必見！PCI DSS要件11.1の実効性を担保するWi-Fi監視ソリューション

1部/ｆｊコンサルティング株式会社　代表取締役CEO　瀬田 陽介

2部/株式会社スプライン・ネットワーク　代表取締役社長　雪野 洋一

2019年6月11日
PCI DSSセキュリティフォーラム2019 講演資料

2019/6/11
PCI DSSセキュリティフォーラム2019 講演資料

fjconsulting, INC.

必見！PCI DSS要件11.1の実効性を担保する Wi-Fi監視ソリューション

ｆ ｊコンサルティング株式会社
2019年6月11日

アジェンダ

1．自己紹介

2．PCI DSSと無線アクセスポイント検査

3．無線IDS/IPSによる監視

4．PCI DSSへの適用事例

会社概要

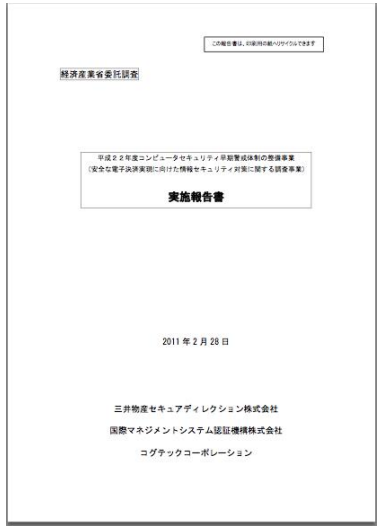
- 会社名　　ｆ ｊコンサルティング株式会社
  ｆ ｊの由来は”From Japan”
- 役員　　代表取締役CEO　瀬田　陽介
  取締役COO　　大澤　志津
  非常勤取締役　　須田　騎一朗
  （ユナイトアンドグロウ株式会社 代表取締役社長）
  非常勤取締役　　谷口　芳伸
  （ユナイトアンドグロウ株式会社 執行役員）
  監査役　　肥後　一雄
  （ユナイトアンドグロウ株式会社 常勤監査役）
- 顧問弁護士　　大井　哲也
  （TMI総合法律事務所 弁護士）
- 本社　　〒101-0062
  東京都千代田区神田駿河台4-3
  新お茶の水ビルディング3F
- 加盟団体　　日本カード情報セキュリティ協議会
  一般社団法人キャッシュレス推進協議会
  一般財団法人沖縄ITイノベーション戦略センター

代表者紹介

- 氏名　瀬田　陽介（1972年3月23日生）
- 経歴
  - 1999年11月～2007年9月
    インフォリスクマネージ(株)ボードメンバー
  - 2007年4月～2013年1月
    国際マネジメントシステム認証機構(株)代表取締役社長
  - 2010年8月～2013年2月
    Payment Card Forensics(株)取締役（現・P・F・C・Fronteo(株)）
  - 2009年11月～2013年3月
    エヌシーアイ(株) ボードメンバー　（現・アイティーエム(株)）
  - 2013年4月～
    fjコンサルティング(株)　代表取締役CEO(現任)
  - 2014年7月～
    (株) GRCS　（旧：NANAROQ (株)）　アドバイザー(現任)
  - 2015年11月～
    BSI Professional Services Japan テクニカルアドバイザー(現任)
  - 2016年8月～
    日本カード情報セキュリティ協議会（JCDSC）　ユーザー部会世話役(現任)

執筆①

- 改正割賦販売法でカード決済はこう変わる　（共著）
  日経BP社　2018年4月発行　　2,000円（税別）
- PCI DSS Version2.0 徹底解説
  CardWave編集部　2011年9月発行　　50,000円(税別)
- PCI DSS Version1.2 徹底解説
  TIプランニング　2010年2月発行　　90,000円(税別)
- 経済産業省委託調査『平成22年度コンピュータセキュリティ早期警戒体制の整備事業
  安全な電子決済実現に向けた情報セキュリティ対策に関する調査事業』



執筆②

- CardWave 2015年11・12月号　Special Report
  『POSマルウェア攻撃に備えるPCI P2PEとは POS加盟店のPCI DSS準拠を現実的なものに』
- CardWave 2016年3・4月号　特集　カード情報を守れ！非対面決済編
  『官民共同案のセキュリティ対策でECにおけるカード決済はどう変わる？』
- CardWave 2016年9・10月号　Special Report
  『ATM18億円不正引き出し事件を検証　銀行の国際ネットワーク対応に影響？』
- CardWave 2017年3・4月号　特集　クレジットカードのセキュリティ考察
  『セキュリティの指針「実行計画2017』のポイント
  改正割賦販売法対応に向けた加盟店の取り組みが焦点に』
- CardWave 2017年9・10月号～2018年5・6月号　PR特集　銀聯カードを理解する
  『「銀聯＝中国のデビットカード」という誤解』 他　（5回連載）
- CardWave 2018年3・4月号　Special Report
  『カード決済セキュリティの指標「実行計画2018」 MOTO加盟店の非保持化・不正使用対策も明確に』
- CardWave 2018年5・6月号　Special Report
  『カード決済セキュリティの指標「実行計画2018」 内回り方式の選択肢が増えたPOS加盟店』
- CardWave 2018年9・10月号　Special Report
  『キャッシュレス推進協議会が目指す「QR コード決済標準化」を読み解く
- CardWave 2019年3・4月号　Special Report
  『「実行計画2019」変更ポイントを解説　EC加盟店に求められる新たな不正対策』

アジェンダ

1．自己紹介

2．PCI DSSと無線アクセスポイント検査

3．無線IDS/IPSによる監視

4．PCI DSSへの適用事例

PCI DSS 要件11.1

要件11.1
四半期ごとにワイヤレスアクセスポイントの存在をテストし（802.11）、すべての承認されているワイヤレスアクセスポイントと承認されていないワイヤレスアクセスポイントを検出し識別するプロセスを実施する。

