(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4236819号
(P4236819)

(45)発行日　平成21年3月11日(2009.3.11)　(24)登録日　平成20年12月26日(2008.12.26)

(51)Int.Cl.		F I		
G06F 13/00	(2006.01)	G06F	13/00	351M
G06F 12/00	(2006.01)	G06F	12/00	537Z
G06F 21/24	(2006.01)	G06F	12/14	530A
G06F 12/16	(2006.01)	G06F	12/14	560B
G06Q 30/00	(2006.01)	G06F	12/16	310J

請求項の数 10　(全 16 頁)　最終頁に続く

(21)出願番号　特願2001-60721(P2001-60721)
(22)出願日　平成13年3月5日(2001.3.5)
(65)公開番号　特開2002-259233(P2002-259233A)
(43)公開日　平成14年9月13日(2002.9.13)
審査請求日　平成14年2月15日(2002.2.15)
審判番号　不服2005-10401(P2005-10401/J1)
審判請求日　平成17年6月6日(2005.6.6)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100109313
弁理士　机　昌彦
(74)代理人　100121290
弁理士　木村　明隆
(74)代理人　100111637
弁理士　谷澤　靖久
(72)発明者　田上　岳夫
東京都港区芝五丁目７番１号
日本電気株式会社内

最終頁に続く

(54)【発明の名称】コンテンツ提供システムおよびコンテンツ提供プログラム

(57)【特許請求の範囲】
【請求項１】
ネットワークを介して利用者のユーザ端末から送信されてきた指定情報に基づいて、第一のホストコンピュータがコンテンツをネットワークを介してユーザ端末に送信するコンテンツ提供システムであって、
ネットワークに接続され、第一のホストコンピュータよりもセキュリティを強化された第二のホストコンピュータを設けて、
第一のホストコンピュータが、不正アクセスによる被害を受けたときに、コンテンツを第二のホストコンピュータに転送し、
第二のホストコンピュータが、第一のホストコンピュータから転送されてきたコンテンツを第二のホストコンピュータ自体に登録して、第一のホストコンピュータの代わりに、ユーザ端末からの指定情報に基づいて、当該コンテンツをネットワークを介してユーザ端末に送信する
ことを特徴とするコンテンツ提供システム。
【請求項２】
ネットワークを介して利用者のユーザ端末から送信されてきた指定情報に基づいて、第一のホストコンピュータがコンテンツをネットワークを介してユーザ端末に送信するコンテンツ提供システムであって、
ネットワークに接続され、第一のホストコンピュータよりもセキュリティを強化された第二のホストコンピュータを設けて、

第二のホストコンピュータが、第一のホストコンピュータからコンテンツの一部を第二のホストコンピュータにあらかじめ複写しておき、第一のホストコンピュータの代わりに、ユーザ端末からの指定情報に基づいて、当該コンテンツをネットワークを介してユーザ端末に送信する
ことを特徴とする、コンテンツ提供システム。
【請求項３】
上記ユーザ端末が、ＤＮＳの検索結果に基づいて、コンテンツを提供する第一のホストコンピュータのＩＰアドレスを入手して、当該第一のホストコンピュータにアクセスすることを特徴とする請求項１に記載のコンテンツ提供システム。
【請求項４】
上記第一のホストコンピュータが、不正アクセスによる被害を受けたとき、ＤＮＳに登録された当該第一のホストコンピュータのＩＰアドレスを第二のホストコンピュータのＩＰアドレスに変更することを特徴とする請求項３に記載のコンテンツ提供システム。
【請求項５】
上記第一のホストコンピュータが、不正アクセスによる被害を受けたとき、当該第一のホストコンピュータのＩＰアドレスを第二のホストコンピュータに割り振ると共に、当該第一のホストコンピュータに他のＩＰアドレスを割り振ることを特徴とする請求項３に記載のコンテンツ提供システム。
【請求項６】
上記ネットワークが、インターネットであることを特徴とする請求項１～５のいずれかに記載のコンテンツ提供システム。
【請求項７】
上記第一のホストコンピュータおよび／または上記第二のホストコンピュータが、Ｗｅｂサーバであることを特徴とする請求項１～６のいずれかに記載のコンテンツ提供システム。
【請求項８】
上記コンテンツが、ホームページであって、第二のホストコンピュータに複写されるコンテンツが、当該ホームページのトップページであることを特徴とする請求項２に記載のコンテンツ提供システム。
【請求項９】
ネットワークを介して利用者のユーザ端末から送信されてきた指定情報に基づいて、第一のホストコンピュータに、コンテンツをネットワークを介してユーザ端末に送信させるコンテンツ提供プログラムであって、第一のホストコンピュータに、不正アクセスによる被害を受けたときに、コンテンツをネットワークに接続され、第一のホストコンピュータよりもセキュリティを強化された第二のホストコンピュータに転送させる処理と、第二のホストコンピュータに、第一のホストコンピュータから転送されてきたコンテンツを第二のホストコンピュータ自体に登録させ、第一のホストコンピュータの代わりに、ユーザ端末からの指定情報に基づいて、当該コンテンツをネットワークを介して
ユーザ端末に送信させる処理を実行させるコンテンツ提供プログラム。
【請求項１０】
ネットワークを介して利用者のユーザ端末から送信されてきた指定情報に基づいて、第一のホストコンピュータに、コンテンツをネットワークを介してユーザ端末に送信させるコンテンツ提供プログラムであって、
ネットワークに接続され、第一のホストコンピュータよりもセキュリティを強化された第二のホストコンピューに、第一のホストコンピュータからコンテンツの一部を第二のホストコンピュータにあらかじめ複写させて、第一のホストコンピュータの代わりに、ユーザ端末からの指定情報に基づいて、当該コンテンツをネットワークを介してユーザ端末に送信させる処理を実行させるコンテンツ提供プログラム。
【発明の詳細な説明】
【０００１】

