クラウドファースト時代のコンプライアンスとセキュリティの進化

Chad Woolf, Director, AWS Risk & Compliance

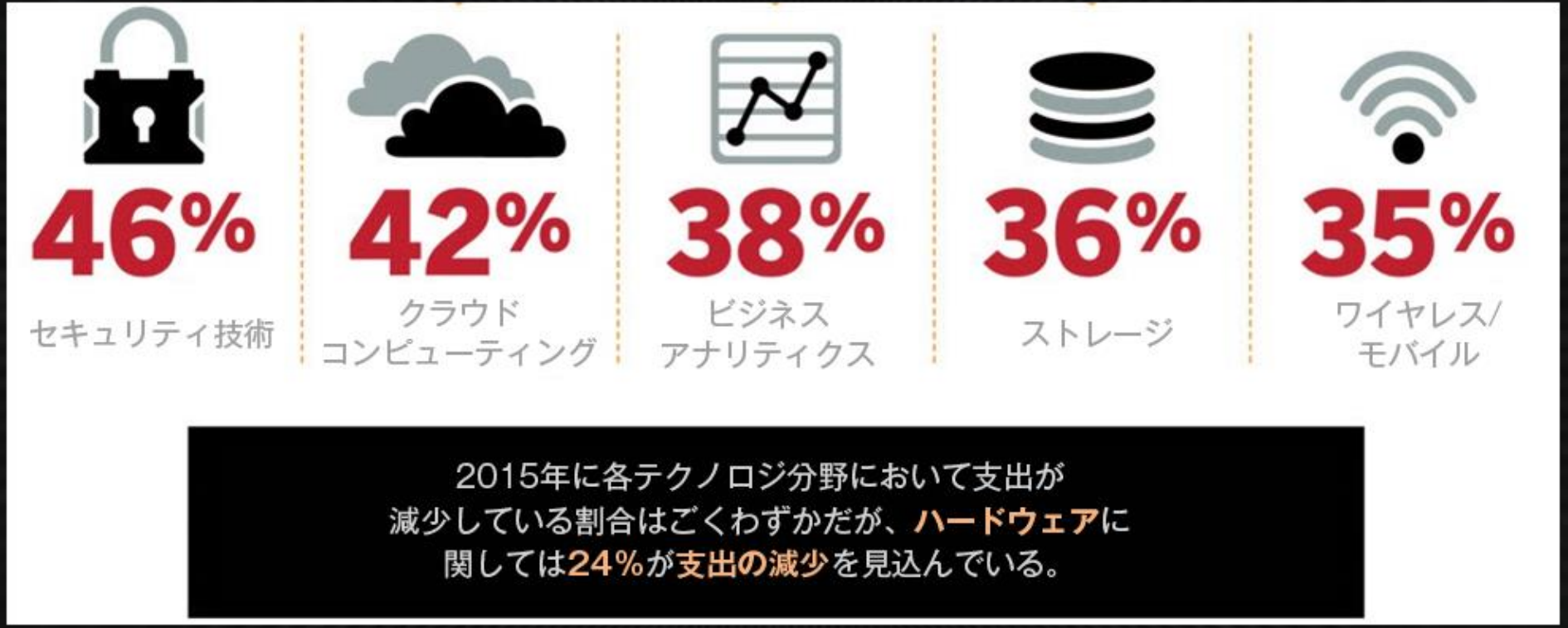
20年来のITセキュリティ政策

- ガバナンスの確立
- 新たな脅威への対処
- 「検出」手段の確立と「予防」への動き
- 整合性と信頼性を高めるための制御の自動化

システム、ネットワーク、ITの複雑さ

- 経済の拡大、複雑化、分散
- クラウド ー インスタントオン方式の、スケーラブルな、従量制のITIL準拠サービス
- モバイルコンピューティング ー どこでも、どのデバイスでもデータを使いたい
- 事業運営と競争力のある知的財産の保有のためにテクノロジが使用され、差別化につながらないタスクは専門家へ外注

支出が増えているテクノロジの上位5つの分野(2015年)



