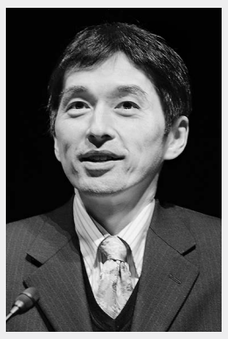
NIKKEI BUSINESS DAILY FORUM
日経産業新聞
フォーラム2016

今、製造業に求められる サイバーセキュリティー対応

企業秘密や顧客情報を狙うサイバー攻撃の手口は巧妙化し、その脅威が増加している。あらゆるものがインターネットに接続するIoTは、製造業の生産現場に革新をもたらすと期待される一方、サイバー攻撃のリスク拡大により業務停止や技術情報の社外流出などにもさらされやすくなる。製造業が情報セキュリティーを経営課題として推進するにあたり、今、知っておくべき課題と解決策とは何か。さきごろ開催された「今、製造業に求められるサイバーセキュリティー対応」セミナー（主催：日本経済新聞社、協賛：KPMGコンサルティング）で、最新動向を各界の専門家が紹介した。

基調講演 サイバー空間をめぐる状況とサイバーセキュリティ戦略

内閣サイバーセキュリティセンター　内閣参事官　三角 育生氏



サイバー空間は企業競争力の源泉

政府は「サイバーセキュリティ」を初めて法律用語として定義したサイバーセキュリティ基本法を、昨年1月9日に全面施行した。サイバーセキュリティーは「電磁的方式により記録される情報の漏洩・滅失・毀損の防止等／ネットワーク等の安全性・信頼性の確保のために必要な措置が講じられ・維持管理されていること」を指す。人の記憶や手書き情報を除いている以外は、情報セキュリティーとほぼ同義だ。

この法律でサイバーセキュリティ戦略の閣議決定と国会報告、およびサイバーセキュリティ戦略本部の創設が義務づけられ、戦略本部が施行日に発足した。戦略本部の役割は戦略の立案および実施推進のほかに、国の行政機関・独立行政法人における対策基準の作成／監査、国の行政機関で発生した重大事象についての原因究明調査、重要施策の企画・調査・審議、経費見積もり方針などの指針の作成、総合調整などがある。私が所属する内閣サイバーセキュリティセンターは、戦略本部の事務局にあたる。

戦略本部は戦略案を昨年5月25日にパブリックコメントに付したが、その直後に日本年金機構で125万件の年金情報流出事案が発生した。これがサイバー攻撃による事件であることを警察が確認し、厚生労働省が6月1日に公表。当センターは厚生労働省に資料提出を求め原因究明調査作業を行った。

詳細は当センターのホームページで公開しているが、ここでは教訓を2つだけ挙げる。1つは、メール添付による攻撃を完全に防ぐことはできず、メール開封を前提とした対策が必要であること。もう1つは、侵入範囲を拡大させないためのシステム設計・構築・運用が重要という点だ。

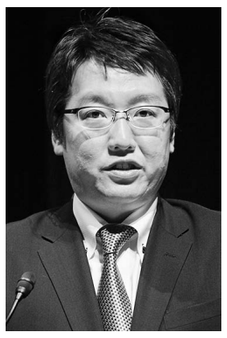
年金機構では本来、個人情報はネット接続していない業務系システムに格納する設計になっていた。しかし、業務系システムが使いにくかったため、ネット接続している情報系システムに個人データを移して使っていた。業務系システムが使いにくいものであれば、こうした事案の発生リスクは常にある。

この事案などを受け、修正したサイバーセキュリティ戦略が昨年9月に、さらに基本法の改正案も今年2月2日に閣議決定した。年金機構は厚生労働省と不可分だったために調査対象となったが、じつは特殊法人だ。改正法では監査・原因究明調査の対象に、戦略本部が指定する特殊法人・認可法人を含めた。また、人員強化の観点から、秘密保持義務などを規定した上で、独立行政法人情報処理推進機構（IPA）など政令で定める法人に一部事務を委託できるようにした。

サイバーセキュリティ戦略ではIoTを単なる業務効率の向上やコストダウンの手段とは考えておらず、サイバー空間は無限の価値を生むフロンティアであり、企業競争力の源泉として位置づけている。情報システムであれば機密性、完全性、可用性がセキュリティーの目的だが、制御系ではこれに加え物理的な安全も考慮しなければならない。サイバーセキュリティーは経営戦略と不可分であり、経営と現場を橋渡しする人材育成を強化する必要もある。政府と民間の両方を視野に入れた人材育成の総合的強化方針を、今年度中をめどにまとめる考えだ。

