第５章　電気系統や回転機器，駆動装置の動作異常よる事故の発生原因とその対策
第６節　プラント制御システムのセキュリティ対策

名古屋工業大学　橋本 芳宏

はじめに

2010 年に Stuxnet[1] というイランの核燃料施設をターゲットにしたマルウェアが発見されて以来，重要インフラに対するさまざまな深刻なサイバー攻撃が行われてきており，日本でも，工場が長期操業停止に追い込まれる例がの系られるが，まだまだ情報え考直しは進められてはいると見所のサイバーセキュリティの研究場や工れている。現サイバーセキュリティ対策ほど進んでいないのが実態である。サイバーセキュリティ対策の問題点を整理するとともに，世界的に進む標準的なアプローチを紹介し，この節が，化学工場や研究所のサイバーセキュリティ対策の進展への一助になればと期待する。

1. 化学工場・研究所をとりまくサイバー攻撃の危険性

危険物を扱う化学工場・研究所では，安全は最重要課題として取り扱われてきている。しかし，セキュリティは全く別の課題であると考えられていたのではなかろうか。正門には守衛がおり，建物・施設の入退出管理も行い，警備員が巡回するという防犯体制は，どの事業所もとられているであろう。そして，技術情報が盗まれるというサイバー犯罪については，多くの報道からすでに意識されており，情報技術者がインターネットから社内ネットワークへの侵入を防ぐために，ゲートウェイを管理しているに違いない。しかし，制御系のネットワークは，情報通信技術者ではなく，計装技術者が担当し，製造やサービスの効率や品質の向上に注力するために，IoT や遠隔監視など様々な技術の導入は進展するものの，IT 部門では普通に適用されているセキュリティ対策が取られていないことが多い。たとえば，パスワードやは，非常事態に運転を交代するときに入力を要求すると，その分，対応が遅れる可能性があるし，PC では常識になっているアンチウィルスソフトやセキュリティパッチも利用されていないことが通常である。これまでは，外部との通信も限定的で，そのゲートウェイを IT 部門に任せておけば，制御ネットワークはサイバーセキュリティ対策をしなくても大丈夫なのではという甘えもあったと思われるが，工事や保全での保守 PC や監視カメラ・ネットワークからの侵入・感染の手口も発生しており，重要インフラの現場を対象にした高度なサイバー攻撃が発生している。独立防護層の重要な安全対策である安全計装（SIS : Safety Instrumentation System）を対象にしたサイバー攻撃も発生しており，工場を対象にした制御系ネットワークのセキュリティ対策は，安全を守るためにも，企業のコンプライアンスのためにも，不可欠な状態になっている。

表 1[2] に，世界的にも制御系セキュリティの重要性の見直しの発端となった Stuxnet から 2019 年までに発生したインシデントの例を示した。ここで，セキュリティの世界では，どんなに甚大で深刻な事故もアクシデントとは呼ばず，インシデントとよぶことに留意いただきたい。化学工場以外の例も示しているが，サイバー攻撃が，身代金の形や報酬といった金銭目的や敵対している組織の信用失墜や事業損失，政治的や軍事的な目的など高度な専門的集団によるものが多くなっていることが理解できる。

また，サイバー攻撃を企画するための開発プラットフォームも充実しており，マルウェアは見つからないことを確認してから野に放たれるし，未知の脆弱性を含む攻撃ツールが流通する闇市場も存在する。図 1[3] に 2005 年から 2019 年までの新たなマルウェアの種類の発生数を示す。2005 年には，1 年間に 170 万種であったのが，2019 年には，9 億種を超えている。攻撃の対象となる脆弱性は，ソフトウェアだけでなく，Intel の CPU などハードウェアにも発生しているが，アメリカの米国標準技術研究所（NIST : National Institute of Standard and Technology）の標準ソフトウェアに発生した脆弱性のデータベースへの登録数毎年 4 桁のコードで表現されていたのだが，2018 年で 1 万件を超えて，登録桁数を増やさねばならない状態になり，現在も登録数は増えている。この脆弱性は，プログラムのバグというよりも攻撃者による発明品とよぶべきもので，こんなことが攻撃の起点にされてしまうと驚くようなものが

