

利用部会主催セミナー in 名古屋

他人事ではすまされない、セキュリティ事情 2014

～つながる時代のセキュリティ対策～

■ 主催:

JSSEC利用部会

■ 協力:

株式会社 トヨタデジタルクルーズ
中部アイティ共同組合

2014年10月24日

一般社団法人

日本スマートフォンセキュリティ協会

理事 事務局長 西本 逸郎

JSSECについて

一般社団法人日本スマートフォンセキュリティ協会（JSSEC）とは

個人を中心に急激に普及しているスマートフォンやタブレット型端末（以降スマートフォン）は、企業や団体でも業務効率化・生産性向上、ならびに新しい事業基盤の中核ツールとしても大きな期待を寄せられています。

しかし、不適切な利用やセキュリティ上の不備、悪意ある行為などにより利用者や事業者へ悪影響などを警戒するあまり、有効活用への機会を逸することが危惧されています。

そのため、通信キャリア、機器メーカ、システムインテグレータ、アプリケーション開発、サービス提供ベンダなどの提供者だけではなく利用企業ならびに関連団体などが協調し、スマートフォンの安全な利活用を図り普及を促進するために、2011年5月25日に任意団体としてスタートし、2012年4月1日より一般社団法人として活動している団体です。

目的

- ・企業・団体における利用者が安心して高度なサービスを受けられるようにする。
- ・実装すべきセキュリティレベルの理解を社会に浸透させ、提供者が安心して事業推進を行えるようにする。
- ・利用者のセキュリティリテラシー向上のための活動も行い、さらに高度なサービスを受けられるようにする。
- ・セキュリティを切り口とした「信頼できるニッポン！」を確立しグローバル市場へアピールする。

日本スマートフォンセキュリティ協会 JSSEC

「第一回スマートフォン“企業利用”実態調査」を開始

実態調査の概要

調査目的

スマートフォンの企業利用のトレンドを掴み、ニーズを把握し、スマートフォンの導入を検討されている企業、本格的なビジネスシーンでの利用を計画されている企業に役立つ調査報告の提供をすることで、スマートフォンの普及促進に貢献する。

調査内容

スマートフォン利用段階を4つのライフサイクル(計画、導入、利用、運用)に分類。訪問調査は約50問

回答対象者

スマートフォンの企業利用を検討・導入されている、情報システム部署責任者、ITインフラ運用責任者、運用担当者

調査実施期間

2012年10月28日(火)～2012年10月31日(水)

回答方法

以下のアンケートページにアクセスしていただき、直接入力をお願いします。

[＜アンケートページへ＞](#)

統計結果は後日、ご報告いたします。

※寄せいただいたご意見は、個人情報を除き、全て公開される可能性があります。

本人等の財産権等を侵害する恐れがある場合は該当箇所を伏せるなどの配慮をします。

※調査についてのお問合せ先: JSSEC事務局(sec@jssec.org)

スマートフォンの業務利用におけるクラウド活用ガイド

～日本のスマートフォンとビジネスマン達の輝ける未来のために～

【β版】

スマートデバイスの堅牢化ガイド

β版

2012年6月5日

日本スマートフォンセキュリティ
技術部会 デバイスワーキンググループ 発表

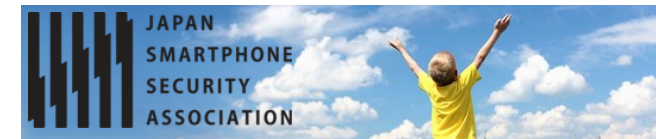
本書では、OSの設計方針に反する不正なアプリケーションも、OSやアプリケーションが設計意図通りに動作する。これは、ユーザーの故意や不注意によって引き起こされることがあり、デバイスの堅牢化において注目すべき

