「セキュリティの本質」とは何か？

～ 書籍の趣意、WG紹介を兼ねて ～

組織で働く人間が引き起こす不正・事故対応WG
甘利 康文
（セコム(株)IS研究所）

組織で働く人間が引き起こす不正・事故対応WG


JNSA PRESS

JNSA ワーキンググループ紹介

組織で働く人間が引き起こす不正・事故対応 WG

WG リーダー　セコム株式会社　甘利　康文

「組織で働く人間が引き起こす不正・事故対応 WG」は、JNSA の WG の中でも新しい（昨年 7 月発足）、

情報セキュリティ分野では、人による情報漏洩が話題になり、多くのベンダーから、技術的にその対策を

活動目的（2012/7 発足時）

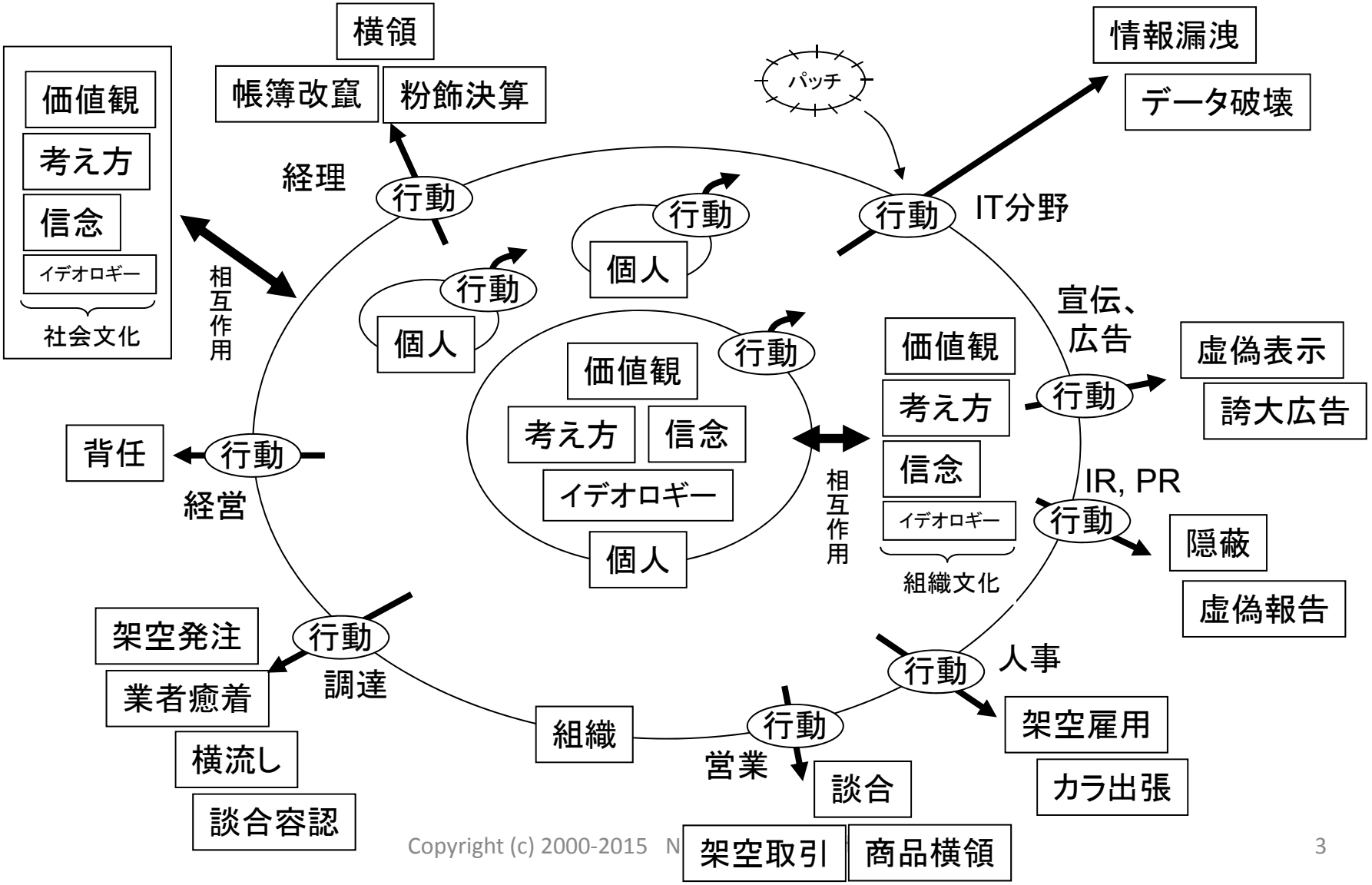
組織で働く人間が引き起こす事故、すなわち意図を持った「内部不正」と、意図のない「ヒューマンエラー」を対象として、これらの「内部不正・事故」の防止／抑止方法論を具体的にまとめること

