Orchestrating a brighter world

NEC

McAfee MPOWER 2019 講演資料

NECが語る、CASB運用 "生の声"

2019年11月7日

日本電気株式会社
経営システム本部 CISOオフィス
/ サイバーセキュリティ戦略本部
シニアエキスパート
宮本　智

Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

Agenda

1. 背景
2. CASB 導入
3. CASB 運用　“生の声”

はじめに

経営システム本部

【経営システム本部のミッション】
プロセス・ＩＴの改革によってＮＥＣグループの事業競争力を強化する

・経営戦略・事業戦略の遂行に必要なルール・業務ﾌﾟﾛｾｽ・ＩＴｼｽﾃﾑを実現する
・業務ﾌﾟﾛｾｽ・ＩＴｼｽﾃﾑの全体最適化により、グループの業務改革を推進する
・情報ｾｷｭﾘﾃｨ対策、内部統制対応の推進により、ｸﾞﾙｰﾌﾟのﾘｽｸ低減を図る

企画Ｇ	NEC経営戦略に基づくグループIT戦略・中期計画の策定 グループIT全体最適化推進、全社重要ITプロジェクト推進
経営管理基盤Ｇ	Ｇ１（＊）標準業務プロセスの推進、グループ展開 Ｇ１システム／グループ標準システムのグループ展開

＊G1システム：NEC標準基幹システム。経理・販売・購買機能

CISOオフィスG	➢ **情報セキュリティ基本方針・規程・ルールの制定** ➢ **情報セキュリティマネジメント、情報セキュリティ基盤、情報セキュリティ人材育成に関する企画、推進** ➢ **サイバーセキュリティ対策企画・推進、ＣＳＩＲＴ（＊）対応** ➢ **セキュア開発・運用、協力会社セキュリティ統括**

