



# 年末年始の 情報セキュリティ対策

株式会社Doctor Web Pacific



© Doctor Web,  
2023

[www.drweb.com](http://www.drweb.com)

# 今回のテーマ

年末年始の休業明けは、ランサムウェア被害に関する多くのお問い合わせが弊社に寄せられています。

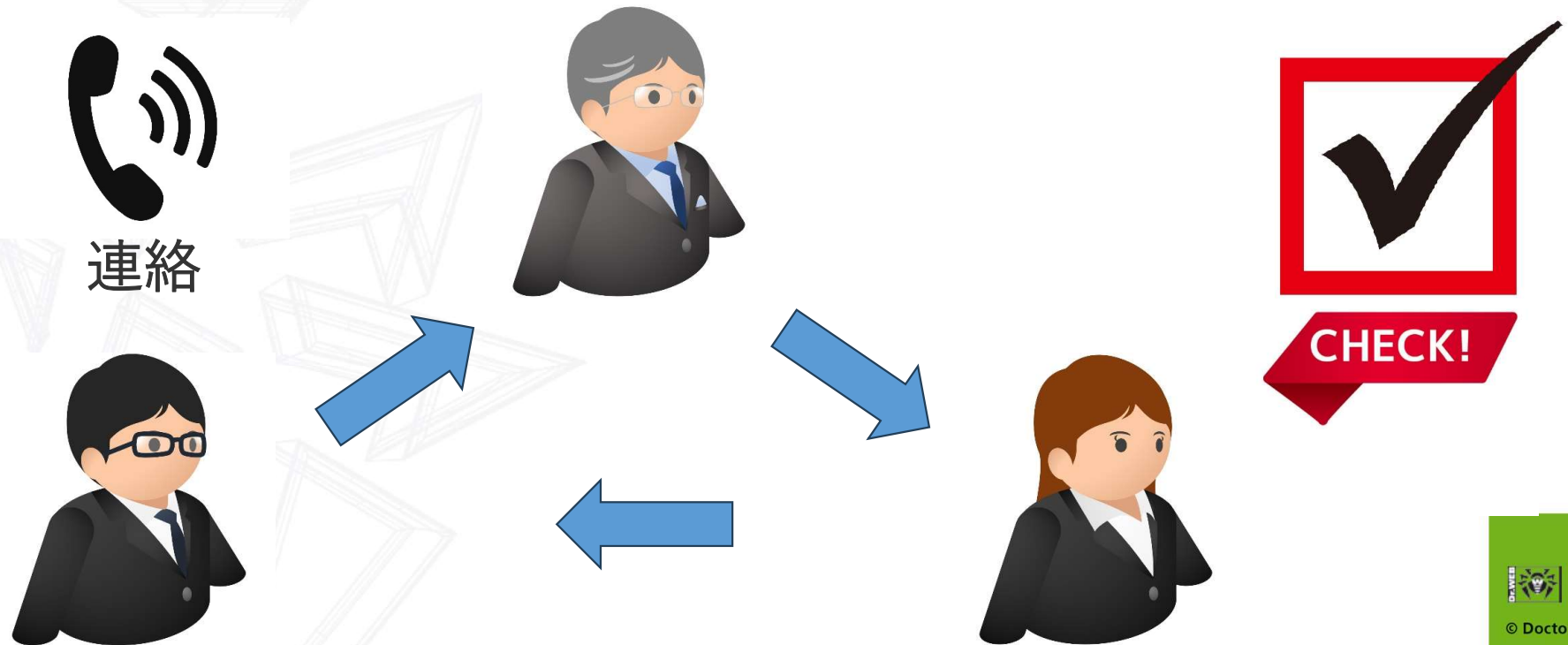
- 企業・組織の対策 管理者編
- 企業・組織の対策 利用者編



# 企業・組織の対策

## 管理者編

## 1. 緊急連絡体制の確認



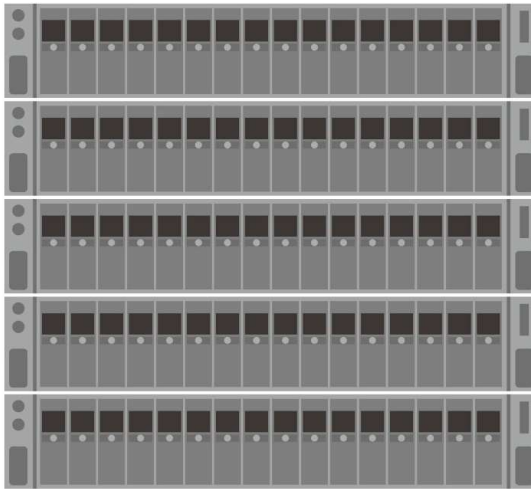
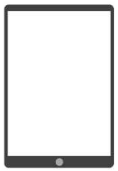
不測の事態が発生した場合に備えて、委託先企業を含めた緊急連絡体制や対応手順等が明確になっているか確認してください。

