2003－ＭＢＬ－27　(9)
2003－ＩＴＳ－15　(9)
2003／11／14

データ保護機能を有する電子保存システムの開発 －モバイル端末への適応－

Development of Data Storage System for the Personal Data Protection －For Mobile Terminal－

青野正宏[*1] 小尾高史[*2] 山谷泰賀[*2] 山口雅浩[*2] 大山永昭[*2]
谷内田益義[*2] 細田泰弘[*3] 佐藤能行[*4] 菅生清[*5] 藤岡伸男[*6]
Masahiro Aono　Takashi Obi　Masahiro Yamaguchi　Taiga Yamaya　Nagaaki Oyama
Masuyoshi Yachida　Yasuhiro Hosoda　Yoshiyuki Sato　Kiyoshi Sugo　Nobuo Fujioka

我々は、ユーザが作成・収集したファイルの更新履歴を、コンピュータウィルスの支配が及ばない安全なサーバで保護することにより、利便性と安全性を両立させた電子データ保護システムを、定位置固定システムを対象に開発した。本稿では、モバイル端末を対象としたシステムへの拡張を検討する。

We have developed the electronic data protection system for a stationary computer, which has convenience and safety. Since the server of the system is not attacked by computer viruses, it can protect the user file update history. In this paper, we discuss the electronic data protection system for a mobile terminal.

1. はじめに

情報システムにおいて、生きている情報はコンピュータシステムのハード・ディスクに一時保存しておくことが便利である。固定ディスクの大容量化により、映像・音声・画像などを除いた狭義のデータのみであれば、ディスクのみで個人が管理する情報は十分保存できるほどである。

しかし、コンピュータシステムにおいて、ディスクの情報は書き換え可能であるため、紛失する危険も大きい。特に、悪質なコンピュータウィルス（以下ウイルスと略す。）によるファイル削除や書き換え攻撃に遭えば被害は大きい。オペレーティングシステムやアプリケーションプログラムは再インストールすれば復元することも可能である。しかし、ユーザの個人的ファイルはそのディスクのみに情報が保存されているのであれば、復元することが不可能である。

ウイルスによる被害をなくすため、多くのベンダがアンチウイルスソフトウェアを開発しているが、確実にウイルスを検出できる手法はない。特に新しいウイルスに対しての検出能力は低い。また、ファイルの更新履歴を保存し、任意の時点の状態まで復元を図るという手法が、製品として存在する[1]。しかし、当該システム上に更新領域を設けているため、その領域自身を攻撃されないという保証はない。さらに、更新履歴を外部のシステムに保存する方式[2]も存在するが、単に外部出力のみでは、更新履歴出力そのものがウイルスなどにより遮断されてしまえば効果がない。このように既存技術ではデータの保全を充分に図ることは困難である。

そのため、われわれは、プロセッサを分離す

*1 東京工業高等専門学校
*2 東京工業大学
*3 NTT コミュニケーションズ
*4 富士総合研究所
*5 リコーシステム開発
*6 日本電気

ることにより、ウイルス支配ができないサーバに領域を設け、そこでファイル更新履歴を保護することにより、ファイル保全を可能とするシステムを開発した。副次的効果として誤操作や悪意のないプログラムバグ、ハードウェア障害などによるファイル破壊からもデータを守ることができる。

2. データ保護システムの基本アーキテクチャ

基本的な考え方は次のとおりである。

2．1 対象

本システムの対象は事務用や個人用に使用されるパーソナルコンピュータ(以下、PC と略す。)を主要なターゲットとしている。具体的なイメージは次のとおりである。業務や個人的に必要なデータをシステム内に保存するとともに、やや危険なメール閲覧や WEB 閲覧をすることもある。データ紛失に関する影響度は直前に作成や入手したデータの紛失は、作り直しや再送依頼をすることも可能なので致命的ではない。しかし、過去からの蓄積保存データを失うことは大きな損失である。