＊CSIRT：Computer Security Incident Response Team

業務プロセス統括Ｇ	業務プロセス改革・改善する主要テーマの決定 個別テーマ毎のプロジェクト立上げ

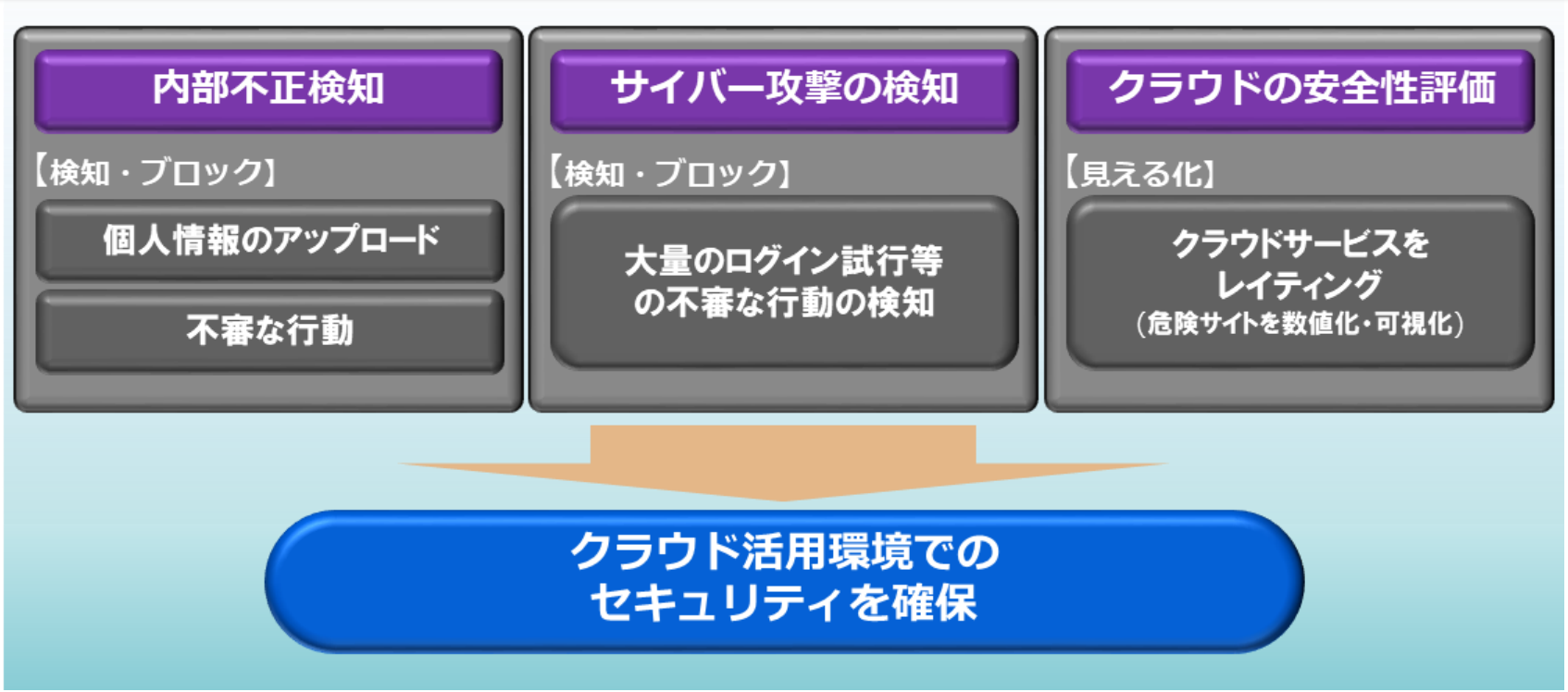
1．背景

NECにおけるクラウドセキュリティの位置づけ

安全・安心にクラウドサービスを利用する環境を実現するため、
クラウドサービス利用におけるセキュリティ対策の強化を実施

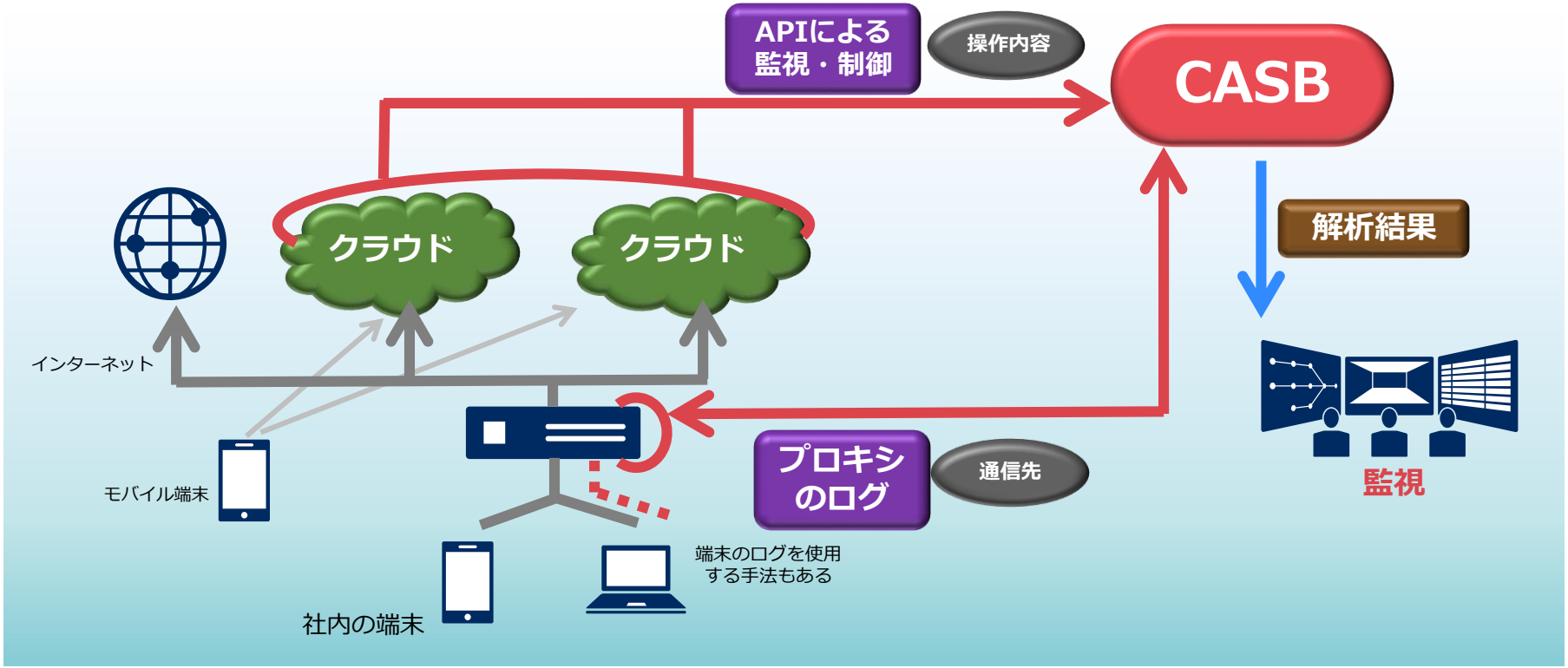
CASB (Cloud Access Security Brokers)とは

クラウド上で発生する「内」と「外」の脅威を監視・抑止・ブロック



CASB (Cloud Access Security Brokers)の概念図

