CHAPTER 2

# 構成のプランニング

このマニュアルは、ASA 5505 の典型的なカスタマー構成を表す、いくつかのシナリオ例に基づいています。 この章の構成シナリオは、後続の設定の章に対応しています。

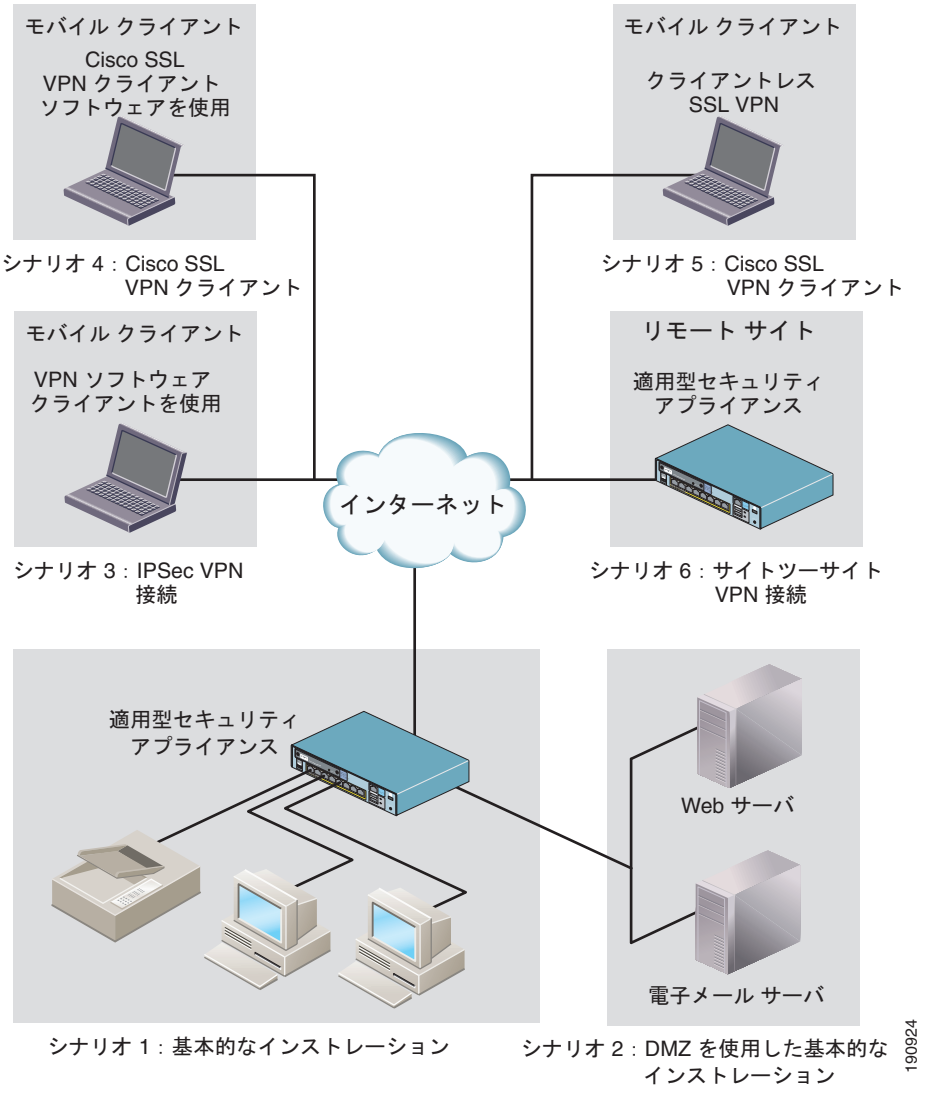
この章には、次の項があります。

# 構成のプランニングと設定のシナリオ

適応型セキュリティ アプライアンスの拡張構成には、この章で説明する 2 つ以上の異なる構成シナリオを含めることができます。この章の構成シナリオを使用して、ネットワーク上の適応型セキュリティ アプライアンスを構成する方法を決定し、該当する設定の章を判別することができます。

