News Release

2015 年 10 月 6 日

「Arcstar Universal One インターネット接続 セキュリティオプション（IWSaaS タイプ）」の提供開始について

～中堅・中小企業における情報漏洩対策をクラウド提供し、迅速かつ低コストに実現～

NTT コミュニケーションズ（略称：NTT Com）は、中堅・中小企業向けに、クラウド型インターネットセキュリティサービスとして、「Arcstar Universal One インターネット接続　セキュリティオプション（IWSaaS タイプ）」を、2015 年 10 月 6 日から提供開始します。

本サービスの提供により、お客さま企業の ICT 環境において、ウイルス感染後に情報流出を行う C&C サーバー[*1] との不正通信の検知・遮断が可能となり、標的型攻撃や不正アクセスなどのセキュリティリスクを大幅に低減します。

1．背景

昨今、従来のウイルス対策ソフトなどによるセキュリティ対策だけでは防ぎきれないサイバー攻撃の多様化やマイナンバー制度施行など、重要情報の漏洩に対する企業のセキュリティ対策強化の必然性が高まってきています。また、厳しい市場環境の中、特に中堅・中小企業において、IT コストの圧縮や運用負担の軽減なども大きな課題になっております。こうした中、NTT Com は、上記課題を解決するため、中堅・中小企業に最適なセキュリティ対策を、クラウド型インターネットセキュリティサービスとして提供を開始します。

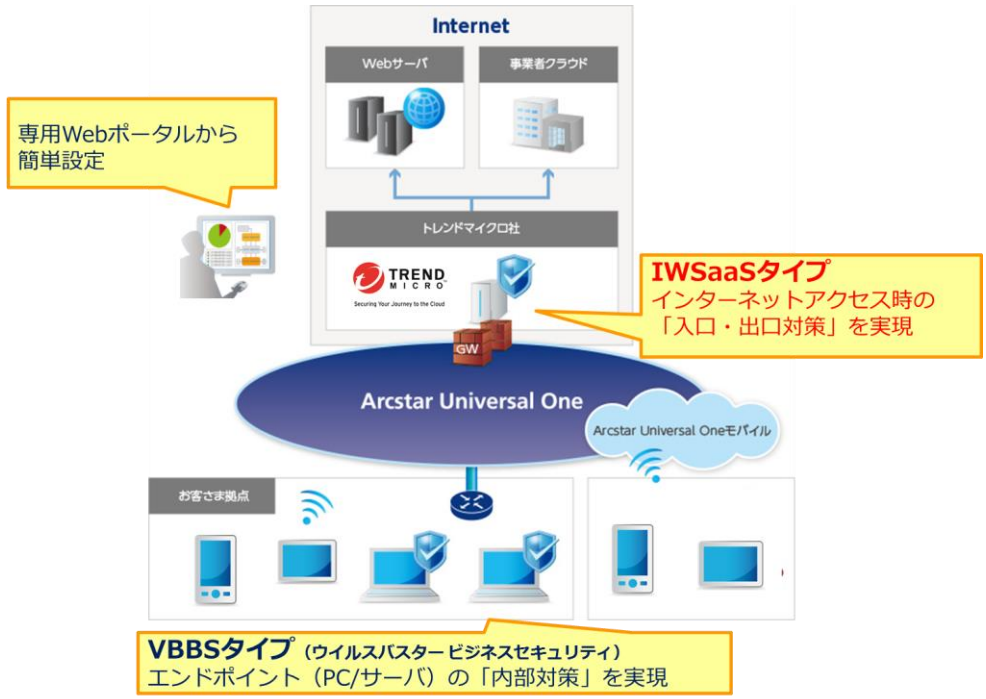
2. サービス概要（詳細は別紙１参照）

NTT Com の企業向け VPN サービス「Arcstar Universal One」と、トレンドマイクロの IWSaaS（InterScan Web Security as a Service）を活用し、ネットワークゲートウェイにおけるセキュリティ対策をクラウドサービスとして提供します。お客さまは、クラウド基盤上にあるセキュリティサーバーを経由して Web サイトへアクセスすることで、不正な Web サイトへのアクセス制限や不正プログラムのダウンロードを防ぐことが可能です。

また、本サービスの導入にあたり、お客さま拠点内の各 PC への新たなソフトウェアインストールは不要で、導入後のウイルスパターンファイルの最新化作業も不要となるため、迅速なセキュリティ対策導入、および導入後の運用負担軽減が可能です。

NTT コミュニケーションズ株式会社　広報室
NTT Communications Corporation　Public Relations Office
〒100-8019　東京都千代田区内幸町 1-1-6
1-1-6 Uchisaiwai-cho, Chiyoda-ku, Tokyo 100-8019, Japan
Tel (03)6700-4010 International +81 3 6700 4010

<サービス利用イメージ>



本サービスと、現在提供中の「インターネット接続機能 セキュリティオプション VBBS タイプ（ウイルスバスター ビジネスセキュリティ）」を組み合わせることにより、エンドポイント（PC やサーバー）からインターネットアクセスまで、トータルなセキュリティ対策強化が可能です。

3. 利用料金（税込）

・月額料金

区分 1	区分 2	単位	月額料金
インターネット接続利用料金	拠点型	1 拠点	3,240 円
	GW 型	1 VPN	54,000 円
	GW 型（帯域確保タイプ）	1 VPN 1 M 確保～	32,400 円～
セキュリティオプション利用料金 ※1	**IWSaaS タイプ**	**10ID～**	**4,320 円～**
	VBBS タイプ	50ID～ ※2	13,500 円～

※ 1 :ご利用開始月の月額料金は無料

※ 2 :2015 年 12 月より、10ID 単位での提供開始予定

・工事料金

区分	単位	工事料金
新規/廃止/変更（ID 数の変更等）	1 工事あたり	5 ,400 円

4. 提供開始日

2015 年 10 月 6 日（火）

5. 提供エリア

日本全国

*1：command and control server の略。外部環境から企業内システムへ侵入し、ウイルス感染などで乗っ取った PC を利用したサイバー攻撃において、乗っ取った PC などを外部から制御したり、命令を出したりする役割を担うサーバーのこと。

【お客さまからのお問い合わせ先】
法人コンタクトセンター
0120-106107
受付時間　9：30～17：00
（土・日・祝日除く）

（別紙 1）サービス内容

セキュリティ機能	対策	概要
ウイルス・スパイウェア対策	入口対策	不正プログラムの侵入をブロック。
Web レピュテーション	入口／出口対策	遠隔操作に使われる C&C サーバー、不正サイトへのリダイレクト通信やフィッシングサイトへのアクセスなど、危険性の高いアクセスを制御。
URL フィルタリング	入口／出口対策	企業運営上、アクセス不要なカテゴリの Web サイトへのアクセスをブロック。
ボット通信検知	出口対策	標的型攻撃などで発生するボット通信を検出し、通信を制御。
Web アプリケーション管理	情報漏洩対策	セキュリティポリシーに従い、アプリケーションによる不正通信や改ざんなどを制御。
マルチデバイス対応	―	Windows PC、Andoroid、iOS に対応。 （対応ブラウザ：IE、FireFox、Chrome、Safari）
レポート機能	―	アクセスログ、ウィルス検知ログや URL フィルタログなどをレポート提供。