経済産業省

資料３

サプライチェーン対策評価制度の基本構想(案)について

2024年9月

商務情報政策局サイバーセキュリティ課

サプライチェーン強化に向けたセキュリティ対策評価制度
― 基本構想（案）―

Ⅰ．制度全体について

(1) 制度の目的

(2) 制度の対象事業者（制度利用者）の範囲

Ⅱ．各段階（★３～★５）について

(1) 対象事業者のイメージ

(2) 対策の実施主体と適用範囲（組織、システム）

(3) 対策の基本的な考え方

- 達成水準のイメージと対処する脅威等
- 各段階でベンチマークとする制度・ガイドライン

(4) 評価スキームの考え方 ： （次回以降提示）

(5) 取得のターゲット(目標)費用 ： （次回以降提示）

Ⅰ　制度全体について

(1) 制度の目的

現状認識

- 企業・業種の垣根を超えたシステム・サービスの連携や、サプライチェーンの複雑化により、局所的なサイバー攻撃が社会全体の機能の麻痺、混乱、停止や、深刻な情報漏洩につながるおそれ。サイバー空間の強靭性(サイバーレジリエンス*)確保のためには、中小企業を含めたサプライチェーン全体の対策底上げが急務。
- これまでも経済産業省・IPAでは、業界毎のガイドライン整備の促進や共通事項の抽出等の検討を進めてきたが、政府・重要インフラ分野の取組みを除いて、必ずしも業種共通の枠組みを形成するには至っていない。対策要求のバラツキにより、発注者企業・サプライチェーン企業では複数基準への対応や確認による工数が増大。

制度の目的

- サプライチェーン企業、ひいてはサプライチェーン全体の強靭性(事業継続性に加えてデータ保護を含む)の確保
- 対策要求の共通化を通じたサプライチェーン対策の重複排除、対策状況の可視化による確認の効率化

* サイバーレジリエンス(Cyber resiliency)
サイバー資源を使用する、またはサイバー資源によって実現するシステムに対する不利な状況、ストレス、攻撃、侵害を予測し、それらに耐え、回復し、適応する能力
https://csrc.nist.gov/glossary/term/cyber_resiliency

「サプライチェーン強化に向けたセキュリティ対策評価制度」により目指す効果

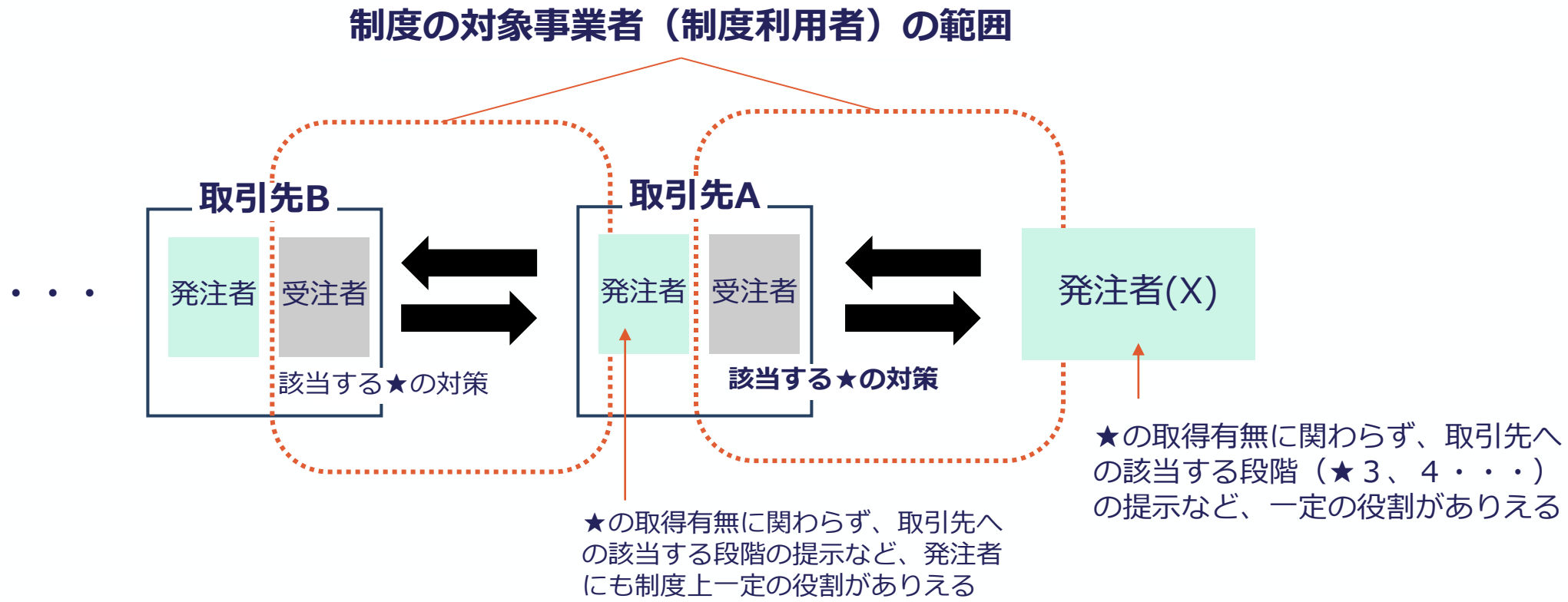
企業にとって
- どのレベルのセキュリティ対策をするべきか選択肢が明確になる
- 対策に要する費用の見える化
- セキュリティサービスの標準化等によるコスト低減

