資料５－２

小売電気事業者のサイバーセキュリティの確保について

2020年 12月 17日

小売電気事業者のためのサイバーセキュリティ対策ガイドラインの作成の経緯

- 小売電気事業者においても、サイバー攻撃の脅威にさらされる可能性があり、対策を怠った場合、自社や電気の使用者の利益を損なうおそれがある。さらに、電力の安定供給に支障を及ぼす可能性がある。
- そこで、第9回SWGにおいて、小売電気事業者において必要なサイバーセキュリティ対策事項をとりまとめた**ガイドライン等を作成することが必要**とされ、本SWGの下に**小売電気事業者を構成員とした勉強会**を設置することとされた。
- 勉強会では、ガイドラインの内容について検討を行った。また、より詳細な議論を行うため、有志の勉強会構成員による作業会を開催し、記載すべき具体例等について議論を行った。

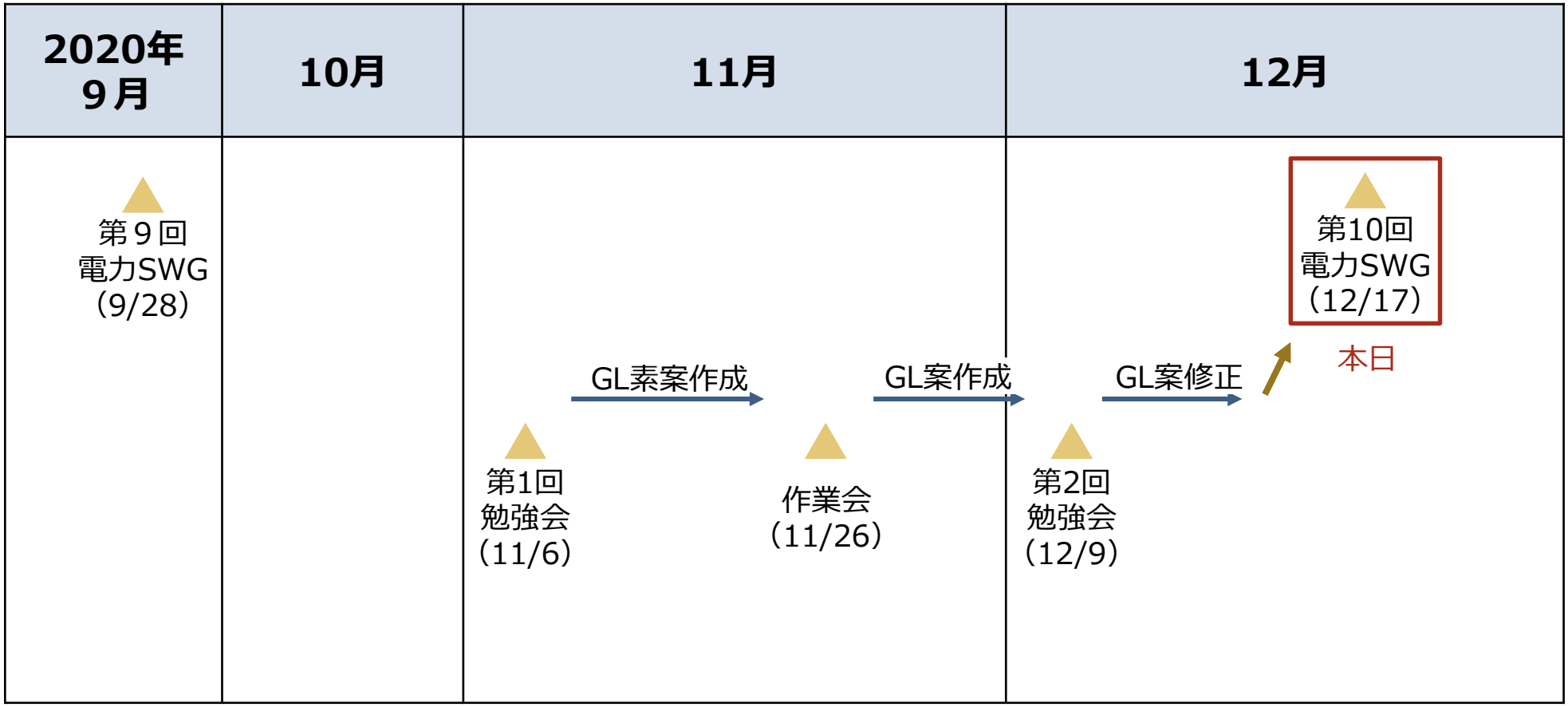
【勉強会出席者】
株式会社アイキューフォーメーション、イーレックス株式会社、出光興産株式会社、ＳＢパワー株式会社、株式会社エナリス、 NTTアノードエナジー株式会社、株式会社エネット、エネラボ株式会社、ＭＣリテールエナジー株式会社、岡山電力株式会社、オリックス株式会社、岐阜電力株式会社、ＫＭパワー株式会社、KDDI株式会社、五島市民電力株式会社、株式会社シグナストラスト、四国電力株式会社、自然電力株式会社、シン・エナジー株式会社、太陽ガス株式会社、株式会社ダイレクトパワー、大和エネルギー株式会社、中部電力株式会社、株式会社東急パワーサプライ、東京ガス株式会社、東京電力エナジーパートナー株式会社、長崎地域電力株式会社、長野都市ガス株式会社、日本テクノ株式会社、ふかやeパワー株式会社、富士山エナジー株式会社、武州瓦斯株式会社、北海道瓦斯株式会社、丸紅新電力株式会社、楽天モバイル株式会社、株式会社RenoLabo（計36社）

