

プライベートCA Gléas ホワイトペーパー

NetWiser でのクライアント証明書認証

Ver.1.0

2024年05月

Copyright by JCCH Security Solution Systems Co., Ltd. All Rights reserved

- JCCH・セキュリティ・ソリューション・システムズ、JS3 およびそれらを含むロゴは日本および他の国における株式会社 JCCH・セキュリティ・ソリューション・システムズの商標または登録商標です。Gléas は株式会社 JCCH・セキュリティ・ソリューション・システムズの商標です。
- その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。
- Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

Copyright by JCCH Security Solution Systems Co., Ltd. All Rights reserved

目次

1. はじ	めに	5
1.1.	本書について	5
1.2.	本書における環境	6
1.3.	本書における構成	8
1.4.	証明書発行時における留意事項	9
2. NetV	Viser の設定	10
2.1.	サーバ証明書の発行と登録	10
2.2.	ルート証明書の登録	
2.3.	失効リスト (CRL) の登録	20
2.4.	実サーバーの登録	22
2.5.	NAT プールの登録	26
2.6.	仮想サーバーの登録	29
2.7.	SSL アクセラレーション設定	
3. Gléa	s の管理者設定 (Windows 向け)	
4. クラ	イアントの設定 (Windows)	
4.1.	クライアント証明書のインポート	

	4.2.	Web サーバアクセス4	.0
5.	Gléas	の管理者設定 (iPhone 向け)4	2
6.	クライ	'アントの設定 (iPhone)4	5
	6.1.	クライアント証明書のインポート4	.5
	6.2.	Web サーバアクセス4	.8
7.	Web	サーバでクライアント証明書情報を取得4	.9
8.	問い合	うわせ5	2

1. はじめに

1.1. 本書について

本書では、弊社製品 プライベートCA Gléas で発行したクライアント証明書を利用し て、セイコーソリューションズ株式会社の NetWiser で SSLオフロードしたロード バランシング (Web負荷分散) 構成でクライアント証明書認証をおこなう環境を構築 するための設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる 環境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例 としてご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合 は、最終項のお問い合わせ先までお気軽にご連絡ください。

1.2. 本書における環境

本書は、以下の環境で検証をおこなっております。

➢ SSLロードバランサー

Netwiser Virtual Edition SX-3990 (v8.4.10)

※以後、「NetWiser」と記載します

> 認証局: JS3 プライベートCA Gléas (バージョン2.7.1)

※以後、「Gléas」と記載します

> Webサーバ: AlmaLinux release 9.2 / Apache 2.4.53

※以後、「Webサーバ」と記載します

クライアント: Windows10 Pro 22H2 / Microsoft Edge 124.0.2478.9

※以後、「Windows」と記載します

▶ クライアント: iPhone14 (iOS 16.3) / Safari

※以後、「iPhone」と記載します

以下については、本書では説明を割愛します。

- NetWiser の基本設定 (ネットワークや基本的な負荷分散に関する設定)
- Webサーバの基本設定 (ネットワークや基本的なWebページ公開設定)
- Gléasでのユーザ登録やクライアント証明書発行などの基本操作
- クライアント端末におけるネットワーク設定など

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱ってい る販売店にお問い合わせください。

1.3. 本書における構成

本書では、以下の構成で検証を行っています。



- Gléasでは、NetWiserにサーバ証明書を、PCとiPhoneにクライアント証明書を発行する。
- 2. PCとiPhoneはGléasより証明書をインポートする。
- 3. PCではEdgeブラウザ、iPhoneではSafariブラウザよりNetWiserの仮想サーバー

にアクセスし、NetWiserはクライアント証明書認証をおこなう。

証明書認証後にロードバランスしているWebページをクライアントに表示。

証明書を提示しない、期限切れ、または失効している、端末はクライアント証明

書認証に失敗。

1.4. 証明書発行時における留意事項

Gléasで電子証明書を発行する際に以下の点に留意する必要があります。

● 本書2.1の方法でサーバ証明書を発行する場合は、事前にサーバアカウントを作

成しておき、[SSLサーバ証明書]ロールグループに参加させる必要があります。

2. NetWiser の設定

2.1. サーバ証明書の発行と登録

仮想サーバーで使用するサーバ証明書をGléasから発行し、NetWiser に登録します。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [SSL] の [SSL証明書] をクリ

ックします。

[SSL証明書]画面で以下を入力し、SSLポリシーを作成します。

● [SSLポリシー]には、任意の名前を入力

			SEIKO
netwije	設定機器情報	リアルタイム情報 統計情報 ログ参照	
ホスト名 : ユーザー名: 権限 : Admin権限	SSL証明書	→/- 表示状態を反映	
設定 ネットワーク アE編成	SUパリシー 削除 SUパリシー (example) 行追加		
SSL SSL証明書 注印書先効リスト ブロキシサーパー ・プロキシサーパー SSL証明書客名要訳作成 ・SSLインボート SSLエクスポート ・SSLエクスポート メニ 目明書の指述 運動音曲参更新 運動音曲参更新	★ 設定内容を変更する		
バランシング			
\$276			

入力後、[設定内容を変更する]ボタンをクリックするとSSLポリシーが作成されます。

続いてCSRを作成します。

メニュー [SSL] の [SSL証明書署名要求作成] をクリックします。

[SSL証明書署名要求作成]画面で以下を入力し、CSRを作成します。 ※以下はRSA 2048 ビット長の鍵を使用してCSRを作成する例です。

- [SSLポリシー名]に、先に作成したSSLポリシーを選択
- [ECC証明書]のチェックを外す
- [公開鍵長]に、[2048] を選択
- [サーバーのFQDN]に、公開する仮想サーバーのFQDNを入力
- [国名 (Country)]を入力
- [都道府県名 (State)]を入力
- [組織名 (Organization)]を入力
- 他の項目は、環境に応じて設定

	-						SEIKO
netwije	er -	設定	機器情報	リアルタイム情報	統計情報	ログ参照	
ホスト名 :		SSL証明書署名要求作成			+/-	表示状態を反映	
推限 : Admin権限		🔤 CSR(署名要求)設定 🜏					
設定		SSLポリシー名		example 🗸			
ネットワーク	×	ECC证明書		□ 有効			
冗長構成	×	公開鍵長		2048 🗸			
SSL	×	楕円曲線パラメーター	3	未選択 🖌			
▶ SSL証明書		サーバーのFQDN	example.jcch-	sss.com			
 証明書失効リスト プロセミサーバー 		国名 (Country)		JP			
SSL証明書署名要求作成		都道府県 (State)	Tokyo				
 SSLインボート SSLインボート 		区市町村 (Locality)	Arakawa-ku				
 ・ 鍵、証明書の削除 		組織名 (Organization)	JCCH-SSS				
証明書自動更新	×	部門名(Organization Unit)					
バランシング	*	メールアドレス(Email Address)					
ヘルスチェック	×				_		
システム	*	3.0.4.0.4.7.7.4.7					
		設定内容を変更する					

入力後、[設定内容を変更する]ボタンをクリックするとCSRが作成されます。

続いて作成したCSRをダウンロードします。

メニュー [SSL] の [SSLエクスポート] をクリックします。

[SSLエクスポート]画面で[csr]リンクをクリックして、CSRをPCにダウンロードします。

			SEIKO
INETWIJE	er	設定 機器情報 リアルタイム情報 統計情報 ログ参照	
ホスト名 : sales-netwiser ユーザー名 : admin 権限 : Admin権限		設定変更後保存されていません。保存する場合は右のボタンより、保存してください。 (以存する)	
設定		SSLエクスポート +/- 表示状態を反映	
ネットワーク	¥	🚍 ファイル選択 📀	
冗長構成	×	ー 右クリックから保存してください.	
SSL	×	- ce: ポリシーク (35歳時) 2000年 → 995200年 cs目2500年/トニノマント第323 cen/常夕正式) cn: (十計) 12 ト) 12/001212寸	
 > SSL証明書 > 証明書先効リスト > プロキシサーバー > SSL証明書署名要求作成 > SSLインポート > SSLインポート > 単、証明書の利能 延明書自動更新 	•		
バランシング	*		
ヘルスチェック	*		
システム	×		

