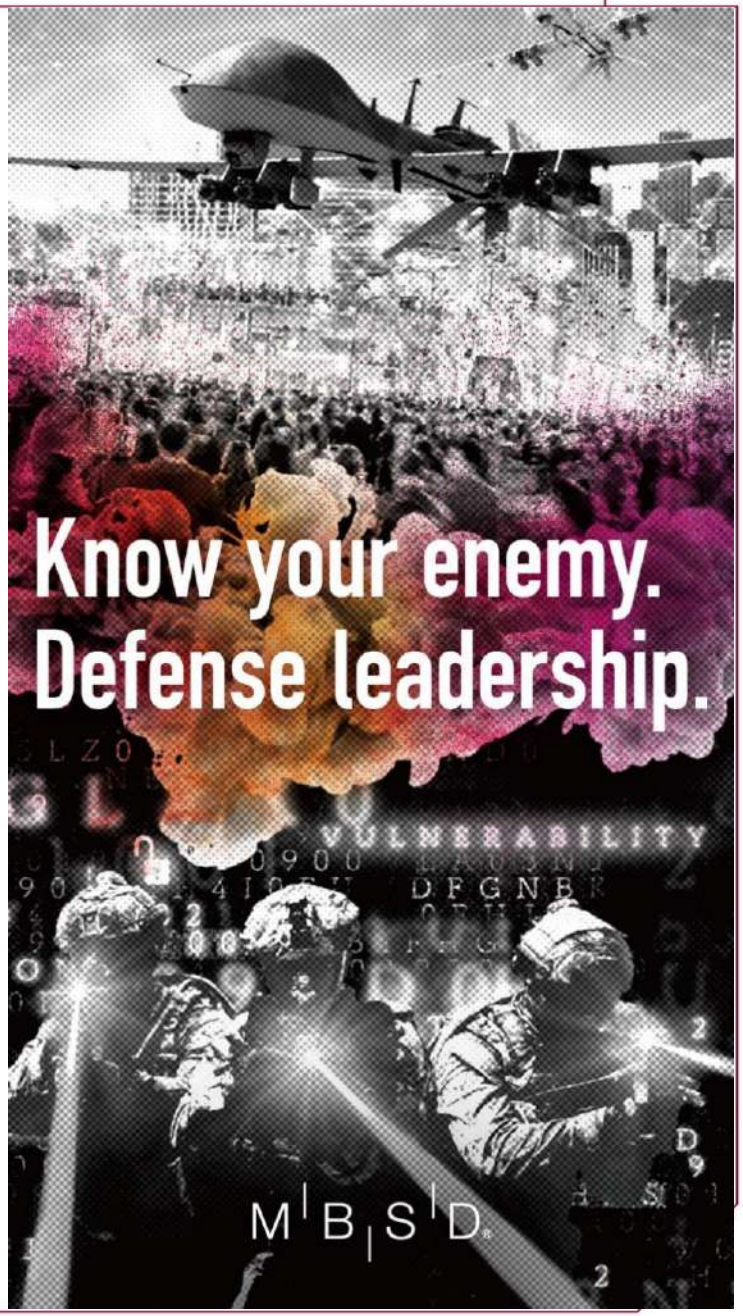
中小企業が海外ビジネスで
押さえておくべき
サイバーセキュリティのポイント

２０２１年１０月２８日



自己紹介

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

近年、セキュリティ事件が多発、連日サイバー攻撃による情報漏洩や被害のニュースが報道されています。

現在のサイバー攻撃は情報漏洩だけでなくシステムやネットワークの停止を引き起こし、業務停止や取引先まで含めたサプライチェーンにも大きな影響を与える問題となってます。

