令和２年度サイバー・フィジカル・セキュリティ対策促進事業
（ビルシステムのサイバーセキュリティ高度化に向けた調査）

調査報告書

株式会社野村総合研究所

2021年3月26日

NRI

Share the Next Values!

目次

１．ビルガイドラインの高度化のための調査

①空調等のビルの個別設備システムの対応策に関する調査

②スマートビルのサイバーセキュリティ対策を意識したユースケース調査

③その他関連する調査

③－１　インシデントレスポンスに対する要求の整理

③－２　ガイドラインへの追加情報の充実化

③－３　ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討

２．ビルシステムのサイバーセキュリティ推進体制の調査

①推進体制の情報提供・共有・相談等の機能の実践的評価

②推進体制のあり方の調査

３．検討会の運営

①ビルSWGの運営

②作業グループの運営

③その他の運営

1．ビルガイドラインの高度化のための調査
①空調等のビルの個別設備システムの対応策に関する調査

- 空調等のビルの個別設備システムの対応策に関する調査では、空調システムを対象として、ビルガイドライン（個別編：空調システム）の取りまとめに向けた検討を行った。
- 後述する作業グループに参加するメンバーが作成したビルガイドライン（個別編：空調システム）の案に対して、作業グループにおいて議論を行い、議論の内容を取りまとめた。
- ビルガイドライン（個別編：空調システム）の案に対する作業グループメンバーからの主な意見を以下に示す。

観点	作業グループメンバーからの主な意見
用語の定義	● エアハンは、エアハンドリングユニット、ビル用マルチは、ビル用マルチエアコンという理解でよいか。
実際のサイバー攻撃事例	● セントラル空調システムを対象としたサイバー攻撃の事例は存在しないのか。
サイバーセキュリティ対策の考え方	● 個別分散空調システムの場合の二重化と、セントラル空調システムの場合の二重化は実態が異なるため、実態を踏まえて書き分けることが必要である。 ● 個別分散空調システムの場合は、コントローラーが直接制御IPネットワークに接続されていない。コントローラー以下の部分について、各社で実態が異なる可能性がある。 ● 大規模ビルのセントラル空調システムで起こり得る攻撃のリスクとしては、制御IPネットワーク以上の部分が大半を占める。そのため、セントラル空調システム特有のリスクはあまり見当たらない。その部分のリスクはガイドライン共通編で整理されているという理解である。
ガイドラインへの記載	● セントラル空調システムは、熱源設備、ポンプ、空調機が一体となって実現されている。4.1．空調システムの管理策の60　空調システムの(1)～(3)について、補足的な説明を追記できるのではないか。

1．ビルガイドラインの高度化のための調査
①空調等のビルの個別設備システムの対応策に関する調査

- 前ページの意見を反映した、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）の案を、参考資料１として取りまとめる。
- 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）の案については、後述するビルSWGにおいて議論を行った。当該案については、読み手が手を付けやすくすること、人命に関わるものを優先すること、一般のビルだけでなく、安全性が強く求められるビルにも活用できること、海外の先行的な事例を取り込むこと、ビルの規模に応じて作成することやマネジメント側に理解されるように作成することが求める意見が出た。ビルSWGで出た意見を次ページ以降に整理した。

ビルSWGで出たガイドライン（個別編：空調システム）に関する意見

- 個別編については、読み手が手を付けやすくすること、人命に関わるものを優先すること、一般のビルだけでなく、安全性が強く求められるビルにも活用できること、海外の先行的な事例を取り込むこと、ビルの規模に応じて作成することやマネジメント側に理解されるように作成することが求められている。

■ 読み手が手を付けやすくすることが必要

- もう少し読み手が手を付けやすい軽いものも記載できるのではないか。例えば、機器の設定等において、30分から１時間に１回程度。温度設定で正しい値を入力し続けると、攻撃があってもすぐに元の状態に戻せることが出来、常に定常状態に保つことが出来るというような制御の方法等もうまく個別編に組み込んでも良いのではないか。一般のユーザの方のアクションも受け入れられるようにしつつ、学習データを蓄積することでビルごとの最適化を行い、攻撃への対応時間を稼ぐということも実現できるのではないかと考える。
- まず始められるところとして、本日構成員の方々から上がった話等を事例集のような形で充実させていくことから取り組んでも良いのではないか。事例集であれば読み手のユーザからしても手に取りやすく、厳密なレベル分けもせずに始められるのではないかと考える。

■ 人命に関わるものを優先することが必要

- 個別編ということで空調についてご説明を頂いたが、空調編以外の個別編の検討は既に始まっているのか。また、今後空調編はパブコメを経てリリースされると思うが、パブコメが実施される時期についてもし決まっていればお伺いしたい。
- 個別編として空調システムが先に出たが、ペンタゴンの例の話も鑑み、電力の配電システムや防災システム、昇降機の監視システム等、人の命にかかわる様な部分の個別編について、優先的に取り組んでいってほしい。

ビルSWGで出たガイドライン（個別編：空調システム）に関する意見

■ 一般のビルだけでなく、安全性が強く求められるビルにも活用できることが必要

- 本ガイドラインは普通のビルだけではなく、場合によっては半導体等最先端の産業用の工場の空調にも使われる可能性があるため、普通のビルだけではなく安全性が強く求められるような工場や施設にも活用できるように記載を追加した方が良いのではないか。
- 昨今の米国テキサス州の大寒波を受け、半導体や素材関係のサプライチェーンが被害を受けたことを鑑みると、工場等の空調のシステム等が安全に高品質に正常に戻るまでに時間がかかることを考えると、システムを止めるという判断も難しいため、対応手順や管理者を設定しておくことも非常に重要だと考える。

■ 海外の先行的な事例を取り込むことが必要

- 米国のペンタゴンがビルのセキュリティに神経質になっている関係で、ビル側でセキュリティ対応を実施していることを明確に求めてきており、ビルシステムを納入するサプライヤー側が混乱したことがあった。個別編が整えられていく上で、このような海外の先行的な事例をとらえ、今後のユーザのハイレベルな要求に応えられるような検討がなされているのかは気になる。海外ではコマンドを暗号化することで、指示内容に触れないようにして防御している先行事例もあり、その際にDPIを一部解除しなくてはいけないという場合も存在する。
- EUでもNIS指令の改正が行われ、重要インフラのオペレーターの対象に大規模工場や大規模設備のオペレーターも追加された。そのため日本の事業者においても、EUに工場や商業施設を保有している事業者は、今後NIS指令の対象となる。今回の改正で、人的管理やマネジメントのセキュリティだけではなく、調達機器のセキュリティ対応も求められるようになった。この観点からも日本においてサプライチェーンの影響が大きく出ると考えており、今後はビルでも最先端な事例では同じような要求が出てくることが想定される。

ビルSWGで出たガイドライン（個別編：空調システム）に関する意見

■ ビルの規模に応じて作成することやマネジメント側に理解されるように作成することが必要

- 空調や受変電といった個別の議論を突き詰めるより、ビルの規模に応じて作成いただいた方がオーナー側としては理解し易い。現状、普通のオフィスビルで起こり得るインシデントはそこまで重たくないと考えているので、そういった実情に応じたガイドラインが良いと考えている。例えば、個別編を読んだところでオーナー側では手に負えず、全体像を理解することが難しい。言い切ってしまえばセキュリティの素人が読んでも理解出来、実施できるガイドラインを作成いただかないと活用することは厳しい。
- 昨今はセキュリティだけではなく、CO2削減の取組が重要で、ビルとして便利になる方向を目指すとセキュリティへの配慮が足りなくなってしまい、セキュリティに配慮をしすぎてしまうと、便利でもなくCO2のコストも重なってしまうことが課題として認識している。セキュリティと他の観点間のバランスを取りたくとも、現状それを解決する指針がないので検討を始めることが出来ず、道は遠いと考える。今後、さらにビル単体だけではなくスマートシティの展開が広がっていく方向性の中で、セキュリティに関する落としどころや折り合いの付け方を示してほしいと考える。
- 現場で使いやすさを求めると記載が詳細になってしまいがちで、全体を把握しようとなると抽象的になって使い勝手が悪くなってしまいがちなのが難しい。せめて議論はどこまでいっているかはステークホルダーで把握できるようにしたい。現場だけではなく全体をマネジメントしている側がチェックできるような体系化や体制を整えていくしかないと考えている。

参考資料

事例①：中部国際空港でのシステム障害の事例

- 2015年10月6日、中部国際空港の旅客ターミナルビルにおいて、大規模なシステム障害が発生した。サーバールームの空調制御装置が故障して、4台の空調機のうち、3台(1台は予備機)が同時に停止し、室内の温度が上昇するに伴い、空港内のシステムが接続する共用ネットワークの機器が40度超の異常な高温の熱を帯びて停止したことが原因であると中部国際空港会社が明らかにした。

中部国際空港でのシステム障害の事例

項目	概要
リスク源	●サーバールームの空調制御装置の故障が、空調機の停止やそれをきっかけとした空港内のシステムが接続する共用ネットワークの機器の停止を引き起こした。
共用ネットワークの機器の停止がもたらしたシステム障害	●共用ネットワークに接続している空港内の 6 つのシステム（①発着便を案内する表示盤の管理システム、②国際線のチェックインシステム、③手荷物取扱いシステム、④店舗のPOSレジシステム、⑤駐車場システム、⑥空港警備システム）が、影響を受けた。 ●上記④や⑤では、店舗と駐車場の精算において、クレジットカード決済のオンライン処理ができなくなった。
システム障害による影響	●国際線の出発便10便に最大 1 時間程度の遅れが発生するとともに、乗客1,500名以上が影響を受けた。
インシデント対応	●8時53分に空調機が停止し、中部国際空港株式会社は9時19分に空調機を復旧し、その後共用ネットワークに接続するシステムを順次復旧、12時43分時点ですべてのシステムの復旧を完了した。

事例②：米国ターゲット社の委託先が標的型攻撃で狙われた事例

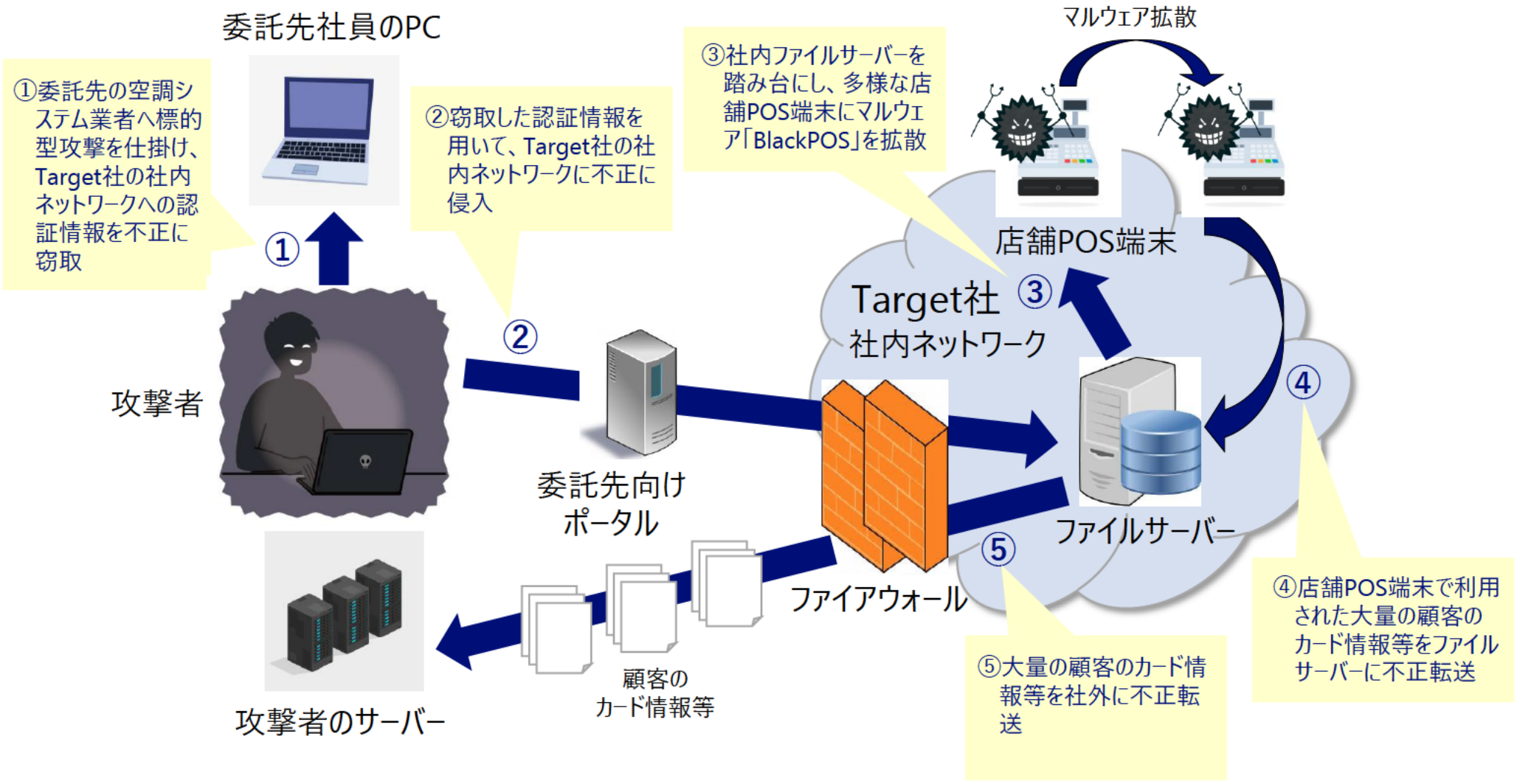
- 米国小売業者のTarget社が、2013年11月から12月にかけて、不正アクセスを受け、顧客のカード情報等を流出した。委託先である空調システム業者(Fazio Mechanical Services社)の社員のPCが標的型攻撃を受け、空調システム業者が、空調機のエネルギー消費量の監視やメンテナンスのために、Target社の社内ネットワークにアクセスする際に使用する認証情報を不正に窃取されたことが原因となった。

米国ターゲット社の委託先が標的型攻撃で狙われた事例

項目	概要
リスク源	●委託先の社員のPCのサイバーセキュリティ対策の不備(ウイルス対策ソフトさえ搭載していない状況)により、Target社の社内ネットワークにアクセスする際に使用する認証情報を不正に窃取されたことが、Target社の社内ネットワークへの不正侵入、それをきっかけとしたマルウェアの拡散による顧客情報の流出を引き起こした。
社内ネットワークへの不正侵入がもたらしたマルウェアの拡散	●社内ファイルサーバーを踏み台にして、マルウェア「BlackPOS」を拡散し、多数の店舗POS端末をマルウェア「BlackPOS」に感染させた。
マルウェアの拡散による影響	●マルウェア「BlackPOS」が、店舗POS端末で利用されていた、約1億円1,000万件にも及ぶ大量の顧客のクレジットカード情報やデビットカード情報等を社内ファイルサーバーに不正転送し、社外にも不正転送した。
インシデント対応	●Target社はセキュリティ監視ツールを導入していたが、当該ツールが発していたアラートを見落としていたため、マルウェアの拡散やカード情報等の流出を許した。カード情報等の流出が始まってから10日後に社外からの通知を受けとるまで、Target社は攻撃を受けた事実に気づくことができなかった。通知を受けた後、影響範囲の特定や対策に更に3日間を要した。

事例②：米国ターゲット社の委託先が標的型攻撃で狙われた事例

- 米国ターゲット社の委託先が標的型攻撃で狙われた事例を図示すると、以下のとおりである。



事例③：米国の病院の空調システムがハッキングで狙われた事例

- 米国テキサス州の病院(W.B.Carrell Memorial Clinic)が、2009年4月から6月にかけて、不正アクセスを受け、暖房換気空調システム(HVAC: Heating Ventilation and Air Conditioning)のHMI画面情報がオンライン上で公開された。同病院に勤務する契約警備員が、同病院の暖房換気空調システムや患者情報を保管するコンピュータに不正に侵入していたことが原因となった。

米国の病院の空調システムがハッキングで狙われた事例

項目	概要
リスク源	●同病院に勤務すると同時に、オンライン上で「Ghost Exodus」という名前で活動し、ハッカーグループ「Electronik Tribulation Army」のリーダーを務めていた契約警備員が、内部犯行として、同病院の暖房換気空調システムや患者情報を保管するコンピュータに不正に侵入できたことが、HMI画面情報の流出や、同病院内のPCへのマルウェア感染を引き起こした。
不正侵入がもたらした情報流出やマルウェア感染	●契約警備員は暖房換気空調システムのHMI画面のスクリーンショットをオンライン上に公開した。当該HMI画面には、手術室のポンプや冷却装置を含め、病院の様々な機能のメニューが含まれていた。また、契約警備員は自らが同病院内のPCにマルウェアをインストールする様子等を撮影し、その動画を公開した。マルウェアのインストールは、同病院内のPCをボットネット化し、大規模なDDoS攻撃を仕掛ける際に活用することを狙ったものであった(但し、DDoS攻撃の計画は未遂で終わる)。
情報流出やマルウェア感染による影響	—
インシデント対応	●病院内部から発覚することはなかった。SCADAセキュリティ専門家がハッカーの知り合いからの情報を得て調査し、FBI及びテキサス州検察局に報告したことで発覚。その後逮捕された。

事例④：BAネットワークへの不正侵入により空調システムをダウンさせる実証実験の事例

- ソフトバンク・テクノロジー、サイバートラスト、竹中工務店は、2018年3月に、ホテルを対象に、ビルへのサイバー攻撃を想定した実証実験を行い、その成果として、BA(Building Automation)ネットワークの脆弱性が攻撃者に利用され、空調システム等が不正操作されるという脅威があることを報告した。

BAネットワークへの不正侵入により空調システムをダウンさせる実証実験の事例

項目	概要
リスク源	●閉域網での運用を前提としたBAネットワークであっても、ホテルの客室など、一般の人が誰でも立ち入れる場所にBAネットワークのケーブルがむき出しのままの状態で配線されている場合には、攻撃者によってBAネットワークに不正機器を接続される可能性がある。
BAネットワークへの不正機器の接続がもたらした空調システム等の不正操作	●BAネットワークに接続された不正機器から、BAネットワーク上のサーバーや機器に不正侵入したり、マルウェアを感染させたりすることによって、標的とする部屋の空調や電灯、カーテンの開閉等が不正操作され、被害を受ける可能性がある。
空調システム等の不正操作による影響	●省エネモニター(ディスプレイ)等、サイバー攻撃を受けることを前提に設計されていないコントローラ機器においては、一部セキュリティ機能が乏しい部分があり、このようなコントローラ機器が踏み台にされれば、ビル制御機器全体に被害が拡大する可能性がある。
インシデント対応	—

事例⑤：BAシステムの脆弱性を狙った攻撃により空調システムをダウンさせる脅威の事例

- 2019年1月に、BA(Building Automation)システムの脆弱性が攻撃者に利用され、データセンターの暖房換気空調システム(HVAC: Heating Ventilation and Air Conditioning)等が不正操作されるという脅威があることが報告された。

BAシステムの脆弱性を狙った攻撃により空調システムをダウンさせる脅威の事例

項目	概要
リスク源	●インターネット経由でアクセス可能なBAシステムの存在が確認されており、攻撃者は、初期設定のユーザ名とパスワードの入力や、ログインの試行の繰り返し等により、BAシステムのログイン画面を突破して、暖房換気空調システムのダッシュボード等への不正アクセスが可能となっている。
暖房換気空調システムへの不正アクセスがもたらしたコンピュータの動作不良	●暖房換気空調システムのダッシュボード等への不正アクセスにより、データセンター内で稼働するサーバー群等を冷却するための空調機のスイッチをオフにすることにより、サーバー群等の動作不良が引き起こされる可能性がある。また、同様の手口で、物理的なアクセス制御システムに不正アクセスを行うことにより、機密性の高い場所に不正に侵入される可能性がある。
コンピュータの動作不良による影響	●攻撃者が、不正アクセス可能なBAシステムを運用するビルのオーナー等に対して、BAシステムの制御の掌握により、ビルを閉鎖すると脅して、ビットコインでの支払いを求める脅迫メール送ることにより、金銭的被害に発展する可能性がある。また実際には、ビルのオーナー等が支払いを拒否したため、標的となったビルは混乱が生じる結果を招いた。
インシデント対応	—

各事例から求められている(検討されている)対応策

事例	対応策
事例①： 中部国際空港でのシステム障害の事例	●インシデント発生後、空調機器制御システムの二重化や設備更新について検討している。
事例②： 米国ターゲット社の委託先が標的型攻撃で狙われた事例	●委託先までも含めて、同様の対策を講じることが必要である。 ●セキュリティ監視ツールを導入しても、最終的には人間がログの振る舞いパターンなどからシステムの異常を迅速に判断しなければならないため、判断基準を明確化していくことが必要である。 ●経営層が、日頃からサイバーセキュリティへの意識を持ち、有事において、経営層と社外の間でのコミュニケーションを取ることができるよう、有事に備えておくことが必要である。
事例③： 米国の病院の空調システムがハッキングで狙われた事例	―
事例④： BAネットワークへの不正侵入により空調システムをダウンさせる実証実験の事例	●BA設備環境へのセキュリティ対策として、社内情報(OA系)ネットワーク経由および閉域網での運用を前提とした制御(BA)ネットワーク自体からの侵入に加えて、機器への物理的な攻撃を想定した対策を講じる必要がある。
事例⑤： BAシステムの脆弱性を狙った攻撃により空調システムをダウンさせる脅威の事例	●BAシステムへのアクセスがどのように保護されているかという観点からしっかりと管理することが必要である。 ●最低でも二要素認証やVPN接続を前提としてBAシステムのログイン画面にアクセスするようにしなければならない。

1．ビルガイドラインの高度化のための調査

①空調等のビルの個別設備システムの対応策に関する調査

②スマートビルのサイバーセキュリティ対策を意識したユースケース調査

③その他関連する調査

③－１　インシデントレスポンスに対する要求の整理

③－２　ガイドラインへの追加情報の充実化

③－３　ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討

2．ビルシステムのサイバーセキュリティ推進体制の調査

①推進体制の情報提供・共有・相談等の機能の実践的評価

②推進体制のあり方の調査

3．検討会の運営

①ビルSWGの運営

②作業グループの運営

③その他の運営

1．ビルガイドラインの高度化のための調査
②スマートビルのサイバーセキュリティ対策を意識したユースケース調査

- スマートビルのサイバーセキュリティ対策を意識したユースケース調査では、具体的なユースケースとして、スマートビルのオーナーに対するヒアリングを実施し、IoTの活用の内容やサイバーセキュリティ対策の取組等について把握した。
- そのうえで、当該スマートビルを対象として、IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）に基づき、リスク分析やリスク評価、対策の方向性、対策の要件を含め、ユースケースを整理した。

各種IoT機能における想定セキュリティリスクと対応策

	照明機器の制御	空調機器の制御	センサネットワーク	免震モニタリング	マルチサインのコンテンツ制御	外構照明の光色の制御
想定リスク	リスク① クラウドベンダーの選定 リスク② 侵入・改ざんの防止 リスク③ 悪意のある操作の防止		リスク① 装置の選定 リスク② 不正データの送出、コマンド発行の防止 リスク③ RFIDによる職員の行動トラッキング	リスク① データの改ざんによる誤判定(例えば、誤判定により、全館避難となった場合に経済的な損失が発生)	リスク① 表示の改ざん、不適切情報の掲載、データ消去 リスク② 装置の選定	リスク① いたずらによる設定変更
リスク対応策	対応策①-1 保守仕様の確認、運用リスクの低減を目的とした特記仕様書の作成 対応策①-2 定期的なデータバックアップ 対応策②-1 IDS/IPSの設置 対応策②-2 システム停止時におけるサービス単位での再デプロイ可能な構成 対応策③ 発停・動作モードの限定、変更不可		対応策① 将来にわたるサポート・アップデート提供の確認 対応策② アンテナアレイの定義に基づく定型データのみの受信 対応策③ 職員用RFIDタグ上の個体識別番号のみを使用し、個人を特定できないように運用	対応策①-1 外部からの不正アクセスの防止 対応策①-2 論理的なネットワーク分離や、特権アカウントによるアクセス制限による内部からの不正アクセスの防止	対応策①-1 CMSのOA系ネットワークからの分離 対応策①-2 職員や来庁者の目が届く場所へのSTBの設置、サイネージ本体のポートの無効化 対応策①-3 VPNまたは閉域網接続 対応策①-4 専用端末の利用や、設定変更・掲載許可の承認プロセスの厳格化による不正使用の防止 対応策② 将来にわたるサポート・アップデート提供の確認	対応策①-1 外部連携の制限 対応策①-2 末端機器からの制御不可や、クラウドまたはサーバー室の機器からのみ設定変更を可能にするなど、制御方式の制限

IoTセキュリティ・セーフティ・フレームワーク検討への示唆

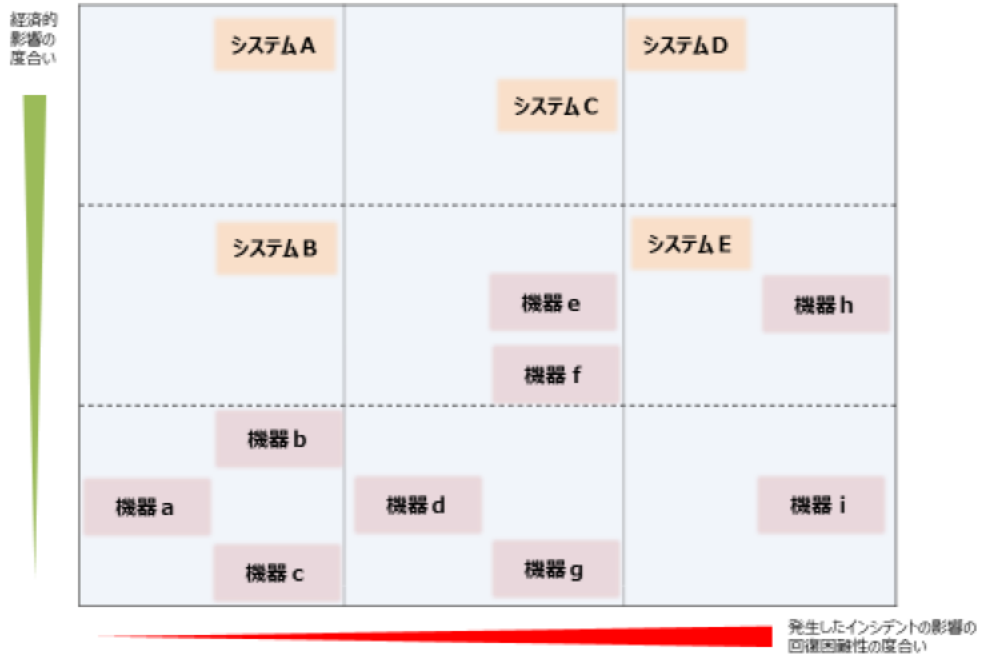
- システムに精通し、庁内のシステム導入を支援できる新しいポジションの人材を確保することが必要である。

	第１の観点 運用前(製造段階等)における フィジカル・サイバー間をつなぐ 機器・システムの確認要求	第２の観点 運用中の フィジカル・サイバー間をつなぐ 機器・システムの確認要求	第３の観点 機器・システムの運用・管理を行う者の 能力に関する確認要求	第４の観点 その他、社会的なサポート等の 仕組みの要求
スマートビルを取り巻く課題	● 機器・システムの運用期間が長期間に及ぶため、その間に、ベンダーから提供されるメンテナンスサービスやソフトウェアのアップデートが終了する可能性がある。 ● ICTの著しい進化により、導入した機器・システムが陳腐化するスピードがこれまで以上に速くなる可能性がある。	● 職員や来訪者の目が届かない場所に機器が設置された場合、不正な機器が設置されたり、不正に操作されたりする可能性がある。	● 庁内各部署が業務で使用する機器・システムについては、運用管理の方法や粒度が各部署に委ねられている場合が多いため、各部署によってセキュリティリスクの有無や軽重にばらつきが生じる可能性がある。	● 複数のシステムの構築が同時並行で進むため、発注者が要件定義の調整を行う相手先(メーカー、システムベンダー、ゼネコン等)の範囲が広範になり、調整に係る負荷が増大する可能性がある。
求められる対応	● 機器の選定やシステムの調達時において、ベンダーに対し、継続的なメンテナンスサービスやソフトウェアのアップデートの提供を求め、将来的なセキュリティ運用を担保することが必要となる。 ● 機器の選定やシステムの調達時において、機器・システムの陳腐化に対応して、継続的な更改を可能とする拡張性を担保することが必要となる。	● 職員や来訪者の目が届く場所への機器の設置やポートの無効化が必要となる。	● 機器・システムが外部のネットワークに繋がっているか、外部のネットワークに繋がっていない場合でも、アクセスポイントをどれぐらい保有しているか等の運用管理の状況をシステム担当部署が一括で確認し、そのうえでセキュリティリスクが存在する場合は、運用管理の方法や粒度の見直しを行い、同リスクを除去・管理することや、同リスクに対処できない機能を無効化することが必要となる。 （機器の選定時やシステムの調達時に上記を確認できると尚よい。）	● スマートビルの建設とIoTセキュリティは、一体不可分の関係であり、ゼネコンがシステムの構築の流れを理解し、メーカーやシステムベンダーと調整できるように、公共工事で使用する施工要領書の中に、IoTセキュリティを含めることが必要である。

IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の策定

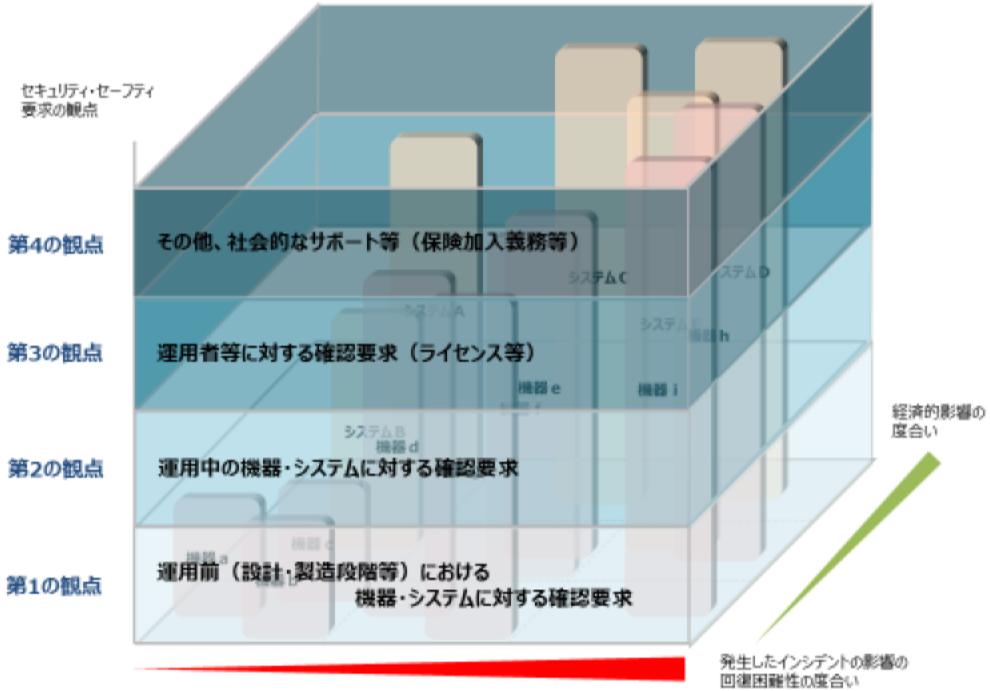
- IoT機器・システムの性質や利用環境によって課題が一様ではないことに着目し、IoT機器・システムをリスクに応じてカテゴライズした上で、それぞれに対するセキュリティ・セーフティ要求を検討することに資するフレームワーク「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）」を策定。
- 世界中から幅広く意見を収集するため、日本語版・英語版のパブコメを実施。 国内外から約100件の意見が寄せられた。パブコメの意見を反映した上で、2020年11月5日にver1.0を公表。

フィジカル・サイバー間をつなげる
機器・システムのカテゴライズのイメージ



※ 同じ機器・システムでも使用形態などによってマッピング先が異なり得る。
例えば、機器gと機器hが同じ機器で異なる使用形態である場合などがあり得る。）

カテゴリに応じて求められる
セキュリティ・セーフティ要求の観点のイメージ



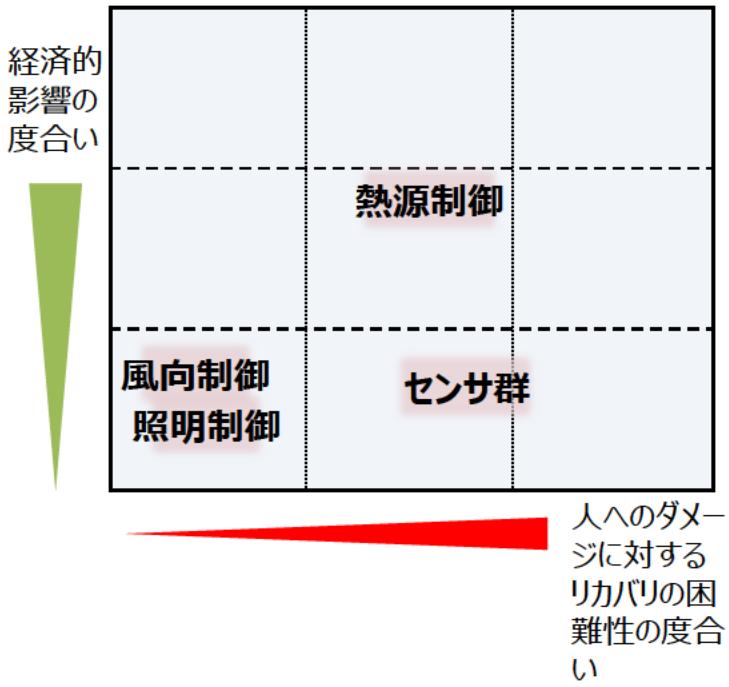
IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の策定

- ダメージに対するリカバリの困難性の度合いと経済的影響の度合いの２つの軸でリスクを評価する。

基準		それぞれの観点におけるカテゴライズ基準の例					
		ダメージに対するリカバリの困難性の度合い	経済的影響の度合い				
		人命/安全	プライバシー	資産	生活影響	社会影響	レピュテーション
Lv.1	限定的な影響	軽傷	漏えい、悪用	損害	不便	悪影響	信用低下
Lv.2	重大な影響	重傷	名誉毀損	大損害	支障	混乱	業績悪化
Lv.3	致命的・壊滅的な影響	人命への影響	人命への影響	破産	困難	大混乱	倒産

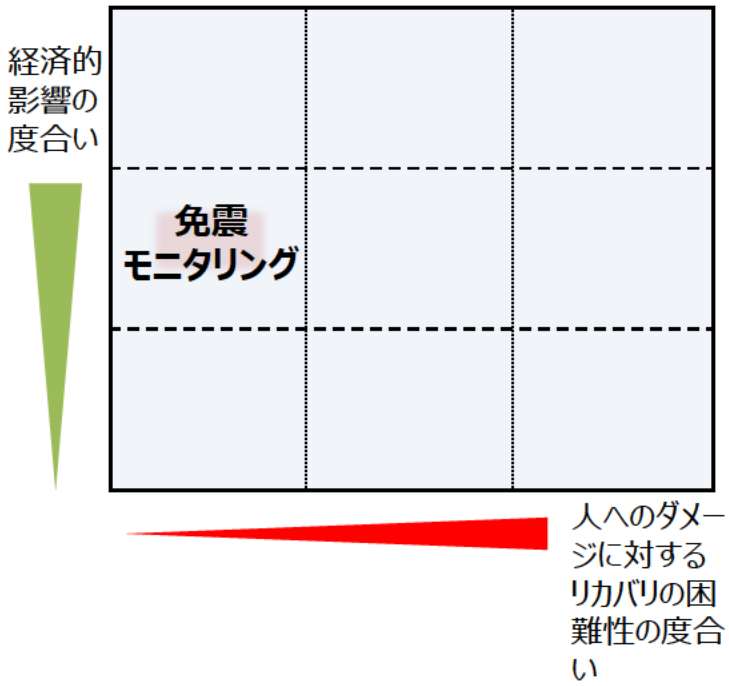
クラウドBEMS

項目		概要
概要		● センサネットワークから得たデータをもとに、クラウドBEMSより、IoT機器の制御を実施する
主な機能		● 環境モニタリング（センサネットワーク） ● 照明制御 ● 空調（風向）制御（熱源制御は行わない）
リスク分析		● 不正データ・コマンド送信による空調・照明の異常動作 ● 職員の行動トラッキング等・・・回復困難性：中（プライバシ）、経済的影響：小
リスク評価		● 回復困難性：中（職員の行動トラッキングの悪用によるプライバシ侵害） ● 経済的影響：中（温度異常によるオフィス利用困難状態が継続。熱源制御によるサーバー設備等への損害）
対策の方向性		● 熱源制御は遠隔（建物外）では行えないようにする ● 職員用RFID上の識別番号と保有職員を紐づけない運用
対策の要件	機器運用前	● アップデートを機動的に行えるよう、共通規格に則る製品を納入。 ● 熱源制御は遠隔（建物外）では行えないようにする。直接制御は照明と空調のみ。
	機器運用中	● アップデートを随時提供する（ベンダ）。職員用RFID上の識別番号と保有職員を紐づけは行わない（ユーザ） ● ユーザ資格・・・なし ● 社会的サポート・・・なし



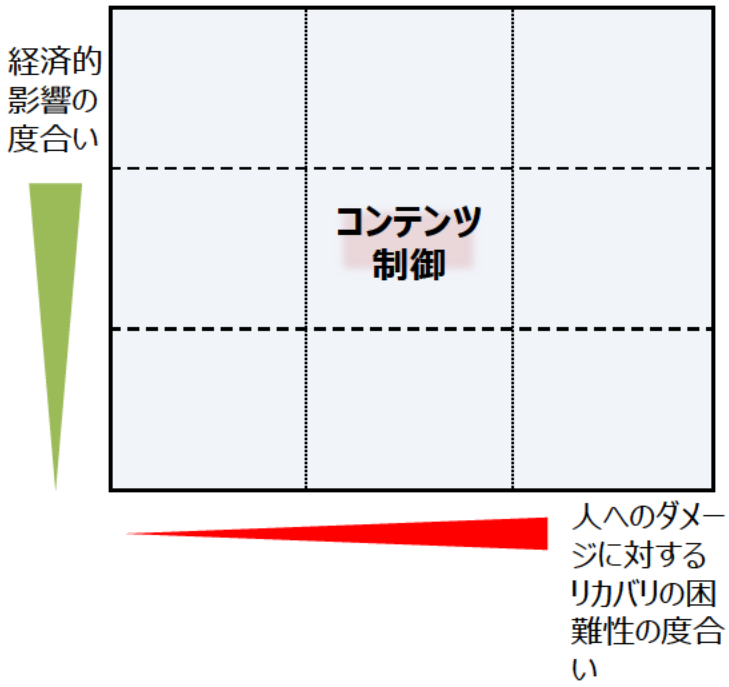
免震モニタリング

項目		概要
概要		● センサネットワークから得たデータをもとに、地震による建物の揺れの程度を自動的に計測し、建物の継続使用可否等の判断を迅速に行う
主な機能		● 免震モニタリング（加速度センサネットワーク） ● 地震による建物の揺れの程度の自動計測 ● 建物の継続使用可否等の判断（判断は人手による）
リスク分析		● 免震モニタリングのデータ改ざんによる建物の揺れの過大な計測 ● 建物の継続使用可否の誤判断・・・回復困難性：小（人命/安全）、経済的影響：中（社会影響）
リスク評価		● 回復困難性：小（避難時のパニック等による人命/安全支障） ● 経済的影響：中（全館避難となった場合の社会的な混乱）
対策の方向性		● アクセス権限のある者しかデータをハンドリングできないようにする
対策の要件	機器運用前	● 論理的なネットワーク分離や特権アカウントによるアクセス権限の設定により、内部からの不正アクセスを防止する ● アクセス権限のある者しかデータをハンドリングできないようにする
	機器運用中	● 外部からの不正アクセスを防止する ● ユーザ資格・・・なし ● 社会的サポート・・・なし



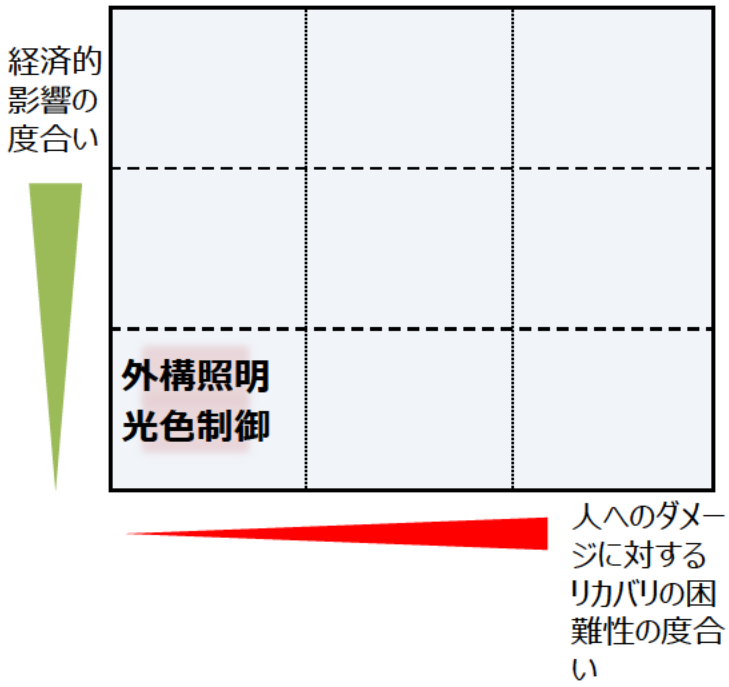
マルチサインのコンテンツ制御

項目		概要
概要		● 各マルチサイン（デジタルサイネージ）に表示するコンテンツについて、CMSを用いて、遠隔より管理・更新を行う
主な機能		● 各マルチサイン（デジタルサイネージ）に表示するコンテンツの遠隔管理・更新
リスク分析		● 表示の改ざん、不適切情報の掲載、データ消去によるコンテンツの有害化 ● CMSの不正利用等・・・回復困難性：中（プライバシ）、経済的影響：中（レピュテーション）
リスク評価		● 回復困難性：中（不適切情報の掲載によるプライバシ侵害） ● 経済的影響：中（表示の改ざんによる行政サービス業務の機能不全）
対策の方向性		● CMSの利用端末を専用端末に限定する運用 ● STBやサイネージ本体を不正操作できないようする運用
対策の要件	機器運用前	● 装置の選定時における、将来にわたるサポート・アップデート提供の確認 ● CMSのOA系ネットワークからの分離、VPNまたは閉域網接続 ● 人目につく場所へのSTBの設置、サイネージ本体のポートの無効化
	機器運用中	● 専用端末の利用や、設定変更・掲載許可の承認プロセスの厳格化 ● ユーザ資格・・・なし ● 社会的サポート・・・なし



外構照明の光色制御

項目		概要
概要		● 近接する遊園地の観覧車の照明装置と市庁舎の外構の照明装置が連携して、同じタイミングで同一色に光色を変化させるなどの制御を行う
主な機能		● 照明装置の光色の連携制御 ● クラウド側からのスケジュール等のデータのダウンロード・適用
リスク分析		● いたずらによる設定変更に伴う照明装置の光色の異常動作 ● 照明装置の光色の異常動作等・・・経済的影響：小（レピュテーション）
リスク評価		● 回復困難性：小（光色の不正制御・点滅による健康障害） ● 経済的影響：小（照明装置の光色の異常動作等による行政の信用低下）
対策の方向性		● 制御方式を制限する運用
対策の要件	機器運用前	● 設定変更可能な端末をクラウドまたはサーバー室の機器に限定する運用（末端機器からの制御は不可とする）
	機器運用中	● 近接する遊園地の観覧車の照明装置以外の外部連携の制限 ● ユーザ資格・・・なし ● 社会的サポート・・・なし



1．ビルガイドラインの高度化のための調査
①空調等のビルの個別設備システムの対応策に関する調査
②スマートビルのサイバーセキュリティ対策を意識したユースケース調査
③その他関連する調査
③－１　インシデントレスポンスに対する要求の整理
③－２　ガイドラインへの追加情報の充実化
③－３　ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討

2．ビルシステムのサイバーセキュリティ推進体制の調査
①推進体制の情報提供・共有・相談等の機能の実践的評価
②推進体制のあり方の調査

3．検討会の運営
①ビルSWGの運営
②作業グループの運営
③その他の運営

１．ビルガイドラインの高度化のための調査
③その他関連する調査
③－１　インシデントレスポンスに対する要求の整理

- インシデントレスポンスに対する要求の整理では、OT系のインシデントレスポンスのガイドライン例について見当たらないため、一般的なIT系のインシデントレスポンスの例として、多くに参照されている、NIST Framework for Improving Critical Infrastructure Cybersecurity（重要インフラのサイバーセキュリティを改善するためのフレームワーク）、NIST SP800-61 Computer Security Incident Handling Guide（コンピュータセキュリティインシデント対応ガイド）を調査・分析した。
- そのうえで、ビルシステムにおいては、インシデントレスポンスの対応者が誰であるのかという実態に即して検討する必要があるが、後述する作業グループにおいて、ビルシステム関係者からの意見聴取を行いつつ、インシデントレスポンスの検討の際に必要となる観点を整理した。
- さらに、インシデントレスポンスの検討の際に必要となる観点については、後述するビルSWGにおいて、有識者、ビルシステム関係者からの意見聴取を行った。

NIST Framework for Improving Critical Infrastructure Cybersecurity （重要インフラのサイバーセキュリティを改善するためのフレームワーク）の概要

- NIST 重要インフラのサイバーセキュリティを改善するためのフレームワークは、重要インフラのサイバーセキュリティリスクマネジメントを改善することを目的として策定され、主に組織がサイバーセキュリティリスクを識別、評価し、管理するための組織的なプロセスについて解説している。

重要インフラ向けのサイバーセキュリティリスクを識別、評価し、管理するための組織的なプロセス

- 識別：主に自組織のリソースや活動上のリスクを確認し、リスクを管理するためのプロセスを定めること等を求めている。
- 防御：リスクから組織や資産を守り、重要サービスを提供するための保護対策、管理方式や手順を定めること、教育等の措置をとることを求めている。
- 検知：サイバー攻撃等の発生をいち早く認識、識別するための対策やその実施を求めている。
- 対応：検知されたサイバー攻撃を封じ込めるための適切な方策、関係者との適切な連絡・調整、対策を確実なものとし、復旧に資する分析を行うことなどを求めている。
- 復旧：サイバー攻撃によって失われた活動を元に戻すための方策、新たな攻撃に備えるための改善活動、それを実現する関係者とのコミュニケーション等を求めている。

NIST Framework for Improving Critical Infrastructure Cybersecurity （重要インフラのサイバーセキュリティを改善するためのフレームワーク）の概要

重要インフラ向けのサイバーセキュリティフレームワークの機能のうち、①識別におけるカテゴリー及びサブカテゴリー

	カテゴリー	サブカテゴリー
①識別	資産管理（ID.AM）：自組織が事業目的を達成することを可能にするデータ、人員、デバイス、システム、施設が、識別され、組織の目的と自組織のリスク戦略における相対的な重要性に応じて管理されている。	● ID.AM-1: 自組織内の物理デバイスとシステムが、目録作成されている。 ● ID.AM-2: 自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。 ● ID.AM-3: 組織内の通信とデータフロー図が、作成されている。 ● ID.AM-4: 外部情報システムが、カタログ作成されている。 ● ID.AM-5: リソース（例:ハードウェア、デバイス、データ、時間、人員、ソフトウェア）が、それらの分類、重要度、ビジネス上の価値に基づいて優先順位付けられている。 ● ID.AM-6: 全労働力と利害関係にある第三者（例:サプライヤー、顧客、パートナー）に対してのサイバーセキュリティ上の役割と責任が、定められている。
	ビジネス環境（ID.BE）：自組織のミッション、目標、利害関係者、活動が、理解され、優先順位付けが行われている。この情報は、サイバーセキュリティ上の役割、責任、リスクマネジメント上の意思決定を伝えるために使用されている。	● ID.BE-1: サプライチェーンにおける自組織の役割が、識別され、周知されている。 ● ID.BE-2: 重要インフラとその産業分野における自組織の位置付けが、識別され、周知されている。 ● ID.BE-3: 組織のミッション、目標、活動の優先順位が、定められ、周知されている。 ● ID.BE-4: 重要サービスを提供する上での依存関係と重要な機能が、定められている。 ● ID.BE-5: 重要サービスの提供を支援するレジリエンスに関する要求事項が、すべてのオペレーション状況（例：脅迫・攻撃下、復旧時、通常時等）について定められている。

NIST Framework for Improving Critical Infrastructure Cybersecurity （重要インフラのサイバーセキュリティを改善するためのフレームワーク）の概要

重要インフラ向けのサイバーセキュリティフレームワークの機能のうち、①識別におけるカテゴリー及びサブカテゴリー

	カテゴリー	サブカテゴリー
①識別	ガバナンス（ID.GV）：自組織に対する規制、法律、リスク、環境、運用上の要求事項を、管理し、モニタリングするためのポリシー、手順、プロセスが理解されており、経営層にサイバーセキュリティリスクについて伝えている。	● ID.GV-1: 組織のサイバーセキュリティポリシーが、定められ、周知されている。 ● ID.GV-2: サイバーセキュリティ上の役割と責任が、内部の担当者と外部パートナーとで調整・連携されている。 ● ID.GV-3: プライバシーや人権に関する義務を含む、サイバーセキュリティに関する法規制上の要求事項が、理解され、管理されている。 ● ID.GV-4: ガバナンスとリスクマネジメントプロセスが、サイバーセキュリティリスクに対処している。
	リスクアセスメント（ID.RA）：自組織は、（ミッション、機能、イメージ、評判を含む）組織の業務、組織の資産、個人に対するサイバーセキュリティリスクを把握している。	● ID.RA-1: 資産の脆弱性が、識別され、文書化されている。 ● ID.RA-2: サイバー脅威に関する情報が、複数の情報共有フォーラムおよび複数のソースから入手されている。 ● ID.RA-3: 内部および外部からの脅威が、識別され、文書化されている。 ● ID.RA-4: ビジネスに対する潜在的な影響とその発生可能性が、識別されている。 ● ID.RA-5: 脅威、脆弱性、発生可能性、影響が、リスクを判断する際に使用されている。 ● ID.RA-6: リスク対応が、識別され、優先順位付けされている。
	リスクマネジメント戦略（ID.RM）：自組織の優先順位、制約、リスク許容度、想定が、定められ、運用リスクに対する意思決定を支援するために利用されている。	● ID.RM-1: リスクマネジメントプロセスが、組織の利害関係者によって定められ、管理され、承認されている。 ● ID.RM-2: 組織のリスク許容度が、決定され、明確に表現されている。 ● ID.RM-3: 自組織によるリスク許容度の決定が、重要インフラにおける組織の役割と、その分野に特化したリスク分析の結果に基づいて行われている。

NIST Framework for Improving Critical Infrastructure Cybersecurity （重要インフラのサイバーセキュリティを改善するためのフレームワーク）の概要

重要インフラ向けのサイバーセキュリティフレームワークの機能のうち、①識別におけるカテゴリー及びサブカテゴリー

①識別

カテゴリー	サブカテゴリー
サプライチェーンリスクマネジメント（ID.SC）：自組織の優先順位、制約、リスク許容度、想定が、定められ、サプライチェーンリスクマネジメントに関連するリスクに対する意思決定を支援するために利用されている。自組織は、サプライチェーンリスクを識別し、分析・評価し、管理するためのプロセスを定め、実装している。	● ID.SC-1: サイバーサプライチェーンのリスクマネジメントプロセスが、組織の利害関係者によって、識別され、定められ、評価され、管理され、承認されている。 ● ID.SC-2: 情報システム、コンポーネント、サービスのサプライヤーと第三者であるパートナーが、識別され、優先順位付けられ、サイバーサプライチェーンのリスクアセスメントプロセスにより評価されている。 ● ID.SC-3: サプライヤーおよび第三者であるパートナーとの契約が、組織のサイバーセキュリティプログラムやサイバーサプライチェーンのリスクマネジメント計画の目的を達成するための適切な対策の実施に活用されている。 ● ID.SC-4: サプライヤーおよび第三者であるパートナーが、監査、テストの結果、またはその他の評価に基づき、契約上の義務を満たしているか、定期的に評価されている。 ● ID.SC-5: 対応・復旧計画の策定とテストが、サプライヤーおよび第三者プロバイダーと共に行なわれている。

NIST Framework for Improving Critical Infrastructure Cybersecurity （重要インフラのサイバーセキュリティを改善するためのフレームワーク）の概要

重要インフラ向けのサイバーセキュリティフレームワークの機能のうち、②防御におけるカテゴリー及びサブカテゴリー

②防御

カテゴリー	サブカテゴリー
アイデンティティ管理、認証／アクセス制御（PR.AC）：物理的・論理的資産および関連施設へのアクセスが、認可されたユーザ、プロセス、デバイスに限定されている。また、これらのアクセスは、認可された活動およびトランザクションに対する不正アクセスのリスクアセスメントと一致して、管理されている。	● PR.AC-1: 認可されたデバイス、ユーザ、プロセスのアイデンティティと証明書が、発行、管理、検証、取り消し、監査されている。 ● PR.AC-2: 資産に対する物理アクセスが、管理され、保護されている。 ● PR.AC-3: リモートアクセスが、管理されている。 ● PR.AC-4: アクセスの許可および認可が、最小権限の原則および役割の分離の原則を組み入れて、管理されている。 ● PR.AC-5: ネットワークの完全性が、保護されている（例：ネットワークの分離、ネットワークのセグメント化）。 ● PR.AC-6: IDは、ID利用者の本人確認がなされ、証明書に紐付けられ、インタラクションで使用されている。 ● PR.AC-7: ユーザ、デバイス、その他の資産は、トランザクションのリスク（例：個人のセキュリティおよびプライバシー上のリスク、その他組織にとってのリスク）の度合いに応じた認証（例：一要素、多要素）が行われている。
意識向上およびトレーニング（PR.AT）：自組織の人員およびパートナーは、関連するポリシー、手順、契約に基づいた、サイバーセキュリティに関する義務と責任を果たせるようにするために、サイバーセキュリティ意識向上教育とトレーニングが実施されている。	● PR.AT-1: すべてのユーザは、情報が周知され、トレーニングが実施されている。 ● PR.AT-2: 権限を持つユーザが、自身の役割と責任を理解している。 ● PR.AT-3: 第三者である利害関係者（例：サプライヤー、顧客、パートナー）が、自身の役割と責任を理解している。 ● PR.AT-4: 上級役員（セキュリティ担当役員）が、自身の役割と責任を理解している。 ● PR.AT-5: 物理セキュリティおよびサイバーセキュリティの担当者が、自身の役割と責任を理解している。

NIST Framework for Improving Critical Infrastructure Cybersecurity （重要インフラのサイバーセキュリティを改善するためのフレームワーク）の概要

重要インフラ向けのサイバーセキュリティフレームワークの機能のうち、②防御におけるカテゴリー及びサブカテゴリー

②防御

カテゴリー	サブカテゴリー
データセキュリティ（PR.DS）：情報と記録（データ）が、情報の機密性、完全性、可用性を保護するための自組織のリスク戦略に従って管理されている。	● PR.DS-1: 保存されているデータが、保護されている。 ● PR.DS-2: 伝送中のデータが、保護されている。 ● PR.DS-3: 資産は、撤去、譲渡、廃棄に至るまで、正式に管理されている。 ● PR.DS-4: 可用性を確保するのに十分な容量が、維持されている。 ● PR.DS-5: データ漏えいに対する防御対策が、実装されている。 ● PR.DS-6: 完全性チェックメカニズムが、ソフトウェア、ファームウェア、および情報の完全性を検証するために使用されている。 ● PR.DS-7: 開発・テスト環境が、実稼働環境から分離されている。 ● PR.DS-8: 完全性チェックメカニズムが、ハードウェアの完全性を検証するために使用されている。
情報を保護するためのプロセスおよび手順（PR.IP）：（目的、範囲、役割、責任、経営コミットメント、組織間の調整について記した）セキュリティポリシー、プロセス、手順が、維持され、情報システムと資産の防御の管理に使用されている。	● PR.IP-1: 情報技術/産業用制御システムのベースラインとなる構成は、セキュリティ原則（例：最低限の機能性の概念）を組み入れて、定められ、維持されている。 ● PR.IP-2: システムを管理するためのシステム開発ライフサイクルが、実装されている。 ● PR.IP-3: 構成変更管理プロセスは、策定されている。 ● PR.IP-4: 情報のバックアップが、実施され、維持され、テストされている。 ● PR.IP-5: 組織の資産の物理的な運用環境に関するポリシーと規制が、満たされている。 ● PR.IP-6: データは、ポリシーに従って破壊されている。 ● PR.IP-7: 防御プロセスは、改善されている。 ● PR.IP-8: 防御技術の有効性に関する情報が、共有されている。 ● PR.IP-9: （インシデント対応および事業継続）対応計画と（インシデントからの復旧および災害復旧）復旧計画が、策定され、管理されている。

NIST Framework for Improving Critical Infrastructure Cybersecurity （重要インフラのサイバーセキュリティを改善するためのフレームワーク）の概要

重要インフラ向けのサイバーセキュリティフレームワークの機能のうち、②防御におけるカテゴリー及びサブカテゴリー

②防御

カテゴリー	サブカテゴリー
(前ページからの続き)	● PR.IP-10: 対応計画と復旧計画が、テストされている。 ● PR.IP-11: サイバーセキュリティには、人事に関わるプラクティス（例:アクセス権限の無効化、人員のスクリーニング）が含まれている。 ● PR.IP-12: 脆弱性管理計画が、作成され、実装されている。
保守（PR.MA）: 産業用制御システムと情報システムのコンポーネントの保守と修理が、ポリシーと手順に従って実施されている。	● PR.MA-1: 組織の資産の保守と修理は、承認・管理されたツールを用いて実施され、ログが記録されている。 ● PR.MA-2: 組織の資産に対する遠隔保守は、承認を得て、ログが記録され、不正アクセスを防止した形式で実施されている。
保護技術（PR.PT）: 技術的なセキュリティソリューションが、関連するポリシー、手順、契約に基づいて、システムと資産のセキュリティとレジリエンスを確保するために管理されている。	● PR.PT-1: 監査記録/ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。 ● PR.PT-2: リムーバブルメディアは、保護され、その使用がポリシーに従って制限されている。 ● PR.PT-3: 最低限の機能性の原則が、必須の機能のみ提供するようにシステムを構成することによって組み入れられている。 ● PR.PT-4: 通信（情報）ネットワークと制御ネットワークが、保護されている。 ● PR.PT-5: メカニズム（例：フェールセーフ、ロードバランシング、ホットスワップ）が、平時及び緊急時においてレジリエンスに関する要求事項を達成するために実装されている。

NIST Framework for Improving Critical Infrastructure Cybersecurity （重要インフラのサイバーセキュリティを改善するためのフレームワーク）の概要

重要インフラ向けのサイバーセキュリティフレームワークの機能のうち、③検知におけるカテゴリー及びサブカテゴリー

③検知

カテゴリー	サブカテゴリー
異常とイベント（DE.AE）：異常な活動は、検知されており、イベントがもたらす潜在的な影響が、把握されている。	● DE.AE-1: ネットワーク運用のベースラインと、ユーザとシステムで期待されるデータフローが、定められ、管理されている。 ● DE.AE-2: 検知したイベントは、攻撃の標的と手法を理解するために分析されている。 ● DE.AE-3: イベントデータは、複数の情報源やセンサーから収集され、相互分析されている。 ● DE.AE-4: イベントがもたらす影響が、判断されている。 ● DE.AE-5: インシデント警告の閾値が、定められている。
セキュリティの継続的なモニタリング（DE.CM）：情報システムと資産は、サイバーセキュリティイベントを識別し、保護対策の有効性を検証するために、モニタリングされている。	● DE.CM-1: ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。 ● DE.CM-2: 物理環境は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。 ● DE.CM-3: 人員の活動は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。 ● DE.CM-4: 悪質なコードは、検知されている。 ● DE.CM-5: 不正なモバイルコードは、検知されている。 ● DE.CM-6: 外部サービスプロバイダの活動は、潜在的なサイバーセキュリティイベントを検知できるようにモニタリングされている。 ● DE.CM-7: 権限のない人員、接続、デバイス、ソフトウェアのモニタリングが、実施されている。 ● DE.CM-8: 脆弱性スキャンが、実施されている。

NIST Framework for Improving Critical Infrastructure Cybersecurity （重要インフラのサイバーセキュリティを改善するためのフレームワーク）の概要