出典: Computerworld 2015 Forecast Study

amazon web services™

クラウド発展の契機

1. 推進力 ー セキュリティ機能
2. 推進力 ー アウトソーシング
3. クラウドファースト
4. エンタープライズ市場でのクラウドの導入
5. 法規のクラウドへの適合

1. 推進力 ー セキュリティ機能

- セキュリティ政策の重要性は増しているが、その達成もより困難になっている
- 従来のセキュリティマネジメント方式では脅威の拡大に対応できない
- 問題は他にもある

セキュリティを革新的なビジネスの妨げにするわけにはいかない

2. 推進力 ー アウトソーシング

- 企業は差別化につながらない作業を外注し、競争力の強化に注力している
- 専門的な機能は外注業者のほうが得意であり、機能とセキュリティにより多くの投資が可能
- ベンダーリスクマネジメントは業務に不可欠なレベルにまで成長している

3. クラウドファースト

- クラウド ー 外注契約の進化版
- 従来のホスティングモデルとCOTSソフトウェアの併用
- アウトソーシングの利点に加えて、アジリティ、セキュリティ、コストマネジメントを改善
- 「クラウドファースト」ー エンタープライズ市場での存在感の拡大
- 「Cloud or Bust」ー クラウドはスタートアップと中小企業のスタンダード

4. エンタープライズ市場でのクラウドの導入

- 「簡易な点からより複雑な点」への焦点の移動
- 監督/監査機関よりも顧客のほうがクラウドの管理についてよく知っている
- 法規はビジネスの動きほどすばやく変化しない

5. 法規のクラウドへの適合

- 法規上のITの定義がクラウドによって崩壊している
- コンプライアンスの解釈の段階でセキュリティとリスクが失われる
- クラウドに対応するために法規が徐々に変化している

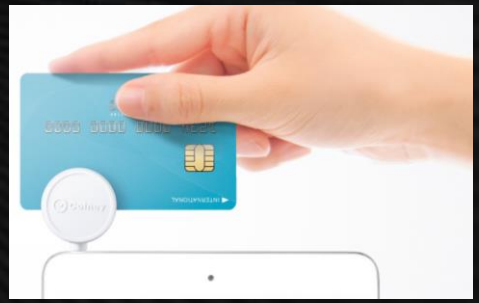
法令に準拠した
AWSの導入事例

ソニー銀行

- 銀行業務システム、社内業務システム等の基盤
  - BIツール、リスク分析、文書管理等
- セキュリティ・リスクについて詳細に分析
  - クラウドのセキュリティ・リスクについての理解
  - AWS上におけるFISCガイドライン、AWSのFISC関連パートナー
  - ソニー銀行独自のシステムリスク分析
- 導入効果
  - 5年で約37%のコスト削減メリット
  - 拡張性、HW保守対応、HW障害対応、BCP対応等

Coiney

- AWSの事前にPCI DSSに対応した環境
  - コンプライアンス対応のための負担の大幅な軽減
  - システム計画から実装を1か月という短期間で実現
- クレジットカード処理のための拡張性
  - オートスケールによるペイメント処理の拡張
  - オートスケールによるインスタンスコストの調整



amazon web services™

リーディングプラクティス：金融業界

- ビッグ “C” ー 政府による規制
- リトル “C” ー 社内基準
- アクセス管理システム
  - コンプライアンス監視システム
  - CloudTrail、Splunkの使用
  - フェデレーションID

全面的な導入：銀行業務

- 「できないことを話すのは時間の無駄。そこで…当社はすべてを（AWSへ）移行するつもりだ」
  - Jeff Smith, CEO, Suncorp Business Services, Suncorp
- 最初に何がうまくいくのか、次にそれをどのようにして加速させるのかに目を向ける
- リスク、セキュリティ、法令、ガバナンスの問題に速やかに対処し、監督機関に概要を説明している

amazon web services™

移動可能なワークロード

例:

- SEC 17a(4)
- 45 CFR 164.312
- NIST SP 800-53R4
- PCI DSS 3.0
- 1995年10月24日の欧州議会および理事会の95/46/EC指令

