経済産業省

資料６

電力分野における
サイバーセキュリティ対策について

平成２８年７月１日

資源エネルギー庁

背景・問題意識

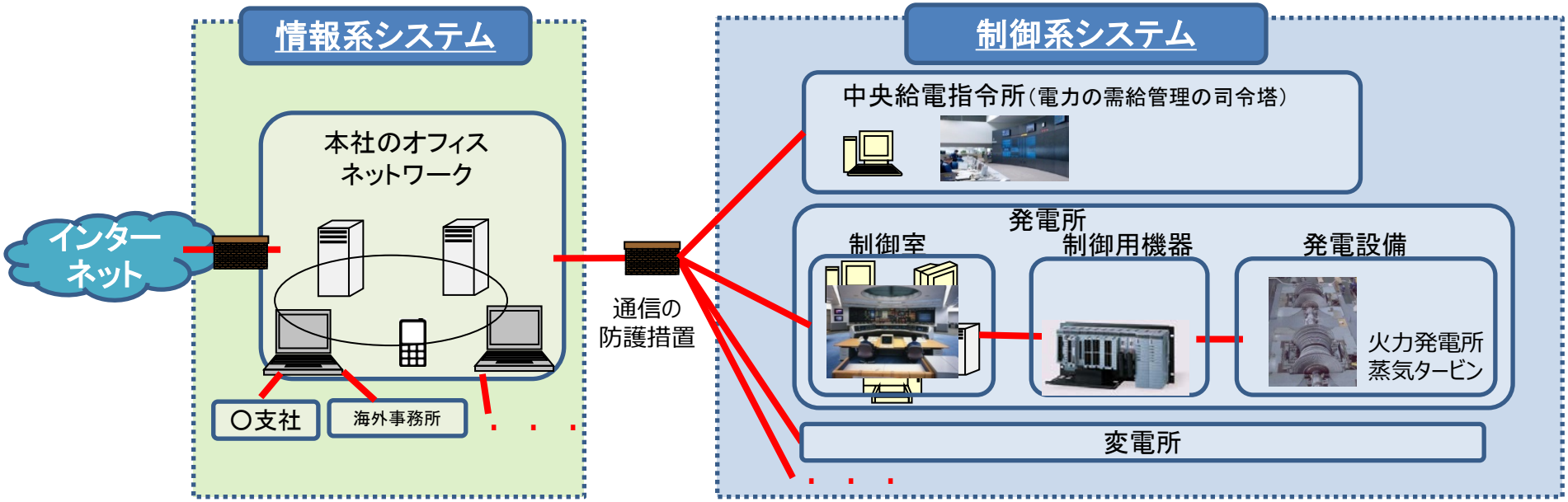
- 技術の発達やデジタル化の進展により、あらゆる分野でサイバー攻撃の脅威が高まる中、電力分野においてもサイバーセキュリティ対策の重要性がこれまで以上に高まっている。
- 加えて、自由化の進展により、コスト低減のための汎用技術の採用やシステムに接続する事業者の増加・多様化が見込まれ、サイバー攻撃のリスクが増大する可能性が高いことから、電力分野全体のサイバーセキュリティを高める取組が求められている。
- このため、昨年来、①セキュリティガイドラインの策定、②ガイドラインに基づく監査の実施（スマートメーターシステム）、③Ｇ７エネルギー大臣会合等を通じた国際的な連携強化等に取り組んできた。
- これらの取組を着実に進めつつ、今後、電力分野の更なるサイバーセキュリティ対策強化に向けて、金融や通信等の他の重要インフラ分野の取組にならい、サイバー攻撃等に関する情報共有や海外との連携等のための新たな体制を整備することとしてはどうか。（論点①）
- また、機密保持に十分な措置を講じた上で、電力の安定供給の中核を担う事業者を中心に、外部有識者も交え、各事業者の取組状況を客観的にレビューする場を設けることとしてはどうか。（論点②）

