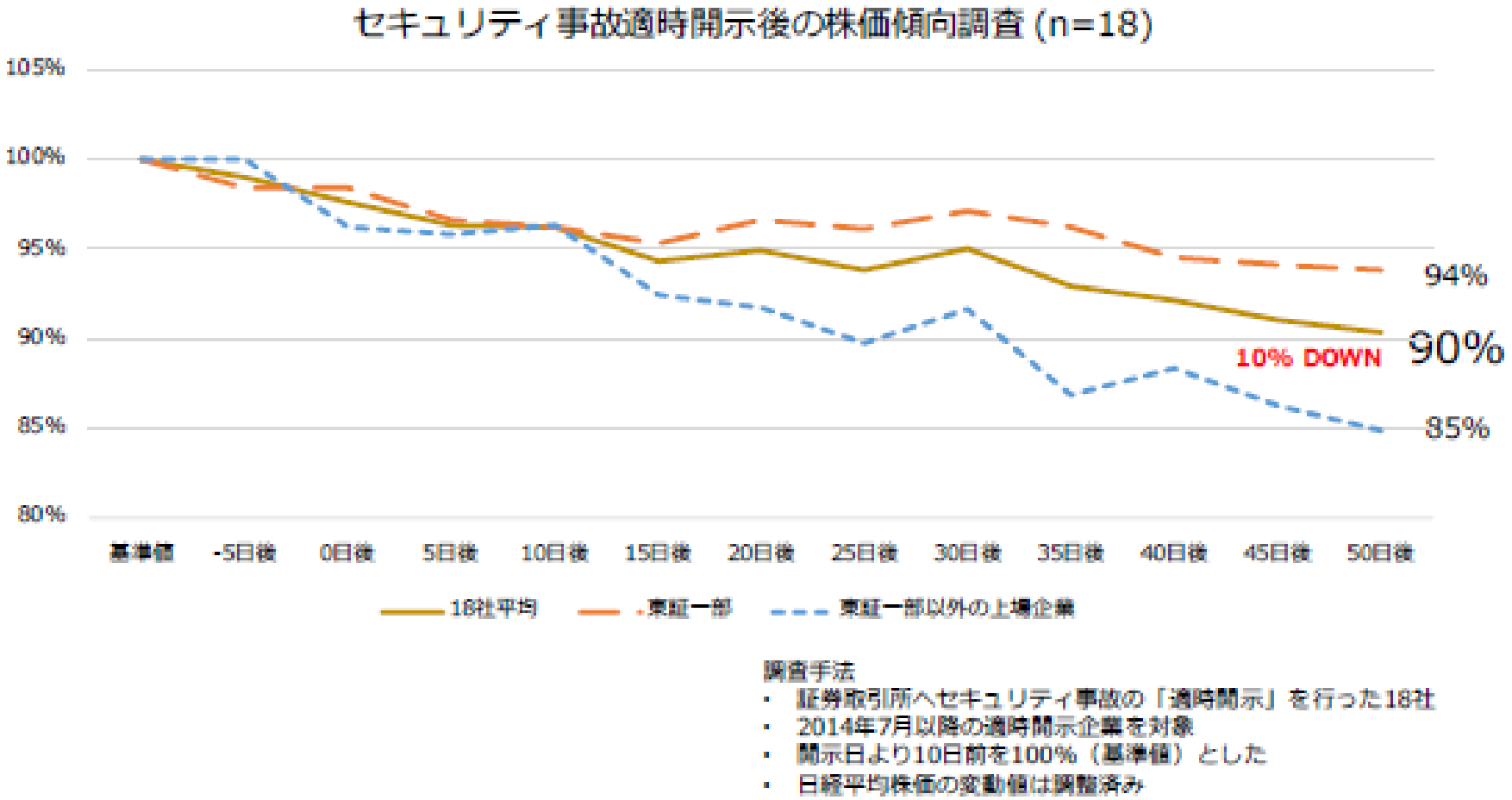
資料７－３

セキュリティ対策の情報開示に係るインセンティブについて

総務省　サイバーセキュリティ統括官室

セキュリティ事故と株価や企業業績への影響

- 日本国内で情報流出等の適時開示を行った企業の調査によれば、適時開示後５０日後には株価が平均１０％下落した。
- このうち、東証一部以外の企業では平均下落率は１５％であることから、セキュリティ事故は中小企業への株価の影響が大きいと考えられる。



（出典）JCIC「取締役会で議論するためのサイバーリスクの数値化モデル　～サイバーリスクの金額換算に関する調査～」（平成30年９月）

セキュリティ対策の開示目的の類型化（想定）

■ 企業の直接的な開示目的としては、①顧客との安定的な取引関係の維持、②販売促進と製品・サービスの差異化、③インシデントや不祥事からの信頼回復、④経営改善などが考えられる。

