~ デジタル・フォレンジック研究会 講演資料 ~

◆実は身近な迫りくる脅威◆
Wi-Fiセキュリティ管理と調査の必要性

Spline-Network Inc.

雪野 洋一

12/15/2020

Spline Network

WiSAS
Wi-Fi Security Assurance Series

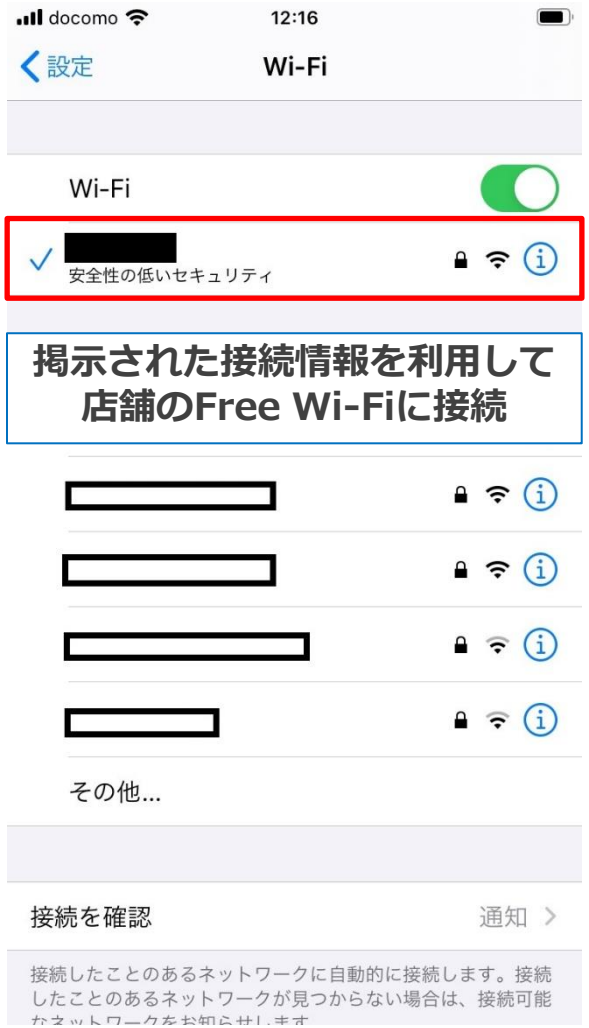
~AGENDA~

1、日常のよくある風景
2、**企業ネットワークの変革と実態**
3、Wi-Fi 環境に潜む様々な脅威
4、WEBで拾ったWi-Fi脅威の事例
5、情報セキュリティ10大脅威の推移
6、身近なWi-Fiの脅威
7、Wi-Fi環境に潜む様々な脅威Ⅱ
8、Wi-Fiセキュリティ担保に必要な施策

WiSAS
Wi-Fi Security Assurance Series

～ 11月某日会社近くのレストランにて～

店舗で掲示されている
FREE Wi-Fiの接続情報



掲示された接続情報を利用して
店舗のFree Wi-Fiに接続

FREE Wi-Fiにつないだことがありますか？
…2179人に対するアンケート調査

YES：56.6%　　NO：15.5%

（調査実施：2019年7月）

1-2. 日常のよくある風景：脆弱なWi-Fセキュリティの実態 ①

WiSAS
Wi-Fi Security Assurance Series

接続情報

セキュリティレベルが **WEP**！！

**WEPはセキュリティレベルが低く
パスワードクラックも容易（数十秒）
総務省も利用しないよう
警鐘を鳴らしている**

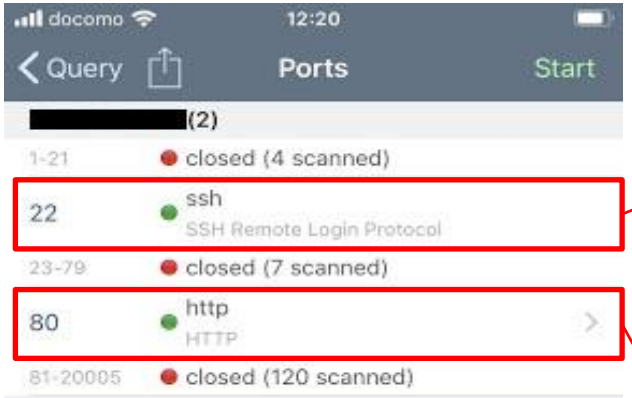
接続情報の詳細

**BUFFALO製の無線LANルータが
利用されていることがわかった**

1-3. 日常のよくある風景：脆弱なWi-Fセキュリティの実態 ②

WiSAS
Wi-Fi Security Assurance Series

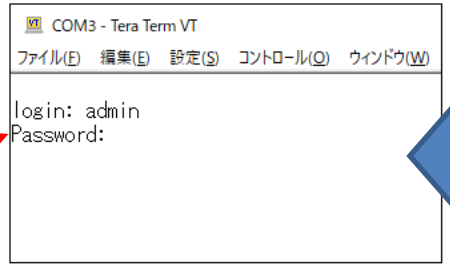
ポートスキャン結果



SSHとHTTPのポートが OPEN！！

無線LANルータの ログイン画面に 容易にアクセスできる状態

パスワードクラックされて 管理者権限を乗っ取られるのも 時間の問題



無線LANルータの CLIログイン画面

無線LANルータの WEBログイン画面

1-4. 日常のよくある風景：脆弱なWi-Fiに接続するリスク

WiSAS
Wi-Fi Security Assurance Series

主なリスクの例

・のぞき見や盗聴
・位置情報の不正取得
・乗っ取りによる遠隔操作
・バックドアを開けて監視
・マルウェアの仕込み etc..