重要インフラ向けのサイバーセキュリティフレームワークの機能のうち、③検知及び④対応におけるカテゴリー及びサブカテゴリー

	カテゴリー	サブカテゴリー
③検知	検知プロセス（DE.DP）：検知プロセスおよび手順が、異常なイベントに確実に気付くために維持され、テストされている。	● DE.DP-1: 検知に関する役割と責任は、説明責任を果たせるように明確に定義されている。 ● DE.DP-2: 検知活動は、該当するすべての要求事項を準拠している。 ● DE.DP-3: 検知プロセスが、テストされている。 ● DE.DP-4: イベント検知情報が、周知されている。 ● DE.DP-5: 検知プロセスが、継続的に改善されている。
④対応	対応計画（RS.RP）：対応プロセスおよび手順が、検知したサイバーセキュリティインシデントに対応できるように実施され、維持されている。	● RS.RP-1: 対応計画が、インシデントの発生中または発生後に実行されている。
	コミュニケーション（RS.CO）：対応活動が、内外の利害関係者との間で調整されている（例：法執行機関からの支援）。	● RS.CO-1: 人員は、対応が必要になった時の自身の役割と行動の順序を認識している。 ● RS.CO-2: インシデントが、定められた基準に沿って報告されている。 ● RS.CO-3: 対応計画に従って、情報が共有されている。 ● RS.CO-4: 利害関係者との間で調整が、対応計画に従って行なわれている。 ● RS.CO-5: サイバーセキュリティに関する状況認識を広げるために、外部利害関係者との間で自発的な情報共有が行なわれている。

NIST Framework for Improving Critical Infrastructure Cybersecurity （重要インフラのサイバーセキュリティを改善するためのフレームワーク）の概要

重要インフラ向けのサイバーセキュリティフレームワークの機能のうち、④対応におけるカテゴリー及びサブカテゴリー

④対応

カテゴリー	サブカテゴリー
分析 （RS.AN）：分析は、効果的な対応を確実にし、復旧活動を支援するために実施されている。	● DE.DP-1: 検知に関する役割と責任は、説明責任を果たせるように明確に定義されている。 ● DE.DP-2: 検知活動は、該当するすべての要求事項を準拠している。 ● DE.DP-3: 検知プロセスが、テストされている。 ● DE.DP-4: イベント検知情報が、周知されている。 ● DE.DP-5: 検知プロセスが、継続的に改善されている。
対応計画（RS.RP）：対応プロセスおよび手順が、検知したサイバーセキュリティインシデントに対応できるように実施され、維持されている。	● RS.AN-1: 検知システムからの通知は、調査されている。 ● RS.AN-2: インシデントがもたらす影響は、把握されている。 ● RS.AN-3: フォレンジックが、実施されている。 ● RS.AN-4: インシデントは、対応計画に従って分類されている。 ● RS.AN-5: プロセスは、内外のソース（例：内部テスト、セキュリティ情報、セキュリティ研究者）から報告された脆弱性情報を、自組織が受け取り、分析し、対応するために定められている。
低減（RS.MI）：活動は、イベントの拡大を防ぎ、その影響を緩和し、インシデントを解決するために実施されている。	● RS.MI-1: インシデントは、封じ込められている。 ● RS.MI-2: インシデントは、緩和されている。 ● RS.MI-3: 新たに識別された脆弱性は、許容できるリスクである場合にはその旨を文書化され、そうでない場合にはリスクが緩和されている。
改善（RS.IM）：組織の対応活動は、現在と過去の検知/対応活動から学んだ教訓を取り入れることで改善されている。	● RS.IM-1: 対応計画は、学んだ教訓を取り入れられている。 ● RS.IM-2: 対応戦略は、更新されている。

NIST Framework for Improving Critical Infrastructure Cybersecurity （重要インフラのサイバーセキュリティを改善するためのフレームワーク）の概要

重要インフラ向けのサイバーセキュリティフレームワークの機能のうち、⑤復旧におけるカテゴリー及びサブカテゴリー

	カテゴリー	サブカテゴリー
⑤復旧	復旧計画（RC.RP）：復旧プロセスおよび手順は、サイバーセキュリティインシデントによる影響を受けたシステムや資産を復旧できるよう実行され、維持されている。	● RC.RP-1: 復旧計画が、サイバーセキュリティインシデントの発生中または発生後に実施されている。
	改善（RC.IM）：復旧計画およびプロセスが、学んだ教訓を将来の活動に取り入れることで改善されている。	● RC.IM-1: 復旧計画は、学んだ教訓を取り入れている。 ● RC.IM-2: 復旧戦略は、更新されている。
	コミュニケーション（RC.CO）：復旧活動は、内外の関係者（例：コーディネーティングセンター、インターネットサービスプロバイダ、攻撃システムのオーナー、被害者、他組織のCSIRT、ベンダ）との間で調整されている。	● RC.CO-1: 広報活動が、管理されている。 ● RC.CO-2: 評判は、インシデント発生後に回復されている。 ● RC.CO-3: 復旧活動は、内外の利害関係者だけでなく役員と経営陣にも周知されている。

NIST SP800-61 Computer Security Incident Handling Guide（コンピュータセキュリティインシデント対応ガイド）の概要

- NIST SP800-61 コンピュータセキュリティインシデント対応ガイドは、組織がセキュリティインシデント対応機能を確立し、インシデントへの対応を効率的に進められることを目的として策定され、主に①コンピュータセキュリティインシデント対応能力の組織化、②初期の準備フェーズから、インシデント発生後に教訓を生かすフェーズに至るインシデント対応プロセスについて解説している。

インシデント対応プロセス

NIST SP800-61 Computer Security Incident Handling Guide（コンピュータセキュリティインシデント対応ガイド）の概要

インシデント対応プロセスのうち、②検知と分析フェーズにおける必要事項

②検知と分析フェーズ

項目	概要
インシデントの分類	● インシデントの分類として、主なインシデントについて解説している。 ➢ サービス不能 ➢ 悪意のコード ➢ 不正アクセス ➢ 不適切な使用 ➢ 複合要素（１つのインシデントで２つ以上のインシデントを包含しているもの）
インシデントの兆候	● インシデントの兆候の例が示されている。 ➢ FTPサーバに対しバッファーオーバーフロー攻撃が仕掛けられたことを検知したネットワーク侵入検知センサーが、警報を発する ➢ ホストがワームに感染したことを検知したウイルス対策ソフトウェアが、警報を発する ➢ ウェブサーバがクラッシュする ➢ インターネット上のホストへのアクセスが遅いという、ユーザからの苦情を受ける ➢ システム管理者が、異常な文字が使われたファイル名を発見する ➢ ユーザがヘルプデスクを呼び出し、脅迫的な電子メールメッセージがあったことを報告する ➢ ホストのログに、監査設定の変更が記録される ➢ アプリケーションが、見慣れないリモートシステムからの、複数回のログインの試みの失敗をログに記録する ➢ 電子メール管理者が、怪しい内容の大量のバウンスメールを見つける ➢ ネットワーク管理者が、典型的なトラフィックフローからの異常な逸脱に気づく

NIST SP800-61 Computer Security Incident Handling Guide（コンピュータセキュリティインシデント対応ガイド）の概要

インシデント対応プロセスのうち、②検知と分析フェーズにおける必要事項

②検知と分析フェーズ

項目	概要
インシデントの兆候（前ページからの続き）	➢ ウェブサーバが、ウェブ脆弱性スキャナの使用を示すエントリーをログに記録する ➢ 組織のメールサーバの脆弱性をターゲットにした、新しいエクスプロイトの告知 ➢ 政治的ハッカーグループが、組織を攻撃するという声明を出して脅迫する
前兆と兆候のソース	● インシデントの兆候を表す情報のソースについて示されている。 ➢ コンピュータセキュリティソフトウェアの警報 • ネットワーク型IDPS、ホスト型IDPS、ワイヤレスIDPS、ネットワーク行動分析用IDPS • ウイルス対策ソフトウェアおよびスパムメール対策ソフトウェア • ファイル完全性チェックソフトウェア • サードパーティの監視サービス • オペレーティングシステム、サービス、アプリケーションのログ • ネットワーク機器のログ ➢ ログ • オペレーティングシステム、サービス、アプリケーションのログ • ネットワーク機器のログ ➢ 公に入手できる情報 • 新しい脆弱性とエクスプロイトに関する情報 • 他の組織でのインシデントに関する情報 ➢ 人（組織内の人間、他の組織の人間）

NIST SP800-61 Computer Security Incident Handling Guide（コンピュータセキュリティインシデント対応ガイド）の概要

インシデント対応プロセスのうち、②検知と分析フェーズにおける必要事項

②検知と分析フェーズ

項目	概要
インシデントの分析	● インシデントの兆候から、インシデントの分析をより簡単かつ効果的に行うための推奨事項について解説している。 ➢ ネットワークとシステムのプロファイル ➢ 正常動作の理解 ➢ 一元化されたログ取得とログ保管ポリシーの作成 ➢ イベント相関処理の実施 ➢ すべてのホストの時刻を同期させておく ➢ 情報の知識ベースの維持と利用 ➢ インターネットのサーチエンジンを使った調査 ➢ パケットスニッファを使った補足データの収集 ➢ データのフィルタリングの検討 ➢ 経験を最優先する ➢ 経験が少ないスタッフのための診断マトリックスの作成 ➢ 他からの支援を求める
インシデントの文書化	● インシデントを記録するデータベースに格納すべき情報が示されている。 ➢ インシデントの現在の状態 ➢ インシデントの概要 ➢ 当該インシデントに対して、インシデント処理担当者がとった行動の内容 ➢ 他の関連者(システム所有者、システム管理者など)の連絡先情報

NIST SP800-61 Computer Security Incident Handling Guide（コンピュータセキュリティインシデント対応ガイド）の概要

インシデント対応プロセスのうち、②検知と分析フェーズにおける必要事項

②検知と分析フェーズ

項目	概要
インシデントの文書化（前ページからの続き）	➢ インシデント調査の際に収集した証拠の一覧 ➢ インシデント処理担当者からのコメント ➢ 次にとるべきステップ(例えば、システム管理者によるアプリケーションへのパッチの適用を待つなど)
インシデントの優先順位付け	● インシデント対応の優先順位付けは、「インシデントによる、現在および将来起こりうる技術的な影響」と「影響を受けたリソースの重要度」により判断することが示されている。
インシデントの通知	● インシデントを分析して優先順位した後、インシデント対応チームは組織内の適切な人間や、場合によっては他の組織に通知する必要がある。一般的な通知先となる関係者が示されている。 ➢ CIO ➢ 情報セキュリティ部門長 ➢ 各地区の情報セキュリティ担当 ➢ 組織内の他のインシデント対応チーム ➢ システムオーナー ➢ 人事部門(電子メールによる嫌がらせなど、職員が関係する場合) ➢ 広報部(公共性があるインシデント事件の場合) ➢ 法務部(法的問題が想定されるインシデントの場合) ➢ US-CERT (連邦政府機関または連邦政府機関の業務を代行するシステムは、報告が義務付けられている)

NIST SP800-61 Computer Security Incident Handling Guide（コンピュータセキュリティインシデント対応ガイド）の概要

インシデント対応プロセスのうち、③封じ込め、根絶、復旧フェーズにおける必要事項

③封じ込め、根絶、復旧フェーズ

項目	概要
封じ込め戦略の選択	● 封じ込めの戦略の基準を明確に文書化しておくことが示されている。また、適切な戦略を決定するための基準には、以下が含まれる。 ➢ リソースに対する潜在的な損害およびリソースの盗難の可能性 ➢ 証拠保全の必要性 ➢ サービスの可用性(ネットワーク接続、外部関係者へのサービス提供) ➢ 戦略を実施するのに必要な時間とリソース ➢ 戦略の有効性(インシデントの部分的な封じ込めや、完全な封じ込めなど) ➢ 対策の期間(たとえば、4時間以内に中止する緊急回避策、2週間以内に中止する一時回避策、恒久策など)
証拠の収集と処理	● 収集・記録されたすべての証拠をどのように保全したかを明確に文書化しておくことが示されている。また、すべての証拠に対して保管すべき詳細なログには、以下が含まれる。 ➢ 識別情報(たとえば場所、シリアル番号、型番号、ホスト名、MAC (Media Access Control)アドレス、コンピュータのIPアドレスなど) ➢ 調査中に証拠を収集・処理した者の名前、役職、電話番号 ➢ 証拠処理の日付と時刻(タイムゾーンを含む) ➢ 証拠の保管場所 ● また、インシデント発生が疑われる場合にはすぐに対象のシステムから証拠を収集することが望ましいことが示されている。また、収集された証拠を保全するための情報が提供されている。

NIST SP800-61 Computer Security Incident Handling Guide（コンピュータセキュリティインシデント対応ガイド）の概要

インシデント対応プロセスのうち、③封じ込め、根絶、復旧フェーズにおける必要事項

③封じ込め、根絶、復旧フェーズ

項目	概要
証拠の収集と処理（前ページからの続き）	➢ 標準コンピュータを対象としたフォレンジック ➢ モバイルデバイスを対象としたフォレンジック
アタッカーの特定	● インシデント対応チームは、あくまで封じ込め、根絶、復旧に重点を置くべきであること(アタッカーの特定は時間がかかる割には効果がないプロセスであること)が示されている。アタッカーを特定するために最も一般的に行われる活動について解説している。 ➢ アタッカーのIPアドレスの確認 ➢ アタッカーのシステムをスキャン ➢ サーチエンジンを使ったアタッカーの調査 ➢ インシデントデータベースの利用 ➢ 可能性のあるアタッカーの通信チャネルの監視
根絶と復旧	● インシデントを封じ込めた後、インシデントの要素を削除するための根絶を行わなくてはならない場合があることや、復旧では管理者がシステムを通常の運用状態に戻し、(該当する場合には)同様のインシデントが起きないようにシステムを強化する必要があることが示されている。なお、詳細な内容は、本ガイドの対象外となっている。

NIST SP800-61 Computer Security Incident Handling Guide（コンピュータセキュリティインシデント対応ガイド）の概要

インシデント対応プロセスのうち、④インシデント後の対応フェーズにおける必要事項

④インシデント後の対応フェーズ

項目	概要
教訓	● インシデント対応の最も大切な部分の一つが学習と改善であり、各インシデント対応チームは、新しい脅威に対して進化し、技術を向上させ、教訓を学ぶべきであることが示されている。その際にはすべての関係者が参加する「反省会」を開催することがセキュリティ対策とセキュリティ処理プロセス自体を改善するのに非常に有効であることが示されている。反省会で答えるべき質問には、以下の情報が含まれる。 ➢ 正確に何がいつ起きたか ➢ スタッフとマネジメント層がどの程度上手くインシデントに対処したか。文書化された手順に従ったか。それは適切であったか ➢ すぐに必要になった情報は何か ➢ 復旧を妨げたかもしれないステップや行動があったか ➢ 次に同様のインシデントが起きた場合、スタッフやマネジメント層は、どのような違った行動をとるか ➢ どのような是正措置があれば、将来にわたって同様のインシデントが起きるのを防げるか ➢ 将来、インシデントを検出、分析、軽減するために、どのようなツールやリソースが追加で必要となるか
収集されたインシデントデータの利用	● 収集されたインシデントデータについては、インシデント対応チームの追加投資の正当化や、インシデント対応チームの成功の評価、インシデント情報の報告を義務付けられている組織への報告に利用できるようにすることが有効であることが示されている。

NIST SP800-61 Computer Security Incident Handling Guide（コンピュータセキュリティインシデント対応ガイド）の概要

インシデント対応プロセスのうち、④インシデント後の対応フェーズにおける必要事項

④インシデント後の対応フェーズ

項目	概要
収集されたインシデントデータの利用（前ページからの続き）	● インシデント関連のデータに対する評価基準には、以下の基準が含まれる。 ➢ 処理したインシデントの数 ➢ インシデントごとの時間 • 当該インシデントに費やした労力の合計 • インシデントの開始から解決までに経過した時間 • インシデント処理プロセスの各ステージの経過時間 • 最初に報告を受けてから、インシデント対応チームが対応するまでの時間 • インシデントをマネジメント層に報告するまでに要した時間 ➢ 各インシデントの客観的な評価 • 確立したインシデント対応ポリシーや手順に準拠しているか • インシデントがどの程度効果的に記録されているか、インシデントのどの前兆や兆候が記録されているか • インシデントを検知する前にダメージを受けているか否か • インシデントの実際の原因が見つかったか否か • インシデントによる金銭的な損害の見積額 • どのような対策をしていればインシデントを予防できたか ➢ 各インシデントの主観的な評価
証拠の保管	● 証拠の保管のポリシーを確立することや、ポリシーを策定する際に考慮すべき要因(告訴、データの保管、コスト)が示されている。

要求①　ビル管理会社におけるインシデント対応力の強化

- 一般的なビルの場合、ビルのネットワーク内で何か問題が発生したときに対応する司令塔が不在であり、多くの場合において、ビル管理会社が最初に対応することになる。しかしながら、ビル管理会社においては、必ずしも十分な対応知識や対応スキル・ノウハウを持ち合わせておらず、原因(機器故障、ヒューマンエラー、サイバー攻撃等)の切り分けが難しい。
- 他方、ビル管理会社が原因の調査や封じ込め等の実際の対応を行う際に、かなりの部分は、BAベンダーに頼らざるを得ないのが実情である。

インシデントレスポンスに対する要求の整理

No	要求
1	ビル管理会社が行うべき対応の範囲を、これまでの機器故障だけでなく、ヒューマンエラーやサイバー攻撃によるシステム障害等にまで拡げて、その周知を行っていくことで、当該対応範囲での対応力を強化していくことが必要である。
2	ビル管理会社は、ベンダーや協力会社等の外部リソースや、内部リソースを含め、限られたリソースを活用して、ヒューマンエラーやサイバー攻撃によるシステム障害が発生した際に、どこまで対応が可能であるか等具体的な対応方法を事前に検討しておくことが必要である。
3	NIST SP800-61を参考にしようとしても、専門用語が多く、また実施すべき対策が多すぎる。ビル管理会社側のリソースが足りない現状を鑑みると、対策の中身をかみ砕いて行動レベルにまで落とし込んで、どのようにすれば実施してもらえるようになるかを検討しておくことが必要である。
4	ビル管理会社は、日頃からBAベンダーと連携し、インシデント対応における協働体制の構築を行うことが必要である。

要求①　ビル管理会社におけるインシデント対応力の強化

インシデントレスポンスに対する要求の整理（前ページからの続き）

No	要求
5	特に主要な制御機器については、何か問題が発生したときの対応処置について、ビル管理会社側でどこまで自律的に対応できるか(どこからは自律的に対応できないか)を検討し、予め対応計画に落とし込んでおくことが必要である。
6	事前に対応計画に定めた対応処置については、実際に問題が発生したときに、ビル管理会社が慌てることなく、適切に対応できるよう、対応マニュアルづくりや定期的な教育・訓練を行うことが必要である。
7	ビル管理会社で原因の切り分けができない場合は、通常、機器故障時に運用する対応プロセスと、CSIRTの運用による対応プロセスを同時並行で走らせることが必要である。またその際に、どのようなクリティカルな状況が発生した場合に、同時並行で対応プロセスを走らせるか、その判断基準を定めておくことも必要である。

要求②　ビルオーナーにおけるインシデント対応へのコミットメントの強化

- 機器故障の場合には、現場に出向き、データを見て、ユーザがどのように設定を行っているか等問題を確認・検知・分析し、その場で対応する。その場で対応できなければ、メーカーサポートにて対応する。一方、サイバー攻撃によるシステム障害の場合は、機器故障の場合に対応可能であった問題の確認・検知・分析が課題になる。
- ビルのネットワーク内で何か問題が発生した場合、原因に関わらず、すべての報告がビル管理会社に伝達される仕組みになっている。
- また、古いビルの制御システムの場合に、新しい処理プロセスを後から実装することは難しい。
- ビルの故障対応について対応するチームは、ビルごとに配備されているが、インシデント対応について対応できるSIRTを構築しているところは存在しない。インシデント対応についても、対応できる範囲は、故障対応の範囲を超えない。

インシデントレスポンスに対する要求の整理

No	要求
1	ビルオーナーにおいて、問題対応の当事者意識を持つことが必要である。
2	ビルオーナーが、インシデント対応を有効に機能させるため、ビル管理会社がインシデント対応を行ううえで必要となる仕組み(例：システムログの活用の仕組み、防災センター(中央監視室)のネットワーク接続のGW(ネットワークアクセスを制御するコントローラー)で通信パケットの解析を行う仕組み等)を導入することが必要である。

要求③　インシデント対応のレベル分け

- ビルの種類や規模に応じて、セキュリティ上の影響レベルが異なるため、それぞれのレベルに見合うインシデント対応が必要である。

インシデントレスポンスに対する要求の整理

No	要求
1	ビルの種類や規模に応じて、セキュリティ上の影響レベルを設定し、それぞれの影響レベルに見合うインシデントの捉え方や運用可能な対応の範囲・方法を検討することが必要である。

ビルSWGで出たインシデントレスポンスに関する意見

- インシデントレスポンスについては、権限整備関連の文書化とそれに基づく対応計画マニュアルづくり、ビルのレベル別や規模別の対応検討が求められている。

■ 権限整備関連の文書化とそれに基づく対応マニュアルづくりが必要

- 権限整備関連の文書化を追加してほしい。権限を文書化することで、インシデントが発生した際に、文書化されたマニュアルやルールに沿って、誰がどういったアクションをとるべきかを明確化してほしい。インシデントが発生してしまった際に属人的な判断に頼るのではなく、文書に規定されている行動を、決められた担当者が行えるようにしておくことがスムーズなインシデントレスポンスの実現に繋がると考える。
- 空調で例を挙げると、熱源系は一旦止めてしまって30分以内に再起動すると爆発するケースもあるので、権限整理等と合わせながらこういうことは実施しない、こういうことは気を付ける等を検討していきたいと考える。

■ ビルのレベル別や規模別の対応検討が必要

- JDCCのインシデント対応ガイドブックのターゲットはデータセンターであるため、一般的なビルにとっては若干ハードルの高い指標になっている。例を挙げるとすれば、一般のビルでは空調が停止したらインシデントとなるが、データセンターにおいては空調の停止は大事故になる。そのためそのまま一般のビルに適応するのは過剰品質になってしまうと思うため、どのようにビルセキュリティガイドラインに適応していくかは検討が必須になる。今後のビルセキュリティガイドラインの検討には、ビルのレベル別や規模別の対応検討が必須になってくる。

1．ビルガイドラインの高度化のための調査
①空調等のビルの個別設備システムの対応策に関する調査
②スマートビルのサイバーセキュリティ対策を意識したユースケース調査
③その他関連する調査
③－１　インシデントレスポンスに対する要求の整理
③－２　ガイドラインへの追加情報の充実化
③－３　ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討

2．ビルシステムのサイバーセキュリティ推進体制の調査
①推進体制の情報提供・共有・相談等の機能の実践的評価
②推進体制のあり方の調査

3．検討会の運営
①ビルSWGの運営
②作業グループの運営
③その他の運営

1．ビルガイドラインの高度化のための調査
③その他関連する調査
③－２　ガイドラインへの追加情報の充実化

■ビルガイドラインの高度化のための調査における現在のガイドラインへの追加情報の充実化の一つとして、ビルシステムにおける個別の対策事例を参考情報として蓄積するレポジトリ『ビルシステム・ネットワークの構成管理とセキュリティ対策』を作成した。

■ビルシステム・ネットワークの構成管理とセキュリティ対策に関する機能を有する製品として、以下の製品について調査を行った。それぞれの製品の概要を次頁以降に整理する。

No.	製品名	事業者名	製品概要	URL
1	ビル向けサイバーセキュリティソリューション	株式会社NTTファシリティーズ	リスクの見える化とそれによるセキュリティ対策の立案・提供を行う「コンサルティングサービス」、ネットワークの常時監視によるサイバー攻撃の予兆検知、分析、即時遮断を実施する「マネージド・セキュリティサービス」の2つのサービス構成により、万全のセキュリティ体制を築く。	https://www.ntt-f.co.jp/service/fm/cyber_sec/
2	三菱電機サイバーセキュリティーソリューション OTGUARD®（オオティガード）	三菱電機株式会社	１．OT・ITを活用した脆弱性診断により、サイバー攻撃のリスクを見える化 ２．サイバー攻撃の検知と遮断を一体で行う当社独自のセキュリティースイッチにより、強固なセキュリティー対策を実現 ３．幅広い運用サービスの提供により、事業継続を支援	https://www.mitsubishielectric.co.jp/business/biz-t/special/hot-topics/security/otguard.html
3	DPI(Deep Packet Inspection)製品	マクニカネットワークス株式会社	既存のシステムに影響を与えず、ネットワーク監視、異常検知、ネットワーク構成図作成、アセット管理等を自動で行えるようにする。	https://www.macnica.net/forescout/building.html/
4	SilentDefenseソリューション	マクニカネットワークス株式会社	ネットワーク可視化、異常検知の２つを、ネットワークに負荷を与えないパッシブ構成で実現する。	https://www.macnica.net/forescout/building.html/
5	Macnica Physical Finderソリューション	マクニカネットワークス株式会社	BACnet による操作対象となる物理デバイスをSilentDefense 上で可視化する。	https://www.macnica.net/forescout/building.html/
6	VISUACT™-X	アズビル株式会社	ITシステムに侵入したサイバー攻撃を検知するネットワークセンサ。発見することが困難なITシステム内部に侵入してしまった高度なサイバー攻撃の検知を独自のWindows解析技術で実現	https://www.visuact.jp/vx/

NTT ファシリティーズ：ビル向けサイバーセキュリティソリューション

◆ NTT ファシリティーズ：ビル向けサイバーセキュリティソリューション

- セキュリティアセスメント&プランニング

  ビル制御システムの現状を調査し、リスクシナリオ分析および IEC 62443 等の業界ベストプラクティスとギャップ分析により、事業インパクトに基づく対策を立案

- セキュリティ管理プログラム構築支援

  セキュリティ管理基準（組織・プロセス）、セキュリティ対策基準（技術的対策）、インシデント対応手順等のセキュリティポリシーを作成

- セキュリティ対策の設計・導入支援

  ネットワークのセグメント化、セキュリティツール導入の設計および構築

- 脅威検知・通知

  ビル制御ネットワークを流れる通信を常時監視し、サイバーセキュリティインシデントの兆候を発見

- サイバー攻撃遮断

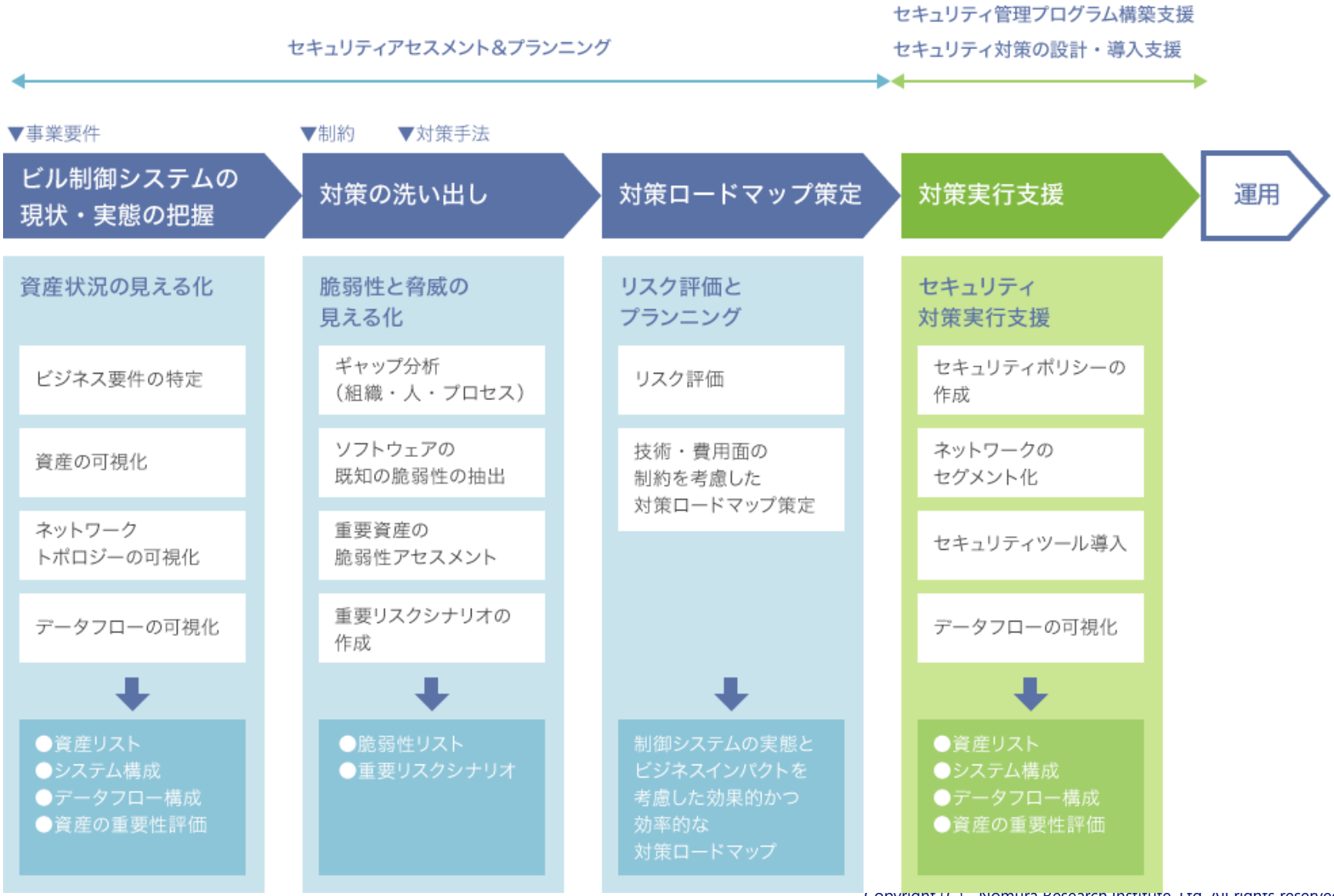
  常時監視の結果に基づき、不正な通信を遮断し、サイバーセキュリティインシデントの被害を最小化

- アセット状況の月次レポート

  通信状況の分析に基づき、ビル制御ネットワークの構成変更や新規端末の接続状況をレポート

NTT ファシリティーズ：ビル向けサイバーセキュリティソリューション

◆ NTT ファシリティーズ：ビル向けサイバーセキュリティソリューション

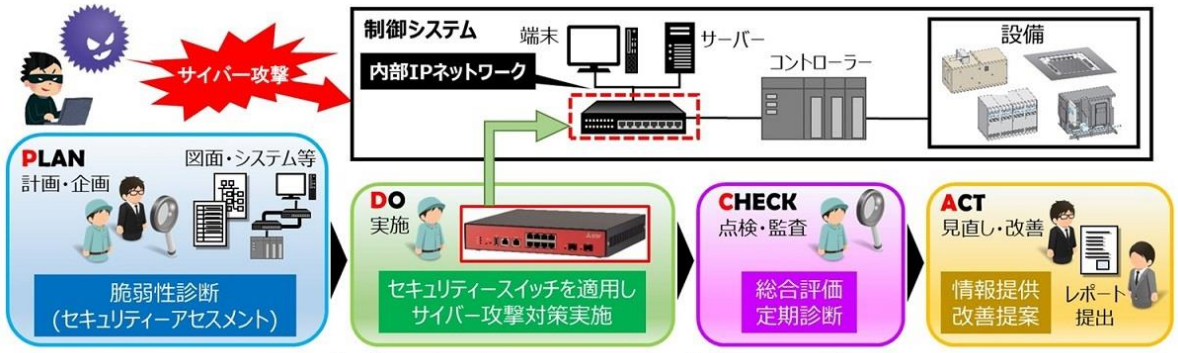


三菱電機サイバーセキュリティーソリューション：OTGUARD（オオティガード）

◆ 三菱電機サイバーセキュリティーソリューション：OTGUARD（オオティガード）

独自開発の「セキュリティースイッチ」により、送信元IPや宛先IP、パケット数、タイムスタンプなどのパケット情報をリアルタイムに分析し、有害通信を遮断する

- セキュリティスイッチは、ビル制御システム内のデータを集約するコントローラーと、サーバや端末との中間に配置
- OT・ITを活用した脆弱性診断により、サイバー攻撃のリスクを見える化
- 重要インフラをはじめ数多くの制御システム構築や保守サービスで培ったOT・ITを活用した脆弱性診断により、サイバー攻撃のリスクを見える化
- 診断結果に基づき、ニーズに合わせたPDCAサイクルを構築し、ワンストップで継続的な対策を支援
- 新規だけでなく既存の制御システムにも大規模なシステム改修を行わずに容易に導入可能
- 脆弱性診断に基づき、制御システム内の最適な場所に設置可能
- 幅広い運用サービスの提供により、事業継続を支援サポート窓口によるお問い合わせ対応や、技術者派遣による更新・故障対応、24時間遠隔システム監視サービス、改善提案など幅広い運用サービスを提供



三菱電機サイバーセキュリティーソリューション「OTGUARD®」の概要

マクニカネットワークス株式会社：DPI(Deep Packet Inspection) 製品

◆ マクニカネットワークス株式会社：DPI(Deep Packet Inspection) 製品

既存のシステムに影響を与えず、ネットワーク監視、異常検知、ネットワーク構成図作成、アセット管理等を自動で行う製品

- ベースライン設定

  システム内の正常通信をベースラインとして学習し、そこから外れる通信を異常として検知する機能。ビルシステムにおける異常をネットワークレベルで網羅的に検知する為に用いられる。

- 脅威インテリジェンス

  ビルシステムに対して脅威となり得る攻撃や、攻撃を受ける可能性のある危険な状態を検知する為にメーカによって用意されたシグネチャ。 ベースライン設定と組み合わせて利用する事で、検知した異常の内容をより詳細にユーザに通知する為に用いられる。

- ネットワークマッピング

  各デバイスをネットワーク構成図にマッピングし、通信方向や各機器の役割と合わせて表示する機能。 異常発生時の被害デバイスの特定およびその復旧や、ネットワーク構成上リスク判定を行う為に用いられる。

- アセット管理

  各デバイスの持つIPアドレスやMACアドレスに加えて、ベンダ名、通信プロトコル、ファームウェアバージョン等の詳細情報のリストを作成する機能。サイバー攻撃被害発生時や保守/整備の際に各デバイスの情報を確認するためのアセット台帳とする為に用いられる。

- ダッシュボード

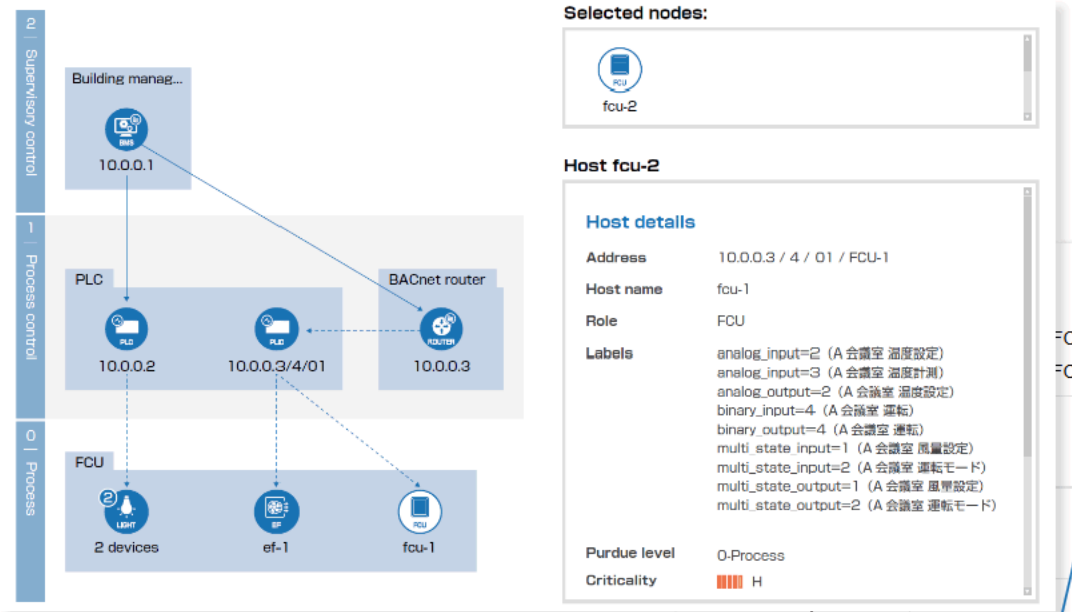
  検知したアラート内容や通信量等、DPI製品で取得した情報を表やグラフで表示する機能。ビルシステムの現在の状況や過去からの推移状況を表やグラフで可視化する為の機能。

ガイドラインへの追加情報の充実化

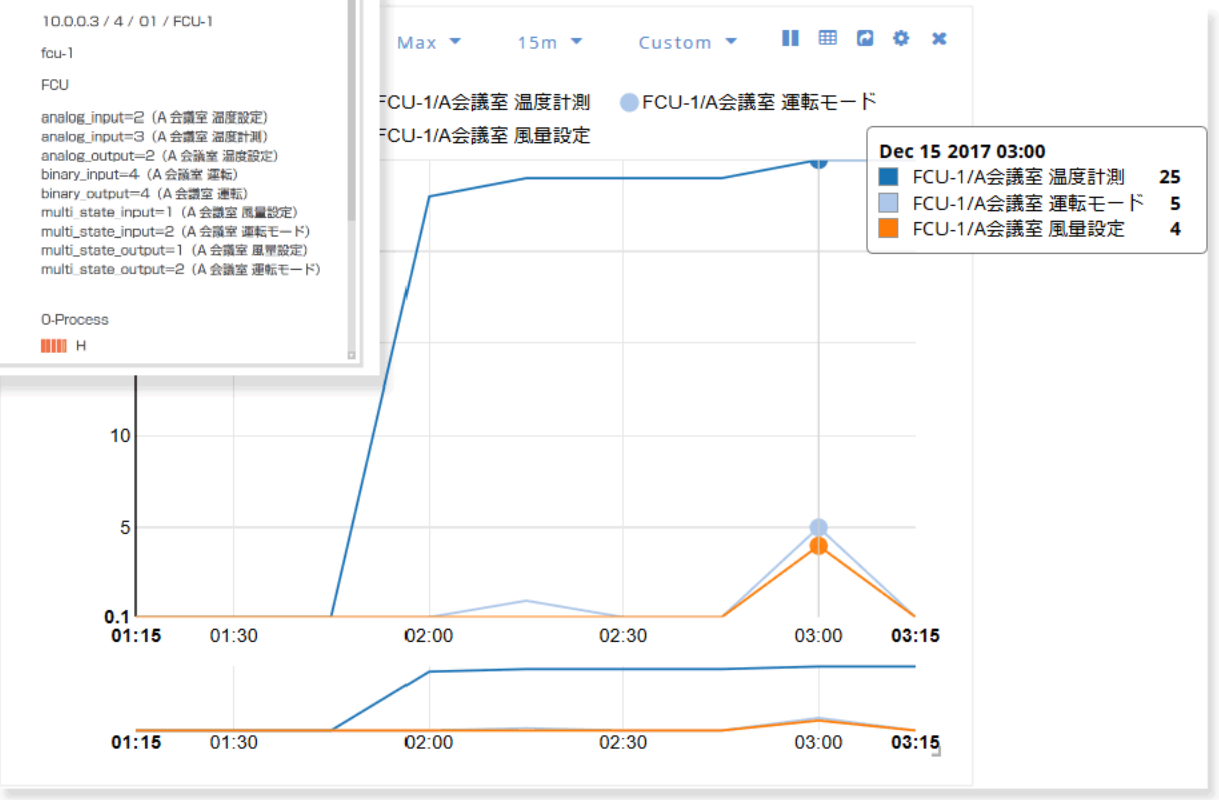
マクニカネットワークス株式会社：DPI(Deep Packet Inspection) 製品

◆ マクニカネットワークス株式会社：DPI(Deep Packet Inspection) 製品

物理デバイスまで含めた ネットワークの可視化 イメージ図



空調設備の値の監視　イメージ図



マクニカネットワークス株式会社：SilentDefense ソリューション

◆ マクニカネットワークス株式会社：SilentDefense ソリューション

ネットワーク可視化、異常検知の 2 つを、ネットワークに負荷を与えないパッシブ構成で実現する。

- ネットワークマップ機能

  監視センサーで収集したネットワーク情報をコマンドセンターでグラフィカルに閲覧する機能。ネットワークマップ機能により、特定期間や特定通信においてどういったプロトコルが多いのか？通信先はどこなのか？などのネットワークの傾向を確認することが可能。また、スニフィングしたパケットにより、モデル名、ファームウェアバージョン、脆弱性情報、システム間のプロトコルなど詳細なアセット情報をネットワーク経由で得て、アクティブでないホスト、脆弱性を持ったPLCを見つけることが可能。さらに、役割（ロール）あるいはネットワーク階層などを自動グルーピングすることも可能。

- セキュリティ検知

  Built-in ModuleやスレッドライブラリなどのForeScout社により実装された検知ロジックや、LAN CPやDPBIなどの事前学習によるホワイトリスト方式の検知機能。また、SD Scriptでは、ユーザが自身でLUA言語でスクリプトを書くことが可能。この機能により、SilentDefense で対応していないプロトコルや制御機器に対して、独自で追加開発してルールを実装することが可能。

- 3rdパーティ連携

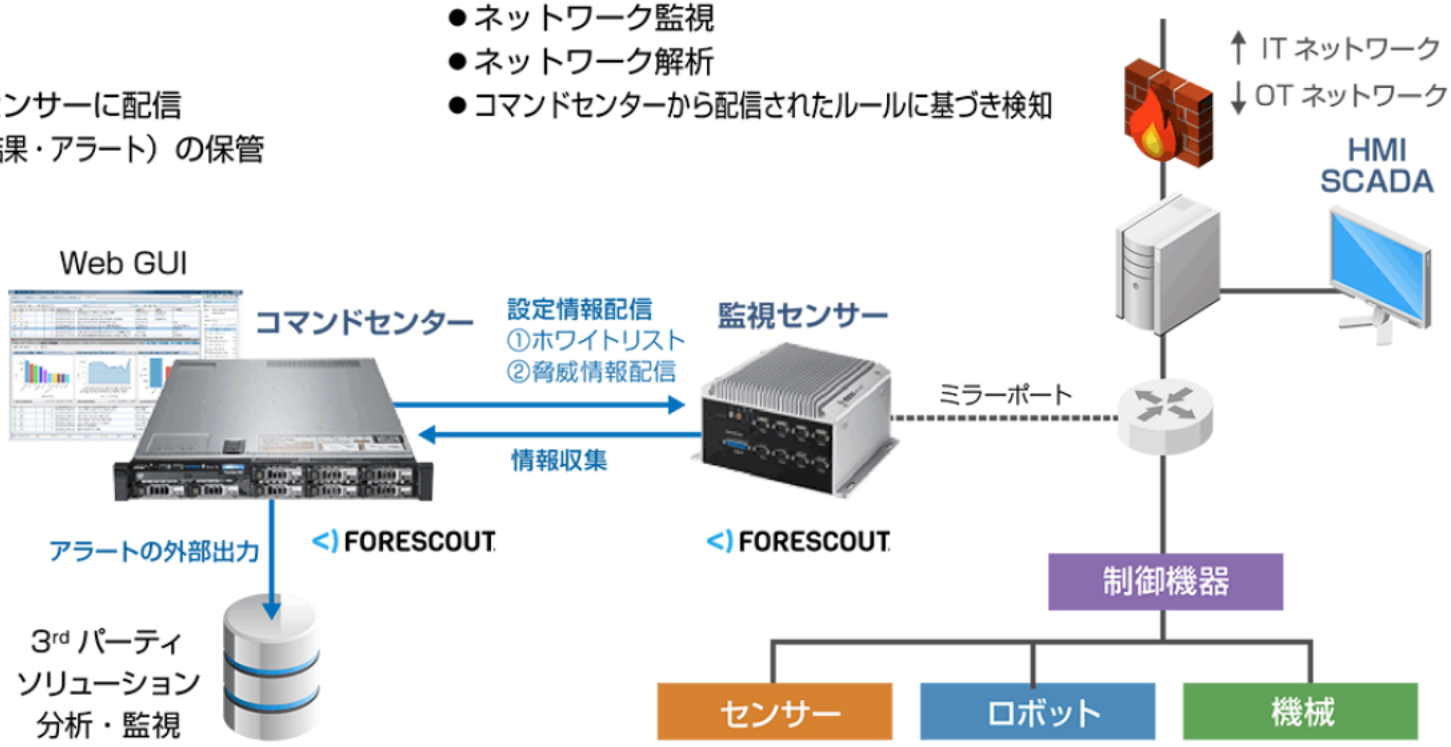
  SilentDefense で得た情報をログとして外部に出力することが可能。ArcSight,Splunk,McAfeeSIEM,QRadar などの分析ツールに Syslog でアラートログを出力、通信ログやステイタスログを Syslog サーバに出力することが可能。また、社内にある既存のADやLDAPなどの認証サーバの情報を取り込んで、分析をユーザ名ベースで行うことが可能。

マクニカネットワークス株式会社：SilentDefense ソリューション

◆ マクニカネットワークス株式会社：SilentDefense ソリューション

- グラフィカル表示
- ルール設定
- 設定したルールを監視センサーに配信
- データ（ネットワーク解析結果・アラート）の保管

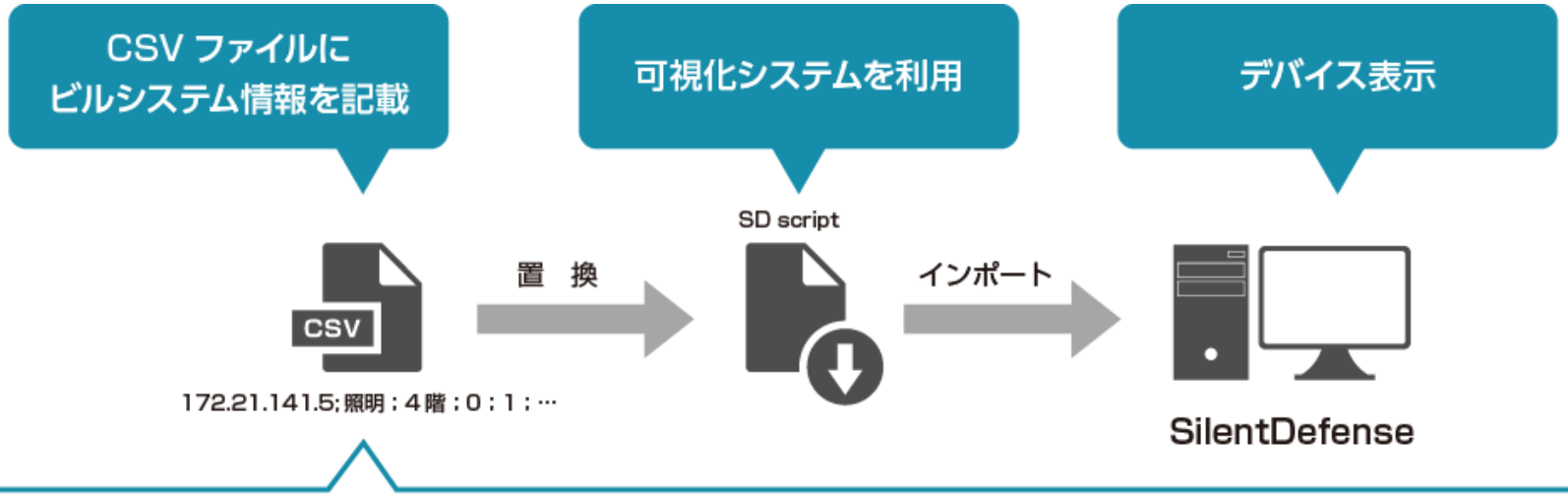
- ネットワーク監視
- ネットワーク解析
- コマンドセンターから配信されたルールに基づき検知



マクニカネットワークス株式会社：Physical Finder ソリューション

◆ マクニカネットワークス株式会社：Physical Finder ソリューション

BACnet による操作対象となる物理デバイスを SilentDefense 上で可視化。



BACnet ポイント

デバイス名	場　所	動　作
Light-1	3Fフロア	点灯
Light-2	4F事務室	点灯
EF-1	B1駐車場	運転
FCU-1	A会議室	温度設定
FCU-1	A会議室	温度計測
FCU-1	A会議室	運転
FCU-1	A会議室	風量設定
FCU-1	A会議室	運転モード

現在値

Dev. ユニット	Object type フォルダ	Inst. タグ
2	3	1
2	30	2
3	0	1
3	0	2
3	0	3
3	3	4
3	13	1
3	13	2

出力値

Dev. ユニット	Object type フォルダ	Inst. タグ
2	4	1
2	4	2
3	1	1
3	2	2
3		
3	4	1
3	14	1
3	14	2

状態

Present value					
0	1	2	3	4	5
消灯	点灯				
点灯	点灯				
停止	運転				
停止	運転				
	自動運転	弱運転	中運転	強運転	
	自動運転	弱運転	中運転	強運転	

アズビル株式会社：VISUACT-V

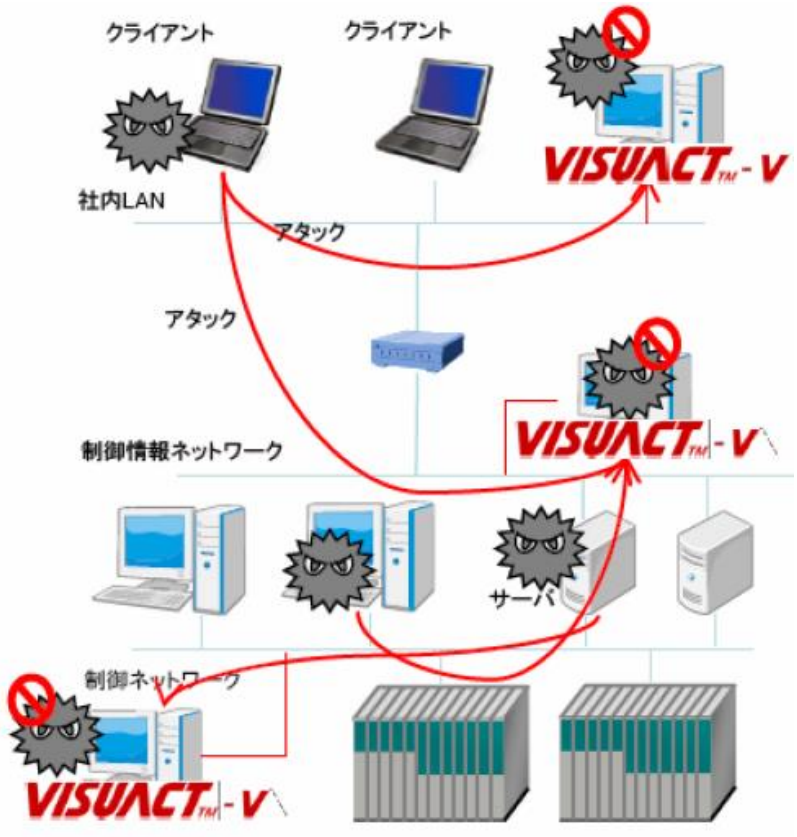
◆ アズビル株式会社：VISUACT-V

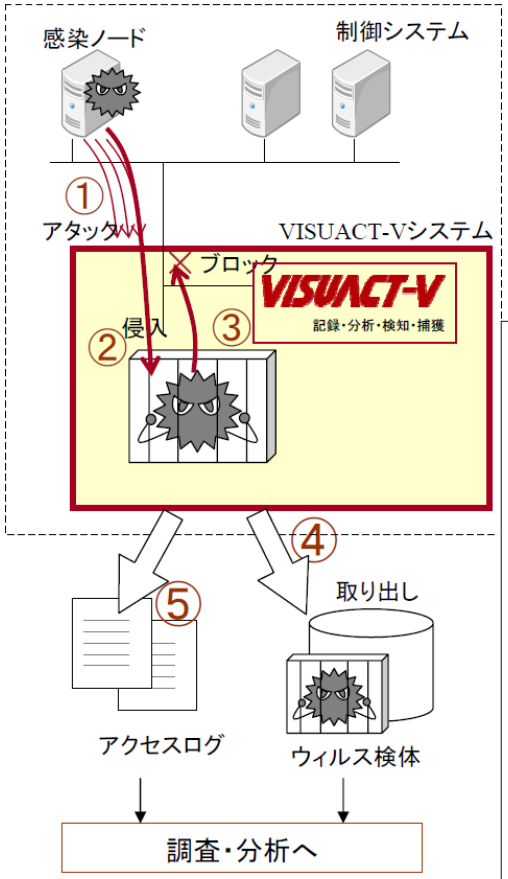
制御ネットワークにおいてウィルスの活動を検知するマルウェアセンサー

- 機能
  - ✓ VISUACTテクノロジーによりネットワークを監視／分析し、ウィルスの攻撃を検知・通知
  - ✓ 内部に侵入したウィルスの活動を検知し、ウィルスの検体を安全に捕獲
  - ✓ ファイヤーウォール機能により、捕獲したウィルスによる制御ネットワークへの攻撃を完全にブロック
  - ✓ 捕獲したウィルスをPCイメージごと安全に取り出すことが可能
  - ✓ 攻撃（通信内容）の詳細ログを、制御システムの外部（VISUACT-V内）に記録
- 特長
  - ✓ 稼働中の制御システムでも安全に着脱可能
  - ✓ ネットワークに接続するだけで使用できる
  - ✓ 制御ノードへのソフトウェアのインストールが不要
  - ✓ ネットワークへの通信負荷は一切ない
  - ✓ 独自開発したTAAN1(tm)（ティ・エー・エー・エヌ・ワン）テクノロジとVISUACT テクノロジ（Windows®ネットワークを見える化する技術）を組み合わせて搭載することにより、IT システムに侵入したサイバー攻撃の早期検知を実現
  - ✓ ネットワーク監視型を採用しているため、他のシステムと干渉せず、稼働中のＩＴシステムに悪影響なく導入することが可能
  - ✓ エンドポイントやゲートウェイ監視などのセキュリティ製品と組み合わせることで、精度の高いサイバー攻撃検知システムの構築が可能
  - ✓ 制御システム内に侵入したマルウェアを確保し、安全に取り出す機能を搭載

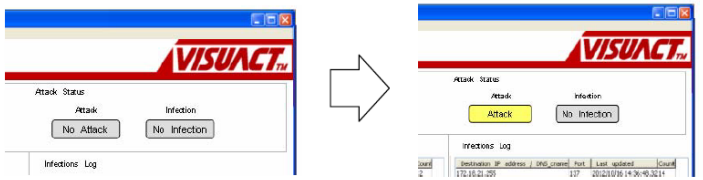
アズビル株式会社：VISUACT-V

◆ アズビル株式会社：VISUACT-V

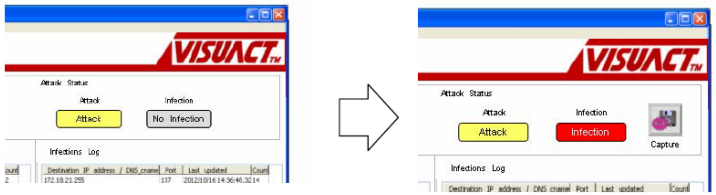




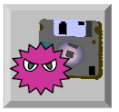
①攻撃→内部へのウィルスの侵入を検知



②侵入
③感染（拡散活動はブロック）



④ウィルスの検体を保存（捕獲）



⑤アクセスログを出力

レポジトリ：ビルシステム・ネットワークの構成管理とセキュリティ対策

レポジトリ：ビルシステム・ネットワークの構成管理とセキュリティ対策

［読み手］

ビルオーナー、設計事務所、個別システム事業者(ビル管理システム、ビルネットワーク)

［キーワード］

システム・設備・空間	ビルシステム、ビルネットワーク
ライフサイクル	設計・仕様(Planning/Procurement)、運用(Operation)、改修・廃棄(Reforming)
対策	システム・ネットワークの資産管理・構成管理・変更管理とセキュリティ対策

［キーメッセージ］

ビルオーナー、設計事務所、個別システム事業者(ビル管理システム、ビルネットワーク)は、ビルシステム・ネットワークの設計・構築・運用において、ビルシステム・ネットワークの資産管理・構成管理・変更管理を適切に実施すること。 また、ビルシステム・ネットワークを構成する機器に応じた適切なサイバーセキュリティ対策を実施すること。

【背景・状況】

IoT の導入やクラウドの利活用による BEMS の進展などに伴い、ビルシステムを構成する機器が多様化している。また、機器の多様化に合わせて、それらの機器と通信を行うためのさまざまなネットワーク機器が設置されるようになっている。

このような状況下、ビルシステム・ネットワークを構成する機器やネットワークの資産情報、システム構成・ネットワーク構成および変更履歴を適切に管理することが、ビルシステムの安定的な運用と適切なセキュリティ対策の実施において重要となっている。

しかし、現状においては、全てのビルオーナーが、ビルシステム・ネットワークの構成や、使用されている機器、変更履歴を正確に把握できているわけではない。

また、最新のシステム構成・ネットワーク構成を文書化して保管しているビルオーナーや、システムやネットワークの変更が行われた場合に、システム構成図・ネットワーク構成図を更新するための手続きや体制を整備しているビルオーナーは少ないと考えられる。

そのような状況においては、以下のようなリスクが存在する。

ガイドラインへの追加情報の充実化

レポジトリ：ビルシステム・ネットワークの構成管理とセキュリティ対策

- ✓ 機器にインストールされているOS・ソフトウェアの脆弱性管理を適切に行うことができず、脆弱性をついたサイバー攻撃のターゲットとなる。
- ✓ ビルシステム・ネットワークのどこにどのような機器が接続されているのかがわからないと、ビル内に不正に侵入した部外者によってシステムに不正な機器が接続されたことを検知することができず、不正に接続された機器を通じてシステムへの不正侵入を受ける。
- ✓ ビルシステム・ネットワークのネットワーク構成を正確に把握できていない場合、どの機器がどのネットワークに接続しているかがわからないため、不正なコマンドが検知された場合にどのネットワークセグメントで発生したのかを特定することができず、迅速な対応ができないだけでなく、事後調査・検証が困難になる。
- ✓ ビルシステム・ネットワークのネットワークと外部インターネットとの接続ポイントの管理が適切に実施されていないと、セキュリティ対策が十分ではない外部インターネット接続ポイントから不正侵入を受ける。

【適用範囲】

新築ビル、既存ビルを含め、すべてのビルを対象とする。

【必要とされる対策】

ビルシステム・ネットワークの設計・構築・運用において、ビルシステム・ネットワークの資産管理・構成管理・変更管理を適切に実施するための手続き・体制を整備する。

必要に応じて、ビルシステム・ネットワークの資産管理・構成管理・変更管理を自動化するための仕組み・ツールを導入する。

ガイドラインへの追加情報の充実化
レポジトリ：ビルシステム・ネットワークの構成管理とセキュリティ対策

【具体的な対策事例】

[ビルシステム・ネットワークに関する文書の適切な管理]

ビルの新築時や改築時に、設計事務所、個別システム事業者(ビル管理システム、ビルネットワーク)に対して、ビルシステム・ネットワークの完成図面の引き渡しを求める
個別システム事業者(ビル管理システム、ビルネットワーク)に対して、ビルシステム・ネットワークに変更があった場合に、ビルシステム・ネットワークの変更管理の適切な実施および、最新のシステム・ネットワークの構成図の引き渡しを求める。

[ビルシステム・ネットワークの資産管理・構成管理を行う責任者の任命]

システム・ネットワークの資産管理・構成管理を行う責任者を任命し、システム・ネットワークの資産管理・変更管理を適切に行う体制を整備することにより、ネットワーク、サーバ、PC 等の情報資産の正確な把握や、システム構成・ネットワーク構成の可視化が適切に実施されるようにする。

[ネットワーク機器、サーバ、PC 等の情報資産の正確な把握]

担当者へのヒアリング、社内に保管されている文書・図面の調査、システム・ネットワークを構成する機器が設置されている現場における目視調査等により、ネットワーク機器、サーバ、PC 等の情報資産を正確に記録した情報資産台帳を作成する。
情報資産台帳には、各機器に割り当てられた IP アドレスや MAC アドレス、OS・ファームウェアのバージョン、製造元のベンダ名、使用している通信プロトコル・ポート番号等を記載する。

ネットワーク機器、サーバ、PC 等の情報資産の定期的な棚卸しを実施し、情報資産台帳を常に最新の状態に維持する。

リソースや予算が確保できない等の事情により、人手による情報資産の正確な把握が難しい場合は、各機器に割り当てられた IP アドレスや MAC アドレス、OS・ファームウェアのバージョン、製造元のベンダ名、使用している通信プロトコル・ポート番号等の詳細な資産情報のリストを自動的に作成することができるツールを利用することも選択肢となる。

ガイドラインへの追加情報の充実化

レポジトリ：ビルシステム・ネットワークの構成管理とセキュリティ対策

[システム構成・ネットワーク構成の可視化]

担当者へのヒアリング、社内に保管されている文書・図面の調査、システム・ネットワークを構成する機器が設置されている現場における目視確認、ネットワークを流れるデータパケットの調査等を実施し、システム構成図・ネットワーク構成図を作成する。

システム構成図・ネットワーク構成図には、機器のモデル名やソフトウェア・ファームウェアのバージョン、脆弱性情報、システム間で使用されている通信プロトコル、使用しているポート番号、システムの相互接続状況、接続している外部システム、インターネット接続ポイント等を記載する。

システム構成・ネットワーク構成の定期的なレビューを実施し、システム構成図・ネットワーク構成図を常に最新の状態に維持する。

リソースや予算が確保できない等の事情により、人手によるシステム構成・ネットワーク構成の可視化作業が難しい場合は、資産の把握やネットワーク構成図作成等を自動で行うツールを導入することも選択肢になる。
たとえば、システム内でやりとりされる通信パケットを監視・解析することにより、機器のモデル名やソフトウェア・ファームウェアのバージョン、脆弱性情報、システム間で使用されている通信プロトコル、使用しているポート番号などの詳細なアセット情報を収集することができるツールが市販されている。
機器をネットワーク構成図にマッピングし、通信方向や各機器の役割を表示することができるツールもある。

