知らないでは済まされない、ログ管理の本質とは
～ PCI DSS 要件10へのスムーズな対応法 ～

2013年7月10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

1. インフォサイエンスのご紹介
2. ログ管理の目的とPCI DSS
3. 統合ログ管理システム「Logstorage」
4. LogstorageによるPCI DSSログ管理要件への対応
5. PCI DSS 対応事例
6. ログの積極活用への展開

◆設立
1995年10月

◆代表者
宮 紀雄

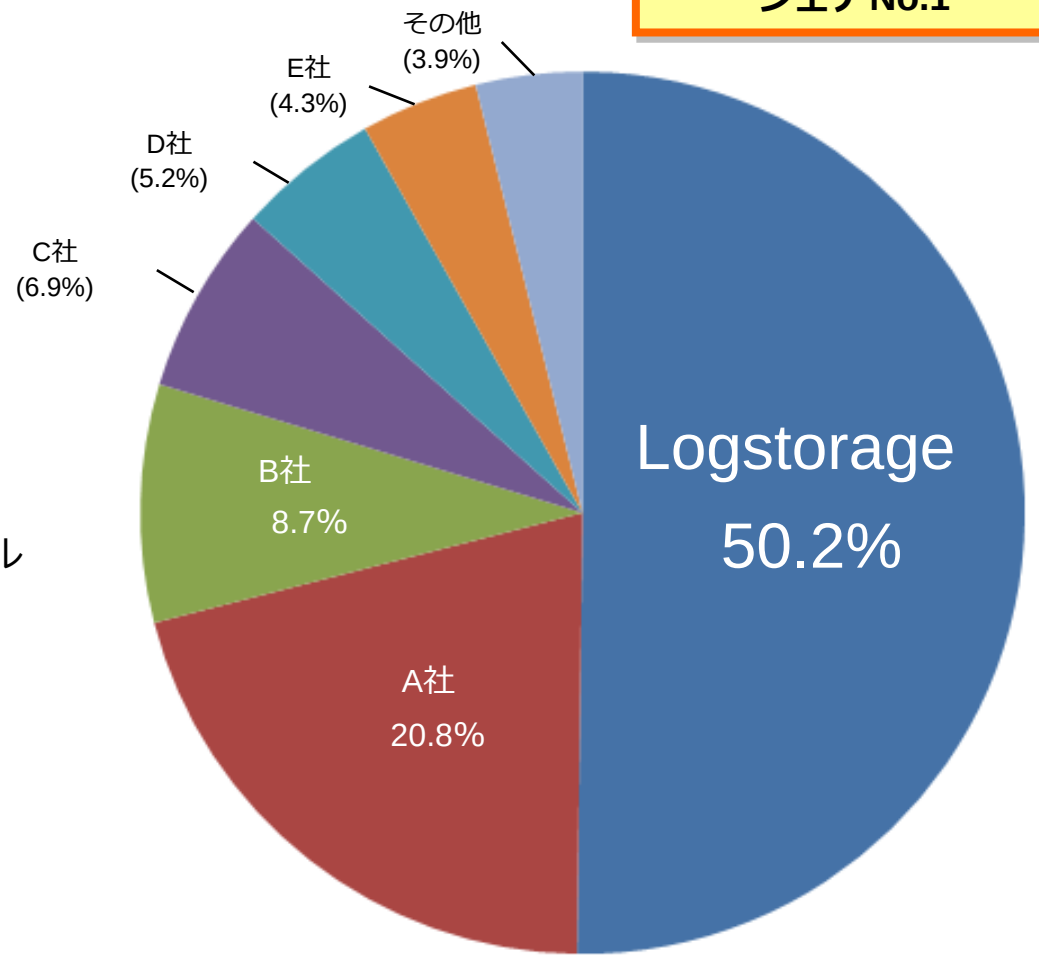
◆資本金
1億円

◆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)」

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

