ALog V8 説明資料
～ ファイルアクセスログの変更点～

日付： 2021/02/24
会社名： 株式会社網屋
部署名： 技術本部

はじめに

ALog V8は、V7をベースにし、様々な機能拡張を行っております。
本資料ではV7とV8において異なる点をメインに解説します。
本資料の他に以下の資料も必要に応じてご確認ください。

① バージョンアップガイド	…サポートサイトに掲載
② インストールガイド	…製品に同梱
③ ユーザーズガイド	…製品に同梱
④ ユーザーズガイド(EVA)	…製品に同梱
⑤ リスクスコアリング ユーザーズガイド	…製品に同梱
⑥ WorkTime ユーザーズガイド	…製品に同梱

はじめに

- V7からV8へのバージョンアップは、「setup.exeを実行して上書きインストール」となります。V7のマイナーアップデート時の手順と同様です。
  - アーキテクチャに変更はありませんので大きな構築しなおしは発生しません。
  - 引き続き、ALog V8をインストールすることで、ALogの各製品すべてを管理することができます。
    (for Windows/for NetApp/for EMC/for Isilon/for SQL Server/for Oracle/for Linux/ALog EVA/管理機能/検索機能)
  - 詳細は、バージョンアップガイドを参照してください。

- Webコンソールに大きな変更点はありません。
  - 管理画面のページはメニュー項目の増加に伴い、メニューの順番変更や再構成を行ないました。

- V6からV8へは直接移行できません。一度V7へ移行してからV8へバージョンアップしていただくか、V8を新規で構築していただく必要があります。

- 特別なオプションを使用しているお客様は、サポートへお問い合わせください。
- 本書ではIsilonと表記していますが、製品上はV8.1.5よりPowerScaleとなっています。ご了承ください。

目次

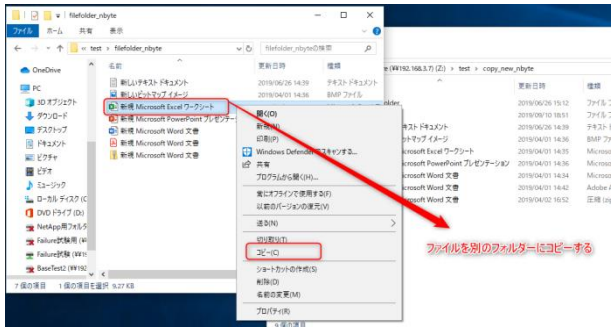
ファイルアクセスは下記の内容についてそれぞれ説明します。

1-1. V7とV8でアクセスログの出方が変わる理由 （1/3）

【対象：ファイルアクセスログ全般】

・なぜV8でアクセスログの出方が変わるの？
☞ イベントログの解析が進み、よりユーザー操作に近いアクセスログを出力できるよう精度の向上を図りました。

<解説>
V7までのイベントログの変換では、ユーザーの操作を区別しづらいケースがありました。
例えば、エクスプローラー上でファイルをコピーした時、コピー先に「WRITE」が出力されるが、コピー元では「READ」しか出力されないため、上書き保存したのか、それともコピーされたのか区別がつきにくい、といったことが一例として挙げられます。



1-1. V7とV8でアクセスログの出方が変わる理由 （2/3）

V7では、コピー元のファイルを選択したので「READ」が出力され、コピーした時に「WRITE」が出力されますが、それだけでは「保存した結果WRITEが出力された」場合と区別し辛い状況でした。

「filefolder」フォルダーのExcelファイルを「copy_new_nbyte」フォルダーへコピーした時のアクセスログ

◆V7のアクセスログ(対象、操作、詳細のみ抜粋)

"C:¥test¥filefolder¥新規 Microsoft Excel ワークシート.xlsx","READ","Count:1"
"C:¥test¥copy_new_nbyte¥新規 Microsoft Excel ワークシート.xlsx","WRITE","Count:1"

① この2行だけを見ても、「filefolder」フォルダー配下のExcelファイルを開いて（閲覧して）
② 「copy_new_nbyte」フォルダー配下のExcelファイルを保存した
だけのように見えるので、関連性があるとは読み解きにくい

1-1. V7とV8でアクセスログの出方が変わる理由 （3/3）

V8ではコピー元のファイルで操作欄に「COPY」と出力し、詳細項目に「To」でコピー先のパスを出力することにより、関連性をわかりやすくしました。

「filefolder」フォルダーのExcelファイルを「copy_new_nbyte」フォルダーへコピーした時のアクセスログ

◆V7のアクセスログ(対象、操作、詳細のみ抜粋)

"C:¥test¥filefolder¥新規 Microsoft Excel ワークシート.xlsx","READ","Count:1"
"C:¥test¥copy_new_nbyte¥新規 Microsoft Excel ワークシート.xlsx","WRITE","Count:1"

◆V8のアクセスログ(対象、操作、詳細のみ抜粋)

“C:¥test¥filefolder¥新規 Microsoft Excel ワークシート.xlsx”,“**COPY**”,“Count:1
To:C:¥test¥**copy_new_nbyte**¥新規 Microsoft Excel ワークシート.xlsx“
"C:¥test¥**copy_new_nbyte**¥新規 Microsoft Excel ワークシート.xlsx","WRITE","Count:1"

**「COPY」の場合は詳細項目に「To」が出力される。
コピー先のフォルダー名が入るため、その後出力される「WRITE」のアクセスログの対象欄と見比べやすくなっている。**

**条件に合った場合に「COPY」と出力。
ただし、条件に合わない場合はこれまでのV7と同じように出力される。**

1-2. 出力されなくなるログはあるか （1/3）

【対象：ファイルアクセスログ全般】

・出力されなくなってしまうアクセスログはあるか？

☞ **ユーザーが実際には操作していないような一部の余計なアクセスログの出力を抑えられるようになりました。**

<解説>

例えばエクスプローラーの操作において、ファイルやフォルダーを右クリックして
コンテキストメニュー内の操作(コピー、切り取りなど)を行った際にも、READの元となる
イベントログが出力され、V7ではそのイベントログを翻訳してREADと出力していました。

