**サイバーセキュリティに関するフレームワークとISMS～第1回 サイバー経営ガイドとCSF**

2015年12月に経済産業省および情報処理推進機構（以下、IPA）から「サイバーセキュリティ経営ガイドライン」が公開されました。本ガイドラインには、サイバー攻撃から企業を守る観点で、経営者が認識する必要のある原則や指示事項などが書かれています。また、ここ数年、日本以外の国からもサイバーセキュリティに関するさまざまなフレームワークが公開されてきており、そのいくつかは日本でも利用されています。

これらの各フレームワークには、どのような違いがあるのでしょうか？一般的にもっとも使用されるセキュリティのフレームワークであるISMS（ISO/IEC27001、27002）とはどう違うのでしょうか？ここでは代表的な以下の4つのフレームワークを見ていきます。

* **「サイバーセキュリティ経営ガイドライン」**（経済産業省、IPA）
* **「重要インフラにおけるサイバーセキュリティフレームワーク」**（米国 国立標準技術研究所）
* **「Critical Security Controls for Effective Cyber Defense」**（米国の非営利団体Center for Internet Security）
* **「Strategies to Mitigate Targeted Cyber Intrusions」**（オーストラリア 国防信号局）

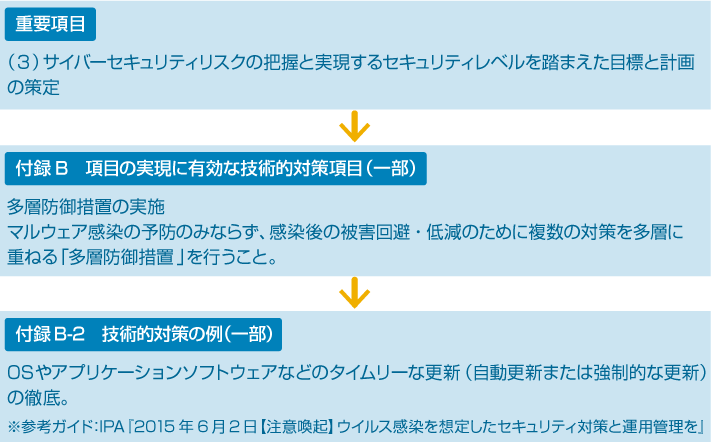
**「サイバーセキュリティ経営ガイドライン」とは？**

「サイバーセキュリティ経営ガイドライン」は、主に経営者やCISO（最高情報セキュリティ責任者）など向けに書かれているもので、経営におけるサイバーセキュリティ経営の原則およびCISOなどに指示すべき重要項目について記載されています。

