情報処理学会論文誌 Vol.58 No.3 683–694 (Mar. 2017)

リスクベースセキュリティによる記憶媒体の自己保全

二村 和明[1,2] 矢崎 孝一[1] 中村 洋介[1] 西垣 正勝[2]

受付日 2016年6月26日, 採録日 2016年12月1日

概要：近年，情報機器のデータをクラウド側に置き利用することが多くなってきているが，ネットワークが不安定な状態でもシームレスに動作させるため，デバイス側にもデータのコピーを残すHTML5のような技術が利用されており，依然重要なデータをローカルに残した状態で運用がなされている．この状態で，PCなどの情報機器がネットワークから切り離され，さらにハードディスクなどの記憶媒体が情報機器から切り離された状態になると，その中に置かれたデータの情報漏えいリスクが高まることになる．そこで，ふだんとは異なる状況であると判断される場合に追加のセキュリティアクションを起こすリスクベースセキュリティのコンセプトを導入し，通常利用の中で記憶媒体自身が接続される情報機器の状態を自律的に検証，そしてリスクを検知した場合に追加のセキュリティアクションとして，自身のデータを自動で廃棄可能なレベルに消去する自己保全機能を実現することで，情報漏えいのリスクを軽減できるようにした．

キーワード：リスクベースセキュリティ，ユーザ認証，パスワード，ハードディスク，SSD，消去，PC

Self-wipe Capability for Hard Drive Derived from Risk Based Security

Kazuaki Nimura[1,2] Kouichi Yasaki[1] Yousuke Nakamura[1] Masakatsu Nishigaki[2]

Received: June 26, 2016, Accepted: December 1, 2016

Abstract: Recently, data in information devices increasingly stored in the Cloud service, however to overcome the network instability, copy of the data is remained in local medium using HTML5 technology for seamless use of the information device. In such situation, if an information device such as a PC is separated from network or a medium such as a hard drive is pulled from an information device for some reason, then the data in the medium would face the risk of data leakage. In this paper, to solve the issue of the information leakage by pulling the medium off from the information devices, we introduce a concept of risk based security that would take additional security action when recognized it is not normal behavior. Then we propose a concrete solution that realizes the hard drive be disposable when detecting a risk by issuing wipe command from the hard drive itself to protect the data as the additional security action, then minimal the risk of information leakage.

Keywords: risk based security, user authentication, password, hard drive, solid state drive, wipe, PC

1. はじめに

近年のクラウドサービスの発展により，情報機器のデータをクラウド側に置き利用することが多くなっている．しかし，ネットワーク速度や接続性など可用性の観点から，現状のネットワーク環境では，ローカルにデータを保持しておくことで利便性が高まる場合が多々あり，情報機器側にもデータのコピーを残しておくことで，ネットワークが不安定な状態でもシームレスな動作を実現することができるHTML5のような技術が策定・利用されている．たとえば，ウェブページであれば，トップページをダウンロードした際に，子ページも含めダウンロードおよびキャッシュがなされ，オフラインであってもウェブページの閲覧が可能になっている．このため，依然ローカル環境に置かれたデータをいかにセキュアに保つかが重要な課題として残っている．

PCなどの情報機器やそのデータの管理において，デバイスマネージメント機能を使ってネットワーク越しで監視す

[1] 株式会社富士通研究所
Fujitsu Laboratories Ltd., Kawasaki, Kanagawa 211–8588, Japan
[2] 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University, Hamamatsu, Shizuoka 432–8011, Japan

ることも可能になってきているが，ネットワークから切り離された状態や，ハードディスク（Hard Disk Drive，Solid State Drive の両方を指す）などの記憶媒体が何らかの理由で情報機器から抜き取られた状態になると，その中に置かれたデータの情報漏えいリスクが高まることになる．

そこで本論文では，PC など情報機器がネットワークから切り離され，さらに記憶媒体が情報機器から切り離されたことによる情報漏えいを防止するため，ふだんとは異なる状況であると判断した場合に追加のセキュリティアクションを起こすリスクベースセキュリティのコンセプト[*1]を導入する．通常利用において記憶媒体が接続される情報機器の状態を，記憶媒体自体が外部機能に頼ることなく自律的に検証し，リスクを検知した場合に追加のセキュリティアクションとして，自身のデータを自動で廃棄可能なレベルに消去する機能を記憶媒体本体に組み込む．この自己保全型の手法は，通常利用時に利用者が本機能の存在を意識することがなく，操作性を損ねることもないという特徴を備える．また，万一誤動作が生じて本機能による保全処理が行われたとしても，前述のクラウド側のデータを書き戻すことで容易にイメージを復元できることから，提案方式のように安全サイドに倒した運用をとることは理に適っている．提案手法がプラクティカルな手法であることを示すために，実現コストを意識して業界標準のハードディスクを対象とし，ソフトウェアのみで提案方式の機構を実装するとともに，実動作検証した結果を提示する．なお，本論文は文献 [15] を基に，提案方式の理論体系，手法，実装，評価を深化させたものである．

2. 課題と提案手法

ここでは，本論文が対象とする課題をまとめ，解決に向けた要件および提案手法について述べる．

2.1 課題

本論文では，PC などの情報機器がネットワークから切り離された状態であっても，さらに情報機器からハードディスクなどの記憶媒体が切り離された状態であっても，その中に置かれたデータが解析されるなど情報漏えいの危険性が残ったままになることを課題とする．

2.2 要件

この課題に対し，課題解決に向けた要件は以下のようになると考える．

(A) 保全実行の確実性を満たすこと

記憶媒体が危険な状態になった場合に，記憶媒体を廃棄可能なレベルにする保全実行を行うことで，解析に対する安全を確保できること．これを確実に実行するためには，以下 3 つの要件を満たすことが必要になると考えられる．

(A-1) 危険を検知できること

記憶媒体の置かれた危険度を測定・判断し，通知できること．

(A-2) 劣悪環境下で保全実行できること

危険だと判断される場合に，現実的な手段を用いて情報漏えいが発生することがないよう保全実行し，記憶媒体を廃棄可能なレベルにできること．これには，たとえば，物理的な破壊によりデータを読み取れない状態にすることが考えられるが，PC などの情報機器の盗難・紛失時にこれを期待するのは困難である．また，消去など情報漏えい対策のための保全処理は，一般的に時間がかかりバッテリ残量も必要になることから，十分短い時間で，十分少ない電池残量で確実に実行することが必要になる．

(A-3) 第三者の手にある状態で保全実行できること

第三者の手にわたり，ネットワーク環境から切り離された状態であっても，さらに，PC などの情報機器本体から記憶媒体が抜き取られた状態であっても保全実行ができること．その際，ブートディスクとして接続されて利用されていた記憶媒体を，不正者が抜き取り，ブートディスクあるいはセカンドディスクとして接続して解析する場合にも保全実行が機能すること．

このためには情報機器がネットワーク環境から切り離された状態になることを想定して，ネットワークをまたいだ外部の危険検知機構による通知信号に頼ることなく，自律的に危険検知・通知を機能させるとともに，記憶媒体が情報機器から切り離された状態になることを想定して，危険検知と保全実行の両方の機構を記憶媒体本体に組み込むことで保全実行を確実にする必要がある．

