資料２

関係省庁の取組状況について

金融庁　　金融分野のサイバーセキュリティレポートについて（資料２－１）

総務省　　サイバーセキュリティ対策情報開示の手引きの策定・公表について（資料２－２）

放送分野における「サイバーセキュリティの確保に関する技術的条件」の検討開始について

経済産業省　経済産業省におけるサイバーセキュリティ対策強化のための各種取組について（資料２－３）

金融分野のサイバーセキュリティレポート（令和元年６月）の概要

資料２－１

１．背　景

○ デジタライゼーションの加速的な進展、国際的な議論の進展、2020年東京オリンピック・パラリンピック競技大会等、金融機関を取り巻く環境変化等を踏まえ、「金融分野におけるサイバーセキュリティ強化に向けた取組方針」をアップデート（2018年10月）

取組方針の重点項目：(1)デジタライゼーションの加速的な進展を踏まえた対応、(2)国際的な議論への貢献・対応、(3)2020年東京大会等への対応、(4)金融機関のサイバーセキュリティ管理態勢の強化、(5)情報共有の枠組みの実効性向上、(6) 金融分野の人材育成の強化

○ 同取組方針に沿った取組みにおいて、把握した実態や共通する課題等を取りまとめレポートとして公表

２．主なポイント

事項	取組内容	結果（概要）
(1) デジタライゼーションの加速的な進展を踏まえた対応	◆デジタライゼーションの金融サービスにおける実態、サイバーリスクやその対応策等について、ITベンダーや大手金融機関等へのヒアリングを通じて、把握・分析	✓ 大手金融機関では、特にクラウドサービスやRPAなどの活用が進んでおり、適切にリスクを管理するため、ノウハウ・専門人材の確保などを進めつつ、これまでのサイバーセキュリティのフレームワークに沿ったセキュリティ対策を実施 ✓ デジタライゼーションの進展による外部依存度の高まりを踏まえ、外部委託を含めた適切な対策が必要。また、あらゆるサイバー攻撃を事前に防御することは難しく、侵入されることを前提とした対策がより重要。外部委託先を含めた情報資産の把握、リスク評価、入口・内部・出口対策（多層防御）に加え、監視・検知機能の強化、重要な外部委託先も含めたBCPの整備と演習・訓練を通じた実効性の向上を図っていく必要
(2) 国際的な議論への貢献・対応	◆G7財務大臣・中央銀行総裁会議に設置された「サイバーエキスパートグループ」における国際的なサイバーセキュリティに係る取組みに貢献・対応	✓「脅威ベースのペネトレーションテスト（TLPT）」及び「サードパーティのサイバーリスクマネジメント」に関する基礎的要素を策定・公表（2018年10月） ✓ G7諸国がクロスボーダーに連携して実施する合同演習へ参加。演習を通して得た知見や教訓を国内外の今後の取組みにつなげていく必要
(3) 2020年東京大会等への対応	◆金融分野の各関係団体と連携し、大規模インシデントを含むサイバー事案発生時における相互の情報連携ができるよう、「サイバーセキュリティ対策関係者連携会議」を立上げ（2019年６月）	✓ 連携会議を活用し、2020年東京大会を見据えた大規模インシデント発生時の連携態勢について、官民の関係団体との間で連携手順を共有するとともに、演習等を通じて実効性を確認していく必要

