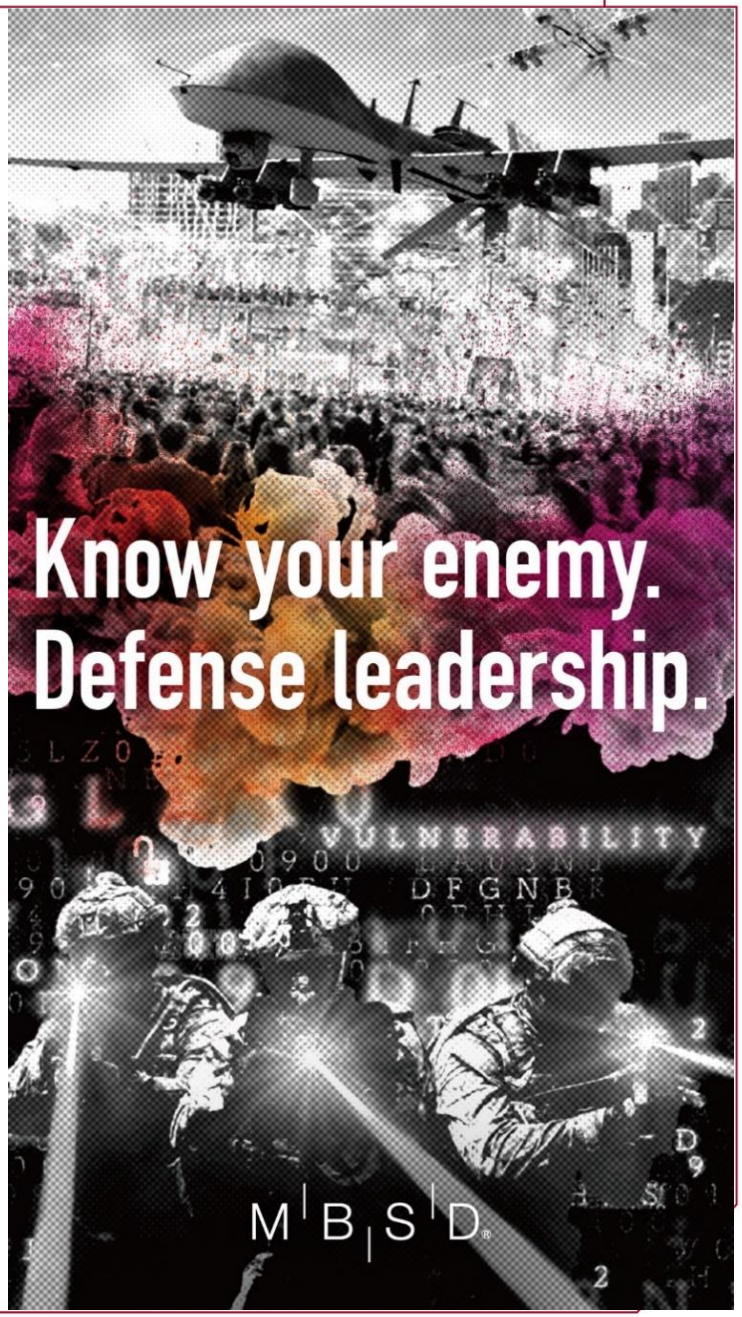
中小企業の
サイバーセキュリティ対策
＜医療関連分野＞

２０２１年１１月２２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
執行役員（コンサルティングサービス事業本部・公共事業部管掌）
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11159541号(2021年10月26日)/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
- 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

【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

はじめに

昨今、世界中でサイバー攻撃が多発しています。
サイバー犯罪による被害額は毎年数千億円にも上ると言われており、サイバー攻撃により窃取した身代金や、詐欺により奪った金銭は、さらに犯罪組織の活動を拡大させるという流れが活発化していると言えます。

規模や業種を問わず、あらゆる企業がサイバー攻撃の脅威に晒され、システムやネットワークの停止に伴う業務停止、大企業等の取引先への侵入の踏み台となり、さらには信用失墜や損害賠償といったリスクを抱える可能性があります。

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

サイバー攻撃被害例（医療関連）

・2018年10月 宇陀市立病院（奈良県宇陀市）- ランサムウェア感染
電子カルテシステムがランサムウェア感染し約２日間使用できない状態に。
非管理のインターネット接続機器が接続されたことが原因である可能性も。

・2019年5月　佐世保共済病院（長崎県佐世保市）- マルウェア感染
電子カルテシステムにつながるPC数台でマルウェア感染。
感染拡大防止のためにネットワーク停止し、新規患者の受入を中止。