V8ではイベントログの読み方を変えたことにより、上記のような余計な操作の読み込みを
抑えられ、より正確なアクセスログになりました。

1-2. 出力されなくなるログはあるか （2/3）

ファイルを右クリックしてコンテキストメニューから貼り付けでファイルを移動した場合に、
コンテキストメニュー表示中もREADの元となるイベントログが出力されることにより、
単純な操作しかしていないのに、大量のアクセスログが出力されるように見えました。

「filefolder」のフォルダーからExcelファイルを「move_overwrite_nbyte」フォルダーへ上書き移動した時のアクセスログ

◆V7のアクセスログ(時刻、対象、操作、詳細のみ抜粋)

"2019/03/25 16:58:57.647","C:¥test¥filefolder¥新規 Microsoft Excel ワークシート.xlsx","READ","Count:1“
"2019/03/25 16:58:57.823","C:¥test¥filefolder¥新規 Microsoft Excel ワークシート.xlsx","READ","Count:1“
“2019/03/25 16:58:57.827","C:¥test¥filefolder¥新規 Microsoft Excel ワークシート.xlsx","DELETE","Count:1“
"2019/03/25 16:58:57.884","C:¥test¥move_overwrite_nbyte¥新規 Microsoft Excel ワークシート.xlsx","READ","Count:1“
"2019/03/25 16:59:06.755","C:¥test¥filefolder¥新規 Microsoft Excel ワークシート.xlsx","RENAME","Count:1“
"2019/03/25 16:59:06.760","C:¥test¥move_overwrite_nbyte¥新規 Microsoft Excel ワークシート.xlsx","READ","Count:1"

ファイルを右クリックしてコンテキストメニューを表示して「貼り付け」操作をしただけで、その分イベントログが出力され、アクセスログに変換されるので読み解きづらく感じる。

1-2. 出力されなくなるログはあるか （3/3）

V8ではイベントログの読み方が変わったことにより、一部の余計なログの出力を削減しています。

※注意※　全てにおいて**「余計なログが減らせる」ということではありません。**
OSがファイルやフォルダのアクセスした形跡が記録されたイベントログを翻訳対象としてきちんと読まないと、
逆に「操作したはずなのにアクセスログにならない」ということが起こってしまうからです！
V8ではイベントログの読み方を変えたことで、これまでより正確に「実際に動作が起こった箇所」をピックアップできるよう、
精度の向上を図った結果、**一部の**余計なログを出力しないようになりました。

「filefolder」のフォルダーからExcelファイルを「move_overwrite_nbyte」フォルダーへ上書き移動した時のアクセスログ

◆V7のアクセスログ(時刻、対象、操作、詳細のみ抜粋)

"2019/03/25 16:58:57.647","C:¥test¥filefolder¥新規 Microsoft Excel ワークシート.xlsx","READ","Count:1“
"2019/03/25 16:58:57.823","C:¥test¥filefolder¥新規 Microsoft Excel ワークシート.xlsx","READ","Count:1“
"2019/03/25 16:58:57.827","C:¥test¥filefolder¥新規 Microsoft Excel ワークシート.xlsx","DELETE","Count:1“
"2019/03/25 16:58:57.884","C:¥test¥move_overwrite_nbyte¥新規 Microsoft Excel ワークシート.xlsx","READ","Count:1“
"2019/03/25 16:59:06.755","C:¥test¥filefolder¥新規 Microsoft Excel ワークシート.xlsx","RENAME","Count:1“
"2019/03/25 16:59:06.760","C:¥test¥move_overwrite_nbyte¥新規 Microsoft Excel ワークシート.xlsx","READ","Count:1"

◆V8のアクセスログ(時刻、対象、操作、詳細のみ抜粋)

"2019/03/25 16:58:57.884","C:¥test¥move_overwrite_nbyte¥新規 Microsoft Excel ワークシート.xlsx","READ","Count:1"
“2019/03/25 16:59:06.755”,“C:¥test¥filefolder¥新規 Microsoft Excel ワークシート.xlsx”,“**MOVE**”,“Count:1
To:C:¥test¥move_overwrite_nbyte¥新規 Microsoft Excel ワークシート.xlsx“
"2019/03/25 16:59:06.760","C:¥test¥move_overwrite_nbyte¥新規 Microsoft Excel ワークシート.xlsx","WRITE","Count:1"

新ロジックでは、「実際に動作が起こった箇所」をより高い精度で抽出できるようにした結果、アクセスログが読みやすくなった。

1-3. 「COPY」「MOVE」の製品別出力情報

【対象：ファイルアクセスログ全般】

・「COPY」と「MOVE」はどの製品でも出力できるんですよね？
☞ いいえ、「COPY」はWindowsのみです。
「MOVE」はWindows、NetApp、Isilonのみです。