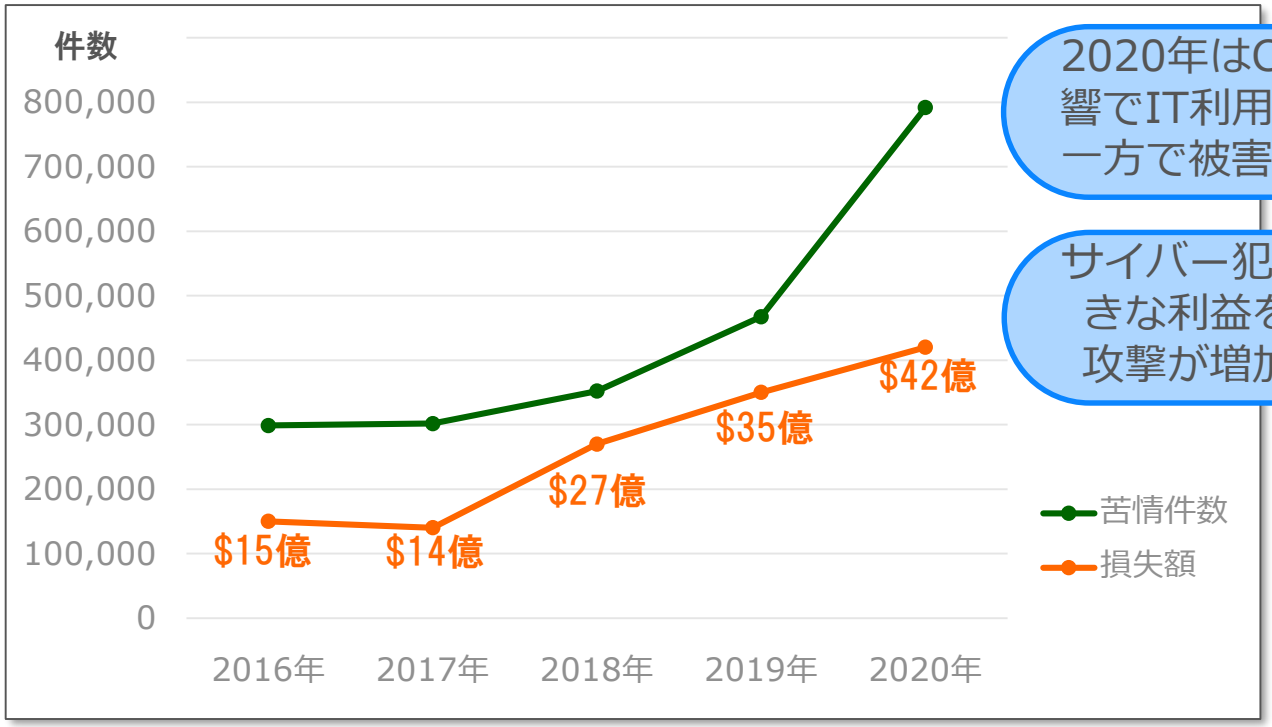
米国などでは情報漏洩による損害賠償事例も多く発生している他、
日本企業でも特に海外拠点・子会社でのセキュリティ事件が多数発生しています。

海外企業とのやり取りで特定のスマートフォンアプリでのコミュニケーションが前提になるなど通常と異なるインフラを用いた業務や、海外への送金、各国法など海外ビジネスにおいて国内と異なる環境でのセキュリティの考慮が必要になってきます。

考慮すべきポイントは対象となる国、ビジネスの内容などにより多岐に渡りますが、今回は、海外ビジネスを手掛けられている中小企業様に押さえて頂きたいポイントをいくつかご紹介させて頂きます。

サイバー攻撃による被害の増大

米国インターネット犯罪苦情センター（Internet Crime Complaint Center：IC3）が2020年に受け付けたインターネット犯罪に関する訴えに基づく統計レポートによると、報告された件数は**791,790件**(**前年467,361件で324,429件増加**)で、年間損失額は42億ドルとされており、サイバー攻撃は年々増加しています。



