

Part 2: Windows Server 2003とIIS6の技術的特長 ～ネットワークとセキュリティ機能～

マイクロソフトプロダクトディベロップメントリミテッド
野坂 昌己 (masakino@microsoft.com)

このセッションの目標

- Windows Server 2003およびIIS6を使い、WWWサーバを立ち上げるために必要な情報をご紹介します
- IIS6の特徴と新機能をご紹介します

アジェンダ

- Windows Server 2003およびIIS6におけるセキュリティについて
- IIS6のスケールビリティについて
- 高可用性および高信頼性について
- IIS6の運用方法について

一般的に、Webサーバに求められるものは？

セキュリティ

ある意味最もホットな問題。最初からセキュアであることが望ましいが、現実的には如何に日々セキュリティを向上させていけるか、が問題

スケーラビリティ

水平方向への拡張性の容易さ(Scale Out)
垂直方向への拡張性の容易さ(Scale Up)

高可用性、高信頼性

24x7 無停止。No Single Point of failure.
一部のコンポーネントの問題が全体に影響を及ぼさない

運用、管理の容易さ

必ずしもHigh Skillのエンジニアが常時管理できるわけではない。管理の自動化。ヘルスマニタ

SD3+Communication

Secure by Design

- バッファオーバーフローの防止
- 設計の段階からセキュアであること

Secure by Default

- 最初の導入時からセキュアであること

Secure by Deployment

- 実環境へのセキュアな展開

Communication

- Windows Update
- White Paper
- MSAD
- マイクロソフトからの情報の開示

Secure by Design

Secure by Design

- バッファオーバーフローの防止
- セキュリティ保護されたASP
- IISワーカープロセスは低い権限で実行されます

Secure by Default

- IISはWindows Server 2003にデフォルトではインストールされません。
- IISはロックダウンされた状態で出荷されます。
- Windows Serverをアップグレードした場合、IISは無効になります

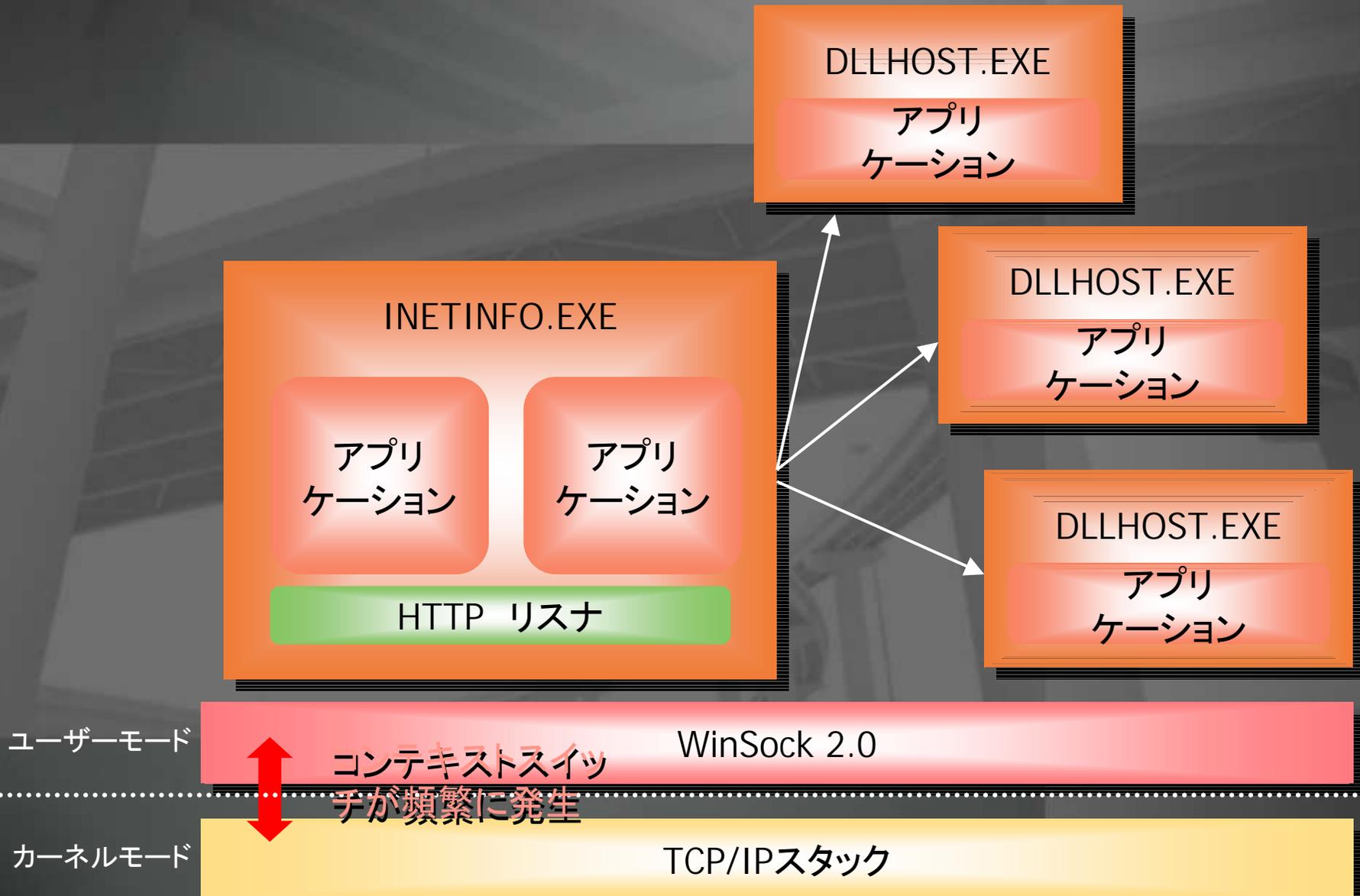
Secure by Deployment

- グループポリシーを介したIISの無効化が可能です
- 六つの基本方針

Communication

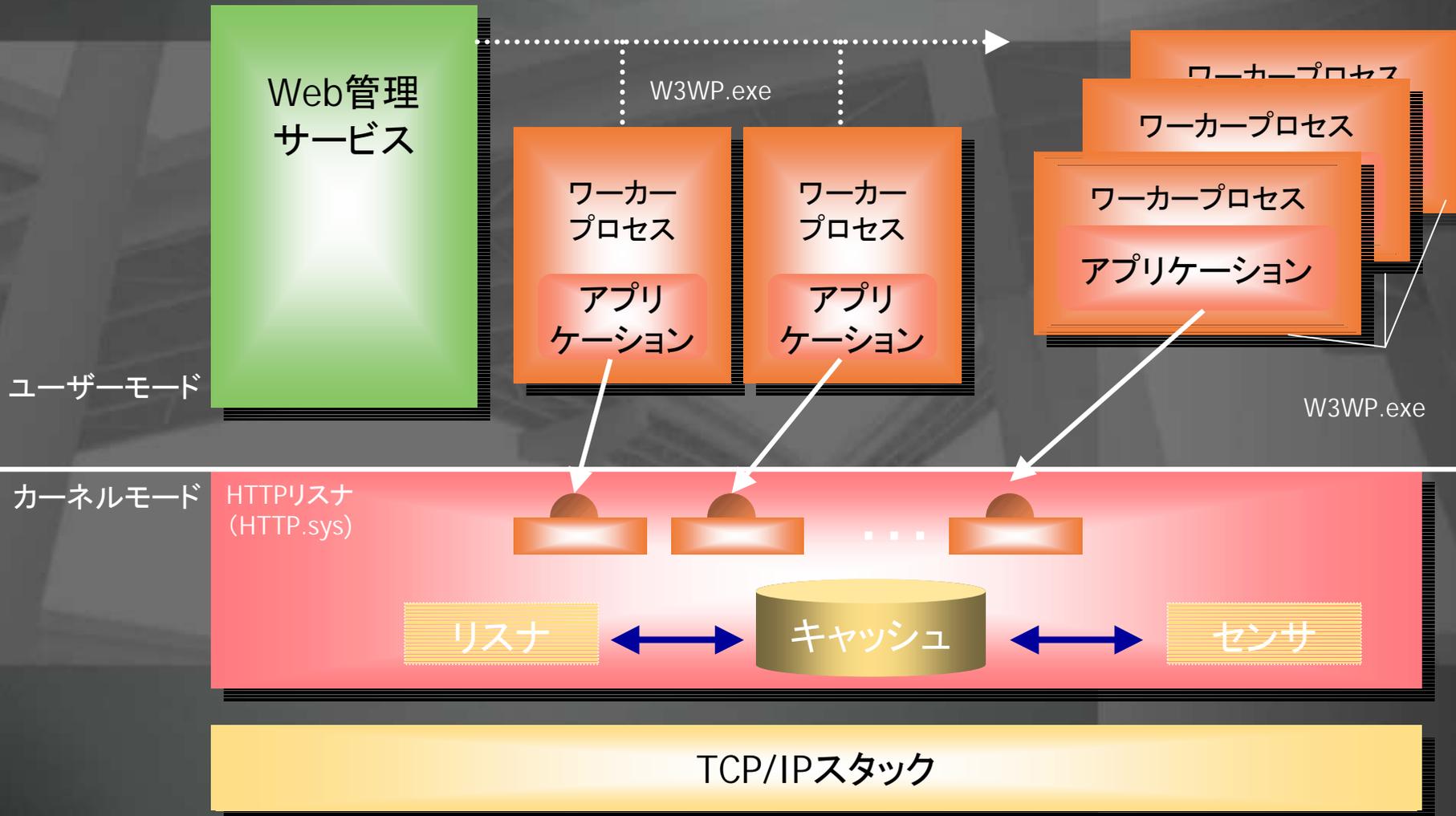
- Windows Update
- White Paper
- Knowledge Base
- MSDN

