SECCON
インフラ検討／構築／運用

2013/1/29

SECCON 2013 実行委員
宮本 久仁男

宮本の担当

SECCON インフラ

主に
ネットワーク

ときどき
クラウド運用

一番の
大仕事は…

SECCON

予選で使う
ネットワーク
設計と構築

制約条件1
構成の
安定性

制約条件2
機器の
調達容易性

制約条件3
機器の
経済性

制約条件4
機器の
可換性

制約条件5
操作の
容易性

制約条件6

有線

ネットワーク構成の基本：2012年度決勝で使ったネットワーク

選んだもの1

コアルータ

RTX1200

理由：

ファームが枯れている

&高性能
&まぁ安価

選んだもの２
エッジルータ
BBR-4MG/HG

理由：
ロングセラー
＆性能そこそこ

&どこでも
入手可能
&安価

使う数：コアルータ1

&エッジルータ
たくさん
（チーム数分）

＋スペア

（壊れたら繋ぎ直すだけ状態）


SECCON
Broad Station
4
SECCON
Broad Station
22
SECCON
Broad Station
6
SECCON
Broad Station
1
SECCON
Broad Station
17
SECCON
3

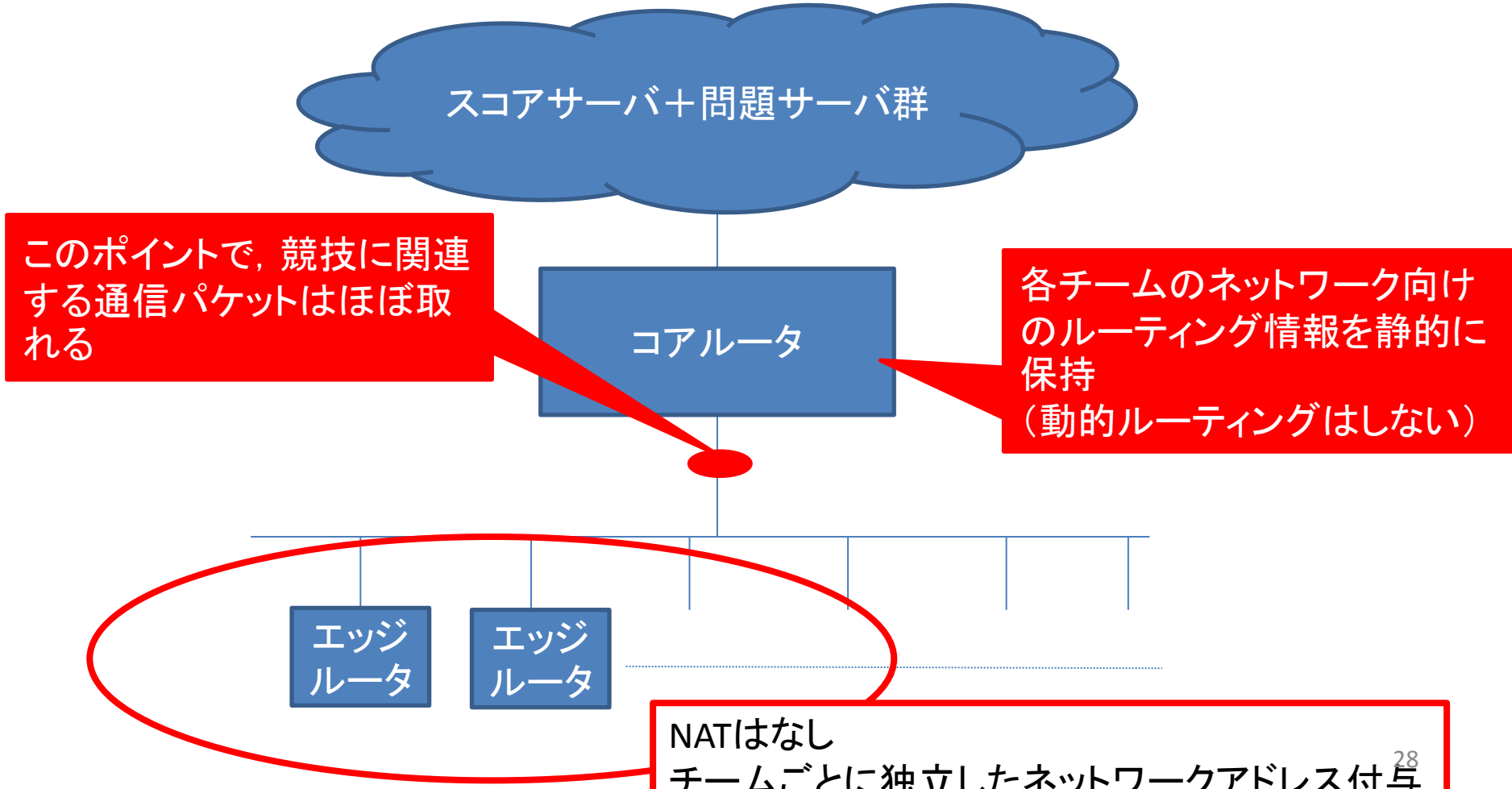
これらを
地方大会2回分
準備した

あとは
ミラーポート使える
スイッチとか

SECCON

結果：
つなぐだけで
CTFネットワーク
完成

基本構成


スコアサーバ＋問題サーバ群
このポイントで，競技に関連する通信パケットはほぼ取れる
コアルータ
各チームのネットワーク向けのルーティング情報を静的に保持
（動的ルーティングはしない）
エッジルータ
エッジルータ
NATはなし
チームごとに独立したネットワークアドレス付与