2．2 耐ウィルスシステム

広義のウイルスに対するファイル破壊を防止すること（データ保護）が本研究の第一の目的であるが、ウイルスを検出し駆除することは直接の目的としていない。ウイルスによるファイル破壊活動の被害に遭っても、ファイル復元を可能にすることを目的とする。その意味で抗（アンチ）ウィルスシステムでなく耐ウィルスシステムである。従って、既存の抗ウイルスソフトウェアに取って代わるものでなく、併用することを前提としている。その基本原理は、ファイルの更新（新規作成、消去を含む。）が発生した場合、更新の記録を保存することにより万一ファイルの破壊が発生した場合、更新履歴から復元を行うことにより、ファイルの保全を行うものである。また、ウイルスのみでなく、汎用ソフトウェアのバグや捜査ミス、ハードウェア障害によるファイル紛失にも有効に作用する。

2．3 未知のウイルスへの対応機能

既知のウイルスの行動パターンのみでなく未知のウイルスにも対応できるものとする。本システムの仕様は運用時にユーザが設定する暗号鍵を除いて、公開または解読されることを前提とする。従って、本システムの仕様を熟知して仕掛けてくるウイルス攻撃にも耐えられることが必要である。なお、システムを使用するユーザ及びシステム管理者は信頼できるものとする。

2．4 モバイルコードの実行を認めるプロセッサと認めないプロセッサとの多重構成

一般的なコンピュータシステムでは、エージェントや Office のマクロプログラムなどの外部から読み込んだプログラム(モバイルコード)の実行を認めている。モバイルコードの実行を認めなければ、システムの利便性が著しく減少するからである。しかし、モバイルコードにウイルスが潜んでいれば、ウイルスにシステムを乗っ取られ、ファイルを勝手に消去される危険が存在している。そのため、モバイルコードの実行を認めるプロセッサ（フレキシブル・プロセッサと呼ぶこととする。）と認めないプロセッサ（クリーン・プロセッサと呼ぶこととする。）の両方で構築する。フレキシブル・プロセッサはウイルスに乗っ取られる危険もあるが、ファイル保全に関する必要な保護はクリーン・プロセッサに任せることにより、データの保全を図る。クリーン・プロセッサは外部から読み込んだ情報はあくまでデータとして扱い、制御権をモバイルコードに渡すことはしない。クリーン・プロセッサのプログラムは目的を限定し、複雑な機能を搭載する必要性がないため、セキュリティホールの危険性は小さい。

2．5 基本構成とその役割

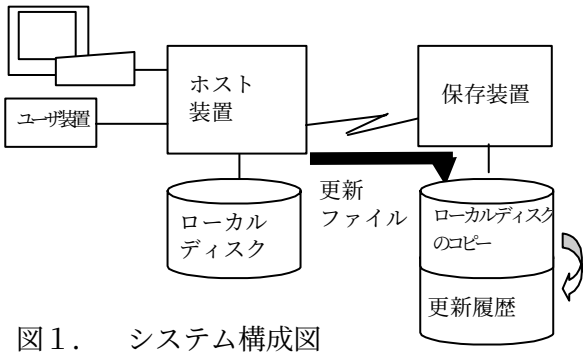

図１．　システム構成図

基本システムは、フレキシブル・プロセッサであるホスト装置とクリーン・プロセッサであるユーザ装置および保存装置から構成する。ホスト装置は、汎用のＯＳやソフトウェアを動作させる一般的なコンピュータである。これに、本システム用のソフトウェアを追加インストールして構成する。現用の一般的なコンピュータの使い方をそのまま認めるので、モバイルコードの実行も有りうる。従って利便性は現行のコンピュータ利用法と同様に確保される。しかし、ウイルスに侵される危険もある。保護対象となるホスト装置のファイルが更新されれば、ホスト装置からホスト装置とネットワークで接続されているサーバとしての保存装置に変更情報を送る。ここでファイルの更新とは、ファイルの新規作成、消去、名前の変更、ディレクトリの変更なども含む。保存装置は、保護対象となるホスト装置のファイルの複製を保持するとともにファイルの更新履歴を管理する機能を有する。保存装置はファイル更新情報を受信するとホスト装置の保護対象ファイルの複製を更新する。同時にファイルの更新履歴情報を保存装置の更新履歴領域に書き込む。更新履歴情報は更新の種別情報や更新の種別がファイルの書き換えや消去の場合は更新前の情報を記録する。この保存装置はクリーン・プロセッサとし、ウイルスが浸入する余地をなくす。保存装置はユーザと離れた場所にある場合が一般的であるので、保存装置とユーザとの情報交換のためユーザ装置を設ける。ユーザ装置は、USB などでホスト装置に接続する簡易なインテリジェント端末であり、クリーン・プロセッサとして構成する。ユーザ装置と保存装置間の情報交換はホスト装置を経由して行う。 (図 1 参照)

