東京都

東京都中小企業サイバーセキュリティ向上支援事業

事業概要

こんなお悩みありませんか？

セキュリティ対策が不十分

近年、セキュリティ対策の弱い中小企業への　サイバー攻撃が　さらに深刻化。

サイバー攻撃が原因なのか判定が難しい

トラブル時に原因の特定・判断等が難しくどうしたらいいかわからない。

専門知識を有する人材の不足

IT専門人材が不足、経営者自らが構築・運用するケースも多いのが現状。

1．事業概要

東京都中小企業サイバーセキュリティ向上支援事業とは

- 中小企業に対する「**サイバー攻撃の実態を把握**」するとともに「**自立的なサイバーセキュリティ対策の後押し**」「**サイバーセキュリティ対策に対する意識の向上**」を行うことを目的とした**東京都による中小企業支援事業**です
- 請負事業者(NTT東日本)が事業主体となり、**中小企業のサイバーセキュリティ対策支援**を行います

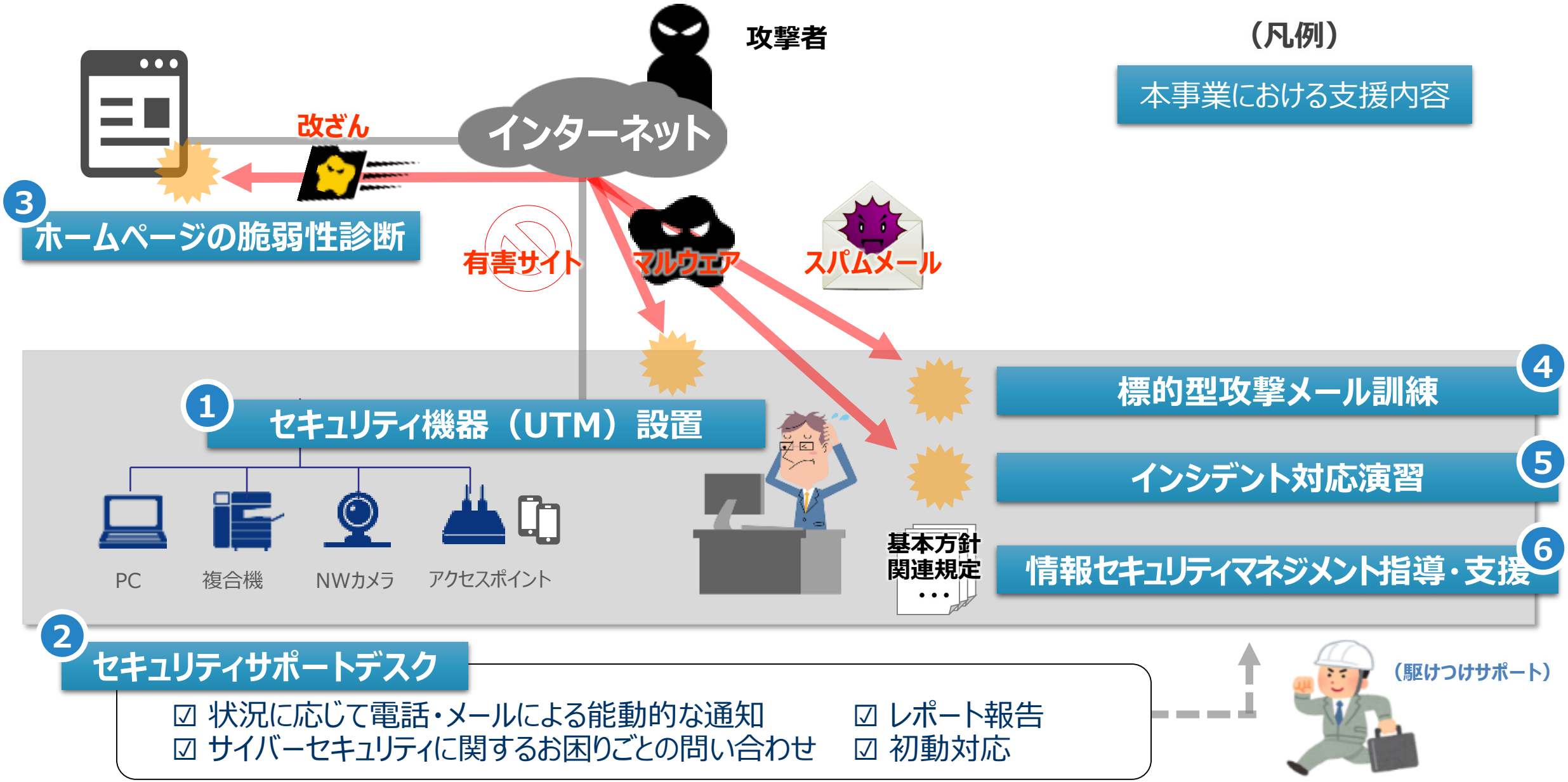
２．実施概要

■主な支援内容

（参加企業の費用負担はありません）

- **セキュリティ機器の設置**によるサイバー攻撃状況の把握･分析
- **セキュリティサポートデスク･駆けつけサポート**の提供
- **標的型攻撃メール訓練、インシデント対応演習**の実施
- **ホームページの脆弱性診断**の実施
- **情報セキュリティマネジメント指導･支援**の実施

2．実施概要


攻撃者
（凡例）
本事業における支援内容
インターネット
改ざん
3 ホームページの脆弱性診断
有害サイト
マルウェア
スパムメール
1 セキュリティ機器（UTM）設置
PC
複合機
NWカメラ
アクセスポイント
基本方針
関連規定
・・・
4 標的型攻撃メール訓練
5 インシデント対応演習
6 情報セキュリティマネジメント指導・支援
2 セキュリティサポートデスク
☑ 状況に応じて電話・メールによる能動的な通知