正常性バイアス

心理学用語。
都合の悪い情報を無視し
過小評価すること。
自分に限って、、
自分だけは大丈夫
と思う心理。

・脆弱な公共のWi-Fiに接続すると簡単に通信内容が傍受される
・総務省が利用しないよう警鐘を鳴らしているWEPも未だ健在
・公共のWi-Fiに接続したことで仮想通貨が盗まれる事件が発生
　→日本国内で100万円弱の被害
　→海外でも同様の手口で1300万円の被害
・「スマホを落としただけなのに」はフィクションではない！

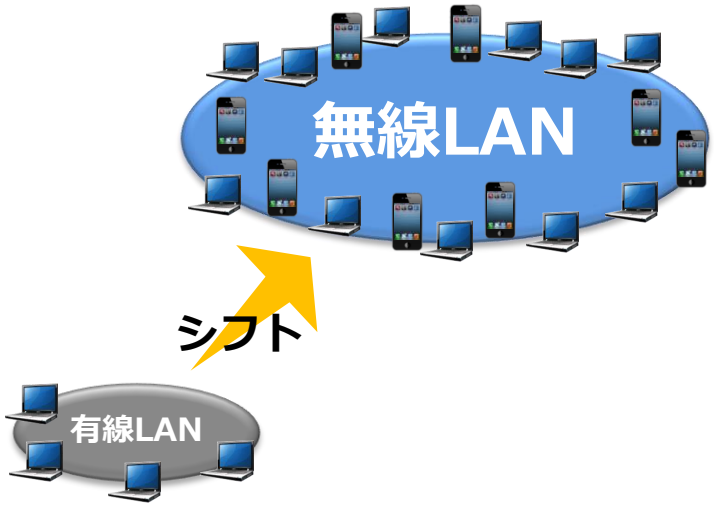
2-1. 企業ネットワークの変革と実態：有線から無線へ

WiSAS
Wi-Fi Security Assurance Series

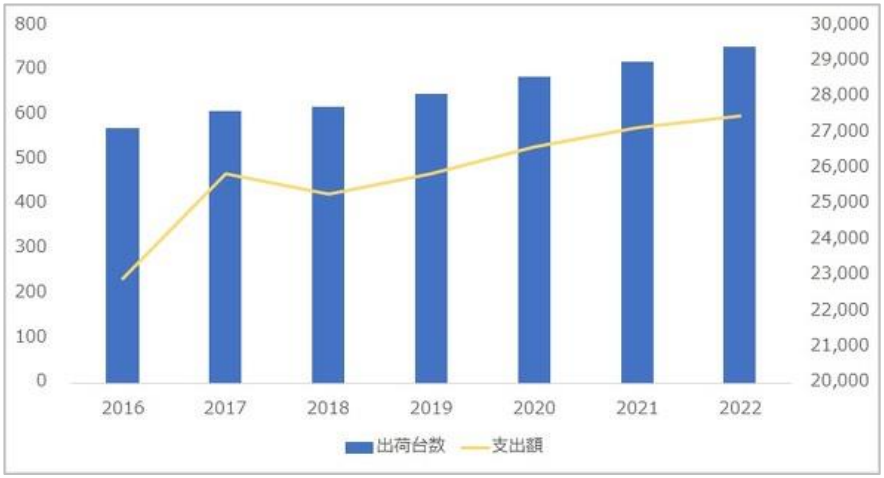
- 無線LANが企業ネットワークに浸透
- クライアント端末が有線から無線にシフト
- あらゆる機器にWi-Fi機能が内蔵
- IoT時代で無線LANの利用は今後も拡大
- スマートフォンのビジネス利用が拡大
- ワークスタイルの変革による利用激増