金融分野のサイバーセキュリティレポート（令和元年6月）の概要

事項	取組内容	結果（概要）
(4) 金融機関のサイバーセキュリティ管理態勢の強化	①平時のサイバー対策 ➢ 中小金融機関等 ◆ 地域銀行、信金・信組、証券会社等について、実態把握を通じた基礎的な態勢整備と脆弱性診断等の実施状況を確認 ◆ 信金・信組については、本年3月までにリスク評価・コンチプラン策定を完了させるよう要請し、アンケート等を通じて結果を確認。リスクプロファイルを踏まえたリスクベースでの実態把握を実施 ➢ 大手金融機関 ◆ 3メガについては、グローバルな動向等を念頭に、定期的な対話を通じて、サイバー対策のもう一段の高度化の状況を確認 ◆ 他の大手金融機関（大手証券、大手生損保、ゆうちょ銀行）については、対応能力のもう一段の引き上げのため、業界内・他業態との比較分析等を実施 ②有事のサイバー対策 ➢ 中小金融機関等 ◆ 業界全体のサイバー対策の強化を図るために、新たな業態としてFX業者、暗号資産（仮想通貨）交換業者を追加し、金融庁演習（DeltaWallⅢ）実施（2018年10月） ➢ 大手金融機関 ◆ 国際的な合同演習への参加、TLPT等の高度な評価手法の活用・促進	①平時のサイバー対策 ➢ 中小金融機関等 ✓ 地域銀行については、経営陣も関与して取組計画を策定し、自主的に強化を図っている状況。一方、脆弱性診断等については意識的に実施している先は一部に留まり、実施基準も定められておらず、必要性が十分浸透していない ✓ 信金・信組については、大部分はリスク評価・コンチプラン策定を完了。今後はリスク評価に基づく対策が重要。脆弱性診断等は地銀以上に浸透していない ✓ 証券会社等については、取組みが進展している金融機関が増えている一方、依然として取組未着手・停滞状態の先が多くみられた ➢ 大手金融機関 ✓ 3メガについては、海外の最新動向を踏まえた自組織の取組計画を策定し、高度化に向けた取組みを実施。サイバー攻撃の複雑化・巧妙化、国際的な動向等を踏まえ、グループ・グローバルでの一元的な管理態勢の更なる高度化に期待 ✓ 他の大手金融機関については、リスク評価に基づき、サイバーセキュリティ態勢の強化に継続的に取り組んでいる。一方、グループ・グローバルでの一元的な管理態勢や脆弱性対応に改善の余地があり、継続的な改善・高度化に期待 ②有事のサイバー対策 ➢ 中小金融機関等 ✓ 多くの金融機関がコンチプラン等の見直しや社内外の情報連携強化に向けた対応を実施し、演習を通じて対応態勢を改善。一方、インシデント対応時における委託先との連携や顧客対応等が不十分、インシデント対応に必要な人員が確保できていないなどの課題が認められ、対応能力の向上を図っていく必要 ➢ 大手金融機関 ✓ 「合同演習」への参加を通じて、大規模なインシデントに対する我が国金融システム全体の対応能力を向上。「脅威インテリジェンス」の活用など、TLPTの深度を更に高めていく必要

金融分野のサイバーセキュリティレポート（令和元年６月）の概要

事項	取組内容	結果（概要）
(5) 情報共有の枠組みの実効性向上	◆金融ISAC等の情報共有機関を活用した「共助」の意義について機会を捉えて周知するとともに、地域内の情報共有の推進 ◆FISC主催の「サイバーセキュリティワークショップ」に当庁からも講師を派遣	✓金融ISACの加盟金融機関数は着実に増加。特に新たに導入されたトライアル会員制度は、多くの中小金融機関の「共助」参加への第一歩として機能 ✓FISC主催のワークショップに関して、信金・信組や地域証券の参加が増えるなど相応にサイバーセキュリティ対策への関心や「共助」の意識に高まり。一方で、極端に参加が少ない地域もあり、「共助」に対する意識に差
(6) 金融分野の人材育成の強化	◆財務（支）局とも連携し、金融機関の経営層向けセミナー等を開催	✓財務局主催のセミナーやワークショップを開催し、経営層の意識改革を促した。今後、こうした取組みを他の地域にも展開していくことが重要 ✓2020年東京大会に向けて、経営層のリーダーシップの下、サイバーセキュリティに係るリスクを重大なビジネスリスク・コーポレートリスクの一つとして捉えて取組みを進めることが重要

3. 金融庁における今後の取組み

➢ デジタライゼーションの進展により、金融機関のビジネスモデルの革新、プラットフォーマーと呼ばれる非金融プレイヤーの参入など、金融分野を取り巻く環境は急速に変化。また、サイバー攻撃が一層複雑化・巧妙化する中、今後「2020年東京大会」などの国際的なイベントを控え、当局として、金融業界全体のもう一段のサイバーセキュリティ対策の強化を図っていくため、以下の取組みを重点的に推進していく

□デジタライゼーションの進展を踏まえた対応

- 金融機関の規模・特性を踏まえつつ、デジタライゼーションの進展状況等の把握に取り組む。 また、非金融プレイヤーを含む様々な主体から積極的に情報を収集し、金融分野に対してサイバーセキュリティの観点から必要な対応をプロアクティブに促していく

□2020年東京大会に向けた対応

- 2020年東京大会に向けて、実態把握や対話等を通じた各金融機関のサイバー対策の強化、脆弱性診断・TLPTや演習等を通じたサイバー 対策の実効性向上に取り組む
- 「サイバーセキュリティ対策関係者連携会議」等を活用し、金融ISACやFISC等とともに、金融分野における大規模インシデントへの対応等への態勢強化を推進

