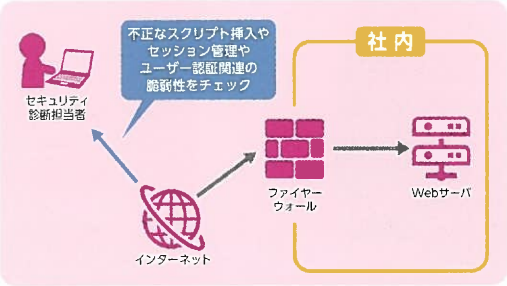
情報セキュリティコンサル診断メニュー
～①ホームページ診断編～

HRI 株式会社百五総合研究所

ホームページ診断とは



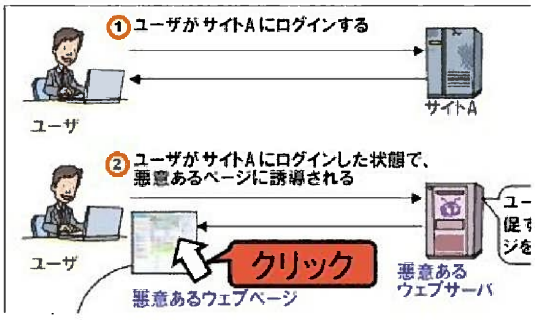
現在、ホームページは企業の情報発信の場として定着しています。企業の顔と言っても過言ではありません。そのＷｅｂサイトが改ざんされると、好意を持って訪問した方が意図しないページに誘導されてしまい、そこで個人情報を抜き取られる等の被害が発生します。
改ざんされ易い作りか否かを専門家が診断します。
（下図は、報告書から一部転記しました）

No.	脆弱性区分	脆弱性名	危
1	クリックジャキング攻撃	X-Frame-Options ヘッダーの欠如	M
2	サイバー攻撃	Cookie set without HttpOnly flag	M
3	クロスサイトスク	WebBrowserXSS Protection Not	

1.1. クリックジャッキング攻撃の例

クリックジャッキング攻撃では、例えば次のような流れで攻撃が行
リックジャッキング攻撃への対策をしていないサイト、悪意あるウェ
ウェブページを送信するサーバとする。

① ユーザがサイトＡにログインする
② ユーザがサイトＡにログインした状態で、悪意あるウェブペー
ユーザのブラウザ上には、ページ上の特定箇所のクリックを促
③ ユーザが悪意あるウェブページのコンテンツをクリックする（
ンツをクリックしている）
④ その結果、意図せずサイトＡの設定を変更してしまう。



Webアプリケーションを対象に診断を行い、報告書において脆弱性区分、脆弱性名、危険度、起こりうる事件、対応方法等をご報告します。
一部専門性が高くなりますので、詳細につきましては下記担当までお問合せください。

- SQLインジェクション
- クロスサイトスクリプティング（XSS）
- クロスサイトリクエストフォージェリ（CSRF）
- 意図しないリダイレクト　等の攻撃から守るための設定となります。

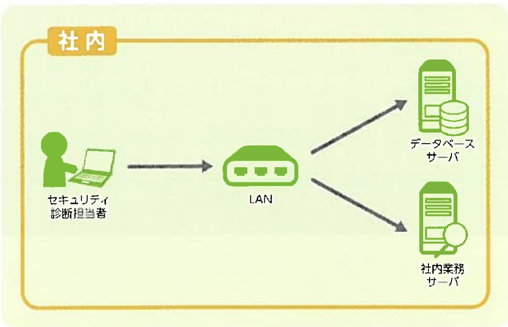
診断メニュー　1項目：16.5万円（診断15万円+税10%）

HRI 株式会社 百五総合研究所　　お問合せ　経営コンサルティンググループ
《TEL》059(228)9105 《FAX》059(228)9380　担当　古市、梅川

