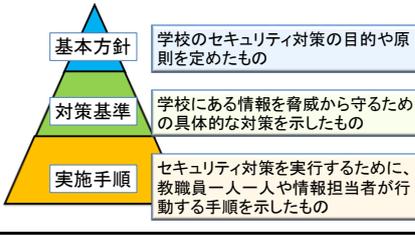


スライド 1	<div style="text-align: center;"> <h2>情報セキュリティ</h2>  <p>愛媛県総合教育センター 教育開発部 情報教育室</p> </div>	<p>(自校の情報セキュリティポリシーを、配布しておく。)</p> <p>本日は、「情報セキュリティ」について研修します。</p> <ul style="list-style-type: none"> ● 						
スライド 2	<p>1 情報セキュリティとは</p> <p style="text-align: center; color: blue;">情報資産を安全に守ること</p> <div style="text-align: center; background-color: yellow; padding: 5px; border: 1px solid black;"> 情報セキュリティ対策 </div> <p style="text-align: center;">↓</p> <p>全ての教職員が <u>正しい知識と行動</u>を身に付ける。</p>	<p>情報セキュリティとは、一言で言うと「情報資産を安全に守ること」です。</p> <p>学校には、児童（生徒）の成績はもとより、テストや配布物などのたくさんの情報資産があり、全ての教職員が取り扱っています。</p> <ul style="list-style-type: none"> ●情報セキュリティ対策をする上で、最も大切なことは、 ●全ての教職員が、正しい知識と行動を身に付けることです。 ● 						
スライド 3	<p style="text-align: center;">情報セキュリティの3要素</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #ADD8E6; text-align: center; padding: 5px;">機密性</td> <td style="padding: 5px;">・許可された人以外は使えないこと。</td> </tr> <tr> <td style="background-color: #90EE90; text-align: center; padding: 5px;">完全性</td> <td style="padding: 5px;">・正確で改ざんされていないこと。</td> </tr> <tr> <td style="background-color: #FFDAB9; text-align: center; padding: 5px;">可用性</td> <td style="padding: 5px;">・利用すべき時に利用できること。</td> </tr> </table>	機密性	・許可された人以外は使えないこと。	完全性	・正確で改ざんされていないこと。	可用性	・利用すべき時に利用できること。	<p>情報セキュリティには、機密性、完全性、可用性という三つの要素が必要です。</p> <ul style="list-style-type: none"> ●機密性とは、許可された人以外は使えないことです。 <p>紙媒体のものは金庫で保管したり、デジタルデータはパスワードの設定や暗号化して保存したりするなど、関係者以外は使えないようにすることが重要です。</p> <ul style="list-style-type: none"> ●完全性とは、データが正確で改ざんされていないことです。 <p>各情報資産の管理者を明確にし、その人が責任を持って管理することが重要です。</p> <ul style="list-style-type: none"> ●可用性とは、利用すべき時に利用できることです。 <p>非常時に備えて、データのバックアップをとることが重要です。</p> <ul style="list-style-type: none"> ●
機密性	・許可された人以外は使えないこと。							
完全性	・正確で改ざんされていないこと。							
可用性	・利用すべき時に利用できること。							

ス ラ イ ド 4	<p>2 情報セキュリティの具体策</p> <p>学校としての取組</p> 	<p>それでは、情報セキュリティの具体策について、学校のルールとして取り組まなければならないことについて説明します。</p> <ul style="list-style-type: none"> ●
ス ラ イ ド 5	<p>情報セキュリティポリシー</p> <p>情報資産の管理に関する方針を示した文書</p>  <p>基本方針 学校のセキュリティ対策の目的や原則を定めたもの</p> <p>対策基準 学校にある情報を脅威から守るための具体的な対策を示したもの</p> <p>実施手順 セキュリティ対策を実行するために、教職員一人一人や情報担当者が行動する手順を示したもの</p>	<p>(自校の情報セキュリティポリシーと「基本方針」「対策基準」「実施手順」の言葉が合わない場合は、変更してください。)</p> <p>お配りしている情報セキュリティポリシーを御覧ください。</p> <p>この情報セキュリティポリシーは本校の決まりであり、学校にある情報資産の管理に関する方針を示した文書です。</p> <p>情報セキュリティポリシーには、基本方針、対策基準、実施手順が記載されていますが、</p> <ul style="list-style-type: none"> ●基本方針とは、学校のセキュリティ対策の目的や原則を定めたものです。 ●対策基準とは、学校にある情報を脅威から守るための具体的な対策を示したものです。 ●実施手順とは、セキュリティ対策を実行するために、教職員一人一人や情報担当者が行動する手順を示したものです。 <ul style="list-style-type: none"> ●
ス ラ イ ド 6	<p>情報セキュリティの検討</p> <ol style="list-style-type: none"> (1) 何を守るのか。 (2) どのような脅威があるのか。 (3) ぜい弱性は何か。 (4) どのような損失が発生するか。 (5) どのようにして守るか。 	<p>情報セキュリティを検討する時に考えなければならないことには、次の五つがあります。</p> <ul style="list-style-type: none"> ●(1) 何を守るのか。 ●(2) どのような脅威があるのか。 ●(3) ぜい弱性は何か。 ●(4) どのような損失が発生するか。 ●(5) どのようにして守るか。 <p>各検討内容について、詳しく説明します。</p> <ul style="list-style-type: none"> ●

