ピコテクノロジーズ株式会社

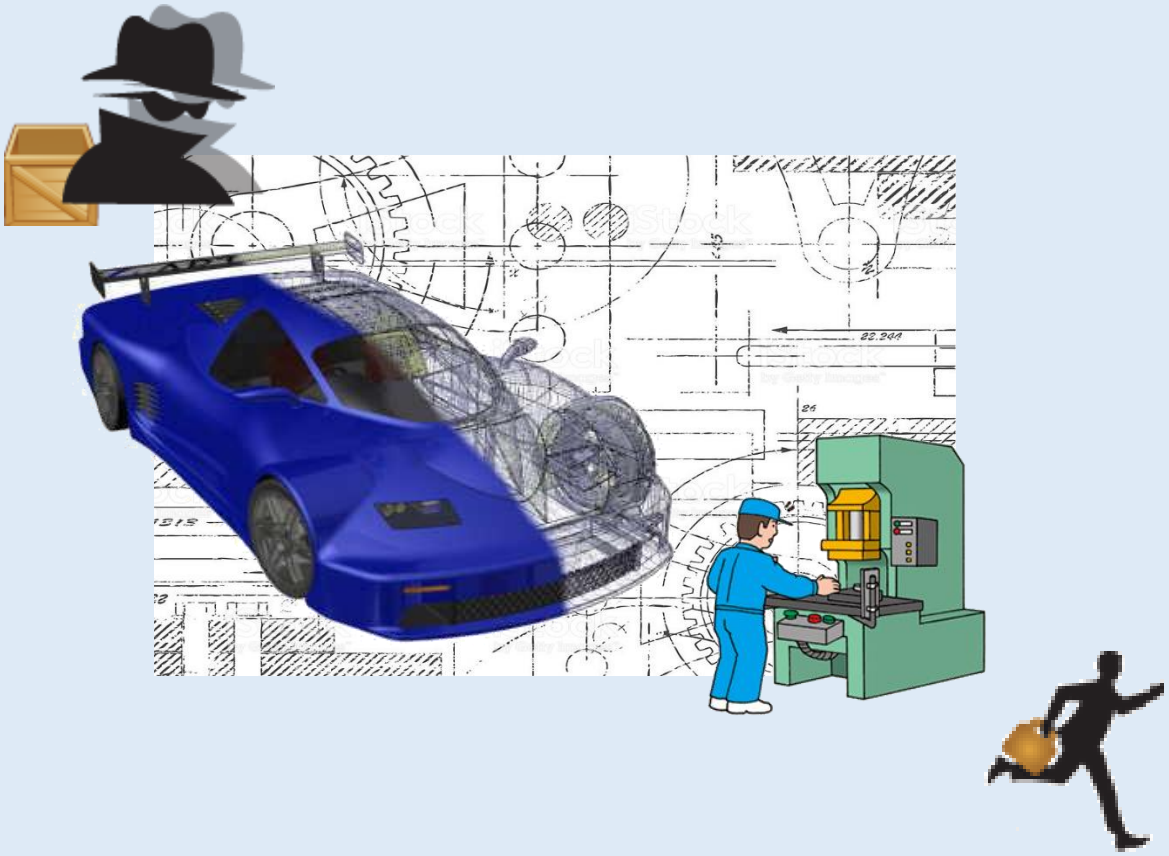
情報セキュリティ　【製造業編】

ものづくりの現場に必要な情報漏洩対策

会社の存続にかかわる重要な情報

～　簡単に流出される図面データ
～　職人技といわれている加工ノウハウ

あなたならどう守る？



平成２９年７月

１．　エンジニアリング業務におけるセキュリティ対策の基本

製造業のものづくり現場には、新製品情報、新技術情報、特許出願前の情報など、まだ世に出ていない重要な機密情報をはじめとし、ものづくりの各工程（企画、デザイン、概念設計、詳細設計、試作、解析・試験、製造、組み立て、検査、出荷）でも CG、CAD モデル、CAD 図面、解析データ、加工図面などの多くの製品に係わる情報を作り出すとともに、各工程でそれらの情報を社内的に扱ったり、また時には、取引先や外注先との打ち合わせなどで情報を社外に持ち出したり、必要に応じて社外関係者に情報そのものを渡したりして、製品が作られています。情報漏洩により、これらの情報が競合他社に渡ることで、独自技術を真似され、顧客を失いかねません。そのような事態に陥らないためにも、製造業のエンジニアリング情報の情報漏洩対策は不可欠です。

当然のことながら、社内で働いている従業員（雇用者）は会社との雇用契約によって会社側が提示している規則を守らなければなりません。また逆に、雇用者は雇用契約によって雇用者の権利も守られています。では、なぜ多くの企業で情報漏洩事件や事故が起きているのでしょうか？
大きくは、過失・故意・第三者の３つの原因に分けられます。

【過失】
過失とは、結果発生を認識すべきであったにもかかわらず、認識しなかったことを言い、具体的には次のような過失のケースから情報漏洩が起きています。

・仕事を家に持ち帰るために、必要な情報を USB メモリに入れて会社を出たが、帰宅途中に USB メモリを落として紛失したことで、USB メモリ内の情報が流出してしまった。(外部記憶デバイスの盗難・紛失事故)

