ZJMR20198306

報道関係者各位

プレスリリース

2019 年 9 月 4 日

ゾーホージャパン株式会社

# サイバーセキュリティ経営ガイドラインの対応状況を可視化！

# 「サイバーセキュリティ評価チェックシート」を無償提供開始

セキュリティ対策で遅れを取っている日本。各企業はただちに対応を

ゾーホージャパン株式会社（代表取締役：迫 洋一郎、本社：横浜市）は、政府系や金融、大手企業向けでのセキュリティコンサルティングで多くの実績を誇る、ニュートン・コンサルティング株式会社の監修を受け、サイバーセキュリティ経営ガイドラインにより自社を評価する際に活用できるツール「サイバーセキュリティ評価チェックシート」の無償提供を 2019 年 9 月 4 日に開始しました。

## ■サイバーセキュリティ経営ガイドラインとは

これまでサイバーセキュリティ対策は IT 部門やセキュリティ担当者の責任で行うという風潮がありました。サプライチェーン全体を狙う攻撃への対策など、部門や担当者の責任範囲を超えているのは明らかです。
経済産業省という省庁レベルで「サイバーセキュリティ経営ガイドライン」が策定され、“やっと”サイバーセキュリティ対策は経営責任であると定義されたのです。

## ■サイバーセキュリティ経営ガイドラインの適用に際して

サイバーセキュリティ経営ガイドラインの適用には次のような点を意識して進めると良いでしょう。

**どの人員が実行すべき対策かを理解する**

サイバーセキュリティ経営ガイドラインは、サイバーセキュリティ対策を強化したい企業の次のような人員を想定して作成されています。

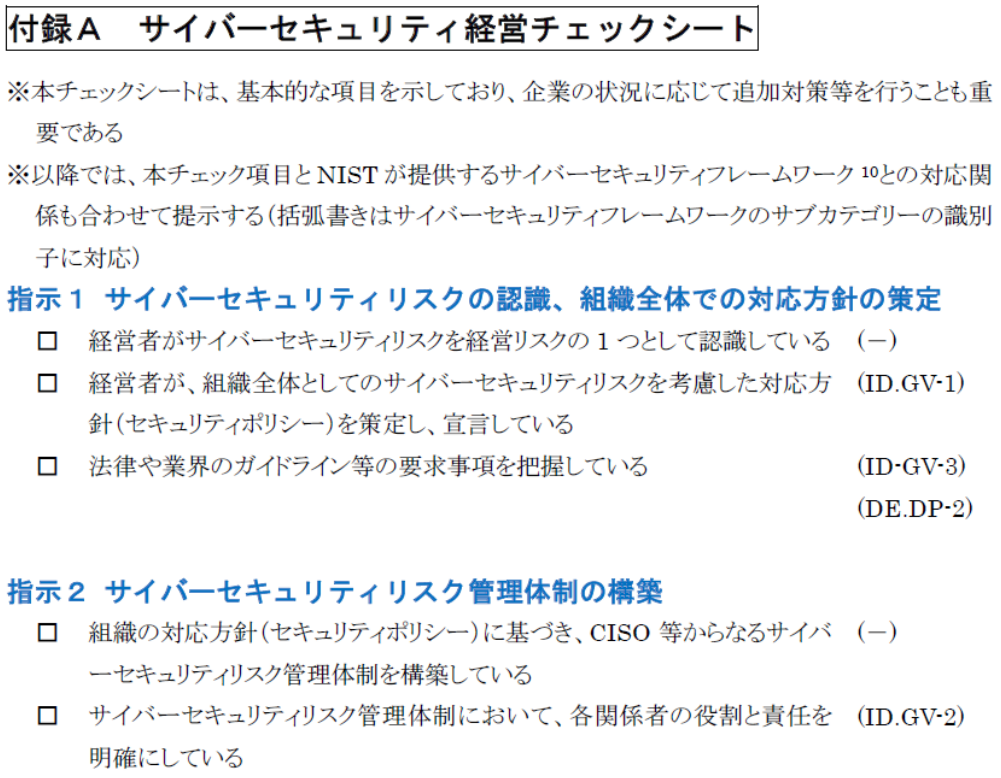
- 経営者
- サイバー攻撃対策を実施する上での責任者となる幹部（CISO 等）
- サイバー攻撃対策の担当者、CSIRT のメンバー等（セキュリティ担当者）
- 上記人材の育成や支援を担当する社内部門や社外の事業者（人材育成・支援担当者）

