。

(3) 内部統制

(i) 組織において、SCP の概要を示すポリシー、手順を書面で準備していること。

(ii) 組織において、OFAC リスク評価の結果に対応する内部統制制度を整備していること。

(iii) 内部監査、外部監査を通じて上記ポリシー及び手順を組織内において実行すること。

(iv) 必要十分な記録管理ポリシー及び手順を整備すること。

(v) 内部統制システムの脆弱性を把握した場合、直ちに実効的な対策をとること。

(vi) SCP のポリシー及び手順について社内に周知徹底すること。

(vii) SCP のポリシー及び手順を日常業務に実装するための人員を配置すること。

(4) テスト及び監査

(i) 経営陣が、テスト及び監査機能に責任を持ち、テスト及び監査の実施は経営陣から独立して行われ、その実施部隊に十分な権限、リソースが付与されていること。

(ii) 当該組織における SCP のレベルと緻密さに応じてテスト及び監査が実施され、テスト及び監査が包括的かつ客観的であるようにすること。

(iii) テスト及び監査の結果がよくなかった場合、直ちに実効的な対策をとること。

(5) 研修

(i) OFAC 研修プログラムにおいて十分な情報及び説明を従業員に対して提供すること。

(ii) 組織が提供する製品及びサービスに適した OFAC 研修プログラムを提供するよう取り組むこと。

(iii) 組織の OFAC リスク評価及びリスク内容に応じて、適切な頻度で OFAC 研修プログラムを実施すること。

(iv) テスト及び監査の結果がよくなかった場合、直ちに従業員に対し必要な研修等を提供すること。

(v) 関連する従業員すべてが簡単にアクセスできる研修資料・リソースを用意すること。

現在存在する制裁の対象国と制裁内容は、OFAC のウェブサイトで確認することが可能である[103]。直近では、2021 年 2 月 26 日、3 月 2 日、3 月 3 日、3 月 5 日に内容が更新された制裁があり、遵守するには相当の頻度で確認しておく必要がある。

[103] https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information。同ガイドライン注 43 に記載のウェブサイト。

13) 訳注 13

大統領命令 No. 13694「重大な悪意のあるサイバー活動に従事する特定の者の資産の凍結」（Blocking the Property of Certain Persons Engaged in Significant Malicious Cyber-Enabled Activities）は、オバマ大統領が発付したものであり、合衆国の国家安全保障、外交政策、健全な経済、金融の安定に重大な脅威をもたらし、又は当該脅威に相当程度寄与する悪意のあるサイバー活動について責任のある者、又はそれに関与した者（個人又は団体）に対して取引の停止や資金の凍結を命じるという内容のものである[104]。これに基づき、同年、本書注 94 に詳述した 50 U.S.C. § § 1708 が、2015 年国防権限法（National Defense Authorization Act）として制定された。なお、この大統領命令は、選挙の過程に介入し、侵害する目的で情報を改ざん、改変、濫用する個人又は団体に対して制裁を加えるべく、大統領命令 No. 13757「サイバー活動に関する国家緊急事態に対応するための追加方策（Taking Additional Steps to Address the National Emergency With Respect to Cyber-Enabled Activities）」[105]によって、改定されている。

14) 訳注 14

通信傍受法 18 U.S.C. § 2512 (1)は、一定の例外を除き、故意に、主として傍受に有用な設計であることにつき悪意又は善意有過失で、当該設計を有する電子装置、機械装置、その他の装置を、(a) 州際間取引又は外国取引において郵送、送付、運搬した者、(b) 製造、組立て、所持、販売した者、(c) 新聞や電子媒体等に広告を出した者は、本章に従って罰金又は/及び 5 年以下の有期刑が科される、と定める。

15) 訳注 15

Luis v. Zang 事件[106]は、オンライン通信をひそかに傍受するために使用されたソフトウェアの製造者と、そのソフトウェアを妻の通信を傍受するために使用した夫に対する、妻の通信相手による 18 U.S.C. § 2511（傍受禁止）違反及びプライバシー違反に基づく損害賠償請求において、夫に対する請求は認容したものの製造者に対する請求は棄却した第一審について、製造者に対する請求についても認容すべきであるとして破棄差戻しをした事件である。

前提として、通信傍受法（Wiretap Act）では、一定の例外を除き、音声通信（wire communication）、口頭又は電気通信（electronic communication）による通信を故意に傍受し、傍受することを試み、人に傍受させ、傍受を試みさせることを禁じており[107]、傍受された被害者が通信を傍受、開示、故意に使用した者に対して仮処分、衡平法上の処分、損害賠償（合理的な弁護士費用も含む）を求める民事上の請求権を認める[108][109]。

