Deloitte.
デロイト トーマツ

“足下”セキュリティは大丈夫？

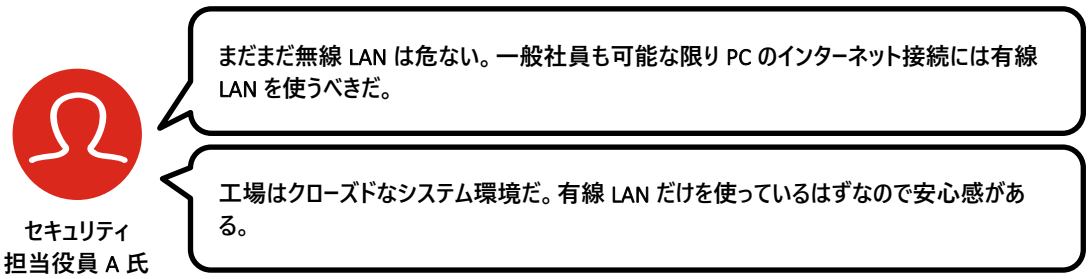
～無線 LAN と有線 LAN のセキュリティ～

身の回りのネットワークに潜む脅威とは

突然だが『身の回りのネットワーク環境』について正しく把握しているだろうか。自身のネットワーク環境をあまり意識せずに利用している方も多いのではないだろうか。

昨今、オフィスでは無線 LAN が設置、運用されていることは一般的な状況となっている。サイバーセキュリティに関する代表的なカンファレンスでは例年無線 LAN について多くのハッキング手法や脆弱性が発表されており、無線 LAN のセキュリティは我々の業界内ではホットな話題と言える。

このような世間の動向もあり、無線 LAN のセキュリティは注目を浴びている。そのため、対策をしっかり行っている企業も多いことだろう。しかしながら、無線 LAN に対する漠然とした不安から、次のような意見も少なくないと実感している。



上記の意見の通り、確かに有線 LAN であれば、無線 LAN と異なり LAN ケーブルが目に見えるため、漠然とした無線 LAN の不安は払拭できるだろう。では、本当に有線 LAN であれば安心して利用できるだろうか。

本稿では、まず無線 LAN のセキュリティリスクについて解説し、漠然とした不安をクリアにした後、A 氏の発言の妥当性について考察する。そして有線 LAN に潜むリスクと対策例にも視野を広げ、最終的には、有線 LAN 運用のポイントについてまとめる。さらには、企業におけるネットワークの運用を担当している方にインターネット環境を改めて見直してもらうことに加え、セキュリティ意識を高めてもらうことを期待したい。

無線 LAN におけるセキュリティリスク

『無線 LAN のセキュリティ』と聞いて漠然とした不安を抱く人は少なくないだろう。そのため、有線 LAN の設置を推奨し、無線 LAN の導入を見送るオフィス環境も少なくない。そこで、まずは、実際に無線 LAN のハッキング方法を実際に知ることで一旦思考をリセットし、ゼロベースで検討してみたい。そこで、まずは次の 2 つの攻撃事例を紹介する。

① Wi-Fi スニッフィング

Wi-Fi を攻撃する代表的な手法として、『スニッフィング（嗅ぎまわり行為）』がある。

外部の攻撃者が、攻撃対象のハードウェア（機器）である AP（Access Point）の通信を不正に盗聴・収集し、パスワードのクラックやデバイス情報などの収集を行うものである。本攻撃手法を実現可能とするツールがネット上に複数公開されており、特殊なハードウェアなど必要なく、PC さえあれば比較的手軽に攻撃を実施できてしまう。

② Wi-Fi スポットのなりすまし

情報を傍受し、不正に窃取する方法として、偽の AP を用いて高度に攻撃を実施する『Wi-Fi スポットのなりすまし』がある。

ファーストフード店などが提供している Wi-Fi と自宅の Wi-Fi の電波を見分けるためには、SSID（Service Set Identifier）に店名を入れるといったように、区別可能な ID 設定することが多い。その ID と全く同じものを設定した AP を設置した場合、周囲のユーザはどちらが真の AP か判断できず、接続してしまう可能性が高い。

このように AP の SSID をなりすまし、周囲のアクセスしたユーザの通信内容などを傍受し、そこから不正に個人情報の奪取などを試みる攻撃が、この「Wi-Fi スポットのなりすまし」である。この攻撃はまるで同じ AP が 2 つ存在してしまうことから、『悪魔の双子攻撃』と呼ばれることもある。

