JNSA 全国セミナー向け
MY CISO ハンドブック・テンプレート
Ver α00

JNSA　CISO 支援ワーキンググループ

目次

はじめに

多くの中小企業では、業務の執行体制が不明瞭で、担当の兼任が多く、明確な責任者が決められておらず、IT やセキュリティに対する執行体制が出来ている企業は、現状では稀な存在だと考えられます。一方で、今日においては、IT システムなしで企業経営や業務執行を行うことは現実的ではありません。そして、セキュリティ事案（事件・事故）が起きた場合には、情報システム部門だけの問題ではなく、企業全体に大きな影響をもたらします。

このような状況において、企業におけるセキュリティを取りまとめる CISO というポジションが注目されています。JNSA CISO 支援ワーキンググループでは、CISO の業務執行をサポートする目的で、2018 年 5 月に「CISO ハンドブック[1]」を公表しました。CISO ハンドブックでは、主に明確な経営体制を持つ企業を想定していることから、ここで述べたような中小企業の CISO には、必ずしも使いやすいものにはなっていません。

「MY　CISO ハンドブック・テンプレート」では、中小企業の CISO やセキュリティ担当者が、セキュリティに関わる業務を執行し、経営陣と適切なコミュニケーションを進めるうえで明確にすべき項目と内容を例示しました。例示したものを自社に則した内容に変えていくことで、ご自身の「MY CISO ハンドブック」として活用し、日常的な業務の中にセキュリティ業務を組み込でいただけるものと考えます。

なお、注意していただきたい点があります。「MY CISO ハンドブック」も作成は、入り口でありゴールではなく、また、初めから良いものが出来るものではありません。まずは、「MY CISO ハンドブック」の作成を通じて、ご自身や会社の現状と方針を明らかにすることが最初のステップとなります。これを、日々の運用の中でブラッシュアップしていくことで、徐々に完成度が高まり、セキュリティ対策の推移が記録されていくものと考えます。

計画・実施・評価を適切に行える、いわばグリップ感を持って業務執行と、関係者からの協力と評価を得るためのツールとして、「MY CISO ハンドブック」を活用いただければ幸いです。

---

[1] CISO ハンドブック(JNSA)　https://www.jnsa.org/result/2018/act_ciso/index.html

現状把握

まずは、現状を把握できなくては、セキュリティ計画の立案もできません。ここでは、最低限把握すべきと考えられる項目と、その例をご紹介いたします。

業務とシステムおよびデータの関連性確認

社内にどのようなIT システムと、業務内容の関連性をまとめます。それぞれ、担当者を明らかかにするとともに、許容できる停止時間と、データの重要性についてまとめます。

これは、いわゆるリスク分析のベースとなり、セキュリティ投資を行う際の根拠の一つとなるものです。加えて社内の業務とシステムの担当責任者もそれぞれ明確にします。なお、業務やシステムについては、ご自身の組織に合わせてご利用ください。

この表を作成する際には、すべての情報が㊙としたくなると思いますが、多くの情報を㊙としてしまうと、コストが膨大になることに加えて、使いにくいシステムになってしまいます。このため、事前に情報のクラシフィケーション（分類）方法を明確にし、㊙とすべき条件を決めておくことをお勧めします。

表 1　業務とシステムの関連表（別紙参照）

				ITシステム:許容停止期間(時：数時間、日：数日、週：一週間程度、－：それ以上）、データクラス（㊙、〇）								
				メール	ファイル共有	カレンダー	チャット	ワークフロー	給与通知	ｵﾝﾗｲﾝﾊﾞﾝｸ	クラウドA
			担当	IT:高橋	IT:荒木	IT:深谷	企画:小屋	総務:田中	人事:福岡	IT:佳山	開発:山本
主要業務	製造・販売	製品企画	北澤	時:㊙	日:㊙	時:㊙	日:㊙	日:㊙	N/A	N/A	日:〇
		資材調達	池上	時:㊙	日:㊙	時:㊙	日:㊙	日:㊙	N/A	N/A	日:〇
		製造	西尾	日:㊙	日:㊙	日:〇	-:〇	週:㊙	N/A	N/A	N/A
		販売	唐沢	時:㊙	時:㊙	時:〇	時:㊙	時:㊙	N/A	N/A	N/A
		配送	下村	時:㊙	時:〇	時:㊙	時:㊙	日:㊙	N/A	N/A	N/A
		受発注	赤羽	時:㊙	時:㊙	時:㊙	時:㊙	時:㊙	N/A	N/A	N/A
		サービスA	武田	時:㊙	時:㊙	時:㊙	時:㊙	時:㊙	N/A	N/A	N/A
	庶務	労務管理	丸山	時:㊙	日:㊙	時:㊙	時:㊙	日:㊙	N/A	N/A	N/A
		経理	林	時:㊙	日:㊙	日:㊙	時:㊙	時:㊙	N/A	時:㊙	N/A
		給与支給	黒川	時:㊙	日:㊙	日:㊙	時:㊙	時:㊙	時:㊙	時:㊙	N/A
		総務	村上	時:㊙	日:㊙	日:㊙	時:㊙	時:㊙	時:㊙	時:㊙	N/A
	RD	研究	河野	時:㊙	日:㊙	時:㊙	時:㊙	日:㊙	N/A	N/A	N/A
		開発	佐々木	時:㊙	日:㊙	時:㊙	時:㊙	日:㊙	N/A	N/A	時:㊙
	スタッフ	経営陣	佐藤CEO	時:㊙	日:㊙	時:㊙	時:㊙	日:㊙	N/A	N/A	N/A
		経営企画	長谷川	時:㊙	日:㊙	時:㊙	時:㊙	日:㊙	N/A	N/A	N/A
		役員秘書	猿田	時:㊙	日:㊙	時:㊙	時:㊙	日:㊙	N/A	N/A	N/A
		広報	坂口	時:㊙	日:㊙	時:㊙	時:㊙	日:㊙	N/A	N/A	N/A
		受付	清水	時:㊙	日:㊙	時:㊙	時:㊙	日:㊙	N/A	N/A	N/A
		情シス	牧野	時:㊙	日:㊙	時:㊙	時:㊙	日:㊙	N/A	N/A	時:㊙

