



Tripwire Enterpriseのご紹介
～ セキュリティ対策に欠かせない整合性監視とは～

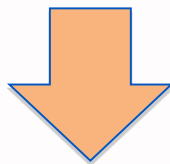
株式会社イーセクター

ファイル整合性監視とは

整合性とは……

欠落がなく、また当初の状態から変わっていないことを示します。

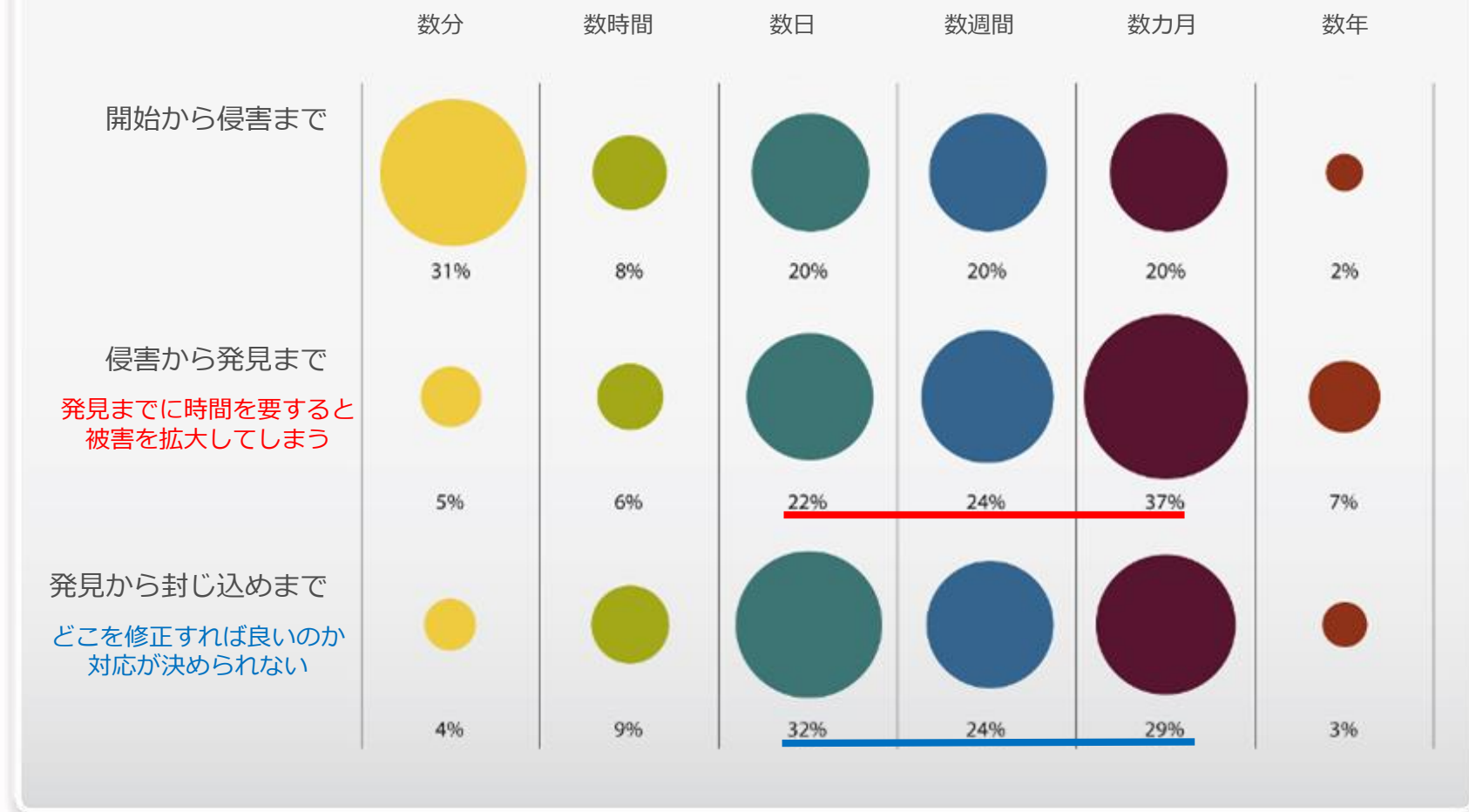
- ❶ 重要なシステムファイル、レジストリ、アプリケーションが変更されたことを知らせる = 整合性(完全性)監視



