統合ログ管理システム Logstorage
PCI DSS / IT全般統制への対応例

Infoscience

インフォサイエンス株式会社
プロダクト事業部

Infoscience Corporation
www.infoscience.co.jp info@logstorage.com
Tel: 03-5427-3503 Fax: 03-5427-3889

PCI DSSと統合ログ管理システム

PCI DSS 12の要件

安全なネットワークの構築・維持	
要件１	カード会員データを保護するためにファイアウォールを導入し、最適な設定を維持すること
要件２	システムパスワードと他のセキュリティ・パラメータにベンダー提供のデフォルトを使用しないこと
カード会員データの保護	
要件３	保存されたカード会員データを安全に保護すること
要件４	公衆ネットワーク上でカード会員データを送信する場合、暗号化すること
脆弱性を管理するプログラムの整備	
要件５	アンチウィルス・ソフトウェアまたはプログラムを利用し、定期的に更新すること
要件６	安全性の高いシステムとアプリケーションを開発し、保守すること
強固なアクセス制御手法の導入	
要件７	カード会員データへのアクセスを業務上の必要範囲内に制限すること
要件８	コンピュータにアクセスする利用者毎に個別のＩＤを割り当てること
要件９	カード会員データへの物理的アクセスを制限すること
定期的なネットワークの監視およびテスト	
要件１０	ネットワーク資源およびカード会員データに対する全てのアクセスを追跡し、監視すること
要件１１	セキュリティ・システムおよび管理手順を定期的にテストすること
情報セキュリティ・ポリシーの整備	
要件１２	従業員と契約社員のための情報セキュリティに関するポリシーを整備すること

統合ログ管理システムの適用が有効

Logstorage

要件10と統合ログ管理

PCI DSS準拠に統合ログ管理が求められる理由

項番	要件
10.1	システム・コンポーネントに対するすべてのアクセス（特にルートなどのアドミニストレータ権限を持つユーザによるもの）を個々のユーザーとリンクするための手順を確立する
10.2	すべてのシステム・コンポーネントに対して、以下のイベントを追跡するための手順を確立する 「カード会員データに対する、個人ユーザーによる全てのアクセス」「ルートまたはアドミニストレータ権限を持つ個人が行った全ての操作」「すべての監査証跡へのアクセス」「無効な論理的アクセスの試行」「識別および認証メカニズムの使用」「監査ログの初期化」「システムレベルのオブジェクトの作成と削除」

