Making Compliance Count <有意義なコンプライアンスの実現>

David Lenoe (デイビット・レノー) | アドビ システムズ 社

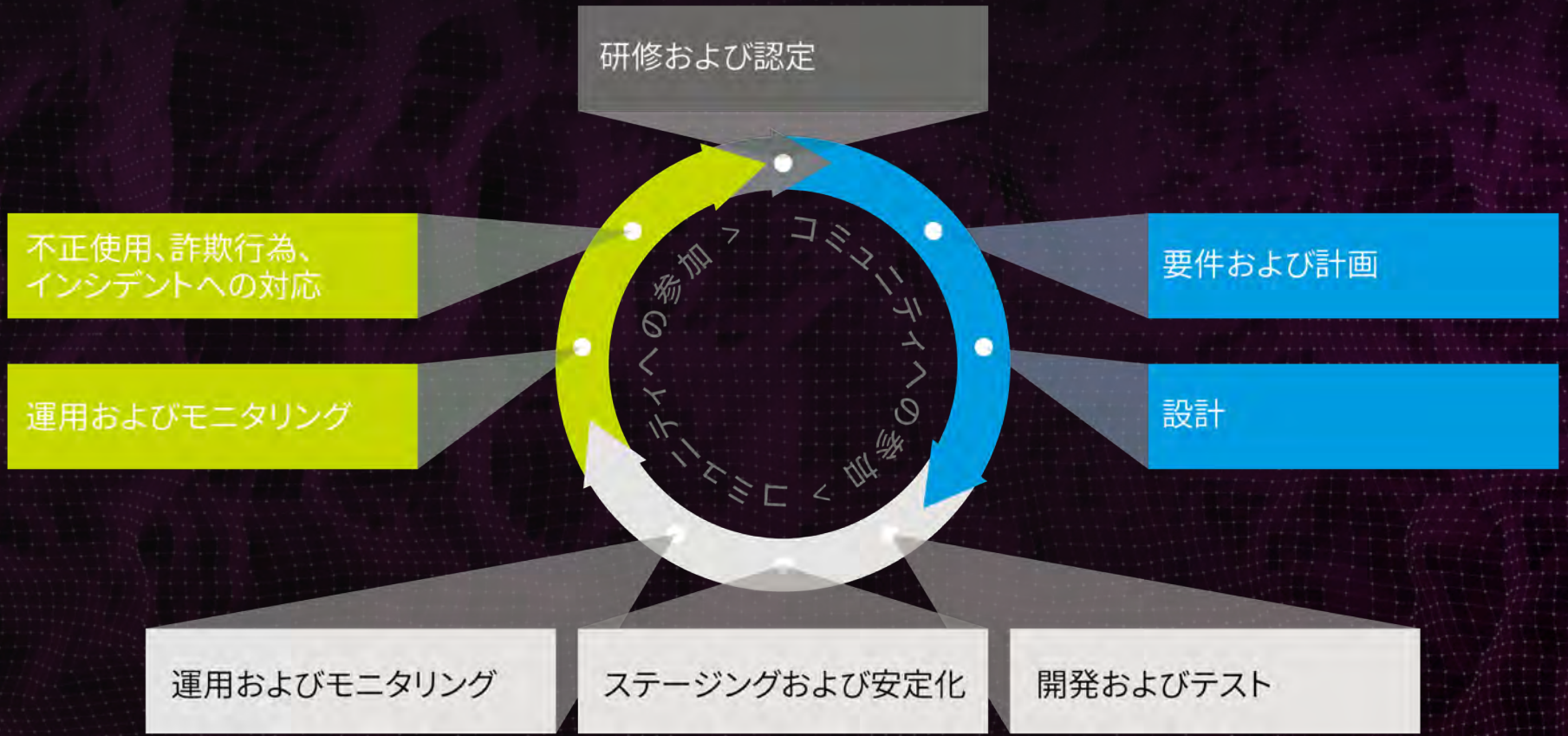
ビジネス競争方法の変革

「モノ」より「体験」

「アート」と「サイエンス」

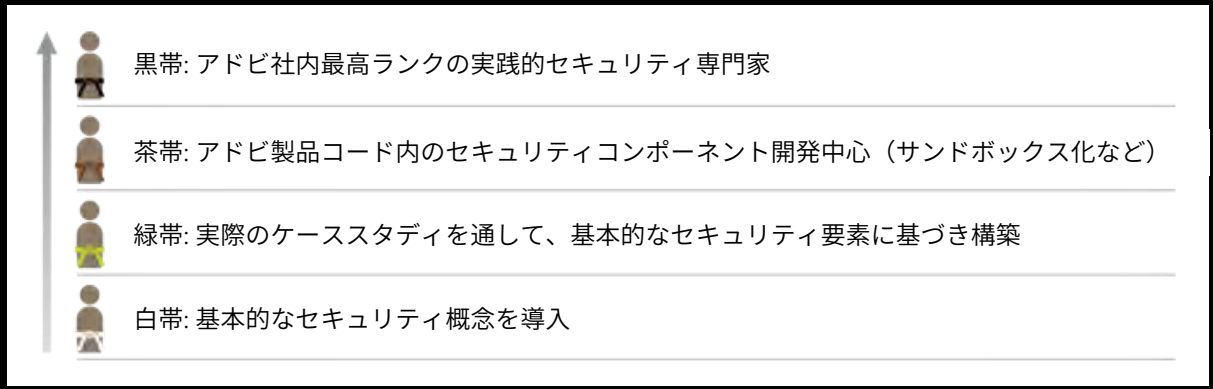
顧客体験のための
基本設計

Secure Product Lifecycle（SPLC）



全社を対象としたセキュリティ方針

- 全社員向けに年次セキュリティ意識トレーニングの義務付け
- アプリケーションセキュリティ認定に、最新の脅威に関する業界のベストプラクティスを盛り込み、ベルト（帯）システムを導入
- 会社全体でセキュリティ訓練を受けたエンジニアを数千人規模で配備
- 各所に「セキュリティチャンピオン」が配備されたネットワーク
- ブートキャンプ、CTF、内部バグバウンティ（脆弱性報酬金制度）その他の活動
- 外部カンファレンスとトレーニング



