PCI DSS 数据安全标准 V2.0

变更分析

Xiangdong Gao,atsec China

xiangdong@atsec.com

atsec(Beijing) information technology Co., Ltd

Room 119, Building 2, No.1, Street 7, Shangdi,

Haidian District, Beijing, P.R.China 10085
Tel +86-10-84834011
Fax +86-10-82890017

www.atsec.com

目　录

前言

在 2010 年 10 月， PCI 安全标准委员会发布了新版本的 PCI-DSS 和 PA-DSS 标准。作为周期性的新版本发布，该版本主要基于 PCI 标准在使用过程中各种信息反馈，对数据安全的要求进行完善，并未产生重大的变化。PCI 标准主要是卡品牌（Card brand）从持卡人数据所存在安全风险的角度，制定了覆盖数据安全所涉及的各个方面的安全标准。

对于新版本所引入的变更，本文旨在通过新版本与旧版本变化的角度，对新版本所涉及的主要变化进行解读，使读者能较快地理解和掌握标准变更的主要方面。如需要了解所有的变更，感兴趣的读者可通过 PCI 标委会网站所提供的“Summary of Changes from PCI DSS Version 1.2.1 to 2.0”以及 PA-DSS 的相应内容了解全部变更细节。

本文适用于各支付行业的服务供应商、商户及收单行的技术和管理人员使用。为加深对新版本的理解，建议对原版本做相应的了解，原版本中未变化的部分在本文中不再罗列。本文所涉及的内容重点在 PCI-DSS 标准，并未对 PA-DSS 所涉及的变化进行展开。

在本文的编写过程中，各位同事给予了大力的帮助，并提出了很多宝贵建议，在此向刘岩和陈谨运表示感谢！

声明：

本文对 PCI DSS 标准变化的解读所涉及的分类和说明等内容均基于 atsec 长期的知识积累、安全实践和对标准的认识，并不代表 PCI 安全标准委员会的观点。

1 变更概述

PCI 安全标准委员会（PCI SSC）最近发布了关于 PCI-DSS 和 PCI PA-DSS 的更新版本 V2.0。该版本的发布，经过了近两年从客户和厂商收集，并将审议的结果体现于新版本中。值得注意的是，V2.0 并未引入新的重大要求。下载地址如下：https://www.pcisecuritystandards.org/security_standards/updates.php

1.1 新标准产生的影响

对于 PCI-DSS 的变更，整体上趋向于更合理、更严格，同时也更多地引用和借鉴了业界的标准和实践。（具体内容请参照下一章节）

在原版本的 PCI PA-DSS 中，频繁地引用至 PCI DSS，使得客户和评估人员在完成 PCI PA-DSS 审核时要同时打开两个标准。由此，在 PA-DSS 的新版本中投入了大量工作以消除 PCI-DSS 和 PA-DSS 这两个标准间的信息冗余。

1.2 新标准的转换日期

对于 PCI DSS 和 PA-DSS 这两个标准的转换日期是一致的，如下表所示：

日　期	所应用的标准
2010 年 12 月 31 日前	V1.2.1 版本用于评估。在 2010 年不可使用 V2.0 版本。
在 2011 年	可使用 V1.2.1 或 V2.0 用于评估。V2.0 于 2011 年 1 月 1 日正式生效。
在 2012 年	评估中必须使用 V2.0。
2012 年 7 月 1 日	自该日起，PCI-DSS 要求 6.2、6.5.6 和 11.1 变为正式要求。在之前，这三个条款为最佳实践。

对于当前正基于 V1.2.1 版本进行评估的用户，意味着还有大约 11 个月的时间完成评估。客户也可选择在 2011 年使用 V2.0 展开评估。总之，在 2011 年，客户可基于新版本或旧版本展开评估，但在 2012 和 2013 年，所有评估必须使用 V2.0 版本。

atsec 在此建议需要通过 PCI-DSS 标准的组织尽早展开新版本的转换工作，以减少合规建设过程中对信息系统的影响。对于正在开展 PCI-DSS 合规的组织，推荐使用新版本进行 PCI 合规。

2 PCI DSS 的变更

以下内容主要侧重于 PCI DSS 的主要变化，因篇幅原因未能覆盖所有变化。

注：本章内容所描述的“原版本”指的是 PCI-DSS 的 V1.2.1 版本，“新版本”指的是 PCI-DSS 的 V2.0 版本。

2.1 适用性更强

为适应于组织的发展和合规的要求，在新版本中将所涉及适用范围和合规要求方面进行了更加明确的描述，使得某些概念更清晰、要求更明确。同时，也更多地引用了大量的业界标准和最佳实践，使得组织在合规过程中有更多的依据可寻。具体来看，适用性的变化主要体现在如下方面：

