ITソリューションプロバイダー
株式会社日本キャスト

Nihon Cast Corporation

激しさを増すサイバー攻撃をよりスピーディーに対策！

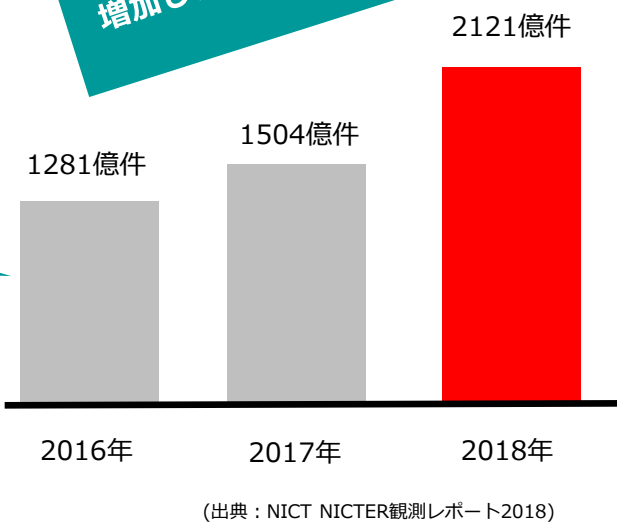
出口対策くん

情報漏洩阻止！！

サイバー攻撃は年々増加している状況ではあるが、中でも**標的型攻撃により情報の流出**が拡大している。2018年に観測されたサイバー攻撃関連通信は、過去最悪の合計2,121億件に上る状況にある。

2018年度は過去最悪の
2,121億件
1日5.8憶件もの攻撃を観測

増加し続けるサイバー攻撃



(出典：NICT NICTER観測レポート2018)

入口対策・内部対策だけでは情報漏洩を阻止するのは困難な時代

入口対策を充実させるの時間とコストだけじゃなく、高いスキルが必要になり大変。。。

時間とコストかけて入口対策してる間に情報漏洩するかもしれない

すぐに対策できる方法はないか。。。

出口対策くん

会社の生命線である顧客情報や社員の情報を外部に漏洩させないために導入

少ない投資で高いセキュリティ対策を実現！

マルウェアの侵入を前提に出口対策し情報漏洩を食い止める！！

★出口対策くん

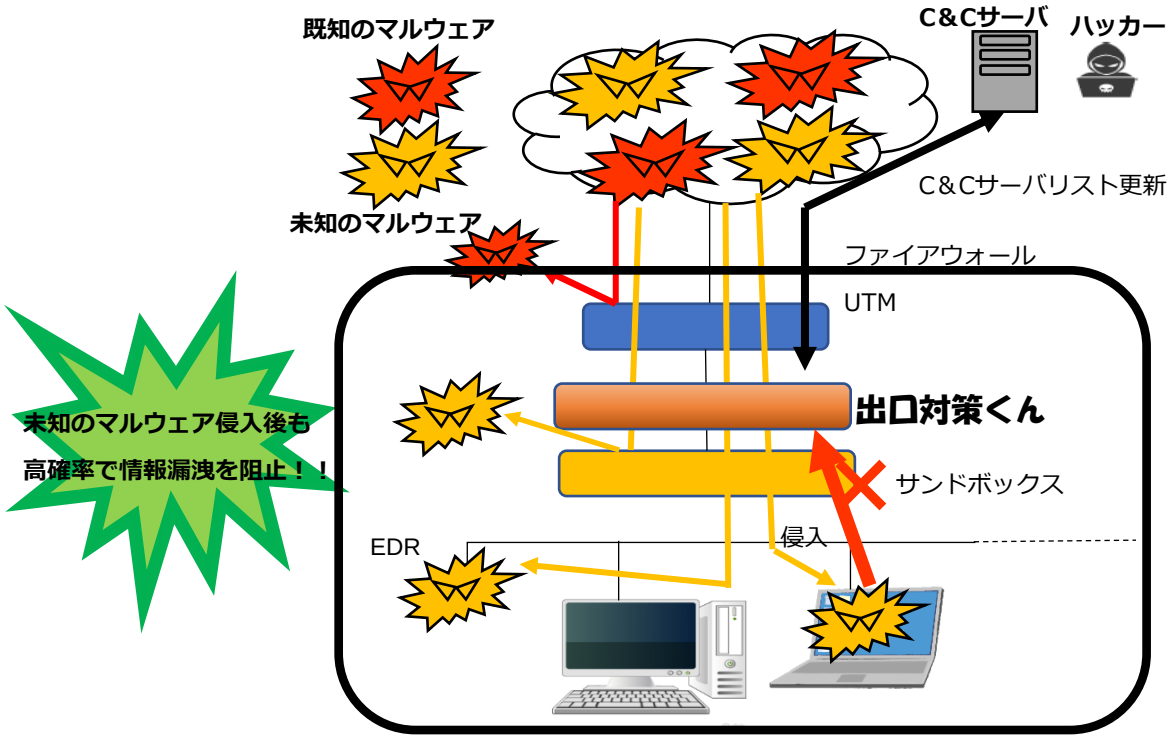
【機能】

侵入したマルウェアによるC＆Cサーバへの通信を検知・ブロックし、被害を食い止める。

また不正な通信内容に関するログを収集しているため、経路等の分析も可能。

C＆CサーバリストはLACが提供。

システムへの組み入れが簡単！！



インシデント発生時にも安心

調査、対策にかかる費用を300万円まで補償

出口対策製品を導入し、如何に高い確率で情報漏洩を防ぐことができるかが鍵となりますが、本製品は国内最大のセキュリティ監視センター「JSOC」で監視した不正通信結果に基づき、C&Cサーバのリストをタイムリーに出口対策くんに連携することにより、高精度の検知率を提供します。

当製品に関するお問い合せ先

株式会社日本キャスト
インフラソリューション部
高見　和寛
〒１０１－００６４
東京都千代田区神田猿楽町2-8-16 平田ビル6階
TEL　０３－５５７７－３１９０
E-mail deguchi-kun@n-cast.co.jp
URL：https://www.n-cast.co.jp/index.html

・当資料の一部または全部を、無断で複写、転載することを禁じます。
・当資料は予告なく変更する場合があります。