経済産業省

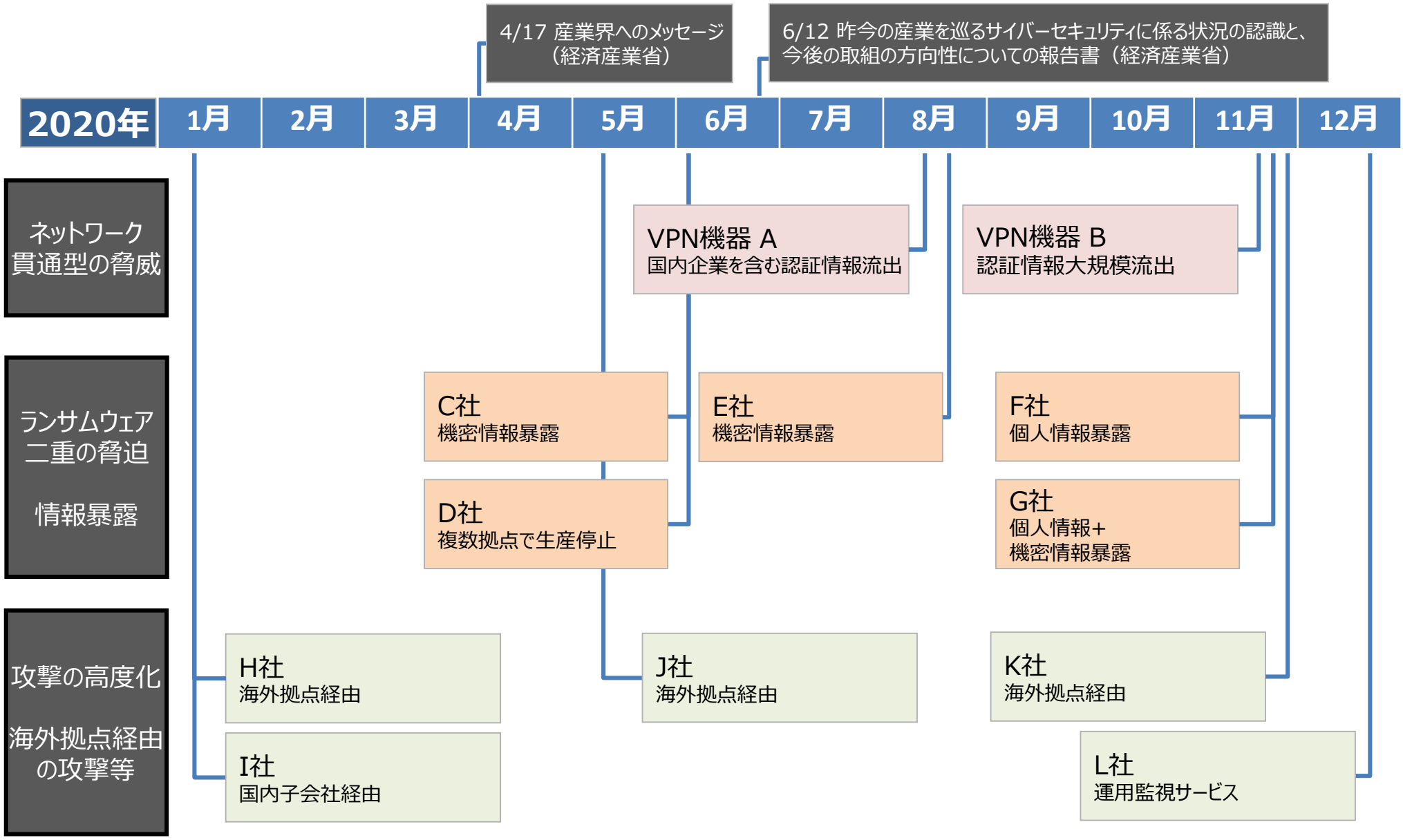
DX時代のサイバーセキュリティ対策

経済産業省　商務情報政策局

サイバーセキュリティ課

2020年の主なサイバー攻撃事案

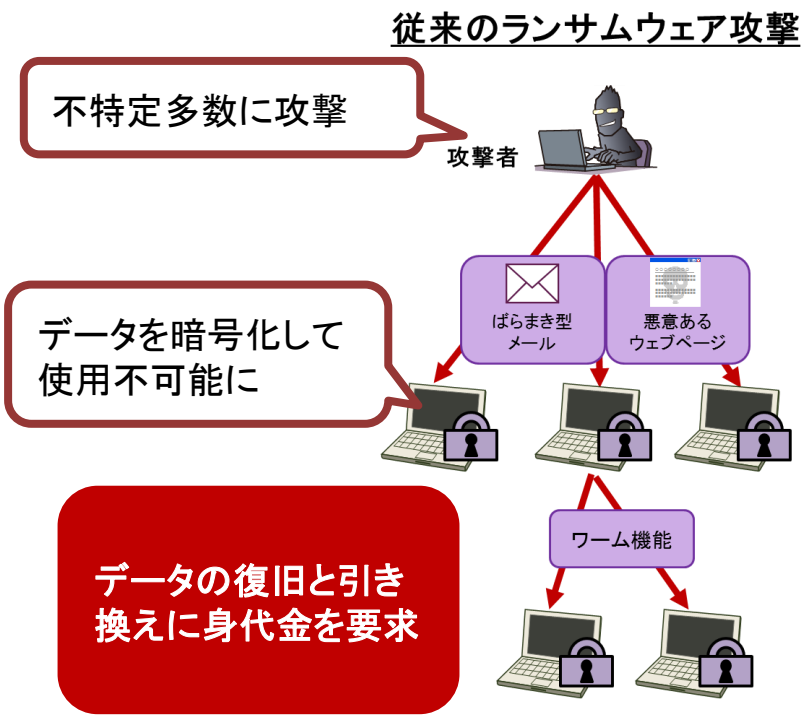
2020年12月18日公開資料

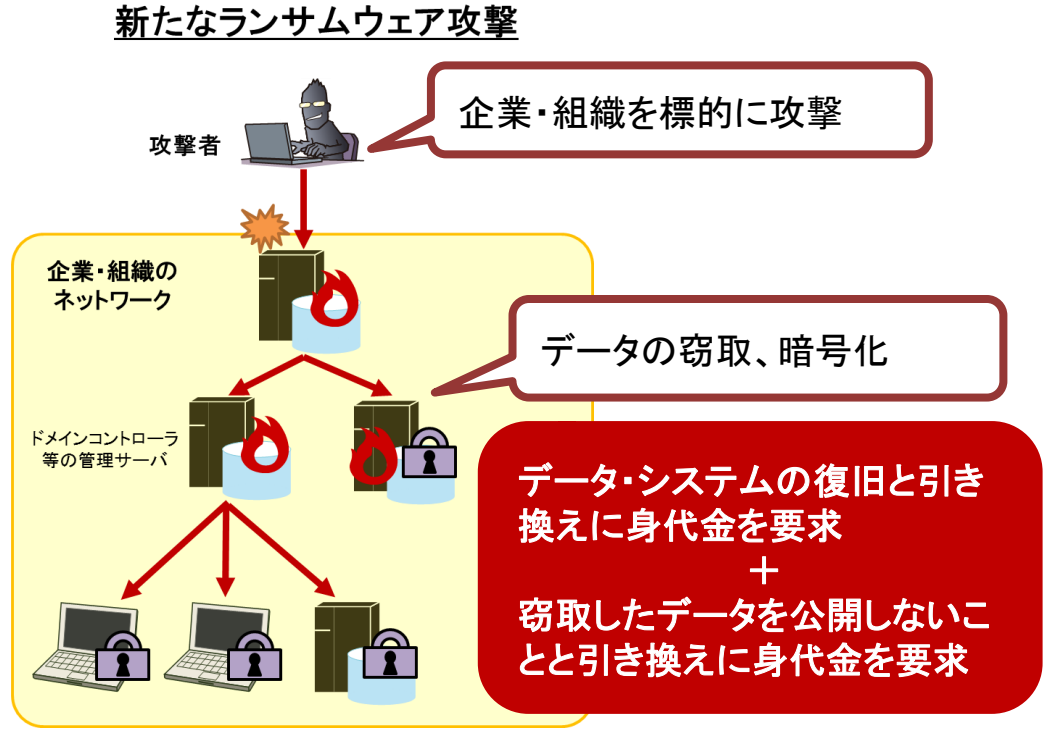


※攻撃開始時期ではなく、報道・公表された時期等でマッピング

（参考）ランサムウェアとその手口の変化（二重の脅迫）

- ランサムウェアは「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。感染したパソコンのデータを暗号化するなど使用不可能にし、その**解除と引き換えに金銭を要求**する。
- **新たな（標的型）ランサムウェア攻撃（二重の脅迫）とは**
  - ターゲットとなる企業・組織内のネットワークへ侵入し、パソコン等の端末やサーバ上のデータを窃取した後に一斉に暗号化してシステムを使用不可能にし、脅迫をするサイバー攻撃。
  - システムの**復旧に対する金銭要求**に加えて、窃取した**データを公開しない見返りの金銭要求**も行うので、**二重の脅迫**と恐れられる。窃取された情報に顧客の情報や機微情報を含む可能性がある場合には、被害組織はより困難な判断を迫られることになる。





