サイバーセキュリティ対策マネジメントガイドライン

Ver2.0

2020 年 11 月 17 日

特定非営利活動法人　日本セキュリティ監査協会

目　　次

改訂版の序文

本書は 2018 年 1 月 18 日に発行したサイバーセキュリティ対策マネジメントガイドラインの改訂版である。発行して 2 年を経過しており，その間にサイバーセキュリティに関する状況は一層深刻になり，これに呼応するように組織の認識が深まってきた。また，サイバーセキュリティの概念に関わる議論も進展し，対策技術も広がりを見せている。これらの状況に加えて，組織のサイバーセキュリティ対策に対する監査を実施していく動きが加速してきた。このため，サイバーセキュリティ管理基準の策定が待たれるところである。これらのことを踏まえて，最新の動向を反映し，かつ管理基準のベースとなるよう管理策を見直すこととした。見直しに当たって，ガイドラインとしての使いやすさの観点から，ISO/IEC27009 に完全に準拠するよりは，JIS Q 27001 及び JIS Q 27002 の追補版としての体裁とした。

なお，本書の改訂は，下記に示す当協会の専門監査人 WG のメンバーによって行われた。

専門監査人 WG メンバーリスト

リーダ　登玉 晃弘（株式会社富士通ソーシアルサイエンスラボラトリ）

メンバー　岡田 勲　（日本電気株式会社）

河島 君知（エヌ・ティ・ティ・データ先端技術株式会社）

栗田 博司（株式会社日立製作所）

倉谷 秀雄（富士通株式会社）

太田 博之（富士通株式会社）

JASA 編集担当者

永宮 直史　エグゼクティブフェロー

芹川 健二郎　事務局長

序文

本書は，JIS Q 27001:2014 を実装している組織が，その ISMS を生かしサイバーセキュリティ対策を実施するための要求事項ならびに管理策のガイダンスを提供するものである。本規格は ISO/IEC27009：2016 に準拠して，作成されている。

1　適用範囲

本書は，JIS Q 27001:2014 に基づき ISMS を確立し，実施し，維持し，継続的に改善している組織が，サイバーセキュリティのための対策を，ISMS 活動に取り入れ,実施するための要求事項を提供する。

本書が規定する要求事項は，汎用的であり，形態，規模又は性質を問わず，全ての組織に適用できることを意図している。組織が本書への適合を宣言する場合には，4 章から 10 章に規定するいかなる要求事項の除外も認められない。

本書においては，ISMS は確立された情報セキュリティマネジメントシステムに，サイバーセキュリティ対策を追加し統合したマネジメントシステムを指す。

2　引用規格

次に掲げる規格は，本書に引用されることによって，本書の規定の一部を構成する。この引用規格は，その最新版（追補を含む。）を適用する。

JIS Q 27001:2014 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項

JIS Q 27002:2014 情報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範

3　用語及び定義

本書で用いる主な用語及び定義は，JIS Q 27000 による他,以下の用語を用いる。

3.1　サイバーセキュリティ

人々，組織，社会，国をサイバー空間上のリスクから防ぐこと

3.2　サイバーレジリエンス

サイバーセキュリティに対する複雑かつ変化する環境下での組織の適応できる能力

注記　レジリエンスは，中断・阻害を引き起こすリスクを運用管理する組織の力である。

（JIS Q 22300）

サイバーセキュリティ対策マネジメントガイドライン JIS_Q_27001：2014 追記事項

11 サイバーセキュリティへの対応

ISMS の中で，サイバーセキュリティに対応する組織は，箇条 1～箇条 10 の要求事項に加えて，本章の内容を含めて対応しなければならない。

11.1 サイバーセキュリティ対応体制の整備

トップマネジメントは，サイバー攻撃による被害の発生を最小化するために，サイバーセキュリティ対応体制を整備することが望ましい。サイバーセキュリティ対応体制は，次の構成要素を含め，各体制の役割と責任，及び各体制間の連携手段，連携の機会を明確にすることが望ましい。