取引先にとって
- サプライチェーン企業に期待する対策水準の決定が容易になる
- サプライチェーン企業における対策状況が簡易に把握できる

社会にとって
- サイバー攻撃への備えのある企業等への適切な評価
- サプライチェーン全体の底上げを通じた経済・社会全体のサイバーレジリエンスの強化

(2) 制度の対象事業者（制度利用者）の範囲

- 本制度で定めるセキュリティ**対策の実施主体として想定するのは、サプライチェーン企業（２社間の契約における受注者側）。**なお、取引によっては発注者にも受注者にもなりえる。
- ただし、サプライチェーン企業が対策を実施するに当たっては、**発注者による協力が必要な事項もある**ため、制度が想定する対象事業者（制度利用者）の範囲は、赤枠囲いとする。



Ⅱ 各段階（★３～★５）について

Ⅱ．各段階（★３～★５）について

- 「サプライチェーン強化に向けたセキュリティ対策評価制度」の内容を具体化していくにあたり、構成要素の (1)(2)(3) について、現状での考え方を整理した。

	三つ星（★３）	四つ星（★４）	五つ星（★５）
	・ ビジネス観点（データ保護、事業継続）及びシステム観点で取引先を評価し、重要度に応じて★3/4/5に区分		
(1) 対象事業者のイメージ	・原則としてサプライチェーンを形成するすべての者	・ビジネス観点：重要度中　または ・システム観点：接続あり	・ビジネス観点：重要度大
(2) 対策の適用範囲（組織、システム）	・組織的対策 ・システム的対策（自社IT基盤）	・組織的対策 ・システム的対策 （自社IT基盤に加えて、発注者内部NWへの接続点）	追加の組織的対策は無し（★４取得が前提） ・システム的対策 （自社IT基盤への高度な対策上乗せ、OT等業務システムへの対策の追加）
	・ NISTサイバーセキュリティフレームワーク2.0の６分類に、サプライチェーン対策である「取引先管理」を加えた７分類で検討		
(3) 対策の基本的な考え方	全てのサプライチェーン企業が最低限実装すべきセキュリティ対策として、基礎的な組織的対策とシステム防御策を中心に構成	上記に該当する企業等が、標準的に目指すべきセキュリティ対策として、ガバナンスからシステム防御・検知、インシデント対応等包括的な対策にて構成	上記に該当する企業等が、高度なサイバー攻撃への対処を念頭に目指すべきセキュリティ対策として、侵入の早期検知と被害の極小化などシステムに対するより高度な対策にて構成
(4) 評価スキームの考え方 (5) 取得のターゲット（目標）費用		※既存のガイドラインや認証制度など活用可能なスキームを検討 （次回以降提示）	