また，記憶媒体の接続形態として，ブートディスクとして接続された場合と，セカンドディスクとして接続された場合を想定し，両者で危険検知と保全実行を動作させる必要がある．ここで，ブートディスクは，記憶媒体を PC などの情報機器に内蔵し，OS（Operating System）を起動する接続形態を指している．また，セカンドディスクは，記憶媒体を外部デバイスとして，起動中の情報機器に接続する接続形態を指している．これには，情報機器に外付けで記憶媒体などを接続するための e-SATA（external Serial ATA）による接続や，USB インタフェースアダプタを介した接続がある．

(B) 保全実行の可用性を満たすこと

以下のような利用状況において，要件 (A) を満たす機構が動作すること．

(B-1) OS の種類を問わず動作すること

情報機器の OS の種類に依存せず，要件 (A) を満たす機構が動作すること．これは，機構に OS 依存性があると，

[*1] リスクベースセキュリティの定義に関しては，著者の知る限り明確に定義しているところはないが，リスクベース認証 [1], [14] の上位概念として，リスクに基づいてセキュリティ施策を追加するもの全般をここではリスクベースセキュリティと位置づける．

OS 間の差異を埋めるための手法の実現が別途必要になり，保全機構をそのまま機能させることが困難になるためである．

(B-2) PC の種類を問わず動作すること

PC の種類に依存せず，要件 (A) を満たす機構が動作すること．これは，機構に PC 依存があると，PC の差異を埋めるための手法の実現が別途必要になり，保全実行をそのまま機能させることが困難になるためである．

(B-3) ユーザに保全機能を無効化させないこと

たとえばパスワードを定期的に変えさせるなど人間の特性を超えた作業を求めると，それをメモに残し貼っておくなど，より危険度の高い状態を誘発することが起こりうる．すなわち，QoE（Quality of Experience）が損なわれると，ユーザはその機能を使おうという気が起きなくなり，セキュリティ機能を利用していた場合でもそれを外したくなる．人間の特性を考えたセキュリティの運用をしない限りその効果が期待できないため，QoE の考慮が重要になる．そこで，要件 (A) に対する解決策を導入しても，普段利用の中で使用感に影響を与えることがなく，ユーザが保全機能の使用を中止する気にならないようにする必要がある．

2.3 提案手法

ネットワークや情報機器から切り離された状態での保全実行（前述の (A-3)）を実現するため，リスクベースセキュリティのコンセプトを導入した記憶媒体のための新しい保全手法を検討する．

リスクベース認証 [1], [14] では，Web サービスなどを利用する際の認証において，ふだんと異なる環境からのアクセスであると判断した場合に，通常のユーザ ID・パスワードの入力に加え，追加のセキュリティアクションとして，さらなる認証をユーザに促すことで，ユーザと情報機器の関係を確認・許容する．我々は，このコンセプトを拡張し，記憶媒体向けに「記憶媒体自身がリスクを監視し，いつもと異なる環境に置かれたことによる記憶媒体のリスクを検知した場合に，追加のセキュリティアクションとして，自身のデータを自動で廃棄可能なレベルにすることで情報漏えいを防止する」手法の導入を提案する．

Gartner は 2014 年のレポート “Top 10 Technology Trends of 2015” の中で，トレンドの 1 つとして，“Risk-Based Security and Self-Protection” をあげ [2]，アプリの悪意のある振舞いを監視し，保護のために自動的に自身の設定を変える “runtime application self-protection” が必要だとしている．上記のリスクベースセキュリティに基づく提案は，この方向性とも一致するものである．

以下では，それぞれの要件に対する機構を示す．

(A-1) 危険検知

記憶媒体の置かれた危険度の測定・判断を実現するために，安全な接続環境を表すプロファイルを記憶媒体自体にホワイトリストとして記録できるようにして，その後の利用時に，接続された環境に対するプロファイルを取得してホワイトリストと比較する（チェック機構）．そして，両者が異なる場合に危険度が高いと判断する．

(A-2) 劣悪環境下で保全実行

保全機能の実現には，以下 2 つのタイプが考えられる．

アクティブ型：PC など情報機器からの記憶媒体の抜き取りがあった場合に，即座に記憶媒体がそれを情報漏洩リスクとして検知してデータの消去を行うタイプ．このために，記憶媒体内に抜き取り検知回路，消去機能，バッテリなどの追加ハードウェアを備え，タイムリーにリスクをとらえることを可能とする．

パッシブ型：記憶媒体が情報機器に接続され，情報機器が利用されるタイミングで情報漏洩リスクを計測・検知して，データの消去を行うタイプ．このための機能の実装はソフトウェアのみで実現し，バッテリなどの追加ハードウェアを備えることはなく，記憶媒体に外部供給される電力によって駆動させる．

しかし，これらによっても，少ない電池残量において，短時間で廃棄可能なレベルを実現するには不十分であり，記憶媒体を暗号化し，その鍵の更新だけで消去機能を実現できることが好ましいと考えられる．

アクティブ型には瞬時実行が可能なメリットがあるが，電源供給部など追加ハードウェアによるコスト増を招くことが想定されるため，本論文では，より実用に向けた障壁が低いと考えられるパッシブ型をベースに，鍵更新による消去を組み合わせた手法の実現について検討を行う．

(A-3) 第三者の手にある状態で保全実行

記憶媒体がネットワークおよび情報機器から切り離されることに対処するため，危険検知と保全実行を記憶媒体のみで行えるようにする (A-3-a)．

また，記憶媒体の接続形態を問わず機能させるため，記憶媒体にはブートディスクとして利用する場合と，セカンドディスクとして利用する場合のそれぞれに対応する機構を作り，危険検知と保全実行を機能させる (A-3-b)．

(B-1) OS の種類を問わない

ブートディスクとして利用する場合は，情報機器起動時の OS 呼び出しに対してフックを設定し，OS 起動の直前に機構を実行することで，OS 依存性を発生させないようにする．セカンドディスクとして利用する場合は，抜き取った記憶媒体を不正者がいかなる種類の情報機器に接続したとしても，機構をバイパスすることができないようにすることによって，不正者が使用する情報機器に対する OS 依存性を実現する．また，(A-3-a) で述べたように記憶媒体内の機構ですべてを実現することで，OS の改造は不要である．

(B-2) PC の種類を問わない

PC のハードウェアの違いが吸収される BIOS（Basic

Input Output System）起動後において，すべての PC が備える情報のみを検証に利用することで，PC 依存性を発生させないようにする．また，(A-3-a) で述べたように記憶媒体内の機構ですべてを実現することで，PC の改造は不要である．

(B-3) 保全機能を無効化させない

保全機能をユーザに無効化させないようにするため，ユーザの使用感に影響を与えないようにする．このため，ふだんの PC 利用のフローの中で，記憶媒体自身が PC に対して後付けでチェック機能を働かせ，必要な場合のみセキュリティアクションを実行することで，PC 利用方法への変更をいっさい求めず，ユーザにその動作を意識させることがないようにする．通常利用では記憶媒体の接続環境に変化がないため，(A-1) で設定したプロファイルと一致し，記憶媒体はふだんどおりに機能することになり，ユーザにも何ら動作は見えない．しかし，記憶媒体が異なる環境で利用される場合には，プロファイルとの不一致をチェック機構が検知し，データ消去を起こす．この時点になってユーザは，本機能の存在に気づくことになる．

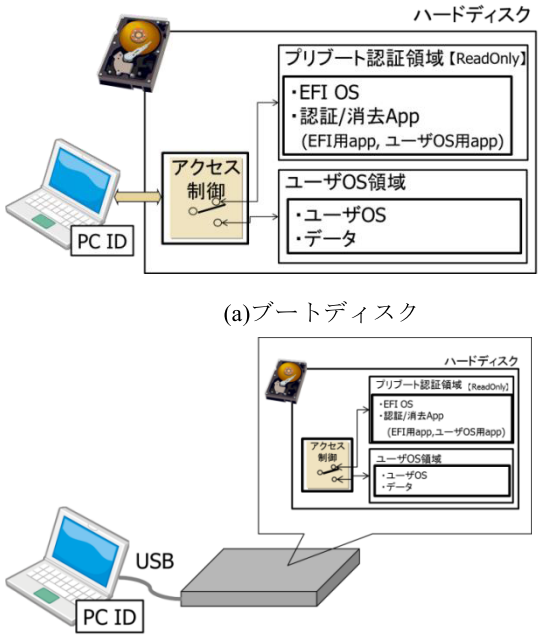

図 1 提案手法の TCG ハードディスクへの実装
Fig. 1 Implementation to TCG hard drive.