「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」

2020年12月18日公開資料

●サイバー攻撃は規模や烈度の増大とともに多様化する傾向にあり、実務者がこれまでの取組を継続するだけでは対応困難になっている。
●アップデート等の基本的な対策の徹底とともに、**改めて経営者のリーダーシップが必要に**。

① 攻撃は格段に高度化し、被害の形態も様々な関係者を巻き込む複雑なものになり、技術的な対策だけではなく関係者との調整や事業継続等の判断が必要に。改めて経営者がリーダーシップを。

② ランサムウェア攻撃による被害への対応は企業の信頼に直結。経営者でなければ判断できない問題。

●「二重の脅迫※」によって、顧客等の情報を露出させることになるリスクに直面。日常的業務の見直しを含む事前対策から情報露出に対応する事後対応まで、経営者でなければ対応の判断が困難。
●金銭支払いは犯罪組織への資金提供とみなされ、制裁を受ける可能性のあるコンプライアンスの問題。

③ 海外拠点とのシステム統合を進める際、サイバーセキュリティを踏まえたグローバルガバナンスの確立を。

●国・地域によってインターネット環境やIT産業の状況、データ管理に係るルール等が異なっており、海外拠点とのシステム統合を通じてセキュリティ上の脆弱性を持ち込んでしまう可能性も。
●拠点のある国・地域の環境をしっかりと評価し、リスクに対応したセグメンテーション等を施したシステム・アーキテクチャの導入や拠点間の情報共有ルールの整備等、グローバルガバナンスの確立が必要。

④ 基本行動指針（高密度な情報共有、機微技術情報の流出懸念時の報告、適切な場合の公表）**の徹底を。**

※攻撃者が、被攻撃企業が保有するデータ等を暗号化して事業妨害をするだけではなく、暗号化する前にあらかじめデータを窃取しておいて支払いに応じない場合には当該データを公開することで、被攻撃企業を金銭の支払いに応じざるをえない状況に追い込む攻撃形態。

経済産業省「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起（2020年12月18日）」https://www.meti.go.jp/press/2020/12/20201218008/20201218008.html

サイバーセキュリティ経営ガイドライン

平成27年12月28日策定
平成28年12月8日改訂（Ver.1.1）
平成29年11月16日改訂（Ver2.0）

- セキュリティはコストではなく投資であると位置づけ、経営者がリーダーシップを取ってセキュリィ対策を推進していくことが重要であることを示したガイドライン。
- 経営者が認識すべき３原則と、経営者がCISO（最高情報セキュリティ責任者）等に指示すべき10の重要事項から構成。

