仕　様　書

データ共有、ログ収集・管理システム及びメール環境の構築　一式

平成 27 年 2 月

東京大学医科学研究所

件名　：データ共有、ログ収集・管理システム及びメール環境の構築　一式

目的　：
本調達は、厚生労働科学研究費補助金「ヒト幹細胞を用いた再生医療を臨床実用化のための基盤構築に関する研究」で整備した「幹細胞関連情報の基盤システム」のシステムの機能拡張として、データ共有機能、ログ収集管理システム及びメール環境の構築を行うものである。

期間　：平成 27 年 2 月 16 日～平成 27 年 3 月 20 日

作業実施場所　：
主な作業実施場所は東京大学医科学研究所総合研究棟 8 階（以下、中核拠点）とする。

業務従事者　：
請負者は、業務を遂行するための専門技術・経験を有しているもの 1 名以上（以下「業務従事者」）と全体を管理・統括するもの 1 名（以下「業務管理者」）を選定し，これを実施するものとする。

作業対象機器　：
日立 BladeSymphony500　3 台（CentOS 4VM, RHEL　2VM）
HA8000/RS440AL(Red Hat Enterprise Linux 5.6)
HA8000/RS210AM　8 台(RHEL 4 台、Windows Server 2008 4 台)
HA8000/RS110BM　4 台(RHEL 2 台、Windows Server 2008 2 台)
HA8000/TS10-h　2 台(RHEL 2VM、Windows Server 2008 2VM)
FortiGate-100D　5 台 FortiOS
FortiGate-200B　2 台 FortiOS
FortiGate-60C　4 台 FortiOS
Apresia15000　5 台
Apresia13200　1 台
ApresiaLight　4 台

作業内容　：
(1)ネットワーク環境設計及び設定変更
基盤システム内のネットワークにて、データ共有機能、ログ収集・管理システム web サービス及びメール環境を構築するために必要なネットワーク環境設計及び設定変更を行うこと。ネットワーク設計においては、既存拠点間の通信におけるセキュリティに十分配慮

した設計とすること。既設のネットワークケーブル以外に配線が必要となる場合は必要に応じて、各種スイッチ類の物理的な配線作業も実施すること。
ネットワーク環境の設定変更、配線作業等に際しては、既存ネットワークの動作に影響を与えないように事前に既存ネットワークの設定及び配線状況を調査し実施すること。また、運用中の既存拠点間の通信にあたえる影響が最小限となるように作業計画を策定し作業すること。

(2)データ共有サーバ構築作業

中核拠点の HA8000/RS440AL にデータ共有サーバ機能を持たせるため、ownCloud(オープンソース版)をインストールし設定すること。HA8000/RS440AL の OS は、Red Hat Enterprise Linux 5.6 であるため HA8000/RS440AL にて動作可能かつ ownCloud 最新版が動作する Red Hat Enterprise Linux もしくは、CentOS の最新版にアップグレードすること。

データ共有サーバ構築においては、HA8000/RS440AL の内蔵ディスク及び SAS 接続の外部ディスク、VFP600(NAS サーバ)上の必要なデータを扱えるように設計・設定すること。

ownCloud の UI のテーマは、ownCloud の標準機能で設定可能な範囲で、統合システムに準拠していること。

(3)ログ収集・管理システム構築作業

各拠点機器の稼働状況の把握、異常検出を運用管理者が容易に行うことを目的とし、各拠点 HA8000(Linux サーバ,Windows サーバ)及び FortiGate の各種ログ収集のために、オープンソースソフトウェア fluentd を必要な機器にインストールし設定すること。
収集したログを容易に検索し可視化できるよう中核拠点の BladeSymphony500 に、オープンソースソフトウェア Elasticsearch および Kibana をインストールし設定すること。Kibana が動作するサーバでは、HTTP サーバ機能として、Nginx をインストールし設定すること。

Kibana の UI のテーマは、Kibana の標準機能で設定可能な範囲で、統合システムに準拠していること。

(4)メール環境構築作業

中核機関のサーバからインターネット向けにメール配送を行うために、基盤システムのサーバ機器・メール配信設定に対して、Postfix 及び DNS サーバ（bind）を設定変更すること。別途、準備する外部メールサーバに対してセキュアにメール送信できるよう設定すること。

作業に際しては、運用中のシステムに影響を与えないよう現システムの動作を熟知したうえで適切な試験を行うこと。

(5) システムテスト実施

構築中及び納品前の各段階において、システム上でシステムテスト（稼働試験）を行うこと。システムテストに際しては、運用中のシステムに影響を与えないよう現システムの動作を熟知したうえで適切な試験を行うこと。

