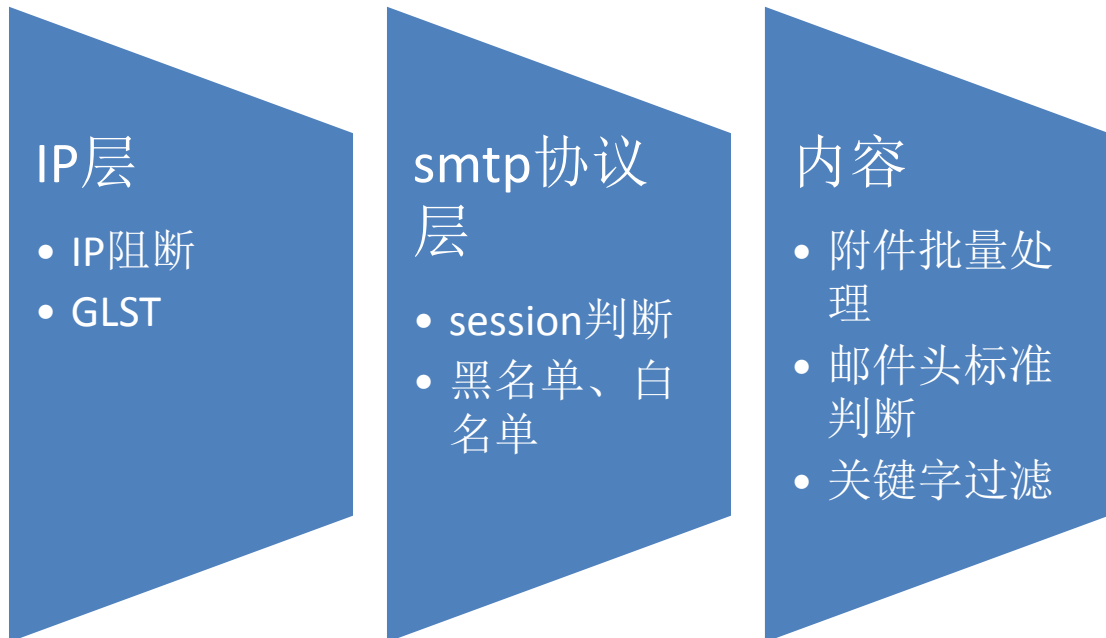


JDMail V3.10 反垃圾邮件技术一览

对付垃圾邮件，只有用综合各种技术手段，在 IP 层、协议层、内容层，综合防治，才能取得比较好的效果。



JDMail V3.10 在 IP 层用到 IP 阻断技术，IP 并发连接限制，IP 发送频率限制技术；在协议层用到 MAIL From /RCPT TO 黑名单、白名单技术；在内容层，用到关键字过滤技术。此外还用到 GLST（灰名单）和 S25R 技术，这 2 个技术对付垃圾邮件很有效果。

具体功能如下：

- 垃圾邮件发送者的 IP 地址管理：为防止垃圾邮件，对垃圾邮件发送者进行 IP 级的限制。
- 垃圾邮件地址管理：登记垃圾邮件发送者地址(SMTP session 的 MAIL FROM:)。
- 垃圾邮件发送者管理 2(S25R 检查)：为防止垃圾邮件，拒绝来自最终用户 PC 的连接。
- GLST 的管理：GLST 灰名单，是一个实用的反垃圾邮件工具。
- 垃圾邮件关键字管理：监控发送接收邮件的邮件头（header）和正文，进行垃圾邮件处理。
- 垃圾邮件文件夹的管理(垃圾邮件的管理)：[垃圾邮件发送者管理 2(S25R 检查)]和 [垃圾邮件的管理] 管理您的每个邮件帐户被过滤的垃圾邮件文件夹。

反垃圾邮件

垃圾邮件发送者 IP 管理

反垃圾邮件

菜单

垃圾邮件发送者IP管理

为防垃圾邮件，对发送者进行IP地址级别的访问限制。

序号	IP地址	子网掩码	选项	备注	处理
1	220.117.94.130	255.255.255.0	立刻拒绝		编辑 删除

添加一个新的定义

IP地址: . . .

子网掩码: . . .

添加位置: 末尾

选项
(请选择匹配主机对应的定义):
☒ 如果SMTP认证成功, 就从垃圾邮件发送者排除。
☐ 在会话开始无条件地断开。
☐ 在SMTP指令间插入 秒的Session许可的延迟。

备注(空白可):

添加

为防垃圾邮件，对发送者进行 IP 地址级别的访问限制。



不适用于[SMTP 白名单的管理]定义的主机。
垃圾邮件主机的检查按顺序执行，匹配后结束检查。
设置信息保存在 `spammers.tab` 。

■ 示例 1

收到的垃圾邮件来自网段 210.196.149.0/24 。

210.196.149.0	255.255.255.0	直接拒绝
---------------	---------------	------

■ 示例 2

收到垃圾邮件来自 210.255.58.145 。

210.196.149.0	255.255.255.0	直接拒绝
210.255.58.145	255.255.255.255	直接拒绝

■ 示例 3

垃圾邮件自动发送程序的对策，SMTP 连接插入 30 秒的延迟。

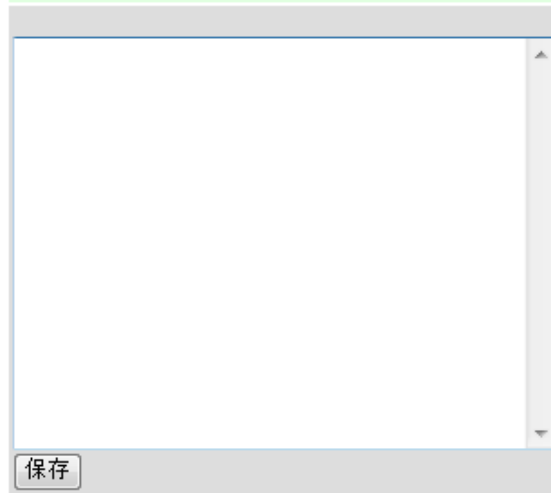
0.0.0.0	0.0.0.0	30 秒的延迟插入
---------	---------	-----------

