

# カスペルスキーのサイバー演習で インシデントレスポンスを体験しませんか

## サイバー事故からシステムを守ろう !!

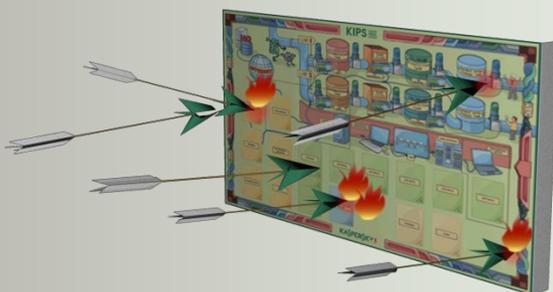
kaspersky

MHIパワーコントロールシステムズ  
MHI Power Control Systems



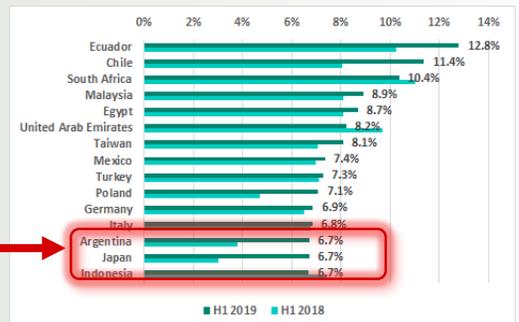
### サイバー攻撃は人を狙う

世界各地で拡大し始めたサイバー攻撃はITインフラだけでなく、さまざまな業種のシステムに対して行なわれています。カスペルスキーのICS CERTは2019年9月30日発表した産業用制御システムに対する脅威状況の調査レポートでランサムウェア\* 攻撃の急増をお伝えしていますが、ランサムウェアを検知した産業用コンピュータのうち19.6%はWannaCryによるものでした。また、産業インフラ内の主要な脅威源は過去数年間、上位をインターネット(24.5%)、リムーバブルメディア(8.3%)、電子メールの添付ファイル(5.6%)が占めていますが、このうち電子メールの添付ファイルによる脅威の割合は増加傾向となっており、検知された上位15ヶ国の中に日本が含まれるようになりました。これらの攻撃に対処するには、ツールを導入するだけでは足りません。実はサイバーセキュリティの向上に一番効果があるのは「教育」なのです。それはサイバー攻撃のほとんどが人間を経由した攻撃だからです。



\* ) サイバー：インターネットの、仮想空間の  
\* \* ) 感染するとPC内の全ファイルを勝手に暗号化し復号の為に身代金を要求するマルウェアの一種。

日本は圏外から14カ国目に上昇



電子メールの添付ファイルによる脅威上位15カ国  
(2019年上半期：)

## システムの防御対策

# カスペルスキー提供によるサイバー演習ゲームで システムのセキュリティ対策を学びませんか

チームに分かれて、システムを安定操業、そこに迫りくるウィルスやサイバー攻撃の脅威。  
上手な対策で、事業継続と収益確保をめざします。でも、その結果はいかに？  
シミュレーションでサイバー攻撃とセキュリティ対策を体験。

- ▶ 楽しみながら短時間で基礎を理解(2時間)
- ▶ 共同作業でチームワークを育成
- ▶ チーム間の競争を通じて分析スキルを向上
- ▶ ゲームを通してサイバーセキュリティ対策を理解
- ▶ 深い専門性は不要



## 現場とITだけでなく事業責任者にも必須

サイバー攻撃は、実環境で「体験」することはできません。そこで、シミュレーションで体験できる演習「KIPS (Kaspersky Interactive Protection Simulation)」を開発しました。  
このプログラムを受講することで、現場の方から事業責任者の方まで容易にサイバー攻撃を体験できます。  
KIPSは世界中のセキュリティの専門家が集まる国際会議などで実施されています。  
KIPSはシステムにおけるセキュリティーの基本を演習を通して学んでいただけます。ITシステム管理担当者、工場の現場のシステム担当者はもちろんのこと、事業の収益責任を負っているみなさんにも、サイバー攻撃によってどのような事態が発生する可能性があるのかについて学んでいただけます。

### サイバー演習に関するお問い合わせ

当社では、CSMS認証取得のノウハウを生かし、サイバー攻撃、制御セキュリティ技術の動向、お客様システムのセキュリティシステムの構築について、最適なものをご提案します。  
ご要望により、制御セキュリティの説明会の開催、セキュリティ対策の支援を行うことができます。

 045-285-0115

〒231-8715 神奈川県横浜市中区錦町12  
株式会社MHIパワーコントロールシステムズ  
営業戦略室 営業部

 当社ホームページ「お問い合わせ」

URL : <https://cs.power.mhi.com/>

株式会社MHIパワーコントロールシステムズ  
**MHI Power Control Systems Co., Ltd.**