（別紙）

「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について（案）」に対する意見公募の実施結果について

No.	御意見の概要	御意見に対する考え方
1	小売電気事業者についてのものであるので、当然にあるかと思われた、主に顧客とのネットワーク経由での連絡等についての記述がほぼ無かったので、以下の意見を行う。 顧客との各種のネットワーク経由での連絡等（ホームページを通してのもの、電子メールを通してのもの等）においては、一般的なサイバーセキュリティについて、まず妥当かつ確立されたものを導入・実装していく事が重要であると考える。 HTTPS及びTLSは当然であるが、メールのTLS保護（SMTPoverTLS及びSTARTTLS。ネットワーク中を平文で重要情報を含むメールが行き来する事の無いように、また相手を認証しての通信が行われるようにするためにも、これは必須的に必要と考えられるものである。）及び電子署名（重要情報を含むメールには電子署名があるべきである。）、SSH（トンネル用ツールとしての利用を各所で行っていくと簡易にセキュリティレベルを大きく上げる事が可能と思われる。）の利用については確実に行っていくべきと考える。 （その様な事によって、各所でのユーザアカウントやパスワードの漏えいが少なくなり、またフィッシング的事態や盗聴の被害も減少する事になるかと思われる。また万が一の際の刑事捜査等においても不正アクセス関係の明確な犯罪行為の存在によって捜査・公訴が行いやすくなるかと考える。） これらについては、（有料となる認証局証明書の発行以外（※なお、現在では））およそ無料で可能となるソフトウェア的な手法となるもののはずだが、この様な低費用かつ妥当なセキュリティ関係措置が、地道に、確実になされていく事で、大きくサイバーセキュリティが向上するのではないかと考える。 また、ガイドラインにおいて、CSO、CISOの語句についての記述が無かったが、これらについては、市井における各種のWebサイトの記事との対応付けを行うためにも、記述を行っておく方が良いのではないかと思われた。 意見は以上である。	御指摘を踏まえ、需要家向けのポータルサイト等の通信の安全性の保護について記載させていただきます。 　また、本ガイドラインが参考としている「サイバーセキュリティ経営ガイドライン」における表現と整合をとりつつ、CISOについて補足の記載をさせていただきます。
2	「サイバーセキュリティー対策」が重要な構造と、私し個人は思います。例えばですが、「センサー技術、 ネットワーク技術、デバイス技術」から成る「CPS（サイバーフィジカルシステム）」の導入により、「ゼネコン（土木及び建築）、 船舶、鉄道、航空機、自動車、産業機器、家電」等が融合される構造と、私は考えます。具体的には、「電波規格（エレクトロリカルウェーブスペック）」及び「通信規格（トランスミッションスペック）」での「回線（サーキット）」の事例が有ります。（ア）「通信衛星回線（サテライトシステム）」における「トランスポンダー（中継器）」から成る「ファンクションコード（チャンネルコード及びソースコード）」のポート通信での「DFS（ダイナミックフレカンシーセレクション）」の構造。（イ）「電話回線（テレコミュニケーション）」における基地局制御サーバーから成る「SIP サーバー（セッションイニテーションプロトコル）」の構造。（ウ）「インターネット回線（ブロードバンド）」におけるISPサーバーから成る「DNSサーバー（ドメインネイムシステム）」の構造。（エ）「テレビ回線（ブロードキャスト）」における「通信衛星回線、電話回線、インターネット回線」の構造。具体的には、「方式（システムスペック）」での「回線（サーキット）」の事例が有ります。（ア）「3G（第3世代）」における「GPS（グローバルポジショニングシステム）」から成る「3GPP方式（GSM方式及びW-CDMA方式）」の構造。（イ）「4G（第4世代）」における「LTE方式（ロングタームエボリューション）」から成る「Wi-Fi（ワイアーレスローカルエリアネットワーキング）」の構造。（ウ）「5G（第5世代）」での「NR（New Radio）」における「MCA方式（マルチチャンネルアクセス）」から成る「DFS（ダイナミックフレカンシーセレクション）」の構造。具体的には、「情報技術（IT）」及び「人工知能（AI）」での「回線（サーキット）」の事例が有ります。（ア）クラウドコンピューティングでは、「ビッグデータ（BD）」から成る「データーベース（DB）」の導入により、ITネットワークの構造。例えばですが、ファイアーウォールにおける強化では、ルーターとスイッチを挟み込む様に導入する事で、「クラウド側（プロバイダー側）←ルーター⇔ファイアーウォール⇔スイッチ→エッジ側（ユーザー側）」を融合する事で、ハードウェアーの強化の構造。（イ）エッジコンピューティングでは、Web上における「URL（ユ ニフォームリソースロケーター）」での「HTML（ハイパーテキストマークアップラングエッジ）」から成る「API（アプリケーションプログラミングインタフェース）」に導入により、「HTTP 通信（ハイパーテキストトランスファープロトコル）」における暗号化によるソフトウェアーでの「HTTPS（HTTP over SSL/TLS）」の融合により、AIネットワークの構造。具体的には、「サイバー空間（情報空間）」及び「フィジカル空間（物理空間）」での「回線（サーキット）」の事例が有ります。（ア）「サイバー空間（情報空間）」では、「SDN/NFV」における「仮想化サーバー（メールサーバー、Web サーバー、FTP サーバー、ファイルサーバー）」から成る「リレーポイント（中継点）」での「VPN（バーチャルプライベートネットワーク）」が主流な構造。（イ）「フィジカル空間（物理空間）」では、「AP（アクセスポイント）」が主流な構造。要約すると、「ボット（機械における自動的に実行する状態）」による「DoS攻撃」及び「DDoS攻撃」でのマルウェアーにおける「C＆Cサーバー（コマンド及びコントロール）」では、「LG-WAN（ローカルガーブメントワイドエリアネットワーク）」を導入した「EC（電子商取引）」の場合では、クラウドコンピューティング及びエッジコンピーティングにおける「NTP（ネットワークタイムプロトコル）」の場合では、「検知（ディテクション）⇒分析（アナライズ）⇒対処（リアクションメソッド）」での「サイバーセキュリティー対策」が重要と、私は考えます。	今後の検討にあたり、参考とさせていただきます。