【発明の属する技術分野】
本発明は、インターネット，一般公衆回線等のネットワークを利用したコンテンツ提供サービス、特にネットワーク上の不正アクセス対策のための技術に関する。
【０００２】
【従来の技術】
近年、ネットワークを利用したコンテンツ提供サービスが爆発的に普及してきているが、いわゆる不正アクセスが急増してきており、インターネットビジネスが本格化するにつれて、ネットワーク上のセキュリティが問題になってきている。
特に、Ｗｅｂサーバをターゲットとしたコンテンツの改竄やサービスの使用停止攻撃等が頻発してきており、これらの不正アクセスによる被害を受けると、再び被害にあわないようにするための対策に時間がかかることになり、その間コンテンツの提供を行なうことができなくなってしまう。
【０００３】
このような不正アクセスを防止するためには、個別のホストコンピュータやシステム毎に、ホストコンピュータ上のセキュリティを強化したり、ネットワーク上にて所謂ファイアウォールシステムや不正アクセス監視装置を導入する等の不正アクセス対策が採用されている。
【０００４】
【発明が解決しようとする課題】
しかしながら、このようなファイアウォールシステムや不正アクセス監視装置等の不正アクセス対策は、上述したように、個別のホストコンピュータやシステム毎に行なわれているので、十分なセキュリティ対策を行なおうとすると、常時監視体制の整備やセキュリティシステムの導入に膨大なコストが発生することになるので、完全な対策の実現が実際上困難である。
また、このような不正アクセス対策を行なったとしても、一旦、不正アクセスの被害を受けると、再び被害にあわないようにするためのさらなる対策が必要になるため、コンテンツ提供サービスの再開までに時間がかかってしまう。
【０００５】
本発明は、上記の問題を解決すべくなされたものであり、不正アクセスの被害を受けたときに、セキュリティ強化を行なって不正アクセスによる被害を受けにくくしてある別のホストコンピュータ上にて、同じコンテンツ提供サービスを迅速に再開できるようにして、不正アクセスによる被害を最小限に抑制するようにしたコンテンツ提供サービスおよびコンテンツ提供プログラムの提供を目的とする。
【０００６】
【課題を解決するための手段】
この目的を達成するため、本発明の請求項１記載のコンテンツ提供システムは、ネットワークを介して利用者のユーザ端末から送信されてきた指定情報に基づいて、第一のホストコンピュータがコンテンツをネットワークを介してユーザ端末に送信するコンテンツ提供システムであって、ネットワークに接続され、第一のホストコンピュータよりもセキュリティを強化された第二のホストコンピュータを設けて、第一のホストコンピュータが、不正アクセスによる被害を受けたときに、コンテンツを第二のホストコンピュータに転送し、第二のホストコンピュータが、第一のホストコンピュータから転送されてきたコンテンツを第二のホストコンピュータ自体に登録して、第一のホストコンピュータの代わりに、ユーザ端末からの指定情報に基づいて、当該コンテンツをネットワークを介してユーザ端末に送信する構成としてある。
【０００７】
コンテンツ提供システムをこのような構成とすると、何者かによる不正アクセスの被害を受けたとき、第一のホストコンピュータに代わって、第二のホストコンピュータが同じコンテンツの提供サービスを行なうことにより、コンテンツ提供サービスの中断時間が大幅に短縮される。したがって、不正アクセスの被害によるコンテンツ提供サービスが迅速に

再開されることになる。

【０００８】

この場合、第二のホストコンピュータは、セキュリティを強化することによって、不正アクセスの被害を受けにくくしてあるので、再び不正アクセスの被害を受けることが実質的にない。そして、第二のホストコンピュータによりコンテンツの提供サービスが行なわれている間に、第一のホストコンピュータについて、再度不正アクセスの被害を受けないように十分なセキュリティ対策が行なわれた後、再び第二のホストコンピュータから第一のホストコンピュータに切り替えて、コンテンツの提供サービスを行なうことができる。

【０００９】

また、この目的を達成するため、本発明の請求項２記載のコンテンツ提供システムは、ネットワークを介して利用者のユーザ端末から送信されてきた指定情報に基づいて、第一のホストコンピュータがコンテンツをネットワークを介してユーザ端末に送信するコンテンツ提供システムであって、ネットワークに接続され、第一のホストコンピュータよりもセキュリティを強化された第二のホストコンピュータを設けて、第二のホストコンピュータが、第一のホストコンピュータからコンテンツの一部を第二のホストコンピュータにあらかじめ複写しておき、第一のホストコンピュータの代わりに、ユーザ端末からの指定情報に基づいて、当該コンテンツをネットワークを介してユーザ端末に送信する構成としてある。

【００１０】

コンテンツ提供システムをこのような構成とすると、第一のホストコンピュータが提供するコンテンツの一部、例えば第一のホストコンピュータが提供するコンテンツとしてのホームページのうち、重要なページ例えばトップページを第二のホストコンピュータに複写しておくことにより、例えばトップページがセキュリティが強化され不正アクセスの被害を受けにくくしてある第二のホストコンピュータにより利用者に提供されることになる。

したがって、このような重要なページ、例えばトップページについて、セキュリティが強化され、不正アクセスを受けにくくしてあるので、例えば不正アクセスによりホームページのトップページが不正に改竄されたり、コンテンツ提供サービスが停止してしまうようなことがない。

【００１１】

請求項３記載のコンテンツ提供システムは、上記ユーザ端末が、ＤＮＳの検索結果に基づいて、コンテンツを提供する第一のホストコンピュータのＩＰアドレスを入手して、当該第一のホストコンピュータにアクセスする構成としてある。コンテンツ提供システムをこのような構成とすると、ユーザ端末は、ＤＮＳの検索によりコンテンツを提供する第一のホストコンピュータのＩＰアドレスを入手するようになっているので、コンテンツ提供者は、ＤＮＳに登録してある第一のホストコンピュータのＩＰアドレスを変更することにより、容易にホストコンピュータを切り替えることができる。

【００１３】

請求項４記載のコンテンツ提供システムは、上記第一のホストコンピュータが、不正アクセスによる被害を受けたとき、ＤＮＳに登録された当該第一のホストコンピュータのＩＰアドレスを第二のホストコンピュータのＩＰアドレスに変更する構成としてある。

【００１４】

コンテンツ提供システムをこのような構成とすると、上記第一のホストコンピュータが不正アクセスによる被害を受けたとき、第一のホストコンピュータが、ＤＮＳに登録された当該第一のホストコンピュータのＩＰアドレスを第二のホストコンピュータのＩＰアドレスに変更する。これにより、ユーザ端末がＤＮＳの検索結果により当該第一のホストコンピュータのＩＰアドレスを入手しようとしたとき、検索結果として既に切り替えられている第二のホストコンピュータのＩＰアドレスを入手することになる。

