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

資料5

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構築について

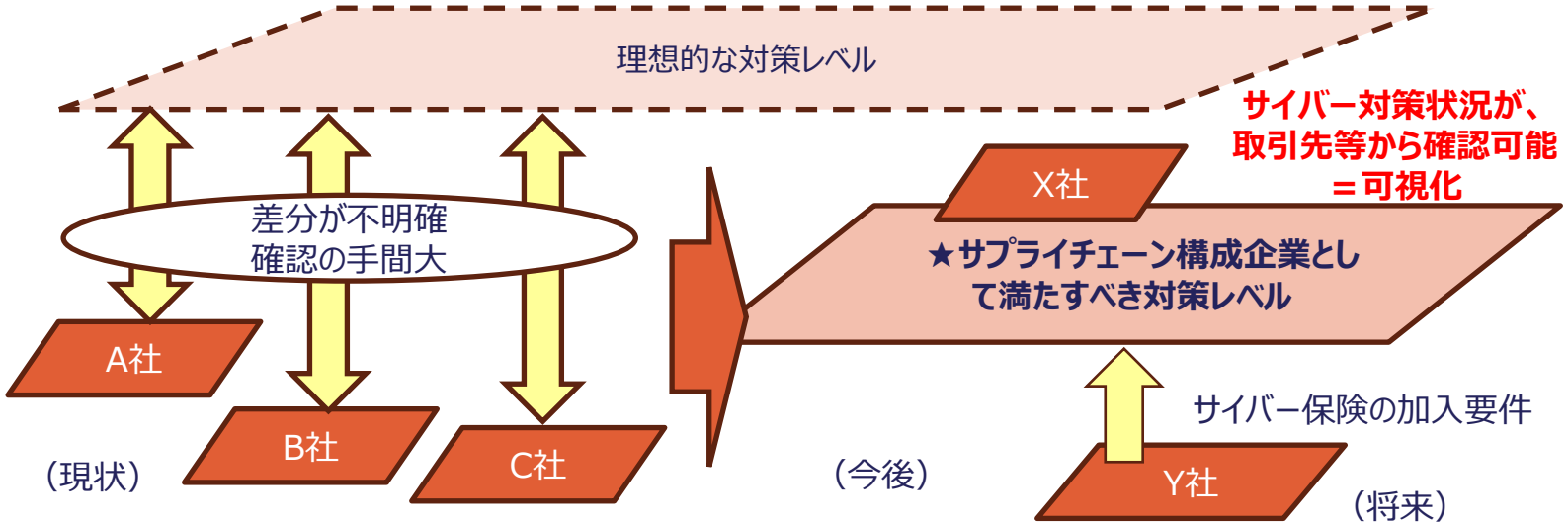
2024年７月１２日
（独）情報処理推進機構
セキュリティセンター

IPA Better Life with IT

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ついて

- 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（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の底上げが急務。**
- 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。一方で諸外国では、企業等のサイバー対策の可視化やレーティング（格付け）の動きが活発化。
- 将来的な国際連携や相互承認も視野に、**サプライチェーン企業のセキュリティ対策の強化が図れるよう、業種横断的に活用できる「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」の検討を進めてはどうか。**

＜サイバー対策レベルの可視化による全体的な底上げ＞



セキュリティ対策評価制度（イメージ）

三つ星（★３）	四つ星（★４）	五つ星（★５）
サプライチェーン形成企業として最低限満たすべき基準	サプライチェーン形成企業として標準的に満たすべき基準	重要インフラ事業の関連サプライヤーが満たすべき基準
（該当するガイドライン） • ○○ガイドライン… （対策の確認方法） • 自己宣言	• △△ガイドライン… • 診断ツール	• ●●ガイドライン… • 第三者確認

①海外・国内の取り組み例
（サプライチェーン企業向け・可視化の取組を中心に）

サイバー対策の可視化・格付け（海外の取組例）

①米国CMMC - Cybersecurity Maturity Model Certification-

- CMMC（サイバーセキュリティ成熟度モデル認証）は、請負業者において連邦契約情報（FCI）及び管理された非格付け情報（CUI※）を適切に保護させるための米国国防省のプログラム。
- 対象事業者は、FCIまたはCUIを処理、保管、送信する国防請負業者およびその下請業者。
- 認証は、レベル１からレベル３までの3段階で構成
- CMMCで求めるセキュリティ要件は、CUIの適切な取り扱いを規定したNIST SP800-171,172に基づき策定

