Software ISAC が選ぶ
開発者（企業）が注目すべき 10 大ニュース

Software ISAC

2021 年 1 月

目次

序文

Software ISAC が選ぶ、開発者（企業）が注目すべき 10 大ニュース

平素は、Software ISAC ならびに一般社団法人コンピュータソフトウェア協会（以下、CSAJ とします。）の活動にご協力いただき誠にありがとうございます。2020 年はコロナ禍の影響もありソフトウェア産業も大きな影響を受けたことと思います。サイバー空間においてもコロナ禍の影響で攻撃態様に変化があり、攻撃者の動きが活発化しております。日本においてもサイバー攻撃の被害に遭ってしまった企業も多く存在しています。そこで Software ISAC ならびに CSAJ セキュリティ委員会では、2020 年に起こった 10 大ニュースをまとめ公開することにより、2021 年特に注意が必要な対策について、理解を深めていただき自社のセキュリティ強化に役立てていただきたいと思い、10 大ニュースを編纂しました。

今後とも Software ISAC ならびに CSAJ セキュリティ委員会の活動、公開する文書を参照いただくことで、会員企業の皆さまが安全に事業を発展できることをサポートしていきたいと思います。

1.改正民法に対応した「情報システム・モデル取引・契約書」

2020 年 4 月に施行された改正民法によって、請負契約の規律に大幅な変更が行われました。具体的には、瑕疵担保の責任期間を引き渡しから 1 年としていたものを、改正法ではシステムの不具合が発見された時点から 1 年以内に通知、5 年以内に損害賠償請求（不具合の改修、解除等）をすればよいとなりました。

この変更は受託開発に重大な影響がでるため、IPA が事務局となり経産省モデル契約の改訂作業がなされました。

ワーキンググループでは、ベンダー側は「激変」となるため、従来通り引き渡しから 1 年以内の不具合の改修責任とすべきと主張し、ユーザー側は、法改正の趣旨に基づき改正法の通りとすべきとし、真っ向から対立しましたが、最終的には、例え契約で 1 年間の改修責任となっていても、不具合がベンダーの故意・重過失に起因する場合は、期間制限を適用除外するという事となりました。

従って、SQL インジェクションなどで情報が漏洩した場合は、10 年間（消滅時効）は損害賠償責任を負うことになります。（もちろん契約自由の原則から、故意・重過失でも免責という契約もあり得ます）

一方で、セキュリティ要件をユーザーが取りまとめることは困難な状況です。そこで、ベンダーがセキュリティ仕様をまとめて実装するケースが多いのはご承知の通りです。ところで、そのシステムにインシデントが発生した場合、ベンダーの取りまとめた仕様に重過失があったとユーザーに指摘されることは十分予想できるので、ベンダーは結果的に「10 年間」システム保守を維持しなければならなくなります。

これは、ベンダーにとって大変な負担になり、結果として、その費用はユーザーに転嫁されますので、どちらも不利益を被ることになります。

そこで、CSAJ が IPA、経産省に提案し、Software ISAC が事務局となって、交通 ISAC、J-Auto-ISAC、医療 ISAC の参画を得て「情報システム開発契約のセキュリティ仕様作成のためのガイドライン Windows Active Directory 編」が策定されました。

実際に発生した攻撃でよく利用される Technic に対して、Windows Active Directory での具体的な緩和策と、必要最低限の Group Policy の設定や、脆弱なプロトコルの排除などの具体的な設定方法が述べられています。

ユーザーとベンダーは、実際の攻撃をベースにリスクを検討し、セキュリティ仕様について合意することで、ベンダーは重過失の指摘を免れるとともに、ユーザーもセキュリティ上の課題を認識し、より堅牢な運用を行うことでインシデントを招かないロバストなシステムを入手できることとなります。

詳細は、https://www.softwareisac.jp/ipa を参照ください。

（解説記事：アップデートテクノロジー株式会社 代表取締役社長 板東直樹）

2.出荷判定チェックリストを公開

CSAJ および Software ISAC から「ソフトウェア出荷判定セキュリティ基準チェックリスト」（以下、出荷判定チェックリストとします。）がアップデートされました。出荷判定チェックリストは、クリエイティブコモンズライセンスに基づき、CSAJ 会員のみならず誰もが自由に利用でき、自社利用はもとより、改変や商用利用も可能となっています。出荷判定チェックリストは、初版が 2016 年に公開されておりましたが、4 年間の時を経て、「プロトコルやアルゴリズムに脆弱性が発見され推奨されなくなった」、「新たな脆弱性が発見された」、「利用者の要求に変化がみられた」などの要因から全面的な見直しを図りました。項目数は、43 項目から 113 項目と大幅に増やし、参考文献、脅威シナリオの記述を充実化、また他の団体が公開しているセキュリティ文書との紐づけを行っています。

