AMIYA

ALog

監査レポート集

ALog ConVerter®

ALog ConVerter® DB

Resource Athlete®

ver.3.6

目次

1．アカウント管理

RA	グループアカウントとグループ構成の一覧	P.2
RA	長期未ログオンのアカウント	P.3
RA	一定日数以上パスワード未変更のアカウント	P.4
RA	管理者アカウント	P.5
ACV	ユーザーアカウントの追加／削除	P.6
DB	データベースユーザーへの特権付与	P.7

2．アクセス権管理

RA	全フォルダのアクセス権	P.8
RA	全フォルダのアクセス権（前回との差分）	P.9
ACV	ファイル／フォルダのアクセス権変更（※1）	P.10

3．証跡管理（ログ管理）

ACV	重要フォルダへのアクセス状況	P.11
ACV	夜間のアクセス	P.12
ACV	不正アクセス	P.13
DB	特定アプリケーション以外のテーブル操作	P.14
DB	特権管理者のデータベース操作履歴	P.15

4．システム運用・保守

RA	ハードウェアインベントリ	P.16
RA	プロセス稼働状況	P.17
RA	一定期間アクセスの無いファイル	P.18

5．情報セキュリティ管理

RA	ウィルス対策ソフトインストール状況	P.19
ACV	重要ファイルの印刷ログ（※2）	P.20
ACV	退職予定者のアクセス状況	P.21

※1：ALog ConVerter for Linux では対応していません。
※2：ALog ConVerter for Windows のみの機能です。

グループアカウントとグループ構成の一覧

監査基準

監査基準（管理要件）	グループアカウントを定期的に棚卸し、その構成および状況を適切な状態に保つこと。
監査手続き	グループアカウントの定期的な棚卸の実績があることを確認する。 ※以下をもって棚卸実施の実績とする ・監査レポートが定期的に出力されていること ・過去分の監査レポートが適切に保管されていること
前提条件	（なし）
監査対象	ドメインコントローラ
監査レポート	グループアカウントとグループ構成の一覧【Resource Athlete】
評価指標（確認項目）	グループアカウントの定期的な棚卸を 実施している・・・・適合 実施していない・・・不適合

監査レポート（サンプル）

ALog

グループアカウントとグループ構成の一覧

クエリ実行日時: 2013/07/03 17:20:36　　Printed on 2013/07/03 17:22:49

件数: 147件

ドメイン名	グループ名	ユーザー名	説明
amiya.co.jp	amiya.co.jp¥lmm	amiya.co.jp¥ueta_emi amiya.co.jp¥kokubunn_sayaka amiya.co.jp¥ezaki_natsumi amiya.co.jp¥itabashi_nana amiya.co.jp¥koga_sora amiya.co.jp¥kumasawa_haruka amiya.co.jp¥konishi_hideki	ﾗｲﾝﾏﾈｰｼﾞｬ(新grazie)
amiya.co.jp	amiya.co.jp¥mgr	amiya.co.jp¥ueta_emi amiya.co.jp¥kokubunn_sayaka amiya.co.jp¥ezaki_natsumi amiya.co.jp¥itabashi_nana amiya.co.jp¥koga_sora amiya.co.jp¥kumasawa_haruka	ｾﾞﾈﾗﾙﾏﾈｰｼﾞｬ(新grazie)
amiya.co.jp	amiya.co.jp¥keiki	amiya.co.jp¥kumasawa_haruka amiya.co.jp¥kameyama_masaya	経営企画室(新grazie)taka
amiya.co.jp	amiya.co.jp¥jk	amiya.co.jp¥katase_takashi amiya.co.jp¥kumasawa_haruka	企画事業部(新grazie)
amiya.co.jp	amiya.co.jp¥mk		ﾏｰｹﾃｨﾝｸﾞ室(新grazie)
amiya.co.jp	amiya.c	amiya.co.jp¥kameyama_masaya	TQC執行室(新grazie)
amiya.co.jp	amiya.c	amiya.co.jp¥ueta_emi amiya.co.jp¥nasu_hiroshi amiya.co.jp¥kitahara_miwako amiya.co.jp¥kokubunn_sayaka amiya.co.jp¥fukushi_houshi	ｾｷｭﾘﾃｨ事業部(新grazie)

グループ別にユーザをリストアップすれば、退職者や異動者のグループ変更忘れをひと目でチェックでき、アクセス権を適切に保てます。

長期未ログオンのアカウント

監査基準

監査基準（管理要件）	長期間利用されていないユーザアカウントや、退職者のユーザアカウントなどの有無を定期的に点検し、必要に応じて削除すること。
監査手続き	長期間利用されていないユーザアカウントの定期的な棚卸の実績があること、および記録が適切に保管されていることを確認する。
前提条件	（なし）
監査対象	ドメインコントローラ
監査レポート	長期未ログオンのアカウント【Resource Athlete】
評価指標（確認項目）	長期間利用されていないユーザアカウントの定期的な棚卸を 実施している・・・・適合 実施していない・・・不適合

監査レポート（サンプル）

ALog

長期未ログオンのアカウント

クエリ実行日時: 2011/04/18 1:02:36　　Printed on 2011/09/28 17:19:39

最終ログオン日時が90日よりも古いユーザをピックアップします。(クエリのフィルタ設定によって比較日数を変更できます)

件数: 8件

ドメイン名	ユーザ名	フルネーム	最終ログオン日時	アカウントは無効か？
AUDITDEMO1	Administrator		2011-04-15 13:17:26	No
AUDITDEMO1	DemoUser	デモユーザー		No
AUDITDEMO1	Guest			Yes
AUDITDEMO1	Guest2	Guest2		No
AUDITDEMO1	hi-doi	hi-doi	2011-04-15 13:14:48	No
AUDITDEMO1	sa-suzuki	鈴木聡史		No
AUDITDEMO1	yamamoto	山本　孝		Yes
AUDITDEMO1	yo-hisanabe		2011-04-14 13:51:09	No

アカウントの消し忘れ、停止忘れが一目で分かるので、
システム管理者様の日々の業務にも活用できます。

一定日数以上パスワード未変更のアカウント

監査基準

監査基準（管理要件）	ユーザはパスワードを90日ごとに変更すること。
監査手続き	現在有効なドメインユーザアカウントに、90日以上パスワードを変更していないユーザアカウントが存在しないことを確認する。
前提条件	（なし）
監査対象	ドメインコントローラ
監査レポート	一定日数以上パスワード未変更のアカウント【Resource Athlete】
評価指標（確認項目）	パスワードを90日以上変更していないユーザが 存在しない・・・・適合 存在する・・・不適合

監査レポート（サンプル）

ALog

一定日数以上パスワード未変更のアカウント

クエリ実行日時: 2011/04/15 9:29:16　　Printed on 2012/01/25 15:12:25

90日以上パスワードを変更していないユーザのパスワードに関する情報の一覧を作成します。パスワードの最終変更日時、時間で失効するか、現在有効か等を示します。

件数: 163件

ドメイン名	ユーザ名	フルネーム	パスワード変更日時	パスワードが無期限か？	パスワードが期限切れか？
amiya.co.jp	amiya.co.jp¥anndou_houshi	安藤 法嗣	2009-09-14 08:38:56	Yes	Yes
amiya.co.jp	amiya.co.jp¥maekawa_yutaka	前川 豊	1999-04-05 08:51:08	No	No
amiya.co.jp	amiya.co.jp¥nakano_mitsuru	中野 満	1999-12-20 14:15:17	Yes	No
amiya.co.jp	amiya.co.jp¥yanagida_rie	柳田 りえ	2007-07-19 19:05:46	Yes	Yes
amiya.co.jp	amiya.co.jp¥nishihara_yuu	西原 優	2008-04-15 11:31:56	No	Yes
amiya.co.jp	amiya.co.jp¥hirata_shouko	平田 翔子	2008-11-10 11:03:57	Yes	Yes
amiya.co.jp	amiya.co.jp¥nasu_hiroshi	那須 宏	2006-09-12 13:29:07	Yes	Yes
amiya.co.jp	amiya.co.jp¥ashiya_akira	芦屋 明	2002-09-10 13:08:43	No	No
amiya.co.jp	amiya.co.jp¥takasawa_masahiko	高沢 雅彦	2000-07-17 17:12:22	No	No
amiya.co.jp	amiya.co.jp¥toda_kaoru	戸田 薫	2006-06-02 17:30:19	Yes	No
amiya.co.jp	amiya.co.jp¥oogo_subaru	大後 昴	2002-04-01 10:58:31	Yes	Yes
amiya.co.jp	amiya.co.jp¥tamada_momoko	玉田 桃子	2008-02-01 17:44:31	No	No
amiya.c	co.jp¥itou_shunji	伊東 俊二	2004-06-14 18:31:48	Yes	No
amiya.	himura_nana	内村 奈々	2006-05-08 09:06:10	Yes	Yes
amiya	wanaka_kogan	川中 小雁	2002-06-04 12:12:59	No	No
amiya	asaki_ukyou	岩崎 右京	2001-11-16 12:31:33	No	No
amiya.co.jp	ako_keiko	佐古 恵子	2002-05-31 10:35:58	Yes	No
amiya.co.jp				Yes	No
				No	