◆COPYとMOVEの製品別対比表

製品	COPY	MOVE
Windows	○	○
NetApp	×	○
Isilon	×	○
EMC	×	×
その他	×	×

1-4. COPYが出力される条件 （1/3）

【対象：for Windows】

・COPYは別ドライブや別サーバにコピーしても出ますよね？
☞ 別サーバにコピーした場合は出力されません。同じサーバでは別ドライブも含め出力できます。

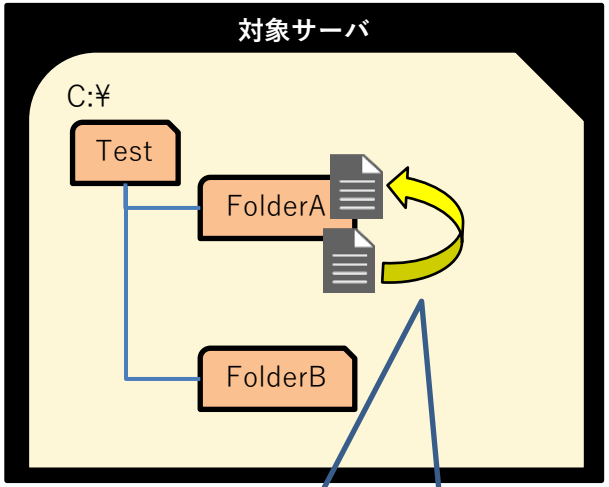
<解説>
「COPY」となる条件は、
☞ 「同サーバ」内のコピー操作のみ
☞コピー元とコピー先が、同じフォルダー＋異なるファイル名＋同じ拡張子（※1）
☞コピー元とコピー先が、違うフォルダー＋同じファイル名＋同じ拡張子(※2)

（※1）コピー元とコピー先が、同じフォルダー＋異なるファイル名＋同じ拡張子
“C:¥FolderA¥**Text.txt**”,“COPY”,“Count:1 To:C:¥FolderA¥**Text - コピー.txt**”
“C:¥FolderA¥**Text - コピー.txt**",“WRITE",“Count:1”

（※2）コピー元とコピー先が、違うフォルダー＋同じファイル名＋同じ拡張子
・同ドライブ内のコピー例
“C:¥FolderA¥**Text.txt**",“COPY",“Count:1 To:C:¥FolderB¥**Text.txt**”
“C:¥FolderB¥**Text.txt**”,“WRITE”,“Count:1”
・別ドライブでのコピー例
“C:¥FolderA¥**Text.txt**",“COPY",“Count:1 To:D:¥FolderB¥**Text.txt**”
“D:¥FolderB¥**Text.txt**",“WRITE",“Count:1”

1-4. COPYが出力される条件 （2/3）

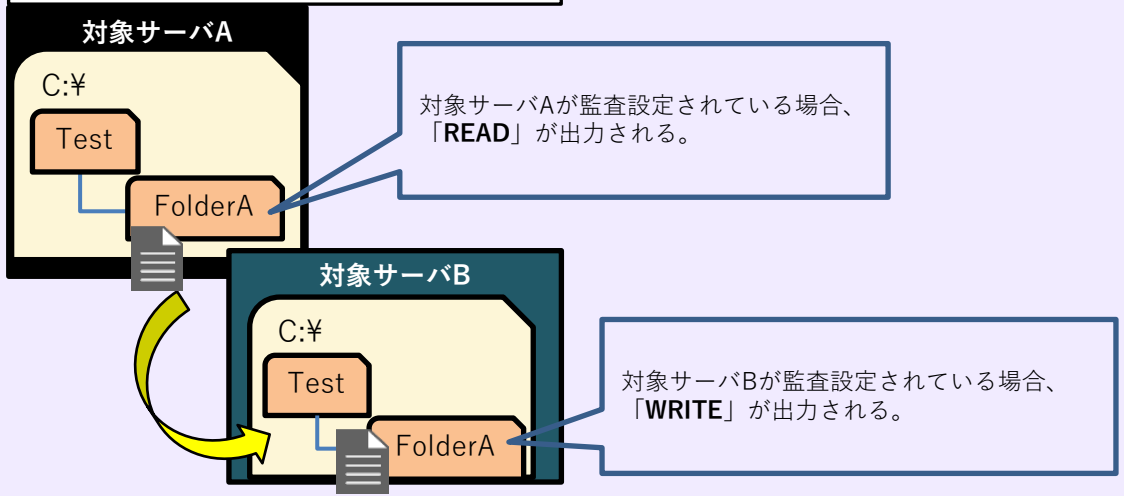
COPYが出るケース：コピー元とコピー先が、同じフォルダー＋異なるファイル名＋同じ拡張子
“C:¥FolderA¥**Text.txt**”,“COPY”,“Count:1 To:C:¥FolderA¥**Text - コピー.txt**”
“C:¥FolderA¥**Text - コピー.txt**",“WRITE",“Count:1”



ファイルを選択してコピーし、同じフォルダーで貼り付け操作した場合
(Ctrl＋C⇒Ctrl＋Vでファイルを複製するようなよくやる操作)