レポジトリ：ビルシステム･ネットワークの構成管理とセキュリティ対策

[ビルシステム・ネットワークに対する適切なサイバーセキュリティ対策の実施]

1. 脆弱性管理

作成した情報資産台帳を利用して、ネットワーク機器、サーバ、PC 等の脆弱性管理を行う。脆弱性管理には、ベンダから提供される修正プログラムの適用も含まれる。

必要に応じて、脆弱性診断を実施する。

ビルシステム・ネットワークの規模が大きく、管理対象のネットワーク機器、サーバ、PC 等の数が多い場合には、脆弱性管理を自動化するツールを利用することも選択肢となる。

脆弱性管理ツールには、修正プログラム適用対象の機器に対して適用を促すメッセージを表示したり、修正プログラムを適用していない機器のインターネット接続を抑止する機能を有するものがある。

また、ビルシステム･ネットワークを構成する機器の中には、タイムリーに修正プログラムを適用することが困難であったり、修正プログラムを適用すること自体が困難なものがあるので、そのような場合には、修正プログラムの適用ができないことにより脆弱性が残存していることを許容し、当該機器の不要な(使用しない機能)の抑止、インターネット接続ポイントの集約・制限、ネットワークのセグメント化、ネットワーク監視の強化等の補完的なセキュリティ対策を実施する。

2. リスク分析の実施

システム構成図・ネットワーク構成図に基づいてリスク分析を実施する。リスク分析の詳細については、他の資料やリポジトリの他の項目(セキュリティアセスメントを起点とした多段防御による総合対策等)を参照。

レポジトリ：ビルシステム・ネットワークの構成管理とセキュリティ対策

3. セキュリティ対策の実施

リスク分析の結果に基づいてセキュリティ対策を実施する。セキュリティ対策の詳細については、他の資料やリポジトリの他の項目(セキュリティアセスメントを起点とした多段防御による総合対策等)を参照。

ビルシステム・ネットワークの資産管理・構成管理に関連して利用可能なセキュリティ対策製品・サービスとして、以下のようなものがある。

- サイバー攻撃の検知・遮断を行うハードウェア

システム内でやりとりされる通信パケットの送信元IPや宛先IP、送信されたパケットの数、タイムスタンプなどの情報をリアルタイムに分析することにより、通常とは異なる通信を遮断する機能を有するハードウェア

- セキュリティ対策の立案・提供、サイバー攻撃の予兆検知・遮断サービス

リスク分析に基づいてセキュリティ対策の立案・提供を行うコンサルティングサービスおよび、ネットワークの常時監視によるサイバー攻撃の予兆検知、分析、即時遮断を行うサービスをワンストップで提供する事業者もあるので、そのようなサービスを利用することも選択肢となる。

- 不正接続機器の検知ツールの導入

ビルシステム・ネットワークへの不正侵入防止策として、ビルシステム・ネットワークに不正に接続された機器を自動的に検知し、アラートを発行する仕組みを導入する。

ガイドラインへの追加情報の充実化

レポジトリ：ビルシステム・ネットワークの構成管理とセキュリティ対策

【調達時の仕様書の記載例】

- 設計事務所、個別システム事業者(ビル管理システム、ビルネットワーク)は、ビルの新築時や改築時に、ビルシステム・ネットワークを構成する機器の設置場所、各機器に割り当てられた IP アドレスや MAC アドレス、OS・ファームウェアのバージョン、製造元のベンダ名、使用している通信プロトコル・ポート番号等の詳細な資産情報を記録した情報資産台帳を作成し、納入すること。

- 個別システム事業者(ビル管理システム、ビルネットワーク)は、ビルシステム・ネットワークの構築時に、システムの相互接続状況、機器にインストールされているソフトウェア、使用している通信プロトコル、接続している外部システム、インターネット接続ポイント等が記載された、ビルシステム・ネットワーク構成図を作成し、納入すること。

- 個別システム事業者(ビル管理システム、ビルネットワーク)は、ビルシステム・ネットワークに変更があった場合に、ビルシステム・ネットワークの変更管理を適切に実施すること。また、最新のビルシステム・ネットワークの構成図を作成し、納入すること。

- ビルオーナー、設計事務所、個別システム事業者(ビル管理システム、ビルネットワーク)は、ビルシステム・ネットワークの設計・構築・運用において、ビルシステム・ネットワークの資産管理・構成管理・変更管理を適切に実施すること。

- 個別システム事業者(ビル管理システム、ビルネットワーク)は、脆弱性を管理するための仕組み・ツールを導入すること。

個別システム事業者(ビル管理システム、ビルネットワーク)は、ビルシステム・ネットワークを構成する機器に対して適切なサイバーセキュリティ対策を実施すること。

1．ビルガイドラインの高度化のための調査
①空調等のビルの個別設備システムの対応策に関する調査
②スマートビルのサイバーセキュリティ対策を意識したユースケース調査
③その他関連する調査
③－１　インシデントレスポンスに対する要求の整理
③－２　ガイドラインへの追加情報の充実化
③－３　ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討

2．ビルシステムのサイバーセキュリティ推進体制の調査
①推進体制の情報提供・共有・相談等の機能の実践的評価
②推進体制のあり方の調査

3．検討会の運営
①ビルSWGの運営
②作業グループの運営
③その他の運営

１．ビルガイドラインの高度化のための調査
③その他関連する調査
③－３　ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討

- ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討では、昨年度に引き続きIEC62443の調査を実施した。
- 今年度調査では、IEC62443の全体構成や更新情報を確認した後、実際にIEC62443-3-1、IEC62443-3-2、IEC62443-3-3、IEC62443-4-1、IEC62443-4-2を購入し、それぞれの対象範囲、分析や対策等の粒度、記載内容等の調査を実施した。
- そのうえで、現状版のビルガイドラインとIEC62443の対応関係を確認するための考え方を２通り検討し、それぞれの考え方に沿って、IEC62443とビルガイドラインの記載内容の比較を行った。
- そのうえで明らかになった比較内容を元に、現状版のガイドラインに取入れ可能な情報の整理を行った。

IEC62443シリーズの構成

③１．ビルガイドラインの高度化のための調査
③その他関連する調査
③－３　ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討　IEC62443シリーズの構成

：　開発中であり未発行

IEC 62443

シリーズ内共通事項 62443-1-X

- 62443-1-1：用語、シリーズ全体で参照されるコンセプト・モデルの説明
- 62443-1-2：シリーズ全体で参照されるマスター用語、略語集
- 62443-1-3：システムセキュリティ対策の定量的な指標
- 62443-1-4：制御システムのライフサイクル全体モデル、セキュリティの取組方法、ユースケース、ステークホルダーの役割

システムの開発・運用組織のセキュリティの運用ポリシー・手順 62443-2-X

- 62443-2-1：制御システムのアセットオーナー向けのセキュリティ対策の管理・運用の枠組みの要件
- 62443-2-2：セキュリティ対策における技術対策と運用対策による、セキュリティ対策レベルの評価方法
- 62443-2-3：制御システム環境におけるパッチ管理の要求事項
- 62443-2-4：システムベンダーなどが制御システムのオーナーに対してサービスを提供する上でのセキュリティプログラムの要件
- 62443-2-5：制御システムのアセットオーナー向けセキュリティプログラムの実装ガイダンス

システムのセキュリティ要件 62443-3-X

- 62443-3-1：制御システム環境に利用可能なセキュリティ技術の報告書
- 62443-3-2：制御システムのセキュリティ設計手順書
- 62443-3-3：セキュリティレベルの基準とシステムのセキュリティ機能要件

コンポーネントのセキュリティ要件 62443-4-X

- 62443-4-1：制御システムのコンポーネントベンダー向けセキュリティ開発プロセスの要件
- 62443-4-2：制御システムを構成するSW/HW/NW装置等のコンポーネントのセキュリティ機能要件

IEC62443シリーズとビルセキュリティガイドラインの対応関係

③１．ビルガイドラインの高度化のための調査
③その他関連する調査
③－３　ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討
対応関係の整理にあたっての基本的考え方

ビルセキュリティガイドラインの特徴

ビルセキュリティガイドラインは、4.1. 全体管理と4.2. 機器ごとの管理に大別され、後者は場所ごと、機器ごとにセキュリティポリシーが記載されており、それゆえネットワーク機器やサーバなど同じ種類の機器の場合、概ね同じ内容のセキュリティポリシーが繰り返し記載されている。

整理にあたっての基本的考え方①

機器の種類の観点(62443-4-2)や、セキュリティ対策の運用・管理(62443-2-1)、パッチ管理(62443-2-3)、事前検疫(62443-2-4)、リスクアセスメント・リスク評価(62443-3-2)のような特定の個別対策分野の観点からみて、ビルセキュリティガイドラインとの対応関係の整理が可能

整理にあたっての基本的考え方②

62443-3-3と62443-4-2は、制御システムのセキュリティの各基本要件(７つの基本要件)ごとにシステム要件とコンポーネント要件に分け、求められる技術面の対策の要件が記載されている。また、62443-4-1は、各システム開発プロセスごとに、セキュリティ確保のために求められる運用面の対策の要件が記載されている。以上より、技術面の対策の観点や運用面の対策の観点からみて、ビルセキュリティガイドラインとの対応関係の整理が可能

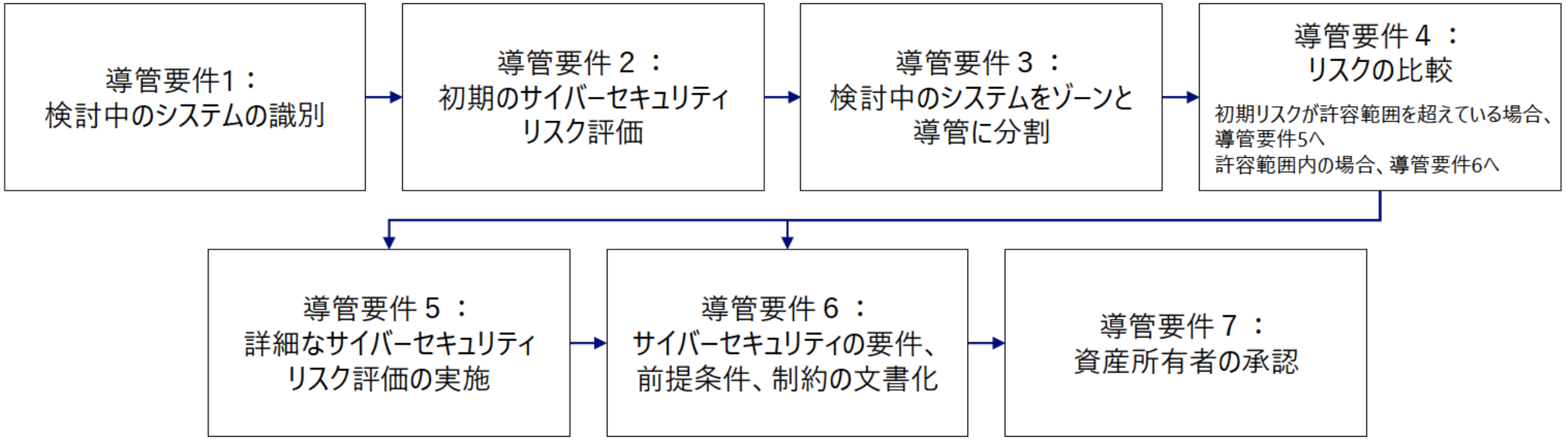
③１．ビルガイドラインの高度化のための調査
③その他関連する調査
③－３　ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討
対応関係の整理にあたっての基本的考え方

基本的な考え方／対応関係①

対応関係の整理にあたっての基本的考え方①

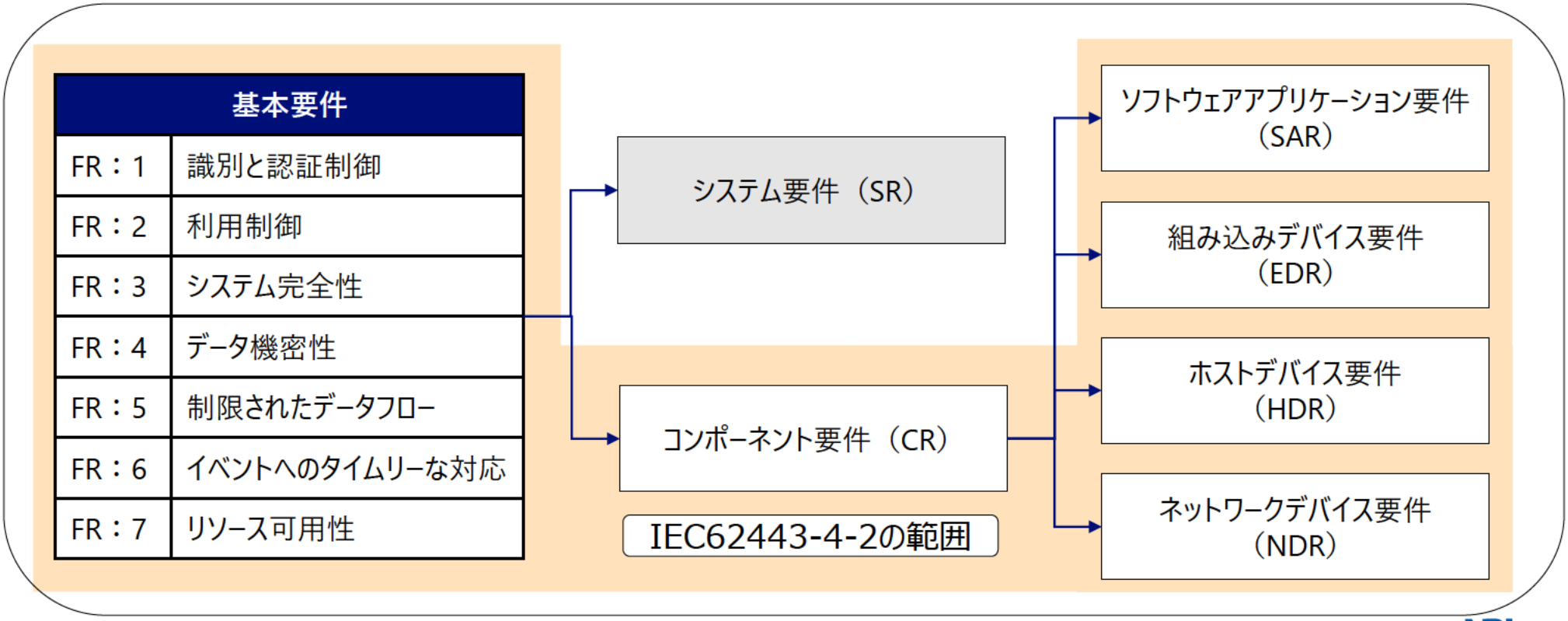
IEC 62443-3-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design

- ゾーン（システム内領域）やそれらを連結するコンジットに関するセキュリティについて規定した国際標準。
- システムのセキュリティ設計手順、ゾーン（システム内領域）及びコンジットやセキュリティ要求事項の定義などが規定されている規格。

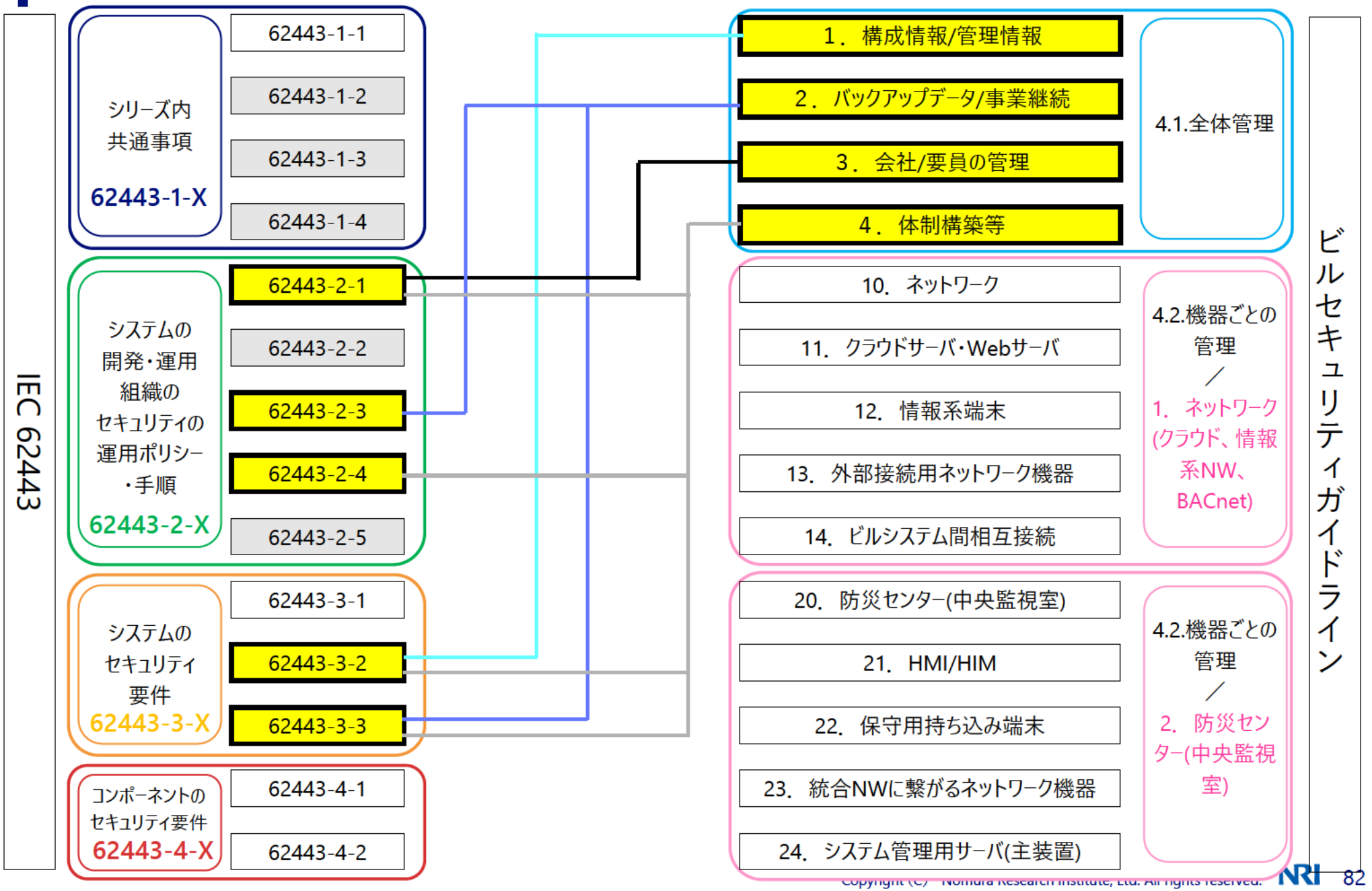


IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

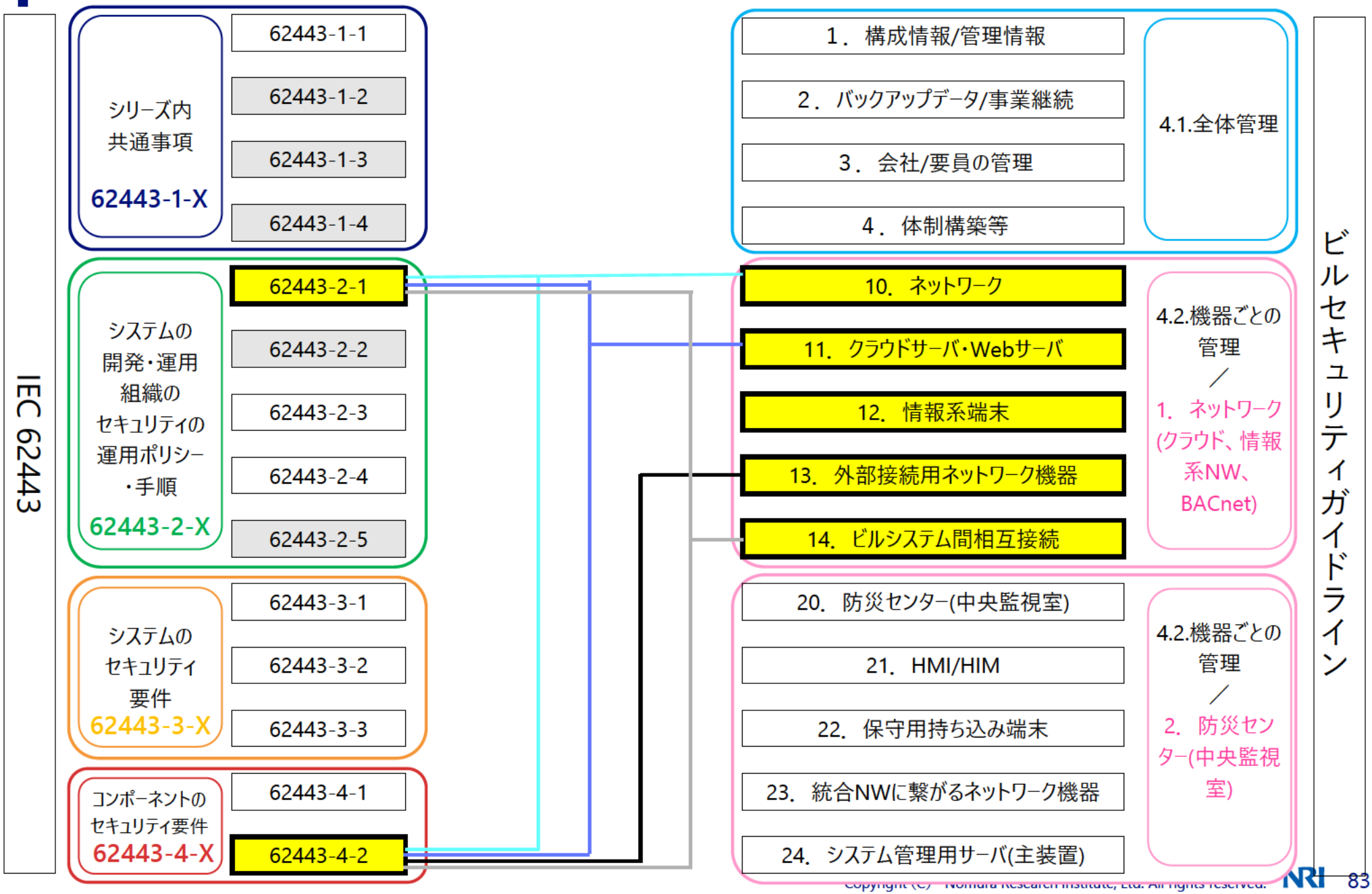
- コンポーネントのセキュリティ要件を規定した国際標準。
- デバイスに搭載されるセキュリティ機能を規定。ISA Secure のEDSA（FSA）をベースにしており、セキュリティ機能の実装評価に関する要求事項を記載。
- IEC62443-3-3の要件をベースに、各種コンポーネントに合わせて最適化を目指す。



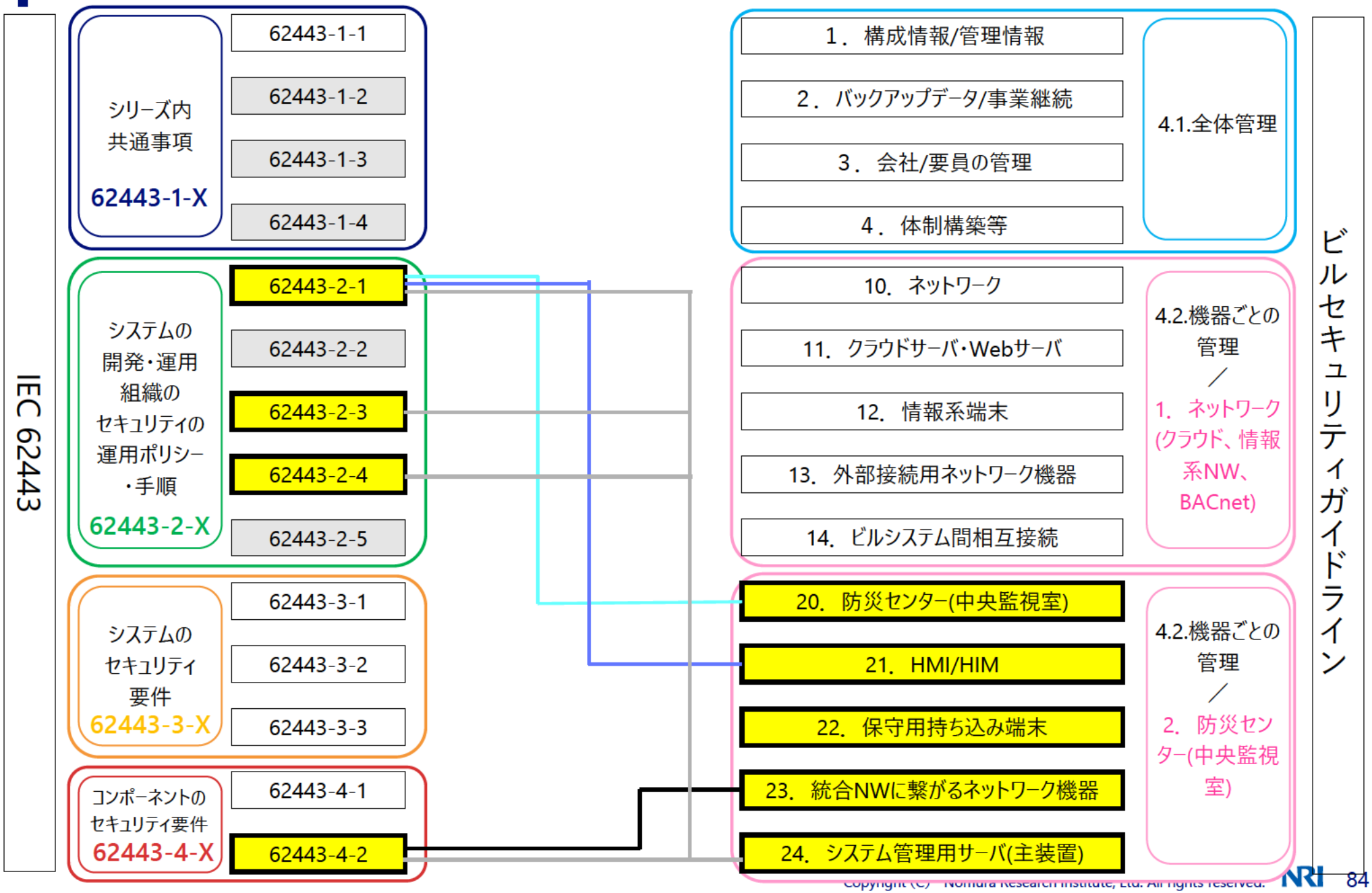
IEC62443シリーズとビルセキュリティガイドラインの対応関係



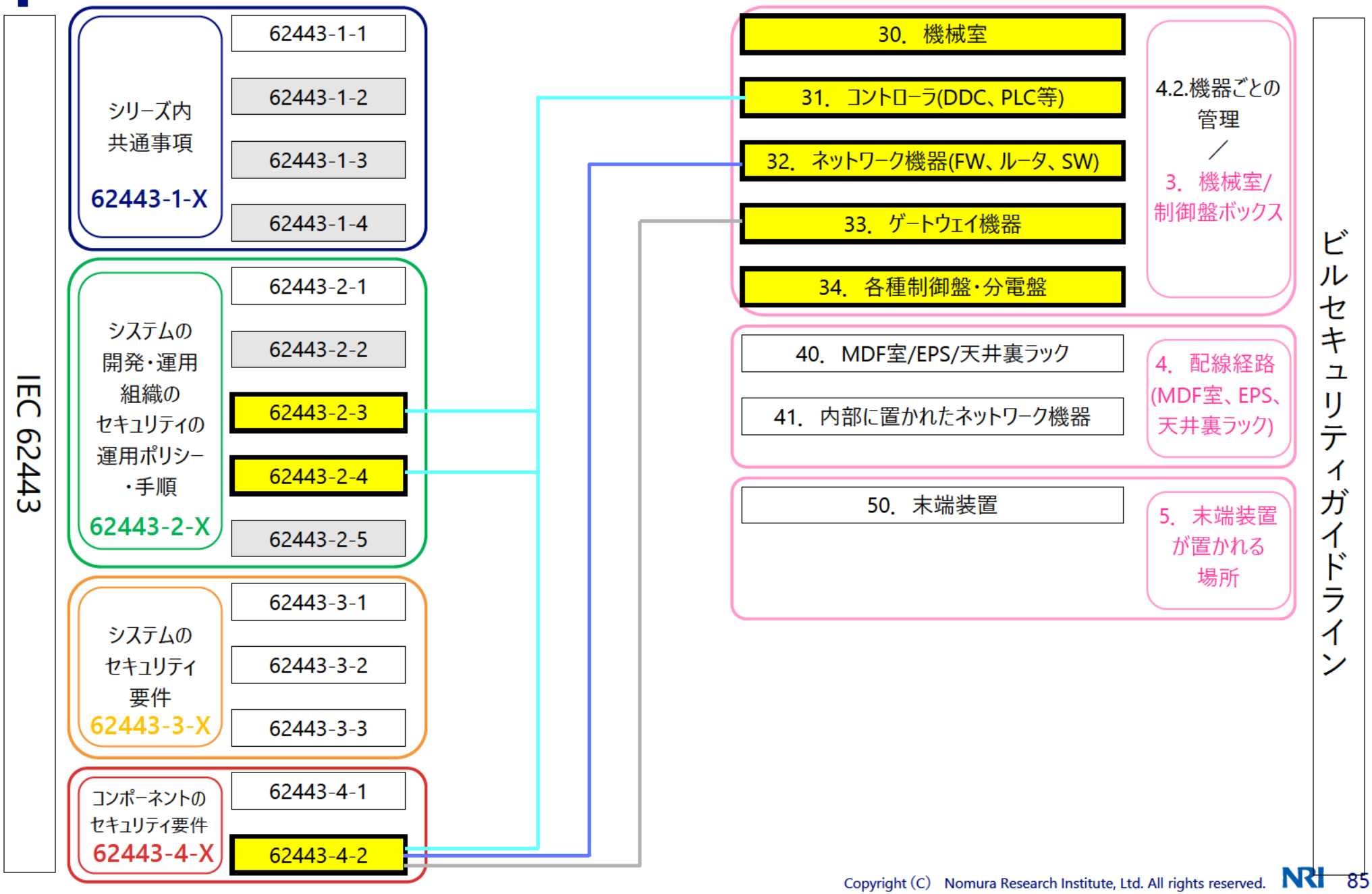
IEC62443シリーズとビルセキュリティガイドラインの対応関係



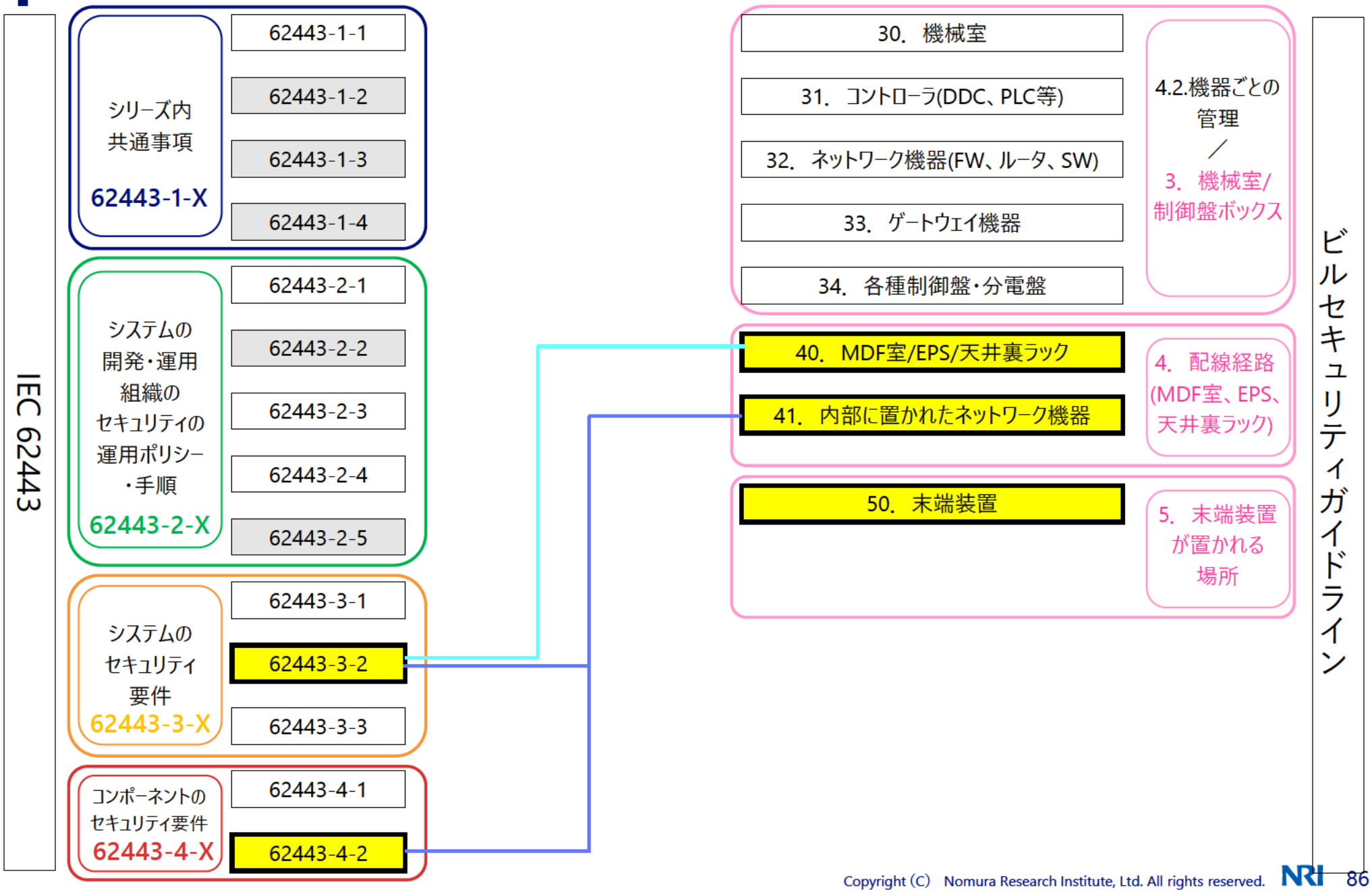
IEC62443シリーズとビルセキュリティガイドラインの対応関係



IEC62443シリーズとビルセキュリティガイドラインの対応関係



IEC62443シリーズとビルセキュリティガイドラインの対応関係



基本的な考え方／対応関係①の例　（1）

62443-4-2
ネットワークデバイス要件（NDR）

NDR 1.6：無線アクセス管理
要件：無線アクセス管理をサポートするネットワーク機器は、無線通信に従事するすべてのユーザー（人間、ソフトウェアプロセスまたはデバイス）を識別し、認証する機能を提供すること。
補足：いかなる無線技術も、ほとんどの場合、単なる通信プロトコルの選択肢の一つと考えることができ、またそうすべきです。そのため、IACS が利用する他の通信タイプと同様に、IACS のセキュリティ要件に従うべきです。しかし、セキュリティの観点から見ると、有線通信と無線通信には少なくとも1つの大きな違いがあります。物理的なセキュリティ対策は、一般的に無線を使用する際には効果的ではありません。

NDR1.6(1)：（拡張要件）固有の識別と認証
要件：ネットワーク機器は、無線通信に従事するすべてのユーザー（人間、ソフトウェアプロセスまたはデバイス）を一意に識別し、認証する機能を提供すること。

NDR 1.13：信頼されていないネットワーク経由でのアクセス
要件：ネットワークへアクセスする端末は、信頼されていないネットワークを介した端末への全てのアクセス方法を監視および制御する機能を提供すること。
補足：信頼されていないネットワークを経由して端末にアクセスする例としては、一般的にリモートアクセス方法（ダイアルアップ、ロードバンド、無線等）や、会社のオフィス（非制御システム）ネットワークからの接続が挙げられます。端末は、アクセスコントロールリスト機能を提供することで、以下の方法でアクセスを制限することができます。
・イーサネットスイッチなどの 2 層レイヤー：①MACアドレス、②VLAN
・ルーター、ゲートウェイ、ファイアウォールなどのレイヤー3転送装置：①IPアドレス、②ポートおよびプロトコル、③仮想プライベートネットワーク

NDR1.13(1)：（拡張要件）明示的なアクセス要求の承認
要件：ネットワーク機器は、割り当てられた役割によって明示的に承認されない限り、信頼できないネットワーク経由のアクセス要求を拒否する機能を提供すること。

ビルセキュリティガイドライン別紙
13.外部接続用ネットワーク機器（ファイアウォール、ルータ）

インシデント：外部ネットワーク接続経由で攻撃を受ける。

リスク源：外部接続用ネットワーク機器のセキュリティ対策が十分ではない。

外部との境界にはDMZを置き内部と外部で直接アクセスはせず、データの交換を行う。	設計・仕様
境界にファイアウォールを立て、かつプロキシサーバを立てて外部とのアクセスは間接アクセスとする。	設計・仕様
境界にファイアウォールを設ける。	設計・仕様
－	建設
外部アクセスが制限されていることを確認する。	施工検査
許可されたアクセスのみ実施されていることを定期的に確認する。	運用
廃棄時にはネットワーク機器の設定データ（管理者パスワードを含んで）を消去するか物理的に破壊しアクセスできないようにする。	改修・廃棄

基本的な考え方／対応関係①の例　（２）

62443-4-2
ネットワークデバイス要件（NDR）

NDR 2.4：モバイルコード
要件：ネットワーク機器がモバイルコード技術を利用する場合、ネットワーク機器は、モバイルコード技術の利用に関するセキュリティポリシーを実施する機能を提供すること。セキュリティポリシーでは、ネットワーク機器で使用されている各モバイルコード技術に対して、少なくとも以下のアクションを許可すること。
a) モバイルコードの実行を制御する。
b) どのユーザ（人間、ソフトウェアプロセス、またはデバイス）がネットワークデバイスとの間でモバイルコードの転送を許可されるかを制御する。
c) モバイルコードの整合性チェックに基づいて、コードが実行される前にコードの実行を制御する。
補足：モバイルコードの技術には、Java、JavaScript、ActiveX、PDF、Postscript、Shockwaveムービー、Flashアニメーション、VBScriptなどが含まれますが、これらに限定されるものではありません。使用制限は、サーバーにインストールされたモバイルコードの選択と使用、および個々のワークステーションでダウンロードして実行するモバイルコードの選択と使用の両方に適用されます。制御手順は、コンポーネントが存在する制御システム内で、容認できないモバイルコードの開発、取得、または導入を防止する必要があります。例えば、モバイルコードの交換は、制御システム内で直接行うことはできないが、 IACS の要員が管理する制御された隣接環境では許可されるかもしれません。モバイルコードは、コード自体（アプリケーション層）に整合性、真正性、認証のチェックを加えることで安全性を確保したり、これらの属性を提供する安全な通信トンネルを介してモバイルコードを送信することで「ジャストインタイム」にコードを実行したり、あるいはこれらのオプションと同等のメカニズムを使用することができます。

NDR2.4(1)：（拡張要件）モバイルコードの認証チェック
要件：ネットワーク機器は、コードが実行される前の真正性チェックの結果に基づいて、モバイルコードの実行を制御することができるセキュリティポリシーを実施する機能を提供すること。

NDR 2.13：物理的な診断およびテストインターフェースの使用
要件：ネットワーク機器は、工場出荷時の物理的な診断・テスト用インターフェース（JTAGデバッグなど）が不正に使用されないように保護されていること。
補足：工場診断・試験用インターフェースは、コンポーネント内の様々な場所に作成され、コンポーネントの開発者や工場関係者が機能的な実装を試験する際に役立ち、またエラーが発見された場合には、その後コンポーネントから取り除くことができます。しかし、これらのインターフェースは、IACS に提供される本質的な機能を保護するために、権限のない者からのアクセスから注意深く保護されなければなりません。工場出荷時の診断・試験用インタフェースは、機器とのネットワーク通信を使用する場合があります。このような場合、これらのインターフェースは本文書の全ての要求事項に従わなければなりません。なお、診断・テスト用インターフェースが、製品の制御や非公開情報へのアクセス機能を提供しない場合には、認証機構は必要ありません。これは、脅威評価によって決定されるべきです。例えば、JTAGデバッグのように、JTAGを使ってプロセッサを制御し、任意のコマンドを実行する場合と、JTAGバウンダリスキャンのように、JTAGを使って単に情報（公開されている情報かもしれない）を読み取る場合があります。

62443-4-2との対応関係なし

ビルセキュリティガイドライン別紙
13.外部接続用ネットワーク機器（ファイアウォール、ルータ）

インシデント：外部ネットワーク接続経由で攻撃を受ける。	
リスク源：外部接続用ネットワーク機器のセキュリティ対策が十分ではない。	
外部との境界にはDMZを置き内部と外部で直接アクセスはせず、データの交換を行う。	設計・仕様
境界にファイアウォールを立て、かつプロキシサーバを立てて外部とのアクセスは間接アクセスとする。	設計・仕様
境界にファイアウォールを設ける。	設計・仕様
－	建設
外部アクセスが制限されていることを確認する。	施工検査
許可されたアクセスのみ実施されていることを定期的に確認する。	運用
廃棄時にはネットワーク機器の設定データ（管理者パスワードを含んで）を消去するか物理的に破壊しアクセスできないようにする。	改修・廃棄

基本的な考え方／対応関係①の例　（３）

62443-4-2
ネットワークデバイス要件（NDR）

NDR2.13(1)：（拡張要件）アクティブなモニタリング
要件：ネットワーク機器は、機器の診断およびテストインターフェースを積極的に監視し、これらのインターフェースへのアクセスの試みが検出された場合には、監査ログエントリを生成すること。

NDR 3.2：悪意のあるコードからの保護
要件：ネットワーク機器は、悪意のあるコードからの保護を提供すること。
補足：ネットワーク機器が補償制御を利用できる場合、悪意のあるコードからの保護を直接サポートする必要はありません。例えば、ネットワークのパケットフィルタリング装置を使用して、転送中の悪意のあるコードを識別して除去することができます。IACS は、必要な保護機能を提供する責任があると想定されています。しかし、ローカルのUSBホストにアクセスするようなシナリオでは、悪意のあるコードからの保護の必要性を評価する必要があります。

NDR 3.10：更新のサポート
要件：ネットワーク機器は、アップデートやアップグレードの機能をサポートすること。
補足：ネットワーク機器は、インストールされた期間中、アップデートやアップグレードのインストールが必要になる場合があります。また、ネットワーク・デバイスが本質的な機能をサポートまたは実行している場合もあります。このような場合、ネットワーク・デバイスは、高可用性システムの本質的な機能に影響を与えることなく、パッチやアップデートをサポートするメカニズムを備えている必要があります。この機能を提供する例として、ネットワーク・デバイス内の冗長性をサポートすることが挙げられます。

NDR3.10(1)：（拡張要件）信頼性と完全性の更新
要件：ネットワーク機器は、ソフトウェアのアップデートやアップグレードをインストールする前に、その真正性と完全性を検証すること。

NDR 3.11：物理的な改ざんの検出
要件：ネットワークデバイスは、デバイスへの不正な物理的アクセスから保護するために、耐タンパー性と検出メカニズムを提供すること。
補足：改ざん防止機構の目的は、攻撃者が IACS 機器に対して不正な物理的行為を行おうとするこ とを防止することです。防止に加えて、不正操作が行われた場合の検知と対応が重要です。いたずら防止機構は、重要な部品へのアクセスを防止するために組み合わせて使用するのが効果的です。耐タンパー性とは、特殊な材料を用いてデバイスやモジュールの改ざんを困難にすることです。これには、強化された筐体、ロック、カプセル化、セキュリティスクリューなどの機能が含まれます。また、空気の通り道を確保することで、製品内部を探ることが難しくなります。タンパーエビデンスの目的は、改ざんが発生したときに、目に見える証拠や電子的な証拠が残るようにすることです。多くの単純な証拠技術は、シールやテープで構成されており、物理的な改ざんが行われたことを明らかにします。より高度な技術としては、スイッチが挙げられます。

NDR3.11(1)：（拡張要件）改ざんが試行されたことの通知
要件：ネットワーク機器は、不正な物理的アクセスの試みを発見した場合、設定可能な一連の受信者に自動的に通知を行うことができること。改ざんの通知はすべて、全体的な監査ログ機能の一部として記録されること。

62443-4-2との対応関係なし

ビルセキュリティガイドライン別紙
13.外部接続用ネットワーク機器（ファイアウォール、ルータ）

インシデント：外部ネットワーク接続経由で攻撃を受ける。	
リスク源：外部接続用ネットワーク機器のセキュリティ対策が十分ではない。	
外部との境界にはDMZを置き内部と外部で直接アクセスはせず、データの交換を行う。	設計・仕様
境界にファイアウォールを立て、かつプロキシサーバを立てて外部とのアクセスは間接アクセスとする。	設計・仕様
境界にファイアウォールを設ける。	設計・仕様
－	建設
外部アクセスが制限されていることを確認する。	施工検査
許可されたアクセスのみ実施されていることを定期的に確認する。	運用
廃棄時にはネットワーク機器の設定データ（管理者パスワードを含んで）を消去するか物理的に破壊しアクセスできないようにする。	改修・廃棄

基本的な考え方／対応関係①の例　（4）

62443-4-2
ネットワークデバイス要件（NDR）

NDR 3.12：信頼のため製品サプライヤーの情報等を提供
要件：ネットワーク機器は、機器の製造時に、1つまたは複数の「ルートオブトラスト」として使用される製品供給者の鍵およびデータの機密性、完全性、および真正性を提供し、保護する機能を提供すること。
補足：コンポーネントが、製品供給者から提供されたハードウェア、ソフトウェア、およびデータの真正性と完全性を検証できるようにするためには、検証プロセスを実行するための信頼できるデータソースを所有している必要があります。この信頼できるデータ源は、システムの「ルートオブトラスト」と呼ばれる。この信頼できるデータ源は、既知の優良なソフトウェアの暗号ハッシュのセットであったり、暗号署名の検証に使用される非対称暗号鍵ペアの公開部分であったりします。この信頼データは、コンポーネントのファームウェアやオペレーティング・システムを起動する前に、重要なソフトウェア、ファームウェア、データを検証するために使用されることが多く、これにより、コンポーネントが、すべてのセキュリティ・メカニズムが動作可能であり、かつ侵害されていない既知の優良な状態で起動することを検証します。ルートオブトラストとなるデータは、多くの場合、ソフトウェアまたはハードウェアに実装されたメカニズムによって保護されており、コンポーネントの通常動作中にデータが変更されることはありません。製品供給者のルートオブトラストデータの修正は、通常、製品供給者のプロビジョニングプロセスに限定されます。代わりに、信頼の根源に対して検証されるべき情報は、保護されたデータを公開することなく検証を実行して結果を返すハードウェアまたはソフトウェアの API を通じて検証プロセスに提出されます。

62443-4-2との対応関係なし

ビルセキュリティガイドライン別紙
13.外部接続用ネットワーク機器（ファイアウォール、ルータ）

インシデント：外部ネットワーク接続経由で攻撃を受ける。	
リスク源：外部接続用ネットワーク機器のセキュリティ対策が十分ではない。	
外部との境界にはDMZを置き内部と外部で直接アクセスはせず、データの交換を行う。	設計・仕様
境界にファイアウォールを立て、かつプロキシサーバを立てて外部とのアクセスは間接アクセスとする。	設計・仕様
境界にファイアウォールを設ける。	設計・仕様
–	建設
外部アクセスが制限されていることを確認する。	施工検査
許可されたアクセスのみ実施されていることを定期的に確認する。	運用
廃棄時にはネットワーク機器の設定データ（管理者パスワードを含んで）を消去するか物理的に破壊しアクセスできないようにする。	改修・廃棄

基本的な考え方／対応関係①の例　（５）

62443-4-2
ネットワークデバイス要件（NDR）

NDR 3.13：資産保有者の情報等を提供
要件：ネットワーク機器は以下の通りとする。
a)「信頼の根源」として使用される資産所有者の鍵およびデータの機密性、完全性、および真正性をプロビジョニングし保護する機能を提供すること。
b) デバイスのセキュリティゾーン外にある可能性のあるコンポーネントに依存せずにプロビジョニングする能力をサポートすること。
補足：製品のサプライヤーは、そのコンポーネントに搭載されているソフトウェアやファームウェアが本物であること、そして、そのソフトウェアやファームウェアの完全性が損なわれていないことを保証する仕組みを確立しています。これにより、製品サプライヤーは、資産家が操作できる既知の良好な状態を提供することができます。しかし、多くの製品供給者は、モバイルコードやユーザープログラムなどを用いて、資産家が機器の機能を拡張するための仕組みも提供しています。コンポーネントのセキュリティを保護するためには、コンポーネントの機能を拡張する際に、その拡張機能が許可されているかどうか、また、資産所有者がその拡張機能の起源を承認しているかどうかを検証することが重要です。このような検証を行うために、コンポーネントには、有効な起源と無効な起源を区別するためのデータが含まれていなければなりません。有効な起源と無効な起源のリストは、資産所有者によって異なり、製品供給者が製造時にすべての有効な起源の可能性の完全なリストを持っていることはあり得ません。したがって、製品の供給者は、資産所有者が自らの「ルートオブトラスト」を安全に提供する方法を提供することが重要です。この「ルートオブトラスト」は、資産所有者のセキュリティ・ポリシーで許可されたオリジンとそうでないオリジンを区別する機能を提供します。これらの「ルートオブトラスト」の信頼性と完全性は、悪意のある行為者が信頼の根源を追加してコンポーネン トに対する操作能力を付与できないように保護されなければなりません。
NDR 2.4-モバイルコード（15.4）などの要件では、モバイルコードの実行前に、コンポーネントがモバイルコードの真正性チェックを完了することが求められている。この要件で提供される信頼の根源は、モバイルコードの起源と完全性を検証するために必要なデータを提供し、コードの実行が許可されているかどうかをコンポーネントが独自に判断できるようにする。信頼の根源は、CR 3.1「通信の完全性」（7.3）で要求される通信の完全性や、CR 4.1「情報の機密性」（8.3）で要求される通信の機密性など、通信のセキュリティを提供するために使用されます。

62443-4-2との対応関係なし

ビルセキュリティガイドライン別紙
13.外部接続用ネットワーク機器（ファイアウォール、ルータ）

インシデント：外部ネットワーク接続経由で攻撃を受ける。	
リスク源：外部接続用ネットワーク機器のセキュリティ対策が十分ではない。	
外部との境界にはDMZを置き内部と外部で直接アクセスはせず、データの交換を行う。	設計・仕様
境界にファイアウォールを立て、かつプロキシサーバを立てて外部とのアクセスは間接アクセスとする。	設計・仕様
境界にファイアウォールを設ける。	設計・仕様
－	建設
外部アクセスが制限されていることを確認する。	施工検査
許可されたアクセスのみ実施されていることを定期的に確認する。	運用
廃棄時にはネットワーク機器の設定データ（管理者パスワードを含んで）を消去するか物理的に破壊しアクセスできないようにする。	改修・廃棄

基本的な考え方／対応関係①の例　（6）

62443-4-2
ネットワークデバイス要件（NDR）

NDR 3.14：ブート処理の完全性
要件：ネットワーク機器は、コンポーネントのブートプロセスに必要なファームウェア、ソフトウェア、および設定データの整合性を、ブートプロセスで使用する前に確認すること。
補足：コンポーネントのセキュリティ機能が損なわれていないことを資産所有者に保証するためには、コンポー ネントのソフトウェアおよびファームウェアが改ざんされていないこと、およびソフトウェアおよび ファームウェアがコンポーネント上で実行可能な有効なものであることを確認する必要がある。したがって、コンポーネントは、ブート・プロセスの前に、コンポー ネントのファームウェアおよび/またはソフトウェアの整合性および真正性を検証するチェックを 実行し、コンポーネントが安全でない、または無効な動作状態でブートしないようにする必要がある。

NDR3.14(1)：（拡張要件）ブートプロセスの認証
要件：ネットワーク機器は、コンポーネントのブートプロセスに必要なファームウェア、ソフトウェア、設定データがブートプロセスで使用される前に、そのコンポーネントの製品供給者のルーツオブトラストを使用して、その真正性を検証すること。

NDR 5.2：ゾーン（システム内領域）境界の保護
要件：ゾーン境界にあるネットワーク機器は、リスクベースのゾーンおよびコンジットモデルで定義された 区分けを実施するために、ゾーン境界での通信を監視および制御する機能を提供すること。
補足：各セキュリティゾーンの外部への接続は、効果的なアーキテクチャで配置された適切な境界保護装置（例えば、プロキシ、ゲートウェイ、ルータ、ファイアウォール、一方向ゲートウェイ、ガード及び暗号化トンネル）で構成される管理されたインタフェースを介して行われるべきである（例えば、DMZに存在するアプリケーションゲートウェイを保護するファイアウォール）。指定された代替処理サイトにおける制御システムの境界保護は、プライマリサイトと同レベルの保護を提供する必要がある。

NDR5.2(1)：（拡張要件）すべてを拒否し、例外的に許可
要件：ネットワークコンポーネントは、デフォルトでネットワークトラフィックを拒否し、例外的にネットワークトラフィックを許可する機能を提供すること（すべてを拒否し、例外的に許可とも呼ばれる）。

NDR5.2(2)：（拡張要件）アイランド（孤立）モード
要件：ネットワークコンポーネントは、制御システム境界を介したいかなる通信からも保護する機能を提供しなければならない（アイランドモードとも呼ばれる）。
注：この機能を使用できる例としては、制御システム内でセキュリティ違反や侵害が検出された場合や、企業レベルで攻撃が発生している場合などがある。

NDR5.2(3)：（拡張要件）フェイルクローズ（故障の際は、完全に停止かつネットワーク遮断）
要件：ネットワークコンポーネントは、境界保護機構の運用障害（フェイルクローズとも呼ばれる）が発生した場合に、制御システムの境界を介したあらゆる通信から保護する機能を提供しなければならない。
注：この機能が使用できる例としては、ハードウェアの故障や停電により、境界保護装置が劣化したモードで機能したり、完全に故障したりする場合がある。

ビルセキュリティガイドライン別紙
13.外部接続用ネットワーク機器（ファイアウォール、ルータ）

インシデント：外部ネットワーク接続経由で攻撃を受ける。	
リスク源：外部接続用ネットワーク機器のセキュリティ対策が十分ではない。	
外部との境界にはDMZを置き内部と外部で直接アクセスはせず、データの交換を行う。	設計・仕様
境界にファイアウォールを立て、かつプロキシサーバを立てて外部とのアクセスは間接アクセスとする。	設計・仕様
境界にファイアウォールを設ける。	設計・仕様
－	建設
外部アクセスが制限されていることを確認する。	施工検査
許可されたアクセスのみ実施されていることを定期的に確認する。	運用
廃棄時にはネットワーク機器の設定データ（管理者パスワードを含んで）を消去するか物理的に破壊しアクセスできないようにする。	改修・廃棄

基本的な考え方／対応関係①の例　（７）

62443-4-2
ネットワークデバイス要件（NDR）

NDR 5.3：汎用的な個人間通信制限
要件：ゾーン境界にあるネットワーク装置は、制御システムの外部にいるユーザまたはシステムから、 汎用の個人間メッセージを受信しないように保護する機能を提供するものとする。
補足：汎用的な個人間通信システムには、電子メールシステム、ソーシャルメディア（Twitter、Facebook、フォトギャラリーなど）、あらゆるタイプの実行可能ファイルの送信を可能にするメッセージシステムなどが含まれますが、これらに限定されるものではありません。これらのシステムは、通常、制御システムの運用とは関係のない個人的な目的で利用されるため、これらのシステムがもたらすリスクは、通常、認識されている利益を上回ります。これらのタイプの汎用通信システムは、制御システムにマルウェアを導入したり、読み取り権限のある情報を制御システムの外部に渡したり、セキュリティ問題の発生や制御システムへの攻撃に使用できる過剰なネットワーク負荷を導入したりするための攻撃ベクターとして一般的に使用されます。ネットワーク機器は、ポート番号や送信元/送信先アドレスに基づいて特定の通信をブロックしたり、アプリケーション層のファイアウォールでより詳細なチェックを行うなどして、このような制限を実現することができる。

62443-4-2との対応関係なし

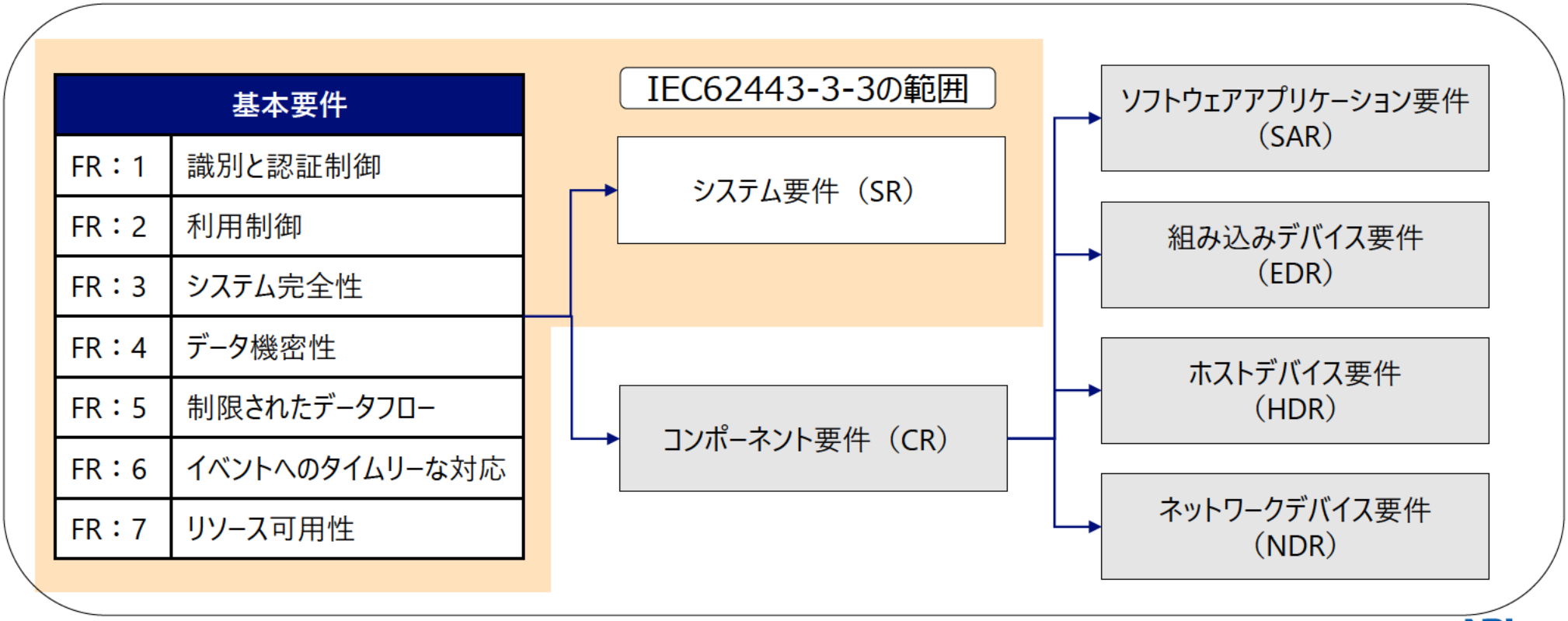
ビルセキュリティガイドライン別紙
13.外部接続用ネットワーク機器（ファイアウォール、ルータ）

インシデント：外部ネットワーク接続経由で攻撃を受ける。	
リスク源：外部接続用ネットワーク機器のセキュリティ対策が十分ではない。	
外部との境界にはDMZを置き内部と外部で直接アクセスはせず、データの交換を行う。	設計・仕様
境界にファイアウォールを立て、かつプロキシサーバを立てて外部とのアクセスは間接アクセスとする。	設計・仕様
境界にファイアウォールを設ける。	設計・仕様
－	建設
外部アクセスが制限されていることを確認する。	施工検査
許可されたアクセスのみ実施されていることを定期的に確認する。	運用
廃棄時にはネットワーク機器の設定データ（管理者パスワードを含んで）を消去するか物理的に破壊しアクセスできないようにする。	改修・廃棄