Wi-Fi 導入率
中小企業：約7割
大企業　：約9割
（2019年調査）

企業ネットワーク



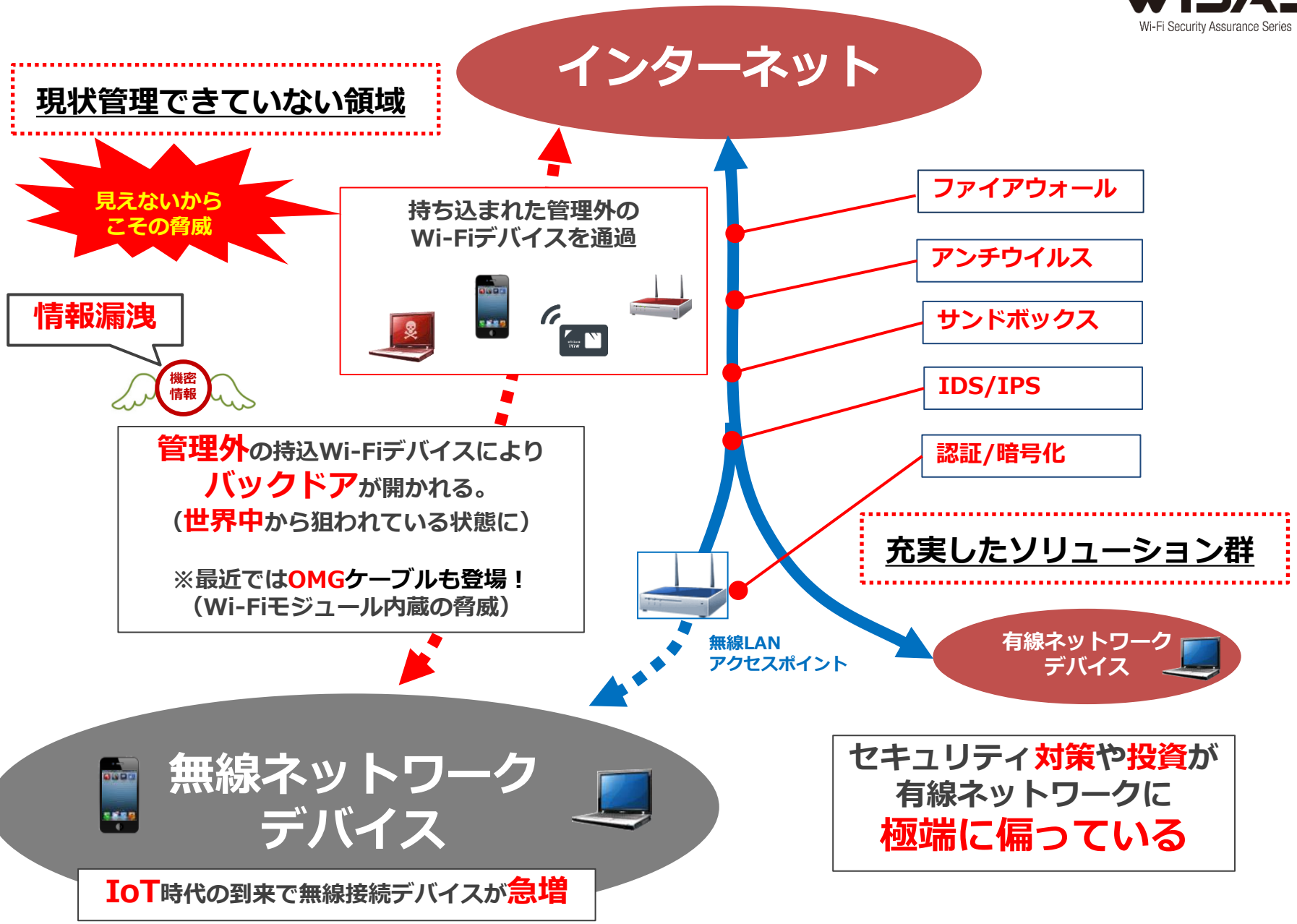
国内企業向け無線LAN機器市場
（2016年～2022年の出荷台数および支出額予測）