SPAM 对策 [安全性]-[垃圾邮件地址的管理]，[安全性]-[垃圾邮件的管理] 另外，[环境配置]-[JDWA 环境配置]的[SMTP 接收限制]也能使用。

垃圾邮件地址的管理

登记/删除垃圾邮件发送者的地址(SMTP session时的MAIL FROM:)。jdmail拒绝接收来自这里被登记了的地址。

■请每行指定电子邮件的完整地址或部分地址。



登记/删除垃圾邮件发送者的地址(SMTP session时的MAIL FROM:)。jdmail拒绝接收在这里登记了的地址。

本功能不是检查邮件header的From:地址。MAIL FROM:地址和From:地址不一定相符。请使用[垃圾邮件关键字的管理]根据邮件的内容拒绝接收。

地址的域名前面的@(at)是必须的。

地址可使用(*)通配符。如果要拒绝来自个别的用户和邮件列表特定地址的邮件,请使用[用户的管理]或[邮件列表的管理]的[接收拒绝]菜单。

设定信息保存在spam-address.tab。

SPAM 对策 [安全性]-[垃圾邮件主机的管理], [安全性]-[垃圾邮件消息的管理]另外, [环境配置]-[JDWA 环境配置]的[SMTP 接收限制]也能使用。

(S25R
检查) -
基本设置

 ● 反垃圾邮件

● 菜单

垃圾邮件发送者管理2(S25R检查) - 基本设置

[基本设定](#) | [白名单](#) | [黑名单2](#) | [黑名单](#) | [垃圾邮件记录](#)

监测连接主机的IP地址或反向的FQDN (Fully Qualified Domain Name)，判断是最终用户的PC从而拒绝连接。

■ DNS测试

S25R使用原始访问获取主机的域名，然后做DNS检查
(Domain Name System)。如果他的DNS不能用，运行S25R检查可能会损害Jmail的关键操作。要确定是否可以正确使用DNS，可以通过smtp.sina.com.cn的正向查询(查询IP地址)，从那个结果再进行反向查询，查询结果在右边表示。确实不能获取查询结果的情况下，不应该实行S25R检查。

正向查询结果	202.108.3.190 如果显示IP地址表示OK
反向查询结果	mail13-190.sinamail.sina.com.cn 如果显示***sinamail.sina.com.cn表示OK

■ 过滤的执行

☒ 执行过滤。(※1)

■ 过滤的类型

☒ SMTP RCPT 后实行过滤处理。(※2)
☐ SMTP DATA 后实行过滤处理。(※2)

■ 过滤详细信息

☒ 不能得到DNS反向查询结果的连接拒绝。(※3)
☒ 查询白名单。(※5)
☒ 查询黑名单。(※5)
☐ 记录被拒绝的连接。(※6)

■ 过滤的基本条件(拒绝对象 FQDN 或 IP 正则表达式)(※7)

```
[^.]*[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$  
[^\[\]]*[0-9]{1,3}$  
([^\[\]]*\.[^\[\]]*)?([0-9]{1,3}\.)*\.[^\[\]]*\.[^\[\]]*$  
[^\[\]]*[0-9]{1,3}\.([^\[\]]*[0-9]{1,3})$  
[^\[\]]*[0-9]{1,3}\.([^\[\]]*[0-9]{1,3})\.[^\[\]]*\.[^\[\]]*$  
(dhcp|dialup|ppp|[achrsvx]?dsl)[^\[\]]*[0-9]
```

■ 垃圾邮件判定后的对应方法 - 在 SMTP DATA 后处理的场合有效

☐ 立即断开，不保存邮件(※8)。
☒ 利用垃圾邮件文件夹功能能保存邮件后，断开连接(※9)。
☐ Subject:标记 (不可以用中文) 在邮件主题上打上标记(※10)。
☐ 邮件头扩展字段 邮件Header添加TAG标识(※11)。

■ 断开连接时SMTP响应代码和消息(※12)

和过滤基本条件匹配的主机应答如下。
451 Please try again later
不能进行DNS反向查询的主机应答如下。
451 Please try again later
主机在黑名单内的应答如下。
550 Connection not accepted due to spam

■ 设置垃圾邮件文件夹(※13) - 便于WEB管理

☐ 主题和正文都是空的不保存。
☒ 给非本地用户的邮件在以下位置保存。

☐ 给本地用户帐户的邮件在以下非垃圾邮件夹保存。

用户的 PC 从而拒绝连接。

S25R 使用原始访问获取主

机的域名，然后做 DNS 检查 (Domain Name System)。如果您的 DNS 不能用，运行 S25R 检查可能会损害 jdm ail 的关键操作。要确定是否可以正确使用 DNS，可以通过 smtp.sina.com.cn 的正向查询(查询 IP 地址)，从那个结果再进行反向查询，查询结果在右边表示。确实不能获取查询结果的情况下，不应该实行 S25R 检查。



关于： S25R (Selective SMTP Rejection)检查

S25R 检查是一种垃圾邮件过滤策略，简单地说，就是"接受来自邮件服务器的 SMTP 访问而拒绝来自 End User 的访问"。详细信息请参照以下说明。

» 根据国外研究报告，有效率可达 99%。
(<http://www.gabacho-net.jp/anti-spam/anti-spam-system.html>)

