AMIYA

アクセスログ管理
監視ポイント集

ver.1.1

Copyright Amiya Corporation. All rights reserved.

目次

Copyright Amiya Corporation. All rights reserved.

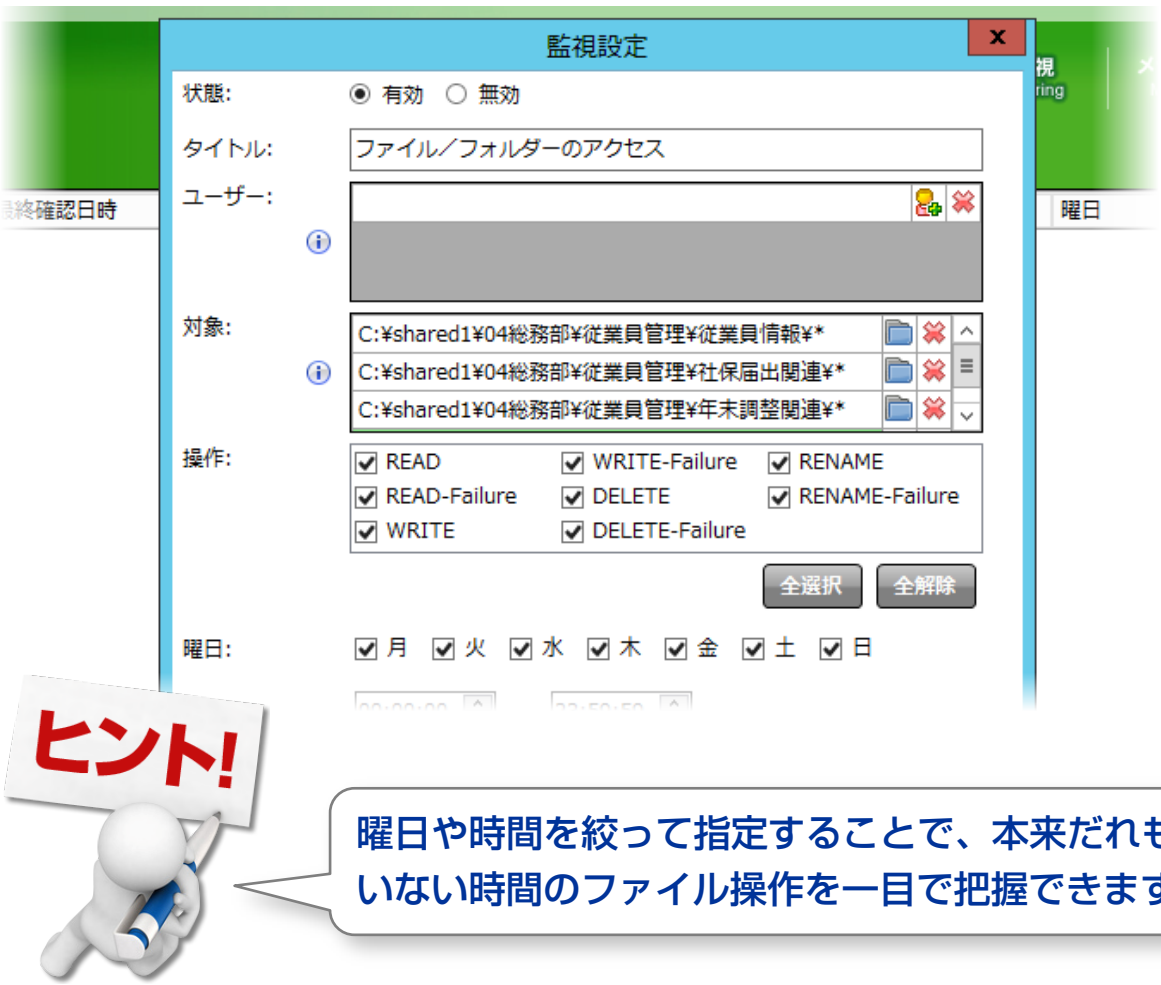
ファイル／フォルダーへのアクセス

監視ポイント

管理要件	重要情報に関連するファイル／フォルダーに対するすべてのアクセスを継続的に記録すること。
監視方法	重要情報に関連するファイル／フォルダーに対するアクセス履歴が保管されていることを確認する。
前提条件	重要情報に関連するファイル／フォルダーが識別できること。
監視対象	重要情報格納ファイルサーバ

設定方法（監視設定）

ユーザ	指定なし
対象	重要情報関連ファイルを格納したフォルダー名（フルパス）
操作	すべての操作
曜日	すべての曜日
時間帯	00:00:00　～　23:59:59



Copyright Amiya Corporation. All rights reserved.