トラブル時：
機器交換で対応
（実績あり）

SECCON

オンライン予選

…

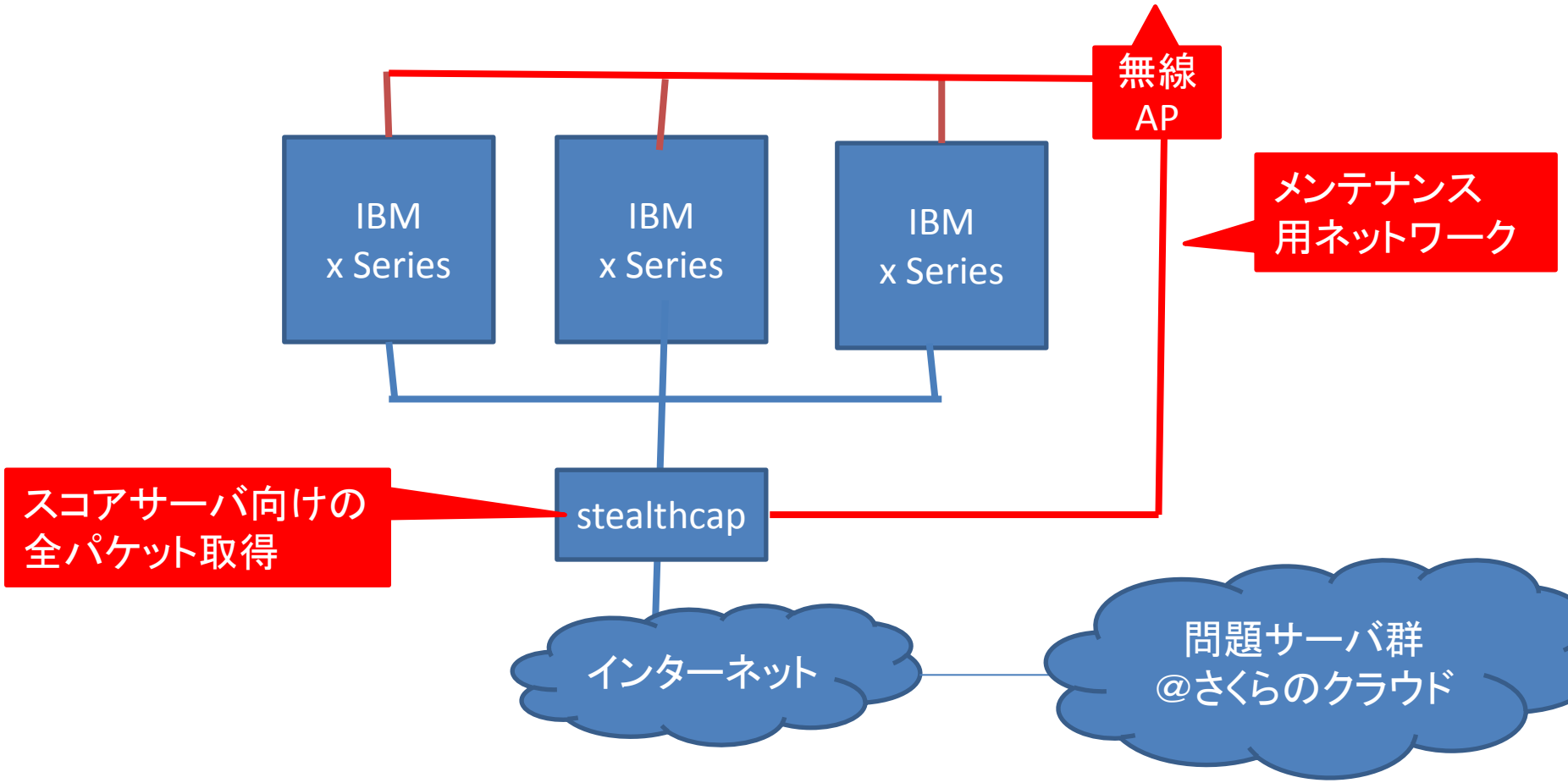
地方予選と全然違うw

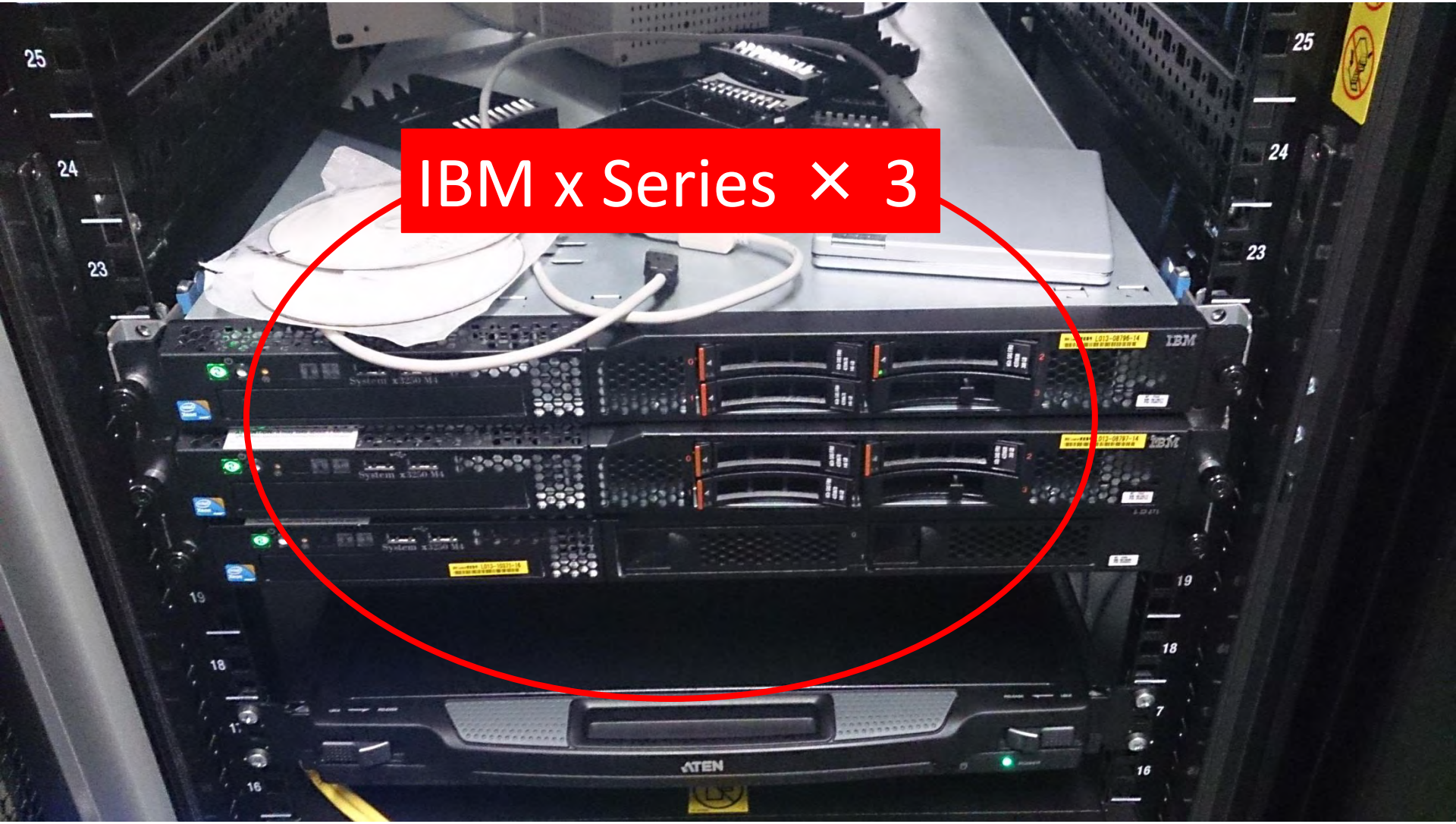
