（報道発表資料）

２０１９ 年 ７ 月 １６ 日
東日本電信電話株式会社
北 海 道 事 業 部

情報セキュリティリーフレット（第２弾）を作成しました
～サイバー犯罪の被害のリスクを軽減するために！～

東日本電信電話株式会社北海道事業部（事業部長　髙橋　庸人、以下　NTT 東日本）は、サイバー犯罪の被害防止・被害軽減のため、情報セキュリティリーフレット（第２弾）を作成しました。

情報セキュリティ対策には、**情報セキュリティに対する倫理やモラル、情報リテラシーの向上が有効**であり重要です。弊社はこれまで、小学生を対象としたネット安全教室(※1)や公益財団法人日本電信電話ユーザ協会(※2)、商工会議所、商工会、北海道警察と連携し情報セキュリティセミナーを実施してきました。

この情報セキュリティリーフレット（第２弾）を活用し、地域の皆様の情報セキュリティ啓発活動に努めます。

記

1. これまでの情報セキュリティ向上の取り組みについて
   ①ネット安全教室(※1)の実施
   ②公益財団法人日本電信電話ユーザ協会(※2)主催による情報セキュリティセミナーの実施
   ③情報セキュリティ「リーフレット」の作成

2. 情報セキュリティ「リーフレット」の活用について
   ・ネット安全教室(※1)での活用
   ・公益財団法人日本電信電話ユーザ協会(※2)等が主催する情報セキュリティセミナーへの利用
   ・北海道警察への提供

3. 情報セキュリティ「リーフレット」の作成にあたって
   北海道におけるサイバー犯罪等に関する数値は、北海道警察から情報提供いただきました。
   また、企業の情報セキュリティ対策状況については、総務省公表「平成 30 年度通信利用動向調査の結果（2019 年 5 月）」の一部を抜粋しています。

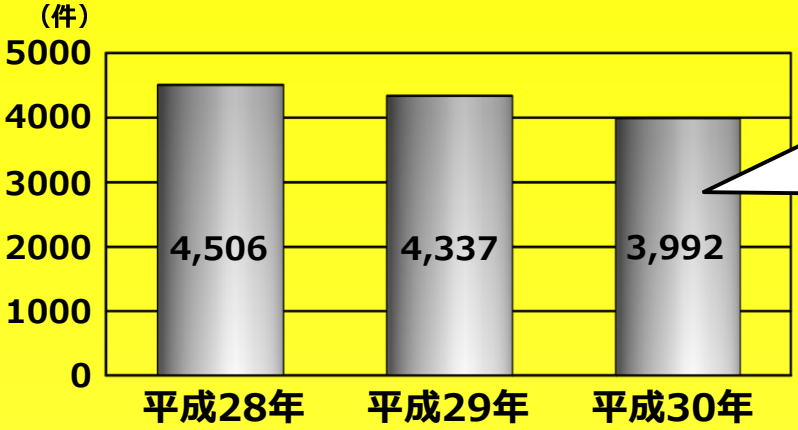
4. その他
   ※1：「ネット安全教室」とは、CSR 活動の一環として「次世代の ICT 社会を担う人材の育成」として弊社社員が地域の小学校へ講師としてお伺いし、インターネット上のコミュニケーションのしかた、マナーをテーマにした出張授業を実施する取り組みです。
   ※2：「公益財団法人日本電信電話ユーザ協会」とは、1976 年電気通信利用の実態調査・サービスの評価・普及、各種相談受付・教育等を目的に設立された財団法人です。
   なお、2012 年に現在の公益財団法人へ移行しました。

CAUTION CAUTION CAU

NTT東日本

サイバー犯罪の被害のリスクを軽減するために!

北海道警察で受理したサイバー犯罪等に関する相談件数



１日あたり
約10.9件!!
近年、ほぼ同水準で推移!!

サイバー攻撃の情勢

情報窃取を企図したとみられる標的型メール攻撃は、近年増加傾向

標的型メール攻撃
（全国件数）
6,740件!!

出典：警察庁「平成30年におけるサイバー空間をめぐる脅威の情勢等について」（2019年3月）

近年のサイバー犯罪

詐欺	インターネットで注文したが商品が届かない
名誉毀損	インターネット掲示板に「誹謗中傷する内容が書き込まれた」
不正アクセス	ID・パスワードが盗まれ「勝手にサービスを利用された」
ウイルス感染	スマホやパソコンがウイルス感染し「情報が盗まれた」「ロックされ金銭を要求された」
偽メール	実在企業を装ったメールで誘導され「カード情報などを入力させられた」「別口座に入金させられた」

サイバー犯罪の攻撃・手口が悪質・巧妙化
金銭要求・情報窃取などの被害が深刻化

■発行：ＮＴＴ東日本 北海道事業部　■情報提供元：北海道警察
問合先：ビジネスコンタクトセンタ　TEL：0120-266488（平日9:00～17:00）＜年末年始（12/30～1/5）は除く＞