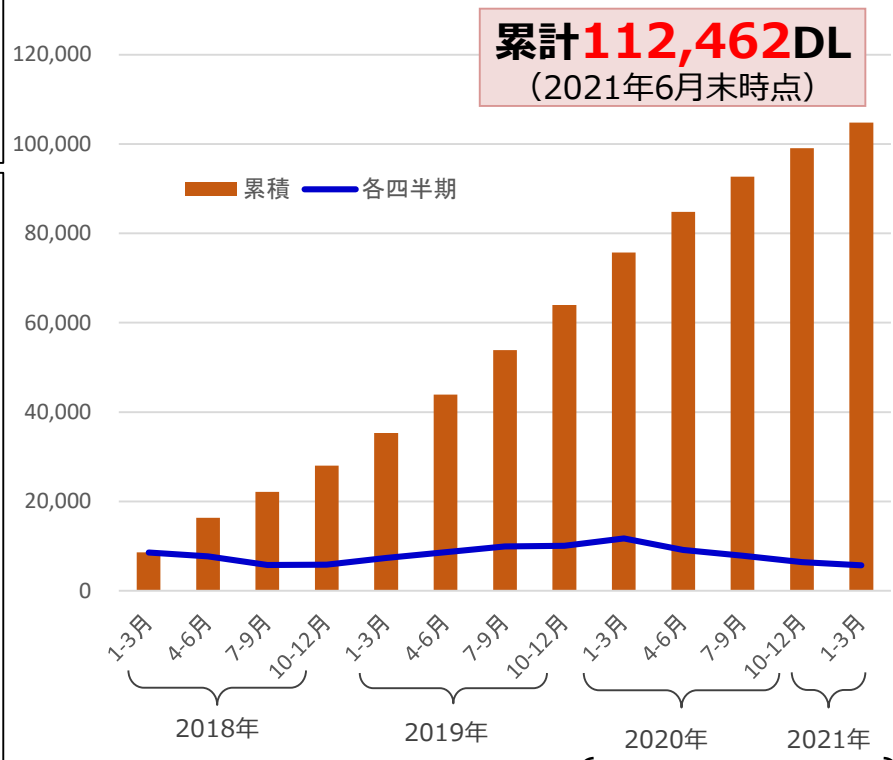
１．経営者が認識すべき３原則

（１）経営者が、**リーダーシップを取って対策**を進めることが必要
（２）自社のみならず、**ビジネスパートナーを含めた対策**が必要
（３）平時及び緊急時のいずれにおいても、**関係者との適切なコミュニケーション**が必要

２．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築	**指示１** 組織全体での対応方針の策定 **指示２** 管理体制の構築 **指示３** 予算・人材等のリソース確保
リスクの特定と対策の実装	**指示４** リスクの把握と対応計画の策定 **指示５** リスクに対応するための仕組みの構築 **指示６** PDCAサイクルの実施
インシデントに備えた体制構築	**指示７** 緊急対応体制の整備 **指示８** 復旧体制の整備
サプライチェーンセキュリティ	**指示９** サプライチェーン全体の対策及び状況把握
関係者とのコミュニケーション	**指示10** 情報共有活動への参加

サイバーセキュリティ経営ガイドラインV2.0のダウンロード数推移



【参考】上場企業数　第一部　2,192社
第二部　474社
（日本取引所グループ公表 2021年５月31日時点）

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

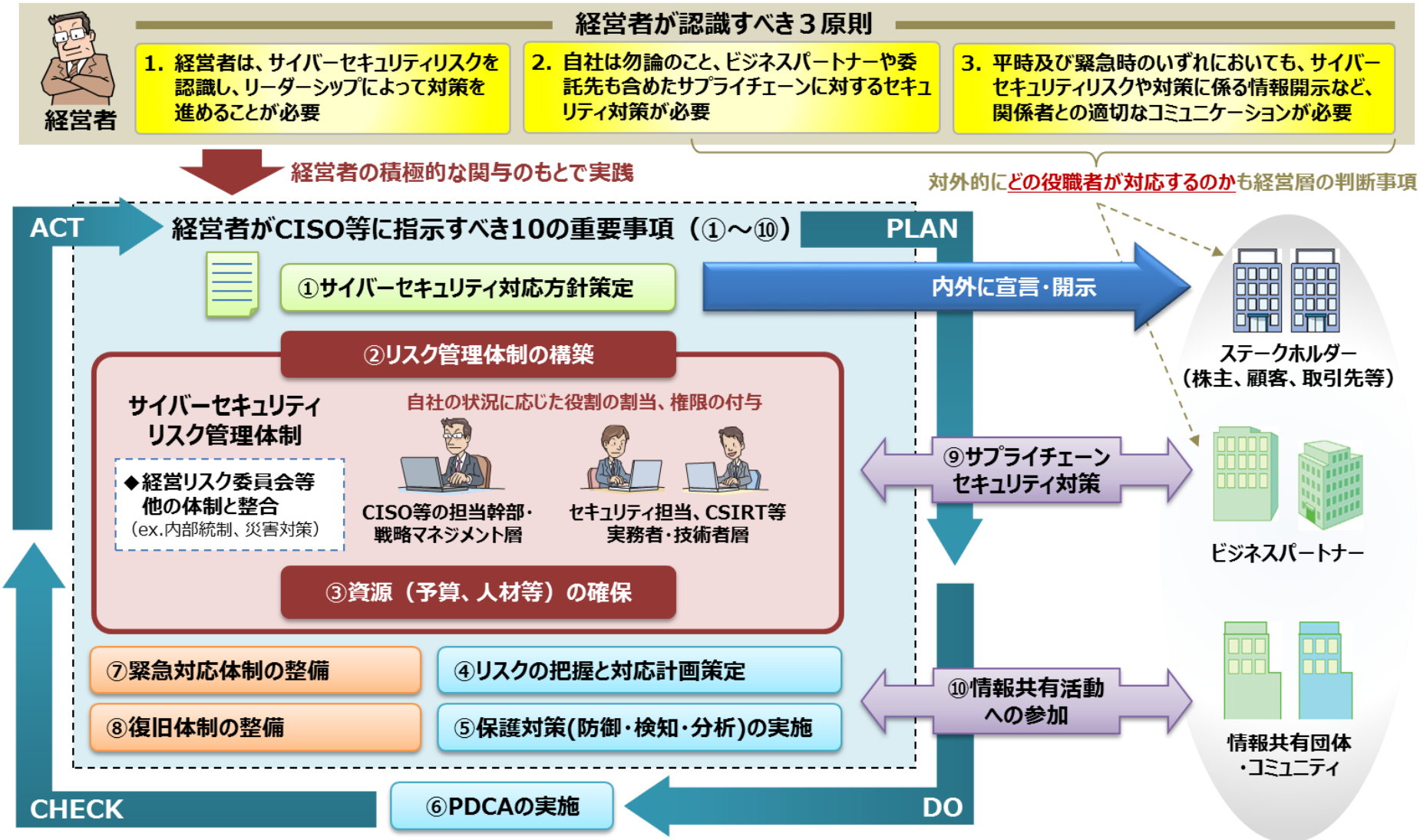
『セキュリティ体制構築・人材確保の手引き』（「サイバーセキュリティ経営ガイドライン」付録F）

