

# 盗難・紛失・不正アクセスから 企業秘密を守る 適切な管理とは

我社に必要な情報漏洩対策はどうすべきか？

## → 近年の状況



近年、特定秘密保護法や情報セキュリティ関連のニュースが紙面を賑わせています。

国家レベルで情報セキュリティについての意識が高まっていますが、脅威は数多く存在し、多岐にわたっています。



- 顧客情報・機密情報の持ち出し
- 研究データの国外流出事件
- パソコン遠隔操作事件
- 重要な内部資料流出事件



コピーして  
持ち出し



紛失・漏洩のリスク



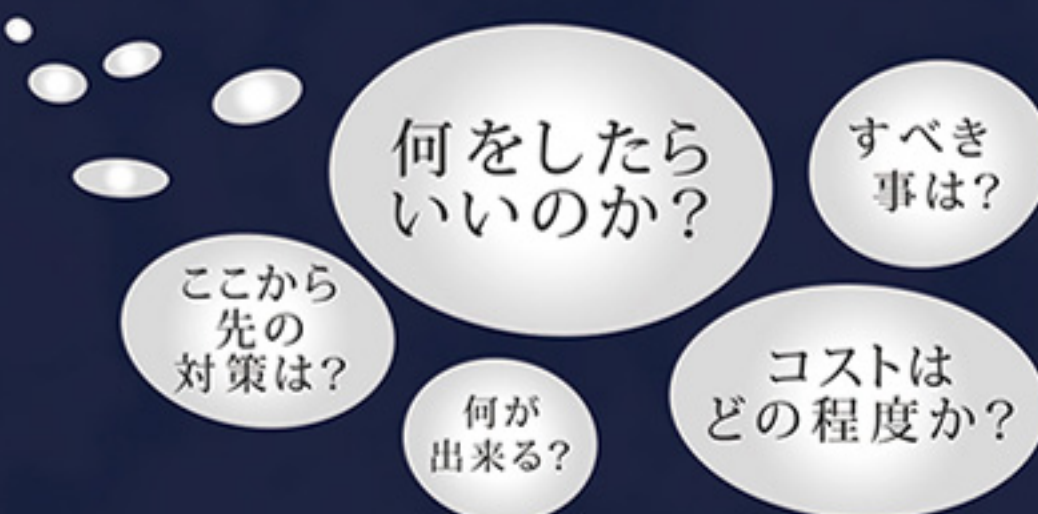
## → 我社の現状は？

我社の対策を確認すると、  
ウイルスソフトのみだった。



ウイルス  
対策  
ソフト

これから  
どうすべきか…。



情報(顧客情報、特許情報、技術情報、プロジェクト情報、研究データ)を守るために、どのような対策が必要になるのか。

管理はどのように行うのが良いか。

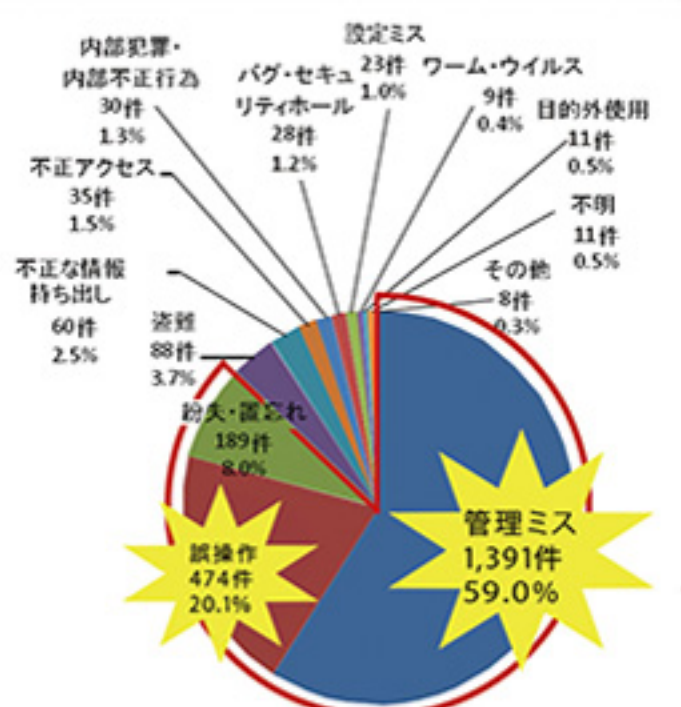
外部からのサイバー攻撃、内部からの情報流出に対して、それぞれどのように防ぐのか…。



# 情報漏洩を防ぐには、企業内

情報漏洩原因の大部分は、管理ミスや誤操作、紛失や置忘れ等、企業内に原因がある。  
(スマートフォン)、電子メール、インターネット、パソコン本体等。内部からの情報

## → 情報漏洩は内部から



原因別の漏洩件数

JNSA2012年情報セキュリティインシデントに関する調査

## 企業内のセキュリティ対策が不可欠!!

情報漏洩を防ぐには、内部セキュリティの強化が必要!