(6) 納品物

①サーバ及びネットワーク機器の各種コンフィグファイル・パラメタファイル
②システム設計書
③システムテスト結果報告書
④システム取扱説明書
（インストール・セットアップ方法を含むシステム管理マニュアル）
⑤システム使用説明書（ユーザーマニュアル）

(7) その他

本仕様書に定めのない事項について、請負者は発注者と十分に協議の上、方針を決定すること。

HITACHI
Inspire the Next

ログ収集・管理システムとメール環境の構築

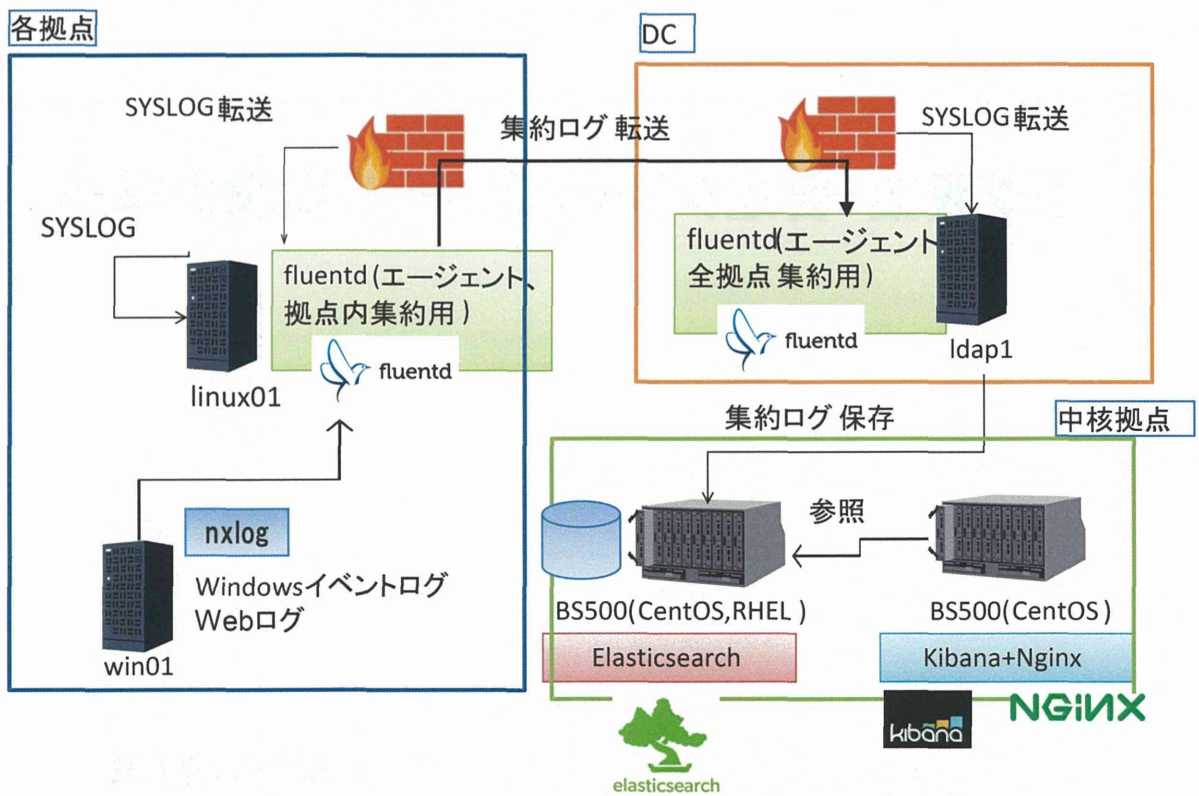
2015年1月28日

(株)日立製作所

Human Dreams.
Make IT Real.

