

デジタル化支援で気を付けたい 情報セキュリティ

2025年1月28日

ひょうごデジタル経営研究会 例会

西川 和予

本日の流れ

1. 自己紹介
2. 情報セキュリティの基礎
3. 中小企業における情報セキュリティ
4. 中小企業診断士としての関わり

情報セキュリティの基礎

情報セキュリティとは

- 情報にアクセスできる人の制限
- 情報の欠損の防止
- 情報が必要な時に問題なく使える状況

※ISO27002

コンピュータセキュリティ

コンピュータを破損や破壊、間違った操作、不正アクセスから守る

ネットワークセキュリティ

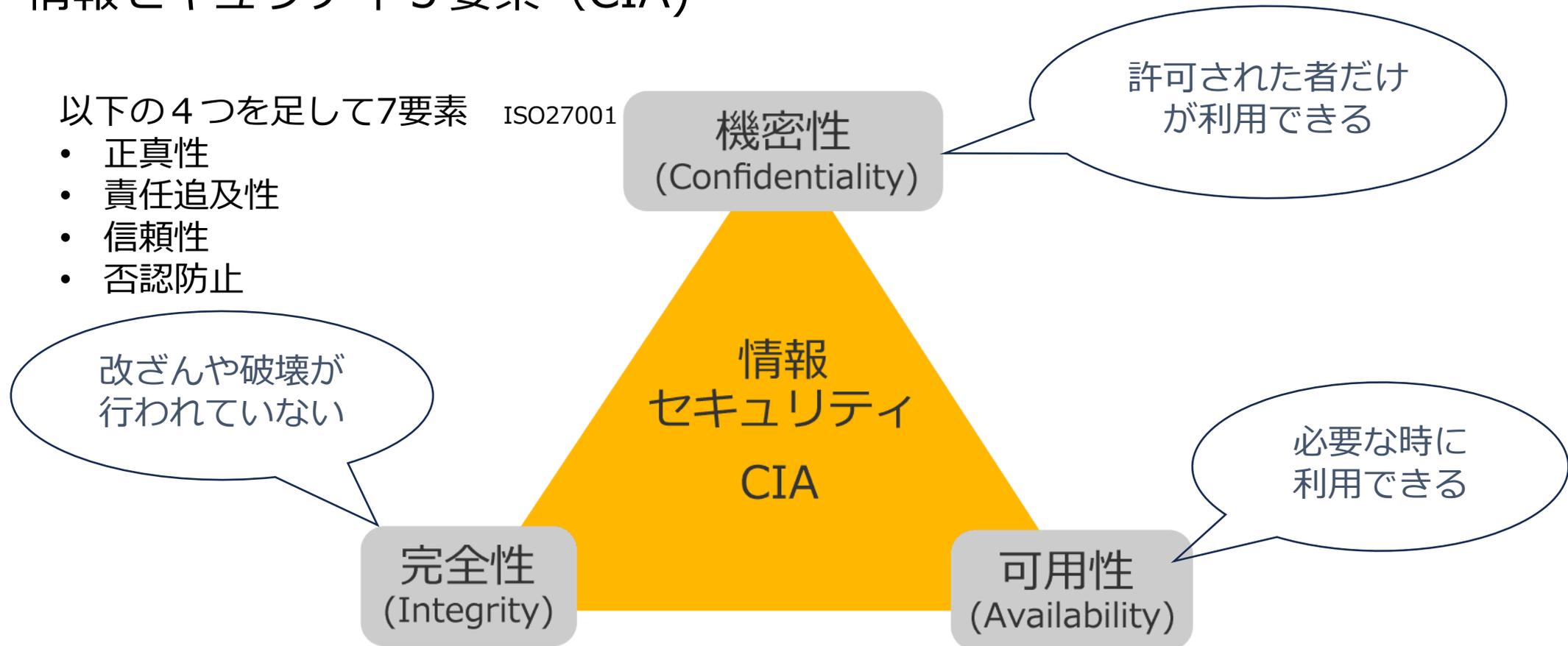
コンピュータや家庭内LAN、社内LANなどの内部ネットワークと、インターネットからアクセスできる外部との境界線を守る

情報セキュリティの基礎

情報セキュリティ 3要素 (CIA)

以下の4つを足して7要素 ISO27001

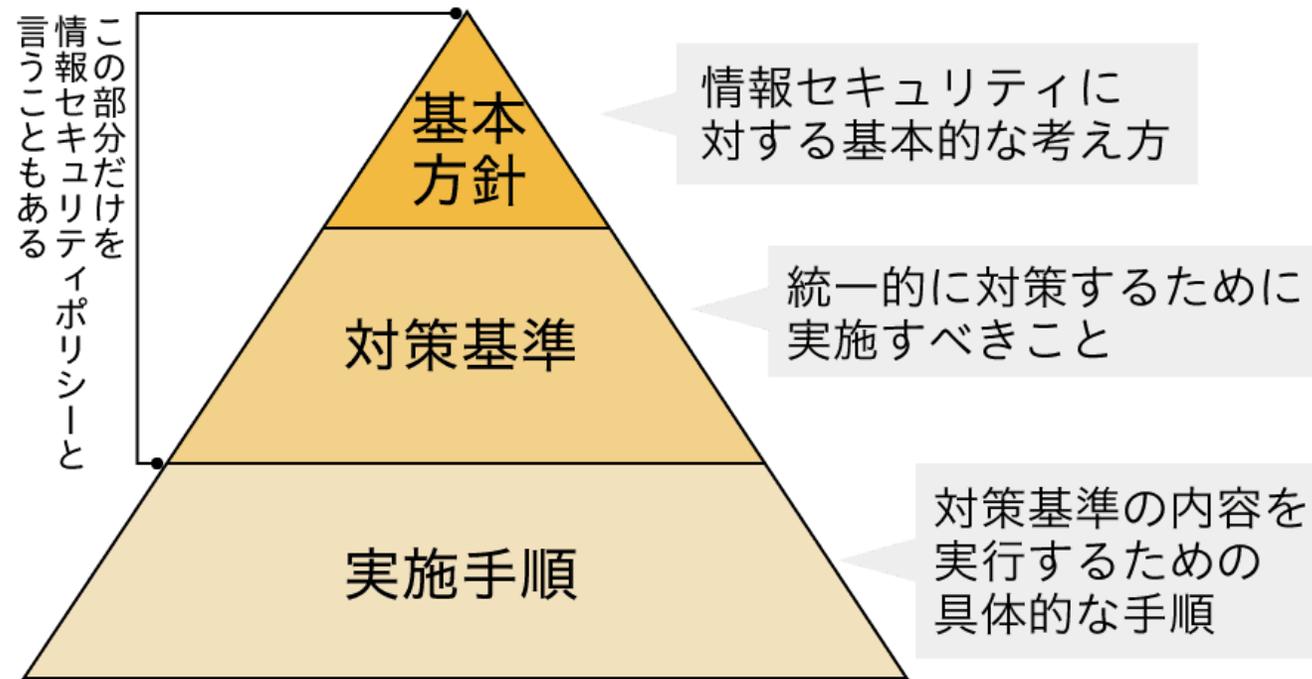
- 正真性
- 責任追及性
- 信頼性
- 否認防止



3つのバランスが崩れると企業経営に大きな影響を与える

情報セキュリティの基礎

情報セキュリティ対策基準



情報セキュリティの脅威

- ① 人的脅威 不正、誤り、意識の低さ
- ② 技術的脅威 コンピュータウイルス、マルウェア感染
- ③ 物理的脅威 災害等によるシステム停止（完全性、可用性）

リスク対策

リスク対策にはいくつかの段階があります

- ① 弱点をなくす ➡ セキュリティパッチを適用する、システムをアップデートする
- ② 弱点を攻められないように守る ➡ ファイアウォールなどを導入する
- ③ 攻められたらすぐに見つけて抑える ➡ ウイルスチェックを行う
- ④ やられたらすぐに元に戻す ➡ バックアップを作る