経費削減（複合機のログ分析等）

労務管理（入退室ログ分析等）

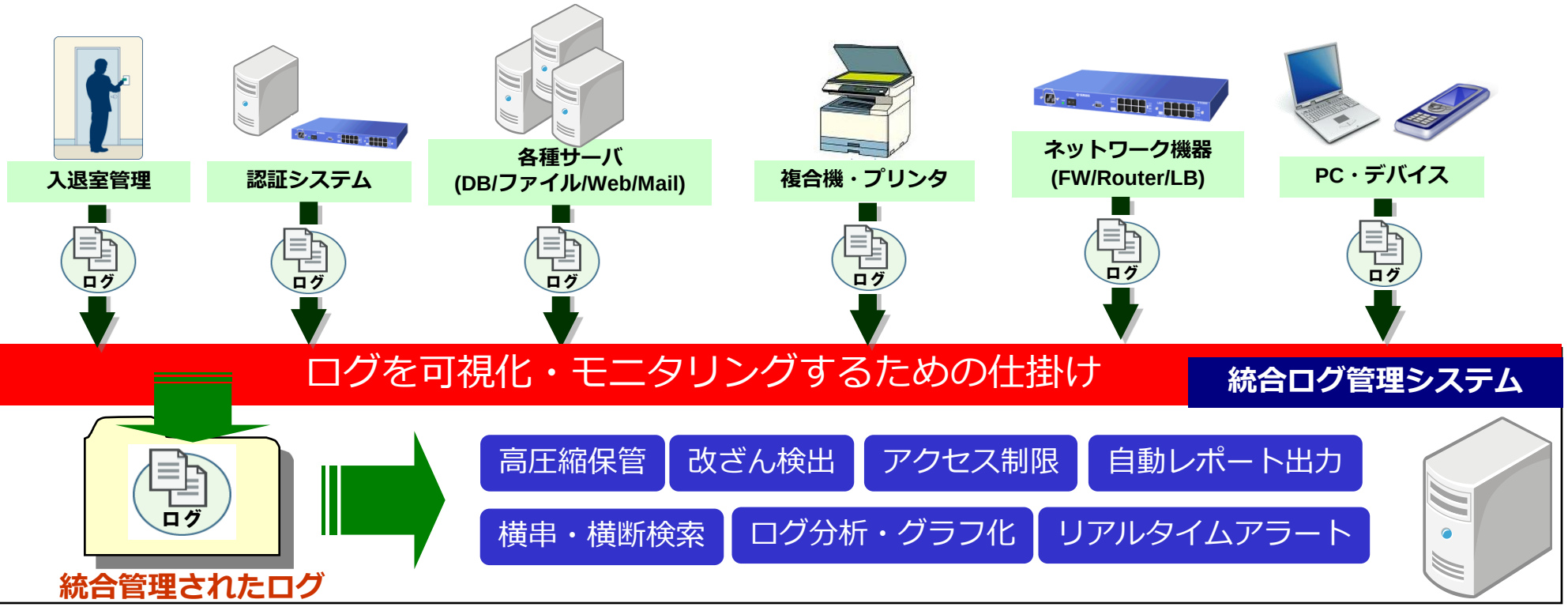
その他・・・

これらの多種多様な要件に対し、「統合ログ管理」が必要な理由は何か？

個別のログ管理から統合ログ管理へ

・ログの「管理」に関わる様々な課題・問題への対応
- サーバ・機器上でログが改ざんされるリスク／ログ保管容量・期間の問題

・ログの「分析」に関わる様々な課題・問題への対応
- ログの可読性／複数ログの追跡性／多様な分析要件



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

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。

統合ログ管理システム「Logstorage」

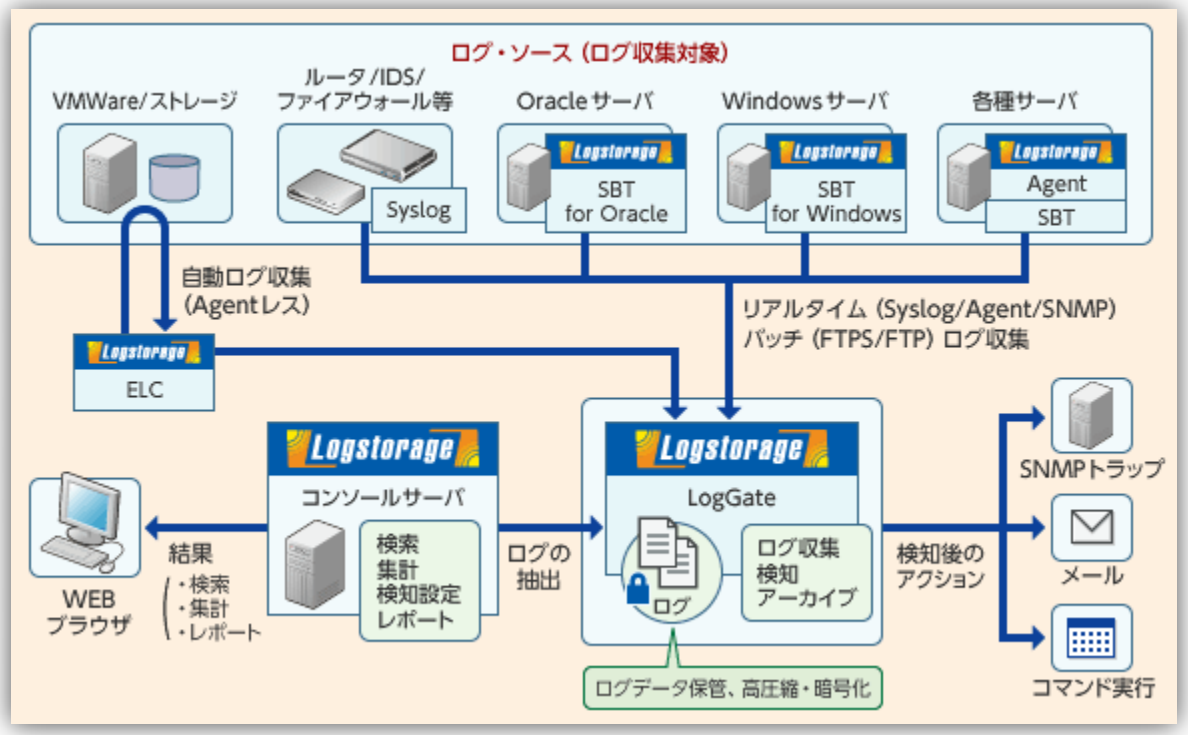
ログ収集機能

[受信機能]