3. 実装

提案手法の実装構成として，調達や開発がしやすい標準のハードウェアを使用し，その上にソフトウェアのみで実装することで実現コストを最小に抑え，実用レベルの実装を追求する．以下では，実装対象と提案手法の実装詳細について述べる．

3.1 実装対象

ハードディスクについては，国際業界標準化団体である TCG（Trusted Computing Group）によって策定されたハードディスク仕様を利用する．また提案機能を実装するためのベース OS として，BIOS（Basic Input Output System）の新標準規格である EFI（Extensible Firmware Interface）を利用する．以下では，これら TCG ハードディスクと EFI の特徴についてまとめる．

3.1.1 TCG ハードディスク

TCG ハードディスクとは，TCG で策定されたストレージセキュリティの仕様である TCG Storage Architecture Core Specification [3] と Opal SSC（Opal Security Subsystem Class）[4] に準拠したハードディスクを指している．これに準拠したハードディスクが各社から製品出荷されている．このハードディスクは以下のような特徴を備える．

- ディスク全体の暗号化機能（Full Disk Encryption）を標準で備えている．
- データの消去は，暗号鍵の更新により行われる．このため消去処理は瞬時に完了する．これは従来のディスク全体に書き込みを行うような，数十分から数時間かかる消去に比べて，効率的な情報漏洩対策として適用できるメリットがある．

プリブート認証のための領域（PBA: Pre Boot Authentication 領域）を備えている．プリブート認証領域は，Windows などのユーザ OS やデータを格納するユーザ OS 領域とは別に用意されたハードディスク領域である（図 1）．このプリブート認証領域に，パスワード認証，生体認証，IC カード認証といった認証プログラムを組み込むことで，プリブート認証が可能になる．

- プリブート認証領域とユーザ OS 領域を切り替えるためのアクセス制御を行う，MBR shadowing（Master Boot Record shadowing）機能を備えている．MBR shadowing 機能がイネーブルされていると，電源の投入時には，プリブート認証領域のみが見え，ユーザ OS 領域は隠蔽された状態になる．アクセス制御の設定を扱うアクセス制御レジスタには，8 名のユーザ（User1〜User8）のプロファイルを保持可能であり，ここに事前登録されているユーザのみがアクセス制御の切替えを実行できる．すなわち，ユーザが正しいプロファイルを提示することができた場合にのみ，アクセス制御の切替えが実行され，ユーザ OS 領域にアクセスできるようになる．

3.1.2 EFI

EFI は比較的新しい BIOS の標準規格である．Windows が標準でサポートしていることから EFI は広く利用可能になっている．EFI は，本提案手法の実装にあたり，以下のような好ましい特徴を備えている．

- EFI は，従来の BIOS に変わるファームウェアとしてすでに採用されており [5]，TCG ハードディスクのプリブート認証機能に対してシームレスな実装が可能である．
- Windows などのユーザ OS を CALL する前に EFI アプリを動作させる仕組みがある．
- EFI 未サポートの Legacy OS を EFI Legacy OS Loader によって呼び出す Legacy ブートをサポートしている．
- EFI では，開発環境が無償でオープンソースとして提供されている [6]．

3.2 提案手法の実装方針

前述の TCG ハードディスクおよび EFI を用いて，危険検知を行う認証機能および保全実行としてのデータ消去機能をソフトウェアで実現する「認証/消去 App」の実装について述べる．

認証/消去 App は，ブートディスク利用形態において動作する EFI 用 App と，セカンドディスク利用形態において動作するユーザ OS 用 App があり，TCG ハードディスクのプリブート認証領域の中に，EFI 環境とともに配置して使用する（図 1 (a)）．EFI は BIOS に相当するファームウェアであるが，提案手法においては，PC の BIOS を EFI に置き換えるのではなく，TCG ハードディスクのプリブート認証領域内のアプリ（プリブートアプリ）をサポートするための簡易 OS として EFI 環境を活用していることに注意されたい．本論文ではこの簡易 OS を「EFI OS」と呼ぶ．

なお，プリブート認証領域は様々なプリブートアプリが組み込まれうる共通領域であることを考慮すると，提案手法はプリブート認証領域を圧迫することがないコンパクトなアプリ実装が望まれる．また，ハードディスク内のユーザ OS 領域には，Windows などの一般的なユーザ OS がインストールされている．ユーザ OS が立ち上がった後に利用される各種データが格納されるのも，ユーザ OS 領域である．

通常のブートディスク動作では，PC の BIOS がブートローダを起動し，ブートローダがハードディスク内のユーザ OS を起動する．一方で，提案手法のブートディスク動作では，PC の BIOS がブートローダを起動し，ブートローダがプリブート認証領域内の EFI OS を起動する（PC 起動時に見えているのはプリブート認証領域のみであることに注意）．その後，プリブート認証領域に置かれ EFI 用認証/消去 App が自動的に呼び出され，ハードディスクの接続されている PC がホワイトリストに登録されている情報機器であるか否かが確認される．確認に問題がない場合に，認証/消去 App は，ハードディスクのアクセス制御を行い，プリブート認証領域にアクセス可能な状態からユーザ OS 領域にアクセス可能な状態に切り替えるとともに，再度ブートローダを起動させることでユーザ OS を起動する．このとき，プリブート認証領域の EFI OS は PC 起動時の BIOS のような役割を果たしている．

セカンドディスクとして接続される場合もハードディスク内の構成および動作は変わらない（図 1 (b)）．セカンドディスクでの動作としては，抜き取ったハードディスクを USB 接続機能を持つハードディスクケースに入れて利用することを想定しており，2 つの利用形態が考えられる．

- セカンドディスク（外付け File System）：PC の OS は USB ストレージ機能をサポートしている場合が多く，USB 経由でハードディスクを接続することで OS がサポートする File System を持った外付けストレージとして動作させ，ハードディスクの中の情報にアクセスすることができる．
- セカンドディスク（USB ブート）：PC の BIOS が USB ブートをサポートしている場合には，セカンドディスクを USB ブートで動作させることができる．このときセカンドディスクはブートディスクと同じ動作になるため，ここでは説明を割愛する（以降，本論文では，外付け File System としてのハードディスクの利用形態を「セカンドディスク」と呼ぶ）．