対策方法には3つの種類があります

物理的対策

不法侵入や破壊、紛失、盗難などに対応
例) 監視カメラ

技術的対策

システムやデータ、ネットワークなどのリスクに対応
例) ウイルス対策

人的（組織的）対策

従業員のミスや不正など人によるリスクに対応
例) ルール、教育

残念ながら万能な対策はない！
アセスメントの結果や環境に合わせて対策を選ぶことが重要

リスク対策

4つの方法のいずれか又は複数を組み合わせてリスク対応を行う

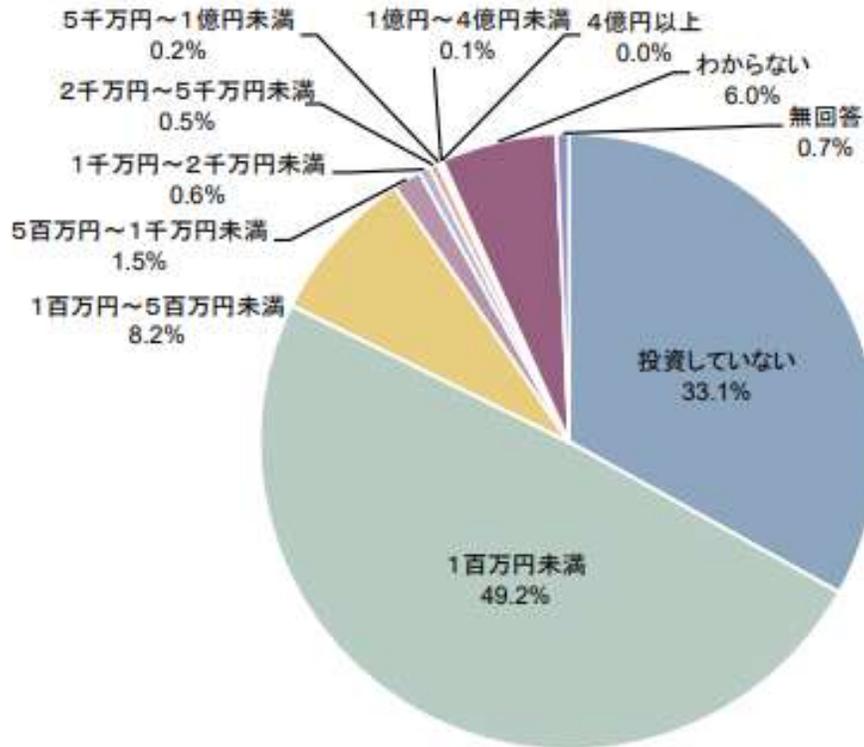


特定したリスクに対してどのような対応を取るかは、リスクの発生確率の高さと、発生した場合の影響度（事故の深刻さや企業の損失など）の高さをもとに決めるのが一般的

中小企業の実態

直近過去3期の情報セキュリティ対策投資額

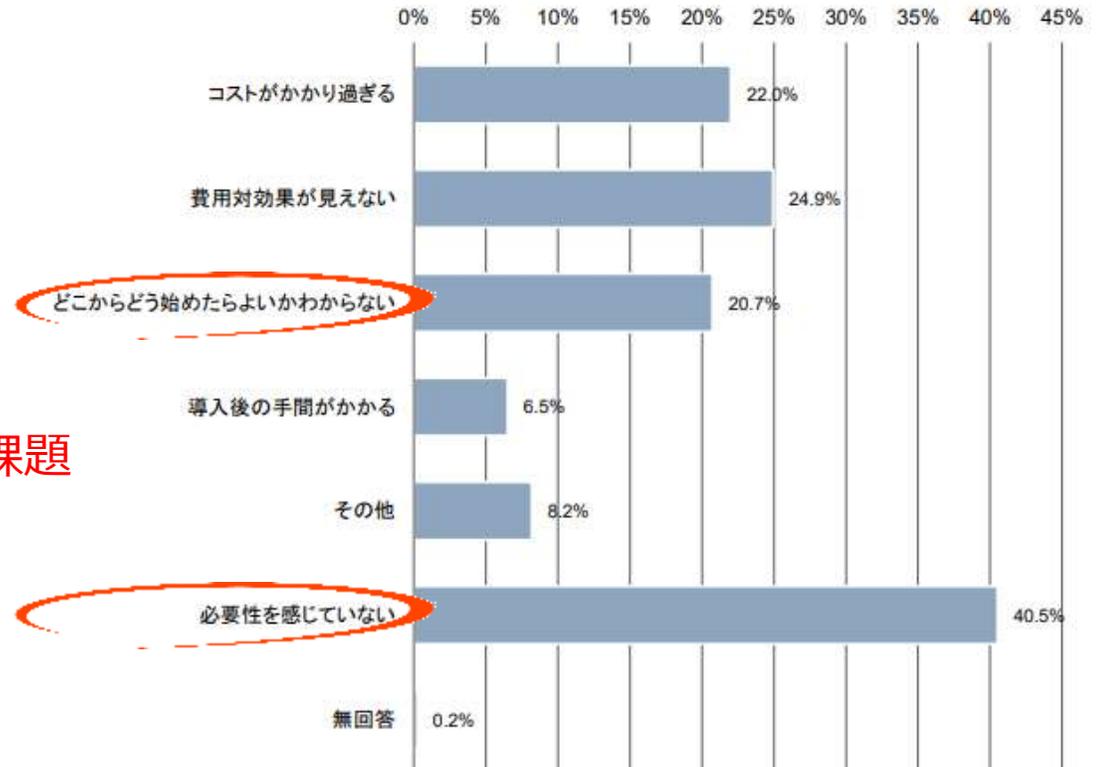
n=3,802



ここが課題

情報セキュリティ対策投資を行わなかった理由

n=1,259



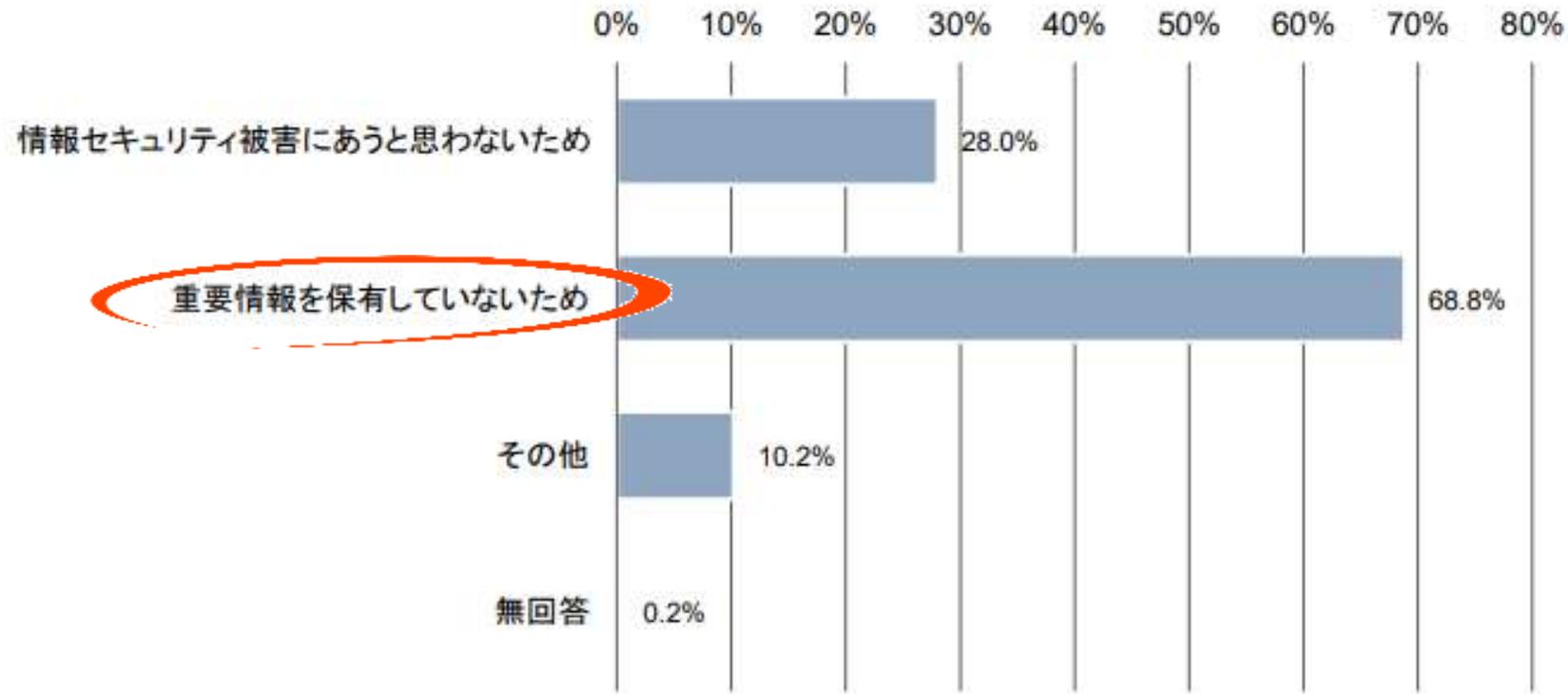
- ・製造現場にはセキュリティの専門家がいるわけではない
- ・迫っている脅威、リスクの大きさに気づいていない

