ウィルス感染事故　再発防止策

管理体制の強化	【セキュリティ監査員の配置】	**＊各拠点毎にセキュリティ監査員を配置し、抜き打ち監査及び作業員への教育活動を実施する。** ・ 監査員は既存セキュリティールールならびに再発防止策が徹底されているか常時注意を払う。 ・ 監査員は各拠点のセキュリティー状況を把握し月次で代表取締役へ報告する。 ・ 監査員は月1回の抜き打ち検査を行い、ルールが厳守されているかチェックし、代表取締役へ報告する。
リムーバブルメディアの管理・運用	【メディア台帳管理方法の変更】	**＊既存規定を厳格化し、管理項目を追加・記帳は日時更新とする。** A) 社内使用許可メディア（記録管理用/検査用）に対しラベリングを行う。 ・業務上使用する全メディアに対し管理ラベルを付け管理外メディアの使用を排除。 B) メディア台帳へ履歴を記録する。 ・使用者（持出者）、メディアの使用数量及びウィルスチェックの状況を記帳。
	【ウィルスチェック・フォーマットの管理】	**＊外部メディアに関する既存規定を厳格化し、不定期で行っていたウィルスチェックを毎日実施する。** ・各工程担当者が事務所棟セキュリティエリアに設置されたウィルスチェック専用端末にてウィルスチェック・フォーマットを行う。 ・セキュリティエリア内の定められた施錠可能保管場所に保管。 ・セキュリティ拠点管理者はウィルスチェック・フォーマット状況・個数差異の有無を確認後検印する。 毎日業務終了後に実施する。
検査手順	【デバイスチェックの順序変更】	**＊コンシューマ機リペア生産ラインにおける作業工程を見直す事で、外部メディアからの感染リスクを排除する。** 既存：動作確認 → データ消去 → リカバリー → デバイスチェック → 動作確認 → 再起動確認 新：動作確認 → デバイスチェック → データ消去 → リカバリー → 動作確認 → 再起動確認 ・検査棟生産ライン横にウィルスチェック専用端末を設置し、デバイスチェックで使用した検査用メディアは毎回ウィルスチェック・フォーマットを行い、使用回数とウィルスチェック回数を突合・検査台帳へ記録する。

平成22年6月24日
インバースネット株式会社