- 検出対象には少なくとも以下を含む。
  - サーバーのネットワークポートとUSBポート
  - ネットワーク機器のネットワークポートとUSBポート
  - ネットワークポートまたはネットワークデバイスに接続されたワイヤレスデバイス
- 承認されていない無線アクセスポイント（無線AP）が検出された場合は、インシデント対応計画を発動（要件11.1.2／要件12.10）
- 無線なしのネットワークでも実施する必要がある。
- 全てのPCI DSS対象範囲の拠点が対象となる。

従来の無線AP検査の方法①

要件11.1（続き）
注）プロセスで使用される方法には、ワイヤレスネットワークのスキャン、システムコンポーネントおよびインフラストラクチャの論理的/物理的な検査、ネットワークアクセス制御（NAC）、無線 IDS/IPS が含まれるがこれらに限定されるわけではない。

現在の実施手法は以下のいずれかであることが多い。

1. 無線（ワイヤレス）ネットワークのスキャン
2. システムコンポーネントおよびインフラストラクチャの論理的/物理的な検査

従来の無線AP検査の方法②

１．無線ネットワークのスキャン

- PCI DSS対象範囲の拠点をウォークスルーして無線ネットワークスキャンを実施
- 未知の無線APを発見した場合、バックボーンネットワークスイッチを調査し、ネットワーク接続の有無を調査
- PCI DSS対象範囲内のネットワークに無許可の無線APが接続されていたらインシデント対応計画を発動

【問題点】

① スマートフォンのWi-Fiを無線APとして検出してしまう。

② 悪意ある攻撃者がMACアドレスやSSIDを偽装することは容易

③ 検査に人手がかかるが、有効性に疑問

④ 人手がかかるため、実施頻度を上げることが難しい。

⑤ 四半期ごとの検査の間の期間に接続された場合、発見できない。

従来の無線AP検査の方法③

fjconsulting, INC.

2. システムコンポーネントおよびインフラストラクチャの物理検査

- 全てのネットワーク機器のポートやサーバのUSBポートに無許可の無線APが接続されていないことを目視確認
- スマートフォンのWi-Fi等により、無線ネットワークに影響を受けやすいオフィス環境では、効率的で安定した手法なので多くの組織で実施されている。

【問題点】

① サーバ数が多かったり、ネットワーク機器数（ポート数）が多かったりするシステムには不向き

② 対象範囲内でスマートフォンのテザリングやモバイルWi-Fiルータなど、ネットワークに有線接続されていない無線APを発見できない。

③ 人手がかかるため、実施頻度を上げることが難しい。

④ 四半期ごとの検査の間の期間に無許可の無線APが接続された場合、発見できない。

PCI DSS要件11.1対応の現状の課題

fjconsulting, INC.

- 従来の方法は手間や人手がかかるのに、有効性が不十分

- 「無許可の無線AP」は発見次第インシデント対応計画が発動されるほどの重大インシデントであり、本来は四半期に一度の検査ではなく24時間/365日の監視が望ましい。

