2013年10月26日ISACA　CISMカンファレンス

クラウドセキュリティに於ける内部ガバナンスと外部ガバナンス

日本クラウドセキュリティアライアンス
理事　山崎英人
ISO27000,CRISC

CSAJC cloud security alliance Japan Chapter

はじめまして

- SEから法務部、情報セキュリティ、コンプライアンス、内部統制、危機管理、監査を経験してきました。

監査の独立性
アセンブラー
ルーター
ハッカー逮捕
偽計業務妨害
Oracle
Fire wall
IT全般統制
ISMS
震災対策
Audit
Linux
金融商品取引法
Sybase
SQL

本プレゼンテーションは山崎の個人的な見解によるものであり、所属する企業や団体の見解を反映したものでは無い事を御承知置き下さい。

CSAの御紹介

- クラウドセキュリティに関するベストプラクティスの作成と調査研究
- 世界規模の非営利団体
- 35,678名以上の個人会員
- 123社の法人会員
- 64の支部

CSAの主な活動/成果物

Security, Trust & Assurance Registry

CSA Security Guidance V3.0

クラウドコンピューティングのためのセキュリティガイダンス

CAI Cloud Audit

CSA STAR

Cloud SIRT

CCM

コントロールマトリクス

他の基準との連結

ISO27001/HIPAA/HITECH Act/AICPA/COBIT4.1/ ENISA IAF/ FedRAMP/ PCI DSS v2.0

CCSK Certificate of Cloud Security Knowledge

WGや研究活動

CSA Mobile

Big Data

その他、ヘルスケア等

CSAJC cloud security alliance Japan Chapter

CSAジャパンの概要

- 名称：日本クラウドセキュリティアライアンス
- 英文：Cloud Security Alliance Japan Chapter
- 会員：約290名（LinkedIn JC Subgroup登録人数）
- Board of Directors：（50音順）
  - 勝見　勉　　加藤雅彦　　上村竜也　　笹原英司
  - 佐藤元彦　　塩崎哲夫　　須崎有康　　高橋郁夫
  - 塚田栄作　　二木真明　　原田要之助　　丸山満彦
  - 諸角昌宏　　山崎英人　　吉井和明
    - 全員がボランティアとして活動
- 設立：2010年6月（世界で2番目の公認支部）

CSAジャパン　主な活動

- 2012/9/28　CSA-KPMG（あずさ監査法人）合同セミナ
- 2012/11/8-10　CSA Congress参加&発表
- クラウドコンピューティングのためのセキュリティガイダンスV3翻訳　2013年4月リリース

https://chapters.cloudsecurityalliance.org/japan/files/2011/05/csaguide.v3.0.1_J.pdf

- CCM日本語版の作成　　2013年6月　CCM1.4Jリリース
  - https://chapters.cloudsecurityalliance.org/japan/files/2011/05/CSA_CCM_v1.4-J.pdf