ス
ラ
イ
ド
7

(1) 何を守るのか

情報資産	管理者	保存場所	公開対象者	重要度
生徒(児童)名簿	教頭	サーバー	校内	大
同窓会名簿	教頭	サーバー	校内	大
定期考査問題	教務主任	USB	職員	大
成績一覧	教務主任	サーバー	職員	大
緊急連絡網	教頭	サーバー	校内・該当学級	大
保健統計	養護教諭	サーバー	校内・保護者	大
入試成績	担任	サーバー	校内	大
調査書	担任	サーバー	校内	大
通知票の下書き	担任	U S B		大
所属別名簿	教頭	USB	校内	中
評価基準	教務主任	CD	校内・保護者	中
学校要覧	教頭	サーバー	一般	小
教育計画	教務主任	サーバー	一般	小
進路結果	進路指導	CD	一般	小

(1) 何を守るのか

学校において、情報資産は、基本的に帳票という形で保存されています。

●児童（生徒）名簿、同窓会名簿、定期考査問題などです。

重要なことは、各帳票の管理者を明確にし、責任を持って管理することです。

●帳票ごとに、管理者、保存場所、公開対象者、重要度を決めていますので、その範囲内で使用してください。

●特に、重要度の高い帳票には、児童（生徒）の個人情報が含まれていますので、取扱いに注意してください。

ただし、この表は一つの例ですので、本校の取扱いのルールについては、情報セキュリティポリシーで確認してください。

●

ス
ラ
イ
ド
8

(2) どのような脅威があるのか



(2) どのような脅威があるのか

情報資産に対して、好ましくない影響を及ぼすものを脅威と呼びます。

脅威を大きく分けると、●環境的脅威、●偶発的脅威、●意図的脅威の三つに分けられます。

●環境的脅威とは、地震、津波、火災、洪水、落雷などの自然災害です。

この脅威によって、情報消失や業務停止のおそれがあります。有効な対策は、データのバックアップです。

●偶発的脅威とは、入力ミス、データ削除、設定ミス、紛失などの自分自身がしてしまうミスです。

●意図的脅威とは、盗聴、改ざん、不正アクセス、ウイルス、車上荒らしなどの、第三者による悪意のある行為です。

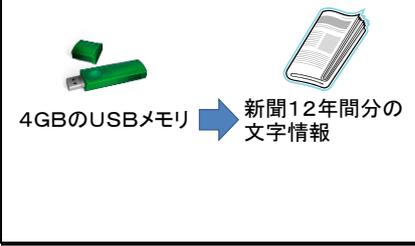
偶発的脅威、意図的脅威のことを人的脅威と言いますが、これにより、情報漏えい、情報消失、業務停止の恐れがあります。

