

# Cyber Insights Catalog Ver1.0の内容を一部紹介

※内容の詳細及び他のテーマにご関心のある方は、「お問い合わせフォーム」にて、お気軽にご連絡ください。

御担当者様

うちのサイバーの仕組みもスリム化できるかも！しかもセキュリティレベルは落とさずに！

**【テーマ14】**  
無駄なくシンプル！“リーン”なセキュリティとは？  
- CS Insights Catalog for Awareness -  
Ver1.0  
GLOBE-ING  
PASSION FOR WINNING

**【経営 이슈】 無駄なくシンプル！“リーン”なセキュリティとは？**

背景  
サイバーセキュリティ施策の強化は、それに伴う組織の高度化の投資効果は高まっている。一方で、過度なセキュリティ対策は経営活動に支障をきたす可能性がある。そのため、一度導入したセキュリティ対策に対して「無駄」を省くことが必要である。

論点  
「リーン」(無駄のない)を、サイバーセキュリティ対策へどう導入できるのか？  
どんなアプローチで進めるべきか？

解説  
ECRSの原則は「Eliminate (排除)」「Combine (統合)」「Rearrange (再編成)」の3つである。これらを踏まえ、セキュリティ対策の見直しを行う。その際、以下の原則に従って対策を再構築する必要がある。

ECRSの原則は「Eliminate (排除)」「Combine (統合)」「Rearrange (再編成)」の3つである。これらを踏まえ、セキュリティ対策の見直しを行う。その際、以下の原則に従って対策を再構築する必要がある。

ECRSの原則は「Eliminate (排除)」「Combine (統合)」「Rearrange (再編成)」の3つである。これらを踏まえ、セキュリティ対策の見直しを行う。その際、以下の原則に従って対策を再構築する必要がある。

**詳細解説：ECRSの原則に基づく“リーン”なアプローチ**

ECRSの原則  
Eliminate (排除)：不要なプロセスを排除する。  
Combine (統合)：重複するプロセスを統合する。  
Rearrange (再編成)：プロセスの順序を最適化する。

アナロジー思考  
ECRSの原則を、現場の業務プロセスに適用する。例えば、セキュリティ対策の見直しにおいて、不要な対策を排除し、重複する対策を統合し、残った対策の順序を最適化する。

評価方法  
「リーン」なセキュリティ対策の導入により、セキュリティレベルが低下しないことを確認する。また、業務プロセスが簡素化され、コストが削減されることを確認する。

御担当者様

規程は単にルールをまとめた文書ではなく、説明・遂行というミッションを踏まえた位置付けにしないと！

**【テーマ15】**  
単なる“紙つべら”ではない、規程類のあるべき姿とは？  
- CS Insights Catalog for Awareness -  
Ver1.0  
GLOBE-ING  
PASSION FOR WINNING

**【経営 이슈】 単なる“紙つべら”ではない、規程類のあるべき姿とは？**

背景  
サイバーセキュリティ対策は、単にルールをまとめた文書ではなく、説明・遂行というミッションを踏まえた位置付けにしないと、効果が期待できない。

論点  
規程類の目的は「1つは限らない、目的に応じた文書体系を戦略的に検討すべき」。

解説  
規程類の目的は「1つは限らない、目的に応じた文書体系を戦略的に検討すべき」。

**詳細解説：“本音”と“建前”が融合した規程類の体系**

規程類の位置付けは「1つは限らない、“狙い”に応じた文書体系を戦略的に検討すべき」。

文書体系  
基本構造：Policy (方針), Procedure (手順), Guideline (ガイドライン), Standard (標準), Manual (マニュアル), Form (フォーマット), Record (記録), Report (報告), Notice (通知), Memo (メモ), Letter (文書), Contract (契約), Agreement (協定), Policy (方針), Procedure (手順), Guideline (ガイドライン), Standard (標準), Manual (マニュアル), Form (フォーマット), Record (記録), Report (報告), Notice (通知), Memo (メモ), Letter (文書), Contract (契約), Agreement (協定)。

文書体系の位置付け  
「本音」と「建前」が融合した規程類の体系を構築する。各文書の目的・役割を明確にし、文書の整理・関係性を明確にする。

御担当者様

最近、社内のクラウド環境もカオス気味だな・・CCoEが統制を利かせる仕組みで、リスクヘッジしないと！

**【テーマ22】**  
CCoEでクラウドセキュリティのガバナンス強化へ！  
- CS Insights Catalog for Awareness -  
Ver1.0  
GLOBE-ING  
PASSION FOR WINNING

**【経営 이슈】 CCoEでクラウドセキュリティのガバナンス強化へ！**

背景  
近年、ビジネス環境におけるクラウドサービスの利用は急増している。その結果、クラウドセキュリティのリスクも増加している。そのため、クラウドセキュリティのガバナンスを強化することが必要である。

論点  
クラウドセキュリティのガバナンスを強化するための方法として、CCoE(クラウドセンター of Excellence)の導入が有効である。

解説  
クラウドセキュリティのガバナンスを強化するための方法として、CCoE(クラウドセンター of Excellence)の導入が有効である。

**詳細解説：セキュリティ視点で見るCCoEの重要性**

Cloud Center of Excellence (CCoE)の重要性  
CCoEは、クラウドサービスの利用を促進し、リスクを軽減するための組織です。セキュリティ視点から見た場合、CCoEは以下の役割を果たします。

CCoEの役割  
① 標準化の推進  
② 教育・研修の実施  
③ 最新のセキュリティ対策の導入  
④ 脆弱性の発見と修正  
⑤ インシデント対応の支援  
⑥ 監査・報告の実施