表 1　制御系システムのインシデント事例

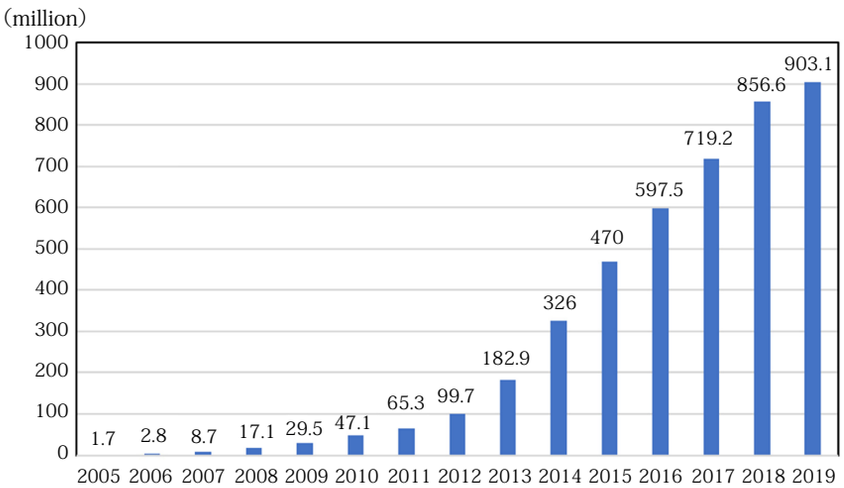
事例名	業界／分野	発生国	発生年月	影響・被害	内容（原因等）
ウラン濃縮施設の遠心分離機における Stuxnet 感染	電力	イラン	2010 年 11 月	ウラン濃縮施設の遠心分離機がマルウェアに感染し，約 8,400 台の遠心分離機が 停止した。	USB メモリを介して，マルウェア（ワーム）Stuxnet に感染。Stuxnet は，周波数変換 装置を制御する PLC に侵入し，周波数を変え回転速度を通常よりも上げたり下げたりすることで，最終的に遠心分離機を破壊 した。
国際宇宙ステーションにおけるマルウェア感染	宇宙	ロシア	2013 年 5 月	マルウェアに感染した時期や感染による影響については明らかにされていない。	国際宇宙ステーション（ISS）がロシア人宇宙飛行士によって持ち込まれた USB メモリからマルウェアに感染した。
エネルギー業界を標的とした産業制御システムへの攻撃	電力	米国 スペイン フランス イタリア ドイツ トルコ ポーランド	2014 年 6 月	攻撃を仕掛けているのは Dragonfly と呼ばれる集団で，スパイ活動や継続的なアクセスを目的として多数の組織に侵入している。攻撃側がその気になれば，電力供給網に対する妨害工作を仕掛けられる恐れもあった。	Dragonfly は，産業制御システム（ICS）メーカーのソフトウェアに，リモートアクセス機能を持ったトロイの木馬を感染させ，ソフトウェアアップデート経由で ICS を運用しているコンピュータにマルウェアをダウンロードさせる手口を使っていた。
ドイツの製鉄所へのサイバー攻撃	鉄鋼	ドイツ	2014 年 12 月	ドイツの製鉄所で，サイバー攻撃によって溶鉱炉が正常にシャットダウンできず，装置及び製鉄システム（操業）に大きな損害を与える事件が発生した。	攻撃は，特定の従業員らに対する標的型攻撃（スピアフィッシング）を通じて認証情報や機微な情報を窃取して，OA ネットワークに侵入し，その後，生産システムに侵入を拡大した。
ウクライナ電力施設へのサイバー攻撃	電力	ウクライナ	2015 年 12 月	ウクライナ西部の州の半分と州都の一部で停電が発生，復旧までに約 6 時間を要し 40 ～ 70 万人程度が影響を受けた。ICS が使えず，復旧は手動により行われた。	変電所を監視する SCADA システムに侵入し，ワークステーションやサーバをマルウェア BlackEnergy3 に感染させた。その後，監視機能を停止させると共に SCADA システムのファイルを削除した。
イスラエル電力公社への大規模なサイバ ー攻撃	電力	イスラエル	2016 年 1 月	電力供給を管轄する電力公社が大規模なサイバー攻撃を受け，コンピュータ多数が使用不能になる深刻な事態に陥った。	電力公社のコンピュータを使用不能に陥れたのはランサムウェア。メールで送られてきたマルウェアが公社内のネットワーク全体に広がって多数のコンピュータが暗 号化され，身代金を要求するメッセージが 表示されていた。
ドイツの原子力発電所におけるマルウェア感染	電力	ドイツ	2016 年 4 月	原子力発電所で，核燃料棒を操作しているコンピュータがマルウェアに感染しているのが発見された。マルウェアが発見されたコンピュータは，インターネットに接続していなかったため，マルウェアが活動を始めることはなく，発電所の運転に影響はなかった。	3 基の原子炉のうち，稼働中の B 号機のコンピュータから，PC を遠隔操作できる W32.Ramnit と，PC 内部のファイルを盗み取る Conficker という 2 種類のマルウェアが，発電所の技師により発見された。また，原子炉の操作システムを管理している場所から離れた別のオフィスでは，マル ウェアに感染した USB メモリ 18 本が見つかった。なお，Conficker と W32.Ramnit は，どちらも USB メモリ経由で拡散する。
サウジアラビアの空港，政府機関への攻撃	航空	サウジアラビア	2016 年 11 月	民間航空総局の事務管理システムの PC 数千台が破壊される被害が発生，業務が数日間停止した。運航や空港業務，航空システムには影響は出ていない。少なくとも 8 つの政府系組織で被害が確認された。	マルウェア Shamoon の新型が攻撃に使われた。Shamoon は，起動時に読み込まれるマスターブートレコードを消去し，コンピュータを機能不全にする。
サンフランシスコの交通システムにおけるランサムウェア感染	交通	米国	2016 年 11 月	サンフランシスコの交通公社で，最大 2,112 台のコンピュータがランサムウェアに感染し，料金徴収が不能になった。電車やバスの運行自体には影響なく，市営鉄道の改札を開放して対応し，3 日後に完全復旧した。	コンピュータがランサムウェアに感染し，ハッカーらは復号鍵と引換えに 100 ビットコインを要求し，支払わなければ盗んだ 30GB のデータを公開するとも脅迫したが，内部調査の結果データ窃取はハッカ ーのハッタリと判断し，脅しを無視した。感染経路は従業員によるメールの添付ファイル／ポップアップ／リンクのクリックと見られる。
ウクライナ電力施設へのサイバー攻撃	電力	ウクライナ	2016 年 12 月	ウクライナの首都キエフ北部とその周辺地域において停電が発生した。手動運用に切り替え，30 分以内に電力供給が再開され，約 1 時間 15 分後に完全に復電した。	電力会社のシステムがマルウェア Industroyer/Crashoverride に感染し，送電変電所の遮断機が不正操作された。