http://www.jnsa.org/jnsapress/vol35/4_WG.pdf

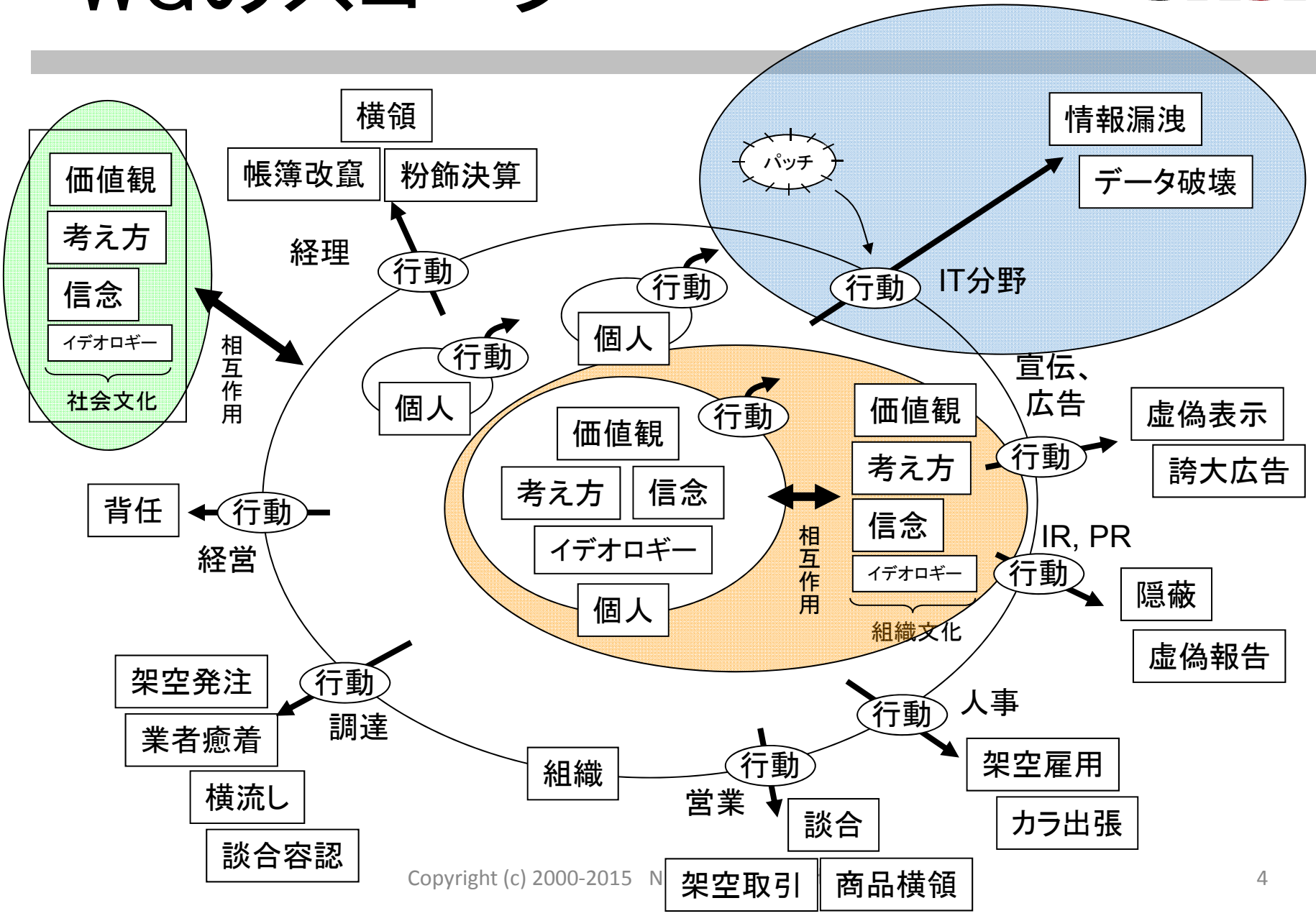
「内部不正・事故」の対象想定：
使い込み、内部窃盗、不正経理、取引先等との癒着、意図的不作為・隠蔽、カルテル、組織の私物化（公私混同）、ハラスメント、ヒューマンエラーなど、組織で働く人間が引き起こす違法（脱法）行為、ルール違反全般（システムからの情報漏洩などのIT分野に限りません）

