制御システムセキュリティカンファレンス 2018

生産工場制御システム向けサイバー攻撃対策の取組み ～JPCERTアセスメントによる推進事例～

2018年2月7日

大陽日酸株式会社　経営企画室　情報システム部
中辻 利一

TAIYO NIPPON SANSO
The Gas Professionals

会社概要

社名	大陽日酸株式会社
設立年月日	1910年10月30日
本社所在地	東京都品川区
従業員数	15,860名（連結）
グループ会社数	191社
2017年度売上高	5,815億円

その他ガス関連事業

炭酸ガス


ヘリウム（液化ヘリウムコンテナ）


水素（移動式水素ｽﾃｰｼｮﾝ）


アセチレン

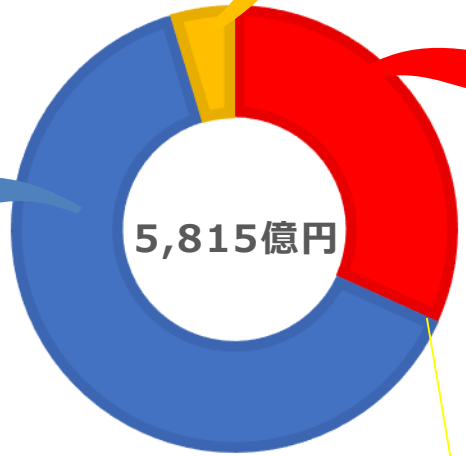
半導体材料ガス

LPガス

・・・・

サーモス他事業

本日のお話



セパレートガス事業
（酸素、窒素、アルゴン）


セパレートガス製造


貯蔵・供給体制

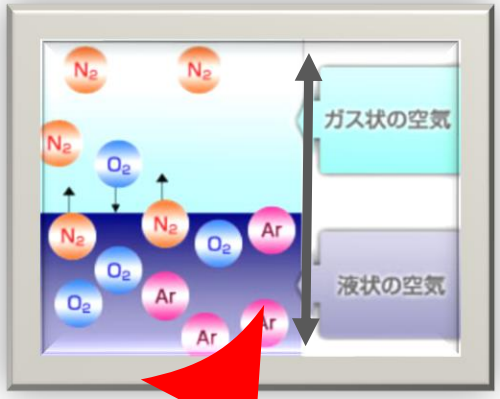
セパレートガス製造プラント“空気分離装置”