出荷判定チェックリストの利用方法として、自社に必要なセキュリティ要件をチョイスし、自社プロダクト出荷時のチェックリストに適用するという使い方を想定しています。その他にも、開発工程の標準化や、社内の担当者のスキル向上、ソフトウェア・クラウドサービスの調達基準の一部にするなどの利用方法も考えられます。

Software ISAC では、今後も出荷判定チェックリストのアップデートを考えています。OWASP アプリケーションセキュリティ検証標準の取り込みや、OAuth に関するチェック項目の追記などを実施し、より最新のセキュリティ要件を取り込み利用しやすいものを目指して行きます。より出荷判定チェックリストを使いこなしたい、もっと深く知りたい場合は、出荷判定チェックリストのアップデート活動にご協力いただくことが近道と思います。皆さまの Software ISAC 活動へのご協力をお願いします。

参考資料：

ソフトウェア出荷判定セキュリティ基準チェックリストをバージョンアップ（CSAJ）

https://www.csaj.jp/NEWS/pr/201201_sec-release-decision.html

（解説記事：サイボウズ株式会社 セキュリティ室長 明尾 洋一）

3. ISMAP の登録申請が開始されました

政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））の登録申請が開始されました。ISMAP とは、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図る制度です。

ISMAP への登録が妥当と判断されたクラウドサービスは、ISMAP クラウドサービスリストに登録され、リストが公開されることになります。調達府省庁等は ISMAP クラウドサービスリストに掲載されているクラウドサービスの中から調達を行うことが原則となります。今後は、日本政府の情報システムのみならず地方公共団体や、重要インフラ提供事業者、民間企業がクラウドサービスを選定する場面においても活用される可能性があります。

クラウドサービスを提供している事業者は、ISMAP の概要を確認し、登録コスト・メリットを把握したうえで登録申請すべきか判断をしていくことが重要です。

参考資料：

ISMAP 概要（IPA）

https://www.ipa.go.jp/security/ismap/summary.html

（解説記事：サイボウズ株式会社 セキュリティ室長 明尾 洋一）

4. 多数の不正アクセス・情報漏えい事故

2020 年もピーティックスへの不正アクセス事件など、数多くの不正アクセス・情報漏えい事故が発生し、個人情報や、クレジットカード情報、また不正に預金を送金するなどで直接な金銭被害につながる事案も発生しました。2020 年 12 月 13 日には、IT 管理ソフトの開発を行う SolarWinds が開発する Orion Platform にバックドアが含まれていたことを公表。正規アップデートにより、バックドアが仕込まれ、利用していた組織のクレデンシャル情報が窃取されました。被害は米国政府など多岐にわたり、セキュリティ会社 FireEYE 社の RedTeam 用ツールが窃取されたことまで発表されています。

IPA が個人情報漏えいなどの外部への漏えいに対する基本的な対策をまとめています。経営者やユーザー、EC サイト運営者、システム管理者向けに必要な対策がまとまっているので、定期的なチェックを実施してください。

また、CSAJ セキュリティ委員会 および Software ISAC では、このような不正アクセスや情報漏えい事故を起こさないための対策およびセキュア開発手法について、研究し情報発信を続けていきます。情報発信した内容についてご確認いただければと思います。しかし、どのような対策を実施していても、攻撃者の能力が向上しており、依然攻撃者優位の状況にあります。事故が発生することを前提に、発生した場合に被害を最小限にとどめるための対策を早期に実施できるような連絡体制の確保も検討が必要です。