→ **全てのアクセスを個々のユーザとリンクし、それを追跡するための仕組み作りは、監査証跡（ログ）が点在したままでは不可能。**

（ ⇒ 統合ログ管理 ）

項番	要件
10.5	監査証跡は、改変できないように保護する
10.7	監査証跡履歴は、少なくとも１年は保管、最低３ヶ月間はオンラインで閲覧利用できるようにする

→ **監査証跡（ログ）が点在している状況では、それらを個々に改ざんから守るのは困難。また、機器によってはログを数か月分保管出来ないものも多い。**

（ ⇒ 統合ログ管理 ）

要件10に対するLogstorage適合状況

項番	要件	適合	備考
10.1	システム・コンポーネントに対するすべてのアクセス（特にルートなどのアドミニストレータ権限を持つユーザによるもの）を個々のユーザーとリンクするための手順を確立する	○	Logstorageの柔軟なログ収集機能(syslog/FTP/File/SNMP/Agent/イベントログのAgentレス収集)により、分散するログの一元管理が可能。 また、Logstorageのログフォーマット定義機能により、異なるシステムのログを横断的に検索・分析することが可能。 アドミニストレータ権限によるアクセスと個々のユーザのリンクについては、例えば、そのシステム・コンポーネントに対する操作ログとOS/認証サーバ等の認証ログの突合せにより可能。
10.2	すべてのシステム・コンポーネントに対して、以下のイベントを追跡するための手順を確立する 「カード会員データに対する、個人ユーザーによる全てのアクセス」「ルートまたはアドミニストレータ権限を持つ個人が行った全ての操作」「すべての監査証跡へのアクセス」「無効な論理的　　アクセスの試行」「識別および認証メカニズムの使用」「監査ログの初期化」「システムレベルの　オブジェクトの作成と削除」	○	Logstorageの検索機能により、ログに含まれる全ての情報を切り口とした追跡、分析が可能。 また、ログのトラッキング機能により、検索結果からの再検索・絞込みがマウスのクリック操作で可能。
10.3	すべてのシステム・コンポーネントにおいて、イベントごとに少なくとも次の監査証跡を記録する。 「ユーザID」「イベントのタイプ」「日付と時刻」「成功または失敗の表示」「イベントの起点」「 影響を受けたデータ」「システムコンポーネント」「リソースの識別子もしくは名前」	○	左記の監査証跡がシステム・コンポーネント側で出力されていれば、全てLogstorageに取り込む事が可能。 また、Logstorageのログフォーマット定義機能により、各フィールドに意味づけを行う事が出来るため、異なるフォーマットのログが複数あった　場合でも、「ユーザID」や「日付範囲」でのログ追跡が可能。
10.4	すべての重要なシステム・クロックと実際の時刻を同期させる。	○	Logstorageの機能では無いが、NTPサーバを用いて、時刻同期を行う。 また、システム・コンポーネントによって、出力されるログのタイムゾーンが異なる場合、Logstorageのログ収集時の機能により、タイムゾーンを統一する事が可能。
10.5	監査証跡は、改変できないように保護する	○	ログをリアルタイムでLogstorageに送信する事により、各システム・コンポーネント側でログの改ざんが行われた場合でも、Logstorageで収集したログの原本性は保たれる。 また、Logstorageの改竄検出機能により、ログが改ざんされた／されていない事の検証が可能。
10.6	全てのシステム・コンポーネントのログを、少なくとも一日１回はレビューする。ログのレビューの対象は、intrusion detection system(IDS)とauthentication, authorization, and accounting protocol(AAA)サーバ、（例：RADIUS)のようなセキュリティ機能を果たすサーバを含む。	○	Logstorageの自動出力レポート機能により、各システム・コンポーネントのログの分析・レビューが可能。 また、Logstorageの検知機能により、ポリシー違反時に出力されるログを検知し、アラートをあげる事も可能。
10.7	監査証跡履歴は、少なくとも１年は保管、最低３ヶ月間はオンラインで閲覧利用できるようにする。	○	ログデータに特化したLogstorage独自DB技術を用いた高速検索・集計機能により、大量ログからの追跡も可能。 また、オンライン期間を過ぎたログの自動アーカイブにも対応。

要件10.5(詳細)

要件10.5 監査証跡は、改変できないように保護する

項番	要件	適合	備考
10.5.1	監査証跡の閲覧は、それが業務上必要な人々に制限する	○	Logstorageのグループ・ユーザ管理機能により、ログ閲覧可能な 範囲をシステム・コンポーネントやアプリケーション毎に細かく指定 可能。
10.5.2	監査証跡ファイルは、改ざんされないように保護する	○	ログをリアルタイムでLogstorageに送信する事により、各システム・ コンポーネント側でログの改ざんが行われた場合でも、Logstorage で収集したログの原本性は保たれる。
10.5.3	監査証跡ファイルを、集中ログ・サーバまたは改ざんが難しい媒体に、直ちにバックアップする	○	「集中ログ・サーバ」がLogstorageに相当する。また、Logstorage から、WORMストレージへのログのバックアップも可能。
10.5.4	無線ネットワークのログを、内部のLAN上のログ・サーバにコピーする	○	syslog/FTP/File/SNMP/Agent/イベントログのAgentレス収集のいずれかの方法にて、ログの収集（コピー）が可能。
10.5.5	既存のログ・データが改ざんされた時に必ずアラートが発せられるよう、ログに対してファイルの完全性 監視／変更検知ソフトウェアを使用する（新しいデータの追加に対しては、アラートは起こらない）	○	Logstorageの改竄検出機能により、ログが改ざんされた／されていない事の検証が可能。