図 2-1 に、このマニュアルに記載されているほとんどの構成シナリオと設定シナリオが含まれる拡張ネットワーク構成を示します。

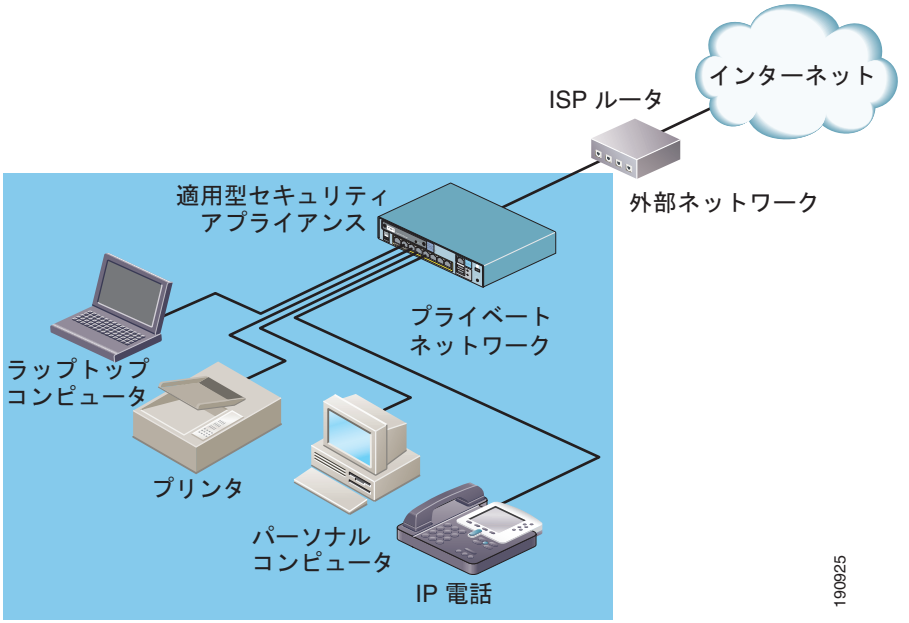
**図 2-1　拡張ネットワーク構成**



# シナリオ 1：外部接続を使用したプライベート ネットワーク

図 2-2 に、小規模なプライベート ネットワークで一般的な基本構成を示します。

**図 2-2　外部接続を使用したプライベート（内部）ネットワーク**




この例では、適応型セキュリティ アプライアンスを使用することにより、プライベート ネットワーク上のすべてのデバイスが互いに通信を行い、プライベート ネットワーク上のユーザがインターネット上のデバイスと通信を行うことができます。

（注）　この構成は PIX 501 を使用するセキュリティ構成に類似しています。 ファイアウォールの背後にあるデバイスが内部および外部で通信できる PIX 501 セキュリティ アプライアンスを使用したセキュリティ構成をすでに使用している場合は、同じ構成をそのまま使用し、PIX 501 デバイスを ASA 5505 デバイスに交換できます。

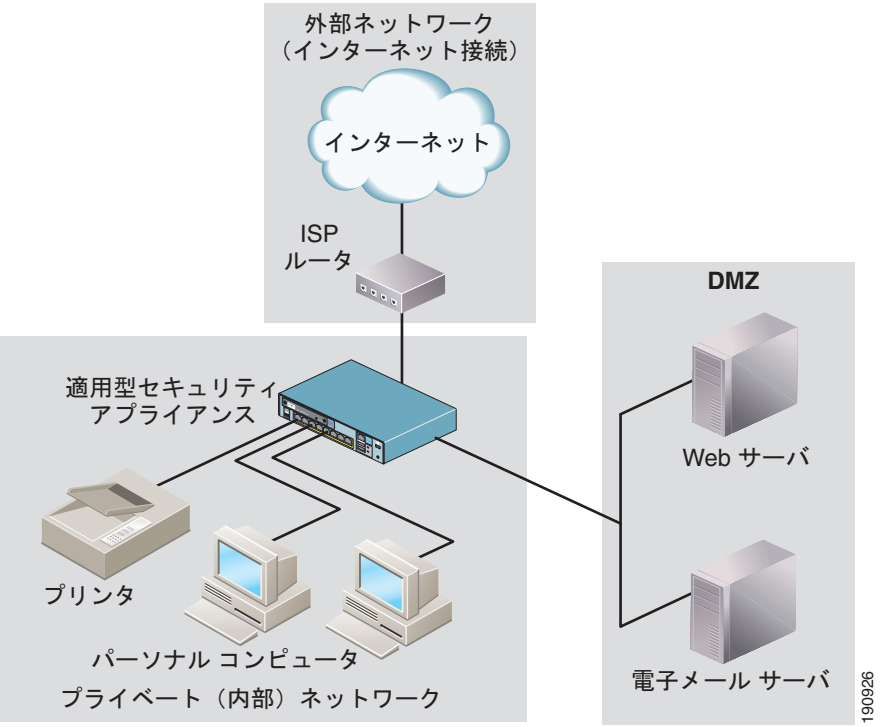
適応型セキュリティ アプライアンスをこの構成用に設定する方法の詳細については、第 5 章「適応型セキュリティ アプライアンスの設定」を参照してください。