※CUI（Controlled Unclassified Information、管理された非格付け情報）:機密扱い以外の重要情報、例えば、有害物質の取り扱い情報や、予算、買収関連情報、路線の安全情報等が含まれる

	対策数	セキュリティ要件	アセスメント要件	
LEVEL 3	110項目 +24項目	CUIを処理、保存、または送信できる、あるいは実行するすべての資産について、レベル２に加えて、NIST SP 800-172の24のセキュリティ管理策	• 国防総省による評価を通じて、左記要件すべての実装を検証	
LEVEL 2	110項目	CUIを処理、保存、または送信する全ての資産に関して、SP 800-171の110のサイバーセキュリティ管理策	• 自己評価または認定された第三者審査機関によりセキュリティ要件がすべて実施されていることを検証	-CMMC Level2 Certification Assessment -CMMC Level2 Self-Assessment
LEVEL 1	15項目	FCIを処理、保管、または送信する全ての資産に関して、SP 800-171から選ばれた15のサイバーセキュリティ管理策	• 自己評価を通じて確認 • 評価結果をサプライヤー・パフォーマンス・リスク・システム(SPRS)に電子的に入力	

参考URL https://www.federalregister.gov/documents/2023/12/26/2023-27281/cybersecurity-maturity-model-certification-cmmc-program-guidance

サイバー対策の可視化・格付け（海外の取組例）

②英国サイバー・エッセンシャルズ

- 英国Cyber Essentialsは、代表的なサイバー攻撃への普遍的な防御策として、英国のセキュリティ機関であるNCSC（National Cyber Security Center）が提供するフレームワーク。企業の規模によらず、一般的なサイバー攻撃全般から組織を保護するのに役立つとされている。
- 自己診断で取得可能な「Cyber Essentials」と、第三者による脆弱性診断や確認を伴う「Cyber Essentials Plus」の二段階の認証がある（いずれも、講ずるべき対策は同一）
- 英国の公的機関の調達において必須要件として課される場合が多い。また、鉄道など一部民間分野でも取引要件として一般的に活用されつつある。（2023年3月段階で、12万以上の者がCEを取得）

	対策数	セキュリティ要件（共通）	アセスメント要件
CYBER ESSENTIALS PLUS	—	・ファイアーウォール ・セキュアな構成 ・セキュリティアップデート管理 ・ユーザアクセス制御 ・マルウェア対策 の５つのカテゴリで要求事項を提示	• Cyber Essentialsの取得を前提として、実地検査として認定機関による技術検証を受けることが必要 （脆弱性診断、権限管理など具体的なテスト項目と仕様を提示）
CYBER ESSENTIALS		※認証の適用範囲の評価を行う際に、対象資産に関する設問があり、資産管理についても間接的に要求していると解釈できる	• インターネット上でのオンライン審査にて自己診断を行い、認定機関に所属する有資格の審査員が回答内容を評価。 • 合格した場合は認定証が授与され、不合格の場合は今後の助言等が示される。

参考URL　https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf
https://assets.publishing.service.gov.uk/media/652d2b6ad86b1b000d3a4fbe/2023-10-11_Updated_PPN_09_23_Cyber_Essentials_eg.pdf

サイバー対策の可視化・格付け（海外の取組例）

③フランス　サイバースコア法

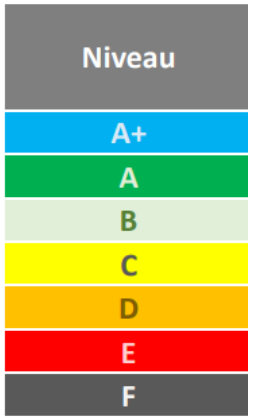
- フランスでは、Webサイトを対象に、サイバーセキュリティに係るスコアリングの実施を法律により義務付け。
- 消費者の個人情報保護の観点から、Webサイトにおけるセキュリティ確保とデータ保護に係る信頼性を消費者に通知することを目的とするもの。
- 対象は、2024年時点でフランス領土からの月間ユニークビジター数が2,500万人以上のサイト。対象サイトの運営者等に対して、サイバーセキュリティ監査の実施及び監査結果から算出されたスコアの提示を義務化。
- スコアの算出は、ANSSIによって指定されたプロバイダーによる監査を通じて行われる。

