組織で働く人間による不正・事故は止められるのか？
～「内部不正対策14の論点」発売記念セミナー～

HITACHI
Inspire the Next

内部不正はセキュリティ製品で防げるか？
～CIOの内部不正という極論で考えてみる対策の効果～

2015年9月9日

株式会社日立ソリューションズ
武田　一城

HITACHI
Inspire the Next

Contents

HITACHI
Inspire the Next

1. 自己紹介

1. 自己紹介

HITACHI
Inspire the Next

株式会社　日立ソリューションズ
兼：日本PostgreSQLユーザ会　理事
武田　一城　（1974年　千葉県生まれ）

情報セキュリティ、システムプラットフォーム他の分野でのマーケティング戦略立案
や各種プロモーションの企画を担当。
（オープンソースやBCP、最近トレンドの教育ICTなど・・・、節操なく色々とやってます）

**つまり、もちろん研究者でもなければ、
セキュリティ技術者ですらありません。**

1. 自己紹介

HITACHI
Inspire the Next

ただ、ここ数年でいろいろな場でお話や文章を書かせていただく機会が多くなってきたこともあって、以下のような活動をさせてもらっています。

Webメディアへの寄稿

講演活動

執筆活動

・・・あまり他に居ないのでニッチなニーズがあるみたいです。

1. 自己紹介（教育ICT分野の寄稿）

HITACHI
Inspire the Next

TechTaeget Japan

1. 今、理解しておきたい「学校IT化の現実」

- 教室のIT化で見落としがちな「5つの落とし穴」とは？
- 学校IT化を本気で成功させる「グランドデザイン」の作り方

2. 失敗しない「学校IT製品」の選び方

- 学校無線LANの「つながらない」「危ない」は“正しい理解”で解消できる（無線LAN/前編）
- 学校無線LAN選びを本気で成功させる「4つの視点」（無線LAN/後編）
- 学校IT化の“無法地帯”を一掃する「シンクライアント」の威力（シンクライアント/前編）
- 学校のシンクライアント導入がうまくいかない「４つの理由」（シンクライアント/中編）
- ChromeBookも有効「シンクライアントは高すぎる」という学校への代替策（シンクライアント/後編）
- 「目隠し型セキュリティ」は子どもをダメにする（セキュリティ/前編）
- LINEを悪者扱いする前に「情報モラル」を学ぶべき（セキュリティ/中編）

ICT教育ニュース

先生のための初級ICT教育講座

- 教育ICTの本格普及の前にやるべき情報セキュリティ対策
- 武南学園の中高一貫新設校で見た“未来の学校”

1．自己紹介（セキュリティ分野の寄稿）

HITACHI
Inspire the Next

IT media エンタープライズ

日本型セキュリティの理想と現実　（隔週でのweb連載）

- セキュリティインシデントが繰り返される理由
- 戦国ファンならわかる？　城郭の変遷とセキュリティ環境
- 「進撃の巨人」で理解する多層防御
- 常時接続から始まったセキュリティ対策の無間地獄
- 利便性 vs 安全性　交通安全に学ぶセキュリティの行方