IIS5の構造



IIS6の構造

Webガーデン



Secure by Design

- 3rd ベンダーアプリケーションを含め、Webアプリケーションは全てワーカープロセス内で動作し、他のワーカープロセス及びその中で動く他のアプリケーションに影響を及ぼさない
- 内部のデータ構造の見直し
- 内部および外部のエンジニアによるコードレビュー
- ツールによるコードのチェック(PREfix/PREfast)
- ワーカープロセスはデフォルトで、低い権限で動作する

Secure by Default

Secure by Design

- バッファオーバーフローの防止
- セキュリティ保護されたASP
- IISワーカープロセスは低い権限で実行されます

Secure by Default

- IISはWindows Server 2003にデフォルトではインストールされません。
- IISはロックダウンされた状態で出荷されます。
- Windows Serverをアップグレードした場合、IISは無効になります

Secure by Deployment

- グループポリシーを介したIISの無効化が可能です
- 六つの基本方針

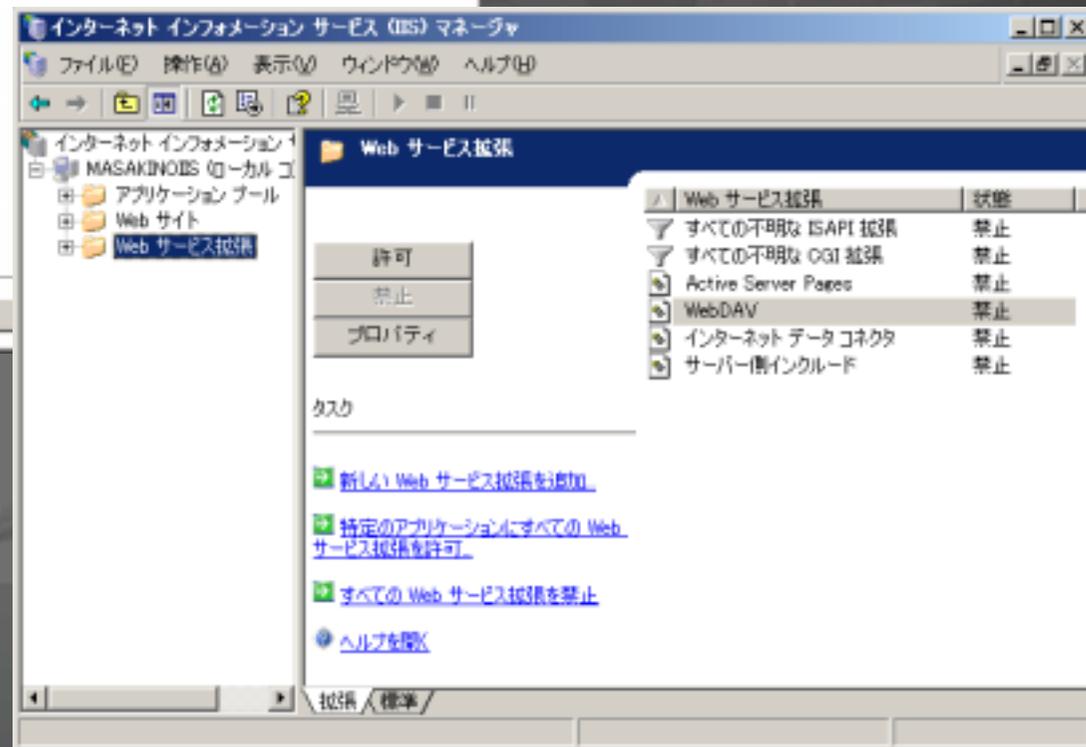
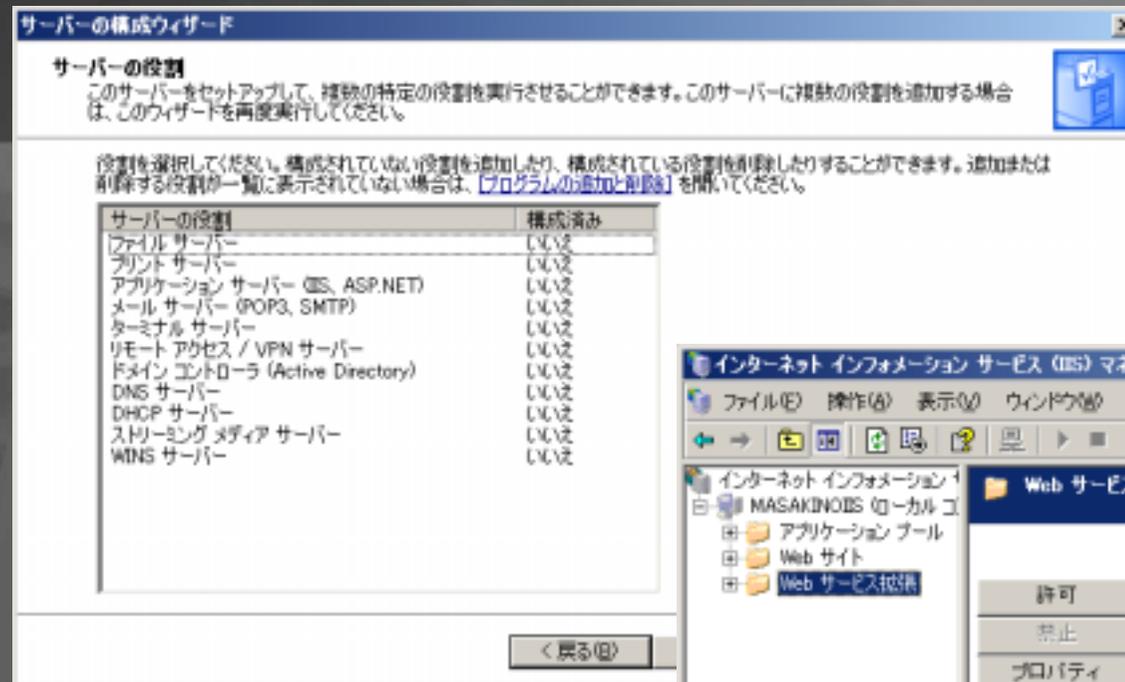
Communication

- Windows Update
- White Paper
- Knowledge Base
- MSDN

Secure by Default

- IIS6はデフォルトではインストールされません
- IIS6をインストールしてもデフォルトでは静的コンテンツのみサポートします
- FrontPage等の拡張機能を有効にするには、必要に応じて追加インストールの必要があります
- Windows 2000 Serverからアップグレードした場合でも、アップグレード直後はIIS6は無効になっています
- IIS6のワーカークロセスは低い権限で動作します

ロックダウンされた状態で出荷



IIS5と比べると？

IIS コンポーネント	IIS 5.0 clean install	IIS 6.0 clean install
静的ファイルサポート	有効	有効
ASP	有効	無効
Server-side includes	有効	無効
Internet Data Connector	有効	無効
WebDAV	有効	無効
Index Server ISAPI	有効	無効
Internet Printing ISAPI	有効	無効
CGI	有効	無効
Frontpage Server Extensions	有効	無効
Password Change Functionality	有効	無効
SMTP	有効	無効
FTP	有効	無効
ASP.NET	X	無効
BITS	X	無効

注意 !!

