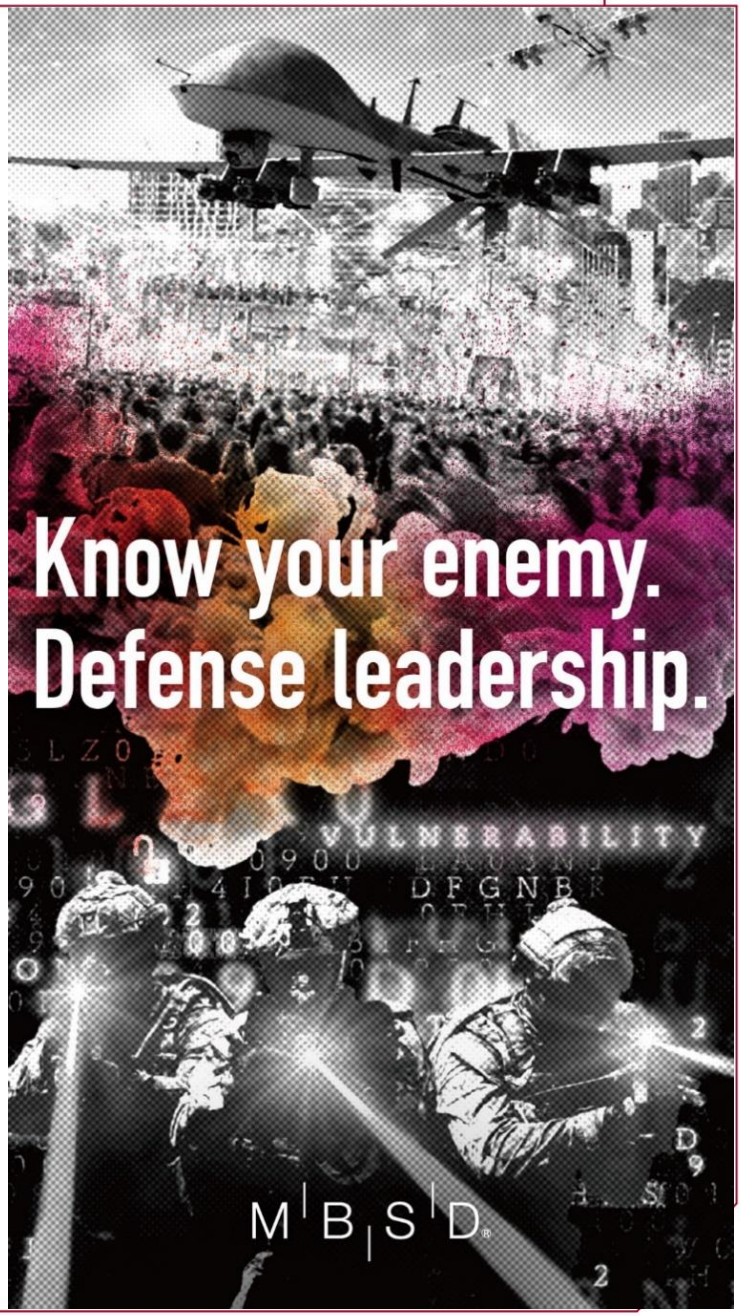
中小企業向けセキュリティ対策とサイバー保険



２０２１年９月２８日

関原　優　（Masaru Sekihara）

三井物産セキュアディレクション株式会社
コンサルティングサービス事業本部長 兼 公共事業部長
情報処理安全確保支援士（第000073号）

三井物産で情報セキュリティ専門会社である三井物産セキュアディレクションの設立に携わる。
20年程、IT・サイバーセキュリティのサービス事業に従事し、SOC構築、サイバー攻撃分析、
疑似攻撃によるWebサイトやネットワークの診断、自社SIEMなどのセキュリティツール開発、
官公庁やグローバル企業等に対するセキュリティコンサルティングなどを手掛ける。

配下部門には１５０名超のコンサルタント・セキュリティ技術者（高度なサイバー攻撃をログなどから発見するThreat Hunter、マルウェア解析技術者など）を擁し、顧客組織のセキュリティ対策にあたっている。

【特許】

- 米国特許_第10264002号/国内特許_第5996145号 発明者
  概要:暗号化時のファイル特性を利用したランサムウェア検知・防御技術
- 国内特許_第5955475号 発明者
  概要:自己多重起動抑止特性を利用したマルウェア感染防御・無効化技術
- 国内特許_第6219550号 発明者
  概要:ファイルマッピングによる暗号化に対するランサムウェア検知・防御技術