（IDC Japan調べ。出荷台数の単位は千台、支出額の単位は百万円）

2-2. 企業ネットワークの変革と実態：無策なWi-Fiセキュリティ環境

WiSAS
Wi-Fi Security Assurance Series



3-1. Wi-Fi環境に潜む様々な脅威：代表例

WiSAS
Wi-Fi Security Assurance Series

① DoS攻撃

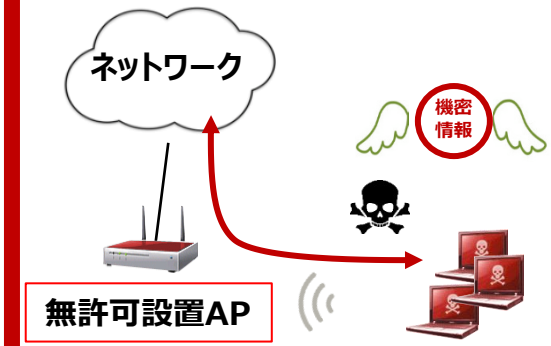
無線APのシステム負荷により、パフォーマンス劣化やシステムダウン

② ポータブルWi-Fi 等

管理外AP接続で、ウィルス感染や不正侵入、情報漏洩の恐れ

③ 無線LANルーター

有線内の無許可APにより、不正侵入や情報漏洩、ウィルス感染



④ Wi-Fi Direct

Wi-Fi Direct機能ONのプリンターからネットワークに不正侵入

⑤ スマホテザリング

テザリングから不正侵入、あるいは発信で情報流出やウイルス感染

⑥ なりすましAP

管理APになりすました不正APに接続した端末から情報漏洩

※ 脅威の事例については別途資料が御座います。

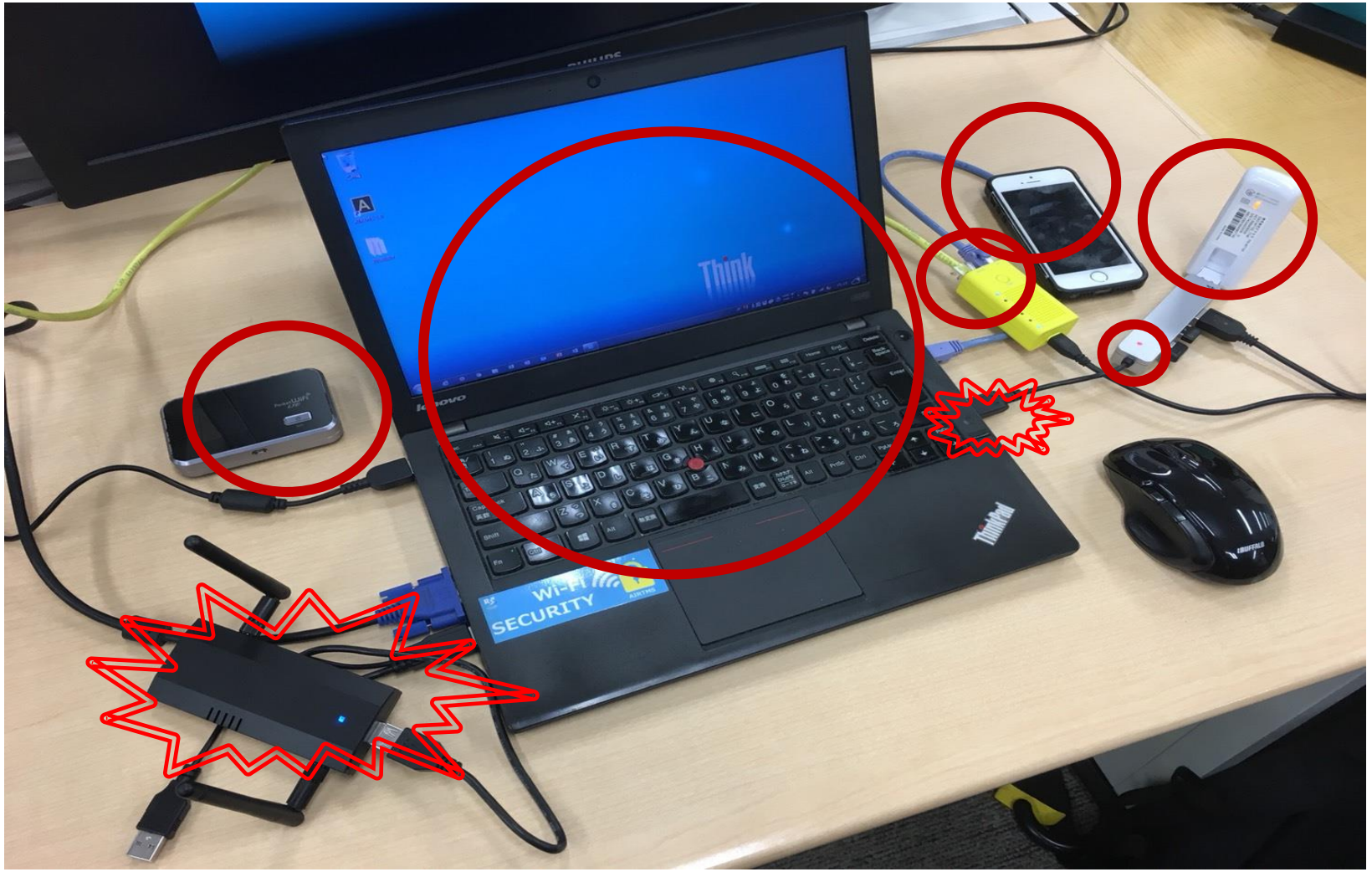
WiSAS
Wi-Fi Security Assurance Series

アクセスポイントは何個あるでしょう？

10

WiSAS
Wi-Fi Security Assurance Series

正解は 8個 !!

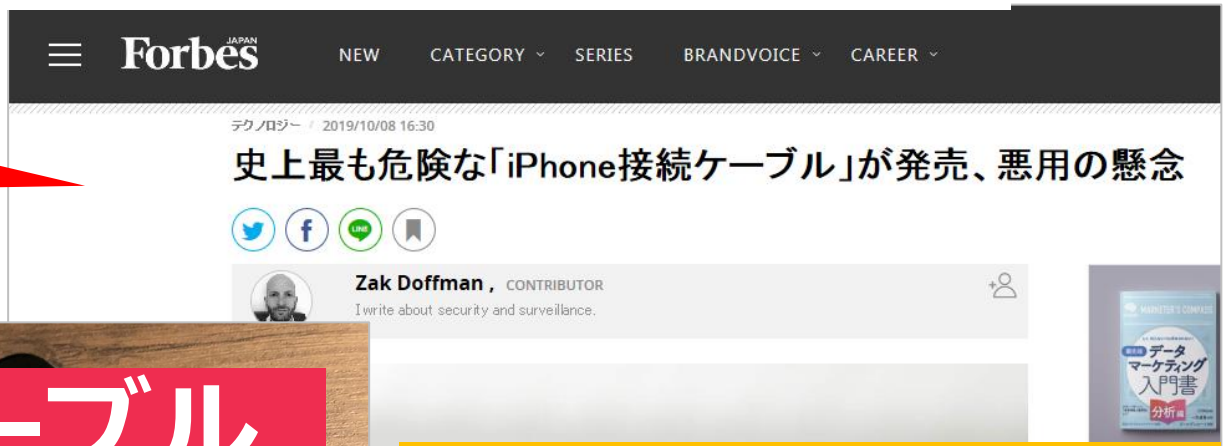


11

WiSAS
Wi-Fi Security Assurance Series

Wi-Fiで遠隔からスマホを乗っ取ることができる充電ケーブルが量産販売を開始（2019年10月）

身近に迫る脅威



Wi-Fiモジュール内臓

見た目では判別不可！

iPhoneもAndroidも！

ネットで簡単に購入可能
しかも1万円程度と安価

100m以上先まで電波が！
（電波法無視）

3-5. Wi-Fi環境に潜む様々な脅威：新たな手口と脅威 ②

WiSAS
Wi-Fi Security Assurance Series

iPhone
Android
Tablet
遠隔操作

身近に迫る脅威

外部AP

ハッカー

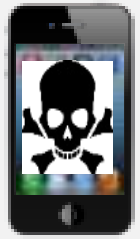
Wi-Fi

オフィス

偽装充電ケーブル

iPhone
Android
Tablet etc

①接続



③データ流出

②乗っ取り
（マルウェア感染）

ケーブルをつないだだけなのに・・

iPhoneを乗っ取られると・・・・

①スマホ内のデータハッキング
②マイクを遠隔操作して音声録音
③カメラを遠隔操作して写真撮影
④もちろん、動画も撮影可能　…etc.

ケーブルを挿しているときしか
電波を出さない

未端から侵入、潜航、
気付かせずに本丸へ!!