日数は任意に変更できますので、組織のパスワードポリシーに沿ったチェックが可能です。

管理者アカウント

監査基準

監査基準（管理要件）	特権ユーザアカウントは、その発行数および利用者数をいつでも把握できる状態で管理すること。
監査手続き	すべての情報システムにおいて、特権ユーザアカウントの台帳を作成していることを確認する。
前提条件	（なし）
監査対象	ドメインコントローラ, ファイルサーバ, データベースサーバ　等
監査レポート	管理者アカウント【Resource Athlete】
評価指標（確認項目）	特権ユーザアカウントの台帳を 作成している・・・適合 作成していない・・・不適合 ※監査レポートの出力をもって台帳の作成とみなす。

監査レポート（サンプル）

ALog

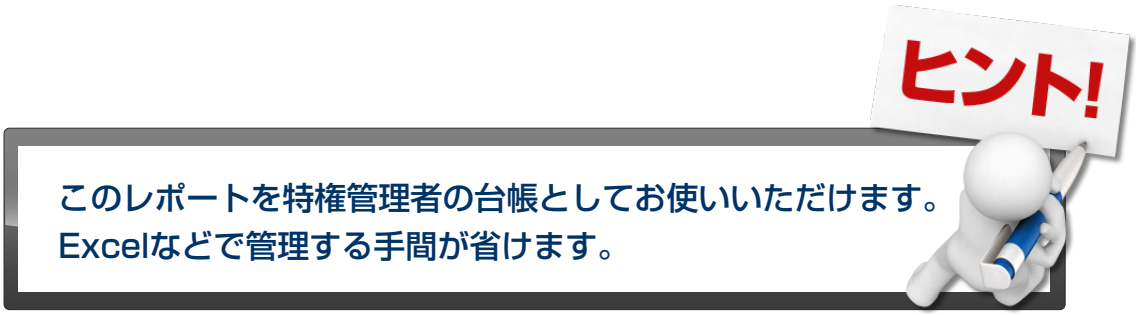
管理者アカウント

クエリ実行日時: 2011/04/18 1:02:36　　Printed on 2011/09/28 17:18:48

管理者権限を所有するユーザをリストアップします

件数: 3件

ドメイン名	ユーザ名	フルネーム	ユーザの説明
AUDITDEMO1	Administrator		コンピューター/ドメインの管理用 (ビルトイン アカウント)
AUDITDEMO1	hi-doi	hi-doi	
AUDITDEMO1	yo-hisanabe		



ユーザーアカウントの追加／削除

監査基準

監査基準（管理要件）	ユーザが退職等により情報システムへアクセスする必要がなくなった場合は、速やかにユーザアカウントを削除すること。
監査手続き	ユーザアカウントを削除した時期と、ユーザの退職時期が合致していることを確認する。
前提条件	退職者のユーザアカウントおよび退職時期が識別できること。
監査対象	ドメインコントローラ
監査レポート	アカウントの追加と削除【ALog ConVerter】
評価指標（確認項目）	ユーザアカウントを削除した時期と、ユーザの退職時期が 合致する・・・・適合 合致しない・・・不適合

監査レポート（サンプル）

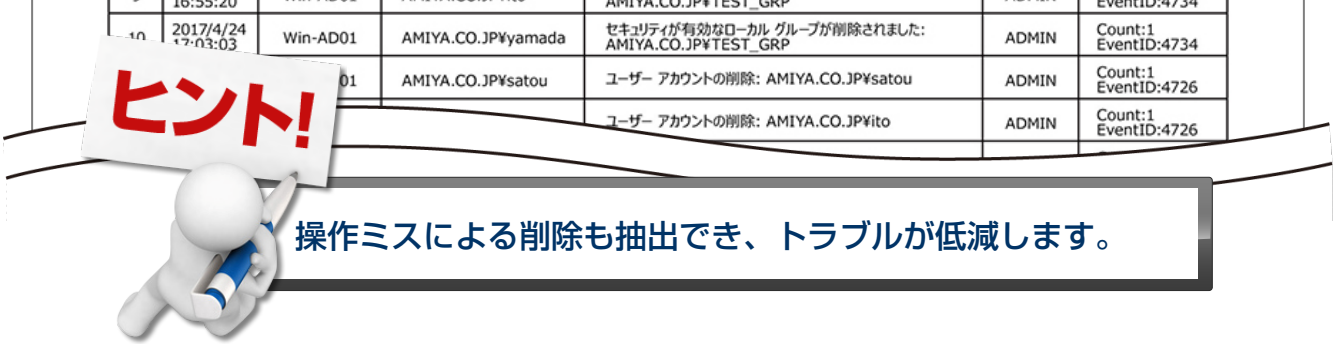
ALog

アカウントの追加と削除

Printed on 2018/01/15 9:28:51

結果: 29件

No	時刻	サーバ	ユーザー	対象	操作	詳細
1	2017/4/13 14:04:05	Win-AD01	AMIYA.CO.JP¥satou	セキュリティが有効なローカル グループ メンバが追加されました: AMIYA.CO.JP¥TEST_GRP	ADMIN	Count:1 EventID:4732
2	2017/4/13 14:08:32	Win-AD01	AMIYA.CO.JP¥ito	セキュリティが有効なローカル グループ メンバが追加されました: AMIYA.CO.JP¥TEST_GRP	ADMIN	Count:1 EventID:4732
3	2017/4/13 14:26:41	Win-AD01	AMIYA.CO.JP¥yamada	セキュリティが有効なローカル グループ メンバが追加されました: AMIYA.CO.JP¥TEST_GRP	ADMIN	Count:1 EventID:4732
4	2017/4/24 13:12:55	Win-AD01	AMIYA.CO.JP¥satou	セキュリティが有効なローカル グループ メンバが削除されました: AMIYA.CO.JP¥TEST_GRP	ADMIN	Count:1 EventID:4733
5	2017/4/24 13:33:02	Win-AD01	AMIYA.CO.JP¥ito	セキュリティが有効なローカル グループ メンバが削除されました: AMIYA.CO.JP¥TEST_GRP	ADMIN	Count:1 EventID:4733
6	2017/4/24 13:52:38	Win-AD01	AMIYA.CO.JP¥yamada	セキュリティが有効なローカル グループ メンバが削除されました: AMIYA.CO.JP¥TEST_GRP	ADMIN	Count:1 EventID:4733
7	2017/4/24 16:08:05	Win-AD01	AMIYA.CO.JP¥tanaka	セキュリティが有効なローカル グループ メンバが削除されました: AMIYA.CO.JP¥AMIYA_GRP	ADMIN	Count:1 EventID:4733
8	2017/4/24 16:32:27	Win-AD01	AMIYA.CO.JP¥satou	セキュリティが有効なローカル グループが削除されました: AMIYA.CO.JP¥TEST_GRP	ADMIN	Count:1 EventID:4734
9	2017/4/24 16:55:20	Win-AD01	AMIYA.CO.JP¥ito	セキュリティが有効なローカル グループが削除されました: AMIYA.CO.JP¥TEST_GRP	ADMIN	Count:1 EventID:4734
10	2017/4/24 17:03:03	Win-AD01	AMIYA.CO.JP¥yamada	セキュリティが有効なローカル グループが削除されました: AMIYA.CO.JP¥TEST_GRP	ADMIN	Count:1 EventID:4734
		01	AMIYA.CO.JP¥satou	ユーザー アカウントの削除: AMIYA.CO.JP¥satou	ADMIN	Count:1 EventID:4726
				ユーザー アカウントの削除: AMIYA.CO.JP¥ito	ADMIN	Count:1 EventID:4726



データベースユーザーへの特権付与

監査基準

監査基準（管理要件）	重要な情報を保管するデータベース、特に財務報告に係るデータベースに特権ユーザアカウントを追加する場合は、適切な権限を持つ者（原則として情報システム管理者）が、情報システム責任者の承認を得たうえで行うこと。
監査手続き	特権ユーザアカウントの作成または権限変更の作業が情報システム管理者によって実施されていることを確認する。併せてその際の手続き（承認、指示等）を確認する。
前提条件	情報システム管理者のユーザアカウントが識別できること。
監査対象	データベースサーバ
監査レポート	データベースユーザへの特権付与【ALog ConVerter DB】
評価指標（確認項目）	データベースの特権ユーザアカウントの作成または権限変更を実施したアカウントが 情報システム管理者のものである・・・・適合 情報システム管理者のものではない・・・不適合