セカンドディスク（外付け File System）の場合においても，PC 接続時に最初に見えるのは，プリブート認証領域のみである．そこに Windows や Linux 上で動作可能なアプリとしてユーザ OS 用認証/消去 App が配備されており，ユーザ OS 用認証/消去 App が自動起動される（最近は，マルウェア対策のために，自動起動の際にユーザに実行の可否を問い合わせる OS も多い）[*2]．認証に問題がない場合のみハードディスクのアクセス制御切替えが行われる．この認証を経ない限りハードディスクの中のユーザ OS 領域にアクセスすることはできない．

すなわち，ブートディスクで使用する EFI 用認証/消去 App とセカンドディスク（外付け File System）で使用するユーザ OS 用認証/消去 App のハードディスクへのアクセス制御の仕方は同じ機構だが，EFI 用認証/消去 App は BIOS（が呼び出すブートローダ）によって起動されるのに対し，ユーザ OS 用認証/消去 App はユーザ OS（の Auto Run 機能）によって起動される点が異なる．

3.3 各要件の実装方針

以下では，提案手法において，各要件に対応する解決策の実装について説明する．

(A-1) 危険検知

要件である危険度の測定・判断は，記憶媒体が接続される PC など情報機器の状態を確認することによって行う．

[*2] ユーザ OS がセカンドディスクの Auto Run 機能をサポートしていない場合は，ユーザ自身がユーザ OS 用認証/消去 App を起動する必要がある．

具体的には，ハードディスク内の認証/消去 App は，そのハードディスクがふだん接続される PC の固有 ID を，当該ハードディスクが許可する「信頼のできる PC」のプロファイルとして設定する．本論文では，認証/消去 App でプロファイルの設定を行った登録済みの機器 ID を持つ PC を “登録 PC”，登録していない機器 ID を持つ PC を “登録外 PC” と呼ぶ．すなわち，記憶媒体に接続された情報機器が登録外 PC である場合に，危険度が高いと判断されて保全実行が機能することになる．

また，パスワード認証などのユーザ認証を利用して，危険度の測定・判断を行うことも可能である．具体的には，認証/消去 App は，ユーザの認証用情報（たとえばパスワード）を，ハードディスクが許可する「信頼のできるユーザ」のプロファイルとして設定する．本論文では，認証/消去 App でプロファイルの設定を行った登録済みのユーザを “登録ユーザ”，登録していないユーザを “登録外ユーザ” と呼ぶ．すなわち，記憶媒体に接続された情報機器が登録外ユーザに利用されている場合に，危険度が高いと判断されて保全実行が機能することになる．

これらの危険度の測定は，ブートディスクとして利用する情報機器の起動時とセカンドディスクとして利用する記憶媒体挿入時の 2 カ所で情報機器の動作へのフックを設定することで行い，必ず危険検知機構を通過するようにする．

(A-2) 劣悪環境下で保全実行

保全実行は，暗号化ハードディスクの鍵消去，すなわち計算量的安全に基づくデータの消去を採用し，瞬時に全データを無効化することで実施の確実性を最大限に高める．

(A-3) 第三者の手にある状態で保全実行

(A-3-a) 記憶媒体のみで実行：(A-1)，(A-2) の機能を一体化した認証/消去 App は記憶媒体へのソフト実装のみにより行う．

(A-3-b) セカンドディスクで機能：ブートディスクとセカンドディスクの 2 つの接続形態に合わせた 2 種類の認証/消去 App を用意し，どちらの認証/消去 App も記憶媒体内のプリブート認証領域に配置することによって対応する．すなわち，ブートデバイス向けには，EFI OS 上で実行される EFI 用認証/消去 App を用意し，記憶媒体がブートデバイスとして接続された場合に，この認証/消去 App により危険検知・保全実行を行う．セカンドディスク向けには，ユーザ OS 上で動作するユーザ OS 用認証/消去 App を開発し，記憶媒体がセカンドディスクとして接続された場合に，この認証/消去 App により危険検知・保全実行を行う．

(B-1) OS の種類を問わない

記憶媒体がブートディスクとして利用される場合には，OS の違いは，BIOS 起動後，かつユーザ OS の起動前に機構を動作させることで吸収する．従来の PC においては，PC 起動時に BIOS がブートローダ経由でユーザ OS を起動するのに対し，提案手法では，PC 起動時にはプリブート認証領域のみが開かれており，BIOS によってユーザ OS の代わりに EFI OS が呼ばれることになる．これをフックの起点として，EFI OS 上で動作する認証/消去 App を実行させる．これにより危険検知が行われ，問題がないと判断される場合に，アクセス制御を行ってユーザ OS 領域に切り替えるとともに，int13 call を行い，ユーザ OS を起動しフックを完了させることで，OS への依存性を発生させないようにする．

このアクセス制御への制御権を設定するため，TCG ハードディスクにおける User1 用のアクセス制御レジスタに対し，機器 ID のハッシュ値をプロファイルとして登録する．また，User2 用には，ユーザのパスワードのハッシュ値をプロファイルとして登録する．これらが登録 PC あるいは登録ユーザを識別するためのホワイトリストとして用いられる．登録 PC，登録ユーザが複数ある場合には，User3〜User8 への登録を行い，アクセス権を付与することができる．

記憶媒体がセカンドディスクとして接続された場合には，3.2 節で説明したように，BIOS が EFI 用認証/消去 App を起動するのではなく，ユーザ OS がユーザ OS 用認証/消去 App を起動する．このため，ユーザ OS 用認証/消去 App は OS ごとに実装する必要がある．そこで，セカンドディスク向けには，「抜き取った記憶媒体を不正者がいかなる種類の情報機器に接続したとしても，機構をバイパスすることができないようにする」という方法によって，不正者が使用する情報機器に対する OS 依存性を解消する．具体的には，記憶媒体内のプリブート認証領域にユーザ OS 用認証/消去 App を配置することで，認証にパスしない限りユーザ OS 領域にはアクセスできないようにする．

(B-2) PC の種類を問わない

PC の違いは BIOS で吸収し，BIOS 起動後に危険検知などの機構を動作させる．その際，登録 PC の判別に利用する機器 ID としては，どの PC も保持している情報であり，PC の不揮発性記憶領域に保存されている BIOS UUID（Universally Unique Identifier），またはこれに相当する情報を利用することで，PC の種類を問わずつねに機能させる．登録ユーザの判別に利用するパスワードも，PC の種類を問わず利用できる情報としての条件を満たしている．

なお，記憶媒体がセカンドディスクとして接続された場合には，ハードディスクと PC を接続する USB が PC の種類への非依存性を提供する．

(B-3) 保全機能を無効化させない

(B-1) に示した実装により，ブートディスク形態では毎回のチェックが PC 起動時に自動的に行われるようにし，危険検知などの機構をユーザにとって透過的に動作させる．また，提案手法の導入段階においても，インストーラを用意することで，ユーザ OS が利用可能な状態からワンクリックで提案手法の設定を完了させるようにする．

なお，記憶媒体がセカンドディスクとして接続された場合にも，ユーザ OS 用認証/消去 App を起動して認証をパスすることなく，ユーザ OS 領域への切替え（ユーザ OS 領域内のデータへのアクセス）を行う手段は存在しない．

4. 評価

以下では，提案手法の理論評価と動作評価を行った結果を示す．理論評価では追加のセキュリティアクションとして使用する鍵消去の強度について検証する．動作評価では，基本動作確認により要件 (A-1)，(A-2)，(A-3-a) を評価し，様々な状況での動作確認により要件 (B-1)，(B-2)，(A-3-b) を評価，ユーザビリティ評価により要件 (B-3) を評価する．