- Syslog / FTP(S) / 共有フォルダ / SNMP

[ログ送信・取得機能]
- Agent
- EventLogCollector
- SecureBatchTransfer

ログ保管機能

- ログの圧縮保存／高速検索
- ログの改ざんチェック機能
- ログに対する意味（タグ）付け
- ログの暗号化保存
- 保存期間を経過したログを自動アーカイブ
- ログの保存領域管理機能



<Logstorage システム構成>

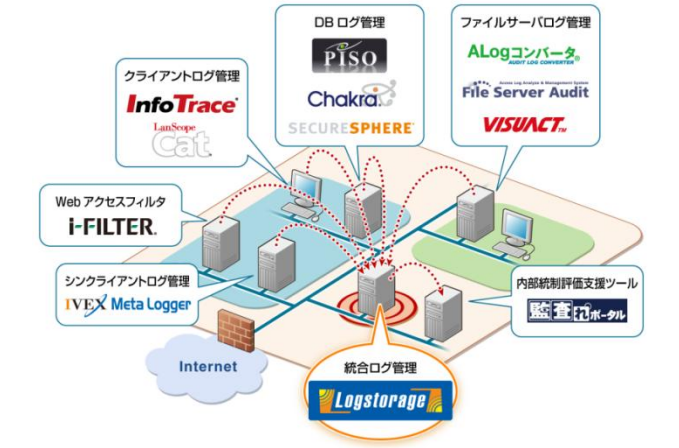
ログ検知機能

- ポリシーに合致したログのアラート
- ポリシーはストーリー的に定義可能(シナリオ検知)

検索・集計・レポート機能

- ログの検索／集計／レポート生成
- 検索結果に対する、クリック操作による絞込み
- レポートの定期自動実行(HTML/PDF/CSV/TXT/XML)
- レポートの出力形式のカスタマイズ

