Cloud Gate SSO Active Directory設定手順書

(Windows Server 2012 Standard Edition)



1.Active Directory 証明局のイントール	3
2.証明書の有効期限	35
3.証明書の作成	37
4.証明書のエクスポート	42

.

Active Directory 証明局のインストール
 ※既にインストールされている場合はこの手順は不要です。
 ※Windows Server のインストールディスクが求められる場合があります。

		-/- {*->-					_
€∋- サーバー	マネージャー・ダッシュボード	•	· ③ 🖡	, 管理(M) ツール(T)	表示(V)	へルプ(H)	
III ダッシュポード ■ ローカル サーバー ■ すべてのサーバー ■ ファイル サービスと記憶域… ト	サーバー マネージャーへようこそ 1 この 0 2 役 3 管理 最新情報(W) 4 サー	ーカル サーバーの構成 割と機能の追加 里するサーバーの追加 -バー グループの作成					- III
	 送細情報(L) 役割とサーバー グループ 役割の窓:1 サーバー グループの窓:1 役割の窓:1 サーバー グループの窓:1 ブアイル サービスと記憶 1	サーバーの合計数:1 ■ ローカル サーバー ④ 管理状態 イベント	1	すべてのサーバー 管理状態 イベント	非表: 1	*	~

左下「サーバーマネージャーボタン」をクリックして起動します。 その後「役割と機能の追加」をクリックします。

B	役割と機能の追加ウィザード
開始する前に	対象サーバー AMAZONA-GOUIOC5
開始する前に インストールの種類 サーバーの選択 サーバーの役割	このウィザードを使用すると、役割、役割サービス、または機能をインストールできます。ドキュメントの共有や Web サイト のホストなどの組織のコンピューティング ニーズに応じて、インストールする役割、役割サービス、または機能を決定しま す。 役割、役割サービス、または機能を削除するには、次の手順を実行します: 役割と機能の削除ウィザードの起動
機能 確認 結果	 ・管理者アカウントに強力なパスワードが設定されている ・管理者アカウントに強力なパスワードが設定されている ・静的 IP アドレスなどのネットワークの設定が構成されている ・Windows Update から最新のセキュリティ更新プログラムがインストールされている 前提条件が完了していることを確認する必要がある場合は、ウィザードを閉じて、それらの作業を完了してから、ウィザードを再度実行してください。 続行するには、[次へ] をクリックしてください。
	 田定でこのページを表示しない(S)

「次へ」をクリックします。

ħ	役割と機能の追加ウィザード	_ 🗆 X		
インストールの種類	の選択	対象サーバー AMAZONA-GOUIOC6		
開始する前に	インストールの種類を選択します。役割および機能は、実行中の物理コンピューター、 ンの仮想ハード ディスク (VHD) にインストールできます。	仮想コンピューター、またはオフライ		
インストールの種類 サーバーの選択	 役割ベースまたは機能ベースのインストール 役割、役割サービス、および機能を追加して、1台のサーバーを構成します。 			
サーバーの役割機能	 リモートデスクトップ サービスのインストール 仮想デスクトップ インフラストラクチャ (VDI) に必要な役割サービスをインストール ミュン ベースのデスクトップ展開を作成します。 	して、仮想マシン ベースまたはセッ		
確認 結果	ンヨノハースのナスクトッノ皮膚化作成します。			
<前へ(P) 次へ(N) > インストール(I) キャンセル				

「役割ベースまたは機能ベースのインストール」を選択し「次へ」をクリックします。

a	役割と機能の追加ウィザード
対象サーバーの選	対象サーバー AMAZONA-GOUIOC6
開始する前に インストールの種類 サーバーの役割 機能 確認 結果	 役割と機能をインストールするサーバーまたは仮想ハード ディスクを選択します。 ● サーバー プールからサーバーを選択 ● 仮想ハード ディスクから選択 サーバー プール フィルター: ユパレター: 名前 IP アドレス オペレーティング システム AMAZONA-GOUIOC6 10.131.43.77 Microsoft Windows Server 2012 Standard 1 台のコンピューターが見つかりました このページには、Windows Server 2012 を実行しており、サーバーマネージャーの [サーバーの追加] コマンドを使用して追加されたサーバーが表示されます。オフライン サーバーや、データ収集が完了していない、新たに追加された サーバーは表示されません。
	<前へ(P) 次へ(N) > インストール(I) キャンセル