## 2. 社内ネットワークへの機器接続ルールの確認と遵守



メンテナンス作業などで社内ネットワークに接続する場合は、  
聞き接続ルールを事前に準備・確認し、遵守してください。

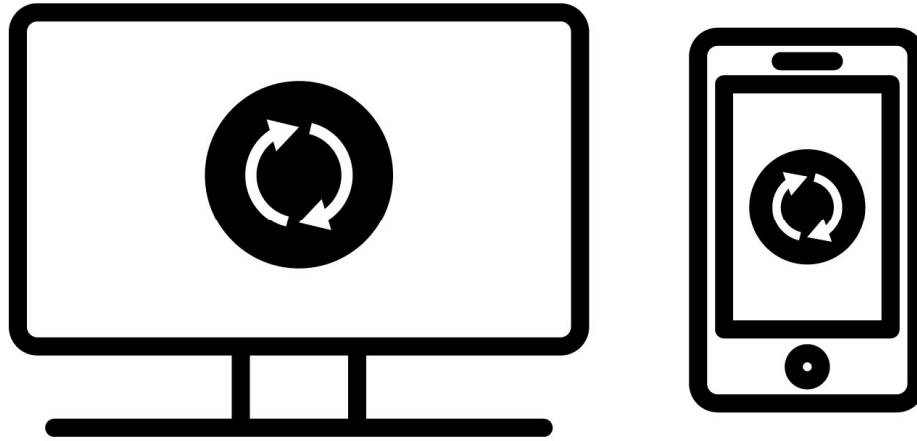
### 3. 使用しない機器の電源OFF



年末年始の休業中に使用しない機器は全て電源をOFFにしてください。

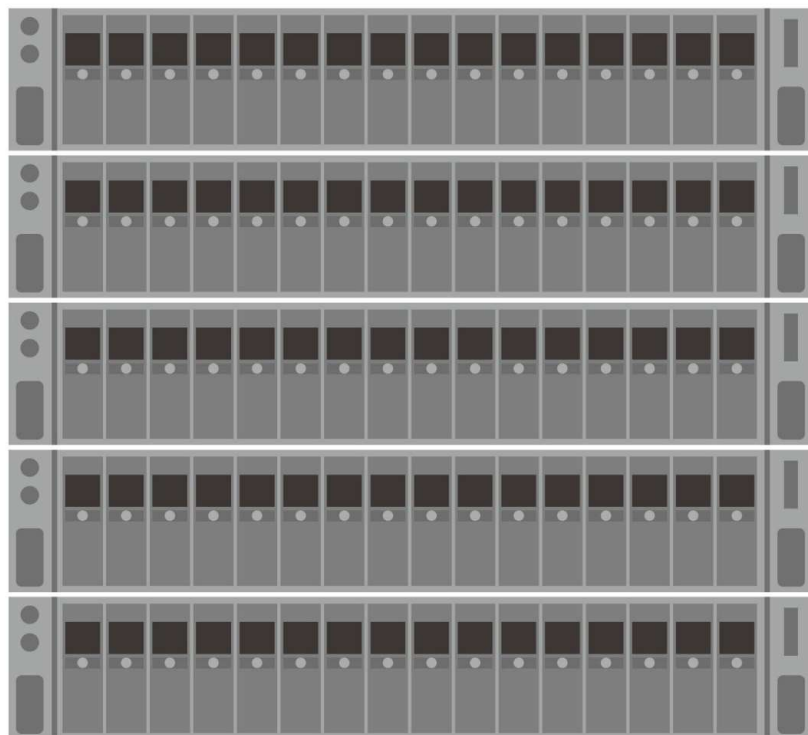


## 1. 修正プログラムの適用 定義ファイルの更新



OSや各種ソフトウェアの修正プログラムが公開されている場合は適用してください。  
セキュリティソフトの定義ファイルを最新に更新してください。

## 2. サーバ等における各種ログの確認



```
Thu Oct 22 18:47:28 2015 [notice] Digest: generating secret for digest authentication ...
Thu Oct 22 18:49:28 2015 [notice] Digest: done
Thu Oct 22 18:49:28 2015 [notice] FastCGI: process manager initialized (pid 1113)
Thu Oct 22 18:49:28 2015 [notice] Apache/2.2.34 (Ubuntu) Mod_SSI/2.0.6 Python/2.7.13 PHP/7.3.8 mod_ssl/2.2.34 OpenSSL/1.0.2o DAV/2 mod_fastcgi/mod_fastcgi-SNAP-091802141 mod_perl/
2.0.18 Perl/5.24.0 configured -- resuming normal operations
Thu Oct 22 18:51:18 2015 [notice] Successful restart requested, doing restart
Thu Oct 22 18:51:28 2015 [error] [22]Invalid argument: FastCGI: read() from pipe failed (0)
Thu Oct 22 18:51:29 2015 [alert] [22]Invalid argument: FastCGI: the pm is shutting down, Apache seems to have disappeared - bye
Thu Oct 22 18:51:29 2015 [notice] Digest: generating secret for digest authentication ...
Thu Oct 22 18:51:29 2015 [notice] Apache/2.2.34 (Ubuntu) Mod_SSI/2.0.6 Python/2.7.13 PHP/7.3.8 mod_ssl/2.2.34 OpenSSL/1.0.2o DAV/2 mod_fastcgi/mod_fastcgi-SNAP-091802141 mod_perl/
2.0.18 Perl/5.24.0 configured -- resuming normal operations
Thu Oct 22 11:04:09 2015 [notice] FastCGI: process manager initialized (pid 1190)
Thu Oct 22 11:04:09 2015 [notice] Successful restart requested, doing restart
Thu Oct 22 11:04:09 2015 [notice] Digest: generating secret for digest authentication ...
Thu Oct 22 11:04:09 2015 [notice] Apache/2.2.34 (Ubuntu) Mod_SSI/2.0.6 Python/2.7.13 PHP/7.3.8 mod_ssl/2.2.34 OpenSSL/1.0.2o DAV/2 mod_fastcgi/mod_fastcgi-SNAP-091802141 mod_perl/