講演① 製造業に求められるサイバーセキュリティー対策

KPMGコンサルティング　サイバーセキュリティ　アドバイザリーグループ　パートナー　田口 篤氏



製造業には、2つの悩みがある。1つは、制御系や工場独自のシステム全体を情報システム部門が把握できていないこと。装置一式が納入される生産ラインには、いつの間にかウィンドウズ系のOSが乗っていたりする。もう1つは、リソース不足や複雑な統制ラインのため海外拠点の管理状況が分からないこと。機能ごとに吸収することの多いM&Aも、一元管理の難しさの要因になっている。

一方、サイバー攻撃の主体は、かつての腕試し的な個人ハッカーから、企業に対する抗議活動や敵対行動を目的としたプロ化、多様化が進んでいる。攻撃対象も本社のOA系だけでなく、制御系システムやIoT、子会社や取引先などに広がっている。攻撃手法も既知のものからアンノウンアタックや、対象企業固有の攻撃手法がとられたりする。

こうした状況下で製造業がとるべき対策は、被害を受けることを前提とした検知・回復対策の強化に加え、制御系システムのセキュリティー対策と海外拠点の対策強化だ。対策にはセキュリティーを運営する管理組織が必要であり、リージョンごとの拠点統括と全体の統括組織を構築すべきだ。

現場のオペレーションとしては現在、多くの企業ではセキュリティー監視やインシデント対応に注力しているが、脅威情報を収集・分析して脅威を事前に予測する「脅威インテリジェンス」も視野に入れながら、古典的ともいえる「脆弱性管理（パッチマネジメント）」でセキュリティーホールを適切に埋めることが求められる。

制御系の場合は特に、リスクシナリオの作成も重要だ。狙われる理由や攻撃対象は会社や業種によって異なるため、リスクを見える化しなければ的確な対策は立てられない。金銭的ダメージや抗議行動では、生産ラインの停止の方がインパクトが大きいため、制御系は狙われやすいと認識すべきだ。

制御系はサテライト型の組織整備が有効

制御系システムは安定稼働が重視されるため、誤作動を起こさないようにウイルス対策を実施するのは、実際にはかなりハードルが高い。しかし、対策を怠れば致命的な結果を招きかねない。まずは、人材の多い情報システム部門から各拠点に常駐スタッフを派遣し、本部と連携しながら現場のセキュリティースキルや知識をシェアするサテライト型の組織を整備するのが有効だ。

海外拠点も、対策をしてから監査するのではなく、まずはグローバルのセキュリティー監査をして全体を見える化してから対策に着手することが有効だ。

講演② デジタルで描く製造業の未来 ～透明性がもたらす競争優位～

KPMGコンサルティング　テクノロジー・コンサルティングユニット　アナリティクス統括ディレクター　林 泰弘氏

デジタル化がもたらす変革への対応は不可避だ。欧米や日本の一部の製造業では、IoTを活用した製造業のサービス化が加速している。例えば、建設機械メーカーでは建設作業の生産性分析、燃費効率改善支援、作業オペレーションの効率化支援など、マシン間のデータをインターフェースを介して分析し、サービスとして提供している。

タイヤメーカーでも、タイヤの内側に設置したセンサーでゆがみや加速度、圧力、温度などを測定し、路面状態やタイヤの摩耗度などをドライバーの安全性向上に役立てようとしている。フォークリフトなどの倉庫内の運搬機械でも、製品位置、震度センサーや加速度センサー、温度センサーなどを付け、補修サービスと結びつけている。

推定像ではなく実像測定で透明性高める

一方、冷蔵庫のインテリジェント化やスマートハウスなど、消費財においては顧客体験価値という新しい価値の提供が進んでいる。スマートフォンのアプリを活用したオンデマンドタクシーや宿泊サービス、センサー内蔵のスポーツ用品などもその一例だ。

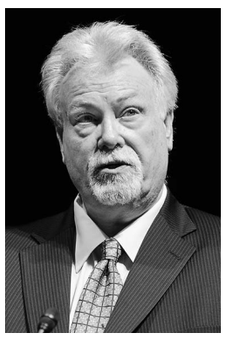
デジタル化が進むことで製造業の収益モデルも、新規・更新時期での販売による収益増からサービスの高度化による顧客価値の増加へと変わる。時間経過とともに低下する製品価値ではなく、サービス利用料による右肩上がりの収益モデルを構築できるようになる。こうしたサービス化の鍵を握るのはインターフェースであり、サイバーセキュリティーの重要性は今後さらに増加する。

では、こうしたデータサイエンス時代の経営課題とは何か。現在はまだ、課題あるところにデータありの段階で、仮説検証に必要なデータを都度収集しているケースが多い。しかし今後は、組織内を血液のように流れるデータを可視化し、常にモニタリングすることになる。

サンプルデータからの推定像ではなく、実像を直接測定することで透明性が高まり、データの分析・活用の精度とスピードは大きく向上する。分析のループを常に回し、その結果を全体最適の視点で各部門に反映させる。そうしたデジタルによる透明性が競争優位の源泉であり、透明性を維持するためのサイバーセキュリティーが不可欠になる。

