Web Services 的访问控制研究综述*)

许 峰 林果园 黄 皓

(南京大学软件新技术国家重点实验室 南京 210093) (南京大学计算机系 南京 210093)

摘 要 随着 Web Services 的发展,它本身的安全问题已经成为制约其发展的关键因素。本文主要论述了 Web Services 的访问控制技术的研究现状及其问题。首先,从协议层次出发讨论了 Web Services 的访问控制技术的研究方法。然后分别介绍了 XML 文档和 SOAP 协议的访问控制技术,以及 Web Services 的相关访问控制规范。最后总结全文并提出了需要进一步研究的问题。

关键词 Web 服务,访问控制,安全,XML

A Survey on Access Control for Web Services

XU Feng LIN Guo-Yuan HUANG Hao

(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)

(Department of Computer Science and Technology, Nanjing University, Nanjing 210093)

Abstract Security is currently one of the biggest concerns about future development of Web services. This paper brief reviews the state of the research for access control in the Web service environment. In this paper, we first discuss the way to study the access control technology from the protocol stack of the Web services. Then we discussed the access control technology of XML documents and the SOAP protocol, as well as correlation standard. Finally, the conclusion is given and the problems are pointed out, which should be resolved in further reserach.

Keywords Web Service, Access control, Security, XML

1 引言

Web Services 是构建新一代动态电子商务的核心技术,在体系结构、设计、实现与部署等方面比传统的分布式对象技术更加合理。与传统的 Web 开发方式相比,Web Services 构建的商务逻辑更加开放和标准化,使其在安全性上更加脆弱,主要表现在以下几个方面:

① Web Services 允许将复杂的功能分布到可重用组件中,对外提供了调用的接口,给外来用户提供了访问敏感信息和控制业务逻辑的能力。

② Web Services 带来了新的挑战,由于 XML 文档以文本形式编码,而不是以二进制形式,使其能够穿越传统的防火墙,从而带来了新的安全隐患。

③ Web Services 是一个发展中的技术,随着新的技术和标准的产生,可能会引入新的安全问题。

随着 Web Services 技术和产品的进一步推广,其安全性已经成为关键性问题。访问控制是最重要的安全技术之一,也是可信计算机系统评估标准(TESEC)中的评价系统安全的主要指标之一。所以 Web Services 的访问控制技术已经成为了研究的热点问题。

本文着重介绍了 Web Services 访问控制技术的研究现状和发展趋势。文章第 2 节介绍了 Web Servics 的协议栈及其安全问题;第 3 节重点讨论了 Web Services 的访问控制技术;最后总结全文并提出了还需要进一步解决的问题。

2 Web Services 的协议栈及其安全问题

Web Services 体系建立在现有的和新兴的开放性规范之上,它们构成了 Web Services 的协议栈。这些规范包括:HTTP 协议、可扩展标记语言(Extensible Markup Language,简称 XML)、简单对象访问协议(Simple Object Access Protocol,简称 SOAP)、Web 服务描述语言(Web Service Description Language,简称 WSDL)、通用描述发现和集成协议(Universal Description Discovery and Integration,简称 UDDI)[17],以及商业流程执行语言规范(Business Process Execution Language for Web Services,简称 BPEL4WS)[19]等。Web Services 的协议栈[13]可分为:工作流层、服务描述和发现层、消息层以及通信层。这些主要的层次由几个标准协议构成,如图 1 所示。工作流层支持事务处理和业务模型的表示;服务描述和发现层负责描述服务、定位服务和发布服务,把 Web 服务定义为端点(endpoint)的集合,接收并处理文档信息或者过程信息;消息层负责消息的封装与传递,主要工作协议是 SOAP,它在其中扮演了基于 XML 消息的封装器的角色,SOAP 包含了消息封装、路由、可靠投递和安全性方面的内容;网络层采用已有的协议(如 HTTP、FTP 等)负责在网络中传输信息。

W3C[13]提出的 Web Services 的模型为从协议栈层次研究安全技术指明了方向。从协议栈层次看,在通信层可以采用已有的安全机制,而其他层次的安全问题需要进一步研究。目前有很多研究集中于消息层次,主要针对 XML 和 SOAP 协

