



CASB WG 活動報告

*Koichi Ueda, CSA CASB-WG
2016, Nov.22*

はじめに (お約束で)

- “CASB”
を聞いたことがありますか？
- “CASB”の導入、または提案を
具体的に検討したことが
ありますか？

2年前

いち早く。より深く。さらに高みへ。

The Only One Value



CSA Japan Congress 2014

クラウド・SaaSに怯えない

リスク管理・ポリシー設定・セキュリティ対策で積極活用にシフトチェンジ

2014年11月21日

マクニカネットワークス株式会社

ビジネスディベロップメント室

渋谷勝則

CASB (Cloud Access Security Broker)

- 調査会社のガートナーが2014年情報セキュリティテクノロジーTop10の最初に記載
 - 2016年までに大手企業の25%はCASBプラットフォームを介してクラウドサービスへのセキュアなアクセスを行う
 - Adallom
 - Bitglass
 - CipherCloud
 - Elastica
 - FireLayers
 - Netskope
 - Perspecsys
 - Skyfence
 - Skyhigh Networks
 - など多くのベンダーが現れてきているエリア
- リスクスコアリング、モニタリング、暗号化、トークナイズ、クラウドDLPなど実装は様々

Strategic: What are the leading enterprises doing with cloud now?

戦略： 先進的な企業はどのようにクラウドを扱っていますか？

- CASB: Cloud Access Security Broker
CASB: クラウドアクセスセキュリティブローカ
(クラウドへの安全なアクセスを提供する業者)
- DevOps
- Container technologies: Docker, Rocket
コンテナ技術: Docker, Rocket
- Security analytics
セキュリティ・アナリティクス
- Integration of Internet of Things
IoTの統合
- Creating new native cloud security strategies
新しいクラウド固有のセキュリティ戦略の構築

1年半前

この夏の報道でも...

● ガートナー

「2016年 注目すべき情報セキュリティ・テクノロジーのTop10」

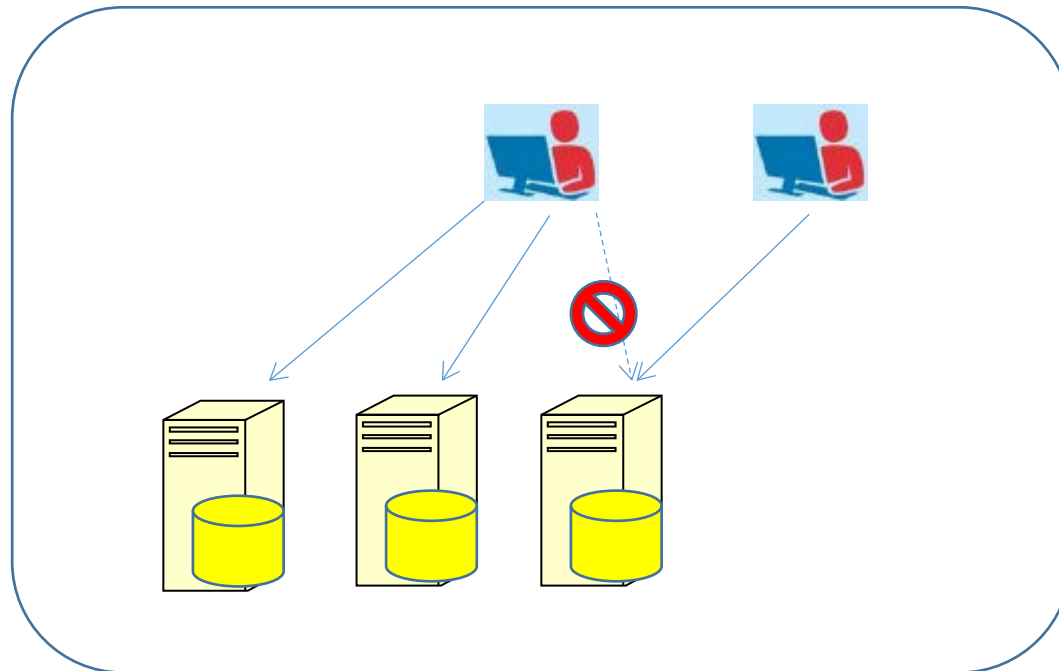
- クラウド・アクセス・セキュリティ・ブローカ(CASB)
- エンドポイントの検知／対応 (EDR)
- エンドポイントのセキュリティ保護に対するノンシグネチャ型アプローチ
- ユーザー／エンティティ挙動分析 (UEBA)
- マイクロセグメンテーションおよびフローの可視性
- DevOpsのためのセキュリティ・テスト
- インテリジェンス主導型セキュリティ・オペレーション・センター (SOC) のオーケストレーション・ソリューション
- リモート・ブラウザ (ネットワーク分離)
- 偽装テクノロジー (Deception)
- 広域なトラスト・サービス

