2019.03.19

InterRisk Thai Report ＜2019 No.06＞

製造業のサイバーリスク

【要旨】
■ 製造業も過去に多数のサイバー攻撃を受け、大きな損害が発生しています。
■ IoT(Internet of Things)の普及により生産現場のサイバーリスクは今後益々高くなります。

1. 企業を対象としたサイバー攻撃の目的と方法

企業を標的としたサイバー攻撃は、「機密情報、顧客情報の窃取」、「金銭の獲得」、「企業活動の停止」を主な目的としています。また、これらの目的を達成するための準備として行われる攻撃（例：マルウェアを送り付ける準備としてメールアカウントを窃取するために行われる攻撃 など）もあります。

サイバー攻撃には下表に示すいくつかの代表的な方法があります。

表　サイバー攻撃の方法

種類	方法	主な目的
標的型メール攻撃	業務メールを装って悪意のある添付ファイルや偽サイトに誘導するための URL リンクを攻撃対象となる組織の従業員に送信し、PC 等をマルウェアに感染させる。	➢ 情報の窃取 ➢ 金銭の獲得 *感染させたマルウェアの種類による。
水飲み場攻撃	攻撃対象となる組織のユーザーが普段アクセスするウェブサイトを特定、改ざんし、アクセスした利用者の PC 等をマルウェアに感染させる。	
バックドア	マルウェアの一種。ネットワークに裏口（バックドア）を設け、システムへ自由に侵入できる環境を確保する。システムを遠隔操作し、ID、パスワードや機密情報などを外部（攻撃者）へ送信する。	➢ 情報の窃取
ランサムウェア	マルウェアの一種。感染したシステムをロックしたりファイルを暗号化したりすることによって使用不能にし、元に戻すことと引き換えに「身代金」を要求する。	➢ 金銭の獲得 ➢ 企業活動の停止
フィッシング攻撃	金融機関の Web サイトやクラウドメールのログイン画面を装ったホームページに攻撃者を誘導し、入力された暗証番号やクレジットカード番号、メールアカウントの認証情報などを窃取する。	➢ 金銭の獲得 ➢ 他の攻撃の準備
ビジネスメール詐欺	フィッシング攻撃等で得たメールアカウントを利用して従業員宛てに偽の送金指示メールや偽の請求書等を送付する。例えば経営幹部を装った偽送金指示メール（CEO 詐欺）を経理担当者等に送り不正な送金を処理させる手口や、取引先を装って偽の振込口座が記載された請求書を送付する手口などがある[*1]。	➢ 金銭の獲得
(D)Dos*攻撃 *(Distributed) Denial of Service	攻撃目標であるサイトやサーバに大量のデータを送りシステムを妨害する。受信側はトラフィックが異常に増大し、負荷に耐えられなくなったサーバやサイトがダウンする。DDoS 攻撃は乗っ取られた複数のマシンからデータを送る進化型の Dos 攻撃であり、攻撃対象により大きな負荷がかかる。	➢ 企業活動の停止

2. 製造業が標的となったサイバー攻撃の事例

製造業に特有のサイバーリスクには、サイバー攻撃による「生産の停止」と「生産技術などに関する機密情報の漏洩」があります。また、生産に関わる制御や監視などを行う計測・制御システムの多くはインターネットと直接つながっていないクローズドネットワークですが、ここ数年、サイバー攻撃によって被害を受けるケースが発生しています。

過去に製造業が標的となった主なサイバー攻撃について下表にまとめます。

表　製造業が標的となった主なサイバー攻撃[*2]

