資料１－４

政策課題１

サイバーセキュリティ確保のための新たな開発・監視・対処体制の構築

令和3年1月

内閣サイバーセキュリティセンター（NISC）
基本戦略第１グループ

検討論点と有識者からいただいたご意見

注：以下では各xSIRTと呼ばれるものに関する分析を行っているが、企業・組織内にそれぞれ体制として設ける必要性を示すものではなく、体制の検討にあたっては、全社的なリスクマネジメントが必要であることは論を待たない。

①xSIRT（例えば、CSIRT、PSIRT、DSIRT/SSIRT）ごとに特徴的な機能や体制等はあるか。また、それらの構築や普及にあたっての課題は何か。

②DX に伴いデジタル・サービスが増加する際に重要となる開発・監視・対処のプラクティスとは何か。その実現にあたっての人的資源・体制につき考慮すべきことは何か。

＜有識者からの主なご意見＞

○「CSIRT」への認識・役割は、例えば日常の体制／危機対応の体制という違いなど、企業によって異なる。具体的にどのような機能を指すのか、表現に注意する必要性がある。

○xSIRTのそれぞれがサイロ化されすぎると、企業側は付加的に体制をつくり人員を確保しなければならないと考え、導入をためらってしまう。全体の普及のためには、シンプルなワーディングにして、カバレッジを広げた方がよい。

○xSIRTは、あまり概念を細分化せず、全体のリスクに対応できるような組織体制とすべき。

○SSIRTの機能において、どのようなスキル、どのような人材が必要となるのか明らかにしてはどうか。

○自動車の分野では、国連のWP29にてサイバーセキュリティ対策の国際規格について検討が進んでいる。日本では海外に先行して、自動車のファームウェアのOTA（オンライン更新）におけるサイバーセキュリティの確保について法令化されており、他の業種にもこの流れは波及していくのではないか。

③実践や普及をどのように政策的に後押ししていくか。

＜有識者からの主なご意見＞

○企業にとってはどのように立ち上げるべきか、ベストプラクティスのようなものが共有されると参考になる。

○一部の先進的な取組事例だけではなく、だれでもできるという事例や失敗事例の共有が重要である。

○企業のセキュリティに関する取り組みを評価する基準や指標の導入も、環境整備の上では有効。経産省主管で議論されている「デジタルガバナンスコード」等に、セキュリティの要素を盛り込んで活用するのも一案。

○国際的にもちいられている「サステナビリティ・インデックス」で今年からセキュリティも評価項目に加えられた。このような評価の枠組みやカリキュラムを通じ、経営計画の中にセキュリティ要素が加えられると受け入れやすくなる。

xSIRTごとの特徴的な機能

注：以下は各xSIRTと呼ばれるものの機能的な面を中心に整理を試みたものであり、企業・組織内にそれぞれ体制として設ける必要性を示すものではない。体制の検討にあたっては、経済産業省の手引き[1]が示すように、近年、デジタル技術の活用の進展に伴い、全社的なリスクマネジメントが必要となってきている。

