



異常調査

【行動】

現場



情報カード①を引く。

工場の製造に利用されているすべてのシステムの運転状況を確認

条件：情報カード①

またどこかで不具合が発生したのかな・・・。



CYBER
SECURITY
COMMUNICATION

【行動①】

②再起動の指示

【行動】

工場長



情報カード②を引く。

不具合が発生しているシステムの再起動を現場担当に指示する。

条件：情報カード①

再起動すれば直るだろう・・・。



CYBER
SECURITY
COMMUNICATION

【行動②】

③

システム 再起動

【行動】

現場



情報カード③を引く。

原料システムの再起動を
実施

マニュアルの通りに慎重に・・・。



CYBER
SECURITY
COMMUNICATION

【行動③】

④

不具合調査 指示

【行動】

工場長



情報カード④を引く。

現場担当にシステムの不
具合調査を指示する
条件：情報カード③

また不具合が発生したのか・・・。



CYBER
SECURITY
COMMUNICATION

【行動④】

⑤

システム 不具合調査

【行動】

現場



情報カード⑤を引く。

原料システムにシステム
面での不具合が発生して
いないか調査
条件：情報カード④

この前も調査したばかりだけど・・・。



CYBER
SECURITY
COMMUNICATION

【行動⑤】

⑥

サイバー観点 調査依頼

【行動】

CSIRT



情報カード⑥を引く。

工場長にサイバー攻撃の
観点を含めた調査を依頼
する。

条件：情報カード⑤

前に同じ事象が発生した際に共有
してほしかった・・・。



CYBER
SECURITY
COMMUNICATION

【行動⑥】

⑦

ITシステム 調査依頼

【行動】

CSIRT



情報カード⑦を引く。

SOC(Security Operation Center)等のセキュリティ部隊に状況を確認し、IT部門に不具合調査を依頼
条件:情報カード⑤

ITは何事も無くあってくれ・・・。



CYBER
SECURITY
COMMUNICATION

【行動⑦】

⑧

ITシステムの 不具合調査

【行動】

IT
部門



情報カード⑧を引く。

ITシステムで利用している
各システムで不具合の
発生状況を調査する。
条件：情報カード⑦

特に問題はないはず・・・。



CYBER
SECURITY
COMMUNICATION

【行動⑧】

⑨

復旧作業 依頼

【行動】

CSIRT



情報カード⑨を引く。

異常が発生しているシステムの再起動およびバックアップからの復旧を依頼
条件: 情報カード⑧

異常発生していたのか・・・。



CYBER
SECURITY
COMMUNICATION

【行動⑨】

10

システム 復旧作業

【行動】

IT
部門



情報カード⑩を引く。

異常が見つかったシステムの再起動およびバックアップからの復旧作業を実施する。

条件: 情報カード⑨

これで問題なく直るはず・・・。



CYBER
SECURITY
COMMUNICATION

【行動⑩】



サイバー観点 調査指示

【行動】

工場長



情報カード⑪を引く。

サイバーの観点で、工場のシステムに異常が無いか、現場担当へ確認を指示。
条件：情報カード⑥

事前に共有はしてるけど・・・。



CYBER
SECURITY
COMMUNICATION

【行動①①】

12

システム 異常調査

【行動】

現場



情報カード⑫を引く。

サイバー観点でシステムの
異常を調査。

条件：情報カード⑪

サイバー攻撃ではないでしょ・・・。



CYBER
SECURITY
COMMUNICATION

【行動⑫】

⑬

サイバー攻撃 と判断

【行動】

CSIRT



情報カード⑬引く。

今回の事象をサイバー攻撃と判断し、CSIRTメンバーを工場に派遣。

条件：情報カード⑩, ⑫

まさか自社で発生するとは・・・



CYBER
SECURITY
COMMUNICATION

【行動⑬】

⑭ 経営層へ報告 (特別体制上申)

【行動】

CSIRT



情報カード⑭を引く。

経営層に現状の報告および特別体制の立ち上げを上申する。

条件：情報カード⑩, ⑫

経営層に怒られないといいが…。



CYBER
SECURITY
COMMUNICATION

【行動⑭】

15

支援依頼

【行動⑮】

CSIRT



情報カード⑮を引く。

顧客影響が発生した場合に備えて、対外対応(プレス等)の準備をバックオフィスに依頼する。

条件: 情報カード⑭

プレスにならなければいいが...