監査レポート（サンプル）

ALog

データベースユーザへの特権付与

Printed on 2018/01/16 12:22:03

結果: 10件

No	時刻	サーバ	ユーザー	対象	操作	詳細
1	2017/4/1 15:34:53	Oracle01¥KAIKEIDB	SYS_TAJIMA	[KAIKEI]にシステム権限が与えられました	DB_ADMIN	AppName:SQL*Plus ClientName:PC001 Count:1 Schema:[unknown]
2	2017/4/1 15:34:53	Oracle01¥KAIKEIDB	SYS_TAJIMA	[KAIKEI]にシステム権限が与えられました	DB_ADMIN	AppName:SQL*Plus ClientName:PC001 Count:1 Schema:[unknown]
3	2017/4/1 15:34:53	Oracle01¥KAIKEIDB	SYS_TAJIMA	[KAIKEI]にシステム権限が与えられました	DB_ADMIN	AppName:SQL*Plus ClientName:PC001 Count:1 Schema:[unknown]
4	2017/4/1 15:34:53	Oracle01¥KAIKEIDB	SYS_TAJIMA	[KAIKEI]にシステム権限が与えられました	DB_ADMIN	AppName:SQL*Plus ClientName:PC001 Count:1 Schema:[unknown]
	2017/4/1	Oracle01¥KAIKEIDB	SYS_TAJIMA	[KAIKEI]にシステム権限が与えられました	DB_ADMIN	AppName:SQL*Plus ClientName:PC001 Count:1 Schema:[unknown]
		KAIKEIDB	SYS_TAJIMA	[KAIKEI]にシステム権限が与えられました	DB_ADMIN	AppName:SQL*Plus ClientName:PC001 Count:1 Schema:[unknown]
				[KAIKEI]にシステム権限が与えられました	DB_ADMIN	AppName:SQL*Plus ClientName:PC001 Count:1

操作の失敗も記録できるので、不正に権限を与えようとした行為のアラート通知が可能です。

全フォルダのアクセス権

監査基準

監査基準（管理要件）	情報資産へのアクセス権は、ユーザの業務の種類ごとに、必要な範囲に限定して付与すること。
監査手続き	各フォルダに業務に関係のないユーザへアクセス権が付与されていないことを確認する。（サンプリング調査とする）
前提条件	ユーザの業務内容からアクセスするフォルダが識別できること。
監査対象	ファイルサーバ
監査レポート	全フォルダのアクセス権【Resource Athlete】
評価指標（確認項目）	調査対象となったフォルダにアクセスする必要のないユーザが アクセス権を与えられていない・・・・適合 アクセス権を与えられている・・・不適合

監査レポート（サンプル）

全フォルダのアクセス権（前回との差分）

監査基準

監査基準（管理要件）	アクセス権は定期的に棚卸し、前回の棚卸結果との差異を記録すること。
監査手続き	最新のフォルダアクセス権の棚卸結果において、前回の棚卸実施時との差異が記録されていることを確認する。
前提条件	（なし）
監査対象	ファイルサーバ
監査レポート	全フォルダのアクセス権（前回との差分）【Resource Athlete】
評価指標（確認項目）	棚卸実施結果において前回の棚卸実施時との差異が 記録されている・・・・適合 記録されていない・・・不適合

監査レポート（サンプル）

ALog

全フォルダのアクセス権（前回との差分）

クエリ実行日時: 2011/01/20 10:47:18
（前回実行日時: 2011/01/20 10:43:20）
Printed on 2012/01/25 15:24:26

全フォルダのアクセス権限を作成します。前回クエリ実行時との差分のみ抽出し、レポート化します。

件数: 4件

変更種別	マシン名	ディレクトリ名	許可の状態	アカウント	許可の種類
M	AuditDemo1	C:¥監査対象¥技術部¥90_Work¥ALogWin¥system	許可 許可－ 許可－ 許可－ 許可－ 許可－	AUDITDEMO1¥Users Everyone SYSTEM AUDITDEMO1¥Administrators CREATOR OWNER AUDITDEMO1¥技術部	変更 フルコントロール フルコントロール フルコントロール フルコントロール フルコントロール
A	AuditDemo1	C:¥監査対象¥技術部¥90_Work¥ALogWin¥新しいフォルダー	許可－ 許可－ 許可－ 許可－ 許可－	Everyone SYSTEM AUDITDEMO1¥Administrators CREATOR OWNER AUDITDEMO1¥技術部	フルコントロール フルコントロール フルコントロール フルコントロール フルコントロール
A	AuditDemo1	C:¥監査対象¥技術部¥90_Work¥ALogWin¥新しいフォルダー¥document	許可－ 許可－ 許可－ 許可－ 許可－	Everyone SYSTEM AUDITDEMO1¥Administrators CREATOR OWNER AUDITDEMO1¥技術部	フルコントロール フルコントロール フルコントロール フルコントロール フルコントロール
D	AuditDemo1	C:¥監査対象¥技術部¥90_Work¥ALogWin¥uninstall	許可－ 許可－ 許可－ 許可－ 許可－	Everyone SYSTEM AUDITDEMO1¥Administrators CREATOR OWNER AUDITDEMO1¥技術部	フルコントロール フルコントロール フルコントロール フルコントロール フルコントロール

前回調査時からアクセス権が変更されたフォルダだけを抽出すれば、膨大な台帳の突き合わせを行う手間が省けます！

ファイル／フォルダのアクセス権変更

監査基準

監査基準（管理要件）	ファイル／フォルダのアクセス権の付与および削除に係る手続きは、適切な権限を持つ者（原則として情報システム管理者）が行うこと。
監査手続き	アクセス権の付与および削除の作業が情報システム管理者によって実施されていることを確認する。
前提条件	情報システム管理者のユーザアカウントが識別できること。
監査対象	ファイルサーバ
監査レポート	ファイルフォルダのアクセス権変更【ALog ConVerter】
評価指標（確認項目）	アクセス権の変更を実施したアカウントが 情報システム管理者のものである・・・・適合 情報システム管理者のものではない・・・不適合

監査レポート（サンプル）

※本レポートはALog ConVerter for Linux では対応していません。

ALog

ファイル/フォルダのアクセス権変更

Printed on 2018/01/15 10:08:19

結果: 166件

No	時刻	サーバ	ユーザー	対象	操作	詳細
1	2017/2/10 13:35:48	bvdemo2	BVDEMO2¥yo-kamei	C:¥Users¥Administrator.bvdemo2-PC¥Desktop¥製品紹介資料倉庫	P-ACCESS	ClientIP:192.168.1.144 Count:1
2	2017/2/10 13:35:48	bvdemo2	BVDEMO2¥yo-kamei	C:¥Users¥Administrator.bvdemo2-PC¥Desktop¥製品紹介資料倉庫¥1015_Seminar	P-ACCESS	ClientIP:192.168.1.144 Count:1
3	2017/2/10 13:35:48	bvdemo2	BVDEMO2¥yo-kamei	C:¥Users¥Administrator.bvdemo2-PC¥Desktop¥製品紹介資料倉庫¥1015_Seminar¥セミナー資料.ppt	P-ACCESS	ClientIP:192.168.1.144 Count:1
4	2017/2/10 13:35:48	bvdemo2	BVDEMO2¥yo-kamei	C:¥Users¥Administrator.bvdemo2-PC¥Desktop¥製品紹介資料倉庫¥1015_Seminar¥セミナー本日の流れ.ppt	P-ACCESS	ClientIP:192.168.1.144 Count:1
5	2017/2/10 13:35:49	bvdemo2	BVDEMO2¥yo-kamei	C:¥Users¥Administrator.bvdemo2-PC¥Desktop¥製品紹介資料倉庫¥1015_Seminar¥特権ID管理セミナー171015.ppt	P-ACCESS	ClientIP:192.168.1.144 Count:1
6	2017/2/10 13:35:49	bvdemo2	BVDEMO2¥yo-kamei	C:¥Users¥Administrator.bvdemo2-PC¥Desktop¥製品紹介資料倉庫¥7133_2ReALogについて.msg	P-ACCESS	ClientIP:192.168.1.144 Count:1
7	2017/2/10 13:35:49	bvdemo2	BVDEMO2¥yo-kamei	C:¥Users¥Administrator.bvdemo2-PC¥Desktop¥製品紹介資料倉庫¥ALog資料	P-ACCESS	ClientIP:192.168.1.144 Count:1
	2017/2/10	bvdemo2	BVDEMO2¥yo-kamei	C:¥Users¥Administrator.bvdemo2-PC¥Desktop¥製品紹介資料倉庫¥ALog資料¥ALogV7	P-ACCESS	ClientIP:192.168.1.144 Count:1
			BVDEMO2¥yo-kamei	C:¥Users¥Administrator.bvdemo2-PC¥Desktop¥製品紹介資料倉庫¥ALog資料¥ALogV7¥ALogV7取扱項目検討.xls	P-ACCESS	ClientIP:192.168.1.144 Count:1
			BVDEMO2¥yo-kamei	C:¥Users¥Administrator.bvdemo2-PC¥Desktop¥製品紹介資料倉庫¥ALog資料¥ALogV7¥ALogV7概要.ppt	P-ACCESS	ClientIP:192.168.1.144 Count:1
11			BVDEMO2¥yo-kamei	C:¥Users¥Administrator.bvdemo2-PC¥Desktop¥製品紹介資料倉庫¥ALog資料¥ALogV7¥リリースロードマップ.ppt	P-ACCESS	ClientIP:192.168.1.144 Count:1

ヒント!