セキュリティ認定：Common Controls Framework（CCF）

10種類以上の基準、合計1,000項目におよぶ
セキュリティコントロール要件を…

…アドビの環境に合わせた20の管理ドメイン全体で、
最大237の共通項目に合理化

SOC 2 (5 Principles) – 116 CRs
サービス・オーガニゼーション・コントロール

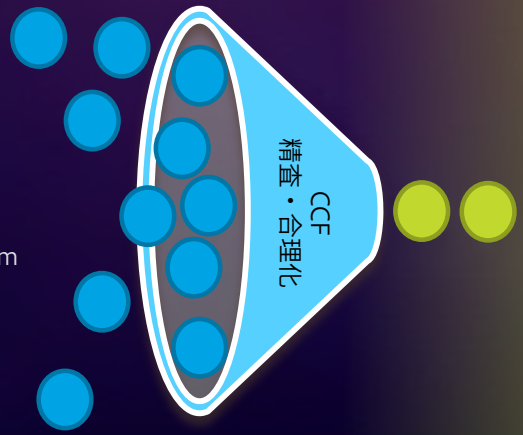
ISO 27001 – 26 CRs
国際標準化機構

PCI DSS – 247 CRs
PCIデータセキュリティスタンダード

FedRAMP - 325 CRs
Federal Risk and Authorization Management Program

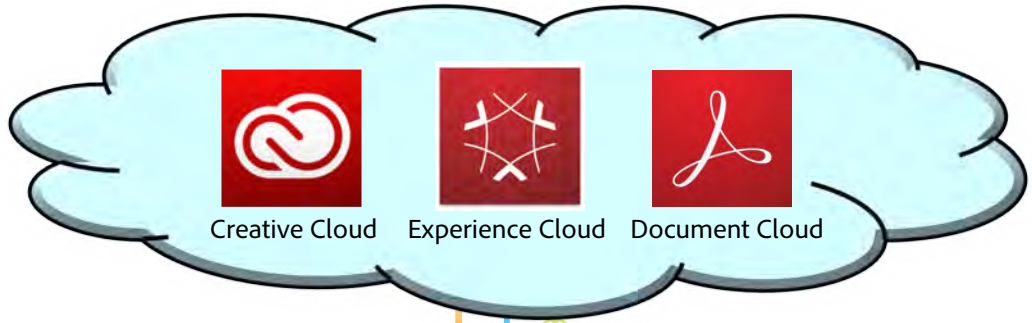
ISO 27002 – 114 CRs
国際標準化機構

SOX 404 (IT) – 63 CRs
サーベンス・オクスリー（SOX）法 404



アセット管理 – 11項目
バックアップ管理 – 5項目
ビジネス継続性 – 5項目
変更管理 – 6項目
構成管理 – 15項目
Data Management – 24項目
IDおよびアクセス管理 – 49項目
インシデント対応 – 7項目
モバイルデバイス管理 – 4項目
ネットワーク運用 – 19項目
人事 – 6項目
リスク管理 – 8項目
セキュリティガバナンス – 20項目
サービスライフサイクル – 7項目
サイト運用 – 7項目
システム設計ドキュメンテーション – 16項目
システムモニタリング – 30項目
サードパーティ管理 – 11項目
研修と啓発 – 6項目
脆弱性管理 – 21項目

