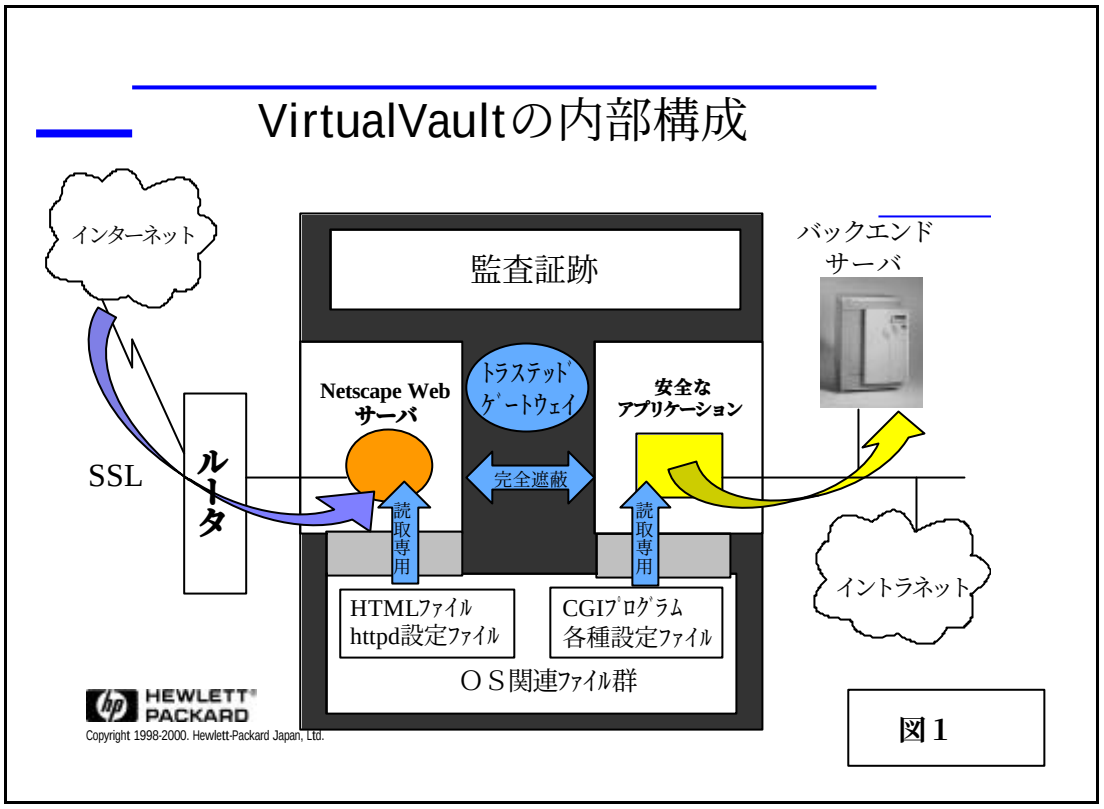

製品概要

最強のセキュリティを約束する、ＯＳ一括型のＷｅｂサーバ・ソフトウェア製品で、HP-UXの動作するサーバ各機種に対応しています。（一部の旧型機種ではサポートされませんので対応機種についてはお問い合わせください）

製品特長

① ＯＳからＷｅｂまでの一括インストール
② ISO15408 のソースの１つである TCSEC-BLS 強度の改ざん防止能力を装備
③ シンプルな運用管理ＧＵＩを装備

特長１：ＯＳ一括型

通常、Ｗｅｂサーバ構築では、プラットフォームとして使うＯＳをインターネットで安全に使えるようにするＯＳ設定作業に多くの知識を要し手間がかかります。
これは、Ｗｅｂサーバのプラットフォームに汎用のＯＳを使うためで、それらのＯＳは、安全なイントラネットに接続されることを想定してネットワーク・レディ（ネットワークがすぐに使える状態）に初期設定されているからです。その方がイントラネットで使うには、手間いらずとなるためよいのですが、インターネット・サーバとして使うときには、逆にそのことが裏目に出てしまいます。

