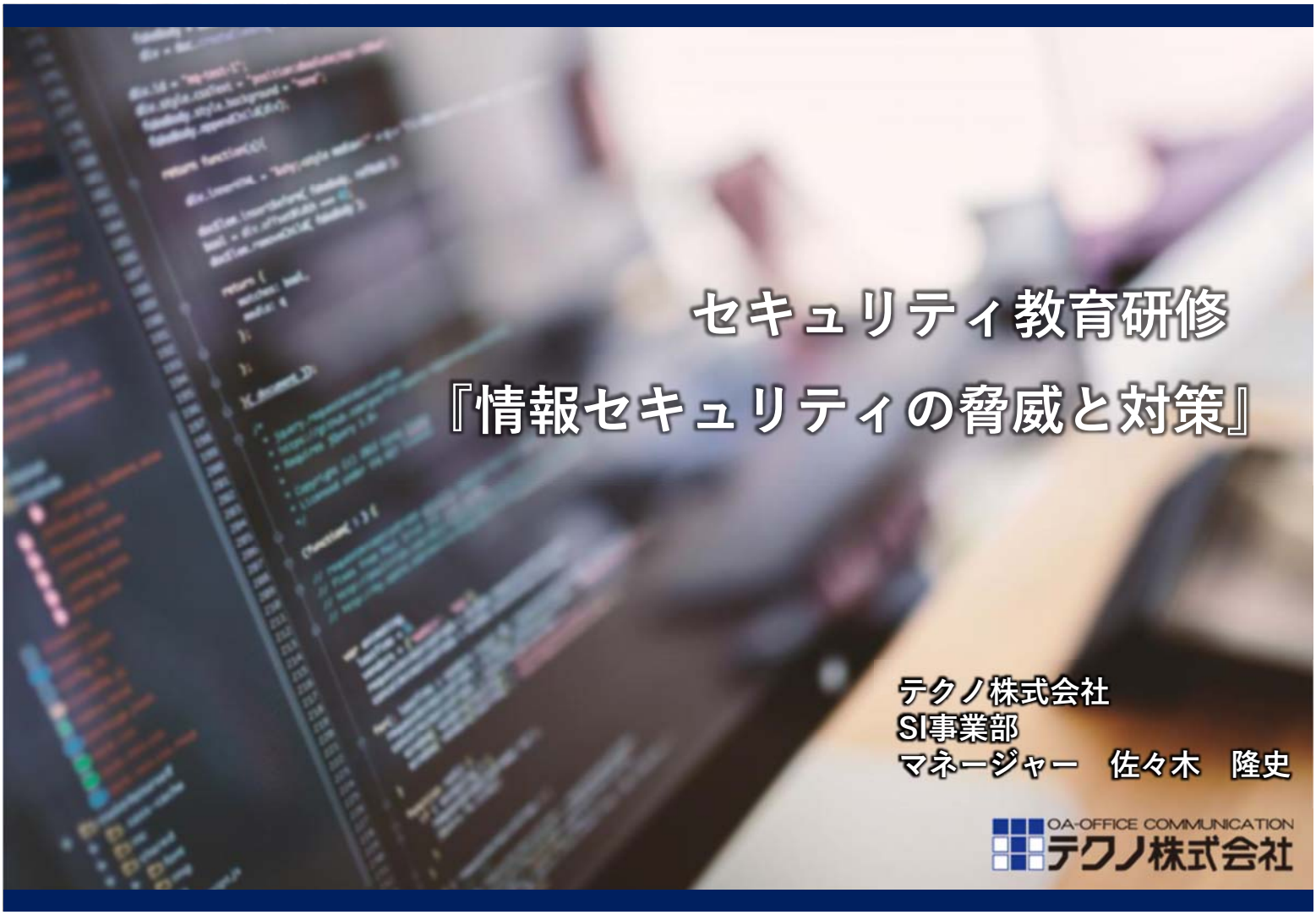


セキュリティ教育研修
『情報セキュリティの脅威と対策』

テクノ株式会社
SI事業部
マネージャー　佐々木　隆史

OA-OFFICE COMMUNICATION
テクノ株式会社

会社説明

OA-OFFICE COMMUNICATION
テクノ株式会社

会社名　テクノ株式会社

所在地
[本社]　〒０２０－０１２４　岩手県盛岡市厨川３丁目１０－１
[青森営業所]　〒０３０-０８４６　青森県青森市青葉２丁目６－３

設立　昭和６０年１２月７日

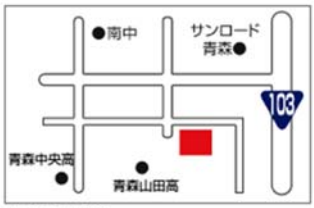
代表者　代表取締役　長谷川　修

事業内容
◆自治体・学校向けシステムの導入及びサポート
◆福祉関連システム販売／サポート、及び個別開発
◆一般企業向けシステム開発/導入、及び運用サポート
◆セキュリティ対策導入及び運用サービス

発表者
SI事業部 マネージャー　佐々木　隆史
保有資格　経済産業省認定 情報処理技術者 情報セキュリティマネジメント
日本教育工学振興会（JAPET）認定　教育情報化コーディネータ
マイクロソフト認定プロフェッショナル（MCP）

MAP

▲本社



▲青森営業所

本日の研修内容

テクノ株式会社

1．「情報セキュリティの脅威」

2．「対策の基本的な考え方」

3．「必要なセキュリティ対策」

1．「情報セキュリティの脅威」

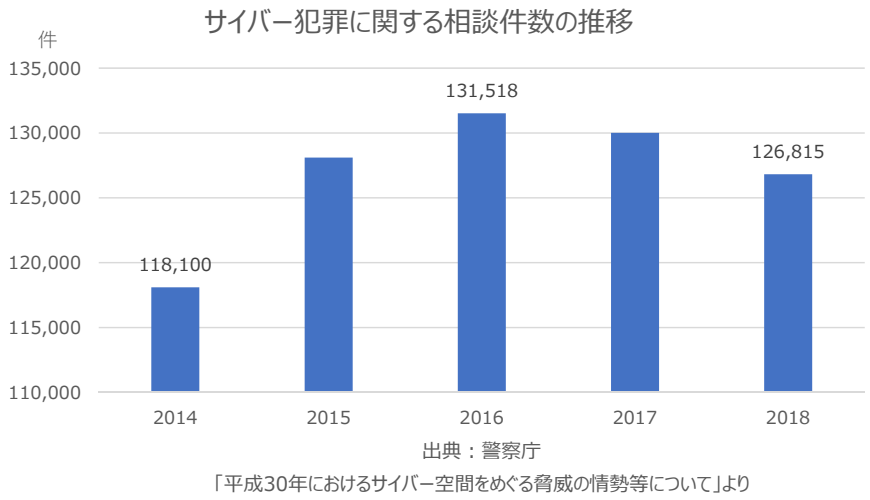
