監視アラート対応手順書(FOR LINUX)

【ポート監視アラート対応手順】

Version.1.0

株式会社クララオンライン

2014/07/16

更新履歴

改定日	版	改定者	改定内容
2014/7/16	1.0	クララオンライン	新規作成

CONFIDENTIAL

目次

はじめに

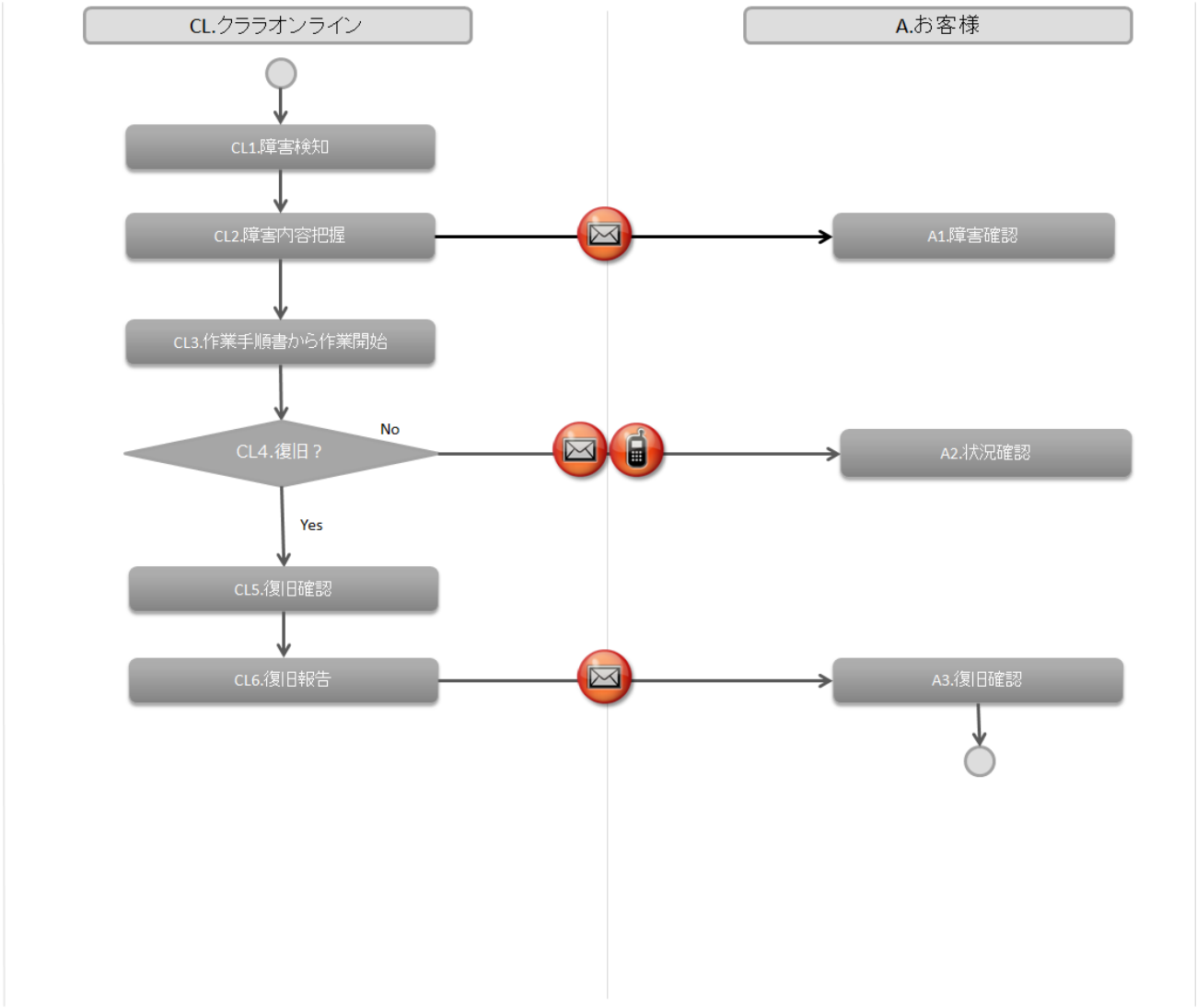
Linux 向けシステムのアラートが発生した際の操作手順を記載致します。

1. 監視項目

1.1. 監視一覧(基本内容)