システム停止

・2019年5月　多摩北部医療センター - マルウェア感染/メールアカウント乗っ取り
医師のPC・メールアカウントに対する不正アクセスあり。
当該医師は、患者や医療関係者ら3761件の情報等を有しており、流出の可能性も。
当該病院ではその他のPC数台でも感染判明。（EMOTETに感染していたことが判明）

・2020年9月 ドイツ - ランサムウェアで人の命が奪われる事件が発生
デュッセルドルフ病院の30台のサーバがランサムウェアにより暗号化され、救急患者を受け入れることができずに、30キロ以上離れた別の病院に搬送せざるを得なくなったために死亡したと報じられている。

・2021年10月　つるぎ町立半田病院（徳島県美馬郡つるぎ町）- ランサムウェア感染
電子カルテシステムがランサムウェア感染し復旧できない状態に。
10月末から現在も復旧の目途は立っておらず、予約

システム停止

その他、米国では2019年だけで764もの医療機関がサイバー攻撃の被害を受けたと報じられている。

サイバー攻撃被害例（医療関連）

・2020年、英国の医療機関の81%がランサムウェアに見舞われたとの情報

英オブレラ・セキュリティ・インダストリーズの調査によると、英国の医療機関の5分の4以上(81%)が昨年ランサムウェア攻撃を受けたとされる。

保健セクターの100人のサイバーセキュリティマネージャーを対象とした調査によると、英国の医療機関の38%がファイルを取り戻すために身代金要求を支払うことを選択したと言う。44%は需要の支払いを拒否したが、結果として医療データを失ったことを明らかにした。

この研究では、医療機関に対するサイバー攻撃のより広範な影響についても検討しており、回答者の3分の2近く(64%)が、サイバー攻撃のために組織が対人予約をキャンセルしなければならなかったと認めました。さらに心配なことに、65%はシステムに対するサイバー攻撃が人命の喪失につながる可能性があると考えています。

