

今後の再発防止策

1. カードキーと指紋認証による入退出

- └入荷エリア・・・カードキーによる入退出
- └データ消去室・・・カードキーと指紋認証による入退出
- └梱包と出荷エリア・・・カードキーによる入退出



2. 入退出ログ管理

- └誰がいつ入退出したか社員固有IDキーと指紋認証で紐付けしています。

日付	曜日	入室時間	退出時間	扉番号	ID	氏名
2019/11/8	金	8:50	12:00		1	
2019/11/8	金	9:00	11:30		1	
2019/11/8	金	12:45	15:30		2	
2019/11/8	金	13:00	13:45		2	
2019/11/8	金	13:15	14:00		3	
2019/11/8	金	14:00	18:00		3	
2019/11/8	金	14:30	18:00		4	
2019/11/8	金	16:00	18:30		4	

3. 24時間監視カメラ

- └監視カメラにより24時間録画しております。



4. 1台1台の個体管理

└個体に管理番号と管理バーコードラベルを貼付けし、1台1台の入荷からデータ消去、出庫まで荷物の個体管理をしています。



5. 私物管理（持ち込み・持ち出し防止）

└設備内に私物を持ち込まないように専用ロッカー設置し、持ち出し防止に手荷物検査をしています。



6. 開閉アラーム警報

└1分間開いていたら警報を発します。



7. ポケット縫い付け専用ユニフォーム

└ポケットが縫いつけられている専用ユニフォームを着用しています。



1. 物理破壊

ハードディスク専用の物理破壊機により、4か所に穴を開けてディスクを物理的に破壊します。



2. 磁気破壊

直流強磁場を瞬間照射し、ハードディスク等の磁気記録媒体に記録されているデータを一瞬で完全破壊します。



3. ソフトウェア消去

データ消去ソフトウェアを用いて消去いたします。1回又は希望によって3回上書き書き込みを行います。



4. メディアシュレッダー

CD-RやUSBフラッシュメモリー、SDカード等を粉碎破壊しています。



消去完了明細 (希望されたお客様のみ提出)

内容

- ・メーカー名
 - ・型番
 - ・PCシリアル番号
 - ・HDDシリアル番号
 - ・お客様管理番号
- ※PC及びHDDシリアル番号の取得明示は希望されたお客様のみ提出します。

ソフトウェア消去証明書 (希望されたお客様のみ提出)

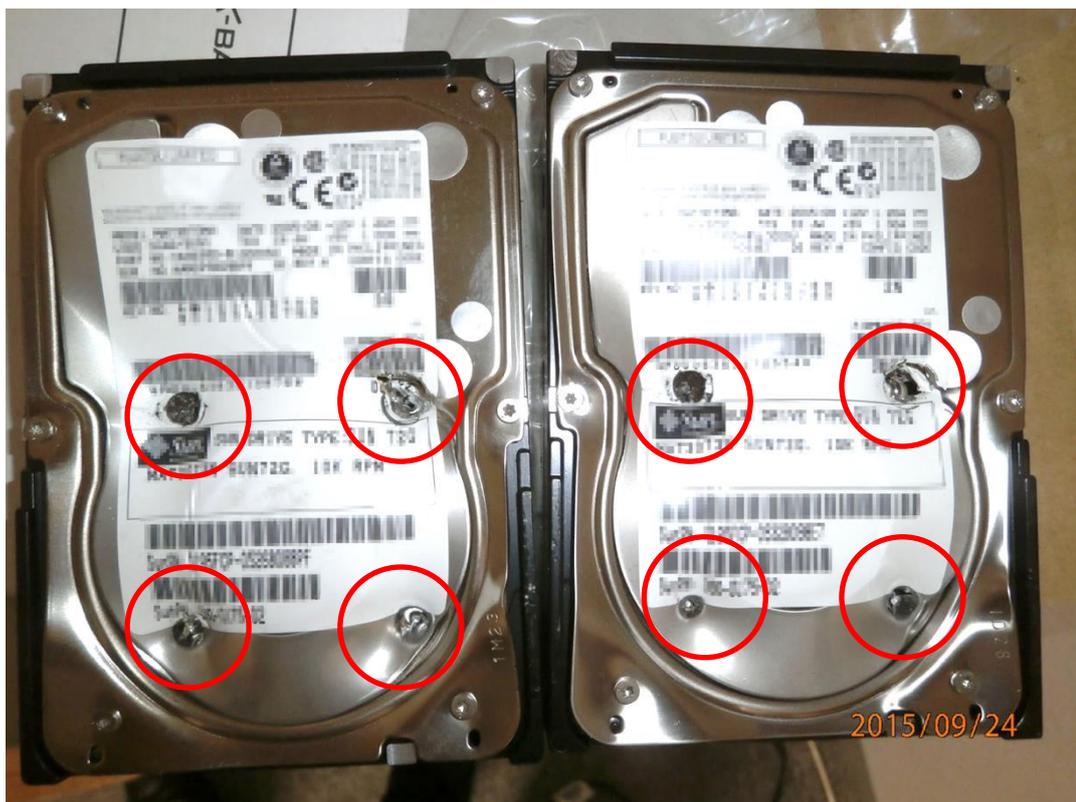
内容

- ・より詳しい1台1台の消去ログデータ
- OS、PCスペック、HDD名、消去回数等

破壊前



破壊後



<第一段階>

1. 従来はご要望に応じてハードディスクの物理破壊前と破壊後の写真撮影を行っていましたが、すべての物理破壊前と後の写真撮影実施を開始いたしました。
2. 作業時間帯の入退出時は、有人によるハンディ金属探知機での身体チェックと手荷物検査を東京本部テクニカルセンターから開始いたしました。準備が整い次第、警備員検査に移行いたします。

※他拠点テクニカルセンターも順次実行予定。



イメージ画像

<第二段階>

3. 入退出セキュリティゲート設置と警備員によるハンディ金属探知機での身体確認及び手荷物検査を実施いたします。



イメージ画像

4. セキュリティカメラを増設し管理体制を強化いたします。
5. 外部講師によるセキュリティ研修教育の頻度を増やし、定期的に実施いたします。