Gléas (RA) にログインし、該当のサーバアカウントのページへ移動します。

サーバ属性の[編集]をクリックし、ホスト名に公開する仮想サーバーの FQDN を入力

します。

小メニューの[証明書発行]をクリックします。

細			■認証局 ■ログ ■管理者 ■ヘルブ ■ログア	
7カウント		· · · · · · · · · · · · · · · · · · ·		三三〇 ▶ クイックナビ
example.jcch-sss.com				<u>2 8 ユーザ証明書</u>
▶ アカウント情報 ······		ᇦ グループ情報 · · · · ·		▲ <u>マン200月書</u> ■ <u>サーバ証明書</u>
▶サーバ 登録	录日時:2024/05/14 11:18	▶ユーザグループ	■参加	🏦 認証局証明書
> ステータス: 有効		> <u>SSLサーバ証明書</u>	⊠ <u>削除</u>	
▶ サーバ属性 最終更新	:2024/05/14 11:18 編集		a 4 m	
> 木スト名:example.jcch-sss.com		SRL.	L S/II	保存
★ 証明書発行の履歴 ······				▶ ドック ■ アカウント (0)
P1				★証明書(0)
# シリアル 開始	有効期限 ステ	ータス 失効日	暗号種別 トークン	
	証明書は発行さ	れていません。		
▶ テンプレート情報				
■ テンプレート情報 ····································				
 ► テンプレート情報 ► サブジェクト 経別 		必須テンプレート	任意テンプレート	
► テンプレート情報 ◆ サブジェクト 種別 飯名(CN)	example.jcch-sss	必須テンプレート .com	任意テンプレート	
 ► ナンプレート情報 ► サブジェクト 値81 - 般名(CN) ドンインコンボーネント(DC) 	example.jcch-sss jcch-sss com	必須テンプレート .com	任意デンブレート	
 ⇒ テンブレート情報 > サラジェクト 	example.jcch-sss jcch-sss com	必須デンプレート com	任意デンブレート	
 ► テンプレート情報 ● サブジェクト ④ 値別 一般名(CN) ドメインコンボーネント(DC) ▶ 間性 	example jcch-sss jcch-sss com	必須デンブレート .com 必須テンプレート	任意デンプレート	
 ► テンプレート情報 ► サブジェクト 経約 一般名(CN) ドメインコンボーネント(DC) ▶ 既性 経約 発行局 	example.jcch-sss jcch-sss com JCCH-SSS demo2	心須テンプレート .com 必須テンプレート CA	任意デンプレート	
 ► テンプレート情報 ► サブジェクト 程別 ー般名(CN) ドメインコンボーネント(DC) ▶ 器性 種別 発行局 ■第ラアルゴリズム 	example.jcch-sss jcch-sss com JCCH-SSS demo2/ RSA#375	必須テンプレート .com 必須テンプレート CA	任意デンプレート	
 ► テンプレート情報 ► サブジェクト 任引 最名(CN) F≫(ンコンボーキント(DC) ► 居性 私別 発行局 昭号アルニリズム 健長 	example.jcch-sss jcch-sss com JCCH-SSS demo2 / RSA语号 2048bit	必須テンプレート com 必須テンプレート CA	任意デンプレート	
 ► テンプレート情報 ► サブジェクト 単初 ● 単句 ● 単句<!--</td--><td>example jcch-sss jcch-sss com JCCH-SSS demo2 / RSA8특芬 2048bit SHA256</td><td>必須デンプレート .com 必須デンプレート CA</td><td>任意デンプレート</td><td></td>	example jcch-sss jcch-sss com JCCH-SSS demo2 / RSA8특芬 2048bit SHA256	必須デンプレート .com 必須デンプレート CA	任意デンプレート	
 ► テンプレート情報 ● サブジェクト	example jcch-ses jcch-ses com JCCH-SSS demo2 / RSA语号 2048时 SHA256 1年	 必須デンプレート com 必須デンプレート CA 	任意テンプレート	
 ► テンプレート情報 ► サブジェク사 ④ 但別 ● 応名(CN) ► ドット(ンコンボーキント(DC) ▶ 時世 ● 初期 ● 近日 	example jcch-sss jcch-sss jcch-sss jcch-sss jcch-sss jcch-sss demo2 JCCH-SSS demo2 RSA音号 2048时 SHA256 1年 電子署名 握分增号比	 必須テンプレート com 必須テンプレート CA 	任意デンブレート	
 ► テンプレート情報 ● サブジェクト ■ 運動 - 成名(CN) ドメイノコンボーネント(DC) ▶ 既性 ● 既性 ・ 取り 一般行局 昭等アル・コンズム 一般系 ※ ダイジェストアル・コンズム 第二、「アル・コンズム 第二、 ※ 現用途 201 201	example.jcch-sss jcch-sss com JCCH-SSS demo2 / RSA程号 2048bit SHA256 1年 電子署名 課の培若化 SSLサー/花器 SSLサー/花器	 	任意デンプレート	
 ► テンプレート情報 ▲ サブジェクト ▲ 経別 - 成名(CN) ドメインコンボーキント(DC) ▶ R性 ● 花り 発行局 昭号アルコンズム 総長 ダイジェストアルコンズム 福号用途 超信線用途 野ど(DNS) 	evample.jcch-sss icch-sss com JCCH-SSS demo2 RSA용하 2048bit SHA256 1年 電子署名 建아뮤콤仁 SSLサ-기 단질프 SSLサ-기 단질프 SSLサ-기 단질프 SSLサ-기 단질프 SSLサ-기 관점프	 必須テンプレート com 必須有シンプレート CA com 	任意デングレート	

上級者向け設定を展開し、以下の操作をおこないます。

● 証明書要求 (CSR) ファイルをアップロードする : の[ファイルの選択]ボタンより

ダウンロードした CSR ファイルを選択

アカウント」>証	明書発行	■認証局 ■ログ ■管理者 ■ヘルブ ■ログアウト	●サイドバー 📮
🖕 アカウント	7カウント		▶ クイックナビ
Account	example.jcch-sss.com		<u> 고 - <i>サ証明書</i></u>
ラ グループ Group	<u> </u>		
- 137 RB 32	★ 証明書発行		🔳 サーバ証明書
Certificate	この画面では証明書要求の作成を行います。		会認証局証明書
認証デバイス Device	左側の「サブジェクト」と「腐性」の内容で証明書要求を作成します。 右側のテンプレートの中から必要なものを選択して「発行」を押してください。		
テンプレート	▶ 証明書発行		
remplate	> 下記の内容で証明書を発行します。よろしければ「発行」を押してください。		保存
アカウント操作	 第 1 1		
アカウント一覧	> 証明書要求(CSR)ファイルをアップロードする: ファイルの選択 example.csr		▶ ドック ● アカウレト (0)
登録申請者一覧	> □ CSRファイルの内容を確認する		●証明書 (0)
アカウント新規作成		17	
▶証明書発行			
	▶ サブジェクト	▶ 選択されているテンプレート ■全て解除	
	> CN=example.jcch-sss.com	> 必須 デフォルト設定	
	> DC=jcch-sss, com	▶必須 SSLサーバ証明書	
	▶属性	▶ 選択可能なテンプレート	
	> 発行局:JCCH-SSS demo2 CA	> /al.	
	> 暗号アルゴリズム:RSA暗号		
	> 鍵長: 2048bit		
	> 3/1 シェスドアルコリスム; SHA200 、 右加日数・1年		
	> 2010年10日本・1日 → 2011年11日本・1日 → 2011年1日本・1日 → 2011年1日本・1日本・1日本・1日本・1日本・1日本・1日本・1日本・1日本・1日本・		
	> 拡張鏈用途:SSLサーバ認証,SSLクライアント認証		
	> 別名(DNS): example.jcch-sss.com		