2．6 データ保護

ホスト装置の保護対象のファイルが物理的要因により傷つけられた場合は、保存装置に複製が残されているため復元が可能である。また、誤操作、ソフトウェアのバグ、ウイルスによる悪意のファイル消去などにより、ホスト装置のファイルが破壊された場合は、保存装置の複製も破壊されるが、ファイル更新前の履歴情報が保存装置に残されているため、この履歴情報を用いて復元することが可能である。[3]

3. 基本アーテクチャに対するウイルス攻撃の課題と対策

前章で述べた基本アークテクチャのみでは、いくつかの弱点が存在する。その弱点と対策について、以下に述べる。

3．1 ファイル更新情報の出力妨害

ホスト装置を乗っ取ったウイルスが、保存装置に出力するファイル更新情報の出力を妨害したり、その内容を改ざんしたりする攻撃方法が考えられる。この場合、ホスト装置のファイルと保存装置の複製ファイルが不一致となる。保存装置のファイル更新履歴も不正確となる。この状態でホスト装置のファイルが破壊されると、そのファイルの復元は不能となる。また、ウイルスによる妨害でなくても、ホスト装置から保存装置に出力する更新ファイルが、通信障害などの理由で届かないこともある。このとき、ホスト装置のファイルが正常である間に、ユーザがホスト装置のファイルと保存装置のファイルの不一致に気がつけば、正常な状態に戻すことができる。

このため、定期的にホスト装置のファイルと保存装置のファイルが一致していることを確認する。ファイル一致の確認の方法としてホス

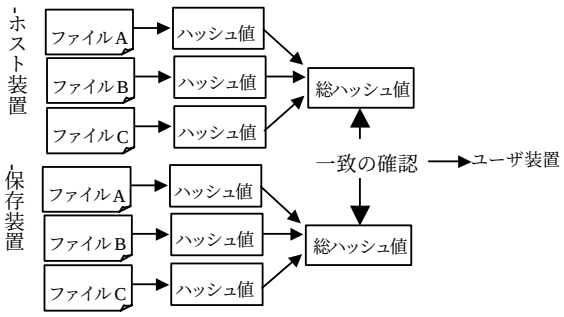

図 2. ファイル一致確認の方法

ト装置と保存装置それぞれが、異なる元データから同じ計算結果を求めることが困難なハッシュ計算法を用いて、ハッシュ値を求める。このハッシュ値が一致していれば、両装置のファイルは一致しているものとみなす。このとき、保護すべきファイルの総サイズが大きいとハッシュ値計算に時間がかかる。また、保存装置に送る更新ファイルの内容を暗号化する場合は、保存装置とホスト装置のファイルのハッシュ値を一致させることはできない。このため、個々のファイルのハッシュ値をファイルが更新されるたびに、ホスト装置と保存装置それぞれが計算し、それぞれ記憶しておく。(保存装置にファイルを暗号化して送る場合は、ホスト装置で暗号化後のハッシュ値を計算する。) ファイル一致確認の必要が生じると、ホスト装置と保存装置それぞれが、各ファイルのハッシュ値から総ハッシュ値を計算し、ホスト装置から保存装置に送って、一致の確認を保存装置で行なう。もし、不一致であれば、その情報をユーザ装置に送って、ユーザに警告を行う。(図 2 参照)

