2019 年 12 月 23 日
株式会社スプライン・ネットワーク

Wi-Fi 環境の整備・セキュリティに特化した先進システムを、サービスとして提供
新ソリューション「Wi-Fi Security Assurance Series」（略称：WiSAS）
― 脅威を自動検出・遮断／監視レポートを自動出力 ―

Wi-Fi ネットワークセキュリティの株式会社スプライン・ネットワーク（本社：東京都渋谷区、代表取締役社長：雪野洋一）は、セキュアで快適な Wi-Fi 環境をサービスで提供する Wi-Fi セキュリティソリューション「Wi-Fi Security Assurance Series」（略称 WiSAS…ワイサス、Wi-Fi セキュリティアシュアランス シリーズ）を開発し、2020 年 1 月 14 日から提供を開始します。

WiSAS は、Wi-Fi セキュリティ専用センサー「WiSAS センサー」と、「WiSAS クラウドマネージャー」の 2 つのコンポーネントで構成される「WiSAS システム」をベースに、調査、データ分析、診断、アラート、報告、監視のシステムを独自に開発構築してサービス製品としたもので、3 タイプのアセスメントサービスと、2 タイプの常時監視サービスの合計 5 つのサービスで構成されています。本製品は、Wi-Fi セキュリティに詳しい人材が不足している日本の多くの企業に向けて、Wi-Fi 環境を快適に使用するための可視化や最適化支援、および不正利用やサイバー攻撃による情報漏洩を防止する機能をサービスとして提供します。

高性能な Wi-Fi スキャニング機能を有する WiSAS センサーは初期セットアップが不要。対象エリアに設置し電源を入れるだけで、エリア内の Wi-Fi をスキャンして常時監視を開始します。ポリシーや分析内容は WiSAS クラウドマネージャー側で設定。非認可の不正アクセスポイント（AP）や不正デバイスを検知した際には、自動で判断し、直ちに当該接続を遮断し、Wi-Fi 環境の脅威を排除します。