# シナリオ 2：DMZ を使用した基本的なインストレーション

このシナリオでは、適応型セキュリティ アプライアンスを使用して、内部ネットワークに加えて Demilitarized Zone（DMZ; 非武装地帯）にあるネットワーク リソースを保護します。DMZ は、プライベート（内部）ネットワークとパブリック（外部）ネットワークとの間の中立帯に位置する別個のネットワークです。

プライベート ネットワーク上の HTTP クライアントは、DMZ 内の Web サーバにアクセスでき、インターネット上のデバイスとも通信できます。

**図 2-3　DMZ を使用したプライベート ネットワーク**

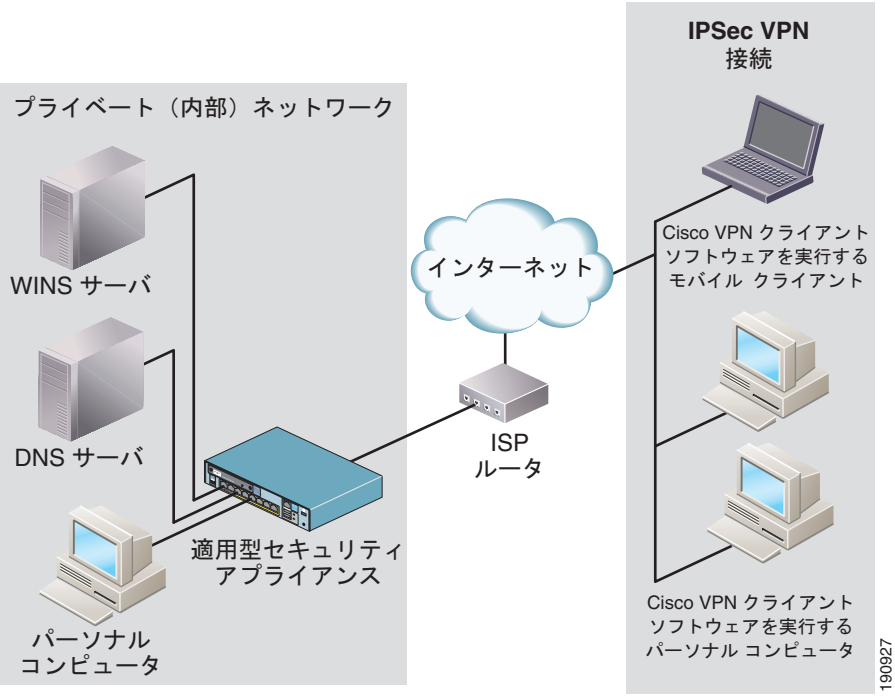



DMZ 構成の設定方法の詳細については、第 6 章「シナリオ：DMZ 設定」を参照してください。

# シナリオ 3：IPSec リモートアクセス VPN

このシナリオでは、リモートアクセス IPSec VPN 接続を受け入れるよう、適応型セキュリティ アプライアンスを設定します。リモートアクセス VPN を使用すると、インターネットを越えてセキュアな接続（トンネル）を作成でき、オフサイトのユーザにセキュアなアクセスを提供できます。

