すべてのステークホルダーから信頼され支持される企業へ
ADMIRED COMPANY

クラウド時代に潜むセキュリティリスクとは？
クラウドを最大限に利活用するためのセキュリティ対策

ネットワンが提唱する

クラウド活用推進のためのセキュリティ

2018年12月13日

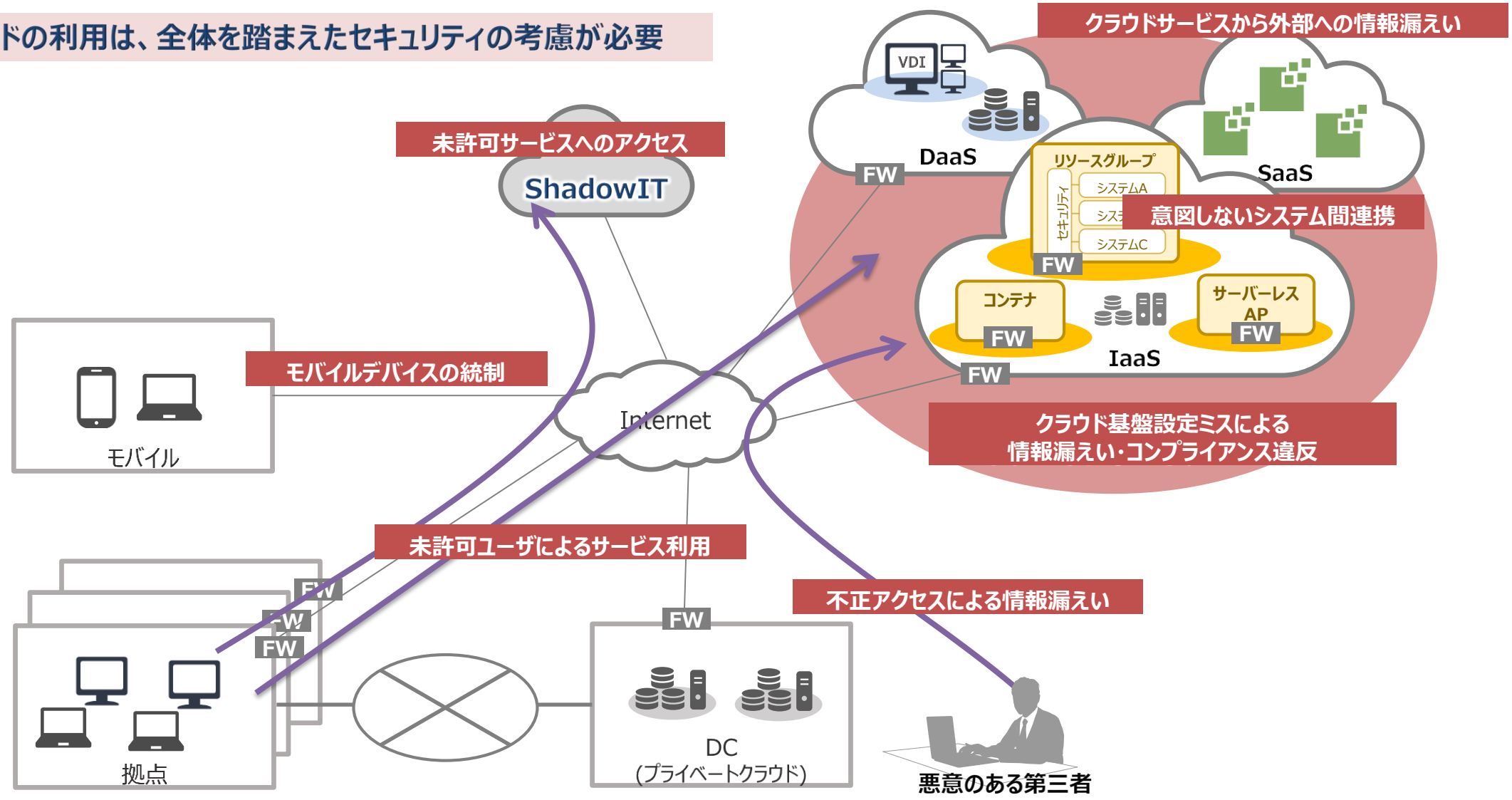
ネットワンシステムズ株式会社

net one

クラウド環境におけるセキュリティリスクと対策