- CCSK試験問題の翻訳by あずさ監査法人
- 事務局体制の整備への取組み

2013年11月に法人化を予定

まもなく会員募集開始

WGによる特定分野に特化した、問題の検討や意見交換

ガイダンスやコントロールマトリクスなどのレビュー参加やβ版等の早期入手

定例会/セミナー等での最新情報入手と情報交換

メーリングリストや意見交換掲示版での交流

詳しくは
info@jp.chapters.cloudsecurityalliance.org
にお問い合わせください

CSAJC cloud security alliance SM Japan Chapter

初めに

本プレゼンテーションでお話する事
◎クラウドの基礎知識や脅威
◎企業の義務(ガバナンス)
◎クラウドセキュリティ
◎クラウドセキュリティのガバナンス

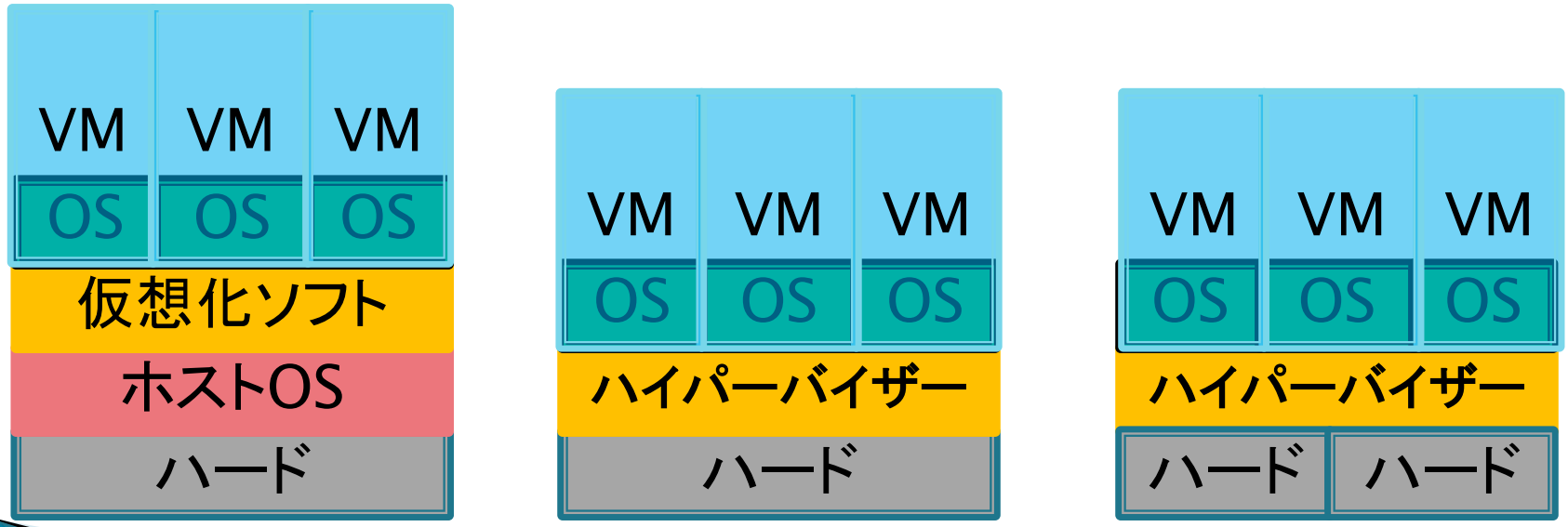
クラウドの基礎知識や脅威

クラウドの
基礎知識
や脅威

仮想化技術とクラスタリング

クラウドの基礎知識や脅威

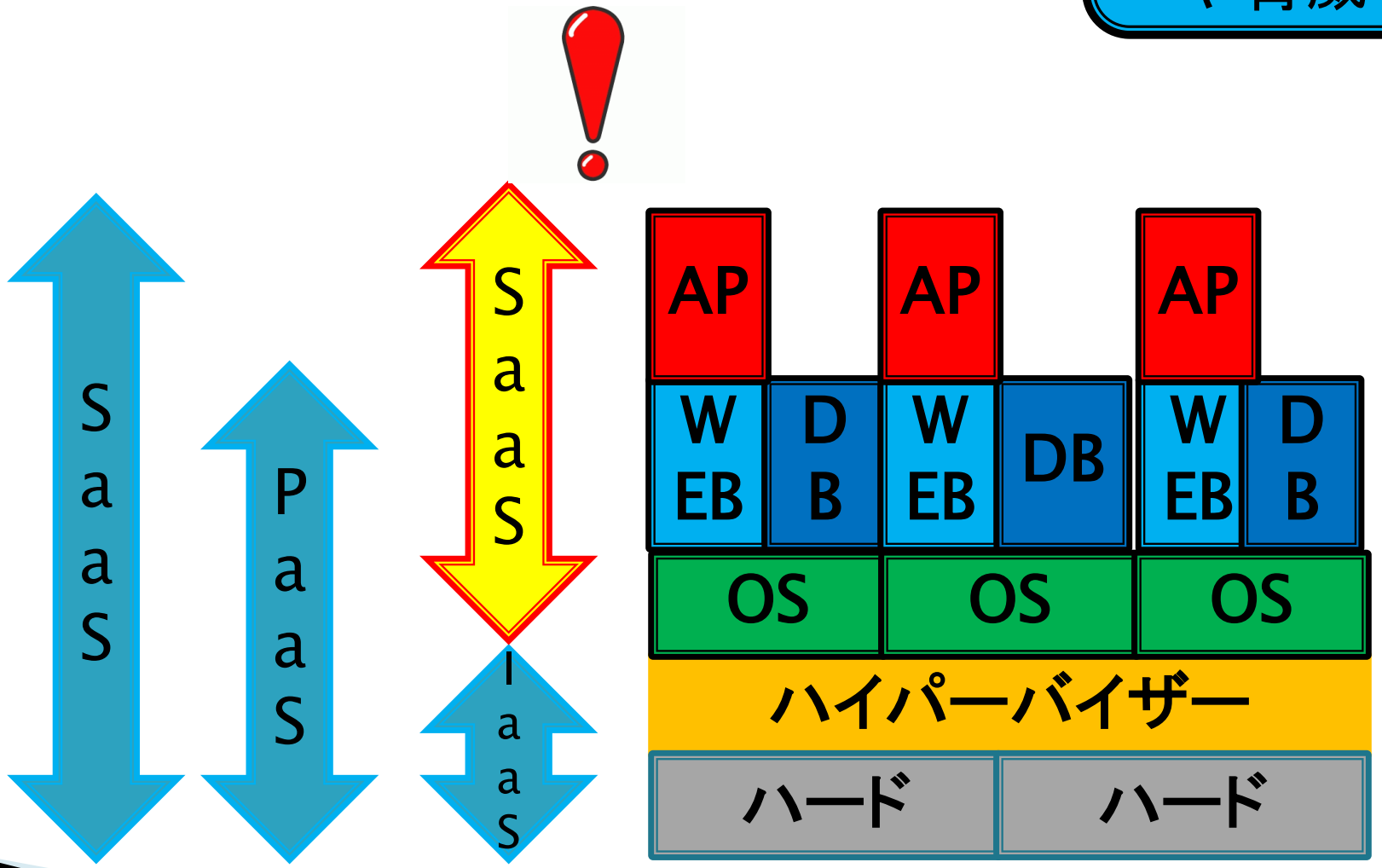
