～ 日本カード情報セキュリティ協議会 ～

Wi-Fi の脆弱性が感染拡大の踏み台に！
ネットワーク内外の
Wi-Fi脅威やハッキング手法

～2022年に顕在化した新たな脅威～

株式会社スプライン・ネットワーク

2023年1月20日

クレジット業界を中心に制定された国際的なセキュリティ基準。カード情報を「保存、処理、または伝送する」企業であるカード加盟店、銀行、決済代行など行うサービス・プロバイダーが準拠する必要があり、対象企業はクレジット、決済代行、銀行、加盟店、航空、鉄道、流通、通信、携帯電話、新聞社など、その範囲は広範にわたる。（関連：割賦販売法）

Wi-Fiセキュリティ対応の要件11概略抜粋

【ワイヤレスAPを特定監視し、許可および未許可の両方を管理・識別する必要がある】

1、外部・内部の脆弱性を定期的に特定

2、既知のAPリストを定義し、接続状況の把握
（リスト外のデバイスを介した接続の脅威）

3、なりすましAP等への接続状況の監視

4、企業が**Wi-Fi機器使用を禁止している場合でも必須**

5、自動監視を使用する場合、アラート通知が必要

※テスト/検出/識別は少なくとも３か月に１度行うこと

⇒**3か月に1度行えば良いのでしょうか？？**

（引用：Payment Card Industryデータセキュリティ基準より）

韓国におけるWi-Fiセキュリティ事情

☆2000年代よりWi-Fiセキュリティで官民連携開始、既に法制度化

2009年3月：安全行政部無線LANセキュリティガイド
→第4章（無線LAN/無線装備運営政策）
無線LANの不正利用に対する保安点検はリアルタイムで行われてこそ効果ある

ーーーーーー2010～2018省略（政府主導で技術開発／官民連携）ーーーーーー

2019年6月：国家情報保護基本方針
→第29条（ネットワークセキュリティ管理）
管理者は、非認可者のネットワーク侵入を防止するため、安全性を検証し、検知/遮断システムの運用等、関連保安対策を講じなければならない

2020年9月：通信網の利用及び情報保護等に関する**法律**
→第45条（ネットワークの安定性確保等）
・情報通信サービスのネットワーク安定性/信頼性を確保し、科学技術情報通信部長官はそれを勧告できる
・不正な者のネットワークにアクセス/侵入を防止し、情報保護システムの設置・運営等の技術的/物理的保護措置をとらなければならない

IDF主催：第19回デジタル・フォレンジック・コミュニティ2022 in TOKYO

デジタル・フォレンジックにおける官民連携イベント
「進展するサイバー空間とフォレンジック」

※座長の名和氏から、Wi-Fi領域のセキュリティ対策が急務とのことでパネル登壇に招聘されました。

座長：名和 利男 氏／SOMPO 李 宏宇 氏／SNI 雪野 洋一

IPA(独立行政法人情報処理推進機構)による第三者的有効性検証結果

IPAは、経済産業省の産業サイバーセキュリティ研究会の議論を受けて、専門家による客観的な「セキュリティ製品の有効性検証」について製品を選定、第三者的に製品機能、性能、運用性、導入容易性の４つの観点から検証を実施し、その有効性を確認した。

（2021年4月26日IPA資料より抜粋）

■検証結果URL：https://www.ipa.go.jp/files/000090567.pdf

管理すべきエリアネットワーク

見えないからこその脅威

インターネット

管理できていない領域

野良デバイス

シャドーIT

IoTデバイス

スマート家電

情報漏洩

機密情報

管理外のWi-Fiデバイス

侵入/マルウェア感染
ハッキング/バックドア
偽装/なりすまし…etc.

