重要インフラ・サイバーセキュリティ新ガイドライン 2026

パブリックコメント結果を踏まえた「経営・法務・実務」の読み方

2026年9月11日 確定版

弁護士法人三宅法律事務所
弁護士　渡邉雅之

今日の結論 - まず5点

1 経営課題になった

「IT部門のセキュリティ」ではなく、任務保証・経営リスク・取締役責任の問題。

2 対象は“外”まで広がる

クラウド、委託先、サプライチェーン、IT/OT、海外拠点まで一体管理。

3 防ぐだけでは足りない

侵入・停止を前提に、検知・対応・復旧・BCPまで含むレジリエンスを要求。

4 AIで時間軸が変わる

脆弱性の発見から悪用まで短縮。優先順位付け、迅速パッチ、代替策が重要。

5 法務の出番が増える

CISO任命、契約条項、報告・公表、取締役会議事録、リスク受容の証跡が実務ポイント。

【CISO】Chief Information Security Officer ／ 最高情報セキュリティ責任者

組織のサイバーセキュリティに最終的な責任を負う役員級の責任者。方針の策定、資源配分、インシデント時の意思決定を統括する。本ガイドラインは、①経営層の責任において任命する、②CIO等との兼務ではなく専任者とすることを検討する、③組織トップと直接コミュニケーションできる位置づけが望ましい、としており、その任命手続は会社法上の論点となる（p.11〜12で詳述）。