4.1 理論評価

理論評価では，暗号化機能付きハードディスクが備えている鍵消去機能の利用が記憶媒体を廃棄レベルにする手段として適切なのか検証を行う．また，ハードディスクが抜き取られた場合の保護についても検証する．

4.1.1 鍵消去の強度

TCG ハードディスクの鍵消去では，データの読み書きの際に利用される暗号鍵を，異なる鍵に再生成（鍵 1 → 鍵 2）することで鍵の無効化が行われ，以前のデータを読むことができなくなる．TCG ハードディスクではこの基本的な鍵更新に加えて，消去時に各社が独自の強化策を加えており，鍵更新の強度以上に解読は困難になる．

Secure Sanitization に関する論文 [7] によれば，暗号化ハードディスク内での暗号鍵消去は十分な強度を持ち，廃棄可能な手段に分類されている．このため暗号鍵の消去手法は，廃棄手段と見なして使用しても問題がないと考えられる．一方で，鍵消去の後に従来の書き込みによる消去を併用することを推奨しており，電源供給に問題がなく，時間が許すのであれば，鍵消去の後，従来手法を実施するのがよいのであろう．

また，NIST の文献 Guidelines for Media Sanitization [8] によれば，消去コマンドによるハードディスクの消去は最先端の攻撃によってもデータのリカバリが不可能とされる “Purge” にカテゴライズされており，メディアの廃棄において十分な強度が認められている．よって，この文献からも消去を実用的な廃棄手段として使用しても問題がないと判断される．

4.1.2 抜き取り時の保護

PC には，生体認証や IC カードなどの高機能な認証機能が標準搭載されている場合がある．これらは，PC の起動時，あるいは OS の起動時，または両タイミングで，認証を行い不正者による利用を排除している．前者の PC 起動時におけるユーザ認証については，生体認証などによるユーザ認証の結果を，BIOS パスワードおよびハードディスクパスワードとリンクさせ，そのユーザ認証結果が正しい場合に，BIOS パスワードの代替とし，PC 側にあらかじめ記憶しておいたハードディスクパスワードをハードディスクに設定する場合が多い．しかしこのようなユーザ認証は，PC 側に機構が組み込まれているため，ハードディスクを PC から抜き取ると機能せず，結局のところ暗号化されたハードディスクとパスワードによる保護のみとなってしまう．一方で本提案手法では，登録外の PC に接続された場合にハードディスクの消去が行われるため，より高いセキュリティが担保される．これはブートディスクおよびセカンドディスクにおいて機能する．

なお，抜き取ったハードディスクは，セカンドディスクとして接続され解析されることが多いと推測される．ただし，抜き取ったハードディスクを BIOS パスワードが設定されていない PC に換装することによって，BIOS パスワードをバイパスすることが可能であり，不正者がそのような目的で，抜き取ったハードディスクを別の PC のブートディスクとして接続する場合もあると考えられる．

4.2 動作評価

ここでは，提案手法の動作評価の結果を示す．評価の際の機器構成は図 1 と同様に，PC とハードディスクから構成される．すべての PC は，不揮発性記憶領域を備え，この不揮発性記憶領域には PC 固有の機器 ID が含まれている．プロファイルとして，**表 1** の PC1 の機器 ID をハードディスク上の認証/消去 App に登録 PC として事前登録した後，動作評価を行った．

なお，EFI OS と，開発した認証/消去 App を合計したイメージのサイズは 1.1 Mbyte 程度であり提案機能を小さくおさえること（3.2 節で述べたコンパクトなアプリ実装）ができている．

4.2.1 基本動作確認

ここでは，提案手法が実際の動作から，要件 (A-1)，(A-2)，(B-3-a) を評価し，要件の充足検証を行う．

図 2 は，本提案手法のハードディスクから PC に対する実際のやりとりを示したものである．これは以下の 5 つの動作からなる．

① ロード：PC ブート時に，PC 起動をフックし，EFI OS および EFI 用認証/消去 App がプリブート認証領

表 1 評価に使用した PC
Table 1 PCs used for evaluation.

登録 PC	PC1	FMV-A8260 (Intel Celeron CPU 1.86GHz, メモリ 2GB,)
登録外 PC	PC2	SONY VAIO PCG-7171N (Intel Core2 Duo 2.53GHz, メモリ 4GB)
	PC3	ACER ASPIRE ONE (Intel Atom N270, 1.6GHz メモリ 1GB)
	PC4	MV-E8260 (Intel Core2 Duo 2.10GHz, メモリ 4GB)

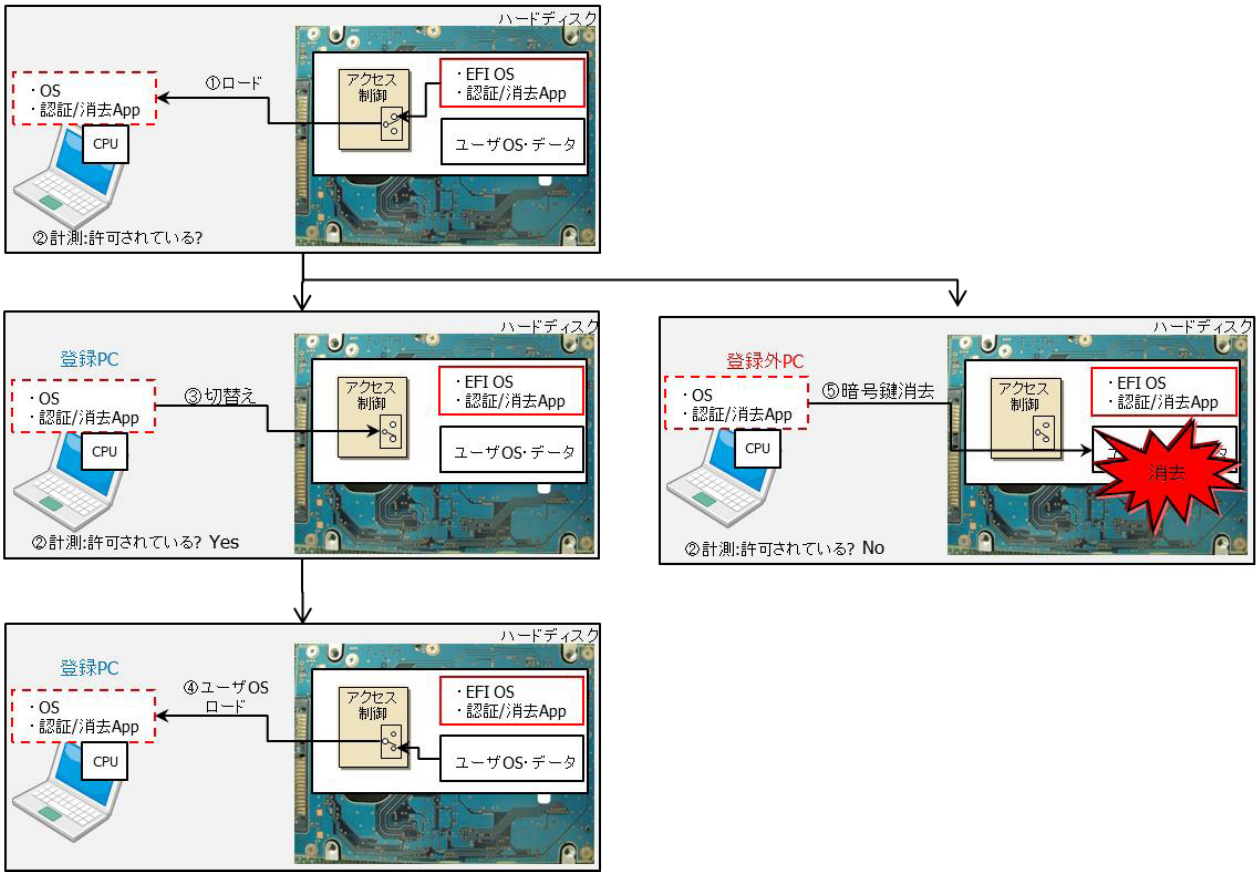

図 2 TCG ハードディスクから PC へのやりとり
Fig. 2 Access from TCG hard drive to PC.