☑ サイバーセキュリティに関するお困りごとの問い合わせ
☑ レポート報告
☑ 初動対応
（駆けつけサポート）

2．実施概要

①セキュリティ対策機器（UTM） ・ ②セキュリティサポートデスク

支援期間	原則3カ月以上
対象者	本事業のご参加企業
支援内容	✓事業所内に**セキュリティ対策機器（UTM）を設置**し、**ウィルスや不正アクセスをブロック**します ✓ブロック状況について、**月次でレポートを配信**、**自社のサイバー攻撃状況を把握**できます ✓サポートデスクにて**サイバー攻撃に係る各種お困りごとやインシデント判断・遠隔駆除を実施**します

＜UTM機器の機能＞

不正アクセスブロック	**不正プログラム対策**	不正な通信、プログラムによる攻撃を検知し、内部感染を発見する機能
	Webサイトアクセスブロック	不正プログラムによる感染、フィッシング詐欺被害を未然に防止する機能
不正侵入対策	**ファイアウォール**	外部のネットワークからの攻撃や不正なアクセスをブロックする機能
	IPS※(不正侵入防御)	ネットワーク内に侵入した不正なパケットを検知し、攻撃を防御する機能
メールセキュリティ対策		メールに含まれる不正プログラムの検知やスパム（迷惑）メールを判定する機能
URL指定によるアクセス制御		特定のサイトのみをブロックしたり、ブロックしたカテゴリから、特定のサイトのみをアクセス可能とする機能
アプリケーション利用制限		設定したアプリケーションの利用制限に基づき、通信の検出・ブロックを行う機能

2．実施概要

③ホームページの脆弱性診断

支援期間	本事業期間中に1回実施
対象者	本事業参加企業様のうち、**希望者のみ（定員制、先着順）**
支援内容	✓ホームページに情報漏えいやホームページの**改ざんにつながる脆弱性が無いか、ホームページが改ざんされて不正なホームページへのリンクが埋め込まれていないかを診断**し、結果を通知します

