

## NEC Enterprise SDN Solutions

## サイバー攻撃自動防御ソリューション

サイバー攻撃の検知から対処までを自動化※

会社の信用失墜などを引き起こすセキュリティリスクを低減

※セキュリティインシデントを検知すると、SDN (Software -Defined Networking) で該当端末の通信を自動的に遮断します。

## 課題／解決策

## セキュリティに関する課題

- ① 人手による初動対応は時間がかかり、人的ミスのリスクにつながる
- ② 情報漏えいや二次感染等による被害の拡大を防ぎたい

SDN  
×  
セキュリティ

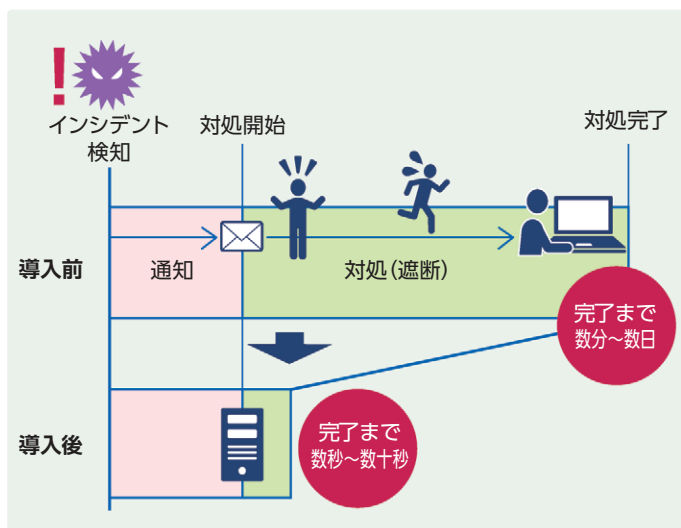
## 解決策

- ① 初動対応の自動化により、被害拡大のリスクを低減
- ② 感染端末の通信をネットワーク上で遮断し、内部への拡散を局所化

## 機能／特長

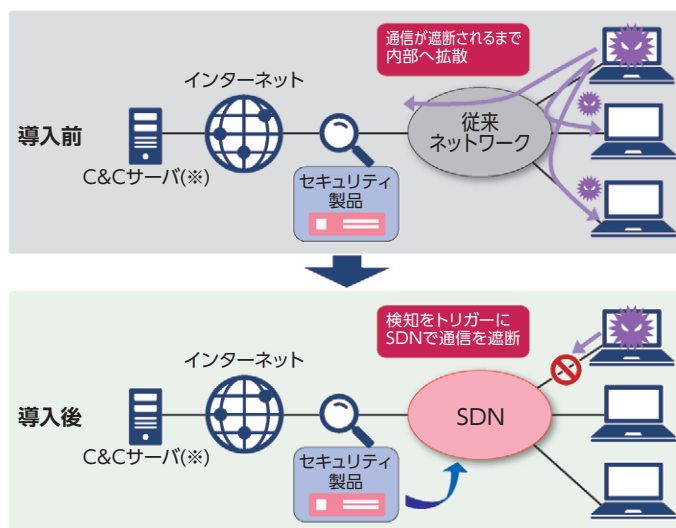
## ① 初動対応の自動化

## 検知から対処までの時間比較



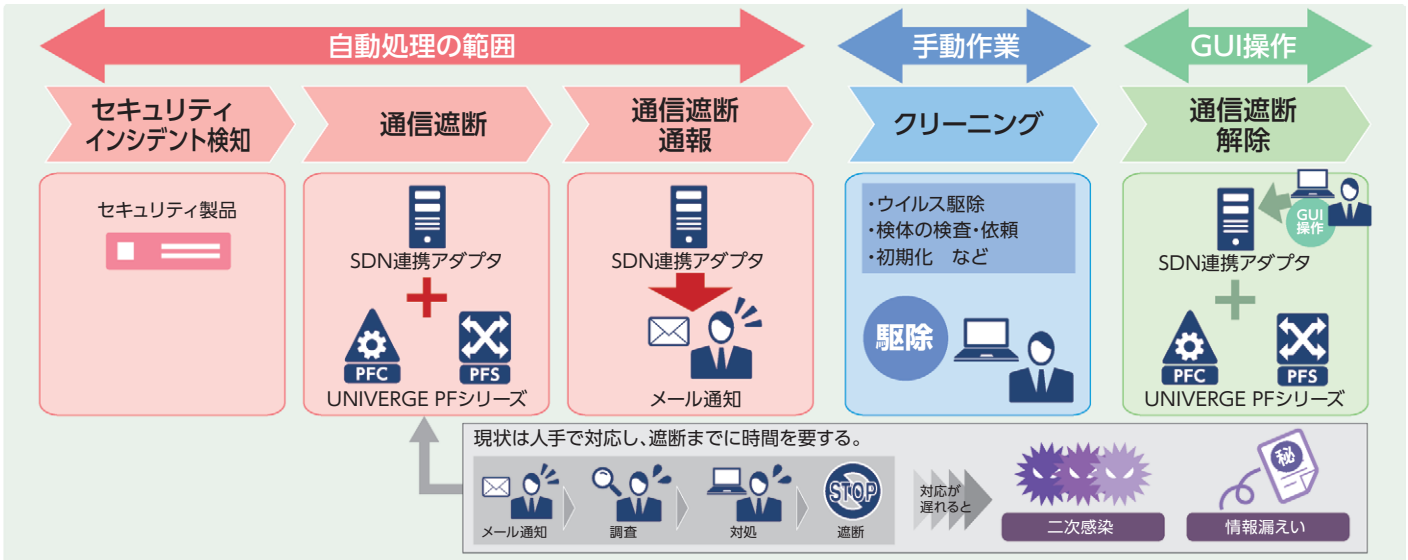
## ② 内部拡散の局所化

## 感染端末を遮断し内部拡散を局所化

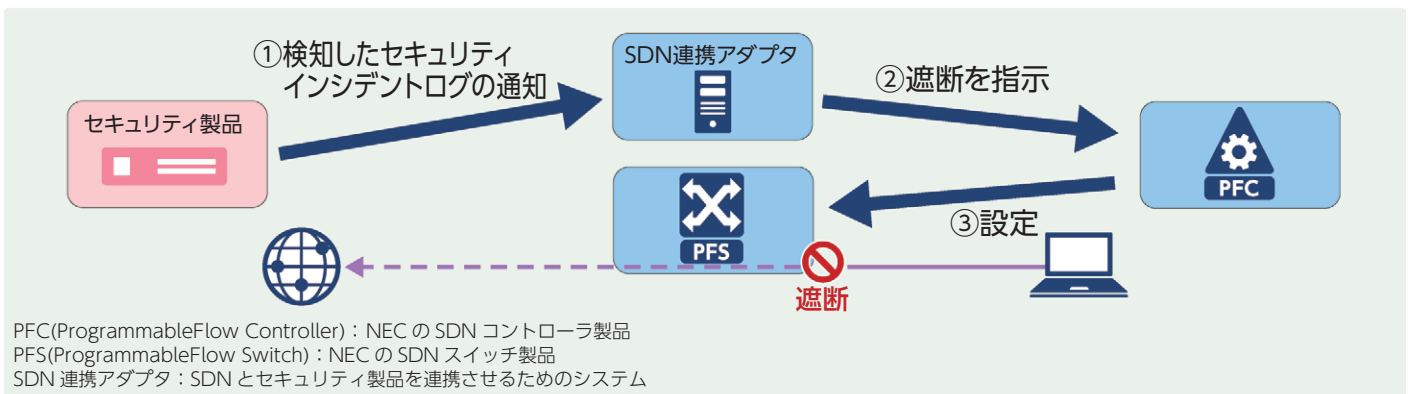