IPA「2021年度中小企業における情報セキュリティ対策に関する実態調査」より抜粋
有効回答数4,074（製造業11.8%）

中小企業の実態

情報セキュリティ対策の必要性を感じない理由

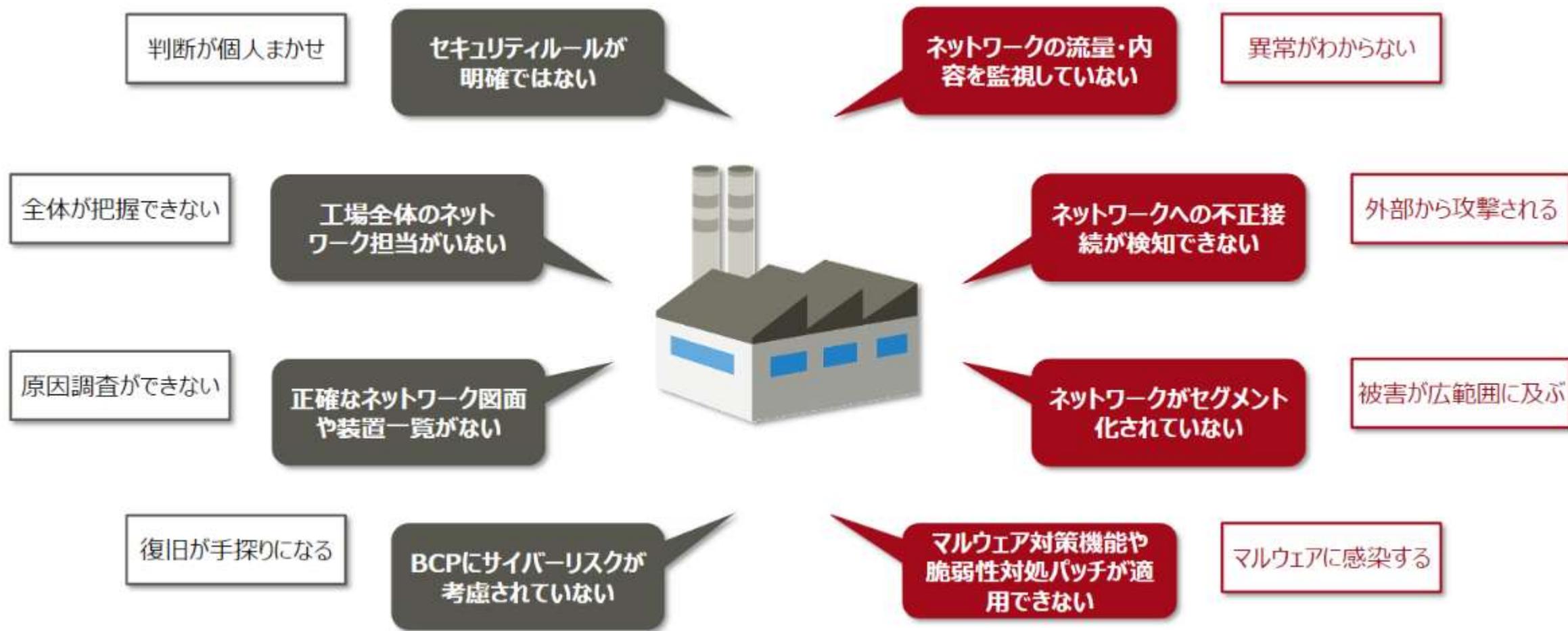
n=1,259



IPA「2021年度中小企業における
情報セキュリティ対策に関する実態調査」より抜粋
有効回答数4,074（製造業11.8%）

**情報セキュリティリスクは機密性（情報漏洩）だけではない
特に製造業は可用性（生産を止めない）が重要。止まっても大丈夫な工場はない！**

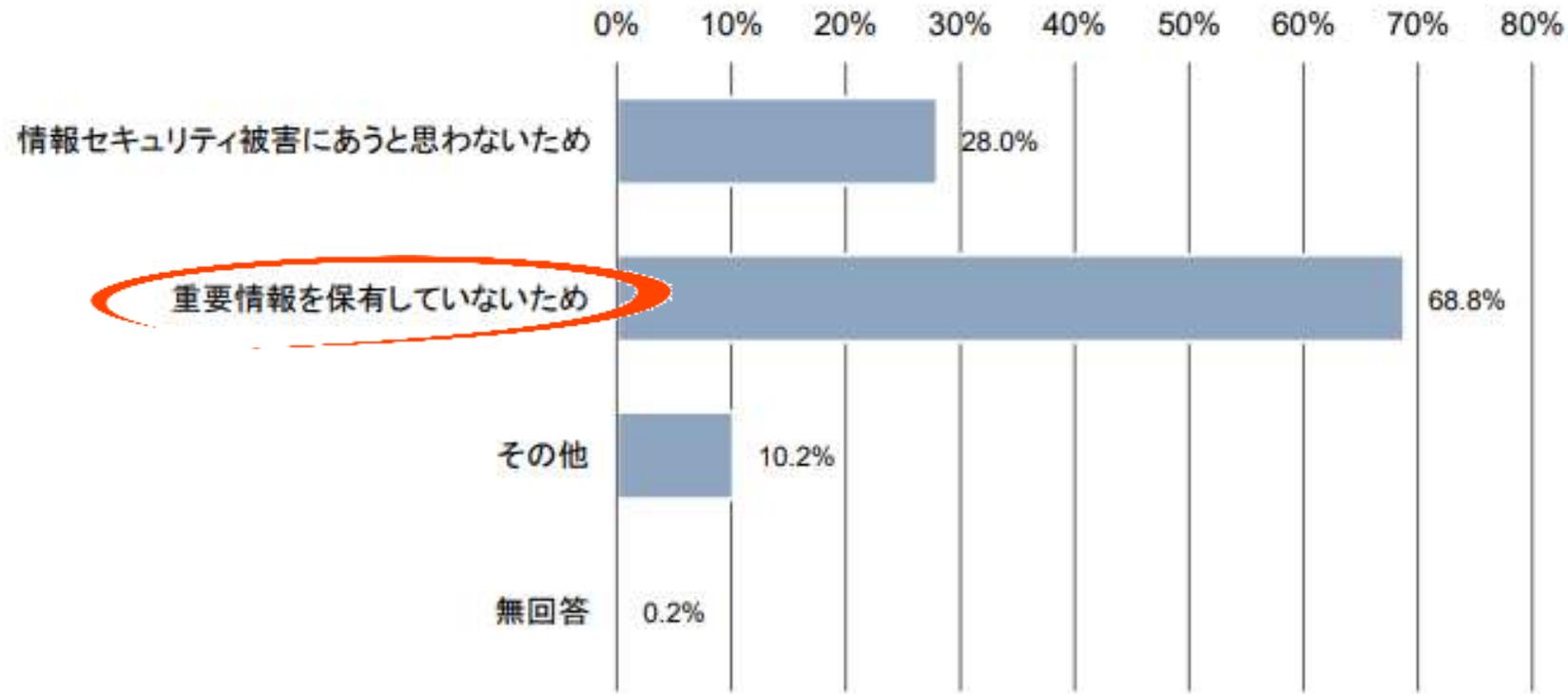
多くの中小工場が抱える課題



中小企業の実態

情報セキュリティ対策の必要性を感じない理由

n=1,259

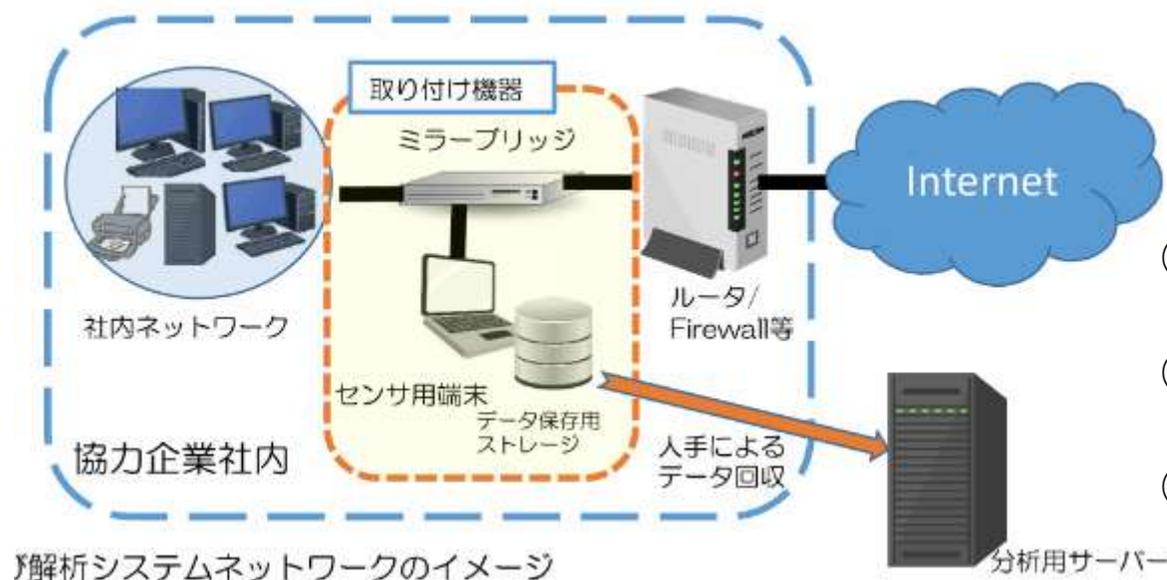


IPA「2021年度中小企業における
情報セキュリティ対策に関する実態調査」より抜粋
有効回答数4,074（製造業11.8%）

**情報セキュリティリスクは機密性（情報漏洩）だけではない
特に製造業は可用性（生産を止めない）が重要。止まっても大丈夫な工場はない！**

中小企業の実態

大阪商工会議所のサイバー攻撃調査では30/30社で不正通信を検知



解析システムネットワークのイメージ

- ①外部から社内の端末をリモート操作の可能性
- ②社内端末と悪性サイトとの通信
- ③DDoS攻撃を目的としたパケットを受信

具体的な事例①

●マルウェアを飼っている工場

2008年に「コンフィッカー」というワームが爆発的に蔓延。しかし、工場内では目立った被害が出ないために、いまだに感染した機器が稼働している工場がある。

- 工場では機器の稼働年数が情報系と比べて長い
工場内にもWindowsOSで動作している機器が多数あるが、その認識はない
工場内にはマルウェアを検知する手段がない

●LANカード2枚刺しパソコンでネットワーク分離

生産情報の連携などのために、OTとOAをネットワークでつなぐ必要が出てきたが、ネットワークスイッチ（HUB/L2スイッチ）やNIC2枚刺しPCでつなぐケースが多く見られる。

- 中小製造業のネットワーク構築は、地場の電気工事事業者などが手掛けることが多い。
セキュリティ知識やノウハウのある人材が社内にはいない。

具体的な事例②

●セキュリティのイメージ

リスクアセスメントハンドブックの作成中に現場のご意見を伺いたく、実際の工場を訪問した際、「セキュリティ」と聞いて思い浮かぶことをお訊ねしたら、「セコムさんとかですかね」という回答だった。

→ 敢えて「情報セキュリティ」とは言わなかったが、やはり、あまり関心がないことが伺われる。

●セキュリティ侵害を受ける可能性

同様に、実際の工場でUSBメモリーを例にアセスメントの方法を説明したところ、「USBメモリーは使っているが、これがリスクになるとは知らなかった」というお話を聞いた。

→ 加えて、工場はインターネットにつながっていないとのことだが、事務所とはつながっていて、事務所はインターネットにアクセスできる環境だった。

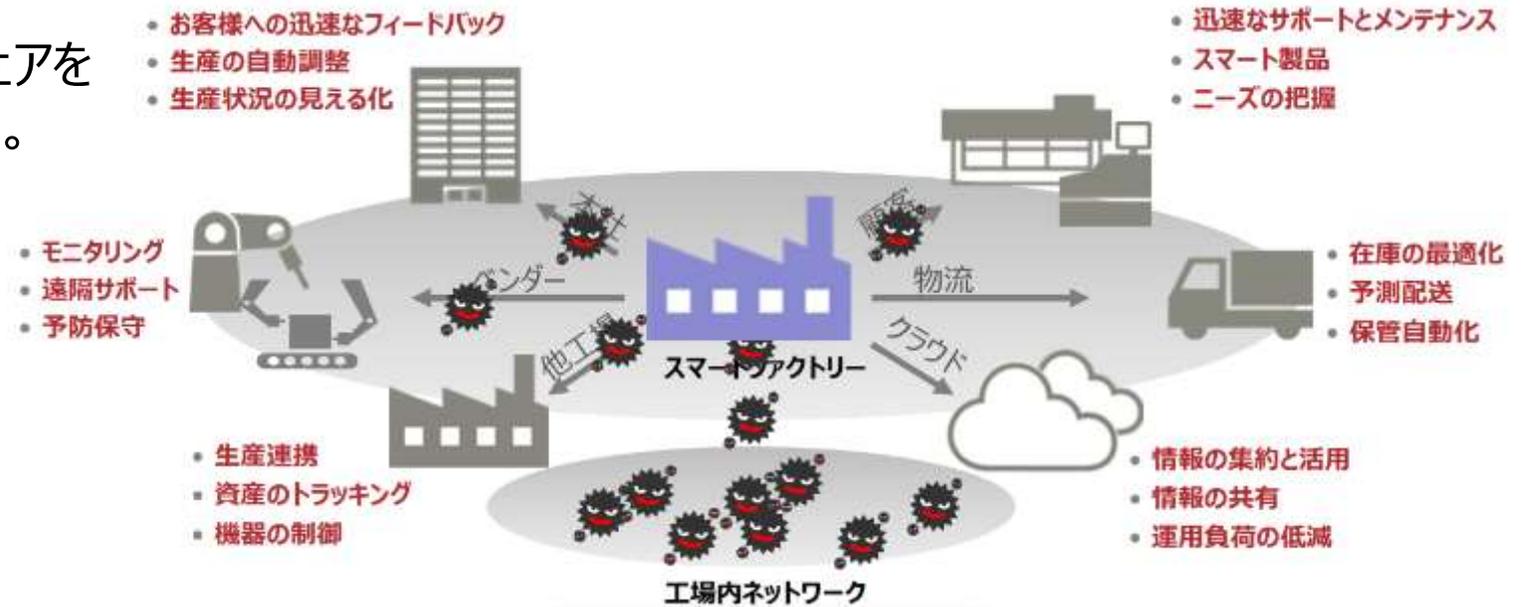
被害者から加害者へ

●生産停止の影響

基本的な対策を怠っているとセキュリティ侵害による生産停止の責任を問われる

●DXの推進で新たな脅威

