COBIT 5 for Information Security
(情報セキュリティに関するCOBIT 5)

イントロダクション

翻訳：CISM委員会WG

COBIT5 プロダクトファミリー

COBIT 5 for Information Security

- ✓COBIT5の拡張
- ✓情報セキュリティの観点からの、各コンポーネントについての説明

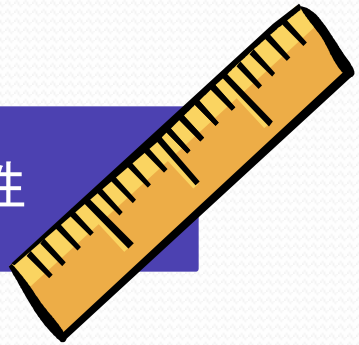
それには何が含まれていますか？

適用指針や利点

情報セキュリティの原則

イネーブラーによるサポート

他の規格との整合性



動機

「COBIT 5 for Information Security」開発の主な動機は以下の通りです:

1. 企業を取り巻く環境に応じた、情報セキュリティを記述するニーズ
2. 企業における以下のような増大するニーズ:
   - リスクを許容できるレベルに維持する
   - システムとサービスの可用性を維持する
   - 関連する法規制への準拠
3. その他の主要な標準およびフレームワークと連携整合するニーズ
4. 全ての主要なISACA研究、フレームワーク、ガイドを関連付けるニーズ

利点

「COBIT 5 for Information Security」を利用して次のように多くの結果につなげることが出来ます:

- 改善され導入容易な情報セキュリティ標準に依る複雑性の減少とコスト効果の増大
- 情報セキュリティの配置と結果によるユーザ満足度の向上
- 企業における情報セキュリティ構築の改善
- 周知したリスクの決定とリスクの認識
- 改善した予防、発見、復旧
- セキュリティ事故に対する影響の軽減
- 革新と競争力に関する強化したサポート
- 情報セキュリティ機能に関する改善したコスト管理
- 情報セキュリティに関するより良い理解

COBIT 5 for Information Securityと、その他のフレームワーク、モデル、グッドプラクティス、標準の関係

「COBIT 5 for Information Security」は、情報セキュリティのための他のフレームワーク、グッドプラクティスと標準をつなぐ包括的フレームワークを目指しています。

「COBIT 5 for Information Security」は、企業全体で情報セキュリティを説明し浸透させるための、イネーブラーによる包括的なフレームワークを提供しています。しかし、その他のモデルも特定のトピックについて詳しく説明されており、同様に役立ちます。例を以下に示します。

- Business Model for Information Security (BMIS)–ISACA
- Standard of Good Practice for Information Security (ISF)
- ISO/IEC 27000 シリーズ
- NIST SP 800-53a
- PCI-DSS

COBIT 5 for Information Security

（情報セキュリティに関するCOBIT5）

COBIT４とCOBIT５の比較

COBIT４とCOBIT５の比較

統制活動の基盤として利用可能な点は同じです。
以前のCOBITバージョンに基づいて構築された統制活動は、COBIT5に容易に移行することが出来ます。

- COBIT５で追加された視点
  1. **ステークホルダの価値と、ビジネスニーズの観点**
     「価値の創造」:　目標の段階的展開
  2. **ガバナンス（EDM）とマネジメント（PBRM）の定義**
  3. **５個のプリンシプル（Principles）**
  4. **７個のイネーブラー（Enabler）**

（参照文献）

ISACA　（英語）
http://www.isaca.org/COBIT/Documents/Comparing-COBIT.pdf
ITGI　Japan （日本語）
http://itgi.jp/cobit/difference.html

情報とは

- 情報は全ての企業にとって、鍵となる資源です。
- 情報は作成、利用、公開、破棄されるものです。
- 情報にかかるこれら全ての活動に関し、技術は鍵となる役割をはたします。
- 仕事のみならずプライベイトの生活においても全面的に、技術が広汎に浸透しつつあります。

情報と技術は企業にどのような利点をもたらすのでしょうか？

企業にとっての利点

企業およびその幹部は次のような課題に奮闘しています。

- 業務戦略決定を支援する質の高い情報を保有、維持していくこと。
- IT投資から事業価値を創造すること。すなわち、ITの効果的かつ革新的な利用から戦略的な目標を達成し業務収益を実現すること。
- 信頼性高く効率的な技術の採用により卓越した業務運営を達成すること。
- IT関連のリスクにつき受容可能なレベルに抑えること。
- ITサービス、技術のコストを最適化すること。