制度は「3階建て」で読む

① 重要インフラ統一基準

国が分野横断で示す統一的な基準（2026年10月1日施行予定）

↓

② 安全基準等策定ガイドライン

所管省庁・業界団体等が「安全基準等」を作る際の詳細な参照文書

↓

③ 分野別の安全基準等
→ 各社の内規・運用

強制基準／推奨基準・ガイドライン／業界標準／事業者の内規へ具体化

実務の注意：ガイドラインを「直接の一律義務」と読むのではなく、各分野の安全基準等へどう落ちるかを追う

誰に、どの基準が適用されるのか

重要インフラ15分野と所管省庁

金融庁	金融
総務省	情報通信／地方公共団体
厚生労働省	医療
経済産業省	電力／ガス／化学／クレジット／石油
国土交通省	航空／空港／鉄道／水道／物流／港湾

・重要インフラ事業者等＝基本法12条2項3号の重要社会基盤事業者等（事業者＋その組織する団体＋地方公共団体）

・重要インフラサービス＝影響度を考慮し、特に防護すべきとして分野ごとに定めるもの（別紙2）

・重要システム＝事業者等ごとに定めるもの。範囲を過度に狭く設定するおそれがパブコメで指摘された（意見No.29）

「安全基準等」の4類型と法的性質

① 強制基準

関係法令に基づき政府機関が定める

法令上の義務。違反には業法上の監督措置

② 推奨基準・ガイドライン

関係法令に準じて政府機関が定める

行政指導の基礎。善管注意義務の判断要素となり得る

③ 業界標準・ガイドライン

業界団体等が業界横断的に定める

自主規制。取引条件・契約を通じて実効性を確保

④ 内規

事業者自らが定める

内部統制システムの一部。取締役会決議事項との接続

実務：本ガイドラインは所管省庁等向けの参照文書。自社を拘束するのは、①〜④のどれとして落ちてくるかで決まる。

なぜ2026年に大きく変わったのか

旧制度の課題

具体的・統一的な評価基準が乏しく、分野・事業者によって取組水準にばらつき。

新制度の狙い

分野横断の共通ベースラインを置き、政府側の評価・改善サイクルも強化。

→「自主的な取組」中心から、より“基準・評価・改善”を意識する時代へ

ガイドラインの読み方：「講ずべき」と「望ましい」

講ずべき対策事項

分野・事業者横断で講ずべきベースライン。

所管省庁等が安全基準等を策定する際の中核。

「解説」は対応方法を一律に固定するものではないが、実務の具体化に重要。

講ずることが望ましい対策事項

直ちに一律実施が難しいが、可能な範囲で実施が望まれる上積み。

高リスク分野、コスト・人材、OT固有事情、先進技術などを想定。

リスクベースで水準を引き上げるための“次の一手”。

法務的には、ラベルだけで「任意／義務」を決め打ちしない。分野別基準・契約・内部統制・事故後の説明責任まで見て評価する。

163頁を1枚で：6つのレイヤー

OVERVIEW

2 組織統治

経営方針、責任・権限、CISO、監査、開示、サプライチェーン

3 識別

資産・脅威・脆弱性、リスクアセスメント、対応計画

4 防御

認証、教育、データ、バックアップ、開発、ネットワーク、クラウド

5 検知

監視・分析体制、継続監視、事象分析

6 対応・復旧

BCP、インシデント管理、報告・軽減・復旧、危機管理

7 技術・脅威

ランサム、AIシステム、高性能AI悪用、PQC移行

ポイント：NIST CSF型の流れに「組織統治」と「技術・脅威の動向」が強く乗っている

核心は「任務保証」- 守るのはシステムではなくサービス

GOVERN

任務
社会に対して
何を提供するか

→

最低水準
停止しても
守るサービス範囲

→

重要業務・資源
人・設備・IT/OT・
データ・委託先

→

リスク
何が任務遂行を
不確かにするか

→

対策・復旧
許容水準まで低減し
早期に回復

経営会議での問い

「どのサーバが重要か？」ではなく、「最低限、何時間以内に、どのサービスをどこまで戻す必要があるか？」から始める。

NCO ガイドライン p.4-5, p.10

「完全防御」から「レジリエンス」へ

GOVERN

事前

識別・防御

侵入確率を下げる
被害範囲を限定する

発生

検知・判断

早期発見
経営判断につなぐ

直後

対応・封じ込め

拡大を止める
証拠を残す

復旧

復旧・改善

重要サービスから戻す
再発防止へ

“侵入されたら失敗”ではない。重大サービスの影響を許容範囲に抑えることが成功条件。

経営層の責任を明記 - サイバーは会社法の問題でもある

GOVERN

ガイドラインの明示

サイバーセキュリティ対策は企業の存続の鍵となり得る重要な経営課題。

体制が規模・業務内容に照らして不十分で損害が生じた場合、善管注意義務違反・任務懈怠等に基づく責任を問われ得る。

実務への翻訳

取締役会・経営会議で
①任務とリスク許容度
②CISO・責任分界
③予算・人材
④重大リスク受容
⑤BCP・演習結果
を“意思決定の記録”として残す。

事故後に問われるのは「侵入されたか」だけでなく、「合理的なプロセスで決め、見直していたか」。

NCO ガイドライン p.4-5, 18-20

CISO任命：ガイドラインが会社法まで踏み込んだ

GOVERN

原則となるメッセージ

・CISO等は経営層の責任で任命
・CIO等との兼務ではなく、専任者とすることを検討
・組織トップと直接コミュニケーションできる位置づけが望ましい
・権限を定期レビュー

会社法上の論点

取締役会設置会社では、CISO等が通常「重要な使用人」に当たる場合、原則として取締役会決議が必要との整理。

機関設計別の整理は次頁のとおり。

実務：肩書を置くだけでなく、任命権限・職務権限・報告経路・牽制機能を規程と議事録で整える。

NCO ガイドライン p.23-24

CISO任命の会社法上の手続 — 機関設計別

GOVERN

前提：CISO等の任命は、通常「重要な使用人の選任」（会社法362条4項3号）に該当する

監査役（会）設置会社	原則として取締役会で決定しなければならない	**362条4項柱書・3号**
監査等委員会設置会社	原則は取締役会決定。ただし取締役の過半数が社外取締役の場合、又は定款の定めがある場合は担当取締役に委任可	**399条の13第4項3号／同5項柱書本文／同6項**
指名委員会等設置会社	取締役会決議で執行役に委任可。委任しない場合に限り取締役会で決定	**416条4項柱書本文**
取締役会非設置会社	取締役会設置会社とのバランス上、取締役の過半数の賛成が必要と考えられる（CISO等は通常「支配人」に該当しない）	**348条2項／同3項柱書・3号**

法務が施行前に点検すべきこと

・Q&AハンドブックVer2.0・19頁は、サイバーセキュリティに関する内部統制システムの構築において「必要な内部組織及び権限」等を取締役会で決定されるべき事項としている