無線ネットワーク

無線LAN
アクセスポイント

充実した管理領域

ファイアウォール

アンチウイルス

サンドボックス

IDS/IPS

認証/暗号化

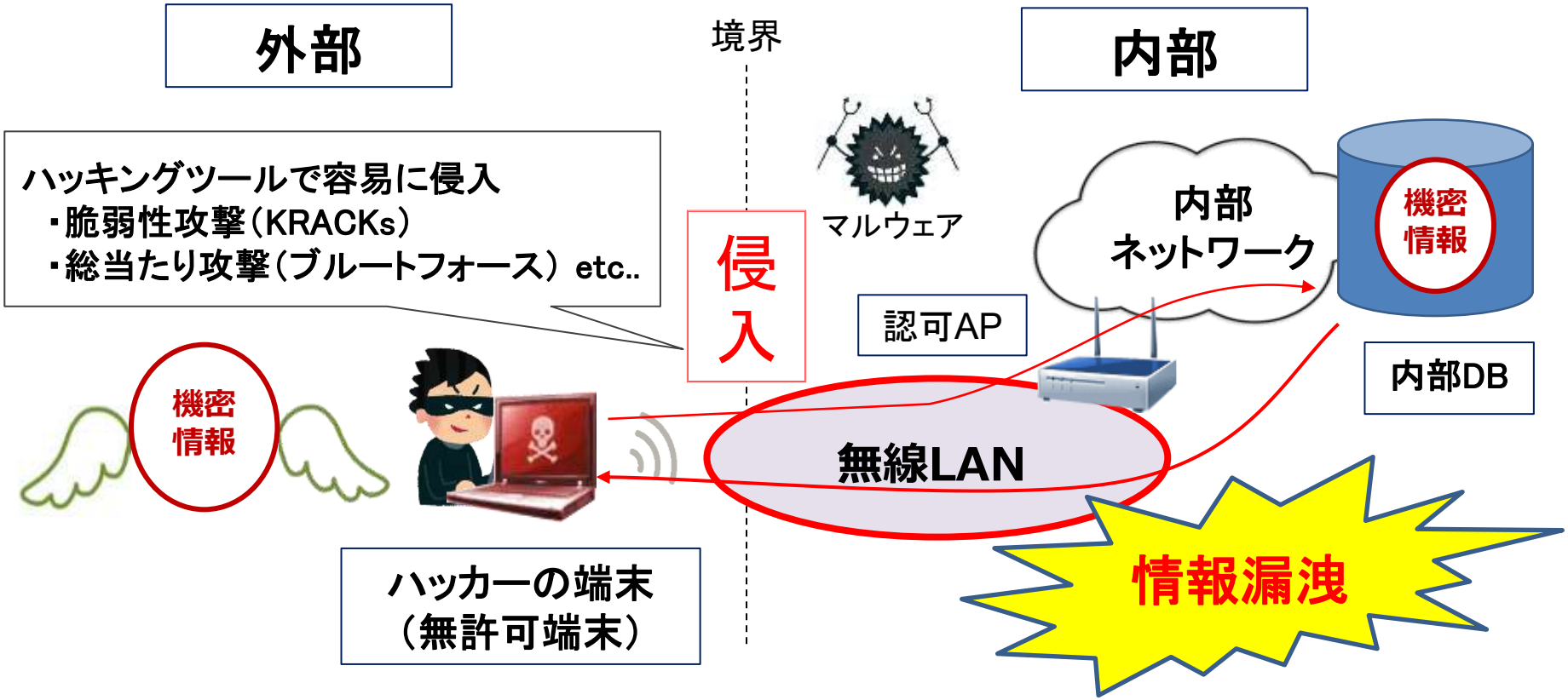
有線ネットワーク

<提言>
無線ネットワークは増加の一途
有線＋無線＝エリア全体のネットワークセキュリティ対策が必須

2-2. Wi-Fi脅威の代表例：非認可端末

概要：無許可の端末が正規AP(無線LAN)に接続してしまうリスク

結果：無線LAN経由でネットワークに侵入され、マルウェア感染や機密情報漏洩



{WiSAS発見事例}
製造メーカー、大手データセンター、製薬会社、システムインテグレーター、外資系保険会社、クレジットカード発行会社、セキュリティ監視センターなど

