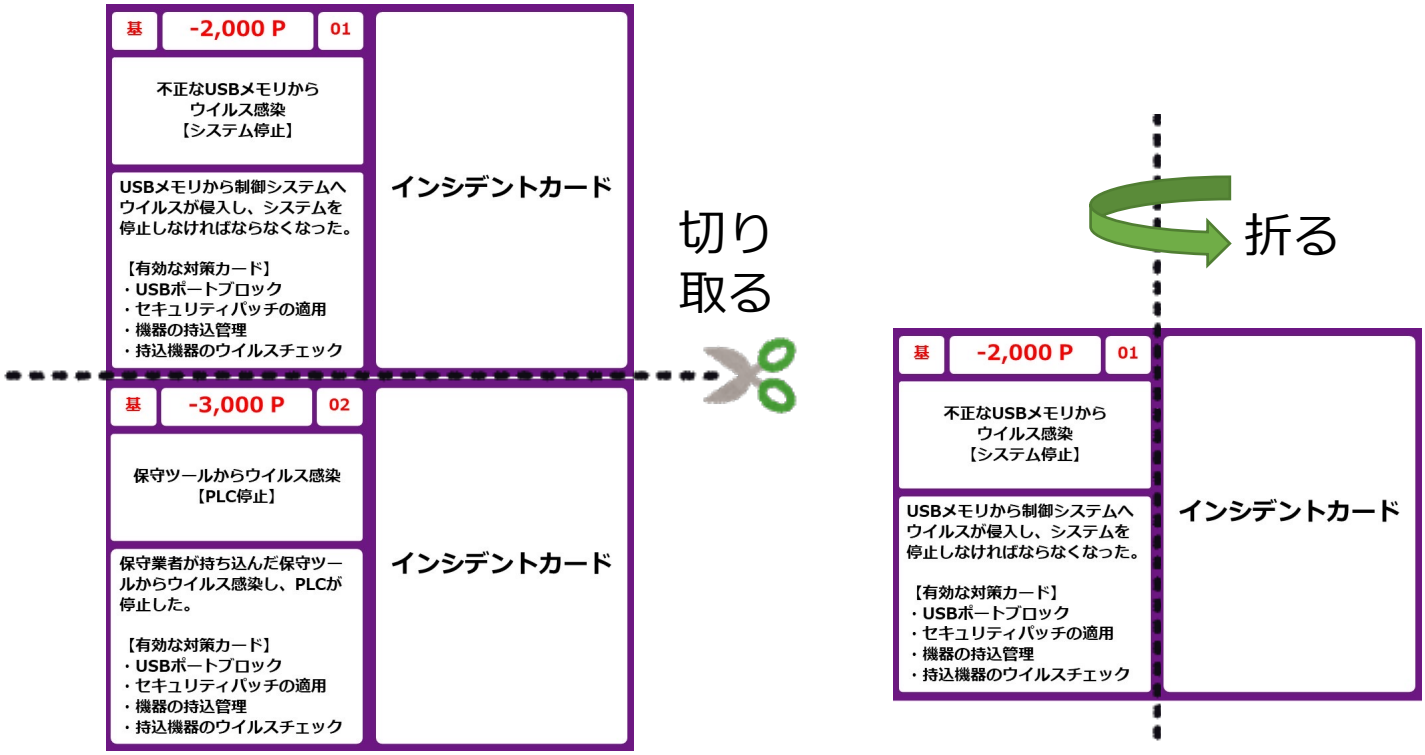
インシデントカード
基礎編

インシデント（サイバー攻撃やうっかりミス等によって引き起こされる好ましくない出来事）が発生し、ポイントが減るカードの基礎編です。
インシデントカードは全部で７枚あります。

