LIBRUS

資料３

サイバーセキュリティ産業 振興にかかる御提言

2024年12月24日

Librus株式会社
代表取締役 鎌田光一郎

はじめに

本日はサイバーセキュリティ市場の「供給者」を対象に、どのような分野/方法で政策資源を投ずるかの議論材料を提供することを目指します。

本日のテーマとゴールに関する認識

サイバーセキュリティ産業政策として、サービス/製品の供給者に対してどのような支援が望ましいか、どのような領域に政策資源を投入するべきかを検討する。

サイバーセキュリティ産業におけるサービス/製品の切り口で、政策として支援が必要となる具体的な領域、方法、関連論点を明確にする。

本日のゴール

本日のテーマに沿った形で経済産業省として、サイバーセキュリティ産業育成の観点での政策インサイトにつながる議論

議論全体像（検討のアプローチ）

・**産業全体の課題分析/洞察**：産業全体としてASIS/TOBE分析を行い、全体的な課題導出を行う。
・**需要サイドに関する洞察**：具体的にどの業種に対して政策リソースを展開するべきか、また当該事業者においてはどのようなリスクが存在し、どのような対策が求められるのかに関する洞察を行う（あくまで供給サイドに関する洞察を行うにあたっての参考として行う）。
・**供給サイドに関する洞察**：現状どのようなサービス/製品が市場で台頭していて、それぞれがどの程度、市場規模、市場成熟性（顧客認知や市場浸透の程度）、市場成長性、技術革新性を有しているか、相対的な検討をする。またその検討結果をふまえて、政策優先度を導出する。
・**供給者支援政策の検討**：「供給サイドに関する洞察」の中で特に効果が期待される政策案に関して、個別に図解し、より具体的な検討/議論を行うことで、政策練度の向上に資する。

会社概要

社名	Librus株式会社
設立年月	2017年11月
本社所在地	〒105-0004　東京都港区新橋6丁目13-12 VORT新橋Ⅱ 4F
主な事業	・サイバーセキュリティ関連サービス ・システム開発サービス（受託/準委任） ・コンサルティングサービス（戦略/IT/マーケティング等）
従業員数	85名（2024年10月1日時点、業務委託社員含む）
認証	ISO 9001、ISO/IEC 27001 情報セキュリティサービス基準適合サービスリスト
HP	http://librus.co.jp/

サイバーセキュリティ産業の課題分析/洞察

産業における主な課題として、国内セキュリティ人材の質量向上と海外展開によるベンダーの販路拡大が挙げられます。

	As Is	To Be
クライアント	・大手企業は対策に意欲は高い一方、中小企業の意欲は低い。 ・大手企業内でも対策レベルに格差がある。金融業（メガバンク）や情報通信業の関心度、練度は高い一方でその他の企業は対策レベルの練度が低いケースが散見される。 ・業種によっては官公庁によるガイドラインやルールブックが存在する。 ・業種を問わず、サプライチェーン攻撃や内部不正、標的型攻撃（国家支援型等）において甚大な被害を出している。 ・大手企業において海外拠点やグループ会社、取引先などのサプライチェーン管理は後手に回っている。	・大企業から中小企業まで幅広くサイバーセキュリティ対策が構築されている。 ・サイバーセキュリティに関する**企業向けサービスがインフラ化**されている（社会的なリテラシーの醸成環境、公益性の高い被害時の相談先組織、技術研鑽や国際的知見の醸成を推進する社会的な仕組み等）。 ・クラッカーにとってサイバー攻撃をすること自体、割りの悪い国づくりの推進。 ・**サプライチェーンマネジメント**の取り組みとして、海外拠点やグループ会社、取引先のセキュリティマネジメントが推進されている。
ベンダー（ソリューション）	・ビジネスモデルが稚拙で部分最適化された機能や商品が販売されている一方、技術と販売が一体化できておらず、「技術は超一流だが、使いにくい（コスト含む）」というプロダクトが多数存在する。 ・ソリューションがカオス化している（ベンダー自身、多くのケースでサイバーセキュリティに関するソリューションマップを正しく理解していない）。 ・ウイルスソフトなど海外発のプロダクトが席巻しており、国内ベンダーのソリューションは後発的かつ未浸透の状態が続いている。	・クライアントにとって、わかりやすくコストパフォーマンスの高いプロダクトが開発され、企業規模に限らず、社会に浸透している。 ・社会浸透を通じて、新たな研究開発に投資ができており、国際的な競争力を有している。 ・今後、人口動態の中心的な存在になるであろう**発展途上国**を中心にITサービス/ITインフラセットで浸透している。
ベンダー（サービス）	・非完全市場化（情報の非対称性、需要に対する提供力が過小）が進んでおり、利益率が非常に高い。 ・外資系企業が参入しにくく、M&Aなどにも取り組むものの、苦戦している。 ・コンサルティングファームと大手Slerが市場を寡占しているが個人や中小企業（ベンチャー企業）も一定の需要獲得をしており、相互に協力的な関係がある。 ・売り手市場化が過度に進み、独善的であったり劣悪なサービス品質のベンダーでも生き残れてしまう環境となっている。 ・サービス提供において規格に準じていないベンダーも一定数存在する（規格を認識していながら、コスト削減や技術力の未熟さゆえに十分な水準のサービスを提供しない等）。	・クライアントに対して、明確にベンダー選定の基準や関連情報が提供されている（**最適なベンダー選定が促進される環境の醸成**）。 ・Sler寡占に伴うセキュリティ対策のブラックボックス化の解消、第三者ベンダーを通じたパンドラの箱現象の解決。 ・官民連携によるサイバーセキュリティ技術研鑽や情報連携、サイバー攻撃対策/対応体制の構築。 ・（国ごとのセキュリティ、インテリジェンス事情、市場性等を正しく理解しながら）**サイバーセキュリティソリューションの海外輸出**が盛んに行われる。