外部関係者一覧

緊急時の連絡体制をまとめるために社外の関係者の一覧を作成します。連絡先を入れる

場合は、保管の方法に注意し、閲覧の権限についても検討してください。

表 2　外部関係者一覧

取引先	窓口	担当	取引内容等
AB 商事	阿部部長	北澤	XXX の主要な販売先
JNSA	下村社長	池上	材料 XXX の仕入れ先
JASA	土井課長	西尾	材料 YYY の仕入れ先
TT 法律事務所	森弁護士	唐沢	顧問弁護士
YM 会計事務所	佐藤税理士	下村	会計処理
経済産業省	小山課長補佐	赤羽	

事故・事件の対応手順

事故や事件に備えるため、最低限の対応手順をまとめます。本来であれば、より詳しい手順が望ましいのですが、すぐにできる作業として、まずは、この最低限の手順をまとめることをお勧めします。なお、より詳しい内容については、「CISO ハンドブック」のインシデントシミュレーションをご参照ください。

例）

1. 情報セキュリティの事件・事故対応は、CISO と情シスを中心に緊急対応チームを立ち上げ対応を行う
2. システム停止等、業務への影響が及ぶ場合は、できるかぎり関係部門への連絡を試みるが、緊急の場合は緊急対応チームが判断をしてかまわない
   - ただし、経営陣に対して一報を入れるものとする。
3. 外部への公表は、広報を通じて行う。SNS などへの書き込みを行わない
   - 社員にも徹底させるために、逐次状況を社員に周知する
4. 法的な判断が必要な場合は、顧問弁護士に連絡をする
   - できるだけ素人判断は避けるが、対応が後手にまわることは避ける
5. ウィルス感染の際は証拠保全よりも復旧を優先する
   - ただし、緊急性が高いと判断をした場合は、専門業者への相談を検討する
6. 社内で解決ができない、判断ができない場合は、JNSA 「サイバーインシデント緊急対応企業一覧」を参考にする
   - JNSA 「サイバーインシデント緊急対応企業一覧」
     https://www.jnsa.org/emergency_response/

関連業務規程等とコンプライアンス対応状況

対応が必要な法律などについて、社内規定などの対応状況をまとめます。業種により、多様な規定があると思いますが、ここではセキュリティと関連の深い、個人情報保護法を例示します。

- 個人情報保護法

  例）

  - 個人情報保護責任者が任命されている
  - 個人情報の取得に関する方針が社内外に明示され、実施されている
  - 個人情報の安全管理措置が明記され、実施されている。
    - 第三者提供について明示されている
    - オプトアウトを受け付ける窓口が社内外に明示されている
    - 開示請求の窓口と体制が社内外に明示されている
  - 匿名加工情報に関する方針が明記され、実施されている
  - 個人情報が漏洩した際の対応が明記されている

個人情報保護法ハンドブック（個人情報保護委員会）
https://www.ppc.go.jp/files/pdf/kojinjouhou_handbook.pdf

- GDPR
  - GDPR の対象になるかどうか確認をする
  - 外部サービス（SaaS 等）の選定にあたっては、GDPR 対応状況を確認する

運用状況の把握

情報システムやセキュリティ担当者は、日々の運用をこなすことで精いっぱいとなり、現状把握がおろそかになりがちです。しかし、日々の状況を把握し、小さなトラブルの種を見つける作業を続けないと、対策が適切に実施されているのか、また、そもそも対策は適切であるのか判断することができません。そして、情報漏洩などの大きな事件につながる兆候をつかむことも難しくなります。

また、システムやセキュリティを適切に維持し続けるためには、大変な労力を使う必要がありますが、これを他部門の方に理解してもらうことは容易ではありません。適切な運用状況の把握を行い、事実に基づいた報告を行っていくことが、経営陣や事業部門と適切なコミュケーションを取るための重要な礎となっていきます。

計画の実施状況の把握

日々の運用から、セキュリティ計画の実施状況を把握するようにします。推奨される項目は以下の通りです。

例）

- ウィルスの検知状況
- スパムの検知状況
- システムエラーなどの障害
- セキュリティポリシーなどの順守状況
  - セキュリティパッチの適用率
  - 最新のパターンファイルをリアルタイムで利用
  - OS やアプリのバージョン
  - 多要素認証の利用率
- 情報システム部門への依頼事項
  - チケットシステムなどで管理することが望まれます。
- 情報システムにかかわる障害
- 侵入などの物理的なインシデント

事故・事件の把握

実際にセキュリティを担当すると、日常的に何らかの事件・事故が発生していることに驚く方も多いと思います。ひとつひとつの事件・事故を適切に処理することはもちろん重要で