では、上述した無線 LAN における、2 つの攻撃事例に伴うセキュリティリスクについては、有線 LAN を利用することで、果たして回避できるのだろうか。上記①の攻撃手法については、有線 LAN を用いるとそもそも外部の攻撃者はその通信を遠隔で傍受できなくなるため回避できる。また、上記②の攻撃手法についても、有線 LAN であれば、設置されている LAN ポートが正規のものであるか、目視で判断できるため、こちらも遠隔からの盗聴のリスクは回避できる。そのため、冒頭で紹介した A 氏の発言は正しいように思える。

しかしながら、実態としては、有線 LAN によるネットワークを構築するだけでは、セキュリティ対策としては決して十分とは言えない。なぜなら、有線 LAN にも固有の弱点もあるからだ。次に、有線 LAN に潜むリスクを洗い出し、その理由について掘り下げていく。

有線 LAN の仕組み

普段利用するインターネット環境では有線 LAN はどのように利用されているだろうか。例として、一般的なオフィスなどの有線 LAN によるネットワーク環境を（図 1）に示す。

有線 LAN は PC 同士や、その他ネットワーク機器同士を LAN ケーブルで接続することによって通信を行う。また、ネットワークスイッチ（以下、スイッチ）と呼ばれるネットワークを管理する機器がネットワーク切分けなどを担っており、各通信を束ねている。このスイッチに、ルータと呼ばれるネットワークの経路を制御する機器や、PC などが接続されている。このようにして、有線 LAN によるネットワーク環境は構築されている。

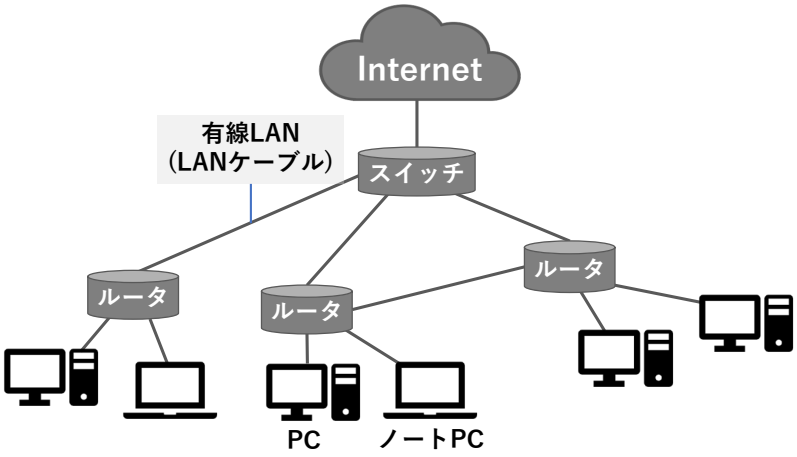


図 1　一般的な有線 LAN によるネットワーク環境

有線 LAN に潜むセキュリティリスク

次に、前述の仕組みを前提とした上で、私たちの“足下”にある有線 LAN における見落としがちなリスクについて紹介する。本稿ここでは、有線 LAN に関する 2 つの侵入方法について、ネットワークの管理を行うスイッチからの侵入と、LAN ケーブルからの侵入について取り上げてみたい（図 2）。

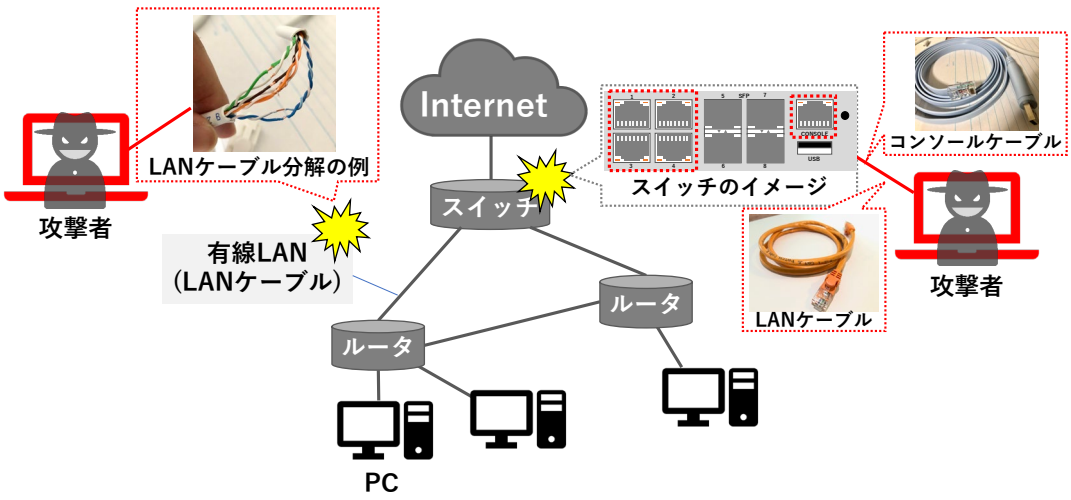


図 2　一般的な有線 LAN を含むネットワーク環境における侵入方法のイメージ

① ネットワークスイッチの空ポートからの侵入

有線 LAN を含むネットワーク環境における大きなセキュリティリスクとして、ネットワーク上にある様々な機器における空ポートからの侵入の恐れがある。その代表的なネットワーク上の機器の一つがスイッチである。

