

---

# Table of Contents

Introduction	1.1
--------------	-----

---

## ネットワーク環境

SophosXG	2.1
SophosXGバックアップ概要	2.1.1
バックアップ構成設定値	2.1.2

---

## 専用サーバ契約情報(Nocix)

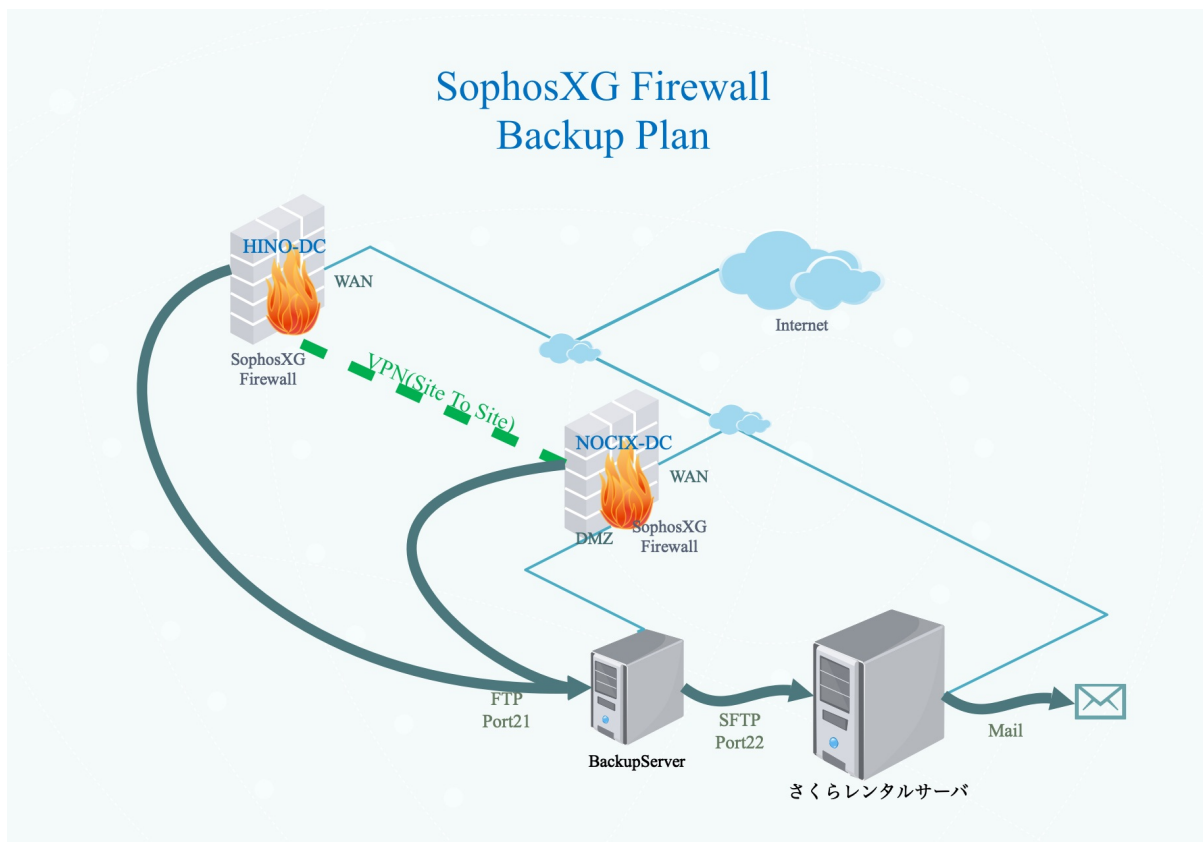
仮想基盤	3.1
仮想マシン一覧	3.2
仮想マシン	3.3
バックアップサーバ	3.3.1
監視サーバ(Zabbix)	3.3.2

---

## URL一覽

- [Ssh\\_Attack\\_Reporter](#)
- [phpmyadmin](#)
- [Blog](#)
- [Zabbix](#)

## バックアップ構成概要



各拠点のSophosXGのコンフィグのバックアップを次の3箇所に日次で作成する。

- バックアップサーバ
- さくらレンタルサーバ
- 管理用メールボックス

バックアップは下記の要項で実施する。

1. SophosXG標準機能で、日次でバックアップへFTPでアップロードする。
2. バックアップサーバもSophosXG影響下にいる為、SophosXGのコンフィグをさくらレンタルサーバへもアップロードする。（バックアップサーバ上のCronでSFTPでバックアップするシェルスクリプトを実行）
3. さくらレンタルサーバのメールサーバを使い、圧縮したSophosXGのコンフィグをメールで送付する。