検討論点①

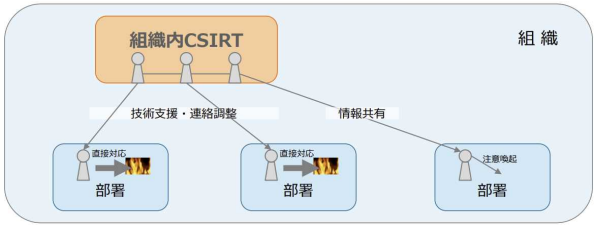
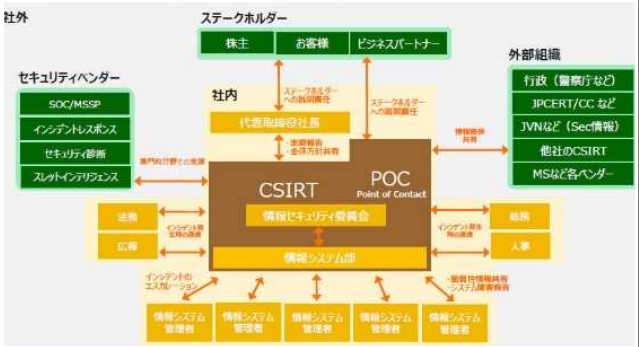
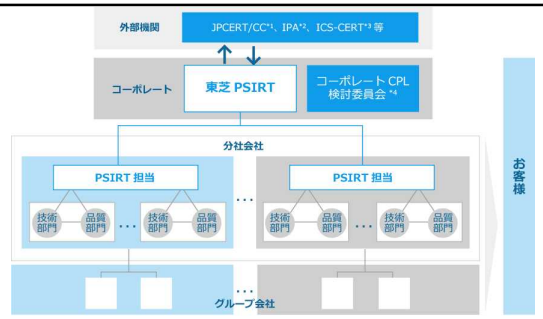
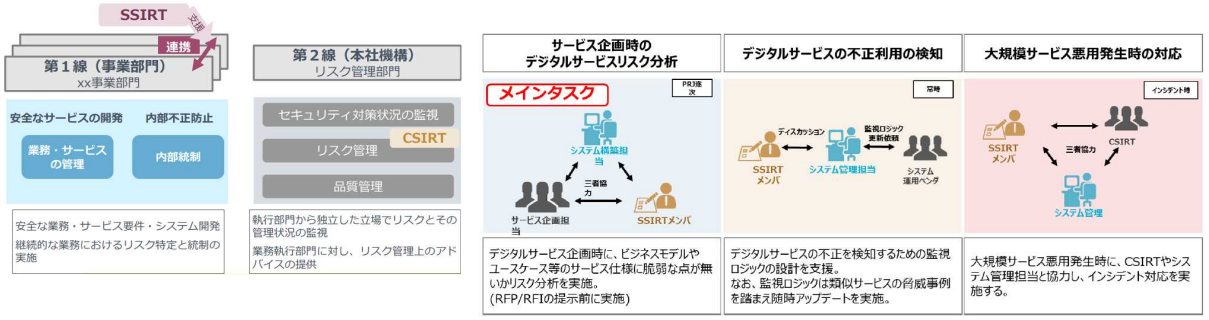
xSIRT	対象	主な活動	設置部署
CSIRT（組織内CSIRT） （Computer Security Incident Response Team）	組織内CSIRTは、組織内の業務運営に用いるコンピュータやネットワークといった情報システムの安定稼働とそこで取り扱われる情報保護を対象として、セキュリティ・インシデントに対処する。 ※全組織的なセキュリティ統括機能が設置される場合はその機能の1つとして上記を担う。	インシデントの検知や受付を経て、その原因分析や影響範囲の調査、問題への対応、復旧を行う。あるいは、そのための技術支援を関係部署に提供する。 経営層や関係部署との連絡調整や情報共有なども行う。 平常時には、パッチ適用などの脆弱性対応、従業員への普及啓発・注意喚起なども担う。	情報システム部門やIT部門と呼ばれる部署に設置されることが多い。 なお、なお、インシデントの検知や深堀分析をSOC（Security Operation Center）と呼ばれる専門組織が担い、CSIRTと連携する場合が多い。自組織CSIRTと外部の専門組織の役割分担は組織によって異なる。
PSIRT （Product Security Incident Response Team）	PSIRTは、顧客に販売されネットワークに接続された製品および顧客の安全確保・情報保護を対象として、セキュリティ・インシデントに対処する。 ここでいう製品にはハードウェア製品とソフトウェア製品がある。	インシデントの検知や受付を経て、CSIRTが設置されている場合はCSIRTと分担・連携しつつ、製品に係る原因分析や影響範囲の調査、問題への対応、復旧を行う。 更に、製品の顧客へのパッチ提供や対策支援等の脆弱性対応なども行う。 活動の際には、製品開発や品質管理を担う部署と協調することが求められる。	事業部門ごとに、製品開発や品質管理を担う部署と連携する部署として設置されることが多い。 その際、製品開発プロセスにおけるセキュリティ・バイ・デザインの管理を兼ねる場合もある。また、複数の事業部門がある場合は、全組織的に統括的なPSIRTが置かれる場合がある。
DSIRT/SSIRT （Digital Service Security Incident Response Team）	Service SIRTは、顧客が利用するデジタル・サービスの継続的提供・品質維持および顧客の資産保護・情報保護を対象として、セキュリティ・インシデントに対処する。	インシデントの検知や受付を経て、デジタル・サービスを提供する事業部門が原因分析や影響範囲の調査、問題への対応、復旧を行うが、Service SIRTは、各事業部門を横断的・俯瞰的に確認し、事業部門に対して実務的な助言・支援を行う。 主に、サービス企画時のサービスリスク分析、サービスの不正を検知する監視ロジックの設計・更新支援、大規模サービスインシデント発生時の対応が挙げられる。 全組織的なCSIRTがある場合は必要に応じ連携する。	デジタル・サービスを提供する事業部門と横並びの独立部署、もしくは、各事業部門のセキュリティ担当を集めたバーチャル組織として設置されることが多い。

