ISMSとインシデント経験からの学び

2019年12月27日
川崎市立橘高校
情報科　布村 覚

発生：10月27日（日）早朝→tgmnファイル生成時刻

発見：10月28日（月）午前7時半前後（火入れ時）

異常：・サーバへのアクセス不可（ポート不通）

・教員からファイルにアクセスできない旨連絡

特異性：サーバ直撃

従来のウィルス感染

➡クライアントにトロイ、マルウェア、WINMX/WINNY

橘高サーバー、ウイルス感染　アクセスできず、資料暗号化

サイバー犯罪　社会 神奈川新聞 2019年11月01日 19:33 配信記事より引用

川崎市役所

　川崎市教育委員会は１日、市立橘高校（中原区）の校内ネットワーク・サーバーがコンピューターウイルスに感染したと発表した。サーバーへのアクセスができなくなったほか、保存されていたデータファイルが使用できない状態となっている。データの外部流出は同日現在、確認されていない。

　市教委によると、１０月２８日に同校教諭がパソコンからサーバーにアクセスしたところ、資料の一部が暗号化されていたほか、画面上にウイルス感染を示唆する英文の文章があるのを確認した。

　サーバーには生徒が授業で作った資料のほか、教諭が作成した進路指導資料などが保存されている。一部のデータの復元は不可能とみられるが、同校は保守業者に復旧作業を依頼し、可能な限りデータの復元に努めるとしている。

被害：指導用LANサーバ⇒ランサムウェア、暗号化

ウィルス対策ソフトウェア破壊

Active Directory、File、Proxy、Call、Backup全域

個人ドキュメントドライブ：.doc→.tgmn（暗号化）

教材用ドライブ、共有用ドライブ：全ての拡張子

提出用ドライブ　合計1．4TB

脅迫文

・全フォルダに！TGMNで始まるテキストファイル

・作成日時　10月27日（日）05:30～09:13

被害範囲

教員：英語科・体育科・情報科など教科教材

生徒成果物（評価対象）、その他

生徒：教科成果物ドキュメント・コンテンツ

生徒会各組織(部活動）ドキュメント・コンテンツ

原因：不明～復旧を優先

リスク：電子メール添付ファイル、Webサイト

※ 2017年インシデント…ランサムウェア「WannaCry」

→ポート445から遠隔侵入　NHK「クロ現」より

過去１４年間

初期の数年間：教科情報での指導～生徒会活動

現在　教科から離れて生徒の文化伝承へ

➡メディアデザイン（音声・動画・ＣＧ編集）

　専門学科・生徒会行事・部活動の問題解決学習

➡ドキュメンテーション共有化による協働学習

当時の流行語：ＰＢＬ

problem based learning

project based learning

生徒への影響例

放送委員会	学校説明会用コンテンツ編集
国際科	学科説明会用コンテンツ編集、語学研修に係る企画運営ドキュメント
	実践画像及び生徒による編集・メディアコンテンツ
スポーツ科	学校説明会用、学科発表編集ドキュメント・メディアコンテンツ
	スポーツテスト企画運営ドキュメント・メディアコンテンツ、
	小学校テスタ企画運営ドキュメント・メディアコンテンツ、
	体育祭企画運営ドキュメント・メディアコンテンツ
	学年スポーツ企画ドキュメント・メディアコンテンツ
進路指導室	AO・公募推薦指導用ベネッセドキュメント　小論文・面接過去問
英語科	ES１・２・３授業、国際理解授業運営、課題研究
情報科	情報の科学・社会と情報授業
部活動	陸上競技　トレーニング・大会データ分析
	ダンス部　ＢＧＭコンテンツ
	将棋部・山岳部・天文科学部ドキュメント…
３学年	卒業アルバム編集作業・画像の蓄積
国際科	学科説明会デモンストレーション授業
各クラス	歌合戦、文化祭関係ドキュメント・メディアコンテンツ

共有ドライブ		第2階層	第3階層	第4階層	第5階層
定時制	全日制	2016年度	略		
		2017年度	略		
		2018年度	略		
		2019年度	学年	1学年	1～7組
				2学年	1～7組
				3学年	1～7組
					卒業アルバム
			生徒会	委員会	歌合戦
					体育祭
					文化祭
					放送
				部活	各部
			国際科	任意	
			スポーツ科	任意	