安易なネットワーク化は新たな脅威を生むことになる。
知らずに飼っていたマルウェアを
まき散らす原因になるかも。



水平方向の対策



→ すり抜けた攻撃を見逃さない

→ 被害範囲を特定して対処

中小企業診断士が関われること

中小企業では情報セキュリティに関する認識が薄い

技術面はベンダー企業にまかせる
ただしベンダー企業との橋渡しが必要

人材教育は、ある程度の知識があれば可能

中小企業診断士が関われること

リスク認識の共有（BCP対策）

入社してから
退社するまで

中小企業診断士が関われること

セキュリティアクション、情報セキュリティポリシー策定

情報セキュリティ
ポリシーサ
ンプル



セキュリティ対策自己宣言



セキュリティ対策自己宣言

中小企業診断士が関われること

ベンダー企業との橋渡し、双方の翻訳

セキュリティバ
イデザイン

中小企業診断士が関われること

セキュリティ教育

ここから
セキュリティ

情報セキュリティ10大脅威

新入社員教育

3rd STEP BCP策定

2023年12月1日に大阪で「NSF in KANSAI 2023」を開催
工場内でのセキュリティ事故を想定したワークショップを実施



どのような行動をとればいいのか、事前に決めておくことが重要であると実感

参考資料

IPAポイント学習

https://www.ipa.go.jp/security/sec-tools/5mins_point.html

サイバーセキュリティ経営ガイドライン

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

情報セキュリティポリシーサンプル

<https://www.jnsa.org/result/west/2016/2016-019.pdf>

情報セキュリティ対策手引き9to5

<https://www.jnsa.org/result/west/2014/2014-001.pdf>

JNSA西日本支部成果物

<https://www.jnsa.org/result/west/index.html>

中小企業の情報セキュリティ対策ガイドライン

<https://www.ipa.go.jp/security/guide/sme/about.html>

情報セキュリティガイドライン

<https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf>

IPAセミナー案内

中小企業向けセミナー

<https://www.ipa.go.jp/security/seminar/sme/supportseminar.html>

サイバーセキュリティ演習（兵庫・2月14日・神戸市産業振興センター）

<https://www.ipa.go.jp/security/seminar/sme/t6hhco000000h903-att/20250214hyougo.pdf>

サイバーセキュリティ演習（堺・2月13日・堺市産業振興センター）

<https://www.ipa.go.jp/security/seminar/sme/t6hhco000000h903-att/20250213sakai.pdf>

関西万博までにやっておきたいセキュリティ

<https://www.ipa.go.jp/security/seminar/sme/t6hhco000000h903-att/20250219osaka.pdf>