資料２－２

サイバーセキュリティ対策情報開示の手引き（概要）

総務省　サイバーセキュリティ統括官室

令和元年　7月

サイバーセキュリティ対策情報開示の手引きについて

■総務省では、平成29年12月より、サイバーセキュリティタスクフォース（座長：安田　浩　東京電機大学　学長）の下で「情報開示分科会」（主査：岡村久道　英知法律事務所 弁護士）を開催。同分科会において、民間企業のサイバーセキュリティ対策の情報開示に関する課題を整理し、民間企業における サイバーセキュリティ対策の情報開示を促進するために必要な方策等について検討。

■今般、検討結果を踏まえ総務省において民間企業にとって参考となり得る情報開示の事例等をまとめた「サイバーセキュリティ対策情報開示の手引き」（案）を作成し、意見公募を経て令和元年6月に公表。

背景

✓ サイバー攻撃が深刻化する中、民間企業においてサイバーセキュリティ対策は重要な経営課題となっているが、企業としての社会的責任を果たしステークホルダーからの信頼を得るためには、**サイバーセキュリティ対策の実施のみならずその内容について適切な情報開示が重要。**

目的

✓ 民間企業による**サイバーセキュリティ対策**やその対策の**情報開示の重要性**の認識を促進。

✓ 民間企業にとって参考になり得るような**既存の情報開示の実例**を**事例集として**示す。

活用主体

✓ **サイバーセキュリティ対策の情報開示**に一定の関心のある民間企業の開示の実務担当者等を想定。

対象とする情報開示

✓ **開示書類**を通じた情報開示を取り扱う。

✓ 開示書類の読み手は、**投資家、融資元、顧客・契約者・取引先、従業員、競合他社等を含む、社会全体の広範なステークホルダー**を想定。

ICT利活用の進展

- 今日の社会・経済において、ICT（情報通信技術）の利活用は不可欠であり、様々な産業でデータの収集・分析・活用が進み、高付加価値化が進んでいる。
- 我が国が目指すべき社会像としてのSociety5.0を迎え、今後、サイバー空間とフィジカル空間の一体化が一層進展することが想定される。

ブロードバンド化

通信ネットワークは
ブロードバンドサービスが幅広く
普及し、社会に必要不可欠
な基幹インフラとなっている。

超高速ブロードバンド整備率
固定系：99.2%　移動系：99.8% (2018年時点)

モバイル化

スマートフォンの普及に伴っ
てモバイル化が進み、企業
活動や生活の隅々にまで
ICTの利活用が浸透し
始めている。

モバイル契約者数：1億8千万件 (2018年時点)

デジタル経済の発展

クラウド化

クラウドサービスが普及し、
各ユーザがネットワーク経由
で様々なサービスを安価で
利用できるようになっている。

クラウドサービス利用企業の割合：57% (2017年時点)

IoT化

IoTを活用した既存の
ビジネスモデルなどの
高付加価値化により、
企業の競争力が差別化
されていくことが想定される。

世界のIoT機器数：275億個 (2017年時点)

サイバーセキュリティリスクの増大

- サイバー攻撃の手法は多様化しており、その被害の種類も、個人情報の漏えいからランサムウェアやDDoS攻撃等によるシステムの停止に至るまで多岐に渡る。
- ICTの利活用が進み、あらゆる組織・人・物が情報通信ネットワークでつながる社会になると、「被害のチェーン」が情報通信ネットワークを介して発生する可能性があり、サイバーセキュリティ対策は企業の社会的責務となりつつある。

サイバーセキュリティリスク ＝ インシデントの影響の大きさ × 発生確率

→ 社会全体がICTに依存する中でサイバーセキュリティリスクが増大

被害の例：

個人情報の漏えい

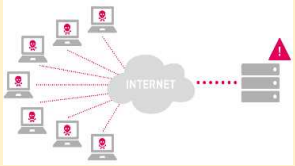
日本年金機構において、不審な電子メールに添付されたファイルを開封した職員のPCがマルウェアに感染。100万人以上の個人情報が流出。

ランサムウェアによるシステム停止

WannaCryが世界150か国30万台以上のPCに感染。データを使用不能にした後、身代金にビットコインを要求。多数企業の情報システム等の稼働に大きな影響。

DDos攻撃によるシステム停止

マルウェアに感染した10万台を超えるIoT機器からDyn社のシステムに対し大量の通信が発生。Dyn社のDNSサービス上の多数大手インターネットサービスなどに影響。