表 1　つづき

事例名	業界／分野	発生国	発生年月	影響・被害	内容（原因等）
英国最大の病院におけるランサムウェア感染	医療	英国	2017 年 4 月	英国で最大規模の病院グループで，IT 障害のため 136 件の手術と数百件のがん患者の化学療法の予約をキャンセルする事態が発生した。抗がん剤を処方するシステムや医用画像情報システムが使用不能になったほか，血液検査等も不能になった。遠隔で画像を確認することもできなくなった。	WannaCry（ランサムウェア）の感染が原因であった。なお，同病院では，セキュリティに問題がある Windows XP が現役で使われていた。
日本国内の自動車の生産システムにおけるランサムウェア感染	製造（自動車）	日本	2017 年 6 月	自動車の生産工場で，工場設備に付帯する PC が WannaCry に感染しているのが発見され，約 1 日間生産ラインを停止し，1,000 台が生産できなかった。他工場への影響はなく，同工場も翌日には操業を再開した。	生産ラインの管理等に使用する PC が WannaCry に感染した。5 月に世界中で WannaCry 感染が報告されたのを受けて対策を固めていたが，完全に防ぐのは難しいことが改めて示された。
オーストラリアヴィクトリア州の交通関連のカメラにおけるランサムウェア感染	交通	オーストラリア	2017 年 6 月	ヴィクトリア州で，159 台のスピード違反取り締まりカメラと交差点監視カメラが，WannaCry に感染した。感染により断続的に再起動を繰り返す状態が発生した。7,500 件の違反切符について一旦取り消すと発表した。	保守作業用に持ち込まれた USB メモリによって WannaCry に感染した。
重要インフラ事業者の制御システムへの侵入による安全計装システムのマルウェア感染	製造（化学）	サウジアラビア	2017 年 8 月	事業者が使用している特定の安全計装システム（SIS）を狙ったマルウェア Triton（別名 Trisis, HatMan）に，SIS が感染した。何台かの SIS コントローラが異常状態に陥ったため緊急シャットダウンが作動し，一部の制御プロセスが停止した。	SIS のエンジニアリングワークステーションにリモートアクセスされ，Triron に感染した。Tiriton は SIS コントローラと通信し，プログラムを改ざんする機能を持っており，攻撃の過程で攻撃者のミスにより誤って緊急シャットダウンが引き起こされたと推測されている。
ノルウェーのアルミニウム生産会社におけるランサムウェア感染	製造（非鉄金属）	ノルウェー	2019 年 3 月	世界有数のアルミニウム生産会社のコンピュータシステムがランサムウェア LockerGoga に感染した（22,000 台の PC のうち 11,000 台が感染／2,700 台が暗号化，3,000 台のサーバのうち 1,100 台が感染／500 台が暗号化）。一部生産ラインが停止したほか，他の生産ラインも手動での運用を強いられた。生産ラインの操業は約 1 ヶ月後にほぼ通常に戻ったものの，IT システムの完全復旧には数ヶ月を要した。金銭的損失は，2019 年前半で 5.5 億～ 6.5 億クローネ（約 66 億～ 78 億円）と発表。	2018 年 12 月，従業員に既知の第三者とのやり取りを悪用したなりすましメールが送られ，従業員が本文中の URL をクリックし，バックドア型不正プログラム Gootkit に感染したことが発端となった。
米国の電力事業者への DoS 攻撃	電力	米国	2019 年 3 月	再生可能エネルギー電力会社のファイアウォールを数時間にわたって繰り返し再起動させる DoS 攻撃が発生。12 の太陽光発電設備および風力発電設備との通信が，各施設最大 5 分間中断した。発電への影響はなかった。	ファイアウォールの既知の脆弱性が悪用され，ファームウェアのパッチをあてることで収束した。セキュリティベンダは「続く攻撃が行われなかったことから，推測だが，当該脆弱性をスキャンしていた攻撃者が，意図せず DoS を引き起こしたのではないか」と話している。
ベルギーの航空機部品メーカーにおけるランサムウェア感染	製造（航空）	ベルギー	2019 年 6 月	航空機部品メーカー大手の工場が 6 月 7 日にランサムウェアに感染し，生産が停止。併せてドイツ，米国，カナダの工場もシャットダウン。1,400 人の従業員のうち約 1,000 人が自宅待機に。なお，生産拠点ではないフランスとブラジルの事務所は影響なし。6 月 28 日時点で「一部の操業を再開したが，完全復旧がいつになるかは不明」と発表。	感染の経緯等は明らかにされていない。
ドイツの自動車部品メーカーにおけるマルウェア感染	製造（自動車）	ドイツ	2019 年 9 月	ドイツの自動車部品メーカーが，ブラジル，メキシコ，米国の工場がマルウェアに感染し，製造に多大な影響が出ていると発表。恐らく 2 ～ 4 週間続く見込みで，週に 328 万 ～ 438 万ドル（約 3 億 5 千万～ 4 億 6 千万 円）の損失を被ると予想。なお，工場外部の同社の IT システムは影響なし。	感染の経緯等は明らかにされていない。

続々と発生している。

すでに化学工場では合理化・省力化によって，生産計画や保全情報などの通信が操業現場に対して不可欠になり，製品出荷にもトレーサビリティの情報が不可欠となっているので，たとえ，安全が確保できて，ものが製造できる状態でも，情報が得られないと，操業は継続できないという状況も発生するようになっている。被害は発生していなかったが，ウィルスを駆除するために操業を停止し，その後，駆除がうまくできず，1 か月以上の操業停止に陥った事業所は日本にも存在し，安全は確保できても，甚大な経済的損失が発生する可能性があることにも留意が必要である。この操業停止の例は，届け出が義務付けられているわけではないので，統計には現れておらず，統計に現れていない被害は，すでに日本でも多数発生している。



The AV-Test Security Report
https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2018-2019.pdf

図 1　2005年から発生したマルウェアの種類の積算数

2.　制御系のサイバーセキュリティに関する世界的な取り組み

Security for Industrial Automation and Control Systems に関する世界標準として，表 2[4] に示すように IEC62443 が制定され，現在も検討が進められている。この規格は，セキュリティポリシー，手順，システム，コンポーネントという観点，あるいは，制御系のユーザー，システム構築，装置ベンダという立場を広くカバーする指針となるものである。これに対応したコントロールベンダーや装置に対する認証も IEC62443 が認証資格になって，中東など海外でのプロセス制御系の調達においては，それらの認証取得を契約条項として取り入れられるようになっている。日本でも 2013 年に経済産業大臣認可法人として技術研究組合「制御システムセキュリティセンター」（CSSC : Control System Security Center）が設立され，EDSA（Embedded Device Security Assurance）認証活動を開始している[5]。さらに 2014 年には，日本で CSMS（Cyber Security Management System for IACS [Industrial Automation and Control Systems]）認証が設立され，日本情報経済社会推進協会 JIPDEC がその認定を進めている[6]。

重要インフラのサイバーセキュリティ強化への指令として，2013 年 2 月にアメリカでは大統領令（US Executive Order）[7] が，EU では欧州指令（EU Cybersecurity Directive）[8] が発令された。そして，2014 には，サイバーセキュリティ強化のための標準的なアプローチを示すものとして，米国標準技術研究所 NIST から Cybersecurity Framework の ver. 1.0 が発行され，2018 年には ver. 1.1 が発行されている。このフレームワークについは後に詳説する。日本においても，表 3 に示すような各種ガイドラインが 2016 ～ 2017 年にかけて制定された[7]。石油・化学業界についても制定されているので，ぜひ一読いただきたい。

防護レベル：Security Program Rating

ML4	SPR0	SPR1	SPR2	SPR3	SPR4
ML3	SPR0	SPR1	SPR2	SPR3	SPR4
ML2	SPR0	SPR0	SPR0	SPR0	SPR0
ML1	SPR0	SPR0	SPR0	SPR0	SPR0
	SL0	SL1	SL2	SL3	SL4

組織的運用評価：Maturity Level

ML4	体制が最適化され継続的な改善が行われる
ML3	体制として定着している
ML2	手順は文書化されていて，実施できる人はいる
ML1	実施はしているが，文書化されていない