重要なワークロードを AWSへ移動するときに 対処すべき問題

問題1 ー サービスとセキュリティ

- サービスはビジネスの成功を可能にする
- AWSのセキュリティサービス ー インフラストラクチャとソフトウェアのセキュリティに対する多額の投資を継承
- サービスとセキュリティを結合 ー サービスのセキュアな利用
- クラウドによるクラウドのセキュリティ

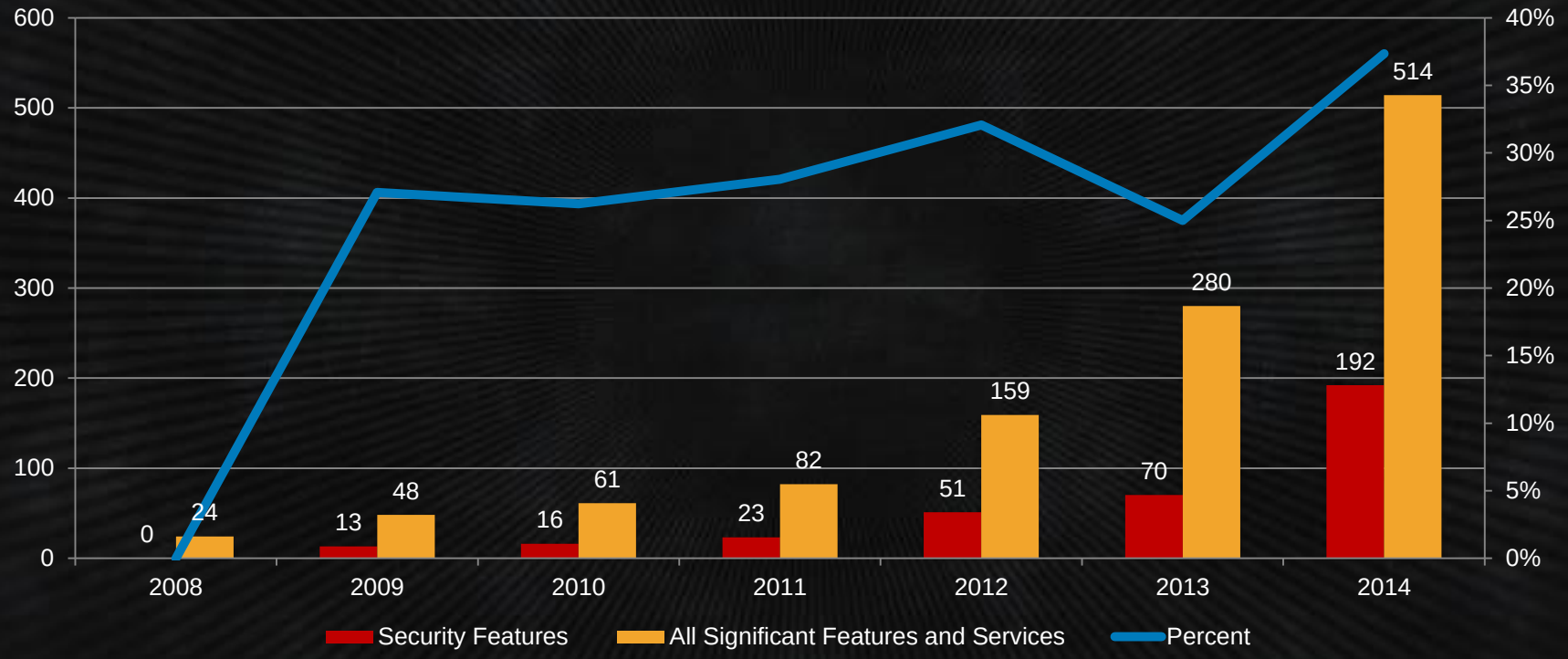
「…組織の機密保持やコンプライアンスの管理を強化する意味でもクラウドサービスが導入されるだろう。クラウド以外の方法では、それほど効率的または効果的にこれらを実現することはできない」

