

## 課題情報シート

テーマ名 :	セキュアなネットワーク構築・統合監視システムの開発				
担当指導員名 :	平澤 博、友添 信雄	実施年度 :	26 年度		
施設名 :	九州職業能力開発大学校				
課程名 :	応用課程	訓練科名 :	生産システム技術系		
課題の区分 :	開発課題実習	学生数 :	8 人	時間 :	48 単位 (864h)

### 課題制作・開発のポイント

#### 【開発（制作）のポイント】

インターネットサーバ関連のシステム構築に際して、企業ニーズに対応するために、外部接続サーバとしての VPS(Virtual Private Server)を契約し、課題実習用ドメインを取得して、実際のインターネット上での動作検証を行ない、サーバアプリケーションシステムの構築・導入・設定を行ない、企業の実導入に際してのドキュメント作成・提供しています。

実際の外部環境導入については、九州校独自のグループ研究費用を利用しているが、別途、対象企業の方から提供された VPS 環境へ提案システムの一部を実導入しています。

学内から外部の VPS などへの接続に際しては、企業からモバイルルータとノート PC を借用して接続・設定作業を行なっています。

初年度は「外部の ISP(Internet Service Provider)に委託していた Web・Mail 維持費の削減ということで VPS 利用を提案」を主眼としていましたが、2 年目の本年度は「近距離企業との経営統合に向けた業務データなどのセキュアな情報共有手法の検討」「各種アプリケーションサーバ監視：通報機能の検証」「サーバ室の温湿度監視と侵入検知・通報の検証」などを行い、実記環境での「遠隔管理・運用処方などの実機検証」も行なっています。

【学生数の内訳】 VPS サーバ：1 名、VPN・トンネリング：1 名、統合監視：2 名、ファイルサーバ：1 名、温湿度監視：2 名、侵入検知・画像監視：1 名

#### 【訓練（指導）のポイント】

学内の実習でのサーバ構築実習は、学内ネットワークのセキュリティ対応に基づく内部ネットワーク上での構築作業しかできないため、サーバ構築などの実習には使いづらい環境となっています。実際に学外に設置されている本実験サーバへの接続環境の確保と接続利用時のセキュリティ対応などの理解が必要となってきます。学内セキュリティポリシーに従って、本実験サーバへの外部接続をどのように実現すれば良いか苦慮するところであります。

企画(5月)および仕様(7月)、デザインレビュー(10月)、や最終(3月)の長期に亘り客員教授や諸先生方からもアドバイスを頂くとともに、企業の方への進捗状況報告と最終成果報告会を 12 月・3 月に行ない、学生のモチベーションを高める工夫をしました。

## 課題に関する問い合わせ先

施設名 : 九州職業能力開発大学校  
住所 : 〒802-0985 福岡県北九州市小倉南区志井 1665-1  
電話番号 : 093-963-0125 (代表)  
施設 Web アドレス : <http://www3.jeed.or.jp/fukuoka/college/>

## 課題制作・開発の「予稿」および「テーマ設定シート」

次のページ以降に、本課題の「予稿」および「テーマ設定シート」を掲載しています。

# セキュアなネットワーク構築・統合監視システムの開発

生産電子システム技術科  
生産情報システム技術科

## 1. 目的

VPS(Virtual Private Server)、社内サーバ、ファイルサーバ、外部とのネットワーク機能、侵入検知システム、温湿度監視システムを構築して、企業想定ネットワーク環境を作成した。

また企業からの依頼で、140m 程度の 2 拠点間を無線 LAN 通信が可能かどうか検討し、可能であれば無線 LAN を用いた業務連携のためのセキュアな情報共有手法を検討、提案することを目的とする。

## 2. 課題概要

企業想定ネットワーク環境において以下を検討した。

- ①VPS を利用した、インターネットサーバ(DNS、Mail、Web)維持費の削減。
- ②サーバ室の温湿度監視のため、温湿度センサからデータの取得とその可視化の検討。
- ③サーバ室想定物理的なセキュリティ確保のために、侵入検知や画像監視の検討。
- ④社内サーバにおいて、各種ソフトウェア監視ツールを利用した統合監視機能の検討。
- ⑤各種サーバ機能の障害を検知した場合に、管理者へメールで通報する機能の検討。
- ⑥ファイルサーバにおいて、ログの表示や、ファイルのアクセス権限をつける機能の検討。
- ⑦VPN を用いてサーバ間をセキュアに通信させる手法の検討。
- ⑧外部ネットワークから、VPN を用いて各種メンテナンス作業を行う手法の検討。
- ⑨140m 程度の 2 拠点間を無線 LAN 接続し、セキュアに情報の共有化を行う手法の検討。