2020年はCOVID19の影響でIT利用が急拡大した一方で被害も大きく拡大

サイバー犯罪組織等が大きな利益を得てさらに攻撃が増加する流れに

その中でも最も被害額が大きかったのはビジネスメール詐欺（Business Email Compromise）とメールアカウント侵害(Email Account Compromise)であり、その**損失額は18億ドル以上**であると報告されています。

出典：IC3 Internet Crime Report 2020
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

※損失額には事業損失や賃金、修復サービス利用等の費用は含まれていないためランサムウェアなどの損失は実際よりも低くなっていると注記あり
※IC3は米国FBIとNW3Cが連携して設立された政府機関、インターネット関連犯罪の苦情受付や調査を実施

ビジネスメール詐欺（BEC）

BECとはBusiness Email Compromise の略で、

巧妙に細工したメールのやりとりにより、企業の担当者を騙し攻撃者の口座へ送金させたり、情報を窃取する詐欺の手口です。

☞ 特に海外取引先とのやり取りで、BECの被害に遭う可能性を抑えておいて頂きたい。

主な手口：

・取引先との請求書を偽装

取引中のメールを盗聴、請求のタイミングで振込口座が変わったなど

不正メールを送付して騙し、偽の口座に振込させる。

・経営者や弁護士などの第３者へのなりすまし

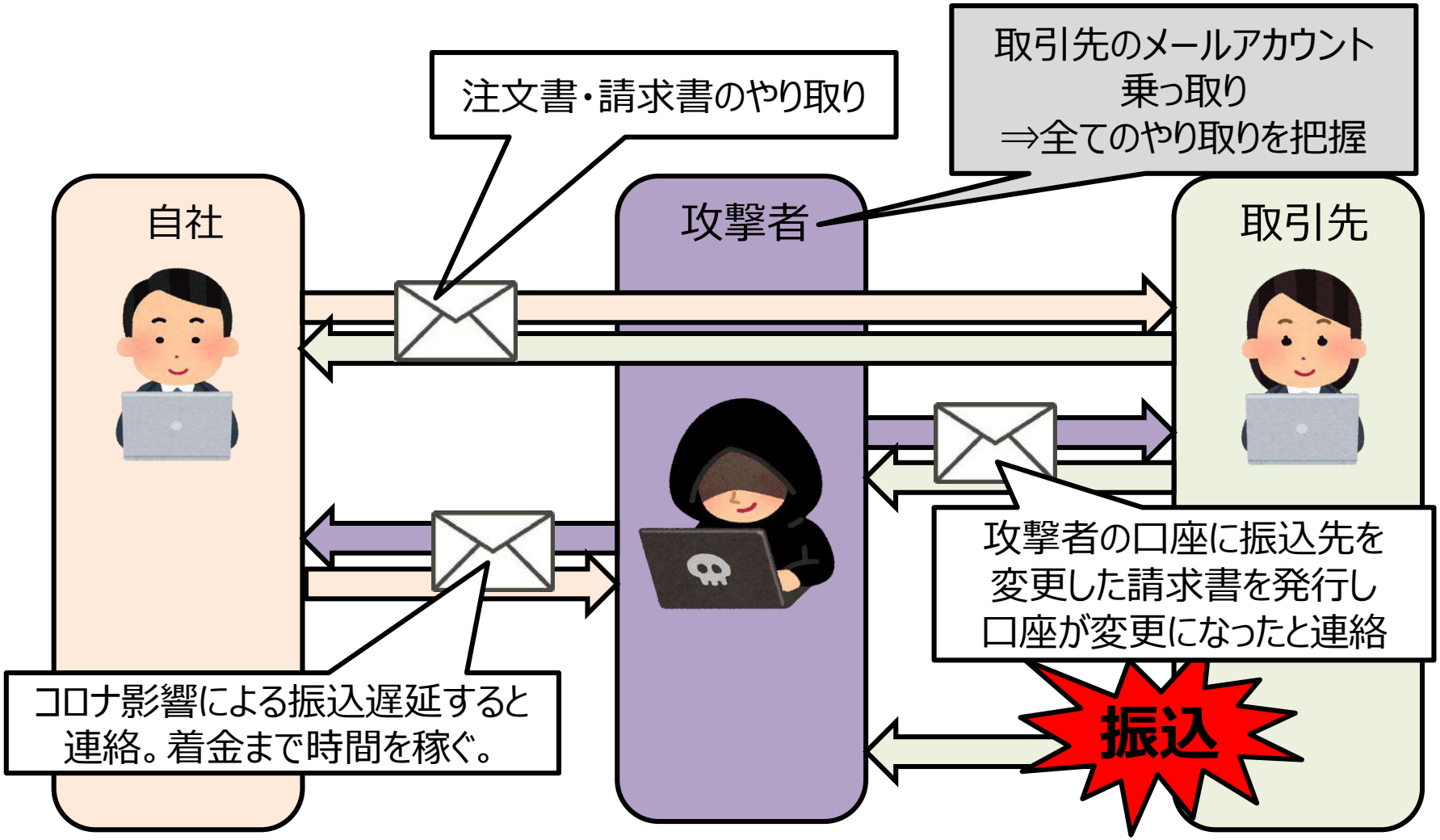
社長からの特命での依頼や、社長から依頼を受けた弁護士などと偽って騙して金銭を

振り込ませる。

など

ビジネスメール詐欺（BEC）