这个方法是对付垃圾邮件的一种强有力的对策。不过，在使用时需要注意。为了不拒绝正规的连接，请进行以下的工作。

如果可能请强制正规用户使用 SMTP 认证的连接。JDWA 对在 SMTP 认证上成功的连接不进行 S25R 检查。

请持续维护白名单和黑名单列表。特别是白名单的维护很重要。

为了 S25R 检查需要进行 DNS 的逆向查询, 在 DNS 不能使用的环境会对 JDMail 的服务造成延迟和障碍发生的可能性。为确保 DNS 没有问题, 请经常定期做检查。

S25R 检查用于反垃圾邮件, 可能会造成 "无法接收重要邮件" 的风险。请慎重使用。

为了实现 S25R 检查, 需要开启[过滤器的管理]-[过滤器的开/关] "SMTP RCPT 后处理过滤器(在线)", 或 "SMTP DATA 后处理过滤器(在线)"。如果对 DNS 反向解析没有充分的知识的情况下, 实行 S25R 检查的事不能贸然推进。

如果使用 ADSL 的用户访问了 JDMail, 有根据 S25R 检查被拒绝连接的可能性。这个情况, 让合法用户进行 SMTP 认证的连接或在白名单登记。

由于通过 SMTP 认证的 JDMail 用户的连接不进行 S25R 检查, 建议对本地合法用户只准许 SMTP 认证的连接。请在[环境配置]-[JDMail 环境配置]中把"许可(EnableAuthSMTP-POP3)"设为无效, 把"POP before SMTP"设为有效。

(*1) JDWA 的 S25R 检查顺序如下。

JDWA 的过滤器对 JDMail 的连接不是 SMTP 认证的情况, 开始对连接原主机进行 S25R 检查。

过滤器使用 `gethostbyaddr` 函数取得连接原主机的 FQDN。

过滤器判断如果与连接原主机的信息白名单的东西相符, 则判断是来自正规用户的连接。

过滤器判断如果与连接原主机的信息黑名单的东西相符, 则判断是来自垃圾邮件的连接。

过滤器最终地通过[过滤基本条件]和连接原主机的信息比较进行判断。

过滤器, 指示如果最终判断连接原主机是垃圾邮件发送主机, JDMail 是强行终止 SMTP 会话还是继续。强行终止的情况把邮件保存到垃圾邮件夹下, 继续后续处理则在邮件头部添加 SPAM 标识。

在 SMTP DATA 后进行 S25R 检查, 根据检查被判定为垃圾邮件, 将会在邮件头部 (message header) 添加详细信息。比如 "X-S25R-JDWA-Check:1; NonFQDN(x.x.x.x, RC:451)", "X-S25R-JDWA-Check:1; BlackList(x.x.x.x, RC:554, yy.yy.yy)", "X-S25R-JDWA-Check:1; DefaultRule(x.x.x.x, RC:451, yy.yy.yy)" 的信息被添加。(x.x.x.x: IP 地址, RC:451 应答编码, yy.yy.yy 是 DNS 反向解析结果)。分别表示"反向解析名没找到", "在黑名单内", "符合过滤条件"。

(*2) 选择 SMTP RCPT 后还是 SMTP DATA 后进行 S25R 检查。

SMTP RCPT 后处理的情况, 是在收到邮件数据(邮件头和邮件体)之前的处理, 对系统的负荷轻。

SMTP DATA 后处理的情况, 是在接收邮件数据后进行处理, 对系统的负荷重。

(*3) DNS 正常, 但是不能得到查询结果, (1) 继续试图连接 (2) DNS 设置有误,

一般是垃圾邮件的可能性比较大。

(*5) 为了灵活使用 S25R 检查，需要经常维护白名单和黑名单。可以查看[垃圾邮件日志(记录)]，如果发现有正常的连接请加入到白名单。如果有被判断为正常的非法连接请添加到黑名单。

(*6) 如果 JDMail 在短时间内有大量邮件访问，为减少系统负荷，建议暂时关闭 S25R 日志记录。

(*7) 垃圾邮件主机和判定的连接原主机的 FQDN 再以正则表达式指定 IP 地址。指定条件从前往后顺序匹配，最先相符条件的垃圾邮件处理被执行，条件的编辑需要正则表达式的知识。一般使用默认设置即可。

(*8) 如果判断是垃圾邮件主机的连接而强行终止连接，邮件不保存。这个情况，(1)SMTP 客户端不进行再次发送，(2)尝试重发。

(*9) 请参照关于垃圾邮件文件夹功能 (*12)。

(*10)(*11) 在 S25R 检查阶段不进行处理(连接切断)，想以后进行某种垃圾邮件处理的情况这个选择有效。如在 Subject:加上标记，[S25R-Spam]等。还可以在邮件头部增加 X-Spam-Host: Yes 标识。

(*12) 象以下的示例一样指定切断跟垃圾邮件主机连接的应答编码和应答消息。

451 Please try again later

550 Connection not accepted due to spam

554 Transaction failed

(什么都没指定的情况，JDMail 既定的应答编码(500)退回到垃圾邮件主机)

如果返回 451，有从同样的主机同样的邮件被再次发送的可能性。如果返回 500，被看做是致命的错误，没有再送的可能性。

(*13) 根据 S25R 检查被判定了实行垃圾邮件文件夹功能，垃圾邮件到达时，如果那个地址是本地用户，相应用户的邮箱内会创建 spam 这个邮件夹，并在那里保存。

这个功能 "SMTP DATA 后处理"开启才可能生效，需要从[过滤器的管理]菜单开启。如果"SMTP RCPT 后处理"进行 S25R 检查这个功能不能运行。
[JDWM 管理]-[环境设置]-[基本设置] "垃圾邮件文件夹功能的使用" 设置为 "许可" 。

