カード会員データへのアクセスの追跡・監視の具体的手法

2014年7月29日

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

Contents

◆設立
1995年10月

◆代表者
宮 紀雄

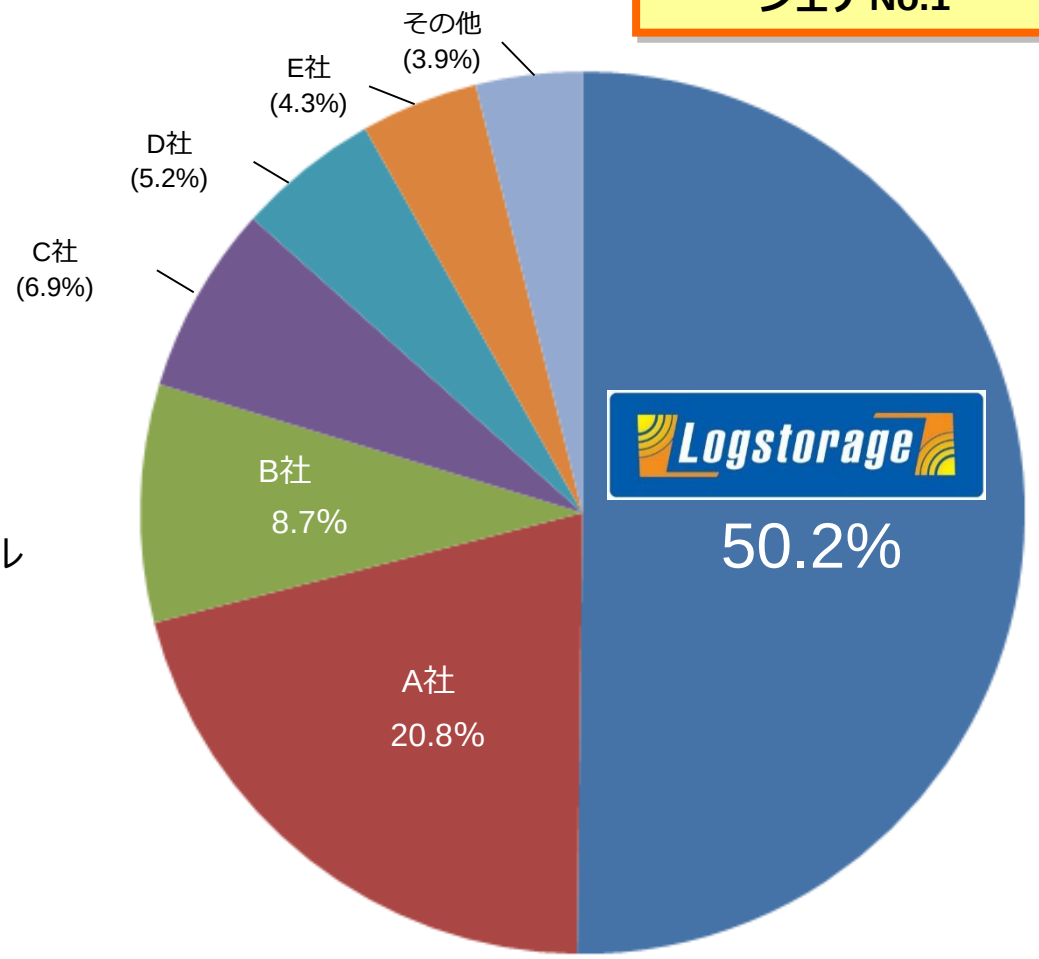
◆資本金
1億円

◆事業内容
- パッケージソフトウェアの開発
- データセンタ運営
- 受託システム開発サービス
- 包括システム運用サービス

◆所在地
東京都港区芝浦2丁目4番1号 インフォサイエンスビル

統合ログ管理システム「Logstorage」

導入社数 7年連続
シェアNo.1



出典：ミック経済研究所「情報セキュリティソリューション市場の現状と将来展望2013(統合ログ管理市場)」

ログ管理の目的とPCI DSS要件

ログ管理の目的

様々なルールや脅威への対応のために、ログの管理が行われている

- 個人情報保護法
- 金融商品取引法
- 不正アクセス禁止法
- 国際ペイメントブランド/PCI DSS
- 経産省/クラウドセキュリティガイドライン
- プライバシーマーク
- ISO27001/ISMS
- APT/標的型攻撃
- 情報漏洩（内部犯行）
- サイバー犯罪捜査

セキュリティ「制御」には限界がある。
「ログ」のモニタリングにより、リスクを早期に発見する。

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

今日のお話
ログ管理

PCI DSS ログ管理要件の確認 - 要件10

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」	
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」	
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。	
10.5	監査証跡は、改変できないように保護する	
	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
	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
	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
	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
	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）
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。	
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。	