このような操作ではCOPYは出ません！！！！

出ないケース：
別サーバのフォルダーにコピー

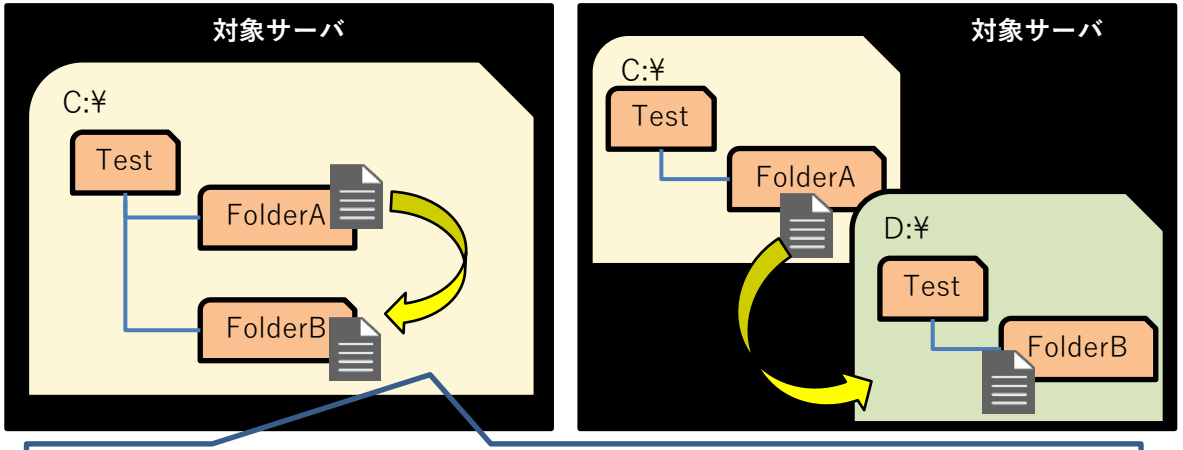


1-4. COPYが出力される条件 （3/3）

COPYが出るケース：コピー元とコピー先が、違うフォルダー＋同じファイル名＋同じ拡張子

“C:¥**FolderA**¥**Text.txt**",“COPY",“Count:1 To:C:¥**FolderB**¥**Text.txt**”
“C:¥**FolderB**¥**Text.txt**”,“WRITE”,“Count:1”

“C:¥**FolderA**¥**Text.txt**",“COPY",“Count:1 To:D:¥**FolderB**¥**Text.txt**”
“D:¥**FolderB**¥**Text.txt**”,“WRITE”,“Count:1”



同じドライブ内または別ドライブにおいて、下記2パターンの操作が該当する。
●新規で違うフォルダーにコピーする。
●コピー先に同じファイル名（同じフォルダー名）が存在していて、上書きする場合。

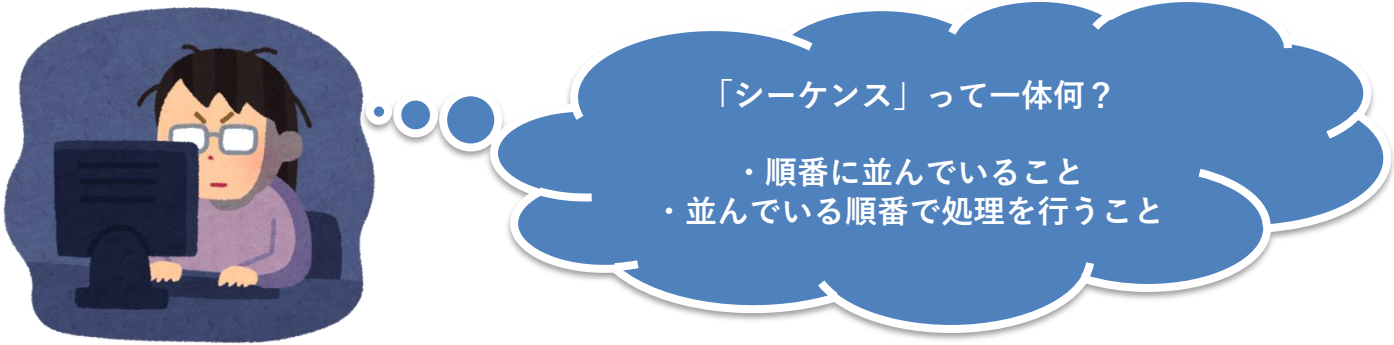
1-5. Windows以外で「COPY」を出さない理由

【対象：for Windows / NetApp / Isilon / EMC】

・WindowsみたいにCOPYは出せないの？
☞ COPYと確実に読み取れる監査イベントが存在しない為、COPYは出さない仕様としています。

<解説>
・Windows：イベントログのシーケンスに終わりがある特徴を捉え、イベントログ内の並行した2つのシーケンスの関連性を見て、関連性がある場合に「COPY」とすることが可能。

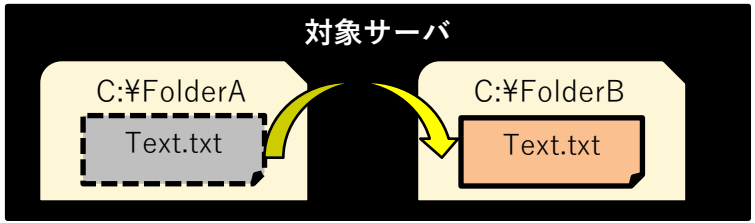
・NetApp/Isilon/EMC：NAS系はシーケンスに終わりがない。
並行したシーケンスが追えなければ、「COPY」としての判別が困難。



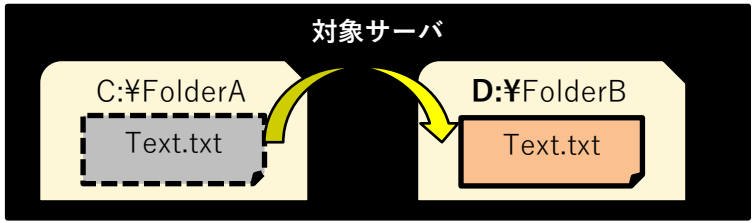
1-6. 「MOVE」は必ずしも出力されない （1/2）

【対象：for Windows / NetApp / Isilon】

・ファイル/フォルダーを移動した場合は必ずMOVEが出力されるの？
☞ Windows、NetApp、Isilonとも、必ずMOVEが出るとは限りません。以下に例を記載します。



◆V8のアクセスログ(対象、操作、詳細のみ抜粋)
“C:¥FolderA¥Text.txt",“**MOVE**",“Count:1 To:C:¥FolderB¥Text.txt”
“C:¥FolderB¥Text.txt",“WRITE",“Count:1”



◆V8のアクセスログ(対象、操作、詳細のみ抜粋)
“C:¥FolderA¥Text.txt",“**DELETE**",“Count:1”