この縁でお話させていただくことになりました

日本ネットワークセキュリティ協会（JNSA）

組織で働く人が引き起こす不正事故対応ワーキンググループ　著

「内部不正はセキュリティ製品で防げるか？」

書籍

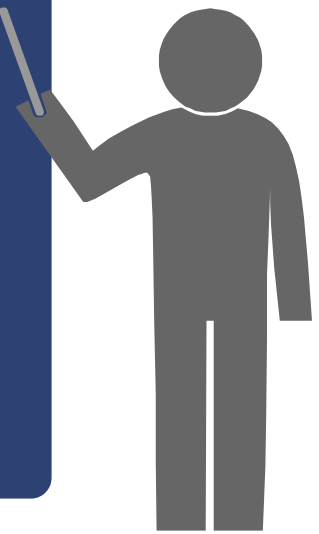
11人の共著

Amazon.co.jp
セキュリティ管理部門1位
（8/5時点の瞬間値）

出版記念セミナー in品川
（おかげ様で満席）

HITACHI
Inspire the Next

本日は、セキュリティ分野の
マーケティング活動の経験と
視点からの内部不正対策の
お話をさせていただきます。



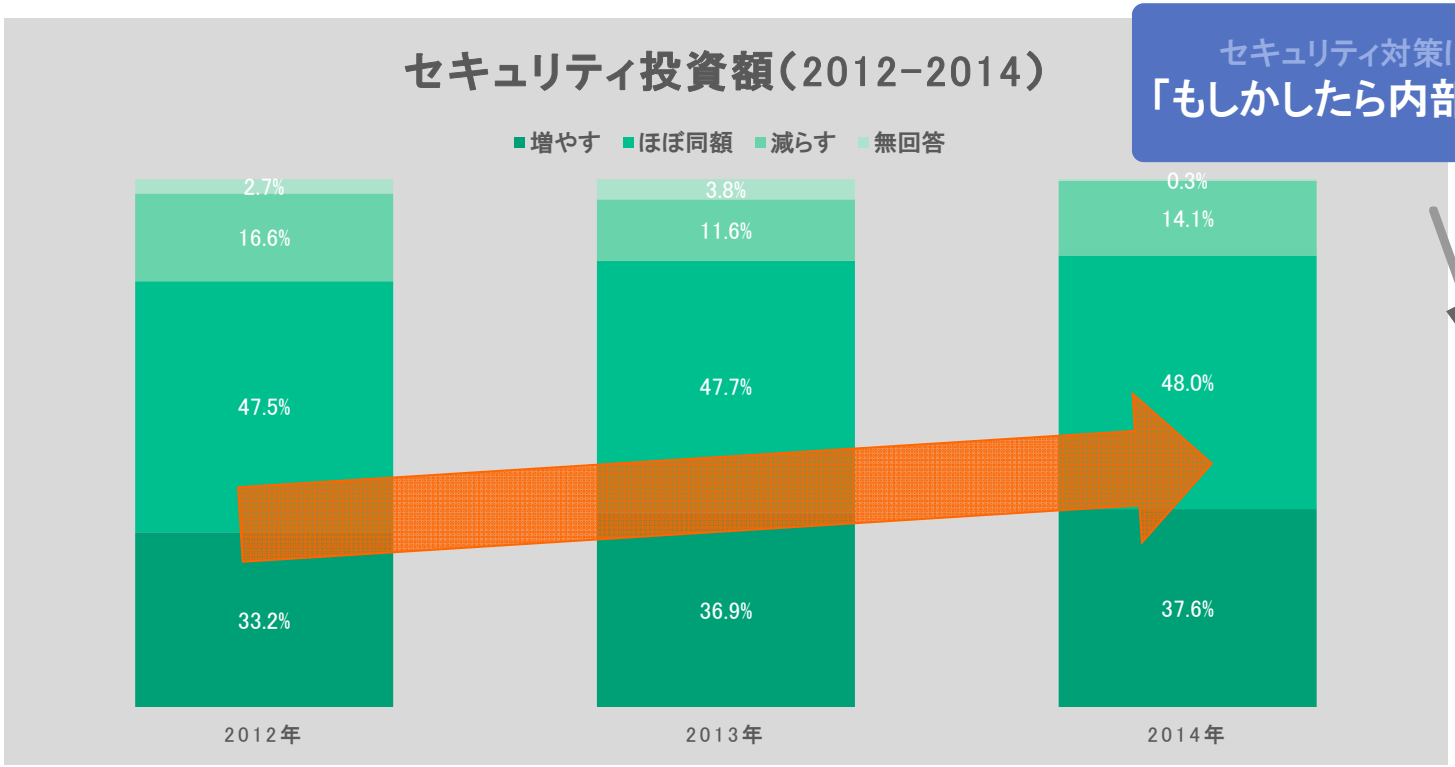
HITACHI
Inspire the Next

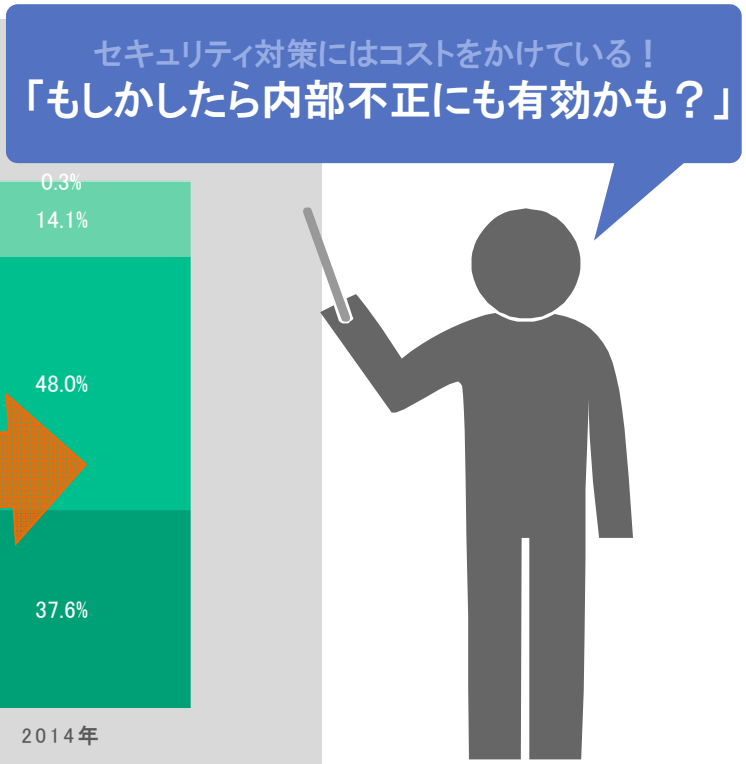
2. 内部不正はセキュリティ製品で防げるか？

2. 内部不正はセキュリティ製品で防げるか？

HITACHI
Inspire the Next

連日のようにサイバー攻撃による被害のニュースがメディアで報道されています。そのため、セキュリティ対策の予算も右肩上がりで拡大しています。





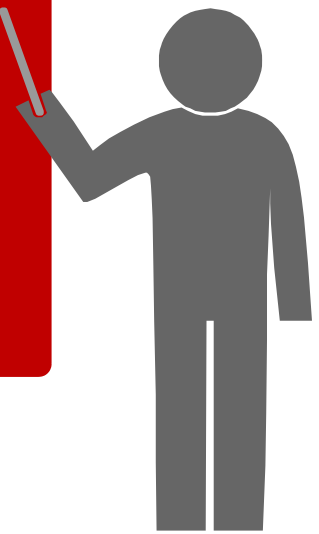
【出典】企業における情報セキュリティ実態調査/NRIセキュアテクノロジーズ

2. 内部不正はセキュリティ製品で防げるか？

HITACHI
Inspire the Next

あらためまして・・・。