*)本课题得到国家"863"高技术(NO:2001AA142010)经费资助。许 峰 博士生,主要研究领域为网络安全;林果园 博士生,主要研究领域为网络安全;黄 皓 教授,博导,主要研究领域为网络安全。

议进行安全问题研究，包括对 XML 文档[2,3]安全以及 SOAP[8,9]等标准协议的安全性研究。主要采用了加密和数字签名技术，可以对 XML 文档和 SOAP 消息的全部和部分进行加密和签名。为了实现支持跨平台的安全性，提出了安全的认证授权描述语言[4,5,11]。对于信息的机密性和完整性，可以将已有的网络通信的安全技术与 XML 加密[2]、签名[3]技术结合，满足实际应用中不同层次的安全需求。

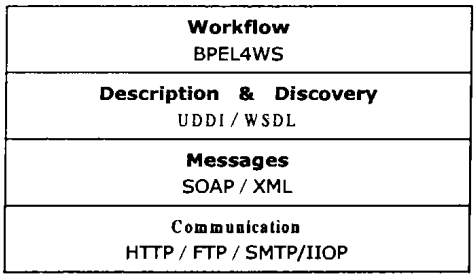


图 1　Web Services 的协议栈

3　Web Services 的访问控制技术

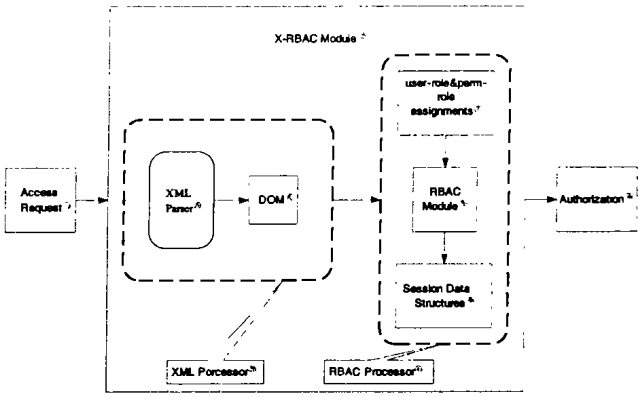
访问控制的目标是防止对任何资源的未授权访问。Web Services 环境中，除了传统的信息资源外，还有两类新的资源：XML 文档和 Web 服务。对应到 Web Services 协议栈，其基础是 SOAP 和 XML 协议。对于 Web Services 访问控制技术，将从以下三个方面进行阐述：XML 文档的访问控制技术研究，基于 SOAP 的访问控制技术的研究，以及访问控制的相关标准规范的研究。

3.1　XML 文档的访问控制

在 XML 语言出现前典型的 Web 的访问控制都是在文件系统级上的，访问控制与被保护的数据相对独立，部分原因是由于 HTML 语言的限制[15]。XML 出现后改变了这种状况，可以根据文档的结构和内容，定义和实施访问控制。米兰大学的 Bertino 等人最早提出了 XML 文档上的访问控制的问题[20~22]。针对 XML 文档的层次结构特征以及内部的索引结构[20]，在 XML 文档的保护模型中加入了一些新的特征，提出了三种不同的授权传递方式和两种 XML 信息发布形式（即信息推和信息拉）。Authox-X[21]是该模型基于 JAVA 组件的原型系统。

Daminai 等人利用 XML 结构化的特性来进行访问控制，在 XML 文档中引入授权表[14,15]，以完成细粒度的访问控制。研究表明采用 XML schemas[15,16,23]进行访问控制比 DTD[14]更具有优势。他们提出的细粒度的 XML 文档访控模型[15,16,23]和 Bertino 模型[20~22]相比，对主体和客体的描述进行了扩展，主体不再仅仅是用户 ID，还考虑了组的划分和主体请求的来源。客体使用 XPath 进行表示，可理解性和实现性都大大增强。而 Bertino 模型比较灵活性，该模型将 XML 文档看成网状结构，授权传递不仅可以向下传递，而且可以向上传递。尽管这些特征增加了模型的灵活性，但其可理解性不如 Daminai 模型[23]，并且也显著地增加了实现的难度。

