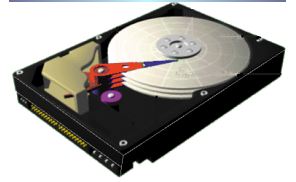


高速処理を実現したネットワーク版 PCデータ消去プログラム

RemoteClear Pro



「RemoteClear Pro」はネットワークに接続した状態で 同時に多数の消去対象パソコンのハードディスクを消去出来る画期的なプログラムとして開発しました。



商品構成

「パッケージ内容」

- ・管理コンソールプログラム RemoteClear Server RemoteClear GUI
- ・クライアント プログラム RemoteClear Client
- ・ハードウェアとして ICカード、ICカードリーダー/ライター 及び基本プログラム(各1個付属)



動作環境

【RemoteClear Server、RemoteClear GUI】

- ・PC/AT互換機 Pentium互換以上
日本語Windows 2000 Server/ Windows XP Pro / Windows Server 2003/ IIS 5.0以上

【RemoteClearクライアント】

- ・PC/AT互換機 Pentium互換以上
日本語Windows 98SE / Windows ME / Windows 2000 / Windows XP

開発背景

パソコン(PC)のリース / レンタル期限切れにともない、PCを返却、廃棄、リサイクルする際に格納されている機密データの存在が問題視されています。Windowsでのデータ書き込み時には、データと共にデータの呼出順序(インデックス)が書込まれており、記録されたデータの消去はOSの仕様上、完全フォーマットを行ってもインデックスのみが消去されるだけでデータそのものは消去されずに残ってしまいます。その為、市販のデータ復旧ソフトを使用しインデックス部分を復元させることにより、簡単にデータを復元することができてしまうことからHDDデータの完全消去の必要性が唱えられています。その上、年々増大するHDD容量により消去の手間や時間が無視できない状況となり、短時間に大量のPCを同時消去するニーズが高まってまいりました。

RemoteClearPro の特徴

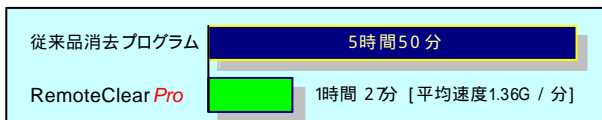
ネットワークを介して複数台のPCを同時消去が可能ですので省力化に寄与します。又、生きたネットワークに接続していることでPCデータは消去直前までセキュリティ管理下にあります。消去完了後、初めてネットワークから外すことで実消去までの空白時間が存在しないため極めて安全です。

消去対象PCの特定や管理コンソールとの通信セッション確認など誤消去を防止する仕組みを確立。消去命令を出す管理コンソールを起動するにはICカード認証が必要で操作者を限定することができます。消去プログラムはセッション確立後、ダウンロードされる消去管理情報に基づき消去FDが作成されます。消去完了と共にプログラムは消滅する仕組みで消去プログラムの散逸を防ぎ、安全性が確保されます。

消去時間は業界トップレベルを実現、弊社の従来品と比較して3～4倍のスピード消去が可能ですので、大容量のHDDデータ消去や数回の上書き指定でも作業時間を大幅に短縮できます。

40GB 消去時間比較

米海軍準拠方式書込み
[固定値1、固定値2、固定値3、検証]



消去時間は選択した消去方式やPCのハードウェア環境によって左右されます。

その他の特徴

- ・管理コンソール上では、多数の消去対象PCの進行状況を文字や色によって表示することで瞬時に状態把握できるGUIを準備しています。
- ・プログラムの取扱いを起動用、消去用（起動用に消去用プログラムを加えたもの）と2段階に分けると共に最終の消去命令は第二パスワード認証を求めるなど消去プログラムの管理、セキュリティには留意しています。
- ・消去対象PCの一部がネットワーク接続できないケースも想定し、管理コンソールではスタンドアローン型の消去FDを作成できる機能を有しています。作成されたFDで消去した情報や消去ログはネットワークで消去したデータと共に管理されますので業務の一貫性を維持できます。
- ・消去プログラムは扱いを誤るとウイルス同様に危険な道具ともなりかねません。そこでネットワーク上から多数の消去対象PCのみを安全に消去するため、**厳格なセキュリティの仕組みを考案し特許出願**いたしました。