---

[104] https://www federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities
[105] https://www federalregister.gov/documents/2021/01/25/2021-01714/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious
[106] *Luis v. Zang*, 833 F.3d 619, 635 (6th Cir. 2016)
[107] 18 U.S.C. § 2511(1)(a)。
[108] 18 U.S.C. § 2520(a)(b)。
[109] したがって、セキュリティ担当者が購入した盗聴マルウェアを使用した場合には、刑事上の責任のみならず、被害者から損害賠償請求されるおそれもある。

本判決では、①18 U.S.C. § 2511 の「傍受」が送信中の通信内容を取得することを意味する、すなわち保存された通信を事後的に取得することは「傍受」にあたらないという判例法理（同時性の要件）を改めて確認したこと、②傍受に使用されたソフトウェアによって、送信中の通信内容が製造者のサーバを経由して使用者に送信される仕組みとなっていたことをもって、製造者が「傍受」したと認めたこと、③18 U.S.C. § 2520 は、傍受された被害者について通信を傍受、開示、故意に使用した者に対する民事上の損害賠償請求権を認める旨定めており、一見 18 U.S.C. § 2511（傍受禁止）違反の場合に限り適用される（よって傍受装置の製造等を禁じる§ 2512 違反には適用されない）ように読め、単に傍受装置を所持しただけでは「通信を傍受、開示、故意に使用」したとはいえないが、本件のように、傍受装置を宣伝、販売し、自らのサーバを使用して装置のユーザによる傍受に関与している場合には、「通信を傍受、開示、故意に使用」したといえ、被害者による 18 U.S.C. § 2512 違反に基づく損害賠償請求は成立すると判断したこと、が注目に値する。

4.3.5 日本におけるサイバー脅威インテリジェンスを収集し、不法な情報源からデータを購入する際の法的考慮事項についての論点の検討

(1) 日本における論点の法的位置づけ

前掲「オンラインサイバー脅威インテリジェンスを収集し、不法な情報源からデータを購入する際の法的考慮事項」で種々の論点が提起されている。

検討すべき論点としては、「被害者にならないこと」「加害者にならないこと」「オンラインフォーラムでの合法的な情報収集」「盗難データや脆弱性の購入」「コンプライアンスのためのベストプラクティス」がある。

これらの論点のうち、「被害者にならないこと」は、通常のサイバーセキュリティの保護措置の重要性、サイバーセキュリティ実践そしてそれらのための脅威インテリジェンスの重要性を意味しており、ここでは、詳述はしない。

「加害者にならないこと」「オンラインフォーラムでの合法的な情報収集」「盗難データや脆弱性の購入」において論じられている事項は、個々の行為の適法性の問題となる。一方、「コンプライアンスのためのベストプラクティス」については、脅威インテリジェンスの提供の問題／推奨事項の問題については、また、別個の問題としてみていくことができよう。

(2) 適法性の検討

「加害者にならないこと」は、司法省ガイドラインにおいて「本文書で取り上げている活動の一部は、連邦刑法に関係しており、州法に違反したり民事責任を問われたりする可能性がある。これらの活動に従事することを計画している組織は、その活動の合法性を評価するために弁護士と相談すべきである。」（常に従うべき２つのルール）とされている。そこで、具体的には、「オンラインフォーラムでの合法的な情報収集」「盗難データや脆弱性の購入」についての検討がなされている。以下、これらの二つの局面について日本法の観点から、検討する。

また、同ガイドラインにおいてもふれられているように資金洗浄／テロリストの支援を規制する法律等との論点についても検討する必要がある。この論点は、本調査第１章でも検討した事項である。

1) オンラインフォーラムでの合法的な情報収集

ここでの問題は、フォーラムへのアクセスの問題（認証情報の利用、不正アクセスの問題、ポリシーに反するアクセス）、フォーラムでの活動の問題（潜伏、投稿、情報交換）がある。

フォーラムへのアクセスへの問題をみる場合に前提として、不正アクセス禁止法をみていくことにする。不正アクセス禁止法は、「電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図」ろうとする法律である。同法は、「不正アクセス行為」を定義しており（同法２条４項１ないし３号）、他人の識別符号を悪用する行為及びコンピュータプログラムの不備をつく行為をそれぞれ処罰している。また、ここで問題となる「アクセス制御機能」というのは、「当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（略）であることを確認して、当該特定利用の制限の全部又は