したがって、ユーザ端末は、この新たなＩＰアドレスにより、コンテンツ提供サービスを行なう第二のホストコンピュータにアクセスして、コンテンツ提供サービスを受けることができる。

【００１５】
請求項５記載のコンテンツ提供システムは、上記第一のホストコンピュータが、不正アクセスによる被害を受けたとき、当該第一のホストコンピュータのＩＰアドレスを第二のホストコンピュータに割り振ると共に、当該第一のホストコンピュータに他のＩＰアドレスを割り振る構成としてある。
【００１６】
コンテンツ提供システムをこのような構成とすると、上記第一のホストコンピュータが不正アクセスによる被害を受けたとき、第一のホストコンピュータが、ＤＮＳに登録された当該第一のホストコンピュータのＩＰアドレスを第二のホストコンピュータに割り振る。これにより、ユーザ端末が当該第一のホストコンピュータのＩＰアドレスにより当該第一のホストコンピュータにアクセスしようとしたとき、同じＩＰアドレスが割り振られた第二のホストコンピュータにアクセスして、コンテンツ提供サービスを受けることができる。
この場合、ユーザ端末は、コンテンツ提供サービスを行なうホストコンピュータが、第一のホストコンピュータか否かを認識することなく、コンテンツ提供のサービスを受けることができる。
【００１７】
請求項６記載のコンテンツ提供システムは、上記ネットワークが、インターネットである構成としてある。
請求項７記載のコンテンツ提供システムは、上記第一のホストコンピュータおよび／または上記第二のホストコンピュータが、Ｗｅｂサーバである構成としてある。
【００１８】
コンテンツ提供システムをこのような構成とすると、インターネットにより接続されたＷｅｂサーバである第一のホストコンピュータが、インターネットを介してアクセスしてくる利用者のユーザ端末に対してコンテンツ提供サービスを行なう際に、不正アクセスの被害を受けたとき、第一のホストコンピュータから第二のホストコンピュータに切り替えて、コンテンツ提供のサービスを迅速に再開することができる。
【００１９】
請求項８記載のコンテンツ提供システムは、上記コンテンツが、ホームページであって、第二のホストコンピュータに複写されるコンテンツが、当該ホームページのトップページである構成としてある。
【００２０】
コンテンツ提供システムをこのような構成とすると、第一のホストコンピュータが提供するコンテンツとしてのホームページのうち、重要なページ例えばトップページを第二のホストコンピュータに複写しておくことにより、例えばトップページがセキュリティが強化され不正アクセスの被害を受けにくくしてある第二のホストコンピュータにより利用者に提供されることになる。
したがって、このような重要なページ、例えばトップページについて、セキュリティが強化され、不正アクセスを受けにくくしてあるので、例えば不正アクセスによりホームページのトップページが不正に改竄されたり、コンテンツ提供サービスが停止してしまうようなことがない。
【００２１】
また、上記目的を達成するため、本発明の請求項９記載のコンテンツ提供プログラムは、ネットワークを介して利用者のユーザ端末から送信されてきた指定情報に基づいて、第一のホストコンピュータに、コンテンツをネットワークを介してユーザ端末に送信させるコンテンツ提供プログラムであって、第一のホストコンピュータに、不正アクセスによる被害を受けたときに、コンテンツをネットワークに接続され、第一のホストコンピュータよりもセキュリティを強化された第二のホストコンピュータに転送させる処理と、第二のホストコンピュータに、第一のホストコンピュータから転送されてきたコンテンツを第二のホストコンピュータ自体に登録させ、第一のホストコンピュータの代わりに、ユーザ端

末からの指定情報に基づいて、当該コンテンツをネットワークを介してユーザ端末に送信させる処理を実行させる構成としてある。

【００２２】

コンテンツ提供プログラムをこのような構成とすると、何者かによる不正アクセスの被害を受けたとき、第一のホストコンピュータに代わって、第二のホストコンピュータに同じコンテンツの提供サービスを行なわせることにより、コンテンツ提供サービスの中断時間が大幅に短縮される。したがって、不正アクセスの被害によるコンテンツ提供サービスが迅速に再開されることになる。

【００２３】

この場合、第二のホストコンピュータを、セキュリティを強化することによって、不正アクセスの被害を受けにくくしてあるので、再び不正アクセスの被害を受けることが実質的にない。そして、第二のホストコンピュータによりコンテンツの提供サービスが行なわれている間に、第一のホストコンピュータについて、再度不正アクセスの被害を受けないように十分な対策が行なわれた後、再び第二のホストコンピュータから第一のホストコンピュータに切り替えて、コンテンツの提供サービスを行なうことができる。

【００２４】

さらに、上記目的を達成するため、本発明の請求項１０記載のコンテンツ提供プログラムは、ネットワークを介して利用者のユーザ端末から送信されてきた指定情報に基づいて、第一のホストコンピュータに、コンテンツをネットワークを介してユーザ端末に送信させるコンテンツ提供プログラムであって、ネットワークに接続され、第一のホストコンピュータよりもセキュリティを強化された第二のホストコンピュータに、第一のホストコンピュータからコンテンツの一部を第二のホストコンピュータにあらかじめ複写させて、第一のホストコンピュータの代わりに、ユーザ端末からの指定情報に基づいて、当該コンテンツをネットワークを介してユーザ端末に送信させる処理を実行させる構成としてある。

【００２５】

コンテンツ提供プログラムをこのような構成とすると、第一のホストコンピュータが提供するコンテンツの一部、例えば第一のホストコンピュータが提供するコンテンツとしてのホームページのうち、重要なページ例えばトップページを第二のホストコンピュータに複写しておくことにより、例えばトップページがセキュリティが強化され不正アクセスの被害を受けにくくしてある第二のホストコンピュータにより利用者に提供されることになる。

したがって、このような重要なページ、例えばトップページについて、セキュリティが強化され、不正アクセスを受けにくくしてあるので、例えば不正アクセスによりホームページのトップページが不正に改竄されたり、コンテンツ提供サービスが停止してしまうようなことがない。