1. ログ収集・管理システムの構築

- 構築期間、サーバリソースを考慮し、取得するログを最小限に絞り構築する
  - linux01,win01のSYSLOG
  - FortigateのSYSLOG
  - WEBアプリケーションのアクセスログ
- 構築後、東大のみでカスタマイズ・運用することを前提とし、拡張できるようにマニュアルを整備する
- 札幌DCが無くなる場合を考慮し、中井研とDCで機能を分ける
- DCの機能はfluentdの中継のみとする



Elasticsearch, Kibina+Nginxは下記マシンにインストールすることを想定する
BS500#2
①ブレード#0 DBサーバ#0 Red Hat Enterprise Linux 6.4 [redacted]
②ブレード#0 DBサーバ#1 Red Hat Enterprise Linux 6.4 [redacted]
③ブレード#1 CentOSサーバ#0 CentOS [redacted]
④ブレード#1 CentOSサーバ#1 CentOS [redacted]
⑤ブレード#2 CentOSサーバ#0 CentOS [redacted]
⑥ブレード#2 CentOSサーバ#1 CentOS [redacted]

1. ログ収集・管理システムの構築

【各サーバ構成】

(1)各拠点
linux01,win01にfluentdエージェント構築
・win01は、イベントログ及びWebログをnxlogにより syslog転送
・linux01は、自身とwin01のログを集約して札幌DCの集約用fluentdに転送
・linux01にfortigateのSYSLOG用プラグイン配置

(2)札幌DC
・拠点のログを集約するfluentdを構築
・中井研のElasticSearchに保存する
・DCが中井研に移設された場合はfluentdだけ再構築

(3)中核拠点(中井研)
・ElasticSearchはCPUリソースとディスクを消費するため、BS500のサーバを4台使用し(構築時に台数を評価)クラスタを構築
・データはBR1650のローカルに保存。
・httpサーバとしてNginxを使用し、Nginxサーバで Kibanaを動作させる

(4)その他
・中井研、札幌DCのサーバも拠点と同様にfluentd エージェントによりログを収集する

【監視ログ内容(当初は最小限で収集)】

・FWの外部からのアクセスログ
ログレベル、アクセス元(IP、地域)、内容、障害等
・WEBアクセスログ
アクセス元、アクセス先
・サーバSYSLOG
ログレベル、ファシリティ、内容等

1. ログ収集・管理システムの構築

【日程】
2月は設計・ヒアリング、社内簡易環境による確認、設計書・手順書・拡張マニュアルの作成
3月1週で構築
3月2～4週でチューニング(表示などを調整しながら進める)

全体で1人×1月の作業量を想定

2. メール環境の構築

【メール環境の構築】

既存のサーバ機器・メール配信設定を利用し
メール環境の再構築を行う

(1) 外部へのメール通知方法(当面、下記②での運用を想定)

①外部とのSMTP送受信ができるように設定する
→ ドメイン登録、セキュリティ対策作業が必要だが
今回の作業外として、必要に応じて次年度以降とする

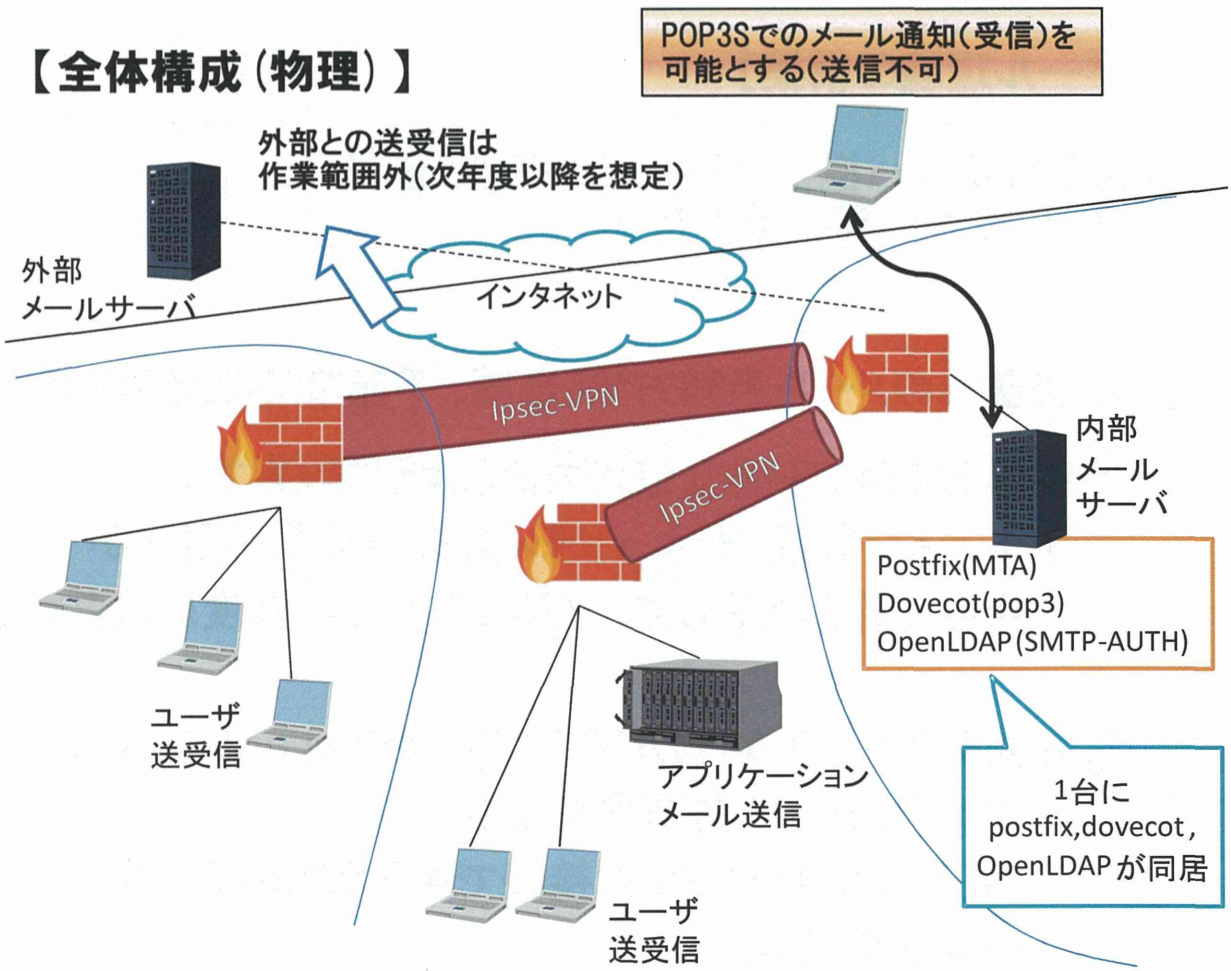
②特定IPアドレスからのPOP3S(POP3 over SSL)のみ
ファイアウォール許可を与える
SINET,インターネットに接続できる端末のメーラで
メール受信可能
限定的なアドレスとユーザのみ利用を許可する
(当面、中井研内のユーザを想定)