- CGIなどの動的コンテンツは初期インストール状態では使用できません。明示的に有効にする必要があります。
- 静的コンテンツであっても、拡張子が登録されていない場合、HTTP Error 404が返されます。

Secure by Deployment

Secure by Design

- バッファオーバーフローの防止
- セキュリティ保護されたASP
- IISワーカープロセスは低い権限で実行されます

Secure by Default

- IISはWindows Server 2003にデフォルトではインストールされません。
- IISはロックダウンされた状態で出荷されます。
- Windows Serverをアップグレードした場合、IISは無効になります
-

Secure by Deployment

- グループポリシーを介したIISの無効化が可能です
- 六つの基本方針

Communication

- Windows Update
- White Paper
- Knowledge Base
- MSDN

Secure By Deployment

六つの基本方針

1. Webサーバの脆弱な面を減らす
2. Webサイトとアプリケーションに対する認証されていないアクセスを防止する
3. Webサイトとアプリケーションをできるだけ分離する
4. 適切なユーザ認証を使う
5. 重要なデータは暗号化してやり取りする
6. 日々Webサイトとアプリケーションをセキュアにするようにメンテナンスする

Webサーバの脆弱な面を減らす

- 本当に必要なWindows Server 2003のコンポーネントとサービスだけをインストールする
- 本当に必要なIIS6のコンポーネントとサービスだけをインストールする
- 本当に必要なWebサービス拡張だけを有効にする
- 本当に必要なMIMEタイプだけを有効にする
- Windows Server 2003をセキュアに設定する

Webサイトとアプリケーションに対する 認証されていないアクセスを防止する

- WebコンテンツはOSとは独立したディスクボリュームに格納する
- IISのWebサイトパーミッションを適切に設定する
- IPアドレス、もしくはドメイン名に対する制限を使う
- NTFSのファイルパーミッションを活用する

Webサイトとアプリケーションをできるだけ分離する

- アプリケーションの互換性の観点から偽装の効果を評価すること
 - ASPアプリケーションに対する偽装の振る舞いを特定しておく
 - ASP.NETアプリケーションに対する振る舞いを選択する
- Webサイトとアプリケーションをできるだけ個々に分離するように設定する

適切なユーザ認証を使う

- Webサイト認証を設定する
- Web認証の方式を選択する

重要なデータは暗号化してやり取りする

- SSLを使う
- IPSecその他のほかのVPNを使う

日々Webサイトとアプリケーションをセキュアにするようにメンテナンスする

- 最新のセキュリティパッチを適用する
- Windows Server 2003のセキュリティログを有効にする
- Webサイトのコンテンツに対するファイルアクセス監査を有効にする
- IISのアクセスログを適切に設定する
- セキュリティポリシー、プロセス、手順を定期的にレビューする

一般的に、Webサーバに求められるものは？

セキュリティ

ある意味最もホットな問題。最初からセキュアであることが望ましいが、現実的には如何に日々セキュリティを向上させていけるか、が問題

スケーラビリティ

水平方向への拡張性の容易さ (Scale Out)
垂直方向への拡張性の容易さ (Scale Up)

高可用性、高信頼性

24x7 無停止。No Single Point of failure.
一部のコンポーネントの問題が全体に影響を及ぼさない

運用、管理の容易さ

必ずしもHigh Skillのエンジニアが常時管理できるわけではない。管理の自動化。ヘルスマニタ

スケーラビリティ

- アクセスが増大してもパフォーマンスを落とすことはできない。
- パフォーマンスの劣化は、ビジネスチャンスの喪失につながりかねない
- 最初から多大な投資をすることは難しい。パフォーマンスとコストのバランスが重要
- では、アクセスの増大に伴いコストリスクを低減し、如何にスケーラビリティを確保するのか？

水平方向と垂直方向の拡張性

- 64bit CPU
- Itanium 2/Athron64
- SMP

- 64bit版Windows Server 2003
- Datacenter Edition SMP MAX 32 CPU

- 台数が増えるため、運用コストが上がる場合もある。
- ただし、運用の仕方によっては、運用コストは低く抑えることができる場合もある。
- システム全体として強固な構成にできる
- そもそも台数を分ける構成ができない場合だってある

- 新規に導入する場合、一般にマシンの調達コストが上がる傾向がある。
- CPUを増設する場合など、逆にアップグレードコストを低く抑えることができる場合もある。
- 台数を少なくできるので、運用コストが下がる場合もある。
- 一台落ちると全部ダメ。クラスターとの併用も考慮に

- NLB
- Web Edition
- MSCS

- L4 switch
- DNS round robin
- Reverse Proxy
- Network Load Balancer (NLB)

DNS ラウンドロビンによる負荷分散

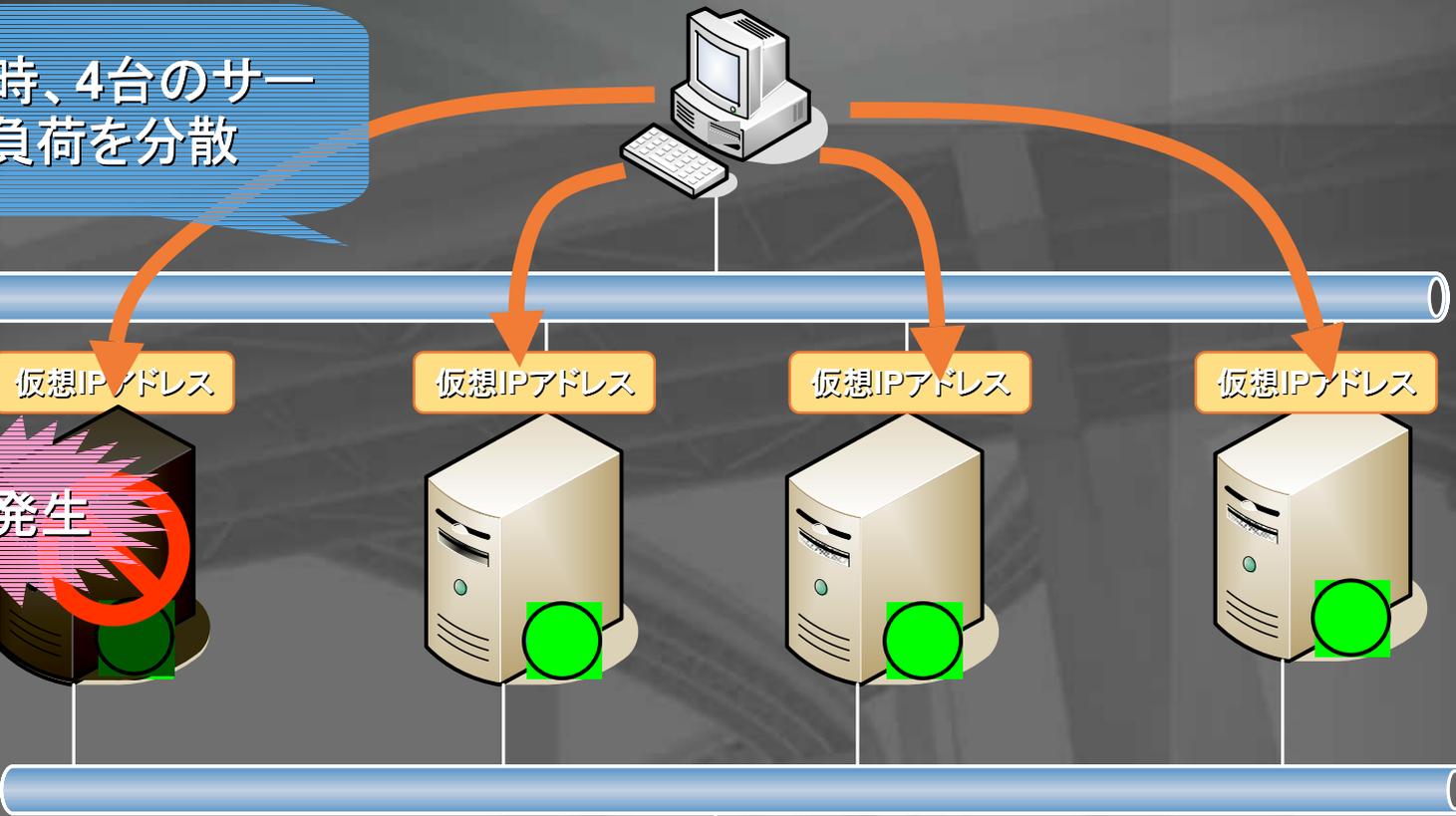
- 最も安価に負荷分散が可能
- 均等な負荷分散は難しい
- N台中の1台が故障した場合、 $1/N$ の確率で依然そのサーバへのアクセスが続くため、冗長性の向上にはならない。
- ゾーン情報を更新してもそれが伝播するには時間がかかる