**図 2-4　IPSec リモートアクセス VPN 接続**



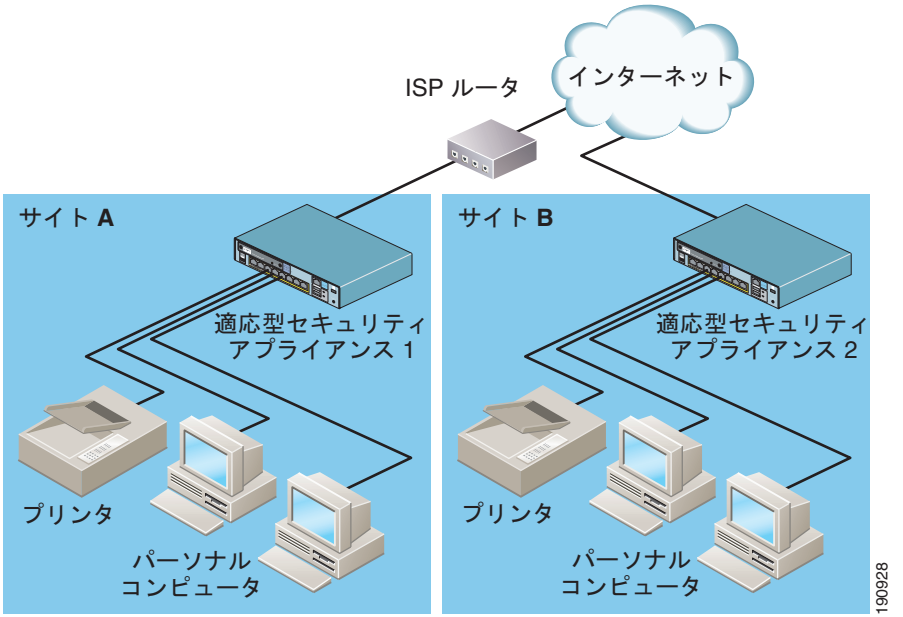

IPSec リモートアクセス VPN 構成の設定方法の詳細については、第 7 章「シナリオ：IPSec リモートアクセス VPN 設定」を参照してください。

# シナリオ 4：サイトツーサイト VPN

このシナリオでは、2 つの適応型セキュリティ アプライアンスを設定して、サイトツーサイト VPN を作成します。

サイトツーサイト VPN を構成すると、企業はネットワーク セキュリティを維持したまま、ネットワークを拡張してビジネス パートナーや世界中のリモート オフィスとの間で低コストのパブリック インターネット接続を実現できます。VPN 接続では、セキュアな接続、つまりトンネル経由で 1 つの場所から別の場所へデータを送信できます。これは、まず接続の両端を認証し、次に 2 つのサイト間で送信されるすべてのデータを自動的に暗号化することによって可能になります。