電力分野の課題：制御系システムの対策強化

2/9 第４回電力基本政策小委
事務局提出資料（一部加工）

- 産業用のシステムは、オフィスネットワーク等の情報系システムと、機器制御等を行う制御系システムとに大別され、電力供給を含めた重要インフラサービスは、基本的に制御系システムによってコントロールされる。　※制御系システムを有さない重要インフラ業種も存在
- 制御系システムは、情報系システムに比べ、①外部との直接の接続が少なく、②事業者毎に固有の仕様部分が多いといった特徴を有し、従来、詳細な内部仕様等を把握できない限り、外部からの攻撃が困難だった。
- しかし、標準技術・汎用製品利用の増加や外部ネットワークへの接続などにより、制御系システムについても外部からのサイバー攻撃の可能性は増しており、攻撃の脅威が存在することを前提とした対策が必要とされている。

＜情報系・制御系システムの模式図（電力分野の例）＞



（参考）ウクライナ西部で発生した大規模停電について

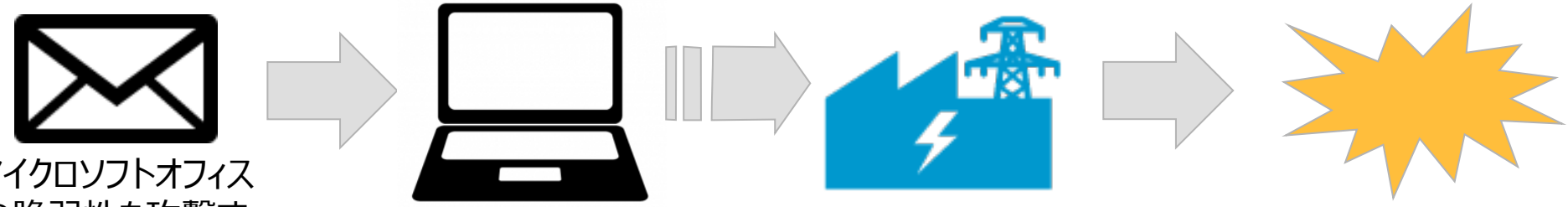
2/9 第４回電力基本政策小委
事務局提出資料

- 昨年１２月、ウクライナ西部数万世帯で、数時間に渡る大規模停電が発生。
- 同停電の原因はサイバー攻撃（マルウェア付きメールによる標的型攻撃が発端）と見られる。
- 同停電はサイバー攻撃によって実際に大規模な停電に至った初めての事例と見られる。

＜概要＞

発生日時：２０１５年１２月２３日
場所：イヴァーノ＝フランキーウシク州（ウクライナ西部）
関連するウィルス：Black Energy3（ロシアのハッカー集団sandwormが開発したとされるマルウェア）等
侵入先：州内電力会社（最大3社）関連設備
被害：リモートからのシステム制御を通じ、変電所（３０カ所）のブレーカー遮断とカスタマーサービスセンターへの問い合わせ遮断
備考：手動で復旧したため、早期（３－６時間）に停電は解消された。

＜停電までの経緯＞



マイクロソフトオフィスの脆弱性を攻撃するマルウェアが添付されたメール

電力会社（２～3社）の情報系PCに侵入

州内変電所（３０カ所）のブレーカー遮断

大規模停電発生

（出典：SANS, 各種報道等）

※現段階で発表・報道されている情報を集約したもの。詳細は現在国際的に調査中。

電力分野の最近の取組①：セキュリティガイドラインの策定

- 電力分野のサイバーセキュリティ対策強化に向けて、本年３月にスマートメーターシステムセキュリティガイドライン、本年５月に電力制御システムセキュリティガイドラインを日本電気技術規格委員会（JESC）が策定。
- 今後、これらのガイドラインを電気事業法下の技術基準及び保安規程に組み込むことにより、実効性を担保する予定。