【００２６】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照して説明する。

【００２７】

本発明のコンテンツ提供システムの第一の実施形態について、図１乃至図３を参照して説明する。

図１は、本実施形態のコンテンツ提供システムの構成を示すブロック図である。

【００２８】

図１に示すように、コンテンツ提供システム１０は、利用者１００と、コンテンツ提供センター２００と、ネットワーク３００と、を設けてある。

なお、図１においては、利用者１００は、一つだけ図示されているが、一つに限定されるものではない。

【００２９】

また、ネットワーク３００は、インターネット，一般公衆回線網あるいは専用回線網等のネットワークであって、インターネット接続サービスを提供するものである。

【００３０】
利用者１００は、コンテンツ提供サービスを受けようとする者であって、ネットワーク３００を介してコンテンツ提供センター２００に接続して、コンテンツ提供センター２００内に登録されたコンテンツを受信することができる。
なお、利用者１００は、コンテンツ提供センター２００にアクセスするための端末機器としての例えばパーソナルコンピュータ等のユーザ端末１１０や、携帯電話，ＰＨＳ等の各種情報端末機器や専用端末機器を使用することができ、このユーザ端末１１０の画面上に表示されるブラウザ等のソウトウェアによる画面表示にしたがって、コンテンツ提供センター２００にアクセスして、所望のコンテンツを受信できるようになっている。
【００３１】
さらに、利用者１００は、コンテンツ提供センター２００にアクセスするために、前もって利用者情報（氏名，住所，メールアドレス等）を登録して、当該利用者１００を一意に特定できる識別符号およびパスワードを有するようにしてもよい。
これにより、利用者１００が、コンテンツ提供センター２００に接続する際、ネットワーク３００を介して識別符号およびパスワードを送信することによって、コンテンツ提供センター２００が、利用者１００を一意に特定して、コンテンツ提供センター２００へのアクセスを許可する。
【００３２】
コンテンツ提供センター２００は、適宜の箇所に設けられた情報管理装置としての第一のホストコンピュータ２１０および第二のホストコンピュータ２５０から構成されている。
第一のホストコンピュータ２１０は、通常使用されるＷｅｂサーバ等のホストコンピュータであって、入出力部２２０と、記憶部２３０と、を有しており、アクセスしてくる利用者１００に対して、例えば企業等のホームページ等としてのコンテンツ２４０を提供する。
【００３３】
また、第二のホストコンピュータ２５０は、第一のホストコンピュータ２１０が不正アクセスの被害を受けたとき使用されるＷｅｂサーバ等のホストコンピュータであって、同様に入出力部２６０と、記憶部２７０と、を有しており、アクセスしてくる利用者１００に対して、例えば企業等のホームページ等としてのコンテンツ２８０を提供する。
なお、第二のホストコンピュータ２５０は、第一のホストコンピュータ２１０に対して、後述するように不正アクセスに対するセキュリティを強化してある。
【００３４】
ここで、上記入出力部２２０，２６０は、共にネットワーク３００に接続されており、利用者１００のユーザ端末１１０からネットワーク３００を介して送信されてくる指定情報１２０を受信して、この指定情報１２０に基づいて記憶部２３０，２７０から指定されたコンテンツ２４０，２８０を読み出して、ネットワーク３００を介して利用者１００のユーザ端末１１０に送信するようになっている。
【００３５】
　また、上記入出力部２２０，２６０のうち、第一のホストコンピュータ２１０の入出力部２２０は、ネットワーク３００を介して不正アクセスの被害を受けたとき、その記憶部２３０からコンテンツ２４０を読み出して、ネットワーク３００を介して第二のホストコンピュータ２５０に転送する。これにより、第二のホストコンピュータ２５０の入出力部２６０は、第一のホストコンピュータ２１０から転送されたコンテンツ２４０を、コンテンツ２８０として記憶部２７０に登録する。
　なお、転送されるコンテンツ２４０は、記憶部２３０に登録されている最新のコンテンツ、あるいは定期的にバックアップされているコンテンツが使用される。
【００３６】
上記記憶部２３０，２７０のうち、第一のホストコンピュータ２１０の記憶部２３０には、アクセスしてくる利用者１００に対して提供すべきコンテンツ２４０が登録されている。

また、第二のホストコンピュータ２５０の記憶部２７０は、第一のホストコンピュータ２１０が不正アクセスの被害を受けたとき、第一のホストコンピュータ２１０に登録されたコンテンツ２４０が第一のホストコンピュータ２１０により複写されて、コンテンツ２８０として登録される。

【００３７】

さらに、上記第一のホストコンピュータ２１０および第二のホストコンピュータ２５０は、それぞれＤＮＳ（ｄｏｍａｉｎ　ｎａｍｅ　ｓｙｓｔｅｍ）を備えており、このＤＮＳによりホスト名を示す所謂ＵＲＬとＩＰアドレスの対応付けを設定している。

【００３８】

そして、第一のホストコンピュータ２１０は、不正アクセスの被害を受けたとき、第一のホストコンピュータ２１０自身のホスト名に対して割り振られているＩＰアドレスを第二のホストコンピュータ２５０のＩＰアドレスに変更する。

その後、第一のホストコンピュータ２１０が不正アクセスに対するセキュリティ対策が完了した後、第一のホストコンピュータ２１０は、第一のホストコンピュータ２１０自身のホスト名に対して割り振られている第二のホストコンピュータ２５０のＩＰアドレスを再び第一のホストコンピュータ２１０自身のＩＰアドレスに変更する。

【００３９】

さらに、第二のホストコンピュータ２５０は、セキュリティを強化することによって、不正アクセスの被害を受けにくくしてある。

このセキュリティの強化は、例えば第二のホストコンピュータ２５０自体のセキュリティ対策と、ネットワーク３００上でのセキュリティ対策を実施することによって、行なわれる。

【００４０】

次に、本実施形態のコンテンツ提供システム１０によるコンテンツ提供について、図２～図３を参照して説明する。

コンテンツ提供システム１０は、図２に示す通常のコンテンツ提供作業，図３に示す不正アクセスを受けたときのコンテンツ提供作業の各ステップで利用される。

【００４１】

まず、通常のコンテンツ提供作業について、図２を参照して説明する。

図２において、利用者１００は、ユーザ端末１１０にて例えばブラウザ等のソフトウェアを立ち上げて、符号Ａ１で示すように、ネットワーク３００を介してコンテンツ提供センター２００のホスト名を指定して、コンテンツ提供センター２００の第一のホストコンピュータ２１０が提供するホームページにアクセスする。

