2022年1月28日

# 地域Secunity サイバーセキュリティセミナー in 熊本

## 創業70年老舗中小企業サイバー被害の実例


ネットワークとオートメーションで心豊かな社会の実現に貢献します

創ネット株式会社

# なぜ、私がここでお話しているか

サイバー被害に遭ったからです…

# 会社概要

社名　　：創ネット株式会社

本社　　：福岡県福岡市博多区築港本町6-3

北九州営業所：福岡県北九州市戸畑区元宮町8-11

創業　　：1950年12月6日（現72期）3代目

従業員　　：26名（県外在宅勤務者2名、役員・パート含む）

資本金　　：2,000万円

事業内容　　：ファクトリーオートメーションを提案する
**地域**密着型エンジニアリング専門商社
物販83%　エンジニアリング17%（2020年度）

専門　　：工場で使用する
生産機械（ロボット、電機・制御・電子・電材・機構部品…）
ユーティリティ設備（電気、照明、エア、蒸気、空調、省エネ機器…）

OMRON
MITSUBISHI ELECTRIC Changes for the Better
Pro-face by Schneider Electric
Orientalmotor
SIEMENS
PATLITE
NIKK SWITCHES
国自机器人

# 経営理念

- 経営理念

私たちは、**ネットーワーク**と**オートメーション**で心豊かな社会の実現に貢献し、社員の幸せを追求します。

私たちは、「お客様のお役に立てて良かった」をもっとも大切な使命と心得ていきます。
（お役・・・良い商品・サービスの提供と、顧客の仕事の代行である）

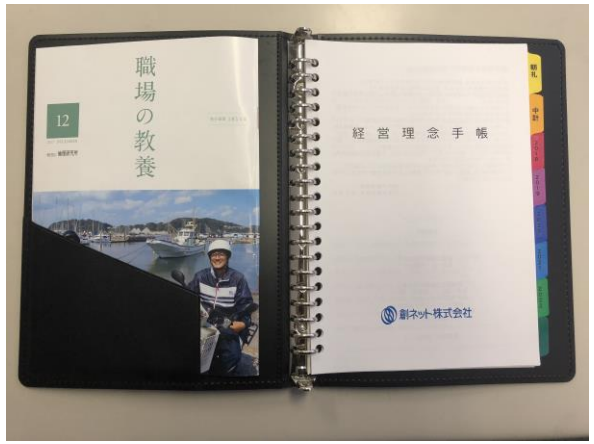
私たちは、一人一人が尊重され自己実現を追及する、いきいきとした組織づくりを目指します。