ログに関する内容は基本的に「要件10」に書かれている。現状、ログ管理に関してここまで細かく示されているガイドラインは他に無く、カード情報保護に限らずセキュリティガイドラインとして採用する企業もある。

PCI DSS 2.0 – 3.0 要件10の変更点

要件	PCI DSS 2.0	PCI DSS 3.0
10.6	少なくとも日に一度、すべてのシステムコンポーネントのログを確認する。 ログの確認には、侵入検知システム（IDS）や認証、認可、アカウンティングプロトコル（AAA）サーバ（RADIUSなど）のようなセキュリティ機能を実行するサーバを含める必要がある。 注: 要件 10.6 に準拠するために、ログの収集、解析、および警告ツールを使用できる。	すべてのシステムコンポーネントのログとセキュリティイベントを調べ、異常や怪しい活動を特定する。 注: この要件に準拠するために、ログの収集、解析、および警告ツールを使用することができます。
10.6.1	（なし）	毎日一度以上、以下をレビューする • すべてのセキュリティイベント • カード会員データ(CHD)や機密認証データ(SAD)を保存、処理、または送信する、またはCHDやSADのセキュリティに影響を及ぼす可能性のあるすべてのシステムコンポーネントのログ • すべての重要なシステムコンポーネントのログ • すべてのサーバとセキュリティ機能を実行するシステムコンポーネント（ファイアウォール、IDS/IPS、認証サーバ、電子商取引リダイレクションサーバなど）のログ
10.6.2	（なし）	組織のポリシー、および年間リスク評価によって決定されたリスク管理戦略に基づいて他のシステムコンポーネントすべてのログを定期的にレビューする。
10.6.3	（なし）	レビュープロセスで特定された例外と異常をフォローアップする。
10.8	（なし）	ネットワークリソースとカード会員データへのすべてのアクセスを監視するためのセキュリティポリシーと操作手順が文書化され、使用されており、影響を受ける関係者全員に知られていることを確認する。