2.1.1 引用概念的变化

为更灵活地适应各种组织形式、组织规模以及组织的架构，新版本通过相应的概念变化使得组织在合规过程中的范围更清晰、要求更明确。

变化的方面	概念的变化	备 注
合规所涉及对象的变化	评估对象由旧版本的 company 变更为新版本的 entity。	这使得标准所适用的组织范围更广。
合规所涉及人员的变化	组织所涉及的人员由 employee 变更为 personnel。	该变化将组织的外部和相关人员均纳入到 PCI-DSS 的要求之中，通用性更强。
授权管理人员的变化	对管理过程的授权人员由 management 变更为 authorized party。	这使得授权和批准过程的管理更适用。

除此之外，新版本对 PCI DSS 所涉及的”介质 media”、“现场人员 onsite personnel”、“访客 visitor”等均给出了更明确的定义。

2.1.2 部分要求的合理化

在原版本的技术要求中，有些要求的通用性不高，使得组织在合规过程中的可选措施较少。新版本更多地关注于技术措施的有效性，在某些点不再局限于具体的某一种技术，使得组织在合规建设中的可选措施的范围更广一些。新版本主要对地址隐藏、帐号安全性要求、公共网络上的信息传输等方面提出了更为合理的技术要求，并在服务器的功能分布方面进行了合理化。主要的变化如下：

要求所在的条目	原版本的要求	新版本的要求
外向流量的访问（Requirement 1.3.5）	限制内网到互联网的访问。只能访问到DMZ，由后者转发至互联网。	允许内网流量在经过授权的前提下访问到互联网。（访问还需满足requirement 1.3.3非直接连接的要求）
地址隐藏方法（Requirement 1.3.8）	明确要求使用NAT和使用私有地址空间来隐藏地址。	添加了将持卡人数据环境置于代理服务器和内容缓存之内、删除和过滤路由通告等方法以隐藏地址空间。
“每台服务器一个主要功能”的解释（requirement2.2.1）	对 “每台服务器一个主要功能”有明确要求，未给出过多解释，使得组织在认证过程中对该要求有较多争议。	明确主要功能是处于同一安全级别的功能，这使得在合规过程中服务器上的主要功能的分布更加合理。 同时，明确了虚拟化的系统也视同于一台服务器，以适应于技术的发展和变化。
特定情况下的敏感认证数据存储（requirement3.2）	原版本中不允许在任何情况下存储敏感认证数据。	允许发卡行或支持发卡服务的公司在业务需要的情况下安全存储CHD。 这使得标准的适用性更强。
提供公共访问的服务（requirement4.1）	对于提供公共访问的服务使用SSL时，要求支持最新的补丁版本，使得组织必须频繁地关注于这些公开服务的最新补丁。	要求所有提供公共访问的协议（包括SSL）仅使用安全的配置，并且不支持不安全的版本。这使得公共服务的安全维护更合理，减少了不必要的补丁更新。
通过公共网络传输主帐号	在使用消息协议（requirement如	除可使用强加密措施外，也可以使用其它措施