- 経営指針

経営に対する考え方
基本方針
行動指針
組織風土
仕事の考え方
社員に対しての考え方

お客様に対しての考え方
仕入先に対しての考え方
課題・トラブルに対する考え方
地球環境に対する考え方
商品に対する考え方

※経営＝見える化



# なぜ、私がここでお話しているか

それは

製造業と農業の時代の流れが似てるからです。

## 製造業の流れ

手作業

第1次産業革命

機械化

第2次産業革命

電化

第3次産業革命

オートメーション化

第4次産業革命

デジタル化

スマートファクトリー化
スマート農業化

## サプライチェーン

サプライヤ → メーカー → 卸 → 小売 → 消費者

デジタル変革

調達 → 生産 → 物流 → 販売

＋

事業承継

# はじめに

## 経営とは…

顧客の創造
社員の幸せ
利益の追求
キャッシュフローの改善
成長、繁栄
永続、信頼
上場
株主満足
・
・
・


**リスク回避**　外的：災害、交通事故、コロナ・・・・・サイバー被害
内的：就業規則（安全衛生、服務）・・・情報漏洩

# システム概要

社内情報共有

サイボウズ Office　Chatwork　Google ドライブ　E-Mail

仕入先
約350社

EDI⇔RPA
WinActor®

販売管理システム

見積・発注・入荷・在庫・受注・納品・請求

BtoB プラットフォーム 請求書

顧客
約580社

マーケティングオートメーション

aperza cloud

顧客・営業管理システム

ZOHO

セールスフォース・ドットコム

会計・給与

クラウド
WEB

経費

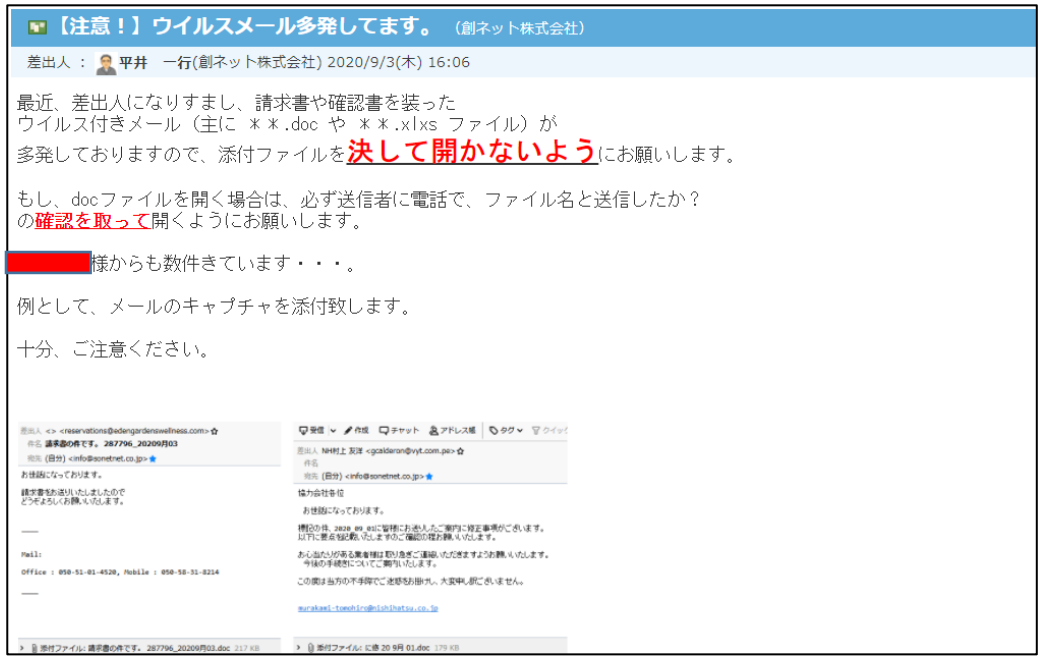
楽楽精算

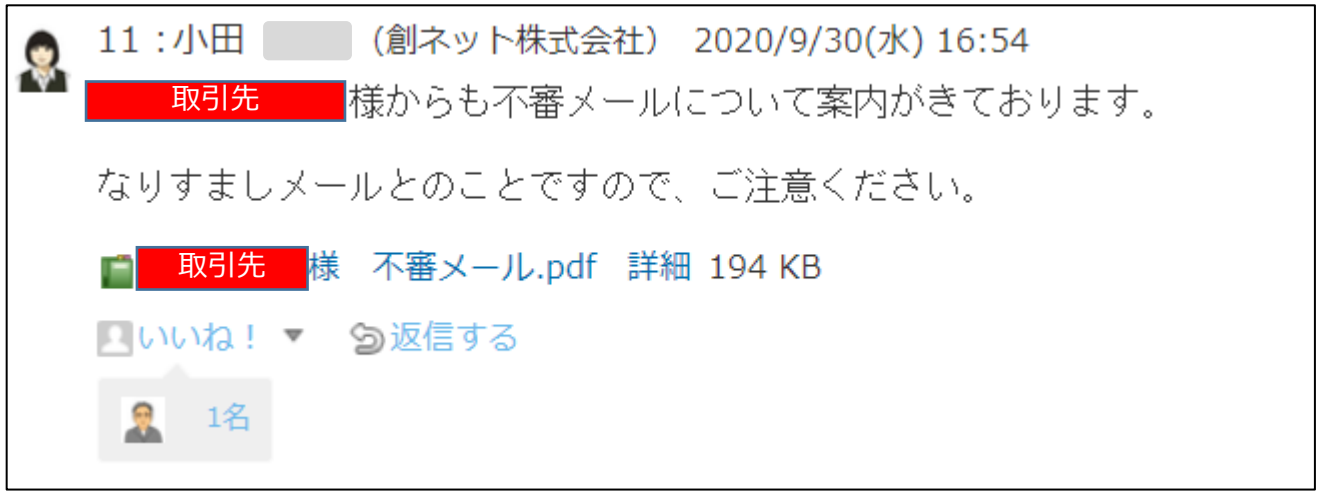
※WinActorはNTTアドバンステクノロジ株式会社の登録商標です

それなりにIT化、出来ているが…

・サイバーセキュリティ対策　システム


・教育：注意喚起（グループウェア）




過去にも数度あり

# サイバー被害

## 在宅ワーク中の社員がお客様の「なりすましメール」を開き感染

2：平井　一行（創ネット株式会社）　2020/9/16(水) 18:43（※グループウエア）

お疲れ様です。

本日、１４時頃 社員 が、メール添付のｄｏｃファイルを開き