内部不正はセキュリティ製品を導入すれば防げるか？



結論：

ほとんど無理

2. 内部不正はセキュリティ製品で防げるか？

HITACHI
Inspire the Next

外部からの攻撃の標的型攻撃（APT）より
内部不正の対策ははるかに大変だから！

外部攻撃 ＜ 内部不正

2. 内部不正はセキュリティ製品で防げるか？

HITACHI
Inspire the Next

HITACHI
Inspire the Next

Question 1

一般的なセキュリティ製品の目的は何でしょうか？

2. 内部不正はセキュリティ製品で防げるか？

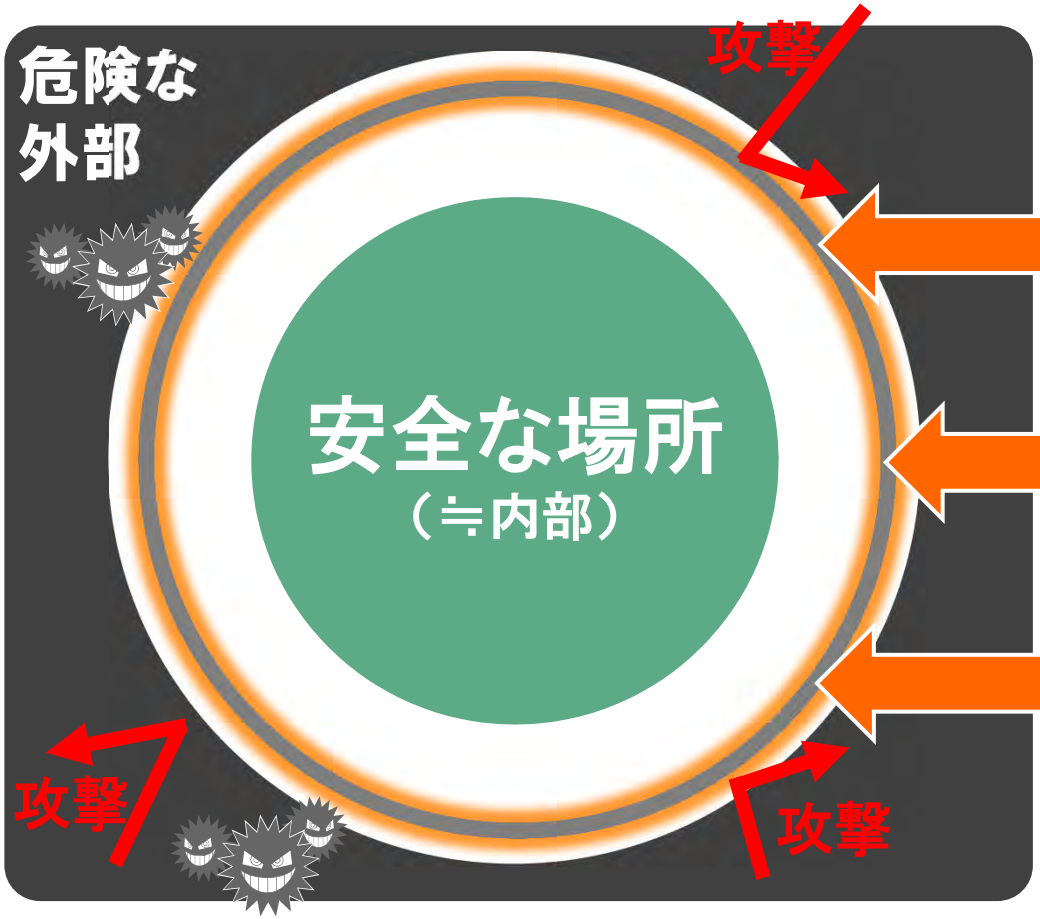
HITACHI
Inspire the Next

Answer

外部の攻撃から
内部の重要なもの
を守れる構造を作る

2. 内部不正はセキュリティ製品で防げるか？

HITACHI
Inspire the Next



＜代表的なセキュリティ製品＞

ファイアウォール
（ゲートウェイの扉/防火壁）

IDS/IPS
（不正侵入検知/防御）

アンチウィルスソフト
（ウィルス・マルウェアの侵入を防ぐ）

2. 内部不正はセキュリティ製品で防げるか？

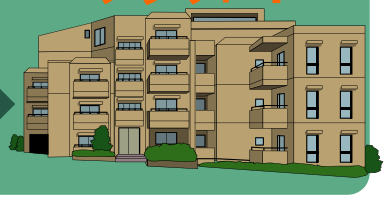
HITACHI
Inspire the Next

防御壁をつくることによって、内部の安全地帯に攻撃者を入れないようにする防御思想

オンプレミス？

一戸建てやマンションに塀を立てたり鍵をかけることと同じ