「サーバープールからサーバーを選択」後、該当のサーバーを選択し「次へ」をクリックします。

a	役割と機能の追加ウィザード	_ D X
► は、していたいでは、このでは、このでは、このでは、このでは、していたいでは、 日本のでは、	役割と機能の追加ウィザード 遅択したサーバーにインストールする役割を 1 つ以上選択します。 役割 □ Active Directory Rights Management サービス ^ □ Active Directory ドメイン サービス □ Active Directory フェデレーション サービス □ Active Directory フェデレーション サービス □ Active Directory 証明書サービス □ DHCP サーバー □ DNS サーバー □ FAX サーバー □ Hyper-V	よります。 ための、証明機関および関連する役割サービス の、証明機関および関連する役割サービス に入るために使用します。
	Web サーバー (IIS) Windows Server Update Services Windows 展開サービス アブリケーション サーバー ネットワーク ポリシーとアクセス サービス く III く III く III ン) > インストール(I) キャンセル

「Active Directory 証明書サービス」を選択します。

Active Directory 証明書サービス に必要な機能を追加し ますか?
この機能を管理するには次のツールが必要ですが、同じサーバーにインストール する必要はありません。
 ▲ リモート・サーバー管理ツール ▲ 役割管理ツール ▲ Active Directory 証明書サービス ツール [ツール] 証明機関管理ツール
 ✓ 管理ツールを含める (存在する場合) 機能の追加 キャンセル

「機能の追加」をクリックします。

a	役割と機能の追加ウィザード	_ D X		
サーバーの役割の道	選択	対象サーバー AMAZONA-GOUIOC6		
開始する前に	選択したサーバーにインストールする役割を 1 つ以上選択します。			
インストールの種類	役割	説明		
サーバーの選択 サーバーの役割 機能 AD CS 役割サービス 確認 結果	 Active Directory Rights Management サービス Active Directory ドメイン サービス Active Directory フェデレーション サービス Active Directory ライトウェイト ディレクトリ サービス ✓ Active Directory 証明書サービス DHCP サーバー DNS サーバー FAX サーバー Hyper-V Windows Server Update Services Windows 展開サービス アプリケーション サーバー ネットワーク ポリシーとアクセス サービス ✓ 	Active Directory 証明書サービス (AD CS) は、さまざまなアプリケーションで 使用する証明書を発行および管理するた めの、証明機関および関連する役割サー ビスを作成するために使用します。		
	<前へ(P) 次へ(N) > インストール(I) キャンセル			

「次へ」をクリックします。

B	役割と機能の追加ウィザード	_ D X
機能の選択		対象サーバー AMAZONA-GOUIOC6
開始する前に	選択したサーバーにインストールする機能を 1 つ以上選択します。	
インストールの種類	機能	説明
サーバーの選択 サーバーの役割 機能 AD CS 役割サービス 確認 結果	 ▶ ■ .NET Framework 3.5 Features (インストール済み) ▶ ■ .NET Framework 4.5 Features (インストール済み) ■ BitLocker ドライブ暗号化 ■ BitLocker キットワーク ロック解除 ■ BranchCache ■ HTTP プロキシを経由した RPC □ IP アドレス管理 (IPAM) サーバー □ iSNS サーバー サービス □ LPR ポート モニター ■ Management OData IIS 拡張機能 ■ Media Foundation □ NFS クライアント ■ RAS 接続マネージャー管理キット (CMAK) ■ RDC (Remote Differential Compression) ▼ 	.NET Framework 3.5 では、.NET Framework 2.0 API の機能にアプリ ケーション作成用の新しいテクノロジが加 わりました。ユーザーは、魅力的なユー ザーインターフェイス、顧客の個人情報保 護、シームレスで安全な通信を利用でき ます。また、さまざまなビジネス プロセスを モデル化することができます。
	<前へ(P) 次へ(N) > インストール(I) キャンセル

「次へ」をクリックします。

B	役割と機能の追加ウィザード	_ 🗆 X
Active Director	y 証明書サービス	対象サーバー AMAZONA-GOUIOC6
開始する前に インストールの種類 サーバーの選択	Active Directory 証明書サービス (AD CS) は、安全なワイヤレス ネットワーク、仮想フ ターネット プロトコル セキュリティ (IPSec)、ネットワーク アクセス保護 (NAP)、暗号化ファ・ ト カード ログオンなどのシナリオを実現するための証明書基盤を提供します。	プライベート ネットワーク、イン イル システム (EFS)、スマー
サーバーの役割 機能 AD CS	 エニック・ このコンピューターの名前およびドメイン設定は、証明機関 (CA) のインストール後は変更 名の変更、ドメインの追加、またはこのサーバーのドメイン コントローラーへの昇格を行う場 にこれらの変更を完了する必要があります。詳細については、証明機関の名前付けを参 	更できません。コンピューター 易合、CA のインストール前 照してください。
役割サービス 確認 結果		
	Active Directory 証明書サービスの概要	
	<前へ(P) 次へ(N) > (2)2	(I) キャンセル