迅速な発見が重要！！

早期発見の重要性

- ① セキュリティ強化には、**防御／監視**のバランスの取れた対策が必要
- ② かなり改善はされているが、引き続き発見スピードの改善が必要



(引用) ベライゾン ビジネス "データ漏洩／侵害調査報告書 2013"

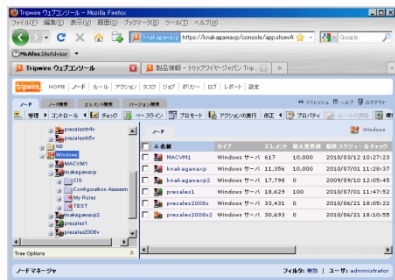
求められている整合性監視とは？

- 何を監視すれば良いのかを示してくれる
- 素早く導入できる
- 怪しい変更 = 整合性違反を迅速、的確に検知する
- コストを掛けない自動運転
- 監査レポートの作成
- 監視対象システムに負荷を掛けない



対象はオープンシステム全体です

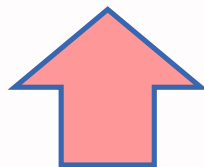
Tripwire Enterprise / Server



Web ブラウザ

変更の検知

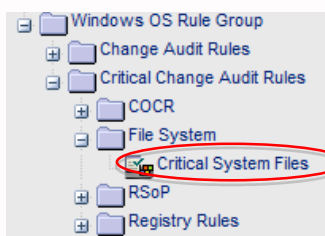
変更監査証跡



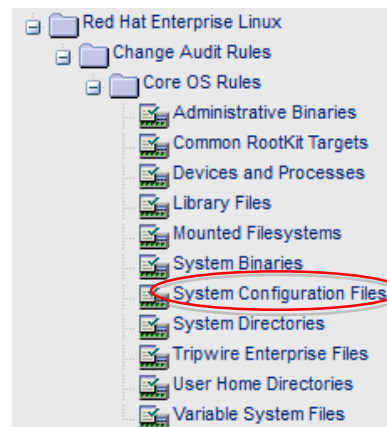
Tripwire Enterprise : デフォルト監視ルール

⑧ オペレーティングシステムなどを監視するルールを提供

- Critical Change Audit Rules
- Change Audit Rules



エレメント
C:\WINDOWS\system32\drivers\tcpip.sys
C:\WINDOWS\system32\drivers\svr.sys
C:\Windows\System32\drivers\srvtcp.sys
C:\Windows\System32\drivers\svr2.sys
C:\Config.Msi
C:\WINDOWS\system32\drivers\afd.sys
C:\WINDOWS\system32\drivers\mrxsm.sys
C:\Windows\System32\drivers\mrxsm10.sys
C:\Windows\System32\drivers\mrxsm20.sys
C:\workspace
C:\Windows\System32\drivers\point32.sys
C:\Windows\System32\drivers\usbccgp.sys
C:\Windows\System32\drivers\nuidfltr.sys
C:\WINDOWS\system32\drivers\usbd.sys
C:\WINDOWS\system32\drivers\usbehci.sys
C:\WINDOWS\system32\drivers\usbhub.sys
C:\WINDOWS\system32\drivers\usbport.sys









エレメント
/var/log/secure
/etc/smardtd.conf
/etc/sysconfig/hwconf
/etc/rc.d/rc3.d/S95twd daemon
/etc/reader.conf
/etc/rc.d/rc1.d/K95twd daemon
/etc/rc.d/rc5.d/S95twd daemon
/etc/printcap
/etc/rc.d/rc0.d/K94twt rmd
/etc/vmware-tools/icu
/etc/rc.d/rc0.d/K95twd daemon
/etc/rc.d/rc6.d/K94twt rmd
/etc/blkid/blkid.tab.old
/etc/rc.d/rc2.d/K94twt rmd
/etc/blkid/blkid.tab
/etc/rc.d/rc1.d/K94twt rmd
/etc/rc.d/init.d/twd daemon
/etc/vmware-tools/locations
/etc/rc.d/rc3.d/S94twt rmd

