SAMPLE

株式会社 XXXXXX 御中

リモートアクセスサービス設計書

作成者：株式会社レッツワン

作成日時：2011/MM/DD

更新日時：2011/MM/DD

SAMPLE

目次

本書の目的

本書は、株式会社 XXXX 様の社内ネットワークに設置される Cisco ASA5520 及び ASA5505 を使用した、IPsec-VPN と SSL-VPN によるリモートアクセスサービスについての設計内容を記述する。

※本書のパラメーター項目やパラメーター値の記述は、Cisco ASA5500 シリーズの GUI 管理ツールである ASDM 上の表記を可能な限り踏襲する形で記載する。

SAMPLE

1. ハードウェア構成

1-1. ハードウェアスペック

本システムに使用する機器のハードウェアスペックを以下に示す。

項目	アクティブ機	スタンバイ機
ホスト名	RAS01	RAS01
機器名	Cisco ASA5520	Cisco ASA5520
機器タイプ	セキュリティアプライアンス	セキュリティアプライアンス
システム フラッシュ	256MB	256MB
メモリ	512MB	512MB
ファイアーウォールスループット	最大 450 Mbps	最大 450 Mbps
VPN のスループット	最大 225Mbps	最大 225Mbps
同時セッション数	280,000	280,000
インターフェイス	10BASE-T / 100BASE-TX / 1000BASE-T ×4 管理用 10BASE-T / 100BASE-TX×1	10BASE-T / 100BASE-TX / 1000BASE-T ×4 管理用 10BASE-T / 100BASE-TX×1
冗長化機能	アクティブ/アクティブ構成 アクティブ/スタンバイ構成	アクティブ/アクティブ構成 アクティブ/スタンバイ構成
電源電圧	100 ～ 240 VAC	100 ～ 240 VAC
定格出力 / 最大出力	150 W / 190 W	150 W / 190 W
シリアルナンバー		

1-2. デバイス情報

本システムに使用する機器のデバイス情報とライセンス情報を以下に示す。

項目	アクティブ機	スタンバイ機
ASA バージョン	8.2.3	8.2.3
ASDM バージョン	6.3.4	6.3.4
ファイアーウォールモード	Routed	Routed
コンテキストモード	Single	Single
ライセンス	VPN Plus	VPN Plus
最大コンテキスト数	2	2
最大 VLAN 数	150	150
最大物理接続数	Unlimited	Unlimited
Failover 機能	Active/Active	Active/Active
IPsec VPN ピア数	750	750
SSL VPN ピア数	2	2
VPN DES Encryotion	Enable	Enable
VPN 3DES and AES Encryotion	Enable	Enable
AnyConnect Mobile	Disable	Disable