L4/L7 switchによる負荷分散

- スイッチ自体が高価
- スイッチ自身の冗長性をどうするのか？
VRRPとかを使うのか？
- L7スイッチの場合、アプリケーションやパケットの内容に依存した処理を行うことができる
- L7スイッチの場合、スイッチの処理の負荷も高くなるかもしれない

NLBによる負荷分散

通常時、4台のサーバで負荷を分散



障害発生時も残ったサーバでサービスを継続

共有ストレージ

一般的に、Webサーバに求められるものは？

セキュリティ

ある意味最もホットな問題。最初からセキュアであることが望ましいが、現実的には如何に日々セキュリティを向上させていけるか、が問題

スケーラビリティ

水平方向への拡張性の容易さ (Scale Out)
垂直方向への拡張性の容易さ (Scale Up)

高可用性、高信頼性

24x7 無停止。No Single Point of failure.
一部のコンポーネントの問題が全体に影響を及ぼさない

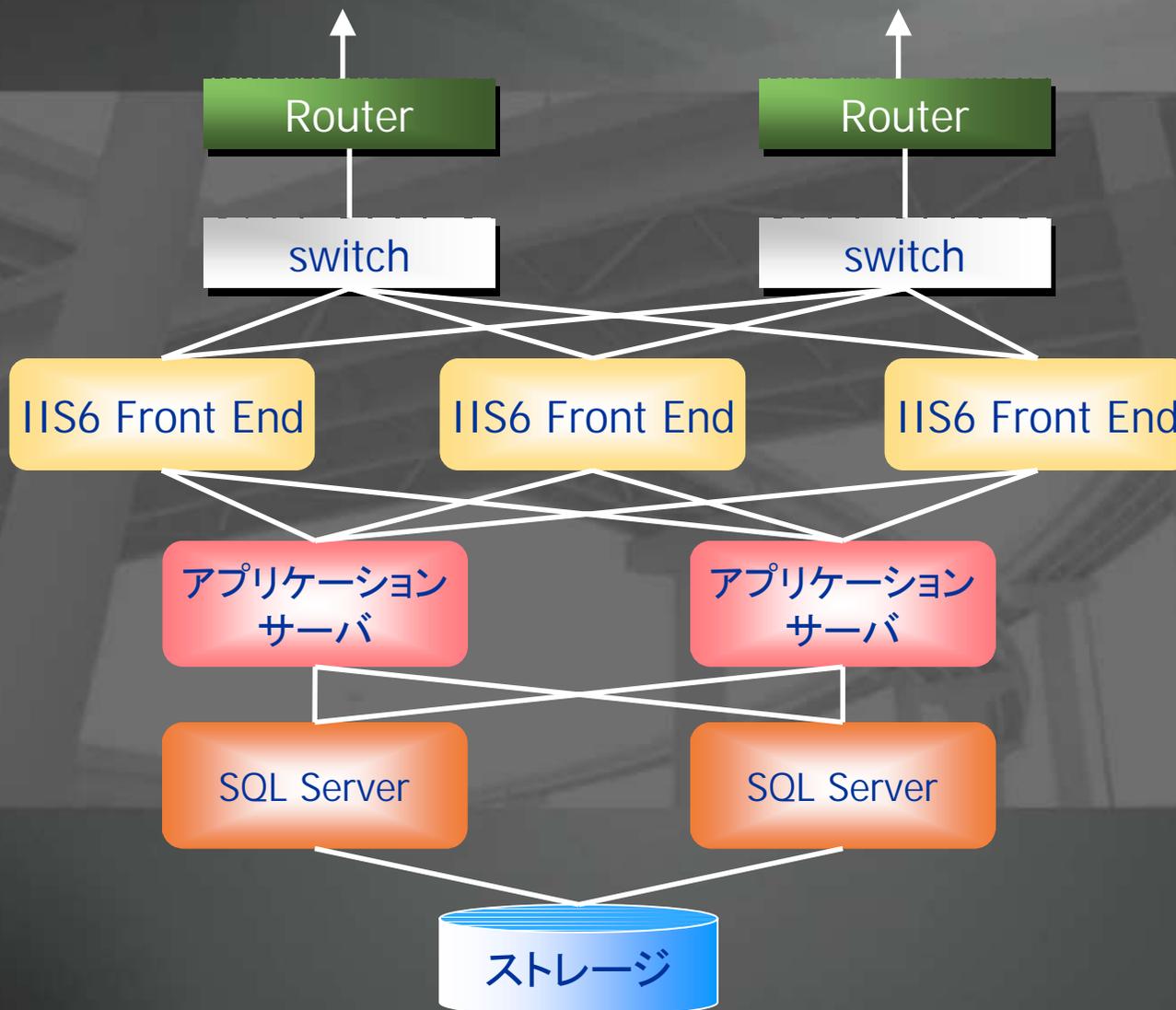
運用、管理の容易さ

必ずしもHigh Skillのエンジニアが常時管理できるわけではない。管理の自動化。ヘルスマニタ

高可用性と信頼性

- フォールトトレラントプロセスアーキテクチャ
- アプリケーションプール
- ヘルスモニタ
- ラピッドフェール保護
- 自動プロセスリサイクル
- プロセスの孤立化
- 中断されない TCP/IP 接続
- CPU およびプロセス帯域幅調整