※なお、製造業などにおいては自社の工場や生産ラインの安定稼働や作業員の安全確保の為に、サイバー攻撃の監視・対処を行うFSIRT(Factory Security Incident Response Team)と呼ばれる組織が生産管理部門に設置される場合もある。

※ [1]、[3]、その他の資料を参照して事務局にて作成。

xSIRTごとの特徴的な体制

検討論点①

xSIRT	体制例	規模感
CSIRT（組織内CSIRT）	 （出典）組織内CSIRTの役割とその範囲、JPCERT/CC （2015年11月18日） https://www.jpcert.or.jp/csirt_material/files/02_role_of_csirt20151126.pdf  （出典）「CSIRT」の構築・運用のポイントとは？、マイナビニュース（2019年2月14日） https://news.mynavi.jp/article/20190214-770901/	• 大きな組織では、数名から十数名の人員を配置することが多くみられる。一方、ユーザ企業では組織によっては他の業務と兼務となる場合が多くみられる。 ・各部署にセキュリティ対応力が備わっている場合、問題に直接対応する必要がないため、組織内CSIRTの規模は小さくなる。
PSIRT	 *1:Japan Computer Emergency Response Team / Coordination Center *2:Information-technology Promotion Agency Japan *3:Industrial Control Systems Cyber Emergency Response Team *4:CPL:CL（契約に基づく品質保証責任）とPL（製造物責任）を合わせた略称 （出典）東芝 PSIRT、株式会社 東芝（2020年11月30日確認） https://www.toshiba.co.jp/security/psirt	• 事業部門毎にPSIRTが設置され、それぞれに数名の人員を配置することがみられるが、組織によっては他の業務と兼務となる場合もある。 • 全組織的に統括的なPSIRTでは、事業部門とは別途、数名程度配置することがみられる。
DSIRT/SSIRT	 （出典）普及啓発・人材育成専門調査会 第13回会合「資料3 DXサービスに必要なセキュリティ対策（ＮＲＩセキュアテクノロジーズ株式会社 説明資料）」（2020年7月31日）	• 一部の先進的な取組を行う企業で設置がみられる。 • 顧客に提供するデジタル・サービスが複数でも類似する場合には、人員の増加は少ないと考えられる。

※ [1]、[3]、その他の資料を参照して事務局にて作成。

機能構築や普及にあたっての課題

検討論点①

xSIRT	機能構築にあたっての課題	普及にあたっての課題
CSIRT （組織内CSIRT）	（ CSIRTの機能構築に関しては多くの事例や参考情報がある。） ※ 機能構築にあたっては、経済産業省の手引き[1]や日本シーサート協議会のスターターキット[2]、JNSAらのセキュリティ対応組織の教科書[3]などが参考となる。	1） ユーザ企業を中心にIT・セキュリティ人材への不足感がある。また、中小企業など経営リソース（資金、人）に限りのある場合がある。
PSIRT	1） 事業部門とIT・セキュリティの両方の知識を備えた人材は極めて少なく、確保が困難。 2） 部品のサプライヤとの間で、セキュリティ確保のための連携体制の構築が必要。	1） 事業部門とIT・セキュリティの両方の知識を備えた人材は極めて少なく、確保が困難。[再掲]
DSIRT/ SSIRT	1） 広範囲に渡るサービスリスク分析などこれまでよりも高度なリスク管理業務を行う専門的知見・人材の蓄積が少ない。 2） 複数の異なる事業部門や他の組織の提供するサービスとの連携におけるセキュリティ・インシデントに対処する連携体制の構築が必要。 ※ CSIRTや既存部署とのすみ分け・役割分担の整理に留意が必要。	1） 広範囲に渡るサービスリスク分析などこれまでよりも高度なリスク管理業務を行う専門的知見・人材の蓄積が少ない。[再掲] 2） デジタルサービスの普及やサービス間連携の増加の一方で、参照できるDSIRT/SSIRT導入事例はまだ少ない。 3） 事業部門横断的な組織が必要なため、経営層や経営企画部門が問題意識をもって取り組むことが不可欠。