参考情報：

弊社が運営する「Peatix」への不正アクセス事象に関する第三者調査機関による調査結果のご報告と今後の対応について

https://announcement.peatix.com/20201216_ja.pdf

米政府などへの大規模サイバー攻撃、SolarWinds のソフトウェア更新を悪用

https://japan.cnet.com/article/35163843/

（CNET Japan ニュース記事）

漏れたら大変！個人情報

https://www.ipa.go.jp/security/kojinjoho/

（IPA）

（解説記事：サイボウズ株式会社 セキュリティ室長 明尾 洋一）

5. ランサムウェア / ランサム DDoS 攻撃

2020 年は、国内企業においてもランサムウェアの被害に遭う企業が急増しました。ランサムウェアの侵入手口は、リモートデスクトップ、VPN など、リモートワークを実施するうえで必要なポートを狙い、脆弱性が未対応な機材・OS があれば侵入するという手口（Human Operated Ransomware Attacks）もあれば、マルウエアが添付されたメールを送り付け実行させることで感染させる手口もあります。ランサムウェアの被害企業が、有名な大企業のみが対象というわけではありません。中小企業のソフトウェア開発会社がランサムウェアの被害に遭っているケースも確認されています。CSAJ および Software ISAC ではソフトウェア開発企業におけるランサムウェアの対策 10 ケ条を公開し注意喚起をしています。また、ランサム DDoS 攻撃も観測されており、身代金を支払わなければ DDoS 攻撃を仕掛けるという脅迫をする事例もあり、JPCERT/CC が注意喚起をしています。攻撃の影響を受ける可能性のあるシステムの特定およびリスク評価、攻撃を検知・防御の対策状況の確認、検知・認識した場合の対応手順・方針の確認、攻撃による影響が発生した場合の連絡体制や連絡方法の確認などを実施することが推奨されています。

参考資料：

ランサムウェアからソフトウェア開発企業を守るためのガイドライン
https://www.csaj.jp/NEWS/pr/1208_ransomware-measures.html
（CSAJ セキュリティ委員会 / Software ISAC）

【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について
https://www.ipa.go.jp/security/announce/2020-ransom.html
（IPA）

DDoS 攻撃を示唆して仮想通貨による送金を要求する脅迫行為 (DDoS 脅迫) について
https://www.jpcert.or.jp/newsflash/2020090701.html
（JPCERT/CC）

（解説記事：サイボウズ株式会社 セキュリティ室長 明尾 洋一）

6. IPA「脆弱性対処に向けた製品開発者向けガイド」が公開されました

2020 年 8 月独立行政法人情報処理推進機構（以下、IPA とします）は「脆弱性対処に向けた製品開発者向けガイド」を公開しました。インターネットやホームネットワーク等のネットワークに接続する以下のような機器、ネットワーク家電・プリンタ・ネットワークカメラ・スマートフォンやパソコンのアプリケーションなどを開発している事業者（主に中小規模）を対象としており、製品の脆弱性への対処すべき項目が記載されています。

本ガイドが公開された背景は、サイバー攻撃の脅威は高まりつつも、製品開発者の脆弱性対処は一般消費者からの製品選定の優位性に結びついていない現状があり、結果的に脆弱性への対処が進んでいないことがあげられています。ガイドには、脆弱性の対処項目以外にも、一般消費者に自組織の取組みをアピールすべきことがあげられています。

本ガイドの利用方法は、①チェックリストで自組織の対応状況を確認する、②ガイドを参照しチェック内容をもとに対処内容を確認する、③チェック内容をもとに対応方針を決定する、④ガイドの内容を踏まえて対応する、のステップで脆弱性対処を進めていくことが想定されています。

本ガイドによると、製品開発者が実施すべきことは、「製品セキュリティポリシーの策定」、「セキュリティサポート方針の明示」、「製品セキュリティを維持するための体制と管理」具体的には PSIRT の設置、「セキュリティを確保するための設計」、「アップデートを考慮した設計」、「既知の脆弱性解消」、「セキュアコーディング」具体的にはセキュアコーディング規約・教育・実装・レビューの実施、「開発環境のセキュリティ確保」、「開発時の脆弱性検査」、「製品と構成要素の脆弱性監視」、「脆弱性報告の受付・対策情報の公表」「一般消費者の製品利用時における実施事項の明示」があげられています。

別紙にチェックリストが付いており、実施済みの項目を確認することで、自組織の脆弱性対処のレベルを測定することが可能です。

本ガイドを、製品開発者が確認し、脆弱性対処のレベルをあげていただくことも重要ですが、一般消費者にも、本ガイドの存在を知っていただきガイドに沿った対処を実施し情報を公開している組織の製品を購買するという行動に結び付けることが、日本のインターネットの安全を守るうえで大切なことだと思います。