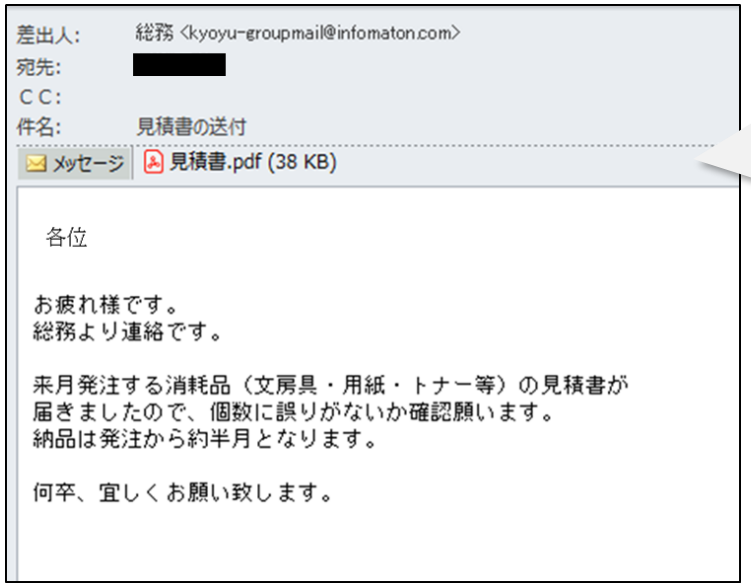
＜診断結果イメージ＞

2．実施概要

④標的型攻撃メール訓練

支援期間	本事業期間中に2回実施予定
対象者	本事業のご参加企業（各社2アドレスまで）
支援内容	✓指定いただいたメールアドレス宛に**「標的型攻撃メール」を装ったメールを送付**します ✓メールの添付資料等を開いた場合・開かなかった場合どちらの場合でも、本訓練により**「社員のセキュリティ意識醸成」**にお役立ちいただけます。

＜標的型攻撃メール訓練　本文サンプル＞



添付資料を開いた場合のイメージ

これは標的型攻撃メールの訓練メールです

今回は訓練として、皆様に標的型メール攻撃を疑似的に体験していただくため、標的型メール攻撃の訓練」を実施しました。

（中略）

不審なメールを『 受け取った 開いてしまった』場合は、上長または関係部署に速やか にエスカレーションしてください。

2．実施概要

⑤インシデント対応演習

支援期間	本事業期間中に1回実施（複数回実施する内の1回にご参加）
対象者	本事業参加企業様のうち、**希望者のみ（定員制、先着順）**
支援内容	✓中小企業経営者や担当者の目線で、**サイバー攻撃発生時に適切な判断ができるか、カードゲーム形式で演習**を実施します

＜演習イメージ＞

イベントを提示

発生したイベントに対して、どのようなアクションをとるか決定

ゲームを通じ事故対応の難しさを体験することで事故対応ノウハウを学ぶことができます

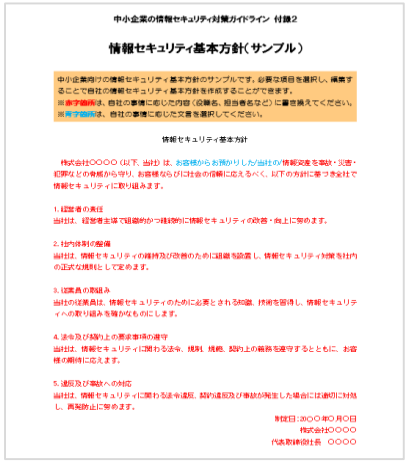
2．実施概要

⑥情報セキュリティマネジメント指導・支援

支援期間	本事業期間中に4回の指導を実施
対象者	本事業参加企業様のうち、**希望者のみ（定員制、先着順）**
支援内容	✓サイバーセキュリティに関する**基本方針や規定等の策定等に向けた指導・支援**を行います ✓合計**4回の指導を実施し、セキュリティ基本方針等を策定しながら対策・運用の実施計画を作成**することで支援業務終了後の自律的な運用を目指します