サイバーセキュリティ需要者に関する洞察

LIBRUS

経済産業省として特に重点的に政策資源を展開するべき５つの業種と、業態に付随する主なリスクシナリオ、企業が求められる対応策の洞察を行なっております。

業種カテゴリ	具体例	主なリスクシナリオ（例）	想定する主なサイバー攻撃	リスクシナリオに対する対応策
製造業	自動車、電子機器、食品、衣類、化学製品の製造など	・産業用IoTデバイスが乗っ取られ、生産ラインが停止する ・設計データが盗まれ、知的財産が流出する	・産業用IoT機器へのパスワードリスト攻撃 ・APT（高度標的型攻撃）による知的財産の窃取 ・フィッシングメールでのエンジニア情報の収集	・産業用IoTデバイスのセキュリティパッチを定期的に適用し、セキュリティ監視のためにSIEMソリューションを導入する ・知的財産を保護するためのデータ暗号化とアクセス監視を導入する
電気ガス熱供給水道業	電力供給、ガス供給、上下水道管理、熱供給など	・エネルギー管理システムに対する攻撃で供給が妨害される ・スマートグリッドがハッキングされ、大規模な停電が発生する	・スマートグリッドへのSCADAシステム攻撃 ・エネルギー施設の無線通信を盗聴して情報収集 ・内部者が行う不正操作で供給システムを妨害	・エネルギーインフラへの侵入防止システムを導入し、24時間監視を行う ・スマートグリッドへのアクセス権を厳格に管理し、異常検知を強化する
情報通信業	ソフトウェア開発、通信サービス、インターネット関連事業	・通信ネットワークにDDoS攻撃が仕掛けられ、サービスが中断する ・顧客データベースが不正アクセスにより流出する	・DNSハイジャックで通信サービスを中断 ・DDoS攻撃で大規模なネットワーク障害を発生 ・クラウドサービスの設定ミスを利用したデータ流出	・DDoS攻撃対策として、クラウドベースの防御ソリューションを導入する ・データベースへのアクセス制御を強化し、侵入試行を監視する クラウドサービスのデータ保護に暗号化と多要素認証を実装する
運輸業、郵便業（貿易業/商社）	鉄道、航空、海運、物流、郵便宅配サービスなど	・物流管理システムに対する攻撃で配送遅延が発生する ・車両管理システムがハッキングされ、運行が妨害される	・物流システムへのSQLインジェクション攻撃 ・不正アクセスで配送データを改竄 ・ランサムウェアで車両管理システムをロック	・物流管理システムに多要素認証を導入し、アクセス制御を強化する。 ・物流管理システムのセキュリティを定期的にテストし、脆弱性を修正する ・車両管理システムのセキュリティを見直し、不正アクセスを防ぐ
卸売業、小売業	卸売業、スーパーマーケット、百貨店、ネット通販など	・オンラインストアの顧客情報が漏洩し、信用が失われる ・決済システムが攻撃を受け、売上に影響が出る	・Webアプリケーション攻撃で顧客情報を盗む ・クレジットカード情報のスキミング攻撃 ・Eメールフィッシングで管理者権限を取得	・ECサイトのセキュリティを強化し、Webアプリケーションファイアウォールを導入する ・顧客データ流出に備えて、データ漏洩保険を検討する