K19-0690【1907-2006】

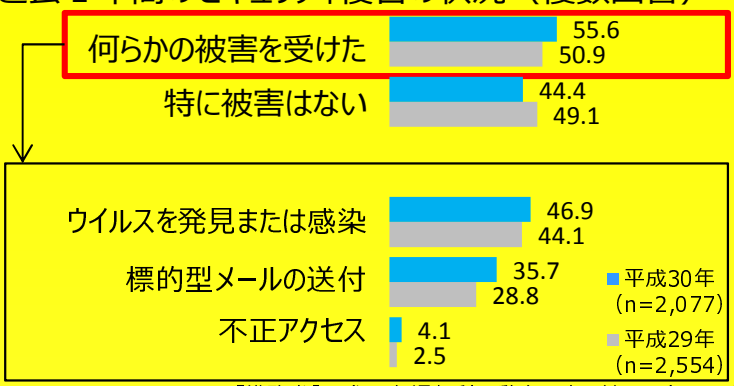
CAUTION CAUTION CAU

CAUTION CAUTION CAU

企業の情報セキュリティ対策状況

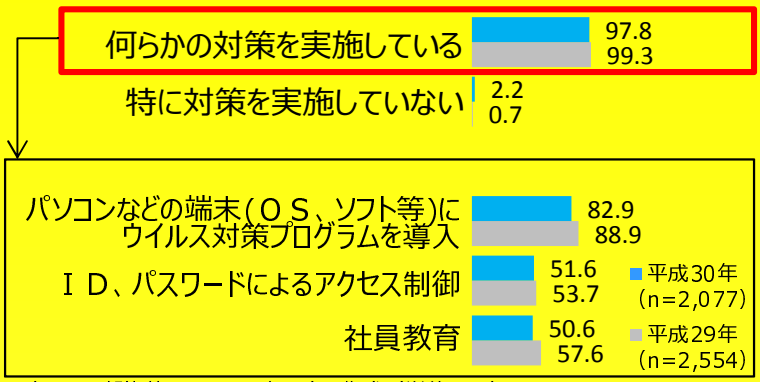
55.6%の企業が何らかの被害を受けている

過去１年間のセキュリティ侵害の状況（複数回答）



企業の97.8%が対策済みと回答している

セキュリティへの対応状況（複数回答）



『総務省「平成30年通信利用動向調査の結果」（2019年5月）』を一部抜粋し、ＮＴＴ東日本で作成（単位：%）

出典　総務省　H30通信利用動向調査結果

考えられる情報セキュリティ対策をすべて講じても１００%感染を防ぐことはできません！！

情報セキュリティ対策の目的は・・・

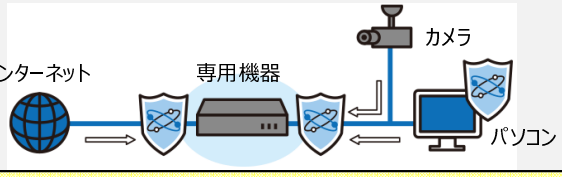
- **サイバー攻撃による被害のリスクを軽減する**

複数の情報セキュリティ対策を組み合わせることが効果的!!

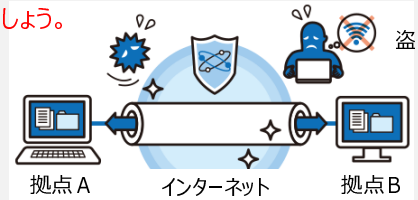
企業の情報資産を守るための４つのポイント

第三者の不正アクセスを防ごう！
【 ①ネットワークセキュリティ対策 】

ネットワークの出入口に専用機器を設置し、不正アクセスや迷惑メールなどを検知、ブロックする対策を講じましょう。

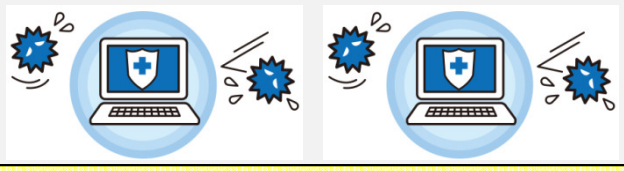


拠点間のデータのやり取りは、安全なプライベートネットワークを利用しましょう。



ウイルス感染から端末を守ろう！
【 ②端末セキュリティ対策 】

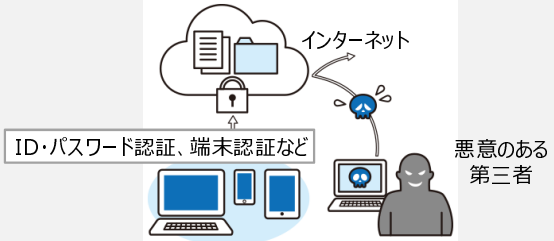
複数あるパソコンなどのウイルス定義の更新を一括管理できる“ウイルス対策ソフト”を導入し、ウイルス感染しないようにしょう。



USBメモリを利用できないようにシステムで禁止し、個人USB使用によるウイルス感染が発生しないようにしましょう。

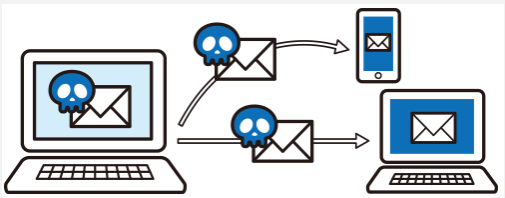
重要な企業情報・データを守ろう！
【 ③バックアップ対策 】

重要データは安全なクラウド上へ保管しましょう。



社員教育を徹底しよう！
【 ④人的対策 】

標的型攻撃メールに模したメールを送信する訓練サービスもあるので、社員の実践的な訓練に活用しましょう。



CAUTION CAUTION CAU