令和7年度

中小企業サイバーセキュリティ
実践力強化プログラム
事業説明会

中小企業サイバーセキュリティ
実践力強化プログラム　運営事務局

※本事業は東京都より委託を受けて株式会社NTT ExCパートナーが運営しております。

１.事業概要

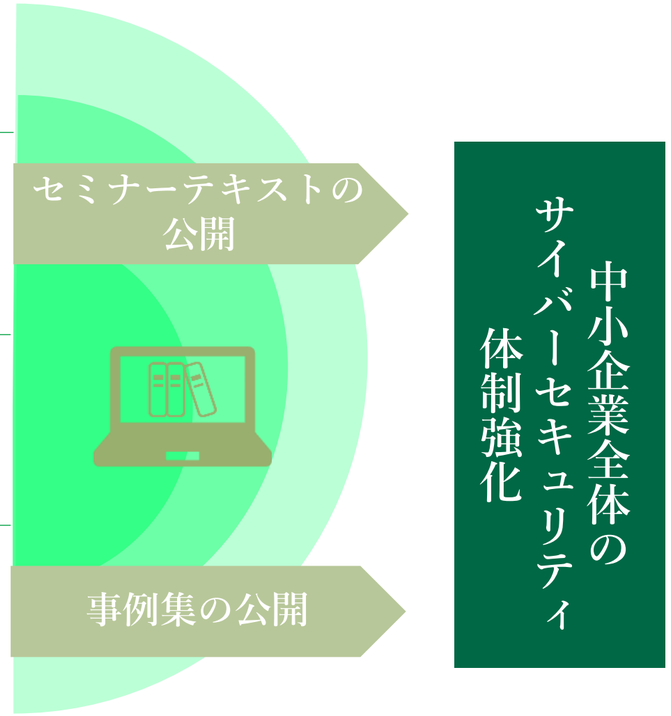
本事業について

事業目的

◆一定程度のセキュリティ対策を実施し、次のステップを目指す中小企業を対象に、サイバーセキュリティ人材の育成支援や実践的な課題解決を通じて、**「次に何をしたらいいか分からない」状態を解消**し、**セキュリティ対策の自走**を後押しします。

◆また、本事業の取り組みを広く社会へ波及させることで、**中小企業全体のサイバーセキュリティ体制強化**を目指します。

	支援	内容
	**サイバーセキュリティ人材育成支援（セミナー）**	セキュリティ対策を計画的に実行できる知識やノウハウが身につくセミナー
	**サイバーセキュリティ対策に関するワークショップ**	課題解決型実践ワークショップ
	**支援対象企業への専門家派遣**	個社ごとの課題を解決する専門家派遣



東京都事業における本事業の位置づけ

レベル１	レベル２	レベル３	レベル３＋α
普及・啓発	**機器・規定整備**	**社内体制整備（人材育成）**	**社内体制整備（インシデント対応）**
中小企業サイバーセキュリティ **啓発事業**	中小企業サイバーセキュリティ **基本対策事業**	中小企業サイバーセキュリティ **実践力強化プログラム**	中小企業サイバーセキュリティ **インシデント対応力強化**
社内全体でセキュリティ対策の必要性を認知する支援	セキュリティ機器の導入や規定策定などの一歩目を踏み出す支援	継続的なセキュリティ対策ができる人材の育成を支援	インシデント対応に特化した体制整備を支援
●サイバー攻撃対応演習セミナー ●標的型攻撃メール訓練 ●ネットワーク調査・構成図作成	●UTMの試行導入 ●EDRの試行導入 ●専門家による規定策定支援 （二つ星宣言までサポート）	●セミナー・ワークショップ （全10回） ●専門家による課題解決支援 （全４回） ●テキスト・事例集の公開	●専門家による体制整備支援 （全６回） CSIRT構築、IT-BCP策定

情報発信・セキュリティ対策点検

中小企業サイバーセキュリティ
社内体制整備（フォローアップ）

過去支援企業を中心にセキュリティ対策の継続や見直しを支援

●レベル別に合わせたコンテンツの提供やセミナーの開催
●セキュリティ対策点検

本事業の支援対象

支援対象

◆東京都内に主たる事業所がある**中小企業**※
◆UTMやEDR等の**一定程度のセキュリティ機器・ソフトウェアを導入**し、**情報セキュリティポリシーを整備済み**