Tripwire Enterprise : ネットワーク機器の監視

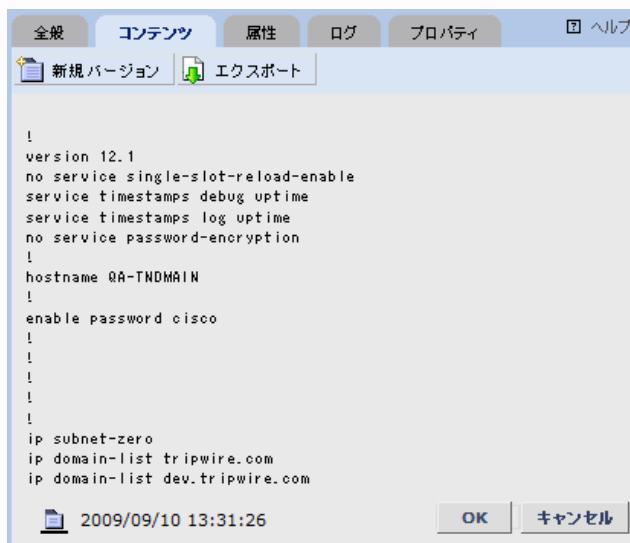


ネットワークデバイス
ルーター
ファイアウォール
スイッチ

SSH、Telnetでログインし、SCP、TFTP、SFTPにてファイル転送が可能なすべてのネットワーク機器をサポートします。

 startup-config	 2009/09/10 13:31:26	 Cisco IOS Configuration Rule
 running-config	 2009/09/10 13:31:26	 Cisco IOS Configuration Rule

コンフィグレーション情報を
Tripwire Enterprise/Serverは、
保持しています。



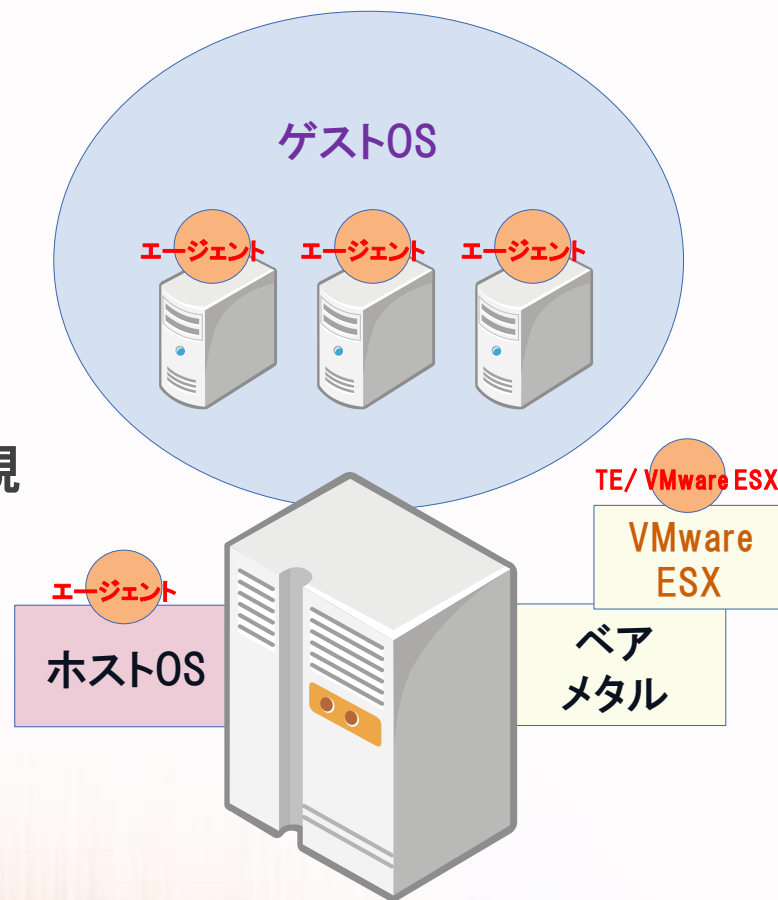
```
全般 コンテンツ 属性 ログ プロパティ ヘルプ
新規バージョン エクスポート
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname QA-TNDMAIN
!
enable password cisco
!
!
!
!
!
!
ip subnet-zero
ip domain-list tripwire.com
ip domain-list dev.tripwire.com
2009/09/10 13:31:26 OK キャンセル
```

