

## 英特尔® 防盗技术评估

- 适用于采用 2010 英特尔® 酷睿™ 博锐™ 处理器的笔记本电脑。
- 如果硬件及存储的数据丢失或被盗，则禁用硬件及数据。
- 提供多层保护，包括防盗监测和将平台与数据轻松恢复至最初状态。

最近，英特尔 IT 部门对 2010 英特尔® 酷睿™ 博锐™ 处理器的笔记本电脑上采用的英特尔® 防盗技术（英特尔® AT）进行了技术评估。

如图 1 所示，英特尔® 防盗技术是一项基于硬件的技术，可帮助监测盗窃行为并在笔记本电脑丢失或被盗时禁用电脑。这项技术有助于保护宝贵的企业数据和知识产权及硬件本身。此外，通过保护数据，即使在加密密钥不可用的情况下，英特尔® 防盗技术也可为全磁盘加密带来更大价值。在英特尔® 防盗技术开发过程中，我们与加密供应商携手合作，旨在帮助确定可满足企业需求的强大功能。

在评估中，我们与英特尔® 防盗技术产品事业部门和供应商合作，基于可行的企业使用案例，在无线 LAN (WLAN)、LAN 及虚拟专用网 (VPN) 上进行了多项特性的测试。在案例中，服务中心技术人员禁用丢失了的笔记本电脑。

评估结果表明，英特尔® 防盗技术能够提高保护公司拥有的笔记本电脑及数据和知识产权的能力。我们计划于近期在移动 3G 网络上对相同的特性进行测试。

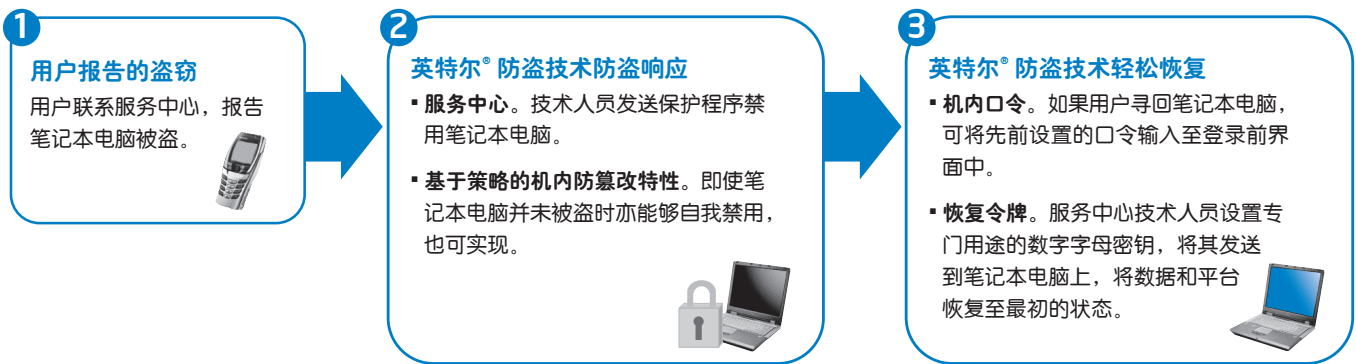


图 1. 英特尔® 防盗技术（英特尔® AT）可帮助监测盗窃并在笔记本电脑丢失或被盗时禁用电脑。

## 业务挑战

每年约有 200 万台笔记本电脑被盗，其中的 97% 的电脑无法寻回。<sup>1</sup> 这表明企业不仅在丢失硬件方面面临着巨大的风险，更重要的是丢失数据和知识产权。

英特尔 IT 部门负责调查丢失或被盗的企业电脑对企业带来怎样的影响。我们对有助于规避这些风险的工具和措施进行了调查，并根据调查结果评估了英特尔® 防盗技术。

## 确定英特尔® 防盗技术的要求和特性

在 2008 年 12 月，我们开始与英特尔® 防盗技术产品事业部合作制定和评估英特尔® 防盗技术。在 2009 年，产品事业部希望我们与加密供应商合作，帮助制定能够使英特尔® 防盗技术在企业环境中发挥更大价值的架构。

我们与供应商召开了一系列面对面的计划会议，来定义企业级要求和功能。这些会议主要针对以下主题：

- 英特尔® 防盗技术控制台以何种方式放置在企业网络中的哪一位置。
- 与访问控制和事件日志有关的安全要求。
- 包括可扩展性在内的企业要求，以便英特尔® 防盗技术能满足众多客户端的要求。
- 用于制定策略和报告的层级管理接口。

此外，这支合作团队还讨论了那些没有将防盗技术通过外部供应商外包或托管防盗服务的企业如何使用英特尔® 防盗技术。

## 技术概述

通过为硬件和存储的数据提供多层保护，英特尔® 防盗技术减少了笔记本电脑被盗和丢失情况。

### 盗窃监测

当用户报告笔记本电脑被盗时，服务中心技术人员向笔记本电脑发送远程盗窃告警，禁用电脑。此外，英特尔® 防盗技术还可利用可编程触发器监测可疑行为，并禁用笔记本电脑。英特尔® 防盗技术通过三种方式发挥作用：