その後、[発行]ボタンをクリックします。

証明書発行完了後、証明書詳細画面の証明書ファイル欄の「証明書:あり」リンクをク

明書]>詳細	● 認証局 ● ログ ●管理者 ● ヘルブ ● ログアウト	● サイドバー
アカウント 証明書		▶クイックナビ
Account	► <u>122</u>	<u> ユーザ証明書</u>
Group 参 訂明書情報		■ <u>マンノ部明書</u>
証明書 Certificate	開始日:2024/05/14 12:02 終了日:2025/05/14 12:02	☆認証局証明書
認証デバイス Device ▶説明:	最終更新:2024/05/14 12:03 <mark>編集</mark>	
テンプレート	人表本情報	
Template	> 作成日:2024/05/14 12:01	保存
明書操作 >都道府県:Tokyo	> 有幼日数:365	5 Pm/2
唐一覧 > 市区町村: Arakawa-ku	> 失効日:	▶ トック ■ アカウント (0)
»勉処理 > 組織: JCCH-SSS	> 失効理由:	★証明書 (0)
▶ 一般名: example.jcch-sss.com	> 期限終了日:	
ックに入れる	> 状態: 有効な証明書	
	> 处理(2)状態:有効な証明書	
	>トージン必要: 、パージーン・・・・	
▶ 証明書情報		
> 認証局: <u>JCCH-SSS demo2 CA</u>		
> 暗号アルゴリズム:rsa		
> タインエストアルコリスム:sna256 > 304 E + 2049		
> 練用途: 電子署名 練の暗号化		
> 拡張鍵用途: SSLサーバ認証 SSLクライアント認証		
> 別名: <u>DNS名:example.jcch-sss.com</u>		
▶ 証明書ファイル		
> 証明書要求: <u>赤リ</u>		
作成日時 2024/05/14 12:01		
> 証明書: あり (ただ日間: 2024/05/14 12:02)		
1 10×10 9 2024000 14 12:03		
a no mate - roo	•	

リックし、発行された証明書をダウンロードします。

NetWiserのWeb管理画面に戻り、メニュー [SSL] の [SSLインポート] をクリックしま

す。

[SSLインポート]画面で以下を入力し、サーバ証明書をインポートします。

- [SSLポリシー名] に作成したSSLポリシーを選択
- [サーバ証明書]の[ファイルの選択]をクリックし、先にダウンロードした証明書フ

NECLVVIJEC 設定 機器信組 リアルタイム信組 転計信組 ロク参照 ポストス・: コーサーキ: コーサーキ: マーサーキ: マーサーキ: オーサーキ: オーサーキ: オーサーキ: マーサーキ: オーキ: オーサーキ: オーサーキ: オーサーキ: オーサーキ: オーキ: オーサーキ: オーサーキ: オーキ: オーサーキ: オーサーキ: オーサーキ: オーキ: オーキ: オーキ: オーサーキ: オーキ: オーサーキ: オーキ: オーキ: オーキ: オーキ: オーキ: オーキ: オーキ: オ	NIATING OF			SEIKO
ALMA: A: Administration Batta Stage (# per a tr. Uv # th.i. # # Pr 5 % = dia ta Om/ Po / s / 0. # # Pr 5 % = dia ta Om/ Po / s / 0. # # Pr 5 % = dia ta Om/ Po / s / 0. # # Pr 5 % = dia ta Om/ Po / s / 0. # # Pr 5 % = dia ta Om/ Po / s / 0. # # Pr 5 % = dia ta Om/ Po / s / 0. # # Pr 5 % = dia ta Om/ Po / s / 0. # # Pr 5 % = dia ta Om/ Po / s / 0. # # Pr 5 % = dia ta Om/ Po / s / 0. # # Pr 5 % = dia ta Om/ Po / s / 0. # # Pr 5 % = dia ta Om/ Po / s / 0. # # # # # # # # # # # # # # # # # #	netwijer	設定	機器情報 リアルタイム情報 統計情報 ログ	参照
放定 SSLインホート 4/- 弦示状盤を反映 オットワーク * # 証明書情報 プロス細点 * # 近日書書 * 55L * * * <	たスト名 : ユーザー名 : ケ限 : Admin権限	設定変更後保存されていません。	保存する場合は右のボタンより、保存してください。 保存する	
ネットワーク (単) 組 証券当格組 万度風炊 (一) パンジー名 (コーノー証券当) (A 紅琴海音) (A 紅琴) (A 紅琴海音) (A 紅琴) (A 紅琴) (A 紅琴) (A 紅 田 山雪) (A 山 山雪) <th< td=""><td>設定</td><td>SSLインポート</td><td>+/- 表示状態を</td><td>反映</td></th<>	設定	SSLインポート	+/- 表示状態を	反映
TXEAM イリシー名 サーバー経明書 中国国明書 び名目標 PASE SSL * 2048 * SSL管備書 * 2048 * SSL管備書を表示れな、 SSL(インボート * 2048 * SSL(F) * * SSL(F) * (example) * SSL(F) * (example) * SSL(F) * (example) * SSL(F) * (example) * SSL(F) * (example) * SSL(F) * (example) * SSL(F) * (example) * SSL(F) * (for the field of	ネットワーク ×	▶ 鍵、証明書情報		
SSL	冗長構成 ※	ポリシー名 サーバー証明書 中	問証明書 CA証明書 秘密鍵	
	SSL ×	example	2048	
Erringたがリントへ SSLポリシー名 SSLポリシー名 Example SSLポリシーA SSLポリシーA Example SSLポリシーA Example PKCSL2形式 Jアイルの選択 ファイルが選択されていません SSLペンパート SSLペンパート SSLペンパート SSLポリシーA Example Jアイルの選択 ファイルが選択されていません SSLペンパート SSLポリシーA SSLポリシーA Example Jアイルの選択 ファイルが選択されていません SSLポリシーA SSLポリカリ SSLポリ SSL	▶ SSL証明書	🚍 ファイル選択 🕜		
SQL は明書名表示作成 SQL インパート PKCS12形式 ファイルの選択 ファイルが選択されていません SQL TO スパート ・	 証明書矢切り入下 プロキシサーバー 	SSLポリシー名	example 🗸	
シミレアパート 秘密健 ファイルの選択 ファイルの選択 ファイルの選択 ファイルの選択 実現者自動受新 × /パスフレーズ	 SSL証明書署名要求作成 SSL証明書署名要求作成 	PKCS12形式	ファイルの選択 ファイルが選択されていません	
▶ は 社の語の制作 実現自由登録 ※ バランジング ※ サーバー互明書 ファイルの選択 download.crt	 SSLエクスポート 	秘密鍵	ファイルの選択 ファイルが選択されていません	-
バランシング × サーバー証明書 ファイルの選択 download.ct	 ・ 類、証明書の削除 証明書自動更新 	パスフレーズ		
	バランシング ×	サーバー証明書	ファイルの選択 download.crt	
ヘルスチェック ※ 中間証明書 ファイルの選択 ファイルが選択されていません ○上書き ◎ 階層化	ヘルスチェック ×	中間証明書	 ファイルの選択 ファイルが選択されていません 〇 上書き ◎ 階層化	
	э л г ь ×	 CA局証明書(クライアント認証)	ファイルの選択 ファイルが選択されていません ○上書き ◎ 階層化	 \$

ァイルを選択しアップロード

入力後、[ファイルをインポートする]ボタンをクリックすると、SSL ポリシーに紐づく

サーバ証明書がインポートされます。

サーバ証明書がインポートされると、[SSL インポート]画面の[サーバ証明書]欄に

[valid]と表示されます。

SSLインオ	ペート			
🔒 鍵、証明書	彗情報			
ポリシー名	サーバー証明書	中間証明書	CA証明書	秘密鍵
example	valid			2048

2.2. ルート証明書の登録

クライアント証明書によるSSL認証を利用するためには、ルート証明書の登録が必要で す。これは、クライアントから提示される証明書が正しいことを検証する際に利用する ためです。

本手順の前にGléasよりルート証明書をダウンロードします。

※GléasのデフォルトCAのルート証明書 (PEM形式) のダウンロードURLは以下となります http://[GléasのFQDN]/crl/ia1.pem

NetWiserのWeb管理画面にログインし、[設定]タブを選択、メニュー [SSL] の [SSLイ

ンポート]をクリックします。

[SSLインポート]画面で以下を入力し、サーバ証明書をインポートします。

- [SSLポリシー名] に2.1章で作成したSSLポリシーを選択
- [CA証明書 (クライアント認証)]の[ファイルの選択]をクリックし、Gléas よりダ

							SEIKO	
INGUMINE	?r	設定	機器情報 リス	アルタイム情報	統計情報	ログ参	照	
ホスト名 : ユーザー名 : 権限 : Admin権限		設定変更後保存されていません。	呆存する場合は右のボタンよ	:り、保存してください	/)。 保存する			
設定		SSLインポート			+/- 쿺	も示状態を反	B.	
ネットワーク	×	▶ 鍵、証明書情報						
冗長構成	×	ポリシー名 サーバー証明書 中	間証明書 CA証明書 秘密的	8				
SSL	×	example valid	204	8				
▶ SSL証明書		🚍 ファイル選択 😢						
 ゴロキシサーバー 		SSLポリシー名		example 🗸				
 SSL証明書署名要求作成 SSLインポート 	_	PKCS12形式	ファイルの	■択 ファイルが選	択されていません			
▶ SSLエクスポート	-	秘密鍵	ファイルのネ	■択 ファイルが選	択されていません			
▶ 疑、証明書の削除 証明書自動更新	*	パスフレーズ						
バランシング	*	サーバー証明書	ファイルの3	護択 ファイルが選	択されていません			
ヘルスチェック	×	中間証明書	ファイルの選択 ファ-	 イルが選択されてい:	ません ○上書き	◎ 階層化		
システム	*		ファイルの選択 ia1.pe	m	○上書き	◎ 階層化		