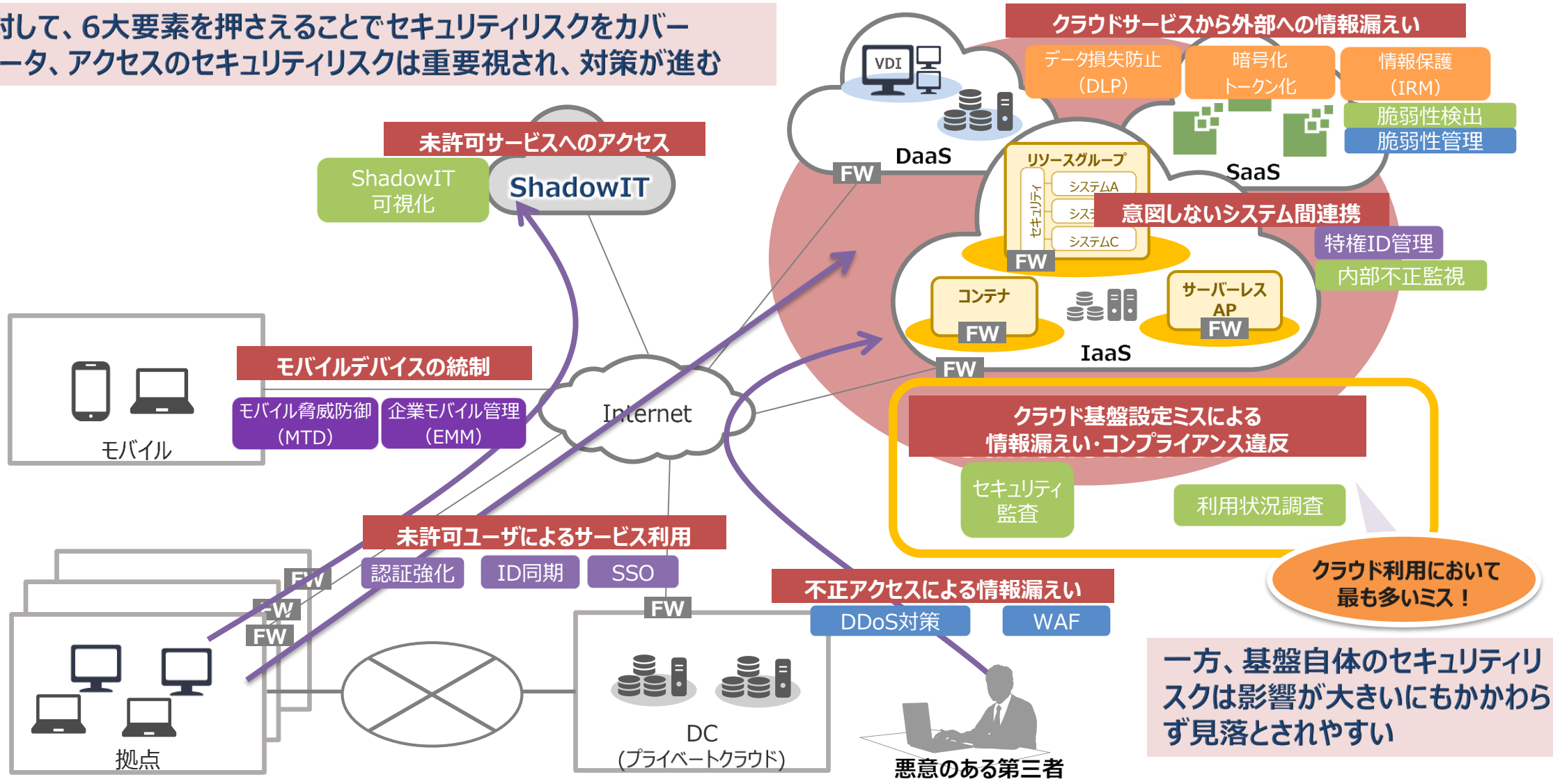
2-1. クラウド特有のセキュリティリスク

クラウドの利用は、全体を踏まえたセキュリティの考慮が必要



2-2. クラウド特有のセキュリティリスク

リスクに対して、6大要素を押さえることでセキュリティリスクをカバー
中でもデータ、アクセスのセキュリティリスクは重要視され、対策が進む

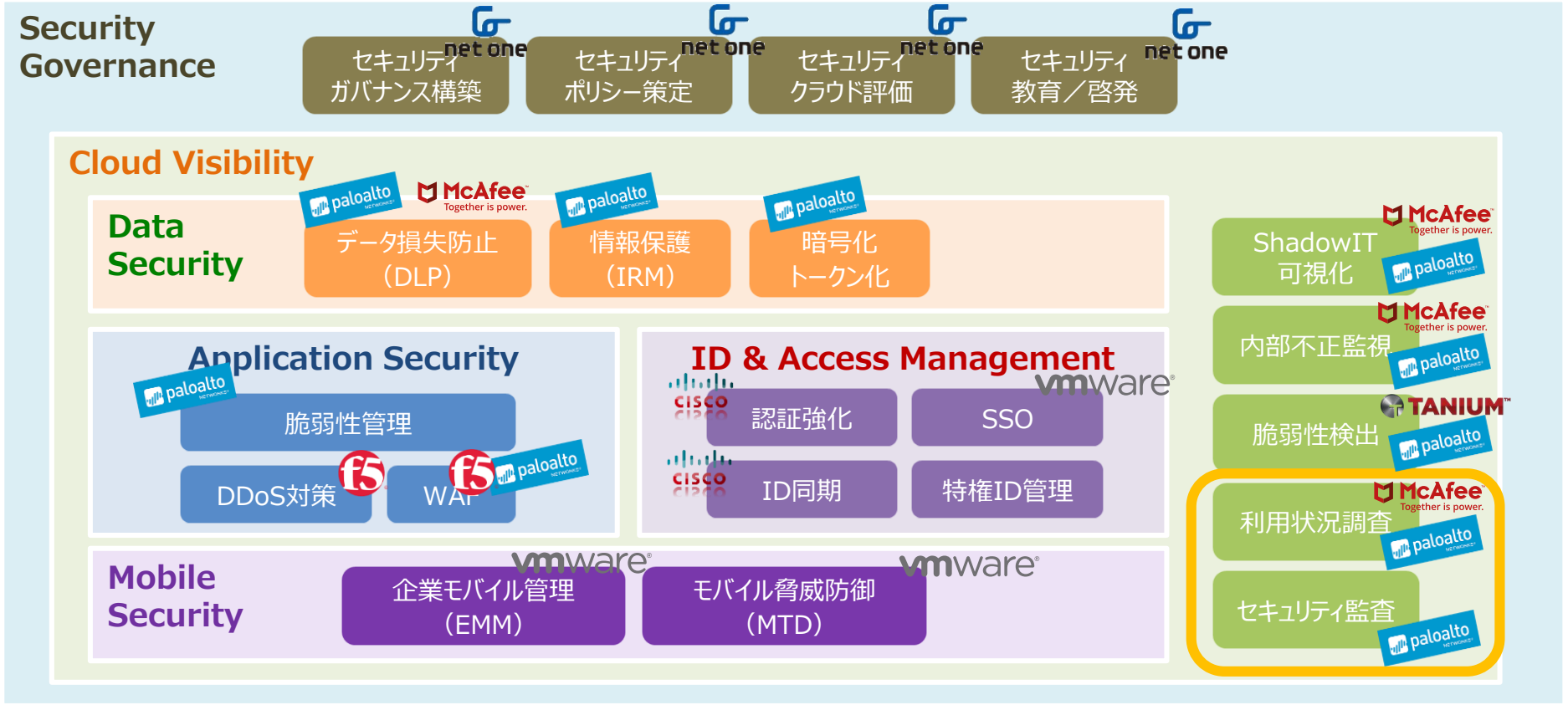


一方、基盤自体のセキュリティリスクは影響が大きいにもかかわらず見落とされやすい

2-3. クラウドセキュリティ ６大要素

クラウドサービスを利用する上で、検討する必要のあるセキュリティ要素は６つにまとめられる

Security Governance | Data Security | ID & Access Management | Application Security | Mobile Security | Cloud Visibility