発生年	攻撃の概要	主な被害
2005 年	ドイツの自動車工場でマルウェア感染により 50 分間生産が停止。外部から持ち込まれたノート PC が原因と考えられている。	サプライヤにも感染し生産停止および復旧費用等で 17 億円程度の損害
2008 年	トルコの石油パイプラインで、監視カメラの脆弱性を利用した動作制御系への不正アクセスがあり、パイプ内の圧力が異常に高められ爆発が発生。	生産設備の爆発
2010 年	イランの原子力発電所のウラン濃縮施設で、マルウェア感染により約 8,000 台すべての遠心分離機が停止。そのうち約 1,000 台の遠心分離機が破壊。	生産停止および生産設備の破壊
2011 年	米国のゲーム会社が所有するデータベースへの不正アクセスにより 5 万件以上の顧客個人情報（メールアドレス、パスワード、住所、生年月日など）が漏洩。	情報漏洩
2011 年	カナダの自動車製造会社が所有するデータベースへの不正アクセスにより最大 283,000 件の顧客個人情報（氏名、住所、車両識別番号など）が漏洩。	情報漏洩
2013 年	日本の食品製造会社の EC サイトへの不正アクセスにより 965 名分の顧客個人情報（氏名、住所、電話/FAX 番号、メールアドレス、クレジットカード番号、有効期限など）が漏洩。	情報漏洩
2014 年	ドイツの製鉄所の社員が標的型攻撃メールを開封しマルウェアに感染。溶鉱炉の制御システムが外部から操作され、制御不能となった上、停止できなくなり設備が損傷。	生産設備の損傷
2015 年	ウクライナの電力供給会社が標的型メール攻撃を受け、マルウェアに感染。約 80 万世帯で 3 時間から 6 時間の停電が発生。同電力会社のコールセンターは停電と同時に DoS 攻撃を受け、問い合わせを受けられない状態となった。	生産停止
2016 年	DDoS 攻撃により日本の自動車製造会社の Web サーバに閲覧障害が発生。	システム障害
2017 年	ランサムウェア「WannaCry」が全世界 150 カ国、200,000 社以上の端末に感染。	（後述）
2017 年	マルウェア「NotPetya」がウクライナおよび欧米諸国を中心に少なくとも 64 カ国で感染。複数の企業で多額の損害が発生。	
2017 年	サウジアラビアの石油処理プラントが標的型攻撃を受け、安全システムがマルウェアに感染。安全システムの妨害（プロセスに異常が発生しても安全システムが反応しないようにする）によるプラントの爆破が目的とされているが、攻撃側のコーディングミスにより失敗。	なし（爆発未遂）

3. マルウェア”WannaCry”, “Not Petya”によるサイバー攻撃

2017 年に発生したマルウェア”WannaCry”と”Not Petya”の大規模なサイバー攻撃による主な企業の被害を下表にまとめます。

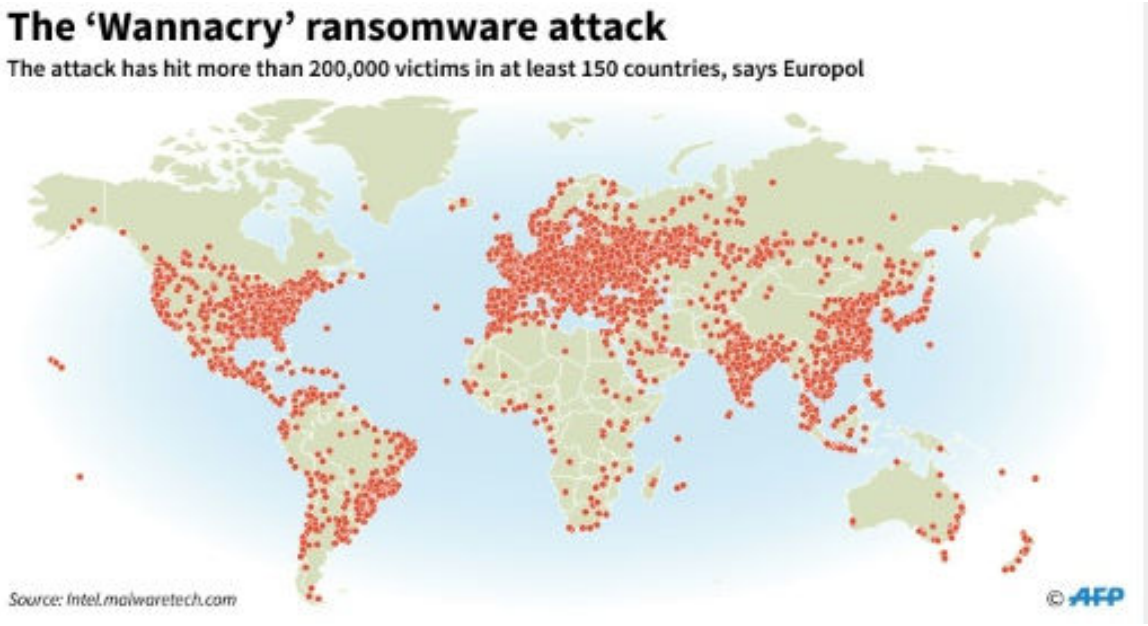
表　WannaCry, Not Petya による企業の被害[*3]

