今すぐ実践できる工場セキュリティハンドブック
リスクアセスメント編　第 1.1 版

2022 年 6 月

JNSA 日本ネットワークセキュリティ協会

西日本支部

今すぐ実践できる工場セキュリティ対策のポイント検討 WG

改版履歴

第 1.1 版

2022 年 6 月 13 日　改版履歴追加

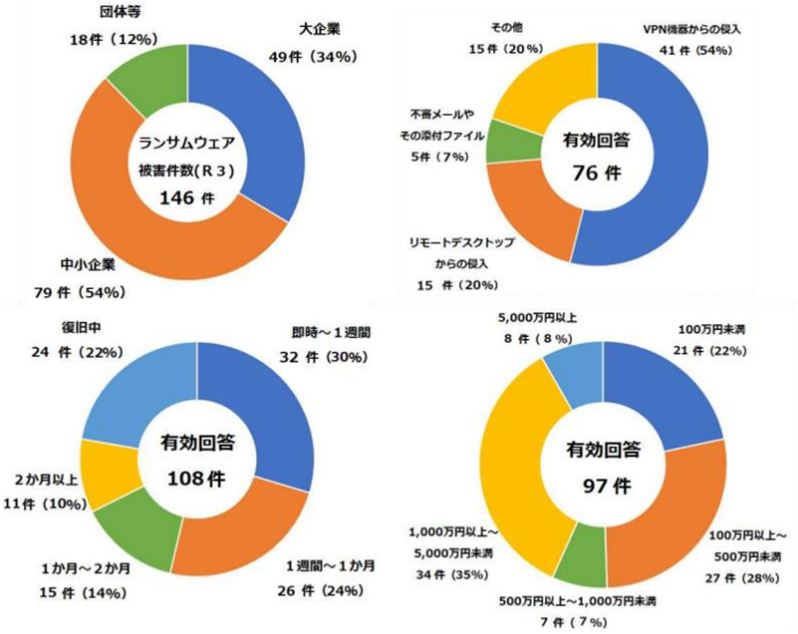
2022 年 6 月 13 日　P17 誤字修正（無声 WiFi→無線 WiFi）

目次

工場セキュリティハンドブック・リスクアセスメント編

１．はじめに

ここ数年、ランサムウェアなどによって工場の稼働が停止する事件・事故が増えてきました。これは、これまで比較的、外の環境（例えばオフィス環境やインタネット環境）とは接点を持たず、閉じた環境で稼働していた製造現場が、昨今の IoT 活用や DX の推進などをきっかけに、外部環境と接点を持ち始めたことに関係していると思われます。「うちの工場はインターネットや事務所のネットワークから切り離されているから大丈夫」と思われる事業者も多いようですが、よく調べると既につながっていたり、保守用のネットワーク（VPN 接続等）や持ち込んだ PC からの侵入で被害に遭うケースもあります。



警察庁広報資料令和4年4月7日
「令和３年におけるサイバー空間をめぐる脅威の情勢等について」より引用

労働安全衛生法では、労働災害の防止を主な目的として、事業者が自主的に事業所の設備や原材料、作業などに起因する危険性や有害性などの調査を実施するリスクアセスメントの実施が定められています。設備の高度化とともにネットワークを活用した生産性向上やサプライチェーン連携などが進められるなか、これまであまり関係がないと思われてきた情報セキュリティリスクが労働災害を引き起こす原因となったり、経営に大きな影響を及ぼす脅威となる可能性が高まってきており、リスクアセスメントの対象に情報セキュリティリスクを加える必要があります。

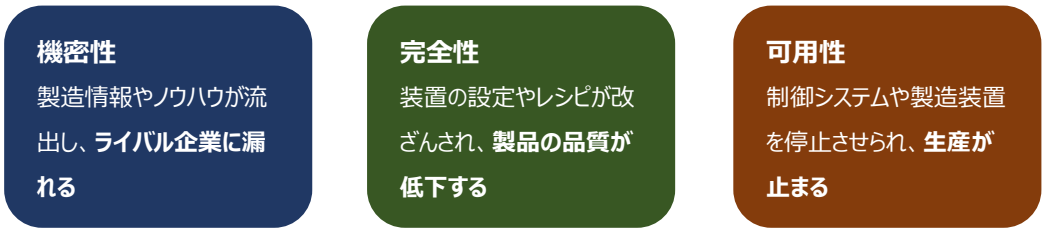
工場における情報セキュリティリスクアセスメントは、情報セキュリティに関連する脅威による危険性や有害性を特定し、この対策をするための第一歩として非常に重要ですが、一方で情報セキュリティの専門知識を持つ人材を確保することが難しいという現実があります。

この工場セキュリティハンドブック・リスクアセスメント編は、中小企業において、製造現場で従事する方々が、もっと容易にセキュリティ対策に取り組んでいただけるように、専門知識をあまりお持ちでない方が読みやすいよう、できるだけ平易な解説と具体的な事例をもとに実践方法をまとめたものです。

1．1　ハンドブック・リスクアセスメント編活用の目的

製造装置の誤動作や停止、あるいは品質低下につながるような情報セキュリティリスクを理解し、自社の製造現場における現状を正しく把握するためには、脅威の存在と客観的なリスク評価が必要です。

では、製造現場と情報セキュリティリスクにはどのような繋がりがあるのでしょうか。例えば、一般的なオフィス環境では、情報を適切に管理するために、「機密性」、「完全性」、「可用性」の３つの観点が用いられて情報セキュリティリスクを考えます。これに倣って、例えば、製造現場がコンピュータウイルス（脅威）に感染した場合、どのようなリスクがあるのか、３つの観点との関係性を考えてみます。



全ての製造現場で、このようなリスクが存在するわけではありません。工場セキュリティリスクアセスメントは、このようなリスクが実際に存在するのかどうかを確かめることであり、本ハンドブックは、**自らの手**で実践できるようになるための参考書として活用されることを目的としています。

1．2　対象事業者

設計から出荷までの製品製造工程の中で、コンピュータおよび電子技術を利用し、計算や情報の処理および組み立てや加工、検査などを自動的に行う設備を導入している中小製造業（製造される物の分野は問いません）が対象となります。

1．3　アセスメント実施者

本ハンドブックを参考にしたリスクアセスメントは、経営者および情報システム責任者、製造現場責任者が推進し、製造現場責任者、工場システム担当者、情報システム担当者、もしくはこれに準ずる担当者が実施することを想定しています。（製造現場の状況を把握していることを前提として、方法や解説が記載されています）

1．4　アセスメント対象

本ハンドブックがリスクアセスメントの対象とする領域は、コンピュータおよび電子技術を利用し、計算や情報の処理および組み立てや加工、検査などを自動的に行う設備とこれらをつなぐネットワーク、ならびに装置やネットワークが設置された場所とします。（詳細は付録　４．１　アセスメント対象の俯瞰図）

