NVC

mailログの確認方法

Mail Logs

メールログ内の識別子

ICID　: Injection Connection ID(受信接続ID)

システムと個々のSMTP接続の識別子

DCID : Delivery Connection ID(送信接続ID)

送信のため他のサーバーとの個々の接続識別子

MID　: Message ID(メッセージID)

メッセージを追跡するために使用する

RID　: Recipient ID(受信者ID)

各メッセージ受信者に割当てられる識別子

Mailの流れとログの関係

1. *SMTP接続が発生*

Ironport内処理

ICID

MID

RID

受信者多数の場合は
RIDが増えます

この段階でIronport内の配送キューに書き込まれます

配送キューから配送されます

2. *配送先MTA*

DCID

クライアントの状態とIronportのログの関係

SMTPクライアント	Ironportのログ
[mechy3@mail mechy3]$ telnet 172.16.27.2 25 Trying 172.16.27.2... Connected to 172.16.27.2 (172.16.27.2). Escape character is '^]'. 220 ironport.test ESMTP	Wed Jan 30 11:31:28 2008 Info: New SMTP ICID 1002674 interface Data 2 (172.16.27.2) address 172.16.27.3 reverse dns host unknown verified no Wed Jan 30 11:31:28 2008 Info: ICID 1002674 RELAY SG RELAYLIST match 172.16.27.3 SBRS rfc1918 SMTP接続が発生した段階で送信者評価が入り、問題ない場合はICIDが発行されます
HELO <technvc.com> 250 ironport.test MAIL FROM:<mechy3@technvc.com> 250 sender <mechy3@technvc.com> ok	Wed Jan 30 11:32:52 2008 Info: MID 1536772 ICID 1002674 From: <mechy3@technvc.com> MAIL FROMコマンドの後でMIDが発行されます
RCPT TO:<hsumida@nvc.co.jp> 250 recipient <hsumida@nvc.co.jp> ok	Wed Jan 30 11:33:54 2008 Info: MID 1536772 ICID 1002674 RID 0 To: <hsumida@nvc.co.jp> PCPTコマンドの後で RIDが発行されます

NVC

クライアントの状態とIronportのログの関係2

DATA
354 go ahead

test123
test456
.
250 ok: Message 1536772 accepted

ピリオドでアンチスパムスキャンが入り、キューに書かれ配送待ちになります

その後DCIDを発行し、配送を開始

221 ironport.test
Connection closed by foreign host.

```
Wed Jan 30 11:35:57 2008 Info: MID 1536772 Message-ID '<6ki453$1eso4@ironport.test>'
Wed Jan 30 11:35:57 2008 Info: MID 1536772 ready 137 bytes from <mechy3@technvc.com>
Wed Jan 30 11:35:57 2008 Info: MID 1536772 matched all recipients for per-recipient policy 1 in the outbound table
Wed Jan 30 11:35:57 2008 Info: MID 1536772 interim verdict using engine: CASE spam negative
Wed Jan 30 11:35:57 2008 Info: MID 1536772 using engine: CASE spam negative
Wed Jan 30 11:35:57 2008 Info: MID 1536772 interim AV verdict using Sophos CLEAN
Wed Jan 30 11:35:57 2008 Info: MID 1536772 antivirus negative
Wed Jan 30 11:35:57 2008 Info: MID 1536772 queued for delivery
Wed Jan 30 11:35:57 2008 Info: New SMTP DCID 125285 interface 122.212.247.186 address 210.255.80.238 port 25
Wed Jan 30 11:35:57 2008 Info: Delivery start DCID 125285 MID 1536772 to RID [0]
Wed Jan 30 11:35:58 2008 Info: Message done DCID 125285 MID 1536772 to RID [0]
Wed Jan 30 11:35:58 2008 Info: MID 1536772 RID [0] Response 'ok:  Message 6065881 accepted'
Wed Jan 30 11:35:58 2008 Info: Message finished MID 1536772 done
Wed Jan 30 11:36:03 2008 Info: DCID 125285 close
```

配送完了

quit
221 ironport.test

Connection closed by foreign host.

```
Wed Jan 30 11:38:17 2008 Info: ICID 1002674 close
```

quitコマンドの受理に伴いICIDがcloseされます

今回はtelnetでの確認ですが、通常は送信後にquitが発行されますので、ICIDの記録はDCICの前に記録されます