HUNSLAB INC, の理念

私どもは、21 世紀のセキュリティモデルに必要な環境整備を行い企業、団体の協力を元に、現在脅威となっている様々な課題に技術面での課題解決を行うことを理念として持っています。

その為には、クラウドの利活用によりサービスコスト負担を軽減するモデル化が必須であると考えています。負担を軽減する方法としては、高コストなデザインから分散型ネットワークなどを利用した低コストモデルが有効だと考えています。

今までのセキュリティデザインでは高額な機器やシステムを前提にしていますが、これでは企業のスケールメリットより多額なコストが発生し、成果が出るまでに体力が続かないケースが出てきています。

結果、セキュリティへの予算が削られ、脆弱となったところから、情報漏洩による社会的イメージダウン、侵入、ランサムウェア、マルウェアによる物理データ被害などが起きる確率が増大しています。

HUNSLAB では、既存のネットワーク構成に手を入れず、ネットワークを仮想化し、通信の安全性を最適化する新たなデザインが必要であると考えています。

現在、セキュリティモデルとしては積み上げと組み合わせ型、つまり足し算による防御を前提にしています。その大きな理由は多くのセキュリティ製品や高価な機器を買わせたいという思惑があるからです。

一方、引き算のセキュリティモデルというのも存在します。その為にはゼロトラストという概念を理解する必要があります。

インターネットを利用するには ISP の契約が必要です。私どもは、安全な通信しか許可しない ISP を政府機関に提言しましたが、インターネットの自由を侵すなどと反対されました。

現在の ISP は、インターネットに相互接続のコンセントを作ることしかしてくれません。それは家の電気に例えると、ブレーカーもなく、雷サジ対策の何もない環境で電気を使うという事に似ています。

過電流が流れても遮断するブレーカーが存在しませんから家電製品から発火することがあるかもしれません。

これは、インターネットに置き換えると、ウィルスやマルウェアが ISP の回線を通して侵入し、被害を及ぼすのと全く同じ構図であると理解できるでしょう。

通常、インフラと呼ばれる環境については国が規定する安全基準を設けます。

電気であれば、100V という電圧を提供する義務を負わせています。そこに 500V とかは流してはいけないように様々な対策が電力会社によって行われています。

上水道についても同様です。安心して飲める安全な水の供給には様々な検査を経て、人体に影響のない安全な水を提供しています。

インターネットが社会インフラの一部なってもう 30 年以上になりますが、いまだに安全基準が決められる事無く、利用する際の責任を丸々利用者に責任を押しつけ利用させている事実には驚愕されるばかりです。

総務省が電気通信事業者を保護するという立場はわかりますが、インタネットの利用が政府機関から民間企業そして一般ユーザにまで利用範囲がリテラシーの低い人々向けて展開がなされた現在、安全に利用できるインターネット通信事業を推進するべき時期に来ていることは誰もが感じていることです。

一般のユーザや企業の多くが、海外からの攻撃で、また、ランサムウェアが通信する先も海外の国の IP が利用されています。

こうした防御の多くは、ISP 側で行えるものです。

一般のユーザは、何の知識もなく、インターネットを利用したいということで、ISP と契約しますが、ISP はインターネットが安全に使えるという保証はしてくれません。

HUNSLAB では、安全な通信しかさせない ISP の普及を全世界で推進しています。（しかし、それが出来ない国に対しては、）

一般のユーザ、また企業が安全なインターネット環境を要求しているのに相反した利害によって提供されない現実をどのように改善できるだろうかということで、

ゼロトラスト＝何も信用しない

という画期的なモデルを作ろうと考えました。ただ、この考え方は、ナショナルセキュリティなどの分野では当たり前のデザインとして採用されています。

しかしながら当初は、その設計と構築、また運用には莫大な費用を掛け、セキュリティクリアランスという制度を履行させるなどし、非常に厳格なモデルとして確立されています。欧米諸国ではすでに実施していますが、日本はまだそういう点では遅れをとっている状況です。

上場企業の多くは、様々なセキュリティ製品を導入し、その購入費用、運用、メンテナンスに多くの時間とコストを費消しています。

これでは、企業のセキュリティ担当者は疲弊する一方ですし、また利用者の負担も増大し、そして経営者にとってはコストだけ増大するだけで、何もメリットもない投資では無く損金となってしまっています。

投資ではなく損金損失なのでこれが増大すればするほど企業利益は減少します。

本来の業務を効率させるための IT 化が逆に、情報漏洩やリスク管理などの責務を負わされ、業務効率を落としてしまう結果となっている企業が少なくありません。

複雑なモデルには多くの脆弱性が混在するようになりその多くが、他の製品の問題だとかゼロディ攻撃は防御できないと唱えています。逆にシンプルなモデルでは、機能を限定し、出来ることを定義するホワイト方式＝トラストモデルとして設計するので問題のある箇所を見える可ができるようになります。

例えば、
ChromeBook しかない LAN 環境で、NAS を利用する環境ではウィルスの心配が不要なのでセキュリティデザインがとてもシンプルになります。

弊社の SmartSecret を利用した CENEMO では、既存の LAN 環境の変更を一切しないで導入することが可能です。

そして、現在ご利用いただいている LAN 環境の仮想化に加え、インターネットをより安全にした仮想インターネットをご利用いただけます。

こうしたオーバーレイ構造によって、物理層から隔離された相互に安全な通信を行いたいデバイスのみが参加する仮想インターネットを実現させます。

この仮想空間上にも仮想の FW、フィルタリング機能がご利用いただけます。

HUNSLAB では、安全な DNS の利用、コンテンツのフィルタリング、また利用されるパソコンのセキュリティの向上などを一元的に行う事で、新たなセキュリティ製品を導入する事無く、ナショナルセキュリティ機関で採用されているセキュリティファシリティクリアランスと同様の安全なプラットフォームを届けることを使命とし、それを実現することを理念としています。

HUNSLAB INC.
https://hunslab.net