※ 次の表のいずれかに該当する中小企業基本法第２条第１項に規定する中小企業者

業種	資本金及び従業員
製造業、建設業、運輸業、その他	３億円以下又は 300 人以下
卸売業	1億円以下又は100人以下
サービス業	5,000万円以下又は100人以下
小売業	5,000万円以下又は50人以下

支援の全体像

参加前の企業
・サイバーセキュリティに関する
より実践的知識や**自社の課題を発見し、解決すること**に課題を感じている。

専門家派遣

セミナー・ワークショップで得た気づき、
課題を確認し、支援内容を検討。
またセミナー・ワークショップ以外での相談
や課題について幅広い角度から支援を実施。

課題への取組実践

セミナー・ワークショップや専門家派遣を通
した支援内容をもとに取組を実践。
不明点があれば、LMS（後述）を通じて参加
企業相互に連携、専門家サポートを実施。

課題の解決
課題の洗い出し
課題の共有

ワークショップ

中小企業が自社のサイバーセキュリティ課題
を特定し、実践的な解決策を検討・
導入できる体制を構築。
セミナーで学んだ内容のアウトプット、
自社の課題感を明確にし
専門家派遣相談に活用。

セミナー

「次に何をするべきか」に対するヒント
を提供し、中小企業が持続的なセキュリティ
対策につながる下地になるノウハウを提供。
ワークショップ・専門家派遣による取組をも
とに具体的な対策を全員に共有。

テキスト・事例集

事業を通して、テキスト・事例集を作成。
自社のサイバーセキュリティ対策や実践力強化に活用。

参加後の企業
・セキュリティに対する
より深い知識やノウハウの獲得
・実践的な課題解決の経験
・課題の洗い出しと改善行動の明確化
・自律自走できる社内体制の構築

支援のスケジュールイメージ

支援内容	7月	8月	9月	10月	11月	12月	1月	2月	3月
セミナー／ワークショップ（全１０回）	7/25（金）	8/8（金）	8/27（水） 9/11（木）	9/25（木） 10/10（金）	10/27（月） 11/17（月）	12/12（金）	1/16（金）		
専門家派遣（全４回）	１回目		２回目	３回目	４回目				
事例集						ご参加いただいた企業様への取材	事例集作成期間	公表３月下旬～	

２.支援内容

支援を通じて活用するシステムについて

学習管理システム（LMS）

◆支援にあたり、学習管理システム（Learning Management System:以下、LMS）を活用いたします。
◆主に以下の内容を本システムにて配信、参加企業の皆様に活用いただきます。

＜配信コンテンツ＞

- セミナーのオンデマンド配信
- ワークショップ前事：簡易アンケート
- セミナー／ワークショップ後のアンケート
- 情報セキュリティに関するeラーニングコンテンツ配信
  （約１時間　支援期間中無償提供）