(a) CRO（事業リスク管理責任者）
事業リスクに関する組織全体の意思決定者

(b) CISO（情報セキュリティ管理責任者）
情報セキュリティ全般の意思決定者

(c) 組織全体の情報セキュリティ担当者（サイバーセキュリティ対策責任者）
サイバーセキュリティ対策に関する指揮監督者

(d) サイバー攻撃の検出，分析，対応策のアドバイス等を行う組織
（例：SOC（Security Operation Center））
注）本組織は，自組織内，専門業者への委託，どちらでも構わない。

(e) 各部門の情報セキュリティ担当者

(f) 内部／外部組織との連携窓口

(g) 外部の情報セキュリティ専門家

また，サイバーセキュリティ対応体制は，サイバー攻撃の発生を想定した訓練を定期的に実施し，必要に応じて見直しを実施し，最新の状態を維持することが望ましい。

11.2 サイバーセキュリティに関する文書化した情報

組織は，サイバー攻撃による被害の発生を最小化するために，次の事項を含むサイバーセキュリティに関する文書化した情報を管理しなければならない。

(a) 11.1 に定める関係者間の時系列での連携がわかる対応フロー

(b) (a)の対応フローを補足する手順

(c) サイバーセキュリティインシデントの定義

(d) サイバーセキュリティインシデントの重大性を判定する判断基準

(e) 利用者・システム主管部門・サイバー攻撃の検出，分析，対応策のアドバイス等を行う組織からサイバーセキュリティ対策責任者への通報フォーム

(f) 外部（警察，セキュリティ専門団体等）からの依頼に対する情報開示の基準

(g) 内部／外部組織との連携窓口

11.3 サイバーセキュリティリスク評価

サイバーセキュリティリスクは，時々刻々と変化することを鑑み，サイバー攻撃を検知した際に，サイバーセキュリティ対策責任者はサイバーセキュリティリスクを評価し，トップマネジメントに報告し，トップマネジメントの指示を仰ぐことが望ましい。その際には，予め報告基準を定めておかなければならない。

また，定期的に過去に発生したサイバーセキュリティインシデントの傾向や発生時の対処を分析し，継続的に改善することが望ましい。

11.4 善意の第三者への悪影響の防止

組織は，不正アクセスによる善意の第三者への悪影響を防止するために，利害関係者に善意の第三者を加え，それを特定し，情報セキュリティ目的に善意の第三者の保護を加えなければならない。

11.5 サイバーセキュリティに関するコミュニケーション

組織は，7.4 に加えて，サイバーセキュリティに関する内部及び外部のコミュニケーションとして，以下を予め決定しておかなければならない。

(a) 利害関係者とのサイバーセキュリティに関する情報の共有と調整方法
(b) サイバーセキュリティが侵害された場合の外部への公表方法
(c) サイバーセキュリティインシデントによる利害関係者とのコミュニケーションの方法

