『サプライチェーンのサイバーセキュリティ・リスク』(草案) の概要

2019 年 2 月 27 日
NEDO ワシントン事務所

北米電力信頼度協議会 (North American Electric Reliability Corporation：NERC) は 2019 年 2 月 6 日、電力系統に関し、電子アクセス制御・監視システム (Electronic Access Control and Monitoring Systems：EACMS)及び物理的アクセス制御システム (Physical Access Control Systems：PACS) に係るサプライチェーン・リスクを分析し、その対応策を提言した報告書『サプライチェーンのサイバーセキュリティ・リスク (*Cybersecurity Supply Chain Risks*)』(草案) [1]を発表した。

電力系統に係るサプライチェーンについて、連邦エネルギー規制委員会 (Federal Energy Regulatory Commission：FERC) は 2018 年 10 月 18 日にサプライチェーン基準を承認 [2] した際、将来的に EACMS 及び PACS を追加的に検討する必要性を提示。今回報告書は同提示に応えて作成されたもの。この中で、①EACMS 及び PACS をサプライチェーン基準に組み込むこと、及び、②基幹電力系統 (Bulk Electric Service：BES) サイバーシステムの調達プロセスを策定する際、第三者認証及びハードウェアやソフトウェアの安全配送といった業界ガイドライン及びプラクティスを参照すること、等を提言している。

＜注目点＞　今回報告書は、（サプライチェーン基準の発効が 2020 年 7 月予定のところ、）左記までに基準を随時、時点反映・具体化している一環。特に、EACMS 及び PACS に係る検討を進めており、具体的に「構成部品の確認、供給業者の特定、当該装置に係る特定リスクの評価」等、サプライチェーンに係る対応策を盛り込んでいる点が特徴。電力系統においては、従来の Utility に加え、再生可能エネルギーや蓄電池、それらを活用した各種サービスを担う第三者の参入増が見込まれる中、系統の脆弱性対策が喫緊の課題であり、左記に対して、FERC/NERC ともに検討を加速。

ここでは、現行のサプライチェーン基準の概要、及び、今回報告書のポイントを以下詳述する。

I. 現行のサプライチェーン基準

FERC は、サイバーセキュリティ・リスクへの電力業界の対応強化を目的として、昨年 10 月に 3 件の「重要インフラストラクチャー保護 (Critical Infrastructure Protection：CIP)」信頼度基準を承認。「サプライチェーン基準」は下記 3 件の CIP 基準の総称。

(i) CIP 基準 005-6 (供給業者リモートアクセス)

- 対象は、① 影響尺度 (Impact Rating)[3] が高程度の BES サイバーシステム、及び関連する保護されたサイバー資産 (Protected Cyber Assets：PCA)；② ルーティング可

[1] 同報告書の全文は、下記リンクの MRC Meeting Agenda Package の Item-09 (35 頁～73 頁) に掲載。
https://www.nerc.com/gov/bot/MRC/Agenda%20Highlights%20nad%20Minutes%202013/MRC_Meeting_Agenda_Package_February-6-2019.pdf

[2] Sidley Austin 法律事務所の『DATA MATTERS：Cybersecurity, Privacy, Data Protection, Internet Law and Policy』 (2018 年 10 月 29 日) によると、同基準の発効日は 2020 年 7 月 1 日

[3] 影響尺度のクライテリア (高、中、低) は、CIP-002-5 (BES サイバーシステム、及び、関連する BES サイバー資産の特定・分類) の Attachment 1 にて定義

能な外部接続 (external routable connection) を備えた、影響尺度が中程度の BES サイバーシステム及び関連する PCA
- 供給業者リモートアクセスの接続中セッションを監視する方法を 1 つ以上、及び、接続中セッションを停止する方法を 1 つ以上確立

(ii) CIP 基準 010-3 (ソフトウェアの信頼性及び信ぴょう性)
- 対象は、影響尺度が高・中程度の BES サイバーシステム
- 既存のベースライン構成 (baseline configuration) を変えるソフトウェアを実装する前に、責任当事者 (Responsible Entity) はソフトウェアの発信源及びその信ぴょう性を確認

