日本のサイバーセキュリティを「連携」「学び」「創造」

JNSA活動報告会

社会活動部会の紹介

2025年7月25日

部会長：唐沢 勇輔（Japan Digital Design 株式会社）

JNSA活動全体図

JNSA

部会/支部

- 社会活動部会 4WG
- 調査研究部会 9WG
- 標準化部会 4WG
- 教育部会 4WG
- 会員交流部会 3WG
- マーケティング部会
- 事業コンプライアンス部会
- U40部会 3WG
- 国際連携部会
- 西日本支部 1WG

委員会等

- 産学情報セキュリティ人材育成検討会
- セキュリティコンテスト実行委員会(SECCON) 5WG
- サイバーセキュリティ産学連携推進協議会

傘下団体

- 情報セキュリティ教育事業者連絡会(ISEPA) 2WG
- 日本セキュリティオペレーション事業者協議会(ISOG-J) 6WG
- 日本トラストテクノロジー協議会(JT2A)

※WG：ワーキンググループを表す。合計41WG（2025.7現在）

社会活動部会とは

JNSA

JNSA活動の企画検討、
対外連携を担っている部会

社会活動部会でやっていること

定期的なもの

- 毎月の部会開催（原則、毎月第一木曜日 16:00～18:00）
- JNSAメルマガのコラム記事検討

不定期なもの

- 省庁との意見交換会
- 会員勉強会（JNSA会員向け勉強会）
- 記者懇談会（プレス向け勉強会）

毎月の部会での議論していること

定常的に議論しているアジェンダは以下の通り。
これ以外にセミナーの企画などを議論することも。

1. 重要セキュリティニュース振り返り
2. メルマガ、しんだん、勉強会
3. パブコメ
4. IT団体連盟（セキュリティ委員会）
5. 各WGの状況
6. 関係省庁や団体との動き
7. 記者懇談会・記者向け勉強会
8. 政策提言について

こんな方におすすめ

- 専門家の間で話題になっているセキュリティニュースにどんなものがあるか知りたい
- セキュリティ業界や政策の動向を知りたい
- JNSAの活動に関与、貢献したい

過去に主催した勉強会

実施日	テーマ	参加対象
2024/5/24	セキュリティ・クリアランス法案	JNSA会員限定
2024/9/20	パスキー	同上
2025/2/28	セキュリティベンダー・ITベンダーにとってのPQC移行問題	同上
2025/5/8	選挙とサイバーセキュリティ	同上
2025/7/10	能動的サイバー防御	同上
2025/7/29	証券口座乗っ取り問題	同上

突然ですが

JNSA

評判のよかったメルマガコラム記事
ランキング発表！(2024年度)

JNSAメルマガについて

- JNSAで配信している会員向けメールマガジン（原則 隔週金曜日発行）を、会員以外の方々へも配信
- 読者数：会員・非会員あわせて5000名超
- 配信内容
  - 連載リレーコラム
  - 部会/ワーキンググループからのお知らせ
  - セミナー/イベント情報（不定期）
  - 事務局からの連絡、お知らせ など

コラム記事アンケート

【お問い合わせ】
ご不明な点がございましたら、お気軽にお問い合わせください。

【JNSA西日本支部からのお知らせ】
JNSA西日本支部では、工場セキュリティに関するセミナーやイベントを定期的に
開催しています。また、メンバーも随時募集しています。ぜひご参加ください。

（※事務局注：部会・ワーキンググループへのご参加は原則として
JNSA会員の方のみとなっております）
＃連載リレーコラム、ここまで

＜お断り＞本稿の内容は著者の個人的見解であり、所属団体及びその業務と
関係するものではありません。

＜ワンクリックアンケートお願い＞
今回のメールマガジンの感想をお寄せください。
https://tinyurl.com/3hykzv7u
※googleアンケートフォームを利用しています。

【JNSAイベントのお知らせ】
★「JNSA2025年度活動報告会」（オンライン）
2025年7月23日（水）～25日（金）　3日間開催！！参加受付を開始しました。

評判の良かった記事ランキング

順位	対象号	タイトル	合計得点	平均点	総合スコア（正規化平均）
1位	第289号	LINEヤフーの個人情報漏洩と資本見直しを巡る騒動（2024.6.14配信）	62	4.769	0.934
2位	第299号	サイバーインテリジェンスとセキュリティ（2024.11.1配信）	35	5.000	0.763
3位	第290号	暗号の2030年問題をご存じですか？（2024.6.28配信）	29	4.833	0.663
4位	第300号	いまさら聞けないパスワードにまつわる問題とその対応（2024.11.15配信）	36	4.500	0.629
5位	第298号	脆弱性管理における対処の優先度付けの重要性～大量の脆弱性対処に溺れない、実態に即した対処優先度を判断する～（2024.10.18配信）	32	4.571	0.614