TAIYO NIPPON SANSO
The Gas Professionals

・空気成分ガスである酸素・窒素・アルゴンを、沸点差を利用した蒸留方式にて分離する。
・このプラントに生産制御システム（DCS/FCS）が使用されている。

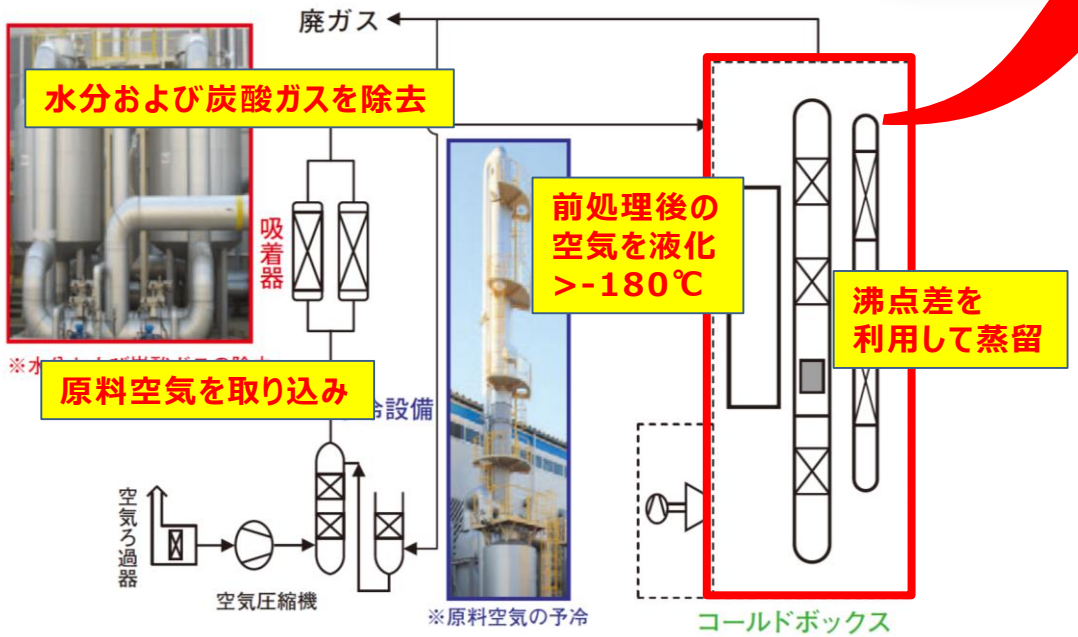
中央操作室風景

本日のお話



※沸点

窒素	-195.8℃
アルゴン	-185.8℃
酸素	-183.0℃



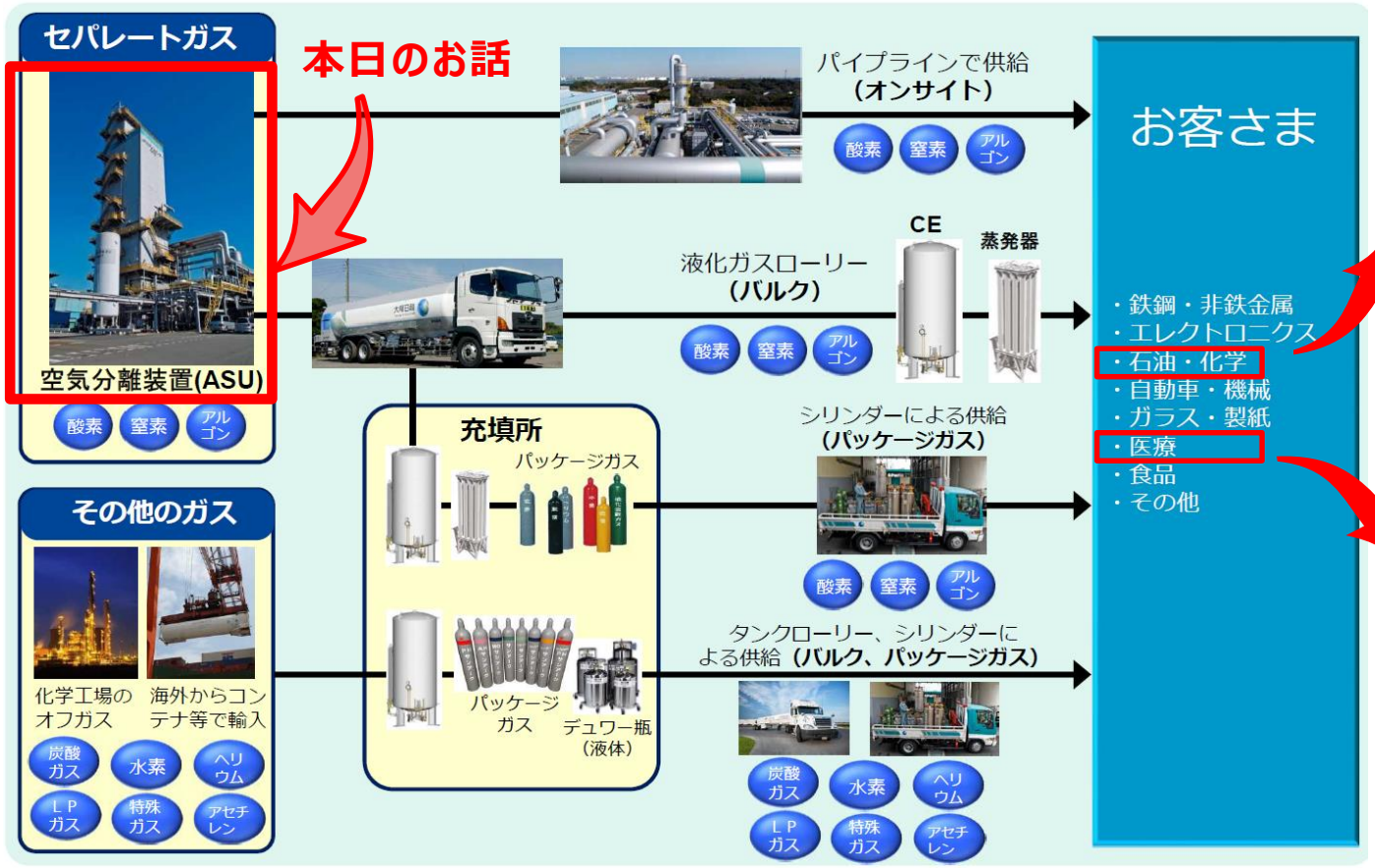
→窒素ガス	>99.99 vol%
→酸素ガス	>99.5 vol%
→アルゴンガス	>99.9 vol%
→液体酸素	>99.5 vol%
→液体窒素	>99.99 vol%