「次へ」をクリックします。

a	役割と機能の追加ウィザード	_ D X
	役割ご機能の追加リイサード 尺 Active Directory 証明書サービス のインストールする役割サービス 役割サービス 「▽」 証明機関 □ オンライン レスポンダー	対象サーバー AMAZONA-GOUIOC6 を選択します 説明 証明機関 (CA) は、証明書を発行およ び管理するために使用されます。複数の CA をリンクさせることで公開キー基盤を
機能 AD CS 役割サービス 確認 結果	 □ ネットワーク デバイス登録サービス □ 証明機関 Web 登録 □ 証明書の登録 Web サービス □ 証明書の登録ポリシー Web サービス 	構成できます。
	< 前へ(P) 次へ(N) > インストール(I) キャンセル

「証明機関」を選択し「次へ」をクリックします。

A	役割と機能の追加ウィザード	_ _ X
トレンストールオプシーンストールオプシーズーの運類 サーバーの運択 サーバーの役割 機能 AD CS 役割サービス	役割と機能の追加ウィザード マコンの確認 選択したサーバーに次の役割、役割サービス、または機能をインストールするには 必要に応じて対象サーバーを自動的に再起動する オブションの機能(管理ツールなど)は、自動的に選択されるため、このページに引 らのオブションの機能をインストールしない場合は、[前へ]をクリックして、チェック が Active Directory 証明書サービス 証明機関 リモート サーバー管理ツール 役割管理ツール 証明機関管理ツール	
	構成設定のエクスポート 代替ソース パスの指定 < 前へ(P) 次へ(N) >	インストール(I) キャンセル

「インストール」をクリックします。



インストール完了後、「対象サーバーに Active Directory 証明書サービスを構成する」をクリックします。

a	AD CS の構成	_ D X
資格情報	AM	対象サーバー IAZONA-GOUIOC6
 資格情報 役割サービス 確認 進行状況 結果 	 役割サービスを構成するための証明書を指定してください 次の役割サービスをインストールするには、ローカルの Administrators グループに属して スタンドアロン証明機関 証明機関 Web 登録 オンラインレスポンダー 次の役割サービスをインストールするには、Enterprise Admins グループに属している。 エンタープライズ証明機関 証明書の登録ポリシー Web サービス 証明書の登録 Web サービス 証明書の登録 Web サービス そットワーク デバイス登録サービス 資格情報: AMAZONA-GOUIOC6¥Administrator 変更(C)) こいる必要があります: 必要があります:
	AD CS サーバーの役割の詳細	
	<前へ(P) 次へ(N) > 構成	(C) キャンセル

「次へ」をクリックします。

	AD CS の構成	_ □ X
役割サービス		対象サーバー AMAZONA-GOUIOC6.test.local
資格情報 20割サービス セットアップの種類 CA の種類 秘密キー 暗号化 CA 名 有効期間 証明書データベース 確認 進行状況 結果	構成する役割サービスの選択	
	<前へ(P) 次へ(N) > 構成(C) キャンセル

「証明機関」のチェック確認後、「次へ」をクリックします。

a	AD CS の構成
セットアップの種類	対象サーバー AMAZONA-GOUIOC6.test.local
資格情報 役割サービス セットアップの種類 CA の種類 秘密キー 暗号化 CA 名 有効期間 証明書データベース 確認 進行状況 結果	CA のセットアップの種類を指定してください エンタープライズ証明機関 (CA) は、Active Directory ドメイン サービス (AD DS) を使用して証明書の管 理を簡略化できます。スタンドアロン CA では、AD DS を使用して証明書を発行または管理することはありませ ん。 ③ エンタープライズ CA(E) エンタープライズ CA(E) エンタープライズ CA はドメイン メンバーである必要があり、証明書または証明書ポリシーを発行するために通 常はオンラインです。 ③ スタンドアロン CA(A) スタンドアロン CA(A) スタンドアロン CA はワークグループまたはドメインのメンバーとなることができます。スタンドアロン CA は AD DS を必要とせず、ネットワーク接続なし (オフライン) で使用できます。
	セットアップの種類の詳細
	<前へ(P) 次へ(N) > 構成(C) キャンセル