サイバーセキュリティ対策マネジメントガイドライン JIS_Q_27002：2014 追記事項

19 サイバーセキュリティ管理策

19.1 CSIRT 機能の確立

目的 サイバーセキュリティリスクに対応するための管理体制を確立することが望ましい。

19.1.1 サイバーセキュリティ管理体制の確立

管理策

組織は，サイバーセキュリティとしてセキュリティインシデント対応するために，CSIRT を構築し運用することが望ましい。

実施の手引

サイバーセキュリティ管理体制の構築から運用までの手順は以下とすることが望ましい。

a） CSIRT 構築に向けてトップマネジメントから理解を得る

1） 取り巻く環境の変化などから組織全体としてのインシデント対応体制整備の必要性を確認。

2） サイバーセキュリティのインシデント対応体制に求める機能の確認。

3） サイバーセキュリティのインシデント対応として組織内 CSIRT 構築の必要性，メリットの理解。

b） 組織内の現状を把握する

1） 守るべき情報資産と脅威，リスクの把握

2） 既存のインシデント対応体制，環境，リソース，対応内容の把握

3） 既存のセキュリティポリシーや規定，セキュリティ関連文書の把握

c） 組織内 CSIRT 構築活動のためのチームを結成して構築を進める

1） 構築活動を行う人を選定しチームを結成

2） チームメンバーのうち1名をリーダとし，活動を推進する

注）推進リーダはサイバーセキュリティに関する力量を考慮して決定することが望ましい。

d） 組織内 CSIRT を設計し，その活動計画を立てる

1） 対象となるインシデントを定義する

組織の事業内容，規模，事業に対する脅威やリスクによって定義する。

2） 組織内インシデント対応活動内容を定義する

例）活動には事前対応，事中対応，事後対応，セキュリティ品質マネジメントに関する活動がある。

3） ミッションステートメントを決める

目標，目的，何をはたすべきかを明確にして決める。

4） サービス対象を決める

5） サービスの分類を明確にする

例）

・事後対応型のサービス:

インシデントの被害局限化を目的とした，インシデントやインシデントに関連する事象への対応を行うためのサービス，アラートと警告，インシデントの分析，インシデント対応，脆弱性の分析などがある。

・事前対応型サービス

インシデントの発生抑制を目的とした，インシデントやセキュリティイベントの検知や，発生の可能を減少させるための活動，告知，技術動向監視，セキュリティ監査または審査，セキュリティツールの開発，セキュリティ関連情報の提供などがある。

・セキュリティ品質マネジメントに関するサービス

組織のセキュリティ品質を向上させることを目的とした活動。

CSIRT としての視点や専門知識での見識を提供し，マネジメント事務局と連携することにより，効果的な活動を実施できる。間接的にインシデントの発生抑制をすることが可能。リスク分析，セキュリティ意識向上，教育/トレーニングなどがある。

6) 組織内の CSIRT の位置づけを決める

CSIRT の位置，役割，他組織との相互関係を決める。

7) 他 CSIRT との関係を決める

他 CSIRT との協力及び連携内容を明確する。

8) 文書化する

1)～7)の項目を整理し，CSIRT 体制及び役割図，CSIRT 記述書としてまとめる。

e) 必要な予算やリソースを確保し環境を整備する

1) 組織内 CSIRT の設立，運営に必要な予算を確保する

2) 組織内 CSIRT に必要な要員を確保する

3) 組織内 CSIRT の運営に必要な設備等(インフラ，セキュリティツール等)を準備する

4) 組織内，組織外からのインシデントに関する報告や連絡を受ける窓口を設置する

5) 活動に利用する機器のメンテナンス及び正常性の確認を適切に実施する

但し，組織の状況によって確認内容及び方法は定めてよい。

f) 組織内 CSIRT に関連する規則類を整備する

1) ポリシーの整備

インシデント対応に関するポリシー，情報セキュリティに関するポリシーを整備する。

なお，インシデント対応に関するポリシーには，インシデント発生時から解決及び再発防止策までの一連のインシデントハンドリング(検知/連絡受付，トリアージ，インシデントレスポンス，報告/情報公開)のポリシーも含まれる。

2) 手順の整備

インシデント対応に関する手順はインシデント対応マニュアルとして作成し，併せて情報セキュリティ活動に関する手順を見直す。

なお，インシデント対応に関する手順には，インシデントハンドリング(検知/連絡受付，トリアージ，インシデントレスポンス，報告/情報公開)の手順も含まれる。

また，インシデント対応に関する手順に OODA ループ[1]を組み込むことを考慮する。

[1] OODA ループ：「観察（Observe）」「仮説構築（Orient）」「意思決定（Decide）」「実行（Act）」の 4 つの頭文字をとった意思決定方法。PDCA は工程が定義されたプロセスの改善に適している一方、OODA（ウーダ）は工程が不明確な場合に効果的であるといわれる。