ウンロードしたルート証明書ファイルを選択しアップロード

入力後、[ファイルをインポートする]ボタンをクリックすると、SSL ポリシーに紐づく

ルート証明書がインポートされます。

ルート証明書がインポートされると、[SSL インポート]画面の[CA 証明書]欄に[valid]と

表示されます。

SSL	インオ	ペート			
<mark>}•</mark> 鍵、	証明書	身情報			
ポリシ	シー名	サーバー証明書	中間証明書	CA証明書	秘密鍵
exar	mple	valid		valid	2048

2.3. 失効リスト (CRL) の登録

クライアント証明書によるSSL認証を利用するためには、失効リストの登録が必要です。 これは、クライアントから提示される証明書が失効されていないことを検証する際に利 用するためです。

NetWiserのWeb管理画面にログインし、[設定]タブを選択、メニュー [SSL] の [証明書 失効リスト] をクリックします。

[証明書失効リスト]画面で以下を入力し、サーバ証明書をインポートします。

- [SSLポリシー名] に2.1章で作成したSSLポリシーを選択
- [証明書失効リストダウンロードURL] に、Gléas のCRLダウンロードURLを入力。
 ※Gléasのデフォルト発行局の失効リスト (DER形式) のダウンロードURLは以下となります

http://[GléasのFQDN]/crl/ia1.crl

● [更新間隔]に失効リストを自動更新する間隔を入力

		SEIKO
netwije	設定 機器情報 リアルタイム情報 統計情報 ログ参照	
ホスト名 : ユーザー名: 権限 :Admin権限	設定変更後保存されていません。保存する場合は右のボタンより、保存してください。 保存する	
設定	証明書失効リスト	
ネットワーク	※ ■ 証明書失効リスト 🕑	
冗長構成	※ 剤除 SSLポリシー 証明書失効リストダウンロードURL 更新間隔	
SSL ► SSL証明書 証明書未効リスト ► プロキシサーバー ► SSL証明書名を取作成 ► SSLTグパート ► SSLエクスパート ► は証明書の削除 証明書を更新	 ▼ (axample ▼) http://demo2.jcch-sss.com/cr/ia1.cr/ 0 ▼ 川向 ♥ 川向	
バランシング	*	
ヘルスチェック	×	
システム	*	

入力後、[設定内容を変更する]ボタンをクリックすると、SSL ポリシーに紐づく失効リ

ストがインポートされます。

※この設定により、[更新間隔]で指定した間隔で[証明書失効リストダウンロードURL]から失効リ ストを自動取得されます。 ※失効リストの登録を行わない場合、クライアント証明書認証時に証明書の失効確認が行われな くなります。

登録されている失効リストは以下の方法で確認できます。

NetWiserのWeb管理画面にログインし、[設定]タブを選択、メニュー [SSL] の [SSLエ

クスポート]をクリックします。

		SEIKO
設定機器情報	リアルタイム情報 統計情報 ロ・	グ参照
設定変更後保存されていません。保存する場合は右のボタ	ンより、保存してください。 保存する	
SSLエクスポート	+/- 表示状態	を反映
- ファイル選択 😮		
右クリックから保存してください.		
SSLポリシー名 秘密鍵 証明書 中間証明書 CA局証明 example <u>key</u> <u>Cett</u>	著(クライアント祝田) (CSK(単名表状) (CAL(失効リ .client CSY CI	ZF) PKC512801 pkc512
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>		設定 機器情報 リアルタイム情報 純好情報 ロ 設定変更像保存されていません。保存する場合は右のボタンより、保存してください。 保存する SSLTクスポート ・/・支索状態 > SSLTクスポート ・/・支索状態 コフイル版件 ・ オクリックから保存してください。 SSLTクスポート ・/・支索状態 マンタカから保存してください。 SSLTクスポート SSLTクスポート ・/・支索状態 マンタカから保存してください。 SSLポリシー名 SSLポリシー名 総合語 単晶証明書 SSLポリシー名 総合語 SE マロックから保存してください。 SSLポリシー名 SSLポリシー名 SSLポリシー名 総合語 は時期 中間証明書 CAB証明書(クライアント総証) CSR(第名要求) マロック MAR SE SE SE マロック MAR SE SE SE

[SSL エクスポート]画面で SSL ポリシー名に対応する[crl]ボタンをクリックすると、登

録されている失効リストがダウンロードされます。

2.4. 実サーバーの登録

ロードバランス先のWebサーバの情報をNetWiserに登録します。

まず、WebサーバのIPアドレスに名前を付与します。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [システム] > [ネットワーク]

の [IPアドレス名の定義] をクリックします。

[IPアドレス名の定義]画面で以下を入力します。

- [IPアドレス名]には、任意の名前を入力
- [IPアドレス名]には、WebサーバのIPアドレスを入力
- 複数のIPアドレスを登録する際は、[行追加]ボタンをクリックして入力

登定 更後保存されていません。保存 ドレス名の定義 アドレス名設定 ④ 峰 IPアドレス名 [real-server-1	機器情報 リアルタイム情報 する場合は右のボタンより、保存してくだ IPアドレス	統計情報 ロク参照 さい。 保存する 1/- 表示状態を反映	
 要後保存されていません。保存 ドレス名の定義 アドレス名設定 ② <u>IPアドレス名</u> <u>Ireal-server-1</u> 	する場合は右のボタンより、保存してくだけ する場合は右のボタンより、保存してくだけ リアドレス	さい。 保存する 4/- 表示状態を反映	l
ドレス名の定義 アドレス名設定 ? 降 IPアドレス名 real-server-1	IPアドレス	+/- 表示状態を反映	
アドレス名設定 ? 除 IPアドレス名 real-server-1	IPアドレス		-
除 IPアドレス名 real-server-1	IPアドレス		
real-server-1			
	1000 000 000 000		
real-server-2			
内容を変更する			
	2 内容を変更する	内容を変更する	内容を変更する

入力後、[設定内容を変更する]ボタンをクリックするとIPアドレスに名前が付与されま

す。

次に、WebサーバのListenアドレス、ポートを登録します。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [バランシング] > [実サーバー]

の [実サーバー設定] をクリックします。

[実サーバー設定]画面で以下を入力しします。

- [実サーバーIP]に、先に定義したWebサーバのIPアドレスの名前を入力
- [ポート]には、Webサーバの待ち受けポート番号を入力
- [プロトコル]は、[tcp]を選択
- [有効]をチェック
- 他の項目は、環境に応じて設定
- 複数のWebサーバを登録する際は、[行追加]ボタンをクリックして入力

	設定 機器情報 連後保存されていません。保存する場合は右の	リアルタイム情報 Dボタンより、保存してくださ	統計情報 い。 保存する	ログ参照	
ホスト名 : ユーザー名 : 権限 : Admin権限	要後保存されていません。保存する場合は右の	Dボタンより、保存してくださ	い。 保存する		
20.00 定 世					
EXAC XV	ーバー設定		-+/-	表示状態を反映	
ネットワーク × = 実	サーバー設定 🕗				_
冗長構成 ※ ■消	I除 実サーバーIP	ポート	プロトコル	最大コネクション	有効
SSL ×	real-server-1	80	®tcp ⊖udp	0	☑ 有効
バランシング ×	real-server-2	80	®tcp ○udp	0	☑ 有効
実サーバー ※ テサーバー設定 ト sorryコンデンツインポート					
NATプール ×	内容を変更する				
仮想サーバー ※	FIE CX2.9 0				
SSLアクセラレーション ×					
ホットワーク ◇ ヘルスチェック ×					
2274 ×					