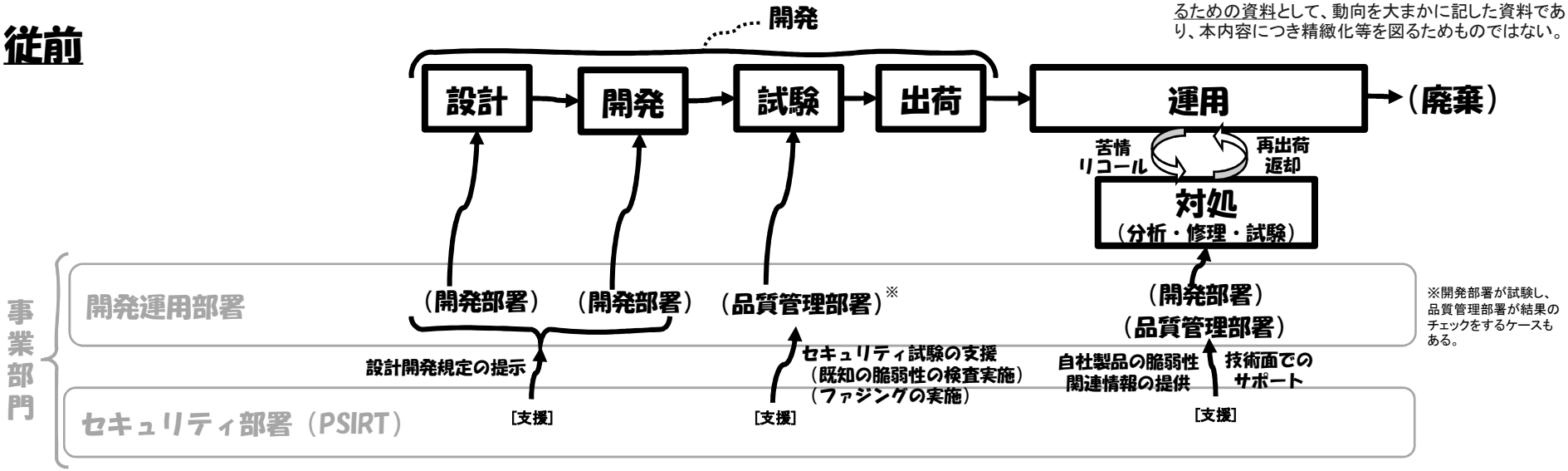
※ [1]サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き、経済産業省（2020年9月30日）
[2] CSIRTスタータキット Ver2.0、日本シーサート協議会（2011年8月1日）
[3] セキュリティ対応組織（SOC/CSIRT）の教科書 ～機能・役割・人材スキル・成熟度～ 第2.1版、日本ネットワークセキュリティ協会（JNSA）、日本セキュリティオペレーション事業者協議会（ISOG-J）（2018年3月30日）

DXやデジタル技術の活用が進展する際に**PSIRTに関連する開発・監視・対処プラクティス**はどう変わるか。その動向を踏まえ、**今後の人的資源・体制につき考慮すべきこと**は何か。