サーバ
（IBM x Series）
＋クラウド
（さくらのクラウド）

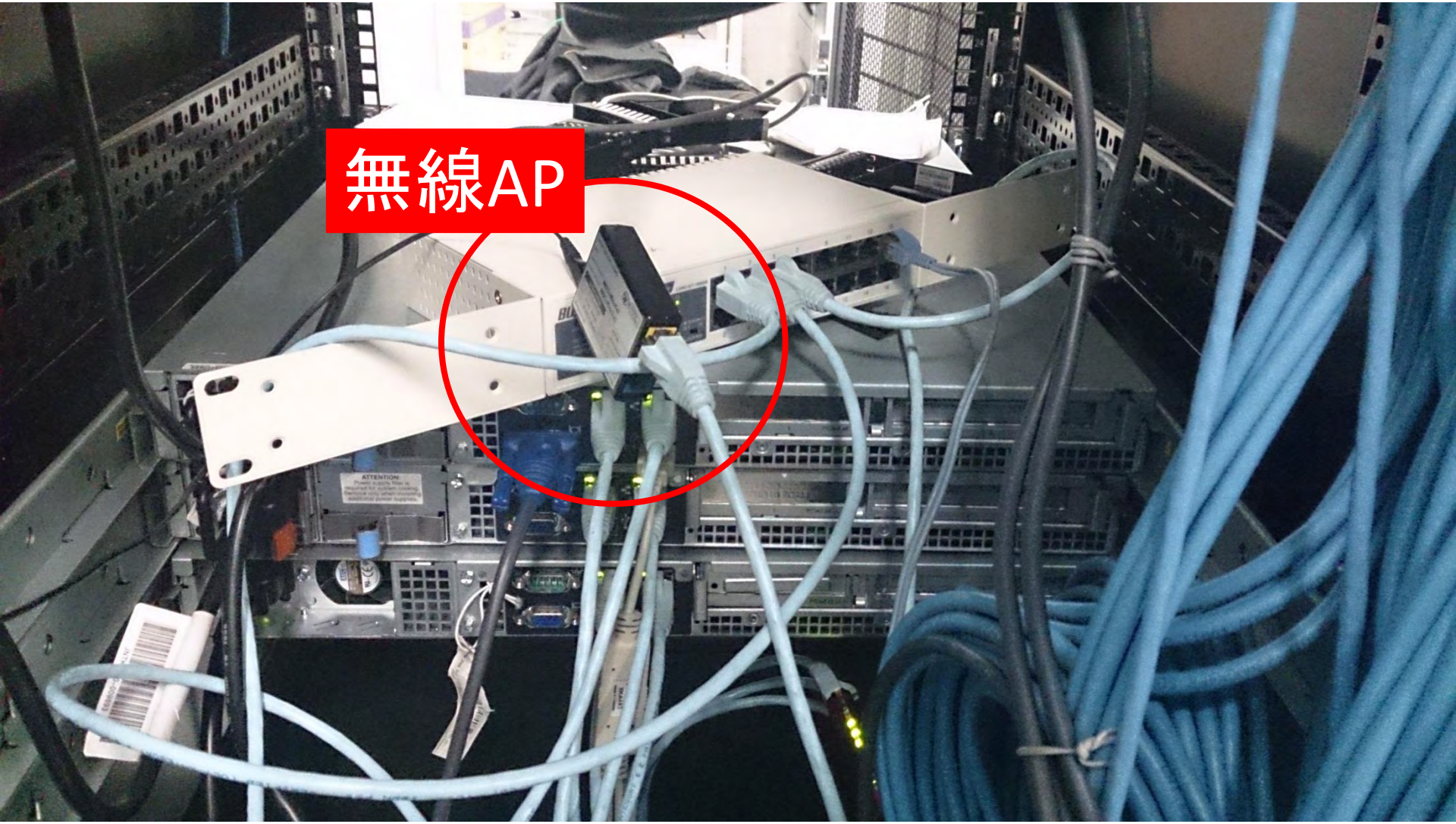
SECCON

＋ネットワーク
＋ラックスペース
（IISECの場所借用）

基本構成


無線
AP
メンテナンス
用ネットワーク
IBM
x Series
IBM
x Series
IBM
x Series
スコアサーバ向けの
全パケット取得
stealthcap
インターネット
問題サーバ群
@さくらのクラウド