出典：https://www.infosecurity-magazine.com/news/healthcare-ransomware-last-year/

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

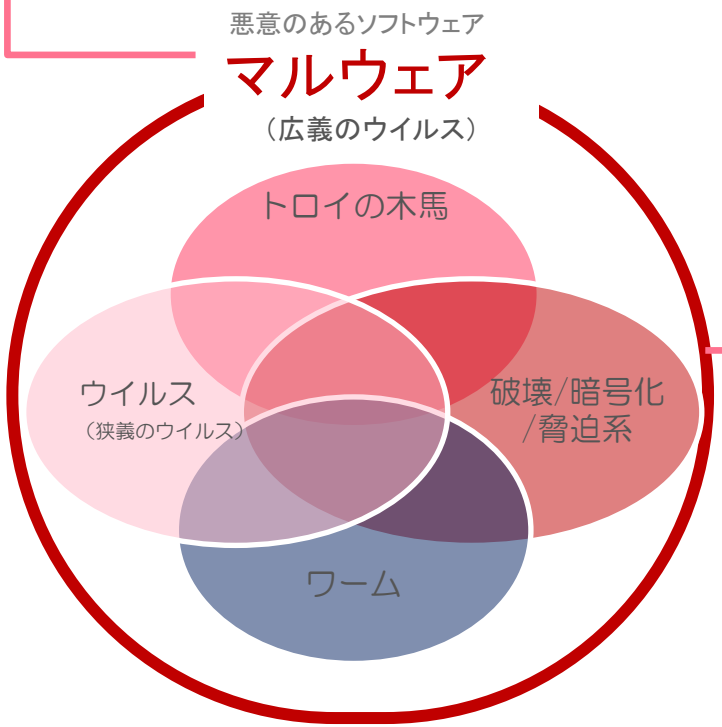
マルウェア ＝ Malicious Software

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スが増えている。

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

システム管理者権限での
ファイル暗号化でシステム停止や
感染被害抑止のためのネットワーク停止によって業務停止に発展する事案が多数！！！

攻撃者の目的は
金銭を得ること

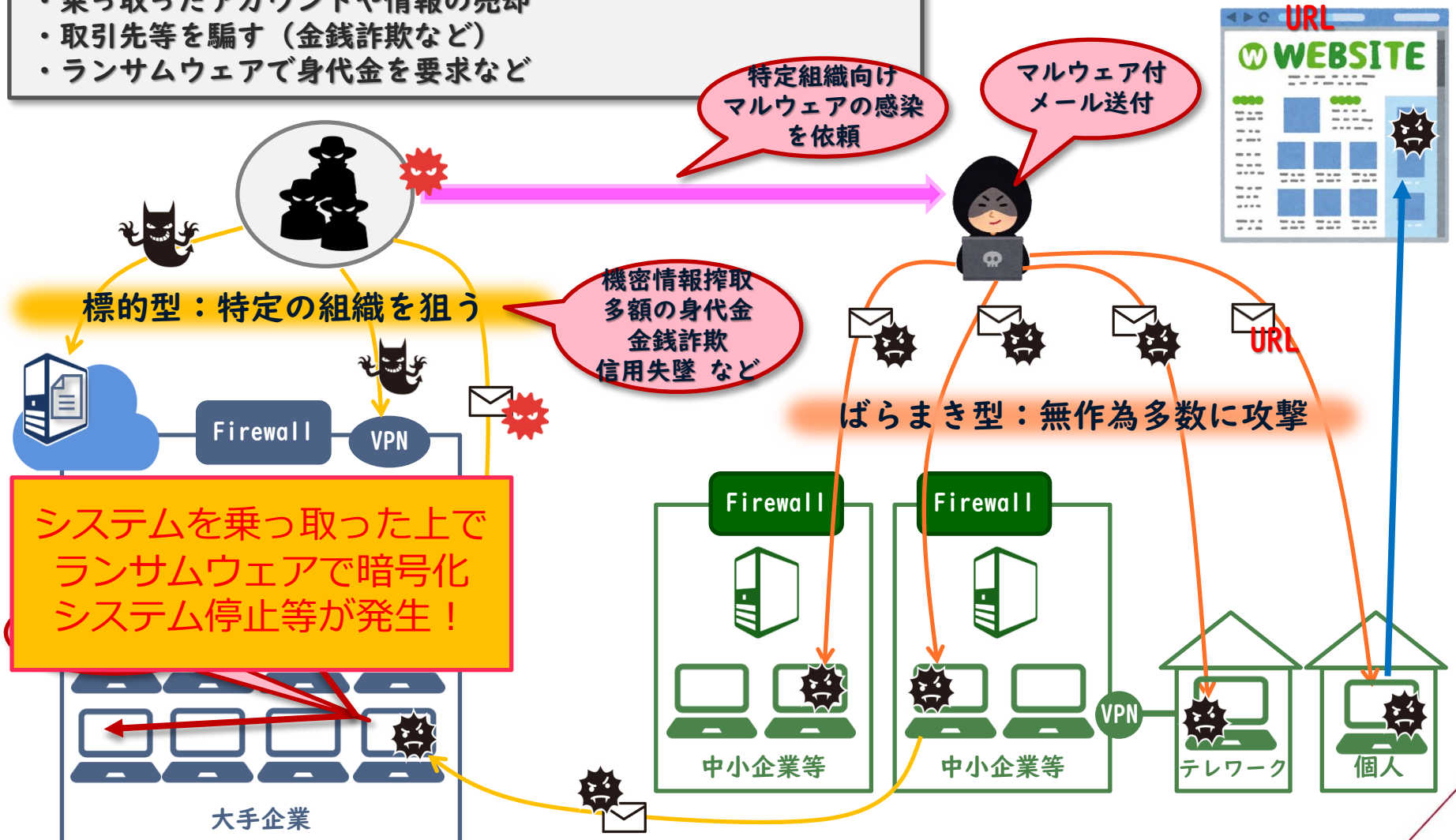
昨今、多重の脅迫を行う手口へと展開

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

サイバー攻撃の実態

サイバー攻撃は大企業だけを狙うものではありません。
様々な目的のため、無作為にもサイバー攻撃が来ます。

- 攻撃の踏み台（2次攻撃利用・標的の取引先情報搾取など）
- 乗っ取ったアカウントや情報の売却
- 取引先等を騙す（金銭詐欺など）
- ランサムウェアで身代金を要求など



ばらまき型攻撃の例（EMOTET）

EMOTET（エモテット）とは

感染したコンピュータからメール関連の情報を盗んで成りすまし、感染を拡大するマルウェア。
世界で最も危険ともいわれるほど世界中で猛威を振るった。

- JPCERT/CC - マルウエア Emotet の感染に関する注意喚起（2019年12月更新）
  https://www.jpcert.or.jp/at/2019/at190044.html
- IPA「Emotet」と呼ばれるウイルスへの感染を狙うメールについて（2021年11月16日 追記）
  https://www.ipa.go.jp/security/announce/20191202.html