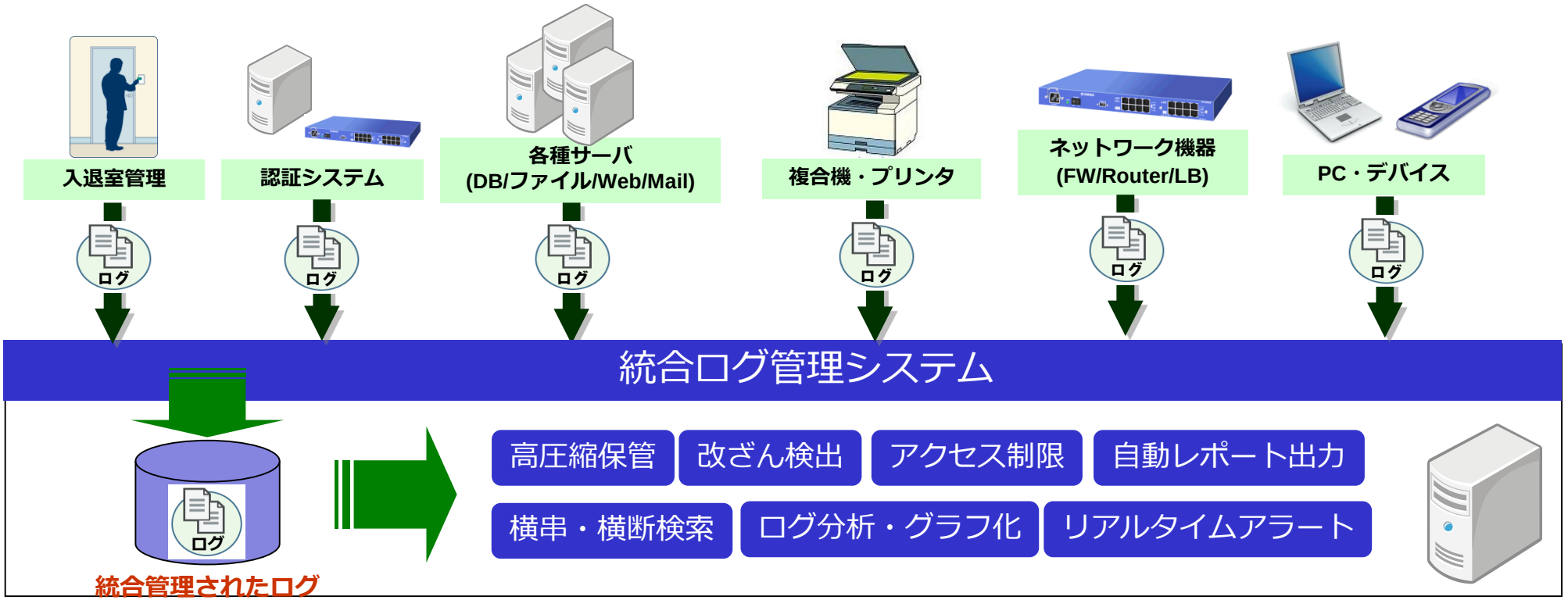
要件10.6 の詳細化が中心。
どのように、ログのレビューを効率化するのか？

ログの収集・保管

「ログ管理」と「統合ログ管理」

【PCI：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

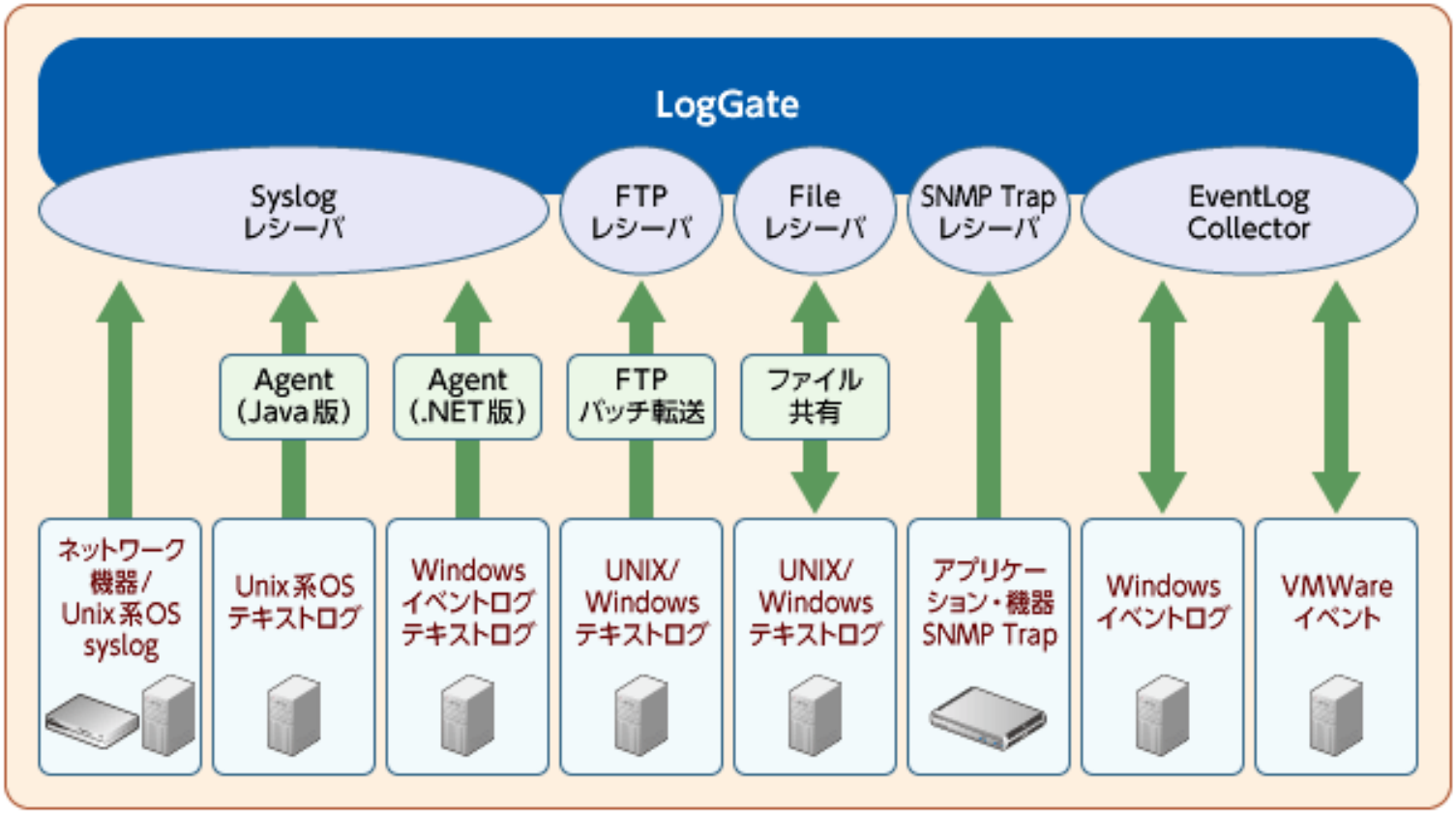
【PCI：10.4 】
すべての重要なシステム・クロックと実際の時刻を同期させる



ログの収集方法

【PCI : 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

【PCI : 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



統合ログ管理システム「Logstorage」のログ収集機能例

【PCI：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

求められる機能：ログ毎の閲覧権限設定

設定例	
DB管理者グループ	DBサーバの全てのログを閲覧可能。
運用管理者グループ	全サーバのシステムログのみ閲覧可能。 DBアクセスログ等は閲覧不可。
ネットワーク管理者グループ	全てのFirewall/Switchのログのみ閲覧可能。 サーバのログは閲覧不可。