2020年9月30日　Ver.1.0 公表
2021年4月26日　Ver.1.1 公表

- 企業におけるサイバーセキュリティ対策の推進において、その基盤となる**「リスク管理体制の構築」及び「人材の確保」**（**「サイバーセキュリティ経営ガイドライン」指示２・３に該当**）は経営者が積極的に関与して実践すべき取組。その具体的検討のための参考文書として、手引きを作成。

累計6,925DL
（2021年6月末時点）

「サイバーセキュリティ経営ガイドライン」における『セキュリティ体制構築・人材確保の手引き』の位置づけ



（参考）『セキュリティ体制構築・人材確保の手引き』のポイント

サイバーセキュリティリスク管理体制の構築（指示２）

１）経営者のリーダーシップ下でのセキュリティ体制検討	①デジタル技術の活用の進展に伴い、従来とは異なる全社的なセキュリティ体制を。 ②全社的なセキュリティ体制確立は経営者の責務。経営者がリーダーシップを。
２）セキュリティ統括機能の検討	①全社的なセキュリティ体制の確立のためには、CISO等の経営層を補佐する「セキュリティ統括機能」の設置を。 ②セキュリティ統括機能には４類型あり、自社の状況に合わせた検討を。
３）関連タスクを担う部門・関係会社の特定・責任明確化	①セキュリティ統括機能と連携しつつセキュリティ関連タスクを担う部門・関係会社を特定する際には、ITSS＋（セキュリティ領域）を参考として、外部委託先も含めた見える化を。 ②外部委託先の選定では、情報セキュリティサービス基準適合サービスリスト等の活用を。

サイバーセキュリティ対策のための資源確保（指示３）

１）「セキュリティ人材」の確保	①まずはサイバーセキュリティの専門性を備えたセキュリティ統括人材の確保を。 ②担当する人材の育成を通じた質的充足を。
２）「プラス・セキュリティ」の取組推進	①「セキュリティ人材」の確保のみならず、「プラス・セキュリティ」の取組（※）も推進を。 ※ 事業部門等においてそれぞれの業務に従事する人材が、セキュリティを意識し、業務遂行に伴う適切なセキュリティ対策の実施やセキュリティ人材との円滑なコミュニケーションに必要な能力を育成する取組 ②ITSS+（セキュリティ領域）等を活用し、関連部門でセキュリティ関連タスクを担う人材の特定・育成・配置等を。
３）教育プログラム・試験・資格等の活用と人材育成計画の検討	①各分野に求められる知識・スキルを踏まえた教育プログラムや試験・資格の活用を。 ②自社に必要な人材の配置計画をもとに、キャリアデザインを含めた育成計画を。