## 3. 装置仕様

今年度制作した、ネットワーク構成図を図 1 に示す。昨年度は本社と第二工場間のネットワーク想定だったのに対して、今年度は企業間の業務提携のため、T 社と S 社間のネットワーク想定になっている。これに準じて社内サーバを二つ用いることにした。さらに新たに追加された要素として、企業からの依頼であった 140m 程度の近距離であ

る 2 拠点の「無線 LAN 環境を利用したセキュアな情報共有手法」について、実際に無線 LAN ルータを用いて検討した。

また昨年度課題として残された、ファイルサーバにおいてログの表示や、アクセス制限などの、セキュアにデータを扱う方法や、人感センサや jpeg カメラを用いたサーバ室の物理的なセキュリティの確保を昨年度に引き続き検討した。

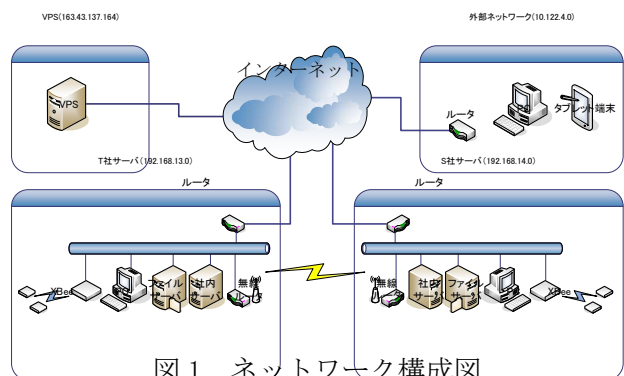


図 1 に書かれているセンサデバイスの仕様を表 1、外部ネットワークから社内のネットワークに接続するためのトンネリング機能や VPN 機能を実現するためルータの高性能化を行うルータの仕様を表 2 に示す。また、今年度追加された無線 LAN ルータの仕様を表 3 に示す。社内サーバには Raspberry Pi<sup>®</sup>を使用する。その仕様を表 4 に示し、ファイルサーバの仕様を表 5 に示す。

表 1 センサデバイス仕様

項目	内容
SH マイコン	SH7144
データ通信	RS232C, XBee <sup>®</sup>
温湿度センサ	TMP102、LM35DZ
人感センサ	PIR センサ RevA
電源	AC アダプタ (5V、1.5A)
外形寸法 (mm)	親機 (W110×D90×H40)
質量	子機×3 (W80×D50×H40) 各 100g 程度

表 2 ルータの仕様

項目	内容
製品名	WHR-300HP2 (BUFFALO)®
ポート数	LAN:4 WAN:1
データ転送速度	100/10Mbps
最大消費電力	8.2W
外形寸法	55×159×131mm

表 3 無線 LAN ルータの仕様

項目	内容
製品名	WZR-1750HP (BUFFALO)®
ポート数	LAN:4 WAN:1
WLAN 対応規格	IEEE802.11 ac/a/b/g/n
WLAN 対応周波数	5.2-5.7GHz 帯
データ転送速度 (最大)	ac : 1300Mbps n : 450Mbps a, g : 54Mbps b : 11Mbps
最大消費電力	18.2W
外形寸法	34×212×183mm

表 4 社内サーバ (RaspberryPi) 仕様

項目	内容
Soc	Broadcom® BCM2835
CPU	700MHz/ARM1176JZF-S コア
メモリ (SDRAM)	512MB
USB2.0 ポート	2
ストレージ	SD メモリカード
ネットワーク	10/100Mbps イーサネット
電源電圧	5V
大きさ	85.60×53.98mm
OS	Debian

表 5 ファイルサーバ仕様

項目	内容
製品名	NAS LS-V2.0TLJ (BUFFALO)®
メモリ (電波)	2.0TB (AC100V 50/60Hz)
大きさ	45×175×150mm
環境条件	温度 5~35℃ 湿度 20~80%

## 4. 各部機能

### 4.1. センサデバイス

#### 4.1.1. 温度・湿度計測部

離れた場所の温度・湿度を計測するため、計測部と送信部に分け、製作する。また計測部を子機、送信部を親機とした温度・湿度センサからの出力を SH マイコンで制御し、XBee®により子機から親機へデータを送信する。