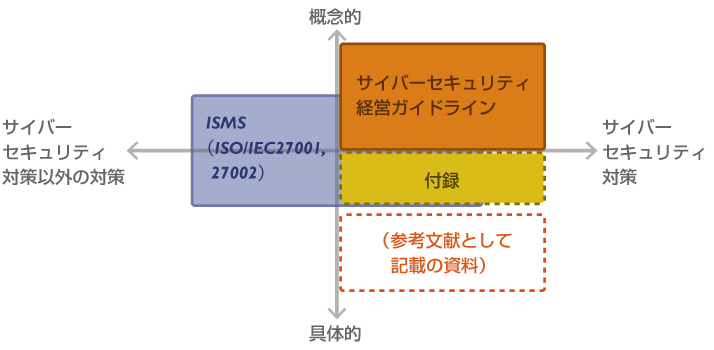
|  |  |
| --- | --- |
| 【CISO等に指示すべき「重要10項目」】 | |
| **No.** |  |
| **1** | サイバーセキュリティリスクへの対応について、組織の内外に示すための方針（セキュリティポリシー）を策定すること。 |
| **2** | 方針に基づく対応策を実装できるよう、経営者とセキュリティ担当者、両者をつなぐ仲介者としてのCISO等からなる適切な管理体制を構築すること。その中で、責任を明確化すること。 |
| **3** | 経営戦略を踏まえて守るべき資産を特定し、セキュリティリスクを洗い出すとともに、そのリスクへの対処に向けた計画を策定すること。 |
| **4** | 計画が確実に実施され、改善が図られるよう、PDCAを実施すること。また、対策状況については、CISO等が定期的に経営者に対して報告をするとともに、ステークホルダーからの信頼性を高めるべく適切に開示すること。 |
| **5** | 系列企業やサプライチェーンのビジネスパートナーを含め、自社同様にPDCAの運用を含むサイバーセキュリティ対策を行わせること。 |
| **6** | PDCAの運用を含むサイバーセキュリティ対策の着実な実施に備え、必要な予算の確保や人材育成など資源の確保について検討すること。 |
| **7** | ITシステムの運用について、自社の技術力や効率性などの観点から自組織で対応する部分と他組織に委託する部分の適切な切り分けをすること。また、他組織に委託する場合においても、委託先への攻撃を想定したサイバーセキュリティの確保を確認すること。 |
| **8** | 攻撃側のレベルは常に向上することから、情報共有活動に参加し、最新の状況を自社の対策に反映すること。また、可能な限り、自社への攻撃情報を公的な情報共有活動に提供するなどにより、同様の被害が社会全体に広がることの未然防止に貢献すること。 |
| **9** | サイバー攻撃を受けた場合、迅速な初動対応により被害拡大を防ぐため、CSIRT（サイバー攻撃による情報漏えいや障害など、コンピュータセキュリティにかかるインシデントに対処するための組織）の整備や、初動対応マニュアルの策定など緊急時の対応体制を整備すること。また、定期的かつ実践的な演習を実施すること。 |
| **10** | サイバー攻撃を受けた場合に備え、被害発覚後の通知先や開示が必要な情報項目の整理をするとともに、組織の内外に対し、経営者がスムーズに必要な説明ができるよう準備しておくこと。 |

引用：「サイバーセキュリティ経営ガイドライン」（経済産業省、IPA）

なお、当ガイドラインの本文及び付録には、上記の重要10項目をベースとした実施担当者（システム部門やセキュリティ部門の担当者）向けの対策項目が書かれています。  
例えば、重要項目３は、以下のようにブレークダウンされています。



なお、「付録C　国際規格ISO/IEC27001及び27002との関係」を参照することで、「セキュリティ経営ガイドライン」と、対応するISMSの規格要求事項を確認することができるようになっています。



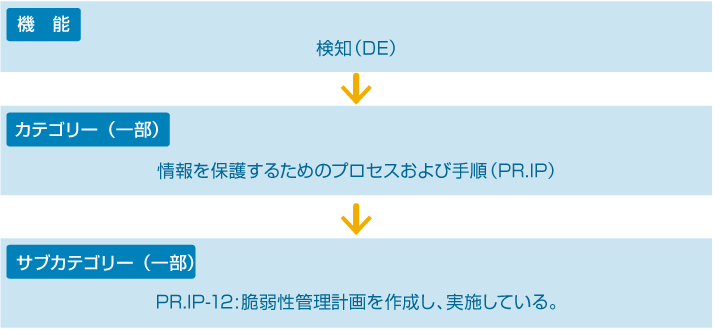
**「重要インフラにおけるサイバーセキュリティフレームワーク（CSF）」とは？**

「重要インフラにおけるサイバーセキュリティフレームワーク」（”Framework for Improving Critical Infrastructure Cybersecurity”）は、2014年2月に米国の国立標準技術研究所（NIST）から公開されており、その邦訳版をIPAが公開しています。主に重要インフラに携わる企業向けに書かれていますが、それ以外の組織でも十分活用できる内容になっており、「CSF」とも呼ばれて海外では急速に利用が広がっています。  
2015年11月にプライスウォーターハウスクーパース株式会社が発表した「グローバル情報セキュリティ調査2016」によると、グローバル企業での当フレームワークの使用は35%となっており、ISO/IEC27001の40%に迫る勢いとなっています（複数回答ありの数値です）。  
当フレームワークは、サイバーセキュリティ対策を、「特定」、「防御」、「検知」、「対応」、「復旧」の5つの機能に分類し、それらの機能を22のカテゴリーで示しています。