攻撃手段	発生国	企業	主な被害※
Wannacry	日本	本田技研工業（狭山工場）	✓ 生産停止：1 日
	スロベニア	ルノー子会社 Revoz	✓ 生産停止：1 日以上
	英国	日産（サンダーランド工場）	✓ 生産停止：一時的
	日本 他	日立製作所（国内拠点、海外子会社）	✓ メール管理システム、受発注管理システムの一部で障害発生
	台湾	TSMC（台南・新竹・台中工場）	✓ 生産停止：2～3 日 ✓ 出荷遅延：数ヶ月間継続 ✓ 損失額：190～250 万ドル ✓ 株価：1%程度下落
	インドネシア	ダルマイス病院	✓ 受付システムで障害が発生し数百人の患者が待機
	タイ	-	✓ 2 箇所の電光掲示板で障害発生
	シンガポール	-	✓ 商業施設数箇所の電光掲示板で障害発生
	韓国	-	✓ 国内企業 18 社が被害届を提出
Not Petya	デンマーク	AP Moller-Maersk（海上運送）	✓ 通信不能：数週間（コンピュータがオフラインとなり顧客とのやり取りが出来ない状態） ✓ 操業停止：香港、ムンバイ、ニューヨーク、バルセロナ、ロッテルダム等の港湾ターミナルで 1 週間程度 ✓ 損失額：2 億 5 千万～3 億ドル
	米国	Fedex 子会社 TNT（物流）	✓ 損失額：3 億ドル
	米国	Modelez International（製菓）	✓ 損失額：1 億 5 千万ドル
	米国	Merck（製薬）	✓ 生産停止：原薬の完全復旧に半年以上、調剤は 1 ヶ月以上、梱包は 1 ヶ月 ✓ 売上への影響は回避
	英国	Reckitt Benckiser（衛生用品製造）	✓ 生産停止：一部の工場で約 1 週間 ✓ 損失額：1 億 3 千万ドル

※損失額には売上げの減少、原因調査費用、マルウェア駆除費用、対策費用等が含まれます。

(1) ランサムウェア WannaCry の特徴

WannaCry の大規模感染は 2017 年 5 月に始まり、Intel 社の調査によれば全世界 150 カ国、200,000 以上の端末が感染しました。感染した端末では脅迫文書が表示され、300 ドル相当のビットコインの支払い（3 日以内に支払わない場合は 2 倍の 600 ドル）が要求されました。犯行グループが手にした金額は約 14 万ドルと言われています[*4]。



WannaCry 感染発生場所[*6]

WannaCry の大規模感染の特徴は以下の通りです。

①Windows の脆弱性を攻撃

WannaCry は Windows の脆弱性を攻撃する「EternalBlue」とバックドア「DoublePlusar」が組み合わされたものであり、脆弱性を持つ端末に「EternalBlue」が仕掛けられ、「DoublePlusar」がメモリ上に設置されることによって攻撃者が端末を操作することが可能になります。外部ネットワークに接続可能な脆弱性を持つポートから WannaCry がシステムに送り込まれると、同じネットワーク上の（脆弱性を持つ）全ての端末に自動的に感染します。TSMC では Windows7 環境の PC が 1 万台以上感染しました。

WannaCry の脅迫文書[*5]

②大規模感染の 2 ヶ月前に Microsoft がセキュリティ更新プログラムを公開

WannaCry の大規模感染が始まる 2 ヶ月前に Microsoft が「EtarnalBlue」に対するパッチを公開していましたが、多くの組織が同パッチを適用しておらず、感染が広がりました。本田技研工業のケースでは

生産設備に使われていた古い PC の一部が、日立製作所のケースでは欧州の拠点にある検査機器（顕微鏡）が最初に感染しました。また、TSMC のケースは大規模感染が始まった 1 年後の 2018 年 8 月に被害が発生していますが、これはサプライヤーが新しいツールのソフトウェアをインストールした際に感染したことが原因です。

(2) マルウェア NotPetya の特徴[*7]