対応関係の整理にあたっての基本的考え方②

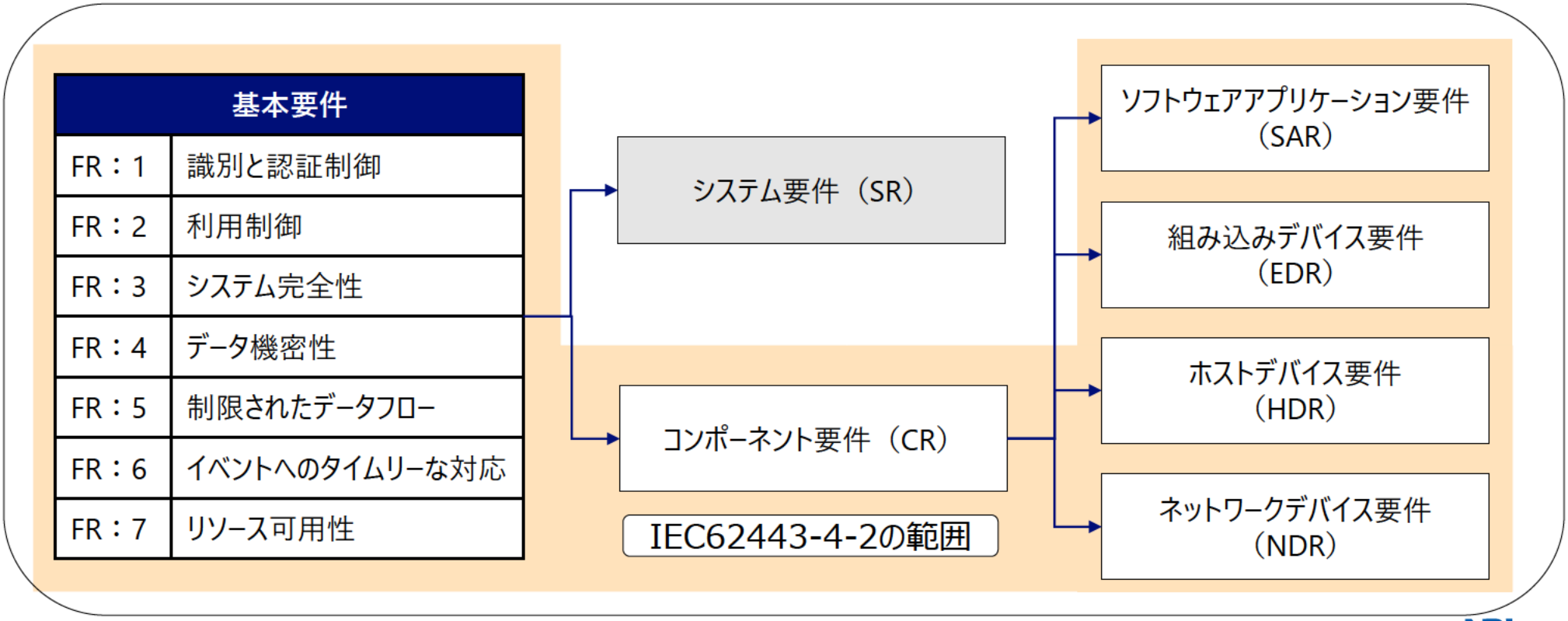
IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

- システムのセキュリティ要件を規定した国際標準。
- 基本要件（FR）とシステム要件（SR）をベースに、各種システムに合わせて最適化を目指す。



IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

- コンポーネントのセキュリティ要件を規定した国際標準。
- デバイスに搭載されるセキュリティ機能を規定。ISA Secure のEDSA（FSA）をベースにしており、セキュリティ機能の実装評価に関する要求事項を記載。
- IEC62443-3-3の要件をベースに、各種コンポーネントに合わせて最適化を目指す。



IEC 62443-4-1：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

- コンポーネントの開発要件を規定した国際標準。
- セキュアなコンポーネントを開発するための要件を規定しており、IACSコンポーネントベンダのセキュリティ開発プロセスをベースにしている。
- ソフトウェア開発プロセスを８つの実践分野に分けて、それぞれのセキュリティに関する要求事項を記載。

Practice 1	セキュリティマネジメント（SM）
Practice 2	セキュリティ要求仕様（SR）
Practice 3	セキュリティ設計（SD）
Practice 4	セキュリティ実装（SI）
Practice 5	セキュリティ検証・妥当性評価（SVV）
Practice 6	セキュリティ課題管理（DM）
Practice 7	セキュリティアップデート管理（SUM）
Practice 8	セキュリティガイドライン（SG）

基本的な考え方／対応関係②の例　（1）

62443-4-1
セキュリティ検証・妥当性評価（SVV）

SVV-1：セキュリティ要件テスト
要件：製品のセキュリティ機能がセキュリティ要件を満たしていること、および製品がエラーシナリオや無効な入力を正しく処理していることを検証するためのプロセスを採用すること。テストの種類には以下が含まれるものとする。
a) セキュリティ要求事項の機能テスト。
b) 性能と拡張性のテスト。
c) セキュリティに特化していない境界/エッジ条件、ストレス、不正な入力や予期せぬ入力のテスト。
補足：このプロセスは、製品がその製品に対して定義されたセキュリティ要求事項（セキュリティ課題管理（DM））を満たしていることを保証するために必要です。このプロセスがあるということは、製品が文書化されたセキュリティ要求事項を満たしていることを、製品の供給者がテストによって検証することを意味します。
セキュリティ要求事項の対象となる機能の種類の例としては、次のようなものがあります。
a) 一般的なセキュリティ機能（特徴）。
b) API（アプリケーション・プログラミング・インターフェース）。
c) 権限の委譲。
d) アンチタンパリングおよびインテグリティ機能。
e) 署名入り画像の検証、および
f) 秘密の安全な保存

SVV-2：脅威の軽減テスト
要件：脅威モデルで特定・検証された脅威に対する緩和策の有効性をテストするためのプロセスを採用すること。活動には以下が含まれるものとする。
a) 特定の脅威に対処するために実装された各ミティゲーションが、設計どおりに機能することを確認するための十分なテストを行うための計画を作成し、実行すること。
b) 各ミティゲーションを阻止するための計画を作成し、実行すること。
補足：脅威モデルで特定された脅威に対するミティゲーションの有効性は、この実践の一環としてテストされます。脅威の緩和策のテストの例としては、なりすまし、改ざん、否認、情報開示、サービス拒否、特権の昇格（STRIDE）を用いて特定された緩和策を阻止しようとする試みがあります。例えば、STRIDEでスプーフィングの緩和策として認証が特定された場合、脅威の緩和策のテストでは、認証のバイパスに焦点が当てられます。緩和策として層状の防御戦略を採用した場合、各層の有効性をテストします。例えば、製品が改ざんを阻止するために、認証、承認、監査ログの組み合わせを層状防御戦略として採用している場合、各層はこの緩和戦略への貢献度をテストします。このプロセスは、製品の深層防御および脅威緩和の戦略と能力が効果的であることを確認するために必要です。

ビルセキュリティガイドライン別紙
31.コントローラ（DDC、PLC等）の施工検査

- 共通：設計通りの機能が入っているか検査する。
- 設置端末全てに対してマルウエア対策を施す。
  ログ取得、解析のシステムが動作していることを確認する。
- ネットワーク監視の仕組みが導入され正しく動作していることを確認する。
- 竣工検査時にホワイトリスト機能が正常に動作するか確認する。
- システム全体がマルウエア感染がないことを確認する。
- 竣工時にID・パスワードのリストを納入する。
- 工場出荷前及び引渡し前に、その時点で脆弱性情報に対して、適切に対応できているか確認する。
- 利用しない空USBポートは治具でふさぐ。
  現場搬入後、引渡しまで施錠管理を実施する。
  USBを接続する場合は、ウィルス検疫等確認したものに限る。
- USBを接続する場合は、ウィルス検疫等確認したものに限る
  外部媒体も使用する場合も同じ。
- 外部持込端末を接続する場合は、ウィルス検疫等確認したものに限る。

基本的な考え方／対応関係②の例　（２）

62443-4-1
セキュリティ検証・妥当性評価（SVV）

SVV-3：脆弱性テスト
要件：製品に潜在するセキュリティ上の脆弱性を特定し、その特徴を明らかにすることに重点を置いたテストを実施するプロセスを採用すること。既知の脆弱性のテストは、少なくとも、確立された、業界で認められた、既知の脆弱性に関する公的な情報源の最近の内容に基づいていること。テストには以下が含まれるものとする。
a) セキュリティ上の問題を発見することを目的とした、不正使用のケースや、不正な入力や予期せぬ入力のテスト。これには、手動または自動の不正使用テスト、およびツールが存在するすべての外部インターフェースとプロトコルに関する特殊なタイプの不正使用テストが含まれる。例えば、ファズテストやネットワークトラフィックの負荷テスト、容量テストなどがある。
b) システムに出入りするすべての経路、脆弱なACL、公開されたポート、昇格した特権で実行されているサービスなどの一般的な脆弱性を判断するための攻撃表面分析。
c) ブラックボックスによる既知の脆弱性スキャンでは、製品のハードウェア、ホスト、ソフトウェアのコンポーネントに存在する既知の脆弱性を検出します。例えば、ネットワークベースの既知の脆弱性スキャンがこれにあたる。
d) コンパイルされたソフトウェアについて、製品にインストールするために供給者から提供された組み込みファームウェアを含むすべてのバイナリ実行ファイルのソフトウェア構成分析。この分析は、少なくとも以下の種類の問題を検出するものとする。
1) 製品ソフトウェアコンポーネントの既知の脆弱性。
2) 脆弱なライブラリへのリンク。
3) セキュリティルールの違反。
4) 脆弱性につながる可能性のあるコンパイラの設定。
e) 静的コード解析では見えない欠陥を検出する動的ランタイムリソース管理テスト。これには、ランタイムハンドルの解放失敗によるサービス拒否状態、メモリリーク、認証なしに行われる共有メモリへのアクセスなどが含まれ るが、これらに限定されない。このテストは、そのようなツールが利用可能な場合に適用するものとする。
補足：記載なし

ビルセキュリティガイドライン別紙
31.コントローラ（DDC、PLC等）の施工検査

共通：設計通りの機能が入っているか検査する。

設置端末全てに対してマルウエア対策を施す。
ログ取得、解析のシステムが動作していることを確認する。

ネットワーク監視の仕組みが導入され正しく動作していることを確認する。

竣工検査時にホワイトリスト機能が正常に動作するか確認する。

システム全体がマルウエア感染がないことを確認する。

竣工時にID・パスワードのリストを納入する。

工場出荷前及び引渡し前に、その時点で脆弱性情報に対して、適切に対応できているか確認する。

利用しない空USBポートは治具でふさぐ。
現場搬入後、引渡しまで施錠管理を実施する。
USBを接続する場合は、ウィルス検疫等確認したものに限る。

USBを接続する場合は、ウィルス検疫等確認したものに限る
外部媒体も使用する場合も同じ。

外部持込端末を接続する場合は、ウィルス検疫等確認したものに限る。

基本的な考え方／対応関係②の例　（３）

62443-4-1
セキュリティ検証・妥当性評価（SVV）

SVV-4：侵入テスト
要件：製品のセキュリティ脆弱性の発見と利用に焦点を当てたテストにより、セキュリティ関連の問題を特定し、特徴づけるためのプロセスを採用すること。
補足：侵入テストでは、特に製品の機密性、完全性、可用性を損なうことに焦点を当てます。侵入テストでは、深層防御設計の複数の側面を破ることができます。例えば、認証をバイパスして製品にアクセスしたり、特権の昇格を利用して管理者権限を獲得したり、暗号化を解除して機密性を侵害したりすることが挙げられます。この例が示すように、侵入テストでは、攻撃者のようにテストに臨み、多くの場合、製品の連鎖的な脆弱性を利用します。このプロセスは、製品が悪用される可能性のある、製品や製品の文書におけるセキュリティ関連の問題を発見するための努力がなされていることを確認するために必要です。このプロセスがあるということは、製品の供給者が、侵入テストによって製品のセキュリティを侵害しようとすることを意味します。侵入テストでは、製品の機能や深層防御戦略の脆弱性が悪用され、製品のセキュリティが侵害される可能性があることを確認します。このテストには、テストされる製品の種類に関する深い知識と、セキュリティテストツールや技術が必要です。侵入テストには、手動の技術、テストツール、またはその組み合わせが使用されます。

ビルセキュリティガイドライン別紙
31.コントローラ（DDC、PLC等）の施工検査

共通：設計通りの機能が入っているか検査する。

設置端末全てに対してマルウエア対策を施す。
ログ取得、解析のシステムが動作していることを確認する。

ネットワーク監視の仕組みが導入され正しく動作していることを確認する。

竣工検査時にホワイトリスト機能が正常に動作するか確認する。

システム全体がマルウエア感染がないことを確認する。

竣工時にID・パスワードのリストを納入する。

工場出荷前及び引渡し前に、その時点で脆弱性情報に対して、適切に対応できているか確認する。

利用しない空USBポートは治具でふさぐ。
現場搬入後、引渡しまで施錠管理を実施する。
USBを接続する場合は、ウィルス検疫等確認したものに限る。

USBを接続する場合は、ウィルス検疫等確認したものに限る
外部媒体も使用する場合も同じ。

外部持込端末を接続する場合は、ウィルス検疫等確認したものに限る。

基本的な考え方／対応関係②の例　（4）

62443-4-1
セキュリティ検証・妥当性評価（SVV）

SVV-5：独立した監督者
要件：テストを実施する個人が、表に従って製品を設計・実装した開発者から独立していることを保証するためのプロセスを採用しなければならない。

テストの種類	リファレンス	独立性のレベル
セキュリティ要求事項のテスト	SVV-1：セキュリティ要件テスト	独立した部門
脅威軽減テスト	SVV-2：脅威の軽減テスト	独立した部門
悪用ケースのテスト	SVV-3：脆弱性テスト	独立した担当者
静的コード解析	SI-1：セキュリティ導入レビュー	なし
攻撃表面分析	SVV-3：脆弱性テスト	独立した担当者
既知の脆弱性スキャン	SVV-3：脆弱性テスト	独立した担当者
ソフトウェア構成分析	SVV-3：脆弱性テスト	なし
侵入テスト	SVV-4：侵入テスト	独立した部門もしくは組織

独立性のレベルは以下のように定義されています。
・なし：独立性を必要としない。開発者がテストを行うことができる。
・独立した人：テストを実施する人は、製品の開発者の一人であってはならない。
・独立した部門：テストを実施する人は、製品の開発者と同じファーストラインマネージャーに報告することはできません。あるいは、品質保証（QA）部門のメンバーであっても構いません。
・独立した組織：テストを実施する人は、その製品の開発者と同じ組織に所属することはできません。組織とは、独立した法人、企業の一部門、または、副社長などの別の役員に報告する企業の部門を指します。
補足：独立したテスト実施者は、プログラミングチームの中で働いているテスト実施者や、職業としてプログラマーであるテスト実施者よりも、より多くの、他の、異なる欠陥を発見できることがよくあります。そのようなテスト実施者は、テストやレビューに異なる前提条件を持ち込むので、隠れた欠陥や問題を明らかにするのに役立つことが多いのです。さらに、上級管理者に報告する独立したテスト実施者は、同僚や、最悪の場合、管理者の仕事の問題点を指摘することによる報復を気にすることなく、正直に自分の結果を報告することができます。

62443-4-2との対応関係なし

ビルセキュリティガイドライン別紙
31.コントローラ（DDC、PLC等）の施工検査

共通：設計通りの機能が入っているか検査する。

設置端末全てに対してマルウエア対策を施す。
ログ取得、解析のシステムが動作していることを確認する。

ネットワーク監視の仕組みが導入され正しく動作していることを確認する。

竣工検査時にホワイトリスト機能が正常に動作するか確認する。

システム全体がマルウエア感染がないことを確認する。

竣工時にID・パスワードのリストを納入する。

工場出荷前及び引渡し前に、その時点で脆弱性情報に対して、適切に対応できているか確認する。

利用しない空USBポートは治具でふさぐ。
現場搬入後、引渡しまで施錠管理を実施する。
USBを接続する場合は、ウィルス検疫等確認したものに限る。

USBを接続する場合は、ウィルス検疫等確認したものに限る
外部媒体も使用する場合も同じ。

外部持込端末を接続する場合は、ウィルス検疫等確認したものに限る。

現状版のガイドラインに取入れ可能な情報の整理

1．ビルガイドラインの高度化のための調査
③その他関連する調査
③－３　ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討
現状版のガイドラインに取入れ可能な情報の整理

ビルセキュリティガイドラインと62443シリーズを比較、整理するため、①特定の個別対策分野の観点からと②技術面の対策と運用面の対策の観点から検討を実施した。
比較、整理の結果、現状版のガイドラインに取入れ可能な情報の観点としては、以下の２つが想定される。

- 機器の種類(62443-4-2)や、セキュリティ対策の運用・管理(62443-2-1)、パッチ管理(62443-2-3)、事前検疫(62443-2-4)、リスクアセスメント・リスク評価(62443-3-2)のように、特定の個別対策分野の観点ごとにポリシーの追加、整理を実施する。
- 既にビルセキュリティガイドラインに記載されているポリシーに、62443-3-3と62443-4-2に見られるような技術面の対策の要件と、運用面の対策の要件を追加し、網羅的な情報の追加、整理を実施する。

整理にあたっての基本的考え方①

特定の個別対策分野の観点からみて、ビルセキュリティガイドラインとの対応関係の整理が可能

現状版のガイドラインに取入れ可能な情報の観点①

既存のポリシーに機器の種類や、セキュリティ対策の運用・管理、パッチ管理、事前検疫、リスクアセスメント・リスク評価等、特定の個別対策分野ごとの情報を追加し、整理を実施することが想定可能。

整理にあたっての基本的考え方②

技術面の対策の観点や運用面の対策の観点からみて、ビルセキュリティガイドラインとの対応関係の整理が可能

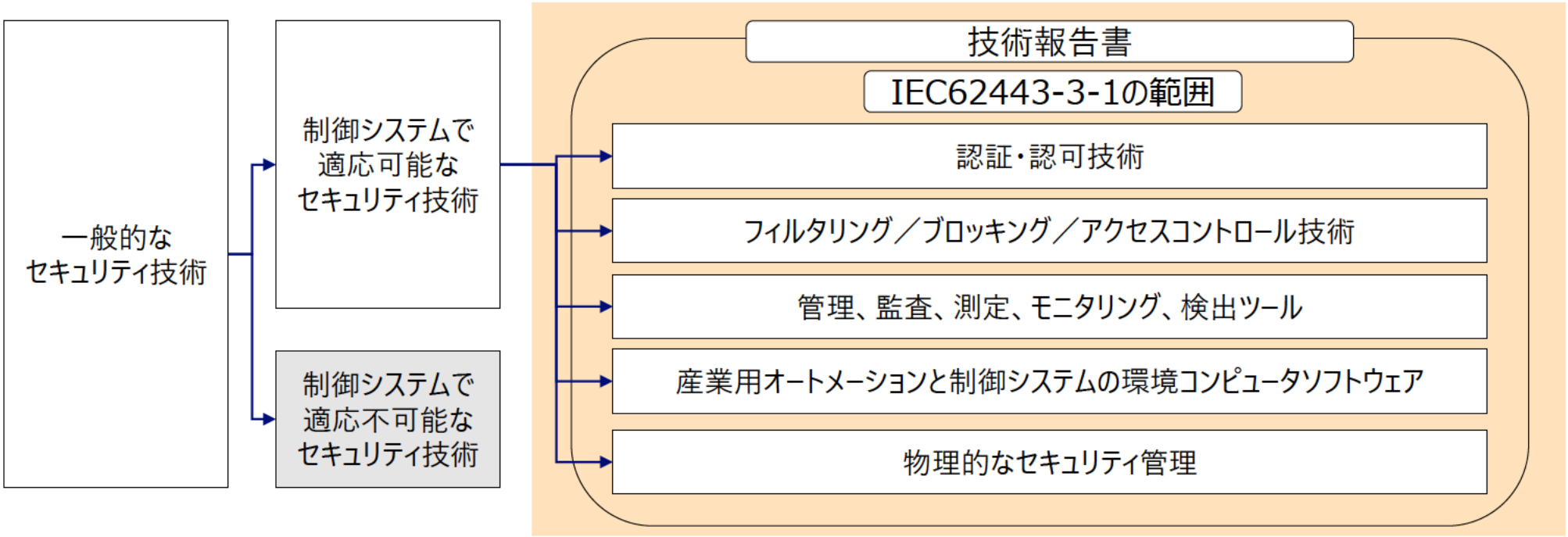
現状版のガイドラインに取入れ可能な情報の観点②

既存のポリシーの情報は限定的であるため、技術面の対策の要件と運用面の対策の要件を追加し、ポリシーの内容が網羅的になるよう、情報の追加、整理を実施することが想定可能。

【参考】IEC 62443-3-1：TECHNICAL REPORT

IEC 62443-3-1：TECHNICAL REPORT
Industrial communication networks – Network and system security –
Part 3-1: Security technologies for industrial automation and control systems

- 一般的なセキュリティ技術のうち、制御システムで適用可能なものについて、以下を記載した技術報告書。
  - ①概要、②対処するセキュリティ上の脆弱性、③典型的な展開例、④既知の問題点と弱点、⑤産業用自動化制御システムの環境下での使用評価、⑥今後の方向性、⑦提言とガイダンス、⑧情報源と参考資料
- セキュリティ技術の解説書という位置づけ。



IEC 62443-3-1：TECHNICAL REPORT
Industrial communication networks – Network and system security –
Part 3-1: Security technologies for industrial automation and control systems

	セキュリティ技術
認証・認可技術	一般的な認証・認可技術
	役割ベースの認証ツール
	パスワード認証
	チャレンジ/レスポンス認証
	物理/トークン認証
	スマートカード認証
	生体認証
	位置情報に基づく認証
	パスワード配布・管理技術
	端末間認証

IEC 62443-3-1：TECHNICAL REPORT
Industrial communication networks – Network and system security –
Part 3-1: Security technologies for industrial automation and control systems

	セキュリティ技術
フィルタリング／ブロッキング／アクセスコントロール技術	一般的なフィルタリング／ブロッキング／アクセスコントロール技術
	ネットワークのファイアウォール
	ホストベースのファイアウォール
	仮想ネットワーク

IEC 62443-3-1：TECHNICAL REPORT
Industrial communication networks – Network and system security –
Part 3-1: Security technologies for industrial automation and control systems

	セキュリティ技術
暗号化技術とデータ検証	一般的な暗号化技術とデータ検証
	秘密鍵の暗号化
	公開鍵暗号化と鍵配布
	仮想プライベートネットワーク（VPN）

IEC 62443-3-1：TECHNICAL REPORT
Industrial communication networks – Network and system security –
Part 3-1: Security technologies for industrial automation and control systems

	セキュリティ技術
管理、監査、測定、モニタリング、検出ツール	一般的な管理、監査、測定、モニタリング、検出ツール
	ログ管理の効用
	ウイルスや悪意のあるコードの検出システム
	侵入検知システム（IDS）
	脆弱性スキャナー
	鑑識・分析ツール（FAT）
	ホスト構成管理ツール（HCM）
	自動化されたソフトウェア管理ツール（ASM）

IEC 62443-3-1：TECHNICAL REPORT
Industrial communication networks – Network and system security –
Part 3-1: Security technologies for industrial automation and control systems

	セキュリティ技術
産業用オートメーションと制御システムの環境コンピュータソフトウェア	一般的な産業用オートメーションと制御システムの環境コンピュータソフトウェア
	サーバーおよびワークステーションのオペレーティングシステム
	リアルタイムおよび組み込みOS
	ウェブ技術

IEC 62443-3-1：TECHNICAL REPORT
Industrial communication networks – Network and system security –
Part 3-1: Security technologies for industrial automation and control systems

	セキュリティ技術
物理的なセキュリティ管理	一般的な物理的なセキュリティ管理
	物理的な措置
	人的セキュリティ

IEC 62443-3-1：TECHNICAL REPORT
Industrial communication networks – Network and system security –
Part 3-1: Security technologies for industrial automation and control systems

一般的な記載例（２ページ～３ページ程度）　5.9 パスワード配布・管理技術

認証・認可技術 / パスワード配布・管理技術

観点	内容
概要	ポリシーに基づいた一貫した方法で更新・変更される再利用可能なパスワードと組み合わせたユーザー識別は、制御システムのオペレータとユーザーのためのシステム識別と承認メカニズムの最も一般的な形式です。パスワードは、個人を認証するために使用される文字の保護されたシーケンスです。認証要素は、ユーザが知っているもの（例えばパスワード）、持っているもの（例えばスマートカード）、または存在するもの（例えばバイオメトリック）に基づいています。そのうちパスワードは、ユーザーが知っているものです。パスワードは、制御システムへのアクセスのために採用されている最も普及している認証メカニズムの一つであるため、高度に保護される必要があります。パスワードが強固で適切に管理されていることが重要であり、そのため、安全であると同時に、長期的な一貫した使用や不注意による誤った開示を防止するための更新と、その変更が保証された方法で配布されていることが重要です。
対処するセキュリティ上の脆弱性	パスワードが適切に生成され、更新され、秘密にされていれば、効果的なセキュリティを提供することができます。パスワードは、制御システムのユーザが持っているもの（例えばスマートカード）とは対照的に、ユーザが知っていることに基づいて認証されます。
典型的な展開例	パスワードは、中央制御室、産業組織内の遠隔地、または産業組織外のいずれかからログオンプロセス中に使用され、無線または有線モード、またはそれらの組み合わせを介して転送することができます。
既知の問題点と弱点	パスワードは最も一般的に使用されている認証メカニズムですが、最も弱いセキュリティメカニズムの一つと考えられています。パスワードの弱点は、ユーザが容易に推測できるパスワードを選択し、他人にパスワードを教え、付箋紙にパスワードを書き、制御室のコンピュータやHMIの近くのどこかに隠したりしていることが多いという事実に起因しています。ほとんどの制御システムのユーザーにとって、セキュリティは通常、コンピュータとHMIを使用する上で最も重要な、または興味深い部分ではありません。コンピューターに侵入して情報を盗むか、もっと悪いことに、自動化されたシステムを混乱させたり、キーコントロールシステム資産の操作することに目的がある攻撃者（インサイダーを含む）は次の手法を試してパスワードを取得し、最終的にセキュリティを危険にさらす可能性があるため、システムを安全に保つには、パスワードの機密を保持し、定期的に変更、さらには更新する必要があります。 • 電子監視：攻撃者は、特にユーザーが認証サーバーにパスワードを送信しているときに、ネットワークトラフィックを盗聴して情報を取得できます。パスワードは、攻撃者が別のときにコピーして再利用する可能性があります。パスワードの再利用は「リプレイ攻撃」と呼ばれます。 • パスワードファイルへのアクセス：パスワードファイルは通常、認証サーバーにあります。パスワードファイルには多くのユーザーのパスワードが含まれており、侵害された場合、多くの損害の原因となる可能性があります。パスワードファイルは、アクセス制御メカニズムと暗号化で保護する必要があります。 • ブルートフォース攻撃：攻撃者は、考えられる多くの文字、数字、記号の組み合わせを循環するツールを使用して、パスワードを発見できます。 • 辞書攻撃：攻撃者は、一致するものが見つかるまで、数千語のファイルを使用してユーザーのパスワードと比較します。 • ソーシャルエンジニアリング：攻撃者は、特定のリソースにアクセスするために必要な権限を持っていることを個人に偽って説得、交渉します。

IEC 62443-3-1：TECHNICAL REPORT
Industrial communication networks – Network and system security –
Part 3-1: Security technologies for industrial automation and control systems

一般的な記載例（２ページ～３ページ程度）　5.9 パスワード配布・管理技術

認証・認可技術

パスワード配布・管理技術

観点	内容
産業用自動化制御システムの環境下での使用評価	パスワードは、産業オートメーションプロセスまたは制御システムへのアクセスにおいて最も強力または最も弱いリンクになる可能性があります。 静的パスワード（一定期間同じままであるパスワード）は、動的パスワードが実用的でない多くの状況で使用されます。 静的パスワードは毎週など定期的に変更することをお勧めします。動的パスワード（ログオンごとに新しいパスワード）を使用すると、セキュリティが向上するため、実用的な場合に使用する必要があります。 動的パスワードの詳細については、次の節を参照してください。
今後の方向性	今後は、脆弱性に対する認識の高まりとハッカーの能力の向上により、セキュリティの重要性が増していくと考えられます。例えば、企業ネットワークにウイルスを介して埋め込まれたキーストローク・ロギング・プログラムや制御LANへの侵入など、新たに開発された高度なツールによって、ハッカーはその能力を飛躍的に高めることができます。セキュリティを向上させるための戦略の1つは、ワンタイムパスワードを使用することです。ワンタイムパスワードは、ダイナミックパスワードとも呼ばれます。動的パスワードは、認証の目的で使用され、一度使用したパスワードは無効になるため、ハッカーが入手しても再利用できません。このタイプの認証メカニズムは、静的パスワードよりも高いレベルのセキュリティを必要とする環境で使用されます。ワンタイムパスワード生成トークンには、同期型と非同期型の2つの一般的なタイプがあります。それぞれについて以下に説明します。トークンデバイスは、ユーザが認証サーバに送信するためのワンタイムパスワードを生成します。トークンデバイス（パスワード生成器）は、通常、液晶ディスプレイとキーパッドを備えたハンドヘルドデバイスである。このハードウェアは、ユーザがアクセスしようとするコンピュータとは別個のものです。トークンデバイスと認証サービスは、ユーザーを認証することができるようにするために、以下の手順で同期されている必要があります。。トークン装置は、コンピュータにログオンする際にパスワードとして入力される文字のリストをユーザに提示します。トークンデバイスと認証サービスは、これらの文字の意味を知っています。両者は同期しているため、トークンデバイスは、認証サービスが期待しているパスワードを正確に提示します。これは、トークンとも呼ばれるワンタイムパスワードであり、最初の使用後は無効になります。同期トークンデバイスは、認証プロセスの中核部分として時間またはカウンタを使用して認証サービスと同期します。同期が時間ベースの場合、トークンデバイスと認証サービスは、その内部時計の中で同じ時間を保持しなければならない。トークンデバイス内の時間値と秘密鍵を用いてワンタイムパスワードを作成し、ユーザに表示します。ユーザは、この値とユーザIDをコンピュータに入力し、認証サービスを実行しているサーバに渡します。認証サービスはこの値を復号化し、期待した値と比較します。2 つの値が一致した場合、ユーザーは認証され、コンピュータとリソースの使用が許可されます。トークンデバイスと認証サービスがカウンター同期を使用している場合、ユーザーはコンピュータ上でログオンシーケンスを開始し、トークンデバイスのボタンを押す必要があります。これにより、認証サービスのトークンデバイスは次の認証値に進みます。この値と基本秘密がハッシュ化され、ユーザに表示されます。ユーザは、この結果として得られた値を、認証されるユーザIDとともに入力します。時間ベースまたはカウンターベースの同期では、トークンデバイスと認証サービスは、暗号化および復号化に使用される秘密の基本鍵を共有しなければならない。非同期トークン生成方式を使用しているトークンデバイスは、チャレンジアンドレスポンス方式を使用してユーザを認証します。この場合、認証サーバはユーザにチャレンジを送信します。ユーザーはこのランダムな値をトークンデバイスに入力し、トークンデバイスはこの値を暗号化して、ユーザーがワンタイムパスワードとして使用する値を返します。ユーザはこの値をユーザ名とともに認証サーバに送信します。認証サーバが値を暗号化でき、それが以前に送信されたものと同じチャレンジであれば、ユーザは認証されます。同期トークンシステムと非同期トークンシステムの両方とも、ユーザが自分の識別情報を共有し、トークンデバイスが共有されたり盗まれたりした場合、攻撃者の餌食になる可能性があります。また、トークンデバイスは、認証の成功を妨げるバッテリーの故障やその他の誤動作を起こす可能性があります。しかし、トークンデバイスを使用しているシステムは、電子的な盗聴、盗聴、パスワードの推測に対して脆弱ではありません。

IEC 62443-3-1：TECHNICAL REPORT
Industrial communication networks – Network and system security –
Part 3-1: Security technologies for industrial automation and control systems

一般的な記載例（２ページ～３ページ程度）　5.9 パスワード配布・管理技術

		観点	内容
認証・認可技術	パスワード配布・管理技術	提言とガイダンス	セキュリティの程度は、情報やプロセスの価値、特に制御システムの場合は、それが保護する重要な産業用資産や機器と一致している必要があります。価値ある情報を含まない、あるいは取るに足らない良性資産に接続され、価値あるプロセスを制御せず、インターネットに接続されていない小規模なスタンドアロン制御システムは、簡単なパスワードで保護することができます。一方、相互に接続されていて、価値のある情報を含み、価値のあるプロセスを制御したり、価値のある危険なプロセスや機器を制御したりするシステムでは、より高度なパスワードセキュリティが必要となります。この場合、認知パスワードとワンタイムパスワードが適切であり、長期的には費用対効果が高くなります。補償プロセスでは、1回のハッカーの侵入で数百万ドルの収益の損失、システムや製品への深刻な損害、機密情報の損失、人員や環境への被害が発生する可能性があります。
		情報源と参考資料	以下の文献を参考文献を参照しています。 • Harris, Shon, All-in-One CISSP Exam Guide, Third Edition, ISBN 0072229667, McGraw-Hill/Osborne, New York, NY, 2005. • Inform IT, Security, Access Control Systems, Part 2, Verifying the Authenticity of an Identity, 2006.11.07, <http://www.informit.com/guides/>

IEC 62443-3-1：TECHNICAL REPORT
Industrial communication networks – Network and system security –
Part 3-1: Security technologies for industrial automation and control systems

最も詳細な記載例（5 ページ程度）　7.4 仮想プライベートネットワーク（VPN）

		観点	内容
認証・認可技術	仮想プライベートネットワーク（VPN）	概要	データを暗号化する方法の一つにVPNがあります。VPNは、公共インフラ上のオーバーレイとして動作するプライベート・ネットワークです。これには以下の3つのコンポーネントが含まれており、VPN の受信側で処理されます。 • 真正性と認証：送信、メッセージ、発信者、または特定のカテゴリーの情報を受信する個人の権限を検証する手段の妥当性を確立するために設計されたセキュリティ対策を実施する。 • 完全性：正式なセキュリティモードでは、完全性は、情報の不正な変更や破壊からの保護を意味するように、より狭く解釈されています。 • 機密性:：情報が無許可の個人、プロセス、デバイスに開示されないことを保証する。 VPNの二次的な構成要素は認可であり、これには次のようなものが含まれます。 • 特定のデータへのアクセス、読み取り、変更、挿入、削除、または特定のプログラムを実行するためにユーザに付与される権限。 • ユーザ、プログラム、またはプロセスに付与されたアクセス権限。 マルチプロトコルラベルスイッチング、フレームリレー、非同期転送モードなどの他のクラスの技術は、プライベートネットワークが公共インフラ上で動作することを可能にするため、VPNと誤解を招くように呼ばれることがあります。しかし、これらの技術は、上述したようにVPNの主要な構成要素をすべて含んでいるわけではありません。
		対処するセキュリティ上の脆弱性	VPNは、プライベート・ネットワークがパブリック・ネットワーク上で機能するようにすることを目的としています。VPNは、企業の情報や資料を物理的な施設間で安全に輸送するための装甲車と同じように、ネットワーク上のセキュリティを提供することができます。これは、「外部」の世界から輸送中の情報を保護します。IACS 環境の場合、外部の世界とは、通常、コントロールセンターの機器を操作する権限を持たない企業の LAN ユーザーが含まれます。VPN は以下のサービスを提供します。 • 認証による信頼されたネットワークへのアクセス制御。 • 信頼されていないネットワーク上の信頼されたデータの整合性を維持する。 • トラフィック監視、分析、侵入検知に役立つ情報を記録する。

IEC 62443-3-1：TECHNICAL REPORT
Industrial communication networks – Network and system security –
Part 3-1: Security technologies for industrial automation and control systems

最も詳細な記載例（5 ページ程度）　7.4 仮想プライベートネットワーク（VPN）

		観点	内容
認証・認可技術	仮想プライベートネットワーク（VPN）	典型的な展開例	一般的に、セキュリティゲートウェイとホストを使用して VPN 接続を作成する VPN導入には、3つの分類があります。 • セキュリティゲートウェイは、一対のセキュリティゲートウェイを横切るトラフィックを保護するために VPN 技術を使用する中間システムです。また、セキュリティゲートウェイは、デバイスを横断するトラフィックの認証を実装するために一般的に使用されます。セキュリティゲートウェイの機能は、ファイアウォール、ルータ、スイッチなどの既存のインターネット接続機器に実装されています。VPN コンセントレータや VPN ゲートウェイなどの新しい用語は、大量の VPN トラフィックを終端する専用のコンピューティングデバイスのために作成されました。 • ホストは、VPN 技術を使用して、ホストを発端とする、またはホストを宛先とするトラフィックを安全に保護します。ホストが使用するVPN技術は、ホストのネイティブ オペレーティング システムに含まれているか、またはVPNアクセスを有効にするためにホストのオペレーティングシステムに追加されています。 以下では、VPN展開の 3 つの分類について詳細に説明します。 • セキュリティ・ゲートウェイからセキュリティ・ゲートウェイ（図表による説明有り）：VPNの2つのエンドポイントは、信頼されたネットワークから別の信頼されたネットワークにトラフィックを渡す中間デバイスであり、信頼されていないトランスポート・ネットワーク上のトラフィックをVPN技術に依存して安全に保護します。このタイプのVPNは、一般的にサイト間VPNまたはLAN-to-LAN VPNと呼ばれています。 • ホストからセキュリティゲートウェイ（図表による説明有り）：一方のエンドポイントはホスト・コンピューティング・デバイスであり、もう一方のエンドポイントは中間デバイスであり、信頼されていないネットワーク上のトラフィックをVPN技術に頼りながら、ホストからセキュリティ・ゲートウェイの背後にある信頼されたネットワークにトラフィックを渡します。このタイプのVPNは、一般的にリモートアクセスVPNと呼ばれています。 • ホスト間（図表による説明有り）：VPNトンネルの各エンドポイントは、ホスト計算装置である。ホスト装置は、信頼されないネットワーク上の通信を確保するために、ホスト上のVPN技術を利用します。

IEC 62443-3-1：TECHNICAL REPORT
Industrial communication networks – Network and system security –
Part 3-1: Security technologies for industrial automation and control systems

最も詳細な記載例（5 ページ程度）　7.4 仮想プライベートネットワーク（VPN）

		観点	内容
認証・認可技術	仮想プライベートネットワーク（VPN）	典型的な展開例 （続き）	現在実装されているVPN技術の中で最も一般的なものは以下の通りです。 • インターネットプロトコルセキュリティ（IPsec）：IPsecは、公共ネットワーク上のデータの安全な通信を管理し、すべてのIPユニキャスト対応アプリケーションを安全に保護するためにIETFによって定義された一連の標準規格です。この規格によると、マルチキャストアプリケーションはIPsecを使用できません。しかし、IPsec を使用してマルチキャストトラフィックを保護することに特化した IETF ワーキンググループがあります。代替として、マルチキャストと非IPベースのプロトコルは、これらのプロトコルをIPユニキャスト対応のプロトコルにカプセル化し、希望するVPN受信デバイスごとに送信を複製することで、IPsec VPNを介して転送することができます。例えば、マルチキャストトラフィックは、暗号化されてIPsecを介して転送される前に、適切なヘッダにカプセル化することで、ルータからルータに渡すことができます。IPsecは、現在の多くのオペレーティングシステムに含まれているツールです。この標準の意図は、ベンダーのプラットフォーム間の相互運用性を保証することです。ベンダ間の相互運用性のための標準がある一方で、マルチベンダ実装の相互運用性の判断は、エンドユーザ組織が実施する特定の実装テストに依存しているのが現実です。プロトコルは、個々のユーザ認証やネットワークアドレス変換（NAT）デバイスのトランスバーサルに対応するためのプロトコルの拡張など、市場からの特定の要件に対応するために継続的に強化されてきました。これらの拡張は一般的にベンダー固有のものであり、主にホストからセキュリティゲートウェイ環境において相互運用性の問題を引き起こす可能性があります。 • セキュア・ソケット・レイヤー（SSL）：SSL は 2 台のマシン間で安全なチャネルを提供します。チャネルは通過するデータには気づかれません。IETFはSSLバージョン3プロトコルにわずかな変更を加え、TLS（Transport Layer Security）と呼ばれる新しいプロトコルを作成しました。SSLとTLSはしばしば互換的に使われています。このレポートでは、一般的にSSLの用語を使用しています。SSL は、HTTP トラフィックの安全性を確保するために最もよく認識されています。このプロトコルの実装は、HTTPセキュア（HTTPS）として知られています。しかし、SSL は HTTP トラフィックの保護だけに限定されるものではなく、多くの異なるアプリケーション層のプログラムの保護に使用することができます。SSL ベースの VPN 製品が受け入れられるようになったのは、「クライアントレス」VPN 製品の市場があるからです。クライアントレスは、ほとんどのネットワーク・オペレーティング・システムでは、オペレーティング・システムに組み込まれたウェブブラウザにSSLの実装が含まれているため、適切であると考えられています。VPN管理者は、サードパーティ製のVPN「クライアント」ソフトウェアをインストールする必要がなく、「クライアントレス」VPNを作成することができます。本当の利点は、実装がクライアントレスであるということではなく、クライアントのインストールがほとんど、あるいは全く必要ないということです。 • セキュアシェル(SSH)：SSH は、リモートコンピュータに安全にアクセスするためのコマンドインターフェイスおよびプロトコルです。ネットワーク管理者がウェブや他のタイプのサーバを遠隔操作するために広く使われています。最新版の SSH2 は IETF7F8 から提案されている標準セットです。一般的に、SSH は telnet アプリケーションの安全な代替手段として配備されています。しかし、SSH はポートフォワーディングを行う機能も持っており、上記の 3 つの展開で使用することができます。SSH は市場に出回っている UNIX® ディストリビューションの大部分に含まれており、一般的にはサードパーティのパッケージを介して他のプラットフォームに追加されます。 セキュリティ境界線を介して安全なアクセスを提供するために、VPN 技術を互いにオーバーレイすることが可能です。例えば、企業は、企業のエッジ境界線へのセキュアなアクセスを提供するために IPsec VPN を導入することができます。また、特定のユーザーが社内に埋め込まれたセキュリティ境界線へのアクセスを許可するために、SSL VPN サーバーを導入することもできます。

IEC 62443-3-1：TECHNICAL REPORT
Industrial communication networks – Network and system security –
Part 3-1: Security technologies for industrial automation and control systems

最も詳細な記載例（5 ページ程度）　7.4 仮想プライベートネットワーク（VPN）

認証・認可技術 ／ 仮想プライベートネットワーク（VPN）

観点	内容
既知の問題点と弱点	VPN は、ほとんどのデータ駆動型攻撃（ウイルスなど）、一部のサービス拒否攻撃、ソーシャルエンジニアリング攻撃、悪意のあるインサイダーからネットワークとワークステーションを保護することはできません。選択した VPN 技術にもよりますが、VPN の主な課題は以下の通りです。 • 相互運用性：この問題は、IPsec RFC の解釈が異なるため、主に IPsec に関連しており、一般的には、特定のベンダーから標準的な IPsec VPN クライアントと終端デバイスを選択することで、企業内で緩和されます。 • セットアップ：上述したように、新しい技術を導入するか、既存の技術の使いやすさを向上させることで、VPN のセットアップを容易にするための取り組みが市場にはいくつかあります。 • 継続的なサポートとメンテナンス：VPN は既存のネットワークへの技術オーバーレイであるため、企業はオーバーレイを維持し、基盤となるインフラが変化したときにオーバーレイを変更するために運用リソースを費やす必要があります。 VPN技術にはそれぞれトレードオフがあります。例えば、SSL ベースの VPN は、クライアント上の IPsec VPN よりも設定が簡単であると考えられていますが、IPsec VPN のように多種多様なアプリケーションやプロトコルをサポートすることはできません。
産業用自動化制御システムの環境下での使用評価	VPNは、信頼できないネットワークからPCNへのセキュアなアクセスを提供するために、IACS環境で最も頻繁に使用されます。信頼されていないネットワークは、インターネットから社内LANに至るまで様々です。適切に構成された VPN は、制御システムのホスト コンピュータやコントローラへのアクセスを大幅に制限し、セキュリティを向上させることができます。また、中間ネットワークから無許可の非必須トラフィックを除去することで、PCN の応答性を向上させることができます。他にも、ホストベースのセキュリティゲートウェイやミニスタンドアロンのセキュリティゲートウェイを使用して、個々の制御デバイスの前に挿入したり、個々の制御デバイス上で実行したりすることも可能です。個々のデバイスベースで VPN を実装するこの手法は、管理上のオーバーヘッドが大きくなる可能性があります。 IACS 環境で VPN を使用する場合のその他の問題点としては、以下のようなものがあります。 • Foundation Fieldbus®、PROFIBUS®、シリアルベースのネットワークなど、IP ベースではないプロトコルに対応した VPN 製品がないこと。AGA-12 のような新しいアプローチは、いくつかのレガシー通信プロトコル用に開発されています。 • PLC、RTU、DCS に見られる典型的なコントローラベースのオペレーティング・システム用のホストベース (ソフトウェア) VPN 製品がないこと。 • ホストベース (ソフトウェア) VPN 製品と Windows® または UNIX® 制御システムソフトウェアとの間に互換性がない可能性があること。 • 制御システム通信にレイテンシが追加されること。この問題については、さらなる調査とテストが必要です。 • VPN の再接続時間が長すぎて、ミッションクリティカルなリンクで使用できない可能性があります。この問題については、さらなる調査とテストが必要です。 • PROFInet®, Ethernet/IP®, Foundation Fieldbus HSE®, Modbus/TCP® などの IACS プロトコルのトランスポート層の暗号化スキームがサポートされていないこと。 • 産業用アプリケーションのための大規模な VPN を設計した経験がないこと。 • SCADA 環境の典型的な、広範囲に分散したシステムで VPN を管理するために必要なオーバーヘッド。

IEC 62443-3-1：TECHNICAL REPORT
Industrial communication networks – Network and system security –
Part 3-1: Security technologies for industrial automation and control systems

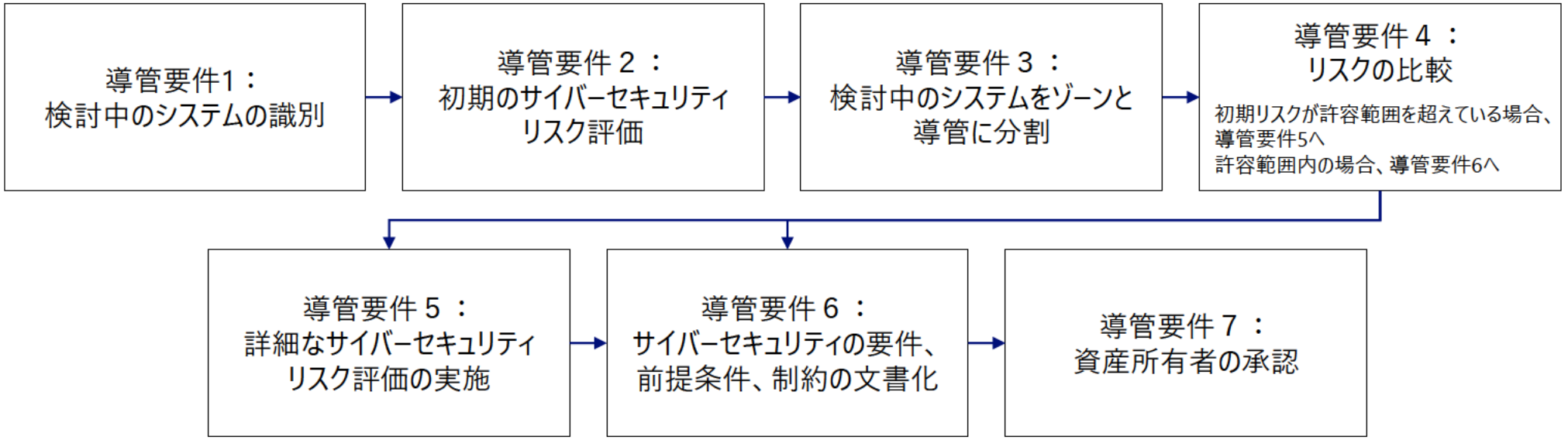
最も詳細な記載例（5 ページ程度）　7.4 仮想プライベートネットワーク（VPN）

		観点	内容
認証・認可技術	仮想プライベートネットワーク（VPN）	今後の方向性	今後の方向性としては、ネットワークやエンドデバイスに埋め込まれたVPN技術が挙げられます。
		提言とガイダンス	制御システムを保護するために使用されるVPN装置は、VPN技術がアプリケーションと互換性があり、VPN装置が実装のトラフィック特性に容認できないほどの影響を与えないことを確認するために、徹底的にテストされるべきです。
		情報源と参考資料	以下の文献を参考文献を参照しています。 • Smith, Richard E. (1997), Internet Cryptography, Addison Wesley, <www.awprofessional.com>. インターネットに適用される暗号技術の主題について、商用展開の例を交えて読みやすく紹介しています。この論考の多くは、多少の変更を加えて制御システムにも適用できます。本書はAESよりも前に書かれているため、最新の詳細についてはAESのウェブサイトを参照してください。 • E. Rescorla, Addison-Wesley, 2000, SSL and TLS – Designing and Building Secure Systems, <http://www.awprofessional.com>

【参考】IEC 62443-3-2：INTERNATIONAL STANDARD

IEC 62443-3-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design

- ゾーン（システム内領域）やそれらを連結するコンジットに関するセキュリティについて規定した国際標準。
- システムのセキュリティ設計手順、ゾーン（システム内領域）及びコンジットやセキュリティ要求事項の定義などが規定されている規格。



IEC 62443-3-2：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design

導管要件1：検討中のシステムの識別

実施内容	要求事項
ZCR 1.1：検討中のシステム（SUC）の周囲とアクセスポイントの特定	組織は、セキュリティ境界線の明確な区分け、および検討中のシステム（SUC）へのすべてのアクセスポイントの識別を含め、検討中のシステム（SUC）の範囲 を明確に識別しなければならない。

導管要件2：初期のサイバーセキュリティリスク評価

実施内容	要求事項
ZCR 2.1：初期のサイバーセキュリティリスク評価の実施	組織は、ミッションクリティカルな IACS の運用への干渉、違反、混乱、または無効化に起因して発生する可能性のあるサイバーセキュリティリスクを特定するために、検討中のシステム（SUC）のサイバーセキュリティリスク評価を実施するか、または実施済の初期サイバーセキュリティリスク評価がまだ適用可能であることを確認しなければならない。

IEC 62443-3-2：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design

導管要件３：検討中のシステムをゾーンと導管に分割

実施内容	要求事項
ZCR 3.1：ゾーン（システム内領域）と導線の確立	組織は、セキュリティ境界線の明確な区分け、および検討中のシステム（SUC）へのすべてのアクセスポイントの識別を含め、検討中のシステム（SUC）の範囲 を明確に識別しなければならない。
ZCR 3.2：事業と産業用自動制御システム（IACS）資産の分離	産業用自動制御システム（IACS）資産は、業務または企業システム資産から論理的または物理的に分離されたゾーン（システム内領域）にグループ化されなければならない。
ZCR 3.3：安全関連資産の分離	安全関連産業用自動制御システム（IACS）資産は、非安全関連産業用自動制御システム（IACS）資産のあるゾーンから論理的又は物理的に分離されたゾーン（システム内領域）にグループ化されなければならない。ただし、分離できない場合は、ゾーン（システム内領域）全体を安全関連ゾーン（システム内領域）して識別しなければならない。
ZCR 3.4：一時的に接続されたデバイスの分離	検討中のシステム（SUC）への一時的な接続を許可されているデバイスは、産業用自動制御システム（IACS）への恒久的な接続を意図している資産から別のゾーン（システム内領域）にグループ化されなければならない。
ZCR 3.5：ワイヤレスデバイスの分離	ワイヤレスデバイスは、有線デバイスから分離された1つ以上のゾーン（システム内領域）に存在しなければならない。
ZCR 3.6：外部ネットワークを介して接続された別々のデバイス	検討中のシステム（SUC）の外部ネットワークを介して検討中のシステム（SUC） への接続が許可されているデバイスは、別のゾーン（システム内領域）にグループ化されなければならない。

IEC 62443-3-2：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design

導管要件４：リスクの比較

実施内容	要求事項
ZCR 4.1：初期リスクと許容可能なリスクの比較	「導管要件２：初期のサイバーセキュリティリスク評価」で決定された初期リスクを、組織の許容リスクと比較する。初期リスクが許容可能なリスクを超えている場合、組織は、「導管要件５：詳細なサイバーセキュリティリスク評価の実施」に定義されている詳細なサイバーセキュリティリスクアセスメントを実施しなければならない。

導管要件５：詳細なサイバーセキュリティリスク評価の実施

実施内容	要求事項
ZCR 5.1：脅威の識別	ゾーン（システム内領域）または導管内に含まれる資産に影響を与える可能性のある脅威のリストを作成しなければならない。
ZCR 5.2：脆弱性の特定	ゾーン（システム内領域）または導管は、アクセスポイントを含む、ゾーン（システム内領域）または導管内に含まれる資産に関連する既知の脆弱性を特定し、文書化するために分析されなければならない。
ZCR 5.3：結果と影響の判定	各脅威のシナリオは、脅威が実現した場合の結果と影響を決定するために評価されなければならない。その内容は、最悪の場合の人員の安全、財務上の損失、事業の中断、環境などのリスク領域への影響を含む。
ZCR 5.4：無制限の可能性の判定	各脅威は、無制限の可能性を視野に入れて評価されなければならない。これは、脅威が実現する可能性を示すものである。

IEC 62443-3-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design

導管要件5：詳細なサイバーセキュリティリスク評価の実施（続き）

実施内容	要求事項
ZCR 5.5：無制限のサイバーセキュリティリスクの判定	各脅威に対する最小化されないサイバーセキュリティリスクは、「ZCR 5.3：結果と影響の判定」で決定された影響度の尺度と「ZCR 5.4：無制限の可能性の判定」で決定された最小化されない可能性の尺度を組み合わせて決定されなければならない。
ZCR 5.6：対象セキュリティレベルの判定	各ゾーン（システム内領域）または導管にセキュリティレベルを判定しなければならない。
ZCR 5.7：軽減されていないリスクと許容可能なリスクの比較	「ZCR 5.5：無制限のサイバーセキュリティリスクの判定」で特定された各脅威について決定された最小化されていないリスクは、組織の許容可能なリスクと比較されなければならない。軽減されていないリスクが許容リスクを超える場合、組織は、リスクを受け入れるか、移転するか、または軽減するかを決定しなければならない。リスクを軽減するためには、「ZCR 5.8：既存の対策の特定と評価」から「ZCR 5.12：追加のサイバーセキュリティ対策の特定」を完了することにより、脅威の評価を継続するものとする。そうでなければ、組織は「ZCR 5.13：結果の文書化と共有」に結果を文書化し、次の脅威に進むことができる。
ZCR 5.8：既存の対策の特定と評価	検討中のシステム（SUC）内の既存の対策を特定し、その可能性や影響を低減するための対策の有効性を評価しなければならない。
ZCR 5.9：可能性と影響力の再評価	対策とその有効性を考慮して、可能性と影響を再評価しなければならない。

IEC 62443-3-2：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design

導管要件5：詳細なサイバーセキュリティリスク評価の実施（続き）

実施内容	要求事項
ZCR 5.10：残存リスクの判定	「ZCR 5.1：脅威の識別」で特定された各脅威の残留リスクは、「ZCR 5.9：可能性と影響力の再評価」で決定された緩和された尤度指標と緩和された影響値を組み合わせて決定されなければならない。
ZCR 5.11：残存リスクと許容可能なリスクの比較	「ZCR 5.1:脅威の識別」で特定された各脅威について決定された残留リスクは、組織の許容リスクと比較されるものとする。残存リスクが許容リスクを超える場合、組織は、組織の方針に基づき、残存リスクを受け入れるか、移転するか、または緩和するかを決定しなければならない。
ZCR 5.12：追加のサイバーセキュリティ対策の特定	残存リスクが組織の許容可能なリスクを超えている場合、組織がリスクを許容するか移転することを選択しない限り、技術的、管理的、手続き的なコントロールなどの追加的なサイバーセキュリティ対策を特定して、リスクを軽減しなければならない。
ZCR 5.13：結果の文書化と共有	詳細なサイバーリスク評価の結果は、文書化し、報告し、組織内の適切な利害関係者が利用できるようにしなければならない。また適切な情報セキュリティ 文書の機密性を保護するために、分類を割り当てるものとする。 文書には、各セッションが実施された日付、参加者の氏名、肩書きが含まれるものとする。サイバーリスクアセスメントの実施に役立った文書（システムアーキテクチャ図、PHA、脆弱性評価、ギャップ評価、脅威情報源など）は、サイバーリスクアセスメントと一緒に記録し、保管しなければならない。

IEC 62443-3-2：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design

導管要件6：サイバーセキュリティの要件、前提条件、制約の文書化

実施内容	要求事項
ZCR 6.1：サイバーセキュリティ要件仕様	詳細なリスクアセスメントの結果に基づく検討中のシステム（SUC） の必須のセキュリティ対策と、会社またはサイト固有の方針、基準、関連法規に基づく一般的なセキュリティ要求事項を文書化するために、サイバーセキュリティ要求事項仕様書（CRS）を作成しなければならない。
ZCR 6.2：検討中のシステム（SUC）の記述	検討中のシステム（SUC）のハイレベルな説明と描写が、サイバーセキュリティ要求事項仕様書（CRS）に含まれるものとする。最低限、サイバーセキュリティ要求事項仕様書（CRS）には、検討中のシステム（SUC） の名称、機能の高度な説明、および意図された使用方法の説明、ならびに管理下にある装置またはプロセスの説明を含めなければならない。
ZCR 6.3：ゾーン（システム内領域）と導管（コンジット）の図面	組織は次のことを行わなければならない。 a) SUC 全体のゾーン（システム内領域）と導管（コンジット）の分割を図示した図面または図面のセットを作成する。 b) SUC内の各資産をゾーン（システム内領域）と導管（コンジット）に割り当てる。

IEC 62443-3-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 3-2: Security risk assessment for system design

導管要件6：サイバーセキュリティの要件、前提条件、制約の文書化（つづき）

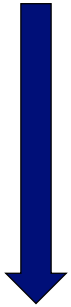
実施内容	要求事項
ZCR 6.4：ゾーン（システム内領域）と導管（コンジット）の特性	定義されたゾーン及びコンジットごとに、以下の項目を識別し、文書化しなければならない。 a) 名前及び/又は固有の識別子 b) 説明責任のある組織 c) 論理的境界の定義 d) 物理的境界の定義（該当する場合） e) 安全性の指定 f) すべての論理アクセスポイントのリスト g) すべての物理的アクセスポイントのリスト h) 各アクセスポイントに関連するデータフローのリスト i) 接続されたゾーンまたは導管 j) 資産のリストとその分類、重要度、ビジネス価値 k) セキュリティレベル l) 適用可能なセキュリティ要件 m) 適用されるセキュリティポリシー n) 前提条件と外部依存関係
ZCR 6.5：動作環境の前提条件	サイバーセキュリティ要求事項仕様書（CRS）は、検討中のシステム（SUC）が配置されている、または配置される予定の物理的・論理的環境を特定し、文書化しなければならない。
ZCR 6.6：脅威環境	サイバーセキュリティ要求事項仕様書（CRS）には、検討中のシステム（SUC）に影響を与える脅威環境の記述が含まれるものとする。この記述には、脅威情報のソースを含め、現在の脅威と新たな脅威の両方を含めるものとする。

IEC 62443-3-2：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design

導管要件6：サイバーセキュリティの要件、前提条件、制約の文書化（つづき）

実施内容	要求事項
ZCR 6.7：組織的なセキュリティポリシー	組織的なセキュリティポリシーを実施するセキュリティ対策や機能をサイバーセキュリティ要求事項仕様書（CRS）に含めなければならない。
ZCR 6.8：許容可能なリスク	検討中のシステム（SUC）に対する組織の許容可能なリスクは、サイバーセキュリティ要求事項仕様書（CRS）に含めなければならない。
ZCR 6.9：規制要件	検討中のシステム（SUC）に適用される関連するサイバーセキュリティ規制要件は、サイバーセキュリティ要求事項仕様書（CRS）に含まれなければならない。

IEC 62443-3-2：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design



導管要件7：資産所有者の承認

実施内容	要求事項
ZCR 7.1：資産所有者の承認の取得	検討中のシステム（SUC）が管理するプロセスの安全性、完全性及び信頼性に責任を負うアセットオーナー管理者は、リスクアセスメントの結果をレビューし、承認しなければならない。

IEC 62443-3-2：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design

一般的な記載例（1 / 4 ページ～ 1 / 2 ページ程度）　ZCR 3.1：ゾーン（システム内領域）と導線の確立

導管要件3：検討中のシステムをゾーンと導管に分割	ZCR 3.1：ゾーン（システム内領域）と導線の確立	観点	内容
		要件	組織は、リスクに応じて、IACS 及び関連資産をゾーンまたは導管にグルーピングする。グループ化は、当初のサイバーセキュリティリスクアセスメントの結果や、資産の重要度、運用機能、物理的または論理的な位置、必要なアクセス（例えば、最小特権原則など）、責任組織の他の基準等に基づいて行うものとする。
		根拠と補足ガイダンス	資産をゾーンと導管に分類する目的は、共通のセキュリティ要件を持つ資産を特定し、リスクを軽減するために必要な共通のセキュリティ対策を特定できるようにすることです。IACS 資産のゾーン及び導管への割り当ては、詳細なリスク評価の結果に基づいて調整することができる。これは一般的な要件ですが、安全計装システム、無線システム、インターネットのエンドポイントに直接接続されたシステム、IACS にインターフェースを提供しているが、他のエンティティ（外部システムを含む）によって管理されているシステム、モバイルデバイスなどの安全関連システムには特に注意を払う必要があります。 例えば、施設は、まず、材料の保管、加工、仕上げなどのオペレーションエリアに分けられるかもしれません。オペレーションエリアは、製造実行システム（MES）、監視システム（ヒューマンマシンインターフェース（HMI）など）、主制御システム（BPCS、DCS、リモートターミナルユニット（RTU）、プログラマブルロジックコントローラ（PLC）など）、安全システムなどの機能層にさらに分けることができます。IEC 62264-1で定義されているパデュー参照モデルなどのモデルが、この部門の基礎として使用されることがよくあります。IACS 製品サプライヤのリファレンスアーキテクチャも参考になります。