初めてセキュリティ道場をプレイする場合は、
基礎編のインシデントカードを使用してください。

上下で切り取り、左右で折ってご使用ください。



基

-2,000 P

01

不正なUSBメモリから
ウイルス感染
【システム停止】

USBメモリから制御システムへウイルスが侵入し、システムを停止しなければならなくなった。

【有効な対策カード】
・USBポートブロック
・セキュリティパッチの適用
・機器の持込管理
・持込機器のウイルスチェック

インシデントカード

基

-3,000 P

02

保守ツールからウイルス感染
【PLC停止】

保守業者が持ち込んだ保守ツールからウイルス感染し、PLCが停止した。

【有効な対策カード】
・USBポートブロック
・セキュリティパッチの適用
・機器の持込管理
・持込機器のウイルスチェック

インシデントカード

基 | -2,000 P | 03

攻撃検知が遅れて被害拡大
【危険物の漏えい】

サイバー攻撃と気づかず通常の異常として機器交換を行った。交換した機器が同じ弱点を突かれて再度サイバー攻撃され、危険物（化学薬品等）の漏えいを引き起こした。

【有効な対策カード】
・初期パスワード変更
・セキュリティ部署への連絡

インシデントカード

基 | -1,000 P | 04

外部からの侵入者
【機器の破壊】

外部からの侵入者により、制御機器が破壊された。

【有効な対策カード】（必要枚数:2）
・侵入検知/遠隔監視システム
・2人ルールの徹底
・施錠管理の徹底
・入退室管理の徹底

インシデントカード

基 | -1,000 P | 05

内部資料から機密情報の窃取
【機密情報の漏えい】

機密情報が記載された資料（紙・CD・ハードディスク等）を、そのまま廃棄場に出したため部外者によって情報が窃取された。

【有効な対策カード】
・機密資料の細断・溶解処理
・社内のセキュリティ教育

インシデントカード

基 | -1,000 P | 06

飲み会でうっかり（１）
【ソーシャルエンジニアリング】

飲み会で同僚と、工場の入退場管理の仕組みを雑談し、犯罪者に情報が漏えいしてしまった。

【有効な対策カード】
・社内のセキュリティ教育

インシデントカード

基

-2,000 P

07

IDカードの不正利用による侵入
【システム緊急停止】

他人のIDカードを利用した侵入者により、不正な操作を実行され、制御システムが緊急停止した。

【有効な対策カード】
・2人ルールの徹底
・施錠管理の徹底
・入退室管理の徹底

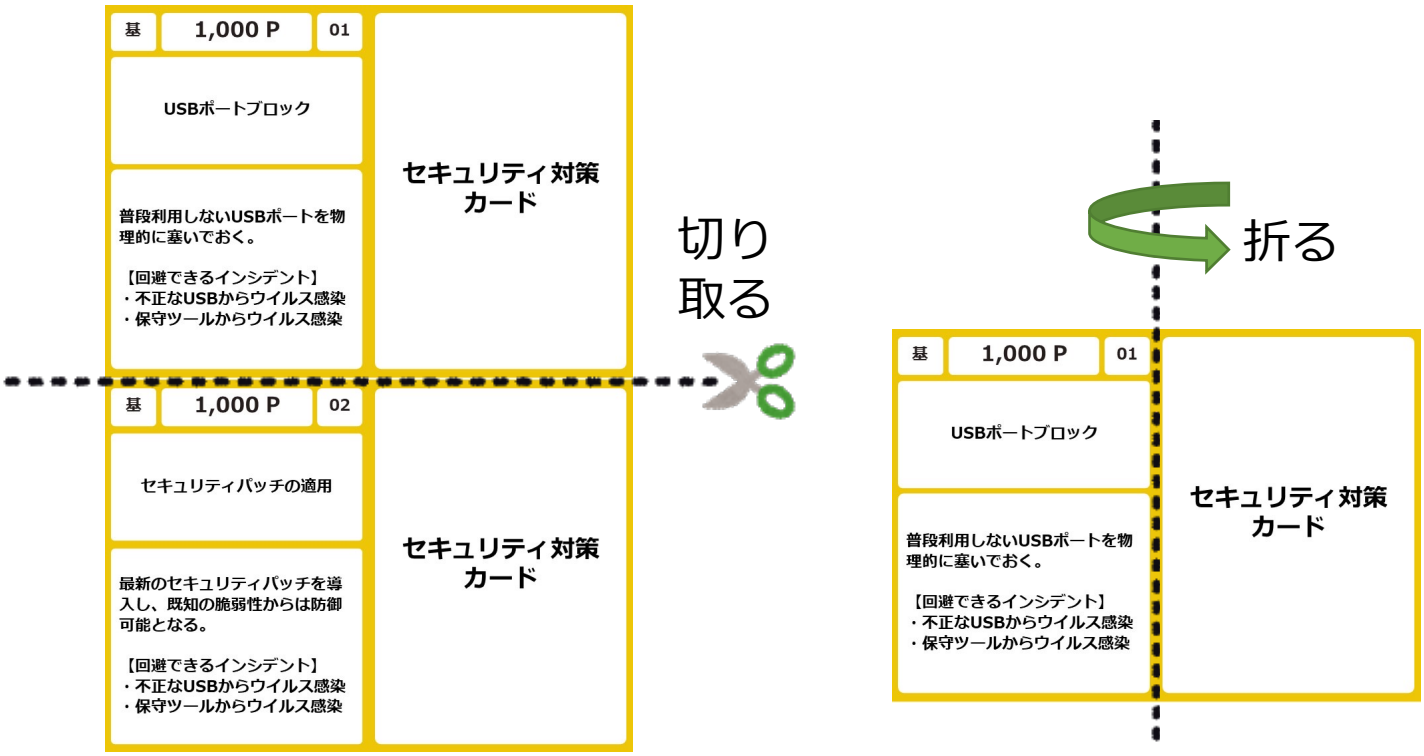
インシデントカード

セキュリティ
対策カード基礎編

インシデントカードの対策となるカードの基礎編です。
セキュリティ対策カードは全部で１２枚あります。

初めてセキュリティ道場をプレイする場合は、
基礎編のセキュリティ対策カードを使用してください。

上下で切り取り、左右で折って
ご使用ください。



基

1,000 P

01

USBポートブロック

普段利用しないUSBポートを物理的に塞いでおく。

【回避できるインシデント】
・不正なUSBからウイルス感染
・保守ツールからウイルス感染