【PCI：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

【PCI：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

求められる機能：ログデータの暗号化
ログデータの改ざん検出

ログのモニタリング（１）

- ログ形式の違いの吸収
- Windowsイベントログへの対応

ログ形式の違いの吸収

【PCI : 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

【PCI : 10.2】
すべてのシステム・コンポーネントに対して、イベントを追跡するための手順を確立する

例：ユーザID

入退室管理

タグ:ユーザID

1,カード認証OK ,2007/6/15 08:56,**000500**　山田　太郎,ｶｰﾄﾞ操作記録,ｶｰﾄﾞ:施解錠状態,(01011001)(扉1-1),解錠入室

認証

タグ:ユーザID

SmartOn,SOL,2007/06/15 08:58:27,2131,0,**yamada**,192.168.0.1,PC01,192.168.111.124,SMO01.local,Windowsにログオンしました。

メール

タグ:ユーザID

qmail: May 15 07:15:57 192.168.0.100 qmail: [ID 748625 mail.info] 1239747357.775176 info msg 322844: bytes 15515 from <**yamada@example.com**> qp 2924 uid 7791

DB監査

タグ:ユーザID

"ora104","192.168.0.1",“**domain1¥yamada**","ROOT","ORACLEDBCOLLECT",28,"localhost.localdomain","",10,29177,"Query","2006-06-15 13:04:10","2006-06-15 13:04:10",0,"2006-06-15 13:04:10",1,0,0,2,2,223,486,"select * from user where userid=‘admin' and password="*****“…

ログ形式の違いの吸収

いつ? **誰が?** **どうした?** **何処で?/何に対して?**

ﾀｲﾑｽﾀﾝﾌﾟ	ユーザID	ｱﾌﾟﾘｹｰｼｮﾝ	ｱｸｼｮﾝ	対象
2010-02-15 08:56:00	yamada	e-SG	カード認証OK(入室)	(01011001)(扉1-1)
2010-02-15 08:58:27	yamada	認証ログ	Windows ログオン成功	PC01
2010-02-15 09:17:23	yamada	ApeosPort-Ⅱ	コピー	
2010-02-15 10:24:37	yamada	認証ログ	コンピュータロック	PC01
2010-02-15 10:25:00	yamada	e-SG	カード認証OK(退室)	(01011001)(扉1-1)
2010-02-15 10:29:00	yamada	e-SG	カード認証OK(入室)	(01011001)(扉1-1)
2010-02-15 10:30:00	yamada	認証ログ	コンピュータロック解除	PC01
2010-02-15 10:30:12	yamada	EventLogCollector	ファイル読み込み	顧客名簿2009.doc
2010-02-15 10:30:32	yamada	EventLogCollector	ファイル読み込み	顧客名簿.doc
2010-02-15 10:31:00	yamada	MylogStar	コピー	¥¥192.168.1.123¥共有フォルダ¥持出厳禁¥顧客名簿.doc
2010-02-15 11:29:42	yamada	MylogStar	クライアント(印刷)	PDT0613C.pdf
2010-02-15 11:29:42	yamada	ApeosPort-Ⅱ	プリント	PDT0613C.pdf
2010-02-15 12:02:09	yamada	認証ログ	コンピュータロック	PC01
2010-02-15 12:03:00	yamada	e-SG	カード認証OK(退室)	(01011001)(扉1-1)
2010-02-15 12:49:00	yamada	e-SG	カード認証OK(入室)	(01011001)(扉1-1)
2010-02-15 12:57:00	yamada	認証ログ	コンピュータロック解除	PC01
2010-02-15 13:04:10	yamada	CRM	ログイン	
2010-02-15 13:04:10	yamada	Chakra	参照	user

統合ログ管理システム「Logstorage」のログ検索画面例

共通IDの付与によるログの追跡

統合ログ管理システム

① ログ送信

マスタ連携フィルタ

② 共通ID取得

③ 共通ID付与/ログ保存

ログ

共通IDマスタ

サーバ・機器名	ID	共通ID
ネットワーク機器A	adm001	yamada
メールA	yamada@example.com	yamada
入退出管理	00050	yamada

