2023年2月16日

各　位

会　社　名　サイバートラスト株式会社
代表者名　代表取締役社長 CEO 眞柄　泰利
（コード番号：4498　東証グロース）
問合せ先　取締役 常務執行役員 CFO 清水　哲也
（TEL 03-6234-3800）

2023年3月期 第3四半期に関する質疑応答集2

当社の 2023 年3月期 第3四半期決算に関して、これまで株主、投資家などの方々からいただいたお問い合わせ、感想、当社からの回答をまとめましたので、以下の通りお知らせいたします。
なお、本開示は市場参加者のご理解を一層深めることを目的に、当社が自主的に実施するものです。
皆様のご理解を賜ることを目的として一部内容・表現の加筆・修正を行っております。

Q1．第3四半期決算の補足説明では、「通期業績予想の確実な達成はもちろん」と開示されていますが、第4四半期での業績上積み要素について、改めて教えてください。

A1．第4四半期につきましては、以下、売上と、収益の見込みを達成すべく取り組んでおります。

- 認証・セキュリティ、Linux/OSS、IoT の3つの事業における、年度サービス更新によるリカーリングビジネス、並びに、年度末に集中する「iTrust®」サービス利用数の増大による従量課金
- IoT 事業において、IoT 機器開発向けの基本 OS である「EMLinux」の個別機能受託開発、並びに国際安全基準への適合に関するセキュリティコンサルテーション

また、認証・セキュリティ、Linux/OSS、IoT の3つの事業における、年度末に向けて生じる中小規模案件の獲得により、通期業績を達成しつつ、並行して来期売上に繋がる取り組みを行なっております。

Q2．IoT サービスとは具体的にどのようなビジネスですか？

A2．認証・セキュリティと Linux/OSS の技術を融合し、国際安全基準に適合させた IoT 機器の開発から利用、破棄にいたるライフサイクルマネジメントサービスです。

IoT 機器はサイバー攻撃を受けることで情報の流出や、機器の停止や誤作動等により社会や個人の生命、財産に大きな損害を与える恐れがあります。各国の重要インフラでは、利用される IoT 機器の製造に必要となる部品を安全に調達するためのサプライチェーンの確立が求められています。各国では産業機器の汎用制御システムの国際標準である「ISO/IEC62443」や、米国セキュリティ規格である「NIST SP800」などの国際安全基準への準拠が求められてきております。

当社は、オープンソースソフトウェア(OSS)のグローバル開発コミュニティと連携し安全なソフトウェア開発の指針づくりに貢献しております。ハードウェアの国際安全基準への準拠による安全なモノ作りと運用サービスの提供とともに、その上で動く OS やミドルウェアについて国際的なセキュリティ対策に貢献できることが大きな強みです。

当社は電子認証局の運用と認証サービスを提供し、かつ Linux/OSS の技術を有しているため、このような世界的に先行して安心安全な IoT サービスを提供することができる数少ない企業です。

IoT サービスは、国際安全基準に準拠し、より安全に長期に IoT 機器を利用管理できるもので、具体的なビジネスとしては、大きく2つあります。

1つ目は IoT 機器の開発向けの基本 OS である「EMLinux」を提供し長期脆弱性対策サポートを行うリ

カーリングビジネスです。
もう1つは、機器の真正性を認証し、ライフサイクル管理をする「Secure IoT Platform®（以下、SIOTP）」サービスを提供するリカーリングビジネスです。
現在、リカーリングビジネス売上の比率は低く、主に製造業のお客様において様々な IoT 機器を「EMLinux」で開発され売り上げを伸ばしている段階です。この開発の中で、IoT 機器向けの個別機能開発や、セキュリティコンサルによる売上が伸長しております。

Q３．1/31 発表の「クオンティニュアムの量子強化型秘密鍵を サイバートラストの新認証基盤に連携し実証を完了」では、「中長期に当社グループの業績向上に寄与する」とのことであるが、具体的に何がどう伸びるのか？

