「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（個別編：空調システム）（案）」のパブリックコメントで寄せられた御意見に対する考え方

No.	提出者	提出意見		御意見に対する考え方
		該当箇所	意見内容	
1	企業	p5 「2.2. 実際のサイバー攻撃事例 この場合、空調システムを基幹ネットワークから切り離した状態 で、空調機能を単独で維持できることが重要となる。 　個別分散空調方式では、サイバー攻撃によってプロトコル変換器が攻撃され、空調システムとして正常動作しない場合を想定し、空調機を操作できるコントローラ等の別の手段を設計時に配慮しておくことが望まれる。」	「単独で維持」→「単独で手動運転」 「操作できるコントローラ等の別の手段」 　→「単独で手動操作できるコントローラ等の別の手段」	いただいた御意見も参考に、修正いたします。具体的には、空調システムをネットワークから切り離して独立して動作できるようにすることを求めているものであり、その趣旨の記述を追記します。一方、手動と言うとリモコン等で１つ１つの空調機を制御するという誤解を生じる可能性があるため、当初記述通りとします。 修正箇所：2.2の第2段落に「単独で」を挿入。
2	企業	p7 「万一、サーバ攻撃を受けた際には、空調システムの保持していた計測データや設定値が、失われる可能性がある。したがって、サイバー攻撃から、スムーズに復帰するためには、これらのデータや設定値を適切な間隔でバックアップしておくことが重要である。」	万一、サーバ攻撃を受けた際には、空調システムの保持していた計測データや設定値が、失われる可能性がある。また、システムが破壊される最悪の事態にはPCを初期化して再インストールが必要となる場合がある。したがって、サイバー攻撃から、スムーズに復帰するためには、これらのデータや設定値及びシステム全体を適切な間隔でバックアップしておくことが非常に重要である。	いただいた御意見も参考に、修正いたします。具体的には、最低限保持するべき空調機能や復旧の優先度を考えて対応することを求めているものであり、システム全体のバックアップもこの優先度の中で考えるべきであるため、その趣旨の記述を追記します。 修正箇所：3の「万一、サーバ攻撃を受けた際には、」から始まる段落に「復旧の優先順位を考え、機能維持の最低限のコントローラを速やかに戻せるように、必要なバックアップ」を実施する旨を挿入。
3	企業	p7 「また、HMI からの操作制御であっても、空調システムとして異常値を設定されたことを検出する手段を設け、HMI 異常の際には、その操作設定を無視できる機能（設定値上下限監視）の実装やコントローラをネットワークから分離又はネットワークを介さずに、現場での手動操作で対応できる体制を構築しておく必要がある。」	また、HMI からの操作制御であっても、空調システムとして異常値を設定されたことを検出する手段を設け、HMI 異常の際には、その操作設定を無視できる機能（設定値上下限監視）を自動制御設備の空調機コントローラでの実装やコントローラをネットワークから分離又はネットワークを介さずに、現場での手動操作で対応できるシステム構築と体制の整備をしておく必要がある。	いただいた御意見については、自動制御装置側のコントローラに限定した対策を述べているものではないため原案のとおりとさせていただきます。
4	企業	p12 「② 空調状態や空調システムの運用状態の管理 　万一の異常発生に備え、異常時の対応体制を構築しておく。」	② 空調状態や空調システムの運用状態の管理 　万一の異常発生に備え、システムのフルバックアップ 　保存、日次処理による設定・計測データの自動保存化、 重要機器(サーバ、コントローラ)の予備器の確保、異常時 の対応体制の構築等を行っておく	いただいた御意見を踏まえ、修正いたします。具体的には例示いただいたもののうち、対策はそれぞれの要求に応じて選択するべきという考えにもとづき、過剰対策とならない範囲で追記します。 修正箇所：3.2.1.1項②の箇条書きの後に例示を追記。
5	企業	p12 「③ -1 中央監視盤のサイバー攻撃を想定する（図 3-4 (a)） A) 中央監視盤から空調設定値を空調機に再設定し、正常に設定されることを確認する。 B) 空調監視盤から空調設定温度を再設定できない場合には、制御IP ネットワークに接続しているプロトコル変換器を遮断（電源off するか、ネットワーク接続線を抜く）し、空調専用コントローラによる制御に切り替える。」	③ -1 中央監視盤のサイバー攻撃を想定する（図 3-4 (a)） C)システムが破壊された最悪の場合は代替機に交換し、予め用意されているフルバックアップデータを用いて再インストールする。	いただいた御意見は、今後の検討に向けた参考にさせていただきます。具体的には現在のガイドラインでも最低限の空調機能を維持できる仕組みを提供しており、予備機への代替やフルバックアップの利用をするべきかはさらに検討を要します。