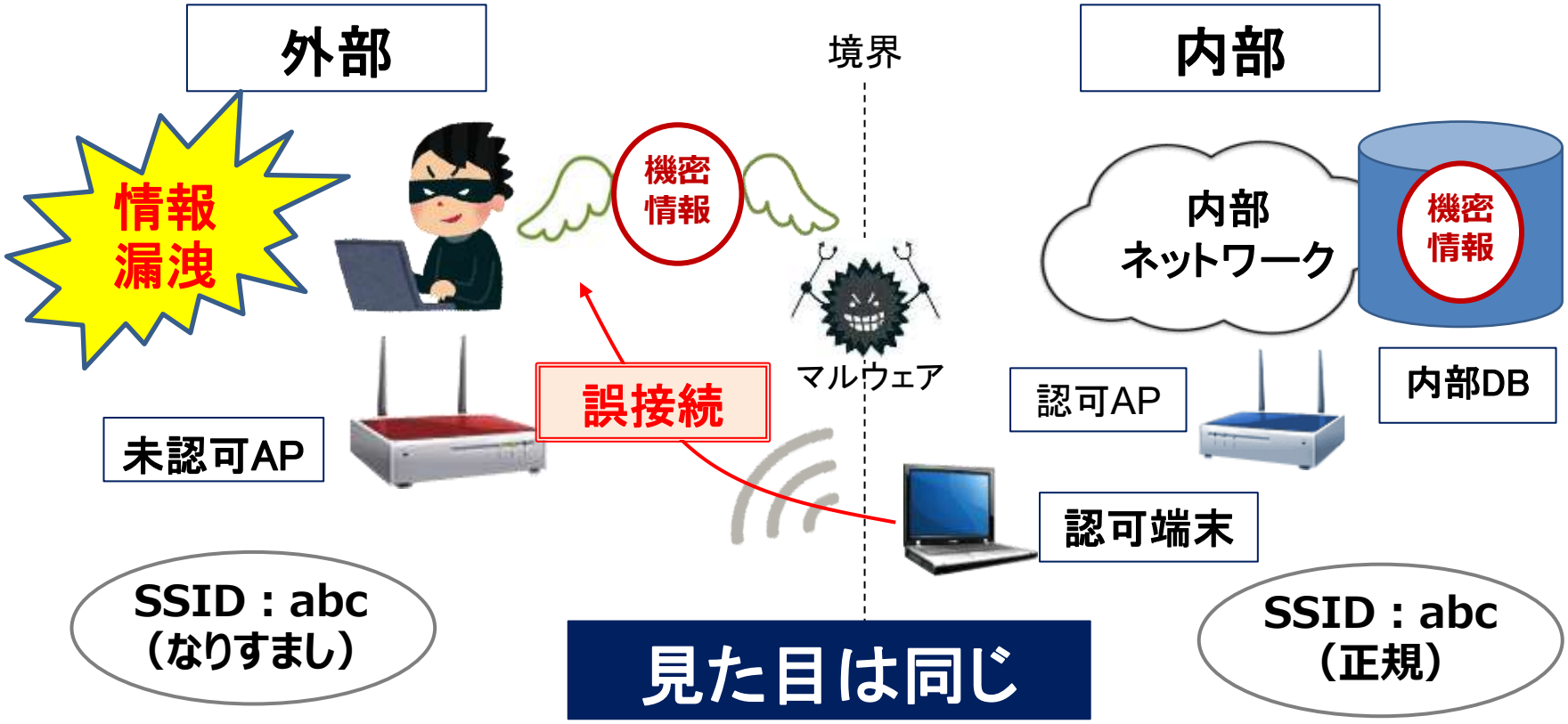
概要：正規の端末が、未認可APの無線LANに接続してしまうリスク

結果：管理外のネットワークが確立し、マルウェア感染や機密情報が漏洩

{WiSAS発見事例}
大手データセンター、製薬会社、大手BPOセンター、国立研究開発法人、大手デジタル放送配信会社、大手製造業、セキュリティSier、不動産業など