『サイバーセキュリティ経営ガイドラインVer2.0実践のためのプラクティス集』

- 2019年3月、**「サイバーセキュリティ経営ガイドラインVer2.0実践のための経営プラクティス集」を公開**。経営ガイドラインの重要10項目の実践事例に加え、セキュリティ担当者の日常業務における悩みに対する具体的対応策を提示。プラクティスを追加した**第2版を2020年6月3日に公表**。

＜特徴＞

「情報セキュリティの取組みはある程度進めてきたが、サイバー攻撃対策やインシデント対応は強化が必要。それに向けた体制づくりや対策は何から始めるべきか」と考えている経営者やCISO等、セキュリティ担当者を主な読者と想定し、ガイドラインの「重要10項目」を実践する際に参考となる考え方やヒント、実施手順、実践事例を掲載。

＜イメージ＞

＜構成＞

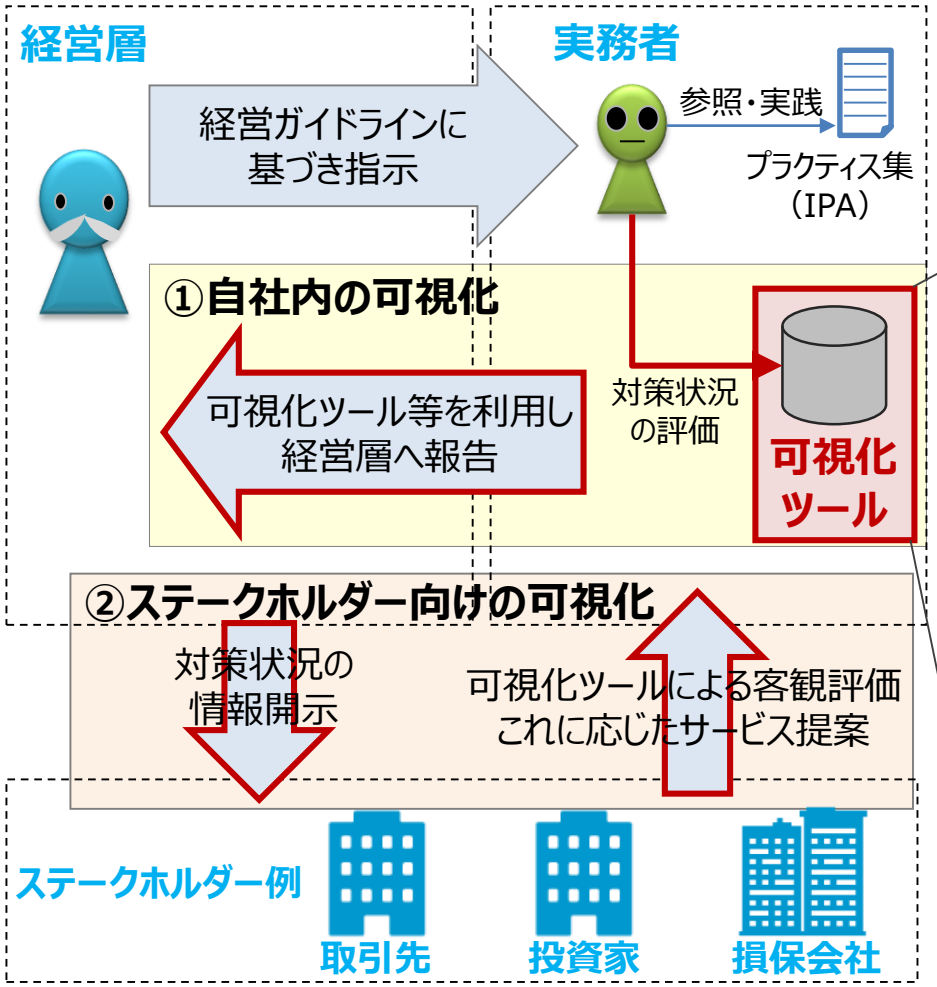
- **はじめに**
- **第1章　経営とサイバーセキュリティ**
- **第2章　サイバーセキュリティ経営ガイドライン実践のプラクティス**
  サイバーセキュリティ強化のために実践していただきたいファーストステップを、重要10項目ごとにまとめて掲載。
- **第3章　セキュリティ担当者の悩みと取組みのプラクティス**
  事例の妨げとなる課題やセキュリティ担当者の悩みに対し、実際に試みられた工夫の事例を紹介。
- **付録**
  サイバーセキュリティに関する用語集
  サイバーセキュリティ対策の参考情報

