今からできるセキュリティ対策

２０２６年2月２５日
NTT東日本株式会社

今からできるセキュリティ対策

●サイバー攻撃を防ぐための基本

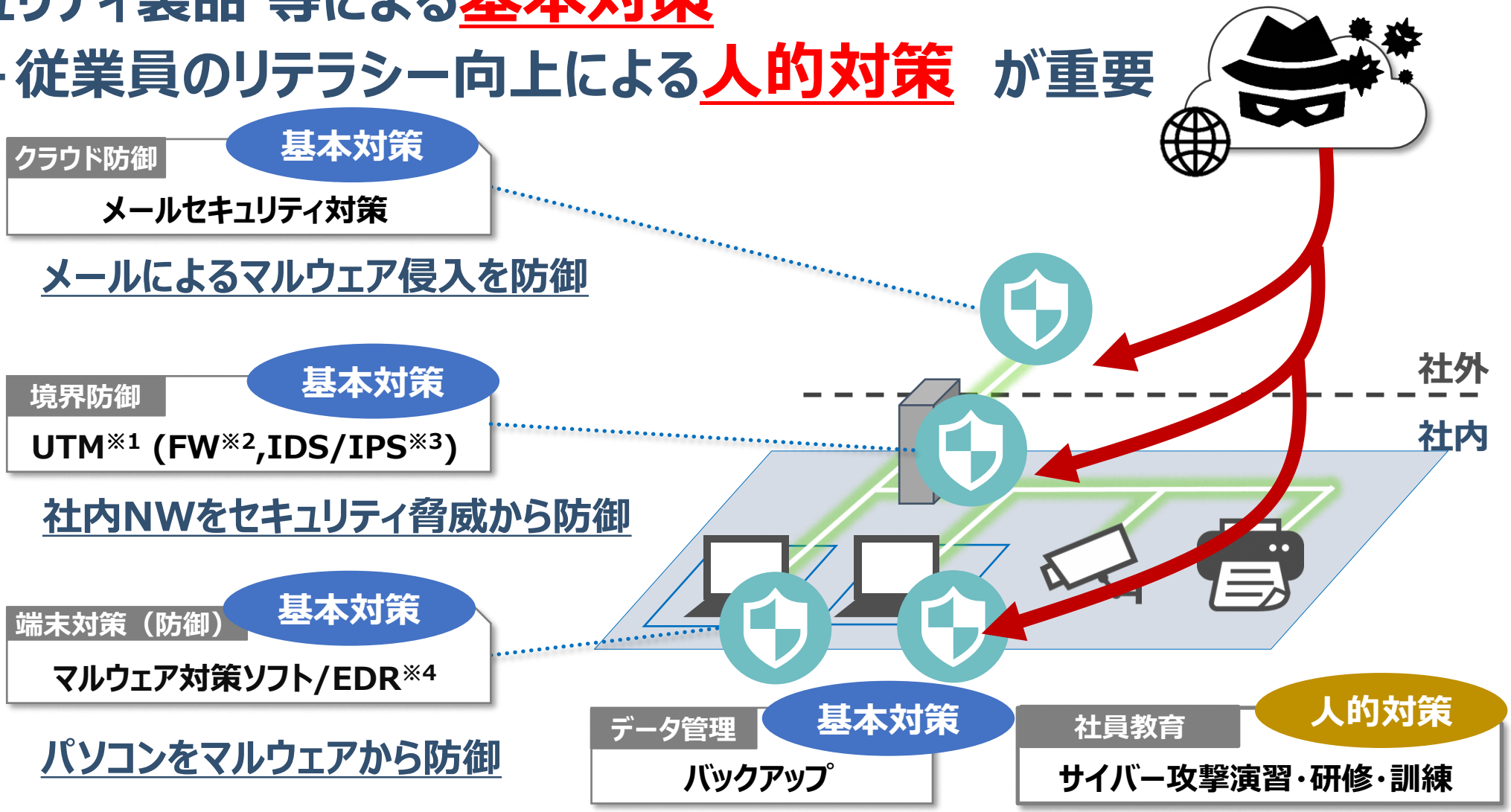
- Windowsアップデート
- ソフトウェアアップデート
- 推測しにくいパスワード設定
- セキュリティリスクの把握
- セキュリティ製品の導入