次の場合を想定する。ホスト装置でファイルを作成したとき、ホスト装置のウイルスがそのファイルの情報を保存装置に送ることを妨害する。保存装置から総ハッシュ値計算要求が来たとき、保存装置に送ることを妨害したファイルのハッシュ値を計算から除外して総ハッシュ値を求めれば、保存装置で計算した総ハッシュ値と一致させることができてしまう。その結果、ウイルスは、ホスト装置のファイルと保存装置のファイルが不一致であるにかかわらず、ユーザにそれを気付かせないことができてしまう。

その対策として、ファイル更新を保存装置で検出すれば、ユーザ装置にその情報を伝える。ユーザ装置は着信音でユーザにファイル更新を知らせる。ユーザはファイル更新処理のアクションを行ったにもかかわらず着信音がなければ異常に気がつくことができる。これで信頼性が大きく向上する。

ホスト装置をウイルスが支配しているとすれば、保存装置に送り出した偽の更新ファイルのハッシュ値をホスト装置内に記憶しておいて総ハッシュ値計算要求がくれば、そのハッシュ値を用いて計算すれば保存装置の総ハッシュ値と一致させることは可能である。しかし、そのためには、ウイルスは極めて複雑で難しい機能を必要とする。そうであれば、そのようなウイルスは特殊であるから比較的抗ウイルスソフトで検出が容易であると考えられる。仮にそのウイルスが活動し、ホスト装置のファイルと保存装置のファイルが不一致となっても、ホスト装置のファイルが破壊される前にユーザが、ウイルスに気がつけばデータ保全が可能である。またホスト装置のファイルが破壊されても、被害は、不一致状態になった後の更新ファイルに限られる。このため、上述の対策で許容できるものと考えた。

3.2 更新履歴領域食い潰し攻撃

保存装置における更新履歴領域は当然のことながら有限であるため、異常検出時に復元できるファイルの量には限界がある。そのため、仮にウイルスが大量のファイル破壊や同一ファイルの多数回繰り返し更新を行えば、正常なファイルまで復元できないおそれがある。このため、保存装置は短期間に閾値を越える大量のファイル更新情報が送信されてきたとき、保存装置の複製ファイル更新を一時中断し、更新正当性の可否をユーザ装置経由でユーザに問い