以下、参考

フラッシュメモリストレージ使用上の注意点

皆さんがお使いのUSBメモリ、SDカード、SSD・・・

- ✓ データは消えていません
- ✓ データは化けて（変化して）います

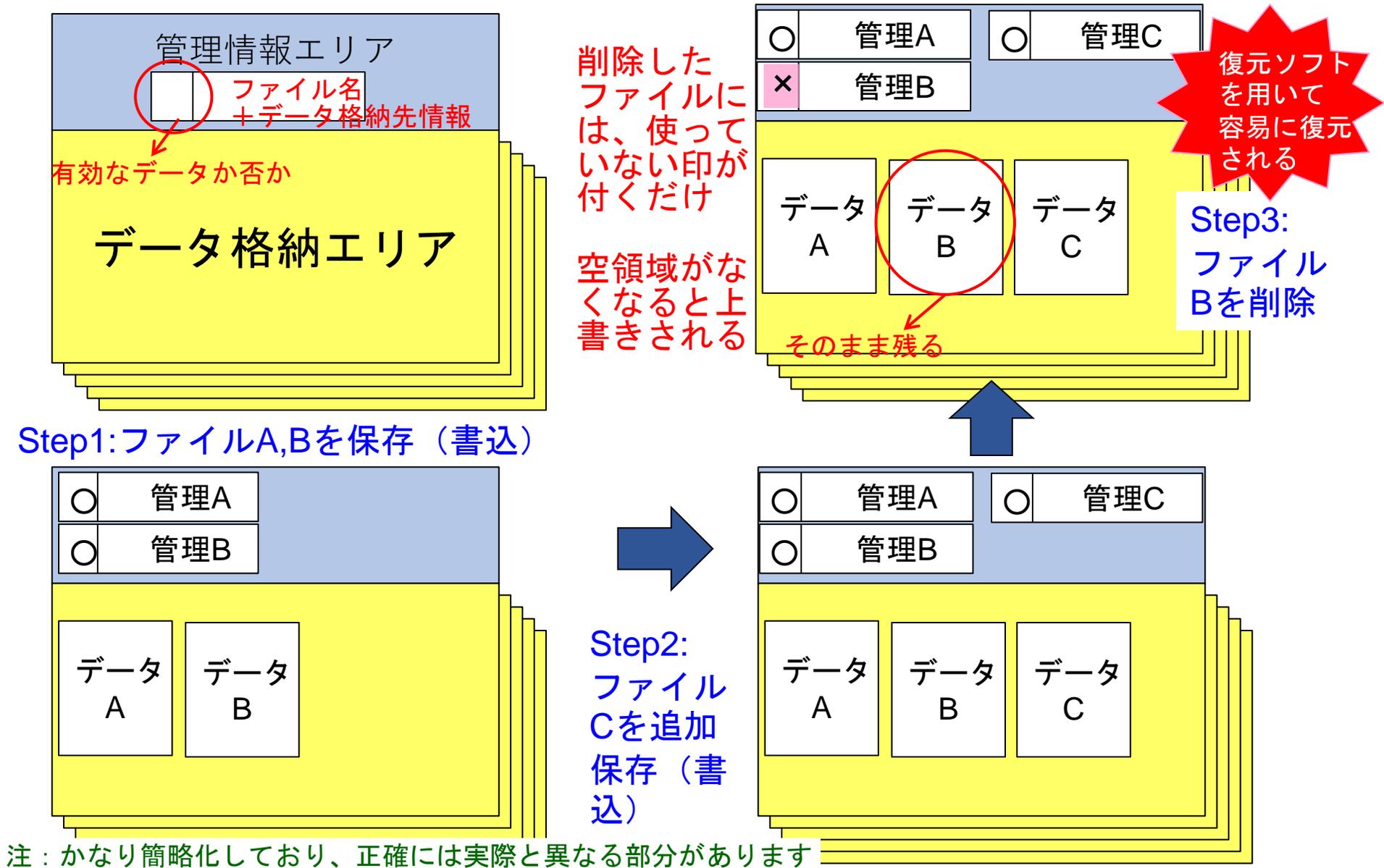
問題点 1

消したつもりでも
管理領域が消えているだけ

問題点 2

長期間放置していると
データが化ける

ファイル管理の仕組み概略



ソフトウェアによる完全消去（HDD）

HDDのデータ消去は下記のように複数回の書き込みを行わないと完全消去性が損なわれます。

<http://it.jeita.or.jp/infosys/committee/network/guideline0407/standard.html> より

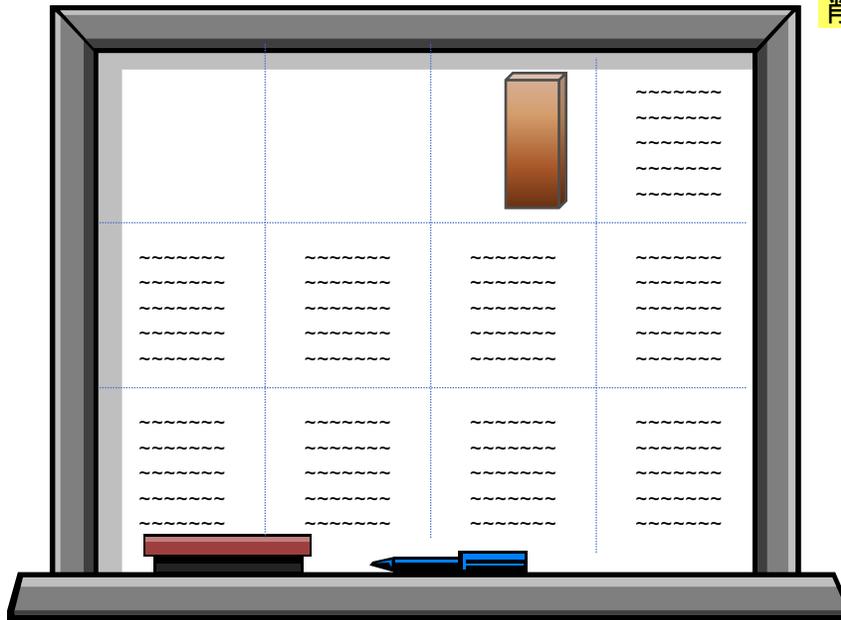
レベル	HDDのデータ抹消方式	スピード	抹消力
0	“00”データ書き込み	速	弱
1	乱数書き込み	↑	↓
2	NSA推奨方式(乱数2回書き込み ⇒ “00”書き込み)		
3	NCSC推奨方式(固定値1 ⇒ 固定値1の補数 ⇒ 固定値2)		
4	米陸軍準拠方式(乱数 ⇒ 固定値1 ⇒ 固定値1の補数)		
5	米海軍準拠方式(固定値1 ⇒ 固定値1の補数 ⇒ 乱数 ⇒ 検証)		
6	米空軍準拠方式(“00”書き込み ⇒ ”FF”書き込み ⇒ 固定値1 ⇒ 検証)		
7	米国防総省準拠方式(固定値1 ⇒ 固定値1の補数 ⇒ 乱数 ⇒ 検証)		
8	グートマン推奨方式(乱数4回 ⇒ 固定値1 ⇒ . . . ⇒ 固定値27 ⇒ 乱数4回)	遅	強

HDDでは、これらの消去方式をサポートした消去ソフトを適用することにより、時間をかければ限りなく完全消去に近い状態にすることができます。

HDDとFlashストレージとの違い

Hard Disk Drive

論理アドレスと物理アドレスは1対1に対応している



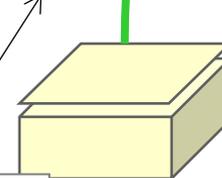
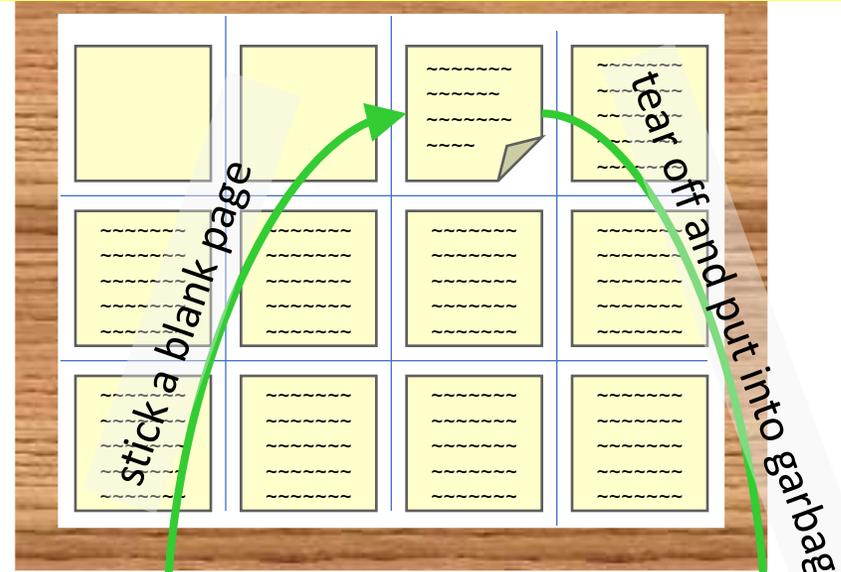
Repeat overwriting to same area to avoid erase-residues. (Previous data may be remained)