経営のガイドラインながらセキュリティ担当者や社外の事業者向けに技術的な情報も盛り込んでいる点は画期的と言えます。

**チェックシートの問いが抽象的**

サイバーセキュリティ経営ガイドラインの付録には「サイバーセキュリティ経営チェックシート」があります。

チェックシートながら、チェック用の問いが大まかであり、より具体的にチェックを行うことで効果を高められます。



付録A　サイバーセキュリティ経営チェックシート

※本チェックシートは、基本的な項目を示しており、企業の状況に応じて追加対策等を行うことも重要である

※以降では、本チェック項目とNISTが提供するサイバーセキュリティフレームワーク[10]との対応関係も合わせて提示する（括弧書きはサイバーセキュリティフレームワークのサブカテゴリーの識別子に対応）

**指示１　サイバーセキュリティリスクの認識、組織全体での対応方針の策定**

| | |
|---|---|
| □ 経営者がサイバーセキュリティリスクを経営リスクの１つとして認識している | （－） |
| □ 経営者が、組織全体としてのサイバーセキュリティリスクを考慮した対応方針（セキュリティポリシー）を策定し、宣言している | （ID.GV-1） |
| □ 法律や業界のガイドライン等の要求事項を把握している | （ID-GV-3）<br>（DE.DP-2） |

**指示２　サイバーセキュリティリスク管理体制の構築**

| | |
|---|---|
| □ 組織の対応方針（セキュリティポリシー）に基づき、CISO 等からなるサイバーセキュリティリスク管理体制を構築している | （－） |
| □ サイバーセキュリティリスク管理体制において、各関係者の役割と責任を明確にしている | （ID.GV-2） |

例えば「経営者がサイバーセキュリティリスクを経営リスクの１つとして認識しているか」というチェック項目があり、自社の状況について Yes または No で回答するように指示されています。

「認識しているかどうか」の問いに客観性を持って回答するのはどの企業でも難しいでしょう。
サイバーセキュリティ経営ガイドラインを理解しても、その適用にはセキュリティ専門家の知見をもって“認識している”とはどのような状態かを定義しておく必要があります。

## ■「サイバーセキュリティ評価チェックシート」の公開

この度、ゾーホージャパン株式会社は、このサイバーセキュリティ経営ガイドラインを各企業で適用する際にお使いいただける「サイバーセキュリティ評価チェックシート」を無料で公開いたしました。

サイバーセキュリティ評価チェックシートの特長を示します。

**サイバーセキュリティ評価結果**

【全体】

| 評価段階 | 5 |
|---|---|

| # | 大項目 | 大項目要約 | 評価(対象項目) | | |
|---|---|---|---|---|---|
| | | | 満点 | 得点 | 平均点 |
| (1) | サイバーセキュリティリスクの認識、組織全体での対応方針の策定 | (1)リスク認識、対応方針の策定 | 40 | 27 | 3.4 |
| (2) | サイバーセキュリティリスク管理体制の構築 | (2)リスク管理体制の構築 | 25 | 17 | 3.4 |
| (3) | サイバーセキュリティ対策のための資源（予算、人材等）確保 | (3)資源(予算、人材等)確保 | 45 | 31 | 3.4 |
| (4) | サイバーセキュリティリスクの把握とリスク対応に関する計画の策定 | (4)リスク把握とリスク対応計画の策定 | 190 | 125 | 3.3 |
| (5) | サイバーセキュリティリスクに対応するための仕組みの構築 | (5)リスクに対応する仕組みの構築 | 155 | 92 | 3.0 |
| (6) | サイバーセキュリティ対策におけるPDCAサイクルの実施 | (6)PDCAサイクルの実施 | 65 | 38 | 2.9 |
| (7) | インシデント発生時の緊急対応体制の整備 | (7)インシデントによる緊急対応体制の整備 | 170 | 102 | 3.0 |
| (8) | インシデントによる被害に備えた復旧体制の整備 | (8)インシデントによる復旧体制の整備 | 60 | 36 | 3.0 |
| (9) | ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握 | (9)サプライチェーン全体の対策及び状況把握 | 55 | 35 | 3.2 |
| (10) | 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供 | (10)情報共有活動への参加、攻撃情報の入手と有効活用 | 40 | 26 | 3.3 |