设置信息保存在 spam-s25r-conf.tab、spam-r25r-def.tab(过滤基本条件)。

SPAM 对策在 [反垃圾邮件]菜单内的[垃圾邮件地址的管理]，[垃圾邮件主机的管理]，[垃圾邮件消息的管理]，[安全性]-[SMTP 连接数限制]等功能都可以使用。

垃圾邮件处理的记录通过本页的[垃圾邮件日志(记录)]能浏览。同时，[访问日志(记录)]-[过滤器处理的日志(记录)3(JDWA-S25R 检查)]也能查看。

垃圾邮件发送者管理 2
(S25R 检查) - 白名单

反垃圾邮件

菜单

垃圾邮件发送者管理2 (S25R检查) - 白名单

基本设定 | 白名单 | 白名单2 | 黑名单 | 垃圾邮件记录

S25R不检查登记的FQDN或IP地址。

白名单的定义

\.126\.com\$
\.163\.com\$

保存/更新

白名单是排除 S25R 检查所有匹配定义的主机。
持续地观察垃圾邮件 LOG 记录，如果正常连接被拒绝，请加 FQDN 或 IP 地址白名单。

通过 SMTP 认证使用邮件系统的用户不需要白名单登记。

定义可以使用正则表达式。
行尾 #后面可以加注释。

^ 匹配字符串开始。
\$ 匹配字符串末尾。
. 域名的分隔(点)前 用 ESC(\)转义必须的。
除此以外，[,], (,) 也请谨慎使用。

定义内容保存在 spam-s25r-wlist.tab 。

垃圾邮件
发送者管
理 2
(S25R
检 查) -
白名单 2

反垃圾邮件

菜单

垃圾邮件发送者管理2(S25R检查) - 白名单2

基本设定 | 白名单 | 白名单2 | 黑名单 | 垃圾邮件记录

登记不进行S25R检查的收件人地址(RCPT TO:或To:)。

白名单2的定义

保存/更新

登记不进行 S25R 检查的收件人地址(RCPT TO:或 To:)。

SMTP Session 的 RCPT TO: 指令的值或邮件头部的 To: 域的值和本定义匹配の場合, S25R 不进行检查。可以用在特定帐户有必要收取所有邮件的场合。此外, 对垃圾邮件策略有不满的本地用户, 也可以暂时停止过滤。

定义必须符合正则表达式。行尾 # 后面可以放入注释。

^ 匹配字符串开始。
\$ 匹配字符串末尾。
. 域名的分隔(点)前 用 ESC(\)转义必须的。
除此以外, [,], (,) 也请谨慎使用。

定义内容保存在 spam-s25r-wlist2.tab 。

垃圾邮件发送者管理 2 (S25R 检查) - 黑名单

反垃圾邮件

■ 菜单

垃圾邮件发送者管理2(S25R检查) - 黑名单

基本设定 | 白名单 | 白名单2 | 黑名单 | 垃圾邮件记录

登记的 FQDN 或 IP 地址无条件看作垃圾邮件发送者的连接。

■黑名单的定义

```
\. (internetdsl|adsl|sdi)\.tpnet\.pl$
~user.+\.mindspring\.com$
^[0-9a-f]{8}\. (.+\. )?virtua\.com\.br$
\.catv\.broadband\.hu$
[0-9a-f]{4}\. [a-z]+\.pppool\.de$
\.dip[0-9]+\.\t-ipconnect\.de$
\.dip\.\t-dialin\.net$
\.dyn\.optonline\.net$
\. (adsl|cable)\.wanadoo\.nl$
\.ipt\.aol\.com$
```

