客户案例

东京证交所上市之金融机构

Bloombase® Spitfire StoreSafe™
安全存储服务器

Bloombase® Spitfire KeyCastle™
密钥管理服务器

Bloombase® Spitfire™ 高可用性模块

日本个人信息保护法 (PIPA) 早已于 2005 年 4 月 1 日生效，对日本公司提出了极为严格的信息保密要求。一家日本金融机构于是采用 Bloombase® Spitfire StoreSafe™ 存储加密解决方案，克服政府的严峻考验，成功对其分布式子系统进行信息保护，以低成本、高容错的数据服务，确保客户信息的私密和安全。

项目背景

客户背景

- 于东京证券交易所上市金融机构
- 员工: 6,000 人以上

项目简介

严格遵守日本个人信息保护法 (PIPA) 要求，为东京的生产系统及大阪的灾难恢复 (DR) 存储子系统中保护客户个人信息。

主要挑战

- 不改变最终用户、管理员及操作员使用流程
- 支持 Microsoft Active Directory
- 敏感信息的物理存储需全方位加密，不容存在任何非加密的物理存储原文件或拷贝
- 确保灾难恢复 (DR) 数据中心的操作员无从读取存储数据
- 备份文件同样需要加密
- 支持透明的数据服务故障保护
- 兼容同步存储实时数据复制服务
- 高性能的加密与解密

概述

该东京证交所上市金融机构通过租用的广域网专线，分别在东京和大阪托管一个核心业务数据中心，及灾难恢复 (DR) 中心，支撑日本各地 6000 多名员工的日常业务操作。核心支撑系统包涵一个客户记录及查询子系统，存储着客户的姓名、社会身份、银行帐户信息、交易历史以及信用信息。

东京的客户数据库主系统存储着 100 万个客户记录，数据总量超过了 1 兆兆字节，且需要实时与灾难恢复 (DR) 系统进行数据复制，一旦主数据中心出现故障，灾难恢复 (DR) 系统可以取而代之，实现不间断的业务运作。

根据 2005 年 4 月 1 日生效的日本个人信息保护法 (PIPA)，任何个人信息管理者，即利用超过 5,000 个人的个人信息来开展业务的公司，都必须保证个人信息受到保护及保密，其中个人信息指有关个人的任何信息。

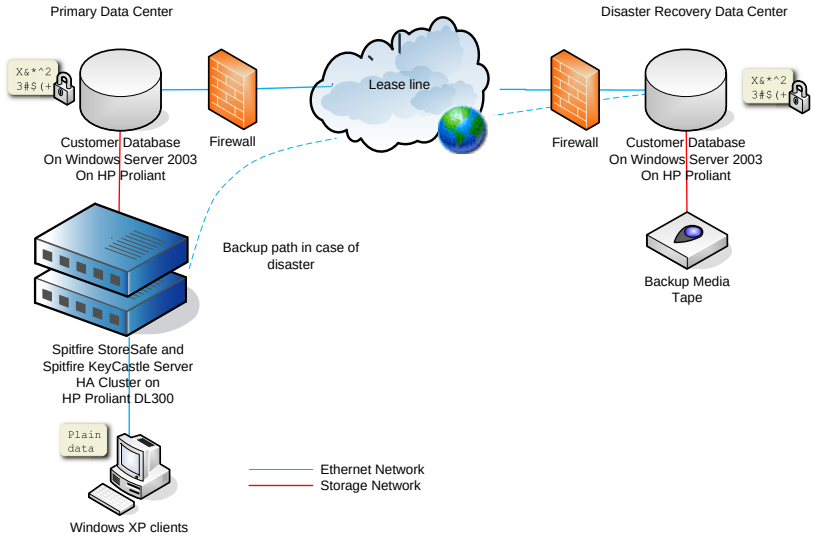
个人信息管理者必须遵守有关个人信息管理的一系列限定，包括有关向第三方提供、披露、信息修正以及限制性个人信息的暂停使用等各方面。如发生信息外泄且未能如实报告，个人信息管理者的负责人最多可被判处最长 6 个月的监禁或最高 30 万日元的罚款。

