NTT東日本
東日本電信電話株式会社
News Release

2017 年 6 月 7 日

セキュリティインシデント監視・復旧支援サービス「おまかせサイバーみまもり」を提供開始

～ネットワークセキュリティの強化・運用は NTT 東日本にお任せ！～

- NTT 東日本は、これまでに培ってきたネットワーク保守・運用、およびユーザサポートノウハウを活用した新たなセキュリティサービス「おまかせサイバーみまもり」（以下、本サービス）を 2017 年 6 月 29 日（木）より提供開始いたします。
- 本サービスは、お客さまのオフィス内に不正通信の検知・遮断機能を搭載した専用 BOX を設置することでネットワークセキュリティを強化するとともに、NTT東日本のセキュリティサポートデスクによる不正通信状況の監視・有事の際の復旧支援を提供するサービスです。
- 本サービスは、ネットワークセキュリティの強化に加えて、万が一ウイルス感染による不正通信を検知した際にはお客さまへご連絡し、電話等によるウイルス駆除や端末の復旧を支援いたします。電話等での対応が困難な状況においては、訪問によるサポートも実施するため、より安心・安全なセキュリティ対策が可能となります。
- なお、本サービスはトレンドマイクロ株式会社のネットワークセキュリティ対策技術を活用して提供いたします。

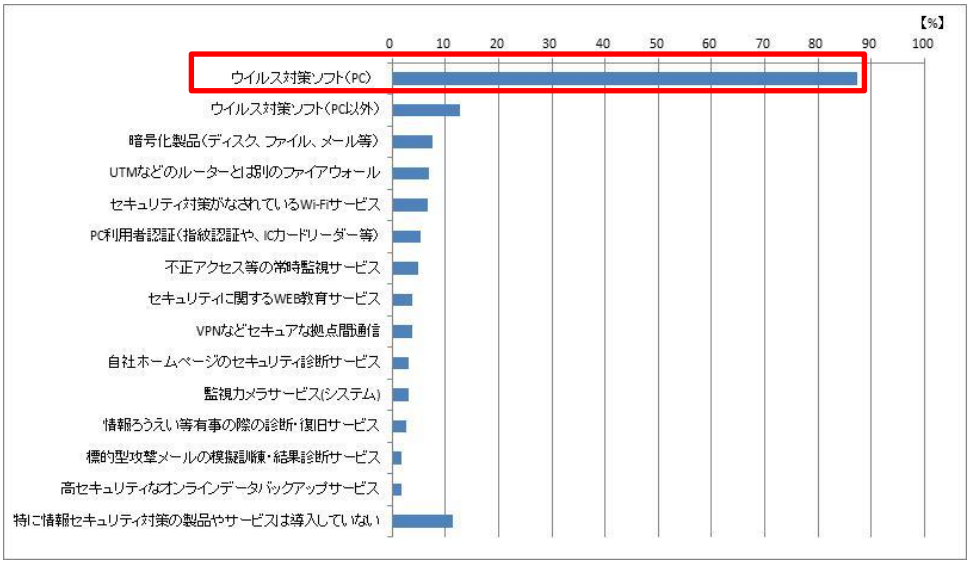
1.提供の背景と目的

近年多様化するサイバー攻撃等のセキュリティリスクは中小企業にまで及んでいるものの、セキュリティ対策がパソコンへのウイルス対策ソフトの導入に留まる中小企業が多くを占めています(図 1)。一方で、昨今のサイバー攻撃は、パソコンのみならずネットワークカメラや複合機等、ネットワークにつながる全ての機器が対象となっており、感染したウイルスによって企業の端末がネットワークを通じて外部のサーバーと不正な通信を行うことで、個人情報の流出などにつながる事例も発生しています。このため、ウイルス感染リスクの低減に向けたネットワークへのセキュリティ対策や、ウイルス感染時の迅速な事後対応の必要性が増しています。

また、専任のセキュリティ担当者を置いていない中小企業（図 2）からは、「ウイルス対策以外にどのようなセキュリティ対策に着手すればいいのかわからない」といった声や、UTM 等のウイルス対策ソフト以外のセキュリティ対策を施していながらも、「日々の不正通信のモニタリングができない」「万が一ウイルスに感染した場合の対処方法がわからない」等の声が多く上がっており、実効性のあるセキュリティ対策の運用が課題となっています。

