思科为行业领先制造商打造邮件安全解决方案

执行摘要

小松公司简介

总部所在地：日本东京

业务性质：全球工业设备及工业车辆制造商

2007 年收入：净销售总额 16 亿美元

员工人数：33836（雇员）；6231（独立员工）

CISCO IRONPORT 的优点

- 通过功能强大的邮件安全设备和安全管理设备，提供主动和被动威胁防御及管理功能
- 提供专为小松公司及其分公司配置的 Cisco IronPort C350 邮件安全设备，实现出色的安全性和可靠性
- 部署后不到一周，检测到的垃圾邮件数量即增加了约 75%
- 支持无缝的管理和更新，不仅减轻了管理负担并减少了停机时间，而且实现了较低的拥有低成本

概述

总部位于东京的小松有限公司是一家领先的全球制造商，其业务涉及建筑设备、采矿设备、工业机械及工业车辆等诸多领域。该公司最近与思科®建立了合作关系，准备实施积极而全面的解决方案，来保护其庞大的电子邮件网络免于受到垃圾邮件、病毒及相关威胁的影响。

客户背景

2004 年，日本开始对流入或流出组织的敏感信息实施更严格的监管审查规定（包括出台日本版的《萨班斯-奥克斯利法案》）。在此大环境下，小松公司对全公司的邮件安全和威胁阻拦能力进行了积极评估，以确保最大限度地满足法规要求。

研究显示，该公司的垃圾邮件防御能力不断下降。2005 年，小松公司曾选择一家安全供应商来帮助公司应对这一日益突出的问题。但是，该供应商的解决方案无法提供准确而有效的检测和保护。到 2007 年夏季，小松公司日本国内公司收到的垃圾邮件数量已呈指数级增长：从 2005 年的每天约 4 万封增加到每天 20 万封。这导致最终用户收到的欺诈邮件大幅增加。

更糟的是，一些病毒以垃圾邮件附件或邮件内嵌 URL 的形式进入网络。该公司当时的安全系统无法及时自动删除新出现的病毒码文件，防止病毒扩散。这迫使小松公司不得不与其安全供应商签订一份新协议，要求对方提供更高级别的安全服务，包括提供免疫程序软件以及全天候的客户服务和系统支持。

> “通过实施 Cisco IronPort 产品，我们获得了很好的效果。我们感到非常满意。”
>
> **— Kenichi Tabata，小松公司部门主管**

技术挑战

最终，小松公司意识到，要防御基于邮件的威胁，必须使用更全面的解决方案，而不能只是一味地碰到问题解决问题。该公司确定，他们需要的解决方案必须具有同类最佳的威胁检测率，而且能在病毒出现时立即加以识别和防御。

小松公司部门主管 Kenichi Tabata 指出：“面对急剧增加的垃圾邮件，信息安全（曾经）是一项严峻的挑战。我们对（过去使用的）垃圾邮件检测率较低的产品不太满意。所以我们决定考虑实施新的解决方案。我们也希望能在得到定义文件之前隔离带有可疑附件的邮件。”

Cisco IronPort 的优点

经过全面的研究，小松公司最终选择思科作为新的邮件安全供应商。他们决定使用经过验证的强大 Cisco IronPort® C350 邮件安全设备为其提供高级威胁防御和垃圾邮件拦截功能，并帮助其轻松实施公司策略。Cisco IronPort C350 专为满足具有子公司的中型企业的邮件安全需求而设计，它结合使用主动和被动方法来抵御垃圾邮件。Cisco IronPort 信誉过滤器可提供实时威胁评估，并能识别可疑发件人。Cisco IronPort 反垃圾邮件技术可部署一个功能强大、独一无二的扫描引擎，用于检查每封邮件的完整情景信息，从而在最大范围阻止各种威胁危害用户。此外，Cisco IronPort 垃圾邮件隔离功能为最终用户提供了一个用于放置垃圾邮件的安全区域，该隔离区可以轻松与现有目录和邮件系统集成。

© 2010 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

安装 Cisco IronPort C350 邮件安全设备后仅仅一周，小松公司每天检测到的垃圾邮件数量就从 20 万增加到 34.6 万。这一成果使最终用户对该技术十分满意，也很快建立了信任。

Cisco IronPort 爆发过滤器是该邮件安全设备的另一个强大功能。这些过滤器为小松公司提供了关键的第一道防线，可准确检测并自动隔离可疑的邮件附件（通常比传统的病毒特征码正式发布还要早数个小时）。完全集成的 Sophos 和 McAfee 反病毒技术可提供额外的防御，帮助确保防患于未然。

Cisco IronPort C350 还提供集成的合规性过滤器，可防御有碍合规性的威胁；其高级加密功能可保护机密数据并满足客户的监管要求；它还能隔离被内容扫描引擎标记为可疑邮件的邮件。

先进的邮件身份验证和整个企业范围的管理工具有助于用户清楚了解出现的威胁。这不仅减轻了处理问题邮件的管理负担，而且通过将邮件操作和安全保护整合到单一平台而降低了成本。通过作为网络网关的缓冲器，保护用户免受垃圾邮件、病毒及相关问题的威胁，这些设备还有助于提高工作效率。

此外，通过实施 Cisco IronPort M650 安全管理设备，小松公司能够灵活而全面地在其网关控制与 Cisco IronPort 邮件安全设备相关的所有政策、报告和审计信息。该集中报告功能使管理员可以整合来自多个安全设备的流量数据，获得完全集成的报告。

小松公司部门主管 Kenichi Tabata 表示：“在思科的帮助下，我们不仅大大降低了总拥有成本，而且成功获得了有效防御病毒和垃圾邮件的新功能。通过实施 Cisco IronPort 产品，我们获得了很好的效果。我们感到非常满意。”

本文档于 2008 年 1 月首次发布。在经过有限的非重大更新后，于 2010 年 8 月再次发布。

美洲总部
Cisco Systems,Inc.
加州圣荷西

亚太总部
Cisco Systems(USA)Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

Cisco 在全球设有 200 多个办事处。思科网站 **www.cisco.com/go/offices** 中列出了各办事处的地址、电话和传真。

Cisco 和 Cisco 徽标是 Cisco Systems, Inc. 和/或其附属公司在美国及其他国家/地区的商标。在 www.cisco.com/go/trademarks 上可查看思科商标列表。提及的第三方商标为其相应所有者的财产。使用“合作伙伴”一词并不暗示思科和任何其他公司存在合伙关系。(1005R)

美国印刷 C36-599562-00 10/10

© 2010 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。