特集

ノートパソコンの遠隔操作による情報漏えい対策ソリューション：CLEARSURE

Anti-theft Solution for Mobile Personal Computers: CLEARSURE

あらまし

ノートパソコンのモバイル利用が増加している中で，セキュリティに対しても考慮が必要になってきている。以前からノートパソコンの盗難・紛失による顧客情報の漏えい事故が増加していたが，個人情報保護法の制定・施行以降も後を絶たない。そのため，盗難・紛失したノートパソコンから情報が漏えいすることを危惧し，モバイル利用による生産性向上を認識しつつもモバイル利用に踏み切れない，もしくはモバイル利用に厳しい運用ルールを設けている企業が増えている。富士通はこのような不安に対して，利用者の遠隔操作により瞬時にHDD（Hard Disk Drive）内の全データを無効化するソリューションCLEARSUREを開発した。これにより持運び時の安全性が高められ，ノートパソコンの機動性を活用したモバイル利用の促進が期待できる。

本稿では，CLEARSUREの概要およびセキュリティサービスを支える技術について紹介する。

Abstract

There are now needs to consider security in accordance with the increasing mobile use of notebook personal computers. Incidents of customer information leakage owing to stolen or lost notebook personal computers have been increasing, and many such incidents have occurred even after the establishment and enforcement of the Personal Information Protection Law. For this reason, more and more companies will not employ, or have established strict operational rules on, mobile use of computers for fear of information leakage if they are stolen or lost, despite knowing the possible improvements in productivity that mobile use could bring. To address these anxieties, Fujitsu has developed CLEARSURE, a solution that immediately deletes all data on the hard disk via the user's remote operation. This enhances security when carrying computers, and may accelerate mobile use that takes advantage of the mobility of notebook personal computers. This paper outlines CLEARSURE and presents technologies that support security services.

坂巻健士
（さかまき　けんじ）

ソリューション開発統括部 所属
現在，個人認証や盗難対策などのPC用セキュリティソリューションの開発に従事。

永利秀之
（ながとし　ひでゆき）

ソリューション開発統括部 所属
現在，盗難対策などのPC用セキュリティソリューションの開発に従事。

向地賢記
（むこうち　まさき）

ソリューション開発統括部 所属
現在，盗難対策などのPC用セキュリティソリューションの開発に従事。

二村和明
（にむら　かずあき）

ヒューマンセントリックコンピューティング研究所パーソナルシステム研究部 所属
現在，セキュリティシステムに関する研究開発に従事。

ま　え　が　き

昨今，ノートパソコン（以下，PC）を日常的に使うのは特別なことではなくなっている。以前は社内で使うことが多かったノートPCも，日常，常に持ち歩き，出張先，移動中，顧客先などで使用するモバイル利用が注目されて久しい。ネットワーク環境などのインフラが整備されてきたことや，ノートPCそのものがモバイルを前提として軽量かつ駆動時間の延伸を図られたものが提供されてきていることもそれらの運用方法・形態を後押しする一因となっている。

このような状況の中で，モバイル利用時のノートPCのセキュリティに対して考慮が必要になってきている。以前からもノートPCの盗難・紛失から顧客情報の漏えいが増加していたが，個人情報保護法の制定・施行以降も後を絶たず，情報が漏えいした際のリスクについても以前とは比較にならないほど甚大なものになってきている。

そのため，ノートPCの盗難・紛失時にPCに保存された情報が漏えいすることを危惧し，モバイル利用による生産性向上を認識しつつもモバイル利用に踏み切れない，もしくはモバイル利用に厳しい運用ルールを設けている企業が増えている。

富士通は，このような不安を解消するソリューションとして，PHS（Personal Handyphone System）回線を利用し，遠隔操作で暗号化機能付HDD（Hard Disk Drive）/暗号化機能付SSD（Solid State Drive）（以下では，このうち，暗号化機能付HDDの場合を紹介する）の内容を消去することが可能なCLEARSURE[1]を開発した。これにより，持運び時の安全性が高められ，ノートPCの機動性を活用したモバイル利用促進に貢献できるようになった。

本稿では，CLEARSUREの概要およびセキュリティサービスを支える技術について紹介する。

概　　要

CLEARSUREは，CLEARSURE対応PCのロックおよびHDD消去サービスを提供する。

CLEARSUREのシステム全体構成と動作概念を図-1に示す。

● 管理サーバ

管理サーバは，データ消去を行うCLEARSURE対応PCを特定するためのPC固有情報を持つ。管理サーバは利用者からの指示により，PCロック/データ消去を行いたいCLEARSURE対応PCに対しPCロック/消去コマンドを発行する。さらに，PCロック/データ消去を実行したCLEARSURE対応PCからの結果レポートを受信し，利用者に通知する。