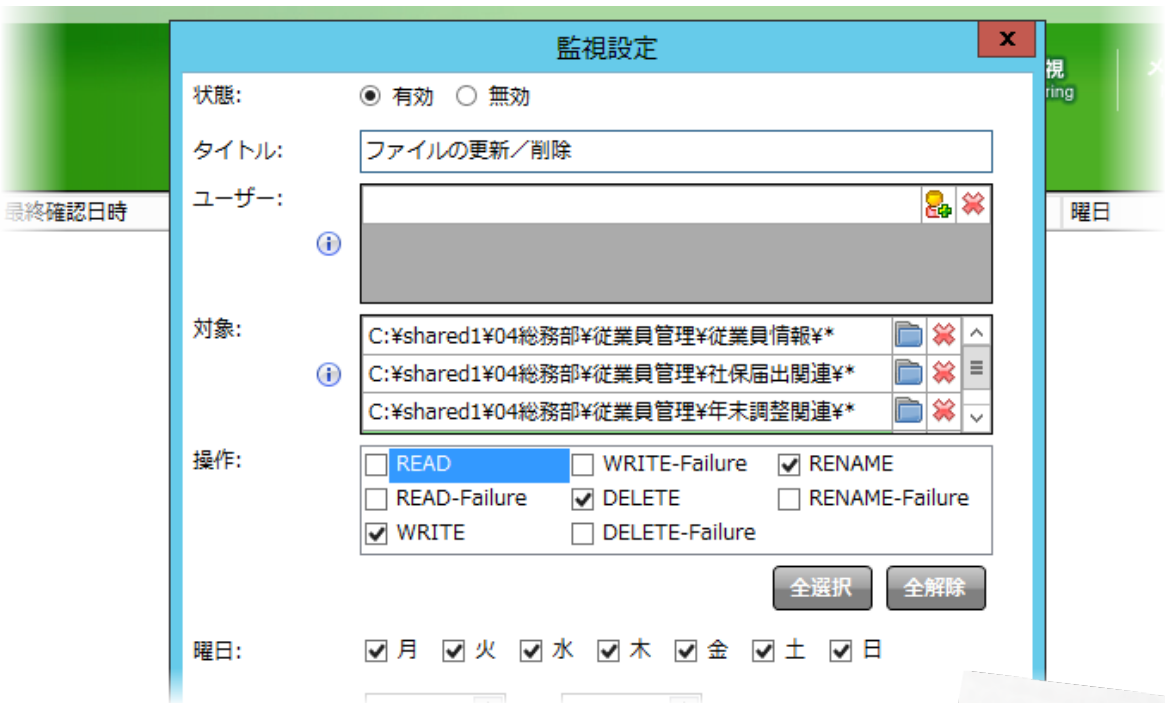
ファイルの更新／削除

監視ポイント

管理要件	定期的にアクセス記録の点検を行い、重要情報に関連するファイル／フォルダーに対する不正な更新及び削除の有無を確認すること。
監視方法	重要情報に関連するファイル／フォルダーに対する更新及び削除の記録を取得し、定期的に点検する。
前提条件	重要情報に関連するファイル／フォルダーが識別できること。
監視対象	重要情報格納ファイルサーバ

設定方法（監視設定）

ユーザ	指定なし
対象	重要情報関連ファイルを格納したフォルダー名（フルパス）
操作	WRITE・DELETE・RENAME
曜日	すべての曜日
時間帯	00:00:00　～　23:59:59



意図せず削除されたファイルやフォルダー名を指定することで、だれがいつ削除したかを特定できます。

Copyright Amiya Corporation. All rights reserved.