CASB(Cloud Access Security Broker)

- 調査会社のガートナーが、2012年に初めて提唱
- 組織のクラウド利用において共通のポリシーを適用可能とするもの(テクノロジー、フレームワーク、業者)
- 4つの柱からなる
 - 可視性
 - コンプライアンス
 - データ保護
 - 脅威からの防御

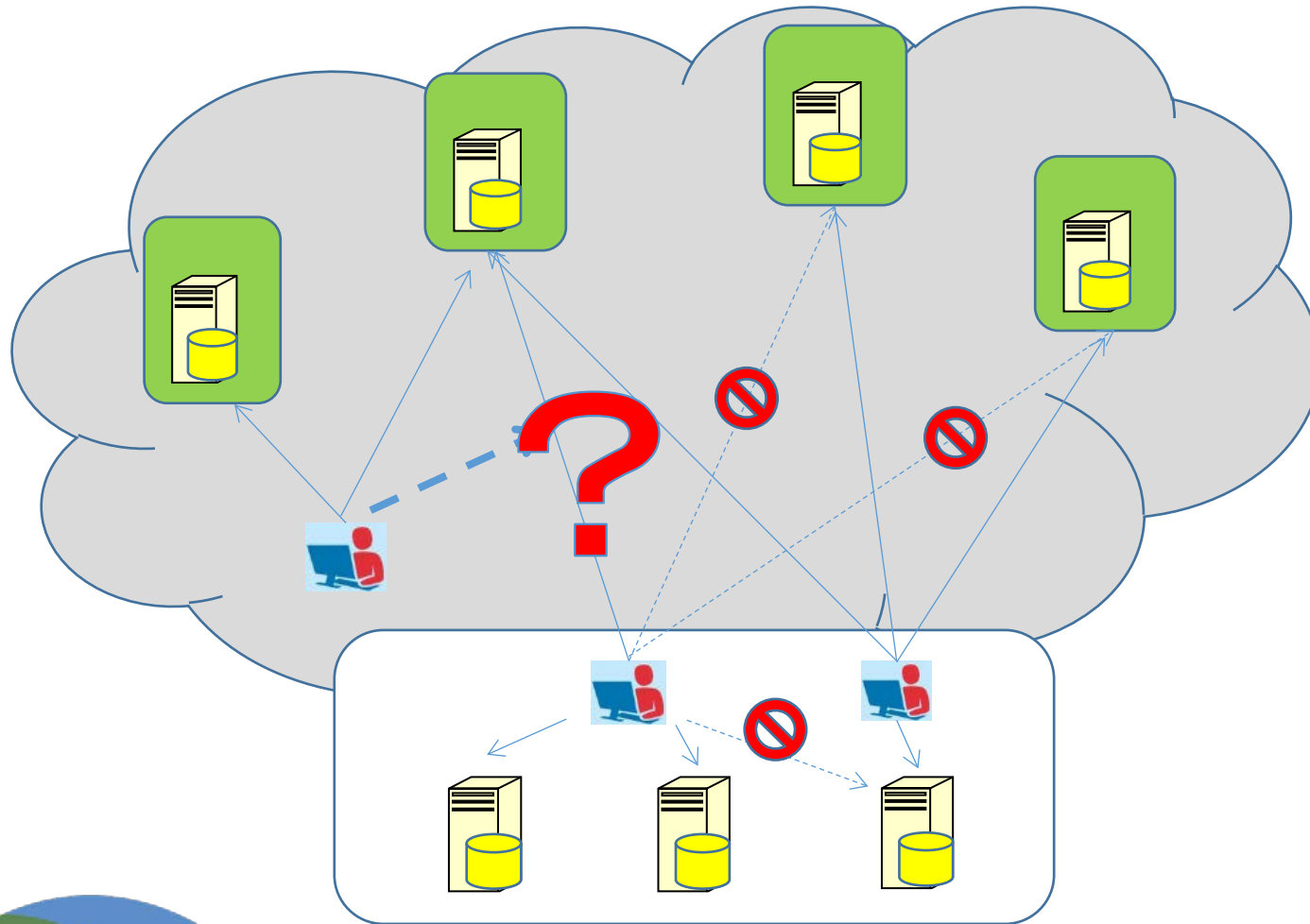
従来型セキュリティ

- データ、利用者、アクセス経路などは、あくまで自組織内部
- その中で、可視性、コンプライアンス、データ保護等を実現