● CLEARSURE対応PC

CLEARSURE対応PCは，専用PHS通信モジュール，暗号化機能付HDD，専用BIOS（Basic I/O System）を搭載している。データの消去機能はOS（Operating System）に依存せず，暗号化機能付HDDの暗号鍵を消去することを目的とする。

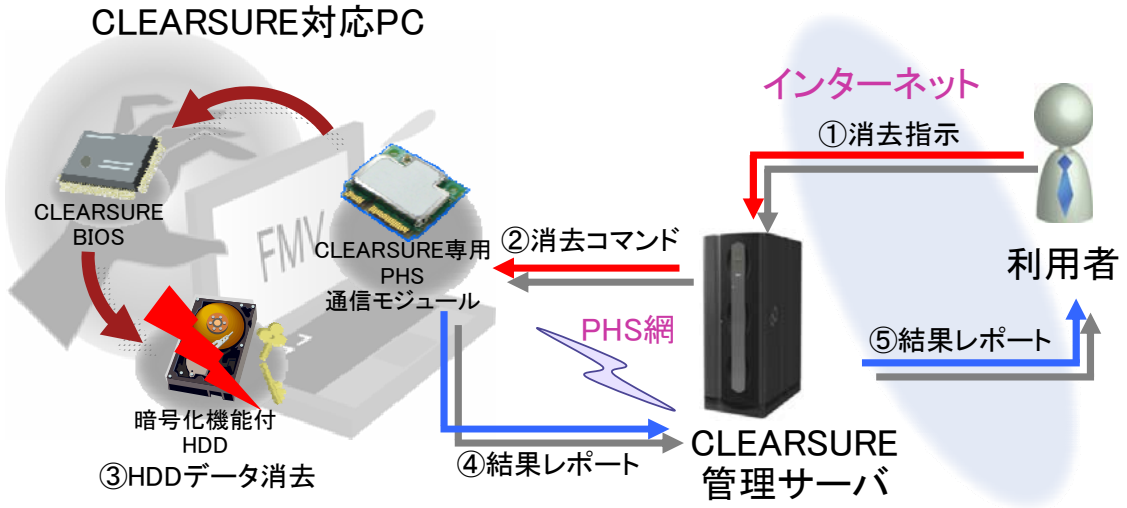


図-1　CLEARSUREのシステム構成と動作概念
Fig.1-System structure and basic action.

以下，それぞれの役割を説明する。

(1) 専用PHS通信モジュール

専用PHS通信モジュールは，CLEARSURE専用のWWAN（Wireless Wide Area Network）モジュールで，管理サーバからのコマンド受信と結果レポート送信を行うことに特化した機能を持つ。

CLEARSURE対応PCが電源オフやサスペンド状態であっても，専用PHS通信モジュールは通信ができるように構成されており，消去コマンド受信と結果レポートの送信処理が行える。

なお，CLEARSURE対応PCでは専用PHS通信モジュールはOS上からのアクセスはできないように構成し，セキュリティを高めている。

(2) 暗号化機能付HDD

暗号化機能付HDDにはAES（Advanced Encryption Standard）128ビット以上で暗号化されたデータが保存されている。暗号鍵を消去することで暗号化データを無効化している。

(3) BIOS

CLEARSURE対応PCのBIOSは，専用PHS通信モジュールの制御と，内蔵されている暗号化機能付HDDの鍵消去を行うプログラムを実装している。

つぎに，図-1を使ってCLEARSUREによるデータ消去の基本動作フローを説明する。

利用者からの指示により（①），管理サーバはPHS網経由でデータ消去コマンドを発行する（②）。管理サーバから送信された消去コマンドをCLEARSURE対応PCが受け取り，暗号化機能付HDDの暗号鍵消去によるHDDデータ消去を実行すると（③），PHS網を利用して結果レポートを管理サーバに送信する（④）。利用者は，結果レポートを受け取った後，管理サーバにアクセスし結果レポートの詳細を確認することができる（⑤）。

データ消去の仕組み

データ消去は，盗難・紛失時を想定していることを踏まえた上で，最適な手法を選択する必要がある。CLEARSUREでは，PCがサスペンド状態や電源オフの状態であってもリモートでデータ消去を実行できるように実装されている。以下では，CLEARSUREにおける消去手法の選択背景を示す。