g) CSIRT 要員(スタッフ)への教育を実施する

1) f)項の各ポリシー，手順についての教育を実施する

2) e)項の 3)の必要な設備に対しての適切な利用方法を含めて教育を実施する

3) 各要員の役割に応じて教育を実施する

4) インシデント対応の事前訓練を実施する

5) その他，業務に必要な知識習得を行う

h) CSIRT の告知と活動を開始する

1) 組織内に CSIRT に関して告知する

例)サービス対象，活動内容，情報共有及び連携活動する関連部署及び外部組織，報告手段など

2) 組織内からのフィードバックを反映する

例)告知内容についての意見，インシデント対応の実施した結果からのフィードバックなど

3) PDCA サイクルでフィードバック結果や活動内容をもとに改善を図る

i) CSIRT 活動中における情報管理は適切に行う

CSIRT はインシデント対応に関するデータ，情報を安全かつ適切に取り扱う。

1) 情報分類

機密情報と公開情報を適切に分類する。

2) 情報の入手/開示

情報保護の観点から適切な方法で入手及び開示する。

3) 情報の保護

情報の保管場所，アクセスについて適切に管理すること。

4) 情報の保持

情報の保持期間を定める，また適切にバックアップを行う。

5) 情報の廃棄

情報の廃棄方法を定め，適切に廃棄すること。

6) e)項の 3)の設備について適切に利用する

関連情報

＊インシデント対応マニュアルの記述例

下記の項目をまとめてインシデント対応マニュアルとして作成し運用することが望ましい。

a) 組織にとってのインデントの定義，重要度レベル，責任，担当を明確にする

b) インシデント対応する人及び組織の体制及び役割を明確にする

c) インシデント報告窓口を設置し，関係者に周知する

d) インシデント対応に必要な連絡先を確保する

e) インシデント報告内容，基準を明確にする

f) 検知/連絡受付をフローなどにして明確にする

g) トリアージをフローなどにして明確にする

h) インシデントレスポンスをフローなどにして明確にする

i) 組織の規則，規程類を確認しフローに反映する
j) 必要に応じて手順や内容を確認，チェックするシートを作成する

＊インシデントハンドリングの例
インシデント発生から解決までのインシデントハンドリングを行う。
インシデントハンドリングとは，インシデントの検知と連絡受付，トリアージ，インシデントレスポンス，報告と情報公開の一連の処理を示す。
a) インシデントの検知と連絡受付
b) トリアージ
インシデント内容から対応すべきインシデントか切り分け，対応の優先順位，インシデント対応する担当を検討する。
c) インシデントレスポンス
・事象の分析から対処を行う
・インシデント発生被害の抑制に向けて，抑制措置の手段，抑制措置による事業への影響，期間を明確にして進める
・常にトップマネジメントと情報共有して対処を進める
・経験したインシデントかそうでないかを判断，過去に経験したインシデントの場合は，過去の対応ノウハウを活用して対処する
・過去に経験したことのないインシデントの場合は，過去のインシデント対応経験者の意見や外部組織含めて他組織における類似例の情報共有，連携して対処する
d) インシデンントに関する報告と情報公開
・外部組織に報告する内容を整理し，必要に応じて告知する
・告知の範囲（誰に，どの範囲を）を明確する
・告知の方法，手段について妥当性を検討して対応する
（自社 Web サイト，新聞やメディアなど）
・インシデントの発見者，被害者などから必要な情報を取得できるよう，報告項目例をテンプレートとして公開し，インシデント発見者及び被害者は，そのテンプレートをもとに報告できるようにする
e) インシデント事後対応
・インシデント復旧後のモニタリング，他に影響がないか確認を実施する
・同様なインシデントの再発防止策を検討し教育などの対策を実施する

19.1.2 サイバーセキュリティインシデントの検知

管理策

コンピュータセキュリティインシデントを検知するために，組織にあった検知方法（発見者からの連絡受付，情報収集，機器の利用など）をもとに早期発見に備えることが望ましい。