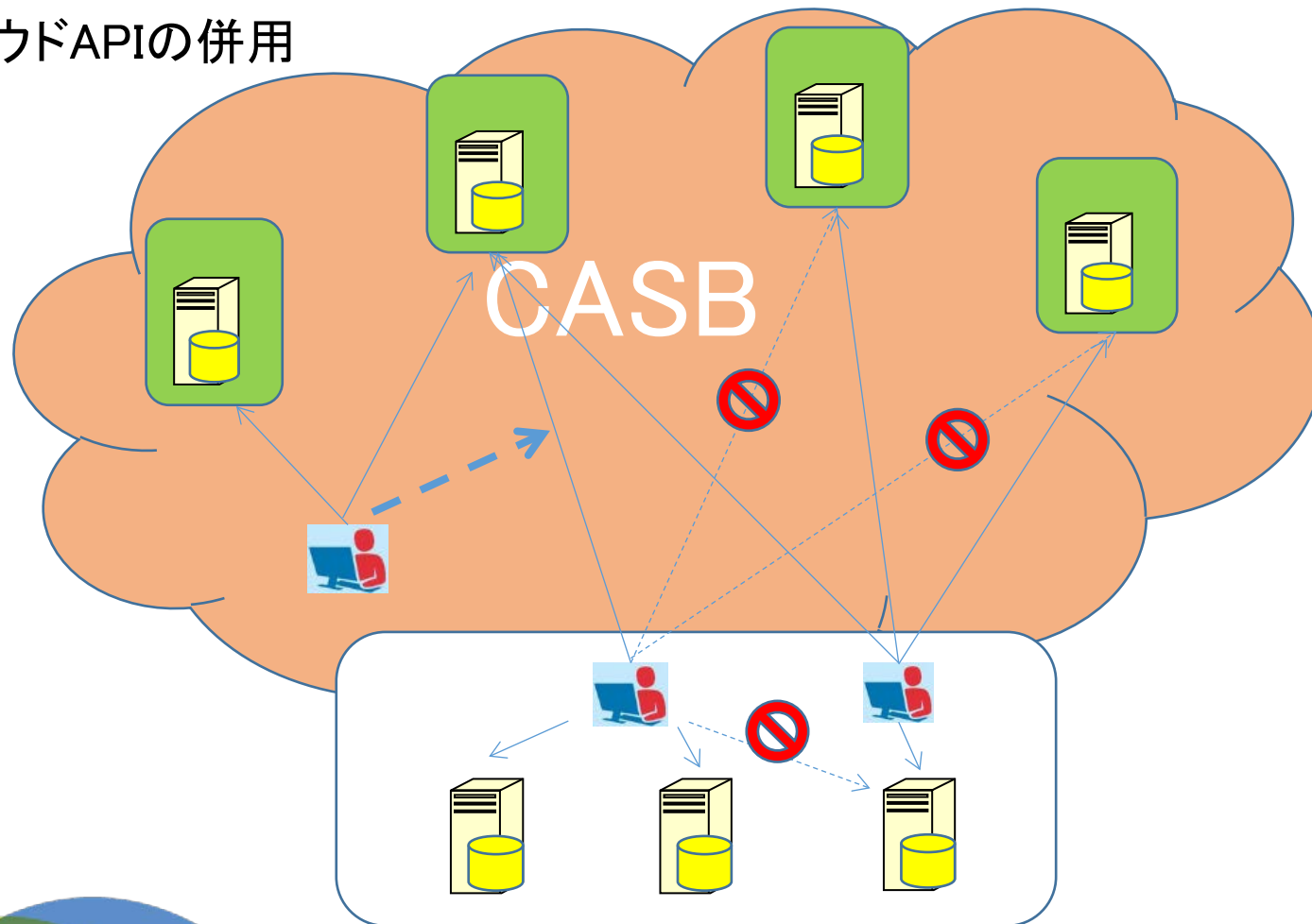
マルチクラウドではどうなるか

- 「可視性」「コンプライアンス」「データ保護」「脅威からの防御」



そこでCASB

- 「可視性」「コンプライアンス」「データ保護」「脅威からの防御」の実現
- リバースプロキシ、フォワードプロキシなどの実装
- クラウドAPIの併用



CASB導入事例（海外：テレコム会社）

- 課題

- 従業員15,000名
- Google Apps利用におけるデータセキュリティの担保

- 要件

- 企業のポリシーに反するファイルの検知
- 機密情報を含むファイルの検知
- ファイルに対する選択的な暗号化の実施

可視化
コンプライアンス
データ保護

- 結果

- ポリシー違反のファイルをGoogle Apps上で自動で特定、検知
- その他3rdパーティクラウドへの機密情報保存を禁止制御
- 制御すべきシャドーITの見極めと監査

CASB-WGについて

- CASBに関するCCM連携研究、情報提供、普及を目的に設立
- 2016年2月に活動開始
- 当初、共通の用語集作成を目指す
- 現在ホワイトペーパー作成に取り組む
- 現在、会員数10弱のメンバーで活動中
(企業会員、個人会員)