※: C&Cサーバ (Command & Control サーバ):  
インターネット経由でマルウェア感染した端末を制御したり命令を出すサーバ

## 運用イメージ

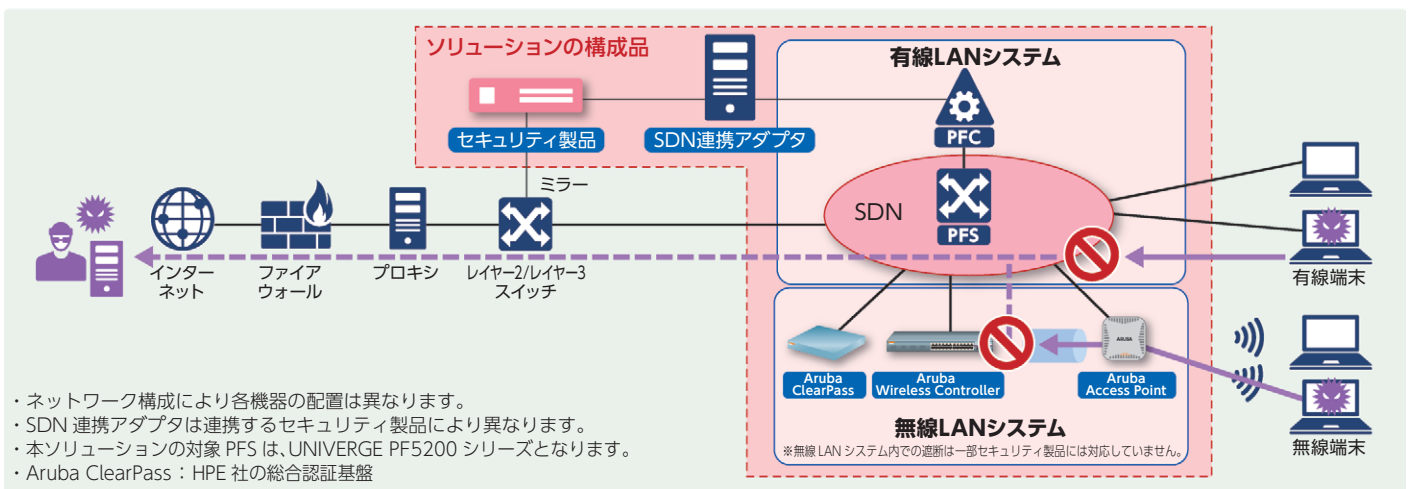


## 動作概要



## 構成例

セキュリティ製品でセキュリティインシデントを検知すると、NECのSDNで該当端末の通信を自動的に遮断します。さらに、該当端末が無線の場合は、無線LAN環境の中で遮断することもできます。



お問い合わせは、下記へ

NEC ビジネスクリエイション本部

E-mail: inquiry@sdn.jp.nec.com

URL: http://jpn.nec.com/sdn/

- 本紙に掲載された社名、商品名は各社の商標または登録商標です。
- 本製品の輸出（非居住者への役務提供等を含む）に際しては、外国為替及び外国貿易法等、関連する輸出管理法等をご確認の上、必要な手続きをお取りください。
- ご不明な場合、または輸出許可等申請手続きに当たり資料等が必要な場合には、お買い上げの販売店またはお近くの弊社営業拠点にご相談ください。
- 本紙に掲載された製品の色は、印刷の都合上、実際のものとは多少異なることがあります。また、改良のため予告なく形状、仕様を変更することがあります。