■メールでの取引中に何者かが偽の銀行口座を通知 (取引先が振込)したケース



攻撃者はメールのやり取りを把握し、見計らった
タイミングで偽の口座へ変更をさせようとする。

ビジネスメール詐欺（BEC）

■類似ドメインのメールアドレスを用いて取引先や上長と誤認させる

正）sekihara@mbsd.jp

誤）sekihara@rnbsd.jp

誤）sekihara@m6sd.jp

誤）masaru.seklhara@freemail.sample

誤ったアドレスが正しい取引先や上長だと誤認させて情報を搾取したり、振込をさせる。

見た目が近い文字のドメイン名を取得して不正メールを送ってくる。

例）

i ≒ l ≒ 1

m ≒ rn

sekihara@mbsd.jp

ドメイン名

なぜか本当に出張中

実際の事例を元に作成したサンプルメール

BECへの対応

■担当者含めて共有して対応すべき事項

☞ 少しでも**不審な点があったら周囲へ相談**する。
口座が変わった、なんらかの理由で別口座を利用したいなどの連絡
メールアドレスが通常と異なる、気が付いたらフリーメールが宛先に含まれていた、など

☞ 振込先の口座変更の連絡や、口座変更が行われたかという確認が入った場合は、
メールとは異なる手段 (名刺やHP記載の電話など) で先方へ連絡する。
メールに記載されている電話番号で攻撃者が実際に電話で応対するケースがある。
請求書やサインされたレターなどもデータを搾取して偽装したものを提示してくる。

☞ 業務プロセスを見直し、経理の担当者**個人で口座変更処理が完結できない**
よう、上長や経理部門責任者などの承認者を設ける
（過去の取引内容と比較するチェックシートも設けるなども有効）
⇒口座変更は内容を電話などメール以外の手段で確認したかチェックするなど