- *Security's Cloud Revolution Is Upon Us*, Forrester Research, Inc., August 2, 2013

問題2 ー ガバナンス

- AWSの使用法をポリシーに反映させる
- 自動制御の実装
- 既存の制御構造との統合
- デフォルトでセキュアな、法令に準拠したAWSアカウントの作成

イノベーションの速度：全体に対するセキュリティの割合



amazon web services™

イノベーションは監査機能にも

監査中心のサービスと機能

- 新サービス: AWS Config
- 新サービス: AWS KMS（Key Management Service）
- Trusted Advisorのチェック
- AWSへの最終サインイン日時
- AWS CloudTrail
- IAM認証情報レポート
- ポリシー

問題3 ー ベンダーのリスク計画

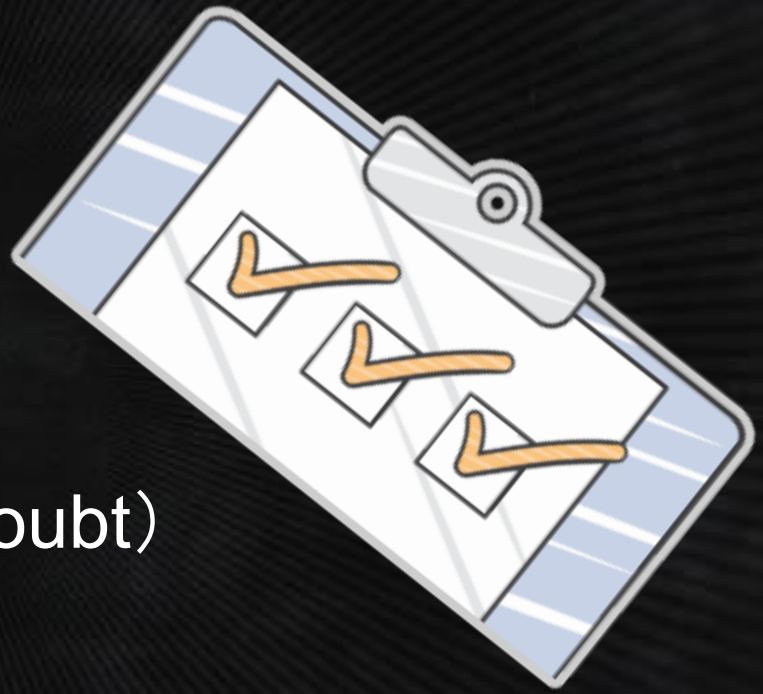
- 更新予定日
- クラウド固有の注意事項を盛り込む
- コンプライアンスの枠にとらわれない考え方

問題4 ー オーディターと監督機関

- クラウドのリスク管理計画を立てる
- クラウドとオンプレミスの制御フレームワークを統合する
- テスト計画を作成する
- 自分の立場を守る
- オーディターを教育する

オーディターとリスクマネージャーの心理

- 「去年と同じ」
- 従来のリスクフラグ
- 基準の解釈
- 技術的な理論
- FUD（Fear, Uncertainty, Doubt）



オーディターの傾向

- ああ、クラウドね！
- デューディリジェンス（適正評価）
- 物理的なアクセス
- 客観的な監査
- 自動化に対する要求
- ITのモバイル性と複雑さに合わせた調整
- レベルアップ

amazon web services™

オーディターの傾向：信頼を優先

amazon web services™

やるかやらないかではなく、いつやるかの問題

規制対象の機密データは
クラウドに格納し、クラウド
で処理するほうが適切

amazon web services™

次なるステップ：参考資料

1. 共同責任、セキュリティ、プライバシーを理解する
   - 共同責任モデルの概要を示す3分の動画
   - aws.amazon.com/compliance ー ホワイトペーパー、ケーススタディ、AWS認定、AWSコンプライアンスイネーブラー
2. 技術を身につける
   - 自分のペースで進められる実習と短期集中講座（Qwiklabs）ー https://run.qwiklab.com/
   - “Auditing Your AWS Security Architecture”

awscompliance@amazon.com