基本のキ。セキュリティ入門（第7回）

社内ネットワークを構築する手順や構築時のポイント

2020.12.28



業務を円滑に進めるには、社内のパソコンやプリンターなどの機器を接続する社内ネットワークが非常に重要です。いまや大小の違いはあっても、どのような企業も社内ネットワークを構築したうえで業務を行っているケースがほとんどでしょう。

一方で、これから新しく社内ネットワークを構築したい、現在の社内ネットワークを見直したいという方も多いのではないでしょうか。

この記事では、社内ネットワークの概要から構築する手順、構築の際の注意点を解説します。

社内ネットワークとは？

社内ネットワークは企業内で利用するローカルなネットワークを表します。従業員が利用するパソコンやプリンターなどの機器を接続し、データ通信するためのネットワークです。

ネットワークの規模や利用できる仕組みには、いくつか種類があります。

＜有線・無線LANを利用したローカルネットワーク＞
社内ネットワークを構築する際、はじめに考えるべきはLAN（Local Area Network）です。LANはインターネットとは異なるローカルなネットワークで、敷地内や建物内など範囲が限定されます。

LANには、パソコンなどの機器同士を接続するためにケーブルを利用する有線LANと、Wi-Fiなどの無線通信を利用する無線LANが存在します。LANを構築する際には、接続する機器の種類や台数、従業員の利便性、機器の導入コストなどを考え、有線・無線を選択するとよいでしょう。

＜WANを利用した広域ネットワーク＞
WANとはWide Area Networkの略称で、LANよりも広域のネットワークを表します。フロア内やビル内で構築するLANとは異なり、WANは本社と支社（各拠点）のパソコン同士をつなげる仕組みです。

WANを利用することで、遠く離れた本社と拠点間でも同一フロア・ビル内にいるようにネットワークが利用できます。なお、LANは自社内で完結するネットワークですが、WANは距離が離れた場所と接続するので、通信事業者が提供するネットワークを利用します。

社内ネットワークを構築する手順について解説



社内ネットワークは主にLANで構成され、必要に応じてWANを利用します。構築する際にはどのような手順を踏むのでしょうか。ここでは、社内ネットワークを構築する際の手順を簡単にご紹介します。

＜ステップ1.現状調査＞
はじめに行うのは自社の現状調査です。新規に社内ネットワークを構築する場合はもちろん、既存の社内ネットワークを再構築する場合でも、自社が現状抱えるネットワークの問題点や実現したいことを明確にしましょう。

例えば、従業員のほとんどがノートパソコンを利用し、フロア間の移動が多い企業で有線LANによる社内ネットワークを構築してしまうと、利便性の損なわれた社内ネットワークになってしまいます。構築した後に困らないよう、まずは問題点を洗い出す作業が必要です。

＜ステップ2.要件定義＞
現状調査の結果を基に、自社で必要なネットワーク環境の要件を細かく定義していきます。

例えば、ネットワークでつなぐ拠点の数やユーザー数、扱うデータの種類、必要な回線速度、有線LANか無線LANかなど、具体的な要件を明らかにしましょう。他にも、個人で使う端末の有無や使用するアプリケーションの優先度、専任技術者の必要性、コストなどの基本方針を定めておくと、構築作業がスムーズに進みます。

＜ステップ3.システム設計＞
要件定義に従って社内ネットワークのシステム設計を行います。システムの設計は、物理的な機器の設計とデジタル部分の設計に大きく分けられます。

ネットワークはシステムにおける根幹部分なので、一度構築すると変更には多大な労力を要します。加えて、セキュリティ対策を講じる必要もあり、利便性が損なわれないように安全なネットワークの設計が求められます。

複雑なシステム設計は問題が発生しやすくなります。できるだけシンプルな設計を心がけるとよいでしょう。

＜ステップ4.運用管理体制を整える＞
社内ネットワークの構築後は、主に通常時、システム更新時、トラブル発生時の対応が求められます。社内ネットワークは業務を円滑にする基幹システムなので、常に迅速な対応ができるように運用体制を整えましょう。

具体的には、運用管理の専用ツールや外部のソリューションを利用するのが有効です。社内ネットワークにつなげている機器を把握しやすく、ソフトウエアやセキュリティシステムの更新、通信状況のチェックが効率的に行えるため、安定したネットワークの運用につながります。

＜ステップ5.運用管理マニュアル化＞
運用管理の専用ツールやソリューションの導入ができたら、社内ネットワーク運用管理のマニュアル作成を進めましょう。新規購入したパソコンをネットワークにつなげる際や、通信に遅延が発生した場合などの対応手順をマニュアル化しておくと、スムーズな運用管理が可能です。