1．5　アセスメント後の対応

本ハンドブックを参考にリスクアセスメントを実施した後の対応を支援するために、以下の続編を予定しています。併せてご活用下さい。

- 工場セキュリティハンドブック・リスク対策編（リスクに合わせた具体的な対策実施の事例集）
- 工場セキュリティハンドブック・サイバーBCP 策定編（工場セキュリティに着目した BCP 策定のヒント）

2．工場セキュリティリスクアセスメントとは

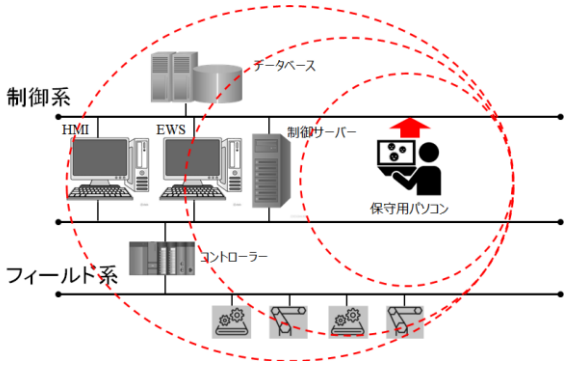
製造現場におけるセキュリティリスクとはどのようなものなのか、具体的にリスクアセスメントを実施するにはどのような方法があるのか、アセスメント結果とリスク対策はどのようにつながるのかなどについて、詳しく解説します。

2．1　製造現場におけるセキュリティリスク

リスクとは「損害を受ける可能性」であり、これを現実のものにする引き金が「脅威」、この脅威を受けてしまう弱点が「脆弱性」です。従って、脆弱性がなければ、リスクは現実のものにはならないということです。では、実際の製造現場には、どのような脆弱性と脅威があるのでしょうか？まずは脅威の入口となり得るものの例を下記に列挙します。

＜USB メモリー＞ ＜パソコン＞ ＜スマホ･タブレット＞ ＜IoT 機器･センサー＞ ＜複合機＞ ＜ハンディターミナル＞ ＜OA ネットワーク＞ ＜インターネット＞ ＜WiFi＞ ＜機器保守用回線＞ ＜クラウド＞ ＜電子部品･原材料＞ ＜新規導入機器＞

これらの入口に脆弱性があった場合、どのようなリスクが考えられるのか、一例を示します。



保守用パソコンがマルウェアに感染していることを知らずに製造現場 LAN に接続してしまうと、ネットワークの通信速度に比例してマルウェアが工場内の装置に広がります。マルウェアに感染した装置は正常に動作せず、工場全体が止まってしまいます。

【解説】マルウェア
マルウェア（malware）とは、不正かつ有害に動作させる意図で作成された、悪意のあるソフトウェアや悪質なコードの総称。コンピュータウイルスが代表例。感染拡大には様々な方法が使われる。

2．2　リスクアセスメントの位置づけ

リスクアセスメントは、情報セキュリティ対策の最初のステップです。どこに脆弱性があるかが分からなければ、有効な対策を行うことはできません。

先に挙げた「入口」を全て塞げば、脅威は工場の中には侵入できません。従って、工場内に脆弱性が存在しても、リスクはないということになります。しかし、現実には、この「入口」を全て塞げば生産はできなくなります。そこで、どの入口からどんな脅威が侵入してくる可能性があるのか、その脅威は、工場のどの脆弱性にどんなダメージを与えるのかをしっかり見極めないと、必要な対策ができないということです。

例えば、マルウェアが仕込まれた USB メモリーを製造現場の装置に差し込むと、製造装置がマルウェアに感染し、誤動作をしたり、停止したりするリスクがあります。このリスクに対する対策は、USB メモリーを使わない、USB メモリーを使用する前にマルウェアのチェックをする、製造装置にマルウェアを検知する機能を備える、などが考えられます。

当工場では、USB メモリーを使うのか使わないのか、使うならどのような条件があるのか、どのように守るのか、などを正しく把握しなければ、リスクの有無も対策の方法もわからないということになります。このように、リスクアセスメントは、最適な対策を決めるためには不可欠な作業ということです。

2．3 リスクアセスメントの実施

リスクアセスメントの実施には、いくつかの標準的な方法がありますが、本ハンドブックでは、リスクベースアプローチを主体として、情報セキュリティにあまり詳しくなくても実践できるような方法を紹介します。もし、社内のオフィス部門において、セキュリティリスクアセスメントを実施されている場合は、その手法に合わせて工場でも実施する方法もあります。その場合は、本ハンドブックに記載されている工場でのリスクの考え方などを参考にして下さい。

【解説】リスクベースアプローチ

脅威が侵入してくるシナリオを用意し、これに対して現在の環境でどういう条件の場合に攻撃が成功し、どのような対策を導入すればその脅威の可能性を下げられるのかを検証する方法

3　工場セキュリティリスクアセスメントの実践

本ハンドブックで紹介するリスクアセスメントは、工場が抱えるリスクを網羅的に洗い出すことではなく、今すぐにでも取り組まなければならない緊急性の高いリスクの把握に重点が置かれています。また、手順や考え方をできるだけ単純化し、実践のしやすさを第一に考えられています。

3．1　脅威シナリオ

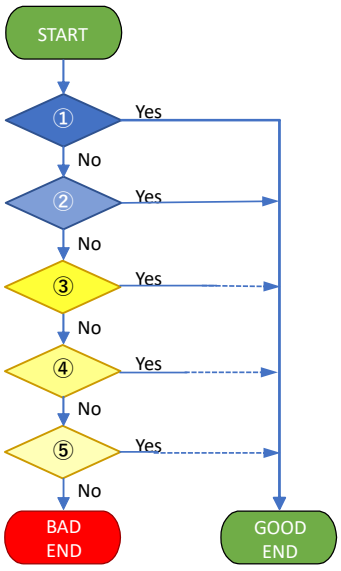
緊急性が高いと考えられる脅威のシナリオは、製造業における過去の情報セキュリティ事故事例や、本ハンドブック検討メンバーの知見から選定されています。表１は、本ハンドブックで取り扱う脅威のシナリオの一覧です。

