汎用PCを　シンクライアント化することによる

安全かつ多目的な　コンピュータ利用環境

汎用PCを　シンクライアント化することによる

安全かつ多目的な　コンピュータ利用環境

汎用PCを　シンクライアント化することによる

安全かつ多目的な　コンピュータ利用環境

汎用PCを　シンクライアント化することによる

安全かつ多目的な　コンピュータ利用環境

機械･OSの設定やプログラムを嗜好・間違い・悪意等々によって書き換える

⇒

次に使う時に不都合(あやしい壁紙・必要なプログラムのショートカットが消えている･ウィルス蔓延等々)

汎用PCを　シンクライアント化することによる

安全かつ多目的な　コンピュータ利用環境

機械･OSの設定やプログラムを嗜好・間違い・悪意等々によって書き換える

⇒ 次に使う時に不都合(あやしい壁紙・必要なプログラムのショートカットが消えている･ウィルス蔓延等々)

どうやって防ぐか

⇒ 書き換えられなくすれば良い

汎用PCを シンクライアント化することによる

安全かつ多目的な コンピュータ利用環境

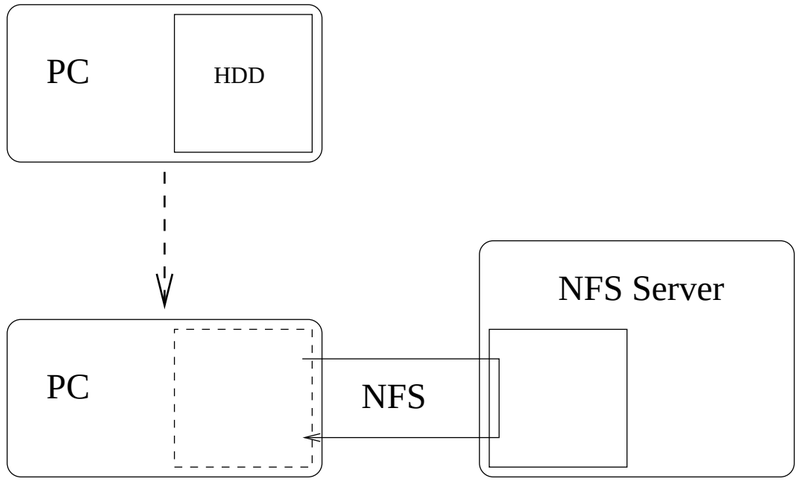
どうやって防ぐか

⇒ 書き換えられなくすれば良い

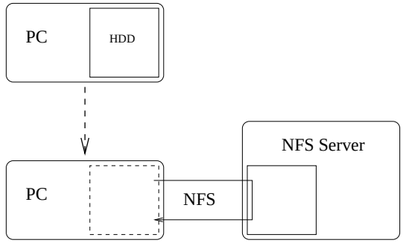
機械･OSの設定やプログラムを嗜好・間違い・悪意等々によって書き換える

⇒ 次に使う時に不都合(あやしい壁紙・必要なプログラムのショートカットが消えている･ウィルス蔓延等々)

- ディスクスペースを別の機械に移して(シンクライアント化)
- リードオンリーマウント



- ディスクスペースを別の機械に移して(シンクライアント化)



- リードオンリーマウント

どうやって防ぐか

⇒ 書き換えられなくすれば良い

- 授業によって複数のOSを使い分けたいが、機械を増やす金も場所も無い
- ユーザ別のディスクスペースも必要

- 普通のOSを完全にリードオンリーなファイルシステム上で動作させるのはややこしい

- 普通のハードウェアの上でOSを起動させると、アクセス制限をかいくぐる方法は沢山ある

⇒ · · ·

- 授業によって複数のOSを使い分けたいが、機械を増やす金も場所も無い
- ユーザ別のディスクスペースも必要

- 普通のハードウェアの上でOSを起動させると、アクセス制限をかいくぐる方法は沢山ある

⇒···

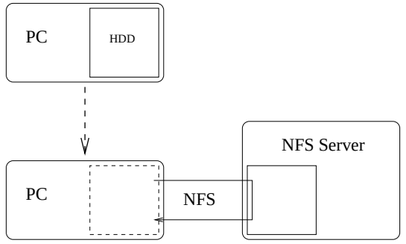
- 普通のOSを完全にリードオンリーなファイルシステム上で動作させるのはややこしい

- ディスクレスマシン上でVMwareを動かして、ターゲットOSはVMware上のゲストOSとして動かす

- ユーザ用スペースのためのファイルサーバを別に用意

- ディスクスペースを別の機械に移して(シンクライアント化)