【著書】

訴訟・コンプライアンスのためのサイバーセキュリティ戦略/NTT出版 など

サイバー攻撃の蔓延

はじめに　～昨今の状況～

昨今、世界中でサイバー攻撃が多発し、多数の企業・組織が被害に遭っていることが連日報道などで明るみになっています。

サイバー攻撃を完全に防ぐのは困難

世界中でサイバー攻撃が蔓延！
大企業でも多数被害に遭っている状況

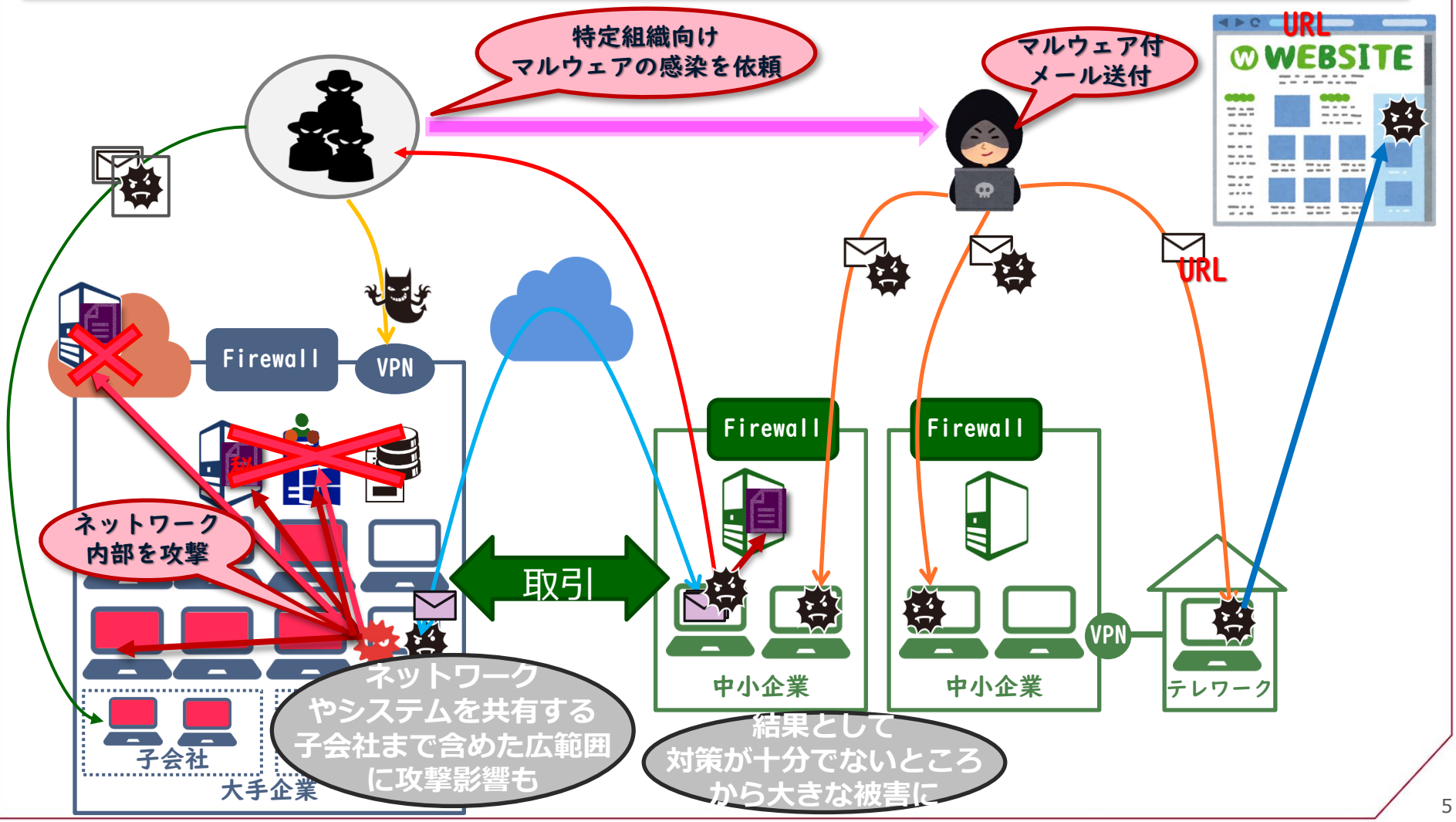
サイバー攻撃は情報搾取だけでなくシステム停止/破壊を引き起こす
工場や生産システムの停止など
ビジネス影響の甚大化