その後、暫くしてアンチウイルスが「トロイの木馬を発見・削除した」と
通知が出たそうです。

その後、仕入先などから、ウイルス付きの　なりすましメールが来ていると
連絡がきたと、報告がありました。

状況としては、添付のウイルスの活動を、任意で許可した為、ウイルスにより
メールの情報を抜かれウイルスサーバーに転送され情報漏洩となります。
その後、ウイルスサーバーより「なりすましメール」を発信し続けている状態ですので、
注意喚起以外の手の打ちようがありません。

先ほど、ホームページのトピックスに、注意喚起とお詫びの記事を載せました。
https://www.sonet.ne.jp/modules/topics/index.php?page=article&storyid=231

尚、現在、 社員 ＰＣはフルスキャン２度を行い、ＰＣ内にはウイルスはいないと思われます。

ウイルスの内容は下記の記事の通りですので、一読下さい。
https://www.ipa.go.jp/security/announce/20191202.html

くれぐれも、添付ファイルを開くときは十分注意ください。

特に、マイクロソフトＷｏｒｄの添付ファイル（＊＊＊．ｄｏｃ）は、
開かないようお願いしたいです。

宜しくお願い致します。

いいね！ ▾　返信する

大切な取引先に
なりすましメールで
ウイルスをばらまく

どこも被害、損失は無かったが…

※取引先が被害に遭っていると分からない

# サイバー被害時の対応（コスト＝時間）

被害：ノートパソコン1台

| | | |
|---|---|---|
| 1. | 既存の共用PCに基幹システム、IPアドレスの設定など代替PCの準備 | 2時間 |
| 2. | 必要なファイルデータを外付けHDDに移動 | 2時間 |
| 3. | 感染PCの準備及びクリーンインストール | 1時間 |
| 4. | 初期設定とIPやワークグループなどの基本設定 | 1時間 |
| 5. | Windowsアップデート | 2時間 |
| 6. | 販売管理システム、Office、プリンタドライバ等インストール＆設定 | 2時間 |
| 7. | 必要なファイルデータを外付けHDDから移動 | 1時間 |
| 8. | 情報収集、Webサイト掲載、社内共有等 | 2時間 |
| | 合計 | 13時間 |