●セキュリティ事故事例からの教訓

- Windowsアップデート → システムで無効、Win7など古いOSを利用も
- ソフトウェアアップデート → VPN装置の脆弱性放置
- 推測しにくいパスワード設定 → 最小5桁、ロックアウト機能を無効に
- セキュリティリスクの把握 → 不正アクセス・内部不正の脅威に気付かず
- セキュリティ製品の導入 → 業務システムが動かなくなるため無効

今からできるセキュリティ対策

●セキュリティ製品 等による基本対策
＋従業員のリテラシー向上による人的対策 が重要



※1 Unified Threat management
※2 Firewall
※3 Intrusion Detection System/Intrusion Prevention System
※4 Endpoint Detection & Response

１．　情報セキュリティの現状分析

● 現状分析を通じて得られる3つのメリット

リスクの特定と優先順位の設定

✓ 企業が直面しているセキュリティ脅威やリスクを明確化
✓ リスクに応じた優先順位を設定し、計画的な対策が可能

コストの最適化

✓ 必要なセキュリティ対策を精査してリソースを最適に配分
✓ 無駄なセキュリティ投資を省くことで、コスト削減を実現

コンプライアンス遵守と信頼性の確保

✓ 法的規制や業界標準への準拠状況を確認
✓ 企業の信頼性を高め、顧客や取引先からの信頼を獲得

● ５分でできる！情報セキュリティの自社診断について

IPA 独立行政法人 情報処理推進機構から公開されている、**情報セキュリティ対策のレベルを数値化し、問題点を見つけるためのセキュリティアセスメントツール(無料)**

自社セキュリティ対策の現状分析の第一歩として、本日は実演を交えて、活用方法についてご紹介します

出典元： IPA 5分でできる！情報セキュリティ自社診断
https://www.ipa.go.jp/security/guide/sme/5minutes.html

情報セキュリティの現状分析

● 実施のながれ

診断

- 情報セキュリティに関する、25個の診断項目に回答
- 会社の情報セキュリティの現状を簡単に点数化
- PDF版(※1)とオンライン版(※2)があり、オンライン版ではレーダーチャートを用いた結果出力や同業他社との比較が可能

解説

- 診断結果の点数に応じた、取り組むべき推奨事項を解説
- 対策ができていない項目ごとに、対策を立てる上での考え方や具体的な対策案を解説

診断項目	No	診断内容
Part 1 基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1は最新の状態にしていますか？
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？
	4	重要情報※2に対する適切なアクセス制限を行っていますか？
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？
Part 2 従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？
	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？
	10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？
	15	関係者以外の事務所への立ち入りを制限していますか？
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？
Part 3 組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？
	25	情報セキュリティ対策（上記１～24 など）をルール化し、従業員に明示していますか？

※1　5分でできる！情報セキュリティ自社診断(PDF版)
　　https://www.ipa.go.jp/security/guide/sme/ug65p90000019c86-att/000055848.pdf
※2 5分でできる！情報セキュリティ自社診断(オンライン版)
　　https://security-shien.ipa.go.jp/diagnosis/