信息的安全措施（requirement4.2）	邮件、即时消息等）通过公共网络传输主帐号信息时，要求使用强加密对主帐号进行保护。	把主帐号变得不可读来达到标准的要求。
分离了WEB程序和常规程序的安全漏洞（requirement6.5）	WEB和常规程序的安全要求未分离。	新版本更新了OWASP更新的TOP10漏洞，并将WEB程序和常规程序的漏洞检查要求分开，使得检查的要求更明确。
对计算机的访问人员分配唯一的帐号（requirement8）	未明确不涉及帐号要求的情况，使得帐号管理成为PCI-DSS合规中的难点之一。	明确帐号唯一性的所有要求适用于所有管理帐号，包括POS帐号以及用于访问持卡人数据的帐号。此处明确要求所涉及的范围是非客户的用户（non-consumer user），使得组织在合规过程中的技术措施更有针对性。 明确对处理单笔交易用户帐号的适用范围，明确部分要求（包括8.1分配唯一帐号、8.2认证方法、8.5.8不允许组密码、8.5.9每季度更改口令、8.5.10密码长度要求、8.5.11密码复杂度、8.5.12密码历史、8.5.13帐号锁定、8.5.14锁定周期和8.5.15闲置会话超时)不适用于该类帐号，使得帐号的安全要求更合理。
时间同步的来源（requirement10.4）	外部更新时间源为特定调频、GPS卫星以及UTC等。	明确为特定的、业界可接受的时间源，使得标准的适用性更强。
无线访问点的检查（requirement11.1）	要求使用Wireless Analyzer或无线的入侵检测系统对无线接入点进行检查。	添加了物理和逻辑监控、网络访问控制等方法进行检查，使得方法的选择更为灵活，明确只要达到有效探测到非授权设备即可。
入侵检测系统的监控位置（requirement11.4）	对于持卡人环境的入侵检测和响应，原版本要求监控持卡人环境的所有流量。	要求进行边界的检查，并对持卡人环境的关键点进行检查。该变化使得入侵检测系统的监控范围更为合理。
文件完整性监控的软件要求（requirement11.5）	使用文件完整性监控软件对关键文件的完整性进行监控。	将“软件”的要求变更为“工具”，使得一些系统自带的完整性监控工具也同样可用于标准的合规。
远程访问时对持卡人数据的操作（requirement12.3）	明确要求远程访问时禁止拷贝、移动和存储持卡人数据，不存在例外。	通过明确业务的需求论证和授权，并对数据进行安全保护的前提下，可对持卡人数据进行授权的操作。
安全意识教育（requirement12.6.1）	未提出更明确的要求。	明确可基于组织的不同角色及访问持卡人数据的级别进行不同的培训和教育，使得安全意识教育的开展更灵活。

2.1.3 对业界实践的广泛借鉴

在新版本的标准中，更多地借鉴了优秀的业界标准和实践。主要体现在：

所在的条目	原版本的参照标准	新版本的参照标准
密钥管理流程（requirement3.6）	要求以至少每年一次的频率定期执行密钥变更。	定义了密钥周期（cryptoperiod）的概念，要求组织参照业界实践NIST SP 800-57以及厂商的应用建议制定更新周期。
安全编码的实践引用（requirement6.5）	在安全编码方面要求的是参照OWASP。	除引用OWASP指导外，还包括SANS CWE top25，CERT secure coding等优秀业界实践的引用。
风险管理实践的借鉴（requirement12.1.2）	未定义风险评估所使用的方法论。	明确所推荐的风险评估方法论指导，包括OCTAVE、ISO 27005及NIST SP 800-30等。这使得组织在制定适用于自身的风险管理过程有更多的实践参考。

2.2 要求更严格

在新版本的要求中，除更加适用外，还对组织的安全措施和审核方面提出了更高要求。为便于进行说明，从组织的安全要求和QSA审核要求两个方面进行展开。

2.2.1 对组织的要求更严格

新版本在漏洞管理流程、系统配置标准的应用、主密钥的替换条件以及无线网络的识别等过程提出了更高要求。其中的主要要求变更包括：

所在的条目	原版本的要求	新版本的要求 （加粗字体为主要的变化）
记录并论证不安全协议的使用（requirement1.1.5）	原版本仅明确FTP协议作为不安全的协议。	而在新版本中，所要求的“不安全协议” 包括了FTP、Telnet、POP3、IMAP、SNMP等存在**明文口令传输、漏洞较多**的协议。
互联网与持卡人数据环境间的访问（requirement1.3.1-1.3.7）	要求明确的网络分段分隔互联网、DMZ区和持卡人数据区域，并且访问是业务所需要的。	在论证是业务所必须的前提下，添加要求所有的入站和出站要经过相应的**授权**。
	对于持卡人数据系统组件的分段，明确要求独立于DMZ区域。	对于持卡人数据系统组件的分段，明确要求独立于DMZ区域和**不可信网络区域**。
地址隐藏方法（requirement1.3.8）	无相应要求。	新版本要求在向外部透露内部地址和路由信息时，必须经过授权。
个人防火墙的安装范围（requirement 1.4.b）	要求移动用户须安装个人防火墙软件。	添加要求，员工**自有的电脑**也应使用个人防火墙软件。
安全配置标准（requirement2.2.b和2.2.d）	未明确配置标准在何时需要更新。	明确在组织**识别到新的安全漏洞时**，需要进行配置标准的更新，以应对新的安全威胁。
	要求对现有系统应用配置标准。	要求除现有系统外，对于**新的系统**也要应用安全配置标准。
	要求禁用所有不安全的组件、服务和协议。	要求配置标准**仅启用安全的**服务、进程和组件，并将所启用的服务、进程和协议的安全特性进行文档化
非控制台管理访问（requirement2.3）	要求对非控制台管理访问使用加密措施进行保护。	要求非控制台访问使用**强加密**进行保护。（提醒：DES算法已不被视作强加密算法）
持卡人数据存储和销毁管理体系（requirement3.1）	要求通过策略的实施，最小化持卡人数据的存储。	要求的体系范围更广，要求通过**策略、规程和流程**的实施以最小化持卡人数据的存储。
	未明确要求。	要求明确不同持卡人数据的保留要求，**制定安全流程**以删除不再需要的持卡人数据，并明确要求**每季度进行检查**。
使主帐号不可读的方法（requirement3.4）	使用单向哈希算法，未提出更多要求。	要求在使用单向哈希时，其结果的**来源必须是整个主帐号**。
	未提出更多要求。	要求哈希结果不能用于替换截掉的主帐号信息。 另外还要求哈希和截断同时存在时，要实施额外的控制措施以确保不可使用两者以恢复主帐号。
密钥的保护（requirement3.5）	未明确提出该要求同样适用于主密钥。	要求**主密钥的强度**至少与普通密钥一样强壮，并要求存储于尽可能少的位置和形式。
替换密钥的条件（requirement3.6）	要求在密钥变旧或者出现可疑情况时执行密钥的替换操作。	要求出现任何密钥的**完整性被弱化**时执行替换操作，密钥的管理更为严格。 另外，明确要求被替换掉的密钥不可再用于任