一部を解除する」と定義されている（同法２条３項）。

これらの解釈については、①入力先が、「アクセス制御機能を有する特定電子計算機」であること②「電気通信回線を通じて」行う者であること③入力されるものが、「当該アクセス制御機能にかかる他人の識別符号」であること④「入力」した結果として、「特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をしうる状態にさせる」こと、などが要件として求められている。

これらの解釈を前提に、上記の問題について検討する。

ここで、認証情報の利用というのは、アクセスのための資格や招待を必要とする公衆がアクセスしうるといえないインターネット上のエリアにアクセスして情報を取得する行為、もしくは、ディープウェブ／ダークウェブといわれるエリアにアクセスして情報を取得する行為の問題である。具体的には、招待を受ける、料金を支払う、入会「テスト」をクリアする、専門用語を使えることを示す、オンラインセキュリティに関する情報を交換することによりアクセスしうる領域にアクセスして情報を得る行為ということになる。我が国の不正アクセス禁止法においては、「他人の識別符号を入力して当該特定電子計算機を作動させ」るか、「アクセス制御機能による特定利用の制限を免れることができる情報又は指令を入力」することによってアクセスすることを処罰している。アクセスのための資格や招待を必要とするとしても、そのための資格や招待を受けることにより特定のアクセスのための権限を得ることは、「他人の識別符号を入力」することでないのは、もちろんのこと、「アクセス制御機能による特定利用の制限を免れることができる情報又は指令を入力」とはいえない。したがって、日本法上においては、これらの行為は、処罰の対象とはならないと解される。

不正アクセスの問題というのは、脆弱性を悪用したり、盗まれた認証情報を使用したりする場合の問題である（司法省２　（２）イ（イ）参照）。これについては、米国と同様であり、これらの行為は、上記不正アクセス禁止法にいう不正アクセス行為として処罰の対象となる。

また、他人名義といっても架空の名義でみずから取得した識別符号の入力は、構成要件に該当しない。上記のように「他人」の識別符号であることが求められていることから、「他人名義も架空の名義で取得した識別符号の入力についてみると（略）、アクセス管理者との関係においては、当該識別符号を取得したものが利用権者であるから、そのものが当該識別符号を入力しても不正アクセス行為とはならない」とされている。また、入力の「結果として」、アクセスしうる状態になることが求められているので、そもそもアクセスしうる状態である場合には、成立の余地はない。SNS で友人に限って公開とされる情報について、虚偽の事実を申告して、友人になって、それらの特別の情報にアクセスする場合でも同様である。SNS で公開している本人に対して虚偽の事実を申告することは、それらの情報について特定利用の制限を免れる情報を入力したということはできない。

フォーラムでの活動の問題（潜伏、投稿、情報交換）については、どうか。米国においては、提供した情報が犯罪に使用された場合には、犯罪の幇助・教唆（aid and abet）、共謀罪が成立する可能性もあるとされているところである。この理については、我が国においても、全く同様である。従って、このような活動には、従事するべきではないということがいえる。米国においては、特定の条件のもとで、誤解を避けるように試みた上で、活動の可能性は否定されていないが、我が国においては、柔軟な対応が実務的に期待できるとも思われないし、また、犯罪捜査の開始自体のもつインパクトが非常に強いこともあるので、そのような行為

については、現に慎むべきであるということがいえる。

2) 「盗難データや脆弱性の購入」

インテリジェンスの成果は、それ自体としては、脅威を引き起こす可能性のある人物、脅威の態様、その対象、脆弱性の情報などである。それらは、一般には、情報自体として取引が禁止される、いわば、「禁制品」というものではない。しかしながら、それらの情報が、違法な手段によって取得されているときにかかる成果が法的にどのように評価されるのか、というのが問題となる。

この点を考えるのにあたっては、資金洗浄／テロリストの支援を規制する法律等や反社会的勢力の排除ポリシーとの関係についてについて考える必要がある。

3) 資金洗浄／テロリストの支援を規制する法律等

我が国における資金洗浄／テロリストの支援を規制する法律として、犯罪による収益の移転防止に関する法律（平成十九年法律第二十二号）（以下、犯罪収益移転防止法という）、組織的な犯罪の処罰及び犯罪収益の規制等に関する法律（平成十一年法律第百三十六号）（以下、組織的犯罪処罰法という）などがあげられる。また、外国為替及び外国貿易法（外為法）」についても検討する必要がある。