■ また、ステークホルダーとの関係で情報開示の質を向上させていく流れの中で、開示が可能になる程度までセキュリティ対策そのものの質やレベルも向上させていくという派生的な開示目的も考えられる。

開示企業

派生的な開示目的

セキュリティ対策の質やレベル向上

対策の好循環

直接的な開示目的

セキュリティ対策情報開示

顧客との安定的な取引関係の維持	販売促進と製品・サービスの差異化	インシデントや不祥事からの信頼回復	経営改善	…
サプライチェーン上の取引先に対して、セキュリティ要求事項の遵守姿勢・状況をアピール	セキュリティの視点から自社のブランド価値を高め、株主・投資家、顧客に対して、自社製品・サービスのセキュリティレベルの高さをアピール	株主・投資家等に対して、再発防止策をアピール	株主・投資家に対して、セキュリティ対策費用の高騰抑制による適切な利益管理をアピール	

ステークホルダー

受発注への影響　　株価への影響

ステークホルダーにもたらす影響

開示側へのヒアリング（概要）

（1）対象企業

- ✓ 日経225の企業のうち、①セキュリティ対策の情報開示が全般的に進んでいる業界の企業、及び②セキュリティ対策の情報開示が全体としてあまり進んでいない業界の中で特に開示が進んでいる企業を中心にヒアリングを実施。

（2）目的

- ✓ 実際に開示を行っている企業に対してヒアリングを行うことにより、現時点での企業の開示に対するモチベーションやインセンティブを明らかにする。

（3）質問項目

- ✓ なぜセキュリティ対策の情報開示を進めようと考えていますか（又は考えていないか）？
- ✓ セキュリティ対策の開示を行って良かったことはありますか？
- ✓ 同業他社の開示動向は把握していますか？自社の開示又は対策の参考にしていますか？
- ✓ セキュリティ対策の情報開示に対して経営層は関与していますか？
- ✓ 御社自身のセキュリティ対策の情報開示に関してどのような課題を感じていますか？

開示側へのヒアリング結果【暫定版】

質問事項	A社（※※※※）	B社（※※※※）	C社（※※※※）
なぜセキュリティ対策の情報開示を進めようと考えているか（又は考えていないか）？	✓**自社のセキュリティ対策の取組のレベルが上がり、外部へのアピール材料が揃ってきた**ので、**情報開示を今後どのように進めていくべきかについて、環境・社会貢献・PR・IR担当の役員と相談しながら決めていく段階**に入った。 ✓サイバーセキュリティ対策に真剣に取り組むことが、**お客さまの信頼を獲得し、企業価値の向上につながる**と考え、**取組自体の充実と一定レベルでの公表という方針を、経営層によるリスクマネジメント委員会において合意**した。 ✓また、業務委託先がインシデントを起こすケースが後を絶たない中で、**自らの対策内容を開示することで、業務委託先のメーカやテナントにもチェックがかかるように**していき、**当社と同等のレベルにまで対策レベルを引き上げていきたい**という考えもある。	✓当社はITに関するレポートを公表しているが、想定読者として株主・投資家をメインターゲットとしており、**※※※※に選ばれる**ということを重視している。 ✓攻めのITとして事業のIT化の取組を行っており、本業である※※※※を支えるインフラとしてのITについて知ってもらうことも目的の一つである。 ✓（就職を控えた）学生に※※※※以外の当社の取り組みについて知ってもらうことも目的の一つであり、あまり堅苦しい冊子にならないようにしている。 ✓セキュリティ対策はあくまで自衛のためという位置づけであり、今のところの**開示の目的のメインはITの利活用のアピール。** ✓経営トップのマインドとしては、**情報セキュリティをマネジメントにおける重要事項の一つとして認識しているが、開示については特に意識はしていない。**	✓**お客様に安心してお付き合い頂く**ためにも情報セキュリティ対策の取組をしっかり開示することが重要だと考えている。 ✓また、社内の営業SEにおいては、これまで社内における情報セキュリティ対策の取組を断片的にしか見ることができなかったが、**情報セキュリティ報告書を通じて、自社の取組への理解が深まる**とともに、情報セキュリティ報告書が網羅的に取組が記載されていることから、お客さまの要請に対して情報セキュリティ報告書を見せて説明するなど標準的な**販促・営業ツール**としての活用もできている。