＜スマートメータシステムセキュリティガイドライン＞

・平成27年2月　資源エネルギー庁を中心としたスマートメーター制度検討会セキュリティ検討WGにて、ガイドライン策定要件等をとりまとめ。

・平成28年3月　第85回JESC委員会にてガイドライン策定。

＜電力制御システムセキュリティガイドライン＞

・平成26年9月　日本電気技術規格委員会（JESC）で検討開始。

・平成27年6月　同委員会情報専門部会を新たに設置。

・平成28年5月　第86回JESC委員会にてガイドライン策定。

（共通事項）

■　セキュリティ管理組織の設置及びマネジメントシステムの構築、教育の実施等を記載。

機器	・セキュリティ仕様　・ファームウェアアップデート
通信	・通信プロトコル　・暗号　・ネットワーク分離
システム	・コマンド管理　・外部記憶媒体利用制限
運用	・管理者権限管理　・ログ取得　・データ管理
物理	・セキュリティ区画保護　・アクセス管理

設備・システム	・ネットワーク分離　・通信データ保護 ・不正処理防止　・アクセス制御
運用・管理	・セキュリティ仕様　・データ管理 ・管理者権限割当　・セキュリティパッチ

＋

安定供給等の観点から、システムの重要度を定義

↓

重要度に応じた追加的セキュリティ対策を提示

・ログの取得　・入退管理

電力分野の最近の取組②：ガイドラインに基づく監査の実施

- 本年２・３月、策定中のスマートメーターシステムセキュリティガイドラインに基づき、各電力会社はスマートメーターシステムのセキュリティ対策に関する内部監査を実施。
- 内部監査は、各社において日本セキュリティ監査協会が定める「情報セキュリティ監査人補」以上の資格保有者が対応。各社とも、監査結果として重大な指摘事項は無かった。
- 今後、スマートメーターシステムの運用が開始されたことも踏まえながら、リスク・重要度に応じた内部監査へと発展させていく予定。

2015年度の結果	今後の対応
○初年度のため、全項目を監査する必要があり、かつ、スマートメーターシステムの運用開始と時期が重なったため、負担感が大きかった。	○リスク分析を行い、各社の事情等も踏まえた上で、メリハリをつけた監査を実施。例えば、重要項目を深掘りし、そうでない項目は監査実施を数年に一度とする。
○事業部門（情報システム部門）が主となって監査を行った会社もあった。	○監査体制の客観性をより明確化すべく、「情報セキュリティ内部監査における監査人の独立性ガイドライン」を策定 ○日本セキュリティ監査協会と連携し、研修・資格取得等の機会を引き続き活用していく。