		何加密操作。（只能用于业务所需要的解密和验证目的）
新漏洞的识别流程（requirement6.2）	要求建立流程以识别新的安全漏洞，并未细化具体的建立过程。	对安全漏洞的识别提出了更高要求，要求**建立新漏洞的评分过程**。评分过程的建立要求基于业界最佳实践、CVSS等级以及厂商关于紧急和影响的分类等信息展开。
初始化密码的唯一性要求（requirement8.5.3）	要求新用户在密码初始化时使用唯一的初始密码。	要求新用户和**现有用户**在密码重置时均要满足唯一性的需求。
远程维护的管理（requirement8.5.6）	要求所有的远程维护帐号默认是禁用的，只在需要的时候开启访问。	将适用的范围扩大至远程维护、远程支持等各种**外部方的远程访问**，并要求在远程访问时进行必要的**监控**。
物理设施的访问保护（requirement9.1.3）	要求限制对无线接入点、网关以及手持设备的物理访问。	除原版本的要求外，添加对**网络和通讯硬件以及通讯的线路**进行物理保护的要求。
时间同步（requirement10.4）	未提出进一步的要求。	要求指定的**时间服务器间**也需要保持同步。
	未提出进一步的要求。	要求对关键服务器的时间变更要进行**记录、监控和检查**。
无线访问点的检查（requirement11.1）	检查的范围是无线访问点。	将检测的范围扩展到**系统组件所连接的**WLAN卡、可移动无线设备以及连接到网络接口和网络设备的无线设备。
	未提出检查策略和流程的要求。	要求制定**文件化的流程**以检测无线访问点。
文件完整性监控措施的实施（requirement11.5）	未提出明确告警和比对要求。	要求对监控工具进行配置以在出现未授权更改时**产生告警**，并明确至少每周执行一次关键文件的**比对**。

2.2.2 对审核过程的要求

作为QSA审核阶段最重要的工作，新版本对QSA审核范围和抽样的确定提出了更明确的要求。

2.2.2.1 更多的审核要求

在原版本的某些要求中，存在对测试规程的多个描述，具体所要求的条目不够清晰。在新版本中，将这些规程分隔分解为独立的要求，使得要求更明确。比如将原版本中1.1.3要求验证配置标准包括防火墙以及确认所提供的拓扑结构是最新，新版本则分解为两个流程1.1.3.a和1.1.3.b。

2.2.2.2 审核范围的确定过程

在范围的确定过程中，新版本进一步明确主帐号（PAN）是PCI DSS是否适用的定义性因素。新版本明确要求通过首先识别持卡人数据的位置和流向，进而确定支撑业务的IT系统，由QSA最终确定持卡人数据环境的范围。