そして、利用者１００は、符号Ａ２で示すように、ユーザ端末１１０により、所望のコンテンツを指定する指定情報１２０を、ネットワーク３００を介して、第一のホストコンピュータ２１０に対して送信する。

【００４２】

これを受けて、コンテンツ提供センター２００の第一のホストコンピュータ２１０の入出力部２２０は、符号Ａ３で示すように、利用者１００のユーザ端末１１０からネットワーク３００を介して送られてくる指定情報１２０に基づいて、記憶部２３０から指定されたコンテンツ２４０を読み出して、符号Ａ４で示すように、ネットワーク３００を介して利用者１００のユーザ端末１１０に対して送信する。

【００４３】

これにより、利用者１００のユーザ端末１１０は、符号Ａ５で示すように、ブラウザによりこのコンテンツ２４０を受信して、ユーザ端末１１０の表示部に画面表示する。したがって、利用者１００は、ユーザ端末１１０の表示画面を見ることにより、所望のコンテンツ２４０を視認することができる。

このようにして、通常のコンテンツ提供作業が完了する。

【００４４】

次に、不正アクセスの被害を受けたときのコンテンツ提供作業について図３を参照して説

明する。
図３において、コンテンツ提供センター２００の第一のホストコンピュータ２１０が、符号Ｂ１で示すように、不正アクセスの被害を受けると、第一のホストコンピュータ２１０は、符号Ｂ２で示すように、記憶部２３０に登録されているコンテンツ２４０を読み出して、ネットワーク３００を介して、第二のホストコンピュータ２５０に転送する。
これを受けて、セキュリティ対策が強化されている第二のホストコンピュータ２５０は、符号Ｂ３で示すように、第一のホストコンピュータ２１０から転送されたコンテンツ２４０を、コンテンツ２８０として記憶部２７０に登録する。
【００４５】
ここで、転送されるコンテンツ２４０は、そのとき記憶部２３０に登録されている最新または直前のコンテンツであってもよく、また定期的にバックアップされているバックアップデータとしてのコンテンツであってもよい。
特に不正アクセスの被害を受けたときには、記憶部２３０に登録されているコンテンツ２４０自体が改竄されているおそれがあるため、バックアップデータとしてのコンテンツを転送することが好ましい。
【００４６】
続いて、第一のホストコンピュータ２１０は、符号Ｂ４で示すように、当該第一のホストコンピュータ２１０のホスト名と割り振られたＩＰアドレスの対応付けを行なっているＤＮＳの設定を変更して、当該ホスト名に対応するＩＰアドレスを、第一のホストコンピュータ２１０のＩＰアドレスから第二のホストコンピュータ２５０のＩＰアドレスに変更する。
これにより、コンテンツ提供センター２００にてコンテンツ提供サービスを行なうホストが、第一のホストコンピュータ２１０から第二のホストコンピュータ２５０に切り替えられる。
【００４７】
この状態で、利用者１００が、符号Ｂ５で示すように、ユーザ端末１１０により、当該コンテンツ提供センター２００のホスト名で当該コンテンツ提供センター２００にアクセスすると、上述したＤＮＳのホスト名に対応付けられたＩＰアドレスの変更によって、自動的に第二のホストコンピュータ２５０にアクセスすることになる。
そして、利用者１００は、符号Ｂ６で示すように、ユーザ端末１１０により、所望のコンテンツを指定する指定情報１２０を、ネットワーク３００を介して、第二のホストコンピュータ２５０に対して送信する。
【００４８】
これを受けて、コンテンツ提供センター２００の第二のホストコンピュータ２５０の入出力部２６０は、符号Ｂ７で示すように、利用者１００のユーザ端末１１０からネットワーク３００を介して送られてくる指定情報１２０に基づいて、記憶部２７０から指定されたコンテンツ２８０を読み出して、符号Ｂ８で示すように、ネットワーク３００を介して利用者１００のユーザ端末１１０に対して送信する。
【００４９】
これにより、利用者１００のユーザ端末１１０は、符号Ｂ９で示すように、ブラウザによりこのコンテンツ２８０を受信して、ユーザ端末１１０の表示部に画面表示する。したがって、利用者１００は、ユーザ端末１１０の表示画面を見ることにより、所望のコンテンツ２８０を視認することができる。
【００５０】
この場合、利用者１００は、コンテンツ提供センター２００における第一のホストコンピュータ２１０から第二のホストコンピュータ２５０への切り替えを意識することなく、コンテンツ提供センター２００にアクセスして、所望のコンテンツを入手することができる。
また、第二のホストコンピュータ２５０は、前述したようにセキュリティを強化することによって、不正アクセスの被害を受けにくくしてあるので、実質的に不正アクセスの被害