2021年1月法執行機関等による対応で停止していましたが、
2021年11月活動を再開。今後大規模な攻撃に発展する可能性があります。

EMOTETに感染するとどうなるのか

●**取引先や顧客など連絡先とメールの内容**が窃取され攻撃者の元に送信される
→感染した本人だけでなく、やり取りした相手や組織内全てに影響が及ぶ

●感染端末に保存した**あらゆるパスワードや認証情報**が窃取される
→メールだけでなくコンピュータ内の様々な認証情報が漏洩する

●感染した社員を偽り、取引先やその他の外部組織に**大量の不審メールを送信**してしまう

●**他のマルウェアがダウンロード**され感染する可能性がある
→ 感染を拡大させたい意図の一つに、別のマルウェアへの多重感染がある
別のマルウェアや**ランサムウェア**による２次被害が将来突然発生する可能性がある。
海外ではEMOTETに感染した後、ランサムウェアをダウンロードしてくる事例多数有

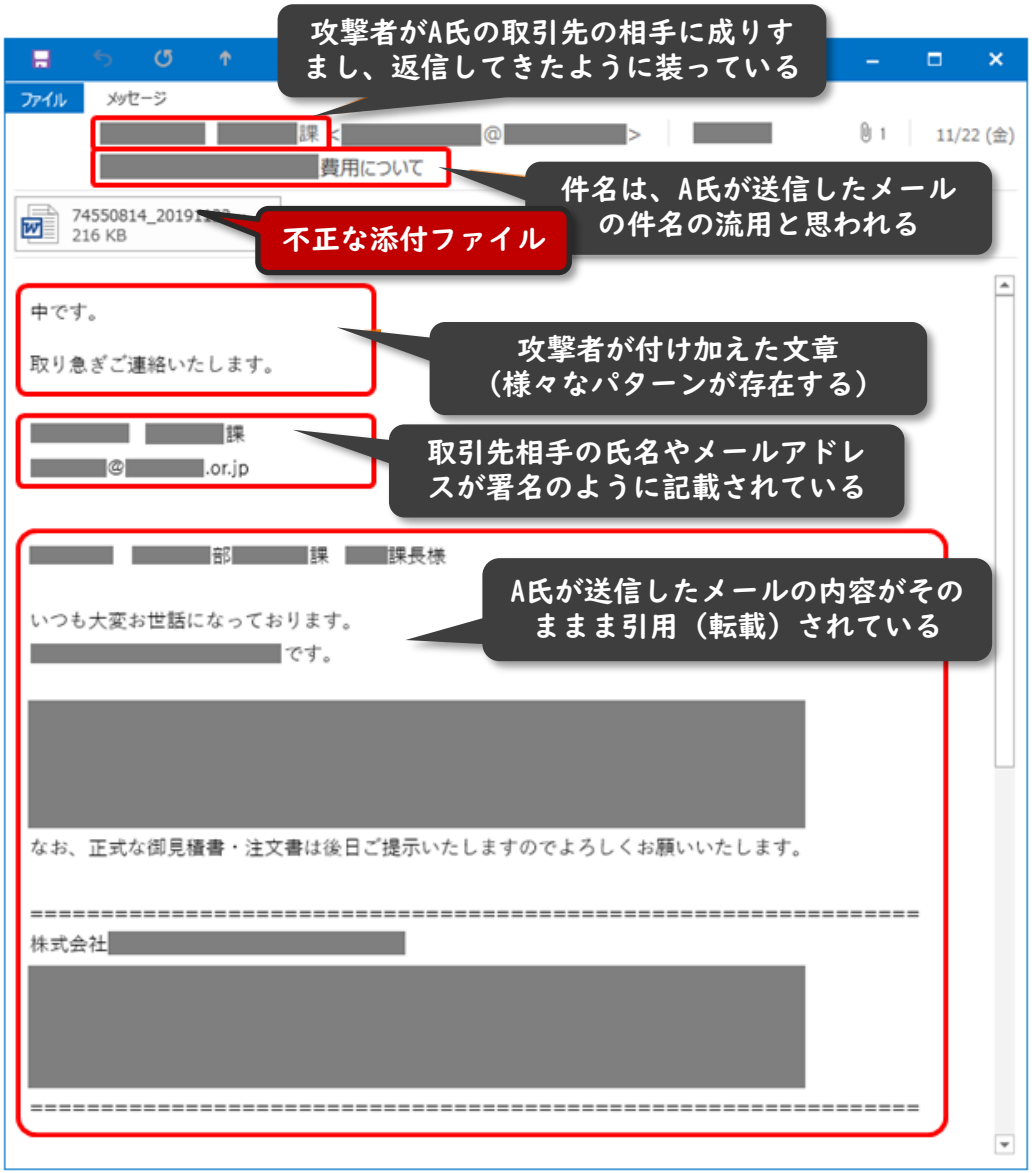
ばらまき型攻撃の例（EMOTET）

騙されやすく危険性が高い攻撃手口の例

正規のメールへの返信を装う手口

右図は、受信者（A氏）が過去に取引先に送信したメールを丸ごと引用され、取引先相手からの返信のように見える内容で、A氏へ送り付けられてきた攻撃メールの一例となる。

昨今は**パスワード付zipファイルを添付**してくる例も発生している。



画像引用元：
https://www.ipa.go.jp/security/announce/20191202.html

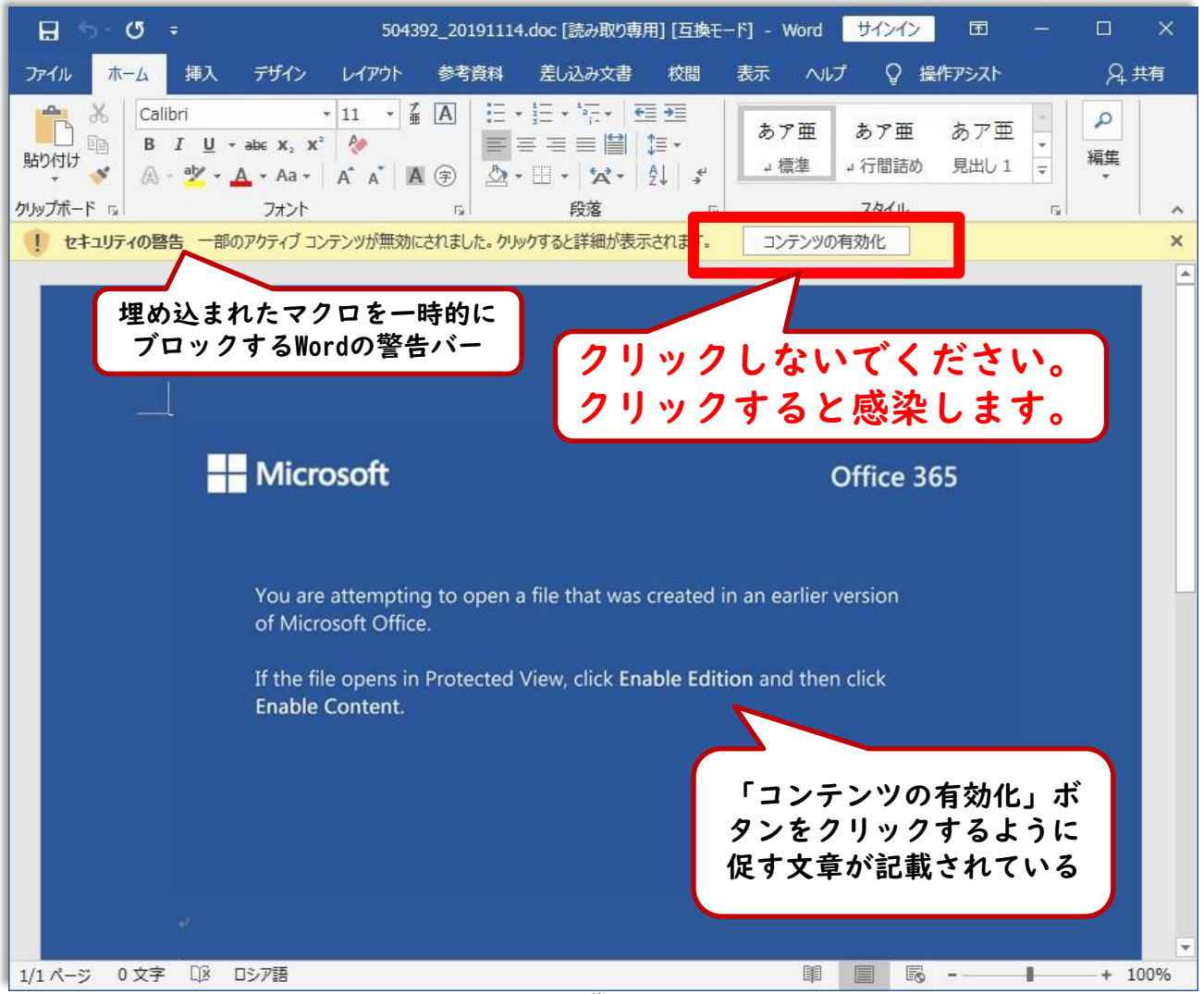
ばらまき型攻撃の例（EMOTET）

メールの添付ファイルまたはリンク先からダウンロードされる不正な文書ファイル

不正な文書ファイルには**マクロ**が埋め込まれており、標準の設定では文書ファイルを開いただけでは感染しない。