「エンタープライズ CA」選択後、「次へ」をクリックします。

a	AD CS の構成
CA の種類	対象サーバー AMAZONA-GOUIOC6.test.local
資格情報 役割サービス セットアップの種類 CA の種類 秘密キー 暗号化 CA 名 有効期間 証明書データベース 確認 進行状況 結果	CA の種類を指定してください Active Directory 証明書サービス (AD CS) をインストールする場合は、公開キー基盤 (PKI) 階層を作成 または拡張します。ルート CA は、PKI 階層の最上位に位置し、自身の自己署名証明書を発行します。下位 CA は、PKI 階層内の上位の CA から証明書を受け取ります。 (・ ルート CA (R) ルート CA (は、PKI 階層で構成される最初の、また場合によっては唯一の CA です。 ・ 下位 CA(U) 下位 CA は、確立された PKI 階層を必要とし、階層内の上位の CA によって証明書の発行を許可されま す。
	CA の種類の詳細
	<前へ(P) 次へ(N) > 構成(C) キャンセル

「ルート CA」選択後、「次へ」をクリックします。

a	AD CS の構成
秘密キー	対象サーバー AMAZONA-GOUIOC6.test.local
資格情報 役割サービス	秘密キーの種類を指定してください
ゼットアップの種類 CA の種類 秘密キー	 ● 新しい秘密キーを作成する(R) 秘密キーがない場合、または新しい秘密キーを作成する場合は、このオプションを使用します。
暗号化 CA名 有効期間 証明書データベース 確認 進行状況 結果	 ○ 既存の秘密キーを使用する(U) CA の再インストール時に、以前に発行された証明書との連続性を確保する場合は、このオプションを使用します。 ○ 証明書を選択し、関連付けられている秘密キーを使用する(C) このコンピューターに既存の証明書がある場合、または証明書をインポートしてそれに関連付けられている 秘密キーを使用する場合は、このオプションを選択します。 ○ このコンピューターの既存の秘密キーを選択する(E) 以前のインストールの秘密キーを保持している場合、または代替ソースからの秘密キーを使用する場合 は、このオプションを選択します。 秘密キーの詳細
	<前へ(P) 次へ(N) > 構成(C) キャンセル

「新しい秘密キーを作成する」選択後、「次へ」をクリックします。

Ē.	AD CS の構成	_ _ ×
CA の暗号化	AMAZONA-G	対象サーバー GOUIOC6.test.local
資格情報 役割サービス	暗号化オプションを指定してください	
セットアップの種類	暗号化プロバイダーの選択(C): キー長(K):
CA の種類	RSA#Microsoft Software Key Storage Provider	•
秘密キー 暗号化 CA名 有効期間 証明書データベース 確認 進行状況 結果	この CA から発行された証明書の署名に使用するハッシュ アルゴリズムを選択(H): SHA256 SHA384 SHA512 SHA1 MD5 CA が秘密キーにアクセスするときに、管理者による操作を許可する。(A)	
		(C) +

各設定項目はデフォルトのままで「次へ」をクリックします。

	AD CS の構成
CA の名前	対象サーバー AMAZONA-GOUIOC6.test.local
資格情報 役割サービス セットアップの種類 CA の種類 秘密キー 暗号化 CA 名 有効期間 証明書データベース 確認 進行状況 結果	CA の名前を指定してください この証明機関 (CA) を識別する共通名を入力します。この名前は、CA で発行されるすべての証明書に付加さ れます。識別名のサフィックスは自動的に生成されますが、変更できます。 この CA の共通名(C): test 識別名のサフィックス(D): DC=test,DC=local 識別名のプレビュー(V): CN=test,DC=local
	CAの名前の詳細
	<前へ(P) 次へ(N) > 構成(C) キャンセル

「この CA の共通名」に適当な名称を入力して、「次へ」をクリックします。

a	AD CS の構成
有効期間	対象サーバー AMAZONA-GOUIOC6.test.local
資格情報 役割サービス セットアップの種類 CA の種類 秘密キー 暗号化 CA 名 有効期間 証明書データベース 確認 進行状況	有効期間を指定してください この証明機関 (CA) に対して生成される証明書の有効期間を選択(V): <u> 5</u> <u> 年間</u> ▼ CA の有効期限: 2018/06/04 7:02:00 この CA 証明書に対して構成する有効期間は、その CA が発行する証明書の有効期間を超えている必要があ ります。
	有効期間の詳細
	<前へ(P) 次へ(N) > 構成(C) キャンセル

