



前号でご案内させていただいた「情報セキュリティセミナー」は、お陰様で盛況のうちに終了し、皆様のセキュリティへの関心の高さを強く感じました。

そこで、今回はセキュリティに関する旬な話題と当社の取り組みを特集してみました。ご参考になれば幸いです。

-CONTENTS-

ご存知ですか、新たな脅威はポート80からあなたの情報を狙っています。

PDF ファイルアタックが日本上陸！

「情報セキュリティセミナー」盛況の中、無事終了！

知っ得！～Excel マメ知識～

ご存知ですか。

新たな脅威はポート 80 からあなたの情報を狙っています。

いま、Web (HTTP ポート 80 番) を狙った新しい脅威が問題になっていることをご存知でしょうか。

Web サイトを改ざんし、アクセスしてきたユーザの知らないうちに、ウイルスやスパイウェアを次々とダウンロードさせ、不正に企業情報や個人情報などを取得し、密かに感染被害を広げる脅威が数多く報告されています。

パソコンを使っていて、こんな経験はありませんか？

自分では開いたつもりのない知らないサイトに勝手に誘導された。

自分では公開したことのないメールアドレスに、スパムメールが届いた。

Webサイトにアクセスしたら、勝手に何かをダウンロードされた。

画像をダウンロードしたら、ずいぶん時間がかかっていた。

フィッシングメールが届いた。

オンラインバンクから、知らないうちにお金が引き出された。



こうした事例はすべて、「Web からの脅威」の一部です。

「Web からの脅威」、その狙いとは？

最近のニュースでも、オンラインバンク犯罪やフィッシング詐欺被害の拡大、社員が自宅にパソコンを持ち帰った際に、ウイルス感染し、情報漏えい事件に発展した例など、「Web からの脅威」が発端となる被害が多数報告されています。

- Web からの脅威「3つの狙い」 -

1. 企業や個人の機密情報を不正に収集し、闇市場で売買
2. 盗まれた顧客情報をフィッシング詐欺などに不正利用
3. ユーザの気付かないうちに、DDoS 攻撃などの踏み台に利用

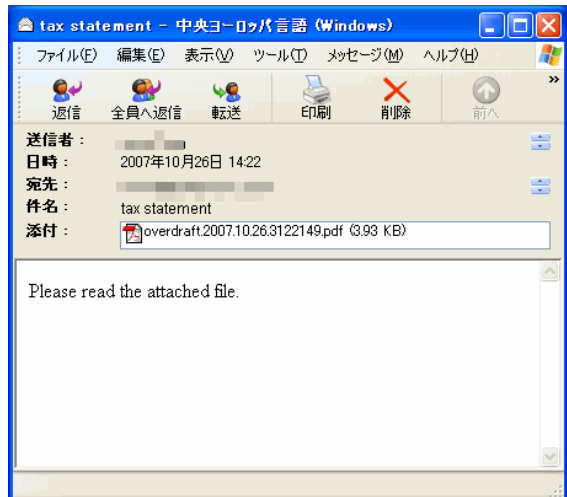
「Web からの脅威」の狙いは、企業や個人の機密情報の不正取得、それらを悪用した金銭目的の犯罪が急増しています。

PDF ファイルアタックが日本上陸！

懸念されていた PDF ファイルアタックの日本上陸が確認されました。

問題の PDF ファイルはメールによる拡散が確認されており、企業内で実際に流通しているような会計書類を装っています。

これらの悪意ある PDF ファイルはウイルスドロッパーとして動作します。ファイルを開き、脆弱性が悪用されることで、「1dr.exe」という「TSPY_PAPRAS.CF」トロイの木馬型スパイウェアがダウンロードされます。



現在、PDF ファイルアタックにて確認されているメール件名は次の通りです。

email title



- ・ Balance Report
- ・ Credit report
- ・ Personal Balance Report
- ・ Personal Credit report
- ・ Personal Financial Statement
- ・ tax statement
- ・ Your Credit points
- ・ Your Credit report
- ・ Your Credit File



この対策で予防しましょう！

- ・ 出所不明のメールを開かない。
- ・ 不審な PDF ファイルを開かない。
- ・ ウイルス対策ソフトを最新の状態にする。
- ・ アドビシステムズ社が提供する修正プログラムの適用を推進する。

10月5日(金)13:30より、県民ふれあい会館にて「内部統制と情報セキュリティ」のセミナーを開催いたしましたところ、多数のご参加をいただき無事終了することができました。

第一部ではトレンドマイクロ殿による「内部統制時代に向けて～トレンドマイクロの取組み～」と題し、内部統制時代における企業戦略とセキュリティ戦略のあり方、セキュリティリスクとIT統制のメリットについて熱く語っていただきました。また、最近の脅威である「Webからの脅威(前頁参照)」に対する注意喚起とその対策について享受いただきました。



第二部では当社の情報リスク管理に対する取組みとして、情報セキュリティ委員会の活動内容、運用中の情報セキュリティマネージメントシステム(ISO27001)の資産管理、人的資源管理、物理的環境的管理、通信・運用管理/モバイルPC管理、電子メール利用管理、セキュリティインシデント管理、アクセス管理、個人情報管理、ウイルス対策についてご紹介させていただきました。(以下、一部抜粋)

通信・運用管理 / モバイルPC管理

- ネットワーク接続管理
- ネットワーク接続は申請要(IPアドレス) 1
- システムログインの認証要(ID・パスワード)
- モバイルPCの認証、暗号化 2
- システム運用管理
- リソース管理
- ハード・ソフト導入の承認要 3



[以下のツールにより運用状況の監査等を実施しております]

- 1:未登録端末の監視を情報漏洩対策ツールの「C-WAT」にて常時監視
- 2:認証は登録拒否率0%(実績値)、経時変化対応の指紋認証装置「e-UBF」、暗号化は「秘文AE InformationCypher」
- 3:資産管理ツールの「PALLET CONTROL」により情報収集

また、併せて行いました「セキュリティプロダクト」の展示及びミニセミナーについても熱心にご見学頂きました。

セミナー終了後のアンケートにおいては「有益であった」、「有効であった」とのご回答を多数いただき、改めて経営者の皆様の情報セキュリティに対する意識の高さを感じることができました。
記:情報セキュリティ担当

本記事に関してお問合せ等ございましたら、弊社担当にお声掛けください。

？ オートフィルをもっと簡単に行うには？

オートフィルはセルのフィルハンドルをドラッグすることによって、セルの内容のコピーや、連続データの入力ができる便利な機能ですが、行数が多い場合はドラッグするのに苦労することもあります。



そんな時はドラッグではなく、ダブルクリックでオートフィルを行なってみましょう。一瞬で実行することができます。

Operation

1. オートフィルを行ないたいセルのフィルハンドル(図-1ではC2セルの右下)をダブルクリックします。
2. 下方方向へデータが連続入力されます。(図-2)

図-1

	A	B	C	D
1				
2			木	
3		11月1日		
4		11月2日		
5		11月3日		
6		11月4日		
7		11月5日		
8		11月6日		

ダブルクリック!!

図-2

	A	B	C	D
1				
2			木	
3		11月1日	金	
4		11月2日	土	
5		11月3日	日	
6		11月4日	月	
7		11月5日	火	
8		11月6日	水	



ポインタの形が「+」の状態ダブルクリックしてね。ダブルクリックのオートフィルは縦方向にだけ使えるよ。また隣の列にデータが入力されている必要があるよ。