技術的評価：Security Level

SL4	巧妙な手法，拡張リソース，IACS に特化したスキルを有し， かつ高い動機を持つ攻撃者による意図的なセキュリティ違反から保護
SL3	巧妙な手法，中程度のリソース，IACS に特化したスキルを有し， かつ中程度の動機を持つ攻撃者による意図的なセキュリティ違反から保護
SL2	単純な手法，限られたリソース，一般的なスキルを有し， かつ低い動機を持つ攻撃者による意図的なセキュリティ違反から保護
SL1	偶発的，または偶然のセキュリティ違反からの保護
SL0	特定のセキュリティ保護がない

https://www.jpcert.or.jp/present/2020/ICSR2020_04_HITACHI.pdf から編集

図 2　IEC62443 におけるセキュリティ管理レベルの評価

表 2　IEC62443（Security for Industrial Automation and Control Systems）[4)]
IEC : International Electrotechnical Commission

区分	主対象者	IEC	原本名	詳細
共通	一般	62443-1-1	Concepts and models	セキュリティ概念，参照モデル（5 段階）資産モデル，ゾーン＆経路モデル
		62443-1-2	Master glossary of terms and abbreviations	用語と省略表示の解説
		62443-1-3	System security compliance metrics	セキュリティの評価指標
		62443-1-4	IACS security lifecycle and use-cases	制御システムのライフサイクルとユースケース
方針と手順	事業・運用者	62443-2-1	Security program requirements for IACS asset owners	事業者へのセキュリティプログラム要件
		62443-2-2	IACS protection levels	制御システムの防御レベル
		62443-2-3	Patch management in the IACS environment	制御システムのパッチマネジメント
		62443-2-4	Security program requirements for IACS service providers	制御システムのプロバイダーへのセキュリティプログラム要件
		62443-2-5	Implementation guidance for IACS asset owners	制御システムの実装ガイド
システム	構築事業 . SIer	62443-3-1	Security technologies for IACS	セキュリティ技術の解説書：認証，フィルタリング／ブロッキング，アクセス制御，暗号／データ保護，管理・監査・証跡，ソフト管理，物理セキュリティ人的セキュリティ
		62443-3-2	Security risk assessment and system assign	セキュリティリスク評価と対策配備
		62443-3-3	System security requirements and security levels	システムに対するセキュリティ要件，保証レベル（3 段階）の要件
部品	装置ベンダ	62443-4-1	Secure product development lifecycle requirements	セキュアなコンポーネントの開発ライフサイクルに対する要件
		62443-4-2	Technical security requirements for IACS components	制御システムの部品に対するセキュリティ機能要件
共通	一般	62443-5-1	Guidance on how to write a profile	プロファイルの書き方のガイド

表 3　制御システムの各種ガイドライン

重要インフラ分野の基準・ガイドライン等

分野		発行元	名称
情報通信	電気通信	総務省	情報通信ネットワーク安全・信頼性基準
			電気通信事業法／電気通信事業法施行規則／事業用電気通信設備規則
		電気通信事業者協会	電気通信分野における情報セキュリティ確保に係る安全基準（第 3 版）
	放送	放送セプター	放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン
	ケーブル	日本ケーブルテレビ連盟	ケーブルテレビの情報セキュリティ確保に係る「安全基準等」策定ガイドライン
金融	銀行等 生命保険 損保保険 証券	金融情報システムセンター	金融機関等におけるセキュリティポリシー策定のための手引書
			金融機関等コンピュータシステムの安全対策基準・解説書
			金融機関等コンピュータシステムの安全対策基準・解説書
航空	航空運送	国土交通省	航空運送事業者における情報セキュリティ確保に係る安全ガイドライン（第 4 版）
	航空管制		航空管制システムにおける情報セキュリティ確保に係る安全ガイドライン（第 4 版）
鉄道			鉄道分野における情報セキュリティ確保に係る安全ガイドライン（第 3 版）
電力		電気事業連合会	電力制御システム等における技術的水準・運用技術に関するガイドライン
		日本電気協会	スマートメータシステムセキュリティガイドライン
			電力制御システムセキュリティガイドライン
ガス		日本ガス協会	製造・供給に係る制御系システムのセキュリティ対策ガイドライン
石油		石油連盟	石油分野における情報セキュリティ確保に係る安全ガイドライン
化学		石油化学工業協会	石油化学分野における情報セキュリティ確保に係る安全基準
水道		厚生労働省	水道分野における情報セキュリティガイドライン
物流		国土交通省	物流分野における情報セキュリティ確保に係る安全ガイドライン（第 3 版）
医療		厚生労働省	医療情報システムの安全管理に関するガイドライン（第 4.3 版）
クレジット		日本クレジット協会	クレジット CEPTOAR における情報セキュリティガイドライン
政府・行政サービス		総務省	地方公共団体における情報セキュリティポリシーに関するガイドライン

NTTdata 解説 / 制御系システムのセキュリティ（1）
http://www.intellilink.co.jp/article/column/sec-controlsys01.html

3.　プロセス制御系独自のサイバーセキュリティの問題点

情報セキュリティで重要な三要素は，機密性（Confidentiality）完全性（Integrity）可用性（Availability）である。化学工場・研究所におけるセキュリティでは，24 時間安全操業が求められるので，安全確保も含めたプロセス制御システムの可用性が特に重要である。そのため，情報ネットワークで一般的なセキュリティ対策を採用できない面がある。

例えば，インターネットに接続していない制御システムでは，毎日のように行われるアンチウィルスのデータベー

ス更新や OS のセキュリティパッチの適用はできない。インターネットに接続して更新が可能であるとしても，アンチウィルスソフトによる CPU 負荷増加がリアルタイム制御演算に支障を与える可能性や OS パッチによる制御用ソフトウエアの不具合発生が懸念され，やはり容易に適用することはできない事情がある。

また，制御システムの更新頻度は 15 ～ 20 年と情報系よりもずっと低いのが通常であり，90 年代に開発された機材が未だに稼動している。これらの，旧来型のシステムで用いられているフィールドバスやネットワークの設計には，最新のサイバーセキュリティの観点は取り込まれておらず，通信には認証や暗号化が採用されていないのが実情である。