クラウド基盤自体のセキュリティリスク「設定ミス」と その対策「クラウド監査」

2-6. なぜ「設定ミス」がセキュリティリスクとなるのか

クラウドならではの利便性、責任モデルがセキュリティリスクを生み出す原因となっている

課題①

クラウドはインターネットに近い性質上、悪意を持った第三者からのアクセスが容易

課題②

クラウドは誰でも簡単に利用、設定ができる環境が用意されている

課題③

クラウド設定のセキュリティリスクは、利用者側で担保する必要がある

2-8. 設定のセキュリティリスクは事業者側は関知しない

たとえばAWSは責任モデルについて、公式には
「 While AWS manages security of the cloud, security in the cloud is the responsibility of the customer. 」としており、**設定通りに動くこと**は管理するが、
セキュリティなどに関する設定の妥当性については利用者側の責任としている。

お客様

クラウド内の
セキュリティに
対する責任

- カスタマーデータ
- プラットフォーム、アプリケーション、アクセス管理
- オペレーティングシステム、ネットワーク、ファイアウォール構成
- クライアント側のデータ、暗号化とデータ整合性、認証
- サーバ側の暗号化（ファイルシステムやデータ）
- ネットワークトラフィックの保護（暗号化、整合性、アイデンティティ）

インスタンスの管理

この部分は
お客様自身でチェック

AWS

クラウドの
セキュリティに
対する責任

- ソフトウェア
- コンピュート
- ストレージ
- データベース
- ネットワーキング
- ハードウェア/AWSグローバルインフラストラクチャ
- リージョン
- アベイラビリティゾーン
- エッジロケーション