CYBER
SECURITY
COMMUNICATION

【行動⑮】

16

プレス準備

【行動①⑥】

オフィス
バック



情報カード①⑥を引く。

サイバー攻撃に関する情報収集およびプレス準備を開始。

条件：情報カード①⑤

サイバーのプレスって何するの・・・。



CYBER
SECURITY
COMMUNICATION

【行動①⑥】

17

復旧プラン 実施指示

【行動】

工場長



情報カード⑰を引く。

復旧プラン実施を意思決定し、現場担当に復旧プランを駆け付けたCSIRTと一緒に実施を指示する。

条件：情報カード⑬

予定通りに実施すれば大丈夫だろ。



CYBER
SECURITY
COMMUNICATION

【行動⑰】

18

復旧プラン 実施

【行動】

現場



情報カード⑱を引く。

現場に駆け付けたCSIRT
と共にシステムの復旧プ
ランを実施
条件：情報カード⑰

直ってくれ・・・。



CYBER
SECURITY
COMMUNICATION

【行動⑱】

19

異常調査

【行動】

CSIRT



情報カード⑱を引く。

工場に駆け付けている
CSIRTが工場他端末
の異常を調査
条件：情報カード⑱

手当たり次第原因を探すしかない。



CYBER
SECURITY
COMMUNICATION

【行動①⑨】

20

工場全停止 決定

【行動】

工場長



情報カード⑳を引く。

工場の全停止を判断し、
経営層に上申したうえで
現場担当に指示する。

条件：情報カード⑱

全停止は避けたかったが、やむなし
か・・・。



CYBER
SECURITY
COMMUNICATION

【行動②〇】

②①

工場全停止

【行動】

現場



情報カード②①を引く。

工場を全停止させる。
条件：情報カード②①

後で責任取らされるのかな・・・。



CYBER
SECURITY
COMMUNICATION

【行動②】

②② 外部機関報告

【行動】

オフィス
バック



情報カード②②を引く。

監督官庁に事態を報告する。

条件：情報カード②①

問合せ来たら答えられない・・・。



CYBER
SECURITY
COMMUNICATION

【行動②②】

②③ プレス実施

【行動】

オフィス
バック



情報カード②③を引く。

経営層の承認を得て、
顧客向けのプレスを会社
ホームページに掲載
条件：情報カード②①

どこまで公表しよう・・・。



CYBER
SECURITY
COMMUNICATION

【行動②③】

24

問合せ 窓口設置

【行動】

オフィス
バック



情報カード②④を引く。

問合せ用のコールセンタ
ー窓口を開設
条件:情報カード②④

誰も答えられないぞ・・・。



CYBER
SECURITY
COMMUNICATION

【行動②④】

25

封じ込め 計画作成

【行動】

CSIRT



情報カード②⑤を引く。

封じ込めを実施するための
計画作成し、経営層
に上申する。

条件：情報カード②①

被害が広がらないように・・・。



CYBER
SECURITY
COMMUNICATION

【行動②⑤】

26

ネットワーク
切り離し

【行動】

CSIRT



情報カード②⑥を引く。

封じ込め対応(IT/OTの境
界を切り離し)を実施する
条件: 情報カード②①, ②⑤

何が何でも封じ込めしないと・・・。



CYBER
SECURITY
COMMUNICATION

【行動②⑥】

②⑦ 封じ込め依頼

【行動】

CSIRT



情報カード②⑦を引く。

封じ込めのためのITシステム側の調査を依頼
条件：情報カード②①、②⑤

何としても封じ込めしないと・・・。



CYBER
SECURITY
COMMUNICATION

【行動②⑦】

②⑧ 封じ込め対応

【行動】

IT
部門



情報カード②⑧を引く。

封じ込め対応(ネットワーク機器の調査)を実施する
条件: 情報カード②⑦

何としても封じ込めしないと・・・。



CYBER
SECURITY
COMMUNICATION

【行動②⑧】

②⑨ 封じ込め対応

【行動】

IT
部門



情報カード②⑨を引く。

資産管理外の端末を物理
的に調査

条件：情報カード②⑧

管理外の端末なんてあるはずない
が・・・。



CYBER
SECURITY
COMMUNICATION

【行動②⑨】

30

システム 再復旧依頼

【行動】

CSIRT



情報カード③⑩を引く。