NTT EAST

SAMPLE

● 診断結果の出力イメージ

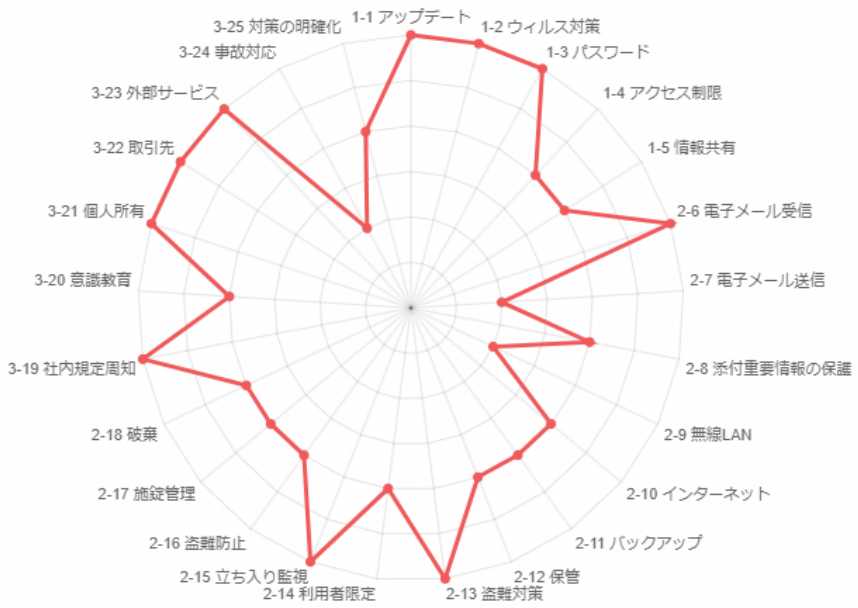
合計点

合計点

64 / 100

合計点算出基準

実施しているの合計点	40点
一部実施しているの合計点	24点
実施していないの合計点	0点
わからないの合計点	0点



推薦する資料、ツール一覧

概要

診断の結果に合わせてお薦めする資料およびツールです。

資料、ツール名：**中小企業の情報セキュリティ対策ガイドライン**

推薦のコメント：

「中小企業の情報セキュリティ対策ガイドライン」（以下「本ガイドライン」）は、情報セキュリティ対策に取り組む際の、(1)経営者が認識し実施すべき指針、（2）社内において対策を実践する際の手順や手法をまとめたものです。経営者編と実践編から構成されており、個人事業主、小規模事業者をも含む中小企業（以下「中小企業等」）の利用を想定しています。

資料、ツール名：**5分でできる！情報セキュリティ自社診断(印刷版）で対策を確認**

推薦のコメント：

「5分でできる！情報セキュリティ自社診断」の各チェック項目について解説や対策例を掲載しています。

資料、ツール名：**情報セキュリティ5か条**

推薦のコメント：

情報セキュリティ５カ条は、企業の規模に関わらず、必ず実行すべき重要な対策をまとめています。共通的な基本的対策ですので、必ず実行しましょう

資料、ツール名：**情報セキュリティ啓発映像　中小企業のセキュリティ対策**

推薦のコメント：

人間ドックの結果を聞きに医院に訪れた中小企業の社長。そこで待っていたのは中小企業の情報セキュリティを診断する女医だった…。中小企業における情報セキュリティ対策の必要性とまず実践してほしい対策「情報セキュリティ5ヶ条」を人間ドックの診断に見立ててわかりやすくご説明いたします。

● 一緒に取り組んでみましょう

ここからは「５分でできる！情報セキュリティの自社診断」について、簡単に体験いただこうと思います。

全設問２５問のうち、３問を抜粋し回答の考え方や対策方法について解説します。

ご自身の認識・理解の範囲で構いませんので、今の時間に一緒に取り組んでいただき、自社の情報セキュリティの振り返りや改善に活かしていただければ幸いです。

問1　基本的対策

パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？

問2　従業員としての対策

パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？

問3　組織としての対策

従業員にセキュリティに関する教育や注意喚起を行っていますか？

問1　基本的対策

パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？

1

実施している

例）・　パソコンやスマホのOSやソフトウェアを**常に最新の状態に保つ**ように、設定もしくはツール等で制御している

2

一部実施している

例）・　OSや主要なソフトウェアについては手動で定期的に更新しているが、**全てのソフトウェアに対しては未対応**
・　パソコンやスマホの利用者に、アップデートするように**ルール化をしているが、状態は確認できていない**