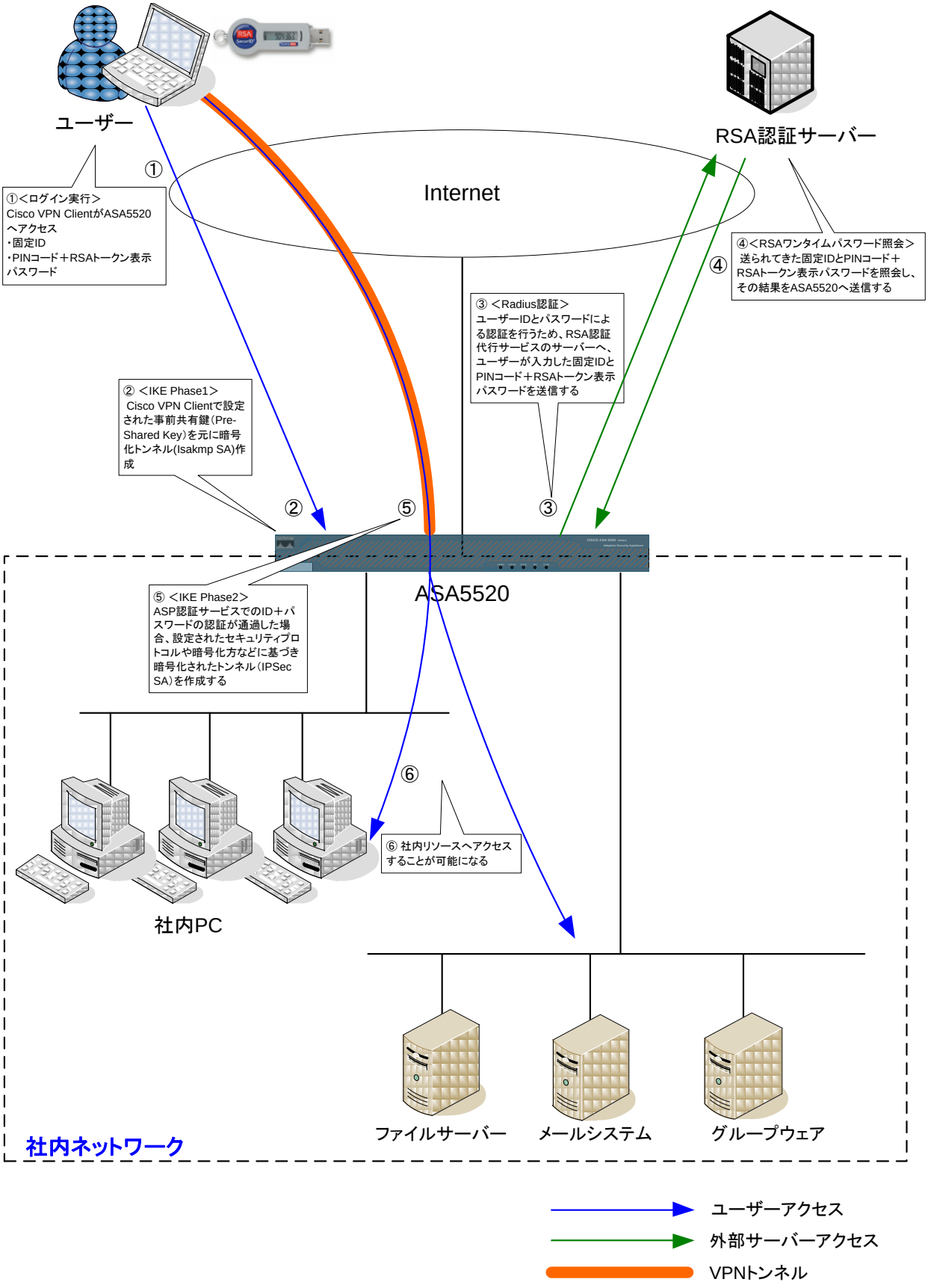
1-3. HA 構成

本システムの HA（高可用性）構成は Cisco ASA5520 をフェールオーバーによるアクティブ/スタンバイ構成で運用を行う。アクティブ機に障害が発生した際はスタンバイ機への自動的に切り替わり、サービスの継続が可能となる。

IPsec-VPN 設計

1-4. IPsec-VPN 通信フロー図

IPsec-VPN 接続時の通信フロー図を以下に示す。



1-5. Cisco VPN Client について

ユーザーの IPsec-VPN への接続には Cisco VPN Client を使用する。

1-5-1. Cisco VPN Client

使用する Cisco VPN Client のバージョンと、サポートされるクライント環境の条件を以下に示す。

項目	値
Cisco VPN Client バージョン	・Cisco VPN Client 5.0.07.0290
サポート OS	・Windows 7 on x64 (64-bit) ・Windows 7 on x86 (32-bit) ・Windows Vista on both x86 (32-bit) and x64 ・Windows XP on x86
システム要件	・Pentium®-class processor or greater ・Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.) ・50 MB hard disk space. ・128 MB RAM(256 MB recommended) ・Administrator 権限

1-6. IPsec トンネリング設定

1-6-1. アクセス許可インターフェイス

IPsec-VPN でアクセスを許可するインターフェイス設定を以下に示す。

Interface <インターフェイス名>	Allow Access <アクセス許可>
outside	Enable
inside	Disable

1-6-2. IKE Phase1 設定

※5-1.IPsec-VPN 通信フロー図内②で使用される設定。

IKE Phase1 のパラメーターを以下に示す。

項目	値
暗号化方式	AES-128bit
ハッシュアルゴリズム	SHA-1
ライフタイム	86400 秒
認証方式	Pre-Shared Key
DH グループ	2

1-6-3. IKE Phase2 設定

※5-1.IPsec-VPN 通信フロー図内⑤で使用される設定。

IKE Phase2 のパラメーターを以下に示す。

項目	値
セキュリティプロトコル	ESP
暗号化方式	AES-128bit
認証アルゴリズム	HMAC-SHA1
ライフタイム	86400 秒
認証方式	Pre-Shared Key

1-7.

1-7-1. IPsec-VPN 接続用グループポリシー設定

IPsec-VPN 接続用のグループポリシー設定を以下に示す。

Name	IPSEC-Policy
Address Pool	VPN-Address-Pool（***.***.***.*** - ***.***.***.***）
Tunneling Protocol	IPsec
IPv4 Filter ＜IPv4 アクセ制御設定＞	VPN-Client_Access_Policy ＜※項番 5-6-4 の設定＞
IPv6 Filter ＜IPv6 アクセス制限設定＞	未設定
Access Hours ＜アクセス許可時間帯＞	未設定
Simultaneous Login ＜同時ログイン数＞	未設定
Restrict access to VLAN ＜VLAN へのアクセス制限＞	未設定
Connection Profile(Tunnel Group) Lock ＜トンネルグループの固定＞	MNTR-IPSEC-VPN_Grp
Maximum Connect Time ＜最大接続時間＞	未設定
Idle Timeout ＜タイムアウトするアイドル時間＞	30 minutes