スマートフォンネットワークセキュリティ実装ガイド

～スマートフォンの業務利用における安全なネットワーク利用のために～

【第一版】

2012年12月1日



JSSEC

MDM導入・運用検討ガイド

～スマートフォンの適切なセキュリティ管理のために～

【第1版】

平成25年1月24日

Android アプリのセキュア設計 セキュアコーディングガイド

【みんなでスマホが安全に使える世界へ!】



2012年11月1日版

日本スマートフォンセキュリティ協会 (JSSEC)

スマートフォン&タブレットの業務利用に関するセキュリティガイドライン

～その特性を活かしたワークスタイル変革のために～

【第一版 (BYOD 基礎資料収録版)】

Security Guideline for using Smartphones and Tablets

- Advantages for work style innovation -

[Version 1]

BYODの現状と特性

～あなたの組織はどのパターンですか～

December

an Smartphone
Utilization Con

2012年10月26日

日本スマートフォンセキュリティ協会 (JSSEC)
利用部会 ガイドラインワーキンググループ
BYODタスクフォース

会員 募集中:

幹事会員: 33社(24万円/年)

正会員: 94社(6万円/年)

幹事会員: 運営や企画に参加。

正会員: すべての活動に参加。

日本を代表する多くの方と一緒に、
活動しませんか？

サービス提供者、利用者ともに、
メリットのある活動をしています。



わたし



にし もと いっ ろう
西 本 逸 郎

CISSP

昭和33年
昭和59年3月
昭和59年4月
昭和61年10月

福岡県北九州市生まれ
熊本大学工学部土木工学科中退
情報技術開発株式会社入社
株式会社ラック入社

ブログ どうらいつ

@dry2

検索

プログラマーとして数多くの情報通信技術システムの開発や企画を担当。2000年より、情報通信技術のさらなる利活用を支えるため、サイバーセキュリティ分野にて新たな脅威への研究や対策に邁進。

わかりやすさをモットーに、サイバーセキュリティ対策の観点で、官庁や公益法人、企業、大学、各種イベントやセミナーなどでの講演や新聞・雑誌などへの寄稿、テレビやラジオなどでコメントなど多数実施。

株式会社ラック 取締役 CTO サイバー・グリッド・ジャパン GM
サイバー救急センター 調査員
一般社団法人 日本スマートフォンセキュリティ協会 理事、事務局長
特定非営利活動法人 日本ネットワークセキュリティ協会 理事
データベースセキュリティコンソーシアム 理事、事務局長
セキュリティキャンプ実施協議会 事務局長

2009年度情報化月間 総務省 情報通信国際戦略局長表彰
2013年情報セキュリティ文化賞

内閣官房 情報セキュリティ政策会議普及啓発・人材育成専門委員会 歴任
総務省 スマートフォン・クラウドセキュリティ研究会 歴任
経済産業省 サイバーセキュリティと経済 研究会 歴任
警察庁 総合セキュリティ対策会議 委員

産業技術大学院大学 運営諮問委員



国・企業・メディアが決して語らない
サイバー戦争の真実

著者：西本逸郎・三好尊信
定価：1,050 円(税込)
ページ数：208
初版発行：2012-02
ISBN：978-4-8061-4293-5

2011年7月に、米国防省が「サイバー攻撃は戦争行為だ」との見解を表明し、サイバー空間は陸・海・空・宇宙に続く第5の戦場として規定されました。本書は、現在のサイバー空間を取り巻く環境を紹介し、世界各国や大企業の攻防から私達個人のセキュリティまでをわかりやすく解説します。

日本経済新聞社「いますぐはじめる サイバー護身術 なりすまし、不正アクセス…どう防ぐ？」(日経e新書)

1. 現状理解

→ 今起きていることを理解して取り組む

① 今って

スマート時代
あらゆる機器と
人が繋がる
IoT → IoTへ

大人も子供も
技術・用心ともに
未熟のまま暴走!

危なっかしい。

「やらかし」含め
どう、考えます?