・中小企業に、情報システム専門部[illegible]は無[illegible]務の片手間での13時間は物凄い負担

・まして、サイバーセキュリティ[illegible]ない[illegible]ため情報収集に時間がかかる

・被害に遭ったら、誰に相談[illegible]からない＝専門業者に当日頼んだら物凄い金額

**自主管理では限界**

# サイバー被害時の対応

## 創ネットWebサイト掲載

### 【重要】迷惑メール（なりすましメール）に関するお詫びおよび注意喚起に関して

2020-09-16

お取引先様各位

平素は格別のご高配を賜り、厚く御礼申し上げます。

令和2年9月16日15時頃から、当社および当社の社員を装った、
いわゆる「なりすましメール」が複数の方々に発信されている事実を確認致しました。
メールの送信の対象となりました皆様には多大なご迷惑をお掛けしています事を深くお詫び申し上げます。

また、当社からのメールで、「内容に心当たりがない」「怪しい」「業務に無関係」などのメールを受信された場合は、
ウイルス感染、フィッシングサイトへの誘導のリスクが高いため、メールの開封、添付ファイルの参照、
或いはメール本文中のURLのクリック等を行うことなく削除して頂きますよう、よろしくお願い致します。

当社メールとなりすましメールの見分け方は、下記の通りとなります。
◆**なりすましメール**の例
　※「送信者名(差出人)」と「送信元メールアドレス」が異なっています。
　※弊社のメールの@以降は、「sonetnet.co.jp」になります。
差出人：創ネット(株) *****　@tafsol.com>

◆通常メール
差出人：創ネット(株) ***** <*****@sonetnet.co.jp>

※マイクロソフトWordのファイル(***.doc)が添付していることが多いようです。
※なかには、Wordのファイルを圧縮した、***.zip　の場合もございます。
※ウイルスにつきましては、下記サイトもご参照下さい
https://www.ipa.go.jp/security/announce/20191202.html

当社におきましては、不正アクセスの防止など情報セキュリティには十分注意しておりますが、
引き続き対策を強化して参りますので、ご理解とご協力をいただきますよう、よろしくお願い致します。