サイバー犯罪の高利益化
世界中で被害が拡大
想定被害額は毎年数千億円とも言われる
そして新たなマルウェア開発や
攻撃人材の採用へとビジネスが拡大

狙われるのは大企業だけではない
グループ企業や取引先など含めた
ターゲットと繋がりを持つサプライチェーンへの攻撃

サプライチェーンを狙うサイバー攻撃

ネットワーク・システム的、人的含め何らかの取引ややり取り関係を持つ企業・組織のつながりを狙って攻撃が行われる。自社ネットワークを守るだけでは不足、グループ企業や重要取引先まで含めた取り組みが必要となっている。



対策のための知識

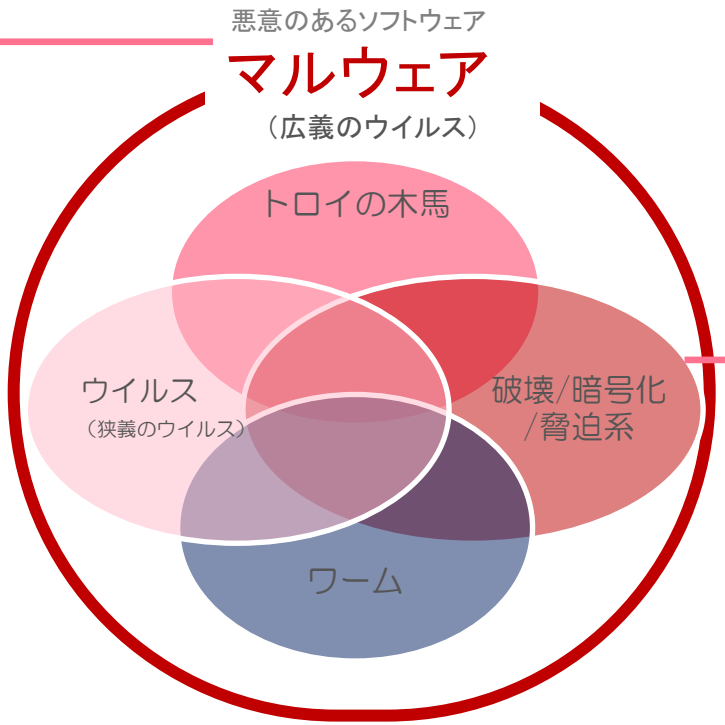
マルウェアとランサムウェア

2つの単語を組み合わせた造語

マルウェア ＝ Malicious Software
和訳：悪意のある　ソフトウェア

2つの単語を組み合わせた造語

ランサムウェア ＝ Ransom Software
和訳：身代金　ソフトウェア



近年脅威が拡大

ランサムウェアは
マルウェアの一種

ランサムウェアとは

昨今は企業等のネットワークを侵害しシステムの管理者権限などを奪取してからランサムウェアで攻撃するケールが増えている。

ランサムウェアは攻撃手段の一つであり、ネットワークに侵入するサイバー攻撃全体を考慮する必要があります。

サイバー攻撃により暗号化したファイルの復元と引換に身代金を要求

攻撃者の目的は
金銭を得ること

昨今、多重の脅迫を行う手口へと展開