クラウド？



これが一昔前のセキュリティ対策の常道

境界防御と言います

2. 内部不正はセキュリティ製品で防げるか？

HITACHI
Inspire the Next

大きく風向きが変わったのが・・・

2011年

高度な対策を駆使し尽しているはずの国内の防衛産業の複数社からの情報漏えいが明らかになった

2. 内部不正はセキュリティ製品で防げるか？

HITACHI
Inspire the Next

一般企業とは別次元の高度な
セキュリティ対策をしていたに
もかかわらず、侵入された。

内部は安全という前提が崩壊

2. 内部不正はセキュリティ製品で防げるか？

HITACHI
Inspire the Next

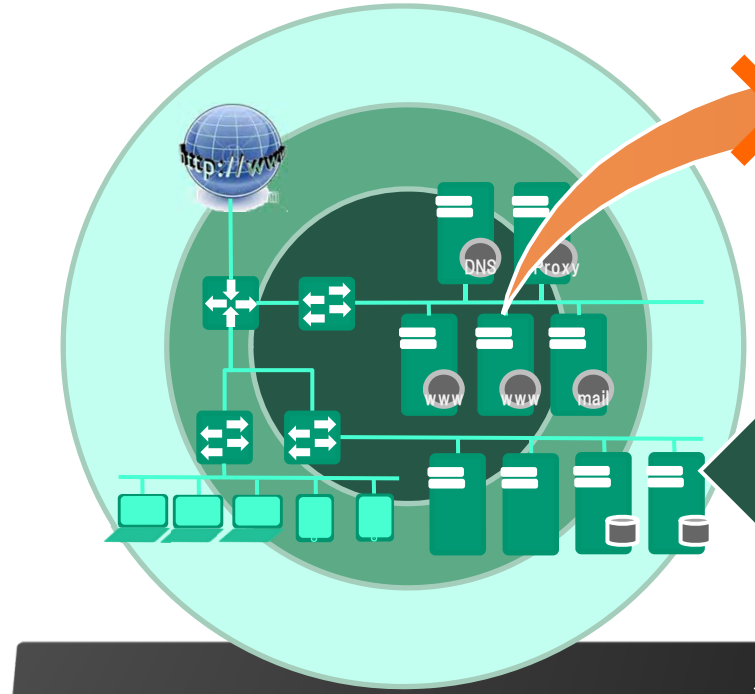
どんな堅固な壁を築いても

安全な場所は無くなった

2. 内部不正はセキュリティ製品で防げるか？

HITACHI
Inspire the Next

その結果、多層防御という考え方が一般化した！



攻撃者が目的達成する
途中の段階で対策ができる
（内から外への対策）

多層防御構造
（攻撃者が重要情報に辿り着くまでの時間を稼ぎ）

監視・管理
（攻撃者の痕跡をつかむ）

セキュリティマネジメント

2. 内部不正はセキュリティ製品で防げるか？

HITACHI
Inspire the Next

内部不正はセキュリティ製品を導入すれば防げるか？

ほとんど無理

（外部からの攻撃より内部不正の対策ははるかに高度！）

抑止効果と予兆検知