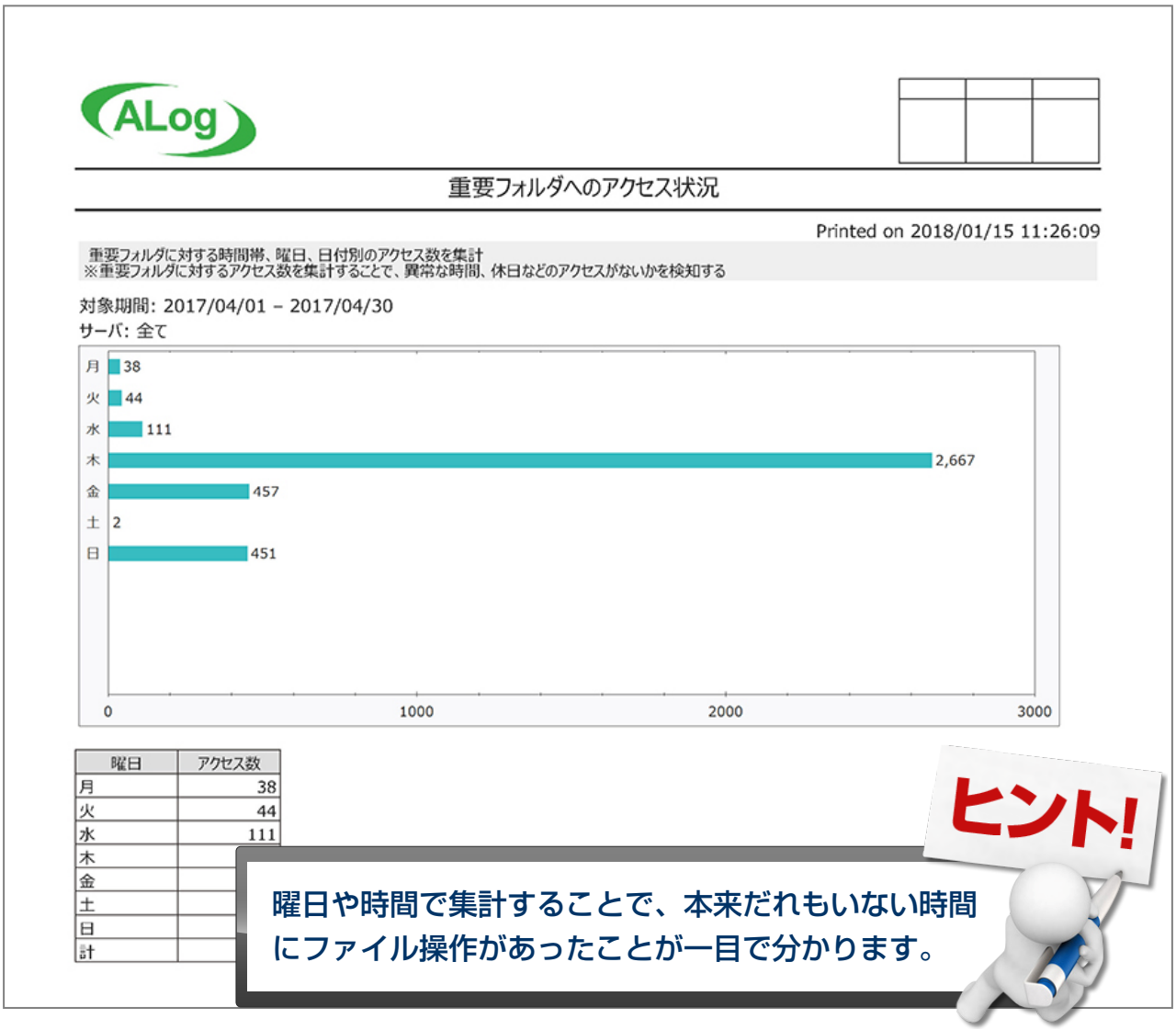
申請書の日付と突き合せれば操作の正当性も証明できます。

重要フォルダへのアクセス状況

監査基準

監査基準（管理要件）	重要な情報資産に対するすべてのアクセスを継続的に記録すること。
監査手続き	重要な情報資産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	重要な情報が格納されているフォルダが識別できること。
監査対象	ファイルサーバ
監査レポート	重要フォルダへのアクセス状況【ALog ConVerter】
評価指標（確認項目）	情報資産に対するアクセス履歴が 保管されている・・・・適合 保管されていない・・・不適合

監査レポート（サンプル）

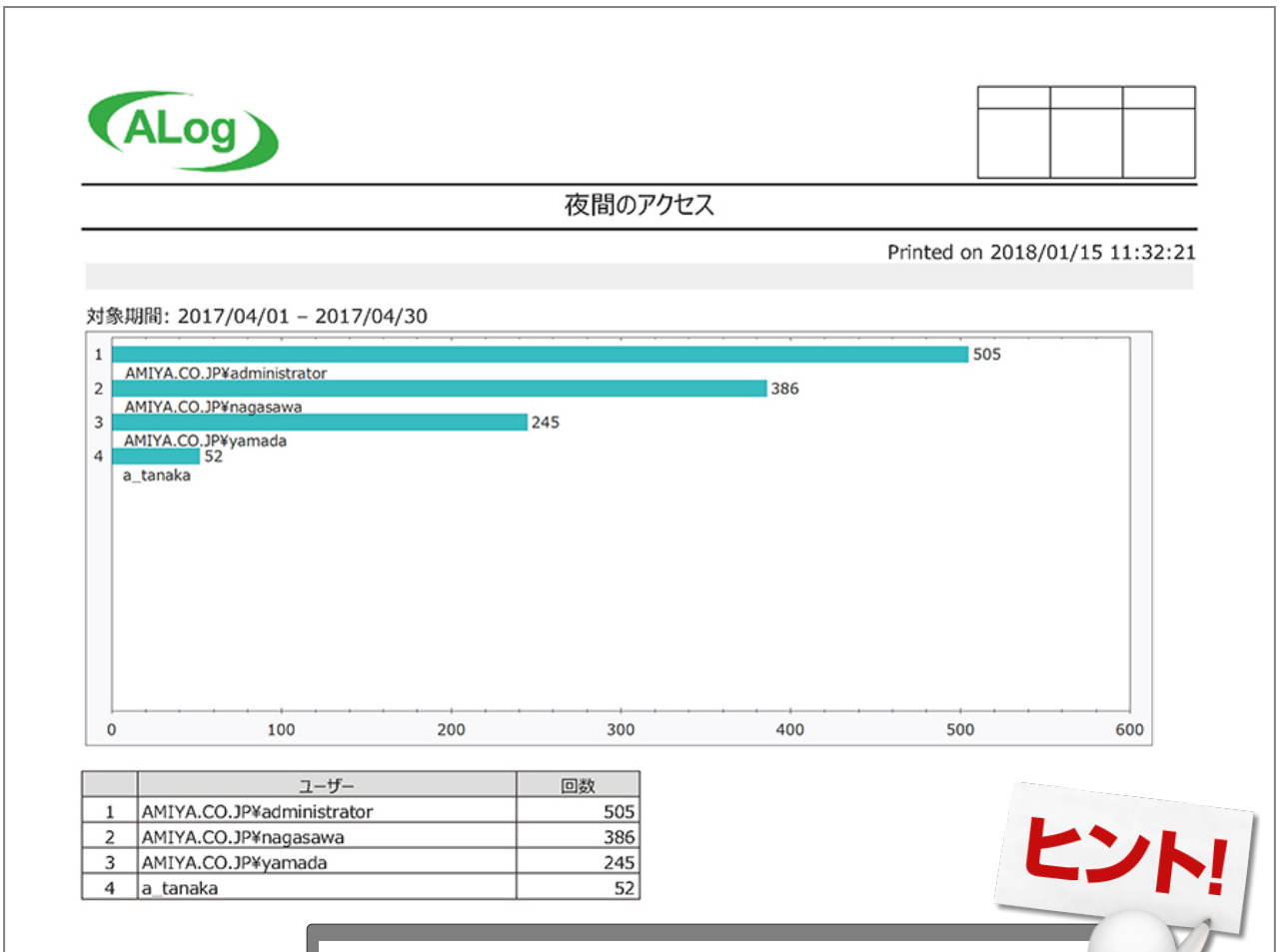


夜間のアクセス

監査基準

監査基準（管理要件）	定期的に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。
監査手続き	情報資産に対するアクセス記録を定期的に取得し、点検していることを確認する。
前提条件	（なし）
監査対象	ファイルサーバ
監査レポート	夜間のアクセス【ALog ConVerter】
評価指標（確認項目）	不正アクセス、異常アクセスの有無を 確認している・・・・適合 確認していない・・・不適合