# サイバー被害の原因

入口対策のみの導入で、不正サイトへのアクセス対策（出口対策）が出来ておらず感染

**①マルウェア感染**
**対策：入口対策**

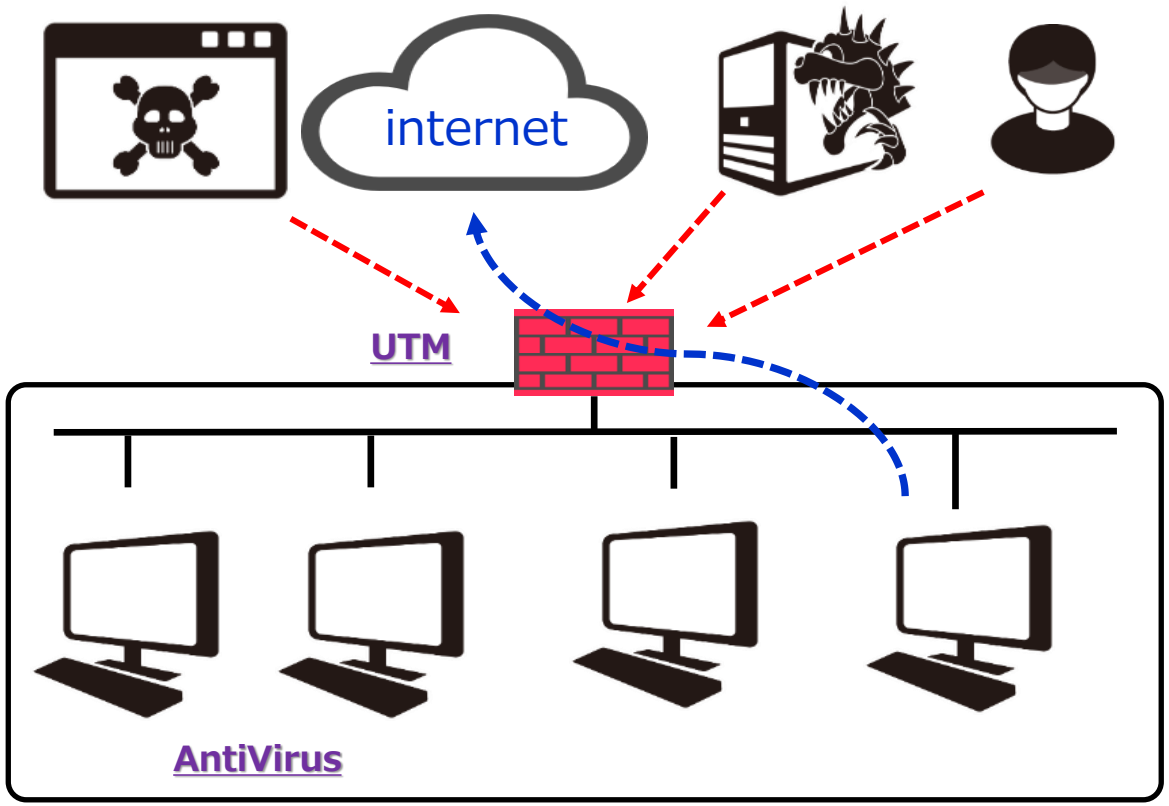
**②リモートコントロール**
**対策：出口対策**

**③感染拡大**
**対策：内部対策**

**④目的遂行**
**対策：証跡調査/対処等**

①UTM
②EndPoint:アンチウイルスソフト
（パターンファイル）

※② ～ ③の対策が必要！



簡易構成図

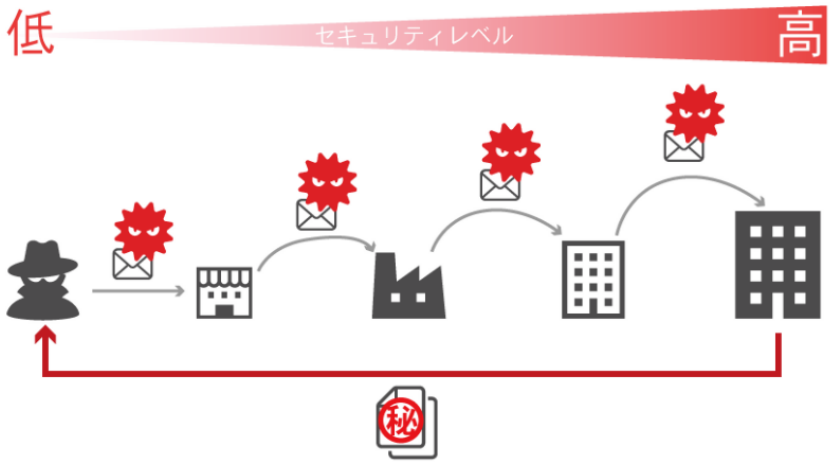
皆さんはウイルスに感染したらどうしますか？

PCに詳しい社員が居て13時間／PC

もし、社内ネットワークで感染拡大（クラスター）したら…

サイバーセキュリティ対策　≒　新型コロナウイルス感染対策

・ウイルスを入れない
・ウイルスがありそうなところに行かない、行かせない
・誰かが感染したら隔離する（被害を最小限に）
・大切な取引先に感染させない
・製造業はサプライチェーン攻撃に注意（中小→大企業）




※令和の時代、サイバーセキュリティ対策は取引条件の必須項目

引用：株式会社FFRIセキュリティ　Webサイト「サプライチェーン攻撃」
https://www.ffri.jp/special/Target-is-SME-Supply-chain-attack.htm