サイバーセキュリティ供給者（サービス）に関する洞察

LIBRUS

日本におけるサイバーセキュリティ能力は特にレジリエンス領域に課題があり、その解決を目指すことが最優先事項となります。

サービス名	サービス概要	利用シーンの具体例	市場規模	市場成熟度	市場成長性	技術革新性	政策優先度	具体的な政策案（既存政策含む）
セキュリティ診断（脆弱性診断、侵入テスト等）	システムやネットワークの脆弱性を洗い出し、侵入シミュレーションを実施することで、潜在的なリスクを特定し、組織のセキュリティ対策改善に寄与。	新サービスリリース前のセキュリティチェック、定期的なセキュリティチェック、外部委託開発システムの受け入れ検査、M&Aにおけるセキュリティデューデリジェンスなど	特高	特高	高	高	**特高**	・特定事業者への定期診断義務化 **・ベンダー認証制度の強化（もしくは免許制度導入）** ・上場企業会社等の取り組み表彰制度設立
脅威インテリジェンス	サイバー脅威情報を収集・分析し、予防策や対応策の提案を行うサービス。	ランサムウェアや標的型攻撃の発生リスクを未然阻止	高	高	高	特高	高	・国際的な脅威インテリジェンス共有ネットワークの構築 **・専門人材育成補助金制度（インテリジェンス分析人材）**
セキュリティ運用センター（SOC）サービス	24時間体制での監視、脅威検出、インシデント対応を実施する運用サービス。	金融機関や大企業による常時監視体制を導入	特高	特高	高	特高	**特高**	・SOC先進技術の研究促進 ・SOC運用基準標準化（ガイドライン作成/普及）
マルウェア除去	感染したシステムからマルウェアを特定・除去し、再感染防止策を提供。	業務用PCがランサムウェア感染	高	高	高	特高	高	・感染時対応手順標準化（ガイドライン作成/普及） ・マルウェアに関する研究支援
デジタルフォレンジック	サイバー犯罪の証拠を収集・解析し、法的手続きに対応するための調査を実施。	情報漏洩の原因特定や内部不正の証拠収集	高	高	高	特高	**特高**	・捜査機関とのデジタル証拠共有プラットフォーム構築 **・サイバー攻撃被害に関する民間企業特化の相談窓口強化** **・専門人材育成補助金制度（フォレンジック専門家）**
CSIRT支援	インシデント対応チームの構築・運用を支援し、迅速かつ的確な対応体制を整備。	サイバーレジリエンス能力の向上を企図したCSIRT設立や既存のチーム強化	高	高	特高	高	**特高**	・CSIRT運用方針標準化（ガイドライン作成/普及） **・CSIRTサービスに関する認証制度** **※IPA「情報セキュリティサービス基準適合サービスリスト」による**
脆弱性管理	脆弱性の発見、優先順位付け、対応策の実施を一元管理するサービス。	定期的に公開される脆弱性情報に対する網羅的対応	高	中	高	高	高	・公的脆弱性情報データベースの強化 ・企業間での脆弱性情報共有プラットフォーム構築

サイバーセキュリティ供給者（製品）に関する洞察

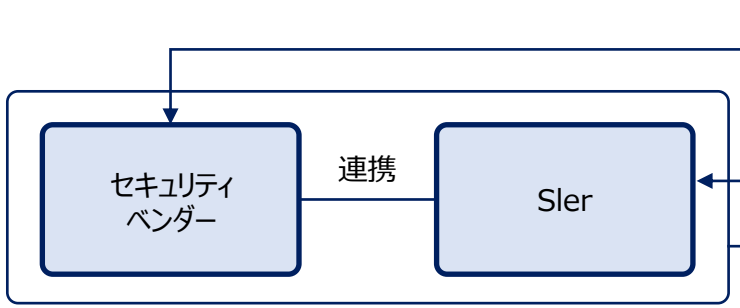
セキュリティ製品において世界的展開を前提とした開発を行うことができなければ、結果的に日本国内においても性能/機能で海外製品に淘汰されることが想定されます。ただし、こうした製品の開発は莫大な投資と卓越した技術力、体制が必要となります。こうした世界的にも厳しい競争環境において、政府としては資金提供に限らない全方位的な支援が必要となります。