a. 犯罪収益移転防止法

犯罪収益移転防止法は、犯罪による収益が組織的な犯罪を助長するために使用されるとともに、これが移転して事業活動に用いられることにより健全な経済活動に重大な悪影響を与えるものであること、及び犯罪による収益の移転が没収、追徴その他の手続によりこれをはく奪し、又は犯罪による被害の回復に充てることを困難にするものであることから、犯罪による収益の移転を防止することが極めて重要であることに鑑み、特定事業者による顧客等の本人特定事項等の確認、取引記録等の保存、疑わしい取引の届出等の措置を講ずる旨を定めた法律である。犯罪収益移転防止法上の特定事業者については、本人確認義務（犯罪収益移転防止法４条）、取引記録等の作成義務（同法６条）や疑わしい取引の届出義務（同法８条）等を負う。仮想通貨（制定法上は、暗号資産）の交換業者は、同法上の特定事業者であるとされています（同法２条２項３１号）。もっとも、ここで、疑わしい取引というのは、収受した財産が犯罪による収益である疑いがある、又は顧客等が当該取引に関し組織的犯罪処罰法第十条の罪若しくは麻薬特例法第六条の罪に当たる行為を行っている疑いがあると認められる場合をいう（同法８条）。被害者もしくは、そのために活動をするものが、突如として法貨を仮想通貨に交換し、多額の金額を攻撃者に対して支払う行為は、それ自体は、上記要件に該当するとは考えられない。しかしながら、金融庁は、「疑わしい取引の参考事例」として、仮想通貨交換業者については、通常は取引がないにもかかわらず、突如多額の仮想通貨の売買又は他の仮想通貨との交換が行われる口座に係る取引（同第４　取引の携帯に着目した事例（1））、資金洗浄・テロ資金供与対策に非協力的な国・地域又は不正薬物の仕出国・地域に拠点を置く顧客に係る取引（第５　外国との取引に着目した事例）などを具体例としてあげている。従って、それらの事例と認識される可能性があり、関係者は、弁護士等のアドバイスを求める必要があるといえる。

b. 組織的犯罪処罰法等

組織的犯罪処罰法は、組織的に行われた殺人等の行為に対する処罰を強化し、犯罪による収益の隠匿及び収受（略）を目的とする行為を処罰するとともに、犯罪による収益に係る没収及び追徴の特例等について定めている。まず、そこでは、3 条において、同法が対象とする犯罪が、「組織的な殺人等」として明らかにされている。一般的なサイバー犯罪は、この犯罪の定義に含まれていない。しかし、組織としてランサムウェアを利用して身代金を取得している場合には、同条 1 項 14 号の恐喝の罪を行っているものと考える[110]。そのような場合には、同法 10 条は、取得若しくは処分につき事実を仮装し、又は犯罪収益等を隠匿する行為を処罰している。また、同法 11 条は、情を知った犯罪収益等の収受を処罰している。もっとも、ランサムウェアの被害者が、送金等を行ったという場合には、その収受を幇助したということに該当するというのは、困難であろうと考える。

c. 外為法

外国為替、外国貿易その他の対外取引は自由に行われることを基本とするが、種々の要請から、対外取引に対し必要最小限の管理又は調整を行うことか必要とされることになる。これにより、対外取引の正常な発展並びに我が国又は国際社会の平和及び安全の維持を期すことが可能になる。このような目的から制定されているのが、外国為替及び外国貿易法である。

同法によると、我が国の平和及び安全の維持のため特に必要があるときは、閣議において、対応措置を講ずべきことを決定することができる。この対応措置としては、支払いに対する許可の指定（同 16 条）、（21 条）、などがある。また、同 19 条は、支払手段等の輸出入として、　財務大臣は、支払手段（第六条第一項第七号ハに掲げる支払手段が入力されている証票等を含む。）又は証券を輸出し、又は輸入しようとする者に対して、許可を受ける義務を課することができるとしている。外為法は、1997 年の改正時において、同法 6 条 7 号により、仮想通貨による送金の許可の義務をさだめることができるようになっていた（同法 16 条 1 項）。もっとも、現時点においては、特定のサイバーテロリスト集団が指定されているとう事実はないので、当該規定の適用については、考えられないことになる。

d. 反社会的勢力の排除ポリシーとの関係について

反社会勢力とは、暴力、威力と詐欺的手法を駆使して経済的利益を追求する集団又は個人をいう（指針 1 頁　脚注）。具体的には、平成 19 年 6 月 19 日の、犯罪対策閣僚会議の「企業が反社会的勢力による被害を防止するための指針」の申し合わせをもとに、これの遵守によって実際に行われている。