Cyber Score

スコア算出上考慮される主な基準

「組織とガバナンス」
「データ保護」
「デジタルサービスに対する知識と習熟」
「アウトソーシングのレベル」
「インターネット上での露出度」
「セキュリティインシデント対処体制」
「セキュリティ監査の実施」
等の９つのカテゴリで監査基準を提示

段階分け



スコアはFからA+の7段階で定義される
（現状、それぞれの段階の定義は公表されていない）

参考URL　https://www.cyberscore.fr/
https://www.entreprises.gouv.fr/files/files/secteurs-d-activite/numerique/ressources/consultations/projet-arrete-cyberscore.pdf

サイバー対策の可視化・格付け（海外の取組例）

④オーストラリア　エッセンシャル・エイト

- エッセンシャル・エイトは、オーストラリアのセキュリティ機関ACSC(Australian Cyber Security Center）が策定した基準。
- 4段階の成熟度を定義し、攻撃者の手口や脅威のレベルに応じて、組織が段階的に実施できるよう設計
- 豪州内のすべての組織を対象として想定。なお成熟度２は、パブリックガバナンス・パフォーマンス・アクト（PGPA Act）の対象となる豪州の中央政府及びその他の公的団体等では必須要件とされている。
- 組織がサイバーセキュリティインシデントを軽減するための８つの重要な緩和策を提示。（パッチ適用、パッチ運用システム、多要素認証、特権の制限、アプリケーション管理、Microsoft Officeマクロの制限、ユーザーアプリケーションの堅牢化、定期的なバックアップ）

組織の成熟度	定義	セキュリティ要件 （レベル毎に詳細な対策を提示）
レベル 3	より適応力が高く、公開ツールやテクニックへの依存度がはるかに低い攻撃者への対応を念頭に置く	8分類150項目（＝全項目）
レベル2	レベル1より高度な攻撃者で、ツールの有効性に対してより多くの時間の投下を厭わない者への対応を念頭に置く	8分類107項目
レベル1	広く入手可能で汎用的な技術の活用で満足する攻撃者への対応を念頭に置く	8分類48項目
レベル 0	組織の全体的なサイバーセキュリティ態勢に弱点がある	－　（求められるセキュリティ要件無し）

参考URL　https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

サイバー対策の可視化・格付け（海外の取組例）

- 事業者のセキュリティ対策の状況を一定の尺度で可視化するという観点は共通性あり。
- 制度の目的に応じて、対象事業者やセキュリティ要件の設定、段階分けの考え方を整備。
- 米CMMCと英サイバーエッセンシャルズは、取引活動を通じたセキュリティ対策浸透方策となっている。

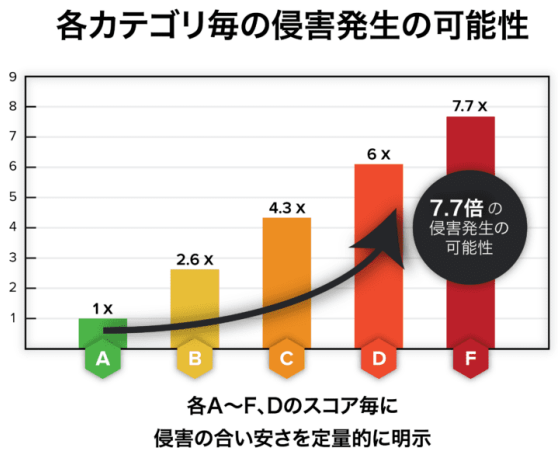
	米　CMMC	英　サイバーエッセンシャルズ	仏　サイバースコア	豪　エッセンシャルエイト
制度の目的	• 防衛調達に関連する請負事業者におけるFCI/CUIの保護の徹底	• 比較的スキルの低い者によって実行される一般的なサイバー攻撃全般から、効率的に組織を保護	• 消費者の個人情報保護を目的に、Webサイトにおけるセキュリティ確保とデータ保護に係る信頼性を消費者に通知	• 様々なサイバー脅威から組織を守る • 攻撃者の手口や脅威のレベルに応じて、組織が段階的に実施できるよう設計
対象として想定する事業者	• 国防請負業者および下請業者	• 特になし （企業の規模によらず適用可能）	• 適用対象となるウェブサイトの運営事業者	• 特になし （豪州内のすべての組織）
セキュリティ要件の概要	• SP800-171/172をベースに段階ごとに設定	• 5つのカテゴリで要求事項を提示	• ９つのカテゴリで監査基準を提示	• ８つのカテゴリで、段階ごとの詳細な要求事項を提示
段階分け	• ３段階	• ２段階	• ７段階（A+～F）	• ４段階
評価・認証の仕組み	• 自己評価または第三者認証（段階ごとに規定）	• 自己評価 • 自己評価＋第三者評価	• 監査を通じてスコア算出	• なし
普及方策（政府調達との関連付けなど）	連邦規則集が最終化されると、FCIまたはCUIを扱う防衛調達の請負事業者は、必要なCMMCレベル取得が必須となる	英国の公的機関の調達において必須要件として課される場合が多い （鉄道など、一部民間分野でも取引要件として一般的に活用）	（法律により義務化）	（豪州の中央政府等はレベル２準拠が必須）