を受けることがない。
【００５１】
このようにして、コンテンツ提供センター２００が第二のホストコンピュータ２５０によりコンテンツ提供サービスを行なっている間に、第一のホストコンピュータ２１０は、符号Ｂ１０で示すように、再び不正アクセスの被害を受けることがないように十分なセキュリティ対策が行なわる。
【００５２】
そして、第一のホストコンピュータ２１０は、符号Ｂ１１で示すように、再びＤＮＳの設定を変更して、当該ホスト名に対応するＩＰアドレスを、第二のホストコンピュータ２５０のＩＰアドレスから第一のホストコンピュータ２１０のＩＰアドレスに変更する。
これにより、コンテンツ提供センター２００にてコンテンツ提供サービスを行なうホストが、第二のホストコンピュータ２５０から第一のホストコンピュータ２１０に変更され、不正アクセスの被害を受ける前の状態に戻される。
【００５３】
そして、利用者１００のユーザ端末１１０からコンテンツ提供センター２００にアクセスがあった場合、図２に示すように、再び第一のホストコンピュータ２１０によってコンテンツの提供が行なわれる。
【００５４】
このようにして、不正アクセスを受けたときのコンテンツ提供作業が完了する。
この場合、コンテンツ提供センター２００の第一のホストコンピュータ２１０が不正アクセスの被害を受けたとき、コンテンツ提供センター２００のコンテンツ提供サービスを行なうホストが、第一のホストコンピュータ２１０から第二のホストコンピュータ２５０に切り替えられる。
これにより、コンテンツ提供サービスの中断時間が非常に短く、また利用者１００は、ホストコンピュータ２１０，２５０の切り替えを意識することなく、コンテンツ提供サービスを受けることができる。
したがって、コンテンツ提供サービスが見かけ上迅速に再開されることになると共に、切り替えられた第二のホストコンピュータ２５０は前もってセキュリティ対策が強化されているので、再び不正アクセスの被害を受けることが実質的にない。
【００５５】
次に、本発明のコンテンツ提供システムの第二の実施形態について、図４及び図５を参照して説明する。
図４は、本実施形態のコンテンツ提供システムの構成を示すブロック図である。
【００５６】
図４に示すように、コンテンツ提供システム２０は、利用者１００と、コンテンツ提供センター４００と、ネットワーク３００と、を設けてある。
ここで、利用者１００とネットワーク３００については、図１及び図３に示したコンテンツ提供システム１０における利用者１００とネットワーク３００と同様の構成であるので、その説明は省略する。
【００５７】
コンテンツ提供センター４００は、図１乃至図３に示したコンテンツ提供センター２００とは、第一のホストコンピュータ２１０の記憶部２３０に登録されるコンテンツ２４０のうち、一部のコンテンツ、例えばホームページのトップページ（例えばｉｎｄｅｘ．ｈｔｍｌ）を示すコンテンツ２４１が、第二のホストコンピュータ２５０の記憶部２７０に登録されており、第一のホストコンピュータ２１０の記憶部２３０に記憶されているコンテンツ２４０が、このコンテンツ２４１からリンクされている点でのみ異なる構成になっている。
そして、これに伴って、コンテンツ提供センター２００のホスト名またはニックネームに対応するＵＲＬは、第二のホストコンピュータ２５０のＩＰアドレスに対応付けられている。

【００５８】
次に、本実施形態のコンテンツ提供システム２０によるコンテンツ提供について、図５を参照して説明する。
コンテンツ提供システム２０は、図５に示すコンテンツ提供作業で利用される。
【００５９】
図５において、利用者１００は、ユーザ端末１１０にて例えばブラウザ等のソフトウェアを立ち上げて、符号Ｃ１で示すように、ネットワーク３００を介してコンテンツ提供センター４００のホスト名を指定して、コンテンツ提供センター４００が提供するホームページにアクセスする。
このとき、当該ホームページのトップページは、第二のホストコンピュータ２５０の記憶部２７０に登録されているので、利用者１００のユーザ端末１１０は、コンテンツ提供センター４００の第二のホストコンピュータ２５０にアクセスすることになる。
そして、利用者１００は、符号Ｃ２で示すように、ユーザ端末１１０により、所望のコンテンツを指定する指定情報１２０を、ネットワーク３００を介して、第二のホストコンピュータ２５０に対して送信する。
【００６０】
これを受けて、コンテンツ提供センター４００の第二のホストコンピュータ２５０の入出力部２６０は、符号Ｃ３で示すように、利用者１００のユーザ端末１１０からネットワーク３００を介して送られてくる指定情報１２０に基づいて、記憶部２７０から指定されたコンテンツ２４１を読み出して、符号Ｃ４で示すように、ネットワーク３００を介して利用者１００のユーザ端末１１０に対して送信する。
【００６１】
これにより、利用者１００のユーザ端末１１０は、符号Ｃ５で示すように、ブラウザによりこのコンテンツ２４１を受信して、ユーザ端末１１０の表示部に画面表示する。したがって、利用者１００は、ユーザ端末１１０の表示画面を見ることにより、所望のコンテンツ２４１を視認することができる。
【００６２】
そして、利用者１００がユーザ端末１１０の画面に表示されたコンテンツ２４１を見ながら、符号Ｃ６で示すように、例えば画面をクリックすることにより、トップページより深い階層の他のコンテンツ２４０を指定する指定情報１２０をネットワーク３００を介してコンテンツ提供センター４００に送信すると、このコンテンツ２４０が第一のホストコンピュータ２１０の記憶部２３０に登録されていることから、利用者１００のユーザ端末１１０は、コンテンツ提供センター４００の第一のホストコンピュータ２１０にアクセスすることになり、上記指定情報１２０は第一のホストコンピュータ２１０に送信される。
【００６３】
これを受けて、コンテンツ提供センター２００の第一のホストコンピュータ２１０の入出力部２２０は、符号Ｃ７で示すように、利用者１００のユーザ端末１１０からネットワーク３００を介して送られてくる指定情報１２０に基づいて、記憶部２３０から指定されたコンテンツ２４０を読み出して、符号Ｃ８で示すように、ネットワーク３００を介して利用者１００のユーザ端末１１０に対して送信する。
【００６４】
これにより、利用者１００のユーザ端末１１０は、符号Ｃ９で示すように、ブラウザによりこのコンテンツ２４０を受信して、ユーザ端末１１０の表示部に画面表示する。したがって、利用者１００は、ユーザ端末１１０の表示画面を見ることにより、所望のコンテンツ２４０を視認することができる。
このようにして、通常のコンテンツ提供作業が完了する。
【００６５】
また、コンテンツ提供センター４００のホスト名にてホームページのトップページに対して不正アクセスがあると、この不正アクセスは、第二のホストコンピュータ２５０に対して行なわれることになる。

ここで、第二のホストコンピュータ２５０は、前述したようにセキュリティを強化することによって、不正アクセスの被害を受けにくくしてあるので、実質的に不正アクセスの被害を受けることがない。

【００６６】

なお、一般的に不正アクセスは、ホームページのトップページに対して行なわれることが多いので、上述のように、トップページに対応するコンテンツ２４１を第二のホストコンピュータ２５０に登録して、ホームページを運用することにより、多くの不正アクセスが直接に第一のホストコンピュータ２１０にアクセスすることを回避することができる。

【００６７】

このようにして、本発明によるコンテンツ提供システム１０，２０によれば、コンテンツ提供サービスを行なうホストコンピュータ毎に、個別に不正アクセスに対するセキュリティ対策を強化することなく、第二のホストコンピュータ２５０のみについてセキュリティ対策を強化して、不正アクセスによる被害を受けにくくすることにより、低コストで不正アクセスに対するセキュリティ対策を行なうことができる。