保存/更新

定义必须符合正则表达式。
行尾 # 后面可以加注释。

^ 匹配字符串开始。

\$ 匹配字符串末尾。

. 域名的分隔(点)前 用 ESC(\)转义必须的。

此外, [,], (,), {, }, -, |, *, ?, + 字符请谨慎使用。

定义内容保存在 spam-s25r-blist.tab 。

默认设置适合大多数情况, 一般无需改动。

垃圾邮件 LOG 记录 -S25R 检查

垃圾邮件LOG记录 - S25R检查							
No.	当地时间	远程IP	发件人地址	收件人地址	拒绝理由	远程FQDN	拒绝条件
#00001	2010/03/03 (星期三)	11:51:61.235.69.232	zhu@tvcf.org	hr@chundi.com	无效名称		
#00002	2010/03/03 (星期三)	11:51:88.96.115.118	miebkj@808-96-115-118.dsl.sen...	hr@chundi.com	基本条件匹配 88-96-115-118.dsl.sen.co.uk		'[.]'=[0-9]{'
#00003	2010/03/03 (星期三)	11:50:219.134.245.152	wodegong@699@126.com	hr@chundi.com	基本条件匹配 152.245.134.219.broad.s...		'[.]'=[0-9]{'
#00004	2010/03/03 (星期三)	11:49:123.89.138.211	zhanglei@hufosen.com	hr@chundi.com	无效名称		
#00005	2010/03/03 (星期三)	11:35:61.235.69.232	yxkucj@handevax.org	hr@chundi.com	无效名称		
#00006	2010/03/03 (星期三)	11:35:88.96.115.118	miebkj@808-96-115-118.dsl.sen...	hr@chundi.com	基本条件匹配 88-96-115-118.dsl.sen.co.uk		'[.]'=[0-9]{'
#00007	2010/03/03 (星期三)	11:28:61.235.69.232	dpaq@tpjjv.net	hr@chundi.com	无效名称		
#00008	2010/03/03 (星期三)	11:27:124.14.5.217	wang61522891@yahoo.com.cn	hr@chundi.com	无效名称		
#00009	2010/03/03 (星期三)	11:23:61.235.69.232	wxaxman@camcglu.org	hr@chundi.com	无效名称		
#00010	2010/03/03 (星期三)	11:19:113.111.115.158	huangmeijun@yuxin.cn	hr@chundi.com	无效名称		
#00011	2010/03/03 (星期三)	11:18:88.96.115.118	miebkj@808-96-115-118.dsl.sen...	hr@chundi.com	基本条件匹配 88-96-115-118.dsl.sen.co.uk		'[.]'=[0-9]{'
#00012	2010/03/03 (星期三)	11:14:113.65.251.208	xingshengren@xingshengren...	hr@chundi.com	无效名称		
#00013	2010/03/03 (星期三)	11:08:113.65.251.208	2010nianyingjiesheng@2010nian...	hr@chundi.com	无效名称		
#00014	2010/03/03 (星期三)	11:03:88.96.115.118	miebkj@808-96-115-118.dsl.sen...	hr@chundi.com	基本条件匹配 88-96-115-118.dsl.sen.co.uk		'[.]'=[0-9]{'
#00015	2010/03/03 (星期三)	11:01:113.111.115.158	huangmeijun@yuxin.cn	hr@chundi.com	无效名称		
#00016	2010/03/03 (星期三)	10:53:121.34.192.213	VVG@11.LL1188	hr@chundi.com	无效名称		
#00017	2010/03/03 (星期三)	10:51:222.129.33.87	771936@96062938859480.net	hr@chundi.com	无效名称		
#00018	2010/03/03 (星期三)	10:51:222.129.33.87	771936@96062938859480.net	hr@chundi.com	无效名称		
#00019	2010/03/03 (星期三)	10:49:112.93.34.17	filejv@jv@fjv@fjv@fjv@fjv...	hr@chundi.com	无效名称		
#00020	2010/03/03 (星期三)	10:48:58.47.25.120	gd@fhghghghghghghghghghghgh...	hr@chundi.com	无效名称		
#00021	2010/03/03 (星期三)	10:48:66.148.136.165	batkcm@bdev.com	hr@chundi.com	基本条件匹配 66.148.136.165.nv...		'[.]'=[0-9]{'
#00022	2010/03/03 (星期三)	10:46:88.96.115.118	miebkj@808-96-115-118.dsl.sen...	hr@chundi.com	基本条件匹配 88-96-115-118.dsl.sen.co.uk		'[.]'=[0-9]{'
#00023	2010/03/03 (星期三)	10:41:113.92.126.0	seel@shanghaiyouxi.cn	hr@chundi.com	无效名称		
#00024	2010/03/03 (星期三)	10:34:116.16.97.239	vjrf@werg.com	hr@chundi.com	无效名称		
#00025	2010/03/03 (星期三)	10:30:113.111.115.158	huangmeijun@yuxin.cn	hr@chundi.com	无效名称		
#00026	2010/03/03 (星期三)	10:29:88.96.115.118	miebkj@808-96-115-118.dsl.sen...	hr@chundi.com	基本条件匹配 88-96-115-118.dsl.sen.co.uk		'[.]'=[0-9]{'
#00027	2010/03/03 (星期三)	10:25:121.34.88.200	feetth@access-net.com	hr@chundi.com	无效名称		
#00028	2010/03/03 (星期三)	10:24:183.0.247.171	shp@shp@fz.org	hr@chundi.com	无效名称		
#00029	2010/03/03 (星期三)	10:23:61.235.69.232	soficq@anemoage.net	shenay@chundi.com	无效名称		
#00030	2010/03/03 (星期三)	10:18:119.39.194.207	tiguo@beiguangyi.com	hr@chundi.com	无效名称		
#00031	2010/03/03 (星期三)	10:16:61.235.69.232	ucyq@fcngshup.com	shenay@chundi.com	无效名称		
#00032	2010/03/03 (星期三)	10:15:61.235.69.232	peabw@ryellit.net	shenay@chundi.com	无效名称		
#00033	2010/03/03 (星期三)	10:14:88.96.115.118	miebkj@808-96-115-118.dsl.sen...	hr@chundi.com	基本条件匹配 88-96-115-118.dsl.sen.co.uk		'[.]'=[0-9]{'
#00034	2010/03/03 (星期三)	10:05:58.47.25.120	fjhfg@kjhghghghghghghghghghghgh...	hr@chundi.com	无效名称		
#00035	2010/03/03 (星期三)	10:04:183.3.225.11	dfh@fktullu@ghjuykhulvkhjkg.co...	hr@chundi.com	无效名称		
#00036	2010/03/03 (星期三)	09:59:61.235.69.232	yxh@jqacwi.org	shenay@chundi.com	无效名称		
#00037	2010/03/03 (星期三)	09:58:88.96.115.118	miebkj@808-96-115-118.dsl.sen...	hr@chundi.com	基本条件匹配 88-96-115-118.dsl.sen.co.uk		'[.]'=[0-9]{'
#00038	2010/03/03 (星期三)	09:49:113.65.251.208	xingshengren@xingshengren...	hr@chundi.com	无效名称		
#00039	2010/03/03 (星期三)	09:49:113.111.115.158	huangmeijun@yuxin.cn	hr@chundi.com	无效名称		
#00040	2010/03/03 (星期三)	09:42:88.96.115.118	miebkj@808-96-115-118.dsl.sen...	hr@chundi.com	基本条件匹配 88-96-115-118.dsl.sen.co.uk		'[.]'=[0-9]{'
#00041	2010/03/03 (星期三)	09:31:211.102.166.95	bashenwei@sina.com	hr@chundi.com	无效名称		

GLST 管理

反垃圾邮件

GLST的管理

GLST的管理

进行反垃圾邮件工具 GLST 的环境配置。更新内容将立刻生效。

重发要求消息(rejmsg)