- PCI DSS要件11.1では、プロセスで使用される方法の例として「無線IDS/IPSの導入」を挙げているが、これまで有効な方法がなかった。

アジェンダ

1．自己紹介

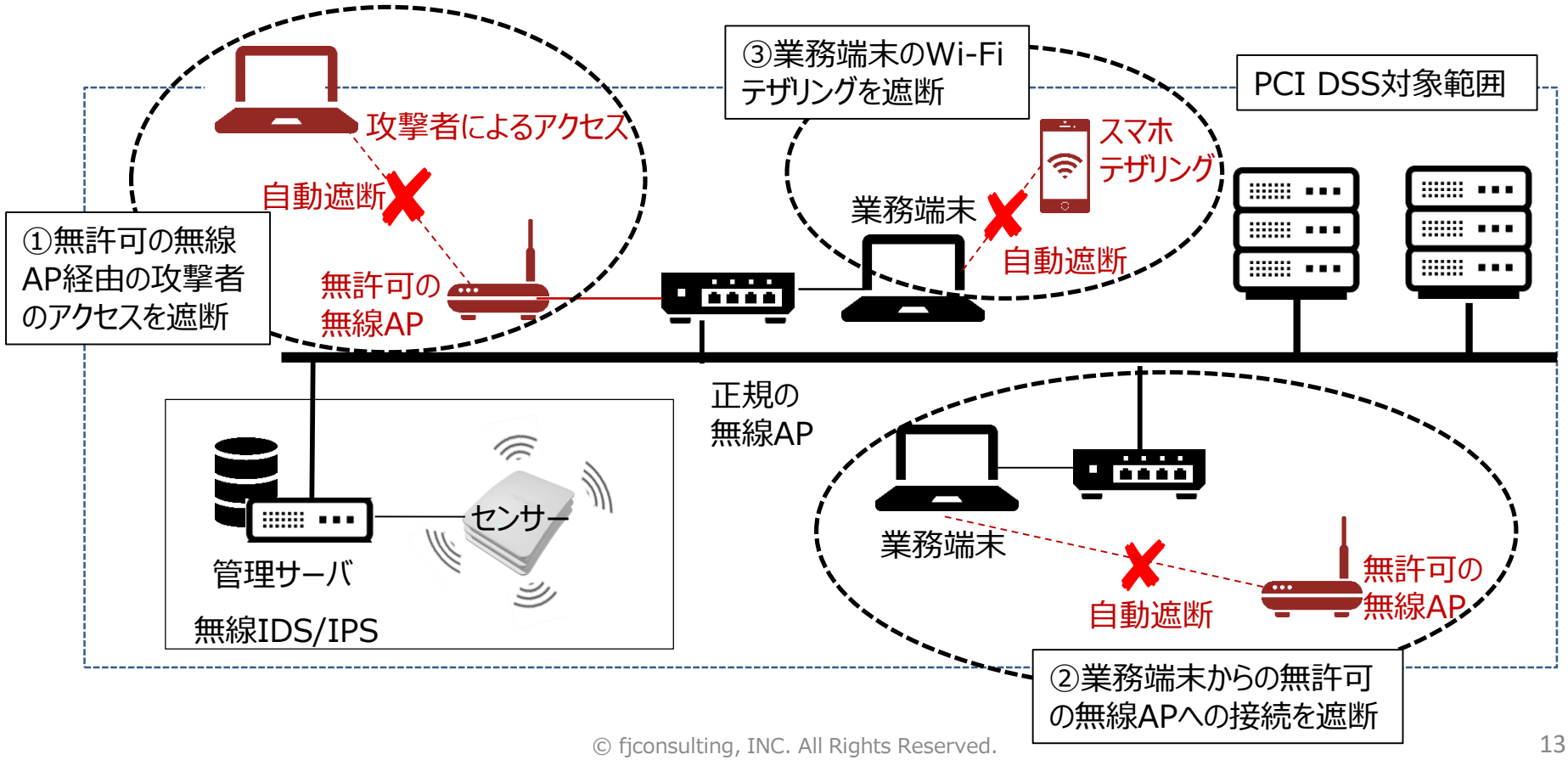
2．PCI DSSと無線アクセスポイント検査

3．無線IDS/IPSによる監視

4．PCI DSSへの適用事例

無線IDS/IPSでできること

- 無線ネットワークを24時間/365日監視
- 無許可の無線AP（SSID/MACアドレス）を検知して即時遮断
- 偽装したMACアドレスやSSIDについても検知可能