＜コミュニティ機能：トークボード＞

- 事務局へのお問い合わせ（日常的な疑問の解消）
- 参加企業同士の交流

セミナー／ワークショップ概要

セミナー

◆ 最新の動向を踏まえたセキュリティの知識習得のみならず、**中小企業が持続的なセキュリティ対策**につなげるための下地になる知識・ノウハウを提供いたします。

ワークショップ

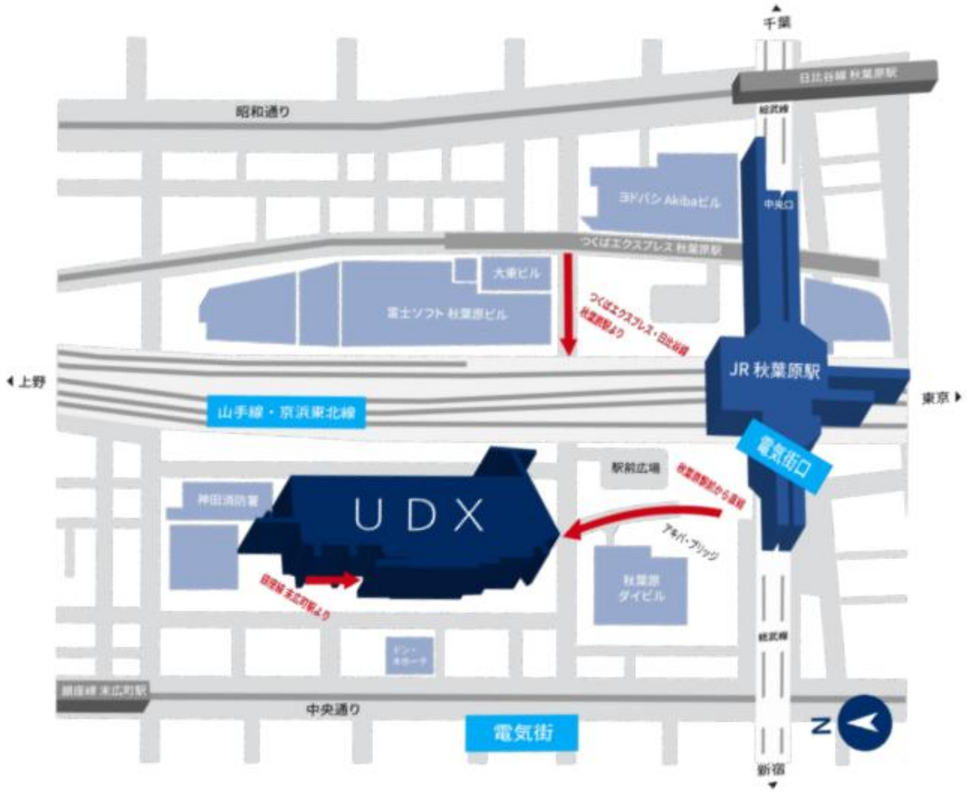
◆ セミナーで得た知識・ノウハウをもとに、**自社のサイバーセキュリティ課題を特定**し、実践的なワークショップをもとに、解決策を検討・導入できる体制の構築を目指します。

●実施期間：**令和７年7月25日（金）～令和8年1月16日（金）**
●開催数　：**全10回**
●開催形式：会場での**対面形式を推奨**しておりますが、オンラインでの参加も可
●条件等　：**全日程（10 回）への参加が必須**
●その他　：各回のセミナー・ワークショップが終わり次第、**アンケート**にご協力願います。

セミナー／ワークショップ日程（予定）

開催回	開催日	会場（詳細は次頁） UDX AKIHABARA SPACE	時間帯	
			セミナー	ワークショップ
第１回	令和７年７月25日（金）	カンファレンスE	13:00～15:00	15:30~17:30
第２回	令和７年８月８日（金）	カンファレンスD		
第３回	令和７年８月27日（水）	カンファレンスD		
第４回	令和７年９月11日（木）	カンファレンスD		
第５回	令和７年９月25日（木）	カンファレンスD		
第６回	令和7年10月10日（金）	カンファレンスE		
第７回	令和7年10月27日（月）	カンファレンスD		
第８回	令和7年11月17日（月）	カンファレンスD		
第９回	令和7年12月12日（金）	カンファレンスD		
第10回	令和8年1月16日（金）	カンファレンスD		

セミナー／ワークショップ会場

アクセス	地図
【所在地】 〒101-0021 東京都千代田区外神田4-14-1 秋葉原UDX 6F 【交通機関】 JR秋葉原駅　徒歩2分 東京メトロ銀座線　末広町駅　徒歩3分 つくばエクスプレス　秋葉原駅　徒歩3分 東京メトロ日比谷線　秋葉原駅　徒歩4分	

講師紹介

矢野　泰広（やの　よしひろ）

業務経験：26年（セキュリティ経験：15年）
専門分野：情報セキュリティ、DX、ICT、クラウド技術、
ネットワーク技術、DB設計・構築、プロジェクト
マネジメント、WEBシステム設計・構築、
サーバ設計・構築
保有資格：情報処理安全確保支援士（第004005号）
情報処理技術者試験 プロジェクトマネージャ

中小企業を中心にDX、ネットワーク、クラウド技術および情報セキュリティに関する構築や導入支援やコンサルティングの経験が豊富。併せて長年にわたり大手通信事業者のSE（技術営業）を対象に指導を行ってきた事から、幅広い業種、業態の企業の状況を認識しており、中小企業の課題点を的確に捉え、各企業が取り組みやすい解決策を提示する対応力に定評がある。

セミナー内容（予定）

※全10回のセミナーで下記のテーマを学びます。

セミナー内容 （テーマ）
◘ サイバーセキュリティを取り巻く背景
◘ 中小企業に求められるデジタル化の推進とサイバーセキュリティ対策
◘ これからの企業経営で必要なIT活用とサイバーセキュリティ対策
◘ セキュリティ事象に対して組織として策定すべき対策基準と具体的な実施
◘ 各種ガイドラインを参考にした対策の実施
◘ ISMS等のワークフレームの種類と活用法の紹介
◘ ISMSの構築と対策基準の策定と実施手順
◘ 具体的な構築・運用の実践
◘ 組織として実践するためのスキル・知識と人材育成
◘ サイバーレジリエンス能力の育成
◘ 全体総括