No	脅威の入口	脅威が引き起こす可能性のある事象	懸念されるリスク
1	USBメモリー	USBメモリーから制御システムや製造装置にマルウェアの感染が広がる	工場停止
2	持込パソコン	持込パソコンから制御システムや製造装置にマルウェアの感染が広がる	工場停止
3	スマホ・タブレット	スマホ・タブレットに感染したマルウェアが利用者の意図しない動作をさせる	情報漏洩
4	IoT機器・センサー	IoT機器・センサーが第三者に遠隔操作される	工場停止
5	複合機	複合機が第三者に遠隔操作される	情報漏洩
6	ハンディターミナル	ハンディターミナルに感染したマルウェアがプログラムやデータを改竄する	情報改竄
7	OAネットワーク	OAネットワークからマルウェアの感染が広がる	工場停止
8	インターネット	インターネットからマルウェアの感染が広がる	工場停止
9	Wi-Fi（無線AP）	Wi-Fi通信が傍受されたり、通信が妨害される	情報漏洩
10	保守用ネットワーク	保守用ネットワークからマルウェアの感染が広がる	工場停止
11	クラウドサービス	認証情報が不正に利用される	情報漏洩
12	部品・原材料	組み込んだ部品のセキュリティ不具合が悪用される	品質低下
13	新規購入機器	新規購入した機器から制御システムや製造装置にマルウェアの感染が広がる	工場停止

表１　脅威シナリオ一覧

3．2　アセスメント方法

それぞれの脅威シナリオには、いくつかのチェックポイントが設けられており、それぞれのチェックポイントで示されている条件（＝対策）と現状の環境を比較し、ギャップを確認することで、リスクアセスメントが行えるようになっています。



左図の例では①～⑤がチェックポイントであり、いずれかのチェックポイントで現状が条件を満たした場合は、脅威シナリオで示されたリスクは回避できることを示しています。ただし、下位になるほど、十分な回避力にはなりません。（点線で表現）

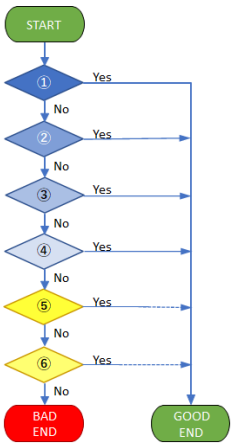
従って、上位で条件を満たすほど、リスク回避力が高いことから、対策は自社の環境や状況を考慮した上で、上位から順に検討することが望ましいと言えます。（詳しくは「工場セキュリティ対策編」を参考にして下さい）

どのチェックポイントでも条件を満たさなかった場合は、現状では、脅威シナリオで示されたリスクが現実のものとなる可能性が高いと判断できます。

3．3　各脅威シナリオとチェックポイント

(1)USB メモリー

製造装置に USB メモリーを差し込みデータの授受を行ったところ、当該製造装置（もしくはその他の製造装置）の動作が異常となった。



現状の対策状況		対策の効果等
①	USBメモリーが使える製造装置はない	USBメモリーによる脅威はない
②	USBメモリーは使用禁止であり、ルールを確実に運用している	USBメモリーの脅威を持ち込まない
③	マルウェアチェック済みのUSBメモリー以外は使用しないルールを確実に運用している	USBメモリーからマルウェアを取り除き、安全な状態で利用できる
④	製造装置にマルウェア対策を導入している	マルウェアに感染したUSBメモリーが持ち込まれても製造装置側でマルウェア感染が防げる
⑤	製造現場LANの通信内容をモニタリングしている	マルウェアの感染拡大の動きを検知して、蔓延する前に対処することができる
⑥	製造装置の動作不良の原因調査にはセキュリティ観点も加えている	装置ログや通信ログを分析して、何らかのマルウェアが原因であることが判明すれば、適切な応急・復旧処置ができる

※ルールは徹底され、適切に運用されていることが前提

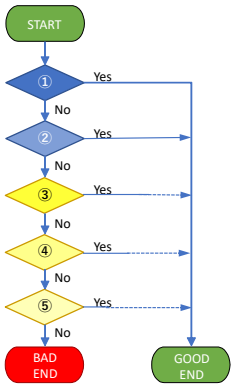
【補足】

- 製造装置の動作が異常になる原因は、USB メモリーにマルウェアが混入していて、ここから感染が広がり、製造装置も感染してしまうことによるものです。
- 製造装置がマルウェアに感染した場合、その影響で装置の動作が不安定になったり、意図的に必要なファイルが暗号化され動作ができなくなったり、装置内の情報を外部に送信されたりする被害が発生する可能性があります。
- 特に暗号化されるケースでは、暗号化を解除する代償に、金銭を要求するランサムウェアと呼ばれるマルウェアの被害が多くなっています。（金銭を払っても解除される保証はありません）
- 情報の窃取が目的のマルウェアに感染した場合は、装置の動作に大きな変化が現れないこともあります。
- ⑤の「モニタリング」とは、工場内の通信の内容を専用の仕組みで見張ることです。マルウェアが拡散時に行う特有の通信の有無を見張ることで、マルウェアの存在を検知することができます。
- ⑥の「セキュリティ観点を加える」とは、機械的な故障ではなく、マルウェア感染などが原因であることを調査するための手順やツールを準備することです。

MEMO

(2)持込パソコン

製造装置の保守のために製造現場 LAN に保守用 PC を接続したところ、当該製造現場の装置（もしくはその他の製造現場の装置）の動作が異常となった。



	現状の対策状況	対策の効果等
①	マルウェアチェック済の許可されたPC以外は接続しないルールを確実に運用している	安全な状態でPCが利用できる
②	製造装置にマルウェア対策を導入している	マルウェアに感染したPCが持ち込まれても、製造装置側でマルウェア感染が防げる
③	PCが製造現場LANに接続されたことがすぐに検知できる	無断でPCが接続されても、すぐに取り外すことができる。ただし、既にマルウェアが拡散してしまった可能性がある
④	製造現場LANの通信内容をモニタリングしている	マルウェアの感染拡大の動きを検知して、蔓延する前に対処することができる
⑤	製造装置の動作不良の原因調査にはセキュリティ観点も加えている	装置ログや通信ログを分析して、何らかのマルウェアが原因であることが判明すれば、適切な応急・復旧処置ができる

※ルールは徹底され、適切に運用されていることが前提

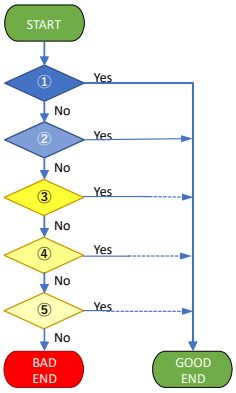
【補足】

- 製造装置の動作が異常になる原因は、保守用 PC にマルウェアが混入していて、ここから感染が広がり、製造装置も感染してしまうことによるものです。
- 製造装置がマルウェアに感染した場合、その影響で装置の動作が不安定になったり、意図的に必要なファイルが暗号化され、動作ができなくなったり、装置内の情報を外部に送信されたりする被害が発生する可能性があります。
- 特に暗号化されるケースでは、暗号化を解除する代償に、金銭を要求するランサムウェアと呼ばれるマルウェアの被害が多くなっています。（金銭を払っても解除される保証はありません）
- 情報の窃取が目的のマルウェアに感染した場合は、装置の動作に大きな変化が現れないこともあります。
- ③の「LAN に接続されたことが検知できる」とは、製造現場の LAN に接続されているネットワーク機器や LAN を監視し、新たに接続された機器を見つけることができるような仕組みです。これにより、PC が無断で接続されることを防ぐことができます。
- ④の「モニタリング」とは、工場内の通信の内容を専用の仕組みで見張ることです。マルウェアが拡散時に行う特有の通信の有無を見張ることで、マルウェアの存在を検知することができます。
- ⑤の「セキュリティ観点を加える」とは、機械的な故障ではなく、マルウェア感染などが原因であることを調査するための手順やツールを準備することです。