451 4.7.1 Please try again later

初期收信拒绝继续时间(timeo)

300 (秒)

再送待机时间(lametimeo)

28800 (秒)

认证信息有效时间(exptimeo)

3110400 (秒)

白名单(xnet)

保存

垃圾邮件管理 - 基本设定

反垃圾邮件

菜单

垃圾邮件的管理 - 基本设定

基本设定 | 关键字登记 | 条件检索 | 除外指定 | 垃圾邮件LOG记录

监控发送或收到的邮件的头和正文，被判定为垃圾邮件的将被删除。

过滤的执行

☒ 实行过滤。

过滤的类型(*1)

☒ 实行在线过滤(批处理)。

☒ 过滤给本地帐户的邮件(离线)。

☐ 过滤出站邮件(离线)。

过滤详情(1) - 检查会话信息

☒ 对在SMTP认证上成功的连接不进行垃圾邮件检查。

☐ MAIL FROM: 指令的值和 RCPT TO: 指令的值如果相同，看做是:

过滤详情(2) - 邮件头/邮件体(邮件正文)的检查

☒ From: 如果该字段为空，认为是垃圾邮件。

☒ To: 如果该字段为空，认为是垃圾邮件([注意] 邮件列表可能为空)

5

如果目标地址 To: 有一个以上，认为是垃圾邮件。(*3)

5

如果抄送地址 Cc: 有一个以上，认为是垃圾邮件。(*3)

☒ Date: 域是空白，认为是垃圾邮件。

☒ Date: 字段不是RFC格式(Wed, 01 Oct 2008 或 1 Oct 08)认

☒ Date: 字段的年是 1970 年以前或 2037 年以后，认为是垃圾邮

☒ Subject: 字段、正文二者都是空白，认为是垃圾邮件。

☒ Subject: 字段是空白，认为是垃圾邮件。

☒ 邮件正文为空，认为是垃圾邮件。

☒ 在正文中搜索关键字(*5)。

10

KB 以上的不在邮件正文中搜索。

设置灰名单 GLST。GLST 是一个实用的反垃圾邮件工具。设置好后，自动执行，无需人为干预。

使用 GLST 需要在 JDMail 的过滤器定义文件 filters.pre-data.tab 进行启动 GSLT 的登记。请通过[过滤器的管理]-[SMTP DATA 预处理]完成。

设置信息保存在 glst\glst.conf。

监控发送或收到的邮件的头和正文，被判定为垃圾邮件的将被删除。

本功能设置垃圾邮件过滤的详细规则。

- ☒ **Subject:** 字段和正文内5位的HTML标记合计存在 10 个以上, 认为是垃圾邮件。(*6)
- ☒ 整个邮件 (标题和正文) 如果找不到中文 (2) 字节的字符, 被视为垃圾邮件。

■ 过滤详情 (3) - Received: 字段检查 (建议离线处理) (*7)

- ☐ 最新的 **Received:** 字段如果是 "from localhost" 认为是垃圾邮件 (*8 - 设定注)
- ☒ 最新的 **Received:** 字段如果是 "from (不正确的域名字符串)" 认为是垃圾邮件 (*9)
- ☐ 最新的 **Received:** 字段如果是 "from (IP地址)" 并且 IP 地址与实际的发送者 I
- ☒ 最新的 **Received:** 字段如果是 "from (本地域名)" 并且 比较访问原和本地的 I

» 本地域名列表

本地IP列表

■ 过滤详情 (4) - 垃圾邮件的处理

(判定为垃圾邮件的头部强制加上 X-Spam-Flag: Yes 字符串标识)

- ☒ **Subject:** 字段和正文都是空白, 立刻删除。(*12)。
- ☐ 转发给黑洞 (*13)。
- ☒ 放入本地用户垃圾邮件夹 (*14、WebMail 方便管理!!)。
- ☐ 直接投递 (*15)。
- ☒ "X-Spam-Status: Yes" 添加头部标记 (*16)。
- ☒ "X-Spam-Level: *****" 添加头部标记 (*17)。
- ☒ "X-Spam-Checker-Version: JDWA" 添加头部标记 (*18)。
- ☒ **Subject:** 字段前面的字符串 [SPAM] (中文不可) 自动插入 (*19)。

■ 地址黑洞 - 指定垃圾邮件的目的地 (*20)

目标域	地址黑洞 (只有一个地址)	垃圾邮件的浏览/处理
chundi.com		
long-d.cn		
mailer.cn		
mailer.com.cn		
其它目的地		
所有域		



(*1) 在线过滤 SMTP session 中被执行, 不仅仅是给本地帐号的邮件还有外发邮件(外发中继邮件)也全部成为处理对象。

要过滤包含出站邮件的所有邮件请使用在线过滤器。在线处理比离线处理对服务器的负荷轻。但是, 不能对每个地址帐号进行开/关处理。同时, 如果检查最新的 **Received:** 字段需要离线处理也运行。

为了使用 JDWM 垃圾邮件扫描相关菜单, 需要[本地帐号邮件(离线)]选中。

(*2) 收件人、发件人如果相同, 通常被认为是垃圾邮件。自己发给自己的这种情况除外。

如果允许合法用户自己发给自己, 就不要做此项限制。

(*3) 收件人地址(To:)和抄送地址(Cc:)可以用逗号指定多个。如果想限制数量, 可以在这里指定个数。JDMail 默认最大 100 个地址(用启动选择 -Sr 控制)。

(*4) 如果邮件头部的 **Date:** 字段为空或者异常, 有可能是垃圾邮件。

(*5) 如果邮件正文也检索, 一般需要指定邮件尺寸上限。普通垃圾邮件大部分分数 k 字节以内。

(*6) 为了避免被过滤, 有些垃圾邮件内容使用 HTML entity 标记, 例如"万艾可" 用 バイアグラ 编码表示。为了运行这个功能 [邮件正文内关键字检索]需要选中。