（参考）民間のサイバーリスク可視化ツール（SaaS）

- 機械的な診断に基づいてサイバーリスクを評価・可視化するツールが存在。日本でも、自社診断や取引先・関連会社の対策状況の把握の観点から、関心・導入が広がっている。

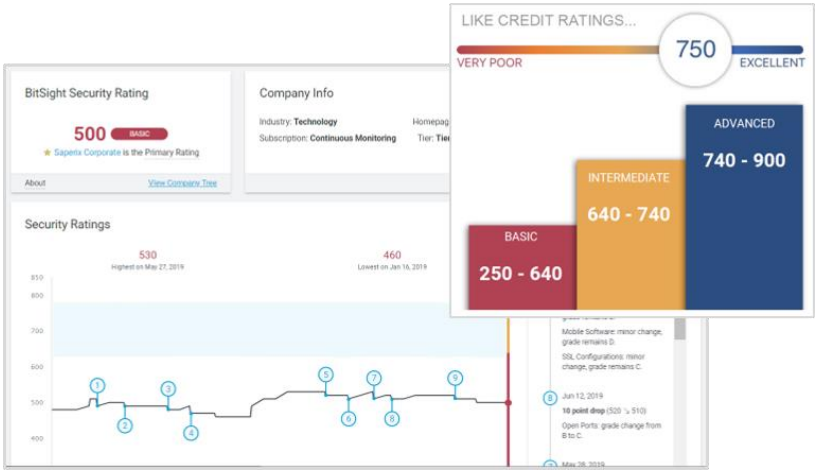
Security Scorecard社（米）

攻撃者の視点で自社/グループ会社/取引先のセキュリティリスクを可視化、将来的にサイバー侵害を受ける可能性との相関性のあるスコアを提示。優先的に対応すべきイシューを提案。



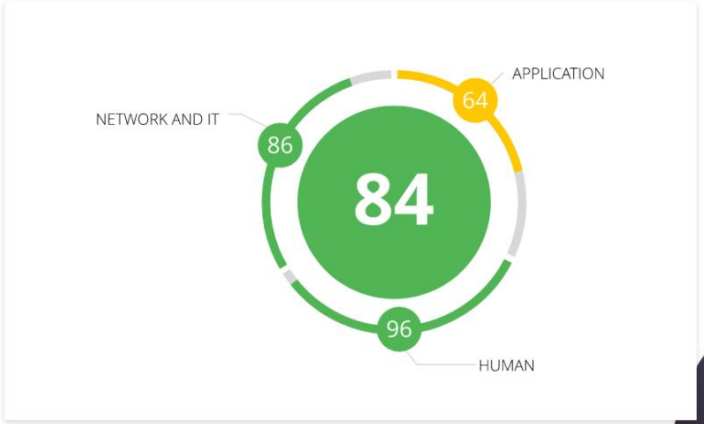
Bitsight社（米）

「どれくらい攻撃されやすい組織なのか」を可視化するツール。同社日本語サイトでは、同ツールを利用して、関連会社や取引先のセキュリティレベルを同じ指標で客観的に数値化する事例が紹介されている。



SOMPOリスクマネジメント社 サプライチェーンリスク評価サービス（Panorays）

SOMPOリスクマネジメント社が提供するSaaS型のセキュリティリスク評価システム。外部から入手可能なデータの分析を通じて、各企業のアタックサーフェスを評価。取引先等サードパーティーのセキュリティリスク可視化にも利用可能。