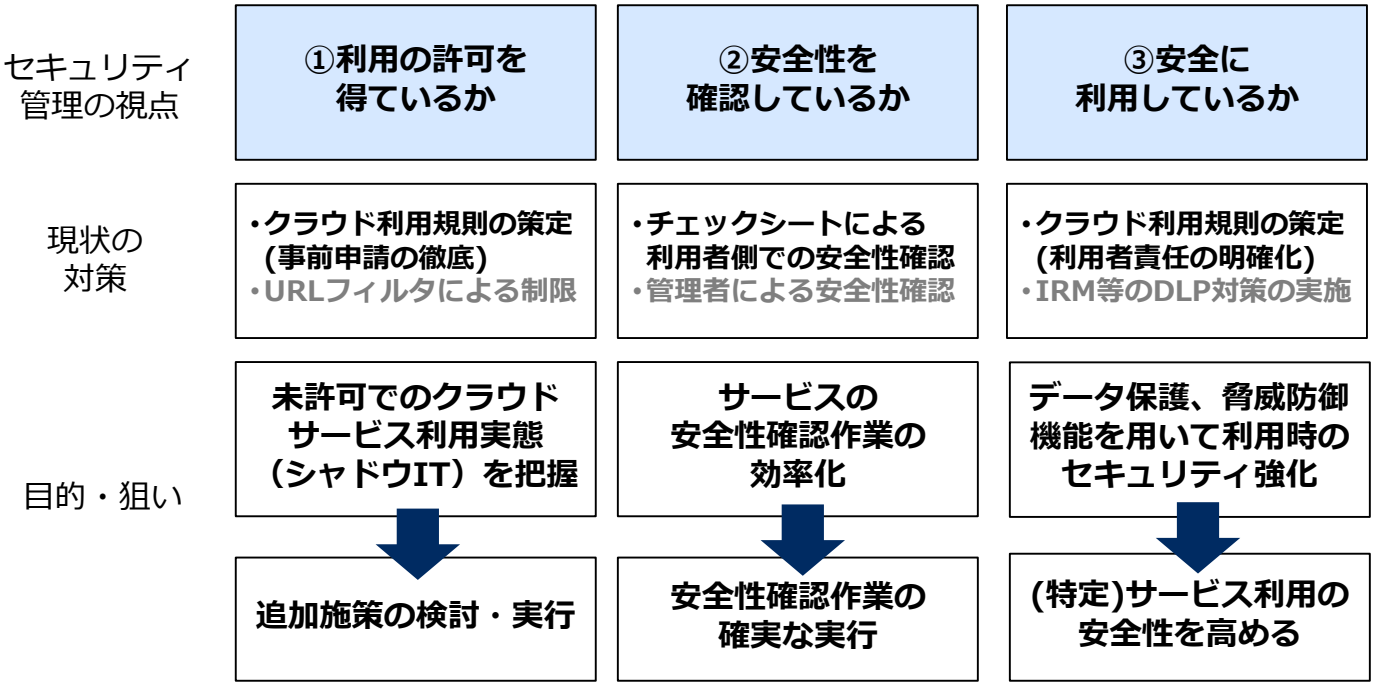
「クラウド」と「プロキシ」を分析し、攻撃・不正を監視・制御



2．CASB 導入

クラウドセキュリティ対策の目的・狙い

ITガバナンスの観点を含め、クラウドサービス利用時のセキュリティ対策をどのレベルまで強化するか、重点を置くべきか(*1)について、整理

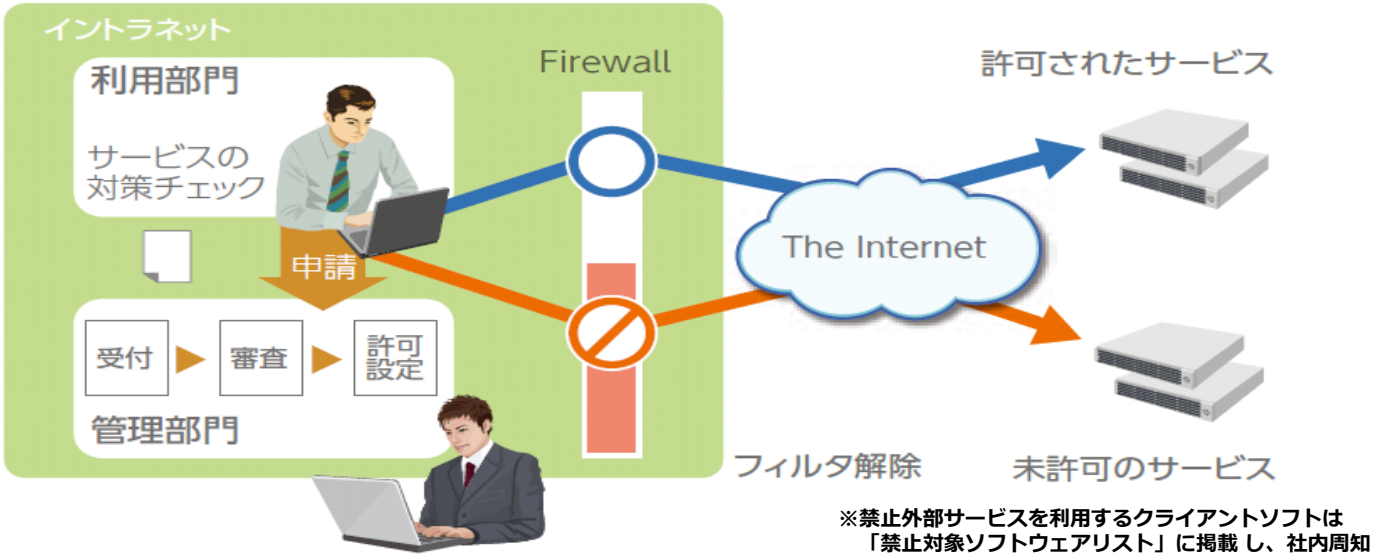


(*1) クラウドセキュリティガイドライン活用ガイドブック(2013)　経産省

クラウドサービスの利用許可

①利用の許可については、業務に利用する際に「外部サービス利用基準」を用いて利用可否を判断

- クラウド等の外部サービスの利用に関して基準を設け、外部サービスのセキュリティ対策についてチェックシートによる事前評価を行い、利用を許可
- セキュリティリスクが高い外部サービスは、利用を禁止※