【勉強会オブザーバー（敬称略）】
有村　浩一（JPCERT/CC）、大友　洋一（電力ISAC）、門林　雄基（奈良先端科学技術大学院大学）、國松　亮一（JEPX）、桑名　利幸（IPA）、佐竹　潔泰（JEPX）、堀　英樹（OCCTO）、山田　博之（OCCTO）

【作業会構成員】
株式会社エナリス、株式会社エネット、岡山電力株式会社、オリックス株式会社、シン・エナジー株式会社、丸紅新電力株式会社（計6社）

（参考）ガイドラインの策定の過程

- ガイドラインの策定は、以下に示す過程を経て検討を進めてきた。



ガイドラインの記載方針について

- 第１回勉強会の中で、以下の理由から**サイバーセキュリティ経営ガイドラインの構成を踏襲**しながら、**小売電気事業者の特性等を反映したガイドラインとしてまとめる方針**を採用した。
  - 小売電気事業者の抱える課題は様々であり、包括的な視点から対策事項を示す必要があること
  - 小売電気事業者のシステムは情報システム中心の構成が標準的であること
  - 多くの小売電気事業者からサイバーセキュリティ経営ガイドラインを参照しているとの回答があったこと
  - 汎用ガイドラインの分野別拡張が有効に機能している事例があること（ビルセキュリティガイドライン等）
- また、小売電気事業者向けのガイドラインであることを踏まえ、
  - ✓ 小売電気事業者の事業特性やシステム構成を加味したサイバーリスクの例や、
  - ✓ 小売電気事業者の事業形態を踏まえた類型

  について記載すべきとの議論がなされた。
- さらに、多様な規模、事業形態が存在する小売電気事業者に資する内容とするため、
  - ✓ **勉強会の構成員やオブザーバーから具体的な好事例を収集した上で、**
  - ✓ 小売電気事業者において**共通的に活用されるべき対策をリスト的に記載する**とともに、
  - ✓ **「詳細対策事例」**として、**具体的な取組内容**について、**当該取組に至った背景**等も含めて記載することとした。

（参考）勉強会、作業会での具体的な意見の例と記載方針案について

	具体的な意見の例	ガイドライン記載方針
1	• 自社のセキュリティーポリシーの検討に活用したい • 組織的対策と技術的対策の視点が含まれるべき	• 複数事業者でポリシー検討に活用中であるサイバーセキュリティ経営ガイドラインの構成を踏襲し、網羅的な視点から整理
2	• 経営層への訴求や社内調整に本ガイドラインを使いたい • 電力分野におけるサイバー攻撃事例の情報がほしい	• 1章にガイドラインの位置づけ及び具体的な国内外のサイバー攻撃事例を記載することで、対策の必要性を強調 • また、別途、攻撃事例集を整理（資料５－４）
3	• 小売電気事業者独自の観点を盛り込んでほしい • 扱う情報や関係組織にも着目した分類を行ってほしい	• 2章に小売電気事業者の特徴と事業の類型の解説を記載。3章の対策には特に関わりの深い類型を紐づけ
4	• 対策リストとして活用したい	• 3章に事業者の対策事例をリスト化して記載
5	• 中小規模の事業者でも対応可能な水準のまとめがほしい • 幅広い事例の中で自社にあてはまる水準を検討したい	• これから対策に取り組む事業者にとっても活用しやすいような詳細事例解説を追記
6	• 個人情報保護の観点を重視して記載してほしい	• 特に低圧で重要な個人情報保護の観点からの対策は、ガイドライン3章においてもポイントを明示