(2) メール環境LDAP連携(Postfix + OpenLDAP)

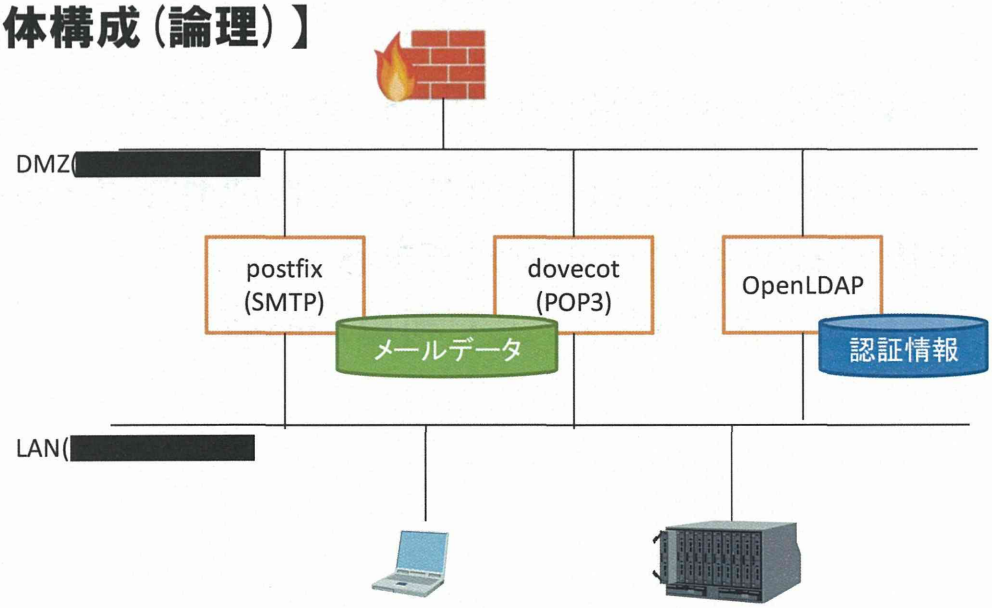
メールサーバにLinuxアカウントを作成せずメールのみを
利用するアカウントを作成できる
(管理上とセキュリティ上で利点がある)

2. メール環境の構築

【全体構成（物理）】



【全体構成（論理）】



2. メール環境の構築

【作業項目】

- LDAPのスキーマ追加
  - メールアドレスに関するスキーマを既存環境に追加する
- Postfix、dovecotの設定
  - 既にある環境について、LDAP化、バーチャルメールボックス等の設定
- 鍵作成(要調査)
- テスト