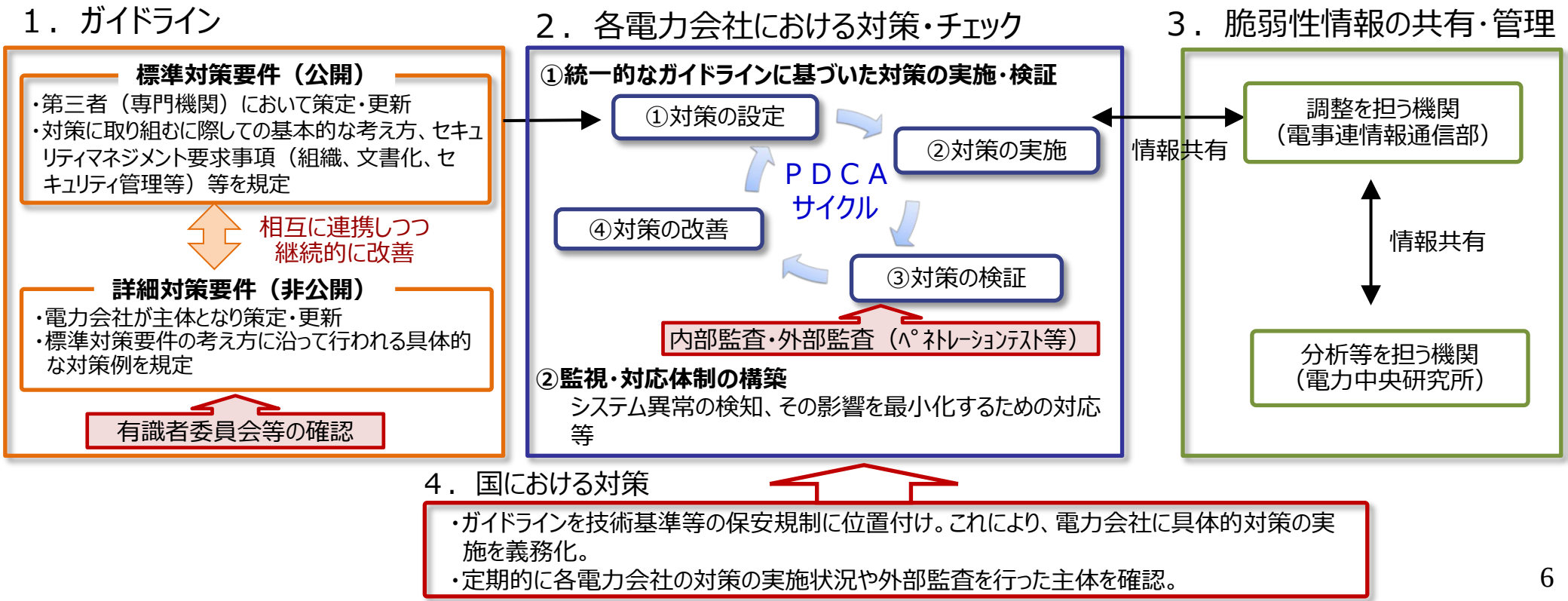
（参考）スマートメーターシステムのセキュリティ対策　（対策の枠組み）

1．**ガイドラインの策定**・継続的改善。

2．各電力会社において、ガイドラインに基づいた**対策の実施・検証（ペネトレーションテストを含む外部専門家による監査**等）、監視・対応体制の構築。

3．電力会社間における**脆弱性関連情報の共有・分析体制**の構築。

4．国において、ガイドラインを技術基準等の**保安規制に位置付け**。これにより、電力会社に具体的対策の実施を義務化。あわせて、定期的に各電力会社の対策の実施状況や外部監査を行った主体を確認。



（参考）スマートメーターシステムのセキュリティ確保に向けた電力会社の取組

	社内規定の整備	監査の実施		体制の構築		追加的な取組
		内部監査	ﾍﾟﾈﾄﾚｰｼｮﾝﾃｽﾄ（注）	セキュリティ運用・管理体制	システム監視・対応体制	
北海道	整備済（2016年3月）	実施済（2016年3月）	実施済（2016年3月）	構築済（2016年3月）	構築済（2016年3月）	教育を適宜実施
東北	整備済（2016年3月）	実施済（2016年3月）	実施済（2016年3月）	構築済（2016年3月）	構築済（2016年3月）	本店社員向け教育を実施
東京	整備済（2015年7月）	実施済(2016年3月)	実施済（2015年1月、2016年3月）	構築済（2015年7月）	構築済（2015年7月）	ｽﾏｰﾄﾒｰﾀｰｵﾍﾟﾚｰｼｮﾝｾﾝﾀｰを設置（24時間監視、社外人材活用） 有識者委員会の下、脅威分析、セキュリティ評価を実施済 訓練を実施済（2015年6月、9月、半期に1回程度予定）、教育を適宜実施
中部	整備済（2016年3月、2014年10月に一部整備済）	実施済（2016年3月）	実施済（2014年11月、2015年5月）	構築済（2014年10月。2015年11月全社大体制）	構築済（2014年10月）	ｽﾏｰﾄﾒｰﾀｰ制御管理ｾﾝﾀｰを設置（24時間監視、社外人材活用） 訓練を実施済（2016年3月、今後、年に1回程度予定）、教育を適宜実施
北陸	整備済（2016年3月改定）	実施済(2016年3月)	実施済(2016年3月)	構築済（2016年3月改定）	構築済（2016年2月改定）	訓練を実施（2016年2月） 教育を適宜実施
関西	整備済（2016年2月改定）	実施済（2016年3月）	実施済（2016年3月）	構築済（2012年6月）	構築済（2012年6月）	訓練・教育を定期的に実施
中国	整備済（2016年3月）	実施済（2016年3月）	実施済（2016年3月）	構築済（2016年3月）	構築済（2016年3月）	訓練・教育等計画を検討中
四国	整備済（2016年3月）	実施済（2016年3月）	実施済（2016年3月）	構築済（2016年3月）	構築済（2016年3月）	訓練・教育等計画を適宜実施
九州	整備済（2016年1月）	実施済（2016年2月）	実施済（2016年2月）	構築済（2016年2月）	構築済（2016年2月）	訓練・教育を定期的に実施することで社内規定に制定済み
沖縄	整備済（2016年3月）	実施済（2016年3月）	実施済（2016年3月）	構築済（2016年3月）	構築済（2016年3月）	訓練・教育の社内規定は整備済み。具体的な実施計画を検討中。