講演③ サプライチェーンセキュリティー 組織のセキュリティー強度は、組織とつながる最もぜい弱な部分と同じレベルにしかならない

ノース・コーポレーション　共同設立者／COO　スキップ・フォス氏



ノース社は世界約30のバックボーンルーター拠点で、セキュリティー脅威の解析ネットワークをもち、Tier1の通信業者と同規模の運用を行っている。現在は1秒当たり3万回の攻撃を検知しており、毎日1万件の未知のマルウエア（悪意あるソフトウエア）を発見している。

ベライゾン社の2015年調査によると、製造業における侵害は内部犯行4%、クライムウエア（財務情報収集など犯罪行為を目的としたマルウエア）18%、サイバースパイ（情報窃盗）31%、サービス妨害（DoS＝大量アクセス攻撃、DDoS＝分散DoS）34%だ。

侵害の犯人では、クライムウエアは犯罪組織が73%を占めており、特に東欧ブロックのロシア語を話す組織が中心的存在だ。サイバースパイの場合は国家が主体だ。サービス妨害ではDDoS攻撃の31%をアクティビストが占めており、環境保護団体が地球温暖化に影響する企業を攻撃する例が多い。

侵害には、①偵察・調査、マルウエアの選定②マルウエアの侵入と対象の盗みだし③マルウエアでイトに侵害があったため、当該ベンダーとの通信を即時停止するようにクライアントに連絡し、事なきを得た。発見から助言まで要した時間は2時間だ。

今後、サイバー攻撃の対象は指数関数的に増加する。デバイスの数や通信量は飛躍的に増え、企業に対する侵害の可能性も高まる。例えば、スマートカーやウエアラブル機器は通信にブルートゥースを使用しているが、これは侵害しやすく、車そのものやウエアラブル機器を身につけた社員がマルウエアの運び屋になり得る。

自社ポリシーに合致するベンダーを選べ

侵害対策の第一歩は、侵害されたデバイスを切り離す、パッチを必ず当てる、機密情報は安全な場所に保管する、管理・運用の監督体制を守るなどだ。その上で、セキュリティーセンターを企業内に設け、ベンダーを管理するプログラムを作ることが望ましい。特にベンダー管理は重要で、自社のセキュリティーポリシーに合致するところを選定することが要となる。

講演④ 事例にみる情報漏洩事件・事故の影響と法的責任

内田・鮫島法律事務所　パートナー　弁護士　伊藤 雅浩氏

技術情報と個人情報の流出事例を紹介する。まず、技術情報については営業秘密に属するものは顧客情報などとともに、日本では不正競争防止法のもとで法的に保護されている。これを侵害した場合は差し止め、損害賠償のほか刑事罰が科されることもある。近年、営業秘密の保護の要請が高まったことから、この法律は過去14年間に7回も改正されてきた。裁判上で重要なのは、「客観的に秘密として管理されていると認められる状態」にあるかどうかだ。

2011年9月27日に知的財産高等裁判所で判決の出たポリカーボネート樹脂製造プラント事件は、原告の石油会社から中国企業に製造プラントの設計図が流出した事件だ。本件では、最終的な流出先である中国企業が被告となったわけではなく、データ持ち出しに関与し、中国企業に交付した国内企業らが被告となった。

本件では秘密管理性が認められ、同等技術のライセンス提供額に基づいて、被告に3億円の損害賠償を命じた。しかし、日本の仲介企業に対して差し止めはできたが、中国企業に対しては差し止めになっていない。技術は流出したままだ。

次に、個人情報保護法があるが、これは行政が事業者をコントロールするための法律であり、情報漏洩事故が起きた場合の民事的な紛争には、プライバシー侵害や保守契約等の契約が問題となる。

14年1月23日に東京地裁で判決が出たクレジットカード情報漏洩事件では、原告の販売サイト運営会社がサイトの実質的な管理会社であるIT（情報技術）事業者に損害賠償を求めた。SQLインジェクションという古典的な攻撃手段が使われ、約1万件のカード情報が流出した。被告は契約書で定められた責任限定条項による免責を主張していたが、契約時の技術水準に沿ったセキュリティー対策を怠っていたとして、債務不履行、契約違反の重過失責任が認められた。

法的保護には限界があり事前防衛が重要

事例の教訓としては、情報は一度漏洩したら元に戻せないという性質のため、事後的な法的救済には限界があり、勝訴しても真の救済には不十分なことから、事前防衛が重要ということだ。また、IT事業者もきちんと対策をとらなければ、訴訟リスクがある。まずは、可能な限りセキュリティー対策を整備し、ベンダー管理をきちんと行い、流出を最小限にとどめる手段を確立することが重要だ。

広　告
企画・制作
日本経済新聞社クロスメディア営業局

協賛：KPMG