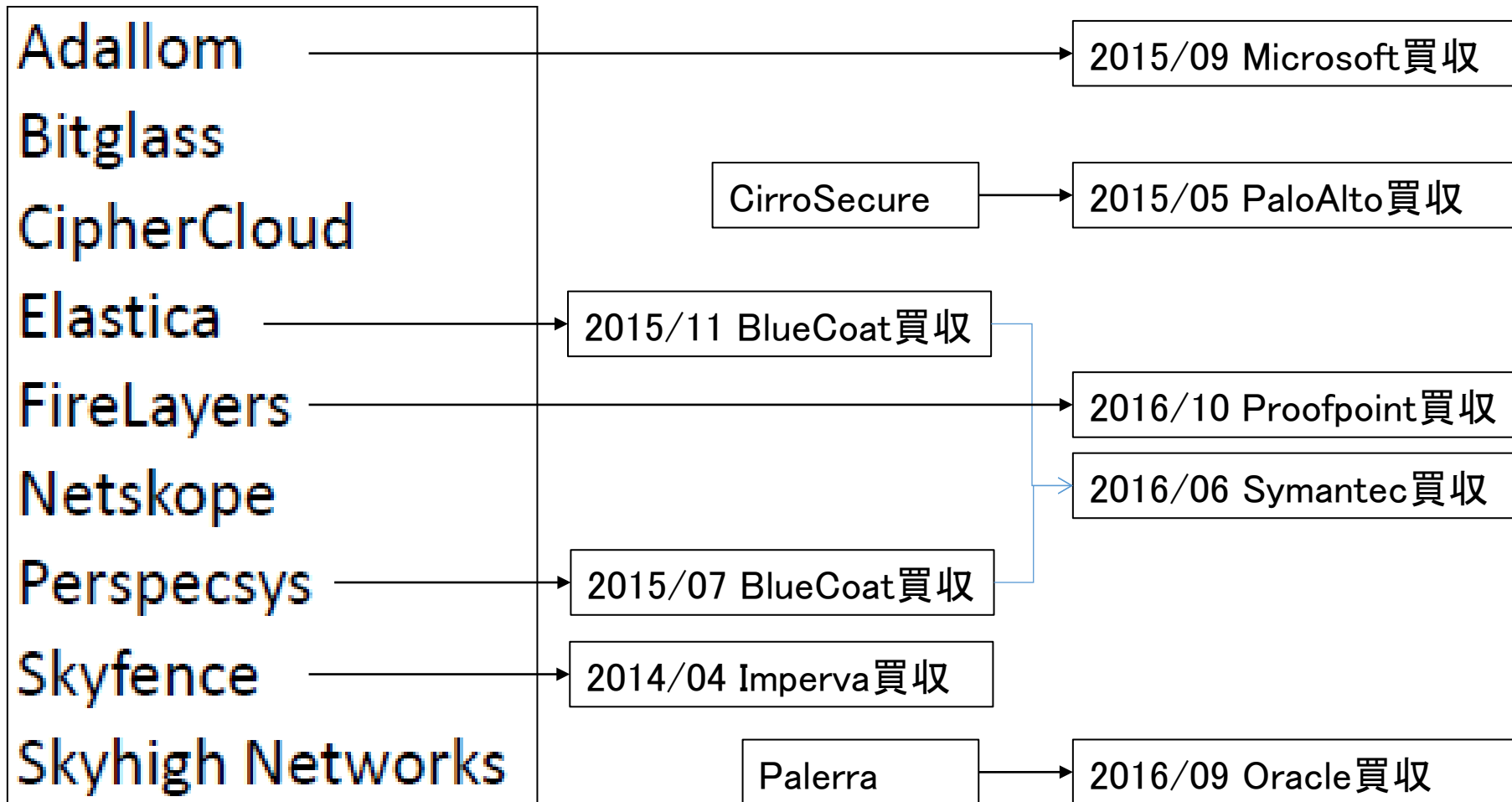
WGでの議論

- 用語の不統一は、想定程にはなかったが、理解には事例が必要
- 事例抽出の軸は？
 - シャドーIT対策、内部不正対策、事業者監査？
- CASBの説明とクラウドセキュリティ全体の説明のバランス
- 中立性の確保
- 最終的にガートナーの4つの柱に落ち着く

CASB (Cloud Access Security Broker)

- 調査会社のガートナーが2014年情報セキュリティテクノロジーTop10の最初に記載
 - 2016年までに大手企業の25%はCASBプラットフォームを介してクラウドサービスへのセキュアなアクセスを行う
 - Adallom
 - Bitglass
 - CipherCloud
 - Elastica
 - FireLayers
 - Netskope
 - Perspecsys
 - Skyfence
 - Skyhigh Networks
 - など多くのベンダーが現れてきているエリア
- リスクスコアリング、モニタリング、暗号化、トークナイズ、クラウドDLPなど実装は様々

それから2年...



最後に (お約束で)

- 非常に動きの速い分野ですので、CSAジャパンとしても注目してウォッチしてまいります。
- ホワイトペーパーは近日公開予定です。
- CASB-WGの活動メンバーを募集しております。
 - 以下の方々の参加がございます。
 - 製品ベンダー
 - インテグレータ、ディストリビュータ
 - ユーザ企業
- ご興味のある方はぜひお声掛けください！

ありがとうございました