National Institute of Advanced Industrial Science and Technology
AIST

Japan Computer Emergency Response Team Coordination Center

CSSC

セキュリティバリアデバイスのストレージ保護機能とその活用

戸田賢二　古原和邦

（独）産業技術総合研究所（AIST）

[制御システムセキュリティセンター（CSSC）との連携研究]

National Institute of Advanced Industrial Science and Technology
AIST

講演内容

CSSC

- 開発の背景
- SBD（セキュリティバリアデバイス）の概念
- データ保護機能の動作方式
- ハードウェア及びセキュリティタグ
- セクタ単位のアクセス制御
- ファイル単位のアクセス制御（NTFS）
- アクセスログ
- SBDの制約と可能性

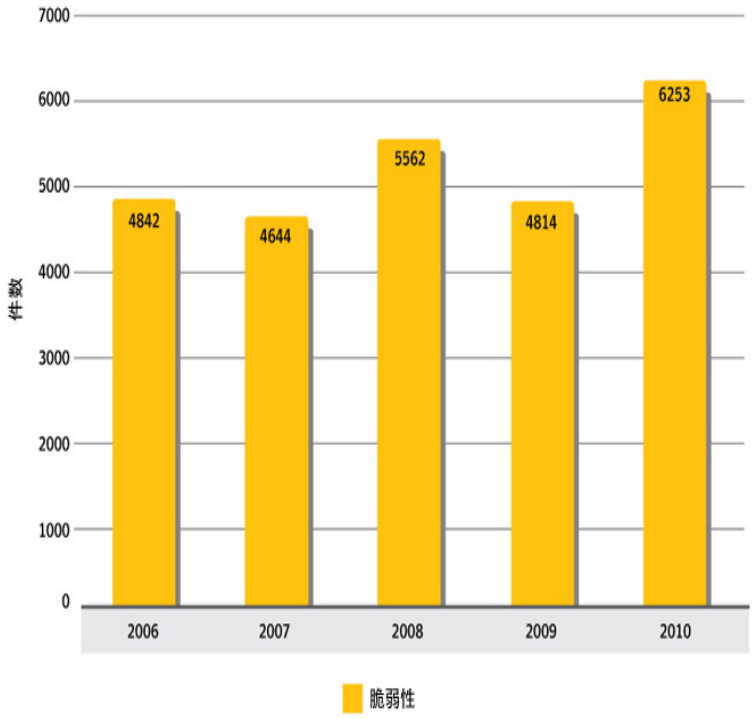
National Institute of Advanced Industrial Science and Technology
AIST

研究の背景:PCやサーバ

CSSC

- 巨大となったOSやアプリの脆弱性を完全にふさぐことは困難(増加傾向)

- 未発見の脆弱性や発見されてから対策が行われるまで間はゼロデイと呼ばれ無防備な状態



脆弱性特定数の推移

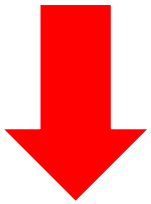
(http://www.symantec.com/ja/jp/threatreport/topic.jsp?id=vulnerability_trends&aid=total_number_of_vulnerabilities)

National Institute of Advanced Industrial Science and Technology
AIST

研究の背景：制御システム

CSSC

- ハードウェアの制約上負荷のかかるセキュリティソフトの導入が困難
- 動作検証や可用性の問題から古いOSやアプリをセキュリティパッチもあてずに使い続けるケースも多い