実施の手引

a) 組織内／外の被害者，発見者からの連絡受付及び情報共有する

1) 被害者，発見者からの連絡を速やかに受け付ける
2) 被害者，発見者からの連絡内容については，インシデント対応マニュアルなどをもとにヒアリングを行い，事象の確認及び必要な情報の入手につとめる
3) 入手した情報の内容は速やかに関係者と共有する

b) サイバーセキュリティに関する情報収集を行う

1) 組織が定めた安全を脅かす脅威，脆弱性をもとにインシデント顕在化の兆候となるべき情報取得につとめる
2) 組織の状況及び必要に応じて組織外のコミュニティとの情報交換を行う
3) 収集した情報からインシデント発見，検知に活用する

c) 組織内の機器を有効に活用する

1) ネットワーク内のトラフィックの変化を見る
2) ネットワーク内の機器のログを有効に活用する

・見るべきログの把握

組織で定義したインシデント内容を検知するために，ネットワーク内の機器からどのような情報（ログ）が取得できるか事前に把握する。

また，取得する情報（ログ）については定常的な状態を把握しておく。

・ログの定期的な確認

定常的な状態とは異なるログが出力されていないかを確認する。

・外部からの情報を起点とするログ確認

提供された情報をもとに，その情報に一致するログが存在しないかを確認する。

・ログの適切な保管

インシデントの内容の全体像を正しく分析するために，ログは長期間保存しておく。

保存期間は1年以上とすることが望ましい。

・機器のクロック同期

NTP などを利用してネットワーク内の機器のクロックを同期させ，各機器から取得できるログのタイムスタンプを合わせておく。

・ログの一括管理

ネットワーク内の機器からログの収集及びログを一括管理できるツールやシステムの導入することが望ましい。

3) システムなどの振る舞いを検証する
・外部からの通信や入手したデータの検証
・端末上の挙動の検出と分析
4) 組織の状況，構成に応じてネットワーク内の機器のメンテンスを適切に行う
・ソフトウェア，ファームウェア，各種運用に関するデータのアップデート
・定期的な動作チェック

d) 組織にあった運用を行う
1) 組織で定義したインシデントの内容に合った検知方法を明確にして検知に備える
例えば，1～3 項の検知方法内容から，組織で実施できる方法を選択し，且つ組み合わせて活用する。
2) ログの収集や通信内容の監視については，組織の状況に応じて監視サービスなどを利用する事も検討する

関連情報

＊サイバー攻撃における，ログで検知可能な攻撃内容及びログ取得機器の例
サイバー攻撃を攻撃段階毎に分解すると，例えば偵察，武器化，デリバリ，エクスポロイト，インストール，C&C，目的の実行に分けられる。
そのうち，デリバリ段階から目的の実行の段階までについて，ログ取得機器の事例を以下に示す。

a) デリバリ
・攻撃内容　：攻撃者によるマルウェア添付メールの送信
攻撃者によるマルウェア設置サイトへの誘導メールの送信と誘導
・ログ取得機器：メールサーバ，Web プロキシサーバ
b) エクスプロイト
・攻撃内容　：コールバック（Web プロキシサーバを介さない外部への通信，HTTP，HTTPS 等のプロトコルによる外部への通信）
・ログ取得機器：Firewall，DNS サーバ，Web プロキシサーバ
c) C&C
・攻撃内容　：コールバック（Web プロキシサーバを介さない外部への通信，HTTP，HTTPS 等のプロトコルによる外部への通信），感染活動（脆弱な PC や内部サーバの探索など），ファイルサーバなどへのアクセスや権限の奪取
・ログ取得機器：Firewall，DNS サーバ，Web プロキシサーバ，AD ログ
d) 目的の実行
・攻撃内容　：コールバック（Web プロキシサーバを介さない外部への通信，HTTP，HTTPS 等のプロトコルによる外部への通信），機密情報持ち出し（メールサーバ経由）
・ログ取得機器：Firewall，DNS サーバ，Web プロキシサーバ，メールサーバ

＊用語 サイバー攻撃を段階毎に分けた場合の段階例

a) 偵察
・インターネットなどから組織や人物を調査し，対象組織に関する情報を取得する
b) 武器化
・マルウェアなどサイバー攻撃用の武器を作成する
c) デリバリ
・なりすましメール（マルウエアを添付）を送付する
・なりすましメール（マルウエア設置サイトに誘導）を送付し，ユーザにクリックさせるように誘導する
d) エクスプロイト
・ユーザにマルウェア添付ファイルを実行させる
・ユーザをマルウェア設置サイトに誘導し，脆弱性を使用したエクスプロイトコードを実行させる
e) インストール
・エクスプロイトの成功により，標的(PC)がマルウェアに感染する
f) C&C
・マルウェアにより C&C サーバと通信させ，感染 PC を遠隔操作し，追加のマルウェアやツールなどをダウンロードさせることで，感染を拡大する，あるいは内部情報を探索する
g)目的の実行
・探し出した内部情報を，加工（圧縮や暗号化等）した後，情報を持ち出す