「コンテンツの有効化」ボタンを押すことで初めて感染する。

※文章ファイルの中身の記述については様々なパターンが存在するため一意ではない。

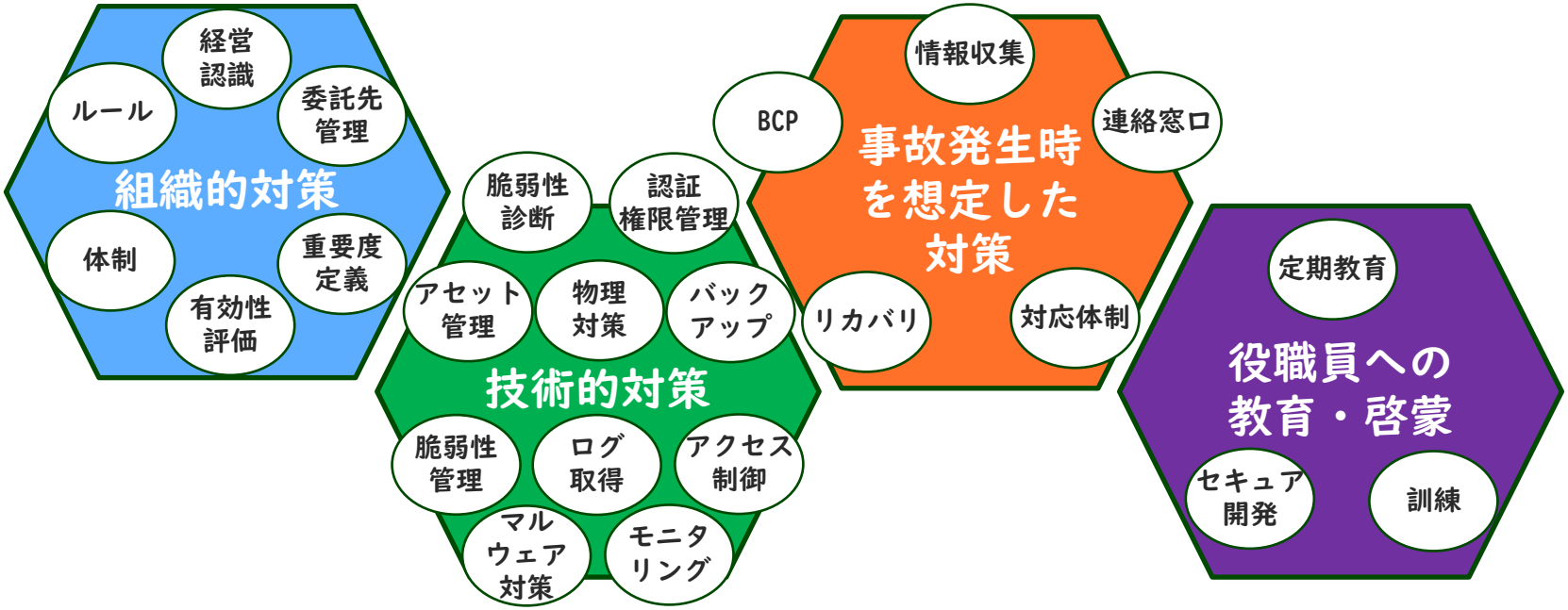


画像引用元：
https://www.ipa.go.jp/security/announce/20191202.html

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。

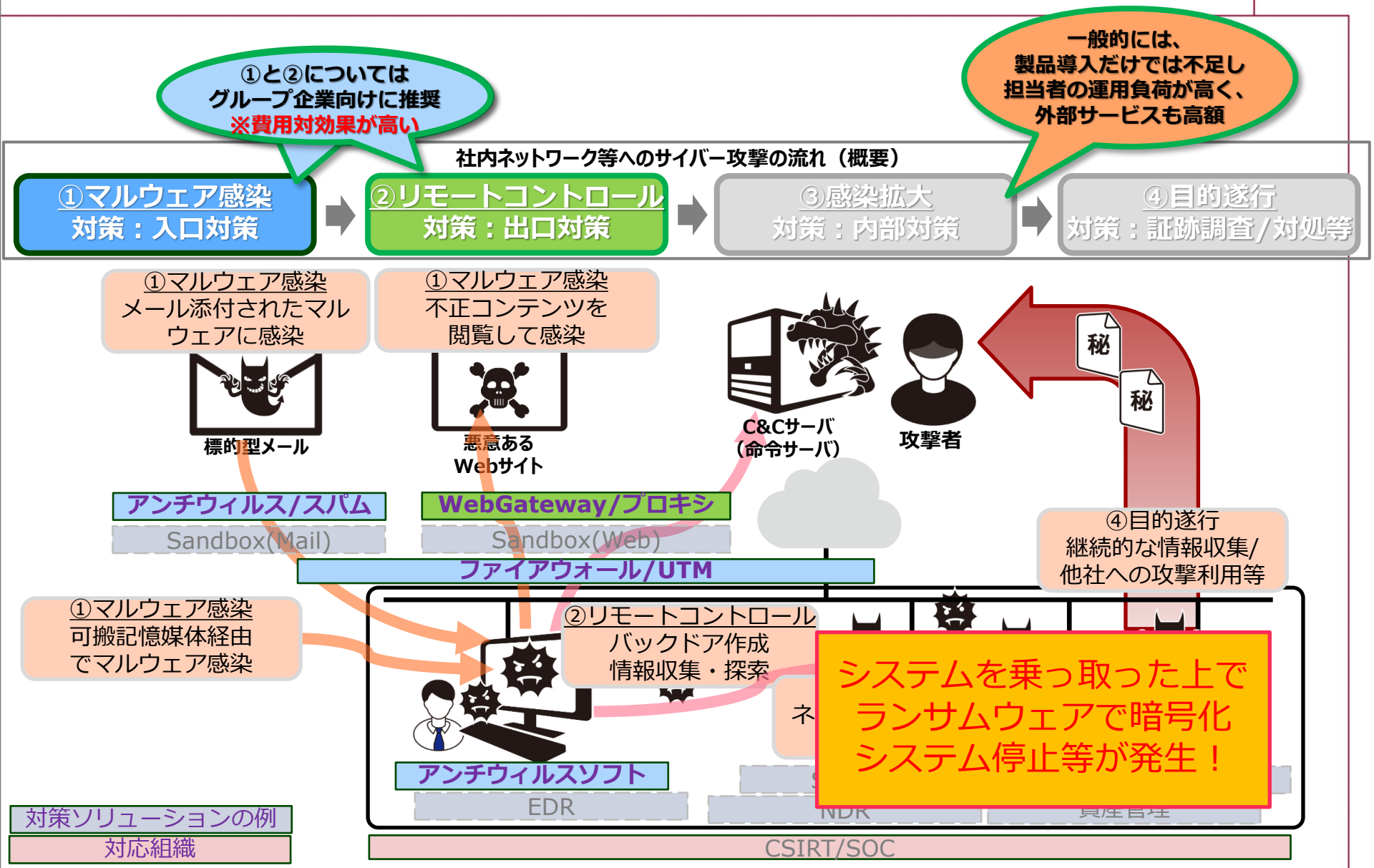
多くの企業様でファイアウォールとアンチウィルスはほぼ導入済ですが、
もしも不足している場合は導入を推奨します。
※導入しても攻撃は対策をすり抜けますが、それでも一定防いでくれる
　ため費用対効果が高いです。

・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。

※データだけでなくシステム自体を動作・復旧できないケースが多々あります。
バックアップデータからシステムの復旧が出来る状態を維持する必要がありますが、バックアップデータ自体も攻撃されてしまいます。

☞ **ポイント**

1．事業継続上、重要なシステム/データのバックアップを定期的に取得
2．バックアップ時のみ対象機器と接続（接続中は攻撃を受けるため）
3．複数の装置・媒体にバックアップ（バックアップ中の感染、汚染データでの上書きへ対応）
4．バックアップ妥当性の定期的な確認
　1） リストア時の有効性確認
　2） 新たな攻撃手法に対するバックアップ有効性確認
5．システムの再構築を含めた復旧計画の策定（サイバーBCP）
6．リストア時にネットワーク隔離状態、またOSがクリーンな状態でリストア可能なこと
　→データが安全でもOSが侵害済/アカウント搾取状態であるケースあり、継続攻撃を受けない状態にリストアする必要あり。