1．暗号化したファイルの復元と引換に身代金を要求

2．ファイルを暗号化するだけでなく、搾取した情報を暴露すると脅迫し暴露しないことを引換に身代金を要求

3．さらに身代金を支払うまで、Webサイトに大量の通信を発生させてWebサイトが閲覧できない状態にするDDoS攻撃をしかけて脅迫

4．さらに搾取情報が暴露された際に被害者となる顧客へ連絡して脅迫

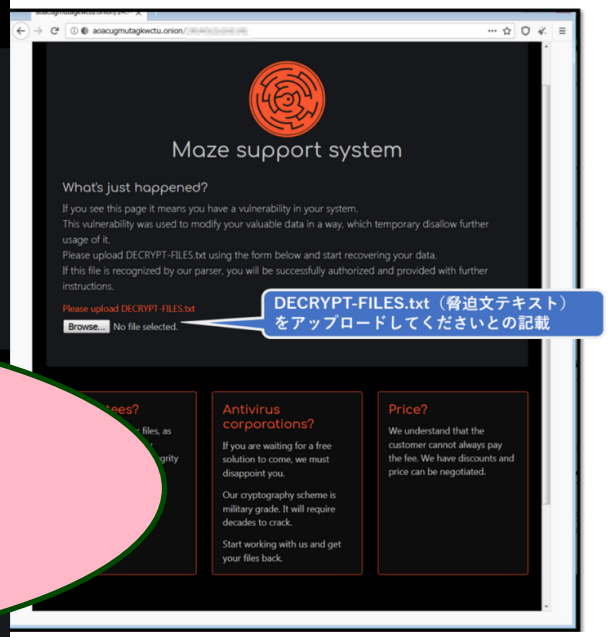
ランサムウェアによる暴露：攻撃グループのリークサイト例（MAZE）

ポイント

企業がランサムウェア感染や
漏洩を公表していなくとも脅迫のために
一部データを公開されて被害が明るみに

脅迫文に記載されたURLにTorブラウザでアクセスするとどうなるか？

▼以下のようなMazeランサムウェアのサポートページが表示される



サポートシステムが用意され、チャットによるサポートや一部ファイルのお試し復号機能などが提供されている。

※MAZEのサイト：情報を搾取したと表明、一部情報を公開している対象などが列挙されている。

2020年7月 トヨタ自動車と取引のある、金型設計・製造などを手掛ける愛知県のTMW社がサイバー攻撃を受けて上記MAZEサイトで公表されたことを各種メディアで報道された。

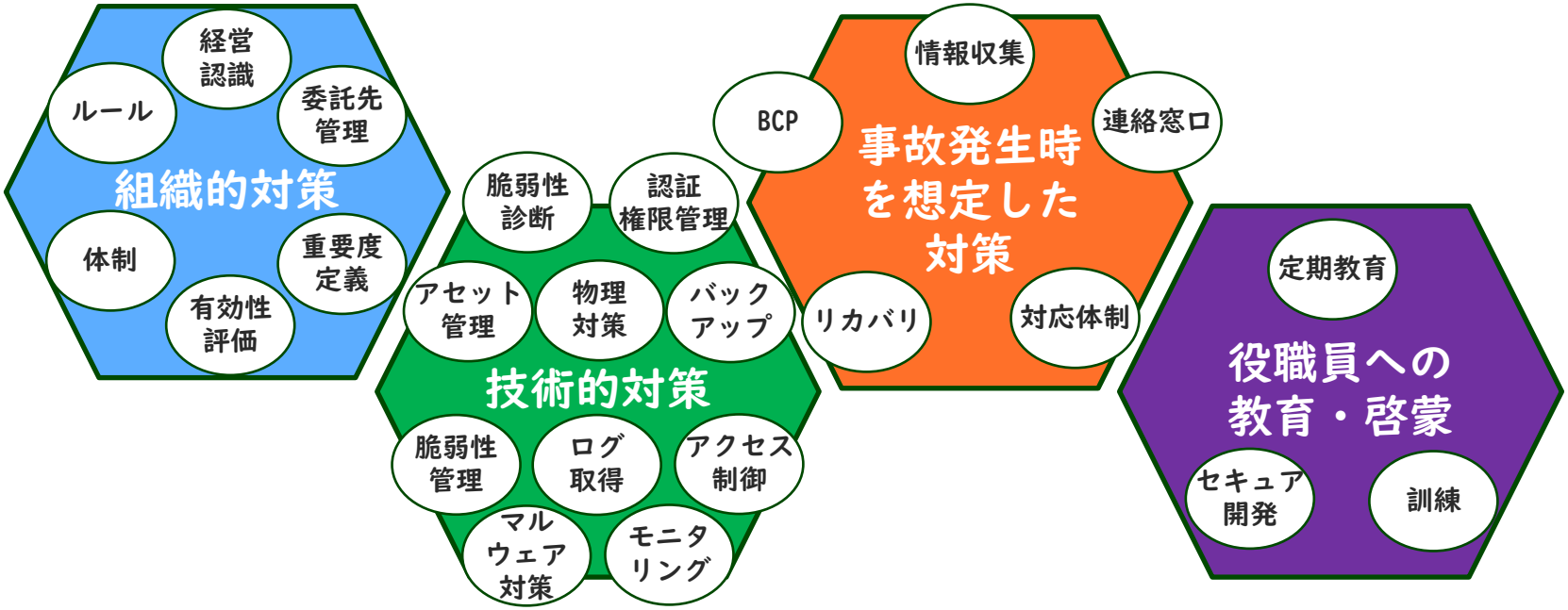
出典：https://www.nikkei.com/article/DGKKZO61620670W0A710C2TJ2000/