・取締役会規則・職務権限規程の点検、CISO等の任命決議の有無と議事録の記載、CIO等との兼務可否の検討記録

予算・人材：「コスト」ではなく必要不可欠な投資

GOVERN

1 予算

将来の損失を抑える投資。直接ROIだけで削らない。

2 人材

社内育成＋外部専門家。役割別の力量を可視化。

3 教育

全職員 年1回以上。経営層にも学習機会。

4 演習

実践的な訓練を定期実施し、課題を計画に反映。

人材不足を理由に「やらない」のではなく、委託・共同・資格者活用で補完する発想が一貫。

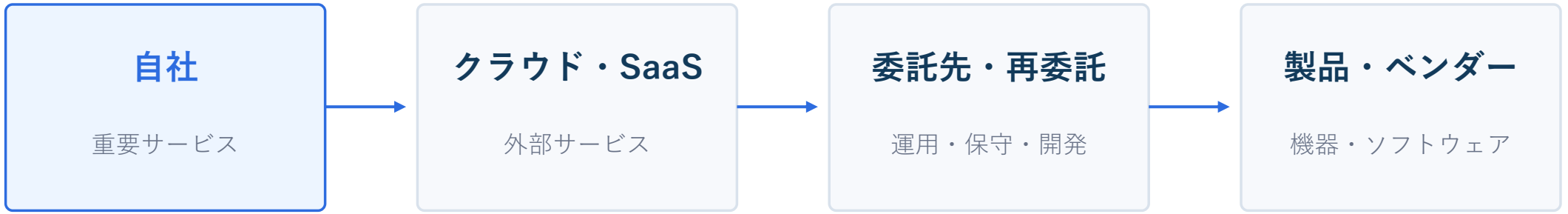
監査・モニタリング・情報開示・改善を1つのループに

GOVERN

NCO ガイドライン p.31-37

サプライチェーン：自社の境界はもう防御境界ではない

SUPPLY CHAIN



1 把握

依存関係・委託先台帳・セキュリティ状況

2 評価

重要度、アクセス権限、データ、供給途絶

3 統制

契約・監査・改善要求・共同訓練

リスクは「移転」できても、説明責任まで丸投げはできない。

NCO ガイドライン p.38-46

委託契約に入れるべきサイバー条項

責任・統制

- 役割分担／責任分界
- 監査権限
- 再委託手続
- 遵守ルール

事故・脆弱性

- 通知対象・通知方法・期限
- 脆弱性診断・報告
- 重大脆弱性への対応
- 共同演習・訓練

データ

- 所在・保管・保持
- 移転・返却・削除
- 暗号・アクセス制御
- 終了時の措置

保証・終了

- 第三者保証／認証
- 改善要求
- 契約終了条件
- 証拠・ログの確保

契約締結時だけでなく、履行状況を定期／リスクに応じて確認し、必要な改善を求める。

NCO ガイドライン p.41-43

委託先デューデリジェンスは「重要度」で濃淡をつける

1 データ
どの情報を処理・保有するか

2 権限
自社システムへのアクセスの深さ

3 機能
止まると重要サービスへどう影響するか

Tier 1	重要	現地/詳細DD、契約強化、定期監査、共同演習
Tier 2	中	外部評価＋質問票、年次確認
Tier 3	低	標準条項＋外部認証等で効率化

認証・評価制度を「自前確認の省力化」に使う

SCS評価制度

サプライチェーン企業の対策を共通基準で評価・可視化（2026年度末頃の制度開始予定）

JC-STAR

IoT製品のセキュリティ要件適合評価・ラベリング

ISMAP

クラウドサービスの政府向けセキュリティ評価

JISEC

IT製品のセキュリティ評価・認証

SBOM

ソフトウェア構成要素を可視化し、脆弱性対応を高速化

“認証があるから安全”ではない。重要度に応じて、外部評価＋自社固有要件を組み合わせる。

NCO ガイドライン p.39, 45-46

資産管理：見えていないものは守れない

IDENTIFY

IT	サーバ・端末・NW
OT	制御機器・PLC
SW	OS・アプリ・FW
Cloud	SaaS / PaaS / IaaS
Data	情報・媒体
External	外部公開資産・ASM