そして，メンテナンスやパフォーマンス監視を省力化するために，コントローラの状況がインターネットを介したリモートアクセスによって確認できるようになっているシステムも少なくない。どのコントローラのマニュアルもインターネットで検索でき，操作量の変更やフィードバックの符号の変更の手順も簡単に入手できる。あてずっぽうでコントローラのアドレスを指定して，異常な操作を指示する単純な攻撃であれば，実現はたやすいと考えられる。もし，制御ネットワークにそのようなウィルスが入ってきたら，すべてのコントローラが同時に破綻してしまうという事態が発生することも想像に難くない。

制御ネットワークへのインターネットからの侵入は，ファイアーウォールなどで防御されているものの，一旦侵入されてしまうと脆弱性の高い環境になっている。そして，侵入経路は，インターネットからだけでなく，USB や保守用のリモート回線，あるいは点検整備用に持ち込まれる PC，さらには，開発時点からマルウェアが潜んでいたケースすら存在する。セキュリティを確保するための情報技術の進歩は速いが，新たなサイバー攻撃手法が次々と現れ，イタチごっこは免れない。対策が開発されたとしても，制御システムセキュリティ専任のスタッフが居ない現場では，適用の遅れや漏れが発生する可能性が高い。そのため，被害は発生するという前提で対策を検討することが重要である。そして，危険物を扱うプラントで採用されている，被害が発生したとしても大事故にはならないように対応するための「フェールセーフ」の考え方をセキュリティ対策についても導入すべきである。

なお，情報セキュリティでは脆弱性が見つかった場合，情報を公開してセキュリティパッチを交付するが，制御システムセキュリティでは，脆弱性の存在を知ってもすぐに対策が適用されない可能性や対策の開発に時間がかかる可能性が高い。そのため，脆弱性情報の開示や共有に関しても情報系とは異なる体制が必要である。

4. プロセス制御系のリスク解析とセキュリティ対策

4.1 化学プラントで考慮すべきサイバーリスクと特徴的な対策

化学工場にとって，最も重要なのは安全の確保である。サイバー攻撃も安全を破綻させる原因の一つであり，侵入・ウィルス感染の如何に関わらず，攻撃者ができることはインテリジェントを有する装置の遠隔操作か無効化である。そのため，サイバー攻撃は「悪意の誤操作，悪意の誤動作」と考えることができる。発生する事故は，サイバー攻撃の手段がどのように巧妙になったとしても攻撃手口で決まるものではなく，攻撃されたプラントが持つ特性で定まる。

ただし，サイバー攻撃を対象にした安全解析では，同時多発での発生を前提として故障と誤操作の影響を想定する必要がある。つまり，サイバー攻撃者は成果を確実にするために，悪意の操作を重複させる可能性があり，ウィルスでは多くの個所を同時に襲うことも可能である。これまでの安全解析では，同じ装置を複数設置して多重化すれば事故発生率は低下するとした。しかし，サイバー攻撃では攻略できる装置をいくら多重化しても効果はない。そのため，これまでの安全解析とは異なるアプローチが必要になる。

通常，1 つのプラントに対して 1 つの DCS として計装を行うが，攻撃対象となる DCS を分割して，例えば，ボイラーの温度制御と液位制御のネットワークを分離し，同時に攻撃に陥落しにくいようにできると，温度制御が破綻して，ヒーターがつきっぱなしになっても，水が存在する限りは大事故にならず，水位制御が破綻して水がなくなっても，ヒーターを遮断できれば，やはり大事故は防げるというように，リスク軽減が実現できる。このコントローラ群をゾーンに分割することにより，隠ぺい工作を見破れる可能性も発生するので，プラントの特性を利用したセキュリ

ティ対策として一考の価値があると考える[10,11]。

実は，このような制御システム自体をゾーンに分割するという発想は，ほとんどのサイバーセキュリティのアプローチには，取り上げられていないが，自動計装の異常動作だけがサイバー攻撃による安全の破綻源であることを強く意識すれば，その一部が破綻しても，残る部分で安全を確保できるような構成を検討することは，自然なアプローチであり，ほとんどのガイドが情報通信技術者を中心に検討されており，プロセス自体への関心の低さが影響していると考えられる。DCS を分割しなくても，一部をハードリレーにするとか，手動操作と組合すという工夫もありうる。ぜひ，プロセス技術者の立場から，サイバー攻撃からの防御を主体的に検討していただきたいと期待する。

また，安全が確保できれば，それでよいというわけにはいかない。サイバー攻撃により，コントローラの指示がずれ，品質が悪化してしまうと，製造ロスが発生するし，顧客のところに不適切な製品が送られることになると，クレームやリコールが発生して，経済的損失だけでなく，信用失墜にもつながる。薬品製造のような厳しい品質管理を行うものでも，工程での情報を活用することで，製品の検査を簡略化する方向にあり，工程での情報を改ざんされることの影響は，どんどん深刻になっていると考えられる。

さらに，安全は確保できたものの，復旧までに時間がかかるというリスクも重要な検討課題である。ウィルス駆除だけで 1 か月も操業停止になった事業所も存在するように，その復旧までの手順の整備は重要検討課題である。

4.2　制御系セキュリティの標準的なアプローチ NIST の Cybersecurity Framework

制御系セキュリティ対策の標準として，前述の大統領令[7]に従い，2014 年に米国標準技術研究所 NIST から提案された Cybersecurity Framework をここで紹介する。これは，様々な基準やガイドライン，実施例をもとに，組織が以下のような活動を実施するにあたり，一般的な分類法や手法を示すものである。

1）現行のサイバーセキュリティの取り組みを説明する
2）目標とするサイバーセキュリティ耐悪の実施状況を説明する
3）継続的かつ繰り返し実施可能な改善を特定し，優先付けを行う
4）目標達成までの進捗を評価する
5）社内外の利害関係者とサイバーセキュリティリスクについてコミュニケーションを行う

この Framework は，対象の組織規模や業種，IT セキュリティや制御セキュリティに関わらず適用できるものとして提案されている。

図 3 に Cybersecurity Framework に示されている組織内の情報と意思決定の流れを示す。Framework では，経営陣の参画の重要性が強く意識されており，経営陣でのリスクマネジメントと操業現場での実装が正しくつながるように，真ん中のビジネス層の役割が明確化されることになる。

図 3 の右側の 2 つの矢印は，経営層からのセキュリティポリシーとそれによる事業戦略や予算を受けて，ビジネス層は予算配分を適切にきめて，フレームワークのプロファイルを設計し，現場での実装に渡すという流れを示す。左側の矢印は，現場の脆弱性の変化や最新の攻撃の情報を取り入れ，リスク分析を行い，その結果を経営層に提言し，意思決定を促すという流れである。この両方の流れがうまく廻ることによりサイバーセキュリティは確保される。