WiSAS
Wi-Fi Security Assurance Series

「サイバーセキュリティお助け隊」で対応したサイバー攻撃事例：中小企業もサイバー攻撃の対象となっている実態が改めて浮き彫りに

- 1,064社が参加した実証期間中に、全国８地域で**計910件のアラート**が発生。重大なインシデントの可能性ありと判断し、**対処を行った件数**は**128件**。対処を怠った場合の**被害想定額**が**5,000万円**近くなる事案も。

＜駆け付け支援件数＞

対応種別	総数	内容	発生件数
インシデント対応	128件	電話及びリモートによるインシデント対応※	110件
		訪問によるインシデント対応	18件

※電話及びリモートによるインシデント対応には、訪問によるインシデント対応の一次対応を含む。

＜駆け付け支援の対象となった特徴的な対応事例＞

古いOSの使用

・Windows XPでしか動作しないソフトウェア利用のために、**マルウェア対策ソフト未導入のWindows XP端末を使用**。

・社内プリンタ使用のために、社内LANに接続したことで、意図せずにインターネット接続状態になり、マルウェアに感染。

・検知・駆除できていなかった場合の**想定被害額は5,500万円**。

私物端末の利用

・社員の**私物iPhoneが会社のWi-Fiに無断で接続**されていたことが判明。

・私物iPhoneは、過去にマルウェアやランサムウェアの配布に利用されている攻撃者のサーバと通信していた。

・検知・駆除できていなかった場合の**想定被害額は4,925万円**。

ホテルWi-Fiの利用

・社員が**出張先ホテルのWi-Fi環境**でなりすましメールを受信し、添付されたマルウェアを実行したことで**Emotetに感染**。

・感染により悪性PowerShellコマンドが実行され、アドレス情報が抜き取られた後、**当該企業になりすまして、取引先等のアドレス宛に悪性メールが送信**された。

サプライチェーン攻撃

・実証参加企業でマルウェア添付メールを集中検知。

・**取引先のメールサーバがハックされてメールアドレスが漏えい**し、それらのアドレスからマルウェア添付メールが送付されていた。

・メールは賞与支払い、請求書支払い等を装うなりすましメールであり、**サプライチェーンを通じた標的型攻撃**であった。

4-1. WEBサイトで拾ったWi-Fi脅威の事例：オリンピック編

WiSAS
Wi-Fi Security Assurance Series

オリンピック編（2016年）

世界で最も危険なWiFiスポットは**リオ五輪**　「ハッカーの祭典」状態に
https://forbesjapan.com/articles/detail/13194

オリンピック編（2018年）

平昌冬期五輪を、さらなるサイバー攻撃が襲った――マルウェア「Olympic Destroyer」の正体！
https://wired.jp/2018/02/16/olympic-destroyer-malware/

オリンピック編（2020年）

東京五輪の妨害狙い、ロシアがサイバー攻撃　英政府が発表！
https://www.bbc.com/japanese/54610569

オリンピック編（総括）

進化する五輪へのサイバー攻撃の推移！
https://home.kpmg/jp/ja/home/insights/2019/09/cyber-olympic-highly.html

オリンピックはハッカーの祭典

オリンピックのような世界が注目するイベントは、悪意のあるハッカーにとっても祭典です。
自己顕示欲もさることながら、ブラックマーケットでは展示会場化して、不正取引の場、あるいは
情報の刈取場にもなっているとセキュリティアナリストが警告しています。
その後の企業への影響は、計り知れないものがあろうかと思います。

4-2. WEBサイトで拾ったWi-Fi脅威の事例：侵入手口

WiSAS
Wi-Fi Security Assurance Series

Wi-Fiルータのハッキング

米中央情報局（CIA）が、長年にわたり無線ルータをハッキング
https://japan.cnet.com/article/35102901/

感染スマホを“踏み台”にマルウェア拡散

巧妙化する「Roaming Mantis」の手口 （お客様の荷物が不在で・・など）
https://www.itmedia.co.jp/news/articles/2003/17/news018.html

BYOD端末が狙われたNTTコミュニケーションズ

BYODとして使用していた社員の私用端末から正規のアカウントを盗用！
https://piyolog.hatenadiary.jp/entry/2020/07/03/180308

Wi-Fiアプリから情報入手

公衆Wi-Fiのリストアプリから、200万件以上ものユーザー／パスワードの情報が漏れていた。
https://cybersecurity-info.com/news/wi-fi-information-leak/

iPhoneを簡単に乗っ取れる脆弱性(AirDrop)

iPhoneの安全神話崩壊：今すぐ最新版へアップデートを！
https://news.mynavi.jp/article/20201203-1552764/

メルアカ奪われ、マルウェア付迷惑メール

社員のメールから、情報搾取となりすましメール
https://cybersecurity-jp.com/news/44908

16

4-3. WEBサイトで拾ったWi-Fi脅威の事例：インシデント

WiSAS
Wi-Fi Security Assurance Series

最近の傾向：Dive(潜行)⇒Spread(蔓延)⇒Explosion(爆発)

サイバー攻撃発覚に平均383日？
https://www.sbbit.jp/article/bitsp/46287?ref=201207btsw#continue_reading

三菱電機で不審な端末通信

三菱電機は、社内で使っていた端末で不審な通信が行われていることを確認。！

https://www.itmedia.co.jp/news/articles/2001/20/news085.html

流出情報は闇市場で取引　企業へのサイバー攻撃相次ぐ

個人情報などの重要な情報は商品として売買（国内の法律では取引自体を罪に問えない）
https://www.itmedia.co.jp/news/articles/2003/17/news018.html

ホンダへのサイバー攻撃

事前に内部に侵入するなどして周到に準備
https://www3.nhk.or.jp/news/html/20200615/k10012471271000.html

他：マリオットホテル、カプコン、神戸製鋼、日経、NTTコミュニケーションズ、、などなど多数。

Emotet がWi-Fi 経由で拡散（IcedIDにも注意）

ボットネットの Emotet が、最近Wi-Fi ネットワークを通して拡散できるように進化！
https://www.watchguard.co.jp/security-news/emotet-evolves-to-gain-the-wi-fi-attribute.html