プロセッサ　NW　メモリ　ストレージ



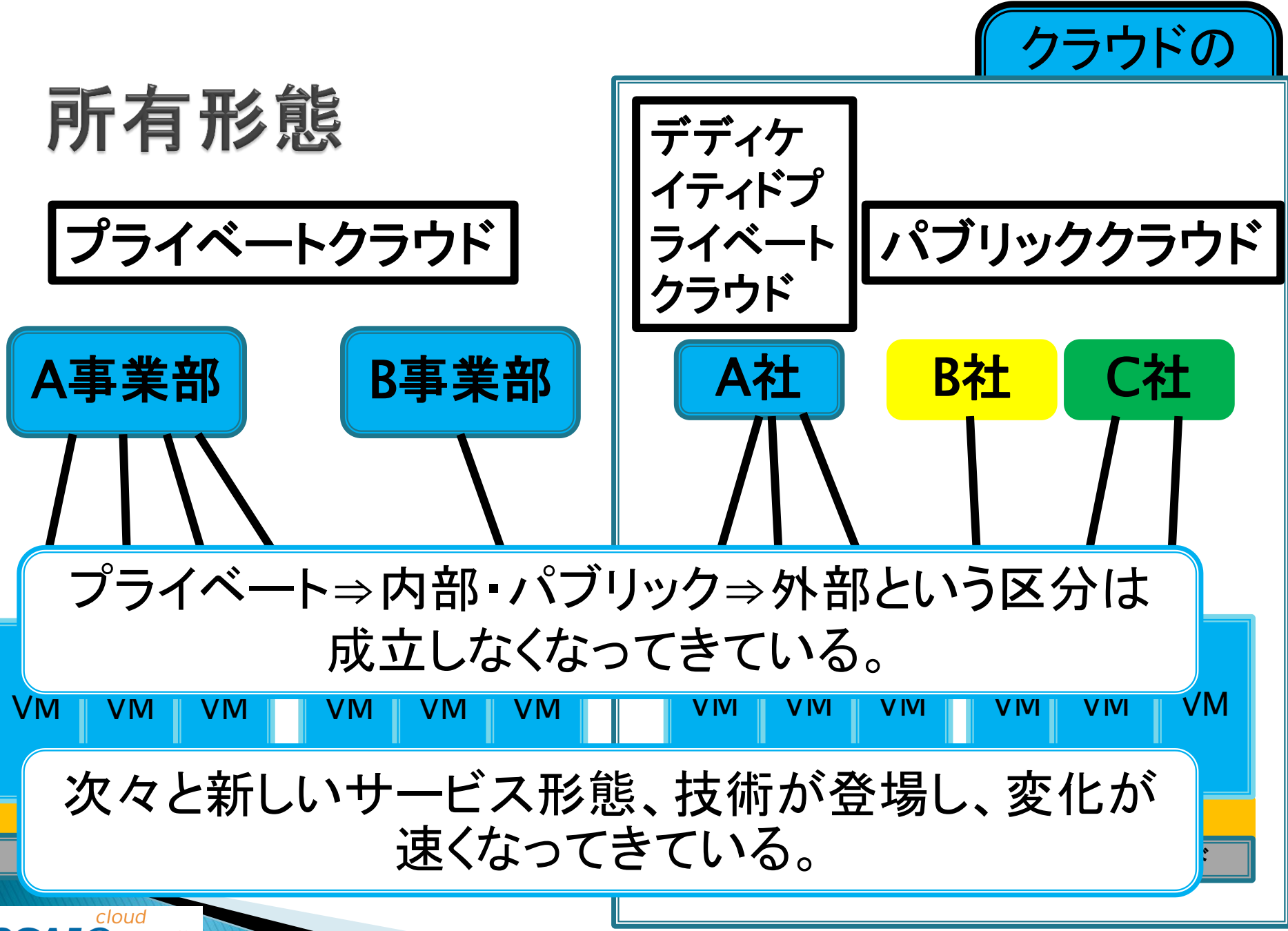
仮想化ソフト≒ハイパーバイザー

クラウドの提供形態

クラウドの基礎知識や脅威



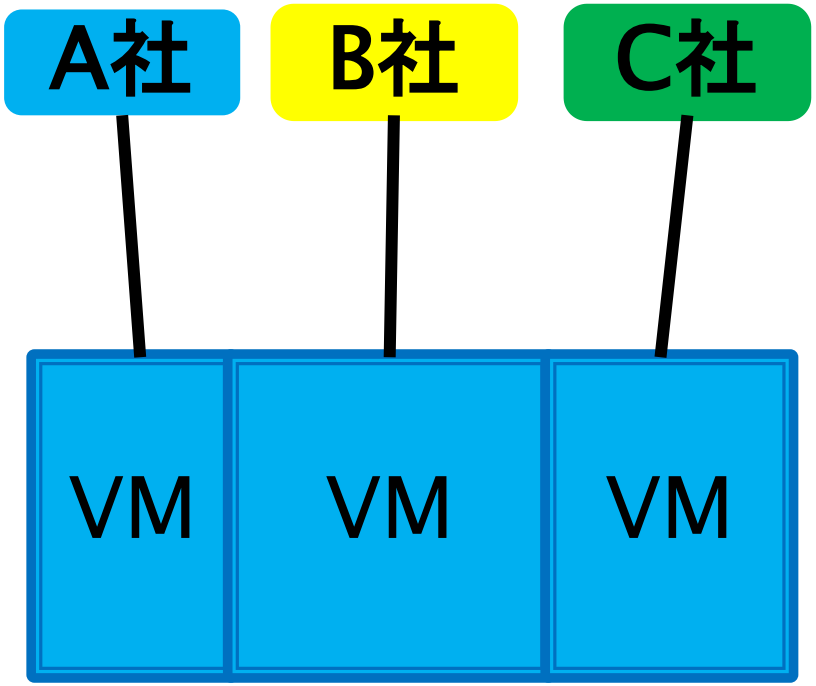
所有形態



プライベート⇒内部・パブリック⇒外部という区分は成立しなくなってきている。

次々と新しいサービス形態、技術が登場し、変化が速くなってきている。

コミュニティクラウド



業界特化型SaaS

クラウドの脅威は?