実施しないもの

- サイジング
  - 既設環境への構築であるため拡張できない
  - 当面実行ユーザが10人程度と予想される
    - そのため、設計書・手順書で拡張・再構築を明示する
- ファイアウォールのポート解放
  - 東大再生医療HWのドメインがないため(作業範囲は内部向けのみにするが、外部通信に拡張できることを前提として構築)
- ユーザ作成
  - テスト用のみを作成し、テスト終了後に削除
  - 実際のユーザは東大殿にて作成する
- WEBメール、IMAP4は構築しない

2. メール環境の構築

【日程】

- ヒアリング(2日)
  - 構成説明
  - レビュー
- LDAP設計(1日)
  - パラメタシート
- postfix、dovecot設計(6日)
  - 手順書(3日)
  - パラメタシート(2日)
- 鍵作成(1日)
  - 手順
- 構築(5日)
- テスト(3日)
  - テスト計画書作成
  - SMTPテスト
  - メールクライアントテスト
  - 予備
- 全体で1人×1月の作業量を想定


HITACHI
Inspire the Next

HITACHI
Inspire the Next

データ共有サーバ(owncloud)システム構成

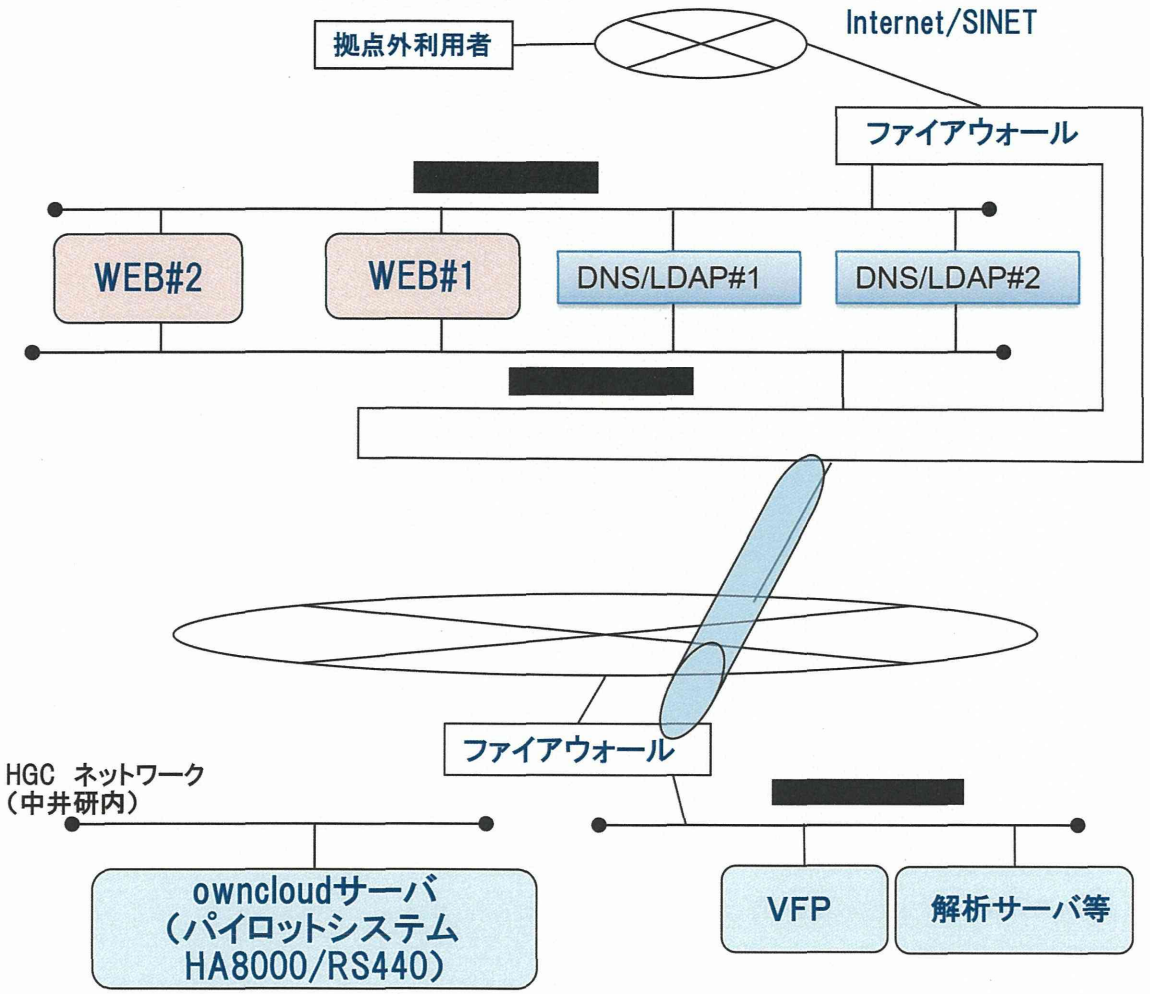
2015年1月22日

Human Dreams.
Make IT Real.