小売電気事業者のためのサイバーセキュリティガイドラインの全体構成

- 勉強会、作業会の議論を踏まえ、ガイドラインの構成と各章の記載内容を以下のとおり整理した。

目次構成	記載内容
１．はじめに	**〇小売電気事業者へのサイバー脅威と本ガイドライン策定の背景** 経営層向けに対策の必要性を喚起するために、脅威動向の情報、ガイドライン策定の検討が適切な経緯で行われたことを記載 **〇本ガイドラインの構成と活用方法** ガイドラインの構成と想定読者、サイバーセキュリティ経営ガイドラインとの関係を記載。
２．小売電気事業者のサイバーセキュリティ対策における特徴	**〇小売電気事業者の企業環境とサイバーリスク** **〇小売電気事業者の情報システム構成の例** **〇サイバーセキュリティ対策における小売電気事業者の類型** 小売電気事業者の事業特性やシステム構成を加味したサイバーリスクの特徴と小売電気事業者の事業形態を踏まえた類型について記載。
３．小売電気事業者における重要１０項目の実践規範	**〇指示１～〇指示１０** サイバーセキュリティ経営ガイドラインと同様に、重要１０項目の指示事項のそれぞれについて、「**対策を怠った場合のシナリオ**」と「**小売電気事業者の対策実践例**」を記載した。 また、本ガイドライン独自の取組として、「**詳細対策事例**」として、より具体的な取組に至った背景やノウハウに関する記述を含む事例集を追記した。

（参考）詳細対策事例の一覧

指示事項別の詳細対策事例

- 指示１ サイバーセキュリティリスクの認識、組織全体での対応方針の策定
  ［最小限のセキュリティポリシーからの開始］［第三者認証取得を通じたセキュリティポリシーの精緻化］
- 指示２ サイバーセキュリティリスク管理体制の構築
  ［セキュリティ専任担当を配置できない状況での体制構築］［各部門のセキュリティ担当者による定期的な会議体の設置］
- 指示３ サイバーセキュリティ対策のための資源（予算、人材等）確保
  ［経営層への定期的な情報提供］［役割の付与による育成］
- 指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
  ［個人情報のリスク分析と対応］［サイバーセキュリティ保険への加入］［CPSFの活用］
- 指示５ サイバーセキュリティリスクに対応するための仕組みの構築
  ［システム更改のタイミングを有効活用する］［一般消費者向けサービスの不正アクセス対策］
  ［組織全体のセキュリティ基礎能力の底上げ］［CPSFの活用］
- 指示６ サイバーセキュリティ対策における PDCA サイクルの実施
  ［SECURITY ACTIONへの参加］［たすき掛け方式による内部監査の実施］
- 指示７ インシデント発生時の緊急対応体制の整備
  ［通常運用手順と緊急対応手順の関連付け］［特定の状況を想定したシナリオ型演習］
  ［机上演習等の活用］［インシデント報告時の具体的な連絡先の整理］
- 指示８ インシデントによる被害に備えた復旧体制の整備
  ［外部機関との予備のデータ送受信方式を用意する］［システムバックアップとリカバリテストの実施］
  ［外部サービスの停止を想定したBCP］
- 指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
  ［システムベンダとのセキュリティ要件の共有］［委託先検査方法の使い分け］
- 指示１０ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供
  ［公的機関の情報源からの情報収集］［情報共有コミュニティへの参加］

勉強会及び作業会での議論③ガイドラインの活用方針等

- 本ガイドライン案の活用方針や、今後への期待として、以下のとおり構成員及びオブザーバーから意見があった。

- 社内でのセキュリティ対策を検討する際の関係法令リストに本ガイドラインを加え、本ガイドラインと比較する形で自社の対策状況をチェックし、未対策の箇所は、リスクとコストのバランスを見ながら更なる対策を検討したい。
- 本ガイドラインを活用し、関連会社（代理店、BGメンバー）とのセキュリティ対策の共通基準を作ることを検討したい。
- 経営層へのサイバーセキュリティ対策の必要性の説明に活用したい。
- 今後のサイバーセキュリティの環境変化を踏まえ、随時見直しを行うべき。