※禁止外部サービスを利用するクライアントソフトは
「禁止対象ソフトウェアリスト」に掲載 し、社内周知

クラウドサービスの安全性確認・安全な利用

②安全性を確認しているか、および③安全に利用しているか、についてCASBを利用して実現

②安全性を確認しているか

- クラウドサービスの安全性を業界標準の指標を用いて見える化
- クラウドサービスの脆弱性をチェック

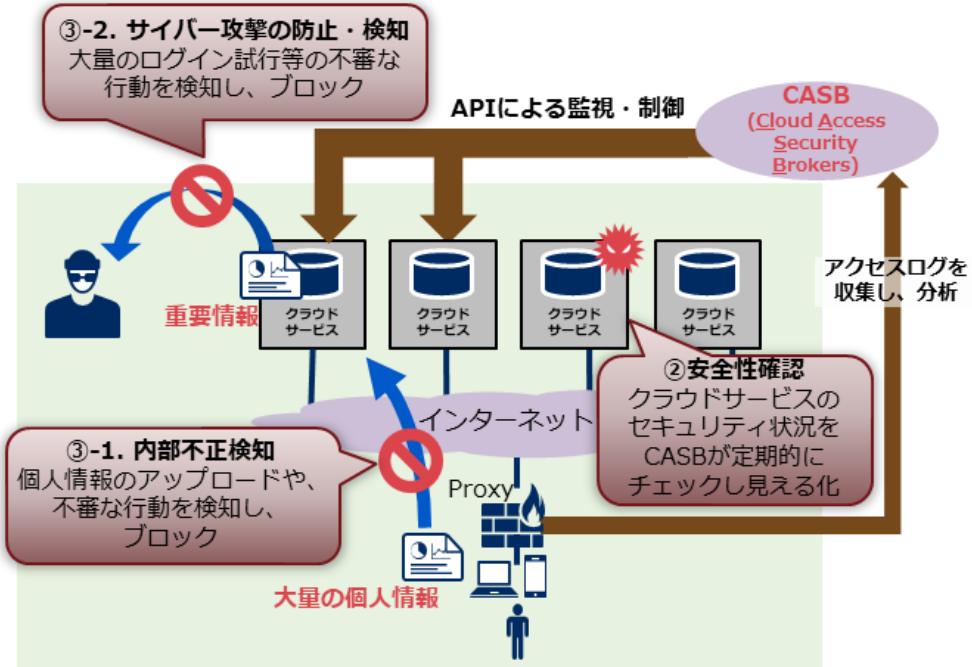
③安全に利用しているか

1. 内部不正検知

- 行動分析により不審な行動(大容量ファイルアップロード、大量の個人情報アップロード、普段と異なる行動等)を検知し、必要に応じてブロック

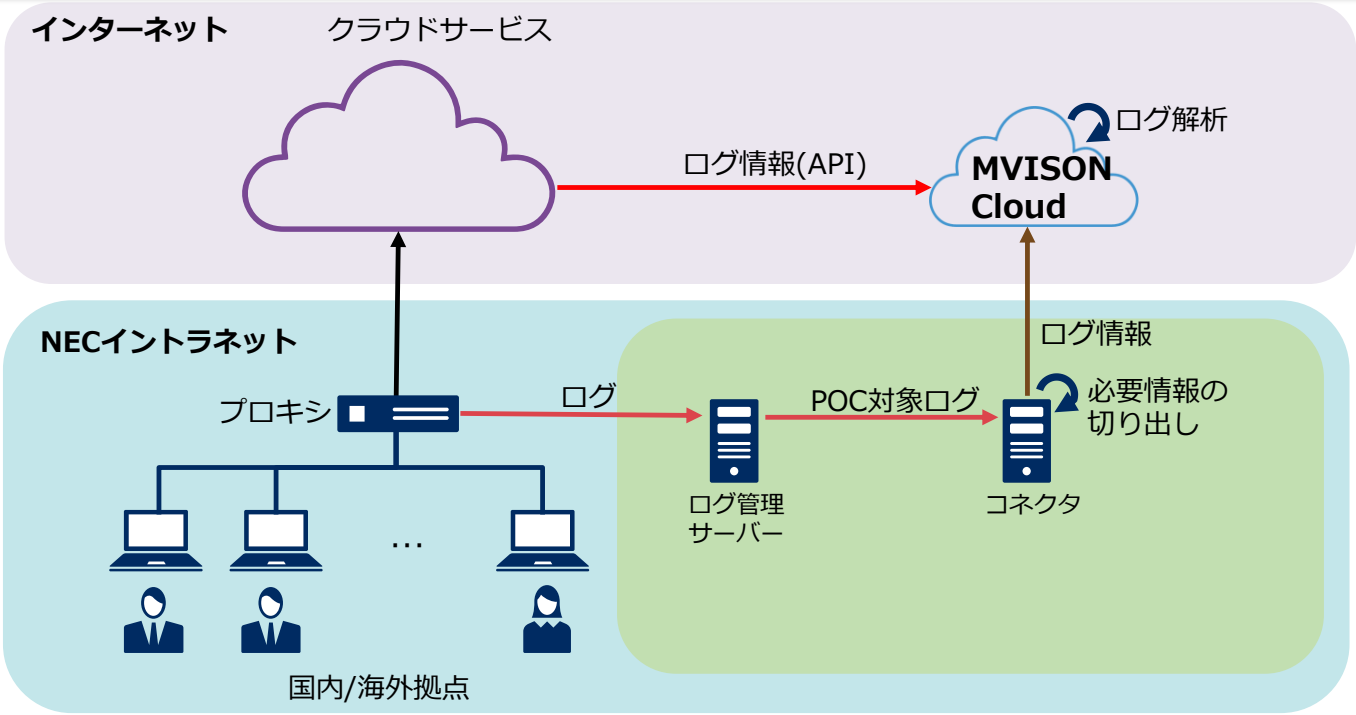
2. サイバー攻撃の防止・検知

- サイバー攻撃の予兆(ログイン試行攻撃、複数の国で同時ログイン、普段と異なる行動等)を検知し、必要に応じて通信のブロック・アラート



導入前にPOCを実施

実環境にCASBを試験導入し、POCを行うことで効果の検証を実施した。
（NECでは、サンクションITとシャドーITの両機能に対し、POCを実施）



POC結果と導入判断

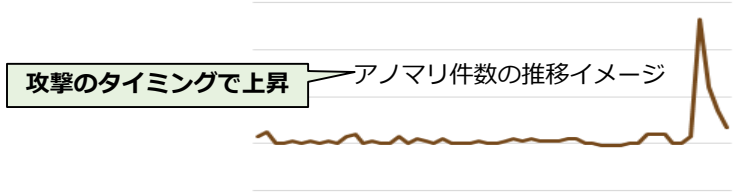
POCを実施した結果、実際にサイバー攻撃等のリスクを見える化し、効果を確認できたことから、導入を決定。