<解説>
・同ドライブのフォルダー間の移動では、MOVEと出力される。(※Windowsは出ない場合あり。詳細は後述)
・別ドライブのフォルダーへの移動では、移動元ドライブのフォルダーのDELETEが出力される。
・クライアントマシンへの移動では、移動元ドライブのフォルダーのDELETEが出力される。(※詳細は後述)

1-6. 「MOVE」は必ずしも出力されない （2/2）

Windowsはファイル/フォルダーを移動した場合、MOVEではなくRENAMEになる場合もあります。

<解説>

☞**WindowsにはNetAppやIsilonのような「明確なRENAME」のイベントログが存在しません。**
Windowsの場合、「RENAMEとなり得る」イベントログの並びを更に解析して「MOVE」と出力しています。よって、MOVEであると十分な判別が**できない場合は「RENAME」**となります。

<補足>

共通点は、「RENAMEとなるログ」を使ってMOVEと出力するようにしている点です。
つまり、「明確なRENAME」のイベントログさえあれば、「MOVE」になります。

1-7. RENAMEやMOVE後のパスがWRITEにならないケースがある理由（1/3）

【対象：for Windows】

・なぜWindowsはRENAMEやMOVE先のパスがWRITEにならない場合があるの？
☞ Windowsの場合、書き込み先の情報がイベントログから特定することが非常に困難な場合があります。
①RENAME後の書き込み先パスがイベントログに出力されていない場合がある
②RENAME後の書き込み先パスがイベントログに出力されていても、特定できない場合がある

<解説>
Windows製品に上記の特徴があるため、V7のアクセスログでも移動操作で書き込み先のパスが特定できずに出力できないケースがありました。

V8でも同様ですが、更にイベントログの解析を進め、RENAME(MOVE)後の書き込み先パスがイベントログに**出力されていて、その関連性が判別できる場合に限り**、書き込み先を特定して出力するようにしています。

1-7. RENAMEやMOVE後のパスがWRITEにならないケースがある理由 （2/3）

V8では、以下のようにRENAME(MOVE)のアクセスログを出力しています。

①移動後のパスがイベントログの並びを見ても確定できない場合

RENAME/MOVE(移動元)⇒READ(移動先)

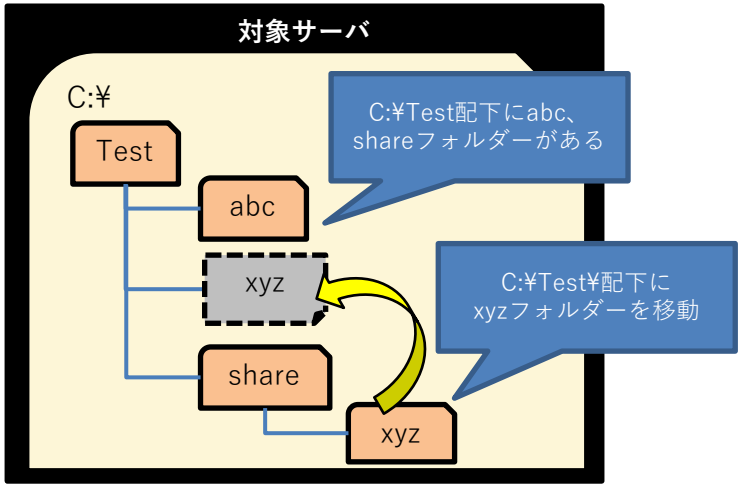
②移動後のパスがイベントログの並びを見て確定できる場合

RENAME/MOVE(移動元)⇒WRITE(移動先)

③移動後のパスがイベントログに記録されない等の理由で確定できない場合

RENAME（移動元）⇒出力なし(移動先)

①移動後のパスがイベントログの並びを見ても確定できない場合



◆V7のアクセスログ(対象、操作、詳細のみ抜粋)

“C:¥Test¥share¥xyz”,“RENAME”,“Count:1“

“C:¥Test¥**abc**”,“READ”,“Count:1“

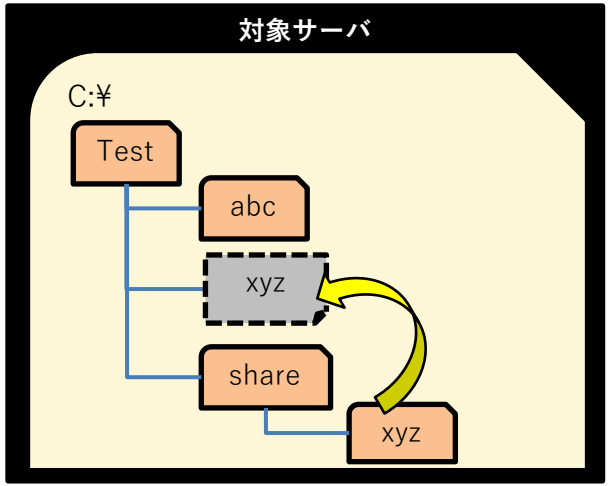
◆V8のアクセスログ(対象、操作、詳細のみ抜粋)

“C:¥Test¥share¥xyz”,“MOVE”,“Count:1 To:C:¥Test¥xyz“

“C:¥Test¥xyz“,“READ“, “Count:1“

V7では、イベントログを見ても移動後のパスが確定できない場合、
別のパスが出力されることがあった。
V8では、イベントログ内の書き込み先を特定する精度を向上させ、
書き込み先をより正しく特定。

1-7. RENAMEやMOVE後のパスがWRITEにならないケースがある理由 （3/3）



②移動後のパスがイベントログの並びを見て確定できる場合

◆V7のアクセスログ（対象、操作、詳細のみ抜粋）
“C:¥Test¥share¥xyz”,“RENAME”,“Count:1“
“C:¥Test¥xyz”,“**READ**”,“Count:1“