1. 拠点外からのデータ共有システム

1.1 2015/3時点 システム構成

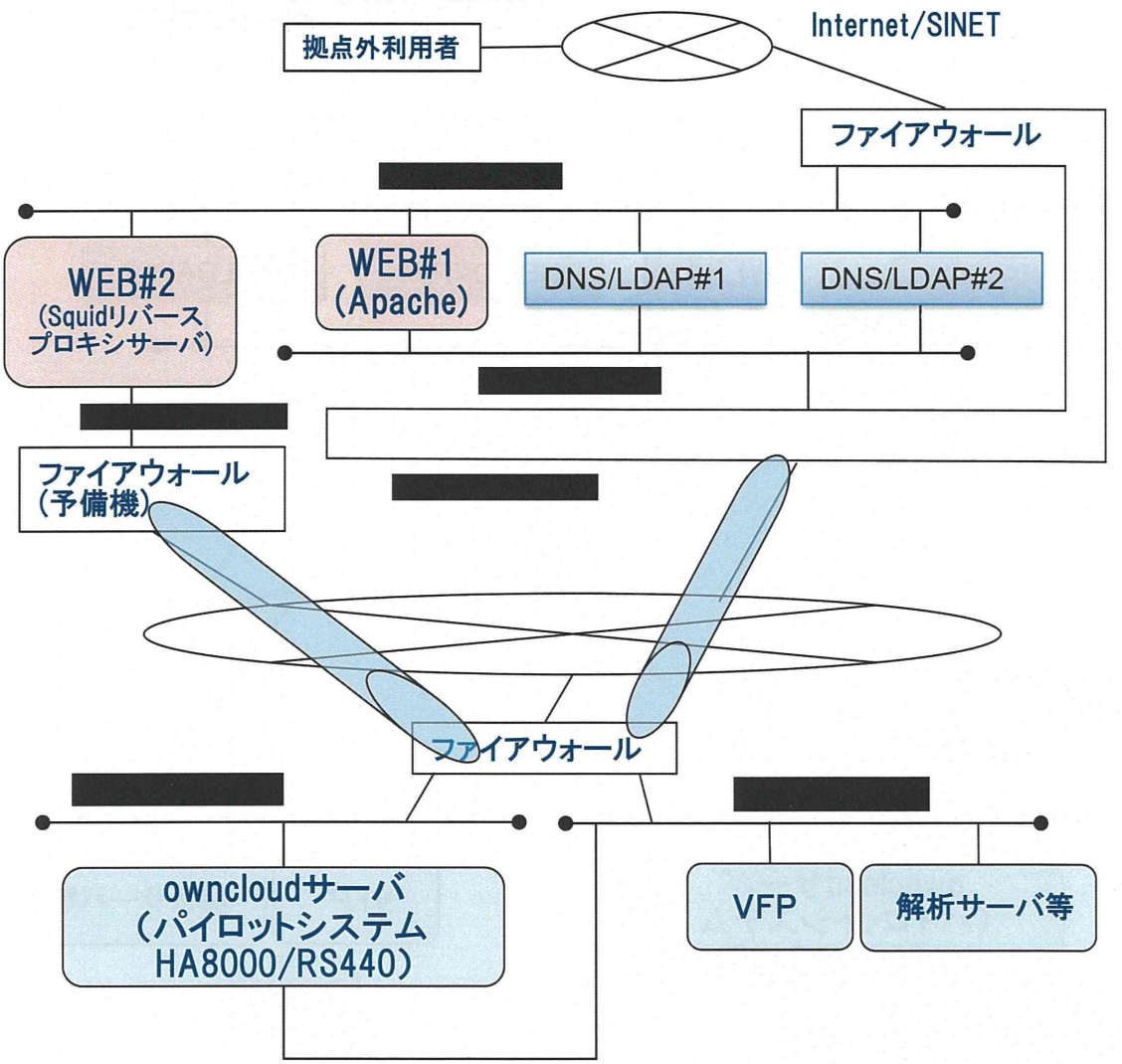
1.1.1 ネットワーク概略(論理構成)