セキュリティ対策カード

基

1,000 P

02

セキュリティパッチの適用

最新のセキュリティパッチを導入し、既知の脆弱性からは防御可能となる。

【回避できるインシデント】
・不正なUSBからウイルス感染
・保守ツールからウイルス感染

セキュリティ対策カード

基 | 1,000 P | 03

機器の持込管理

保守ツール（PC）やUSBメモリ、CD/DVD、SDカード等、現場に持ち込まれる機器は事前申請制とする等、厳密に管理する。

【回避できるインシデント】
・不正なUSBからウイルス感染
・保守ツールからウイルス感染
・不正な端末からの攻撃

セキュリティ対策カード

基 | 1,000 P | 04

持込機器のウイルスチェック

保守ツール（PC）やUSBメモリ等、現場に持ち込まれる機器は、必ずウイルス対策ソフトでチェックする。

【回避できるインシデント】
・不正なUSBメモリからウイルス感染
・保守ツールからウイルス感染

セキュリティ対策カード

基

1,000 P

05

初期パスワード変更

工場出荷時で設定されている初期パスワードは容易に推測できる機器が多いため、英数字と「@」や「!」を組み合わせた複雑なパスワードに設定し直した。

【回避できるインシデント】
・工場設備情報が漏洩
・攻撃検知が遅れて被害拡大

セキュリティ対策カード

基

1,000 P

06

セキュリティ部署への連絡

通常とは異なる不審な事象（同時多発的な故障や何度も繰り返される同じ異常等）は、サイバー攻撃の可能性があるため、セキュリティ部署へ連絡が有効。

【回避できるインシデント】
・攻撃検知が遅れて被害拡大

セキュリティ対策カード

基

1,000 P

07

侵入検知/遠隔監視システム

敷地境界や建屋外壁、室内等に設置された監視カメラやセンサー等により、不正な侵入を検知する。

【回避できるインシデント】
・外部からの侵入者
・内部脅威者による犯行

セキュリティ対策カード

基

1,000 P

08

機密資料の細断・溶解処理

機密情報が記載された資料（紙・CD・ハードディスク等）を物理的・化学的に破壊して破棄します。

【回避できるインシデント】
・内部資料から機密情報の窃取

セキュリティ対策カード

基

1,000 P

09

2人ルールの徹底

制御盤室など重要な部屋への入室は2人以上でないと入室できないルールを設定したり、電子錠等により、内部犯や不法侵入者への抑止になる。

【回避できるインシデント】
・外部からの侵入者
・IDカードの不正利用による侵入
・内部脅威者による攻撃

セキュリティ対策カード

基

1,000 P

10

施錠管理の徹底

制御盤やラック等の施錠を徹底し、鍵の貸出管理を厳格に実施することで、不正利用や不正アクセスの抑止につながる。

【回避できるインシデント】
・外部からの侵入者
・IDカードの不正利用による侵入
・内部脅威者による攻撃

セキュリティ対策カード

基 | 1,000 P | 11

社内のセキュリティ教育

セキュリティの意識が高まり、インシデントを回避しやすくなる。

【回避できるインシデント】
・内部資料から機密情報の窃取
・飲み会でうっかり(1), (2)