不正発生モデル（JNSA内部不正対応WG）

（出典）甘利康文: 組織で働く人間が引き起こす不正・事故対応WG, JNSA Press, Vol.35, pp.6-7 (2013)



WGのスコープ



WGの活動目的

以下の3方向から「組織で働く人間が引き起こす不正・事故」に対する考察を深め、ソリューションの提言、提案を行うことを目的とする。

(1) 人の意識や組織文化、
(2) 組織の行動が影響を受ける社会文化や規範、
(3) 不正を防ぐシステム

内部不正対策 14の論点

オンデマンド (ペーパーバック):　232ページ
出版社: インプレスR&D (2015/6/5)
ISBN-10: 4802090056
ISBN-13: 978-4802090056

第1部 セキュリティの本質

セキュリティが守るべきもの(甘利(セコム))

1. 「組織のオペレーションを守る」のがセキュリティ
2. 防犯や、情報セキュリティ対策もその一環
3. 働く人を守る
4. 罪による統制と、恥による統制

第2部 情報セキュリティ

内部不正はセキュリティ製品で防げるか（武田（日立ソリューションズ））

これまで、各組織が情報セキュリティ対策として導入している各製品が内部不正の対策の観点からその有効性とそれらの効果的な利用方法を提示・解説

内部不正と情報漏えい対策（塚田（日立ソリューションズ））

情報セキュリティ対策の考え方と段階的導入についての概観、解説

情報セキュリティ事件にみる温故知新（山岸）

日本の「コンピュータ犯罪史」を振り返る　（日本情報経済社会推進協会JIPDEC）

情報漏えいの事後処理（山田（DIT））

インシデント対応とフォレンジックについて解説

第3部 組織行動と社会規範

職場環境の整備で防ぐ内部不正(島(NEC))

職場におけるどの環境条件が内部不正に関係するかについての統計分析

「内部不正防止ガイドライン」を活用した組織横断的対策(益子(IPA))

IPAが公表している内部不正防止ガイドラインを活用する方法について解説

内部不正から企業を守る法制度(宮内(五番町法律事務所))

内部不正から組織を守るための法制度を解説

内部不正の原因と対策に関する考察(野津(大日本印刷))

印刷産業を例に「不正のトライアングル」と組織文化による抑制について考察

個人情報保護と営業秘密管理の動向(小川(みずほ情報総研))

個人情報と営業秘密の取り扱いに関する世の中の動向を解説

第4部 人の意識と組織文化

環境犯罪学からのアプローチ(高木(東大))

街づくりや社会の防犯で使われる「環境犯罪学」を、内部不正に応用する手法を解説

内部不正抑制に応用できる犯罪理論(甘利(セコム))

内部不正抑制に適用出来る、各種の犯罪・防犯理論について紹介

状況的犯罪予防論による内部不正・事故抑制手法(甘利(セコム))

犯罪抑制のための各種防犯理論を、内部不正対策に活用するための提言

組織文化に基づいた内部不正・事故抑制手法(甘利(セコム))

働く人間に対する職場のあり方という観点から組織論的な内部不正対策について提言

セキュリティの本質とは？

世の中の（食糧やエネルギー供給、情報セキュリティまで含めた）すべてのケースを包括した形で、セキュリティを一般化して考える．．．

セキュリティの（上位概念的）定義†

> オペレーション（日々の営み）が、運営主体によってあらかじめ定められたプランに則って運営され、理由の如何によらず、それが阻害されないこと

オペレーションを阻害する何らかの要因

→ インシデント

（オペレーションのホメオスタシスを維持すること）

† 甘利康文：セキュリティの上位概念的考え方について，信学技報Vol.105, No.687, pp.5-8 (2006)