MEMO

(3)スマホ・タブレット

工場内の様子（写真、録音）や装置情報などがインターネット上の掲示板や SNS で拡散された。



	現状の対策状況	対策の効果等
①	製造現場の内でのスマホ・タブレットは、使用禁止であるルールを確実に運用している	スマホ・タブレットによる脅威はない
②	マルウェアチェック済の許可されたスマホ・タブレット以外は、製造現場に持ち込みを禁止するルールを確実に運用している	安全な状態でスマホ・タブレットが利用できる
③	スマホ・タブレットが製造現場LANに接続されたことがすぐに検知できる	無断でスマホ・タブレットがLANに接続されても、すぐにすぐに取り外すことができる。ただし、既にマルウェアが拡散してしまった可能性がある
④	製造現場LANの通信内容をモニタリングしている	マルウェアの感染拡大の動きを検知して、蔓延する前に対処することができる
⑤	自社の情報が外部にもれていないかをチェックする体制や仕組みがある	装置ログや通信ログを分析して、何らかのマルウェアが原因であることが判明すれば、適切な応急・復旧処置ができる

※ルールは徹底され、適切に運用されていることが前提

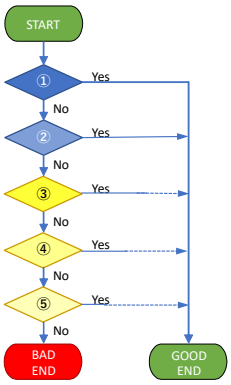
【補足】

- 情報漏えいの原因は、スマホ・タブレットにマルウェアが混入していて、スマホ・タブレットのカメラやマイクが不正に操作されたり、マルウェアがネットワークに接続されている装置に拡散し、装置情報が不正に収集され、インターネット上に公開されることによるものです。
- マルウェアが原因ではなく、故意に人が盗撮、盗聴を行う可能性もあります。
- ③の「LAN に接続されたことが検知できる」とは、製造現場の LAN に接続されているネットワーク機器や LAN を監視し、新たに接続された機器を見つけることができるような仕組みです。これにより、スマホやタブレットなどが無断で接続されることを防ぐことができます。
- ④の「モニタリング」とは、工場内の通信の内容を専用の仕組みで見張ることです。マルウェアが拡散時に行う特有の通信の有無を見張ることで、マルウェアの存在を検知することができます。
- ⑤の「チェックする体制や仕組み」は、定期的にインターネット上の情報を検索したり、ログを分析するような対応を組織的に実行することです。

MEMO

(4)IoT 機器・センサー

直接インターネットに接続されていない製造装置が IoT 機器やセンサーから攻撃を受け、生産が停止した



	現状の対策状況	対策の効果等
①	IoT機器・センサーは使用していない	IoT機器・センサーによる脅威はない
②	センサーネットワークと製造現場LANは分離されている	Iot機器・センサーからの脅威（攻撃）を受けない
③	セキュリティ対策が考慮されているIoT機器・センサー製品を使用している	IoT機器・センサーのマルウェア感染が防げる
④	IoT機器・センサーの脆弱性情報を入手し、適宜対処を行っている	IoT機器・センサーのマルウェア感染が防げる（対処が遅れるとマルウェアに感染する可能性がある）
⑤	製造現場LANの通信内容をモニタリングしている	大量通信データの流入を早期に検知し、ネットワークを切り離すことで、被害を最小限に抑えることができる

※ルールは徹底され、適切に運用されていることが前提

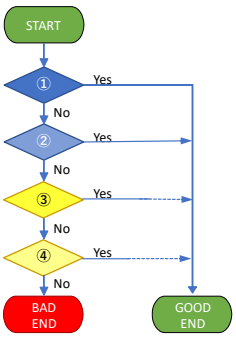
【補足】

- 製造装置への攻撃の原因は、マルウェアに感染した IoT 機器やセンサー（例えば監視用カメラや赤外線センサーなど）が遠隔で操作されることによるものです。
- IoT 機器・センサーにはセキュリティ対策が不十分なものも多く存在し、不正アクセスやマルウェア感染の脅威を受けやすいと考えられています。
- ③の「ネットワーク分離」とは、製造現場 LAN とは物理的に接続せずに、IoT 機器・センサー専用の LAN を作る方法や、物理的にはつながっていても、製造現場 LAN とは直接通信できないようにネットワーク機器の設定で分離する方法などがあります。
- ④の「脆弱性情報」とは、IoT 機器・センサーのベンダーが公開しているプログラムの不具合情報であり、これを取得して速やかに対処を行うことが望ましいです。
- ⑤の「モニタリング」とは、IoT 機器・センサーの挙動を見張ることです。製造機器を攻撃するような通信の有無を見張ることで、マルウェアの存在を検知することができます。

MEMO

(5)複合機

製造現場内の複合機でコピーした図面などが、インターネット上の掲示板や SNS で拡散された。



現状の対策状況		対策の効果等
①	複合機内のデータ暗号化機能や自動削除機能を利用している	ハードディスク内に残っている情報の漏洩を防ぐことができる（該当機能を有する複合機に限る）
②	複合機の管理者IDやパスワードを有効にして、第三者が複合機の内部情報にアクセスできないように設定している	不正アクセスを制限できる
③	複合機のリモート監視やコピーカウンター情報の収集のために必要なネットワーク回線は、電話回線に限定している	外部からのアクセスを制限できる
④	ネットワーク機器（ファイアウォールやルータなど）で外部から複合機への特定の通信のみに制限している（アクセス制御）	接続を制限することで製造現場LANへの不正侵入を防止できる