この情報の流れに示されているフレームワークのプロファイルは，セキュリティ対策の様々な側面の情報をもつものであるが，表 4 に示されるコア Core の項目を細分化として整理され，事業所ごとの情報を反映して決められる。セキュリティ対策を 5 つの段階で整理したコアの最初の［特定］（Identify）には，サイバー攻撃で起こりうるインシデントを特定するための技術が整理され，次に，［防護］（Protect）のための技術が整理される。インシデントが発生した順に関係する［検知］（Detect），［対応］（React），［復旧］（Recover）がつづく。

評価対象の事業所に応じて，コアのカテゴリごとに，管理レベルを Tier1 から Tier4 として整理して，現状と目標の Tier を設定し，改善を計画するというアプローチが図れる。

この Tier の整理では，コアのカテゴリという観点だけでなく。図 4 に示す People, Processes, Products, Partners という 4P の観点で整理するアプローチもあるし，図 4 の ① から ⑥ で示すような観点での整理もありうる。組織の課題，特性に応じて，使い分けながら，セキュリティリスクの低減や適正な管理を実現することをめざせればよい。

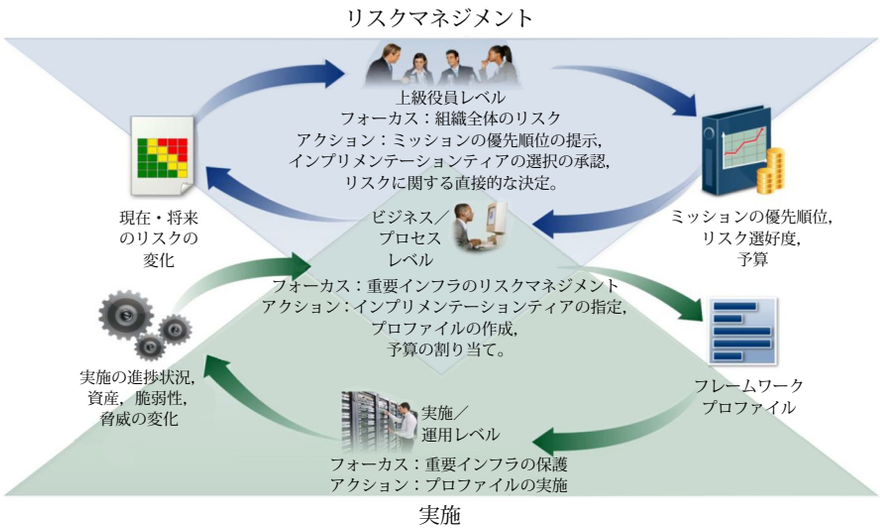


図 3　NIST Cyber Security Framework での組織内の情報の流れと意思決定の流れ

表 4　NIST Cybersecurity Framework のコアとティア

コア(Core)	コアのカテゴリー	管理レベル				現状 Tier	目標 Tier
		Tier 1	Tier2	Tier3	Tier4		
特定 (Identify)	アセット管理 サプライチェーン管理						
防護 (Protect)	ID管理＆アクセス制御 啓発・教育						
検知 (Detect)	異常検知 モニタリング						
対応 (Respond)	対応計画、通信遮断 手動操業、フォレンジック						
復旧 (Recovery)	復旧計画、バックアップ切替、改善策						
		部分的理解	リスク理解	反復可能	適応可能		

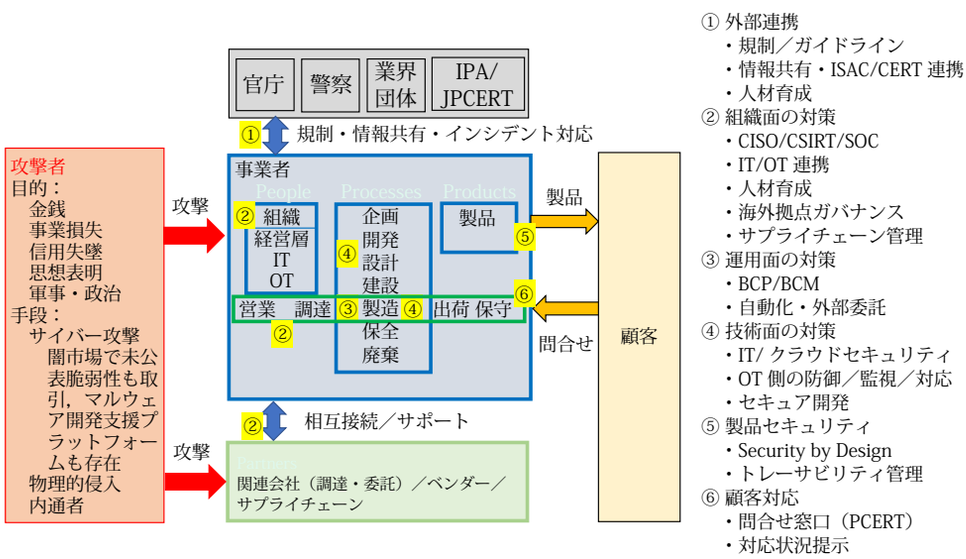


図 4　事業活動におけるサイバーセキュリティ対策の観点

2015 年発刊のこの工場・研究所の安全ハンドブックには，USB の禁止やホワイトリスト，ハニーポットの導入などの対策案を書き並べたが，それ以降，様々なインシデントが発生しており，表 5 に示すように 2016 年と 2019 年でも懸案となる優先順位が変化している。購入できるものから導入していくとか，思い付きで対策を選択している場合ではないと考え，ここでは，NIST の Framework というシステマティックなアプローチを紹介し，それを活用して，自分なりの対策を策定していただきたいと考えている。選択可能なツールも充実してきているし，新たなものも開発されるであろうから，その状況に応じた選択をされることを期待する。

表 5　IPA「産業用制御システムのセキュリティ 10 大脅威と対策」2019
https://www.ipa.go.jp/files/000079818.pdf