クラウドの
基礎知識
や脅威

IPA 2013年版10大脅威　**身近に忍び寄る脅威**

http://www.ipa.go.jp/security/vuln/10threats2013.html

10大脅威の中のクラウド

クラウドの基礎知識や脅威

【6位】予期せぬ業務停止

～自然災害やハードウェア障害、人的ミスが思わぬ事態を引き起こす～

http://www.ipa.go.jp/security/vuln/10threats2013.html

- システムのクラウド化が進む中、2012年は、レンタルサーバー事業者において人為的ミスによる大規模障害が発生した。また、2011年の東日本大震災によって、自然災害が原因となりシステムが停止するリスクが浮き彫りとなったように、不測の事態に備える必要性が組織に求められる。

クラウドの基礎知識や脅威

10大脅威の中のクラウド

3章：今後注目すべき脅威
1. クラウド利用における課題

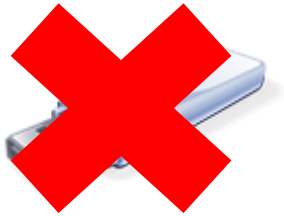
～クラウド導入の利点と主なセキュリティ事故～

http://www.ipa.go.jp/security/vuln/10threats2013.html

- クラウドサービスは、業務システム、個人向けストレージ、災害時の代替システムなど様々な用途で活用されている。一方で、個人によるクラウド利用の拡大に伴い、内部データをクラウド上の無料ストレージへ複製されるなど、システム管理者にとって新たな課題が出てきている。システム管理の責任者は、情報システムを**自身の完全な管理下に置けないことを前提に**、インシデント発生時の対応を検討しておく必要がある。

勝手なクラウド利用の脅威

クラウドの基礎知識や脅威

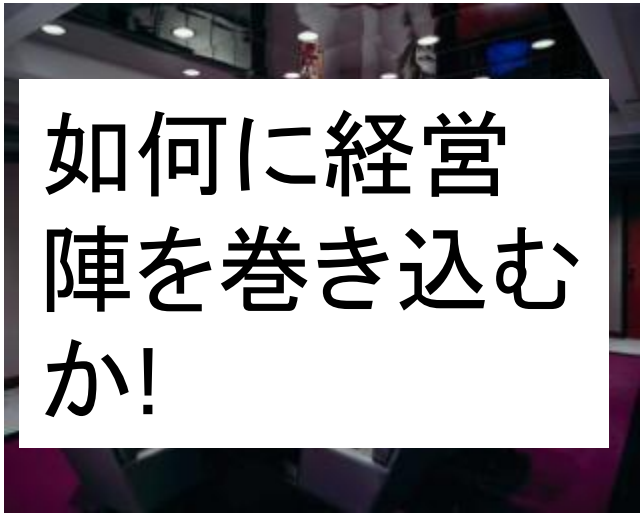


企業の義務(ガバナンス)

企業の義務
(ガバナンス)

増加するガバナンスの重要性

企業の義務
(ガバナンス)



他社・他組織に自社と同等以上の取り組みをお願いする/選ぶ!

本セッションでは、
自組織内に対するガバナンスを内部ガバナンス
他組織に対するガバナンスを外部ガバナンス
と表現します

ではガバナンスとは?

企業の義務
(ガバナンス)

- ISACAのCobit5では
  - 原則 5:ガバナンスとマネジメントの分離 —
    - **ガバナンスとマネジメントを明確に区別**
- CISMレビューマニュアルでは
  - **ガバナンスは経営幹部の責任**
- CSAのガイダンス3.0では
  - **ガバナンスとエンタープライズリスクマネージメントにより組織を超え、費用対効果に優れたセキュリティ管理プログラムをもたらす。**

ちょっと一息

企業の義務
(ガバナンス)

- ITガバナンスは、コーポレート・ガバナンス (企業統治) から派生した概念です。コーポレート・ガバナンスに関する議論では、「誰が誰を統治するのか」「誰の利益を守るのか」「誰が意思決定し、誰が執行し、誰が監査するのか」「誰が誰に対して説明責