3

実施していない

例）・　アップデートの実施や判断はルール化されてなく、パソコンやスマホの利用者の判断にまかせている

問2　従業員としての対策

パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？

1

実施している

例）・ **バックアップポリシーを制定**し、全社員のパソコンとサーバーのデータが**日次または週次で自動的にバックアップ**している

2

一部実施している

例）・ バックアップの頻度は**不定期**であり、**最新のデータが常に保護されている状態ではない**

3

実施していない

例）・ バックアップポリシーを定めてなく、対象や頻度は従業員個人の裁量にまかせている

問3　組織としての対策

従業員にセキュリティに関する教育や注意喚起を行っていますか？

1

実施している

例）
- セキュリティポリシーを策定しており、**定期的な周知**を行っている
- 年に数回、**全従業員を対象**にセキュリティに関する研修を実施している

2

一部実施している

例）
- セキュリティポリシーは策定しているが、**周知は更新時のみ**。もしくは**周知していない**。
- 新入社員向けに入社時のセキュリティ教育を行っているが、**既存社員に対する定期的なセキュリティ研修は実施していない**

3

実施していない

例）
- セキュリティポリシーがない。または、形骸化している
- 組織としての実施計画はなく、セキュリティに関する学習は従業員個人の裁量にまかせている

👉 フィードバック

情報セキュリティの現状分析

フィードバック

問1　基本的対策

サプライチェーン対策

パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？

問2　従業員としての対策

ランサムウェア対策

パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？

問3　組織としての対策

内部不正による情報漏えい対策

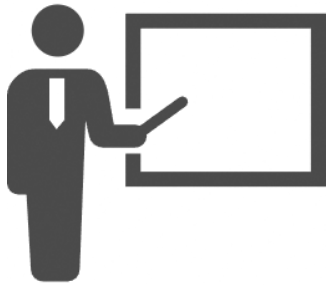
従業員にセキュリティに関する教育や注意喚起を行っていますか？

問1　基本的対策

サプライチェーン対策

フィードバック

パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？



解説

OSやソフトウェアを古いまま放置すると、セキュリティ上の問題が解決されずに、それを悪用したウイルスに感染する危険性あります。
修正プログラムを適用する、または最新版を利用するようにしましょう。

対策例

最低限やってほしいこと

- ✓ 定期的なアップデートの実施と確認

次にやること

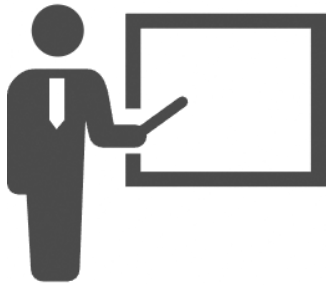
- ✓ 自動更新機能の有効化
- ✓ ソフトウェア管理ツールの導入での一括管理・更新

問2　従業員としての対策

ランサムウェア対策

フィードバック

パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？



解説

ウイルス感染などにより、パソコンやサーバの中に保存したデータが消えてしまうことがあります。
不足の事態に備えて、バックアップを取得しておきましょう。

対策例

最低限やってほしいこと

- ✓ 重要情報のバックアップをとる

次にやること

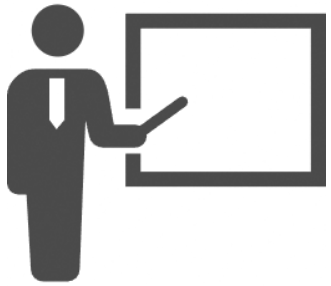
- ✓ バックアップ間隔を決めて、自動的に取得できるようにする
- ✓ 問題なくリストアできるか、バックアップ方式の妥当性を定期的に確認する
- ✓ 複数のバックアップ先を利用し、そのうち１つは遠隔地に保存する

問3　組織としての対策

内部不正による情報漏えい対策

フィードバック

従業員にセキュリティに関する教育や注意喚起を行っていますか？



解説

日々の仕事では常に様々な情報を扱いますが、日常的であるがゆえに管理の意識が疎かになりがちです。
そのため、従業員に対しては繰り返しの意識づけを行うことが重要です。