ルールは徹底され、適切に運用されていることが前提

【補足】

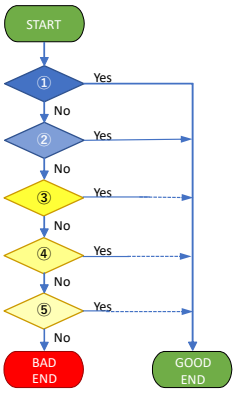
- 情報漏洩の原因は、複合機（コピー機含む）に内蔵されたハードディスクなどに一時的に保存されているコピー情報がネットワークを介して不正に窃取されることによるものです。
- ①では、内部に情報を残さないようにする機能の利用です。（機能がない機種もあります）
- ②では複合機の管理者機能を特定の管理者のみに割り当てるものです。
- ③④では外部から複合機のリモート監視やカウンターの使用量を収集するためのアクセスを特定の保守業者などに制限するものです。
- このシナリオとは別に、複合機を入れ替える場合など、内蔵のハードディスクに情報が残っている状態で廃棄されると、ここから情報が漏洩する可能性があります。廃棄時には確実に内部情報を削除するなどの注意が必要です。また、複合機の機種選定時に、ハードディスクの暗号化機能を有する機種を選定することも対策として有効です。

MEMO

(6)ハンディターミナル

最近、原材料の工場在庫や製品出荷数データに誤りが多く、管理業務に大きな影響が出ている。

注）ハンディターミナルからデータを受信するサーバーは、情報系（OA)環境にあるサーバーと同等のセキュリティ対策が施されていることが前提



	現状の対策状況	対策の効果等
①	使用しているハンディターミナルは、遠隔でファームウェア、OS、アプリケーションソフトのアップデートを行う機能はない	外部からプログラムを書き変えることができないため、マルウェアが侵入することはない
②	使用しているハンディターミナルのOSは、ベンダー固有で独自のものが使用されている	一般的なOSではないため、脆弱性を見つけることが難しく、マルウェアが侵入しにくい
③	ハンディターミナルのファームウェア、OS、アプリケーションソフトは、常に最新化している	最新化することで既知の脆弱性が対処される
④	定期的にハンディターミナルのマルウェアチェックを行っている	感染したマルウェアを駆除できる可能性がある
⑤	データの不整合は早期に検出でき、異常のあるハンディターミナルを交換する手順が定まっている	ハンディターミナルを交換することで、被害を最小限に抑えられる

※ルールは徹底され、適切に運用されていることが前提

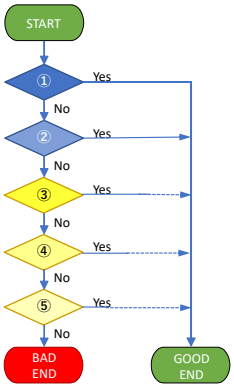
【補足】

- データ誤りの原因は、ハンディターミナルのプログラムが改ざんされたことによるものです。（プログラムの不具合の場合もあります）
- ①のようなハンディターミナルでは、プログラムはハードウェア的に組み込まれているため、外部からプログラムを改ざんすることはできません。
- ②のようなハンディターミナルでは、OS の詳細情報が公開されていないため、第三者の攻撃の対象になる可能性が低くなります。
- ⑤は、データ不整合の原因が不明でも、不具合のあるハンディターミナルを速やかに交換し、該当ハンディターミナルを保守業者やメーカーで詳しく調査してもらうことで、被害を最小限に抑えるとともに、再発防止対策に役立ちます。

MEMO

(7)OA ネットワーク

リアルタイムな生産情報収集のために、新たに工場と OA 棟（一般オフィス棟）をネットワークで接続したところ、工場内の生産制御システムに異常が発生し、生産が停止した



	現状の対策状況	対策の効果等
①	OAネットワーク（一般オフィスネットワーク）と工場ネットワーク（製造現場LAN）は物理的に繋がっていない	物理的に繋がっていないので、ネットワークを経由して脅威が侵入することはない
②	工場ネットワークには、OAネットワーク内の特定のPCやサーバー以外はつながらないように制限されている	工場ネットワークにつながる機器を制限することで、OAネットワークの影響を軽減することができる
③	工場ネットワーク内のPCや生産制御システム（サーバー）にはウイルス対策ソフトが導入されている	ウイルス対策ソフトの導入により、マルウェアの感染を防止できる。ただし、ウイルス対策ソフトが導入できない機器は感染する可能性がある
④	製造現場LANの通信内容をモニタリングしている	マルウェアの感染拡大の動きを検知して、蔓延する前に対処することができる
⑤	製造装置の動作不良の原因調査にはセキュリティ観点も加えている	装置ログや通信ログを分析して、何らかのマルウェアが原因であることが判明すれば、適切な応急・復旧処置ができる

※ルールは徹底され、適切に運用されていることが前提

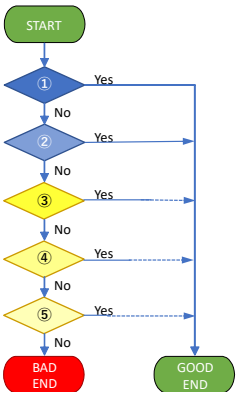
【補足】

- 生産制御システムの異常の原因は、OA ネットワークから拡散されたマルウェアが生産制御システムに感染したことによるものです。
- OA ネットワーク内の PC やサーバーはセキュリティ対策が施されているので、感染することはなくても、工場ネットワークのみが被害に遭う場合もあります。
- ②のように OA ネットワーク内から工場ネットワークへアクセスできる機器を制限する方法としては、ネットワーク機器（ファイアウォールやルーターなど）で設定する方法が一般的です。
- ③のように工場ネットワーク内の PC や生産制御システムにウイルス対策ソフトが導入されていれば、完全ではないですが、多くのマルウェアによる攻撃を防ぐ効果があります。また、その機器のバージョンアップやセキュリティパッチを適用することで脆弱性が解消され、マルウェアに感染した PC からの攻撃は防御できます。
- ④の「モニタリング」とは、工場内の通信の内容を専用の仕組みで見張ることです。マルウェアが拡散時に行う特有の通信の有無を見張ることで、マルウェアの存在を検知することができます。
- ⑤の「セキュリティ観点を加える」とは、機械的な故障ではなく、マルウェア感染などが原因であることを調査するための手順やツールを準備することです。

MEMO

(8)インターネット

生産性とデリバリースピードの向上を図るために、新たに工場からインターネット回線を活用してサプライチェーンを強化したところ、製造装置が次々と停止し、生産ができなくなった



	現状の対策状況	対策の効果等
①	インターネット接続はない	インターネットからの脅威はない
②	工場内からのインターネット利用はサプライチェーンに関わる事業者との接続や特定のクラウド利用、機器の保守のみに制限している	信頼できる接続先のみに制限することで、リスクを低減できる
③	メールの送受信やWEBアクセスは専用のPCからのみに制限し、当該PCはウイルス対策ソフトの導入とパッチ適用を確実に行っている	インターネット上のサービスを利用する環境を堅牢にすることでリスクを低減できる
④	製造現場LANの通信内容をモニタリングしている	マルウェアの感染拡大の動きを検知して、蔓延する前に対処することができる
⑤	製造装置の動作不良の原因調査にはセキュリティ観点も加えている	装置ログや通信ログを分析して、何らかのマルウェアが原因であることが判明すれば、適切な応急・復旧処置ができる