テクノ株式会社

・「情報セキュリティって私たちになんの関係があるの？」

・「情報セキュリティ？なにそれ？」

・「なんとなく聞いたことがあるけど、情報セキュリティって具体的になにをするの？」

1．「情報セキュリティの脅威」



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」より

【 参考 】サイバー犯罪に関する相談
不正アクセス等、コンピュータ・ウイルスに関する相談
○ 宅配業者を装ったショートメールに記載されていたURLに接続し、表示された画面に個人情報を入力したところ、何者かに不正に利用された。

詐欺・悪質商法に関する相談
○ インターネット閲覧中に、身に覚えのないアダルトサイト閲覧等料金未納の画面が表示され、料金を請求された。
○ インターネットのサイトで商品を購入し、代金を振り込んだが品物が届かない。

1．「情報セキュリティの脅威」

危険の認識

1）インターネットに潜む危険

2）メールに潜む危険

3）日常業務に潜む危険

4）情報流出の責任

出典： IPA 情報セキュリティ読本 四訂版

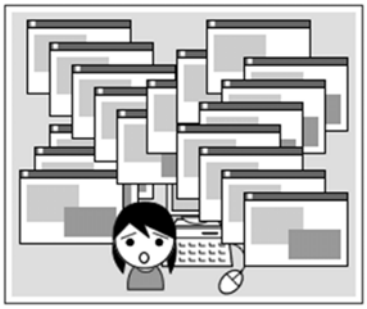
1）インターネットに潜む危険

- Webページを閲覧しただけで不正プログラムに感染してしまう
- リンクをクリックしただけで不正な請求をされたり、個人情報を盗まれるなどの被害に遭うことがある
- 不正なプログラムを誤ってダウンロードしてしまう

