図11　SSLの負荷分散

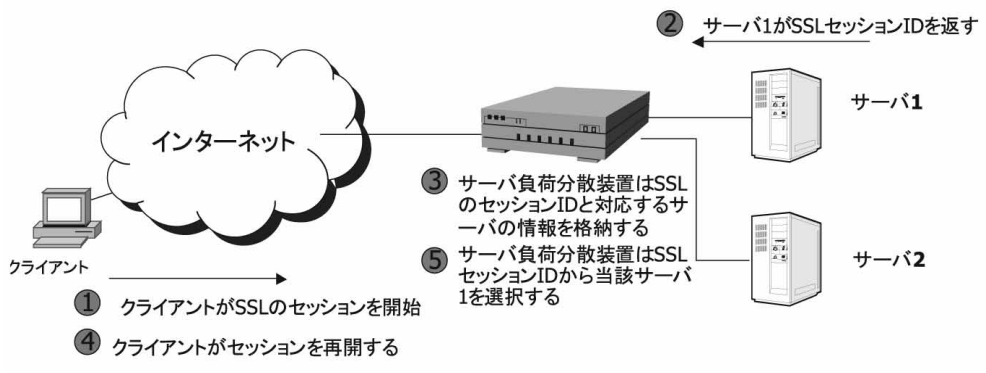
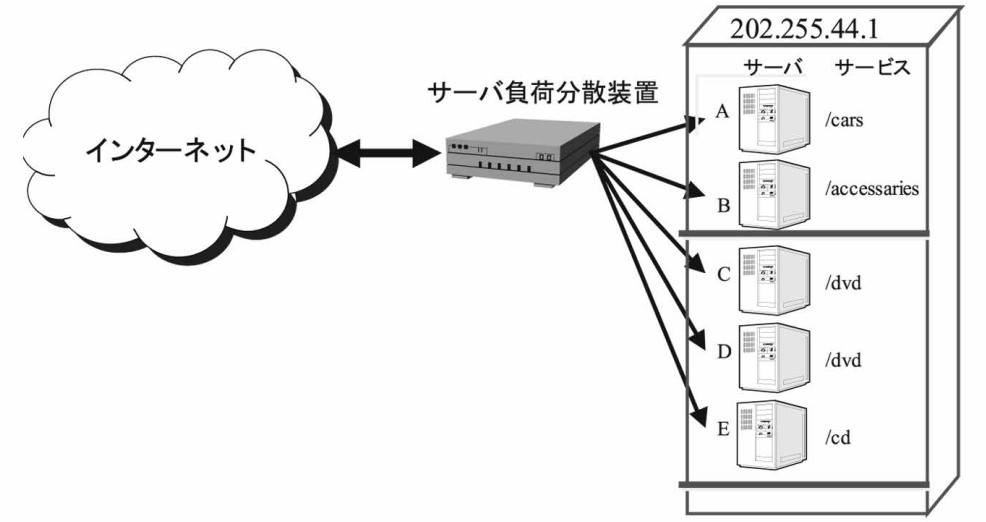


図12　URLスイッチング



処理を負荷分散することが必要になる。一つの方法として、SSLの処理をサービス提供用のサーバから切り離し、専用マシンで処理する構成が考えられている。図11は、SSLの処理がサービス提供サーバで行うにせよ、行わないにせよ、SSL処理サーバの処理負荷を負荷分散により低減することを狙った構成を示している。

⑹　アクセスする実サーバをURL単位で変更できること

WEBのホスティング・サービスを行う場合、顧客単位でセキュリティを管理するため、顧客ごとに別のサーバにコンテンツを収容する場合がある。この場合、URLのサフィックスで参照サーバが異なる。図12に、202.255.44.1のマシンのFQDNをwww.server.comとした場合、http://www.server.com/cars、http://www.server.com/accessaries、http://www.server.com/dvd、http://www.server.com/cdがそれぞれ、サーバA、サーバB、サーバCとD、サーバEにアクセスするように構成した事例を示した。

5　ミッション・クリティカルなネットワークの提供

この条件を以下に示す。

⑴　種々のレベルでフォールトトレラントであること

⑵　高速であること

⑶　エッジ・ルータの利用効率が良いこと

⑷　大容量サーバを持ち、かつスケーラビリティがあること

6　ファイヤーウォールのロードバランス

顧客のファイアーウォールがサービス上のボトルネックにならないよう、スケーラブルかつ高速なファイヤーウォール機能を提供できなければならない。

⑴　複数のファイヤーウォールによるロードバランス

図13には、３台のファイヤーウォールをロードバランスし、ファイヤーウォールに障害があったときの対策を考えた冗長構成例を示した。

⑵　スイッチレベル、回線レベル、ファイヤーウォール各部の障害時に対応できるホット／スタンバイ機能があること

図14には、図13の構成をさらに拡張し、３台のファイヤーウォールをロードバランスする際、ロードバランスに使っているスイッチ・ルータ（サーバ負荷分散装置）や接続回線に障害があったときの対策を考えた冗長構成例を示した。

7　データセンタの世界展開

IDCの運用上の信頼性を増すには、情報セキュリティやネットワーク・セキュリティだけを考慮するのではなく、物理セキュリティを向上させることが重要である。特に、自然災害、人災、あるいはテロ等によるサービス断を避けるためには、同一箇所における設備の二重化・冗長構成だけでなく、地理的に分散した冗長構成が必要になる。