XML 文档存取控制的研究最初可以看作是 DAC 的一种延续。针对 XML 文档和应用的特点，对 DAC 进行了多方面的扩充。近年来随着学术界对 RBAC 模型的关注，基于角色的访问控制也引入到 XML 的访问控制中。考虑到 XACML 无法描述针对角色的授权，Bhatti 等人[16]提出了一个基于 XML 的 RBAC 策略描述框架，实现了 XML 文档的基于角色的授权。提出的规范语言提供了简洁的访问控制策略，符合 NIST 的 RBAC 模型。X-RBAC 是其基于 Java 的原型系统。这个框架在概念、视图、实例和元素层能够被用来说明和强制 RBAC 策略，允许动态获取内容信息。如图 2 所示，X-RBAC 系统主要由 XML Processor 和 RBAC Processor 组成。XML Processor 主要完成对 XML 的解析和生成 DOM；RBAC Processor 实现对于角色和用户权限的分配。



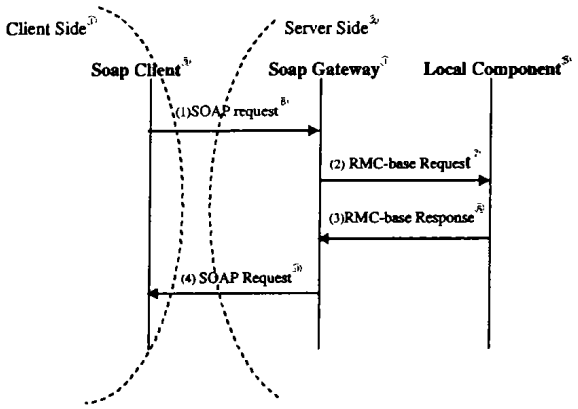
①访问请求 ②X-RBAC模块 ③XML处理器 ④RBAC处理器 ⑤XML解析 ⑥DOM生成器 ⑦用户角色权限分配 ⑧RBAC模块 ⑨会话数据结构 ⑩授权

图 2　基于角色的 XML 访问控制系统结构 X-RBAC

3.2　基于 SOAP 访问控制

基于 SOAP 访问控制的研究[1,8,9,11]，利用了 SOAP 协议基于 XML 表示的特点，在很多方面使用了 XML 的安全技术，包括 XML 的加密、签名等技术。其方法主要是通过对 SOAP 信息的 Header 部和 Body 部扩展，来增强其安全性，从而实现对 Web 服务的访问控制。

在系统实现方面，Damiani 等人[11]提出了基于 SOAP 消息的过滤机制，将 SOAP 信息转化为 RMC（远程调用）以实现对本地组件的访问控制。图 3 是其原理图。服务器端由 SOAP 网关和本地组件构成。该系统根据嵌入在 SOAP 信息头中的认证信息，对其进行身份认证，过滤和修改。SOAP 调用请求被直接发送给 SOAP 网关，SOAP 网关解析和评估认证后实现对 Web 服务的访问限制。根据认证结果和系统策略，SOAP 请求可能被拒绝，被允许或参数被修改后转换为 RMC 调用，发送给本地组件。



①客户端 ②服务器端 ③SOAP 客户端 ④SOAP 网关 ⑤本地组件模块 ⑥SOAP 请求 ⑦RMC 调用 ⑧RMC 响应 ⑨SOAP 响应

图 3　基于过滤的 SOAP 访问控制

由于该系统构建于原有系统的安全架构上，是一个从传统的应用架构向 Web Services 过渡的方案，并不完全符合 Web Services 的开放性要求。

3.3 相关的标准规范

目前有许多组织致力于制定 Web Services 的相关标准和规范。在访问控制方面主要包括以下几个规范：安全性断言标记语言（Security Assertion Markup Language，简称 SAML）[4]、可扩展访问控制标记语言（Extensible Access Control Markup Language，简称 XACML）[5]、可扩充版权标记语言（Extensible Rights Markup Language，简称 XrML）[6]，XML 密钥管理规范（XML Key Management Specification，简称 XKMS）[7]，Web 服务安全性规范（Web Services Security specification，WS-Security）[1]。通过 XACML 和 SAML 联合使用提供了标准化 XML 文档访问控制的方法。其层次图如图 4 所示。