除个人信息保护法外，企业客户还要符合日本金融厅的要求 (FSA)，确保其客户信息私密受到严密

BLOOMBASE®
博隆兴中

保护。日本金融厅的指导纲要要求金融机构汇报个人信息外泄事件，并提出防止外泄再次发生的措施。

数据安全对金融机构至关重要，在最坏的情况下，一旦客户信息丢失，公开通告令尴尬之余，势必影响机构的声誉、客户的信心，还有最要命的股价。灾难恢复 (DR) 中心是外包给第三方的。如何既能保护客户私密信息不被第三方操作人员读取，同时又能让他们正常进行系统维护及日常备份操作，这是核心数据安全项目面临的最大挑战。



开放式的平台　高安全的加密

最终用户需要在东京之外有一个备份中心，确保在电力、硬件故障或恶意攻击发生时可以实现不间断的业务运作，但潜在的客户信息泄露风险令他们感到为难。客户要求其数据可以实时备份到灾难恢复 (DR) 中心，不仅网络渠道的信息需要加密，两个数据中心的 Microsoft Windows 存储子系统同样要受到保护。在实现高度的信息私密性及完整性的同时，还要让第三方灾难恢复 (DR) 数据中心的操作员可以透明地完成日常的备份、恢复及存储分配工作，就像没有任何加密一样。

通过 Bloombase Spitfire StoreSafe 企业存储加密解决方案，客户部署了含 Spitfire High Availability (HA) 的 Spitfire StoreSafe 双节点集群，对实时有线存储数据进行可容错的加密及解密。在正常情况下，Spitfire StoreSafe 集群作为客户东京主站数据库的存储代理，按需求自动对数据进行加密保护，并通过租用专线对大阪灾难恢复 (DR) 站的备份存储子系统进行客户信息更新。一旦主站发生数据服务故障，备份存储取而代之，经过 Spitfire StoreSafe 的加密保护，继续提供高可用性的数据服务。

灵活的加密保护　满足客户需求

机密客户数据通常存储在物理磁盘上，管理员及操作员若想不破坏加密来读取这些数据，在技术上是不可能做到的。经过 Spitfire StoreSafe 加密的客户数据文件，存储在 Windows NTFS 格式的磁盘上，并且支持原有数据复制、备份及恢复设备的访问，无需昂贵的软件投入、培训或运行步骤。

最终用户可以轻松地访问客户数据库，就像没有任何加密一样。灾难恢复的用户流程大大简化，当机时间从 1 小时最大程度地缩减到了 5 分钟以内。

更多信息

如需了解更多关于 Bloombase 银行及金融安全解决方案的信息，请联络您的 Bloombase 销售代表，或访问我们的网站 ：

www.bloombase.com

项目目标

- 保护存储在 Windows 文件服务器上的客户机密数据的私密性和安全性
- 为备份文件进行加密，确保信息私密、安全
- 经过加密的存储数据可及时备份至当前

方案与服务

- Spitfire StoreSafe™ 企业存储安全服务器
- Spitfire KeyCastle™ 密钥管理服务器
- Spitfire 高可用性模块

选择 BLOOMBASE 的理由

- 直接支持 Microsoft Windows 2003 Server 平台
- 在银行、金融及政府机关实时关键数据存储系统加密保护方面拥有多个成功案例
- 易于部署
- 数据所有权与操作权完美分离
- 高速、自动化的加密与解密

项目实施特点

首次通过广域网 (WAN) 在远程 Windows 文件服务器上部署高可用性模式的 Spitfire StoreSafe 加密保护

主要优点

- 满足个人信息保护法要求
- 增强了数据可用性及安全性
- 无需培训第三方数据提供商维护人员
- 高可用性、高容错性
- 高性能的加密保护
- 透明的故障保护

硬件

- HP Proliant DL320 系列服务器
- HP Proliant DL380 系列服务器

操作系统

- Microsoft Windows Server 2003

© 2006 Bloombase, Inc. 版权所有。Bloombase, Spitfire, Keyparc, StoreSafe 及其它 Bloombase 产品与服务及相关标识均为 Bloombase, Inc. 在美国、中国、香港及全球其它几个国家的商标或注册商标。所有其它产品名称均为其所属公司的商标。

本文档所含信息可以在不经通知的情况下随时更改。Bloombase 产品与服务仅遵循其附带的书面保证声明。本文件所含任何信息均不作为额外的产品与服务保证。Bloombase 不对本文档可能包含的任何技术或编辑性错误或遗漏承担责任。

4AA0-0838AAA 09/2006

BLOOMBASE® 博隆兴中