監査レポート（サンプル）



	ユーザー	回数
1	AMIYA.CO.JP¥administrator	505
2	AMIYA.CO.JP¥nagasawa	386
3	AMIYA.CO.JP¥yamada	245
4	a_tanaka	52

「休日のアクセス」「一定回数以上のアクセス」
などのレポートも分析に有効です。

不正アクセス

監査基準

監査基準（管理要件）	認証に関するエラー、アクセスに関するエラーを点検し、不正なアクセスの有無を確認すること。
監査手続き	ユーザ認証のエラーやファイルアクセスのエラーに関する記録が定期的に点検されていることを確認する。
前提条件	（なし）
監査対象	ドメインコントローラ、ファイルサーバ
監査レポート	不正アクセス【ALog ConVerter】
評価指標（確認項目）	不正アクセスの有無を 確認している・・・・適合 確認していない・・・不適合

監査レポート（サンプル）

ALog

不正アクセス

Printed on 2018/01/15 10:30:18

結果: 76件

No	時刻	サーバ	ユーザー	対象	操作	詳細
1	2017/4/1 8:59:29	GRAZIE	AMIYA.CO.JP¥goto	172.20.1.255	LOGON-Failure	AuthType:Kerberos Count:1 ErrorCause:ユーザ名を認識できないか、またはパスワードが間違っています
2	2017/4/1 8:59:29	GRAZIE	AMIYA.CO.JP¥goto	172.20.1.255	LOGON-Failure	AuthType:Kerberos Count:1 ErrorCause:ユーザ名を認識できないか、またはパスワードが間違っています
3	2017/4/3 9:05:52	GRAZIE	AMIYA.CO.JP¥suzuki	172.20.1.208	LOGON-Failure	AuthType:Kerberos Count:1 ErrorCause:ユーザ名を認識できないか、またはパスワードが間違っています
4	2017/4/3 9:05:52	GRAZIE	AMIYA.CO.JP¥suzuki	172.20.1.208	LOGON-Failure	AuthType:Kerberos Count:1 ErrorCause:ユーザ名を認識できないか、またはパスワードが間違っています
5	2017/4/7 8:54:48	GRAZIE	AMIYA.CO.JP¥yamaguchi	172.20.1.202	LOGON-Failure	AuthType:Kerberos Count:1 ErrorCause:ユーザ名を認識できないか、またはパスワードが間違っています
6	2017/4/7 8:54:48	GRAZIE	AMIYA.CO.JP¥yamaguchi	172.20.1.202	LOGON-Failure	AuthType:Kerberos Count:1 ErrorCause:ユーザ名を認識できないか、またはパスワードが間違っています
			AMIYA.CO.JP¥yamada	D:¥管理部¥一般書類テンプレート¥届出フォーム(労務)¥届出書(勤怠).doc	WRITE-Failure	ClientIP:172.20.1.238 Count:11
			AMIYA.CO.JP¥yamada	D:¥管理部¥一般書類テンプレート¥届出フォーム(労務)¥届出書(勤怠).doc	WRITE-Failure	ClientIP:172.20.1.238 Count:11
			AMIYA.CO.JP¥yamada	D:¥管理部¥一般書類テンプレート¥届出フォーム(労務)¥届出書(勤怠).doc	WRITE-Failure	ClientIP:172.20.1.238 Count:11
10						38

ログオンの失敗を繰り返すユーザ、ファイル削除の失敗を繰り返すユーザなど、さまざまな観点で不正を検知することができます。

特定アプリケーション以外のテーブル操作

監査基準

監査基準（管理要件）	定期的に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。
監査手続き	情報資産に対するアクセス記録を定期的に取得し、点検していることを確認する。
前提条件	（なし）
監査対象	データベースサーバ
監査レポート	特定アプリケーション以外のテーブル操作【ALog ConVerter DB】
評価指標（確認項目）	不正アクセス、異常アクセスの有無を 確認している・・・・適合 確認していない・・・不適合

監査レポート（サンプル）

ALog

特定アプリケーション以外のテーブル操作

Printed on 2018/01/16 12:02:41

結果: 10件

No	時刻	サーバ	ユーザー	対象	操作	詳細
1	2017/4/1 11:55:26	MsSQLServer01	sa	テーブル「T_URIKAKE」のデータが参照されました。	DB_SELECT	AppName:SQLCMD ClientName:PC001 Count:1 DB:kaikeidb
2	2017/4/1 11:55:26	MsSQLServer01	sa	テーブル「T_URIKAKE」のデータが更新されました。	DB_UPDATE	AppName:SQLCMD ClientName:PC001 Count:1 DB:kaikeidb
3	2017/4/1 11:59:08	MsSQLServer01	sa	テーブル「T_URIKAKE」のデータが追加されました。	DB_INSERT	AppName:SQLCMD ClientName:PC001 Count:1 DB:kaikeidb
4	2017/4/1 11:59:27	MsSQLServer01	sa	テーブル「T_URIKAKE」のデータが参照されました。	DB_SELECT	AppName:SQLCMD ClientName:PC001 Count:1 DB:kaikeidb
5	2017/4/1 11:59:34	MsSQLServer01	sa	テーブル「T_URIKAKE」のデータが参照されました。	DB_SELECT	AppName:SQLCMD ClientName:PC001 Count:1 DB:kaikeidb
6	2017/4/1 11:59:34	MsSQLServer01	sa	テーブル「T_URIKAKE」のデータが更新されました。	DB_UPDATE	AppName:SQLCMD ClientName:PC001 Count:1 DB:kaikeidb
7	2017/4/2 11:59:26	MsSQLServer		_URIKAKE」のデータが参照されました。	DB_SELECT	AppName:SQLCMD ClientName:PC002 Count:1 DB:kaikeidb
8	2017/4/3 11:59:33	MsSQLServer01				AppName:SQLCMD ClientName:PC003
9	2017/4/22 11:59:01	MsSQLServer01	sa			
10	2017/4/22 11:59:12	MsSQLServer01	sa			

コマンドラインツールなど、業務アプリ以外のツールによるテーブル操作を監視することで、不正アクセスの予防につながります。

特権管理者のデータベース操作履歴

監査基準

監査基準（管理要件）	重要な情報を保管するデータベース、特に財務報告に係るデータベースに対し特権を用いて実施した操作を記録すること。
監査手続き	特権ユーザアカウントの操作履歴の有無を確認する。
前提条件	特権が付与されているデータベースユーザ名が識別できること。
監査対象	データベースサーバ
監査レポート	特権管理者のデータベース操作履歴【ALog ConVerter DB】
評価指標（確認項目）	重要なデータベースへの特権を用いた操作の記録が 保管されている・・・・適合 保管されていない・・・不適合

監査レポート（サンプル）

ALog

特権管理者のデータベース操作履歴

Printed on 2018/01/16 10:28:42

結果: 57件

No	時刻	サーバ	ユーザー	対象	操作	詳細
1	2017/4/1 11:59:18	Oracle01¥KAIKEIDB	SYSTEM	[T_URIKAKE]のデータが追加されました	DB_INSERT	AppName:SQL*Plus ClientName:PC001 Count:1 Schema:KAIKEI
2	2017/4/1 11:59:35	Oracle01¥KAIKEIDB	SYSTEM	[T_URIKAKE]のデータが参照されました	DB_SELECT	AppName:SQL*Plus ClientName:PC001 Count:1 Schema:KAIKEI
3	2017/4/1 11:59:48	Oracle01¥KAIKEIDB	SYSTEM	[T_URIKAKE]のデータが更新されました	DB_UPDATE	AppName:SQL*Plus ClientName:PC001 Count:1 Schema:KAIKEI
4	2017/4/1 15:34:53	Oracle01¥KAIKEIDB	SYS_TAJIMA	ユーザ[KAIKEI]が削除されました	DB_ADMIN	AppName:SQL*Plus ClientName:PC001 Count:1 Schema:SYSTESM
5	2017/4/1 15:34:53	Oracle01¥KAIKEIDB	SYS_TAJIMA	ユーザ[KAIKEI]が作成されました	DB_ADMIN	AppName:SQL*Plus ClientName:PC001 Count:1 Schema:SYSTESM
6	2017/4/1 15:34:53	Oracle01¥KAIKEIDB	SYS_TAJIMA	[KAIKEI]にシステム権限が与えられました	DB_ADMIN	AppName:SQL*Plus ClientName:PC001 Count:1 Schema:[unknown]
7	2017/4/1 15:34:53	Oracle01¥KAIKEIDB	SYS_TAJIMA	[KAIKEI]にシステム権限が与えられました	DB_ADMIN	AppName:SQL*Plus
8	2017/4/1 15:34:53	Oracle01¥KAIKEIDB	SYS_TAJIMA	[KAIKEI]にシステム権限が与えられました	DB_ADMIN	
9	2017/4/1	Oracle				

ヒント!