アジェンダ

1．自己紹介

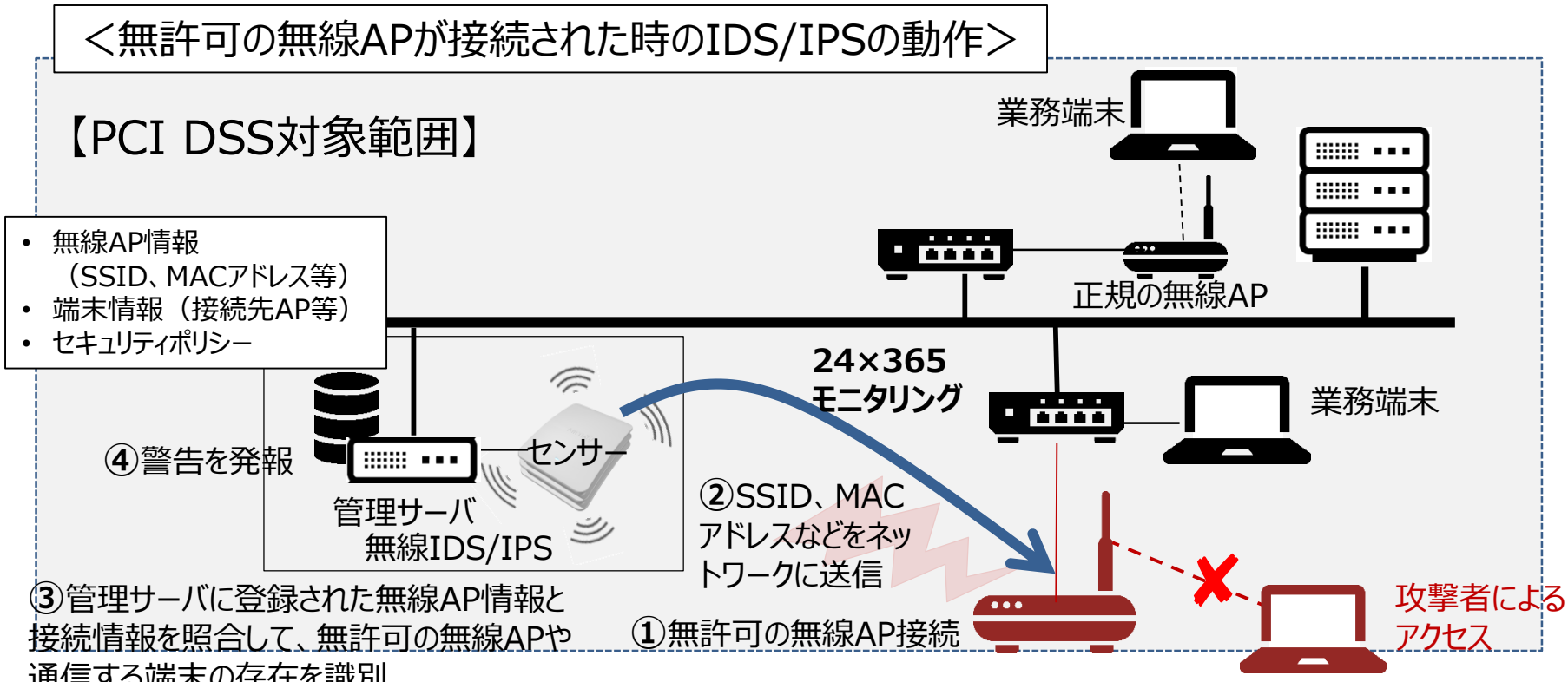
2．PCI DSSと無線アクセスポイント検査

3．無線IDS/IPSによる監視

4．PCI DSSへの適用事例

PCI DSS対象範囲における無線IDS/IPSの事例

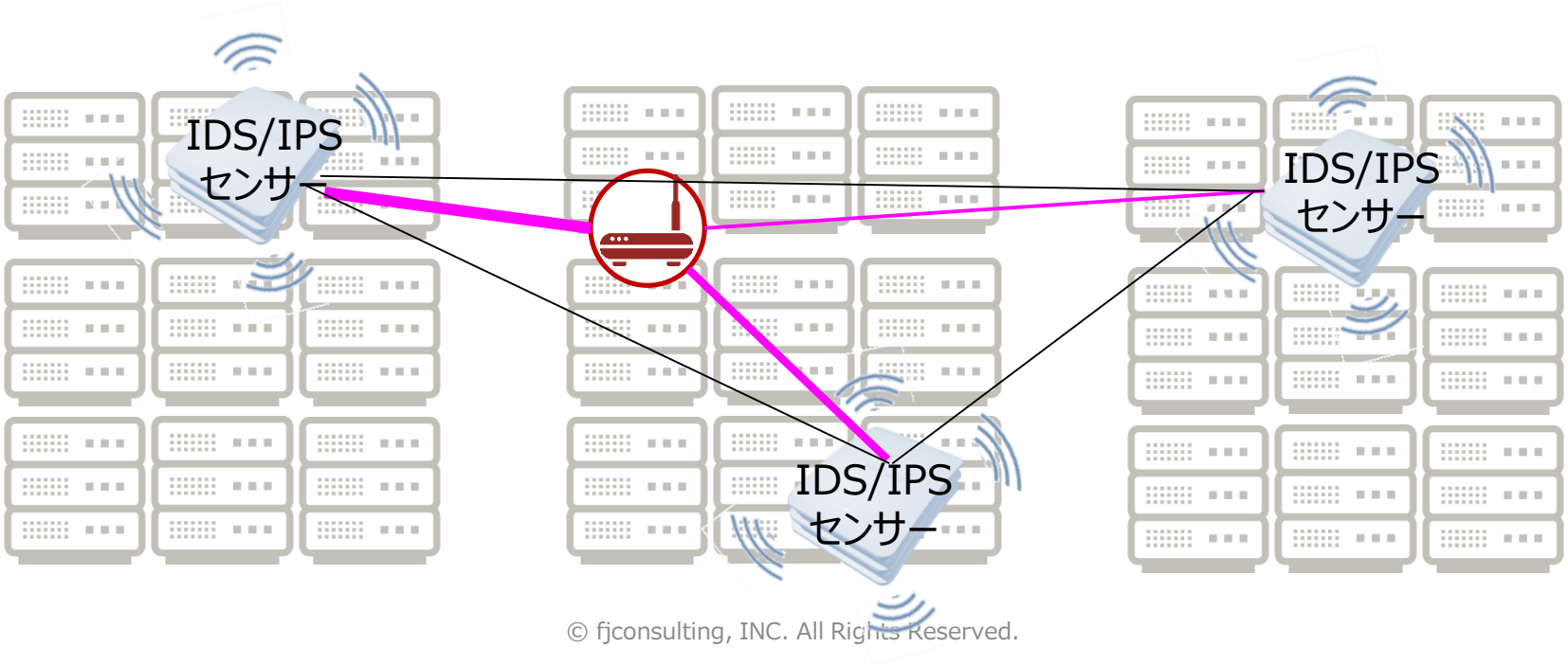
- PCI DSS対象範囲内にある無線AP情報（SSID、MACアドレス）および端末情報（MACアドレス）をあらかじめIDS/IPSの管理サーバにホワイトリストとして登録
- 端末ごとの許可された接続先などのセキュリティポリシーも同様に登録
- PCI DSS対象範囲内に設置したセンサーで常時範囲内の無線AP情報・端末情報を受信し、それぞれの接続状態をを無線IDS/IPS管理サーバに送信



データセンタにおける無許可の無線APの検知

- 多数のサーバラックがあるマシンルーム内で物理検査により無線APを探すのは困難
- スキャンしても場所の特定が困難でウォークスルーの有効性が低下

- 無線IDS/IPSセンサーの電波受信強度を元に無線APまでの距離を推定できる。
- センサー3台を使い三点測位を利用してアクセスポイントの位置を特定する。



まとめ

- 無許可の無線APはPCI DSSにおいて重大なセキュリティインシデントにつながる。
- スマートフォンの普及によりオフィス環境での無線スキャンは困難に
- 無線IDS/IPSにより、人手・手間をかけず無許可の無線APの常時監視が可能になる。