「次へ」をクリックします。

B	AD CS の構成	_ D X
CA データベース	AMAZ	対象サーバー ZONA-GOUIOC6.test.local
資格情報	データベースの場所を指定してください	
セットアップの種類	証明書データベースの場所(C):	
CA の種類 ™応tー	C:+windows+system32+CertLog	
暗号化	C:¥Windows¥system32¥CertLog	
CA 名		
有効期間 証明書データベース		
確認		
進行状況		
結果		
	CA テータハースの計構	
	<前へ(P) 次へ(N) >	構成(C) キャンセル

「次へ」クリックします。

a	AD CS	の構成	_ D X
確認		AMAZONA-GOUIC	対象サーバー OC6.test.local
 資格情報 役割サービス セットアップの種類 CAの種類 秘密キー 暗号化 CA名 有効期間 証明書データベース 確認 進行状況 結果 	次の役割、役割サービス、または機制 Active Directory 証明書サ 証明機関 CA の種類: 暗号化プロバイダー: ハッシュ アルゴリズム: キー長: 管理者による対話操作を許可する: 証明書の有効期間: 識別名: 証明書データベース ログの場所: 証明書データベース ログの場所:	eを構成するには、[構成] をクリックします。 ナービス エンタープライズ ルート RSA#Microsoft Software Key Storage Provide SHA1 2048 無効 2018/06/04 7:02:00 CN=test,DC=test,DC=local C:¥Windows¥system32¥CertLog C:¥Windows¥system32¥CertLog	r
		<前へ(P) 次へ(N) > 構成(C)	キャンセル

「構成」をクリックします。

æ	AD CS の構成	_	D X
結果		対象 AMAZONA-GOUIOC6.tes	サーバー st.local
資格情報	次の役割、役割サービス、または機能が構成されま	した:	
役割サービス	▲ Active Directory 証明書サービス		
セットアップの種類	訂旧挑組		
CA の種類	CA 構成の詳細		
秘密キー			
暗号化			
CA 名			
有効期間			
証明書データベース			
確認			
進行状況			
結果	1		
	<前へ(P	?) 次へ(N) > 閉じる キャ	ンセル

「閉じる」をクリックします。



左下「Windows PoserShell ボタン]をクリックして起動し mmc と入力します。

· ·	コンソール1 - [コンソール ルート]	_ 🗆 X
ファイル(F) 操作(A) 表示(V) お気に入り(O) ウィンドウ(W)	(H)	_ & ×
◆ 新規作成(N) Ctrl+N		
□ 開く(0) Ctrl+0		操作
上書き保存(S) Ctrl+S	このビューに表示する項目はありません。	コンソール ルート 🔺
		他の操作 ▶
ステックインの追加と削除(M) Ctrl+M		
1. COWindows/autom/20/appnmant	-	
2 C:¥Windows¥system32¥eventywr		
3 C:¥Windows¥system32¥wbadmin		
終了(X)		
ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー	できます。	1

ウィンドウが開きますので、「ファイル」→「スナップインの追加と削除」をクリックしま す。

Microsoft and	Ĥ		払振の編集(X)
	1		
Microsoft Cor			削除(R)
Microsoft Cor			Dava (4
Microsoft Cor			
Microsoft Cor			上へ移動(U)
Microsoft Cor			下へ抱動(の)
Microsoft Cor		追加(A) >	
Microsoft Cor			
Microsoft Cor	=		
Microsoft Cor			
Microsoft Cor	$\overline{}$		詳細設定(V)
	Microsoft Cor Microsoft Cor	Microsoft Cor Microsoft Cor	Microsoft Cor Microsoft Cor

「証明機関」を選択し、「追加」をクリックします。

証明機関	x
このスナップインで管理するコンピューターを選択してください。 このスナップインで管理するコンピューター: ・ ローカル コンピューター(L): (このコンソールを実行しているコンピューター) ・ 別のコンピューター(A): ・ コマンド ラインから起動したときは、選択されたコンピューターを変更できるようにする(O) ごれば、コンソールを保存した場合にのみ適用されます。	
< 戻る(B) 完了 キャンセル ヘルプ	