開示側へのヒアリング結果【暫定版】

質問事項	A社（※※※※）	B社（※※※※）	C社（※※※※）
セキュリティ対策の開示を行って良かったことはありますか？	✓セキュリティ対策の開示はまさにこれからである。	✓※※※※におけるIoTの導入・活用が進展しており、その際にセキュリティの裏付けがあると、**信頼性や安心感という点において説得力が増す**のではないかと考えている。	✓特に情報セキュリティ報告書は**販売活動に実際に役立っており、**今後も継続して作成・公表をしていきたいと考えている。
同業他社の開示動向は把握していますか？自社の開示又は対策の参考にしていますか？	✓社内で勉強会を開催して、**※※※※をケーススタディとして、開示のメリットやデメリットについて勉強**し、参考にしている。開示のメリットとしては、**お客さまの信頼を獲得することが大きい**と見ている。 ✓インシデント発生時の情報共有については、※※※※や、**※※※※の事例**を参考にして、そこから得られるヒントがあった。	✓他社の開示動向については多少調査を行ったが、あまり意識はしていない。 ✓**※※※※の社員の方に社外取締役をお願い**していることもあり、**※※※※の※※※※報告書**は参考にした。 ✓内容や記載方法の面で最も参考にしたのは**※※※※の報告書**である。当社は、IT製品・サービスの提供を本業とする企業ではないので、**本業における ITの利活用という点において**参考にした。	✓※※※※や※※※※とは、日々のセキュリティ上の課題にどのように取り組んでいるかについて、普段から意見交換を行っており、**情報セキュリティ報告書についてもお互いのものを確認しながら作成を進めている**ので、書きぶりが少し異なるが、ほぼ同じ内容が記載されている。

開示側へのヒアリング結果【暫定版】

質問事項	A社（※※※※）	B社（※※※※）	C社（※※※※）
セキュリティ対策の情報開示に対して経営層は関与していますか？	✓**経営層によるリスクマネジメント委員会において、ITリスク**や雇用の問題**への対応について本格的に検討**し、対策に取り組んできており、その**成果の公表についても、リスクマネジメント委員会の総意として賛同**を得ている。	✓経営トップが情報セキュリティを経営課題として位置づけている。CISOには役員を任命している。 ✓グループ情報セキュリティ委員会を含むガバナンス体制を構築している。 ✓**情報開示を行うようになったきっかけは、軽微なインシデントの発生**であり、インシデントの発生後に実施した**対策の一つとして、※※※※-SIRTの設立**がある。 ✓なお、IT 委員会は以前から存在していた。	✓情報セキュリティ報告書は**CISOの承認のもとで公表**される。副社長やCISOに対し、経営システム本部が説明をしており、内容は見ているが、細かい文章までは確認していない。CXOは社長が全権委任した者で全責任を負っているため、CISOの承認は社長の承認にもなる。

開示側へのヒアリング結果【暫定版】

質問事項	A社（※※※※）	B社（※※※※）	C社（※※※※）
御社自身のセキュリティ対策の情報開示に関してどのような課題を感じていますか？	✓**直近に策定したグループ統一ポリシーをもとに、規程類を整備し、グループ各社との調整を行っている**が、守れているところとそうでないところがある。**足並みが揃っていない状態でそれを公表すれば、信頼を失うことに繋がりかねないため、開示に対しては慎重な対応が必要**と考えている。 ✓グループ内の企業によっては、規程において例外的な項目を設けている場合があり、調整に難航している。特に海外のグループ会社の場合は、アセアン諸国を中心として、厳格な法律対応が求められるため、訴訟リスクについて考えておかないといけない。 ✓**どこまで調整が出来ていれば、グループ内全社で実施していると言えるのか、グループの規程として公表できるのかといった部分については、判断が難しい。**	✓セキュリティ対策の情報開示について**株主から指摘を受けたことはない。** ✓定量的な数値を記載することは考えているが、情報セキュリティの場合、**数値によってはセキュリティ対策を実施していないこと、あるいは、どこにセキュリティ上の弱点があるかがわかってしまうケースがある**のでなかなか難しい。 ✓取引先からは、個人情報保護対策について求められることはある。GDPRの影響もあるのではないか。契約書に個人情報保護対策について記載することでOKとしている。	✓20※※年※月に最初の情報セキュリティ報告書を公表したが、**情報セキュリティ報告書の作成には、かなりのマンパワーを要する**ことから、当初は公表のタイミングは隔年ごととした（ただしその後毎年公表することに方針に変更）。 ✓**どこまで公開してもよいかどうかの判断**が難しい。**他社の開示内容もみて、それと比較しながら、チェックし、関連部門と調整**している。 ✓当社は常に攻撃ターゲットに晒されているため、対策についても、例えば、ログの統合管理についてもどのようなインテリジェンスをもとに、どのような脅威のハンティングを行っているかまでは言わないよう、**記載のレベルはある程度のレベルにとどめて**いる。