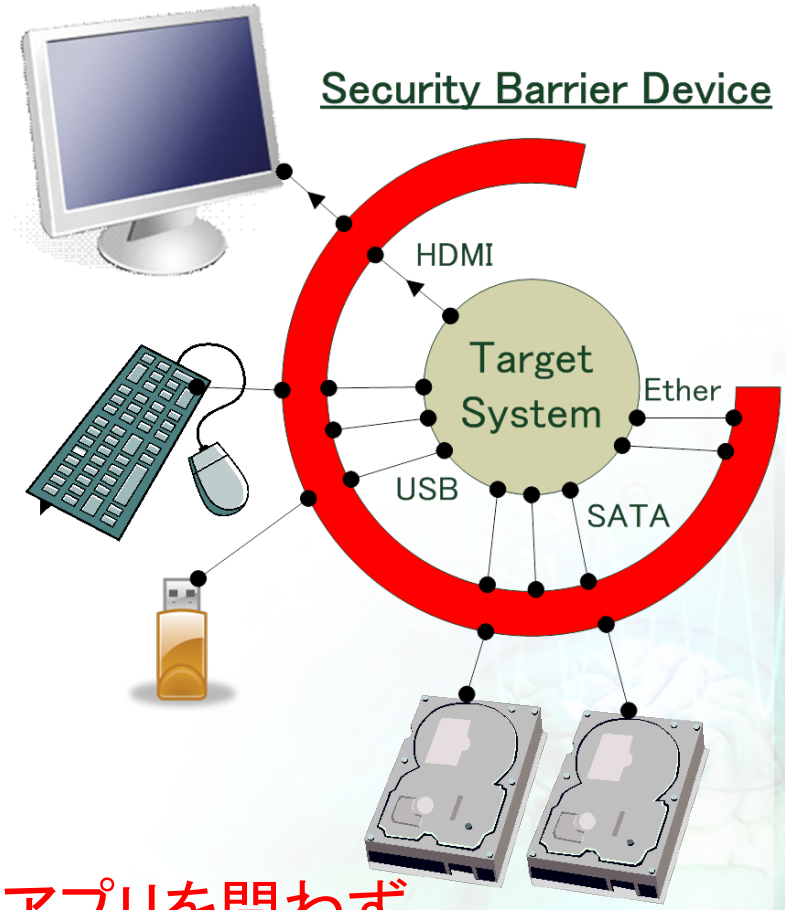
ファイルシステムは現在
NTFSにのみ対応

- 簡単に後付けでき、ソフトのインストールが不要で、OSやアプリを問わず装着するだけで、指定した重要データを防御する本発表のSBDの開発

National Institute of Advanced Industrial Science and Technology
AIST

CSSC

SBD装着概念図



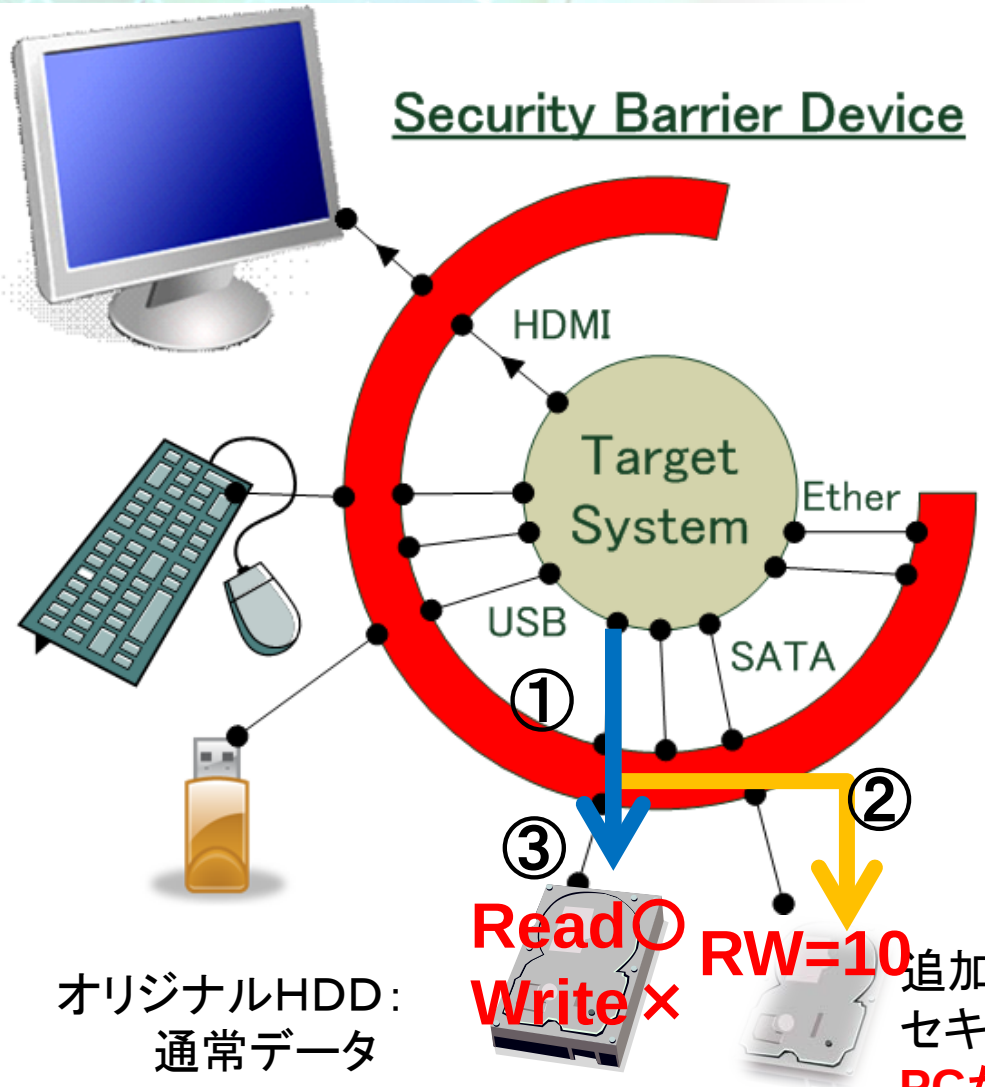
ソフトもハードもそのままで
IOポートにSBDを挟むだけ

OSやアプリを問わず
データアクセスを保護！

National Institute of Advanced Industrial Science and Technology AIST

CSSC

SBD: データ保護機能の動作方式



①ターゲットシステム（防御対象システム）からストレージにIOリクエスト発生

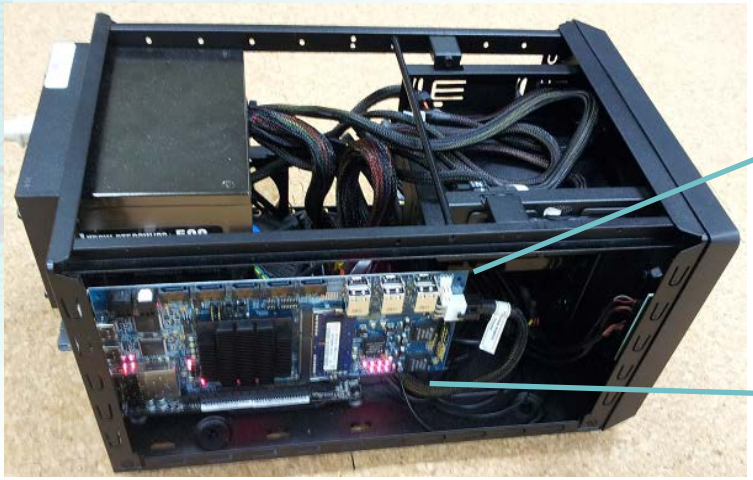
①SBDは、対応するIOブロックのセキュリティ情報を同時に読み出す

②セキュリティ情報に応じて、アクセスを制限したり、ユーザに確認したりする

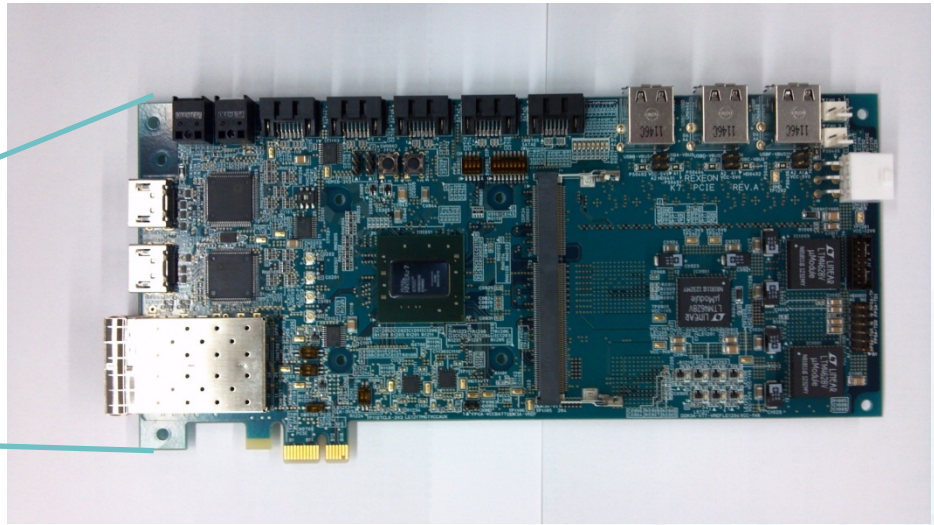
National Institute of Advanced Industrial Science and Technology
AIST