2.0.18 Perl/5.24.0 configured -- resuming normal operations
Thu Oct 22 11:04:09 2015 [notice] FastCGI: process manager initialized (pid 1903)
Thu Oct 22 14:11:36 2015 [notice] caught SIGTERM, shutting down
Thu Oct 22 18:47:07 2015 [notice] Digest: generating secret for digest authentication ...
Thu Oct 22 18:47:07 2015 [notice] FastCGI: process manager initialized (pid 2363)
Thu Oct 22 18:47:07 2015 [notice] Apache/2.2.34 (Ubuntu) Mod_SSI/2.0.6 Python/2.7.13 PHP/7.3.8 mod_ssl/2.2.34 OpenSSL/1.0.2o DAV/2 mod_fastcgi/mod_fastcgi-SNAP-091802141 mod_perl/
2.0.18 Perl/5.24.0 configured -- resuming normal operations
Thu Oct 22 19:01:48 2015 [error] [client 113] File does not exist: /Applications/MAMP/htdocs/favicon.ico, referer: http://localhost:8888/
Thu Oct 22 19:06:07 2015 [notice] Digest: generating secret for digest authentication ...
Thu Oct 22 19:06:07 2015 [notice] FastCGI: process manager initialized (pid 2836)
Thu Oct 22 19:06:07 2015 [notice] Apache/2.2.34 (Ubuntu) Mod_SSI/2.0.6 Python/2.7.13 PHP/7.3.8 mod_ssl/2.2.34 OpenSSL/1.0.2o DAV/2 mod_fastcgi/mod_fastcgi-SNAP-091802141 mod_perl/
2.0.18 Perl/5.24.0 configured -- resuming normal operations
Thu Oct 22 19:06:07 2015 [notice] FastCGI: process manager initialized (pid 3363)
Thu Oct 22 19:06:07 2015 [notice] Successful restart requested, doing restart
Thu Oct 24 19:18:56 2015 [notice] Digest: generating secret for digest authentication ...
Thu Oct 24 19:18:56 2015 [notice] Apache/2.2.34 (Ubuntu) Mod_SSI/2.0.6 Python/2.7.13 PHP/7.3.8 mod_ssl/2.2.34 OpenSSL/1.0.2o DAV/2 mod_fastcgi/mod_fastcgi-SNAP-091802141 mod_perl/
2.0.18 Perl/5.24.0 configured -- resuming normal operations
Thu Oct 24 19:18:56 2015 [notice] FastCGI: process manager initialized (pid 5392)
Thu Oct 24 19:18:56 2015 [error] [client 113] File does not exist: /Users/masasori/Documents/htdocs/test/favicon.ico, referer: http://cafe-tokyo.com/8888/wp-admin/install.php
