

サイバーコネクトSHIG@

今、注目のサイバーセキュリティに関する情報をお届けします。

Cyber connect shig@

～大阪・関西万博の開催まで、あとわずか!!～

各種情報システム・セキュリティ設定
の点検をお願いします!!

世界のサイバー攻撃集団等は、国際的な大規模イベント開催の機会を狙って、サイバー攻撃を仕掛けてます。

理由その① 多種多様な国や企業が参加するイベントをサイバー攻撃の好機と考えている。

サイバー攻撃集団は、世界的な注目を集める大規模イベント開催時は政治的な主張を誇示したり、不正に資金を獲得する絶好の機会と考えています。

理由その② サイバーテロは、時間や場所に関係なく敢行できる。

サイバー攻撃集団は、いつでも、何処からでも、国境を越えて攻撃します。

理由その③ セキュリティが脆弱な所を狙い、最大の効果を上げようとする。

開催地の大阪府や万博実行委員会が狙われる可能性は非常に高いですが、周辺地域でセキュリティ対策が不十分なところが狙われる傾向があり、滋賀県内の自治体や企業にサイバー攻撃が仕掛けられる可能性は否定できません。



【最近のサイバー攻撃の傾向】

- ① 攻撃者の「職業化」が著しく、販売されているランサムウェア等のツールキットを使えば簡単に攻撃できたり、お金を払えばDDos攻撃を依頼できるなど、サイバー攻撃を容易に実行しやすい環境が整っている。
- ② サイバー攻撃集団は、周到に準備をしたうえで巧妙にサイバー攻撃を仕掛けており、攻撃が発覚するまでに時間がかかる傾向にある。
- ③ セキュリティの強固な大企業を直接狙わずに、関係会社などでセキュリティ対策が不十分な個所を探して侵入し、横展開するなどして目的の企業に侵入する。
- ④ アイデンティティ攻撃と言われるIDやパスワードの窃取を目的とした攻撃に重点を置き、侵入後、権限を昇格させて、より価値の高いデータを狙ったり、システムを乗っ取って踏み台として利用する。



セキュリティ対策をお願いします!!

セキュリティ設定の点検 

- ウイルス対策ソフトのパターンファイルは定期的に更新していますか？
- OSの更新プログラムやVPN機器、通信関係機器のファームウェアの更新プログラムは的確に適用していますか？
- 機器等の脆弱性が発表された際、各ベンダーが提供する修正プログラムを的確に適用していますか？
- 自社やサプライチェーン、末端機器などに外部から業務システムへ容易にアクセスできる設定になっていませんか？
- インターネット接続やリモートデスクトップなどの境界線防衛を見直していますか？

セキュリティ意識の向上 

- 業務システムで使用しているパスワードは適正に運用されていますか？使い回しはしていませんか？
- 各種システムへのアクセス権限は、必要の人に必要な権限を付与していますか？
- 自社の情報システム部門が許可していない端末を従業員が勝手に業務に使っていませんか？
- 情報セキュリティに関する社員教育を定期的実施し、セキュリティ意識を自社全体に浸透させていますか？
- 社全体でインシデント対応などのトレーニングをしていますか？

★定期的なチェックと見直しを★



注意！「トクリユ」にあなたの家も狙われている!? 住宅強盗対策の強化を！

滋賀県警察本部 警備第一課 サイバー攻撃対策係 077-522-1231 (代表)