「ローカルコンピューター」を選択し、「完了」をクリックします。

用できるスナップイン(S):			選択されたスナップイン(E):	
スナップイン	ペンダー	^	💷 コンソール ルート	拡張の編集(X)
🚽 ディスクの管理	Microsoft and		🔤 証明機関 (ローカル)	
📲 デバイス マネージャー	Microsoft Cor			削除(R)
♪テレフォニー	Microsoft Cor			
🔊 パフォーマンス モニター	Microsoft Cor			上へ移動自由
<u> </u> フォルダー	Microsoft Cor			T. 45 80(0)
🧊 ポリシーの結果セット	Microsoft Cor			下へ移動(D)
シルーティングとリモート アク	Microsoft Cor			
b ローカル バックアップ	Microsoft Cor			
투 ローカル ユーザーとグループ	Microsoft Cor			
🔋 共有フォルダー	Microsoft Cor			
🖪 承認マネージャー	Microsoft Cor	_		
氯証明機関	Microsoft Cor			
記明書	Microsoft Cor			
副 証明書テンプレート	Microsoft Cor	\sim		詳細設定(V)
明: 証明書スナップインを使うとユーサ	デー、サービス、また(お)	>ピコ	用書ストアの内容を閲覧できます。	

「証明書」を選択し、「追加」をクリックします。

	証明書スナ	ップイン		X
このスナップインで管理する証明書: 〇 ユーザー アカウント(M) 〇 サービス アカウント(S) ④ コンピューター アカウント(C)				
		< 戻る(B)	次へ(N) >	キャンセル

「コンピューターアカウント」を選択し、「次へ」をクリックします。

コンピューターの選択	x
このスナップインで管理するコンピューターを選択してください。 このスナップインで管理するコンピューター: ● ローカル コンピューター(L): (このコンソールを実行しているコンピューター)	
○別のコ>ピューター(A): 参照(R)	
□ コマンド ラインから起動したときは選択されたコンピューターを変更できるようにする(W) これは、コンソールを保存した場合にのみ適用されます。	
< 戻る(B) 完了 キャンセル	

「ローカルコンピューター」を選択し、「完了」をクリックします。

•		■コンソール ルート 「毎証明機関 (ローカル) 「↓ 証明書 (ローカル コンピューター)	拡張の編集(X) 削除(R)
		。証明機関(ローカル) □ 証明書(ローカル コンピューター)	 削除(R)
		☞ 証明書 (ローカル コンピューター)	削除(R)
			上へ移動(U)
h			
			下へ移動(D)
	追加(A) >		
=			
_			
\sim			詳細設定(V)
	=		

「証明書テンプレート」を選択し、「追加」をクリックします。

			スナップイン	の追加と削除	X
コンピューターで利用できるスナッフ は、どの拡張を有効にするかを構成	インからこのコンソールI 成できます。	₽使	用するスナップインを	選択したり、選択したスナップインを構成した!	りできます。 拡張可能なスナップインで
利用できるスナップイン(S):				選択されたスナップイン(E):	
スナップイン ディスクの管理 デバイスマネージャー 参テレフォニー (1)パフォーマンスモニター フォルダー 「ポリシーの結果セット 夏ルーティングとリモートアク ゆーカル バックアップ テローカル ユーザーとグループ 認 共有フォルダー 「 スマネージャー	ペンダー Microsoft and Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor		追加(A) >	 □ コンソール ルート □ 証明機関 (ローカル) □ 証明書 (ローカル コンピューター) ☑ 証明書テンプレート 	拡張の編集(X) 削除(R) 上へ移動(U) 下へ移動(D)
■ 証明機関 ■ 証明書 ■ 証明書テンプレート 説明:	Microsoft Cor Microsoft Cor Microsoft Cor	~			詳細設定(V) OK キャンセル