- リードオンリーマウント



- OSの核はリードオンリーなスペースに置くが、一時ファイル等用の書き込み可能なスペースも用意する

- VMwareのsnapshot機能の一部を利用して、リードオンリーなスペースにあるOSの核部分も書き込み可能に見せかけるが、再起動すると元に戻るようにする

- ディスクレスマシン上でVMware を動かして、ターゲットOSはVMware上のゲストOSとして動かす

- ユーザ用スペースのためのファイルサーバを別に用意

- OSの核はリードオンリーなスペースに置くが、一時ファイル等用の書き込み可能なスペースも用意する

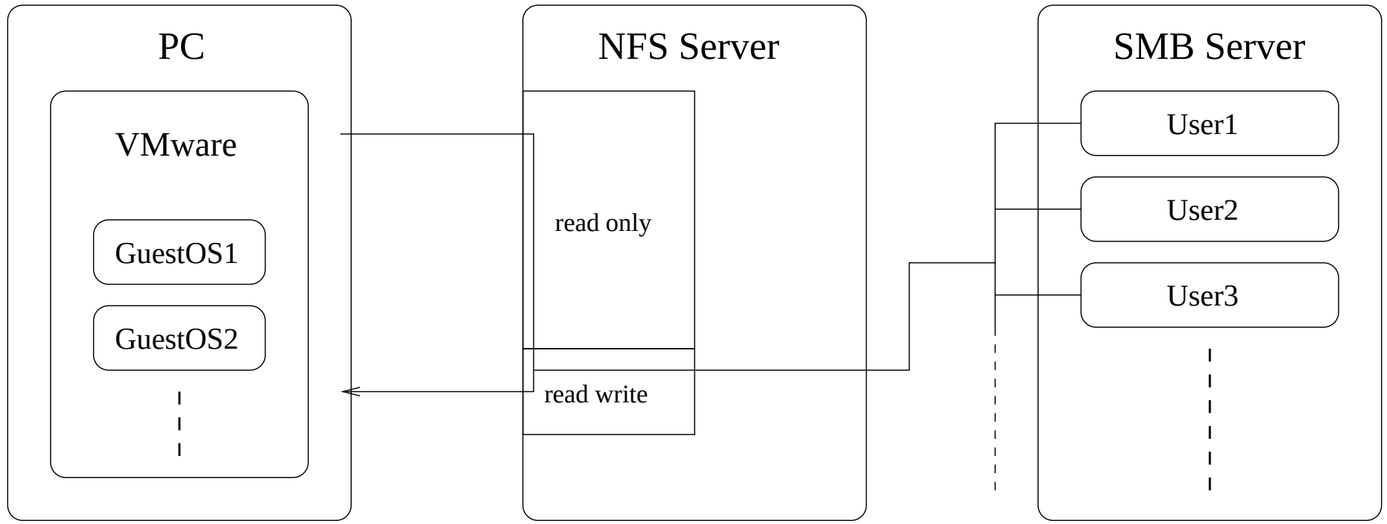
- VMwareのsnapshot機能の一部を利用して、リードオンリーなスペースにあるOSの核部分も書き込み可能に見せかけるが、再起動すると元に戻るようにする

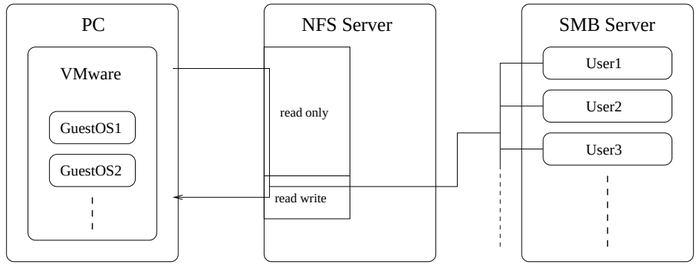
- 授業によって複数のOSを使い分けたいが、機械を増やす金も場所も無い
- ユーザ別のディスクスペースも必要