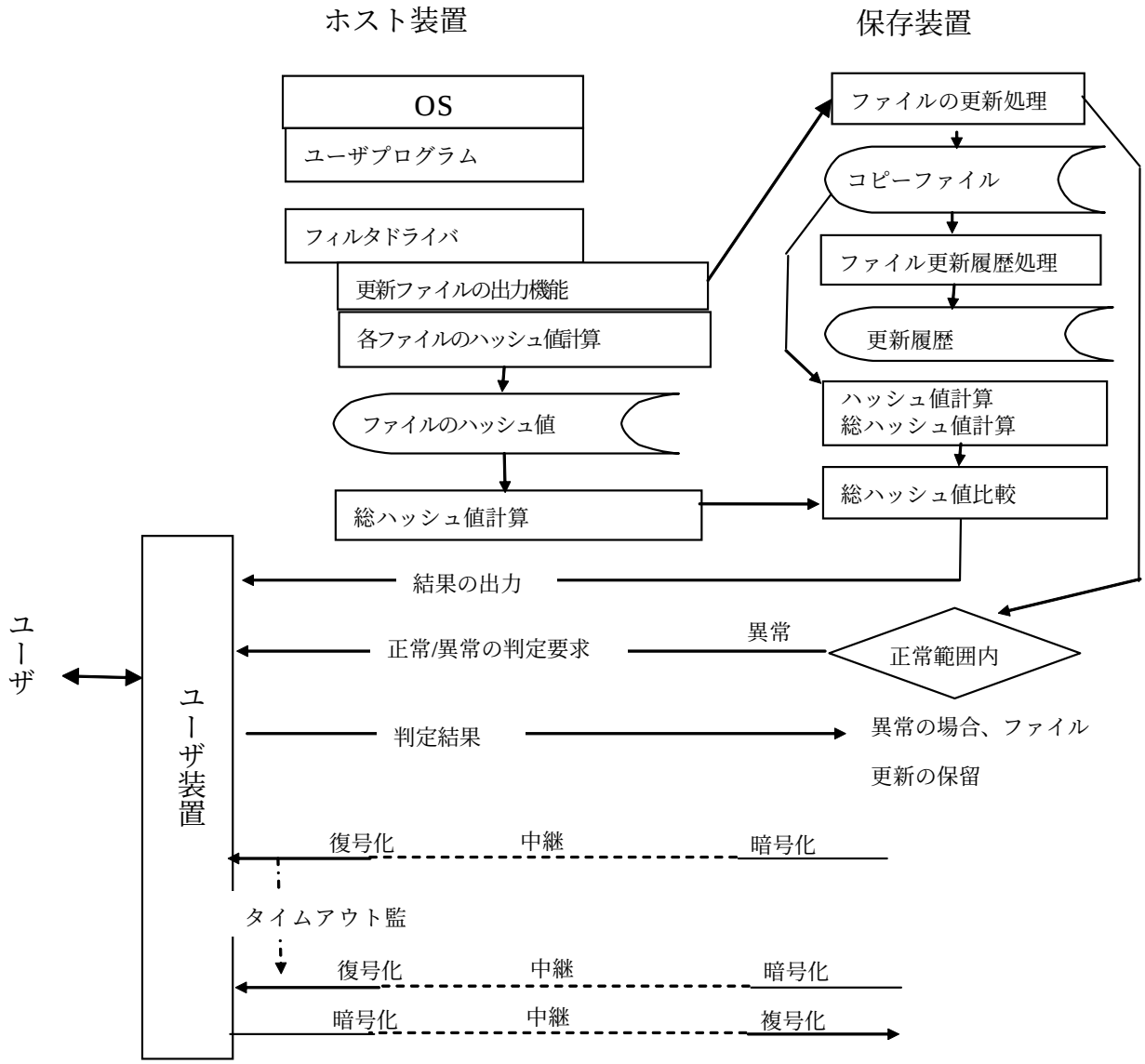

図 3 データ保護システムの主要ソフトウェア構成

合わせる。ユーザが正当であると判断すれば、続行の指示をユーザ装置に入力し、ユーザ装置から保存装置に回答して処理を続行する。ユーザが異常であると判断すれば、処理を中断してウイルス駆除など必要な手段を講じる。

3．3 保存装置とユーザ装置の通信中継妨害

保存装置からユーザへの警報や確認の情報及びユーザから保存装置への応答やファイル復元要求などの情報は、ホスト装置、ユーザ装置を経由して行う。ホスト装置がウイルスに支配された場合、この通信の妨害や改ざん、なりすましが行われる危険がある。そのため、保存装置とユーザ装置間の通信は暗号化して行う。ホスト装置が中継を行わずに遮断する場合も考慮して、ヘルシーメッセージをユーザ装置と保存装置間で交換する。交換するメッセージの通番管理により、ホスト装置が選択的に交換メッセージを遮断しても、ユーザは異常に気がつき、回復処理をとるきっかけを掴むことができる。[4]

4. システムのソフトウェア

ホスト装置は汎用のクライアントＰＣで構

築可能であり、汎用 OS のアプリケーション、更新ファイルの送信と各ファイルのハッシュ値を計算・保存するフィルタドライバ、ユーザ装置と保存装置間で情報の中継を行う中継プログラム、各ファイルのハッシュ値を用いる総ハッシュ値の計算プログラム、ファイルをホスト装置と保存装置間で一致させる同期化や復元の処理を保存装置と連携して行うファイル管理プログラムなどをインストールする。

