UHY Tokyo & Co
Certified Public Accountants

# サイバーセキュリティ戦略本部：「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針の改定」を公表

UHY Tokyo ニュースレター / 2018年4月

政府は平成30年4月4日、サイバーセキュリティ戦略本部第17回会合を開催し、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針の改定」を公表しました。本指針では、重要インフラ事業者等が分野特性に応じた必要な情報セキュリティ対策を着実に実施し、また継続的に改善していくにあたって参照すべきガイドラインとして、平成29年4月にサイバーセキュリティ戦略本部で決定された「重要インフラの情報セキュリティ対策に係る第４次行動計画」を踏まえた改定がなされています。主な改定点は下記の通りであり、本指針の全文は下記URLからご確認ください。

https://www.nisc.go.jp/active/infra/pdf/shishin5.pdf

## １．主な改定点

・「重要インフラサービスの安全かつ持続的な提供」の観点から特に考慮すべき情報セキュリティの対策項目をPDCAサイクルに沿って例示。

・情報セキュリティの対策項目は、情報セキュリティの国際標準である「情報セキュリティマネジメントシステム」に加えて、米国NISTの「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」や「CSMS認証基準」等の重要インフラ関連の情報セキュリティの標準も考慮し、本指針によって重要インフラに関する主要な基準を網羅できるように構成。

・情報セキュリティ対策のPDCAサイクルを進める上で、経営層があらかじめ認識しておくべき事項や、経営層の積極的な関与が期待される場面、具体的な関わり方等を明確化。

・サイバー攻撃への初動対応や事業継続のための復旧対応の方針等を定める際において考慮すべき、「サイバー攻撃リスクの特性」並びに「対応及び対策の考慮事項」を整理。

・指針の関連文書として、「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」を新規策定

## ２．機能保証の考え方とは

機能保証の考え方は、「重要インフラの情報セキュリティ対策に係る第４次行動計画」において下記の通りとされています。

「重要インフラサービスは、それ自体が国民生活及び社会経済活動を支える基盤となっており、その提供に支障が生じると国民の安全・安心に直接的かつ深刻な負の影響が生じる可能性がある。このため、各関係主体は、重要インフラサービスを安全かつ持続的に提供するための取組（機能保証）が求められる。

なお、本行動計画において、「機能保証」とは、各関係主体が重要インフラサービスの防護や機能維持を確約することではなく、各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うことを意図している。すなわち、各関係主体が重要インフラ防護の目的を果たすために、情報セキュリティ対策に関する必要な努力を適切に払うことを求める考え方である。」

本指針の改定により、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、仮に発生した場合には迅速な復旧を図ることにより重要インフラサービスの安全かつ持続的な提供を実現することが期待されています。

---

ご質問やご要望がございましたら、お気軽にお問い合わせください。

---

※なお、本稿の意見に関する部分は、筆者の個人的な見解であることをあらかじめお断りします。

---

## コンタクト


**UHY東京監査法人**
小野　琢司 – IT・内部統制 PG
Email: takuji.ono@uhy-tokyo.or.jp

〒107-0052　東京都港区赤坂 7-3-37　プラース・カナダ 3F
Tel: +81 3 5410 1391 / Fax: +81 3 5410 2474
Website : http://www.uhy-tokyo.or.jp/