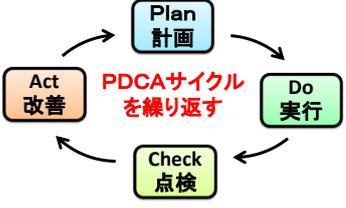
●これらの脅威によってもたらされる事故で、最も怖いのは情報漏えいです。

●

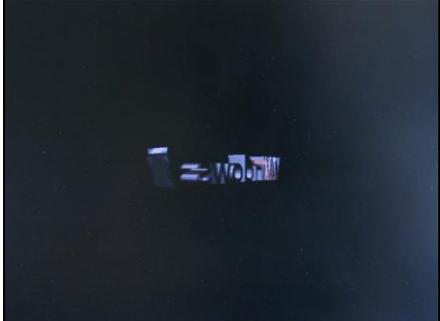
<p>ス ラ イ ド 9</p>	<p>個人情報漏えい事故例</p> 	<p>情報セキュリティが問題となった事件や事故の多くに情報漏えいがあります。 実際に個人情報が漏えいした事故例をいくつか紹介します。</p> <ul style="list-style-type: none"> ●
<p>ス ラ イ ド 10</p>	<p>愛媛県の県立高等学校で、就学支援金の関係書類などを紛失した。</p> <p>生徒138人分の氏名や住所、保護者の所得状況などが書かれた書類を紛失した。誤って廃棄された可能性もある。(H28. 6. 15)</p> 	<p>一つ目は、紛失・管理ミスです。 (読み上げ)</p> <ul style="list-style-type: none"> ●
<p>ス ラ イ ド 11</p>	<p>愛媛県内の公立中学校で、生徒の保健調査票を紛失した。</p> <p>生徒35人分の氏名や住所、既往症、保護者の連絡先などが書かれた書類を紛失した。(H28. 7. 15)</p> 	<p>ほかにも (読み上げ) 教職員の情報管理の不備によるものです。管理者の監督責任が問われる事例です。</p> <ul style="list-style-type: none"> ●
<p>ス ラ イ ド 12</p>	<p>大分県の県立学校で、置き忘れによりクラス分け資料が無料通信アプリによって拡散した。</p> <p>104人分の成績が入った資料を生徒が撮影し、撮影した画像が生徒間で拡散した。保護者からの情報提供により発覚した。(H28. 4. 8)</p> 	<p>三つ目は、名簿の置き忘れです。 (読み上げ) 皆さんは、教室に忘れ物をしてヒヤットしたことはありませんか。 スマートフォンやインターネットの利用が広がったという状況ならではのケースです。こうなると回収はできません。人から人へ、拡散していきます。</p> <ul style="list-style-type: none"> ●

<p>ス ラ イ ド 13</p>	<p>栃木県内の小中学校3校でパソコンがウイルスに感染し、個人情報が出た可能性がある。</p> <p>職員がパソコンで受信したメールの添付ファイルを開いたことでウイルスに感染した。在校生や卒業生の氏名や住所、成績情報、写真など約1,600人分の個人情報が出た可能性がある。(H28. 6. 24)</p> <p style="text-align: center;">ウイルス感染</p>	<p>四つ目は、添付ファイルを開いたことによるウイルス感染です。</p> <p>(読み上げ)</p> <p>メールによる標的型攻撃により、不正に情報が搾取された可能性がある事例です。</p> <p>潜伏型の不正プログラムは、目に見える動きをしないので、発見が遅れがちになります。</p> <p>不審メールは、さもありそうなメールに偽装されているので、ついつい添付ファイルを開きそうになるので、注意しなければなりません。</p> <p>このような不審メールがありえることを十分に認知しておくことが大切です。</p> <p>●</p>																				
<p>ス ラ イ ド 14</p>	<p>学校の情報漏えい事件や事故の件数</p> <table border="1"> <thead> <tr> <th>年度</th> <th>件数</th> </tr> </thead> <tbody> <tr> <td>23年度</td> <td>144</td> </tr> <tr> <td>24年度</td> <td>172</td> </tr> <tr> <td>25年度</td> <td>172</td> </tr> <tr> <td>26年度</td> <td>167</td> </tr> <tr> <td>27年度</td> <td>159</td> </tr> </tbody> </table> <p style="text-align: center;">一向になくならない</p>	年度	件数	23年度	144	24年度	172	25年度	172	26年度	167	27年度	159	<p>このような個人情報漏えい事故は、●一向に無くなる気配は見られません。</p> <p>残念ながら2・3日に一件は、全国のどこかの学校で何らかの事故が起こっています。</p> <p>●</p>								
年度	件数																					
23年度	144																					
24年度	172																					
25年度	172																					
26年度	167																					
27年度	159																					
<p>ス ラ イ ド 15</p>	<p>個人情報漏えい事故の原因</p> <table border="1"> <thead> <tr> <th>原因</th> <th>割合</th> </tr> </thead> <tbody> <tr> <td>紛失・置き忘れ</td> <td>67.9%</td> </tr> <tr> <td>盗難</td> <td>15.7%</td> </tr> <tr> <td>不正アクセス</td> <td>1.3%</td> </tr> <tr> <td>誤操作</td> <td>1.3%</td> </tr> <tr> <td>誤送信</td> <td>3.1%</td> </tr> <tr> <td>誤配布</td> <td>4.4%</td> </tr> <tr> <td>誤公開</td> <td>5.0%</td> </tr> <tr> <td>ワーム・ウイルス感染</td> <td>0.6%</td> </tr> <tr> <td>その他</td> <td>0.6%</td> </tr> </tbody> </table> <p style="text-align: center;">約80%</p> <p>平成27年度学校・教育機関における個人情報漏えい事故の発生状況 一調査報告書～第1版より (ISEN)</p>	原因	割合	紛失・置き忘れ	67.9%	盗難	15.7%	不正アクセス	1.3%	誤操作	1.3%	誤送信	3.1%	誤配布	4.4%	誤公開	5.0%	ワーム・ウイルス感染	0.6%	その他	0.6%	<p>情報漏えい事故の原因を表したグラフです。</p> <p>「紛失・置き忘れ」が最も多く、「盗難」が二番目に多く発生しています。この二つを合計すると約80%にもなります。</p> <p>情報漏えい事故のほとんどが、学校内部の教職員が関係した人的脅威によるものです。</p> <p>セキュリティポリシーのルールを破ったことやうっかりミスが原因です。</p> <p>●</p>
原因	割合																					
紛失・置き忘れ	67.9%																					
盗難	15.7%																					
不正アクセス	1.3%																					
誤操作	1.3%																					
誤送信	3.1%																					
誤配布	4.4%																					
誤公開	5.0%																					
ワーム・ウイルス感染	0.6%																					
その他	0.6%																					
<p>ス ラ イ ド 16</p>	<p>個人情報漏えい媒体</p> <table border="1"> <thead> <tr> <th>媒体</th> <th>割合</th> </tr> </thead> <tbody> <tr> <td>書類</td> <td>53.1%</td> </tr> <tr> <td>USBメモリ</td> <td>22.9%</td> </tr> <tr> <td>インターネット</td> <td>8.7%</td> </tr> <tr> <td>パソコン本体</td> <td>4.7%</td> </tr> <tr> <td>SDカード</td> <td>3.5%</td> </tr> <tr> <td>外付けハードディスク</td> <td>2.3%</td> </tr> <tr> <td>デジタルカメラ</td> <td>1.2%</td> </tr> </tbody> </table> <p style="text-align: center;">約80%</p> <p>平成27年度学校・教育機関における個人情報漏えい事故の発生状況 一調査報告書～第1版より (ISEN)</p>	媒体	割合	書類	53.1%	USBメモリ	22.9%	インターネット	8.7%	パソコン本体	4.7%	SDカード	3.5%	外付けハードディスク	2.3%	デジタルカメラ	1.2%	<p>どのようなものから漏えいしたのかというと、書類が最も多いのですが、二番目はUSBメモリです。パソコン本体、外付けハードディスクといった機器もあります。</p> <p>USBメモリは、取り扱う情報量が多い反面、簡単に持ち運べますが、情報漏えいの原因となりやすいので取扱には注意が必要です。漏れた情報が、インターネット上で拡散すると回収不可能です。</p> <p>●</p>				
媒体	割合																					
書類	53.1%																					
USBメモリ	22.9%																					
インターネット	8.7%																					
パソコン本体	4.7%																					
SDカード	3.5%																					
外付けハードディスク	2.3%																					
デジタルカメラ	1.2%																					