● 確実なデータ消去

確実なデータ消去を行うために，PCの置かれた状態に依存せず，重要なデータを消去することが必要となる。このため，以下の条件を満たす必要がある。

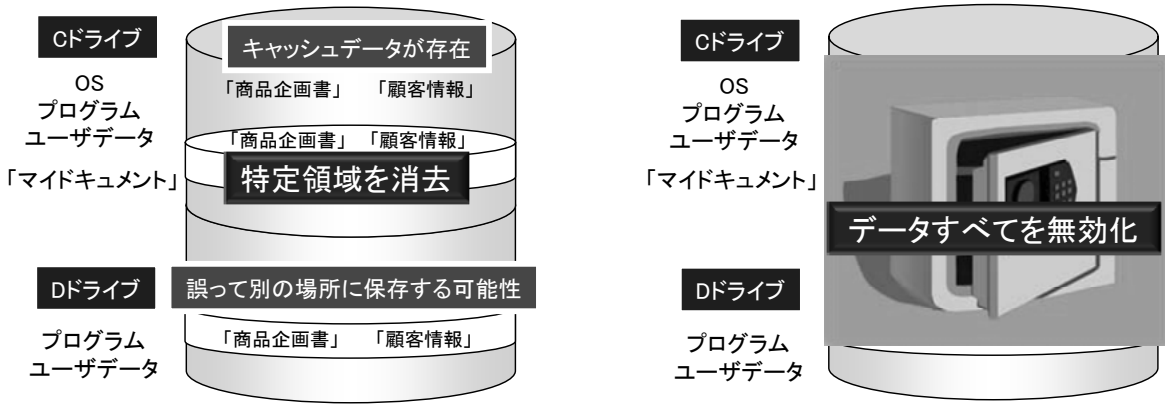
(1) バッテリ運用に耐える消去であること

ノートPCが利用者の手元になく，バッテリ運用の可能性が高く，実行時のバッテリ残量が不明であるため，少量のバッテリ残量であっても消去を機能させる必要がある。

(2) 消去実行に気付かれないこと

従来，HDDを上書き消去する方式があったが，全消去は数時間にわたることが多いため，盗難時を想定した場合，悪意のあるものが消去実行途中で気がついて消去を停止する可能性が考えられる。このため，消去実施時間は可能な限り短くする必要がある。

上記（1），（2）の条件は，HDDのデータ消去時間を短くすることによって満たされる。これには以



（a）特定領域（重要データ領域）のみの消去　　（b）全領域を消去（無効化）

図-2　データ消去の手法
Fig.2-Method of data erasing.

下に示す二つの方式がある。

【特定領域（重要なデータを格納）のみを対象とした消去】

顧客情報など重要なデータのみに絞り，消去対象のデータ量を減らすことで消去時間を短縮する｛**図-2**（a)｝。これを実施するためには，重要なデータを特定領域にまとめておくなどのルールを，利用者が正しく運用することが必要である。紛失時に，利用者が自身の運用に不安があれば，たとえ特定領域の消去を実行できたとしても，情報漏えいがなかったことを主張することは難しくなる。また，第三者により情報漏えいがなかったことを検証することも困難である。

【暗号化機能付HDDの暗号鍵の消去】

暗号化機能付HDDでは，データの暗号的な消去が行われる。この消去に要する時間は1秒以下で，OSを含めたPCの扱うデータすべてを無効化することができる｛図-2（b)｝。**図-3**は暗号化機能付きHDDの動作概要を示している。暗号化機能付HDDは，その内部に暗号化・復号機能を備え，PCから書き込まれるデータをHDD内部に置かれた暗号鍵を使って暗号化しディスク上に保存する。またディスク上に置かれたデータを，暗号鍵を使って復号し，PCに渡す。その読書きは以下のように表される。

書込み：$Y=\mathrm{E}_k(X)$

読出し：$X=\mathrm{D}_k(Y)$

ここで，E_kは鍵kによって暗号化すること，D_kは鍵kによって復号する処理を表すものとする。

データ消去は，データの暗号化，復号に使用する暗号鍵kを瞬時に無相関なランダムな値に置き換える。すなわち一度置き換えられると，元のデータを復元させることはできない。

利用者の運用に依存せず確実かつ高速にデータ消去を実現することを目的とするCLERESUREでは，暗号化機能付HDDを採用し暗号鍵の消去によってデータ全体を無効化している。

● 鍵消去の安全性

暗号鍵はHDD内で生成され，暗号鍵はHDD内に閉じて更に暗号化して置かれ，外に取り出すことができない。よって，メモリなどノートPC内に鍵データが残る心配はない。また，外から暗号鍵を設定するアプリケーションインタフェースなどを持たない。したがって，鍵消去後はその鍵を復活させる手段がない。