ご質問＆お問い合わせなど

Email： admin@fjconsulting.jp

http://www.fjconsulting.jp/

TEL:03-4570-8580

Facebook :
facebook.com/fjconsultinginc

Wi-Fi Security Assurance

Spline Network

Wi-Fi Security Assurance

~ 無線LAN IDS/IPSサービス ~

Wi-Fiセキュリティ脆弱性診断

Wi-Fiマネージドセキュリティ

PCI DSSセキュリティフォーラム2019 講演資料

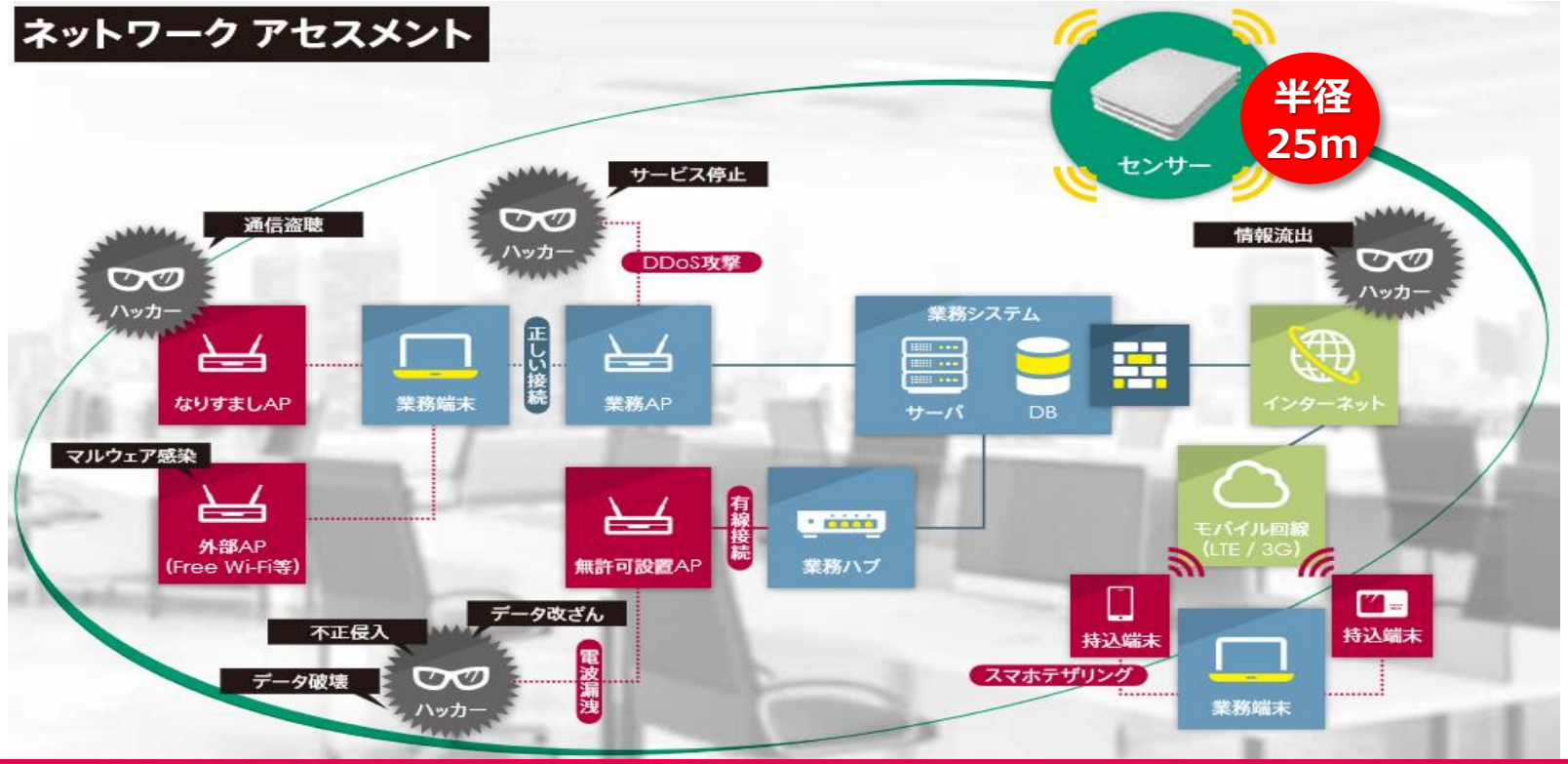
2019年6月11日

株式会社スプライン・ネットワーク

CONFIDENTIAL

Spline Network

Wi-Fi 環境（アクセスポイント/端末）の可視化＆分析ソリューション



Wi-Fiネットワーク状況の可視化

周囲アクセスポイント
及び端末の詳細情報をレポート

Wi-Fiネットワーク セキュリティ脅威のの明確化

不正アクセス端末の検知、
偽装アクセスポイント等の
可視化＆シグネチャ分析

Wi-Fiネットワーク 環境（電波皮質）の最適化

電波干渉、電波の不感知、
微弱電波状況の調査と最適化

Spline Network

Wi-Fi 環境（アクセスポイント/端末）の可視化&分析ソリューション

Wi-Fiネットワーク状況の可視化

周囲アクセスポイント
及び端末の詳細情報をレポート

Wi-Fiネットワーク セキュリティ脅威の明確化

不正アクセス端末の検知、
偽装アクセスポイント等の
可視化&シグネチャ分析

Wi-Fiネットワーク 環境（電波品質）の最適化

電波干渉、電波の不感知、
微弱電波状況の調査と最適化

調査・報告

Wi-Fiのアクセスポイント及び、端末を調査し報告

Wi-Fiで通信を行う機器が対象：PC、スマートフォン、ポータブルWi-Fi、プリンター など

取得項目

- ■アクセスポイント及び端末のSSID
- ■MAC Address
- ■接続先アクセスポイント
- ■認証方式
- ■暗号化方式
- ■プロトコル
- ■利用チャンネル
- ■電波の強度など

※Wi-Fi通信でのパケットキャプチャはしません。
※プロトコルのみを取得して分析。通信データの内容は対象外です。

3. Wi-Fi セキュリティ脆弱性診断　～サービスメニュー～

Spline Network

1Day	1Week	1Month
調査期間	調査期間	調査期間
1日（24時間）	1週間 （24時間 x 7日間）	1ヶ月 （24時間 x 30日間）
とりあえずWi-Fi状況を見てみたい	曜日別のWi-Fi使用状況の傾向を把握したい	月末月初のWi-Fi使用状況の傾向を把握したい

Wi-Fi分析内容

- Wi-Fi使用状況の分析：アクセスポイント数、端末数、接続状況
- セキュリティ分析：セキュリティの状態を分析
  ※ご使用のアクセスポイント、端末情報「MAC Address,SSID」を提示が必要
- リスク分析：シグネチャによるリスク分析