想定するモデル



例えば、IGP
マルチホームして
EGP, MPLSでもよい

例えば、VRRP, HSRP

例えば、NLB, DNS
Round Robin, L4 sw

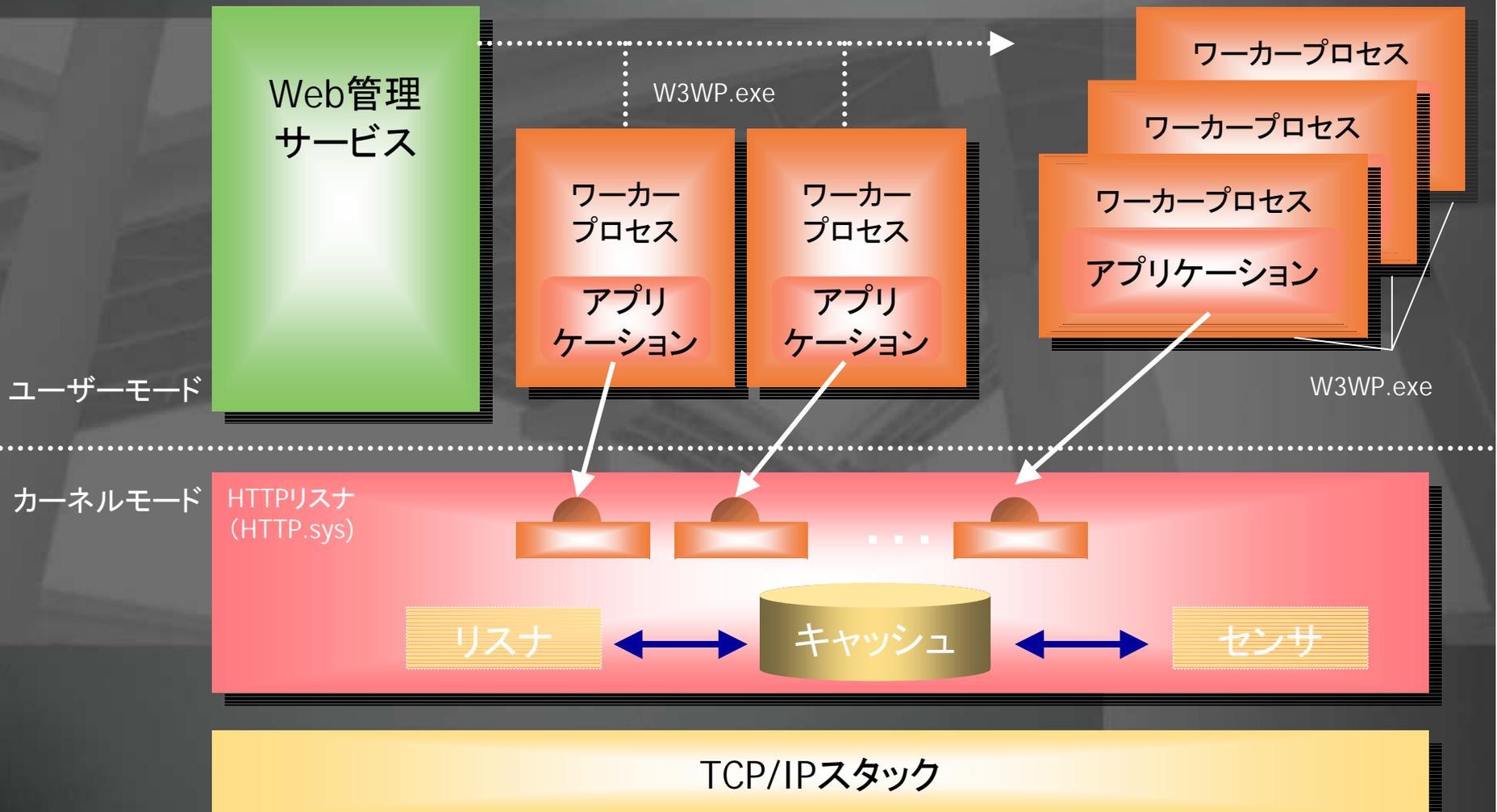
例えば、コンポーネン
ト負荷分散

例えば、サーバークラ
スター(MSCS)

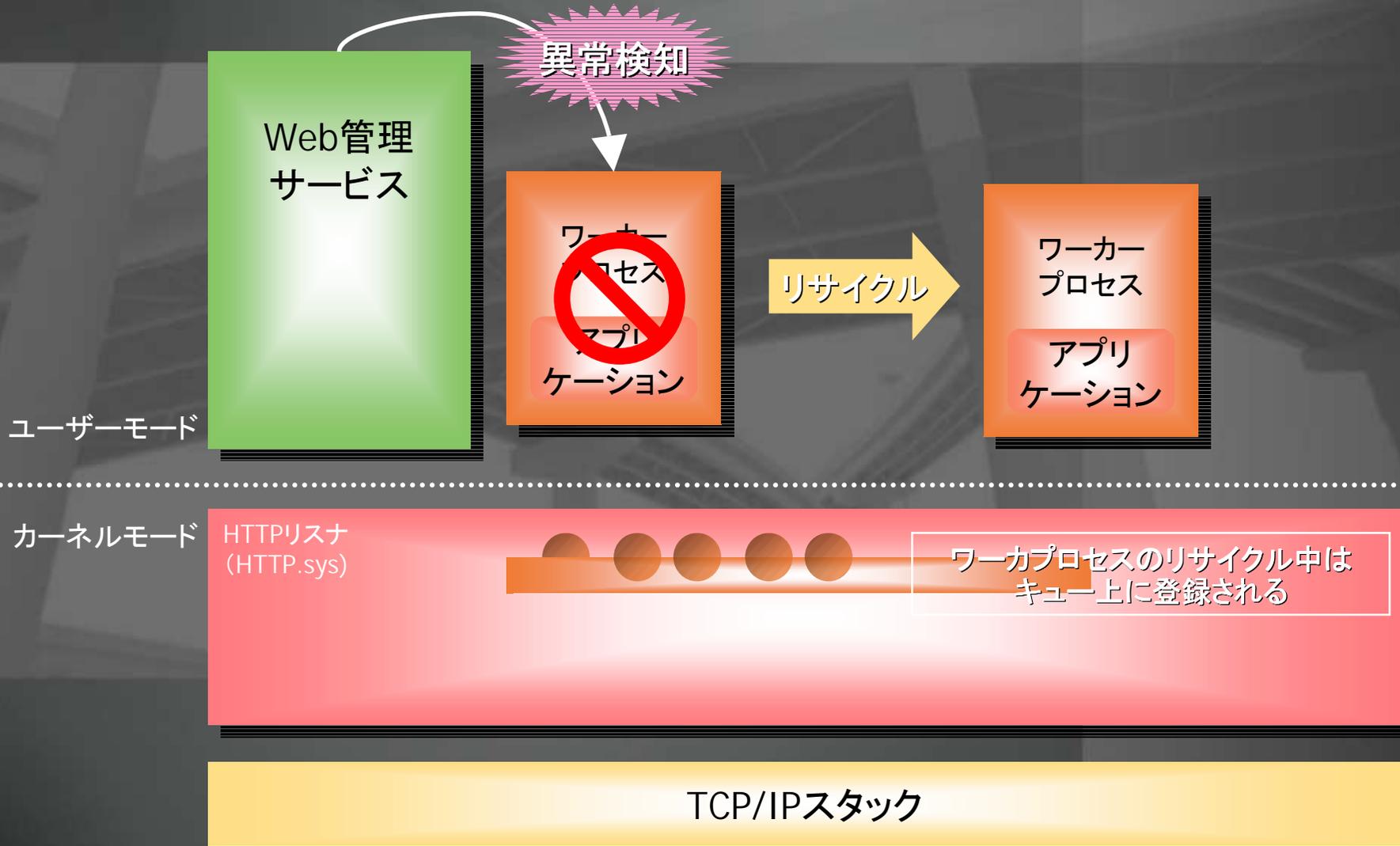
例えばSAN。
RAIDも

フォルトトトレランスアーキテクチャ

Webガーデン



ワーカープロセスのリサイクル

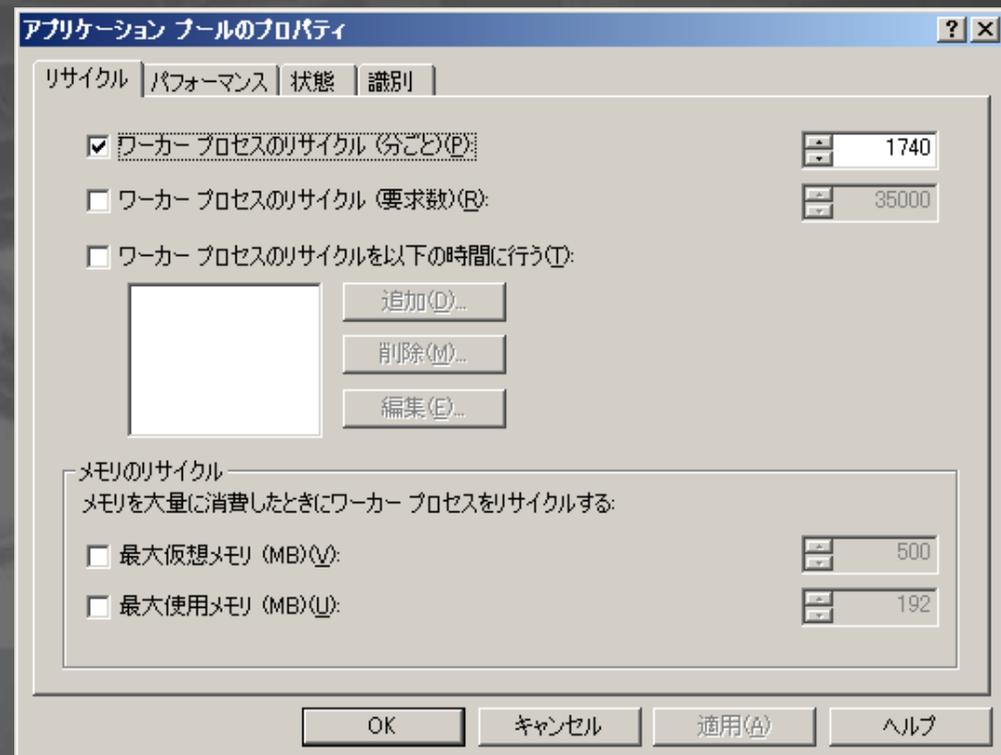


自動プロセスリサイクル

注意!