概要：未認可APが認可APと同じSSIDになりすまし誤接続してしまうリスク

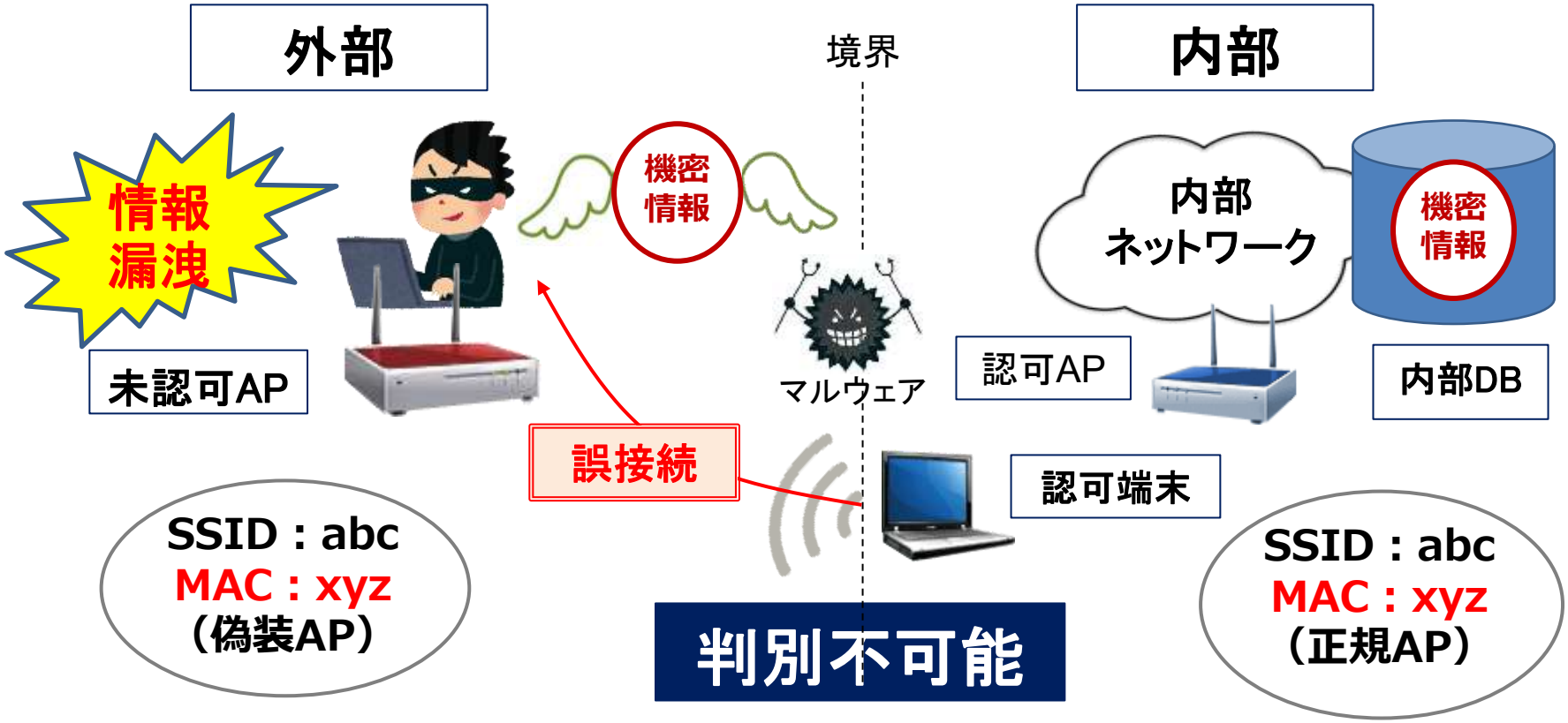
結果：なりすましAP経由でマルウェア感染、端末をハッキングされ機密情報漏洩



{WiSAS発見事例}
外資系大手ホテル、セキュリティ・システムインテグレーターでハニーポット(なりすまし)発見。**長期間**に渡り、機密情報を盗まれていたことが発覚。

概要：未認可APが正規APと同じMACアドレスに偽装し、接続させるリスク

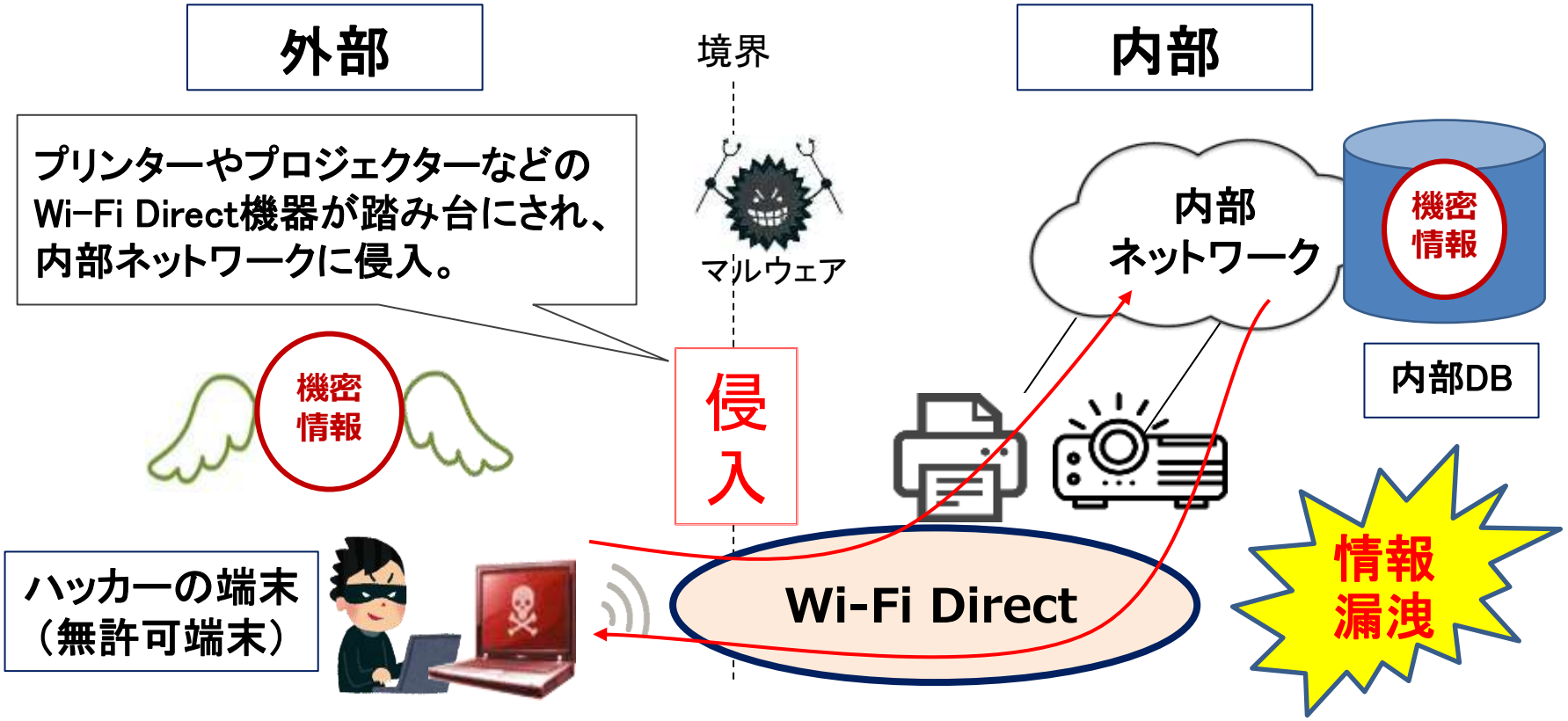
結果：MAC偽装AP経由でマルウェアに感染、端末をハッキングされ機密情報漏洩



{WiSAS発見事例}
有名ホテルチェーン。他、国内で頻発している。(某セキュリティアナリスト)
日本のホテル業界でダークホテルが蔓延、**世界の感染源の1/3を占める**。