1. 拠点外からのデータ共有システム

1.2 外部公開時システム構成

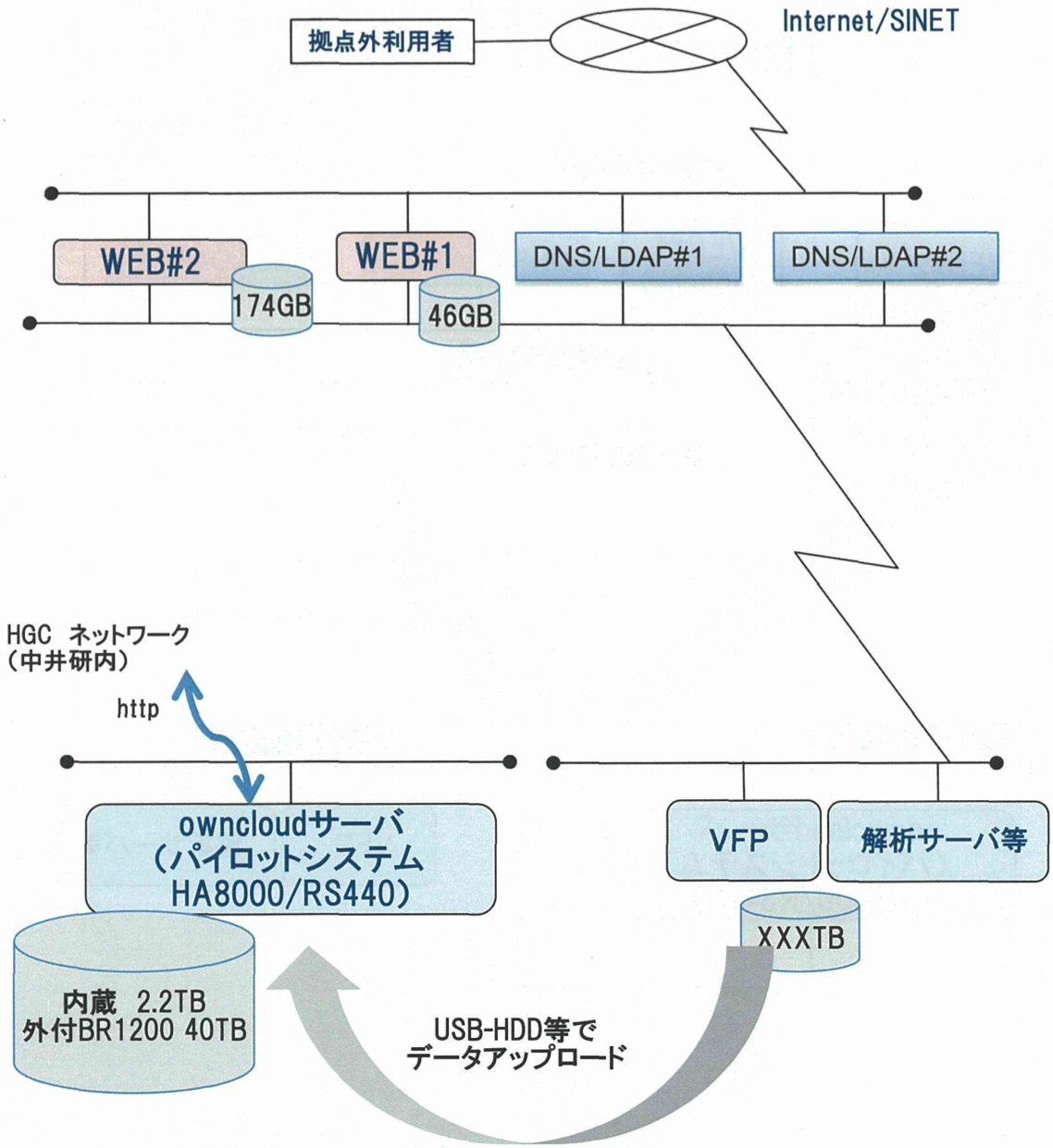
1.2.1 ネットワーク概略(論理構成)



1. 拠点外からのデータ共有システム

1.3 2015/3時点 システム構成

1.3.1 owncloud関連サーバ(論理構成)