IEC 62443-3-2：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design

最も詳細な記載例（１ページ半程度）　ZCR 6.4：ゾーン（システム内領域）と導管（コンジット）の特性

導管要件6：サイバーセキュリティの要件、前提条件、制約の文書化

ZCR 6.4：ゾーン（システム内領域）と導管（コンジット）の特性

観点	内容
要件	定義されたゾーン及びコンジットごとに、以下の項目を識別し、文書化しなければならない。 • a) 名前及び/又は固有の識別子 • b) 説明責任のある組織 • c) 論理的境界の定義 • d) 物理的境界の定義（該当する場合） • e) 安全性の指定 • f) すべての論理アクセスポイントのリスト • g) すべての物理的アクセスポイントのリスト • h) 各アクセスポイントに関連するデータフローのリスト • i) 接続されたゾーンまたは導管 • j) 資産のリストとその分類、重要度、ビジネス価値 • k) セキュリティレベル • l) 適用可能なセキュリティ要件 • m) 適用されるセキュリティポリシー • n) 前提条件と外部依存関係

IEC 62443-3-2：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design

最も詳細な記載例（１ページ半程度）　ZCR 6.4：ゾーン（システム内領域）と導管（コンジット）の特性

導管要件6：サイバーセキュリティの要件、前提条件、制約の文書化

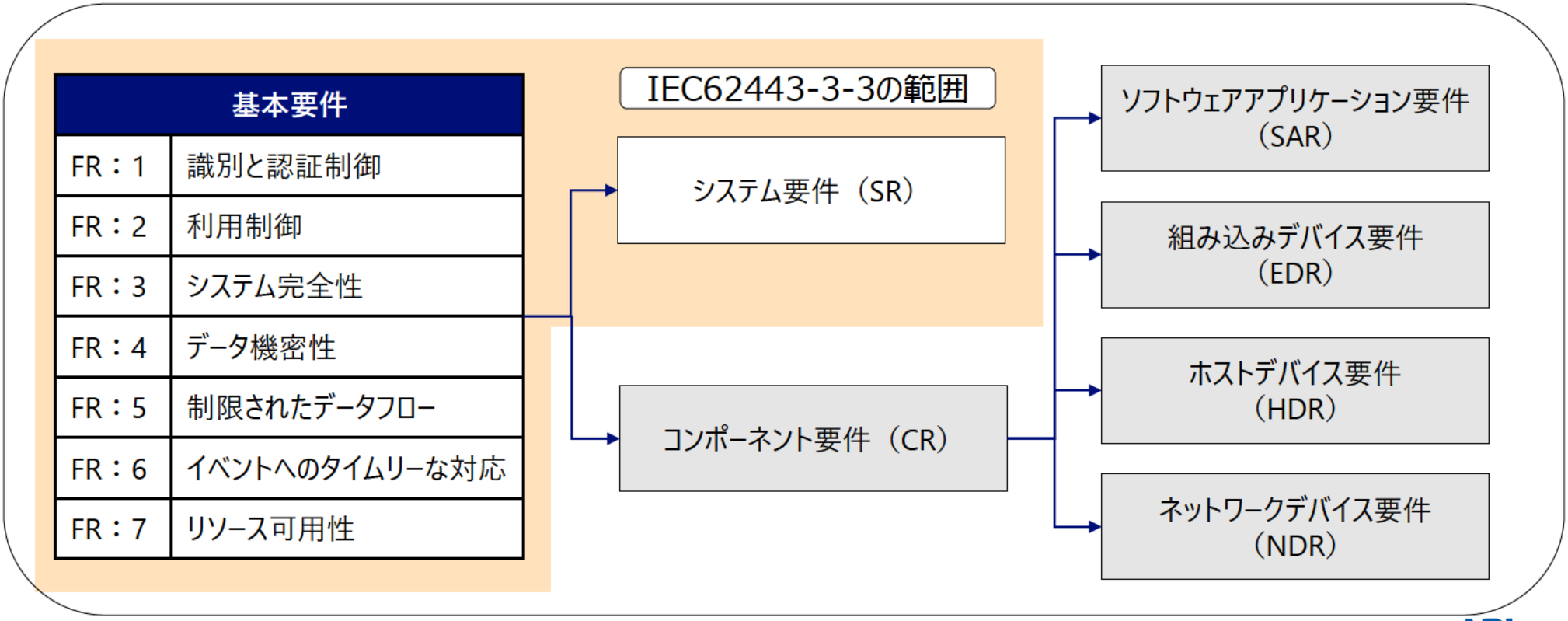
ZCR 6.4：ゾーン（システム内領域）と導管（コンジット）の特性

観点	内容
根拠と補足ガイダンス	ゾーンまたはコンジットの属性を特徴づけ、文書化することが重要である。上記の要求事項に記載されている各項目は、以下に説明するように特定の目的を持っている。 • a) 名前および/または一意の識別子：各ゾーンまたはコンジットを一意に識別できるようにすることは、設計および文書化の目的で重要である。 • b) 説明責任のある組織：説明責任のある組織とは、ゾーンまたはコンジットのセキュリティに責任を持ち、説明責任を負う 個人、グループまたはグループのことである。注：説明責任のある組織と責任のある組織は異なる場合がある。その場合は、両者を識別する。 • c) 論理的境界：論理的境界は、ゾーンまたはコンジットとシステムの他の部分との境界を明確にするために重要である。また、ゾーンまたはコンジットに出入りするすべての通信の境界線を特定するのにも役立つ。 • d) 物理的境界：ゾーンまたはコンジットがSL-Tを達成するために物理的セキュリティを必要とする場合、物理的境界を文書化することが重要である。物理的セキュリティが SL-T を向上させる可能性がある場合（必須ではないが）は、好ましくは文書化されるべきである。 • e) 安全性の指定 ：ゾーンまたはコンジットが安全に関連しているか、または安全に関連した資産が含まれているかを識別することが重要である。 • f) 論理アクセスポイントのリスト：論理アクセスポイントとは、電子情報がゾーンまたはコンジットの論理的境界を越えることができる場所である。論理アクセスポイントは、脅威によって悪用される可能性のある脆弱性を持つ可能性があるため、特定され、文書化される必要がある。 • g) 物理的アクセスポイントのリスト：物理的アクセスポイント(例えば、フェンス、ドア、エンクロージャ)とは、ゾーンまたはコンジットの資産に人員が物理的にアクセスできる場所のことである。物理的アクセスポイントは、不正アクセスを監視し、防止するための適切な手段を決定するために、特定され、文書化される必要がある。 • h) データフローのリスト：異常を検出するためには、システム全体の予想されるデータフロー(例えば、ソース、デスティネーション、プロトコル)を特定し、文書化することが重要であり、特に、ゾーンやコンジットに出入りするデータのフローを特定することが重要である。 • i) 接続されたゾーンまたは導管：システムへの論理的なアクセスポイントとシステム内のすべての論理的なアクセスポイントを特定するために、ゾーンと導管の間の接続性を特定することが重要です。通常、これはゾーンとコンジットの図で示されます。 • j) 資産のリストとその分類、重要度、ビジネス価値：各ゾーンまたはコンジット内に含まれる IACS 資産とその分類、重要度、ビジネス価値を特定することは、ゾーンまたはコンジットに障害が発生した場合の影響を理解するために重要です。結果を特定する際には、問題のゾーン/コンジットだけでなく、他のゾーン/コンジットへの影響も考慮することが重要である。 • k) SL-T：SL-Tはリスクアセスメントの結果に基づいて、ゾーン又はコンジットに必要な保護レベルを伝える。詳細は4.6.7を参照のこと。 • l) 適用されるセキュリティ要件：各ゾーン及びコンジットについて、SL-Tを達成するために必要な適用されるセキュリ ティ要件を特定する必要がある。いくつかの要求事項は、SUC内のすべてのゾーンまたは導管に共通である場合もあるが、他の要求事項は特定のものである場合もある。注：詳細なリスクアセスメントが完了するまで、セキュリティ要求事項の仕様を確定することはできない。 • m) 適用可能なセキュリティポリシー：各ゾーン及びコンジットについて、SL-T を達成するために必要な適用可能な組織のセキュリティポリシーを特定する必要がある。ポリシーの中には、SUC 内のすべてのゾーンまたは導管に共通するものもあれば、特定のものもある。 • n) 前提条件と外部依存性：ゾーンまたはコンジットのセキュリティは、クリーン電力や物理的およびネットワークセキュリティの追加レイヤなど、ゾーンまたはコンジットの外部要因に依存していることが多い。これらの仮定及び相互依存性は、文書化されるべきである。

【参考】IEC 62443-3-3：INTERNATIONAL STANDARD

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

- システムのセキュリティ要件を規定した国際標準。
- 基本要件（FR）とシステム要件（SR）をベースに、各種システムに合わせて最適化を目指す。



IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

FR：1　識別と認証制御で求められるセキュリティレベル

SL1	認証されていない存在による偶発的または偶然のアクセスから保護するメカニズムにより、すべてのユーザー（人間、ソフトウェアプロセス、およびデバイス）を識別し、認証する。
SL 2	低リソース、一般的なスキル、およびモチベーションの低い単純な手段を用いた、ある存在による意図的な認証されていないアクセスから保護するメカニズムにより、すべてのユーザ（人間、ソフトウェアプロセス、およびデバイス）を識別し、認証する。
SL 3	適度なリソース、IACS特有のスキル、および適度なモチベーションを持つ洗練された手段を用いた、ある存在による意図的な認証されていないアクセスから保護するメカニズムにより、すべてのユーザー（人間、ソフトウェアプロセス、およびデバイス）を識別し、認証する。
SL 4	拡張されたリソース、IACS特有のスキル、および高いモチベーションを持つ洗練された手段を用いた、ある存在による意図的な認証されていないアクセスから保護するメカニズムによって、すべてのユーザー（人間、ソフトウェアプロセス、およびデバイス）を識別し、認証する。

FR：1　識別と認証制御

システム要件（SR）	セキュリティレベル			
	SL1	SL2	SL3	SL4
SR 1.1：人間のユーザー識別と認証	○			
SR1.1(1)：（拡張要件）固有の識別および認証		○	○	○
SR1.1(2)：（拡張要件）信頼されないネットワークに対する多要素認証			○	○
SR1.1(3)：（拡張要件）すべてのネットワークに対応した多要素認証				○
SR 1.2：ソフトウェアプロセスとデバイスの識別と認証		○		
SR1.2(1)：（拡張要件）固有の識別および認証			○	○
SR 1.3：アカウント管理	○	○		
SR1.3(1)：（拡張要件）アカウント管理の統一			○	○

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

FR：1　識別と認証制御

システム要件（SR）	セキュリティレベル			
	SL1	SL2	SL3	SL4
SR 1.4：管理の識別	○	○	○	○
SR 1.5：認証機能の管理	○	○		
SR1.5(1)：（拡張要件）認証機器のハードウェアセキュリティ			○	○
SR 1.6：無線アクセス管理	○			
SR1.6(1)：（拡張要件）固有の識別および認証		○	○	○
SR 1.7：パスワードベースの認証の強度	○	○		
SR1.7(1)：（拡張要件）人間のユーザーのパスワード生成と有効期限の制限			○	
SR1.7(2)：（拡張要件）すべてのユーザ（人間、ソフトウェアプロセス、またはデバイス）のパスワードの有効期限の制限			○	○
SR1.8：公開鍵の基盤証明書		○	○	○
SR1.9：公開鍵ベースの認証の強度		○		
SR1.9(1)：（拡張要件）公開鍵ベース認証のためのハードウェアセキュリティ			○	○
SR1.10：認証機能のフィードバック	○	○	○	○
SR1.11：ログインに失敗した試行	○	○	○	○

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

	システム要件（SR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
FR：1 識別と認証制御	SR1.12：システム利用通知	○	○	○	○
	SR 1.13：信頼されていないネットワーク経由でのアクセス	○			
	SR1.13(1)：（拡張要件）明示的なアクセス要求の承認		○	○	○

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

FR：2　利用制御で求められるセキュリティレベル

SL1	特定の権限に従ってIACSの使用を制限し、偶発的または偶然の誤用から保護する。
SL 2	低リソース、一般的なスキル、およびモチベーションの低い単純な手段を用いた、ある存在による迂回行為から保護するために、指定された特権に従ってIACSを使用することを制限する。
SL 3	適度なリソース、IACS特有のスキル、および適度なモチベーションを持つ洗練された手段を用いた、ある存在による迂回行為から保護するために、指定された特権に従ってIACSを使用することを制限する。
SL 4	拡張されたリソース、IACS特有のスキル、および高いモチベーションを持つ洗練された手段を用いた、ある存在による迂回行為から保護するために、指定された特権に従ってIACSを使用することを制限する。

FR：2　利用制御

システム要件（SR）	セキュリティレベル			
	SL1	SL2	SL3	SL4
SR 2.1：認証の実施	○			
SR2.1(1)：（拡張要件）すべてのユーザー（人間、ソフトウェアプロセス、デバイス）に権限付与		○	○	○
SR2.1(2)：（拡張要件）認証の役割マッピング		○	○	○
SR2.1(3)：（拡張要件）監督者の変更			○	○
SR2.1(4)：（拡張要件）二重認証				○
SR 2.2：無線利用制御	○	○		
SR2.2(1)：（拡張要件）許可されていない無線デバイスを特定、報告			○	○

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

	システム要件（SR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
FR：2 利用制御	SR 2.3：携帯機器やモバイル機器の利用制御	○	○		
	SR2.3(1)：（拡張要件）携帯機器・モバイル機器のセキュリティの強化			○	○
	SR 2.4：モバイルコード	○	○		
	SR2.4(1)：（拡張要件）モバイルコードの完全性チェック			○	○
	SR 2.5：セッションロック	○	○	○	○
	SR 2.6：リモートセッションの終了		○	○	○
	SR 2.7：同時進行セッションの制御			○	○
	SR 2.8：監査対象のイベント	○	○		
	SR2.8(1)：（拡張要件）集中管理されたシステム全体の監査証跡			○	○
	SR 2.9：監査の記憶容量	○	○		
	SR2.9(1)：（拡張要件）監査記録の保存容量が閾値に達した場合の警告			○	○
	SR 2.10：監査処理の不備への対応	○	○	○	○

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

	システム要件（SR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
FR：2 利用制御	SR 2.11：タイムスタンプ		○		
	SR2.11(1)：（拡張要件）時刻同期			○	○
	SR2.11(2)：（拡張要件）時間源の完全性の保護				○
	SR 2.12：否認防止			○	
	SR2.12(1)：（拡張要件）すべてのユーザーへの否認防止				○

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

FR：3　システム完全性で求められるセキュリティレベル

SL1	何気ない操作や偶然の操作からIACSの完全性を守る。
SL 2	低リソース、一般的なスキル、およびモチベーションの低い単純な手段を用いた者による操作からIACSの完全性を保護する。
SL 3	適度なリソース、IACS特有のスキル、および適度なモチベーションを持つ洗練された手段を用いた者による操作からIACSの完全性を保護する。
SL 4	拡張されたリソース、IACS特有のスキル、および高いモチベーションを持つ洗練された手段を用いた者による操作からIACSの完全性を保護する。

FR：3　システム完全性

システム要件（SR）	セキュリティレベル			
	SL1	SL2	SL3	SL4
SR 3.1：通信の完全性	○	○		
SR3.1(1)：（拡張要件）暗号の完全性保護			○	○
SR 3.2：悪意のあるコードからの保護	○			
SR3.2(1)：（拡張要件）入口と出口において悪意のあるコードの保護		○	○	○
SR3.2(2)：（拡張要件）悪意のあるコード保護のための集中管理とレポート			○	○
SR 3.3：セキュリティ機能の検証	○	○		
SR3.3(1)：（拡張要件）セキュリティ機能検証のための自動化メカニズム			○	○
SR3.3(2)：（拡張要件）通常運用時のセキュリティ機能の検証				○

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

	システム要件（SR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
FR：3 システム完全性	SR 3.4：ソフトウェアと情報の完全性		○		
	SR3.4(1)：（拡張要件）完全性侵害の自動通知			○	○
	SR 3.5：入力の検証	○	○	○	○
	SR 3.6：決定的な出力		○	○	○
	SR 3.7：エラー処理	○	○	○	○
	SR 3.8：セッションの完全性		○		
	SR3.8(1)：（拡張要件）セッション終了後のセッションIDの無効化			○	○
	SR3.8(2)：（拡張要件）固有のセッションIDの生成			○	○
	SR3.8(3)：（拡張要件）セッションIDのランダム性				○
	SR 3.9：監査情報の保護		○	○	
	SR3.9(1)：（拡張要件）書き込みメディアの監査記録				○

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

FR：4　データ機密性で求められるセキュリティレベル

SL1	盗聴や偶然の暴露による情報の不正な開示を防止する。
SL 2	低リソース、一般的なスキル、およびモチベーションの低い単純な手段を用いて、積極的に情報を探している存在への情報の不正な開示を防止する。
SL 3	適度なリソース、IACS特有のスキル、および適度なモチベーションを持つ洗練された手段を用いて、積極的に情報を探している存在への情報の不正な開示を防止する。
SL 4	拡張されたリソース、IACS特有のスキル、および高いモチベーションを持つ洗練された手段を用いて、積極的に情報を探している存在への情報の不正な開示を防止する。

FR：4　データ機密性

システム要件（SR）	セキュリティレベル			
	SL1	SL2	SL3	SL4
SR 4.1：情報の機密性	○			
SR4.1(1)：（拡張要件）信頼されていないネットワークを利用時の静止時またはトランジット中の機密性の保護		○	○	○
SR4.1(2)：（拡張要件）ゾーン（システム内領域）の境界を越えた守秘義務の保護				○
SR 4.2：情報の持続性		○		
SR4.2(1)：（拡張要件）共有メモリのリソースの消去			○	○
SR 4.3：暗号技術の利用	○	○	○	○

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

FR：5　制限されたデータフローで求められるセキュリティレベル

SL1	ゾーン（システム内領域）と導管のセグメンテーションの偶発的または偶然の迂回を防止する。
SL 2	低リソース、一般的なスキル、およびモチベーションの低い単純な手段を用いた、ある存在によるゾーン（システム内領域）と導管のセグメンテーションの意図的な迂回を防止する。
SL 3	適度なリソース、IACS特有のスキル、および適度なモチベーションを持つ洗練された手段を用いた、ある存在によるゾーン（システム内領域）と導管のセグメンテーションの意図的な迂回を防止する。
SL 4	拡張されたリソース、IACS特有のスキル、および高いモチベーションを持つ洗練された手段を用いた、ある存在によるゾーン（システム内領域）と導管のセグメンテーションの意図的な迂回を防止する。

FR：5　制限されたデータフロー

システム要件（SR）	セキュリティレベル			
	SL1	SL2	SL3	SL4
SR 5.1：ネットワークのセグメント化	○			
SR5.1(1)：（拡張要件）物理的なネットワークのセグメント化		○	○	○
SR5.1(2)：（拡張要件）非制御系ネットワークからの独立性			○	○
SR5.1(3)：（拡張要件）重要なネットワークの論理的・物理的分離				○
SR 5.2：ゾーン（システム内領域）境界の保護	○			
SR5.2(1)：（拡張要件）すべてを拒否し、例外的に許可		○	○	○
SR5.2(2)：（拡張要件）アイランド（孤立）モード			○	○
SR5.2(3)：（拡張要件）フェイルクローズ（故障の際は、完全に停止かつネットワーク遮断）			○	○

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

FR：5　制限されたデータフロー	システム要件（SR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
	SR 5.3：汎用的な個人間通信制限	○	○		
	SR5.3(1)：（拡張要件）すべての汎用的な個人間通信の禁止			○	○
	SR 5.4：アプリケーションの分割		○	○	○

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

FR：6　イベントへのタイムリーな対応で求められるセキュリティレベル

SL1	IACSの構成要素の動作を監視し、インシデントに対応する。
SL 2	IACSの構成要素の運用状況を監視し、インシデント発見時には、積極的に証拠を収集し、定期的に報告することにより、インシデントへの対応を行う。
SL 3	IACSの構成要素の運用状況を監視し、インシデント発見時には、積極的に詳細な証拠を収集し、適切な当局に報告することにより、インシデントへの対応を行う。
SL 4	IACSの構成要素の運用状況を監視し、インシデント発見時には、積極的に詳細な証拠を収集し、適切な当局に報告することにより、ほぼリアルタイムでインシデントへの対応を行う。

FR：6　イベントへのタイムリーな対応	システム要件（SR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
	SR 6.1：監査ログへのアクセス性	○	○		
	SR6.1(1)：（拡張要件）プログラムによる監査ログへのアクセス			○	○
	SR 6.2：継続的なモニタリング		○	○	○

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

FR：7　リソース可用性で求められるセキュリティレベル

SL1	制御システムが通常の生産条件の下で確実に動作することを保証し、ある存在の偶発的または偶然の行動によって引き起こされるサービス停止を防止する。
SL 2	制御システムが通常の生産条件の下で確実に動作することを保証し、低リソース、一般的なスキル、およびモチベーションの低い単純な手段を用いたある存在によるサービス停止を防止する。
SL 3	制御システムが通常の生産条件の下で確実に動作することを保証し、適度なリソース、IACS特有のスキル、および適度なモチベーションを持つ洗練された手段を用いたある存在によるサービス停止を防止する。
SL 4	制御システムが通常の生産条件の下で確実に動作することを保証し、拡張されたリソース、IACS特有のスキル、および高いモチベーションを持つ洗練された手段を用いたある存在によるサービス停止を防止する。

FR：7　リソース可用性

システム要件（SR）	セキュリティレベル			
	SL1	SL2	SL3	SL4
SR 7.1：サービス停止からの保護	○			
SR7.1(1)：（拡張要件）通信負荷の管理		○	○	○
SR7.1(2)：（拡張要件）他のシステムやネットワークへのDoSの影響を制限			○	○
SR 7.2：リソース管理	○	○	○	○
SR 7.3：制御システムのバックアップ	○			
SR7.3(1)：（拡張要件）バックアップの検証		○	○	○
SR7.3(2)：（拡張要件）バックアップの自動化			○	○

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

	システム要件（SR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
FR：7 リソース可用性	SR 7.4：制御システムの復旧・再構築	○	○	○	○
	SR 7.5：非常用電源	○	○	○	○
	SR 7.6：ネットワークとセキュリティの設定	○	○		
	SR7.6(1)：（拡張要件）現在のセキュリティ設定のうち、機械で読み取り可能なレポート			○	○
	SR 7.7：最小限の機能	○	○	○	○
	SR 7.8：制御システムのコンポーネント在庫		○	○	○

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

拡張要件がない記載例（１/２ページ程度）　SR 1.4：管理の識別

FR：1　識別と認証制御	SR 1.4：管理の識別	観点	内容
		要件	制御システムは、ユーザ、グループ、役割、または制御システムのインタフェースによる識別子の管理をサポートする機能を提供しなければならない。
		根拠と補足ガイダンス	識別子は、特定の制御システム制御ドメインまたはゾーン内でエンティティに実行を許可する権限とは区別される(6.3, SR 2.1を参照)。人間のユーザが単一のグループとして機能する場合（制御室のオペレータなど）、ユーザ識別は、役割ベース、グループベース、またはデバイスベースであってもよい。いくつかの制御システムでは、オペレータとの即時対話のための機能が重要である。制御システムの局所的な緊急アクションが、識別要件によって妨げられるべきではない。これらのシステムへのアクセスは、適切な代償措置によって制限されてもよい。識別子は、制御システムの一部に要求されることがあるが、必ずしも制御システム全体に要求されるわけではない。例えば、無線デバイスは一般的に識別子を必要とするが、有線デバイスはそうでない場合もある。識別子の管理は、IEC 62443-2-1 に準拠して確立されたローカルポリシーと手順によって決定されます。
		拡張要件	なし。
		セキュリティレベル	SR 1.4：管理の識別はSL1～SL4に適応する。

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

拡張要件がある記載例（２ページ程度）　SR 2.1：認証の実施

FR：2 利用制御 / SR 2.1：認証の実施	観点	内容
	要件	制御システムは、ユーザ、グループ、役割、または制御システムのインタフェースによる識別子の管理をサポートする機能を提供しなければならない。
	根拠と補足ガイダンス	利用制御ポリシー（例えば、アイデンティティベースのポリシー、ロールベースのポリシー、ルールベースのポリシー）と、関連する読み書きアクセス強制メカニズム（例えば、アクセス制御リスト、アクセス制御マトリクス、暗号化）は、ユーザ（人間、ソフトウェアプロセス、デバイス）と資産（例えば、デバイス、ファイル、レコード、ソフトウェアプロセス、プログラム、ドメイン）との間の利用を制御するために採用される。制御システムがユーザ（人間、ソフトウェアプロセスまたはデバイス）の身元を確認した後、要求された操作が、定義されたセキュリティポリシーと手順に従って実際に許可されているかどうかを確認しなければならない。例えば、ロールベースのアクセス制御ポリシーでは、制御システムは、検証されたユーザやアセットにどのロールが割り当てられているか、また、どの権限がこれらのロールに割り当てられているかをチェックします。これにより、職務の分離と最小権限の執行が可能になります。使用法の施行機構は、制御システムの運用性能に悪影響を及ぼすことがあってはならない。制御システムのコンポーネントに対する計画的または計画外の変更は、制御システムの全体的なセキュリティに重大な影響を及ぼす可能性があります。したがって、アップグレードや変更を含む変更を開始する目的で、資格を持ち、権限を与えられた個人のみが、制御システムのコンポーネントの使用を得るべきである。
	拡張要件	（拡張要件1）すべてのユーザー（人間、ソフトウェアプロセス、デバイス）に権限付与：すべてのインタフェースにおいて、制御システムは、職務の分離と最小特権をサポートするために、制御システムの使用を制御するために、すべてのユーザ（人間、ソフトウェアプロセス、およびデバイス）に割り当てられた権限を強制する機能を提供しなければならない。
		（拡張要件2）認証の役割マッピング：管理システムは、権限を与えられたユーザまたはロールが、すべての人間のユーザのために、権限のロールへのマッピングを定義し、変更する機能を提供しなければならない。 注：ロールを固定された階層に限定しないことは、一般的に受け入れられているグッドプラクティスです。例えば、システム管理者は、一般的には必ずしもオペレータの権限を含むとは限りません。 注：この拡張要件は、ソフトウェアプロセスやデバイスにも適用されます。

IEC 62443-3-3：INTERNATIONAL STANDARD
Industrial communication networks – Network and system security –
Part 3-3: System security requirements and security levels

拡張要件がある記載例（２ページ程度）　SR 2.1：認証の実施

FR：2 利用制御	SR 2.1：認証の実施	観点	内容
		拡張要件 （つづき）	（拡張要件3）監督者の変更：制御システムは、構成可能な時間またはイベントシーケンスのために、現在の人間のユーザ権限のスーパバイザ ーの手動オーバーライドをサポートしなければならない。 注：緊急事態やその他の深刻なイベントが発生した場合には、自動化されたメカニズムの制御され、監査された、手動によるオーバーライドの実装が必要になることが多い。これにより、スーパーバイザは、現在のセッションを閉じて、より高い特権を持つ人間のユーザーとして新しいセッションを確立することなく、オペレータが異常な状態に迅速に対応できるようになります。
			（拡張要件4）二重認証：制御システムは、産業プロセスに重大な影響を及ぼす可能性がある場合には、二重承認をサポートしなければならない。 注：二重承認を、信頼性が高く正確に実行されるという非常に高いレベルの信頼性を必要とする行為に限定することは、一般的に受け入れられているグッドプラクティスである。二重承認を要求することは、正しい行動の失敗から生じる結果の深刻さを強調することになる。二重承認が要求される状況の例としては、重要な工業プロセスの設定点の変更がある。例えば、工業プロセスの緊急停止など、HSEの結果を保護するために即時対応が必要な場合には、二重承認メカニズムを使用しないことは、一般的に受け入れられているグッドプラクティスである。
		セキュリティレベル	SR 1.4：認証の実施はSL1に適応する。 SR 1.4 拡張要件1：認証の実施はSL2～SL4に適応する。 SR 1.4 拡張要件2：認証の実施はSL2～SL4に適応する。 SR 1.4 拡張要件3：認証の実施はSL3～SL4に適応する。 SR 1.4 拡張要件4：認証の実施はSL4に適応する。

【参考】IEC 62443-4-1：INTERNATIONAL STANDARD

IEC 62443-4-1：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-1: Secure product development lifecycle requirements

- コンポーネントの開発要件を規定した国際標準。
- セキュアなコンポーネントを開発するための要件を規定しており、IACSコンポーネントベンダのセキュリティ開発プロセスをベースにしている。
- ソフトウェア開発プロセスを８つの実践分野に分けて、それぞれのセキュリティに関する要求事項を記載。

Practice 1	セキュリティマネジメント（SM）
Practice 2	セキュリティ要求仕様（SR）
Practice 3	セキュリティ設計（SD）
Practice 4	セキュリティ実装（SI）
Practice 5	セキュリティ検証・妥当性評価（SVV）
Practice 6	セキュリティ課題管理（DM）
Practice 7	セキュリティアップデート管理（SUM）
Practice 8	セキュリティガイドライン（SG）

IEC 62443-4-1：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

Practice 1 セキュリティマネジメント（SM）	SM-1：開発プロセス	• 一般的な製品開発/保守/サポートプロセスは、一般的に受け入れられている製品開発プロセスと一貫性をもって統合・文書化され、実施されること
	SM-2：責任の所在の明確化	• 本文書で要求される各プロセスの組織的な役割と責任者を特定するプロセスを採用すること
	SM-3：適用性の識別	• 本文書が適用される製品（または製品の一部）を識別するためのプロセスを採用すること
	SM-4：セキュリティの専門知識	• 「SM-2：責任の所在の明確化」で規定された組織的な役割と義務に割り当てられた要員が、そのプロセスに適したセキュリ ティの専門知識を実証していることを確実にするために、セキュリティ教育と評価プログラムを特定し、提供するためのプロセスを採用すること
	SM-5：プロセスのスコーピング	• 文書化されたセキュリティ分析による正当化を含むプロセスを採用すること • プロジェクトの本文書への準拠レベルをスコープ化するための正当化は、適切なセキュリティ専門知識を持つ担当者によるレビューと承認を受けること
	SM-6：ファイルの完全性	• 製品に含まれるすべてのスクリプト、実行可能ファイル、その他の重要なファイルの完全性検証メカニズムを提供するためのプロセスを採用すること
	SM-7：開発環境のセキュリティ	• 開発、生産、引渡しの間、製品を保護するために、手順的及び技術的な管理を含むプロセスを採用すること。設計、実装、テスト、リリースの間の製品または製品の更新（パッチ）を保護することを含む
	SM-8：秘密鍵の管理	• サプライヤーは、コード署名に使用される秘密鍵を不正なアクセスや変更から保護するために、手続き上および技術上の管理を行うこと
	SM-9：外部提供コンポーネントのセキュリティ要件	• 製品内で使用されるすべての外部提供コンポーネントのセキュリティリスクを特定し、管理するためのプロセスを採用すること

IEC 62443-4-1：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

Practice 1 セキュリティマネジメント（SM）	SM-10：サードパーティのサプライヤからカスタム開発された部品	• サードパーティからの部品の製品開発ライフサイクルプロセスが、以下の基準を満たしている場合、本文書で使用する要求事項に適合していることを確実にするためのプロセスを採用すること
		  • その部品は、特定の目的のため、単一のサプライヤーのために特別に開発されている
		  • その部品は、セキュリティに影響を与えることができる

	SM-11：セキュリティ関連の問題の評価と対処	• 製品やパッチが、そのセキュリティ関連の問題が対処され、回復するまでリリースされないことを検証するためのプロセスを採用すること
	SM-12：プロセスの検証	• 製品リリースに先立ち、「SM-5：プロセスのスコーピング」で要求されるすべての適用可能なセキュリティ関連プロセスが完了したことを検証するためのプロセスを採用し、各プロセスの完了を記録すること
	SM-13：継続的な改善	• セキュリティ開発ライフサイクルを継続的に改善するためのプロセスを採用すること。このプロセスには、現場に流出したコンポーネント/サブシステム/システム技術のセキュリティ欠陥の分析を含む

IEC 62443-4-1：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

Practice 2 セキュリティ要求仕様（SR）	SR-1：製品のセキュリティ状況	• 意図した製品のセキュリティ状況が文書化されていることを確実にするためのプロセスを採用
	SR-2：脅威モデル	• すべての製品が、製品の現在の開発範囲に固有の脅威モデルを持つことを確実にするためのプロセスを採用すること
	SR-3：製品のセキュリティ要件	• 開発中の製品／機能のセキュリティ要件が文書化されていることを確実にするためのプロセスを採用すること。これには、設置、運用、保守、廃止措置に関連するセキュリティ機能の要件も含む
	SR-4：製品のセキュリティ要件の内容	• セキュリティ要求事項に十分な相曽が含まれていることを確実にするためのプロセスを採用すること
	SR-5：セキュリティ要件の見直し	• 明確性、妥当性、脅威モデルとの整合性、検証能力を確保するために、セキュリティ要件を見直し、必要に応じて更新し、承認するためのプロセスを採用すること。このプロセスには、代表的な各部門が参加するものとし、監督者は独立していること

IEC 62443-4-1：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-1: Secure product development lifecycle requirements

Practice 3 セキュリティ設計（SD）	SD-1：セキュリティ設計の原則	• 物理的および論理的インタフェースを含む製品の各インタフェースを識別し、特徴づけるセキュア設計を開発し、文書化するためのプロセスを採用すること
	SD-2：複数の層からなる設計の防御	• 脅威モデルに基づくリスクベースのアプローチを用いて、複数の層のフェンスを実装するためのプロセスを採用すること。防御の各層に責任を割り当てるためのプロセスを採用すること
	SD-3：セキュリティ設計の見直し	• 設計レビューを実施するためのプロセスを採用し、安全性が確保されていることの各重要な改訂に関連するセキュリ ティ関連の問題を特定し、特徴づけ、回復まで追跡すること
	SD-4：セキュリティ設計のベストプラクティス	• 安全な設計のベストプラクティスが文書化され、設計プロセスに適用されることを確実にするための プロセスを採用すること。これらの慣行は定期的に見直され、更新されること

Practice 4 セキュリティ実装（SI）	SI-1：セキュリティ導入レビュー	• 実施レビューを確実に実施するためのプロセスを採用し、安全設計の実施に関連するセキュリティ関連の問題を特定し、特徴付けし、回復まで追跡すること
	SI-2：安全なコーディングの標準	• 実施プロセスには、定期的に見直し・更新されるセキュリティコーディング基準を取り入れること

IEC 62443-4-1：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

Practice 5 セキュリティ検証・妥当性評価（SVV）	SVV-1：セキュリティ要件テスト	• 製品のセキュリティ機能がセキュリティ要求事項を満たしていること、エラーシナリオや無効入力を正しく処理していることを検証するプロセスを採用すること
	SVV-2：脅威の軽減テスト	• 脅威モデルで特定され、検証された脅威に対する緩和の有効性をテストするプロセスを採用すること
	SVV-3：脆弱性テスト	• 製品の潜在的なセキュリティ脆弱性を特定し、特性化することに焦点を当てたテストを実施するためのプロセスを採用すること。既知の脆弱性テストは、少なくとも、既知の脆弱性に関する確立された、業界で認知された、公開されたソースの最近の内容に基づくものとする
	SVV-4：侵入テスト	• 製品のセキュリティ脆弱性の発見と活用に焦点を当てたテストを通じて、セキュリティ関連の問題を特定し、特性化するためのプロセスを採用すること
	SVV-5：独立した監督者	• テストを実施する監督者が、製品を設計・実装した開発者から独立していることを保証するためのプロセスを採用すること

IEC 62443-4-1：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

Practice 6 セキュリティ課題管理（DM）	DM-1：セキュリティ関連問題の通知を受信	• 内部及び外部の情報源から報告された製品のセキュリティ関連の問題を受領し、回復まで追跡するためのプロセスが存在すること
	DM-2：セキュリティ関連問題の見直し	• 報告されたセキュリティ関連の問題が適時に調査され、判断するためのプロセスが存在すること
	DM-3：セキュリティ関連の問題の評価	• 製品のセキュリティ関連の問題を分析するためのプロセスを採用すること
	DM-4：セキュリティ関連の問題への対応	• セキュリティ関連の問題に対処し、影響評価の結果に基づいて報告するかどうかを決定するためのプロセスを採用すること。サプライヤーは、各問題に対処する適切な方法を決定する際に適用される、許容可能な残留リスクレベルを設定すること
	DM-5：セキュリティ関連事項の開示	• サポート対象製品における報告可能なセキュリティ関連の問題について、タイムリーに製品ユーザに通知するためのプロセスを採用すること
	DM-6：セキュリティ欠陥管理の実践の定期的な見直し	• セキュリティ関連の課題管理プロセスの定期的なレビューを実施するためのプロセスを採用すること。管理プロセスが完全で、効率的で、問題解決につながったかどうかを判断すること。各セキュリティ関連問題の管理を定期的に見直します。セキュリティ関連問題の管理の定期的な見直しのプロセスを少なくとも年1回実施すること

IEC 62443-4-1：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-1: Secure product development lifecycle requirements

Practice 7 セキュリティアップデート管理（SUM）	SUM-1：セキュリティ更新資格	• 確認のためのプロセスを採用すること
	SUM-2：セキュリティ更新のドキュメント	• 製品のセキュリティ更新に関する文書が、製品ユーザーが利用できるようにするためのプロセスを採用すること
	SUM-3：依存するコンポーネントまたはオペレーティングシステムのセキュリティ更新	• 依存するコンポーネントまたはオペレーティングシステムのセキュリティ更新に関する文書が、製品ユーザーが利用できるようにするためのプロセスを採用すること
	SUM-4：セキュリティアップデート配信	• すべてのサポート対象製品および製品バージョンのセキュリティアップデートが、セキュリティパッチが本物であることの検証を容易にする方法で、製品ユーザが利用できるようにするためのプロセスを採用すること
	SUM-5：セキュリティパッチのタイムリーな配信	• 製品ユーザへのセキュリティ更新プログラムの提供と確認の時間枠を指定するポリシーを定義し、このポリシーの遵守を確実にするためのプロセスを採用すること

IEC 62443-4-1：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

Practice 8 セキュリティガイドライン（SG）	SG-1：製品防御の深さ	• インストール、運用、保守をサポートするための製品のセキュリティ防御の深層戦略を記述した製品ユーザー文書を作成するためのプロセスが存在すること
	SG-2：環境で期待される深層防御対策	• 製品が使用される外部環境によって提供されることが期待されるセキュリティ防御の深層対策を記述した製品ユーザ文書を作成するプロセスを採用すること
	SG-3：セキュリティ強化ガイドライン	• 製品のインストールおよび保守時に製品を硬化させるためのガイドラインを含む製品ユーザー文書を作成するためのプロセスを採用すること
	SG-4：確実な廃棄ガイドライン	• 製品の使用を中止するためのガイドラインを含む製品ユーザー文書を作成するためのプロセスを採用すること
	SG-5：安全な運用のためのガイドライン	• 製品をユーザーが安心して利用するための製品ユーザー文書を作成するためのプロセスを採用すること
	SG-6：アカウント管理ガイドライン	• 製品の使用に関連したユーザーアカウントの要件と推奨事項を定義する製品ユーザー文書を作成するためのプロセスを採用すること
	SG-7：ドキュメントのレビュー	• セキュリティガイドラインを含むすべてのユーザーマニュアルに含まれるエラーや漏れを特定し、特徴づけ、回復まで追跡するためのプロセスを採用すること

IEC 62443-4-1：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

一般的な記載例（1 / 4 ページ～ 1 / 2 ページ程度）　SM-1：開発プロセス

セキュリティマネジメント（SM）	SM-1：開発プロセス	観点	内容
		要件	一般的な製品開発/保守/サポートプロセスは、一般的に受け入れられている製品開発プロセスと一貫性をもって統合・文書化され、実施されることとする。以下のプロセスを含みますが、これらに限定されるものではありません。 • a) 変更管理と監査ロギングを伴う構成管理。 • b) 要件トレーサビリティを伴う製品記述及び要件定義 • c) モジュラー設計などのソフトウェア又はハードウェアの設計及び実装方法 • d) 再現可能なテストの検証及び検証プロセス • e) すべての開発プロセス記録のレビューと承認 • f) ライフサイクルサポート
		根拠と補足ガイダンス	このプロセスは、製品供給者が、本文書で規定された要件をサポートするために拡張可能な、十分に定義された実証済みの製品開発プロセスを確実に実施していることを確認するために必要である。本文書で定義された要求されるプロセスは、成熟した製品開発ライフサイクルが存在することを前提としている。セキュアな製品開発ライフサイクルは、これらのプロセスなしには効果的ではなく、また、これらのプロセスが存在することに依存している。一般に受け入れられている製品開発プロセスの例としては、ISO 9001及びISO/IEC 27034に準拠したプロセスがある。このプロセスを持つということは、製品サプライヤが製品開発のライフサイクルの中で、構成管理、要件定義、設計、実装、および試験を最低限サポートする技術を使用していることを意味する。

IEC 62443-4-1：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-1: Secure product development lifecycle requirements

最も詳細な記載例（１ページ半程度）　SD-1：セキュリティ設計の原則

セキュリティ設計（SD）

SD-1：セキュリティ設計の原則

観点	内容
要件	物理的および論理的インタフェースを含む製品の各インタフェースを識別し、特徴づけるセキュア設計を開発し、 文書化するためのプロセスを採用しなければならない。 • a) インタフェースが外部から（他の製品から）アクセス可能であるか、内部から（製品の他の構成要素から）アクセス可能であるか、またはその両方であるかを示すこと • b) 外部インタフェースに対する製品セキュリティコンテキスト（第6項参照）のセキュリティ上の意味合い • c) インタフェースの潜在的な利用者及びそれを介してアクセス可能な資産（直接的又は間接的） • d) インタフェースへのアクセスが信頼の境界を越えるかどうかの判断 • e) 該当する脅威を含む、製品セキュリティコンテキスト内でのインターフェイスの使用に関連するセキュリ ティ上の考慮事項、前提条件及び／又は制約 • f) インタフェースを使用し、上記 c)で定義された資産にアクセスするために必要な、セキュリティ上の役割、特権／権利及びアクセス制御許可 • g) 入力の検証、出力及びエラー処理を含む、インターフェース及び上記 c)に定義された資産を保護するために使用されるセキュリティ能力及び／又は補償メカニズム • h) インタフェースを実装するためのサードパーティ製品の使用及びそのセキュリティ能力 • i) インタフェースが外部からアクセス可能な場合のインタフェースの使用方法を記述した文書 • j) 設計が脅威モデルで特定された脅威をどのように緩和するかの記述
根拠と補足ガイダンス	このプロセスは、資産へのアクセスのためのセキュリティが、攻撃を仕掛けられる製品の外部インターフェイスと内部インターフェイスの観点から総合的に対処されることを保証するために必要です。このプロセスを持つということは、製品のインタフェースを識別し、その上で行われる相互作用（例えば、データや制御フロー）、それらを保護するために設計されたセキュリティメカニズム、および適切に保護されていない場合に危殆化する可能性のある資産によって特徴付けられることを意味します。インターフェイスには、ネットワーク（イーサネットなど）やデバイス（キーボード、モニター、USB/コンパクトディスク[CD]/デジタル多目的ディスク[DVD]メディアなど）への物理的および無線接続が含まれます。論理インターフェースは、製品コンポーネント間のデータ制御フロー（例えば、アプリケーションメッセージング）をサポートし、アプリケーションプログラミングインターフェース（例えば、構造化クエリ言語[SQL]）や通信プロトコル（例えば、送信制御プロトコル[TCP]）などのメカニズムを含みます。保護メカニズムには、一般的なハードニング機能（例えば、セキュリティポリシー設定）、ユーザアクセス制御（例えば、アカウント管理）、およびセキュリティイベントの検出と報告などが含まれます。製品セキュリティコンテキストが提供する設定内でインタフェースを表示することで、製品セキュリティコンテキストが提供する保護と、それに起因する脆弱性（例えば、攻撃を受ける可能性のある場所）の両方を含む、製品が動作することが期待される特定の環境に焦点を当てることができるようになります。設計の内部構成要素については、製品セキュリティコンテキストの概念は、周囲の製品構成要素によって提供されるセキュリティコンテキストを含むように拡張される。例えば、産業用制御システム製品の一部であるワークステーション上で実行されるアプリケーションプログラムの製品セキュリティコンテキストには、ワークステーションが接続するネットワークと、アプリケーションが実行されるワークステーションのソフトウェア環境が含まれます。

IEC 62443-4-1：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

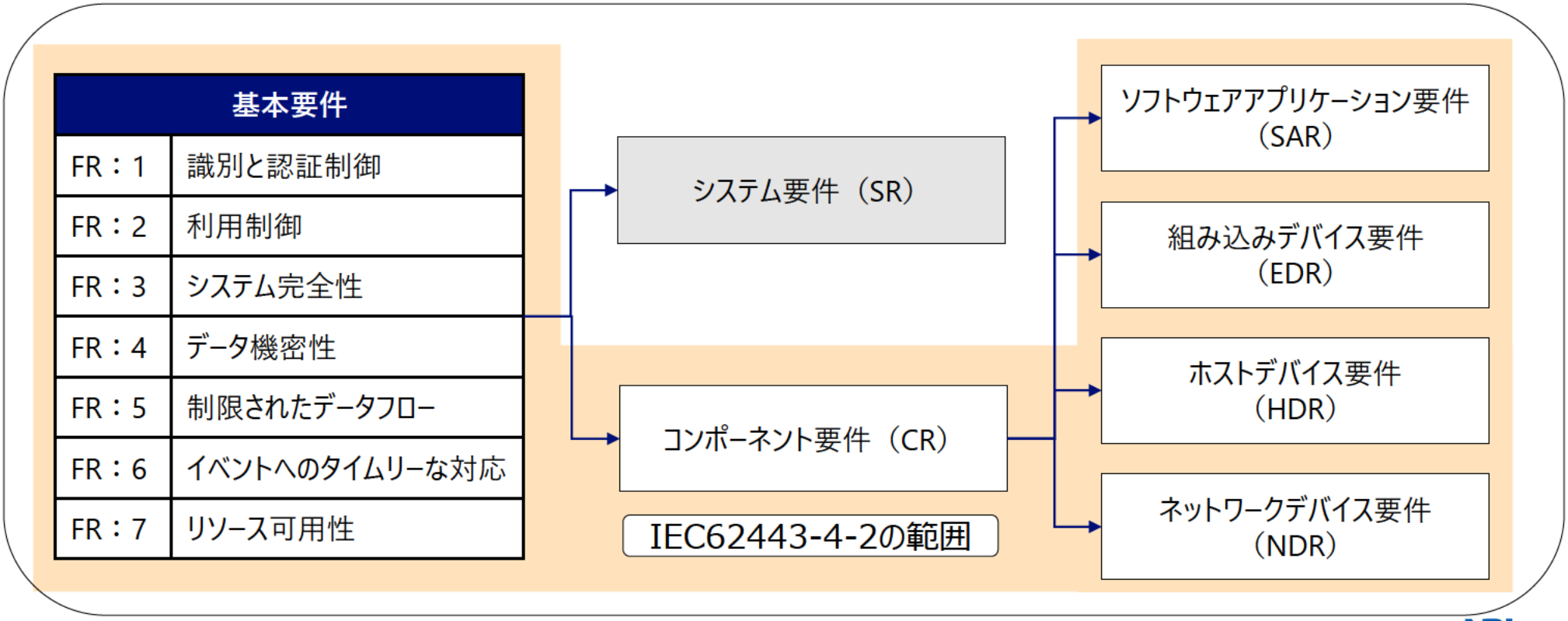
最も詳細な記載例（１ページ半程度）　SD-1：セキュリティ設計の原則

セキュリティ設計（SD）	SD-1：セキュリティ設計の原則	観点	内容
		根拠と補足ガイダンス（つづき）	インターフェースに関連する脅威、ユーザー、資産、信頼境界を特定することは、誰がインターフェースを使用することが予想されるかを特定し、脅威や未知の主体がインターフェースやそれを介してアクセス可能な資産にアクセスできる可能性がある場所を示すことになります。これにより、インターフェイスの数を可能な限り削減し、残りのインターフェイスとそれを介してアクセス可能な資産に適切なセーフガードを提供することが可能となる。信頼境界を特定することは、将来のゾーンと導管の定義をサポートする（IEC 62443-3-2を参照）ため、製品のセキュリティアーキテクチャの定義における主要な要素となる。サンプルのデータ資産（リソース）には、以下のものが含まれる。 • a) データベースとデータベーステーブル • b) 設定ファイル • c) 暗号鍵ストア • d) アクセス制御リスト（ACL） • e) レジストリキー • f) Web ページ (静的および動的) • g) 監査ログ • h) ネットワークソケット/ネットワークメディア • i) プロセス間通信(IPC)、サービスおよびリモートプロシージャコール(RPC)リソース • j) その他のファイルおよびディレクトリ • k) その他のメモリリソース 製品のセキュリティ要件、製品のセキュリティコンテキスト及び信頼境界の考慮事項の分析に基づいて、インターフェイスの設計を開発することができ、そのインターフェイスを使用するために必要なユーザの役割、特権及び承認／アクセス許可の定義と、追加のセーフガードを提供する特定のセキュリティ機能（例えば、認証、暗号化及びロギング）を含むインターフェイスのための設計を開発することができる。深層防御戦略の設計の一部として、補償メカニズム及びサードパーティのハードウェア又はソフトウェアコン ポーネントの予想される使用は、深層防御戦略の妥当性の評価に役立つ。最後に、外部からアクセス可能なインタフェースを使用するための文書を準備することで（例えば、ユーザや第三者により）、誤って使用される可能性を減らすことができます。

【参考】IEC 62443-4-2：INTERNATIONAL STANDARD

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

- コンポーネントのセキュリティ要件を規定した国際標準。
- デバイスに搭載されるセキュリティ機能を規定。ISA Secure のEDSA（FSA）をベースにしており、セキュリティ機能の実装評価に関する要求事項を記載。
- IEC62443-3-3の要件をベースに、各種コンポーネントに合わせて最適化を目指す。



IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

FR：1　識別と認証制御で求められるセキュリティレベル

SL1	認証されていない存在による偶発的または偶然のアクセスから保護するメカニズムにより、すべてのユーザー（人間、ソフトウェアプロセス、およびデバイス）を識別し、認証する。
SL 2	低リソース、一般的なスキル、およびモチベーションの低い単純な手段を用いた、ある存在による意図的な認証されていないアクセスから保護するメカニズムにより、すべてのユーザ（人間、ソフトウェアプロセス、およびデバイス）を識別し、認証する。
SL 3	適度なリソース、IACS特有のスキル、および適度なモチベーションを持つ洗練された手段を用いた、ある存在による意図的な認証されていないアクセスから保護するメカニズムにより、すべてのユーザー（人間、ソフトウェアプロセス、およびデバイス）を識別し、認証する。
SL 4	拡張されたリソース、IACS特有のスキル、および高いモチベーションを持つ洗練された手段を用いた、ある存在による意図的な認証されていないアクセスから保護するメカニズムによって、すべてのユーザー（人間、ソフトウェアプロセス、およびデバイス）を識別し、認証する。

FR：1　識別と認証制御

コンポーネント要件（CR）	セキュリティレベル			
	SL1	SL2	SL3	SL4
CR 1.1：人間のユーザー識別と認証	○			
CR1.1(1)：（拡張要件）固有の識別および認証		○	○	○
CR1.1(2)：（拡張要件）全インターフェースでの多要素認証			○	○
CR 1.2：ソフトウェアプロセスとデバイスの識別と認証		○		
CR1.2(1)：（拡張要件）固有の識別および認証			○	○
CR 1.3：アカウント管理	○	○	○	○
CR 1.4：管理の識別	○	○	○	○

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

FR：1 識別と認証制御

コンポーネント要件（CR）	セキュリティレベル			
	SL1	SL2	SL3	SL4
CR 1.5：認証機能の管理	○	○		
CR1.5(1)：（拡張要件）認証機器のハードウェアセキュリティ			○	○
CR 1.6：無線アクセス管理 （ネットワークコンポーネント固有の要件であり、ネットワークデバイス要件（NDR）に記載）				
CR 1.7：パスワードベースの認証の強度	○	○		
CR1.7(1)：（拡張要件）人間のユーザーのパスワード生成と有効期限の制限			○	
CR1.7(2)：（拡張要件）すべてのユーザ（人間、ソフトウェアプロセス、またはデバイス）のパスワードの有効期限の制限			○	○
CR1.8：公開鍵の基盤証明書		○	○	○
CR1.9：公開鍵ベースの認証の強度		○		
CR1.9(1)：（拡張要件）公開鍵ベース認証のためのハードウェアセキュリティ			○	○
CR1.10：認証機能のフィードバック	○	○	○	○
CR1.11：ログインに失敗した試行	○	○	○	○
CR1.12：システム利用通知	○	○	○	○
CR 1.13：信頼されていないネットワーク経由でのアクセス （ネットワークコンポーネント固有の要件であり、ネットワークデバイス要件（NDR）に記載）				

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

FR：1 識別と認証制御	コンポーネント要件（CR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
	CR 1.14：対象鍵ベースの認証の強度		○		
	CR1.14(1)：（拡張要件）対象鍵ベース認証のためのハードウェアセキュリティ			○	○

IEC 62443-4-2：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components

FR：2　利用制御で求められるセキュリティレベル

SL1	特定の権限に従ってIACSの使用を制限し、偶発的または偶然の誤用から保護する。
SL 2	低リソース、一般的なスキル、およびモチベーションの低い単純な手段を用いた、ある存在による迂回行為から保護するために、指定された特権に従ってIACSを使用することを制限する。
SL 3	適度なリソース、IACS特有のスキル、および適度なモチベーションを持つ洗練された手段を用いた、ある存在による迂回行為から保護するために、指定された特権に従ってIACSを使用することを制限する。
SL 4	拡張されたリソース、IACS特有のスキル、および高いモチベーションを持つ洗練された手段を用いた、ある存在による迂回行為から保護するために、指定された特権に従ってIACSを使用することを制限する。

	コンポーネント要件（CR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
FR：2　利用制御	CR 2.1：認証の実施	○			
	CR2.1(1)：（拡張要件）すべてのユーザー（人間、ソフトウェアプロセス、デバイス）に権限付与		○	○	○
	CR2.1(2)：（拡張要件）認証の役割マッピング		○	○	○
	CR2.1(3)：（拡張要件）監督者の変更			○	○
	CR2.1(4)：（拡張要件）二重認証				○
	CR 2.2：無線利用制御	○	○	○	○
	CR 2.3：携帯機器やモバイル機器の利用制御（コンポーネントレベルの要件はなし）				

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

	コンポーネント要件（CR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
FR：2 利用制御	CR 2.4：モバイルコード （コンポーネント固有の要件であり、ソフトウェアアプリケーション要件（SAR）、組み込みデバイス要件（EDR）、ホストデバイス要件（HDR）、ネットワークデバイス要件（NDR）にそれぞれ記載）				
	CR 2.5：セッションロック	○	○	○	○
	CR 2.6：リモートセッションの終了		○	○	○
	CR 2.7：同時進行セッションの制御			○	○
	CR 2.8：監査対象のイベント	○	○	○	○
	CR 2.9：監査の記憶容量	○	○		
	CR2.9(1)：（拡張要件）監査記録の保存容量が閾値に達した場合の警告			○	○
	CR 2.10：監査処理の不備への対応	○	○	○	○
	CR 2.11：タイムスタンプ	○			
	CR2.11(1)：（拡張要件）時刻同期		○	○	○
	CR2.11(2)：（拡張要件）時間源の完全性の保護				○

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

FR：2 利用制御	コンポーネント要件（CR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
	CR 2.12：否認防止	○	○	○	
	CR2.12(1)：（拡張要件）すべてのユーザーへの否認防止				○

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

FR：3　システム完全性で求められるセキュリティレベル

SL1	何気ない操作や偶然の操作からIACSの完全性を守る。
SL 2	低リソース、一般的なスキル、およびモチベーションの低い単純な手段を用いた者による操作からIACSの完全性を保護する。
SL 3	適度なリソース、IACS特有のスキル、および適度なモチベーションを持つ洗練された手段を用いた者による操作からIACSの完全性を保護する。
SL 4	拡張されたリソース、IACS特有のスキル、および高いモチベーションを持つ洗練された手段を用いた者による操作からIACSの完全性を保護する。

FR：3　システム完全性	コンポーネント要件（CR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
	CR 3.1：通信の完全性	○			
	CR3.1(1)：（拡張要件）通信の認証		○	○	○
	CR 3.2：悪意のあるコードからの保護 （コンポーネント固有の要件であり、ソフトウェアアプリケーション要件（SAR）、組み込みデバイス要件（EDR）、ホストデバイス要件（HDR）、ネットワークデバイス要件（NDR）にそれぞれ記載）				
	CR 3.3：セキュリティ機能の検証	○	○	○	
	CR3.3(1)：（拡張要件）通常運用時のセキュリティ機能の検証				○

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

FR：3　システム完全性

コンポーネント要件（CR）	セキュリティレベル			
	SL1	SL2	SL3	SL4
CR 3.4：ソフトウェアと情報の完全性	○			
CR3.4(1)：（拡張要件）ソフトウェアや情報の認証		○	○	○
CR3.4(2)：（拡張要件）完全性侵害の自動通知			○	○
CR 3.5：入力の検証	○	○	○	○
CR 3.6：決定的な出力	○	○	○	○
CR 3.7：エラー処理	○	○	○	○
CR 3.8：セッションの完全性		○	○	○
CR 3.9：監査情報の保護		○	○	
CR3.9(1)：（拡張要件）書き込みメディアの監査記録				○
CR 3.10：更新のサポート （コンポーネント固有の要件であり、ソフトウェアアプリケーション要件（SAR）、組み込みデバイス要件（EDR）、ホストデバイス要件（HDR）、ネットワークデバイス要件（NDR）にそれぞれ記載）				
CR 3.11：物理的な改ざんの検出 （コンポーネント固有の要件であり、ソフトウェアアプリケーション要件（SAR）、組み込みデバイス要件（EDR）、ホストデバイス要件（HDR）、ネットワークデバイス要件（NDR）にそれぞれ記載）				

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

	コンポーネント要件（CR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
FR：3 システム完全性	CR 3.12：信頼のため製品サプライヤーの情報等を提供 （コンポーネント固有の要件であり、ソフトウェアアプリケーション要件（SAR）、組み込みデバイス要件（EDR）、ホストデバイス要件（HDR）、ネットワークデバイス要件（NDR）にそれぞれ記載）				
	CR 3.13：資産保有者の情報等を提供 （コンポーネント固有の要件であり、ソフトウェアアプリケーション要件（SAR）、組み込みデバイス要件（EDR）、ホストデバイス要件（HDR）、ネットワークデバイス要件（NDR）にそれぞれ記載）				
	CR 3.14：ブート処理の完全性 （コンポーネント固有の要件であり、ソフトウェアアプリケーション要件（SAR）、組み込みデバイス要件（EDR）、ホストデバイス要件（HDR）、ネットワークデバイス要件（NDR）にそれぞれ記載）				

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

FR：4　データ機密性で求められるセキュリティレベル

SL1	盗聴や偶然の暴露による情報の不正な開示を防止する。
SL 2	低リソース、一般的なスキル、およびモチベーションの低い単純な手段を用いて、積極的に情報を探している存在への情報の不正な開示を防止する。
SL 3	適度なリソース、IACS特有のスキル、および適度なモチベーションを持つ洗練された手段を用いて、積極的に情報を探している存在への情報の不正な開示を防止する。
SL 4	拡張されたリソース、IACS特有のスキル、および高いモチベーションを持つ洗練された手段を用いて、積極的に情報を探している存在への情報の不正な開示を防止する。

FR：4　データ機密性

コンポーネント要件（CR）	セキュリティレベル			
	SL1	SL2	SL3	SL4
CR 4.1：情報の機密性	○	○	○	○
CR 4.2：情報の持続性		○		
CR4.2(1)：（拡張要件）共有メモリのリソースの消去			○	○
CR4.2(2)：（拡張要件）検証の消去			○	○
CR 4.3：暗号技術の利用	○	○	○	○

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

FR：5　制限されたデータフローで求められるセキュリティレベル

SL1	ゾーン（システム内領域）と導管のセグメンテーションの偶発的または偶然の迂回を防止する。
SL 2	低リソース、一般的なスキル、およびモチベーションの低い単純な手段を用いた、ある存在によるゾーン（システム内領域）と導管のセグメンテーションの意図的な迂回を防止する。
SL 3	適度なリソース、IACS特有のスキル、および適度なモチベーションを持つ洗練された手段を用いた、ある存在によるゾーン（システム内領域）と導管のセグメンテーションの意図的な迂回を防止する。
SL 4	拡張されたリソース、IACS特有のスキル、および高いモチベーションを持つ洗練された手段を用いた、ある存在によるゾーン（システム内領域）と導管のセグメンテーションの意図的な迂回を防止する。

FR：5　制限されたデータフロー

コンポーネント要件（CR）	セキュリティレベル			
	SL1	SL2	SL3	SL4
CR 5.1：ネットワークのセグメント化	○	○	○	○
CR 5.2：ゾーン（システム内領域）境界の保護 （ネットワークコンポーネント固有の要件であり、ネットワークデバイス要件（NDR）に記載）				
CR 5.3：汎用的な個人間通信制限 （ネットワークコンポーネント固有の要件であり、ネットワークデバイス要件（NDR）に記載）				
CR 5.4：アプリケーションの分割 （コンポーネントレベルの要件はなし）				