「OK」をクリックします。

- E - E - E - E - E - E - E - E - E - E	コンソール1 - [コンソール ルート¥証明書	テンプレート (AMAZONA	-GOUIC)C6.test.local)]	_ D X
逼 ファイル(F) 操作(A) 表示(V)	お気に入り(O) ウィンドウ(W) ヘルプ(H)				_ 8 ×
🗢 🄿 🖄 🖬 🗎 🖬 🖬					,,
📔 コンソール ルート	テンプレート表示名	スキーマのバージョン	八	使用目的 ^	操作
▶ 🚋 証明機関 (ローカル)	💷 キー回復エージェント	2	105.0	キー回復エージュ	証明書テンプレート(Δ ▲
▶ 🗊 証明書 (ローカル コンピューター) .	🗟 クロス証明機関	2	105.0		
図 証明書テンプレート (AMAZOI)	凰 コード署名	1	3.1		
	🖳 コンピューター	1	5.1		ドメイン コントローラーの 🔺
	🖳 スマート カード ユーザー	1	11.1		他の操作 ▶
		1	6.1		
	■ ディレクトリ電子メール レプリケーション	2	115.0	ディレクトリ サーと	
		1	4.1		
	◎ ドメイン コントローラーの認証	。 変制ない	110.2	クライアント認証,	
-		吃毁(U)	3.1		
· · · · · · · · · · · · · · · · · · ·	■ユーザー署名のみ 証明書保持者	をすべて再登録する(E)	4.1		
· · · · · · · · · · · · · · · · · · ·	別 ルーター (オフライン要求 すべてのタスク	(K) I	4.1		
· · · · · · · · · · · · · · · · · · ·	■ ルート証明機関 プロパティ(R)	1	5.1		
1	图 ワークステーション認証		.01.0	クライアント認証	
1	図 トロの証明機関 へルプ(H)		p.1	-	
· · · · · · · · · · · · · · · · · · ·	圏管理者	1	4.1		
1	圏 基本 EFS 同 伝統uztamed	1	3.1		
1	■ 信頼リストの著名	1	3.1		
1		1	4.1		
	Ξ 豆琢エーンエノド (コノビエーダー) □ 認証されたないとっと。	1	D.1		
·	(語) 私のお上〇! いっピッション	T	5.1	~	
< III >	٢ ١١١			>	
選択した項目のプロパティ ダイアログ ボック	スを開きます。				

2.証明書の有効期限

「証明書テンプレート」をクリックし、「ドメインコントローラの認証」で右クリックして、「プ ロパティ」を選択します。

	ドメイン コントローラーの認証のプロパティ
発行の要件	優先するテンプレート 拡張機能 セキュリティ サーバー
モカレート表示	_ 互換性 要求処理 暗号化 サノジェクト名 示名(F):
「シインコントロ	コーラーの認証
テンプレート名(Έλ:
DomainCon	trollerAuthentication
有効期間(V):	更新期間(R):
20 年	6週 ~ ~
L	
Active Dir	rectory の証明書を発行する(P) e Directory に重複する証明書がある場合、自動的に再習録しない(D)
	OK キャンセル 適用(A) ヘルプ

「有効期限」を確認し、20年などの長い期間に設定し、「OK」をクリックします。

3.証明書の作成

	コンソール	1 - [コンソー	ルルート¥証明書	(ローカル	, コンピュータ-	-)¥個人¥証明	月書]		-	x
🚟 ファイル(F) 操作(A) 表示(V)	お気に入り(0)	ウィンドウ (W)	へルプ(H)							 5 ×
🗢 🄿 🖄 📰 📋 🗟 😹	?									
🧰 コンソール ルート	発行先	•	発行者			有効期限	目的	操作		
▶ 🔝 証明機関 (ローカル) ▲ 🗊 証明書 (ローカル コンピュータ	ltest		test			2018/06/04	<97(>	証明書		-
⊿ 1 個人								他の操作		•
▶ 📔 信頼されたルート証明機関		র শ্বে <i>তা</i> গ	スク(K)	▶ <u></u>	记い証明書の要	駛 (R)				
▶ エンターフライスの信頼 ▶ 11 中間証明機関		最新の情	報に更新(F)	1	ンポート (I)		_			
▶ 🧰 信頼された発行元		一覧のエク	Ⴢスポート (∟)	t i	細設定操作(A)	•			
▶ 📔 信頼されていない証明書		表示(V)		•						
▶ 📔 目頼されたユーザー		アイコンの	整列(I)	•						
▶ 📔 クライアント認証発行者		等間隔に	整列(E)							
▶ 🛄 リモート テスクパック ▶ 🛅 証明書の登録要求		へレプ(H)	1							
▶ 📋 スマートカードの信頼された										
▶										
			III				>			
F×1 ンの証明機関 (CA) から新しい温い	明香を要求します									

左ペインで「証明書」→「個人」→「証明書」を選択します。 中央ペインの何もないところで右クリックし、「すべてのタスク」→「新しい証明書の要 求」をクリックします。

	x
📮 証明書の登録	
開始する前に	
次の手順では証明書をインストールします。証明書はデジタル資格情報で、ワイヤレス ネットワークへの接続、コンテンツの 保護、識別情報の確立、およびその他のセキュリティ関連タスクの実行に使用されます。	
証明書を要求する前に、次の点を確認してください:	
使用するコンピューターがネットワークに接続されている 証明書を取得する権利があることの確認に使用できる資格情報を持っている	
<u>デジタル証明書の詳細</u> について表示します	
次へ(N) キャンセル	