対策例

最低限やってほしいこと

- ✓ 情報管理の大切さや関連する法令などを従業員に説明する

次にやること

- ✓ 全従業員に対して、定期的なセキュリティに関する研修の機会を設ける
- ✓ 身近なインシデント事例等の周知による、セキュリティ意識の向上を図る

2．NTT東日本でのお手伝い

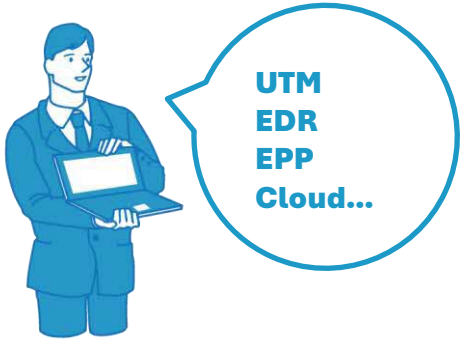
専門家による“セキュリティアセスメント”の受講も有効です

- セキュリティ専門人材による**脆弱なポイントの的確なアドバイス**
- ガイドライン準拠のアセスメントツールを使った**現状の可視化**
- リスクに応じたセキュリティ対策の**優先順位づけ**

セキュリティに不安がある

過去にサイバー攻撃にあったか、周りで感染した企業がいたかなどのヒアリングを実施
情シスはいるものの、あまりセキュリティのアップデートができていない企業におすすめです。

ベンダーからの勧め



いつも取引しているベンダーからセキュリティ商材を提案されているが、**優先順位がわからない**/とりあえず導入してくれと頼まれているなどの意見がある際は、アセスメントを判断材料にしていただくことが可能です。

資格取得の検討

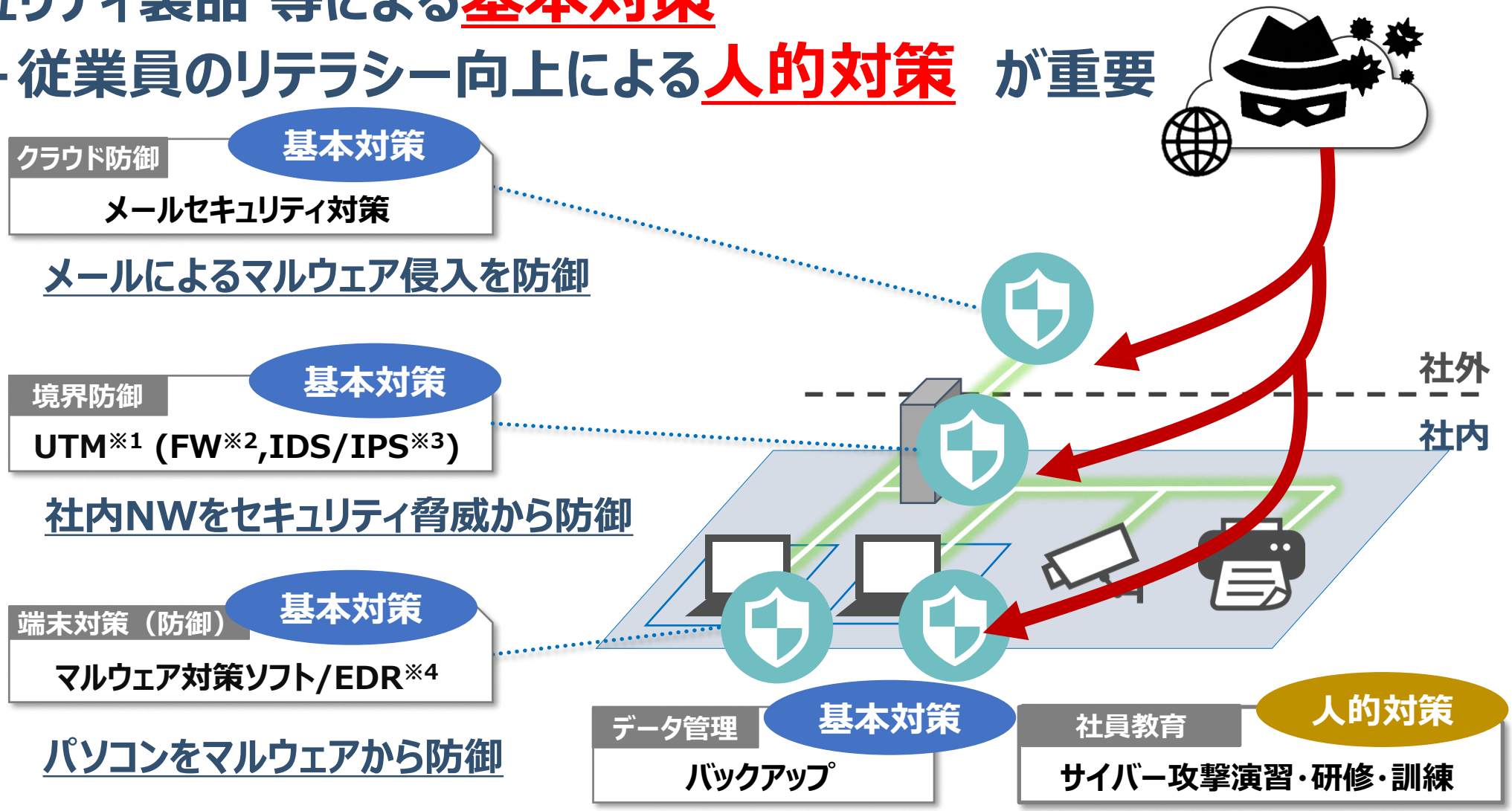
International Organization for Standardization
ISO
27001