セパレートガス事業について

TAIYO NIPPON SANSO
The Gas Professionals

・鉄鋼や化学、半導体をはじめ、10,000箇所（届け先ベース、日本）を超える幅広い産業、数多くのお客様にご利用いただいている。
・この中には、化学工場・石油コンビナート向けの防爆用窒素、医療用酸素といった安定供給が決して欠かせない用途が含まれる。

⇒重要インフラ事業と認識



安定供給が決して欠かせない用途例

防爆用窒素

合成空気供給システム

医療用酸素ボンベ

セパレートガス生産拠点

TAIYO NIPPON SANSO
The Gas Professionals

20人未満の小規模工場が多く、下図以外にも、特定のお客様への供給に特化した生産拠点（ガスセンター）を加え、その総数は国内で４５拠点になる。

本日のお話の対象

サイバー攻撃被害と新聞報道

TAIYO NIPPON SANSO
The Gas Professionals

・2016年3月、当社データセンタでサイバー攻撃を受けた。
・2017年1月、関連する一部新聞報道があったが、その主旨は**「化学プラントを保有するインフラ企業」へのサイバー攻撃、生産設備に攻撃が及ぶことの懸念を連想させる**内容だった。
・そこで、生産制御システムのセキュリティ対策を改めて確認するため、**JPCERT/CC「制御システムアセスメントサービス」**を実施した。

ガス大手にサイバー攻撃

大陽日酸 管理者権限奪われる

化学プラントや医療機関で必要な産業ガスの国内最大手・大陽日酸（東京）がサイバー攻撃を受け、システム内の情報を広範囲に見られる管理者権限が奪われていたことが分かった。社員ら約1万人分の個人情報など内部情報が盗まれた可能性があり、専門家は「インフラ企業を標的とした次のサイバー攻撃につながる恐れがある」と警告している。

社員らの情報流出か

同社によると、2016年3月、内部情報のあるサーバーに管理者権限を使った不審な接続があることに気づき、調査を始めた。調べた結果、サーバーが少なくとも4種類のウイルスに感染して管理者権限が奪われ、外部からの遠隔操作で、システム内の大半にあたる6百数十台のサーバーに接続できる状態だった。同月には、サーバーの一つが2回にわたり外部と不正通信を行い、そのサーバーには、何者かが約1ギ

管理者権限　システム内のサーバーや端末に自由に接続したり、設定を変更したりできる権限。専用IDやパスワードが必要で、本来はシステム保守などを行う管理者だけが持つ。サイバー攻撃の攻撃者が入手すれば、情報を大量に引き出し、侵入の痕跡を分かりにくくすることもできる。

大陽日酸へのサイバー攻撃のイメージ

・ヴィ（A4判文書約35万枚相当）の大量のデータを複数の圧縮ファイルにまとめていた。データには、同社やグループ会社の社員ら約1万人分の所属やメールアドレスなどが含まれており、同社はウイルスの駆除などの対策を実施し、翌月、警視庁に相談した。

同社は、化学プラントなどの爆発防止用の窒素や病院で使われる酸素などの産業ガスの製造・販売の国内最大手で、世界5位。16年3月期の売上高は6415億円。同社は「サイバー攻撃を受け、情報が流出した可能性があることは真剣に受け止め、外部との不正な