第289号：LINEヤフーの個人情報漏洩と資本見直しを巡る騒動（2024.6.14配信）

- 若江雅子氏・読売新聞編集委員
- 発端：LINE利用者等の個人情報50万件以上が漏洩。原因はネイバー委託先のマルウェア感染と認証基盤の共通化。
- 構造的問題：ネイバーに技術・人材面で依存。ログ管理もネイバー側にあり、LINEヤフーの統制が不十分。
- 資本と委託のねじれ：ネイバーが大株主でありながら委託先でもあるため、ガバナンスが逆転。
- 総務省の対応：資本関係見直しを行政指導で要請。LINEヤフーは委託ゼロを表明、ネイバーは協議継続。
- 韓国国内の反発：日本による「奪取」や「差別」との声も。政治的影響も懸念。
- 本質的課題：国籍ではなく、透明性と説明責任の欠如が問題。技術依存と統治の不整合がリスクを拡大。

第299号：サイバーインテリジェンスとセキュリティ（2024.11.1配信）

- 軍司祐介氏（株式会社マキナレコード 代表取締役）
- **「インテリジェンス」と「情報（インフォメーション）」は異なる概念**
  - インテリジェンス＝意思決定支援のために分析・加工された情報
  - 例：天気予報は複数の気象データを分析し、服装などの判断を助ける「インテリジェンス」
- **情報 → インテリジェンスへの変換プロセス**
  - 情報（点）を分析・評価し、背景（コンテキスト）を加えて立体的に加工（線→立体）
  - 信頼性・関連性・背景を加味して意思決定に活用可能な形にする
- **インテリジェンスの重要性**
  - 限られたリソースで迅速・正確な意思決定を行うための手段
  - 特にサイバー領域では、攻撃の高度化・複雑化により必要性が増大
- **企業への応用**
  - 軍事由来の概念を企業経営やセキュリティ対策に応用
  - 予算・人材不足を補い、攻め手有利な状況を打破する手段として注目
- **結論**
  - 「敵を知り己を知れば百戦危うからず」
  - 情報を活かし、インテリジェンスとして活用することで業務効率と社会の安全性が向上

第290号：暗号の2030年問題をご存じですか？（2024.6.28配信）

- **2030年問題の概要**
  - 量子コンピューターの進化により、現行の公開鍵暗号（例：RSA）が破られる可能性
  - 「2030年までに2048bit鍵が破られる」との警告もある（諸説あり）
- **量子コンピューターの脅威**
  - 素因数分解・離散対数問題を高速に解けるようになる → 公開鍵暗号が脆弱に
  - 共通鍵暗号は影響が少ないとされる
- **PQC（耐量子暗号）とは**
  - 量子コンピューターでも解読困難な数学問題に基づく新しい暗号技術
- **PQCの課題**
  - 処理速度の低下、鍵長の肥大化など技術的課題
  - 標準化はNISTで最終段階、2025年夏に確定予定
  - 初期は古典暗号とのハイブリッド運用が推奨される
- **すでに使われているPQC**
  - Google Chrome 123以降で「ハイブリッドポスト量子TLS鍵交換」が既定で有効
  - 一部のセキュリティ機器で通信障害の報告もあり
- **過去の類似事例：2010年問題**
  - RSAやSHA-1からの移行に数年かかった経験
  - 今回も長期的な対応が必要。早期の情報収集と準備が重要

第300号：いまさら聞けないパスワードにまつわる問題とその対応（2024.11.15配信）

- 宮本久仁男氏（NTTデータグループ セキュリティマスター）
- **主な提言**
  - パスワードは「複雑さ」より「長さ」が重要（10文字以上推奨）
  - 忘れる前提で、PCやスマホに覚えさせるのが現実的
  - 再設定可能なシステムでは、臆せず長いパスワードを設定
- **利用者側の課題**
  - パスワードの使い回しによる不正侵入
  - 短いパスワードによる総当たり攻撃の脆弱性
- **対応アプローチ**
  - Webブラウザやパスワード管理ツールの活用
  - 自分で覚えず、デバイスに記憶・生成させる
  - 再設定手順の確認と実践を推奨
- **最も守るべきはメールアカウント**
  - 認証の基盤となるため、MFAやパスキーで強固に保護
  - Gmailなどの高セキュリティサービスの活用を推奨

第298号：脆弱性管理における対処の優先度付けの重要性 ～大量の脆弱性対処に溺れない、実態に即した対処優先度を判断する～（2024.10.18配信）

- 山下諒輔氏（株式会社マクニカネットワークスカンパニー）
- **背景**
  - 年間約30,000件の脆弱性が公開されるが、実際に悪用されるのは約3%
  - 全件対応は非現実的で、リソースを効率的に使う必要があり、Attack Surface Managementの取り組みへの注目が世界的に高まっている
- **優先すべき脆弱性とは**
  - 攻撃難易度・悪用事例・PoCの有無など「現実的なリスク」に着目
  - 日系企業ではVPN・FW機器・RDPがランサムウェアの初期侵入口の約80%
- **CVSSスコアの限界**
  - CVSSは理論上の深刻度であり、現実的なリスクとは限らない
  - 高スコアでも悪用されない／低スコアでも悪用される例あり
- **まとめ**
  - 実態に即した優先度付けが不可欠
  - 自社の脆弱性対応方針を見直し、製品選定にもリスクベースの視点を

ぜひ部会にご参加ください
（ご興味をもっていただいた方は事務局まで）