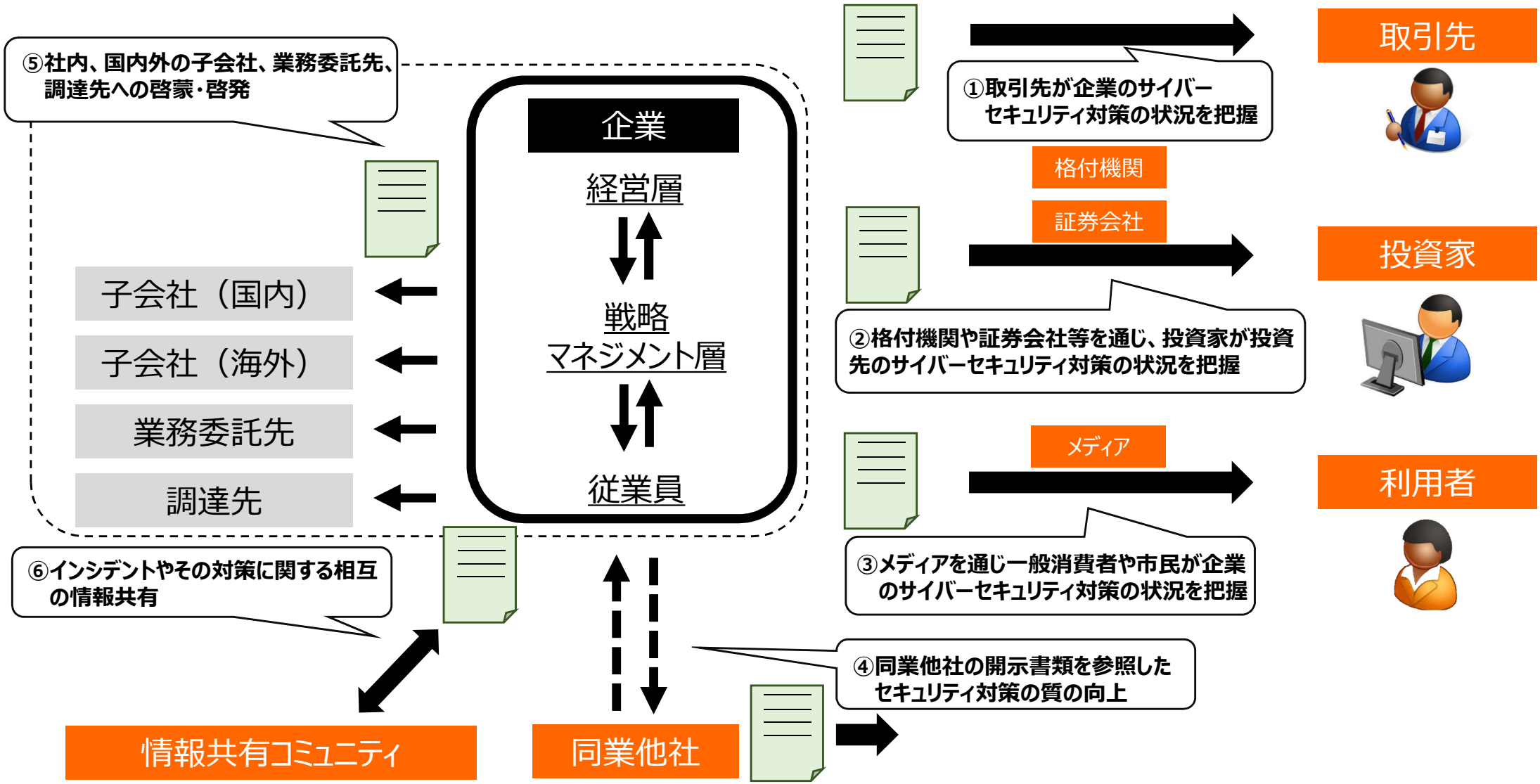


現代の生活やビジネスは各種情報・取引のネットワークに依拠しており、
ある企業の被害が別の企業の被害の起点となる「被害のチェーン」が生じるおそれがある。

サイバーセキュリティ対策は企業の社会的責務となりつつある。

企業をとりまく様々なステークホルダーとサイバーセキュリティ対策の情報開示

- 取引先や投資家、利用者等のステークホルダーへの説明責任を果たすため、サイバーセキュリティ対策の情報開示が重要。
- 同業他社との比較やコミュニティでの情報共有、社内、グループ内、業務委託先、調達先への啓蒙を通じ、サイバーセキュリティ対策の向上に資する。



「サイバーセキュリティ対策情報開示の手引き」の内容・構成について

本編　サイバーセキュリティ対策情報開示の手引き

1．本手引きの趣旨・目的

【内容】
- ✓ サイバーセキュリティリスクの増大と対策の必要性
- ✓ サイバーセキュリティ対策の情報開示の意義
- ✓ 本手引きの目的、想定参照主体、及び内容・構成等