※ルールは徹底され、適切に運用されていることが前提

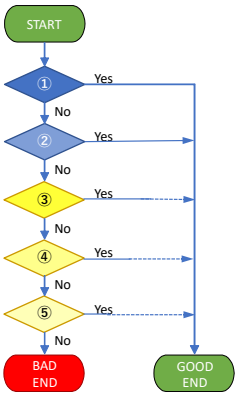
【補足】

- 製造装置が停止した原因は、接続した社外事業者からのマルウェア拡散やメール受信やWEB 閲覧によるマルウェア感染などによるものです。
- ②のように接続先を制限することは重要ですが、接続先の事業者のセキュリティ対策が不十分であれば、その影響を受けることになりますので、事前に状況を確認したり、契約等で責任を明確にしておくことが望ましいです。
- ③のようにメールや WEB を利用する場合は、確実なセキュリティ対策を実施しなければ、無防備な工場内装置は多大な被害を受けることがあります。
- ④の「モニタリング」とは、工場内の通信の内容を専用の仕組みで見張ることです。マルウェアが拡散時に行う特有の通信の有無を見張ることで、マルウェアの存在を検知することができます。
- ⑤の「セキュリティ観点を加える」とは、機械的な故障ではなく、マルウェア感染などが原因であることを調査するための手順やツールを準備することです。

MEMO

(9)Wi-Fi（無線 AP）

製造現場内に新たに Wi-Fi を導入したところ、徐々に通信速度が遅くなり、生産が止まっている夜間でも、無線 AP の通信ランプが激しく点滅している



	現状の対策状況	対策の効果等
①	工場内で無線WiFiは使用していない	無線WiFiからの脅威の侵入はない
②	工場敷地外に電波が漏れないように出力や設置場所などを調整している	敷地外からの第三者の不正アクセスを防ぐ
③	無線接続できる端末を制限している	特定の端末のみの接続に制限することで、不正アクセスを防ぐ
④	端末接続にはできるだけ安全な方式を使用し、第三者による不正接続や盗聴ができないように無線機（無線AP）を設定している	暗号化や認証方式の強度を高めることで不正アクセスの可能性を低減できる
⑤	無線機（無線AP)のログを定期的にチェックし、不審な接続がないかを確認している	装置ログや通信ログを分析して、意図しないアクセスの有無を確認し、不正アクセスを検知する

※ルールは徹底され、適切に運用されていることが前提

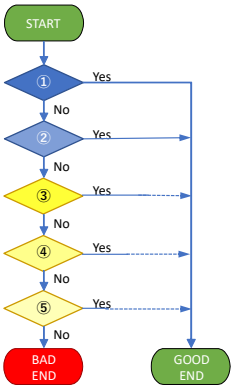
【補足】

- 通信速度が遅くなった原因は、Wi-Fi が第三者に無断で使用されていることによるものです。
- 製造現場 LAN に無線 AP を接続している場合、第 3 者の無線 AP への電波妨害や許可していない無線端末の不正な接続により、無線 AP の動作が停止、不安定となり、生産活動を妨害される場合もあります。
- 電波の届く距離内に、不正な端末を持ち込ませないことで Wi-Fi を保護することができます。ただし、強度な妨害電波による支障（意図的な攻撃だけではなく、周辺環境が原因の場合もあります）については防御が困難なため、妨害リスクの低減ではなく、無線をやめて有線にする、別の電波帯を使用する方式に変えるなどの根本的な見直しが必要です。
- ③の方法として、EAP-TLS（デジタル証明書による認証。証明書を持っているもののみが接続を許可される）や、MAC アドレスフィルタリング（装置固有の MAC アドレスで接続を許可する端末を識別する）などがあります。
- ④については、できるだけ最新の認証方式と暗号化方式を選択するのが望ましいです。

MEMO

(10)保守用回線

保守用回線経由で工場ネットワークへ侵入され、複数の工場内製造装置の動作に異常が発生した



	現状の対策状況	対策の効果等
①	保守用回線はない（接続していない）	保守用回線経由での脅威に侵入はない
②	保守作業でアクセスする製造設備や制御システムには、ウイルス対策ソフトが導入されている	保守用回線経由でマルウェアが侵入しても検知することができる
③	保守用回線から工場内部へのアクセスは、特定の端末からのみ許可するように設定している	特定の端末のみの接続に制限することで、マルウェアの侵入リスクを低減できる（保守業者が使用する端末にセキュリティ対策が実施されていることが前提）
④	保守用回線から工場内部へのアクセスは、特定の装置へのみ許可するように設定している	保守用回線経由で工場内の装置に自由にアクセスできること防御できる（被害の最小化）
⑤	保守用回線から工場内部への通信をモニタリングしている	装置ログや通信ログを分析して、何らかのマルウェアが原因であることが判明すれば、適切な応急・復旧処置ができる

※ルールは徹底され、適切に運用されていることが前提

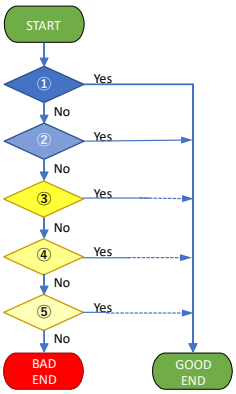
【補足】

- 製造装置の異常の原因は、保守用回線を経由して侵入したマルウェアや意図的な不正アクセスなどによるものです。
- 保守用回線は、工場内の制御システムや製造装置を遠隔でメンテナンスするために機器ベンダーなどが用意するケースが多く、どのような仕組みになっているかをしっかりと把握しておく必要があります。
- ③の方法としては、保守業者が使用する特定の端末にソフトウェアを導入し、工場側と専用の通信チャネルでのみ接続を許可するなどが考えられます。
- ④の方法としては、ネットワーク機器の設定により、保守用回線経由での通信の行先を制限するなどが考えられます。
- ⑤の「モニタリング」とは、工場内への通信の内容を専用の仕組みで見張ることです。マルウェアの拡散や不正なアクセスの有無を見張ることで、異常に対して適切に対処することができます。

MEMO

(11)クラウドサービス

生産の効率化を図るために、製造情報分析のクラウドサービス活用を始めたが、情報が漏えいしていると第三者から連絡を受けた（クラウドサービス側からの漏えいはないとの回答）