ネットワーク機器のコンフィグレーションの変更
を検知します。

リストア機能を持っています。

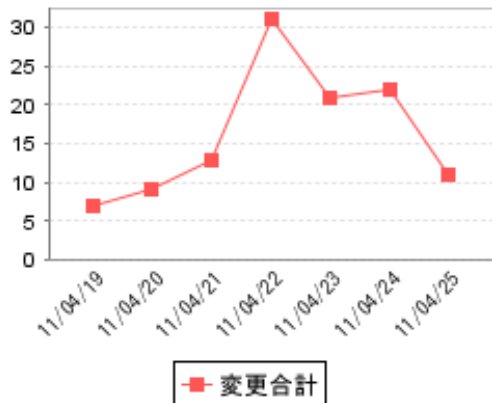
仮想環境の監視

- » ホストOS:TE / FSで監視
- » ゲストOS:TE / FSで監視
 - ・ OS毎にエージェントを導入
 - ・ 仮想環境サポートの実施
- » VMware ESX:TE / VMware ESXで監視
 - ・ ハイパーバイザのパラメータを監視

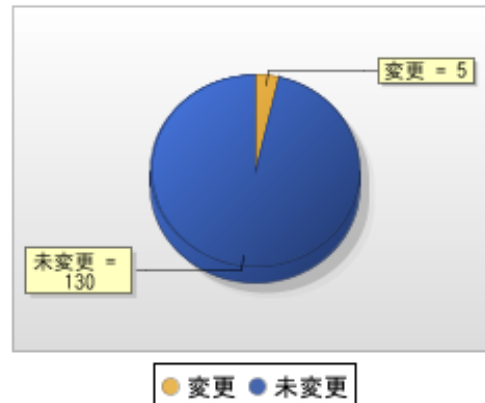


変更を可視化するレポート

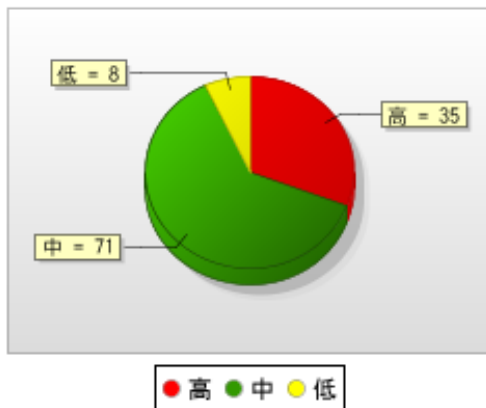
1. 週次 変更レート



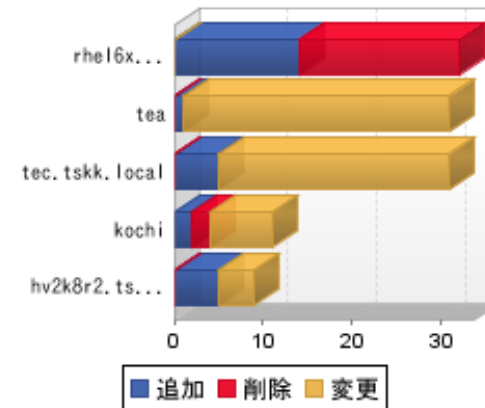
2. 週次 変更されたノード



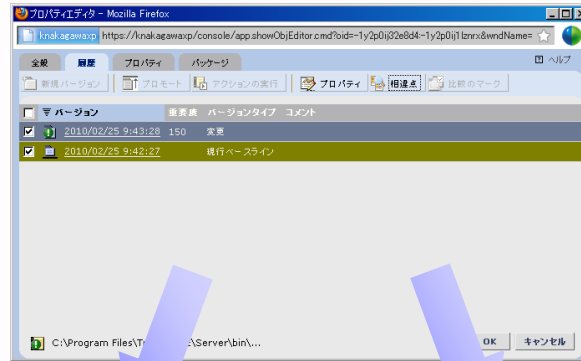
3. 週次 重要度ごとの変更



4. 週次 変更頻度の高いノード上位5



いつ、何が、誰によって、どのように変更されたのか



正しい状態(ベースライン)と
変更があった状態を比較

監視属性の比較

コンテンツの比較

属性	2010/02/25 9:42:27	2010/02/25 9:43:28
Create	09/02/20 14:54	09/02/20 14:54
DACL	BUILTIN\Administrators, アクセス許可タイプ: 標準権利 (Standard) 削除, 読み取り制御_DACの書き込み, 所有者の書き込み, 同期 (Specific) 01ff	BUILTIN\Administrators, アクセス許可タイプ: 標準権利 (Standard) 削除, 読み取り制御_DACの書き込み, 所有者の書き込み, 同期 (Specific) 01ff
NT AUTHORITY\SYSTEM, アクセス許可タイプ:	標準権利 (Standard) 削除, 読み取り制御_DACの書き込み, 所有者の書き込み, 同期 (Specific) 01ff	標準権利 (Standard) 削除, 読み取り制御_DACの書き込み, 所有者の書き込み, 同期 (Specific) 01ff
KNAKAGAWAXP\knmagawa, アクセス許可タイプ:	標準権利 (Standard) 読み取り制御, 同期 (Specific) 00e9	標準権利 (Standard) 読み取り制御, 同期 (Specific) 00e9
Group	KNAKAGAWAXP\なし	KNAKAGAWAXP\なし
Hidden	false	false
Owner	KNAKAGAWAXP\knmagawa	KNAKAGAWAXP\knmagawa
Read-Only	false	false
SACL	(null)	(null)
SHA-1	bc740c54acc3119193be637e95f5e31981b72e2	86c192032bf3f3c715ed5c96256864236c75ce40
Size	7131	7119
Stream Count	1	1
Stream SHA-14213fab907c6625ab221be408...	4213fab907c6625ab221be408e61cfd37be723f	4213fab907c6625ab221be408e61cfd37be723f
System	false	false
Type	File	File
Write	09/02/20 15:03	10/02/25 9:43

ベースライン (正しい状態)
検知された変更

```

84 # Log file to use for wrapper output logging.
