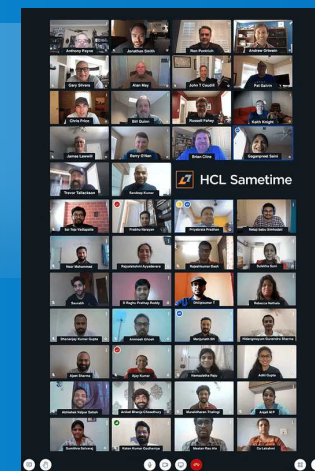


HCL Sametime V11.6 Premium インストール

ノーツコンソーシアム パブリックビューイング

2021年10月28日

株式会社 エイチシーエル・ジャパン
HCL ソフトウェア



HCL Sametime 11.6

- 一言で言えば、チャットとミーティングを提供するサーバー
 - オープン、低コスト、利便性（ブラウザーだけで利用可能）、セキュリティー
- オンプレソリューション？
 - いいえ、IaaSソリューション。インハウスでもクラウドでもデプロイ可能
- 登場人物
 - Community サーバー: チャット機能でDominoのタスクとして動作。VPプロトコル（1533）
 - Proxy サーバー: ブラウザーやモバイルアプリ用変換サーバー（HTTP/443）
 - Meeting サーバー: Dockerで提供。画面共有、音声/ビデオ、録画機能のセット。
 - MongoDB: チャット履歴保管とミーティング情報保管
- 9.0.1時代との比較
 - 登場人物の数とサーバーの数の減少
 - 起動、再起動の複雑さ、インストール手間、トラブル時、バージョンアップ時の手間の大幅減少
 - WebSphereからの解放
 - ブラウザープラグインがなくなった（トラブルの温床）
 - 複雑なクラスター構成の設計と運用からの解放
 - V12では CommunityサーバーとProxyサーバーもDocker対応



HCL Sametime による解決のご提案

HCL Sametime は、自社ホスティング型 (IaaSや自社環境)のチャットとミーティング製品です。

課題 1 : セキュリティー

- SaaSのデータプライバシー問題
- 事件・事故による情報漏洩のリスク
- ログを取得不可による監査問題



解決 1: 自社で管理

- IaaSや自社にデプロイ
- データは自社で保有、管理
- 堅牢なプライバシー・暗号化機能
- ログ監査

課題 2 : コスト

- 高コストで全員配布不可
 - 複雑な課金体系による最適化とコスト管理が困難
- ほとんど使わない機能
- インターネット回線増強



解決 2: コストの最適化

- 1ユーザー1ライセンスで制限なし
- 安価なライセンスで全員配布
- インターネット回線増強なしにイントラネットのみでも実現

課題 3 : 利便性

- 誰でもいつでも使えない
 - 契約不足
 - 個人会議室が持てない
- プラグインのインストールや起動操作・時間で手間取る



解決 3: 常時即座に利用可能

- 全員利用可能、無制限の会議室数
- 個人の会議室
- ブラウザのみでプラグイン不要
- URLを開くだけで即座に開始

はじめに

- 2台のサーバーを使った最小構成でインストールをAWS上で行います。
 - Windows: Domino サーバー + Sametime Community サーバー + Sametime Proxy サーバー + MongoDB
 - ノーツコンソーシアムで利用中のDomino環境への追加 Domino サーバーとしてインストール（現在利用中の認証がそのまま使えます）
 - Linux: Sametime Meetings サーバー
- 今回の撮影は一発撮りで、入れ直しや撮り直しはありません。カットなしの「そのままのインストール作業」です。
 - 若干のドタバタや失敗がありますがご容赦ください。
 - 管理者ユーザーのパスワードを失念して、途中でパスワード探しが発生
 - 設定ファイルの記入位置の間違って動作不良
 - 早回しの編集を行っています。要所要所はスピードを落としています。
- 所要時間
 - Windows側: 約1.5時間
 - Linux側: 約1時間
 - 証明書: 0.5時間
- その他
 - 証明書はLet's Encryptを使用、認証ディレクトリーはDominoディレクトリーサーバーを使用（LDAP不使用）

1.1. 全体概要図

【凡例】
サーバ、クライアント通信アドレスポート

物理アドレス
リバプロ物理アドレス

社外ユーザー (ブラウザ / iOSアプリ)