すが、プロセスを明確化し、記録を取り、再発防止策を実施していくことで、事件・事故が起こりにくくすることも重要です。

例）

- チケットシステムなどで管理する
  - メールやチャットでのやり取りも転記する
- 程度にもよるが小さな事案も記録する
  - プロセスが常に動いているようにする
- 事案を憎んでも人は（できるだけ）憎まない
  - 高圧的な対応を行うと、事件が隠蔽されるようになる
  - ただし、重大事案の時は厳格な対応も必要
- セキュリティ情報も収集し、自社の対策状況検証の材料とする
  - 深刻な脆弱性の公表
  - 話題となったセキュリティ事件
- 適切な報告を実施する
  - 緊急のものは即時、そうでない場合は、月次などで経営陣に報告をする

通常オペレーション

アカウントの作成、ネットワークのトラブル対応など、様々な日常業務が発生します。これらの、取るに足らないような業務についても、できるかぎり記録を取るようにします。

例えば、ある会社では、かならずチャットシステム（slack）に概要を投稿することで、関係者が状況を把握しやすくするとともに、作業の履歴となるようにしています。

経営陣への報告

情報システム部門、セキュリティ部門の労力が報われないひとつの要因として、適切な報告が行えていないことが考えられます。事業部門は数字（売上など）で成果を計測することができますが、情報システム部門、セキュリティ部門は、金額に該当する数字を適用することは難しい面があります。

このため、経営に沿った業務を行い、合理的な評価を得るためには、経営陣や事業部門と良好なコミュニケーションを構築し、目に見える形で成果を伝える必要があります。経営陣への報告は、このための重要なツールとなります。

週次報告（主に関係者向け）

一週間の状況をまとめることは、日々の業務の助けになるばかりでなく、関係者が同じ認識を持つための重要な取り組みです。

週次でまとめる項目としては、以下のものが考えられます。

例）

- 特記事項
  - 事件
  - 事故
  - その他
- モニタリング項目
  - ウィルス検知状況
  - ダウンタイム
- セキュリティ計画の進捗状況
  - 表かチャート、または箇条書き
- 先週のイベント[2]
  - 先週のイベントの実施状況、課題、その他
- 今週のイベント
  - ネットワーク工事
  - ソフトの更新
  - 社内イベント

[2] イベント: アプリ・サービス・システム等の新設、開始、更新、停止、終了など、IT に関わる計画的な作業の総称

- 報道等
  - 他社の事故や事件など

月次報告

可能であれば、月次で経営陣への報告を行うようにします。最初は、技術者言葉で書いてしまうと思いますが、経営陣とのやり取りを通じて、共通の言語を構築し、経営陣の一員として考えるべき事柄や、あり方も学ぶようにします。

- 特記事故（事件・事故）
- セキュリティ計画の進捗状況
  - プロジェクト面
  - 予算面
  - 追加の計画（内容、予算）
- モニタリング項目
  - 淡々と一覧で
- 前月の主要なイベントとその結果等
- 今月予定される主要なイベント
- 共有すべき報道等

四半期～年間の報告

基本的には月次の延長となりますが、PDCA の Check を意識した予算と業務の執行状況、必要な Action、そして何をどのように改善・向上させていくかをまとめます。

- 月次のまとめ
- 修正をすべき計画
- 改善・向上施策

緊急の報告

問題が発生した場合、状況把握に時間を取ってしまい、報告が後手になることが少なくありません。たとえ状況がはっきりしていない場合でも、経営陣に一報を入れ、必要であれば待機を要請するなど、ワーストケースに備えた対応が望まれます。

先にまとめた「事故・事件の対応手順」に基づいて対応を行い、うまくいった点、いかなかった点を「事故・事件の対応手順」に反映するようにします。

例）インシデント概要

項目	内容
いつ(when)	時刻の標準時（JST/UTC など）を明確にする
どこで(where)	システム名、組織名など
何が(what)	XX システムが停止した XX システムの YY が漏洩した
どのように(how)	不正アクセスが疑われる システム障害の可能性が高い
なぜ(why)	この段階では究明を急がない
誰が(who)	この段階では究明を急がない
補足事項	

例）影響と対策

項目	状況
情報資産の影響度 （深刻度は厳密には定義しない）	□ S:既に深刻な状況である □ A:深刻な影響である可能性が高い □ B:一定の影響がある可能性が高い □ C:軽微な影響の可能性
緊急度	
影響のある情報の種類	
影響を受ける顧客数と特徴	
想定される二次被害	
推奨する緊急対応	
事故の原因・要因/再発防止策	この段階では分析・究明を急がない

むすび

セキュリティには限りませんが、日本では技術者が経営を学ぶ機会は極めて少ないこともあり、技術者が経営にかかわっていくことは容易ではありません。幸か不幸か経営陣に加わった技術者は、大変な思いで難しい業務に取り組んでいるものと思います。

一方で、技術者の特性として、概念モデルが構築できれば、比較的容易にこなすことができる傾向があります。経営についても、技術者が理解しやすい概念モデルがあれば、より多くの方が、経営陣の一員として力を発揮できるものと考えています。CISO 支援ワーキンググループでは、実務者や有識者の知見を集め、技術者が経営の概念モデルを構築し、これを実践していくための取り組みを行っています。

巻末に、参考にしていただきたい代表的な JNSA の成果物をご紹介します。

覚えて損のない今日的なセキュリティ TIPs

ここでは、「MY CISO ハンドブック」を制作していくうえで参考としていただける、今日的なセキュリティ TIPs をご紹介します。

特定の担当者に依存しすぎてはダメ

中小企業では、IT 業務が特定の担当者に任されていて、その担当者以外は何がどうなっているかがわかないという場合が少なくありません。優秀な担当者が、自身の判断で業務をできるので効率的ではあるのですが、様々なリスクがあります。