NAND Flashの書込み単位・書込み順序の制限と書換回数の限界の問題から、上書きができない。

Flash Memory Drive

論理アドレスと物理アドレスは1対1対応ではなく、かつ変動する関係にあり、物理アドレスのほうが多くなっている

削除時は付箋をボードからはずすだけで、まだ廃棄はされていない

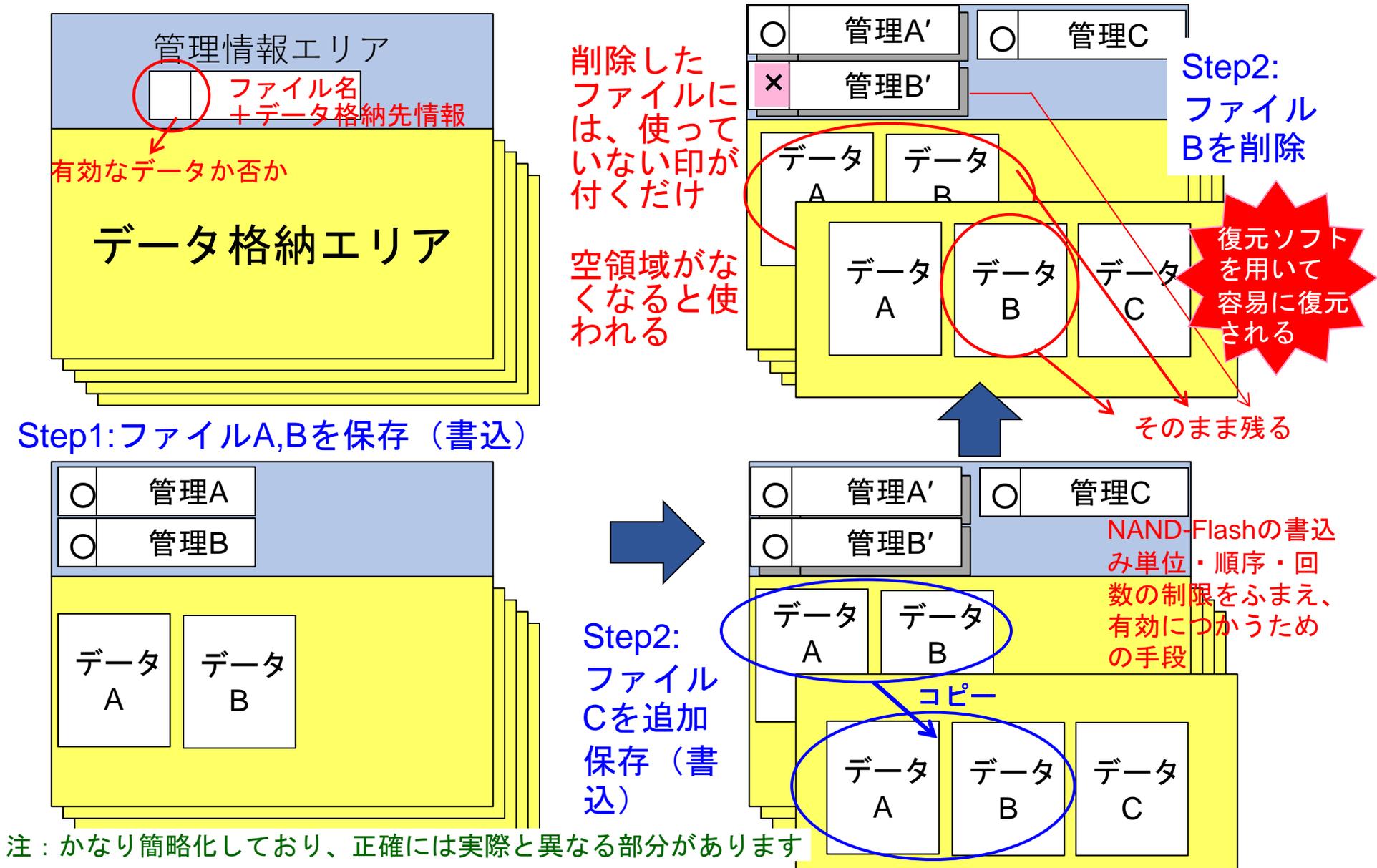


Garbage Collection



create blank pages by erasing old data

Flash Storageにおけるファイル書き込み原理



【参考】 SSDにおけるコピーされたファイル数

前述のように、いくつもコピーができていき、その数は予測が難しい。
ある論文の報告では、同じファイルのコピーが16個も確認されています。

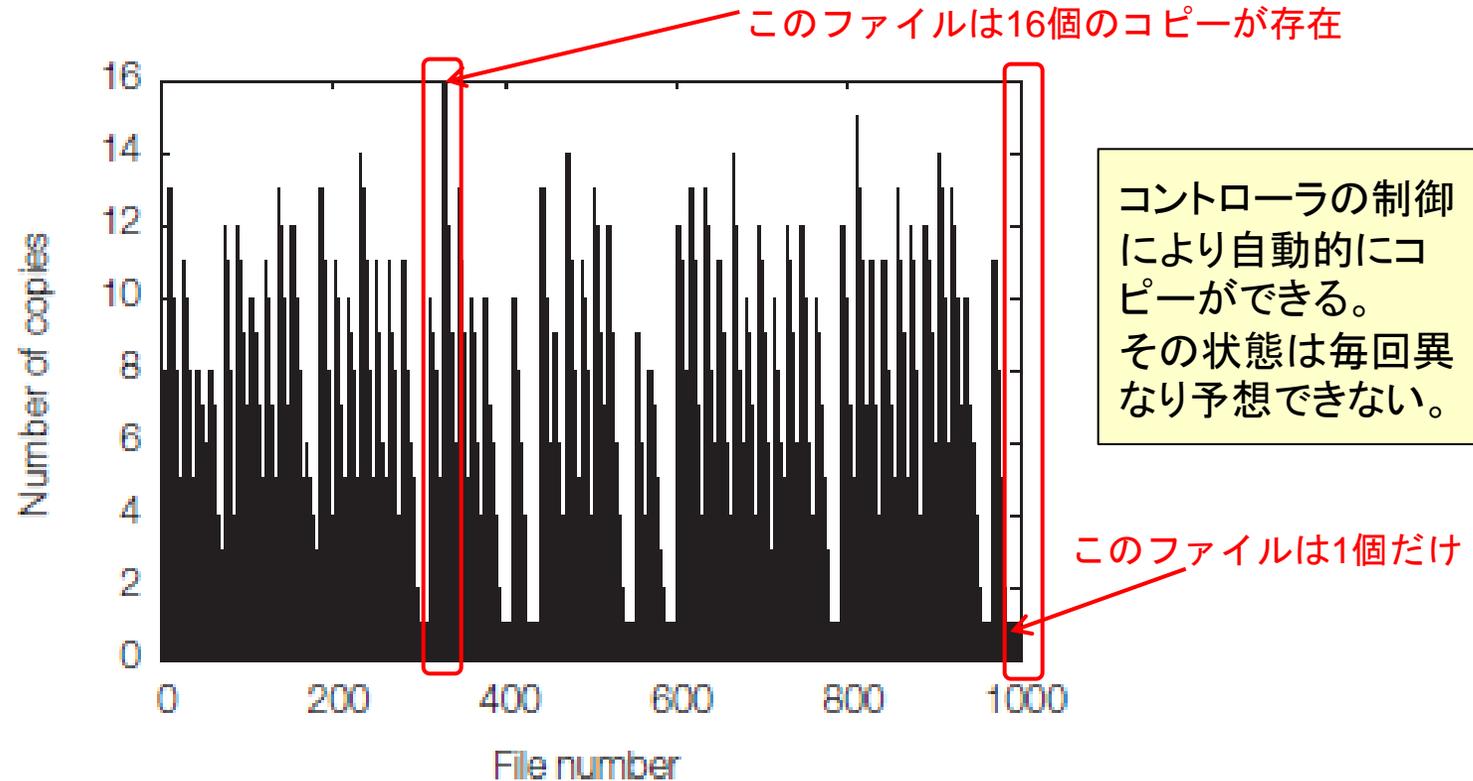


Figure 1: Multiple copies This graph shows The FTL duplicating files up to 16 times. The graph exhibits a spiking pattern which is probably due to the page-level management by the FTL.