概要：ネットワーク内のWi-Fi Direct機器を踏み台に内部侵入されるリスク

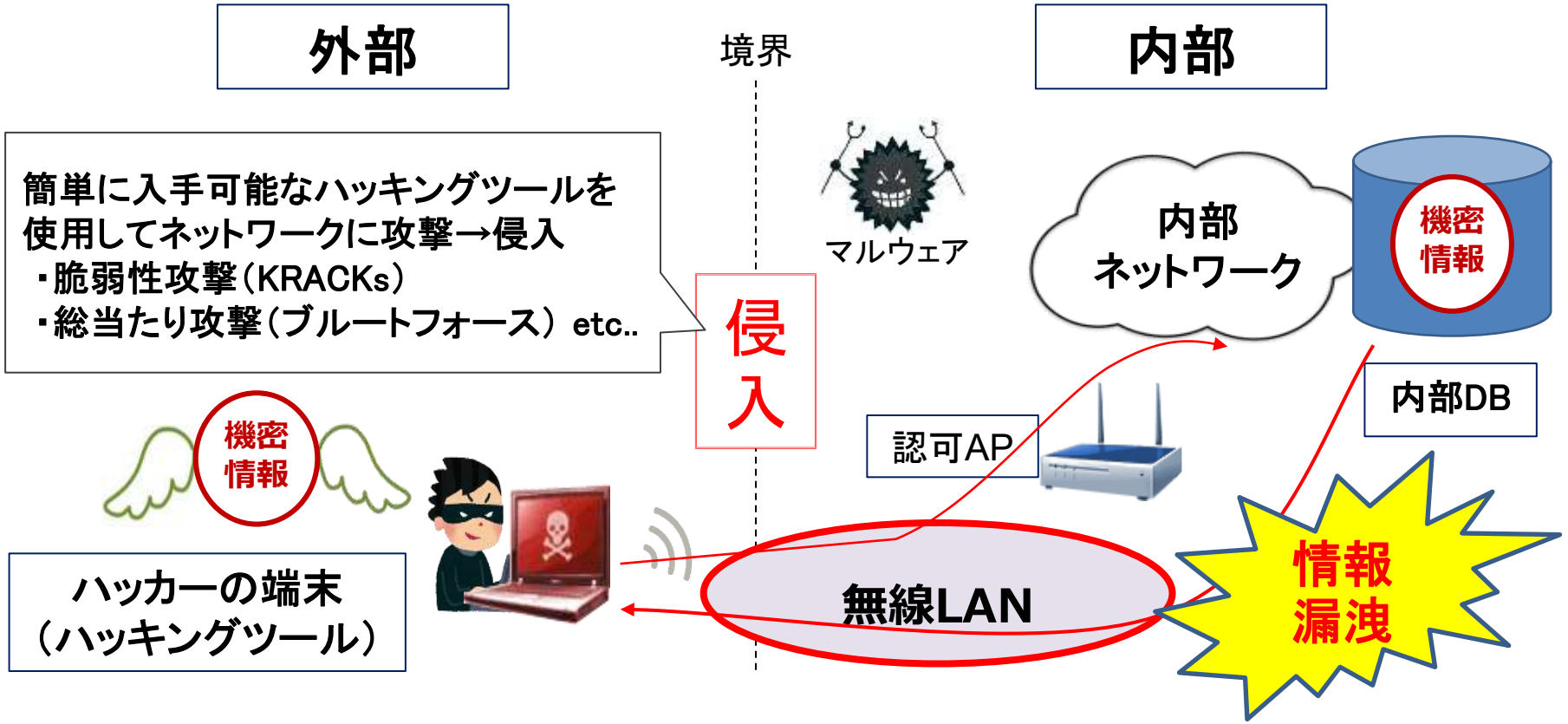
結果：Wi-Fi Direct経由で侵入、端末ハッキング/マルウェア感染で機密情報漏洩



{WiSAS発見事例}
製薬会社、デジタル放送配信会社、不動産業、カード情報関連、多くのSier、セキュリティコンサルタント、製造業など、**ほとんどの企業で未対応**。

概要：ハッキングツール(デバイス)を利用して、不正侵入されてしまうリスク

結果：Wi-Fi Direct機器経由で侵入、端末ハッキングやマルウェア感染等



**USB充電ケーブルに偽造したOMGケーブル(iPhoneもAndroidも存在)や
USBデバイスに似せた新手のハッキングツール(デバイス)が続々と誕生。
手口も年々進化し、誰でも容易に入手可能（ネット販売）なため警戒が必要。**

特許取得済

WiSAS
Wi-Fi Security Assurance Series

Wi-Fiセキュリティ対策の最適解
WiSASの概要

WiSAS（Wi-Fiセキュリティ・アシュアランス・シリーズ）には、３つの診断分析サービスと3つの常時監視サービスがあります。

診断分析

- WiSAS 環境 スキャン
- WiSAS 脆弱性診断
- WiSAS 環境最適化支援

常時監視

- WiSAS NORA
- WiSAS 24H365D
- WiSAS 24H365D PLUS

WiSAS診断分析とは？

- Wi-Fiネットワーク環境の健康診断
- 知識のいらない手軽な１Shotサービス
- 有線ネットワークへの接続の必要なし
- 取得データはWi-Fiのヘッダー情報のみ

