



停止システム 発見

【情報】



上流の原料システムが停止していることを発見。

(他工程は問題なく、半日は製造継続可能。)

本来なら個別アラートが発報するはずなんだけどな・・・。



CYBER
SECURITY
COMMUNICATION

【情報①】

② 再起動指示

【情報】



このカードは**現場担当**に渡す。

不具合が発生している原料システムの再起動指示がでた。

この前も同じようなことがあったな。



CYBER
SECURITY
COMMUNICATION

【情報②】

③

システム 再起動失敗

【情報】



原料システムの再起動に
失敗し、復旧することがで
きない。

マニュアルの通りに実施したんだけ
どな・・・。



CYBER
SECURITY
COMMUNICATION

【情報③】

④ システム不具合 調査指示

【情報】



このカードは**現場担当**に渡す。

不具合が発生している原料システムの調査の指示がでた。

設備故障はしてなさそうだが・・・。



CYBER
SECURITY
COMMUNICATION

【情報④】

⑤

システム
異常なし

【情報】



原料システムに不具合を
発見できなかった。

システムベンダーに確認
するも原因不明であった。

サイバー攻撃の可能性も・・・？



CYBER
SECURITY
COMMUNICATION

【情報⑤】

⑥

調査方法

【情報】



このカードは**工場長**に渡す。

制御システムへのサイ
バー攻撃の観点でチェッ
クすべき項目。

どうせちょっとした不具合だろ・・・。



CYBER
SECURITY
COMMUNICATION

【情報⑥】

⑦

調査依頼

【情報】



このカードは**IT部門**に渡す。

ITシステムに影響が出て
いないか調査を依頼。

SOCから「IT/OT境界の
通信量が増加」と報告有。

IT側を巻き込まないでくれよ・・・。



CYBER
SECURITY
COMMUNICATION

【情報⑦】

⑧

調査結果

【情報】



ITシステムについて調査した結果、会計システムに異常が発生し使用できないことを発見。

利用者にも連絡しなきゃ・・・。



CYBER
SECURITY
COMMUNICATION

【情報⑧】

⑨

復旧作業 依頼

【情報】



このカードは**IT部門**に渡す。

異常が発生している会計
システムの再起動および
バックアップからの復旧作
業を依頼。

大事にならなければいいが・・・。



CYBER
SECURITY
COMMUNICATION

【情報⑨】

10

システム 復旧失敗

【情報】



会計システムの再起動や
バックアップからの復旧を
実施しても異常は解消せ
ず。

どうして直らないんだ・・・。



CYBER
SECURITY
COMMUNICATION

【情報⑩】



調査方法

【情報】



このカードは**現場担当**に渡す。

制御システムへのサイ
バー攻撃の観点でチェッ
クすべき項目。

サイバー攻撃なんて起こるのか。



CYBER
SECURITY
COMMUNICATION

【情報①①】

12

調査結果

【情報】



原料システムのファイルを確認したところ、暗号化されていることが判明。

これは・・・サイバー攻撃かも・・・。



CYBER
SECURITY
COMMUNICATION

【情報⑫】

⑬

CSIRTメンバー 派遣

【情報】



このカードは**工場長**に渡す。

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。

とにかく状況把握と対応を急ごう。



CYBER
SECURITY
COMMUNICATION

【情報⑬】

14

特別体制 立ち上げ承認

【情報】



このカードは**テーブル上**に出す。

特別体制立ち上げが承認。
危機対策会議が開催され、
現在CSIRTが保有する
**すべての情報カードを全
員に共有。**

今までの事象を共有しよう。



CYBER
SECURITY
COMMUNICATION

【情報⑭】

15

対外報告 準備依頼

【情報】



このカードは**バックオフィス**に渡す。

サイバー攻撃により顧客
影響が発生した場合に備
えて、事前に対外報告の
準備を依頼される。

サイバー攻撃でもプレスするのか。



CYBER
SECURITY
COMMUNICATION

【情報⑮】

16

対外報告 準備を開始

【情報】



対外対応に向けた準備を開始(顧客影響が発生した場合、対外報告を実施する)。

サイバーと公開するか否か・・・。



CYBER
SECURITY
COMMUNICATION

【情報①⑥】

17

復旧プラン 実施指示

【情報】



このカードは**現場担当**に渡す。

復旧プランの実施を指示
される。

CSIRTのサポートが必要だな・・・。



CYBER
SECURITY
COMMUNICATION

【情報⑰】

18

復旧プラン 失敗

【情報】



復旧プランを実施するも、
復旧できなかった。

復旧できなかった…どうしよう。



CYBER
SECURITY
COMMUNICATION

【情報⑱】

19

暗号化端末 発見

【情報】



他システムでも暗号化され、安全が担保できない状態であることが判明。

ここも暗号化されてる…どうしよう。



CYBER
SECURITY
COMMUNICATION

【情報①⑨】

20

工場全停止 指示

【情報】



経営層から承認を得て工場の全停止が指示される。復旧に必要な期間は最低2日を見込む。

丸2日停止…損害額はいくらだ…。



CYBER
SECURITY