監視概要	監視項目	監視閾値	監視間隔/リトライ/試行回数	対応手順
ポート監視	22	LISTEN 状態	5 分/1 分/3 回	手順へ
	21			手順へ
	80			手順へ
	443			手順へ
	53			手順へ
	25			手順へ
	110			手順へ
	8443			手順へ

2. アラート起点の対応フロー



3. お客様へのご連絡

障害検知時即時連絡	メール連絡致します。
復旧時報告	メール報告致します。
記録	メール報告致します。

※手順書通りの対応にて復旧出来ない場合は、電話連絡を行います。

4. 障害時連絡レベル

4.1. 障害と連絡方法

連絡レベル	レベル内容	連絡方法
1	手順書通りの対応にて復旧	メール連絡致します。
2	手順書通りの対応に復旧不可	電話連絡(連絡先一覧記載連絡先)、メール連絡致します。

4.2. 電話連絡方法

連絡先	予め指定された電話番号へ連絡を行います。
連絡回数	予め指定された電話番号に連絡が取れない場合、連絡順序通りに 2 周連絡を行います。 予め指定された電話番号へ 2 周しても連絡が取れない場合、メールにて状況報告を行うのみと致します。
留守電	予め指定された電話番号に連絡して、留守電に切り替わった場合、留守電に「3.3 連絡内容」を報告致します。

4.3. 連絡内容

①	障害発生(検知)時間
②	対象ホスト名
③	対象 IP アドレス
④	検知内容
⑤	現象と対応内容
⑥	サービス影響

4.4. メール連絡時の本文内容(テンプレート)

クララオンライン
障害受付センターでございます。

下記のとおり弊社の監視システムによる発報がございましたので、
報告致します。

■対象 ホスト名 ：
■対象 IP アドレス ：
■発報時間 ：yyyy 年 mm 月 dd 日 HH 時 MM 分
■復旧時間 ：yyyy 年 mm 月 dd 日 HH 時 MM 分
■発報内容 ：<例：port_HTTP_DHIT>
■対応内容 ： 対応前連絡では空欄、対応後は内容を記載
<例 httpd 再起動>>

---

5. ポート監視アラート対応手順

5.1. 22 番ポートアラート

1.以下の項目での確認結果で OK とならない場合は、「2」へ進みます。
・ssh 接続不可
※ログイン可能な場合は、以下手順にて確認致します。
#netstat -nltup
以下の状況である事を確認致します。

```
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN      -
```

※上記 1 で問題がなく、なお且つリカバリーメールを確認した場合、以下手順には進まず、連絡(メール)のみと致します。

2.コンソールによる sshd 再起動
IPMI からコンソールログイン致します。
 # /etc/init.d/sshd restart

3.sshd 再起動後、上記 1 の手順にて、ポート状態を確認致します。
3-1.ポート状態が正常の場合、メールにて復旧連絡を行います。
3-2.ポート状態が異常の場合、電話及びメールにて状況報告を行います。

※IPMI 接続出来ない場合、現地対応致します。

備考	

5.2. 21 番ポートアラート

1.以下の項目での確認結果で OK とならない場合は、「2」へ進みます。
・ssh 接続不可
※ログイン可能な場合は、以下手順にて確認致します。
#netstat -nltup
以下の状況である事を確認致します。

```
tcp        0      0 0.0.0.0:21                  0.0.0.0:*                   LISTEN      -
```

※上記 1 で問題がなく、なお且つリカバリーメールを確認した場合、以下手順には進まず、連絡(メール)のみと致します。

2.ftp のパッケージ確認
 # rpm –qa | grep ftp

3.リモートログインし、FTP 再起動
3-1. vsftpd 再起動
 # /etc/init.d/vsftpd start
3-2.xined の場合
 # /etc/init.d/xinetd restart