保存装置はサーバとしての役割を果たす。1 つの保存装置で複数台のホスト装置に対応可能である。例えば事務所であれば部門ごとに 1 台の専用サーバとして設置すれば良い。家庭の個人のＰＣであれば、プロバイダが保存装置を付加サービスとして実現する方法が考えられる。あるいは、ホームネットワークが発達すればホームサーバに保存装置の機能を持たせることもできる。汎用のサーバをベースに構築可能であるが、モバイルコードの実行機能は排除しなければならない。保存装置の機能としては、対象となるホスト装置ファイルの複製を持つ機能、ファイル更新履歴を管理する機能、ホスト装置からのファイル更新情報を監視する機能、ユーザに適宜情報を伝える機能、保存装置の複製ファイルのハッシュ値を計算する機能、ユーザ装置からの指示を受けてファイルの同期化や復元処理を行う機能を有する。

ユーザ装置のみは、後述するモバイル端末の場合を除いて、専用のセットトップボックス(以下、STB と略す。)を想定している。ホスト装置を中継して保存装置と通信を行う機能を有するため、コマンドや警告、応答の入出力機能、ヘルシーメッセージ交換機能、メッセージの暗号化復号化機能を有する。また、保存装置に更新ファイルを送るときに暗号化を行うとすれば、復元に備えてその鍵をホスト装置とともにユーザ装置にも保持しておく必要がある。

保存装置は常時稼動を前提とするが、ホスト装置は必ずしも常時稼動しているとは限らない。従って保存装置から見て、ホスト装置との接続が切れていても必ずしも異常ではない。逆にユーザがホスト装置／ユーザ装置が動作させたときは、保存装置と接続されていなければ異常と判断することにより、ウイルスの妨害活動を監視する。(図 3 参照)

5. モバイル端末におけるデータ保護

5. 1　モバイル端末の特徴

これまで述べたとおり、我々が現在開発しているデータ保存システムのユーザ装置はホスト装置に STB として接続する形態を想定している。このシステムのホスト装置は、定位置で使用することを前提としている。(以下、定位置 PC と呼ぶ。) しかし、モバイル端末をホスト装置 (以下、モバイル PC と呼ぶ。) とする場合、次の問題がある。

- モバイル PC がホスト装置の場合、端末使用時でも、保存装置と接続されているとは限らない。
- ユーザ装置を携帯することは、実用上困難である。

従って、モバイル PC がホスト装置の場合、定位置の場合とは少々異なるアーキテクチャが必要である。

5. 2　モバイル端末の利用形態とデータ保護の必要性

モバイル端末に関してデータ保護の必要性はどの程度あるだろうか。ユーザにより、三通りの使用形態が考えられる。

第 1 の形態は、同じモバイル端末を職場や自宅で作業するときも外出時も、常時同じ端末を使用する場合である。データの重要性は定位置ホスト装置の場合と変わらない。

第 2 の形態は、ユーザは定位置 PC を職場やホームに持ち、大部分の作業は定位置ホスト装置を用いて作業を行う。第二の PC として、モバイル PC を持ち外出時に使用する。重要なデータは定位置ホームにある PC のディスクにある。外出時には必要なデータのみをモバイル

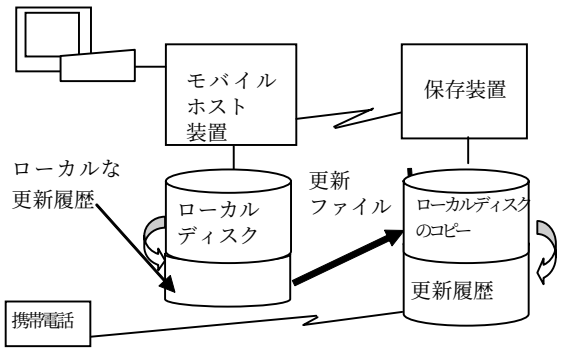

図 4.　モバイル端末の場合のデータ保護システム構成図

PC にコピーして利用する。外出先で作成・収集したデータはモバイル端末に保存し、帰着後、ホームのホスト PC に保存する。この場合、モバイル端末の情報が失われても外出時に作成･収集したデータのみであるから被害はやや軽い場合が多いが、外出時の作成・収集データの重要性によっては紛失があってはならないこともある。