（多層防御構造と痕跡を見つける監視・管理体制が必須！ただし、防止というまでの効果は疑問）

2. 内部不正はセキュリティ製品で防げるか？

HITACHI
Inspire the Next

内部不正の防止とまで言い切れる対策は難しいものの・・・。


そして、少しだけ朗報なのは・・・

2. 内部不正はセキュリティ製品で防げるか？

HITACHI
Inspire the Next

次世代型ファイアウォール
（ネットワークを通るアプリケーションの可視化）

サンドボックス
（未知のマルウェア解析）

ログ解析
（ビッグデータ技術の応用／膨大なログ収集と解析が可能）

攻撃手法が巧妙化

セキュリティ製品も進化

内部不正にも一定の効果

セキュリティ対策製品も
それなりに進化していること

つまり、

外部からの攻撃が巧妙化して、攻撃者が内部に入られてから
の対策をしなければならない必要に迫られた結果・・・

内部不正対策としても効果を持つようになった

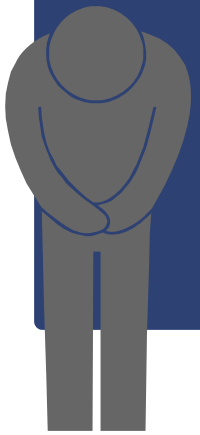
HITACHI
Inspire the Next

3. CIOの内部不正は防げるか？

3. CIOの内部不正は防げるか？

HITACHI
Inspire the Next

情報に関する最高責任者のCIOが、万が一にも内部不正をしたら・・・というのを思いついたので、「仮定の話」として考えてみました。



あくまで**極論**としての一考察です。


ここに登る
感じ・・・
つまり、ただでさえ難易度の高い内部不正対策
