実践セキュリティ特論 I

28G23027
川原尚己

VPN の中にはインターネット VPN とクローズド VPN がある[1]．インターネット VPN では，インターネット回線をそのまま使用し，クローズド VPN では，インターネットを経由せずに物理的・論理的に隔離されたネットワーク上でデータの送受信を行う．
以下に，インターネット VPN とクローズド VPN のそれぞれのメリット及びデメリットを示す．

- インターネット VPN のメリット
  - VPN 装置によって送受信するデータを暗号化することで低コストで利用することができる．
  - インターネットを同時に使用することができる．
- インターネット VPN のデメリット
  - セキュリティ面についてはクローズド VPN の方が優れている．
  - インターネットを経由するためその時々の通信環境に左右されることが多く，トラブルが発生しやすい．
- クローズド VPN のメリット
  - 隔離されたネットワーク上でデータの送受信を行うため，インターネット VPN と比べてセキュリティ強度が高い．
  - ネット環境の影響を受けにくく，安定した送受信を行うことができる．
- クローズド VPN のデメリット
  - 一般的なインターネットに接続されていないため，同時にインターネットを使用することができない．

以上のように，インターネット VPN かクローズド VPN かで性質は大きく異なるため，どのような事業形態で運用するかによって選択することが重要となる．

以下では VPN に関するセキュリティリスクについて考えていく．

- VPN 機器そのものの脆弱性[2]

  VPN ではトンネルのように閉鎖された仮想的な通信路を構築することによって安全性を確保しているが，そもそもこのトンネリングに使用している VPN 機器に脆弱性が存在している場合には攻撃によってセキュリティが侵害される可能性がある．導入を検討している VPN 機器に対し過去の記録等を吟味した後に導入を行うことが重要である．また，現在使用している VPN 機器に脆弱性が発見された場合には，対応パッチを導入し，過去にサイバー攻撃を受けた形跡がないかどうか調査する必要がある．
- テレワーク端末のマルウェア感染

前述のとおり VPN を使用することによって通信路の中に関するセキュリティは保護することができるが，実際に運用を行う場合には通信端末についても安全性を確認する必要がある．もしウイルスに感染した端末を VPN を使用して社内ネットワークに接続してしまった場合には社内ネットワーク全体に感染が広がる可能性がある．
また，VPN ではアンチウイルスソフトのようなウイルスを発見して排除する機能は存在しないため怪しげなサイトを閲覧する等，ウイルスに感染する可能性がある行動は行うべきではない．

このように，VPN を使用する際にも注意すべき点がいくつか存在する．

これらのような問題が発生しないように，VPN に関するセキュリティ強化対策を以下に示す[2].

- 自社に合わせた VPN を選択

  VPN には特徴の異なる 2 つの種類がある．自社の規模や運用形態に合わせて適切な種類の VPN を選択することが重要である．また，低コストで運用できると謳っているサービスの場合は通信が遅かったり，万一トラブルが発生した際の対応が不十分であったり，修復に時間がかかったりと提供内容に問題がある可能性があるため，VPN のサービス内容・サポート体制が自社の規模や用途に見合っているかを調べてから導入を決定すべきである．

- 認証システムの強化

  VPN にログインすると会社の機密情報にアクセスできるため，不正にログインされないように強固な認証システムを使うする必要がある．例えば，ログイン時に二段階認証を行うことで，ログイン ID・パスワードのみよりも不正ログインをされにくいようにすることができる．

- 運用管理や保守

  VPN を使用する上で運用管理を行わなければならない．例えば，テレワークやコワーキングスペースでの働き方を推奨するのならば端末の持ち出しや社内ネットワークへの接続時のルールを明確にしておくことが必要である．例を挙げると「端末に不要な社内データを保存しない」，「紛失や盗難にあった時のためにデバイスや記憶媒体に暗号化を施す」などがある．他にも，インターネット VPN を使用することでインターネットに接続できる場所であればどこでも通信路に関するセキュリティとしては安全に通信することができるが，公共性が高い場所で作業を行うとソーシャルエンジニアリング[3]によって機密データが盗まれてしまう等のリスクが考えられるため，そのような場所では作業を行わない・非常に機密性が高いデータに関してはオンラインではアクセスできないようにする等といったルール作りをすべきである．

以上で VPN の種類やそのメリット・デメリット，VPN を利用する上で存在するセキュ

リティリスク，そしてセキュリティ強化方法について紹介した．実際に VPN を導入する際には上記で示したことを守りながら，セキュリティ的に安全に業務を行うことが重要である．

参照

[1]NTT コミュニケーションズ，VPN は本当に安全？知っておきたいセキュリティリスクと対策，https://www.ntt.com/business/services/network/internet-connect/ocn-business/bocn/knowledge/archive_21.html
[2]大塚商会，VPN のセキュリティは安全ではない？ VPN の仕組みとリスク対策について解説，https://www.otsuka-shokai.co.jp/solution/keyword/network/vpn-security/
[3]総務省，ソーシャルエンジニアリングの対策，https://onl.sc/V6PZBba