この指針は、1　反社会的勢力による被害を防止するための基本原則、2　基本原則に基づく対応 （(1) 反社会的勢力による被害を防止するための基本的な考え方、(2) 平素からの対応、(3) 有事の対応（不当要求への対応））、3　内部統制システムと反社会的勢力による

[110] なお、恐喝行為の実行行為者が、海外であることがどのように影響するかという論点があるが、被害が我が国で起きている限り、組織犯罪処罰法の 12 条で引用される刑法 4 条の 2 の問題ではなく、国内犯として扱われるものと考える。

被害防止との関係、から成り立っている。組織としては、脅威インテリジェンス情報のための情報購入やランサムウェアへの支払いを考えると、この申し合わせとの関係を検討する必要がでてくる。ここで特に検討されるべきは、(3) 有事の対応（不当要求への対応）の問題であって、上記指針においては「反社会的勢力への資金提供は、反社会的勢力に資金を提供したという弱みにつけこまれた不当要求につながり、被害のさらなる拡大を招くとともに、暴力団の犯罪行為等を助長し、暴力団の存続や勢力拡大を下支えするものであるため、絶対に行わない」とされているところである。しかしながら、上記脅威インテリジェンス情報のための情報購入やランサムウェアへの支払いについては、それ相応の合理性もあり、この衝突について、どのように考えるべきかという論点が生じる。

この論点については、我が国では、正面から議論されていない。報告者としては、本報告を契機として、議論が正面からなされることが望ましいものと考える。

(3) 違法な手法によって取得した情報をもとに脅威インテリジェンスサービスを提供／利用することの法的問題と推奨事項

1) 脅威インテリジェンスサービスの利用について

脅威インテリジェンスサービスを利用するにあたって、提供されるインテリジェンスを構築するためのデータが違法な手法によって取得される可能性がある場合について、どのように考えるのか、という問題がある。

この点については、我が国においても、また、諸外国においても明確な回答は得られていないということができよう。まず、インテリジェンスとそれを生成するために利用されるデータとは別個であるという前提がある、もっとも、そのような違法な手法によってデータを取得することを促進するかのような価格その他でのサービスの購入は、インテリジェンス利用者自身のコンプライアンス体制の問題も生じるものと考えられる。

このように考えると、脅威インテリジェンスサービスの利用については、そのインテリジェンスのソースたるデータの取得方法についても留意を払いながら、その取得及び利用に関する種々の情報を総合的に判断して、利用者の組織のコンプライアンス体制のもとで、その利用の是非等を判断すべきということになる。また、その際に、疑念が生じる場合においては、法律専門家の意見書等を取得することが推奨されることになろう。

2) 脅威インテリジェンスサービスの提供について

我が国において、脅威インテリジェンスサービスを提供する者についても、同様の観点からコンプライアンスを考えなければならないのは、いうまでもない。

自ら違法な行為に基づいて脅威インテリジェンスのためのソースとなるデータを取得することは現に慎まなければならない、ということが前提となる。インテリジェンスサービスの提供者といっても、例えば、海外の会社などからインテリジェンスの成果の提供を受け、その成果を自らのものとして販売する場合には、自ら、社会的責任を果たす、公正で透明性のあるサービスを果たすという理念から、違法行為がないことを確認し、それを積極的に確からしくする必要があることになる。サプライチェーンのコンプライアンスという観点から考えた場合において、このような義務が求められるものと考えられる。このような観点から

は、そもそも、そのようなリスクをも踏まえたコンプライアンス体制を構築し、そのポリシーを徹底するとともに、契約、周知徹底、書面確認、現地監査の各手法等をリスクに応じて採用し、コンプライアンスの観点から、対応しなければならないこととなる。

4.4 情報セキュリティサービス提供者と法執行機関・監督官庁などとの協力

4.4.1 意義

法執行機関・官公庁が果たすべき役割を民間のサイバーセキュリティ会社・脅威インテリジェンス会社が協力することがよく行われているということがいわれる[111]。これは、サイバー犯罪の調査に関していえば、法執行機関は、人的スタッフにも予算にも限りがあるからである。また、特に攻撃者側の手法や状況等についての知識は、サイバー犯罪の状況を明らかにして、将来の攻撃を抑止する効果もあるとされる。また、サイバーセキュリティ会社・脅威インテリジェンス会社にとっても、その専門的な知識を社会の秩序の維持に役立たせることができれば、それは、その企業の社会的な責任を果たすという見地からも望ましいものということができる。