スイッチが設置される位置はネットワーク構成上、セグメントを管理するため比較的重要な箇所に設置されていることが多い。このスイッチには一般的に直接管理者がアクセスすることのできる『コンソールポート』と呼ばれる接続口がある。管理者は、設定変更などの際には、直接ノートパソコンなどとコンソールポートを、コンソールケーブルと呼ばれる特殊なケーブルで接続する。

設定などは型番などで検索をかけるとリファレンスが公開されており、各種設定情報変更や、接続機器の情報を取得するためのコマンドは誰でも知ることができる。そのため、ネットワーク上の機器の把握はもちろん、設定変更によるネットワーク経路の切断や外部への不正なデータ送信など様々なことが可能となってしまう。

スイッチは通常サーバ室などに設置されており、人の監視が常時行き届いていないスイッチは多いと考えられる。もしこのスイッチのコンソールポートへのアクセスが放置されている場合は非常に危険である。同様に、スイッチにある LAN ポートについても放置されている場合は、攻撃者による不正アクセスを容易に許してしまう危険がある。

② LAN ケーブルの改造による侵入

ネットワーク上の機器からではなく、LAN ケーブルから直接侵入される恐れもある。それは、LAN ケーブルが銅軸であるため、分解し、物理的および電気的に接続することで侵入・盗聴される可能性である。簡単な分解工具などがあれば実施可能であるため、非常にシンプルな攻撃である（図 3）。

攻撃者は、はじめに侵入箇所とする LAN ケーブルの周り、および内部の銅軸ケーブルの皮膜を剥がして銅線をむき出しにする。このむき出しにした銅線を、攻撃者側の細工した LAN ケーブルと電気的に接続することで攻撃者は盗聴が可能となる。
その状態で、攻撃者 PC 側でパケットモニタリングツールを用いると、接続先 URL の入手や通信先 IP アドレスなどが窃取されてしまう恐れがある。

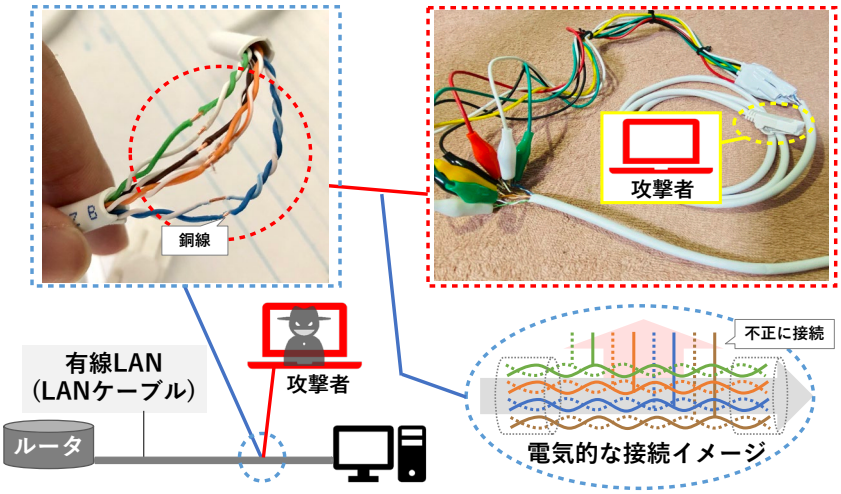


図 3　LAN ケーブルからの侵入イメージ

有線 LAN 運用におけるポイントのまとめ

以上のように、有線 LAN にも固有のセキュリティリスクがあることがわかる。有線 LAN の環境において必要となる対策について以下の（表 1）にまとめる。

ソフトウェアの観点では、設定環境へのログインを強固なものにすることや、不正な設定変更を検知する仕組みを導入することが有効である。

ハードウェアの観点では、物理的にコンソールポートへのアクセスを防ぐことや、そもそも LAN ケーブルを露出しないことが有効である。さらに、現在の各機器の使用状況や設置場所の状況を常に管理し、監視カメラや入退室記録による状況の可視化、定期的な状況の確認と点検によって、早期に攻撃を検知可能になり、セキュリティリスクを低減することができる。