【００６８】

また、コンテンツ提供システム１０によれば、不正アクセスの被害を受けた場合には、コンテンツ提供サービスを行なうホストを、第一のホストコンピュータ２１０から第二のホストコンピュータ２５０に切り替えることにより、コンテンツ提供サービスを迅速に再開することができると共に、利用者１００はホストコンピュータ２１０，２５０の切り替えを何ら意識することなく、コンテンツ提供サービスを受けることができる。

【００６９】

さらに、コンテンツ提供システム２０によれば、不正アクセスを受け易いホームページのトップページを、セキュリティ対策が強化されている第二のホストコンピュータ２５０に登録して、ホームページを運用することによって、不正アクセスによる被害を実質的に受けることがない。

【００７０】

上述した実施形態においては、第二のホストコンピュータ２５０は、コンテンツ提供センター２００を運営する事業者により設けられているが、これに限らず、別の業者によって設置されていてもよい。この場合、コンテンツ提供センター２００を運営する事業者は、通常は不正アクセスに対するセキュリティ対策を強化する必要がないので、コンテンツ提供センター２００の運営コストを低減することができる。

【００７１】

また、上述した実施形態においては、第二のホストコンピュータ２５０の記憶部２７０には、第一のホストコンピュータ２１０が不正アクセスの被害を受けたときに、そのコンテンツ２４０が転送されるようになっているが、これに限らず、定期的に行なわれるバックアップにより、コンテンツ２４０のバックアップデータが、第二のホストコンピュータ２５０の記憶部２７０に、コンテンツ２８０として登録されるようにしてもよい。

【００７２】

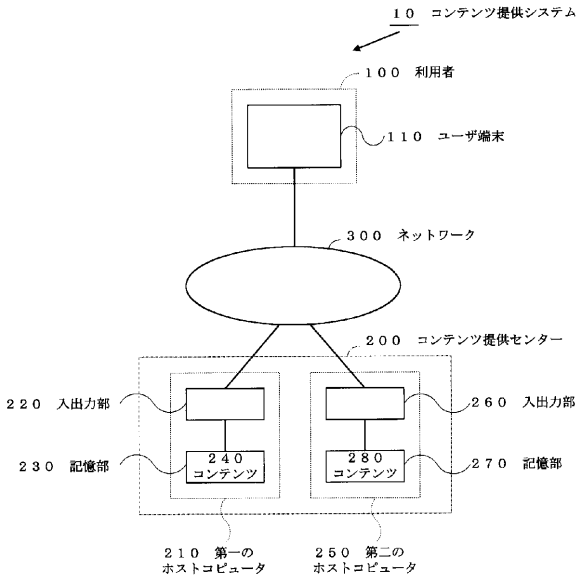
さらに、上述した実施形態においては、ネットワーク３００は、所謂インターネットとして構成されているが、これに限らず、例えば企業内ＬＡＮ等の構内ネットワークであってもよいことは明らかである。

さらにまた、上述した実施形態においては、第二のホストコンピュータ２５０は、第一のホストコンピュータ２１０に対してネットワーク３００を介して接続されているが、これに限らず、専用回線を利用して直接に接続されるようにしてもよい。

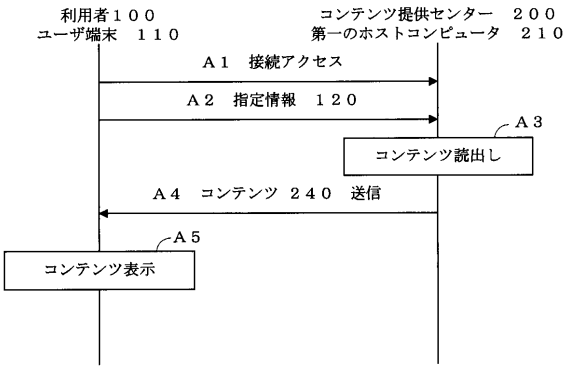
なお、上記実施形態におけるコンテンツ提供センターの情報処理装置である第一および第二のホストコンピュータでの処理は、プログラムに制御されることにより実行される。このプログラムとしては、例えば磁気ディスク，半導体メモリ，その他の任意のコンピュータで読み取り可能なものを使用することができる。また、プログラムは、プログラムを記録してある媒体を直接コンピュータに装着して当該コンピュータに読み込ませてもよく、また通信回線を介してコンピュータに読み込ませてもよい。

【００７３】
【発明の効果】
以上のように、本発明によれば、何者かによる不正アクセスの被害を受けたとき、第一のホストコンピュータに代わって、第二のホストコンピュータが同じコンテンツの提供サービスを行なうことにより、コンテンツ提供サービスの中断時間が大幅に短縮される。したがって、不正アクセスの被害によるコンテンツ提供サービスが迅速に再開されることになる。
この場合、第二のホストコンピュータは、セキュリティを強化することによって、不正アクセスの被害を受けにくくしてあるので、再び不正アクセスの被害を受けることが実質的にない。そして、第二のホストコンピュータによりコンテンツの提供サービスが行なわれている間に、第一のホストコンピュータについて、再度不正アクセスの被害を受けないように十分なセキュリティ対策が行なわれた後、再び第二のホストコンピュータから第一のホストコンピュータに切り替えて、コンテンツの提供サービスを行なうことができる。
【図面の簡単な説明】
【図１】本発明の第一の実施形態のコンテンツ提供システムの構成を示すブロック図である。
【図２】図１のコンテンツ提供システムにおける通常のコンテンツ提供作業を示すフローチャートである。
【図３】図１のコンテンツ提供システムにおける不正アクセスの被害を受けたときのコンテンツ提供作業を示すフローチャートである。
【図４】本発明の第二の実施形態のコンテンツ提供システムの構成を示すブロック図である。
【図５】図４のコンテンツ提供システムにおけるコンテンツ提供作業を示すフローチャートである。
【符号の説明】
１０，２０　コンテンツ提供システム
１００　利用者
１１０　ユーザ端末
１２０　指定情報
２００，４００　コンテンツ提供センター
２１０　第一のホストコンピュータ
２２０，２６０　入出力部
２３０，２７０　記憶部
２４０，２８０　コンテンツ
２４１　コンテンツ（トップページ）
２５０　第二のホストコンピュータ（セキュリティ強化ホストコンピュータ）
３００　ネットワーク