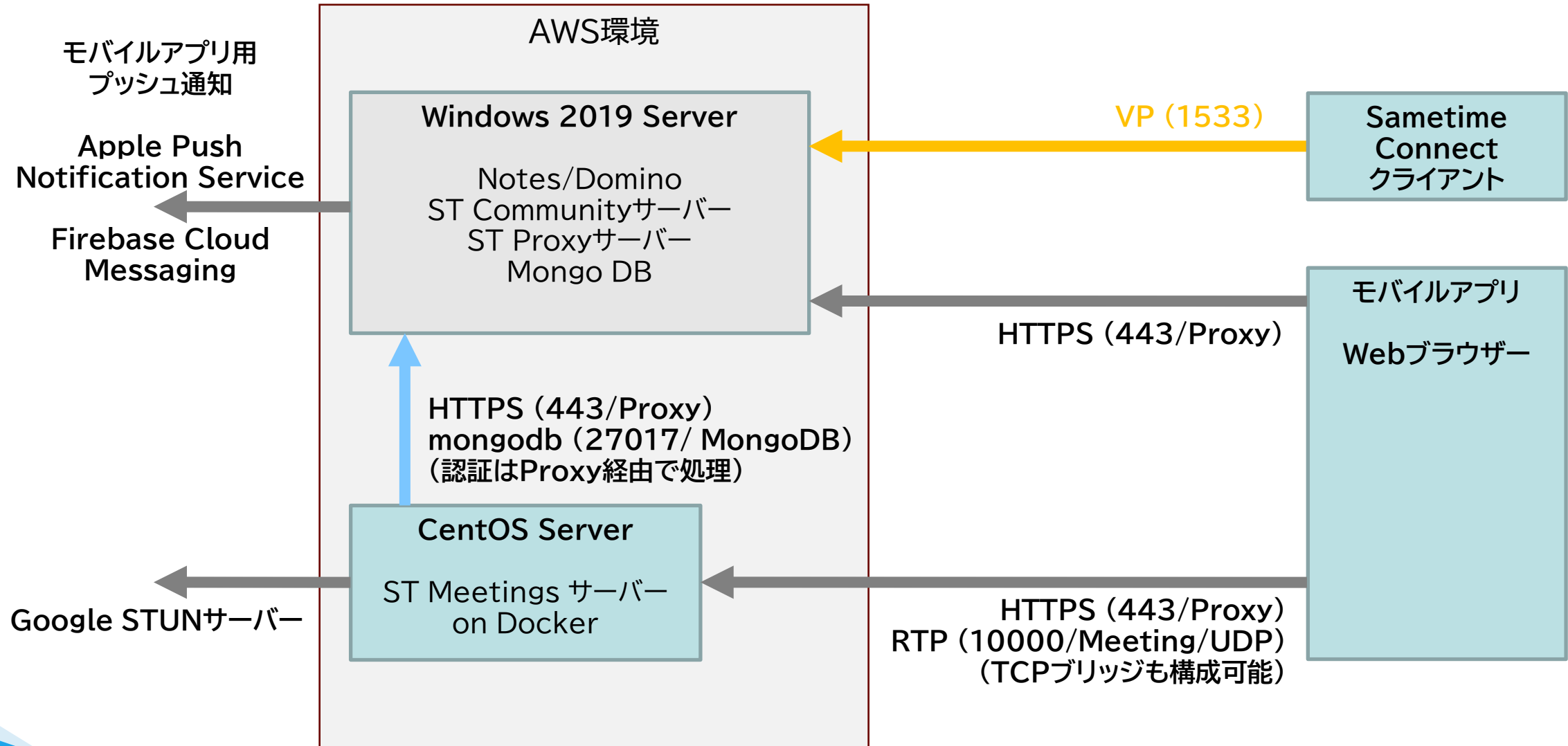
社内ユーザー (Notesプラグイン)