図13　ファイヤーウォールの負荷分散

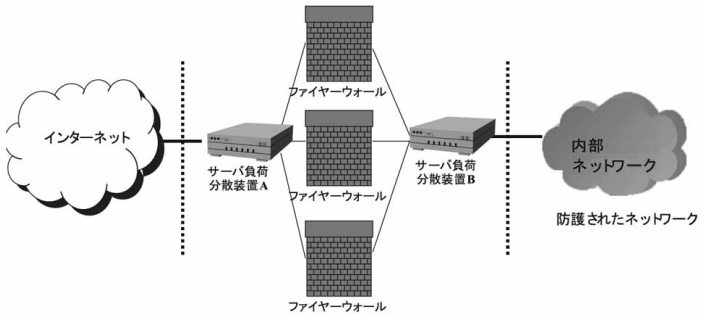


図14　ファイヤーウォールとフォールトトレラントな負荷分散装置

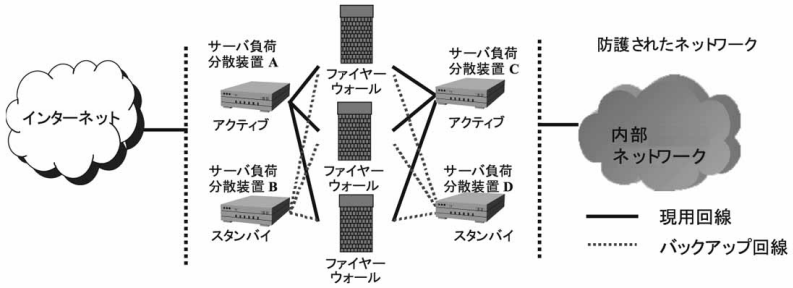
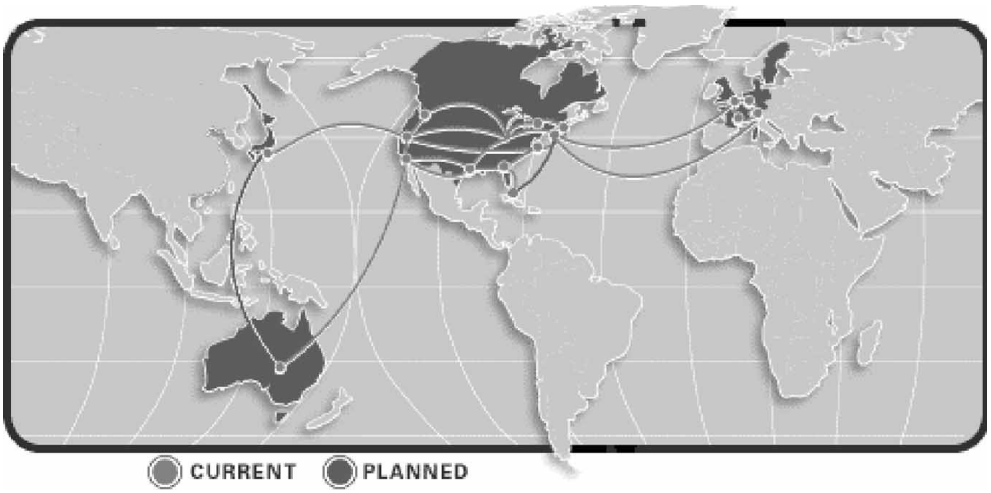


図15　IDCの世界展開の例（EXODUS）



http://www.exodus.com/network/network_map.html

そのための機能が、4．1節に解説した機能（⑼、⑽）である。クライアントからは単一のサーバに見えること、かつクライアントに最もネットワーク的に近いサーバを割り当てられることが構成上のポイントである。また、IDC内のサーバが何らかの意味でクラッシュしたときは、クライアントが最適の代替サーバにアクセスするようガイドできなければならない。この結果、自然災害やテロ（サイバーおよび物理的の両方の意味で）により、特定の場所にあるIDCがシステムダウンした場合でも、IDC群に収容されたサーバのサービス自体を停止させることなく運用できる。従って、今後の電子政府サービスをIDCを使って提供していくためには、基盤となる機能と言える。

このような観点と、顧客からのアクセスビリティも考え、個々のIDCを高速回線で結んだIDCの分散化が進んでいる。図15にはEXODUSの例を示す。

データセンタを電子政府関連のサーバの収容に使用する際に、最後（最終的）に考えるべき点は、データセンタの地理的位置をテロリスト等から隠蔽することである。これは対テロ対策上不可避の施策であり、例えば現在でもインターネットの .com、.org、.netのルート・ネームサーバの運用を任されているVeriSign社は、彼らのIDC群の中で中心的機能を担っているワシントンD.C. のIDCに関しては、地理的位置が判らないように運用している。自然災害には地理的分散による冗長構成が有効であるが、テロに対してはさらにIDCの位置を非公開にすることも重要である。

日本の場合、IDCにできる建物で秘密裏に運用できるような条件のものは少なく、業界通なら大体どこの建物か見当がつく状況にある。電子政府等のサーバを収容していくには、今までの設計思想と異なる非公開IDCを建設し、運用していくことが不可欠である。ただし、これは、国民の情報が秘密のIDCに収容されることを意味するため、何らかの意味での国民的合意が必要となろう。