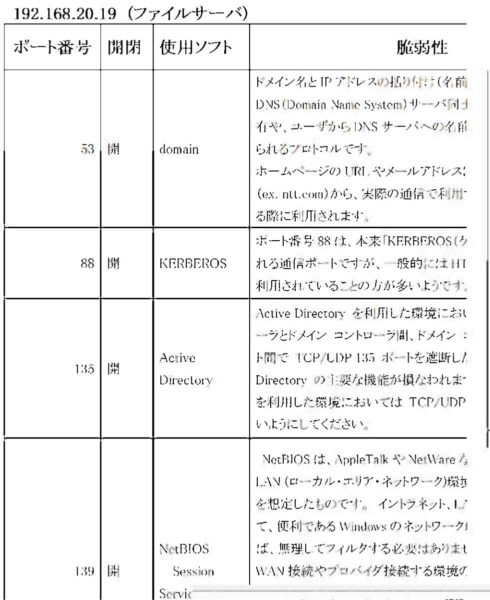
情報セキュリティコンサル診断メニュー
～②社内ネットワーク診断編～

HRI 株式会社百五総合研究所

社内ネットワーク診断とは

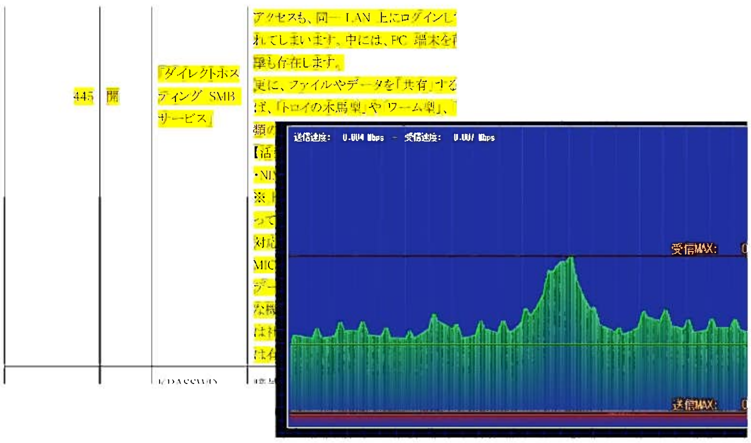


メールに添付されたファイル開封からランサムウェア（身代金要求のマルウェア）が社内LANに侵入するとデータファイルが暗号化されてしまい業務に多大な支障を来します。
設置されているファイルサーバの不要なポートを事前に閉じておくことで感染を防げる場合があります。また、無線AP（Wi-Fi機器）が乗っ取られると敷地外からでも社内LANにアクセスがされてしまいます。現状を診断します。
（下図は、報告書から一部転記しました）



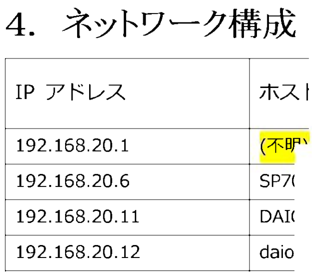
192.168.20.19（ファイルサーバ）

ポート番号	開閉	使用ソフト	脆弱性
53	開	domain	ドメイン名とIPアドレスの括り付け(名前 DNS(Domain Name System)サーバ同士 有や、ユーザからDNSサーバへの名前 られるプロトコルです。 ホームページのURLやメールアドレス (ex. ntt.com)から、実際の通信で利用 る際に利用されます。
88	開	KERBEROS	ポート番号88は、本来「KERBEROS(れる通信ポートですが、一般的にはHT 利用されていることの方が多いようです。
135	開	Active Directory	Active Directory を利用した環境におい ーラとドメイン コントローラ間、ドメイン ト間で TCP/UDP 135 ポートを遮断した Directory の主要な機能が損なわれま を利用した環境においては TCP/UDP いようにしてください。
139	開	NetBIOS Session Servic	NetBIOSは、AppleTalkやNetWare LAN(ローカル・エリア・ネットワーク)環 を想定したものです。イントラネット、L て、便利であるWindowsのネットワーク ば、無理してフィルタする必要はありま WAN接続やプロバイダ接続する環境の



445	開	「ダイレクトホスティング SMBサービス」	アクセスも、同一LAN上にログインし れてしまいます。中には、PC端末を 撃も存在します。 更に、ファイルやデータを「共有」する ば、「トロイの木馬型」や「ワーム型」、

SSID	Channel	Signal	認証	MACアドレス	ベンダー	暗号
	2	46%	オープン	88:57:ee:f4:3a:b9		WEP
	2	46%	WPA2-パーソナル	88:57:ee:f4:3a:b8		CCMP
	3	58%	オープン	00:16:01:04:e1:30	Buffalo Inc.	WEP
	8	72%	オープン	00:1d:73:88:9d:e6	Buffalo Inc.	WEP



4. ネットワーク構成

IP アドレス	ホスト
192.168.20.1	(不明
192.168.20.6	SP7
192.168.20.11	DAI
192.168.20.12	daio

オンプレミス(自社設置)のファイルサーバー等のポートの空き状態を調査、空いている場合に起こり得る障害・事象を調査報告します。LAN上のパケット調査を行い異常パケットの存在有無の調査。調査時点で接続可能な無線AP（SSID）一覧から不明なAPが運用されていないか、暗号化レベルの分析から脆弱性報告。同一セグメントでIPアドレスを持つ機器を調査しネットワーク構成一覧表の作成を行いご報告します。