**図 2-5　サイトツーサイト VPN 設定シナリオのネットワーク レイアウト**




サイトツーサイト VPN 構成の設定方法の詳細については、第 8 章「シナリオ：サイトツーサイト VPN 設定」を参照してください。

# シナリオ 5:ハードウェア VPN クライアントとして構成された ASA 5505

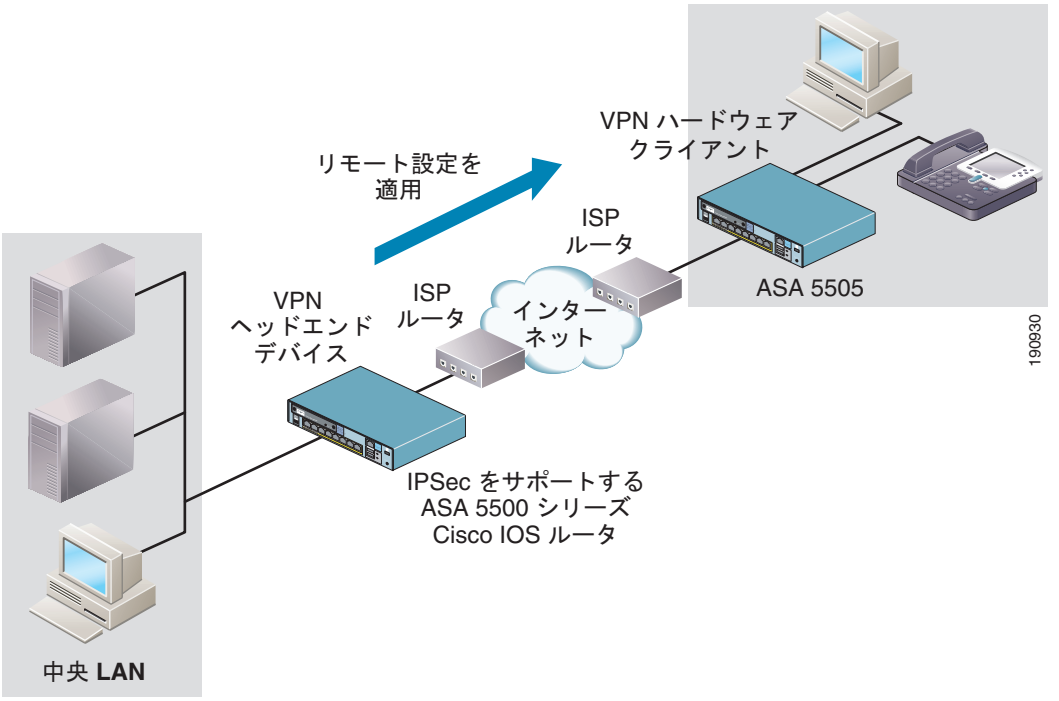
このシナリオでは、ASA 5505 をハードウェア クライアント（リモート デバイスとも呼ばれる）として構成します。VPN ヘッドエンド デバイスを使用して 1 つまたはそれ以上の VPN ハードウェア クライアントを構成すると、複数のサイトを持つ企業は、そのサイト間の安全な通信を確立して、ネットワーク リソースを共有できます。

ハードウェア クライアントを使用して Easy VPN ソリューションを構成すると、次の方法で VPN の構成と管理が簡素化されます。

- リモート サイトのホストが VPN クライアント ソフトウェアを実行する必要がなくなる。
- 中央サーバにセキュリティ ポリシーが常駐し、VPN 接続が確立されると、セキュリティ ポリシーがリモート ハードウェア クライアントに適用される。
- ローカルに設定する必要がある設定パラメータがほとんどないため、オンサイト管理の必要性を最小限に抑えられる。

図 2-6 に、各種 Easy VPN コンポーネントを構成する方法を示します。

**図 2-6　VPN ハードウェア クライアントとして設置された ASA 5505**




ASA 5505 を VPN ハードウェア クライアントとして設定する方法の詳細については、第 9 章「シナリオ : Easy VPN ハードウェア クライアント設定」を参照してください。

# 各シナリオに対する設定手順

このマニュアルには、この章の各構成シナリオに対応する設定の章があり、構成タイプに合わせて ASA 5505 を設定する方法が記載されています。

| ASA 5505 を設定する構成シナリオ | 参照する章 |
|---|---|
| シナリオ 1：外部接続を使用したプライベート ネットワーク | 第 5 章「適応型セキュリティ アプライアンスの設定」 |
| シナリオ 2：DMZ を使用した基本的なインストレーション | 第 6 章「シナリオ：DMZ 設定」 |
| シナリオ 3：IPSec リモートアクセス VPN | 第 7 章「シナリオ：IPSec リモートアクセス VPN 設定」 |
| シナリオ 4：サイトツーサイト VPN | 第 8 章「シナリオ：サイトツーサイト VPN 設定」 |
| シナリオ 5：ハードウェア VPN クライアントとして構成された ASA 5505 | 第 9 章「シナリオ：Easy VPN ハードウェア クライアント設定」 |

# 次の作業

第 3 章「VLAN 構成のプランニング」に進みます。