このような問題意識から、本章においては、世界で実際に行われているサイバーセキュリティ会社・脅威インテリジェンス会社のサイバー犯罪対応等に対する協力を明らかにしようと努めるものである。

具体的な協力の態様としては、民間において自らがサイバーセキュリティ会社等に依頼して、その依頼の結果を法執行機関等に提供する場合と、法執行機関が自らの業務を行うのに際して、サイバーセキュリティ会社等に協力を求める場合とがある。これらの場合について、世界における具体的な状況を明らかにするものである。なお、当該調査については、現時点において、我が国でも一般的なものとして認識されていると考えられるデジタルフォレンジックス・機器の調査・通信傍受への協力の例は除くものとする。「犯罪捜査のプレゼンスに民間企業の知見を取り入れる必要」に限って調査するということになる。また、児童ポルノ等の発見、通報等を民間によっていわばアウトソースするという点についても、本調査の対象とはしない。

4.4.2 法執行機関・監督官庁などとの協力

具体的なサイバー犯罪対応のための法執行機関と民間企業の協力という観点から、脅威アナリストは、捜査官のために刑事事件を立証するためのサポートと十分に開発されたリードを消化しやすくするためには、まず範囲と被害を明確にすること、攻撃者との結びつきと問題となる法域を明らかにすること、業務と連絡の一元化をすること、人的なネットワーキングの重要性を認識すること、法執行機関の人員も事件に関するフィードバックや最新情報を提供することで、情報のループを閉じること、が推奨されている。これは、民間の脅威アナリストとの法執行機関との連携が、実際に頻繁に行われていること、そして、きわめ

[111] Levi Gundert, ”5 steps for a successful public-private cyber crime fighting partnership”（https://gcn.com/articles/2019/02/28/cyber-crime-fighting-partnership.aspx）

て重要であることを物語っている[112]。

また、国連においても、その関心から、「誰が、サイバー犯罪の捜査を指揮するのか？」という報告がなされている[113]。そこでは、もっぱら、サイバー犯罪に対する証拠の収集という観点から、種々の捜査主体があげられている。刑事司法機関、国家安全保障機関、民間企業、官民連携とタスクフォースに分けてそれぞれ検討されている。民間企業に関していえば、特に重要インフラを運営している企業においては、それ自体が、サイバー犯罪の探知、防止、緩和、捜査に関して重要な役割をはたす。重要インフラは、民間企業によって保有、運営されているために、サイバー犯罪者の標的となりうるので、サイバー犯罪／犯罪者をプロアクティブに特定し、サイバー犯罪を防止し、緩和し、対応することができるようにセキュリティ措置を展開することが良いとされている。また、官民パートナーシップについても注目がなされており、米国における NCFTA、日本における JC3、欧州における 2 Centre が紹介されている。

特に、脅威インテリジェンスを法執行機関が利用することについては、サイバー捜査における官民協力のための新しいモデルが、執行活動を可能にするための民間部門の重要性がよりよく理解されている特定の法域で出現しており、成功しているものがいくつかあるとして[114]、全米サイバーフォレンジック・トレーニング・アライアンス（NCFTA、以下、NCFTA という）、ユーロポールの EC3 諮問グループ、金融セクタ ISAC（FS-ISAC）、マイクロソフトのデジタル犯罪対策本部などが紹介されている。これらについては、以下において、具体的に検討する。

4.4.3 世界における協力状況と法

(1) 米国

1) NCFTA（国家サイバーフォレッジックス・トレーニング・アライアンス）

NCFTA は、2002 年に民間、政府、学会からなるサイバー犯罪を特定、緩和、根絶するために相互協力を可能にする中立的で、信頼しうる環境を構築する目的のために、創立された。2015 年から 2019 年までの間に、2517 件を法執行機関に連絡し、1096 人が逮捕されていると報告されている。NCFTA は、ブランド・消費者保護（BCP）、サイバー金融（CyFin）、マルウェア及びサイバー脅威（MCT）の三つのプログラムを有している。ブランド・消費者保護（BCP）は、偽造品対策・偽医薬品・小売業の保護の分野に注力している。サイバー金融（CyFin）は、金融業に対するサイバー脅威対応に注力している。マルウェア及びサイバー脅威（MCT）は、ダークウェブの傾向に対応するものである。マルウェアのサンプルを分析し、攻撃のインディケータの情報共有の起点となっている。

---

112 上記 Gundert 論文。

113 UNODC ”Who conducts cybercrime investigations?”（https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/who-conducts-cybercrime-investigations html）

114 Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime（https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime）