◆V8のアクセスログ（対象、操作、詳細のみ抜粋）
“C:¥Test¥share¥xyz”,“MOVE”,“Count:1 To:C:¥Test¥xyz“
“C:¥Test¥xyz“,“**WRITE**“, “Count:1“

書き込み先が断定できる場合、
移動先のパスを「READ」ではなく、
「WRITE」と出力。

③移動後のパスがイベントログに記録されない等の理由で確定できない場合

移動先のパスが特定できないので、RENAME後の
移動先パスの出力はできない。
V7でも同じであり、このケースではV7とV8に
違いはない。

◆V7のアクセスログ（対象、操作、詳細のみ抜粋）
“C:¥Test¥share¥xyz”,“RENAME”,“Count:1“
（出力なし）

◆V8のアクセスログ（対象、操作、詳細のみ抜粋）
“C:¥Test¥share¥xyz”,“RENAME”,“Count:1“
（出力なし）

1-8. 詳細フィールドの「To」について

【対象：for Windows / NetApp / Isilon】

・詳細フィールドで「To」と出す操作にはどのようなものがあるの？
また、どの製品で出るの？
☞ V7ではNetAppのみ「RENAME」操作で「RenameTo」に書き込み先を出力していましたが、V8ではWindows、NetApp、Isilonの製品において「COPY」「MOVE」「RENAME」で「To」に書き込み先を出力できるようになりました！

「新規 Microsoft Excel ワークシート.xlsx」のファイル名を「R新規 Microsoft Excel ワークシート.xlsx」に名前変更時のアクセスログ

◆V7のアクセスログ(対象、操作、詳細のみ抜粋)
"C:¥test¥rename¥新規 Microsoft Excel ワークシート.xlsx","RENAME","Count:1“
"C:¥test¥rename¥R新規 Microsoft Excel ワークシート.xlsx","READ","Count:1"

◆V8のアクセスログ(対象、操作、詳細のみ抜粋)
“C:¥test¥rename¥新規 Microsoft Excel ワークシート.xlsx”,“RENAME”,“Count:1
To:C:¥test¥rename¥R新規 Microsoft Excel ワークシート.xlsx“
"C:¥test¥rename¥R新規 Microsoft Excel ワークシート.xlsx","WRITE","Count:1"

V7では書き込み先がないため、前後のログで何をしたのかわかりにくい面がありました。

Windowsでも書き込み先が明確になったので、前後のログで何をしたかがわかりやすくなりました。

1-9. 詳細フィールドに「Zone」「Protocol」が追加

【対象：for Isilon】

・その他に詳細フィールドがV7と変わっていますか？

☞ **V8ではIsilonの製品において詳細フィールドに「Zone」「Protocol」を出力できるようになりました。**
Zone：ドメイン毎にアクセス制御を行う時などに使用される単位。アクセスゾーン。
Protocol：ファイル操作時のプロトコル。NFSの場合に限り「Protocol:NFS」と出力される。

zone2上でLinux端末（NFS）から「新規テキストドキュメント.txt」を読み込んだ時のアクセスログ

◆V7のアクセスログ(対象、操作、詳細のみ抜粋)
“¥¥ifs¥zone2¥share¥新規テキストドキュメント.txt",“READ",“Count:1“Z

◆V8のアクセスログ(対象、操作、詳細のみ抜粋)
“¥¥ifs¥zone2¥share¥新規テキストドキュメント.txt",“READ",“Count:1 **Protocol:NFS Zone:zone2**“

Protocol、Zoneの概念が無い為、どちらのアクセスかが
わからなくなっていました。

V8ではどのZoneから、どのプロトコルからという情報が詳細
フィールドに出力されるようになり、経路等が明確になりました。
※変換エンジンはCIFS領域を想定しており、NFS領域は変換
精度の保証ができません。

1-10. テンポラリファイルの除外について

【対象：for Windows / NetApp / Isilon】

・Officeテンポラリファイルの余計なログは出てくるの？

☞ **V7ではOffice操作時におけるテンポラリファイル「.tmp」もアクセスログに出力されていました。**
V8では上記のようなテンポラリファイルのアクセスログを除外する事ができるようになりました。

「新規 Microsoft Excel ワークシート.xlsx」を編集後、上書き保存した時のアクセスログ
（下記はfor Isilonのアクセスログ）

◆V7のアクセスログ(対象、操作、詳細のみ抜粋)

“¥¥ifs¥share¥新規 Microsoft Excel ワークシート.xlsx",“WRITE",“Count:1“
“¥¥ifs¥share¥EF3116A7.tmp",“WRITE",“Count:1“
“¥¥ifs¥share¥75CF7DBE.tmp",“RENAME",“Count:1“

◆V8のアクセスログ(対象、操作、詳細のみ抜粋)