5. 情報セキュリティ10大脅威の推移 （IPA発表資料より抜粋）

WiSAS
Wi-Fi Security Assurance Series

“脅威の変遷・トレンド”

<2018年>

順位	組織	昨年順位
1位	標的型攻撃による被害	1位
2位	ランサムウェアによる被害	2位
3位	ビジネスメール詐欺による被害	ラン
4位	脆弱性対策情報の公開に伴う悪用増加	ラン
5位	脅威に対応するためのセキュリティ人材の不足	ラン
6位	ウェブサービスからの個人情報の窃取	3位
7位	IoT機器の脆弱性の顕在化	8位
8位	内部不正による情報漏えい	5位
9位	サービス妨害攻撃によるサービスの停止	4位
10位	犯罪のビジネス化（アンダーグラウンドサービス）	9位

<2019年>

順位	組織	昨年順位
1位	標的型攻撃による被害	1位
2位	ビジネスメール詐欺による被害	3位
3位	ランサムウェアによる被害	2位
4位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW
5位	内部不正による情報漏えい	8位
6位	サービス妨害攻撃によるサービスの停止	9位
7位	インターネットサービスからの個人情報の窃取	6位
8位	IoT機器の脆弱性の顕在化	7位
9位	脆弱性対策情報の公開に伴う悪用増加	4位
10位	不注意による情報漏えい	12位

“内部不正による情報漏えいが激増”
“Wi-Fi が絡む事件が多発”

<2020年>

順位	組織	昨年順位
1位	標的型攻撃による機密情報の窃取	1位
2位	内部不正による情報漏えい	5位
3位	ビジネスメール詐欺による金銭被害	2位
4位	サプライチェーンの弱点を悪用した攻撃	4位
5位	ランサムウェアによる被害	3位
6位	予期せぬIT基盤の障害に伴う業務停止	16位
7位	不注意による情報漏えい（規則は遵守）	10位
8位	インターネット上のサービスからの個人情報の窃取	7位
9位	IoT機器の不正利用	8位
10位	サービス妨害攻撃によるサービスの停止	6位

6-1. 身近なWi-Fi脅威の事例（当社調査）

WiSAS
Wi-Fi Security Assurance Series

某国立研究開発法人

人命が絡む最重要セキュリティエリアでは、厳密なルールがありながら全国から研究者が集まる組織故に形骸化していた。センサーによるWi-Fiセキュリティの脆弱性診断をしたところ、私物のWi-Fiによる**テザリング**や**ポータブルWi-Fi**の利用が多く散見された。

某大手製造メーカー

情報漏えいの原因調査の一環でセンサーによるWi-Fiセキュリティ診断をしたところ、内部ネットワークサーバーに接続された**超小型の無線AP**が発見された。監視カメラの映像から社内の人間が賄賂をもらって**産業スパイ行為**を助力していたことが判明した。

某大手BPO事業会社

取引先の重要な金融データを預かる業態故にPCI DSSに準拠し、3カ月に一度ウォークスルー検査を実施していたが、念のためセンサーによるWi-Fiセキュリティ診断をしたところ、**ポータブルWi-Fi**の利用が数件あり、その後の調査でお客様のデータを**個人のiCloudにアップ**していたことが判明した。

某大手データセンター

定期的にウォークスルー検査を実施していたが、センサーによるWi-Fiセキュリティ診断を実施した。結果、サーバールーム内に意図せず有効化された**電話ルータWi-Fi**を発見。同時にサーバールーム入室時にロッカーに預けたスマホのテザリングをONにし、最重要セキュリティエリアでの作業を確認。

6-2. 身近なWi-Fi脅威の事例（当社調査）

WiSAS
Wi-Fi Security Assurance Series

某大手デジタル放送配信会社

Wi-Fi 関連機器のBYODに対してルールはあったものの、PCI DSS準拠の前段階でセンサーによるWi-Fiセキュリティの脆弱性診断をしたところ、私物スマホによるテザリングやポータブルWi-Fiへ会社貸与のPC接続が多くみられた。

某大手デジタル放送配信会社

センサーによるWi-Fiセキュリティ診断をしたところ、社内に意図せず有効化されたWi-Fi Direct機器が複数検知された。ネットワークに接続不要なものはOffにし、必要なものはデフォルトのPWDからユニークなものへ変更した。（プリンター、スキャナー、プロジェクター）

某大手デジタル放送配信会社

Wi-Fi不調の原因として無線DoS攻撃の可能性が浮上したのでセンサーによる診断を実施した。
結果、社員が無許可で持ち込んだ「粗悪」なポータブルWi-Fiが、BeaconFlood(DoS攻撃の一種)を行っていたことが判明。

某大手デジタル放送配信会社

センサーによるWi-Fi不調の原因調査や脆弱性診断で、BYOD（スマホやポケットWi-Fi）やWi-Fi Directの機器の位置分析を実施。悪意なき社員のIT武装に対し、ルールの徹底を図り、情報漏えいの原因になりえる要素を排除した。

6-3. 身近なWi-Fi脅威の事例（当社調査）

WiSAS
Wi-Fi Security Assurance Series

大手Sier & セキュリティ調査会社など

セキュリティを生業とする企業において、自社のWi-Fi脆弱性診断に疑問を感じ、センサーによるWi-Fi脆弱性診断を実施。結果、**持ち込みWi-Fi端末**を多数検知、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、プロジェクター、スキャナー）、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の誤接続を確認した。

某大手ホテルチェーン

ホテルを中心に狙った「**ダークホテル**」というマルウェアが未だに蔓延しているところから、某大手ホテルチェーンにおいて、なりすまし調査を実施。結果、ラウンジスペースにて**なりすましAP**を発見。