セキュリティ対策カード

基 | 1,000 P | 12

入退室管理の徹底

IDカードによる入退室管理と、そのカードの所有者が一致しているかを確認を行い、入退室履歴も管理する。

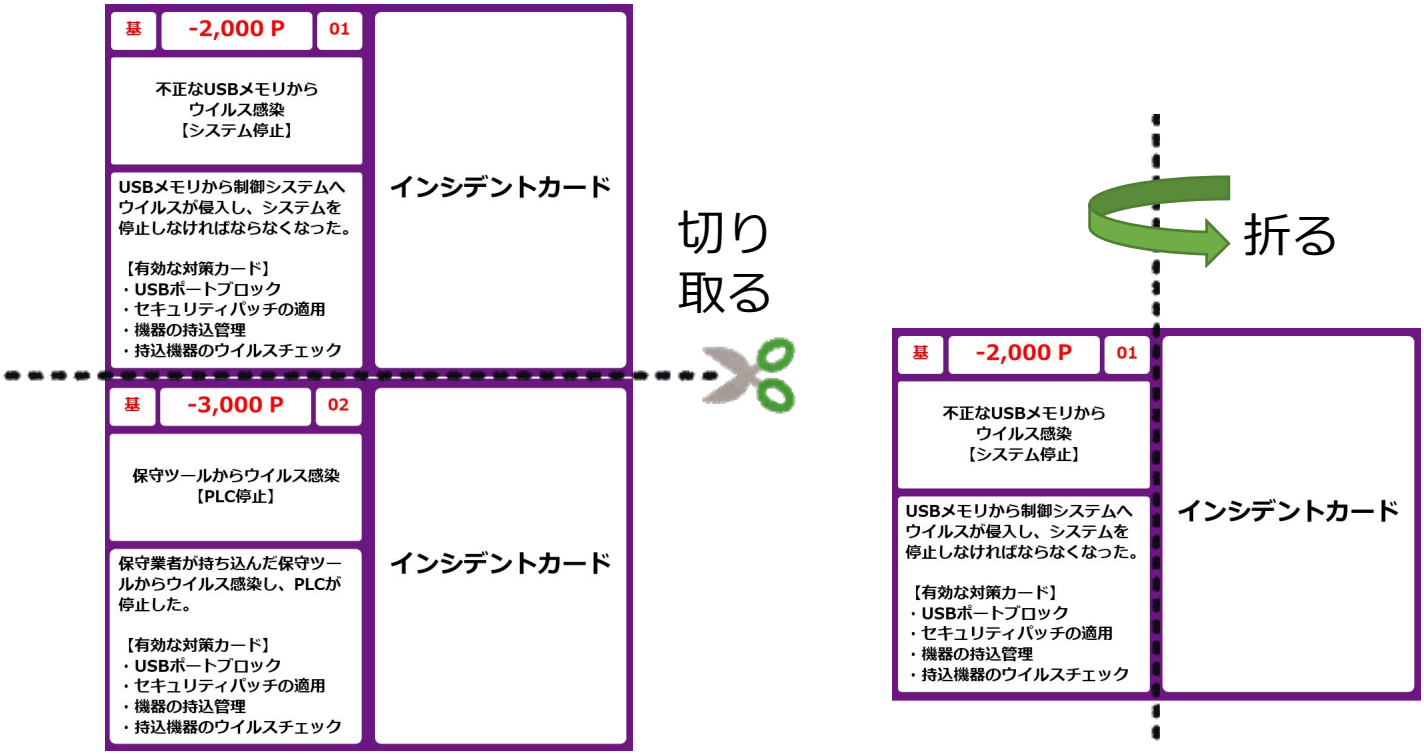
【回避できるインシデント】
・外部からの侵入者
・IDカードの不正利用による侵入
・内部脅威者による犯行