SBD: 全体写真

CSSC



セキュリティバリアデバイス

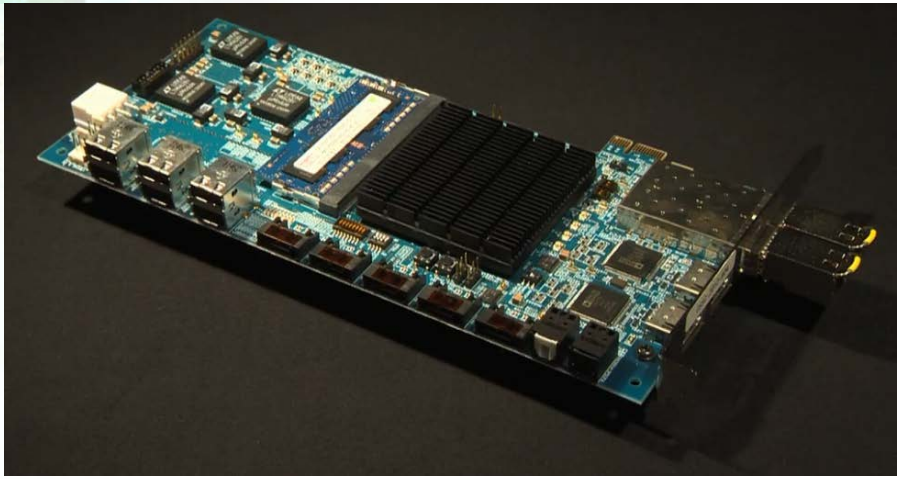


SBD用FPGAボード

National Institute of Advanced Industrial Science and Technology
AIST

SBD: ボードとその仕様

CSSC

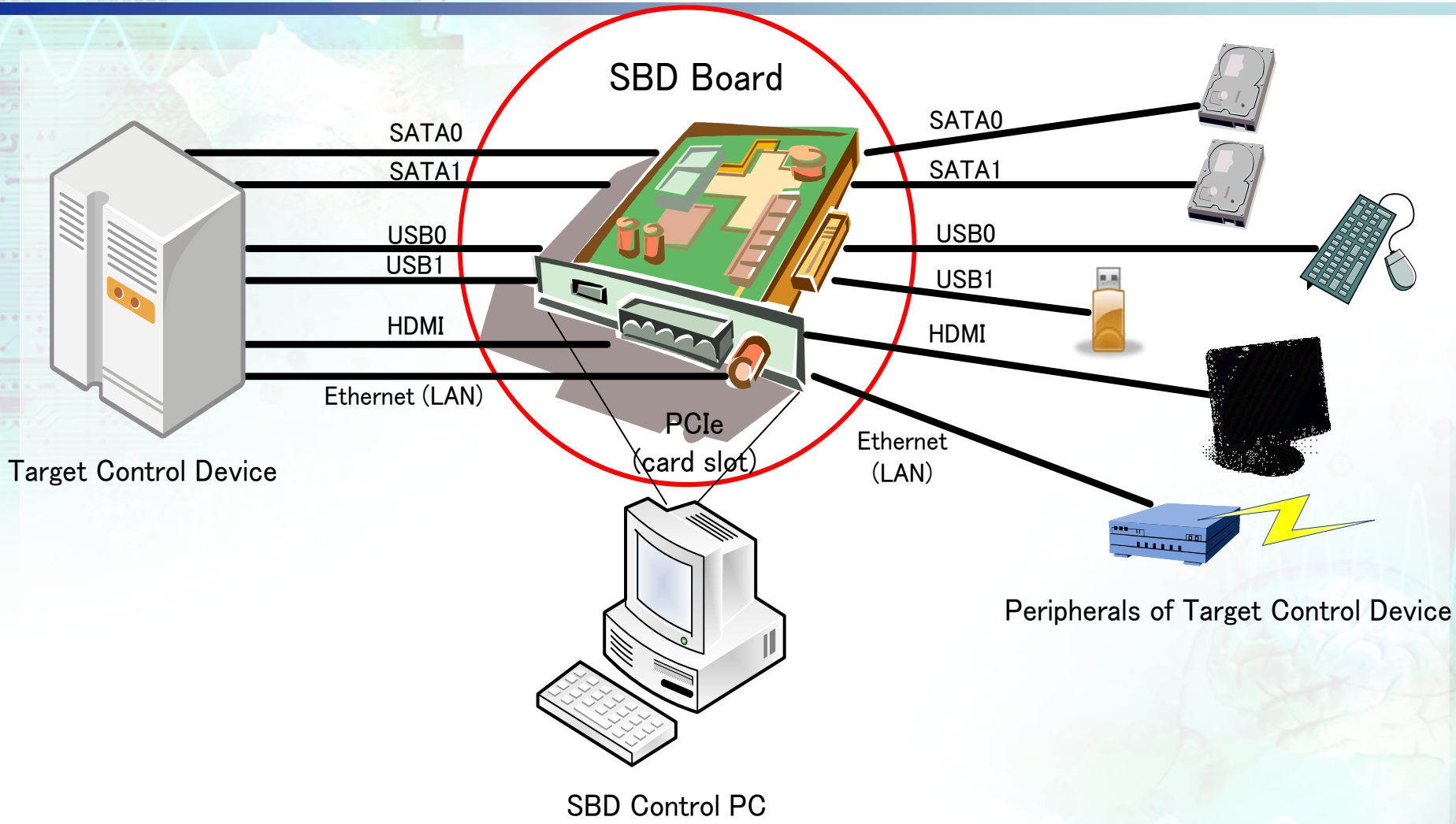


- ボード大きさ: PCI Expressカード形状（突起部除き長さ230mm高さ110mm）
- FPGAチップ: Xilinx Kintex-7　676ピン　XC7K325T
- コンフィギュレーション用フラッシュロム: 電源ON時にFPGAへの回路書き込み用
- メモリI/F: DDR3 SODIMM×1ポート
- 映像入力: HDMI×1ポート（コピー制御機能HDCPなし）
- 映像出力 : HDMI×1ポート（コピー制御機能HDCPなし）
- 光オーディオ: 入力×1，出力×1
- ストレージI/F: SATA (7ピン)×5ポート
- 通信用I/F: 1G/100Mビットイーサ（RJ-45）×2ポート
- 汎用I/F: USB (Type A)×6ポート（USB2.0対応）
- SBD制御PC用I/F: PCI Express×1