85 # Log file to use for wrapper output logging.
86 # Format of output for the console.
87 wrapper.console.format=M
88 # Log Level for console output.
89 wrapper.console.loglevel=INFO
90 # Format of output for the log file.
91 wrapper.logfile.format=LPTM
92 # Log Level for log file output.
93 wrapper.logfile.loglevel=INFO
94 # Maximum size that the log file will be allowed to grow to before
95 # the log is rolled. Size is specified in bytes. If left unspecified
96 # this defaults to a value of 0, which disabled log rolling.
97 # Maximum size that the log file will be allowed to grow to before
98 # the log is rolled. Size is specified in bytes. If left unspecified
99 # this defaults to a value of 0, which disabled log rolling.
100 wrapper.logfile=DEBUG
101 # Maximum size that the log file will be allowed to grow to before
102 # the log is rolled. Size is specified in bytes. If left unspecified
103 # this defaults to a value of 0, which disabled log rolling.
104 # Maximum size that the log file will be allowed to grow to before
105 # the log is rolled. Size is specified in bytes. If left unspecified
106 # this defaults to a value of 0, which disabled log rolling.
    
```

削除
変更
追加

ベースライン (正しい状態)
検知された変更

変更監査： 変更管理プロセスの見える化

ベースライン



プロモート
(再ベースライン化)

変更の検知

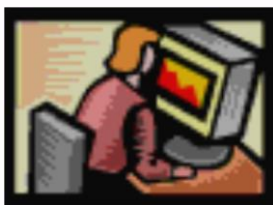
変更の評価

A screenshot of a software version history table. The table has columns for version, importance, version type, and comment. The top row is highlighted in yellow and labeled '変更の履歴です' (This is the change history) with a red arrow. The table shows a sequence of changes, including promotions to baseline, changes, additions, and deletions, all performed by an administrator.