ドメインコントローラやファイルサーバの管理者
操作履歴もALogシリーズでレポート可能です。
目的に合わせて製品をお選びください。

ハードウェアインベントリ

監査基準

監査基準（管理要件）	情報システムを構成するハードウェアを識別し、その構成を管理すること。
監査手続き	情報システムを構成するハードウェアの構成情報が適切に保管されていることを確認する。
前提条件	（なし）
監査対象	ドメインコントローラ, ファイルサーバ, データベースサーバ　等
監査レポート	ハードウェアインベントリ【Resource Athlete】
評価指標（確認項目）	ハードウェアの構成情報が 管理されている・・・・適合 管理されていない・・・不適合

監査レポート（サンプル）

ALog

ハードウェアインベントリ

クエリ実行日時: 2011/09/28 16:04:03　　Printed on 2011/09/28 17:24:18

サーバのCPUとOS情報、メモリ、ディスク、IPアドレスなどの一覧表を作成します

件数: 3件

ドメイン名	マシン名	OSバージョン	メモリ容量(MB)	HDD容量(GB)	HDD残量(GB)	IPアドレス	プロセッサ種別
amiya.co.jp	dev01	Windows 2003	4094.12	2794.52	1252.54	192.168.107.1	Quad-Core AMD Opteron(tm) Processor 1381
amiya.co.jp	fania	Windows 2008	4060.07	2328.71	1201.97	192.168.0.78	Intel(R) Core(TM)2 Quad CPU Q8200 @ 2.33GHz
amiya.co.jp	unix-eval	Windows 2008	4029.19	1397.26	441.42	192.168.0.36	Intel(R) Xeon(R) CPU 3050 @ 2.13GHz

収集項目は自由にカスタマイズできます。定期的にレポーティングすれば、システムリソースのモニタリングにも活用できます。

プロセス稼働状況

監査基準

監査基準（管理要件）	情報システムの稼働状況を定期的に点検し、異常なプロセス等の情報セキュリティインシデントの予兆または発生がないか確認すること。
監査手続き	情報システムのプロセスの稼働状況が定期的に点検されていることを確認する。
前提条件	（なし）
監査対象	ドメインコントローラ, ファイルサーバ, データベースサーバ　等
監査レポート	プロセス稼働状況【Resource Athlete】
評価指標（確認項目）	情報システムのプロセス稼働状況が 定期的に点検されている・・・・適合 定期的に点検されていない・・・不適合

監査レポート（サンプル）

ALog

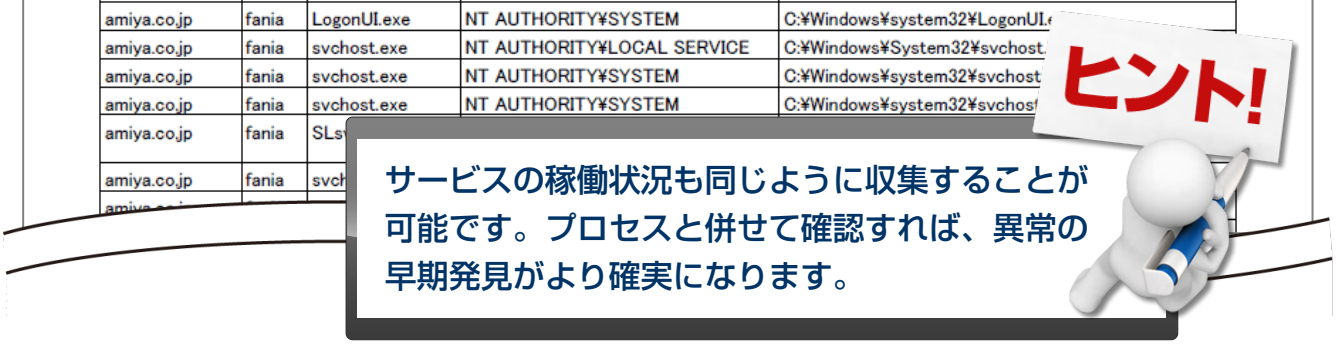
プロセス

クエリ実行日時: 2011/09/28 15:48:34　　Printed on 2011/09/28 17:25:51

サーバで実行中のプロセス一覧を作成します

件数: 55件

ドメイン名	マシン名	プロセス名	ユーザ名	パス
amiya.co.jp	fania	System Idle Process		
amiya.co.jp	fania	System		
amiya.co.jp	fania	smss.exe	NT AUTHORITY¥SYSTEM	
amiya.co.jp	fania	csrss.exe	NT AUTHORITY¥SYSTEM	C:¥Windows¥system32¥csrss.exe
amiya.co.jp	fania	csrss.exe	NT AUTHORITY¥SYSTEM	C:¥Windows¥system32¥csrss.exe
amiya.co.jp	fania	wininit.exe	NT AUTHORITY¥SYSTEM	C:¥Windows¥system32¥wininit.exe
amiya.co.jp	fania	winlogon.exe	NT AUTHORITY¥SYSTEM	C:¥Windows¥system32¥winlogon.exe
amiya.co.jp	fania	services.exe	NT AUTHORITY¥SYSTEM	C:¥Windows¥system32¥services.exe
amiya.co.jp	fania	lsass.exe	NT AUTHORITY¥SYSTEM	C:¥Windows¥system32¥lsass.exe
amiya.co.jp	fania	lsm.exe	NT AUTHORITY¥SYSTEM	C:¥Windows¥system32¥lsm.exe
amiya.co.jp	fania	svchost.exe	NT AUTHORITY¥SYSTEM	C:¥Windows¥system32¥svchost.exe
amiya.co.jp	fania	svchost.exe	NT AUTHORITY¥NETWORK SERVICE	C:¥Windows¥system32¥svchost.exe
amiya.co.jp	fania	LogonUI.exe	NT AUTHORITY¥SYSTEM	C:¥Windows¥system32¥LogonUI.e
amiya.co.jp	fania	svchost.exe	NT AUTHORITY¥LOCAL SERVICE	C:¥Windows¥System32¥svchost.
amiya.co.jp	fania	svchost.exe	NT AUTHORITY¥SYSTEM	C:¥Windows¥system32¥svchost
amiya.co.jp	fania	svchost.exe	NT AUTHORITY¥SYSTEM	C:¥Windows¥system32¥svchos
amiya.co.jp	fania	SLs		
amiya.co.jp	fania	svch		



一定期間アクセスの無いファイル

監査基準

監査基準（管理要件）	情報システムを構成するコンピュータに、一定日数以上利用されない不要なファイルがないか定期的に確認し、必要に応じて削除すること。
監査手続き	情報システムを構成するコンピュータにおいて、定期的に不要なファイルの棚卸がされ、必要に応じて削除されていることを確認する。
前提条件	情報システムを構成するコンピュータが識別できること。
監査対象	ドメインコントローラ, ファイルサーバ, データベースサーバ　等
監査レポート	一定期間アクセスの無いファイル【Resource Athlete】
評価指標（確認項目）	不要なファイルの棚卸および削除が 定期的に実施されている・・・・適合 定期的に実施されていない・・・不適合