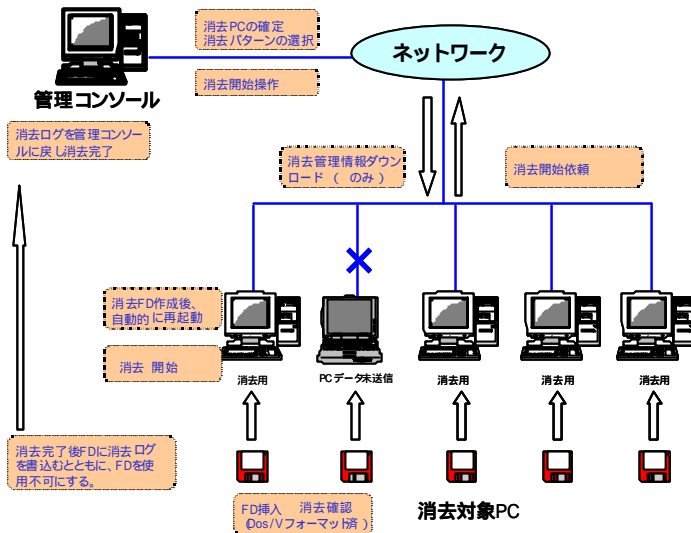
消去方法

管理コンソール上で消去パターンを選択するとともに消去対象PCの確定作業を行い、消去準備を行う。

[消去対象PCの個別情報を登録ツールによって事前に管理コンソールに登録しておく必要があります。登録作業の外、資産管理データを消去管理テーブルとして使用することも可能です。]

消去方式	書き込み回数	書き込みパターン
乱数r回 (n=1~9)	n回	乱数r回
NSA推奨方式	3回	乱数回 0
米陸軍準拠方式	3回	乱数回 固定値1 固定値
米海軍準拠方式	3回	固定値1 固定値2 固定値3 検証
米空軍準拠方式	7回	(0 1)×3回 固定値1 検証
米国防総省準拠方式	3回	固定値1 固定値2 乱数1回 検証
NCSC準拠方式	3回	固定値1 固定値2 固定値3
NCSC準拠方式×2	6回	NCSC準拠方式×2回
ゲートマン推奨方式	35回	乱数4回 固定値1 ... 固定値27 乱数4回

消去対象PCのFDドライブにFDを挿入する。
消去対象PCのクライアントソフトから管理コンソールに消去開始依頼を行うとともに、現状の個別情報を管理コンソールに送信する。管理コンソールでは 予め登録していた情報と比較し、同じであれば通信セッションを張る。
管理コンソールの起動にはICカード認証を必要とし、消去開始命令時にはさらに第二パスワード認証作業を必要とします。
消去対象PCでは管理コンソールよりダウンロードされた消去管理情報に基づき消去FDが作成される。
消去FDが作成されると消去対象PCが自動的に再起動される。
再起動後 で選択した消去パターンに従って消去が開始される。
消去完了後FDに消去ログを書き込むと共に消去プログラムは使用不可となる。
消去完了ログを管理コンソールにインポート又は、別PCの登録用プログラムから送信し、消去完了となる。

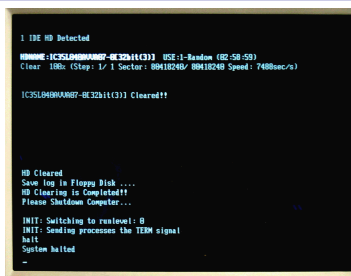


消去フロー

状態	ネットワーク消去対象PC 操作	管理コンソール 操作	スタンドアローン操作
事前準備	消去PC通信情報の送信	消去PC情報登録	
初期		消去確定作業	FD作成
消去確定	FDを挿入・FD作成をクリック		
消去待機	実行	消去開始作業	
消去開始	消去プログラムダウンロード		
消去中	再起動 消去開始 消去完了		
消去完了	ログ情報送信	消去完了[登録]	FD回収ログ確認

検証方法 [消去証明]

- ・消去開始後は消去経過を各消去 PC モニター画面上で確認することができます。消去状態は%表示されますので進行状況の把握が可能です。消去完了時には完了画面が表示されます。
- ・消去完了後、消去 Log をテキスト形式でFDに書き出します。さらに、指定した消去アルゴリズムで確かに消去終了したのかを確認するため、再度 HDD を読み込み実データを抽出します。結果はバイナリーデータとして取り出すことができます。これにより詳細な消去証明書を管理コンソールで作成することができるほか、消去証明を一覧表形式で印刷することも可能です。
- ・主な消去ログ項目として、消去方式、PC管理番号、HDD型名、HDD製造番号等を記録しますので、データ消去を行った媒体の特定が出来ることでより消去トレースの信頼性を高めています。



消去完了画面 (PC画面にて)

消去証明書 (印刷)



開発元

株式会社CSPフロンティア研究所

〒151-0073 東京都渋谷区笹塚3-2-3 CSPテクノプラザ

TEL : 03-5304-4521 FAX: 03-5304-4522

Email : info@csp-frontier.jp

販売元