暗号鍵長は128/256ビットである。128ビットの暗号鍵は，$2^{128}\fallingdotseq 3.4\times10^{38}$（通り）の組合せとなる。100 GHz/CPU×67億個の並列のコンピュータを用いて（67億人が持つ100 GHzのPCの並列を想定）総当たり攻撃をした場合を想定すると6.7×10^{20}（通り/秒）の処理能力を持つが，このコンピュータを持ってしても総当たりを行うには5×10^{17}（秒）≒150億年を要することになる（ちなみに宇宙の誕生が約130億年前と言われている)。256ビット鍵では，さらに時間を要することなり，現実的な実行は不可能と考えられる。

結果レポート

CLEARSUREでは，暗号化機能付HDDのデータ消去を実施した場合に，**図-4**のような消去実行結果レポートを利用者に提供する。

ここには（1)，(2）二つの情報が記載されており，CLEARSURE対応PC内のデータが正しく消去された事実と，盗難・紛失時間がCLEARSURE対応PCの最終起動日時より後であれば，情報漏えいがなかったことを保証できる。(1)，(2）が示す詳細は以下のとおりである。

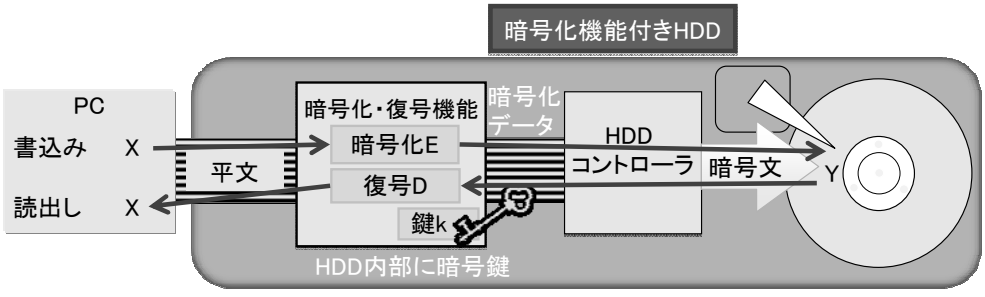


図-3　暗号化機能付きHDDの動作概要
Fig.3-HDD with encryption function.

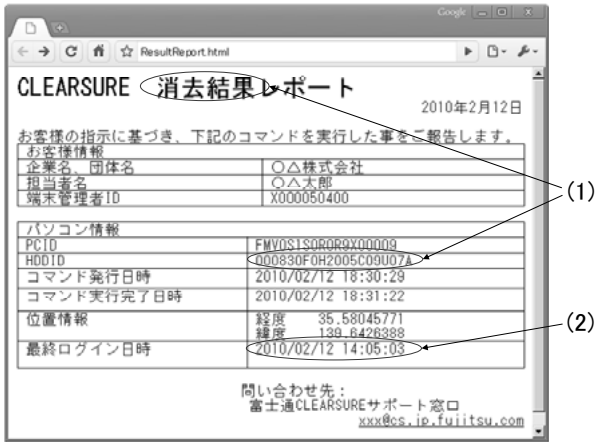


図-4　結果レポート
Fig.4-Result report.

(1)　使っていた暗号化機能付HDDのデータが消去されたこと

消去実行結果レポートに記載されたHDDIDは，消去実行した暗号化機能付HDDを特定するIDであり，事前に管理サーバに登録したHDDIDと比較することで，使っていた暗号化機能付HDDのデータを消去したかどうかを判断できる。すなわち，このIDが一致した場合には，CLEARSURE対応PCの中にOSを含め何も情報が残っていないことが分かる。

また，消去実行結果レポートに記載している実行結果とHDDIDの信頼性は，以下により保証する。

・HDDIDは，出荷時にディスクベンダによりユニークなIDが書き込まれており，かつ外部から変更することができない。
・暗号化機能付HDDの暗号鍵が消去されたことは，BIOSによって消去コマンドの応答を確認し，実行結果を消去実行結果レポートに記載する。BIOS改ざんに関しては，不正BIOSへの書換えができない仕組みを搭載している。

以上により，使っていた暗号化機能付HDDのデータが消去されたことを保証できる。

(2)　盗難・紛失後～消去完の間にPCの不正利用がないこと

消去実行結果レポートに記載される最終起動日時は，最後にBIOS認証が成功した日時である。最終起動日時と，盗難・紛失日時を比較することで，盗難・紛失発生時から消去までの間にPC（BIOS&OS）に不正ログインされなかったかどうかを判断できる。