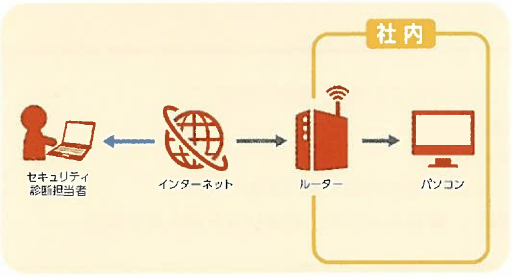
診断メニュー　1項目：16.5万円(診断15万円+税10%)

HRI 株式会社 百五総合研究所
《TEL》059(228)9105 《FAX》059(228)9380
お問合せ　経営コンサルティンググループ
担当　古市、梅川

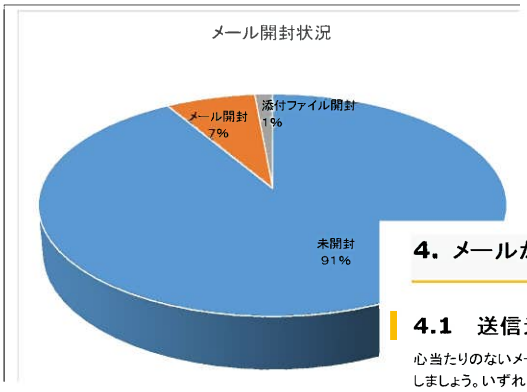
情報セキュリティコンサル診断メニュー
～③メール攻撃への脆弱性診断編～

HRI 株式会社百五総合研究所

メール攻撃への脆弱性診断とは

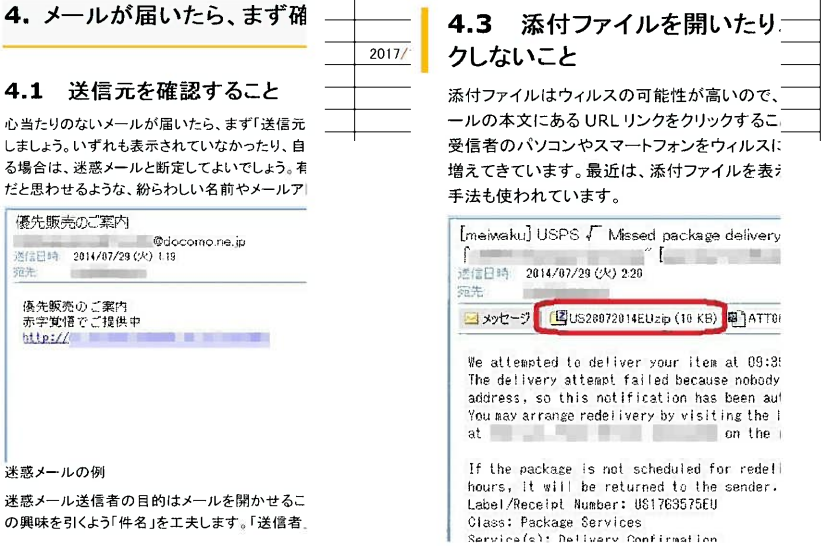


過去取引した企業担当者から突然メールを受信。メールを開封、添付のWordファイルを開封し、マクロを実行！その瞬間にマルウェアに感染しています。 感染すると社内に蔓延、また同様に取引先へ貴方が迷惑メールをばら撒いてしまい、企業として信用がガタ落ちします。
職員宛に疑似メールを送信し、対応状況を診断します。（対象アドレス数：80件以下）
（下図は、報告書から一部転記しました）



■結果一覧

	名前	1回目	添付ファイル開封	2回目	添付ファイル開封
1		2017/12/4 6:24			
2		2017/12/4 8:38			
3					
4					
5				2017/12/11 7:37	


4. メールが届いたら、まず確
4.1 送信元を確認すること
心当たりのないメールが届いたら、まず「送信元
しましょう。いずれも表示されていなかったり、自
る場合は、迷惑メールと断定してよいでしょう。有
だと思わせるような、紛らわしい名前やメールア
優先販売のご案内
@docomo.ne.jp
送信日時 2014/07/29 (火) 1:19
宛先
優先販売のご案内
赤字覚悟でご提供中
http://
迷惑メールの例
迷惑メール送信者の目的はメールを開かせるこ
の興味を引くよう「件名」を工夫します。「送信者
4.3 添付ファイルを開いたり
クしないこと
添付ファイルはウィルスの可能性が高いので、
ールの本文にある URL リンクをクリックするこ
受信者のパソコンやスマートフォンをウィルスに
増えてきています。最近は、添付ファイルを表
手法も使われています。
[meiwaku] USPS √ Missed package delivery
送信日時 2014/07/29 (火) 2:20
宛先
メッセージ
US28072014EUzip (10 KB)
ATT0
We attempted to deliver your item at 09:3
The delivery attempt failed because nobody
address, so this notification has been au
You may arrange redelivery by visiting the
at on the
If the package is not scheduled for redel
hours, it will be returned to the sender.
Label/Receipt Number: US1763575EU
Class: Package Services
Service(s): Delivery Confirmation