これらから、どのようにして企業のステークホルダにとっての価値を実現するのでしょうか？

ステークホルダにとっての価値

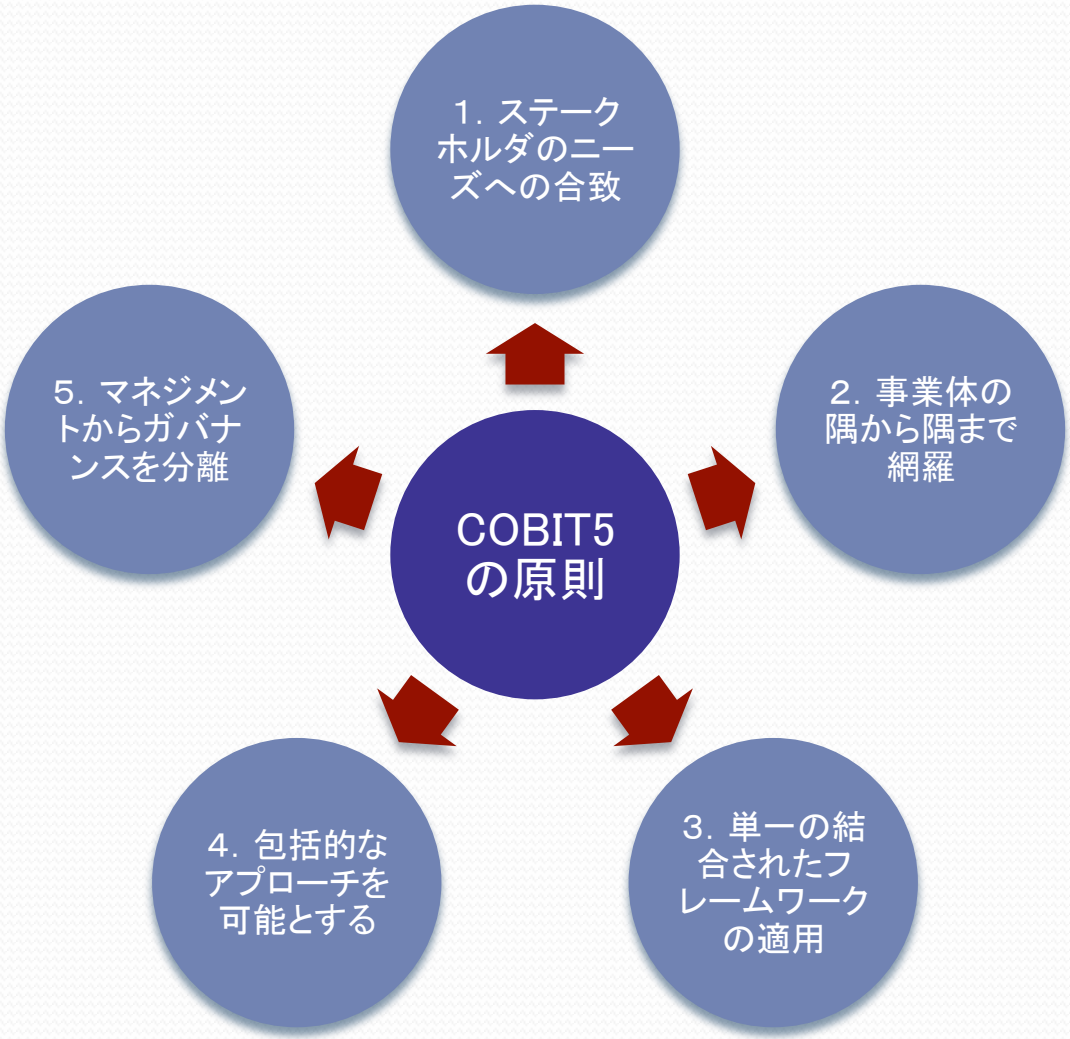
- 企業ステークホルダに価値を分配するためには、情報技術（IT）資産の良好な統治と管理が必要です。
- 企業の役員、幹部社員、そして管理者は、主要業務同様にITに意欲をもって積極的に対応する必要があります。
- 企業の情報技術（IT）への法規制、当局規制、契約上の遵守項目は、要求が増加、高度化しており、もしも違反があれば、企業価値を脅かすこととなります。