出典：IPA 情報セキュリティ読本 四訂版

1）インターネットに潜む危険

事例：ホームページを見ただけで・・・



好きな歌手のファンが集まる電子掲示板を見ていたAさんは、「次回のコンサートのチケットが安く手に入るみたい。限定30枚だって。」という書き込みを発見しました。早速、参照先のホームページのリンクをクリックしてみると、画面にウィンドウが次々と現れて、マウスで次々と閉じても、とても間に合いません。しばらくすると、キーボードもマウスも動かなくなり、コンピュータが停止（フリーズ）してしまいました。

これは、リンク先がブラウザクラッシャ、通称ブラクラと呼ばれる悪質なプログラムが置かれたホームページであったことが原因です。ブラウザクラッシャにはいくつかの種類がありますが、無限に新しいウィンドウを開くプログラムや、電子メールの新規ウィンドウを呼び出すプログラムを利用したものが有名です。電子掲示板やチャットなどで、参加者に対するいやがらせとして行われることが多いようです。

出典：総務省『国民のための情報セキュリティサイト』をもとにテクノ株式会社作成
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/case/03.html

2）メールに潜む危険

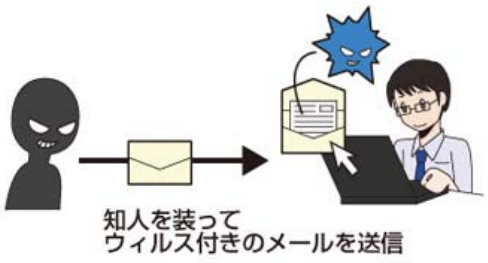
- スパムメール（迷惑メール）
- マルウェア　に感染
- フィッシングメール

マルウェア：コンピュータウイルス、スパイウェア、ボットなどの不正なプログラムのこと

出典：IPA　情報セキュリティ読本　四訂版

2）メールに潜む危険

事例：標的型攻撃で、企業の重要情報が・・・



ある組織が所有している機密情報が、電子メールで外部に送信されていることが判明しました。
この組織の内部から外部に向けた通信の中で、不審な通信が発見されたため、その通信元のパソコン1台を特定し、ただちにネットワークから切り離して調査をしました。その結果、その1台のパソコンがウイルス感染していることが判明したのです。さらに、その後の長い調査の結果、このパソコンに感染していたウイルスによって、組織内部の情報収集が実行されていた痕跡と外部と通信していた事実が確認されました。

発端は、ある職員の電子メールアドレスに、知人を装ったウイルス付きのメールが送られたことからでした。職員はこのメールを不審なメールであると全く疑わずに業務用のパソコンで開封し、ウイルスに感染してしまいました。しかもその後も、パソコンの調子に特に変わったところがなかったので、ずっと感染に気づかなかったのです。しかし、このメールは実際には知人から送られたメールではなく、送信元を偽った標的型攻撃のメールだったのです。
たった1通の標的型攻撃メールより、たった1台のパソコンがウイルス感染したことから、重要な組織情報が盗まれるという事態に発生することもあります。標的型攻撃には十分に注意しなければなりません。