インフラの監視

AWS

2-9. 一つの対策

オンプレミスと同じ「使わせない、変えさせない」
厳しい制限を掛けることでセキュリティリスクを低減する。

課題①
誰でも簡単に利用、設定ができる環境が用意されている

課題②
設定のセキュリティリスクは利用者側で担保する

課題③
性質上悪意を持った第三者からのアクセスが容易

制限

特定の管理者しか
利用、変更させない

利用、変更に伴い
全て事前審査を行う

システム外への公開は原則禁止

2-9. 一つの対策

オンプレミスと同じ「使わせない、変えさせない」
厳しい制限を掛けることでセキュリティリスクを低減する。

課題①

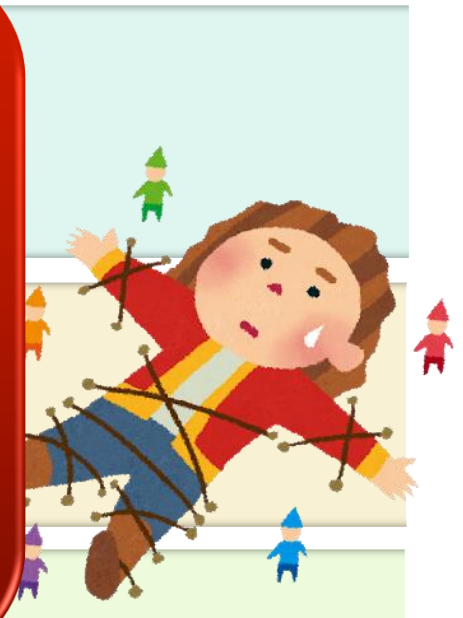
誰でも
環境

課題②

設定の
利用者

課題③

性質上
第三者からのアクセスが容易



システム外への公開は原則禁止

高速性、柔軟性といった
「クラウドの良さ」がつぶれてしまう

2-10. ネットワンが推奨する対策

常に**監査**することで「クラウドの良さ」を残しつつセキュリティリスクを低減する。

課題①
誰でも簡単に利用、設定ができる
環境が用意されている

課題②
設定のセキュリティリスクは
利用者側で担保する

課題③
性質上悪意を持った
第三者からのアクセスが容易

監査

自由に利用、設定させるが
アクティビティを常に**把握、改善**する

常に監査することで
セキュリティリスクを
素早く**検知、改善**する。

素早く**検知、改善**
を行うことでアクセスされる
リスクを低減する。

安心安全

安心安全

安心安全

2-10. ネットワンが推奨する対策

常に**監査**することで「クラウドの良さ」を残しつつセキュリティリスクを低減する。

課題①

誰でも簡
環境が

が
改善する

安心安全

課題②

設定の
利用者

安心安全

課題③

性質上悪