# クラウド型出口対策ソリューションの導入

**クラウド型**
**セキュリティサービス**

**②リモートコントロール**
**対策：出口対策**

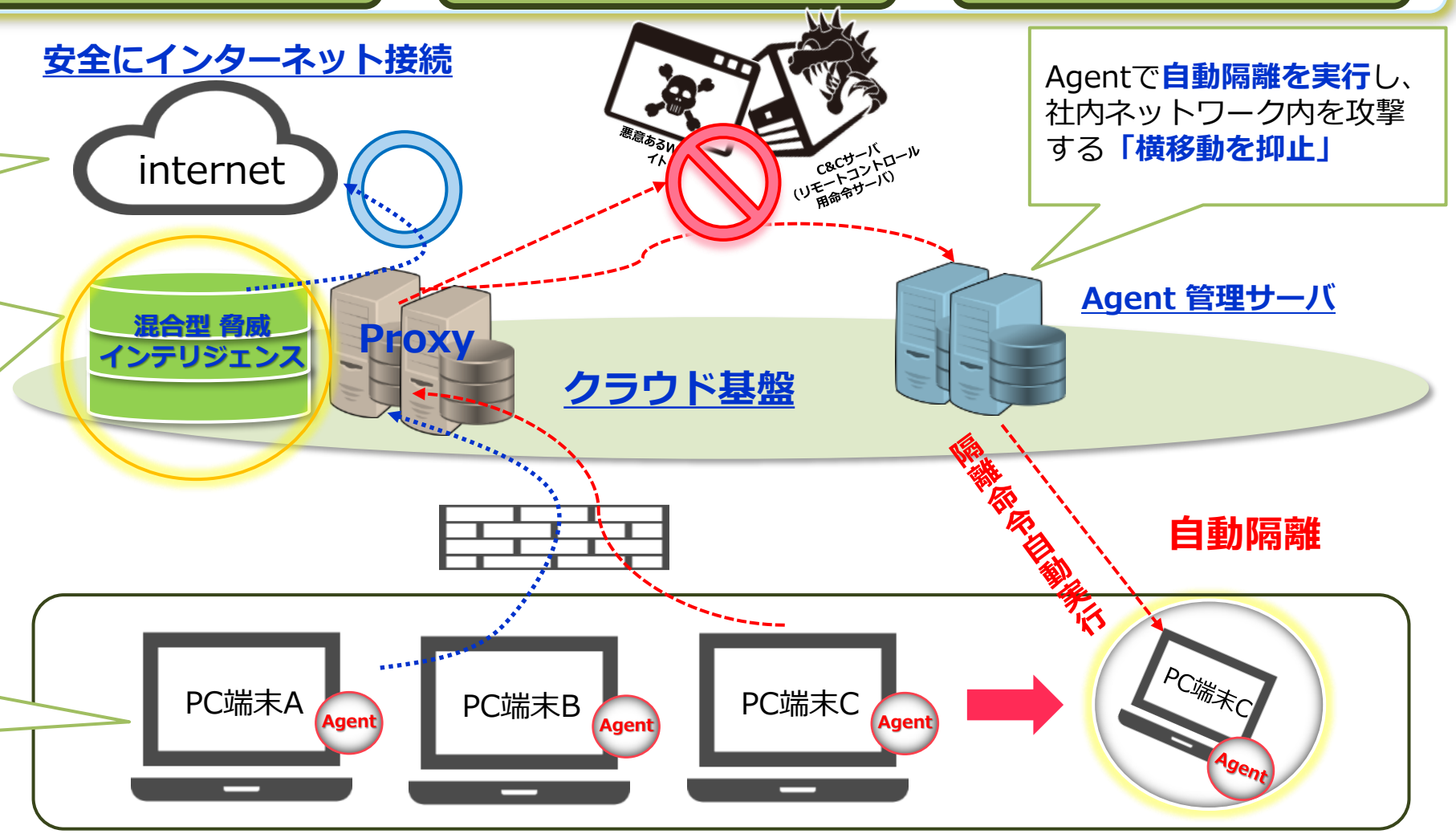
**③感染拡大**
**対策：内部対策**

**④目的遂行**
**対策：証跡調査/対処等**

安全と判断されたコンテンツのみアクセス可能となる

- **Secure Proxy**を提供、多段Proxyも可能
- 接続先のURLを脅威インテリジェンス（**300億の不正URLを保持**）に照会
- 通信の履歴情報が記録され、**どのようなサイトを閲覧したか、どの程度ブロックされたかが確認できる**

