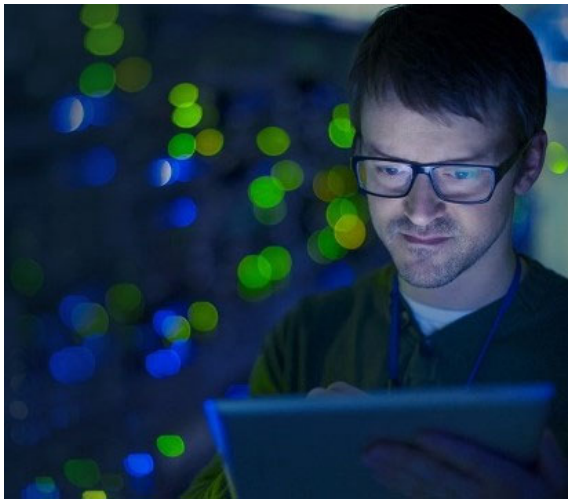
事業継続リスク下における サイバーセキュリティの警戒態勢の維持

2020年5月12日

COVID-19（新型コロナウイルス感染症）の感染拡大を抑止するための措置により、化学および機能性化学品業界の組織は、リモートアクセスへの依存度を高め、現場の作業人員を減らさざるを得ず、このことがサイバーセキュリティへの懸念を高めています。原油価格の落ち込みが資本関係に影響を及ぼすなか、同セクターがどのようにサイバーセキュリティを強化しようとしているのかについて、KPMGの化学部門グローバルヘッドであるPaul Harnickが解説します。



米国の化学企業のサイバーオペレーションはCOVID-19によりどのような影響を受けているのでしょうか？

世界中のビジネスリーダーやテクノロジーリーダーと同様に、化学企業の情報セキュリティ最高責任者（CISO）は、従業員の健康を維持しながら、情報技術（IT）および運用技術（OT）を保護するためのサイバーオペレーションを維持できるか危惧しています。「起こすか起こさないかではなく、いつ起こすか」というスローガンの下、システム攻撃がこれまで以上に企てられることでしょう。

COVID-19がサプライチェーン全体に混乱をもたらしていることにより、化学関連組織の多くがキャッシュと運転資本の確保を進めています。しかし、セキュリティの維持が急務であるにもかかわらず、サイバー関連のプロジェクトは延期または中止されています。ソーシャル・ディスタンス措置の導入増加を受け、プラントのターンアラウンド（受注から発送までの過程）が削減または遅延していることから、企業の経営陣は効率化を重視してあらゆる検討を進めていますが、このことは潜在的にOTの展望において安全性とセキュリティのリスクを増大させる可能性があります。

さらに、高齢者はCOVID-19による合併症のリスクが高いと考えられています。平均して数十年間にわたる経験を有するプラントの作業員と豊富な業務知識を有するシニアエンジニアを抱えていることを踏まえると、COVID-19が化学プラントの運営に及ぼす潜在的な影響は高いと考えられます。

化学業界のITとOTに特有のサイバーセキュリティに関する懸念にはどのようなものがあるのでしょうか？

悪意のあるサイバー攻撃者はオペレーション能力が弱まるこの時期に便乗しようとするため、フィッシング攻撃件数の増加が予想されます。実際、米国連邦捜査局は偽のCDCメールやフィッシングメールを含むCOVID-19関連のサイバー攻撃の増加を注意喚起している[1]ほか、英国のサイバーセキュリティ専門家はオンライン攻撃が増加し、進化していると指摘しています[2]。確かに、サイバー攻撃者はすでにこの状況に付け入っており、マルウェアのペイロードとともに、COVID-19関連のフィッシングメールは急増しています[3]。

攻撃ベクトル（攻撃の経路）は通常、悪意のあるサイバー攻撃者がITとOTの両方に関与している従業員のアカウントを識別した時点で、企業のITを介して産業ゾーンに到達します。

1 出典：Federal Bureau of Investigation, Alert Number I- 032020-PSA: FBI sees rise in fraud schemes related to the Coronavirus (COVID-19) pandemic.