参考資料：

「脆弱性対処に向けた製品開発者向けガイド」（IPA）

https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html

（解説記事：サイボウズ株式会社 セキュリティ室長 明尾 洋一）

7. Flash サポート終了など、その他 OSS などのセキュリティアップデートに注意

Flash サポート終了など、各種製品のサポート終了に注意

企業組織、家庭での利用を問わず、サポート対象の製品を利用し、セキュリティ更新プログラムを適用することは、必ず実施するべき基本的なセキュリティ対策です。

企業組織においては、電子メールやインターネットの閲覧を行うことの多いビジネスの業務を行う環境はもちろんのこと、インターネットに直接接続を行っていない開発環境においても、ベンダーからのサポートライフサイクル内の製品を利用し、セキュリティアップデートを適用して最新の状態を保つことが、安全な製品の開発には欠かせません。

2020 年、および 2021 年にサポートが終了する主な製品について、組織内での利用状況を確認し、サポートが終了する製品については、より新しいバージョンへの移行を検討しましょう。

2020 年にサポートが終了した主な製品

サポート終了日	製品ベンダー	製品
2020 年 1 月	MongoDB	MongoDB 3.4
2020 年 1 月 14 日	Microsoft	Windows 7, Windows 2008, Windows Server 2008 R2
2020 年 1 月 31 日	Microsoft	Internet Explorer 10
2020 年 2 月	PostgreSQL	PostgreSQL 9.4
2020 年 4 月 11 日	MariaDB	MariaDB 5.5
2020 年 6 月 30 日	Debian	Debian 8
2020 年 7 月 7 日	Adobe	Acrobat Reader DC 2015, Acrobat Standard DC 2015
2020 年 7 月 14 日	Microsoft	Visual Studio 2010 (すべてのエディション), Visual Basic 2010 Express Visual C# 2010 Express, Visual C++ 2010 Express, Visual Web Developer 2010 Express

2020 年 10 月 13 日	Microsoft	Microsoft Office 2010 (すべてのエディション) Office 2016 for Mac (すべてのエディション)Windows Embedded Standard 7
2020 年 11 月 30 日	CentOS	CentOS-6
		Red Hat Enterprise Linux 5
2020 年 12 月 25 日	Elasticsearch	Elasticsearch 7.2.x
2020 年 12 月 31 日		Adobe Flash Player • Adobe Flash Player 法人向けサポート終了 (Adobe 社) • Internet Explorer および Microsoft Edge での Flash の今後の対応について (マイクロソフト社) • Flash Roadmap - The Chromium Projects • Plugin Roadmap for Firefox - Plugins | MDN (mozilla.org) • Adobe Announces Flash Distribution and Updates to End | WebKit
2020 年 12 月 31 日	Oracle	Oracle Database 11.2.0.4

2021 年にサポートが終了する主な製品

2021 年 2 月	PostgreSQL	PostgreSQL 9.5
2021 年 2 月	MySQL	MySQL 5.6
2021 年 3 月 9 日	Microsoft	Edge (HTML-based)
2020 年 4 月	MongoDB	MongoDB 3.6
2021 年 4 月 13 日	Microsoft	Lync 2010 (すべてのエディション) Lync Server 2010 (すべてのエディション) Windows Embedded Compact 7 SharePoint Server 2010
2021 年 7 月 31 日	Microsoft	Skype for Business Online
2021 年 8 月 16 日	Microsoft	Microsoft 365 における Internet Explorer 11 の接続 Microsoft 365 apps say farewell to Internet Explorer 11 and Windows 10 sunsets Microsoft Edge Legacy - Microsoft Tech Community
2021 年 10 月 12 日	Microsoft	Silverlight 5, Dynamics AX 2009 Dynamics AX 2012 Dynamics AX 2012 R2, Microsoft Diagnostics and Recovery Toolset 7.0, Windows Embedded POSReady 7, Windows Thin PC
2021 年 10 月 17 日	MariaDB	MariaDB 10.1
2021 年 11 月	PostgreSQL	PostgreSQL 9.6
2021 年 12 月 18 日	Elasticsearch	Elasticsearch 7.8.x
2021 年 12 月 31 日	CentOS	CentOS 8