(*7) 邮件头部的 Received: 字段检查, 在线处理不能检查最新的数据(在线处理结束之后实行 session 的 Received: 字段添加)原因, 请启用离线处理。

(*8) 邮件头部的最新的 Received: 字段发送者域指定 "from localhost ..."的邮件看作垃圾邮件。

如果使用 JDWM 和 JDML 时, 把这个选择做为开需要注意。请修改各自的环境配置文件 config.local.cgi, 将环境变量 smtphele 值改为 localhost 以外。

同时, 如果在 JDMail 相同的主机上使用某种邮件发送机能也需要注意。

(*9) 邮件头部最新的 Received: 字段的发送者域名字符串不合法, 看作是垃圾邮件。推荐选中。

(*10) 邮件头部最新的 Received: 字段发送者域指定有 IP 地址时, 与实际的发送原 IP 地址不相符的情况被看作是垃圾邮件。

(*11) 如果邮件头部最新的 Received: 字段发送者域 "from (域名)"不存在, 被看作是垃圾邮件。比较 SMTP Session 中原服务器的 IP 地址和在你的域使用的 IP 地址, 如果不一致, 认为是垃圾邮件。本地域名不能使用通配符。同时, IP 地址的输入格式与是「除外指定」的情况同样,不能放入注释。

(*12) 一般 Subject: 都加上检查。

(*13)

(*14) 地址是本地用户的情况, 保存邮件到垃圾邮件文件夹。这个情况, 在相符合本地用户的邮箱内创建 spam 这个名字的邮件夹。如果不选中, 垃圾邮件将进入收件箱。建议由用户管理自己的垃圾邮件。

[JDWM 的管理]-[环境设置]-[基本设置] "垃圾邮件夹的使用" 设为 "许可"。被 spam 文件夹保存了的邮件 30 日后没有警告地自动删除。实行删除动作发生在 (1) spam 文件夹内新的邮件被追加保存的时候, (2)用户在 JDWM 里进入[垃圾邮件]菜单的时候。

(*15) 处理到此结束。

(*16) "X-Spam-Status:" 字段用于部分邮件客户端软件判断垃圾邮件用。

(*17) "X-Spam-Level:" 垃圾邮件级别。

(*18) "X-Spam-Checker-Version:" 垃圾邮件处理器的信息。

(*19) 邮件头 Subject:(主题)的开始插入特定文字 "[spam]" 。能作为垃圾邮件标识方便分类处理。

(*20) 如果指定了黑洞地址，所有被认为是垃圾邮件的都投递到这个地址。

黑洞地址即使是本地帐户，也不进入垃圾邮件夹。

设置信息保存在 spamwords-conf.tab 。

SPAM 对策 [反垃圾邮件]菜单内[垃圾邮件地址的管理]，[垃圾邮件主机的管理]，[垃圾邮件主机的管理 2(S25R 检查)] [安全性]-[SMTP 连接数限制]也能使用。

垃圾邮件处理的记录由本页的 [垃圾邮件日志(记录)]能阅览。同时，[访问日志(记录)]-[过滤器处理的日志(记录)2(JDWA)]也能查看。

为了可以通过 JDWM 实现过滤设定， "实行过滤" 需启用。

垃圾邮件管理-关键字登记

反垃圾邮件

菜单

垃圾邮件的管理 - 关键字登记

基本设定 | 关键字登记 | 条件检索 | 除外指定 | 垃圾邮件LOG记录

判定垃圾邮件的关键字的登记・管理。

■指定邮件头和邮件体检索「未许可广告」的关键字。

» 在线处理用关键字
(批处理所有邮件)

» 给本地用户的邮件
适用的关键字(离线)

» 出站邮件
适用的关键字(离线)

保存/更新

判定垃圾邮件的关键字的登记・管理。

指定邮件头和邮件体检索「SPAM 邮件」的关键字。

如果有指定不合适的关键字，正常邮件将会被删除，请注意。



1 个关键字的长度不能超过 100 字节。
关键字可以使用中文。
关键字可以使用通配符文字(*?)，不支持正则表达式。
如果个别的用户/邮件列表添加关键字，请使用[用户的管理]、[邮件列表的管理]菜单。
关键字列表保存在 spamwords-offline-in.tab(本地用户)、spamwords-offline-out.tab(出站)、spamwords-online.tab(在线)。
SPAM 对策还可以使用[垃圾邮件地址的管理]，[垃圾邮件主机的管理]，此外[安全性]-[SMTP 连接数限制]也能使用。

垃圾邮件的管理-条件检索

反垃圾邮件

菜单

垃圾邮件的管理 - 条件检索

基本设定 | 关键字登记 | 条件检索 | 例外指定 | 垃圾邮件LOG记录

根据指定条件检索邮件。

■条件检索的实行

☒ 执行条件检索。

■检索规则的添加

规则名: (可用中文)

检索对象字段 关键字 判断方法 正则表达式

■登记的规则一览

序号	规则名	字段	关键字	判断方法	正则表达式	删除/移动
检索规则没登记。						

根据指定的规则过滤垃圾邮件。



正则表达式是关闭的情况，关键字字符串通配符(?)能使用。
正则表达式是开启的情况，进行关键字字符串的语法检查。如果添加了不正当的正则表达式，系统的动作不被保证。同时，正则表达式不能使用中文。
如果存在多个规则，按照添加的顺序依次执行，最先匹配的规则垃圾邮件处理被执行。
"判断方法" 如果没有选择，被认为开启正则表达式，如果表达式内容为空，被认为是表达式关闭。
被判定为垃圾邮件的消息的处理用[基本设定]菜单能指定。
垃圾邮件处理的日志 [访问日志(记录)]-[过滤器处理的日志(记录)2(JDWA)]能浏览