資産目録には、責任者・利用制限・OS/バージョン・接続先・プロトコル等を用途に応じて持たせる。

NCO ガイドライン p.47-50

「閉域網だから安全」は明確に否定された

IDENTIFY

✕ 閉域網だから安全

✕ 専用OSだから安全

✕ 独自仕様だから安全

OT/制御システムで見るべき変化

汎用OS・TCP/IPの採用、遠隔監視・保守、USB等の外部媒体、IT/OT境界、ベンダー接続、機器更改による接続性の増大。

パッチが難しい場合も「何もしない」ではなく、分離・監視・仮想パッチ等の代替策をリスクベースで選ぶ。

可用性を守るために、サイバー対策で可用性を壊さない - OT特有のバランスが必要。

NCO ガイドライン p.5-6

リスクアセスメント：3つの視点を重ねる

IDENTIFY

① 資産ベース

資産ごとに
「重要度 × 脅威 × 脆弱性」
を評価。

何を守るかの基本。

② 事業被害ベース

先に回避したい事業被害を定義
。

例：広域サービス停止、決済不
能、操業停止。

経営層が理解しやすい。

③ HSE

Health / Safety / Environment

人命・安全・環境影響をCIAだ
けでなく評価。
OTでは特に重要。

「情報漏えいの金額」だけでなく、社会サービス・人命・安全まで事業被害として評価する。

NCO ガイドライン p.55-58

AI時代の脆弱性管理：「重要度×悪用状況」で優先順位

IDENTIFY

AIが変えたのは「時間」

生成AI等の悪用で、脆弱性の発見から攻撃手法の確立までが短時間化。インターネット公開資産や重要資産は、従来の月次・四半期運用では間に合わない場面がある。

NCO ガイドライン p.63-69

認証：MFAは「あるか」より「破られにくいか」

最低限

・重要システムへインターネット経由ログイン → MFA
・デフォルトパスワード変更
・管理者権限を最小化
・退職等で不要となったアカウントは速やかに無効化

さらに望ましい

重要情報を扱うクラウド、管理者アクセス、重要NW機器などへMFAを拡大。

利用者アクセスの定期レビューも実施。

次の標準

フィッシング耐性のあるMFA
例：FIDO / PKI

プッシュ通知だけならMFA疲労攻撃に留意し番号照合等を利用。

ID・パスワード＋SMS/OTPだけで「MFA済み」と安心しない。

データ・暗号・メール：地味だが事故を大きく左右する

1 秘密情報

認証情報・秘密鍵・APIキー・トークンを平文保存しない。ログやチケットへの不用意な記録も避ける。

2 通信

外部通信は転送中データを保護。閉域網でもタッピング等のリスクを考慮。

3 メール

STARTTLS、SPF/DKIM、DMARC。DMARCはp=quarantine / rejectを基本に。

4 暗号移行

非推奨・脆弱な暗号資産を特定し、更新計画を策定。PQC対応の土台にもなる。

バックアップ：ランサム対策は「復元できる」までがセット

PROTECT

取る

重要システムのデータ＋OS設定＋スクリプト＋パラメータ。OTはPLCロジックや設計図面等も。

切り離す

元システムと異なるセグメント／オフライン。イミュータブルや異なる媒体も検討。

戻す

復旧手順を整備し、リカバリー検査・復旧テストで「本当に戻る」を確認。

バックアップが同じ認証基盤・同じ管理経路で破壊される設計では、バックアップがあっても救えない。

NCO ガイドライン p.89-91

検知：ログを「集める」から「意味を読む」へ

DETECT

ログ

重要サービス障害につながる事象を検知できるログを取得。

IoCだけでなくアノマリ（異常値）も見る。

継続監視

ネットワーク、物理環境、人の活動・操作を継続監視。

OTへ製品導入する際は性能・安全性への影響をテスト。

分析

インシデントの範囲・レベルを事前定義。

SIEM等で複数のアラート・ログを組み合わせ、自動化も活用。

監視は「SOCに任せた」では終わらない。何を監視していないかまで把握する。

NCO ガイドライン p.120-124

CSIRT：技術チームではなく「危機対応のハブ」

RESPOND

役割分担・対応手順は、平時に合意しておく

NCO ガイドライン p.27-29, 129-140

BCP：サイバーは自然災害と違う

RESPOND

1	**攻撃者がいる**	目的を持ち、こちらの対応を見ながら変化する
2	**原因が見えにくい**	侵入時点・範囲・残存が不明なまま判断が必要
3	**復旧が再侵入を招く**	感染・資格情報・脆弱性を残したまま戻すと再被害
4	**証拠が必要**	フォレンジック・捜査・報告のためログ等を保全
5	**能動停止もある**	安全確保のため自らサービス／システムを止める判断