Thu Oct 24 19:13:59 2015 [notice] Successful restart requested, doing restart
Thu Oct 24 19:13:59 2015 [notice] Digest: generating secret for digest authentication ...
Thu Oct 24 19:13:59 2015 [notice] FastCGI: process manager initialized (pid 5443)
Thu Oct 24 19:13:59 2015 [notice] Apache/2.2.34 (Ubuntu) Mod_SSI/2.0.6 Python/2.7.13 PHP/7.3.8 mod_ssl/2.2.34 OpenSSL/1.0.2o DAV/2 mod_fastcgi/mod_fastcgi-SNAP-091802141 mod_perl/
2.0.18 Perl/5.24.0 configured -- resuming normal operations
Thu Oct 24 19:14:48 2015 [notice] Successful restart requested, doing restart
Thu Oct 24 19:14:48 2015 [error] [22]Invalid argument: FastCGI: read() from pipe failed (0)
Thu Oct 24 19:14:48 2015 [alert] [22]Invalid argument: FastCGI: the pm is shutting down, Apache seems to have disappeared - bye
Thu Oct 24 19:14:48 2015 [notice] Digest: generating secret for digest authentication ...
Thu Oct 24 19:14:48 2015 [notice] FastCGI: process manager initialized (pid 4064)
Thu Oct 24 19:14:48 2015 [notice] Apache/2.2.34 (Ubuntu) Mod_SSI/2.0.6 Python/2.7.13 PHP/7.3.8 mod_ssl/2.2.34 OpenSSL/1.0.2o DAV/2 mod_fastcgi/mod_fastcgi-SNAP-091802141 mod_perl/
2.0.18 Perl/5.24.0 configured -- resuming normal operations
Thu Oct 24 19:25:53 2015 [error] [client 113] File does not exist: /Users/masasori/Documents/htdocs/test
Thu Oct 24 19:18:28 2015 [notice] caught SIGTERM, shutting down
Thu Oct 29 17:18:28 2015 [notice] Digest: generating secret for digest authentication ...
Thu Oct 29 17:18:28 2015 [notice] FastCGI: process manager initialized (pid 1036)
Thu Oct 29 17:18:28 2015 [notice] Apache/2.2.34 (Ubuntu) Mod_SSI/2.0.6 Python/2.7.13 PHP/7.3.8 mod_ssl/2.2.34 OpenSSL/1.0.2o DAV/2 mod_fastcgi/mod_fastcgi-SNAP-091802141 mod_perl/
2.0.18 Perl/5.24.0 configured -- resuming normal operations
Thu Oct 31 11:22:26 2015 [notice] caught SIGTERM, shutting down
Thu Oct 31 11:22:26 2015 [notice] Digest: generating secret for digest authentication ...
```