- 企業の情報技術（IT）の効率的な統括と運営を通して、企業が戦略目標を達成し、価値を創造するための、包括的なフレームワークを提供するのがCOBIT5です。

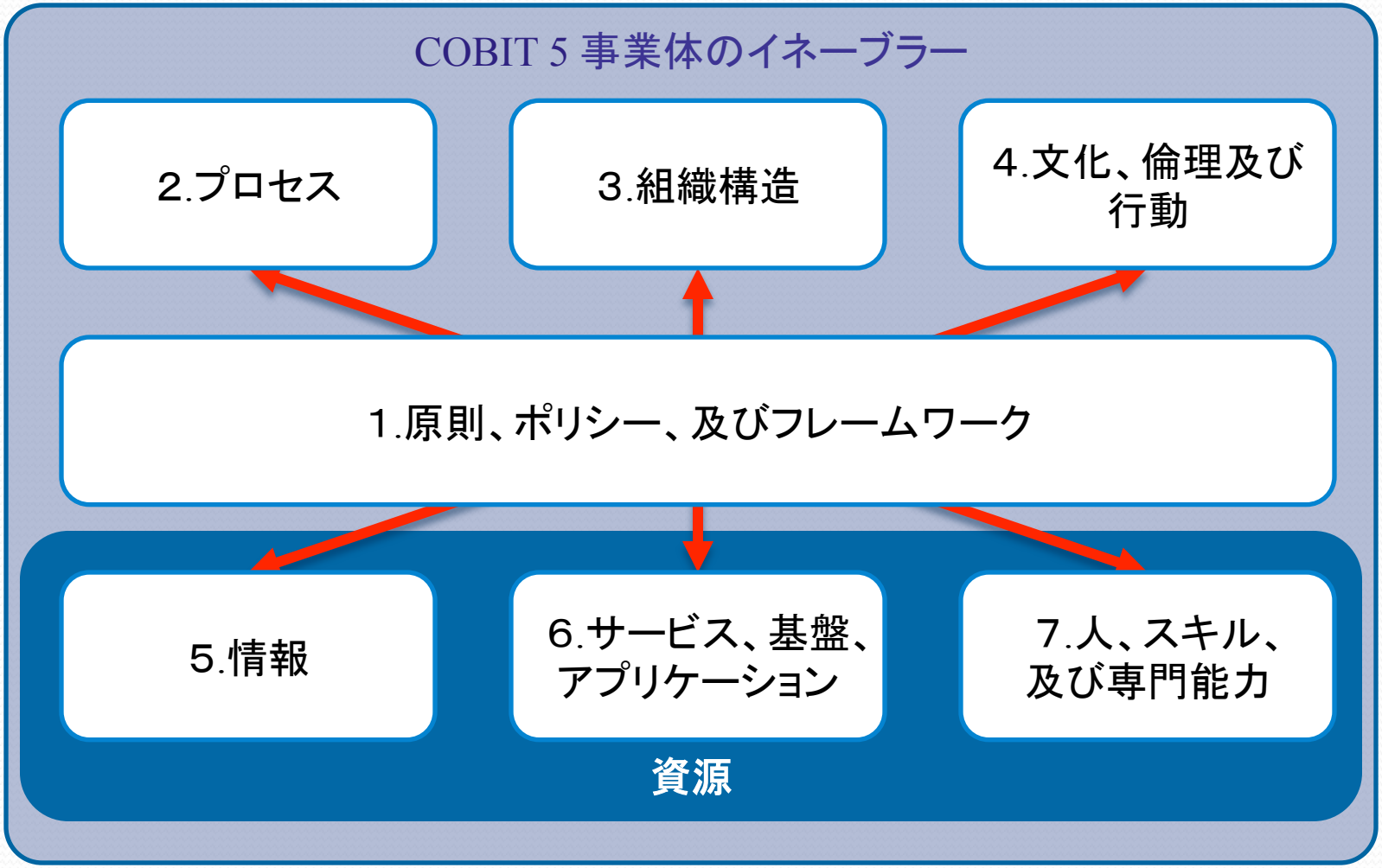
COBIT5のフレームワーク

- 簡潔にいえば、COBIT5は、企業が、資源の使用、リスクレベルの最適化、および、利益の実現のバランスを維持しながら、ITから最適な価値を創造することを支援します。
- COBIT5は、企業内外のステークホルダのITへの関心を考慮しながら、企業の業務および組織機能の、あらゆる責任分野において、企業全体に対し、包括的、一元的な手法で、情報およびそれに関連する技術を統治、管理することを可能とします。
- COBIT5の「原則」と「イネーブラー」は、営利企業であれ、非営利企業や公的部門であれ、あらゆる規模の企業、組織にとって共通であり、有益です。

COBIT5 の原則



COBIT5 イネーブラー



Source: COBIT® 5, figure 12. © 2012 ISACA® All rights reserved.