・客先で打ち合わせをするために、会社からパソコンを持ち出して出掛けたが、移動中にパソコンが入った鞄を紛失して、パソコン内の情報が悪用された。(パソコンの盗難・紛失事故)

・本来はメールでやり取りを禁止されている重要な情報を、先方からの急ぎの依頼で、メールに添付して送ったつもりだったが、慌てた際にメールアドレスを打ち間違えて送信してしまった。(メール誤送信事故)

【故意】
故意とは結果発生を認識し容認していることを言い、具体的には次のような故意のケースから情報漏洩が起きています。

・知人から情報を売ってお小遣い稼ぎしないかと持ち掛けられ、知人の指示に従って、社内の情報をこっそり盗んだ。

・転職先が決まり辞表も受理されて、退職日までの間身の回りの整理をしている中で、転職先でも使えそうな資料や情報を私物と一緒に箱に詰めて自宅に送った。

・同業他社に転職するために転職活動をしていたが、面接で「ある製品の図面を持って入社してくれれば、高給で採用する」と言われ、退職前に指示された製品図面を盗んだ。

【第三者】
第三者とは内部要因とは異なりほとんどが外部要因であり、具体的には次のような外部要因のケースから情報漏洩が起きています。

・標的型攻撃により社内のパソコンがウィルス感染してしまったことに気付かずにいたら、知らぬ間に情報が漏洩されていた。

・会社のパソコンで悪質な Web サイトにアクセスしたら、ウィルスに感染してしまい、結果的に社内の情報が流出されていたことが後でわかった。

・外出途中で急ぎの仕事が入ったため、外の無料無線 LAN（Free Spot）にパソコンを接続してメールやインターネットをしていたら、パケットを盗聴されて、ウィルスにも感染してしまった。

【過失、故意、第三者の判断がしにくいケース】

・会社帰りに同僚と近くの居酒屋で飲食しながら仕事の話をしていたが、つい酔った勢いで、発売前の新製品の話をしてしまったら、誰かに聞かれたらしく、同業他社に情報が漏れてしまった。

官公庁、地方自治体、金融機関などでは、閉ざされた環境下の限られた範囲でしか情報を扱うことができなくても、仕事の結果が出せるのだが、製造業のエンジニアリング業務においては、それでは仕事にならない。多くの企業と協業することで製品が造られ、協業関係の中で頻繁に情報のやり取りが発生していることを無視することはできない。そんな環境下で日本国内の協力関係だけではなく、生産コストを削減するために海外企業との協業も積極的に行っている。
つまり、製造業のエンジニアリング業務における情報漏洩対策は、先に述べた社内の【過失】と【故意】といった内部に起因する内部要因に対する対策と、外部からの【第三者】の犯行に対する対策のみならず、外部の【過失】と【故意】にも目を向けて情報漏洩対策に取り組んでいかなければならない。ここでの外部の【過失】と【故意】に対する対策を【二次漏洩対策】とよく言われている。

製造業のエンジニアリング業務におけるセキュリティ対策とは、次の６つの脅威を未然に防ぐ対策のことである。

① 社内の過失に起因する脅威（内部要因）
② 社内の故意に起因する脅威（内部要因）
③ 社外の第三者の犯行に起因する脅威（外部からの攻撃）
④ 社外の過失に起因する脅威（二次漏洩）
⑤ 社外の故意に起因する脅威（二次漏洩）

２．　それぞれのケースに有効な各種セキュリティ製品

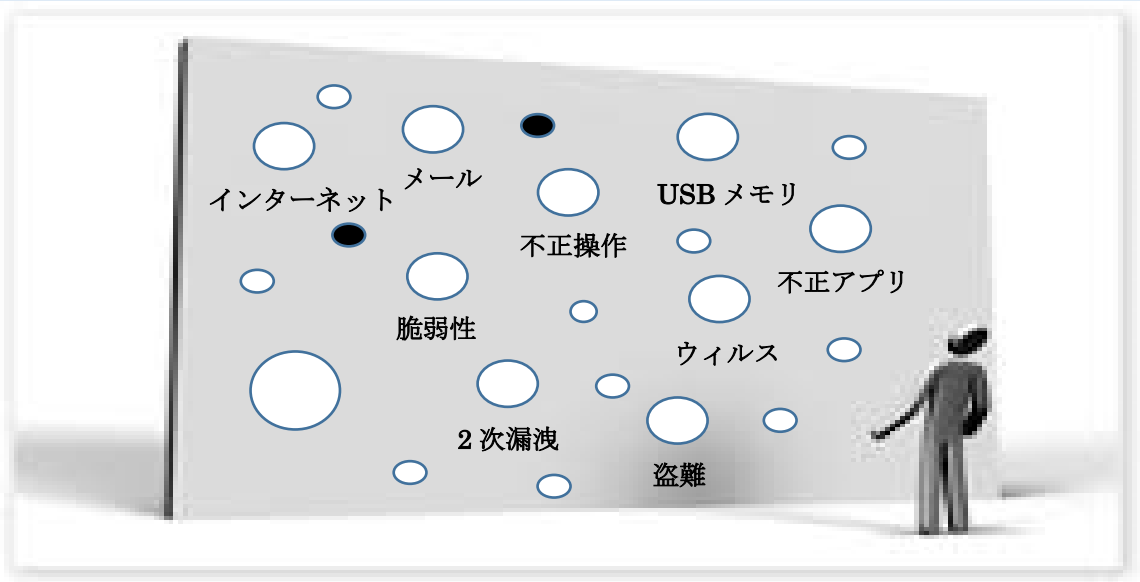
セキュリティ対策用のセキュリティ製品には、用途や目的ごとに多種多彩な製品が数多く存在するため、セキュリティ製品を選択するときには、しっかり用途や目的を定めておく必要がある。