(1) 対象事業者のイメージ

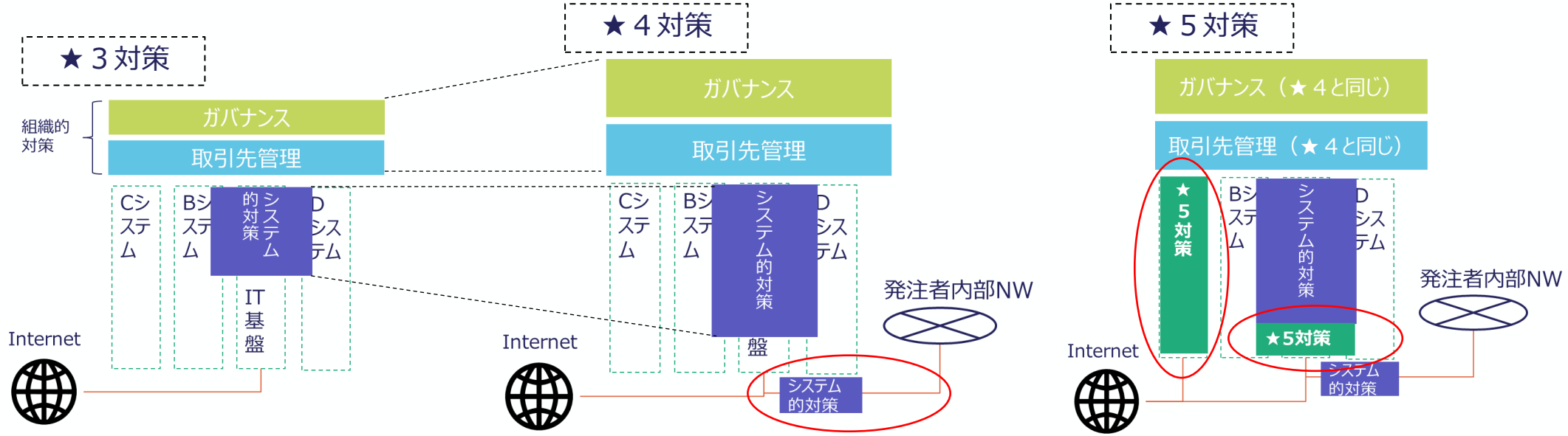
- 発注者は取引先を、どのような考え方で★3/4/5と分けるべきか。
  - 基本的には、ビジネス観点（データ保護、事業継続のいずれか又は双方）で取引先を評価し、重要度に応じて★3/4/5に区分することが考えられる。
  - ただし、取引先環境から発注者内部ネットワークへのアクセスが可能な場合については別途考慮が必要。
  - 対策の脆弱な取引先環境からの不正侵入による被害拡大防止の観点から、発注者内部ネットワークへのアクセス可能な場合については、ビジネス観点での区分によらず、取引先に★4以上の対策要請を推奨。

<table>
<tr><th>判断主体</th><th colspan="2">判断の観点</th><th>★３</th><th>★４</th><th>★５</th></tr>
<tr><td rowspan="3">発注者</td><td rowspan="2">ビジネス観点</td><td>a) データ保護
（取引先がアクセス可能な情報の重要度）</td><td rowspan="2">原則として、全ての取引先（ビジネスサプライチェーン及びサービスサプライチェーン企業）</td><td>中
(右記以外の個人情報、営業秘密等)</td><td>高
(多数または重大損害を及ぼす個人情報(例：口座番号、暗証番号)、営業秘密等)</td></tr>
<tr><td>b) 事業継続
（取引先による供給製品・サービスの重要度（代替可能性を含む））</td><td>中
(発注者による製品・サービス供給停止につながるリスク中)</td><td>高
(発注者による製品・サービス供給停止につながるリスク高)</td></tr>
<tr><td>システム観点</td><td>発注者内部ネットワークへの取引先環境からのアクセス手段(例：ネットワーク共有)の有無</td><td>• 無し</td><td colspan="2">• 有り
※ ビジネス観点で★3相当とされている場合であっても★4以上に変更推奨</td></tr>
</table>

(2) 対策の適用範囲（組織、システム）

- 組織的な対策は二段階（★3/4）とし、事業単位でよりレジリエンスを求められるシステムを対象に★５を適用することを想定。
- ビジネス観点（データ保護、事業継続）「高」のケースは、企業全体でなく特定事業やプロジェクトにおいて発生すると考えられるため。