ワークショップ内容（予定）

ワークショップの流れ

テーマ紹介と目標設定

簡易アンケート

事前課題
（LMSを通じて配信）

グループ討議

発表と質疑応答

講師コメント・フィードバック

意見交換とアクションプラン

グループ討議の具体的な流れ
①役割・時間配分決め
②事前課題に基づく
グループテーマ決め
③議論の発散（各社取組・事例・課題感の共有）
④議論の収束（対応策、方法論の検討）
⑤発表準備

アウトプット内容の共有

ワークショップは各回のセミナーテーマと連動します。

- ☐ サイバーセキュリティを取り巻く背景
- ☐ 中小企業に求められるデジタル化の推進とサイバーセキュリティ対策
- ☐ これからの企業経営で必要なIT活用とサイバーセキュリティ対策
- ☐ セキュリティ事象に対して組織として策定すべき対策基準と具体的な実施
- ☐ 各種ガイドラインを参考にした対策の実施
- ☐ ISMS等のワークフレームの種類と活用法の紹介
- ☐ ISMSの構築と対策基準の策定と実施手順
- ☐ 具体的な構築・運用の実践
- ☐ 組織として実践するためのスキル・知識と人材育成
- ☐ サイバーレジリエンス能力の育成
- ☐ 全体総括

専門家派遣の概要

◆ 参加企業それぞれが洗い出した課題の解決を支援するため、**多数の専門領域を持つサイバーセキュリティの専門家**が、参加企業の状況に対応したサポートを提供いたします。

◆ セミナーやワークショップで得た知見を活かし、参加企業の皆様が自ら対策を立案できるようアドバイスを行います。

●実施期間：**令和７年7月～令和8年1月**
●実施回数：**計４回**
●実施時間：**約2時間／回**
●開催形式：**ご訪問orオンライン**
●条件等　：原則として、**全4回の専門家派遣の受入れが必要**です。
●その他　：日程については、参加企業のご要望を踏まえて実施いたします。
　　初回は、7月上旬～を予定しております。

専門家派遣の流れ

回	支援時期	目的	専門家による支援内容
1回	セミナー/ワークショップ開始前	支援対象企業のサイバーセキュリティの現状分析と基礎構築	**◎支援対象企業のサイバーセキュリティ状況を分析** 現状のセキュリティ規程・ルールと組織のリスク評価を実施 支援対象企業が把握していないと思われる課題の抽出も可能な限り実施 **◎新技術によるリスクの議論** デジタルトランスフォーメーションや生成AI等の現状活用状況や中期的な計画を把握し、リスクを予測 **◎次のステップの計画** １年後の目指すゴールを想定して、２回～４回の支援内容のすり合わせと今後必要なISMSなどのフレームワークの活用について準備
2回	セミナー/ワークショップ開始後	抜け漏れなく、また過剰な対策もない様にバランスよく管理策を活用	**◎サイバーセキュリティ対策の基盤強化（組織的管理策・人的管理策の適用）** サイバーセキュリティ対策を有効に機能させるため、先ずは組織的管理策、人的管理策の課題を解決 **◎サイバーセキュリティ対策の実践準備（技術的管理策の選定）** 技術的管理策に追加で必要なる可能性のあるシステム・ツールの検討 **◎支援対象企業の物理的環境を確認（物理的管理策の確認）** 物理的管理策のチェック（支援対象企業の物理的環境を確認）
3回	セミナー/ワークショップ中盤～終盤	セミナー/ワークショップの内容を実践	**◎セミナー/ワークショップで学んだ内容を実践** 作成したツール・フレーム等を用いて実活用を試行 修正・変更対応が必要な部分を支援企業と共に実行 フォローが必要な人員へセミナー/ワークショップの情報を改めて共有
4回	セミナー/ワークショップ終盤～終了後	セキュリティ対策の継続ノウハウを実践	**◎持続可能な手法の習得/内部体制構築の手法を習得** 支援対象企業が次年度以降もが持続的に情報セキュリティサイバーセキュリティ対策を実行できるよう、内部監査体制の構築支援や外部監査の活用方法を支援 **◎外部専門家との連携** IPAの活用方法やISMS審査員など外部専門家との連携方法を把握