産業用制御システムのセキュリティ 10 大脅威（2019 年）		2016 年
1 位	リムーバブルメディアや外部機器経由のマルウェア感染	2 位
2 位	インターネットおよびイントラネット経由のマルウェア感染	3 位
3 位	ヒューマンエラーと妨害行為	5 位
4 位	外部ネットワークやクラウドコンポーネントへの攻撃	8 位
5 位	ソーシャルエンジニアリングとフィッシング	1 位
6 位	DoS/DDoS 攻撃	9 位
7 位	インターネットに接続された制御機器	6 位
8 位	リモートアクセスからの侵入	4 位
9 位	技術的な不具合と不可抗力	7 位
10 位	スマートデバイスへの攻撃	10 位

4.3　教育・訓練，人材育成

さまざまなガイドラインでも，人材育成や演習の必要性が述べられている。比較的進んでいる情報セキュリティの世界でも，人材不足が叫ばれているが，制御系セキュリティとなるとさらに専門的な立場になれる存在は少ない。その欠乏よりも，経営者の意識が，そこに至っていないことの方が問題であるかもしれない。そこで，ここでは，制御系セキュリティの人材育成について論じることにしたい。経済産業省のプロジェクトとして，2017 年から産業サイバーセキュリティセンター [14] が情報処理推進機構内に設立され，中核人材育成プログラム [15] も始まった。これは仕事を離れ，1 年間座学演習を繰り返し，エキスパートを要請するクラスで年間 80 名弱を輩出している。経営者向きにもより短期間で適切な気づきを与え，具体的なアプローチを身につけるための講習も行っている。関心を高めるためのゲーム形式の演習も開発されており，気軽にまず始めてもらい，制御系セキュリティ向上への活動につながること意識したものになっている。

あらゆる操業現場が制御系セキュリティに関係し，特に，サプラインチェーン攻撃といって，重要視されているプラントではなく，それに付随する部分を攻撃することで。チェーンとしてのサービスを停止させてしまうという攻撃も危惧されているので，部品供給の子会社や関連会社のセキュリティ担保も課題になる。それぞれの現場にサイバーセキュリティの専門家を確保することは困難であるので，その専門家が存在しない前提で，必要な対応をとれる体制を築く必要がある。

内閣サイバーセキュリティセンター（NISC : National center of Incident readiness and Strategy for Cybersecurity）が実施している分野横断型演習 [16] は，大規模なもので，2019 年には参加者数は約 5000 人に達した。インシデントのシナリオを用いて，疑似体験を行う演習で有効なものであるが，1 年に 1 回，企業の中のどこかの事業所が対象という実施形態になるのが惜しい点てある。サイバー攻撃が関係する部署は，一部だけではなく，また PDCA（Plan Do Check Action）サイクルを廻す必要があるため，さらに広範囲で頻度高く演習を繰り返す必要がある。そのため，内閣府の戦略的イノベーション創造プログラム（SIP）の 11 番目のテーマである重要インフラ等のサイバーセキュリティの確保の中に，人材育成の課題が設定され，より実施しやすく，サイバー攻撃を身近に感じて，主体的にサイバー

セキュリティに取り組む原動力になるインシデント対応演習[17]が開発された。これ以外にも，前述の中核人材育成プログラム[15]などにおいても，セキュリティ向上のための演習が開発されている。セキュリティの向上には，関係者の意識の向上が不可欠で，このような演習が早く普及することを願っている。

おわりに

2015年に発行された「化学工場・研究所の事故・災害対策とリスク管理」にもサイバーセキュリティの節を寄稿したが，それから5年間で，サイバーセキュリティ関連の状況には大きな変化があり，プロセス制御システムもExxon Mobilを主体に，これまでのDCSオペレーションから，仮想環境やクラウドを駆使した新たなOpen Process Automation[18]への変革もうたわれている。2020年には，COVID-19の蔓延により，世界経済は大きな打撃を受け，在宅勤務という働き方だけでなく，生活様式の変更が求められるようになってきている。この大きな変革は，情報通信の役割がより重要となってきているが，その中でも新たなサイバー攻撃がぞくぞく現れており，セキュリティ対策の重要性はますます高まってきている。ここではセキュリティフレームワークというセキュリティのとらえ方，進め方の基本的な考え方が存在することを紹介し，セキュリティに対する意識を向上させ，PDCAを推進するための演習についても紹介した。安全対策も重要であるが，セキュリティ対策にもぜひ主体的に取り組んでいただければと期待する。

文　　献

1）JP-CERT : Stuxnet ～制御システムを狙った初のマルウエア～
https://www.jpcert.or.jp/ics/2011/20110210-oguma.pdf（2011）

2）IPA［制御システムのセキュリティリスク分析ガイド］第２版
https://www.ipa.go.jp/files/000080712.pdf

3）The AV-TEST Security Report
https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2018-2019.pdf

4）藤田淳也，制御システムセキュリティの標準化動向：JPCERT
https://www.jpcert.or.jp/present/2020/ICSR2020_04_HITACHI.pdf

5）CSSC認証ラボラトリー　http://www.cssc-cl.org/

6）経済産業省：世界初！制御システムのセキュリティマネジメントシステム（CSMS）の国際標準に対する認証を日本企業が取得しました
http://www.meti.go.jp/press/2014/04/20140425003/20140425003.pdf（2014）

7）B. Obama : Executive Order 13636 (Improving critical infrastructure cybersecurity)
http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (2013)

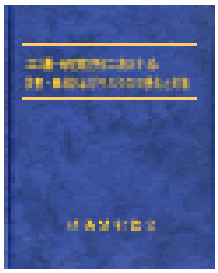
8）European Commission : EU Cybersecurity plan to protect open internet and online freedom and opportunity-Cyber Security strategy and Proposal for a Directive
http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security (2013)

9）制御系システムのセキュリティ（1）/NTTDaTa
http://www.intellilink.co.jp/article/column/sec-controlsys01.html

10）Y. Hashimoto, et. al., Safety securing approach against cyber-attacks for process control system, Computers and Chemical Engineering, 57, 181-186 (2013)

11）H. Moritani et. al., Development of CAD for Zone Dividing of Process Control Networks to Improve Cyber Security, ICC AS 2014, Korea (2014)

12）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
https://www.ipa.go.jp/files/000071204.pdf
13）［ドイツ BSI］産業用制御システム（ICS）のセキュリティ－ 10 大脅威と対策 2019 －
https://www.ipa.go.jp/security/controlsystem/bsi2019.html
14）産業サイバーセキュリティセンター　https://www.ipa.go.jp/icscoe/
15）産業サイバーセキュリティセンター中核人材育成プログラム
https://www.ipa.go.jp/icscoe/program/core_human_resource/index.html
16）分野横断型演習について
https://www.nisc.go.jp/conference/cs/ciip/dai16/pdf/16shiryou06.pdf
17）戦略的イノベーション創造プログラム（SIP）重要インフラ等におけるサイバーセキュリティの確保　研究開発成果集 p. 30，31，78，79
https://www.nedo.go.jp/content/100907028.pdf
18）ExxonMobil 向けオープンプロセスオートメーションのテストベッド構築へ
https://www.yokogawa.co.jp/news/press-releases/2019/2019-07-09-ja/