2．情報開示の手段

【内容】
- ✓ 代表的な開示書類の紹介

3．企業における情報開示の在り方

【内容】
- ✓ 企業において実施されるのが望ましいサイバーセキュリティ対策
- ✓ 開示にあたってのポイントと記載例

4．今後の方向性について

【内容】
- ✓ 手引きの改定の在り方等の今後の方向性

参考資料①　関連施策等の紹介

【内容】
- ✓ 本手引きに関連した様々な施策やガイドライン等について紹介

参考資料②　開示書類の事例集

【内容】
- ✓ サイバーセキュリティ対策の情報開示にかかる実際の開示書類の例について紹介

ステークホルダーと情報開示の関係性

企業（群）

- 経営層
- 戦略マネジメント層
- 従業員
- グループ会社
- 外部委託・調達先

企業がとるべき対策

①サイバーセキュリティ対応方針策定
②経営層によるリスク管理体制の構築
③資源（予算、人員等）の確保
④リスクの把握と対応計画策定
⑤保護対策（防御・検知・分析）の実施
⑥PDCAの実施
⑦緊急対応体制の整備
⑧復旧体制の整備
⑨取引先・委託先やグループ単位のセキュリティ対策
⑩情報共有活動への参加

ステークホルダー

- 取引先
- 情報共有コミュニティ
- 証券会社 → 投資家
- メディア → 利用者
- 悪意の攻撃者
- 同業他社

：NDAなどを締結した関係者間でのより密度の濃い情報提供・共有

：不特定多数の者に向けた開示書類による情報開示

サイバーセキュリティ対策の情報開示のポイント

■ サイバーセキュリティ対策に関する情報開示は、例えば以下の性質を満たすのが望ましいと考えられる。

①目的適合性	✓ 記載事項の決定にあたっては、ステークホルダーへの説明責任を果たすために開示を行うという目的を踏まえること。 ✓ 以下の②～⑤を踏まえつつ、ステークホルダーにとって有益と思われる情報を提供すること。
②表現真正性	✓ 自社のサイバーセキュリティ対策について、真実を忠実に表現すること。 ✓ 情報の完全性、中立性、合理性を可能な限り確保すること。
③比較可能性	✓ 同業種・同規模間、同じ企業の異時点間等の一定の範囲で比較可能にするための基礎となる情報を提供すること。 ✓ 定量的な情報や、対策の有無が直接記載の有無につながるような情報など、客観的な評価が可能な情報を記載すること。
④理解容易性	✓ 読み手に特別な専門知識がなくても理解できるよう、簡潔かつ明瞭な表現で十分な情報を記載すること。 ✓ 必要に応じて専門用語に注釈等を付すこと。 ✓ 概念図や写真等を活用し、読み手に受け入れやすいものとすること。
⑤適時公表性	✓ 社会的に大きなインシデント等の発生後や新たな法規制の導入など、ステークホルダーの関心があるタイミングで適切な情報を速やかに公表すること。

経済産業省

資料２－３

経済産業省におけるサイバーセキュリティ対策強化のための各種取組

経済産業省　商務情報政策局

サイバーセキュリティ課

１．ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第1版公開

２．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

３．サイバーセキュリティお助け隊

2．①ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（第1版）

- 産業サイバーセキュリティ研究会WG1（制度・技術・標準化）の下のビルSWGにおいて、ビルの管理・制御システムに係る各種サイバー攻撃のリスクと、それに対するサイバーセキュリティ対策を整理し、ビルに関わるステークホルダーが活用できるガイドラインを作成。**6月17日付で第1版を公開**。

目次

（非公開の部分）

主に教育・啓発的内容
・なぜビルのサイバー対策が必要か？
・誰が考えるべきか？

主にガイドラインの作り／考え方
・対象システムのモデル
・対策を導き出す思考アプローチ

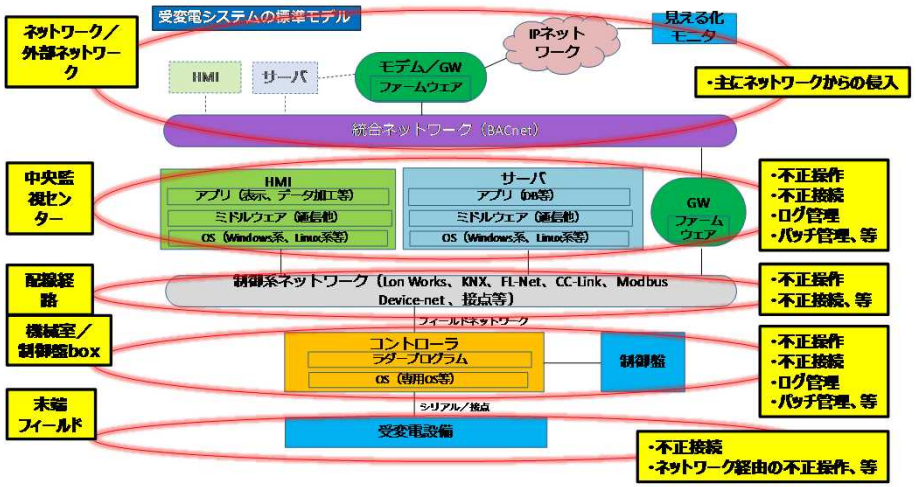
対象ごとの考え得る**インシデント、リスク源、対策（ポリシー）**をワンセットで記載