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

FR：6　イベントへのタイムリーな対応で求められるセキュリティレベル

SL1	IACSの構成要素の動作を監視し、インシデントに対応する。
SL 2	IACSの構成要素の運用状況を監視し、インシデント発見時には、積極的に証拠を収集し、定期的に報告することにより、インシデントへの対応を行う。
SL 3	IACSの構成要素の運用状況を監視し、インシデント発見時には、積極的に詳細な証拠を収集し、適切な当局に報告することにより、インシデントへの対応を行う。
SL 4	IACSの構成要素の運用状況を監視し、インシデント発見時には、積極的に詳細な証拠を収集し、適切な当局に報告することにより、ほぼリアルタイムでインシデントへの対応を行う。

FR：6　イベントへのタイムリーな対応	コンポーネント要件（CR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
	CR 6.1：監査ログへのアクセス性	○	○		
	CR6.1(1)：（拡張要件）プログラムによる監査ログへのアクセス			○	○
	CR 6.2：継続的なモニタリング		○	○	○

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

FR：7　リソース可用性で求められるセキュリティレベル

SL1	コンポーネントが通常の生産条件の下で確実に動作することを保証し、ある存在の偶発的または偶然の行動によって引き起こされるサービス停止を防止する。
SL 2	コンポーネントが通常の生産条件の下で確実に動作することを保証し、低リソース、一般的なスキル、およびモチベーションの低い単純な手段を用いたある存在によるサービス停止を防止する。
SL 3	コンポーネントが通常の生産条件の下で確実に動作することを保証し、適度なリソース、IACS特有のスキル、および適度なモチベーションを持つ洗練された手段を用いたある存在によるサービス停止を防止する。
SL 4	コンポーネントが通常の生産条件の下で確実に動作することを保証し、拡張されたリソース、IACS特有のスキル、および高いモチベーションを持つ洗練された手段を用いたある存在によるサービス停止を防止する。

FR：7　リソース可用性

コンポーネント要件（CR）	セキュリティレベル			
	SL1	SL2	SL3	SL4
CR 7.1：サービス停止からの保護	○			
CR7.1(1)：（拡張要件）コンポーネントからの通信負荷の管理		○	○	○
CR 7.2：リソース管理	○	○	○	○
CR 7.3：制御システムのバックアップ	○			
CR7.3(1)：（拡張要件）バックアップの完全性の検証		○	○	○
CR 7.4：制御システムの復旧・再構築	○	○	○	○
CR 7.5：非常用電源 （コンポーネントレベルの要件はなし）				

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

FR：7 リソース可用性	コンポーネント要件（CR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
	CR 7.6：ネットワークとセキュリティの設定	○	○		
	CR7.6(1)：（拡張要件）現在のセキュリティ設定のうち、機械で読み取り可能なレポート			○	○
	CR 7.7：最小限の機能	○	○	○	○
	CR 7.8：制御システムのコンポーネント在庫		○	○	○
	CR7.3(1)：（拡張要件）バックアップの完全性の検証		○	○	○

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

	ソフトウェアアプリケーション要件（SAR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
FR：2	SAR 2.4：モバイルコード	○			
	SAR2.4(1)：（拡張要件）モバイルコードの認証チェック		○	○	○
FR：3	SAR 3.2：悪意のあるコードからの保護	○	○	○	○

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

	組み込みデバイス要件（EDR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
FR：2	EDR 2.4：モバイルコード	○			
	EDR2.4(1)：（拡張要件）モバイルコードの認証チェック		○	○	○
	EDR 2.13：物理的な診断およびテストインターフェースの使用		○		
	EDR2.13(1)：（拡張要件）アクティブなモニタリング			○	○
FR：3	EDR 3.2：悪意のあるコードからの保護	○	○	○	○
	EDR 3.10：更新のサポート	○			
	EDR3.10(1)：（拡張要件）信頼性と完全性の更新		○	○	○
	EDR 3.11：物理的な改ざんの検出		○		
	EDR3.11(1)：（拡張要件）改ざんが試行されたことの通知			○	○
	EDR 3.12：信頼のため製品サプライヤーの情報等を提供		○	○	○
	EDR 3.13：資産保有者の情報等を提供		○	○	○
	EDR 3.14：ブート処理の完全性	○			
	EDR3.14(1)：（拡張要件）ブートプロセスの認証		○	○	○

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

	ホストデバイス要件（HDR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
FR：2	HDR 2.4：モバイルコード	○			
	HDR2.4(1)：（拡張要件）モバイルコードの認証チェック		○	○	○
	HDR 2.13：物理的な診断およびテストインターフェースの使用		○		
	HDR2.13(1)：（拡張要件）アクティブなモニタリング			○	○
FR：3	HDR 3.2：悪意のあるコードからの保護	○			
	HDR3.2(1)：（拡張要件）コード保護の報告データ		○	○	○
	HDR 3.10：更新のサポート	○			
	HDR3.10(1)：（拡張要件）信頼性と完全性の更新		○	○	○
	HDR 3.11：物理的な改ざんの検出		○		
	HDR3.11(1)：（拡張要件）改ざんが試行されたことの通知			○	○
	HDR 3.12：信頼のため製品サプライヤーの情報等を提供		○	○	○
	HDR 3.13：資産保有者の情報等を提供		○	○	○
	HDR 3.14：ブート処理の完全性	○			
	HDR3.14(1)：（拡張要件）ブートプロセスの認証		○	○	○

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

	ネットワークデバイス要件（NDR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
FR：1	NDR 1.6：無線アクセス管理	○			
	NDR1.6(1)：（拡張要件）固有の識別と認証		○	○	○
	NDR 1.13：信頼されていないネットワーク経由でのアクセス	○	○		
	NDR1.13(1)：（拡張要件）明示的なアクセス要求の承認			○	○
FR：2	NDR 2.4：モバイルコード	○			
	NDR2.4(1)：（拡張要件）モバイルコードの認証チェック		○	○	○
	NDR 2.13：物理的な診断およびテストインターフェースの使用		○		
	NDR2.13(1)：（拡張要件）アクティブなモニタリング			○	○
FR：3	NDR 3.2：悪意のあるコードからの保護	○			
	NDR 3.10：更新のサポート	○			
	NDR3.10(1)：（拡張要件）信頼性と完全性の更新		○	○	○
	NDR 3.11：物理的な改ざんの検出		○		
	NDR3.11(1)：（拡張要件）改ざんが試行されたことの通知			○	○
	NDR 3.12：信頼のため製品サプライヤーの情報等を提供		○	○	○

IEC 62443-4-2：INTERNATIONAL STANDARD
Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components

	ネットワークデバイス要件（NDR）	セキュリティレベル			
		SL1	SL2	SL3	SL4
FR：3	NDR 3.13：資産保有者の情報等を提供		○	○	○
	NDR 3.14：ブート処理の完全性	○			
	NDR3.14(1)：（拡張要件）ブートプロセスの認証		○	○	○
FR：5	NDR 5.2：ゾーン（システム内領域）境界の保護	○			
	NDR5.2(1)：（拡張要件）すべてを拒否し、例外的に許可		○	○	○
	NDR5.2(2)：（拡張要件）アイランド（孤立）モード			○	○
	NDR5.2(3)：（拡張要件）フェイルクローズ（故障の際は、完全に停止かつネットワーク遮断）			○	○
	NDR 5.3：汎用的な個人間通信制限	○	○	○	○

IEC 62443-4-2：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components

拡張要件がない記載例（１/２ページ程度）　SR 1.3：アカウント管理

FR：1 識別と認証制御	SR 1.3：アカウント管理	観点	内容
		要件	コンポーネントは、IEC 62443-3-3-3 SR 1.3 に従って直接、又はアカウントを管理するシステムに統合して、すべてのアカウントの管理をサポートする能力を提供しなければならない。
		根拠と補足ガイダンス	コンポーネントは、上位レベルのアカウント管理システムに統合することで、この能力を提供することができる。ケイパビリティが上位レベルのアカウント管理システムに統合されていない場合は、コンポーネントはそのケイパビリティをネイティブに提供することが期待される。この要件を満たす一般的なアプローチは、IEC 62443-3-3 SR 1.3で要求されるアカウント管理能力を提供するディレクトリサーバー（LDAPやActive Directoryなど）に認証の評価を委譲するコンポーネントである。コンポーネントがアカウント管理機能を提供するために上位システムに統合する場合、上位システムの機能が利用できなくなった場合のコンポー ネントへの影響を考慮する必要がある。
		拡張要件	なし。
		セキュリティレベル	SR 1.3：アカウント管理はSL1～SL4に適応する。

IEC 62443-4-2：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components

拡張要件がある記載例（２ページ程度）　SR 2.1：認証の実施

FR：2 利用制御	SR 2.1：認証の実施	観点	内容
		要件	コンポーネントは、割り当てられた責任に基づいて、すべての識別され、認証されたユーザに対して、認可の実施メカニズムを提供しなければならない。
		根拠と補足ガイダンス	利用制御ポリシー（例えば、アイデンティティベースのポリシー、ロールベースのポリシー、ルールベースのポリシー）と、関連する読み書きアクセス強制メカニズム（例えば、アクセス制御リスト、アクセス制御マトリクス、暗号化）は、ユーザ（人間、ソフトウェアプロセス、デバイス）と資産（例えば、デバイス、ファイル、レコード、ソフトウェアプロセス、プログラム、ドメイン）との間の利用を制御するために採用される。制御システムがユーザ（人間、ソフトウェアプロセスまたはデバイス）の身元を確認した後、要求された操作が、定義されたセキュリティポリシーと手順に従って実際に許可されているかどうかを確認しなければならない。例えば、ロールベースのアクセス制御ポリシーでは、制御システムは、検証されたユーザやアセットにどのロールが割り当てられているか、また、どの権限がこれらのロールに割り当てられているかをチェックし、要求された操作が権限によってカバーされていれば実行され、そうでなければ拒否されます。また、どの権限がこれらのロールに割り当てられているかをチェックすることにより、、職務の分離と最小権限の執行が可能になります。使用法の施行機構は、制御システムの運用性能に悪影響を及ぼすことがあってはならない。制御システムのコンポーネントに対する計画的または計画外の変更は、制御システムの全体的なセキュリティに重大な影響を及ぼす可能性があります。したがって、アップグレードや変更を含む変更を開始する目的で、資格を持ち、権限を与えられた個人のみが、制御システムのコンポーネントの使用を得るべきである。
		拡張要件	（拡張要件1）すべてのユーザー（人間、ソフトウェアプロセス、デバイス）に権限付与：コンポーネントは、割り当てられた責任と最小の特権に基づいて、すべてのユーザに対して認可を実施する仕組みを提供しなければならない。
			（拡張要件2）認証の役割マッピング：コンポーネントは、直接または補償的なセキュリティメカニズムを介して、すべての人間のユーザのために権限のロールへのマッピングを定義し、変更するために、権限を与えられたロールを提供しなければならない。役割は、より高いレベルの役割が、より低い特権を持つ役割のスーパーセットである固定された入れ子の階層に限定されるべきではない。例えば、システム管理者は、必ずしもオペレータ権限を含むべきではありません。 注：この拡張要件は、ソフトウェアプロセスやデバイスにも適用可能である。

IEC 62443-4-2：INTERNATIONAL STANDARD Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components

拡張要件がある記載例（２ページ程度）　SR 2.1：認証の実施

FR：2 利用制御	SR 2.1：認証の実施	観点	内容
		拡張要件（つづき）	（拡張要件3）監督者の変更：コンポーネントは、構成可能な時間又は一連のイベントのための監督者の手動オーバーライドをサポートしなければならない。 注：緊急事態又はその他の重大な事象が発生した場合に、自動化されたメカニズムの制御され、監査された、及び手動によるオーバーライドを実装することにより、スーパバイザは、現在のセッションを閉じて、より高い特権を持つ人間のユーザとして新しいセッションを確立することなく、オペレータが異常な状態に迅速に対応できるようにすることができる。
			（拡張要件4）二重認証：コンポーネントは、工業プロセスに重大な影響を及ぼす可能性がある場合、二重承認をサポートしなければならない。　二重承認は、それらが確実かつ正確に実行されるという非常に高いレベルの信頼性を必要とする行為に限定されるべきである。二重承認を要求することは、正しい行為が行われなかった場合に生じる結果の重大性を強調することになる。二重承認が要求される状況の例としては、重要な工業プロセスの設定点の変更がある。二重承認メカニズムは、例えば、工業プロセスの緊急停止など、HSEの結果を保護するために即時対応が必要な場合には採用すべきではない。
		セキュリティレベル	SR 1.4：認証の実施はSL1に適応する。 SR 1.4 拡張要件1：認証の実施はSL2～SL4に適応する。 SR 1.4 拡張要件2：認証の実施はSL2～SL4に適応する。 SR 1.4 拡張要件3：認証の実施はSL3～SL4に適応する。 SR 1.4 拡張要件4：認証の実施はSL4に適応する。

1．ビルガイドラインの高度化のための調査
①空調等のビルの個別設備システムの対応策に関する調査
②スマートビルのサイバーセキュリティ対策を意識したユースケース調査
③その他関連する調査
③－１　インシデントレスポンスに対する要求の整理
③－２　ガイドラインへの追加情報の充実化
③－３　ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討

2．ビルシステムのサイバーセキュリティ推進体制の調査
①推進体制の情報提供・共有・相談等の機能の実践的評価
②推進体制のあり方の調査

3．検討会の運営
①ビルSWGの運営
②作業グループの運営
③その他の運営

2．ビルシステムのサイバーセキュリティ推進体制の調査
①推進体制の情報提供・共有・相談等の機能の実践的評価

- 推進体制の情報提供・共有・相談等の機能の実践的評価では、昨年度と同様、 2021年1月下旬より、MLを開設し、ビルセキュリティ情報を配信するとともに、配信情報に関する問合せ・相談機能を提供した。
- 昨年度は、ビルSWGの参加メンバーを対象としてビルセキュリティ情報の配信を行ったが、今年度はビルSWGの参加メンバーに加えて、参加メンバー各社の社内他部署やグループ会社等に対象を広げて、配信希望者を募ったうえで配信を行った。その結果、配信先としては、107名(うち、経済産業省、野村総合研究所の事務局メンバーが９名)にまで拡大した。
- ビルセキュリティ情報の配信に対して、「ビルオーナー・関連団体」、「ゼネコン・サブコン・設計事務所」、「ベンダー・関連団体」の３つの業界ごとに、グループヒアリングを実施し、ビルセキュリティ情報の配信の活用方法や活用上の課題等について把握した。
- また、上記を踏まえ、ビルセキュリティ情報の配信や問い合わせ・相談機能について、今後評価すべき観点・項目について整理した。

ビルセキュリティ情報の配信状況

■ビルセキュリティ情報の配信実績を以下に示す。

配信	日時	主な配信内容		
		配信情報	情報ソース	解説内容
第１回配信	2021年1月21日	三菱電機製MELSEC iQ-Rシリーズの PLCに運用妨害（DoS）を引き起こす脆弱性	脆弱性（JVNipedia/ICS-CERT等）	MELSEC PLCとは、リスクの解説、該当する製品とバージョン、想定される影響、推奨事項、本リスク低減のため、特に有効なビルガイドライン対策項目
		WAGO製750-88x および 750-352シリーズのPLCに運用妨害（DoS）を引き起こす脆弱性	脆弱性（JVNipedia/ICS-CERT等）	WAGO製 750-88x および 750-352シリーズのPLCとは、リスクの解説、該当する製品とバージョン、想定される影響、推奨事項、本リスク低減のため、特に有効なビルガイドライン対策項目
		NETGEAR GS108Ev3（スイッチ）の管理画面における入力チェックの不備により、意図しない操作を実行される	脆弱性（JVNipedia/ICS-CERT等）	NETGEAR GS108Ev3（スイッチ）とは、リスクの解説、該当する製品とバージョン、想定される影響、推奨事項、本リスク低減のため、特に有効なビルガイドライン対策項目
第２回配信	2021年1月25日	OpenSSLの脆弱性に関する注意喚起：CVE-2020-1971	注意喚起（JPCERT/CC等）	OpenSSLとは、リスクの解説、該当する製品とバージョン、想定される影響、推奨事項、本リスク低減のため、特に有効なビルガイドライン対策項目
		リアルタイムOSやIoT製品をはじめとした多くの製品で使用されている複数の組み込みTCP/IPスタックで、メモリ管理の不備に起因する複数の脆弱性	脆弱性（JVNipedia/ICS-CERT等）	組み込みTCP/IPスタックとは、リスクの解説、該当する製品とバージョン、想定される影響、推奨事項、本リスク低減のため、特に有効なビルガイドライン対策項目
		三菱電機製 MELSEC iQ-F シリーズにおけるサービス運用妨害 (DoS) の脆弱性：CVE-2020-5665	脆弱性（JVNipedia/ICS-CERT等）	MELSEC PLCとは、リスクの解説、該当する製品とバージョン、想定される影響、推奨事項、本リスク低減のため、特に有効なビルガイドライン対策項目

ビルセキュリティ情報の配信状況

■ 前ページからの続き

配信	日時	主な配信内容		
		配信情報	情報ソース	解説内容
第３回配信	2021年1月28日	Reolink 製 P2P Camerasシリーズ（IPカメラ）への不正侵入につながる脆弱性：CVE-2020-25169、25173	脆弱性（JVNipedia/ICS-CERT等）	Reolink 製 P2P Camerasとは、リスクの解説、該当する製品とバージョン、想定される影響、推奨事項、本リスク低減のため、特に有効なビルガイドライン対策項目
		パナソニック製PLCプログラミングソフト（FPWIN Pro）に任意のコード実行の脆弱性：CVE-2020-16236	脆弱性（JVNipedia/ICS-CERT等）	パナソニック製PLCプログラミングソフト（FPWIN Pro）とは、リスクの解説、該当する製品とバージョン、想定される影響、推奨事項、本リスク低減のため、特に有効なビルガイドライン対策項目
第４回配信	2021年2月4日	Siemens 製 HMI 製品に重要な機能に対する認証の欠如の脆弱性	脆弱性（JVNipedia/ICS-CERT等）	SIMATIC HMI 製品とは、リスクの解説、該当する製品とバージョン、想定される影響、推奨事項、本リスク低減のため、特に有効なビルガイドライン対策項目
第５回配信	2021年2月12日	パナソニック Video Insight VMS において任意のコードが実行可能な脆弱性	脆弱性（JVNipedia/ICS-CERT等）	パナソニック Video Insight VMSとは、リスクの解説、該当する製品とバージョン、想定される影響、推奨事項、本リスク低減のため、特に有効なビルガイドライン対策項目
第６回配信	2021年2月19日	sudo にヒープベースのバッファオーバーフローの脆弱性（CVE-2021-3156）	脆弱性（JVNipedia/ICS-CERT等）	sudoとは、リスクの解説、該当する製品とバージョン、想定される影響、推奨事項、本リスク低減のため、特に有効なビルガイドライン対策項目
第７回配信	2021年2月26日	Johnson Controls製 Metasys Reporting Engine Web Servicesにパストラバーサルの脆弱性	脆弱性（JVNipedia/ICS-CERT等）	Johnson Controls製Metasys Reporting Engine Web Servicesとは、リスクの解説、該当する製品とバージョン、想定される影響、推奨事項、本リスク低減のため、特に有効なビルガイドライン対策項目
第８回配信	2021年3月5日	PerFact Innovation製 OpenVPN-Clientにシステム構成または設定を外部から制御可能な脆弱性（CVE-2021-27406）	脆弱性（JVNipedia/ICS-CERT等）	PerFact Innovation製OpenVPN-Clientとは、リスクの解説、該当する製品とバージョン、想定される影響、推奨事項、本リスク低減のため、特に有効なビルガイドライン対策項目

ビルセキュリティ情報の配信状況

■ 前ページからの続き

配信	日時	主な配信内容		
		配信情報	情報ソース	解説内容
第 9 回配信	2021年3月12日	Schneider Electric 製 EcoStruxure Building Operation 製品群に複数の脆弱性（CVE-2021-27406）	脆弱性（JVNipedia/ICS-CERT等）	Schneider Electric 製 EcoStruxure Building Operationとは、リスクの解説、該当する製品とバージョン、想定される影響、推奨事項、本リスク低減のため、特に有効なビルガイドライン対策項目
第10回配信	2021年3月18日	Schneider Electric 製 Interactive Graphical SCADA System (IGSS) にバッファエラーの脆弱性 (CVE-2021-22709他)	脆弱性（JVNipedia/ICS-CERT等）	Schneider Electric 製 Interactive Graphical SCADA System (IGSS) とは、リスクの解説、該当する製品とバージョン、想定される影響、推奨事項、本リスク低減のため、特に有効なビルガイドライン対策項目
第11回配信	2021年3月〇日			

業界ごとのグループヒアリングの実施

- 「ビルオーナー・関連団体」、「ゼネコン・サブコン・設計事務所」、「ベンダー・関連団体」の３つの業界ごとに、グループヒアリングを実施し、ガイドラインの活用方法やガイドラインの活用上の課題、セキュリティ情報の配信の活用方法等について把握した。

ビルオーナー・関連団体グループインタビュー

会合	開催日時	参加メンバー
第１回会合	2021年３月11日（木）9:00～	イーヒルズ、三菱地所、日本生命、日本ビルヂング協会連合会、不動産協会
第２回会合	2021年３月19日（金）9:00～	イーヒルズ、三井不動産、横浜市

ゼネコン・サブコン・設計事務所グループインタビュー

会合	開催日時	参加メンバー
第１回会合	2021年３月17日（水）17:00～	鹿島建設、竹中工務店、きんでん、日建設計

ベンダー・関連団体グループインタビュー

会合	開催日時	参加メンバー
第１回会合	2021年３月12日（金）10:00～	アズビル、ダイキン工業、日立ビルシステム、日立ジョンソンコントロールズ空調、ジョンソンコントロールズ、ビルディング・オートメーション協会
第２回会合	2021年３月17日（水）11:00～	ダイキン工業、日立製作所、、日立ビルシステム、日立ジョンソンコントロールズ空調、ジョンソンコントロールズ、ビルディング・オートメーション協会、三菱電機、CSSC

業界ごとのグループヒアリングで出たビルセキュリティ情報の配信に関する意見

- ビルセキュリティ情報の配信や問い合わせ・相談機能については、継続してもらいたいという声や、ガイドラインの利用促進や普及という側面から認識を深める場として有効であるという声が聞かれた。

ベンダーへの問い合わせ確認におけるセキュリティ情報配信の活用

- セキュリティ情報配信については、有効に活用している。内容は非常に難解であるが、ベンダー名が記載されているため、当該ベンダーに対して、導入したビルシステムに関係しているものかどうかを都度問い合わせを行い、確認している。継続してもらいたい。

セキュリティに関する業界横断的な情報共有・情報交換の難しさ

- 自社が今後取り組んでいきたいことについて情報共有しなければならないと考えるとなかなか難しい。相談という形は難しい。どこまでの範囲で情報を共有できるかを考えることが必要になる。新しい情報を収集したい一方で、企業秘密を守ることとのバランスを保持することが難しい。
- ベンダー各社の悩みを聞けることはよいが、自社の悩みについては、情報を出しづらい。
- 各社が競合関係にある中で、各社のセキュリティ対応の取組状況を共有するというよりも、ガイドラインの利用をどう広げていくか、その普及という側面から認識を深める場として位置付けることができると有効である。
- 他業界の思いや状況を知ることや、新しいトレンドを知ることにおいては、情報共有の場は有効である。

ビルセキュリティ情報の配信や問い合わせ・相談機能について、今後評価すべき観点・項目

- ビルセキュリティ情報の配信や問い合わせ・相談機能について、今後評価すべき観点・項目について、以下に整理する。

■ （観点１）配信情報の内容が難解であるとの指摘があるが、どのようなセキュリティ意識レベルの読み手や、読み手のどのような活用方法に合わせて改善することが必要であるか。

- ビルセキュリティ情報が必要となる読み手とそのセキュリティレベル
- 読み手が実施している活用方法（記載されているベンダー名に基づき、導入したビルシステムに関係しているものであるかを問い合わせ・確認等）

■ （観点２）配信情報の内容について、日本のビルシステムではほとんど扱われていないような製品が含まれるなど、現状とのミスマッチが発生しているとの指摘があるが、情報の提供価値を高めるために、どのように改善することが必要であるか。

- 配信情報について、読み手からフィードバックが得られる仕組みを配信の仕組みと併せて実装する
- 週1回の配信など形式にとらわれ過ぎない内容重視の配信

■ （観点３）問い合わせ・相談機能について、自社における取組状況や取組上の課題を他社に共有することは難しいとの指摘があるが、問い合わせ・相談機能の活用に向けて、どのように改善することが必要であるか。

- ビルセキュリティ情報として、注意喚起（JPCERT/CC等）や脆弱性情報（JVNipedia/ICS-CERT等）、フィッシングメール等、不正なメールの観測（ニュース/フィッシング対策協議会等）以外に必要と考える情報
- 読み手が想定している活用方法や問い合わせ・相談内容

1．ビルガイドラインの高度化のための調査
①空調等のビルの個別設備システムの対応策に関する調査
②スマートビルのサイバーセキュリティ対策を意識したユースケース調査
③その他関連する調査
③－１　インシデントレスポンスに対する要求の整理
③－２　ガイドラインへの追加情報の充実化
③－３　ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討

2．ビルシステムのサイバーセキュリティ推進体制の調査
①推進体制の情報提供・共有・相談等の機能の実践的評価
②推進体制のあり方の調査

3．検討会の運営
①ビルSWGの運営
②作業グループの運営
③その他の運営

2．ビルシステムのサイバーセキュリティ推進体制の調査
②推進体制のあり方の調査

- ビルガイドラインの普及・啓発や業界におけるセキュリティ対策推進上の課題の共有を含め、ビルシステムのサイバーセキュリティ推進体制構築に必要な要件を整理するため、「ビルオーナー・関連団体」、「ゼネコン・サブコン・設計事務所」、「ベンダー・関連団体」の３つの業界ごとに、グループヒアリングを実施した。
- グループヒアリング結果をもとに、ビルガイドラインの活用方法やビルガイドラインの活用上の課題、セキュリティ対策推進上の課題、セキュリティに関する取組の状況等といった観点からみた、各業界ごとのビルシステムのサイバーセキュリティ推進体制構築に必要な要件を整理した。
- また、推進体制のあり方検討の参考となる既存の国内外のサイバーセキュリティ推進組織の調査を実施した。

業界ごとのグループヒアリングの実施

- 「ビルオーナー・関連団体」、「ゼネコン・サブコン・設計事務所」、「ベンダー・関連団体」の３つの業界ごとに、グループヒアリングを実施し、ガイドラインの活用方法やガイドラインの活用上の課題、セキュリティ対策推進上の課題、セキュリティに関する取組の状況等について把握した。

ビルオーナー・関連団体グループインタビュー

会合	開催日時	参加メンバー
第１回会合	2021年３月11日（木）9:00～	イーヒルズ、三菱地所、日本生命、日本ビルヂング協会連合会、不動産協会
第２回会合	2021年３月19日（金）9:00～	イーヒルズ、三井不動産、横浜市

ゼネコン・サブコン・設計事務所グループインタビュー

会合	開催日時	参加メンバー
第１回会合	2021年３月17日（水）17:00～	鹿島建設、竹中工務店、きんでん、日建設計

ベンダー・関連団体グループインタビュー

会合	開催日時	参加メンバー
第１回会合	2021年３月12日（金）10:00～	アズビル、ダイキン工業、日立ビルシステム、日立ジョンソンコントロールズ空調、ジョンソンコントロールズ、ビルディング・オートメーション協会
第２回会合	2021年３月17日（水）11:00～	ダイキン工業、日立製作所、、日立ビルシステム、日立ジョンソンコントロールズ空調、ジョンソンコントロールズ、ビルディング・オートメーション協会、三菱電機、CSSC

ビルオーナー・関連団体グループヒアリング

ビルオーナー・関連団体におけるガイドラインの活用方法

- ガイドラインの活用方法としては、①実現可能なセキュリティ対策の仕分け、②クラウド化が進むビルでの活用、③分散管理型の検討での活用、④自社のセキュリティ対策ルールの更なる充実強化のための活用が挙がっている。

■ ①実現可能なセキュリティ対策の仕分け

- ビルオーナー側では、ガイドラインのセキュリティ対策の中身について勉強し、「対応可能な対策」と「対応困難な対策」を仕分けした。そのうえで更に、対応可能な対策については、「東京2020の開催までにすぐに取り組まないといけない対策」と「中長期的にみて取り組まないといけない対策」を仕分けした。東京2020の開催までにすぐに取り組まないといけない対策としては、特に運用に関わる対策に注力している。
- また、ビルオーナー以外で対応が必要となる対策については、ビル管理関係者(ビル管理会社、BAベンダーとその系列保守会社)との意見交換を行いながら、ビル管理関係者に対して、対応をお願いする対策を絞り込んだ。そのうち、費用をかけずに取り組むことができる対策について、業務の修正を行っているところである。
  他方、費用がかかる対策としては、制御システムのセキュリティ対策が挙げられ、 BAベンダーとの意見交換により、導入を検討している製品・ソリューションで出来ることと出来ないことを整理し、ビルの改修などの適切なタイミングで導入できるよう準備しているところである。

■ ②クラウド化が進むビルでの活用

- 新築ビルの場合、クラウド化を進めているため、クラウド化で必要となるセキュリティ対策について、ガイドラインを活用している。

ビルオーナー・関連団体におけるガイドラインの活用方法

■ ③分散管理型の検討での活用

- アフターコロナの時代にはテナント運営が厳しくなるため、ビルシステムのセキュリティ対策に掛けられる予算が減少し、費用対効果もこれまで以上に強く求められるようになる。中小のビルでは、中央管理型ではなく、以前の分散管理型に戻す方がよいのではないかというビル制御の形態の見直しに関する議論も出ている。すべてを中央管理型にすると、システムが複雑になり、コストもかかるため、シンプルにそれぞれのビルで管理し、無理にIoT化する必要はない、分散管理型に戻してよいのではないかという声が上がっている。ガイドラインはそのような検討の際に１つの指針として活用している。

■ ④自社のセキュリティ対策ルールの更なる充実強化のための活用

- セキュリティ対策については自社のルールがあり、足りていないところに、ガイドラインで求められている対策を追加して実施しようとしている。古いビルで対応できないものは、新しい対策を入れずにそのままの状態で放置しているものもある。
- ビルガイドラインのB版を踏まえて、独自のガイドラインを作成している。独自のガイドラインを作成してから、大きな更新はないが、必要に応じてマイナーチェンジを行っている。コロナ禍においても、外部に接続している機器の洗い出しやリスク評価に取り組んでおり、ガイドラインを更新しようとしている。また、ビルガイドラインのB版における運用面の対策は非常に参考になり、大いに活用している。現在、追加していく作業の最中である。さらに大型ビルとの比較で、中小のビルにおいて、どこまで対策が必要になるかの仕分けも行っている。独自のガイドラインについて、セキュリティ対策として足りているかどうかを客観的に評価することが必要であるという認識から、外部のITコンサルを入れて、チェックを行った。

ビルオーナー・関連団体におけるガイドライン活用上の課題

- ガイドライン活用上の課題としては、①既存ビルの改修のタイミング、②設計事務所側の理解度に合わないガイドラインの内容、③必要最低限実施すべき対策の明確化、④トータルにビルのセキュリティをマネジメントする人の不在、⑤対応が求められているセキュリティ対策の見せ方の工夫、⑥OT系のセキュリティリスクの把握、⑦ガイドライン対応の難しさ、が挙がっている。

■ ①既存ビルの改修のタイミング

- ガイドラインについては使いこなせていない。既存ビルの改修のタイミングが来ないと、ガイドラインのセキュリティ対策に手を出せないのが現状である。

■ ②設計事務所側の理解度に合わないガイドラインの内容

- ビルの設計フェーズにおいて、セキュリティ対策を実装しようとして、設計事務所にガイドラインを使って説明を行ったが、設計事務所側では要所が分からないという事態になった。設計事務所側で要所が分からないものは、ビルオーナー側としても使いづらい。結局、ビルオーナー側で内容をかみ砕いたものを、設計事務所側に伝えるというプロセスを踏んでいる。
- ガイドラインの別表は、漏れがないように作られているがゆえに、取っつきにくい内容になっている。現場側、設計側の双方においても理解が進んでいない。

■ ③必要最低限実施すべき対策の明確化

- ガイドラインの別表は、すべての対策について対応しなければいけないように見えてしまう。コストを低く抑えて、効果的にセキュリティを上げる方法もあるはずである。先ず実施するなら、このあたりから始めるというものが必要である。必要最低限の対策を決めてほしい。

ビルオーナー・関連団体におけるガイドライン活用上の課題

■ ④トータルにビルのセキュリティをマネジメントする人の不在

- 新築ビルを建設するときに、ガイドラインを使って、ガイドラインで求められているレベルのセキュリティ対策を実施しようとした。その際に、関連業者30数社を集めて、説明会を開催し、実施してもらおうとしたが、業者間で理解のレベルに大きな差があり、その差を埋めるのが難しいことが分かった(理解してもらえるのは2～3社程度)。業界の構造上、トータルにビルのセキュリティをマネジメントする人が不在であり、本来は設計事務所やゼネコンにセキュリティの専門家がいて担当してほしいが、それができない(現場の最前線には来ない)のでビルオーナー側で実施しているのが現状である。ベンダーがトータルでビルのセキュリティをマネジメントしようとしたことがあったが、ベンダー側で対応できないものは、制御の対象外になってしまうようなことが起きた。それも課題である。

■ ⑤対応が求められているセキュリティ対策の見せ方の工夫

- ガイドラインの別表で対応が求められているセキュリティ対策については、設置場所ごとに同じ内容のセキュリティ対策が記載されている場合が多く、一見すると、対応が求められているセキュリティ対策の数が多く見えてしまう。

■ ⑥OT系のセキュリティリスクの把握

- OT系のセキュリティについて、具体的なリスクが何かが把握できていない。お金をかけて、何をどこまで対策する必要があるのかが悩ましい。

ビルオーナー・関連団体におけるガイドライン活用上の課題

■ ⑦ガイドライン対応の難しさ

- ガイドラインの対策項目で足りていないものがあるという感じはしないが、取り込むに際して対応が厳しいというものはある。配線の部分でガイドラインの要求通り、外からアクセスできないようにしようとしたが、ジャックが外に出てしまっているものが多少残ってしまった。また施工者や設計者にガイドラインについて周知していたが、施工者が本当に不正なことを実施していないのかの確認を含めて、どこまで実施できていたかはよく分からない。さらに、IoT機器についても、ガイドラインの仕様どおりに対応されているか、１台１台をチェックすることはできない。施工側のチェックリストやチェックの仕組みが必要ではないか。

セキュリティ対策の推進上の課題

- セキュリティ対策の推進上の課題としては、①中小のビルオーナーの対応リソース不足、②コロナ禍におけるセキュリティ課題の相対的な位置づけの低下、③ビル内に設置されているIoT機器のセキュリティに関する問題意識の欠落、④IoT機器の更新時期を見据えた管理計画の策定、⑤ビル建設後の構成管理のレベル維持、⑥APIの標準化、が挙がっている。

■ ①中小のビルオーナーの対応リソース不足

- 大手のビルオーナーは、自らがセキュリティ対策を考えて実装しているが、中小のビルオーナーは、新型コロナウイルス対策に手を取られていて、セキュリティ対策にまで手が回っていないのが実情である。

■ ②コロナ禍におけるセキュリティ課題の相対的な位置づけの低下

- 新型コロナウイルスの感染拡大の影響を受けて、今後の街づくりのあり方や、各社が事業活動の中でどう対応するかが議論されている。新規の追加投資よりも、既存ストックの有効活用の方が重要視されており、そのような方向性に今後進んでいくと考えている。セキュリティ対策は、このような大きな課題の中の一部として扱われており、セキュリティ対策だけを採り上げて議論するようなことはない。また、ビル単体を採り上げて議論するようなこともない。

■ ③ビル内に設置されているIoT機器のセキュリティに関する問題意識の欠落

- さまざまなIoT機器がビル内に入ってきているが、そのIoT機器のセキュリティは話題になっていない。ビルオーナー側ではそれ自体大きな問題であると捉えている。

セキュリティ対策の推進上の課題

■ ④IoT機器の更新時期を見据えた管理計画の策定

- ガイドラインのセキュリティ対策に準じて、ビルを建設し、かなりレベルの高いセキュリティを実現することができた。その後、管理計画を策定する段階に入ったが、IoT機器の更新時期が、ビルの更新時期と異なっているため、現場は悩んでいる。予防保全の考え方や故障対応の考え方などがある中で、標準がないため、IoT機器の更新時期についてどのように考えればよいかが今後の検討課題になっている。

■ ⑤ビル建設後の構成管理のレベル維持

- 新築ビルの建設時に構成管理について担当した者が、人事異動によって担当者が代わってしまったときに、建設時と同じレベルで管理を行うことができるか、更新した機器や更新の内容の引継ぎが上手くできるか、構成管理のレベル維持が課題となっている。。

■ ⑥APIの標準化

- ビルにおいては、コントローラ等の端末の数が膨大な数になり、セッション数も多くなるので、APIは標準化して、今のものをなるべく代替した方がよい。端末の数が多くなりすぎると、容量の大きいNATなどプロバイダー級の設備を導入する必要があるということも、ビル側でも気にしなくてはならない。

セキュリティに関する取組の状況

- セキュリティに関する取組としては、①さまざまな問題への対応に向けた調査・研究の実施、②ビル関係者向けサイバー演習への参加要請、③ネットワーク監視の充実、④IoT機器の継続的な保守のためのメーカーとの連携、⑤ネットワーク構成管理ツールの導入、⑥セキュリティ情報配信の活用、が挙がっている。

■ ①さまざまな問題への対応に向けた調査・研究の実施

- ガイドラインに記載されていないような問題が起きることがあり、ビルオーナー側が自ら対応することがある。例えば、テナント側がプログラムを作って動かし、テナント側から想定外のアクセスが届くという不具合が発生したときに、ビルオーナー側ではどういう通信が発生しているか、厳格に調査・研究を行った。また、コロナ禍において、ビルシステムの遠隔制御について検討したが、やはり現地対応が重要という判断となり、現地での点検における省力化について研究している。
- IoT機器がビルのネットワークに繋がれたときに、それが正しい機器であることを確認し担保することは難しい。IoT機器用の安価な証明書を導入できるかを研究している。またローカル5G等も使えるのであれば、SIM等の活用についても今後そこまで対応する必要があるかも含めて検討している。コストとの見合いでどのようなものが使えるのかを研究している。

■ ②ビル関係者向けサイバー演習への参加要請

- すべてのビル建築で概ね関わっているような関係者が10数社存在するが、そのよな関係者に３～４回ビル関係者向けサイバー演習に参加してもらい、セキュリティ意識の啓発を行っている。その中にはかなり意識レベルが上がったところもあった。

セキュリティに関する取組の状況

■ ③ネットワーク監視の充実

- ネットワーク監視について、通常の挙動以外に起こりえない挙動を検知することができないか検討している。

■ ④IoT機器の継続的な保守のためのメーカーとの連携

- IoT機器の寿命について考えると対応は相当厳しい。廃番や生産終了について、細かく管理しないと更新することができない。廃番や部品の生産終了に関わる情報については、分かり次第、メーカーから情報を上げてもらうように依頼している。以前はメーカーでもストックを十分持っているところが多かったが、厳しいコスト管理により、それを持てなくなっているところが出てきている。ビルオーナー側では、メーカーから廃番や部品の生産終了に関わる情報が上がってきたら、将来の故障を見込んで、製品や部品を買い込んでいる。

■ ⑤ネットワーク構成管理ツールの導入

- ネットワーク構成管理について、ツールを導入し、システム的な把握を行っている。

■ ⑥ベンダーへの問い合わせ確認におけるセキュリティ情報配信の活用

- セキュリティ情報配信については、有効に活用している。内容は非常に難解であるが、ベンダー名が記載されているため、当該ベンダーに対して、導入したビルシステムに関係しているものかどうかを都度問い合わせを行い、確認している。継続してもらいたい。

ゼネコン・サブコン・設計事務所グループヒアリング

ゼネコン・サブコン・設計事務所におけるガイドラインの活用方法

- ガイドラインの活用方法としては、①関係者への説明会の開催や、②チェックリストへの落とし込み、③ビルオーナーへの説明での活用、④東京2020大会の開催に向けたビルのセキュリティチェック、が挙がっている。

■ ①関係者への説明会の開催

- 全国各支店にある設計部を訪問して、経産省、JDCC双方のガイドラインを知ってもらうために、設備設計担当者への説明会を開催した。一般的なビルの場合、クラウドBAを構築する部分をゼネコンが取りまとめているが、BAベンダー、設備ベンダーにも経産省、JDCC双方のガイドラインを説明して、セキュリティについて検討してもらい、それを設計部に上げてもらえるような体制を整備した。他方、特殊ビルの場合、10名程度のクラウドBAを担当する者に対して、経産省、JDCC双方のガイドラインを読み込んでもらい、担当者が自分たちでセキュリティについて判断できるような体制を整備している。

■ ②チェックリストへの落とし込み

- ガイドラインをもとに、自社の設計標準に照らし合わせて、求められるセキュリティ対策を抽出し、それらをチェックリストにして活用している。設計部で業務で守るものは、建築基準法と社内の設計標準の２つであり、設計標準に求められるセキュリティ対策を落とし込んでいる形になる。ガイドラインは基準・レベルに幅があり、それよりも対策項目の網羅性の方が役に立った。
- 自社の現在地を知る意味合いから、ガイドラインを活用して、求められるセキュリティ対策について、自社における対応の有無を整理することは有用である。基準・レベルが提示されていないので、幅のある解釈が出来て使いやすい。

ゼネコン・サブコン・設計事務所におけるガイドラインの活用方法

■ ③ビルオーナーへの説明での活用

- 大型ビルや特殊ビルの場合、ビルオーナーにセキュリティについて説明する際に、ガイドラインを指針として活用している。こういうセキュリティ対策を導入したいという提案に結び付いている。ガイドラインの対策項目の網羅性は有用であり、セキュリティ対策の導入についてビルオーナーと調整する際に、ガイドラインをベースにすると、話がスムーズに進みやすい。

■ ④東京2020大会の開催に向けたビルのセキュリティチェック

- 東京2020大会のスポンサーでもある大手銀行の本店があるビルについて、セキュリティ上の問題がないか、チェックの依頼があった。チェックした結果を報告し、改善方針を提案したところで、コロナ禍の騒ぎとなり、その先の具体化に向けた動きに入ると止まってしまった。
- チェック対象としては、施設部所管のシステムのみを対象とした(15程度のシステムで、金融業務系システムは含まれない)。施設部所管のシステムについては、これまでセキュリティについて考えられてこなかったが、オリンピックスポンサーがサイバー攻撃の標的にされやすいこともあり、万が一、事故が発生したら大変な事態になることが予想されるため、対応が不十分なところを中心に改善するためにチェックを始めた。調査からベンダーヒアリング、報告書作成まで含めて３～４か月間を要した。

ゼネコン・サブコン・設計事務所におけるガイドライン活用上の課題

- ガイドライン活用上の課題としては、①ガイドラインに対する関心の低さ、②個別編を含めた会社対応方針の検討、③設計標準への落とし込み、④現実的な落としどころへの着地、⑤ビルオーナーにおけるセキュリティ対応意識の希薄、⑥守らなければならない対策としての具体性の欠如、⑦OT系ベンダーの意識の低さ、⑧インターネット接続・クラウド接続のオプション扱い、が挙がっている。

■ ①ガイドラインに対する関心の低さ

- 全社員が集まる社内会議で、ビルシステムに必要なセキュリティ対策がまとめられたガイドラインであるという説明を行った。その際、ビルオーナーやゼネコンから、セキュリティについて対応したいという相談があれば、本社サイドにその情報を上げるように依頼したが、そのような相談の件数は少ない。相談が来るのは、首都圏の大型ビルぐらいである。ゼネコンや設計事務所が作成した設計図をもとに、サブコンでは工事を進めるが、設計図でガイドラインの準拠を求めてくるようなケースはほとんどない。森ビルなど一部の大手ビルオーナーから相談・指示はあるが、その他大勢のビルオーナーからは特に相談・指示はないような状況である。
- インシデントや被害がほとんどないので、セキュリティの認識は広がっていない。議論も進んでいる感じがしない。ただ大きなインシデントが起きて、大騒ぎになれば、意識は変わるのではないか。

■ ②個別編を含めた会社対応方針の検討

- 設備設計の部署に対して、ガイドラインの説明会を開催した。その際に、共通編と個別編についても説明したが、個別編が出てきてから、会社としての対応方針を検討しようという話になり、現状では情報共有にとどまっている。

ゼネコン・サブコン・設計事務所におけるガイドライン活用上の課題

■ ③設計標準への落とし込み

- 設計事務所社内でガイドラインを周知しているが、設計標準に落とし込むところまでは出来ていない。

■ ④現実的な落としどころへの着地

- 対策について新しいものを導入しようとする際には、現実的な落としどころをどうするかを考えて、7 割が運用でカバーすることになり、残り 3 割が設置場所の変更などの実施方法の修正になっている。

■ ⑤ビルオーナーにおけるセキュリティ対応意識の希薄

- ガイドラインが公表されても、プロジェクトの 9 割は何も変わらない状況である。実際にインシデントや被害が起きていない中で、ビルオーナー側もセキュリティ対策にコストをかけるとは言ってくれない。残りの 1 割は、データセンターのようなプロジェクトであり、セキュリティについてチェックするので、図面を持って説明に来てほしいと言われる。スマートシティでは、BAシステム間のネットワーク接続も進んでいくことになるが、オーナーの発注要件にセキュリティチェックが盛り込まれている。
- 発注の上流部において、セキュリティ対策は、柱や梁と同様に大事であるという認識にならなければ、早い段階で予算を確保し、セキュリティ対策を組み込むことはできない。また追加でセキュリティ対策を導入することは難しい。発注側の意識啓発・啓蒙活動が必要である。
- ガイドラインで求められるセキュリティ対策について、ビルオーナーがお金をかけて実施するものと、ビルオーナーがお金をかけられないが、実施できるものを整理して、後者について設計段階にきちんと織り込めるようにし、設計の質を上げていきたい。そうすることで、ビルオーナーの対応意識も高められるとよい。

ゼネコン・サブコン・設計事務所におけるガイドライン活用上の課題

■ ⑥守らなければならない対策としての具体性の欠如

- ガイドラインは、既存のビルやビルシステムを対象としたセキュリティ評価には使いやすいが、新築ビルの建設時に、ガイドラインをもとに、関係者の中で議論していく際には、非常に労力を要する。法的拘束力がないので、選択肢に幅ができ、具体的に記載されていないのはやむを得ないが、関係者の中で議論するような場合には向かない。セキュリティ対策が設計基準書に盛り込まれるようにするには、もう少し基準・レベルとして守らなければならないものについて具体性が必要である。ビルの規模や用途、重要度に応じた実績ができれば、一定の基準・レベルに収束していき、将来的にまとまっていくことになる。
- ガイドラインを使うBAベンダーや設備ベンダーにとって、拠り所になるように基準を示す形でガイドラインを改善することが必要である。

■ ⑦OT系ベンダーの意識の低さ

- OT系システムのガイドラインとしてみたときに、OT系の作法として、セキュリティについてはそこまで対応しないということが基本になっており、100％対応するというところまで行き着かない状況がある。ベンダーからは何故そこまで対応することが必要になるのかと言われ、かなり意識の差がある。OT系ベンダーの中でも、IT系の事業を実施しているところや、開発を行っているところはまだよいが、OT系のみ事業を実施しているところや、運用保守を行っているところは、セキュリティ対応の意識がない。

■ ⑧インターネット接続・クラウド接続のオプション扱い

- 設計図面を見て、現場でセキュリティを考えるように指示しているが、インターネット接続の部分やクラウド接続の部分はあくまでオプション扱いとなっているため、積極的な議論にはならない。

ベンダー・関連団体グループヒアリング

ベンダー・関連団体におけるガイドラインの活用方法

- ガイドラインの活用方法としては、①セキュリティ対策の実施根拠としての提示や、②客観的にみたセキュリティ対策の対応レベルの提示、③ゼネコン等と連携・協働した取組、が挙がっている。

■ ①セキュリティ対策の実施根拠としての提示

- ベンダーとしての心構えとして、ガイドラインが参考になった。具体的には、顧客から脆弱性情報の説明を求められる機会が増えており、脆弱性に対応できていることを説明するための資料の内容の拡充に繋がっている。また、コントローラーで対応可能なセキュリティ対策を盛り込み、顧客に提供することが出来ている。顧客に説明する際に、ガイドラインのこの部分に記載されているという説明ができることで、顧客に分かってもらいやすくなっている。
- ビルオーナー側から、ガイドラインのこのセキュリティ対策を入れてほしいと指示をもらう方がよい。ガイドラインやセキュリティ対策に関心がないビルオーナーに、セキュリティ対策の必要性を説明することの方が大変である。指示をもらうような場合でも、ビルオーナーと相談しながら、方針を決めて、実現可能性についてすり合わせを行っている。また指示以外に、一緒に考えてほしいと言われ、提案を求められることがある。

■ ②客観的にみたセキュリティ対策の対応レベルの提示

- ベンダーの活動としては、このレベルまで対応すればよいという指標が示されるという意味合いで、ガイドラインは参考になっており、使い勝手がよい。自社の意見ではなく、第三者の意見として示しつつ、説明や提案・紹介ができるのはよい。顧客にも納得してもらいやすい。

ベンダー・関連団体におけるガイドラインの活用方法

■ ③ゼネコン等と連携・協働した取組

- ゼネコン等と一緒に、ガイドラインをベースに、セキュリティ対策の中身の確認や、脆弱性・リスクの検証を行う取組を実施している。

ベンダー・関連団体におけるガイドライン活用上の課題

- ガイドライン活用上の課題としては、①確認依頼の問い合わせの減少、②ガイドラインに対する関心の低さ、③発注側の独自ガイドラインへの利用シフト、④ガイドラインの周知・啓蒙活動の強化、⑤ガイドラインの標準規格化に向けた動き、⑥国が定める設計仕様書・発注仕様書へのセキュリティ要件の記載、⑦ビルオーナー側からの実際に起きているインシデントや被害の紹介、が挙がっている。

■ ①確認依頼の問い合わせの減少

- ガイドラインの公開後しばらくの間は、顧客からガイドラインとの対応づけについて確認を依頼されることがあったが、直近はそのような確認依頼の問い合わせが減っている。

■ ②ガイドラインに対する関心の低さ

- 以前、大手のビルオーナーからセキュリティの問い合わせを受けることはあったが、抽象的な内容が多く、ガイドラインに記載されている内容まで踏み込んだ形での問い合わせはもらっていない。中小のビルオーナーからは問い合わせはない。また、自社のエレベータの遠隔監視のセキュリティチェックに使いたいと考えているが、まだまだガイドラインに関して社内での関心は低い。
- 工場などでは、ガイドライン準拠の要求が上がってきている状況があるが、ビルについては、まだまだこれからである。ビルオーナーやゼネコンからセキュリティ対策の要件が上がってきていないのが現状である。
- 営業フロント側と開発側でガイドラインで求められるセキュリティ対策の確認を行っているが、ガイドラインに沿った問い合わせがほとんどない。啓蒙活動を含めて取り組んでいるような状況である。
- ゼネコンやサブコンのセキュリティ担当者はまだまだ少数であり、セキュリティに対する理解も不十分である。実案件においても、セキュリティ要求がベンダーまで落ちてこない状況がずっと続いている。大手ビルオーナー以外では、もともとセキュリティ要求がなく、提案しても予算取りが後付けになるため、なかなか導入してもらえない。

ベンダー・関連団体におけるガイドライン活用上の課題

■ ③発注側の独自ガイドラインへの利用シフト

- 大手のデベロッパにおいては、独自にガイドラインを作成し更新しているため、ガイドラインに関する問い合わせは直近にはない。外部接続は、IP-VPNまたは専用線を用いているが、公開サーバーやインターネットの接続ポイントについても、大手のデベロッパから問い合わせはないが、中小のデベロッパからは問い合わせがある。
- 独自ガイドラインの場合、顧客によってそれぞれ違う内容が要求される訳ではないので、対応が煩雑になることはない。

■ ④ガイドラインの周知・啓蒙活動の強化

- ガイドラインについて、(中小の)ビルオーナーを含めて、どこまでの関係者に認知されているのかが疑問である。自治体や公共建築を含め、関係者にガイドラインを認知してもらい、参照するように啓蒙活動を行うことが必要である。特に工事業者において、ガイドラインやセキュリティ対策に対応することについての認識が希薄である。
- ガイドラインが公開されたことは認識しているが、ガイドラインの内容について理解している関係者は必ずしも多くない。ガイドラインはビルシステム全体のセキュリティをマネジメントするためのものであり、ベンダーだけ対応すればよいという訳ではなく、顧客側でマネジメントしなければならないが、それを説明することが難しい状況である。

■ ⑤ガイドラインの標準規格化に向けた動き

- ガイドラインは標準規格化がされていないと、なかなか普及浸透に繋がらない。セキュリティを維持管理していくためにはコストがかかるため、標準規格化がされていると、セキュリティ対策にもう少し踏み込めるのでよい。

ベンダー・関連団体におけるガイドライン活用上の課題

■ ⑥国が定める設計仕様書・発注仕様書へのセキュリティ要件の記載

- 設計仕様書や発注仕様書を独自に作成しているが、ベースとなっているのは、国土交通省の設計仕様書や発注仕様書であり、それに自社で必要となるものを追加している。国土交通省の設計仕様書や発注仕様書の中に、セキュリティ対策を実施することが要件として記載されれば、ガイドラインが参照・活用されることになる。そのような動きは、民間の分野にも広がる。また、ビルオーナーが直接見てなくても、設計事務所やゼネコンは、当該要件をベースに、ガイドラインの基準に対応することになる。
- OT系システム向けのサイバーセキュリティ製品を開発して、ビルオーナーに営業したが、重い腰が上がっていない。結局、ビル以外の異なる分野に営業している。公共設備におけるセキュリティ対策の実装が進んでいないので、国の方でもっと積極的に検討してもらいたい。提案ベースでセキュリティ対策を追加しているような状況では、なかなか導入が進まない。

■ ⑦ビルオーナー側からの実際に起きているインシデントや被害の紹介

- 日本のビルシステムについて、実際にサイバーセキュリティに関わる事故が起きているのか、海外から問い合わせを多く受けているが、回答に苦慮している。ビルオーナー側に、そのような事故や被害が起きているのかどうかを紹介してほしい。そうなれば、ガイドラインの活用も進むのではないか。

セキュリティ対策の推進上の課題

- セキュリティ対策の推進上の課題としては、①顧客のネットワーク利用によるセキュリティの低下や、②セキュリティ対策への意識の低い顧客の意識啓発、③末端の担当者レベルまでのセキュリティ知識の普及啓発、④セキュリティ認証の難しさ、⑤セキュリティに関する業界横断的な情報共有・情報交換の難しさ、が挙がっている。

■ ①顧客のネットワーク利用によるセキュリティの低下

- 設備の稼働・運転情報を外部に出したくないという背景から、ネットワークを統一したいという要望が顧客から出てきており、これまではベンダー各社がネットワークを構築していたが、顧客のネットワークを利用することで、セキュリティが弱くなるケースが発生し、困っている。そのような場合のセキュリティについて、どのように対応すべきかをしっかりと考えていく必要がある。
- セキュリティが弱くなることについての説明や解決策の提示は難しいが、顧客に説明できるように最低限の準備を行っている。
- 自社のセキュリティポリシーがあり、顧客のネットワークに繋げるということは、自社のネットワークにも繋がってしまうことになるので、セキュリティポリシーに合致しないという説明を行い、何とか納得してもらっている。

■ ②セキュリティ対策への意識の低い顧客の意識啓発

- 製品そのものに要求されるスペックの中には、PW設定など一部セキュリティ対策の機能を組み込んでいるが、顧客にどう使ってもらうかが課題となっている。また、ネットワーク構成に関して提案をどのように行っていくかが課題であるが、その際にも、顧客側でセキュリティポリシーや運用方針が規定されていないため、顧客と一緒にセキュリティ対策を実装するところの意識づけから始めないといけない。

セキュリティ対策の推進上の課題

■ ③末端の担当者レベルまでのセキュリティ知識の普及啓発

- ビルオーナー、ゼネコンを含め、ベンダーの中でも、セキュリティ知識を強化するために、末端の担当者レベルまで普及啓発を実施することが必要である。
- ベンダーの中にも、防火機器や入退管理システムのベンダーのように、大中小入り混じってベンダーの数が多いところがあり、セキュリティ知識レベルの温度差がある。

■ ④セキュリティ認証の難しさ

- ビルのセキュリティ認証が導入されたとしても、ビジネスに直結することは難しい。
- コスト負担をどのように考えるかが重要になる。日本においては、コスト負担は厳しいが、プラント系などの海外案件では、ハードウェア、ソフトウェアのセキュリティ上の担保について要求されることがあり、認証取得を含めて検討することがある。海外案件では、エンジニアリング会社がRFPにセキュリティ要求を記載している。
- 製品開発プロセス、製品そのものなど、どの範囲で認証を取得するかにもよるが、それぞれに難しさがあると考えられる。
- 業界として均一なセキュリティレベルを求められるようになれば、セキュリティ認証は必要になってくる。また、ビルのインシデントや被害が発生するようになって、保険の導入が求められるようになれば、保険に加入する際に何らかのセキュリティ担保が必要になるので、セキュリティ認証は必要になってくる。ただし現在はそのような状況にない。

セキュリティ対策の推進上の課題

■ ⑤セキュリティに関する業界横断的な情報共有・情報交換の難しさ

- 自社が今後取り組んでいきたいことについて情報共有しなければならないと考えるとなかなか難しい。相談という形は難しい。どこまでの範囲で情報を共有できるかを考えることが必要になる。新しい情報を収集したい一方で、企業秘密を守ることとのバランスを保持することが難しい。
- ベンダー各社の悩みを聞けることはよいが、自社の悩みについては、情報を出しづらい。
- 各社が競合関係にある中で、各社のセキュリティ対応の取組状況を共有するというよりも、ガイドラインの利用をどう広げていくか、その普及という側面から認識を深める場として位置付けることができると有効である。
- 他業界の思いや状況を知ることや、新しいトレンドを知ることにおいては、情報共有の場は有効である。

セキュリティに関する取組の状況

- セキュリティに関する取組の状況としては、①クローズドな環境で運用されてきた遠隔監視システムに対するセキュリティ対策強化の検討、②外資系の顧客からの要求への対応、③コーポレートPSIRTの構築、④クリティカルな施設におけるデータ保護対策、が挙がっている。

■ ①クローズドな環境で運用されてきた遠隔監視システムに対するセキュリティ対策強化の検討

- エレベータの遠隔監視は、クローズドなネットワークで行ってきたため、今までセキュリティ対策について力を入れていなかったが、ビル全体で考えると、IoT化が進む中でさまざまネットワークに繋がっているため、今後はセキュリティ対策に注力しなければならない。
- コロナ禍において、遠隔監視の問い合わせは数は多くないがあり、自社で対応している場合がある。そのような場合においても、自社の中に閉域網で接続するというセキュリティポリシーが存在するため、対応はあくまでその範囲内にとどめている。

■ ②外資系の顧客からの要求への対応

- 外資系の顧客から、独自のネットワークを活用したいと要求されることがあるが、そのような場合には、顧客側のセキュリティポリシーに準拠して対応している。外資系の顧客からの要求は厳しいというよりも、仕様やプロトコルの開示を求められる。外資系の顧客は、自ら回線やハードウェアを管理したいということである。そのため、回線やハードウェアも自ら調達している。

セキュリティに関する取組の状況

■ ③コーポレートPSIRTの構築

- 空調機器における具体的なセキュリティ対策の実装に関わる検討はこれからであるが、基盤づくりとして、コーポレートPSIRTを構築し、脆弱性の報告を行うなど、空調機器の脆弱性対策に取り組んでおり、空調機器の脆弱性に関する認識は高まっている。

■ ④クリティカルな施設におけるデータ保護対策

- データセンターや研究所などクリティカルな施設においては、データを安全に守るためのセキュリティ対策が必要であり、データインテグリティの観点からの要求が盛り込まれることがある。

国内外のサイバーセキュリティ推進組織の調査

■ 以下に示す国内外で活動している他の分野のISACを対象として、必要となる機能やメンバー体制等を調査した。

①一般社団法人ICT-ISAC
②一般社団法人金融ISAC
③その他のISAC（電力ISAC、Software ISAC、米国におけるISACの取組）

①一般社団法人ICT-ISAC
１）目的と活動内容

【目的】

情報通信技術（以下「ＩＣＴ」という）の普及、発展により、日常生活、経済、行政、安全保障・治安確保などのあらゆる活動がサイバー空間に依存するようになり、高度化・複雑化するＩＣＴへの脅威は深刻な社会的脅威となっている。

このような現状に鑑み、ＩＣＴに関わるセキュリティの対策・対応レベルの向上に資する活動を行うために、社員間の幅広い相互連携を図り、安定した情報流通、情報伝達を維持することで、安全なＩＣＴ社会の形成に寄与することを目的とする

【活動内容】

1．情報セキュリティに関する情報収集・調査・分析
ICTに関わる情報セキュリティ対策に資する情報（インシデント情報を含む。）を収集、調査、分析する活動

2．情報共有の推進（情報共有）
情報セキュリティに関する情報を目的に応じて共有し、それを活用しつつ会員企業間で相互協調する仕組みを整備し、それを促進する活動

3．セキュリティ人材の育成、セキュリティ啓発（普及啓発・人材育成）
会員企業のセキュリティ人材育成を促進する活動およびユーザが安全にICTを利用するための普及啓発活動