WannaCry とほぼ同時期の 2017 年 6 月に大規模感染が始まった NotPetya による攻撃では複数の企業で多額の損害が生じています。Cybereason の推計によると全世界での損害額の合計はおよそ 12 億ドルに上ります。

NotPetya による攻撃の特徴は以下の通りです。

①市販ソフトウェアの正規アップデートファイルで感染

NotPetya は市販ソフトウェアである会計アプリケーションのアップデートファイルに仕掛けられており、同ファイルをダウンロード、実行した際に感染するものでした。これは特定の企業を狙い打ちにしたものではなく、ほぼ無差別な攻撃であったことを意味しています（一部では標的型メールによる攻撃も併用されています）。

②金銭の獲得を目的としていない

NotPetya は当初ランサムウェアとして認識されていましたが、身代金を払っても暗号化を解除できないことなどが後に判明し、金銭の獲得ではなくデータの破壊やシステムを使用できなくすること自体が目的であったとされています。比較的単純な仕組みのマルウェアですが、ファイルを暗号化した上でさらにその暗号化キーを削除するものであり、全てのデータが回復不能になるという意味では感染した端末のハードディスクを上書きして消去することに等しいと言えます[*8]。企業活動に大きなダメージを与えるマルウェアであったため、多額の損害が発生したものと考えられます。

4. IoT (Internet of Things) の普及によるサイバーリスクの増大

製造業では各種センサーによる機械の自動制御、故障予知、稼働状況の見える化など、新たな技術が導入され始めており、様々なもの（機械、設備 等）がネットワークに繋がる IoT (Internet of Things)が推進されています。前述のとおり、クローズドネットワークである従来の制御システムでもサイバー攻撃による被害が発生していますが、IoT の普及により生産現場のサイバーリスクは今後益々高くなっていくものと考えられます。

IoT へのサイバー攻撃で想定されるリスクには次のようなものがあります[*9]。

- ✓ 工場の機械が停止・遠隔操作される
- ✓ 検査データが改ざんされ、知らぬ間に不良品が出荷される
- ✓ 稼働データが改ざんされ、機器の異常発見が遅れる
- ✓ サイバー攻撃により自社の工場が停止することで、取引先に影響を与える

執筆者：InterRisk Asia (Thailand) Co., Ltd. 佐藤 公紀

参照

*1: Trend Micro (https://blog.trendmicro.co.jp/archives/17003)

*2: ICT サイバーセキュリティ経営ガイドライン等を基に作成

*3: Cybereason。JPCERT コーディネーションセンター「制御システム・セキュリティの現在と展望」等を基に作成

*4: ZD Net Japan の記事を参照

*5: Kaspersky Security

*6: Intel

*7: Cyberason の記事を基に作成

*8: トレンドマイクロ株式会社「ランサムウェアの多様化が生んだ「WannaCry」」

*9: JPCERT「工場における産業用 IoT 導入のためのセキュリティ ファーストステップ」

MS&AD インターリスク総研株式会社は、MS&AD インシュアランスグループに属する、リスクマネジメントに関する調査研究およびコンサルティングを行う専門会社です。タイ進出企業さま向けのコンサルティング・セミナー等についてのお問い合わせ・お申込み等はお近くの三井住友海上、あいおいニッセイ同和損保の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
MS&AD インターリスク総研（株） 総合企画部 国際業務グループ
TEL.03-5296-8920
https://www.irric.co.jp/

インターリスクアジアタイランドは、タイに設立された MS&AD インシュアランスグループに属するリスクマネジメント会社であり、お客様の工場・倉庫等における火災リスク調査や洪水リスク評価、ならびに交通リスク、サイバーリスク等に関する各種リスクコンサルティングサービスを提供しております。お問い合わせ・お申し込み等は、下記の弊社お問い合わせ先までお気軽にお寄せ下さい。

お問い合わせ先
InterRisk Asia(Thailand) Co., Ltd.
175 Sathorn City Tower. South Sathorn Road.Thungmahamek. Sathorn. Bangkok 10120. Thailand
TEL: +66-(0)-2679-5276
FAX: +66-(0)-2679-5278
https://www.interriskthai.co.th/

本誌は、マスコミ報道など公開されている情報に基づいて作成しております。
また、本誌は、読者の方々に対して企業の CSR 活動等に役立てていただくことを目的としたものであり、事案そのものに対する批評その他を意図しているものではありません。