域から PC のメモリに対してロードされる．

② 計測：EFI 用認証/消去 App は，PC にアクセスし機器 ID を読み取る．取得した機器 ID のハッシュをとり，プロファイルと一致するかどうか確認することで，登録 PC であるか判断する．

③ 切替え：登録 PC である場合に，ユーザ OS 領域にアクセスできるよう切り替え ④ へ．このとき，EFI 用認証/消去 App 実行後，EFI の legacy OS loader, BIOS の int13 命令を利用して，PC を再起動することなくユーザ領域の OS を立ち上げることで，ふだんの OS 起動と同様の動作をしている．

④ ユーザ OS ロード：ユーザ OS 領域から，ユーザ OS を PC にロードする．

⑤ 消去：登録外 PC の場合，危険と判断し，PC 上にロードされた EFI 用認証/消去 App から暗号鍵消去コマンドを発行し，ユーザ OS 領域上のデータをすべて消去する．

このように提案手法では，記憶媒体に置かれたプログラムを PC 側で実行することにより記憶媒体の危険度を測定・判断するように動作する．そして，登録外の PC に接続された場合には，情報漏えいの危険があると判断し，鍵消去を実行する追加のセキュリティアクションを実施している．すなわち，これは要件 (A-1) 危険検知，(A-2) 劣悪環境下で保全実行，を満たす動作をしているといえる．また，これらの機構は記憶媒体内にアプリとしてすべて実装されており，要件 (A-3-a) 記憶媒体のみで実行，も満たしているといえる．

4.2.2 様々な状況での動作確認

ここでは，要件 (B-1)，(B-2)，(A-3-b) の様々な状況での動作を評価する，

(B-1) OS の種類を問わない

どのような OS からでも提案手法が動作するのか確認するため，ユーザ領域の OS として，3 種類の OS（Windows Vista，Windows XP，Fedora Linux）を利用し検証を実施した．その結果，ユーザ OS を入れ替えても提案手法が機能し，OS が起動することを確認した．

(B-2) PC の種類を問わない

どのような PC でも提案手法が動作するのか確認するために，異なるメーカの PC を使って動作検証を実施した．登録および登録外 PC として，表 1 のような PC を用いた（いずれの PC もユーザ OS は EFI 非対応であることから，本提案手法内の EFI OS から EFI 非対応 OS を呼び出す際には EFI Legacy OS Loader が機能する）．そして，登録 PC では通常起動し，登録外 PC ではデータの消去が起こることを確認した．この実験結果から，ハードディスク自身のみで，セキュリティ機構を実施可能であることを確認

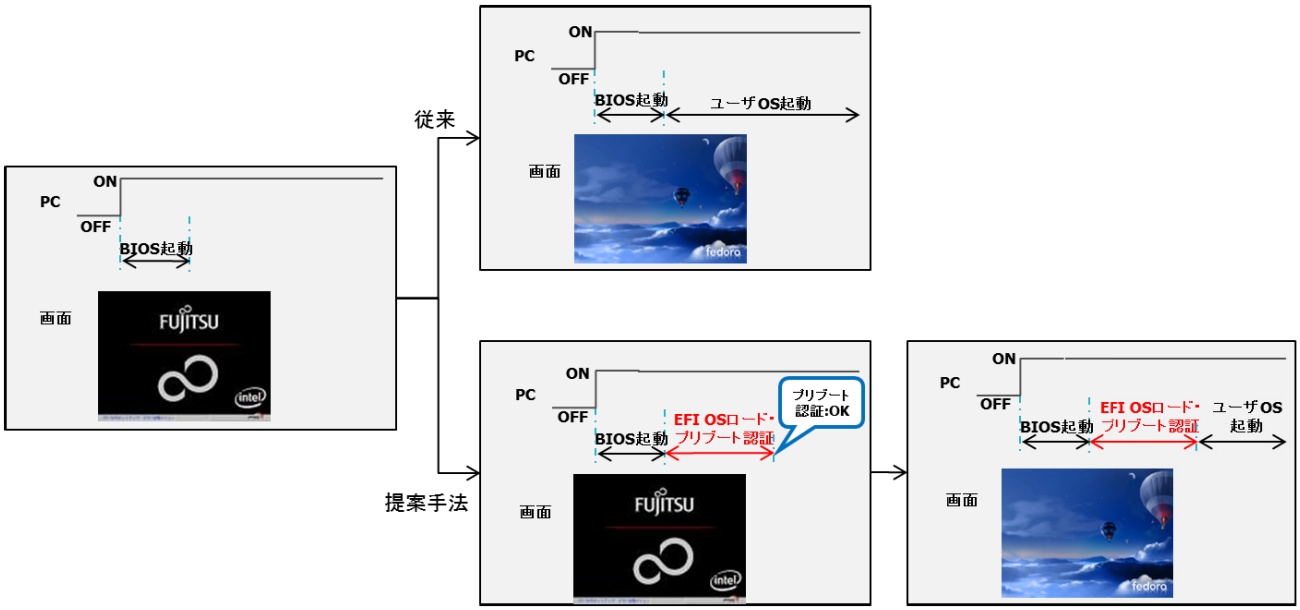

図 3 PC のブート動作
Fig. 3 Boot characteristics of PC.

できたといえる．

(A-3-b) セカンドディスクで機能

ハードディスクのブートディスク接続については，前項で動作確認を実施済みであるため，ここでは，PC に対してハードディスクを USB アダプタ経由で接続したセカンドディスク利用の場合について，以下の動作を確認した．

- ユーザ OS 用認証/消去 App の起動によって，提案手法の認証が行われ，登録 PC あるいは登録ユーザであれば，そのユーザ OS の中身を見ることができること．
- 登録外 PC であれば消去が実行されデータが消えること．

これらより，記憶媒体の接続形式によらずハードディスクがリスクを自分で判断し動作することが分かる．

4.2.3 ユーザビリティ評価

本手法の動作画面の確認と起動時間測定により，(B-3) 保全機能を無効化させない，に対する影響を評価する．

図 3 のように，従来の PC 起動では，PC に電源が入ると，BIOS 起動表示画面が現れ，その後ユーザ領域の OS が起動される．一方，提案手法では，PC に電源が入り，BIOS 起動画面が現れた後，プリブート認証領域にある EFI OS と認証/消去 App が読み込まれリスクベースセキュリティのフェーズが加わる．EFI を利用しているため，再び BIOS 起動画面が表示され，この間に登録 PC かどうか確認が行われる．そして，それが確認されると，ユーザ領域の OS が起動される．すなわち，このときユーザから見た動作は，従来の起動と同じであり，本手法を適用しても PC の再起動をともなうことなく OS が起動でき，ユーザの手間を煩わせるような追加手続きは発生しないことが分かる．よって，要件 (B-3) も満たしているといえる．

表 2 追加起動時間
Table 2 Additional boot time.