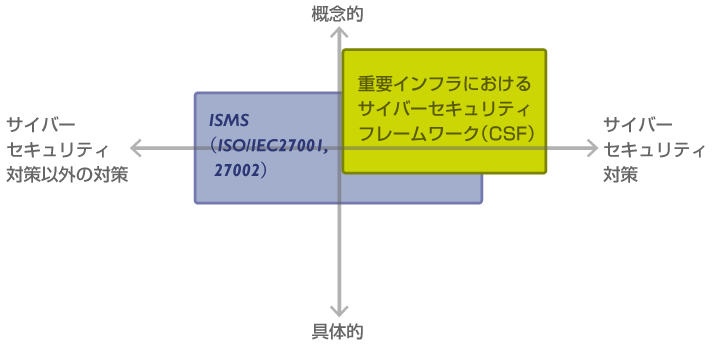
|  |  |  |  |
| --- | --- | --- | --- |
| **機能** | **カテゴリー** | **機能** | **カテゴリー** |
| **特定 (ID)** | 資産管理 | **検知 (DE)** | 異常とイベント |
| ビジネス環境 | セキュリティの継続的なモニタリング |
| ガバナンス | 検知プロセス |
| リスクアセスメント | **対応 (RS)** | 対応計画の作成 |
| リスク管理戦略 | 伝達 |
| **防御 (PR)** | アクセス制御 | 分析 |
| 意識向上及びトレーニング | 低減 |
| データセキュリティ | 改善 |
| 情報を保護するためのプロセスおよび手順 | **復旧 (RC)** | 復旧計画の作成 |
| 保守 | 改善 |
| 保護技術 | 伝達 |

引用および一部抜粋：「重要インフラにおけるサイバーセキュリティフレームワーク」（IPA）

それぞれのカテゴリーは、さらにいくつかのサブカテゴリーに分かれており、サブカテゴリーは全部で98にのぼります。対策の記述レベルはあまり細かくはなく、技術的な手段までは言及していません。例えば、「検知」は以下のようにブレークダウンされています。



本文の「表２　フレームワークコア」には、各サブカテゴリーに関連するISMSの管理策を確認することができるようになっています。サブカテゴリーに関連するISMSの管理策は94にのぼっており、ISMS管理策が全部で114であることを考えると、重複する範囲は多いと言えます。



今回見たサイバー経営ガイドとCSFの2つのフレームワークは、サイバー攻撃に対する直接的な対策そのものだけでなく、その前段となる「守るべき資産の特定」や「リスクアセスメント」についても記載があることから、比較的カバー範囲が広く、ISMSとの類似性も高いと言えます。

次回は、「Critical Security Controls for Effective Cyber Defense」および「Strategies to Mitigate Targeted Cyber Intrusions」について見ていきたいと思います。

# サイバーセキュリティに関するフレームワークとISMS ～第2回 CSC20とTop35 Mitigation Strategies

今回ご紹介する２つのフレームワークは、第一回で登場したフレームワークとは異なり、対策の優先度付けがされているのが特徴です。また、初版公開以降、すでに1回以上更新されており、完成度が向上していると考えられます。  
それではどの対策の優先度が高いとされているのでしょうか？その内容を見ていきましょう。

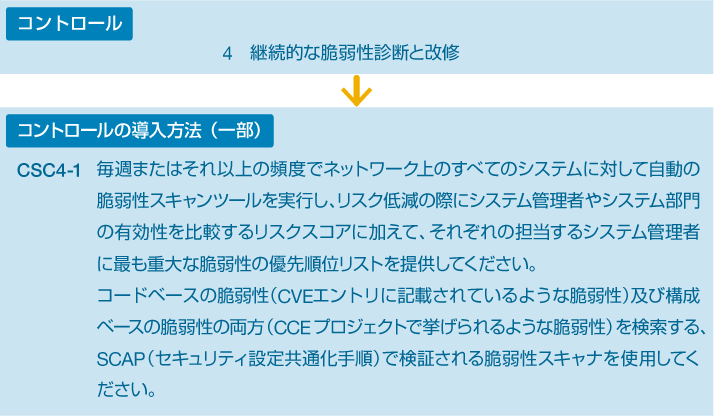
## 「Critical Security Controls for Effective Cyber Defense」(CSC20)とは？