IBM x Series × 3

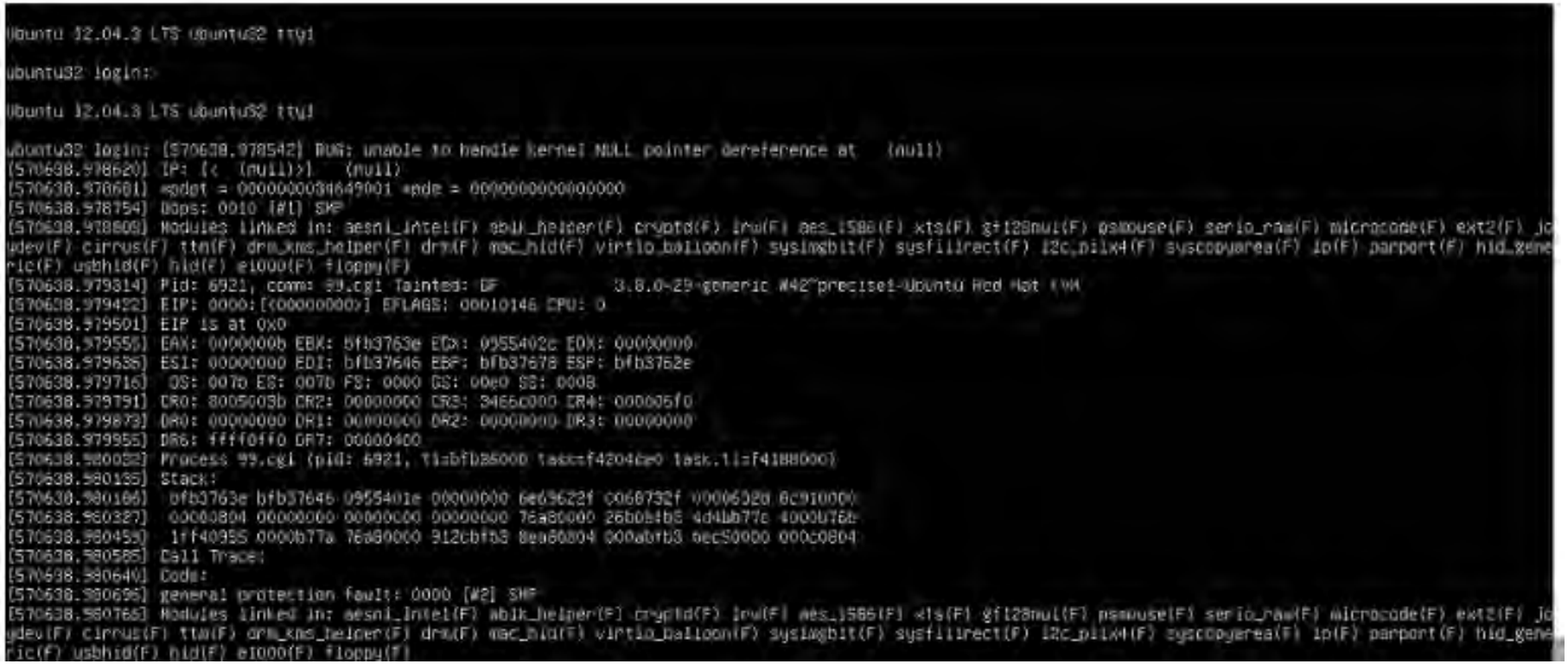

無線AP


stealthcap
Shuttle
スコアサーバへの通信情報が
バリバリたまります

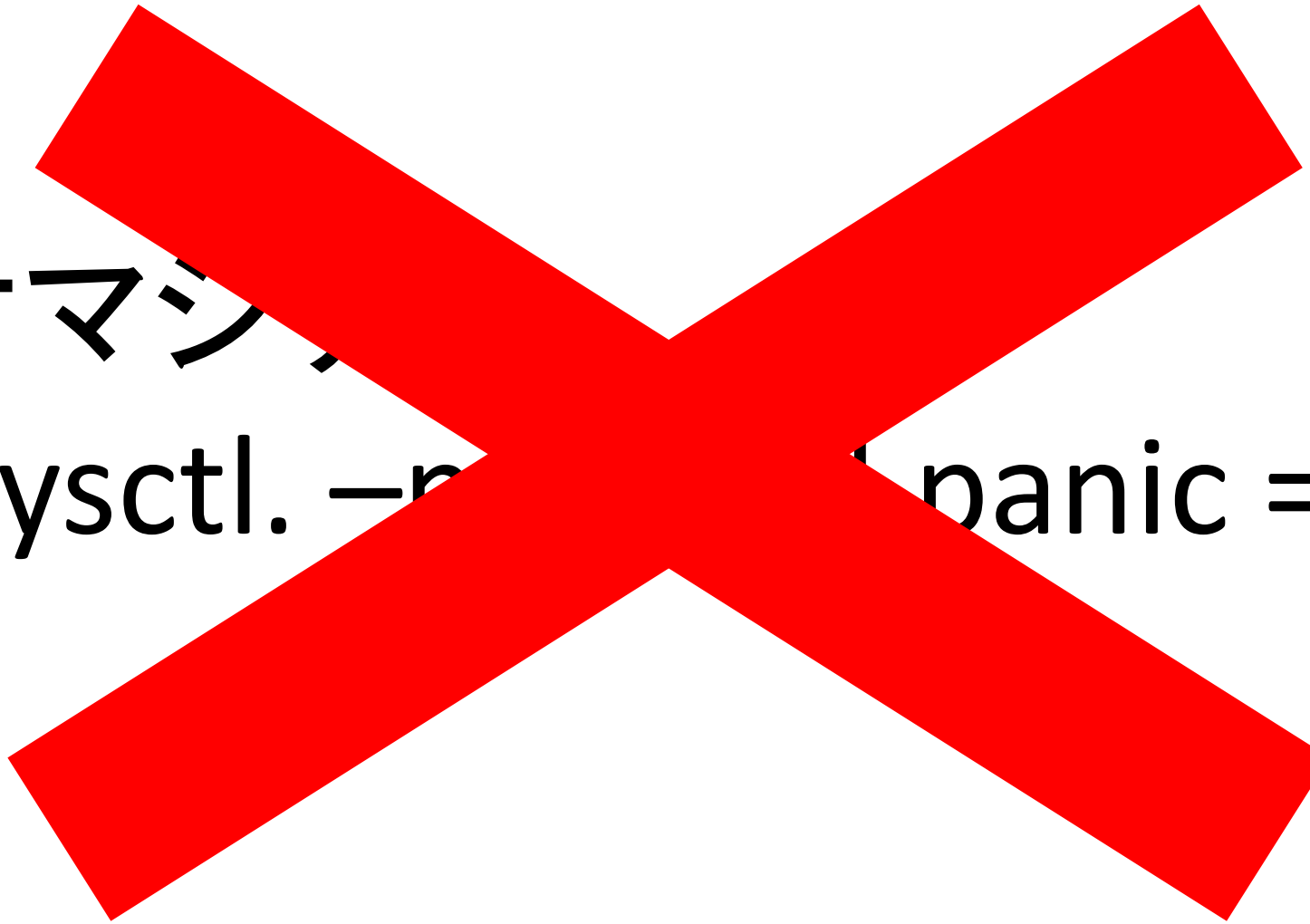

Shuttle
Shuttle
競技終了時に
一旦ネットワーク抜去

トラブル：クラウドのインスタンスが不調になるなど

画面の例


Ubuntu 12.04.3 LTS ubuntu32 tty1
ubuntu32 login:
Ubuntu 12.04.3 LTS ubuntu32 tty1
ubuntu32 login: [570638.978542] BUG: unable to handle kernel NULL pointer dereference at (null)
[570638.978620] IP: [< (null)>] (null)
[570638.978681] *pdpt = 0000000036649001 *pde = 0000000000000000
[570638.978754] Oops: 0010 [#1] SMP
[570638.978809] Modules linked in: aesni_intel(F) ablk_helper(F) cryptd(F) lrw(F) aes_i586(F) xts(F) gf128mul(F) psmouse(F) serio_raw(F) microcode(F) ext2(F) jo
