本当にあったインシデント

―― 忘れてはいけない記録 ――

2026年6月19日

株式会社NS・コンピュータサービス
カスタマーサービス本部　IDCサービス部
小杉 健太

自己紹介

名前	小杉 健太		
年齢	51（セキュリティおじさん）		
所属	（株）NS・コンピュータサービス		
	カスタマーサービス本部　IDCサービス部　サービス課		
仕事	システム営業（複合機営業）	9年	パジェロミニ→HR-V
	ユーザーサポート（文教・公共）	9年	HR-V→スイフト→フリード
	ユーザーサポート（親会社・グループ）	8年	フリード
	社内サポート	2年	フリード→N-BOX
趣味	インドア（マンガ・アニメ・ゲーム・ガンプラ・TCG）		
	アウトドア（キャンプ、ソフトボール）		

インシデントとは？

いつも通り仕事をしている、そのとき。

画面が止まる。
ログインできない。
データが消える。
「何もしてないのに壊れた…」

――それが、インシデント。

そのページは何度も蘇る…

1、そのページは何度も蘇る…

2004年ごろ　N県　卸Z社

社長PCのホームページが勝手に変わるという電話連絡があった。

該当のPCを確認すると、すでにIEは侵されていて、
ホームページは見知らぬサイトへと書き換えられていた…。

いつものYahoo！に変更するものの、再起動で元に戻ってしまう。

1、そのページは何度も蘇る…

通報前夜、社長自身でフリーソフトウェアをPCへインストールしたとのこと。

そのツールにブラウザハイジャッカーが混入していたため、
ホームページが書き換わった模様。

レジストリからホームページ設定を修正し、一件落着。

ウイルス対策ソフト、デスクトップPC一式　後日お買い上げ。

そこにあったはずの写真…

2、そこにあったはずの写真…

2010年ごろ　N県　Y小学校

整理中に気づいた。

共有フォルダの写真が、消えている。
10年分、まとめてだ。
バックアップはない。

復元しても、戻るのはわずか一部だけ。

あとの記録は――二度と触れられない場所に消えていた。

2、そこにあったはずの写真…

共有フォルダの整理を行っていた。

バックアップ用外付けHDDに「移動」を行っていたところ、
操作を誤り写真保存フォルダを丸ごとどこかへ移動した。

復元ソフト（フリー）を試すが、1割程度復元して終わり。
フルバックアップがない状況のため、それ以上の復旧は見送り。

児童の写真は、もうどこにも残っていなかった…。

保護者から写真提供され、卒業アルバムは完成した…。

全て読めなくなった日…

3、全て読めなくなった日…

2017年ごろ　N県　X中学校

サポートの電話が鳴った。

「共有フォルダのファイルが開けない」
Excel、Word、PowerPoint――すべてが、突然開けなくなったという。

確認を進めるうちに、異変は広がる。対象のフォルダだけではない。
X中学校の領域にあるファイルまでも、次々と開けなくなっていく。

まるで順番に、“読めない存在”へと変えられていくかのように…

3、全て読めなくなった日…

開けないファイルの特徴である、
- ファイル名がランダム文字列
- 暗号化されて開けない

また、感染PCの身代金要求画面表示から、当時流行していた
ランサムウェア「WannaCry」の感染を推測。

感染PCは、そのまま初期化された。
暗号化ファイルはバックアップから復元したため、真相は闇の中…。

幸い、バックアップを別ストレージに取っていたため、事なきを得た。

閉鎖環境で広がる侵食…

4. 閉鎖環境で広がる侵食…

2018年ごろ　N県　製造業W社

オフラインだから安全だ、と誰もが思っていた。
ネットワークはつながらない。インターネット接続もない。

だが、USBメモリだけは使われていた。

ある日を境に、様子が変わる。

通信もないのに、異変が広がっていく。
どこから来たのかも分からないまま、
その環境は、内側からゆっくり侵されていった…。

4. 閉鎖環境で広がる侵食…

完全オフライン環境である、測定機材が設置されている棟で、
70台以上のPCがマルウェアに感染した。

ある測定機材のPCがマルウェアの巣となり、
それに挿入されたUSBメモリを媒介に、1棟丸ごと感染。
事務棟のPCも複数台が感染した。

完全オフライン環境だから、大丈夫だろうと思われていた。

USBタイプの駆除ツールを駆使し、10日間ですべて駆除した。

開かない扉…

5、開かない扉…

2023年ごろ　V国　製造業V社

7日間の入れ替え作業計画。準備は万全だった。
作業は順調に進んでいた――最初の2日間は。

その後、少しずつ歯車が狂い始める。
原因の分からないトラブル。
積み重なる違和感。

そして帰国当日。
Administratorが、拒否される。
もう取り戻せないところまで、変わっていた。

5. 開かない扉…

ADサーバー2台の入れ替え、NW機器更新の対応で2名で渡越。

帰国当日、納品研修の直前に、
Administratorでサーバーへログインできないことが発覚。

日本側からリモートでNW機器ログを確認したところ、
同日深夜に社内からADサーバーに対しパスワード変更ログがあること発見。

操作者に確認し、新パスワードでログインできることを確認の上、検収完了。

以降、Administrator以外の管理ユーザーを即作成するようになりました。

インシデントとは？

セキュリティインシデントの多くは「人の行動」に起因する。

悪意ある攻撃だけでなく、善意の誤操作や判断ミス、
さらには問題の隠蔽によって被害が拡大するケースも多い。

そのため、技術対策だけでなく「人はミスをする前提」で
組織・仕組みを設計することが重要である。

―セキュリティおじさん

次はあなたの番かもしれない…