サービス名	サービス概要	利用シーンの具体例	市場規模	市場成熟度	市場成長性	技術革新性	政策優先度	具体的な政策案（既存政策含む）
脅威インテリジェンスプラットフォーム	脅威情報を収集・分析してサイバーリスクを軽減するプラットフォーム	攻撃の兆候を把握して早期対策を実施	高	中	高	高	高	・国内外の脅威情報共有ネットワークの構築支援 ・R&Dにおける国際的な協力体制の構築 ・研究開発費に関する補助金
サプライチェーンリスク管理ソリューション	サプライチェーン全体のリスクを評価・管理するソリューション	サプライチェーンの依存関係とリスク評価	中	中	高	高	高	・サプライチェーン全体のリスク評価基準 ・研究開発費に関する補助金
WAF	Webアプリケーションの攻撃を防ぐためのファイアウォール	Webアプリケーションを通じた攻撃防御	高	高	高	高	高	・研究開発費に関する補助金 ・政府関連機関での試験的な導入 ・R&Dにおける国際的な協力体制の構築
脆弱性管理ソリューション	システムやアプリケーションの脆弱性を管理するツール	脆弱性修正スケジュールの管理	高	高	中	高	高	・研究開発費に関する補助金 ・R&Dにおける国際的な協力体制の構築
データ暗号化ソリューション	データを暗号化して保護するツール	通信やストレージデータの暗号化	中	中	高	高	高	・研究開発費に関する補助金 ・防衛、医療等の公共部門、政府関連機関での試験的な導入、海外輸出支援

政策提言①：サイバー攻撃被害に関する民間企業特化の相談窓口とベンダーマッチングPF

民間企業が安心して相談できる政府窓口（マッチングPF）を用意することで、ベンダーの販路拡大を実現しつつ、企業の被害最小化を企図します。

これまでのサイバー攻撃対応のあり方

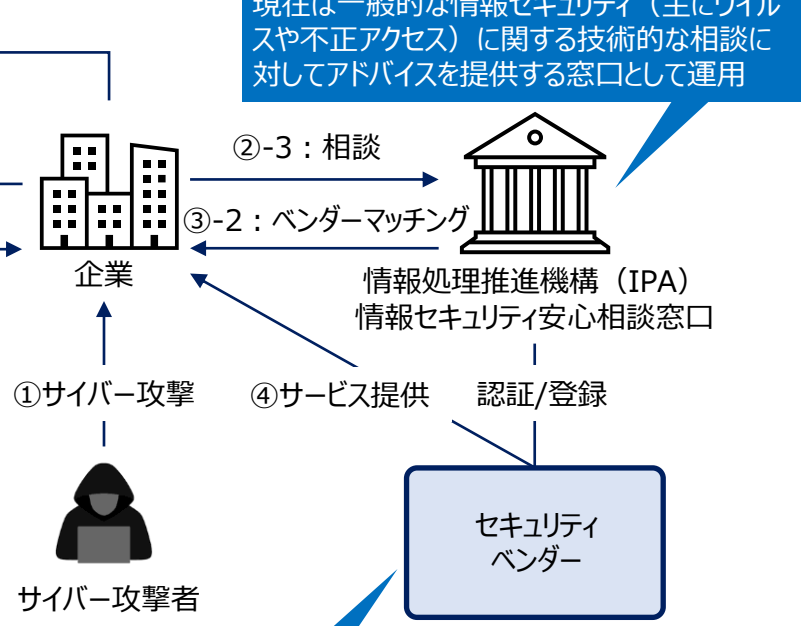


- ✓ 多くのケースで、企業システムがサイバー攻撃を受けた際、一次的にSlerに相談されるが、保守契約のなかにサイバー攻撃に対する対応が含まれていないことがあり、その場合において、企業は専門家による対応の拠り所を失う懸念が生じる。
- ✓ Slerがサイバー攻撃対応を行う場合は、提携しているセキュリティベンダーと連携してサービス提供するケースが多い。
- ✓ 企業がセキュリティベンダーに直接相談して、対応に当たるケースもあるが、ベンダー選定～取引においてトラブルになるケースがある。
- ✓ 企業側としては、サイバー攻撃を受けている状態でセキュリティベンダーとの新規取引によって、事態が悪化するリスク（さらなる情報漏洩や高額取引など）も懸念されるため、自社リソースだけで対応にあたり、問題が泥沼化するケースもある。