udev(F) cirrus(F) ttm(F) drm_kms_helper(F) drm(F) mac_hid(F) virtio_balloon(F) sysimgblt(F) sysfillrect(F) i2c_piix4(F) syscopyarea(F) ip(F) parport(F) hid_gene
ric(F) usbhid(F) hid(F) e1000(F) floppy(F)
[570638.979314] Pid: 6921, comm: 99.cgi Tainted: GF 3.8.0-29-generic #42~precise1-Ubuntu Red Hat KVM
[570638.979422] EIP: 0000:[<00000000>] EFLAGS: 00010146 CPU: 0
[570638.979501] EIP is at 0x0
[570638.979555] EAX: 0000000b EBX: bfb3763e ECX: 0955402c EDX: 00000000
[570638.979636] ESI: 00000000 EDI: bfb37646 EBP: bfb37678 ESP: bfb3762e
[570638.979716] DS: 007b ES: 007b FS: 0000 GS: 00e0 SS: 0068
[570638.979791] CR0: 8005003b CR2: 00000000 CR3: 3466c000 CR4: 000006f0
[570638.979873] DR0: 00000000 DR1: 00000000 DR2: 00000000 DR3: 00000000
[570638.979955] DR6: ffff0ff0 DR7: 00000400
[570638.980032] Process 99.cgi (pid: 6921, ti=bfb36000 task=cf4204e0 task.ti=cf418000)
[570638.980135] Stack:
[570638.980186] bfb3763e bfb37646 0955401e 00000000 6e69622f 00687320 8c910000
[570638.980327] 00000804 00000000 00000000 00000000 76a80000 26b0b4b8 4d4bb77c 4000b78c
[570638.980458] 1ff40385 0000b77a 76a80000 912cbf53 08a80804 000abfb3 aec50000 000c0804
[570638.980585] Call Trace:
[570638.980640] Code:
[570638.980696] general protection fault: 0000 [#2] SMP
[570638.980765] Modules linked in: aesni_intel(F) ablk_helper(F) cryptd(F) lrw(F) aes_i586(F) xts(F) gf128mul(F) psmouse(F) serio_raw(F) microcode(F) ext2(F) jo
udev(F) cirrus(F) ttm(F) drm_kms_helper(F) drm(F) mac_hid(F) virtio_balloon(F) sysimgblt(F) sysfillrect(F) i2c_piix4(F) syscopyarea(F) ip(F) parport(F) hid_gene
ric(F) usbhid(F) hid(F) e1000(F) floppy(F)