さらに詳細な対応を、**ビルのライフサイクルのそれぞれの場面にブレークダウン**（別表としてインデックス化）

実装レベルの対策（対策の具体的解説や、実際の対策事例）は、関係者のみで共有

1．②ガイドライン第1版の概要

場所→場所に置かれる機器→機器に想定されるリスク という流れで整理



ガイドラインの構成：対象とした場所及び機器の一覧、それぞれへの対策要件

- **場所及びその場所に設置される機器等を対象に、想定されるインシデントとリスク源を整理し、その対策をポリシーレベルで整理**

場所によらない全体的事項をリストアップ

場所及びその場所に設置される機器をリストアップ

4.1 全体管理		
1.	構成管理／管理情報	
2.	バックアップデータ／事業継続	
3.	会社／要員の管理	
4.	体制構築等	
4.2 機器		
1.	ネットワーク（クラウド、管理系IT、BACnet）	
	10	ネットワーク
	11	クラウドサーバ・Webサーバ
	12	管理系端末
	13	外部接続用ネットワーク機器（FW、ルータ）
	14	ビルシステム間相互接続
2.	防災センター（中央監視室）	
	20	防災センター（中央監視室）
	21	操作盤HMI
	22	保守用持ち込み端末
	23	複合NWにつながるネットワーク機器（FW、ルータ、SW）
	24	システム管理用サーバ（ビルシステム主装置）
3.	機械室／制御盤ボックス	
	30	機械室
	31	コントローラ（DDC、PLC等）
	32	ネットワーク機器（FW、ルータ、SW）
	33	ゲートウェイ機器
	34	各種制御盤・分電盤
4.	配線経路（MDF室、EPS、天井裏ラック）	
	40	MDF室／EPS／天井裏ラック
	41	内部に置かれたネットワーク機器（SW類）
5.	本端装置が置かれる場所	
	50	本端装置