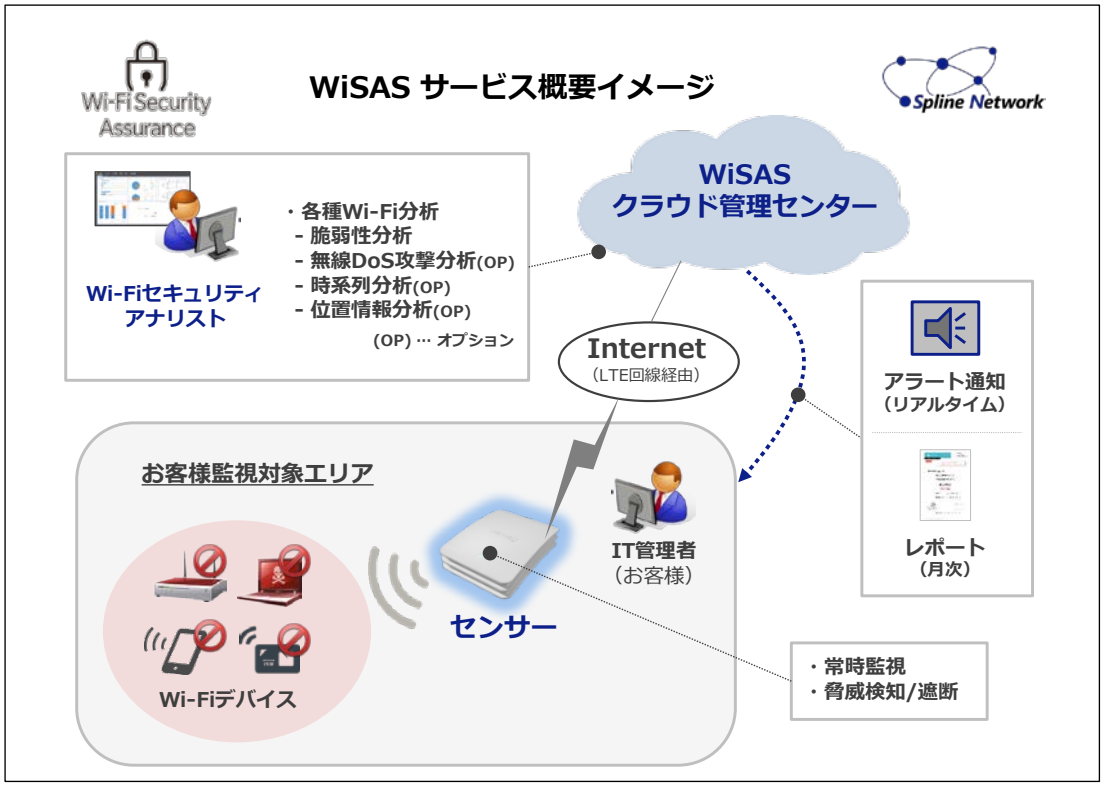

Wi-Fi セキュリティ専用センサー
「WiSAS センサー」

本センサーは、WiSAS の専用センサーであり、過去実用に耐えなかった無線 AP 組込型センサーとは異なり、厳密なスキャン性能と高速な遮断対応により、WIDS（＝Wireless Intrusion Detection System、無線侵入検知システム）と WIPS（＝Wireless Intrusion Prevention Systems、無線侵入防止システム）を実行します。

本センサーによりデータは暗号化され、NTT ドコモの LTE 回線経由でマネージャーに伝送されます。LTE 回線利用により独立したアドオンシステムとしての導入が可能で、専用 SIM カードがセット提供されるのでマネージャーとの連繋における通信品質の安定が確保されます。監視エリアでの作業はセンサーの設置のみであり、既存システムを変更することなく導入でき、運用から監視、報告書作成まですべてクラウド型サービスで提供するため、新たな管理者リソースを必要としません。

WiSAS クラウドマネージャーはユーザー毎のポリシーを管理。WiSAS センサーが収集したデータを可視化し、管理項目毎に各 WiSAS 分析サーバーに振り分けます。インシデント発生時には WiSAS アラートサーバーと連携し、隙のない監視体制を維持します。機能はすべてクラウドサービスとして提供されるため、ユーザー企業は社内リソースに負荷をかけることなく、Wi-Fi 環境の最適化とセキュリティ監視が可能になります。

監視分析レポートの充実も本サービスの特長であり、AP や接続端末の一覧はもとより、非認可や不正な端末、なりすましや MAC 偽装、不正接続 AP 等の監視、Wi-Fi 環境の時系列分析等々、セキュアで最適化された Wi-Fi 環境の確保に必要な情報を網羅しています。



■Wi-Fi Security Assurance Series（WiSAS）サービス構成

WiSAS は、以下のとおり、1）「WiSAS 環境スキャンサービス」、2）「WiSAS 最適化支援サービス」、3）「WiSAS セキュリティ脆弱性診断サービス」のワンショットで提供する 3 つのセキュリティ・アセスメントサービスと、4）「WiSAS セキュリティ 24H365D」、5）「PCI DSS 要件 11.1 WiSAS マネージドセキュリティ」の 2 つの常時監視セキュリティサービスとで構成されています。

■セキュリティ・アセスメントサービス　（以下 1,2,3）

●1. WiSAS 環境スキャンサービス

無線ネットワーク(Wi-Fi)の電波をスキャンし可視化することで、電波状況を正確に把握し、Wi-Fi の適切な運用管理に活用することが可能です。

【Wi-Fi ネットワーク利用状況の可視化】

1）無線 AP(含:ステルス）と端末 MAC アドレス、及び信号強度(dBm)
2）無線 AP が使用している無線プロトコル、電波チャンネル、認証／暗号化方式
3）端末が接続している AP/SSID 情報
→スキャン実施から 3 営業日程度で結果報告書を提出

●2. WiSAS 最適化支援サービス

無線ネットワーク（Wi-Fi）の電波を一定間隔で取得し、時系列で分析することで、無線 LAN の非効率な利用や AP の異常な振る舞い、あるいは Wi-Fi 環境の突発的な変化を明確にし、Wi-Fi 環境の最適化を支援します。(時系列データ取得は 30 分毎／12 時間／24 回が基本、結果はグラフ化されます)