“¥¥ifs¥share¥新規 Microsoft Excel ワークシート.xlsx",“WRITE",“Count:1“

V7ではOfficeファイルの操作における、テンポラリファイルのアクセスログが出力されため、フィルターを設定してもらい除外していました。

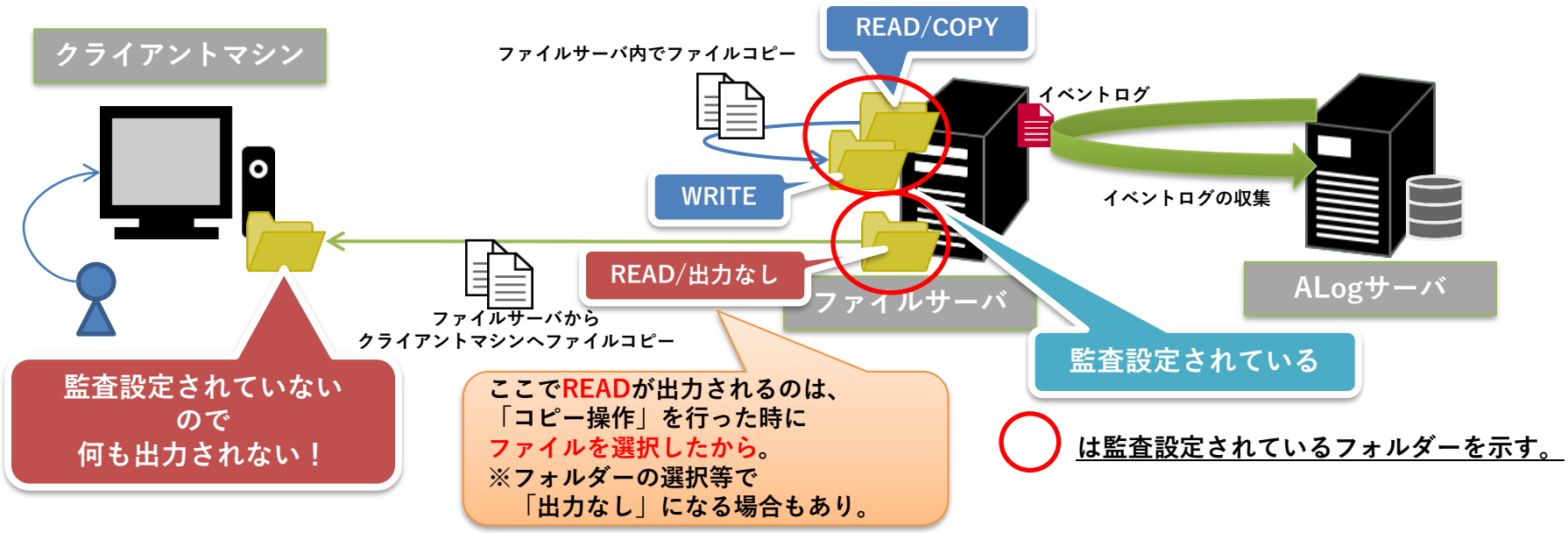
V8ではテンポラリのアクセスログを除外する事ができ、よりユーザー操作に近いアクセスログが出力できるようになりました。

1-11. ファイルサーバからクライアントマシンにコピー操作した時のアクセスログ （1/2）

【対象：ファイルアクセスログ全般】

・クライアントマシンにコピーしたときアクセスログは出ますか？
☞ クライアントマシンは監査設定されていないので出ません。（バージョンに関係なく）

＜図解＞



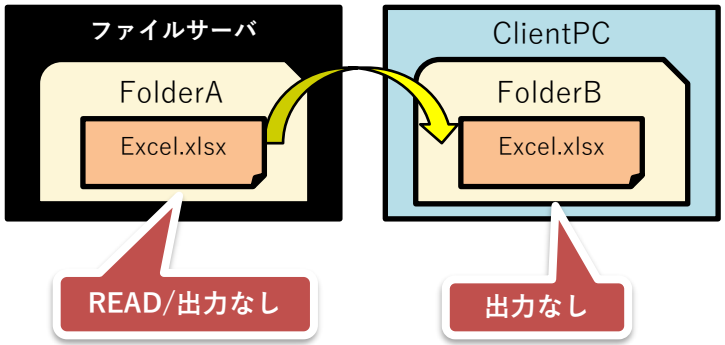
1-11. ファイルサーバからクライアントマシンにコピー操作した時のアクセスログ　(2/2)

◆ファイルサーバからクライアントマシンにファイルをコピーした時のアクセスログ例

「新規 Microsoft Excel ワークシート.xlsx」をファイルサーバからクライアントマシンへコピーする。

◆V7のアクセスログ(対象、操作、詳細のみ抜粋)
"C:¥test¥copy_nbyte¥新規 Microsoft Excel ワークシート.xlsx","READ","Count:1"

◆V8のアクセスログ(対象、操作、詳細のみ抜粋)
"C:¥test¥copy_nbyte¥新規 Microsoft Excel ワークシート.xlsx","READ","Count:1"