また，消去実行結果レポートに記載している最終起動日時の信頼性は，以下により保証する。

・BIOS認証が成功した場合のみ，BIOS時刻を読み出し，「最終起動日時」として更新する。また，最終起動日時はBIOSの不揮発領域に保存し，改ざんを防止している。
・BIOS時刻は，BIOS管理者権限を持ったものだけが修正することができる。またその時刻は，ボタン電池による電源供給によって動作し，そのカウントは止まることがない。

よって，CLEARSUREの消去実行結果レポートを受け取ることができれば，情報漏えいがなかったことを確認できることになる。

位置情報を利用した運用例

ここではPC置き忘れ発生時の，CLEARSUREを使った運用例を示す。

利用者がCLEARSURE対応PCを電車や飲食店などに置き忘れ，ある時点でPCの置き忘れに気がついた場合，

・管理サーバから，まずPCロックコマンド発行する。
・結果メールを受信する。
・利用者は管理サーバの結果レポートでロックが正しく実行されCLEARSURE対応PCが利用できない状態になったことと，ロック実行時の位置情報（PHSの基地局位置情報）を確認する。
・このとき位置情報が，利用者が想定し得る場所を示すものであった場合（例：乗っていた電車の終点駅付近や食事をした飲食店付近を示している場合），利用者はPCを取り戻すために行動を起こす。
・もし位置情報が利用者の行動の範囲外であった場合（例：利用者の通常の行動範囲が関東だがそれ以外の場所を示している場合），第三者にCLEARSURE対応PCが渡ったと考え，管理サーバからデータ消去コマンドを発行する。CLEARSUREではロック/消去実行時の位置情報を提供する。**図-5**はGoogle Earthに図-4の位置情報を与えた結果を示す。中央のピンが位置を示す。
・利用者は，管理サーバの結果レポートでデータ消去コマンドが正しく実行されたこと，HDDIDが使用時のものと一致すること，および最終ログイ

図-5　位置情報による確認方法例
Fig.5-Cofirmation method using location information.

ン日時が紛失日時よりも前であることを確認することで，情報漏えいがなかったことを知ることができる。

CLEARSUREの導入

一般の通信モジュール内蔵PCでは通信回線の契約は利用者と回線事業者の間で行われるが，複数台を導入する企業にとっては非常に手間のかかる作業となっていた。

通信回線を使用するCLEARSUREではこの問題を解決するために富士通が回線事業者と一括で契約する形を取っている。CLEARSURE対応PCの本体価格に1年間（オプション選択により延長可）の利用料も含まれているため，利用者はCLEARSURE対応PCを購入するのみで個別の通信契約を行う必要はない。

専用PHS通信モジュールはPC出荷の段階で電話番号が登録されているため，BIOSでCLEARSUREの機能を有効にするだけで通信が可能となっている。

これにより，利用者は管理サーバのアカウント取得後，購入したCLEARSURE対応PCを管理サーバに登録するだけですぐにサービスの利用を開始できる。

通信圏外の対策など

CLEARSUREはPHSの公衆回線網を使用しており，通信エリアは人口カバー率で99.4%となっている。しかし，公衆回線網を利用している関係上，どのような通信方式であっても通信圏外となる場所は発生してしまう。

このように通信ができない場合は，遠隔操作によるコマンドを送信することができないため，それに備えて「ローカルロック・消去」機能をBIOSで実装している。

これはBIOSパスワードを指定回数入力ミスした場合にCLEARSURE対応PCのロックや暗号化機能付HDDのデータ消去を行うものである。これにより通信圏外で盗難にあった場合でも盗難者によるBIOSパスワード入力ミスでCLEARSURE対応PCのロックや暗号化機能付HDDのデータ消去を行うことができる。ローカルロックを解除できるのは管理サーバからのコマンドのみであるため盗難者はロックを解除する手段を持たない。

また，この場合でも専用PHS通信モジュールは結果レポートの送信待ちとなるため，通信ができるようになれば直ちに実行結果を管理サーバへ通知する。

さらに，通信圏外ではCLEARSURE対応PCの起動ができないように設定することも可能である。

む　す　び

本稿では，PHS回線を使った暗号化機能付HDDの暗号鍵消去法による情報漏えい対策を紹介した。そしてCLEARSUREの消去実行結果レポートを受け取ることができれば，情報漏えいがなかったことを確認できることを示した。CLEARSUREは，ノートPCを持出し禁止から再びモバイル利用のツールとして復活させ，企業の生産性向上と業務の効率化を推進するソリューションとして企業への採用拡大を期待している。

参 考 文 献

(1)　富士通：CLEARSURE（クリアシュア）のご紹介.
http://www.fmworld.net/biz/fmv/lifebook/clearsure/