検討論点②

※今後の人的資源・体制につき考慮すべき点を議論するための資料として、動向を大まかに記した資料であり、本内容につき精緻化等を図るためのものではない。

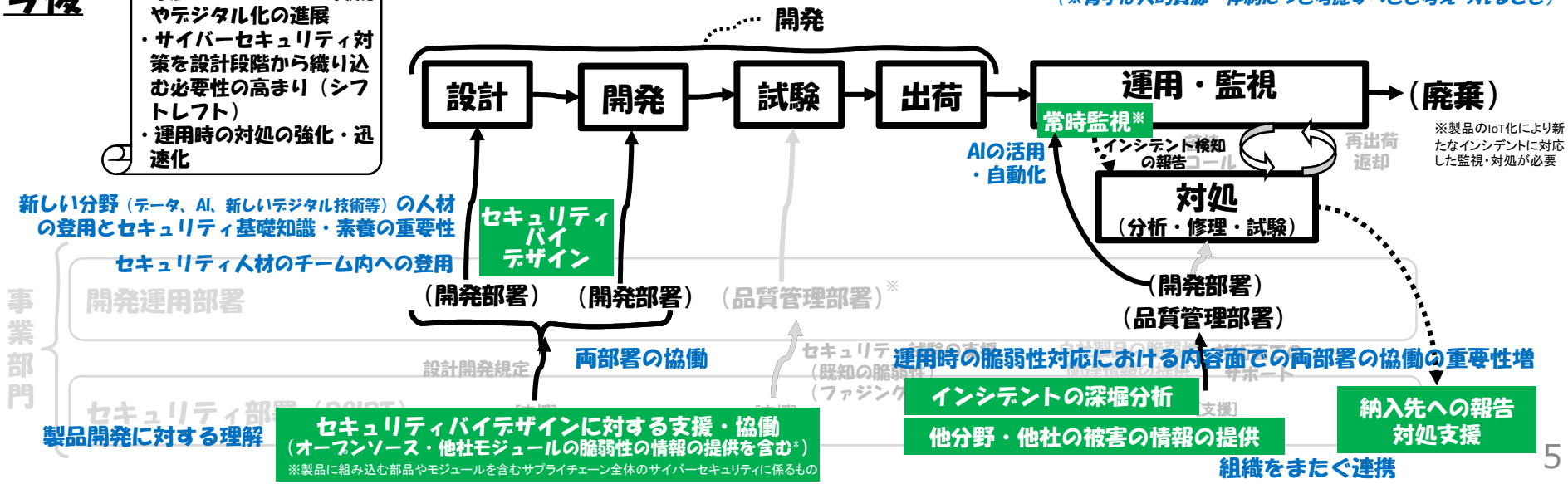
従前



今後

（今後起きうること）
- 製品のネットワーク接続やデジタル化の進展
- サイバーセキュリティ対策を設計段階から織り込む必要性の高まり（シフトレフト）
- 運用時の対処の強化・迅速化

（※緑は重要性が増すと考えられるプラクティス）
（※青字は人的資源・体制につき考慮すべきと考えられること）

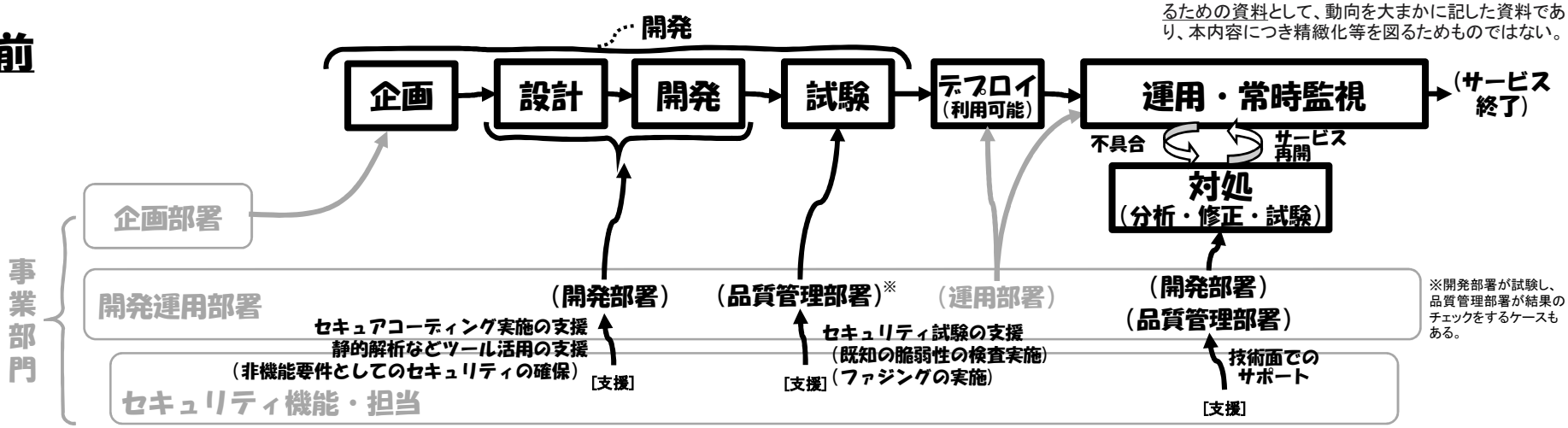


検討論点②

DXやデジタル技術の活用が進展する際に**デジタル・サービスに関連する開発・監視・対処のプラクティス**はどう変わるか。その動向を踏まえ、**今後の人的資源・体制につき考慮すべきこと**は何か。

