今すぐにでも必要なサイバーセキュリティ

～ デジタル変革社会への対応 ～

我が社は大丈夫だと言い切れますか？
リスクが特定分析され必要な対策が機能していますか？
事業継続・危機管理体制は必要な時に機能しますか？
システム・ネットワークは安心・安全に利用できていますか？
任せられる人材は育成できていますか？

サイバーセキュリティは経営問題です
その価値と実践手法をピンポイントで解説

（セミナー内容）

1. **サイバーセキュリティ経営ガイドライン（経産省）と**
   サイバーセキュリティフレームワーク導入
   ３原則と 10 項目とフレームワーク５つの機能
2. **リスクを合理的かつ最適な方法で管理してリターンを最大化し企業価値を高める活動の実践手法**
   シンプルで効果的な導入手法のご紹介
3. リスク対策状況を可視化する
   『フィット＆ギャップ分析』手法のご紹介
4. **稼ぐ力を支えるリスクマネジメントを定着させる必要とされる人材を育成するために**

開催日程：2019 年 9 月 20 日（受講無料）
14:00～17:00（CPD3 時間実績対応）

開催会場：東京秋葉原
アイ・エヌ・ジーシステムセミナールーム
東京都台東区台東 1-11-10 大木ビル 2F

受講申請：アイ・エヌ・ジーシステム
担当：柏倉　潤
kashiwakura_j@ingsystem.co.jp
講師：中西 孝治
nakanishi@isms-society.com

サイバーセキュリティ経営ガイドライン が発行されています（経済産業省）

企業のITの利活用は、業務の効率化による企業の収益性向上だけでなく、グローバルな競争をする上で根幹をなす企業として必須の条件となっている。さらに、IoTといった新たな価値を生み出す技術が普及しつつある中で、AIやビッグデータなども活用した、新しい製品やサービスを創造し、企業価値や国際競争力を持ったビジネスを構築していくことが企業として求められている。

サイバー攻撃は年々高度化、巧妙化してきており、サイバー攻撃によって純利益の半分以上を失う企業が出るなど、深刻な影響を引き起こす事件が発生している。さらには、攻撃の踏み台にされて外部へ攻撃をしてしまうだけでなく、国の安全保障上重要な技術情報の流出、重要インフラにおける供給停止など、国民の社会生活に重大な影響を及ぼす可能性のある攻撃も発生しており、その脅威は増大してきている。経営者が適切なセキュリティ投資を行わずに社会に対して損害を与えてしまった場合、社会からリスク対応の是非、さらには経営責任や法的責任が問われる可能性がある。また、国内外に関わらずサプライチェーンのセキュリティ対策の必要性も高まっており、業務を請け負う企業にあっては、国際的なビジネスに影響をもたらす可能性が出てきている。

また、セキュリティ投資は事業継続性の確保やサイバー攻撃に対する防衛力の向上にとどまるものではなく、ITを利活用して企業の収益を生み出す上でも重要な要素となる。セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要である。

このように、サイバー攻撃が避けられないリスクとなっている現状において、経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務である。

本ガイドラインは、大企業及び中小企業（小規模事業者を除く）の経営者を対象として、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がある「３原則」、及び経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO等）に指示すべき「重要１０項目」をまとめたものである。

経営者が認識すべき３原則

1. 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要（リスクマネジメントの定着）
2. 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要（監視・監査体制の整備）
3. 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要（危機管理体制の整備）

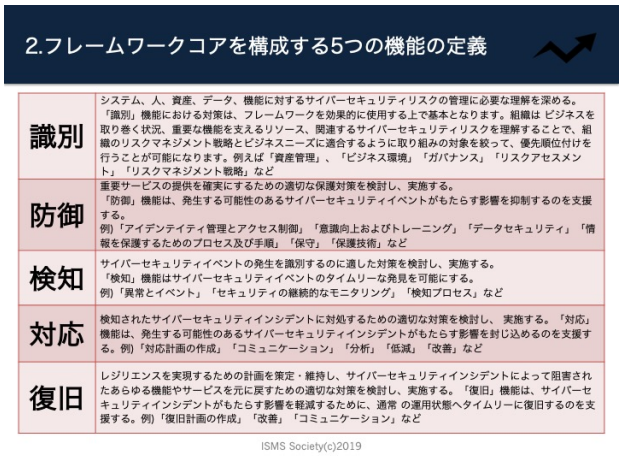
本セミナーでは、経営課題を解決することを目的として、サイバーセキュリティ経営ガイドラインを基にその効率的で効果的な実践方法を解説します。

重要インフラのサイバーセキュリティを 改善するためのフレームワーク（NIST）

NIST:アメリカ国立標準技術研究所

2014 年に米国国立標準研究所（NIST）が CSF（サイバーセキュリティフレームワーク）の 1.0 版を公開して以降、セキュリティ対策の検討・推進のフレームワークに、新たな選択肢が加わりました。あれから５年、年々進化するサイバーセキュリティリスクの高まりとともに、現在では多数あるセキュリティフレームワークの中でも、一番手の選択肢として、多くの企業・組織に利用されています。

人気・支持が高い一方で、NIST CSF を分かりやすく、体系的に解説しているコンテンツが少ないことを課題に感じてきました。このような状況をふまえて、NIST CSF の構成や特長を、可能な限りシンプルに ISMS（情報セキュリティマネジメントシステム）やリスクマネジメントシステムと共に解説します。



識別・防御・検知・対応・復旧に必要な対策（管理策）を考え実装する（ISMS 認証企業に於いては既存の管理策を見直す）ためのポイントを理解することが大切です。

デジタル変革によりビジネス環境が変化し続けています。安心・安全に事業目標を達成するために管理体制の再構築が求められており、一人一人のパフォーマンス向上を目的として稼ぐ力を支える人材の育成にも重点を置きます。

本セミナーでは、稼ぐ力を支えるリスクマネジメントの定着を目的として、情報セキュリティ・サイバーセキュリティ対策のあるべき姿をわかりやすく解説します。