サイバー攻撃の現状と施策案

平成２８年１１月９日
Ｓ＆Ｊ株式会社
代表取締役社長　三輪信雄

略歴：　昭和６０年３月　同志社大学工学部電気工学科卒業
昭和６０年４月　住友ゴム工業株式会社入社
平成　２年３月　株式会社ラック入社
平成１５年９月　株式会社ラック　代表取締役社長就任
平成１９年１月　辞任
平成２０年１１月　S&J株式会社設立

現在：　S&J株式会社 代表取締役社長、
総務省 最高情報セキュリティアドバイザー、
神奈川県警サイバー犯罪捜査顧問、
セキュリティキャンプ実施協議会会長、
株式会社セキュアスカイ・テクノロジー　技術顧問、
サイバーセキュリティリスクと企業経営に関する研究会委員、
産業構造審議会 商務流通情報分科会 情報経済小委員会委員、
東京電力スマートメーターシステムの情報セキュリティに関する有識者委員会委員、
その他非公開政府系委員、上場企業情報セキュリティ委員会委員

歴任：　ファイア・アイ株式会社 VP/CTO、
独立行政法人 情報処理推進機構 情報セキュリティ関連事業審議委員会委員、
Firewall Defenders(FWD)会長、BUGTRAQ-JPモデレータ、
内閣官房情報セキュリティポリシーガイドラインWG委員 、情報ネットワーク法学会発起人、
日本ネットワークセキュリティ協会(JNSA)理事、
警察庁セキュリティビジネス調査WG委員、警察庁不正プログラム調査WG委員、
会計検査院研修講師、警察大学校講師、金融財政事情研究会経営幹部研修講師、人事院研修講師、
情報セキュリティ講座講師(早稲田大学、琉球大学)、総務省統一研修講師、
内閣官房情報セキュリティ基本問題委員会第一分科会・第二分科会委員、
経済産業省商務情報政策基本問題小委員会委員、
セキュリティ＆プログラミングキャンプ　実行委員長　（2004年～2014年）、
サイバー犯罪に関する白浜シンポジウム 危機管理コンテスト審査委員長（2007年～2016年）、
内閣官房情報セキュリティセンター(NISC)　第２次情報セキュリティ政策会議　基本計画検討委員会委員、
その他非公開政府系委員多数

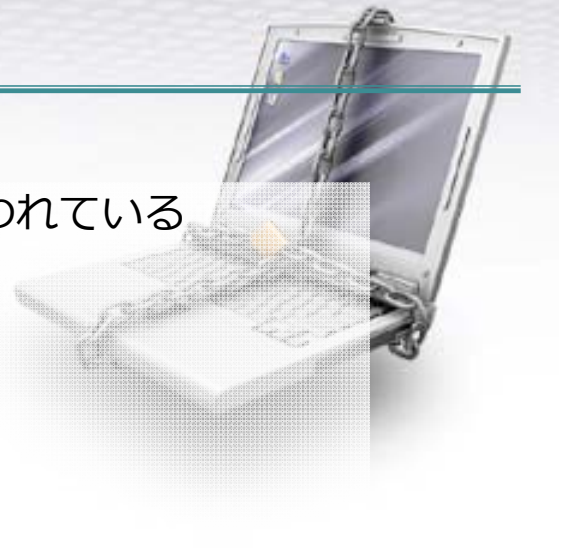
表彰など：　財団法人日本情報処理開発協会 創立40周年 個人表彰、平成２０年度経済産業省情報化月間　専門家コミュニティ活動個人表彰、
経済産業大臣賞（株式会社ラック社長）、第１回情報セキュリティ文化賞、経済産業大臣賞（個人）

1995年より日本で情報セキュリティビジネスの先駆けとして事業を開始し業界をリードした。また、日本のWindows製品,Netscape,TrendMicroその他多くの製品の脆弱性を発見してきた。また、無線LANの脆弱性やWebアプリケーションの脆弱性について日本でいち早く問題を指摘・公開し、現在のWebアプリケーションセキュリティ市場を開拓した。また、セキュリティポリシーという言葉が一般的でなかったころからコンサルティング事業を開拓し、さらに脆弱性検査、セキュリティ監視など日本のセキュリティサービスビジネスの先駆けとなった。その後、上場企業社長として、３年連続増収増益を達成し、経営者としての視点でも情報セキュリティを論じることができる。
今後、情報セキュリティの成熟化が進み、自社内でのセキュリティ対策が主流になるという思いからS&J社を起業した。教科書通りのマネジメント重視の対策に異論をもち、グローバルスタンダードになるべき実践的なセキュリティシステムの構築に意欲的に取り組んでいる。

@IT　Security & Trust　セキュリティ、そろそろ本音で語らないか　http://www.atmarkit.co.jp/ait/articles/1405/15/news013.html
翔泳社 EnterpriseZine連載 ニューズレター http://enterprisezine.jp/iti/detail/6039