National Institute of Advanced Industrial Science and Technology
AIST

SBDボードの接続形態

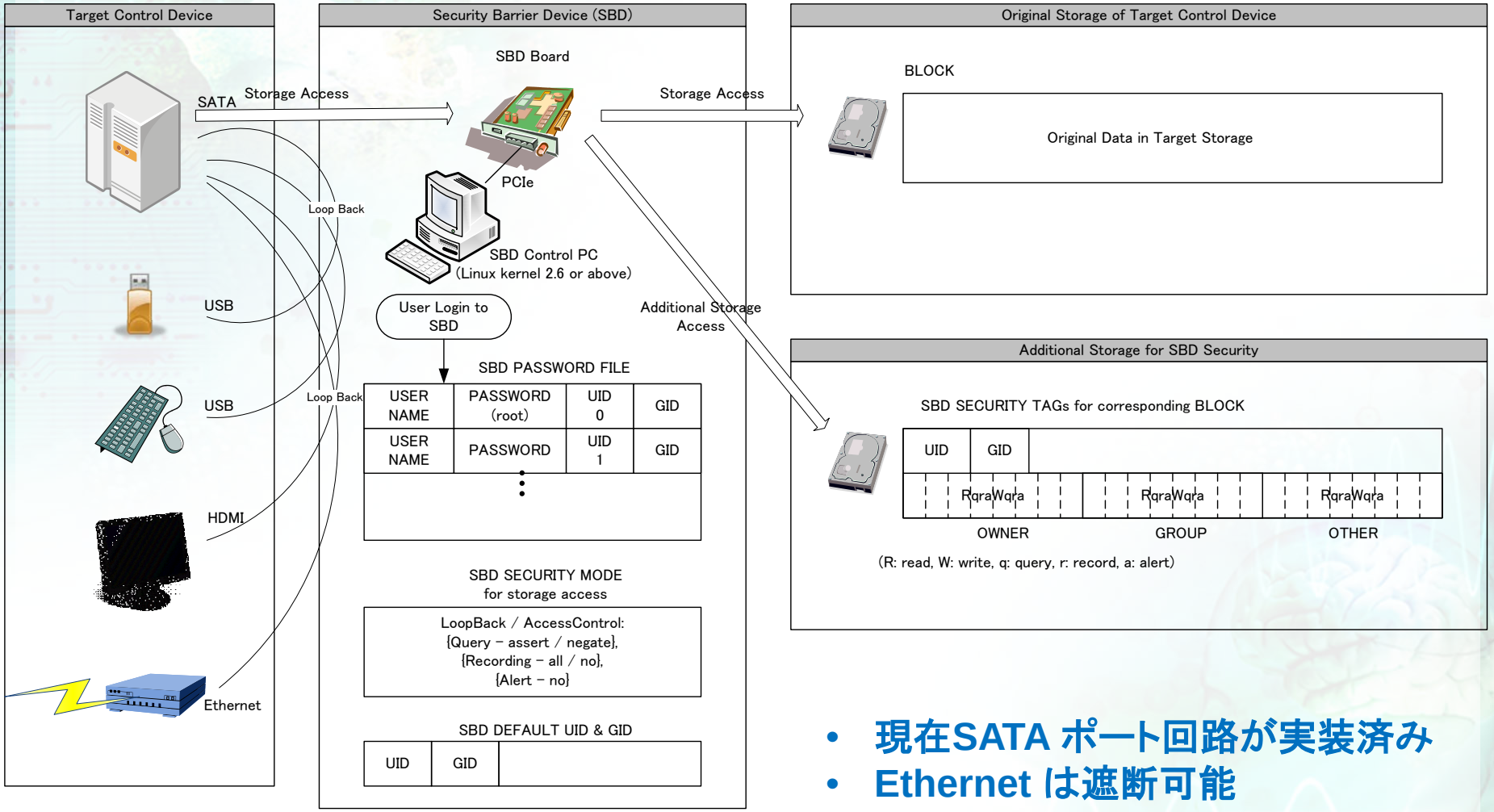
CSSC



National Institute of Advanced Industrial Science and Technology
AIST

CSSC

SBD: セキュリティタグの構成（セクタ単位の制御）



- 現在SATA ポート回路が実装済み
- Ethernet は遮断可能

National Institute of Advanced Industrial Science and Technology AIST

セキュリティバリアデバイス(SBD):ファイル単位のアクセス制御　動機

CSSC

ファイル単位の防御ができれば利便性が大幅に向上する:

- システムや重要データは多くの場合ファイルである
- ファイルを防御用パーティションに移動しなくてよい
- オリジナルのデータディスクをそのまま保護可能
- 防御対象ファイルの指定や解除が極めて容易
- SBDの着脱のストレスがゼロ(コネクタ着脱のみ)

National Institute of Advanced Industrial Science and Technology AIST

SBD:ファイル単位のアクセス制御 CSSC
高解像度化の実現

ファイルのデータ ＋ ルートからのパス を保護

ディレクトリやポインタ領域のアクセス単位

≦セクタサイズ512B

アクセス制御の高解像度化が必要

1. セクタに対応するセキュリティ情報に必要とされる解像度を記録
2. 当該セクタをストレージに書き込むとき，その解像度の単位でアクセス制御の処理を行う：書き込み禁止であれば，書き込み禁止の部分のデータはストレージから読み出した方を用いて当該ディレクトリ領域上のデータは変更しない

National Institute of Advanced Industrial Science and Technology AIST

SBD:ファイル防御の動作（リード禁止）

CSSC

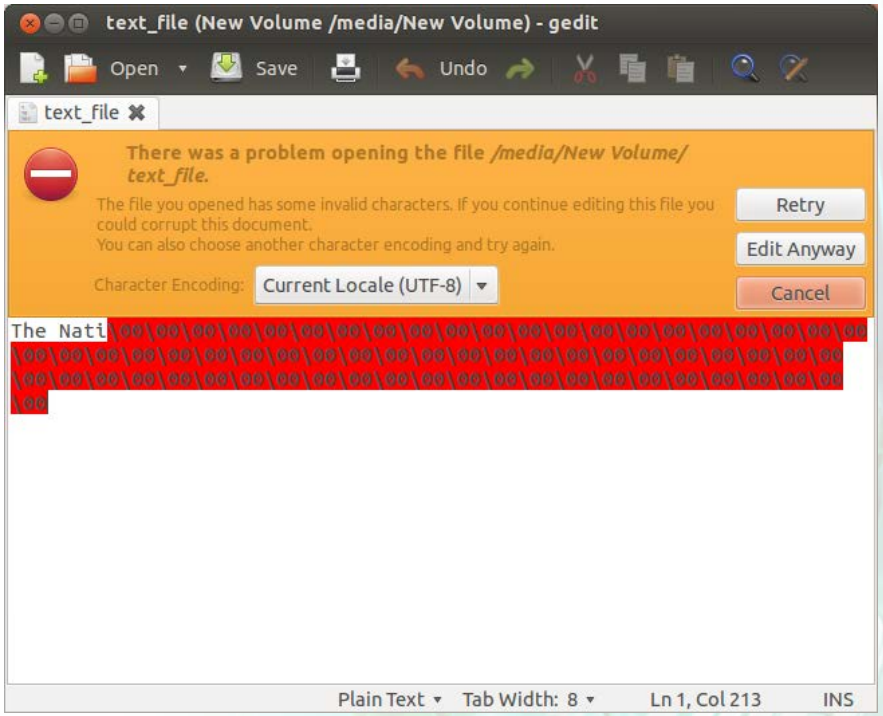
リード禁止:

1. 防御対象のファイル情報をSBDに書き込む（バイト単位で禁止可能）
2. そのファイルを防御対象PCから読む(SBDはユーザに警告を出す）

➡0が内容として返される

先頭8バイトより後ろを読み出し禁止にした場合：

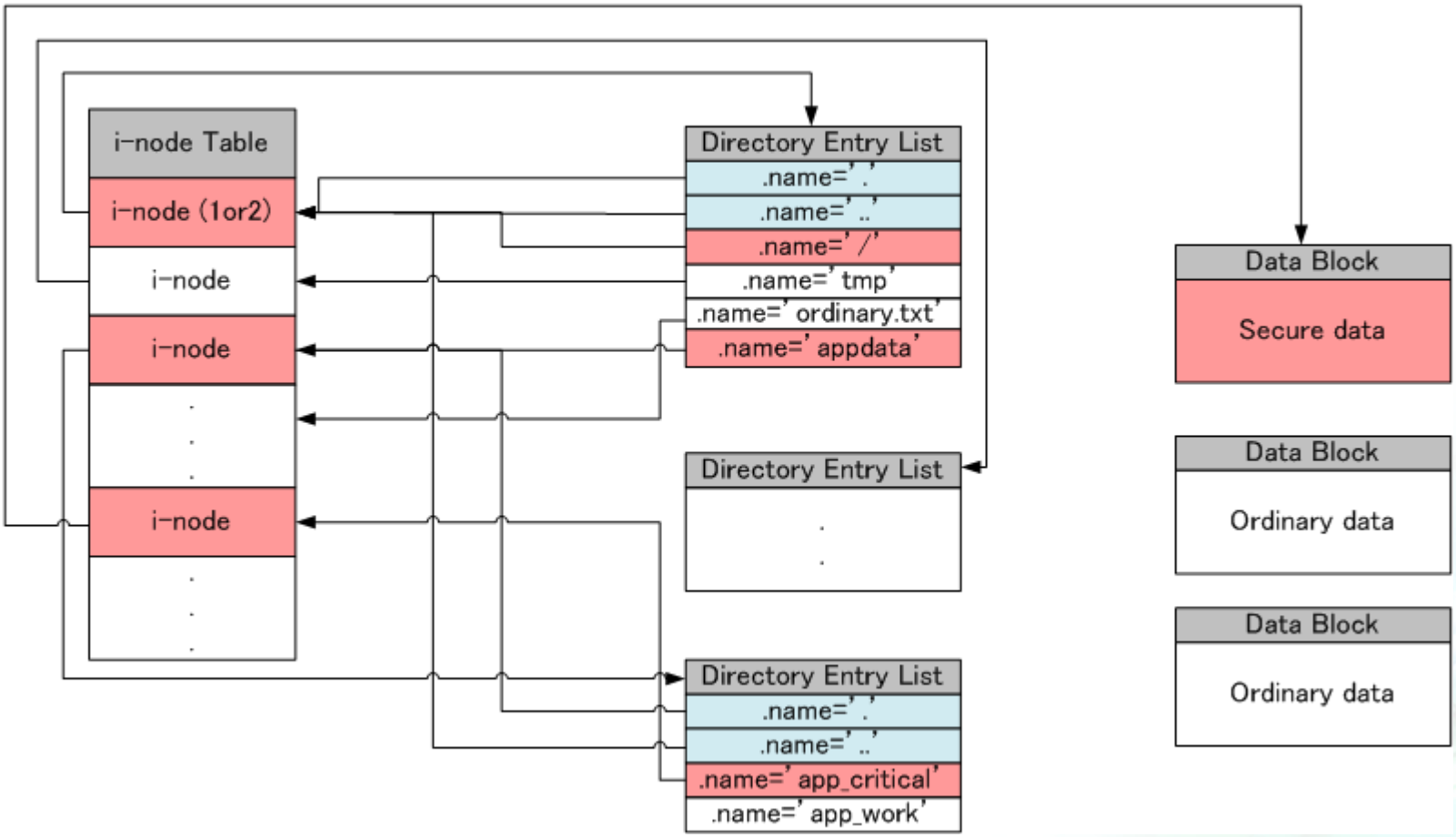
防御対象PCでのエラーメッセージ(Ubuntu) →



National Institute of Advanced Industrial Science and Technology AIST

SBD:書き込み禁止の要件
EXT2(Linux)ファイルシステムの例

CSSC



- /appdata/app_critical がセキュアデータ:
  ルートからのパスも保護が必要

National Institute of Advanced Industrial Science and Technology AIST

ファイル単位のアクセス制御：高解像度化しても残る困難

CSSC

NTFSファイルのライト禁止制御：

① PCメモリ上のディスクのキャッシュの内容とディスクの内容が異なってしまうためファイルシステムが破損しOSがクラッシュする可能性がある。

② ライト禁止ファイルのルートからのパス（すなわちそのファイルまでのディレクトリ群）もライト禁止する必要があるが、NTFSでは、ディレクトリ内のファイルへのポインタエントリはBalanced Treeのアルゴリズムで管理され、ライト禁止ファイルのエントリの位置が、通常ファイルの追加や削除により変動する。←SBDは固定領域の保護を想定したFPGA上の回路で高速化を達成しており、可変領域への対応は性能ペナルティを招く。

National Institute of Advanced Industrial Science and Technology AIST

SBDのファイル単位のアクセス制御：OSのキャッシュとの整合

CSSC

【問題点】 WindowsやLinuxではメモリ上のキャッシュを活用し高速化：

- スーパーブロック（ブロックグループデスクリプタ，フリーブロックやフリーi-nodeのビットマップ情報など）
- i-nodeキャッシュ
- ディレクトリエントリキャッシュ
- バッファキャッシュ（ディスクブロックのデータに対応）
- ページキャッシュ（ファイルのデータに対応）

書き込み時にストレージ上のデータ書き込みを禁止すると

キャッシュとの齟齬が発生！

National Institute of Advanced Industrial Science and Technology AIST

ファイル単位のアクセス制御：困難を克服

CSSC

SBDでOSの挙動を観察・実験

NTFSファイルのライト禁止制御：

① PCメモリ上のディスクのキャッシュの内容とディスクの内容が異なってしまうためファイルシステムが破損しOSがクラッシュする可能性がある。

→SBDからエラーを返し意図的に疑似不良ブロックを発生させる！

② ライト禁止ファイルのルートからのパス（すなわちそのファイルまでのディレクトリ群）もライト禁止する必要があるが、NTFSでは、ディレクトリ内のファイルへのポインタエントリはBalanced Treeのアルゴリズムで管理され、ライト禁止ファイルのエントリの位置が、通常ファイルの追加や削除により変動する。←SBDは固定領域の保護を想定したFPGA上の回路で高速化を達成しており、可変領域への対応は性能ペナルティを招く。

→ファイル内の親ディレクトリへのポインタは位置固定！

National Institute of Advanced Industrial Science and Technology AIST

CSSC

ファイル単位のアクセス制御：書き込み禁止時のエラー種別の実験

書き込み禁止ファイルへ書き込みに対しSBDがOS（win7）に次のエラーを返した場合(書換／リネーム／削除)

- Write Protect エラー：OSの応答が悪くなり、再起動するのに3分必要（終了時にも当該領域の書き込みリトライを繰り返すため）→ファイルは書換前の状態に戻るが書き込み禁止時にシステムが不安定

- Device Fault エラー：OSは当該セクタを不良セクタと認識し、正常なセクタと入れ替える。ユーザはSBDから警告を受け取るだけで、OSは正常。OSを再起動する際SBDが疑似不良セクタを元に戻す→ファイルは書換前の状態に戻る＆システムは常に安定

National Institute of Advanced Industrial Science and Technology AIST

SBD: Windows7における ファイル防御の動作(ライト禁止)