2.2.2.3 抽样过程的论证

对于抽样过程，增加了对抽样论证的要求，要求QSA采用抽样方法论，并在合规性报告（ROC）中论证抽样方法的合理性和充分性。

2.2.2.4 代码发布过程的审核（6.3.2）

在审核过程中，要求QSA抽取最近的应用变更，并依据标准所提及的安全编码、编码检查、变更审批、影响分析、回退方案以及实施验证等过程进行验证。

3 PCI-DSS 合规建议

如前一章节所述的主要变化可以看出，新版本除了对合理性和可用性进行了完善，也在相当大地程度上提高了标准的具体要求。这就需要合规的组织需要作出更多地努力，以达到PCI DSS标准的合规。以下是几点建议，希望对组织在PCI DSS的合规工作中有所帮助。

3.1 安全实践与业务系统的有效融合

组织无论是在应对各种安全风险，还是在各种合规过程中，都涉及具体的安全措施。从新标准对大量业界实践的引入以及更侧重于全过程安全控制的变化来看，积累更多地实践并不遗余力地将其应用到业务过程中是一个行之有效的积累和建设过程。我们也能看到，经过充分融合的安全过程，其在合规过程中所带来的痛点也会小得多。

3.2 充分借助和利用现有体系和措施

组织在信息安全的建设中，会有一些在体系建设方面和安全措施方面。在体系建设过程中，组织可最大化地重用已有的成熟的体系建设成果和安全措施，如ISMS管理体系中的人力资源管理要求就可以较全面地满足PCI DSS在人力资源方面的要求，这在实践中证明是投入最小的办法。

3.3 持续合规与改进

PCI DSS的合规并不是一劳永逸的工作，需要每年进行审核，同时ASV、风险评估、渗透测试等等各种工作也要定期开展。不建议为获得PCI DSS的资质而花费大量资源通过认证，认证过后放松安全要求的做法。组织虽然通过了PCI DSS，但在不合规状态下出现安全事故，其后果与未进行PCI DSS合规的后果是一样的。由此看来，PCI DSS的合规是需要持续合规与改进。建议组织在通过PCI DSS后，更多地关注于PCI DSS要求与现有业务运行体系的有效融合，并通过持续改进的方法使组织一直处于合规状态。

参考文献

[1] PCI SSC V2.0 版本以及变更摘要（Change summary）

https://www.pcisecuritystandards.org /security_standards/documents.php

[2] atsec newsletter 2010/12

http://www.atsec.com/downloads/documents/News_USA_12_2010_web.pdf

[3] “ What to expect from a PCI QSA led assessment“ by Fiona Pattinson

http://www.atsec.com/downloads/presentations/What_to_expect_from_a_QSA_assessment.pdf

[4] “ Payment Card Industry Compliance For Large Computing Systems“ from atsec

http://www.atsec.com/downloads/white-papers/PCI_Compliance_for_LCS.pdf

[5] “navigating the PCI DSS v2.0“ from PCI SSC website

https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf

关于 **atsec**

艾特赛克信息安全（atsec information security）是一家独立且基于标准的信息技术（IT：Information Technology）安全服务公司(www.atsec.com)，它很好地将商业导向的信息安全方法和深入的技术知识以及全球的经验相结合。atsec在德国慕尼黑成立于2000年，并且通过美国、德国、瑞典和中国的办公室开展了广泛的国际业务。atsec提供的服务包括正式的实验室测试和评估、独立的测试和评估以及信息安全咨询。

atsec提供PCI SSC体系下的服务，并且atsec是一家能够提供PCI DSS和PA-DSS标准的评估服务的QSA公司。atsec的渗透测试、应用安全、ASV（Approved Scanning Vendor）服务和信息安全咨询服务，作为评估服务工作的有力支撑。atsec是一家独立的公司，并且与其它产品供应商没有任何商业关系。

atsec提供美国国家标准与技术研究委员会（NIST：National Institute of Standards and Technology）和加拿大通讯安全协会（CSEC：Communications Security Establishment Canada）制定的密码模块验证体系下的密码模块和算法测试服务。atsec同时提供NIST个人身份验证体系（NPIVP）、密码算法测试（CAVP：Cryptographic Algorithm Validation Program）和安全内容自动化协议（SCAP：Security Content Automation Protocol Program）下的正式的测试，以及GSA FIPS 201 EP下的产品认可测试。

atsec的客户包括全球首屈一指的公司如苹果、IBM、Hewlett and Packard、Honeywell、Quantum Corporation、Red Hat、Watchdata、华为和中兴通讯等，并一直维持密切合作关系。

多年以来，atsec 对PCI DSS标准持续关注，积累了大量的最佳实践和合规建议，并形成了一整套完整的方法论，在此也希望为涉及PCI DSS合规的服务供应商、商户和收单机构的合规性建设提供相应的支持和帮助！