（注）システムに対する疑似的攻撃による評価

電力分野の最近の取組③：G7エネルギー大臣会合

- G7エネルギー大臣会合の準備会合付属会合として、本年3月、エネルギー分野（特に電力分野）におけるサイバーセキュリティ対策の強化をテーマに、各国エネルギー事業者、セキュリティ事業者、政府関係者、国際機関等によるワークショップを開催。
- エネルギー（電力）のサイバーセキュリティに関する各地域・国際機関の取組を互いに紹介しつつ、国際的な協力のあり方について議論を行った。
- ワークショップの成果も踏まえ、５月のG7エネルギー大臣会合では国際機関、民間機関同士の国際的な協力や、G7各国のエネルギーサイバーセキュリティの取組の共有等について、引き続き緊密に連携していくことが合意された。

Ｇ７エネルギー大臣会合声明（抜粋）

サイバーセキュリティは、エネルギーの供給確保を保証する上で重要な要素となっている。エネルギー・ネットワークがよりデジタル化し分散化したシステムに転換する中、新たなサイバーの脅威が増している。我々は、2015年11月にベルリンで、2016年3月に東京で開催されたG7エネルギー・サイバーセキュリティ・ワークショップの成功を歓迎する。我々は、新たなサイバーの脅威に効果的に対応し、重要な機能を維持するため、電力、ガス及び石油を含み、強靱なエネルギー・システムを促進することを確約する。

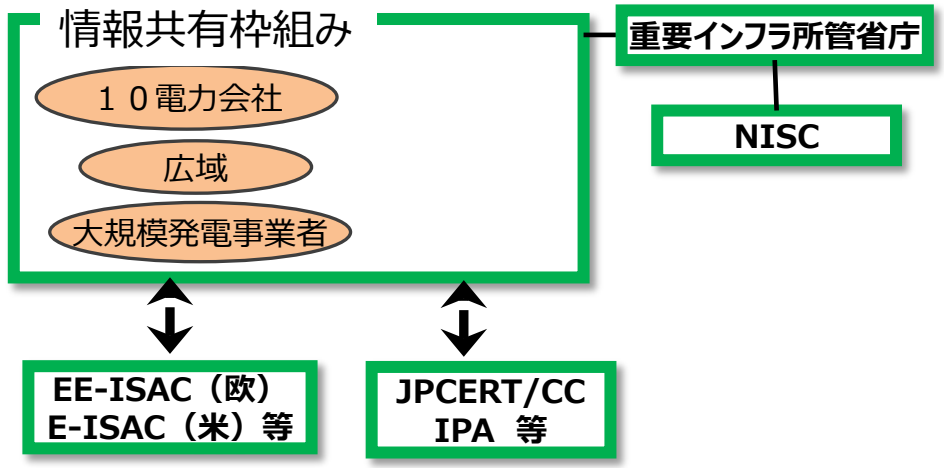
我々は、エネルギー分野のサイバーセキュリティに関して、サイバーの脅威に関する情報と知見の共有を円滑化し、このような脅威への対応をとるため、各国のコンピューター緊急時対応チーム（CERT）を含む専門家間の、地域及び分野を超えた連携を円滑化し、また、新たなサイバー関連の強化ツール及び技術の研究開発に関する継続的な対話を支持する。我々は、共通の要素及びベスト・プラクティスを特定するため、エネルギー安全保障政策の観点から、G7各国のエネルギー分野のサイバーセキュリティ対策の調査を行う。