https://www.ipa.go.jp/security/fy30/reports/ciso/index.html

サイバーセキュリティ経営ガイドライン実践状況の可視化ツール

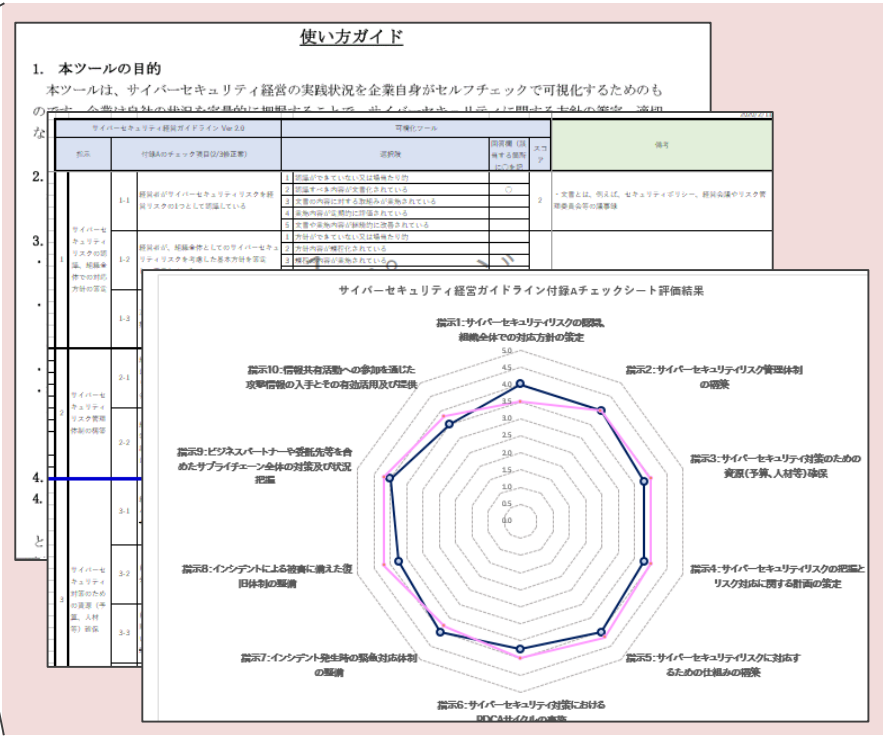
- 2020年3月25日、可視化ツールβ版（Excel）をIPAから公開。
- 2020年度はユーザ企業、投資家等ステークホルダー向けにそれぞれβ版でテストを行い、ブラッシュアップを実施。**2021年夏頃のVer1.0（Web版）公開**に向けて開発推進中。

累計**6,154**ダウンロード
（2021年６月末時点）



可視化ツールβ版の特徴：

- 「使い方ガイド」「チェックリスト」「可視化結果」の３種類のシート
- 39個の質問にセルフチェックで回答
- 回答方式は５段階の選択式（成熟度モデル）
- グループ会社間等での比較も可能



https://www.ipa.go.jp/security/economics/checktool/index.html

中小企業のセキュリティ対策

● 中小企業の情報セキュリティ対策ガイドライン（第3版 2019年3月）

–中小企業が情報セキュリティ対策に取り組む際の経営者が認識し実施すべき指針、社内において対策を実践する際の手順や手法をまとめたもの。

–第3版より、付録６として、クラウドサービスを安全に利用するための留意事項やチェック項目を記載した手引きを追加。

中小企業の情報セキュリティ対策ガイドライン

経営者向けの解説

経営者が認識すべき３原則と実施すべき重要７項目を解説

実践者向けの解説

企業のレベルに合わせて**段階的にステップアップ**できるような構成で解説

付録6:クラウドサービス安全利用の手引き

【クラウドサービス導入時の考慮ポイントの例】

- ✓ クラウドで扱う情報と業務の重要性（情報漏洩、改ざん、サービス停止した際の影響等）
- ✓ 自社・事業者間でのセキュリティルール・水準の整合性（データアップデート時の暗号化やパスワード強度の警告等）
- ✓ 利用者の範囲、権限の管理（利用目的に合わせ利用者、権限を設定等）
- ✓ クラウド事業者・サービスの安全・信頼性（セキュリティ対策の開示状況等）　等

● 「SECURITY　ACTION」

中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度。15万者を超える中小企業が宣言（2021年6月末時点）。