参考情報：

Microsoft

2020 年にサポートが終了する製品 , 2021 年にサポートが終了する製品

IBM

IBM software lifecycle - IBM Support

Oracle

Oracle Hardware and Systems Support Policies

Lifetime Support Policy - リソース | Oracle Support | Oracle 日本

Java SE のサポート期間と Oracle Fusion Middleware Policy

VMWare

Product Lifecycle Matrix (vmware.com)

Elastic

Elastic Product End of Life Dates | Elastic

Adobe

製品とテクニカルサポート期間 (adobe.com)

CentOS

About/Product - CentOS Wiki

Debian

Debian Release Management

MariaDB

About MariaDB Server - MariaDB.org

MongoDB

MongoDB Support Policy | MongoDB

（解説記事：Microsoft Corporation セキュリティ レスポンス チーム

セキュリティ プログラム マネージャー 垣内由梨香）

8. OWASP ASVS 日本語版公開

CSAJ および Software ISAC は、2020 年 9 月に OWASP アプリケーションセキュリティ検証標準（以下「ASVS」）の日本語版を公開しました。

ASVS は、アーキテクト、開発者、テスター、セキュリティ専門家、ツールベンダー、アプリケーション利用者などが、最新の Web アプリケーションおよび Web サービスを設計、開発、テストする際に必要となる、機能的および非機能的なセキュリティ対策の定義に焦点を当てた、セキュリティ要件や対策の枠組みを確立するためのドキュメントです。OWASP の長年にわたる取り組みと ASVS を利用する業界からのフィードバックの集大成となっており、安全なソフトウェア開発のライフサイクルを通して、さまざまなユースケースに簡単に採用できるようになっています。

Software ISAC は今後この日本語邦訳文書を活用し、Software ISAC の会員企業向けに「ASVS をベースとした Web アプリケーションの検証方法の勉強会」や「ASVS をベースとしたセキュア開発方法の勉強会」などの提供、セキュリティベンダー向けに「ASVS をベースとした Web アプリケーションの検証プログラムを提供」するためのメニュー化の推進、ユーザー企業向けに「ASVS を Web アプリケーション開発の検収条件としていくための啓発活動」や「脆弱性対応に要するコスト理解の促進」などの活動に繋げていくことを検討しています。

参考文書：

OWASP「アプリケーションセキュリティ検証標準 4.0」の日本語邦訳文書公開について
https://www.csaj.jp/NEWS/pr/200903_asvs.html
（CSAJ）

（解説記事：株式会社 GSX CSO 萩原 健太）

9. TLS 暗号設定ガイドライン

TLS 暗号設定ガイドラインの更新版が公開

2020 年 7 月、CRYPTREC による SSL/TLS の利用ガイドラインである「TLS 暗号設定ガイドライン」(旧名 SSL/TLS 暗号設定ガイドライン) の改定版 (第 3 版) が公開されました。「TLS 暗号設定ガイドライン」は、暗号技術評価プロジェクト CRYPTREC が作成・公開している SSL/TLS サーバの構築者のための実際に設定すべき設定をまとめたガイドラインです。SSL/TLS といっても、利用するプロトコルのバージョン、暗号アルゴリズム、鍵交換の設定など設定の項目は多くあり、目標とする安全性レベルを達成するためには適切な設定が必要です。このガイドラインでは、安全性の確保と相互接続の必要性のトレードオフにより、三段階の設定基準を設けていて、利用するシステムに応じて設定基準を選べるようになっています。

今回の改定では、2018 年に RFC が正式に発行され、順次実装も進んでいる TLS 1.3 に関するガイダンスも新たに加わりました。また、安全ではない古いプロトコル SSL 3.0 の禁止が行われ、各要求項目でより強い安全性を持つ設定が求められています。今回の改定のポイントは、

1. ガイドラインタイトルの変更

   「TLS 暗号設定ガイドライン」に名称が変更になりました。

2. 設定基準の要求設定における「遵守項目」と「推奨項目」の区分けの新設

   以前は全ての設定項目について一律に「要求 設定」と位置付けていました。今回は、設定項目のおける安全性への寄与度を考慮し、TLS 暗号設定ガイドライン (version 3.x) では、選択した設定基準としての最低限の安全性を確保するために必ず満たさなければならない「遵守項目」と、当該設定基準としてよりよい安全性を実現するために満たすことが望ましい「推奨項目」とに分け、より現実的かつ実効性が高い要求設定としました。