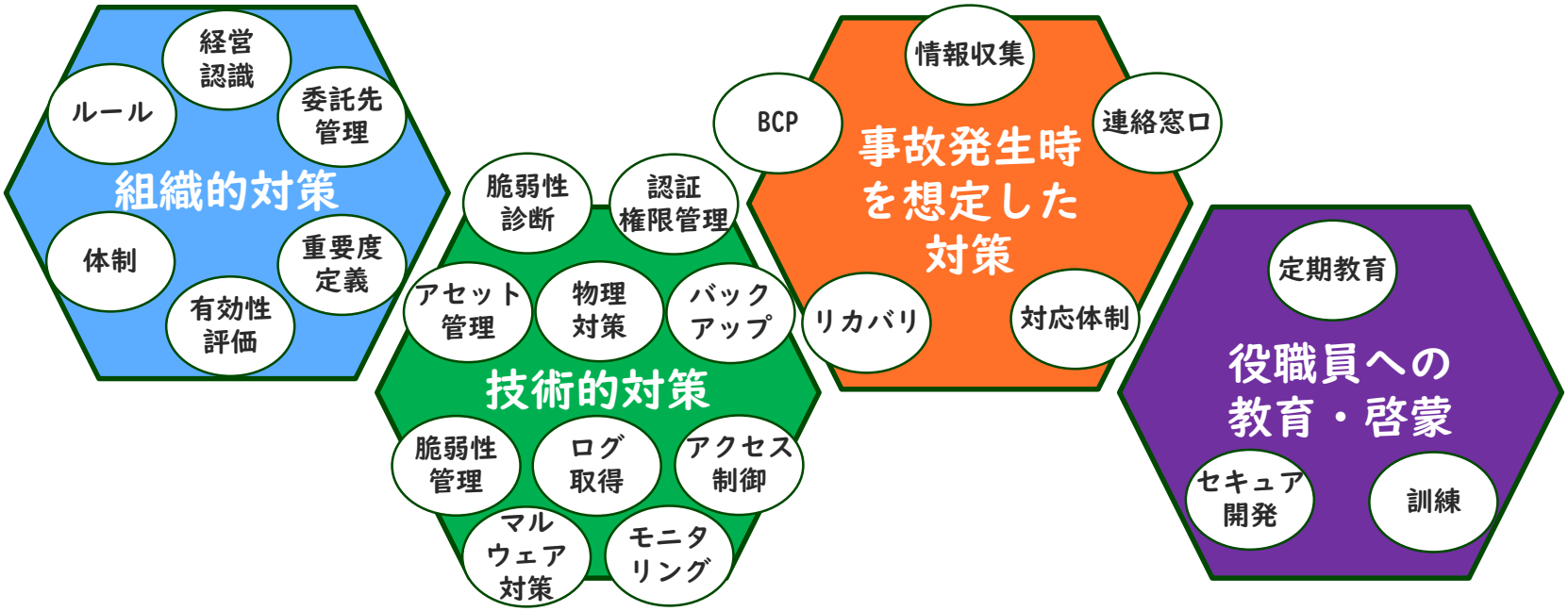
■もし振り込んでしまったら
⇒銀行に送金を止める依頼をする。早ければ早いほど良く、送金停止できることもある。

■相手が誤って振り込んでしまったら
⇒自社がマルウェアに感染あるいはメールアドレスを乗っ取られていたか疑われることも
該当取引先との送受信メールを保管しておく。 ※一定の対策をしておく必要あり。。