	現状の対策状況	対策の効果等
①	クラウドサービスを利用していない	クラウドサービス経由で情報が漏洩することはない
②	クラウドサービスへのアクセス方法を制限している	社外の第三者がアクセスすることが難しくなる
③	クラウドサービスにログインする際の認証方式に多要素認証を利用している	正規ユーザ以外の第三者がアクセスすることが難しくなる
④	クラウドサービスにログインするID・パスワードは、他のサービスで利用していないもの、かつ複雑なものを利用している	正規ユーザのID/パスワードを入手しないかぎり、第三者がアクセスすることが難しくなる
⑤	クラウドサービスへのアクセスログを定期的に確認している	不要な利用履歴の有無を確認し、不正アクセスの兆候がある場合には、対処を行うことができる

※ルールは徹底され、適切に運用されていることが前提

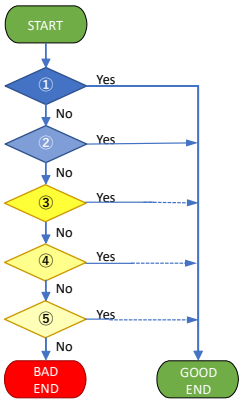
【補足】

- 情報漏洩の原因は、クラウドサービスを利用するための認証情報（ID/パスワード）の管理が不十分で、外部に漏れたか推測されたかによって不正にアクセスされたことによるものです。
- 第三者が認証情報を取得する方法としては、初期パスワードのまま運用、単純なパスワードによる運用、他サイトでの認証情報の使いまわしなどが挙げられます。
- ②の「アクセス方法の制限」の一例として、クラウドサービスによっては、サービスにアクセスできるネットワークを指定して、アクセス元を制限することができるようなことが挙げられます。
- ③のように、多要素認証（端末認証など複数の認証の仕組みを利用すること）で、不正アクセスのリスクが下がります。
- ④のように、ID・パスワードが外部に流出していたり、簡易な ID・パスワードを利用している場合は、第三者が不正にログインしやすい状態といえます。
- ⑤のログ確認では、同時期に連続したアクセスや大量のデータダウンロードがないかを確認し、すでに発生している場合は、対処を行う必要があります。

MEMO

(12)部品・原材料

コスト削減のため、組み込みの制御モジュール部品の調達先を変更したところ、当社の出荷製品のトラブルが急激に増加した



	現状の対策状況	対策の効果等
①	部品の不具合情報の提供を受ける仕組みがある	情報セキュリティに関する脆弱性を含んだ情報を早期に受け取る仕組みは、トラブルを未然に防ぐことにつながる
②	購入した部品に対して、情報セキュリティに関するテストを行う体制がある	新しい部品を調達した際、テストを行うことにより、トラブルを回避できる
③	製品の構成要素の脆弱性情報を収集している	日々、関連する脆弱性情報を収集し、早期に対応により被害を最小限に抑えることができる
④	情報セキュリティに関するトラブル対策を行う部門がある	製品出荷後の速やかな改修により、被害を最小限に抑えることができる
⑤	製品の不具合情報を公表する手順が確立している	情報セキュリティに関連する不具合情報を公開することで、被害を最小限に抑えることができる

※ルールは徹底され、適切に運用されていることが前提

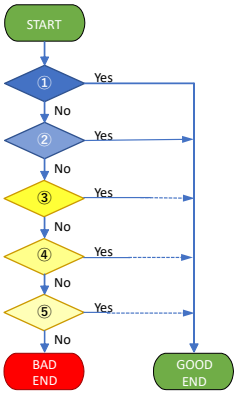
【補足】

- トラブル急増の原因は、調達した制御モジュール部品に情報セキュリティに関する脆弱性があり、これを悪用した不正アクセスによるものです。
- 高度なプログラムを含む電子回路などのモジュールには、情報セキュリティに関する脆弱性が残存している可能性があります。これを製品に組み込んだ場合、出荷後に何らかのトラブルになるケースも考えられます。
- ①③のように部品に関する脆弱性情報をタイムリーに入手することは、その後の対応にとって非常に重要になります。
- ②④のように専門の組織を持つことが望ましいですが、人材やスキルなどの面で難しい場合は、外部に委託するなども有効な手段です。
- 出荷した製品に情報セキュリティに関する脆弱性が含まれていることが判明した場合、速やかに経緯や対応方法を公開する必要があります。

MEMO

(13)新規購入機器

製造装置の老朽化に伴い、新しい装置を導入したところ、他の装置でのトラブルが増加し生産効率が悪化した（新製造装置の仕様は入れ替え前の装置と完全互換）



現状の対策状況		対策の効果等
①	新製造装置のネットワーク接続はない	既存環境には影響はない
②	装置メーカーが出荷時にマルウェアが入り込んでいないかをチェックしている。もしくは受け入れ時に工場側でチェックをしている	新製造装置から既存環境へ脅威を持ち込まない
③	既存製造装置にマルウェア対策を導入している	既存製造装置側でマルウェア感染が防げる
④	製造現場LANの通信内容をモニタリングしている	マルウェアの感染拡大の動きを検知して、蔓延する前に対処することができる
⑤	製造装置の動作不良の原因調査にはセキュリティ観点も加えている	装置ログや通信ログを分析して、何らかのマルウェアが原因であることが判明すれば、適切な応急・復旧処置ができる