POCから確認できた、主な効果

●サイバー攻撃の検知

- **Office365やboxに対する外部からの攻撃を検知し、予防的な対応が行えることを確認した。**
  ⇒ CASBを導入していない場合、気づかぬうちに情報漏えいが発生しているリスクあり
- 特にCASBはアカウントの振る舞いを監視することから、EDR等では対応できない攻撃に対応でき、導入効果が高いと判断した。

例：短期間に集中した大量のアカウントに対するログイン試行
　–同一アカウントに対する継続的なログイン試行



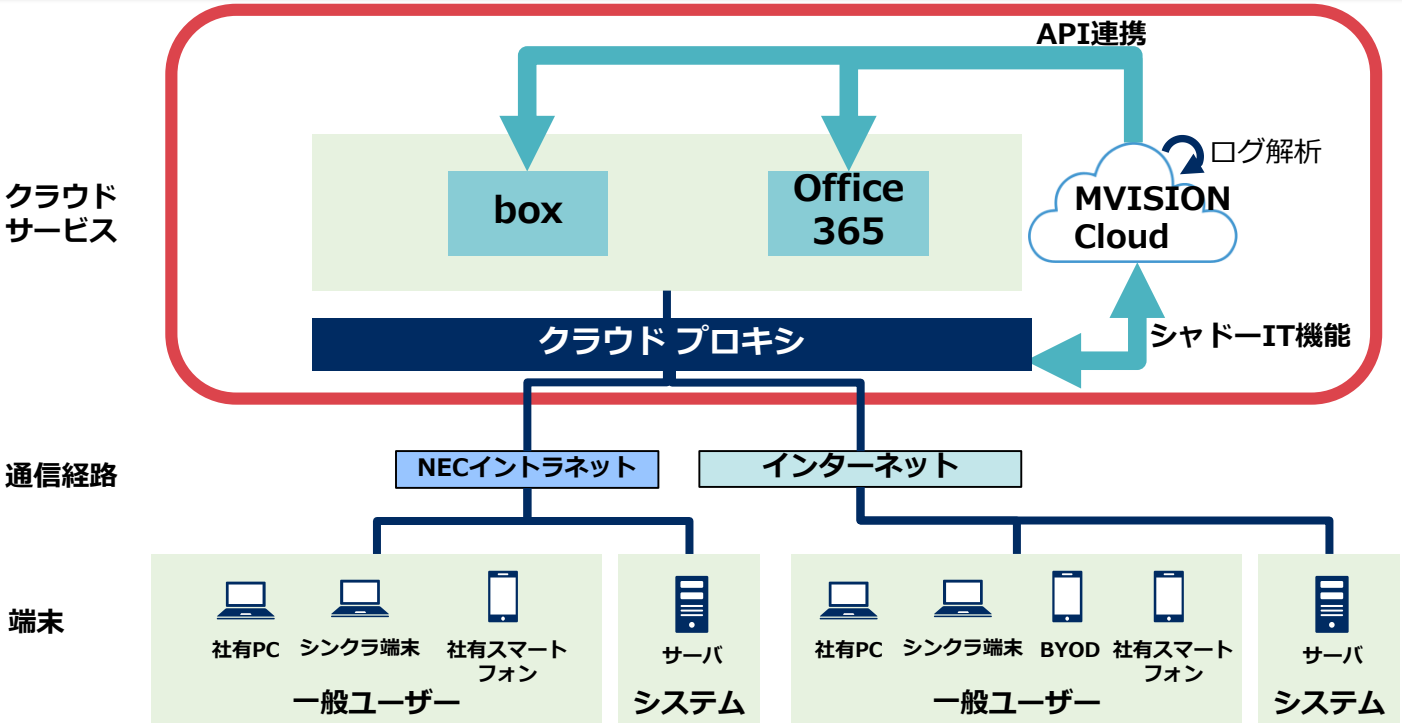
●クラウドサービスの利用状況の監視

- CASBのシャドーIT機能により、NECグループ全体に対してクラウドサービスの利用状況を監視できることを確認した。
- また、リスクの高いクラウドサービスが利用されている場合、他クラウドサービスに誘導する等の対策が可能であることを確認した。