PC1	2.2 秒
PC2	15 秒
PC3	8 秒
PC4	2.2 秒

一方で，登録外 PC が接続された場合には，ユーザ領域全体が消去され，次回の PC 起動時に，OS が消去された状態になり “OS not found” が表示され，ユーザが保全処理の実施に気づくことになる．

仮に BIOS パスワードが設定されている場合には，ユーザはいずれの場合においてもパスワード入力を行う．BIOS パスワードはハードディスクパスワードに紐付けられている場合が多く，この BIOS パスワードが正しい場合に，ハードディスクパスワードも解除される．その後，従来では PC がユーザ OS を起動し，提案手法では，プリブート認証領域にある EFI OS と認証/消去 App が読み込まれることになる．

また，表 1 の PC を使って，提案機能を使った場合に，通常 PC の BIOS/OS 起動時間に対してどれくらいのインパクトがあるのか確認を行った結果を**表 2** に示す．増加した起動時間は，EFI OS と EFI 用認証/消去 App の実行によるものである．実行時間にはばらつきがあるが，基本性能としては 2.2 秒程度の追加時間をともなうものと考えられる．いくつかの PC では起動時間がより長くなっているが，これはそれぞれの BIOS においてハードディスク認識/EFI 処理の最適化がなされていないためであると考えられ，今後 EFI が幅広く適用され適切な開発が行われた場

合には，2 秒程度に収まるものが増えると予想される．

一方，登録外 PC に接続された場合の消去時間に関しては，その実行が瞬時で完了するため，差異となって表れる追加の時間は確認されなかった．

5. 関連技術

表 3 にあげた関連技術について触れ，要件との比較を通じて提案手法の妥当性を考察する．結論として，提案手法の要件をすべて満たすものはなく，本論文が対象とする課題を解決できる関連技術が存在しないことが分かる．

5.1 アクティブ型 USB メモリ

2 章において，リスクベースのセキュリティによるデバイス保全には，アクティブ型とパッシブ型があると述べた．本論文ではパッシブ型による提案を行ったが，アクティブ型の例としてあげられるのが Tamatebako [9] である．これは，USB メモリ内にバッテリおよび専用回路を備え，接続時のチェックに加え，指定した時間が経過した場合や，パスワード入力ミスをした場合に，記録したデータをすべて自動的に消去する機能を備えている．アクティブ型は，外部から電源が与えられなくても危険を検知できるため，パッシブ型よりもリスク検知の機能が優れる．以下では，それぞれの要件に対する概要をまとめる．

(A-1)：時間経過とパスワードミスが危険検知の対象であり，記憶媒体が接続される環境までは対象としていない．

(A-2)：消去機能を備えており，危険検知の際に機能する．ただし PC 内蔵ディスクのデータまで消去することはできない．

(A-3-a)：(A-1) と (A-2) を記憶媒体内に備える構成となっており，記憶媒体単体で機能する．しかし，セカンドディスクとしての利用を目的とするものであり，ブートディスクとしての利用は想定していない．ブートディスクとして利用するには，ユーザがメモリに OS をインストールし，さらに (A-1) と (A-2) の機能を持つアプリを実装する必要がある．

(A-3-b)：セカンドディスクとしての利用が第 1 目的である．

(B-1)：USB ストレージクラスであたるため，OS の種類を問わない．

(B-2)：USB をインタフェースとしており，PC の種類を問わない．

(B-3)：ユーザが USB メモリを差し込む手間が発生するため，仮に提案手法と相当の機能を準備したとしても，機能のオフが容易に起こりうる．

5.2 パッシブ型 USB メモリ

パッシブ型 USB メモリは，バッテリを必要とせず，パスワードロック機能を提供する USB メモリを指し，たとえば I/O データ社の製品 [10] などが例としてあげられる．以下では，それぞれの要件に対する概要をまとめる．

(A-1)：パスワードミスが危険検知の対象であり，記憶媒体が接続される環境までは対象としていない．

(A-2)：消去機能は備えていない．

(A-3-a)：(A-1) の機能を備えるのみであり，記憶媒体単体での保全実行は行わない．また，セカンドディスクとしての利用を目的とするものであり，ブートディスクとしての利用は想定していない．

(A-3-b)：セカンドディスクとしての利用が第 1 目的である．

(B-1)：USB ストレージクラスであるため，OS の種類を問わない．

(B-2)：USB をインタフェースとしており，PC の種類を問わない．

(B-3)：ユーザが USB メモリを差し込む手間が発生するため，仮に提案手法と相当の機能を準備したとしても，機能のオフが容易に起こりうる．セカンドディスクとして利用されるものであり，ブートディスクとして利用するために，OS をインストールしたとしても，USB ブートではパ

表 3 関連技術と要件充足

Table 3 Related technologies and sufficiency of requirements.

要件 / 関連技術	(A-1) 危険検知	(A-2) 劣悪環境下で保全実行	(A-3) 第三者の手にある状態で保全実行		(B-1): OS の種類を問わない	(B-2): PC の種類を問わない	(B-3): 保全機能を無効化させない
			(A-3-a) 記憶媒体のみで実行	(A-3-b) セカンドディスクで機能			
アクティブ型 USB メモリ	△	○	○	○	○	○	×
パッシブ型 USB メモリ	△	△	○	○	○	○	×
指紋認証機能付き USB メモリ	△	△	○	○	○	○	×
リモート消去 PC	×	○	×	×	○	×	—
物理セキュリティ保護機能付き USB メモリ	×	○	×	×	○	○	○
データ無効化ハードディスク	○	○	○	—	—	○	—
提案手法	○	○	○	○	○	○	○

スワードをそのまま使うことができない．

5.3 指紋認証機能付き USB メモリ

指紋認証機能付き USB メモリ [11] は，USB メモリ内のデータを暗号化して指紋で守る機能と，OS ログオンを指紋で守る機能を提供する．本論文のスコープである前者の機能としては，パッシブ型 USB メモリと同じであり，認証手段（パスワードであるか指紋であるか）が異なるのみである．

5.4 リモート消去 PC

リモート消去 PC は，PC に対して遠隔から消去信号を送信することで，ハードディスクの消去を可能にする PC を指す．リモート消去 PC では，消去コマンドの発行機能はネットワーク越しの管理機能あるいは PC 側に搭載されるため，ハードディスクが PC から抜き取られた場合には，本論文が対象とする課題に直面することになる．以下では，それぞれの要件に対する概要をまとめる．