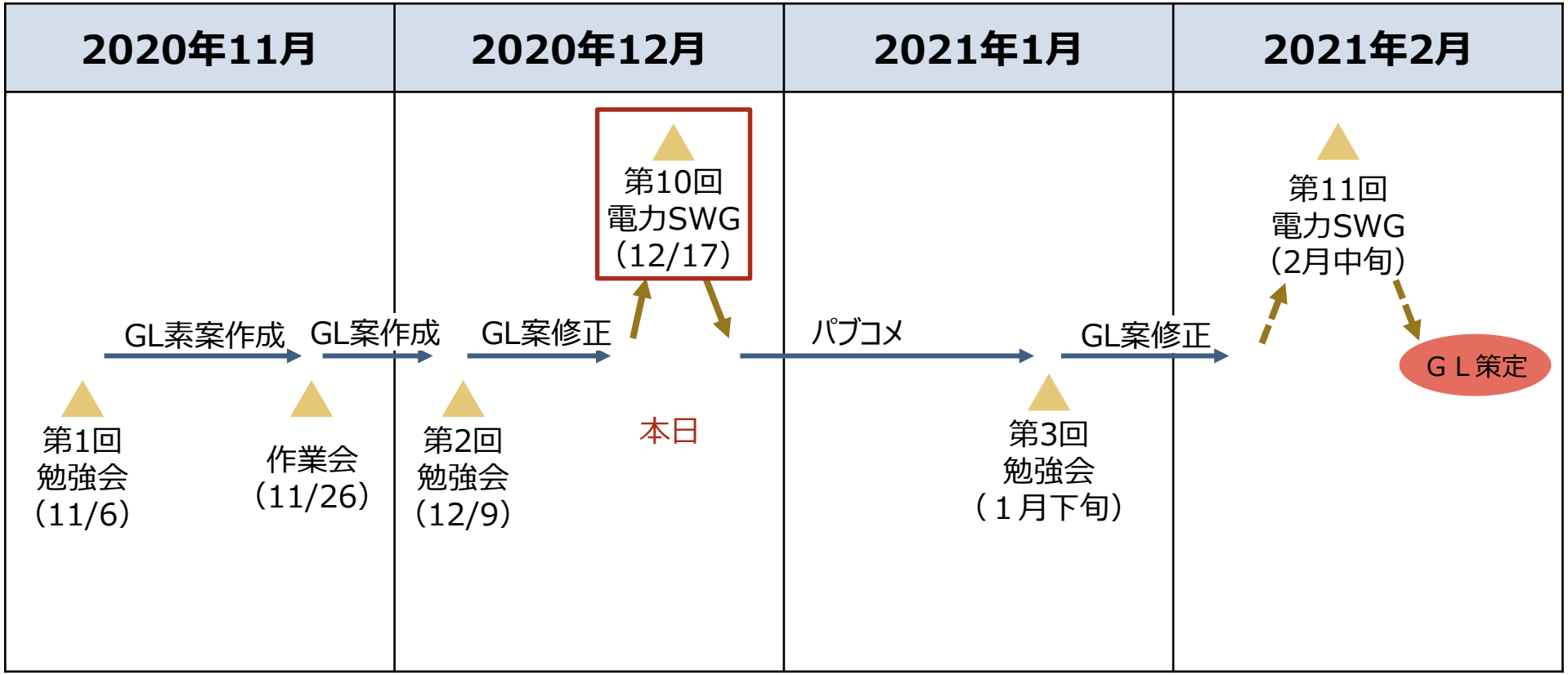
本日御議論いただきたいこと

- 小売電気事業者向けガイドラインにおける構成や各項目の記載方針、具体的な対策事例の内容は前頁までのとおり。これらの内容に沿ってガイドライン案（資料５－３）を作成した。
- **本日は、上記内容について御確認いただきたい。**
- 本SWG後の進め方については、**ガイドライン案についてパブリックコメントを実施**した後、**今年度中に本SWGの名義でガイドラインの策定・公表を目指す**こととしてはどうか。
- また、本ガイドライン策定後は、より多くの小売電気事業者に活用してもらえるよう、登録申請時の自己チェックリスト※で本ガイドラインを紹介するなど、周知に努めることとしてはどうか。

※申請書類に関する注意事項や登録後の各種義務や手続き、参考資料等をまとめたチェックリスト（年内公表予定）

- なお、本ガイドライン策定後もサイバーセキュリティを取り巻く環境は変化していくことを踏まえ、こうした変化の状況に応じ、**今後も本ガイドラインを見直していくこととしてはどうか**。

（参考）ガイドラインの策定に向けたスケジュール（案）



※第3回勉強会、第11回電力SWGの日程は、仮のものであり、現時点で未定。