「Critical Security Controls for Effective Cyber Defense」（効果的なサイバー防御のための重要なセキュリティコントロール）は、Version6.0が2015年10月に米国のCenter for Internet Securityから公開されています（以前はSANS Instituteから公開）。これは、サイバー攻撃に対する重要なセキュリティ対策を20のコントロールに分類・優先度付けをしたもので、極力自動化された技術的対策が主体となっています。

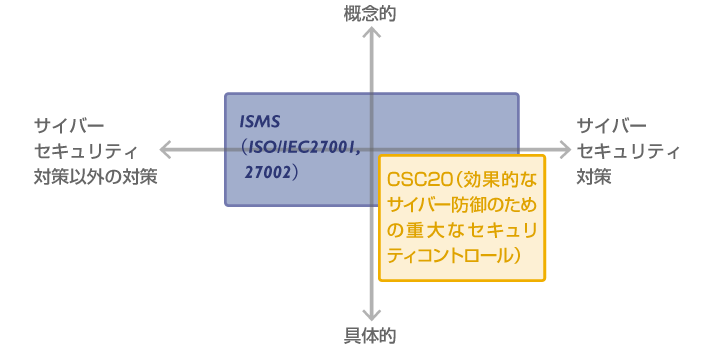
|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **コントロール** | **No.** | **コントロール** |
| **1** | 許可および無許可の機器のインベントリ | **11** | ファイアウォールやルーター、スイッチなどのネットワーク機器のセキュアな構成 |
| **2** | 許可および無許可のソフトウェアのインベントリ | **12** | 境界防御 |
| **3** | モバイル機器、ラップトップ、ワークステーション、サーバにおけるハードウェアおよびソフトウェアのセキュアな構成 | **13** | データ保護 |
| **4** | 継続的な脆弱性診断と改修 | **14** | 知る必要性に基づいた、管理されたアクセス |
| **5** | 管理者権限のコントロールされた使用 | **15** | 無線のアクセスコントロール |
| **6** | 監査ログの保守、監視、および分析 | **16** | アカウントのモニタリングおよびコントロール |
| **7** | 電子メールとWebブラウザの保護 | **17** | 不足を補完するためのセキュリティスキル評価および適切なトレーニング |
| **8** | マルウェア防御 | **18** | アプリケーションソフトウェアのセキュリティ |
| **9** | ネットワークポート、プロトコル、サービスの制限およびコントロール | **19** | インシデント対応と管理 |
| **10** | データ復旧能力 | **20** | ペネトレーションテストおよびレッドチームによる訓練 |

引用：「Critical Security Controls for Effective Cyber Defense」（Center for Internet Security）  
※邦訳版は公開されていません。

それぞれのコントロールは、いくつかのサブコントロールに分かれており、サブコントロールは全部で150にのぼります。  
例えば、「継続的な脆弱性診断と改修」は以下のようにブレークダウンされています。



20のコントロールは、ほぼすべてがISMSの管理策に関係していると考えられますが、ISMS管理策との関連を示す資料は公開されていません。  
なお、当文書の「AppendixC: The NIST Framework for Improving Critical Infrastructure Cybersecurity」を参照することによって、20のコントロールがNIST「重要インフラにおけるサイバーセキュリティフレームワーク」（第一回を参照）のどのカテゴリーに対応しているのかを確認することができます。



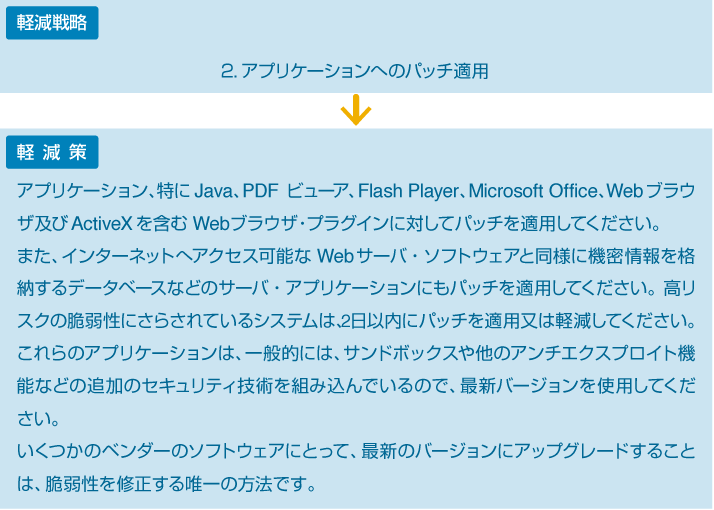
## 「Strategies to Mitigate Targeted Cyber Intrusions」(Top35 Mitigation Strategies)とは？

