ウォッチガード、安全な無線接続を実現するセキュアな無線アクセスポイントの新モデル「AP300」を発表

2016年1月19日（火）

ー企業向け統合化セキュリティプラットフォームのグローバルリーダであるWatchGuard（R）Technologiesの日本法人、ウォッチガード・テクノロジー・ジャパン株式会社（本社：東京都港区、社長執行役員
根岸正人、以下ウォッチガード）は、セキュアな無線アクセスを実現する新アクセスポイント「AP300」を発表しました。AP300は、ウォッチガードの実績豊富なUTM（統合脅威管理）アプライアンスのFireboxをコントローラとして連携させて利用し、最先端の無線アクセスとともに各種の高機能セキュリティサービスを提供することで、Wi-Fiネットワークの安全を確保します。AP300は、最新の802.11ac標準に対応し、VoIP端末との通信品質改善を可能にする「高速ローミング」、クライアントのAP間切り替え接続を低信号で迅速に処理する「高速ハンドオーバー」、またはクライアントが高品質の5GHz帯を利用できる「バンドステアリング」など、企業が抱える無線接続の課題を解決する新機能を備えています。

昨今、ビジネス、店舗、企業環境や公共スペースなど、あらゆる場所でWi-Fiが利用されるようになり、無線接続は増加傾向にあります。企業や団体ではお客様向けにゲストWi-Fiアクセスを提供するようになり、携帯電話、ノートPC、および各種デバイスから無線によるオンライン接続が可能になっています。しかしながら、爆発的に普及し始めている今日の無線接続にとって非常に重要な要素となる、セキュリティが見過ごされていることが多々あります。無線接続利用の増加は、同様に無差別または標的型の攻撃に対する脆弱性の拡大をも意味しています。

ウォッチガードのプロダクトマネジメント担当ディレクタであるRyan Orsi（ライアン・オルシ）は、次のように説明しています。「あらゆる業種の組織では、顧客、販売店、および従業員から無線アクセスの要望が高まっています。しかし、ハッカーもネットワークへの侵入の足掛かりを常に窺っているのも事実です。つまり組織にとって、特にWi-Fiネットワークの安全を守る必要性が出てきています。ゲスト用ホットスポットを含むWi-Fiネットワークの適正な安全を確保できない企業は、顧客、パートナー、社内ユーザをあらゆるリスクに晒すことになってしまいます。AP300は、最先端の無線LAN技術とベストインクラスのセキュリティ機能を併せて提供することで、Wi-Fiネットワーク経由の脅威から企業を守ることが可能になります。」

IT管理者は顧客に対して、高速で信頼性の高いセキュアな無線LANネットワークを提供する必要があります。

Quasar DataのCTO（チーフテクノロジオフィサー）であるCasey Jones（ケーシー・ジョーンズ）氏は、以下のようにコメントしています。「ウォッチガードの高機能ネットワークセキュリティ製品は、我々のビジネスに大いに貢献しています。同様に、セキュア無線LANもウォッチガードを活用しています。WatchGuard AP300の設定は非常に簡単で、オフィス並びにデータセンタで優れたカバレッジを実現しています。新たなローミング機能により、オフィスからデータセンタまでの移動においても、常時高速スピードで途切れることなくネットワーク接続を維持しています。」