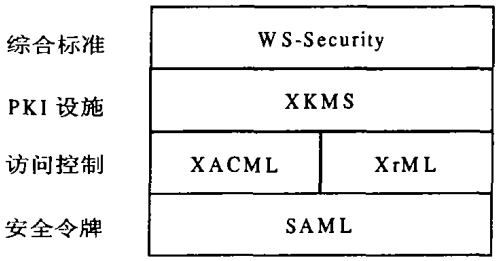


图 4 Web Services 访问控制的相关标准的层次图

3.3.1 SAML SAML 是 OASIS 组织制定的，其目的是作为一种用于交换安全性信息的基于 XML 的框架。SAML 使用签名的断言或者 Token 去陈述用户的权利。它并不创造新的认证协议，而是一种获取已有认证协议的认证数据的方法。与其它安全性方法相比，SAML 采用有关多个主体的断言的形式来表述安全性；而其它方法使用中央认证中心来发放证书，这些证书保证了网络中从一点到另一点的安全通信。利用 SAML 网络中的任何点都可以断言它知道用户或数据块的身份。它使得一次登录机制（single sign-on）和跨域的授权模型（authorization models that cross domain boundaries）成为可能。它是一种用于不同安全系统和平台中共享授权信息的通用标准。

使用 SAML 要求参与者间的相互信任，但是 SAML 协议本身并不能提供建立这种信任的保证。SAML 本身不能保证断言在传送过程中的机密性，一致性和不可抵赖性。这些安全性保证，需要采用其他的安全机制。

3.3.2 XACML XACML 是 OASIS 组织制定的一个基于 XML 的规范，目标是标准化访问控制信息。它表述了在 XML 文档或任何其他电子资源的细粒度访问控制策略。其中资源可以是一个完整的文档、多个文档或者部分文档。其目标对象的控制粒度可以到单个文档的元素。

XACML 的主要思想是围绕一个四元组（subject、resource、action、condition）来定义访问控制授权策略。subject 为授权访问用户，resource 代表访问的资源，action 表示对资源的访问操作，condition 表示采取特定操作的先决条件。在制定策略时，首先根据资源 resource，确定对于 subject 元素所描述的访问者，是否被授予执行 action 操作的权限。condition 元素用于定义特定访问操作的先决条件，这使得策略控制的描述制订可以非常灵活，制定的访问策略可以方便地应用于各种不同的场合。

XACML 提出了一个抽象的数据流模型，与实际的访问控制实施结构相独立，其重点在于描述通信协议。在该模型中收到一个 SAML 请求后，策略决策点（PDP）就根据定义的策略集来判断，决定是否允许请求使用某项资源；然后策略实施点（PEP）根据 PDP 的决策负责执行策略。XACML 规范定义了编码规则，策略绑定规则，以及多规则或策略的选择和组合算法。并提出了策略语言模型和制定了策略描述的语法定义。需要注意的是文档中虽然讨论了其安全威胁和相应的安全措施，在实际实施中要采用其他安全技术加强安全性。

3.3.3 XrML XrML 是一种首选的数字版权语言。XrML 提供了安全地规定和管理有关任何数字内容和服务版权条件的一个通用性方法。XrML 规定了一种使用权限的表达语言（Right Expression Language，简称 REL）。可以用 XrML 制定使用权限许可证，这种语言可以被用来在一个受托系统上进行信息使用权限的表示，并在受托的权限管理系统上被强制执行。其使用权限许可证可被用于任何形式的信息，如电子邮件、办公应用程序、数据库和客户公共关系管理系统等。

XrML 将促进数字内容的传播以及网络服务的发展，它的应用并不受限于技术平台、商业模型和媒体类型、媒体格式、提供商等范围。XrML 的一般目的是表示权利和状况，例如有效时间，数字资源和服务。XrML 主要用于数字版权管理，和 XACML 有交叉。XACML 是更加完整和复杂的规范。XrML 容易使用，但不适合于复杂的存取策略和规则。XrML 并没有说明如何认证和保护版权的表示。

3.3.4 XKMS VeriSign，Microsoft 和 WebMethods 制定了 XKMS[7]，XKMS 将许多 PKI 协议和数据格式，如证书管理协议和简单证书注册协议等，替换成一个基于 XML 的协议。在 XKMS 环境中，信任的决定是由一个公共的服务器完成的。XKMS 是建立在 XML 的数字签名和加密标准基础之上，其关键的思想是提供 Web 上的可信服务（trust server），把复杂的密钥认证处理过程隐藏起来，这样 XML 应用可以不用太关注 PKI 细节，简化了用户的使用，降低了对服务请求者的要求。XKMS 包含两个子协议：XML 密钥信息服务规范（X-KISS）和 XML 密钥注册服务规范（X-KRSS）。