被害が発生しているシステムをバックアップデータから復旧を再度依頼
条件：情報カード②⑨

今度こそ復旧できるはず・・・。



CYBER
SECURITY
COMMUNICATION

【行動③〇】

31

システム 復旧

【行動】

IT
部門



情報カード③①を引く。

利用できないシステムに
ついて再度バックアップデ
ータから復旧を実施
条件：情報カード③①

何とかこれで戻ってくれ・・・。



CYBER
SECURITY
COMMUNICATION

【行動③】

③②

復旧プラン 再実行依頼

【行動】

CSIRT



情報カード③②を引く。

他システムも含めて工場
長に再度の復旧プラン実
施を依頼する。

条件：情報カード②⑨、③①

工場も復旧できるはず・・・。



CYBER
SECURITY
COMMUNICATION

【行動③②】

③③ システム復旧

【行動】

工場長



情報カード③②を引く。

再度の復旧プラン実施を
指示

条件：情報カード③②

今回こそは戻ってくれ……。



CYBER
SECURITY
COMMUNICATION

【行動③③】

③4

復旧プラン 再実施

【行動】

現場



情報カード③4を引く。

停止しているシステムに対して復旧プランを再度実施

条件：情報カード③3

何とかこれで戻ってくれ・・・。



CYBER
SECURITY
COMMUNICATION

【行動³⁴】

③⑤ 工場再立ち上げ 指示

【行動】

工場長



情報カード③⑤を引く。

システムの復旧が完了し、
経営層から工場の再立ち
上げを承認を得て、現場
担当に指示する。

条件：情報カード③④

工場も復旧できるはず・・・。



CYBER
SECURITY
COMMUNICATION

【行動③⑤】

③⑥

工場 再立ち上げ

【行動】

現場



情報カード③⑥を引く。

工場全体の再立ち上げを
実施

条件：情報カード③⑤

早く元通りになってくれ・・・。



CYBER
SECURITY
COMMUNICATION

【行動³⁶】

③⑦ 工場復旧目途 報告

【行動】

工場長



情報カード③⑦を引く。

工場の復旧目途が立ち、2
日後には生産が再開する
ことを経営層に報告する。
条件：情報カード③⑥

2日の停止で済んでよかった・・・。



CYBER
SECURITY
COMMUNICATION

【行動³⁷】

38

外部機関 報告

【行動】

オフィス
バック



情報カード③⑧を引く。

監督官庁に状況を報告する

条件：情報カード③⑦

何とかになって良かった・・・。



CYBER
SECURITY
COMMUNICATION

【行動³⁸】

③⑨ プレス実施

【行動】

オフィス
バック



情報カード③⑨を引く。

再度プレスをホームページに記載。

条件：情報カード③⑦

思ったより問合せは少なかったな。



CYBER
SECURITY
COMMUNICATION

【行動³⁹】

④0

体制解散 上申

【行動】

CSIRT



情報カード④0を引く。

応急対応(プレスや外部機関報告含む)が完了し、特別体制の解散を上申
条件:情報カード③7,③8,③9

とりあえず一息つけるぞ・・・。



CYBER
SECURITY
COMMUNICATION

【行動④〇】



情報共有

【行動】

工場長



テーブル中央に情報カードを置く

情報を全体に共有する。
(共有すべき情報カードを
任意の枚数選ぶ。)

皆が知りたい情報ってなんだ・・・!



CYBER
SECURITY
COMMUNICATION

【行動①】



情報共有

【行動】

CSIRT



テーブル中央に情報カードを置く

情報を全体に共有する。
(共有すべき情報カードを
任意の枚数選ぶ。)

皆が知りたい情報ってなんだ・・・!



CYBER
SECURITY
COMMUNICATION

【行動①】



情報共有

【行動】

二
部
門



テーブル中央に情報カードを置く

情報を全体に共有する。
(共有すべき情報カードを
任意の枚数選ぶ。)

皆が知りたい情報ってなんだ・・・!



CYBER
SECURITY
COMMUNICATION

【行動①】



情報共有

【行動】



テーブル中央に情報カードを置く

情報を全体に共有する。
(共有すべき情報カードを
任意の枚数選ぶ。)

皆が知りたい情報ってなんだ・・・！



CYBER
SECURITY
COMMUNICATION

【行動①】