【技術的対策除く】

| # | 大項目 | 大項目要約 | 評価(対象項目) | | |
|---|---|---|---|---|---|
| | | | 満点 | 得点 | 平均点 |
| (1) | サイバーセキュリティリスクの認識、組織全体での対応方針の策定 | (1)リスク認識、対応方針の策定 | 40 | 27 | 3.4 |
| (2) | サイバーセキュリティリスク管理体制の構築 | (2)リスク管理体制の構築 | 25 | 17 | 3.4 |
| (3) | サイバーセキュリティ対策のための資源（予算、人材等）確保 | (3)資源(予算、人材等)確保 | 45 | 31 | 3.4 |

**数値化し客観的な評価が下せる**

サイバーセキュリティ経営ガイドラインの重要 10 項目の質問は曖昧で、実使用において必要な情報が不足しています。「サイバーセキュリティ評価チェックシート」では、実際の評価担当が数字で評価できるだけの材料となる「実施の目安」および「実施の確認事項」を示しています。

| 【大項目】 | 【中項目】 | 【実施の目安】 | # | チェック | 【実施の確認事項】 |
|---|---|---|---|---|---|
| サイバーセキュリティリスクの認識、組織全体での対応方針の策定 | (1)-1 経営者がサイバーセキュリティリスクを経営リスクの１つとして認識している | セキュリティポリシーに、サイバーセキュリティリスクを経営リスクとして認識していること、及び経営者の関与と責任について記載している。 | 1 | □ | サイバーセキュリティリスクに特化したセキュリティポリシーを新たに策定する場合には、サイバーセキュリティリスクを経営リスクとして認識していること、及び経営者の関与と責任に関する事項が記載されていることを確認する。 |
| | | 経営会議や経営リスクに関する委員会等において、サイバーセキュリティリスクを検討している。 | 2 | □ | 既存の「情報セキュリティポリシー」や「情報セキュリティの取り組みについて」等にサイバーセキュリティへの対策を記する場合には、サイバーセキュリティリスクを経営リスクとして認識していること、及び経営者の関与と責任に事項が追記されていることを確認する。 |
| | | | 3 | □ | 経営会議や経営リスクに関する委員会等において、議事内容にサイバーセキュリティリスクや対応に関する事あることを検証する。 |
| | (1)-2 経営者が、組織全体としてのサイバーセキュリティリスクを考慮した対応方針（セキュ | サイバーセキュリティリスクに対する対応方針（セキュリティポリシー）を策定していること、及びサイバーセキュリティリスクに対しては組織全体で対策することを記載している。 | 4 | □ | サイバーセキュリティリスクに対する対応方針（セキュリティポリシー）を策定し、サイバーセキュリティリスクに対し組織全体を対象に対策することを記載していることを確認する。 |
| | | 策定したセキュリティポリシーを経営者が承認、周知している。 | 5 | □ | 策定したセキュリティポリシーが、経営者に承認されていることを確認する。 |

重要 10 項目のひとつから例を挙げると「経営者がサイバーセキュリティリスクを経営リスクの１つとして認識しているか？」という問いでは、評価者も Yes または No で客観的な回答を下すことはできません。

**サイバーセキュリティ評価チェックシートの「実施の確認事項」で示される**

「サイバーセキュリティリスクに特化したセキュリティポリシーを新たに策定する場合には、サイバーセキュリティリスクを経営リスクとして認識していること、及び経営者の関与と責任に関する事項が記載されていることを確認する。」という問いのように“記載されているかどうか”という質問に対しては Yes または No での回答が容易です。

**他の主要なガイドラインも加味**

サイバーセキュリティ評価チェックシートは、サイバーセキュリティ経営ガイドラインを中心と位置づけ、ニュ

ートン・コンサルティング株式会社のこれまでのセキュリティコンサルティングにおける知見や次のような主要なガイドラインの内容も取り込んだチェックリストとなっています。

- JISQ15001:2017 付属書 A
- 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 Ver1.1
- NIST SP 800-171 Revision1
- CIS Controls version7
- ISO27001:2013 付属書 A
- ISO27017:2015 付属書 A
- 中小企業の情報セキュリティ対策ガイドライン第 3 版
- PCI－DSS バージョン 3.2.1