ISMS導入：2006年度構築～校務（業務）

個人情報保護に係る情報資産管理の現場対応

→ISO27001の研究：運用面のリスクアセスメント

機密性・脆弱性・完全性・可用性の4観点

・リスク値設定（ISOは任意性を認めている）

・リスク評価式（リスク評価法）設定

・受容リスク値設定（係争費用、損害賠償額など除く）

リンク先：情報の科学　3編　問題解決

「モデル化とシミュレーション」

P：データの重要性	値
成績・健康などセンシティブ情報	4
データ自体で個人を特定可能	3
他のデータと併せると個人を特定可能	2
Q1：機密性（保管場所の物理状態）	値
制限なくアクセス可能	4
職員在室による弱い制限	3
入室管理又は施錠による制限	2
Q2：脆弱性（保管場所の管理状態）	値
制限なし	4
形式的対策あり（帳簿記載）	3
物理的対策あり（鍵付棚・暗号等）	2

R:完全性(データ管理)	値
一切の誤記・改ざん不許	4
特定担当が必要な訂正を可能	3
必要な訂正を可能とする	2
S:可用性(影響の範囲)	値
学校全体	4
各組織	3
担当者	2

T：脅威度（紛失・漏洩の頻度）T=Q1*Q2	値
誰でも持出し・読取り可能(1月に1度程度)	16
従事者の過失で逸失・改変(1年に1度程度)	9
悪意の人的行為で逸失・改変(10年に1度程度)	4
自然災害・戦争争乱時に逸失（50年に1度程度）	1

本件インシデントの要因

ISO規格➡想定内

セキュリティに関する対策脅威度算出法（本校）

評価式を以下に設定

総リスク値＝P×Q1×Q2×R×S＞＝324（受容）

脅威度（紛失・漏洩頻度）T＝Q1×Q2＞＝9（受容）

➡機密性Ｑ１、脆弱性Ｑ２改善によりセキュリティレベル向上

ISO27001が求めるリスク評価法における脅威度

➡機密性・脆弱性２つの要素により算定

インシデントに対する振り返りと教訓

システム管理側の側面

・要求仕様策定時におけるLAN自体へのリスク評価

ルータ、ファイアウォール、プロキシ

➡ハードウェア、ソフトウェア両面

リスクの定量化、現状：ＰＣ性能、通信速度偏重

指導上の側面（ユーザとしての構え）

・指導用ネットワークへのＩＳＭＳ運用

ネットワークセキュリティの分担

遠隔操作による攻撃･･･ハードウェア・ソフトウェアを活用した防御

インターネット

365日24時間導通状態･･･常時攻撃を受ける可能性

ルータ･･･経路制御

ファイアウォール（ハード）･･･LANへの攻撃に対する防御

プロキシ･･･フィルタリング（アクセス可能なサイトを制限）

サーバ･･･ウィルス対策ソフト（ソフト）

ファイアウォール（ソフト）･･･PC単体の通信ポート制限、プロトコル制御

クライアントPC･･･ウィルス対策ソフト（ソフト）

可搬媒体、WEBサイト閲覧・ダウンロード、電子メールからの侵入対策

･･･操作上の防御手段＝ウィルスチェック

入退出管理、利用後の端末電源管理

システム管理者の役割

エンドユーザの役割

残留課題

進路指導（フロントヤード）

外部通信を可能とする環境設定必須

B社プログラムに依存

・模試結果→クラウド上でデータ分析結果

・志望校の過去問　　・受験カレンダー

WEB出願の実行

進路指導（バックヤード）

外部通信不可

セキュリティポリシー

校務用コンピュータ

・

当面の解決案

・指導用LANを活用しつつ、保存先を外部可搬媒体とする。

・筐体の保管先は施錠可能なロッカーとする。

・ファイルは可搬媒体を介して、校務用ネットワークへ移動。

１０月２８日～１２月１３日　**「情報の科学」アンプラグドでの授業**

・ＲＤＢ	ペン紙　テーブル切り貼り
・モデル化とシミュレーション	手計算
・統計／分析	ペン紙でプロット➡ヒストグラム／散布図
	手計算で標準偏差と偏差値まで
・プログラミング	ペン紙でアルゴリズム➡ソート・サーチ
	（JavaScript　前期に終了）

上記項目に**ネットワークの範囲を加えて後期定期考査実施**

➡正答率は前年度比で若干の向上　**問題の解法理解に実習は無関係**

昨年度ＳＱＬでオンラインＤＢ

➡定期考査後　ＡＣＣＳＥＳＳでオフラインＤＢ

５０分①ＣＳＶからインポート　②クエリで結合・射影・選択　③Excel出力

資料格納　strnun mountain view

http://strnun.fool.jp