国内の取組例　ー自工会・部工会　サイバーセキュリティガイドライン2.1版

- 自動車産業全体のサイバーセキュリティ対策のレベルアップや、対策レベルの効率的な点検の推進のため策定された基準。自動車産業に関係するすべての会社（自動車メーカー、サプライチェーンを構成する各社）を対象としている。
- 中小企業を含めた全ての企業が活用できるよう、最低限実装すべき項目（Lv1)から、標準的に目指す項目(Lv2)、最終到達点として目指すべき項目(Lv3)まで、３段階のセキュリティレベルを定義
- 各企業において、本ガイドラインに沿った毎年度の自己評価の実施と、評価結果の提出が推奨されている。

〈自工会/部工会・サイバーセキュリティガイドライン2.1版（概要）〉

レベル	定義	各レベルの達成を目指すべき会社	要求事項/達成条件
Lv3	現時点※で自動車産業が到達点として目指すべき項目　※2022年4月	・会社規模・技術レベルの観点で自動車業界を代表し牽引すべき立場の会社またはそれを目指す会社	24類型153項目（＝全項目）
Lv2	自動車業界として標準的に目指すべき項目	以下のいずれかに該当する会社 ・サプライチェーンにおいて社外の機密情報を取り扱う会社 ・自動車業界として重要な自社情報/情報を有する会社 ・相応の規模/シェアを有し、不慮の供給停止等により業界のサプライチェーンに多大な影響を及ぼし得る会社	24類型124項目
Lv1	自動車業界として最低限実装すべき項目	・自動車業界に関連するすべての会社	20類型50項目

参考URL　https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_V02_01.pdf

国内の取組例　－SECURITY ACTION ～セキュリティ対策自己宣言

- 企業の情報セキュリティへの取組姿勢を自己宣言できる仕組み。
- 想定ユーザーは中小企業。業種を問わず利用可能であり、宣言事業者は35万者を達成　※2024年6月末時点。一つ星・二つ星合計
- 二つ星では25の対策項目を提示。これに沿った自社の状況把握を自己宣言の要件としており、実施の有無や内容を評価するものではない。

	使用要件	
★★二つ星 	「５分でできる！情報セキュリティ自社診断」の実施と、情報セキュリティ基本方針を定め、外部に公開したことを宣言	自社診断項目 **Part1. 基本的対策（＝情報セキュリティ5か条）** **Part2. 従業員としての対策（13項目）** （情報の持ち出し対策、バックアップ取得等） **Part3. 組織としての対策（7項目）** （従業員へのセキュリティ教育等）
★一つ星 	「情報セキュリティ5か条」に取組むことを宣言	**情報セキュリティ5か条** 1.OSやソフトウェアは常に最新の状態にしよう！ 2.ウイルス対策ソフトを導入しよう！ 3.パスワードを強化しよう！ 4.共有設定を見直そう！ 5.脅威や攻撃の手口を知ろう！

参考URL　https://www.ipa.go.jp/security/sme/list.html

②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
構成・内容イメージ

「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」構成・内容イメージ

- サイバー攻撃により、取引上共有している機微情報の漏洩や部品・サービスの供給途絶など、自社のみならずサプライチェーン全体に影響を及ぼす事態が発生しうる。このようなインシデントの予防・抑制を目的に、サプライチェーン構成企業全体のセキュリティ対策レベルの向上と、実施状況の効率的な確認ができる手法として「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」を提案。
- 中小企業を含めた多様なサプライチェーン企業が参照できるよう、三段階のセキュリティレベルを想定。