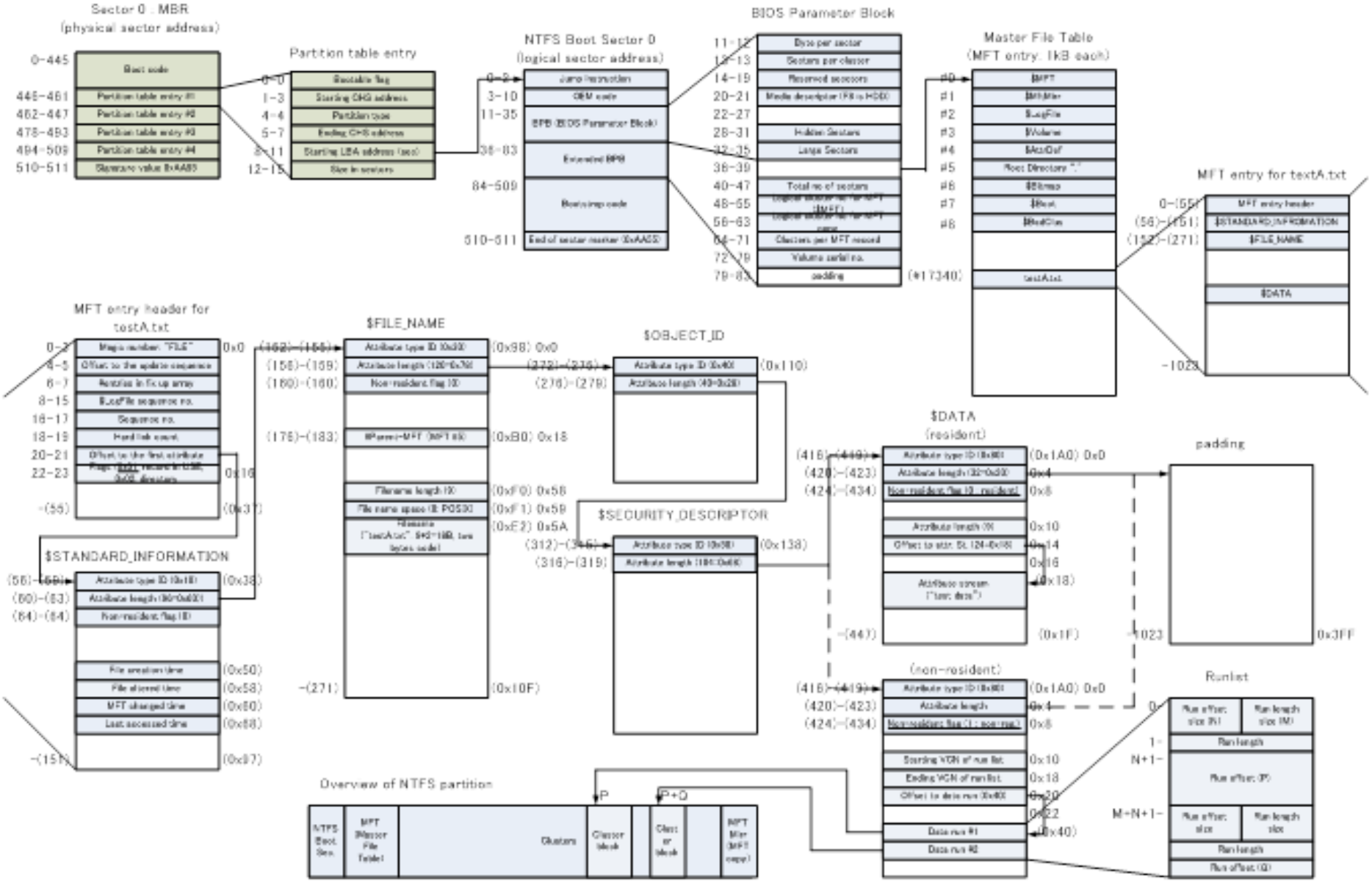
CSSC

ライト禁止(上書き／リネーム／消去):

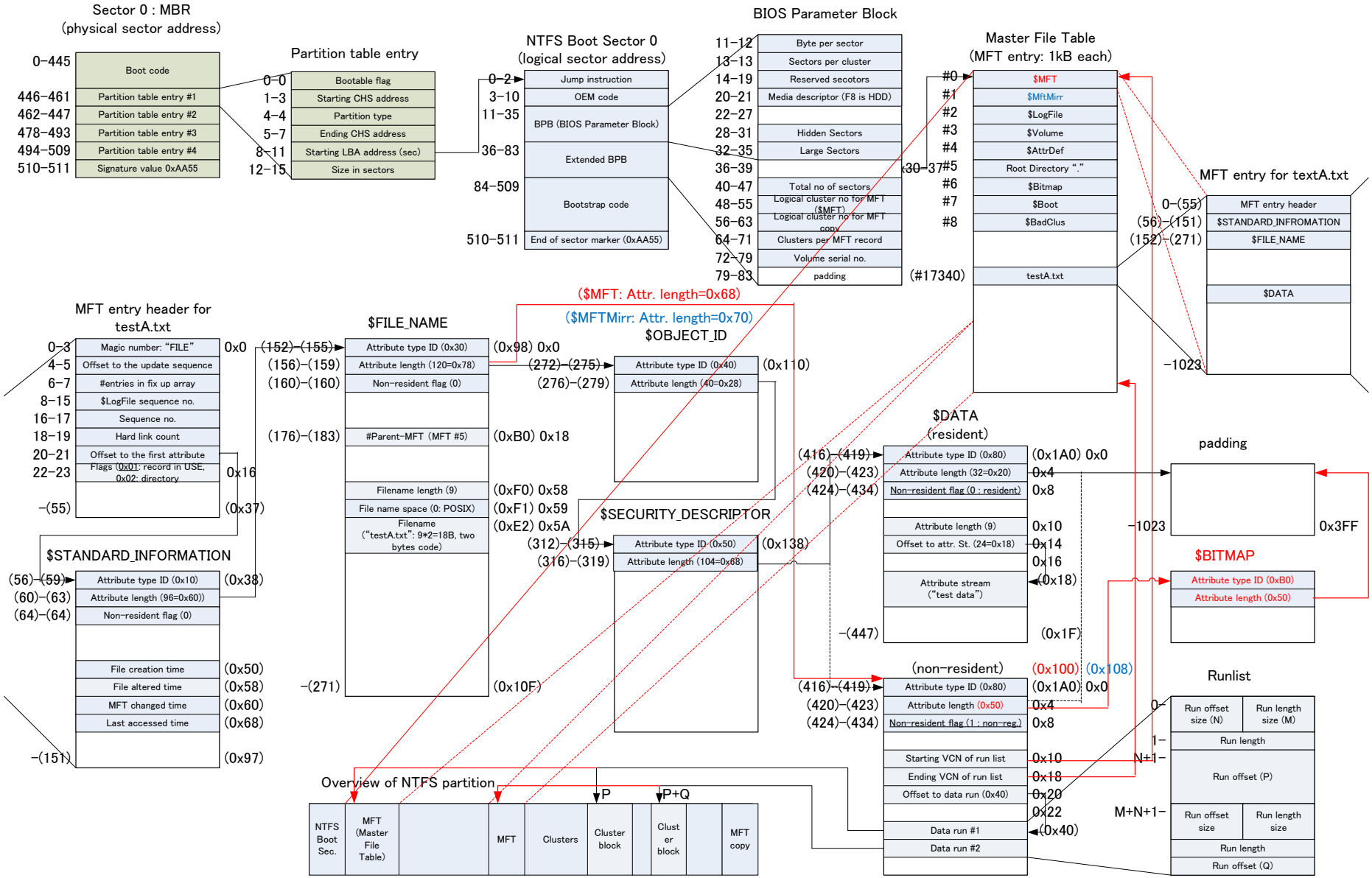
1. 防御対象のファイル情報をSBDに書き込む
2. 防御対象PC を再起動(キャッシュを無効化するため)
3. そのファイルを防御対象PCから 上書き／リネーム／消去 する、とその操作は完了する(SBDは、Device Fault エラーを返し疑似不良セクタを発生させると共に、ユーザに警告を出す)
4. 防御対象PCに chkdsk をスケジュールして終了
5. SBDが防御対象ディスクの$MFT(i-nodeテーブル)を疑似不良セクタの無かった状態に戻す
6. 防御対象PCを起動(chkdskが実行されてからOS起動)