論点①：電力分野における新たな情報共有体制の整備

- 従来、電力分野におけるサイバー攻撃情報等の情報共有は、独占的に電力供給を担う電力会社10社を中心として行われてきた。
- しかしながら、電力自由化の進展により新規参入者が増加し、10電力会社のみで電力分野のサイバーセキュリティを確保することはより困難となっていくことから、金融や通信等の他の重要インフラ分野の取組にならい、**業界大のサイバーセキュリティ対策強化に向けて、新たな体制を整備することとしてはどうか。**
- 具体的には、電力の安定供給の中核を担う事業者が参画する組織（電力ISAC※）を新たに整備し、①サイバー攻撃やシステムの脆弱性に関する情報共有、②ベストプラクティスの共有、③海外との連携等を担うこととしてはどうか。

※ISAC：Information Sharing and Analysis Center

＜新たな情報共有体制のイメージ＞



（参考）他分野、諸外国のISACについて

＜金融ISAC（日本）＞

- 2014年発足の一般社団法人。会員数は200社以上。主要銀行の非公式枠組みから発展。
- 情報の共有（コレクティブインテリジェンス）と共通課題への対応策の検討（リソースシェアリング）の2つが活動の柱。米国の金融ISACとも連携（情報共有等）。
- 会員の位置づけ（正会員、準会員等）に応じた会費あり。

＜ICT-ISAC（日本）＞

- 2016年発足の一般社団法人。会員数は約30社。国内主要通信事業者の自主的枠組みから発展。
- 通信事業者に加え、放送事業者、ソフトウェアベンダーが参加。当面は会員間の情報共有がメイン。
- 会費あり。

＜米国電力ISAC（E-ISAC）＞

- 2000年に発足。北米電力信頼度協議会（NERC）に併設され、同協議会の会員がメンバーとなる。会員数1,900社以上。
- 電力分野のサイバー攻撃情報の収集と分析、分析結果の発信が主な活動。
- NERCの予算で運営されており、会費なし。