※MAZEは既に活動を停止していますが、同様のリークサイトを有する攻撃組織が数十存在

中小企業向け対策

求められるセキュリティ対策

必要なセキュリティ対策は、経営層、IT/セキュリティ担当者、コーポレート/営業の担当者、一般役職員など内容も対象も多岐にわたり、対応は容易ではありませんが、最低限の内容でも、継続的に実施し続けていく必要があります。



大企業などはグループ会社や取引先にこのような多岐にわたるセキュリティ対策をどの程度対応できているか把握するところから、不足している部分については対応を求めていく流れになってきていますが、予算も人員も限られるようなグループ会社や中小企業などでは、コスト的にも人員リソース的にも**セキュリティ対策を全般強化していくことは難しい**ことが多々あります。

※上記は必要なセキュリティ対策の例であり全てではありません。

中小企業向けのセキュリティ対策として

組織的対策

最重要

・**経営層や管理職の方々が自社/組織リスクを理解して意識する。**
自社のビジネスリスクを認識することが重要です。
セミナー受講やセキュリティ対策に取り組まれている中小企業の方々の話をお聞きして自分事で考えてみること、経営層の方々に考えて頂ける様に情報共有や話を聞く場を設けることを推奨します。

※コストをかけて製品を買うことではなく、自社に必要なことが何か考える/考えさせることが重要
他社よりセキュリティ対策が不要かもしれないし、もっと必要かもしれない

・**担当者をアサインする。（兼務でも良い）**
情報収集するにも、連絡を取り合うにも、意識を持ってもらうためにも担当者を決めておくべきです。窓口を地域のセキュリティコミュニティ等に共有しておけば、情報を得ることもできます。

技術的対策

・最低限の入口対策実施（ファイアウォールとアンチウィルス）

家の扉や窓を開けっぱなしでは犯罪者が入りやすくなるのと同様に、
最低限、扉をつける、鍵をかけるなどの対応をすべきです。

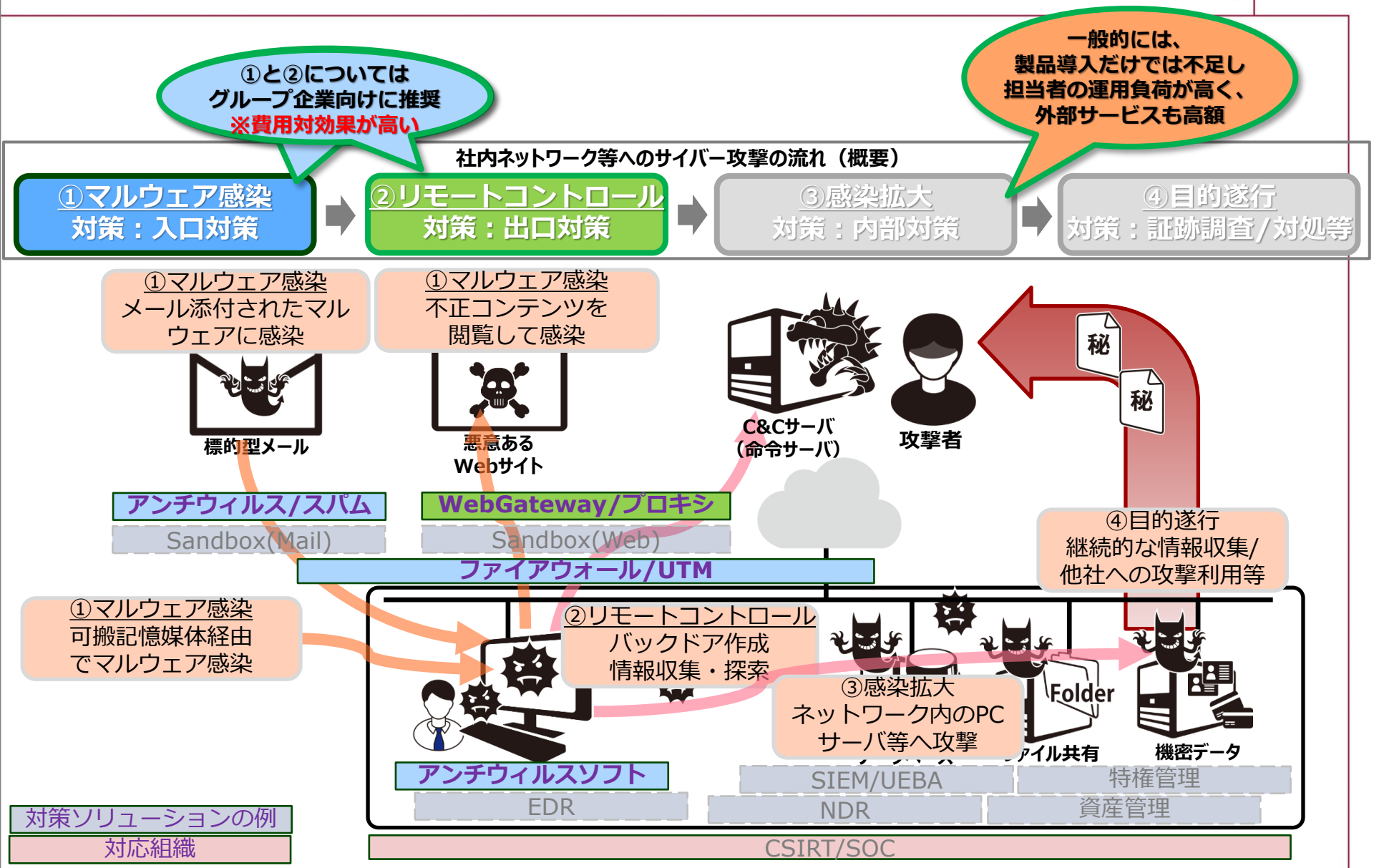
多くの企業様でファイアウォールとアンチウィルスはほぼ導入済ですが、
もしも不足している場合は導入を推奨します。
※導入しても攻撃は対策をすり抜けますが、それでも一定防いでくれる
　ため費用対効果が高いです。