共通IDを付与したログ

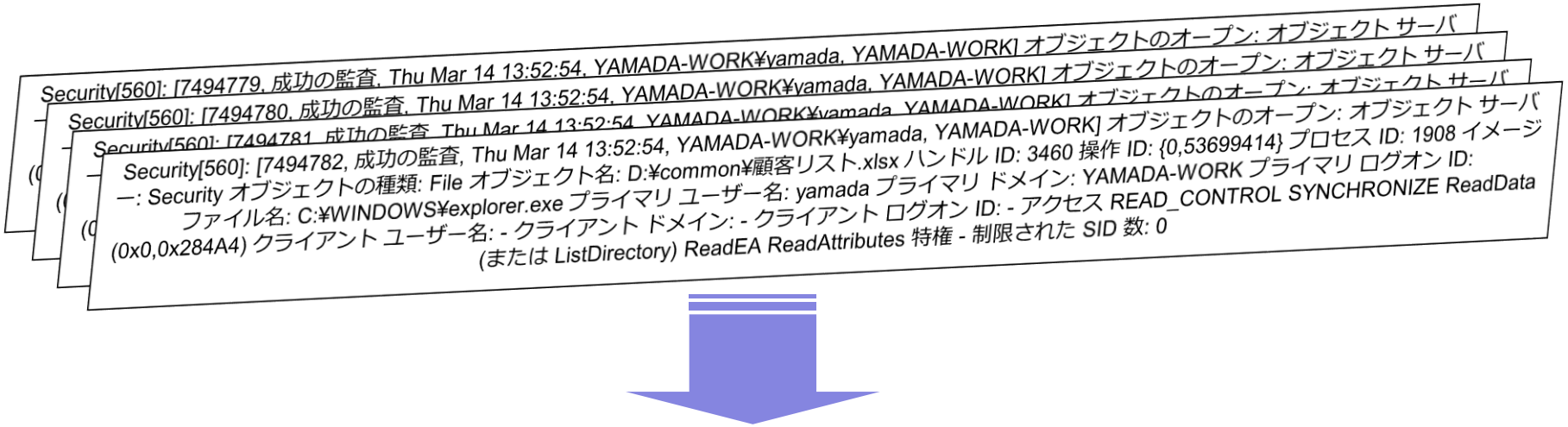
2013/1/15 08:56, 192.168.0.1, 入室しました…00050.., yamada

2013/1/15 08:56,192.168.0.2, yamada, login success…..