② システムの状況変化

もともと、IT化は「合理化」が目的

「合理化」へ、リスクへの考慮はありえない。ましてやセキュリティ対策も。必要ない。

合理化なので、余計なことは考えない。

ところが、つながる時代になり、合理化システムが結合し、今まで見向きもされなかった、「データ」に脚光が！

ITシステムが価値を生み出すか。若しくは経営や事業を行う時代へ。

昨日 (20世紀) は「機能」の時代。

今は「データ」の時代。

「データ経営」 「機械経営」



③ 「天動説」から「地動説」へ

シャドウITやBYODってご存知ですか？
(影の情報システム)とも呼ばれている。

「天動説」自身のシステムが世界の中心
現在、「社会がIT化」している。社会のIT装置化。IT社会ではなく、「社会IT」の誕生でもある。つまり、社会や個人側のIT活用的一般化。

BYODなど、裏に隠れて勝手に使われる情報システム

課題は、社会ITに存在している従業員活用と、自身の社会ITへの参画となる。

「地動説」では、
「社会IT」への適応が鍵となる。



④ スマート時代の潮流

社会のIT化に適応する。

1) スマホは基本的に「社会ITへの窓」

2) 「社会ITへの窓」の社内利用とは？



(1) 社会ITの従業員 → ワークスタイル・ライフスタイル・多様性