のハードルをさらに、めちゃくちゃ上げてみた！

ちなみに副題にしてしまったことに

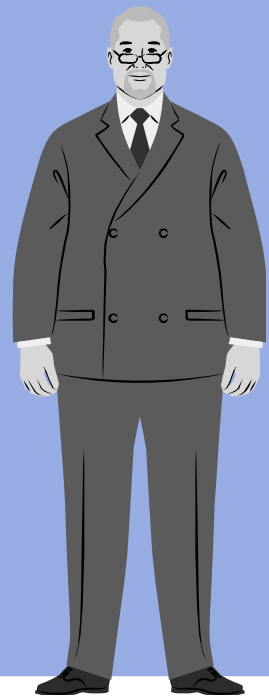
後悔はありません

（副題公開は資料作成前の7月）

HITACHI
Inspire the Next

Question 2

CIOとはなにか？



3. CIOの内部不正は防げるか？

HITACHI
Inspire the Next

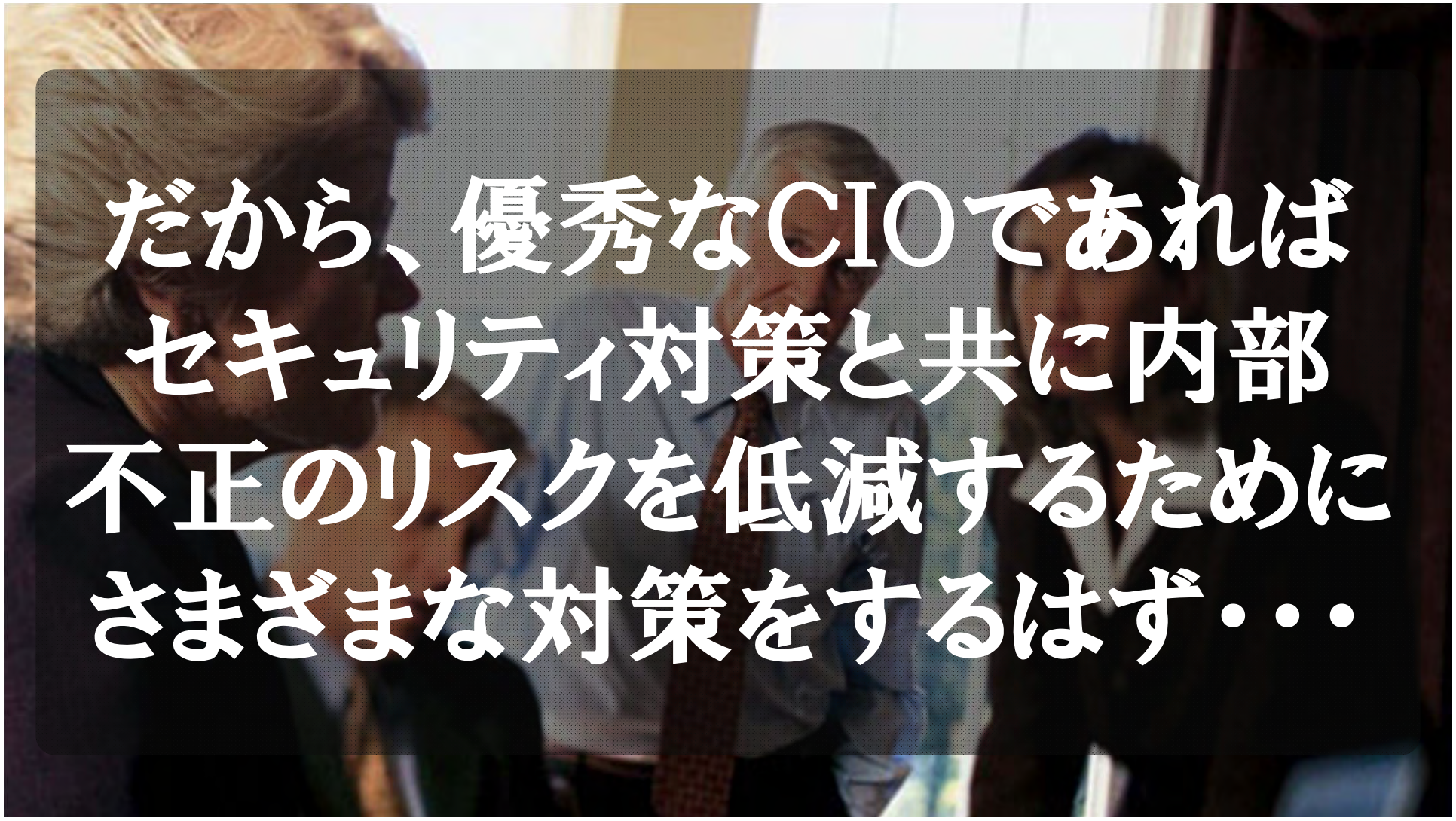
CIO【Chief Infomation Officer】：最高情報責任者

CIOとは、企業内の情報システムや情報の流通を統括する担当役員。
「最高情報責任者」「情報統括役員」などと訳される、企業の情報戦略のトップである。元は米国の企業で用いられていた呼び名だが、情報戦略に注目が集まるにつれて日本でも採用する企業が増えつつある。情報システムの構築や運営に関する技術的な能力だけでなく、そうして得られた情報を基にCEO（最高経営責任者）ら経営陣に対して適切な報告・助言を行うことも求められ、経営戦略に関する深い理解と能力も必要とされている。

【出典】IT用語辞典：e-word

経営視点からITの最高責任を持つ役員

（1990年あたりに米国では役割も定まる。驚くことに米国のCIOはIT部門出身は既に少数派らしい・・・）


だから、優秀なCIOであれば
セキュリティ対策と共に内部
不正のリスクを低減するために
さまざまな対策をするはず・・・

3. CIOの内部不正は防げるか？