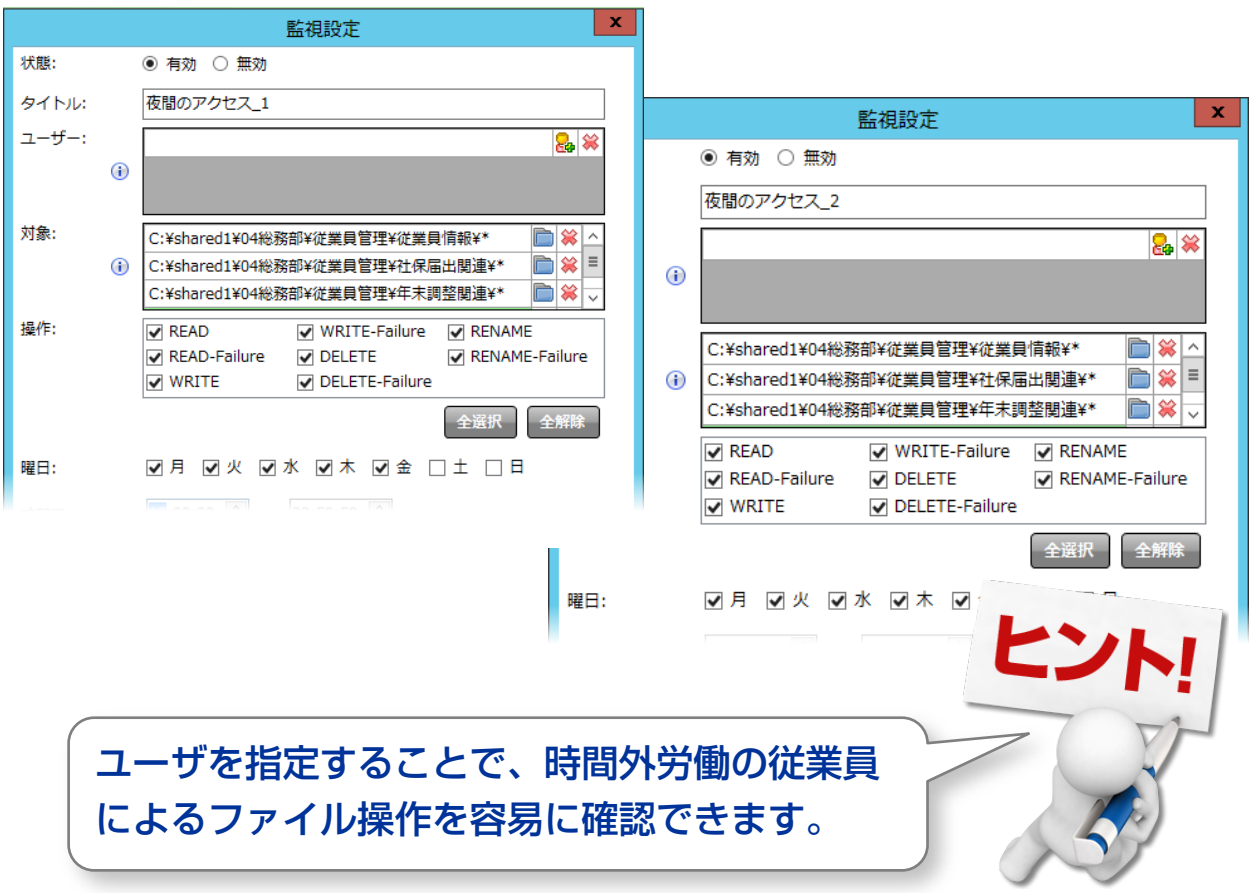
夜間のアクセス

監視ポイント

管理要件	定期的に夜間（定時外）におけるアクセス記録の点検を行い、不正アクセスの有無、異常アクセスの有無を確認すること。
監視方法	重要情報に関連するファイル／フォルダーに対する、夜間のアクセス記録を取得し、定期的に点検する。
前提条件	重要情報に関連するファイル／フォルダーが識別できること。
監視対象	重要情報格納サーバ（データベースは除く）

設定方法（監視設定）

ユーザ	指定なし
対象	重要情報関連ファイルを格納したフォルダー名（フルパス）
操作	すべての操作
曜日	営業日（例：月曜日～金曜日）
時間帯	業務時間外 （例：18:00:00　～　23:59:59/00:00:00　～　8:59:59） ※日を跨ぐ場合は、監視設定を2つに分ける必要があります



ユーザを指定することで、時間外労働の従業員によるファイル操作を容易に確認できます。

Copyright Amiya Corporation. All rights reserved.

土日のアクセス

監視ポイント

管理要件	定期的に土日におけるアクセス記録の点検を行い、不正アクセスの有無、異常アクセスの有無を確認すること。
監視方法	重要情報に関連するファイル／フォルダーに対する、土日のアクセス記録を取得し、定期的に点検する。
前提条件	重要情報に関連するファイル／フォルダーが識別できること。
監視対象	重要情報格納サーバ（データベースは除く）

設定方法（監視設定）

ユーザ	指定なし
対象	重要情報関連ファイルを格納したフォルダー名（フルパス）
操作	すべての操作
曜日	休日（例：土曜日・日曜日）
時間帯	00:00:00　～　23:59:59

Copyright Amiya Corporation. All rights reserved.

不正アクセス

監視ポイント

管理要件	権限を有しないユーザーのアクセス記録を点検し、不正なアクセスの有無を確認すること。
監視方法	権限を有しないユーザーによるファイル／フォルダーへのアクセスの記録を取得し、定期的に点検する。
前提条件	（なし）
監視対象	重要情報格納サーバ（データベースは除く）

設定方法（監視設定）

ユーザ	重要情報関連事務担当ユーザー以外
対象	重要情報関連ファイルを格納したフォルダー名（フルパス）
操作	READ・WRITE・DELETE・RENAME
曜日	すべての曜日
時間帯	00:00:00　～　23:59:59

重要情報にアクセスする必要のないユーザーがアクセスしていないか監視することで、不正をいちはやく検出することができます。

Copyright Amiya Corporation. All rights reserved.

退職予定者のアクセス状況

監視ポイント

管理要件	重要情報を取り扱う従業員の異動や退職、契約の変更または終了等の際、特定個人情報の不正使用が起こらないよう、当該ファイル／フォルダーへのアクセス状況を管理すること。
監視方法	重要情報を取り扱う従業員の異動や退職、契約の変更または終了にあたって、重要情報に関連するファイル／フォルダーへのアクセス状況を点検する。
前提条件	重要情報に関連するファイル／フォルダーが識別できること。
監視対象	重要情報格納サーバ（データベースは除く）

設定方法（監視設定）

ユーザ	退職予定のユーザーアカウント名
対象	重要情報関連ファイルを格納したフォルダー名（フルパス）
操作	すべての操作
曜日	すべての曜日
時間帯	00:00:00　～　23:59:59

退職予定者がどのようなファイル操作をしているか
監視することで、情報漏えいの予防に繋がります。

Copyright Amiya Corporation. All rights reserved.