Adobe Common Control Framework（CCF） – 概念モデル



クラウドコンプライアンス制御
最大60%

製品オペレーション
モニタリング　資産管理　論理的アクセス
設定　変更管理　インシデント対応

クラウドコンプライアンス制御
10%未満

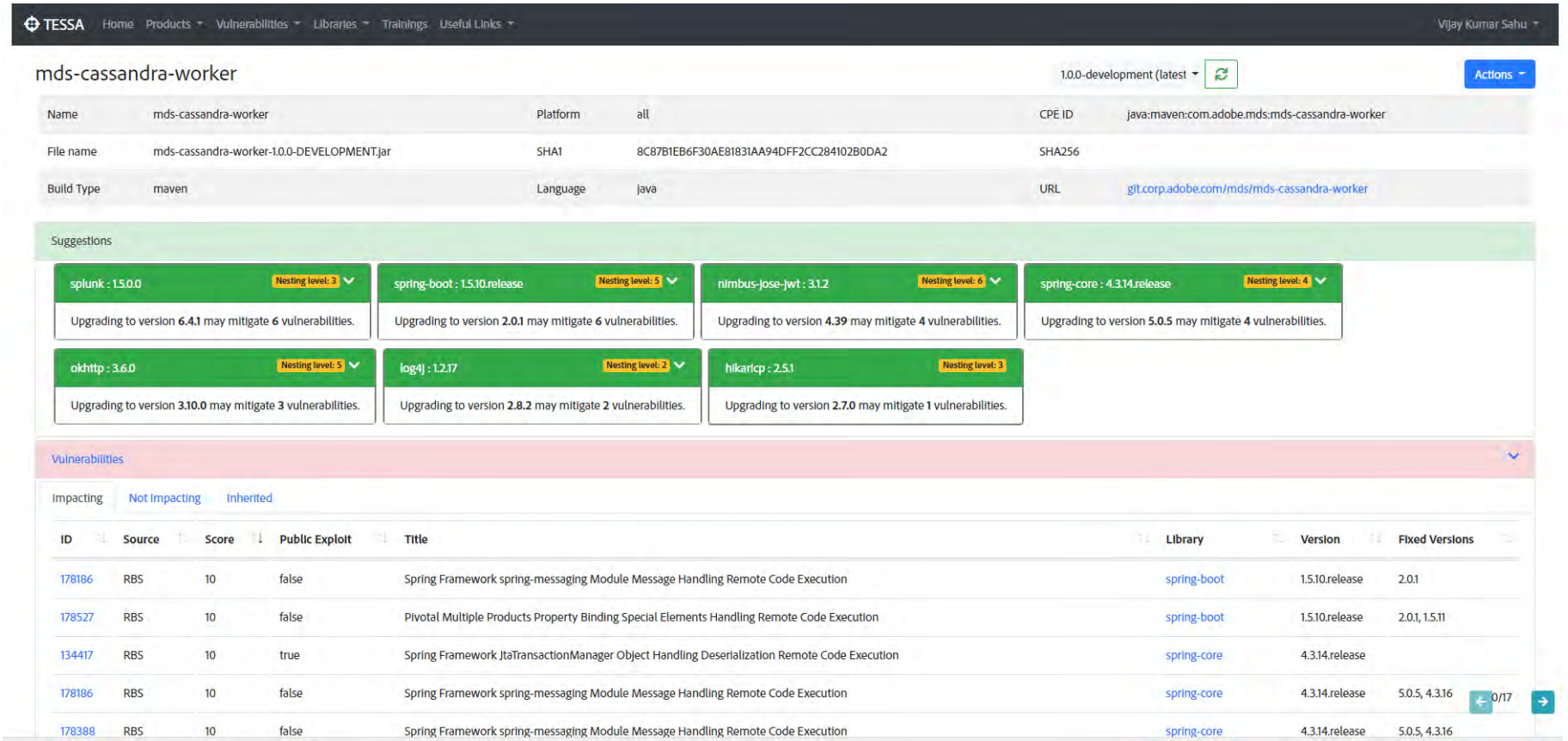
製品エンジニアリング
システム開発ライフサイクル

クラウドコンプライアンス制御
最大30%

アドビ社
ビジネス継続性　データプライバシー
セキュリティガバナンス　人材

開発フェーズ – サードパーティーコンポーネントのリスク管理

- TESSAは、あらゆるアドビ製品やプラットフォームで使用されるサードパーティーコンポーネントの脆弱性を検知



テストフェーズ – 侵入テストの種類

- ベンダーによる侵入テスト
- クラウドソーシングによるバグバウンティ（脆弱性報酬金制度）
- 社内チームによる侵入テスト
- 社内でのバグバウンティ

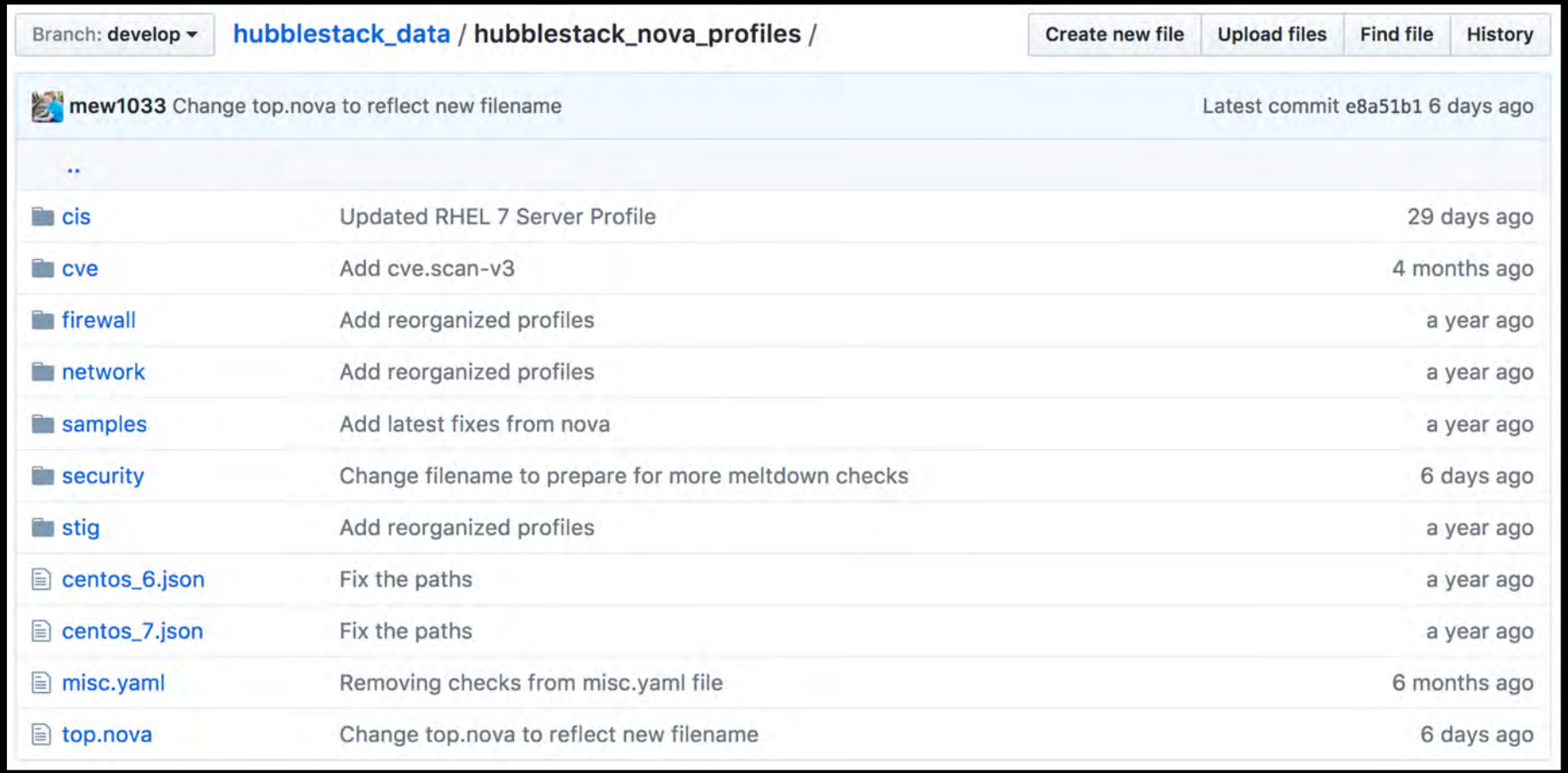
クラウドソーシングによる侵入テスト（バグバウンティ）

- メリット
  - 数十人から数百人規模で実施可能
  - 実際の攻撃をシミュレーション
  - セキュリティ関連コミュニティによる介入増
- デメリット
  - 根本原因分析／提案は行われない
  - テスト範囲の正確な測定が難しい
- この侵入テストに適した製品
  - 成熟度の高い製品
  - ベンダーテストでほとんどバグが発見されていない製品

社内でバグバウンティ

- ルール: 構造と保護
- 既存のプロセスを使用
- 対象の選定: 最も効果的な個所を狙う
- 報酬: お金と名誉

オペレーションとモニタリング: 自動監査 – HubbleStackを使用したCompliance as codeを実践