入力後、[設定内容を変更する]ボタンをクリックすると実サーバーが登録されます。

続いて、登録した実サーバーを監視する設定を行います。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [ヘルスチェック] の [ヘルス

チェック設定]をクリックします。

[ヘルスチェック選択]画面で[新規]ボタンをクリックします。

[ヘルスチェック設定]画面で以下を入力しします。

- [ヘルスチェック方法]に、[L4-7ヘルスチェック]を選択
- [ヘルスチェック名]には、任意の名前を入力
- [有効]をチェック
- 他の項目は、監視方法に応じて設定
- 複数の実サーバーを監視する際は、[行追加]ボタンをクリックして入力

		SEIKO
netwoel	設定 機器情報 リアルタイム情報 統計情報 ログ参照	
ホスト名 : ユーザー名: 権限 : Admin権限	設定変更後保存されていません。保存する場合は右のパタンより、保存してください。 保存する	
設定	ヘルスチェック設定 +/- 表示状態を反映	
ネットワーク ×	🚍 ヘルスチェック対象サーバー 📀	
冗長構成 ※	ヘルスチェック方法 ○ pingヘルスチェック ⑧ L4-7ヘルスチェック	
SSL ×		
バランシング ×	ヘルスチェック名 ヘルスチェック対象サーバー L7プロトコル SSL 有効	
ヘルスチェック ×	Inc-real-server-1-nttp real-server-1.80.tcp V は 保険にする 単 有効にする 単 有効にする トレート	
 ヘルスチェック設定 ヘルスチェック一括設定 ヘルスチェック組み合わせ設定 ヘルスチェック知み合わせ設定 		
▶ ハレステエック 有加/無効	項目名 入力	
	送信間隔 5 秒 デフォルトに戻す	
	Down判定しきい他 2 回 デフォルトに戻す	
	手動期日 日 有効にする	
	設定内容を変更する	
	MCHBCXC/V	

入力後、[設定内容を変更する]ボタンをクリックするとヘルスチェックが開始されます。

- SEIKO NetwiJer 設定 機器情報 リアルタイム情報 統計情報 ログ参照 ホスト名 : ユーザー名 : 権限 : Admin権限 設定 設定変更後保存されていません。保存する場合は右のボタンより、保存してください。 保存する ヘルスチェック選択 +/- 表示状態を反映 ネットワーク → ハルスチェック選択 ②
 ■ 前除 へハレスチェック名 実サーバーIP ボート プロトコル 有効 × 冗長構成 × hc-real-server-1-http://real-server-1 80 tcp SSL × ~ バランシング × ヘルスチェック ※ ヘルスチェック設定 ・ヘルスチェック一括定 ・ヘルスチェック組み合け設定 ・ヘルスチェック相角合け設定 ・ヘルスチェック有効/無効 システム ※ * 新規 削除 × コピー
- [ヘルスチェック選択]画面に戻り、登録状況が確認できます。

2.5. NATプールの登録

NetWiserがWebサーバにアクセスする際の送信元となるソースNAT用IPアドレスを登

録します。

まず、ソースNAT用のIPアドレスに名前を付与します。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [システム] > [ネットワーク]

の [IPアドレス名の定義] をクリックします。

[IPアドレス名の定義]画面で以下を入力します。

- [IPアドレス名]には、任意の名前を入力
- [IPアドレス]には、ソースNAT用のIPアドレスを入力

設定 後習情報 時されていません。保存する場合は ス名の定義 1025に。2	リアルタイム情報 統計情 統計情	#留 ログ参照 #797る ↓/- 表示状態を反映	
辞されていません。保存する場合(ス名の定義 ノス名設定 2 1072 N L - スタ	は右のボタンより、保存してください。 🛛 🧕	¥存する +/- 表示状態を反映	
ス名の定義 ノス名設定 ?		+/- 表示状態を反映	
▶ ス名設定 🕜			
10751.72			
PT PD AG	IPアドレス		
real-server-1	10, 10, 10, 10, 10		
real-server-2	10.000.00.00		
vip-internal	10.4.1		
を変更する			
	real-server-2 vip-internal	real-server-2 vip-internal [を変更する	real-server-2 vip-internal を変更する

入力後、[設定内容を変更する]ボタンをクリックするとIPアドレスに名前が付与されま

す。

次に、NATプールをWebサーバのListenアドレス、ポートを登録します。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [バランシング] > [NATプール]

の [NATプール] をクリックします。

[NATプール選択]画面で[新規]ボタンをクリックします。

[NATプール設定]画面で以下を入力します。

- [NATプール名]には、任意の名前を入力
- [開始IPアドレス]には、先に定義したソースNAT用のIPアドレスの名前を入力

		SEIKO
netwijer	設定 機器情報 リアルタイム情報 統計情報 ログ参照	
ホスト名 : ユーザー名: 権限 : Admin権限	設定変更後保存されていません。保存する場合は右のボタンより、保存してください。 保存する	
設定	NATプール設定 +/- 表示状態を反映	
ネットワーク ×		
冗長構成 ×	NATプール名 src-nat	
SSL ×		
バランシング ×	- 100 100 100 100 100 100 100 100 100 10	
実サーバー ※ NATプール ※ NATプール ※ 仮想サーバー ※ SSLアクセラレーション ※ ネットワーク ※	vip-internal 行道版 設定内容を変更する	
ヘルスチェック ※		
システム ×		

入力後、[設定内容を変更する]ボタンをクリックするとNATプールが登録されます。

- SEIKO NetwiJer 設定 機器情報 リアルタイム情報 統計情報 ログ参照 ホスト名 : ユーザー名 : 権限 : Admin権限 設定 設定変更後保存されていません。保存する場合は右のボタンより、保存してください。 保存する NATプール選択 +/- 表示状態を反映 ネットワーク × 冗長構成 * SSL × バランシング × バランシング 実サーバー NATプール NATプール 仮想サーバー SSLアクセラレーション ネットワーク 新規 削除 * » » » ヘルスチェック × システム ×
- [NATプール選択]画面に戻り、登録状況が確認できます。

2.6. 仮想サーバーの登録

NetWiserが公開する仮想サーバーを登録します。

まず、公開する仮想サーバーのIPアドレスに名前を付与します。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [システム] > [ネットワーク]

の [IPアドレス名の定義] をクリックします。

[IPアドレス名の定義]画面で以下を入力します。

- [IPアドレス名]には、任意の名前を入力
- [IPアドレス名]には、仮想サーバーのIPアドレスを入力

	F				SEIKO
INGLINITE	:r	設定	機器情報 リアルタイム情報	統計情報 ログ参照	
ホスト名 : ユーザー名 : 権限 : Admin権限	設定	変更後保存されていません。	保存する場合は右のボタンより、保存してください。	保存する	
設定	IP:	アドレス名の定義		+/- 表示状態を反映	
ネットワーク	× = 1	Pアドレス名設定 🕗			_
冗長構成	*	削除 IPアドレス名	IPアドレス		
SSL	* (real-server-1	100,000,000,000		
バランシング	* (real-server-2	100,000,000,00		
ヘルスチェック	* (vip-internal	100.000.00.000		
システム	*	vip-external			
ネットワーク IPアドレス名の定義 ▶ SNMP設定 ▶ SvLOG設定 ▶ NATLOG設定 ▶ DNSサーパー ▶ NTササーパー	※ 行道 ▶ ●	主内容を変更する			
ユーザー管理	*				

入力後、[設定内容を変更する]ボタンをクリックするとIPアドレスに名前が付与されま

す。

次に、仮想サーバーを登録します。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [バランシング] > [仮想サーバ

-]の[仮想サーバー]をクリックします。

[仮想サーバー選択]画面で[新規]ボタンをクリックします。

[仮想サーバー	設定]画面で以	下を入力	します。
---------	---------	------	------

	項目名	値	
仮想サーバーID設定	仮想サーバー名	任意の名前	
	仮想サーバーIP	仮想サーバーのIPアドレスの名前	
	ポート	待ち受けポート(443)	
	プロトコル	[tcp]	
	有効にする	チェック	
仮想サーバー基本設定	分散アルゴリズム	[ラウンドロビン]	
	セッション維持方法	[IPアドレス]	
	セッションタイムアウト値	30分	
	ソースNATプール	2.5章で作成したNATプール	
	ヘッダー挿入機能(x-forwarded-for)	チェック	
	ヘッダー挿入機能(x-forwarded-proto)	チェック	
実サーバーバインド設定	実サーバーIP.ポート	2.4章で登録した実サーバー	
		※複数ある場合は[行追加]をクリックし	
		て登録	
	重み	1	