BCPには「復旧する」だけでなく、隔離・調査・安全確認を経て復旧する条件を組み込む。

NCO ガイドライン p.125-142 / 別紙 p.152-163

別紙：サイバー攻撃リスクの7つの特性

RESPOND

①	**攻撃者の存在と多様な攻撃目的**	事前に攻撃者や攻撃目的を知ることは困難。被害発生に至るシナリオを作成し対応を検討する
②	**攻撃手口の高度化**	新たな手口に対し現状のCP・BCPで対応可能か確認し、必要に応じ見直す。一定期間、監視機能・体制を強化
③	**急速な被害拡大に繋がる攻撃**	通信の遮断やシステムの停止も視野に。遮断・停止前に失われるメモリ・プロセス情報等の収集手順を検討
④	**執拗な攻撃が行われる可能性**	復旧前に被害原因を分析・特定・対処。対処チームと復旧チームを分ける。復旧後も一定期間は監視を強化
⑤	**同時多発的な攻撃**	メインと非常用システムの同時使用不能を低減。手動制御・代替業務・代替サービス、複数の情報共有手段を用意
⑥	**検知が困難な攻撃**	外部への調査依頼時のログ・機器の開示手続（責任者・判断基準・提供手段・開示不可情報）を明確化しておく
⑦	**誤った判断や対処を誘発する攻撃**	管理システム自体が改ざんされている可能性を考慮。目視確認・手動制御等、複数の監視・対応手段を用意する

法務が主導すべきは③「遮断・停止前の証拠保全」と⑥「外部調査時の開示手続の事前整備」。

NCO ガイドライン 別紙 p.152-163（CP・BCPの策定・改定時の考慮事項）

技術・脅威の動向：第7章は経営者向けの“未来予告”

THREATS

1 ランサムウェア

脆弱性・認証・バックアップ・ログ・分割・監視を横断適用

2 AIシステム

AI自体の機密性・完全性・可用性、人間の介在も検討

3 高性能AI悪用

攻撃の高速化・大規模化を前提にパッチ・BCP・監視を強化

4 PQC移行

2035年を視野に、暗号資産の把握と移行準備

「今ある基準にチェックを付ける」だけでは追いつかないため、動向監視と柔軟な更新を要求。

NCO ガイドライン p.143-151

ランサムウェア：身代金支払を「厳に慎む」と明記

講ずべき対策

・VPN/RDP等の侵入経路と脆弱性・認証情報を管理
・バックアップ削除リスクを考慮
・ネットワーク分割、ログ、継続監視
・ベンダー等と協力関係を構築
・金銭の支払は厳に慎む

危機時に事前決定しておく事項

①誰が支払可否を決めるか
②法執行機関・所管省庁への連絡
③制裁・AML等の法的確認
④保険・専門家への連絡
⑤復号の実効性・再攻撃リスク
⑥公表・ステークホルダー説明

「払う／払わない」を感染後にゼロから議論しない。危機管理方針に組み込む。

PQC：2035年は遠くない - まず「暗号の棚卸し」

今

クリプト・インベントリ
暗号方式・鍵長・用途・
委託先

→

次

重要度・寿命・移行困難
度で
優先順位付け

→

移行期

暗号アジリティ
ベンダー・クラウドとの
調整

→

2035目標

政府機関等に加え
重要インフラも原則目標
を意識

法務・調達の論点

長期保守契約やクラウド契約で「PQC対応・暗号変更への協力・費用負担・EoL」を今から確認する。

案から修正・追記された11か所

PUBLIC COMMENT

確定版にすべて反映済み。改定履歴として押さえておくべき箇所

2.5.2①-2 解説	「有効的と考えられる」を「有効と考えられる」に修正	**No.75**
2.9①-1 解説	依存関係の把握を行うに当たっての観点を追記	**No.76**
3.6②-1 解説	脆弱性診断の対象にクラウドで構築されるシステムも含まれ得る旨を追記	**No.84**
3.6②-2 解説	代替措置に仮想パッチの適用も含まれる旨を明確化	**No.82**
4.1.1①-4	「アカウント管理が不要」→「アカウントが不要」に修正	**No.119**
4.1.2①-4	「デフォルト認証情報」を「デフォルトパスワード」に統一	**No.122**
4.3.3①-1	「年1回以上」は横断的な最低限の頻度の趣旨であること、対象データの特性の考慮を追記	**No.101・106・120**
4.3.3①-2 解説	イミュータブルバックアップ、異なる媒体・環境での保存を追記	**No.101・110・113**
4.4.4①-2	マルチエンジン型のマルウェア検知ソフトに限定されない表現に修正	**No.107**
5.1①-2 解説	委託先の対策内容の把握に関する参考情報（ISOG-J「MSS選定ガイドライン」）を追記	**No.125**
7①-3-1 解説	制御システム等へのパッチ適用が困難な場合の仮想パッチ等リスク低減策を追記	**No.144**