使用しているASPアプリケーションが、ワーカプロセスがリサイクルされている間のセッション状態を保持するように設計されていない場合、そのセッション状態が失われてしまうことがあります。

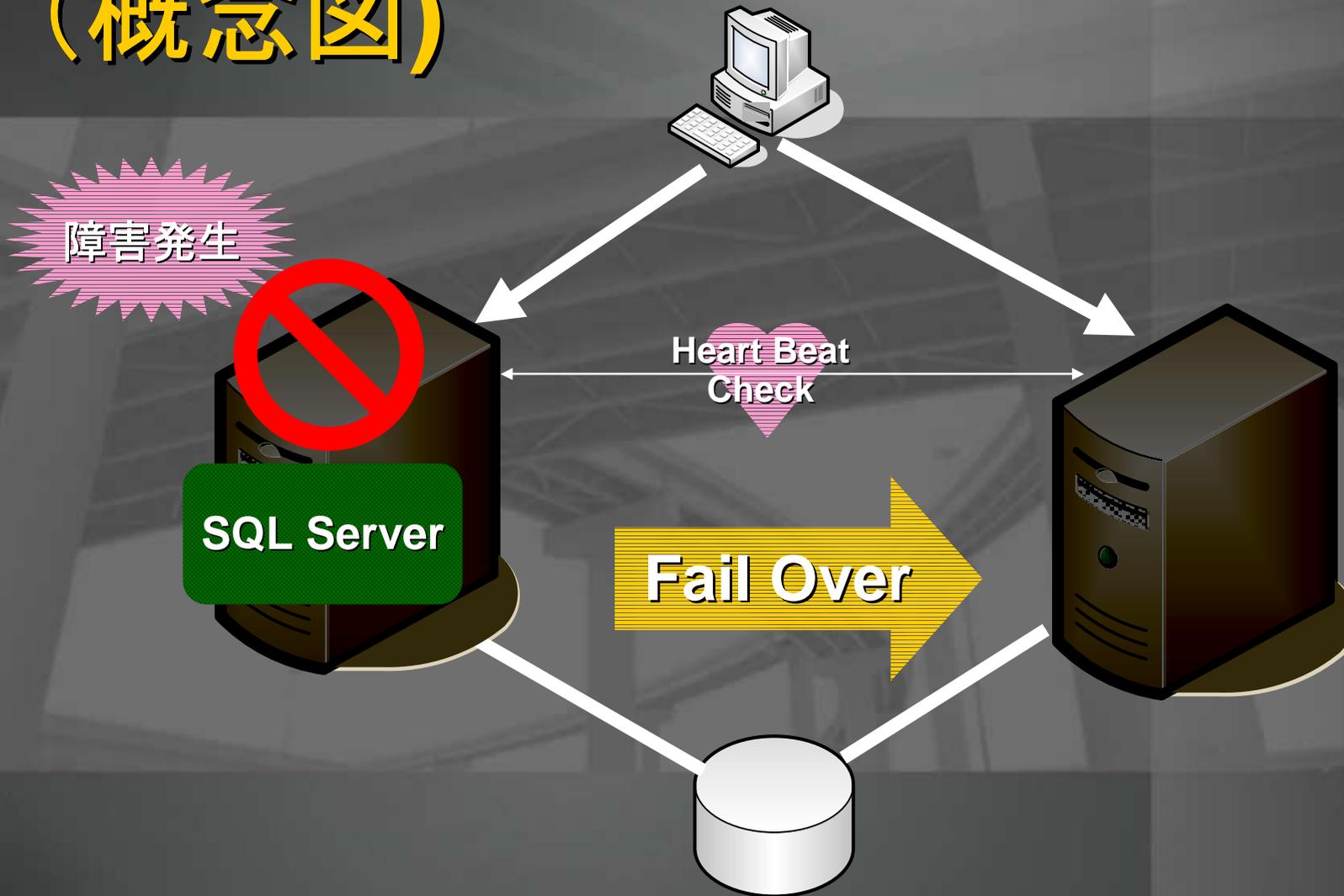
この問題を解決するには、セッション状態をデータベースに保存するか、ワーカプロセスのリサイクルを無効にする必要があります。



ラピッドフェール保護

- 指定した時間内に、特定回数のワーカークラスエラーが発生した場合に、アプリケーションプールを無効にする機能
- デフォルトでは、5分間に 5回

サーバークラスター (MSCS) (概念図)



MSCS

- 8ノードまでのクラスタのサポート
- 64bit CPUのサポート
- MNS (Majority Node Set) サポート
- 地理的に分散したクラスタ
- Windows 2000 Serverクラスタからのローリングアップグレード
- 構築、および管理が容易に

一般的に、Webサーバに求められるものは？

セキュリティ

ある意味最もホットな問題。最初からセキュアであることが望ましいが、現実的には如何に日々セキュリティを向上させていけるか、が問題

スケーラビリティ

水平方向への拡張性の容易さ
垂直方向への拡張性の容易さ

高可用性、高信頼性

24x7 無停止。No Single Point of failure.
一部のコンポーネントの問題が全体に影響を及ぼさない

運用、管理の容易さ

必ずしもHigh Skillのエンジニアが常時管理できるわけではない。管理の自動化。ヘルスマニタ

運用

- XML 構成データ
 - 実行時の編集
 - 構成のバージョン付けおよびロールバック
 - 構成のインポートおよびエクスポート
 - 別のマシンへの復元
- 管理コンソール
 - グラフィカル ユーザー インターフェイスを使用した管理 (IIS マネージャ)
 - Microsoft 管理コンソール (MMC) との統合
 - Web ベースの管理
- コマンドライン管理
 - スクリプト ベースの管理
 - Windows Management Instrumentation (WMI) のサポート
 - Active Directory Service Interface (ADSI) のサポート
- リモート管理 (IIS マネージャ、Web ベース管理ツール、ターミナルサービス)
- バイナリおよび Unicode Transformation Format-8 (UTF-8) のログ
- HTTP サブ状態コード ログ