＜作成を支援する規定等の内容（サンプル）＞

①情報セキュリティ基本方針



中小企業の情報セキュリティ対策ガイドライン 付録2

情報セキュリティ基本方針（サンプル）

中小企業向けの情報セキュリティ基本方針のサンプルです。必要な項目を選択し、編集することで自社の情報セキュリティ基本方針を作成することができます。
※赤字箇所は、自社の事情に応じた内容（役職名、担当者名など）に書き換えてください。
※青字箇所は、自社の事情に応じた文言を選択してください。

情報セキュリティ基本方針

株式会社○○○○（以下、当社）は、お客様からお預かりした/当社の情報資産を脅威・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

1. 経営者の責任
当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

2. 社内体制の確備
当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。

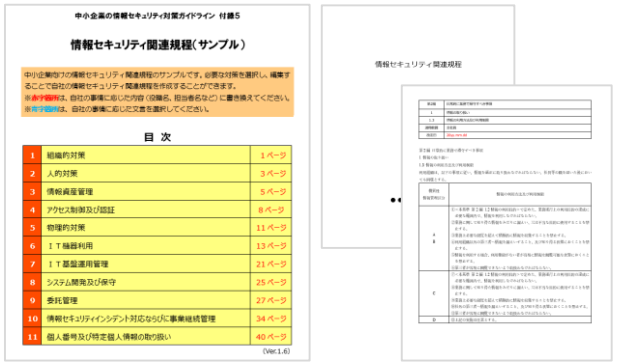
3. 従業員の教育
当社の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを怠りなくものにします。

4. 法令及び契約上の要求事項の遵守
当社は、情報セキュリティに関わる法令、規則、規範、契約上の義務を遵守するとともに、お客様の期待に応えます。

5. 違反及び事故への対応
当社は、情報セキュリティに関わる法令違反、契約違反及び事故が発生した場合には適切に対処し、再発防止に努めます。

制定日：20○○年○月○日
株式会社○○○○
代表取締役社長　○○○○

②情報セキュリティ関連規定



中小企業の情報セキュリティ対策ガイドライン 付録5

情報セキュリティ関連規程（サンプル）

中小企業向けの情報セキュリティ関連規程のサンプルです。必要な対策を選択し、編集することで自社の情報セキュリティ関連規程を作成することができます。
※赤字箇所は、自社の事情に応じた内容（役職名、担当者名など）に書き換えてください。
※青字箇所は、自社の事情に応じた文言を選択してください。

目　次

(Ver1.6)

情報セキュリティ関連規程

③セキュリティ対策の実施計画書

セキュリティ対策実施計画書

令和●年　●月●日
企業名：

◇実施体制

◇関連規定

◇実施ロードマップ

3．ご留意いただきたい事項

募集期間	定員に達し次第終了
対象	**東京都内に主たる事業所をお持ち**であり、 **東京都のサイバーセキュリティ対策を目的とする他の補助事業を活用していない**中小企業者※1様
募集数	**250社程度※2を予定（先着順）**
ご参加時の留意事項（概要）	✓中小企業に対するサイバー攻撃の実態把握を目的に、**支援期間中に得たサイバー攻撃レポート結果等を集計・分析し東京都様に報告**いたします。 ✓支援開始時・支援終了時等に実施するセキュリティ対策に関わる**アンケートの記入・提出**へのご協力をお願いします。 ✓本事業にご参加いただいた企業様の中から、中小企業のサイバーセキュリティ対策の参考となる取り組み等についてヒアリング調査をさせていただく場合がございますのでご協力をお願いいたします。
費用負担	本事業参加にあたって、参加企業様に費用負担を求めることはありません