VirtualVault のインストールでは、ディスクの初期化から始まり後述する高信頼性ＯＳと Netscape Enterprise Server を一括してインストールすることができます。ＯＳは、危険なインターネットに接続されることを想定して、Ｗｅｂサーバとして必要のないサービスをすべて禁止の状態で初期化してあります。

Copyright © 2000 by Hewlett Packard

ＯＳをインストール後に、ＯＳに必要なセキュリティ設定を施し、Ｗｅｂサーバとして必要のないＯＳサービスなどを手作業で停止してから、Ｗｅｂサーバソフトをインストール、設定するという従来わずらわしかった手間がかかりません。

特長２：軍用の超強力セキュリティを搭載

VirtualVault では、そのＯＳとして、Ｂレベルと呼ばれる高信頼性ＯＳを使用しています。それはＯＳ内の資源を間仕切りする機能を備えています。
標準ＯＳ（Unix や WindowsNT）がファイルやディレクトリを保護するのに READ や WRITE のパーミションを設定できるのに加えて、高信頼性ＯＳではＯＳ資源を目的別の個室を区切って、その中で管理することができます。その意味では、標準ＯＳは共有の１つの部屋の中にすべての資源が混在していることになります。高信頼性ＯＳでは、ある個室から他の部屋にアクセスすることは、部屋と部屋の間に設ける間仕切りの種類によって制限できます。特に VirtualVault が採用しているのは、Ｂレベルを上回るＣMW仕様のＯＳで、間仕切りに２種類のタイプを装備しています。
１つは、部屋間を完全に分離するコンクリートのような壁で、隣りの部屋に何が存在するかすら確認できません。もう１つは、ガラスのような壁で、ある部屋から他方を参照することはできますが書き換えることはできません。つまり、読み取り専用にすることができます。この時ガラスの強度は、あたかもＣＤ－ＲＯＭをマウントしているようなもので、書き込みはファイルごとのパーミッションとは無関係に不可能です。

VirtualVault では、図１のように外部ネットワークと内部ネットワークをコンクリートの壁で完全に分離し、また、ＷｅｂやＣＧＩプログラムなどに対してＯＳやＨＴＭＬファイル、設定ファイルなどをガラスの壁で囲うことで読み取り専用にしています。
ＯＳやＨＴＭＬファイル、ＣＧＩプログラムファイルなどはＣＤ－ＲＯＭに存在するようなことを想像していただければよいと思います。
従って、ＷｅｂサーバやＣＧＩプログラムにセキュリティの問題が発生しても、ＨＴＭＬや大切な設定ファイル、ＣＧＩプログラムへの不正な改ざんを防ぐことができるのです。

特長３：運用管理は、シンプルなＧＵＩ

これまでの説明からすると、運用や管理に難しい知識や操作が必要になると思われるかもしれませんが、VirtualVault はＷｅｂサーバに特化することで、シンプルで平易な運用管理用のＷｅｂブラウザベースのＧＵＩを標準提供しています。
たとえば、マシンのシャットダウンのためにネットワーク経由でリモート・ログインする必要はなく、ＷｅｂのＧＵＩからシャットダウンのアイコンをクリックするだけです。
逆にこのようにすることで、運用担当者に自由な操作をさせず、Ｗｅｂの運用に必要最小限の操作だけを許可することで、担当者による操作ミスや不正操作を抑止することができます。
また、運用担当者はＷｅｂブラウザから操作するため、Ｗｅｂサーバの設定により担当者の認証強度を自由に設定できます。ユーザ名、パスワードだけで認証するのか、クライアント証明書を要求するのかなどで強度を選ぶこ