工場･研究所における災害･事故および各種リスクの可視化と対策

～AI，IoTの利用 ／ 地震，風水害，火災爆発，異物混入，漏洩対策 ／ BCPの整備～

発刊日 ： 2020 年 8 月31日　体 裁 ： A4判 770 頁
定 価：80,000 円(税抜)　ISBN：978-4-86104-802-9

東京工業大学	中村 昌允	大成建設(株)	上田俊彦
(株)KRI	阪井敦	大成建設(株)	薦田香織
半田化学プラント安全研究所	半田安	大成建設(株)	山口亮
工学院大学	市川紀充	大成建設(株)	関山雄介
クレインテクノコンサルティング	門眞博行	千葉大学	町田基
芝浦工業大学	諏訪好英	千葉大学	天野佳正
(株)テクノ菱和	鈴木政典	MS＆ADインターリスク総研(株)	三和多賀司
(株)奈良機械製作所	高島久継	音羽電機工業(株)	酒井志郎
BS＆Bセイフティ･システムズ(株)	那須貴司	清水技術士事務所	清水健康
(国研)産業技術総合研究所	中山良男	(株)ヒューマン･ナレッヂ	前田康秀
和光純薬工業(株)	岩田勉	岡山大学	五福明夫
(株)住化分析センター	菊池武史	大阪市立大学	岡田明
東洋エンジニアリング(株)	矢部一明	千葉大学	諏訪園靖
レイズネクスト(株)	大館佑介	千葉大学	渡邉由芙香
マルイ鍍金工業(株)	遠瀬惇	千葉大学	能川和浩
マルイ鍍金工業(株)	石見清隆	(株)日輪	金原慎一郎
マルイ鍍金工業(株)	上田英貴	大阪大学	釘原直樹
日本ピラー工業(株)	村上涼平	7S3T田中塾	田中豊
小波技術士事務所	小波盛佳	保全革新研究所	佐藤信義
ファルマハイジーンサポート	島一己	大阪大学	石丸裕
崇城大学	里永憲昭	出光興産(株)	長谷川勝宣
(株)高田工業所	劉信芳	(国研)産業技術総合研究所	牧野良次
新川電機(株)	瀧本孝治	明治大学	金子弘昌
アズビル(株)	田中雅人	日本電気(株)	相馬知也
名古屋工業大学	橋本芳宏	(株)三菱総合研究所	古屋俊輔
東芝三菱電機産業システム(株)	金子宏一	みずほ情報総研(株)	貴志孝洋
(株)フジ環境サービス	高橋朋也	横浜国立大学	小柴佑介
サラヤ(株)	原田裕	【元】サムスン	棚橋高成
【元】Panasonic	冨岡敏一	JFEスチール(株)	山岸新一
西野技術士事務所	西野敦	住友化学(株)	宮田栄三郎
関西大学	冨岡敏一	ダイキン工業(株)	北野達也
横浜国立大学	座間信作		

執筆者：63名

橋本の原稿を読みたかったら、高価な書籍を購入しろと、宣伝しているように思われるのは、不本意だけど、書籍の宣伝には協力したいということで、私の原稿をつけて、この書籍を宣伝することを、出版社から許可いただいています。

私の原稿は、ごく一部で、安全に関する多面的な検討が一線の方々により解説されている書籍になっています。

高価ですが、著者紹介により、企業の方には２割引きの64,000円、大学の方には30,000円でご購入いただける設定もございますので、hashimoto@nitech.ac.jpまでご連絡いただけましたら、割引での購入手続きをお伝えします。

どうぞ、よろしくお願いします。

https://www.gijutu.co.jp/doc/b_2062.htm

第1章　工場・研究所における事故・トラブル発生要因，その分類
第2章　火災・爆発事故の発生原因とその対策
第3章　薬品の取扱い，化学反応異常による事故の発生原因とその対策
第4章　容器配管の老朽化・閉塞・漏洩事故の発生原因とその対策
第5章　電気系統や回転機器，駆動装置の動作異常よる事故の発生原因とその対策
第6章　異物混入や汚染による事故の発生原因とその対策
第 7 章　地震・風水害・災害によるトラブルの発生原因とその対策
第 8 章　プラントの現場管理者の安全教育について
第 9 章　ヒューマンエラーおよび負傷・疾病とその対策
第 10 章　健全性評価，異常検査技術やリスク予測およびセンシング技術，IoT，AI の活用
第 11 章　工場・研究所における災害時の事業継続性(BCP)への対応
第 12 章　各企業における工場・研究所の安全管理の取り組み，事例紹介

◇第1章　工場・研究所における事故・トラブル発生要因，その分類　◇

第 1 節　工場・研究所における事故の予防や安全対策―概論―

1.安全管理の基本
　1.1　基本的な考え方
　1.2　リスク管理の手順
　1.3　リスクアセスメントと危険予知
　1.4　日常管理
　　1.4.1　危険予知(KY)
　　1.4.2 4S(整理，整頓，清掃，清潔)
　　1.4.3　ヒヤリハット
　　1.4.4　ツールボックス(作業開始時)ミーティング
　　1.4.5　職場巡視(パトロール)
2.工場と研究所との違い
　2.1　研究開発における安全
　2.2　工場と研究所との比較
3.日本と欧米との安全管理に対する考え方の比較
4.これからの安全管理

◇第5章　電気系統や回転機器，駆動装置の動作異常よる事故の発生原因とその対策◇

第 6 節　プラント制御システムのセキュリティ対策

1.化学工場・研究所をとりまくサイバー攻撃の危険性
2.制御系のサイバーセキュリティに関する世界的な取り組み
3.プロセス制御系独自のサイバーセキュリティの問題点
3.プロセス制御系のリスク解析とセキュリティ対策
　3.1　化学プラントで考慮すべきサイバーリスクと特徴的な対策
　3.2　制御系セキュリティの標準的なアプローチ　NIST の Cybersecurity Framework
　3.3　教育・訓練，人材育成