監査レポート（サンプル）

ALog

一定期間アクセスの無いファイル

クエリ実行日時: 2011/05/06 14:54:36　　Printed on 2011/09/28 17:23:10

指定期間以上アクセスされていないファイルを表示します。
現在の設定は180日です。

件数: 179件

ドメイン名	マシン名	ファイル名	所有者	最終アクセス日時	階層
WORKGROUP	localhost	c:¥監査対象¥営業部¥作業用¥作業日誌.xls	BUILTIN¥Administrators	2009-12-19 15:00:14	2
WORKGROUP	localhost	c:¥監査対象¥営業部¥営業部-共有¥Ontap対応Ver一覧(200906).xls	BUILTIN¥Administrators	2009-06-23 17:11:40	2
WORKGROUP	localhost	c:¥監査対象¥営業部¥営業部-共有¥(最新)ALog_ConVerter_DBシリーズ_v4_19_6.ppt	BUILTIN¥Administrators	2010-07-29 09:36:40	2
WORKGROUP	localhost	c:¥監査対象¥営業部¥営業部-共有¥(最新)ALog_ConVerter_NASシリーズ_v4_19_6.ppt	BUILTIN¥Administrators	2010-07-29 09:36:46	2
WORKGROUP	localhost	c:¥監査対象¥営業部¥営業部-共有¥(最新)ALog_ConVerter_Windows_v4_19_4.ppt	BUILTIN¥Administrators	2010-07-29 11:17:12	2
WORKGROUP	localhost	c:¥監査対象¥営業部¥営業部-共有¥(最新)ALog_v4_価格表_縦_v1.3.ppt	BUILTIN¥Administrators	2010-07-29 09:57:58	2
WORKGROUP	localhost	c:¥監査対象¥技術部¥03_VMData¥2008SP2_AD¥564d3d3a-3b30-c915-1bc1-16a5a9e955f1.vmem	BUILTIN¥Administrators	2010-04-26 09:27:24	3
WORKGROUP	localhost	c:¥監査対象¥技術部¥90_Work¥ALogWin¥alog_remote¥bin¥addevent.vbs	BUILTIN¥Administrators	2008-06-26 10:32:12	5
WORKGROUP	localhost	c:¥監査対象¥ g_remote¥bin¥atproc.exe	BUILTIN¥Administrators	2009-08-03 15:40:10	5
WORKGROUP	localhost	c:¥監査対象¥ og_remote¥bin¥compile.bat	BUILTIN¥Administrators	2009-02-15 13:07:30	5
WORKGROUP	localhost	c:¥監査対象¥技術部¥ log_remote¥bin¥getsysapp.dat	BUILTIN¥Administr	2009-01-19	5
WORKGROUP	localhost	c:¥監査対象¥技術部¥9			

ファイルサーバの容量がひっ迫しているときに不要なファイルを探すなど、日々のメンテナンス業務にも役立ちます。

ウィルス対策ソフトインストール状況

監査基準

監査基準（管理要件）	ウィルスへの感染、拡大による被害を防ぐため、クライアントPCにウィルス対策ソフトをインストールすること。
監査手続き	ウィルス対策ソフトがインストールされていないクライアントPCがないことを確認する（サンプリング調査とする）
前提条件	組織内で利用されているウィルス対策ソフトが特定できること。
監査対象	クライアントPC
監査レポート	ウィルス対策ソフトインストール状況【Resource Athlete】
評価指標（確認項目）	ウィルス対策ソフトが インストールされている・・・・適合 インストールされていない・・・不適合

監査レポート（サンプル）

ALog

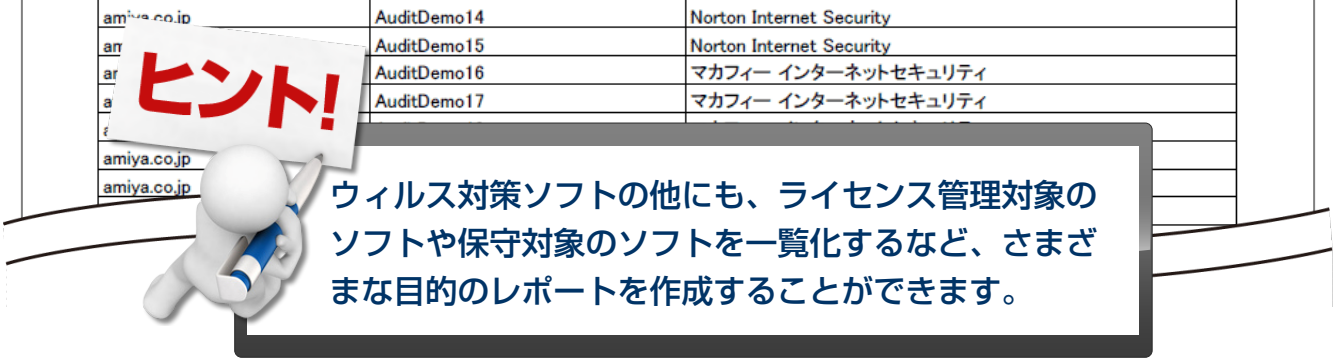
ウィルス対策ソフトインストール状況

クエリ実行日時: 2012/03/05 1:00:09　　Printed on 2012/03/05 14:19:28

ウィルス対策ソフトのインストール状況を取得します。
アプリケーション名のフィルタで任意のウィルス対策ソフトのアプリケーション名を指定してください。

件数: 50件

ドメイン名	マシン名	アプリケーション名
amiya.co.jp	AuditDemo1	ESET Smart Security
amiya.co.jp	AuditDemo2	ESET Smart Security
amiya.co.jp	AuditDemo3	Norton Internet Security
amiya.co.jp	AuditDemo4	Norton Internet Security
amiya.co.jp	AuditDemo5	ウイルスバスター
amiya.co.jp	AuditDemo6	ウイルスバスター
amiya.co.jp	AuditDemo7	ウイルスバスター
amiya.co.jp	AuditDemo8	ウイルスバスター
amiya.co.jp	AuditDemo9	ウイルスバスター
amiya.co.jp	AuditDemo10	マカフィー インターネットセキュリティ
amiya.co.jp	AuditDemo11	マカフィー インターネットセキュリティ
amiya.co.jp	AuditDemo12	Norton Internet Security
amiya.co.jp	AuditDemo13	Norton Internet Security
amiya.co.jp	AuditDemo14	Norton Internet Security
amiya.co.jp	AuditDemo15	Norton Internet Security
amiya.co.jp	AuditDemo16	マカフィー インターネットセキュリティ
amiya.co.jp	AuditDemo17	マカフィー インターネットセキュリティ
amiya.co.jp		
amiya.co.jp		



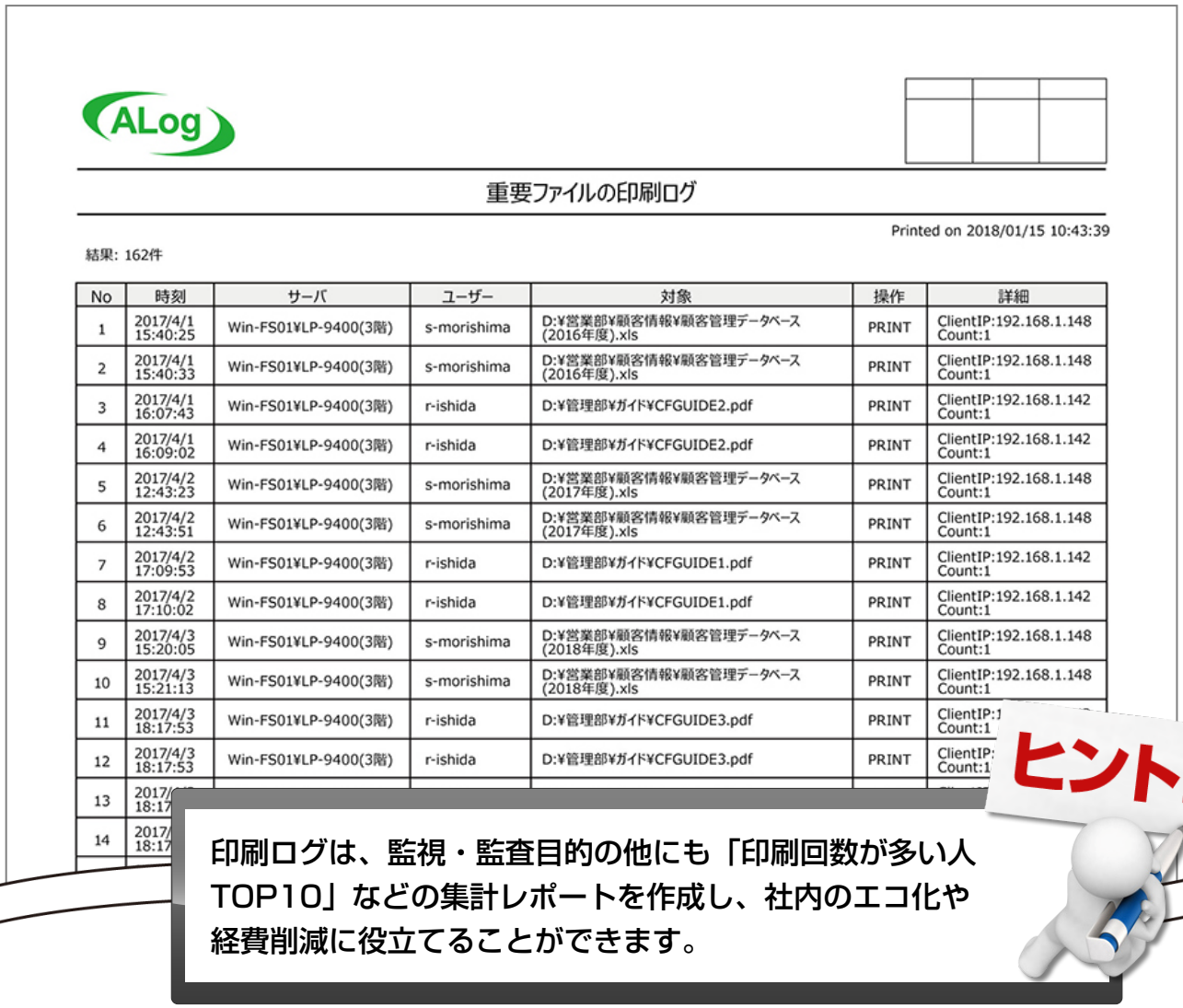
重要ファイルの印刷ログ

監査基準

監査基準（管理要件）	重要な情報を印刷する場合はその記録を残すこと。
監査手続き	重要な情報の印刷に関する記録が保管されていることを確認する。
前提条件	重要な情報に類するファイルが特定できること。
監査対象	プリントサーバ
監査レポート	重要ファイルの印刷ログ【ALog ConVerter】
評価指標（確認項目）	重要な情報の印刷に関する記録が 保管されている・・・・適合 保管されていない・・・不適合