WiSAS常時監視とは？

- 24時間365日対応の監視サービス
- サブスクタイプの年間契約サービス
- 検知即遮断機能搭載(無線IDS/IPS)
- フルリモート＆フルマネージドサービス

3-2. WiSAS 常時監視ソリューション　システムイメージ

- 様々な脅威を検知（遮断）
- 設置に特別な知識は必要なし
- 取得データはヘッダー情報のみ
- 社内ネットワークへ接続必要なし
- 完全独立型のフルリモート
- 様々な監査に利用可能

WiSAS
クラウド管理センター
（日本国内）

Internet
LTE回線経由

アラート通知

月次レポート

監視対象エリア

WiSASセンサー

IT管理者
（お客様）

Wi-Fiデバイス

電波取得可能エリアの目安
半径40m~50m
（環境により変わります）

- 常時監視
- 脅威検知/遮断

センサー電源ONで作業完了！

3-3. 従来型訪問検査とWiSAS（クラウド型無線 IPS/IDS）比較

ウォークスルー検査とWiSASの違い				
比較内容	ウォークスルー検査		WiSAS（クラウド型）	
手間	×	訪問が必須 日程や人員調整が手間	○	センサー電源ONのみ （訪問は不要）
テスト頻度(継続性)	△	調査が訪問時に限定	○	スポット対応はもちろん、 常時監視対応可能
テスト内容	△	不正な個体の検知は可能だが 増加する攻撃手段への対応不可	○	シグネチャを逐次更新し、 最新型の攻撃も検知
テスト／報告書品質	△	テスト作業員(含：委託先)の スキルに依存。	○	フルマネージドなので安定品質 ※報告書サンプルを参照下さい
管理負荷	×	対象拠点毎に管理／調整が必要	○	クラウド型ゆえ集中管理
リアルタイム対応	×	訪問時のみ不正発見、 しかも一部の脅威に限られる	○	リアルタイム監視(常時監視) 緊急時にはアラート発報
不正発見時の対応	△	現地訪問による不正デバイスの 位置特定と物理的な撤去	○	リアルタイムにアラート/対処 （WIDS/WIPS機能搭載）
Wi-Fiデバイス管理	△	ウォークスルーの手法上、 ほぼ不可能	○	セーフ/ブロック/未確認で データベース管理

3-4. WiSAS 常時監視ソリューション　3つの特徴！

Wi-Fi利用状況を24時間365日 **常時監視**
Wi-Fi不正APを即座に **検知・遮断**


アラート通知

接続履歴

対策自動化

位置追跡(OP)

◆◆◆サブスクリプションモデル ◆◆◆

PCI DSS対応!!

～ 3つの重要なポイント ～

WIDS／WIPS機能!!