・最低限の出口対策と通信履歴の保管（ウェブゲートウェイ/プロキシ）

攻撃にはウェブ通信が最も良く利用されます。
防御にも有効ですが、万が一の調査の際にPCやサーバのログは攻撃者に
消去されたり、履歴が残らないように攻撃されるため調査が困難になります。
取引先への報告などのためにも通信履歴（ログ）の保管を推奨します。

クラウドサービスなどではログ保管されている場合もあり保管期間を確認下さい。
社内などにシステムとして導入（オンプレミス）されている場合はログ取得設定
と保管環境を確認下さい。
※保管ログが社内への攻撃により消去されない環境

入口対策・出口対策の補足



事故発生時を想定した対策

・**最低限、事業継続に必須なデータを攻撃されない様に保存**

昨今は、ランサムウェアによりシステム停止に加えて、ビジネス継続に必要なデータがバックアップごと暗号化されて利用不可能になるケースがあります。データ復旧が困難となり、決算や継続取引に影響を及ぼすケースも多々あるため、最低限消失した場合に事業影響がある取引データなどを、サイバー攻撃を受けないオフライン/書換不可能な状態で継続的に保存しておくことを推奨します。

役職員への教育・啓蒙

・サイバーセキュリティの話を継続的に話す/定期教育の実施

経営層からの社内通知や、集合会議での管理職からの話でも、
時折、話題として取り上げることを推奨します。

無償セキュリティセミナーへの参加、公開資料の説明などからでも、
年１回以上、社内セキュリティ教育を実施し、定期的に教育を
実施していると言える状況にしておくことを推奨します。

※上記は必要なセキュリティ対策の例であり全てではありません。

中小企業向けのセキュリティ対策として

■まとめ

組織的対策

- **経営層や管理職の方々が自社/組織リスクを理解して意識する。**
  自社のビジネスリスクを認識する。
- **担当者をアサインする。（兼務でも良い）**

技術的対策

- **最低限の入口対策実施（ファイアウォールとアンチウィルス）**
- **最低限の出口対策と通信履歴の保管（ウェブゲートウェイ/プロキシ）**

事故発生時を想定した対策

- **最低限、事業継続に必須なデータを攻撃されない様に保存**
  ランサムウェア攻撃などにより事業影響がある取引データなどを、
  サイバー攻撃を受けないオフライン/書換不可能な状態で継続的に保存

役職員への教育・啓蒙

- **サイバーセキュリティの話を継続的に話す/定期教育の実施**
  無償セキュリティセミナーへの参加、公開資料の説明などからでも、
  年１回以上、社内セキュリティ教育を実施し、定期的に教育を
  実施していると言える状況にしておく

