

# 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

## 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」とともに「自主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の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。

### ● 実態把握について

1. 現場調査やアンケート等によるサイバーセキュリティ**対策状況の実態把握**
2. セキュリティ対策機器(UTM)の設置による**サイバー攻撃の状況及び相談内容等の把握**
3. 「標的型攻撃メール訓練」等による**セキュリティ意識把握**

# 3. 参加申し込みの流れ

## 事業参加お申し込み

「本事業における中小企業等の定義」等の対象条件に則り参加決定を判断いたします

※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

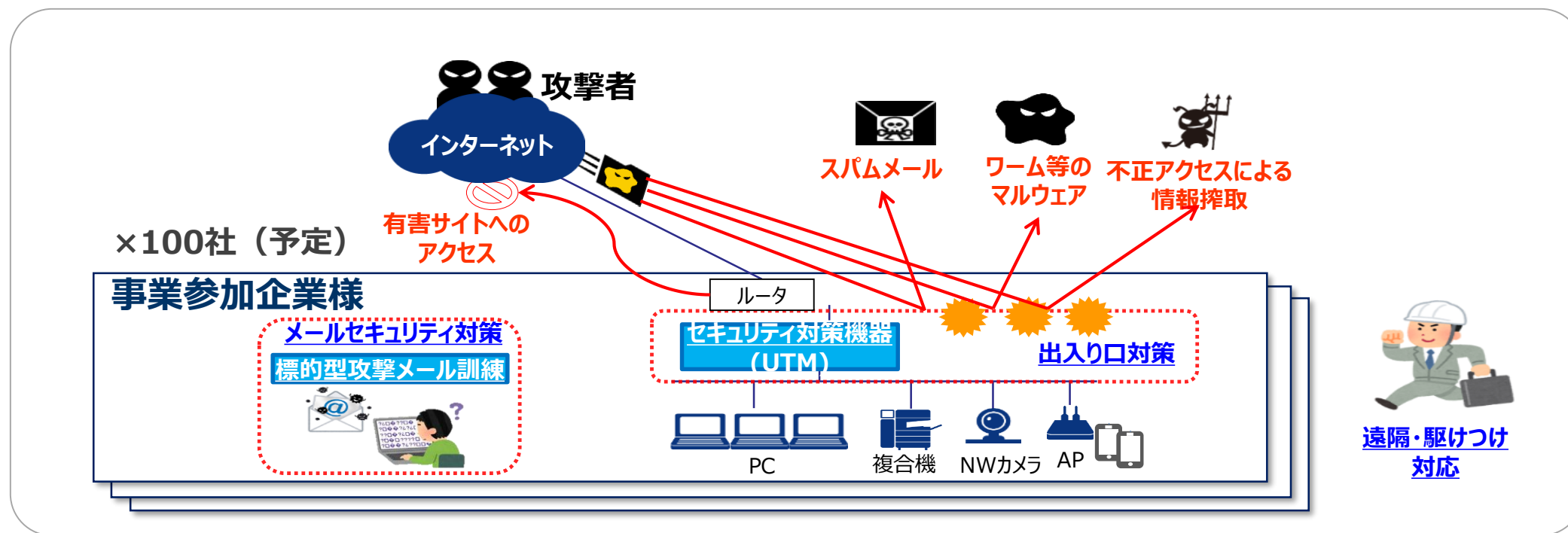
## 現状・実態把握

- ✓ 事前アンケート
- ✓ 環境調査
- ✓ 機器設置
- ✓ 事後アンケート

# 3. 参加申し込みの流れ







## 支援・相談

- ✓ セキュリティ対策サービス体験
- ✓ 相談窓口等の利用



# 3. 参加申し込みの流れ

本事業において設置するUTMが提供するネットワークセキュリティ対策機能は以下の通りです

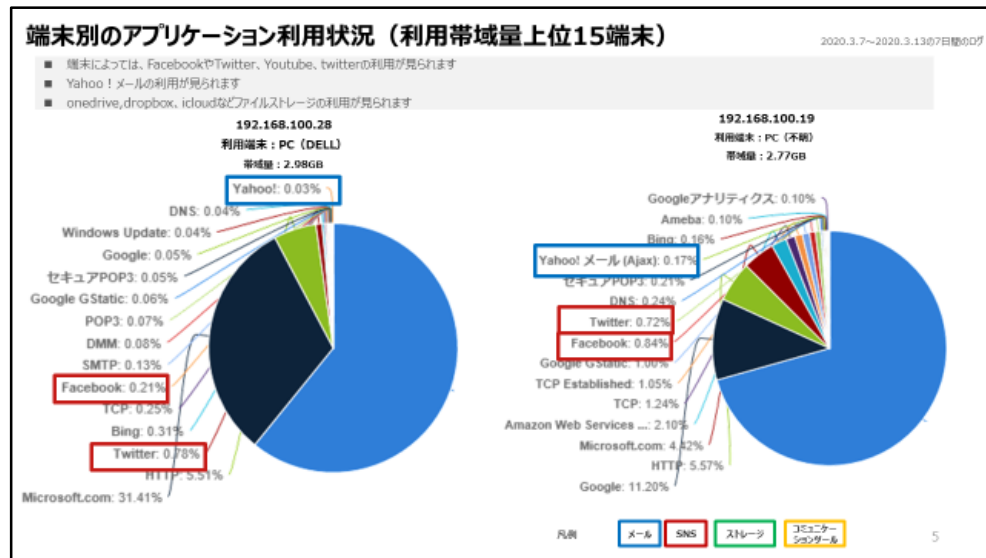
	不正アクセス ブロック	不正プログラム対策	不正な通信、プログラムによる攻撃を検知し、 内部感染を発見する機能
		Webサイトアクセスブロック	不正プログラムによる感染、フィッシング詐欺被害 を未然に防止する機能
 	不正侵入対策	ファイアウォール	外部のネットワークからの攻撃や不正なアクセスを ブロックする機能
		IPS(不正侵入防御)	ネットワーク内に侵入した不正なパケットを検知し、 攻撃を防御する機能
	メールセキュリティ対策		メールに含まれる不正プログラムの検知や スパム（迷惑）メールを判定する機能
	URL指定によるアクセス制御		特定のサイトのみをブロックしたり、特定のサイトの 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

# 3. 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

### ■ レポート報告例



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

# 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。





### 3. 参加申し込みの流れ

**参加申し込み**又は**ご興味のある方**は  
下記までお問い合わせください。

**【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](mailto:cs-tokyo-ml@east.ntt.co.jp)**