＊事例 1:サイバー攻撃に応じて検知する機器の例
〈マルウェア感染〉
・アンチウイルスソフト
・SIEM などのログ分析ツール
〈標的型攻撃〉
・アンチウイルスソフト
・IDS/IPS 機器
・SIEM などのログ分析ツール
〈SQL インジェクションなど Web サーバへの攻撃〉
・IDS/IPS 機器
・ファイアウォール
・Web アプリケーションファイアウォール
・SIEM などログ分析ツール

＊事例 2:各ネットワーク内機器における検知例
〈メールサーバ〉
a) 攻撃の発見に利用できる代表的なログ項目

1）メールクライアントで表示される表記名，送信者アドレス，実際のメール送信者アドレス
2）添付ファイル名

b）攻撃とそれを発見するための手法例

1）From フィールドの表示名偽装の場合

・攻撃行為：送信元を偽装したメールを送り付けて，油断させて開かせる
・手掛かり ：受信メールの送信者情報の不自然な設定
例：エンベロープとメールヘッダのメールアドレスが異なるものを抽出

2）実行ファイル添付

・攻撃行為：マルウェアである実行ファイルを添付したメールを送り付ける
・手掛かり ：実行ファイル形式が添付されたメール
例：ファイル名の拡張子が実行形式であるものを抽出

〈Firewall〉

a）攻撃の発見に利用できる代表的なログ項目

1）送信元アドレス，送信先アドレス，送信先ポート

b）攻撃とそれを発見するための手法の例

1）組織内から組織外への不正な通信の場合

・攻撃行為：Web プロキシサーバを経由せずに，ボットに感染した PC が C&C サーバに，
または，ダウンローダに感染した PC がダウンロードサイトに通信を試みる
・手掛かり ：Web プロキシを経由せずに直接インターネットへの通信を試みる通信を Firewal のログから検知する
例：組織内から組織外へ通信で，かつ許可されていない通信を抽出

2）異なるセグメントに収容された PC 間の不正な通信の場合

・攻撃行為：マルウェアに感染した PC が，他の PC 等に対して感染を広げるための通信を行う
・手掛かり ：セグメント間で許可されていない通信を，Firewall の通信ログから検知する
例：組織内から組織内へ通信で，かつ許可されていない通信を抽出

〈Web プロキシ〉

a）攻撃の発見に利用できる代表的なログ項目

1）URL アドレス，送信先サイトのポート，メソッド，アクセス時間

b）攻撃とそれを発見するための手法の例

1）不審な送信先への通信の場合

・攻撃行為：マルウェアに感染した PC が C&C サーバやダウンロードサイトへの通信を試みる
・手掛かり ：高度サイバー攻撃に関連する情報（IP アドレスやドメインなど）で検索

2）CONNECT メソッドで 80，443 以外のポートへ通信の場合

0，443 番ポート以外の CONNECT メソッドの通信を抽出
・攻撃行為：HTTP や HTTPS 通信の偽装を行い，組織外との通信を試みる
・手掛かり ：80，443 番ポート以外の CONNECT メソッドの通信を抽出

3) 標準利用以外の User Agent による通信
・攻撃行為：マルウェアに感染した PC が C&C サーバやダウンロードサイトへの通信を試みる
・手掛かり ：組織内で標準利用しているブラウザの User Agent と異なる User Agent による通信を検索

4) 定期的に発生する HTTP 通信
・攻撃行為：ボットに感染した PC は C&C サーバへの通信を定期的に行い，情報の取得やコントロールの受信を試みる
・手掛かり ：業務利用しない URL を日ごとに集計。不自然なアクセスが続いているものを抽出