日本国内で利用されているものを中心に250種類以上のログ収集実績



【Logstorage アライアンス製品】

Palo Alto Networks next-generation firewalls	SecureCube / AccessCheck
LanScope Cat	SecureSphere DMG
CWAT	Sendmail
InfoTrace	Auge AccessWatcher
MylogStar	ALog ConVerter
i-FILTER	IVEX Logger シリーズ
SecurePrint!	ARCACLAVIS Revo
Chakra	MaLion3
SSDB監査	VISUACT
AUDIT MASTER	File Server Audit
PISO	監査れポータル

[OSシステム・イベント]
- Windows
- Solaris
- AIX
- HP-UX
- Linux
- BSD

[クライアント操作]
- LanScope Cat
- InfoTrace
- CWAT
- MylogStar
- IVEX Logger
- MaLion3
- 秘文
- SeP
- QND/QOH

[サーバアクセス]
- ALog ConVerter
- VISUACT
- File Server Audit
- CA Access Control

[ICカード認証]
- SmartOn
- ARCACLAVIS　Revo

[運用監視]
- Nagios
- JP1
- Systemwalker
- OpenView

[Lotus Domino]
- Lotus Domino
- Notes AccessAnalyzer2
- Auge AccessWatcher

[Web/プロキシ]
- Apache
- IIS
- BlueCoat
- i-FILTER
- squid
- Delegate
- WebSense
- WebSphere
- WebLogic
- Apache Tomcat
- Cosminexus

[データベース]
- Oracle
- SQLServer
- DB2
- PostgreSQL
- MySQL

[データベース監査ツール]
- PISO
- Chakra
- SecureSphere DMG/DSG
- SSDB監査
- AUDIT MASTER
- IPLocks
- Guardium

[アンチウィルス]
- Symantec AntiVirus
- TrendMicro InterScan
- McAfee VirusScan
- HDE Anti Vuris

[複合機]
- imageRunner
- Apeos
- SecurePrint!

[ネットワーク機器]
- Cisco PIX/ASA
- Cisco Catalyst
- NetScreen/SSG
- PaloAlto PA
- VPN-1
- Firewall-1
- Check Point IP
- SSL-VPN
- FortiGate
- NOKIA IP
- Alteon
- SonicWall
- FortiGate
- BIG-IP
- IronPort
- ServerIron
- Proventia

[メール]
- MS Exchange
- sendmail
- Postfix
- qmail
- Exim

[その他]
- VMware vCenter
- SAP R/3 (ERP)
- NetApp (Storage)
- EMC (Storage)
- ex-SG (入退室管理)
- MSIESER
- iSecurity
- Desk Net's
- HP NonStop Server