図 2 に温度・湿度計測部を示す。

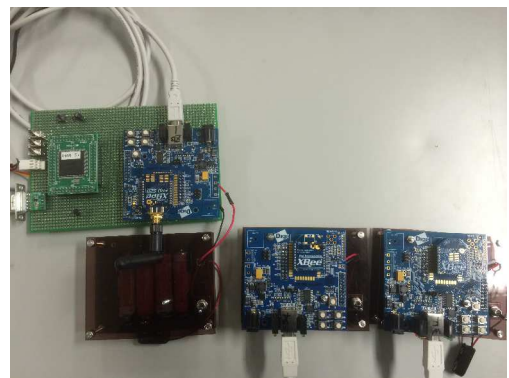


図 2 温度・湿度計測部

#### 4.1.2. 侵入検知システム部

サーバ室の侵入者を検知するシステムであるため、出入りに人感センサを取り付ける。人感センサが感知すると JPEG カメラで画像を撮るようにする。画像データは、社内サーバの Web サーバに送信され、ブラウザに表示される。図 3 に侵入検知システム部を示す。

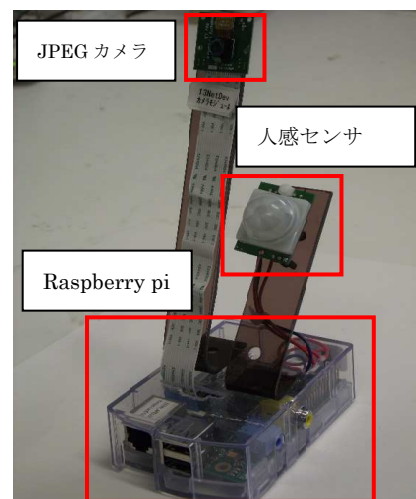


図 3 侵入検知システム部

### 4.2. VPS とレンタルサーバ

インターネットサーバ (DNS・Web・Mail) 維持費の削減提案として VPS とレンタルサーバの利用操作・運用管理手法などの比較検討を行う。

#### 4.2.1. VPS

インターネットサーバ (DNS・Web・Mail) を導入することで、インターネットサーバ維持費の削減を行う。

運用管理手法として、統合監視ツールを導入し、さらに、クラウドサーバツールを導入し、クラウドサーバ化も検討する。

#### 4.2.2. レンタルサーバ

Web ページの公開やメールアドレスの追加、メールの送受信を容易に設定・利用すること

ができる。月額 125 円であることや安定性などの点から、さくらレンタルサーバイトによる利用操作や運用管理手法を理解し、VPS 利用操作・運用管理などとの比較検討を行う。

#### 4.3. 社内サーバ

社内サーバには RaspberryPi® を使用する。その RaspberryPi® に基本的なサーバを構築し MRTG、Munin、Nagios、Zabbix® を実装することで統合監視環境を構築し、Zebedee、OpenVPN を実装することで、セキュアなネットワーク環境を構築する。

#### 4.4. VPN

企業を想定とするネットワークには T 社と S 社があり、2 地点のネットワークは分離されている。T 社と S 社との拠点間 VPN を構築することで、2 地点のネットワークは単一のネットワークと同様に通信可能とする。

また、出張等の外出で社外にいた場合は、インターネットを利用して、トンネリング機能や VPN (Virtual Private Network) 機能により社内サーバに接続しメンテナンスを行うことができる。

#### 4.5. ルータ

##### 4.5.1. 高機能化

ルータに DD-WRT というファームウェアを使用し、ルータを高機能化することで、ルータに SSH を使って接続できるようになる。これにより、ルータに接続されている PC に何かしらの異常が発生したときに、外部からルータに対して SSH 接続をすることで異常のある PC へのトンネリングが可能になる。

##### 4.5.2. 無線通信

無線 LAN ルータを用いて 140m 程度の 2 拠点間を無線 LAN 接続する実験を行い、無線 LAN を用いたセキュアな共有手法の検討を行う。通信規格は 11ac と 11n を用い、140m ほどの直線距離に無線 LAN を設置して実験を行う。

#### 4.6. ファイルサーバ

NAS を LinuxBox 化し、ファイルサーバとする。その際、ユーザのログイン認証を行なう。

セキュリティ保護のため、共有フォルダからファイルをコピーすることを禁止し、外部への情報の流出を防ぐようにする。また、アクセスログをとることで、ファイルサーバの利用を監視する。また、AMP 環境対応オープンソースの

グループウェアアプリを導入し、各種情報共有手法も検討する。

### 5. 製作費用内訳

今回製作したシステムの費用の概算を表 6 に示す。

表6 製作費用概算

分野(品目)	価格
生産電子 XBee®, センサ等の電子部品、マイコン等	61,184
生産情報 ルータ、NAS、RaspberryPi等	130,200
概算合計	191,384