1-7-2. VPN 接続用 IPv4 アクセス制御設定

IPv4 アクセス制御の設定を以下に示す。（本設定は IPsec-VPN と SSL-VPN で共通の設定を用いる）

■VPN-Client_Access_Policy

#	Enabled	Source <送信元>	Destination <送信先>	Service	Protocol	Action	Logging
1	On	any	Inside-network/24	RDP(3389)	tcp	permit	Default
2	On	any	any	IP	-	Deny	Default

株式会社 ＊＊＊
テレワーク勤務規程

平成 21 年 10 月 1 日
第１版 制定

第1条　【目的】

この規程は、株式会社＊＊＊（以下「会社」という。）における、在宅勤務およびサテライトオフィスでの勤務（以下、テレワーク勤務という）に関する取扱いについて定めるものである。

第2条　【本規程での用語の定義】

テレワーク勤務：パソコンやインターネット等の IT 環境を使用して業務を遂行するうえで、結果物の作成に場所の制限が無く、従業員の自宅又は会社の指定するサテライトオフィスにおいて行う勤務のこと。

在宅：自宅

サテライトオフィス：レンタルオフィスやそれらに準ずるプライバシーの守られた空間

第3条　【対象者】

この規定で定めるテレワーク勤務は、以下の条件、環境を満たしている者を対象とする。

（1）　時間管理能力、集中力があり、一定時間に定められた結果を出せること

（2）　情報および成果物を紛失しないよう丁寧に扱い、第三者が閲覧やコピーなどができないよう最大の注意を払うこと。この規定において従業員の親族も第三者とみなす

（3）　業務遂行上の必要性が認められること

（4）　テレワーク勤務を会社へ申請し、適切な者から許可を受けていること

（5）　会社が準備する、もしくは費用を全額支払う物理的環境（パソコン、アプリケーションソフト、インターネット接続用回線）が準備されていること。下記のいずれかを要件とする。

勤務場所	PC およびインストールされるソフトウェア	回線
在宅（回線別）	会社所有	モバイル用回線など会社名義
在宅（VPN）	会社所有	会社所有の VPN 機器によるインターネット VPN 接続
サテライトオフィス	サービス提供業者所有/レンタル費用は会社負担	サービス提供業者所有/レンタル費用は会社負担

第4条　【勤務の申請・許可】

テレワーク勤務を希望する者は、勤務該当日の前日までに、「テレワーク勤務申請および結果報告書」に記入し、ファクシミリ又は電子メール等により会社へ申請し、課長以上の所属上司の許可を受けなければならない。

２．会社は、在宅勤務を希望する者が前条の要件を満たすと認めるときは、「テレワークの勤務申請および結果報告書」へのメール返信もしくは、自筆署名によって許可を行い、勤務を命ずるものとする。

３．本人の独断による、会社への申請および上司承認の無いテレワーク勤務は労働時間と認めない。

第5条　【勤務時間の算定および結果の報告】

テレワーク勤務従業員は、勤務結果を「テレワーク勤務申請および結果報告書」に記入し、ファ

クシミリ又は電子メール等により適宜会社へ報告しなければならない。テレワーク勤務時間は、「テレワーク勤務申請および結果報告書」の結果報告した時間を勤務したものとみなす。また、勤務時間が 1 日の所定勤務時間を超えると認めるときは、申請に基づき、該当勤務時間を時間外労働として承認する。

２．「テレワーク勤務申請および結果報告書」によって報告・承認された勤務時間は会社所定の「勤怠記録簿」にテレワーク勤務である旨を明記して記入すること

第6条　【機器の貸与】

会社は、在宅勤務を行う場合に必要となるパソコン等のＩＴ機器を貸与する。

２．会社が貸与するパソコンへは、会社が認めるもの以外のアプリケーションをインストールしてはならない。

第7条　【本人所有の機器使用の原則禁止】

テレワーク勤務従業員は、やむを得ない理由により自ら所有する機器を使用したい場合には、「私物機器の業務使用許可申請書」に必要事項を記載のうえ会社に申請するものとする。

２．会社は前項の申請により機器使用の可否を審査する。

第8条　【本人所有の機器使用の例外】

テレワーク勤務に際し、アクセス制限がかけられている以下システムを利用する業務は私物パソコンによるアクセスを許可する。

（1）　会社グループウェアへの入力、編集

第9条　【費用の負担】

機器準備、使用に関する費用は会社が負担する。

２．本人所有の機器を使用する場合であって、会社が必要と認めるときは、機器使用に要した費用に関し、明細書を提出しなければならない。

（付　則）

本規則は、平成　２１　年　１０月　１　日から施行する（第１版）