【参考】JPCERT/CC「制御システムセキュリティアセスメントサービス」

TAIYO NIPPON SANSO
The Gas Professionals

※JPCERT/CC ホームページより抜粋

はじめに：メリット その１

制御システムのセキュリティ、何から手をつけたらいいのか分からない
現状把握の必要性はわかるが、評価時間があまりかけられない

JPCERT/CC による
セキュリティアセスメント

セキュリティ対策の第一歩として現状把握ができる

第三者評価による気付きが得られる

結果の有効活用

2種類のアセスメントをご提供（SSATとTR）

SSATまたはTRのいずれかを選択いただきます。
SSAT：SCADA Self Assessment Tool
TR： Technical Review

導入から運用までの全般のアセスメントを行いたい場合はSSAT
ファイアウォールの設定内容等の技術面の詳細なアセスメントを
行いたい場合はTRを選択してください

	SSAT	TR
アプローチ	ベースライン	ベースライン
基準	日本版SSAT	NIST SP800-53 NIST SP800-82
分野	全般（デザイン、購買、導入、運用）	技術的（設計、運用）

NIST SP800-53 連邦政府情報システムにおける推奨セキュリティ管理策
NIST SP800-82 産業用制御システム(ICS)セキュリティガイド

8 |

アセスメントの流れ（詳細）

	事前打ち合わせ	事前確認シート記入	オンサイトアセスメント	レポート作成
所要時間	約2時間	約4時間	約8時間	1か月
内容	■アセスメント詳細説明 ■事前確認シートの記入方法説明		■オンサイトアセスメント ■証跡の確認 ■ラップアップ会議	■スコア ■主要ポイントに対するコメント
アセットオーナー	○	○	○	
JPCERT/CC	○		○	○

アセスメント結果

TAIYO NIPPON SANSO
The Gas Professionals

※投影のみとさせていただきます。

本対策取組みの目標と進め方

TAIYO NIPPON SANSO
The Gas Professionals

同アセスメントの結果を踏まえ、当社が設定した生産制御システムサイバー攻撃対策の目標と進め方は以下とした。

１．「化学プラントを保有するインフラ企業」といった当社の社会的責任に鑑み、同アセスメントに対して合格点（６０点）が得られ、その対策を対外的に説明できるレベルに引き上げる。

２．そのためには、技術的対策のみならず、生産制御システムのサイバー攻撃による生産設備の停止、破壊を重要リスクと認識し、ポリシー、対策推進体制、現場のＰＤＣＡサイクルの確立を目指す。

対策取組みの本日ご紹介内容

主に以下５項目についてご紹介する。

１．リスクと脅威の理解

２．管理体制の構築

３．ファイアウォール管理体制の見直し

４．サイバー攻撃起点になりやすい端末の対処

５．ガイドライン策定と想定成果物

１．リスクと脅威の理解

TAIYO NIPPON SANSO
The Gas Professionals

JPCERT/CCアセスメントツールの以下設問に対する取組み。

１．**制御システムに起こりうる脅威を特定していますか？**
「はい」を選択した場合、それは過去12 ケ月以内に見直していますか？

２．１．で特定した脅威のシナリオを考慮して、脅威評価（発生場所×発生頻度×システムへの影響）を行っていますか？
「はい」を選択した場合、それは過去12 ケ月以内に見直していますか？

３．過去12 ケ月以内に、制御システムの脆弱性評価/状態チェック（ソフトウエア、ハードウエアの現存する脆弱性の確認、システム全体（最も弱い部分）の保護水準の確認）を実施していますか？