犯罪者は、次々と新しい手法で攻撃を仕掛けてきます。
最新の手法を研究し、職員の対応状況を調査し、対応結果をご報告します。
職員の意識レベルの診断と併せて更なる意識向上をご支援します。
全社レベルでの対応訓練（BCP訓練）とお考え下さい。
対象アドレス数上限を超える診断を希望される場合、下記担当までご相談ください。

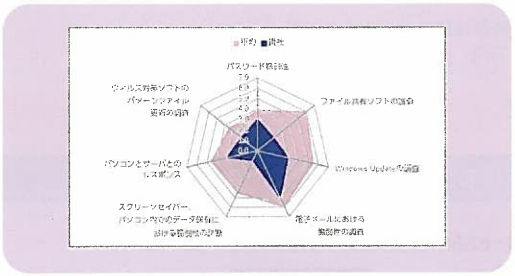
診断メニュー　1項目：16.5万円（診断15万円+税10%）

HRI 株式会社 百五総合研究所
《TEL》059(228)9105 《FAX》059(228)9380
お問合せ　経営コンサルティンググループ
担当　古市、梅川

情報セキュリティコンサル診断メニュー
～④重要情報を取り扱うPCの脆弱性診断編～

HRI 株式会社百五総合研究所

重要情報を取り扱うパソコンの脆弱性診断とは



マイクロソフトは、最新OSのWin10であってもサポート終了を発表していることをご存じでしょうか？年に２回機能アップデートを実施しており、３世代以上古いバージョンには修正プログラムが提供されなくなります。最新バージョンで運用できているか、意図しないプログラムが稼働していないか等診断します。（下図は、報告書から一部転記しました）

主な診断項目を以下に列挙します。

	診断項目	内容
1	使用しているOS	OSのバー
2	パスワード脆弱性	パスワード
3	ファイル共有ソフトの調査	ファイル共確認
4	Windows Update の調査	Windows U
5	PCにインストールされているソフトウェア製品が最新のバージョンであるかを確認する	脆弱性対策
6	ウィルス対策ソフトのパターンファイル更新の調査	ウィルス対新の確認
7	当社作成のウイルスがチェックされるかの確認	ウィルス対
8	スクリーンセイバー、パソコン内でのデータ保有における脆弱性の調査	スクリーンセタ保有にお

チェック対象 SW製品名	チェ (IPA が重
Adobe Flash Player	バージョン 10.x 以降 ※ブラウザ(Internet E: まれている Adobe Flash
Adobe Reader	バージョン 8.x、9.x、 Reader DC
Google Chrome	バージョン 11.x、12.x
JRE (Java 実行環境)	バージョン 1.5.x(5.x)、 1.8.x(8.x)、9.x
Lhaplus	バージョン 1.5.x 以降

バージョン	サポート終了日	必要な対応
バージョン 1803 以前	既に終了	20H2 への更新が必須
バージョン 1809	2020 年 11 月 10 日に終了	20H2 への更新が必須
バージョン 1903	2020 年 12 月 8 日に終了	20H2 への更新が必須
バージョン 1909	2021 年 5 月 11 日に終了	継続使用可能
バージョン 2004（20H1）	2021 年 12 月 14 日に終了	継続使用可能

最新のWindows 10である「October 2020 Update」（以下20H2と表記）は、2020年10月13日（現地時間。日本時間は翌14日の午前3時）に配布が開始された。

6. 当社作成のウィ

当社が作成したウィルス

問題ありませんでした。

番号	IP アドレス	ID
1	192.168.11.58	t-
2	192.168.11.117	k-

システムベンダーにすべて委ねて安心していたらアップデートを止めてありサポートが切れていた。このような事態を招く前に、PC個々のOSご利用バージョン、脆弱性を有するソフトウエアのバージョン、アンチウイルスソフトが模擬ウイルスを捕獲するか、不明なアプリケーションが稼働していないか等の定期健診をお奨めします。
重要情報を取り扱うPC数台を選定いただき、Windows OSのアップデート状況の確認や、疑似ウイルスへのアンチウイルス検知状況などを診断し結果をご報告します。

診断メニュー　1項目：16.5万円（診断15万円+税10%）

HRI 株式会社 百五総合研究所　　お問合せ　経営コンサルティンググループ
《TEL》059(228)9105 《FAX》059(228)9380　担当　古市、梅川