### 6. 製品評価

#### 6.1. センサデバイス

##### 6.1.1. 温度・湿度計測部

温度監視システムのセンサデバイスは完成。無線での温度データの取得を行うことができる。

今回無線通信のため使用する XBee® は、実際に室内で使用する際にデータの取得は可能である。しかし、壁を隔てた別の部屋の監視をする際には、XBee® を窓際に置くなどして感度の調整を行う必要がある。

##### 6.1.2. 侵入検知システム部

人感センサが反応することによって JPEG カメラで写真を撮影することができる。また即座にウェブ上に掲載されサムネイルとして最新のデータを表示することができる。

問題点として RaspberryPi® のメモリ容量 512M バイトを超えてしまうとカメラの撮影が停止してしまう。

#### 6.2. VPS とレンタルサーバ

##### 6.2.1. VPS

インターネットサーバ DNS・Web・Mail サーバの構築、動作確認ができる。

利点としては、機能の制限がほぼなくサーバの高速化処理や最新技術を取り入れることができる。欠点としては、レンタルサーバと比較してコストが高い点である。

##### 6.2.2. レンタルサーバ

既存の Web、Mail サーバを用いてウェブ上での情報の公開、メールの送受信ができる。

利点としては、導入が簡単でコストが安いという点である。欠点としては、機能が制限されており、設定できる範囲も限界があるという点である。

### 6.3. 社内サーバ

それぞれのネットワーク監視ツールの動作の確認ができる。閾値を超えるなどの異常時の管理者へのメールの送信ができる。

### 6.4. VPN

メンテナンスを行う外部端末を Android® のスマートフォンで検証し、社内サーバに対して接続を確認できた。コマンド実行、統合監視ツールの閲覧もすることができた。

### 6.5. ルータ

#### 6.5.1. 高機能化

ルータに DD-WRT を導入し、拠点間 VPN を構築することができた。異なるネットワークの 2 拠点間を VPN で通信をすることができた。

#### 6.5.2. 無線通信

2 拠点間の無線 LAN 接続ルータによる情報の共有ができない。

無線 LAN の間に障害物が挟んだ場合、通信が 10m 程度までしか安定しなかった。直線距離の場合は 70m 程度まで安定した通信を行うことができた。この結果から、2 社間の通信を行うには直線距離や障害物の問題の考慮や、中継機を置くなどの検討が必要である。

### 6.6. ファイルサーバ

管理者及び、複数のユーザアカウントを作成し、ログイン認証を行うことができる。各フォルダに権限を付与し、ファイル操作の制限を加えることができる。またアクセスのログをとることができる。

## 7. 作業工程表

今回の開発作業の予定と実績を示した作業工程表を表 7 に示す。青い線が計画であり、斜線が実績である。また実績が 2 月末まで伸びている項目、まとめについては未完成である。

表 7 作業工程表

	4	5	6	7	8	9	10	11	12	1	2	3
開発環境の設定	斜線	斜線	斜線	斜線								
仕様検討	斜線	斜線	斜線	斜線								
ルータ高性能化					青							
拠点間VPN構築					青							
トンネリング・端末間VPN構築					青							
無線LAN設定・検証					青							
統合監視ツール設定					青							
VPS構築					青							
Xbee通信					青							
発電センサ回路作成					青							
JPEGカメラ設定					青							
温度・湿度計測回路作成					青							
ファイルサーバ					青							
まとめ												青

## 8. まとめ

現在(2/13)、システム全体の完成度は 8 割である。当初予定していた基本的な機能に関してはほぼ構築、動作の確認が取れている。残りの 2 割は、湿度データの取得、XBee から社内サーバへのデータの受け渡し、NAS へのファイルサーバ構築、ネットワーク環境、統合監視システムの脆弱性を NESSUS という専用ツールを用いて確認することである。また、企業へ本システムの導入を提案するためのドキュメントの作成がまだ途中である。

### 【参考文献】

- 1)平成 25 年開発課題実習報告書「セキュアなネットワーク構築・統合監視システムの開発」,九州職業能力開発大学校,2014/3/14
- 2)Nagios 統合監視[実践]リファレンス,技術評論社,2011/3/25
- 3)Zabbix 統合監視徹底活用,技術評論社,2014/2/7