報告内容

- Wi-Fi電波状況の統計報告
- 各サービス毎の時系列報告
  ※報告書のサンプルは、P.26 ～ P.30 をご参照ください）

特徴

- センサーの取得ログは暗号化
- お客様のネットワーク環境は使用しません（LTE回線を使用するため）

Spline Network

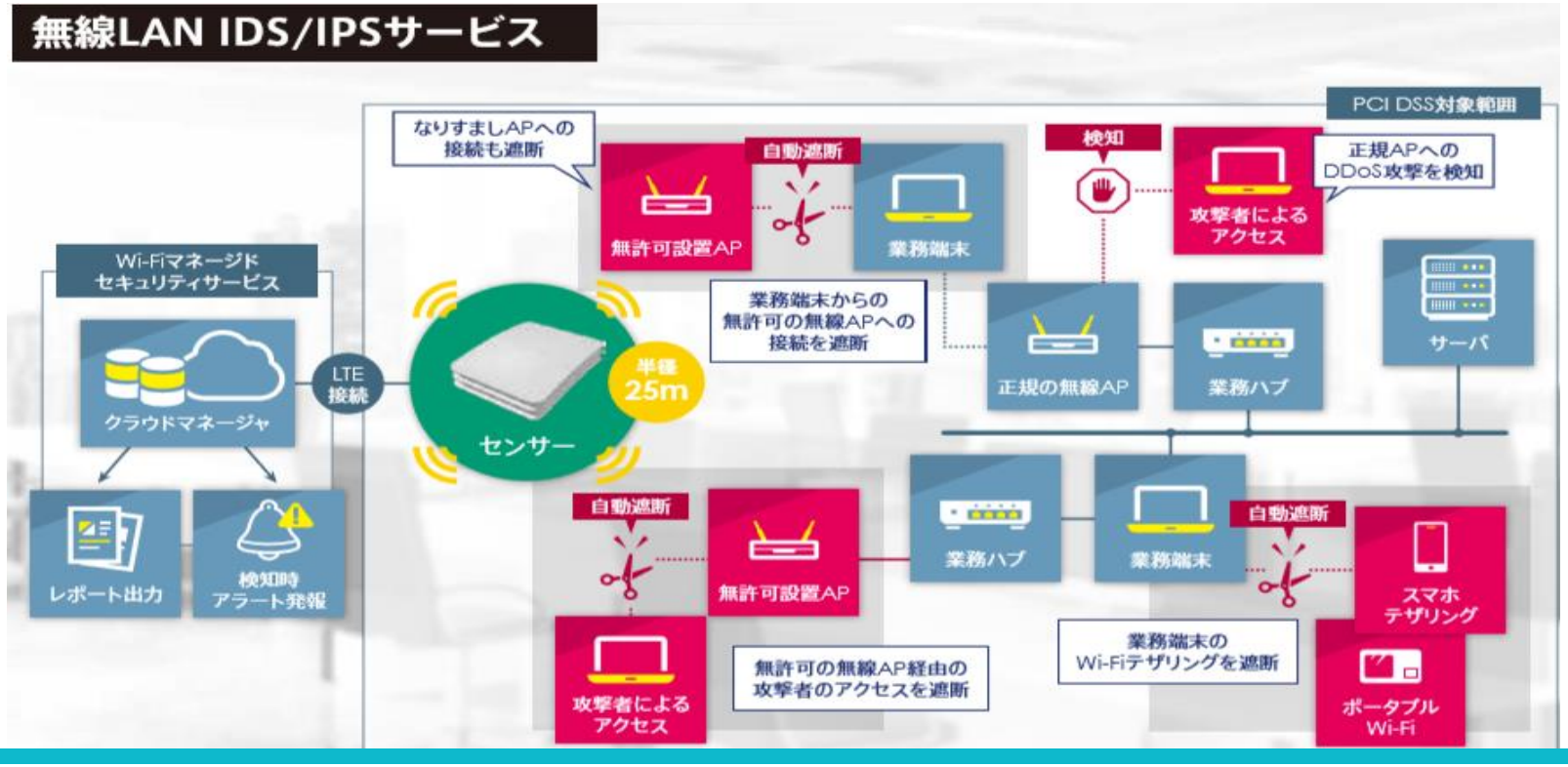
オプションサービス

センサー位置設計と設置（現地調査込※1）	● 現地平面図を基にした、センサーの最適な設置位置の設計 ● 位置情報分析時における位置を正確に取得する為のセンサー設置位置設計 ● 現地におけるセンサーの電波取得状況の確認
時系列情報分析	サービス期間内のアクセス状況を1時間毎に取得、分析（グラフ化）
位置情報検知	セキュリティポリシー違反のアクセスポイント、端末の位置の特定※2
電波環境分析	AP間の電波干渉、微弱電波、不感知など、Wi-Fiパフォーマンスに影響する電波状況の分析
結果報告と対策	お客様を訪問し報告書の内容を説明、分析結果を基にセキュリティポリシー策定やセキュリティ対策・運用、Wi-Fi環境改善の支援及び実施

※1：設置場所が東京23区外となる場合、別途交通費をいただきます。また、厚生労働省が定める労働安全衛生法により、高さが2メートル以上の作業においては高所作業と定められており、別途費用が必要となります。
※2:位置情報検知には、センサーが3台以上必要となります。状況によって精度が変わる可能性があります。