ス ラ イ ド 17	<p style="text-align: center;">USBメモリの情報量</p> 	<p>USBメモリで考えてみます。 4ギガバイトのUSBメモリは、新聞に換算してみると、どのくらいの情報が保存できると思いますか？</p> <p>●12年間分の文字情報に値します。 これだけの情報量を、簡単に持ち運べてしまうため、USBメモリの使用を禁止している学校も多くあります。</p> <p>●</p>
ス ラ イ ド 18	<p>(3) ぜい弱性は何か</p> <p>管理面 ・セキュリティポリシーの不徹底 ・セキュリティの運用管理の不備</p> <p>システム面 ・ウイルス対策の不徹底 ・重要データの暗号化の不備</p> <p>人的な面 ・ずさんなパスワード管理 ・情報セキュリティ研修の不徹底</p>	<p>(3) ぜい弱性は何か ぜい弱性とは、保安上の弱点のことを意味します。管理面、システム面、人的な面の三つの視点から考えてみます。</p> <p>●管理面では、セキュリティポリシーの不徹底、セキュリティの運用管理の不備などが挙げられます。 ●システム面では、ウイルス対策の不徹底、重要データの暗号化の不備などです。 ●人的な面では、ずさんなパスワード管理、情報セキュリティ研修の不徹底などです。 すなわち、我々のセキュリティに対する意識の低さが、システムの弱点になってしまいます。</p> <p>●</p>
ス ラ イ ド 19	<p>(4) どのような損失が発生するか</p> <p>(例) USBメモリの紛失 ウイルス感染や操作ミス → 情報消失 書類等のずさんな管理 → 情報漏洩</p> <p>民事裁判</p> <p>懲戒処分</p> <p>信用失墜</p>	<p>(4) どのような損失が発生するか</p> <p>●例えば、USBメモリの紛失、ウイルス感染や操作ミス、書類等のずさんな管理によって、情報消失、情報漏えいが起こります。</p> <p>その結果、</p> <p>●民事裁判で、多額の賠償金を求められることがあります。 ●問題を起こした本人には、懲戒処分の可能性もあります。 ●そして、何よりも大きな損失は、「信用失墜」です。一度失った信頼は、なかなか取り戻せません。一人のミスは、学校全体に関わる大きな損失につながってしまいます。</p> <p>●</p>