セミナーテキストと事例集について

セミナーテキスト

◆ 各セミナーの内容はテキストとして作成します。

事例集

◆ 参加企業の皆様が事業を通じて取り組んだ過程や得られた成果などをまとめた事例集を作成します。

活用例

- 参加企業の皆様のセミナー内容の復習用
- 中小企業のセキュリティ対策実践マニュアル
- 社内教育や情報共有のツール
- 取引先やパートナー企業との情報共有ツール
- 他社の事例を参考に、自社のセキュリティ対策の改善・見直し

※昨年度事例集

参加企業同士の交流

◆ コミュニケーションを通じた相互学習・相互理解・気軽に相談できる場を活用いただき、**継続的な横のつながりを参加企業の皆様で創り上げること**を目指します。

ワークショップ

リアルな課題に対する相互学習（協力）

- 属する業界や事業規模、状況でグループ分け
- 共通の目標に従って、企業同士で課題解決

座談会（任意参加）

お互いを知ることでさらに信頼感を深める

- ワークショップのグループ、グループを超えて、相互理解の深化
- 自社での取組紹介、他社の取組を知ることを通して、多様な気づき

オンラインコミュニティ（LMS）

日常的な悩みや困りごとを共有

- トークボードによる参加者同士の情報交換
- 「いいね」や返信による相互フィードバック
- 各回のセミナーやワークショップの感想や気づきを共有

サポート体制

対応窓口

●電話番号：0120-003-788

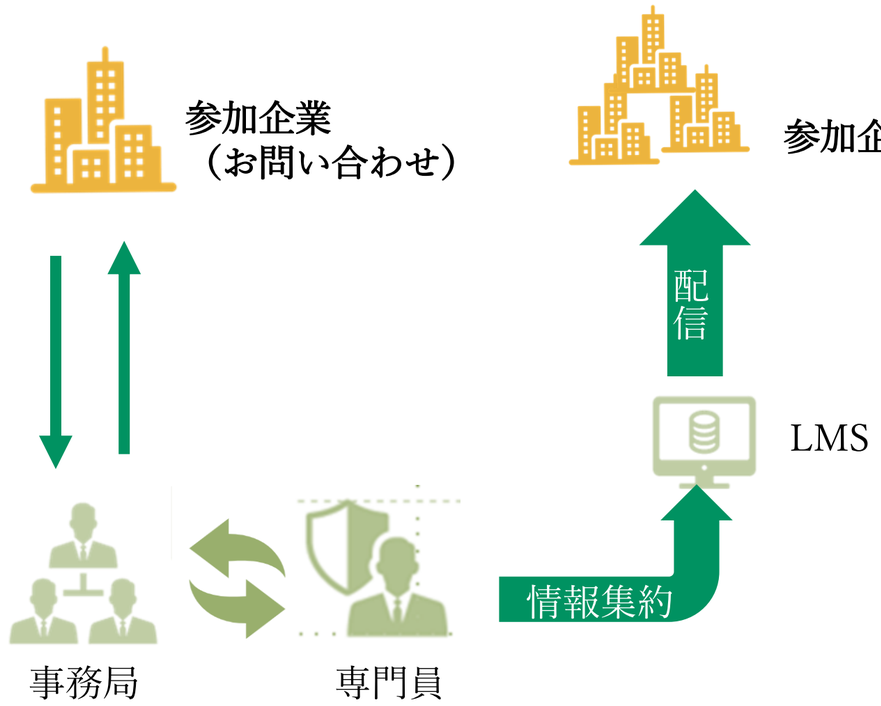
●メールアドレス：
2025.syanaitaisei-ml@nttls.co.jp

●事業ホームページ：
https://zissenkyouka.metro.tokyo.lg.jp/

●LMS（参加企業のみ）
：トークボードからのお問い合わせ

※対応時間：平日9:00～17:00

専門的な相談について



- 専門的な相談については、専門員と連動しながら回答いたします。
- 情報を集約し、お問い合わせ内容が他社様にも有益な内容となる場合は、LMSを通じて情報配信いたします。

３．募集概要

募集概要

申込期限	令和７年６月30日（月）
支援対象	①東京都内に主たる事業所を有する中小企業者 ②UTMやEDR 等の一定程度のセキュリティ機器・ソフトウェア を導入し、情報セキュリティポリシーを整備済みである中小企業
受講対象	本事業における取組に意欲的に参加できる経営者・セキュリティ担当者等
募集企業数	40社 （**小売・卸売枠**10社程度、**建設・製造枠**10社程度、**サービス・その他枠**20社程度）
参加費用	無料 （交通費・通信費等は参加企業の自己負担となります）
会場	（セミナー/ワークショップ）東京都千代田区外神田4-14-1　秋葉原UDX 6F （専門家派遣）参加企業様の事務所等