「Strategies to Mitigate Targeted Cyber Intrusions」（標的型サイバー侵入の軽減戦略）は、2014年2月に2014年版がオーストラリアの国防信号局から公開されています。標的型攻撃を主な脅威と想定したセキュリティ対策を、優先度順に35のカテゴリーで示したものです。

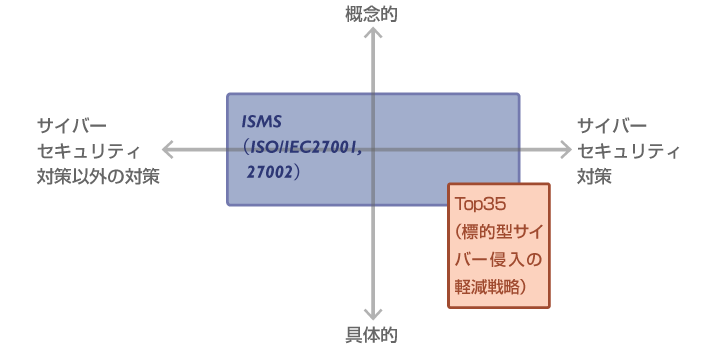
|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **軽減戦略** | **No.** | **軽減戦略** |
| **1** | アプリケーションのホワイトリスティング | **19** | 全てのドメインにおけるWebドメインのホワイトリスト化 |
| **2** | アプリケーションへのパッチ適用 | **20** | なりすまし電子メールのブロック |
| **3** | OSの脆弱性へのパッチ適用 | **21** | ワークステーション及びサーバの設定管理 |
| **4** | 管理者権限の制限 | **22** | ヒューリスティックな手法と自動化したインターネット型のレピュテーション・レーティングを用いたアンチウイルスソフト |
| **5** | ユーザーアプリケーション設定の要塞化 | **23** | ワークステーションからインターネットへの直接接続の拒否 |
| **6** | 自動化された動的解析 | **24** | サーバ・アプリケーション設定の要塞化 |
| **7** | OSに対する一般的なexploitの軽減メカニズム | **25** | 強固なパスワードポリシーの強制 |
| **8** | ホスト型のIDS/IPS | **26** | 可搬型及び携帯型メディアの管理 |
| **9** | ローカル管理者権限の無効化 | **27** | SMBおよびNetBIOSへのアクセス制限 |
| **10** | ネットワークの分割及び分離 | **28** | ユーザ教育 |
| **11** | 多要素認証 | **29** | ワークステーション上のMicrosoft Officeのファイルの検査 |
| **12** | 外部から入ってくるネットワークトラフィックを遮断するソフトウェア型のアプリケーション・ファイアウォール | **30** | シグネチャ型のアンチウイルスソフト |
| **13** | 外部へ出ていくネットワークトラフィックを遮断するソフトウェア型のアプリケーション・ファイアウォール | **31** | 電子メールサーバ間のTLS暗号化 |
| **14** | 一時的に仮想化かつサンドボックス化された信頼できる運用環境 | **32** | IPアドレスによってWebサイトにアクセスする試みのブロック |
| **15** | 成功又は失敗したコンピュータイベントの一元化かつ同期されたログの取得 | **33** | ネットワーク型のIDS／IPS |
| **16** | 許可された又は遮断されたネットワークイベントの一元化かつ同期されたログの取得 | **34** | ゲートウェイのブラックリスト化 |
| **17** | 電子メールコンテンツのフィルタリング | **35** | ネットワークトラフィックのキャプチャ |
| **18** | Webコンテンツのフィルタリング |  |  |

引用：「Strategies to Mitigate Targeted Cyber Intrusions」（オーストラリア国防信号局）  
※邦訳版は公開されていません。