ス ラ イ ド 20	<p>(5) どのようにして守るか</p> <p>情報セキュリティポリシー</p> 	<p>(5) どのようにして守るか</p> <ul style="list-style-type: none"> ●まず、全教職員が情報セキュリティポリシーを守ることです。 ●計画を立て、●実行し、●一人一人がチェックシートなどで自己評価します。 <p>また、情報技術は日々進化しています。</p> <ul style="list-style-type: none"> ●そのため、情報セキュリティポリシーは毎年見直していますので、毎年確認するようにしてください。 ●このように、PDCAサイクルの実施によって、情報セキュリティポリシーは意味のあるものになります。
ス ラ イ ド 21	<p>情報セキュリティの最大の課題</p> <p>全教職員が関わる問題という認識</p> <p>「私は、得意ではないから・・・。」 「私は、専門家ではないから・・・。」</p>	<p>情報セキュリティの最大の課題は</p> <ul style="list-style-type: none"> ●「全教職員が関わる問題という認識」の有無です。 ●「私は、得意ではないから」とか、 ●「私は、専門家ではないから」 <p>関係ないという考えを持った教職員が一人でもいれば、●情報セキュリティは守られなくなってしまいます。</p>
ス ラ イ ド 22	<p>2 情報セキュリティの具体策</p> <p>個人としての取組</p> 	<p>次に、一人一人の教職員が個人としての取り組むべき内容について説明します。</p>
ス ラ イ ド 23	<p>守るべきこと</p> <ol style="list-style-type: none"> 1 情報資産は重要性分類に従い正しく管理する。 2 情報資産は許可なく校外へ持ち出さない。 3 パスワード付きのスクリーンセーバーを使用する。 4 安易なログインパスワードを設定しない。 5 ウイルス対策ソフトを最新の状態で使用する。 6 OSのアップデートを迅速かつ確実に行う。 7 使用ソフトウェアのアップデートを確実に行う。 8 不審なメールを開かない。 9 業務に関係しないWebサイトの閲覧をしない。 	<p>個人として、守るべきことは、次のようなことです。</p>