用途・目的	種別	代表的な製品
外部からの侵入や攻撃対策	ネットワークセキュリティ製品	統合脅威管理 UTM WAF IPS
ウィルス感染対策	Microsoft 製品 ウィルス対策ソフトウェア製品 挙動検知ソフトウェア製品 振舞検知ソフトウェア製品	Windows Update McAfee Avast Symantec TREND MICRO
インターネットによる脅威対策	Web フィルタリング製品	iFILTER InterSafe WebFilter
メールによる脅威対策	メール誤送信対策製品 メールの無害化製品	CipherCraft mFILTER Active Zone
USB メモリ盗難・紛失対策	USB メモリ暗号化製品	BitLocker BUFFALO
PC の盗難・紛失対策	ハードディスク暗号化製品	SecureDoc BitLocker
PC の不正使用・誤操作対策	資産管理製品	SKYSEA QND LanScope Cat AssetView Malion IP-guard V3
無許可端末の不正使用対策	ネットワーク監視製品	OpManager
PC の操作監視による監査	資産管理製品	SKYSEA QND LanScope Cat AssetView IP-guard V3

用途・目的	種別	代表的な製品
ファイルのローカル利用禁止	シンクライアント製品	Citrix ZenDesktop/ZenApp
ファイルサーバへのアクセス制御	Microsoft 製品	Active Directory
ファイルの利用制限 （二次漏洩対策）	ファイル暗号化製品	Microsoft RMS TotalFileGuard IP-guard V+ InfoCage FileShell InterSafeIRM FinalCord DataClasys DocumentSecurity 秘文 File Encryption

３．　統合セキュリティ対策ソフトウェアの存在

企業・組織・団体によってセキュリティ対策の考え方は様々であるが、共通して考えなければならないのは、情報漏洩が起こり得る全ての可能性を未然に防ぐことが、本来のセキュリティ対策であることを忘れてはいけない。
一つの用途、一つの目的を一つのセキュリティホール（穴）とした場合、情報漏洩リスクとなるセキュリティホールは数えきれないほど存在する。企業のセキュリティ対策となるとこの無数のセキュリティホールを全てふさぐことがベストなのだが、用途や目的ごとにセキュリティ製品を選択していたのでは、費用的にもコストが膨らみ、運用管理面では管理が煩雑、複雑になってしまう。



そんな課題を解決してくれるセキュリティ製品がある。
大きくは、「外部からの攻撃に対する対策製品」、「内部要因に対する対策製品」、「二次漏洩対策に有効な製品」の３つに種別される。

外部からの攻撃に対する対策製品		
	統合脅威管理（UTM）	Firewall、VPN、IPS、アンチウィルス、アンチスパム、URL フィルタリング、アプリケーションコントロールが標準的にセキュリティ機能として提供されている。（最近では DLP 機能が付いた製品もある。）
	メール無害化対策製品	受信メールの無害化、送信メールの承認監査、URL フィルタリングなどのインターネットによるメール関連の対策機能が充実している。
内部要因に対する対策製品		
	端末操作の「記録」、「制御」、「監査」、「資産管理」製品	資産管理製品の中でもセキュリティ機能を強化して、セキュリティ対策として申し分のないソフトウェアがある。資産管理機能の他に、ファイルの操作制御、印刷制御、メール制御、デバイス制御、メッセンジャー制御、Web 閲覧制御、アプリケーション制御、ネットワーク制御、帯域制御といった各種制御機能と、リモート機能、画面モニタリング機能が一つになった非常に多機能な内部要因に対するセキュリティ対策ツールがある。（最近では、二次漏洩対策機能として、ファイル暗号機能を合わせ持った製品もある。）
二次漏洩対策に有効な製品		
	ファイル暗号化製品	MS Office ファイルや PDF ファイルなどを暗号化して、社外の協力会社や取引先に暗号ファイルとして渡し、渡した暗号ファイルを扱うことができる端末や環境を制限することで二次漏洩を防ぐことができる。ファイル暗号化製品によっては、対応できるファイル形式やアプリケーションが限定される。特に製造業で必須となる CAD/CAM/CAE 等のエンジニアリング系のアプリケーションに対応できるファイル暗号化製品は少ない。