2013/1/15 08:56,192.168.0.3, adm001, login failure….., yamada

共通IDを付与し、ログ追跡時のキーとして利用する

Windowsイベントログの生ログは読めない

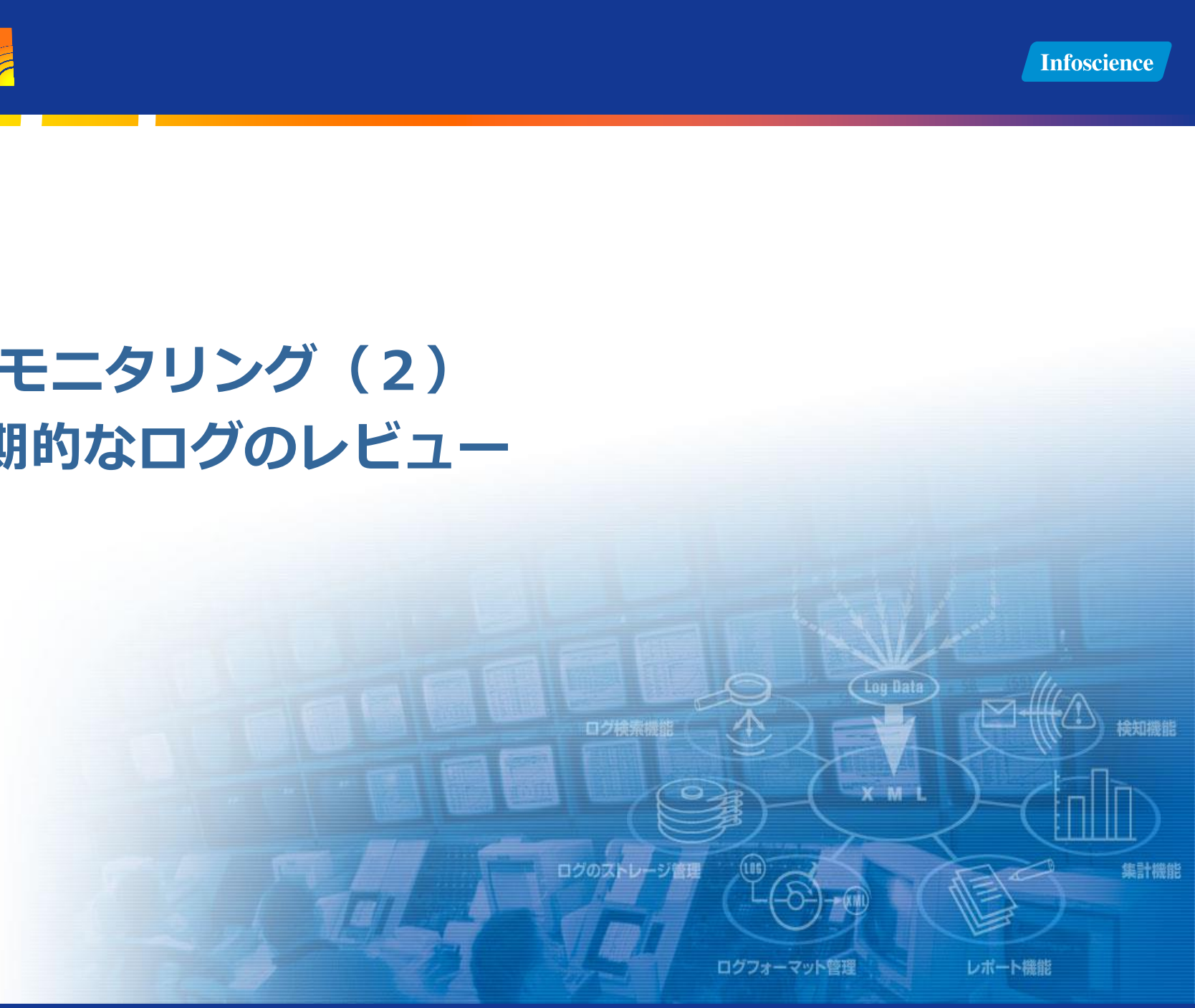


人間が見て理解できる形式への変換が必要

日時	サーバ名	アクション	ドメイン名	ユーザ	接続元ホスト名	接続元IPアドレス	成功／失敗
2013-03-01 00:00:00	FS01	ログオン（ローカル認証）	infoscience	yamada	–	–	成功
2013-03-01 01:00:00	FS01	ログオン（リモート認証）	infoscience	yamada	YAMADA-WORK	192.168.0.1	成功

日時	サーバ名	アクション	ドメイン名	ユーザ	ファイルパス	ファイル名	成功／失敗
2013-03-01 00:00:00	FS01	ファイル読み込み	infoscience	yamada	D:¥common¥	顧客リスト.xls	成功
2013-03-01 01:00:00	FS01	ファイル書き込み	infoscience	yamada	D:¥common¥	顧客リスト.xls	成功
2013-03-01 02:00:00	FS01	ファイルリネーム	infoscience	yamada	D:¥common	コピー ～ 顧客リスト.xlsx	–

ログのモニタリング（２）
- 定期的なログのレビュー



定期的なログのレビュー

【PCI：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。

10.6.1	毎日一度以上、以下をレビューする • すべてのセキュリティイベント • カード会員データ(CHD)や機密認証データ(SAD)を保存、処理、または送信する、またはCHDやSADのセキュリティに影響を及ぼす可能性のあるすべてのシステムコンポーネントのログ • すべての重要なシステムコンポーネントのログ • すべてのサーバとセキュリティ機能を実行するシステムコンポーネント（ファイアウォール,IDS/IPS,認証サーバ,電子商取引リダイレクションサーバなど）のログ
10.6.2	組織のポリシー、および年間リスク評価によって決定されたリスク管理戦略に基づいて他のシステムコンポーネントすべてのログを定期的にレビューする。
10.6.3	レビュープロセスで特定された例外と異常をフォローアップする。
10.8	ネットワークリソースとカード会員データへのすべてのアクセスを監視するためのセキュリティポリシーと操作手順が文書化され、使用されており、影響を受ける関係者全員に知られていることを確認する。

効率的なログレビューをどのように行うのか？

ログレビューの観点

・システムのエラー
・失敗した操作
・ログの消去
・時刻変更
・ユーザ権限の変更
・ポリシーの変更（ファイアウォールのルール、ログの監査設定など）

・**許可**されていない接続元からのアクセス
・**申請**されていないアクセス
・**ルール**違反（USBメモリの使用・クラウドストレージの利用など）
・**通常**とは大きくかけ離れたアクセス数

作業申請と作業ログの突合せ

マスタデータ（作業申請）

ユーザID	作業開始時間	作業終了時間
suzuki	2012/03/21 10:00:00	2012/03/21 12:00:00

突合

ログデータ（サーバログオン・ログオフ）

時刻	ｱｸｼｮﾝ	ユーザID
2012/03/21 13:12:31	ログオン	yamada
2012/03/21 14:49:35	ログオフ	yamada
2012/03/21 10:31:23	ログオン	suzuki
2012/03/21 12:38:21	ログオフ	suzuki

突合レポート

ユーザID	作業開始時間（申請）	作業終了時間（申請）	ログオン時間	ログオフ時間	判定結果
yamada	申請なし	申請なし	2012/03/21 13:12:31	2012/03/21 14:49:35	×
suzuki	2012/03/21 10:00:00	2012/03/21 12:00:00	2012/03/21 10:31:23	2012/03/21 12:38:21	×