		★３	★４	★５
対策の適用範囲	組織的対策	• ガバナンス領域 • 取引先管理	• ガバナンス領域 • 取引先管理	ー （企業としては★４取得を前提とする）
	システム的対策	• インターネットに接続している自社IT基盤（IT基盤に接続している社内システムの接続部を含む）	• インターネットに接続している自社IT基盤（IT基盤に接続している社内システムの接続部を含む） • 発注者内部ＮＷの接続点	• 自社IT基盤への高度な対策上乗せ または、 • 自社IT基盤以外のシステム（ビジネス観点の影響が大きいOT等）への対策の追加



(3) 対策の基本的な考え方

- NISTサイバーセキュリティフレームワーク2.0の６分類に、サプライチェーン対策である「取引先管理」を加えた７分類で検討。
- 本仕組みが「サプライチェーン全体のレジリエンス」を目的としていることから、取引先管理をより強調するため独立した分類としたもの。
- ★３は基礎的なシステム防御策を中心に構成。★４は包括的な対策とし、★５はシステムに対するより高度な対策を想定。

分類	★3	★4	★5
対策の基本的な考え方	**全てのサプライチェーン企業が最低限実装すべきセキュリティ対策**として、**基礎的な組織的対策とシステム防御策**を中心に構成	該当する企業等が**標準的に目指すべきセキュリティ対策**として、**ガバナンスからシステム防御・検知、インシデント対応等包括的な対策**にて構成	該当する企業等が**高度なサイバー攻撃への対処を念頭に目指すべきセキュリティ対策**として、早期の侵入検知、被害の極小化など**防護対象システムに対するより高度な対策**にて構成
ガバナンスの整備	• **社内の役割とポリシーを明確化**している。 • 自社の対策状況について正しく認識している。	• **組織的なガバナンス**が適切に構築・運用されている。(★4/5で共通)	
取引先管理	• **外部ICTサービスが把握**されている。	• **サードパーティのリスク評価**が行われ、リスクに応じた対応が講じられている。(★4/5で共通)	
リスクの特定	• IT資産管理台帳、重要な情報資産の一覧作成(取引先から受領したデータ等)を通じて、**資産が把握されている**。	• IT環境を対象に、**資産管理台帳が作成、管理**されている。 • 重要システムにおいて、**定期的な脆弱性検査等**によりリスク認識が更新されている。	• **OTも含めて網羅的に**資産とそのリスクが管理されている。 • 資産とそのリスクの管理が**リアルタイム**に行われている。
システムの防御	• **初期侵入及び内部拡大の防止に係る対策**のうち、効果が大きいものが実装されている。	• ★3で網羅されていないものも含めて**包括的に要求事項が規定**されている。	• **高度なサイバー攻撃への対処を念頭**に、★４より高い強度の対策がなされている。
攻撃等の検知	• **外部ネットワークとの境界部分**にて通信が監視されている。	• 外部ネットワークとの境界に加え、**内部ネットワーク上の適切な場所及び端末等**で通信やその他の挙動が監視されている。	• 組織内の**複数箇所のログ等を相関**させ、異常が検知されている。 • 収集した**脅威インテリジェンス情報が検知活動に活用**されている。
インシデントへの対応	• **インシデント対応計画**が整備されている。	• **対応計画**が定められており、内容が定期的にレビューされている。	• 迅速な対応のため、対応の**一部が自動化**されている。
インシデントからの復旧	-	• **事業継続計画**(BCP)が定められており、内容が定期的にレビューされている。	• 対応の**一部が自動化**されている。 • サイバー攻撃BCPが策定・実施されている。