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

BECで数百万円から億円レベルの損害が発生するかもしれない。
取引先が詐欺に遭い商品代金が入金されない状況になるかもしれない。

・**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。

経理担当の方が相談する社内担当の方など。
不審なメールやBECの疑いなどあれば、一緒に確認してみる。

技術的対策

一定の対策は実施していると説明できる状態にしておく必要がある。

・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）

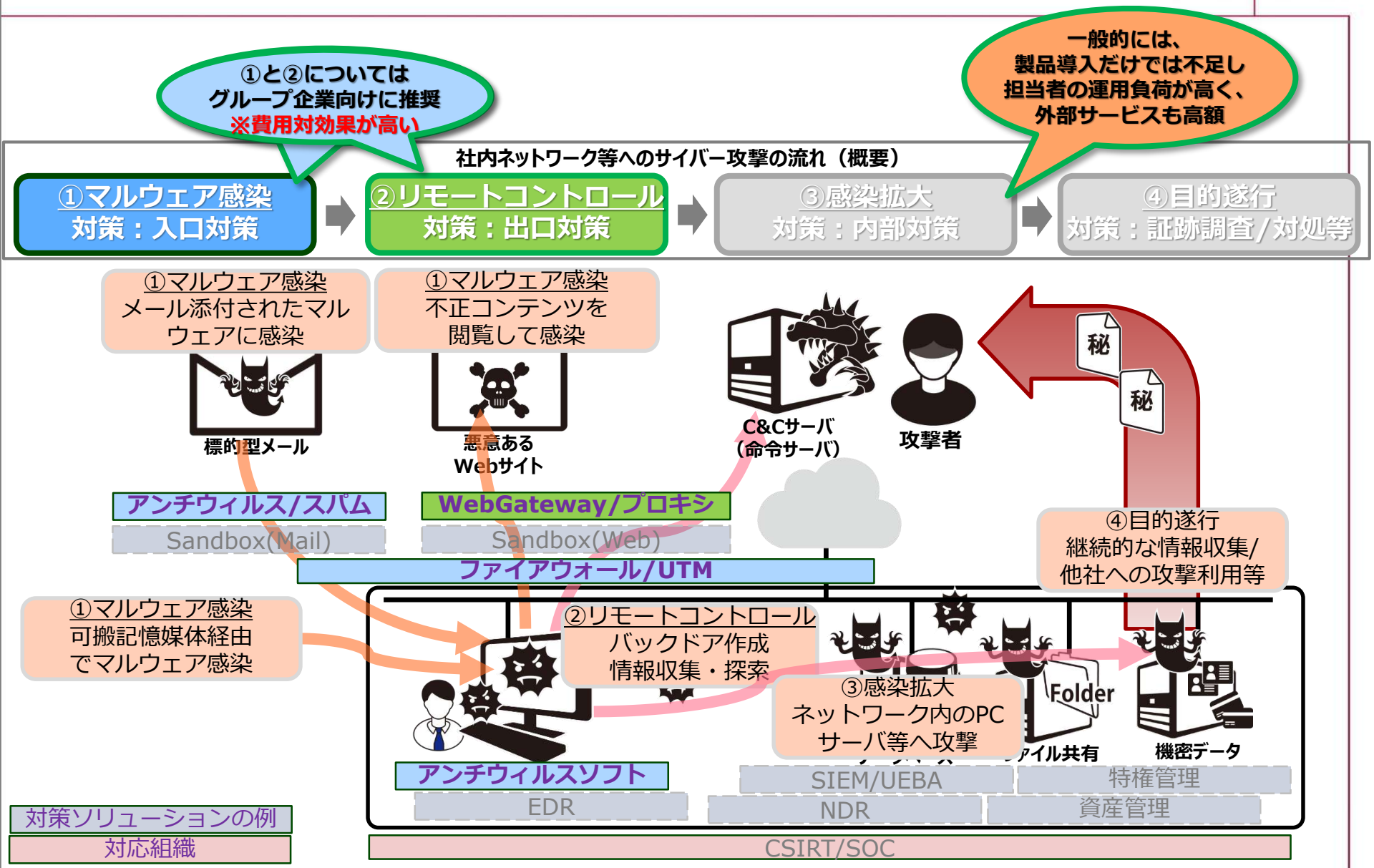
攻撃にはウェブ通信が最も良く利用されます。
防御にも有効ですが、万が一の調査の際にPCやサーバのログは攻撃者に
消去されたり、履歴が残らないように攻撃されるため調査が困難になります。
取引先への報告などのためにも通信履歴（ログ）の保管を推奨します。

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

・メールの送受信履歴やBECなどのインシデント時のメールの保管

事前に手順の確認など準備をしておけば、有事に慌てなくて済みます。

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。

BECや不審メールの
事例紹介なども有用で
す。
特に経理担当の方など

※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）**
- **メールの送受信履歴とBECなど発生時のメールの保管/事前確認**