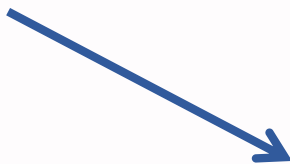
バージョン	重要度	バージョンタイプ	コメント
2010/02/08 13:44:58		現行ベースライン	10/02/08 13:44 に administrator によりプロモートされました...
2010/02/08 13:37:41	10,000	変更	
2010/02/05 14:39:15		ベースライン	10/02/05 14:39 に administrator によりプロモートされました...
2010/02/05 14:29:45	10,000	変更	
2010/02/03 15:00:06		ベースライン	10/02/03 15:00 に administrator によりプロモートされました...
2010/02/03 14:58:57	10,000	追加	
2010/02/03 14:58:42	10,000	削除	
2010/02/03 11:51:57		ベースライン	10/02/03 11:51 に administrator によりプロモートされました...
2010/02/03 11:46:08	10,000	変更	
2010/02/02 11:59:02		ベースライン	10/02/02 11:59 に administrator によりプロモートされました...
2010/02/02 11:28:34	10,000	変更	
2010/02/01 14:31:06		ベースライン	10/02/01 14:31 に administrator によりプロモートされました...

変更の履歴です

自動プロモートによる整合性監視の円滑化



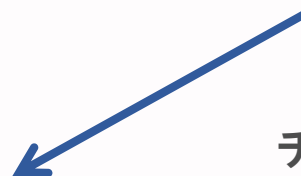
ファイル情報
時間
ユーザID
アプリケーション



監視対象サーバ



変更管理
チケットングシステム
Remedy ARやHP Service Desk など



ステージング環境
テスト環境



変更リクエスト

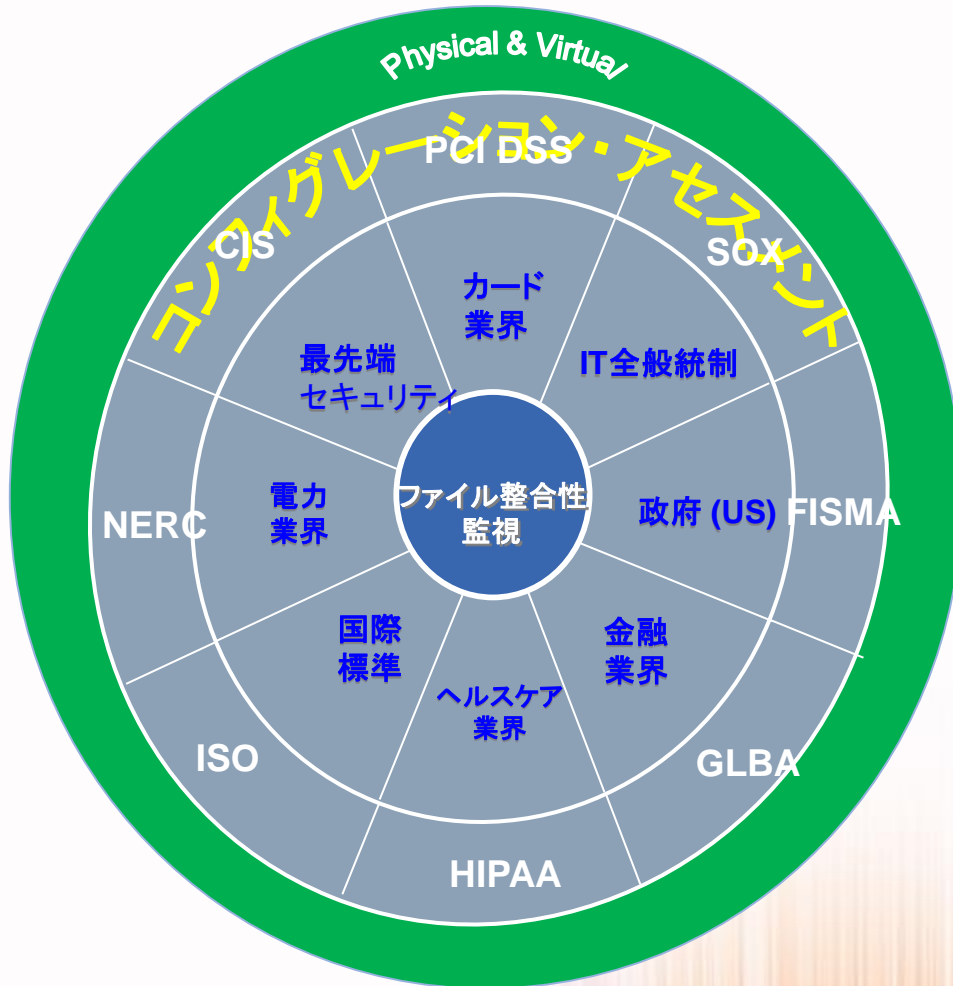
変更の適応

影響の検討



変更の承認

ポリシーテンプレート (CIS, PCI DSSなど)



Security

- Center for Internet Security (CIS)
- Defense Information Systems Agency (DISA)
- National Institute of Standards & Technology (NIST)