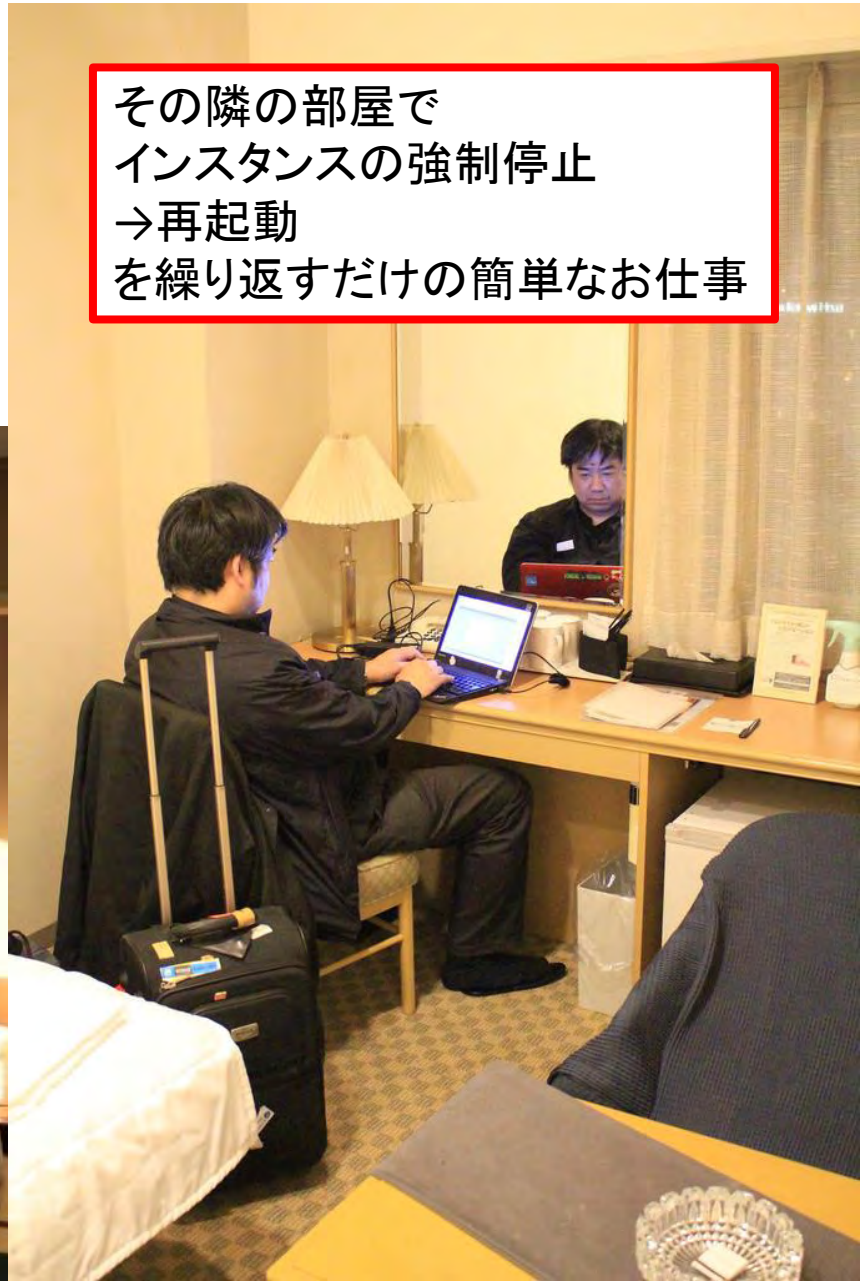

CPU負荷が急上昇→さまざまな症状が発生
・割込多発
・カーネルパニック
・無応答
CPU TIME
msec
1000
500
0
12:00
14:00
16:00
18:00
20:00
22:00
26Jan
02:00
04:00
06:00
08:00
10:00
NIC: #0
Send
Receive
Kbps
10000
5000
ディスク: #1 aikoさんむけ (Ubuntu+32bit)
Write
Read
こうなると「強制終了→起動」とするしかない



オマジ

“sysctl. –n panic = 5”

現地スタッフの宿泊部屋



その隣の部屋で
インスタンスの強制停止
→再起動
を繰り返すだけの簡単なお仕事

2013全国大会

…現在検討中

Thank you!