第三者からのアクセスが容易

を行うことでアクセスされる
リスクを低減する。

安心安全

「クラウドの良さ」をつぶさず
セキュリティを確保

「設定ミス」を発見するクラウド監査とは

3-1.「設定ミス」が発生する3つの要因

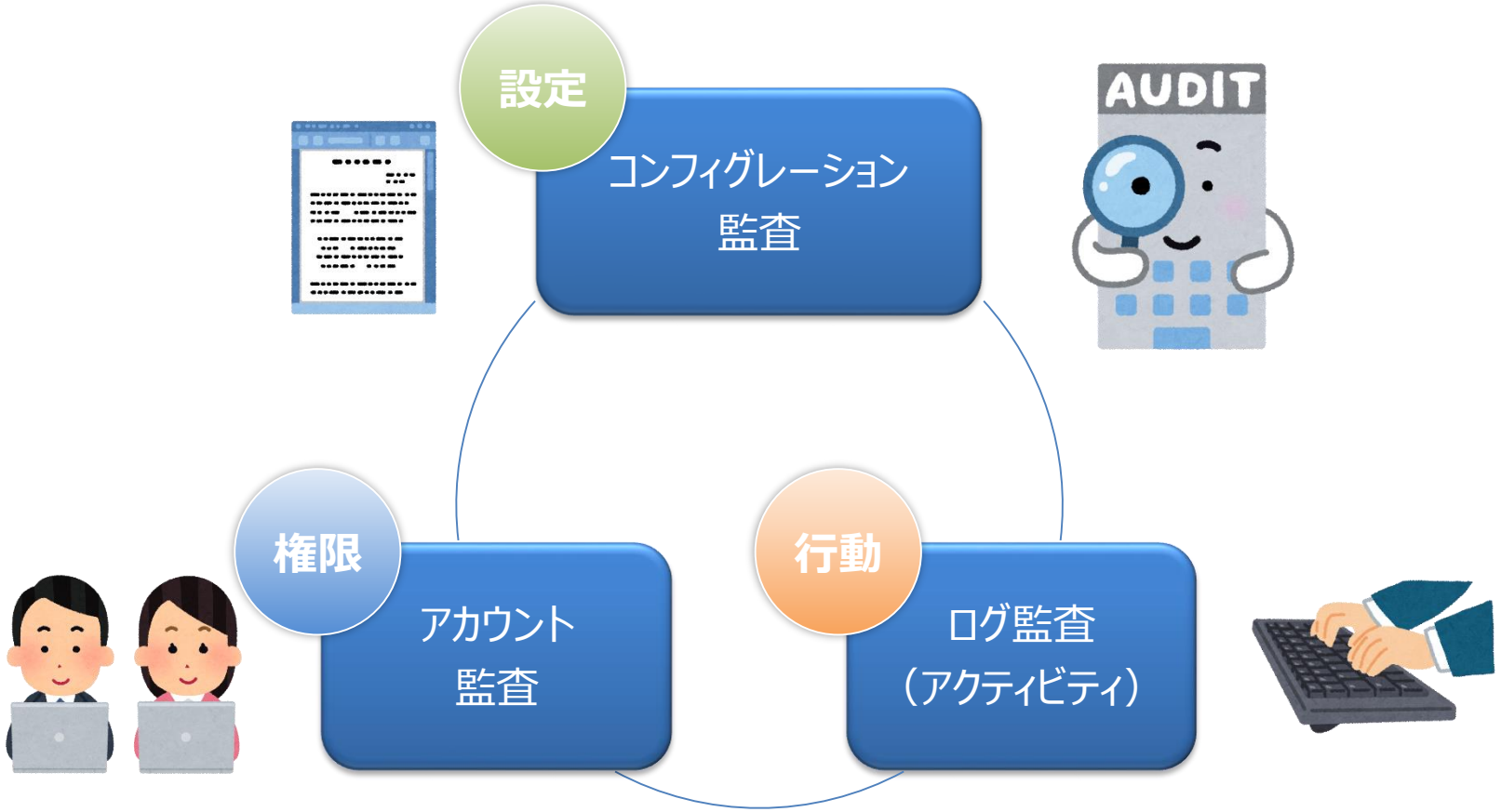
「設定ミス」が発生する3つの要因

「設定」は「権限」を持ったアカウントが「行動」した結果によって生まれる。
そのため、「設定ミス」は以下の3つが原因となる。結果としての「設定」と、
原因としての「権限」と「行動」を監査することで設定ミスを検知する。

- 誤った権限
- 誤った行動
- 誤った設定の影響認識
  (誤も気づかないシステム上の影響があった　など)

3-2. 設定ミスによるインシデントを防ぐための3つの要素

3つの要因対象を監査で検知し、セキュリティを確保する

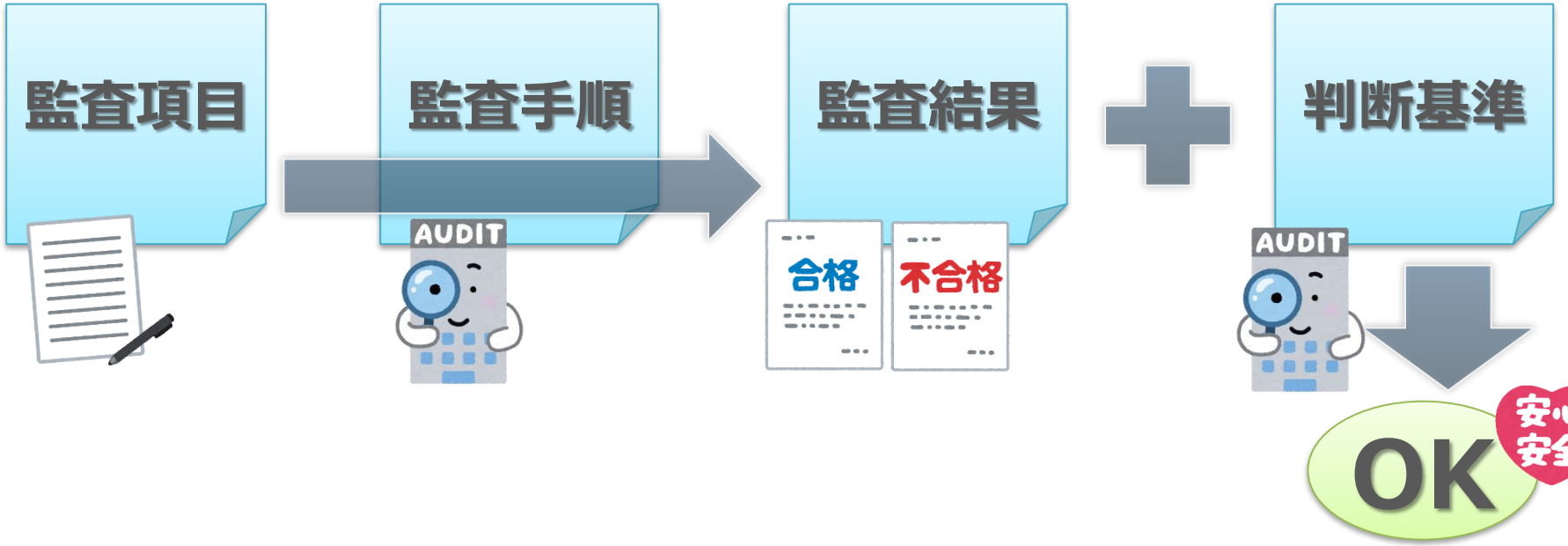


3-3. 監査実施に必要な知識

監査実施に必要な項目、知識
・対象の決定
・項目の決定
・手順の把握
・正常性判断基準の知識

クラウドならではの
要素がある

監査対象



3-4. 監査を行う上での課題

変化の激しいクラウドで正しく監査を行っていくうえでの課題、テクノロジーによる支援

課題①　**項目が不明**

課題②　**基準が不明**

課題③　**手順が不明**

各種ガイドラインや社内規定
CIS/FISC/ISO27001/GDPR
＋クラウドならではの項目

クラウドならではの判断基準

項目を取得するテクニック

テクノロジーでカバー

3-5. Netoneが提供するソリューション

お客様の環境、要件に合わせ最適なサービス・ソリューションをご提供

net one

セキュリティサービス

paloalto NETWORKS®

McAfee™
Together is power.