5) 業務時間外に発生する HTTP 通信
・攻撃行為：マルウェアに感染した PC は，変則的な時間帯にも，C&C サーバ等へ通信を試みる
・手掛かり ：業務時間外の時間帯でシステムメンテナンス利用を除いたものを抽出不自然なアクセスがないか確認

6) 大量の HTTP 通信
・攻撃行為：マルウェアに感染した PC が C&C サーバやアップロードサイトへの通信を試みる
・手掛かり ：同一の送信先に対する POST メソッド，それに続く CONNECT メソッドを抽出し，データ量の合計値が異常に大きなものを確認

〈DNS サーバ〉

a) 攻撃の発見に利用できる代表的なログ項目

1) クエリログ(PC などのクライアントが DNS サーバにホスト名の解決を行ったクエリ)，Src(ホスト名の解決を行ったクエリが送られた送信元ホストの IP アドレス)

b) 攻撃とそれを発見するための手法の例

1) 不審な送信先への通信
・攻撃行為：マルウェアに感染した PC が C&C サーバやダウンロードサイトへの通信を試みる
・手掛かり ：高度サイバー攻撃に関連する情報（URL やドメインなど）で検索

〈認証サーバ〉

a) 攻撃の発見に利用できる代表的なログ項目

1) セキュリティログ（イベントログ）資格認証，Kerberos 認証，特殊なログオンの要求と結果

b) 攻撃とそれを発見するための手法の例

1) 管理者アカウントに関連したイベントの調査の場合
・攻撃行為：マルウェアに感染した PC から，目的の情報を得るため，特権が必要な操作を試みる
・手掛かり ：管理者が通常使用する IP アドレスと異なる IP アドレスからの管理者権限要求など

2) 通常の運用では発生しないようなイベント
・攻撃行為：侵入の痕跡を消すために，ログの消去を試みる
・手掛かり ：通常の運用では発生しない特殊な操作要求を確認

19.2 事業インパクトの緩和

目的 サイバーセキュリティインシデントによる事業インパクトを緩和するため。

19.2.1 事業インパクトの緩和

管理策

サイバーセキュリティインシデントによる事業インパクトを緩和するために，全社リスク管理体制におけるサイバーセキュリティリスクの位置づけを明確にし，事業の継続性を目的としたサイバーレジリエンスや事業継続計画(BCP)と連携することが望ましい。

実施の手引

a) 組織横断的リスク管理体制との連携

サイバーセキュリティインシデントにより，社会に対して損害を与えてしまった場合には経営責任や法的責任が問われる可能性がある。そのため情報システム部門などの特定部門だけではなく，組織横断的にサイバーセキュリティリスクを議論することが望ましい。例えば，リスク管理委員会などの組織横断的リスク管理体制や BCP との連携を整備することが望ましい。整備するポイントは以下となる。

1) 任命された担当幹部(CISO など)は，組織内に設置された経営リスクに関する委員会に参加する
2) 経営リスクに関する委員会のテーマの一つにサイバーセキュリティリスクを盛り込み，CISO が報告・審議を行う
    i. 特定した守るべき情報に対するサイバー攻撃の脅威，脆弱性を識別し，経営戦略を踏まえたサイバーリスクとして把握する。リスクの影響の度合いに従ってリスク対応計画を策定し，委員会で報告する
    ii. 新たなサイバーセキュリティリスクの発見等により追加対処が必要な場合には，対応計画を修正して委員会で報告する
    iii. サイバーセキュリティリスク管理に関する KPI[2]を定め，委員会で状況をトップマネジメントに報告する
3) インシデント発生などの緊急時において，組織横断的リスク管理体制と連携する対応体制を構築する
    i. 緊急連絡網，組織外を含む情報開示の通知先一覧を組織横断的リスク管理の観点から整備し，対応に従事するメンバーと共有する
    ii. 初動対応時の業務影響を検討し，組織横断的リスク管理体制と速やかに協力できるよう予め取り決めをしておく
    iii. トップマネジメントが責任をもって組織の内外へ説明ができるように，組織横断的リスク管理体制に従い，トップマネジメントへの報告ルート，公表すべき内容やタイミングなどを定める
4) インシデントにより業務停止などに至った場合の復旧目標計画や手順書，体制を，組織横断的 BCP と整合を取って定める
    i. 担当幹部(CISO など)は，組織内における BCP の整備計画を適時共有できる体制を構築する
    ii. BCP の整備計画がある場合には，整合性の確保のための検討を行い，BCP と共通の実施手順を整備する