…その他

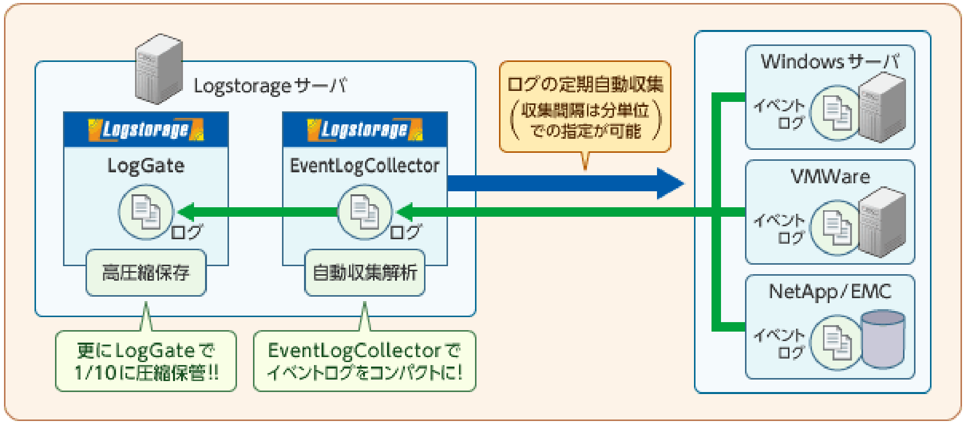
ログ管理・活用に於いて特に重要な２つの事

・生ログをそのまま管理・活用しようとしない

・ログを見るための「軸」を持つ

Windowsイベントログの解析

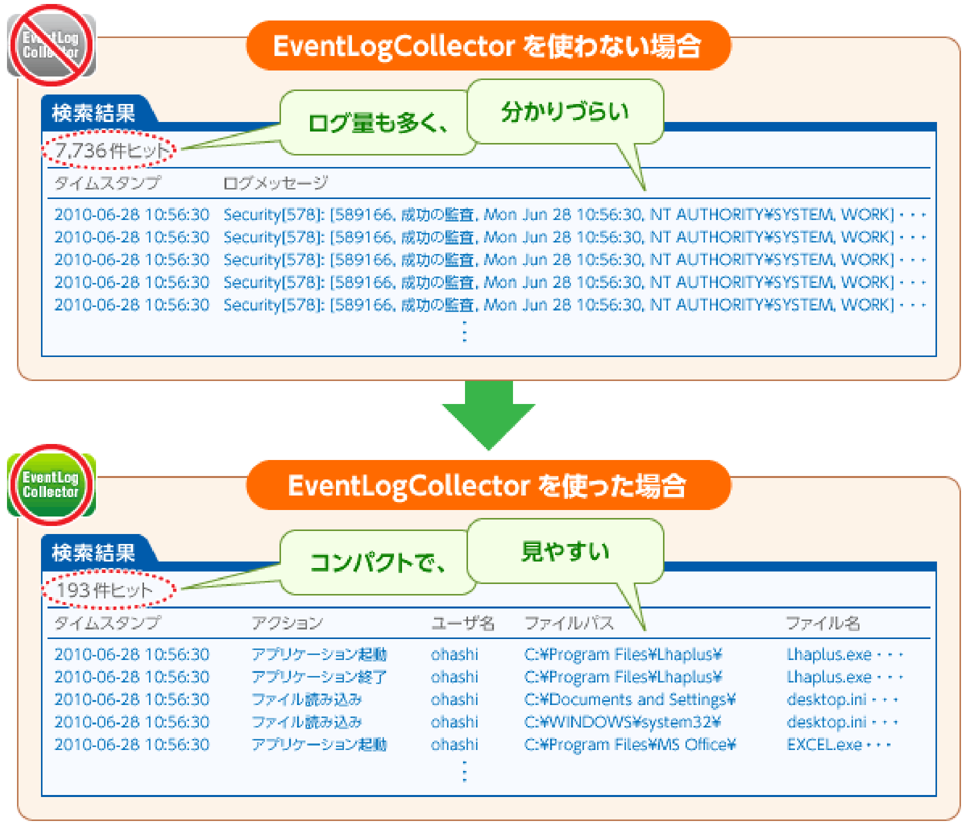
【Logstorage EventLogCollector】



いつもと違う端末からログインしてきているのは誰か?

重要ファイルを削除したのは誰か?

管理者操作がどの端末から行われているのか?



**ファイルアクセスなど、複雑な内容で記録されるWindows
イベントログを、人間が見て理解できる形に解析・変換する**

外部データ連携（URLリスト連携）

元ログ

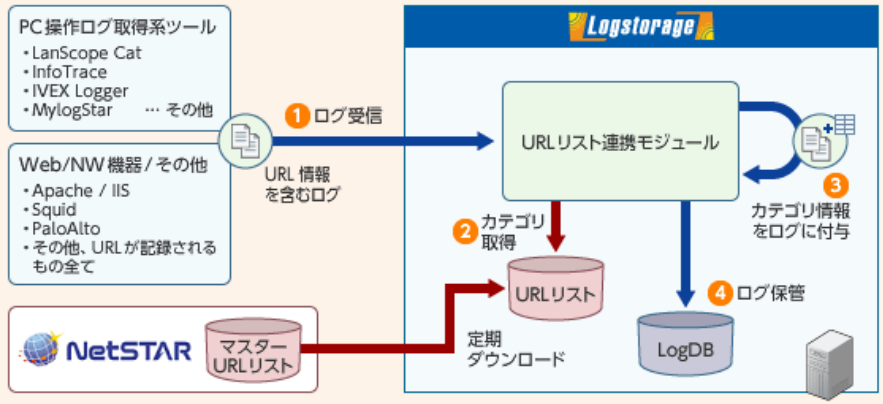
ユーザID	IPアドレス	…	アクセスURL
Yamada	192.168.0.1	…	http://xxx.com
Suzuki	192.168.0.2	…	http://yyy.co.jp
Suzuki	192.168.0.2	…	http://zzz.ne.jp