## ■おわりに

欧米諸国と比較して日本の各企業におけるセキュリティ対策は遅れを取っていると言われています。

各企業ではまず「サイバーセキュリティ経営ガイドライン」を理解し、ガイドラインへ準拠できているか自社を数値評価しましょう。

企業の評価の際には、ニュートン・コンサルティング株式会社の知見が凝縮された「サイバーセキュリティ評価チェックシート」を是非、ご活用ください。

**【「サイバーセキュリティ評価チェックシート」　ダウンロードリンク】**

**関連リンク**

- 「サイバーセキュリティ評価チェックシート」のダウンロード
- サイバーセキュリティ経営ガイドライン Ver.2.0
- サイバーセキュリティ経営ガイドライン 解説書
- サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集
- JISQ15001:2017 付属書 A
- 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 Ver1.1
- NIST SP 800-171 Revision1
- CIS Controls version7
- 中小企業の情報セキュリティ対策ガイドライン第 3 版
- PCI－DSS バージョン 3.2.1

## ニュートン・コンサルティング株式会社について

ニュートン・コンサルティング株式会社は企業/組織のリスクマネジメントに特化したコンサルティング会社です。2006 年 11 月、英 NewtonIT の日本法人として設立され、官公庁をはじめ様々な企業/組織に対する豊富な支援実績を有しています。特に全社的リスクマネジメント(ERM)、事業継続（BCP/BCM）、サイバーセキュリティの分野に注力。また、プロのコンサルタントがリスクマネジメントに関する知識やテクニックを解説する講座「ニュートン・アカデミー」を積極的に開催しています。

## ManageEngine について

ManageEngine は、ゾーホージャパン株式会社が提供するネットワークや IT サービス、セキュリティ、デスクトップ・ノート PC、ビジネスアプリケーションなどを管理する製品・サービス群です。必要十分な機能に限定、かつ、直感的な操作が可能な画面設計により、短期間での導入が可能であり、その後の運用フェーズにおいても手間がかからず、よりシンプルな IT 運用管理を実現します。

また、中堅・中小企業でも導入しやすいリーズナブルな価格で、これまで大手 IT ベンダーが提供する複雑で高額なツールを利用していた企業や、ツールを自社開発していた組織にも採用されてきました。現在では、日本国内の一般企業、官公庁や自治体などへ、5,000 ライセンスを超える販売実績があり、安心して使える製品・サービスです。

最大で 29 言語に対応する製品・サービスは、北米、欧州をはじめ、南米、中東、アジアなど世界で 18 万社以上の企業や組織が導入し、企業・組織の IT 運用管理のシンプル化、グローバル化に貢献しています。

ManageEngine

https://www.manageengine.jp/

## ゾーホージャパン株式会社について

ゾーホージャパン株式会社は、ワールドワイドで事業を展開する Zoho Corporation Pvt. Ltd.（本社：インド　タミル・ナドゥ州チェンナイ　CEO：Sridhar Vembu）が開発/製造したネットワーク管理開発ツールや企業向け IT 運用管理ソフトウェア、企業向けクラウドサービスを日本市場に提供すると同時に関連するサポート、コンサルティングなども提供しています。

企業向け IT 運用管理ツール群「ManageEngine」は、世界 18 万社を超える顧客実績を誇り、国内でも販売本数を伸ばしています。「ManageEngine」は、ネットワーク管理の OEM 市場でスタンダードとして認知されてきたネットワーク管理開発ツール「WebNMS」のノウハウや経験を生かして開発されたものです。

また、業務改善/生産性向上を支援する企業向けクラウドサービス群「Zoho」は、世界で 4,500 万人を超えるユーザーに利用されています。国内では「Zoho CRM」を中心にユーザー数を増やしており、40 種類以上の業務アプリケーションを 1 セットで利用できる「Zoho One」の提供も始まっています。

ZOHO

http://www.zoho.co.jp/

**【お問い合わせ先】**

■報道関係からのお問い合わせ先：ゾーホージャパン株式会社　マーケティング部
Mail：jp-memarketing@zohocorp.com　TEL：045-319-4613
■お客様からのお問い合わせ先：ゾーホージャパン株式会社　営業部
Mail：jp-mesales@zohocorp.com　TEL：045-319-4612
■ゾーホージャパン URL：http://www.zoho.co.jp/
■ManageEngine 事業サイト URL：https://www.manageengine.jp/