	三つ星（★３）	四つ星（★４）	五つ星（★５）
段階の考え方（企業がどういう状態にあるか）	**現場レベルや部分的なレベルでのセキュリティ対策が実践されている**	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**	サイバー空間上の**リスクを適宜適切に把握し、合理的な対策を実施、継続的改善がなされている**
対象として想定する事業者	サプライチェーンを形成するすべての企業等	・産業界を代表・牽引する立場の企業等（それを目指す企業等を含む）の**サプライチェーンにおいて重要な機能・役割等を担うサプライヤー企業**	・産業界を代表・牽引する立場の企業等（それを目指す企業等を含む）の**サプライチェーンにおいて特に重要な機能・役割等を担うサプライヤー企業**等
対策セットの考え方（対策の規模感）	上記に該当する企業等が、最低限実装すべきセキュリティ対策の水準（１５項目程度）	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の水準（～５０項目程度）	上記に該当する企業等が、現時点で到達点として目指すべきセキュリティ対策の水準（１００項目～）
	※既存のガイドラインや認証制度などを活用可能なスキームを検討※		
実施状況の評価・確認方法	・自己適合宣言（社内外の登録セキスペ等専門家による確認）	・自己適合宣言　（★３と同様） ・第三者評価 と二段階に分けることも考えられる（★４、★４plus）	・第三者評価

対策の規模感　～国内・海外の取組例との比較～

- 国内・海外の先行制度で求めているセキュリティ要件の規模感に注目し、
  - ★３は、防御、検知など厳選した特定のセキュリティ要件の実装を求めることで、一般的なサイバー攻撃への備えとする
  - ★４は、組織的なガバナンスから、識別・防御・検知といったシステムへの標準的なセキュリティ要件を求めることで、★３で想定しているものより高度なサイバー攻撃への備えとする
  - ★５は、現時点で考えられるベストプラクティスを取り込むことで、最も高度なサイバー攻撃を含めた備えとすることを想定

※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

（参考「自工会/部工会サイバーセキュリティガイドライン2.1版における要求事項（Lv1））

レベル	要求事項数
Lv 3	◆Lv1,2,3の全項目を達成 24分類、153項目
Lv 2	◆Lv1,2の全項目を達成 24分類、124項目
Lv 1	◆Lv1の全項目を達成 20分類、50項目

	ラベル	数	要求事項の例
共通	1方針	2	・自社のセキュリティポリシーの策定・文書化 ・自社のセキュリティポリシーの社内周知
	2機密情報を扱うルール	2	・自社の守秘義務ルールを規定
	3法令順守	2	・情報セキュリティ法令を考慮したルール策定、周知
	4体制（平時）	3	・平時の体制と責任・役割を明確化
	5体制（事故時）	3	・情報セキュリティ事件・事故発生時の対応体制と責任・役割を明確化
	6事故時の手順	2	・情報セキュリティ事件・事故時の対応手順を定めている
	7日常の教育	5	・電子メールのマルウェア感染に関する社内教育
特定	8他社との情報セキュリティ要件	2	・他社との間で機密情報の取扱い方法が明確になっている
	9アクセス権	3	・アクセス権の棚卸を定期的、または必要に応じて実施
	10情報資産の管理(情報)	3	・機密区分に応じた情報管理ルール制定 ・機密区分に応じた情報管理
	11情報資産の管理(機器)	3	・情報機器、OS、ソフトウェア情報の一覧作成
	12リスク対応	3	・CIAを確保できない場合のリスク特定

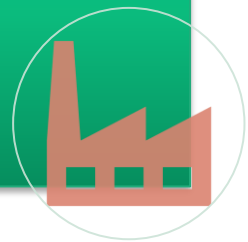
	ラベル	数	要求事項の例
特定	13取引内容・手段の把握	1	・会社ごとに取り交わす情報・手段を一覧化
	14外部への接続状況の把握	3	・利用している外部情報システムを一覧化
	15社内接続ルール	1	・業務利用する情報機器の自社ネットワークへの接続ルールを規定
防御	16物理セキュリティ	2	・サーバー等設置エリアへの入場可能者を制限
	17通信制御	–	（FWによる通信制御、フィルタリング設定の確認、リモートアクセス確認等）
	18認証・認可	4	・ユーザーＩＤの個人ごと割り当て ・ユーザーＩＤと特権ＩＤの権限分離
	19パッチやアップデート適用	1	・パッチやアップデート適用を実施
	20データ保護	–	（データの適切な暗号化）
	21オフィスツール関連	–	（メール誤送信対策、社外送付メール監査等）
検知	22マルウェア対策	2	・パソコン、サーバーへのウィルス対策ソフト導入
	23不正アクセスの検知	–	（通信の常時監視、検知・遮断等）
対応復旧	24バックアップ・復元	3	・適切なタイミングでのバックアップ取得