「次へ」をクリックします。

■ 証明書の登録
証明書の登録ポリシーの選択 証明書の登録ポリシーは、あらかじめ定義された証明書テンプレートに基づく登録を可能にするものです。場合によっては、 証明書の登録ポリシーは既に構成されていることがあります。
システム管理者が構成します
Active Directory 登録ポリシー ~
ユーザーが構成します 新規追加
次へ(N) キャンセル

「Active Directory 登録ポリシー」を選択し、「次へ」をクリックします。

		_ D X
📮 証明書の登録		
証明書の要求		
次の種類の証明書を要求できます。要求する証明	目書を選択し、[登録]をクリックしてください。	
Active Directory 登録ポリシー		
☐ Kerberos 認証	🤨 状態: 利用可能	詳細 ~
□ ディレクトリ電子メール レプリケーション	••• 状態:利用可能	詳細 ~
□ Ҟメイン コントローラー	 以 状態:利用可能 	詳細 ~
✓ ドメイン コントローラーの認証	🕠 状態:利用可能	詳細 ~
□ すべてのテンプレートの表示(A) 証明書の詳細について表示します		
ALCOHOLOGIC AVICANDOS >		
	R. S.	登録(E) キャンセル

「ドメインコントローラの認証」を選択し、「登録」をクリックします。

🗔 it	明書の登録		– – X
	証明書インストールの結果		
	次の証明書が登録され、コンピューターにイ:	ンストールされました。	
	Active Directory 登録ポリシー		
	☑ ドメイン コントローラーの認証	√ 状態: 成功	詳細 ~
			完了(F)

「完了」をクリックします。

4.証明書のエクスポート



中央ペインでさきほど作成したものを選択して右クリックで表示されるメニューから、 「すべてのタスク」→「エクスポート」を選択します。



「次へ」をクリックします。

×
📀 🐓 証明書のエクスポート ウィザード
秘密キーのエクスポート
秘密キーを証明書と一緒にエクスポートすることができます。
秘密キーはパスワードで保護されています。秘密キーを証明書と一緒にエクスポートする場合は、パスワードを 入力する必要があります。
証明書と一緒に秘密キーをエクスポートしますか?
○ はい、秘密キーをエクスポートします(Y)
● いしえ、秘密キーをエクスポートしません(0)
注意: 関連付けられた秘密キーにはエクスポート不可能フラグが付いています。証明書だけをエクスポート できます。
<u>秘密キーのエクスポートの詳細</u> を表示します
次へ(N) キャンセル

「いいえ、秘密キーをエクスポートしません」がチェックされていることを確認し、「次 へ」をクリックします。

	^
エクスポート ファイルの形式	
さまざまなファイル形式で証明書をエクスポートできます。	
使用する形式を選択してください:	
O DER encoded binary X.509 (.CER)(D)	
Base 64 encoded X.509 (.CER)(S)	
○ Cryptographic Message Syntax Standard - PKCS #7 証明書 (.P7B)(C)	
□ 証明のパスにある証明書を可能であればすべて含む(I)	
O Personal Information Exchange - PKCS #12 (.PFX)(P)	
□ 証明のパスにある証明書を可能であればすべて含む(U)	
□ 正しくエクスポートされたときは秘密キーを削除する(K)	
□ すべての拡張プロパティをエクスポートする(A)	
○ Microsoft シリアル化された証明書ストア (.SST)(T)	
<u>証明書ファイルの形式の詳細</u> を表示します	
次へ(N) キャンセ	JL

「Base 64 encoded X.509(.CER)」を選択し、「次へ」をクリックします。

	X
중 🥩 証明書のエクスポート ウィザード	
エクスポートするファイル	
C:¥Users¥Administrator¥Desktop¥test.cer	参照(R)
· · ·	
	次へ(N) キャンセル

「ファイル名」を入力し、「次へ」をクリックします。 ※ファイル名はなんでも構いません。

중 중 証明書のエクスポート ウィザー	4	X
	証明書のエクスポート ウィザード	『の完了
	証明書のエクスポート ウィザードが正常に完	了しました。
	次の設定が指定されました:	
	ファイル名	C:¥Users¥Admini
	キーのエクスボート	いいえ
	証明のバスにあるすべての証明書を言める	UNIZ Dece 64 Enceded
	× m	
		完了(F) キャンセル

「完了」をクリックします。



「OK」をクリックします。

参考:証明書の内容

tes	: - Xモ帳	X	i i
ファイル(F) 編集(E) 書式(O) 表示(V) ヘノレプ(H)			
III CARDING CARDING CONTRACT AND CONTRACT			
		 1.5	(* 188.) 1