3-6. コンフィグレーション監査

セキュリティリスクにつながるコンフィグレーションを定期的に監査。米国の非営利団体CISが公表している標準的なベンチマーク等をベースとし、クラウドサービスに合わせた要素を追加して監査する。

(例)

amazon web services

・AWS CloudTrail
・AWS Elastic Load Balancing
・AWS Virtual Private Cloud Flow

API

McAfee Together is power. MVISION Cloud

paloalto NETWORKS RedLock Apeture

【監査項目例】

- マシンイメージへの無制限アクセス設定の監視
- リレーショナルデータベースへの無制限アクセス設定の監視
- ポートへの無制限のインバウンドアクセスなどの監視
- アクティビティログ削除するためにMFAの有効化
- AWSルートアカウントのMFAまたはセキュリティ設定の変更を必要すること
- 不正なアクセスキーの洗出し、削除
- 非アクティブなIAMユーザ/アクセスキーの洗出し、削除

3-7. アカウント監査

アカウントに関するアクティビティを取得、不審な行動を監視。

(例)

amazon web services™

・AWS Identity and Access Management
・AWS CloudTrail

API

McAfee Together is power.

MVISION Cloud

paloalto NETWORKS

RedLock
Apeture

【監査項目例】

- アカウント アクティビティ監視
  （プロビジョニング、機密データへのアクセスなど）
- 不審行動の監視
- ロケーション監視（異なるロケーションから短時間でログイン）
- AWSアカウントに割り当てられたIAM権限を一元表示
- 未利用アカウントの洗出し
- ユーザーアカウント/グループおよびADユーザーと比較し不整合なアカウントの洗出し、削除
- 適切なアクセスレベルを提供

3-8. アクティビティ監査、行動分析

**クラウドから得たアクティビティ情報を解析し、ユーザー、管理者のアカウントを監視。
不正なアクティビティがないか確認することにより、いち早く脅威を発見する。**

(例)

amazon web services

・AWS CloudTrail

API

McAfee Together is power.

MVISION Cloud

paloalto NETWORKS

RedLock
Apeture

【監査項目例】

- AWS Manegement Consoleへのアクセス や AWS APIコールを監視し、IPアドレス、時刻、接続元IPアドレスなどの異常を監査します。

- CloudTrailデータを標準化された一連のアクティビティにマッピングします。

3-9. まとめ

- ✓ クラウド監査は設定、権限、行動の３つを押さえる必要がある。
- ✓ 監査を人力で行うことも可能だが、
  テクノロジーのサポートを利用することで効率的に行える。

継続的監査のすすめ

4-1. 継続的監査の重要性

監査は1回やっておけば良い?

- クラウドは利用者側だけでなく、クラウド事業者側のサービス追加や変更で設定が変わってしまうこともある。
- 知らないうちにセキュリティ問題が発生していることも。

断続的な**監査と改善**による
「健康状態の維持(サイバーハイジーン）」が効果的

4-2. サイバーハイジーンという考え方

- サイバーハイジーンとはシステムにおける**健康診断**といわれる。
- 人体の健康維持と同じく**定期的に監査**を行い、**改善**を行うことにより、セキュリティリスクを**圧倒的に低減**することができる。
- 一般的には、**CISで定義されている以下の５項目**を定期的に診断するだけでも**高い対策効果**が期待できるといわれている。

診断項目

- ■CSC1:　ハードウェアデバイスの管理
- ■CSC2:　ソフトウェアの管理
- ■CSC3:　セキュリティ・コンフィグレーションの管理
- ■CSC4:　脆弱性への対応管理
- ■CSC5:　管理者権限の管理　一部