3. CASB運用 "生の声"

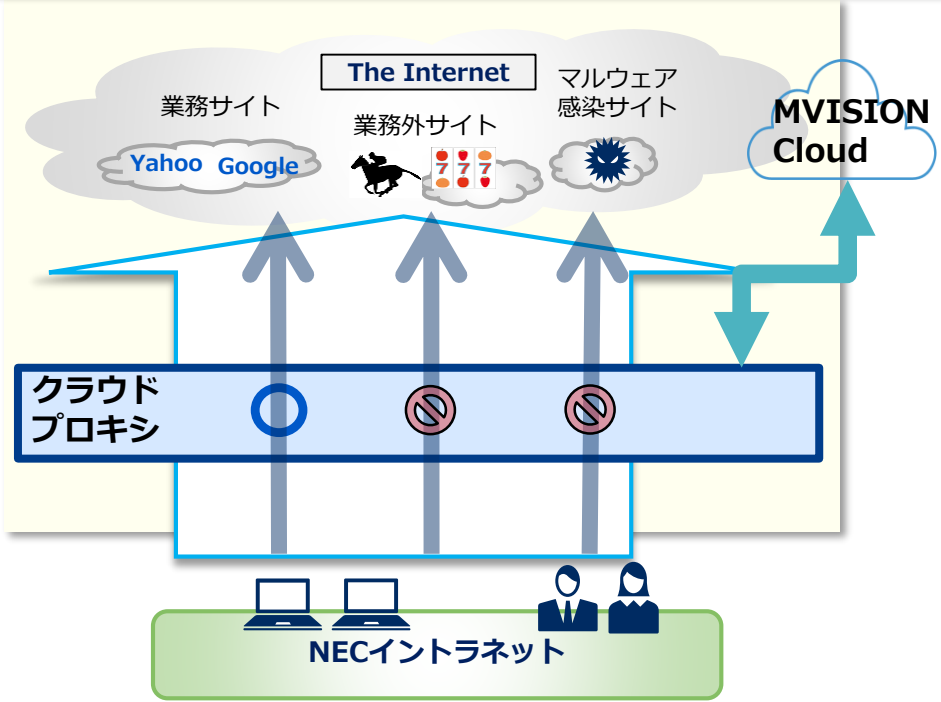
クラウドサービスへのCASBを活用したセキュリティ対策

CASBを活用し、①クラウドサービスの利用可視化、②クラウドサービスの安全性の確認、③クラウドサービスの安全な利用を実施



クラウドプロキシ/CASB連携

クラウドプロキシとCASBとの連携により、不許可のクラウドサービスへのアクセス制御を実現（シャドーIT対策）。



クラウドプロキシとCASB連携

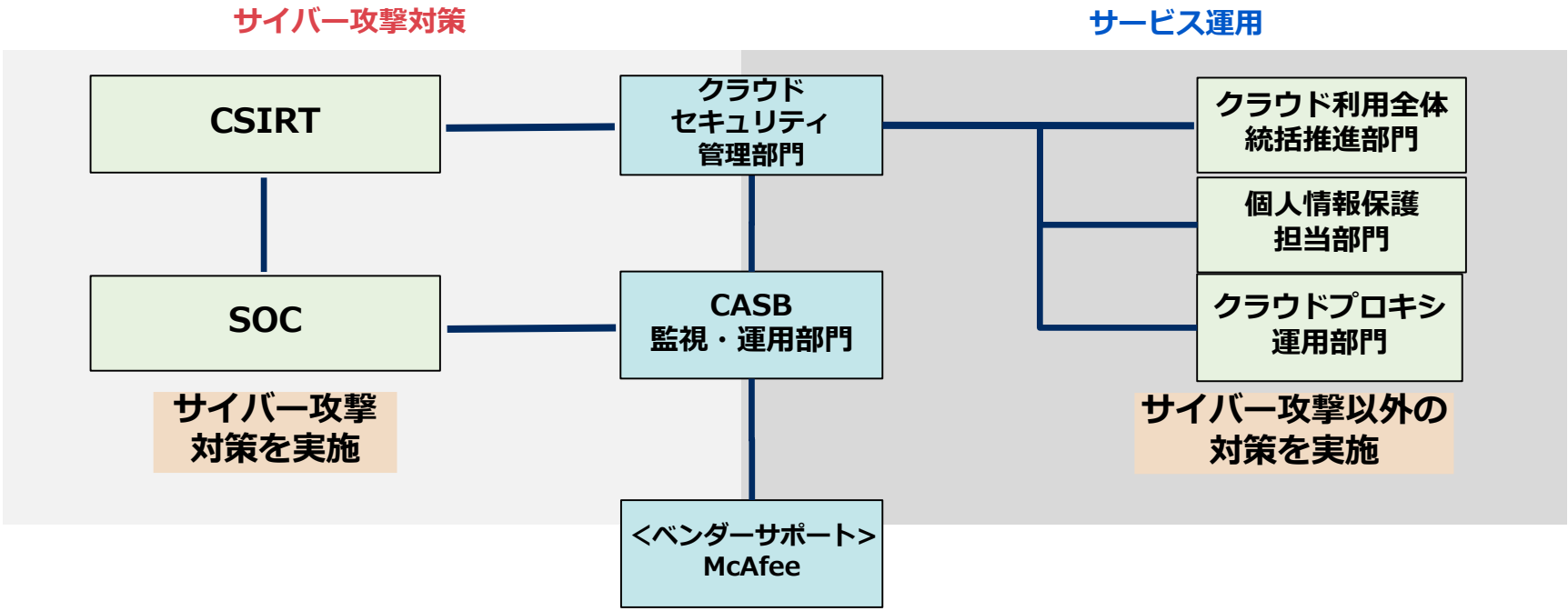
- CASBの検知情報、レイティング情報に基づき、社外サイトのアクセスを制御
  - 不許可のクラウドサービスの利用を制御
- トレーサビリティ
  - クラウドプロキシでのロギング情報に基づき、シャドーIT対策を実施