実務的に影響が大きいのは4.3.3（バックアップ）。「年1回以上」が独り歩きしないよう、最低限の頻度である旨とデータ特性の考慮が明記された。

パブコメの読み方と、採用されなかった主な意見

PUBLIC COMMENT

① 基本構造は維持

章立て、「講ずべき／望ましい」の2段階、経営統治・サプライチェーン・AI/PQCという大枠は案と最終版で一貫

② 実装の具体化を読む

MSS選定ガイドライン、仮想パッチ、イミュータブルバックアップなど、実行時の補助線が加わった

③ 「緩和された」とは読まない

リスクベースの柔軟性はあるが、経営責任・委託先管理・レジリエンスという方向性はむしろ明確になった

マイクロセグメンテーション／SIEMによる分析自動化を「講ずべき」に格上げ	コスト・人材・専門知識等の観点から、必ずしもすべての事業者にとって導入が容易とは言い難い	No.111・112・124・132
脅威ハンティングの実施を必須化	「脅威ハンティングの普及促進・実施等に係る基本方針」（2026年7月31日決定）の取組状況を踏まえ今後検討	No.123
SBOM等を「原則として求める対策」に格上げ	不正機能等の埋め込みへの対策は「講ずることが望ましい対策事項」の定義に該当する	No.44
特定国製品・特定国籍者の排除を義務化	統一基準は特定の国や企業の製品を排除するものではない（役職員の管理2.5.4とサプライチェーン管理2.9で対応）	No.48・49・55・72・73
インシデント報告のワンストップ化・様式統一	本ガイドラインは安全基準等策定のための詳細事項。今後の情報共有の在り方の検討に当たって参考とする	No.128・129・131・133
対策事項の「実装レベルモデル」による階層化	「講ずべき」「望ましい」の2段階＋成熟度モデル（CI-CSA等）の活用により対応済み	No.9・33