Branch: develop ▾ | hubblestack_data / hubblestack_nova_profiles / | Create new file | Upload files | Find file | History

mew1033 Change top.nova to reflect new filename — Latest commit e8a51b1 6 days ago

..

cis	Updated RHEL 7 Server Profile	29 days ago
cve	Add cve.scan-v3	4 months ago
firewall	Add reorganized profiles	a year ago
network	Add reorganized profiles	a year ago
samples	Add latest fixes from nova	a year ago
security	Change filename to prepare for more meltdown checks	6 days ago
stig	Add reorganized profiles	a year ago
centos_6.json	Fix the paths	a year ago
centos_7.json	Fix the paths	a year ago
misc.yaml	Removing checks from misc.yaml file	6 months ago
top.nova	Change top.nova to reflect new filename	6 days ago

自動化: ハイジャックプロジェクト（サブドメイン乗っ取り防止）の例

- シナリオ例:
  - example.comには、CNAMEのレコードが存在します。
  - この企業が後にこのS3バケットを削除しましたが、レファレンスは変わっていません。
  - 訪問者がexample.comに移動すると、「a bucket not found error」（バケットが見つかりません）というエラーが表示されます。
  - 攻撃者は、この完全に削除されていないレファレンスを利用し、 example.s3.aws.amazon.comという同じドメインを持つ不正バケットを登録します。
  - その結果、このサブドメインが攻撃者のものとなり、 example.comにはCNAMEのレファレンスが残っているものの、訪問者はこの組織ではなく、攻撃者が所有するサブドメインに移動するようになりました。

結論

- コンプライアンスを負担や義務に感じないでください。これは、実世界のリスクを減らすチャンスです。
- 自動化を利用して、簡単に確認できる部分（設定の真意、バージョン番号、脆弱なライブラリなど）に対応してください。
- 侵入テストでは、ありとあらゆるオプションを自由に取り入れてください。状況ごとに適した方法は異なります。
- 創造力を働かせてください（クラウドソーシングによるPCIテスト、社内バグバウンティなど）。両者が得する方法を探してください（社内セキュリティの可視性を向上、セキュリティ関連コミュニティによる介入増）

Adobe

リファレンス

- トレーニング:
  - https://safecode.org/training/
- Common Controls Framework:
  - https://www.adobe.com/go/open-source-ccf
- HubbleStack:
  - https://hubblestack.io/

関連リソース

Adobe Trust Center
https://trust.adobe.com

Security @ Adobeブログ
https://blogs.adobe.com/security/

アドバイザリーと更新情報
https://www.adobe.com/jp/support/security

Twitter：@AdobeSecurity

Adobe

MAKE IT AN EXPERIENCE