2) 金融セクタ ISAC（FS-ISAC）[115]

FS-ISAC は、インテリジェンス・プラットフォーム、回復力のあるリソース、信頼できるピアツーピアの専門家ネットワークを活用して、金融機関、ひいてはその顧客にサイバー脅威の予測、緩和、対応のサービスを提供する金融サービスに特化した唯一のグローバルなサイバーインテリジェンス共有コミュニティである。もともとは、1998 年の米国大統領指令に対応して発足したもので、米国の重要インフラを保護するために、官民が物理的・サイバーセキュリティの脅威と脆弱性に関する情報を共有することを義務づけている。その後、2013 年以降、よりグローバルなアプローチをとるようになっている。

その活動は、インテリジェンス、レジリエンス、トラストの三つの分野に分かれている。インテリジェンスの分野においては、種々の分析やピアツーピアの情報共有がなされている。レジリエンスの分野においては、演習、ベストプラクティス、教育・トレーニングプログラム、危機対応などがある。トラストの分野においては、イベント・コミュニティ活動・セミナーなどがある。

3) ボットネットテイクダウン等における協力（マイクロソフト）

マイクロソフトのデジタル犯罪対策部門（(Digital Crimes Unit、DCU）は、お客様を保護し、マイクロソフトの信頼を促進するために、技術の革新的な応用、フォレンジック、市民活動の革新的な応用をなし弁護士、調査員、データ科学者からなる国際的なチームであり、サイバー犯罪との戦いをリードしている[116]。マルウェアによってなされるサイバー犯罪や国家支援活動を特定し、調査し、撲滅する活動を行っている。2010 年から、22 のマルウェア活動を撲滅している。具体的な事件としては、Gamure（Andromeda）（2018）、Citadel（2013）、Game over Zeus（2012）、Rustock（2011）などがある。

また、国家支援活動に対する対抗策としては、Strontium（2016）に対する活動がある。これは、マイクロソフト社が、裁判所命令を取得し、マイクロソフト類似のドメインへの通信をシンクホールに誘導することが可能になった。また、Strontium によって新しく登録されるドメインに対抗するためにスペシャルマスターを指名してもらい，それらの攻撃を防止した。

国際 BEC（電子メール詐欺）に対して、戦略執行チーム（GSET）が、対抗している。また、技術サポート詐欺に対してデータ分析・機械学習をも活用して対抗している。

(2) 欧州

1) 欧州サイバー犯罪センター（European Cybercrime Center）

欧州警察機構（Europol）は EU におけるサイバー犯罪への法執行の対応を強化し、欧州市民、企業、政府をオンライン犯罪から守ることを目的として 2013 年に欧州サイバー犯罪センター（EC3）を設立した。EC3 は、数十件の注目を集める作戦や数百件の現場での作戦支

[115] https://www fsisac.com/
[116] https://3er1viui9wo30pkxh1v2nh4w-wpengine netdna-ssl.com/wp-content/uploads/prod/sites/358/2018/12/DCUOverview.pdf

援活動に携わり、何百人もの逮捕者を出し、何十万ものファイルを分析してきている。

(3) イギリス

1) シンクホール手法等における協力

英国において、法執行機関等と民間企業が、協力して積極的な調査手法を活用して、サイバーセキュリティ活動を行うことは、実際によく行われている。その場合に、そのような活動と法執行機関等との関係は、具体的な活動との関係で定まる。一般的な情報提供に関しては、法執行機関・会社・大学などは、情報についての要求者として、リサーチャーとは、情報提供契約を締結して、その情報の取得についての合法性を担保させようとする。具体的な手法として、シンクホールを用いて調査をなすという手法については、英国においては、セキュリティ会社の通常の調査手法であって一般的である。攻撃者、ターゲットのセクタ、被害者になっている者の情報を得ることができることから非常に豊富なインテリジェンスが得られる手法であると考えられている。トラフィック情報については、大変な機密情報を含んでいるということではないし、より、マルウェアが、何を求めたのか、次のコマンドは何か、という情報になる。トラフィックは、100 パーセント被害にあった企業の情報ということになる。セキュリティ会社は、実際に、シンクホールを運用しているし、それは、会社からも法執行機関からも感謝されている。このような運用に際して、法執行機関との協力もなされている。一方、英国において、それ以外の手法、一般の民間のセキュリティ会社が、ボットネットの中立化に自ら協力するなどの手法をとることは、特にないとのことであった。