X-KISS 规范定义一个信任服务协议，用于解析 XML 签名中的公开密钥信息，向用户提供密钥和证书服务。X-KISS 本身包含两类服务：定位服务和确认服务。前者负责提供密钥和证书，后者负责密钥和证书的合法性检验。该协议主要目的是减少应用实施的复杂性。通过将应用作为信任服务的客户端，从而免受基础 PKI 复杂性和语法的影响，而基础 PKI 可以建立在不同的规范上。使用 X-KISS 可以从一个密钥服务器上检索公开密钥，用于加密和验证签名。应用也能够使用 X-KISS 验证某一个密钥是否被取消。XKMS 开创了一种信任服务，通过向 PKI 提供 XML 接口使用户从繁琐的配置中解脱出来。XKMS 用户仅需的配置工作就是服务器的 URL 地址和服务器用来签名的证书，而使用不同的 URL 地址，可支持不同的信任模型。

X-KRSS 用于向密钥和证书的持有者提供密钥管理服务，定义了密钥（证书）注册、密钥（证书）注销、密钥恢复和密钥更新的服务接口。这个规范说明了注册 RSA 和 DSA 密钥和支持其他加密算法（Diffie-Helleman 和椭圆曲线等）的扩展框架。

3.3.5 WS-Security WS-Security[1]是 IBM 和 MS 等共同提出的规范，它定义了一个标准的 SOAP 扩展的集合。WS-Security 解决的是如何在多点消息路径中维护一个安全的环境。WS-Security 通过利用现有标准和规范来实现安全

性，它是一个综合的安全方案。它描述了 SOAP 消息传递的安全增强，通过消息完整性、机密性和单消息认证等方法提供对 SOAP 消息传递的安全保护。另外还提供了关联安全性令牌和消息的通用机制。WS-Security 没有对安全性令牌的具体类型作要求，旨在保证它的扩展性(例如支持多安全性令牌格式)，以便适应各式各样的认证和授权机制。这些基本机制可以通过各种方式组合，以适应构建使用多种加密技术的安全性模型。但是 WS-Security 自身并不保证安全性，也不提供完整的安全解决方案。

WS-Security 在现有规范中添加了一个架构，用于将已有的安全机制嵌入到 SOAP 消息中。WS-Security 定义了一个用于携带安全性相关数据的 SOAP 标头元素。如果使用 XML 签名，此标头可以包含由 XML 签名定义的信息，其中包括消息的签名方法、使用的密钥以及得出的签名值。同样，如果消息中的某个元素被加密，则 WS-Security 标头中还可以包含加密信息(例如由 XML 加密定义的加密信息)。WS-Security 并不指定签名或加密的格式，而是指定如何在 SOAP 消息中嵌入由其他规范定义的安全性信息。WS-Security 主要是一个用于基于 XML 的安全性元数据容器的规范。

使用 WS-Security 中所描述的完整性和机密性机制可以防止消息被篡改和窃听。重放攻击可以通过使用消息时间戳与高速缓存来解决，也可以通过使用其它特定于应用程序的跟踪机制来解决。对于其所有权是通过使用密钥进行验证的 SAML 断言令牌来说，一般可以通过使用主体确认来缓和中间人(man-in-the-middle)攻击。

同时，WS-Security 提出在中介机构与端点之间应建立安全策略和信任模型，以便 Web 服务之间能够安全地相互操作，并在安全策略中嵌入隐私语言；在保证安全的端到端连接方面提出可以建立一种安全会话机制，并以此在异构的联盟环境中管理与代理信任关系等。

总结 近年来虽然在 Web Services 访问控制技术研究方面取得了上述成果，但是在应用方面还很不成熟。Web Service 本身的特性和分布式网络环境的复杂性使得访问控制成为一个富有挑战性的问题。研究时要关注以下关键问题：

由于 Web Services 需要与传统的应用系统进行交互，故其安全架构应该能够与原有系统的安全架构相兼容。在实际应用中需要灵活的 Web Services 访问控制机制，实现基于内容、上下文相关的访问控制，并处理主体和客体的异构性。访问控制必须保持同步，使用户从一个域进入到另一个域时得到认证。