※1中小企業基本法に第二条第一項に定める中小企業者・小規模企業者

※2 支援内容により異なる

４．参加申し込みの流れ

事業参加お申し込み

本事業にご参加いただける条件に則り参加決定を判断

※お客様環境等を総合的に判断し、事業へのお申し込みをお断りする場合もしくは一部サービスのみ提供となる場合がございます

現状・実態把握

事前アンケート、環境調査、機器設置

支援・相談受付

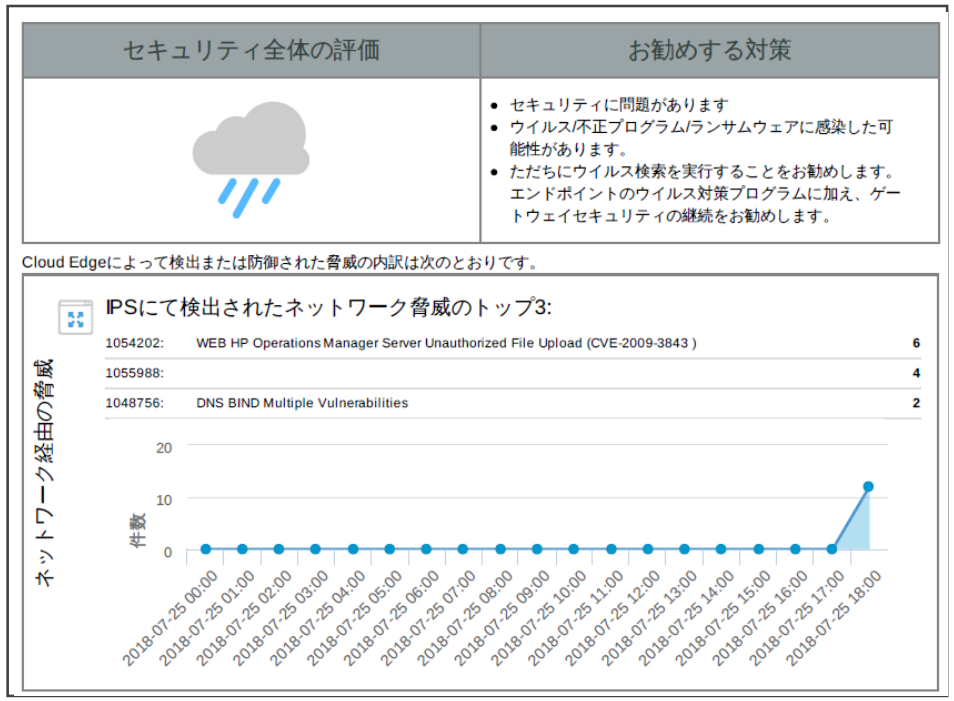
セキュリティ対策サービス・相談窓口等の利用

4．参加申し込みの流れ

改善検討

事後アンケート、個別コンサルティング

UTMレポートイメージ



セキュリティ全体の評価	お勧めする対策
	• セキュリティに問題があります • ウイルス/不正プログラム/ランサムウェアに感染した可能性があります。 • ただちにウイルス検索を実行することをお勧めします。エンドポイントのウイルス対策プログラムに加え、ゲートウェイセキュリティの継続をお勧めします。

Cloud Edgeによって検出または防御された脅威の内訳は次のとおりです。

IPSにて検出されたネットワーク脅威のトップ3:

1054202:	WEB HP Operations Manager Server Unauthorized File Upload (CVE-2009-3843)	6
1055988:		4
1048756:	DNS BIND Multiple Vulnerabilities	2

各企業様へ個別にフィードバック

するとともに

事業全体として統計・分析等

を実施します

５．本事業に関する連絡先

参加申し込み又は**ご興味のある方**は
下記までお問合せください。

【お申込み･お問合せ先】

東日本電信電話株式会社

東京事業部　事務局

E-mail：cs-tokyo-ml@east.ntt.co.jp