特に、ネットワーク障害などの深刻な状況では、運用管理業務が属人化していると対応に遅れが発生し、企業にとって大きな損失につながる可能性があります。マニュアル化することで誰でも対応ができ、ダメージを最小限に抑えられるでしょう。

社内ネットワークを構築する際に注意しておきたいこと

安全で快適な社内ネットワークを構築するために、あらかじめ注意しておくことは次の4つです。

＜1.社内ネットワークのセキュリティ対策＞
社内ネットワークは企業内での限られたネットワークですが、多くの場合はインターネットに接続できるように構築するため、注意したいのはセキュリティ対策です。

インターネット上には企業内の情報を狙う第三者や、不正なソフトウエアであるマルウエアが存在します。社内ネットワークのセキュリティ対策としては、悪意のあるアクセスからネットワークを守るために、ファイアウォールやIDS/IPSといった侵入検知・防止システムを導入します。

さらに、社内の重要データが外部に漏れないように、従業員が利用するパソコンにアンチマルウエアソフトを導入したり、メールの誤送信防止のソリューションを導入したりするなど、セキュリティ強度を高めましょう。

＜2.社内のセキュリティ教育を進める＞
社内ネットワークのセキュリティ対策としては、システム的な対策だけでなく従業員一人ひとりのセキュリティ意識の向上も欠かせません。どれだけシステム的に対策を行っていても、従業員のセキュリティ意識の低さや情報リテラシーの欠如から発生するセキュリティトラブルは避けられないからです。

近年、セキュリティソフトだけでは防げない標的型攻撃メールによるトラブルが多数報告されています。セキュリティ教育に取り組んで従業員のリスクある行動を軽減し、企業全体のセキュリティを強化しましょう。

＜3.ユーザーにとって使いやすいシステムの構築＞
社内システムの利便性が損なわれると業務に支障をきたすため、社内ネットワークを利用するユーザー（従業員）にとって使いやすいネットワークシステムを構築するのが非常に重要です。

従業員が使いやすいシステムを構築するには、業務の実態を細かく把握する必要があります。具体的には現場へのヒアリングや、業務フローの分析などの対策が有効でしょう。

成長中の企業なら、将来的に従業員数が増えてネットワークの規模を大きくする必要があるかもしれません。現状から将来像まで想定したうえで、従業員にとって使いやすい社内ネットワークを構築しましょう。

＜4.トラフィック量に合わせたネットワーク設計・環境構築＞
ネットワークでやり取りするデータのトラフィック量（通信量）は、ネットワークを設計する際にしっかりと把握しておかなければなりません。

社内ネットワークで利用する機器は、それぞれに対応可能なトラフィック量が定められています。規定の量を超える処理はできず、通信速度の低下や、最悪の場合にはネットワークの通信ができなくなる可能性があります。

そのような事態を防ぐためにも、社内ネットワークのトラフィック量を予測・計測したうえで設計・環境構築するようにしましょう。

社内ネットワークのお困りには！NTT西日本の「フレッツ・SDx」

社内ネットワークは、企業内でパソコンやプリンターなどの機器を接続してデータ通信を行うためのネットワークです。主にLANによって構築され、拠点同士のより大規模なネットワークはWANによって構築されます。

社内ネットワークを構築するには、現状調査と要件定義を行い、セキュリティ対策やユーザーの利便性、トラフィック量を考慮したうえでシステムを設計します。運用管理体制を整えるために、専用ツールの導入やマニュアル化も必要でしょう。

ただし、社内ネットワークの設計・構築には専門的な知識が必要であり、拠点間の通信を実現するWANはLANよりも対応が難しい傾向にあります。中にはこんな悩みをお持ちの方もいらっしゃるのではないでしょうか。

・遅延が発生しにくい安定した拠点間通信を実現したい
・高セキュリティなネットワークを実現したい
・集中的に管理したいがネットワークの規模が大きく、維持管理が難しい

NTT西日本では、低遅延・高セキュリティな拠点間通信を実現する「フレッツ・SDx」を提供しています。フレッツ・SDxはインターネットを介さない閉域網のIP-VPNのため高セキュリティを維持しつつ、フレッツ
光ネクストを利用した高速通信で、映像データなどの大容量データも低遅延で通信可能です。

さらに、遠隔操作が可能なコントローラーを通じて各拠点の機器を自動で設定できるため、ネットワーク管理も効率的に行えます。社内ネットワークにおける拠点間通信でお悩みの方はお気軽にご相談ください。

※掲載している情報は、記事執筆時点のものです