Shared Responsibility誕生秘話

日本マイクロソフト株式会社
チーフセキュリティオフィサー
河野 省二, CISSP

Microsoft

2010年の暑い夏 – 経済産業省の会議室

国際標準になることを前提に、JIS Q 27002をベースにクラウドサービス利用者のためのセキュリティガイダンスを作って欲しい。できれば2ヶ月くらいで完成させたい！

27000シリーズは企業の内部向けガイダンスになるため、クラウド事業者が内部組織にどのように関わるのかをモデル化

「公共ITにおけるアウトソーシングに関するガイドライン（総務省、平成15年度版）」を参考にしながら、役割と責任のモデルをいくつか検討

利用者に常に責任はあるとしながら、事業者は求めに応じて必要な機能と情報の提供を行うことにより、利用者の責任を全うするという概念を作成

後にISOの場（SC27国際会議）にて**Shared Role and Responsibility**としてISO/IEC 27017に反映

2010年の暑い夏 – 経済産業省の会議室

国際標準になることを前提に、JIS Q 27002をベースにクラウドサービス利用者のための
セキュリティガイダンスを作って欲しい。できれば2ヶ月くらいで完成させたい！

27000シリーズは企業の内部向け
になるため、
のように関わ

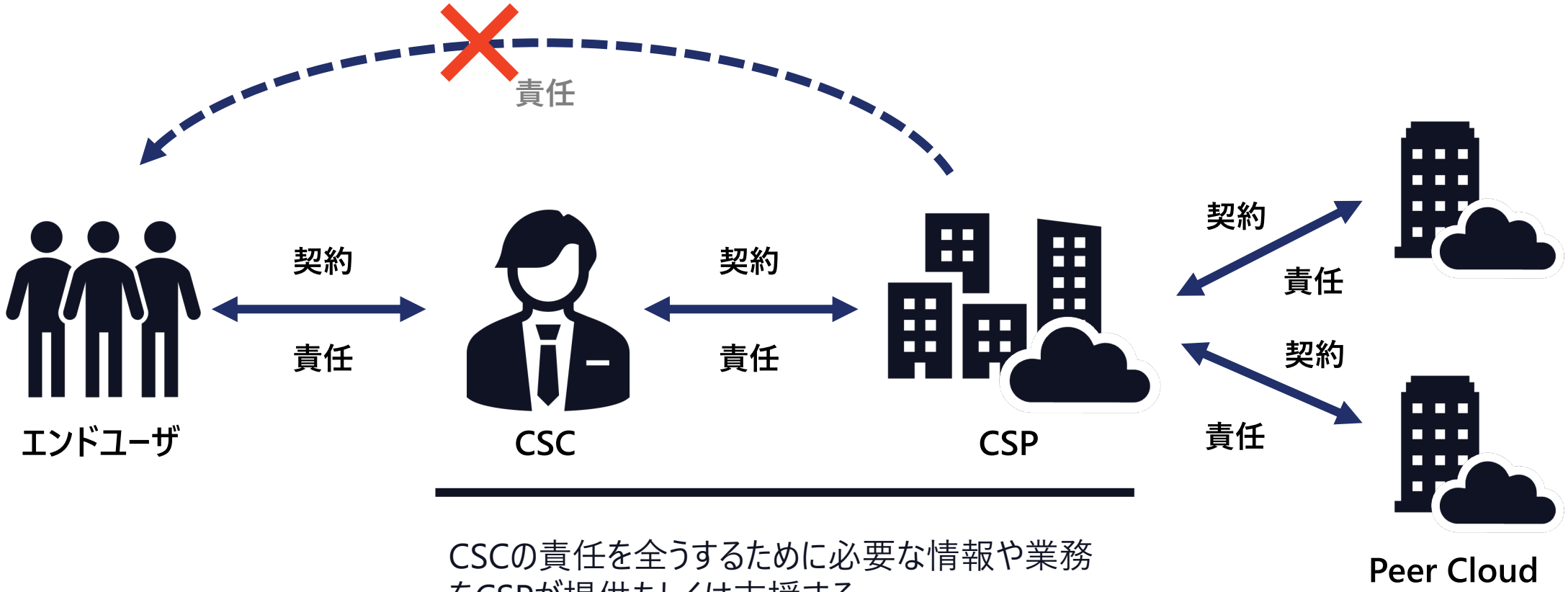
「公共ITにお
ドライン（総務省、平成15年度版）」を参
考にしながら、役割と責任のモデルをいくつか
検討