在 XML 文档的访问控制策略方面，需要研究灵活的、细粒度的访问控制机制。策略需要有足够的弹性，使用户能够根据需要定制安全粒度可能 XML 文档与预定义的格式不同，即 XML 文档结构的丰富性，这在频繁交换信息、不断变化的网络中是很常见的，现有的策略如果没有对其的规定，应考虑如何正确处理。

另外，建立一个全球 Web Services 的安全基础设施将是业界的目标，为了保证安全架构的性能和可伸缩性[10]，需要解决不同的组织提出的标准的兼容性问题。特别是许多不同的但是相关的标准之间的共存以及相互间关系的问题。到目前为止，还没有哪个标准被完全实现和接受。如果这个问题不能很好地解决可能影响到 Web Services 技术的发展。

参 考 文 献

1 Web Services Security (WS-Security) version1.005, April 2002. http://www-106.ibm.com/developerworks/webservices/library/ws-secure/

2 W3C Working Draft. XML Encryption Syntax and Processing, March 2002. http://www.w3.org/TR/xmldsig-core/

3 W3C Recommendation. XML-Signature Syntax and Processing. 2002. http://www.w3.org/TR/xmldsig-core/

4 OASIS Standard. Security Assertion Markup Language, SAML1.1, Oct. 2003. http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf

5 OASIS Standard. XACML 1.0 Specification Set. Feb. 2003. http://www.oasis-open.org/committees/xacml/

6 ContentGuard, Inc. eXtensible Rights Markup Language, XrML 2.0. (2001) http://www.xrml.org

7 W3C Working Note. XML Key Management (XKMS 2.0). http://www.w3.org/2001/XKMS/

8 Web Services Security Core Specification Working Draft 01, 20 September 2002. http://lists.oasis-open.org/archives/wss/200209/pdf00000.pdf

9 W3C NOTE. SOAP Security Extensions: Digital Signature. http://www.w3.org/TR/SOAP-dsig

10 Towards Securing XML Web Services. ACM Workshop on XML Security, November 22, 2002, Fairfax VA, USA

11 Sirer E G, Wang K. An access control language for web services. In: Proc. of the ACM Symposium on Access Control Models and Technologies, ACM Press, 2002. 23～30

12 Nakamur Y, Hada S, Neyama R. Towards the Integration of Web Services Security on Enterprise Environments. Symposium on Applications and the Internet (SAINT) Workshops, 2002, Narar City, Nara, Japan

13 W3C. Web Services Architecture. http://www.w3.org/TR/ws-arch

14 Damiani E, et al. Design and implementation of an access control processor for XML documents, Computer Networks. The International Journal of Computer and Telecommunications Networking, June 2000, 33(1-6): 59～75

15 Damiani E, De Capitani di Vimercati S, Paraboschi S, Samarati P. A Fine-Grained Access Control System for XML Documents. ACM Transactions on Information and System Security (TISSEC), May 2002, 5, (2): 169～202

16 Bhatti R, Joshi J B D, Bertino E, Ghafoor A. Access Control in Dynamic XML-based Web-Services with X-RBAC. Accepted for publication in The First International Conference on Web Services, Las Vegas, June 23-26, 2003

17 UDDI Version 3.0 Published Specification, 19 July 2002. http://uddi.org/pubs/uddi_v3.htm

18 W3C Note. Web Services Description Language (WSDL) 1.1, 15 March 2001. http://www.w3.org/TR/wsdl

19 BPEL4WS, http://www-106.ibm.com/developerworks/webservices/library/ws-bpel/

20 Bertino E, Castano S, Ferrari E, Mesiti M. Controlled Access and Dissemination of XML Documents. Workshop on Web Information and Data Management, 1999. 22～27

21 Bertino E, Braun M, Silvana C, Ferrari E, Mesiti M. Author-X: A Java-Based System for XML Data Protection. DBSec 2000. 15～26

22 Bertino E, Castano S, Ferrari E, Mesiti M. Specifying and Enforcing Access Control Policies for XML Document Sources. ACM Transactions on Information and System Security, Aug. 2002, 5 (3)

23 Damiani E, Vimercati S D C, Paraboschi S, Samarati P. Securing XML Documents. In: Proc. of EDBT 2000, Lecture Notes in Computer Science, Springer, 2000, 1777: 121～135