## バックアップ構成設定値

## SophosXG設定値

項目	設定値（NOCIX-DC）	設定値（HINO-DC）
バックアップモード	FTP	FTP
バックアップのプレフィックス	NOCIX	HINO
FTPサーバのIP	172.16.16.99	172.16.16.99
ユーザー名	localadm	localadm
パスワード	*****	*****
FTPパス	glanz	glanz
頻度	毎日	毎日
スケジュール	00:00	00:00

## バックアップサーバ

項目	設定値	備考
SophosXGコンフィグ格納ディレクトリ	/home/localadm/glanz/	-
バックアップ保管日数	6ヶ月	-
さくらレンタルサーバへのアップロード用バッチ	/root/scripts/DAILY_BACKUP_SCRIPT.sh	-
SophosXGコンフィグ送信先メールアドレス	shinji@k636174.net	-
その他	Cron設定状況は【バックアップサーバ】を参照	

## 専用サーバ契約情報

---

## 仮想基盤

---

## 仮想マシン

---

### 仮想マシン一覧

- [\[MAIN\]monkey2018.k636174.net](#)
- [\[MAIN\]glanz.k737184.net](#)
- [\[MAIN\]ansible.k636174.net](#)
- [\[MAIN\]blog.k636174.net](#)
- [\[MAIN\]drive.k636174.net](#)
- [\[MAIN\]fsv.k636174.net](#)
- [\[MAIN\]gitlab.k636174.net](#)
- [\[MAIN\]syslog.k636174.net](#)
- [\[MAIN\]honeypot.k636174.net](#)
- [\[SophosXG\]](#)

## バックアップサーバ

### 仮想マシン設定情報

項目	設定値
仮想マシン名	[MAIN]glanz.k636174.net
インストールOS	CentOS Linux release 7.6.1810 (Core)
IPアドレス	172.16.16.99
コア数	8コア
メモリ	2046MB
アタッチネットワーク	DMZ
ディスク	16GB(スパース)
主な用途	バックアップ用途

### OS設定値

項目	設定値
ホスト名	glanz.k636174.net
IPアドレス	172.16.16.99

### Cron設定状況

実行日時（間隔）	実行するコマンド
* * * * *	php /var/www/mf_reporter/artisan schedule:run >> /dev/null 2>&1
** 30 **	/root/scripts/sar_k636174_net_certbot.sh
30 0 ***	/root/scripts/DAILY_BACKUP_SCRIPT.sh

### 稼働サービス

- SSH
- vsftpd
- mariadb
- ZabbixAgent
- rsyslog

### DAILY\_BACKUP\_SCRIPT.sh

```
#!/bin/bash

# Variable
TARGET_HOST=k636174.sakura.ne.jp
TARGET_USER=k636174
DEST_DIR=/home/k636174/Backup/`hostname`/
```

```
SOURCE_DIR=/home/localadm/`hostname`

# CREATE DIRECTORY
mkdir -p $SOURCE_DIR/server_status/
chown -R localadm:localadm $SOURCE_DIR

# Server Status
ps -ef > $SOURCE_DIR/server_status/`hostname`_`date +%Y%m%d_%H-%M-%S`.txt

# SophosXG Config Backup
find $SOURCE_DIR -type f -mmin -60 -exec scp '{}' $TARGET_USER@$TARGET_HOST:$DEST_DIR ';'

```

## 監視サーバ(Zabbix)

### 仮想マシン設定情報

項目	設定値
仮想マシン名	[MAIN]monkey2018.k636174.net
インストールOS	Debian GNU/Linux 9.5 (stretch)
コア数	4コア
メモリ	2046MB
アタッチネットワーク	DMZ
アタッチネットワーク2	LAN
ディスク	500GB(スパース)
主な用途	ZabbixServer,SyslogServer

### OS設定値

項目	設定値
ホスト名	monkey2018.k636174.net
IPアドレス	172.16.16.105

### Cron設定状況

実行日時（間隔）	実行するコマンド
-	-

### 稼働サービス

サービス名	バージョン	自動起動
SSH	7.4p1	yes
rsyslogd	8.24.0	yes
zabbix_server	4.0.0	yes
zabbix_agent	4.0.0	yes



## ZabbixServer設定

### アクション

設定値	項目
Name	[MASTER]ZabbixCollector
実行条件	ラベル：A 名前：トリガーの深刻度 以上 未分類
有効	Checked
デフォルトのアクション実行ステップの間隔	5m
ステップ	1-0(無限)
コマンド	curl -F "hostname={HOST.NAME}" -F "ip={HOST.IP}" -F "status={EVENT.STATUS}" -F "trigger_name={EVENT.NAME}" -F "trigger_severity={EVENT.SEVERITY}" -F "item_key={ITEM.KEY}" -F "item_val={ITEM.VALUE}" -F "event_id={EVENT.ID}" -F "trigger_url={TRIGGER.URL}" <a href="http://172.16.16.99/zabbix-collector/api/alerts">http://172.16.16.99/zabbix-collector/api/alerts</a>