セキュリティアセスメントを受講し、適切なセキュリティ対策を講じることで、ISO規格への適合性を向上させることができます。

※ISO27001の認証を取得するには、情報セキュリティシステムを社内で制定・運用、記録し審査の申請が必要

NTT東日本でのお手伝い

●セキュリティ製品 等による基本対策
＋従業員のリテラシー向上による人的対策 が重要



※1 Unified Threat management
※2 Firewall
※3 Intrusion Detection System/Intrusion Prevention System
※4 Endpoint Detection & Response

NTT東日本でのお手伝い

おまかせクラウドアップセキュリティ

メールセキュリティ対策（クラウド防御）

マルウェアの侵入を防御！

おまかせサイバーみまもり

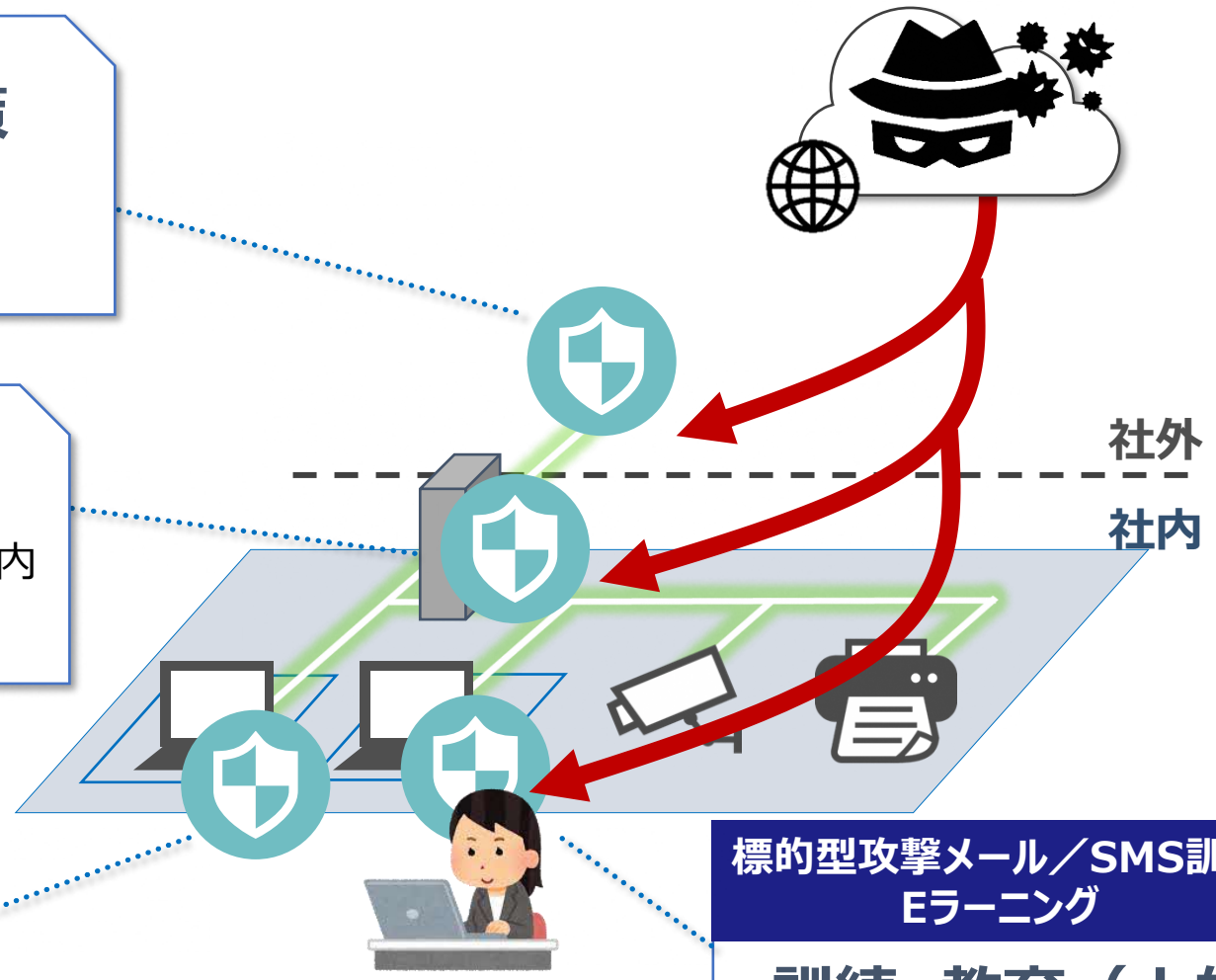
UTM（境界防御）

不正サイトブロック、不正通信監視に　より社内NWをインターネットから防御！

おまかせアンチウイルス

ウィルス対策ソフト（端末対策・防御）

パソコンをマルウェアから防御！



標的型攻撃メール／SMS訓練 Eラーニング

訓練、教育（人的対策）

従業員セキュリティ意識の向上！

おまかせセキュリティ事故駆け込み窓口

不正アクセス、情報漏えいなどセキュリティ事故に遭ってしまったら