- 担当者が退職すると業務が混乱する
- ドキュメント化がおざなりになりやすい
- 業務上のミスが見えにくく、不適切なオペレーションになっていく場合がある
- 内部不正、内部犯行につながりやすい

あるホスティングサービス事業者は、ひとりのスーパーエンジニアに運用の大半を任せていましたが、ある時、このエンジニアのミスから、ホスティングしていたデータをすべて消失するという事故につながりました。このような極端な例ではなくとも、担当者しかわからないというケースは少なくないと思います。

体制の構築（チーム化）、運用の簡素化（クラウドの利用など）、ワークフローの整備、セキュリティ担当の設置、内部監査の実施などを通じて、上記リスクを軽減していく必要があります。

ファイアウォールとアンチウィルスではダメ？

多くの場合、インターネットと社内ネットワーク（イントラネット）をゲートウェイで分離することで、外部からの攻撃はゲートウェイで防御し、侵入したウィルスはアンチウィルスで対応するという、ネットワーク分離モデルがセキュリティ対策ベースとなっています。ネットワーク分離モデルは、今でも重要な対策のひとつですが、効果的な対策とは言えない状況となりました。これは、次のようなネットワーク分離モデルの前提が崩れてしまったためです。

- 重要な情報はイントラネットに存在する
- すべての通信はゲートウェイを解析可能な形態で通る

- アンチウィルスは（ほとんどの）ウィルスを検知・駆除できる

今日では、多くの情報がクラウド等のインターネット上に移動しているため、イントラネット外の情報の守り方を考える必要があります。また、イントラネットを介さずにクラウドとの通信が可能で、マルウエアも暗号化した通信を行うことから、ゲートウェイでは解析できない通信やトランザクションも増えています。

攻撃の検出力にも課題があります。マイクロソフト社の調査によれば、攻撃の 96%は使い捨てのマルウエアが利用されており、ほとんどの場合、これらのマルウエアはパターンファイルでは検出できない状況です。次世代アンチウィルスと呼ばれるパターンファイルに依存しないウィルス対策もありますが、誤検知の対応に手間がかかること、また、PowerShell などの汎用的なツールを使った攻撃を検知することが難しい面があるなど、シルバーブレット（銀の弾丸）とは呼べない状況にあるようです。

第 24 回 マルウェアの 96%は「使い捨て」――マイクロソフトが 3 カ月分析して分かったこと（1/2）
https://www.itmedia.co.jp/enterprise/articles/1712/11/news012.html

ID マネジメント

アンチウィルスやゲートウェイといったセキュリティ対策は、マルウエア等に着目をした「異常系」のセキュリティ対策です。これに対して、誰が何をできるのかに着目をした ID マネジメントとアクセスコントロールは、「正常系」のセキュリティ対策と言えます。

例えば、CISSP（Certified Information Systems Security Professional）では、ID マネジメントを IAAA（Identity, Authentication, Authorization, Accountability）と呼び、セキュリティの基本として位置付けています。これまでも ID マネジメントは重要なセキュリティ対策でしたが、クラウド等の外部サービス利用が一般化した環境においては、より ID マネジメントの重要性が高まっています。クラウド利用を前提とした ID マネジメントのポイントを以下にご紹介します。

- シングルサインオン（SSO: Single Sign One）ができること
  - サービスを選択する際の主要な要件としてください。
  - 入社時に、ID とパスワードを 5 個用意してください、というよう企業は、ID マネジメントが破綻していると考えるべきです。
  - 社内システムも SSO を利用するようにしてください。
  - 社員の PC などのアカウントも SSO の利用が望まれます
- 多要素認証ができること

- 多くの侵入は、ID とパスワードを推測したものです。また、無数のパスワードが漏洩している今日では、ID とパスワードだけでアカウントを守ることは不可能です。
- 多要素認証が選択できるサービスを利用するようにしてください。

デバイスマネジメント

今日の主要なセキュリティ対策のベストプラクティスでは、意外なことにインベントリ（資産の把握・管理）が最重要視されています。例えば、米国 SANS が公表している CIS Controls（旧 Critical Security Controls、SANS TOP20）では、1 番目にハードウェアのインベントリ、2 番目にソフトウェアのインベントリ、そして、3 番目に脆弱性管理、5 番目にセキュリティ設定が挙げられており、マルウエア対策は 8 番目となっています。

インベントリを適切に実施し、管理下にある端末を安全に保つことが、重要であることは明らかだと思います。しかし、ハードウェア・ソフトウェアのインベントリは、意外に手間のかかる業務で、手作業では維持が難しい業務です。これを自動化し、脆弱性対策やセキュリティ設定を自動化するための手段として、デバイスマネジメントの重要性が高まっています。

従来のデバイスマネジメントは、イントラネット内で利用する PC を中心としていますが、MDM(Mobile Device Management)と呼ばれる製品では、スマートフォンなども含めた、多様なデバイスを管理することが可能で、社内から持ち出しをする PC、タブレット、スマートフォンの対応が可能です。また、ウィルスなどに感染した PC をネットワークから遮断や、紛失したデバイスのデータを消去（ワイプ）することも可能です。

現実問題として、セキュリティ設定を社員に指示し、手作業で確認を行うといったやり方では、実効性は極めて低いと考えられます。MDM などを導入して、一括した管理と対応ができる環境にすることが望まれます。