(iii) CIP 基準 013-1 (サプライチェーンのリスク管理)
- 対象機関 [4]は、配電会社、需給制御機関 (Balancing Authority)、発電機の所有者及び運用者、信頼度コーディネーター、及び、送電網の所有者及び運用者
- 対象は、影響尺度が高・中程度の BES サイバーシステム
- BES サイバーシステムを計画・調達する際に、供給業者の製品・サービスがもたらし得るサイバーセキュリティ・リスクに対応するために講じるべき措置を確立。具体的には、以下 6 項目に係るサプライチェーン・サイバーセキュリティ・リスク管理計画書を作成及び遂行：
  - 供給業者は、自社が提供した製品又はサービスについて、サイバーセキュリティ・リスクがあると特定された事象を責任当事者に通知
  - 供給業者が提供した製品又はサービスについて、サイバーセキュリティ・リスクがあると特定された事象への対応調整
  - 離職等により、供給業者職員にオンライン又はオンサイトのアクセス権が打ち切られたことの通知
  - 提供した製品／サービスに関連する、既知の脆弱性の開示
  - 供給業者が BES サイバーシステム用に供給した全てのソフトウェア及びパッチの信ぴょう性及び信頼性の検証
  - 供給業者起動のインタラクティブなリモートアクセスの管理調整、及び、供給業者との拠点間 (system-to-system) リモートアクセスの管理調整

II. 今回報告書の提言（EACMS 及び PACS の追加）

1. サプライチェーンにおける BES サイバーシステムの危殆化がもたらし得るリスクを考慮し、影響尺度が高・中程度の BES サイバーシステムに関連する特定資産をサプライチェーン基準に含めるべく、同基準を以下のとおり改定すべき（EACMS 及び PACS に係る詳細は下表参照）。
   - EACMS、特に電子アクセス制御 (モニタリング及びロギングを除く) を提供する EACMS を統合

[4] カナダ原子力安全委員会が規制する施設のサイバー資産、孤立した ESPs 間の通信ネットワーク及びデータ通信リンクに関連するサイバー資産、連邦規制集 (CFR) 第 10 条第 73・74 章に準じるサイバーセキュリティに基づいて米国原子力規制委員会が規制するシステム・構造体・コンポーネント、及び、影響尺度が高・中の BES サイバーシステムを持たない責任当事者、等を除く

- 物理的アクセス制御 (警告発信、ロギングを除く) を提供する PACS を統合

	電子アクセス制御・監視システム (EACMS)	物理的アクセス制御システム (PACS)
定義	電子セキュリティ境界 (Electronic Security Perimeters：ESPs)[5]、又は、BES サイバーシステムについて、電子アクセス制御・監視を行うサイバー資産。例として、電子アクセスポイント、中間装置 (Intermediate Devices)、認証サーバー、セキュリティイベント監視システム、侵入検知システム等が挙げられる。	物理的セキュリティ境界 (Physical Security Perimeters：PSPs)[6] について、制御、警告発信、ロギングを行うサイバー資産。例として、認証サーバー、カードシステム、ID カード管理システム等が挙げられる。(但し、モーションセンサー、電子施錠メカニズム、ID カード読取り装置のように、PSPs 内に実装されたハードウェアや装置を除く)
BES リスク	1.大手供給業者が危殆化したネットワーク機器であることを知らずに供給。同機器が、影響尺度が高・中程度の BES サイバーシステムに電子アクセス制御を提供する EACMS へ不当にアクセスすることで、信頼性に広範な悪影響をもたらす可能性 2.上述の CIP 基準及び各機関の方針や手順といった技術的制御 [7]、更には EACMS のアーキテクチャや構成等の実験・検証によって、サプライチェーンの危殆化がもたらし得るリスクをある程度軽減可能であるものの、あらゆるリスクへの対応は不可。このため、調達・設置の際にはサプライチェーンの脆弱性を確認・評価することが重要	1.BES サイバーシステムへの物理的アクセスを制御・監視・記録するために様々な手法・システム [8]が使用されるが、これらは通常、第三者により提供されるため、サプライチェーンに入り込むセキュリティ侵害に対して脆弱 2.PACS の危殆化は、BES 運用に直接影響を与えるシステムへのアクセスを可能にし、BES の信頼性に広範な悪影響をもたらす可能性 [9] 3.上述の CIP 基準及び各機関の方針や手順 [10]、更には PACS のアーキテクチャや構成等の実験・検証によって、サプライチェーンのもたらし得るリスクをある程度軽減可能ながら、危殆化 PACS が原因となる悪影響を考慮すると、調達・設置する際にはサプライチェーンの脆弱性を確認・評価することが重要
対応策	1.サプライチェーン基準を改正して、影響尺度が高・中程度の BES サイバーシステムに電子アクセス制御を提供する EACMS を統合 2.基準改正までの暫定措置として、各当事者が EACMS 関連のサイバー資産を調達・設置する際に、下記要素を自主的に確認・評価： a. EACMS 構成部品の確認	1.サプライチェーン基準を改正して、影響尺度が高・中程度の BES サイバーシステムに物理的アクセス制御を提供する PACS を統合 2.基準改正までの暫定措置として、各当事者が PACS 関連のサイバー資産を調達・設置する際に、下記要素を自主的に確認・評価： a. PACS 構成部品 (サーバー、ワークステー