※今後の人的資源・体制につき考慮すべき点を議論するための資料として、動向を大まかに記した資料であり、本内容につき精緻化等を図るためのものではない。

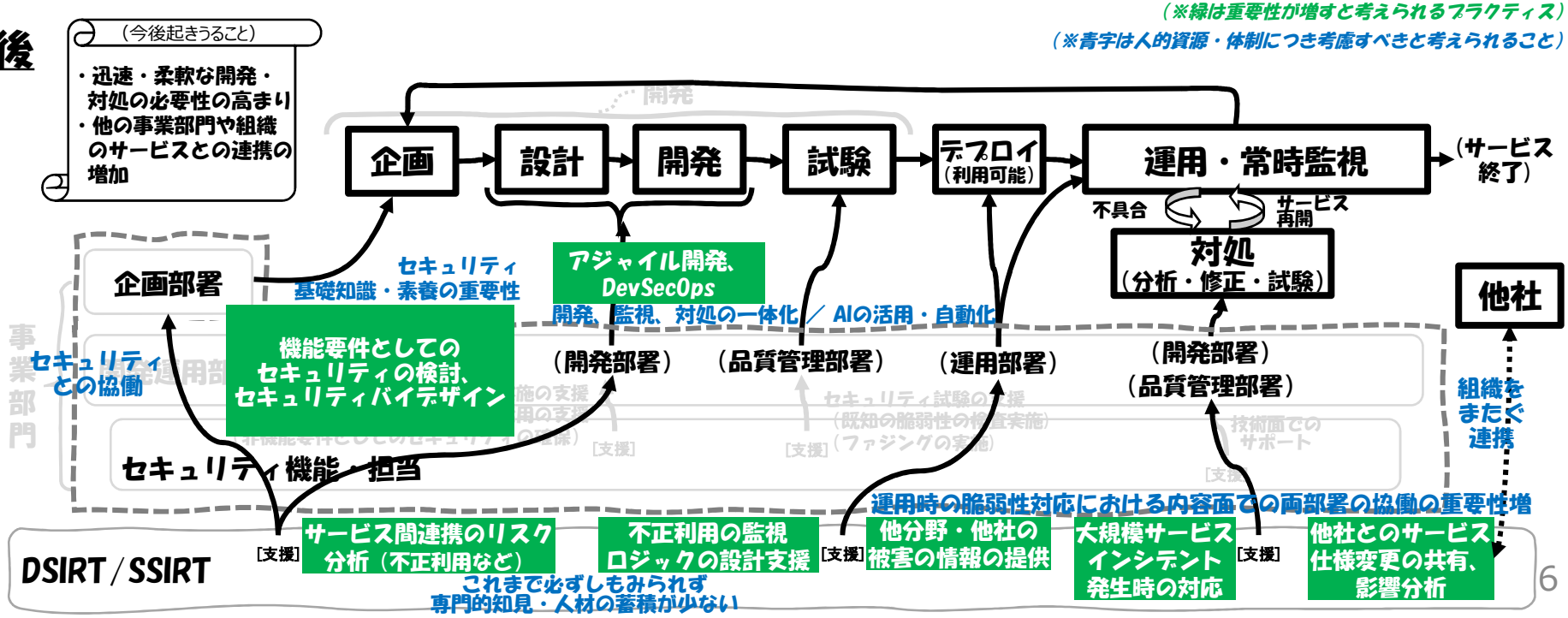
従前



今後

（※緑は重要性が増すと考えられるプラクティス）

（※青字は人的資源・体制につき考慮すべきと考えられること）



（参考）法規制の対象が体制面に及ぶ事例（自動車）

検討論点②

○自動車分野では、自動車の電子制御装置に組み込まれたソフトウェアのアップデートを通じた性能変更や機能追加に当たり、完成車メーカ（OEM）に対し「サイバーセキュリティの確保の業務管理能力」を求める許可制度を導入。
→ 結果として、OEMとサプライヤーの xSIRT（PSIRT）の間で、緊密な連携が求められることとなる。

（別紙1）自動車の特定改造等の許可制度について（概要②）

1. 許可の対象行為

① 保安基準適合性に影響を及ぼすソフトウェアアップデートを電気通信回線の使用によりする行為（Over The Air）
② ①のアップデートを目的として、当該アップデートのためのソフトウェアを整備事業者等に提供する行為

2. 許可の要件

（1）能力： サイバーセキュリティの確保のための業務管理能力※2（上記①の行為）
適切なソフトウェアアップデートの確保のための業務管理能力※3（上記①及び②の行為）
（2）体制： ソフトウェアアップデートに起因した不具合の是正を適確に実施するために必要な体制
（3）保安基準適合性： ソフトウェアアップデートされた自動車の保安基準適合性

原則3年毎の審査
許可1件（型式）毎の審査

※2 車両のサイバーセキュリティに対する脅威及び脆弱性の特定、リスク分析、リスク分析結果を踏まえた対策の実施 等
※3 アップデートが他のシステムに与える影響の評価、アップデート対象車両の特定、ソフトウェア配信経路のセキュリティ確保 等

3. 遵守事項

○ 許可の申請書及びその添付書面に所定の変更事項が生じた場合における国土交通大臣への届出
○ ソフトウェアアップデートの実施状況、当該アップデートに関する情報の記録・保管
○ アップデート車両のサイバーセキュリティに対する脅威及び脆弱性の監視、検出及び対応
○ アップデートの目的、内容及び所要時間、新しい機能の使用方法等に関する情報の使用者への提供 等

4. 公布・施行

○ 公布： 令和2年8月5日（本日）
○ 施行： 道路運送車両法の一部を改正する法律第3条の施行の日（令和2年11月23日※4）
※4 申請の事前受付については、同年8月23日より開始。