(3) 対策の基本的な考え方　ー達成水準のイメージと対処する脅威等ー

- ★3/4/5の各段階での対策の実施により達成するセキュリティ対応の水準及び対処しうる脅威等について整理をした。

		★３	★４	★５
達成水準のイメージ （企業がどういう状態にあるか）		• 組織内の**役割と責任が定義**されている。 • より**一般的なサイバー脅威への対処を念頭に、自社IT基盤への初期侵入、侵害拡大等への対策**が講じられている。 • インシデント発生時に、取引先を含む社内外**関係各所への報告・共有に必要な最低限の手順が定義、実施**されている。	• 自社に合わせたセキュリティ対策の**組織的・継続的な実施・改善**(PDCA)がなされている。 • より広範な既知の脅威への対処を念頭に、初期侵入対策(★3)に加え、**社内外への被害拡大を抑制するための対策がなされている。**	• 高度なサイバー攻撃への対処を念頭に、**サイバー空間上のリスクをタイムリーに把握・評価し、対策を適切に反映**している。 • 攻撃者による**侵入を早期に検知**し、**社内外への被害を効率的に極小化するための対策**がなされている。
対処する脅威等	脅威アクターの水準	限定的なリソースで広く認知された脆弱性等を悪用する攻撃を繰り返す攻撃者	広範囲の既知の攻撃手法にアクセスできる攻撃者	未知の脅威を含めて攻撃を設計する高度な攻撃者
	重点的に対策する脅威の範囲	**初期侵入～内部拡大** (偵察、初期アクセス、権限昇格、クレデンシャルアクセス等)	初期侵入～内部拡大に加え、**探索・企業間を含む水平移動(内部ネット内での情報収集)及び目的遂行(データ持ち出し、破壊等)**	★4に加え、**未知の脅威への対処も念頭に一定の緩和策**を講ずる

（参考）海外制度における第三者提供サービスへのセキュリティ対策の例

	CMMC	Cyber Essentials
統治 (Govern)	• 組織のシステム及び構成要素に関連するサプライチェーンリスクを評価、対応、監視する。[レベル3]	-
特定 (Identify)	• 開発ライフサイクル全体にわたり、システムの基本構成およびインベントリを規定し、維持する。[レベル2] • 誤設定/未承認の構成要素の検知を自動化する。[レベル3]	• サードパーティが提供しているクラウドサービスを一覧化する。
防御 (Protect)		• クラウドサービスに対する認証は常に多要素認証を利用する。
検知 (Detect)	• 外部システムへの接続を検証し、利用を管理・制限する。[レベル1] • リモートアクセスセションを監視し、管理する。[レベル2]	-
対応 (Respond)	-	-
復旧 (Recover)	-	-

海外の先行制度では、取引先や第三者サービスの対策は、「統治」「特定」「防御」等に跨って存在する構成

(3) 対策の基本的な考え方　ー各段階でベンチマークとする制度・ガイドラインー

- 基本的な考え方に加えて、関連制度・ガイドラインとの関係性整理を考慮しつつ、各段階で要求する対策項目を具体化していく。
- ★3のベンチマークとして、米CMMC LV1、英Cyber Essentialsを想定。

7/12　産業サイバーセキュリティ研究会WG1
サプライチェーン強化に向けたセキュリティ対策評価制度に関するSWG　提示資料

※各制度の対策レベルの同等性を示すものではない。また、制度によってセキュリティ要件の記載粒度が異なることに注意

		米 CMMC	英 サイバーエッセンシャルズ	豪 エッセンシャルエイト	日本 自工会･部工会ガイドライン
★5（産業界を牽引する企業等の特に重要なサプライヤー）	★5：100項目～ 米 CMMC Lv2,3 豪 EE Lv2,3 自工会 Lv2,3	Lv3 Expert 110項目（SP800-171）＋24項目（SP800-172）	–	Lv3 8分類150項目	Lv3 24類型153項目
★4（産業界を牽引する企業等の重要なサプライヤー）	★4：50項目程度 自工会･部工会LV1 豪 EE Lv1	Lv2 Advanced 110項目（SP800-171）	･サイバーエッセンシャルズ plus ･サイバーエッセンシャルズ（セキュリティ要件は共通）	Lv2 8分類107項目	Lv2 24類型124項目
★3（サプライチェーンを形成するすべての企業）	★3：15項目程度 米CMMC Lv1 英 CE	Lv1 Foundational 15項目（SP800-171より選ばれた対策）	防御、検知に特化した５つの分野の対策 ＋ 前提としてIT資産管理	Lv1 8分類48項目	Lv1 20類型50項目

13

★3のベンチマーク
- 米CMMC LV1
- 英Cyber Essentials

★4のベンチマーク
- 豪Essential Eight LV1
- 自工会・部工会ガイドライン LV1

★5のベンチマーク
- 米CMMC LV2-3
- 豪Essential Eight LV2-3
- 自工会・部工会ガイドライン LV2-3

重要インフラ分野別ガイドライン等も参照

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html