## 访问控制术语

**Access（访问）**

实施（Performing）一个动作（Action）

**Access control（访问控制）**

通过策略（policy）或策略集（policy set）控制访问

**Action（动作）**

绑定资源的操作

**Advice（建议）**

策略或策略集中的一小片信息，这些信息由PDP（策略决策点）提供给PEP（策略执行点）。

**Applicable policy（匹配的策略）**

（governs）匹配一个决策请求的访问决议的策略集合和策略集集合

**Attribute（特征）**

主体（Subject）、资源（Resource）、动作（Action）或环境（Environment）的特征，这些特征可能被断言或目标引用。

**Authorization decision**

匹配的策略的评估结果，由策略决策点返回给策略执行点。一个结果为”Permit”，“Deny”，“Indeterminate”或“NotApplicable”，和（可选的）一个义务和建议集的函数。

**Bag（袋）**

一个无序的允许有重复元素存在的集合

**Conjunctive sequence（逻辑与连接序列）**

一个由逻辑’AND’操作链接的断言序列

**Context（决策请求响应上下文）**

表示一个决策请求和授权决策响应

**Context handler**

将原始请求格式转化为标准XACML决策请求的系统实体，协调策略信息点将特性值添加到请求上下文，并将XACML授权决策响应转化为原始响应格式。

**Decision（决策）**

一个规则（Rule），策略（policy）或策略集（policy set）的评估结果。

**Decision request（决策请求）**

由策略执行点向策略决策点发起的授权决策请求。

**Disjunctive sequence（逻辑或链接序列）**

一个由逻辑“OR”操作链接的断言序列

**Effect（结果）**

一个匹配的规则（Rule）的预期结果（“Permit”或“Deny”）

**Environment（环境）**

一个与授权决策相关的特性集，这个特性集独立于具体的主体（subject），资源（resource）或动作（action）

**Identifier equality（标识相等）**

标识判等操作

**Issuer（发行人）**

一个描述策略源的特性集合

**Named attribute（命名特性）**

一个由特性名和特性类型以及特性持有者标识（特性持有者可以是主体、资源、动作或环境）和特性发行者标识决定的具体的特性实例。

**Obligation（义务）**

一个由规则，策略或策略集指定的应有策略执行点连同授权决策一起执行的操作

**Policy**

一个规则集，一个规则合并算法和（可选的）义务或建议集。可能是一个策略集组合

**Policy administration point(PAP)策略管理点**

创建策略和策略集的系统实体

**Policy-combining algorithm（策略合并算法）**

合并来自多个策略的决策和义务集的过程

**Policy decision point(PDP)策略决策点**

评估匹配的策略并成仙授权决策的系统实体。

**Policy enforcement point(PEP)策略执行点**

通过发起决策请求和执行授权决策而实施访问控制的系统实体。

**Policy information point(PIP)策略信息点**

表现为一个特性集的来源的系统实体

**Policy set（策略集）**

一个策略或策略集集合，一个策略合并算法和（可选的）一个义务或建议集。可能是其它策略集的组合

**Predicate（断言）**

一个可辨真假的语句

**Resource**

数据，服务或系统组件

**Rule（规则）**

一个目标，一个结果，一个条件和（可选的）一个义务或建议集。一个策略组件

**Rule-combining algorithm（规则组合算法）**

合并来自多个规则的决策的过程

**Subject（主体）**

一个行动者，它的属性（attributes）可以被断言引用

**Target（目标）**

定义在规则，策略或策略集上的条件，通过评估资源，主体和动作来鉴别一个请求是否匹配该规则，策略或策略集

## 访问控制语言所应满足的基本要求

为了表达信息系统安全策略，策略语言所应满足的基本要求：

* 提供一个合并多个独立的规则和策略集为一个策略集的方法，以将该策略集应用于具体决策请求
* 提供一个可以灵活的定义合并规则和策略的过程的方法
* 提供一个可以处理多个主体，不同能力的主体的行动的方法
* 提供一个基于主体和资源的特性进行授权决策的方法
* 提供一个处理多值属性（attributes）的方法
* 提供一个基于资源的内容信息进行授权决策的方法
* 提供一个作用于主体，资源和环境的属性上的逻辑的和数学的操作集
* 提供一个处理分布式策略组件集，抽象策略组件的定位，获取和验证的方法
* 提供一个可以基于主体，资源和动作的属性值快速识别给定的策略是否可以应用给定的动作的方法
* 提供一个可以将策略作者和应用环境隔离的抽象层
* 提供一个指定一组动作必须被联合执行的方法