インターネットの脅威からイントラネットを防御

- URLフィルタリング
  - マルウェアサイトの遮断
  - 業務外サイトの遮断でサボタージュを抑制
- トレーサビリティ

クラウドセキュリティ運用体制

サイバー攻撃対策とサービス運用の2軸で運用体制を構築し、相互連携するCSIRTの位置づけを変える必要あり



クラウドインシデント対応

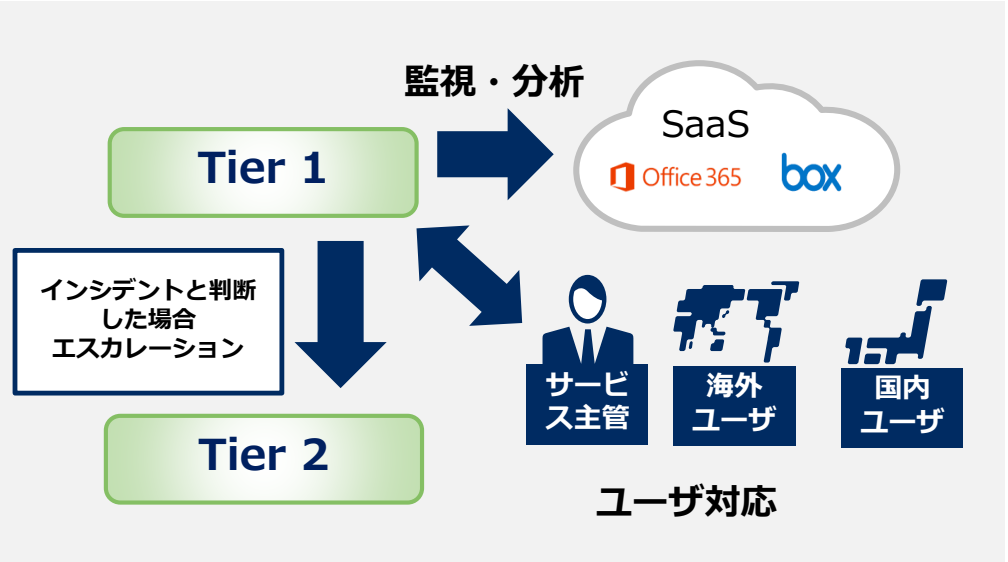
クラウドインシデントの対応は、アノマリ検知・調査・分析をするTier 1インシデントレスポンスを実施するTier 2の2階層で対応する。

Tier 1：アノマリ検知・調査・分析

- **部門:**
  SOC (Security Operation Center),
  NOC (Network Operation Center)
- **対応:** CASBによるクラウド監視・分析
  ユーザ、及び利用部門へのヒアリング
  インシデントと判断した場合、
  Tier2部門に対応依頼

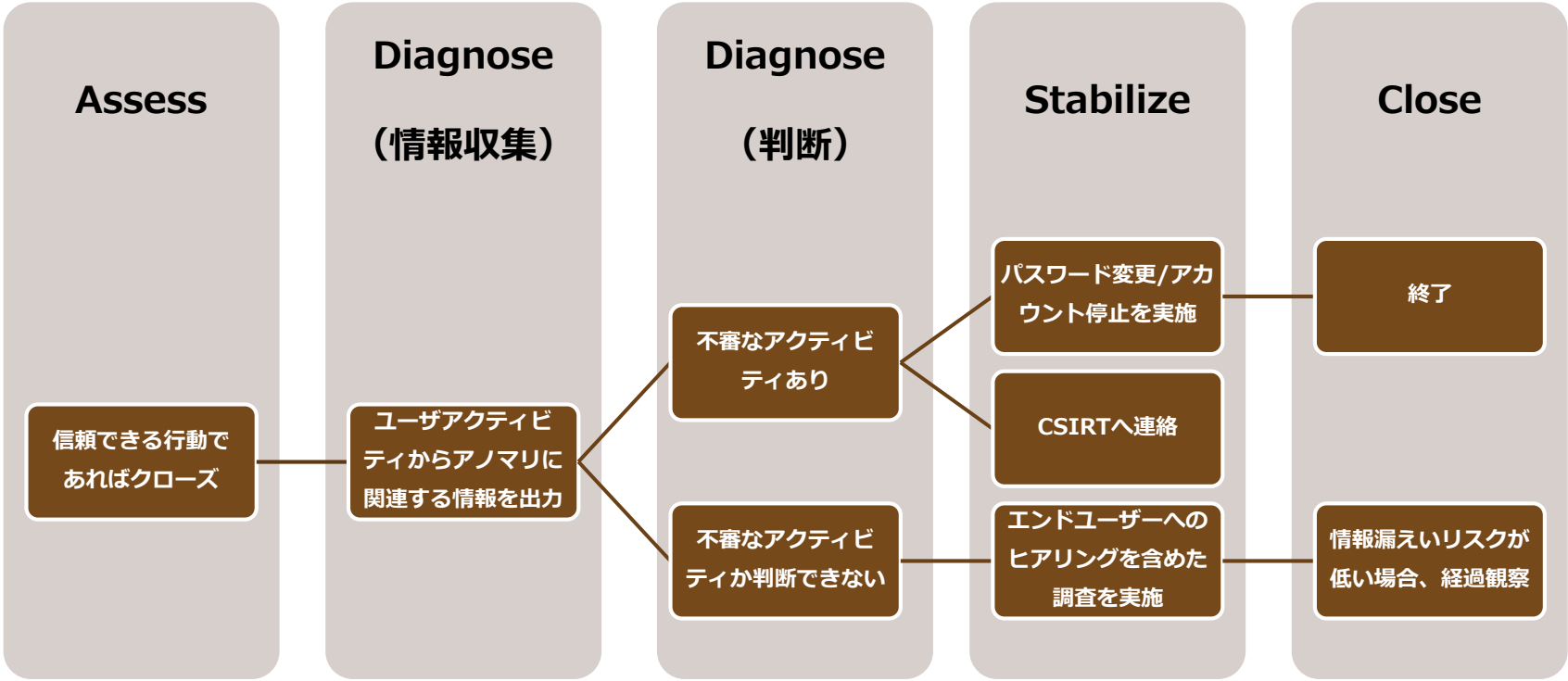
Tier 2：インシデントレスポンス

- **部門:**
  CSIRT
  (Corporate Security Incident Response Team)
  対応: セキュリティインシデント対応