ダークホテルの感染源の2/3は日本からという調査結果。

https://wired.jp/2014/11/12/darkhotel-uses-bogus-crypto-certificates-to-snare-wi-fi-connected-execs/

某大手旅行会社

ホテルにおけるなりすまし事件の報道から、実態調査のためディスカッション。Wi-Fiセキュリティの重要性を認識して頂くため、弊社社員があえてなりすましAPを作成。MTG終了後には、出席者の数人がその**なりすましAPに接続**していた。

6-4. 身近なWi-Fi脅威の事例（当社調査）

WiSAS
Wi-Fi Security Assurance Series

某国立研究開発法人

入室前にAPになり得るものはロッカーに預ける、あるいは申請するという厳密なルールがありながらも不特定多数の出入りがある現場ゆえに、常に監視し、電波の発信元を分析し、対処する必要性が生まれ、断面的な人手による監視ではなく、センサーによる**常時監視**を導入。

某大手ビジネスプロセスアウトソーシング事業会社

センサーによるWi-Fiセキュリティ診断の結果から、**常時監視**のシステムを導入。社内に告知徹底をしたせいもあって、その後は私物のスマホテザリングやポケットWi-Fiの持ち込みがなくなった。
PCI DSSの監査でも高評価を得られた。

某大手クレジットカード会社

全国主要十数拠点において、PCI DSSに準拠するため、要件11.1に則り3カ月に一度、有人ウォークスルー検査を実施していた。Wi-Fiの脆弱性を認識はしていたものの、調査員の対応にムラがあり、しかも断面的な調査ではいつ情報漏えいが発生してもおかしくない状況を憂慮していた。
また、**パンデミック**な状況故に人の移動が制限され、3カ月に一度の調査ルールを守れなくなった。
そこで、センサーによってWi-Fi 環境を常時監視する方法に切り替え、不正なものを**即検知**すると同時に**即対応**できるセキュアな環境を構築した。