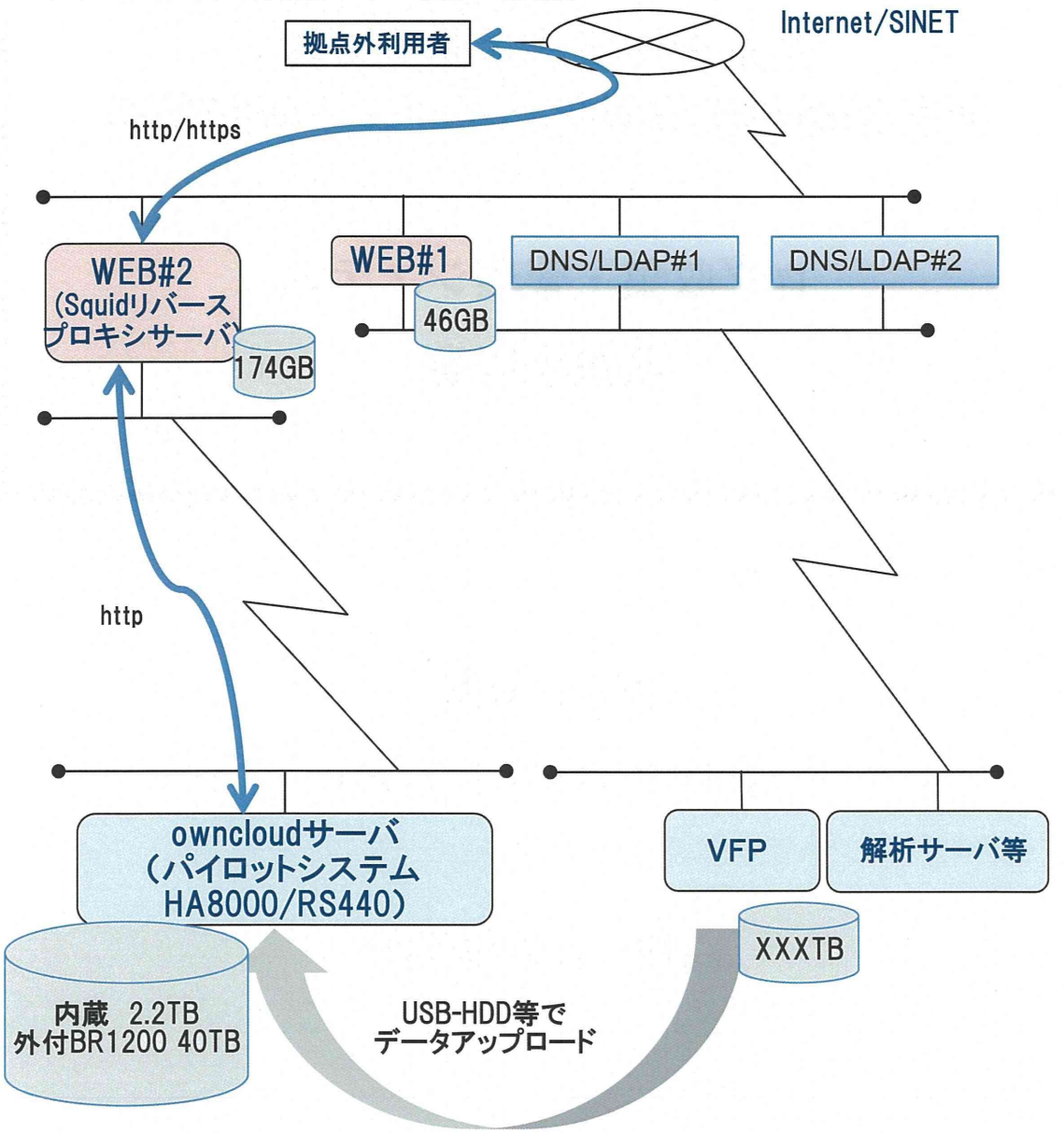


導入時OS RedHat 5.6
→
RedHatもしくは、CentOS 6.X系
へのアップグレード作業が必要

1. 拠点外からのデータ共有システム

1.4 外部公開時システム構成

1.4.1 owncloud関連サーバ(論理構成)



導入時OS RedHat 5.6
→
RedHatもしくは、CentOS 6.X系
へのアップグレード作業が必要

東京大学医科学研究所殿
再生医療臨床実現化ハイウェイ研究事業

ログ収集・管理システム
取扱説明書

第１．０版

２０１５年３月２０日

（株）日立製作所

～　変更履歴　～

#	日付	版数	変更箇所	変更内容	変更者	承認者
1	2015/3/20	1.0	-	新規作成	中島	
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						