（計50項目）

「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



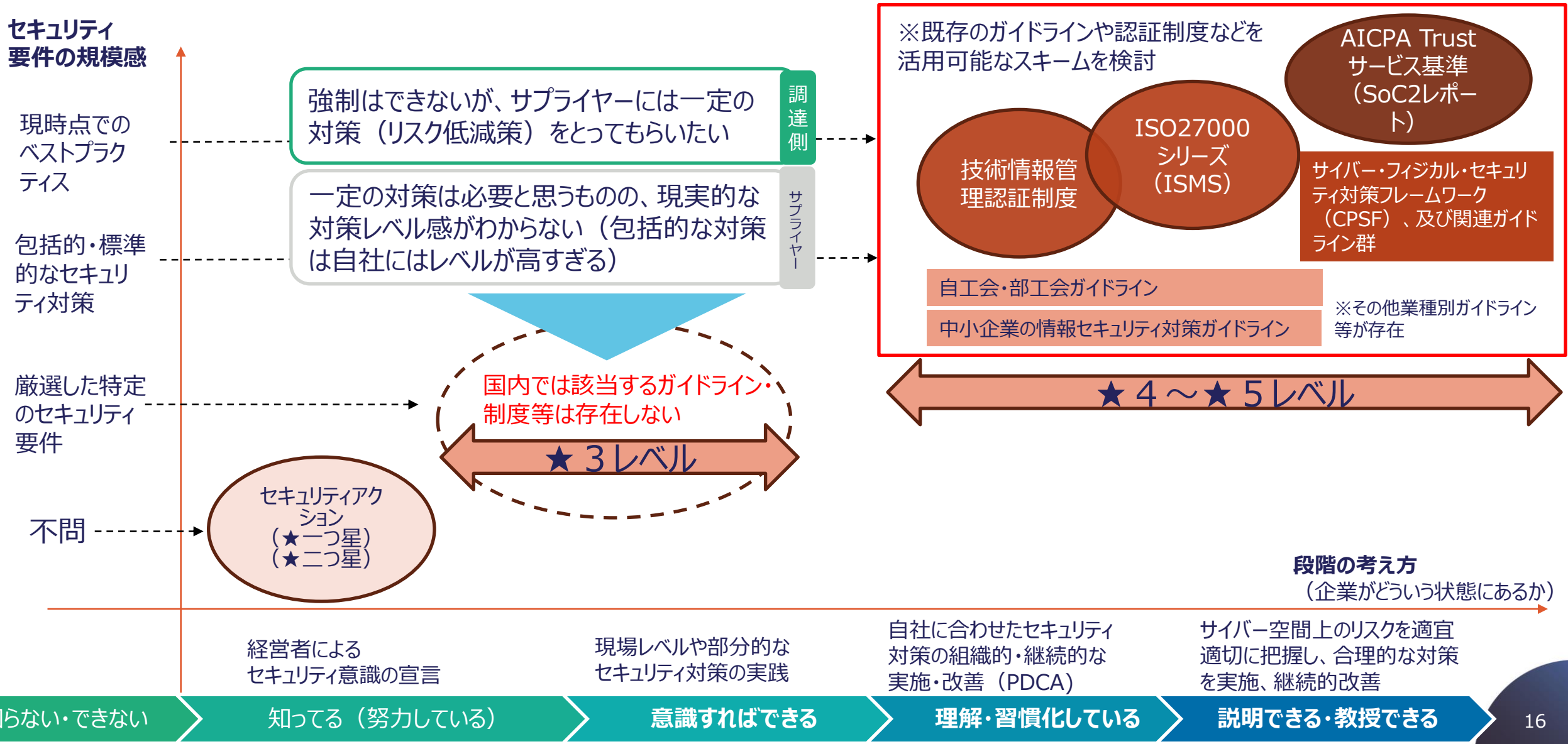
取引先にとって

- 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

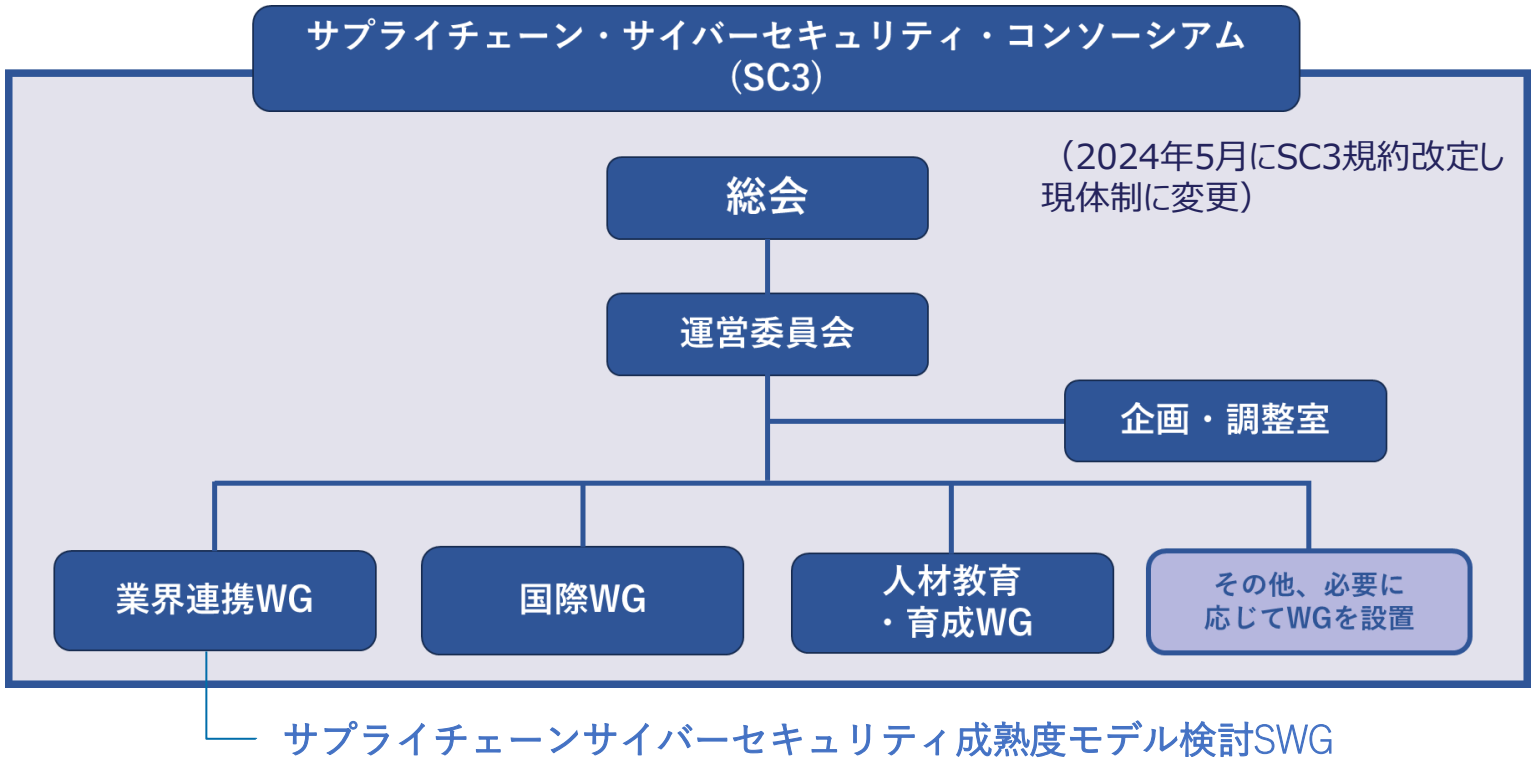
- サイバー攻撃への備えのある企業等への適切な評価
- サプライチェーン全体の底上げを通じた経済・社会全体のサイバーレジリエンスの強化

想定する企業像とセキュリティ要件の規模感



（参考）ＳＣ３（サプライチェーン･サイバーセキュリティ･コンソーシアム）との連携体制

- IPAにおける本件の検討は、サプライチェーン全体でのサイバーセキュリティ対策の検討・推進を目的とする「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3)」と連携して実施している。
- 検討の場として、業界連携ＷＧの下に「サプライチェーンサイバーセキュリティ成熟度モデル検討SWG」を設置



SC３とは…

大企業から中小企業までを含む一連の商流（サプライチェーン）上の弱点を狙って攻撃対象への侵入を図るサイバー攻撃が顕在化・高度化する中、産業界が一体となった取組を進めることが重要。

このような背景のもと、産業界が一体となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進運動を進めていくことを目的に、 2020年11月1日 「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）」が設立された。


IPA