目 次

1.主なサイバー攻撃の対象と対策



1. サイバー攻撃は、**公開サーバ**と**内部ネットワーク**に行われている

2. <u>公開サーバに対する攻撃と対策</u>
   - ① 侵入されて個人情報が漏洩、マルウェア埋め込み
     - 対策：
       - セキュアな開発と検査
       - サイバー攻撃を防ぐ装置(WAF)
   - ② IoT端末による巨大DDoS攻撃
     - 対策：
       - 防ぐことは困難

オリパラに向けて強化すべき対象

3. <u>内部事務系ネットワークに対するサイバー攻撃（＝標的型攻撃）と対策</u>
   - ① すでに多くの企業が侵入されて情報が盗まれ続けている
   - ② 気付いていないケースが多く、目立った実害が感じられない
     - 対策：
       - 最新の防御/監視システム
       - 感染前提の監視/対応体制
       - インターネット分離と画像転送

※ 資料１，２

1.主なサイバー攻撃の対象と対策

4. 内部制御系ネットワークに対するサイバー攻撃と対策
   - ① 工場や発電所、鉄道施設などに侵入して破壊/妨害活動を行う
   - ② 侵入されないことが前提になっているが、侵入されればもろい
     - 対策：
       - 最新の防御/監視システム
       - 感染前提の監視/対応体制

オリパラに向けて強化すべき対象

5. IoTデバイスに対するサイバー攻撃と対策
   - ① Webカメラなどが侵入されDDoS攻撃に悪用される
   - ② 不正に操作される
     - 対策：
       - 安全な設置/運用の手順を行う慣習
       - 開発者へのセキュリティ開発教育

6. 個人に対するサイバー攻撃と対策
   - ① パソコンが乗っ取られてDDoS攻撃に悪用される
   - ② パソコンやスマホが乗っ取られて情報やポイントが盗まれる
   - ③ パソコンやスマホからオンラインバンキングで不正送金される
     - 対策：
       - 安全な使用方法の普及啓発

3.重要インフラのサイバーテロ対策の推進

○下記１．２．について、NISCを中心に、制度化に向けた検討を早急に行い、「第三次行動計画」の見直しに反映すべき。

○その際には、３．から５．までの事項に留意すべき。

1. 重要インフラでのサイバーテロ対策は喫緊の課題
   - ペネトレーションテストを含む徹底的なリスク評価、業種別ガイドラインの策定と実施報告、及び**外部監査**を義務化

2. 重要インフラでは、「サービスの停止」がないと障害として報告されないが、サイバーセキュリティでは**「予兆」が重要**
   - **インシデント及び予兆**の報告を義務化

3. 各重要インフラが独自で対策を検討するのではなく、最低限の対策水準を確保するため、**特定の重要インフラにて検討されたより厳格な対策を横展開**するべき

4. 事務系/制御系に分けて、**ガイドラインの検討が既に進んでいる重要インフラを中心に研究会**を設ける等が考えられる

5. 情報共有は必要であるが、**サイバーテロに関連する**予兆/事案/関連情報に着目して共有し、情報の吸い上げと匿名化による発信だけでなく、**コミュニティの醸成**にも尽力すべき

4.標的型攻撃対策の施策案

○重要インフラ以外の業種についても、例えば、一定規模以上の企業については、以下の事項を義務化すべき。これらの事項についても、NISCを中心に、制度化に向けた検討を早急に行うべき。

1. 事務系ネットワーク

① 対策のガイドラインの遵守

- サイバーセキュリティ経営ガイドライン
- チェックリストの報告義務化

② 事案発生時の報告義務化

- 閾値（回数、データ量）を超えた外部への不審な通信の検知
- 閾値（台数）を超えたPCの感染活動の検知

2. 制御系ネットワーク

① 対策のガイドラインの遵守

- 業種別ガイドラインの策定
- チェックリストの報告義務化

② 事案発生時の報告義務化

- 閾値（台数）を超えたPCの感染活動の検知

5.標的型攻撃対策の施策案に伴う補助的な施策

1. 形だけでないあるべき姿のCISO,CSIRTの定義と普及
   - ① CISO、CSIRTへの**外部監査**
   - ② 実践トレーニングを行う**組織の設置と認定証**発行

2. 職員/従業員の検知/防御能力強化
   - ① **異変に気付く気配り能力**を向上させる仕組み
   - ② サイバー攻撃への**関心を向上**させる仕組み
   - ③ 従業員の能力を向上させる**指導者の育成**