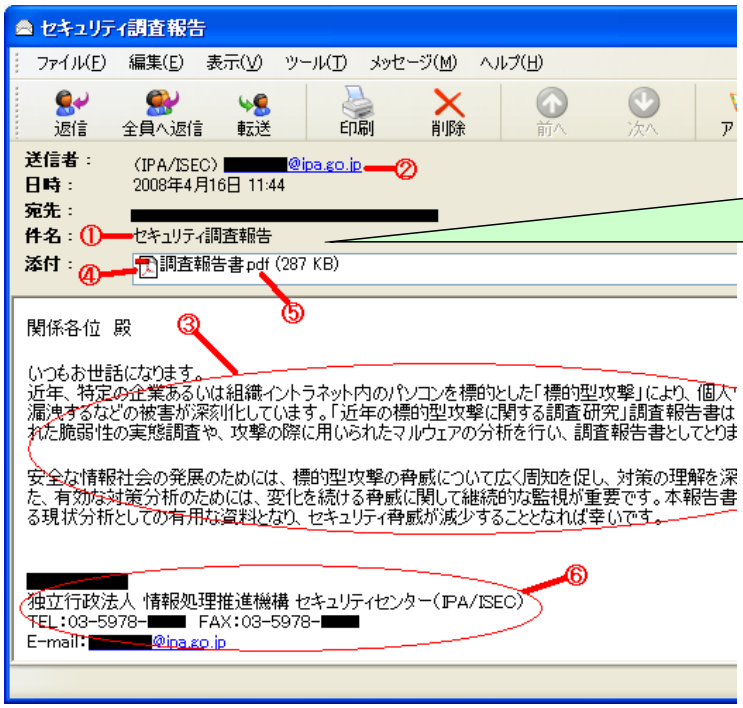
出典：総務省『国民のための情報セキュリティサイト』をもとにテクノ株式会社作成
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/case/09.html

1．「情報セキュリティの脅威」

テクノ株式会社

2）メールに潜む危険

- 公的機関を装う



① メールの受信者が興味を持つと思われる件名
② 送信者のメールアドレスが信頼できそうな組織のアドレス
③ 件名に関わる本文
④ 本文の内容に合った添付ファイル名
⑤ 添付ファイルがワープロ文書やPDFファイルなど
⑥ ②に対応した組織名や個人名などを含む署名

出典： IPA 情報セキュリティ読本 四訂版

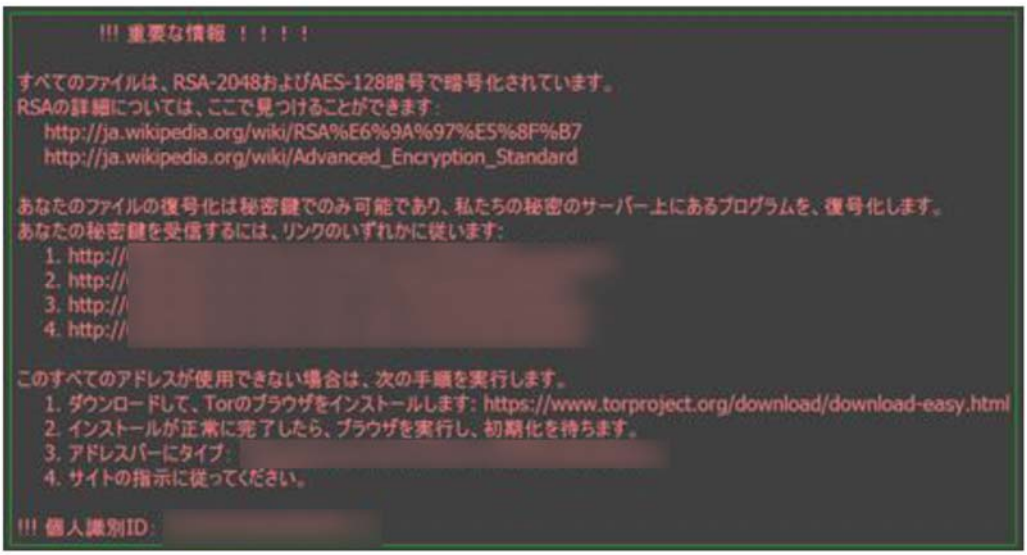
1．「情報セキュリティの脅威」

テクノ株式会社

2）メールに潜む危険

- 身代金要求型ウイルス（ランサムウェア）

パソコン上のファイルを暗号化するなどの障害を意図的に発生させ、その解決のための身代金を要求するマルウェア



出典： IPA ランサムウェアの脅威と対策

3）日常業務に潜む危険

- 外出や出張時に資料（紙の書類、USBメモリなどの記憶媒体）を持ち出す、不要になった書類を廃棄する、歓談時に仕事の話をする、といった何気ない行為が、情報漏えいの原因となることがある。

出典：IPA　情報セキュリティ読本　四訂版

2）日常業務に潜む危険

事例：情報セキュリティ対策は万全だったはずなのに・・・

ある会社での出来事です。Sさんが会社の情報管理担当者になって、もう3年になります。もともとコンピュータが好きなSさんだけあって、会社内の情報セキュリティ対策は万全と考えています。