URLからどのようなWebサイトか判断できないケースが多い

カテゴリ情報付与後ログ

ユーザID	IPアドレス	…	アクセスURL	メインカテゴリ	サブカテゴリ
Yamada	192.168.0.1	…	http://xxx.com	ダウンロード	ストレージサービス
Suzuki	192.168.0.2	…	http://yyy.co.jp	職探し	転職・就職
Suzuki	192.168.0.2	…	http://zzz.ne.jp	コミュニケーション	掲示板

付与されたカテゴリ情報から、Webアクセス状況が見えてくる



突合レポートテンプレート

作業申請・サーバ操作ログ 突合レポート

概要 作業申請で申請された時間帯以外にログオン・ログオフが発生していると、判定結果が「×」となります。
作成日 2012-03-22 5:00:00
対象期間 2012-03-21 00:00:00 - 2012-03-21 23:59:59

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
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	×
yamada			2012-03-21 13:12:31	2012-03-21 14:49:35	×

「基準」の例		実際に発生した事象の記録	「突合」して見つけるもの
作業申請データ	突合	作業対象サーバ上のログ	申請外の作業（申請時間外作業・未申請作業など）
勤務表	突合	入退室管理システムのログ	勤務実態（サービス残業の有無など）
IDカード管理台帳	突合	入退室管理システムのログ	未使用IDカード（退職者の未返却IDカードなど）

ログを有効に活用するには、外部データとの連携、突合せが極めて重要

Logstorageによる
PCI DSS ログ管理要件への対応

ログを追跡可能にする

【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

【ログに記録されるユーザIDの例】

入退室管理

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

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

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

"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="*****“…

ログを追跡可能にする（Logstorage検索画面）

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

システム毎に異なるユーザIDの統一が必要

共通IDの付与によるログの追跡

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

【PCI：10.5】監査証跡は、改変できないように保護する

ログデータの暗号化／非改ざんの証明機能

Logstorage 機能	内容
ログデータの暗号化機能	AES等でログデータを暗号化する機能
ログデータの非改ざん証明機能	ログデータに対応するハッシュ値を持つ事により、改ざんを検出する機能

ログデータに対するアクセスコントロール

Logstorage 機能	内容	
グループ・ユーザ管理機能	ログ毎に閲覧権限を設定する機能。 【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。

仮想環境に於けるログ管理の注意点

Information Supplement: PCI DSS Virtualization Guidelines

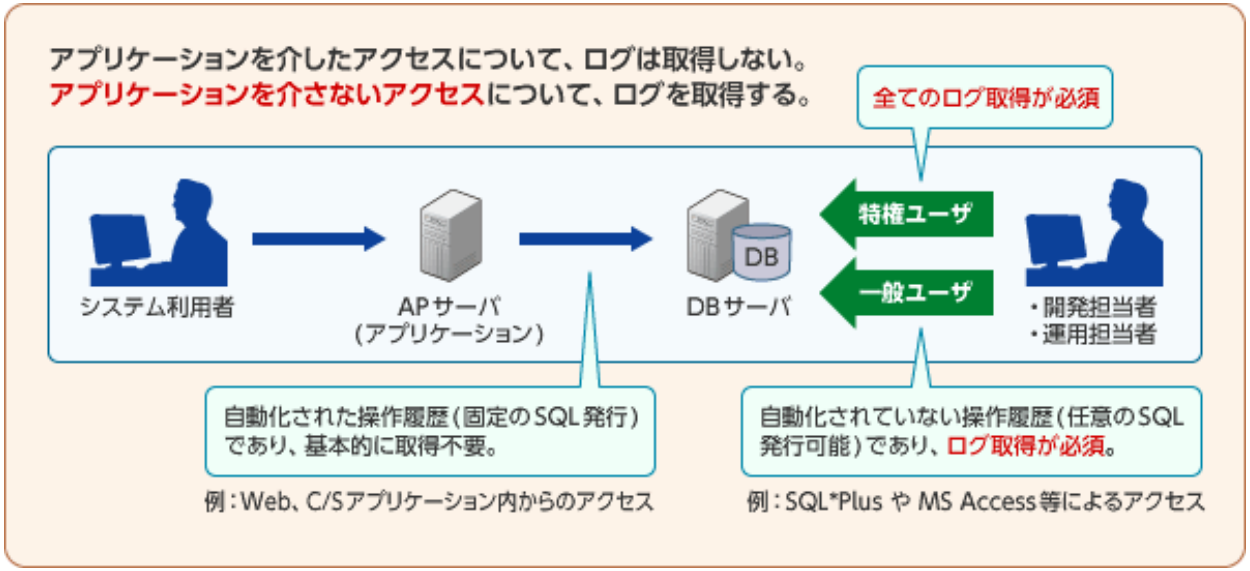
URL: https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