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。

万一のインシデントを想定した訓練も有効です。
もしインシデントが発生したらどう対応するかを組織内で話したり、
考えたりするところからが大切です。

※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

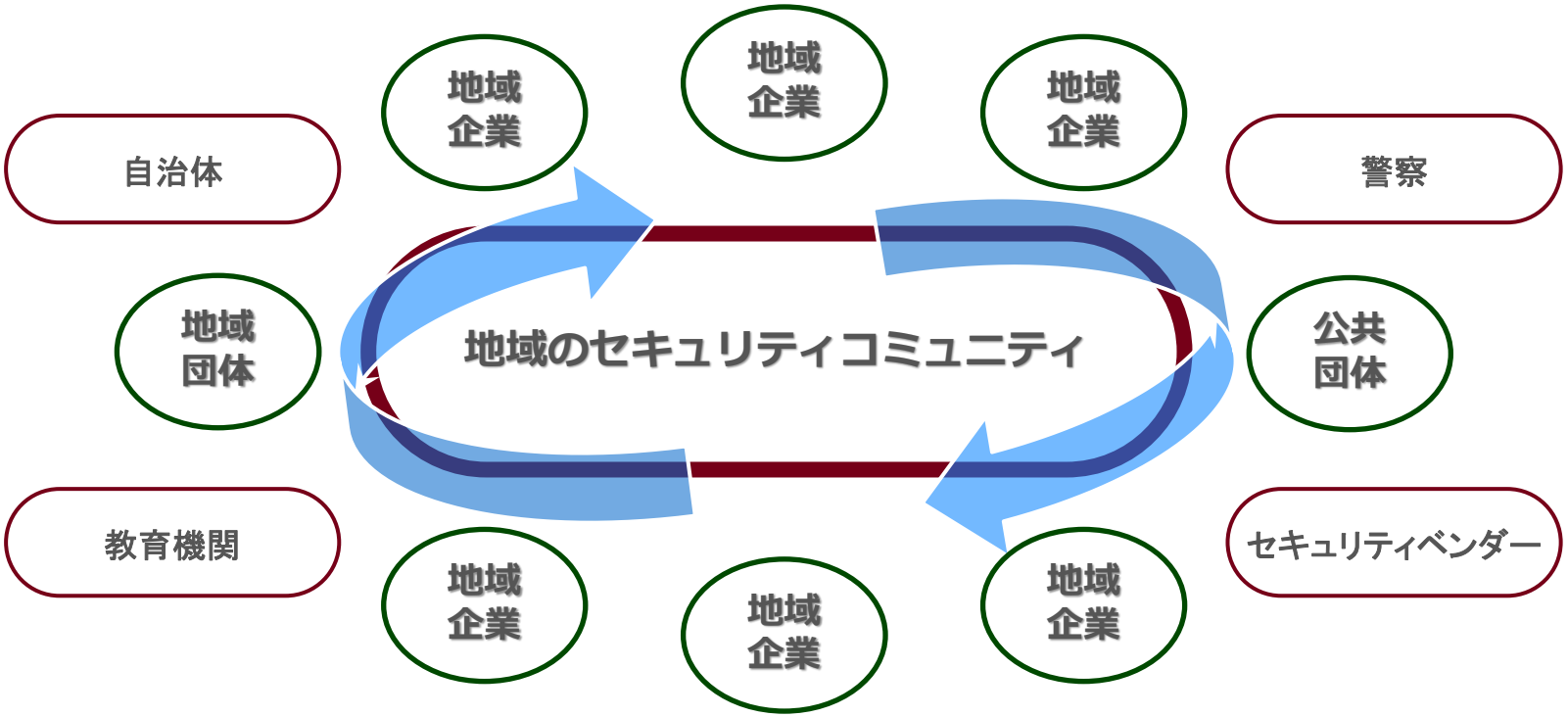
役職員への教育・啓蒙

- **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

地域のセキュリティコミュニティ

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。
身近にセキュリティについて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

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。

技術的なことは難しいと感じてしまうかもしれません。

しかし、どのようなリスクがあるのか把握し、自分ごとと捉えられれば
技術的なことがわからなくても、必要な情報を収集し、自身でできる対策
や対応をすることは、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、単独ではリスクが
わからない場合でも、先に取り組まれている方々と話すことで様々な
気づきがあります。
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