【担当教官】 友添信雄 平澤博

※課題実習情報として、表 6 に記載されていた個々の商品名などを省略したため、以下 1/4 ページ程度の空白となっています。

# 課題実習「テーマ設定シート」グループNo. \_\_\_\_\_

作成日： 3月24日

科名：生産システム技術系

教科の科目		実習テーマ名	
生産ネットワークシステム応用課題実習（生産情報システム技術科） 電子装置設計製作応用課題実習（生産電子システム技術科） 【開発課題実習】		セキュアなネットワーク構築・統合監視システムの開発	
担当教員		担当学生	
○生産情報システム技術科： 平澤 博			
生産電子システム技術科： 友添 信雄			
課題実習の技能・技術習得目標			
セキュアなネットワーク構築・統合監視システムの開発を通して、「ものづくり」全工程を行うことにより、複合した技能・技術及びその活用能力（応用力、創造的能力、問題解決能力、管理的能力等）を習得することを目的としています。具体的には、企業ニーズに基づいた技術要素を主体とした各種ネットワーク技術、通信制御技術、センサー回路技術などを複合的に活用した設計・構築技術とドキュメント作成及び運用管理技術などの習得を目標にします。			
実習テーマの設定背景・取組目標			
実習テーマの設定背景			
<p>福岡県内企業S社では、昨年の11月からT社との経営統合化を推進してきており、業務連携における各種業務データ共有に関して、130m程度の近距離での「無線LAN環境を利用したセキュアな情報共有手法」について相談・依頼がありました。一方のTG社は、H25年度の開発課題において、「インターネット基本サーバ環境に関する維持費の削減」「第二工場とのネットワーク連携」など、今後のインターネット環境と社内ネットワーク環境などの再構築について一定の成果に基づく提案をしていますが、まだ残された課題もあり、KS社との連携を踏まえた、再検討が必要です。</p> <p>こうした企業からの依頼に対して、最新の無線規格を利用した近距離間通信の可能性を検討するとともに、急速に普及してきているVPS(Virtual Private Server)を利用したインターネットサーバ構築・運用技法により、安価でセキュアなインターネット環境構築手法を検討します。</p> <p>そして、セキュアなインターネット環境構築とその運用管理の手法、およびネットワークサーバや機器の監視・障害通報、さらに遠隔管理手法の習得、また、サーバ室などの温度・湿度監視や侵入検知・通報手法などを習得することを目標とした、「セキュアなネットワーク構築・統合監視システムの開発」をテーマとして設定しました。</p>			
実習テーマの特徴・概要			
<p>業務利用しているインターネットサーバ環境の改良・改善であるため、企業想定ネットワーク環境を構築し、企業導入相当の各種サーバ導入を行ない、近距離間の拠点間における無線通信の可能性とともに統合監視手法や障害通報環境を検討します。統合監視機能導入により、各種のネットワーク機器やサーバ機能の障害を検知した場合には、管理者へメール通報します。また、サーバ室の温度・湿度監視のため、温湿度センサデータの取得とその可視化（グラフ表示）を図るとともに、一定の設定値を超えた場合にも、管理者へメール通報します。</p> <p>併せて、サーバ室想定物理的セキュリティ確保のための侵入検知や画像監視と通報技法なども検討します。</p> <p>出張先などの社外で障害通報を受信した管理者は、インターネットを利用して、トンネリング機能やVPN(Virtual Private Network)機能により、社内サーバに接続、各種のメンテナンス作業を行なうことができます。</p> <p>開発した成果物は、セキュリティなどの検証を行ない、企業内ネットワークへの実導入を図ります。</p>			
No	取組目標		
①	相手先企業の要望から仕様を決定し、セキュアネットワークシステム設計・構築技術、マイコン制御装置設計・製作技術を複合的に活用した、セキュアなネットワーク環境構築・統合監視システムを完成させます。		
②	相手先企業内ネットワークへ実導入できるセキュリティ対応などの検証を行ないます。		
③	課題を解決するために必要な情報を収集し、分析・評価して合理的な手順や方法を提案します。		
④	システム機器を設計・構築・製作する際、理論と現場の技能・技術を複合して取り組みます。		
⑤	知識・技能・技術を有機的に結合し、テクニカルスキルを確実に身につけます。		
⑥	グループメンバーの意見に耳を傾け、課題解決に向けた目的や目標及び手順や方法について共通の認識を持ちます。		
⑦	設計製作に際して、品質、コスト及び納期をバランス良く調和させます。		
⑧	企画力・開発技法・設計製作・製品評価・品質管理など技術者としての総合力の発揮を目指して取り組みます。		
⑨	図や表を効率的に利用した分かり易い報告書や発表会予稿原稿を作成し、発表会では制限時間内に伝えたい内容を説明します。		
⑩	5S（整理、整頓、清掃、清潔、躰）の実現に努め、安全衛生活動を行います。		