それぞれの軽減戦略は、さらに下位に細分化されてはいませんが、軽減策の説明が記載されています。例えば、「アプリケーションへのパッチ適用」は以下の説明が記載されています。



35の軽減戦略も、ほぼすべてがISMSの管理策に関係していると考えられますが、ISMS管理策との関連を示す資料は公開されていません。なお、35の軽減戦略は、サイバー攻撃の中でも標的型攻撃を主な脅威と想定した対策であることに注意が必要です。



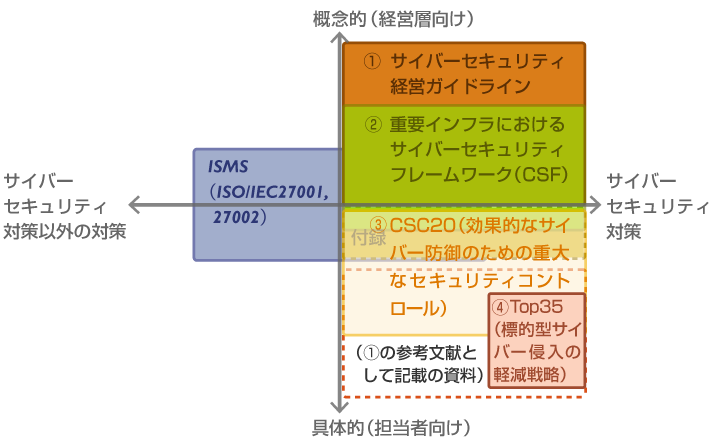
## まとめ

これまで見てきた４つのフレームワークを並べると、以下の違いが見られます。(2016年7月現在)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **フレームワーク** | **対象組織** | **概要** | **公開時期** |
| **1** | サイバーセキュリティ経営ガイドライン | 大企業及び中小企業（小規模事業者除く）のうち、ＩＴに関するシステムやサービス等を供給する企業及び経営戦略上ＩＴの利活用が不可欠である企業 | サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3原則」、及びCISO等に指示すべき「重要10項目」をまとめたもの。 付録に技術的対策の例も掲載。 | 2015年12月 (経済産業省、IPA) |
| **2** | Framework for Improving Critical Infrastructure Cybersecurity（重要インフラのサイバーセキュリティを向上させるためのフレームワーク） | 重要インフラに携わる企業 | サイバーセキュリティの成果を達成するための対策として、「特定」、「防御」、「検知」、「対応」、「復旧」の5つの機能や、それらの機能を細分化した22のカテゴリーについて示したもの。 | 2014年2月 (米国国立標準技術研究所) |
| **3** | Critical Security Controls for Effective Cyber Defense（効果的なサイバー防御のための重要なセキュリティコントロール） | （対象を限定していない） | サイバー攻撃に対する重要なセキュリティ対策を20のコントロールに分類し、優先度付けをしたもの。それぞれコントロールのサブコントロールも優先度付けがされている。 | Version6.0 2015年10月 (Center for Internet Security、SANS Institute) |
| **4** | Strategies to Mitigate Targeted Cyber Intrusions（標的型サイバー侵入の軽減戦略） | （対象を限定していない） | 主に標的型攻撃を対象とした35のセキュリティ対策を優先度順に並べたもの。 | 第2版 2014年2月 (オーストラリア国防信号局) |

４つのフレームワークの位置づけを見ると、サイバーセキュリティ対策としてやるべきことの全体的な整理に適しているのは、「サイバーセキュリティ経営ガイドライン」及び、「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」と考えられます。  
一方、具体的な対策の検討には、「Critical Security Controls for Effective Cyber Defense」及び「Strategies to Mitigate Targeted Cyber Intrusions」が参考にできます。また、「サイバーセキュリティ経営ガイドライン」の付録及び付録に記載の参考文献も対策の検討に役立ちます。

実際には、個々の組織によって事業やシステム構成等の状況は大きく異なるため、守るべき資産やリスクを正確に把握したうえで対策の検討・導入を進めることが望まれます。



## Writer Profile

セキュリティ事業部  
セキュリティコンサルティング担当 チーフコンサルタント  
戸田 勝之