監査レポート（サンプル）

※本レポートはALog ConVerter for Windows のみの機能です。



ALog

重要ファイルの印刷ログ

Printed on 2018/01/15 10:43:39

結果: 162件

No	時刻	サーバ	ユーザー	対象	操作	詳細
1	2017/4/1 15:40:25	Win-FS01¥LP-9400(3階)	s-morishima	D:¥営業部¥顧客情報¥顧客管理データベース(2016年度).xls	PRINT	ClientIP:192.168.1.148 Count:1
2	2017/4/1 15:40:33	Win-FS01¥LP-9400(3階)	s-morishima	D:¥営業部¥顧客情報¥顧客管理データベース(2016年度).xls	PRINT	ClientIP:192.168.1.148 Count:1
3	2017/4/1 16:07:43	Win-FS01¥LP-9400(3階)	r-ishida	D:¥管理部¥ガイド¥CFGUIDE2.pdf	PRINT	ClientIP:192.168.1.142 Count:1
4	2017/4/1 16:09:02	Win-FS01¥LP-9400(3階)	r-ishida	D:¥管理部¥ガイド¥CFGUIDE2.pdf	PRINT	ClientIP:192.168.1.142 Count:1
5	2017/4/2 12:43:23	Win-FS01¥LP-9400(3階)	s-morishima	D:¥営業部¥顧客情報¥顧客管理データベース(2017年度).xls	PRINT	ClientIP:192.168.1.148 Count:1
6	2017/4/2 12:43:51	Win-FS01¥LP-9400(3階)	s-morishima	D:¥営業部¥顧客情報¥顧客管理データベース(2017年度).xls	PRINT	ClientIP:192.168.1.148 Count:1
7	2017/4/2 17:09:53	Win-FS01¥LP-9400(3階)	r-ishida	D:¥管理部¥ガイド¥CFGUIDE1.pdf	PRINT	ClientIP:192.168.1.142 Count:1
8	2017/4/2 17:10:02	Win-FS01¥LP-9400(3階)	r-ishida	D:¥管理部¥ガイド¥CFGUIDE1.pdf	PRINT	ClientIP:192.168.1.142 Count:1
9	2017/4/3 15:20:05	Win-FS01¥LP-9400(3階)	s-morishima	D:¥営業部¥顧客情報¥顧客管理データベース(2018年度).xls	PRINT	ClientIP:192.168.1.148 Count:1
10	2017/4/3 15:21:13	Win-FS01¥LP-9400(3階)	s-morishima	D:¥営業部¥顧客情報¥顧客管理データベース(2018年度).xls	PRINT	ClientIP:192.168.1.148 Count:1
11	2017/4/3 18:17:53	Win-FS01¥LP-9400(3階)	r-ishida	D:¥管理部¥ガイド¥CFGUIDE3.pdf	PRINT	ClientIP:1 Count:1
12	2017/4/3 18:17:53	Win-FS01¥LP-9400(3階)	r-ishida	D:¥管理部¥ガイド¥CFGUIDE3.pdf	PRINT	ClientIP: Count:1
13	2017/ 18:17					
14	2017/ 18:17					

ヒント!

印刷ログは、監視・監査目的の他にも「印刷回数が多い人TOP10」などの集計レポートを作成し、社内のエコ化や経費削減に役立てることができます。

退職予定者のアクセス状況

監査基準

監査基準（管理要件）	従業員の異動や退職、契約の変更または終了等の際、営業秘密および個人情報等の不正使用が起こらないよう適切な安全管理措置を取ること。
監査手続き	従業員の異動や退職、契約の変更または終了にあたって組織が実施している対策を確認し、その妥当性を評価する。
前提条件	（なし）
監査対象	ファイルサーバ, データベースサーバ, プリントサーバ　等
監査レポート	退職予定者のアクセス状況【ALog ConVerter】
評価指標（確認項目）	監査レポートが退職予定者等の不正行為を 監視できるものである・・・・適合 監視できない・・・・・・・・・不適合

監査レポート（サンプル）

ALog

退職予定者のアクセス状況

Printed on 2018/01/15 10:57:37

結果: 17件

No	時刻	サーバ	ユーザー	対象	操作	詳細
1	2017/4/1 15:40:05	Win-FS01¥ LP-9400(3階)	s-morishima	D:¥営業部¥顧客情報¥顧客管理データベース(2015年度).xls	PRINT	ClientIP:192.168.1.148 Count:1
2	2017/4/1 16:07:42	Win-FS01¥ LP-9400(3階)	s-morishima	D:¥営業部¥顧客情報¥顧客管理データベース(2016年度).xls	PRINT	ClientIP:192.168.1.148 Count:1
3	2017/4/1 16:13:08	Win-FS01¥ LP-9400(3階)	s-morishima	D:¥営業部¥顧客情報¥顧客管理データベース(2017年度).xls	PRINT	ClientIP:192.168.1.148 Count:1
4	2017/4/1 18:41:54	Win-FS01¥ LP-9400(3階)	s-morishima	D:¥営業部¥顧客情報¥顧客管理データベース(2018年度).xls	PRINT	ClientIP:192.168.1.148 Count:1
5	2017/4/8 11:58:08	Win-FS01	AMIYA.CO.JP¥suzuki	D:¥管理部¥社内¥就業規則.doc	WRITE-Failure	ClientIP:172.20.1.238 Count:11
6	2017/4/8 11:59:16	Win-FS01	AMIYA.CO.JP¥suzuki	D:¥管理部¥一般書類テンプレート¥届出フォーム(労務)¥届出書(勤怠).doc	WRITE-Failure	ClientIP:172.20.1.238 Count:11
7	2017/4/10 10:22:52	Win-FS01	AMIYA.CO.JP¥suzuki	D:¥管理部¥一般書類テンプレート¥届出フォーム(労務)¥通勤費支給申請書.doc	WRITE-Failure	ClientIP:172.20.1.238 Count:11
8	2017/4/10 13:15:30	Win-FS01	AMIYA.CO.JP¥suzuki	D:¥管理部¥一般書類テンプレート¥届出フォーム(労務)¥給与仮払申請書.doc	WRITE-Failure	ClientIP:172.20.1.238 Count:11
9	2017/4/10 20:08:38	Win-FS01	AMIYA.CO.JP¥s-morishima	D:¥管理部¥顧客情報¥販売管理一覧.xls	READ-Failure	ClientIP:192.168.1.148 Count:1
10	2017/4/10 20:10:38	Win-FS01	AMIYA.CO.JP¥s-morishima	D:¥管理部¥顧客情報¥顧客管理一覧.xls	READ-Failure	ClientIP:192.168.1.148 Count:1
11	2017/4/10 20:12:01	Win-FS01	AMIYA.CO.JP¥s-morishima	D:¥管理部¥社員情報¥社員給与.xls	READ-Failure	ClientIP:192.168.1.148 Count:1
12	2017/4/10 20:13:33	Win-FS01	AMIYA.CO.JP¥s-morishima	D:¥管理部¥社員情報¥社員給与.xls	READ-Failure	ClientIP:192.168.1.148 Co
13	2017/4/10 20:42:08	Win-FS01	AMIYA.CO.JP¥s-morishima	D:¥管理部¥社員情報¥社員給与.xls	READ-Failure	Cl C
14	2017/4/12 10:51:01	Win-FS01	AMIYA.CO.JP¥suzuki	D:¥管理部¥社内¥就業規則171031.doc	WRITE-Failure	C
15	2017/4/12 11:53:32	Win-FS01	AMIYA.CO.JP¥suzuki	D:¥管理部¥一般書類テンプレート¥届出フォーム	WRITE-Failure	

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。