それぞれの社員が使用するコンピュータはもちろん、サーバにもウイルス対策ソフトが導入されています。ウイルス対策ソフトに対しては、定期的なウイルス検知用データの更新も行っています。そして、外部からの侵入に備えて、ネットワークにファイアウォールも装備しました。

しかし、ある日、Sさんがインターネットの電子掲示板を見てみると、なんと自分の会社の顧客情報が漏洩していることがわかりました。いったいどうして・・・。

最近では、このように情報セキュリティ対策を施していたにも関わらず、情報が漏洩してしまったという事例も増えています。たとえば、このケースでは、ある1人の社員が仕事のデータを自宅に持ち帰った際に、自宅のコンピュータがウイルスに感染していて、そこから個人情報が漏洩してしまったということが考えられます。もしくは、誰かが業務データファイルの保存されていたUSBメモリをどこかで紛失してしまったのかもしれません。つまり、情報セキュリティ対策には、万全なものはないのです。

個人情報や機密情報を保有する企業や組織は、システムやソフトウェアによる情報セキュリティ対策だけでなく、厳密な社内ルール（情報セキュリティポリシー）の策定とその徹底、データベースやファイルサーバに対する権限設定など、多角的なセキュリティ対策が要求されるものです。

情報管理担当者は、基本的な情報セキュリティ対策だけでなく、社員への教育の徹底も、大切な情報セキュリティ対策のひとつであるということを心に止めておいてください。

また、情報セキュリティ上のリスクは、時間とともに変化するものです。そのため、現状の情報セキュリティ対策に満足するのではなく、最新の情報セキュリティ脅威の動向に常に気を配り、継続的に対策を見直すことが大切です。

出典：総務省『国民のための情報セキュリティサイト』をもとにテクノ株式会社作成
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/case/06.html

4）情報流出の責任

- 教育関連の企業であるベネッセが2895万人ぶんの顧客情報を流出させる事件がありました。このときに被害者1人あたり500円分の電子マネーなどをお詫びとして配布しました。約200億円以上の補償金を準備して対応したと言われています。

- 金額的な損失もあるが、法人の社会的信用を貶める結果にもなってしまいます。

ベネッセ 赤字136億円
4～6月 情報漏洩で特損260億円

ベネッセホールディングスが31日発表した2014年4～6月期の連結決算は、136億円の最終赤字になった。前年同期は26億円の最終黒字から一転、4～6月期として初めての最終赤字になる。通信講座などの顧客情報の漏洩で、おわびにかかる費用など260億円の特別損失を計上。問題が業績に与える影響を見積もれないとして15年3月期の業績予想を取り下げた。特別損失の内訳は顧客への補償に200億円、おわび文書の発送や事件後、エアバスへの違約金を「相当額負担せざるを得ない可能性がある」として今回、リスクを開示した。エアバスからの解約通知を受け、29日に開いた会見で西乃保慎一社長は「資金繰りに問題はない」としていた。

必ずしも破綻リスクに直結するわけではなく、業績や資金繰りが改善すれば解消される。今回、不採算の地方空港からの撤退や金融機関からの借り入れなどで対応する方針もあわせて発表した。

同社は11年、6機のA380を総額1915億円（現在価格）で購入する契約をエアバスと結んだ。だが支払いが滞ったことなどを理由にエアバスが契約解除を通告し、約700億円の違約金を求める意向とみられる。スカイマークは「違約金は合理性がなく、法的手段も視野に入れて対応する」としている。

海外の教育事業が伸びたほか、有料老人ホームを展開する介護事業の好調で増収を確保した。

本業のもうけを示す営業利益は12%減の49億円となった。国内教育事業は会員数の減少に加え、タブレット教材の導入でコストが増え、部門営業利益が27%減った。同日、福島保副会長と明田英治取締役が31日付で引責辞任する人事も発表した。

対策などに60億円を充てる。「補償の対象や具体的な内容については現在、検討中」（ベネッセ）。

売上高は前年同期比2%増の1155億円だった。主力の通信講座「進研ゼミ」や「こどもちゃれんじ」は会員減で苦戦している。在籍している延べ会員数は1064万人と1年前より5%近く減った。ただ、中国など