4.1.8 ハイパーバイザの強化
・ハイパーバイザー管理者がハイパーバイザーの監査ログの変更、消去、無効化ができないよう管理機能を分離する。
・ハイパーバイザーのログは、物理的に分離された安全なストレージに、可能な限りリアルタイムで送信する。

3.7 休止状態の仮想マシン／3.8 VMイメージとスナップショット
・カード会員データを保持してしまう可能性があるVMイメージやスナップショットに対するアクセスログを取得する。

（PCI DSS Virtualization Guidelines には無いが）
・仮想環境のAPI (VMware API や Hyper-V API)を使用した際のアクセスログを取得する。

DB監査ログ取得上の留意点



•DB監査ログは、何も考えずに全て取得するように設定すると、非常に膨大な量になりやすい。

•上の図のような三層型アプリケーションの場合、データベースの監査設定を有効にした上で図の右側、データベースサーバに対する管理上のアクセスログを取得対象とし、認められていないデータの閲覧や設定の改ざん・更新が行われていないかを、継続的にモニタリングする事が求められる。

•逆にアプリケーションサーバ等からのアクセスについては、基本的に固定的なSQL文のみが発行される形となる為、その取得の優先度は低いと考えられる。
　但し、アプリケーションサーバが外部公開されているケースに於いて、外部からの攻撃に対するモニタリングを強化しようとする場合、上図のアプケーションサーバからDBサーバへのアクセスログを取得するケースも有る。
（が、これはWeb Application Firewall の仕事とも言える）

PCI DSS 対応事例

【最近のLogstorageのPCI DSS案件】

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。

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, ISMS同時取得
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

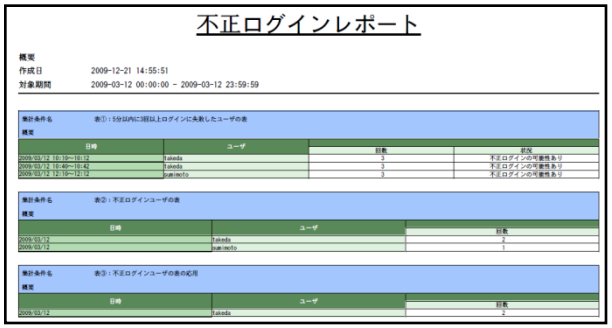
ログレビューの観点/出力レポート例

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

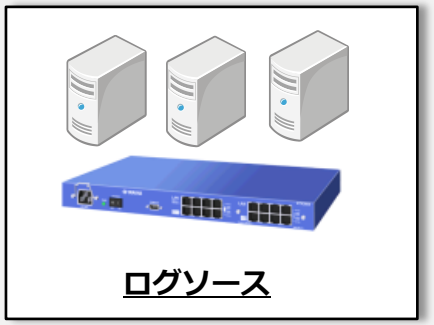
問題の内容をシステム管理責任者に送付し、指示を仰ぐ

問題点検出時

ログの積極活用への展開

- 多様化するログ活用への対応 -

ログ管理・活用インフラとしてのLogstorage



連携パック

クラウド環境

ログソース

マスタデータ

申請データ

ポリシー／ルール

Logstorage

URL分類データ

脅威データ

オープンデータ

分析オプション

Logstorage Connect!

異常検知システム(SIEM)

Logstorage Connect!

外部プロフェッショナルサービス

分析システム(BigData基盤)

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

END

「知らないでは済まされない、ログ管理の本質とは」

2013/7/10

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