表 1　これまでに紹介した有線 LAN ネットワークに対する侵入方法と対策例

	ネットワーク管理者対策	
	ソフト	ハード（物理）
ネットワークスイッチの コンソールポートからの侵入	①コンソールログイン設定を強固なもの（デフォルトではないもの）に変更する ②経路の変更などを検知できる仕組みを導入しておく	①コンソールポート（その他のLANポートも同様）にRJ45コネクタブロッカー*をつける ②設置場所への部屋や場所において鍵、監視カメラ、入室の記録などを実施
LANケーブルの改造による侵入	①通信内容と暗号化の実施状況を把握しておく（リスクを事前認識しておく） ②暗号化通信を使う（VPNなど） ③接続断などを検知できる仕組みを導入する	①LANケーブルを天井や床下に配線する（露出しないようにする） ②露出する場所は監視カメラなどによる記録や、定期的な検査を実施

＊… 大手ショッピングサイトなどで一般的に販売されており、ポートの悪用防止や鍵をかけられるものが存在

このように、有線 LAN を利用することで無線 LAN におけるセキュリティリスクについては回避できるものの、有線 LAN にも固有のセキュリティリスクが存在するのである。

以上を踏まえて、それぞれの攻撃事例及びセキュリティリスクを（表 2）にまとめる。単に「有線 LAN を利用すれば安心」という考え方では、対策として不十分である。有線 LAN を活用する場合、敷設や運用における管理をせず、それらを放置してしまうことが何より危険である。そのため、有線 LAN の適切な運用と管理といった対策を実施していただきたい。

表 2　無線 LAN と有線 LAN におけるセキュリティリスク

	無線LAN	有線LAN
攻撃事例	Wi-Fiスニッフィングや Wi-Fiスポットのなりすまし	ネットワークスイッチの空ポートからの侵入やLANケーブルの改造による侵入
セキュリティリスク	遠隔からの通信アクセスによる個人情報などの情報窃取・盗聴	物理的アクセスによるネットワークへの不正アクセス、及び情報窃取・盗聴

最後に

本稿では無線 LAN と比較して、一見安全に見える有線 LAN のセキュリティリスクについて紹介した。しかし、上述の表で整理した通り、有線 LAN には、無線 LAN のような遠隔からの盗聴リスクはないものの、有線 LAN 固有のセキュリティリスクがあり、物理的アクセスによる侵入や盗聴の恐れがある。

有線 LAN もしくは無線 LAN どちらか一方のみを採用したネットワークの構築は、関係しうる脅威を鑑みると、結果的にはリスクが残ってしまう。「有線 LAN なら安心」という過信も禁物である。結論としては、双方の特性を踏まえた適材適所な利用と、それらの適切な運用と管理が肝要となる。

以上を踏まえ、冒頭の A 氏には次のような発言を期待したい。

セキュリティ
担当役員 A 氏

クローズドなシステム環境だからといって、有線 LAN は絶対的に安心ではない！無線 LAN と有線 LAN それぞれの特性を鑑みて、よりリスク低減効果が期待できるネットワーク環境の運用と管理を検討しよう。

A 氏には勘違いや思い込みがあったが、今一度現状を把握し、セキュリティリスクを特定することで、適切なネットワークの運用を指示することが必要である。そのため、まずはネットワーク環境に関する現状の把握からが始めていただきたい。その上で、有線・無線の特性を踏まえた、適切なセキュリティ対策を検討いただくことを期待したい。

デロイト トーマツ サイバー合同会社
Mail　ra_info@tohmatsu.co.jp
URL　www.deloitte.com/jp/dtcy
【国内ネットワーク】　東京・名古屋・福岡

※貴社および貴社の関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、本サービス　内容がご提供できない可能性があります。詳細はお問合せください。

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT 弁護士法人およびデロイト トーマツ コーポレート ソリューション合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約 30 都市以上に 1 万名を超える専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループ Web サイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよびそれらの関係法人はそれぞれ法的に独立した別個の組織体です。DTTL はクライアントへのサービス提供を行いません。詳細は www.deloitte.com/jp/about をご覧ください。
デロイト アジア パシフィック リミテッドは DTTL のメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける 100 を超える都市（オークランド、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務およびこれらに関連するプロフェッショナルサービスの分野で世界最大級の規模を有し、150 を超える国・地域にわたるメンバーファームや関係法人のグローバルネットワーク（総称して“デロイトネットワーク”）を通じ Fortune Global 500®の 8 割の企業に対してサービスを提供しています。“Making an impact that matters”を自らの使命とするデロイトの約 312,000 名の専門家については、（www.deloitte.com）をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

Member of
Deloitte Touche Tohmatsu Limited

© 2020. For information, contact Deloitte Tohmatsu Cyber LLC.