従来から信頼できるセキュリティベンダーと取引がある企業や、Slerとの保守契約の中でサイバー攻撃対応を盛り込んでいる企業以外の多くの企業は、インシデント時に対応が後手に回ったり、事態をより悪化させるリスクを常に有している。

政策議論の対象として提案したいあり方

現在は一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する技術的な相談に対してアドバイスを提供する窓口として運用



認証/登録を受けたセキュリティベンダーは政府関連機関（IPAなど）のセキュリティ案件を通じて、インシデント被害企業に紹介する際のオーソライズ材料に活用することも検討するべき。

- ✓ **IPA内の安心相談窓口の機能を強化し、民間企業のサイバー攻撃被害時の相談窓口とする。※現状の窓口は個人による相談を主眼としている可能性あり。**
- ✓ **企業インシデント時は相談窓口として、「信頼に値するセキュリティベンダー」を紹介し、企業とマッチングを行う。また個別のインシデントに関する情報収集と研究を行う。**
- ✓ **セキュリティベンダーにとっても案件獲得機会の増加につながり、産業育成につながる。アクティブサイバーディフェンスの文脈とも一致。**

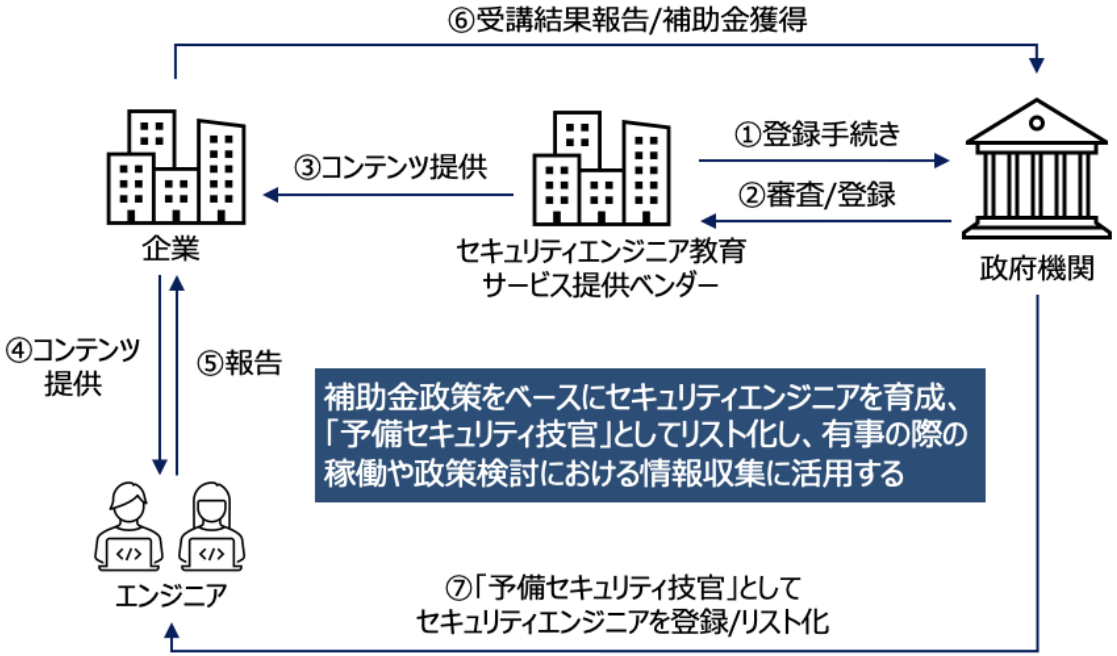
想定される主な論点

論点	コメント
公共機関として、特定の企業を紹介することは憚られるのではないか。	公平性を企図して、下記の方法が考えられる。 ①一律に登録ベンダーに案件情報として配信し、希望するベンダーを企業に紹介する方法。 ②企業にベンダーリストを連携し、企業自らベンダー選定を行う方法。
セキュリティベンダーのマッチングにおいて、どのような企業をつなげるのか	少なくとも当初はIPA「情報セキュリティサービス基準適合サービスリスト」に登録されている企業を対象とすることを想定する。
政策実現にあたって、どのようなコストが必要となるか。	具体的には下記が想定されるが、主に事務局としてのコストとなる。 ①マッチングPF業務を担う人材に関連するコスト ②インシデント情報の収集、研究、公表等に関するコスト ③民間に周知するための広告やPRとしてのコスト
どの程度の相談件数を想定するか。	警察庁発表によるとR6年上半期でのランサムウェア被害報告件数は114件、それ以外が14件とのことであった。

政策提言②：専門人材育成補助金制度/CSIRT･PSIRTサービスに関する認証

専門人材育成補助金制度

セキュリティエンジニア育成専門の補助金制度を実現しつつ、セキュリティエンジニアを政府の予備要員として登録することを企図します。



想定される主な論点

論点	コメント
補助金で育成されたエンジニアは必須で登録となるのか、また登録における条件は想定するか。	登録は任意。特定の実技試験に合格した者を想定する。
「予備セキュリティ技官」の窓口は当該補助金制度以外にどのようなものを想定するか。	有志のうち、「情報処理安全確保技能士」を保有する者もしくは特定の実技試験に合格した者を想定する。