きょう

産相の認可必要

▽…電力会社が家庭など契約電力が50キロワット未満の顧客向けの料金を本格的に引き上げるには、政府の審査を受けたうえで経済産業相の認可が必要となる。企業向け料金は電力会社の判断で自由に変える

計算する大学教授

門委員会

って料金

か検討す

協議し、

1）インターネットに潜む危険への対策

○不審なサイトには近づかない
　さまざまな手法で罠が仕掛けられているので、脆弱性があると被害を受ける

○安易なダウンロードやインストールをしない
　誤ってトロイの木馬やキーロガーなどのウイルスをダウンロードしてしまう可能性がある
　個人情報をむやみに入力しない

○フィッシングの被害に遭わないために、クレジットカード番号などの入力は必要最小限にセキュリティ対策（SSL）が使用されているか確認する

２）メールに潜む危険への対策

〇不審なメールや添付ファイルは開かない

〇添付ファイルは、開く前や実行する前にウイルス検査を行う

〇見た目に惑わされず、添付ファイルの拡張子とアイコンを確認する

3）日常業務に潜む危険への対策

〇個人情報の取り扱いは、慎重に行う
　取り扱う情報に個人情報が含まれていないか確認すること。

〇目的の業務以外に使わない
　業務上得た情報は顧客からの預かりもの。
　個人の私的利用や話題にすることは厳禁。
　業務のみに使用し、適切に管理する。

〇情報を持っての移動、情報の運搬に注意する
　書類やUSBメモリ等の記憶媒体の持ち出し時は、置き忘れなどの紛失、盗難のリスクがあることを理解する。
　書類やUSB等の記憶媒体の持ち出しは、事前の承認を得るなど対応を考える。

いざ、という時のために

- 自分で管理できないコンピュータには、個人情報を入力しない
- USBメモリの取り扱いに注意する
  自分が管理していないUSBメモリは接続しない
  自分が管理していないパソコンには接続しない
- **万が一のために、データは必ずバックアップする**
- ウイルス感染の兆候を見逃さない

- もし、ウイルスに感染してしまったら
  ①**システム管理者に報告**
  ②**該当のPCの利用を速やかに中止し、ネットワークケーブルを外す**

出典：IPA 情報セキュリティ読本 四訂版

危険への共通対策

- 情報セキュリティの基本を知ろう
- ウイルスなどの不正プログラム（マルウェア）について理解しよう
- 実際のセキュリティ対策を施そう
- 情報セキュリティに使われている技術を理解しよう
- 法律について認識しよう

出典：IPA 情報セキュリティ読本 四訂版

2.「対策の基本的な考え方」

・情報セキュリティの基本的な内容

・丁寧に書いてある

・誰でも無料で閲覧可能
（インターネットからダウンロード、スマホアプリも）

出典： 内閣サイバーセキュリティセンター（NISC）

3.「必要なセキュリティ対策」

必要なセキュリティ対策

企業や組織においては、どのような情報資産を持っているかを理解して、ウイルス対策ソフトの導入やファイアウォールと呼ばれる機器を設置することで、ウイルス感染や情報漏洩のリスクを可能な限り軽減する適切な情報セキュリティ対策を行う必要がある。

Fortigate（フォーティゲート）での対策

- Fortigateは世界一のシェアを有する統合脅威管理(UTM)アプライアンスです。フォーティゲート一台でファイアウォール・アンチウィルス・不正侵入防御・コンテンツフィルタリング・アンチスパムなどを利用できます。
- 至誠会様の各施設へ導入されています。

ウイルスバスタービジネスセキュリティでの対策

- 従業員の不注意がセキュリティインシデントにつながることがあります。そのため、従業員が脅威と接触する前に、脅威を阻止することが重要です。ウイルスバスター ビジネスセキュリティは、メール、Web、ファイル共有を保護し、URLフィルタリングによって不適切なWebサイトへのアクセスをブロックします。

- 至誠会様の各施設へ導入されています。

必要なセキュリティ対策の心得

・規則を知り、遵守する
・情報セキュリティ上の脅威と対策を知る
・「自分だけは…」、「これぐらいなら…」は通用しない
・必ず上司、管理者に報告・相談する
・特に、情報漏えいに気を付ける