A３．現在、世界中で電子証明書による暗号化通信等で使われている秘密鍵は、今後の量子コンピュータの時代には解読される危険性があると指摘されています。そのため、当社では今期期初に新設した R&D 部門の研究テーマとして、当社開発の IoT 機器などに高速・大量に証明書を発行・配付可能な新認証基盤と組み合わせる形で、耐量子計算機暗号（PQC）や量子強化型秘密鍵の利用について研究・開発を行ってきました。
今回のクオンティニュアム社とのパートナーシップにより、来る量子コンピュータの時代に備え、最先端の量子強化型秘密鍵と、国際安全基準レベルの鍵管理、認証基盤を組み合わせることで、デジタル社会において高度な機密情報を安全にやり取りするための安全な認証基盤を提供する発表を行いました。当社では、この取り組みにより、秘匿性の高いデータを扱う医療、金融サービスや、化学、医薬品など研究開発分野での高機密情報を扱う先端分野とそれらと連携する IoT 機器への適用を推進してまいります。
当社サービスとしては、膨大かつ機密性の高いデータを取り扱う IoT 機器のライフサイクルマネジメントサービスを提供する「Secure IoT Platform®」への実装を検討しております。
当社では、量子コンピュータの時代に、安心、安全なサービスを他社に先駆けて提供すべく、本件に取り組むことで、将来の業績向上に寄与するものと考えております。

Q４．IoT 事業で、製品やサービスの安全性を高めるため、国際安全基準への準拠やオープンソースのコミュニティに貢献する理由はなぜですか？

A４．世界の IoT 機器の数は 2021 年で 292 億台となると推計されており、これらはインターネット上のさまざまなサービスに接続されたり、人手を介さず機器同士の相互接続により利用される可能性があります。
IoT 機器のセキュリティ問題としては、製造段階における非正規部品や非正規ソフトウェアの混入などが想定されています。こうした場合、IoT 機器がサービスに接続、あるいは、IoT 機器同士が相互接続することにより、情報漏洩、不正金銭授受はもとより、システムの異常作動や停止、誤動作が発生し、社会インフラはもとより、人命に至る影響を及ぼしかねないとされています。
そもそも IoT 機器は製造各メーカーが独自に開発し安全対策も異なります。また、パソコンや携帯電話と異なり、利用者の確認、認証、機器の実在性、真正性の証明、特定が困難です。
こうした状況を踏まえ、2018 年以降、そうした機器の製造段階におけるサプライチェーン、真正性を明確にし、安全性を高める要件が国際安全基準として定められ、産業機器の汎用制御システムのセキュリティガイドラインである「ISO/IEC62443」や、米国セキュリティ規格である「NIST SP800」などへの準拠が求められてきております。特に、この数年では、各国の国民生活や経済活動の基盤を守るため、そうした国際安全基準を各国が指定する重要インフラに関わる業種については、その基準に準拠する機器やシステムを納入する取り組みが海外で始まっており、今後、グローバル市場に投入する IoT 機器やシステムにおいては、国際安全基準に準拠する開発と提供が求められることになります。
より具体的には、ハードウェアに求められる国際安全基準では、IoT 機器(モノ)の製造段階におけるサプライチェーンから機器、機器の利用、そして運用をやめた際のモノの破棄に至るまでのライフサイク

ル管理を含めた要件が策定されています。

この国際安全基準における安全性の担保においては、半導体に電子鍵を組み込むことで、モノの出生証明(ヒトのマイナンバーに相当)として認証できるようにしており、モノを破棄する時点で失効させる(モノの死亡証明に相当)ことが求められています。

また、モノの利用期間中には、セキュリティや機器を動作せるための基本的なプログラムや不具合の修正が求められます。この修正のためには、インターネット上で、真正性の認証ができる正規の端末に、間違いない正規のプログラム修正を適用することが求められます。こうした、インターネット上における端末の修正プログラム適用(OTA - over the air)についても国際安全基準として求められております。