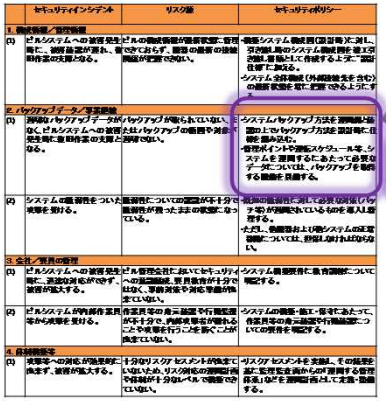
対象ごとに脅威や対策を整理

それぞれの場所、機器毎のインシデントやリスクへの対策をポリシーレベルで記述（要件レベルで記述）

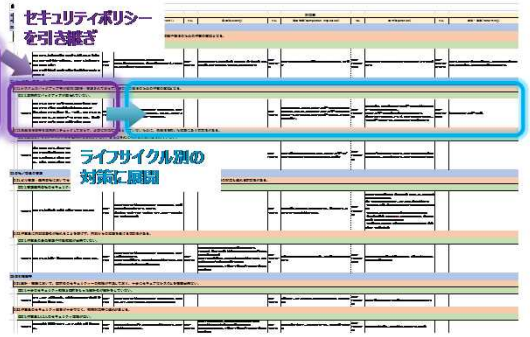
対策要件（ポリシー）からライフサイクル別対応策への展開

- **本編では対策のポリシーまでを記載、具体的対策は別紙としてインデックスと解説を記載**

要素別のリスク、対策ポリシーまでを記載



別紙としてライフサイクルの各フェーズ毎の具体的対策のインデキシング



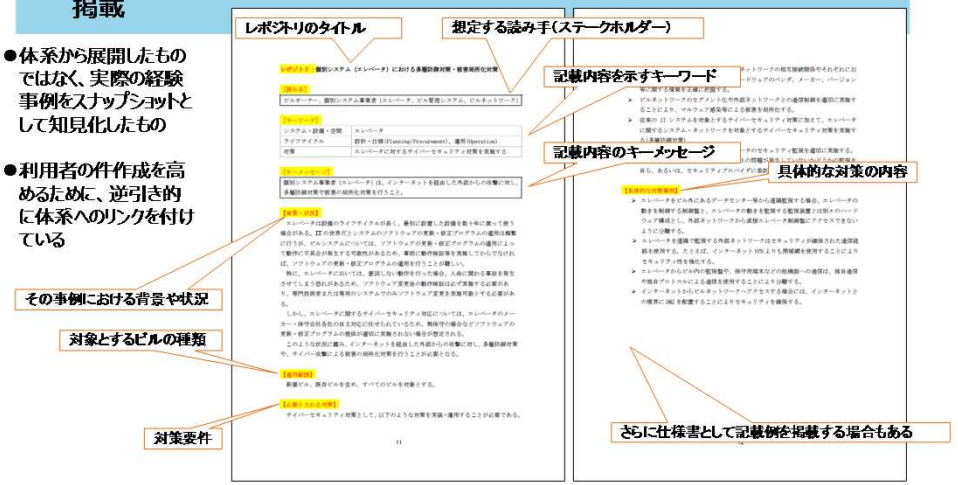
実効的な対策情報の蓄積（関係者のみ共有）

サイバーセキュリティ対策（プラクティス・レポジトリ：非公開）

- 別紙ではサイバーセキュリティ対策を体系的に紹介しているのに対し、プラクティス・レポジトリでは具体的対策を考える上で参考になる事例等を参考情報として掲載

●体系から展開したものではなく、実際の経験事例をスナップショットとして知見化したもの

●利用者の件作成を高めるために、逆引き的に体系へのリンクを付けている



2．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

- **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。
- 業界団体との連携も視野に入れつつ、**継続して収集し、2019年度も改訂を予定。**

第一章：経営とサイバーセキュリティ

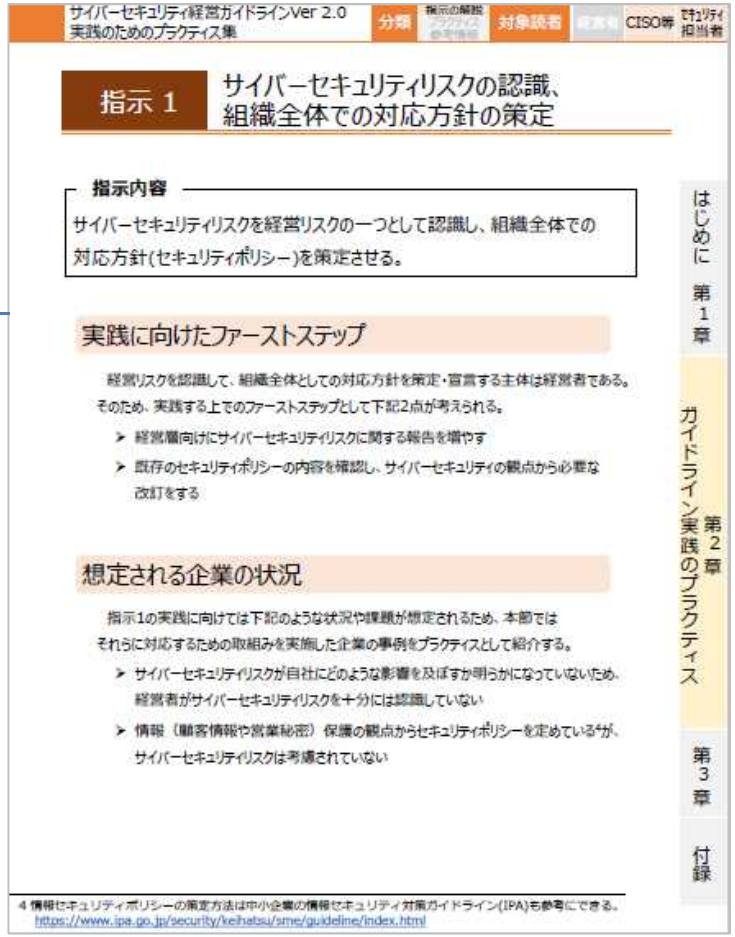
＜経営者、CISO等向け＞
なぜサイバーセキュリティが経営課題となるのか等を解説