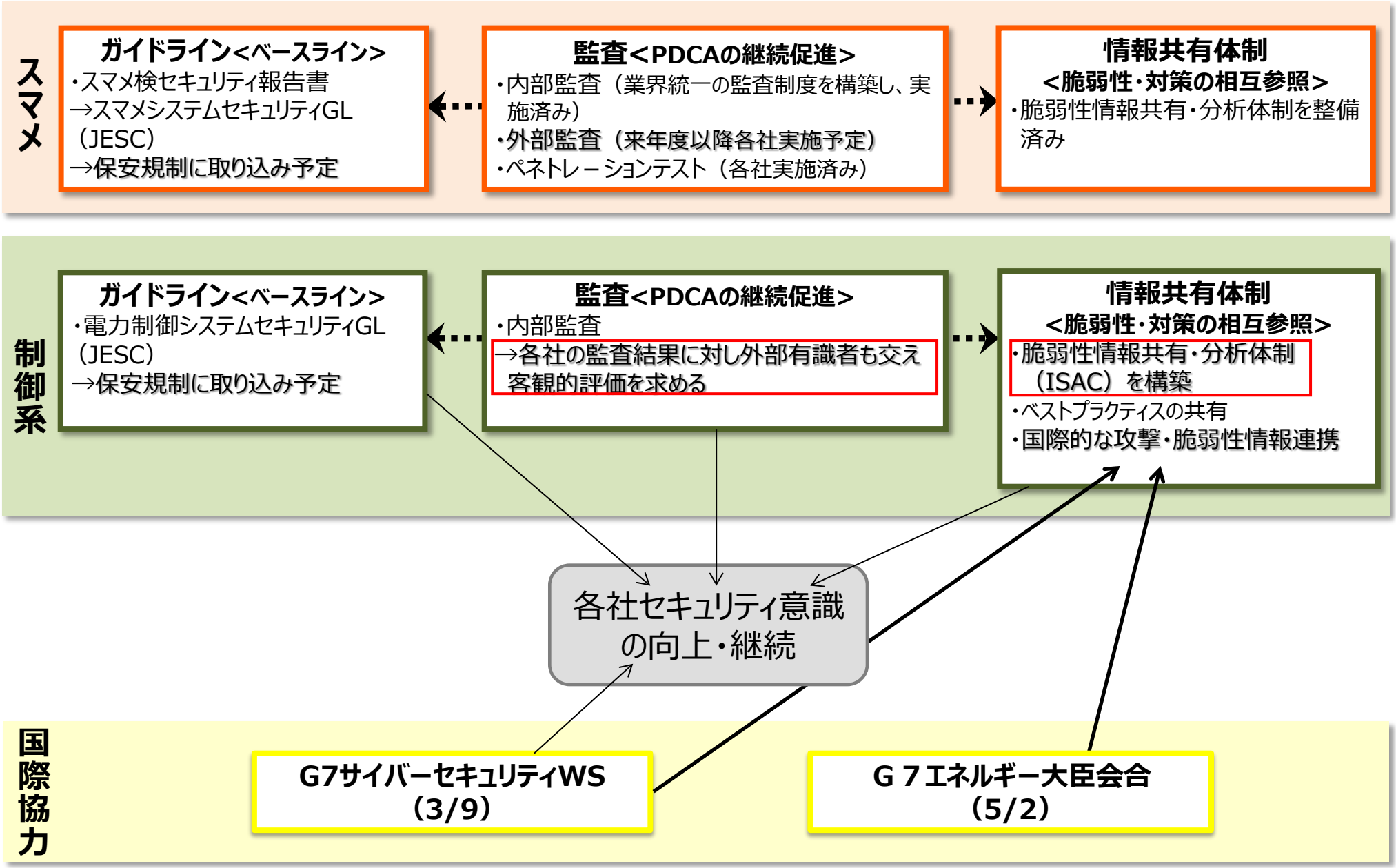
＜欧州電力ISAC（EE-ISAC）＞

- 2015年発足の自主枠組み。会員数約20社、ベンダーや研究機関も会員となる一方、これまでのところ電力会社の参加は極めて限定的。欧州委員会の予算事業から発展。
- 当面は会員間の情報共有がメイン。