社内システムを社会ITへの限定公開？

(2) 社会ITの活用 → 脱ガラパゴスシステム
社内システムを止めて社会ITを活用。

所謂、クラウドやSNSなどの利用、ビッグデータ活用

(3) 社会ITへ展開 → 事業展開

社内システムを社会ITに接続する。社会ITの一員として。

会社としてまずはどういう方針なのかを決める。

すると、スマホを含めたセキュリティ方針を決めることが出来る。

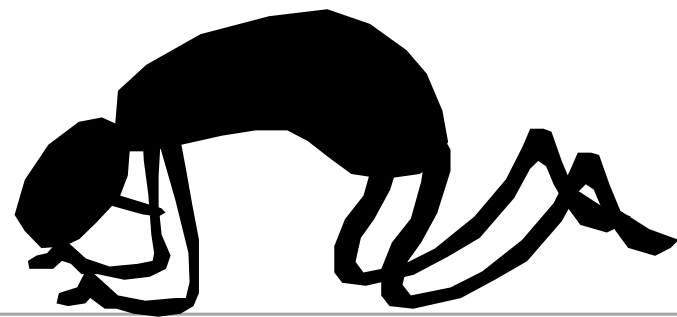
⑤ スマート時代の潮流

さらにウェアラブル

ウェアラブルで健康管理など
スマホ持込禁止はほとんど不可能？

基本的人権の侵害など、訴訟になる
可能性すらある。

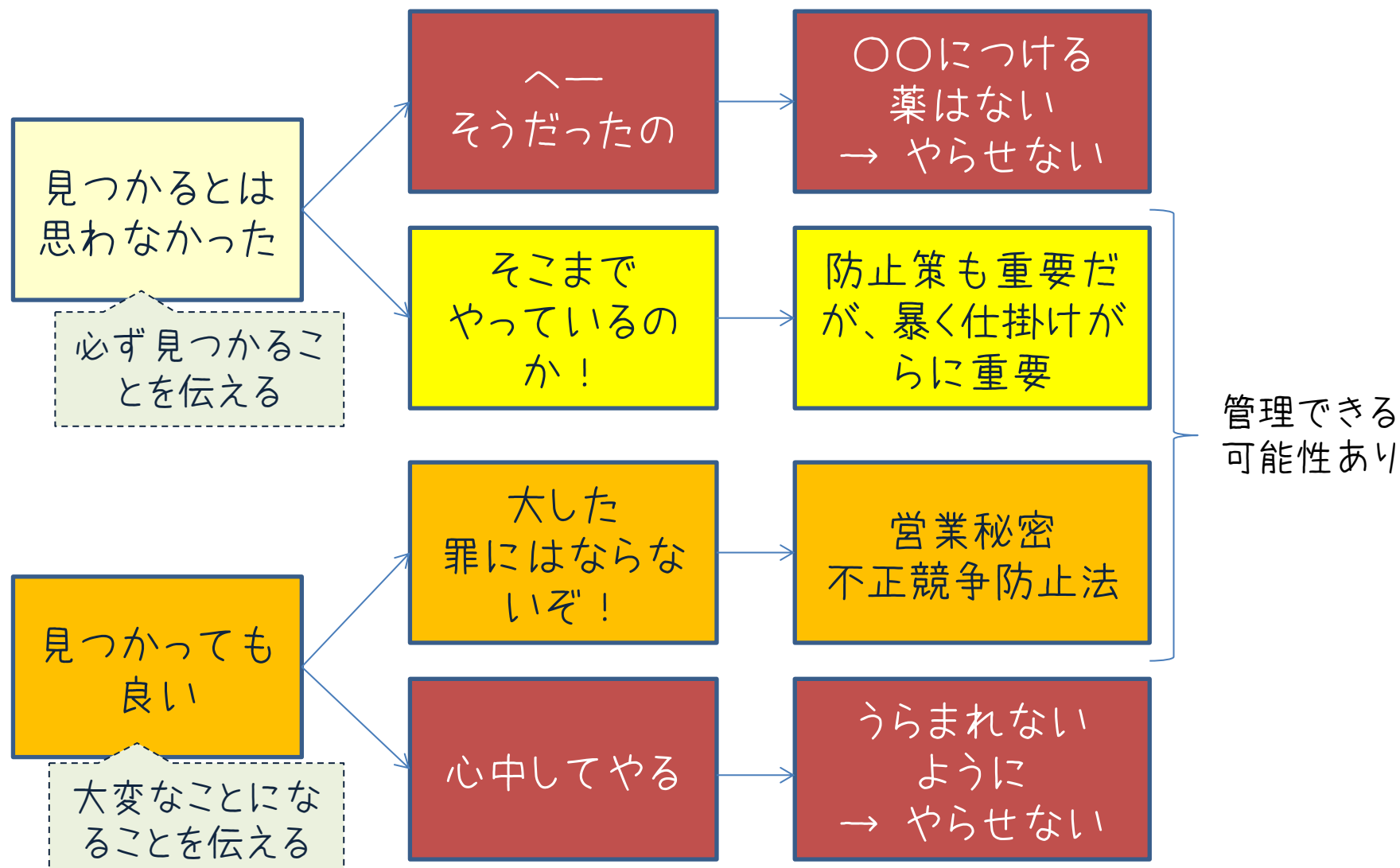
あいたたた



⑥ 内部犯行への考慮

教訓

個人情報保護法と営業秘密指定の抱き合わせが必須となる。



2. 脅威と騒がれているが

→ スマホの現実的な脅威は？ 煽りすぎ？

① 隠れた脅威

1) アプリ

危険度の測定 = 利用機能 × 配布数 × ブランド

危険な機能 → 連絡帳、通話履歴、位置情報、端末情報など

悪意度(攻撃性) = 危険度 - 説明 × わかりやすさ
- 本当か(信頼度)?

2) スマート利用

リテラシー(利用技術と知見)