6	企業	p12 「③ -2 空調専用コントローラのサイバー攻撃を想定する。（図 3-4 （ｂ）） A） 空調設定値を空調機に再設定し、正常に設定されることを確認する。 B） 空調専用コントローラから空調設定温度を再設定できない場合には、空調機独自ネットに接続している空調専用コントローラを遮断（電源off するか、ネットワーク接続線を抜く）し、空調個別リモコンによる制御に切り替える。」	③ -2 空調専用コントローラのサイバー攻撃を想定する。（図 3-4 （ｂ）） C)空調機コントローラが破壊された最悪の場合は代替機に交換し、予め用意されているフルバックアップデータを用いて再インストールする。また、復旧手順書を予め用意しておく。	いただいた御意見は、今後の検討に向けた参考にさせていただきます。具体的には現在のガイドラインでも最低限の空調機能を維持できる仕組みを提供しており、予備機への代替やフルバックアップの利用をするべきかはさらに検討を要します。
7	企業	p14 ４章	全体感として、上位のガイドラインで対策がなされていて、なおかつ空調編としての個別の対策まで実施することについて過剰感を持っています。例えば、インターネット接続部分で通信制限など実施していた場合は、空調部分への対応は不要のようなイメージです。	いただいた御意見も参考に、全体構成などの見直しも含めて修正いたします。具体的には、共通編の一部を再掲している現在の構成が、共通編同等の対策を空調システムにも重複して求めていると誤解される可能性があることから、本編の記述は空調に特化した部分のみに変更します。 修正箇所：4.2節及び4.3節を削除し、付録Bを追加。
8	企業	p15 「セントラル空調の場合」	【追記】 ・システムが破壊され中央監視設備や自動制御設備が故障する最悪の事態を想定し、予め重要設備機器の予備器確保とフルバックアップを行う	いただいた御意見は、今後の検討に向けた参考にさせていただきます。具体的には現在のガイドラインでも最低限の空調機能を維持できる仕組みを提供しており、予備機への代替やフルバックアップの利用をするべきかはさらに検討を要します。

No.	提出者	提出意見		御意見に対する考え方
		該当箇所	意見内容	
9	企業	p17 表４の１　６１の５	作業員の作業を常時監視仕組みの導入とありますが、空調機械室等の全てに死角なしにITVを設置するのは非現実的だと思います。	いただいた御意見も参考に、全体構成などの見直しも含めて修正いたします。具体的には、ガイドラインの対策要件の実施に当たっては完璧な対策を求めているわけではなく、利用者がリスクの存在を認識した上で、それぞれの立場や状況、セキュリティの要求レベルに応じて可能な対策を実施することが大事だと考えているものであり、その趣旨の記述を追記します。 修正箇所：1.3節を追加。
10	企業	p20 表４の３　１０の４	外部接続回線を管理するとあります。趣旨は理解しますが、相当数の数量の通信回線から不明回線を割り出すのは容易ではなく、非現実的と思います。	いただいた御意見も参考に、全体構成などの見直しも含めて修正いたします。具体的には、ガイドラインの対策要件の実施に当たっては完璧な対策を求めているわけではなく、利用者がリスクの存在を認識した上で、それぞれの立場や状況、セキュリティの要求レベルに応じて可能な対策を実施することが大事だと考えているものであり、その趣旨の記述を追記します。また、共通編の一部を再掲している現在の構成が、共通編同等の対策を空調システムにも重複して求めていると誤解される可能性があることから、本編の記述は空調に特化した部分のみに変更します。 修正箇所：1.3節を追加。4.2節及び4.3節を削除し、付録Bを追加。
11	企業	p20 表４の３　１２	オフィス系端末とありますが、空調監視端末はそれ専用であることが多く、事務員が使用する端末とは切り離されています。オフィス系だと誤認すると思います。	いただいた御意見も参考に、全体構成などの見直しも含めて修正いたします。具体的には、共通編の一部を再掲している現在の構成が、共通編同等の対策を空調システムにも重複して求めていると誤解される可能性があることから、本編の記述は空調に特化した部分のみに変更します。 修正箇所：4.2節及び4.3節を削除し、付録Bを追加。