NTT東日本がセキュリティ事故の初期相談を無償サポート!※

※ご相談内容に応じ有償サービスをご案内する場合もあります

おまかせセキュリティ事故駆け込み窓口とは

■ 中小企業のお客さまが情報セキュリティ事故に遭遇した際、被害を最小限に抑制する、事故発生の原因を解析する、事故発生前の状態に復旧するなどのサポートを行う窓口です

■ NTT東日本のサービスをご利用いただいていないお客さまでもご利用いただけます

NTT東日本へご相談ください！
0120-790-113
受付時間　9:00～17:00（土日・休日をのぞく）
おまかせセキュリティ事故駆け込み窓口をご利用いただく際には裏面に記載の「おまかせセキュリティ事故駆け込み窓口　同意書」への同意が必要となります。

まとめ

- サイバー攻撃は企業規模、地域を問わず増加傾向にあります
  中小企業に対しても、数多くのサイバー攻撃の確認、被害が発生しています

- セキュリティ事故が発生すると、非常に大きな被害を負うことに加え、
  最悪の場合は加害者となり取引先等へ影響を及ぼしてしまう場合もあります

- テレワークの拡大や業務のDX化等により、サイバー攻撃の対象となるシステムは増えています。基本的なセキュリティ対策を徹底しつつ、自社に最適なセキュリティ対策の実施、及び継続的な見直しが肝要です

セキュリティ対策にご不安があれば
NTT東日本へご相談ください

0120-116-032

受付時間：平日9:00～17:00（年末年始を除きます）