3) BYOD

現実的に関係のない組織はあり得ない。

現実を直視 → 基本は事故前提

管理責任と責任分解点 → 個人も責任が

② 現実的な脅威

1) スマホの紛失・盗難

1) 過失

さらに、手に入れたスマホの多目的悪用

2) 故意

→特に内部の故意 常識の欠如と新目的

2) 騙される・理解不足

ここは、
ポイント。

1) 技術力・リテラシー

2) 無関心

3) 不正プログラム

どこまで
脅威？

(1) 閲覧するだけで。接続するだけで。 → 基本無い

(2) アプリの管理。 ← ここは要所。

最低限、保有データとアプリの管理。

利用者が「騙されても」影響を最小限に。

3. 対策のヒント

「しなやかでしたたか」な対応



① そもそも論

何故、その事業を？

何故、そのシステムを？

何故、そのデータを？

志、無きまま、
これ以上のIT化を
進めていいのだ
ろうか？



故に

1)どのように社会ITに適応するか？

2)何をするか？

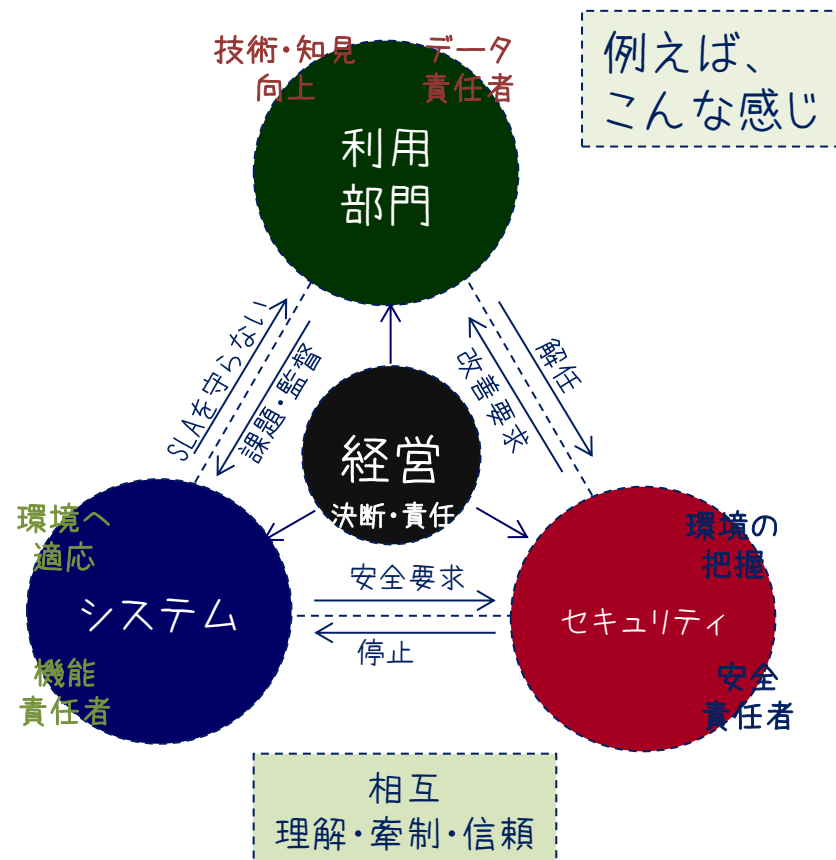
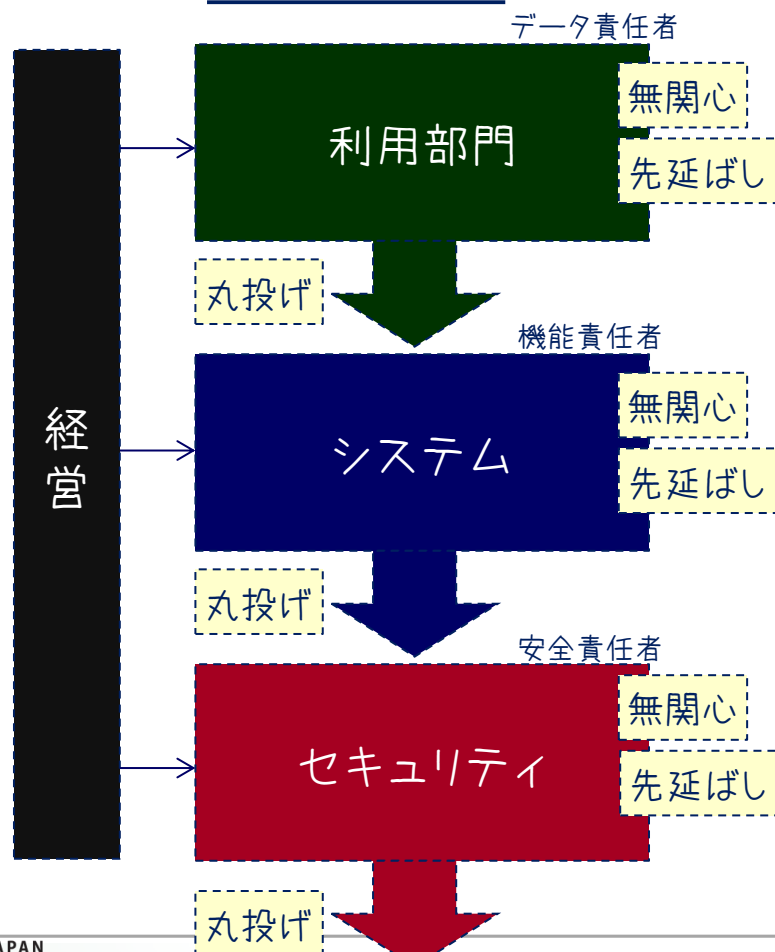
3)どんなセキュリティ対策が必要なのか？