1 完全独立ソリューション

- 既存システムの変更や接続の必要は無し
- 新たな機器の購入無し
- 製品以外のコスト無し

※過去の投資を無駄にしない他社製品と競合無し

2 フルリモート：簡単運用

- 設置はセンサー電源のみ
- 全てのサービスはリモートで実施可能
- 報告書は自動生成

LTE回線使用でクラウド化
レポートもクラウド保管

3 フルマネージド：自動化

- 不正APや不正アクセス検知時はアラート
- 検知即遮断も可
- Wi-Fiデバイス管理機能

WIPS専用機ならではの
高機能、高信頼性、高可用性

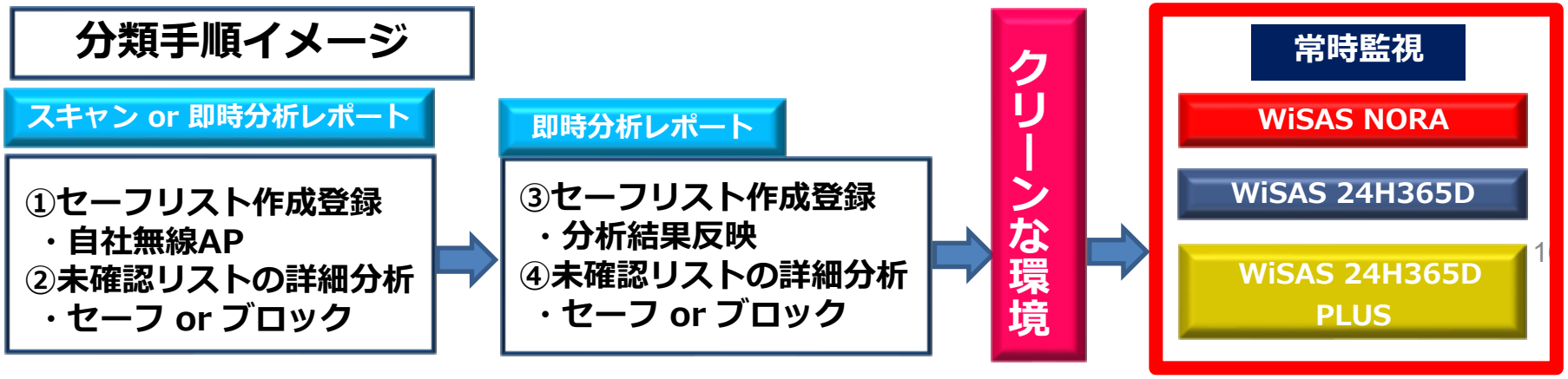
3-5. CONCEPT：WiSASが実現する安全なWi-Fi環境！

※Wi-Fi環境におけるAP／端末の分類に関して（仕分け）

WiSASでは、全てのWi-Fiデバイスを大きく下記3つのグループに分類しています。

1，セーフリスト：警戒する必要のないAP／端末のデバイスのリスト
2，ブロックリスト：明らかに悪意のある、対象ネットワーク内で稼働させたくないデバイスのリスト
3，未確認リスト　：セーフ、ブロックの仕分けができていないデバイスのリスト

分類手順イメージ



Wi-Fi セキュリティを担保するには、上記３の未確認リストを無くすことが重要です。
WiSASは、その目的を達成するための方法やツールを複数提供しています。

※リスト作成方法には、手動登録型と自動生成型（セーフリストのみ）があります。

Wi-Fi環境スキャン(見える化)
先着20社プレゼント！

Wi-Fi 環境を一瞬で可視化（スナップショット）

1、無線AP(含:ステルス）と端末のMACアドレス、信号強度(dBm)
2、無線APの無線プロトコル、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（証跡としてご使用頂けます）

※このサービスは何の準備も必要ありません。
予定された時間に、センサーの電源を入れるだけ。
約3分で「Wi-Fi環境の見える化」ができます。
ご希望の方は、wisas-sales@spline-network.co.jp
までご一報ください。

詳細な説明／デモ／評価のお申込みなど、お気軽にお問い合わせください。

担当部署：WiSAS（ワイサス）事業部

電話：03-5464-5468

チーム代表メール： wisas-sales@spline-network.co.jp

WiSAS専用サイト：https://wisas.jp

WiSAS Facebook： https://www.facebook.com/WiSAS.jp

YouTube製品動画: https://www.youtube.com/@wisas

- 商号　株式会社 スプライン・ネットワーク
- 代表取締役　雪野　洋一
- 本社所在地　〒150-0034
  東京都渋谷区代官山町1-8
  SYLA DAIKANYAMA 6F
- 設立日　2002年 1月 11日

特許取得済のWiSASは、日本で唯一のWi-Fiセキュリティ・ソリューション。
海外でも類を見ないフルマネージド製品は、様々な利活用を考えています。
WiSASを販売、支援、業務提携頂ける企業/団体を求めます。

4-1. WiSAS 診断分析サービス　主な採用事例

WiSAS

WiSAS 脆弱性診断　**WiSAS 環境最適化支援**　**WiSAS 環境スキャン**

■某製造メーカー（WiSAS脆弱性診断）
・内部ネットワークに接続された小型無線APを発見。従業員に賄賂を渡しての設置が判明。
産業スパイが介在したと思われる。

■国立研究開発法人JAXA
・最重要セキュリティエリアでWiSAS脆弱性診断を実施したところ、スマホのテザリングが散見された

■大手Business Process Outsourcing企業・・・PCI DSS準拠企業
・管理外のポータブルWi-Fi ルータ持込みを複数検知。その後の調査で、業務上の機密データ
（含：お客様データ）をクラウド上にアップロードしていたことが判明。

■大手デジタル放送配信会社（WiSAS脆弱性診断＋無線DoS攻撃分析+位置情報分析／環境最適化支援）
①脆弱性診断
・従業員が私物スマホのテザリングで会社貸与のPCを利用していることを複数検知
（管理外の無線ネットワークを経由した情報流出の可能性が浮上）
・意図せず有効化されたWi-Fi Direct機器を複数検知（プリンター、スキャナーなど）
②無線DoS攻撃分析
・無許可のAPによる無線DoS攻撃（BeaconFlood攻撃）を検知（至：接続不良の原因特定）
③位置情報分析
・センサーを3台設置し、不正使用機器の位置を特定、排除
④環境最適化支援
・12hourの時系列分析により、時間帯によるAP接続の偏りを検知、AP接続の最適化を提案

4-2. WiSAS 診断分析サービス　主な採用事例

WiSAS 脆弱性診断　WiSAS 環境最適化支援　WiSAS 環境スキャン

■大手SIer・・・セキュリティサービス提供企業
- 持ち込みWi-Fi端末の検知（把握不可能AP）
- 従業員が私物スマホのテザリングで会社貸与のPCを利用していることを複数検知
  （管理外の無線ネットワークを経由した情報流出の可能性が浮上）
- 有効化されたWi-Fi Direct機器を複数検知（プリンター、プロジェクター、PWDはデフォルト）
- 社内の無線APになりすましたハニーポットAPの存在を検知し、会社貸与PCの誤接続を遮断

