

機密を要する情報システムでインターネット回線の利用を認める基準

令和 2 年 3 月 16 日
情報セキュリティ統括責任者決定
(企画調整局長)
令和 4 年 3 月 30 日
情報セキュリティ統括責任者改定
(デジタル戦略部長)
令和 5 年 4 月 1 日
情報セキュリティ統括責任者改定
(デジタル戦略部長)

「物理的・技術的セキュリティ管理基準」3.3.2 に規定するインターネット VPN (IP Sec-VPN 又は SSL-VPN) 及び TLS 通信に関する基準とは、次のとおりとする。

3.3.2 機密を要する情報システムで使用する回線【対策基準 6.3.4】

ア 対策基準 6.3.4 における「適正な回線」とは、閉域イーサネット、専用線、IP-VPN 等の閉域網をいう。

イ 次の条件にあてはまるときは、情報セキュリティ管理者が許可した場合に限り、機密性 2 以上の情報を取り扱うことができるものとする。

(1) インターネット VPN を利用してシステムまたは外部サービスを利用する場合

(2) ファイアウォール、WAF、IP アドレス制限等の付加的なセキュリティ対策を施したシステムまたは外部サービスとの通信にインターネット回線 (TLS 通信) を利用する場合

【インターネット VPN の利用について】

以下の 1～2 の項目をすべて満たすものについて、インターネット VPN の利用を認めることとする。

1 インターネット VPN の設定が確実に行われること

インターネット VPN は設定ミスから脆弱性が生まれるリスクがあるとされているため、VPN の設定が確実に行われるものでなければ利用を認められない。

2 インターネット VPN の適性が認められること

次に掲げる前提条件、通信の品質、効率性、セキュリティ要件、コストメリットのすべての事項についてインターネット VPN の適性が認められなければならない。

(1) 前提条件

- ① 当該回線の接続先である特定の Web サーバに格納又は格納予定のデータ以外のデータを当該回線で取り扱わないこと
 - ② 当該回線の接続先のサーバ側及び接続元側の双方に VPN 装置が設置可能であること（リモートアクセスの場合は基本的に接続先のサーバ側のみで可）
 - ③ インターネット VPN により制限のあるプロトコルの通信がないこと
 - ④ 接続先又は接続元的一方又は双方がインターネット環境にあること
 - ⑤ マイナンバー利用系ネットワークから接続するものではないこと
- (2) 通信の品質
- ① 回線速度を保証する必要がある用途で利用すること
 - ② BCP に係る通信用途ではないこと
 - ③ 通信経路の断絶等による通信障害の責任を問う必要がないこと
- (3) 効率性
- ① アクセスする PC の特定が可能であること（リモートアクセス型の場合）
 - ② アクセスする PC に専用ソフトを導入することが可能であること（SSL-VPN の場合は一部の特殊な事例を除き導入不要）
 - ③ アクセスする PC への通信のための要求事項が明確であり、対応できること
- (4) セキュリティ要件
- ① ログイン時に原則として二要素以上の認証を実施すること
 - ② 許可された端末以外がアクセスできないユーザ認証・アクセス制御のしくみを採用すること（クライアント証明書等）
 - ③ 世界標準の暗号化技術のうちその時点で最も強度の高い暗号化技術を採用すること（標準技術に依存することで問題ない）なお、運用段階において当該技術に致命的な脆弱性が発見された場合は、可及的速やかに措置を講じること。
- (5) コストメリット
- ① インターネット VPN を用いた場合のコストが、IP-VPN 等を用いた場合のコストと比較して明らかに有利であること
（双方のコスト算出を行っていること）

【インターネット回線（TLS 通信）の利用について】

以下の 1～2 の項目をすべて満たすものについて、インターネット回線（TLS 通信）の利用を認めることとする。

- 1 TLS 1.2 以上を使用すること。
- 2 管理基準 3.3.2 に規定する付加的なセキュリティ対策（IP アドレス制限、多要素認証等、WAF（Web Application Firewall）や FW（ファイアウォール）の設置等）を施すこと。