5. 適用日

施行日と同じ。ただし、自動運行装置搭載車以外の2.（1）の能力審査は、当面の間適用しない。

（出典）「自動車の特定改造等の許可制度を本年11月より開始します―適切なソフトウェアアップデートを確保するための環境整備について―
【別紙１】自動車の特定改造等の許可制度について（概要）、国土交通省、https://www.mlit.go.jp/report/press/content/001358067.pdf

実践・普及に向けた課題（まとめ：SIRT、DSIRT/SSIRT）

検討論点③

＜課題群と方向性（イメージ）＞

①新たな体制構築・プラクティス実践に関する蓄積が少ない　→　モデルやプラクティスの積極共有[次頁以降参照]

②製品・サービスとセキュリティの両方への理解　→　「プラス・セキュリティ」知識の補充できる環境[政策課題２]

③サイバーセキュリティリスクに対する経営問題としての認識／対策に向けたリーダシップの発揮（意識改革）

xSIRT	機能構築にあたっての課題	普及にあたっての課題	DX時代のプラクティス実践に向けた人的資源・体制に係る考慮点
PSIRT	1）事業部門とIT・セキュリティの両方の知識を備えた人材は極めて少なく、確保が困難。 2）部品のサプライヤとの間で、セキュリティ確保のための連携体制の構築が必要。	1）事業部門とIT・セキュリティの両方の知識を備えた人材は極めて少なく、確保が困難。[再掲]	1）新しい分野（データ、AI、新しいデジタル技術等）の人材の登用とセキュリティ基礎知識・素養の重要性 2）セキュリティ人材の開発運用部署チーム内への登用 3）セキュリティと製品開発の融合、あるいはセキュリティ部署における製品開発に対する理解 4）部署間（特に開発運用部署とセキュリティ部署）の連携・協働 5）納入先等他社との組織をまたいだ連携
DSIRT/ SSIRT	1）広範囲に渡るサービスリスク分析などこれまでよりも高度なリスク管理業務を行う専門的知見・人材の蓄積が少ない。 2）複数の異なる事業部門や他の組織の提供するサービスとの連携におけるセキュリティ・インシデントに対処する連携体制の構築が必要。 ※ CSIRTや既存部署とのすみ分け・役割分担の整理に留意が必要。	1）広範囲に渡るサービスリスク分析などこれまでよりも高度なリスク管理業務を行う専門的知見・人材の蓄積が少ない。[再掲] 2）デジタルサービスの普及やサービス間連携の増加の一方で、参照できるDSIRT/SSIRT導入事例はまだ少ない。 3）事業部門横断的な組織が必要なため、経営層や経営企画部門が問題意識をもって取り組むことが不可欠。	1）セキュリティ基礎知識・素養の重要性 2）開発・監視・対処プロセスの一体化 3）部署間（特に企画部署、開発運用部署におけるセキュリティ機能・担当、DSIRT/SSIRT機能を担う組織）の連携・協働 4）サービス連携を行う他社との組織をまたいだ連携