申請無しで作業を行っている、申請時間外に作業を行っている

⇒ 突合せ結果「×」

統合ログ管理システム選定上の注意点

ログ管理システム チェックポイント

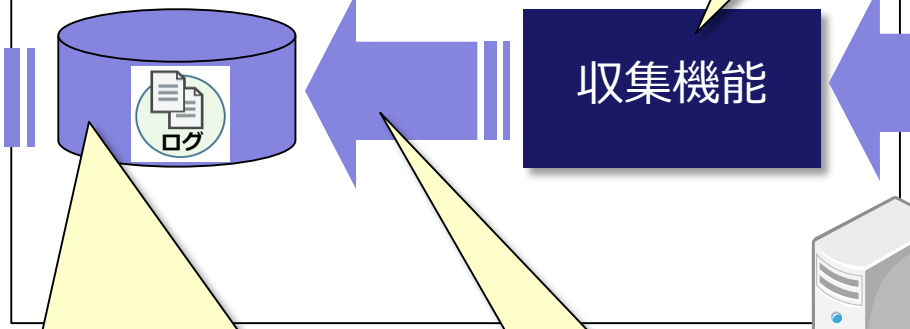
ログと申請データやルールとの
突合せによるレポート出力機能

あらゆるプロトコルの
ログ収集に対応

集計・分析

レポート

検索・追跡



収集したログに対するアクセスコントロール
ログの暗号化・改ざん検出機能

・タグ付け(追跡)
・マスタ連携
・イベントログ解析

ログを収集するための
Agentプログラム

統合ログ管理製品選定上の注意点

○収集できるログに制限はないか？

- クライアントPCのログのみ、syslogのみ、など

○生ログを保管できるか？

- ログ形式を変換しなければならない(原本性が損なわれる)製品には要注意

○製品の将来性・ライフサイクルは？

- 統合ログ管理システムは広くシステムに根を張る為、ディスコンになると悲劇。
- EOSLもチェック。

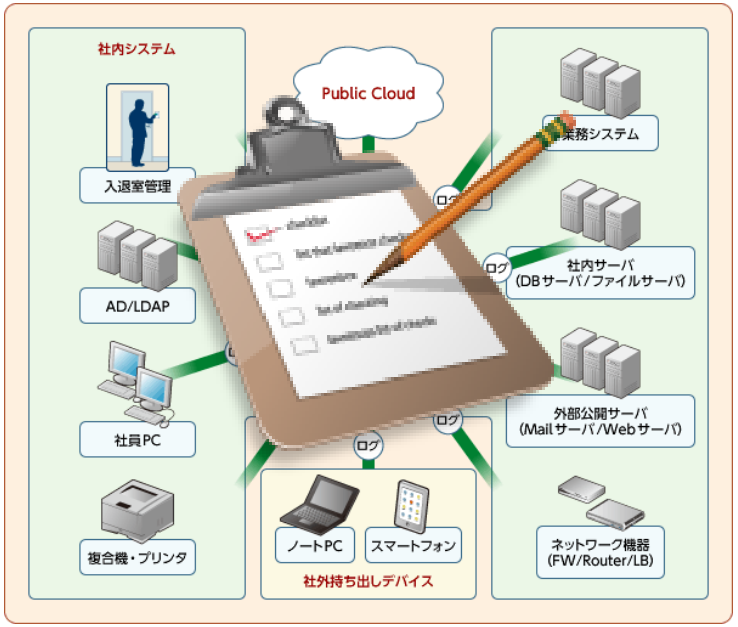
○要件と機能のバランスは取れているか？

- SIEM製品?

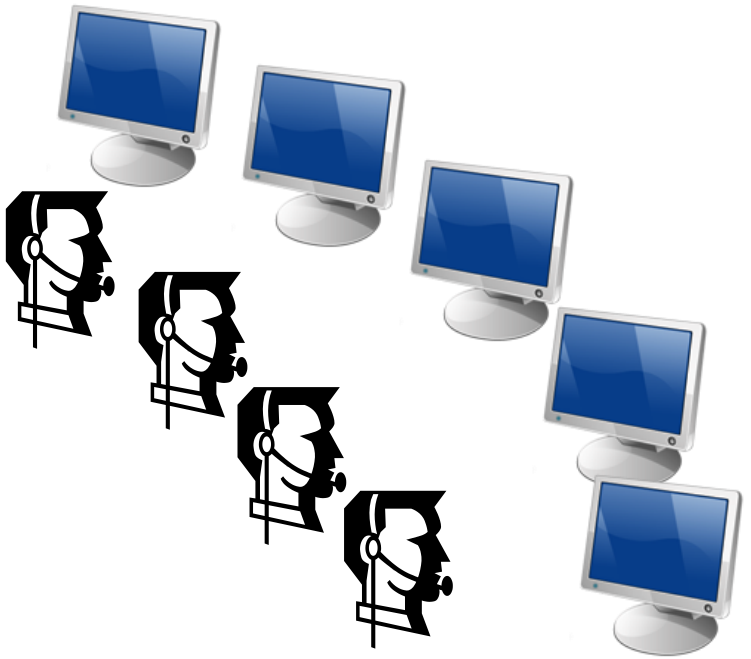
SIEM (Security Information & Event Management)

