テレワークにおける システムセキュリティ対策のポイント

新型コロナウイルスの感染防止対策としてテレワークが急増しているが、セキュリティ対策は後手にまわっていないだろうか。テレワークは「端末」を必要とし、「作業環境」があり、「社内システム」に接続する、といった共通点がある。それをベースに、セキュリティ対策をしっかり検討することが望ましい。

新型コロナウイルスの拡大により、社外でのテレワークが急速に増えている。それに伴い、セキュリティへの懸念も広がっている。

企業のIT環境は業界や規模により大きく異なり、またテレワークの実現方法も多種多様に存在するが、以下の点は共通している。テレワークでは基本的には電子情報を操作、編集するための「端末」を必要とする。その端末は自宅ないし外出先を「作業環境」とし、インターネットを介して、電子情報が保管されている「社内システム」に接続するということである。

ここでは、「端末」、「作業環境」、「社内システム」ごとにセキュリティ対策のポイントを整理しておきたい[1)]。

端末におけるセキュリティ

端末のセキュリティ対策としてまず挙げられるのは、なんといってもウイルス対策の強化である。社内ネットワーク環境で端末を利用する場合、インターネットと社内ネットワークとの境界にマルウェアを検知、除去する機器を導入するケースが多い。しかし、自宅や外出先では、直接インターネットに接続するため、マルウェアなどのウイルス感染のリスクが高くなる。

次に挙げられるのは、セキュリティパッチを見逃さないことである。端末内のソフトウェアは、攻撃となる脆弱性が日々発見されている。一般的に自動更新するよう設定されているはずだが、セキュリティパッチが配布されたら、すぐさま対応することが求められる。これらは何もテレワークに限らず、日常的に求められる習慣ともいえよう。

また、端末の持ち出しの機会も増えるため紛失・盗難対策も欠かせない。最も有効な対策は、データの暗号化である。個別データやアプリケーションの暗号化等様々な種類の暗号化があるが、できれば「ハードディスク全体を暗号化」しておくことが望ましい。また、保存しているデータを遠隔で消去するサービスやシステムを利用することも対策の一つである。

テレワーク環境では、物理的にシステム管理者の目が届かないところで利用されているため、上記のようなセキュリティ対策に漏れが生じる可能性もある。これを防ぐために一括して、全端末の設定を遠隔で収集、操作する仕組みの導入も重要だろう。

作業環境のセキュリティ

テレワーク環境は、自宅と外出先が想定されるが、まず、自宅における対策を考えたい。

通常家庭では、インターネットに接続する際に、自宅内にブロードバンドルーター（以下、ルーター）と呼ばれる機器を設置する。ルーターには、インターネットの住所録にあたるDNS（ドメインネームシステム）情報が登録されている。攻撃者が、この情報を書き換えると、利用者は不正なWebサイトに誘導されてしまう可能性がある。こうした攻撃を防ぐには、2つの対策がある。一つは、ルーターのソフトウェアを常に最新の状態に保つことである。可能であれば、自動更新されるように設定しておくことが望ましい。もう一つは、ルーターの設定を行うための管理者ID、パスワードの変更である。

次に外出先での対策だが、もっとも懸念されるのは、悪意のあるアクセスポイントへの接続が挙げられる。例えば、悪意のある者がレストランの名称や駅名等その場

NOTE

1) そのほかのセキュリティ対策については、「テレワーク時代のセキュリティ」（「月刊資本市場」、2020年6月号）参照。

図表　テレワークにおける代表的なセキュリティ対策

対象	分類	対策
端末のセキュリティ	基本的な対策	ウイルス対策
		セキュリティパッチ適用
		データの暗号化
		データの遠隔削除、紛失・盗難時手順の作成
		端末状況の一元管理
	私用端末の対策	端末の限定
		データの限定
作業環境のセキュリティ	自宅での対策	ブロードバンドルーターのソフトウェア更新
		ブロードバンドルーターの管理アクセス用パスワード変更
		無線LANにおける強固な暗号技術／パスワードの利用
	外出先での対策	不審なアクセスポイントの利用禁止
		利用するアクセスポイントの暗号技術の確認
		不特定多数がいる環境での情報漏洩の注意
社内システムのセキュリティ	社内システムまでの通信に関する対策	VPNの利用
		VPNアクセス許容量の確認
		VPN利用時の多要素認証の利用
	社内システム自体の対策	社内システムのアクセス制御
		端末へのデータDL制限

（出所）NRIセキュアテクノロジーズ

所を想起する名称をアクセスポイントに設定することで、そこを経由する通信が傍受される可能性がある。そのため、実際にアクセスポイントを提供しているかどうかを事前に確認することが重要である。

社内システムのセキュリティ

一般的に、社内システムへのアクセスは社内ネットワークに限定している場合が多い。そのため、社外から社内システムにアクセスする場合は、VPNと呼ばれる技術を用いて、仮想的に社内ネットワークに接続する状況をつくりだす。その際、ポイントとなるのがVPNアクセス時の認証だ。

社外から社内システムにアクセスできるということは、攻撃者も不正なアクセスを試行することができるということである。それを防ぐには、例えば、ID/パスワード（知識認証）と専用のトークンから発行されるワンタイムパスワード（所有物認証）を組み合わせるといった2つ以上の異なる要素を用いた認証（多要素認証）を行うことが望ましい。また、端末に証明書をインストールすることで、許可されていない端末の接続を禁止する設定も可能だ。

以上、端末からアクセスする際のセキュリティ対策の一部を例示したが、社内システム自体のセキュリティ対策も重要である。ここでは2点述べたい。1点目は、社内ネットワークの適切な分離である。攻撃者からの脅威にさらされているので、テレワーク業務として社外からのアクセスを許可する社内システムは、可能な限り他のシステムと「ネットワーク自体を分離すること」が求められる。

2点目はデータのダウンロード制限である。機密度の高い情報は端末にダウンロードできない設定にすることで、情報漏洩のリスクを下げることができる。ただし、ダウンロード制限はシステムに依存するところもあるため、VDI（仮想デスクトップ環境）を社内ネットワークに用意し、作業者はリモートでVDIを操作するのみとし、端末にはデータは一切保存できない環境を整備する対策も有効である。

Writer's Profile

高見澤 涼 Ryo Takamizawa
NRIセキュアテクノロジーズ
セキュリティコンサルタント
専門はグローバルセキュリティガバナンス
focus@nri.co.jp