COMMUNICATION

【情報②〇】

21

工場全停止

【情報】



工場を全停止した。停止
期間は最低2日を見込み
顧客影響が発生する。

被害を抑えるためには身を切る覚
悟が必要だ・・・。



CYBER
SECURITY
COMMUNICATION

【情報②】

22

報告完了

【情報】



監督官庁向けの報告が完了。

原因究明するように釘を刺された…。



CYBER
SECURITY
COMMUNICATION

【情報②②】

23

顧客向け プレス掲載

【情報】



本事象に関して顧客向けの
プレスをホームページに
掲載。但し、サイバー攻撃
起因であることは伏せた。

問合せが無いといいが・・・。



CYBER
SECURITY
COMMUNICATION

【情報②③】

24

対応窓口 設置

【情報】



専用の問合わせ対応窓口
の設置が完了。サイバー
攻撃起因であることは伏
せて回答する方針。

誠実にお客様対応をしなければ…。



CYBER
SECURITY
COMMUNICATION

【情報②④】

25

封じ込め 計画承認

【情報】



作成した封じ込め計画が
経営層に承認された。

今度こそ封じ込めして復旧へ。



CYBER
SECURITY
COMMUNICATION

【情報②⑤】

26

ネットワーク 切り離し

【情報】



被害の封じ込めのために行った境界FWの切り離しが完了。

切り離したし被害拡大しないはず
…。



CYBER
SECURITY
COMMUNICATION

【情報②⑥】

27

封じ込め 依頼

【情報】



このカードは**IT部門**に渡す。

封じ込めのため、ITシステム側の調査を依頼される。

どこから侵入されているんだ・・・。



CYBER
SECURITY
COMMUNICATION

【情報②⑦】

28

外部通信 確認

【情報】



資産管理台帳に存在していない端末から外部通信がされていること確認。

こんな端末知らないぞ…。



CYBER
SECURITY
COMMUNICATION

【情報②⑧】

29

管理外端末 発見・隔離

【情報】



サーバルームに資産台帳
に記載されていない端末
を発見したため、ネット
ワークから隔離。

本当にあった・・・隔離しておこう。



CYBER
SECURITY
COMMUNICATION

【情報②⑨】

30

システム 再復旧依頼

【情報】



このカードは**IT部門**に渡す。

会計システムをバックアップデータを用いて再度復旧を試すように依頼。

これで復旧できるといいけど・・・。



CYBER
SECURITY
COMMUNICATION

【情報③〇】

31

会計システム 復旧

【情報】



バックアップデータを利用して会計システムを復旧することに成功。

やっと戻ったぞ…。



CYBER
SECURITY
COMMUNICATION

【情報③】

③2

復旧プラン 再実行依頼

【情報】



このカードは**工場長**に渡す。

原料システムおよび他システムに対して再度復旧プランの実行を依頼。

これで復旧できるといいけど・・・。



CYBER
SECURITY
COMMUNICATION

【情報③②】

③③

復旧プラン 再実行指示

【情報】



このカードは**現場担当**に渡す。

原料システムおよび他シ
ステムに対して再度復旧
プランの実行を指示

今度こそ復旧してくれ…。



CYBER
SECURITY
COMMUNICATION

【情報③③】

③4

復旧プラン
成功

【情報】



復旧プランが成功し、原料システムを含めたすべてのシステムの再起動が可能に。

もう一度リベンジだ…。



CYBER
SECURITY
COMMUNICATION

【情報③④】

③⑤ 工場再立ち上げ 指示

【情報】



経営層に承認された工場
の再立ち上げについて、指
示がでる。

何とか解決したみたいだな・・・。



CYBER
SECURITY
COMMUNICATION

【情報③⑤】

③⑥ 工場再立ち上げ 開始

【情報】



工場の再立ち上げを開始。
停止期間により温度が低下していたため、操業再開は2日後を予定。

なんとかここまで辿り着いた…。



CYBER
SECURITY
COMMUNICATION

【情報③⑥】

③7

報告指示

【情報】



このカードは**テーブル上**に出す。

工場の再立ち上げ瓦解したため、経営層から各所への報告を指示される。

お客さま第一に考えるように・・・。



CYBER
SECURITY
COMMUNICATION

【情報③⑦】

③⑧ 報告完了②

【情報】



工場の再稼働見込みについて、監督官庁向けの報告が完了。

再開の見込みが立ってよかった…。



CYBER
SECURITY
COMMUNICATION

【情報③⑧】

39

顧客向け
プレス掲載②

【情報】



工場の復旧目途が立ち、2
日後には生産再開するこ
とを顧客向けプレスとして
ホームページに掲載。

本当に良かった・・・。



CYBER
SECURITY
COMMUNICATION

【情報③⑨】

④0

特別体制 解散

【情報】



本インシデントに係る特別体制の解散が承認される。無事インシデント対応を乗り切ることができました。

本当は再発防止策も検討が必要。



CYBER
SECURITY
COMMUNICATION

【情報④〇】

① アラート発生

【情報】



このカードは**現場担当**に渡す。

工場に異常を表す緊急アラートが鳴り響きました。
工場長は現場担当に状況確認を指示しました。



CYBER
SECURITY
COMMUNICATION

【情報①】