セキュリティ対策の

85%

をカバー

4-3. ネットワンのセキュリティサービス

サイバーハイジーンを支援するネットワンのセキュリティサービス

Security Service

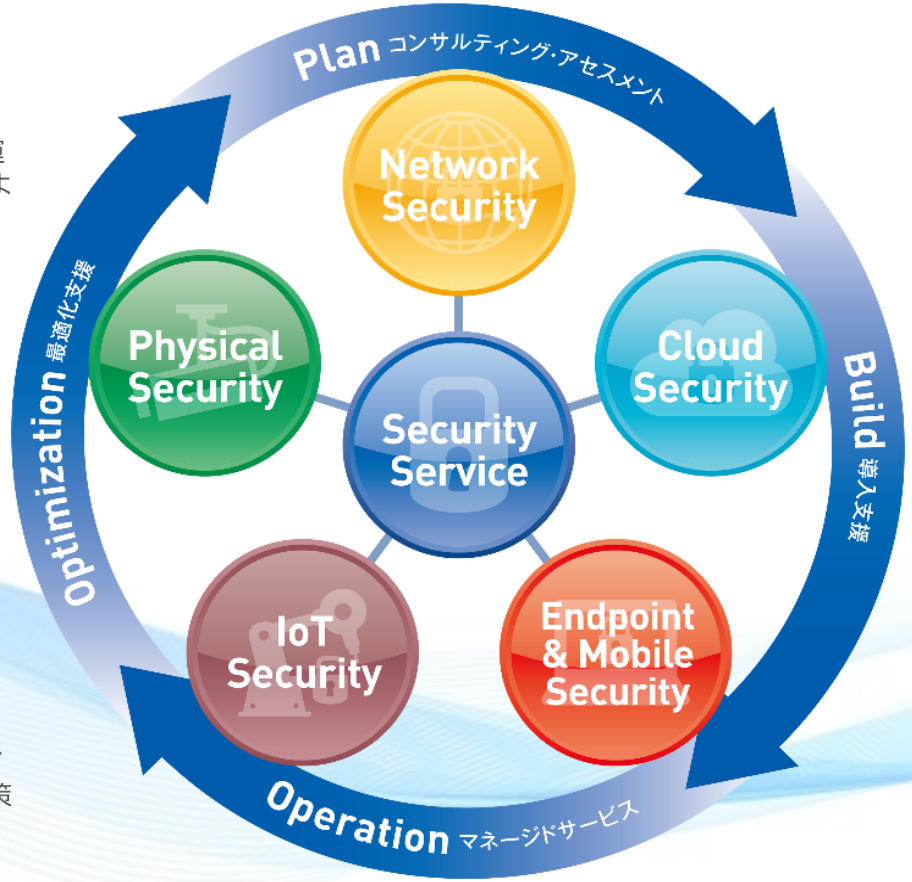
ICT基盤全体のライフサイクル（設計・導入・運用・最適化）の全フェーズを支援することで、より一層のセキュリティ強化を実現

Physical Security

人、モノ、車両の映像検知/解析から入退室管理、それらのシステムを統合管理できるセキュリティプラットフォームまでサポート

IoT Security

工場、産業用制御システム（ICS）などの重要インフラにおけるネットワークの可視化と脅威対策を実現



Network Security

データセンター/本社/支社ネットワークにおける境界線での入口・出口対策から内部対策まで、包括的なセキュリティを実現

Cloud Security

クラウド特有の脅威やリスクからSaaS、IaaS環境の仮想サーバやデータを保護し、安全なクラウド利用を実現することで、組織のセキュリティガバナンス強化を支援

Endpoint & Mobile Security

ファット/シンクライアント、モバイル端末などエンドポイントにおける総合管理、脅威対策、セキュアなリモートアクセスを提供

4-4. まとめ

- ✓ クラウドは変化が激しい。利用者も提供者も。
- ✓ 変化を恐れるのではなく、変化に対応していく。
- ✓ 基盤の安全を確保**し続ける**ことは、情報漏洩防止のみならず「安全である」ということをベースにしてクラウドのさらなる**活用推進**になる
- ✓ 「守り」ではなく**攻めのセキュリティ**
- ✓ 是非NetOneクラウド監査ソリューションを検討して頂きたい

つなぐ ∠ むすぶ ∠ かわる

net one