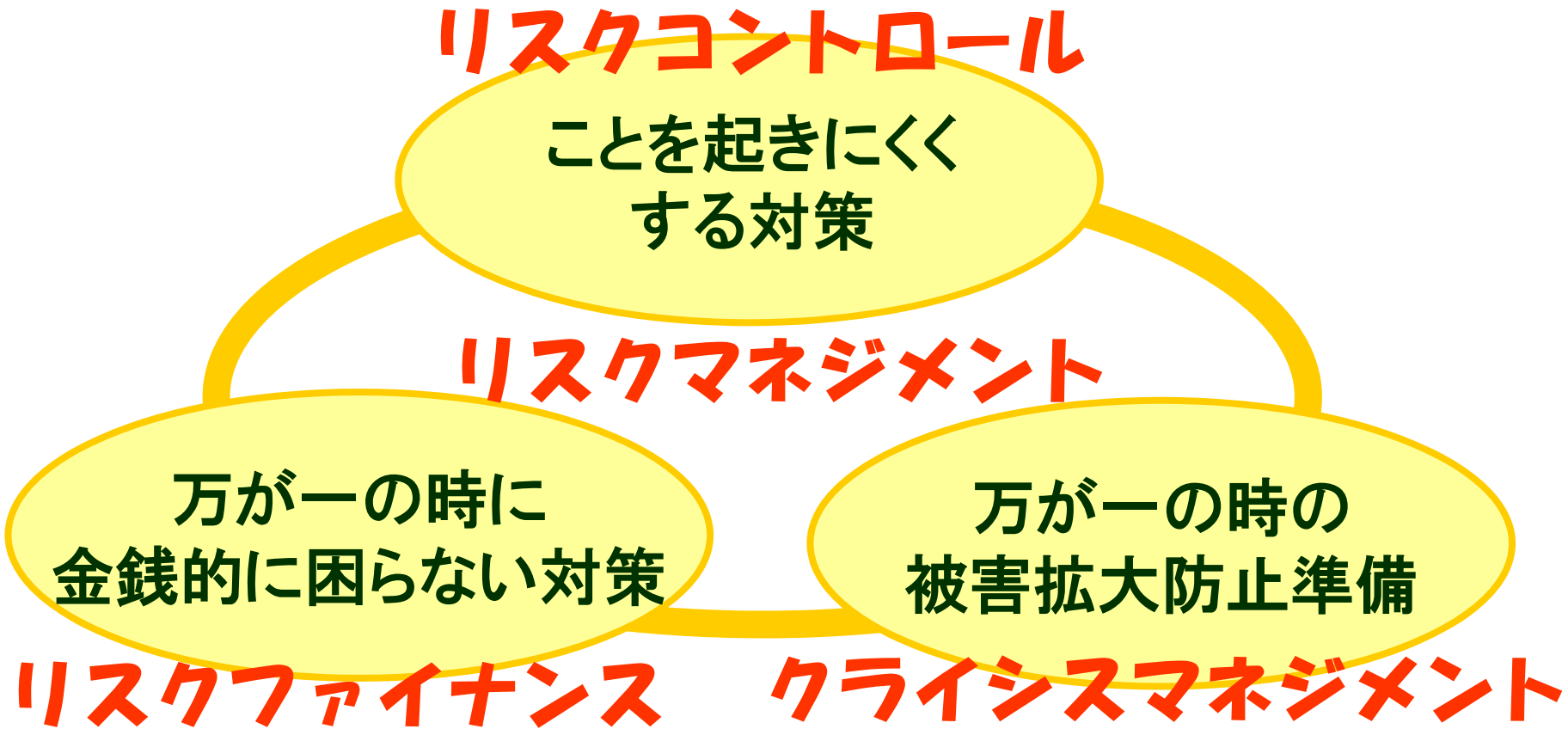
セキュリティを実現するステップ

オペレーションが、運営主体によってあらかじめ定められたプランに則って運営され、理由の如何によらず、それが阻害されないこと

1. 運営主体、対象オペレーション（営み）の明確化
2. オペレーションプラン
3. プラン遂行に必要なリソースプロパティの網羅的洗い出し
4. リソースプロパティの阻害要因（インシデント）の網羅的洗い出し
5. リスクマネジメントの観点からの阻害要因の影響の出来るだけの排除

リスクマネジメントの３要素†

インシデントの影響を最小化するための3つのアプローチ



†甘利康文：セキュリティの基本的考え方とリスクマネジメントの関係について，信学技報Vol.104, No.528, pp.17-20 (2004)

おわりに

セキュリティを考えるうえにおいて、最も重要な守るべき対象は、その組織の“オペレーション”

ご清聴ありがとうございました。