サイバー保険について

■リスクへの備え

・**しっかりと対策を継続していれば、被害に遭う確率や被害の拡大を低減させることができます。**

・それでもサイバー攻撃を防ぎきることが出来ない状況下、**被害に遭ったときにどう対応するかもポイント**になります。

■サイバー保険によるリスク移転の検討

大企業等でもサイバーリスクの高まりに対応して、サイバー保険へ加入または既存の損害保険に対応する補償を追加あるいは、検討されているところが多数あります。

昨今のリスク状況では、中小企業でも同様にリスク移転の検討を行う事は有用です。

サイバー保険に入るかどうかではなく、**リスクマネジメントとして、リスク移転の検討とその結果としてリスク保有して対応または一定のリスク移転をしていることをしっかりと、取引先などへ説明できる状態にしておくことが重要です。**

■検討の例

保険により補償される費用の例

- 事故対応費用
  - 事故原因や影響調査費用、復旧・再発防止などの対応への備え
- 損害賠償費用
  - サイバー攻撃により取引先への賠償が必要な場合などへの備え
- 利益損害費用
  - サイバー攻撃でシステム停止した場合など、喪失した利益や収益減少などへの備え

特に事故原因調査や影響調査には、数百万円以上の費用が必要な場合が多い

少なくとも以下のリスク移転を検討しておくと良い

- 万一の事故調査費用が捻出可能か
- システム停止時の業務継続/復旧費用が捻出できるか

地域のセキュリティコミュニティ

様々な企業のセキュリティ対策を支援する中で

セキュリティ対策を強化
中小規模から大規模まで様々な企業グループ支援の中で聞いてきたこと

具体的に何をすればいいのか？

必要なことは理解しているが、対策にかけられる費用が。。

セキュリティどころかITに詳しい担当もいない。

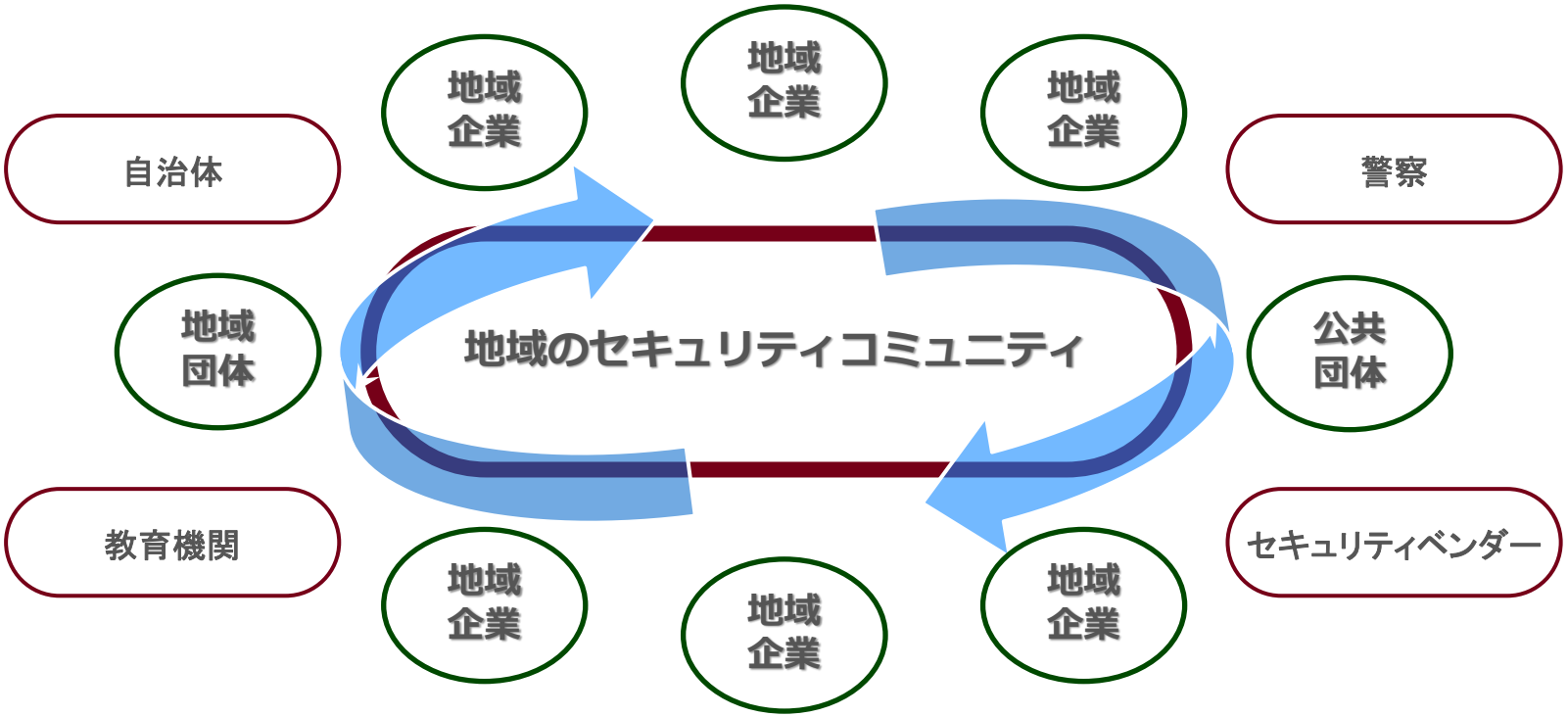
近くにセキュリティベンダーなど相談できる相手がいない。

難しい技術話はわからない。

など・・・・

地域のセキュリティコミュニティ

個々の企業・組織だけで対策を強化するのは難しい。
手洗い・うがい・マスク着用の様なところから、身近に聞ける関係先を持ち、
できることから実施、協力できるコミュニティの形成が進みつつある。



体験の共有	交流	情報の共有
・自分のできたこと/できなかったこと ・同業種、取引先同士のビジネス上のセキュリティ要求状況	・企業同士の交流から新たなビジネスも ・企業と学生の交流から新たな雇用も	・費用をかけずにできること ・費用をかけて実施したこと ・国や公共団体、セキュリティベンダーなどの有用情報