明確に当てはめて説明できる企業は、そう多くないのが現状です。

- ITガバナンス確立に向けた具体的な取り組みを始める前に、まずはこの「誰」という問題と真剣に向き合ってみると良いでしょう。そうすると、ITガバナンスという概念がいかに大きく深いテーマであるかが理解できるはずです。実際、これらの「誰」に、組織や人を明確に当てはめて説明できる企業は、そう多くないのが現状です。

経済産業省　IT経営ポータルより
www.meti.go.jp/policy/it_policy/it_keiei/action/keyword/governance/

CSAのコーポレートガバナンス

企業の義務(ガバナンス)

CSAガイダンス3.0Jより

- 2.1　コーポレートガバナンス
- コーポレートガバナンスは、企業が指示、管理、または統制される方法に影響を及ぼすプロセス、技術、習慣、ポリシー、法律、および制度の集合である。また、コーポレートガバナンスは、多くの利害関係者と会社の目標の間の関係を含む。良いガバナンスは、会社の真の所有者である株主の権利と、受託者としての経営幹部の役割の承認に基づいている。コーポレートガバナンスの多くのモデルがあるが、すべて5つの基本原理に従う:

CSAのコーポレートガバナンス　続き

企業の義務
(ガバナンス)

5つの基本原理

- 監査のサプライチェーン
- 取締役会、経営組織、および手続き
- 企業の責任とコンプライアンス
- 財政的透明性と情報公開
- 統制権の所有構造と行使

把握の取り組み

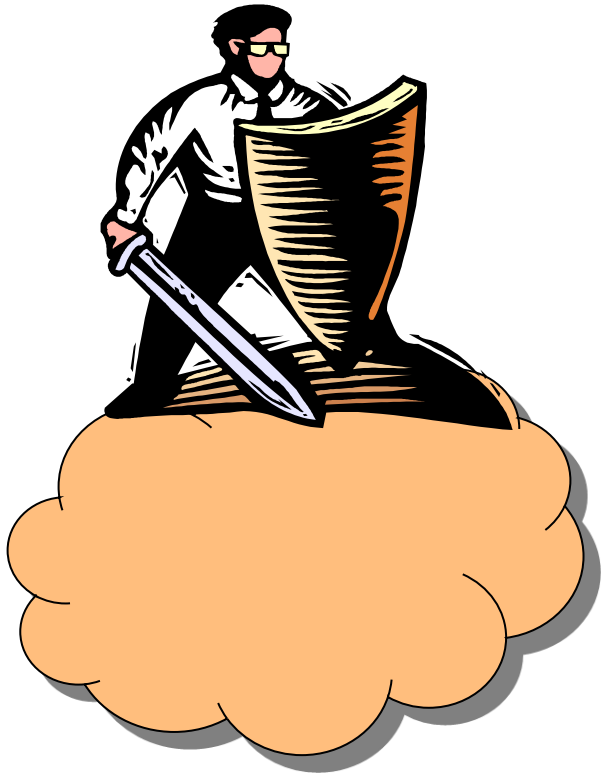
報告を受け対策を案を承認

外部基準に則した判断

エンジニアでも難解なセキュリティ事象を、経営幹部(CxO)に理解させ、対策に関する資源の割当・社内承認を得る事が最大の目的

クラウドのセキュリティ

クラウドの
セキュリティ



クラウドのセキュリティ

クラウドの
セキュリティ

- クラウドコンピューティングにおけるセキュリティコントロールは、IT環境におけるセキュリティコントロールとほとんど変わらない。
- 利用する技術は今迄の物とは大きく異なる。
- クラウドコンピューティングは従来のITソリューションと異なったリスクをもたらす可能性がある。