対象となる端末に出口対策ソリューションソフトを導入




※不正サイトアクセスをブロック、アクセス端末を特定、感染時はネットワーク隔離での対処までを自動実行

# クラウド型出口対策ソリューションの導入　（コスト＝時間≠リスク）

運用に手がかからず必要な対策

① クラウド型出口対策 セキュリティ機能 ✖ ② 日々（平時）の 運用支援サービス付 ✖ ③ 有事対応 （サイバー保険付帯）

平時（日々の運用）

**損害保険会社**

**インシデント受付**

- 受付対応
- 保険適用の判断

**運用支援サービス**

連絡

連絡

**運用支援**

- 状態確認/設定変更
- 月次レポート

**創ネット**

インシデント発生

連絡/問診

現地入館

有事（保険適用時）

有事対応（サイバー保険）

連絡

**インシデント対応**

- 24時間365日受付（TEL/mail）
- お客様へのご連絡(TEL/mail)
- ログ調査

**現地駆け付け支援**

- 駆付け人員手配
- 日本全国駆付け
- 現地対応支援

**解析**

※緊急事態が起きても安心（経営＝リスク回避＝安心）

# 導入のメリット（経営面）

・サイバーセキュリティ専任者がいなくても最新の運用が可能
　＝人件費、採用、コストの削減
　　※24時間365日サポート

・月次レポートの見える化により社員の意識が向上
　＝情報漏洩リスクの低減

・万が一、インシデントが発生しても相談できる安心感
　＝保険付で初動対応が可能
　※他の保険を見直してでも、サイバー保険が必要

・心配なく在宅ワークが可能
　＝優秀な人材の流出防止

・大切な取引先に迷惑をかけない
　＝商品・サービス以外での信頼向上


（導入事例）

## 創ネット株式会社 様

- 過去に複数回のサイバー攻撃を経験
- サイバーセキュリティはサプライチェーンの重要事項
- 月次レポートによる 見える化 は社員の意識向上にも最適

創ネットは、ファクトリオートメーションを提案するエンジニアリング商社です。1950 年の創業以来、社会インフラやものづくり工場の自動化のご支援を行っています。機械ができることは機械に任せ、人はより創造的な仕事を行い、より良い社会をつくるため、新しい商品や技術に加えて企業間の知恵のネットワークを構築し、新たなソリューションを提供しています。

〒812-0021
福岡県福岡市博多区築港本町６－３
https://www.sonet.ne.jp/

### セキュリティ専任者がいなければ運用は難しい

私たちはファクトリーオートメーションやロボットの専門会社です。工場の生産工程や品質検査に関しては誰よりも詳しいと自負しています。当然、社内にパソコンや IT に詳しい社員は大勢いるものの、一方で、セキュリティの専門業者ではありませんから、その方面にはうといと言わざるを得ません。つまり、通常の業務を行いながら、セキュリティに関する対応も掛け持ちで行っています。そのため、セキュリティに関する何らかのトラブルが発生すると社内が騒然となります。また、インシデント発生時に協力会社に依頼をしても、トラブル対応をあらかじめ予約しているわけではありませんから、対応に時間を要して復旧まで時間がかかってしまいます。だからといっ

### 直面していた課題と解決に向けた対策

従来より、当社ではウイルス対策ソフトを全端末に導入しており、それで安心していました。ところが、聞くところによるとマルウェア感染の 80% 以上は標的型メールに含まれる不正なリンクをクリックすることで、新型ウイルスをダウンロードするものだと聞いて驚きました。ウイルス対策ソフトはあらかじめ登録しているパターンファイルに一致する既知のウイルスに対しては有効に働きますが、未知の（新型の）ウイルスに対しては残念ながら全くお手上げだと判ったからです。

