

アクセスログ管理
監視ポイント集



1. ファイル／フォルダーへのアクセス

P.2

指定フォルダ配下のファイル及びフォルダーへのアクセス履歴を監視

2. ファイル／フォルダーの更新/削除

P.3

指定フォルダ配下のファイル及びフォルダーの更新・削除の履歴を監視

3. 夜間のアクセス

P.4

指定フォルダ配下のファイル及びフォルダーの、定時時間外のアクセス履歴を監視

4. 土日祝日のアクセス

P.5

指定フォルダ配下のファイル及びフォルダーの休日のアクセス履歴を監視

5. 不正アクセス

P.6

権限を有しないユーザーによる、指定フォルダ配下のファイル及びフォルダーのアクセス履歴を監視

6. 退職予定者のアクセス

P.7

退職予定者による、指定フォルダ配下のファイル及びフォルダーのアクセス履歴を監視

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



曜日や時間を絞って指定することで、本来だれもいない時間のファイル操作を一目で把握できます。

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、定期的な点検を行う。
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

監視設定

状態: 有効 無効

タイトル:

ユーザー:

対象:

- C:\\$shared1¥04総務部¥従業員管理¥従業員情報¥*
- C:\\$shared1¥04総務部¥従業員管理¥社保届出関連¥*
- C:\\$shared1¥04総務部¥従業員管理¥年末調整関連¥*

操作:

<input type="checkbox"/> READ	<input type="checkbox"/> WRITE-Failure	<input checked="" type="checkbox"/> RENAME
<input type="checkbox"/> READ-Failure	<input checked="" type="checkbox"/> DELETE	<input type="checkbox"/> RENAME-Failure
<input checked="" type="checkbox"/> WRITE	<input type="checkbox"/> DELETE-Failure	

曜日: 月 火 水 木 金 土 日

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。

ヒント!



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。

ヒント!



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

監視設定

状態: 有効 無効

タイトル: 土日のアクセス

ユーザー: [Empty]

対象:

- C:\\$shared1¥04総務部¥従業員管理¥従業員情報¥*
- C:\\$shared1¥04総務部¥従業員管理¥社保届出関連¥*
- C:\\$shared1¥04総務部¥従業員管理¥年末調整関連¥*

操作:

- READ
- WRITE
- RENAME
- READ-Failure
- DELETE
- RENAME-Failure
- WRITE
- DELETE-Failure

全選択 全解除

曜日: 月 火 水 木 金 土 日

時間帯: 00:00:00 ~ 23:59:59

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

監視設定

状態: 有効 無効

タイトル: 不正アクセス

ユーザー:

- ichiro_amiya_soumu
- taro_suzuki_jinji

対象:

- C:\\$shared1¥04総務部¥従業員管理¥従業員情報¥*
- C:\\$shared1¥04総務部¥従業員管理¥社保届出関連¥*
- C:\\$shared1¥04総務部¥従業員管理¥年末調整関連¥*

操作:

READ WRITE-Failure RENAME
 READ-Failure DELETE RENAME-Failure
 WRITE DELETE-Failure

全選択 全解除

曜日: 月 火 水 木 金 土 日

ヒント!



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、不正をいち早く検出することができます。

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

ヒント!

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。