セキュリティ対策カード

インシデントカード応用編

インシデントカードの対策となるカードの応用編です。
インシデントカードは全部で５枚あります。

上下で切り取り、左右で折ってご使用ください。



応

-1,000 P

01

工場設備情報が漏えい
【緊急点検作業】

現場に設置されているWebカメラのパスワードが、初期パスワードのまま変更されておらず、外部から不正アクセスされ設備情報が漏えいした。

【有効な対策カード】
・初期パスワード変更
・ファイアウォール

インシデントカード

応

-2,000 P

02

不正な端末からの攻撃
【パラメータ改ざん/無警報】

制御ネットワークに不正な端末を接続され、DCSのパラメータが改ざんされた。（警報は鳴らなかった）

【有効な対策カード】
・機器の持込管理
・セキュリティHUB（セキュアスイッチ）

インシデントカード

応

-2,000 P

03

IT側からの侵入
【制御ネットワーク通信停止】

IT側から制御系ネットワークに侵入され、全ての通信が停止した。

【有効な対策カード】
・ファイアウォール
・情報系/制御系ネットワーク分離
・セキュリティHUB（セキュアスイッチ）

インシデントカード

応

-2,000 P

04

飲み会でうっかり（２）
【ソーシャルエンジニアリング】

飲み会の席で、自分のカバンに保管していた工場長の名刺を紛失した。
後日、工場長宛にウイルス付きのメールが送られてきた。

【有効な対策】
・社内のセキュリティ教育

インシデントカード

応

-3,000 P

05

内部脅威者による犯行
【工程停止】

上司や同僚に不満を持った社員の犯行により、制御盤室の全機器が停止した。

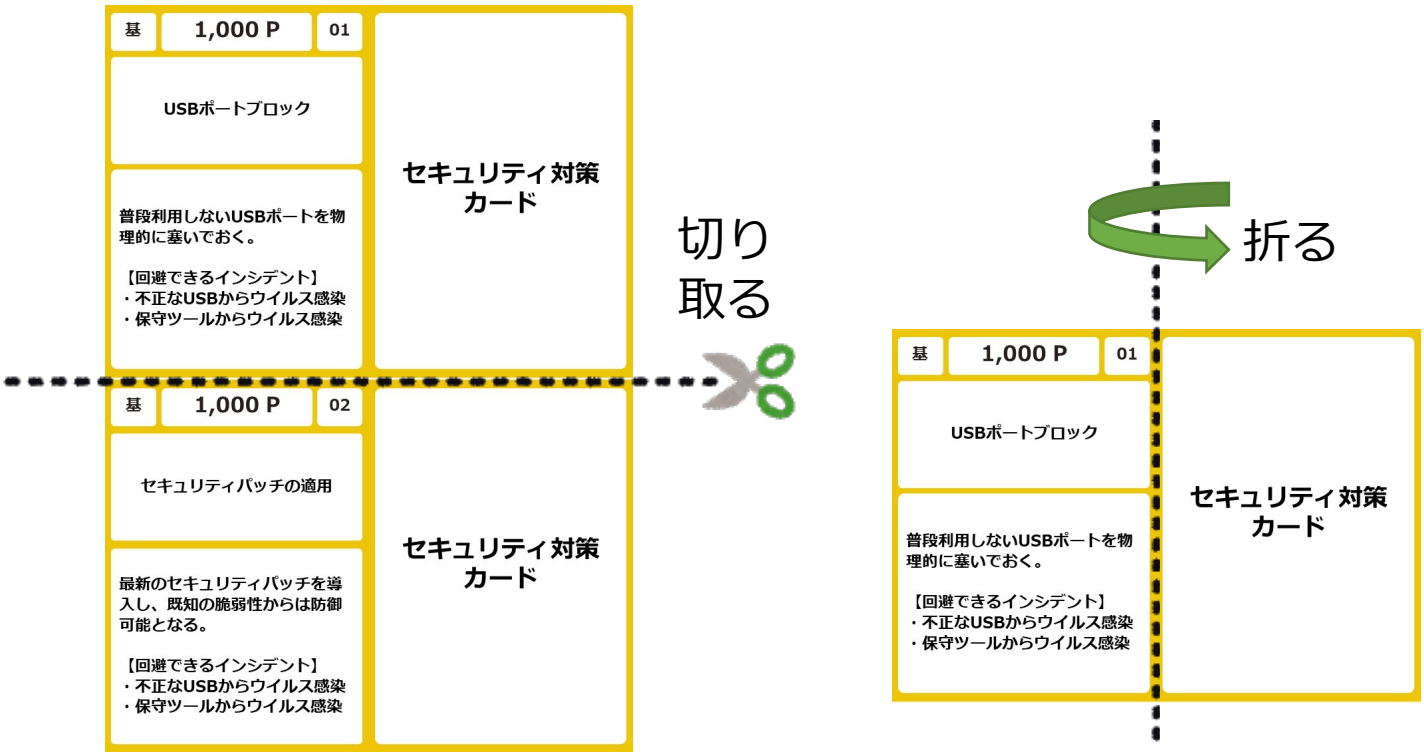
【有効な対策カード】（必要枚数:2）
・侵入検知/遠隔監視システム
・2人ルールの徹底
・施錠管理の徹底
・入退室管理の徹底