- **用户报告的盗窃。**如果笔记本电脑主人联系服务中心，则技术人员会发送保护程序，禁用笔记本电脑。保护程序的格式是加密的短消息服务（SMS）文本信息，可通过 LAN、WLAN 或 3G 网络发送。
- **利用机内宽限期计时器（grace timer）监控篡改。**在出现可疑活动时，如过度频繁地尝试登陆网络或在输入证书前耗时长于一般时长，则笔记本电脑会利用可编程的宽限期计时器自行禁用。
- **利用机内预约计时器（rendezvous timer）监控篡改。**如果笔记本电脑无法在策略限定的时间内（例如每日）登陆网络，则笔记本电脑会利用可编程的机内预约计时器自行禁用。

英特尔® 防盗技术可阻止操作系统加载，即使在硬盘被更换或格式化的情况下也可实现。此外，即使将硬盘移动到其它系统中时，英特尔® 防盗技术还可禁用对加密密钥的访问，并阻止访问硬盘上宝贵的数据。

### 轻松恢复

禁用的笔记本电脑会显示一条带有联系信息的专门的恢复提示，有助于寻找笔记本电脑的主人。笔记本电脑返回到主人手里后，可利用以下两种技巧中的其中之一，在不损坏硬件和数据的情况下恢复电脑：

- **机内口令。**用户预先设置在特定登录前界面中使用的强口令。
- **恢复令牌。**服务中心技术人员设置单一用途的数字字母密钥并将其提供给用户。

### 防止篡改

英特尔® 防盗技术可提供几种特性，阻止企图避开防盗功能的行为。如果恰当的固件已安装在平台上，而笔记本电脑亦已在中央控制台上注册的话，当在 BIOS 中的英特尔® 防盗技术被激活后，即使在 BIOS 闪烁或互补金属氧化物半导体（CMOS）电池被移除时，该功能也可实现。防篡改功能使盗贼更加困难绕过平台和数据保护。

### 系统要求

英特尔® 防盗技术适用于基于 2010 英特尔® 酷睿™ 博锐™ 处理器的笔记本电脑。

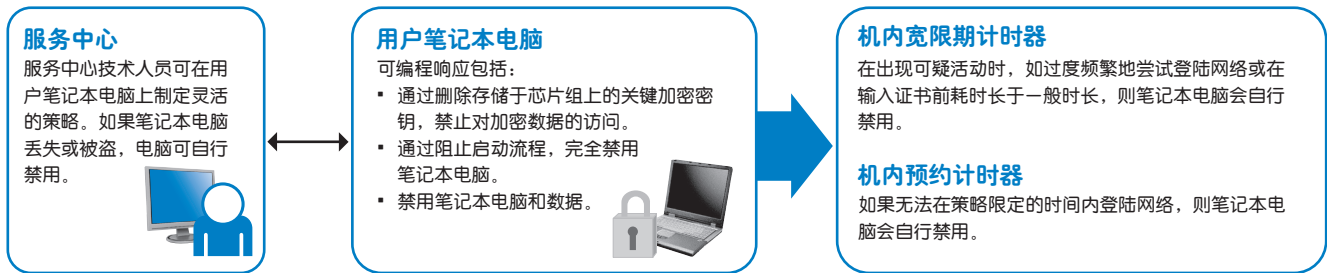


图 2. 英特尔® 防盗技术使服务中心技术人员可以针对笔记本电脑被盗而制定灵活、基于策略的响应措施。

## 技术评估

我们与产品事业部及加密供应商合作，在 WLAN、LAN 和 VPN 上对英特尔® 防盗技术的多种特性进行了测试。此外，我们还集体研究了其它使用案例，如调查支持，并讨论了英特尔® 防盗技术与其它企业安全功能的整合的可能性。

我们的评估基于理论上的使用案例，即用户呼叫服务中心，报告笔记本电脑被盗。服务中心立即响应，技术人员从 IT 管理控制台发送保护程序。通过删除存储在芯片组上的关键加密密钥，保护程序禁止他人访问加密密钥。此外，我们还测试了利用机内口令和远程恢复令牌恢复对加密密钥的访问，从而重新激活已被禁用的笔记本电脑。

## 测试设置和配置

我们在多个系统中成功激活、设定和注册了英特尔® 防盗技术。

- **激活。**我们首先确保每台用于测试的笔记本电脑具有适当级别的 BIOS。然后，我们利用一组配置开关在 BIOS 中启用英特尔® 防盗技术。

- **配置。**我们验证了包含在每台用于测试的笔记本电脑中适当等级的固件。然后，我们在数种版本的客户端操作系统和来自几家 OEM 的笔记本电脑中安装了英特尔® 防盗技术测试代理程序。
- **注册。**通过利用供应商的控制台并连接到英特尔功能许可访问，我们能够获得针对每种安装配置的许可密钥。这个过程可无缝实现。此外，我们还测试了取消注册和重新注册笔记本电脑。