- ISO 27001

Compliance

- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes Oxley (SOX)
- Control Objectives for Information & Technology (COBIT)
- Federal Information Security Management Act (FISMA)
- Federal Desktop Core Configuration (FDCC)
- Gramm-Leach-Bliley Financial Services Modernization Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Protection of Personal Information of Residents of the Commonwealth (MA 201 CMR)
- North American Electric Reliability Corporation (NERC)

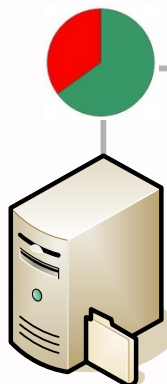
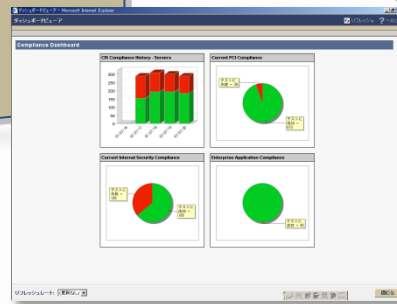
ポリシー・テスト: セキュリティポリシー達成度を診断

ベンダ出荷の
デフォルト値を
使用しない

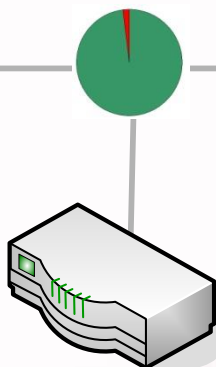
パスワードは7文字以上
90日以内でパスワードを変更

情報セキュリティ ポリシー

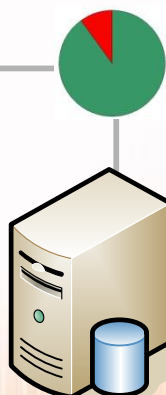
開放しているポートは
TCP XXXX, XXXX番



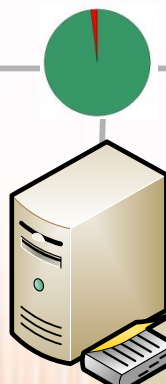
ファイルシステム



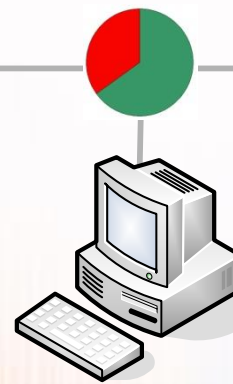
ネットワーク
デバイス



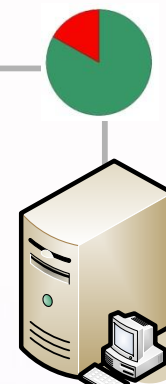
データベース



ディレクトリ
サーバ



デスクトップ
PC



ミドルウェア



<http://www.esector.co.jp>

E-mail ESECinfo@cec-ltd.co.jp

電話 03 (5789) 2443 FAX 03 (5789) 2575

〒150-0022 東京都渋谷区恵比寿南1-5-5 JR恵比寿ビル8F