※ルールは徹底され、適切に運用されていることが前提

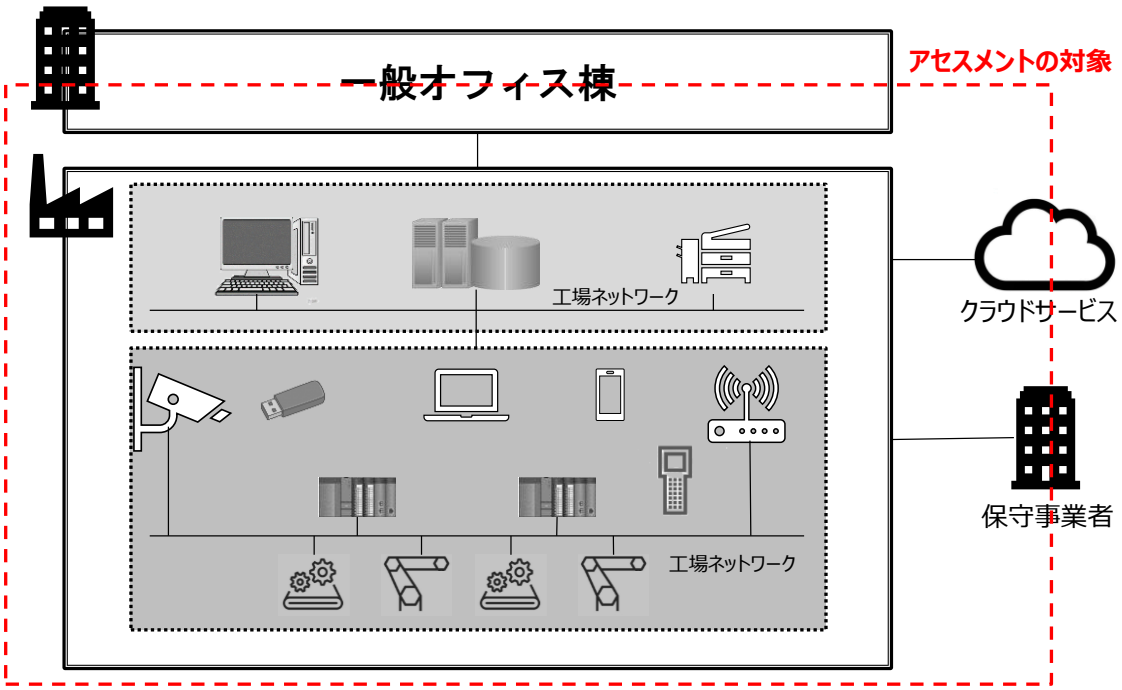
【補足】

- 他の装置でトラブルが増加した原因は、新しく導入した装置にマルウェアが混入していて、ここから感染が広がり、その他製造装置も感染してしまったことによるものです。
- 製造装置がマルウェアに感染した場合、その影響で装置の動作が不安定になったり、意図的に必要なファイルが暗号化され、動作ができなくなったり、装置内の情報を外部に送信されたりする被害が発生する可能性があります。
- 特に暗号化されるケースでは、暗号化を解除する代償に金銭を要求するランサムウェアと呼ばれるマルウェアの被害が多くなっています。（金銭を払っても解除される保証はありません）
- 情報の窃取が目的のマルウェアに感染した場合は、装置の動作に大きな変化が現れないこともあります。
- ④の「モニタリング」とは、工場内の通信の内容を専用の仕組みで見張ることです。マルウェアが拡散時に行う特有の通信の有無を見張ることで、マルウェアの存在を検知することができます。
- ⑤の「セキュリティ観点を加える」とは、機械的な故障ではなく、マルウェア感染などが原因であることを調査するための手順やツールを準備することです。

MEMO

4．付録

4．1　アセスメント対象の俯瞰図



4．2　用語集

【製造装置】
　工場内で稼働している製造に関わるすべての装置

【製造現場 LAN】
　工場内に設置された Ethernet ベースの有線ネットワークおよび Wi-Fi ベースの無線ネットワーク
　工場ネットワーク、OT ネットワークとも呼ばれる

【機密性(Confidentiality) 】
　許可されていない個人、グループ、組織、システムに対して、情報を使用不可又は非公開にする特性

【完全性(Integrity) 】
　情報資産の正確さ及び完全さを保護する特性

【可用性(Availability) 】
　許可された個人、グループ、組織、システムが要求したときに、アクセス及び使用が可能である特性

【脅威(Threat) 】

情報資産（装置などのハードウェアも含む）の機密性、完全性、可用性に危害を与える原因となる事象で、人為的(意図的、作為的)なものと環境的(地震、落雷など)なものに分類される

【脆弱性(Vulnerability) 】

脅威によって利用されるおそれのある弱点

【リスク】

情報セキュリティにおけるリスクとは、情報システムとそのデータやその他の様々な情報資産に損害や悪影響を与える可能性のこと。

リスクの大きさ ＝ 資産の価値 × 脅威の程度 × 脆弱性の程度

で表されることが多い。

【リスクアセスメント】

情報セキュリティに関係するリスクを洗い出し、これを分析してその大きさなどを評価すること。リスクに対する対処を含めてリスクマネジメントと呼ぶ。

【マルウェア】

マルウェア（malware）とは、不正かつ有害に動作させる意図で作成された、悪意のあるソフトウェアや悪質なコードの総称。コンピュータウイルスやワーム、トロイの木馬などが含まれる。特にワームは単独で感染を広げ、悪質なものが多い。

【ランサムウェア】

ランサムウェアとは、身代金（Ransom）とソフトウェアを組み合わせた造語。暗号化などによってファイルを利用不可能な状態にし、そのファイルを元に戻すことと引き換えに金銭を要求するマルウェアのこと。最近では、窃取した情報の公開を身代金取引に使うケースもある。

【ファイアウォール】

ファイアウォールとは、ネットワークの通信において、その通信を許可するか拒否するかを判断する機能をもつもの。専用のハードウェアや PC 上のアプリケーションなどがある。

【セキュリティパッチ】

セキュリティパッチとは、情報システムの脆弱性（欠陥）を修正するためのプログラムのこと。新たに脆弱性が発見されると、そのシステムの提供ベンダーからインターネット等で配布される。

【Wi-Fi（無線 AP）】

Wi-Fi とは、国際標準規格である IEEE 802.11 規格を使用したデバイス間で相互接続ができる無線 LAN に認められた名称。無線 AP は、この規格に準拠した装置で、無線通信を中継したり有線通信の機器に接続したりするもの。AP は「アクセスポイント」の略

【デジタル証明書】

デジタル証明書とは、インターネットの世界で持ち主の情報を正しく証明するためのデータで、現実世界における身分証明書（パスポート、印鑑証明書、運転免許証など）に相当する。デジタル証明書は、認証局と呼ばれる信頼できる第三者機関が発行する。

【MAC アドレス】

MAC アドレスとは、ネットワーク機器やネットワークアダプター（LAN カードなど）に割り当てられるユニークな識別番号のこと。世界中で MAC アドレスは重複しない。一般的に 12 けたの 16 進数で表され、前半の 6 桁がその製品のメーカー固有の数値になっている。

WG メンバー

青木　茂　（協力者）
秋山　健一（日本電気株式会社）
家富　和寿（NEC プラットフォーム株式会社）
井上　陽一（JNSA フェロー）
今西　幸一（株式会社インターネットイニシアティブ）
沖　裕之　（株式会社ソリトンシステムズ）
大財　健治（協力者／ケー・コンサルタント）
岡本　登　（WG リーダー／富士通株式会社）
金子　啓子（JNSA 顧問）
兼子　竜也（ニュートラル株式会社）
河島　君知（エヌ・ティ・ティ・データ先端技術株式会社）
小柴　宏記（ジーブレイン株式会社）
近藤　伸明（株式会社神戸デジタル・ラボ）
塩田　廣美（協力者）
嶋倉　文裕（富士通株式会社）
田野　久敏（ONWARD SECURITY JAPAN 株式会社）
西川　和予（協力者／プライムコンサルティング）
橋本　護　（株式会社さくらケーシーエス）
古川　佳和（大阪商工会議所）
峯浦　梨紗（富士通株式会社）
元持　哲郎（JNSA 西日本支部長／アイネット・システムズ株式会社）
山口　直樹（富士通株式会社）
吉崎　大輔（日本電気株式会社）
米澤　美奈（株式会社ソリトンシステムズ）

敬称略・五十音順