4．セキュリティガイドライン等の整備に関する活動
会員各社がセキュリティ対策を円滑に行う上で必要となるガイドラインの検討および法制度に関する政府研究会等への参画活動

5．認定協会業務
認定送信型対電気通信設備サイバー攻撃対処協会（認定協会）としての活動

7

出所）ICT-ISACのホームページ・公表資料

①一般社団法人ICT-ISAC
2）会員企業数

会員企業（42社）（2020年2月7日現在）

理事長（代表理事）：齊藤忠夫（東京大学名誉教授）
理事： 井伊基之（NTT） 内田義昭（KDDI） 監事：田中啓仁（KDDI） 顧問：飯塚久夫、中尾康二

通信系(21)	日本電信電話株式会社、KDDI株式会社 ソフトバンク株式会社、株式会社インターネットイニシアティブ、NTTコミュニケーションズ株式会社、ビッグローブ株式会社 ソニーネットワークコミュニケーションズ株式会社、株式会社NTTドコモ、株式会社オプテージ 株式会社日本レジストリサービス、ニフティ株式会社、東日本電信電話株式会社、西日本電信電話株式会社 株式会社KDDI総合研究所、アルテリア・ネットワークス株式会社、インターネットマルチフィード株式会社 NTTデータ先端技術株式会社 株式会社QTnet、株式会社NTTエムイー、株式会社朝日ネット、日本ネットワークイネイブラー株式会社
放送系(7)	日本放送協会、株式会社ジュピターテレコム 日本テレビ放送網株式会社、株式会社 TBSテレビ、株式会社フジテレビジョン、株式会社テレビ朝日、株式会社テレビ東京
セキュリティベンダー系(10)	NRIセキュアテクノロジーズ株式会社、NTTセキュリティ・ジャパン株式会社 株式会社FFRI、株式会社カスペルスキー、株式会社サイバーディフェンス研究所、トレンドマイクロ株式会社 マカフィー株式会社、KDDIデジタルセキュリティ株式会社、パロアルトネットワークス株式会社、日商エレクトロニクス株式会社
SI・ベンダー系(4)	日本電気株式会社、富士通株式会社、株式会社日立製作所、沖電気工業株式会社

<オブザーバー>
総務省、国立研究開発法人 情報通信研究機構、一般社団法人電気通信事業者協会、一般社団法人テレコムサービス協会
一般社団法人日本インターネットプロバイダ協会、一般財団法人日本データ通信協会、一般社団法人日本民間放送連盟
一般社団法人日本ケーブルテレビ連盟

出所）ICT-ISACのホームページ・公表資料

①一般社団法人ICT-ISAC
3）WG活動一覧

WG数（21WGうち、業界特化系WGは９WG、業界横断系WGは21WG）（2020年2月7日現在）

【業界特化系WG（通信系）】

- 経路情報共有-WG 2005年7月設置
  ISP間の経路情報の共有、経路情報異常時の迅速な対応。および経路奉行システムの運用
- ACCESS-WG 2007年4月設置
  インターネットアクセスNWサービスの運用品質向上のための情報交換、ベストプラクティス共有や有識者を交えた意見交換
- SoNAR-WG 2007年12月設置
  ネットワークを利用した不正・不法行為対応(ABUSE対応)に関する情報の共有。インシデントの拡大を抑止するフレームワークの策定
- DoS攻撃即応-WG 2011年10月設置
  DoS攻撃への迅速な対応と複数事業者による協調対処の仕組みの検討。日本国内におけるDoS攻撃発生の、予測、早期検出、迅速かつ適切な対応の実現を目指す。
- 認定協会業務推進WG 2018年8月設置
  電気通信事業法等の改正に伴う認定協会(*)業務及びNICT業務について、ICT-ISACの取り組み方針検討及び、必要な組織を立ち上げを行うともに円滑業務推進行うことを目的とする。（*：正式名「認定送信型対電気通信設備サイバー攻撃対処協会」）
- NOTICE-SiG 2019年1月設置
  NOTICEは（総務省、国立研究開発法人情報通信研究機構（NICT）及びISPが連携し、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起を行う取組）に取り組むISP間での情報共有。

【業界特化系WG（放送系）】

- 放送設備サイバー攻撃対策WG 2016年10月設置
  2020オリパラに向けての放送設備のセキュリティ強化のため、放送設備導入時の指針となる「放送設備セキュリティガイドライン(BCDG)」の策定と現場への浸透

【業界特化系WG（ＳＩ・ベンダ系）】

- デバイス脆弱性ハンドリング検討WG 2017年1月設置
  IoT時代で活用されるデバイス全般を対象とすることを見据え、汎用的なソフトウェアに限らない各種ソフトウェア、ファームウェア、ハードウェアに内包されたプログラム等でのセキュリティ侵害リスク脆弱性）のハンドリングについて、対外的に公開することも視野に、その手順の検討

【業界特化系WG（セキュリティ・ベンダ系）】

- セキュリティベンダ課題検討WG 2016年11月設置
  各社相互理解、個社または業界共通の課題の検討。セキュリティトピック等の情報連携の在り方について議論

11

出所）ICT-ISACのホームページ・公表資料

①一般社団法人ICT-ISAC
3）WG活動一覧

【業界横断系WG】

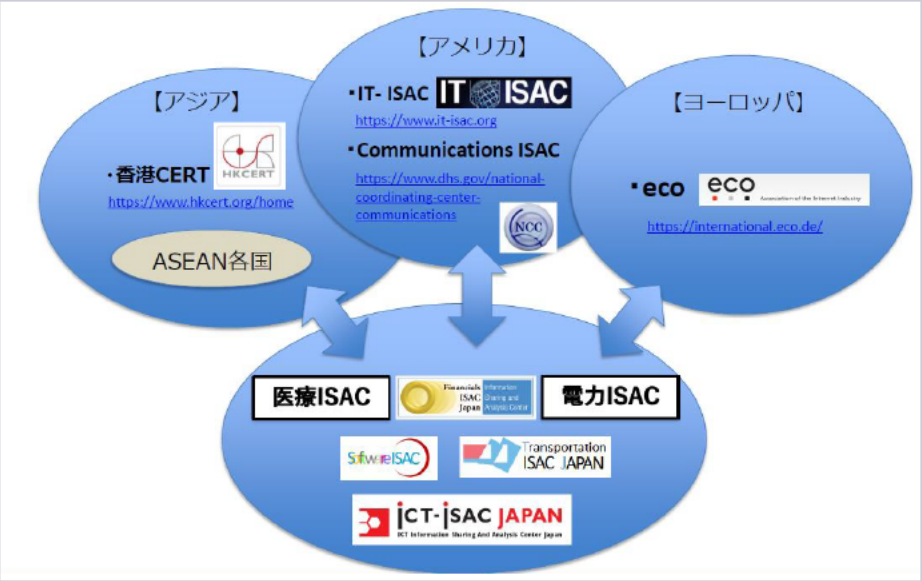
- サイバー攻撃対応演習-WG(CAE-WG) 2009年5月設置
  電気通信事業者等の参加する、サイバー攻撃を想定した対応演習の企画、実施
- 脆弱性保有ネットワークデバイス調査-WG 2013年05月設置
  国内IPに接続されたネットワークデバイスの脆弱性保有状況の全容把握と調査を実施
- ACTIVE業務推進-WG 2013年07月設置
  総務省ACTIVEプロジェクトの施策推進。マルウェアの感染防止、駆除を推進し、より安心・安全なインターネットの実現を目指す
- WiFiリテラシー向上-WG 2013年09月設置
  電波の有効利用（オフロード推進）を目的に、WiFiの利用および設置・運営において障壁となる情報セキュリティ課題の検討、対策の実施
- サイバー攻撃への適正な対処検討のためのWG(通秘-WG) 2013年12月設置
  電気通信事業の業務を整理し通信の秘密に代表される法的な整理を行うことを目的とする
- 情報共有WG 2016年11月設置
  情報共有についての国際連携やISAC 間連携、 ICT -ISAC 内での情報活用のあり方など、大局的な取り組みについての検討
- 交流促進-WG 2016年11月設置
  ICT-ISAC会員企業向けに、ノウハウ・知識等の普及・啓発、ISAC内の活動の活性化、WG間の相互理解促進、会員企業の持つ関連知識の共有・相互理解の促進等を行うと共に、対外的なイベント開催を通じてISAC活動のアピールを行い、会員数拡大にもつなげる
- IoTセキュリティWG 2016年8月設置
  ICT-ISACとして取組むべき「IoTセキュリティ対策」について、国の施策の動向を踏まえつつ、情報共有・議論を進め、我が国及び会員各社のIoTセキュリティに資することを目的とする
- CSA-WG 2019年3月設置
  ICT-ISACとしてもNISCのサイバーセキュリティ協議会に構成員として参加し、国の施策の動向を踏まえつつ、情報共有・議論を進め、我が国及び 会員各社の連携向上に資することを目的とする
- 国内外ISAC連携-WG 2019年４月設置予定
  海外ISACおよび国内他業界ISACとの連携について検討する
  我が国及び 会員各社の連携向上に資することを目的とする
- DNS運用者連絡会-SIG 2008年6月設置
  DNSに関わる、脆弱性対応・情報の共有、DNSSEC化に備えた情報交換
- 若手活躍SIG 2018年7月設置
  若年層にICT-ISACに参加する意義を伝え、また若年層が参加する環境を改善し、若者のセキュリティ離れを食い止める活動を行う

12

出所）ICT-ISACのホームページ・公表資料

①一般社団法人ICT-ISAC
4）主な特徴

項目	主な特徴
会員区分・会費	● 会員区分としては、「プラチナ会員」、「ゴールド会員」、「シルバー会員」、「ブロンズ会員」 ● 会員区分による会費及び提供される価値の傾斜あり ● 年会費は最大500万円
運営形態	● 非営利型、営利型の一体的な運営 ● 会員からの会費収入以外に、国等からの受託事業収入あり ● 事務局は出向者により運営
他のISACとの連携	● サイバーセキュリティの確保に向けて国際的な協力関係を築くため、The Information Technology – Information Sharing and Analysis Center（IT-ISAC）との間で、覚書(MOU: Memorandum Of Understanding)を締結。



出所）ICT-ISACのホームページ・公表資料

②一般社団法人金融ISAC
１）目的と活動内容

目的

金融ISACは、日本の金融機関の間でサイバーセキュリティに関する情報の共有・分析、及び安全性の向上のための協働活動を行い、金融サービス利用者の安心・安全を継続的に確保することを目的としています。

活動概要

金融ISACでは、日々発生するインシデントや脆弱性を会員間で共有する『コレクティブインテリジェンス』と、共通の課題に対しリソースを共有し、協働しながら対策を検討を進めていく『リソース・シェアリング』の２つを活動の柱とし、金融システム基盤全体の安心・安全の向上に寄与するさまざまな活動をしていきたいと考えています。
金融ISACでは専用のポータルサイトを通じ、日々のインシデントや脆弱性情報等をリアルタイムに共有しています。また、特定の重要課題について、テーマごとにワーキンググループ（WG)を設け、会員共同で対策検討等を行いながら、知見と対応力を高めています。これらの成果はワークショップやアニュアルカンファレンス等の場で発表し、ポータルサイトに成果物の蓄積を行っています。

出所）金融ISACのホームページ

②一般社団法人金融ISAC
2）会員企業数

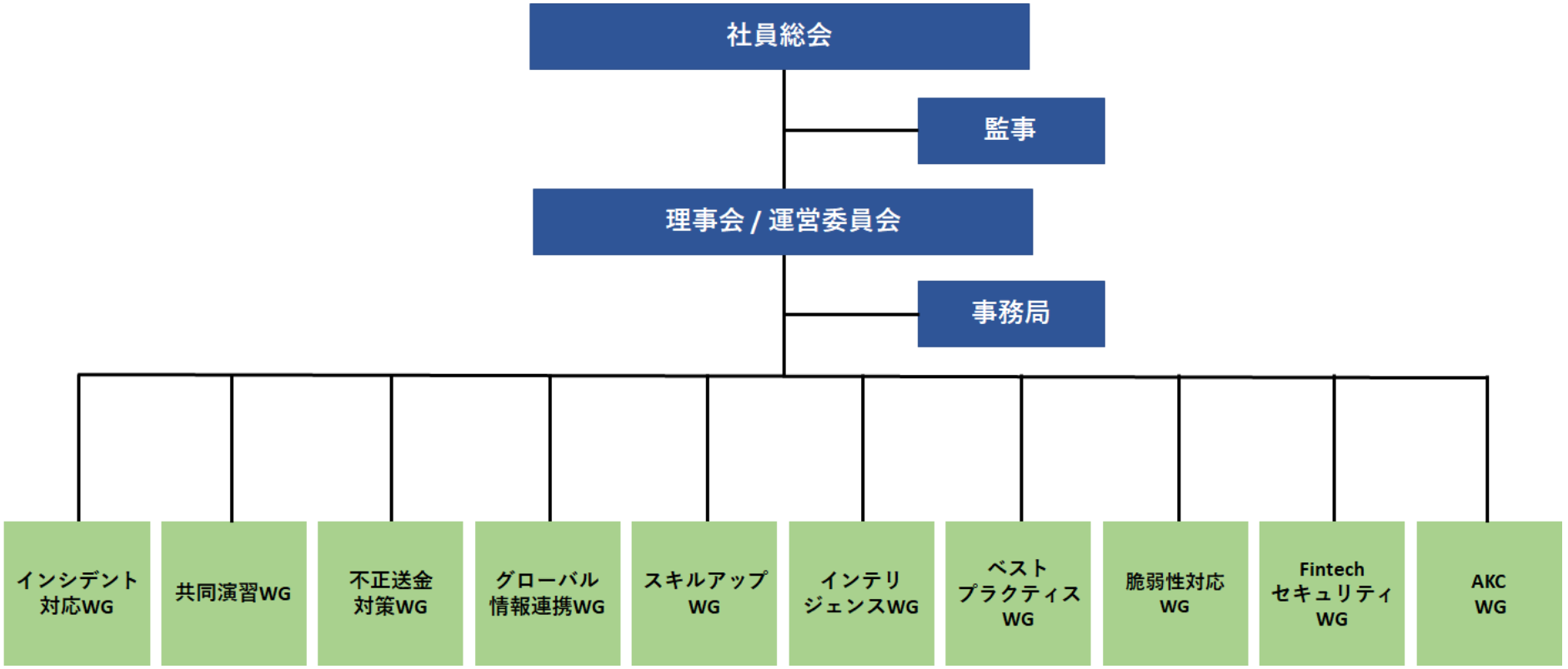
会員企業数（正会員385会員、賛助会員1会員、アフィリエイト会員25会員）（2020年2月7日現在）

会員区分等		主な企業
正会員	ホールディングス（27）	株式会社三菱UFJフィナンシャル・グループ、株式会社みずほフィナンシャルグループ、株式会社三井住友フィナンシャルグループほか
	銀行（133）	株式会社三菱UFJ銀行、株式会社みずほ銀行、株式会社三井住友銀行、株式会社ゆうちょ銀行、株式会社横浜銀行ほか
	証券（52）	野村證券株式会社、SMBC日興証券株式会社、株式会社SBI証券、株式会社大和証券グループ本社ほか
	生命保険（36）	第一生命株式会社、日本生命保険相互会社、明治安田生命保険相互会社、ソニー生命保険株式会社ほか
	損害保険（21）	東京海上日動火災保険株式会社、損害保険ジャパン日本興亜株式会社、三井住友海上火災保険株式会社ほか
	カード・ファイアナンス（11）	三井住友カード株式会社、三菱UFJニコス株式会社、株式会社ジェーシービー、株式会社オリエントコーポレーションほか
	信金・信組（78）	愛知信用金庫、大阪信用金庫、京都信用金庫、高松信用金庫、浜松信用金庫、広島信用金庫ほか
	労働金庫（14）	九州労働金庫、近畿労働金庫、四国労働金庫、中央労働金庫、中国労働金庫、東海労働金庫ほか
	その他（13）	全国共済農業協同組合連合会全国本部、日本郵政株式会社、三井住友トラスト・アセットマネジメント株式会社ほか
賛助会員（1）		一般社団法人JPCERTコーディネーションセンター
アフィリエイト会員	ゴールド（12）	アカマイ・テクノロジーズ合同会社、NRIセキュアテクノロジーズ株式会社、パロアルトネットワークス株式会社、株式会社ラックほか
	シルバー（10）	シスコシステムズ合同会社、デロイト トーマツ リスクサービス株式会社、三井物産セキュアディレクション株式会社ほか
	ブロンズ（3）	アクセンチュア株式会社、株式会社NTTデータ、日本シノプシス合同会社

出所）金融ISACのホームページより作成

②一般社団法人金融ISAC
3）WG活動一覧

WG数（10WG）（2020年2月7日現在）



出所）金融ISACのホームページ

②一般社団法人金融ISAC
4）主な特徴

項目	主な特徴
会員区分・会費	● 会員区分としては、「正会員」、「賛助会員」、「アフィリエイト会員」 ● 会員区分による会費及び提供される価値の傾斜あり ● 正会員の年会費は80万円、アフィリエイト会員の年会費は最大300万円
運営形態	● 非営利型の運営 ● 会員からの会費収入中心 ● 出向者ではなく、プロパーによる運営
他のISACとの連携	● 金融ISACはFS-ISACとISAC間の情報共有など、協力活動を強化

③その他のISAC（電力ISAC、Software ISAC）

電力ISAC

【目的】 電気の安定供給の役割を担う事業者間で、信頼と互助の精神に基づき、サイバーセキュリティに関する情報等を交換や分析することにより、事故の未然防止、発生した事故に対する迅速な対応等を実現すること

【事業概要】
- サイバーセキュリティに関する情報の収集
- 収集した情報の内容を踏まえた情報の分析
- 収集・分析の結果の会員間での共有
- 会員間での情報共有に伴う、ルールの策定及び相互協調活動の促進
- 電力セプター事務局
- その他当会の目的を達成するために必要な事業

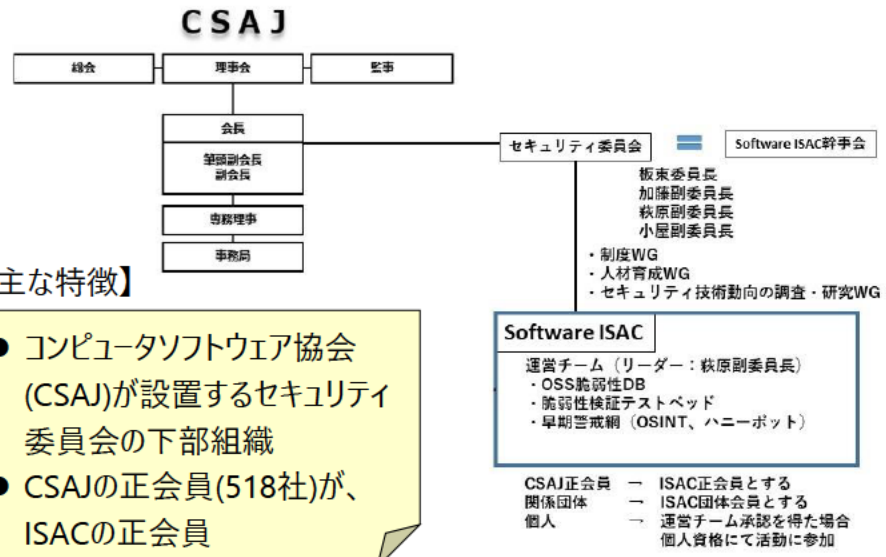
【主な特徴】
- 電力分野のセプター事務局として、重要インフラ事業者と政府機関との連携の役割を担っている
- 電気事業連合会内に事務所を構える
- 正会員は26社、特別会員1団体(電力広域的運営推進機関)
- サイバーセキュリティの確保に向けて国際的な協力関係を築くため、Electricity-Information Sharing & Analysis Center（E-ISAC）およびEuropean Energy-Information Sharing & Analysis Centre（EE-ISAC）との間で、覚書(MOU:Memorandum Of Understanding)を締結。

Software ISAC

【目的】 ソフトウェアのよりセキュアな開発や更新等が行えるように、「Software ISAC」を構築し、ソフトウェア開発や脆弱性管理等の工数最適化や、さらには日本のより安全・安心な社会への貢献を図る。

【活動概要】
- 国内ソフトウェア産業に必要な脅威情報や脆弱性情報の収集や分析
- 開発の上流工程でのセキュリティ仕様の組み込み
- 提供している製品やサービスに係る外部連携
- 新たな脅威および脆弱性情報の把握と発見

組織図



【主な特徴】
- コンピュータソフトウェア協会(CSAJ)が設置するセキュリティ委員会の下部組織
- CSAJの正会員(518社)が、ISACの正会員

出所）Software ISACの公表資料

③その他のISAC（米国におけるISACの取組）
活動しているISAC

■ 米国における ISAC の取組

- 政府、企業、国民のサイバーセキュリティを確保する上で情報共有は重要である。情報共有によって、迅速な対策の実施や被害を最小限に留めるといった効果が期待できる。米国においては、特に金融業界や通信業界において早い段階から情報共有に対する取り組みが行われており、これまでに多くの業界において情報共有のための取り組みが行われている。また、情報共有のためのガイドライン等が政府機関から公開されていることも情報共有に対する取り組みの後押しとなっていると考えられる。
- 情報共有の取り組みのうちの代表的なものとして、Information Sharing and Analysis Centers(ISAC) がある。米国においては、業界ごとにISACが創設され、業界の特性に応じた情報共有のための活動が行われている。2018年 3 月時点で活動しているISAC として、以下がある 。
  - Automotive ISAC
  - Aviation ISAC
  - Communications ISAC
  - Defense Industrial Base ISAC
  - Downstream Natural Gas ISAC
  - Electricity ISAC
  - Emergency Management and Response ISAC
  - Financial Services ISAC
  - Healthcare Ready

③その他のISAC（米国におけるISACの取組）
活動しているISAC

■ 米国における ISAC の取組

- Information Technology ISAC
- Maritime ISAC
- Multi-State ISAC
- National Defense ISAC
- National Health ISAC
- Oil and Natural Gas ISAC
- Real Estate ISAC
- Research & Education Network ISAC
- Retail Cyber Intelligence Sharing Center (R-CISC)
- Surface Transportation, Public Transportation and Over-The-Road Bus ISACs
- Water ISAC

各 ISAC の概要を以下に記載する。

③その他のISAC（米国におけるISACの取組）
各ISACの活動内容

■ Automotive ISAC (www.automotiveisac.com)

ネットワークデータ接続された自動車に関するサイバー脅威、脆弱性、ベストプラクティスに関する情報の共有を目的とする非営利組織で、完成車メーカー、サプライヤに対して、信頼できるコラボーション環境とプラットフォームを提供する。

■ Aviation ISAC (www.a-isac.com)

航空分野にフォーカスしたサイバー脅威、脆弱性、インシデントに関する情報共有を目的とする非営利組織で、脅威情報のリアルタイムでの共有、対処方法の提供、緩和策の実施、ベストプラクティスの導入等を行う。メンバーシップはグローバル航空会社に提供されている。

■ Communications ISAC (www.dhs.gov/national-coordinating-center-communications)

通信事業者、ISP、衛星通信事業者、放送事業者、ベンダ等に対して、物理およびサイバーに関するアラートを提供するために、脅威、脆弱性、侵入、アノマリに関する情報の収集、解析、共有を行うことを目的とする。

■ Defense Industrial Base ISAC (www.dibisac.net)

物理およびサイバーに関するイベント、脅威、侵入に関する情報の収集、解析、共有を行うことを目的とする。セキュリティ脅威、脆弱性、インシデントによるリスクを緩和するために、セキュリティベストプラクティスの共有を推進する。

■ Downstream Natural Gas ISAC (www.dngisac.com)

天然ガス事業者に対して、参加企業、政府機関、重要インフラ事業者間でのコミュニケーションを推進する。電力 ISACと協調して活動し、相互に情報を共有する。政府機関等から収集した、脅威に関する情報およびインディケータの解析、共有を行い、解析結果および、コーディネーションの提供を行う。

■ Electricity ISAC (www.eisac.com)

適時かつ信頼できる情報交換を通じて、状況認識、インシデント管理、コーディネーション、コミュニケーションのための機能を確立する。

③その他のISAC（米国におけるISACの取組）
各ISACの活動内容

■ Emergency Management & Response ISAC (www.usfa.dhs.gov/emr-isac)

緊急サービスセクタに関連する重要インフラ保護およびレジリエンスに関する情報の収集・解析と共有を目的とする。

■ Financial Services ISAC (www.fsisac.com)

サイバー脅威、脆弱性に関する情報共有、緊急事態対応計画の演習、迅速なレスポンスコミュニケーション、教育・研修、他の重要セクターや政府機関との協調を通じたグローバル金融サービスインフラストラクチャのレジリエンスと継続性の確保を目的とする。

■ Healthcare Ready (www.healthcareready.org)

サイバー脅威、脆弱性、インシデントに関する情報共有を目的とする。ソリューションの提供およびベストプラクティスの共有、教育・研修の提供を通じて、ヘルスケアサプライチェーンの強化、官民の協調によるレジリエンスの強化を図っている。

■ Information Technology ISAC (www.it-isac.org)

サイバー脅威情報の自動的共有と解析を行う脅威インテリジェンスプラットフォームを通じて、メンバーは多数の脅威インディケータへのアクセスが可能である。信頼できる解析、協調、コラボーションに基づく情報共有を通じて、メンバーは、リスク管理と意思決定を行うことができる。

■ Maritime ISAC (www.maritimesecurity.org)

船舶運行会社、クルーズ船運行会社、港湾設備運用事業者、ロジスティックス事業者、輸出入事業者および関連する事業者に対して、適時情報配信、業界特有の技術の開発、教育・情報提供を目的とするカンファレンスの開催を通じて、米国および国際における海運のセキュリティを向上させることを目的とする。

③その他のISAC（米国におけるISACの取組）
各ISACの活動内容

■ Multi-State ISAC (www.ms-isac.org)

州政府、地方自治体等を対象とする、サイバー脅威保護、対応、回復に関する中心的な組織。セキュリティオペレーションセンターが、リアルタイムのネットワーク監視、早期サイバー脅威警告・アドバイザリ、脆弱性緩和、インシデント対応サービスを提供する。

■ National Defense ISAC (www.ndisac.org)

軍事産業とそのパートナーを対象として、サイバー脅威情報、ベストプラクティス、緩和戦略に関する情報を共有するためのコミュニティやフォーラムを提供することを通じて、国防セクターのセキュリティおよびレジリエンスを強化することを目的とする組織。

■ National Health ISAC (www.nhisac.org)

保健セクターのレジリエンスおよび継続性を確保するために、物理およびサイバーに関する脅威、インシデント、脆弱性、リスクに関する情報および、それらへの対応を行うための情報の共有を行うための信頼できるコミュニティを提供する。

■ Oil & Natural Gas ISAC (www.ongisac.org)

石油・天然ガス事業者に対して、匿名での情報共有を行うためのメカニズムの提供やサイバーインテリジェンスの解析・共有を通じて、サイバーセキュリティ態勢の向上を支援することを目的とする。

■ Real Estate ISAC (www.reisac.org)

テロリストに関する脅威、警告、インシデント、脆弱性、対応計画に関する情報の共有を通じて、商業施設およびその利用者・従業員を保護することを目的とする。メンバーには、宿泊施設、オフィスビル、小売店舗、賃貸住宅、リゾート施設の所有者および運用者が含まれる。

③その他のISAC（米国におけるISACの取組）
各ISACの活動内容

■ Research & Education Network ISAC (www.ren-isac.net)

高等教育機関、研究機関を対象として、リスク管理、サイバー脅威およびサイバーセキュリティに関する情報共有サービスを提供する。Security Event System を使用して、脅威インテリジェンス情報の追跡・統合を行い、脅威・イベントへの対応におけるメンバーの意思決定を支援する。

■ Retail Cyber Intelligence Sharing Center (R-CISC) (www.r-cisc.org)

小売業者、消費者向け製品・サービス組織およびサイバーセキュリティ業界のパートナーを対象として、コラボーション、脅威インテリジェンス、協調を行うためのサイバーセキュリティコミュニティである。メンバーは、脆弱性、インシデント、脅威および関連する脅威是正措置に関するサイバーインテリジェンスを共有する。

■ Surface Transportation, Public Transportation and Over-The-Road Bus ISACs

(www.surfacetransportationisac.org)

セクターに特化したサイバー脅威、脆弱性、インシデントに関する情報を収集・解析し、アラートを発信するとともに、インシデントレポートを発行する。サイバーセキュリティ、物理セキュリティ、自然災害に関する情報の交換・共有のための信頼できる電子的手段を提供する。

■ WaterISAC (www.waterisac.org)

セキュアウェブポータル、ニュースレターの発行、アラートの発信、ウェビナーの配信、リスク管理・緩和・レジリエンシーに関するガイドラインの提供等を通じて、上下水道セクターの物理セキュリティ・サイバーセキュリティの強化、災害からの復旧能力の強化、総合的な準備態勢およびレジリエンシーの改善を支援すること目的とする。

1．ビルガイドラインの高度化のための調査
①空調等のビルの個別設備システムの対応策に関する調査
②スマートビルのサイバーセキュリティ対策を意識したユースケース調査
③その他関連する調査
③－１　インシデントレスポンスに対する要求の整理
③－２　ガイドラインへの追加情報の充実化
③－３　ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討

2．ビルシステムのサイバーセキュリティ推進体制の調査
①推進体制の情報提供・共有・相談等の機能の実践的評価
②推進体制のあり方の調査

3．検討会の運営
①ビルSWGの運営
②作業グループの運営
③その他の運営

3．検討会の運営
①ビルSWGの運営

■ ビルSWGについては、本事業期間内に 1 回開催した。開催経緯とスケジュールを以下に示す。

■ 第11回会合では、事前の準備として構成員の出欠確認や参加者の取りまとめを行うとともに、会合後は、議事要旨の作成や謝金等の支払いを行った。第11回会合の資料については参考資料 4 、議事要旨については、参考資料 5 に取りまとめる。

会合	開催日時	主な議題
第11回会合	2021年3月22日（月） 10:00～12:00	● ガイドライン・個別編（空調編）の検討について ● 構成員よりの発表（ICSCoE ビル有志・森ビル佐藤様） ● その他報告事項 　• ガイドライン 2 年間の振り返りと課題の共有 　• インシデントレスポンスの検討に向けて 　• レポジトリの充実化について ● 自由討議

ビルSWGの構成員

区分		構成員
有識者		（座長） 江崎 浩 東京大学 教授 松浦 知史 東京工業大学 准教授 技術研究組合制御システムセキュリティセンター ICSCoE 2 期ビルチーム有志
ビルオーナー・関連業界団体		イーヒルズ株式会社 日本生命保険相互会社 三井不動産株式会社 三菱地所株式会社 一般社団法人日本ビルヂング協会連合会 一般社団法人不動産協会
建設事業者	ゼネコン	鹿島建設株式会社 株式会社竹中工務店
	サブコン	株式会社九電工 株式会社きんでん
設計事務所		株式会社日建設計
各設備ベンダー・関連業界団体	ビルディングオートメーションシステム	アズビル株式会社 三菱電機株式会社／三菱電機インフォメーションネットワーク株式会社 一般社団法人ビルディング・オートメーション協会
	空調システム	ダイキン工業株式会社
	エレベータ	株式会社日立製作所／株式会社日立ビルシステム
	監視システム	セコム株式会社
	ネットワーク	株式会社NTTファシリティーズ／NTTコミュニケーションズ株式会社／日本電信電話株式会社
その他(自治体)		横浜市

ビルSWGのオブザーバー

オブザーバー	
国土交通省	大臣官房官庁営繕部設備・環境課
	不動産・建設経済局建設業課
	不動産・建設経済局不動産業課
	住宅局住宅生産課
	総合政策局情報政策課
内閣官房	東京オリンピック競技大会・東京パラリンピック競技大会推進本部事務局
内閣サイバーセキュリティセンター	東京2020グループ
公益財団法人東京オリンピック・パラリンピック競技大会組織委員会	
中部国際空港株式会社／中部国際空港施設サービス株式会社	

1．ビルガイドラインの高度化のための調査
①空調等のビルの個別設備システムの対応策に関する調査
②スマートビルのサイバーセキュリティ対策を意識したユースケース調査
③その他関連する調査
③－１　インシデントレスポンスに対する要求の整理
③－２　ガイドラインへの追加情報の充実化
③－３　ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討

2．ビルシステムのサイバーセキュリティ推進体制の調査
①推進体制の情報提供・共有・相談等の機能の実践的評価
②推進体制のあり方の調査

3．検討会の運営
①ビルSWGの運営
②作業グループの運営
③その他の運営

3．検討会の運営
②作業グループの運営

■ 作業グループについては、本事業期間内に 4 回開催した。開催経緯とスケジュールを以下に示す。

■ ビルガイドラインの個別編：空調システムの検討や国際連携に向けた検討、インシデントレスポンスの検討、ビルサイバー推進体制についての検討、ガイドラインの内容補足に向けた検討について、調査・検討の方向性や調査・検討内容の議論を行い、その成果を取りまとめた。

作業グループ	開催日時	主な議題
第１回作業グループ	2021年3月8日（月） 17:30～19:00	● インシデントレスポンスに対する要求の整理 ● ビルシステムのサイバーセキュリティ対策に関する国際動向の調査
第２回作業グループ	2021年3月11日（木） 13:00～15:00	● ビルシステムのサイバーセキュリティ対策に関する国際動向の調査 ● ビルオーナー個別ヒアリングの報告 ● インシデントレスポンスに対する要求の整理
第３回作業グループ	2021年3月17日（木） 15:00～17:00	● 個別編：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空調システム
第４回作業グループ	2021年3月23日（火） 15:00～17:00	● ビルSWGで出た意見の整理 ● ビルシステムのサイバーセキュリティ対策に関する国際動向の調査 ● レポジトリ ビルシステム・ネットワークの構成管理

作業グループのメンバー

区分		メンバー
ビルオーナー・関連業界団体		イーヒルズ株式会社
建設事業者	ゼネコン	株式会社竹中工務店
	サブコン	株式会社九電工 株式会社きんでん
各設備ベンダー・関連業界団体	ビルディングオートメーションシステム	アズビル株式会社 一般社団法人ビルディング・オートメーション協会
	空調システム	ダイキン工業株式会社 日立ジョンソンコントロール空調株式会社
有識者		技術研究組合制御システムセキュリティセンター ICSCoE 2 期ビルチーム アライドテレシス株式会社 株式会社野村総合研究所 NRIセキュアテクノロジーズ株式会社

1．ビルガイドラインの高度化のための調査
①空調等のビルの個別設備システムの対応策に関する調査
②スマートビルのサイバーセキュリティ対策を意識したユースケース調査
③その他関連する調査
③－１　インシデントレスポンスに対する要求の整理
③－２　ガイドラインへの追加情報の充実化
③－３　ビルシステムのサイバーセキュリティ対策に関する国際動向の調査とガイドラインの国際展開方策の検討

2．ビルシステムのサイバーセキュリティ推進体制の調査
①推進体制の情報提供・共有・相談等の機能の実践的評価
②推進体制のあり方の調査

3．検討会の運営
①ビルSWGの運営
②作業グループの運営
③その他の運営

3．検討会の運営
③その他の運営

■「ビルオーナー・関連団体」、「ゼネコン・サブコン・設計事務所」、「ベンダー・関連団体」の３つの業界ごとに、グループヒアリングを計５回実施し、ガイドラインの活用方法やガイドラインの活用上の課題、セキュリティ情報の配信の活用方法等について把握した。

ビルオーナー・関連団体グループインタビュー

会合	開催日時	参加メンバー
第１回会合	2021年３月11日（木）9:00～	イーヒルズ、三菱地所、日本生命、日本ビルヂング協会連合会、不動産協会
第２回会合	2021年３月19日（金）9:00～	イーヒルズ、三井不動産、横浜市

ゼネコン・サブコン・設計事務所グループインタビュー

会合	開催日時	参加メンバー
第１回会合	2021年３月17日（水）17:00～	鹿島建設、竹中工務店、きんでん、日建設計

ベンダー・関連団体グループインタビュー

会合	開催日時	参加メンバー
第１回会合	2021年３月12日（金）10:00～	アズビル、ダイキン工業、日立ビルシステム、日立ジョンソンコントロールズ空調、ジョンソンコントロールズ、ビルディング・オートメーション協会
第２回会合	2021年３月17日（水）11:00～	ダイキン工業、日立製作所、、日立ビルシステム、日立ジョンソンコントロールズ空調、ジョンソンコントロールズ、ビルディング・オートメーション協会、三菱電機、CSSC


Share the Next Values!

資料3-1

（案）
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）

（2021.3.22 版）

令和３年ｘ月ｘｘ日

産業サイバーセキュリティ研究会

ワーキンググループ 1(制度・技術・標準化)

ビルサブワーキンググループ

変更履歴

発行日	版	概要
2021 年ｘ月ｘｘ日	第１版案（パブコメ版）	パブコメ版発行

目次

図表

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）の策定にあたって

- ビルのサイバーセキュリティについては、これまではビルシステムを構成する制御系がインターネットと切り離されていることや、ビルシステム特有のプロトコル（通信手順、通信内容を解釈するための決まり事）を使っているために攻撃の対象となりづらい、ビルシステムがマルチステークホルダ（多種多様な関係者が関与する構造であること）であり、ビルシステムのサイバーセキュリティ全体を統合管理する体制を組織しづらい等を理由にして対策が遅れている傾向があった。

- しかしながら、サイバー攻撃のレベルの向上により、特有のプロトコルであることをもって攻撃の対象から外れることはなくなってきている。また、利便性の向上の観点からインターネットに繋がるケースが増えてきており、外部との接続を前提にした設計も増加している。

- 世界的に見てもビルシステムを対象としたサイバー攻撃が実際に発生している。

- 一方で、ビルシステムの特徴としてステークホルダ（何らかの利害関係を持つ関係者）が多数存在しており、これらのステークホルダが共通に参照できるサイバーセキュリティ対策のガイドラインが存在していないため、サイバーセキュリティ対策を進める方向性が示されていない。

- こうした問題意識から、2018 年 2 月、産業サイバーセキュリティ研究会 WG1 の下に、ビルシステムに関わる多数のステークホルダが一堂に会し、それぞれの視点も考慮して、ビルシステム向けのサイバーセキュリティ対策について議論を行うビルサブワーキンググループを設置し、検討を行ってきた。

- この検討の成果は、令和元年 6 月 17 日に「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第 1 版」として公開され、ビルシステムに対するサイバーセキュリティ対策向上のために活用されるに至っている。

- このガイドラインは、ビルに導入される様々なシステムに対するサイバーセキュリティ対策の共通編として作成されたもので、このガイドラインの活用をさらに推進するため、個別のサブシステムの状況に特化して配慮すべきことを、今回新たに個別編としてとりまとめた。今回はその第一弾として空調システムを取り上げてサイバーセキュリティ対策の要件をまとめている。

- 今後、本ガイドライン第一版（共通編）と併せて、個別編：空調システムが、ビルシステムや特に空調システムに関わる多数のステークホルダに広く活用され、ビルシステムのサイバーセキュリティ対策が少しでも進むことを期待するものである。

1. はじめに

1.1. ガイドライン（個別編：空調システム）を策定する目的

ビルシステムのサイバーセキュリティ確保のためのガイダンスとして、「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第 1 版」が、令和元年 6 月 17 日に公開され、活用されている。

このガイドラインは、ビルシステムを構成する全てのサブシステムにおける共通的なセキュリティ対策が含まれた共通編として作成され、ビルの関係者が共通に参照し、ビルシステムについての初歩的なサイバーセキュリティ対策を考えていく上での入り口となる情報を提供することを目指したものである。

ガイドライン（共通編）の位置づけ：

- ガイドラインはマスト（レギュレーション）ではないものにする。ビルシステム関係者が何を優先して対策していくか決めるための情報を提供する。
- 対象者は、ビルオーナー、ゼネコン／サブコン、設計者、設備ベンダ、管理者等、ビルの企画・建設から運営管理に関わるステークホルダ全般とする。
- 共通編は初歩的な対策をまとめたものであり、厳し過ぎず、ポイントを押さえたものにする。
- 設計やテスト等の各段階のチェックプロセスについて、関係者間の共通リファレンスを作る。

これに対し、個別のサブシステムに特化した内容については、各サブシステムごとの個別編として別途まとめていくこととしている。

その第一弾として空調システムを対象に、共通編を超える部分についての詳細な方策や更なるセキュリティ投資に関する経営判断の材料を提供する要件をとりまとめた。なお、個別編は各サブシステム特有の要件を共通編との差分として抜き出したものであり、全体に共通する要件については、共通編をあわせて参照して欲しい。

1.2. 対象とする空調システム

空調システムの特徴として、対象とするビルの規模（大規模ビル、中小規模ビル）、利用形態（オーナービル、テナントビル）、用途（オフィスビル、病院、公共施設、データセンタ等）により、設置される空調システムが異なり、サイバーセキュリティ対策として考慮すべき点も異なってくる。

延べ床面積が1万㎡を超える大規模ビルには、「セントラル空調方式」が導入される場合が多い。一方、1万㎡以下の中小規模ビルにおいては、「個別分散空調方式」が導入される場合が多い。近年では、1万㎡を超える大規模ビルにおいても、個別分散空調

方式が採用されることも増えてきた。また、空調方式の特徴を生かすために、空調負荷が大きい大規模空間にセントラル空調方式を採用し、空調負荷変動を吸収するために、個別分散空調方式を併設するような物件も増えてきている。

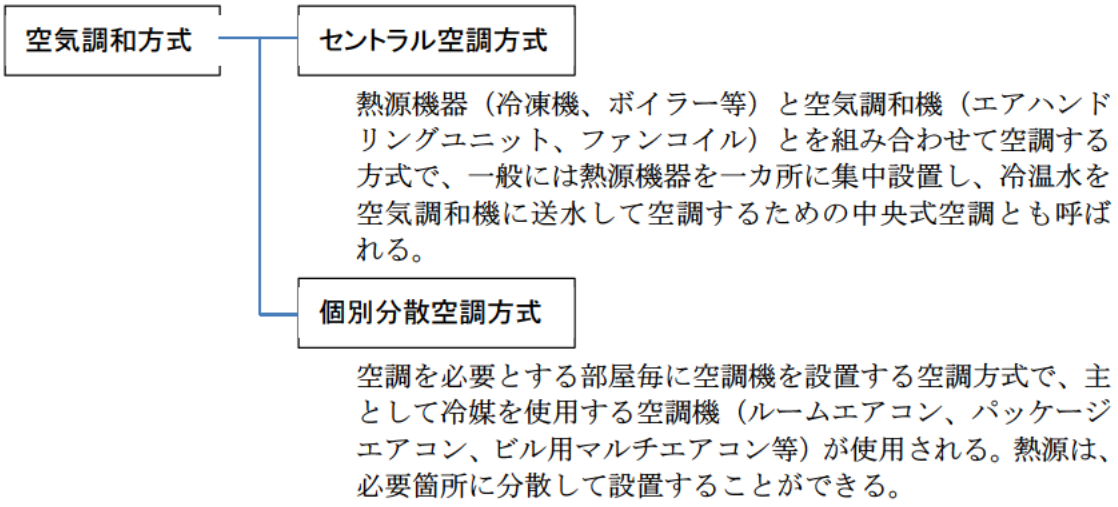
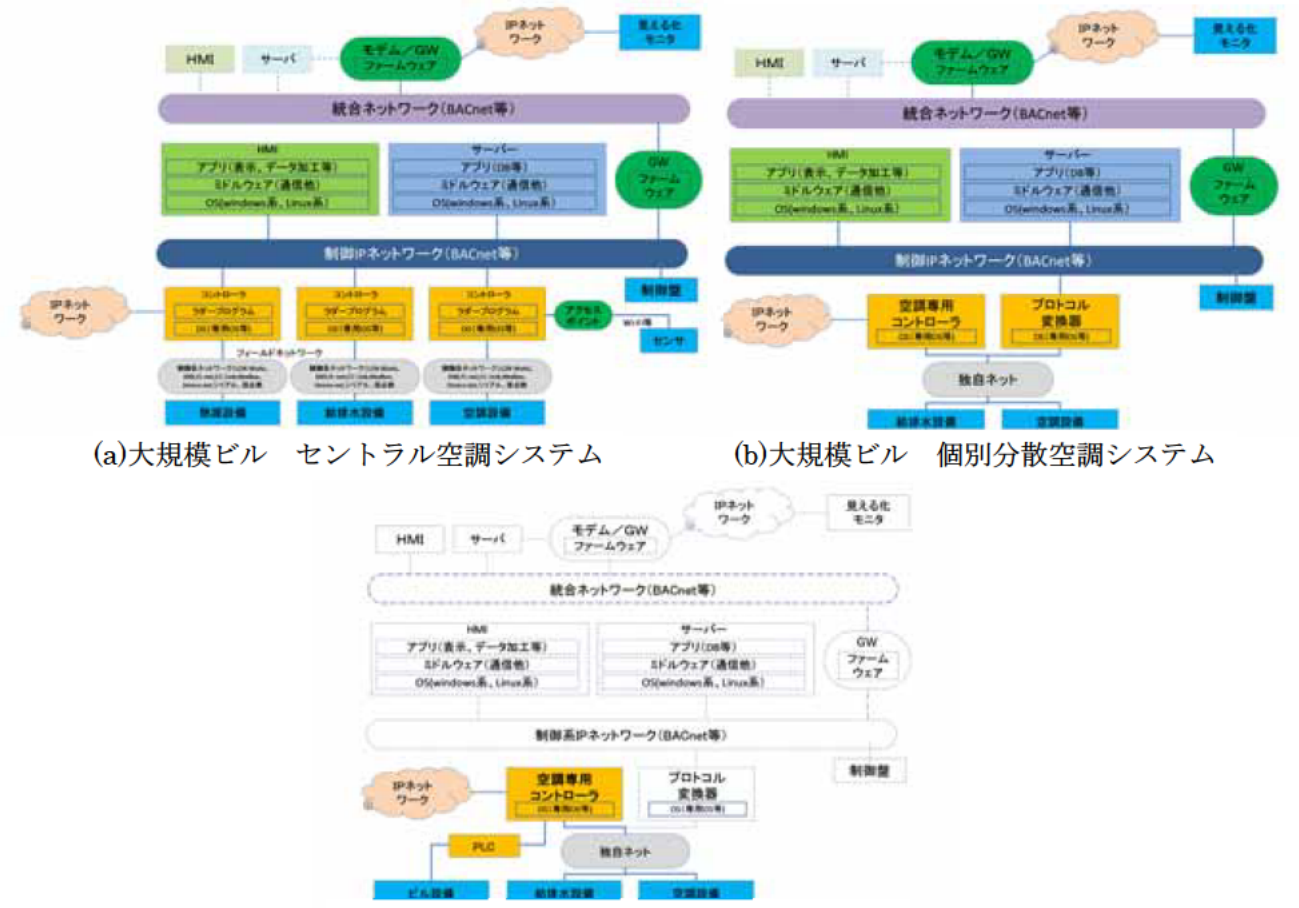


図 1-1　空調システムの違い

大規模ビルにおいては、中央監視装置が設置され、空調システムを監視制御している。中央監視装置とは、セントラル空調方式（**図 1-2** (a)）では、熱源設備、給排水設備、空調設備が、制御 IP ネットワークを介して接続されている。個別分散空調方式（**図 1-2** (b)）では、プロトコル変換ゲートウェイが制御 IP ネットワークを介してのみ接続されており、接続箇所が限定されていることがセキュリティ対策の実施には優位である。

中小規模ビルでは、中央監視装置が設置されない場合が多く、空調専用コントローラが、ビル全体の空調システムを監視制御しており、空調以外のビル設備の異常監視等を行う場合もある。（図 1-2（c））



(a)大規模ビル　セントラル空調システム　　(b)大規模ビル　個別分散空調システム

(c)中小規模規模ビル　個別分散空調システム

図 1-2　ビルの規模と空調システム

2. 空調システムを巡る状況

2.1. 空調システムで起こりうる攻撃パターンと対応の考え方

ビル設備、あるいは空調システムがサイバー攻撃を受け、空調システムに被害が出ている場合、サイバー攻撃を停止させ、被害を回避する方策は重要であるが、並行していち早い空調機能の回復を実施すべきである。データセンタのサーバ室や病弱者が収容された病院、極寒地のホテル等、空調機能を消失することによって深刻なダメージを受ける場合もあり、サイバー攻撃への対策と同時に、空調システムの回復方法を設計時点から盛り込んでおくことが重要となる。

統合ネットワークおよび制御 IP ネットワークから空調機に向かって不正に侵入された場合を想定し、構成している複数制御機器が、逐次一つずつ制御不能になった場合を挙げて、空調システムが受けるサイバー攻撃のパターンを以下に列挙する。

① 上位システムの HMI が攻撃され、空調システムの動作モード、温度設定値等を書き換え、本来の動作から逸脱させてしまう。
② 統合ネットワークに接続された機器を攻撃し、統合ネットワークの通信トラフィックオーバーフローが発生し、上位システムから空調システムの監視制御が出来なくなる。
③ 上位ネットワークと統合ネットワークを接続する G/W がサイバー攻撃を受け、G/W が機能しなくなり上位システムから空調システムの監視制御が出来なくなる。
④ 空調システムの制御コントローラのファームウェアが改竄され、空調システムが機能しなくなる。

これらの具体的な事例を以下に紹介する。

2.2. 実際のサイバー攻撃事例

ビルシステムがサイバー攻撃を受けた際に、統合ネットワークや制御 IP ネットワーク等の基幹ネットワークのトラフィックが増大することで、空調システムの動作に異常をきたす場合が報告されている。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。

また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べきである。さらに、空調機能維持が特に重要である場所については、空調機システムのダウンに対応するため、空調機を二重化して設置することも考慮するべきである。

なお、セントラル空調方式は、複数の設備機器が連動したシステムであり、空調機のみの二重化や復旧では空調システムを維持できない場合もある。上位ネットワークから切り離された場合の各設備機器の制御と連動や、居室等需要側での設定値変更の可・不可について把握し、各コントローラが自律的に行う制御や手動操作で最低限必要なレベルの空調を動作できる設計および体制を構築しておくことが重要である。

2.2.1. ネットワークビジーで中央監視盤がシステムダウンした事例

あるビルにおいて、空調監視制御システムを新規設置する際に、試運転作業用 PC をネットワークにつないだところ、膨大なブロードキャストパケットがネットワークに流れて、それらを受信した中央監視盤がシステムダウンした。作業に使用したPCからは、マルウェア等は発見されなかった。

ビル内のネットワークケーブルの閉ループが形成されていたことが原因で、サイバー攻撃というよりは作業ミスが原因だが、このような場合には、膨大なパケットが発生する可能性があり、意図的な攻撃も成立しえる状況である。作業に使用したPCのセキュリティ・チェックのエビデンスが残っていなかったため、作業用 PC が原因である疑いを否定できず、原因究明までに時間を要した。このような異常が発生した場合には、作業履歴のチェック、設備機器故障のチェック、設置環境のチェック等想定される要因を並行して確認するため、まずは現状復帰が優先され、異常原因を切り分けての明確な原因究明ができない場合が多い。このような事態を避けるために、設備機器や設備の設置状況の履歴、復旧作業に使用する機器のセキュリティ・チェックのエビデンスを残しておき、原因究明にあたることが重要である。

2.2.2. 空調機コントローラが不正アクセスによりデータを消失した事例

ある施設の空調機を遠隔監視制御する空調専用コントローラが、インターネットから不正アクセスを受け再起動した。この結果、空調専用コントローラが、保持していた収集データ、設定値を消失した。

空調専用コントローラは空調機の運転状況データを収集し、定期的にサーバにアップロードするが、再起動するとアップロード待ちの保持データは消失してしまう。このため、サーバ上の収集データに一部欠損が発生した。空調専用コントローラをインターネット接続する際には、ネットワークに対するセキュリティを確保する旨を仕様書には記載していたが、実物件ではそれが守られずにインターネット上から直接アクセス可能な状態になっていた。機器が想定しているセキュリティ対策は、運用環境で守るべきセキュリティ対策の順守が前提であり、これを怠ると、セキュリティホールが発生してしまう。

2.2.3. 空調監視用端末がマルウェア(ランサムウェア)に感染した事例

ある中小規模ビル内の空調機を監視制御する為の空調専用コントローラがランサムウェアに感染し、空調システム監視用プログラムが起動できなくなった。中小規模ビルでは、設備監視室を設置しない場合もあり、空調専用コントローラへの操作アクセス管理が不十分で、オペレータの限定や動作ソフトの限定が十分でない場合がある。このような運用状態では、空調専用コントローラがサイバー攻撃にさらされる可能性が有る。これを避けるためには、不特定多数の人間が操作できる場所への設置を避け、オペレータを限定することで、不要なネットワークアクセスを制限することが重要である。また空調専用コントローラも、USB ポートなどの汎用的なインタフェースを物理的、論理的に制限する対策を実施しておくことが重要である。

3. 空調システムにおけるサイバーセキュリティ対策の考え方

空調システムにおいても、共通編で整理された、サイバーセキュリティ対策のスキームに従って、空調システムの明確化、インシデントや、被害レベルの設定、リスク特定を行うことは重要である。

ビルにおける空調システムは、他の設備と同様に、統合ネットワーク上の HMI から制御されている。HMI がハッキングされ空調システムに異常値が設定された場合、空調システムは、設定値が動作範囲であれば空調環境を変化させてしまう。データセンタや冷凍倉庫、病院の ICU 等、温度維持が重要な施設においては、空調温度が正常範囲であることを監視し、正常範囲を逸脱した場合に、その異常を検出する装置をオフラインで別途設置し、更に空調を正常に稼働できるよう設計時に配慮しておく必要がある。

データセンタや人命に関わる医療施設等、空調システムの停止が、たとえ短時間であっても、多大な被害を発生する場合がある。このような施設においては、異常発生の検出時間、空調システムの復旧対策時間が、対策の重要なポイントになる。施設に要求される検出時間、対策時間は、システム設計時に想定し、復旧対応に必要な設備を設置当初から導入しておくべきである。

また、空調システムは、ビルの運用が始まると、使用状況の変化に応じ、ビルの間仕切り変更への対応、用途変更に応じる居室の空調能力強化のため個別分散空調の追加等、空調システムの構成が変更される場合がある。このため、設計時点や建築段階でのセキュリティ対策は、ビル運用の変化に応じ、逐次見直す必要がある。

近年の空調システムでは、IP ネットワーク経由で、空調の運用データ、室温データを収集し、省エネや室内環境の改善などに利用している。この場合、空調システムの各種設定を変更しながら、室内環境改善、運用改善を実行している。このような運用では、空調システムが、室内状況の計測データ、変更した制御パラメータを逐次収集し保持している。

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、失われる可能性が有る。従って、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。

空調方式により、ビルネットワークへの接続形態が異なっているため、空調方式毎に異なるサイバーセキュリティ対策が必要である。ここでは、空調方式毎に考慮すべきサイバーセキュリティ対策の考え方を示す。

3.1. セントラル空調方式のセキュリティ対策

重要設備においては、サイバー攻撃で上位の HMI 経由で空調システムの温度設定を変更される事を、現場で操作ミス・認識違いに依る誤操作等が起こる場合と同様に

想定すべきである。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の実装やコントローラをネットワークから分離またはネットワークを介さずに、現場で手動操作で対応できる体制を構築しておく必要がある。

セントラル空調方式は、設計の自由度が高く多数の機器メーカの商品から構成されており、一度異常が発生すると、その原因の切り分けには、膨大な時間を要することが多い。従って、システムに異常が発生した場合には、サイバー攻撃、機器故障の両面からその原因究明を円滑に進められる作業手順を、事前に準備しておくべきである。

セントラル空調方式で、空調・熱源を制御するコントローラは、上位と設定値やスケジュールのやりとりをする熱源機器と二次側機器を相互接続する GW を介してインターネット上のサーバと通信をするなど、IP ネットワーク対応が当たり前となっていること、専用コントローラ或いは汎用コントローラに、Linux、windows ベースのコントローラが増加していることから、IP ネットワークを介した攻撃の可能性を考慮し物理的なセキュリティの対策を施すべきである。

コントローラの中にはコントローラメーカが遠隔から監視制御できる機能をもったコントローラも存在しており、制御 IP ネットワークを経由することなく、直接外部クラウドに接続するコントローラも登場している。こうした遠隔からコントローラを監視制御するネットワークセキュリティに関しては、不要なユーザーがアクセスできるようになっていないか、不要なデータのやり取りをしていないか、不要な設定変更ができるようになっていないか等について十分注意を払う必要がある。

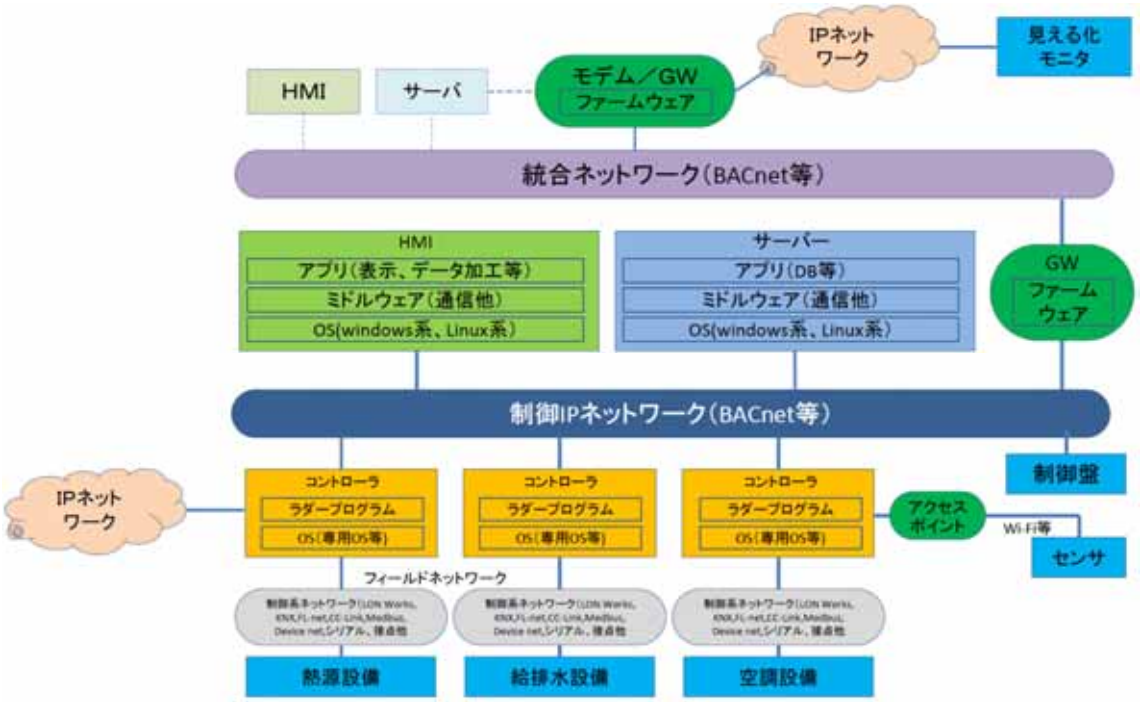


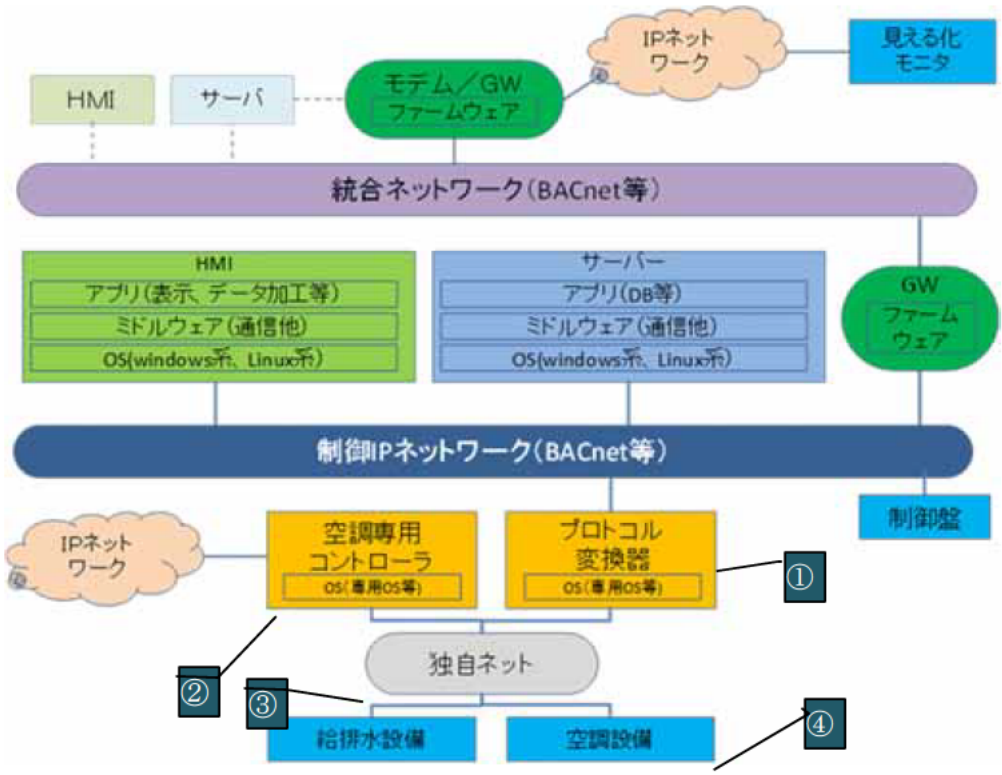
図 3-1　セントラル空調システムのネットワーク接続

3.2. 個別分散空調方式のセキュリティ対策

重要設備においては、サイバー攻撃で上位の HMI 経由で空調システムの温度設定を変更された場合を想定し、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 からの異常値設定の際には、その設定操作を無視できる機能（設定値上下限監視）を実装しておく必要がある。