ガバナンスとマネジメント

- ガバナンスは、ステークホルダのニーズ、条件およびオプションを評価し、達成すべき合意済みの企業目標とのバランスを決定します。また、優先付けと意思決定の過程を通じて方針を設定し、パフォーマンス、コンプライアンスおよび合意された方針と目標に対する準拠性を監視します。

- マネジメントは、企業の目標を達成するためにガバナンスによって設定された方針と整合する活動を計画、構築、実施、監視します。

サマリー …

COBIT5は、企業が総合的な7つのイネーブラーに基き効果的なガバナンスとマネジメントのフレームワークを構築できる5つの原則を提供します。
この7つのイネーブラーは、情報と技術の投資とステークホルダの利益を最適化することが出来ます。

COBIT 5 for Information Security

（情報セキュリティに関するCOBIT5）

概要

情報セキュリティの定義

ISACAは情報セキュリティを次のように定義しています。

企業内において、権限の無いユーザへの情報開示を防ぎ（機密性:confidentiality）、不適切な変更を防ぎ（完全性:integrity）、必用に応じてアクセスできる（可用性:availability）ことを保証するものである。

COBIT 5のイネーブラーを利用することで実現する情報セキュリティの導入

「COBIT 5 for Information Security」が提供する全イネーブラー個別のガイダンス

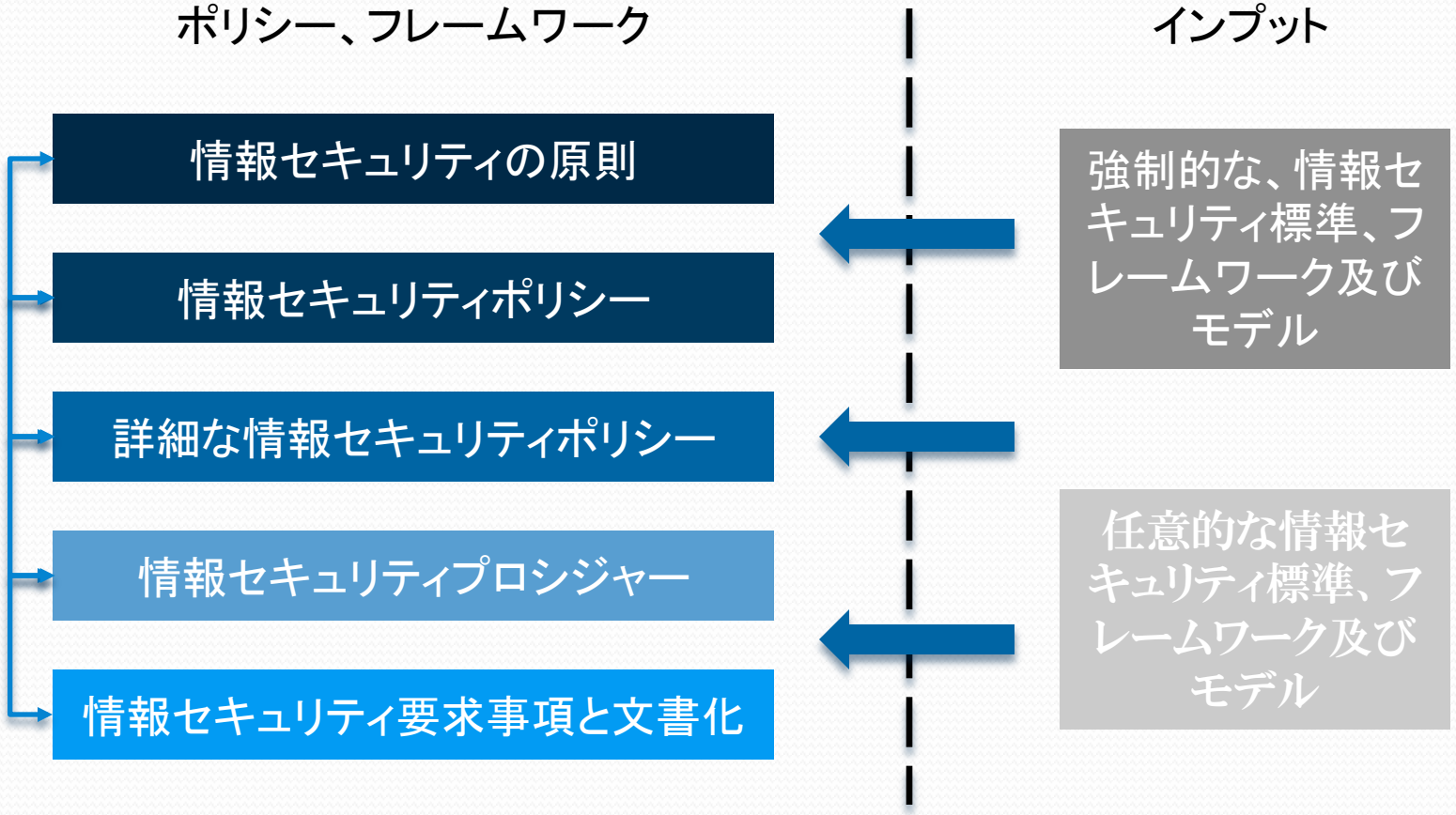
1. 情報セキュリティの原則、ポリシー、フレームワーク
2. 情報セキュリティ特有の活動など詳細を含むプロセス
3. 情報セキュリティ特有の組織構造
4. 文化、倫理、行動と言う意味において、情報セキュリティのガバナンスやマネジメントにおいて成功の是非を左右する要素
5. 情報セキュリティ特有の情報タイプ
6. 企業組織にとって必要な情報セキュリティ機能を提供するためのサービス実行能力
7. 情報セキュリティにおける、人、スキル及び専門能力