【Wi-Fi ネットワーク利用状況の可視化】【電波品質の可視化と時系列分析】

1）AP 別接続台数推移　・・・・・　AP への接続の偏りを可視化／分析
2）AP 別電波強度推移　・・・・・　AP の電波干渉／不安定動作を可視化／分析

3）SSID 別接続台数推移　・・・・　SSID 単位の接続台数の急激な増減を確認
4）アクティブ AP 数推移　・・・・　AP 数の急激な増減を確認
5）チャンネル別 AP 数推移　・・・　電波の混雑状況を確認
※上記 5 つの要素をスプライン・ネットワークの Wi-Fi データアナリストが分析します。
→スキャン実施から 5 営業日程度で結果報告書を提出致します。

●3. WiSAS セキュリティ脆弱性診断サービス

無線ネットワーク（Wi-Fi）の電波を取得し、セキュリティの観点から分析することで、Wi-Fi 環境に潜む脆弱性や問題点を可視化し、脅威を未然に防ぎます。

【Wi-Fi ネットワーク利用状況の可視化】
※周囲の AP、端末の詳細情報を可視化し、レポーティングします。
【Wi-Fi ネットワークセキュリティ脅威の分析】
※不正アクセスや偽装 AP、ハッキングデバイス等を探知し、潜在的な脅威を分析レポーティングします。

＜セキュリティ対策オプション＞
以上のセキュリティ・アセスメントサービスでは、電波状況を可視化したり、さまざまな Wi-Fi に関する脅威を見つけたりすることはできますが、脅威の排除や改善はできません。そのため、不正アクセスポイントの位置情報検知や無線 DoS 攻撃分析等、いくつかの対策オプションを用意しています。
（位置情報検知には、センサー3 台以上の設置が必要です。）
→スキャン実施から 5 営業日程度で結果報告書を提出致します。

■常時監視セキュリティサービス　（以下 4,5）

●4. WiSAS セキュリティ 24H365D　★サブスクリプション・モデル

無線ネットワーク(Wi-Fi）環境を 24 時間 365 日常時監視し、さまざまな観点からセキュリティ脅威の存在を自動検知し、自動遮断することで企業の重要なデータを守ることが可能です。また Wi-Fi 通信状況だけを取得し、社内のデータそのものは取得しないので安全です。

【Wi-Fi 利用状況を 24 時間 365 日、常時監視】【Wi-Fi 不正利用を自動で即座に検知・遮断】
主な特徴：WIDS／WIPS 機能／アラート通知／ログ管理／対策自動化／位置情報検知(OP)
【ポイント】
1）手間いらずの導入
・既存システムの変更無しに、センサーを設置するだけで簡単に導入が可能です。
・取得ログは暗号化され、LTE 回線で WiSAS クラウドマネージャーに転送されます。
2）運用が簡単：レポートの自動化
・Wi-Fi 監視レポートは 1 ヶ月毎に生成され、ユーザー専用のアーカイブサーバーに保存されます。
・Raw データも、共に保管されるので、様々な分析・追跡に使用可能です。
3）緊急時にはアラート／遮断
・不正 AP や不正アクセス検知時にはアラートが出され、遮断します。
（クラウドマネージャーで、予め設定が必要となります）

●5. PCI DSS 要件 11.1 WiSAS マネージドセキリティ　★サブスクリプション・モデル

本サービスは、前項 4「WiSAS セキュリティ 24H365D」を PCI DSS 要件 11.1 の基準に対応させた常時監視ソリューションです。基本的なサービス内容は、24H365D と同じですが、以下の点で異なります。
1）PCI DSS 要件 11.1 に対応した分析報告内容になるため、監視報告項目が多岐にわたります。
2）PCI DSS 要件 11.1 に対応した監視レポートが毎月自動生成され、アーカイブされます。