無線ネットワークに対するセキュリティ脅威は以下のようなものが存在します：

・Wi-Fiパスワードクラッキング：
WEPなど旧式のセキュリティプロトコルを使用している無線LANアクセスポイントは、パスワードが容易に解読されるため、標的にされやすくなります。
・ローグホットスポット：
ホットスポットの近くのSSIDがマッチする外部アクセスポイントに顧客がログインした場合、サイバー犯罪を物理的に阻むものはありません。不正なアクセスポイントに接続したユーザは、知らないうちに悪意あるコードの影響を受けやすくなります。
・マルウェア侵入：
ゲスト無線ネットワークに繋がった顧客は知らないうちに悪意を持った近隣のユーザによりもたらされたマルウェアに感染している可能性があります。ハッカーによる一般的な攻撃手法は、ネットワークにバックドアを植え付け、後日機密データを詐取するというものがあります。
・盗聴：
保護されていない無線ネットワークに接続されたゲストは、サイバー犯罪者により私的会話を盗聴またはパケットを傍受されるリスクがあります。
・情報漏えい：
無線ネットワークに接続する場合、盗聴しているサイバー犯罪者にデータを傍受され、ユーザの私的文書が詐取されるリスクがあります。
・不適切かつ不法な利用：
ゲスト用無線LANアクセスを提供する企業は、広範な不法および潜在的に有害なコミュニケーションを手助けするリスクを負うことになります。アダルトまたは過激なコンテンツは近隣者に不快感を与え、不法なダウンロードは法的訴訟に発展する可能性があります。
・感染端末の接続：
ネットワークでの無線ユーザの数が増加するにつれ、感染デバイスがネットワークに接続されるリスクも増えてきます。AndroidのStagefrightなどのMMS経由での攻撃が、知らない間にゲストの間で感染拡大する可能性があります。

ウォッチガードはこうした脅威からユーザを保護し、ウイルス対策（AV）、不正侵入検知・防御（IPS）、WebBlocker、spamBlocker、アプリケーション制御、レピュテーションセキュリティ（RED）、APT
Blocker、および情報漏えい対策（DLP）など、ウォッチガードのファイアウォールで機能するすべてのセキュリティサービスを駆使して無線LANネットワーク上のトラフィックを検査します。各サービスはすべて一元コンソールで管理され、接続スピードやスループットを犠牲にせずに利用することができます。

販売開始日： 2016年1月19日
出荷開始日： 2016年2月19日
製品価格（参考価格）： 166,500円（税別）より（初年度メーカー保守込み）/1台当たり
※ 電源アダプターはオプションとなっています。

（ウォッチガード・テクノロジー・ジャパン株式会社 社長執行役員 根岸正人）
「現行のAP200のパフォーマンスを向上し、さらに802.11ac対応、802.11r/kのファーストローミング機能に対応したWatchGuard
AP300を、急激に拡大する無線LAN環境のセキュリティ対策として統合セキュリティアプライアンスと連携した安全な無線LAN環境の構築にご活用頂きたいと思います。当社のFireboxと合わせて使用することで、導入コストを節約しつつ、先進のセキュリティ機能と統合することで、安全な高速無線LAN接続をビジネスにご利用頂くことが可能になります。」

【WatchGuard Technologiesについて】
WatchGuard (R)
Technologiesは、業界標準ハードウェア、ベストオブブリードセキュリティ、ポリシーベースの管理ツールを独自アーキテクチャにより統合したビジネスセキュリティソリューションを提供するグローバルリーダとして、全世界の企業にエンタープライズクラスのセキュリティソリューションを提供しています。本社を米国ワシントン州シアトルに置き、北米、ヨーロッパ、アジアパシフィック、ラテンアメリカに支社を展開しています。日本法人であるウォッチガード・テクノロジー・ジャパン株式会社は、多くのパートナーを通じて、アプライアンス製品、セキュリティの「可視化」、セキュリティとネットワークの「管理」など拡大するニーズへのソリューションを提供しています。詳細は http://www.watchguard.co.jp をご覧下さい。

その他追加情報、プロモーション活動、アップデートは以下のSMSにアクセスしてください。
Facebook： https://www.facebook.com/watchguard.jp
LinkedIn： www.linkedin.com/company/watchguard-technologies

WatchGuardは、WatchGuard Technologies,
Inc.の登録商標です。その他の商標は各社に帰属します。

【本プレスリリースに関するお問合せ】
ウォッチガード・テクノロジー・ジャパン株式会社
〒106-0041
東京都港区麻布台1-11-9 CR神谷町ビル5階
マーケティング担当：堀江
Tel： 03-5797-7205
Fax： 03-5797-7207
Email： jpnsales@watchguard.com
URL： http://www.watchguard.co.jp

Generated by ぷれりりプレスリリース
https://www.prerele.com