PCI DSS対応事例

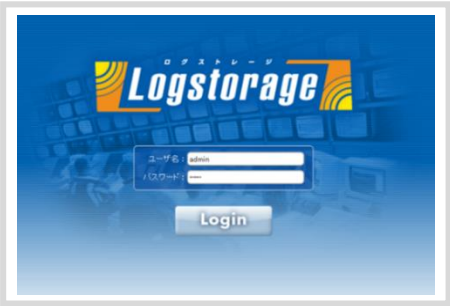
PCI DSS / ログレビューの観点

ログレビューの観点／出力レポート(例)

項番	レポート	PCI	観点
1	認証メカニズムへのアクセス	10.2.5	（レビューは実施しない）
2	ログイン成功一覧	10.2.4	（レビューは実施しない）
3	ログイン失敗一覧	10.2.4	一定時間内に複数回連続してログイン失敗したアクセスを確認する。
4	パスワードの変更履歴一覧	-	パスワード変更の実施履歴を確認する。
5	特権権限への昇格の一覧	10.2.4	特権権限の昇格者と昇格時間を確認し、通常運用における操作で無い場合は、実行コマンドを確認する。
6	管理者権限の操作履歴一覧	10.2.2	通常運用における操作で無い場合は、システム管理責任者に妥当性を確認する。
7	ポリシーの変更の一覧	10.2.2	ポリシーなどが変更されている場合は、システム管理責任者に妥当性を確認する。
8	ログの消去・初期化	10.2.6	イベントログやsyslogが消去されていないか確認する。
9	カード会員データへのアクセスの一覧	10.2.1	カード会員データへのアクセス履歴を確認する。
10	ログへのアクセス履歴の一覧	10.2.3	Logstorageの利用履歴を確認する。 ログレビュー時間外でのアクセスが無い事を確認する。
11	重要なファイルの作成および削除の一覧	10.2.7	システム環境下のファイル作成及び削除履歴を確認する。

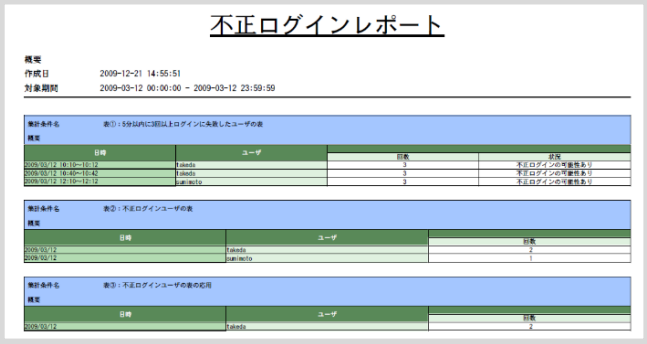
PCI DSS / ログレビューの手順

ログレビューの手順（例）



<ログイン画面>

<レポート履歴画面>



<レポート>

<手順例>

No	手順 （日次）
1	運用担当者は、Logstorage のコンソールにログインする。
2	Logstorage の「レポート」-「レポート作成履歴」を選択し、「レポート作成履歴リスト」画面に遷移する。
3	生成されているレポートの「ファイル名」をクリックし、レポート内容を確認する。
4	問題点を検出した場合は、レポートをシステム管理責任者に送付し、以降の指示を仰ぐ。
5	レポート内容の確認後、「ログレビュー記録」に日付、担当者名などを記入する。
6	「ログレビュー記録」をシステム管理責任者に送付し、承認を得る。

※運用担当者は、原則として毎日10:00-12:00の間に前日分のログの内容を確認する。【PCI:10.6】※運用担当者以外の従業員は、ログの内容を閲覧できるようアカウントは付与しない。【PCI:10.5.1】