内部からの漏洩が

約8割

情報漏洩は、  
管理ミスや誤操作等  
約8割内部に原因がある!!



【様々な漏洩原因】

管理ミス/誤操作/紛失・置忘れ/盗難/不正な情報持ち出し/不正アクセス/内部犯罪・内部不正行為/バグ・セキュリティホール/設定ミス/ワーム・ウイルス/目的外使用

## → 情報セキュリティポリシーの策定

## 情報を持ち出させない。漏洩させない。

CD・DVD、SDカード、携帯電話、スマートフォン、書類(紙媒体)等の業務に必要な媒体の取り扱い方法や管理方法を策定する。

### 情報セキュリティポリシー

ソフトによる管理

1. CD・DVDの使用禁止
2. メモリカード(SD、メモリースティック)の使用禁止
3. 携帯電話、スマートフォンの持込禁止
4. 個人所有USBメモリの使用禁止
5. ファイルをメールで送信する際は暗号化を施す
6. プリンタはネットワークプリンタのみ(ローカルは禁止)
7. Webの閲覧制限
8. パソコンの操作ログ取得
9. ウイルス対策

人による管理

10. 書類の持ち出し禁止
11. 書類破棄時はシュレッダー裁断(破砕)を義務化
12. 入退室管理
13. IDパスワード等、個人権限の貸借禁止



# のセキュリティ強化が不可欠

漏洩媒体は、紙媒体、USBストレージ(USBメモリースティック、外付けハードディスク、  
SSD)等。漏洩を防ぐには、情報の持ち出しが出来ない環境を目指す事が先決である。

## → 情報が持ち出せない環境にするために

### 要望 1

CD・DVDなどは  
使用出来ないようにしたい。



A

CD・DVDの使用を禁止するには、**デバイスの無効化機能**が必要。SDカードやメモリースティックも禁止出来る  
と更にセキュリティが高まります。

### 要望 2

個人所有のUSBメモリを使用  
した場合に起こりうるマルウェア  
等のウイルス感染を防ぎたい。



A

ウイルス対策ソフトの導入及びUSB挿入やCD・DVD  
装着時に自動実行される「オートラン」を無効化する  
**機能**が必要です。

### 要望 3

一般的なUSBメモリを、  
セキュリティUSBと同様に使用する事で  
コストパフォーマンスを向上させたい。



A

ファイル暗号化**機能**が必要。個人所有USBメモリの  
使用禁止や、使用する事が出来るUSBメモリを**セキュ  
アリスト登録機能**にて限定する機能が必要。

### 要望 4

SI企業で働くPC環境に詳しい  
社員でも不正持ち出しでき  
ない様にしたい。



A

管理画面やアンインストール時のパスワード設定やサービス  
停止時には自動的に、**サービスが再起動される機能**  
が必要。

### 要望 5

Wi-Fi、Bluetooth通信  
により接続された機器から  
の漏洩を防ぎたい。



A

Wi-Fi、Bluetooth機器が接続されても**通信を無効  
とする機能**が必要。

### 要望 6

不正な情報持ち出しが発覚した場合は、メール通報  
及び警告音、Windowsログ等で状況が把握出来る  
様にしたい。

A

不正な操作があった場合の通知を行う  
**不正検出時動作機能**と、**Windowsログ出力  
機能**が必要です。



### 要望 7

複数台数をネットワーク接続  
している為、管理を一括で  
行いたい。



A

操作ログや不正アラート情報を共有ファイルや  
NAS等へ**蓄積できる機能**が必要。

### 要望 8

個人で社内に持ち込んだCD・DVD  
等のブランクメディアへコピーされ  
た情報の漏洩を防ぎたい。



A

CD・DVDへ情報がコピー出来ない様、**内蔵型デバイス  
の無効化機能**が必要。

### 要望 9

個人や法人支給のスマートフォン  
やデジタルカメラ等へコピー  
された情報の漏洩を防ぎたい。



A

スマートフォンやデジタルカメラへ情報がコピー出来  
ない様、**スマートデバイス無効化機能**が必要。

### 要望 10

パソコン本体へ不正に接続されたUSB  
接続ローカル複合プリンタからSDカード  
等による情報漏洩を防ぎたい。



A

USB接続ローカル複合プリンタが不正に接続出来ない機能  
が必要。また、接続された場合に警告音が鳴る等の不正  
検出時動作機能があると更にセキュリティが高まります。