[5] BES サイバーシステムがルータブル・プロトコルによって接続されているネットワークを囲む論理的境界線 (logical border)
[6] BES サイバー資産、BES サイバーシステム、又は EACMS の取り付け場所を囲む物理的な境界線
[7] 多要素認証、強度なパスワードの導入、役割別のアクセス制御、認証・認可・報告サービスの活用、アクセス制御リストの導入、リモートアクセス・セッションの暗号化、データ及び管理トラフィック (management traffic) の為に安全性が保証された個別のバーチャル LAN 利用、等。
[8] カード・キー；特殊キー；警備員；バイオメトリック、キーパッド、及びトークン等の認証装置；警報装置、映像記録装置、及び人間によるアクセスポイント監視等の物理的アクセス監視方法；電子化したロギング、映像記録、手書きによるロギング等の物理的アクセス記録
[9] (i) 外的脅威の行使者が PACS の危殆化要因を外部からコントロールすることによって探知されぬままに、電力系統を管理又は運用するコントロールセンター他の施設への物理的アクセスを取得。かかる行使者が PSPs に侵入し、システム運用者を拘束、妨害、排除し、BES サイバーシステムを物理的に掌握してしまうというシナリオ、及び、(ii) PACS アクセス制御部品の悪用、劣化、又は破壊により、内部脅威の行使者が探知されぬままに BES サイバーシステムに対して有害な行動を起こすというシナリオ、等が考えられる。
[10] 厳格な運用又は手順制御、完全遮蔽の「六面」防衛線 (“six-wall” boundary) の導入、二種類以上の物理的アクセス制御の導入、等。

	b. 種類別に EACMS 装置供給業者の特定 c. EACMS の各種装置 (ファイアウォール、ルーター、スウィッチ等) が信頼性を守るために果たす役割の確認 d. 各種の EACMS 装置について、(i) 不正アクセスがあった場合に起こるリスク、(ii) 可能なリスク軽減環境、の確認 e. 各種装置がもたらす特定リスクの評価 f. 特定された各リスクへの対応・軽減戦略又は提言の策定 g. BES サイバーシステム調達プロセスに存在する EACMS リスクに対応する施策の統合、及び、確認されたリスクに対応する既存又は計画中の供給業者による軽減戦略・手順の確認	ション、カメラ等監視装置、アクセス制御サイバー資産のコンポーネント、モニタリング・コンポーネント、ロギング・コンポーネント等) の確認 b. 種類別に PACS 装置供給業者の特定 c. PACS の各種装置が信頼性を守るために果たす役割 (アクセス権の付与及びアクセス許可、検知、レスポンス、モニタリング、ロギング等) の確認 d. 各種の PACS 装置について、(i) 不正アクセスがあった場合に起こるリスク、(ii) 可能なリスク軽減環境、の確認 e. 各種装置がもたらす特定リスクの評価 f. 特定された各リスクへの対応・軽減戦略又は提言の策定 g. BES サイバーシステム調達プロセスに存在する PACS リスクに対応する施策の統合、及び、確認されたリスクに対応する既存又は計画中の供給業者による軽減戦略・手順の確認

2. 責任当事者は自発的に、影響尺度が低程度の BES サイバーシステムに対して CIP 基準 013-1 の要件 1 (サプライチェーン・リスク管理計画) を適用
3. 責任当事者は、保護されたサイバー資産 (PCA)[11] について、付加的なサプライチェーン保護の必要性を判断するために、自社の PCA をケースバイケースで評価
4. 責任当事者は、BES サイバーシステム調達プロセスを策定する際に、サプライチェーン・リスク管理に有効な業界アプローチを参照：
    - 第三者による供給業者の認証
    - ハードウェアやソフトウェアの安全配送
    - 開発対象の製品に特有なセキュリティ上の脅威を特定・分析する脅威モデリング (Threat Modeling)
    - サポートが終了したシステム又はオープンソース技術がもたらし得るリスクへの対処

III. 今後のプロセス

1. 2019 年 4 月に、同提言についての政策見解を集約
2. 2019 年 5 月 8 日に開催される NERC 評議員会の Standards Oversight and Technology Committee の会合で、NERC スタッフ報告書及び政策見解を審議

[11] 影響尺度が高の BES サイバーシステムの一部ではない電子セキュリティ境界 (ESP) 内においてルータブル・プロトコルを介して繋がっている 1 つ以上のサイバー資産