モデルやプラクティスの発信①

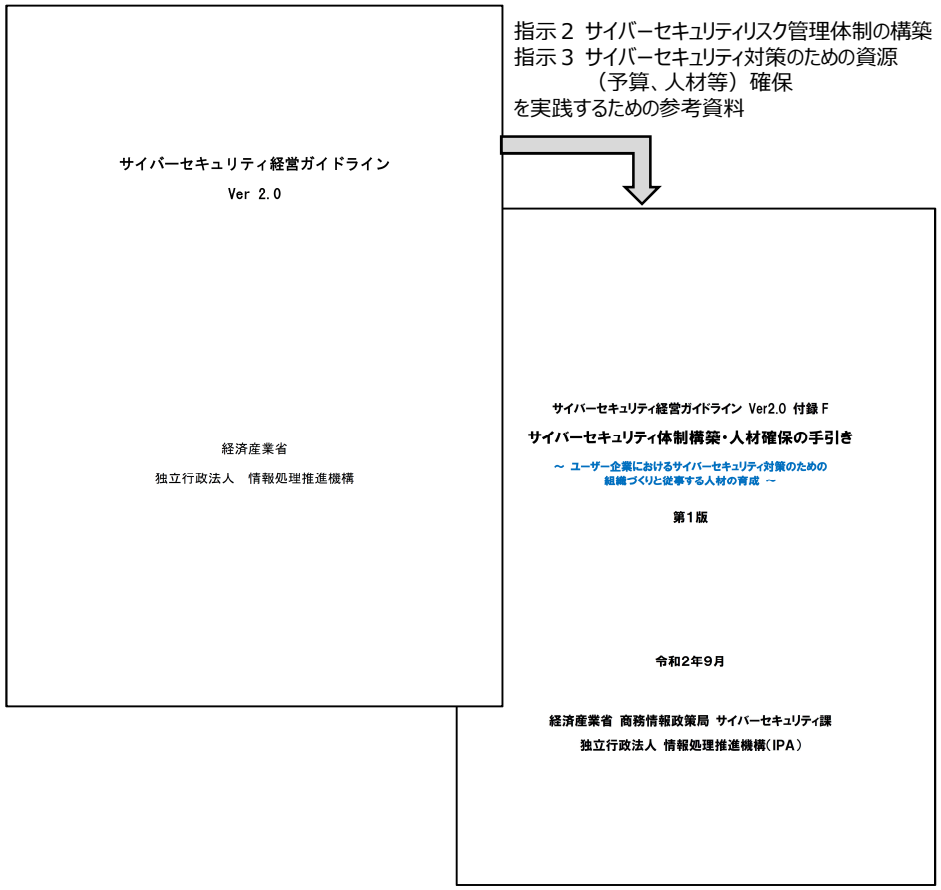
検討論点③

○経済産業省「手引き」（※）では、具体事例等を挙げながら、個別の要素（業種・事業規模・事業のバリエーション・IT子会社の有無・情報システム部門の有無等）を考慮して自社にふさわしい体制を検討することとされている。

（※）サイバーセキュリティ経営ガイドライン Ver2.0 付録 F　サイバーセキュリティ体制構築・人材確保の手引き、経済産業省（2020年9月30日）。
なお、所要の措置の対象となる「DX認定制度」の認定基準の1つとして、「サイバーセキュリティ経営ガイドライン等に基づき対策を行っていること」が確認できることが規定されている。本「手引き」資料は「サイバーセキュリティ経営ガイドライン」の一部を実践するための参考資料と位置付けられている。

→本資料に、検討論点①・②で整理されたモデルやプラクティスを記載することを検討中。

＜「体制構築・人材育成の手引き」の位置づけ＞



＜DX企業認定制度における認定基準：ガバナンスシステム関係＞

● 経営ビジョンやデジタル技術を活用する戦略について、経営者が自ら対外的にメッセージの発信を行っていること。
※経営者名でメッセージが発信されている公開文書等によって確認する。
● 経営者のリーダーシップの下で、デジタル技術に係る動向や自社の IT システムの現状を踏まえた課題の把握を行っていること。
※DX 推進指標等により自己診断を実施していることの説明文書等が提出されることをもって確認する。
● 戦略の実施の前提となるサイバーセキュリティ対策を推進していること。
※サイバーセキュリティ経営ガイドライン等に基づき対策を行い、セキュリティ監査（内部監査を含む）を行っていることの説明文書等が提出されることをもって確認する。
※中小企業においては、SECURITY ACTION 制度に基づき自己宣言（二つ星）を行っていることを確認する方法でも可とする。

（出典）「デジタルガバナンスコード」（2020年11月9日 経済産業省）

モデルやプラクティスの共有②・③

検討論点③

〇加えて、経営層の関与の下で体制構築を進めていくためには、実際に被害を受けた事例の共有を通じて、サイバーセキュリティリスクに対する経営問題としての認識し、対策に向けたリーダシップの発揮してもらうとともに、経験を通じて得られた気づきを共有し対策の底上げや体制構築等に還元してもらうことが重要。

→このため、セミナーを通じた普及啓発活動に取り組むとともに、こうした被害事例に関する「生」の情報は、企業の経営情報や機微情報に触れる可能性があることから、クローズな場で事例の共有・抽出を図り、その内容を集約した「ナレッジ」集を作成していくことを検討中。（調整中）

〇こうしたモデルやプラクティスが反映された「手引き」、「ナレッジ集」といった基礎的マテリアルに加え、DX時代に即したプラクティスを実践するPSIRT、DSIRT/SSIRT構築に関する好事例の収集を行い、当面、関係省庁との連携の下、「NISC普及啓発・人材育成ポータルサイト」等を活用し、共有を図ることを検討中。

＜「NISC普及啓発・人材育成ポータルサイト」への掲載事項（イメージ）＞

	政策課題１	政策課題２	政策課題３
基礎的マテリアル	・「手引き」 ・ナレッジ集【今後作成】	・「プラス・セキュリティ」モデルカリキュラムに関する資料	・スキル等の共通言語化ツール（JTAG、ITSS+等）
先行事例	・DX時代に対応したPSIRTやDSIRT/SSIRT構築事例	・「プラス・セキュリティ」講座	・新たな流動モード事例

◆今後の検討事項：

〇どのような事例を好事例とみなして掲載を行うか。