2) 捜査権限法における捜査技術の拡充と技術者によるコントロール

英国における通信に関するデータの合法的アクセスの法的な規制に関する主な制定法は、シギント（通信、電磁波、信号等に対する傍受等を利用した諜報）活動について定める 2016 年調査権限法 （Investigatory Powers Act 2016）(IPA2016 という） である。同法は、合法的（特定）通信傍受、通信データの取得許可、（特定）機器干渉（Equipment Interference）、一括令状（1 章：一括傍受令状、2 章：一括取得令状、3 章：一括機器干渉令状）、一括・パーソナル・データセット令状などの調査権限を定めている。これらの権限について、適切に行われるように技術助言委員会（Technical Advisory Board）（245 条）、技術助言パネル（246 条）が設けられている。

(4) ドイツ[117]

ドイツにおいては、ISP とボットネットの切断、研究者のボットネットの報告義務において、民間と法執行機関との協力が議論されている。

[117] 基本的に以下の記述は、Liis Vihul, Christian Czosseck, Dr. Katharina Ziolkowski, Lauri Aasmann, Ivo A. Ivanov, Dr. Sebastian Brüggemann, M.A., “Legal Implications of Countering Botnets”, Joint report from the NATO Cooperative Cyber Defence Centre of Excellence and the European Network and Information Security Agency (ENISA)（https://ccdcoe.org/library/publications/legal-implications-of-countering-botnets/）におうところがほとんどである。

1) ボットネットのテイクダウン

ボットネットが検知された場合、警察（連邦レベルのケースになりやすいとはいえ、主な管轄は州警察（the regional Länder Police）にある）は、公衆の安全への危険がある場合、又は生命若しくは身体的な完全性への脅威がある場合には、C&C サーバをテイクダウンするために、適切な法執行命令（捜索令状(Nordrhein-Westfalen (NRW)州警察法（以下「州警察法」という）41 条、42 条[118]))やサーバの没収命令（州警察法 43 条、44 条）に基づいて行動できる。さらに、C&C サーバのテイクダウンは、問題となっているそのボットネットによる攻撃が公衆の安全の危殆化又は公序の侵害を構成するものである場合には、州警察法 1 条の一般条項により正当化されうる。このような場合、当該警察は、C&C サーバをホストしているボットマスター、ISP、同様に感染しているそれぞれのコンピュータの個別の所有者に対して、問題ある行動を止めるように要請することができる。ただし、後者はあまり意味がなく、それゆえほとんど行われていない。

管理しているネットワーク内に C&C サーバがある場合、ISP は、同サーバを切断し、ドイツ民法 314 条に基づいて契約を終了させることさえできる。実際には、C&C サーバをテイクダウンする ISP の権利は、規約に書くことが出来るし、今日では既に、インターネットサービスの多くはそうなっている。

2) 研究者のボットネットの報告義務

なお、研究者の行為規範に関して、ボットネットを見つけた際にそれを報告する義務があるかどうかが問題となる。ドイツ刑法 138 条は犯罪の報告義務違反罪を規定している。もっとも、これは、ボットネットについての知識を有しているだけの者には適用されない。しかし、ドイツ刑法 138 条にあげられている犯罪がボットネットの利用によって行われていることを知っている場合には、報告義務違反罪に該当しうる[119]。

---

[118] https://recht nrw.de/lmi/owa/br_text_anzeigen?v_id=31200711211000360 31 https://www.gesetze-im-internet.de/bgsg_1994/BJNR297900994.html (2021 年 3 月 5 日最終確認)

[119] ドイツ法上、ボットネットの構築や運用それ自体が犯罪に当たるかどうかが立法論的に議論されていることに注意されたい(BT-Drs. 19/1716)。ボットネットをいわば法的に攻撃するアプローチだといえよう。そこでは、現状、ボットネットの構築から運用のそれぞれのプロセスにおいて、一つずつ行為を検討してみると、既存のサイバー犯罪対策規定(ドイツ刑法 202 条 a,b,c、303 条 a,b)のみを利用するのでは処罰の欠缺があるとし、新たにドイツ刑法 202 条 e が提案されていた。もっとも、ボットネットを包括的に処罰し得る本罪は、軽微な事案をも同時に補足してしまうとして批判が強く(詳しくは西貝吉晃「ドイツにおける新たな無権限アクセス罪の立法論」情報法制研究 6 号 36 頁以下参照)、未だ立法にも至っていない点に注意が必要である。

「サプライチェーン・セキュリティ対策に関する調査」
報告書

2021 年 3 月

株式会社三菱総合研究所
デジタル・イノベーション本部
TEL 03-6858-3578