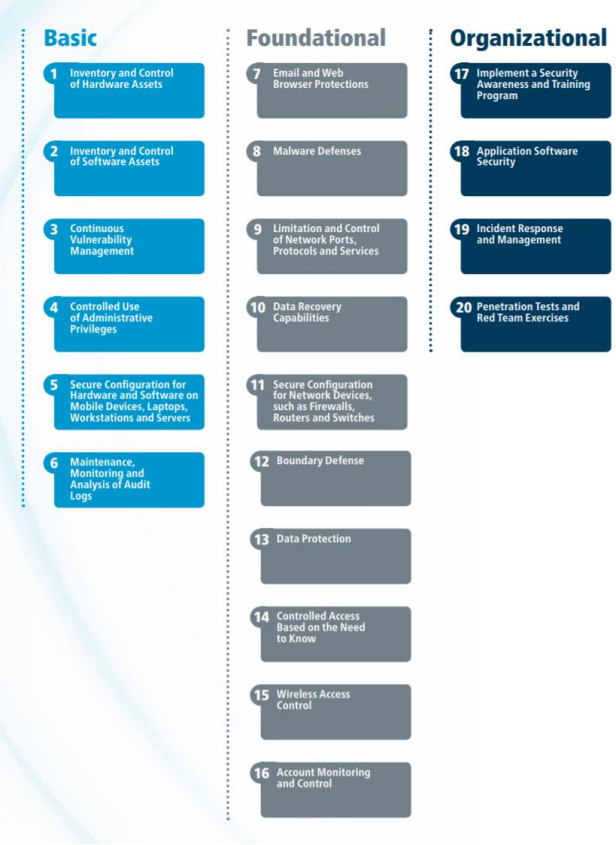


図 1 SANS CIS Control

https://www.cisecurity.org/controls/

外部サービスの選び方

クラウドサービスの普及に伴い、いわゆるオンプレミスとして社内にサーバを設置するケースは激減しています。一方で、外部サービス（メール、チャット、スケジューラ、ファイルサーバ、ワークフロー、ERP、ソースコード管理等）の選択が課題となっています。

つまり、どのような基準でそのサービスの利用を許可したか、許可しなかったかを社内に伝える必要があり、また、インシデントが発生した場合は、社外への公表も求められる可能性があります。大手のサービスプロバイダでは、ISO27017, ISO27018, FedRAMP, SOC2/SOC3, PCI DSS 等の認証を取得することで、利用者がサービスを選択する際のセキュリティ上の根拠を提示しています（個人的には、ISO/IEC27001 はサービス選定の基準としては不十分だと考えています）。しかし、特に日本のサービスプロバイダではこれらの認証を取得していない場合が多く、加えてサービスに対して行っている具体的なセキュリティ対策も公表していません。このような状況では、選択の根拠を示すにはユーザ自らが確認をするしかない状況です。

ある WG メンバーが実際に行っている評価方法をご紹介します。

- Cloud Security Guide for SMEs(ENISA)ベースのリスク評価（別紙）

経営陣など社内で影響力の社員があるサービスを利用したい場合、セキュリティ担当者には許容できないレベルのセキュリティでも、利用を許可せざる得ない場合があります。この際に、どのようなリスクがあり、サービスのどこに問題があるのか、そして自社がどのようなリスクに直面するのかを明確にする必要があります。

ある企業では、ENISA (European Union Agency for Network and Information Security) が公表している、Cloud Security Guide for SMEs をベースに、サービスのセキュリティ評価を行い、サービス利用の可否を判断し記録しています。必ずしも簡単なツールではありませんが、サービスを評価し、問題点を明らかにするために利用することができます。サービスの公式サイトから項目を埋めるための情報を探し出すことは、意外に大変な作業です。海外のサービスでは、英語での記載になりますし、また国内のサービスで、情報自体が公開されていないことも少なくありません。

このツールは有用ではあるのですが、それなりに手間のかかる作業になります。

Cloud Security Guide for SMEs(ENISA)
https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

