Cisco ASA5500シリーズ VPNアクセス方法比較資料 （July 2011 ver）

株式会社レップワン
Rep1 Corp

接続方法	①Cisco VPN Client	②クライアントにｱﾌﾟﾘｹｰｼｮﾝのインストールが不要	③Cisco AnyConnect →②をソフトウェアによって補完する
インターネットVPN種別	IPSec	SSL VPN	SSL VPN
利用に適している場面	・Webや電子メールのアクセスだけでなく幅広いネットワーク・プロトコルに対応する全般的インフラを必要としている場合 ・組織がリモートアクセスユーザーの端末に対して管理権限を持つ場合 ・リモートアクセスユーザーの端末に対してセキュリティ制御（パーソナルファイアウォールやアンチウィルスソフトの必要性など）が必要な場合	・リモートアクセスユーザーがアクセスを必要とするのが、主にWebベースのアプリケーションや電子メールである場合 ・多様なアクセス元端末（ノートPC、家庭用PC、インターネット・キオスク端末など）から情報へのアクセスが必要な場合 ・組織がリモートアクセスユーザーの端末設定の管理権限を持たない場合 ・リモート・アクセスに必要なソフトウェアをユーザの端末にインストールできない場合 ・ファイアウォールやISPによりIPSec接続はできない（IPSecのIKEネゴシエーションが許可されない）が、SSLは許可されている場合	・Webや電子メールのアクセスだけでなく幅広いネットワーク・プロトコルに対応する全般的インフラストラクチャを必要としている場合 ・組織がリモートアクセスユーザーの端末に対して管理権限を持つ場合 ・リモートアクセスユーザーの端末に対してセキュリティ制御（パーソナルファイアウォールやアンチウィルスソフトの必要性など）が必要な場合 ・ファイアウォールやISPによりIPSec接続はできない（IPSecのIKEネゴシエーションが許可されない）が、SSLは許可されている場合
利用できるアプリケーション	すべてのIPアプリケーション（Webアプリケーション、エンタープライズ、電子メール、VoIP、マルチメディア）	主としてWebアプリケーション	ほぼすべてのIPアプリケーション（Webアプリケーション、エンタープライズ、電子メール、マルチメディア）
アクセス方法	IPSecクライアント・ソフトウェア	Webブラウザ	DTLS対応SSL-VPNクライアント・ソフトウェア
情報の制御	指定された人／端末のみにアクセスを許可	ID/パスワードとインターネット接続環境があれば何処からでもアクセス可能	指定された人／端末のみにアクセスを許可
クライアントのセキュリティレベル	中～高レベル	低～中レベル	中～高レベル
拡張性導入性	拡張しやすい	拡張しやすい	拡張しやすい
導入性	導入しやすい	導入しやすい	導入しやすい
アクセス制御	認証、認可、及びアカウンティングに対応	1次認証、2次認証、認可、及びアカウンティングに対応	1次認証、2次認証、認可、及びアカウンティングに対応
操作性	ローカル環境と同様	Webブラウザでアクセスする、 ポータル画面内での操作に限定される	ローカル環境と同様
モバイル端末での利用	可能 iPhoneはこのソフトを標準搭載している Android端末はCisco vpn client Android Appsが必要	可能（WEBブラウザでSSL対応ページにアクセスする）	iOS搭載端末のみ可能 ただしモバイル版のCisco AnyConnect VPN Clientは有償
主な長所	・VPNセッション確立後は、ほぼ**全ての社内リソースにアクセス可能** ・リモートアクセスユーザーの端末に他のセキュリティ機能（パーソナル・ファイアウォール、設定検証など）の組み込みが可能 ・SSL-VPNと比べて通信のオーバーヘッドが少ない分**高速である**	・クライアントソフトウェアの**インストールなし**でのリモートアクセスが可能 ・NAT、プロキシ、ファイアウォールに対して透過的に機能（ほとんどのファイアウォールはSSLトラフィックを許可）するため、接続元のネットワーク環境に左右される可能性が低い ・メール・クライアントなどの一般的アプリケーションはSSLに対応	・VPNセッション確立後は、ほぼ**全ての社内リソースにアクセス可能** ・NAT、プロキシ、ファイアウォールに対して透過的に機能（ほとんどのファイアウォールはSSLトラフィックを許可）するため、接続元のネットワーク環境に左右される可能性が低い ・リモートアクセスユーザー端末に他のセキュリティ機能（パーソナル・ファイアウォール、設定検証など）の組み込みが可能
主な短所	・クライアントソフトウェアの**インストールが必要。**全てのOSがサポートされているわけではない ・リモートアクセスユーザーの端末にインストールされたクライアントソフトウェアが他のアプリケーションと競合する場合がある ・接続元の環境によっては、ゲートウェイの間にあるデバイス（ファイアウォールやNATデバイス）によって接続性が妨げられる場合がある ・クライアントレスSSL-VPNと比べて運用管理が難しい	・SSLにはIPSecよりも多くのゲートウェイの処理リソースが必要 ・ファイアウォールでHTTPS接続内のデータのコンテンツ検査ができない ・WEBブラウザによるアクセスであるため、故意かどうかに関わらず、アクセスに使用した端末に情報が残る可能性がある ・Webアプリケーション以外を利用する場合は別途プラグインの導入が必要になる。	・SSLにはIPSecよりも多くのゲートウェイの処理リソースが必要 ・ファイアウォールでHTTPS接続内のデータのコンテンツ検査ができない ・クライアントソフトウェアのインストールが必要。全てのOSがサポートされているわけではない ・リモートアクセスユーザーの端末にインストールされたクライアントソフトウェアが他のアプリケーションと競合する場合がある ・クライアントレスSSL-VPNと比べて運用管理が難しい