共通する論理：本ガイドラインは所管省庁等が安全基準等を策定するための「詳細事項」であり、事業者に一律の対応を求めるものではない。

パブコメ後に読むべき「実務補助線」

1 監視委託

MSS選定ガイドラインを参照。SOC/MSSに任せても、監視対象・未対策領域・エスカレーションを自社が把握する。

2 サプライチェーン

SCS評価制度、ISMS等を使い、委託先確認を効率化。ただし自社の重要度・アクセス権限・データに応じた上乗せは残る。

3 製品・クラウド

JC-STAR、ISMAP、JISEC、SBOMを調達基準に組み込み、脆弱性対応と透明性を高める。

4 脆弱性判断

CVSSだけでなく、KEV・SSVC・事業影響を重ね、AI時代の攻撃速度に合わせて優先順位を付ける。

読み筋：パブコメ後も「緩和」ではなく、実務で回せるように参照先・評価軸が足されたと見る。

実務ロードマップ：まず180日でここまで

ACTION

0-30日

現状把握

・任務／最低サービス水準
・重要資産／委託先
・既存規程・BCP・契約
・CISO/CSIRT体制

31-90日

ギャップ評価

・講ずべき対策の自己評価
・IT/OT/クラウドの差分
・重要委託先Tiering
・重大脆弱性の棚卸し

91-180日

優先実装

・MFA/特権ID
・バックアップ隔離/復旧試験
・委託契約改定
・経営層演習・監査計画

“全部やる”より、重大サービスに効く順番を決める。

取締役会・経営会議に上げる10問

ACTION

1. 最低限止められないサービスは何か？

2. そのサービスはどのIT/OT・委託先に依存するか？

3. 最大何時間／何日止められるか？

4. CISOはトップへ直接報告できるか？

5. 重大リスクを誰が受容するか？

6. 重要委託先の再委託先まで見えているか？

7. バックアップは攻撃者から切り離され、戻せるか？

8. 高リスク脆弱性を何日で処理できるか？

9. 重大事故時、停止・公表・警察連絡を誰が決めるか？

10. 半年前より成熟度は上がったか？

この10問に答えられない状態は、技術対策が多くても「ガバナンスが弱い」。

NCO ガイドラインの経営論点を講師が10問に整理

法務部門がすぐ着手できる8項目

ACTION

① CISO・CSIRT 任命手続、職務権限、報告ラインを確認

② 規程体系 基本方針・個別方針・BCP・インシデント規程の整合

③ 委託契約 通知・再委託・監査・脆弱性・データ・終了条項

④ リスク受容 例外・パッチ見送り等の承認プロセスと証跡

⑤ 報告義務 所管省庁・法令・契約・個人情報等の報告マップ

⑥ 公表 広報と連携し、判断権者・開示基準・テンプレを準備

⑦ 演習 法務・広報・経営を含めたテーブルトップ演習

⑧ 議事録 リスク説明・資源配分・改善指示を意思決定記録に残す

法務は「事故後に呼ばれる部署」から、「事故前の設計に入る部署」へ。

NCO ガイドライン p.21-46, p.129-140 を中心に講師整理

取締役会議事録に残すべき6つの決定事項

ACTION

1 任務・最低水準

最低限維持・復旧すべきサービス、RTO/RPO、社会的影響を確認。

2 リスク許容度

受容できる停止時間・漏えい・安全影響を経営判断として定義。

3 CISO・権限

任命手続、トップへの直接報告、CIO等との牽制、専任性の検討を記録。

4 資源配分

予算・人材・外部専門家・訓練費用を「必要不可欠な投資」として承認。

5 重大リスク受容

パッチ未適用・代替策・更改見送り等は理由、期限、再評価日を残す。

6 演習・改善指示

訓練結果、事故教訓、監査指摘を方針・BCP・契約に反映する指示。

事故後に効くのは「完璧だった」という主張ではなく、合理的な判断プロセスと見直しの証跡。

事故対応テーブルトップ演習：90分シナリオ

RESPOND

0分

検知

外部公開サーバで不審通信。SOCから高リスクアラート。

20分

範囲不明

AD認証情報流出の疑い。重要システムへの横展開可能性。

45分

経営判断

一部サービス停止・外部接続遮断・ベンダー招集を判断。

70分

報告・公表

所管省庁、警察、個情法、契約先、利用者説明の要否を整理。

90分

復旧方針

クリーン環境、バックアップ、再侵入防止、証拠保全の条件を決める。

演習の狙い：技術対応の正解探しではなく、「誰が、どの情報で、いつ経営判断するか」を確認する。

まとめ：このガイドラインを一言で言うと

SUMMARY

「止めない」ではなく、
“止まっても社会的任務を守り、説明できる組織”を作る

Govern	Know	Protect	Detect	Recover
経営が決める	資産・依存関係を知る	優先順位を付けて守る	早く気づく	安全に戻す

パブコメ後も方向性は一貫：経営責任 × サプライチェーン × レジリエンス × AI時代の速度

主要参照資料

SOURCES

- 1. 内閣官房 国家サイバー統括室「重要インフラのサイバーセキュリティに係る安全基準等策定ガイドライン」（令和8年9月11日）
  https://www.cyber.go.jp/pdf/policy/infra/guideline_2026.pdf
- 2. 同「安全基準等策定ガイドライン（案）」に関するパブリックコメント結果（主な結果一覧／結果の概要。令和8年9月11日公示、41者156件）
  https://www.cyber.go.jp/pdf/policy/infra/pubcom_res_guideline2026_kekkaichiran.pdf
- 3. 同「安全基準等策定ガイドライン（案）」に関する意見の募集について（令和8年8月5日～8月26日）
  https://www.cyber.go.jp/policy/group/infra/pubcom_jyuhurakijun_guideline2026.html
- 4. 同「重要インフラ対策関連」— 重要インフラのサイバーセキュリティ対策のための統一基準（令和8年7月31日戦略本部決定、2026年10月1日施行予定）等
  https://www.cyber.go.jp/policy/group/infra/policy.html
- 5. ガイドライン本文が参照する各種資料：サイバーセキュリティ経営ガイドライン、NIST CSF、CISA KEV/SSVC、ISOG-J MSS選定ガイドライン、CRYPTREC、PQC関係資料 等

本資料はセミナー解説用。個別事案では、各分野の安全基準等・関係法令・監督指針・契約内容を確認してください。