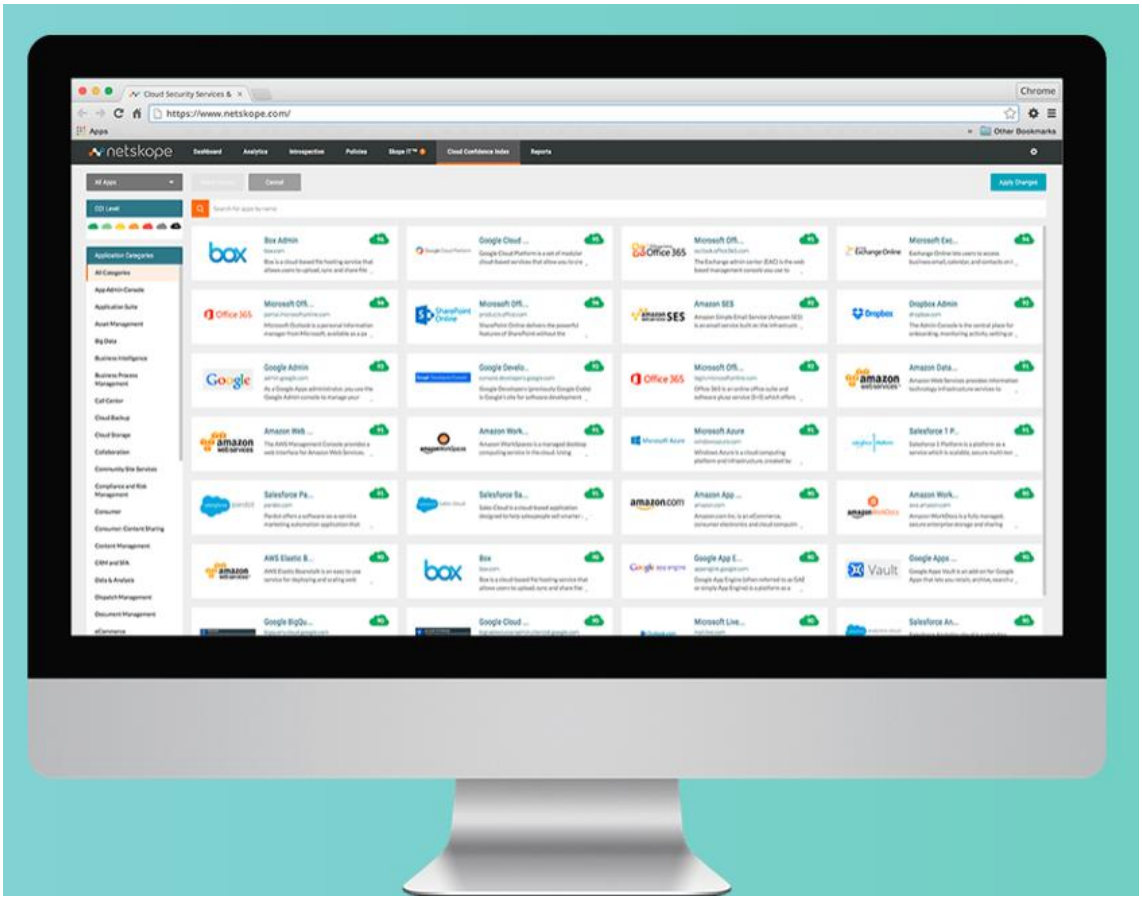
表 3　ENISA ベースのリスク評価表

	A	B	C	D	E	F
1	Sample					
2	**Impact rating**	0	0		**利用回避の判断**	
3	Confidentiality (3 High)	2	0		Sample Proを利用し、限られた人だけアクセス出来るProtected modeの利用義務付けることで、Confidentialを含めた、データの取り扱いを認める。	
4	Integrity (3 High)	1	0		ただし、公開を前提とした論文などのドキュメントに限るものとする	
5	Availability (3 High)	1	0		（2018/06/14）	
6	File Share (1:no, 2: internal, 3:external)	3	0			
7	(1-3)	Rating	Assess			
8	S01: Linkによるファイル共有	3	1.0		**主要な取り扱い情報のインパクト**	
9	S02: ファイル共有機能	3	2.0		申請前の特許情報など、当社にとって機密性の高い情報を取り扱う。これが漏れた場合は、公知の情報とされ、特許の取得が難しくなる可能性があり、特にLink機能を使った共有方法が問題と考えられている。	
10	S03: MFA	3	2.0		取り扱う情報に顧客のCofidential情報が含まれる可能性は低い	
11	S04: SSO	3	2.0			
12	O01: Geographic spread (A)	1	2.7			
13	O02: Elasticity(弾力性・柔軟性) (A)	1	3.0			
14	O03: Standard formats and interfaces	0	0		**セキュリティ評価**	
15	O04: Physical security max(C,I,A)	2	3		アプリケーション開発、サーバーセキュリティ、ネットワークセキュリティについて、Web上に明確な記載がない。	
16	O05: Incident response around-the-clock max(C,I,A)	2	3		取り扱うデータの性格上、データの暗号化ができないなど、セキュリティ面での課題がある。	
17	O06: Software development max(C,I,A)	2	1.0		Sampleのサイトが攻撃を受けた際には、情報が流出する可能性が少なくない。	
18	O07: Patching and updating max(C,I)	2	1.0			
19	O08: Backups (A)	1	1.7			
20	O09: Server-side storage (C)	2	2.0			
21	O10: Security-as-a-service and security add-ons	0	0			
22	O11: Certification and compliance max(C,I,A)	2	2.0			
23	R01: Software security vulnerabilities max(C,I,A)	2	1.0			
24	R02: Network attacks max(C,I,A)	2	1.0			
25	R03: Social engineering attacks max(C,I)	2	1.7			
26	R04: Management GUI and API compromise max(C,I)	2	2.0			
27	R05: Device theft/loss	0	0			
28	R06: Physical hazards (A)	1	2.0			
29	R07: Overloads (A)	1	2.0			
30	R08: Unexpected costs	0	0			
31	R09: Vendor lock-in	0	0			
32	R10: Administrative or legal outages (A)	1	1.0			
33	R11: Foreign jurisdiction issues (A)	1	1.0			
34						

Impact Analysis | Summary | 評価表

- 外部データベースの利用

外部のクラウドサービスのセキュリティ評価結果を利用することも可能です。例えば、Netskope 社が提供している CCA（Cloud Confidence Audit）では、主要なクラウドセキュリティ団体の一つ CSA（Cloud Security Alliance）の Could Controls Matrix に基づいた、クラウドサービスの評価を行っています。ここで評価されている場合、セキュリティ的な評価が一目でわかるため、すぐに利用の可否を判断することが可能です。



出展：Netskope https://www.netskope.com/resources/netskope-cci-audit

- 問診表

リスク評価を実施するための情報が公開されておらず、外部データベースで評価されていないサービスも少なくありません。この場合には、ENISA ベースのリスク評価表では話がかみ合わないことも多いことから、別紙の「セキュリティ上の確認事項」を使って、サービスプロバイダから回答を得るようにしています。