➡ ライト禁止ファイルが復旧

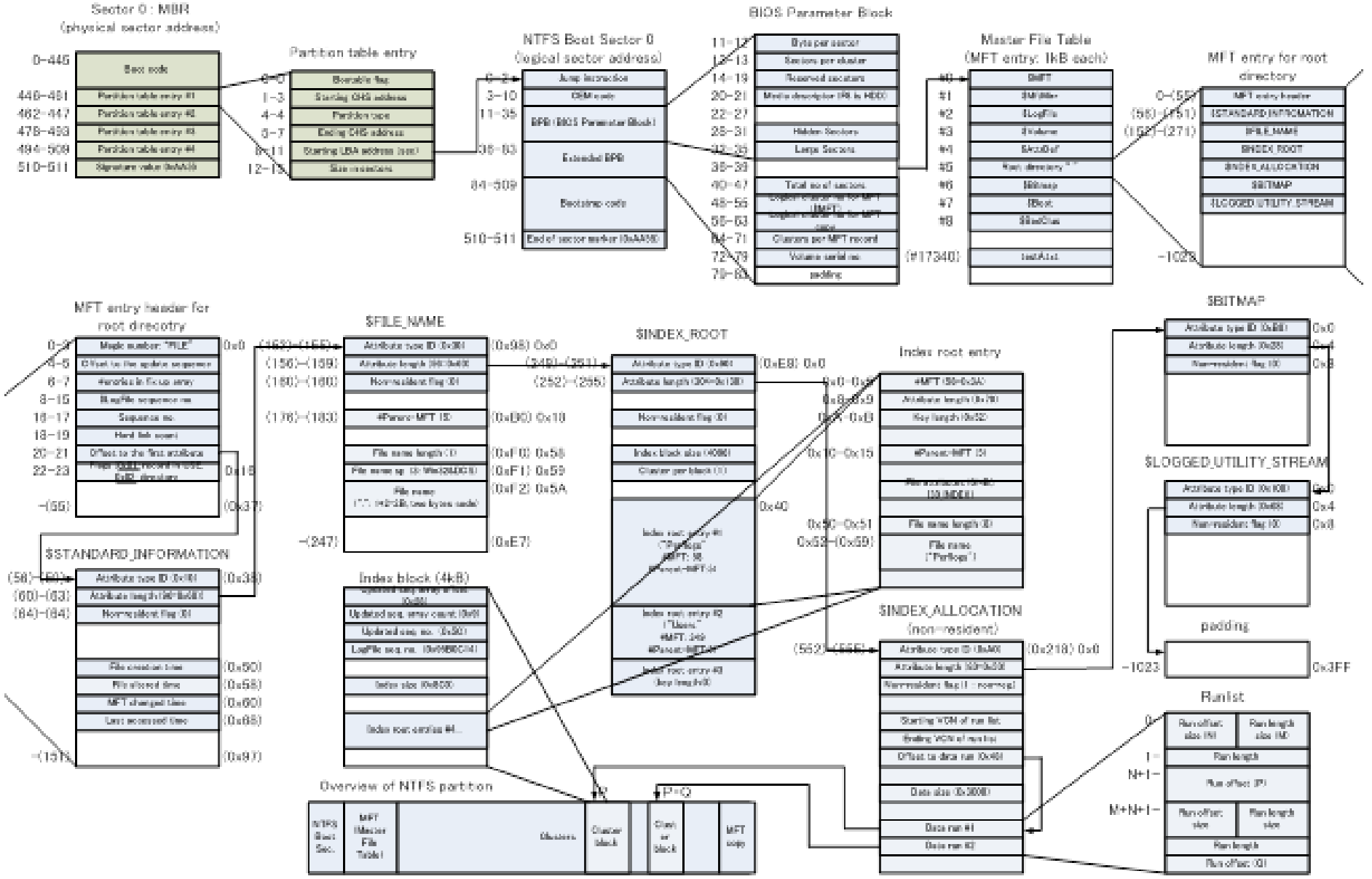
NTFS File System Map (*file*)



NTFS File System Map (file and $MFT&Mirr)



NTFS File System Map (*directory*)



National Institute of Advanced Industrial Science and Technology AIST

SBD:ファイル単位のアクセス制御 ライト禁止の動作形態（まとめ）

CSSC

ライト禁止をOSと整合させて解決！

NFTSファイルのライト禁止制御：

① ライト禁止ファイルへのライト、リネーム、削除などが行われた場合、まずメモリ上のディスクのキャッシュで操作が完了し、書き換えが成功したように見える。

② しかし、間もなくそれは、ディスクに書かれることになり、SBDが検知する。

③ SBDは、疑似不良セクタを発生させ、同時にユーザにライト禁止違反を警告　（SBDは違反をトリガとしてイーサネットを遮断することも可能）

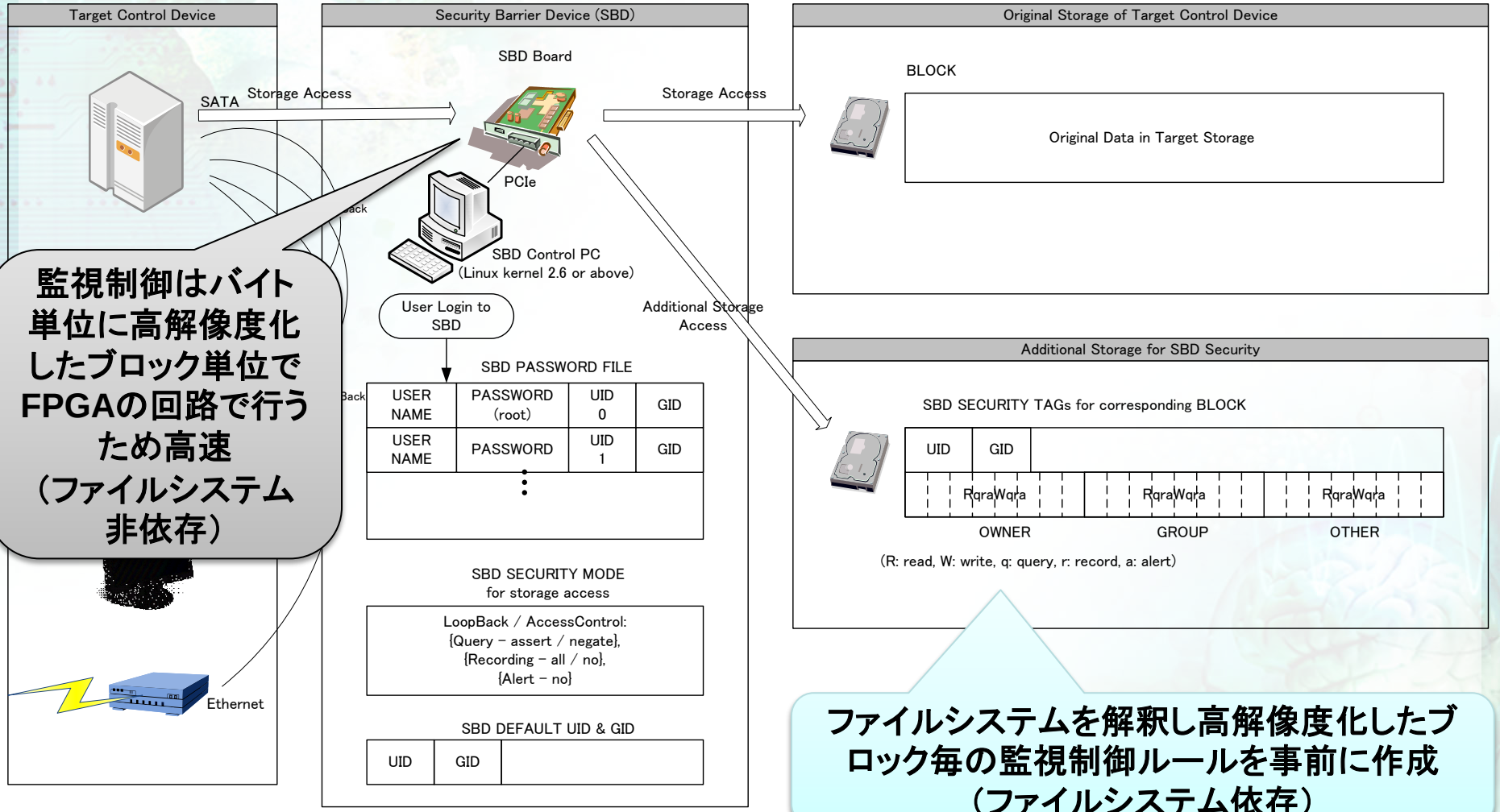
④ ユーザがOSを再起動すると、SBDがファイル復帰動作を行いライト禁止のファイルが元の状態に復活し、PCは元の状態にもどる。