ハイパーバイザーの存在

クラウドの
セキュリティ

利用企業の管理者

VM

ハイパー
バイザー

ハイパーバイザー管理者

クラウドセキュリティのガバナンス

クラウドのセキュリティ

クラウドセキュリティの内部ガバナンス

クラウドのセキュリティ

内部の基準

- 作成指示
- 承認
- 実施指示
- 状況把握
- 改善指示

- 基準作成
- 実施計画作成

- 順守
- 報告

内部ガバナンスとしての セキュリティマネージメント

クラウドの セキュリティ

クラウド サービス 利用ガイド

ハイパー バイザー 管理

仮想ネット ワーク 管理

クラウド 化に伴う 見直し

既存のセキュリティ管理策

cloud security alliance Japan Chapter

クラウドセキュリティの外部ガバナンス

クラウドのセキュリティ

委託管理基準

- 基準作成
- 周知徹底

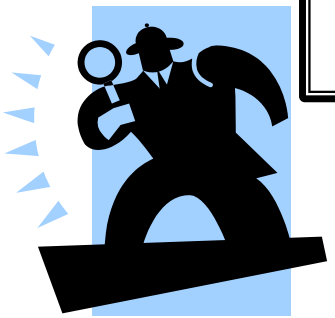
- 作成指示
- 承認
- 実施指示
- 状況把握
- 改善指示

約款/SLA

- 順守
- 報告

外部ガバナンスとしてのセキュリティマネージメント

クラウドのセキュリティ



委託先監査

委託管理基準

SLA

契約

約款

申込

定期報告/モニタリング

内部の基準

CSAの考える監査の留意点

クラウドのセキュリティ

CSAガイダンス3.0Jより

- 10.3.4　監査／コンプライアンス
- 現在のクラウドの展開手法では、企業利用者はクラウドサービスプロバイダの監査情報の閲覧をきわめて制限される。企業は事業運営上の遵守事項に合致しているかだけでなく、**業界標準への適合**と**不正使用の疑念**を持って監査情報にアクセスする必要がある。

厚い壁の向こう側

クラウドのセキュリティ

- 脆弱性情報の入手が難しい。
- 入手した脆弱性情報の判断が難しい。
- 古いプログラムの改修が難しい。
- コストが払えない。

こんな事になって居ない事を確認するのが「目利き」です

事故にあってしまった場合

クラウドのセキュリティ

- 事業者側に重大な過失が無い場合、約款などに定められた額が賠償限度額となる。

ここまでのまとめ

クラウドのセキュリティ

- プライベートクラウドの場合はSLA(Service Level Agreement)により、**要求事項を業者に提示し合意(契約に含む)する事**。
- パブリッククラウドの場合は**サービスメニュー**と**約款**が全て
  - 自社の要求事項・期待しているサービスを提供して居る事業者を探す事

約款を熟読して比較する事

- パブリッククラウドは外部組織に対するガバナンスで有り、安全対策は全て委託先に委ねる事になる。

実務は委ねられても法的責任は逃れられない。

約款で確認したい所

クラウドの
セキュリティ

- バックアップ取得について
  - 自分で取るのか、契約領域内に取るのか等を確認する
  - オフサイトバックアップが必要か?
- データやプログラムの保管場所について
  - 国内か?
- ペネトレーションテストについて
  - SaaSの場合テストをさせてもらえない事が有る。
- 賠償額について
  - 支払金額を上限としている所が多い

こういったリスクの有無等を判り易く経営に報告し、承認を得て行く事からガバナンスは始まる。

小ネタ　JPCERT/CC Alert を活用する

- JPCERT/CC Alert: Microsoft Internet Explorer の脆弱性 (MS13-008) に関する注意喚起
  https://www.jpcert.or.jp/at/2013/at130005.html

I. 概要

マイクロソフト社から Internet Explorer の脆弱性情報が2013年1月15日に緊急公開されました。本情報には、深刻度が**「緊急」**のセキュリティ更新プログラムが 1 件含まれています。

マイクロソフト社によると、本脆弱性を悪用する**標的型攻撃**が確認されているとのことです。

訪問監査した時に、担当者にぜい弱性管理の一環で対応についてサンプル的に聞いてみる

あまりマイナーな事例は、「使っていないので無関係です」と、空振りしまうのでネタの選定が大切です。
相手先から「MS13-008」をリリース後直ちに適用致しました　というのが一番正しい回答です、「MS12-036」とか適当な番号でうなづくと返り討ちにあいますので要注意!

質問により事業者に緊張感を持たせる事も
外部ガバナンスの1つのテクニックです。

Thank You

- https://chapters.cloudsecurityalliance.org/japan/
- info@jp.chapters.cloudsecurityalliance.org