第 3 の形態は、定位置 PC とモバイル PC を持ち、定位置に居る場合は、定位置用の PC を用いるがモバイル PC も接続し、モバイル PC のディスクをホストからアクセスし、主たるユーザファイルとして用いる方法である。定位置 PC とモバイル PC との間でデータ交換を行う必要がない。一般にモバイル PC のディスクは定位置 PC よりディスク容量は小さいが、映像、画像、音声などのマルチメディア・データを除けば、一般には十分な容量を確保できるので、このような利用法も可能である。

5. 3　モバイル端末のデータ保護処理

モバイル端末が保存装置と通信の接続ができない場合は、データの保護はあきらめる。これは厳しいようであるが、より障害の可能性が高いハードウェア障害も考慮すれば単一系のシステム構成では保護が無理なことは自明であること、外出中にたまたま時限爆弾的なウイルスの活動期に入るということを除いて、ウイルスによるファイル破壊の可能性は小さいこと、保護できないのは外出中に作成・収集したデータに限られるので影響は小さいと考えられる。

保存装置との通信が、切断状態時の更新ファイルの履歴は待ち行列として保存しておき、接続できた状態で保存装置に伝送する。

5. 4　ユーザ装置

ユーザ装置に定位置 PC の場合と同様の装置を持ち歩くことは、ユーザ装置を小型化してもユーザには負担となり、普及には障害となる。そのため、ユーザ装置として携帯電話のメール機能を代替として用いる。携帯電話はモバイル端末を持つような人間であれば大部分が所持していると言って良く、ユーザにとって所持は負担と感じない。保存装置からの警報や確認はメールで直接ユーザに連絡する。ユーザから保存装置への問い合わせや連絡もメールを用いる。ただし、保存装置から見て、ホスト装置(モバイル PC)が稼動していなくても異常とは限らないので、ホスト装置から更新ファイルを送られてこなくても警報のメールを送ることはできない。そのため、ユーザから接続開始のメールを送る必要がある。保存装置がホスト装置との接続断を検出すれば、その情報をユーザの携帯端末に送る。ユーザは正常な接続断と判断すれば、無視すれば良い。異常と判断すれば、定位置 PC の場合と同様の処置を行う。この携帯電話を用いる方法は、次の問題がある。第一に、ユーザが接続開始のメールを送るというアクションが必要なことが負担となる。データ保護機能は、普段はまったくこの機能を意識せず、異常時のみ意識するという空気のような存在であることが望ましい。第二に、保存装置と携帯電話との通信がセキュアでないため、なんらかの攻撃を受ける可能性が残る。第三に携帯電話のメール網を用いるため応答が遅い可能性がある。従って定位置 PC システムの場合は、携帯電話をユーザ装置とする方式は採用せず、専用の STB としたものである。しかし、モバ

イル PC の場合、利便性、安全性で多少下がるものの、実用性は十分あるものとして携帯電話をユーザ装置として用いることを提案するものである。

6. まとめ

現在、研究開発を行っているデータ保護機能を有する電子保存システムをモバイル PC に適用する場合について検討した。今後、本機能を実現するために必要なハッシュ計算や暗号化処理などの負荷を計測し、実用性証明の強化を行う予定である。また、ファイル更新コンファーム機能の付加による個別ファイル破壊検出機能の向上、クリーンなプロセッサにおけるファイル出力コンファーム機能によるワームの撒き散らしや個人情報流出防止機能の付加などについても研究の予定である。

謝辞

本研究は通信・放送機構の委託研究テーマ「情報セキュリティ高度化のためのデータ保護技術に関する研究開発」により、行っている。

参考文献

[1]http://www.symantec.com.mx/region/jp/products/goback/

[2]http://www.tripwire.co.jp/products/servers/index.html

[3]耐ウイルス機能を持った情報通信システム構築に関する研究開発, 山口雅浩他、通信・放送機構　平成 12 年度成果報告書(2001 年６月)

[4]　データ保護機能を有する電子保存システムの開発(1) 基本アーキテクチャー”, 青野正宏他 FIT(情報科学技術フォーラム)2002 第 4 分冊 pp.347-348 (2002 年 9 月)