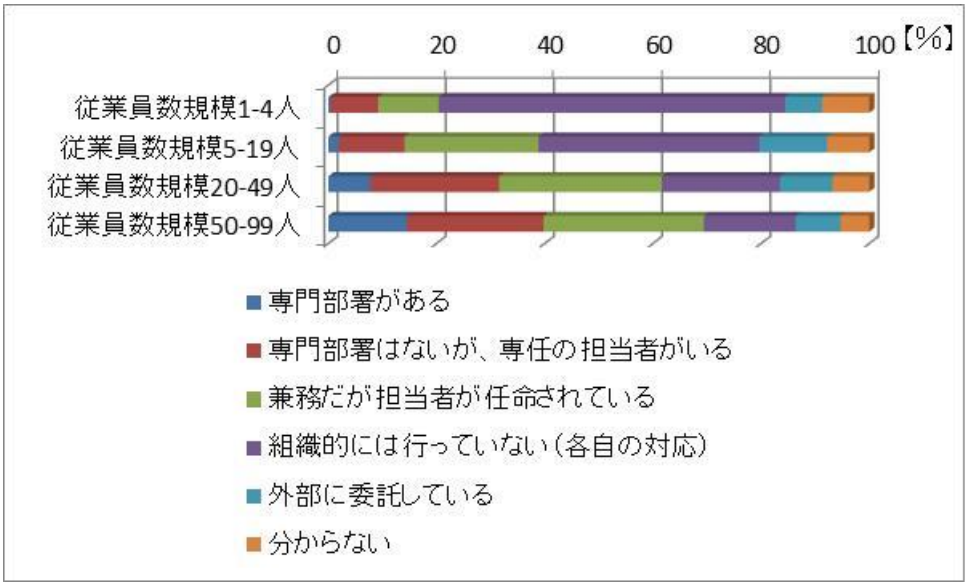
こうした状況を踏まえ、NTT 東日本では、ネットワークへのセキュリティ対策はもちろん、NTT東日本のセキュリティサポートデスクによる不正通信状況の監視・有事の際の復旧支援を提供する、「おまかせサイバーみまもり」を 2017 年 6 月 29 日（木）より提供開始いたします。

図 1：中小企業におけるセキュリティ対策状況



出典：NTT 東日本　Web 調査より（N=1,200 企業、2016 年 12 月）

図 2：中小企業におけるセキュリティ対策体制



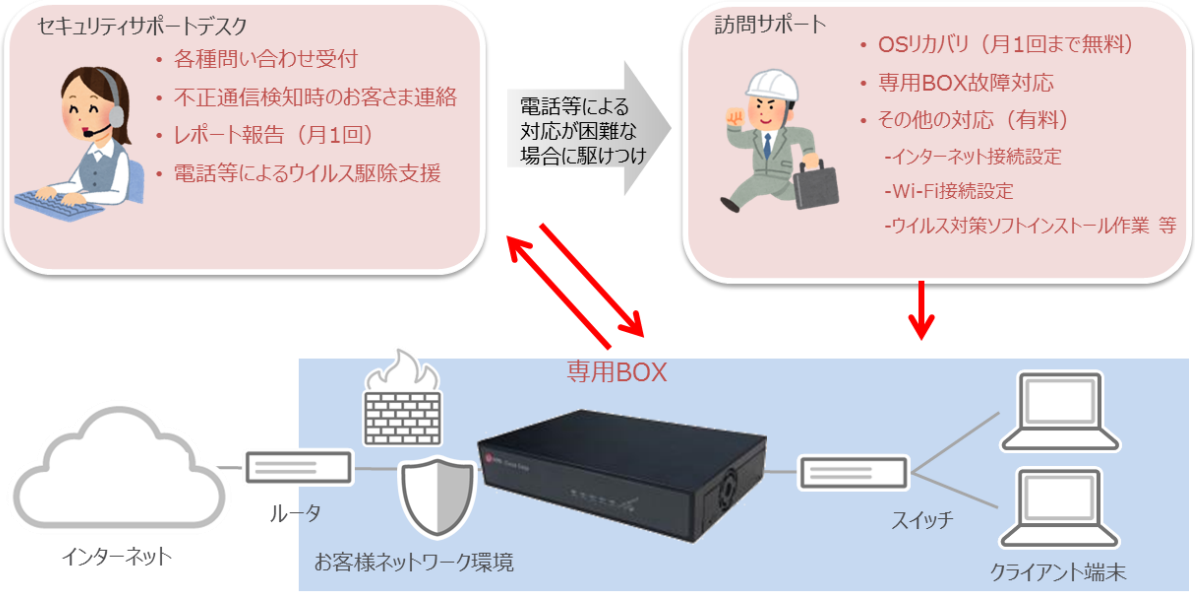
出典：NTT 東日本　Web 調査より（N=1,200 企業、2016 年 12 月）