１．リスクと脅威の理解

TAIYO NIPPON SANSO
The Gas Professionals

※投影のみとさせていただきます。

1．リスクと脅威の理解

前項で本取組みの対象を限定したうえで、その脅威、脆弱性、リスクを以下に特定した。

脅威

1．外部攻撃者
（ハッカー）

2．コンピュータウイルス
（特にワームウイルス）

インターネットに接していなければ被害を受ける可能性は極めて低い。

インターネット

侵入手口・経路

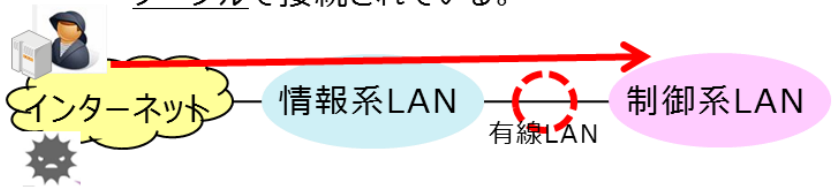
1．サイバー攻撃メール
（不正プログラム/不正サイトURL付）

2．改ざんサイト
（不正プログラム付）

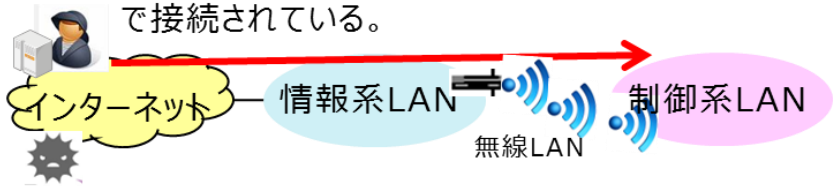
3．ＵＳＢメモリ
（不正プログラム付）

脆弱性

1．情報系LANと制御系LANが無防備に有線LANケーブルで接続されている。

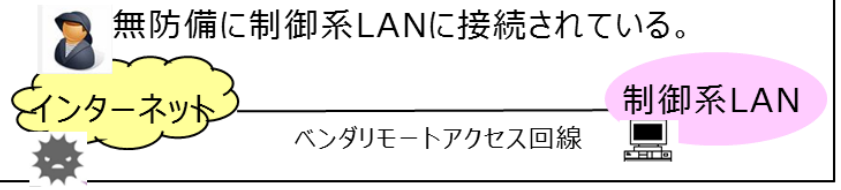


2．情報系LANと制御系LANが無防備に無線LANで接続されている。



3．情報系LANと制御系LANの間のデータの受け渡しに無防備なUSBメモリが使用されている。

4．制御システム保守用ベンダーのリモート回線が無防備に制御系LANに接続されている。



リスク

【脅威】×【脆弱性】

1．外部攻撃者の侵入による高度なサイバー攻撃

2．コンピュータウイルスの蔓延

生産設備の停止・破壊、情報漏えい、改ざん

工場・生産制御システム

【参考】想定リスク例

TAIYO NIPPON SANSO
The Gas Professionals

※投影のみとさせていただきます。

２．管理体制の構築

TAIYO NIPPON SANSO
The Gas Professionals

JPCERT/CCアセスメントツールの以下設問に対する取組み。