XML構成データ

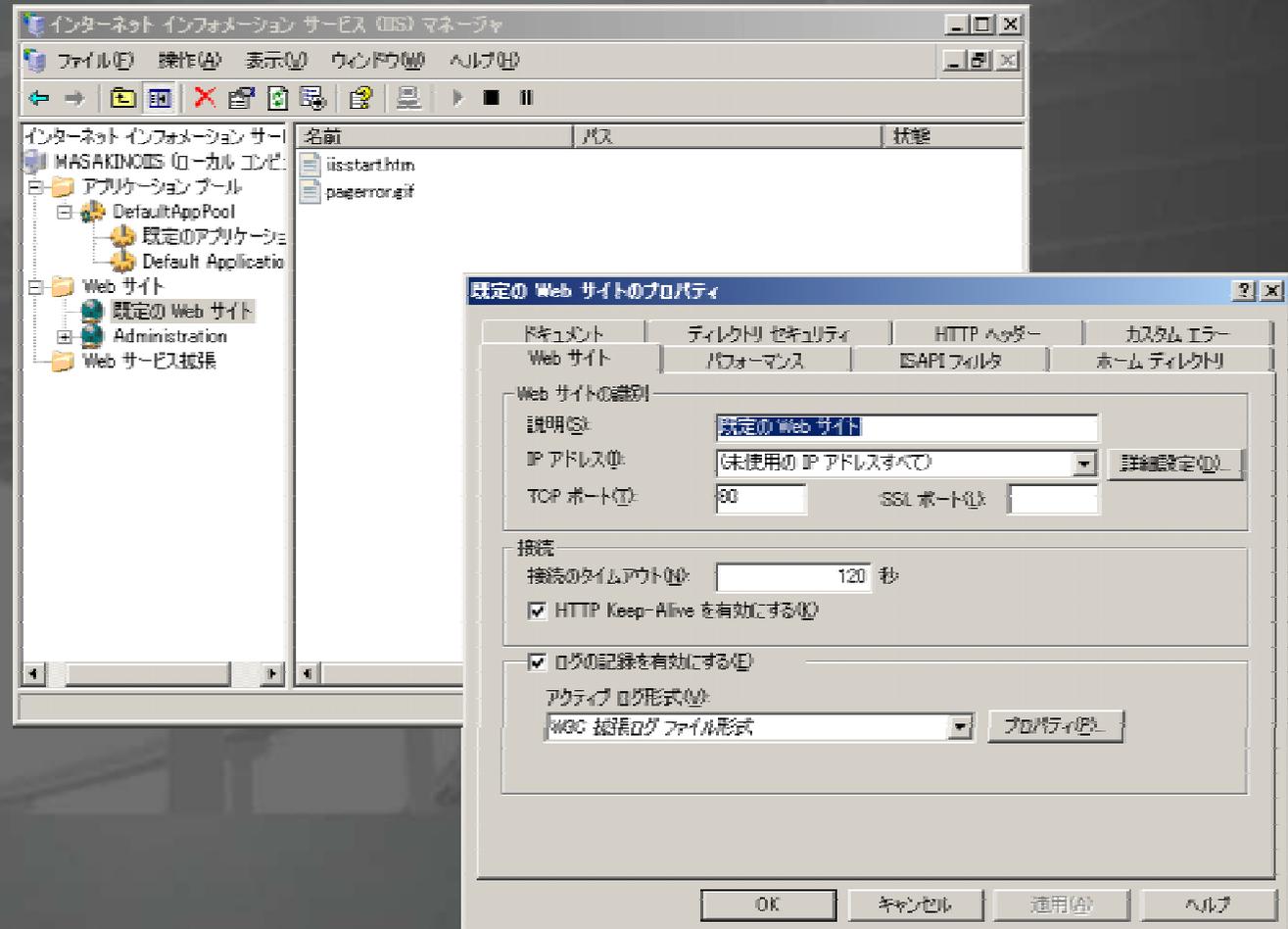
- IIS6の構成情報をXMLでダンプし、これを編集することが可能
- %systemroot%\%system32%\inetsrv\MetaBase.xml
- Metabase Editor

The screenshot displays the Metabase Editor interface. On the left, a tree view shows the configuration hierarchy for 'MASAENOC < local >'. The 'Schema' folder is expanded, showing various configuration elements. The main pane displays a table of these elements with columns for ID, Name, Data Type, Data, and Attributes.

ID	Name	Data Type	Data	Attributes
1802	KeyType	String	SM/MS/Service	none
1813	Connecto	DWORD	130	ISABLE
1814	MaxConn	DWORD	4294967295	ISABLE
1821	Downlent	DWORD	1	ISABLE
2000	AutoClose	String	/loadspeed/whg.asp	ISABLE
2001	AutoExp	String	/loadspeed/acc.asp	ISABLE
2002	AutoMerr	String	/loadspeed/ovr.asp	ISABLE
2007	AutoExp	String	/loadspeed/asp.asp	ISABLE
2008	Password	DWORD	6	ISABLE
2009	AutoMerr	String	/loadspeed/ovr.asp	ISABLE
2070	InProcess	MultiString	C:\WINDOWS\system32\inetn\httpd\DCWEM	ISABLE
2096		DWORD	1	
2097	Applicatio	MultiString	Active Server Pages ASP インターネット サービス	name
2098	WebSrvC	MultiString	D:\inetroot\WWWROOT\MSDOWNS\inetn\http	name
4000	LogType	DWORD	1	ISABLE
4001	LogFileDir	StringEscp	C:\WINDOWS\system32\LogFiles	ISABLE
4002	LogFileFr	DWORD	1	ISABLE
4004	LogFileTr	DWORD	20971820	ISABLE
4007	LogObcD	String	HTTPLOG	ISABLE
4008	LogObcT	String	InternetFile	ISABLE
4009	LogObcU	String	InternetAdmin	ISABLE
4010	LogObcP	String	***Secure Data***	ISABLES
4011	LogPherr	String	FF168693-D320-11CF-800A-00AA00011E00	ISABLE
4012	LogErrFil	DWORD	279900	ISABLE
4016	GenrAbt	DWORD	0	ISABLE
6000	AutoFlags	DWORD	6	ISABLE
6005	DirBrowse	DWORD	1070341988	ISABLE
6006	DefaultDoc	String	Default.htm, Default.asp, index.htm	ISABLE
6008	HttpErrors	MultiString	4004 FILE, C:\WINDOWS\system32\help\comcom\400	ISABLE
6014	ScriptMap	MultiString	asp, 0, \WINDOWS\system32\inetn\http\REGIET	ISABLE
6020	Anonymous	String	3333, MASAENOC	ISABLE
6071	Anonymous	String	***Secure Data***	ISABLE

IISマネージャー

すべてのIIS6
の設定はここ
から



リモートからのデスクトップ管理

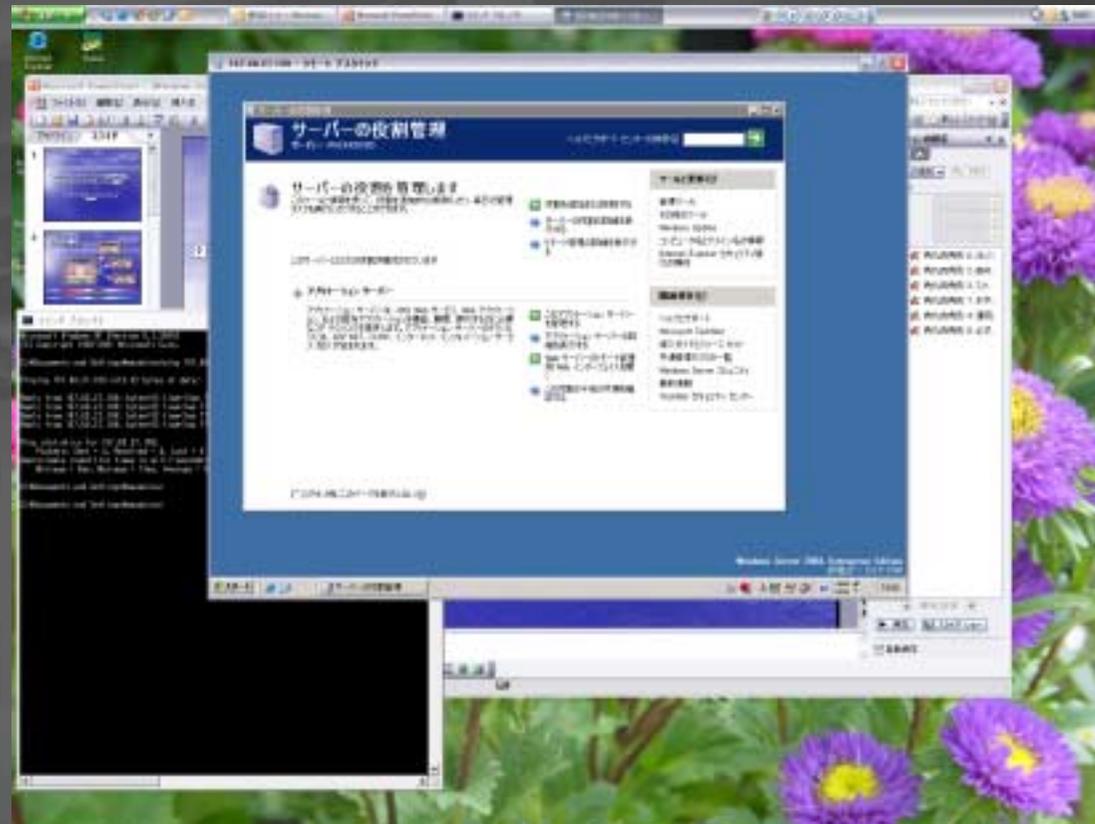
- XP等からリモートデスクトップ接続を通じてサーバをGUIで管理可能。

- どうしてもUNIXのデスクトップからコンソールをとりたいのであれば、VNCなどを使う手も...