ス ラ イ ド 24	<p style="text-align: center;">守るべきこと</p> <ol style="list-style-type: none"> 1 情報資産は重要性分類に従い正しく管理する。 2 情報資産は許可なく校外へ持ち出さない。 3 パスワード付きのスクリーンセーバーを使用する。 4 安易なログインパスワードを設定しない。 5 ウィルス対策ソフトを最新の状態で使用する。 6 OSのアップデートを迅速かつ確実に行う。 7 使用ソフトウェアのアップデートを確実に行う。 8 不審なメールを開かない。 9 業務に関係しないWebサイトの閲覧をしない。 	<p>1 情報資産は重要性分類に従い正しく管理する。 先ほど述べたように、学校で決められたルールに従って、各帳票を正しく管理してください。</p> <p>●</p>
ス ラ イ ド 25	<p style="text-align: center;">守るべきこと</p> <ol style="list-style-type: none"> 1 情報資産は重要性分類に従い正しく管理する。 2 情報資産は許可なく校外へ持ち出さない。 3 パスワード付きのスクリーンセーバーを使用する。 4 安易なログインパスワードを設定しない。 5 ウィルス対策ソフトを最新の状態で使用する。 6 OSのアップデートを迅速かつ確実に行う。 7 使用ソフトウェアのアップデートを確実に行う。 8 不審なメールを開かない。 9 業務に関係しないWebサイトの閲覧をしない。 	<p>2 情報資産は許可なく校外へ持ち出さない。</p> <p>●</p>
ス ラ イ ド 26	<div style="border: 1px solid black; padding: 10px; text-align: center;"> <p style="background-color: #0056b3; color: white; padding: 5px; border-radius: 10px; display: inline-block;">USBメモリを持ち歩く</p></div> <p style="text-align: center;">・紛失による情報漏えい</p> <div style="text-align: center; margin: 10px 0;">  </div> <div style="background-color: #c00000; color: white; padding: 5px; border-radius: 10px; display: inline-block; margin: 0 auto;">校長の許可</div>	<p>特に危険なのが、USBメモリを持ち歩く行為です。 紛失による情報漏えい事故が後を絶ちません。 セキュリティポリシーでは、学校からUSBメモリを持ち出さないこと、私物のUSBメモリを使用しないことになっていると思います。</p> <p>●デジタルデータでも紙媒体でも、個人情報が入った情報資産を持ち出す際は、校長先生の許可を得てください。</p> <p>●</p>
ス ラ イ ド 27	<p>どうしても持ち出す必要がある場合</p> <div style="display: flex; align-items: center; margin: 10px 0;">  <div style="background-color: #333; color: white; padding: 5px; border-radius: 5px; display: inline-block;">管理番号001号</div> </div> <p>公的なもの 管理簿へ記入 パスワードロック 暗号化</p> <div style="background-color: #c00000; color: white; padding: 5px; border-radius: 10px; display: inline-block; margin: 10px auto;">必要最小限のデータ</div>	<p>USBメモリをどうしても持ち出す必要がある場合は、公的なUSBメモリを使用し、管理簿に記入してください。</p> <p>さらに、パスワードロックや暗号化機能の付いたUSBメモリが安心です。</p> <p>●そして、持ち出す情報は必要最小限にしましょう。</p> <p>●</p>
ス ラ イ ド 28	<p style="text-align: center;">守るべきこと</p> <ol style="list-style-type: none"> 1 情報資産は重要性分類に従い正しく管理する。 2 情報資産は許可なく校外へ持ち出さない。 3 <u>パスワード付きのスクリーンセーバーを使用する。</u> 4 安易なログインパスワードを設定しない。 5 ウィルス対策ソフトを最新の状態で使用する。 6 OSのアップデートを迅速かつ確実に行う。 7 使用ソフトウェアのアップデートを確実に行う。 8 不審なメールを開かない。 9 業務に関係しないWebサイトの閲覧をしない。 	<p>3 パスワード付きのスクリーンセーバーを使用する。</p> <p>●</p>

スライド 29	<div style="border: 1px solid black; padding: 10px;"> <div style="text-align: center; background-color: #0056b3; color: white; padding: 5px; margin-bottom: 10px;"> スクリーンセーバーの設定 </div> <ul style="list-style-type: none"> ・離席時の情報漏えい ・ + Lキーでログイン画面にする <div style="text-align: center; margin: 10px 0;"> </div> <div style="text-align: center; background-color: #c00000; color: white; padding: 5px; margin-bottom: 10px;"> 再開時にログオン画面に戻る </div> </div>	<p>スクリーンセーバーの後、マウスを動かさずとすぐに使える状態になっていないでしょうか？ 離席時の情報漏えいの危険があります。</p> <ul style="list-style-type: none"> ● 待ち時間を10分位に設定し、パスワードを入力しないと再開しないように設定しましょう。 <p>また席を離れる際は、電源を切るか、ウィンドウズキーとLキーを押して、ログオン画面の状態にしましょう。</p> <ul style="list-style-type: none"> ●
スライド 30		<p>デスクトップ上で右クリックし、「個人設定」から「スクリーンセーバーの設定」を選べば、このような画面が現れます。</p> <ul style="list-style-type: none"> ● 「再開時にログオン画面に戻る」に、チェックを入れてください。 ●
スライド 31		<p>そうすると、スクリーンセーバー起動中に、マウスを動かすと、</p> <ul style="list-style-type: none"> ●
スライド 32		<p>このように、ログイン画面に戻り、パスワードを入力しなければ使えないようになります。</p> <ul style="list-style-type: none"> ●
スライド 33	<div style="border: 1px solid black; padding: 10px;"> <p style="text-align: center;">守るべきこと</p> <ol style="list-style-type: none"> 1 情報資産は重要性分類に従い正しく管理する。 2 情報資産は許可なく校外へ持ち出さない。 3 パスワード付きのスクリーンセーバーを使用する。 4 <u>安易なログインパスワードを設定しない。</u> 5 ウイルス対策ソフトを最新の状態で使用する。 6 OSのアップデートを迅速かつ確実に行う。 7 使用ソフトウェアのアップデートを確実に行う。 8 不審なメールを開かない。 9 業務に関係しないWebサイトの閲覧をしない。 </div>	<p>4 安易なログインパスワードを設定しない。</p> <ul style="list-style-type: none"> ●