Copyright © 2000 by Hewlett Packard

とができるのです。

典型的なネットワーク構成

VirtualVault を導入する場合の典型的なネットワーク構成を図２に示します。

インターネット接続構成においては、企業内からインターネットへのアクセスが必要なため、それにはファイアウォールを用います。ただし、逆向きのアクセス、すなわち、インターネットから企業の内部に向かってのアクセスをファイアウォールに少しでも許すことは危険なので、その部分に VirtualVault を導入することができます。
典型的にはファイアウォールと VirtualVault を並列に構成するだけです。
これにより、外から内向きの専用ソリューションとして VirtualVault を配置することで、ファイアウォールは内から外向き専用として設定できるようになり、危険な逆向きのアクセスを許可する必要がなくなります。
したがって、VirtualVault はファイアウォールを置き換えるものではなく、ファイアウォールの「穴」をうめることができるようにするものなのです。

納入実績と利用例

VirtualVault のこれまでの納入実績は全世界で１２０サイト以上のインターネット・バンキング（９９年末で７０%シェア）で導入されていますが、説明からわかるようにＷｅｂをフロントエンドとして機密情報を保護したい場合には、金融に限らず、あらゆるところで導入することができるものです。さらにインターネットに限らず、社内の極秘情報などのように社内 LAN からの不正アクセスにセキュリティ対策を施したい場合には、社内 LAN に対して VirtualVault の外側ネットワークを接続して使うことができます。
また、アプリケーションをともなわず、ただ単にホームページだけを絶対に書き換えられたくないという場合にも、簡単にインストールできるＷｅｂサーバとして、VirtualVault を使っていただくことができます。

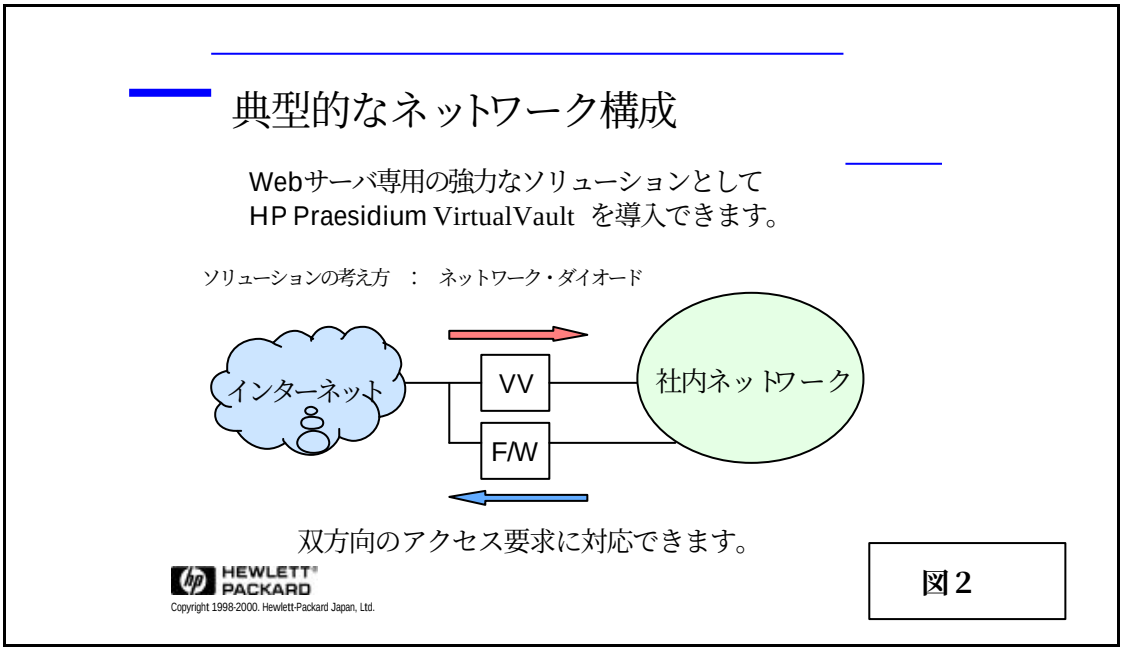

図２

Copyright © 2000 by Hewlett Packard Japan, Ltd.

（日本ヒューレット・パッカード 佐藤慶浩）

Copyright © 2000 by Hewlett Packard