大規模ビルに設置される個別分散空調システムは、セントラル空調システム同様、中央監視盤によって監視制御が行われる。個別分散空調システムも、ビルに設置された制御 IP ネットワークの通信プロトコルに合わせたプロトコル変換器を経由して、ビルの統合ネットワークに接続される。このプロトコル変換器は、専用プログラムによる組込み型の機器や、Linux、windows ベースの機器で構成されている。これらのコントローラを空調メーカが遠隔から監視制御するものも増加しており、制御 IP ネットワークを経由することなく、直接外部クラウドに接続するコントローラも多い。コントローラとメーカの外部クラウドを繋ぐネットワークに関しては、十分なセキュリティ対策を行う必要がある。

これらの機器は、サイバー攻撃の標的に成りえるため、システムの設計段階でサイバー攻撃を受けた場合を想定し、万一の攻撃の際にも、空調機能を消失しない安全設計を行う必要がある。



プロトコル変換器 ： 空調システムを上位の制御ネットワークの通信プロトコル（BACnet 等）で監視制御できるように、プロトコル変換する装置

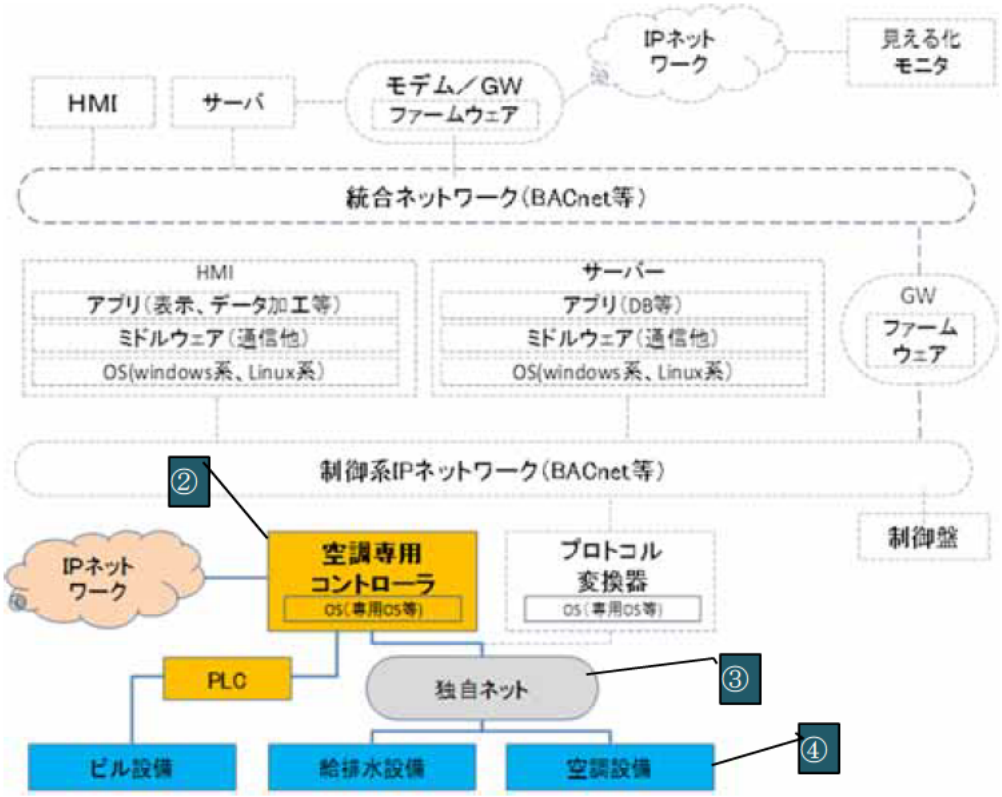
① 空調専用コントローラ ： 中央監視盤から空調システムの制御監視ができない場合、プロトコル変換器をネットから取り外した際に、空調システムを監視制御する装置。

② 独自ネット ： 空調機の室外機と室内機を繋ぐネットワークで、メーカ毎に異なる独自の通信プロトコル、電気信号を使う。

③ 空調設備 ： 複数の室内機、室外機、制御コントローラから構成され、空調システムとしては、これで完結した空調動作、制御ができる。

(a) 大規模ビル 個別分散空調システム

また、中小規模ビルにおいては、上位の中央監視盤を設置しない場合が多く、空調専用コントローラが、他のビル設備の異常信号を監視するようなシステムを構築する場合がある。また、空調専用コントローラが、ビルの統合ネットワーク経由でクラウドサービスに接続される場合もある。従って、空調専用コントローラの運用に関して、セキュリティ対策の観点から、一層厳格な運用が求められる



② 空調専用コントローラ　：　中小規模ビルでは、空調システム以外の設備からも異常の移報を受けビル全体を監視制御する装置

③ 独自ネット　：　空調機の室外機と室内機を繋ぐネットワークで、メーカ毎に異なる独自の通信プロトコル、電気信号を使う

④ 空調設備　：　複数の室内機、室外機、制御コントローラから構成され、空調システムとしては、これで完結した空調動作、制御ができる

(b) 中小規模ビル　個別分散空調システム

図 3-2　個別分散空調システムのネットワーク接続

3.2.1. 個別分散空調システムのセキュリティ対策事例

ビルに設置された空調設備が、サイバー攻撃の標的になった場合、設定した空調環境から逸脱した異常状態を認識した場合に初めて、サイバー攻撃を受けた可能性が生まれる。従って、異常状態が発生していないかを常時監視し、万一異常状態の発生を認識した場合に、サイバー攻撃の有無を確認し、対応を行う。

3.2.1.1. 空調システムの管理

① 空調システムの設置状態の管理

ビルの運用変更に応じ、部屋の間仕切り変更、空調能力増強のため空調機の増設を行う事がある。このような変更に対応し、各室の空調機の設置状態、監視制御系統のネットワーク接続状態を常に把握し管理しておく。

② 空調状態の運用状態の管理

- 空調維持が重要な場所では、空調状態をオフラインで温度計測し許容された温度範囲に維持されていること監視し、異常が無いかを確認する。
- 中央監視装置から空調機を監視制御している場合、運転状態、運転モード、設定温度など空調に関わる設定値に異常が無いかを確認する。
- 空調機のデータを収集している場合、収集したデータに抜け等の異常が無いかを確認する。

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。

③ 異常発生時の対応

③-1 中央監視盤のサイバー攻撃を想定する(図 3-3 (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。

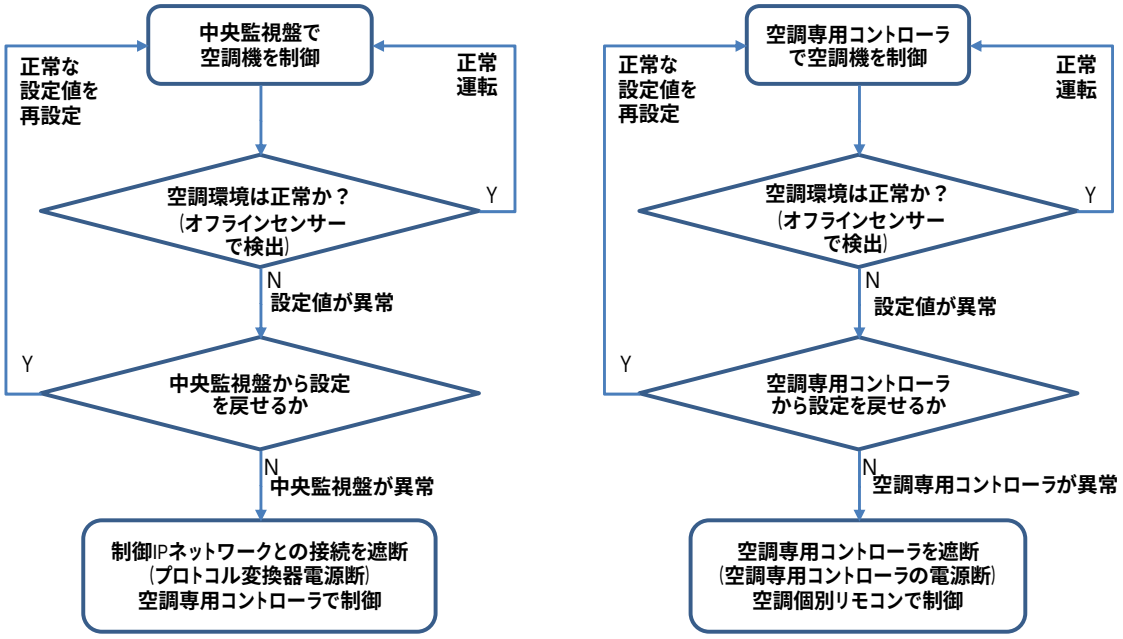
B) 空調監視盤から空調設定温度を再設定できない場合には、制御 IP ネットワークに接続しているプロトコル変換器(コントローラ)を遮断(電源 off)し、空調専用コントローラによる制御に切り替える。

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 3-3 (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)し、空調個別リモコンによる制御に切り替える。

③-3 空調個別リモコンで制御できない場合は、空調機器の故障として処理する。(図 3-4)



a） 中央監視制御盤での監視　　b） 空調専用コントローラでの監視

図 3-3　サイバー攻撃対応フロー

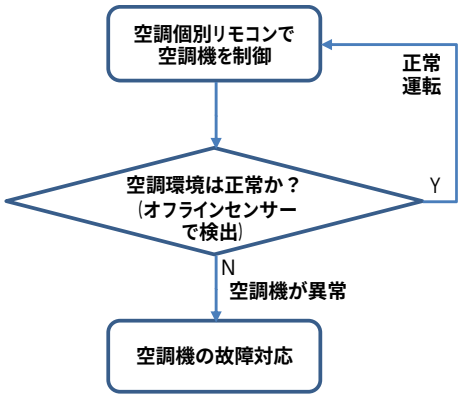


図 3-4　空調機の故障フロー

4. ビルシステムにおけるリスクと対応ポリシー

4.1. 空調システムの管理策

空調システムに関連する設備のセキュリティインシデント、リスク源、セキュリティポリシー（対策要件）を前述のサイバー攻撃対応フローで示した中央監視制御盤および空調専用コントローラの2つに分け、さらに保守用持ち込み端末を加えた 3 つのパターンで整理したものを表 4-1　空調システムのビルシステムのリスクと対策ポリシー表にまとめた。

表 4-1　空調システムのビルシステムのリスクと対策ポリシー

	セキュリティインシデント	リスク源	セキュリティポリシー
6.空調システムを巡る状況			
60	空調システム		
(1)	設置した空調機自体が運転できない状態になる。	設置された空調機への電源や通信線が外される。	・重要な場所を空調する機器（セントラル空調方式の場合は各設備機器）は、不特定多数の者が容易に近づいて操作できる場所に設置しない。
(2)	中央監視盤がサイバー攻撃を受け、空調システムが制御不能となり、空調環境を維持できなくなる。	空調制御システムへのサイバー攻撃により、空調用制御システムがダウンしてしまう。	**分オーダーで空調を復旧させたい場合（例：データセンタ、ICU等）** ・空調システムを二重化し正常動作可能な機器で空調を維持する。 ・空調専用コントローラを併設する。 ・居室単位に個別リモコンを設置する。
			数時間オーダーで空調を復旧させたい場合（例：冷凍倉庫等） ・空調専用コントローラを併設する。 ・居室単位に個別リモコンを設置する。

	セキュリティインシデント	リスク源	セキュリティポリシー
			<u>セントラル空調の場合</u> ・空調制御システムを動かすために必要な設備機器や制御を事前に把握し、空調用制御システムのダウンに繋がる要因について、共通編を参考にリスクおよびポリシーを決定する。 ・さらに、各コントローラが自律的に行う制御や手動操作で最低限必要なレベルの空調を動作できる設計および体制を構築する。
(3)	中央監視盤がサイバー攻撃を受け、空調システムからのデータ収集ができなくなる。	制御 IP ネットワークへのサイバー攻撃で、大量のデータが流れるなどにより、空調制御のデータ送受信に支障をきたす状態が発生する。	・収集データの欠損が問題になる計測時間以内の間隔で、サーバにデータバックアップを実施する。
61	**空調専用コントローラ**		
(1)	メーカークラウドへのアクセスの際に、サイバー攻撃を受ける。	メーカークラウドへのアクセスの際にネットワークセキュリティの確保ができていない。	・メーカークラウド、空調専用コントローラ間の識別・認証を適切な方法で行う。
(2)	USB 経由や、外部アクセスにより不正接続や攻撃を受ける。	一般ユーザーが、空調システム用監視盤を意識せず、USB を使った内部データの取り出し、ネット検索等の操作を行ってしまう。	・ウイルス感染やネットワークからの不正アクセスを防ぐ為に、不必要なインタフェースを制限する。
(3)	中央監視盤がサイバー攻撃を受け、空調システムからのデータ収集ができなくなる。	制御 IP ネットワークへのサイバー攻撃で、大量のデータが流れるなどにより、空調制御のデータ送受信に支障をきたす状態が発生する。	・収集データの欠損が問題になる計測時間以内の間隔で、サーバにデータバックアップを実施する。

	セキュリティインシデント	リスク源	セキュリティポリシー
(4)	所定の作業員以外による画面の盗み見、不正操作が行われる。	・大規模ビルでは、空調コントローラが設置されている防災センター（中央監視室）に対して、許可された入退室に限定するような管理ができておらず、許可者以外の入室を許してしまう。 ・中小規模ビルでは、空調コントローラが、一般居室に設置されるなどにより、操作許可する作業員が限定できていない。	・重要施設用と一般オフィス用を分離し、重要施設用コントローラは、防災センター（中央監視室）に設置する。 ・防災センター（中央監視室）の入場者を登録（事前、都度）して管理する仕組みを入れる。 ・防災センター（中央監視室）への入退室をもれなくチェックし管理する仕組みを入れる。
(5)	所定の作業員が、その権限を越えて、システムや端末／制御盤に不正操作をする。	システムの権限管理や作業監視が十分でなく、権限外の不正操作をされることを防ぐことができない。	・作業員の作業状況を常時監視する仕組みを入れる。 ・許可された作業員以外が作業できない仕組みを入れる。
62	保守用持ち込み端末		
(1)	外部持込端末接続時に、外部持込端末経由でマルウェアに侵入されてしまう。	セキュリティ確認がされていない外部持込端末が容易に接続可能となっている。	・保守用端末は適切に管理されたものを使う。
(2)	USB等の外部媒体経由で、端末がマルウェアに侵入されてしまう。	セキュリティ確認がされていないUSB等の外部媒体が容易に使用可能となっている。	・使用できる外部媒体等をあらかじめ限定した運用を徹底する。

4.2. 全体管理

空調システムに関連し、システム全体の構成情報や組織体制、教育など、場所によらない要素についてのセキュリティインシデント、リスク源、セキュリティポリシー（対策要件）は、基本的に共通編の要件をそのまま適用可能である。このため表 4-2 全体管理に関するビルシステムのリスクと対策ポリシーに共通編の要件を再掲する。

表 4-2 全体管理に関するビルシステムのリスクと対策ポリシー

（共通編 表 4-1 全体管理に関するビルシステムのリスクと対策ポリシーを再掲）

	セキュリティインシデント	リスク源	セキュリティポリシー
1. 構成情報／管理情報			
(1)	ビルシステムへの被害発生時に、被害確認が遅れ、復旧作業の支障となる。	ビルの構成情報が最新状態に管理できておらず、機器の最新の接続関係が把握できない。	・構築システム構成図（設計時）に対し、引渡し時のシステム構成図を竣工引渡し書類として作成するように”設計仕様”に加える。 ・システム全体構成（外部接続先を含む）の最新状態を常に把握できるようにする。
2. バックアップデータ／事業継続			
(1)	適切なバックアップデータがなく、ビルシステムへの被害発生時に復旧作業の支障となる。	バックアップが取られていない、又はバックアップの範囲や対象が適切でない。	・システムバックアップ方法を運用側と確認の上でバックアップ方法を設計時に仕様を組み込む。 ・管理ポイントや運転スケジュール等、システムを運用するにあたって必要なデータについては、バックアップを取得する機能を具備する。
(2)	システムの脆弱性をついた攻撃を受ける。	脆弱性についての認識が不十分で、脆弱性が残ったままの状態になっている。	・既知の脆弱性に対して必要な対策（パッチ等）が適用されているものを導入し管理する。 ・但し、他機器及び他システムの正常稼動については、担保しなければならない。

	セキュリティインシデント	リスク源	セキュリティポリシー
3. 会社／要員の管理			
(1)	ビルシステムへの被害発生時に、迅速な対応ができず、被害が拡大する。	ビル管理会社においてセキュリティへの意識醸成、要員教育が十分ではなく、事前対策や対応準備ができていない。	・システム構築要件に教育訓練について明記する。
(2)	ビルシステムが内部作業員等から攻撃を受ける。	作業員等の身元確認や行動監視が不十分で、内部攻撃者が紛れることや攻撃を行うことを防ぐことができていない。	・システムの構築・施工・保守にあたって、作業員等の身元確認や行動確認についての要件を明記する。
4. 体制構築等			
(1)	攻撃等への対応が効果的にできず、被害が拡大する。	十分なリスクアセスメントができていないため、リスク対応の運用計画や体制が十分なレベルで構築できていない。	・リスクアセスメントを実施し、その結果を基に監理監査面からの「運用する管理体系」などを運用計画として定義・整備する。
(2)	ビルシステムのセキュリティ対策が不十分で、攻撃を防ぐことができない。	ビルシステムの設計・構築にあたって、十分なセキュリティ対策を盛り込むことができていない。	・ビルシステムに対して十分なセキュリティ知識を持った技術者の元で設計を実施する体制を整える。
(3)	攻撃への初動対応が遅れ、被害が拡大する。	作業員の教育、訓練が十分ではなく、十分な対応が取れない。	・入場前に適切にセキュリティ対策を実施する。
(4)	攻撃への対応が体系的に実施できず、被害が拡大する。	運用時のセキュリティ管理体制が十分なレベルで構築できていない。	・設計要件・運用要件を明記する。
(5)	攻撃に対する対応手順が分からず、被害が拡大する。	運用基準の中で、緊急時の対応手順が十分に整備されていない。	・緊急時の対応手順要件について明記する。
(6)	不正なアクセス、通信、操作があっても、気がつくのが遅れたり、見逃したりしてしまい、被害が拡大する。	システムの運用監視が十分ではなかったり、運用状況の監視体制が十分ではない。	・発注主側の運転管理者に対する教育について、明記する。 （教育人数・教育テキスト・教育期間・セキュリティー関連教育を含む・教育場所を明記）

4.3. 機器ごとの管理策

場所ごと、機器ごとのセキュリティインシデント、リスク源、セキュリティポリシー（対策要件）についても共通編の要件がそのまま適用可能であるため、表 4-3 場所ごとのビルシステムのリスクと対策ポリシーを再掲する。

表 4-3　場所ごとのビルシステムのリスクと対策ポリシー

（共通編　表 4-2 場所ごとのビルシステムのリスクと対策ポリシーを再掲）

	セキュリティインシデント	リスク源	セキュリティポリシー
1. ネットワーク(クラウド、情報系 NW、BACnet 等)			
10	ネットワーク		
(1)	ビルシステムの一部に起きたマルウェア感染が、ビル内のネットワーク経由で容易に拡大していく。	ビル内のネットワークに様々なビル設備機器が混在して接続され、マルウェアの感染拡大防止を意識した管理がされていない。	・ビル内のネットワークをセキュリティポリシーに基づいて物理的又は論理的に分離する。
(2)	ビルシステムの一部に起きたマルウェア感染が、ビル内のネットワーク経由で容易に拡大していく。	ビル内のネットワークでやり取りされる通信が適切に管理されておらず、リモートからの不正侵入の防止を意識した管理がされていない。	・ビル内のネットワークにおいては、セグメント間通信を必要最小限に制限する。
(3)	管理外の外部ネットワーク接続経由でマルウェア感染や不正侵入を受ける。	保守等の理由で外部接続が知らぬ間に取り付けられたり、外部との通信ポートが開けられたりするのを十分に管理・制限できていない。	・不正接続の有無を定期的に点検する。 ・外部との接続や通信はファイアウォール等により必要最小限に制限する。
(4)	管理外の外部ネットワーク接続経由で不正接続や攻撃を受ける。	ビルへの引き込み回線の管理が不十分で、勝手に不正な外部回線を引き込まれる。	・ビル内に設置する外部接続回線を管理し、不明回線の有無等を定期的に点検する。
11	クラウドサーバ・Web サーバ		
(1)	外部ネットワーク接続経由で侵入を受ける。	外部接続機器のセキュリティ対策が十分ではない。	・外部からのアクセスに制限を設ける。
(2)	テナント向けの Web 公開システム経由で不正操作をされる。	Web 公開システムの脆弱性対策が十分ではない。	・ビルシステムの制御を行うシステムをインターネットに公開する場合は、アクセス制御を行ったうえで、脆弱性対策の実施体制を構築する。
(3)	クラウドサーバを利用することで意図しない不正アクセスが発生する。	発注側がリスクを把握していない。	・リスクアセスメントを実施したうえで、発注の判断を行う。
12	情報系端末(オフィス系端末)		
(1)	外部ネットワークに接続された情報系端末経由で、ビルシステム内への攻撃を受ける。	外部ネットワークに接続された情報系端末のセキュリティ対策が十分ではない。	・外部からのアクセスに制限を設ける。

	セキュリティインシデント	リスク源	セキュリティポリシー
13	外部接続用ネットワーク機器(ファイアウォール、ルータ)		
(1)	外部ネットワーク接続経由で攻撃を受ける。	外部接続用ネットワーク機器のセキュリティ対策が十分ではない。	・外部からのアクセスに制限を設ける。
14	ビルシステム間相互接続		
(1)	ビルシステムの一部に起きたマルウェア感染が、ビルシステム間の相互接続経由で容易に拡大していく。	ビルシステム間の相互接続環境において、感染拡大防止等のセキュリティ対策が十分ではない。	・正当な端末以外にはアクセスしない、不正な端末からのアクセスを許可しない、といった対策を施す。 ・正しい通信のみ許可するといった通信制限を施す。
2. 防災センター(中央監視室)			
20	防災センター(中央監視室)		
(1)	所定の作業員以外による画面の盗み見、不正操作が行われる。	防災センター(中央監視室)に対して、許可された入退室に限定するような管理ができておらず、許可者以外の入室を許してしまう。	・防災センター(中央監視室)の入場者を登録(事前、都度)して管理する仕組みを入れる。
			・防災センター(中央監視室)への入退室をもれなくチェックし管理する仕組みを入れる。
(2)	所定の作業員が、その権限を越えて、システムや端末／制御盤に不正操作をする。	システムの権限管理や作業監視が十分でなく、権限外の不正操作をされることを防ぐことができない。	・作業員の作業状況を常時監視する仕組みを入れる。
			・許可された作業員以外が作業できない仕組みを入れる。
21	HMI/HIM		
(1)	正規の作業員以外により不正ログイン、不正操作がされる。	端末のログイン管理やログイン情報の管理が不十分である。	・操作者を限定する機能を入れる。 ・パスワード管理を徹底させる。
(2)	所定の作業員が、その権限を越えて、システムや端末に不正操作をする。	端末やシステムの権限管理や作業監視が十分でない。	・作業員の作業状況を常時監視する仕組みを入れる。
			・許可された作業員以外が作業できない仕組みを入れる。
(3)	侵入者にシステム情報を探られ攻撃が拡大する。	ログ情報へのアクセスが容易で、侵入者にログ情報を探られ、次の攻撃のヒントを与えてしまう。	・アクセスログ、操作履歴を適切に管理する。
(4)	不正侵入に対する状況解析が困難で対策が遅れる。	適切にログが取得されておらず、侵入や感染の状況の解析が十分にできない。	・各種ログ情報の導入とログ解析の仕組みを導入する。

	セキュリティインシデント	リスク源	セキュリティポリシー
(5)	不正なアクセス、通信、操作があっても、気がつくのが遅れたり、見逃したりしてしまい、被害が拡大する。	システムの運用監視が十分でない。	・不正なアクセスや操作を定期的に確認する仕組みを入れる。
(6)	マルウェアへの感染判明後、その感染経路が特定できず、対策が十分に取れない。	システム構築の過程や運用の節目でマルウェアの感染のチェックや管理が不十分であるため、いつの間にか感染しており、感染原因や感染経路がすぐに分からない。	・工場出荷前及び引渡し前に事前検疫を実施する。
(7)	侵入者にシステム内部を探られ、不正な操作をされる。	システムの内部構成が単純又は権限管理ができておらず、容易に全体を探られ、次の攻撃のヒントを与えてしまう。	・権限者以外、容易にシステム内部の構造が見られないようにする。
(8)	システムの脆弱性をついた攻撃を受ける。	脆弱性についての認識が不十分で、脆弱性が残ったままの状態となっている。	・既知の脆弱性に対して必要な対策（パッチ等）が適用されているものを導入し管理する。 ・但し、他機器及び他システムの正常稼動については、担保しなければならない。
(9)	外部媒体接続時に、外部媒体経由でマルウェアに侵入されてしまう。	セキュリティ確認がされていないUSB等の外部媒体が容易に接続可能となっている。	・外部媒体等を安易に利用できないようにする。 ・外部媒体等を事前検疫してから利用する。
22	**保守用持ち込み端末**		
(1)	外部持込端末接続時に、外部持込端末経由でマルウェアに侵入されてしまう。	セキュリティ確認がされていない外部持込端末が容易に接続可能となっている。	・保守用端末は適切に管理されたものを使う。
23	**統合NWにつながるネットワーク機器（ファイアウォール、ルータ、スイッチ）**		
(1)	不正端末を接続され、マルウェアを送り込まれる。	空きポートが接続可能な状態で放置されている。	・スイッチ等の空きポートが利用されないような仕組みを導入する。
24	**システム管理用サーバ（ビルシステム主装置）**		
(1)	所定の作業員以外による不正操作が行われる。	サーバが専用の管理区画に設置されておらず、誰でも触ることができる状態にある。	・適切に管理された専用の室、区画の中に機器を設置する。 ・区画内のラックやケースは施錠管理を行う。

	セキュリティインシデント	リスク源	セキュリティポリシー
(2)	所定の作業員以外による不正操作が行われる。	サーバ設置区画への入退室が適切に管理されておらず、誰でも触ることができる状態にある。	・サーバ室、区画への入退室を適切に管理する。 ・関係者以外立ち入らせない。
(3)	侵入者にシステム情報を探られ攻撃が拡大する。	ログ情報へのアクセスが容易で、侵入者にログ情報を探られ、次の攻撃のヒントを与えてしまう。	・アクセスログを記録する機能を入れる。
(4)	不正侵入に対する状況解析が困難で対策が遅れる。	適切にログが取得されておらず、侵入や感染の状況の解析が十分にできない。	・各種ログ情報の導入とログ解析の仕組みを導入する。
(5)	不正なアクセス、通信、操作があっても、気がつくのが遅れたり、見逃したりしてしまい、被害が拡大する。	システムの運用監視が十分ではなかったり、運用状況の監視体制が十分でない。	・不正なアクセスや操作を確認する仕組みを入れる。
(6)	不正な命令を実行してしまい、不正な動作をさせられる。	通信相手を認証する仕組みがなく、なりすまし通信を区別することができない。	・認証されていない相手との通信を遮断する機能を入れる。
(7)	マルウェアへの感染判明後、その感染経路が特定できず、対策が十分に取れない。	システム構築の過程や運用の節目でマルウェアの感染のチェックや管理が不十分であるため、いつの間にか感染しており、感染原因や感染経路がすぐに分からない。	・工場出荷前及び引渡し前に事前検疫を実施する。 ・運用段階においても、検疫を適宜実施する。
(8)	侵入者にシステム内部を探られ、不正な操作をされる。	システムの内部構成が単純又は権限管理ができておらず、容易に全体を探られ、次の攻撃のヒントを与えてしまう。	・権限者以外、容易にシステム内部の構造が見られないようにする。
(9)	システムの脆弱性をついた攻撃を受ける。	脆弱性についての認識が不十分で、脆弱性が残ったままの状態となっている。	・既知の脆弱性に対して必要な対策（パッチ等）が適用されているものを導入し管理する。 ・但し、他機器及び他システムの正常稼動については、担保しなければならない。
(10)	外部媒体や外部持込端末接続時に、これらを経由してマルウェアに侵入されてしまう。	セキュリティ確認がされていないUSB 等の外部媒体や外部持込端末が容易に接続可能となっている。	・外部媒体等を安易に利用できないようにする。 ・外部媒体等を事前検疫してから利用する。

	セキュリティインシデント	リスク源	セキュリティポリシー
3.機械室／制御盤ボックス			
30	機械室		
(1)	所定の作業員以外による不正操作が行われる。	許可された入退室に限定するような管理ができておらず、許可者以外の入室を許してしまう。	・機械室は施錠可能とする。
31	コントローラ（DDC、PLC 等）		
(1)	侵入者にシステム情報を探られ攻撃が拡大する。	ログ情報へのアクセスが容易で、侵入者にログ情報を探られ、次の攻撃のヒントを与えてしまう。	・ログを適切に管理可能な機器・システムを導入する。
(2)	不正侵入に対する状況解析が困難で対策が遅れる。	適切にログが取得されておらず、侵入や感染の状況の解析が十分にできない。	・各種ログ情報の導入とログ解析の仕組みを導入する。
(3)	不正なアクセス、通信、操作があっても、気がつくのが遅れたり、見逃したりしてしまい、被害が拡大する。	システムの運用監視が十分ではなかったり、運用状況の監視体制が十分でない。	・不正なアクセスや操作を確認する仕組みを入れる。
(4)	不正な命令を実行してしまい、不正な動作をさせられる。	通信相手を認証する仕組みがなく、なりすまし通信を区別することができない。	・許可されていない相手との通信を遮断する機能を入れる。
(5)	マルウェアへの感染判明後、その感染経路が特定できず、対策が十分に取れない。	システム構築の過程や運用の節目でマルウェアの感染のチェックや管理が不十分であるため、いつの間にか感染しており、感染原因や感染経路がすぐに分からない。	・工場出荷前及び引渡し前に事前検疫を実施する。 ・運用段階においても、検疫を適宜実施する。
(6)	侵入者に容易にアクセスされ、不正操作をされる。	ID・パスワードが適切に設定されておらず、誰でもアクセス可能な状態にある。	・ID・パスワード管理を必要とする機器においては、適切な ID・パスワードを設定する。
(7)	システムの脆弱性をついた攻撃を受ける。	脆弱性についての認識が不十分で、脆弱性が残ったままの状態となっている。	・既知の脆弱性に対して必要な対策（パッチ等）が適用されているものを導入し管理する。 ・但し、他機器及び他システムの正常稼動については、担保しなければならない。

	セキュリティインシデント	リスク源	セキュリティポリシー
(8)	外部媒体や外部持込端末接続時に、これらを経由してマルウェアに侵入されてしまう。	セキュリティ確認がされていないUSB 等の外部媒体や外部持込端末が容易に接続可能となっている。	・外部媒体等を安易に利用できないようにする。
			・外部媒体等を事前検疫してから利用する。
			・外部持込端末は適正に管理された端末のみ接続を許可する。
32	**ネットワーク機器(ファイアウォール、ルータ、スイッチ)**		
(1)	不正端末を接続され、マルウェアを送り込まれる。	空きポートが接続可能な状態で放置されている。	・スイッチ等の空きポートが利用されないような仕組みを導入する。
33	**ゲートウェイ機器**		
(1)	不正な命令を実行してしまい、不正な動作をさせられる。	通信先を制限する仕組みがなく、なりすまし通信を区別することができない。	・ネットワーク上に、通信先を制限する仕組みを導入する。
34	**各種制御盤・分電盤**		
(1)	所定の作業員以外による不正操作が行われる。	業界で広く通用する鍵がついているため、容易に開錠され、機器に触れることができる状態にある。	・各種制御盤の鍵は、業界で広く使われる種類の鍵以外を使用する。 ・保守時の対応等も考慮して鍵を導入する。
4.配線経路(MDF 室、EPS、天井裏ラック)			
40	**MDF 室／EPS／天井裏ラック**		
(1)	不正端末を接続され、マルウェアを送り込まれる。	ネットワーク配線への人的アクセスが管理されていない。	・ビルシステム主装置以降の配線について、外的要因(人的破壊・意図した工作)に対して十分な保護対策を施す。
41	**内部に置かれたネットワーク機器(スイッチ類)**		
(1)	所定の作業員以外による不正操作が行われる。	機器の設置場所が安全管理されておらず、誰でも触ることができる状態にある。	・適切に管理された専用の室、区画の中に機器を設置する。
			・機器類は許可された作業員以外が容易に触れないようにする。
(2)	不正端末を接続され、マルウェアを送り込まれる。	空きポートが接続可能な状態で放置されている。	・機器類の空きポートには不正利用ができないよう、対策を実施する。

	セキュリティインシデント	リスク源	セキュリティポリシー
5. 末端装置が置かれる場所			
50	末端装置		
(1)	不正端末を接続され、マルウェアを送り込まれる。	空きポートが接続可能な状態で放置されている。	・第三者がアクセス可能な場所には、フィールド機器や IP ネットワークに直結する機器を設置しない。 ・機器には、第三者による不正な操作ができないよう、対策を実施する。
(2)	不正な命令を実行してしまい、不正な動作をさせられる。	通信相手を認証する仕組みがなく、なりすまし通信を区別することができない。	・特定要員以外の利用を遮断するための十分な保護対策を施す。

付録 A　空調システムの種類

空調方式は、暖房時や冷房時に使う熱源システムの設置場所により、セントラル空調方式と個別分散空調方式に分類される。セントラル空調方式では、空調対象（ビル）全体の熱源を一カ所にまとめて設置する。大規模ビルでは地下に、中規模ビルでは屋上に熱源機器を設置する。一方、個別分散空調方式では、熱源機（室外機）と空調機（室内機）の間隔の制限から、中小規模ビルでは、熱源を屋上にまとめて設置、或いはビル周辺の半地下や地上に分散して設置する。大規模ビルでは、各フロアの周辺部に熱源機（室外機）の設置場所を設け、フロア毎に空調機（室内機）を設置することで、個別分散空調方式を実現している。

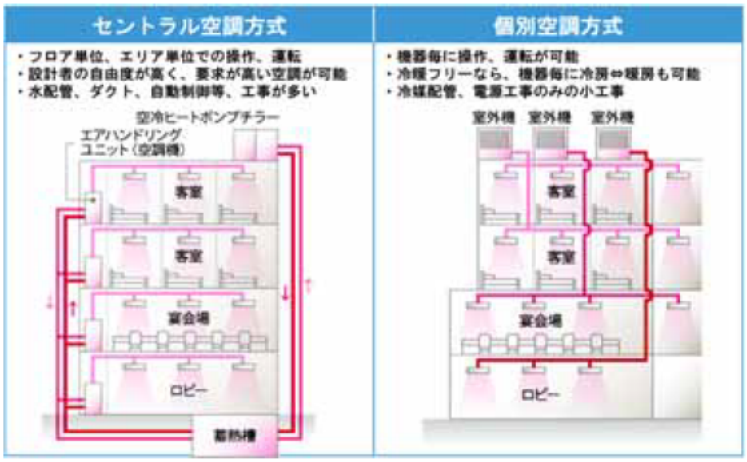


図　付録 A-1　セントラル空調と個別分散空調方式

空調システムでは、熱搬送媒体として、一般的には空気、水（ブライン）、冷媒が使われる。セントラル空調方式では、空気、水が用いられ、個別分散空調方式では、冷媒が用いられる。

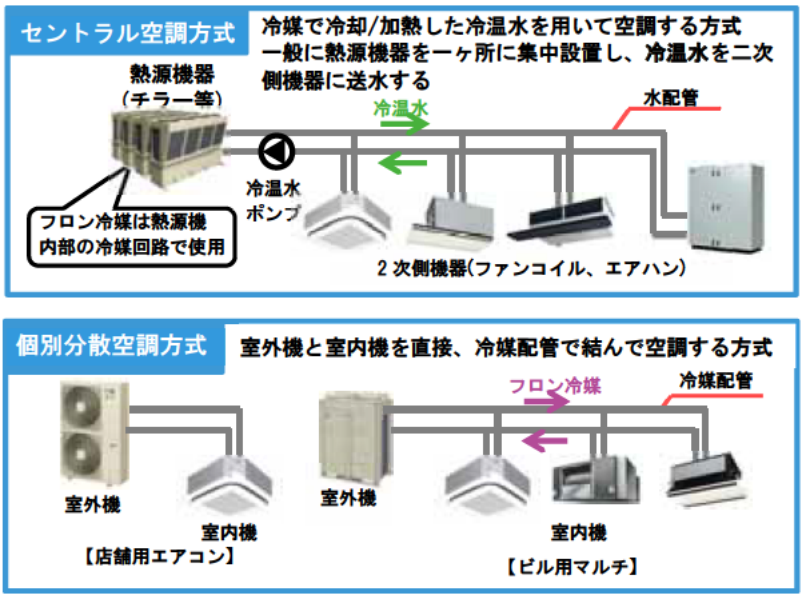


図　付録 A-2　熱搬送媒体の違い

産業サイバーセキュリティ研究会
WG１　ビルSWG　議事要旨

１　日　時

令和３年３月２２日（月）10:00～12:00

２　場　所

WEB 会議（WebEX）による開催

３　出席者

（構成員）

秋山構成員（三菱地所株式会社　専任部長）
安斎構成員（株式会社日建設計　アソシエイト）
池田構成員（日本生命保険相互会社　理事）
伊藤構成員（アズビル株式会社　主任）
岩城構成員（一般社団法人ビルディング・オートメーション協会　理事）
江崎座長（東京大学　教授）
大西構成員（鹿島建設株式会社　課長）
奥住構成員（株式会社きんでん　技監）
加井構成員（ダイキン工業株式会社　産官学連携専任部長）
川西構成員（株式会社日立ビルシステム　本部長）
坂田構成員（NTT コミュニケーションズ株式会社　情報セキュリティ部　担当課長）
忽那構成員（一般社団法人日本ビルヂング協会連合会　事務局次長）
後神構成員（株式会社竹中工務店　専門役（情報エンジ担当））
坂田構成員（NTT コミュニケーションズ株式会社　情報セキュリティ部　担当課長）
佐藤構成員（ICSCoE２期ビルチーム有志（森ビル）課長）
柴田構成員（一般社団法人不動産協会　事務局長代理）
中原構成員（三井不動産株式会社　グループ長）
林構成員（株式会社九電工　副本部長）
福田構成員（横浜市　最高情報統括責任者補佐監/最高情報セキュリティ責任者補佐監）
二名構成員（NTT コミュニケーションズ株式会社　ICT システム部　部門長）
松浦構成員（東京工業大学　准教授）
松本構成員（セコム株式会社　マネージャー）
村瀬構成員（技術研究組合制御システムセキュリティセンター　事務局長）

森永構成員（三菱電機株式会社　担当課長）
渡部構成員（イーヒルズ株式会社　取締役）

（オブザーバー）
国土交通省（大臣官房官庁営繕部設備・環境課、土地・建設産業局建設業課、土地・建設産業局不動産業課、住宅局住宅生産課、総合政策局情報政策課）
内閣官房　東京オリンピック競技大会・東京パラリンピック競技大会推進本部事務局
内閣サイバーセキュリティセンター　東京 2020 グループ
公益財団法人東京オリンピック・パラリンピック競技大会組織委員会
中部国際空港施設サービス株式会社
アライドテレシス株式会社
日立ジョンソンコントロール空調株式会社

（事務局）
経済産業省（商務情報政策局サイバーセキュリティ課、製造産業局産業機械課）
株式会社野村総合研究所
NRI セキュアテクノロジーズ株式会社

４　配布資料

資料１　議事次第・配布資料一覧
資料２　構成員等名簿
資料３　ガイドライン・空調編の検討について
資料３－１　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）
資料４　ビルセキュリティガイドラインを使い倒す（森ビル）
資料５　ガイドライン２年間の振り返りと課題の共有について
資料６　インシデントレスポンスの検討に向けて

５　議事要旨

（１）開　会

経済産業省　商務情報政策局サイバーセキュリティ課　奥家課長より開会のご挨拶。

（２）ガイドライン・個別編（空調編）の検討について

資料３、資料３－１について、事務局　経済産業省　津国様よりご説明。

加井構成員より補足のご説明。

（３）構成員より発表（ICSCoEビル有志・森ビル佐藤様）

資料４について、佐藤構成員よりご説明。

（４）その他報告事項

（ア）ガイドライン２年間の振り返りと課題の共有

資料５について、事務局　経済産業省　津国様よりご説明。

（イ）インシデントレスポンスの検討に向けて

資料６について、事務局　経済産業省　津国様よりご説明。

（ウ）レポジトリの充実化について

（５）自由討議

主な意見等は次のとおり。

松浦構成員： 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)について１点コメントをしたい。個別編：空調システムにおいて、検知やMITRE ATT&CKについて丁寧に記載をしていただいていると思うが、もう少し読み手が手を付けやすい軽いものも記載できるのではないかと考えた。例えば、機器の設定等において、30分から１時間に１回程度。温度設定で正しい値を入力し続けると、攻撃があってもすぐに元の状態に戻せることが出来、常に定常状態に保つことが出来るというような制御の方法等もうまく個別編:空調システムに組み込んでも良いのではないか。緩やかにディテクションした後でも、対応に時間をかけることが出来るというメリットもある。この手法は車の制御装置でよく見られると理解している動きで、車の場合分単位、秒単位の細かいサイクルで再起動等を実施することで、定常状態を保つような手法を取っているので、個別編：空調システムでも参考にできるのではないかと考える。次にインシデントレスポンスに関して、資料６の１ページ目で重要インフラ向けインシデントレスポンスの体系の例を記載いただいておる

が、そこに権限整備関連の文書化の追加を希望する。権限を文書化することで、インシデントが発生した際に、文書化されたマニュアルやルールに沿って、誰がどういったアクションをとるべきかを明確化してほしい。インシデントが発生してしまった際に属人的な判断に頼るのではなく、文書に規定されている行動を、決められた担当者が行えるようにしておくことがスムーズなインシデントレスポンスの実現に繋がると考える。その為今後の個別編：空調システムの拡充において、優先順位高めに実施しても良いのではないかと考えている。事例を紹介すると大学関連でIoT機器の感染が起き、実験機器などが攻撃の対象になる。攻撃の内容はスパムを撒く程度のシンプルな攻撃だが、液体窒素などの制御装置が攻撃受けると、感染しているのは把握できても実際に装置を止めて良いのか、誰に連絡すれば良いのかがわからずに対応が遅れてしまうという事例も多く存在するため、事前に文書化したルール等を共有しておくことが非常に有用だと考える。

江崎座長：ご意見賜った。必要に応じて検討グループ側に松浦構成員もご参加いただいて、個別編：空調システムの拡充を目指していきたい。

加井構成員：松浦構成員に個別編：空調システムの拡充として、軽い監視や制御の手法の追加についてご意見を賜った。そこに補足させていただきたいのだが、デマンドをかけているコントローラー（空調機）については、オフィス等その空調機が設置されている部屋にいる人が設定温度を変更してしまう。しかしながら、一般的な考え方として設定温度を変更した人は、５分程経過してしまうと設定変更したことを忘れてしまうことが多いので、５分経ったら自動に元の設定温度に戻すような機能をデマンド機能として提供している。そのため松浦構成員にご指摘いただいたように、温度設定で一定の数値を入力し続けて設定温度を保つようなことは実現できる。そのため、なにをもって異常なのか、もしくはインシデントなのかを判断できれば、個別空調であればコントローラーで把握して、ローカル側でインシデントへの対応が実施できるかもしれないと考えた。現在でも気温の上下監視等は実施しているが、これまでは人間のミスオペレーションを対象と想定していたが、将来的には攻撃等インシデントの検知にも活用できるかもしれない。

松浦構成員：加井構成員に補足いただいたような５分程度で元の設定温度に戻る機能があることは理解している。例えば20度から25度のように、一定の正常値の幅を設定しておき、一般のユーザの方のアクションも受け入れられるようにしつつ、学習データを蓄積することでビルごとの最適化を行い、攻撃への対応時間を稼ぐということも実現できるのではないかと考える。

渡部構成員：２点コメントさせていただきたい。１点目は松浦構成員からご発言いただいたことは非常に重要だと認識している。合わせてセーフティという観点からもどういう対応をしていくべきか等、インシデントレスポンスを考えていきたい。空調で例を挙げると、熱源系は一旦止めてしまって30分以内に再起動すると爆発するケースもあるので、権限整理等と合わせながらこういうことは実施しない、こういうことは気を付ける等を検討していきたいと考える。２点目は確認事項だが、資料３の３ページ目に、大規模ビルにおける空調システム構成が記載されているが、最近テナント側がIT経由で温度等を制御するという機能が追加されており、この構成図の中でそれはどこに示されるのか。

加井構成員：資料３の３ページ目に、大規模ビルにおける空調システム構成の図自体は左側のセントラルについてはビルガイドラインの基本編から持ってきており、基本的に中央監視の構成を示している。右側の個別空調に関しては、上位、空調制御コントローラー、手元リモコンから制御が実施出来る。

渡部構成員：左側のセントラルではテナント側からの操作について記載されていないという認識で良いか。右側の個別空調で言うと、空調制御コントローラーのIPネットワークから入るという理解で良いか。

加井構成員：左側のセントラルの図はビルガイドラインの基本編からそのまま引用しており、かつ個社としても個別空調をメインに取り組んでいるため、申し訳ないがセントラル側の詳細なお答えは難しい。個別空調においてはテナント側にリモコンがあればそこからコントロールが効き、ビルの管理側から入るのであれば制御コントローラー、中央監視から入るとなっており、操作を実施する人に応じて別の手法で設定することが出来るという理解でいる。

渡部構成員：承知した。

安斎構成員：情報共有をさせていただきたい。佐藤構成員に資料４でご紹介いただいたDPIツールのNOZOMIは、弊社でもサプライヤーにご協力いただいて設置した。古いバージョンのバックネットも読み取れ、幅広く使い勝手のいい製品であったが、学習期間中のデータを踏まえて異常を検知する機能であったため、ビルは季節変動によって温度設定の幅が非常に広いことから、学習期間が短いと使いこなすのが難しいという感想を持った。役に立つ機械ではあるが使い方を吟味しなくてはならないのと、かつ値段が高いのが少し懸念事項かもしれない。

伊藤構成員：先ほどの加井構成員と渡部構成員の資料３の３ページ目に記載されている大規模ビルにおける空調システム構成の図についてコメントを

追加したい。記載されている構成図はあくまで一例であり、必ずしも一致しない例はある。例えば、先ほどのテナント側からの制御で言うと、バックネットや統合ネットワークを介して操作できるパターンも存在する。しかしながら、そのどちらもコントローラーに対する設定値の変更となることに変わりはない。

佐藤構成員：先ほどの安斎構成員のDPIツールのNOZOMIに関する情報提供に感謝する。弊社の使用感としても、学習期間の重要性は認識しており、しばらくはインシデント対応に活用するのではなく、検知してアラートを上げるためのものとして使用していきたいと考えている。

江崎座長：個別編：空調システムのドラフトについて、渡部構成員から熱源系は一旦止めてしまって30分以内に再起動すると爆発するケースもあり、危険なのでセーフティのプロセスを取るべきというお話があったが、本ガイドラインは普通のビルだけではなく、場合によっては半導体等最先端の産業用の工場の空調にも使われる可能性があるため、普通のビルだけではなく安全性が強く求められるような工場や施設にも活用できるように記載を追加した方が良いのではないかと考えた。昨今の米国テキサス州の大寒波を受け、半導体や素材関係のサプライチェーンが被害を受けたことを鑑みると、工場等の空調のシステム等が安全に高品質に正常に戻るまでに時間がかかることを考えると、システムを止めるという判断も難しいため、先ほど松浦構成員にご指摘いただいたような手順や管理者を設定しておくことも非常に重要だと考える。特に産業用の工場や施設での大きな損害を抑えるためにも、ビルガイドラインにおいてそういった応用的な記載も実施した方が良いと考える。

奥家課長（事務局）：個別編：米国のペンタゴンがビルのセキュリティに神経質になっている関係で、ビル側でセキュリティ対応を実施していることを明確に求めてきており、ビルシステムを納入するサプライヤー側が混乱したことがあった。個別編：空調システムが整えられていく上で、こういった海外の先行的な事例をとらえ、今後のユーザのハイレベルな要求に応えられるような検討がなされているのかは気になる。次に先ほどDPIツールのNOZOMIのお話があり、そういったツールは国内での対応事例が存在しているかと思うが、その先に行こうとする場合、海外ではコマンドを暗号化することで、指示内容に触れないようにして防御している先行事例もあり、その際にDPIを一部解除しなくてはいけないという場合も存在する。国内でこのようなコマンド暗号化なども検討している例はあるのかについてお伺いしたい。

佐藤構成員：個人として把握している範囲で、コマンド自体を暗号化という話

は初めて聞いたので国内でそういう検討はまだないかもしれない。

江崎座長：SSHで乗っ取られて攻撃されるということは普通にあり得る話ではないのか。

奥家課長（事務局）：海外だとイタリアのEnel S.p.A.社等はそういった検討を既に実施しており、システムからDPIを少し外さなくてはいけないので少しずつしか検討を進められないという話を聞いた。とにかく国内でもダッシュボード管理は入り口として取り組むべき課題として視野に入れるべきであろうと考えている。現在、個別編：空調システムではどれくらい意識しているのか。

加井構成員：奥家課長にご指摘いただいたようなペンタゴンからのセキュリティに関する指摘に対する空調機の対応については、コントローラーに対して同様の話が来ている。しかしながら、個社としての対応の詳細を今回の個別編：空調システムの記載を突き合わせて記載するというような確認は実施していない。補足が必要であれば社内の基準、実施内容と照らし合わせて補足させていただきたいので、今回の個別編：空調システムにそこまで踏み込んだ記載をするという方向性に決まったら社内で確認させていただきたいと思う。

奥家課長（事務局）：加井構成員のご発言を心強く思う。ペンタゴンの指摘に対してどのように対応していいかわからず、北米市場から追い出されるのではないかという危機感を持っている企業も存在するので、ビルガイドラインでもそういった将来的な対応に資する情報も組み込んで、外に対してセキュリティについて対応、検討を実施していることを示せるように可視化されている状態に出来るとありがたく思う。

江崎座長：ペンタゴンは軍用のシステムを主な対象としていると理解しているが、民間の方にも影響があるのか。米国が昨今サプライチェーン管理を重要視していることを鑑みると、最先端の半導体やバイオ領域にも同様のセキュリティレベルを求めてくる可能性があると認識しても良いのか。

奥家課長（事務局）：DoDは以前、ワシントン周辺の民間ビルを借り、その中に部署を配置していたが、ビルのセキュリティを危惧して、DoD側で新しいビルを建設し、民間ビルに配置していた部署を移して神経質に管理するようになった。こういった動きを鑑みると同様に、DoDと深く関係している民間事業者にもビルのセキュリティについて同等のレベルを求める可能性は十分にあると考えている。機器ベースに関しては電力側で機器内の部品をどのように可視化して把握するかの議論がすごく進んでいる。同様に、サプライチェーンとリスクを段階ごとに検討していくような方向性にもなっている。この様な近しい領域の検討を参考に考えると、ビルセキュリ

ティガイドラインの議論も初めから緩く設定しすぎてしまうと、今後起きることになる検討のスピード感についていけなくなってしまう恐れがあるので、現段階の検討から少しレベルを高く、厳しく設定しておくべきではないかと考える。

江崎座長：普通の、民間ビルだけではなく、セキュリティについて高いレベルが求められるような神経質なビルや施設も対象に含めて、ビルセキュリティガイドライン全般の記載を検討するべきだと理解した。

奥家課長（事務局）：日本だと特に製造業系の事業者が、国際市場に深くかかわっていることから直接的な影響を強く受けてしまうと思うので現段階から対応しておくべきだと考える。

江崎座長：DPIについてなにか補足事項等はあるか。

佐藤構成員：弊社はこれまでキャプチャーしたパケットなどを対象にして実証実験等を実施していたが、これからは実際のビルを対象にしてNOZOMI等のツールを用いた実証実験を実施していけるように検討している。

江崎座長：よくある間違った認識として、DPIやファイアウォールを入れたら安心と思ってしまう事業者が多いと思うため、実際のビルで検討を行い、より詳細な検討を進められると良いと考える。

加井構成員：オフィスビルであればNOZOMI等のDPIツールを活用して学習期間を設け、データを収集して検知するという話があった。関連しての話になるが、限定的に年間通して温度監視を機器側でもパケットを監視することでチェックを実施しており、機能としては既に持っている。ただなにをもって異常とするのかの基準が明確になっていないので、そこが明確になれば末端側でも監視が出来るようになる。

柳田構成員：本ガイドライン検討全体やスケジュールについて２点お伺いしたい。１点目に個別編ということで空調についてご説明を頂いたが、空調編以外の個別編の検討は既に始まっているのか。２点目に、今後空調編はパブコメを経てリリースされると思うが、パブコメが実施される時期についてもし決まっていればお伺いしたい。

津国様（事務局）：まず空調編のリリースの時期について、本日の説明を受けて構成員からご意見を伺う時間を設けたいので、その時間を鑑みると約１か月後にパブコメを実施、その後修正して、大体夏前のリリースをターゲットにして動きたいと考えている。空調以外の個別編はまだ検討を始めておらず、ニーズに合わせて検討を進めていきたいためぜひ要望を挙げてほしい。

後神構成員：インシデントレスポンスについては、JDCCでインシデント対応ガイドブックを作成しており、ほぼ完成している状態である。今週JDCCの運

営委員に向け査読の依頼を実施するので、それが終わり次第、こちらの検討の場にも展開させていただきたいと思う。ただご存知の通り、今回のJDCCのインシデント対応ガイドブックのターゲットはデータセンターであるため、一般的なビルにとっては若干ハードルの高い指標になっている。例を挙げるとすれば、一般のビルでは空調が停止したらインシデントとなるが、データセンターにおいては空調の停止は大事故になる。そのためそのまま一般のビルに適応するのは過剰品質になってしまうと思うため、どのようにビルセキュリティガイドラインに適応していくかは検討が必須であろう。一方、ビルセキュリティガイドラインは既にほかの構成員からもご指摘があったように、広くビル全般を対象としているため、病院やクリーンルームなど一般のビルの中では厳しく管理する必要があるところには適応できる部分があるかもしれない。本日の事務局説明にもあったが、今後のビルセキュリティガイドラインの検討には、ビルのレベル別や規模別の対応検討が必須になってくるであろうと理解している。

奥家課長（事務局）：本日のテーマからずれるかもしれないが、SIPでビル側の取組があったかと理解しており、日立様やセコム様から情報共有いただくことは可能か。

松本構成員：SIPで調査を実施しているが、昨今サプライチェーンセキュリティやサプライチェーンインテグリティが注目されている。いかに工場出荷からのライフサイクルを守るという動きが活発であり、ビルの設備に対しても数年のうちに影響があるかもしれないと考えている。ここでいうサプライチェーンとは、製品の完成から終わりまでと、その完成した製品が色々なところに設置され、接続されるという関係の２つを意味している。

江崎座長：多くの機器、設備が設置され接続されるビルとして、今後SIP関連のサプライチェーンセキュリティやそのマネジメントについて、認識していくべきと考える。

秋山構成員：今後のガイドラインの展開について、個別編：空調システムのガイドラインが先に出たが、先ほどペンタゴンの例の話も鑑み、電力の配電システムや防災システム、昇降機の監視システム等、人の命にかかわる様な部分の個別編を優先的に取り組んでいってほしいと考えている。

松浦構成員：構成員の方のご発言やご議論をお伺いして、今後ビルセキュリティガイドラインにおいて、ビルのレベルごと等で対応を書き分けるべきという話や、安全に関わる部分を優先すべきという話があり、全体の整備が大変だと思ったため、参考になるかもしれない発言をさせていただきたい。まず始められるところとして、本日構成員の方々から上がった話等を事例集のような形で充実させていくことから取り組んでも良いのではないか。

事例集であれば読み手のユーザからしても手に取りやすく、厳密なレベル分けもせずに始められるのではないかと考える。

江崎座長：確かに事例集であれば、全体を通した網羅性が要求されないので取組みやすいかもしれない。

池田構成員：本日のご議論を伺い、感じたことを共有させていただきたい。ガイドラインについて意見を述べさせていただくと、空調や受変電といった個別の議論を突き詰めるより、ビルの規模に応じて作成いただいた方がオーナー側としては理解し易い。現状、普通のオフィスビルで起こり得るインシデントはそこまで重たくないと考えているので、そういった実情に応じたガイドラインが良いと考えている。例えば、個別編：空調システムを読んだところでオーナー側では手に負えず、全体像を理解することが難しい。言い切ってしまえばセキュリティの素人が読んでも理解出来、実施できるガイドラインを作成いただかないと活用することは厳しい。一方で昨今はセキュリティだけではなく、CO2削減の取組が重要で、ビルとして便利になる方向を目指すとセキュリティへの配慮が足りなくなってしまい、セキュリティに配慮をしすぎてしまうと、便利でもなくCO2のコストも重なってしまうことが課題として認識している。こういったセキュリティと他の観点間のバランスを取りたくとも、現状底を解決する指針がないので検討を始めることが出来ず、道は遠いと考える。今後、さらにビル単体だけではなくスマートシティの展開が広がっていく方向性の中で、セキュリティに関する落としどころや折り合いの付け方を示してほしいと考える。

奥家課長（事務局）：ビルセキュリティガイドラインとしても、ビルの全体を把握できているかと言われると確かに現状やり切れていないと認識している。現場で使いやすさを求めると記載が詳細になってしまいがちで、全体を把握しようとなると抽象的になって使い勝手が悪くなってしまいがちなのが難しい。しかしながら、せめて議論はどこまでいっているかはステークホルダーで把握できるようにしたい。最終的に魂は詳細に宿ると考えているが、現場だけではなく全体をマネジメントしている側がチェックできるような体系化や体制を整えていくしかないと考えている。スマートシティについては検討の走り出しは良かったものの、セキュリティについて軽く見すぎてしまったことにより、検討全体が止まっている印象を受ける。米国アトランタやニューヨークのように最初から足並みをそろえていけるように、現場のセキュリティレベルを統合していくしかやり方はないと考えている。実際、今後ビルや機器の全てがサイバーに繋がっていく中で、枠組み全体を考え直さなきゃいけないということ自体にまず気付いていない事業者も存在するので、まずは議論の中で、定期的にお互い情報共

有していくことが大事だと考えている。

江崎座長：池田構成員のご懸念も、奥家課長のご意見もそれぞれ非常に理解することが出来る。ビルガイドラインの検討の中で、セキュリティのマネジメントの全体感が把握でき、サイバーセキュリティをどのように捉えるべきかを何かしらのドキュメントで明確するべきであると考える。

津国様（事務局）：グループヒアリングを受けての印象だが、実際ビルのセキュリティを誰がハンドリングしていくかとなった際に、ビルのゼネコンや設計会社であるべきだと話が出た。そのためそこをうまく支援、盛り立てる仕組みは今後考えていかなくてはいけないと思った。

奥家課長（事務局）：最後に情報共有をさせていただきたい。米国だけではなくEUでもNISディレクティブの改正が行われ、重要インフラのオペレーターの対象に大規模工場や大規模設備のオペレーターも追加された。そのため日本の事業者においても、EUに工場や商業施設を保有している事業者は、今後NISディレクティブの対象となる。今回の改正で、人的管理やマネジメントのセキュリティだけではなく、調達機器のセキュリティ対応も求められるようになった。この観点からも日本においてサプライチェーンの影響が大きく出ると考えており、今後はビルでも最先端な事例では同じような要求が出てくることが想定される。欧米共にビルや工事、設備のセキュリティが厳しい方向に向かっていく中で、統合体となるビルの業界としては、他業界の動きもにらみながらビルセキュリティガイドラインの検討を推進していくべきだと考える。

江崎座長：全体としてFA（ファクトリーオートメーション）の検討も既に始まっており、ビル業界として参考にできる部分があると考える。

奥家課長（事務局）：江崎座長にご発言いただいた通り、FA（ファクトリーオートメーション）の検討についても江崎座長にチームを組んでいただいている。FA（ファクトリーオートメーション）の領域では欧米の動きは確実に影響が出ることが把握できているため、経済産業省内でもNISディレクティブやEUの新しいセキュリティの認証を含めて、対応の検討を各業界団体と連携して始めており、既に産業機械系はEUのパブコメへのコメント出しの準備を実施しているので、FA（ファクトリーオートメーション）の影響が出てくることも認識しておいてほしい。

江崎座長：FA（ファクトリーオートメーション）だけで言うと建物周りの電源や空調は抜けてしまうため、クリティカルな施設における電源や空調の検討等は本検討の場等で推進していかなければいけないと考えている。

（６）閉会

事務局より今後の進め方について事務連絡。

以上