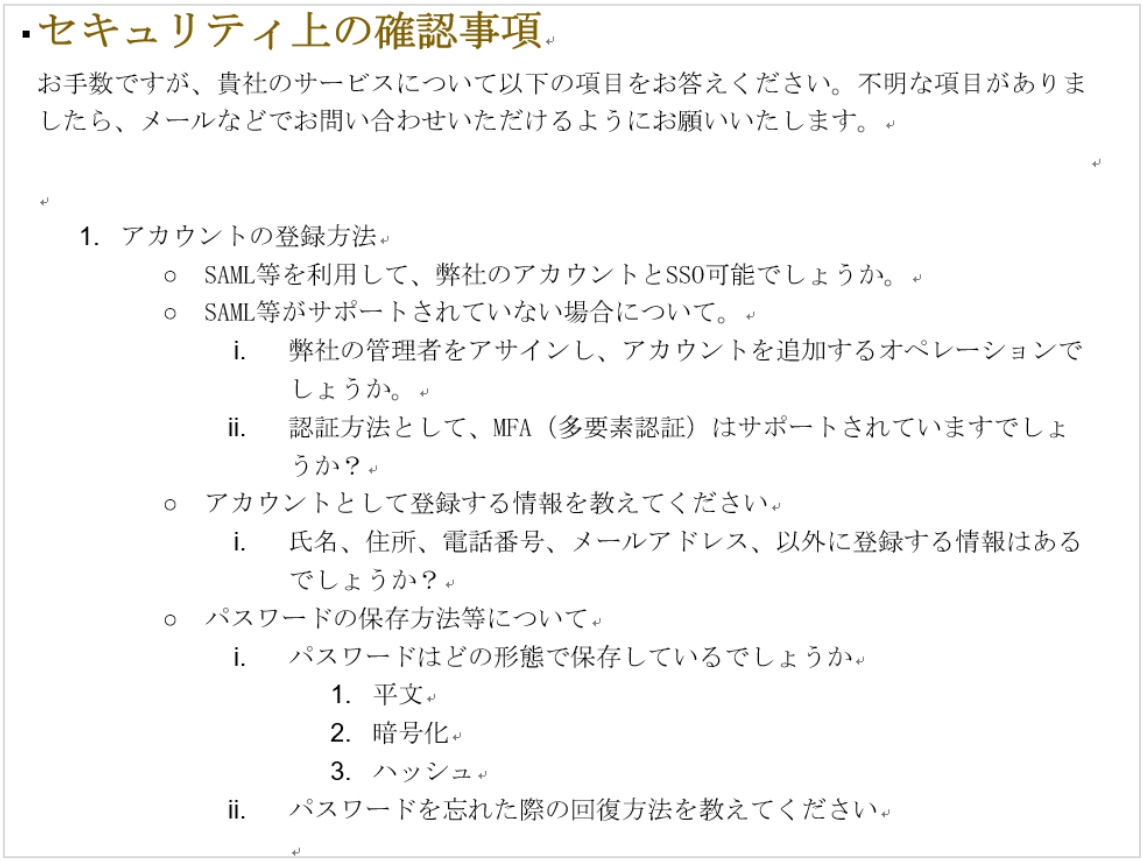


図 2　セキュリティ上の確認事項の例

Free Wi-Fi やホテル・イベント Wi-Fi の利用

Free Wi-Fi や、ホテル、イベント、他社オフィスなどで提供している Wi-Fi の利用は、企業により判断が異なるかもしれませんが、特に Free Wi-Fi についてはポリシーで禁止している企業が多いと思います。一般的な Free Wi-Fi 等の利用に伴うリスクは、以下のものがあります。

Free Wi-Fi 等の利用に伴う一般的なリスク

- 通信の傍受・改竄・リダイレクトが可能
  認証などを含む通信内容の窃取や、トランザクションを改竄が可能
  トネリング、マルウエアのインストールなどにつながる場合もある
- 偽のアクセスポイントの設置が容易
  Free Wi-Fi に限りませんが、偽アクセスポイントの設置が容易で、自動接続を設定している場合、気づかずに偽アクセスポイントに接続している場合があります。

・ Dark hotel[3]のように、施設のインフラへの侵入が行われている場合がある
マルウエアのインストール、クレジットカードの窃取、メール内容の窃取などの危険があります。

一方で、ポリシーで禁止をしていても、実際には利用を完全に止めることは難しい、というのが現状だと思います。特に、海外に出張する際には、通信費用が高額になりやすいこともあり、利用を禁止するだけでは現実的な対策とは言えません。

CISO 支援 WG で、この話題を取り上げたところ、いくつかの対策が提案されたのでご紹介いたします。

・ 会社等の VPN サーバの経由を強制する
特にイントラネットに情報資産が集中している場合に効果的な方法です。
クラウドについても、VPN サーバを経由してインターネットに出ることで、多くの Wi-Fi リスクを避けることができます。一方で設備の用意、維持・運用に費用が掛かる傾向があります。
・ 信頼できる VPN サービスを利用する
VPN サービスを利用することで、PC 等・VPN サーバ間通信の暗号化を担保することができます。このため、暗号化されていない Free Wi-Fi や偽アクセスポイントを経由した場合でも、安全なインターネット利用が可能です。
一方で、VPN サービスやアプリによっては、セキュリティ面、プライバシー面から、信頼できない場合があることから、選定にあたっては注意が必要です[4]。
・ 会社が携帯型の Wi-Fi ルーター（モバイルルーター）を用意する
会社が出張先で利用できる Wi-Fi ルーターを用意する（または費用として認める）ことで、Free Wi-Fi 等の利用を避けるように促します。特に海外への出張の場合に有効だと考えられます。
・ ホテルでは、無線を使わず有線 LAN に限定する
ホテルの設備に侵入されている場合の対策にはなりませんが、偽アクセスポイントのリスクは避けることができます。