入力後、[設定内容を変更する]ボタンをクリックすると仮想サーバーが登録されます。

[仮想サーバー選択]画面に戻り、登録状況が確認できます。



2.7. SSLアクセラレーション設定

2.6章で登録した仮想サーバーに対し、

- サーバ証明書の適用
- 許可する暗号スイート
- クライアント証明書認証
- クライアント証明書情報のWebサーバへの送信

といった設定を行います。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [バランシング] > [SSLアクセ ラレーション] の [SSLアクセラレーション] をクリックします。

[SSLアクセラレーション選択]画面で2.6章で登録した仮想サーバーのリンクをクリック

	P	SEIKO
INGLINIDE	設定 機器情報 リアルタイム情報 統計情報 ログ参照	
ホスト名 : ユーザー名 : 権限 : Admin権限	設定変更後保存されていません。保存する場合は右のボタンより、保存してください。 保存する	
設定	SSLアクセラレーション選択 +/- 表示状態を反映	
ネットワーク 冗長機成 SSL	● 仮想サーバーID 遊択 ② ※ 仮想サーバーC名 仮想サーバーID Wittual-server Vio-external.443.tcp	
	- SSLセッションタイムアウト SSLセッションタイムアウト SSLセッションタイムアウト ・ 学 ・ SSL3.0有効/無効 ・ SSL3.0有効/ ・ SSL3.0 ・ SS	
5 7 74	ULMOKARVO	

して選択します。

[SSLアクセラレーション設定]画面で以下を入力します。

SSL証明書の割り当て

- [追加元] に 2.1 章で登録したサーバ証明書を選択
- [追加]ボタンをクリック ([追加先]に反映される)

SSL アクセラレーション詳細設定

- クライアント証明書の[ヘッダー] に、"X-CLIENT-CERT"と入力
- クライアント証明書の[形式] に、[Base64]を選択
 ※この設定により、実サーバーへの HTTP リクエストの HTTP-X-CLIENT-CERT ヘッダに
 Base64 形式のクライアント証明書が送信されるようになる
- SSL セッション ID ヘッダーの[ヘッダー]に"X-SSL-SESSION-ID"と入力

※この設定により、実サーバーへの HTTP リクエストの HTTP-X-SSL-SESSION-ID ヘッダに NetWiser の SSL セッションを識別する文字列が送信されるようになる

● クライアント認証失敗時処理の[動作]に[403 レスポンス返送]を選択

※この設定により、クライアント証明書認証が失敗した場合に NetWiser はステータスコード 403 を応答するようになる

					SEIKO
netwijer	設定	機器情報 リアルタイム	▲情報 統計情報 ログ参	照	
ホスト名 : ユーザー名 : 権限 : Admin権限	設定変更後保存されていません	v。保存する場合は右のボタンより、保存!	してください。 保存する		
設定	SSLアクセラレーション	/設定	+/- 表示状態を反	E PP	
ネットワーク ×	SSL証明書の割り当て(
冗長構成 ※	追加元	追加	0先		
SSL ×	証明書名▼	ht example (default)	A		
バランシング ※					
実サーバー ※			~		
NATプール ×		削除 デフ	オルト証明書にセットする		
仮想サーバー × SSI アクセラレーション ×	SSI アクセラレーション	洋細設定 💿			
SSLアクセラレーション・	項目名	PTINISXAL 😈	እታ	到除	
ネットワーク ※	- And	DES-CBC-SHA	DES-CBC3-SHA		
ヘルスチェック ×		AES128-SHA	AES128-SHA256		
システム ※		AES256-SHA	AES256-SHA256		
		AES128-GCM-SHA256	AES256-GCM-SHA384		
		DHE-AES128-GCM-SHA256	DHE-AES128-SHA236		
	11 10 1870-T-T-T	DHE-AES256-SHA256	DHE-AES256-GCM-SHA384		
	サーバーか計可する 暗号スイート	ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA256		
	■ 全選択/解除	ECDHE-RSA-AES128-GCM- SHA256	ECDHE-RSA-AES256-SHA		
		ECDHE-RSA-AES256-SHA384	C ECDHE-RSA-AES256-GCM-		
		C ECDHE-ECDSA-AES128-SHA	ECDHE-ECDSA-AES128-SHA250 ECDHE-ECDSA-AES256-SHA		
		SHA256			
		ECDHE-ECDSA-AES256-SHA384	L ECDHE-ECDSA-AES256-GCM- SHA384		
	クライアント ヘッダー	X-CLIENT-	CERT		
	証明書 形式	Base	64 O PEM		
	SSLセッションIDヘッダー	X-SSL-SES	SSION-ID		
	クライアント認証 動作	403レスポンス返送	デフォルトに戻す		
	失敗時処理 URL				
	設定内容を変更する				

入力後、[設定内容を変更する]ボタンをクリックすると仮想サーバーにSSLアクセラレー

ション設定が反映されます。

すべての設定変更が終わったら、[保存する]をクリックして、NetWiserに設定を保存し

ます。

保存する 設定変更後保存されていません。保存する場合は右のボタンより、保存してください。

3. Gléas の管理者設定 (Windows 向け)

GléasのUA (申込局) より発行済み証明書をPCにインポートできるよう設定します。

※下記設定は、Gléas納品時等に弊社で設定を既に行っている場合があります

GléasのRA (登録局) にログインします。

画面上部より[認証局]をクリックし認証局一覧画面に移動し、設定を行うUA (申込局)

をクリックします。

※実際はデフォルト申込局ではなく、その他の申込局の設定を編集します

▶<u>Gleas Generic UA</u> Gleas デフォルト申込局

申込局詳細画面が開くので、基本設定で以下の設定を行います。

● [証明書ストアへのインポート]をチェック

UA 申込局

- 証明書ストアの選択で、[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]

にチェック

▶基本設定	
 トーケンへのインボート ご即明書ストアへのインボート ダウンロードを許可 ダウンロード可能時間(分) 1 CA証明書を含めない 	 管理するトークン Gemalto.NETカード▼ 証明書ストアの種類 ユーザストア ▼ インボートワンスを利用する 登録申請を行わない 登録は著を行わない 登録済みデバイスのみインボート許可

設定完了後、[保存]をクリックし保存します。

また、認証デバイス設定の以下項目にチェックがないことを確認します。

- iPhone/iPad の設定の、[iPhone / iPad 用 UA を利用する]
- Android の設定の、[Android 用 UA を利用する]

以上でGléasの設定は終了です。

4. クライアントの設定 (Windows)

4.1. クライアント証明書のインポート

PC のブラウザ (Edge) で、UA にアクセスします。

※URL https://[UA の FQDN]/[UA の名前]/ua

ログイン画面が表示されるので、ユーザ ID とパスワードを入力しログインします。

O エンドユーザロ	コグイン [UA]
UA D	ーザID、バスワードを入力してロ インしてください。
トユーザID	
▶バスワード	
	ログイン

ログインすると、ユーザ専用ページが表示されます。

[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行

				JEAN-PCA Gleas
スト ユーザー さんのページ	1			ロログアロ
ーザ情報				
🙎 テスト ユーザー さんのべ-	ージ			
🖢 ユーザ情報				
▶ユーザ	登録日時: 2024/01/26 10:56			
>蛙:テスト 名:ユーザー > ユーザID: > メールアドレス: > バスワード:*********				
★ 証明書情報 ······				
201170-0281-0194				
#	発行局	シリアル	有効期限	証明書ストアヘインボート
# <u>\$1</u>	発行局 JCCH-SSS demo2 CA	シリアル	有约期限	証明書ストアヘインボート 証明書のインボート
# <u><u><u><u><u></u></u><u><u><u></u><u></u><u></u><u></u><u></u><u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u></u></u></u></u></u>	発行局 JCCH-SSS demo2 CA	シリアル	有効期限	証明書ストアヘインボート 証明書のインボート
デスロルウムであ # 発 <u>1</u>	発行局 JCCH-SSS demo2 CA	SUTH	有効期限	証明書ストアヘインボート 証明書のインボート
R1	発行局 JCCH-SSS demo2 CA	5407%	有効期限	証明者ストアヘインボート 証明者のインボート
R1	発行局 JCCH-SSS demo2 CA	5497%	有功用影	127月者ストアヘインボート 127月者のインボート
	発行局 JCCH-SSS demo2 CA	349774	有力加强要	129月者ストアヘインボート 129月者のインボート
R 20192498	我行局 JCCH-SSS demo2 CA	340774r	有功加强	1291者ストアヘインボート 129月者のインボート