6.サイバーセキュリティ対策の基礎体力向上の施策

1. 国産セキュリティ産業の育成

① 海外製品購入でセキュリティ先進国にはなれない

② 日本では、**利便性とカスタマイズ**要望が非常に高く、
海外製品/サービスでは対応できないことが多い

③ 国産セキュリティ製品・サービスを**国、関連組織が率先して採用すべき（経験と実績、売上の提供）**

④ 課題：技術力と市場性の**目利きをユーザ主体**にすべき

2. セキュリティ人材の育成

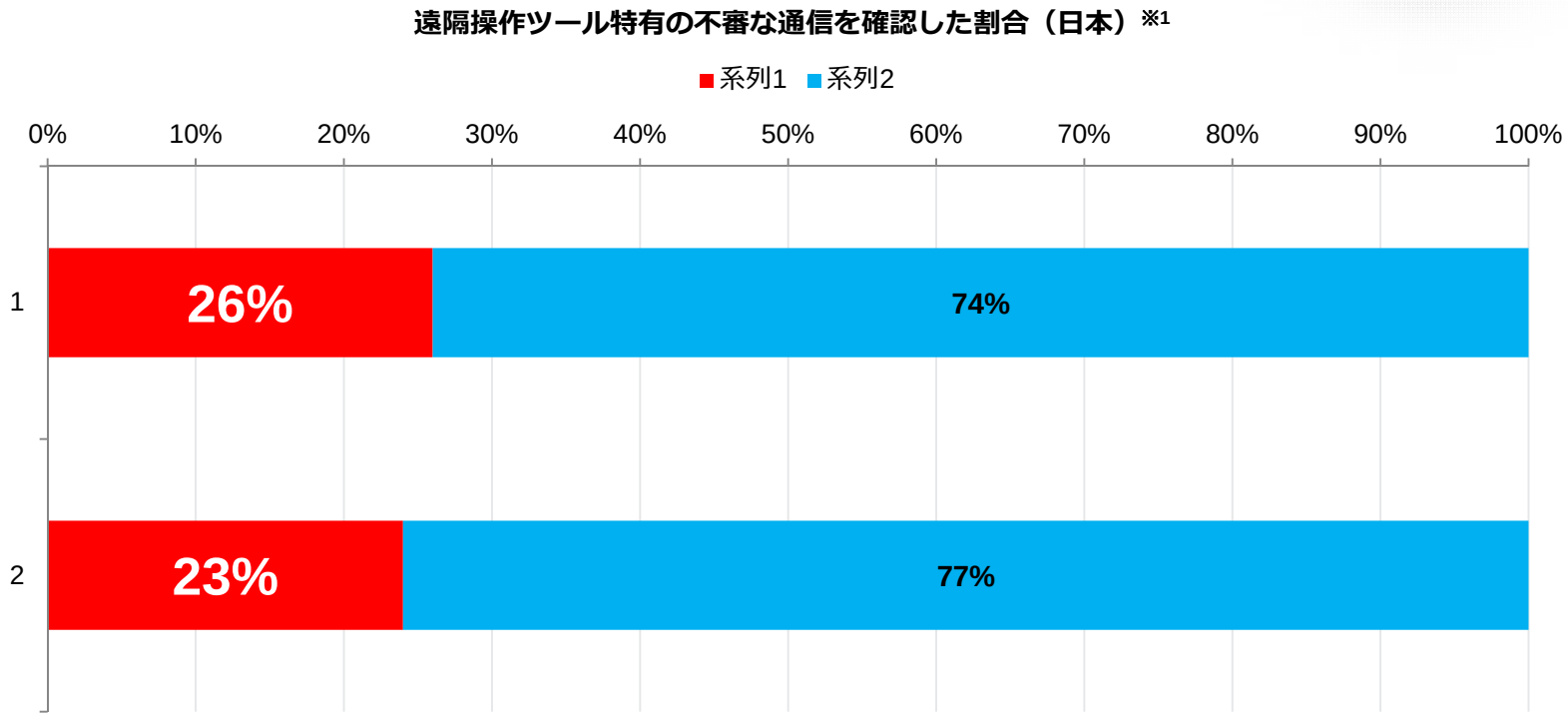
① セキュリティ対策の**推進者**（予算、組織、技術）

② 経営者と技術者の**橋渡し人材**の育成

参考資料１

「継続」する「気づけない攻撃」

- 企業のおよそ**4社に1社**は既に侵入されている※1
- 被害に気づくのは、最初の侵入から**約5か月（平均156日）**が経過したあと※2



※1 2014年1月～12月、2015年1月～12月の期間に、トレンドマイクロが監視サービスを行った事例から無作為に抽出した各100件を調査。
※2 2015年1~7月にトレンドマイクロが標的型攻撃対応支援サービスを行った事例から集計。

参考資料２

- FireEye社の検知装置を取り付けて1ヵ月監視した結果

	メールで攻撃を受けた	外部との不正通信
運輸／物流	100%	**25%**
エネルギー（電力／ガス／石油／新エネルギー）	91%	**62%**
公社／官公庁／学校	78%	**32%**
IT／通信	100%	**50%**
インターネット／広告／メディア	100%	**50%**
医療関連	100%	**43%**
金融	85%	**8%**

FireEye