イネーブラー:
原則、ポリシー、フレームワーク

組織にガバナンスを与えてマネジメントするための指針や手順を示すための、次のようなコミュニケーションのメカニズム実現に関する原則、ポリシー、フレームワークです。

- 原則、ポリシー、フレームワークのモデル
- 情報セキュリティの原則
- 情報セキュリティポリシー
- 企業組織環境にポリシーを適用する
- ポリシーのライフサイフル

イネーブラー:
原則、ポリシー、フレームワーク(続き)



Source: *COBIT 5 for Information Security,* figure 10. © 2012 ISACA® All rights reserved

情報セキュリティの原則

情報セキュリティの原則は、企業組織の規則自体に通じるもので、これらの原則は以下の条件を満たす必要があります。

- 限定された数
- 簡易な言語表現

2010年、ISACA, ISFと(ISC)^2 は協力し、12個の原則を作成しました。これらの原則は、情報セキュリティの専門家が、彼らの組織に対して付加価値を提供するうえで助けとなります。そして、これらの原則は以下の3つの活動を支援します。

- ビジネスを支援するための活動
- ビジネスを守るための活動
- 情報セキュリティについて責任ある行動を促進するための活動

*「原則」は「COBIT 5 for Information Security」に記載されています。または、www.isaca.org/standardsにも存在します。

情報セキュリティポリシー

ポリシーは、実践的な情報セキュリティの導入を実現するうえで、より詳細なガイダンスを提供します。企業によっては、以下のようなポリシーが含まれるでしょう。

- 情報セキュリティポリシー
- アクセスコントロールポリシー
- 従業員向け情報セキュリティポリシー
- インシデント管理ポリシー
- 資産管理ポリシー

「COBIT 5 for Information Security」はポリシーごとに、以下の項目について説明しています。

- 対象範囲
- 妥当性
- 達成目標

イネーブラー：プロセス

COBIT5のプロセス参照モデルは、企業のIT関連の慣習と活動を2つの主な領域（ガバナンスとマネジメント）に分けており、マネジメントは、さらにプロセス領域に分かれています。

- ガバナンスは5つの領域で構成され、各プロセスにて評価、方向の指示、モニタリング (EDM)する手法が定義されています。
- マネジメントは4つの領域で構成され、計画、構築、運用、モニター（PBRM)の責任領域と一致しています。
- 「COBIT 5 for Information Security」では各プロセスを情報セキュリティーの観点から検証しています。

イネーブラー：プロセス（続き）

Source: *COBIT 5 for Information Security*, figure 7. © 2012 ISACA® All rights reserved

イネーブラー：組織構造

COBIT5は、情報セキュリティの観点から組織構造を検証します。

情報セキュリティにおける果たすべき役割と責任が定義されていること。そして、その役割と責任を、現状の組織構造に対してどのように適用するかについて、得失を検証します。