われます。

※証明書インポート時にルート証明書のインポート警告が出現する場合は、システム管理者に拇印を 確認するなど正当性を確認してから[はい]をクリックします

セキュリティ	(普告	\times
	発行者が次であると主張する証明機関 (CA) から証明書をインストールしよ うとしています:	
	JCCH-SSS demo2 CA	
	証明書が実際に "JCCH-SSS demo2 CA" からのものであるかどうかを検証 できません。"JCCH-SSS demo2 CA" に連絡して発行者を確認する必要が あります。次の省号はこの過程で役立ちます:	
	拇印 (sha1):	
	警告: このルート証明書をインストールすると、この CA によって発行された証明書は 自動的に信頼されます。確認されていない拇印付きの証明書をインストール することは、セキュリティ上、危険です。[はい]をクリックすると、この危険を認 識したことになります。	
	この証明書をインストールしますか?	
	はい(Y) しいえ(N)	

インポートワンス機能を有効にしている場合は、インポート完了後に強制的にログアウ

トさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度ロ

グインしてインポートを行うことはできません。

	21			
> m m 〉 テスト ユーザー さんの f	ページ	_		
2				
ユー ジ 1月 ¥0	登録日時: 2024/01/26 10:56			
- ・ 姓: テスト 名:ユーザー				
ユーザID :				
>×=/v/rv/:				
・バスワード:************************************				
·メールアドレス: ・パスワード: ************************************				
·×ール/ドレス: ・バスワード: ************************************				
>>=ル/トレス: >パスワード: ************************************	我行局	うりょう	有分析現象	証明書ストアヘインボート
シンテルアレス: いスワード: ************************************	発行為 JCCH-SSS demo2 CA	ジリアル #757	有幼期家務 2025/05/16	証明書ストアヘインボート ダウンロード済み
シンテルアトレス: 	浅(155) JCCH-SSS demo2 CA	ジリアル #757	有均用原因 2025/05/16	記録なトアヘインボート ダウンロード済み
ッテル/アレス: いスワード: 証明書情報 変 方法の正明念 変 変 1 変 1	現行局 JCCH-SSS demo2 CA	54Jアル #757	제10,8928 2025/05/16	証明度ストアヘインボート ダウンロード流み
メマール/ドレス: いなフロード: 証明書情報 発行済み証明書 考1	死行局 JCCH-SSS demo2 CA	२८४७२७४- #757	북:10,1928 2025/05/16	証明書ストアヘクポート ダウンロード済み
ッペンクード: 証明書情報 ・ 変行流み互明書 変1	発行為 JCCH-SSS demo2 CA	ジノアル #757	者)20月5日 2025/05/16	証明書ストアヘクポート ダウンロード済み
メテルアレス: 13(ス)-F: 13(α)-F: 13(α)	発行局 JCCH-SSS demo2 CA	ジリアル #757	者12,85 <u>8</u> 2025/05/16	証明書ストアヘインボート ダウンロード済み
メテルアレン: 13(スクード: 13(スクード: 第7) 第7) 第7) 第7) 第7) 第7) 第7) 第7)	我行局 JCCH-SSS demo2 CA	メリアル #757	者的期度 2025/05/16	証明書ストアヘインボート ダウンロード済み
>>ール/TUX:):12ワード: 証明書情報 : 変1済み証明念 - 変1	預約局 JCCH-SSS demo2 CA	ジリアル #757	油 \$25495 <u>8</u> 2025/05/16	証明書ストアヘインボート ダウンロード済み

4.2. Webサーバアクセス

PCのブラウザ (Edge) でNetWiserの仮想サーバーのURLにアクセスすると、クライア

ント証明書の提示を求められます。

認証用の証明書の選択		\times
ታイト	では資格情報が必要です:	
Ē	CA	
証明書情報	ОК	キャンセル

[OK]ボタンをクリックし、クライアント証明書認証がおこなわれるとページが表示さ

れます。

※以下は7項の CGI を実行する Web ページにアクセスしている例

W	/elcome Server
	<pre>/elcome Server rp_ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 rp_ACCEPT_LANGUAGE = ja rp_ACCEPT_LANGUAGE = ja rp_ACCEPT_LANGUAGE = ja rp_CONNECTION = keep-alive IP_HOST = example.jcch-sss.com rP_SEC_CH_UA = "chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99" rp_SEC_CH_UA = "chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99" rp_SEC_CH_UA = "chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99" rp_SEC_CH_UA = To rp_SEC_CH_UA = To rp_SEC_FETCH_DEST = document rp_SEC_FETCH_DEST = document rp_SEC_FETCH_USER = 71 rp_UPGRADE_INSECURE_REQUESTS = 1 rp_UPGRADE_INSECURE_REQUESTS = 1 rp_USER_AGENT = Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0 rp_X_CLIENT_CERT = EP2CCAyegAwIBAgICAvQwDQYJKoZIhvcNAQELBQAwfjEaMBgGA1UEAxMRSkNDSC1TU1MgZGVtbzIgQ0ExGDAWBgoJkiaJk/IsZAEZFghqY2NoLXNzczETMBEGCgmSJomT8ix suer: enalNo: ubject CN: rp_X_FORWARDED_FOR = rp_X_FORWARDED_FOR = rp_X_FORWARDED_FOR = https v_CSL_GEST(AD_LD = vID_RDMWTZYGETbr/d002Na58iPIIPOSUACCAYE/ADA= </pre>

証明書を持っていない場合や、失効された証明書を提示した場合はアクセスに失敗しま

す。

※以下は失効されたクライアント証明書でアクセスした例

403 Forbidden

5. Gléas の管理者設定 (iPhone 向け)

Gléas で、発行済みのクライアント証明書を iOS にインポートするための設定を本書で

は記載します。

※下記設定は、Gléas 納品時等に弊社で設定を既に行っている場合があります

GléasのRA (登録局) にログインします。

画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUA (申込局)

をクリックします。

※実際はデフォルト申込局ではなく、その他の申込局の設定を編集します

UA 申込局 ▶<u>Gleas Generic UA</u> Gleas デフォルト申込局

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [ダウンロードを許可]をチェック
- 「ダウンロード可能時間(分)]の設定・[インポートワンスを利用する]にチェック

この設定を行うと、GléasのUAからインポートから指定した時間(分)を経過した 後は、構成プロファイルのダウンロードが不可能になります(インポートロック機 能)。これにより複数台のデバイスへの構成プロファイルのインストールを制限す

ることができます。

▶基本設定	▶上級者向け
 トークンへのインボート 証明書ストアへのインボート ダウンロードを許可 ダウンロード可能時間(分) CA証明書を含めない 	 管理するトークン Gemaito.NETカード × 証明書ストアの種類 ユーザストア × インポートワンスを利用する 登録申請を行わない 登録済みデバイスのみインボート許可

設定完了後、[保存]をクリックし保存します。

[認証デバイス情報]の[iPhone/iPadの設定]までスクロールし、[iPhone/iPad用UAを利

用する]をチェックします。

🖋 認証デバイス情報		
▶ iPhone / iPadの設定		
🗌 iPhone/iPad 用 UA を利用する		
	保存	

構成プロファイルに必要となる情報の入力画面が展開されるので、以下設定を行います。

【画面レイアウト】

- [iPhone用レイアウトを利用する]をチェック
- [ログインパスワードで証明書を保護]をチェック

【iPhone構成プロファイル基本設定】

● [名前]、[識別子]に任意の文字を入力 (必須項目)