当社でも 2020 年 8 月頃からエモテットに感染した取引先からのメールを多数受信しています。また、残念ながら当社の社員も感染してしまい、なりすましメールを取引

創ネット株式会社
代表取締役
小口 幸士氏

8月度月次レポート

[redacted] Gateway
Monthly詳細レポート
■ブロックしたURL･ファイル･カテゴリのアドレス一覧
※http(s)はhxxp(s)に変換

ブロック種別 URL： URLのブロックを示す
ブロック種別 FILE： FILEのブロックを示す
ブロック種別 CAT： CATEGORYのブロックを示す

| 日時 | URL | ブロック種別 | カテゴリ | ホスト名 | クライアントIP |
|---|---|---|---|---|---|
| 2021-08-03 火 09:11:53+09:00 | hxxps://js.users.51.la:443 | URL_BLOCK | マルウェアサイト | [redacted] PC;chrome.exe | 192.168 [redacted] |
| 2021-08-03 火 09:11:56+09:00 | hxxps://js.users.51.la:443 | URL_BLOCK | マルウェアサイト | [redacted] PC;chrome.exe | 192.168 [redacted] |
| 2021-08-10 火 10:47:07+09:00 | hxxps://js.users.51.la:443 | URL_BLOCK | マルウェアサイト | [redacted] PC;firefox.exe | 192.168 [redacted] |
| 2021-08-10 火 10:47:09+09:00 | hxxps://mzzvo.kenco.xyz:443 | URL_BLOCK | フィッシング詐欺/その他詐欺 | [redacted] PC;firefox.exe | 192.168 [redacted] |

# 導入のメリット（運用面）

こちらに意識が無くても、異常なアクセスを数回行っているとお知らせしてくれる。
＝早期対処が可能

Subject: 2021-08-30（月） 週異常性確認について
Date: Mon,
From: 運用支援サービス サポート窓口 <servicedesk@>
To: @sonetnet.co.jp <@sonetnet.co.jp>
CC: 技術担当ML <tech@運用支援サービス サポート窓口 <servicedesk@>

創ネット株式会社　ご担当者様
　平素より大変お世話になっております。
運用支援サービスでございます。
　ブロック数状況から気になる点を確認しましたのでご報告致します。
ご確認のほどよろしくお願い致します。
　コンピュータ名：KOJI_OGUCHI　　IP： 192.168. ブロック数 ：14　時間：2021-08-27 金 14:15:40 ～ 2021-08-27 金 14:16:34
URL_BLOCK：hxxps:// net:443
詳細：コンピュータ名 PCにて、マルウェアサイトのURLブロックが14回ありました。
必要なご対応：脅威による通信を切断済みですので、今回の通知による対応は不要です。

以上、何卒よろしくお願いいたします。

# 導入のメリット（運用面）

月次レポートの共有で効果の見える化
＝月一回のサイバーセキュリティに対する意識付け

| | アクセス件数 | URLブロック数 | FILEブロック数 |
|---|---|---|---|
| 1月 | 2,977,695 | 37 | |
| 2月 | 3,102,701 | 11 | |
| 3月 | 3,624,227 | 7 | 9 |
| 4月 | 3,334,401 | 9 | |
| 5月 | 3,286,738 | 15 | |
| 6月 | 4,117,019 | 81（70/15） | |
| 7月 | 3,775,068 | 62（50/12） | |
| 8月 | 3,775,068 | 62（15/14/33） | |

赤文字は特定端末による複数回ブロック

# まとめ

もし、社内のPCがウイルスに感染し、
大切な取引先に迷惑をかけたらどうしますか？

最後に　**地域**のミカタとして、**地域**の皆がサイバー被害に遭わないように


被害に遭っても相談できる仲間がいますように

# ご清聴ありがとうございました


ネットワークとオートメーションで心豊かな社会の実現に貢献します

創ネット株式会社