## → 要望に応えられるソフト

情報漏洩対策ソフト

# 発見伝 Notice Business

不正検出時動作機能/自動起動(オートラン)を無効にする機能/USBストレージの書込不可とする機能/スマートデバイス制御機能/  
セキュアリスト登録機能/USBロック・解除機能/内蔵型デバイスの無効化機能/不正アンインストール防止機能/メール通報機能/  
ファイル暗号・復号化機能/操作ログ出力機能/操作ログ・不正アラートの集中管理/Wi-Fi、Bluetooth、LANなどの通信無効化/

32bit/64bit対応



オープン価格  
(1PC・1ライセンス/1年間)





## → 発見伝により情報持出を不可に出来るデバイス

| デバイス                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 内蔵型                                                                                                                                                                                        | 外付けUSBポート                                                                                                                                                                                                                                                                                             |
|  <p>CD・DVD<br/>FD<br/>(フロッピーディスク)<br/>SDカード</p> <p>内蔵型デバイスが無効化される<br/>※管理画面で設定</p> <p>インストール直後に無効化される</p> |  <p>USBスティック<br/>USBハードディスク</p> <p>インストール直後に無効化される</p> <p>管理画面にて登録し有効とする。<br/>暗号化</p> <p>USB接続型FD・MO・CD・DVD<br/>USB接続型マルチカードリーダー<br/>スマートフォン<br/>デジタルカメラ</p> <p>内蔵型デバイスの無効化<br/>※管理画面で設定</p> <p>インストール直後に無効化される</p> |

## 不正な情報持ち出しをシャットアウト！

管理者による、操作ログ・不正アラートの一括管理を実現。

USBメモリ、スマートフォンなどのリムーバブルドライブやWi-Fi、Bluetooth、LANなどのネットワークを常時監視し、外部への情報持ち出しを禁止。



## ファイル暗号化！

USBストレージの盗難や紛失時も安心！

USBストレージに、暗号化されたファイルを保存する事が出来るので盗難や紛失時も安心。  
(AES暗号128bit+独自暗号化方式)



USBストレージからファイルを取り込んだパソコンにて復号化し保存する事ができます。(USBストレージから暗号化されたファイルを取り込むパソコンには、「発見伝 Notice Business」がインストールされてなければ復号化できません)

## CD・DVDやリムーバブルドライブの自動起動(オートラン)を無効にする機能

データのやりとりで便利なUSBストレージも、複数のPCで共用しているとウイルス感染が心配です。



「発見伝」では、USBストレージ(CD・DVDを含む)接続時の自動起動(オートラン)を無効化し「マルウェア」からの感染を防ぎます。

※マルウェアなどの感染防止を保障するものではありません。

## 不正アンインストール防止機能

「発見伝」がアンインストールされることはありませんか？



セキュリティソフトが簡単にアンインストール出来てしまうと、元も子もありません。「発見伝」なら、不正アンインストール防止機能があるので大丈夫。パスワード入力が必要(インストール時に設定)なので、悪意のある第三者にてアンインストールされる心配もありません。

## 内蔵型デバイスをすべて無効とする機能

情報の持出手段をシャットアウトして情報漏洩を防ぐ！



フロッピーディスク、SDカード、メモリーカード、CD・DVD等の内蔵型のデバイスをすべて無効に出来ますので、情報の持ち出しを防げます。

## セキュアな管理画面

パスワード入力で管理者以外のセキュアリスト(ホワイトリスト)への登録を禁止！



利用可能なUSBストレージを登録する画面(セキュアリスト画面)は、パスワード入力を要求し管理者以外の登録を禁止する事ができます。



管理画面で登録されたUSBは、安全に使用することができます。USBにより持ち出されたファイル情報が操作ログへ出力されます。

販売元

開発元 株式会社C&Cアソシエイツ

〒900-0021 沖縄県那覇市泉崎2-2-7 ストックハイツ2F  
TEL 098-979-9712 FAX 098-979-9713  
<https://www.cca-co.jp>