インシデントカード

セキュリティ
対策カード応用編

インシデントカードの対策となるカードの応用編です。
セキュリティ対策カードは全部で１０枚あります。

上下で切り取り、左右で折って
ご使用ください。



応

1,000 P

01

機器の持込管理

保守ツール（PC）やUSBメモリ、CD/DVD、SDカード等、現場に持ち込まれる機器は事前申請制とする等、厳密に管理する。

【回避できるインシデント】
・不正なUSBからウイルス感染
・保守ツールからウイルス感染
・不正な端末からの攻撃

セキュリティ対策カード

応

1,000 P

02

初期パスワード変更

工場出荷時で設定されている初期パスワードは容易に推測できる機器が多いため、英数字と「@」や「!」を組み合わせた複雑なパスワードに設定し直した。

【回避できるインシデント】
・工場設備情報が漏洩
・攻撃検知が遅れて被害拡大

セキュリティ対策カード

応

1,000 P

03

ファイアウォール

IT側との境界に設置されたファイアウォールにより、必要最小限の通信のみが許可される。

【回避できるインシデント】
・工場設備情報が漏洩
・IT側からの侵入

セキュリティ対策カード

応

1,000 P

04

情報系/制御系ネットワーク分離

情報系と制御系のネットワークを分離して、境界を跨いだ侵入を防ぐ。

【回避できるインシデント】
・IT側からの侵入

セキュリティ対策カード

応

1,000 P

05

セキュリティHUB
（セキュアスイッチ）

セキュリティ機能を持つネットワーク機器（HUB等）により、不正な端末の接続や不正通信を防御できる。

【回避できるインシデント】
・IT側からの侵入
・不正な端末からの攻撃

セキュリティ対策カード

応

1,000 P

06

侵入検知/遠隔監視システム

敷地境界や建屋外壁、室内等に設置された監視カメラやセンサー等により、不正な侵入を検知する。

【回避できるインシデント】
・外部からの侵入者
・内部脅威者による犯行

セキュリティ対策カード

応

1,000 P

07

2人ルールの徹底

制御盤室など重要な部屋への入室は2人以上でないと入室できないルールを設定したり、電子錠等により、内部犯や不法侵入者への抑止になる。

【回避できるインシデント】
・外部からの侵入者
・IDカードの不正利用による侵入
・内部脅威者による攻撃

セキュリティ対策カード

応

1,000 P

08

施錠管理の徹底

制御盤やラック等の施錠を徹底し、鍵の貸出管理を厳格に実施することで、不正利用や不正アクセスの抑止につながる。

【回避できるインシデント】
・外部からの侵入者
・IDカードの不正利用による侵入
・内部脅威者による攻撃

セキュリティ対策カード

応

1,000 P

09

社内のセキュリティ教育

セキュリティの意識が高まり、インシデントを回避しやすくなる。

【回避できるインシデント】
・内部資料から機密情報の窃取
・飲み会でうっかり(1), (2)

セキュリティ対策カード

応

1,000 P

10

入退室管理の徹底

IDカードによる入退室管理と、そのカードの所有者が一致しているかを確認を行い、入退室履歴も管理する。

【回避できるインシデント】
・外部からの侵入者
・IDカードの不正利用による侵入
・内部脅威者による犯行

セキュリティ対策カード