第二章：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

＜CISO等、セキュリティ担当者向け＞
企業の具体事例をベースとした重要10項目の実践手順、実践内容、取り組む際の考え方を解説

第三章：サイバーセキュリティ対策を推進する担当者の悩みと解決のプラクティス

＜セキュリティ担当者向け＞
サイバーセキュリティ対策を実践する上での悩みに対する、企業の具体的な取組事例を紹介

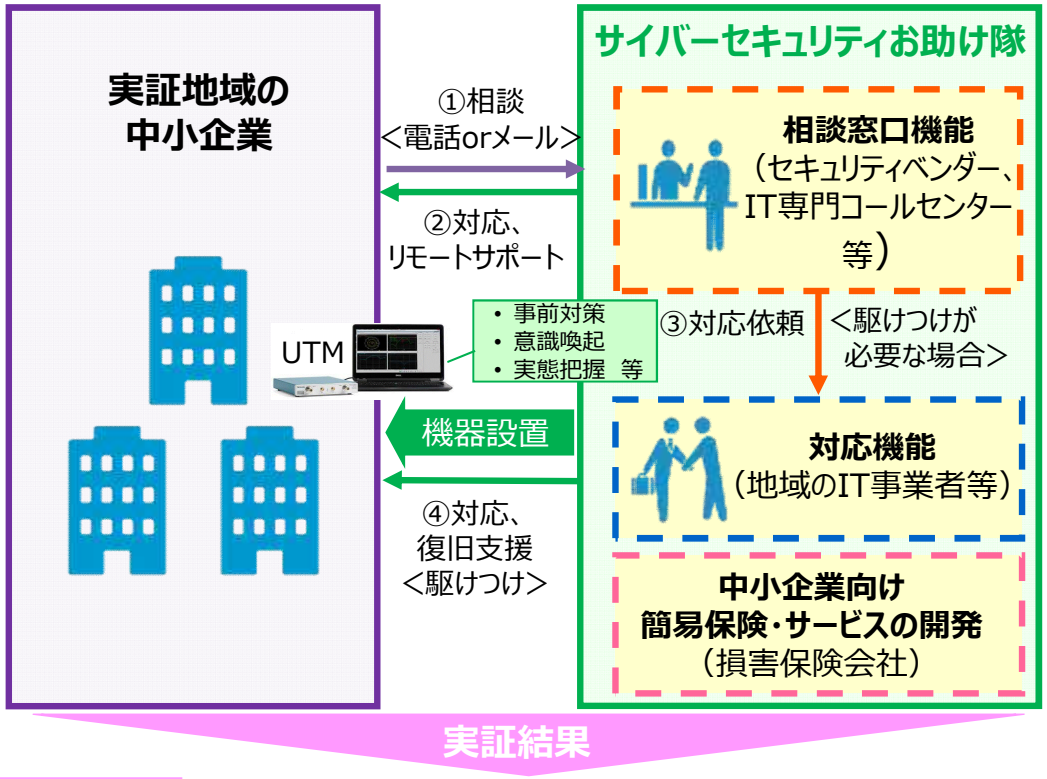


3．①サイバーセキュリティお助け隊

- 中小企業向けにサイバーセキュリティに関する支援の仕組みを新たに構築し、全国最大**8地域**を対象に地域の団体、企業等と連携した**実証**を行い、**サイバー攻撃の実態や対策のニーズを把握するとともに、中小企業の事前対策の促進、意識喚起を図る。**

＜実証地域＞

＜実証のイメージ＞



実証結果

中小企業　側

- 自社の攻撃実態等への気付き
- セキュリティ事前対策の促進
- 事後対応への意識向上　　等

保険会社、セキュリティベンダー　側

- 中小企業のセキュリティ対策状況の把握
- 中小企業の被害実態の把握
- 中小企業が求めるサービスの把握　　等

3．②（参考）全国での事業説明会を開催

- 中小企業のサイバーセキュリティ意識啓発も兼ねたサイバーセキュリティお助け隊の事業説明会を全国８地域で開催。
- IPAのWebページで各事業者の取組状況や事業説明会の詳細を公開中。

実証地域	実施者	開催日
岩手県、宮城県、福島県	株式会社デジタルハーツ	7/29(月)
新潟県	東日本電信電話株式会社	6/25(火)、6/26(水)、6/27(木)
長野県、群馬県、栃木県、茨城県	富士ゼロックス株式会社	7/24(水)、7/26(金)、その他調整中
神奈川県	SOMPOリスクマネジメント株式会社	6/14(金)
石川県	株式会社PFU	7/26(金)、8/28(水)、8/29(木)、8/30(金)
愛知県	MS&ADインターリスク総研株式会社	6/19(水)、6/24(月) ※7/25(木)事業開始説明会
大阪府、京都府、兵庫県	大阪商工会議所	7/5(金)
広島県	株式会社日立製作所	7/24(水)、7/29(月)

詳細情報・参加申し込みはこちら https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html