Spline Network

～ PCI DSS 要件11.1のためのWi-Fi監視運用ソリューション ～



Wi-Fi利用状況を24時間365日 常時監視

検知・遮断 Wi-Fi不正利用を自動で即座に！

アラート通知　ログ管理　対策自動化　位置追跡

運用監視項目

1．登録アクセスポイントと端末のアクセス管理

SSID、MAC Address、認証方式、暗号化方式、プロトコル、利用チャンネル、電波強度、端末の接続先アクセスポイントの管理

2．セキュリティポリシー違反、不正接続を検知、通報、遮断

登録した機器以外のセキュリティポリシー違反、未登録機器の不正接続を検知、通報、遮断

3．シグネチャにより脅威を検知、通報、遮断

シグネチャによりWi-Fiネットワークでの DDoS攻撃などの脅威を検知、通報、遮断

月次報告書

1．Wi-Fi環境使用状況
2．セキュリティ状況
3．シグネチャ状況分析
4．PCI DSS要件11.1の基準を満たす定期報告

※上記は、機器間の通信を暗号化したLTE回線使用が前提です。
自社ネットワークの利用をご希望の場合は、別途ご相談下さい。

Spline Network

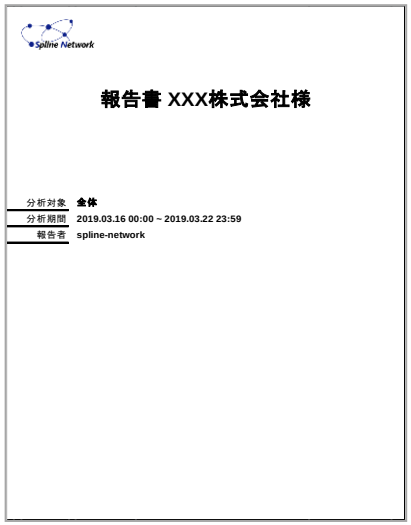
オプションサービス

Wi-Fi環境時系列分析	AP間の電波干渉、微弱電波、不感知など、Wi-Fiのパフォーマンスに影響する 電波状況の時系列分析 a. アクセスポイント、端末の電波検知状況（アクセスポイント、端末の数） b. 指定されたアクセスポイント(MAC Address）のチャンネル別 c. 指定されたアクセスポイント(MAC Address）の電波強度 d. 指定されたアクセスポイント（SSID）と端末の接続状況
位置情報検知	セキュリティポリシー違反のアクセスポイント、端末位置の特定 ※ センサーの設置位置、電波状況により特定位置に誤差が発生します
詳細分析サービス	データに潜んでいる特定のパターンや相関関係の詳細分析
統合報告書作成	複数のセンサー利用時におけるデータ統合及び傾向分析
結果報告と対策	お客様を訪問し報告書の内容を説明、分析結果を基にセキュリティポリシー策定やセキュリティ対策･運用、Wi-Fi環境改善の支援及び実施