🦸 認証デバイス情報		
▶iPhone / iPadの設定		
🔽 iPhone/iPad 用 UA を利	用する	
画面レイアウト		
☑ iPhone 用レイアウトを使 ○ Mac OS X 10.7以降の指	用する 銃を許可	✓ ログインパスワードで証明書を保護
OTA(Over-the-air)		
OTAエンロールメントを利	川用する	 接続する iOS デバイスを認証する
OTA用SCEP URL		
OTA用認証局	デフォルトを利用	×
iPhone 構成プロファイル表	本設定	
名前(デバイス上に表示)	サンプルプロファイル	
識別子(例: com.jcch- sss.profile)	local.jcch-sss.profile	
プロファイルの組織名	JCCHセキュリティ・ソリュー	ション・システムズ
i兑 ¹ 月	サンプル構成プロファイル	

各項目の入力が終わったら、 [保存]をクリックします。

以上でGléasの設定は終了です。

6. クライアントの設定 (iPhone)

6.1. クライアント証明書のインポート

iPhoneのブラウザ (Safari) で、UAにアクセスします。

※URL https://[UA の FQDN]/[UA の名前]/ua

ログイン画面が表示されるので、ユーザ ID とパスワードを入力しログインします。



ログインすると、ユーザ専用ページが表示されます。

[ダウンロード]をタップし、構成プロファイルのダウンロードをおこないます。



※ インポートロックを有効にしている場合は、この時点からカウントが開始されます

画面の表示にしたがい設定を開くと、プロファイルがダウンロードされた旨が表示され

るので、インストールをおこないます。

設定		キャンセル	プロファイル	インストール
Apple ID、iCloud、メディアと購入	>	لا ب المحمد المحمد	プルプロファイル セキュリティ・ソリュー: ムズ	vav•
プロファイルがダウンロード済み	>	Signed by No Description サン Contains 証明	t Signed >プル構成プロファイル 問書: 2	
		More Detail	s	>
		Remo	ove Downloaded I	Profile

[インストール]をタップして続行してください。

インストール中にルート証明書のインストール確認画面が現れるので、内容を確認し

[インストール]をタップして続行してください。

※ここでインストールされるルート証明書は、通常のケースではGléasのルート認証局証明書になります



インストール完了画面になりますので、[完了]をタップして終了します。

	インストール完了	完了
	サンプルプロファイル ICCHセキュリティ・ソリューション・ _{レステムズ}	
Signed by	Not Signed	
Description	サンプル構成プロファイル	
Contains	証明書: 2	

なお [More Details]をタップすると、インストールされた証明書情報を見ることがで

きます。必要に応じて確認してください。

く 戻る	サンプルプロファイル	
証明書	(2)	
Ø		>
Ø	発行元: 有効期限:	>

Safariに戻り、[ログアウト]をタップしてUAからログアウトします。

以上で、iPhoneでの構成プロファイルのインストールは終了です。

なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より 管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロ ード済み」という表記に変わり、以後のダウンロードは一切不可となります。

プライヘ	K-FCA Gléäs 🛯
テスト ユーザー さ	んのページ
ユーザID	
姓	テスト
名	ユーザー
メール	
有効期限	ダウンロード済み
有効期限	ダウンロード済み
	ログアウト

6.2. Webサーバアクセス

iPhoneのブラウザ (Safari) でNetWiserの仮想サーバーのURLにアクセスすると、構成

プロファイルにあるクライアント証明書が自動的に提示されます。

クライアント証明書認証がおこなわれるとページが表示されます。

※以下は7項の CGI を実行する Web ページにアクセスしている例

Welcome Server
wereome berver
HTTP_ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
<pre>HTTP_ACCEPT_ENCODING = gzip, deflate, br</pre>
TTTP_ACCEPT_LANGUAGE = ja
ITTP_CONNECTION = keep-alive
ATTP_HOST = example.jcch-sss.com
TTTP_USER_AGENT = Mozilla/5.0 (iPhone; CPU iPhone OS 16_3 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.3 Mobile/15E148 Safari/604.1
fitp_x_client_cert =
MILEPZCCAyegAWIBAGICAVUWDQYJKoZINVCNAQELBQAWIJEAMBgGATUEAXMRSK
Issuer:
Senaino:
SUDJECT CN.
HTTP_X_FORWARDED_POK =
TTTP_X_SSL_SESSION_ID = 0351Wen3401vvemveBe4YbnJaedtbSU4AGdAInKAgA=
1111_A_55E_5E551014_1D = 0555 w cp54014 valitxqBs4A0pigeall050AA6uAliteAgA=

証明書を持っていない場合や、失効された証明書を提示した場合はアクセスに失敗しま

す。

※以下はクライアント証明書を持っていない状態でアクセスした例

このWebには証明書が必要です 必要な証明書がインストールされてい ません。
了解

7. Web サーバでクライアント証明書情報を取得

NetWiser によってHTTPリクエストヘッダに挿入されたクライアント証明書情報を

Webサーバが受信していることを確認します。

※以下は、Python で作成した CGI を Apache で公開する例

http.conf に以下を追加

ScriptAlias /cgi-bin/ "/var/www/cgi-bin/" <Directory "/var/www/cgi-bin"> AllowOverride None Options +ExecCGI Require all granted AddHandler cgi-script .py </Directory>

● Apache を再起動 systemctl restart httpd ● CGI を作成

vi /var/www/cgi-bin/test.py

スクリプトの内容は以下。

```
#!/usr/bin/env python
import os
import base64
import OpenSSL
print("Content-Type: text/html")
print("Cache-Control: no-cache")
print("")
print("<html><body>")
print("<h1>Welcome Server</h1>")
for headername, headervalue in sorted(os.environ.items()):
  if headername.startswith("HTTP_"):
    print("{0} = {1}<br>".format(headername, headervalue))
  if headername.startswith("HTTP_X_CLIENT_CERT"):
    der = base64. b64decode (headervalue)
    cert = OpenSSL.crypto.load_certificate(OpenSSL.crypto.FILETYPE_ASN1, der)
    print("  {0}: {1}<br>".format("Issuer", cert.get_issuer().commonName))
print("&emsp; {0}: {1}<br>".format("SerialNo", cert.get_serial_number()))
    print("  {0}: {1}<br>".format("Subject CN", cert.get_subject().commonName))
print("</html></body>")
```

ファイルパーミッションを設定

chmod 755 /var/www/cgi-bin/test.py

Web ブラウザから CGI にアクセスすると、環境変数 HTTP_X_CLIENT_CERT に

Base64 エンコードされたクライアント証明書が取得できていることが確認できます。

※以下はPCからEdgeブラウザでアクセスした場合の例

Welcome Server
HTTP_ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 HTTP_ACCEPT_ENCODING = gzip, deflate, br, zstd HTTP_ACCEPT_LANGUAGE = ja HTTP_CONNECTION = keep-alive HTTP_HOST = example.jcch-sss.com HTTP_SEC_CH_UA = "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99" HTTP_SEC_CH_UA = "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99" HTTP_SEC_CH_UA_MOBILE = ?0 HTTP_SEC_CH_UA_PLATFORM = "Windows" HTTP_SEC_CH_UA_EST = document HTTP_SEC_FETCH_DEST = document
HTTP_SEC_FETCH_STLE = NOTE HTTP_UPGRADE_INSECURE_REQUESTS = 1 HTTP_UPGRADE_INSECURE_REQUESTS = 1
HITP_USER_AGENT = MOZIIII/S.O. (WINDOWS NT 10.0; WINDOW; XX4) AppleWeDKI(7537.36 (KHTML, IIKE GECK6) Chrome/124.0.0.0 Safan/537.36 Edg/124.0.0.0 HTTP_X_CLENT_CERT = MIIEP2CCAyegAWIBAgICAvQwDQYJKoZIhvcNAQELBQAwfjEaMBgGA1UEAxMRSkNDSC1TU1MgZGVtbzIgQ0ExGDAWBgoJkiaJk/IsZAEZFghqY2NoLXNzczETMBEGCgmSJomT8i: Issuer: SerialNo: Subject CN:
HTTP_X_FORWARDED_FOR = HTTP_X_FORWARDED_PROTO = https HTTP_X_SSL_SESSION_ID = erLRLPHMw7YY96Tlod99SNq58iRIRQ5UAAGcAK8/AQA=

8. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■Gléasや本検証内容、テスト用証明書の提供に関するお問い合わせ

株式会社JCCH・セキュリティ・ソリューション・システムズ

Tel: 050-3821-2195

Mail: sales@jcch-sss.com