这个过程使我们能够确定使用英特尔® 防盗技术的复杂度等级，并制定出我们的电脑构建团队在获得新笔记本电脑时可以采用的可行流程。

## 特性评估概述

我们成功测试了英特尔® 防盗技术的关键特性。

- **保护程序。**我们模拟了笔记本电脑被盗的情况，用以触发各种英特尔® 防盗技术行为。我们将加密的 SMS 短信发送到“被盗”的笔记本电脑上，禁用电脑。
- **机内宽限期计时器。**我们模拟了一位用户花很长时间输入证书，随后笔记本电脑正如预期的那样会自行禁用。

- **机内预约计时器。**我们模拟了一位用户未在规定时间内登陆，此时，笔记本电脑也会自行禁用。
- **机内口令。**超过宽限期计时器和预约计时器规定时间后，我们利用机内口令使笔记本电脑自行恢复。
- **恢复令牌。**我们模拟丢失或被盗的笔记本电脑被找回，向电脑发送恢复令牌，使数据和平台恢复至初始状态。

此外，我们还测试了通过为宽限期和预约计时器切换策略设置，从测试控制台设置灵活防盗策略的能力，如图 2 所示。例如，一旦笔记本电脑标记为“被盗”，则响应方式可包括：

- 通过删除存储于芯片组上的关键加密密钥，禁止对加密数据的访问。
- 通过阻止启动流程，完全禁用笔记本电脑。
- 禁用笔记本电脑和数据。

我们计划于近期在移动 3G 网络上测试相同的特性和策略设置。

## 结论

英特尔 IT 部门与英特尔® 防盗技术产品事业部及加密供应商的通力合作对于界定英特尔® 防盗技术至关重要。该产品能够提高我们保护英特尔数据和知识产权的能力。

硬盘加密是保护数据安全性的一种重要方法，利用英特尔® 防盗技术使加密密钥不可访问有助于提高加密的价值。借助英特尔® 防盗技术，加密密钥可被远程、自动删除。没有加密密钥，未经授权的用户无法访问

数据。更重要的是，与基于软件的防盗解决方案不同，英特尔® 防盗技术基于硬件，使加密密钥能够在平台恢复的情况下也随之恢复。

## 了解更多信息

如欲了解英特尔® 防盗技术的更多信息并观看演示，请访问：

[www.intel.com/technology/anti-theft](http://www.intel.com/technology/anti-theft)

如欲与英特尔 IT 高管针对本文主题进行直接对话，请访问：[www.intel.com/it](http://www.intel.com/it)

## 作者

Dennis Morgan

英特尔 IT 部门安全战略师

Alan Ross

英特尔 IT 部门首席高级工程师

Tarun Viswanathan

英特尔 IT 部门安全架构师

## 缩写词

CMOS 互补金属氧化物半导体

Intel® AT 英特尔® 防盗技术

SMS 短信服务

VPN 虚拟专用网

WLAN 无线局域网

<sup>1</sup> Evers, Joris, “应对笔记本电脑丢失” (Getting over laptop loss)。CNET News, 2006 年 6 月 30 日。[http://news.cnet.com/Getting-over-laptop-loss/2100-1044\\_3-6089921.html](http://news.cnet.com/Getting-over-laptop-loss/2100-1044_3-6089921.html)

任何电脑系统都不能在所有情况下提供绝对的安全性。英特尔® 防盗技术 (英特尔® AT) 需要电脑配置支持英特尔® AT 的芯片组、基本输入输出系统 (BIOS) 和固件版本，安装支持英特尔® AT 的服务提供商/ISV 应用和订阅服务。检测 (驱动)、响应 (行动) 和恢复机制仅在激活和配置英特尔® 防盗技术功能后才能正常运行。一些 ISV 或服务提供商可能不提供某些功能，某些功能可能仅面向部分国家提供。英特尔不负责承担数据和/或系统丢失或被盗责任，以及因上述情况导致的任何其它损失。

本篇仅用于参考目的。本文件以概不保证“方式”提供，

英特尔不作任何形式的保证，包括对适销性、不侵权性，以及适用于特定用途的担保，或任何由建议、规范或范例所产生的任何其它担保。英特尔不承担因使用本规范相关信息所产生的任何责任，包括对侵犯任何专有权的责任。本文不代表英特尔公司或其它机构向任何人明确或隐含地授予任何知识产权。

英特尔、Intel 标识、Intel Core、英特尔酷睿、Intel vPro 和英特尔博锐是英特尔公司在美国和其他国家 (地区) 的商标。

\*文中涉及的其他名称及商标属于各自所有者资产。

版权所有 © 2010 英特尔公司。保留所有权利。