スライド 34	<div style="text-align: center;">  <p>・安易なパスワード ・パスワードのメモ書き</p>  </div>	<p>ログインパスワードを設定しても、そのパスワードが容易に推測できるものであれば、意味がありません。</p> <p>また、複雑なパスワードであっても、簡単に目に触れるところに書かれていても意味がありません。実際、パスワードが書かれたメモを見て、生徒が教員用サーバーに侵入した事件もあります。</p> <p>●パスワード管理が適切になされなければ、不正アクセスの危険性が高まります。</p> <p>●</p>																												
スライド 35	<div style="text-align: center;"> <p>パスワードの最大解読時間</p> <table border="1" data-bbox="231 739 619 940"> <thead> <tr> <th rowspan="2">文字の種類</th> <th rowspan="2">使用文字数</th> <th colspan="4">入力桁数</th> </tr> <tr> <th>4桁</th> <th>6桁</th> <th>8桁</th> <th>10桁</th> </tr> </thead> <tbody> <tr> <td>英字 (小文字のみ)</td> <td>26</td> <td>約3秒</td> <td>約37分</td> <td>約17日</td> <td>約32年</td> </tr> <tr> <td>英字(大・小) +数字</td> <td>62</td> <td>約2分</td> <td>約5日</td> <td>約50年</td> <td>約20万年</td> </tr> <tr> <td>英字(大・小) +数字+記号</td> <td>93</td> <td>約9分</td> <td>約54年</td> <td>約1千年</td> <td>約1千万年</td> </tr> </tbody> </table> <p><small>※すべての組み合わせを試すために必要な時間を計算。記号は31文字使用できるものとした。 使用パソコン:OS:Windows Vista Business 32bit版、プロセッサ:Intel Core 2 Duo T7200 2.00GHz、メモリ:3GB 引用元 IPA(独立行政法人 情報処理推進機構)</small></p> </div>	文字の種類	使用文字数	入力桁数				4桁	6桁	8桁	10桁	英字 (小文字のみ)	26	約3秒	約37分	約17日	約32年	英字(大・小) +数字	62	約2分	約5日	約50年	約20万年	英字(大・小) +数字+記号	93	約9分	約54年	約1千年	約1千万年	<p>こちらは、パスワードの最大解読時間を表したものです。</p> <p>文字の種類と桁数の違いごとの、パソコンを使用して全ての組み合わせを試すのに必要な時間です。</p> <p>●小文字の英字を4桁で組み合わせで作ったパスワードは、約3秒で破られます。</p> <p>文字の種類や桁数を増やせば、解読に時間が掛かります。</p> <p>●より強固なパスワードになるよう、大文字・小文字の英字と数字、記号を混ぜた8桁のパスワードを設定するようにしてください。</p> <p>●</p>
文字の種類	使用文字数			入力桁数																										
		4桁	6桁	8桁	10桁																									
英字 (小文字のみ)	26	約3秒	約37分	約17日	約32年																									
英字(大・小) +数字	62	約2分	約5日	約50年	約20万年																									
英字(大・小) +数字+記号	93	約9分	約54年	約1千年	約1千万年																									
スライド 36	<div style="text-align: center;"> <p>守るべきこと</p> <ol style="list-style-type: none"> 1 情報資産は重要性分類に従い正しく管理する。 2 情報資産は許可なく校外へ持ち出さない。 3 パスワード付きのスクリーンセーバーを使用する。 4 安易なログインパスワードを設定しない。 5 <u>ウイルス対策ソフトを最新の状態で使用する。</u> 6 <u>OSのアップデートを迅速かつ確実に行う。</u> 7 <u>使用ソフトウェアのアップデートを確実に行う。</u> 8 不審なメールを開かない。 9 業務に関係しないWebサイトの閲覧をしない。 </div>	<ol style="list-style-type: none"> 5 ウイルス対策ソフトを最新の状態で使用する。 6 OSのアップデートを迅速かつ確実に行う。 7 使用ソフトウェアのアップデートを確実に行う。 <p>●</p>																												
スライド 37	<div style="text-align: center;">  <p>・ぜい弱性をついたウイルス感染！</p>  </div>	<p>OSやソフトウェアは、アップデートをしなければ、ぜい弱性をついたウイルス感染の恐れがあります。</p> <p>●常に、最新の状態で使用することが大切です。</p> <p>●</p>																												