１．制御システムのセキュリティに対して、責任をもつ専門のチームまたは個人はいますか？

２．経営者は制御システムのセキュリティ担当者の責務を文書化していますか？

２．管理体制の構築

TAIYO NIPPON SANSO
The Gas Professionals

※投影のみとさせていただきます。

【参考】情報管理委員会/技術的安全対策分科会

TAIYO NIPPON SANSO
The Gas Professionals

※投影のみとさせていただきます。

【参考】制御システムのセキュリティ担当者の責務例

TAIYO NIPPON SANSO
The Gas Professionals

※投影のみとさせていただきます。

３．ファイアウォール管理体制の見直し

TAIYO NIPPON SANSO
The Gas Professionals

JPCERT/CCアセスメントツールの以下設問に対する取組み。

１．制御システムをファイアウォールで他のネットワークから保護していますか？

２．過去12 ケ月以内にファイアウォールの設定を監査していますか？

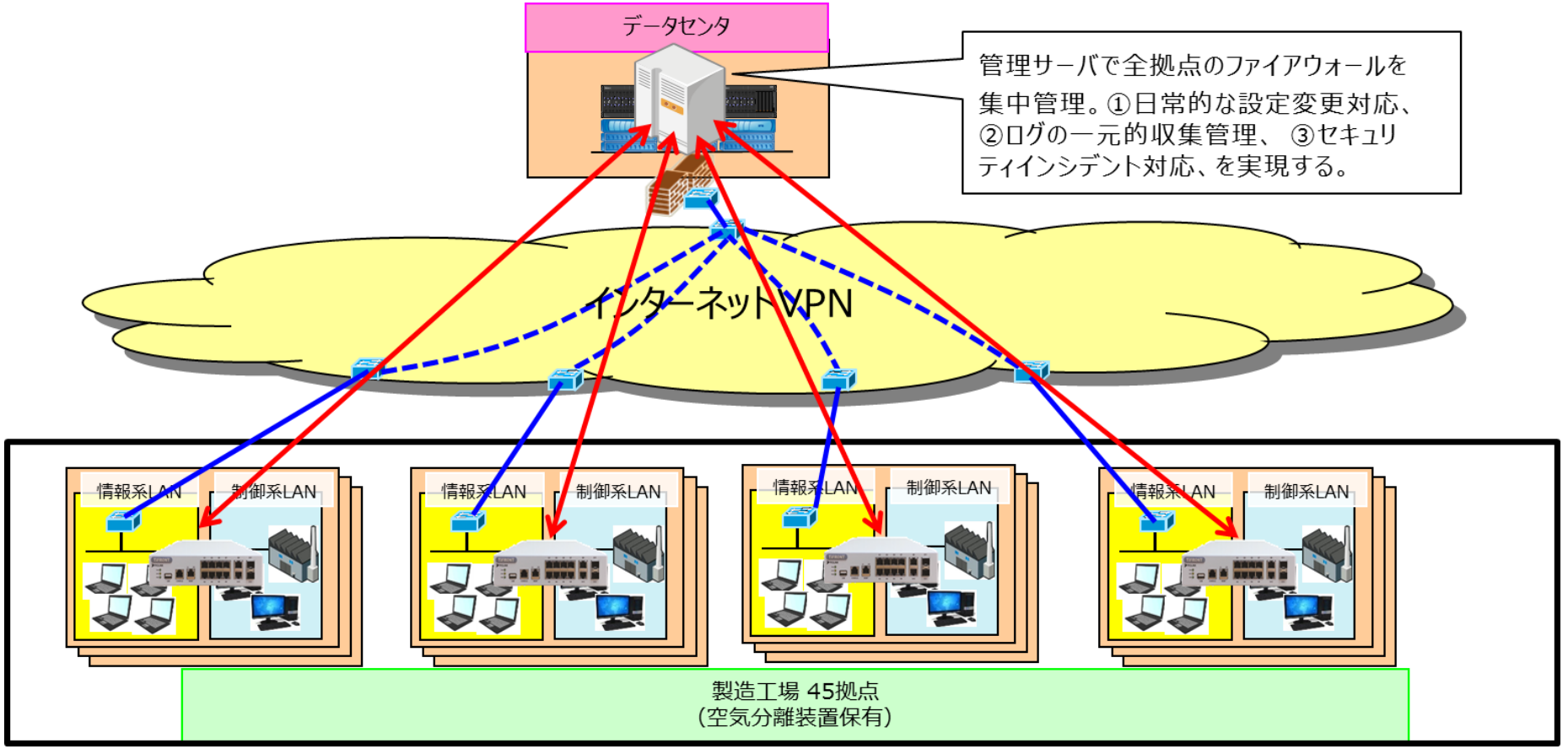
３．現行のファイアウォール機種で、ベンダか専門家のトレーニング、または、それに相当する適切なトレーニング等を実施しましたか？

４．ファイアウォールは24 時間･365 日、監視･管理されていますか？
（ログの記録やエラー発生時の確認など）

３．ファイアウォール管理体制の見直し

TAIYO NIPPON SANSO
The Gas Professionals

・20人未満の小規模工場が多数、セキュリティの専門スタッフが確保できない状況。
・ファイアウォールを工場毎の個別管理から情報システム部門の集中管理に移行することにした。
　①日常的な設定変更対応、②ログの一元的収集管理、③セキュリティインシデント対応