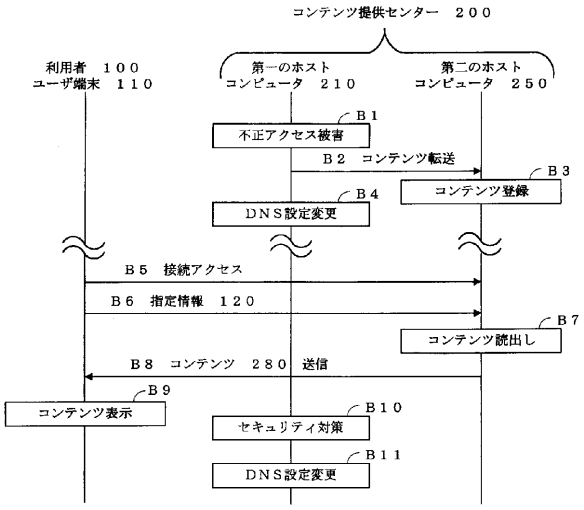
【図１】


１０　コンテンツ提供システム
１００　利用者
１１０　ユーザ端末
３００　ネットワーク
２００　コンテンツ提供センター
２２０　入出力部
２６０　入出力部
２３０　記憶部
２４０
コンテンツ
２８０
コンテンツ
２７０　記憶部
２１０　第一の
ホストコピュータ
２５０　第二の
ホストコピュータ

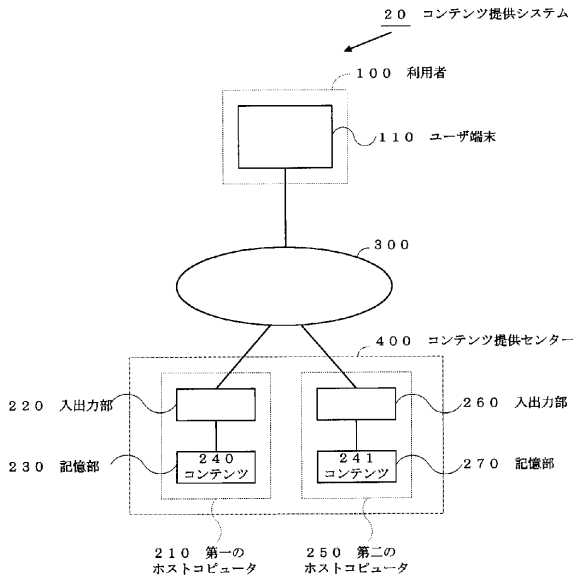
【図２】


利用者１００
ユーザ端末　１１０
コンテンツ提供センター　２００
第一のホストコンピュータ　２１０
Ａ１　接続アクセス
Ａ２　指定情報　１２０
Ａ３
コンテンツ読出し
Ａ４　コンテンツ　２４０　送信
Ａ５
コンテンツ表示

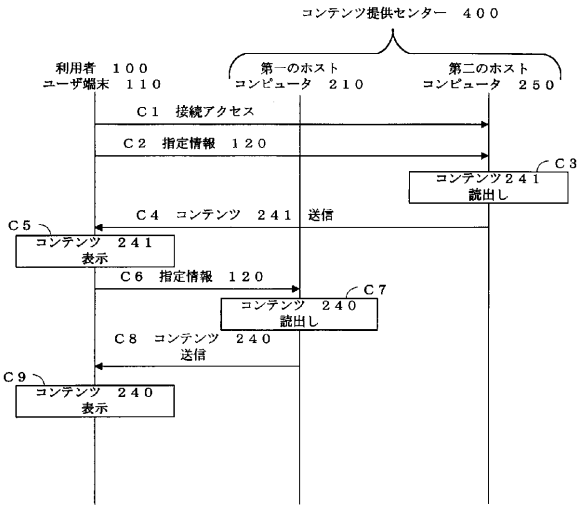
【図３】


コンテンツ提供センター　２００
利用者　１００
ユーザ端末　１１０
第一のホスト
コンピュータ　２１０
第二のホスト
コンピュータ　２５０
Ｂ１
不正アクセス被害
Ｂ２　コンテンツ転送
Ｂ３
コンテンツ登録
Ｂ４
ＤＮＳ設定変更
Ｂ５　接続アクセス
Ｂ６　指定情報　１２０
Ｂ７
コンテンツ読出し
Ｂ８　コンテンツ　２８０　送信
Ｂ９
コンテンツ表示
Ｂ１０
セキュリティ対策
Ｂ１１
ＤＮＳ設定変更

【図４】


２０　コンテンツ提供システム
１００　利用者
１１０　ユーザ端末
３００
４００　コンテンツ提供センター
２２０　入出力部
２６０　入出力部
２３０　記憶部
２４０
コンテンツ
２４１
コンテンツ
２７０　記憶部
２１０　第一の
ホストコピュータ
２５０　第二の
ホストコピュータ

【図５】


コンテンツ提供センター　４００
利用者　１００
ユーザ端末　１１０
第一のホスト
コンピュータ　２１０
第二のホスト
コンピュータ　２５０
Ｃ１　接続アクセス
Ｃ２　指定情報　１２０
Ｃ３
コンテンツ２４１
読出し
Ｃ４　コンテンツ　２４１　送信
Ｃ５
コンテンツ　２４１
表示
Ｃ６　指定情報　１２０
Ｃ７
コンテンツ　２４０
読出し
Ｃ８　コンテンツ　２４０
送信
Ｃ９
コンテンツ　２４０
表示

フロントページの続き

(51)Int.Cl. F I

G06Q 10/00 (2006.01) G06F 17/60 302E

G06F 17/60 512

合議体

審判長 江口 能弘

審判官 篠塚 隆

審判官 清水 稔

(56)参考文献 特開平10－135993（JP，A）

特開平10－27148（JP，A）

特開2000－349823（JP，A）

加藤幹一郎 他，「不正アクセス発信源追跡システムに対する多重化防御方式の検討」，第60回（平成12年前期）全国大会講演論文集（3），社団法人情報処理学会，2000年 3月14日，p．293－294

(58)調査した分野(Int.Cl.，DB名)

G06F 13/00