報告書サンプル

8. 基本報告書サンプル

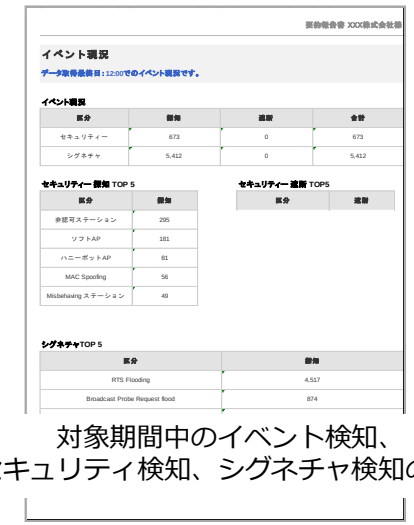
報告書（表紙）



アクセスの現況

対象期間中のアクセスポイント、
端末、センサーの現況

イベント現況



対象期間中のイベント検知、
セキュリティ検知、シグネチャ検知の現況

トラフィックの現況

対象期間中のアクセスポイント、
端末のRX/TXトラフィック状況とTop5の現況

セキュリティ脅威現況

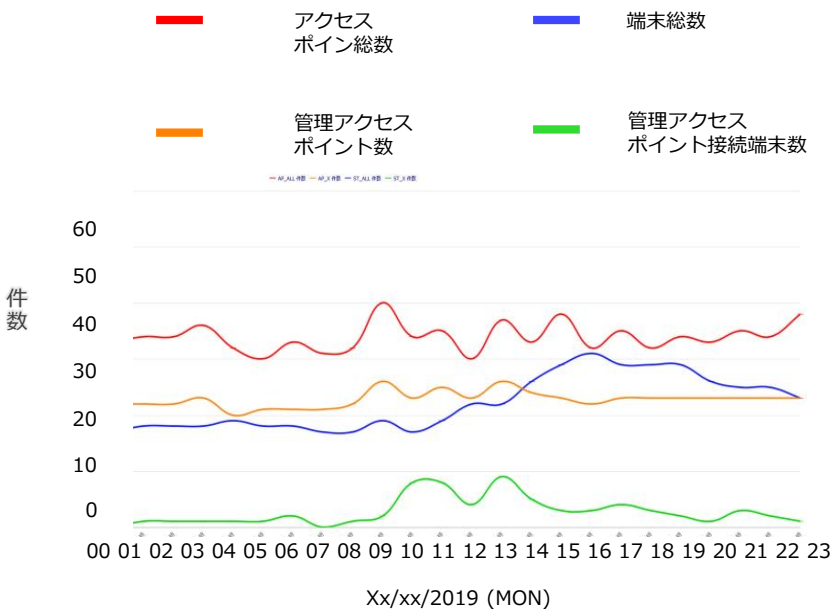
対象期間中の許可端末のセキュリティ状況、
セキュリティ区分の現況

セキュリティ脅威TOP

対象期間中の許可端末の
セキュリティ脅威端末リスト

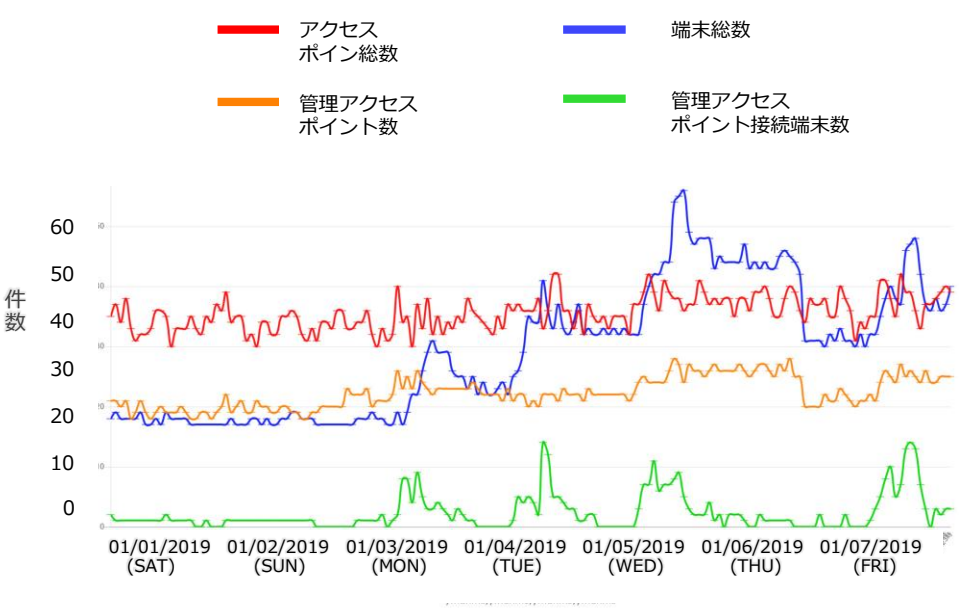
9. オプション報告書サンプル

日別推移グラフ



アクセスポイントおよび端末の24時間のアクセス数を時系列分析

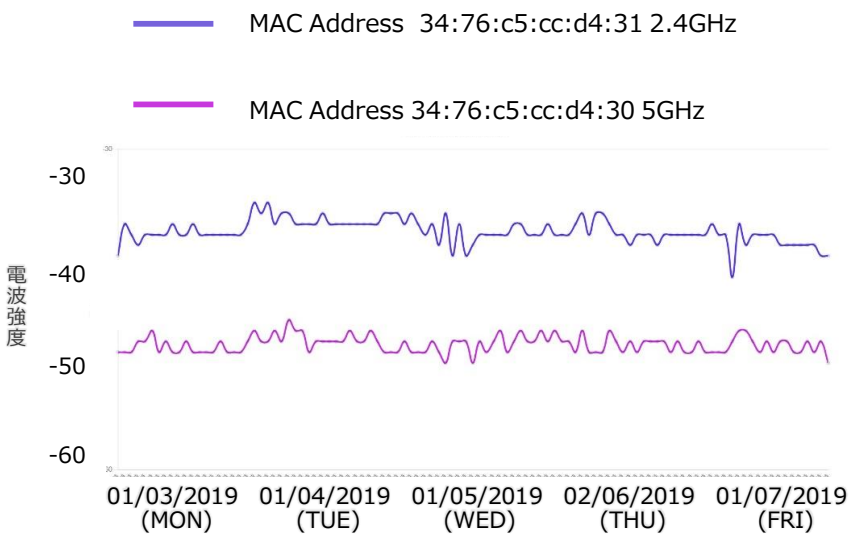
週間推移グラフ



アクセスポイントおよび端末の24時間x7日間の
アクセス数を時系列分析

10. オプション報告書サンプル

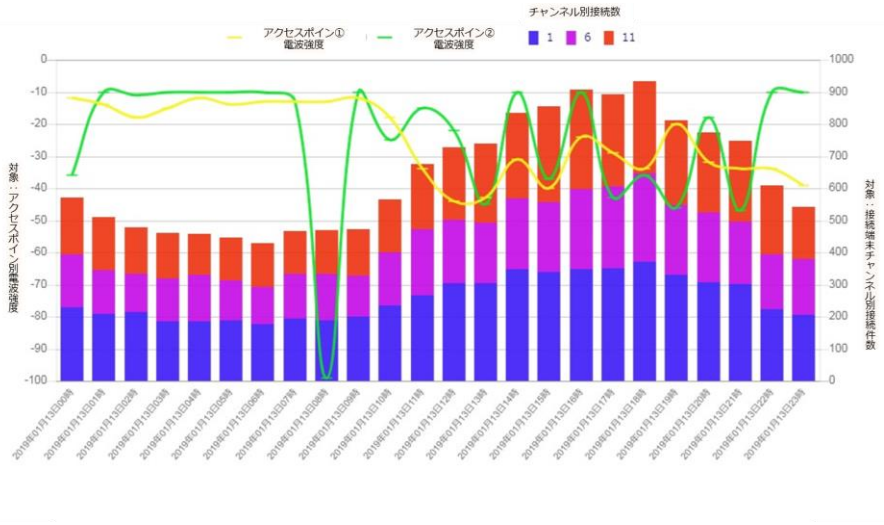
電波強度時系列グラフ



最大：MAC Address x10

指定されたアクセスポイントと接続された端末の電波状況分析

2.4G電波状況とチャンネル別接続状況グラフ



最大：MAC Address x10

指定されたアクセスポイントの
MAC Addressのチャンネル別の端末との接続数

CONFIDENTIAL

位置情報検知