HITACHI
Inspire the Next

内部犯行の低減するためのポイントにも詳しく・・・。

1. TBPのポリシーと処理手順を理解すること
2. アクセスが許可されたIPをモニターすること
3. アクセス権限を管理すること
4. TBPの人事ポリシーと処理手順を理解すること
5. 職場で起こるネガティブな問題点を予測し、管理すること
6. アクセス権限を削除した際、システム上でも確実に実施すること
7. 責務の分離も強化すること
8. 情報を保護する責任がTBPにもあることを、明確に契約に記述すること

※ＴＢＰ：委託先の業者やコンサルタントなど

【出典】IPA：組織内部者の不正行為によるインシデント調査

3. CIOの内部不正は防げるか？

HITACHI
Inspire the Next

内部犯行予防策の５分類も実践できてしまう！
（25の対策）

犯行を難しくする	捕まるリスクを高める	犯行の見返りを減らす	犯行の挑発を減らす	犯罪を容認する言い訳を許さない
犯行対象を防御的に強化する	監視者を増やす	標的を隠す	欲求不満やストレスを減らす	規制を決める
施設への出入りを制限する	自然監視を補佐する	対象を排除する	対立を避ける	指示を掲示する
出口で検査をする	匿名性を減らす	所有物を特定する	感情の高ぶりを抑える	良心的に警告する
犯罪者をそらす	現場管理者の利用	市場を阻止する	仲間からの圧力を緩和する	遵守を補佐する
道具や対抗手段を制御する	フォーマルな監視体制を強化する	利益を否定する	模倣班を阻止する	薬物・アルコールを規制する