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

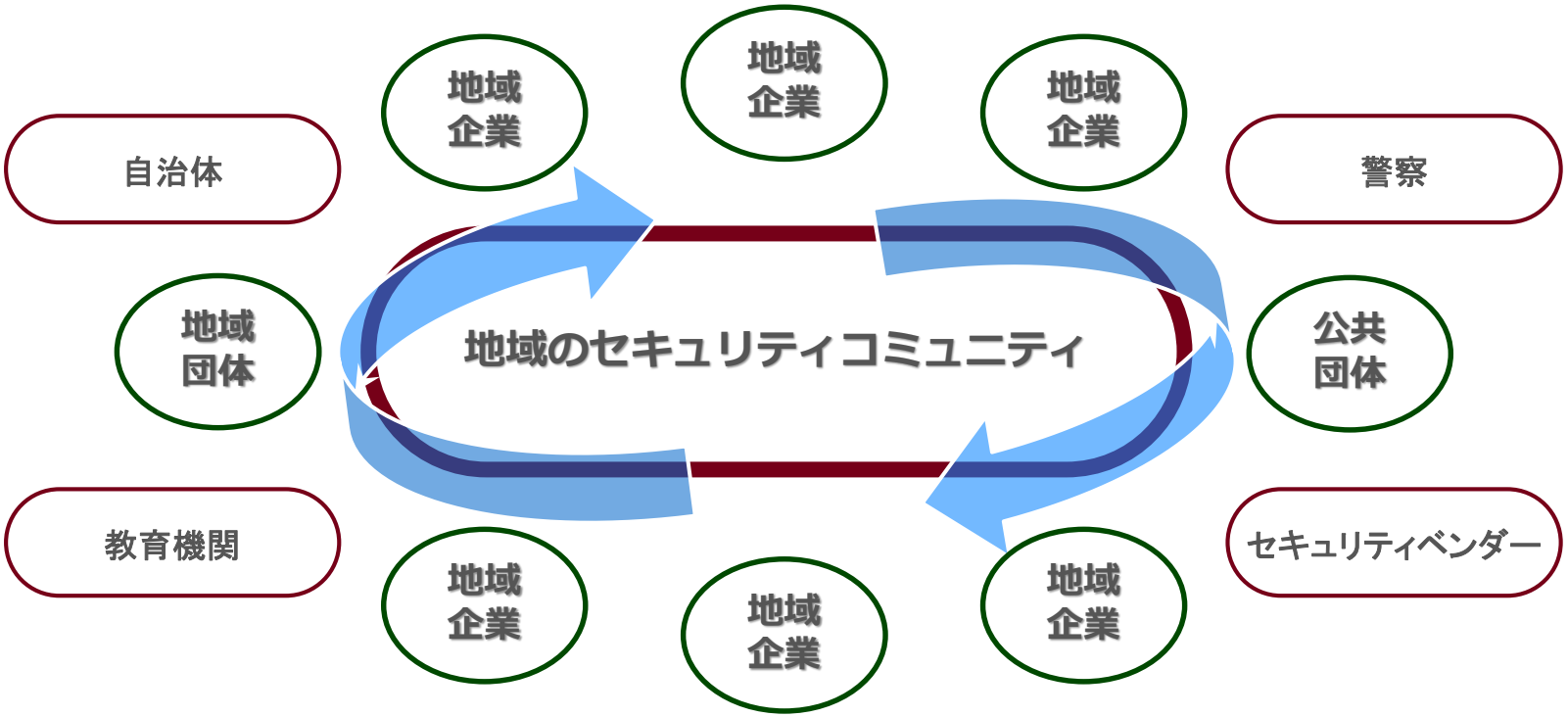
役職員への教育・啓蒙

- **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。
身近に聞ける関係先を持ち、感染症対策の様に手洗い・うがい・マスク着用など
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。
事業におけるリスクを把握し、適切に備えをする。

サイバー攻撃は世界中で多数発生しています。

海外との取引では、BECの様な詐欺行為が多発している状況をとらえて留意しておくことが望まれます。
また、一定のセキュリティ対策の実施を要求する大手企業も増えており、すぐには難しくとも段階的に自組織に合った対策をしていく事が望まれます。

ただし、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。