ソフトウェアによる完全消去 (Flash Drive)

Flash memory DriveをHDDと同じく消去ソフトで消去した場合、先ほどの説明でわかるように上書きによる消去はさらにコピーを増やすことになってしまいます。
下記のように複数回の書き込みを行っても、完全に消去できるかはわかりません。

レベル	HDDのデータ抹消方式	スピード	抹消力
0	“00”データ書込み	速	弱
1	乱数書込み	↑	↓
2	NSA推奨方式(乱数2回書込み ⇒ “00”書込み)		
3	NCSC推奨方式(固定値1 ⇒ 固定値1の補数 ⇒ 固定値2)		
4	米陸軍準拠方式(乱数 ⇒ 固定値1 ⇒ 固定値1の補数)		
5	米海軍準拠方式(固定値1 ⇒ 固定値1の補数 ⇒ 乱数 ⇒ 検証)		
6	米空軍準拠方式(“00”書込み ⇒ “FF”書込み ⇒ 固定値1 ⇒ 検証)		
7	米国防総省準拠方式(固定値1 ⇒ 固定値1の補数 ⇒ 乱数 ⇒ 検証)		
8	グートマン推奨方式(乱数4回 ⇒ 固定値1 ⇒ . . . ⇒ 固定値27 ⇒ 乱数4回)		

<http://it.jeita.or.jp/infosys/committee/network/guideline0407/standard.html> より

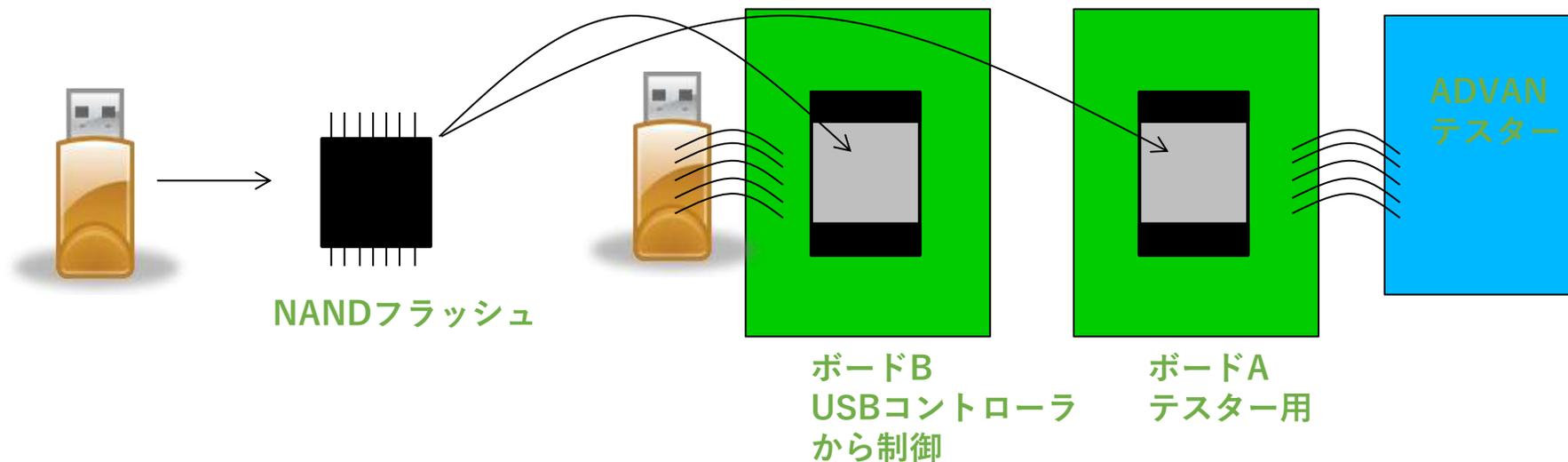
HDDのために開発されたこれらの消去方式を用いても、フラッシュメモリドライブには完全ではありません。しかし、現状他に方法がなく、これらの消去用います。

データ消去確認実験

USBメモリ上でデータを消去しても、USBメモリに搭載されているNANDフラッシュメモリでは、消去動作は行われず、管理領域のデータが書き換えられるのみ。
このようになっている事を実際に、NANDフラッシュメモリのデータを半導体メモリ検査用のテスターにて読み出すことで確認する。

測定手順

- ① ボードAでテスターにてNANDフラッシュを読み出し（データA）
- ② ボードBでUSBメモリとしてファイルの書き込みを実施
- ③ ボードAでテスターにてNANDフラッシュを読み出し（データB）
データAとデータBを比較する。ファイルの削除やフォーマット後の確認も実施する。



USBメモリ (NAND Flash搭載) 実験まとめ

1. USBメモリ上で**データを消去しても**、USBメモリに搭載されているNANDフラッシュメモリでは、消去動作は行われず、**元データは残っていることが確認された。**
2. フォーマット動作を行うと、簡易な復元ソフトでは復元不可能となるが**元データはかなり多く残っていることが確認された。**
3. 市販の完全消去ソフトでは、3回上書き以上でないとも有効性は低いが、3回上書きには**かなり時間がかかる。**しかし、完全消去に近づけるための一定の効果は期待できる。

【参考】

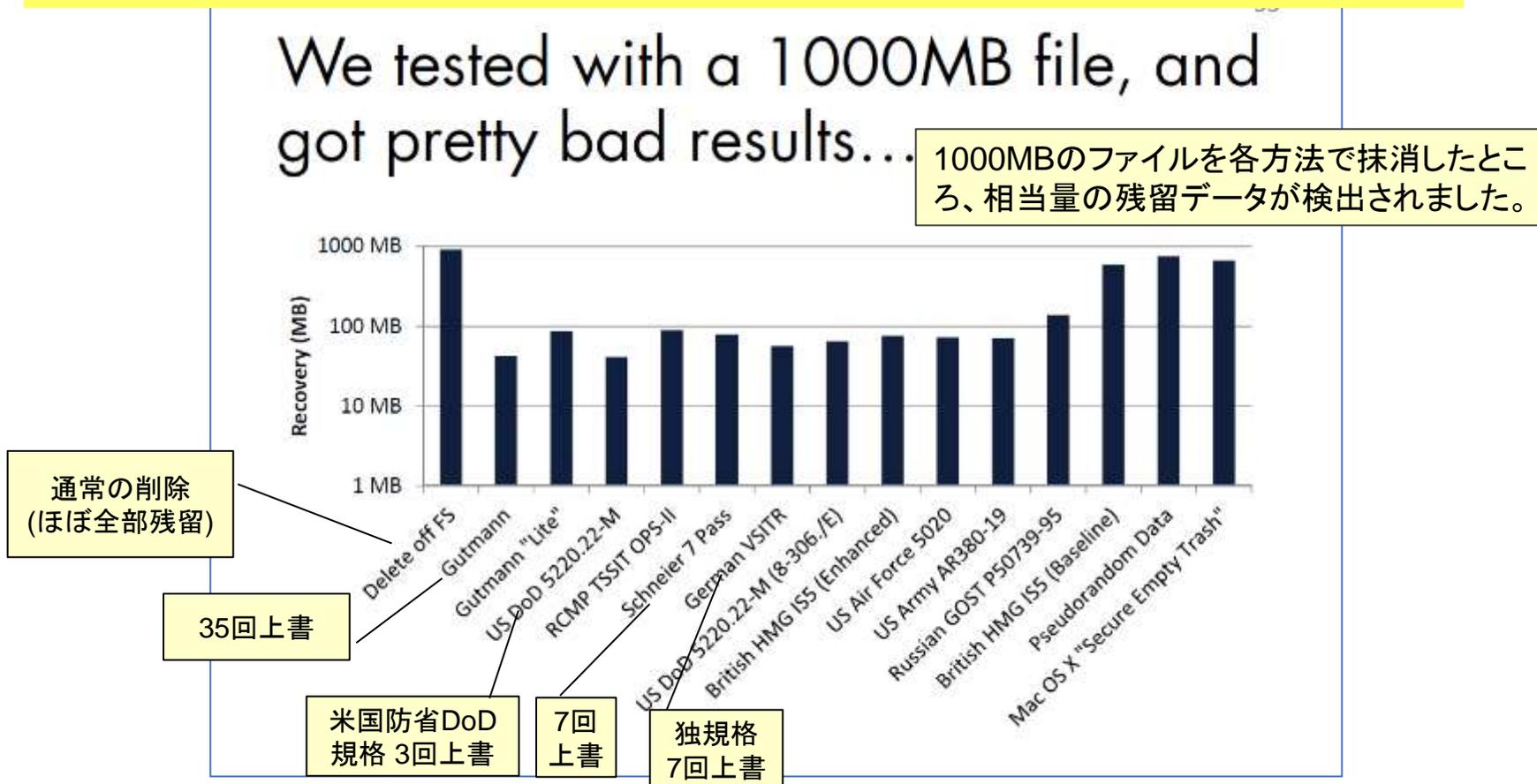
フォレンジックなどに用いられるフラッシュメモリ解析装置は市販されており、一般の人でも購入が可能です。