イネーブラー：文化、倫理及び行動

情報セキュリティの観点から、次の詳細なセキュリティ固有の例から文化、倫理及び行動を検証します。

1. 文化のライフサイクル–セキュリティ文化を長期にわたって測定する–いくつかの行動様式を含む:
   - パスワードの強固さ
   - セキュリティへのアプローチの欠如
   - 変更管理時の慣習への遵守
2. 管理者と最高実力者–これらに示す人が模範例を示し文化に影響を及ぼす:
   - リスクマネージャ
   - セキュリティプロフェッショナル
   - 役員クラスの幹部
3. 望ましい行動–セキュリティ文化にプラスの影響を及ぼす：
   - 情報セキュリティは日常のオペレーションで実践される
   - ステークホルダはどのように脅威に対応するのか知っている
   - 幹部は情報セキュリティのビジネスにおける価値を認識している

イネーブラー：情報

情報は、情報セキュリティの対象というだけではなく、主なイネーブラーです。

1. 情報のタイプを検証し、次を含む関連するセキュリティ情報のタイプも明らかにします。
   - 情報セキュリティ戦略
   - 情報セキュリティ予算
   - 方針
   - 教育資料
   - その他…
2. 情報のステークホルダ、情報のライフサイクルも特定され、セキュリティの観点から詳細化します。情報の保管、共有、使用、廃棄といった情報セキュリティ特有の詳細なことまですべて検討します。

イネーブラー：サービス、基盤、アプリケーション

サービス、基盤、アプリケーションのモデルでは、企業が情報セキュリティに関連する機能を提供するために、必要なサービス機能を識別します。次のリストには、セキュリティサービスのカタログに表示される可能性のあるセキュリティ関連サービスの例が含まれています。

- セキュリティアーキテクチャの提供
- セキュリティ意識の提供
- セキュリティ評価の提供
- 適切なインシデント対応の提供
- マルウェア、外部からの攻撃や侵入の試みに対しての十分な保護の提供
- セキュリティ関連のイベント監視及びアラートサービスの提供

イネーブラー：人物、スキル及び専門能力

効果的に、企業内の情報セキュリティ機能を働かせるには、適切な知識と経験を持った個人がその機能を行使しなければなりません。いくつかの一般的なセキュリティ関連のスキルや能力は、次のとおりです。

- 情報セキュリティガバナンス
- 情報リスク管理
- 情報セキュリティの運用

「COBIT 5 for Information Security」では、スキルや能力ごとに次の属性を定義しています。

- スキル定義
- 目標
- 関連するイネーブラー

第2章:情報セキュリティを実装するための取り組み

企業の情報セキュリティコンテキストを考慮:「COBIT 5 for Information Security」では、あらゆる企業は、以下のような環境に応じた、独自の情報セキュリティ イネーブラーの定義や実装をする必要性があることを助言しています。

- 情報セキュリティに係る文化と倫理
- 適用される法律、規制、およびポリシー
- 既存の施策と実践
- 情報セキュリティの機能と利用可能なリソース

第2章：情報セキュリティを実装するための取り組み（続き）

さらに、以下の内容に基づいて、企業の情報セキュリティ要件を定義する必要があります。

- 事業計画と戦略的意図
- 経営スタイル
- 情報リスクプロファイル
- リスク選好

情報セキュリティへの取り組みを実施するためのアプローチは、あらゆる企業で異なっていたとしても、「COBIT 5 for Information Security」を有効に適用するために明確にする必要があります。

第2章：情報セキュリティを実装するための取り組み（続き）

「COBIT 5 for Information Security」を実装するための重要な他の範囲は次の通りです。

- 適切な環境の構築
- 障害ポイントとトリガーイベントの認識
- 変更管理
- 情報セキュリティは、一過性の取り組みではなくライフサイクルであることの認識

この資料について

この資料は、ISACA本部のCOBIT 5 Overviewsにある、COBIT5-and-InfoSec.pptを基に、CISM委員会にてワーキンググループを作成して翻訳したものです。また、順番を入れ替え、一部COBIT5の項目は別で作成頂いた資料を基に追記しています。

ご協力頂いた皆さんありがとうございます。この場を借りてお礼を申し上げます。

しかし、この資料の最終的な責任は講演者にあります。記載の誤り等ご指摘ございましたら、以下の講演者宛にお願いいたします。

SCSK株式会社
ITマネジメント事業第一事業本部
セキュリティソリューション部　玉木

ma.tamaki@ms.scsk.jp