福岡県警様からの情報共有

コロナ禍におけるサイバー空間の脅威

福岡県警察 CYBER SECURITY
FUKUOKA POLICE
解明する，対処する，育てる，守る

新型コロナウイルスの感染防止のため、テレワークの導入が進む中、セキュリティが確保されていない自宅等のテレワーク環境や、テレワーク用のソフトウェア及びVPN機器の脆弱性等を狙ったサイバー攻撃が発生しています。

ランサムウェアによる被害が深刻化・手口の悪質化

最近の事例ではデータの暗号化のみならず窃取を敢行し、対価を支払わなければ当該データを公開するという二重恐喝（ダブルエクストーション）を行うなど、より悪質なケースが認められています。

また、犯行に用いられるランサムウェアやそれらを用いた二重恐喝の手法そのものが闇サイト上で商品として販売されるなど、これらのより悪質な手口の拡散も見られます。

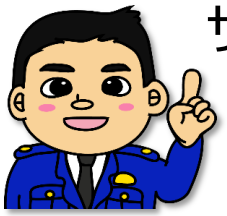
なりすましメールや添付ファイルに注意する
正規サイトからアプリケーションをインストールする
エンドポイントなどのセキュリティ機器の導入

福岡県警からのお願い

福岡県警察 CYBER SECURITY 解明する，対処する，育てる，守る

企業の皆様へ
サイバー犯罪の被害は**警察へ通報**を

ランサムウェア や 不正アクセス は 犯罪 です



サイバー犯罪の実態を明らかにし、被害を拡大させないためには
被害を潜在化させないことが重要です。

このような被害に遭われたら、**最寄りの警察署**へご相談ください

企業の皆様からの情報提供が
サイバー空間の安全
につながります

警察へ寄せられたサイバー犯罪に関する情報を分析し、事件捜査を行うほか、被害企業における対策に必要な情報の提供・助言、他の企業等への被害拡大を防止するための注意喚起等の被害防止のための取組を行っています。

福岡県警サイバー犯罪対策課SNS

福岡県警察
CYBER SECURITY
解明する，対処する，育てる，守る

fukkei_cyber

@fukkei_cyber

最後に

サイバーセキュリティは特別な難しいものと考えない。

感染症と同様に、サイバー攻撃も蔓延しています。

世の中で起きていることを知り、リスクを自分ごとと捉えられれば
費用の大小問わず、自身で対策や対応することは、普段からやっていることと変わりません。

地域の方々との交流を通して、取り組まれている対策を把握したり、
公開情報などを活用して社内教育をしたりなど、
できるところから取り組んで頂ければ幸いです。

三井物産セキュアディレクション株式会社