tdkldap3.tdkgrp.net

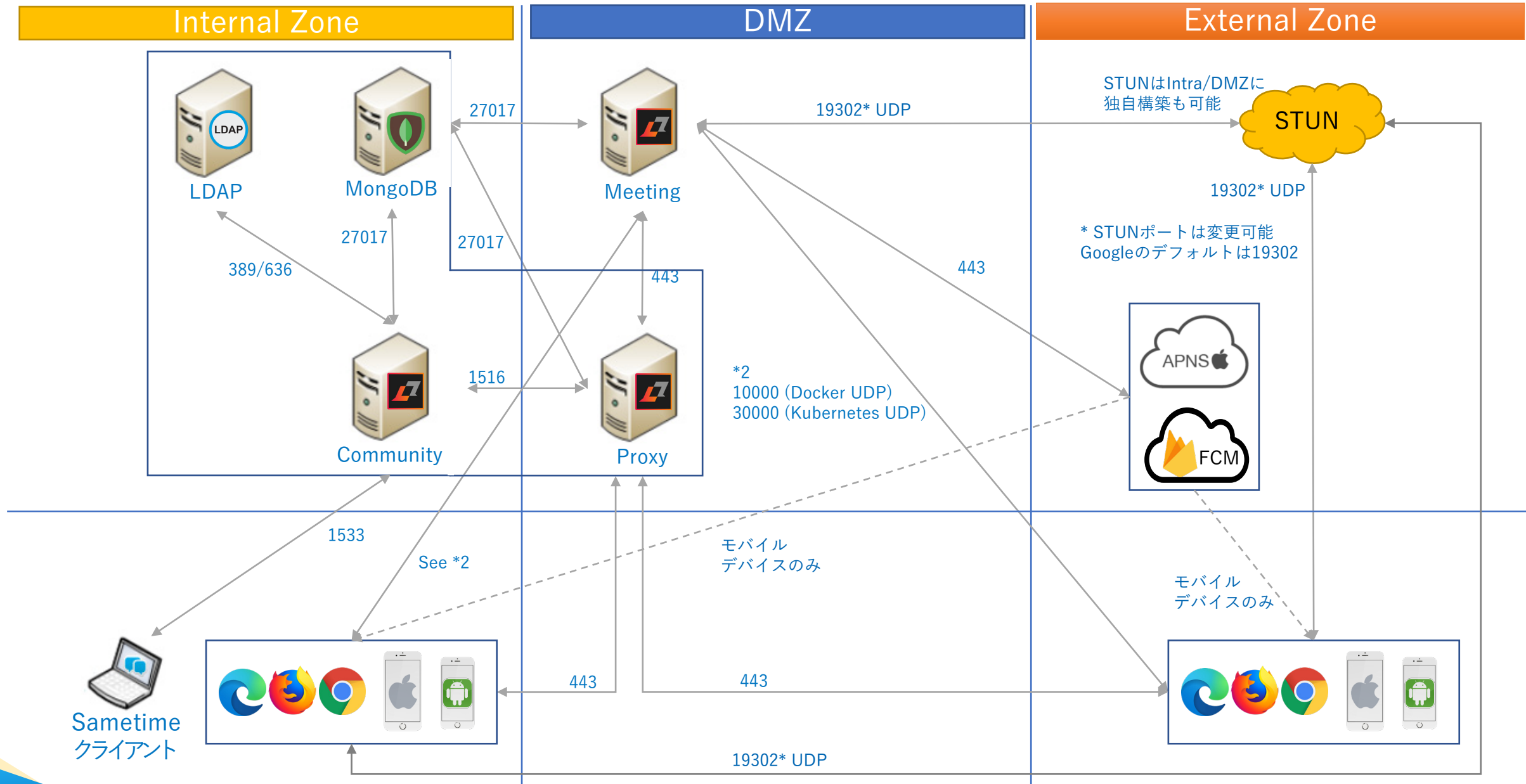
イントラネット各サーバへ

イントラネット DMZ インターネット

構成



HCL Sametime Premium (Intranet & Extranet)



作業の流れ 1/3 (前半: Windows)

- Firewall 穴開け
- Domino サーバー + Language Pack インストール
- Notes + Domino Administrator クライアント インストール
- Domino サーバー + Notes / Domino Administrator クライアント セットアップ
- Domino サーバー起動テスト / 停止
- MongoDB インストール
- MongoDB セットアップ (DB作成など)
- Sametime Community サーバー インストール
 - チャットログ ini 設定
- Sametime Connect クライアント インストール (動作確認用)
- パスワード探しの寄り道の末に動作確認
- Sametime Proxy サーバー インストールとセットアップ
- 動作確認

作業の流れ 2/3 (後半: Linux)

- Docker アンインストールとインストール
- Sametime Meetings 構成設定とインストール
 - 構成ファイル設定
- SSO設定 (トークンの設定)
- チャット機能側で、ミーティング機能利用可能ポリシー設定
- Sametime Proxy サーバーにMeetingサーバー設定追加

作業の流れ 3/3-1 (証明書)

- 本来、1/3と2/3の作業で行うべきもの。準備が間に合わず後からの作業に。証明書がある前提で作業。
- Sametime Meeting: 停止後、証明書をcertbotで取得し、(リネームしながら上書き) コピーし、起動。

左: 今回作成ファイル名 右: Sametime自己証明書

fullchain.pem -- cert.crt
privkey.pem -- cert.key

```
[root@ip-10-0-1-90 letsencrypt]# ls -l live/meeting.notescons.gr.jp/ certbot で取得した証明書
total 4
lrwxrwxrwx. 1 root root 47 Oct 13 10:45 cert.pem -> ../../archive/meeting.notescons.gr.jp/cert1.pem
lrwxrwxrwx. 1 root root 48 Oct 13 10:45 chain.pem -> ../../archive/meeting.notescons.gr.jp/chain1.pem
lrwxrwxrwx. 1 root root 52 Oct 13 10:45 fullchain.pem -> ../../archive/meeting.notescons.gr.jp/fullchain1.pem
lrwxrwxrwx. 1 root root 50 Oct 13 10:45 privkey.pem -> ../../archive/meeting.notescons.gr.jp/privkey1.pem
-rw-r--r--. 1 root root 692 Oct 13 10:45 README
[root@ip-10-0-1-90 letsencrypt]# cd /sametime
[root@ip-10-0-1-90 sametime]# ls -l jitsi-config/web/keys/ Sametime Meeting の自己証明書
total 8
-rw-r--r--. 1 root root 1326 Oct 7 13:30 cert.crt
-rw-----. 1 root root 1708 Oct 7 13:30 cert.key
[root@ip-10-0-1-90 sametime]#
```