アノマリ対応フロー

アノマリ発見時の対応フローは、下記の5ステップで実施



参考：Superhumanの想定シナリオ

アノマリ検知時の想定シナリオをアノマリ毎に定義し、情報収集をした上で、実際どのような状況なのかを検証するシナリオを作成

想定するシナリオ

- ログインの不正な試みが成功しているのではないか

想定するシナリオを検証するための情報収集

- 他にログイン失敗、成功しているアクティビティがないか
- 該当ユーザたちは普段どんなアクティビティなのか（普段より数が増えたのか、質的に変わったか）
- どのような情報をアノマリと判定する原因としているのか（地理的情報・時間間隔）

想定するシナリオの検証結果

- 想定したシナリオは正しかった（ログインの不正な試みが成功していた）
  - CSIRTやCISO案件とするか検討
- 想定したシナリオは否定された（ログインの不正な試みは成功していない）
  - クローズ
- 想定したシナリオの正否は判定できない（ログインの不正な試みが成功しているとはいえない）
  - クローズもしくは経過観察（情報収集の結果を元に判断する）

参考：NEC/Infosecによるクラウド活用支援

NEC社内導入で培ったノウハウを元に、お客様のクラウド活用に向けて、導入から運用までの様々なシーンにおけるお悩みをNECおよびInfosecでご支援します。

導入支援

- クラウド利用時に必要となる規程・ガイドラインの整備をご支援します
- 貴社の環境、ご利用中のクラウドを考慮した導入をご支援します
- 対策に必要な製品・サービスの構築・設計をご支援します

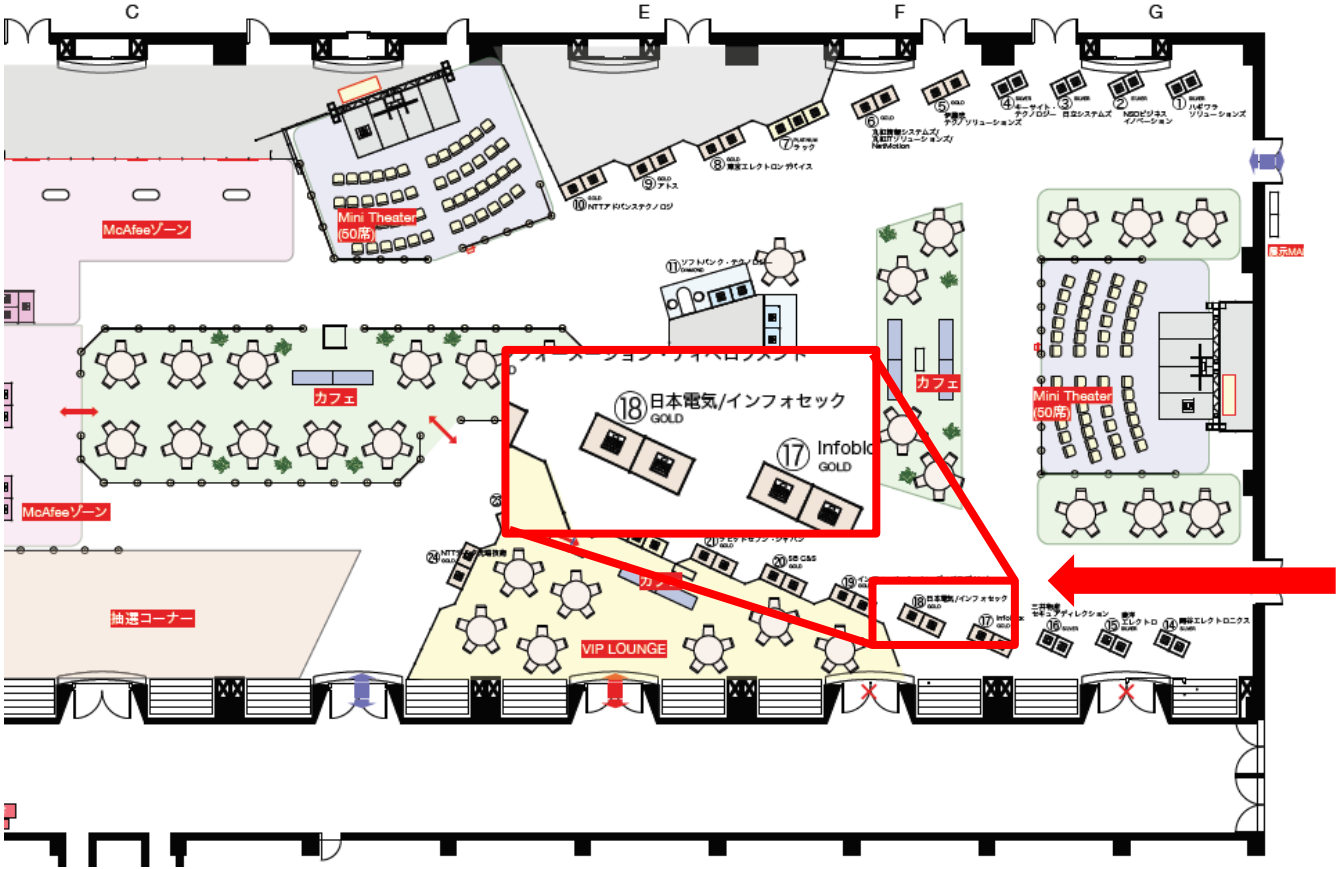
運用設計

- CASB運用設計書及びアノマリ対応フローの策定のご支援をします

定常運用

- アノマリ調査プロセスのレビューを行い、新種攻撃にも対応できるフローへの改善のご支援をいたします。
- その他、利用に伴う各種の改善（利用者認証方法等）を多方面からご支援します

ご案内：Infosec/NECブース



入口目の前
18番ブース


Orchestrating a brighter world
NEC