垃圾邮件的管理-例外指定

反垃圾邮件

菜单

垃圾邮件的管理 - 例外指定

基本设定 | 关键字登记 | 条件检索 | 例外指定 | 垃圾邮件LOG记录

从过滤的对象排除连接的IP地址、收件人地址、发件人地址。(指定的白名单)

■例外指定

» 以下的 IP 地址的收信过滤除外。

» 是以下收件人地址 (RCPT TO: 或 To:header, Cc:header)的情况除外。

» 是以下发件人地址 (MAIL FROM: 或 From:header)的情况除外。

从过滤的对象排除连接的IP地址、收件人地址、发件人地址。(指定的白名单)。

IP 地址能象以下一样地指定。

192.168.1.10

个别指定

10.1.0.0/24

地址段指定

10.1.1.1-10.1.1.100

范围指定

在一个字符(#)后可以继续写注释。

发件人地址和收件人地址可以使用通配符(能指定?*)(正则表达式不可用)，请不要写邮件地址以外的字符串。同时，邮件地址不区分大小写。

name@domain.com
info@*

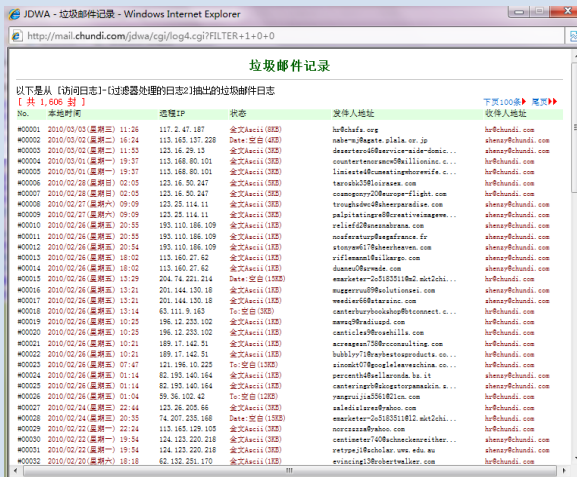
*[@domain.com](#)

设置信息保存在 JDWA 文件夹内的 `_spamscanIP.cgi`、`_spamscanFrom.cgi`、`_spamscanTo.cgi`。

垃圾邮件记录（被过滤的垃圾邮件一览。

序号	邮件标题	发件人	发件人邮箱	收件人邮箱
000001	2020/03/01 (星期三) 11:26	117.4.27.187	hbf@hundi.com	hbf@hundi.com
000002	2020/03/01 (星期三) 14:24	115.165.157.158	hbf@hundi.com	hbf@hundi.com
000003	2020/03/01 (星期三) 11:55	125.169.158	hbf@hundi.com	hbf@hundi.com
000004	2020/03/01 (星期三) 19:37	115.168.80.101	hbf@hundi.com	hbf@hundi.com
000005	2020/03/01 (星期三) 19:37	115.168.80.101	hbf@hundi.com	hbf@hundi.com
000006	2020/03/01 (星期三) 02:05	125.169.247	hbf@hundi.com	hbf@hundi.com
000007	2020/03/01 (星期三) 02:05	125.169.247	hbf@hundi.com	hbf@hundi.com

垃圾邮件
记录（被
过滤的垃
圾邮件一
览）



垃圾邮件 夹管理



垃圾邮件夹管理

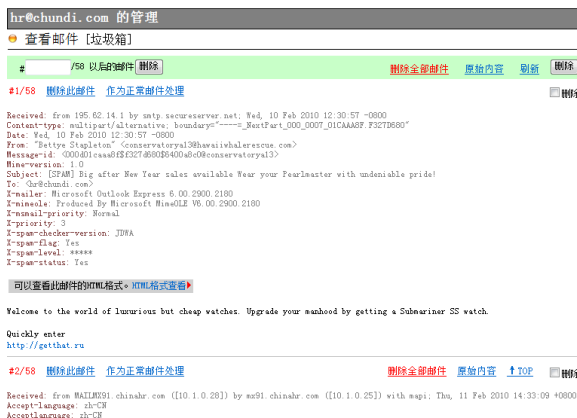
反垃圾邮件 菜单

垃圾邮件夹的管理

管理员可以直接查看普通用户的垃圾邮件夹。

- 邮件数共计保存30日以内的。旧的邮件在扫描的时候被删除。
- [阅览] 显示相符合帐号的垃圾邮件文件夹内邮件一览。
- [批量删除] 成批删除垃圾邮件文件夹内的邮件。不能恢复。
- [技术支持网站](#)。

可以批量删除、单个删除垃圾邮件。



邮件共计保存 30 日以内的。旧的邮件在扫描的时候被删除。

Received: from 195.62.14.1 by smtp.secureserver.net; Wed, 10 Feb 2010 12:30:57 -0800
Content-type: multipart/alternative; boundary="-----NextPart_500_5007_01CAAE8F_F327E690"
Date: Wed, 10 Feb 2010 12:30:57 -0800
From: "Bettey Stapleton" <Betteystapleton3@avast!vsharerescue.com>
Message-ID: <000401c0a8b1c327460046404b08@Betteystapleton3>
Mime-version: 1.0
Subject: [SPAM] Big after New Year sales available New Year's FourBuster with undeniable price!
To: <@chmcl.com>
E-mailer: Microsoft Outlook Express 6.00.2900.2180

```

X-mail-priority: Normal
X-priority: 3
X-spam-checker-version: JDBA
X-spam-flag: Yes
X-spam-level: 00000
X-spam-status: Yes

```

可以想象，垃圾邮件过滤器，利用垃圾邮件头中的