<p>ス ラ イ ド 38</p>	<p style="text-align: center;">やるべきこと</p> <ul style="list-style-type: none"> • ウイルス対策ソフトの使用 -最新のパターンファイル • OS及びソフトウェアのアップデート -Microsoftは毎月第2火曜の翌日 	<p>コンピュータウイルスは、毎日新しいものが発生し続けています。</p> <p>そのため、ソフトウェア会社は、新しいウイルスを発見すると、ウイルスを検知するためのパターンファイルというものを作成しています。</p> <p>ウイルス対策ソフトは、その最新のパターンファイルを入れておかなければ、新しいウイルスを発見できませんので、アップデートをする必要があります。また、OSやその他のソフトウェアも同様です。</p> <p>ちなみに、マイクロソフトは毎月第2火曜の翌日にアップデートプログラムが発表されます。</p> <p>校務用パソコンは自動的にアップデートするように設定されていると思いますが、家庭のパソコンも自動アップデートを設定し、常に最新の状態で使用するようにしてください。</p> <p>●</p>
<p>ス ラ イ ド 39</p>	<p style="text-align: center;">守るべきこと</p> <ol style="list-style-type: none"> 1 情報資産は重要性分類に従い正しく管理する。 2 情報資産は許可なく校外へ持ち出さない。 3 パスワード付きのスクリーンセーバーを使用する。 4 安易なログインパスワードを設定しない。 5 ウイルス対策ソフトを最新の状態で使用する。 6 OSのアップデートを迅速かつ確実に行う。 7 使用ソフトウェアのアップデートを確実に行う。 8 <u>不審なメールを開かない。</u> 9 <u>業務に関係しないWebサイトの閲覧をしない。</u> 	<p>8 不審なメールを開かない。</p> <p>9 業務に関係しないWebサイトの閲覧をしない。</p> <p>先程示した事例にあったように、メールやWebサイトからダウンロードしたファイルに、ウイルスが仕込まれていることがよくありますので、十分注意してください。</p> <p>●</p>
<p>ス ラ イ ド 40</p>	<p style="text-align: center;">不審なメールへの対応</p> <ul style="list-style-type: none"> • 件名やアドレス、メールアドレス、本文を確認し、不審な点があれば、<u>添付ファイルの開封や記載のあるURLのクリックは、絶対に行わず、削除する。</u> • 今までと違うメールアドレスの場合や拡張子が「.exe」の実行ファイルが添付されている場合などは、<u>電話で送信元に送信の有無を確認する。</u> 	<p>不審なメールへの対応として、</p> <p>件名やアドレス、メールアドレス、本文を確認し、不審な点があれば、添付ファイルの開封や記載のあるURLのクリックは、絶対に行わず、削除する。</p> <p>今までと違うメールアドレスの場合や拡張子が「.exe」の実行ファイルが添付されている場合などは、電話で送信元に送信の有無を確認する。</p> <p>この二つは、特に意識して守ってください。</p> <p>●</p>

ス ラ イ ド 41	<p>不審なメールを見分けるポイント</p> <ul style="list-style-type: none"> ・送信者が、心当たりのない個人や組織になっている。 ・メールアドレスが、フリーメールアドレスになっている。 ・メールアドレスが、過去にやり取りしたアドレスと異なっている。 ・メールアドレスから判断できる送信者と本文中にある差出人が一致しない。 ・本文及び添付ファイル名に文字化けや意味不明の文字列がある。 ・添付ファイルの種類が「.vbs」「.bat」等の拡張子になっている。 	<p>不審なメールを見分けるポイントは、送信者が、心当たりのない個人や組織になっている。メールアドレスが、フリーメールアドレスになっている。</p> <p>メールアドレスが、過去にやり取りしたアドレスと異なっている。</p> <p>メールアドレスから判断できる送信者と本文中にある差出人が一致しない。</p> <p>本文及び添付ファイル名に文字化けや意味不明の文字列がある。</p> <p>添付ファイルの種類が「.vbs」「.bat」等の拡張子になっている。(ファイルの拡張子が確認できるように、パソコンの設定をしておく)</p> <p>メールを開く前に、これらのことを必ず確認しましょう。</p> <p>●</p>
ス ラ イ ド 42	<p>最後に 知らなかったでは済まされない時代です。</p> <p>法令の遵守 義務の履行</p> <p>↓</p> <p>情報コンプライアンスの確立</p> <p>↓</p> <p>教職員としての責任ある行動</p>	<p>情報セキュリティは、知らなかったでは済まされない時代です。</p> <p>●法令の遵守と義務の履行によって、学校としての情報コンプライアンスを確立しなければなりません。</p> <p>●そして、何より一人一人が教職員としての責任ある行動をとることが大切です。全教職員の力で学校の情報セキュリティを高めていきましょう。</p> <p>●</p>
ス ラ イ ド 43	<p>情報セキュリティ</p>  <p>愛媛県総合教育センター 教育開発部 情報教育室</p>	<p>以上で、情報セキュリティの研修を終わります。</p>