(A-1)：危険検知の機能は備えておらず，盗難紛失時など利用者が危険性を判断する．遠隔から消去コマンドを発行する．

(A-2)：消去機能を備えており，遠隔から PC が消去コマンドを受け取った際に消去が実行される．

(A-3-a)：(A-2) の機能を備えるが，記憶媒体本体に消去発行機能を備えていない．

(A-3-b)：PC 本体の機能であるため，セカンドティスクによる接続の評価は対象外になる．

(B-1)：PC 本体に搭載される機能であり，OS の種類は問わない．

(B-2)：リモート信号を受信するための機構が PC ハードウェアに必要になる．

(B-3)：ユーザが PC 利用時に機能の存在を意識することがないため，機能をオフにするモチベーションは起こらないと考えられる．

5.5 物理セキュリティ保護機能付き USB メモリ

Cryptek USB [12] は，金属でできたダイヤル錠の中に USB メモリが入る穴が空いており，そこに USB メモリ本体を挿入して，物理的な錠をかけることができる．USB メモリ内のデータも暗号化により保護されている．すなわち，錠と暗号の組合せによるデータ保護を提供する．錠による保護については以下でそれぞれの要件に対する概要をまとめる．暗号による保護については，パッシブ型 USB メモリと同じである．

(A-1)：危険検知機能は備えていない．

(A-2)：消去機能は備えていない．

(A-3-a)：錠で守られている状態では USB メモリは利用できないため消去はできない．

(A-3-b)：セカンドティスクとしての利用を目的とするが，それを使う以前の対策にあたる．

(B-1)：錠で守られている状態では USB メモリは利用できないため，OS と関係しない．

(B-2)：錠で守られている状態では USB メモリは利用できないため，PC と関係しない．

(B-3)：錠で守られている状態では USB メモリは利用できないため，無効化と関係しない．

なお，物理的な錠による保護は，ハードディスクを抜き取り不可能にするための手段であり，提案手法とは補完関係にある．

5.6 データ無効化ハードディスク

データ無効化ハードディスク [13] は，接続された PC が以前のものと異なる場合，ハードディスクを消去する機能を備えており，基本機能は提案手法と同じであると考えられる．一方で，データ無効化ハードディスクは特定メーカのみが開発する製品であるため，ユーザはこのハードディスクが入った PC を購入するか，このハードディスクを購入して購入済み PC のハードディスクと差し替える必要が生じる．提案手法では，標準のハードディスクの上に機能を実現しており，TCG ハードディスクであれば提案手法の機構を後から簡単にインストールすることも可能であるため，可用性に関する大きなメリットがあると考えられる．以下では，それぞれの要件に対する概要をまとめる．

(A-1)：接続された PC の違いにより危険検知できる．

(A-2)：消去機能を備えている．

(A-3-a)：記憶媒体本体に機能を搭載している．

(A-3-b)：公開資料からは判断できず．

(B-1)：公開資料からは判断できず．

(B-2)：ハードディスクインタフェース（Serial ATA）で接続されるため PC ハードウェア依存はない．

(B-3)：公開資料からは判断できず．

6. 終わりに

PC などの情報機器がネットワークから切り離された状態，さらに情報機器から記憶媒体が切り離された状態における情報漏えいの危険性に対し，本論文では，記憶媒体がリスクを検知した場合に，追加のセキュリティアクションを起こす自己保全手法を提案した．提案手法は，記憶媒体内に機構を組み込むことで，PC に手を加えることなく，PC の通常動作に対するフックを後付けにより機能する寄生型のリスクベースのセキュリティ機能であるという特徴を持つ．また実現コストを意識して，業界標準のハードディスクに対して，ソフトウェアのみにより情報漏えい対策を実現する実装を示した．そして，提案手法を実際の環境の中で動作検証し，機能することを示した．本手法は，通常利用時に利用者が本機能の存在を意識することはなく，

操作性を損ねることもない．一方で，その環境が変わると自己消去を行うセキュリティ機構を実行するリスクベースセキュリティのプラクティカルな一実現手法を確立できたと考えている．

参考文献

[1] Schneier, B.: Risk-based authentication, available from ⟨https://www.schneier.com/blog/archives/2013/11/risk-based_auth.html⟩ (accessed 2016-05).
[2] Top 10 Technology Trends of 2015, available from ⟨https://www.conres.com/it-products-solutions/news-events/top-10-technology-trends-2015-10-risk-based-security-self-protection/⟩ (accessed 2016-04).
[3] TCG Storage Architecture Core Specification, available from ⟨www.trustedcomputinggroup.org/resources/tcg_storage_architecture_core_specification⟩ (accessed 2016-03).
[4] TCG Storage Security Subsystem Class: Opal, Version 2.01, Revision 1.00, available from ⟨www.trustedcomputinggroup.org/resources/storage_work_group_storage_security_subsystem_class_opal⟩ (accessed 2016-03).
[5] Unified Extensible Firmware Interface Specification, Version 2.3 (May, 2009), available from ⟨www.uefi.org/home⟩ (accessed 2016-03).
[6] EFI and Framework Open Source Community, available from ⟨www.tianocore.org/⟩ (accessed 2016-03).
[7] Hughes, G.F.: Disposal of Disk and Tape Data by Secure Sanitization, *IEEE Security & Privacy*, July/August pp.29–34 (2009).
[8] NIST Special Publication 800-88, Revision 1, Guidelines for Media Sanitization (Dec. 2014).
[9] Tamatebako, available from ⟨http://www.fujitsu.com/jp/group/kcn/products/device/product-tamatebako.html⟩ (accessed 2016-04).
[10] IODATA：パスワードロック機能搭載 USB メモリー，入手先 ⟨http://www.iodata.jp/product/usbmemory/standard/tb-pw/index.htm⟩.
[11] セキュリティ USB メモリー，入手先 ⟨http://www.orient-computer.co.jp/products/secureusb.php⟩（参照 2016-09）.
[12] ダイヤル錠でデータも本体も暗号化&ロックする USB メモリ「Cryptek USB」，入手先 ⟨http://gigazine.net/news/20111202-cryptek-usb/⟩（参照 2016-09）.
[13] TOSHIBA：想定外の機器接続でデータを無効化するハードディスク MK6461GSYG，入手先 ⟨http://www.orient-computer.co.jp/products/secureusb.php⟩（参照 2016-09）.
[14] IPA：オンライン本人認証方式の実態調査報告書 (2014)，入手先 ⟨https://www.ipa.go.jp/files/000040778.pdf⟩.
[15] 二村和明，矢崎孝一，中村洋介，郭　兆功，山田　勇：自己消去を可能にする HDD 認証強化，コンピュータセキュリティシンポジウム 2009 (2009).

二村 和明　（学生会員）

1969 年生．1994 年東京電機大学大学院情報通信工学修士課程修了，同年富士通株式会社入社．1997 年から富士通研究所勤務．2016 年より静岡大学創造科学技術大学院博士課程．IoT サービス・プラットフォームの研究開発に従事．

矢崎 孝一

1996 年大阪府立大学大学院工学研究科電子工学専攻修士課程修了．IoT サービス・プラットフォームの研究開発に従事．

中村 洋介

1977 年生．2000 年横浜国立大学工学部電子情報工学科卒業．2002 年同大学大学院工学研究科電子情報工学専攻修士課程修了．同年（株）富士通研究所入社．IoT サービス・プラットフォームの研究開発に従事．

西垣 正勝　（正会員）

1990 年静岡大学工学部光電機械工学科卒業．1995 年同大学大学院博士課程修了．日本学術振興会特別研究員（PD）を経て，1996 年静岡大学情報学部助手．同講師，助教授の後，2010 年より同大学創造科学技術大学院教授．博士（工学）．情報セキュリティ全般，特にヒューマニクスセキュリティ，メディアセキュリティ，ネットワークセキュリティ等に関する研究に従事．2013～2014 年情報処理学会コンピュータセキュリティ研究会主査．2015 年より電子情報通信学会バイオメトリクス研究専門委員会委員長．