４．サイバー攻撃起点になりやすい端末の対処

TAIYO NIPPON SANSO
The Gas Professionals

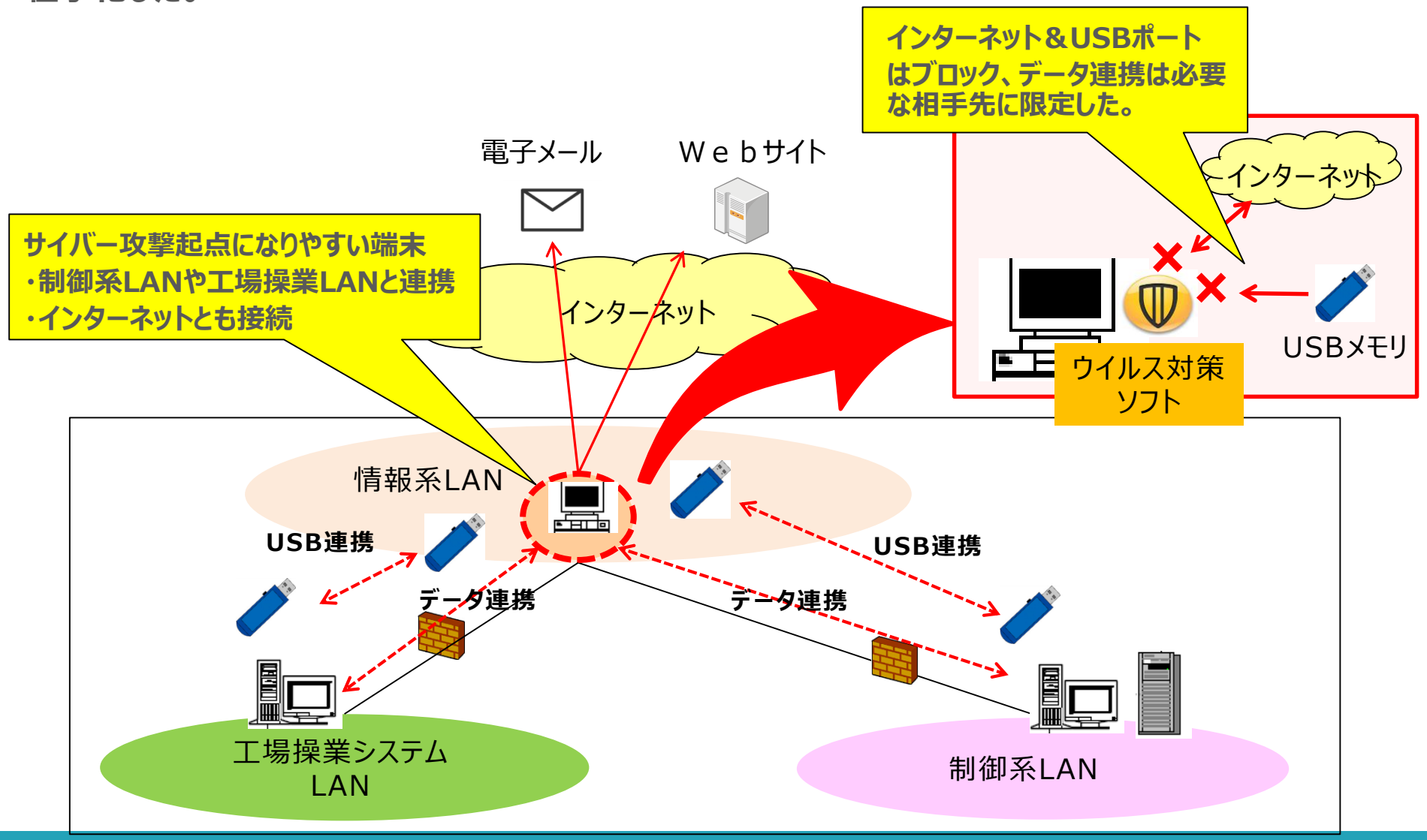
JPCERT/CCアセスメントツールの以下設問に対する取組み。

１．PCや外部メモリ等を制御システムネットワークに接続する前に、それらがウイルスに感染していないことの確認を実施していますか？

２．制御システムネットワークでIP通信を行う制御機器を使用している場合、攻撃に対する対策(ファームウエアやソフトウエアのアップデート、設定の確認など)を行っていますか？

４．サイバー攻撃起点になりやすい端末の対処

制御系LANと接点を持ちながら、インターネットとも接点を持つ端末を特に注視してリスクを極小化した。



５．ガイドライン策定と想定成果物

TAIYO NIPPON SANSO
The Gas Professionals

JPCERT/CCアセスメントツールの以下設問に対する取組み。

１．制御システムのセキュリティポリシーを正式に文書化していますか？

２．文書化されている場合、その内容が徹底されるための方策を取っていますか？

５．ガイドライン策定と想定成果物

TAIYO NIPPON SANSO
The Gas Professionals

※投影のみとさせていただきます。

所感

TAIYO NIPPON SANSO
The Gas Professionals

※投影のみとさせていただきます。

【参考】当社ネットワーク構成

TAIYO NIPPON SANSO
The Gas Professionals

※投影のみとさせていただきます。

TAIYO NIPPON SANSO

The Gas Professionals