2.「おまかせサイバーみまもり」について

(1)概要

「おまかせサイバーみまもり」は、お客さまのオフィス内に不正通信の検知・遮断機能を搭載した専用 BOX を設置することでネットワークセキュリティを強化するとともに、NTT 東日本のセキュリティサポートデスクがお客さまのネットワーク環境における通信状況を監視し、不正通信を検知した場合など、有事の際にはウイルスの駆除や端末復旧をサポートします。NTT 東日本がセキュリティ対策の運用にかかる業務をお引き受けするので、お客さまの業務の効率化や生産性向上、稼働削減につながります。

(2)提供イメージ



(3)特長

・専用 BOX ひとつで企業に求められる複数のセキュリティ対策が可能

専用 BOX を設置していただくことで、下記の機能をご利用いただくことができます。

機能	機能概要
不正アクセスブロック（不正プログラム対策/ Web サイトアクセスブロック）	不正な通信、プログラムによる攻撃を検知し、内部感染を早期に発見。不正 Web サイト、不正 URL へのアクセスを止めることにより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	設定により許可された通信のみを通過させ、さらにその中から悪意ある侵入や攻撃を検知し、遮断する機能。
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	アクセス許可されたカテゴリから特定のサイトのみをブロック可能とする機能。また、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	アプリケーションの利用制限を行う機能。

・不正通信発生時にお客さまへ通知し、ウイルス駆除や端末の復旧を支援

不正通信の発生を検知した際には、通信状況を監視している NTT 東日本のセキュリティサポートデスクからお客さまへご連絡し、電話等により原因究明を行った上で、ウイルス駆除や端末の復旧をサポートいたします。電話等による対応が困難な状況においては、訪問によるサポートも実施いたします。

・セキュリティ全般に対する問い合わせ対応

「ウイルス感染の疑いがある」、「怪しいメールを開封してしまった」、「有害な Web ページが画面に表示されてしまった」等のお客さまからのセキュリティに関するお問い合わせに NTT 東日本のセキュリティサポートデスクが対応します。

・レポートによる不正通信状況のモニタリング結果報告

脅威の侵入や不正サイトへのアクセスをブロックした状況を見える化したレポートを、月 1 回お客さま

へ提供します。視覚的に状況を把握することにより、必要なセキュリティ対策が明らかになります。

＊ セキュリティサポートデスクの電話によるご連絡・お問い合わせ受付時間は 9:00～21:00（年中無休）、メールによるご連絡・お問い合わせ受付時間は 24 時間 365 日です。

＊ 訪問サポートは専用 BOX の設置拠点に限り、電話等での対応が困難なパソコンの OS リカバリに無料で対応いたします。（月 1 回 Standard プラン：1 台、 Professional プラン 3 台まで）この他の訪問サポートメニューをご利用の場合は、別途実費料金が発生いたします。

3. 月額利用料等

推奨接続端末台数に応じて Standard プラン※1（推奨接続端末台数 50 台）、Professional プラン※1（推奨接続端末台数 100 台）をご用意しております。

※1 各プランに用いられる専用 BOX の主な機器仕様は別紙を参照願います。

・月額利用料(専用 BOX1 台あたり、税抜)

①基本サービス

Standard プラン：10,000 円

Professional プラン：17,000 円

②オプションサービス

24 時間訪問修理オプション：2,000 円

・初期費用(税抜)

基本工事費：4,500 円(1 工事あたり)

機器工事費：10,000 円(専用 BOX1 台あたり)

・最低利用期間

60 ヶ月※2

※2 最低利用期間の途中で解約された場合、残月数に応じた所定の解約金を一括でお支払いいただきます。
「Standard プラン」：残月数×2,500 円（税抜）、「Professional プラン」：残月数×3,000 円（税抜）

4.提供条件

提供エリアは東日本エリア※3 です。

ほか、おまかせサイバーみまもりの提供条件については下記 URL をご参照下さい。

URL：https://flets.com/cybermimamori/

※3 神奈川、山梨、長野、新潟以東の 17 都道県となります。

5.提供開始日

2017 年 6 月 29 日（木）

6.お申し込み・お問い合わせ先

お客さまを担当する弊社営業担当者へお申し込み・お問い合わせください。

【別紙】

＜主な機器仕様＞

仕様項目		Standard プラン	Professional プラン
推奨接続端末台数		50 台	100 台
スループット※		147Mbps	226Mbps
インターフェース		WAN ポート：1 LAN ポート：1 （1000Base-TX）	WAN ポート：1 LAN ポート：1 （1000Base-TX）
サイズ	外形寸法	幅：230mm 奥行：170mm 高さ：43mm	幅：232mm 奥行：153mm 高さ：44mm
	重量	1.2kg	1.4kg
冷却ファン		ファンレス仕様	あり
電源仕様	AC 電源	100-240V、1.5A、50/60Hz	100-240V、1.7A、50/60Hz
	消費電力	36W	60W

※ 実際のパフォーマンスは、ネットワーク状態と使用するサービスによって異なります。