<http://www.realvnc.org/>

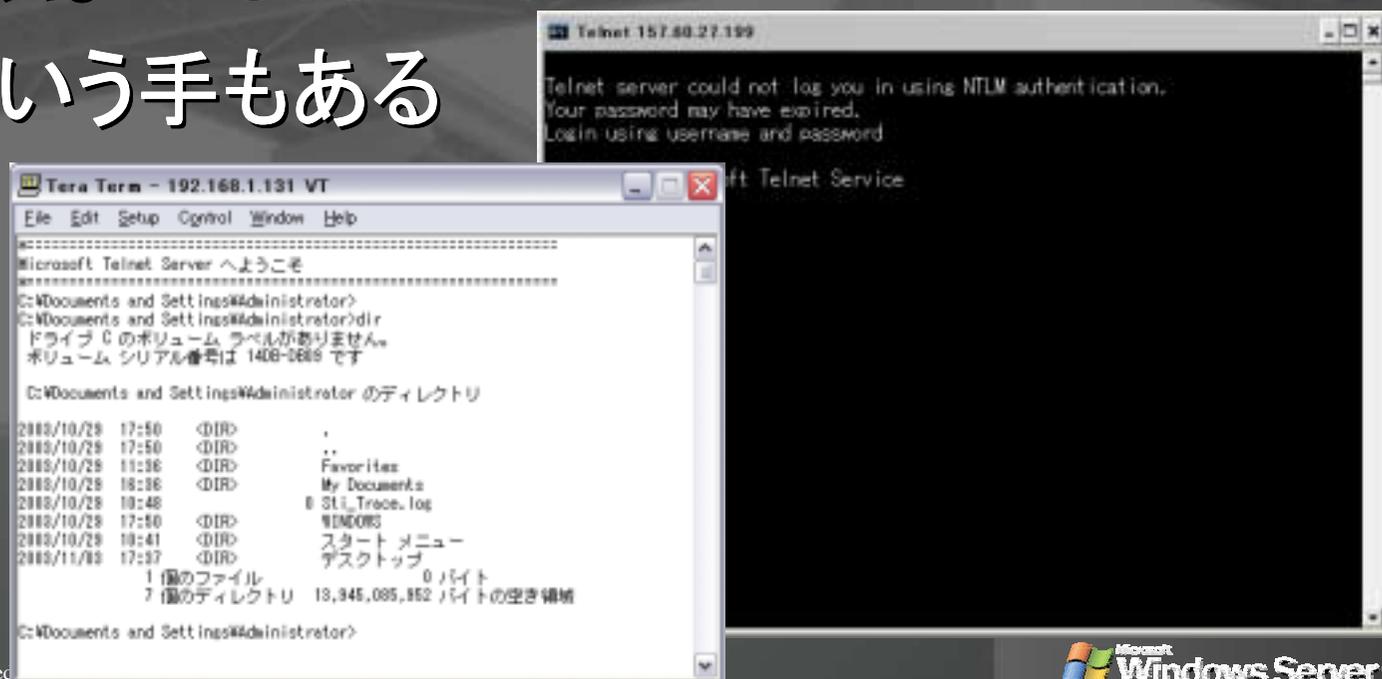
- IPsecと組み合わせてよりセキュアに

- その他、例えばpcAnywhereなどの他社製品の利用も可能



telnetでログインして管理する

- Windowsだってもちろん telnet できます
- でも、普通にtelnetしたのではパスワードもなにもかもが平文で流れてしまう
- お勧めは IPsec + telnet
- sshという手もある



スクリプトで管理を自動化する

- %systemroot%\%system32%に8つのVBScriptがインストールされています
- XPや2003ではほとんどの管理がコマンドラインでも、可能です

lisftp.vbs	FTPサイトの作成、削除、開始、停止、一覧表示
lisvdir.vbs	仮想ディレクトリの作成と削除、指定されたルート of 仮想ディレクトリの表示
iisweb.vbs	Webサイトの作成、削除、開始、停止、一覧表示
lisftpr.vbs	指定されたルート of 下の仮想ディレクトリの作成、削除、または表示
liscnfg.vbs	XMLファイルへのIIS構成のエクスポートとインポート
lisback.vbs	IIS構成のバックアップと復元
lisapp.vbs	現在実行されているワーカプロセス(W3WP.exe)のプロセスIDおよびアプリケーションプールIDの一覧表示
lisext.vbs	Webサービス拡張の設定

Microsoft®

© 2003 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only.
MICROSOFT MAKES NO WARRANTIES, EXPRESS

OR IMPLIED, IN THIS SUMMARY.

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.



Appendix. 追加の情報

- MicrosoftのWebサイト
- White Paper
- MSDN
- TechNet

Microsoft Web サイト

- Windows Server 2003 (日本語)
<http://www.microsoft.com/japan/windowsserver2003/>
- Windows Server 2003 (英語)
<http://www.microsoft.com/windowsserver2003/>

White Paper (技術文書)

- 「Windows Server 2003 技術情報 インデックス」
<http://www.microsoft.com/japan/windowsserver2003/techinfo/overview/articleindex.mspix>
- 「Windows Server 2003 レビューアーズ ガイド」
<http://www.microsoft.com/japan/windowsserver2003/techinfo/overview/reviewersguide.mspix>
- 「クラスタ テクノロジーの技術概要」
<http://www.microsoft.com/japan/windowsserver2003/techinfo/overview/clustering.mspix>
- 「Windows Server 2003 サーバー クラスタのアーキテクチャ」
<http://www.microsoft.com/japan/windowsserver2003/techinfo/overview/servercluster.mspix>
- 「ネットワーキングおよび通信の技術概要」
<http://www.microsoft.com/japan/windowsserver2003/techinfo/overview/netcomm.mspix>

White Paper (技術文書)

- 「インターネット インフォメーション サービス (IIS) 6.0 の技術概要」
<http://www.microsoft.com/japan/windowsserver2003/techinfo/overview/iis.mspx>
- 「インターネット インフォメーション サービス 6.0 の新機能」
<http://www.microsoft.com/japan/windowsserver2003/evaluation/overview/technologies/iis.mspx>
- 「インターネット インフォメーション サービス 6.0 におけるセキュリティの強化」
<http://www.microsoft.com/japan/windowsserver2003/techinfo/overview/iisenhance.mspx>
- 「IIS (Internet Information Services) 6.0 の新機能概要と構成」
http://www.microsoft.com/japan/windowsserver2003/techinfo/planning/walkthroughs/f_iis6.mspx
- 「Internet Information Services (IIS) 6.0 Resource Kit (英語)」
<http://www.microsoft.com/downloads/details.aspx?FamilyID=80a1b6e6-829e-49b7-8c02-333d9c148e69&DisplayLang=en>

MSDN と TechNet

- TechNet – IT proの皆様に技術情報を提供
<http://www.microsoft.com/japan/technet>
- MSDN – 主に開発者向けの情報を定期的に提供。評価版の提供など
<http://www.microsoft.com/japan/msdn/>

その他のツール

- IIS6 resource kit tools (英語版のみ)
<http://www.microsoft.com/downloads/details.aspx?FamilyID=56fc92ee-a71a-4c73-b628-ade629c89499&DisplayLang=en>
- Microsoft Operations Manager 2000
<http://www.microsoft.com/mom/>
- Microsoft Service for UNIX 3.0
<http://www.microsoft.com/japan/windows/sfu/>