【出典】IPA：組織内部者の不正行為によるインシデント調査　状況的犯罪予防（ITセキュリティ対策版）

3. CIOの内部不正は防げるか？

HITACHI
Inspire the Next

もちろん、IPA作成の
組織における内部不正
防止ガイドラインも熟読
しているだろうし・・・

宣伝です！

3. CIOの内部不正は防げるか？

HITACHI
Inspire the Next

多彩な論点で内部不正について語っている良書なんかも読んでしまう。

あからさまな宣伝です！
（買ってね）

だから、万全です


ということには，なかなかならないと思います

3. CIOの内部不正は防げるか？

HITACHI
Inspire the Next

従業員の内部不正より様々な権限が集中する
責任者の対策は、はるかに範囲が広く大変だから！

外部攻撃 ＜ 内部不正 ＜ CIOの内部不正

HITACHI
Inspire the Next

問題①

アクセス制限/特権ID

3. CIOの内部不正は防げるか？

HITACHI
Inspire the Next

【アクセス制御】

- ユーザID/パスワード以外の要素も組み合わせる（多要素制御）
- 職務分掌に基づき必要な権限のみを厳密に付与（職務分掌）

【特権ID管理】

- 一般ユーザと同様にOSとは独立した特権的IDの制御（特権の制御）
- 特権IDを有する個人を特定する仕組み（ログイン制御）

これらの厳密な対策をしたとしても・・・。

CIOは別格（？）

HITACHI
Inspire the Next

問題②

離職の問題


内部不正と離職は、
ものすごくなかよし！

3. CIOの内部不正は防げるか？

HITACHI
Inspire the Next

具体例① 海外鉄鋼大手P社への国内鉄鋼大手の技術流出

方向性電磁鋼板と呼ばれる高機能鋼板の製造技術を元従業員が、海外の競合企業へ流出させる。

1,000億円の損害賠償訴訟の事案

技術情報を持ち出した後に計画的に離職

3. CIOの内部不正は防げるか？

HITACHI
Inspire the Next

具体例② 国内大手プレス機械メーカの技術情報流出

図面データ258点を元従業員が、競合関係にある中国企業へ機密情報を流出させる。

出典：近事の技術流出事例への対処と技術流出の実態調査について（経済産業省　知的財産政策室）

競合企業の関連会社の役員に就任するために離職


まさか、CIOが離職する可能性は低い？

3. CIOの内部不正は防げるか？

HITACHI
Inspire the Next

海外のCIOの平均的な在職期間

米国：約24ヶ月程度
英国：約38ヶ月程度

米国：ＥＤＳ調査による/英国ＦＴＳＥ350企業が対象
海外ＣＮＥＴニュース(2007年8月)

海外では2～3年でCIOが交代する

（一般に雇用の流動性が高いとされる中国の平均在籍期間でも34ヶ月〈LinkdIn調べ〉）

3. CIOの内部不正は防げるか？

HITACHI
Inspire the Next

日本のCIOの平均在職期間

5年4ヶ月

（CIO Magazine Online 2012年読者アンケート）

それは
海外の話で
日本では
違うよね？

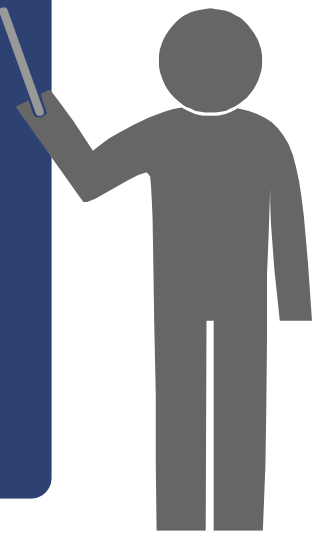

意外と短期間！
ＣＩＯであっても人間。悪意をもって事前に周到に準備されて
離職後の対策を事前に
施すことは非常に難しい
短期間で辞めちゃうなら、なおさらね・・・。

HITACHI
Inspire the Next

4. まとめ

HITACHI
Inspire the Next

内部不正は、システムよりも
脆弱な人間の対策。
だから、絶対的な対策を
することは非常に難しい。
（抑止と予兆検知は、対策として有効性がある）



4. まとめ

HITACHI
Inspire the Next

ただ、内部不正対策を

「従業員の不正に対処する」

と言うと、監視されているようで誰しも気持ちがよくない。

「従業員を守るために備える」

と言えば、前向きに聴こえる！

HITACHI
Inspire the Next

内部不正対策に最も重要なことは？

「対策は非常に難しい」で終わるとまずかろうと、無理にまとめた訳ではありません・・・。


最高の内部不正対策は
人に愛情も持って接すること？
こういう意識を常に持つ
ことが実はもっとも重要
（かもしれません）

HITACHI
Inspire the Next

END

内部不正はセキュリティ製品で防げるか？
～CIOの内部不正という極論で考えてみる対策の効果～

株式会社 日立ソリューションズ
武田　一城

HITACHI

Inspire the Next