問題点未検出

「ログレビュー記録」に日付、担当者名などを記入

「ログレビュー記録」をシステム管理責任者に送付、承認を得る

問題点検出時

問題の内容をシステム管理責任者に送付し、指示を仰ぐ

PCI DSS / 出力レポート例

監査ポリシー変更

概要
作成日　2010-02-24 11:04:48
対象期間　2010-02-24 00:00:00 - 2010-02-24 23:59:59

検索条件名　監査ポリシー変更
概要
件数　2件

ﾀｲﾑｽﾀﾝﾌﾟ	ユーザ名	説明
2010-02-24 10:46:17	inamura	監査ポリシーの変更: 新しいポリシー: 成功 失敗 + - ログオン/ログオフ - - オブジェクト アクセス - - 特権の使用 - - アカウント管理 + - ポリシーの変更 - - システム - - 詳細追跡 - - ディレクトリ サービスのアクセス + +
2010-02-24 10:46:34	inamura	監査ポリシーの変更: 新しいポリシー: 成功 失敗 + - ログオン/ログオフ - - オブジェクト アクセス + - 特権の使用 - - アカウント管理 + - ポリシーの変更 - - システム - - 詳細追跡 - - ディレクトリ サービスのアクセス + +

＜ 監査ポリシーの変更 ＞

不正ログインレポート

概要
作成日　2009-12-21 14:55:51
対象期間　2009-03-12 00:00:00 - 2009-03-12 23:59:59

集計条件名　表①：5分以内に3回以上ログインに失敗したユーザの表
概要

日時	ユーザ	回数	状況
2009/03/12 10:10~10:12	takeda	3	不正ログインの可能性あり
2009/03/12 10:40~10:42	takeda	3	不正ログインの可能性あり
2009/03/12 12:10~12:12	sumimoto	3	不正ログインの可能性あり

集計条件名　表②：不正ログインユーザの表
概要

日時	ユーザ	回数
2009/03/12	takeda	2
2009/03/12	sumimoto	1

集計条件名　表③：不正ログインユーザの表の応用
概要

日時	ユーザ	回数
2009/03/12	takeda	2

＜ 不正ログインレポート ＞

IT全般統制と統合ログ管理システム

IT全般統制とログ管理 [1/2]

システム管理基準 追補版（財務報告に係るIT統制ガイダンス）

■運用の実施記録、ログの採取と保管

「情報システムはアクセス記録を含む運用状況を監視することが望ましく、また情報セキュリティインシデントを記録し、一定期間保管すること」「情報システムで発生した問題を識別するために、システム運用の作業ログ・障害の内容ログ及び原因ログを記録し、保管すること」「取得されたログは内容が改ざんされないように保管すること」が望ましい。

■統制の例

情報システムとデータ処理について、企業にログ採取・分析についての方針があり、それに基づいてログが採取されて、必要な項目がモニタリングされている。

■統制評価手続きの例(リスク：運用時の不正な操作を発見できない)

企業に、ログ採取に関する方針があることを確かめる。次に、必要なログ（不正操作等のモニタリングに必要な項目）が記録され、保管されていること、また、保存されたログを利用できることを確かめる。

■統制の例

情報システムとデータ処理のログが取得されて、ログファイルの完全性、正確性、正当性を保証される（ログが改ざんされずに記録され、保管されている）。

■統制評価手続きの例(リスク：情報システムが処理するデータの信頼性が保証されない)

ログの記録や保管に際して、改ざんや削除ができないかについて確かめる。（例えば、情報システムとデータ処理に関する操作状況を調査する。調査した時間帯のログのサンプルを取得する。入手したサンプルをもとに、取得されたログの完全性と正確性を確かめる）。

IT全般統制とログ管理 [2/2]

代表的な統制としてのログ管理

ログ管理は、他のＩＴ全般統制項目の代替的な統制手段としても用いられる。

例えば、「アクセスコントロール」の不備により、財務諸表監査に影響を及ぼす下記のようなケース。

財務諸表データが格納されているデータベースへのアクセスに関する不備

不備の例１） データベース管理用アカウントが複数担当者で共有されている

不備の例２） 本来必要のないユーザに対して、データベースへのアクセス権限が与えられている

不備の例３） データベースへのアクセス権限を持つ社員のアカウントが、退職後も残っていた

有効なアプリケーション統制下の財務諸表データであっても、上記ＩＴ全般統制の不備により、処理後にデータが変更可能な状態にあったと考えられ、信頼性が失われていると見なされる。