次に、ソフトウェアに求められる安全基準についてです。

IoT 機器のハードウェアの国際安全基準とともに、そこで動作するソフトウェアのセキュリティへの対処は大変重要です。世界中の IoT 機器に多用されるオープンソースソフトウェア（OSS）の脆弱性に焦点が当てられ、これに対処するため昨年 5 月、The Linux Foundation 下で進められているオープンソースソフトウェアのセキュリティ強化を目的として活動するグローバルコミュニティであるオープンソースセキュリティファウンデーション(OpenSSF)により 10 項目のセキュリティ行動計画※1 が発表されました。当社では、そのうちの 3 つ、デジタル署名、SBOM※2 の普及、ソフトウェアのサプライチェーンの改善について OpenSSF に以下の貢献を行うアナウンスをしたところです。

- デジタル署名：ソフトウェアの出所証明となるデジタル署名を付与、検証する sigstore※3 について機能強化への貢献、電子認証局運営の知見共有による厳密で安全な運用の提供
- Software Bill of Materials (SBOM)の普及：ソフトウェアに含まれるコンポーネントや依存関係、ライセンスの種類などを可視化するためのソフトウェア部品表である SBOM の利用状況情報のフィードバック、自社製品、サービスとの SBOM 連携の強化、提供
- サプライチェーンの改善：世界中のソフトウェアの約 80%がオープンソースで開発されています。このオープンソースで開発されたソフトウェアは開発元以外による再利用が可能のため、開発元の真正性、ソフトウェアの脆弱性の問題が大きなリスクとなってまいりました。当社では、ソフトウェアの中でも重要なオペレーティングシステム(OS)を長年開発提供している知見を活かし、OpenSSF コミュニティと連携し、より安心、安全なソフトウェア開発を可能にするサプライチェーンの構築に貢献しております。

なお、ハードウェア、ソフトウェアの国際安全基準に取り組むためには、認証局運営ノウハウ、認証技術、そして、オープンソースにおける知見と技術力が必要であり、当社は、それに取り組むことができる世界の中でも数少ない企業です。

また、上記に関連して次の発表をいたしました。

１．クオンティニュアム社との協業

大量の電子鍵を安全に発行、失効管理するためには、その管理システムが重要となります。当社では、昨年４月 27 日に新認証基盤の発表をしたところです。また、量子コンピュータの時代に備え、１月 31 日発表のとおり、クオンティニュアム社と共同で、量子強化型秘密鍵の新認証基盤との連携にも取り組んでいるところです。

２．セキュア IoT プラットフォーム協議会の「セキュア IoT 認定」

準拠すべき国際安全基準は、IEC62443-4-2 などがあり、当社の IoT 機器開発向けの基本 OS である「EMLinux」、IoT 機器の真正性を認証しライフサイクル管理をする「Secure IoT Platform®」を実現する「サイバートラスト セキュア IoT プラットフォーム認証局」においては、一般社団法人セキュア IoT プラットフォーム協議会により、２月 10 日発表のとおり、それらの国際安全基準に準拠しているとの認定を受けたところです。

※1 「The Open Source Software Security Mobilization Plan」

※2 Software Bill of Materials。ソフトウェアに含まれるコンポーネントや依存関係、ライセンスの種類などをリスト化したソフトウェア部品表。ソフトウェアサプライチェーンにおいてトランスペアレンシー（透明性）とトレーサビリティ（追跡可能性）を確保するための有効な手段として、世界的に普及が進んでいます。

※3　透明性のあるログ技術を使った暗号化ソフトウェア署名の導入により、サプライチェーン攻撃に対する保護を目的にしているオープンソースのソフトウェア署名サービス。The Linux Foundation などによるプロジェクトが開発・推進しています。

＊ iTrust®、Secure IoT Platform®は当社の登録商標です。
＊ 登録商標 Linux® は、Linus Torvalds から排他的ライセンスを受けている The Linux Foundation からサブライセンスを受けて使用しています。
＊ その他本文書に記載されている会社名、製品名、サービス名は、当社または各社、各団体の商標もしくは登録商標です。

以上