【PCI DSS 要件 11.1 対応の背景】
PCI DSS（Payment Card Industry Data Security Standard）は、クレジットカードデータを安全に取り扱うための国際的な業界セキュリティ基準であり、特に要件 11.1 では、Wi-Fi 環境のセキュリティ確保が

定められています。日本でも 2018 年改正割賦販売法で PCI DSS 対応が義務化され、カード情報保護が法制度化されています。

PCI DSS 要件 11.1 では、特に無許可の無線 AP の接続を重大なインシデントの一つとして扱っています。PCIDSS 対象企業の多くが四半期毎の定期検査で済ませていますが、本来は常時監視（無線 IDS/IPS の導入）が望ましいとしています。この対策対応は無線ネットワークの使用の有無にかかわらず必要とされていますが、これまで無線ネットワークの常時監視ができる実用的な無線 IDS/IPS はありませんでした。

WiSAS では、接続情報を常時監視して、無許可の無線アクセスポイントからの通信を検知し、即時遮断します。また監視データを取得することで、PCI DSS 準拠のためのレポートを自動で出力することが可能です。

■販売・展開戦略

価格は、各サービスともにオープン。目安として、ワンショットのスキャンサービスは、最小構成で 7 万円（消費税抜き）程度、診断サービスは 30 万円（同）程度。常時監視サービスは、初期費用 100 万円（同）、月額 10 万円（同）程度としています。いずれも取得するデータ、分析項目、設置規模等によって変わります。

スプライン・ネットワークでは、本ソリューションの導入先として、当面は金融系企業のほか、一般企業、官公庁、独立行政法人、研究機関、製造業、BPO 事業者などを想定しています。販売は、株式会社アイネット、株式会社インフォメーション・ディベロプメント、TIS 株式会社、TIS ソリューションリンク株式会社など、販売パートナー各社を通じて行います。販売提携先は今後も増やしていく方針です。

スプライン・ネットワークは、本事業の垂直立ち上げを目指しており、初年度常時監視サービス契約先を 30 社、事業売上 1 億円を目指し、3 年後に初年度比 5 倍規模の成長達成を目標としています。本事業を通して日本の WiFi 環境のセキュリティ向上の一助となるべく、力を尽くして取り組んでいきます。

以上

■本件報道発表について

Wi-Fi セキュリティアシュアランスシリーズは 2019 年 6 月 10 日付プレスリリースで同月より提供開始と報道発表しましたが、直後に方針を転換しました。同名サービスの販売を一旦取り下げた上で大規模な改良を施し、大幅なラインアップ拡充を行ってから正式に販売に移ることとし開発を継続。並行して各社での実環境への試験導入、先行導入も進め、知見の蓄積を図りました。システムの作り込みと改良を重ねた上で今般正式に製品をリリースするに至り、報道発表を実施します。

■株式会社スプライン・ネットワークについて

2002 年 1 月設立。セキュリティやプリンティングの領域において、様々なソフトウェアソリューションを自社で手掛け、開発からマーケティング、販売、サポートまで一貫したビジネスを展開。目的に即したトナー濃度により印刷コストを最大 75%削減する「TonerSaver」、インタラクティブな MTG を実現する「SmartClick」、情報漏えいから企業を守る印刷イメージログ監視システム「PrintInsight」など、独自の視点で生みだしたユニークなソリューション群は、導入企業から高い評価を得ています。

2017 年より、脆弱性が放置されている WiFi 通信ネットワークが多数散在する状況を前に、Wi-Fi ネットワークを可視化し、Wi-Fi 環境の最適化を支援、Wi-Fi 不正利用を防止し、サイバー攻撃による情報漏洩を防止するソリューション「Wi-Fi セキュリティ アシュアランス シリーズ」（WiSAS）の開発に着手。この立ち上げと普及促進に注力特化するため、2019 年 8 月、従来事業をパートナー会社に移管しました。今後は、快適でセキュアな Wi-Fi 環境の普及拡大の支援に集中して事業展開を行っていきます。

■お問い合わせ先■
株式会社スプライン・ネットワーク　WiSAS 事業部（ワイサス事業部）
e-mail：wifi-sa@spline-network.co.jp ／ Tel：03-5464-5468