上記のような不備があった場合でも、適切にログが保存・管理されていれば、財務諸表データに不要な変更が加えられていないか、ログを使って検証する事も可能。

↓

検証には、**ログのトレーサビリティ** が実現されているかどうかが重要！

IT全般統制対応事例

ログレビューの観点／出力レポート(例)

項番	レポート	観点
1	ログイン成功一覧	ローカル／ネットワーク越しからのログイン成功履歴を確認する。
2	ログイン失敗一覧	ローカル／ネットワーク越しからのログイン失敗履歴を確認する。
3	パスワードの変更履歴	パスワード変更の実施履歴を確認する。
4	特権権限への昇格の一覧	特権権限の昇格者と昇格時間を確認し、通常運用における操作で無い場合は、操作履歴を確認する。
5	特権権限での操作履歴	特権権限での操作履歴を確認する。
6	機密情報／個人情報へのアクセス一覧	機密情報／個人情報へのアクセス履歴を確認する。
7	アカウントの登録／削除	アカウントの登録／削除、権限変更の履歴を確認する。
8	ポリシーの変更の一覧	ポリシーなどが変更されている場合は、管理責任者に妥当性を確認する。
9	パスワードの変更履歴	パスワード変更の実施履歴を確認する。
10	システム障害履歴	システム障害ログの履歴を確認する。

※その他、ログの非改ざんの証明、ログの暗号化が求められる。
※ログレビューの手順は、PCI DSS対応と同様。

重要ファイルへのアクセスレポート

Windows監査1/30(監査対象のみ)

作成日:2006/2/10

概要:監査対象ファイルに対するアクセス数

監査対象リソース名:¥¥ファイルサーバー1¥部内共有¥プロダクト事業部¥顧客情報.xls

集計結果

社員ID	部署	氏名	ユーザ名	アクセス数
11200	経理部	遠藤	endo	144
11002	経理部	榎本	enomoto	93
10002	総務部	高橋	t_takahashi	76
13002	第二営業部一課	田中	tanaka	75
13010	第二営業部一課	末武	suetake	57
-	-	未登録	guest	32
10001	総務部	佐々木	sasaki	30
19001	人事部	千葉	chiba	29
15001	プロダクト開発	佐伯	saeki	24
15002	プロダクト開発	鈴木	suzuki	19
15003	プロダクト開発	斉藤	saito	15
15004	プロダクト開発	高橋	takahashi	3
15005	プロダクト開発	根本	nemoto	2
15006	プロダクト開発	小長谷	konagaya	1
13001	第二営業部二課	浅野	asano	1
13021	第二営業部一課	日野	hino	1
15201	プロダクト開発	塩谷	shioya	1
15211	プロダクト開発	水上	mizukami	1
15209	プロダクト開発	安達	adachi	1
16001	マーケティング部	杉山	sugiyama	1
16003	マーケティング部	青山	aoyama	1