上記のREADはファイルサーバでエクスプローラーからコピー操作を行った時に読み込まれたファイルのREAD。

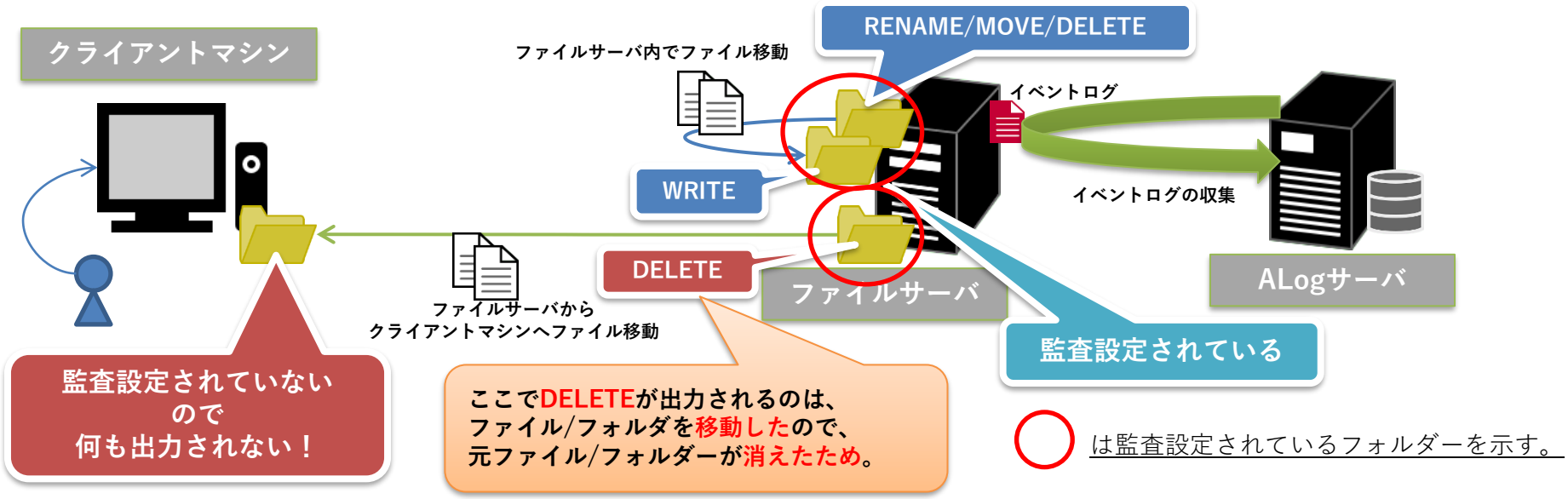
V7、V8などバージョンに依存することなく、仕組み上、クライアントマシン(操作する元)は監査設定されていないため、クライアントマシンへ書き込みされても、当然、アクセスログは何も出力されない。

1-12. ファイルサーバからクライアントマシンに移動操作した時のアクセスログ（1/2）

【対象：ファイルアクセスログ全般】

・クライアントマシンに移動したときアクセスログは出ますか？
☞ クライアントマシンは監査設定されていないので出ません。（バージョンに関係なく）

＜図解＞



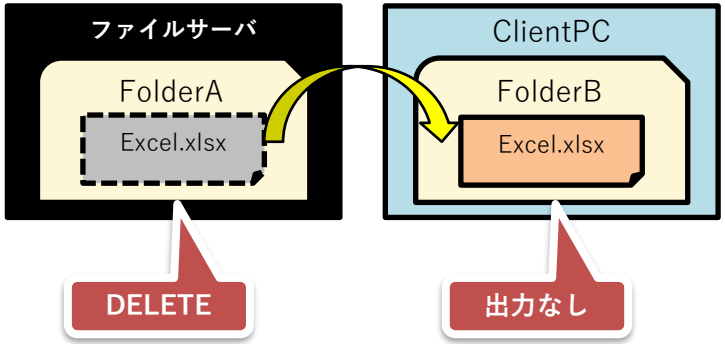
1-12. ファイルサーバからクライアントマシンに移動操作した時のアクセスログ （2/2）

◆ファイルサーバからクライアントマシンにファイルを移動した時のアクセスログ例

「新規 Microsoft Excel ワークシート.xlsx」をファイルサーバからクライアントマシンへ移動する。

◆V7のアクセスログ(対象、操作、詳細のみ抜粋)
"C:¥test¥move_nbyte¥新規 Microsoft Excel ワークシート.xlsx",“DELETE","Count:1"

◆V8のアクセスログ(対象、操作、詳細のみ抜粋)
"C:¥test¥move_nbyte¥新規 Microsoft Excel ワークシート.xlsx",“DELETE","Count:1"



上記のDELETEはエクスプローラーでファイルサーバから
クライアントマシンへ移動操作を行った時に、ファイルサーバ上から
削除された元データのDELETE。

V7、V8などバージョンに依存することなく、仕組み上、
クライアントマシン(操作する元)は監査設定されていないため、
クライアントマシンへ書き込みされても、当然アクセスログは
何も出力されない。

1-13. コンピュータアカウントの除外について

【対象：for Windows / NetApp / Isilon / EMC】

・コンピュータアカウントってどうなったの？

☞ **Isilonでは、V7でコンピュータアカウント（XXX$）のようなシステム側の操作によるアクセスログを出力していました。**
しかし、ユーザー操作のアクセスログではない為、 V8ではIsilonでも除外する事にしました。
※Windows、NetApp、EMCでは以前のバージョンから除外されています。

◆V7のアクセスログ(ユーザー、対象、操作、詳細のみ抜粋)

“DomainA¥UserA”,“¥¥ifs¥share¥新規 Microsoft Word 文書.docx",“WRITE",“Count:1“
“**DomainA¥ComputerA$**”,“¥¥ifs¥share¥新規 Microsoft Word 文書.docx",“READ-Failure",“Count:1“

◆V8のアクセスログ(ユーザー、対象、操作、詳細のみ抜粋)

“DomainA¥UserA”,“¥¥ifs¥share¥新規 Microsoft Word 文書.docx",“WRITE",“Count:1“

製品	V7	V8
Windows	除外	除外
NetApp	除外	除外
Isilon	**出力**	**除外**
EMC	除外	除外

V7ではコンピュータアカウントのアクセスログはフィルター等で除外設定をしてもらっていましたが、
V8ではデフォルトでコンピュータアカウントのアクセスログを除外しました。
※config設定により出力する事は可能。

2. ログオンログの変更点

・AD連携の機能によってログオンのユーザー名は今までと変わってしまうのですか？

☞ **変わるケース、変わらないケースがあります。**
お客様環境(ADのNetBIOS名)、認証の状況によって全く違いますので、
詳しくはお問い合わせください。

ドメイン名が「ABC.co.jp」、NetBIOS名が「ABC」のような環境においては、V7と変わりがないと思われますが、
ドメイン名が「ABC.co.jp」、NetBIOS名が「XYZ」や「XYZ.AD.COM」のように、ドメイン名とNetBIOS名が
異なるような環境の場合、操作によってはユーザー名が変わります。