

クラウド利用研究会

- 原則、毎月第一金曜日、19時30分より開催(ほぼオンライン)
- 参加者は平均6～7名、業界は様々
- クラウド利用者(企業・団体)視線で研究会を実施
- セキュリティに関連したインシデント事例の共有

研究会の活動内容

- クラウド利用研究会では、より実務において有益なガイドラインを共有することを目指し、2020年よりISMAPP、2021年はISMAPPが参照しているNIST SP800シリーズに関する研究を実施。
- **2023年12月からFISC安全対策基準11版で追加されたクラウド関連基準の研究を開始。**
- クラウド利用者がクラウドを利用する際にリスクを勘案し、確認すべき事項を討論
- セキュリティに関連したインシデント事例の共有

ISACA年度 7月～6月 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024

研究会の歩み

東京支部での研究報告

活動

▲監査・保証研究会の分科会として活動

▲両分科会を統合、研究会に発展

▲情報セキュリティ研究会にてクラウドのセキュリティに関する分科会立ち上げ

クラウド導入時のリスク、対策のチェックシート

▲11月

▲6月

CCMの項目をきっかけに議論白熱し長期化

▲7月

CCMと比較し27017要求事項の解釈深掘り

▲7月

▲7月

ISO27017に加えISMAPPの研究を開始

▲12月

ISMAPPが参照しているNIST SP800の研究を開始

▲1月

FISC第11版クラウド基準の研究を開始

▲3月

▲12月

クラウド利用時チェックシート作成

SANS Top20sの研究

クラウド利用時チェックシートへの反映

CCM3.0.1の研究

ISO27017とCCMの比較研究

ISMAPPの研究

NIST SP800-53の研究

NIST SP800-171の研究

FISCの研究

◆経産省ガイドライン33項目
「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」ベース
◆FISC「安全対策基準」へのリファレンス記載

情報セキュリティ対策とコントロールの優先付けを示したコンセンサドキュメント
全44項目のうち、20項目をチェックシートへマッピング・反映
(物理的セキュリティ管理強化)

CSAが作成したセキュリティコントロールのベースライン、クラウドベンダーのリスクを評価。クラウドで導入されるセキュリティ対策の標準を提供
16分野133項目をマッピング・反映

クラウドサービスに関する情報セキュリティ管理策のガイドライン規格
ISO27017要求事項のうち48項目をCCMとマッピング・比較(予定)

ISO27001/27017を参照しているISMAPPについても研究

ISMAPPが参照しているNIST SP800-53についての研究

業務委託先におけるセキュリティ基準であるSP800-171の研究

FISC安対基準(第11版)(23/5発行)ではクラウドに関し大幅改定。**追加されたクラウド関連基準の研究を開始**