合計 607

ログのトレーザビリティ

※【PCI :10.1】 にも対応

検索条件 | 検索結果 | カラムセットアサイン

ログ | カラム　1-37件目表示 (全37件)　1

タイムスタンプ	ユーザID	アプリケーション	アクション	操作種別	対象	ログメッセージ
2021-11-29 08:56:00	suzuki	e-SG	カード認証OK(入室)		(01011001)(扉1-1)	e-SG: 9,カード認証OK
2021-11-29 08:58:27	suzuki	SKYSEA16_3	起動・終了	ログオン	SUZUKI-PC	SKYSEA16_3(time=725
2021-11-29 08:58:27	suzuki	SKYSEA16_3	起動・終了	操作開始	SUZUKI-PC	SKYSEA16_3(time=96):
2021-11-29 10:24:37	suzuki	SKYSEA16_3	起動・終了	操作終了	SUZUKI-PC	SKYSEA16_3(time=96):
2021-11-29 10:25:00	suzuki	e-SG	カード認証OK(退室)		(01011001)(扉1-1)	e-SG: 8,カード認証OK
2021-11-29 10:29:00	suzuki	e-SG	カード認証OK(入室)		(01011001)(扉1-1)	e-SG: 9,カード認証OK
2021-11-29 10:30:00	suzuki	SKYSEA16_3	起動・終了	操作開始	SUZUKI-PC	SKYSEA16_3(time=96):
2021-11-29 10:31:00	suzuki	SKYSEA16_3	ファイル操作	ファイルコピー	C:¥work¥顧客登録CSVデータ.csv	SKYSEA16_3(time=283
2021-11-29 11:29:42	suzuki	IWAMforMEAP	プリント		PDT0613C.pdf	IWAMforMEAP: "プリン
2021-11-29 11:29:42	suzuki	SKYSEA16_3	プリント		PDT0613C.pdf	SKYSEA16_3: EC2AMA
2021-11-29 12:02:09	suzuki	SKYSEA16_3	起動・終了	操作終了	SUZUKI-PC	SKYSEA16_3(time=96):
2021-11-29 12:03:00	suzuki	e-SG	カード認証OK(退室)		(01011001)(扉1-1)	e-SG: 8,カード認証OK
2021-11-29 12:49:00	suzuki	e-SG	カード認証OK(入室)		(01011001)(扉1-1)	e-SG: 8,カード認証OK
2021-11-29 12:57:00	suzuki	SKYSEA16_3	起動・終了	操作開始	SUZUKI-PC	SKYSEA16_3(time=96):

いつ　誰が　どうした　どこで/何に対して

IT全般統制 / 作業申請ログと実作業ログの突合 [1/2]

作業申請内容と作業ログの突合

① 作業者は対象サーバへの作業申請を行う

② 承認者は申請内容の承認を行う
－承認後、申請内容ログをログストレージが収集

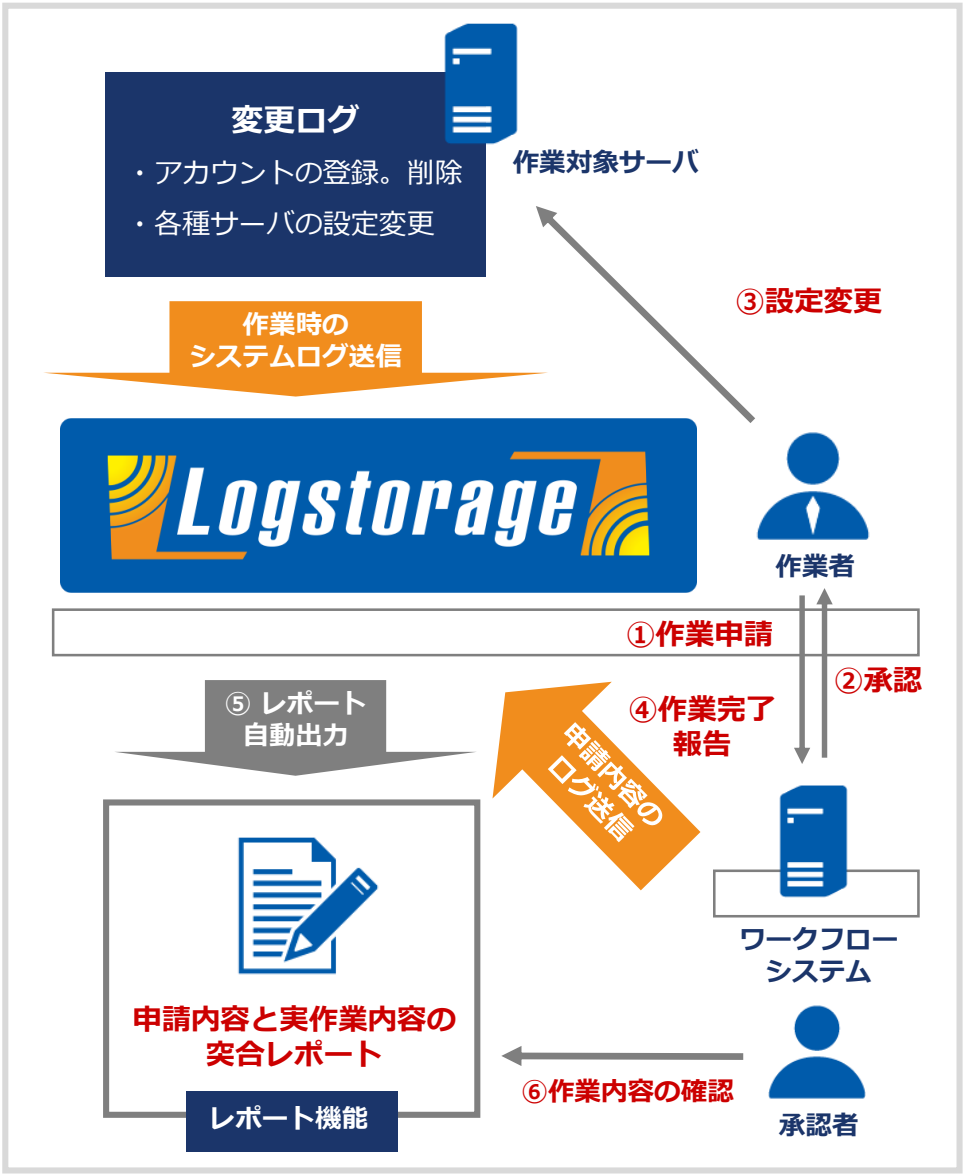
③ 作業者は対象サーバに対して作業を行う
－作業中のアクセスログをログストレージが収集