その他排他的条件や参考制度はあるか。	海外にルーツのある技能者はインテリジェンスの観点から極めて慎重な検討が必要。また予備自衛官制度は参考材料として有意義であると思料する。

CSIRT･PSIRTサービス認証（情報セキュリティサービス基準適合サービスリスト）

情報セキュリティサービス基準適合サービスリストにCSIRT/PSIRTサービスに関する認証を追加し、当該領域を振興することを企図します。

情報セキュリティサービス審査登録制度

情報セキュリティサービス基準について

昨今、サイバー攻撃は増加傾向にあり、その手口はますます巧妙化してきています。セキュリティ対策は、セキュリティ製品を購入しただけでは十分ではなく、事業者が行う情報セキュリティサービスの利用も含めて検討する必要があります。

一方で、現在、多くの情報セキュリティサービスが提供されていますが、専門知識をもたないサービス利用者が、サービス事業者の選定時にそのサービスの品質を判断することは容易ではありません。

そのため、情報セキュリティサービスについて一定の品質の維持向上が図られていることを第三者が客観的に判断し、その結果を台帳等でとりまとめて公開することで、利用者が調達時に参照できるような仕組みの提供が求められます。

本基準は、情報セキュリティサービスに関する一定の技術要件及び品質管理要件を示し、品質の維持・向上に努めている情報セキュリティサービスを明らかにするための基準を設けることで、情報セキュリティサービス業の普及を促進し、国民が情報セキュリティサービスを安心して活用することができる環境を醸成することを目的としています。

■情報セキュリティサービス基準

- 情報セキュリティサービス基準第４版（令和６年４月４日公表）NEW!
- 情報セキュリティサービス基準第３版（令和５年３月３０日公表、令和５年４月１日施行）
- 情報セキュリティサービス基準第２版（令和４年１月３１日公表、令和４年４月１日施行）

※経済産業省サイトより
https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html

政策によって目指す効果/目的

1 サイバーセキュリティCSIRT/PSIRT領域の産業を振興

高品質な認証を取得した企業が市場での競争優位性を確保する環境を構築し、サービスの質や運用方法を標準化することで、CSIRT/PSIRT領域全体の品質を向上させることを目指す。

2 ベンダーの技術力/体制の強化や研鑽を主導

各ベンダーが技術力や体制強化/研鑽することへの強力なインセンティブを付与し、また認証を通じて、組織に適切なCSIRT/PSIRT構築支援を行えるベンダーを可視化。

3 当該認証企業によるサービスを通じて、日本企業のサイバーレジリエンス能力を向上

ベンダーが一定の基準を満たしていることを保証し、企業が安心して利用できる環境を構築。企業のサイバーレジリエンス能力の向上に資する。