不審なアクセスが発生していないか、各種ログを確認してください。

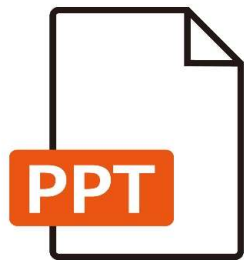




# 企業・組織の対策

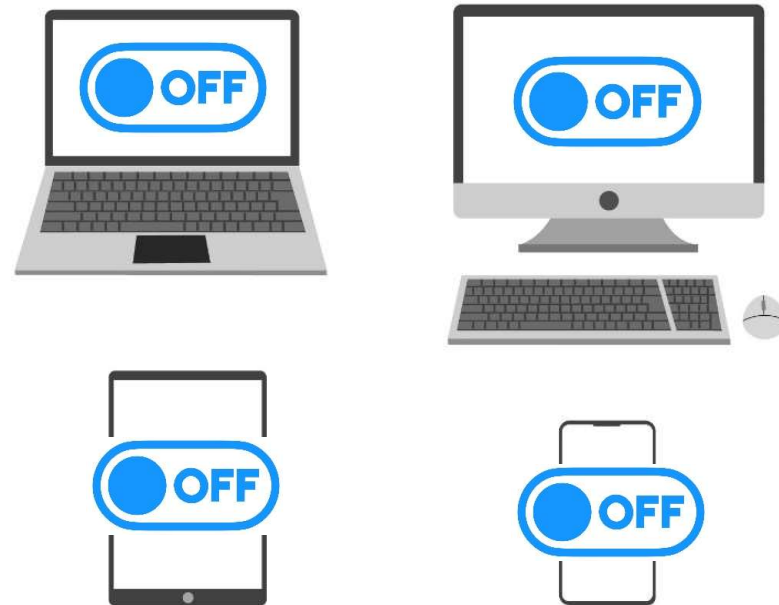
## 利用者編

## 1. 機器やデータの持ち出しルールの確認と遵守



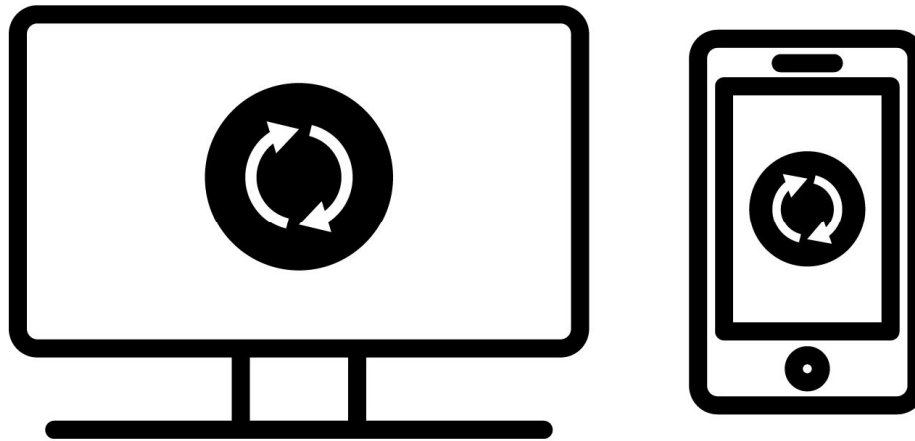
社外での対応が必要となるパソコン等の機器やデータ等の情報を持ち出す場合は、持ち出しルールを事前に確認し遵守してください。

## 2. 使用しない機器の電源OFF



使用しない機器は全て電源をOFFにしてください。

## 1. 修正プログラムの適用 定義ファイルの更新



OSや各種ソフトウェアの修正プログラムが公開されている場合は適用してください。  
セキュリティソフトの定義ファイルを最新に更新してください。

## 2. 持ち出した機器等のウイルスチェック



パソコンやUSBメモリなど外部記憶媒体もセキュリティソフトでウイルススキャンを行ってください。

### 3. 不審なメールに注意



年末年始休業中に届いているメールは非常に危険です。  
アップデート、定義ファイルの更新、ウイルススキャンが完了してから確認してください。





[www.drweb.com](http://www.drweb.com)  
[www.drweb.co.jp](http://www.drweb.co.jp)



© Doctor Web,  
2023

[www.drweb.com](http://www.drweb.com)