作業の流れ 3/3-2 (証明書)

- Sametime Proxy: win-acmeを使ってLet's Encryptの証明書を取得。
- openssl で pem 形式から p12 (pfx) 形式に変換

```
C:\Tools\openssl>openssl pkcs12 -export -in C:\Tools\certs\chat.notescons.gr.jp-crt.pem -inkey C:\Tools\certs\chat.notescons.gr.jp-key.pem -certfile C:\Tools\certs\chat.notescons.gr.jp-chain-only.pem -out C:\Tools\certs\pkcfs12.pfx -passout pass:
Loading 'screen' into random state - done
C:\Tools\openssl>_
```

- Proxy サーバーのキーストアにインポート

```
C:\HCL\sametimeproxy\openjdk\bin>keytool -importkeystore -srckeystore C:\Tools\certs\pkcfs12.pfx -srcstoretype PKCS12 -srcstorepass 
-destkeystore C:\HCL\sametimeproxy\conf\sametime.keystore -deststoretype PKCS12 -deststorepass 
キーストアC:\Tools\certs\pkcfs12.pfxをC:\HCL\sametimeproxy\conf\sametime.keystoreにインポートしています...
別名1のエントリのインポートに成功しました。
インポート・コマンドが完了しました: 1件のエントリのインポートが成功しました。0件のエントリのインポートが失敗したか取り消されました
C:\HCL\sametimeproxy\openjdk\bin>_
```

- c:\HCL\sametimeproxy\conf\server.xml で証明書設定を変更
- keystoreFile= と keystorePass= を変更する (上: 変更前、下: 後)。

```
keystoreFile="conf/stproxy.keystore" keystorePass="
```

```
keystoreFile="conf/sametime.keystore" keystorePass="
```

作業後に発覚したこと: 録画ができない

録画ボタンは表示されるが押しても反応がない。漏れが発覚。3つの作業を実施。

- **1: 「ホスト上の仮想サウンド・デバイスの構成」**

- https://help.hcltechsw.com/sametime/11.6/ja/admin/configure_virtual_devices.html

- 以下は5つ同時に録画する設定 (CPU能力により調整)

```
# configure 5 capture/playback interfaces
echo "options snd-aloop enable=1,1,1,1,1 index=0,1,2,3,4" > /etc/modprobe.d/alsa-loopback.conf
# setup autoload the module
echo "snd_aloop" > /etc/modules-load.d/snd_aloop.conf
# load the module
modprobe snd-aloop
# check that the module is loaded
lsmod |grep snd_aloop
```

- **2: 「ミーティングで MongoDB を有効にする」を行っていないかつ**

- https://help.hcltechsw.com/sametime/11.6/ja/admin/enable_mongodb_meeting.html

- MongoDBサーバーコンソールでロールの設定

```
> use admin
> db.grantRolesToUser( "sametimeUser", [ {role:"readWrite", db:"meeting"}])
```

作業後に発覚したこと: 録画ができない

3: 「Docker デプロイメント用の追加ホストの定義」

- https://help.hcltechsw.com/sametime/11.6/ja/admin/t_installing_centos.html
- docker-compose.yml の以下の2つのセクションが新たに追加。青字部分が追記部分。

recordingsセクション

```
networks:
  sametime.test:
    extra_hosts:
      - "<stproxy_host_name>:<stproxy_ip_address>"
```

catalog:セクション

```
networks:
  sametime.test:
    extra_hosts:
      - "<mongoDB_host>:<mongoDB_IP_Address>"
```

反省・課題

- チャットログ設定の再帰処理
 - MongoDB のログはデフォルトでは、1つのログファイルに追記される設定だが、長期運用を考慮するとローテーションするようにした方がよいと考えられる。

変更前	変更後
Mongod.cfg : logAppend: true	Mongod.cfg : #logAppend: true logRotate: rename

- 技術情報として公開しているものに不足あり（11.6版として近日更新）
 - KB0090513 HCL Sametime 11.5 Premium インストールガイド
 - KB0085431 Sametime 11.5 Meeting Server のインストール手順（Docker 使用）
- その他
 - 社内STUNサーバーデプロイについては今回はスコープ外
 - 証明書取得手順はスコープ外
 - TCPブリッジ構成は今回はスコープ外
 - https://support.hcltechsw.com/csm/ja?id=kb_article_view&sysparm_article=KB0087199