[2] KPI：Key Performance Indicator（重要業績評価指標）。組織目標達成度を定量的に表す指標。

iii. BCP とサイバーセキュリティ関係規定が定める要求事項との違いなどにより，実施の是非の判断が困難な場合には，関係者に連絡するとともに，担当幹部にその旨を報告して指示を得る

b) サイバーレジリエンス

サイバー攻撃を受けたとしても，早期に検知・対処して ICT 環境を復元し，事業への影響を最小限にすることで，通常の業務を再開できるようにするサイバーレジリエンスへの取り組みが望ましい。

サイバーレジリエンスの確保を実現するための技術アプローチを以下に示す。要件に従い，これらの技術を組み合わせて実装することが望ましい。

1) アジャイルにリスクを管理するための適応的対応
   - 動的再構成，動的リソース割り当て，適応的管理
2) 幅広い属性や行動を継続的に監視・分析するための分析モニタリング
   - 監視とダメージ評価，センサー融合と分析，フォレンジックと行動分析
3) 保護メカニズムが設定された通りに効果的に動作することを保証するための協調的保護
   - 調整された多層防御，一貫性分析，オーケストレーション，セルフチャレンジ
4) 脅威を踏まえて，ミッションや事業遂行の継続能力の現状を，構築および維持するためのコンテキスト認識
   - 動的なリソース認識，動的な脅威認識，ミッションの依存関係とステータス
5) 攻撃者をミスリードし，混乱させて，重要な資産を隠蔽したり，密かに汚染した情報を与えたりする欺き手法
   - 難読化，偽情報，誤った方向付け，汚染
6) 一般的な脆弱性を悪用する脅威を最小限に抑えるために，異なったモジュールを組み合わせる多様性
   - アーキテクチャの多様性，設計の多様性，ソフトウェア実装の多様性，情報の多様性，通信手段の多様性，サプライチェーンの多様性
7) 機能やシステムリソースを動的に再配置するための動的ポジショニング
   - センサーの機能的再配置，IT リソースの機能移転，アセットのモビリティ，フラグメンテーション，機能分散
8) 必要となるときだけ，もしくは，限られた時間だけリソースを生成・維持するための非永続性
   - 非永続情報，非永続サービス，非永続的な接続
9) ユーザやシステム要素の属性や環境要因に基づいて特権を制限
   - 信頼ベースの権限管理，属性ベースの使用制限，動的な特権
10) リスクを低減するために現在の組織ミッションやビジネス機能に応じてシステムリソースを再調整
   - 目的化，オフロード，制限，置き換え，専門化
11) 重要リソースについては複数のインスタンスを準備する冗長化
   - バックアップの保護と復元，余剰能力の準備，復元
12) 重要度と信頼性に基づいてシステム要素を分割
   - 定義済みセグメンテーション，動的セグメンテーションと隔離

13) 重要なシステム要素が破綻していないことを実証する整合性
- 整合性チェック，出所追跡，動作検証

14) ランダムもしくは予測不能な変更を加える予測不能性
- 一時的な予測不能性，文脈上の予測不能性

●参考文献

・ログを活用した高度サイバー攻撃（標的型攻撃）の早期発見と分析 JPCERT/CC
・高度サイバー攻撃への対処におけるログの活用と分析方法 JPCERT/CC
・高度サイバー攻撃（APT）への備えと対応ガイド JPCERT/CC
・コンピュータセキュリティログ管理ガイド NIST SP800-92

・経済産業省 サイバーセキュリティ経営ガイドライン
・IPA サイバーセキュリティ経営ガイドライン 解説書 Ver.1.0
・NIST SP800-160 Vol.2 Developing Cyber Resilient Systems: A Systems Security Engineering Approach