2 出典：National Cyber Security Centre Weekly Threat Report（2020年3月27日）

3 出典：Dark Reading "BI Warns of Fake CDC Emails in COVID-19 Phishing Alert."（2020年3月23日）

一方、分散制御システム（DCS）、監視制御システム（SCADA）、プログラマブル論理制御装置（PLC）を含むプラントのシステムは、独自ベンダーのサポートに依拠していますが、そうしたサービスは慣習的にオンサイトまたはサプライヤーの拠点から提供されています。現在の外出禁止令およびソーシャル・ディスタンスの措置により、サプライヤーの担当者はリモートで作業する必要があり、「ホップ（転送・中継設備）」がさらに増えています。これにより、通常のメンテナンスから専門プロジェクト、そして特に重要なものとしてシステムのセキュリティおよびパッチに及ぶ、広範囲の活動が影響を受けています。

化学業界は、いかにしてCOVID-19関連のより広範な課題に取り組むのと同時に、増加するサイバーリスクに対処しているのでしょうか？

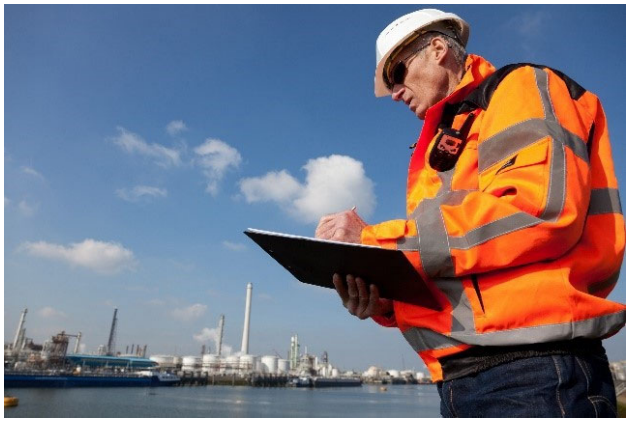
組織によって成熟度や事業対応力、セキュリティ機能の度合いは異なります。とはいうものの、大半の組織がCOVID-19による渡航規制とソーシャル・ディスタンスの制限を受けて事業継続計画（BCP）を発動し、オフィスが無人の状態で運営を続けています。ノートパソコンとVPNアクセスによってリモートで作業できるほとんどの「企業の」従業員には、これが有効となります。

しかし、配置人員を削減され、リモート勤務が増加したことで、IT・OTチームにそれらの運用を管理する負担が集中し、リスクはプラントのオペレーションレベルで潜在的に増加しています。また、前述のように、DCS、SCADA、PLCのプロバイダ等不可欠なサービスのパートナーも、現在はリモートで稼働する必要があります。サプライチェーンの契約でこのような外部企業によるリモートアクセスがすでに許可されている場合には、ベンダーのVPNネットワークを介したよりリモートなアクセスが行われるようになる可能性があり、さらに一段階、手順が省略されます。また、リモートワーカーが従来の方法で社内のITセキュリティツールとリソースにアクセスしなくなり、セキュリティ侵害のリスクが高まるため、サプライヤーのセキュリティインフラにもさらに負荷がかかります。

リモート勤務のニーズに対応するため、化学関連の組織はリモートインフラの活用を増やすことが必要となりつつあります。しかし、これはサイバーセキュリティチームによる監視を必要とする社内システムおよびOTシステム両方のファイアウォールの「穴」が増え、マルウェアが特定の環境で展開された場合、安全性、生産性、運営の統合性に影響を与えるリスクが増大することを意味します。残念ながら、COVID-19がもたらした経済の実情においては、従来のセキュリティプロジェクトの予算が厳しく見直されており、サイバーツールの運用に影響を及ぼし続けることは間違いありません。

一方、健康安全の観点から、プラントの運営において従業員の露出を制限することが検討されるでしょう。これには、リスクの影響度を一定に保つためのシフト編成の整備や、拡大するCOVID-19の影響を制限するためのエンジニアチームの縮小、また同時に可能な場合には、プラント運営の中枢部のリスクの影響度と負担を軽減するため、複数のコントロール室（研修室を含む）の活用が含まれます。ただし、ウイルスがいずれかのチームに影響を及ぼした場合、これには潜在的な課題があります。ウイルスが引き続き従業員の間で蔓延する場合には、現行のBCPの運用をさらに調整する必要がありますが、短期的には、この変化に対応したプロセスは戦術上の問題の軽減につながるはずです。ただし、プラントのターンアラウンドならびにセキュリティパッチを実施する保守点検の時間枠（通常、フロアに最大3倍のスタッフを要する）に対する圧力に加え、経済的な圧力（需要と供給の両方）により、中期的には運用の再考が必要になる可能性があります。

