shaping tomorrow with you
社会とお客様の豊かな未来のために

FUJITSU

サイバーセキュリティ:
2017年の予測

サイバーセキュリティは常に新しい課題に直面します。
毎年現れる新しいセキュリティ脅威の先を超すのは困難です。
しかし、もう少し注意を払って先を見越しておけば
防げた脅威も2016年には多数ありました。

2017年も同じでしょうか。
企業はよりプロアクティブに対処できるでしょうか。
サイバー脅威に対する富士通の10項目の予測についてご説明します。

※当レポートは当社のEMEIAリージョンの分析に基づくものです。

1

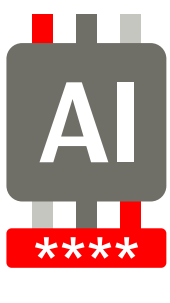
ネットワークの脆弱性に注意

PowerShellなどのセキュリティの脆弱性は、
そのリスクを見過ごす企業の弱点になり続けるでしょう。

2

高性能なコンピュータはよりセキュアか

コンピュータはますます賢くなっています。新しい策略も学習しています。
そのためにセキュリティの見方が完全に変わるかもしれません。
しかし、気をつけてください。ハッカーも同じ策略を使って、セキュリティ管理をすり抜けています。



3

銀行が引き続き攻撃の最前線

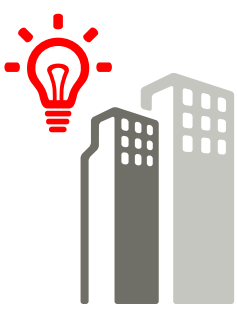
昨年、ハッカーはセキュリティの欠陥をすり抜けて、
大手銀行から大金を手にしました。
対策を講じてはいますが、銀行への攻撃は今年も続くと予測されます。

4

攻撃の標的はモバイルデバイスにシフト

この記事をご覧になっているのはスマホからですか。そのスマホは安全ですか。
個人データを標的にした新しい攻撃に気をつけてください。
写真を見られなくするランサムウェアもあります。

5



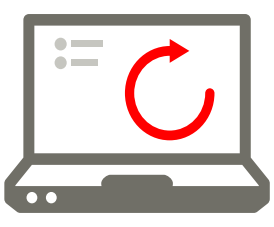
「スマートシティ」の実態が明らかに

スマートモーターウェイの電光板の設計者は、ハッカーが政治的なメッセージを
表示するとは思っていなかったでしょう。
スマートシステムは限界まで試されるでしょう。
制御プラットフォームに対する注意を怠らないでください。

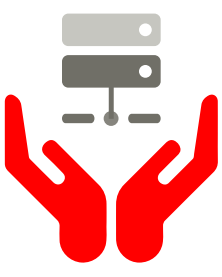
6

信用を守るには、迅速なリカバリが必要

どのようなセキュリティ管理をしていても、企業に対するハッキングは起こりえます。
迅速にリカバリできないと、ビジネスや信用に傷がつきます。準備は万全ですか。



7



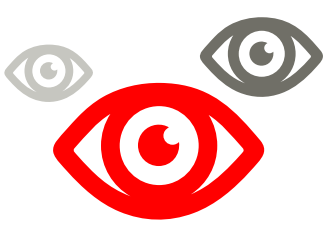
企業はデータを安全に保管する方法を求める

一般データ保護規則(GDPR)がまもなく施行されます。
投資家、株主、顧客、規制当局には、
データを安全に保管する方法が必要になります。

8

グローバル企業はサプライチェーンに目を光らせる

自社内の機密データの安全は確保したかもしれませんが、
サプライチェーンは大丈夫ですか。
大企業は、データ処理のセキュリティを確保できる
サプライチェーンのみを利用するようになるでしょう。



9

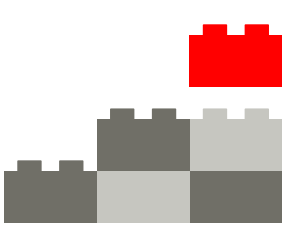
経営幹部がITセキュリティを語り始める

経営幹部は真実に目覚めようとしています。ITセキュリティに問題があると、
ビジネスの収益とブランドの両方が被害を受けます。
しかし、経営幹部は技術用語が苦手なので、シニアITスタッフは
経営幹部が理解できる言葉でニーズを話し合う必要があります。

10

最大の問題はやはり基本動作

セキュリティの問題を突き詰めれば、すべてサイバーハッカーに原因があります。
しかし、本当の敵はもっとつまらないことです。
基本的なITのベストプラクティスを守らないと、セキュリティ侵害には無防備です。



2016年から学べることは、企業がサイバーセキュリティの発展を無視すれば、
自分でリスクを負うことになるということです。
攻撃の危険がない企業はありませんが、
よく組織して注意を怠らなければ、
攻撃や業務停止による影響を避けられる可能性が高まります。

お客様のビジネスをサイバー脅威から保護する方法の詳細は、
セキュアシンキングのWebサイトをご覧ください。

お問い合わせ

富士通株式会社
富士通コンタクトライン(総合窓口)
0120-933-200
受付時間 9時～17時30分
(土曜・日曜・祝日・当社指定の休業日を除く)
http://www.fujitsu.com/jp/solutions/security/

FUJITSU
22 Baker Street
London W1U 3BW
Tel: +44 (0) 1235 79 7711
Email: askfujitsu@uk.fujitsu.com
Web: **uk.fujitsu.com/securethinking**
Ref:3684