12	企業	p21 表４の３　２０の２	前述同様、作業員の作業状況を常時監視となると、防災センター内かなりの台数のITVが必要ですし、監視卓の株にクライアントPCが設置されている事もあるため、死角は必ず出ます。一か所でも死角があると、この対策は意味合いが薄れると思います。	いただいた御意見も参考に、全体構成などの見直しも含めて修正いたします。具体的には、ガイドラインの対策要件の実施に当たっては完璧な対策を求めているわけではなく、利用者がリスクの存在を認識した上で、それぞれの立場や状況、セキュリティの要求レベルに応じて可能な対策を実施することが大事だと考えているものであり、その趣旨の記述を追記します。また、共通編の一部を再掲している現在の構成が、共通編同等の対策を空調システムにも重複して求めていると誤解される可能性があることから、本編の記述は空調に特化した部分のみに変更します。 修正箇所：1.3節を追加。4.2節及び4.3節を削除し、付録Bを追加。
13	企業	p21, p24 表４の３　２１の４と３１の２	ログ解析の仕組みを導入とありますが、ベンダー側は対応できるのでしょうか。仮に対応していたとしても、空調設備にここまで実施する必要があるのでしょうか。コスト効果を検討する必要があると思います。	いただいた御意見も参考に、全体構成などの見直しも含めて修正いたします。具体的には、ガイドラインの対策要件の実施に当たっては完璧な対策を求めているわけではなく、利用者がリスクの存在を認識した上で、それぞれの立場や状況、セキュリティの要求レベルに応じて可能な対策を実施することが大事だと考えているものであり、その趣旨の記述を追記します。また、共通編の一部を再掲している現在の構成が、共通編同等の対策を空調システムにも重複して求めていると誤解される可能性があることから、本編の記述は空調に特化した部分のみに変更します。 修正箇所：1.3を追加。4.2節及び4.3節を削除し、付録Bを追加。
14	企業	p25 表４の３　４０	十分な保護対策とありますが、具体的にはどのようにすれば十分と言えるので しょうか。MDF室やEPS内で施錠管理できていれば可とすべきだと思います。	いただいた御意見も参考に、全体構成などの見直しも含めて修正いたします。具体的には、共通編の一部を再掲している現在の構成が、共通編同等の対策を空調システムにも重複して求めていると誤解される可能性があることから、本編の記述は空調に特化した部分のみに変更します。 修正箇所：4.2節及び4.3節を削除し、付録Bを追加。

No.	提出者	提出意見		御意見に対する考え方
		該当箇所	意見内容	
15	個人	全般	ビル内部での犯行可能性もあるので、外部との通信だけでなく、機器と管理ネットワークの間についても暗号化通信を行えるよう、機器メーカーと管理ネットワーク系ベンダが協力して機器に暗号化通信の機能を持たせるようにしていくべきと考える。 OSI7階層モデルのL2について802.1X類似の技術で暗号化を行い、又はL3-L4でIPsecやSSH等を利用しての暗号化を行うようにすると、一般に通信の盗聴・改竄への防御が備わり攻撃を妨げる効果があると思われるが、簡単な暗号化でも容易な閲覧・改竄を妨げる効果があり、暗号化の突破という追加の法的ペナルティを攻撃側に科す事が可能なので、簡単なもの（時代遅れとなるようなもの）でも実際的な効力を有するのではないかと考える（但し勿論インターネット経由では適切な暗号化が行われているべきであり、ビル内部の通信も本来的には同様である。ここでは廉価なチップでも効力のある技術の実装が行える事を述べ、ハードルが高くない事を強調しているのである。）。 国民としては、スマートメーター等についてもセキュリティについて危惧しているのであるが（無線通信事業者とのモバイル回線が暗号化で保護されているからといって、メーターに平文で電力会社と通信させていたりしていたのである、我が国の電気事業者は。メーターのメーカーにも電力会社にも問題ある精神がある。又スマートメーターは機器内部間の通信に赤外線を用いたりしているが、周辺から鋭敏な機器で盗聴し放題なのではないか。頭が痛くなる様な経済産業関係事業者のセキュリティ意識（故意に個人情報や重要情報漏らそうとしてますよね？）が垣間見える事態があったのである（なお現在問題が全て是正されたとは考え難い。新型のスマートメーターが出ているが、初期版が多くそのまま稼働していたりするのでは。）。）、専門機器での独自プロトコルを扱う者だけでなく、一般的な通信・セキュリティに通じた者を交えセキュリティの技術向上を図るべきと考える。（なおまともなネットワーク技術者ならL2L3L4等のプロトコルについて独自でパケットや通信の仕様等を考えれるのが通常であり、あまり専門機器の独自プロトコルを扱う者達に技術的アドバンテージは無いと考える。ットワーク技術者はかなり程度の高い者である必要はあると思われるが。）	いただいた御意見は、今後の検討に向けた参考にさせていただきます。具体的には内部犯行については物理的なアクセス制御や監視に関する要件として記載済みです。また、ネットワークのアクセス制御についての要件も記載しており、外部との接続要件のうち、メーカークラウドとのアクセスについては、別紙において暗号化にも触れています。