人口統計上リスクが高いとされる高齢の従業員層を考慮し、組織のなかには、エンジニアその他の主要な従業員によるプラントの運営および不可欠な知識の文書化を急速に広範囲で進めている組織があります。こうした文書化の取組みは、多くの場合、プラント運営のためのアラームマネジメントの構築とアラームを配備する必要性に焦点を当てた運営上の安全プロセスの見直しとともに実施されます。



事業を守り、BCPを可能な限り強固にするために、化学企業が留意すべき検討事項は何でしょうか？

- 短期的には、BCPに基づき、予想よりも長い期間にわたり人員を削減した状態で経営を継続する必要性を検討する。また、現在は、混乱が長期化する可能性を考慮して、BCPの更新を開始し、複数の混乱が同時に発生した場合のシナリオに沿ってBCPのストレステストを行う時期でもあることに留意する。
- OT組織のリモートアクセスの取決めと手順の見直しを含む、予定しているセキュリティの見直しの前倒し（外部からプラント内の環境にリモートアクセスできる者に向けたセキュリティのクイックウィンを要求すること）と、戦術的に実施可能なOTの強化の検討を実施する。
- セキュリティオペレーションが強固で、IT・OT両方のレイヤーに対応できるかどうかについての検討を実施するとともに、可能な場合、ネットワークにおける「不正を探知する」組織の能力を向上させる。
- パッチ実施の遅延や、そうした遅延によって引き起こされる可能性のある脆弱性に関するOTのリスクをレビューし、適切な統制が整備されていることを確認する（例： 安全計装システム（SIS）が他のネットワークから引き続き独立していることを確認すること）。
- 施設（特にプラント側のVPN）を点検し、安全性を担保するためのリモート侵入テスト活動を計画および実施する（現在、これには継続的な変更と拡張が必要であるものの、管理、方針の変更および継続的な監視のためのリソースがないという懸念がある）。

- 経営効率性のレビュー：「頭のなかにある知識」を紙に落とすという重要な文書化と、プラントの手順を簡素化する可能性の検討に焦点を当てた、BCP／災害復旧レビューを実施する。
- BCPまたはOPS文書のレビュー、プロセスレビュー、ツールセットのリスクの改善等クイックウィンで防御を強化する方法を評価する。組織全体でベストプラクティスを共有し、増大するリスクの同時発生に対応するのに役立つ適切なリソースを提供できるよう取り組む。

これらの留意事項を念頭に置き、定期的なサイバー危機に対する準備のレビューを確実に実施することで、化学関連組織は、プラントの安全性と機密性を維持しながら、将来再び利用できる多くの新しい効果的な働き方を開発することができるでしょう。

KPMG Global Energy Institute

KPMG Global Energy Institute（GEI）は、エネルギー業界における今日の課題や新たなトレンドを共有するための世界規模のプラットフォームです。2007年に発足して以来、約30,000名以上の方々にご登録いただいており、業界のキートピックに関するさまざまなメディアチャンネル、出版物、ポッドキャスト、イベント、そしてニュースレター等をお届けしております。ビジネストピックや業界の課題に関する貴重なインサイトをご希望の方はread.kpmg.us/geiをご覧ください。

Contact us

眞野 薫
KPMGジャパン
素材・化学セクターリードパートナー
株式会社 KPMG FAS
Strategy & Integration
執行役員パートナー
E: kaoru.mano@jp.kpmg.com

Paul Harnick
Global Head of Chemicals
KPMG in the U.K.
E: paulharnick@kpmg.com

Jason Haward-Grau
Managing Director
Cyber Security Services KPMG in the U.S.
E: jhawardgrau@kpmg.com

home.kpmg

home.kpmg/socialmedia

本レポートで紹介するサービスの一部またはすべては、KPMGの監査クライアントおよびその関連会社に提供が認められない場合があります。