4.FTP 再起動後、上記 1 の手順にて、ポート状態を確認致します。
4-1.ポート状態が正常の場合、メールにて復旧連絡を行います。
4-2.ポート状態が異常の場合、電話及びメールにて状況報告を行います。

※IPMI 接続出来ない場合、現地対応を致します。

備考	

5.3. 80 番/443 番ポートアラート

1.状態確認 **＃netstat –nltup** **以下の状況である事を確認致します。** **tcp 0 0 0.0.0.0:80(443) 0.0.0.0:* LISTEN -** **2.ブラウザよりページ確認** **http://IP アドレス/** **※上記 1 及び 2 で問題がなく、なお且つリカバリーメールを確認した場合、以下手順には進まず、連絡(メール)のみと致します。** **3.リモートログインし、apache 再起動** **# /etc/init.d/httpd restart** **4. apache 再起動後、上記 1 及び 2 の手順にて、ポート状態を確認致します。** **4-1.ポート状態が正常及びブラウザからのページ確認が正常の場合、メールにて復旧連絡を行います。** **4-2.ポート状態若しくはブラウザの確認にて異常の場合、電話及びメールにて状況報告を行います。**
備考

5.4. 53 番ポートアラート

1.状態確認 **＃netstat –nltup** **以下の状況である事を確認致します。** **tcp 0 0 0.0.0.0:53 0.0.0.0:* LISTEN -** **2.リモートログインし、named 再起動** **# /etc/init.d/named restart** **3.named 再起動後、上記 1 の手順にて、ポート状態を確認** **3-1.ポート状態が正常の場合、メールにて復旧連絡を行います。** **3-2.ポート状態が異常の場合、電話及びメールにて状況報告を行います。**
備考

5.5. 25 番ポートアラート

1.状態確認
＃netstat –nltup
以下の状況である事を確認致します。

```
tcp        0      0 0.0.0.0:25                  0.0.0.0:*                   LISTEN      -
```

※上記 1 で問題がなく、なお且つリカバリーメールを確認した場合、以下手順には進まず、連絡(メール及び電話)のみと致します。

2.現在利用している MTA の確認
 # alternative –display mta

3.リモートログインし、MTA の再起動を行います。
3-1.postfix 再起動
 # /etc/init.d/postfix start
3-2.sendmail の場合
 # /etc/init.d/sendmail restart
3-3.qmail の場合
 # /etc/init.d/qmail restart

4.MTA 再起動後、上記 1 の手順にて、ポート状態を確認
3-1.ポート状態が正常の場合、メールにて復旧連絡を行います。
3-2.ポート状態が異常の場合、電話及びメールにて状況報告を行います。

備考	

5.6. 110 番ポートアラート

1.状態確認
＃netstat –nltup
以下の状況である事を確認致します。

```
tcp        0      0 0.0.0.0:110                 0.0.0.0:*                   LISTEN      -
```

※上記 1 で問題がなく、なお且つリカバリーメールを確認した場合、以下手順には進まず、連絡(メール及び電話)のみと致します。

2.リモートログインし、dovecot の再起動を行います。
 # /etc/init.d/dovecot restart

3.MTA 再起動後、上記 1 の手順にて、ポート状態を確認
3-1.ポート状態が正常の場合、メールにて復旧連絡を行います。
3-2.ポート状態が異常の場合、電話及びメールにて状況報告を行い対応協議致します。

備考	

5.7. 8443 番ポートアラート

1.状態確認
＃netstat –nltup
以下の状況である事を確認致します。

tcp	**0**	**0**	**0.0.0.0:8443**	**0.0.0.0:***	**LISTEN**	**-**

※上記 1 で問題がなく、なお且つリカバリーメールを確認した場合、以下手順には進まず、連絡(メール及び電話)のみと致します。

2.リモートログインし、plesk 再起動を行います。
 # /etc/init.d/psa start

3.plesk 再起動後、上記 1 の手順にて、ポート状態を確認
3-1.ポート状態が正常の場合、メールにて復旧連絡を行います。
3-2.ポート状態が異常の場合、電話及びメールにて状況報告を行います。

備考	