そもそもSPIスタックは全く関係ない考え方
SaaS、PaaS、IaaSに関係ない洗練されたモデル

に応じて必要な機能と情報の提
供を行うことにより、利用者の責任を全う
するという概念を作成

後にISOの場（SC27国際会議）にて
Shared Role and Responsibilityとして
ISO/IEC 27017に反映

クラウドサービスにおけるShared Responsibility



CSCの責任を全うするために必要な情報や業務をCSPが提供もしくは支援する

つまり、CSCが自組織もしくはエンドユーザに対して追う責任が明確にならない限り、CSPへの要求事項も決まらない

「データの暗号化」の場合

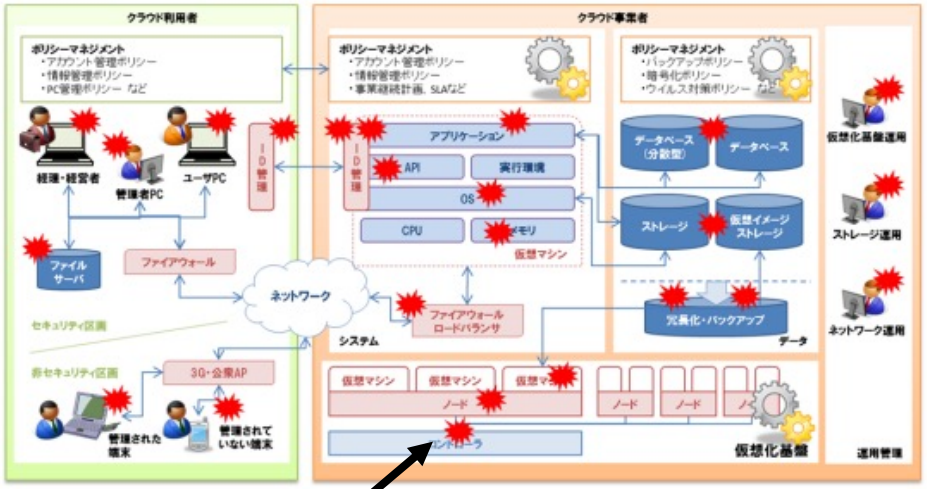
- 「データの暗号化をすること」という対策基準がある場合は、以下のように共同責任を設定することができる

状態	プロバイダ	ユーザ	エビデンス
保存	暗号機能の提供	暗号機能を利用した暗号化もしくは自動暗号化の設定を実施	データを暗号化している状態を示す構成管理データ（ユーザが設定）
転送中	暗号機能の提供（経路、データ本体）	暗号機能を利用した暗号化もしくは自動暗号化の設定を実施	データを暗号化している状態を示す構成管理データ（ユーザが設定）
処理中	適正なデータ処理	–	適正な処理をしていることを示す監査結果（プロバイダが提供）

注）暗号化においては鍵の管理こそが重要だが、ここでは暗号化しているかしていないかだけを示している。鍵の管理の責任主体はユーザにあり、適切な管理をしていない場合のデータの危殆化はユーザの責任となる。プロバイダは鍵管理をユーザ自身が実施できる機能を提供する必要がある

新しい環境のリスクとセキュリティはどう考えるか

1 新しい環境の想定モデルを作る



2 それぞれのポイントでの脅威を探す

構造的かつ潜在的な脆弱性、結合による脆弱性、人間の介入による脆弱性などを分析する

3 脅威に対応する脆弱性を低減する

利用者との通信、サーバ間の通信、リージョン間の通信における脅威

- 通信の傍受
- 中間者攻撃
- なりすまし

コンピュータ環境におけるネットワーク上の脅威

- ネットワーク管理の不備によるシステムダウン
- VLAN 構成におけるトラブルによるシステムダウン

⬇

流れるデータに応じて通信の暗号化を行うことができるように、SaaS、PaaS などでは 予めウェブサーバやアプリケーションサーバなどにおいて暗号通信を標準化もしくは オプションとして選択できるようにする

http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou2013fy.pdf