参加条件

本事業における取組に意欲的に参加できる経営者・セキュリティ担当者等	
要提出物	・参加同意書 ・機密保持の同意書 **本事業への参加者ご自身と所属企業の同意をいただける方**が対象となります。
参加人数	1社につき1名
参加の条件	本事業は継続したプログラムを受講していただく形で構成されている為、 原則として**お申し込み時にご登録いただいた方に最後まで受講していただく** ことが前提になります。

募集企業

日本標準産業分類などを参考に、表の3枠に設定し、合計で**40社**を募集いたします。
※各枠の社数は目安となりますので、応募状況により変動する場合がございます。
※応募多数の場合は、抽選にて参加者を決定します。

募集企業 （定員数） 40社	小売・卸売枠 １０社程度	小売業
		卸売業
	建設・製造枠 １０社程度	建設業
		製造業
	サービス・その他枠 ２０社程度	情報通信業
		運輸業、郵便業
		金融業、保険業
		不動産業、物品賃貸業
		学術研究業、専門・技術サービス業
		宿泊業・飲食サービス業
		生活関連サービス業・娯楽業
		教育・学習支援業
		医療・福祉
		その他の業種

お申し込み時における注意事項

✓ **申込後の事前確認**

：社内にてセキュリティ対策を継続的に実施することを想定した実践的な内容であることから、**一定のセキュリティ対策を実行中の企業**が対象となります。また、お申し込み後３営業日以内に運営事務局から電話にてセキュリティレベルを確認いたします。

✓ **参加規程や遵守事項の了解**

：運営事務局から電話確認をさせていただく際に、参加に当たっての規程や遵守事項をご説明差し上げます。その内容についてご了解の後に、申し込み完了となります。

※申込フォームの送信で、お申込が完了とはなりませんのでご注意ください。

✓ **参加条件への了解**

：・全 10 回のセミナー・ワークショップへの参加
・1 社につき 4 回の専門家派遣に参加

✓ **機密保持の同意書への同意**

：セミナー・ワークショップで、企業のセキュリティ体制等の機密情報に係る事項をテーマとして取り扱い、参加企業間で自社の状況や課題についてディスカッションを行うことが想定されるため、**機密保持の同意書に同意**いただけること。

✓ **参加同意書への同意**

：事例集を作成することへの同意や、作成に必要な参加企業への取材やアンケートへのご協力について、**参加同意書に同意**いただけること

申し込みの流れ

ホームページから
事業申込

▶

運営事務局よりご連絡
▼セキュリティレベルの確認
▼規定、遵守事項の確認

▶

申込結果のご連絡
※応募多数の場合は抽選

▶

参加同意書・
機密保持の同意書提出

▶

参加確定

▶

支援開始

機密保持の同意書と参加同意書

参加同意書

令和　　年　　月　　日

＜企業同意部分＞

企業名：

企業所在地：

代表者氏名：　　社　印

＜参加者同意部分＞

参加者氏名：　　本人印

＜個人情報の取扱いについて＞
・ご記入いただきました事項は万が一、事故等が起きた場合の対応等に使用させて頂く場合がございます。
・その他において第三者に対し、これらの情報を提供する事はありません。

機密保持の同意書

「中小企業サイバーセキュリティ社内体制整備事業」への参加に当たり、当社及び参加者が、上記機密事項に関わる条件に同意した証として、下記に記名捺印の上、運営事務局に提出します。

令和　　年　　月　　日

＜企業同意部分＞

企業名：

企業所在地：

代表者氏名：　　社　印

＜参加者同意部分＞

参加者氏名：　　本人印

注意事項

参加者ご自身と所属企業の**両方の同意**が必要になります。

同意書の内容をよくお読みいただき、同意した上で、署名と**担当者印、社印**を押印していただくようお願いいたします。

お申し込み・お問い合わせ

事業申込フォームからお申し込みください

〈中小企業サイバーセキュリティ実践力強化プログラム　運営事務局〉

電話番号：0120-003-788　受付 平日9:00～17:00

メールアドレス：2025.syanaitaisei-ml@nttls.co.jp

事業ホームページ：
https://zissenkyouka.metro.tokyo.lg.jp/cybersecurity-support-program