- 普通のハードウェアの上でOSを起動させると、アクセス制限をかいくぐる方法は沢山ある

⇒ · · ·

- 普通のOSを完全にリードオンリーなファイルシステム上で動作させるのはややこしい

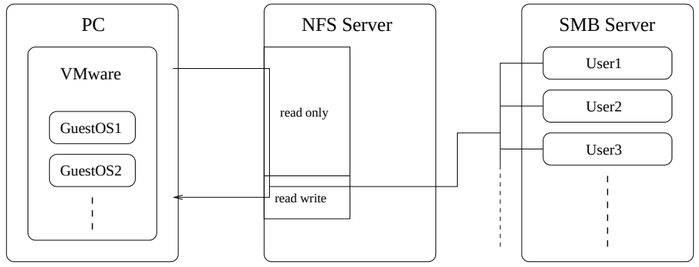


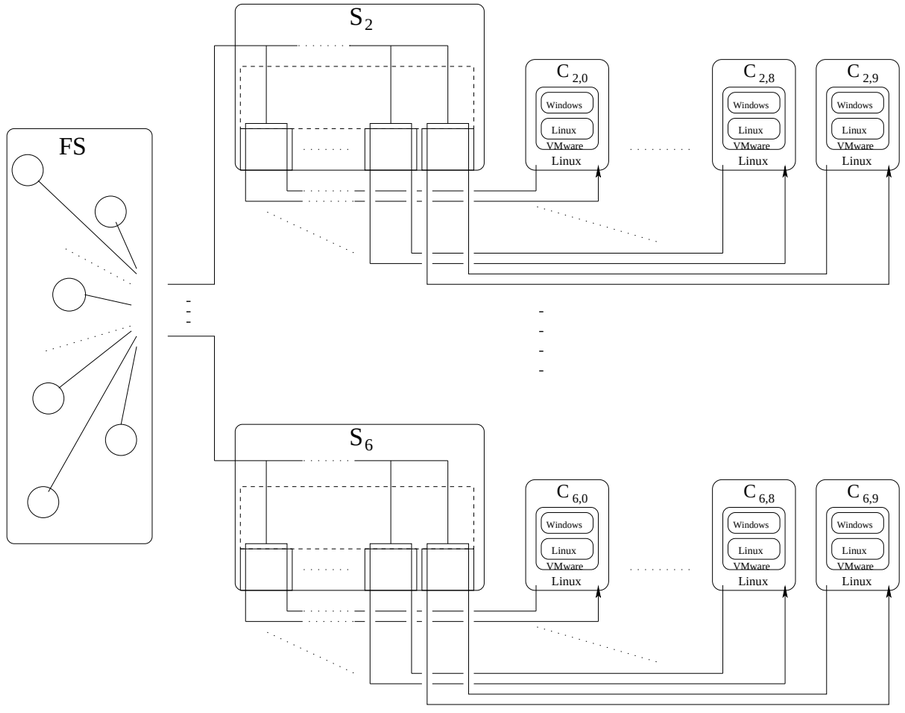


- ディスクレスマシン上でVMware を動かして、ターゲットOSはVMware上のゲストOSとして動かす
- ユーザ用スペースのためのファイルサーバを別に用意
- OSの核はリードオンリーなスペースに置くが、一時ファイル等用の書き込み可能なスペースも用意する
- VMwareのsnapshot機能の一部を利用して、リードオンリーなスペースにあるOSの核部分も書き込み可能に見せかけるが、再起動すると元に戻るようにする

- NFSサーバは各PCに対してNAT ルータとしても働き、各PCで万一あぶないネットワークサービスが起動していても、攻撃をブロック
- VMware のログやホストOSのログを監視して、VMwareの設定変更や、正体不明のUSB デバイスの接続等を完全に抑止
- VMware のホストOS とゲストOS間のファイル共有機能を利用して、ゲストOS にユーザ名や仮想機械の名前を知らせて、微妙に振舞いを変えさせることも可能
- 複数のNFSサーバを用意し、1個のサーバに接続するクライアント数を制限してパフォーマンスを稼ぎ、サーバどうしは互いのバックアップとしても機能する

- NFSサーバは各PCに対してNAT ルータとしても働き、各PCで万一あぶないネットワークサービスが起動していても、攻撃をブロック
- VMware のログやホスト OS のログを監視して、VMware の設定変更や、正体不明の USB デバイスの接続等を完全に抑止
- VMware のホスト OS とゲスト OS 間のファイル共有機能を利用して、ゲスト OS にユーザ名や仮想機械の名前を知らせて、微妙に振舞いを変えさせることも可能
- 複数の NFS サーバを用意し、1個のサーバに接続するクライアント数を制限してパフォーマンスを稼ぎ、サーバどうしは互いのバックアップとしても機能する





全体像

$S_2, \ldots, S_6$ … NFS サーバ
$C_{2,0}, \ldots, C_{6,9}$ … クライアント
FS … 各ユーザ用仮想ディスクのサーバ