3. 各設定基準における設定項目の更新
   - 高セキュリティ型
     - 要求項目に TLS 1.3 の追加
   - 推奨セキュリティ型
     - TLS 1.3 の追加 (オプション)
     - 鍵交換で Perfect Forward Secrecy の特性をもつ ECDHE や DHE を強く推奨

- TLS 1.0 や TLS 1.1 の禁止 (セキュリティ例外型のみで利用可能)

- セキュリティ例外型
  - SSL 3.0 の利用を禁止

また、TLS 暗号設定ガイドラインの更新版の公開と同日には、 CRYPTREC から暗号の鍵を管理するためのガイドライン「暗号鍵管理システム設計指針 (基本編)」も公開されています。

安全な暗号システムは、いまや、セキュリティに関する設計における重要なポイントです。暗号は使っていれば安全ではありません。脅威に合わせた最新の暗号アルゴリズムを利用し、暗号に利用する鍵を適切に管理するシステムを設計、運用することが求められます。安全な開発のために、ぜひ、2020 年に公開された CRYPTREC の参照してください。

（解説記事：Microsoft Corporation セキュリティ レスポンス チーム
セキュリティ プログラム マネージャー 垣内由梨香）

10. ドメインレジストラサービスを狙った攻撃

2020 年 6 月に仮想通貨取引所サービスを提供している Coincheck 社が利用していたドメイン登録サービスの不具合が原因で不正アクセスを受け、DNS の内容が不正に書き換えられるという事案が発生しました。また、2020 年 11 月には、同じく仮想通貨取引所サービスを提供している Liquid 社が利用しているドメイン登録サービスの従業員に対する攻撃が原因で、DNS の内容が不正に書き換えられるという事案が発生しています。

双方の事案とも、DNS の書き換えにより顧客から送信されたメールが攻撃者にわたってしまった可能性があります。DNS の内容が書き換えられた場合の被害は、メールの窃取のみならず、提供しているサービスの停止、不正なサイトへの誘導などの被害も想定されます。

ドメイン登録サービスのアカウントの乗っ取り以外にも、自動更新されるはずのドメインが不測の事態で更新されず第三者に取得されてしまう可能性や、サービスの終了などで利用していたドメインを放棄し、そのドメインを第三者が取得し不適切なサイトが立ち上がってしまう可能性もあります。

このようなドメインに関する事故を防止するためには、利用しているドメイン登録サービスの確認、アカウントのログインに他要素認証が適用されているか、アカウントが従業員個人のメールアドレスとなっている場合その従業員が退職した場合に対処できるかどうかの確認、ドメインが自動更新となっている場合の支払方法にクレジットカードが登録されている場合クレジットカードの有効期限切れで引き落としできなかった場合の連絡に対応できるか、またドメインの管理についてドメイン取得・放棄の社内ポリシーの設置・ドメイン管理などを実施することが望まれます。

参考資料：

「当社利用のドメイン登録サービス「お名前.com」で発生した事象について（最終報告）」
https://corporate.coincheck.com/2020/06/04/98.html
（Coincheck 社 PRESS）

「2020 年 6 月に発生したドメイン名ハイジャックのインシデント対応について」
https://tech.coincheck.blog/entry/2020/06/24/120000
（Coincheck 社 技術ブログ）

「当社利用のドメイン登録サービスにおける不正アクセスについて（第二報）」
https://blog.liquid.com/ja/20201118-important-notice-2
（Liquid ブログ）

ドメインの放棄に関する事案はこちら

「自治体管理ドメイン悪用が相次ぎ発覚、「使い捨て感覚」脱せずアダルト転用も」

https://xtech.nikkei.com/atcl/nxt/column/18/00989/120900041/

（日経クロステック記事）

（解説記事：サイボウズ株式会社 セキュリティ室長 明尾 洋一）

Software ISAC が選ぶ開発者（企業）が注目すべき 10 大ニュース選定委員

アップデートテクノロジー株式会社

代表取締役社長　板東 直樹

株式会社ラック

サイバー・グリッド・ジャパン　主席研究員　加藤 智巳

Microsoft Corporation

セキュリティ レスポンス チーム セキュリティ プログラム マネージャー 垣内由梨香

グローバルセキュリティエキスパート株式会社

CSO 萩原 健太

サイボウズ株式会社

セキュリティ室 室長 明尾 洋一