… SIEMと言えばリアルタイムのセキュリティイベント検知を主眼にしたツールを指し、統合ログ管理ツールとは別ジャンルとされることが多い。ログの蓄積と分析に重きを置くのが統合ログ管理ツール（現在は国産製品が中心に導入が進んでいる）であり、標的型攻撃など新しい脅威への対策に有効だが長期にわたる時間軸での分析には向かないのが、現在海外製品を中心に注目されているSIEMツールと考えればよいだろう。

キーマンズネット「不正行為も一目瞭然！統合ログ管理ツール」 URL：http://www.keyman.or.jp/at/30006863/



統合ログ管理（監査）



SIEM（SOC）

PCI DSS 対応事例

LogstorageのPCI DSS案件例

対象企業	業種	PCI DSS における業態	PCI DSS 準拠対象業務
A社	小売業	加盟店	ネット通販
B社	陸運業	加盟店	予約サイト
C社	小売業	加盟店	ネット通販
D社	小売業	加盟店	ネット通販
E社	小売業	加盟店	ネット通販
F社	ITサービス	加盟店の外部委託先	データセンター事業
G社	ITサービス	加盟店の外部委託先	データセンター事業
H社	金融業	アクワイアラ・イシュア	アクワイアリング・イシュアリング
I社	金融業	アクワイアラ・イシュア	アクワイアリング・イシュアリング
J社	情報・通信業	–	対象業務無し。PCI DSS を社内セキュリティのガイドラインとして利用。
K社	陸運業	加盟店	カード決済
L社	サービス業	加盟店	カード決済
M社	印刷業	加盟店の外部委託先	カード情報を含む印刷業務
N社	金融業	アクワイアラ・イシュア	アクワイアリング・イシュアリング
O社	金融業	アクワイアラ・イシュア	アクワイアリング・イシュアリング
P社	ITサービス	決済代行	決済代行
Q社	コンサル	PCIDSSコンサル	不明
R社	ITサービス	決済代行	決済代行
S社	印刷業	加盟店の外部委託先	カード情報を含む印刷業務
T社	金融業	アクワイアラ・イシュア	アクワイアリング・イシュアリング

主な事業内容：情報システム基盤の企画・設計・構築サービス提供

【PCI DSS 認証取得の目的】
　カード会員データの保管、処理、送信を行うサービスプロバイダが同社のデータセンターを利用する事で、スムーズなPCI DSS準拠を可能とし、新たなビジネスを生み出す。

【統合ログ管理を検討された理由】
　サーバや機器を追加する際、それらのログを収集する仕組みをその都度用意するのは時間もコストも掛かる。また、例えば管理者権限のユーザのログを検索しようとしても、単にログを溜めているだけでは難しい。

【PCI DSS認証取得にあたっての課題】
　PCI DSS対応に必要となる機器やソフトウェアに掛かるコスト。
特に、ログ管理システムについては複数の製品の見積もりを取ってみたが、価格が高いものが多く、認証取得自体を見直す事も考えた程だった。

【Logstorage 選定のポイント】
　同社が必要と考え、PCI DSSで求められるログ管理機能を全て備え、収集・管理を予定していたログについても全て対応実績があった。そして何よりポイントは、低コストで導入できる、費用対効果が高い製品であること。

【導入の結果】

2010年3月 – PCI DSS Ver.1.2 取得
2011年3月 – PCI DSS Ver.2.0 認証取得
※要件10については代替コントロール無し

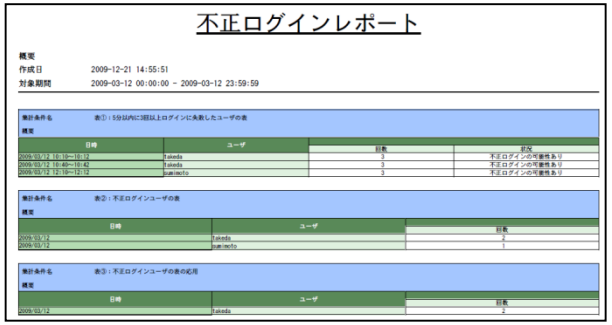
ログレビューの観点/出力レポート例

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）※問題点検出時のみ確認
2	ログイン成功一覧	10.2.4	（レビューは実施しない）※問題点検出時のみ確認
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。

ログレビューの手順

<ログイン画面>

<レポート履歴画面>



<レポート>

<レビュー手順例>

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

END

「カード会員データへのアクセスの追跡・監視の具体的手法」

2014/7/29

インフォサイエンス株式会社 プロダクト事業部
稲村 大介

【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
http://www.logstorage.com/
mail : info@logstorage.com