■某大手データセンター
- 最重要監視ポイントのサーバールーム内で、有効化された電話ルータのWi-Fi を検知
  （PWDはデフォルト状態＝容易に侵入可能）
- スマホのテザリングをONにしたままロッカーに預けてセキュリティエリアに入室、
  そのセキュリティエリア内からロッカー内のスマホでテザリングを行っていたことが判明

■某製薬会社
- 高まるセキュリティ脅威を前に、全国の事業所・研究所・工場20拠点近くを総点検
- 緊急事態宣言で人の移動が制限される中、センサーのみを順送りしリモートWi-Fi脆弱性診断を
  実施。センサー設置はお客様が実施。
- 業務で使用しているにも関わらず、管理外のWi-Fiデバイスを多数発見。既設の管理ツールだけでは
  限界があることを痛感。Wi-Fiデバイス管理の重要性から新たなセキュリティポリシー作成に着手

■某不動産仲介業
- 社内の正規端末が、外部のフリーWi-Fiに接続されていることを確認、すぐに設定変更を実施。

※WiSASは、フォレンジック（事故原因）調査のサイバー保険補償対象になっています。

4-3. WiSAS 常時監視サービス　主な採用事例

1、WiSAS NORA | **2、WiSAS 24H365D** | **3、WiSAS 24H365D PLUS**

■SMBCファイナンスサービス株式会社様・・・ *PCI DSS準拠企業*

- 全国の主要拠点（十数か所）にセンサーを設置
- 人手によるウォークスルー検査（スポット対応）から自動監視へ移行
- 有人による断面的なチェックではなく常時監視のため、セキュア度アップ
- デバイス管理を徹底し、野良Wi-Fiデバイスをリアルタイムで検知
- システム変更の必要がなく、**短期間で導入**できた
- ウォークスルー検査では検知できなかった電波も検知し、多数の電波が飛び交っていることを認識
- コロナ対応など今後のパンデミックを想定すると、**人手を介さない運用は有用**
- 毎月初に**監視報告書が自動的に生成**されるので、運用の手間がほとんどない

■国立研究開発法人 JAXA

- WiSAS脆弱性診断サービスを実施後、常時監視の必要性を認識
- 対象デバイスの**位置情報をリアルタイムで分析**できるようセンサーを多数配置
- 監視範囲を拡充計画策定中

■外資系保険会社様・・・ *PCI DSS準拠企業*

- 全国の主要データセンターにWiSASセンサーを設置！
- 有人によるスポット監視からセキュアな常時監視へ移行
- 滞在時間と電波強度の2軸で監視、閾値を変更できるのがよい
- 導入時に即時分析レポートを数回繰り返し 、対象エリアのWi-Fiデバイスを徹底的に仕分け、**セーフデバイスだけに通信を許可するクリーンな環境**を実現し、本番運用開始
- 人員配置換えやデバイス交換時にも即時分析を実施、クリーンな環境を維持
- NORAの電波強度、並びに接続時間の閾値を実態に合わせ変更できるのが良い
- 毎月のようにデバイス管理データベースを更新

4-4. WiSAS 常時監視サービス　主な採用事例

1、WiSAS NORA　2、WiSAS 24H365D　3、WiSAS 24H365D PLUS

■三井住友カード株式会社
- 過去、人手によるウォークスルー調査で大変だったが、何より簡単かつ調査範囲も広いので導入
- コロナ対応など今後のパンデミックを想定すると、人手を介さない運用は有用である
- 毎月初に監視報告書が自動的に生成されるので、運用の手間がほとんどない
- 3か月に1度義務付けられているPCI DSSの監査に利用
- コロナ対応など今後のパンデミックを想定すると、人手を介さない運用は有用である

■独立行政法人 国際協力機構：JICA沖縄センター
- 執務室にセンサーを設置！管理外の野良デバイスを検知
- システム変更の必要がなく、短期間で導入できた
- 既存ネットワークに接続の必要がないシステムなので、システム構築費用はうれしい
- ウォークスルー検査では検知できなかった電波も検知し、多数の電波が飛び交っていることを認識
- 毎月初に監視報告書が自動的に生成されるので、運用の手間がほとんどない

■大手Business Process Outsourcing企業・・・*PCI DSS準拠企業*
- WiSAS脆弱性診断サービスを実施 ⇒常時監視の必要性を認識し、WiSASを導入
- 年に一度の監査でQSAにWiSASレポートを提出したが、昨年までN/Aだった項目が改善され、高評価を得た。同時に過去例のないほど詳細だったのでむしろ歓迎された
- シャドーITを許さない運用ルールを徹底できる
- 転職者による社内からの情報漏洩防止に役立っている

総論：Wi-Fiセキュリティには、デバイス管理とポリシーの連携が必須である！