$BadClusファイルから疑似不良ブロックを回収

National Institute of Advanced Industrial Science and Technology
AIST

SBD: ファイル単位のアクセス制御 実現方式

CSSC



監視制御はバイト単位に高解像度化したブロック単位でFPGAの回路で行うため高速（ファイルシステム非依存）

ファイルシステムを解釈し高解像度化したブロック毎の監視制御ルールを事前に作成（ファイルシステム依存）

National Institute of Advanced Industrial Science and Technology AIST

SBD: アクセス制御 性能

CSSC

オーバヘッドの大きい高解像度化した状態:

バイト単位のアクセスを監視した状態＝

ファイル単位のアクセスを監視した状態

実験レベルで リード 130MByte/s

ライト 60MByte/s 様々な条件でテスト中

セクタ同士の比較をバイト単位でマスクして行う回路
＋複数セクタをまとめてディスクIOするバッファ回路

測定条件:

データ用及びセキュリティタグ用ディスクとして、Samsung SSD 830, 128GBを用い、UbuntuのDisk UtilityのRead-Only / Write Benchmarkを使用

National Institute of Advanced Industrial Science and Technology AIST

SBD: アクセスログ

CSSC

ソフトウェアによるファイルのアクセスログ機能:

- .NET Framework の FileSystemWatcher クラス(msdn)
- Windows のセキュリティ監査の新機能(technet: グローバル オブジェクト アクセスの監査など)
- 監視ソフトウェア(ファイルモニタなど)
- ハイパーバイザによる実装

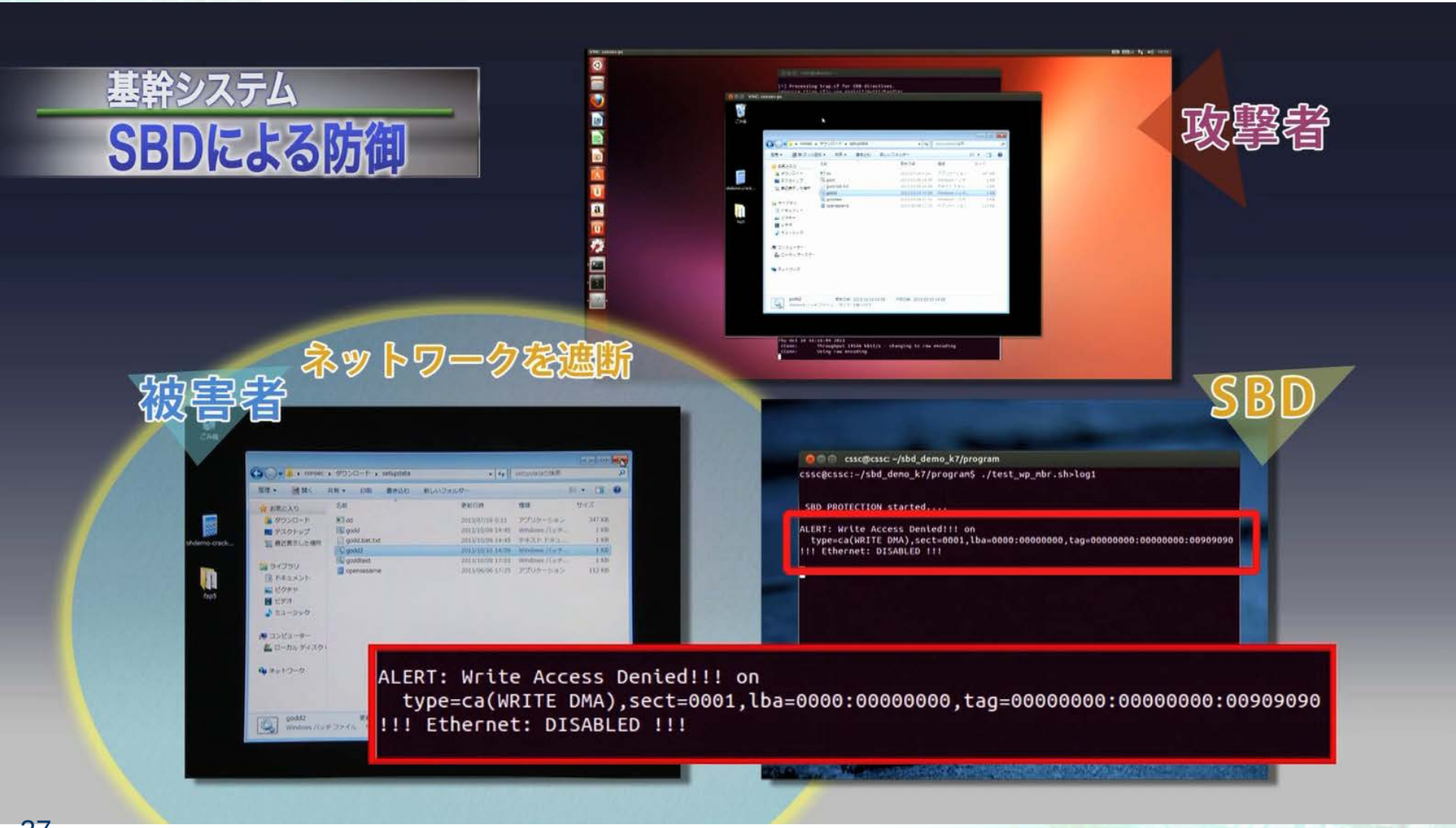
SBDは、マザーボードとディスクの間でSATAを中継しておりファイルへのアクセスを把握可能

- ログ取得がマルウェアから隔離
- ログ取得のオーバヘッドが殆どない
- 取得したログと防御への活用(挙動監視や書き込み禁止など)

National Institute of Advanced Industrial Science and Technology AIST

SBDがブート領域への書き込みを防御しイーサネットを遮断し遠隔操作を断ち切った例

CSSC



National Institute of Advanced Industrial Science and Technology
AIST

SBDの制約と可能性

CSSC

- Windows Update (書き込み禁止システムファイルが含まれる場合)、デフラグ、chkdskなどに際しては、SBDの監視を解除し、事後にセキュリティ情報の更新が必要
- Diskやパーティションの暗号化には非対応。ファイル単位(コンテンツのみ)の暗号化には対応
- ファイル・フォルダ・パーティション・ディスクの秘匿が容易
- 一旦書いた内容は保護される追記型ファイルの実現(ログファイルの改ざん防止にも有効)
- ホームページの改ざん防止・警告
- データサーバでの顧客情報の保護(指定ファイル(群)の(大量)リードなど検出可能。ファイル中の特定データや特定のフィールドを読み出し禁止に設定など可能)
- ディスクアクセス(将来他のポートも)データの取得・解析・制御ツールとして

ご静聴ありがとうございました