★一つ星

情報セキュリティ５か条に取り組む

★★二つ星

情報セキュリティ自社診断を実施し、基本方針を策定

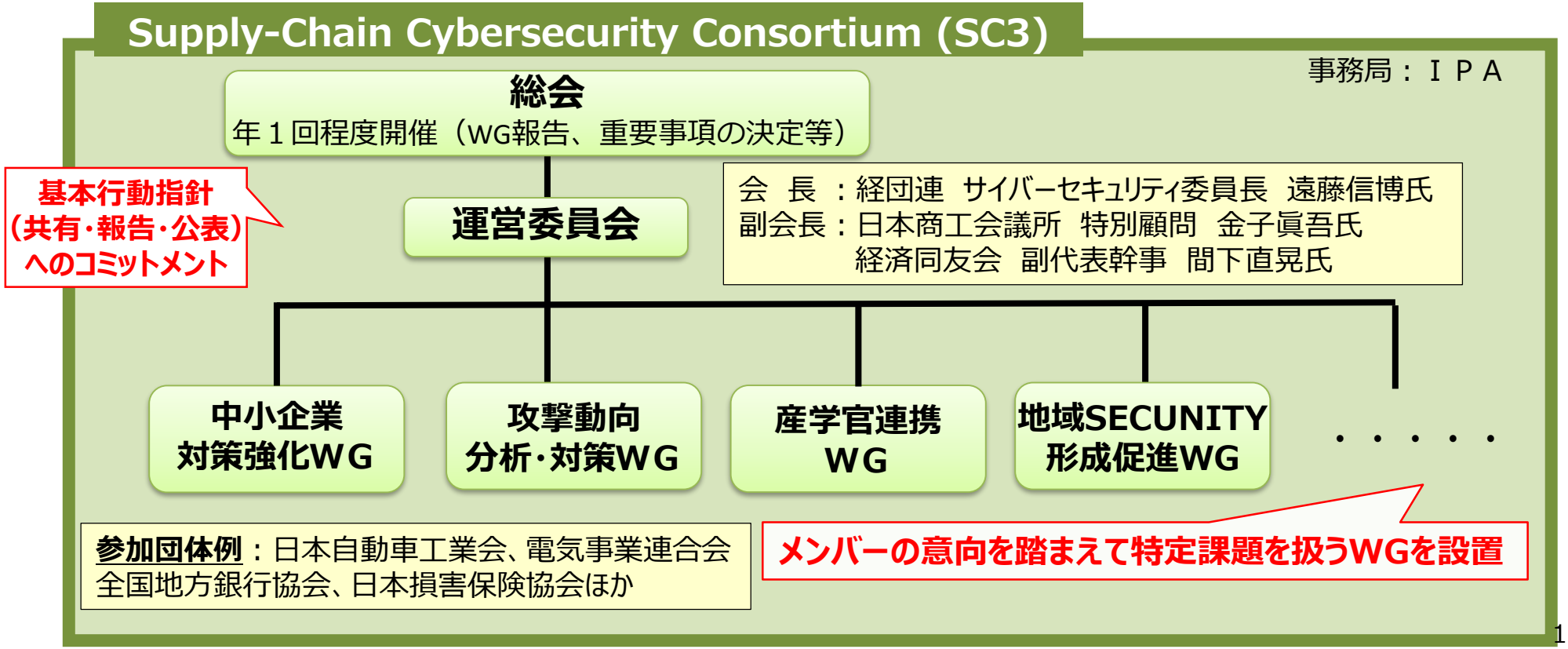
● サイバーセキュリティお助け隊サービス

相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など中小企業のサイバーセキュリティ対策に不可欠な各種サービス内容を要件としてまとめた基準を満たすサービス。（2021年7月時点で5サービス）

サイバーセキュリティ
お助け隊

サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）

- **趣　旨:** 大企業と中小企業がともにサイバーセキュリティ対策を推進するためのコンソーシアムを立ち上げ、「基本行動指針※」の実践と中小企業・地域を含めたサプライチェーンのサイバーセキュリティ対策を産業界全体の活動として展開していく。
  ※サイバー攻撃事案発生時における、「共有、報告、公表」によるリスクマネジメントの徹底。
- **参加者:** 経済団体、業種別業界団体　等（2021年６月末時点で171会員）※団体単位でのご入会をご案内。
- **設立日:** 2020年11月1日（設立総会：2020年11月19日）
- **活　動:** 特定の課題についてWGを設置し、具体的アクションを展開。



METI
Ministry of Economy, Trade and Industry

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html