④ 作業者は作業完了後、作業完了報告を行う

⑤ Logstorageのレポート機能を利用し、作業中のアクセスログ及び申請内容ログの突合せをレポートする。

⑥ 承認者はレポートの内容を確認し、申請外の作業が実施されていない事を確認する。

- 申請時間外に作業が行われていないか
- 申請されたアカウントで作業が行われていたか



IT全般統制 / 作業申請ログと実作業ログの突合 [2/2]

Logstorage

ワークフロー側 （申請情報）	サーバ側 （実作業情報）
・作業時に利用するユーザID ・作業時間 FROM-TO	・ログインユーザID ・ログイン時間

突合レポート

OraServ01へのアクセス

概要　DBサーバ(OraServ01)へのアクセスログと申請情報の突合レポート
作成日　2009-05-25 10:31:53
対象期間　2009-03-12 00:00:00 - 2009-03-12 23:59:59

集計条件名　ログ中に申請のない人が存在する
概要

日時	ユーザ	申請時間	状況
2009/03/12 10:00	inamura	10:00-16:00	OK:申請あり、時間内
2009/03/12 11:00	inamura	10:00-16:00	OK:申請あり、時間内
2009/03/12 11:30	ohashi	11:30-11:50	NG:申請あり、ログインなし
2009/03/12 12:00	konagaya	10:00-16:00	OK:申請あり、時間内
2009/03/12 13:00	nakamura	-	NG:申請なし
2009/03/12 14:00	uchiyama	-	NG:申請なし
2009/03/12 15:00	konagaya	10:00-16:00	OK:申請あり、時間内
2009/03/12 16:00	takeda	-	NG:申請なし
2009/03/12 17:00	inamura	10:00-16:00	NG:申請あり、時間外
2009/03/12 18:00	takeda	-	NG:申請なし
2009/03/12 19:00	nakamura	-	NG:申請なし
2009/03/12 20:00	enomoto	20:00-20:30	NG:申請あり、ログインなし

開発元

インフォサイエンス株式会社
〒108-0023
東京都港区芝浦2-4-1 インフォサイエンスビル
https://www.infoscience.co.jp/

お問い合わせ先

インフォサイエンス株式会社
プロダクト事業部
TEL 03-5427-3503　　FAX 03-5427-3889
https://logstorage.com/
mail : info@logstorage.com