WiSAS
Wi-Fi Security Assurance Series

「なりすましAP」はハッカーでなくても容易に構築が可能。

- ✓ 不正APもネットで手軽に購入できる時代（価格は数万円、納期は数日）
- ✓ 不正APの使い方も動画サイトで公開されている

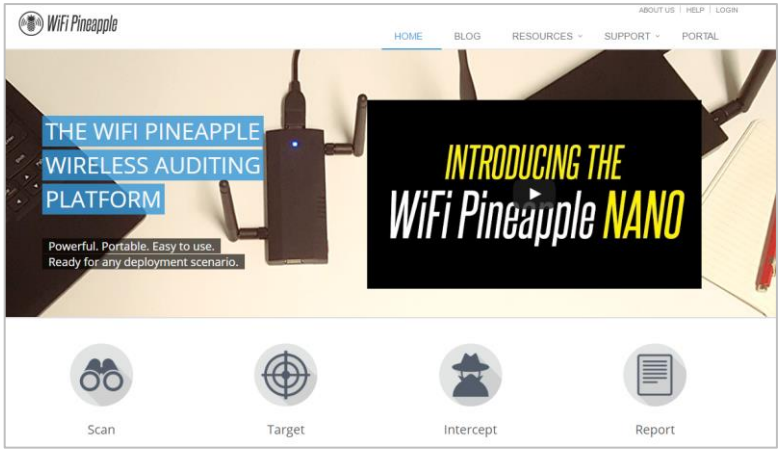
不正AP

2018年に登場

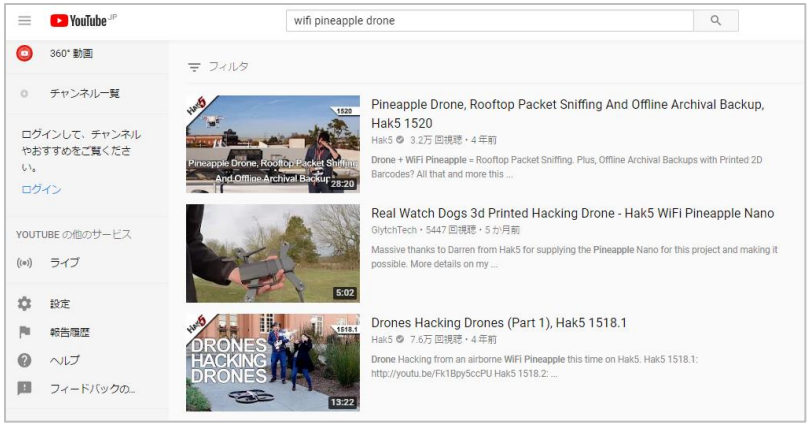
Wi-Fi Pineapple

ドローン型不正AP

不正APの購入WEBサイト

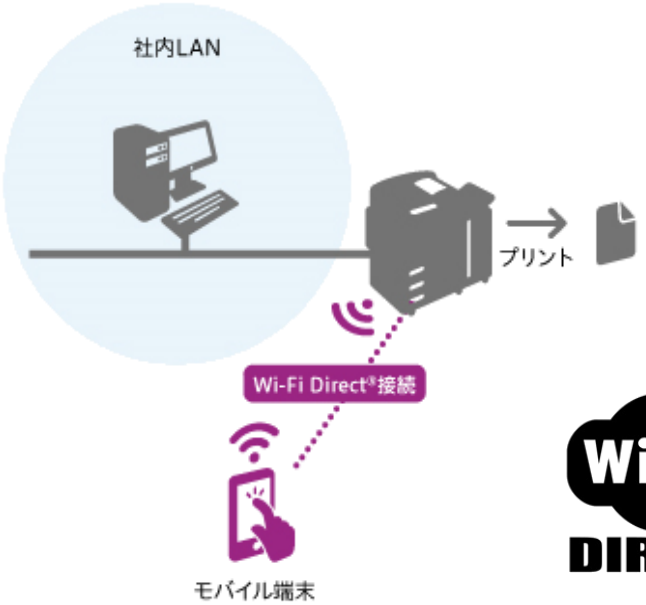


ドローン型不正APの使い方動画サイト



WiSAS
Wi-Fi Security Assurance Series

Wi-Fi Directの脆弱性と脅威



Wi Fi DIRECT™

身近にあるWi-Fi Directの多様性

https://www.wi-fi.org/ja/discover-wi-fi/wi-fi-direct

24

WiSAS
Wi-Fi Security Assurance Series

~1st Step : PLAN~

1、情報漏えい手口のトレンド把握と対策調査
- 進化するハッキング手法と防衛手段の動向調査

2、Wi-Fi脆弱性チェックポイントの見極め
- すべてのAP　・すべての端末　・非認可端末　・不正行為端末
- なりすましAP　・MAC偽装AP　・ Wi-Fi Direct AP
- ハッキングデバイス　・誤設定AP　・Fake AP　・不正接続AP
- WDS AP　・ソフトAP　・アドホック・ネットワーク
- 無線DoS攻撃…etc.

3、自社内セキュリティ施策の把握
- 様々な脅威のカテゴリー化と施策の照らし合わせ
- 有線ネットワークと無線ネットワークの対処方法の違いの認識

4、ホワイトリストの整備
- 警戒する必要のない管理されたデバイス
- 正規の認可AP、端末のリスト化

WiSAS
Wi-Fi Security Assurance Series

~2nd Step：ACTION~

1、Wi-Fi脆弱性診断方法の調査

- チェックポイントを網羅できていること
- 検知だけでなく対策まで一貫してできること
- 調査の深度
  （AP、MAC Address、ベンダー、SSIDと分類、認証方式、
  （暗号化プロトコル、チャンネル、dBm、接続状況…etc.）
- 的確な診断方法と迅速な初動対応力
- 調査継続性の容易さ

2、Wi-Fi脆弱性診断の実施

- Wi-Fi環境の把握＝可視化
- チェックポイントの確認と期間
- 社内に存在するAPや端末の把握と接続状況の把握

DEMO：Wi-Fi環境スキャンの結果！

WiSAS
Wi-Fi Security Assurance Series

~3rd Step：分析~

1、警戒する必要のないものと警戒すべきものの仕分け
- ホワイトリスト／ブラックリストの整理
- グレー（未確認ＡＰ／端末）の判別方法
- 管理されていないAP／端末の有無と通信状況（含：野良）
- 不正行為APと不正行為端末のリスト化

2、Wi-Fセキュリティポリシー策定
- セキュリティを担保する上での必要十分条件
- 有線ネットワークと無線ネットワークの対処（BYOD等）

3、意識改革／社員教育
- 意図せず加害者になるリスク

（例）
本当は怖いテザリング　リスクと対策は
https://techtarget.itmedia.co.jp/tt/news/1812/22/news01.html

無線LANの”抜け穴”から機密情報がダダ洩れ！塞ぐ有効な対策とは？
https://www.ntt.com/bizon/cloud-wifi.html

WiSAS
Wi-Fi Security Assurance Series

～常時監視の必要性～

1、サイバーテロの傾向
- Dive（潜行）⇒Spread（蔓延）⇒Explosion（爆発）

2、Wi-Fiの脅威は、いつ発生するかわからない
- クレジット業界の例・・・PCI DSS要件11.1
  最低でも3カ月に一度？でいいのか？
  検査日は秘密：外部に漏れたら翌日狙われる可能性

3、断面的な調査ではなく、24H365D常時監視の必要性

4、Wi-Fiセキュリティポリシーの徹底
- 対処療法ではなく、即時検知即時対応
- リアルタイム監視とリアルタイム対応がベスト
- 検知：WIDS（Wireless Intrusion Detection System）
- 防御：WIPS（Wireless Intrusion Prevention System）

5、脅威の判定基準の標準化
- パンデミックやディザスター時も視野に！

WiSAS
Wi-Fi Security Assurance Series

サイバー犯罪の隠れたコスト

~米国の戦略国際問題研究所（CSIS）とマカフィーの共同調査　12/8~

マカフィーと米国の戦略国際問題研究所(CSIS)によると、サイバー犯罪が与えた**経済損失は世界のGDPの1%超に相当する1兆ドル(約104.6兆円)以上**だという。これは**2018年調査(約6,000億ドル 約62.7兆円)の1.5倍超**。また、対象企業の92%がそれ以外にも大きな影響を感じている。

経済的損失以外の隠れたコストは「システムのダウンタイム」、「効率の低下」、「インシデント レスポンス コスト」、「ブランドと風評被害」。

また、日本はダウンタイムが世界平均よりも1時間長く、関連コストが世界で最も高い約120万ドル(1億2千万)だったことが判明、ただし2019年度中にインシデントを経験しなかった企業が日本では40%と、世界平均の26%、米国の18%と比較すると、日本は攻撃対象とされる機会が比較的低い可能性が考えられる。

https://scan.netsecurity.ne.jp/article/2020/12/10/44927.html

ご清聴、ありがとうございました。

本資料に関する詳細な説明／お問い合わせは下記までお願いします。

電話：03-5464-5468

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

会社URL：https://www.spline-network.co.jp

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

- **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** 〒150-0033
  東京都渋谷区猿楽町2-13
  F93 Daikanyama 5F
- **設立日** 2002年 1月 11日
- **資本金** 9401万円