価格は思ったほど高くなく、大企業の方ならボーナス1回分くらい！？この装置を使えば、今回の実験で得られたデータを、ファイルの形に複製することも可能になります。



【参考】 データ消去に関する論文よりファイル抹消方法毎のデータ残留量

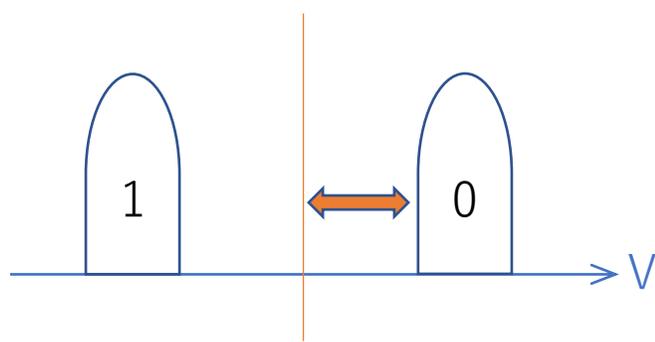
本論文では、各消去方式を用いた詳細な残留データ量が測定されており、Gutmannや米国国防省DoDでも2-3%は残るという結果



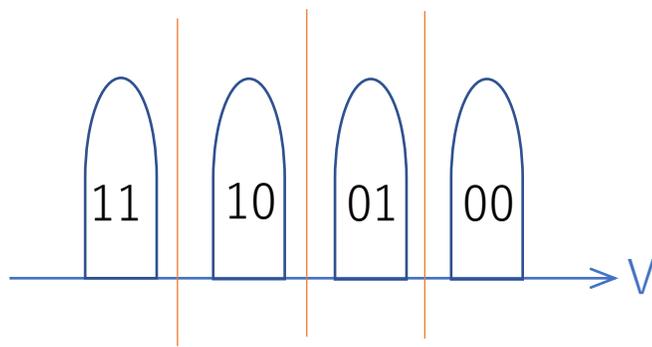
Reliably Erasing Data from Flash-Based Solid State Drives, p53
- Michael Wei, Non-Volatile Systems Laboratory, University of California, San Diego

フラッシュメモリのデータ保持

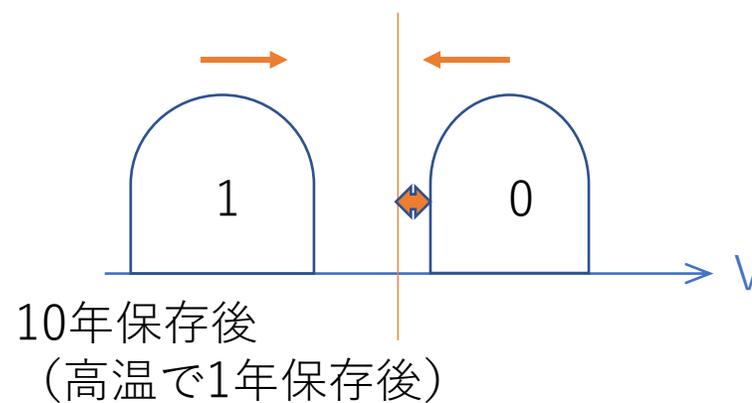
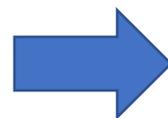
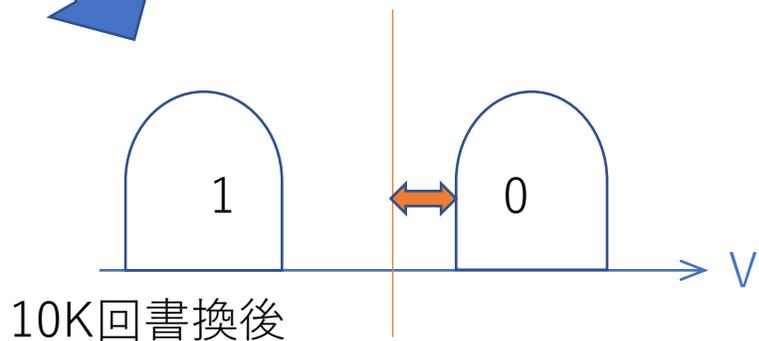
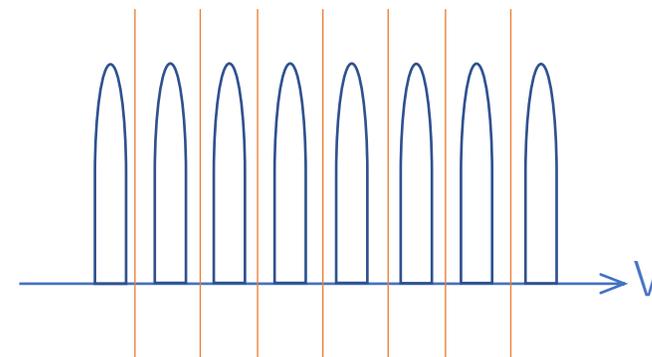
SLC 1bit/cell
0/1



MLC 2bit/cell
00/01/10/11



TLC 3bit/cell
000/001/010/011/
100/101/110/111





ドライブレコーダー SDカードに正しく記録するために

● 映像は定期的に確認しましょう。

テストしたドライブレコーダーには、SDカードの異常を検出して表示や音で知らせる機能がありました。

SDカードに生じた不具合の種類によっては、異常を検出しない銘柄もありました。SDカードや本体に異常がないか確かめるため、**正常に記録されていることを定期的に確認**しましょう。



● SDカードは定期的にフォーマットしましょう。

不良セクタの累積を想定したテストでは、正常に記録できない銘柄がありました。取扱説明書に沿って**定期的にフォーマット**して使用しましょう。

● SDカードは消耗品です。定期的に交換しましょう。

SDカードは繰り返しの記録により劣化していく消耗品です。容量やスピードクラスなど、ドライブレコーダーの仕様合ったSDカードを選択し、**定期的に新品に交換**しましょう。

● 目的や使用方法に合わせて商品を選択しましょう。

ドライブレコーダーの中には、定期的なフォーマットが不要なものや、起動時にSDカードをチェックする機能があるものがあります。また、SDカードには繰り返しの記録に対して耐久性が高いと謳うものもあります。**目的や使用方法に応じて商品を選択**しましょう。



本内容の詳細は、独立行政法人
国民生活センター公式サイトに
掲載しています。
<http://www.kokusen.go.jp/>

くらしの危険

最新号やバックナンバーは
こちらからご覧いただけます。

公式サイト「くらしの危険」コーナー
<http://www.kokusen.go.jp/kyoken/index.html>



●「くらしの危険」は、全国の消費生活センター、国民生活センターから収集した情報をもとに、被害や事故の未然防止・拡大防止のために作られています。●特定の商品・サービス等を推奨するものではありません。●商品やサービス、数量によって価格や事故の賠償を請求する消費生活センターにお尋ねください。●複製転載はお断りいたします。



独立行政法人 国民生活センター

〒252-0229 神奈川県横浜市中区新港3-1-1 TEL: 042-758-3165 ●2018年11月発行
イラスト：川崎 敬祐

くらしの危険 Number 346

ドライブレコーダー

SDカードの異常で映像が記録されないことも



自動車のフロントガラスなどに取り付け、運転のようすを記録^{※1}するドライブレコーダー。事故やトラブル発生時に映像を確認したところ、録画されていなかったという相談が寄せられています。

データの記録に用いられるSDカード^{※2}は、繰り返しの記録により劣化する消耗品です。SDカードの異常の検出や通知方法は、ドライブレコーダーによって異なるので、取扱説明書等を確認しましょう。また、正常に映像が記録されているか定期的に確認し、SDカードのメンテナンスも定期的に行いましょう。

※1：エンジン起動からエンジン停止までの映像を記録し続ける「常時録画」、センサーが一定以上の衝撃を検出した時に映像を記録する「イベント録画」などがあります。
※2：デジタルカメラやスマートフォンなど、写真や映像を記録する機器などに使用される記録媒体。形状によってSDメモリーカードやMicroSDメモリーカードなどに分けられます。

フラッシュメモリストレージまとめ

- ✓ フラッシュメモリストレージの使い方に注意
- ✓ 長期保存用には向かない、一時保存やデータ移動用
- ✓ 産業用途に使う場合は、それなりの製品を選ぶ
- ✓ USBメモリやSDカードを人に渡す場合には注意

すぐに消えるのに
なかなか消えない
特性を理解して活用しましょう

- ✓ 定期的に交換する
- ✓ PCから取り外し処理を行う
- ✓ 大事なデータにはそれなりのお値段のものを
- ✓ データを消してしまっても大丈夫、高い復元費用払う必要なし！