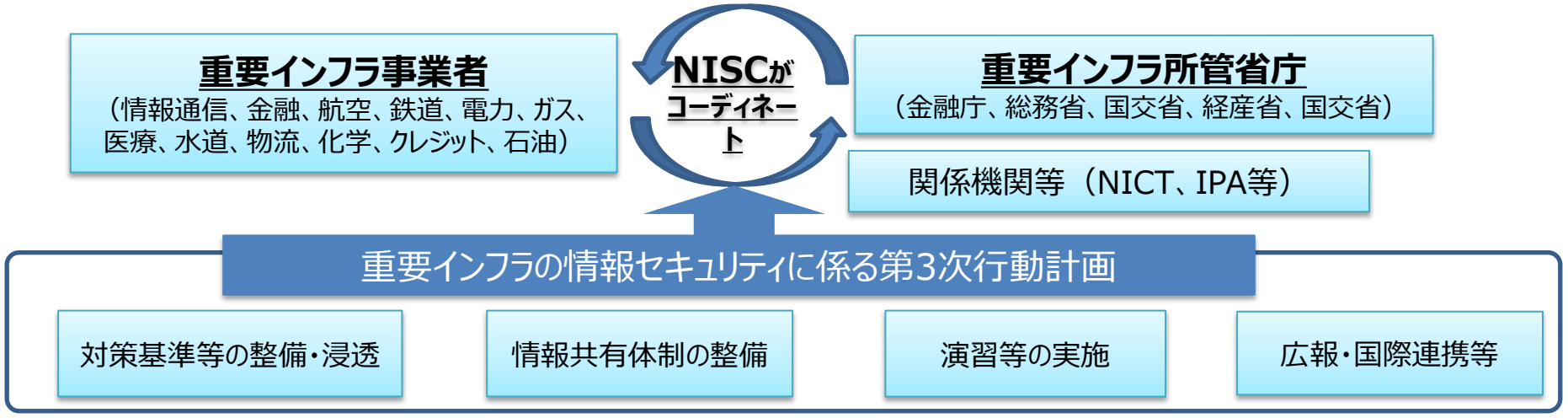
論点②：セキュリティガイドラインに基づく事業者の取組評価

- 本年策定された電力制御システムやスマートメーターシステムに関するセキュリティガイドラインでは、セキュリティマネジメントの一環として、各事業者が自らの取組状況について監査等を行うことが規定されている。
- ただし、セキュリティ専門資格者等の外部専門家による監査については、機密保持の観点や、制御系システムへの知見を有するセキュリティ専門家の不足への懸念等から、ガイドラインでは義務づけられていない。
- しかしながら、業界全体のセキュリティレベルを向上させていく上では、ガイドラインに基づく監査を自社内の取組にとどめることなく、各事業者が自らの取組を客観的に評価する機会を得ることが有益と考えられる。
- このため、機密保持に十分な措置を講じた上で、電力の安定供給の中核を担う事業者の重要なシステムを対象に、外部有識者も交え、各事業者が自ら評価した結果を客観的にレビューする場を設けることとしてはどうか。また、レビューによって得られた有意義な知見については、可能な範囲で共有し、業界としてのセキュリティ対策の向上に役立ててはどうか。

電力分野のサイバーセキュリティ対策の全体像（案）



（参考）重要インフラのサイバーセキュリティ対策の全体像



	対策基準等の整備・浸透	情報共有体制の整備	演習等の実施	広報・国際連携等
＜多くの業界＞	・任意の業界ガイドライン	・セプターの設定	・NISC演習への参加	（基本的にNISCの取組）
＜先進的取組＞	**・ガイドラインの業法への取り込み（通信・金融等）** **・監査（金融）**	**・ISACの設立（通信、金融）** **・海外との情報連携（金融）** ・J-CSIP等への参加	・CSSC等の演習に参加 ・業界独自の演習（通信、金融）	（・海外との情報連携（金融））
＜電力業界＞	・JESCガイドライン **・保安規制への取り込み** **・内部監査・外部有識者評価**	・電力セプターの設立 **・電力ISACの設立** **・海外との情報連携（EE-ISAC、E-ISAC等）** ・J-CSIP等への参加	・NISC演習への参加 ・CSSC等の演習に参加 ・電力業界での演習	（・海外との情報連携（EE-ISAC、E-ISAC等））

影字…電力業界で直近取組予定のもの

＜経産省系の独自取組＞
・IPAによる重要インフラのリスク分析
・CSSCによる演習（模擬訓練）
・J-CSIP（標的型攻撃情報共有）
・サイバーセキュリティ**人材育成・技術開発の中核機関の設立**　等

＜総務省系の独自取組＞
・**研究開発**（認証技術等）
・演習を通じたセキュリティ**人材育成**　等