---

[3] THE DARKHOTEL APT (Kaspersky)
https://media.kaspersky.com/jp/pdf/pr/Kaspersky-WP-DARKHOTEL-PR-1002.pdf?utm_source=kdaily&utm_medium=blog&utm_campaign=jp_kd_organic&utm_content=link&utm_term=jp_kdaily_organic_link_blog_kd

[4] Facebook の VPN アプリ「Onavo Protect」はプライバシーを保護するどころか機能 OFF 状態でも情報を収集しまくっていると判明
https://gigazine.net/news/20180308-onavo-protect-tracking/

CISO が知らないシステムのセキュリティ対策の評価

CISO やセキュリティ担当者が、知らない・理解していないシステムに対して、セキュリティ上の判断を求められることは少なくありません。むしろ、理解しているシステムの方が少ないことが一般的だと思います。

このような場合の判断の仕方として、事故があった場合を想定し、対策の適切性を評価する方法があります。例えば、事故が起きた際に、迅速に以下の内容を顧客に報告できるのか？という問いかけを、システム開発担当とディスカッションをすることで、自身が理解をしていないシステムについても、具体的な対策をヒアリングし、対策を実装していくことが可能になると考えています。

- 合理的なセキュリティ対策を実施していたこと
- ログなどの分析により被害の範囲が（ある程度）特定できている事
- 事故・事件の原因が（ある程度）わかっている事
- 再発防止策を実施できること

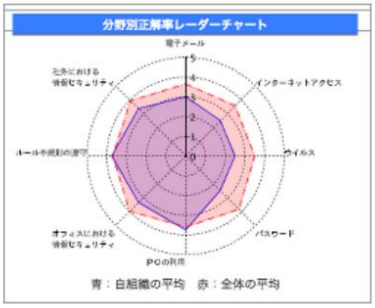
参考にしていただきたい JNSA の主な成果物

1. CISO ハンドブック CISO の業務執行についてまとめたハンドブックで、以下の 4 つのドキュメントで構成されています。 https://www.jnsa.org/result/2018/act_ciso/index.html	CISO ハンドブック CISO ダッシュボード インシデント対応ワークショップ インシデント対応ワークショップ表
2. 2018 年 情報セキュリティインシデントに関する調査報告書 報道された個人情報漏えいインシデントの情報を集計・分析したもので、漏えいした組織の業種、漏えい人数、漏えい原因、漏えい経路などの情報の分類、JO モデル（JNSA Damage Operation Model for Individual Information Leak）を用いた想定損害賠償額の算出しています。 https://www.jnsa.org/result/incident/	
3. JNSA ソリューションガイド セキュリティ製品やサービスをご紹介しているサイトです。 https://www.jnsa.org/JNSASolutionGuide/IndexAction.do	
4. IT 活用促進資金 情報セキュリティ対策要件対応製品リスト JNSA 会員企業が開発・販売・提供しているセキュリティ製品・サービスの中から、IT 活用促進資金のセキュリティ対策要件を満たすと思われるものの一覧です。 https://www.jnsa.org/it_katsuyou/	

5.　情報セキュリティ理解度チェックサイト

この「情報セキュリティ理解度チェック」サイトでは、組織の管理者の方が自組織の社員・職員をユーザ登録し、受講させることで、１人ひとりの受講結果を知ることができます。また、自組織の全体としての情報セキュリティ知識レベルを確認できるだけでなく、さらに同業種の中でのランキングを知ることもでき、自組織の情報セキュリティ知識レベルの客観的な把握が可能になります。

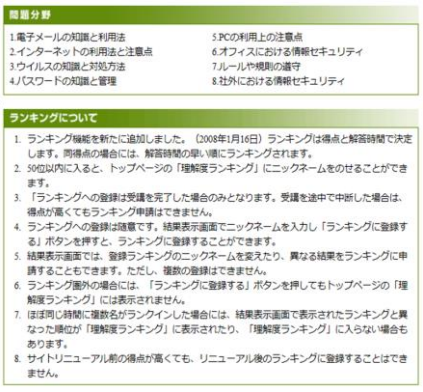
https://slb.jnsa.org/eslb/



6.　情報セキュリティ理解度セルフチェック

情報セキュリティの理解度を確認していただけるよう、情報セキュリティに関する知識を自己診断できるセルフチェックサイトを開設いたしました。このサイトを利用することで、利用者が自分の情報セキュリティの理解度レベルを客観的に把握でき、適切な情報セキュリティ知識を身につけ、セキュリティ上の問題に正しく対応できるようになることを期待しています。

https://slb.jnsa.org/slbm/



7.　JNSA 「サイバーインシデント緊急対応企業一覧」

サイバーインシデントは予期しないタイミングで起こります。また、サイバーインシデントは通常のシステム障害とは異なり、専門知識がないと状態の把握すら困難です。

そのような時に、緊急で対応を請け負ってくれる、頼りになる JNSA 所属企業を取りまとめました。

https://www.jnsa.org/emergency_response/

8.　マイナンバー対応のための情報ポータル（企業向け） すべての民間企業はマイナンバーを取扱うときの業務プロセスや安全管理措置について検討する必要があります。一方で、現実には範囲やゴールを明確にできないまま、手探りで進められているケースも多いかと思います。JNSA ではこうした取り組みを支援すべく、マイナンバーに対応した情報セキュリティ対策の導入や運用に役立つ情報を提供いたします。 https://www.jnsa.org/mynumber/	
9.　その他公開資料 その他、JNSA が公開している資料について、こちらの URL をご覧ください。 https://www.jnsa.org/result/2019.html	
10. JNSA 入会案内 JNSA は、会員を募集しています。こちらの URL をご参考に、ぜひ入会をご検討ください。 https://www.jnsa.org/aboutus/07.html