⇒ 何故ならば100%は無いからである。

②「解決」への系口

仕掛け → 「構造変革」を考える。

垂直構造 → 社会構造(エコシステム)



③ 考え方

対策には経営陣の理解が必要と言うけど、極めて難しい。社会のIT化へ態度による。

経営者として外せないこと

1) ビジネスインパクトの把握。

→ 職責分離など「必要な無駄」への指令。

2) 丸投げ先の状況把握

→ 縦の先から違反を抽出。(システムの無理)

→ データオーナーへ改善命令。(取締り)

プランA: これ以上のIT依存を止めるか、

プランB: 機械の体を手に入れるまで、突き進むか。(笑)

→ どちらも、いばらの道。

④ 社会ITへの適応方針とデータ経営

1) 社会ITの従業員

- ☐ 積極的に推進
- ☐ 他がやりだしたら
- ☐ やらない

2) 社会ITの活用

- ☐ 積極的に活用
- ☐ 他がやりだしたら
- ☐ やらない

3) 社会ITへ展開

- ☐ 積極的に活用
- ☐ 他がやりだしたら
- ☐ やらない

4) データ経営

- ☐ 積極的に推進
- ☐ 他がやりだしたら
- ☐ やらない

どう決断するか？

何故、スマホを？

何故、クラウドを？

何故、データ活用を？

籠城か打って出るか？



⑤ 方針の考え方

1) スマホはどっちにいる

- ☐ 社内
- ☐ 社会
- ☐ 行ったり来たり

2) 端末やアプリの管理

- ☐ 管理する
- ☐ しない

3) 社内システムの利用

- ☐ 利用する
- ☐ させない

4) 社会ITの利用

- ☐ 会社業務として
- ☐ 個人で

5) 端末

- ☐ 会社支給
- ☐ 私物活用
- ☐ 私物排除

一人ひとりが
運転者！

整理してみよう。
それにより、物理的対策、
技術的対策、制度的対策が
見える。いずれにせよ、技
術的対策だけでは不可能



⑥ 対策の骨子

1) 物理的対策

スマホの持込禁止、カメラやマイクの封鎖
金属探知機、施錠、監視カメラなど

2) 技術的対策

MDM、MAM → JSSEC 『MAM/MCM利用ガイド』【β版】
セキュアブラウザ、コンテナ、セキュアアプリなど

3) 制度的対策

JSSEC

『スマートフォン&タブレットの業務利用に関するセキュリティガイドライン』【第二版】

⑦ 松竹梅

会社にとってITシステムは
→ 松竹梅のどれでしょうか？

対策の松竹梅は、
保護責任
社会的責任
データ経営の志向
ITシステムの位置づけ
などで決める。



ご清聴、

ありがとうございました。